MAC Addressing and Functionality of ARP & RARP

1. Introduction

In any modern digital network , whether it's a home Wi-Fi setup, an enterprise Ethernet backbone, or a hybrid of both, communication between devices doesn't begin at the IP level. It starts one layer below, at the data link layer, with a critical device identifier known as the **MAC (Media Access Control) address**. This is a hardware-based address and the first step in identifying and enabling devices to talk to each other on a local network segment.

Before IP packets can route across continents or even across subnets, the local delivery of frames depends on this MAC addresses. Every network interface card (NIC), whether in a laptop, router, or any IoT device, is assigned a unique MAC address, making it the digital fingerprint of a device on a local network. Without MAC addresses, even the most advanced routing protocols and IP-based communication would have no means of reaching the correct device at the physical level.

However, for this local identification to interact with the broader IP-based communication system, translation is required. This is where **ARP (Address Resolution Protocol)** comes into play, acting like a digital phonebook that maps IP addresses to MAC addresses within a local network.

RARP (Reverse Address Resolution Protocol) on the other hand works as the inverse function, allowing devices to discover their IP address based on their known MAC address, though it's now largely obsolete due to the rise of **DHCP(Dynamic Host Configuration Protocol)**.

2. Understanding MAC Addressing

A **MAC address**, also known as a physical address or hardware address, is a **unique identifier** assigned to a network interface controller (NIC) for communications at the **Data Link Layer (Layer 2)** of the OSI model.

- **Format**: MAC addresses are 48 bits (6 bytes) long.
- **Representation**: Typically written in hexadecimal notation: `00:1A:2B:3C:4D:5E` or `00-1A-2B-3C-4D-5E`.
- **Structure**:
  - **First 24 bits (3 bytes)**: Organizationally Unique Identifier (OUI), identifies the manufacturer.
  - **Last 24 bits**: Device-specific , assigned by the manufacturer.

Example: `FC:FB:FB:01:FA:21`

- FC:FB:FB → Apple, Inc. (OUI)
- 01:FA:21 → Device-specific identifier

Key Characteristics:

- **Burned-in** to the NIC by the manufacturer.
- Operates at Layer 2 of OSI.
- **Does not change**, unlike IP addresses.
- Used within local network segments.

3. Role of MAC Address in Networking

- **Determines source and destination at Layer 2 (Data Link Layer):**
  MAC addresses are used to uniquely identify the sender and receiver within the same local network.

- **Used by switches and bridges to forward frames:**
  These devices use MAC address tables to decide where to send Ethernet frames on a LAN.

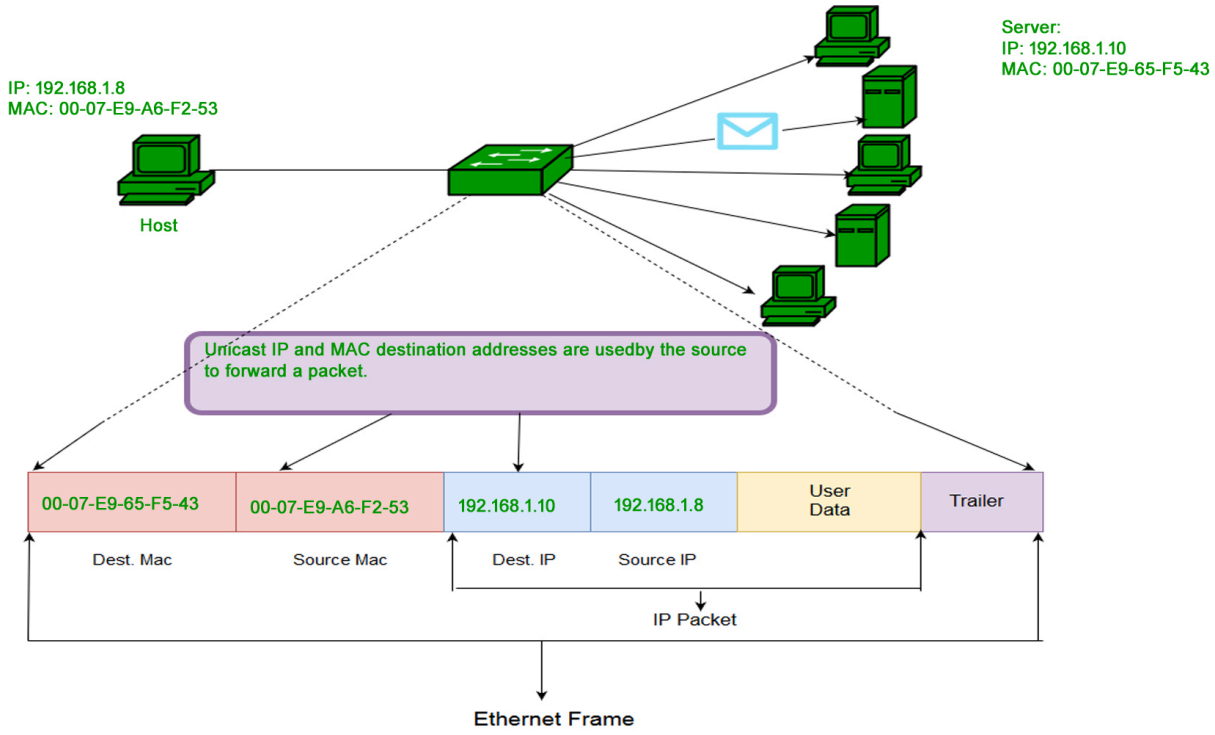
- **Crucial for Ethernet-based LANs:**
  Every device on an Ethernet network must have a MAC address to participate in communication.

- **Ensures accurate frame delivery:**
  Frames are delivered directly to a device based on its MAC not IP, making it vital for point-to-point communication.

- **Helps with collision detection and frame filtering:**
  Especially in older shared-medium Ethernet setups, MAC addresses assist in identifying and handling data collisions.

Why MAC when we have IP?

- IP addresses are logical and can change, MAC addresses are permanent and used for actual delivery inside a local network.
- Routing (IP) happens between networks; switching (MAC) happens within a network.



4. Address Resolution Protocol (ARP)

ARP is used to map **IPv4 addresses to MAC addresses** so devices on an Ethernet LAN can communicate.

How It Works:

1. Device A wants to send data to 192.168.1.10.
2. It checks its ARP table for a MAC corresponding to that IP.
3. If missing, it **broadcasts an ARP Request**: "Who has 192.168.1.10?"
4. The device with that IP replies with its MAC.
5. Device A updates its ARP cache and sends the data.

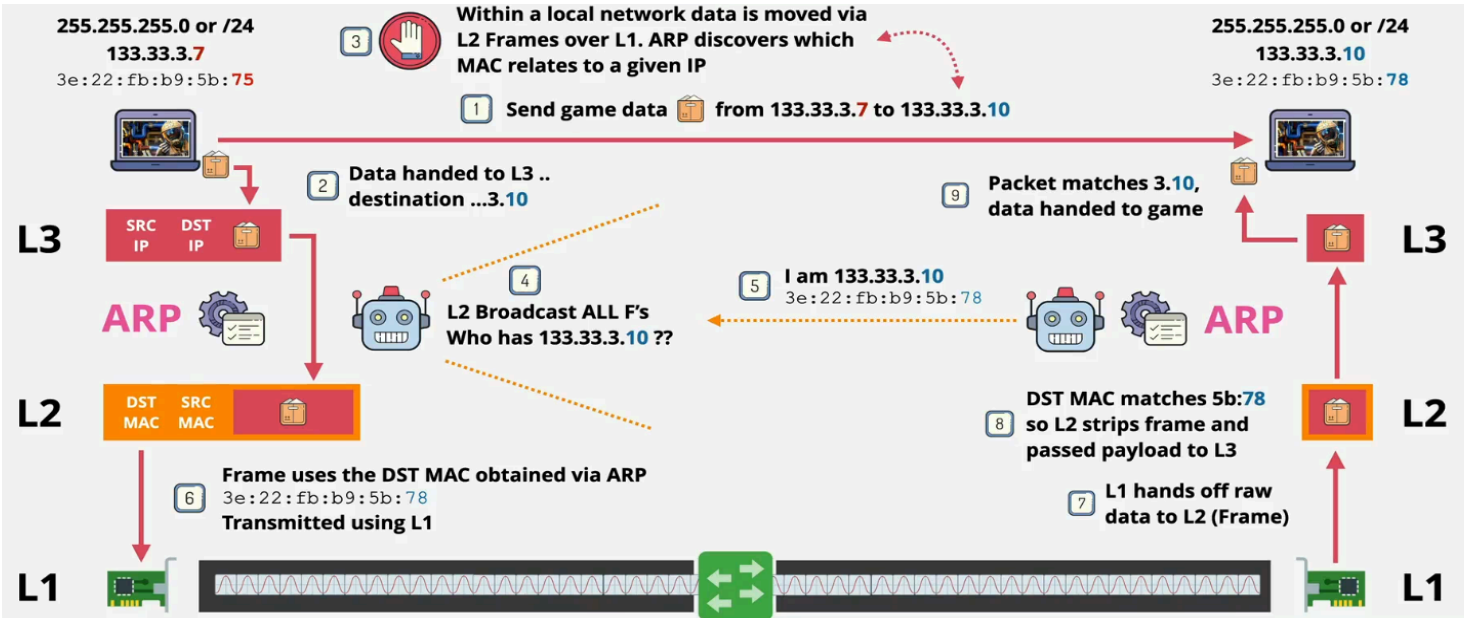
Types of ARP:

- **Request**: Broadcast to find MAC for a given IP.
- **Reply**: Unicast back to requester with MAC.

ARP Cache:

- Temporary table storing IP-to-MAC mappings.
- Prevents repeated ARP queries.

Security Note: ARP can be exploited via **ARP Spoofing** (MITM attacks). Solutions include dynamic ARP inspection and static ARP entries.



5. Reverse Address Resolution Protocol (RARP)

While ARP maps IP to MAC, **RARP** does the reverse: it allows a device to discover its **IP address given its MAC address**.

Why RARP was created:

- Early diskless workstations didn't store IPs.
- These systems could broadcast their MAC and ask for an IP.

How It Works:

1. Host sends a RARP Request with its MAC address.
2. RARP server replies with the corresponding IP address.

Limitations:

- Requires a dedicated RARP server.
- Only supports IP address resolution (no subnet mask, gateway, DNS).

Modern Replacement:

- **BOOTP** and **DHCP** have replaced RARP.
- These provide more configuration data (IP, subnet, DNS, gateway).

6. Real-world Use Case: ARP in Action

- Suppose Host A (192.168.1.5) wants to ping Host B (192.168.1.6)
- Host A looks into ARP table, no entry found
- Sends ARP Request: "Who has 192.168.1.6?"
- Host B replies with its MAC: `00:1B:44:11:3A:B7`
- A sends ICMP Echo (ping) to that MAC, thus communication successful