Cynthia Omauzo

ARP vs Neighbor Discovery

1. WHAT IS ARP

ARP (Address Resolution Protocol) found in IPv4, is used to map an IP address to the device's MAC (Media Access Control) address. The simplest way to describe ARP is this: A device needs to know what IP addresses and MAC addresses are associated with each other. If the device already knows, then no problem. If the IP address is not found in the ARP table (a record of the devices' IP and MAC addresses) the device will send out a broadcast message. This broadcast message is sent to a special IP address for that network which allows all devices on that network to receive it. The message reads something like this “who has IP address ….” and the device with that IP address should respond. In the response the MAC address for that device will be included in the packets. Here, ARP has *resolved* the address.

2. WHAT IS NEIGHBOR DISCOVERY

In IPv6 ARP is no longer used. It has been replaced by Neighbor Address Resolution. The function of Neighbor Discovery (ND) is for a host to learn the IPv6 addresses of its neighbors and that includes learning about other hosts and routers on the local network. Instead of broadcast messages, Ipv6 uses a multicast address and ICMPv6 messages for tracking and discovering other hosts. In order for ND to work, it uses five types of ICMPv6 messages; those are: Neighbor Advertisements, Neighbor Solicitation, Router Advertisement/Solicitation, Duplicate Address Detection, and Neighbor Unreachability Detection.

Neighbor Advertisement (NA) messages are sent every so often to inform of their presence and send their link-layer addresses to other hosts present on the same network. Neighbor Solicitation (NS) messages are sent so that link-layer addresses of specific neighbors can be found. NS is used to detect duplicate addresses, verify of neighbor reachability, and Layer 2/3 address resolution. Router Advertisement (RA) messages are sent for every interface as soon as it's configured. In order to inform hosts about prefixes and also to inform that the router is available as a default gateway, RA messages are sent. In Router Solicitation (RS) routers will send RS messages to all multicast address. This occurs without waiting for RA messages.

Duplicate Address Detection (DAD) is a neighbor solicitation function. When the **autoconfiguration** is performed the host does not automatically know the address is unique. This could lead to duplicate addresses. The way DAD works is that the host will join the *all nodes multicast address* and *solicited-node multicast address* of the address being checked for uniqueness. The host will send NS messages to the solicited-node address. The address field will be undefined with unspecified address “::”. The address being checked is inside the Target Address field. If the host receives any NA responses, it means the address being checked is not unique. In Neighbor Unreachability Detection there are two ways to confirm reachability: a host will send a query to the targeted host's solicited-node multicast address then it is responded with an NA or an

RA; when a host is interacting with the targeted host it gets a hint (TCP ACK is one form) from a higher-layer protocol that two-way communication is functioning correctly.

3. WHAT MAKES ARP DIFFERENT FROM NEIGHBOR DISCOVERY

- Router discovery is part of the base IPv6 protocol set.
- IPv6 hosts do not need to snoop the routing protocols to find a router. IPv4 uses ARP, ICMP router discovery, and ICMP redirect for router discovery.
- IPv6 router advertisements carry **link-local addresses**. No additional packet exchange is needed to resolve the router's link-local address.
- Router advertisements carry **site prefixes** for a link. A separate mechanism is not needed to configure the netmask, as is the case with IPv4.
- Router advertisements enable address autoconfiguration. Autoconfiguration is not implemented in IPv4.
- Neighbor Discovery enables IPv6 routers to advertise an **MTU** for hosts to use on the link. All nodes use the same MTU value on links that lack a well-defined MTU. IPv4 hosts on the same network might have different MTUs.
- IPv6 address resolution multicasts are spread over 4 billion (2^32) multicast addresses. Non-IPv6 machines should not be interrupted at all.
- IPv6 redirects contain the link-local address of the new first hop. Separate address resolution is not needed on receiving a redirect.
- Multiple site prefixes can be associated with the same IPv6 network. By default, hosts learn all local site prefixes from router advertisements. Routers can be configured to omit some or all prefixes from router advertisements. If it is omitted, hosts assume that destinations are on remote networks. Consequently, hosts send the traffic to routers. A router can then issue redirects.
- The recipient of an IPv6 redirect message assumes that the new next-hop is on the local network. In IPv4, a host ignores **redirect messages** that specify a next-hop that is not on the local network, according to the network mask. The IPv6 redirect mechanism is analogous to the XRedirect facility in IPv4.
- IPv6 neighbor unreachability detection improves packet delivery in the presence of failing routers, partially failing/**partitioned links**, and when nodes change link-local addresses. IPv4 has no corresponding method for neighbor unreachability detection.
- Neighbor Discovery detects half-link failures by using neighbor unreachability detection. Neighbor Discovery avoids sending traffic to neighbors when two-way connectivity is absent.
- By using link-local addresses to uniquely identify routers, IPv6 hosts can maintain the router associations. IPv4 does not have a comparable method for identifying routers.
- 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 ICMP redirect messages. IPv4 off-link nodes can also send router advertisement messages.

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

GLOSSARY

CIDR – Classless Inter-domain routing. CIDR notation is a slash at the end of the address that is followed by the prefix in bits.

Link-local Address – Allows machines to automatically have an IP address on a network if they haven't been manually configured or automatically configured by a special server on the network.

Site Prefix – The 48 bits of leftmost fields in an IPv6 address contain the site prefix. Prefix length is stated in CIDR notation.

Example: `2001:db8:3c4d:0015:0000:0000:1a2f:1a2b/48`

Autoconfiguration – Stateful: equivalent to DHCP || Stateless: host gains address via an interface automatically leasing an address and does not require the establishment of a server to delve out address space.

MTU – Maximum Transmission Unit

Redirect Messages – Informs a host to update its routing information (to send packets on an alternate route)

Partitioned Links – Breaking the natural subnet into smaller subnets to provide a complete representation of the address space within the network.

WORKS CITED

Lenzer, George H. “What is a Link Local Address.” *Server Fault*, 02 Mar 2010. Web. 02 Jun 2015.

n.p. “Comparison of Neighbor Discovery to ARP and Related IPv4 Protocols.” *Oracle*, n.d. Web. 02 Jun 2015.

n.p. “Internet Control Message Protocol.” *Wikipedia*, 17 May 2015. Web. 07 Jun 2015.

n.p. “IPv6 Address Space Management.” *Oracle*, n.d. Web. 07 June 2015.

n.p. “Prefixes in IPv6.” *Oracle*, n.d. Web. 07 Jun 2015.

n.p. “What is IPv6 Autoconfiguration.” *Opus*, n.d. Web. 07 Jun 2015.

Reifschneider, Sean. “Networking Basics: How ARP Works.” *Tummy*, 02 Mar 2013. Web. 07 Jun 2015.

Rouse, Margaret. “Maximum Transmission Unit.” *Search Networking*, n.d. Web. 03 Jun 2015.

Valter. “NDP - Neighbor Discovery Protocol.” *How Does Internet Work*, 31 Dec 2012. Web. 07 Jun 2015.