Configuring IPv6 Neighbors

This chapter provides information about IPv6 neighbor discovery. It shows how to add an IPv6 neighbor and how to configure neighbor solicitation messages.

This chapter includes the following sections:

- Information About IPv6 Neighbor Discovery, page 14-1
- Adding an IPv6 Static Neighbor, page 14-2
- Configuring IPv6 Neighbor Discovery, page 14-2
- Editing and Deleting Static Neighbors, page 14-7
- Viewing and Clearing Dynamic Neighbors, page 14-8

Information About IPv6 Neighbor Discovery

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. Finally, 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.

The neighbor discovery process uses IPv6 (ICMPv6) messages and solicited-node multicast addresses. Every IPv6 node is required to join the multicast groups corresponding to its unicast and anycast addresses.

Neighbor solicitation messages are sent on the local link when a node wants to determine the link-layer address of another node on the same local link. This function is similar to the ARP in IPv4, but it avoids broadcasts used in IPv4 ARP messages, where all nodes receive unnecessary broadcast requests that do not concern them. The source node takes the right-most 24 bits of the IPv6 address of the destination node and sends a neighbor solicitation message to the solicited-node multicast group address on the local link. The destination node will respond with its link-layer address. To send a neighbor solicitation message, the source node must first identify the IPv6 unicast address of the destination node using a naming service mechanism, such as DNS. A neighbor solicitation message is also used to verify the reachability of a neighbor after the link-layer address of a neighbor is identified.

The neighbor advertisement message is a response to the neighbor solicitation message. After receiving the neighbor solicitation message, the destination node replies by sending a neighbor advertisement message on the local link. After receiving the neighbor advertisement, the source node and the destination node can communicate. Neighbor advertisement messages are also sent when there is a change in the link-layer address of a node on the local link.
Adding an IPv6 Static Neighbor

Ensure that IPv6 is enabled on at least one interface before attempting to add a neighbor, or ASDM will return an error message indicating that the configuration failed. For information about configuring IPv6 on an interface, see the Chapter 9, “Configuring Interfaces.”

For information about IPv6 Neighbor Discovery, see the “Information About IPv6 Neighbor Discovery” section on page 14-1.

To add an IPv6 static neighbor, perform the following steps:

Step 1 Choose Configuration > Device Management > Advanced > IPv6 Neighbor Discovery Cache.

Step 2 Click Add.

The Add IPv6 Static Neighbor dialog box appears.

Step 3 From the Interface Name drop-down list, choose an interface on which to add the neighbor.

Step 4 In the IP Address field, enter the IPv6 address that corresponds to the local data-link address, or click the ellipsis (...) to browse for an address.

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.

Step 5 In the MAC address field, enter the local data-line (hardware) MAC address.

Step 6 Click OK.

Note Before you apply the changes and save the configuration, you can click Reset to cancel any changes and restore the original values.

Step 7 Click Apply to save the configuration.

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 reachability of a neighbor, and keep track of neighboring routers. For information about adding an IPv6 static neighbor, see the “Adding an IPv6 Static Neighbor” section on page 14-2. For information about IPv6 neighbor discovery, see the “Information About IPv6 Neighbor Discovery” section on page 14-1.

This section includes the following topics:

- Configuring Neighbor Solicitation Messages, page 14-3
- Configuring Router Advertisement Messages, page 14-5
Configuring 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 (ICMPv6 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 14-1 shows the neighbor solicitation and response process.

Figure 14-1  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.

You can configure the neighbor solicitation message interval and neighbor reachable time on a per-interface basis. See the following topics for more information:

- Configuring the IPv6 Neighbor Solicitation Message Interval, page 14-4
- Configuring the IPv6 Neighbor Reachable Time, page 14-4
Configuring the IPv6 Neighbor Solicitation Message Interval

You can configure the interval between IPv6 neighbor solicitation retransmissions on an interface. Valid values range from 1000 to 3600000 milliseconds. The default value is 1000 milliseconds. This setting is also sent in router advertisement messages.

To configure the neighbor solicitation message interval, perform the following steps:

Step 1  Choose **Configuration > Device Setup > Interfaces**.
Step 2  Choose the interface on which to configure the neighbor solicitation interval. The interface must have been configured with an IPv6 address. See the “Configuring IPv6 Neighbor Discovery” section on page 14-2 for more information.
Step 3  Click **Edit**.
   The Edit Interface dialog box appears with three tabs: General, Advanced, and IPv6.
Step 4  Click the **IPv6** tab.
Step 5  In the NS Interval field, enter the time interval.
Step 6  Click **OK**.
Step 7  Click **Apply** to save the configuration.

Configuring the IPv6 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.

Valid time values range from 0 to 3600000 milliseconds. The default is 0; however, when you use 0, the reachable time is sent as undetermined. It is up to the receiving devices to set and track the reachable time value.

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

Step 1  Choose **Configuration > Device Setup > Interfaces**.
Step 2  Select the interface for which you want to configure the time. The interface must have been configured with an IPv6 address. See the “Configuring IPv6 Neighbor Discovery” section on page 14-2 for more information.
Step 3  Click **Edit**.
   The Edit Interface dialog box appears with three tabs: General, Advanced, and IPv6.
Step 4  Click the **IPv6** tab.
Step 5  In the Reachable Time field, enter a valid value.
Step 6  Click **OK**.
Step 7  Click **Apply** to save the configuration.
Configuring Router Advertisement Messages

Router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface of the security appliance. The router advertisement messages are sent to the all-nodes multicast address.

**Figure 14-2  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

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 security appliance to be the default router.
- The IPv6 network prefixes used on the link.
- Whether or not an interface transmits router advertisement messages.
Configuring IPv6 Neighbor Discovery

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 14-6
- Configuring the Router Lifetime Value, page 14-6
- Suppressing Router Advertisement Messages, page 14-7

Configuring the Router Advertisement Transmission Interval

By default, router advertisements are sent out every 200 seconds. Valid values range from 3 to 1800 seconds.

The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if the security appliance is configured as a default router. (See the “Configuring the Router Lifetime Value” section on page 14-6.) To prevent synchronization with other IPv6 nodes, randomly adjust the actual value used to within 20 percent of the desired value.

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

1. Choose Configuration > Device Setup > Interfaces.
2. Select the interface for which you want to configure the time.
   The interface must have been configured with an IPv6 address. See the Chapter 9, “Configuring Interfaces,” for more information.
3. Click Edit.
   The Edit Interface dialog box appears with three tabs: General, Advanced, and IPv6.
4. Click the IPv6 tab.
5. In the RA Interval field, enter a valid transmission interval value.

   Note (Optional) To add a router advertisement transmission interval value in milliseconds instead of the default value in seconds, check the RA Interval in Milliseconds check box, and enter a value from 500 to 1800000 in the RA Interval field.

6. Click OK.
7. Click Apply to save the configuration.

Configuring the Router Lifetime Value

The router lifetime value specifies how long nodes on the local link should consider the security appliance as the default router on the link. Valid values range from 0 to 9000 seconds. The default is 1800 seconds. Entering 0 indicates that the security appliance should not be considered a default router on the selected interface.
To configure the router lifetime value in IPv6 router advertisements on an interface, perform the following steps:

**Step 1** Choose Configuration > Device Setup > Interfaces.

**Step 2** Select the interface for which you want to configure the lifetime value. The interface must have been configured with an IPv6 address. See the Chapter 9, “Configuring Interfaces,” for more information.

**Step 3** Click Edit.

The Edit Interface dialog box appears with three tabs: General, Advanced, and IPv6.

**Step 4** Click the IPv6 tab.

**Step 5** In the RA Lifetime field, enter a valid lifetime value.

**Step 6** Click OK.

**Step 7** Click Apply to save the configuration.

---

### 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 security appliance to supply the IPv6 prefix (for example, the outside interface).

To suppress IPv6 router advertisement transmissions on an interface, perform the following steps:

**Step 1** Choose Configuration > Device Setup > Interfaces.

**Step 2** Select the interface for which you want to configure the lifetime value. The interface must have been configured with an IPv6 address. See the “Configuring IPv6 Neighbor Discovery” section on page 14-2 for more information.

**Step 3** Click Edit.

The Edit Interface dialog box appears with three tabs: General, Advanced, and IPv6.

**Step 4** Click the IPv6 tab.

**Step 5** Check the Suppress RA check box.

**Step 6** Verify that the router advertisement message is suppressed on the interface that is configured for the IPv6 address.

---

### Editing and Deleting Static Neighbors

This section includes the following topics:

- Editing Static Neighbors, page 14-8
- Deleting Static Neighbors, page 14-8
## Viewing and Clearing Dynamic Neighbors

When a host or node communicates with a neighbor, the neighbor is added to the neighbor discovery cache. The neighbor is removed from the cache when there is no longer any communication with the neighbor.

To view dynamically discovered neighbors and to clear neighbors from the IPv6 Neighbor Discovery Cache, perform the following steps:

**Step 1** Choose Monitoring > Interface Graphs > IPv6 Neighbor Discovery Cache.

**Step 2** You can view all static and dynamically discovered neighbors from the IPv6 Neighbor Discovery Cache pane.

**Step 2** To clear all dynamically discovered neighbors from the cache, click **Clear Dynamic Neighbor Entries**.
The neighbor information is removed from the cache.

**Note**  This task clears only dynamically discovered neighbors from the cache. It does not clear static neighbors. To clear static neighbors, see the “Deleting Static Neighbors” section on page 14-8.