ipv6-r1

- vlan configuration, page 70

sec-level minimum

To specify the minimum security level parameter value when Cryptographically Generated Address (CGA) options are used, use the **sec-level minimum** command in Neighbor Discovery (ND) inspection policy configuration mode. To disable this function, use the **no** form of this command.

sec-level minimum *value*

no sec-level minimum *value*

Syntax Description

value	Minimum security level, which is a value from 1 to 7. The default security level is 1. The most secure level is 3.

Command Default

The default security level is 1.

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

Usage Guidelines

The **sec-level minimum** command specifies the minimum security level parameter value when CGA options are used. Use the **sec-level minimum** command after enabling ND inspection policy configuration mode using the **ipv6 nd inspection policy** command.

Examples

The following example defines an ND policy name as policy1, places the router in ND inspection policy configuration mode, and specifies 2 as the minimum CGA security level:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# sec-level minimum 2
```

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.

server name (IPv6 TACACS+)

To specify an IPv6 TACACS+ server, use the **server name**command in TACACS+ group server configuration mode. To remove the IPv6 TACACS+ server from configuration, use the **no** form of this command.

server name *server-name*

no server name *server-name*

Syntax Description

server-name	The IPv6 TACACS+ server to be used.

Command Default

No server name is specified.

Command Modes

TACACS+ group server configuration (config-sg-tacacs+)

Command History

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

Usage Guidelines

You must configure the **aaa group server tacacs** command before configuring this command.

Enter the **server name** command to specify an IPv6 TACACS+ server.

Examples

The following example shows how to specify an IPv6 TACACS+ server named server1:

```
Router(config)# aaa group server tacacs+
Router(config-sg-tacacs+)# server name server1
```

Related Commands

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

show ipv6 access-list

To display the contents of all current IPv6 access lists, use the **show ipv6 access-list**command in user EXEC or privileged EXEC mode.

show ipv6 access-list [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of access list.

Command Default

All IPv6 access lists are displayed.

Command Modes

User EXEC Privileged EXEC

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.
12.0(23)S	The priority field was changed to sequence and Layer 4 protocol information (extended IPv6 access list functionality) was added to the display output.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)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.
12.2(50)SY	This command was modified. Information about IPv4 and IPv6 hardware statistics is displayed.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **show ipv6 access-list** command provides output similar to the **show ip access-list** command, except that it is IPv6-specific.

Examples

The following output from the **show ipv6 access-list**command shows IPv6 access lists named inbound, tcptraffic, and outbound:

```
Router# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
       left 243) sequence 1
    permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
    (time left 296) sequence 2
IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

The following sample output shows IPv6 access list information for use with IPSec:

```
Router#  show ipv6 access-list
IPv6 access list Tunnel0-head-0-ACL (crypto)
     permit ipv6 any any (34 matches) sequence 1
IPv6 access list Ethernet2/0-ipsecv6-ACL (crypto)
     permit 89 FE80::/10 any (85 matches) sequence 1
```

The table below describes the significant fields shown in the display.

Table 1: show ipv6 access-list Field Descriptions

Field	Description
ipv6 access list inbound	Name of the IPv6 access list, for example, inbound.
permit	Permits any packet that matches the specified protocol type.
tcp	Transmission Control Protocol. The higher-level (Layer 4) protocol type that the packet must match.
any	Equal to ::/0.
eq	An equal operand that compares the source or destination ports of TCP or UDP packets.
bgp	Border Gateway Protocol. The lower-level (Layer 3) protocol type that the packet must be equal to.
reflect	Indicates a reflexive IPv6 access list.

Field	Description
tcptraffic (8 matches)	The name of the reflexive IPv6 access list and the number of matches for the access list. The **clear ipv6 access-list** privileged EXEC command resets the IPv6 access list match counters.
sequence 10	Sequence in which an incoming packet is compared to lines in an access list. Lines in an access list are ordered from first priority (lowest number, for example, 10) to last priority (highest number, for example, 80).
host 2001:0DB8:1::1	The source IPv6 host address that the source address of the packet must match.
host 2001:0DB8:1::2	The destination IPv6 host address that the destination address of the packet must match.
11000	The ephemeral source port number for the outgoing connection.
timeout 300	The total interval of idle time (in seconds) after which the temporary IPv6 reflexive access list named tcptraffic will time out for the indicated session.
(time left 243)	The amount of idle time (in seconds) remaining before the temporary IPv6 reflexive access list named tcptraffic is deleted for the indicated session. Additional received traffic that matches the indicated session resets this value to 300 seconds.
evaluate udptraffic	Indicates the IPv6 reflexive access list named udptraffic is nested in the IPv6 access list named outbound.

Related Commands

Command	Description
clear ipv6 access-list	Resets the IPv6 access list match counters.
hardware statistics	Enables the collection of hardware statistics.
show ip access-list	Displays the contents of all current IP access lists.
show ip prefix-list	Displays information about a prefix list or prefix list entries.

Command	Description
show ipv6 prefix-list	Displays information about an IPv6 prefix list or IPv6 prefix list entries.

show ipv6 dhcp conflict

To display address conflicts found by a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server when addresses are offered to the client, use the **show ipv6 dhcp conflict** command in privileged EXEC mode.

show ipv6 dhcp conflict [*ipv6-address*] [**vrf** *vrf-name*]

Syntax Description

ipv6-address	(Optional) The address of a DHCP for IPv6 client.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

When you configure the DHCPv6 server to detect conflicts, it uses ping. The client uses neighbor discovery to detect clients and reports to the server through a DECLINE message. If an address conflict is detected, the address is removed from the pool, and the address is not assigned until the administrator removes the address from the conflict list.

Examples

The following is a sample output from the **show ipv6 dhcp conflict** command. This command shows the pool and prefix values for DHCP conflicts.:

```
Router# show ipv6 dhcp conflict
Pool 350, prefix 2001:0DB8:1005::/48
     2001:0DB8:1005::10
```

Related Commands

Command	Description
clear ipv6 dhcp conflict	Clears an address conflict from the DHCPv6 server database.

show ipv6 interface

To display the usability status of interfaces configured for IPv6, use the **show ipv6 interface**command in user EXEC or privileged EXEC mode.

show ipv6 interface [brief] [*type number*] **[prefix]**

Syntax Description

brief	(Optional) Displays a brief summary of IPv6 status and configuration for each interface.
type	(Optional) The interface type about which to display information.
number	(Optional) The interface number about which to display information.
prefix	(Optional) Prefix generated from a local IPv6 prefix pool.

Command Default

All IPv6 interfaces are displayed.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(4)T	The OK, TENTATIVE, DUPLICATE, ICMP redirects, and ND DAD fields were added to the command output.
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(25)S	Command output was updated to display information on the current Unicast RPF configuration.
12.4(2)T	Command output was updated to show the state of the default router preference (DRP) preference value as advertised by a device through an interface.

Release	Modification
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.
12.4(4)T	Command output was updated to show Hot Standby Router Protocol (HSRP) for IPv6 information.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series devices.
12.4(24)T	Command output was updated to show the Dynamic Host Configuration Protocol (DHCP) originated addresses.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **show ipv6 interface** command provides output similar to the show ip interface command, except that it is IPv6-specific.

Use the **show ipv6 interface** command to validate the IPv6 status of an interface and its configured addresses. The show ipv6 interface command also displays the parameters that IPv6 is using for operation on this interface and any configured features.

If the interface's hardware is usable, the interface is marked up. If the interface can provide two-way communication for IPv6, the line protocol is marked up.

If you specify an optional interface type and number, the command displays information only about that specific interface. For a specific interface, you can enter the prefix keyword to see the IPv6 neighbor discovery (ND) prefixes that are configured on the interface.

Examples

Examples

The **show ipv6 interface**command displays information about the specified interface.

```
Device(config)# show ipv6 interface ethernet0/0
Ethernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:6700
  No Virtual link-local address(es):
  Global unicast address(es):
    2001::1, subnet is 2001::/64 [DUP]
```

```
    2001::A8BB:CCFF:FE00:6700, subnet is 2001::/64 [EUI]
    2001:100::1, subnet is 2001:100::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF00:6700
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

The table below describes the significant fields shown in the display.

Table 2: show ipv6 interface Field Descriptions

Field	Description
Ethernet0/0 is up, line protocol is up	Indicates whether the interface hardware is active (whether line signal is present) and whether it has been taken down by an administrator. If the interface hardware is usable, the interface is marked "up." For an interface to be usable, both the interface hardware and line protocol must be up.
line protocol is up, down (down is not shown in sample output)	Indicates whether the software processes that handle the line protocol consider the line usable (that is, whether keepalives are successful or IPv6 CP has been negotiated). If the interface can provide two-way communication, the line protocol is marked up. For an interface to be usable, both the interface hardware and line protocol must be up.
IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output)	Indicates that IPv6 is enabled, stalled, or disabled on the interface. If IPv6 is enabled, the interface is marked "enabled." If duplicate address detection processing identified the link-local address of the interface as being a duplicate address, the processing of IPv6 packets is disabled on the interface and the interface is marked "stalled." If IPv6 is not enabled, the interface is marked "disabled."
link-local address	Displays the link-local address assigned to the interface.
Global unicast address(es):	Displays the global unicast addresses assigned to the interface.
Joined group address(es):	Indicates the multicast groups to which this interface belongs.

Field	Description
MTU	Maximum transmission unit of the interface.
ICMP error messages	Specifies the minimum interval (in milliseconds) between error messages sent on this interface.
ICMP redirects	The state of Internet Control Message Protocol (ICMP) IPv6 redirect messages on the interface (the sending of the messages is enabled or disabled).
ND DAD	The state of duplicate address detection on the interface (enabled or disabled).
number of DAD attempts:	Number of consecutive neighbor solicitation messages that are sent on the interface while duplicate address detection is performed.
ND reachable time	Displays the neighbor discovery reachable time (in milliseconds) assigned to this interface.
ND advertised reachable time	Displays the neighbor discovery reachable time (in milliseconds) advertised on this interface.
ND advertised retransmit interval	Displays the neighbor discovery retransmit interval (in milliseconds) advertised on this interface.
ND router advertisements	Specifies the interval (in seconds) for neighbor discovery router advertisements (RAs) sent on this interface and the amount of time before the advertisements expire. As of Cisco IOS Release 12.4(2)T, this field displays the default router preference (DRP) value sent by this device on this interface.
ND advertised default router preference is Medium	The DRP for the device on a specific interface.

Examples

The **show ipv6 interface** command displays information about attributes that may be associated with an IPv6 address assigned to the interface.

Attribute	Description
ANY	Anycast. The address is an anycast address, as specified when configured using the **ipv6 address** command.
CAL	Calendar. The address is timed and has valid and preferred lifetimes.

Attribute	Description
DEP	Deprecated. The timed address is deprecated.
DUP	Duplicate. The address is a duplicate, as determined by duplicate address detection (DAD). To re-attampt DAD, the user must use the **shutdown** or **no shutdown** command on the interface.
EUI	EUI-64 based. The address was generated using EUI-64.
OFF	Offlink. The address is offlink.
OOD	Overly optimistic DAD. DAD will not be performed for this address. This attribute applies to virtual addresses.
PRE	Preferred. The timed address is preferred.
TEN	Tentative. The address is in a tentative state per DAD.
UNA	Unactivated. The virtual address is not active and is in a standby state.
VIRT	Virtual. The address is virtual and is managed by HSRP, VRRP, or GLBP.

The following is sample output from the **show ipv6 interface**command when entered with the **brief** keyword:

```
Device# show ipv6 interface brief
Ethernet0 is up, line protocol is up
Ethernet0                  [up/up]
    unassigned
Ethernet1                  [up/up]
    2001:0DB8:1000:/29
Ethernet2                  [up/up]
    2001:0DB8:2000:/29
Ethernet3                  [up/up]
    2001:0DB8:3000:/29
Ethernet4                  [up/down]
    2001:0DB8:4000:/29
Ethernet5                  [administratively down/down]
    2001:123::210:7BFF:FEC2:ACD8
Interface         Status                IPv6 Address
Ethernet0         up                    3FFE:C00:0:1:260:3EFF:FE11:6770
Ethernet1         up                    unassigned
Fddi0             up                    3FFE:C00:0:2:260:3EFF:FE11:6772
Serial0           administratively down unassigned
Serial1           administratively down unassigned
Serial2           administratively down unassigned
Serial3           administratively down unassigned
Tunnel0           up                    unnumbered (Ethernet0)
Tunnel1           up                    3FFE:700:20:1::12
```

Examples

This sample output shows the characteristics of an interface that has generated a prefix from a local IPv6 prefix pool:

```
Device# show ipv6 interface Ethernet 0/0 prefix

interface Ethernet0/0
 ipv6 address 2001:0DB8::1/64
 ipv6 address 2001:0DB8::2/64
 ipv6 nd prefix 2001:0DB8:2::/64
 ipv6 nd prefix 2001:0DB8:3::/64 2592000 604800 off-link
end
.
.
.
IPv6 Prefix Advertisements Ethernet0/0
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default
       N - Not advertised, C - Calendar
     default [LA] Valid lifetime 2592000, preferred lifetime 604800
AD   2001:0DB8:1::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
APD  2001:0DB8:2::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
P    2001:0DB8:3::/64 [A] Valid lifetime 2592000, preferred lifetime 604800
```

The default prefix shows the parameters that are configured using the ipv6 nd prefix default command.

Examples

This sample output shows the state of the DRP preference value as advertised by this device through an interface:

```
Device# show ipv6 interface gigabitethernet 0/1
  GigabitEthernet0/1 is up, line protocol is up
    IPv6 is enabled, link-local address is FE80::130
    Description: Management network (dual stack)
    Global unicast address(es):
      FEC0:240:104:1000::130, subnet is FEC0:240:104:1000::/64
    Joined group address(es):
      FF02::1
      FF02::2
      FF02::1:FF00:130
    MTU is 1500 bytes
    ICMP error messages limited to one every 100 milliseconds
    ICMP redirects are enabled
    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
    ND advertised default router preference is Low
    Hosts use stateless autoconfig for addresses.
```

Examples

When HSRP IPv6 is first configured on an interface, the interface IPv6 link-local address is marked unactive (UNA) because it is no longer advertised, and the HSRP IPv6 virtual link-local address is added to the virtual link-local address list with the UNA and tentative DAD (TEN) attributes set. The interface is also programmed to listen for the HSRP IPv6 multicast address.

This sample output shows the status of UNA and TEN attributes, when HSRP IPv6 is configured on an interface:

```
Device# show ipv6 interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80:2::2 [UNA]
  Virtual link-local address(es):
```

```
    FE80::205:73FF:FEA0:1 [UNA/TEN]
  Global unicast address(es):
    2001:2::2, subnet is 2001:2::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::66
    FF02::1:FF00:2
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ND DAD is enabled, number of DAD attempts: 1
```

After the HSRP group becomes active, the UNA and TEN attributes are cleared, and the overly optimistic DAD (OOD) attribute is set. The solicited node multicast address for the HSRP virtual IPv6 address is also added to the interface.

This sample output shows the status of UNA, TEN and OOD attributes, when HSRP group is activated:

```
Device# show ipv6 interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80:2::2 [UNA]
  Virtual link-local address(es):
    FE80::205:73FF:FEA0:1 [OPT]
  Global unicast address(es):
    2001:2::2, subnet is 2001:2::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::66
    FF02::1:FF00:2
    FF02::1:FFA0:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
```

The table below describes additional significant fields shown in the displays for the **show ipv6 interface** command with HSRP configured.

Table 3: show ipv6 interface Command with HSRP Configured Field Descriptions

Field	Description
IPv6 is enabled, link-local address is FE80:2::2 [UNA]	The interface IPv6 link-local address is marked UNA because it is no longer advertised.
FE80::205:73FF:FEA0:1 [UNA/TEN]	The virtual link-local address list with the UNA and TEN attributes set.
FF02::66	HSRP IPv6 multicast address.
FE80::205:73FF:FEA0:1 [OPT]	HSRP becomes active, and the HSRP virtual address marked OPT.
FF02::1:FFA0:1	HSRP solicited node multicast address.

Examples

When you enable Mobile IPv6 on an interface, you can configure a minimum interval between IPv6 router advertisement (RA) transmissions. The **show ipv6 interface** command output reports the minimum RA interval, when configured. If the minimum RA interval is not explicitly configured, then it is not displayed.

In the following example, the maximum RA interval is configured as 100 seconds, and the minimum RA interval is configured as 60 seconds on Ethernet interface 1/0:

```
Device(config-if)# ipv6 nd ra-interval 100 60
```

Subsequent use of the **show ipv6 interface** then displays the interval as follows:

```
Device(config)# show ipv6 interface ethernet 1/0
Ethernet1/0 is administratively down, line protocol is down
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:5A01 [TEN]
  No Virtual link-local address(es):
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  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 60 to 100 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

In the following example, the maximum RA interval is configured as 100 milliseconds (ms), and the minimum RA interval is configured as 60 ms on Ethernet interface 1/0:

```
Device(config)# show ipv6 interface ethernet 1/0
Ethernet1/0 is administratively down, line protocol is down
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:5A01 [TEN]
  No Virtual link-local address(es):
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  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 60 to 100 milliseconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

The table below describes additional significant fields shown in the displays for the **show ipv6 interface** command with minimum RA interval information configured.

Table 4: show ipv6 interface Command with Minimum RA Interval Information Configuration Field Descriptions

Field	Description
ND router advertisements are sent every 60 to 100 seconds	ND RAs are sent at an interval randomly selected from a value between the minimum and maximum values. In this example, the minimum value is 60 seconds, and the maximum value is 100 seconds.

Field	Description
ND router advertisements are sent every 60 to 100 milliseconds	ND RAs are sent at an interval randomly selected from a value between the minimum and maximum values. In this example, the minimum value is 60 ms, and the maximum value is 100 ms.

Related Commands

Command	Description
ipv6 nd prefix	Configures which IPv6 prefixes are included in IPv6 router advertisements.
ipv6 nd ra interval	Configures the interval between IPv6 RA transmissions on an interface.
show ip interface	Displays the usability status of interfaces configured for IP.

show ipv6 mld snooping

To display Multicast Listener Discovery version 2 (MLDv2) snooping information, use the **show ipv6 mld snooping** command in privileged EXEC mode.

show ipv6 mld [**vrf** *vrf-name*] **snooping** {**explicit-tracking vlan** *vlan*| **mrouter** [**vlan** *vlan*]| **report-suppression vlan** *vlan*| **statistics vlan** *vlan*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
explicit-tracking vlan *vlan*	Displays the status of explicit host tracking.
mrouter	Displays the multicast router interfaces on an optional VLAN.
vlan *vlan*	(Optional) Specifies the VLAN number on the multicast router interfaces.
report-suppression vlan *vlan*	Displays the status of the report suppression.
statistics vlan *vlan*	Displays MLD snooping information on a VLAN.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

You can enter the **show ipv6 mld snooping mrouter** command without arguments to display all the multicast router interfaces.

Examples

This example shows how to display explicit tracking information on VLAN 25:

```
Router# show ipv6 mld snooping explicit-tracking vlan 25
Source/Group                    Interface    Reporter        Filter_mode
-------------------------------------------------------------------------
10.1.1.1/226.2.2.2              Vl25:1/2     10.27.2.3       INCLUDE
10.2.2.2/226.2.2.2              Vl25:1/2     10.27.2.3       INCLUDE
```

This example shows how to display the multicast router interfaces in VLAN 1:

```
Router# show
ipv6 mld snooping mrouter vlan 1
vlan            ports
-----+---------------------------------------
  1          Gi1/1,Gi2/1,Fa3/48,Router
```

This example shows the MLD snooping statistics information for VLAN 25:

```
Router# show ipv6 mld
 snooping statistics interface vlan 25
Snooping staticstics for Vlan25
#channels:2
#hosts   :1

Source/Group            Interface       Reporter      Uptime        Last-Join   Last-Leave
10.1.1.1/226.2.2.2      Gi1/2:Vl25      10.27.2.3     00:01:47      00:00:50      -
10.2.2.2/226.2.2.2      Gi1/2:Vl25      10.27.2.3     00:01:47      00:00:50      -
```

Related Commands

Command	Description
ipv6 mld snooping	Enables MLDv2 snooping globally.
ipv6 mld snooping explicit-tracking	Enables explicit host tracking.
ipv6 mld snooping querier	Enables the MLDv2 snooping querier.
ipv6 mld snooping report-suppression	Enables report suppression on a VLAN.

show ipv6 nd ra-throttle policy

To display information about an IPv6 router advertisement (RA) throttler policy, use the **show ipv6 nd ra-throttle policy** command in privileged EXEC mode.

show ipv6 nd ra-throttle policy *policy-name*

Syntax Description

policy-name	RA throttler policy name.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use the **show ipv6 nd ra-throttle policy** to display IPv6 RA throttler information for troubleshooting purposes.

Examples

```
Device# show ipv6 nd ra-throttle policy policy2

Policy policy2 configuration:
        The throttle period will be coalesced and default to 600 seconds
        Applied to a port, this policy indicates a wired interface
        The maximum number of unthrottled RAs is configured on the vlan and defaults to 10
       The min and max numbers of unthrottled RAs per device will be coalesced and default
 to 10
      The behaviour upon RAs with an RFC 3775 interval option will be coalesced and default
 to passthrough

Policy applied on the following interfaces:
  Et0/0                vlan all
Policy applied on the following vlans:
  10,12-17
```

show ipv6 nd ra-throttle vlan

To display information about the actions of an IPv6 router advertisement (RA) throttler policy on a VLAN, use the **show ipv6 nd ra-throttle vlan** command in privileged EXEC mode.

show ipv6 nd ra-throttle vlan *vlan-id*[**advertising-routers**| **pending-hosts**]

Syntax Description

vlan-id	A VLAN or a collection of VLANs.
advertising-routers	(Optional) Displays information about devices that issued RAs recently.
pending-hosts	(Optional) Displays information about wireless hosts that are expecting RAs.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use the **show ipv6 nd ra-throttle vlan** command to display information about the actions of an IPv6 RA throttler policy on a VLAN.

Examples

```
Device# show ipv6 nd ra-throttle vlan vlan1

general information for vlan1
---------------------------------

 RAs             last period     this period    overall
 passed_through  1               1              2
 throttled       4               2              6

 no pending host

current policy is tutu coalesced as:

  throttle-period 90 seconds remaining 48
  max-through 0
  allow at-least 1 at-most 1
  interval-option passthrough
```

show ipv6 nd raguard policy

To display a router advertisements (RAs) guard policy on all interfaces configured with the RA guard feature, use the **show ipv6 nd raguard policy** command in privileged EXEC mode.

show ipv6 nd raguard policy [*policy-name*]

Syntax Description

policy-name	(Optional) RA guard policy name.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The **show ipv6 nd raguard policy** command displays the options configured for the policy on all interfaces configured with the RA guard feature.

Examples

The following example shows the policy configuration for a policy named raguard1 and all the interfaces where the policy is applied:

```
Router# show ipv6 nd raguard policy interface raguard1

Policy raguard1 configuration:
  device-role host
Policy applied on the following interfaces:
  Et0/0        vlan all
  Et1/0        vlan all
```

The table below describes the significant fields shown in the display.

Table 5: show ipv6 nd raguard policy Field Descriptions

Field	Description
Policy raguard1 configuration:	Configuration of the specified policy.

Field	Description
device-role host	The role of the device attached to the port. This device configuration is that of host.
Policy applied on the following interfaces:	The specified interface on which the RA guard feature is configured.

show ipv6 neighbor binding

To display contents of a binding table, use the **show ipv6 neighbor binding** command in privileged EXEC mode.

show ipv6 neighbor binding [**vlan** *vlan-id*| **interface** *type number*| **ipv6** *ipv6-address*| **mac** *mac-address*]

Syntax Description

vlan *vlan-id*	(Optional) Displays the binding table entries that match the specified VLAN.
interface *type number*	(Optional) Displays the binding table entries that match the specified interface type and number.
ipv6 *ipv6-address*	(Optional) Displays the binding table entries that match the specified IPv6 address.
mac *mac-address*	(Optional) Displays the binding table entries that match the specified Media Access Control (MAC) address.

Command Modes

Privileged EXEC (#)

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

Usage Guidelines

The **show ipv6 neighbor binding** command displays the contents of the binding table. The display output can be specified by the specified VLAN, interface, IPv6 address, or MAC address. If no keywords or arguments are entered, all binding table contents are displayed.

The following keyword and argument combinations are allowed:

- **vlan** *vlan-id*: Displays all entries for the specified VLAN.
- **interface** *type number*: Displays all entries for the specified interface.
- **ipv6** *ipv6-address* + **interface** *type number* + **vlan** *vlan-id*: Displays a single entry that matches these three keyword and argument combinations.

- **ipv6** *ipv6-address* + **interface** *type number*: Displays all entries for the specified IPv6 address and interface.
- **ipv6** *ipv6-address*: Displays all entries for the specified IPv6 address.

Examples

The following example displays the contents of a binding table:

```
Router# show ipv6 neighbor binding

address DB has 4 entries
Codes: L - Local, S - Static, ND - Neighbor Discovery
Preflevel (prlvl) values:
1:Not secure          2:MAC and LLA match   3:Cga authenticated
4:Dhcp assigned       5:Cert authenticated  6:Cga and Cert auth
7:Trusted port        8:Statically assigned
    IPv6 address            Link-Layer addr Interface   vlan  prlvl age state    Time left
ND  FE80::A8BB:CCFF:FE01:F500  AABB.CC01.F500  Et0/0     100  0002    0 REACHABLE  8850
L   FE80::21D:71FF:FE99:4900   001D.7199.4900  Vl100     100  0080 7203 DOWN       N/A
ND  2001:600::1                AABB.CC01.F500  Et0/0     100  0003    0 REACHABLE  3181
ND  2001:300::1                AABB.CC01.F500  Et0/0     100  0007    0 REACHABLE  9559
ND  2001:100::2                AABB.CC01.F600  Et1/0     200  0002    0 REACHABLE  9196
L   2001:400::1                001D.7199.4900  Vl100     100  0080 7188 DOWN       N/A
S   2001:500::1                000A.000B.000C  Fa4/13    300  0080 8676 STALE      N/A
```

The table below describes the significant fields shown in the display.

Table 6: show ipv6 neighbor binding Field Descriptions

Field	Description
address DB has *n* entries	Number of entries in the specified database.

Related Commands

Command	Description
ipv6 neighbor binding	Changes the defaults of neighbor binding entries in a binding table.

show ipv6 neighbors

To display IPv6 neighbor discovery (ND) cache information, use the **show ipv6 neighbors** command in user EXEC or privileged EXEC mode.

show ipv6 neighbors [*interface-type interface-number*| *ipv6-address*| *ipv6-hostname*| **statistics**]

Syntax Description

interface-type	(Optional) Specifies the type of the interface from which IPv6 neighbor information is to be displayed.
interface-number	(Optional) Specifies the number of the interface from which IPv6 neighbor information is to be displayed.
ipv6-address	(Optional) Specifies the 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.
ipv6-hostname	(Optional) Specifies the IPv6 hostname of the remote networking device.
statistics	(Optional) Displays ND cache statistics.

Command Default

All IPv6 ND cache entries are listed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	This command was modified. Support for static entries in the IPv6 neighbor discovery cache was added to the command output.
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.

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 and introduced on Cisco ASR 1000 Series devices.
Cisco IOS XE Release 2.6	This command was modified. This command was updated to display the number and the limit of ND cache entries on a particular interface.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
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

When the *interface-type* and *interface-number* arguments are not specified, cache information for all IPv6 neighbors is displayed. Specifying the *interface-type* and *interface-number* arguments displays only cache information about the specified interface.

Specifying the **statistics** keyword displays ND cache statistics.

Examples

The following is sample output from the **show ipv6 neighbors** command when entered with an interface type and number:

```
Device# show ipv6 neighbors ethernet 2
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH Ethernet2
FE80::203:A0FF:FED6:141E                    0 0003.a0d6.141e  REACH Ethernet2
3001:1::45a                                 - 0002.7d1a.9472  REACH Ethernet2
```

The following is sample output from the **show ipv6 neighbors** command when entered with an IPv6 address:

```
Device# show ipv6 neighbors 2000:0:0:4::2
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH Ethernet2
```

The table below describes the significant fields shown in the displays.

Table 7: show ipv6 neighbors Field Descriptions

Field	Description
IPv6 Address	IPv6 address of neighbor or interface.
Age	Time (in minutes) since the address was confirmed to be reachable. A hyphen (-) indicates a static entry.

Field	Description
Link-layer Addr	MAC address. If the address is unknown, a hyphen (-) is displayed.

Field	Description
State	

Field	Description
	The state of the neighbor cache entry. Following are the states for dynamic entries in the IPv6 neighbor discovery cache: • INCMP (Incomplete)--Address resolution is being performed on the entry. A neighbor solicitation message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received. • REACH (Reachable)--Positive confirmation was received within the last ReachableTime milliseconds that the forward path to the neighbor was functioning properly. While in REACH state, the device takes no special action as packets are sent. • STALE--More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent. • DELAY--More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a neighbor solicitation message and change the state to PROBE. • PROBE--A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received. • ????--Unknown state. Following are the possible states for static entries in the IPv6 neighbor discovery cache: • INCMP (Incomplete)--The interface for this entry is down. • REACH (Reachable)--The interface for this entry is up.

Field	Description
	Note Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the INCMP (Incomplete) and REACH (Reachable) states are different for dynamic and static cache entries.
Interface	Interface from which the address was reachable.

The following is sample output from the **show ipv6 neighbors** command with the **statistics** keyword:

```
Device# show ipv6 neighbor statistics

IPv6 ND Statistics
 Entries 2, High-water 2, Gleaned 1, Scavenged 0
 Entry States
   INCMP 0  REACH 0  STALE 2  GLEAN 0  DELAY 0  PROBE 0
 Resolutions (INCMP)
   Requested 1, timeouts 0, resolved 1, failed 0
   In-progress 0, High-water 1, Throttled 0, Data discards 0
 Resolutions (PROBE)
   Requested 3, timeouts 0, resolved 3, failed 0
```

The table below describes the significant fields shown in this display:

Table 8: show ipv6 neighbors statistics Field Descriptions

Field	Description
Entries	Total number of ND neighbor entries in the ND cache.
High-Water	Maximum amount (so far) of ND neighbor entries in ND cache.
Gleaned	Number of ND neighbor entries gleaned (that is, learned from a neighbor NA or other ND packet).
Scavenged	Number of stale ND neighbor entries that have timed out and been removed from the cache.
Entry States	Number of ND neighbor entries in each state.

Field	Description
Resolutions (INCMP)	Statistics for neighbor resolutions attempted in INCMP state (that is, resolutions prompted by a data packet). Details about the resolutions attempted in INCMP state are follows: • Requested--Total number of resolutions requested. • Timeouts--Number of timeouts during resolutions. • Resolved--Number of successful resolutions. • Failed--Number of unsuccessful resolutions. • In-progress--Number of resolutions in progress. • High-water--Maximum number (so far) of resolutions in progress. • Throttled--Number of times resolution request was ignored due to maximum number of resolutions in progress limit. • Data discards--Number of data packets discarded that are awaiting neighbor resolution.
Resolutions (PROBE)	Statistics for neighbor resolutions attempted in PROBE state (that is, re-resolutions of existing entries prompted by a data packet): • Requested--Total number of resolutions requested. • Timeouts--Number of timeouts during resolutions. • Resolved--Number of successful resolutions. • Failed--Number of unsuccessful resolutions.

show ipv6 protocols

To display the parameters and the current state of the active IPv6 routing protocol processes, use the **show ipv6 protocols** command in user EXEC or privileged EXEC mode.

show ipv6 protocols [summary]

Syntax Description

summary	(Optional) Displays the configured routing protocol process names.

Command Modes

User EXEC (>)

Privileged EXEC (#)

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.
12.4(15)T	This command was modified. The command output was enhanced to provide Enhanced Interior Gateway Routing Protocol (EIGRP) information, including the vector metric.
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 implemented on Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.6	This command was modified. The command output was enhanced to include information about EIGRP IPv6 Nonstop Forwarding (NSF).
15.2(2)S	This command was modified. The command output was enhanced to include information about EIGRP IPv6 NSF.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The information displayed by the **show ipv6 protocols** command is useful in debugging routing operations.

Examples

The following sample output from the **show ipv6 protocols** command displays Intermediate System-to-Intermediate System (IS-IS) routing protocol information:

```
Device# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "isis"
  Interfaces:
    Ethernet0/0/3
    Ethernet0/0/1
    Serial1/0/1
    Loopback1 (Passive)
    Loopback2 (Passive)
    Loopback3 (Passive)
    Loopback4 (Passive)
    Loopback5 (Passive)
  Redistribution:
    Redistributing protocol static at level 1
  Inter-area redistribution
    Redistributing L1 into L2 using prefix-list word
  Address Summarization:
    L2: 33::/16  advertised with metric 0
    L2: 44::/16  advertised with metric 20
    L2: 66::/16  advertised with metric 10
    L2: 77::/16  advertised with metric 10
```

The table below describes the significant fields shown in the display.

Table 9: show ipv6 protocols Field Descriptions for IS-IS Processes

Field	Description
IPv6 Routing Protocol is	Specifies the IPv6 routing protocol used.
Interfaces	Specifies the interfaces on which the IPv6 IS-IS protocol is configured.
Redistribution	Lists the protocol that is being redistributed.
Inter-area redistribution	Lists the IS-IS levels that are being redistributed into other levels.
using prefix-list	Names the prefix list used in the interarea redistribution.
Address Summarization	Lists all the summary prefixes. If the summary prefix is being advertised, "advertised with metric *x*" will be displayed after the prefix.

The following sample output from the **show ipv6 protocols** command displays the Border Gateway Protocol (BGP) information for autonomous system 30:

```
Device# show ipv6 protocols

IPv6 Routing Protocol is "bgp 30"
  IGP synchronization is disabled
  Redistribution:
    Redistributing protocol connected
  Neighbor(s):
    Address                  FiltIn FiltOut Weight RoutemapIn RoutemapOut
    2001:DB8:0:ABCD::1          5       7    200
    2001:DB8:0:ABCD::2                            rmap-in    rmap-out
    2001:DB8:0:ABCD::3                            rmap-in    rmap-out
```

The table below describes the significant fields shown in the display.

Table 10: show ipv6 protocols Field Descriptions for BGP Process

Field	Description
IPv6 Routing Protocol is	Specifies the IPv6 routing protocol used.
Redistribution	Lists the protocol that is being redistributed.
Address	Neighbor IPv6 address.
FiltIn	AS-path filter list applied to input.
FiltOut	AS-path filter list applied to output.
Weight	Neighbor weight value used in BGP best path selection.
RoutemapIn	Neighbor route map applied to input.
RoutemapOut	Neighbor route map applied to output.

The following is sample output from the **show ipv6 protocols summary** command:

```
Device# show ipv6 protocols summary

Index Process Name
0     connected
1     static
2     rip myrip
3     bgp 30
```

The following sample output from the **show ipv6 protocols** command displays the EIGRP information including the vector metric and EIGRP IPv6 NSF:

```
Device# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "bgp 1"
  IGP synchronization is disabled
  Redistribution:
    None
IPv6 Routing Protocol is "bgp multicast"
```

```
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "eigrp 1"
EIGRP-IPv6 VR(name) Address-Family Protocol for AS(1)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0 K6=0
  Metric rib-scale 128
  Metric version 64bit
  NSF-aware route hold timer is 260
  EIGRP NSF enabled
     NSF signal timer is 15s
     NSF converge timer is 65s
  Router-ID: 10.1.2.2
  Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 16
    Maximum hopcount 100
    Maximum metric variance 1
    Total Prefix Count: 0
    Total Redist Count: 0

  Interfaces:
  Redistribution:
    None
```

The following example displays IPv6 protocol information after configuring redistribution in an Open Shortest Path First (OSPF) domain:

```
Device# redistribute ospf 1 match internal
Device(config-rtr)# end
Device# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip 1"
  Interfaces:
    Ethernet0/1
    Loopback9
  Redistribution:
    Redistributing protocol ospf 1 (internal)
IPv6 Routing Protocol is "ospf 1"
  Interfaces (Area 0):
    Ethernet0/0
  Redistribution:
    None
```

show ipv6 route

To display contents of the IPv6 routing table, use the **show ipv6 route** command in user EXEC or privileged EXEC mode.

show ipv6 route [*ipv6-address*| *ipv6-prefix*/*prefix-length* [**longer-prefixes**]| [*protocol*] | [**repair**] | [**updated** [**boot-up**] [*day month*] [*time*]]| **interface** *type number*| **nd**| **nsf**| **table** *table-id* | **watch**]

Syntax Description

ipv6-address	(Optional) Displays routing information for a specific IPv6 address.
ipv6-prefix	(Optional) Displays routing information for a specific IPv6 network.
/*prefix-length*	(Optional) 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.
longer-prefixes	(Optional) Displays output for longer prefix entries.
protocol	(Optional) The name of a routing protocol or the keyword **connected**, **local**, **mobile**, or **static**. If you specify a routing protocol, use one of the following keywords: **bgp**, **isis**, **eigrp**, **ospf**, or **rip**.
repair	(Optional) Displays routes with repair paths.
updated	(Optional) Displays routes with time stamps.
boot-up	(Optional) Displays routing information since bootup.
day month	(Optional) Displays routes since the specified day and month.
time	(Optional) Displays routes since the specified time, in *hh:mm* format.
interface	(Optional) Displays information about the interface.
type	(Optional) Interface type.
number	(Optional) Interface number.
nd	(Optional) Displays only routes from the IPv6 Routing Information Base (RIB) that are owned by Neighbor Discovery (ND).

nsf	(Optional) Displays routes in the nonstop forwarding (NSF) state.
repair	(Optional)
table *table-id*	(Optional) Displays IPv6 RIB table information for the specified table ID. The table ID must be in hexadecimal format. The range is from 0 to 0-0xFFFFFFFF.
watch	(Optional) Displays information about route watchers.

Command Default

If none of the optional syntax elements is chosen, all IPv6 routing information for all active routing tables is displayed.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	This command was modified. The **isis** keyword was added, and the I1 - ISIS L1, I2 - ISIS L2, and IA - ISIS interarea fields were included in the command output.
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. The timer information was removed, and an indicator was added to display IPv6 Multiprotocol Label Switching (MPLS) interfaces.
12.2(13)T	This command was modified. The timer information was removed, and an indicator was added to display IPv6 MPLS virtual interfaces.
12.2(14)S	This command was modified. The **longer-prefixes** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Release	Modification
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **table**, **nsf**, **watch**, and **updated** keywords and the *day, month, table-id*, and *time* arguments were added.
15.2(2)S	This command was modified. The command output was enhanced to include route tag values in dotted-decimal format.
Cisco IOS XE Release 3.6S	This command was modified. The command output was enhanced to include route tag values in dotted-decimal format.
15.1(1)SY	The **nd** keyword was added.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **show ipv6 route** command provides output similar to the **show ip route** command, except that the information is IPv6-specific.

When the *ipv6-address* or *ipv6-prefix*/*prefix-length* argument is specified, the longest match lookup is performed from the routing table, and only route information for that address or network is displayed. When a routing protocol is specified, only routes for that protocol are displayed. When the **connected**, **local**, **mobile**, or **static** keyword is specified, only the specified type of route is displayed. When the **interface** keyword and *type* and *number* arguments are specified, only the specified interface-specific routes are displayed.

Examples

The following is sample output from the **show ipv6 route** command when no keywords or arguments are specified:

```
Device# show ipv6 route

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - IIS interarea
B   2001:DB8:4::2/48 [20/0]
     via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
L   2001:DB8:4::3/48 [0/0]
     via ::, Ethernet1/0
C   2001:DB8:4::4/48 [0/0]
     via ::, Ethernet1/0
LC  2001:DB8:4::5/48 [0/0]
     via ::, Loopback0
L   2001:DB8:4::6/48 [0/0]
     via ::, Serial6/0
C   2001:DB8:4::7/48 [0/0]
     via ::, Serial6/0
S   2001:DB8:4::8/48 [1/0]
     via 2001:DB8:1::1, Null
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

The table below describes the significant fields shown in the display.

Table 11: show ipv6 route Field Descriptions

Field	Description
Codes:	Indicates the protocol that derived the route. Values are as follows: • B—BGP derived • C—Connected • I1—ISIS L1—Integrated IS-IS Level 1 derived • I2—ISIS L2—Integrated IS-IS Level 2 derived • IA—ISIS interarea—Integrated IS-IS interarea derived • L—Local • R—RIP derived • S—Static
2001:DB8:4::2/48	Indicates the IPv6 prefix of the remote network.
[20/0]	The first number in brackets is the administrative distance of the information source; the second number is the metric for the route.
via FE80::A8BB:CCFF:FE02:8B00	Specifies the address of the next device to the remote network.

When the *ipv6-address* or *ipv6-prefix*/*prefix-length* argument is specified, only route information for that address or network is displayed. The following is sample output from the **show ipv6 route** command when IPv6 prefix 2001:DB8::/35 is specified. The fields in the display are self-explanatory.

```
Device# show ipv6 route 2001:DB8::/35

IPv6 Routing Table - 261 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
B 2001:DB8::/35 [20/3]
  via FE80::60:5C59:9E00:16, Tunnel1
```

When you specify a protocol, only routes for that particular routing protocol are shown. The following is sample output from the **show ipv6 route bgp** command. The fields in the display are self-explanatory.

```
Device# show ipv6 route bgp

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
B   2001:DB8:4::4/64 [20/0]
     via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
```

The following is sample output from the **show ipv6 route local** command. The fields in the display are self-explanatory.

```
Device# show ipv6 route local

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
L   2001:DB8:4::2/128 [0/0]
     via ::, Ethernet1/0
LC  2001:DB8:4::1/128 [0/0]
     via ::, Loopback0
L   2001:DB8:4::3/128 [0/0]
     via ::, Serial6/0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

The following is sample output from the **show ipv6 route** command when the 6PE multipath feature is enabled. The fields in the display are self-explanatory.

```
Device# show ipv6 route

IPv6 Routing Table - default - 19 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
.
.
.
B   2001:DB8::/64 [200/0]
     via ::FFFF:172.11.11.1
     via ::FFFF:172.30.30.1
```

Related Commands

Command	Description
ipv6 route	Establishes a static IPv6 route.
show ipv6 interface	Displays IPv6 interface information.
show ipv6 route summary	Displays the current contents of the IPv6 routing table in summary format.
show ipv6 tunnel	Displays IPv6 tunnel information.

show ipv6 snooping capture-policy

To display message capture policies, use the **show ipv6 snooping capture-policy** command in user EXEC or privileged EXEC mode.

show ipv6 snooping capture-policy [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Displays first-hop message types on the specified interface type and number.

Command Modes

User EXEC (>)

Privileged EXEC (#)

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

Usage Guidelines

The **show ipv6 snooping capture-policy** command displays IPv6 first-hop message capture policies.

Examples

The following example shows **show ipv6 snooping capture-policy** command output on the Ethernet 0/0 interface, on which the IPv6 Neighbor Discovery Protocol (NDP) Inspection and Router Advertisement (RA) Guard features are configured:

```
Router# show ipv6 snooping capture-policy

Hardware policy registered on Et0/0
Protocol  Protocol value  Message  Value  Action  Feature
ICMP      58              RS       85     punt    RA Guard
                                          punt    ND Inspection
ICMP      58              RA       86     drop    RA guard
                                          punt    ND Inspection
ICMP      58              NS       87     punt    ND Inspection
ICMP      58              NA       88     punt    ND Inspection
ICMP      58              REDIR    89     drop    RA Guard
                                          punt    ND Inspection
```

The table below describes the significant fields shown in the display.

Table 12: show ipv6 snooping capture-policy Field Descriptions

Field	Description
Hardware policy registered on Fa4/11	A hardware policy contains a programmatic access list (ACL), with a list of access control entries (ACEs).
Protocol	The protocol whose packets are being inspected.
Message	The type of message being inspected.
Action	Action to be taken on the packet.
Feature	The inspection feature for this information.

show ipv6 snooping counters

To display information about the packets counted by the interface counter, use the **show ipv6 snooping counters**command in user EXEC or privileged EXEC mode.

show ipv6 snooping counters [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Displays first hop packets that match the specified interface type and number.

Command Modes

User EXEC Privileged EXEC (#)

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

Usage Guidelines

The **show ipv6 snooping counters** command shows packets handled by the switcher that are being counted in interface counters. The switcher counts packets captured per interface and records whether the packet was received, sent, or dropped. If a packet is dropped, the reason for the drop and the feature that caused the drop are both also provided.

Examples

The following examples shows information about packets counted on interface FastEthernet4/12:

```
Router# show ipv6 snooping counters interface Fa4/12
Received messages on Fa4/12:
Protocol        Protocol message
ICMPv6          RS      RA      NS      NA      REDIR   CPS     CPA
                0       4256    0       0       0       0       0
Bridged messages from Fa4/12:
Protocol        Protocol message
ICMPv6          RS      RA      NS      NA      REDIR   CPS     CPA
                0       4240    0       0       0       0       0
Dropped messages on Fa4/12:
Feature/Message RS      RA      NS      NA      REDIR   CPS     CPA
RA guard        0       16      0       0       0       0       0
Dropped reasons on Fa4/12:
RA guard         16   RA drop - reason:RA/REDIR received on un-authorized port
```

The table below describes the significant fields shown in the display.

Table 13: show ipv6 snooping counters Field Descriptions

Field	Description
Received messages on Fa4/12:	The messages received on an interface.
Protocol	The protocol for which messages are being counted.
Protocol message	The type of protocol messages being counted.
Bridged messages from Fa4/12:	Bridged messages from the interface.
Dropped messages an Fa4/12:	The messages dropped on the interface.
Feature/message	The feature that caused the drop, and the type and number of messages dropped.
RA drop - reason:RA/REDIR received on un-authorized port	The reason these messages were dropped.

show ipv6 snooping features

To display information about about snooping features configured on the router, use the **show ipv6 snooping features** command in user EXEC or privileged EXEC mode.

show ipv6 snooping features

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

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 **show ipv6 snooping features** command shows the first hop features that are configured on the router.

Examples

The following example shows that both IPv6 ND inspection and IPv6 RA Guard are configured on the router:

```
Router# show ipv6 snooping features

Feature name   priority state
RA guard          100   READY
NDP inspection     20   READY
```

The table below describes the significant fields shown in the display.

Table 14: show ipv6 snooping features Field Descriptions

Field	Description
Feature name	The names of the IPv6 global policy features configured on the router.
Priority	The priority of the specified feature.
State	The state of the specified feature.

show ipv6 snooping policies

To display information about the configured policies and the interfaces to which they are attached, use the **show ipv6 snooping policies** command in user EXEC or privileged EXEC mode.

show ipv6 snooping policies [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Displays policies that match the specified interface type and number.

Command Modes

User EXEC (>)

Privileged EXEC (#)

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.

Usage Guidelines

The **show ipv6 snooping policies** command displaying all policies that are configured and lists the interfaces to which they are attached.

Examples

The following examples shows information about all policies configured:

```
Device# show ipv6 snooping policies

NDP inspection policies configured:
Policy      Interface    Vlan
------      ---------    ----
trusted      Et0/0        all
             Et1/0        all
untrusted    Et2/0        all
RA guard policies configured:
Policy      Interface    Vlan
------      ---------    ----
host         Et0/0        all
             Et1/0        all
router       Et2/0        all
```

The table below describes the significant fields shown in the display.

Table 15: show ipv6 first-hop policies Field Descriptions

Field	Description
NDP inspection policies configured:	Description of the policies configured for a specific feature.
Policy	Whether the policy is trusted or untrusted.
Interface	The interface to which a policy is attached.

show ipv6 traffic

To display statistics about IPv6 traffic, use the **show ipv6 traffic**command in user EXEC or privileged EXEC mode.

show ipv6 traffic [**interface** [*interface type number*]]

Syntax Description

interface	(Optional) All interfaces. IPv6 forwarding statistics for all interfaces on which IPv6 forwarding statistics are being kept will be displayed.
interface type number	(Optional) Specified interface. Interface statistics that have occurred since the statistics were last cleared on the specific interface are displayed.

Command Modes

User EXEC Privileged EXEC

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 output fields were added.
12.2(13)T	The modification to add output fields was integrated into this release.
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.
12.2(33)SRC	The *interface* argument and **interface** keyword were added.
12.2(33)SB	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 devices.

Release	Modification
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **show ipv6 traffic**command provides output similar to the **show ip traffic**command, except that it is IPv6-specific.

Examples

The following is sample output from the **show ipv6 traffic**command:

```
Device# show ipv6 traffic
IPv6 statistics:
  Rcvd:  0 total, 0 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a device
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
         0 unicast RPF drop, 0 suppressed RPF drop
  Sent:  0 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 0 received, 0 sent
ICMP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 device solicit, 0 device advert, 0 redirects
```

The following is sample output for the show ipv6 interface command without IPv6 CEF running:

```
Device# show ipv6 interface ethernet 0/1/1
Ethernet0/1/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::203:FDFF:FE49:9
  Description: sat-2900a f0/12
  Global unicast address(es):
    7::7, subnet is 7::/32
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:7
    FF02::1:FF49:9
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  Input features: RPF
  Unicast RPF access-list MINI
    Process Switching:
      0 verification drops
      0 suppressed verification drops
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
```

The following is sample output for the show ipv6 interface command with IPv6 CEF running:

```
Device# show ipv6 interface ethernet 0/1/1
Ethernet0/1/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::203:FDFF:FE49:9
  Description: sat-2900a f0/12
  Global unicast address(es):
    7::7, subnet is 7::/32
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:7
    FF02::1:FF49:9
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  Input features: RPF
  Unicast RPF access-list MINI
    Process Switching:
      0 verification drops
      0 suppressed verification drops
    CEF Switching:
      0 verification drops
      0 suppressed verification drops
  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.
```

The table below describes the significant fields shown in the display.

Table 16: show ipv6 traffic Field Descriptions

Field	Description
source-routed	Number of source-routed packets.
truncated	Number of truncated packets.
format errors	Errors that can result from checks performed on header fields, the version number, and packet length.
not a device	Message sent when IPv6 unicast routing is not enabled.
0 unicast RPF drop, 0 suppressed RPF drop	Number of unicast and suppressed reverse path forwarding (RPF) drops.
failed	Number of failed fragment transmissions.
encapsulation failed	Failure that can result from an unresolved address or try-and-queue packet.
no route	Counted when the software discards a datagram it did not know how to route.

Field	Description
unreach	Unreachable messages received are as follows: • routing--Indicates no route to the destination. • admin--Indicates that communication with the destination is administratively prohibited. • neighbor--Indicates that the destination is beyond the scope of the source address. For example, the source may be a local site or the destination may not have a route back to the source. • address--Indicates that the address is unreachable. • port--Indicates that the port is unreachable.
Unicast RPF access-list MINI	Unicast RPF access-list in use.
Process Switching	Displays process RPF counts, such as verification and suppressed verification drops.
CEF Switching	Displays CEF switching counts, such as verification drops and suppressed verification drops.

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.

throttle-period

To configure the throttle period in an IPv6 router advertisement (RA) throttler policy, use the **throttle-period** command in IPv6 RA throttle policy configuration mode. To reset this command to its default, use the **no** form of the command.

throttle-period { **inherit**| *seconds*}

Syntax Description

inherit	The throttle period setting is inherited from target policies.
seconds	Duration of the throttle period, in seconds. The range is from 10 through 86,400 seconds.

Command Default

600 seconds (10 minutes)

Command Modes

IPv6 RA throttle policy configuration

Command History

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

Usage Guidelines

The **throttle-period** command is only valid for policies attached to a VLAN or VLANs. If you try to configure this command on a port, the port ignores it.

Examples

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# throttle-period 300
```

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.

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

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.

vlan configuration

To configure a VLAN or a collection of VLANs and enter VLAN configuration mode, use the **vlan configuration** command in global configuration mode. To return to the command defaults, use the **no** version of this command.

vlan configuration *vlan-id*

Syntax Description

vlan-id	A VLAN or a collection of VLANs.

Command Default

A VLAN or a collection of VLANs is not configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use the **vlan configuration** command to configure a VLAN or a collection of VLANs. The IPv6 RA throttler, which functions at the VLAN level, counts all RAs from multiple devices over a VLAN during a specified period of time.

Once an IPv6 RA throttler policy has been configured using the **ipv6 nd ra-throttle policy** command, you can attach it to a VLAN or a collection of VLANs using the **ipv6 nd ra-throttle attach-policy** command.

Examples

```
Device(config)# vlan configuration vlan1
Device(config-vlan-config)#
```