R&D Report on MAC Addressing, ARP & RARP

Understanding Layer 2 Communication and Address Resolution Protocols

Prepared by:
Virat Pandey

Celebal Technology
Cloud Infrastructure & Security Internship

Research & Development Document

June 15, 2025

Table of contents

1. Introduction

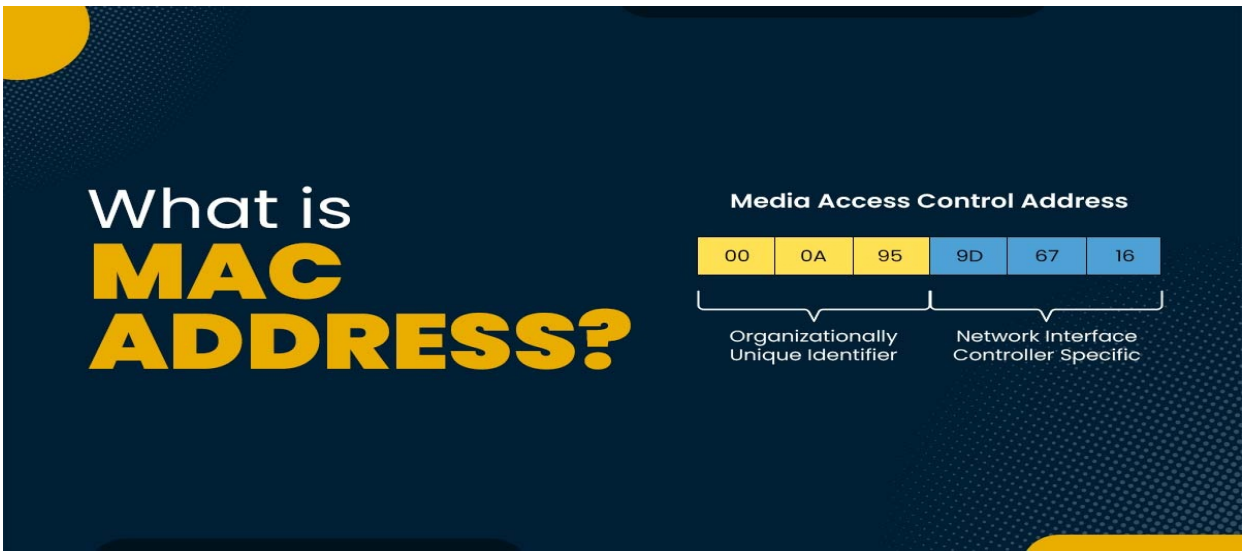
In any network, devices must communicate not just logically, using IP addresses, but also **physically**, over the underlying hardware. While IP addresses help in identifying a device's location in a network, **MAC (Media Access Control) addresses** serve as the unique hardware identifiers that enable **actual data transmission on a local link**.

To bridge the gap between logical (IP) and physical (MAC) addresses, protocols like **ARP (Address Resolution Protocol)** and **RARP (Reverse ARP)** come into play. These protocols help devices translate between **IP and MAC addresses**, ensuring smooth communication within local area networks (LANs).

Understanding MAC addressing and how ARP/RARP work is essential for:

- Diagnosing connectivity issues
- Securing local networks
- Configuring switches, firewalls, and routers
- Managing cloud infrastructure where Layer 2 communication affects virtual networking

This report explores the **basics of MAC addressing**, the **functionality of ARP and RARP**, and their role in enabling efficient data transmission at **Layer 2 of the OSI model**.



2. Basics of MAC Addressing

2.1 What is a MAC Address?

A **MAC (Media Access Control) address** is a **unique hardware identifier** assigned to a device's network interface card (NIC). It operates at **Layer 2 (Data Link Layer)** of the OSI model and is used to ensure that data is delivered to the correct device on a **local network (LAN)**.

Each device that connects to a network such as a computer, printer, router, or virtual machine has a MAC address embedded into its NIC by the manufacturer. This allows devices on the same local network to recognize and communicate with each other.

Think of a MAC address like a permanent serial number for your device's network interface.

2.2 MAC Address Format

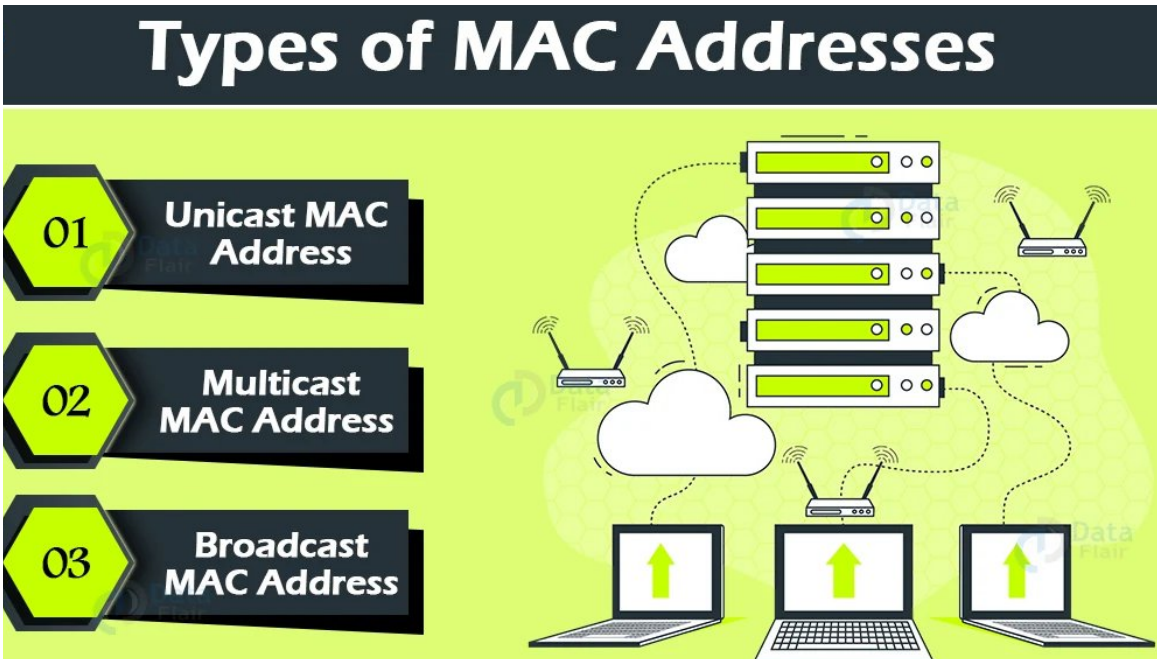
A MAC address is a **48-bit address**, usually displayed as **12 hexadecimal characters** grouped into six pairs:
Example: 00:1A:2B:3C:4D:5E

- Each pair represents **8 bits (1 byte)**
- The first 3 pairs (24 bits) identify the **manufacturer (OUI – Organizationally Unique Identifier)**
- The last 3 pairs are assigned uniquely to the device

2.3 MAC Address Characteristics and Types

- **Permanent:** Assigned by the hardware vendor, typically cannot be changed
- **Flat structure:** No hierarchy like IP addresses
- **Local scope:** Used only within the local network

- **Types:**
    - **Unicast MAC:** One-to-one communication (default)
    - **Broadcast MAC:** ff:ff:ff:ff:ff:ff – sent to all devices on LAN
    - **Multicast MAC:** Sent to a group of devices that "subscribe" to a multicast address



3. ARP – Address Resolution Protocol

3.1. Working of ARP (Address Resolution Protocol)

ARP is a network protocol used to **resolve IP addresses into MAC addresses** on a local area network (LAN). Since IP addresses operate at **Layer 3 (Network Layer)** and MAC addresses at **Layer 2 (Data Link Layer)**, ARP bridges the gap to allow successful data transmission over Ethernet.

Whenever a device on a LAN needs to communicate with another device, it **must know the MAC address** of the destination. If it only knows the IP address (which is typical), it uses ARP to find the corresponding MAC.

Detailed ARP Flow (Step-by-Step):

1. **Initiating Communication:**
   Host A wants to send data to Host B, but only knows Host B's IP (e.g., 192.168.1.10).
2. **ARP Request Broadcast:**
   Host A checks its ARP cache (a local table storing recent IP-to-MAC mappings). If there's no entry for 192.168.1.10, it broadcasts an **ARP Request** to all devices on the subnet:

"Who has IP address 192.168.1.10? Tell me your MAC address."

3. **ARP Reply (Unicast):**
   Host B (the target) receives the request, recognizes its IP, and replies with a **unicast ARP Reply**:

"I am 192.168.1.10, and my MAC address is 00:1A:2B:3C:4D:5E."

4. **Updating the ARP Cache:**
   Host A stores this mapping in its ARP cache for future use, typically with a timeout period (e.g., 2–20 minutes).

5. **Data Transmission Begins:**
   Now Host A can send the Ethernet frame directly to Host B using its MAC address.

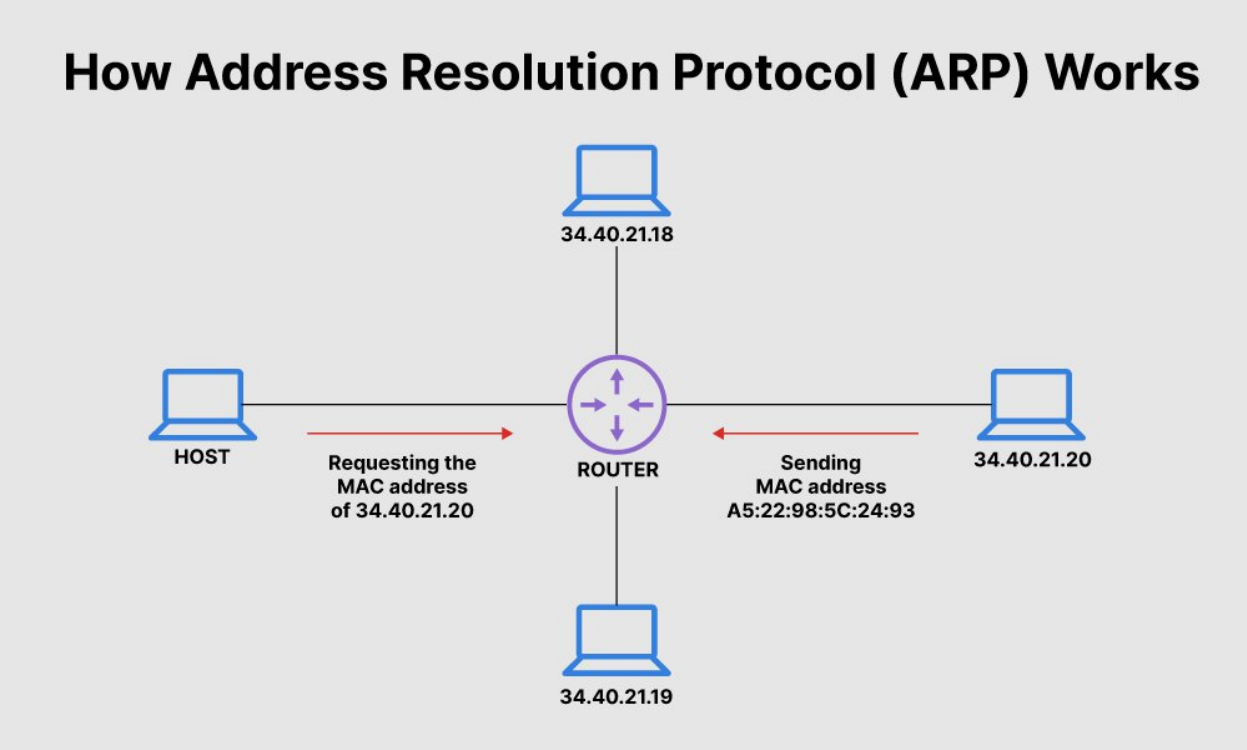
📌 **Key ARP Packet Details:**

- **ARP Request:**
  - Source MAC, Source IP
  - Target IP, Target MAC (set to 00:00:00:00:00:00)
- **ARP Reply:**
  - Fills in Target MAC with actual hardware address

3.2. Use Cases of ARP in Modern Networks

- **Basic LAN Communication:**
  Essential for communication within subnets, including PC-to-PC, VM-to-VM, and VM-to-router.
- **Switches and Routers:**
  Routers rely on ARP to send frames to correct next-hop MAC addresses.
- **Cloud Networking:**
  Virtual networks (like in Azure, AWS) simulate ARP behavior using internal routing logic or virtual routers.
- **Security Monitoring:**
  Tools like Wireshark use ARP to track communication; ARP spoofing is also a well-known vulnerability.
- **Efficiency:**
  ARP caches reduce broadcast traffic and improve network performance.

How Address Resolution Protocol (ARP) Works



Virtualization & Cloud Platforms

In cloud networks (Azure, AWS, etc.), ARP functionality is often simulated:

- Virtual routers use ARP-like logic to resolve MACs of VMs in the same subnet
- Tools like **Azure NSGs** or **AWS security groups** may indirectly depend on Layer 2 behaviors that mimic ARP for routing

4. RARP – Reverse Address Resolution Protocol

4.1 Working of RARP (Reverse ARP)

While **ARP** maps an **IP address to a MAC address**, **RARP (Reverse Address Resolution Protocol)** does the **opposite**: it allows a device to discover **its own IP address** when it only knows its **MAC address**.

RARP was primarily used in older systems and diskless devices (like early networked terminals) that lacked permanent storage to save their IP address. On boot, these devices would **broadcast a RARP request** on the network asking:

"This is my MAC address can someone tell me what IP address I should use?"

A specially configured **RARP server** on the network would respond with the correct IP address assigned to that MAC address.

🔁 **How RARP Works (Step-by-step):**

1. The diskless machine boots up and knows its MAC address (e.g., 00:11:22:33:44:55)
2. It sends a **RARP request broadcast** to the network
3. A RARP server looks up its table and responds:

"MAC 00:11:22:33:44:55 gets IP 192.168.1.25"

4. The machine now configures itself with the assigned IP

4.2 Limitations of RARP and Its Replacement

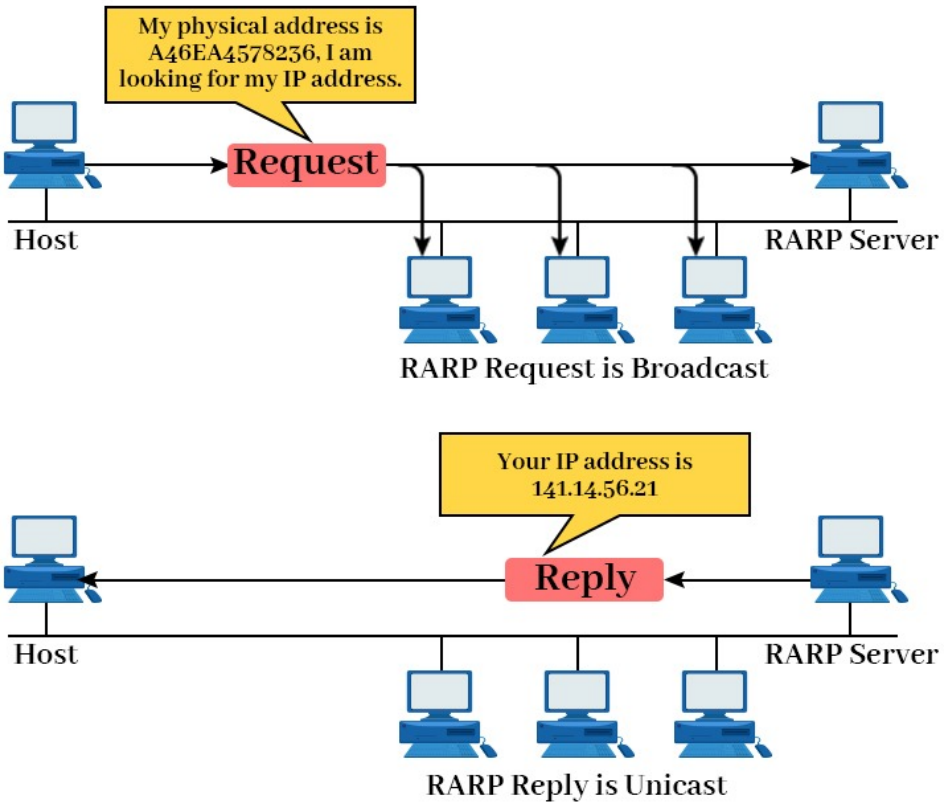
While RARP served its purpose during early networking days, it had several limitations:

Limitation	Explanation
Required a dedicated RARP server	Could not work without one on the network
Very limited functionality	Only resolved MAC-to-IP (no gateway, DNS

Limitation	Explanation
	info)
Not routable	Could not work across different networks
No support for dynamic address config	Static mapping only

Due to these limitations, RARP was eventually replaced by more advanced and flexible protocols:

- **BOOTP (Bootstrap Protocol):** Added gateway and DNS info
- **DHCP (Dynamic Host Configuration Protocol):** Became the modern standard for dynamic IP assignment and full configuration



5. Comparison: ARP vs RARP

Although both ARP and RARP are **address resolution protocols** used in early TCP/IP networks, they serve **opposite purposes** and operate in **different directions** of mapping between IP and MAC addresses.

Aspect	**ARP (Address Resolution Protocol)**	**RARP (Reverse Address Resolution Protocol)**
Function	Resolves IP address to MAC address	Resolves MAC address to IP address
Used By	Any device that knows an IP but needs MAC	Diskless devices that know their MAC but not IP
Direction	IP → MAC	MAC → IP
Network Layer	Operates at Layer 2, used by Layer 3	Operates at Layer 2, used by Layer 3
Request	Broadcas	Broadcast

Type	t	
Response Type	Unicast (direct reply from target host)	Unicast (from RARP server)
Modern Status	Still used widely in IPv4 networks	Obsolete — replaced by BOOTP and DHCP
Requires Server?	No (every device can reply)	Yes (requires a dedicated RARP server)
Use in Virtual Networks	Simulated in VM networks (e.g., cloud VNets)	Not used in cloud environments

6. Real-World Relevance in LANs and cloud Environments

Understanding **MAC addressing, ARP, and even RARP** is crucial not just from a theoretical standpoint, but also for solving real-world challenges in **enterprise networks, cloud platforms, and virtualized environments**.

- **MAC Addressing in Practice**

- **MAC addresses** are used every time two devices communicate on a LAN, whether it's PCs, routers, or virtual machines.
- **Network switches** use MAC addresses to build their internal forwarding tables (MAC address tables).
- **Firewalls and monitoring tools** may log or filter traffic based on MAC addresses for local device identification.

◆ **ARP in Real-World Networks**

- In local networks (both physical and virtual), **ARP enables IP-based communication** by resolving MAC addresses.
- **Routers use ARP** to determine the next-hop MAC when forwarding packets within a subnet.
- **ARP spoofing detection tools** (like Wireshark or arpwatch) are used by IT teams to spot malicious activity.
- In **cloud environments** like Azure and AWS, while traditional Ethernet ARP isn't always exposed, **virtual switches** still simulate ARP behavior for internal IP mapping between VMs.

◆ **Legacy Role of RARP**

- While RARP is no longer in use, understanding it helps explain the **evolution of IP configuration protocols**.
- RARP's foundational logic gave way to **BOOTP**, and ultimately to **DHCP**, which is now a standard in assigning IPs across physical and virtual networks.
- Concepts from RARP are embedded in **PXE booting**, where network devices boot using IP configuration from servers.

7. Conclusion

MAC addressing, ARP, and RARP are foundational elements of computer networking that operate silently behind every data transmission within a local network. While IP addresses allow logical communication across networks, it is the **MAC address** that ensures **physical delivery** of data at the hardware level.

The **Address Resolution Protocol (ARP)** remains a vital component in all modern IPv4-based networks, enabling devices to dynamically discover the MAC addresses of others on the same subnet. Without ARP, devices wouldn't be able to properly deliver Ethernet frames, making local communication impossible.

Although **RARP** is now obsolete, its role in early diskless systems helped shape the evolution of automated network configuration. Its core concept lives on in more advanced protocols like **DHCP**, which now manage dynamic IP assignments on a much larger and more flexible scale.

In enterprise and cloud environments, understanding these protocols enables professionals to:

- Design secure, efficient LANs
- Troubleshoot connectivity issues
- Protect against spoofing or impersonation attacks
- Build virtual networks that mimic real-world Layer 2 behavior

Mastering the flow between **IP and MAC**, and knowing how ARP fits in that chain, equips you with the knowledge to understand both the design and behavior of modern networks — whether on-premise, virtualized, or in the cloud.

8. References

1. ARP Command Reference (Microsoft Learn)
   Microsoft. *(2024)*. *arp – Windows Command Reference*
   learn.microsoft.com+10learn.microsoft.com+10learn.microsoft.com+10

2. ARP Caching Behavior (Microsoft Learn)
   Microsoft. *(2025)*. *Address Resolution Protocol caching behavior – Windows Server*
   learn.microsoft.com+12learn.microsoft.com+12learn.microsoft.com+12
3. Perform ARP Operations Programmatically (Microsoft Learn)
   Microsoft. *(2021)*. *Using the Address Resolution Protocol - Win32 apps*
   learn.microsoft.com+4learn.microsoft.com+4learn.microsoft.com+4
4. Azure ExpressRoute ARP Insights (Microsoft Learn)
   Microsoft Azure. *(2024)*. *Address Resolution Protocol (ARP) and ARP tables – ExpressRoute*
   learn.microsoft.com+15learn.microsoft.com+15learn.microsoft.com+15
5. SendARP Function in Windows (Microsoft Learn)
   Microsoft. *(2021)*. *SendARP function (iphlpapi.h) – Win32 apps*.
   learn.microsoft.com+11learn.microsoft.com+11learn.microsoft.com+11
6. MAC Address Definition (Microsoft Learn)
   Microsoft. *(2023)*. *PhysicalAddress Class – .NET Documentation*
   learn.microsoft.com+15learn.microsoft.com+15learn.microsoft.com+15