Address Resolution

📕 CCNA1v7 Module 9 Address Resolution
🧑‍🏫 Pedro Durán

MAC and IP. Destination on Same Network

There are 2 primary addresses assigned to a device on an Ethernet LAN:

- 💪 **Layer 2 physical address (the MAC address):** Used for NIC to NIC communications on the same Ethernet network.
- 🤖 **Layer 3 logical address (the IP address):** Used to send the packet from the source device to the destination device.

Same network

- Layer 2 addresses are used to deliver frames from one NIC to another NIC.
- If a destination IP address is on the same network, the destination MAC address will be that of the destination device.

MAC and IP. Destination on Remote Network

- When the destination IP address is on a remote network, **the destination MAC address is that of the default gateway**.

⚠️ **ARP (IPv4) or ICMPv6 (IPv6) is used to associate the IP address of a device with the MAC address of the device NIC.**

A device uses ARP to determine the destination MAC address of a local device when it knows its IPv4 address.

ARP provides 2 basic functions:

- 1️⃣ Resolving IPv4 addresses to MAC addresses
- 2️⃣ Maintaining an ARP table of IPv4 to MAC address mappings

ARP Functions

To send a frame, a device will search its **ARP table for a destination IPv4 address and a corresponding MAC address**.

- 🤔 **Destination IP address on the same network?** ➡️ device will search the ARP table for the **destination IP address**.
- 🤔 **Destination IPv4 address on a different network?** ➡️ device will search the ARP table for the **IP address of the default gateway**.

🤔 **Device locates the IP address?** ➡️ its corresponding MAC address is used as the destination MAC address in the frame.
🤔 **There is no ARP table entry found?** ➡️ Device sends an **ARP request**.

Removing Entries from an ARP Table

Entries in the ARP table are not permanent and **are removed when an ARP cache timer expires after a specified period of time**. The duration of the ARP cache timer differs depending on the operating system.

- 🪟 Windows:
  - Show ARP Table ➡️ `arp -a`
  - Remove ARP Table ➡️ `arp -d`
- 🐧 Linux:
  - Show ARP Table ➡️ `ip neigh`
  - Remove ARP Table ➡️ `sudo ip neigh flush all`
- 🦜 Cisco:
  - Show ARP Table ➡️ `show ip arp`
  - Remove ARP Table ➡️ `clear ip arp`

ARP Issues – ARP Broadcasting and ARP Spoofing

ARP requests are received and processed **by every device on the local network.**

- ⛈️ Excessive ARP broadcasts can cause some **reduction in performance**.
- 🤡 **ARP replies can be spoofed** by a threat actor to perform an ARP poisoning attack. Enterprise level switches include mitigation techniques to protect against ARP attacks (DAI: Dynamic ARP Inspection).

IPv6 Neighbor Discovery Messages

IPv6 Neighbor Discovery (ND) protocol provides:

- **Address resolution:** ICMPv6 Neighbor Solicitation (NS) and Neighbor Advertisement (NA)
- **Router discovery:** ICMPv6 Router Solicitation (RS) and Router Advertisement (RA)
- **Redirection services:** ICMPv6 redirect messages

ICMPv6 devices use ND to resolve the MAC address of a known IPv6 address.

ICMPv6 Neighbor Solicitation messages are sent using special Ethernet and IPv6 multicast addresses.

📝 9.3.5 + 9.4.2