IPv6 Neighbor Discovery

About 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.

Nodes (hosts) use neighbor discovery to determine the link-layer addresses for neighbors known to reside on attached links and to quickly purge cached values that become invalid. Hosts also use neighbor discovery to find neighboring routers that are willing to forward packets on their behalf. In addition, nodes use the protocol to actively keep track of which neighbors are reachable and which are not, and to detect changed link-layer addresses. When a router or the path to a router fails, a host actively searches for functioning alternates.

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. After receiving a neighbor solicitation message, the destination node replies by sending a neighbor advertisement message (ICPMv6 Type 136) on the local link.

After the source node receives the neighbor advertisement, the source node and destination node can communicate. 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.

Duplicate Address Detection

During the stateless autoconfiguration process, Duplicate Address Detection verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces.

When a duplicate address is identified, the state of the address is set to DUPLICATE, the address is not used, and the following error message is generated:

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface. If the duplicate address is a global address, the address is not used.

The ASA uses neighbor solicitation messages to perform Duplicate Address Detection. By default, the number of times an interface performs Duplicate Address Detection is 1.

Router Advertisement Messages

The ASA 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 ASA.

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.

Static IPv6 Neighbors

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.

Prerequisites for IPv6 Neighbor Discovery

Configure IPv6 addressing according to Configure IPv6 Addressing.

Guidelines for IPv6 Neighbor Discovery

Firewall Mode Guidelines

The following IPv6 neighbor discovery commands are not supported in transparent firewall mode, because they require router capabilities:

- **ipv6 nd prefix**

- **ipv6 nd ra-interval**
- **ipv6 nd ra-lifetime**
- **ipv6 nd suppress-ra**

Additional Guidelines and Limitations

- The interval value is included in all IPv6 router advertisements that are sent out of 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.
- The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if the ASA 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.
- 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.
- The router lifetime value is included in all IPv6 router advertisements sent out of the interface. The value indicates the usefulness of the ASA as a default router on this interface.
- Setting the value to a non-zero value indicates that the ASA should be considered a default router on this interface. The non-zero value for the router lifetime value should not be less than the router advertisement interval.

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.
- The ICMP syslogs generated are caused by a regular refresh of IPv6 neighbor entries. The ASA default timer for IPv6 neighbor entry is 30 seconds, so the ASA would generate ICMPv6 neighbor discovery and response packets about every 30 seconds. If the ASA has both failover LAN and state interfaces configured with IPv6 addresses, then every 30 seconds, ICMPv6 neighbor discovery and response packets will be generated by both ASAs for both configured and link-local IPv6 addresses. In addition, each packet will generate several syslogs (ICMP connection and local-host creation or teardown), so it may appear that constant ICMP syslogs are being generated. The refresh time for IPV6 neighbor entry is configurable on the regular data interface, but not configurable on the failover interface. However, the CPU impact for this ICMP neighbor discovery traffic is minimal.

Defaults for IPv6 Neighbor Discovery

The following table lists the default settings for IPv6 Neighbor Discovery.

Table 1: Default IPv6 Neighbor Discovery Parameters

Parameters	Default
value for the neighbor solicitation transmission message interval	1000 seconds between neighbor solicitation transmissions.
value for the neighbor reachable time	The default is 0.
value for the router advertisement transmission interval	The default is 200 seconds.
value for the router lifetime	The default is 1800 seconds.
value for the number of consecutive neighbor solicitation messages sent during DAD	The default is one message.
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.

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

Configure IPv6 Neighbor Discovery

Follow this procedure to configure IPv6 Neighbor discovery:

Procedure

Step 1 Configure neighbor discovery settings for each interface.
Step 2 Configure the neighbor solicitation message interval.
Step 3 Configure the neighbor reachable time.
Step 4 Configure the router advertisement transmission interval.
Step 5 Configure the router lifetime value.
Step 6 Configure DAD settings.

Enter Interface Configuration Mode

Configure neighbor discovery settings per interface. To enter interface configuration mode, perform the following steps.

Procedure

Enter interface configuration mode:
interface *name*

Example:

```
ciscoasa(config)# interface gigabitethernet 0/0
```

Configure the Neighbor Solicitation Message Interval

To configure the interval between IPv6 neighbor solicitation retransmissions on an interface perform the following steps.

Procedure

Set the interval between IPv6 neighbor solicitation retransmissions on an interface:
ipv6 nd ns-interval *value*

Example:

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

Valid values for the value argument range from 1000 to 3600000 milliseconds.

This information is also sent in router advertisement messages.

Configure the 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.

Procedure

Set the amount of time that a remote IPv6 node is reachable:
ipv6 nd reachable-time *value*

Example:

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

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.

Configure the Router Advertisement Transmission Interval

To configure the interval between IPv6 router advertisement transmissions on an interface, perform the following steps:

Procedure

Set the interval between IPv6 router advertisement transmissions:
ipv6 nd ra-interval [**msec**] *value*

Example:

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

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. The default is 200 seconds.

The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if the ASA is configured as a default router. For more information, see Configure the Router Lifetime Value, on page 7. To prevent synchronization with other IPv6 nodes, randomly adjust the actual value used to within 20 percent of the desired value.

Configure the Router Lifetime Value

To configure the router lifetime value in IPv6 router advertisements on an interface perform the following steps.

Procedure

Specify the length of time that nodes on the local link should consider the ASA as the default router on the link:
ipv6 nd ra-lifetime [**msec**] *value*

Example:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd ra-lifetime 2000
```

- 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 0 to 9000 seconds.
- Entering 0 indicates that the ASA should not be considered a default router on the selected interface.

Configure DAD Settings

To specify DAD settings on the interface, perform the following steps.

Procedure

Specify the uniqueness of new unicast IPv6 addresses before they are assigned and ensure that duplicate IPv6 addresses are detected in the network on a link basis:
ipv6 nd dad attempts *value*

Example:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd dad attempts 20
```

Valid values for the *value* argument range from 0 to 600. A zero value disables DAD processing on the specified interface.

Suppress Router Advertisement Messages

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 ASA to supply the IPv6 prefix (for example, the outside interface).

To suppress the router lifetime value in IPv6 router advertisements on an interface, perform the following steps.

Procedure

Suppress the router lifetime value:
ipv6 nd suppress-ra *seconds*

Example:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd suppress-ra 900
```

The *seconds* argument specifies the validity of the ASA as a default router on this interface. Valid values range from 0 to 9000 seconds.

A zero indicates that the ASA should not be considered a default router on the specified interface.

Note Entering this command causes the ASA to appear as a regular IPv6 neighbor on the link and not as an IPv6 router.

Configure Address Config Flags for IPv6 DHCP Relay

You can add a flag to IPv6 router advertisements to inform IPv6 autoconfiguration clients to use DHCPv6 to obtain an IPv6 address and/or additional information such as the DNS server address.

Procedure

Step 1 Set the Managed Address Config flag in the IPv6 router advertisement packet:
ipv6 nd managed-config-flag

Example:

```
ciscoasa(config-if)# ipv6 nd managed-config-flag
```

This flag informs IPv6 autoconfiguration clients that they should use DHCPv6 to obtain addresses, in addition to the derived stateless autoconfiguration address.

Step 2 Set the Other Address Config flag in the IPv6 router advertisement packet:
ipv6 nd other-config-flag

Example:

```
ciscoasa(config-if)# ipv6 nd other-config-flag
```

This flag informs IPv6 autoconfiguration clients that they should use DHCPv6 to obtain additional information from DHCPv6, such as the DNS server address.

Configure the IPv6 Prefix in Router Advertisements

To configure the which IPv6 prefixes are included in IPv6 router advertisements, perform the following steps:

Procedure

Configure which IPv6 prefixes are included in IPv6 router advertisements:
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:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd prefix 2001:DB8::/32 1000 900
```

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

Configuring a Static IPv6 Neighbor

To configure a static entry in the IPv6 neighbor discovery cache, perform the following steps:

Procedure

Configure a static entry in the IPv6 neighbor discovery cache:
ipv6 neighbor *ipv6_address if_name mac_address*

Example:

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

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.

Monitoring IPv6 Neighbor Discovery

To monitor IPv6 neighbor discovery parameters, enter the following command:

- **show ipv6 interface**

  This command displays the usability status of interfaces configured for IPv6, including the interface name, such as “outside,” and displays the settings for the specified interface. However, it excludes the name from the command and 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.

History for IPv6 Neighbor Discovery

Table 2: Feature History for IPv6 Neighbor Discovery

Feature Name	Releases	Feature Information
IPv6 Neighbor Discovery	7.0(1)	We introduced this feature. We introduced the following commands: **ipv6 nd ns-interval**, **ipv6 nd ra-lifetime**, **ipv6 nd suppress-ra**, **ipv6 neighbor**, **ipv6 nd prefix**, **ipv6 nd dad-attempts**, **ipv6 nd reachable-time**, **ipv6 address**, **ipv6 enforce-eui64**.
Address Config Flags for IPv6 DHCP Relay	9.0(1)	We introduced the following commands: **ipv6 nd managed-config-flag**, **ipv6 nd other-config-flag**.