IPv6 Commands: ipv6 ospf de to ipv6 sp

ipv6 ospf dead-interval

To set the time period for which hello packets must not be seen before neighbors declare the router down, use the **i pv6 ospf dead-interval**command in interface configuration mode. To return to the default time, use the **no** form of this command.

ipv6 ospf dead-interval *seconds*

no ipv6 ospf dead-interval

Syntax Description

seconds	Specifies the interval (in seconds). The value must be the same for all nodes on the network.

Command Default

Four times the interval set by the **ipv6 ospf hello-interval** command

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
15.1(3)S	Use of the **ospfv3 dead-interval**command can affect the **ipv6 ospf dead-interval**command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 dead-interval**command can affect the **ipv6 ospf dead-interval**command.
15.2(1)T	Use of the **ospfv3 dead-interval**command can affect the **ipv6 ospf dead-interval**command.

Usage Guidelines

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

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.

Examples

The following example sets the Open Shortest Path First version 3 (OSPFv3) dead interval to 60 seconds:

```
interface ethernet 1
 ipv6 ospf dead-interval 60
```

Related Commands

Command	Description
ipv6 ospf hello-interval	Specifies the interval between hello packets that the Cisco IOS software sends on the interface.
ospfv3 dead-interval	Sets the time period for which hello packets must not be seen before neighbors declare the router down.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf demand-circuit

To configure Open Shortest Path First (OSPF) to treat the interface as an OSPFv3 demand circuit, use the **ipv6 ospf demand-circuit** command in interface configuration mode. To remove the demand circuit designation from the interface, use the **no** form of this command.

ipv6 ospf demand-circuit[disable] [ignore]

no ipv6 ospf demand-circuit

Syntax Description

disable	(Optional) Disables OSPFv3 from treating the interface as an OSPF v3demand circuit.
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

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
15.1(3)S	Use of the **ospfv3 demand-circuit**command can affect the **ipv6 ospf demand-circuit**command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 demand-circuit**command can affect the **ipv6 ospf demand-circuit**command.
15.2(1)T	Use of the **ospfv3 demand-circuit**command can affect the **ipv6 ospf demand-circuit**command.
Cisco IOS XE Release 3.8S	This command was modified. The **ignore** keyword was added.

Usage Guidelines

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.

On point-to-point interfaces, only one end of the demand circuit must be configured with this 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 sets the configuration for an ISDN on-demand circuit:

```
interface BRI0
 ipv6 ospf 1 area 1
 ipv6 ospf demand-circuit
```

Related Commands

ospfv3 demand-circuit	Configures OSPFv3 to treat the interface as an OSPFv3 demand circuit.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf encryption

To specify the encryption type for an interface, use the **ipv6 ospf encryption** command in interface configuration mode. To remove the encryption type from an interface, use the **no** form of this command.

ipv6 ospf encryption {**ipsec spi** *spi* **esp** {*encryption-algorithm* [[*key-encryption-type*] *key*]| **null**} *authentication-algorithm* [*key-encryption-type*] *key*| **null**}

no ipv6 ospf encryption ipsec spi *spi*

Syntax Description

ipsec	Specifies IP Security (IPsec).
spi *spi*	Specifies the 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-cdc—**Enables AES-CDC encryption. • **3des—**Enables 3DES encryption. • **des—**Enables DES encryption. • **null** —ESP with no encryption.
key-encryption-type	(Optional) One of two values can be entered: • **0** —The key is not encrypted. • **7** —The key is encrypted.
key	(Optional) Number used in the calculation of the message digest. The number is 32 hexadecimal digits (16 bytes) long. The size of the key depends on the encryption algorithm used. Some algorithms, such as AES-CDC, allow you to choose the size of the key.
authentication-algorithm	Encryption authentication algorithm to be used. The values can be one of the following: • **md5** —Enables message digest 5 (MD5) authentication. • **sha1** —Enables Secure Hash Algorithm 1 (SHA-1) authentication.
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
12.4(9)T	This command was introduced.
15.1(3)S	This command was modified. Use of the **ospfv3 encryption** command can affect the **ipv6 ospf encryption** command.
Cisco IOS XE Release 3.4S	This command was modified. Use of the **ospfv3 encryption** command can affect the **ipv6 ospf encryption** command.
15.2(1)T	This command was modified. Use of the **ospfv3 encryption** command can affect the **ipv6 ospf encryption** command.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

When the **ipv6 ospf encryption** command is enabled, both authentication and encryption are enabled.

You need 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 device. 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 **ipv6 ospf encryption null** command.

Examples

The following example shows how to specify 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 SHA-1.

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 ospf encryption ipsec spi 1001 esp null sha1
123456789A123456789B123456789C123456789D
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPFv3 area.
area encryption	Enables encryption for an OSPFv3 area.

Command	Description
area virtual-link authentication	Enables authentication for virtual links in an OSPFv3 area.
ipv6 ospf authentication	Specifies the authentication type for an interface.
ospfv3 encryption	Specifies the encryption type for an interface.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf flood-reduction

To suppress the unnecessary flooding of link-state advertisements (LSAs) in stable topologies, use the **ip v6 ospf flood-reduction** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 ospf flood-reduction

no ipv6 ospf flood-reduction

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
15.1(3)S	Use of the **ospfv3 flood-reduction**command can affect the **ipv6 ospf flood-reduction**command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 flood-reduction**command can affect the **ipv6 ospf flood-reduction**command.
15.2(1)T	Use of the **ospfv3 flood-reduction**command can affect the **ipv6 ospf flood-reduction**command.

Usage Guidelines

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.

All routers supporting the Open Shortest Path First version 3 (OSPFv3) demand circuit are compatible and can interact with routers supporting flooding reduction.

Examples

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

```
interface serial 0
 ipv6 ospf flood-reduction
```

Related Commands

Command	Description
ospfv3 flood-reduction	Suppresses the unnecessary flooding of LSAs in stable topologies.
show ipv6 ospf interface	Displays OSPFv3-related interface information.
show ipv6 ospf neighbor	Displays OSPFv3-neighbor information on a per-interface basis.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf 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 **ip v6 ospf hello-interval** command in interface configuration mode. To return to the default time, use the **no** form of this command.

ipv6 ospf hello-interval *seconds*

no ipv6 ospf hello-interval

Syntax Description

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.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
15.1(3)S	Use of the **ospfv3 mtu-ignore**command can affect the **ipv6 ospf mtu-ignore**command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 mtu-ignore** command can affect the **ipv6 ospf mtu-ignore**command.
15.2(1)T	Use of the **ospfv3 mtu-ignore**command can affect the **ipv6 ospf mtu-ignore**command.

Usage Guidelines

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.

This 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:

```
interface ethernet 1
 ipv6 ospf hello-interval 15
```

Related Commands

Command	Description
ipv6 ospf dead-interval	Sets the time period for which hello packets must not have been seen before neighbors declare the router down.
ospfv3 hello-interval	Specifies the interval between hello packets that the Cisco IOS software sends on the interface.

ipv6 ospf 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 i**p v6 ospf mtu-ignore** command in interface configuration mode. To reset to default, use the **no** form of this command.

ipv6 ospf mtu-ignore

no ipv6 ospf mtu-ignore

Syntax Description

This command has no arguments or keywords.

Command Default

OSPFv3 MTU mismatch detection is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
15.1(3)S	Use of the **ospfv3 mtu-ignore**command can affect the **ipv6 ospf mtu-ignore**command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 mtu-ignore** command can affect the **ipv6 ospf mtu-ignore**command.
15.2(1)T	Use of the **ospfv3 mtu-ignore**command can affect the **ipv6 ospf mtu-ignore**command.

Usage Guidelines

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.

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:

```
interface serial 0/0
 ipv6 ospf mtu-ignore
```

Related Commands

Command	Description
ospfv3 mtu-ignore	Disables OSPFv3 MTU mismatch detection on receiving DBD packets.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf name-lookup

To display Open Shortest Path First (OSPF) router IDs as Domain Naming System (DNS) names, use the **ipv6 ospf name-lookup** command in global configuration mode. To stop displaying OSPF router IDs as DNS names, use the **no** form of this command.

ipv6 ospf name-lookup

no ipv6 ospf name-lookup

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default

Command Modes

Global configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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

This command makes it easier to identify a router because the router is displayed by name rather than by its router ID or neighbor ID.

Examples

The following example configures OSPF to look up DNS names for use in all OSPF show EXEC command displays:

```
ipv6 ospf name-lookup
```

ipv6 ospf neighbor

To configure Open Shortest Path First (OSPF) routers interconnecting to nonbroadcast networks, use the **ip v6 ospf neighbor** command in interface configuration mode. To remove a configuration, use the **no** form of this command.

ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

no ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

Syntax Description

ipv6-address	Link-local IPv6 address of the 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.
priority *number*	(Optional) A number that indicates the router priority value of the nonbroadcast neighbor associated with the IPv6 prefix specified.The default is 0.
poll-interval *seconds*	(Optional) A number value that represents the poll interval time (in seconds). RFC 2328 recommends that this value be much larger than the hello interval. The default is 120 seconds (2 minutes). This keyword does not apply to point-to-multipoint interfaces.
cost *number*	(Optional) Assigns a cost to the neighbor, in the form of an integer from 1 to 65535. Neighbors with no specific cost configured will assume the cost of the interface, based on the **ipv6 ospf cost**command.
database-filter all out	(Optional) Filters outgoing link-state advertisements (LSAs) to an OSPF neighbor.

Command Default

No configuration is specified.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Release	Modification
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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

X.25 and Frame Relay provide an optional broadcast capability that can be configured in the map to allow OSPF to run as a broadcast network. At the OSPF level you can configure the router as a broadcast network.

One neighbor entry must be included in the Cisco IOS software configuration for each known nonbroadcast network neighbor. The neighbor address must be a link-local address of the neighbor.

If a neighboring router has become inactive (hello packets have not been seen for the Router Dead Interval period), hello packets may need to be sent to the dead neighbor. These hello packets will be sent at a reduced rate called *Poll Interval*.

When the router first starts up, it sends only hello packets to those routers with nonzero priority, that is, routers that are eligible to become designated routers (DRs) and backup designated routers (BDRs). After the DR and BDR are selected, the DR and BDR will then start sending hello packets to all neighbors in order to form adjacencies.

The **priority** keyword does not apply to point-to-multipoint interfaces. For point-to-multipoint interfaces, the **cost** keyword and the number argument are the only options that are applicable. The **cost** keyword does not apply to nonbroadcast multiaccess (NBMA) networks.

Examples

The following example configures an OSPF neighboring router:

```
ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

ipv6 ospf network

To configure the Open Shortest Path First version 3 (OSPFv3) network type to a type other than the default for a given medium, use the **i pv6 ospf network** command in interface configuration mode. To return to the default type, use the **no** form of this command.

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

no ipv6 ospf network

Syntax Description

broadcast	Sets the network type to broadcast.
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

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
12.4(15)XF	The **point-to-multipint** keyword was added to support the Virtual Multipoint Interfaces (VMI) and Mobile Adhoc Networking.
12.4(15)T	This command was integrated into Cisco IOS 12.4(15)T.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(3)S	Use of the **ospfv3 network**command can affect the **ipv6 ospf network**command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 network**command can affect the **ipv6 ospf network**command.
15.2(1)T	Use of the **ospfv3 network**command can affect the **ipv6 ospf network**command.

Usage Guidelines

When the ospfv3 networkcommand is configured with the *process-id* argument, it overwrites the ipv6 ospf networkconfiguration if OSPFv3 was attached to the interface using the ipv6 ospf area command.

NBMA Networks

Using this feature, you can configure broadcast networks as NBMA networks when, for example, routers in your network do not support multicast addressing. You can also configure NBMA networks (such as X.25, Frame Relay, and Switched Multimegabit Data Service [SMDS]) as broadcast networks. This feature saves you from needing to configure neighbors.

Configuring NBMA networks as either broadcast or nonbroadcast assumes that there are virtual circuits from every router to every router or fully meshed networks. However, the assumption is not true for other configurations, such as for a partially meshed network. In these cases, you can configure the OSPFv3 network type as a point-to-multipoint network. Routing between two routers that are not directly connected will go through the router that has virtual circuits to both routers. You need not configure neighbors when using this feature.

Point-to-Multipoint Networks

OSPFv3 for IPv6 has two features related to point-to-multipoint networks. One feature applies to broadcast networks; the other feature applies to nonbroadcast networks:

- On point-to-multipoint, broadcast networks, you can use the **neighbor** command, and you must specify a cost to that neighbor.
- On point-to-multipoint, nonbroadcast networks, you must use the **neighbor** command to identify neighbors. Assigning a cost to a neighbor is optional.

Examples

Examples

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

```
interface serial 0
 ipv6 enable
 ipv6 ospf 1 area 0
 ipv6 ospf network broadcast
 encapsulation frame-relay
```

Examples

The following example illustrates a point-to-multipoint network with broadcast:

```
interface serial 0
 ipv6 enable
 ipv6 ospf 1 area 0
 encapsulation frame-relay
 ipv6 ospf cost 100
 ipv6 ospf network point-to-multipoint
 frame-relay map ipv6 2001:0DB1::A8BB:CCFF:FE00:C01 broadcast
 frame-relay map ipv6 2001:0DB1B:CCFF:FE00:C02 broadcast
 frame-relay local-dlci 200
 ipv6 ospf neighbor 2001:0DB1B:CCFF:FE00:C01
 ipv6 ospf neighbor2001:0DB1B:CCFF:FE00:C02
```

Related Commands

Command	Description
frame-relay map	Defines mapping between a destination protocol address and the DLCI used to connect to the destination address.
ipv6 ospf neighbor	Configures OSPFv3 routers interconnecting to nonbroadcast networks.
ospfv3 network	Configures an OSPFv3 network type to a type other than the default for a given medium.
x25 map	Sets up the LAN protocols-to-remote host mapping.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf priority

To set the router priority, which helps determine the designated router for this network, use the **i pv6 ospf priority** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ipv6 ospf priority *number-value*

no ipv6 ospf priority *number-value*

Syntax Description

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

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
15.1(3)S	Use of the **ospfv3 priority**command can affect the **ipv6 ospf priority**command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 priority**command can affect the **ipv6 ospf priority**command.
15.2(1)T	Use of the **ospfv3 priority**command can affect the **ipv6 ospf priority**command.

Usage Guidelines

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 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).

This priority value is used when you configure Open Shortest Path First version 3 (OSPFv3) for nonbroadcast networks using the **ipv6 ospf neighbor** command.

Examples

The following example sets the router priority value to 4:

```
interface ethernet 0
 ipv6 ospf priority 4
```

Related Commands

Command	Description
ipv6 ospf network	Configures the OSPFv3 network type to a type other than the default for a given medium.
ipv6 ospf neighbor	Configures OSPFv3 routers interconnecting to nonbroadcast networks.
ospfv3 priority	Sets the router priority, which helps determine the designated router for this network.

ipv6 ospf 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 **ip v6 ospf retransmit-interval** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ipv6 ospf retransmit-interval *seconds*

no ipv6 ospf retransmit-interval

Syntax Description

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. The default is 5 seconds.

Command Default

The default is 5 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
15.1(3)S	Use of the **ospfv3 retransmit-interval**command can affect the **ipv6 ospf retransmit-interval**command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 retransmit-interval**command can affect the **ipv6 ospf retransmit-interval**command.
15.2(1)T	Use of the **ospfv3 retransmit-interval**command can affect the **ipv6 ospf retransmit-interval**command.

Usage Guidelines

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 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 this 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:

```
interface ethernet 2
 ipv6 ospf retransmit-interval 8
```

Related Commands

Command	Description
ospfv3 retransmit-interval	Specifies the time between LSA retransmissions for adjacencies belonging to the interface.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 ospf 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 **i p ospf transmit-delay** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ipv6 ospf transmit-delay *seconds*

no ipv6 ospf transmit-delay

Syntax Description

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

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
15.1(3)S	Use of the **ospfv3 transmit-delay**command can affect the **ipv6 ospf transmit-delay**command.
Cisco IOS XE Release 3.4S	Use of the **ospfv3 transmit-delay** command can affect the **ipv6 ospf transmit-delay**command.
15.2(1)T	Use of the **ospfv3 transmit-delay**command can affect the **ipv6 ospf transmit-delay**command.

Usage Guidelines

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.

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:

```
interface ethernet 0
 ipv6 ospf transmit-delay 3
```

Related Commands

Command	Description
ospfv3 transmit-delay	Sets the estimated time required to send a link-state update packet on the interface.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

ipv6 pim

To reenable IPv6 Protocol Independent Multicast (PIM) on a specified interface, use the **ipv6 pim**command in interface configuration mode. To disable PIM on a specified interface, use the **no** form of the command.

ipv6 pim

no ipv6 pim

Syntax Description

This command has no arguments or keywords.

Command Default

PIM is automatically enabled on every interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)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 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

After a user has enabled the **ipv6 multicast-routing** command, PIM is enabled to run on every interface. Because PIM is enabled on every interface by default, use the **no** form of the **ipv6 pim** command to disable PIM on a specified interface. When PIM is disabled on an interface, it does not react to any host membership notifications from the Multicast Listener Discovery (MLD) protocol.

Examples

The following example turns off PIM on Fast Ethernet interface 1/0:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# no ipv6 pim
```

Related Commands

Command	Description
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.

ipv6 pim accept-register

To accept or reject registers at the rendezvous point (RP), use the **ipv6 pim accept-register**command in global configuration mode. To return to the default value, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **accept-register** {**list** *access-list*| **route-map** *map-name*}

no ipv6 pim [**vrf** *vrf-name*] **accept-register** {**list** *access-list*| **route-map** *map-name*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
list *access-list*	Defines the access list name.
route-map *map-name*	Defines the route map.

Command Default

All sources are accepted at the RP.

Command Modes

Global configuration

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.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **ipv6 pim accept-register**command to configure a named access list or route map with match attributes. When the permit conditions as defined by the *access-list* and *map-name* arguments are met, the register message is accepted. Otherwise, the register message is not accepted, and an immediate register-stop message is returned to the encapsulating designated router.

Examples

The following example shows how to filter on all sources that do not have a local multicast Border Gateway Protocol (BGP) prefix:

```
ipv6 pim accept-register route-map reg-filter
route-map reg-filter permit 20
 match as-path 101
ip as-path access-list 101 permit
```

ipv6 pim allow-rp

To enable the PIM Allow RP feature for all IP multicast-enabled interfaces in an IPv6 device, use the **ip pim allow-rp** command in global configuration mode. To return to the default value, use the **no** form of this command.

ipv6 pim allow-rp [**group-list** *access-list*| **rp-list** *access-list* [**group-list** *access-list*]]

no ipv6 pim allow-rp

Syntax Description

group-list	(Optional) Identifies an access control list (ACL) of allowed group ranges for PIM Allow RP.
rp-list	(Optional) Specifies an ACL for allowed rendezvous-point (RP) addresses for PIM Allow RP.
access-list	(Optional) Unique number or name of a standard ACL.

Command Default

PIM Allow RP is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Usage Guidelines

Use this command to enable the receiving device in an IP multicast network to accept a (*, G) Join from an unexpected (different) RP address.

Before enabling PIM Allow RP, you must first use the **ipv6 pim rp-address** command to define an RP.

Examples

NEED CONFIG EXAMPLE HERE

Related Commands

Command	Description
ipv6 pim rp-address	Statically configures the address of a PIM RP for multicast groups.

ipv6 pim anycast-RP

To configure the address of the Protocol-Independent Multicast (PIM) rendezvous point (RP) for an anycast group range, use the **ipv6 pim anycast-RP** command in global configuration mode. To remove an RP address for an anycast group range, use the **no** form of this command.

ipv6 pim anycast-RP {*rp-address peer-address*}

no ipv6 pim anycast-RP

Syntax Description

anycast-rp-address	Anycast RP set for the RP assigned to the group range. This is the address that first-hop and last-hop PIM routers use to register and join.
peer-address	The address to which register messages copies are sent. This address is any address assigned to the RP router, not including the address assigned using the *anycast-rp-address* variable.

Command Default

No PIM RP address is configured for an anycast group range.

Command Modes

Global configuration (config)

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

Usage Guidelines

The anycast RP feature is useful when interdomain connection is not required. Use this command to configure the address of the PIM RP for an anycast group range.

Examples

```
Router# ipv6 pim anycast-rp 2001:DB8::1:1 2001:DB8::3:3
```

Related Commands

Command	Description
show ipv6 pim anycast-RP	Verifies IPv6 PIM RP anycast configuration.

ipv6 pim bsr border

To configure a border for all bootstrap message (BSMs) of any scope on a specified interface, use the **ipv6 pim bsr border**command in interface configuration mode. To remove the border, use the **no** form of this command.

ipv6 pim bsr border

no ipv6 pim bsr border

Syntax Description

This command has no argument or keywords.

Command Default

No border is configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(28)S	This command was introduced.

Command History

12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
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 integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **ipv6 pim bsr border** command is used to configure a border to all global and scoped BSMs. The command filters incoming or outgoing BSMs, preventing the BSMs from being forwarded or accepted on the interface on which the **ipv6 pim bsr border** command is configured.

Examples

The following example configures a BSR border on Ethernet interface 1/0:

```
Router(config)# interface Ethernet1/0
 Router(config-if)# ipv6 pim bsr border
 Router(config-if)# end
Router# show running-config interface e1/0
 Building configuration...
 Current configuration :206 bytes
 !
 interface Ethernet1/0
 ipv6 address 2:2:2::2/64
 ipv6 enable
 ipv6 rip test enable
 ipv6 pim bsr border
 no cdp enable
 end
```

Related Commands

Command	Description
ipv6 pim bsr candidate bsr	Configures a router as a candidate BSR.
ipv6 pim bsr candidate rp	Sends PIM RP advertisements to the BSR.

ipv6 pim bsr candidate bsr

To configure a device to be a candidate bootstrap device (BSR), use the **ipv6 pim bsr candidate bsr**command in global configuration mode. To remove this device as a candidate BSR, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*] **[scope]** [**accept-rp-candidate** *acl-name*]

no ipv6 pim [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*] **[scope]** [**accept-rp-candidate** *acl-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
ipv6-address	The IPv6 address of the device to be configured as a candidate BSR. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
hash-mask-length	(Optional) The length (in bits) of the mask to use in the BSR hash function. The default value is 126.
priority	(Optional) Priority of the candidate BSR.
priority-value	(Optional) Integer from 0 through 192. The BSR with the larger priority is preferred. If the priority values are the same, the device with the larger IPv6 address is the BSR. The default value is 0.
scope	(Optional) BSR will originate bootstrap messages (BSMs), including the group range associated with the scope, and accept candidate RP (C-RP) announcements only if they are for groups that belong to the given scope.
accept-rp-candidate *acl-name*	(Optional) BSR C-RP advertisements will be filtered at the BSR using the named access list (*acl-name*) for the RP candidates.

Command Default

Device is not enabled as a BSR.

Command Modes

Global configuration

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
12.2(18)SXE	The **scope** keyword and *scope-value* argument were added.
12.4	The **scope** keyword and *scope-value* argument are no longer available in syntax.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
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.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.2(1)S	This command was modified. The **accept-rp-candidate** keyword was added.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

This command is used to configure a device as a candidate BSR; however, the device becomes a candidate only if the address belongs to a PIM-enabled interface. When a device is configured, it will participate in BSR election. If elected BSR, this device will periodically originate BSR messages advertising the group-to-RP mappings it has learned through candidate-RP-advertisement messages.

If the **scope** keyword is enabled, the BSR will originate BSMs, including the group range associated with the scope, and accept C-RP announcements only if they are for groups that belong to the given scope. If no scope is configured, all scopes are used.

The **accept-rp-candidate** *acl-name* keyword and argument will restrict the C-RP candidates accepted. If the **accept-rp-candidate** keyword is not configured, BSR C-RP advertisements at the BSR are not filtered.

Examples

The following example configures the device with the IPv6 address 2001:0DB8:3000:3000::42 as the candidate BSR, with a hash mask length of 124 and a priority of 10:

```
ipv6 pim bsr candidate bsr 2001:0DB8:3000:3000::42 124 priority 10
```

The following example will restrict the C-RP advertisements accepted. The ACL, crp, is used to filter the advertisements.

```
ipv6 pim bsr candidate bsr 194::1:1:2 priority 150 accept-rp-candidate crp
acl crp with
permit ipv6 host 192::1:1:1 any log
deny ipv6 any any log
```

Related Commands

Command	Description
ipv6 pim bsr border	Configures a border for all bootstrap message BSMs of any scope.
ipv6 pim bsr candidate rp	Sends PIM RP advertisements to the BSR.

ipv6 pim bsr candidate rp

To configure the candidate rendezvous point (RP) to send Protocol Independent Multicast (PIM) RP advertisements to the bootstrap device (BSR), use the **ipv6 pim bsr candidate rp** command in global configuration mode. To disable PIM RP advertisements to the BSR, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] **[bidir]**

no ipv6 pim [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] **[bidir]**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
ipv6-address	The IPv6 address of the device to be advertised as the candidate RP (C-RP). This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
group-list	(Optional) List of group prefixes. When the **bidir** keyword is not enabled, the **group-list** keyword with the *access-list-name* argument is advertised in the sparse range. If no access list is specified, all valid multicast nonsource-specific multicast (SSM) address ranges are advertised in association with the specified RP address.
access-list-name	(Optional) Name of the IPv6 access list containing group prefixes that will be advertised in association with the RP address. Names cannot contain a space or quotation mark, or begin with a numeral. When the **bidir** keyword is not enabled, the **group-list** keyword with the *access-list-name* argument is advertised in the sparse range. If the access list contains any group address ranges that overlap the assigned SSM group address range (FF3x::/96), a warning message is displayed, and the overlapping address ranges are ignored.
priority	(Optional) Priority of the candidate BSR.

priority-value	(Optional) Integer from 0 through 192 that specifies the priority. The RP with the higher priority is preferred. If the priority values are the same, the device with the higher IPv6 address is the RP. The default value is 192.
interval	(Optional) Configures the C-RP advertisement interval.
seconds	(Optional) Advertisement interval in number of seconds.
scope	(Optional) Device advertises itself as the C-RP only to the BSR for the specified scope.
scope-value	(Optional) Integer from 3 through 15 that specifies the scope.
bidir	(Optional) Device advertises itself as the C-RP for the **group-list** *access-list-name* in the bidirectional range.

Command Default

Device is not enabled as a candidate RP. If no scope is configured, all scopes are advertised.

Command Modes

Global configuration

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
12.2(18)SXE	The **scope** and **bidir** keywords were added. The *scope-value* argument was added.
12.4	The **scope** keyword and *scope-value* argument are no longer available in syntax.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
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)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Release	Modification
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use this command to send PIM RP advertisements to the BSR. The PIM RP advertisement becomes a candidate only if the address belongs to a PIM-enabled interface.

The group prefixes defined by the *access-list-name* argument will also be advertised in association with the RP address. If a group prefix in the access list is denied, it will not be included in the C-RP advertisement.

If the **priority***priority-value* keyword and argument are specified, then the device will announce itself to be a candidate RP with the specified priority.

If the **scope** keyword is used, the device advertises itself as the C-RP only to the BSR for the specified scope. If the **group-list**keyword is specified along with the scope, then only prefixes in the *access-list-name* argument with the same scope as the scope configured will be advertised. If no scope is configured, all scopes are advertised.

Examples

The following example configures the device with the IPv6 address 2001:0DB8:3000:3000::42 to be advertised as the candidate RP, with a priority of 0:

```
Device(config)# ipv6 pim bsr candidate rp 2001:0DB8:3000:3000::42 priority 0
```

The following example configures the device with the IPv6 address 2001:0DB8:1:1:1 as the candidate RP for scope 6 for the group ranges specified in the access list named list1:

```
Device(config)# ipv6 pim bsr candidate rp 2001:0DB8:1:1:1 group-list list1 scope 6
```

Related Commands

Command	Description
ipv6 pim bsr candidate bsr	Configures a device as a candidate BSR.
ipv6 pim bsr border	Configures a border for all BSMs of any scope.

ipv6 pim dr-priority

To configure the designated router (DR) priority on a Protocol Independent Multicast (PIM) router, use the **ipv6 pim dr-priority** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 pim dr-priority *value*

no ipv6 pim dr-priority

Syntax Description

value	An integer value to represent DR priority. Value range is from 0 to 4294967294. The default value is 1.

Command Default

Default value is 1.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)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 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.

Usage Guidelines

The **ipv6 pim dr-priority** command configures the neighbor priority used for PIM DR election. The router with the highest DR priority on an interface becomes the PIM DR. If several routers have the same priority, then the router with the highest IPv6 address on the interface becomes the DR.

If a router does not include the DR priority option in its hello messages, then the router is considered to be the highest-priority router and becomes the DR. If several routers do not include the DR priority option in their hello messages, then the router with the highest IPv6 address becomes the DR.

Examples

The following example configures the router to use DR priority 3:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 pim dr-priority 3
```

Related Commands

Command	Description
ipv6 pim hello-interval	Configures the frequency of PIM hello messages on an interface.

ipv6 pim hello-interval

To configure the frequency of Protocol Independent Multicast (PIM) hello messages on an interface, use the **ipv6 pim hello-interval** command in interface configuration mode. To return to the default interval, use the **no** form of this command.

ipv6 pim hello-interval *seconds*

no ipv6 pim hello-interval *seconds*

Syntax Description

seconds	Interval, in seconds, at which PIM hello messages are sent.

Command Default

Hello messages are sent at 30-second intervals with small random jitter.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)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 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Periodic hello messages are sent out at 30-second intervals with a small jitter. The **ipv6 pim hello-interval**command allows users to set a periodic interval.

Examples

The following example sets the PIM hello message interval to 45 seconds:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 pim hello-interval 45
```

Related Commands

Command	Description
ipv6 mld query-interval	Configures the frequency at which the Cisco IOS software sends MLD host-query messages.
ipv6 pim dr-priority	Configures the DR priority on a PIM router.
show ipv6 pim neighbor	Displays the PIM neighbors discovered by the Cisco IOS software.

ipv6 pim join-prune-interval

To configure periodic join and prune announcement intervals for a specified interface, use the **ipv6 pim join-prune-interval**command in interface configuration mode. To return to the default value, use the **no** form of the command.

ipv6 pim join-prune-interval *seconds*

no ipv6 pim join-prune-interval *seconds*

Syntax Description

seconds	The join and prune announcement intervals, in number of seconds. The default value is 60 seconds.

Command Default

The default is 60 seconds.

Command Modes

Interface configuration

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(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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Periodic join and prune announcements are sent out at 60-second intervals. The **ipv6 pim join-prune-interval** commandallows users to set a periodic interval.

Examples

The following example sets the join and prune announcement intervals to 75 seconds:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 pim join-prune-interval 75
```

ipv6 pim neighbor-filter list

To filter Protocol Independent Multicast (PIM) neighbor messages from specific IPv6 addresses, use the **ipv6 pim neighbor-filter** command in the global configuration mode. To return to the router default, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **neighbor-filter list** *access-list*

no ipv6 pim [**vrf** *vrf-name*] **neighbor-filter list** *access-list*

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
access-list	Name of an IPv6 access list that denies PIM hello packets from a source.

Command Default

PIM neighbor messages are not filtered.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **ipv6 pim neighbor-filter list**command is used to prevent unauthorized routers on the LAN from becoming PIM neighbors. Hello messages from addresses specified in this command are ignored.

Examples

The following example causes PIM to ignore all hello messages from IPv6 address FE80::A8BB:CCFF:FE03:7200:

```
Router(config)# ipv6 pim neighbor-filter list nbr_filter_acl
Router(config)# ipv6 access-list nbr_filter_acl
Router(config-ipv6-acl)# deny ipv6 host FE80::A8BB:CCFF:FE03:7200 any
Router(config-ipv6-acl)# permit any any
```

ipv6 pim passive

To enable the Protocol Independent Multicast (PIM) passive feature on a specific interface, use the **ipv6 pim passive**command in interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 pim passive

no ipv6 pim passive

Syntax Description

This command has no arguments or keywords.

Command Default

PIM passive mode is not enabled on the router.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

Use the **ipv6 pim passive**command to configure IPv6 PIM passive mode on an interface.

A PIM passive interface does not send or receive any PIM control messages. However, a PIM passive interface acts as designated router (DR) and designated forwarder (DF)-election winner, and it can accept and forward multicast data.

Examples

The following example configures IPv6 PIM passive mode on an interface:

```
Router(config)# interface gigabitethernet 1/0/0
Router(config-if)# ipv6 pim passive
```

Related Commands

Command	Description
ipv6 multicast pim-passive-enable	Enables the PIM passive feature on an IPv6 router.

ipv6 pim rp embedded

To enable embedded rendezvous point (RP) support in IPv6 Protocol Independent Multicast (PIM), use the **ipv6 pim rp-embedded**command in global configuration mode. To disable embedded RP support, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **rp embedded**

no ipv6 pim [**vrf** *vrf-name*] **rp embedded**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Default

Embedded RP support is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
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 integrated into Cisco IOS XE Release 2.1.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Because embedded RP support is enabled by default, users will generally use the **no** form of this command to turn off embedded RP support.

The **ipv6 pim rp embedded**command applies only to the embedded RP group ranges ff7X::/16 and fffX::/16. When the router is enabled, it parses groups in the embedded RP group ranges ff7X::/16 and fffX::/16, and extracts the RP to be used from the group address.

Examples

The following example disables embedded RP support in IPv6 PIM:

```
no ipv6 pim rp embedded
```

ipv6 pim rp-address

To configure the address of a Protocol Independent Multicast (PIM) rendezvous point (RP) for a particular group range, use the **ipv6 pim rp-address** command in global configuration mode. To remove an RP address, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-access-list*] **[bidir]**

no ipv6 pim rp-address *ipv6-address* [*group-access-list*] **[bidir]**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
ipv6-address	The IPv6 address of a router to be a PIM RP. The *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.
group-access-list	(Optional) Name of an access list that defines for which multicast groups the RP should be used. If the access list contains any group address ranges that overlap the assigned source-specific multicast (SSM) group address range (FF3x::/96), a warning message is displayed, and the overlapping ranges are ignored. If no access list is specified, the specified RP is used for all valid multicast non-SSM address ranges. To support embedded RP, the router configured as the RP must use a configured access list that permits the embedded RP group ranges derived from the embedded RP address. Note that the embedded RP group ranges need not include all the scopes (for example, 3 through 7).
bidir	(Optional) Indicates that the group range will be used for bidirectional shared-tree forwarding; otherwise, it will be used for sparse-mode forwarding. A single IPv6 address can be configured to be RP only for either bidirectional or sparse-mode group ranges. A single group-range list can be configured to operate either in bidirectional or sparse mode.

Command Default

No PIM RPs are preconfigured. Embedded RP support is enabled by default when IPv6 PIM is enabled (where embedded RP support is provided). Multicast groups operate in PIM sparse mode.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)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	Embedded RP support was added.
12.3(7)T	The **bidir** keyword was added to Cisco IOS Release 12.3(7)T.
12.2(25)S	The **bidir** keyword was added to 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 integrated into Cisco IOS XE Release 2.1.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.

Usage Guidelines

When PIM is configured in sparse mode, you must choose one or more routers to operate as the RP. An RP is a single common root of a shared distribution tree and is statically configured on each router.

Where embedded RP support is available, only the RP needs to be statically configured as the RP for the embedded RP ranges. No additional configuration is needed on other IPv6 PIM routers. The other routers will discover the RP address from the IPv6 group address. If these routers want to select a static RP instead of the embedded RP, the specific embedded RP group range must be configured in the access list of the static RP.

The RP address is used by first-hop routers to send register packets on behalf of source multicast hosts. The RP address is also used by routers on behalf of multicast hosts that want to become members of a group. These routers send join and prune messages to the RP.

If the optional *group-access-list* argument is not specified, the RP is applied to the entire routable IPv6 multicast group range, excluding SSM, which ranges from FFX[3-f]::/8 to FF3X::/96. If the *group-access-list* argument is specified, the IPv6 address is the RP address for the group range specified in the *group-access-list* argument.

You can configure Cisco IOS software to use a single RP for more than one group. The conditions specified by the access list determine which groups the RP can be used for. If no access list is configured, the RP is used for all groups.

A PIM router can use multiple RPs, but only one per group.

Examples

The following example shows how to set the PIM RP address to 2001::10:10 for all multicast groups:

```
Router(config)# ipv6 pim rp-address 2001::10:10
```

The following example sets the PIM RP address to 2001::10:10 for the multicast group FF04::/64 only:

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# permit ipv6 any ff04::/64
Router(config)# ipv6 pim rp-address 2001::10:10 acc-grp-1
```

The following example shows how to configure a group access list that permits the embedded RP ranges derived from the IPv6 RP address 2001:0DB8:2::2:

```
Router(config)# ipv6 pim rp-address 2001:0DB8:2::2 embd-ranges
Router(config)# ipv6 access-list embd-ranges
Router(config-ipv6-acl)# permit ipv6 any ff73:240:2:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff74:240:2:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff75:240:2:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff76:240:2:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff77:240:2:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff78:240:2:2:2::/96
```

The following example shows how to enable the address 100::1 as the bidirectional RP for the entries multicast range FF::/8:

```
ipv6 pim rp-address 100::1 bidir
```

In the following example, the IPv6 address 200::1 is enabled as the bidirectional RP for the ranges permitted by the access list named bidir-grps. The ranges permitted by this list are ff05::/16 and ff06::/16.

```
Router(config)# ipv6 access-list bidir-grps
Router(config-ipv6-acl)# permit ipv6 any ff05::/16
Router(config-ipv6-acl)# permit ipv6 any ff06::/16
Router(config-ipv6-acl)# exit
Router(config)# ipv6 pim rp-address 200::1 bidir-grps bidir
```

Related Commands

Command	Description
debug ipv6 pim df-election	Displays debug messages for PIM bidirectional DF-election message processing.
ipv6 access-list	Defines an IPv6 access list and places the router in IPv6 access list configuration mode.
show ipv6 pim df	Displays the DF -election state of each interface for each RP.
show ipv6 pim df winner	Displays the DF-election winner on each interface for each RP.

ipv6 pim spt-threshold infinity

To configure when a Protocol Independent Multicast (PIM) leaf router joins the shortest path tree (SPT) for the specified groups, use the **ipv6 pim spt-threshold infinity**command in global configuration mode. To restore the default value, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **spt-threshold infinity** [**group-list** *access-list-name*]

no ipv6 pim spt-threshold infinity

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
group-list *access-list-name*	(Optional) Indicates to which groups the threshold applies. Must be a standard IPv6 access list name. If the value is omitted, the threshold applies to all groups.

Command Default

When this command is not used, the PIM leaf router joins the SPT immediately after the first packet arrives from a new source. Once the router has joined the SPT, configuring the **ipv6 pim spt-threshold infinity**command will not cause it to switch to the shared tree.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)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 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Release	Modification
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.

Usage Guidelines

Using the **ipv6 pim spt-threshold infinity**command enables all sources for the specified groups to use the shared tree. The **group-list** keyword indicates to which groups the SPT threshold applies.

The *access-list-name*argument refers to an IPv6 access list. When the *access-list-name*argument is specified with a value of 0, or the **group-list** keyword is not used, the SPT threshold applies to all groups. The default setting (that is, when this command is not enabled) is to join the SPT immediately after the first packet arrives from a new source.

Examples

The following example configures a PIM last-hop router to stay on the shared tree and not switch to the SPT for the group range ff04::/64.:

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# permit ipv6 any FF04::/64
Router(config-ipv6-acl)# exit
Router(config)# ipv6 pim spt-threshold infinity group-list acc-grp-1
```

ipv6 policy route-map

To configure IPv6 policy-based routing (PBR) on an interface, use the **ipv6 policy route-map** command in interface configuration mode. To disable IPv6 PBR on an interface, use the **no** form of this command.

ipv6 policy route-map *route-map-name*

no ipv6 policy route-map *route-map-name*

Syntax Description

route-map-name	Name of the route map to be used for PBR. The name must match the *map-tag* value specified by a **route-map** command.

Command Default

Policy-based routing does not occur on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

You can enable PBR if you want your packets to take a route other than the obvious shortest path.

The **ipv6 policy route-map** command identifies a route map to be used for policy-based routing. The **route-map** commands each have a list of **match** and **set** commands associated with them. The **match** commands specify the match criteria, which are the conditions under which PBR is allowed for the interface. The **set** commands specify set actions, which are the PBR actions to be performed if the criteria enforced by the **match** commands are met. The **no ipv6 policy route-map** command deletes the pointer to the route map.

Policy-based routing can be performed on any match criteria that can be defined in an IPv6 access list.

Examples

In the following example, a route map named pbr-dest-1 is created and configured, specifying the packet match criteria and the desired policy-route action. Then, PBR is enabled on the interface Ethernet0/0.

```
ipv6 access-list match-dest-1
  permit ipv6 any 2001:DB8::1
route-map pbr-dest-1 permit 10
  match ipv6 address match-dest-1
  set interface Ethernet0/0
interface Ethernet0/0
  ipv6 policy-route-map pbr-dest-1
```

Related Commands

Command	Description
ipv6 local policy route-map	Identifies the route map to be used for local IPv6 PBR.
match ipv6 address	Specifies an IPv6 access list to be used to match IPv6 packets for PBR.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Specifies the default interface to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Specifies the default interface to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ipv6 next-hop	Specifies the default interface to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

ipv6 port-map

To establish port-to-application mapping (PAM) for the system, use the **ipv6 port-map** command in global configuration mode. To delete user-defined PAM entries, use the **no** form of this command.

ipv6 port-map *application* **port** *port-num* [**list** *acl-name*]

no ipv6 port-map *application* **port** *port-num* [**list** *acl-name*]

Syntax Description

application	Specifies the predefined application that requires port mapping.
port *port-num*	Specifies a port number. The range is from 1 to 65535.
list *acl-name*	(Optional) Specifies the name of the IPv6 access list (ACL) associated with the port mapping.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

The **ipv6 port-map** command associates TCP or User Datagram Protocol (UDP) port numbers with applications or services, establishing a table of default port mapping information at the firewall. This information is used to support network environments that run services using ports that are different from the registered or well-known ports associated with a service or application.

The port mapping information in the PAM table is of one of three types:

- System-defined
- User-defined
- Host-specific

System-Defined Port Mapping

Initially, PAM creates a set of system-defined entries in the mapping table using well-known or registered port mapping information set up during the system start-up. The Cisco IOS Firewall Context-Based Access Control feature requires the system-defined mapping information to function properly. System-defined mapping information cannot be deleted or changed; that is, you cannot map HTTP services to port 21 (FTP) or FTP services to port 80 (HTTP).

The table below lists the default system-defined services and applications in the PAM table.

Table 1: System-Defined Port Mapping

Application Name	Well-Known or Registered Port Number	Protocol Description
cuseeme	7648	CU-SeeMe Protocol
exec	512	Remote Process Execution
ftp	21	File Transfer Protocol (control port)
h323	1720	H.323 Protocol (for example, MS NetMeeting, Intel Video Phone)
http	80	Hypertext Transfer Protocol
login	513	Remote login
msrpc	135	Microsoft Remote Procedure Call
netshow	1755	Microsoft NetShow
real-audio-video	7070	RealAudio and RealVideo
sccp	2000	Skinny Client Control Protocol (SCCP)
smtp	25	Simple Mail Transfer Protocol (SMTP)
sql-net	1521	SQL-NET
streamworks	1558	StreamWorks Protocol
sunrpc	111	SUN Remote Procedure Call
tftp	69	Trivial File Transfer Protocol
vdolive	7000	VDOLive Protocol

Note You can override the system-defined entries for a specific host or subnet using the **list** keyword in the **ipv6 port-map** command.

User-Defined Port Mapping

Network applications that use non-standard ports require user-defined entries in the mapping table. Use the **ipv6 port-map** command to create default user-defined entries in the PAM table.

To map a range of port numbers with a service or application, you must create a separate entry for each port number.

Note If you try to map an application to a system-defined port, a message appears warning you of a mapping conflict.

Use the **no** form of the **ipv6 port-map** command to delete user-defined entries from the PAM table.

To overwrite an existing user-defined port mapping, use the **ipv6 port-map** command to associate another service or application with the specific port.

Host-Specific Port Mapping

User-defined entries in the mapping table can include host-specific mapping information, which establishes port mapping information for specific hosts or subnets. In some environments, it might be necessary to override the default port mapping information for a specific host or subnet, including a system-defined default port mapping information. Use the **list** keyword for the **ipv6 port-map** command to specify an ACL for a host or subnet that uses PAM.

Note If the host-specific port mapping information is the same as existing system-defined or user-defined default entries, host-specific port changes have no effect.

Examples

The following user-defined port-mapping configuration map port 8080 to the HTTP application:

```
ipv6 port-map http port 8080
```

Host-specific port-mapping configuration maps port 2121 to the FTP application from a particular set of host. First, the user needs to create a permit IPv6 access list for the allowed host(s). In the following example, packets from the hosts in the 2001:0DB8:1:7 subset destined for port 2121 will be mapped to the FTP application:

```
Router(config)# ipv6 access-list ftp-host
Router(config-ipv6-acl)# permit 2001:0DB8:1:7::/64 any
```

The port-map configuration is then configured as follows:

```
Router(config)# ipv6 port-map ftp port 2121 list ftp-host
```

Related Commands

Command	Description
show ipv6 port-map	Displays IPv6 port-mapping information.

ipv6 prefix-list

To create an entry in an IPv6 prefix list, use the **ipv6 prefix-list** command in global configuration mode. To delete the entry, use the **no** form of this command.

ipv6 prefix-list *list-name* [**seq** *seq-number*] {**deny** *ipv6-prefix*/*prefix-length*| **permit** *ipv6-prefix*/*prefix-length*| **description** *text*} [**ge** *ge-value*] [**le** *le-value*]

no ipv6 prefix-list *list-name*

Syntax Description

list-name	Name of the prefix list. • Cannot be the same name as an existing access list. • Cannot be the name “detail” or “summary” because they are keywords in the **show ipv6 prefix-list** command.
seq *seq-number*	(Optional) Sequence number of the prefix list entry being configured.
deny	Denies networks that matches the condition.
permit	Permits networks that matches the condition.
ipv6-prefix	The IPv6 network assigned to the specified prefix list. 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). A slash mark must precede the decimal value.
description *text*	A description of the prefix list that can be up to 80 characters in length.
ge *ge-value*	(Optional) Specifies a prefix length greater than or equal to the *ipv6-prefix*/*prefix-length* arguments. It is the lowest value of a range of the *length* (the “from” portion of the length range).

le *le-value*	(Optional) Specifies a prefix length less than or equal to the *ipv6-prefix /prefix-length* arguments. It is the highest value of a range of the *length* (the "to" portion of the length range).

Command Default

No prefix list is created.

Command Modes

Global configuration (config)

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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 prefix-list** command is similar to the **ip prefix-list** command, except that it is IPv6-specific.

To suppress networks from being advertised in updates, use the **distribute-list out** command.

The sequence number of a prefix list entry determines the order of the entries in the list. The router compares network addresses to the prefix list entries. The router begins the comparison at the top of the prefix list, with the entry having the lowest sequence number.

If multiple entries of a prefix list match a prefix, the entry with the lowest sequence number is considered the real match. Once a match or deny occurs, the router does not go through the rest of the prefix list. For efficiency, you may want to put the most common permits or denies near the top of the list, using the *seq-number* argument.

The **show ipv6 prefix-list** command displays the sequence numbers of entries.

IPv6 prefix lists are used to specify certain prefixes or a range of prefixes that must be matched before a permit or deny statement can be applied. Two operand keywords can be used to designate a range of prefix lengths to be matched. A prefix length of less than, or equal to, a value is configured with the **le** keyword. A prefix length greater than, or equal to, a value is specified using the **ge** keyword. The **ge** and **le** keywords can be used to specify the range of the prefix length to be matched in more detail than the usual *ipv6-prefix*/*prefix-length* argument. For a candidate prefix to match against a prefix list entry three conditions can exist:

- The candidate prefix must match the specified prefix list and prefix length entry.
- The value of the optional **le** keyword specifies the range of allowed prefix lengths from the *prefix-length* argument up to, and including, the value of the **le** keyword.
- The value of the optional **ge** keyword specifies the range of allowed prefix lengths from the value of the **ge** keyword up to, and including, 128.

Note The first condition must match before the other conditions take effect.

An exact match is assumed when the **ge** or **le** keywords are not specified. If only one keyword operand is specified then the condition for that keyword is applied, and the other condition is not applied. The *prefix-length* value must be less than the **ge** value. The **ge** value must be less than, or equal to, the **le** value. The **le** value must be less than or equal to 128.

Every IPv6 prefix list, including prefix lists that do not have any permit and deny condition statements, has an implicit deny any any statement as its last match condition.

Examples

The following example denies all routes with a prefix of ::/0.

```
Router(config)# ipv6 prefix-list abc deny ::/0
```

The following example permits the prefix 2002::/16:

```
Router(config)# ipv6 prefix-list abc permit 2002::/16
```

The following example shows how to specify a group of prefixes to accept any prefixes from prefix 5F00::/48 up to and including prefix 5F00::/64.

```
Router(config)# ipv6 prefix-list abc permit 5F00::/48 le 64
```

The following example denies prefix lengths greater than 64 bits in routes that have the prefix 2001:0DB8::/64.

```
Router(config)# ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
```

The following example permits mask lengths from 32 to 64 bits in all address space.

```
Router(config)# ipv6 prefix-list abc permit ::/0 ge 32 le 64
```

The following example denies mask lengths greater than 32 bits in all address space.

```
Router(config)# ipv6 prefix-list abc deny ::/0 ge 32
```

The following example denies all routes with a prefix of 2002::/128.

```
Router(config)# ipv6 prefix-list abc deny 2002::/128
```

The following example permits all routes with a prefix of ::/0.

```
Router(config)# ipv6 prefix-list abc permit ::/0
```

Related Commands

Command	Description
clear ipv6 prefix-list	Resets the hit count of the IPv6 prefix list entries.
distribute-list out	Suppresses networks from being advertised in updates.
ipv6 prefix-list sequence-number	Enables the generation of sequence numbers for entries in an IPv6 prefix list.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or IPv6 prefix list entries.

ipv6 redirects

To enable the sending of Internet Control Message Protocol (ICMP) IPv6 redirect messages if Cisco IOS software is forced to resend a packet through the same interface on which the packet was received, use the **ipv6 redirects** command in interface configuration mode. To disable the sending of redirect messages, use the **no** form of this command.

ipv6 redirects

no ipv6 redirects

Syntax Description

This command has no arguments or keywords.

Command Default

The sending of ICMP IPv6 redirect messages is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)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

The rate at which the router generates all IPv6 ICMP error messages can be limited by using the **ipv6 icmp error-interval** command.

Examples

The following example disables the sending of ICMP IPv6 redirect messages on Ethernet interface 0 and reenables the messages on Ethernet interface 1:

```
Router(config)# interface ethernet 0
Router(config-if)# no ipv6 redirects
Router(config)# interface ethernet 1
Router(config-if)# ipv6 redirects
```

To verify whether the sending of IPv6 redirect messages is enabled or disabled on an interface, enter the **show ipv6 interface** command:

```
Router# show ipv6 interface
Ethernet0 is up, line protocol is up
  IPv6 is stalled, link-local address is FE80::1
  Global unicast address(es):
    2000::1, subnet is 2000::/64
    3000::1, subnet is 3000::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are disabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
Ethernet1 is up, line protocol is up
  IPv6 is stalled, link-local address is FE80::2
  Global unicast address(es):
    2000::2, subnet is 2000::/64
    3000::3, subnet is 3000::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is disabled, number of DAD attempts: 0
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

Related Commands

Command	Description
ipv6 icmp error-interval	Configures the interval for IPv6 ICMP error messages.

ipv6 rip default-information

To originate a de fault IPv6 route into the Routing Information Protocol (RIP), use the **ipv6 rip default-information**command in interface configuration mode. To remove the default IPv6 RIP route, use the **no** form of this command.

ipv6 rip *name* **default-information** {**only| originate**} [**metric** *metric-value*]

no ipv6 rip *name* **default-information**

Syntax Description

name	Name of the IPv6 RIP routing process.
only	Advertises the IPv6 default route (::/0) only. Suppresses the advertisement of all other routes.
originate	Advertises the IPv6 default route (::/0). The advertisement of other routes is unaffected.
metric *metric-value*	(Optional) Associates a metric with the default route. The *metric-value* range is from 1 through 15.

Command Default

Metric value is 1.

Command Modes

Interface 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.
12.3(14)T	The **metric** keyword and *metric-value* argument 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.

Release	Modification
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **ipv6 rip default-information**command is similar to the **default-information originate** (RIP)command, except that it is IPv6-specific.

Originating a default IPv6 route into RIP also forces the advertisement of the route in router updates sent on the interface. The advertisement of the route occurs regardless of whether the route is present in the IPv6 routing table.

The **metric***metric-value* keyword and argument allow more flexibility in topologies with multiple RIP routers on a LAN. For example, a user may want to configure one of many routers on a LAN as the preferred default router, so that all default route traffic will transit this router. This function can be achieved by configuring the preferred router to advertise a default route with a lower metric than the other routers on the network.

Note To avoid routing loops after the IPv6 default route (::/0) is originated into a specified RIP routing process, the routing process ignores all default route information received in subsequent IPv6 RIP update messages.

Examples

The following example originates a default IPv6 route into RIP on Ethernet interface 0/0 and advertises only the default route in router updates sent on the interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 rip cisco default-information only
```

The following example originates a default IPv6 route into RIP on Ethernet interface 0/0 and advertises the default route with all other routes in router updates sent on the interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 rip cisco default-information originate
```

Related Commands

Command	Description
show ipv6 rip	Displays information about current IPv6 RIP processes.

ipv6 rip enable

To enable an IPv6 Routing Information Pr otocol (RIP) routing process on an interface, use the **ipv6 rip enable**command in interface configuration mode. To disable an IPv6 RIP routing process on an interface, use the **no** form of this command.

ipv6 rip *name* **enable**

no ipv6 rip *name*

Syntax Description

name	Name of the IPv6 RIP routing process.

Command Default

An IPv6 RIP routing process is not defined.

Command Modes

Interface 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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **ipv6 rip enable** interface configuration command is used to enable IPv6 RIP explicitly on required interfaces. In IPv4, the **network***network-number* router configuration command is used to implicitly specify the interfaces on which to run IPv4 RIP.

Examples

The following example enables the IPv6 RIP routing process named cisco on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 rip cisco enable
```

Related Commands

Command	Description
show ipv6 rip	Displays information about current IPv6 RIP processes.

ipv6 rip metric-offset

To set the IPv6 Routing Information Protocol (RIP) metric for an interface, use the **ipv6 rip metric-offset**command in interface configuration mode. To return the metric to its default value, use the **no** form of this command.

ipv6 rip *word* **metric-offset** *value*

no ipv6 rip *word* **metric-offset**

Syntax Description

word	Name of the IPv6 RIP routing process.
value	Value added to the metric of an IPv6 RIP route received in a report message. A number from 1 to 16.

Command Default

The default metric value is 1.

Command Modes

Interface 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

When an IPv6 RIP route is received, the interface metric value set by the **ipv6 rip metric-offset**command is added before the route is inserted into the routing table. Therefore, increasing the IPv6 RIP metric value of an interface increases the metric value of IPv6 RIP routes received over the interface.

Use the **ipv6 rip metric-offset** command to influence which routes are used, as you prefer. The IPv6 RIP metric is in hop count.

Examples

The following example configures a metric increment of 10 for the RIP routing process named cisco on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 rip cisco metric-offset 10
```

Related Commands

Command	Description
show ipv6 rip	Displays information about current IPv6 RIP processes.

ipv6 rip summary-address

To configure IPv6 Routing Information Protocol (RIP) to advertise summarized IPv6 addresses on an interface and to specify the IPv6 prefix that identifies the routes to be summarized, use the **ipv6 rip summary-address**command in interface configuration mode. To stop the advertising of the summarized IPv6 addresses, use the **no** form of this command.

ipv6 rip *word* **summary-address** *ipv6-prefix/prefix-length*

no ipv6 rip *word* **summary-address**

Syntax Description

word	Name of the IPv6 RIP routing process.
ipv6-prefix	Specifies an IPv6 network number as the summary address. 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). A slash mark must precede the decimal value.

Command Default

No default behavior or values.

Command Modes

Interface 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.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **ipv6 rip summary-address**command is similar to the **ip summary-address rip**command, except that it is IPv6-specific.

Use the **ipv6 rip summary-address**command to force IPv6 RIP to advertise specific networks on specific interfaces (assuming that routes to those networks exist).

If the first bits of the prefix length for a route match the value specified for the ipv6-prefixargument, the prefix specified in the ipv6-prefixargument is advertised instead of the route. As a result, multiple routes can be replaced by a single route whose metric is the lowest metric of the multiple routes.

Examples

In the following example, the IPv6 address 2001:0DB8:0:1:260:3EFF:FE11:6770 that is assigned to Ethernet interface 0/0 with an IPv6 prefix length of 64 bits is summarized as IPv6 prefix 2001:0DB8::/35 for the IPv6 RIP routing process named cisco:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 address 2001:0DB8:0:1:260:3EFF:FE11:6770 /64
Router(config-if)# ipv6 rip cisco summary-address 2001:0DB8::/35
```

Note A route advertisement that is suppressed as a result of split horizon is not considered by RIP when RIP is deciding whether to advertise a summary route.

Related Commands

Command	Description
poison-reverse (IPv6 RIP)	Configures the poison reverse processing of IPv6 RIP router updates.
show ipv6 rip	Displays information about current IPv6 RIP processes.

ipv6 rip vrf-mode enable

To enable VRF-aware support for IPv6 Routing Information Protocol (RIP), use the **ipv6 rip vrf-mode enable** command in global configuration mode. To disable VRF-aware support for IPv6 RIP, use the **no** form of this command.

ipv6 rip vrf-mode enable

no ipv6 rip vrf-mode enable

Syntax Description

This command has no arguments or keywords.

Command Default

VRF-aware support is not enabled in IPv6 RIP.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.
15.3(2)S	This command was integrated into Cisco IOS Release 15.3(2)S.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

When VRF-aware support is enabled in IPv6 RIP, you can configure only one RIP instance at a given time. More than one RIP instance is not allowed.

Examples

The following example shows how to enable VRF-aware support for IPv6 RIP routing.

```
Device> enable
Device# configure terminal
Device(config)# ipv6 rip vrf-mode enable
Device(config)# end
```

Related Commands

Command	Description
clear ipv6 rip	Deletes routes from the IPv6 RIP routing table.
debug ipv6 rip	Displays debug messages for IPv6 RIP routing transactions.

Command	Description
show ipv6 rip	Displays information about current IPv6 RIP processes.

ipv6 route

To establish static IPv6 routes, use the **ipv6 route**command in global configuration mode. To remove a previously configured static route, use the **no** form of this command.

ipv6 route [**vrf** *vrf-name*] *ipv6-prefix/prefix-length* {*ipv6-address*| *interface-type interface-number* [*i* **pv6-address**]} [**nexthop-vrf** [*vrf-name1*| **default**]] [*administrative-distance*] [*administrative-multicast-distance*| **unicast**| **multicast**] [*next-hop-address*] [**tag** *tag*] [**name** *name*]

no ipv6 route [**vrf** *vrf-name*] *ipv6-prefix/prefix-length* {*ipv6-address*| *interface-type interface-number* [*i* **pv6-address**]} [**nexthop-vrf** [*vrf-name1*| **default**]] [*administrative-distance*] [*administrative-multicast-distance*| **unicast**| **multicast**] [*next-hop-address*] [**tag** *tag*] [**name** *route-name*]

Syntax Description

ipv6-prefix	The IPv6 network that is the destination of the static route. Can also be a host name when static host routes are configured.
/ *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.
vrf	(Optional) Specifies all virtual private network (VPN) routing/forwarding instance (VRF) tables or a specific VRF table for IPv4 or IPv6 address.
vrf-name	(Optional) Names a specific VRF table for an IPv4 or IPv6 address.
ipv6-address	The IPv6 address of the next hop that can be used to reach the specified network. The IPv6 address of the next hop need not be directly connected; recursion is done to find the IPv6 address of the directly connected next hop. When an interface type and interface number are specified, you can optionally specify the IPv6 address of the next hop to which packets are output. **Note** You must specify an interface type and an interface number when using a link-local address as the next hop (the link-local next hop must also be an adjacent device). This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

interface-type	Interface type. For more information about supported interface types, use the question mark (?) online help function. You can use the *interface-type* argument to direct static routes out point-to-point interfaces (such as serial or tunnel interfaces) and broadcast interfaces (such as Ethernet interfaces). When using the *interface-type* argument with point-to-point interfaces, there is no need to specify the IPv6 address of the next hop. When using the *interface-type* argument with broadcast interfaces, you should always specify the IPv6 address of the next hop or ensure that the specified prefix is assigned to the link. A link-local address should be specified as the next hop for broadcast interfaces.
interface-number	Interface number. For more information about the numbering syntax for supported interface types, use the question mark (?) online help function.
nexthop-vrf	(Optional) Indicator that the next hop is a VRF.
vrf-name1	(Optional) Name of the next-hop VRF.
default	(Optional) Indicator that the next hop is the default.
administrative-distance	(Optional) An administrative distance. The default value is 1, which gives static routes precedence over any other type of route except connected routes.
administrative- multicast-distance	(Optional) The distance used when selecting this route for multicast Reverse Path Forwarding (RPF).
unicast	(Optional) Specifies a route that must not be used in multicast RPF selection.
multicast	(Optional) Specifies a route that must not be populated in the unicast Routing Information Base (RIB).
next-hop-address	(Optional) Address of the next hop that can be used to reach the specified network.
tag *tag*	(Optional) Tag value that can be used as a "match" value for controlling redistribution via route maps.
name *route-name*	(Optional) Specifies a name for the route.

Command Default

No static routes are established.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(4)T	The optional *ipv6-address* argument was added.
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.
12.0(26)S	The optional **unicast** and **multicast** keywords and *administrative-multicast-distance*argument were added.
12.3(4)T	The optional **unicast** and **multicast** keywords and *administrative-multicast-distance*argument were added.
12.2(25)S	The optional **unicast** and **multicast** keywords and *administrative-multicast-distance*argument 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)SRB	The optional **vrf** and **nexthop-vrf** keywords, and *vrf-name* and *next-hop-address* arguments were added.
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 devices.
15.0	The **name** *name* keyword and argument were added.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.

Release	Modification
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

Use the **ipv6 route** command to implement static multicast routes in IPv6. For a static multicast route, the IPv6 address of the next-hop device must be provided. The *administrative-multicast-distance* argument determines the distance that will be used when selecting this route for RPF. When the **unicast** keyword is used, this route will not be used in multicast RPF selection.

When the **ipv6 route** command is used with the **multicast** keyword, the route will not be populated in the unicast RIB. When the optional *administrative-multicast-distance* argument is not specified, the multicast RPF administrative distance defaults to the same value as that determined by the *administrative-distance* argument.

Examples

The following example shows a static route that applies to unicast routing only:

```
ipv6 route 2001::/64 5::5 100 unicast
```

The following example shows a static route used only for multicast RPF selection:

```
ipv6 route 2001::/64 7::7 100 multicast
```

The following example shows a static route used for both unicast routing and multicast RPF selection:

```
ipv6 route 2001::/64 6::6 100
```

The following example shows a static route used for both unicast routing and multicast RPF selection, but with different administrative distances:

```
ipv6 route 10::/64 7::7 100 200
```

The following example configures a static route for use in VPN for IPv6:

```
ipv6 route vrf red 4004::/64 pos 1/0
```

The following example configures a static default route within a VRF. Use of the **global** keyword in this static route provides access to the Internet:

```
ipv6 route vrf red ::0/0 7007::1 global
```

Related Commands

Command	Description
show ipv6 route	Displays the current contents of the IPv6 routing table.
show ipv6 route summary	Displays the current contents of the IPv6 routing table in summary format.
show ipv6 rpf	Displays RPF information for a given unicast host address and prefix.

ipv6 route priority high

To assign a high-priority tag to an integrated Intermediate System-to-Intermediate System (IS-IS) IPv6 prefix to be used for controlling redistribution via route maps, use the **ipv6 route priority high** command in address family configuration mode. To remove the IPv6 prefix priority, use the **no** form of this command.

ipv6 route priority high tag *tag-value*

no ipv6 route priority high tag

Syntax Description

tag *tag-value*	Assigns a tag value that can be used as a match value for controlling redistribution via route maps. The range is from 1 to 4294967295.

Command Default

No priority is assigned to IS-IS IPv6 prefixes.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Release 3.6S	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Examples

In the following example, a high-priority tag of 100 is assigned:

```
Device# configure terminal
Device(config)# router isis
Device(config-router)# address-family ipv6
Device(config-router-af)# ipv6 route priority high tag 100
```

Related Commands

Command	Description
isis ipv6 tag	Configures an administrative tag value that will be associated with an IPv6 address prefix and applied to an IS-IS LSP.

Command	Description
redistribute isis (IPv6)	Redistributes IPv6 routes from one routing domain into another, using IS-IS as both the target and source protocol.
show isis database verbose	Displays additional information about the IS-IS database.
summary-prefix (IPv6 IS-IS)	Creates aggregate IPv6 prefixes for IS-IS.

ipv6 route static bfd

To specify static route Bidirectional Forwarding Detection for IPv6 (BFDv6) neighbors, use the **ipv6 route static bfd** command in global configuration mode. To remove a static route BFDv6 neighbor, use the **no** form of this command.

ipv6 route static bfd [**vrf** *vrf-name*] *interface-type interface-number ipv6-address* [**unassociated**]

no ipv6 route static bfd

Syntax Description

vrf *vrf-name*	(Optional) Name of the virtual routing and forwarding (VRF) instance by which static routes should be specified.
interface-type interface-number	Interface type and number.
ipv6-address	IPv6 address of the neighbor.
unassociated	(Optional) Moves a static BFD neighbor from associated mode to unassociated mode.

Command Default

No static route BFDv6 neighbors are specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.1(2)T	This command was integrated into Cisco IOS Release 15.1(2)T.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
15.1(1)SY	This command was modified. Support for IPv6 was added to Cisco IOS Release 15.1(1)SY.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use the **ipv6 route static bfd** command to specify static route neighbors. All of the static routes that have the same interface and gateway specified in the configuration share the same BFDv6 session for reachability notification. BFDv6 requires that BFDv6 sessions are initiated on both endpoint routers. Therefore, this command must be configured on each endpoint router. An IPv6 static BFDv6 neighbor must be fully specified (with the interface and the neighbor address) and must be directly attached.

All static routes that specify the same values for **vrf** *vrf-name*, *interface-type interface-number* , and *ipv6-address* will automatically use BFDv6 to determine gateway reachability and take advantage of fast failure detection.

Examples

The following example creates a neighbor on Ethernet interface 0/0 with an address of 2001::1:

```
Router(global config)# ipv6 route static bfd ethernet 0/0 2001::1
```

The following example converts the neighbor to unassociated mode:

```
Router(global config)# ipv6 route static bfd ethernet 0/0 2001::1 unassociated
```

Related Commands

Command	Description
show ipv6 static	Displays the current contents of the IPv6 routing table.

ipv6 route static resolve default

To allow a recursive IPv6 static route to resolve using the default IPv6 static route, use the **ipv6 route static resolve default**command in global configuration mode. To remove this function, use the **no** form of this command.

ipv6 route static resolve default

no ipv6 route static resolve default

Syntax Description

This command has no arguments or keywords.

Command Default

Recursive IPv6 static routes do not resolve via the default route.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

By default, a recursive IPv6 static route will not resolve using the default route (::/0). The **ipv6 route static resolve default** command restores legacy behavior and allows resolution using the default route.

Examples

The following example enables an IPv6 recursive static route to be resolved using a IPv6 static default route:

```
Router(config)# ipv6 route static resolve default
```

ipv6 router eigrp

To place the router in router configuration mode, create an Enhanced Interior Gateway Routing Protocol (EIGRP) routing process in IPv6, and configure this process, use the **ipv6**router **eigrp**command in global configurationmode. To shut down a routing process, use the **no** form of this command.

ipv6 router eigrp *as-number* [**eigrp event-log-size event-log-size**]

no ipv6 router eigrp *as-number*

Syntax Description

as-number	Autonomous system number.
eigrp event-log-size *event-log-size*	(Optional) Memory allocation value of the EIGRP event. The *event-log-size* value is the memory allocation, in bytes, calculated dynamically based on available memory. The *event-log-size* value is between 0 and the dynamically calculated number.

Command Default

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	The **eigrp event-log-size** keyword and *event-log-size* argument were added.
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.

Usage Guidelines

Use the **ipv6 router eigrp** command in global configuration mode to place the router in router configuration mode and create a routing process. Once in router configuration mode, you can configure the EIGRP for IPv6 routing process using the **ipv6 router eigrp** command.

Examples

The following example places the router in router configuration mode and allows you to configure an EIGRP for IPv6 routing process:

```
Router(config)# ipv6 router eigrp 400
```

```
eigrp router-id 10.13.14.15
eigrp stub connected summary
eigrp event-log-size 1000
no shutdown
```

Related Commands

Command	Description
ipv6 eigrp	Enables EIGRP for IPv6 on a specified interface.
router eigrp	Configures the EIGRP process.

ipv6 router isis

To configure an Intermediate System-to-Intermediate System (IS-IS) routing process for IPv6 on an interface and to attach an area designator to the routing process, use the **ipv6 router isis**command in interface configuration mode. To disable IS-IS for IPv6, use the **no**form of the command.

ipv6 router isis *area-name*

no ipv6 router isis *area-name*

Syntax Description

area-name	Meaningful name for a routing process. If a name is not specified, a null name is assumed and the process is referenced with a null name. This name must be unique among all IP or Connectionless Network Service (CLNS) device processes for a given device. Required for multiarea IS-IS configuration. Each area in a multiarea configuration should have a nonnull area name to facilitate identification of the area. Optional for conventional IS-IS configuration.

Command Default

No routing processes are specified.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(8)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.
Cisco IOS XE Release 2.4	This command was introduced on Cisco ASR 1000 Series devices.

Release	Modification
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.

Usage Guidelines

Before the IPv6 IS-IS routing process can be configured, IPv6 routing must be enabled using the **ipv6 unicast-routing** global configuration command, and an IPv6 address must be configured on an interface using either the **ipv6 enable** interface configuration command or the the **ipv6 address** interface configuration command. The **ipv6 enable**command will automatically configure an IPv6 link-local address on the interface.

Examples

The following example specifies IS-IS as an IPv6 routing protocol for a process named Finance. The Finance process will run over the Fast Ethernet interface 0/1.

```
Device(config)# router isis Finance
Device(config-router)# net 49.0001.aaaa.aaaa.aaaa.00
Device(config-router)# exit
Device(config)# interface FastEthernet 0/1
Device(config-if)# ipv6 router isis Finance
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 enable	Enables an interface for IPv6 processing and automatically assigns an IPv6 link-local address on the interface.
ipv6 unicast-routing	Enables the forwarding of IPv6 unicast datagrams.
net	Configures an IS-IS NET for a CLNS routing process.
router isis	Enables the IPv4 IS-IS routing protocol.

ipv6 router nemo

To enable the network mobility (NEMO) routing process on the home agent and place the router in router configuration mode, use the **ipv6 router nemo**command in global configuration mode. To disable this function, use the **no** form of the command.

ipv6 router nemo

no ipv6 router nemo

Syntax Description

This command has no arguments or keywords.

Command Default

The NEMO routing process is not enabled on the home agent.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

This command enables the NEMO routing process on the home agent.

Examples

In the following example, NEMO is enabled on the home agent:

```
Router(config)# ipv6 router nemo
```

ipv6 router ospf

To enable Open Shortest Path First (OSPF) for IPv6 router configuration mode, use the ipv6 **router ospf** command in global configuration mode.

ipv6 router ospf *process-id*

Syntax Description

process-id	Internal identification. It is locally assigned and can be a positive integer from 1 to 65535. The number used here is the number assigned administratively when enabling the OSPF for IPv6 routing process.

Command Default

No OSPF for IPv6 routing process is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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 integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was modified. It was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(2)T	This command was modified. Support for IPv6 was added to Cisco IOS Release 15.1(2)T.

Release	Modification
12.2(50)SY	This command was modified. Support for IPv6 was added to Cisco IOS Release 12.2(50)SY.
15.0(1)SY	This command was modified. Support for IPv6 was added to Cisco IOS Release 15.0(1)SY.
15.0(2)SE	This command was modified. Support for IPv6 was added to Cisco IOS Release 15.0(2)SE.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.

Usage Guidelines

Use this command to enter the OSPF for IPv6 router configuration mode. From this mode, you can enter several commands to customize OSPF for IPv6.

Examples

The following example enables the device with OSPF for IPv6 configuration mode and identifies the process with the number 1:

```
ipv6 router ospf 1
```

ipv6 router rip

To configure an IPv6 Routing Information Protocol (RIP) routing process, use the **ipv6 route r rip** command in global configuration mode. To remove a routing process, use the **no** form of this command.

ipv6 router rip *word*

no ipv6 router rip *word*

Syntax Description

word	A word that describes the routing process.

Command Default

No IPv6 RIP routing process is defined.

Command Modes

Global 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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **ipv6 router rip**command is similar to the **router rip**command, except that it is IPv6-specific.

Use this command to enable an IPv6 RIP routing process. Configuring this command places the router in router configuration mode for the IPv6 RIP routing process. The router prompt changes to Router(config-rtr-rip)#.

Examples

The following example configures the IPv6 RIP routing process named cisco and places the router in router configuration mode for the IPv6 RIP routing process:

```
Router(config)# ipv6 router rip cisco
```

Related Commands

Command	Description
ipv6 rip enable	Enables an IPv6 RIP routing process on an interface.

ipv6 routing-enforcement-header loose

To provide backward compatibility with legacy IPv6 inspection, use the ipv6 routing-enforcement-header loose command in parameter map type inspect configuration mode. To disable this feature, use the **no** form of this command.

ipv6 routing-enforcement-header loose

no ipv6 routing-enforcement-header loose

Syntax Description

This command has no arguments or keywords.

Command Default

Backward compatibility is not provided.

Command Modes

parameter map type inspect configuration mode (config-profile)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **ipv6 routing-enforcement-header loose** command provides backward compatibility with legacy IPv6 inspection. Enabling this command ensures that the firewall will not drop IPv6 traffic with routing headers. The default firewall behavior is to drop all IPv6 traffic without a routing header.

Examples

The following example enables backward compatibility with legacy IPv6 inspection on an inspect type parameter map named v6-param-map:

```
Router(config)# parameter-map type inspect v6-param-map
Router (config-profile)# ipv6 routing-header-enforcement loose
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

ipv6 snooping attach-policy

To apply an IPv6 snooping policy to a target, use the **ipv6 snooping attach-policy** command in IPv6 snooping configuration mode, or interface configuration mode. To remove a policy from a target, use the **no** form of this command.

ipv6 snooping policy attach-policy *snooping-policy*

Syntax Description

snooping-policy	User-defined name of the snooping policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).

Command Default

An IPv6 snooping policy is not attached to a target.

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

Once a policy has been identified or configured, it is applied on a target using the **ipv6 snooping attach-policy** command. This command is applied on any target, which varies depending on the platform. Examples of targets (depending on the platform used) include device ports, switchports, Layer 2 interfaces, Layer 3 interfaces, and VLANs.

Examples

The following examples shows how to apply an IPv6 snooping policy named policy1 to a target:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# ipv6 snooping attach-policy policy1
```

Related Commands

Command	Description
ipv6 snooping policy	Configures an IPv6 snooping policy and enters IPv6 snooping configuration mode.

ipv6 snooping logging

To configure IPv6 snooping security logging, use the **ipv6 snooping logging** command in global configuration mode. To disable IPv6 snooping security logging, use the **no** form of this command.

ipv6 snooping logging packet drop

no ipv6 snooping logging packet drop

Syntax Description

packet drop	Enables logging of router advertisements (RAs) dropped.

Command Default

Snooping security logging is not enabled.

Command Modes

Global configuration (config)#

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

Use the **ipv6 snooping logging** command with the **packet** and **drop** keywords to log RAs that are dropped when they are received on an unauthorized port.

Examples

The following example enables the router to log RAs received on an unauthorized port:

```
Router (config)# ipv6 snooping logging packet drop
```

Related Commands

Command	Description
<<**command**>>	<<FID.>>

ipv6 snooping logging packet drop

To enable the logging of dropped packets by the IPv6 first-hop security feature, use the **ipv6 snooping logging packet drop**command in global configuration mode. To disable the logging of dropped packets by the IPv6 first-hop security feature, use the **no** form of this command.

ipv6 snooping logging packet drop

no ipv6 snooping logging packet drop

Syntax Description

This command has no arguments or keywords.

Command Default

Snooping security logging is not enabled.

Command Modes

Global configuration (config)#

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

Use the **ipv6 snooping logging packet drop**command to log packets that are dropped when they are received on an unauthorized port. For example, this command will log RA packets that are dropped because of the RA guard feature.

Related Commands

Command	Description
ipv6 neighbor binding logging	Enables the logging of binding table main events.

ipv6 snooping policy

To configure an IPv6 snooping policy and enter IPv6 snooping configuration mode, use the **ipv6 snooping policy** command in global configuration mode. To delete an IPv6 snooping policy, use the **no** form of this command.

ipv6 snooping policy *snooping-policy*

no ipv6 snooping policy *snooping-policy*

Syntax Description

snooping-policy	User-defined name of the snooping policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).

Command Default

An IPv6 snooping policy is not configured.

Command Modes

Global configuration (config)

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

Use the **ipv6 snooping policy** command to create an IPv6 snooping policy. When the **ipv6 snooping policy** command is enabled, the configuration mode changes to IPv6 snooping configuration mode. In this mode, the administrator can configure the following IPv6 first-hop security commands:

- The **data-glean**/**destination-glean** command enables IPv6 first-hop security binding table recovery using data or destination address gleaning.
- The **device-role** command specifies the role of the device attached to the port.
- The **limit address-count** *maximum* command limits the number of IPv6 addresses allowed to be used on the port.
- **security-level** specifies the level of security enforced.
- The **tracking** command overrides the default tracking policy on a port.

- The **trusted-port** command configures a port to become a trusted port; that is, limited or no verification is performed when messages are received.

Once a policy has been identified or configured, it is applied on a device using the **ipv6 snooping attach-policy** command.

Examples

The following examples show how to configure an IPv6 snooping policy:

```
Device(config)# ipv6 snooping policy policy1
```

Related Commands

Command	Description
ipv6 snooping attach-policy	Applies an IPv6 snooping policy to a target.

ipv6 source-guard attach-policy

To apply IPv6 source guard policy on an interface, use the **ipv6 source-guard attach-policy** in interface configuration mode. To remove this source guard from the interface, use the **no** form of this command.

ipv6 source-guard attach-policy [*source-guard-policy*]

Syntax Description

source-guard-policy	(Optional) User-defined name of the source guard policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).

Command Default

An IPv6 source-guard policy is not applied on the interface.

Command Modes

Interface configuration (config-if)

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

If no policy is specified using the *source-guard-policy* argument, then the default source-guard policy is applied.

A dependency exists between IPv6 source guard and IPv6 snooping. Whenever IPv6 source guard is configured, when the **ipv6 source-guard attach-policy** command is entered, it verifies that snooping is enabled and issues a warning if it is not. If IPv6 snooping is disabled, the software checks if IPv6 source guard is enabled and sends a warning if it is.

Examples

The following example shows how to apply IPv6 source guard on an interface:

```
Router(config)# interface gigabitethernet 0/0/1
Router(config-if)# ipv6 source-guard attach-policy mysnoopingpolicy
```

Related Commands

Command	Description
ipv6 snooping policy	Configures an IPv6 snooping policy and enters IPv6 snooping configuration mode.

ipv6 source-guard policy

To configure an IPv6 source-guard policy and enter source-guard policy configuration mode or switch integrated security features source-guard policy configuration mode, use the **ipv6 source-guard policy** command in global configuration mode. To remove an IPv6 source-guard policy, use the **no** form of this command.

ipv6 source-guard policy *source-guard-policy*

no ipv6 source-guard policy *source-guard-policy*

Syntax Description

source-guard-policy	User-defined name of the snooping policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).

Command Default

An IPv6 source-guard policy is not configured.

Command Modes

Global configuration (config)

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 **ipv6 source-guard policy** command to define a source-guard policy name and enter source-guard policy configuration mode.

The administrator can use the following commands to configure the policy:

- The **permit link-local** command allows hardware bridging for all data traffic sourced by a link-local address.
- The **deny global-autoconf** command denies data traffic from auto-configured global addresses.

Examples

```
Device(config)# ipv6 source-guard policy policy1
Device(config-source-guard)#
```

Related Commands

Command	Description
deny global-autoconfig	Denies data traffic from autoconfigured global addresses.
permit link-local	Allows hardware bridging for all data traffic sourced by a link-local address.

ipv6 source-route

To enable processing of the IPv6 type 0 routing header (the IPv6 source routing header), use the **ipv6 source-route** command in global configuration mode. To disable the processing of this IPv6 extension header, use the **no** form of this command.

ipv6 source-route

no ipv6 source-route

Syntax Description

This command has no arguments or keywords.

Command Default

The **no** version of the **ipv6 source-route** command is the default. When the router receives a packet with a type 0 routing header, the router drops the packet and sends an IPv6 Internet Control Message Protocol (ICMP) error message back to the source and logs an appropriate debug message.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
12.4(15)T	The default was changed to be the **no** version of the **ipv6 source-route** command. When the router receives a packet with a type 0 routing header, the router drops the packet and sends an IPv6 ICMP error message back to the source and logs an appropriate debug message.
12.2(33)SRC	Changes made to this command were integrated into Cisco IOS 12.2(33)SRC.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

The default was changed to be the **no** version of the **ipv6 source-route** command, which means this functionality is not enabled. Before this change, this functionality was enabled automatically. User who had configured the **no ipv6 source-route** command before the default was changed will continue to see this configuration in their **show config** command output, even though the **no** version of the command is the default.

The **no ipv6 source-route** command (which is the default) prevents hosts from performing source routing using your routers. When the **no ipv6 source-route** command is configured and the router receives a packet with a type0 source routing header, the router drops the packet and sends an IPv6 ICMP error message back to the source and logs an appropriate debug message.

In IPv6, source routing is performed only by the destination of the packet. Therefore, in order to stop source routing from occurring inside your network, you need to configure an IPv6 access control list (ACL) that includes the following rule:

```
deny ipv6 any any routing
```

The rate at which the router generates all IPv6 ICMP error messages can be limited by using the **ipv6 icmp error-interval**command.

Examples

The following example disables the processing of IPv6 type 0 routing headers:

```
no ipv6 source-route
```

Related Commands

Command	Description
deny (IPv6)	Sets deny conditions for an IPv6 access list.
ipv6 icmp error-interval	Configures the interval for IPv6 ICMP error messages.

ipv6 spd mode

To configure an IPv6 Selective Packet Discard (SPD) mode, use the **ipv6 spd mode**command in global configuration mode. To remove the IPv6 SPD mode, use the **no** form of this command.

ipv6 spd mode {**aggressive**| **tos protocol ospf**}

no ipv6 spd mode {**aggressive**| **tos protocol ospf**}

Syntax Description

aggressive	Aggressive drop mode discards incorrectly formatted packets when the IPv6 SPD is in random drop state.
tos protocol o spf	OSPF mode allows OSPF packets to be handled with SPD priority.

Command Default

No IPv6 SPD mode is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The default setting for the IPv6 SPD mode is none, but you may want to use the **ipv6 spd mode** command to configure a mode to be used when a certain SPD state is reached.

The **aggressive** keyword enables aggressive drop mode, which drops deformed packets when IPv6 SPD is in random drop state. The **ospf** keyword enables OSPF mode, in which OSPF packets are handled with SPD priority.

The size of the process input queue governs the SPD state: normal (no drop), random drop, or max. When the process input queue is less than the SPD minimum threshold, SPD takes no action and enters normal state. In the normal state, no packets are dropped. When the input queue reaches the maximum threshold, SPD enters max state, in which normal priority packets are discarded. If the input queue is between the minimum and maximum thresholds, SPD enters the random drop state, in which normal packets may be dropped.

Examples

The following example shows how to enable the router to drop deformed packets when the router is in the random drop state:

```
Router(config)# ipv6 spf mode aggressive
```

Related Commands

Command	Description
ipv6 spd queue max-threshold	Configures the maximum number of packets in the IPv6 SPD process input queue.
ipv6 spd queue min-threshold	Configures the minimum number of packets in the IPv6 SPD process input queue.
show ipv6 spd	Displays the IPv6 SPD configuration.

ipv6 spd queue max-threshold

To configure the maximum number of packets in the IPv6 Selective Packet Discard (SPD) process input queue, use the **ipv6 spd queue max-threshold** command in global configuration mode. To return to the default value, use the **no** form of this command.

ipv6 spd queue max-threshold *value*

no ipv6 spd queue max-threshold

Syntax Description

value	Number of packets. The range is from 0 through 65535.

Command Default

No SPD queue maximum threshold value is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.1(3)T	This command was modified. The *value* argument range was changed from 4096 through 65535 to 0 through 65535.

Usage Guidelines

Use the **ipv6 spd queue max-threshold** command to configure the SPD queue maximum threshold value.

The size of the process input queue governs the SPD state: normal (no drop), random drop, or max. When the process input queue is less than the SPD minimum threshold, SPD takes no action and enters normal state. In the normal state, no packets are dropped. When the input queue reaches the maximum threshold, SPD enters max state, in which normal priority packets are discarded. If the input queue is between the minimum and maximum thresholds, SPD enters the random drop state, in which normal packets may be dropped.

Examples

The following example shows how to set the maximum threshold value of the queue to 60,000:

```
Router(config)# ipv6 spd queue max-threshold 60000
```

Related Commands

Command	Description
ipv6 spd queue min-threshold	Configures the minimum number of packets in the IPv6 SPD process input queue.
show ipv6 spd	Displays the IPv6 SPD configuration.

ipv6 spd queue min-threshold

To configure the minimum number of packets in the IPv6 Selective Packet Discard (SPD) process input queue, use the **ipv6 spd queue min-threshold** command in global configuration mode. To return to the default value, use the **no** form of this command.

ipv6 spd queue min-threshold *value*

no ipv6 spd queue min-threshold

Syntax Description

value	Number of packets. The range is from 0 through 65535.

Command Default

No SPD queue minimum threshold is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

Use the **ipv6 spd queue min-threshold** command to configure the SPD queue minimum threshold, which determines IPv6 state transition from normal to random drop state. The minimum threshold value must be lower than the maximum threshold setting.

The size of the process input queue governs the SPD state: normal (no drop), random drop, or max. When the process input queue is less than the SPD minimum threshold, SPD takes no action and enters normal state. In the normal state, no packets are dropped. When the input queue reaches the maximum threshold, SPD enters max state, in which normal priority packets are discarded. If the input queue is between the minimum and maximum thresholds, SPD enters the random drop state, in which normal packets may be dropped.

Examples

The following example shows how to set the IPv6 SPD minimum threshold to 4094 packets:

```
Router(config)# ipv6 spd queue min-threshold 4094
```

Related Commands

Command	Description
ipv6 spd queue max-threshold	Configures the maximum number of packets in the IPv6 SPD process input queue.
show ipv6 spd	Displays the IPv6 SPD configuration.

ipv6 split-horizon eigrp

To enable Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 split horizon, use the **ipv6**split-horizon **eigrp**command in interface configuration mode. To disable split horizon, use the **no** form of this command.

ipv6 split-horizon eigrp *as-number*

no ipv6 split-horizon eigrp *as-number*

Syntax Description

as-number	Autonomous system number.

Command Default

EIGRP for IPv6 split horizon is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

For networks that include links over X.25 packet-switched networks (PSNs), you can use the **neighbor** command in router configuration mode to disable the split horizon feature. Or, you can specify the **no ipv6 split-horizon eigrp** command in your configuration. However, if you do disable the split horizon feature, you must similarly disable split horizon for all routers and access servers in any relevant multicast groups on that network.

Note In general, we recommend that you not change the default state of split horizon unless you are certain that your application requires the change in order to advertise routes properly. Remember that if split horizon is disabled on a serial interface and that interface is attached to a packet-switched network, you must disable split horizon for all routers and access servers in any relevant multicast groups on that network.

Examples

The following example disables split horizon on a serial link connected to an X.25 network:

```
interface serial 0
 encapsulation x25
 no ipv6 split-horizon eigrp 101
```

Related Commands

Command	Description
neighbor (EIGRP)	Defines a neighboring router with which to exchange routing information on a router that is running EIGRP.