[Prefix Discovery]

One of the options typically carried by a router advertisement is the Prefix Information option (type 3). Each prefix information option lists an IPv6 prefix (subnet) reachable on the local link. Remember that it is not uncommon for multiple IPv6 prefixes to reside on the same link, and routers may include more than one prefix in each advertisement. A host which knows what prefixes are reachable on the link can communicate directly with destinations in those prefixes without passing its traffic through a router.

[IPv6 Neighbor Discovery] 이웃 노드 탐색 기법

IPv6 solves a set of problems that are related to the interaction between nodes that are attached to the same link. IPv6 defines mechanisms for solving each of the following problems.

Router discovery – Hosts locate routers that reside on an attached link.

Prefix discovery – Hosts discover the set of address prefixes that define which destinations are attached to the link, sometimes referred to as on-link. Nodes use prefixes to distinguish destinations that reside on a link from those only reachable through a router.

Parameter discovery – A node learns link parameters, such as the link maximum transmission unit (MTU). A node also learns Internet parameters, such as the hop limit value, to place in outgoing packets.

Address autoconfiguration – Nodes automatically configure an address for an interface.

Address resolution – Nodes determine the link-layer address of a neighbor, an on-link destination, with only the destinations's IP address.

Next-hop determination – An algorithm determines mapping for an IP destination address into the IP address of the traffic destination neighbor. The next-hop can be a router or the destination.

Neighbor unreachability detection – Nodes determine that a neighbor is no longer reachable. For neighbors that are used as routers, alternate default routers can be tried. For both routers and hosts, address resolution can be performed again.

Duplicate address detection – A node determines that an address that the node wants to use is not already in use by another node.

Redirect – A router informs a host of a better first-hop node to reach a particular destination.

Neighbor discovery defines five different Internet Control Message Protocol (ICMP) packet types. One type is a pair of router solicitation and router advertisement messages. Another type is a pair of neighbor solicitation and neighbor advertisement messages. The fifth type is a redirect message. The messages serve the following purpose:

Router solicitation – When an interface becomes enabled, hosts can send router solicitations. The solicitations request routers to generate router advertisements immediately, rather than at their next scheduled time.

Router advertisement – Routers advertise their presence, various link parameters, and various Internet parameters. Routers advertise either periodically, or in response to a router solicitation message. Router advertisements contain prefixes that are used for on-link determination or address configuration, a suggested hop limit value, and so on.

Neighbor solicitation – Sent by a node to determine the link-layer address of a neighbor. Also, sent by a node to verify that a neighbor is still reachable by a cached link-layer address. Neighbor solicitations are also used for duplicate address detection.

Neighbor advertisement – A response to a Neighbor Solicitation message, node can also send unsolicited neighbor advertisements to announce a link-layer address change.

Redirect – Used by routers to inform hosts of a better first hop for a destination, or that the destination is on-link.

Router Advertisement

On multicast-capable links and point-to-point links, each router periodically multicasts a router advertisement packet that announces its availability. A host receives router advertisements from all routers, building a list of default routers. Routers generate router advertisements frequently enough that hosts learn of their presence within a few minutes. However, routers do not advertise frequently enough to rely on an absence of advertisements to detect router failure. A separate detection algorithm that determines neighbor unreachability provides failure detection.

Router Advertisement Prefixes

Router advertisements contain a list of prefixes that is used for on-link determination. The list of prefixes is also used for autonomous address configuration. Flags that are associated with the prefixes specify the intended uses of a particular prefix. Hosts use the advertised on-link prefixes to build and maintain a list. The list is used to decide when a packet's destination is on-link or beyond a router. A destination can be on-link even though the destination is not covered by any advertised on-link prefix. In such instances, a router can send a redirect. The redirect informs the sender that the destination is a neighbor.

Router advertisements, and per-prefix flags, enable routers to inform hosts how to perform address autoconfiguration. For example, routers can specify whether hosts should use stateful, DHCPv6, or autonomous, stateless, address configuration.

Router Advertisement Messages

Router advertisement messages also contain Internet parameters, such as the hop limit that hosts should use in outgoing packets. Optionally, router advertisement messages also contain link parameters, such as the link MTU. This feature enables centralized administration of critical parameters. The parameters can be set on routers and automatically propagated to all hosts that are attached.

Nodes accomplish address resolution by multicasting a neighbor solicitation that asks the target node to return its link-layer address. Neighbor solicitation messages are multicast to the solicited-node multicast address of the target address. The target returns its link-layer address in a unicast neighbor advertisement message. A single request-response pair of packets is sufficient for both the initiator and the target to resolve each other's link-layer addresses. The initiator includes its link-layer address in the neighbor solicitation.

Neighbor Solicitation and Unreachability

Neighbor solicitation messages can also be used to determine if more than one node has been assigned the same unicast address.

Neighbor unreachability detection detects the failure of a neighbor or the failure of the forward path to the neighbor. This detection requires positive confirmation that packets that are sent to a neighbor are actually reaching that neighbor. And, that packets are being processed properly by its IP layer. Neighbor unreachability detection uses confirmation from two sources. When possible, upper-layer protocols provide a positive confirmation that a connection is making forward progress. Data that was sent previously is known to have been delivered correctly. For example, new TCP acknowledgments were received recently. When positive confirmation is not forthcoming through such hints, a node sends unicast neighbor solicitation messages. These messages solicit neighbor advertisements as reachability confirmation from the next hop. To reduce unnecessary network traffic, probe messages are sent only to neighbors to which the node is actively sending packets.

In addition to addressing the previous general problems, neighbor discovery also handles the following situations.

Link-layer address change – A node that knows its link-layer address has been changed can multicast unsolicited, neighbor advertisement packets. The node can multicast to all nodes to update cached link-layer addresses that have become invalid. The sending of unsolicited advertisements is a performance enhancement only. The detection algorithm for neighbor unreachability ensures that all nodes reliably discover the new address, though the delay might be somewhat longer.

Inbound load balancing – Nodes with replicated interfaces might want to load-balance the reception of incoming packets across multiple network interfaces on the same link. Such nodes have multiple link-layer addresses assigned to the same interface. For example, a single network driver can represent multiple network interface cards as a single logical interface that has multiple link-layer addresses.

Load balancing is handled by allowing routers to omit the source link-layer address from router advertisement packets. Consequently, neighbors must use neighbor solicitation messages to learn link-layer addresses of routers. Returned neighbor advertisement messages can then contain link-layer addresses that differ, depending on who issued the solicitation.

Anycast addresses – Anycast addresses identify one of a set of nodes that provide an equivalent service. Multiple nodes on the same link can be configured to recognize the same anycast address. Neighbor discovery handles anycasts by setting nodes to expect to receive multiple neighbor advertisements for the same target. All advertisements for anycast addresses are tagged as being non-override advertisements. Non-override advertisements invoke specific rules to determine which of potentially multiple advertisements should be used.

Proxy advertisements – A router that accepts packets on behalf of a target address can issue non-override neighbor advertisements. The router can accept packets for a target address that is unable to respond to neighbor solicitations. Currently, the use of proxy is not specified. However, proxy advertising can potentially be used to handle cases like mobile nodes that have moved off-link. However, the use of proxy is not intended as a general mechanism to handle nodes that do not implement this protocol.

Comparison With IPv4

The neighbor discovery protocol of IPv6 corresponds to a combination of the IPv4 protocols Address Resolution Protocol (ARP), ICMP Router Discovery, and ICMP Redirect. IPv4 does not have a generally agreed on protocol or mechanism for neighbor unreachability detection. However, host requirements do specify some possible algorithms for dead gateway detection. Dead gateway detection is a subset of the problems that neighbor unreachability detection solves.

The neighbor discovery protocol provides a multitude of improvements over the IPv4 set of protocols.

Router discovery is part of the base protocol set. Hosts do not need to snoop the routing protocols.

Router advertisements carry link-layer addresses. No additional packet exchange is needed to resolve the router's link-layer address.

Router advertisements carry prefixes for a link. A separate mechanism is not needed to configure the netmask.

Router advertisements enable address autoconfiguration.

Routers can advertise an MTU for hosts to use on the link. Consequently, all nodes use the same MTU value on links that lack a well-defined MTU.

Address resolution multicasts are spread over 4 billion (2^32) multicast addresses, greatly reducing address-resolution-related interrupts on nodes other than the target. Moreover, non-IPv6 machines should not be interrupted at all.

Redirects contain the link-layer address of the new first hop. Separate address resolution is not needed on receiving a redirect.

Multiple prefixes can be associated with the same link. By default, hosts learn all on-link prefixes from router advertisements. However, routers can be configured to omit some or all prefixes from router advertisements. In such instances, hosts assume that destinations are off-link. Consequently, hosts send the traffic to routers. A router can then issue redirects as appropriate.

Unlike IPv4, the recipient of an IPv6 redirect message assumes that the new next-hop is on-link. In IPv4, a host ignores redirect messages that specify a next-hop that is not on-link, according to the link's network mask. The IPv6 redirect mechanism is analogous to the XRedirect facility. The redirect mechanism is useful on non-broadcast and shared media links. On these links, nodes should not check for all prefixes for on-link destinations.

Neighbor unreachability detection improves packet delivery in the presence of failing routers. This capability improves packet delivery over partially failing or partitioned links. This capability also improves packet delivery over nodes that change their link-layer addresses. For instance, mobile nodes can move off-link without losing any connectivity because of stale ARP caches.

Unlike ARP, neighbor discovery detects half-link failures by using neighbor unreachability detection. Neighbor discovery avoids sending traffic to neighbors with which two-way connectivity is absent.

Unlike in IPv4 router discovery, the router advertisement messages do not contain a preference field. The preference field is not needed to handle routers of different stability. The neighbor unreachability detection detects dead routers and dead switches to a working router.

By using link-local addresses to uniquely identify routers, hosts can maintain the router associations. The ability to identify routers is required for router advertisements. The ability to identify routers is required for redirect messages. Hosts need to maintain router associations if the site uses new global prefixes.

Because neighbor discovery messages have a hop limit of 255 upon receipt, the protocol is immune to spoofing attacks originating from off-link nodes. In contrast, IPv4 off-link nodes can send Internet Control Message Protocol (ICMP) redirect messages. IPv4 off-link nodes can also send router advertisement messages.

By placing address resolution at the ICMP layer, the protocol becomes more media independent than ARP. Consequently, standard IP authentication and security mechanisms can be used.

[https://docs.oracle.com/cd/E19683-01/817-0573/chapter1-40/index.html]

Service discovery is the automatic detection of devices and services offered by these devices on a computer network. A service discovery protocol (SDP) is a network protocol that helps accomplish service discovery.

Service discovery requires a common language to allow software agents to make use of one another's services without the need for continuous user intervention.[1]