CHAPTER 26

Configuring IPv6 Neighbor Discovery

The IPv6 neighbor discovery process uses ICMPv6 messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), verify the readability of a neighbor, and keep track of neighboring routers. For information about how to configure IPv6 Neighbor Discovery in ASDM, see the *Cisco ASA 5500 Series Configuration Guide using ASDM*.

This chapter describes how to enable and configure IPv6 neighbor discovery on the adaptive security appliance and includes the following sections:

Configuring Neighbor Solicitation Messages

This section includes the following topics:

Configuring the Neighbor Solicitation Message Interval

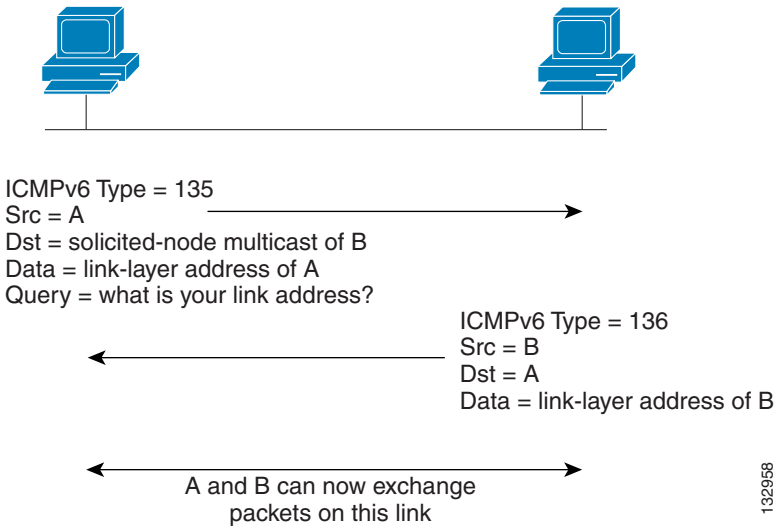
Information About Neighbor Solicitation Messages

Neighbor solicitation messages (ICMPv6 Type 135) are sent on the local link by nodes attempting to discover the link-layer addresses of other nodes on the local link. The neighbor solicitation message is sent to the solicited-node multicast address. The source address in the neighbor solicitation message is the IPv6 address of the node sending the neighbor solicitation message. The neighbor solicitation message also includes the link-layer address of the source node.

After receiving a neighbor solicitation message, the destination node replies by sending a neighbor advertisement message (ICPMv6 Type 136) on the local link. The source address in the neighbor advertisement message is the IPv6 address of the node sending the neighbor advertisement message; the destination address is the IPv6 address of the node that sent the neighbor solicitation message. The data portion of the neighbor advertisement message includes the link-layer address of the node sending the neighbor advertisement message.

After the source node receives the neighbor advertisement, the source node and destination node can communicate. Figure 26-1 shows the neighbor solicitation and response process.

Figure 26-1 IPv6 Neighbor Discovery—Neighbor Solicitation Message



Neighbor solicitation messages are also used to verify the reachability of a neighbor after the link-layer address of a neighbor is identified. When a node wants to verifying the reachability of a neighbor, the destination address in a neighbor solicitation message is the unicast address of the neighbor.

Neighbor advertisement messages are also sent when there is a change in the link-layer address of a node on a local link. When there is such a change, the destination address for the neighbor advertisement is the all-nodes multicast address.

Licensing Requirements for Neighbor Solicitation Messages

The following table shows the licensing requirements for this feature:

Model	License Requirement
All models	Base License.

Guidelines and Limitations for the Neighbor Solicitation Message Interval

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed mode only. Transparent mode is not supported.

Additional Guidelines and Limitations

The interval value is included in all IPv6 router advertisements sent out this interface.

Default Settings for the Neighbor Solicitation Message Interval

Table 26-1 lists the default settings for neighbor solicitation message parameters.

Table 26-1 Default Neighbor Solicitation Messages Parameters

Parameters	Default
value (transmission interval)	1000 seconds between neighbor solicitation transmissions

Configuring the Neighbor Solicitation Message Interval

To configure the interval between IPv6 neighbor solicitation retransmissions on an interface, enter the following command:

Command	Purpose
ipv6 nd ns-interval *value* **Example:** `hostname (config-if)# ipv6 nd ns-interval 9000`	Sets the interval between IPv6 neighbor solicitation retransmissions on an interface. Valid values for the value argument range from 1000 to 3600000 milliseconds. This information is also sent in router advertisement messages.

Examples

The following example configures an IPv6 neighbor solicitation transmission interval of 9000 milliseconds for GigabitEthernet 0/0:

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd ns-interval 9000
```

Monitoring Neighbor Solicitation Message Intervals

To monitor IPv6 neighbor solicitation message intervals, enter the following command:

Command	Purpose
`show ipv6 interface`	Displays the usability status of interfaces configured for IPv6. Including the interface name, such as "outside," displays the settings for the specified interface. Excluding the name from the command displays the settings for all interfaces that have IPv6 enabled on them. Output for the command shows the following: • The name and status of the interface. • The link-local and global unicast addresses. • The multicast groups to which the interface belongs. • ICMP redirect and error message settings. • Neighbor discovery settings. • The actual time when the command is set to 0. • The neighbor discovery reachable time that is being used.

Feature History for the Neighbor Solicitation Message Interval

Table 26-2 lists the release history for this feature.

Table 26-2 Feature History for Neighbor Solicitation Message Interval

Feature Name	Releases	Feature Information
Neighbor solicitation message interval	7.0(1)	The feature was introduced. The **ipv6 nd ns-interval** command was introduced.

Configuring the Neighbor Reachable Time

This section includes the following topics:

Information About Neighbor Reachable Time

The neighbor reachable time enables detecting unavailable neighbors. Shorter configured times enable detecting unavailable neighbors more quickly, however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.

Licensing Requirements for Neighbor Reachable Time

The following table shows the licensing requirements for this feature:

Model	License Requirement
All models	Base License.

Guidelines and Limitations for Neighbor Reachable Time

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed mode only. Transparent mode is not supported.

Additional Guidelines and Limitations

- The interval value is included in all IPv6 router advertisements sent out this interface.
- The configured time enables detecting unavailable neighbors. Shorter configured times enable detecting unavailable neighbors more quickly; however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.

Default Settings for the Neighbor Reachable Time

Table 26-3 lists the default settings for neighbor reachable time parameters.

Table 26-3 Default Neighbor Reachable Time Parameters

Parameters	Default
value (time mode is reachable)	The default is 0.

Configuring Neighbor Reachable Time

To configure the amount of time that a remote IPv6 node is considered reachable after a reachability confirmation event has occurred, enter the following command:

Command	Purpose
ipv6 nd reachable-time *value* **Example:** `hostname (config-if)# ipv6 nd reachable-time 1700000`	Sets the amount of time that a remote IPv6 node is reachable. Valid values for the *value* argument range from 0 to 3600000 milliseconds. When 0 is used for the value, the reachable time is sent as undetermined. It is up to the receiving devices to set and track the reachable time value.

Examples

The following example configures an IPv6 reachable time of 1700000 milliseconds for the selected interface, GigabitEthernet 0/0:

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd reachable-time 1700000
```

Monitoring Neighbor Reachable Time

To monitor IPv6 neighbor reachable time, enter the following command:

Command	Purpose
show ipv6 interface	Displays the usability status of interfaces configured for IPv6. Including the interface name, such as “outside,” displays the settings for the specified interface. Excluding the name from the command displays the settings for all interfaces that have IPv6 enabled on them. Output for the command shows the following: • The name and status of the interface. • The link-local and global unicast addresses. • The multicast groups to which the interface belongs. • ICMP redirect and error message settings. • Neighbor discovery settings. • The actual time when the command is set to 0. • The neighbor discovery reachable time that is being used.

Feature History for Neighbor Reachable Time

Table 26-4 lists the release history for this feature.

Table 26-4 Feature History for Neighbor Reachable Time

Feature Name	Releases	Feature Information
Neighbor solicitation message interval	7.0(1)	The feature was introduced. The **ipv6 nd ns-interval** command was introduced.

Configuring Router Advertisement Messages

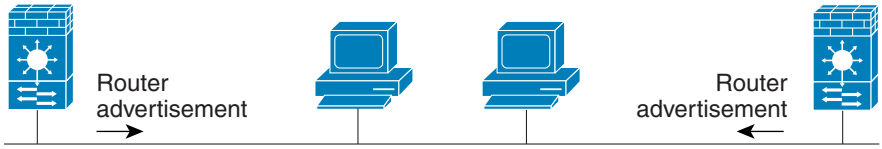
An adaptive security appliance can participate in router advertisements so that neighboring devices can dynamically learn a default router address.

This section includes the following topics:

Information About Router Advertisement Messages

An adaptive security appliance can participate in router advertisements so that neighboring devices can dynamically learn a default router address. Router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface of the adaptive security appliance. The router advertisement messages are sent to the all-nodes multicast address.

Figure 26-2 IPv6 Neighbor Discovery—Router Advertisement Message



Router advertisement packet definitions:
ICMPv6 Type = 134
Src = router link-local address
Dst = all-nodes multicast address
Data = options, prefix, lifetime, autoconfig flag

132917

Router advertisement messages typically include the following information:

- One or more IPv6 prefix that nodes on the local link can use to automatically configure their IPv6 addresses.

- Lifetime information for each prefix included in the advertisement.
- Sets of flags that indicate the type of autoconfiguration (stateless or stateful) that can be completed.
- Default router information (whether the router sending the advertisement should be used as a default router and, if so, the amount of time (in seconds) the router should be used as a default router).
- Additional information for hosts, such as the hop limit and MTU a host should use in packets that it originates.
- The amount of time between neighbor solicitation message retransmissions on a given link.
- The amount of time a node considers a neighbor reachable.

Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled router advertisement message. Because router solicitation messages are usually sent by hosts at system startup, and the host does not have a configured unicast address, the source address in router solicitation messages is usually the unspecified IPv6 address (0:0:0:0:0:0:0:0). If the host has a configured unicast address, the unicast address of the interface sending the router solicitation message is used as the source address in the message. The destination address in router solicitation messages is the all-routers multicast address with a scope of the link. When a router advertisement is sent in response to a router solicitation, the destination address in the router advertisement message is the unicast address of the source of the router solicitation message.

You can configure the following settings for router advertisement messages:

- The time interval between periodic router advertisement messages.
- The router lifetime value, which indicates the amount of time IPv6 nodes should consider the adaptive security appliance to be the default router.
- The IPv6 network prefixes in use on the link.
- Whether or not an interface transmits router advertisement messages.

Unless otherwise noted, the router advertisement message settings are specific to an interface and are entered in interface configuration mode. See the following topics for information about changing these settings:

- Configuring the Router Advertisement Transmission Interval, page 26-8
- Configuring the Router Lifetime Value, page 26-11
- Configuring the IPv6 Prefix, page 26-13
- Suppressing Router Advertisement Messages, page 26-17

Configuring the Router Advertisement Transmission Interval

This section shows how to configure the interval between IPv6 router advertisement transmissions on an interface and includes the following topics:

- Licensing Requirements for Router Advertisement Transmission Interval, page 26-9
- Guidelines and Limitations for the Router Advertisement Transmission Interval, page 26-9
- Default Settings for Router Advertisement Transmission Interval, page 26-9
- Configuring Router Advertisement Transmission Interval, page 26-9
- Monitoring the Router Advertisement Transmission Interval, page 26-10
- Feature History for the Router Advertisement Transmission Interval, page 26-10

Licensing Requirements for Router Advertisement Transmission Interval

The following table shows the licensing requirements for this feature:

Model	License Requirement
All models	Base License.

Guidelines and Limitations for the Router Advertisement Transmission Interval

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed mode only. Transparent mode is not supported.

Additional Guidelines and Limitations

The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if the adaptive security appliance is configured as a default router.by using the **ipv6 nd ra-lifetime** command. To prevent synchronization with other IPv6 nodes, randomly adjust the actual value used to within 20 percent of the specified value.

Default Settings for Router Advertisement Transmission Interval

Table 26-5 lists the default settings for neighbor reachable time parameters.

Table 26-5 Default Router Advertisement Transmission Interval Parameters

Parameters	Default
value (interval between transmissions)	The default is 200 seconds.

Configuring Router Advertisement Transmission Interval

To configure the interval between IPv6 router advertisement transmissions on an interface, enter the following command:

Command	Purpose
ipv6 nd ra-interval [**msec**] *value* **Example:** `hostname (config-if)# ipv6 nd ra-interval 201`	Sets the interval between IPv6 router advertisement transmissions. The optional **msec** keyword indicates that the value provided is in milliseconds. If this keyword is not present, the value provided is in seconds. Valid values for the *value* argument range from 3 to 1800 seconds or from 500 to 1800000 milliseconds if the msec keyword is provided.

Examples

The following example configures an IPv6 router advertisement interval of 201 seconds for the selected interface, GigabitEthernet 0/0:

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd ra-interval 201
```

Monitoring the Router Advertisement Transmission Interval

To monitor IPv6 neighbor reachable time, enter the following command:

Command	Purpose
`show ipv6 interface`	Displays the usability status of interfaces configured for IPv6. Including the interface name, such as “outside,” displays the settings for the specified interface. Excluding the name from the command displays the settings for all interfaces that have IPv6 enabled on them. Output for the command shows the following: • The name and status of the interface. • The link-local and global unicast addresses. • The multicast groups to which the interface belongs. • ICMP redirect and error message settings. • Neighbor discovery settings. • The actual time when the command is set to 0. • The neighbor discovery reachable time that is being used.

Feature History for the Router Advertisement Transmission Interval

Table 26-6 lists the release history for this feature.

Table 26-6 Feature History for Router Advertisement Transmission Interval

Feature Name	Releases	Feature Information
Router advertisement transmission interval	7.0(1)	The feature was introduced. The **ipv6 nd ra-interval** command was introduced.

Configuring the Router Lifetime Value

This section shows how to configure the interval between IPv6 router advertisement transmissions on an interface and includes the following topics:

Licensing Requirements for the Router Lifetime Value

The following table shows the licensing requirements for this feature:

Model	License Requirement
All models	Base License.

Guidelines and Limitations for the Router Lifetime Value

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed mode only. Transparent mode is not supported.

Additional Guidelines and Limitations

The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if the adaptive security appliance is configured as a default router by using the **ipv6 nd ra-lifetime** command. To prevent synchronization with other IPv6 nodes, randomly adjust the actual value used to within 20 percent of the specified value.

Default Settings for the Router Lifetime Value

Table 26-7 lists the default settings for neighbor reachable time parameters.

Table 26-7 Default Router Advertisement Transmission Interval Parameters

Parameters	Default
value (interval between transmissions)	The default is 200 seconds.

Configuring the Router Lifetime Value

To configure the interval between IPv6 router advertisement transmissions on an interface, enter the following command:

Command	Purpose
ipv6 nd ra-interval [**msec**] *value* **Example:** `hostname (config-if)# ipv6 nd ra-interval 201`	Sets the interval between IPv6 router advertisement transmissions. The optional **msec** keyword indicates that the value provided is in milliseconds. If this keyword is not present, the value provided is in seconds. Valid values for the *value* argument range from 3 to 1800 seconds or from 500 to 1800000 milliseconds if the msec keyword is provided.

Examples

The following example configures an IPv6 router advertisement interval of 201 seconds for the selected interface, GigabitEthernet 0/0:

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd ra-interval 201
```

Monitoring the Router Lifetime Value

To monitor IPv6 neighbor reachable time, enter the following command:

Command	Purpose
show ipv6 interface	Displays the usability status of interfaces configured for IPv6. Including the interface name, such as “outside,” displays the settings for the specified interface. Excluding the name from the command displays the settings for all interfaces that have IPv6 enabled on them. Output for the command shows the following: • The name and status of the interface. • The link-local and global unicast addresses. • The multicast groups to which the interface belongs. • ICMP redirect and error message settings. • Neighbor discovery settings. • The actual time when the command is set to 0. • The neighbor discovery reachable time that is being used.

Where to Go Next

Configure the router lifetime value in IPv6 router advertisements on an interface with the **ipv6 nd ra-lifetime** command.

Feature History for the Router Lifetime Value

Table 26-8 lists the release history for this feature.

Table 26-8 Feature History for Router Advertisement Transmission Interval

Feature Name	Releases	Feature Information
Router advertisement transmission interval	7.0(1)	The feature was introduced. The **ipv6 nd ra-interval** command was introduced.

Configuring the IPv6 Prefix

Stateless autoconfiguration uses IPv6 prefixes provided in router advertisement messages to create the global unicast address from the link-local address. The prefix advertisement can be used by neighboring devices to autoconfigure their interface addresses. You can configure which IPv6 prefixes ar e included in IPv6 router advertisements.

This section shows how to configure IPv6 prefixes and includes the following topics:

Licensing Requirements for IPv6 Prefixes

The following table shows the licensing requirements for this feature:

Model	License Requirement
All models	Base License.

Guidelines and Limitations for IPv6 Prefixes

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed mode only. Transparent mode is not supported.

Additional Guidelines and Limitations

The **ipv6 nd prefix** command allows control over the individual parameters per prefix, including whether or not the prefix should be advertised.

By default, prefixes configured as addresses on an interface using the **ipv6 address** command are advertised in router advertisements. If you configure prefixes for advertisement using the **ipv6 nd prefix** command, then only these prefixes are advertised.

The **default** keyword can be used to set default parameters for all prefixes.

A date can be set to specify the expiration of a prefix. The valid and preferred lifetimes are counted down in real time. When the expiration date is reached, the prefix will no longer be advertised.

When onlink is on (by default), the specified prefix is assigned to the link. Nodes sending traffic to such addresses that contain the specified prefix consider the destination to be locally reachable on the link.

When autoconfig is on (by default), it indicates to hosts on the local link that the specified prefix can be used for IPv6 autoconfiguration.

For stateless autoconfiguration to work correctly, the advertised prefix length in router advertisement messages must always be 64 bits.

Default Settings for IPv6 Prefixes

Table 26-9 lists the default settings for neighbor reachable time parameters.

Table 26-9 Default for IPv6 Prefixes Parameters

Parameters	Default
prefix lifetime	The default lifetime is 2592000 seconds (30 days) and a preferred lifetime is 604800 seconds (7 days).
on-link flag	The flag is on by default, which means that the prefix is used on the advertising interface.
autoconfig flag	The flag is on by default, which means that the prefix is used for autoconfiguration.

Configuring IPv6 Prefixes

To configure the which IPv6 prefixes are included in IPv6 router advertisements, enter the following command:

Command	Purpose
ipv6 nd prefix *ipv6-prefix/prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-autoconfig**] **Example:** `hostname (config-if)# ipv6 nd prefix 2001:200:200::/35 1000 900`	Configures which IPv6 prefixes are included in IPv6 router advertisements. The **at** *valid-date preferred-date* syntax indicates the date and time at which the lifetime and preference expire. The prefix is valid until this specified date and time are reached. Dates are expressed in the form *date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire*. The **default** keyword indicates that default values are used. The optional **infinite** keyword specifies that the valid lifetime does not expire. The *ipv6-prefix* argument specifies the IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. The optional **no-advertise** keyword indicates to hosts on the local link that the specified prefix is not to be used for IPv6 autoconfiguration. The optional **no-autoconfig** keyword indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration. The optional **off-link** keyword indicates that the specified prefix is not used for on-link determination. The *preferred-lifetime* argument specifies the amount of time (in seconds) that the specified IPv6 prefix is advertised as being preferred. Valid values range from 0 to 4294967295 seconds. The maximum value represents infinity, which can also be specified with infinite. The default is 604800 (7 days). The *prefix-length* argument specifies the length of the IPv6 prefix. This value indicates how many of the high-order, contiguous bits of the address comprise the network portion of the prefix. The slash (/) must precede the prefix length. The *valid-lifetime* argument specifies the amount of time that the specified IPv6 prefix is advertised as being valid. Valid values range from 0 to 4294967295 seconds. The maximum value represents infinity, which can also be specified with infinite. The default is 2592000 (30 days).

Examples

The following example includes the IPv6 prefix 2001:200::/35, with a valid lifetime of 1000 seconds and a preferred lifetime of 900 seconds, in router advertisements sent out on the specified interface, which is GigabitEthernet 0/0:

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd prefix 2001:200:200::/35 1000 900
```

Command	Purpose
`show ipv6 interface`	Displays the usability status of interfaces configured for IPv6. Including the interface name, such as “outside,” displays the settings for the specified interface. Excluding the name from the command displays the settings for all interfaces that have IPv6 enabled on them. Output for the command shows the following: • The name and status of the interface. • The link-local and global unicast addresses. • The multicast groups to which the interface belongs. • ICMP redirect and error message settings. • Neighbor discovery settings. • The actual time when the command is set to 0. • The neighbor discovery reachable time that is being used.

Additional References

For additional information related to implementing IPv6 router advertisement messages, see the following topics:

- Related Documents for IPv6 Prefixes, page 26-17
- RFCs for IPv6 Prefixes, page 26-17

Related Documents for IPv6 Prefixes

Related Topic	Document Title
ipv6 commands	*Cisco ASA 5500 Series Command Reference*

RFCs for IPv6 Prefixes

RFC	Title
RFC 2373 includes complete documentation to show how IPv6 network address numbers must be shown in router advertisements. The command argument *ipv6-prefix* indicates this network number, where the address must be specified in hexadecimal using 16-bit values between colons.	IP Version 6 Addressing Architecture

Feature History for IPv6 Prefixes

Table 26-10 lists the release history for this feature.

Table 26-10 Feature History for Router Advertisement Transmission Interval

Feature Name	Releases	Feature Information
Router advertisement transmission interval	7.0(1)	The feature was introduced. The **ipv6 nd prefix** command was introduced.

Suppressing Router Advertisement Messages

By default, router advertisement messages are automatically sent in response to router solicitation messages. You may want to disable these messages on any interface for which you do not want the adaptive security appliance to supply the IPv6 prefix (for example, the outside interface).

This section shows how to suppress IPv6 router advertisement transmissions on an interface and includes the following topics:

Licensing Requirements for Suppressing Router Advertisement Messages

The following table shows the licensing requirements for this feature:

Model	License Requirement
All models	Base License.

Guidelines and Limitations for Suppressing Router Advertisement Messages

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed mode only. Transparent mode is not supported.

Additional Guidelines and Limitations

The router lifetime value is included in all IPv6 router advertisements sent out the interface. The value indicates the usefulness of the adaptive security appliance as a default router on this interface.

Setting the value to a non-zero value indicates that the adaptive security appliance should be considered a default router on this interface. The no-zero value for the router lifetime value should not be less than the router advertisement interval.

Default Settings for Suppressing Router Advertisement Messages

Table 26-11 lists the default settings for neighbor reachable time parameters.

Table 26-11 Default for Suppressing Router Advertisement Parameters

Parameters	Default
router lifetime	The default lifetime is 1800 seconds. Setting the value to 0 indicates that the adaptive security appliance should not be considered a default router on this interface.

Suppressing Router Advertisement Messages

To configure the router lifetime value in IPv6 router advertisements on an interface, enter the following command:

Command	Purpose
ipv6 nd ra-lifetime *seconds* **Example:** `hostname (config-if)# ipv6 nd prefix 2001:200:200::/35 1000 900`	Configures the router lifetime value. The *seconds* argument specifies the validity of the adaptive security appliance as a default router on this interface. Valid values range from 0 to 9000 seconds. The default is 1800 seconds. 0 indicates that the adaptive security appliance should not be considered a default router on the specified interface. Entering this command causes the adaptive security appliance to appear as a regular IPv6 neighbor on the link and not as an IPv6 router.

Examples

The following example configures an IPv6 router advertisement lifetime of 1801 seconds for the specified interface, which is GigabitEthernet 0/0:

```
hostname (config)# interface gigabitethernet 0/0
hostname (config-if)# ipv6 nd ra-lifetime 1801
```

Command	Purpose
show ipv6 interface	Displays the usability status of interfaces configured for IPv6. Including the interface name, such as outside, displays the settings for the specified interface. Excluding the name from the command displays the settings for all interfaces that have IPv6 enabled on them. Output for the command shows the following: • The name and status of the interface. • The link-local and global unicast addresses. • The multicast groups to which the interface belongs. • ICMP redirect and error message settings. • Neighbor discovery settings. • The actual time when the command is set to 0. • The neighbor discovery reachable time that is being used.

Feature History for Suppressing Router Advertisement Messages

Table 26-12 lists the release history for this feature.

Table 26-12 Feature History for Suppressing Router Advertisement Messages

Feature Name	Releases	Feature Information
Suppressing router advertisement messages	7.0(1)	The feature was introduced. The **ipv6 nd ra-lifetime** command was introduced.

Configuring a Static IPv6 Neighbor

This section includes the following topics:

Information About a Static IPv6 Neighbor

You can manually define a neighbor in the IPv6 neighbor cache. If an entry for the specified IPv6 address already exists in the neighbor discovery cache—learned through the IPv6 neighbor discovery process—the entry is automatically converted to a static entry. Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process

Licensing Requirements for Static IPv6 Neighbor

The following table shows the licensing requirements for this feature:

Model	License Requirement
All models	Base License.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed mode only. Transparent mode is not supported.

Additional Guidelines and Limitations

The following guidelines and limitations apply for configuring a static IPv6 neighbor:

- The **ipv6 neighbor** command is similar to the **arp** command. If an entry for the specified IPv6 address already exists in the neighbor discovery cache—learned through the IPv6 neighbor discovery process—the entry is automatically converted to a static entry. These entries are stored in the configuration when the copy command is used to store the configuration.
- Use the **show ipv6 neighbor** command to view static entries in the IPv6 neighbor discovery cache.
- The **clear ipv6 neighbor** command deletes all entries in the IPv6 neighbor discovery cache except static entries. The **no ipv6 neighbor** command deletes a specified static entry from the neighbor discovery cache; the command does not remove dynamic entries—entries learned from the IPv6 neighbor discovery process—from the cache. Disabling IPv6 on an interface by using the **no ipv6 enable** command deletes all IPv6 neighbor discovery cache entries configured for that interface except static entries (the state of the entry changes to INCMP [Incomplete]).
- Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.
- The **clear ipv6 neighbor** command does not remove static entries from the IPv6 neighbor discovery cache; it only clears the dynamic entries.

Default Settings

Table 26-13 lists the default settings for static IPv6 neighbor parameters.

Table 26-13 Default Static IPv6 Neighbor Parameters

Parameters	Default
Static IPv6 neighbor	Static entries are not configured in the IPv6 neighbor discovery cache.

Configuring a Static IPv6 Neighbor

To configure a static entry in the IPv6 neighbor discovery cache, enter the following command:

Command	Purpose
ipv6 neighbor *ipv6_address if_name mac_address* **Example:** `hostname)config-if)# ipv6 neighbor 3001:1::45A inside 002.7D1A.9472`	Configures a static entry in the IPv6 neighbor discovery cache. The *ipv6_address* argument is the link-local IPv6 address of the neighbor, the *if_name* argument is the interface through which the neighbor is available, and the *mac_address* argument is the MAC address of the neighbor interface.

Examples

The following example adds a static entry for an inside host with an IPv6 address of 3001:1::45A and a MAC address of 002.7D1a.9472 to the neighbor discovery cache:

```
hostname)config-if)# ipv6 neighbor 3001:1::45A inside 002.7D1A.9472
```

Monitoring Neighbor Solicitation Messages

To monitor IPv6 neighbor discovery, enter the following command:

Command	Purpose
`show ipv6 interface`	Displays the usability status of interfaces configured for IPv6. Including the interface name, such as outside, displays the settings for the specified interface. Excluding the name from the command displays the settings for all interfaces that have IPv6 enabled on them. Output for the command shows the following: • The name and status of the interface. • The link-local and global unicast addresses. • The multicast groups to which the interface belongs. • ICMP redirect and error message settings. • Neighbor discovery settings.

Feature History for Configuring a Static IPv6 Neighbor

Table 26-14 lists the release history for this feature.

Table 26-14 Feature History for Configuring a Static IPv6 Neighbor

Feature Name	Releases	Feature Information
Static IPv6 Neighbor	7.0(1)	The feature was introduced. The **ipv6 neighbor** command was introduced.