A R&D report
on

MAC Addressing, and Functionality of ARP & RARP

Submitted to **Celebal Technologies** in partial fulfilment of the internship task

Week 2

in

Cloud Infra and Security

By

Mr. Ganesh Ghadge

StudentId: CT_CSI_CI_6124

Objective

This document aims to provide a detailed understanding of MAC Addressing and the working of ARP (Address Resolution Protocol) and RARP (Reverse Address Resolution Protocol), focusing on their roles in network communication. By explaining how MAC addresses are used to uniquely identify devices on a network and how ARP and RARP facilitate communication between devices within a local network, this document will help individuals understand the core functionality of these essential network protocols.

The document's objectives are as follows:

- Describe the concept of MAC Addressing, including its structure, significance, and its role in network communication, particularly in Ethernet-based networks.
- Explain the function and working of ARP (Address Resolution Protocol), detailing how it maps IP addresses to MAC addresses and its importance in local area networks (LANs).
- Explain the function and working of RARP (Reverse Address Resolution Protocol), including how it maps MAC addresses to IP addresses, and its historical role in IP address assignment.
- Illustrate the differences between ARP and RARP, highlighting their use cases and relevance in modern networking environments.
- Provide practical examples of ARP and RARP in real-world network scenarios, helping individuals understand how these protocols support the efficient operation of networks.

Introduction

In the context of computer networking, there are two critical elements: MAC (Media Access Control) Addressing and ARP (Address Resolution Protocol). MAC Addressing is important for ensuring that data packets are sent from one device to another device on the Local Area Network (LAN) correctly. IP addressing is necessary when routing data from one network to another, or to send packets to the public Internet, but when data or packets are being routed to a specific device on the same network, they will need a MAC address to properly route to that specific hardware device. At the Data Link Layer, the device has to know how to send data to a specific piece of hardware on a local area network, and this uniqueness is satisfied with the uniqueness of the MAC addresses.

A **MAC Address** is a unique hardware identifier, defined to identify devices for communications on a network segment. Compared to the dynamic nature of IP addresses, where the addressing can change because of a change in the network configuration on the device or the device moves to another network, MAC Addresses are static in that they are physical address assigned to the device that identifies it and they are hard coded in the devices NIC.

ARP is a protocol where a device maps the IP address to the MAC address and allows devices to easily discover each other based on a shared IP address. The ARP protocol informs devices of each other's hardware addresses, allowing for the coordination of data routing within the LAN. RARP (Reverse Address Resolution Protocol), on the other hand, allows a device to find its IP address based on its MAC address. RARP was crucial to help diskless workstations find their IP address via a network.

MAC Addressing

A MAC Address (Media Access Control Address) is a unique numerical identity assigned to a network interface for communications on the physical network segment. A MAC address is used to identify devices in a local area network (LAN) like Ethernet, so it operates at the Data Link Layer of the OSI model. MAC addresses are very critical to guarantee that the data is delivered to the right device in a network. A MAC Address serves as a unique identifier, just like a postal address is unique to a house.

Structure of a MAC Address

A MAC address is typically represented as a 48-bit (6-byte) hexadecimal number, split into two parts:

- **OUI** (**Organizationally Unique Identifier**): The first 3 bytes (24 bits) of the MAC address identify the manufacturer of the network interface card (NIC). This part is assigned by the IEEE (Institute of Electrical and Electronics Engineers).
- **Device Identifier**: The remaining 3 bytes (24 bits) are used to uniquely identify the device produced by that manufacturer. This part is assigned by the manufacturer itself.

MAC address: 00:14:22:01:23:45

In this example:

- 00:14:22 is the OUI, identifying the manufacturer.
- 01:23:45 is the unique device identifier.

MAC Address Types

MAC addresses can be classified into three main types:

MAC Address Type	Description	Example	Address Format
Unicast MAC Address	A unique MAC address is assigned to a single network interface. Used for one-to-one communication.	A computer sends data to a printer.	Individual unique address (e.g., 00:14:22:01:23:45)
Broadcast MAC Address	A special MAC address is used to send data to all devices in the network segment.	A device requests to find other devices on the network.	FF:FF:FF:FF:FF:FF
Multicast MAC Address	Used to send data to a specific group of devices within a network. Common in media streaming.	Devices listening to a multicast IP stream.	A MAC address starting with a prefix (e.g., 01:00:5E:xx:xx:xx)

MAC Address Functions and Importance

MAC addresses are crucial for local network communication. Some key functions and reasons for their importance include:

- Device Identification: Every MAC address is unique to its device, ensuring accurate identification and communication within a network.
- Data Link Layer Communication: Operating at the Data Link Layer, MAC addresses allow devices within the same local network to communicate directly, providing the foundation for Ethernet-based networks.
- Stable Addressing: Unlike IP addresses that can change based on network configuration, MAC addresses are static and embedded into the device's hardware. This permanence ensures reliable communication even if the network setup changes.
- Facilitates ARP Communication: MAC addresses are essential for the Address Resolution Protocol (ARP), which maps an IP address to its corresponding MAC address, ensuring data is sent to the correct device on a local network.

Address Resolution Protocol & Reverse Address Resolution Protocol

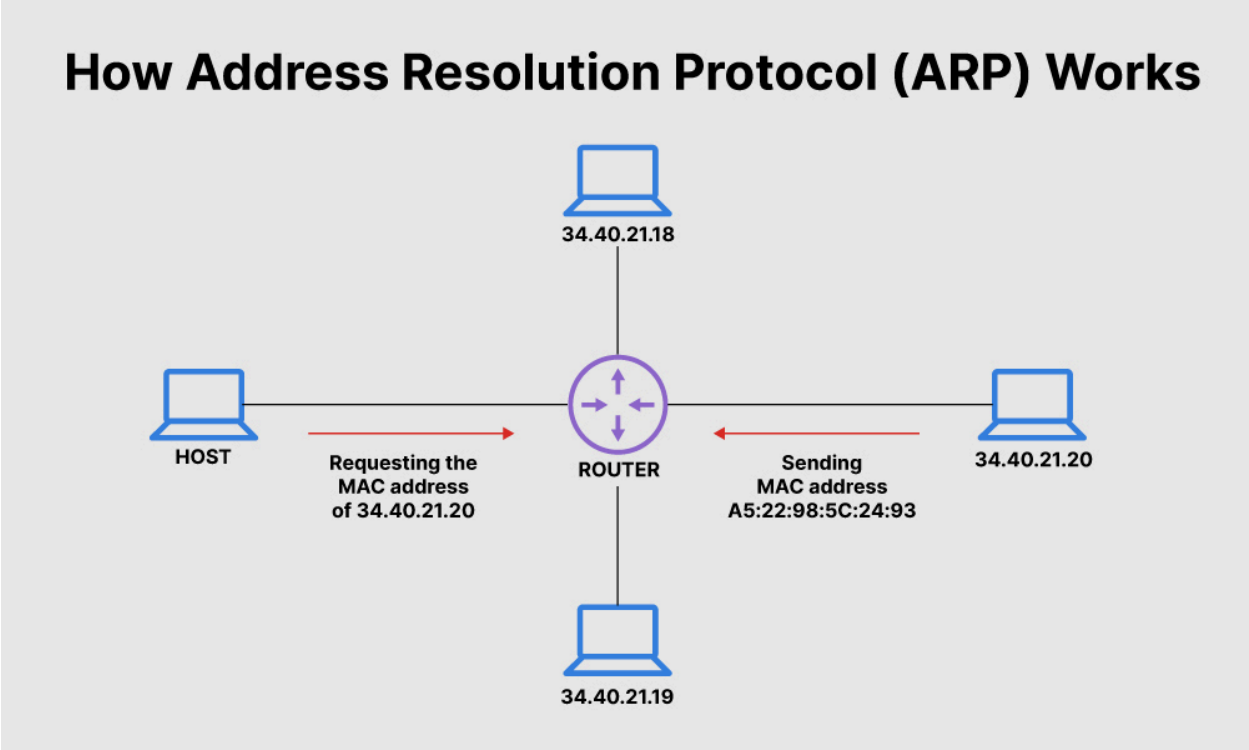
ARP (Address Resolution Protocol) and RARP (Reverse Address Resolution Protocol) are network protocols used for mapping IP addresses to MAC addresses as part of network communications across a local area network (LAN). ARP and RARP are needed to keep the network communications possible so that devices can discover one another and successfully transfer data.

1. **ARP (Address Resolution Protocol)**

ARP is a protocol to resolve an IP address (Layer 3 address) to a MAC address (Layer 2 address) on the local network. ARP allows a device to discover another device's physical address (MAC address) when it has only the IP address. This is possible because IP addresses are used to route data between networks, but a MAC address must be used to communicate on the same local network.

How ARP Works:

- When a device (say, Device A) needs to communicate with another device (Device B) on the same network, it must first know the MAC address of Device B.
- Device A checks its local ARP cache to see if it has a record of the MAC address associated with Device B's IP address.
    - If found, Device A sends the data directly.
    - If not found, Device A sends an ARP request to the network.
- The ARP request is a broadcast message sent to all devices on the local network asking: "Who has IP address X? Please send your MAC address."
- The device that owns the IP address responds with an ARP reply, providing its MAC address.
- Device A stores this mapping in its ARP cache for future use and sends the data to Device B using the discovered MAC address.

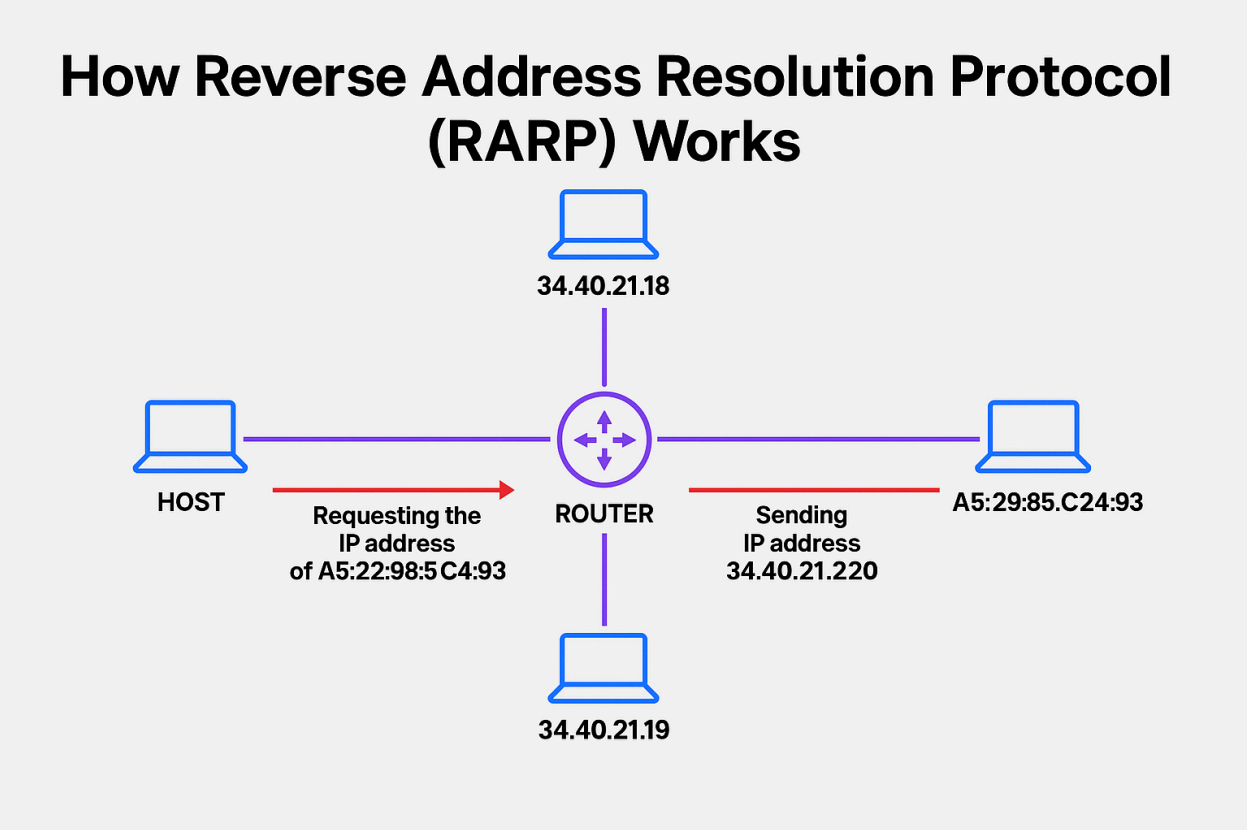


2. **RARP (Reverse Address Resolution Protocol)**

RARP functions in an inverse manner to ARP. It provides a mapping from MAC to IP, so a device requesting an IP address can ascertain its address from its MAC address. RARP is used in situations where there is no direct mapping to an IP address, but a device can provide its MAC address to be assigned an IP address.

How RARP works:

- A device (such as a diskless workstation) that doesn't have an IP address broadcasts a RARP request to the network with its MAC address
- A **RARP server** (typically a router or a dedicated server) listens for RARP requests. When it receives a request, it looks up the MAC address in its database and sends back the corresponding IP address
- The requesting device then uses the assigned IP address to communicate with other devices on the network.



Differences between ARP and RARP :

Feature	ARP	RARP
Direction	Maps IP to the MAC address	Maps MAC to IP address
Use Case	Used by devices to discover the MAC address for a known IP address	Used by devices to discover IP address for a known MAC address
Typical Devices	Computers, routers, and networked devices	Diskless workstations, network booting devices
Protocol Layer	Data Link Layer (Layer 2) & Network Layer (Layer 3)	Data Link Layer (Layer 2) & Network Layer (Layer 3)
Cache Storage	Stores mappings in an ARP cache	Stores mappings in a RARP server
Protocol Type	Broadcast request, unicast reply	Broadcast request, unicast reply

References

1. Cisco- IP Addresses and Unique Subnets for New Users : https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-0/addr_serv/command/reference/ir40asrbook_chapter2.html
2. GeeksforGeeks – ARP and RARP: https://www.geeksforgeeks.org/computer-networks/arp-reverse-arprarp-inverse-arp-inarp-proxy-arp-and-gratuitous-arp/