IPv6 Neighbor Discovery Protocol Explained

https://www.computernetworkingnotes.com/networking-tutorials/ipv6-neighbor-discovery-protocol-explained.html

This tutorial explains IPv6 neighbor discovery protocol in detail including neighbor discovery process and router solicitation, router advertisement and redirect messages.

Internet Protocol version 6 (IPv6) Neighbor Discovery (ND) is a set of messages and processes defined in RFC 4861 that determine relationships between neighboring nodes. ND replaces Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP) router discovery, and the ICMP Redirect message used in IPv4. ND also provides additional functionality.

**ND is used by nodes to do the following:**

* Resolve the link-layer address of a neighboring node to which an IPv6 packet is being forwarded.
* Determine when the link-layer address of a neighboring node has changed.
* Determine whether a neighbor is still reachable.

**ND is used by hosts to do the following:**

* Discover neighboring routers.
* Auto configure addresses, address prefixes, routes, and other configuration parameters.

**ND is used by routers to do the following:**

* Advertise their presence, host configuration parameters, routes, and on-link prefixes.
* Inform hosts of a better next-hop address to forward packets for a specific destination.

There are five different ND messages:

* Router Solicitation (ICMPv6 type 133)
* Router Advertisement (ICMPv6 type 134)
* Neighbor Solicitation (ICMPv6 type 135)
* Neighbor Advertisement (ICMPv6 type 136)
* Redirect (ICMPv6 type 137)

Router Solicitation

The Router Solicitation message is sent by IPv6 hosts to discover the presence of IPv6 routers on the link. A host sends a multicast Router Solicitation message to prompt IPv6 routers to respond immediately, rather than waiting for an unsolicited Router Advertisement message. For example, assuming that the local link is Ethernet, in the Ethernet header of the Router Solicitation message you will find these settings:

* The Source Address field is set to the MAC address of the sending network adapter.
* The Destination Address field is set to 33-33-00-00-00-02. In the IPv6 header of the Router Solicitation message, you will find the following settings:
* The Source Address field is set to either a link-local IPv6 address assigned to the sending interface or the IPv6 unspecified address (::).
* The Destination Address field is set to the link-local scope all-routers multicast address (FF02::2).
* The Hop Limit field is set to 255.

Router Advertisement

IPv6 routers send unsolicited Router Advertisement messages pseudo-periodically—that is, the interval between unsolicited advertisements is randomized to reduce synchronization issues when there are multiple advertising routers on a link—and solicited Router Advertisement messages in response to the receipt of a Router Solicitation message. The Router Advertisement message contains the information required by hosts to determine the link prefixes, the link MTU, specific routes, whether or not to use address autoconfiguration, and the duration for which addresses created through address autoconfiguration are valid and preferred. For example, assuming that the local link is Ethernet in the Ethernet header of the Router Advertisement message, you will find these settings:

* The Source Address field is set to the MAC address of the sending network adapter.
* The Destination Address field is set to either 33-33-00-00-00-01 or the unicast MAC address of the host that sent a Router Solicitation from a unicast address.

In the IPv6 header of the Router Advertisement message, you will find the following settings:

* The Source Address field is set to the link-local address assigned to the sending interface.
* The Destination Address field is set to either the link-local scope all-nodes multicast address (FF02::1) or the unicast IPv6 address of the host that sent the Router Solicitation message from a unicast address.
* The Hop Limit field is set to 255.

Neighbor Solicitation

IPv6 nodes send the Neighbor Solicitation message to discover the link-layer address of an on-link IPv6 node or to confirm a previously determined link-layer address. It typically includes the link-layer address of the sender. Typical Neighbor Solicitation messages are multicast for address resolution and unicast when the reach ability of a neighboring node is being verified. For example, assuming that the local link is Ethernet, in the Ethernet header of the Neighbor Solicitation message, you will find the following settings:

* The Source Address field is set to the MAC address of the sending network adapter.
* For a multicast Neighbor Solicitation message, the Destination Address field is set to the Ethernet MAC address that corresponds to the solicited-node address of the target. For a unicast Neighbor Solicitation message, the Destination Address field is set to the unicast MAC address of the neighbor.

In the IPv6 header of the Neighbor Solicitation message, you will find these settings:

* The Source Address field is set to either a unicast IPv6 address assigned to the sending interface or, during duplicate address detection, the unspecified address (::).
* For a multicast Neighbor Solicitation, the Destination Address field is set to the solicited node address of the target. For a unicast Neighbor Solicitation, the Destination Address field is set to the unicast address of the target.

Neighbor Advertisement

An IPv6 node sends the Neighbor Advertisement message in response to a Neighbor Solicitation message. An IPv6 node also sends unsolicited Neighbor Advertisements to inform neighboring nodes of changes in link-layer addresses or the node’s role. The Neighbor Advertisement contains information required by nodes to determine the type of Neighbor Advertisement message, the sender’s role on the network, and typically the link-layer address of the sender. For example, assuming that the local link is Ethernet, in the Ethernet header of the Neighbor Advertisement message, you will find the following settings:

* The Source Address field is set to the MAC address of the sending network adapter.
* The Destination Address field is set, for a solicited Neighbor Advertisement, to the unicast MAC address of the initial Neighbor Solicitation sender. For an unsolicited Neighbor Advertisement, the Destination Address field is set to 33-33-00-00-00-01, which is the Ethernet MAC address corresponding to the link-local scope all-nodes multicast address.

In the IPv6 header of the Neighbor Advertisement message, you will find these settings:

* The Source Address field is set to a unicast address assigned to the sending interface.
* The Destination Address field is set, for a solicited Neighbor Advertisement, to the unicast IP address of the sender of the initial Neighbor Solicitation. For an unsolicited Neighbor Advertisement, the Destination Address field is set to the link-local scope all-nodes multicast address (FF02::1).
* The Hop Limit field is set to 255.

Redirect

The Redirect message is sent by an IPv6 router to inform an originating host of a better first hop address for a specific destination. Redirect messages are sent only by routers for unicast traffic, are unicast only to originating hosts, and are processed only by hosts. For example, assuming that the local link is Ethernet, in the Ethernet header of the Redirect message, you will find the following settings:

* The Source Address field is set to the MAC address of the sending network adapter.
* The Destination Address field is set to the unicast MAC address of the originating sender.

In the IPv6 header of the Redirect message, you will find these settings:

* The Source Address field is set to a unicast address that is assigned to the sending interface.
* The Destination Address field is set to the unicast IP address of the originating host.
* The Hop Limit field is set to 255.

Neighbor Discovery Processes

The ND protocol provides message exchanges for the following processes:

* Address resolution (including duplicate address detection)
* Router discovery (includes prefix and parameter discovery)
* Neighbor unreachability detection
* Redirect function