ipv6-i1

ipv6 dhcp guard attach-policy

To attach a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) guard policy, use the **ipv6 dhcp guard attach-policy** command in interface configuration or VLAN configuration mode. To unattach the DHCPv6 guard policy, use the **no** form of this command.

Syntax Available In Interface Configuration Mode

ipv6 dhcp guard [**attach-policy** [*policy-name*]] [**vlan** {**add**| **all**| **except**| **none**| **remove**} *vlan-id* [*... vlan-id*]]

no ipv6 dhcp guard [**attach-policy** [*policy-name*]] [**vlan** {**add**| **all**| **except**| **none**| **remove**} *vlan-id* [*... vlan-id*]]

Syntax Available In VLAN Configuration Mode

ipv6 dhcp guard attach-policy [*policy-name*]

no ipv6 dhcp guard attach-policy [*policy-name*]

Syntax Description

policy-name	(Optional) DHCPv6 guard policy name.
vlan	(Optional) Specifies that the DHCPv6 policy is to be attached to a VLAN.
add	(Optional) Attaches a DHCPv6 guard policy to the specified VLAN(s).
all	(Optional) Attaches a DHCPv6 guard policy to all VLANs.
except	(Optional) Attaches a DHCPv6 guard policy to all VLANs except the specified VLAN(s).
none	(Optional) Attaches a DHCPv6 guard policy to none of the specified VLAN(s).
remove	(Optional) Removes a DHCPv6 guard policy from the specified VLAN(s).
vlan-id	(Optional) Identity of the VLAN(s) to which the DHCP guard policy applies.

Command Default

No DHCPv6 guard policy is attached.

Command Modes

Interface configuration (config-if)

VLAN configuration (config-vlan)

Command History

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

Usage Guidelines

This command allows you to attach a DHCPv6 policy to an interface or to one or more VLANs. DHCPv6 guard policies can be used to block reply and advertisement messages that come from unauthorized DHCP servers and relay agents that forward DHCP packets from servers to clients. Client messages or messages sent by relay agents from clients to servers are not blocked.

Examples

The following example shows how to attach a DHCPv6 guard policy to an interface:

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet 0/2/0
Router# switchport
Router(config-if)# ipv6 dhcp guard attach-policy pol1 vlan add 1
```

Related Commands

Command	Description
ipv6 dhcp guard policy	Defines the DHCPv6 guard policy name.
show ipv6 dhcp guard policy	Displays DHCPv6 guard policy information.

ipv6 dhcp guard policy

To define a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) guard policy name, use the **ipv6 dhcp guard policy** command in global configuration mode. To remove the DHCPv6 guard policy name, use the **no** form of this command.

ipv6 dhcp guard policy [*policy-name*]

no ipv6 dhcp guard policy [*policy-name*]

Syntax Description

policy-name	(Optional) DHCPv6 guard policy name.

Command Default

No DHCPv6 guard policy name is defined.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

This command allows you to enter DHCPv6 guard configuration mode. DHCPv6 guard policies can be used to block reply and advertisement messages that come from unauthorized DHCP servers and relay agents that forward DHCP packets from servers to clients. Client messages or messages sent by relay agents from clients to servers are not blocked.

Examples

The following example shows how to define a DHCPv6 guard policy name:

```
Router> enable
Router# configure terminal
Router(config)# ipv6 dhcp guard policy policy1
```

Related Commands

Command	Description
show ipv6 dhcp guard policy	Displays DHCPv6 guard policy information.

ipv6 dhcp ping packets

To specify the number of packets a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server sends to a pool address as part of a ping operation, use the **ipv6 dhcp ping packets** command in global configuration mode. To prevent the server from pinging pool addresses, use the **no** form of this command.

ipv6 dhcp ping packets *number*

ipv6 dhcp ping packets

Syntax Description

number	The number of ping packets sent before the address is assigned to a requesting client. The valid range is from 0 to 10.

Command Default

No ping packets are sent before the address is assigned to a requesting client.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The DHCPv6 server pings a pool address before assigning the address to a requesting client. If the ping is unanswered, the server assumes, with a high probability, that the address is not in use and assigns the address to the requesting client.

Setting the *number* argument to 0 turns off the DHCPv6 server ping operation

Examples

The following example specifies four ping attempts by the DHCPv6 server before further ping attempts stop:

```
Router(config)# ipv6 dhcp ping packets 4
```

Related Commands

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

Command	Description
show ipv6 dhcp conflict	Displays address conflicts found by a DHCPv6 server, or reported through a DECLINE message from a client.

ipv6 dhcp server

To enable Dynamic Host Configuration Protocol (DHCP) for IPv6 service on an interface, use the **ipv6 dhcp server** in interface configuration mode. To disable DHCP for IPv6 service on an interface, use the **no** form of this command.

ipv6 dhcp server [*poolname*| **automatic**] **[rapid-commit]** [**preference** *value*] **[allow-hint]**

no ipv6 dhcp server

Syntax Description

poolname	(Optional) User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).
automatic	(Optional) Enables the server to automatically determine which pool to use when allocating addresses for a client.
rapid-commit	(Optional) Allows the two-message exchange method for prefix delegation.
preference *value*	(Optional) Specifies the preference value carried in the preference option in the advertise message sent by the server. The range is from 0 to 255. The preference value defaults to 0.
allow-hint	(Optional) Specifies whether the server should consider delegating client suggested prefixes. By default, the server ignores client-hinted prefixes.

Command Default

DHCP for IPv6 service on an interface is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(24)T	The **automatic** keyword was added.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Release	Modification
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 dhcp server** command enables DHCP for IPv6 service on a specified interface using the pool for prefix delegation and other configuration through that interface.

The **automatic** keyword enables the system to automatically determine which pool to use when allocating addresses for a client. When an IPv6 DHCP packet is received by the server, the server determines if it was received from a DHCP relay or if it was directly received from the client. If the packet was received from a relay, the server verifies the link-address field inside the packet associated with the first relay that is closest to the client. The server matches this link address against all address prefix and link-address configurations in IPv6 DHCP pools to find the longest prefix match. The server selects the pool associated with the longest match.

If the packet was directly received from the client, the server performs this same matching, but it uses all the IPv6 addresses configured on the incoming interface when performing the match. Once again, the server selects the longest prefix match.

The **rapid-commit** keyword enables the use of the two-message exchange for prefix delegation and other configuration. If a client has included a rapid commit option in the solicit message and the **rapid-commit** keyword is enabled for the server, the server responds to the solicit message with a reply message.

If the **preference** keyword is configured with a value other than 0, the server adds a preference option to carry the preference value for the advertise messages. This action affects the selection of a server by the client. Any advertise message that does not include a preference option is considered to have a preference value of 0. If the client receives an advertise message that includes a preference option with a preference value of 255, the client immediately sends a request message to the server from which the advertise message was received.

If the **allow-hint** keyword is specified, the server will delegate a valid client-suggested prefix in the solicit and request messages. The prefix is valid if it is in the associated local prefix pool and it is not assigned to a device. If the **allow-hint** keyword is not specified, a hint is ignored and a prefix is delegated from the free list in the pool.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. When one of these functions is already enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed:

```
Interface is in DHCP client mode
Interface is in DHCP server mode
Interface is in DHCP relay mode
```

Examples

The following example enables DHCP for IPv6 for the local prefix pool named server1:

```
Router(config-if)# ipv6 dhcp server server1
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 pool and enters DHCP for IPv6 pool configuration mode.
show ipv6 dhcp interface	Displays DHCP for IPv6 interface information.

ipv6 enable

To enable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **ipv6 enable**command in interface configuration mode. To disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **no** form of this command.

ipv6 enable

no ipv6 enable

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 is disabled.

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 integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 enable**command automatically configures an IPv6 link-local unicast address on the interface while also enabling the interface for IPv6 processing. The no **ipv6 enable**command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

Examples

The following example enables IPv6 processing on Ethernet interface 0/0:

```
Device(config)# interface ethernet 0/0
Device(config-if)# ipv6 enable
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 host

To define a static host name-to-address mapping in the host name cache, use the **ipv6 host**command in global configuration mode. To remove the host name-to-address mapping, use the no form of this command.

ipv6 host *name* [*port*] *ipv6-address*

no ipv6 host *name*

Syntax Description

name	Name of the IPv6 host. The first character can be either a letter or a number. If you use a number, the operations you can perform are limited.
port	(Optional) The default Telnet port number for the associated IPv6 addresses.
ipv6-address	Associated IPv6 address. You can bind up to four addresses to a host name.

Command Default

Static host name-to-address mapping in the host name cache is not defined. The default Telnet port is 23.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The first character of the *name* variable can be either a letter or a number. If you use a number, the operations you can perform (such as **ping**) are limited.

Examples

The following example defines two static mappings:

```
Device(config)# ipv6 host cisco-sj 2001:0DB8:1::12
Device(config)# ipv6 host cisco-hq 2002:C01F:768::1 2001:0DB8:1::12
```

Related Commands

Command	Description
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses.

ipv6 icmp error-interval

To configure the interval and bucket size for IPv6 Internet Control Message Protocol (ICMP) error messages, use the **ipv6 icmp error-interval** command in global configuration mode. To return the interval to its default setting, use the **no** form of this command.

ipv6 icmp error-interval *milliseconds* [*bucketsize*]

no ipv6 icmp error-interval

Syntax Description

milliseconds	The time interval between tokens being placed in the bucket. The acceptable range is from 0 to 2147483647 with a default of 100 milliseconds.
bucketsize	(Optional) The maximum number of tokens stored in the bucket. The acceptable range is from 1 to 200 with a default of 10 tokens.

Command Default

ICMP rate limiting is enabled by default. To disable ICMP rate limiting, set the interval to zero. The time interval between tokens placed in the bucket is 100 milliseconds. The maximum number of tokens stored in the bucket is 10.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	Support for IPv6 ICMP rate limiting was extended to use token buckets.
12.0(21)ST	This command, without the extension to use token buckets, was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command, without the extension to use token buckets, was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command, with the support for IPv6 ICMP rate limiting extended to use token buckets, was integrated into Cisco IOS Release 12.0(23)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.
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 2.1	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

Use the **ipv6 icmp error-interval** command to limit the rate at which IPv6 ICMP error messages are sent. A token bucket algorithm is used with one token representing one IPv6 ICMP error message. Tokens are placed in the virtual bucket at a specified interval until the maximum number of tokens allowed in the bucket is reached.

The *milliseconds* argument specifies the time interval between tokens arriving in the bucket. The optional *bucketsize* argument is used to define the maximum number of tokens allowed in the bucket. Tokens are removed from the bucket when IPv6 ICMP error messages are sent, which means that if the *bucketsize* is set to 20, a rapid succession of 20 IPv6 ICMP error messages can be sent. When the bucket is empty of tokens, IPv6 ICMP error messages are not sent until a new token is placed in the bucket.

Use the **show ipv6 traffic** command to display IPv6 ICMP rate-limited counters.

Examples

The following example shows an interval of 50 milliseconds and a bucket size of 20 tokens being configured for IPv6 ICMP error messages:

```
ipv6 icmp error-interval 50 20
```

Related Commands

Command	Description
show ipv6 traffic	Displays statistics about IPv6 traffic.

ipv6 nd cache expire

To configure the length of time before an IPv6 neighbor discovery (ND) cache entry expires, use the **ipv6 nd cache expire** command in interface configuration mode. To remove this configuration, use the **no** form of this command.

ipv6 nd cache expire *expire-time-in-seconds* **[refresh]**

no ipv6 nd cache expire *expire-time-in-seconds* **[refresh]**

Syntax Description

expire-time-in-seconds	The time range is from 1 through 65536 seconds. The default is 14400 seconds, or 4 hours.
refresh	(Optional) Automatically refreshes the ND cache entry.

Command Default

This expiration time is 14400 seconds (4 hours)

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI7	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

By default, an ND cache entry is expired and deleted if it remains in the STALE state for 14,400 seconds, or 4 hours. The **ipv6 nd cache expire** command allows the user to vary the expiry time and to trigger autorefresh of an expired entry before the entry is deleted.

When the **refresh** keyword is used, an ND cache entry is autorefreshed. The entry moves into the DELAY state and the neighbor unreachability detection (NUD) process occurs, in which the entry transitions from the DELAY state to the PROBE state after 5 seconds. When the entry reaches the PROBE state, a neighbor solicitation (NS) is sent and then retransmitted as per the configuration.

Examples

The following example shows that the ND cache entry is configured to expire in 7200 seconds, or 2 hours:

```
Router(config-if)# ipv6 nd cache expire 7200
```

ipv6 nd inspection

To apply the Neighbor Discovery Protocol (NDP) Inspection feature, use the **ipv6 nd inspection** command in interface configuration mode. To remove the NDP Inspection feature, use the **no** form of this command.

ipv6 nd inspection [**attach-policy** [*policy-name*] | **vlan** {**add** | **except** | **none** | **remove** | **all**} **vlan** *vlan-id*]]

no ipv6 nd inspection

Syntax Description

attach-policy	(Optional) Attaches an NDP Inspection policy.
policy-name	(Optional) The NDP Inspection policy name.
vlan	(Optional) Applies the ND Inspection feature to a VLAN on the interface.
add	(Optional) Adds a VLAN to be inspected.
except	(Optional) Inspects all VLANs except the one specified.
none	(Optional) Specifies that no VLANs are inspected.
remove	(Optional) Removes the specified VLAN from NDP inspection.
all	(Optional) Inspects NDP traffic from all VLANs on the port.
vlan-id	(Optional) A specific VLAN on the interface. More than one VLAN can be specified. The VLAN number that can be used is from 1 to 4094.

Command Default

All NDP messages are inspected. Secure Neighbor Discovery (SeND) options are ignored. Neighbors are probed based on the criteria defined in the Neighbor Tracking feature. Per-port IPv6 address limit enforcement is disabled. Layer 2 header source MAC address validations are disabled. Per-port rate limiting of the NDP messages in software is disabled.

Command Modes

Interface configuration (config-if)

Command History

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

Release	Modification
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SY.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 nd inspection** command applies the NDP Inspection feature on a specified interface. If you enable the optional **attach-policy** or **vlan** keywords, NDP traffic is inspected by policy or by VLAN. If no VLANs are specified, NDP traffic from all VLANs on the port is inspected (which is equivalent to using the **vlan all** keywords).

If no policy is specified in this command, the default criteria are as follows:

- All NDP messages are inspected.
- SeND options are ignored.
- Neighbors are probed based on the criteria defined in neighbor tracking feature.
- Per-port IPv6 address limit enforcement is disabled.
- Layer 2 header source MAC address validations are disabled.
- Per-port rate limiting of the NDP messages in software is disabled.

If a VLAN is specified, its parameter is either a single VLAN number from 1 to 4094 or a range of VLANs described by two VLAN numbers, the lesser one first, separated by a dash (for example, **vlan 1-100,200,300-400**). Do not enter any spaces between comma-separated VLAN parameters or in dash-specified ranges.

Examples

The following example enables NDP inspection on a specified interface:

```
Router(config-if)# ipv6 nd inspection
```

ipv6 nd inspection policy

To define the neighbor discovery (ND) inspection policy name and enter ND inspection policy configuration mode, use the **ipv6 nd inspection** command in ND inspection configuration mode. To remove the ND inspection policy, use the **no** form of this command.

ipv6 nd inspection policy *policy-name*

no ipv6 nd inspection policy *policy-name*

Syntax Description

policy-name	The ND inspection policy name.

Command Default

No ND inspection policies are configured.

Command Modes

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

Usage Guidelines

The **ipv6 nd inspection policy** command defines the ND inspection policy name and enters ND inspection policy configuration mode. Once you are in ND inspection policy configuration mode, you can use any of the following commands:

- **device-role**
- **drop-unsecure**
- **limit address-count**
- **sec-level minimum**
- **tracking**
- **trusted-port**
- **validate source-mac**

Examples

The following example defines an ND policy name as policy1:

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

Related Commands

Command	Description
device-role	Specifies the role of the device attached to the port.
drop-unsecure	Drops messages with no or invalid options or an invalid signature.
limit address-count	Limits the number of IPv6 addresses allowed to be used on the port.
sec-level minimum	Specifies the minimum security level parameter value when CGA options are used.
tracking	Overrides the default tracking policy on a port.
trusted-port	Configures a port to become a trusted port.
validate source-mac	Checks the source MAC address against the link-layer address.

ipv6 nd na glean

To configure neighbor discovery (ND) to glean an entry from an unsolicited neighbor advertisement (NA), use the **ipv6 nd na glean** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nd na glean

no ipv6 nd na glean

Syntax Description

This command has no arguments or keywords.

Command Default

The router ignores an unsolicited NA.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI7	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

IPv6 nodes may choose to emit a multicast unsolicited NA packet following the successful completion of duplicate address detection (DAD). By default, these unsolicited NA packets are ignored by other IPv6 nodes. The **ipv6 nd na glean** command configures the router to create an ND entry on receipt of an unsolicited NA packet (assuming no such entry already exists and the NA has the link-layer address option). Use of this command allows a router to populate its ND cache with an entry for a neighbor in advance of any data traffic exchange with the neighbor.

Examples

The following example configures ND to glean an entry from an unsolicited neighbor advertisement:

```
Router(config-if)# ipv6 nd na glean
```

ipv6 nd nud retry

To configure the number of times neighbor unreachability detection (NUD) resends neighbor solicitations (NSs), use the **ipv6 nd nud retry** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nd nud retry *base interval max-attempts*

no ipv6 nd nud retry *base interval max-attempts*

Syntax Description

base	The base NUD value.
interval	The time interval, in milliseconds, between retries.
max-attempts	The maximum number of retry attempts, depending on the base value.

Command Default

Three NS packets are sent 1 second apart.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI7	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

When a router runs NUD to re-resolve the ND entry for a neighbor, it sends three NS packets 1 second apart. In certain situations (for example, spanning-tree events, high traffic, the end host being reloaded), three NS packets sent at an interval of 1 second may not be sufficient. To help maintain the neighbor cache in such situations, use the **ipv6 nd nud retry** command to configure exponential timers for NS retransmits.

The maximum number of retry attempts is configured using the *max-attempts* argument. The retransmit interval is calculated with the following formula:

tm

- *t* = Time interval
- *m* = Base (1, 2, or 3)
- *n* = Current NS number (where the first NS is 0)

The **ipv6 nd nud retry** command affects only the retransmit rate for NUD, not for initial resolution, which uses the default of three NS packets sent 1 second apart.

Examples

The following example provides a fixed interval of 1 second and three retransmits:

```
Router(config-if)# ipv6 nd nud retry 1 1000 3
```

The following example provides a retransmit interval of 1, 2, 4, and 8:

```
Router(config-if)# ipv6 nd nud retry 2 1000 4
```

The following example provides the retransmit intervals of 1, 3, 9, 27, 81:

```
Router(config-if)# ipv6 nd nud retry 3 1000 5
```

ipv6 nd ra-throttle attach-policy

To attach an IPv6 router advertisement (RA) throttler policy to a Layer 2 interface or to a collection of VLANs, use the **ipv6 nd ra-throttle attach-policy** command in interface configuration mode or VLAN configuration mode. To remove the policy, use the **no** form of this command.

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

Syntax Description

policy-name	RA throttler policy name.

Command Default

No policy is attached to an interface.

No policy is attached to a VLAN.

Command Modes

Interface configuration (config-if)

VLAN configuration (config-VLAN-config)

Command History

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

Usage Guidelines

Use the **ipv6 nd ra-throttle attach-policy** command in interface configuration mode to attach the IPv6 RA throttler policy to a Layer 2 interface on the device port. Use the **ipv6 nd ra-throttle attach-policy** command in VLAN configuration mode to attach the IPv6 RA throttler policy to a VLAN or a collection of VLANs. To create the RA throttler policy, use the **ipv6 nd ra-throttle policy** command in global configuration mode.

IPv6 RA throttle policies must be attached at either the VLAN or BOX level in order to operate at the PORT level. If a policy or policies are attached at the PORT level only, IPv6 RA throttler will not function.

When a policy is applied on a port, any value that is not configured in the policy will be inherited from the VLAN configuration. If the value is not set in the VLAN configuration, then the default value is used.

Examples

The following example shows how to create an IPv6 RA throttler policy named policy1 and attach it to the Ethernet0/0 interface:

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# exit
.
.
Device(config)# interface ethernet0/0
Device(config-if)# ipv6 nd ra-throttle attach-policy policy1
```

The following example shows how to create an IPv6 RA throttler policy named policy1 and attach it to a collection of VLANs named vlan1:

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# exit
.
.
Device(config)# vlan configuration vlan1
Device(config-vlan-config)# ipv6 nd ra-throttle attach-policy policy1
```

ipv6 nd ra-throttle policy

To define the router advertisement (RA) throttler policy name and enter IPv6 RA throttle policy configuration mode, use the **ipv6 nd ra-throttle policy** command in global configuration mode. To reset the command to its defaults, use the **no** form of this command.

ipv6 nd ra-throttle policy *policy-name* **no ipv6 nd ra-throttle policy** *policy-name*

Syntax Description

policy-name	RA throttler policy name.

Command Default

- throttle-period: 600 seconds (10 minutes)
- max-through: 10 RAs per VLAN per 10 minutes.
- allow: at-least 1 at-most 1
- interval-option: passthrough
- medium-type: wired (port only)

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use the **ipv6 nd ra-throttle policy** command to define an IPv6 RA throttle policy and enter Pv6 RA throttle policy configuration mode.

The **allow at-least** and **allow at-most** command settings applied at the VLAN level provide the default for all devices in the VLAN. The values can be overwritten on a per-port basis by applying another policy on the specified port.

IPv6 RA throttle policies must be attached at either the VLAN or BOX level in order to operate at the PORT level. If a policy or policies are attached at the PORT level only, IPv6 RA throttler will not function.

When a policy is applied on a port, any value that is not configured in the policy will be inherited from the VLAN configuration. If the value is not set in the VLAN configuration, then the default value is used.

Examples

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

ipv6 nd raguard attach-policy

To apply the IPv6 router advertisement (RA) guard feature on a specified interface, use the **ipv6 nd raguard attach-policy** command in interface configuration mode.

ipv6 nd raguard attach-policy [*policy-name* [**vlan** {**add**| **except**| **none**| **remove**| **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]

Syntax Description

policy-name	(Optional) IPv6 RA guard policy name.
vlan	(Optional) Applies the IPv6 RA guard feature to a VLAN on the interface.
add	Adds a VLAN to be inspected.
except	All VLANs are inspected except the one specified.
none	No VLANs are inspected.
remove	Removes the specified VLAN from RA guard inspection.
all	ND traffic from all VLANs on the port is inspected.
vlan	(Optional) A specific VLAN on the interface. More than one VLAN can be specified (*vlan1*, *vlan2*, *vlan3*...). The range of available VLAN numbers is from 1 through 4094.

Command Default

An IPv6 RA guard policy is not configured.

Command Modes

Interface configuration (config-if)

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

If no policy is specified using the *policy-name* argument, the port device role is set to host and all inbound router traffic (for example, RA and redirect messages) is blocked.

If no VLAN is specified (which is equal to entering the **vlan all** keywords after the *policy-name* argument), RA guard traffic from all VLANs on the port is analyzed.

If specified, the VLAN parameter is either a single VLAN number from 1 through 4094 or a range of VLANs described by two VLAN numbers, the lesser one first, separated by a dash. Do not enter any spaces between comma-separated vlan parameters or in dash-specified ranges; for example, vlan 1-100,200,300-400.

Examples

In the following example, the IPv6 RA guard feature is applied on GigabitEthernet interface 0/0:

```
Device(config)# interface GigabitEthernet 0/0
Device(config-if)# ipv6 nd raguard attach-policy
```

ipv6 nd raguard policy

To define the router advertisement (RA) guard policy name and enter RA guard policy configuration mode, use the **ipv6 nd raguard policy** command in global configuration mode.

ipv6 nd raguardpolicy *policy-name*

Syntax Description

policy-name	IPv6 RA guard policy name.

Command Default

An RA guard policy is not configured.

Command Modes

Global configuration (config)#

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

Use the **ipv6 nd raguard policy** command to configure RA guard globally on a router. Once the device is in ND inspection policy configuration mode, you can use any of the following commands:

- **device-role**
- **drop-unsecure**
- **limit address-count**
- **sec-level minimum**
- **trusted-port**
- **validate source-mac**

After IPv6 RA guard is configured globally, you can use the **ipv6 nd raguard attach-policy** command to enable IPv6 RA guard on a specific interface.

Examples

The following example shows how to define the RA guard policy name as policy1 and place the device in policy configuration mode:

```
Device(config)# ipv6 nd raguard policy policy1
Device(config-ra-guard)#
```

Related Commands

Command	Description
device-role	Specifies the role of the device attached to the port.
drop-unsecure	Drops messages with no or invalid options or an invalid signature.
ipv6 nd raguard attach-policy	Applies the IPv6 RA guard feature on a specified interface.
limit address-count	Limits the number of IPv6 addresses allowed to be used on the port.
sec-level minimum	Specifies the minimum security level parameter value when CGA options are used.
trusted-port	Configures a port to become a trusted port.
validate source-mac	Checks the source MAC address against the link layer address.

ipv6 nd router-preference

To configure a default router preference (DRP) for the router on a specific interface, use the **ipv6 nd router-preference**command in interface configuration mode. To return to the default DRP, use the **no** form of this command.

ipv6 nd router-preference {**high**| **medium**| **low**}

no ipv6 nd router-preference

Syntax Description

high	Preference for the router specified on an interface is high.
medium	Preference for the router specified on an interface is medium.
low	Preference for the router specified on an interface is low.

Command Default

Router advertisements (RAs) are sent with the **medium** preference.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
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 integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

RA messages are sent with the DRP configured by the **ipv6 nd router-preference** command. If no DRP is configured, RAs are sent with a medium preference.

A DRP is useful when, for example, two routers on a link may provide equivalent, but not equal-cost, routing, and policy may dictate that hosts should prefer one of the routers.

Examples

The following example configures a DRP of high for the router on gigabit Ethernet interface 0/1:

```
Router(config)# interface Gigabit ethernet 0/1
Router(config-if)# ipv6 nd router-preference high
```

Related Commands

Command	Description
ipv6 nd ra interval	Configures the interval between IPv6 router advertisement transmissions on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd suppress attach-policy

To apply the IPv6 neighbor discovery (ND) suppress feature on a specified interface, use the **ipv6 nd suppress attach-policy** command in interface configuration mode.

ipv6 nd suppress attach-policy [*policy-name* [**vlan** {**add**| **except**| **none**| **remove**| **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]

Syntax Description

policy-name	(Optional) IPv6 ND suppress policy name.
vlan	(Optional) Applies the IPv6 ND suppress feature to a VLAN on the interface.
add	Adds a VLAN to be inspected.
except	All VLANs are inspected except the one specified.
none	No VLANs are inspected.
remove	Removes the specified VLAN from IPv6 ND suppression.
all	ND traffic from all VLANs on the port is inspected.
vlan	(Optional) A specific VLAN on the interface. More than one VLAN can be specified (*vlan1*, *vlan2*, *vlan3*...). The range of available VLAN numbers is from 1 through 4094.

Command Default

An IPv6 ND suppress policy is not configured.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

If no VLAN is specified (which is equal to entering the **vlan all** keywords after the *policy-name* argument), RA guard traffic from all VLANs on the port is analyzed.

If specified, the VLAN parameter is either a single VLAN number from 1 through 4094 or a range of VLANs described by two VLAN numbers, the lesser one first, separated by a dash. Do not enter any spaces between comma-separated vlan parameters or in dash-specified ranges; for example, vlan 1-100,200,300-400.

Examples

In the following example, the IPv6 ND suppress feature is applied on Ethernet interface 0/0:

```
Device(config)# interface Ethernet 0/0
Device(config-if)# ipv6 nd suppress attach-policy
```

Related Commands

Command	Description
ipv6 nd suppress policy	Enables IPv6 ND multicast suppress and enter ND suppress policy configuration mode

ipv6 nd suppress policy

To enable IPv6 Neighbor Discovery (ND) multicast suppress and enter ND suppress policy configuration mode, use the **ipv6 nd suppress policy** command in global configuration mode.

ipv6 nd suppress policy *policy-name*

Syntax Description

policy-name	IPv6 ND suppress policy name.

Command Default

An ND suppress policy is not configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use the **ipv6 nd suppress policy** command to configure NA suppress globally on a device. After IPv6 ND suppress is configured globally, you can use the **ipv6 nd suppress attach-policy** command to enable IPv6 ND suppress on a specific interface.

Examples

The following example shows how to define the ND suppress policy name as policy1 and place the device in policy configuration mode:

```
Device(config)# ipv6 nd suppress policy policy1
Device(config-nd-suppress)#
```

Related Commands

Command	Description
ipv6 nd suppress attach-policy	Applies the IPv6 ND suppress feature on a specified interface.

ipv6 neighbor binding logging

To enable the logging of binding table main events, use the **ipv6 neighbor binding logging** command in global configuration mode. To disable this function, use the **no** form of this command.

ipv6 neighbor binding logging

no ipv6 neighbor binding logging

Syntax Description

This command has no arguments or keywords.

Command Default

Binding table events are not logged.

Command Modes

Global configuration (config)

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 **ipv6 neighbor binding logging** command enables the logging of the following binding table events:

- An entry is inserted into the binding table.
- A binding table entry was updated.
- A binding table entry was deleted from the binding table.
- A binding table entry was not inserted into the binding table, possibly because of a collision with an existing entry, or because the maximum number of entries has been reached.

Examples

The following example shows how to enable binding table event logging:

```
Router(config)# ipv6 neighbor binding logging
```

Related Commands

Command	Description
ipv6 neighbor binding vlan	Adds a static entry to the binding table database.

Command	Description
ipv6 neighbor tracking	Tracks entries in the binding table.
ipv6 snooping logging packet drop	Configures IPv6 snooping security logging.

ipv6 neighbor binding max-entries

To specify the maximum number of entries that are allowed to be inserted in the binding table cache, use the **ipv6 neighbor binding max-entries** command in global configuration mode. To return to the default, use the **no** form of this command.

ipv6 neighbor binding max-entries *entries* [**vlan-limit** *number*| **interface-limit** *number*| **mac-limit** *number*]

no ipv6 neighbor binding max-entries *entries* [**vlan-limit**| **mac-limit**]

Syntax Description

entries	Number of entries that can be inserted into the cache.
vlan-limit *number*	(Optional) Specifies a neighbor binding limit per number of VLANs.
interface-limit *number*	(Optional) Specifies a neighbor binding limit per interface.
mac-limit *number*	(Optional) Specifies a neighbor binding limit per number of Media Access Control (MAC) addresses.

Command Default

This command is disabled.

Command Modes

Global configuration (config)

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 **ipv6 neighbor binding max-entries** command is used to control the content of the binding table. This command specifies the maximum number of entries that are allowed to be inserted in the binding table cache. Once this limit is reached, new entries are refused, and the Neighbor Discovery Protocol (NDP) traffic source with the new entry is dropped.

If the maximum number of entries specified is lower than the current number of entries in the database, no entries are cleared, and the new threshold is reached after normal cache attrition.

The maximum number of entries can be set globally by number of VLANs or by number of MAC addresses.

Examples

The following example shows how to specify globally the maximum number of entries inserted into the cache:

```
Router(config)# ipv6 neighbor binding max-entries 100
```

Related Commands

Command	Description
ipv6 neighbor binding vlan	Adds a static entry to the binding table database.
ipv6 neighbor tracking	Tracks entries in the binding table.

ipv6 neighbor binding vlan

To add a static entry to the binding table database, use the **ipv6 neighbor binding vlan** command in global configuration mode. To remove the static entry, use the **no** form of this command.

ipv6 neighbor binding vlan *vlan-id* {**interface** *type number*| *ipv6-address*| *mac-address*} [**tracking** [**disable**| **enable**| **retry-interval** *value*]| **reachable-lifetime** *value*]

no ipv6 neighbor binding vlan *vlan-id*

Syntax Description

vlan-id	ID of the specified VLAN.
interface *type number*	Adds static entries by the specified interface type and number.
ipv6-address	IPv6 address of the static entry.
mac-address	Media Access Control (MAC) address of the static entry.
tracking	(Optional) Verifies a static entry's reachability directly.
disable	(Optional) Disables tracking for a particular static entry.
enable	(Optional) Enables tracking for a particular static entry.
retry-interval *value*	(Optional) Verifies a static entry's reachability, in seconds, at the configured interval. The range is from 1 to 3600, and the default is 300.
reachable-lifetime *value*	(Optional) Specifies the maximum time, in seconds, an entry is considered reachable without getting a proof of reachability (direct reachability through tracking, or indirect reachability through Neighbor Discovery Protocol [NDP] inspection). After that, the entry is moved to stale. The range is from 1 to 3600 seconds, and the default is 300 seconds.

Command Default

Retry interval: 300 seconds

Reachable lifetime: 300 seconds

Command Modes Global configuration (config)

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 **ipv6 neighbor binding vlan** command is used to control the content of the binding table. Use this command to add a static entry in the binding table database. The binding table manager is responsible for aging out entries and verifying their reachability directly by probing them (if the **tracking** keyword is enabled). Use of the **tracking** keyword overrides any general behavior provided globally by the **ipv6 neighbor tracking** command for this static entry. The **disable** keyword disables tracking for this static entry. The **stale-lifetime** keyword defines the maximum time the entry will be kept once it is determined to be not reachable (or stale).

Examples The following example shows how to change the reachable lifetime for binding entries to 100 seconds:

```
Router(config)# ipv6 neighbor binding vlan reachable-lifetime 100
```

Related Commands

Command	Description
ipv6 neighbor binding max-entries	Specifies the maximum number of entries that are allowed to be inserted in the cache.
ipv6 neighbor tracking	Tracks entries in the binding table.

ipv6 neighbor tracking

To track entries in the binding table, use the **ipv6 neighbor tracking** command in global configuration mode. To disable entry tracking, use the **no** form of this command.

ipv6 neighbor tracking [**retry-interval** *value*]

no ipv6 neighbor tracking [**retry-interval** *value*]

Syntax Description

retry-interval *value*	(Optional) Verifies a static entry's reachability at the configured interval time, in seconds, between two probings. The range is from 1 to 3600, and the default is 300.

Command Default

Retry interval: 300 seconds

Reachable lifetime: 300 seconds

Stale lifetime: 1440 minutes

Down lifetime: 1440 minutes

Command Modes

Global configuration (config)

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 **ipv6 neighbor tracking** command enables the tracking of entries in the binding table. Entry reachability is tested at every interval configured by the optional **retry-interval** keyword (or every 300 seconds, which is the default retry interval) using the neighbor unreachability detection (NUD) mechanism used for directly tracking neighbor reachability.

Reachability can also be established indirectly by using Neighbor Discovery Protocol (NDP) inspection up to the VERIFY_MAX_RETRIES value (the default is 10 seconds). When there is no response, entries are considered stale and are deleted after the stale lifetime value is reached (the default is 1440 minutes).

When the **ipv6 neighbor tracking** command is disabled, entries are considered stale after the reachable lifetime value is met (the default is 300 seconds) and deleted after the stale lifetime value is met.

To change the default values of neighbor binding entries in a binding table, use the **ipv6 neighbor binding** command.

Examples

The following example shows how to track entries in a binding table:

```
Router(config)# ipv6 neighbor tracking
```

Related Commands

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

ipv6 prefix-list

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

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

no ipv6 prefix-list *list-name*

Syntax Description

list-name	Name of the prefix list. • Cannot be the same name as an existing access list. • Cannot be the name “detail” or “summary” because they are keywords in the **show ipv6 prefix-list** command.
seq *seq-number*	(Optional) Sequence number of the prefix list entry being configured.
deny	Denies networks that matches the condition.
permit	Permits networks that matches the condition.
ipv6-prefix	The IPv6 network assigned to the specified prefix list. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/*prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
description *text*	A description of the prefix list that can be up to 80 characters in length.
ge *ge-value*	(Optional) Specifies a prefix length greater than or equal to the *ipv6-prefix*/*prefix-length* arguments. It is the lowest value of a range of the *length* (the “from” portion of the length range).

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

Command Default

No prefix list is created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

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

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

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

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

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

IPv6 prefix lists are used to specify certain prefixes or a range of prefixes that must be matched before a permit or deny statement can be applied. Two operand keywords can be used to designate a range of prefix lengths

to be matched. A prefix length of less than, or equal to, a value is configured with the **le** keyword. A prefix length greater than, or equal to, a value is specified using the **ge** keyword. The **ge** and **le** keywords can be used to specify the range of the prefix length to be matched in more detail than the usual *ipv6-prefix*/*prefix-length* argument. For a candidate prefix to match against a prefix list entry three conditions can exist:

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

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

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

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

Examples

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Related Commands

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