ARP (Address Resolution Protocol)

ARP (Address Resolution Protocol) is **a network protocol used to map an IP address to a physical MAC (Media Access Control) address on a local area network (LAN)**. ARP is essential in enabling communication between devices on the same network segment because devices need to know each other's MAC addresses to transmit data using Ethernet.

How ARP Works

When a device wants to communicate with another device **on the same local network** (for example, sending a packet from one computer to another), it must know the **MAC address of the destination device**. **ARP is used to resolve the IP address into the corresponding MAC address**.

ARP Process:

1. **ARP Request**

- The device (let's call it Device A) that wants to send data knows the target's IP address (let's say Device B), but not its MAC address.
- Device A sends out a broadcast ARP request to the entire network, asking, "Who has IP address 192.168.1.10?" (where 192.168.1.10 is the IP of Device B).

2. **ARP Response**

- **Every device** on the network receives the ARP request, but **only Device B, which has the IP address 192.168.1.10, responds**.
- Device B sends **an unicast ARP reply back to Device A, saying, "I am 192.168.1.10, and my MAC address is xx:xx:xx:xx:xx:xx."**

3. **Caching the Information**

- Device A now knows the MAC address of Device B and **stores this information in its ARP cache** to avoid sending future ARP requests for the same IP address.
- Device A can now send Ethernet frames to Device B using its MAC address.

Example of ARP

Assume Device A (192.168.1.1) wants to send data to Device B (192.168.1.2) on the same LAN.

- Device A sends an ARP request

```
Who has 192.168.1.2? Tell 192.168.1.1
```

- Device B responds with its MAC address

```
192.168.1.2 is at 00:1A:2B:3C:4D:5E
```

- Device A now knows that to communicate with 192.168.1.2, it should send packets to MAC address 00:1A:2B:3C:4D:5E.

Types of ARP

1. **ARP Request**: Sent by a device to discover the MAC address corresponding to an IP address.
2. **ARP Reply**: Sent by the device that has the requested IP address, containing its MAC address.
3. **Gratuitous ARP**: A device sends an ARP request for its own IP address, often used to update other devices' ARP caches without them having to ask. It's also used during IP address changes or network interface resets.
4. **Reverse ARP (RARP)**: Used to map a MAC address to an IP address, commonly used in older networks where **devices needed to discover their IP address upon booting**.

ARP Cache

- ARP maintains a cache **on each device**, which stores recently resolved IP-to-MAC address mappings. This reduces the need to repeatedly send ARP requests for frequently accessed devices.
- Entries in the ARP cache have a timeout period after which they are discarded, requiring the device to send another ARP request if the mapping is needed again.

ARP Vulnerabilities

While ARP is a simple and essential protocol, it **has several vulnerabilities**, making it a target for certain types of attacks, especially in unprotected LAN environments.

1. **ARP Spoofing/Poisoning**

- ARP Spoofing is an attack where **a malicious device sends fake ARP responses on the network, associating its MAC address with the IP address of another device (such as the default gateway or another host)**.
- Once successful, **the attacker can intercept, modify, or stop data intended for the legitimate device**. This can lead to **Man-in-the-Middle (MITM) attacks or Denial of Service (DoS) attacks**.
- Example:
    - Attacker sends ARP responses claiming that their MAC address corresponds to the IP address of the default gateway.
    - All devices on the network update their ARP cache with this incorrect mapping, routing traffic through the attacker's device.

2. **Prevention of ARP Spoofing**:

- **Static ARP entries**: **Manually configuring ARP tables with fixed IP-to-MAC mappings** can help, though it's impractical in large networks.
- **Dynamic ARP Inspection (DAI)**: A security feature available on some switches that **inspects ARP packets and filters out malicious ARP traffic based on trusted IP-to-MAC bindings**.

Differences Between ARP in IPv4 and IPv6

In IPv4 networks, ARP is used to resolve IP addresses to MAC addresses. However, **in IPv6, ARP is replaced by Neighbor Discovery Protocol (NDP)**, which performs similar functions but with added

features such as better security and auto-configuration.

Summary

- ARP (Address Resolution Protocol) is a **key protocol used to map IP addresses to MAC addresses in IPv4 networks**, enabling devices to communicate over Ethernet.
- ARP Requests and Responses allow devices to discover each other's MAC addresses, while ARP Caches store this information to reduce traffic.
- ARP is vulnerable to attacks like ARP Spoofing, which can be mitigated by network security measures such as static ARP entries and Dynamic ARP Inspection.