IPv6 Commands: sn to v

sntp address

To specify the IPv6 Simple Network Time Protocol (SNTP) server address list to be sent to the client, use the **sntp address** command in DHCP for IPv6 pool configuration mode. To remove the SNTP server address list, use the **no** form of the command.

sntp address *ipv6-address*

no sntp address *ipv6-address*

Syntax Description

ipv6-address	The IPv6 SNTP address of a server to be sent to the client.

Command Default

No SNTP server address is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

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

The SNTP server address list option provides a list of one or more IPv6 addresses of SNTP servers available to the client for synchronization. The clients use these SNTP servers to synchronize their system time to that of the standard time servers.

Clients must treat the list of SNTP servers as an ordered list, and the server may list the SNTP servers in decreasing order of preference. The option defined in this document can be used only to configure information about SNTP servers that can be reached using IPv6.

The SNTP server option code is 31. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to specify the SNTP server address:

```
sntp address 300::1
```

Related Commands

Command	Description
import sntp address	Imports the SNTP server option to a DHCP for IPv6 client.

spd extended-headroom

To configure Selective Packet Discard (SPD) extended headroom, use the **spd extended-headroom**command in global configuration mode. To return to the default value, use the **no** form of this command.

spd extended-headroom *size*

no spd extended-headroom

Syntax Description

size	SPD headroom size, in number of packets.

Command Default

The SPD extended headroom default is 10 packets.

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 integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

Because Interior Gateway Protocols (IGPs) and link stability are tenuous and crucial, such packets are given the highest priority and are given extended SPD headroom with a default of 10 packets. These packets are not dropped if the size of the input hold queue is lower than 185 (input queue default size + SPD headroom size + SPD extended headroom).

Examples

The following example shows how to configure SPD extended headroom to be 11 packets:

```
Router(config)# spd extended-headroom 11
```

Related Commands

Command	Description
show ipv6 spd	Displays the IPv6 SPD configuration.
spd headroom	Configures SPD headroom.

spd extended-headroom

spd headroom

To configure Selective Packet Discard (SPD) headroom, use the **spd headroom**command in global configuration mode. To return to the default value, use the **no** form of this command.

spd headroom *size*

no spd headroom

Syntax Description

size	SPD headroom size, in number of packets.

Command Default

The SPD headroom default is 100 packets.

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 integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

SPD prioritizes IPv6 packets with a precedence of 7 by allowing the software to queue them into the process level input queue above the normal input queue limit. The number of packets allowed in excess of the normal limit is called the SPD headroom, the default being 100, which means that a high precedence packet is not dropped if the size of the input hold queue is lower than 175 (input queue default size + SPD headroom size).

Examples

The following example shows how to configure SPD headroom to be 95 packets:

```
Router(config)# spd headroom 95
```

Related Commands

Command	Description
show ipv6 spd	Displays the IPv6 SPD configuration.
spd extended-headroom	Configures SPD extended headroom.

spf-interval (IPv6)

To configure how often Cisco IOS software performs the shortest path first (SPF) calculation, use the **s pf-interval**command in address family configuration mode. To restore the default interval, use the **no** form of this command.

spf-interval [**level-1**| **level-2**] *seconds* [*initial-wait*] [*secondary-wait*]

no spf-interval *seconds*

Syntax Description

level-1	(Optional) Summarizes only routes redistributed into Level 1 with the configured prefix value.
level-2	(Optional) Summarizes routes learned by Level 1 routing into the Level 2 backbone with the configured prefix value. Redistributed routes into Level 2 IS-IS also are summarized.
seconds	Minimum amount of time between SPF calculations, in seconds. It can be a number from 1 to 120. The default is 5 seconds.
initial-wait	(Optional) Length of time before the first SPF calculation in milliseconds.
secondary-wait	(Optional) Minimum length of time between the first and second SPF calculation, in milliseconds.

Command Default

The default is 5 seconds.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

SPF calculations are performed only when the topology changes. They are not performed when external routes change.

The **spf-interval**(IPv6) command controls how often Cisco IOS software can perform the SPF calculation. The SPF calculation is processor-intensive. Therefore, it may be useful to limit how often the SPF calculation is performed, especially when the area is large and the topology changes often. Increasing the SPF interval reduces the processor load of the router, but it could slow down the rate of convergence.

If IPv6 and IPv4 are configured on the same interface, they must be running the same Intermediate System-to-Intermediate System (IS-IS) level.

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

Examples

The following example sets the SPF calculation interval to 30 seconds:

```
Router(config)# router isis
Router(config-router)# address-family ipv6
Router(config-router-af)# spf-interval 30
```

Related Commands

Command	Description
prc-interval (IPv6)	Controls the hold-down period between PRCs.

split-horizon (IPv6 RIP)

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

split-horizon

no split-horizon

Syntax Description

This command has no arguments or keywords.

Command Default

Split horizon is configured and active by default. However, for ATM interfaces and subinterfaces **split-horizon** is disabled by default.

Command Modes

Router configuration

Command History

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

Usage Guidelines

The **split-horizon**(IPv6 RIP) command is similar to the **ip split-horizon**command, except that it is IPv6-specific.

This command configures split horizon processing of IPv6 RIP router updates. When split horizon is configured, the advertisement of networks out the interfaces from which the networks are learned is suppressed.

If both split horizon and poison reverse are configured, then split horizon behavior is replaced by poison reverse behavior (routes learned via RIP are advertised out the interface over which they were learned, but with an unreachable metric).

Note In general, changing the state of the default for the **split-horizon** command is not recommended, unless you are certain that your application requires a change in order to properly advertise routes. 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 configures split horizon processing for the IPv6 RIP routing process named cisco:

```
Router(config)# ipv6 router rip cisco
Router(config-rtr)# split-horizon
```

Related Commands

Command	Description
neighbor (RIP)	Defines a neighboring router with which to exchange routing information.

standby ipv6

To ac tivate the Hot Standby Router Protocol (HSRP) in IPv6, use the **standby ipv6** command in interface configuration mode. To disable HSRP, use the **no**form of this command.

standby [*group-number*] **ipv6** {*ipv6-global-address*| *ipv6-address /prefix-length*| *ipv6-prefix /prefix-length*| *link-local-address*| **autoconfig**}

no standby [*group-number*] **ipv6** {*ipv6-global-address*| *ipv6-address /prefix-length*| *ipv6-prefix /prefix-length*| *link-local-address*| **autoconfig**}

Syntax Description

group-number	(Optional) Group number on the interface for which HSRP is being activated. The default is 0. The group number range is from 0 to 255 for HSRP version 1 and from 0 to 4095 for HSRP version 2.
ipv6-global-address	IPv6 address of the hot standby router interface.
ipv6-prefix	The IPv6 network assigned to the interface. 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.
link-local-address	Link-local address of the hot standby router interface.
autoconfig	Indicates that a virtual link-local address will be generated automatically from the link-local prefix and a modified EUI-64 format interface identifier, where the EUI-64 interface identifier is created from the relevant HSRP virtual MAC address.

Command Default

The default group number is 0. HSRP is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(4)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.
12.2(33)SXI4	Users can configure a fully routable global virtual IPv6 address.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

An Ethernet or FDDI type interface must be used for HSRP for IPv6. HSRP version 2 must be enabled on an interface before HSRP IPv6 can be configured.

The **standby ipv6** command enables an HSRP group for IPv6 operation. If the **autoconfig** keyword is used, then a link-local address will be generated from the link-local prefix and a modified EUI-64 format interface identifier, where the EUI-64 interface identifier is created from the relevant HSRP virtual MAC address.

If an IPv6 global address is used, it must include an IPv6 prefix length. If a link-local address is used, it does not have a prefix.

Examples

The following example enables an HSRP group for IPv6 operation:

```
Router(config)# standby version 2
Router(config)# interface ethernet 0
Router(config-if)# standby ipv6 autoconfig
```

The following example shows three HSRP global IPv6 addresses with an explicitly configured link-local address:

```
interface Ethernet0/0
 no ip address
 ipv6 address 2001::0DB8:1/64
 standby version 2
 standby 1 ipv6 FE80::1:CAFÉ
 standby 1 ipv6 2001::0DB8:2/64
 standby 1 ipv6 2001:0DB8::3/64
 standby 1 ipv6 2001:0DB8::4/64
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

summary-prefix (IPv6 IS-IS)

To create aggregate IPv6 prefixes for Intermediate System-to-Intermediate System (IS-IS), use the **summary-prefix** command in address family configuration mode. To restore the default, use the **no** form of this command.

summary-prefix *ipv6-prefix*/*prefix-length* [{**level-1**| **level-1-2**| **level-2**}] [**tag** *tag-value*]

no summary-prefix *ipv6-prefix*/*prefix-length* [{**level-1**| **level-1-2**| **level-2**}] [**tag**]

Syntax Description

ipv6-prefix	Summary prefix designated for a range of IPv6 prefixes. The *ipv6-prefix* 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.
level-1	(Optional) Specifies that only routes redistributed into Level 1 are summarized with the configured prefix value.
level-1-2	(Optional) Specifies that summary routes are applied when redistributing routes into Level 1 and Level 2 IS-IS, and when Level 2 IS-IS advertises Level 1 routes reachable in its area.
level-2	(Optional) Specifies that routes learned by Level 1 routing are summarized into the Level 2 backbone with the configured prefix value. Redistributed routes into Level 2 IS-IS will be summarized also.
tag *tag-value*	(Optional) Assigns a tag to an IPV6 summary prefix. The tag value, in the range from 1 to 4294967295, is configured by the **isis ipv6 tag** command.

Command Default

All redistributed routes are advertised individually.

Command Modes

Address family configuration (config-router-af)

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 Aggregation Series Routers.
Cisco IOS XE Release 3.6S	This command was modified. Support for the **tag** keyword was added.

Usage Guidelines

Multiple groups of prefixes can be summarized for a given level. Routes learned from other routing protocols can also be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. This command helps reduce the size of the routing updates generated by the router, resulting in shorter routing tables on neighbor routers.

This command also reduces the size of the link-state packets (LSPs) and thus the link-state database (LSDB). It also helps ensure stability because a summary advertisement is depending on many more specific routes. If one more specific route flaps, in most cases this flapping does not cause a flap of the summary advertisement.

The drawback of summary prefixes is that other routes might have less information with which to calculate the most optimal routing table for all individual destinations.

Note When IS-IS advertises a summary prefix, it automatically inserts the summary prefix into the IPv6 routing table but labels it as a "discard" route entry. Any packet that matches the entry will be discarded to prevent routing loops. When IS-IS stops advertising the summary prefix, the routing table entry is removed.

Examples

In the following example, Routing Information Protocol (RIP) routes are redistributed into IS-IS. The RIP routing table, has IPv6 routes for 3FFE:F000:0001:0000::/64, 3FFE:F000:0002:0000::/64, 3FFE:F000:0003:0000::/64, and so on. This example advertises only 3FFE:F000::/24 into IPv6 IS-IS Level 1.

```
Device(config)# router isis area01
Device(config-router)# address-family ipv6
```

```
Device(config-router-af)# redistribute rip level-1 metric 40
Device(config-router-af)# summary-prefix 3FFE:F000::/24 level-1
```

The following example shows how to assign a tag to a summary prefix:

```
Device(config)# router isis area01
Device(config-router)# address-family ipv6
Device(config-router-af)# summary-prefix 2001:DB::/24 tag 220
```

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.
metric-style wide	Configures a router running IS-IS so that it generates and accepts only new-style type, length, and value.
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 information about the IS-IS database.

summary-prefix (OSPFv3)

To configure an IPv6 summary prefix in Open Shortest Path First version 3 (OSPFv3), use the **summary-prefix** command in OSPFv3 router configuration mode, IPv6 address family configuration mode, or IPv4 address family configuration mode. To restore the default, use the **no** form of this command.

summary-prefix *prefix* [**not-advertise**| **tag** *tag-value*] [**nssa-only**]

no summary-prefix *prefix* [**not-advertise**| **tag** *tag-value*] [**nssa-only**]

Syntax Description

prefix	IPv6 route prefix for the destination.
not-advertise	(Optional) Suppresses routes that match the specified prefix and mask pair. This keyword applies to OSPFv3 only.
tag *tag-value*	(Optional) Specifies the tag value that can be used as a match value for controlling redistribution via route maps. This keyword applies to OSPFv3 only.
nssa-only	(Optional) Limits the scope of the prefix to the area. Sets the nssa-only attribute for the summary route (if any) generated for the specified prefix.

Command Default

No IPv6 summary prefix is defined.

Command Modes

OSPFv3 router configuration mode (config-router)

IPv6 address family configuration (config-router-af)

IPv4 address family configuration (config-router-af)

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.

Release	Modification
15.1(3)S	This command was modified. The command can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The command can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The command can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(4)S	This command was modified. The **nssa-only** keyword was added.
15.1(1)SY	This command was modified. The command can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The summary-prefix command can be used to summarize devices redistributed from other routing protocols. Multiple groups of addresses can be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. This command helps reduce the size of the routing table.

Specify the **nssa-only** keyword to clear the propagate bit (P-bit) when external routes are redistributed into a not-so-stubby area (NSSA). Doing so prevents corresponding NSSA external link state advertisements (LSAs) from being translated into other areas.

Examples

In the following example, the summary prefix 2051:0:0:10::/60 includes addresses beginning at 2051:0:0:10::/60 up to (but not including) 2051:0:0:20::/128. Only the address 2051:0:0:10::/60 is advertised in an external LSA:

```
summary-prefix 2051:0:0:10::/60
```

Related Commands

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

synchronization (IPv6)

To enable the synchronization between IPv6 Border Gateway Protocol (BGP) and your Interior Gateway Protocol (IGP) system, use the **synchronization** command in address family configuration mode. To enable the Cisco IOS software to advertise a network route without waiting for IGP, use the **no** form of this command.

synchronization

no synchronization

Syntax Description

This command has no arguments or keywords.

Command Default

BGP advertises network routes without waiting for IGP.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Unlike the IPv4 version of the **synchronization** command, the IPv6 version is disabled by default.

By default, an IPv6 BGP speaker advertises an IPv6 network route without waiting for the IGP. Use the **synchronization** command in address family configuration mode to synchronize routing advertisements between BGP and your IGP. This feature allows routers and access servers within an autonomous system to have the route before BGP makes it available to other autonomous systems. When synchronization is enabled, IPv6 BGP does not advertise a route to an external neighbor unless that route is local or exists in the IGP.

Use the **synchronization** command if routers in the autonomous system do not speak BGP.

Examples

The following example enables a router to advertise an IPv6 network route without waiting for an IGP:

```
router bgp 65000
address-family ipv6
 synchronization
```

timers (IPv6 RIP)

To configure update, timeout, hold-down, and garbage-collection timers for an IPv6 RIP routing process, use the **timers**command in router configuration mode. To return the timers to their default values, use the **no** form of this command.

timers *update timeout holddown garbage-collection*

no timers

Syntax Description

update	Interval of time (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol.
timeout	Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the *update*argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters a hold-down state. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets.
holddown	Interval (in seconds) during which routing information regarding better paths is suppressed. A route enters a hold-down state when it becomes unreachable and the hold-down timer is a value other than zero. (A learned RIP route becomes unreachable when the route is not refreshed or the route is advertised with a metric of 16.) While in hold-down state, the system ignores any new information about the route from RIP or from any protocols that have a worse administrative distance than RIP. A route with a better administrative distance will replace the unreachable route, even if the route is still in a hold-down state.
garbage-collection	Amount of time (in seconds) that must pass from when a route becomes invalid until the route is removed from the routing table.

Command Default

Update timer: 30 seconds Timeout timer: 180 seconds Hold-down timer: 0 seconds Garbage-collection timer: 120 seconds

Command Modes

Router configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S, and the hold-down timer default value was changed to 0 seconds.
12.2(13)T	The hold-down timer default value was changed to 0 seconds.
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 **timers**(IPv6 RIP)command is similar to the **timers basic**(RIP)command, except that it is IPv6-specific.

Use the *update* argument to set the time interval between RIP routing updates. If no route update is received for the time interval specified by the *timeout* argument, the route is considered unreachable. Use the *holddown* argument to set a time delay between the route becoming unreachable and the route being considered invalid in the routing table. The use of a hold-down interval is not recommended for RIP because it can introduce long delays in convergence. Use the *garbage-collection* argument to specify the time interval between a route being considered invalid and the route being purged from the routing table.

The basic timing parameters for IPv6 RIP are adjustable. Because IPv6 RIP is executing a distributed, asynchronous routing algorithm, it is important that these timers be the same for all routers and access servers in the network.

Note The current and default timer values are displayed in the output of the **show ipv6 rip** EXEC command. The relationships of the various timers should be preserved, as described previously.

Examples

The following example sets updates to be broadcast every 5 seconds. If a route is not heard from in 15 seconds, the route is declared unusable. Further information is suppressed for an additional 10 seconds. Assuming no updates, the route is flushed from the routing table 20 seconds after the end of the hold-down period.

```
Router(config)# ipv6 router rip cisco
Router(config-rtr)# timers 5 15 10 30
```

Caution By setting a short update period, you run the risk of congesting slow-speed serial lines. Also, if you have many routes in your updates, you can cause the routers to spend an excessive amount of time processing updates.

Related Commands

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

timers lsa arrival

To set the minimum interval at which the software accepts the same link-state advertisement (LSA) from Open Shortest Path First (OSPF) neighbors, use the **timers lsa arrival**command in router configuration mode. To restore the default value, use the **no** form of this command.

timers lsa arrival *milliseconds*

no timers lsa arrival

Syntax Description

milliseconds	Minimum delay in milliseconds that must pass between acceptance of the same LSA arriving from neighbors. The range is from 0 to 600,000 milliseconds. The default is 1000 milliseconds.

Command Default

1000 milliseconds

Command Modes

OSPF for IPv6 router configuration (config-rtr) Router configuration (config-router)

Command History

Release	Modification
12.0(25)S	This command was introduced.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	Support for IPv6 was added.
12.2(33)SB	Support for IPv6 was added.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The **timers lsa arrival** command controls the minimum interval for accepting the same LSA. The "same LSA" is defined as an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the LSA is dropped.

We suggest you keep the *milliseconds*value of the **timers lsa arrival** command less than or equal to the neighbors' *hold-interval* value of the **timers throttle lsa all** command.

Examples

The following example sets the minimum interval for accepting the same LSA at 2000 milliseconds:

```
router ospf 1
 log-adjacency-changes
 timers throttle lsa all 200 10000 45000
 timers lsa arrival 2000
 network 10.10.4.0 0.0.0.255 area 24
 network 10.10.24.0 0.0.0.255 area 24
```

Related Commands

Command	Description
show ip ospf timers rate-limit	Displays all of the LSAs in the rate limit queue.
show ipv6 ospf timers rate-limit	Displays all of the LSAs in the IPv6 rate limit queue
timers throttle lsa	Sets rate-limiting values for OSPF for IPv6 LSA generation.
timers throttle lsa all	Sets rate-limiting values for LSAs being generated.

timers pacing flood (OSPFv3)

To configure link-state advertisement (LSA) flood packet pacing, use the **timers pacing flood** command in Open Shortest Path First version 3 (OSPFv3) router configuration mode. To restore the default flood packet pacing value, use the **no** form of this command.

timers pacing flood *milliseconds*

no timers pacing flood

Syntax Description

milliseconds	Time (in milliseconds) at which LSAs in the flooding queue are paced in between updates. The configurable range is from 5 milliseconds to 100 milliseconds. The default value is 33 milliseconds.

Command Default

The default is 33 milliseconds.

Command Modes

OSPFv3 router configuration (config-router)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.1(1)SY	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.

Usage Guidelines

Configuring Open Shortest Path First version 3 (OSPF) flood pacing timers allows you to control interpacket spacing between consecutive link-state update packets in the OSPFv3 transmission queue. This command allows you to control the rate at which LSA updates occur to reduce the high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs.

The default settings for OSPFv3 packet pacing timers are suitable for the majority of OSPFv3 deployments. Do not change the packet pacing timers unless all other options to meet OSPFv3 packet flooding requirements have been exhausted. Specifically, network operators should prefer summarization, stub area usage, queue tuning, and buffer tuning before changing the default flood timers. Furthermore, there are no guidelines for changing timer values; each OSPFv3 deployment is unique and should be considered on a case-by-case basis.

Note The network operator assumes risks associated with changing the default flood timer values.

Examples

The following example configures LSA flood packet-pacing updates to occur in 20-millisecond intervals for OSPFv3 routing process 1:

```
Router(config)# router ospfv3 1
Router(config-router)# timers pacing flood 20
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
show ipv6 ospf	Displays general information about OSPF for IPv6 routing processes.
timers pacing lsa-group	Changes the interval at which OSPF LSAs are collected into a group and refreshed, checksummed, or aged.
timers pacing retransmission	Configures LSA retransmission packet pacing.

timers pacing lsa-group (OSPFv3)

To change the interval at which Open Shortest Path First version 3 (OSPFv3) link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged, use the **timers pacing lsa-group** command in router configuration mode. To restore the default value, use the **no** form of this command.

timers pacing lsa-group *seconds*

no timers pacing lsa-group

Syntax Description

seconds	Number of seconds in the interval at which LSAs are grouped and refreshed, checksummed, or aged. The range is from 10 to 1800 seconds. The default value is 240 seconds.

Command Default

The default interval for this command is 240 seconds. OSPFv3 LSA group pacing is enabled by default.

Command Modes

OSPFv3 router configuration (config-router)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY

Usage Guidelines

This command allows you to control the rate at which LSA updates occur to reduce the high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs. The default settings for OSPFv3 packet pacing timers are suitable for the majority of OSPFv3 deployments. Do not change the packet pacing timers unless all other options to meet OSPFv3 packet flooding requirements have been exhausted. Specifically, network operators should prefer summarization, stub area usage, queue tuning, and buffer tuning

before changing the default flooding timers. Furthermore, there are no guidelines for changing timer values; each OSPFv3 deployment is unique and should be considered on a case-by-case basis.

Note The network operator assumes the risks associated with changing the default timer values.

Cisco IOS software groups the periodic refresh of LSAs to improve the LSA packing density for the refreshes in large topologies. The group timer controls the interval used for group refreshment of LSAs; however, this timer does not change the frequency that individual LSAs are refreshed (the default refresh rate is every 30 minutes).

The duration of the LSA group pacing is inversely proportional to the number of LSAs the router is handling. For example, if you have about 10,000 LSAs, decreasing the pacing interval would benefit you. If you have a very small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might benefit you slightly.

Examples

The following example configures OSPFv3 group packet-pacing updates between LSA groups to occur in 300-second intervals for OSPFv3 routing process 1:

```
Router(config)#
 router ospfv3 1
Router(config-router)#
 timers pacing lsa-group 300
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
show ipv6 ospf	Displays general information about OSPF for IPv6 routing processes.
timers pacing flood	Configures LSA flood packet pacing.
timers pacing retransmission	Configures LSA retransmission packet pacing.

timers pacing retransmission (OSPFv3)

To configure link-state advertisement (LSA) retransmission packet pacing in IPv4 Open Shortest Path First version 3 (OSPFv3), use the **timers pacing retransmission** command in OSPFv3 router configuration mode. To restore the default retransmission packet pacing value, use the **no** form of this command.

timers pacing retransmission *milliseconds*

no timers pacing retransmission

Syntax Description

milliseconds	The time (in milliseconds) at which LSAs in the retransmission queue are paced. The configurable range is from 5 milliseconds to 200 milliseconds. The default value is 66 milliseconds.

Command Default

The default is 66 milliseconds.

Command Modes

OSPFv3 router configuration (config-router)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Configuring OSPFv3 retransmission pacing timers allow you to control interpacket spacing between consecutive link-state update packets in the OSPFv3 retransmission queue. This command allows you to control the rate at which LSA updates occur to reduce high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs. The default settings for OSPFv3 packet retransmission pacing timers are suitable for the majority of OSPFv3 deployments. Do not change the packet retransmission pacing timers unless all other options to meet OSPFv3 packet flooding requirements have been exhausted. Specifically,

network operators should prefer summarization, stub area usage, queue tuning, and buffer tuning before changing the default flooding timers. Furthermore, there are no guidelines for changing timer values; each OSPFv3 deployment is unique and should be considered on a case-by-case basis.

Note The network operator assumes risks associated with changing the default packet retransmission pacing timer values.

Examples

The following example configures LSA flood pacing updates to occur in 100-millisecond intervals for OSPFv3 routing process 1:

```
Router(config)# router ospfv3 1
Router(config-router)# timers pacing retransmission 100
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
show ipv6 ospf	Displays general information about OSPF for IPv6 routing processes.
timers pacing flood	Configures LSA flood packet pacing.
timers pacing lsa-group	Changes the interval at which OSPF LSAs are collected into a group and refreshed, checksummed, or aged.

timers spf (IPv6)

To turn on Open Shortest Path First (OSPF) for IPv6 shortest path first (SPF) throttling, use the **timers spf** command in router configuration mode. To turn off SPF throttling, use the **no** form of this command.

timers spf *delay holdtime*

no timers spf

Syntax Description

delay	Delay (in milliseconds) in receiving a change in the SPF calculation. The range is from 0 through 4294967295. The default is 5 milliseconds.
holdtime	Hold time (in milliseconds) between consecutive SPF calculations. The range is from 0 through 4294967295. The default is 10 milliseconds.

Command Default

OSPF for IPv6 throttling is always enabled.

Command Modes

Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The first wait interval between SPF calculations is the amount of time in milliseconds specified by the *delay* argument. Each consecutive wait interval is two times the current hold level in milliseconds until the wait time reaches the maximum time in milliseconds as specified by the *holdtime* argument. Subsequent wait times remain at the maximum until the values are reset or a link-state advertisement (LSA) is received between SPF calculations.

Examples

The following example shows a router configured with the delay and hold-time interval values for the **timers spf** command set at 40 and 50 milliseconds, respectively.

```
Router(config)# ipv6 router ospf 1
Router(config-router)# timers spf 40 50
```

Related Commands

Command	Description
show ipv6 ospf	Displays general information about OSPF for IPv6 routing processes.

timers throttle lsa

To set rate-limiting values for Open Shortest Path First (OSPF) for IPv6 link-state advertisement (LSA) generation, use the **timers throttle lsa**command in router configuration mode. To restore the default values, use the **no** form of this command.

timers throttle lsa *start-interval hold-interval max-interval*

no timers throttle lsa

Syntax Description

start-interval	Minimum delay in milliseconds for the generation of LSAs. The first instance of LSA is always generated immediately upon a local OSPF for IPv6 topology change. The generation of the next LSA is not before the start interval. The range is from 0 to 600,000 milliseconds. The default is 0 milliseconds, which means no delay; the LSA is sent immediately.
hold-interval	Incremental time in milliseconds. This value is used to calculate the subsequent rate limiting times for LSA generation. The range is from 1 to 600,000 milliseconds. The default value is 5000 milliseconds.
max-interval	Maximum wait time in milliseconds between generation of the same LSA. The range is from 1 to 600,000 milliseconds. The default value is 5000 milliseconds.

Command Default

start-interval : 0 milliseconds*hold-interval:*5000 milliseconds*max-interval*: 5000 milliseconds

Command Modes

OSPF for IPv6 router configuration (config-rtr) Router configuration (config-router)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Release	Modification
15.1(1)SY	This command was modified. It was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The "same LSA" is defined as an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. We suggest you keep the *milliseconds*value of the **timers lsa arrival**command less than or equal to the *hold-interval* value of the **timers throttle lsa**command.

Examples

This example customizes OSPF LSA throttling so that the start interval is 200 milliseconds, the hold interval is 10,000 milliseconds, and the maximum interval is 45,000 milliseconds. The minimum interval between instances of receiving the same LSA is 2000 milliseconds.

```
router ospf 1
 log-adjacency-changes
 timers throttle lsa 200 10000 45000
 timers lsa arrival 2000
 network 10.10.4.0 0.0.0.255 area 24
 network 10.10.24.0 0.0.0.255 area 24
```

This example customizes IPv6 OSPF LSA throttling so that the start interval is 500 milliseconds, the hold interval is 1,000 milliseconds, and the maximum interval is 10,000 milliseconds.

```
ipv6 router ospf 1
 log-adjacency-changes
 timers throttle lsa 500 1000 10000
```

Related Commands

Command	Description
show ipv6 ospf	Displays information about OSPF for IPv6 routing processes.
timers lsa arrival	Sets the minimum interval at which the software accepts the same LSA from OSPF neighbors.

timers throttle spf

To turn on Open Shortest Path First (OSPF) shortest path first (SPF) throttling, use the **timers throttle spf** command in the appropriate configuration mode. To turn off OSPF SPF throttling, use the **no** form of this command.

timers throttle spf *spf-start spf-hold spf-max-wait*

no timers throttle spf *spf-start spf-hold spf-max-wait*

Syntax Description

spf-start	Initial delay to schedule an SPF calculation after a change, in milliseconds. Range is from 1 to 600000. In OSPF for IPv6, the default value is 5000.
spf-hold	Minimum hold time between two consecutive SPF calculations, in milliseconds. Range is from 1 to 600000. In OSPF for IPv6, the default value is 10,000.
spf-max-wait	Maximum wait time between two consecutive SPF calculations, in milliseconds. Range is from 1 to 600000. In OSPF for IPv6, the default value is 10,000.

Command Default

SPF throttling is not set.

Command Modes

Address family configuration (config-router-af) Router address family topology configuration (config-router-af-topology) Router configuration (config-router) OSPF for IPv6 router configuration (config-rtr)

Command History

Release	Modification
12.2(14)S	This command was introduced. This command replaces the **timers spf-interval** command.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was made available in router address family configuration mode.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Release	Modification
12.2(33)SRC	Support for IPv6 was added.
12.2(33)SB	Support for IPv6 was added and this command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The first wait interval between SPF calculations is the amount of time in milliseconds specified by the *spf-start*argument. Each consecutive wait interval is two times the current hold level in milliseconds until the wait time reaches the maximum time in milliseconds as specified by the *spf-max-wait* argument. Subsequent wait times remain at the maximum until the values are reset or a link-state advertisement (LSA) is received between SPF calculations.

Release 12.2(33)SRB

If you plan to configure the Multi-Topology Routing (MTR) feature, you need to enter the **timers throttle spf** command in router address family topology configuration mode in order to make this OSPF router configuration command become topology-aware.

Release 15.2(1)T

When you configure the **ospfv3 network manet** command on any interface attached to the OSPFv3 process, the default values for the *spf-start*, *spf-hold*, and the *spf-max-wait* arguments are reduced to 1000 milliseconds, 1000 milliseconds, and 2000 milliseconds respectively.

Examples

The following example shows how to configure a router with the delay, hold, and maximum interval values for the **timers throttle spf** command set at 5, 1000, and 90,000 milliseconds, respectively.

```
router ospf 1
 router-id 10.10.10.2
 log-adjacency-changes
 timers throttle spf 5 1000 90000
 redistribute static subnets
 network 10.21.21.0 0.0.0.255 area 0
 network 10.22.22.0 0.0.0.255 area 00
```

The following example shows how to configure a router using IPv6 with the delay, hold, and maximum interval values for the **timers throttle spf** command set at 500, 1000, and 10,000 milliseconds, respectively.

```
ipv6 router ospf 1
 event-log size 10000 one-shot
 log-adjacency-changes
 timers throttle spf 500 1000 10000
```

Related Commands

Command	Description
ospfv3 network manet	Sets the network type to Mobile Ad Hoc Network (MANET).

tracking

To override the default tracking policy on a port, use the **tracking**command in Neighbor Discovery (ND) inspection policy configuration mode.

tracking {**enable** [**reachable-lifetime** {*value*| **infinite**}]| **disable** [**stale-lifetime** {*value*| **infinite**}]}

Syntax Description

enable	Tracking is enabled.
reachable-lifetime	(Optional) The maximum amount of time a reachable entry is considered to be directly or indirectly reachable without proof of reachability. • The **reachable-lifetime** keyword can be used only with the **enable** keyword. • Use of the **reachable-lifetime** keyword overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command.
value	Lifetime value, in seconds. The range is from 1 to 86400, and the default is 300.
infinite	Keeps an entry in a reachable or stale state for an infinite amount of time.
disable	Disables tracking.
stale-lifetime	(Optional) Keeps the time entry in a stale state, which overwrites the global stale-lifetime configuration. • The stale lifetime is 86,400 seconds. • The **stale-lifetime** keyword can be used only with the **disable** keyword. • Use of the **stale-lifetime** keyword overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.

Command Default

The time entry is kept in a reachable state.

Command Modes

ND inspection policy configuration (config-nd-inspection)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

The **tracking** command overrides the default tracking policy set by the **ipv6 neighbor tracking** command on the port on which this policy applies. This function is useful on trusted ports where, for example, you may not want to track entries but want an entry to stay in the binding table to prevent it from being stolen.

The **reachable-lifetime** keyword is the maximum time an entry will be considered reachable without proof of reachability, either directly through tracking or indirectly through ND inspection. After the **reachable-lifetime** value is reached, the entry is moved to stale. Use of the **reachable-lifetime** keyword with the **tracking** command overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command.

The **stale-lifetime** keyword is the maximum time an entry is kept in the table before it is deleted or the entry is proven to be reachable, either directly or indirectly. Use of the **stale-lifetime** keyword with the **tracking** command overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.

Examples

The following example defines an ND policy name as policy1, places the router in ND inspection policy configuration mode, and configures an entry to stay in the binding table for an infinite length of time on a trusted port:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# tracking disable stale-lifetime infinite
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the ND inspection policy name and enters ND inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.
ipv6 neighbor binding	Changes the defaults of neighbor binding entries in a binding table.
ipv6 neighbor tracking	Enables tracking of entries in the binding table.

trusted

To allow hardware bridging for all data traffic on the target where the policy is applied, use the **trusted** command in source-guard policy configuration mode or switch integrated security features source-guard policy configuration mode. To disallow hardware bridging, use the **no** form of this command.

trusted

no trusted

Syntax Description

This command has no arguments or keywords.

Command Default

Hardware bridging is not allowed on the target on which the policy is applied.

Command Modes

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

Command History

Release	Modification
15.3(1)S	This command was introduced.

Usage Guidelines

Use the **trusted** command to allow hardware bridging for all data traffic on the target where the source-guard policy is applied. This function disables a source-guard policy on specific ports when IPv6 source guard is configured on a VLAN target.

Examples

```
Device(config)# ipv6 source-guard policy
Device(config-source-guard)# deny global-autoconf
Device(config-source-guard)# trusted
```

Related Commands

Command	Description
deny global-autoconfig	Denies data traffic from autoconfigured global addresses.
ipv6 source-guard policy	Defines an IPv6 source-guard policy name and enters source-guard policy configuration mode.

trusted-port (IPv6 NDP Inspection Policy)

To configure a port to become a trusted port, use the **trusted-port** command in Neighbor Discovery Protocol (NDP) inspection policy configuration mode . To disable this function, use the **no** form of this command.

trusted-port

no trusted-port

Syntax Description

This command has no arguments or keywords.

Command Default

No ports are trusted.

Command Modes

NDP inspection policy configuration (config-nd-inspection)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

When the **trusted-port** command is enabled, limited or no verification is performed when messages are received on ports that have this policy. However, to protect against address spoofing, messages are analyzed so that the binding information that they carry can be used to maintain the binding table. Bindings discovered from these ports will be considered more trustworthy than bindings received from ports that are not configured to be trusted.

Use the **trusted-port** command after enabling NDP inspection policy configuration mode using the **ipv6 nd inspection policy** command.

Examples

The following example defines an NDP policy name as policy1, places the router in NDP inspection policy configuration mode, and configures the port to be trusted:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# trusted-port
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the NDP inspection policy name and enters NDP inspection policy configuration mode.

trusted-port (IPv6 RA Guard Policy)

To configure a port to become a trusted port, use the **trusted-port**command in router advertisement (RA) guard policy configuration . To disable this function, use the **no** form of this command.

trusted-port

no trusted-port

Syntax Description

This command has no arguments or keywords.

Command Default

No ports are trusted.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

When the **trusted-port** command is enabled, limited or no verification is performed when messages are received on ports that have this policy. However, the **device-role** command takes precedence over the **trusted-port** command; if the device role is configured as host, messages will be dropped regardless of **trusted-port** command configuration.

Examples

The following example defines an RA guard policy name as raguard1, places the router in RA guard policy configuration mode, and configures the port to be trusted:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-ra-guard)# trusted-port
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the NDP inspection policy n ame and enters NDP inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

tunnel 6rd br

To bypass security checks on an IPv6 rapid deployment (6RD) customer-edge (CE) router, use the **tunnel 6rd br command** in interface configuration mode. To remove the BR router's address from configuration, use the **no** form of this command.

tunnel 6rd br *ipv4-address*

no tunnel 6rd br *ipv4-address*

Syntax Description

ipv4-address	IPv4 address of the BR router.

Command Default

No BR router is specified.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The **tunnel 6rd br** command is optional for 6RD operation. The command allows the user to specify the BR address, which allows the 6RD router to skip the security checks for packets from that source.

By default at a 6RD router, all incoming packets require that their outer IPv4 source address to be embedded in the 6RD-encoded IPv6 source address. Packets that do not satisfy this criteria are dropped. Configuring the **tunnel 6rd br** command exempts packets with the specified source from this check.

The **tunnel 6rd br** command should be enabled on the customer edge (CE) router, because packets arriving at the CE from the BR typically are traffic from a native IPv6 host, which does not need to have a 6RD-encoded source address.

Examples

The following example sets the BR address to 10.1.4.1:

```
Router(config-if)# tunnel 6rd br 10.1.4.1
```

Related Commands

Command	Description
ip address	Specifies the IPv4 address of an IPv4 interface.

Command	Description
ipv6 address	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.
tunnel destination	Sets the destination address for a tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

tunnel 6rd ipv4

To specify the prefix length and suffix length of the IPv4 transport address common to all the 6RD routers in a domain, use the tunnel 6rd ipv4 command in interface configuration mode. To remove these parameters, use the **no** form of this command.

tunnel 6rd ipv4 prefix-len *length* **suffix-len** *length*

no tunnel 6rd ipv4 prefix-len *length* **suffix-len** *length*

Syntax Description

prefix-len *length*	Specifies the prefix length, in bits, common to all 6RD routers in a domain. • The range is from 0 to 31, and the default is 0. • The sum of the IPv4 prefix length and the IPv4 suffix length cannot exceed 31.
suffix-len *length*	Specifies the suffix length, in bits, common to all 6RD routers in a domain. • The range is from 0 to 31, and the default is 0. • The sum of the IPv4 prefix length and the IPv4 suffix length cannot exceed 31.

Command Default

The prefix length and suffix length are 0.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The **tunnel 6rd ipv4**command is optional for 6RD operation. This command specifies the number of most significant bits and least significant bits of the IPv4 transport address (that is, the tunnel source) that are common to all the 6RD routers in a domain. The valid range is from 0 to 31, and the sum of the IPv4 prefix length and the IPv4 suffix length cannot exceed 31. If the **tunnel 6rd ipv4**command is not configured, and the **tunnel 6rd prefix** command is configured, the system uses the default value of 0.

Examples

The following example shows 6RD configuration, including the number of most and least significant bits of the IPv4 transport address common to all the 6RD routers in a domain:

```
Router(config)# interface Tunnel1
Router(config-if)# ipv6 address 2001:B000:100::1/32
Router(config-if)# tunnel source GigabitEthernet2/0/0
Router(config-if)# tunnel mode ipv6ip 6rd
Router(config-if)# tunnel 6rd prefix 2001:B000::/32
Router(config-if)# tunnel 6rd ipv4 prefix-len 16 suffix-len 8
```

Related Commands

Command	Description
ip address	Specifies the IP address of an IPv4 interface.
ipv6 address	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.
tunnel 6rd prefix	Specifies the common IPv6 prefix on 6RD tunnels
tunnel destination	Sets the destination address for a tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

tunnel 6rd prefix

To specify the common IPv6 prefix on IPv6 rapid deployment (6RD) tunnels, use the tunnel 6rd prefix command in interface configuration mode. To remove the IPv6 prefix, use the **no** form of this command.

tunnel 6rd prefix *ipv6-prefix /prefix-length*

no tunnel 6rd prefix *ipv6-prefix /prefix-length*

Syntax Description

ipv6-prefix	The IPv6 network assigned to the general prefix. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

This command can be enabled only when 6RD is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The **tunnel 6rd prefix** command is mandatory for 6RD operation. It specifies the common IPv6 prefix, and the *prefix-length* argument determines us the position of the IPv4 address in the 6RD delegated prefix (or payload) destination. Configuring a *prefix-length* of 0 is equivalent to removing this command.

The tunnel line state of a 6RD tunnel remains inactive until the **tunnel 6rd prefix**command is configured, and this command is automatically disabled when the **tunnel mode ipv6ip**command is configured to use a keyword other than **6rd**.

Examples

The following example shows 6RD configuration, including the **tunnel 6rd prefix** command:

```
ipv6 general-prefix 6rd1 6rd Tunnel1
```

```
!
interface Tunnel1
 ipv6 address 6rd1 ::1/124
tunnel source GigabitEthernet2/0/0
tunnel mode ipv6ip 6rd
tunnel 6rd prefix 2001:B000::/32
tunnel 6rd ipv4 prefix-len 16 suffix-len 8
```

Related Commands

Command	Description
ip address	Specifies the IPv4 address of an IPv4 interface.
ipv6 address	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.
tunnel destination	Sets the destination address for a tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

tunnel mode ipv6ip

To configure a static IPv6 tunnel interface, use the **tunnel mode ipv6ip** command in interface configuration mode. To remove a static IPv6 tunnel interface, use the **no** form of this command.

tunnel mode ipv6ip [**6rd**| **6to4**| **auto-tunnel**| **isatap**]

no tunnel mode ipv6ip

Syntax Description

6rd	(Optional) Specifies that the tunnel is to be used for IPv6 rapid deployment (6RD).
6to4	(Optional) Configures an IPv6 automatic tunnel using a destination address that is dynamically constructed from an IPv4 address and the prefix 2002::/16 (referred to as a 6to4 address).
auto-tunnel	(Optional) Configures an IPv6 automatic tunnel using an IPv4-compatible IPv6 address.
isatap	(Optional) Configures an IPv6 automatic tunnel using Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) to connect IPv6 nodes (hosts and routers) within IPv4 networks.

Command Default

Static IPv6 tunnel interfaces are not configured.

Command Modes

Interface configuration (config-if)

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 modified. The **isatap** keyword was added to support the addition of ISATAP tunnel implementation.
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.

Release	Modification
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 3.1S	This command was modified. The **6rd** keyword was added. The **auto-tunnel** keyword was deprecated on Cisco ASR 1000 series routers.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.
15.1SY	This command was integrated into Cisco IOS Release 15.1SY. The **auto-tunnel** keyword was deprecated.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

IPv6 tunneling is the encapsulation of IPv6 packets within IPv4 packets and transmitting the packets across an IPv4 routing infrastructure.

Manually Configured Tunnels

The **tunnel mode ipv6ip** command configures an IPv6 tunnel. The devices at each end of the IPv6 tunnel must support both IPv4 and IPv6 protocol stacks.

To use this command, you must first manually configure the following:

- An IPv6 address on the tunnel interface
- An IPv4 address as the tunnel source
- An IPv4 address as the tunnel destination

Automatic Determination of Tunnel Destination

The **tunnel mode ipv6ip auto-tunnel** command configures an automatic IPv6 tunnel. The tunnel source is manually configured. The tunnel destination is automatically determined as the low-order 32 bits of the IPv4-compatible IPv6 addresses. An IPv4-compatible IPv6 address is a 128-bit IPv6 address that contains the IPv6 prefix 0:0:0:0:0:0 in the high-order 96 bits of the address and an IPv4 address in the low-order 32 bits of the address. The devices at each end of the automatic tunnel must support both IPv4 and IPv6 protocol stacks.

6to4 Tunnels

The **tunnel mode ipv6ip 6to4** command configures an automatic 6to4 tunnel where the tunnel endpoint is determined by a globally unique IPv4 address embedded into a 6to4 address. A 6to4 address is a combination of the prefix 2002::/16 and a globally unique 32-bit IPv4 address. (IPv4-compatible addresses are not used in 6to4 tunneling.) The unique IPv4 address is used as the network-layer address in the 6to4 address prefix. The source of the tunnel is an interface that you can manually configure using the **tunnel source** command. The border devices at each end of a 6to4 tunnel must support both IPv4 and IPv6 protocol stacks. Additionally, the traffic that is destined for the network with the 6to4 address prefix must be routed over the tunnel by using the **ipv6 route** command.

6RD Tunnels

The **tunnel mode ipv6ip 6rd** command specifies that the tunnel is to be used for IPv6 RD. The 6RD feature is similar to the 6to4 tunnel feature, but it does not require addresses to have a 2002::/16 prefix. It also does not require that all 32 bits of the IPv4 destination be in the IPv6 payload header.

ISATAP Tunnels

ISATAP tunnels enable the transportation of IPv6 packets within network boundaries. ISATAP tunnels allow individual IPv4 or IPv6 dual-stack hosts within a site to connect to an IPv6 network using the IPv4 infrastructure.

Unlike IPv4-compatible addresses, ISATAP IPv6 addresses can use any initial unicast /64 prefix. The last 64 bits are used as the interface identifier. Of these, the first 32 bits are the fixed pattern 0000:5EFE. The last 32 bits carry the tunnel endpoint IPv4 address.

Examples

Examples

The following example shows how to configure a manual IPv6 tunnel. In this example, tunnel interface 0 is manually configured with a global IPv6 address. The tunnel source and destination are also manually configured.

```
Device(config)# interface tunnel 0
Device(config-if)# ipv6 address 3ffe:b00:c18:1::3/127
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel destination 192.168.30.1
Device(config-if)# tunnel mode ipv6ip
Device(config-if)# end
```

Examples

The following example shows how to configure an automatic IPv6 tunnel that uses Ethernet interface 0 as the tunnel source. The tunnel destination is determined automatically as the low-order 32 bits of an IPv4-compatible IPv6 address.

```
Device(config)# interface tunnel 0
Device(config-if)# no ip address
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel mode ipv6ip auto-tunnel
Device(config-if)# end
```

Examples

The following example shows how to configure a 6to4 tunnel. In this example, Ethernet interface 0 is configured with an IPv4 address 192.168.99.1. The site-specific 48-bit prefix 2002:c0a8:630 is constructed by prepending the prefix 2002::/16 to the IPv4 address 192.168.99.1.

The tunnel interface 0 is configured without an IPv4 or IPv6 address. The tunnel source address is configured manually as Ethernet interface 0. The tunnel destination address is automatically constructed. An IPv6 static route is configured to route traffic that is destined for network 2002::/16 over tunnel interface 0.

```
Device(config)# interface ethernet 0
Device(config-if)# ip address 192.168.99.1 255.255.255.0
Device(config-if)# ipv6 address 2002:c0a8:6301:1::/64 eui-64
Device(config-if)# exit
Device(config)# interface tunnel 0
Device(config-if)# no ip address
Device(config-if)# ipv6 unnumbered ethernet 0
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel mode ipv6ip 6to4
Device(config-if)# exit
Device(config)# ipv6 route 2002::/16 tunnel 0
Device(config)# end
```

Examples

When a tunnel interface is configured using the **ipv6 unnumbered**, **tunnel source**, and **tunnel mode ipv6ip** commands, the tunnel uses the first IPv6 address configured on the source interface as its IPv6 address. For 6to4 tunnels, the first IPv6 address configured on the source interface must be a 6to4 address. In the following example, the first IPv6 address configured for Ethernet interface 0 (6to4 address 2002:c0a8:6301:1::/64) is used as the IPv6 address of tunnel 0:

```
Device(config)# interface tunnel 0
Device(config-if)# ipv6 unnumbered ethernet 0
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel mode ipv6ip 6to4
Device(config-if)# exit
Device(config)# interface ethernet 0
Device(config-if)# ipv6 address 2002:c0a8:6301:1::/64 eui-64
Device(config-if)# ipv6 address 3ffe:1234:5678::1/64
Device(config-if)# end
```

Examples

The following example shows how to configure a 6RD tunnel:

```
Device(config)# interface Tunnel1
Device(config-if)# ipv6 address 2001:B000:100::1/32
Device(config-if)# tunnel source GigabitEthernet2/0/0
Device(config-if)# tunnel mode ipv6ip 6rd
Device(config-if)# tunnel 6rd prefix 2001:B000::/32
Device(config-if)# tunnel 6rd ipv4 prefix-len 16 suffix-len 8
Device(config-if)# end
Device# show tunnel 6rd Tunnel1

Interface Tunnel1:
  Tunnel Source: 10.1.1.1
  6RD: Operational, V6 Prefix: 2001:B000::/32
       V4 Common Prefix Length: 16, Value: 10.1.0.0
       V4 Common Suffix Length: 8, Value: 0.0.0.1
```

Examples

The following example shows how to configure ISATAP tunnel over an Ethernet interface 0. Router advertisements are enabled to allow client autoconfiguration.

```
Device(config)# interface Ethernet 0
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config)# interface Tunnel 0
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel mode ipv6ip isatap
Device(config-if)# ipv6 address 2001:0DB8::/64 eui-64
Device(config-if)# no ipv6 nd ra suppress
Device(config-if)# end
```

Related Commands

Command	Description
ip address	Specifies the IP address of an IPv4 interface.
ipv6 address	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.

Command	Description
ipv6 address eui-64	Configures an IPv6 address for an interface and enables IPv6 processing on the interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 route	Establishes static IPv6 routes.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
no ipv6 nd ra suppress	Reenables the sending of IPv6 router advertisement transmissions on a LAN interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.
show tunnel 6rd tunnel	Displays 6RD information about a tunnel.
tunnel 6rd ipv4	Specifies the prefix length and suffix length of the IPv4 transport address that is common to all the 6RD routers in a domain.
tunnel 6rd prefix	Specifies the common IPv6 prefix on 6RD tunnels.
tunnel destination	Sets the destination address for a tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

validate source-mac

To check the source media access control (MAC) address against the link-layer address, use the **validate source-mac**command in Neighbor Discovery (ND) inspection policy configuration mode .

validate source-mac

no validate source-mac

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

ND inspection policy configuration (config-nd-inspection) RA guard policy configuration (config-ra-guard)

Command History

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

Usage Guidelines

When the router receives an ND message that contains a link-layer address, the source MAC address is checked against the link-layer address. Use the **validate source-mac** command to drop the packet if the link-layer address and the MAC addresses are different from each other.

Examples

The following example enables the router to drop an ND message whose link-layer address does not match the MAC address:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# validate source-mac
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the ND inspection policy n ame and enters ND inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

vrf (DHCPv6 pool)

To associate a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) address pool with a virtual private network (VPN) routing and forwarding (VRF) instance, use the **vrf** command in DHCPv6 pool configuration mode. To remove the VRF name, use the **no** form of this command.

vrf *name*

no vrf *name*

Syntax Description

name	Name of the VRF with which the address pool is associated.

Command Default

No VRF is associated with the DHCPv6 address pool.

Command Modes

DHCPv6 pool configuration (config-dhcp)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Examples

The following example shows how to configure an IPv6 pool named pool1, and associate pool1 with a VRF instance named vrf1:

```
Router(config)# ipv6 dhcp pool pool1
# vrf vrf1
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCPv6 configuration information pool and enters DHCPv6 pool configuration mode.