Prepared by: Nandini Goyal
Intern at Celebal Technologies
Department: Cloud Infra & Security
Date: 13 June 2025

R&D Document

Basics of MAC Addressing and Functionality of ARP & RARP

Table of Contents

1. Introduction

MAC addressing, ARP (Address Resolution Protocol), and RARP (Reverse Address Resolution Protocol) are foundational components of computer networking, operating primarily at the Data Link Layer (Layer 2) and interfacing with the Network Layer (Layer 3). MAC addresses provide unique device identification within a network, while ARP and RARP facilitate the mapping between IP and MAC addresses for communication. This document explores the structure and role of MAC addresses, the functionality of ARP and its variants (e.g., Proxy ARP, Gratuitous ARP), the historical significance of RARP, and their replacements like DHCP and NDP (for IPv6). It includes practical examples, comparison tables, and real-world applications to provide a comprehensive understanding for network design and troubleshooting.

2. MAC Addressing

2.1 Definition

A MAC (Media Access Control) address is a unique 48-bit identifier assigned to a network interface card (NIC) or other network-capable device. It operates at the Data Link Layer (Layer 2) of the OSI model to enable communication within a local network.

2.2 Characteristics

- **Uniqueness:** MAC addresses are globally unique, assigned by the device manufacturer under IEEE guidelines.
- **Layer 2 Operation:** Used for local network communication (e.g., Ethernet, Wi-Fi) to identify source and destination devices.
- **Static Nature:** Typically hard-coded into the NIC, though some devices allow software-based MAC address changes (spoofing).
- **Scope:** MAC addresses are only relevant within a local network segment and are not routable across networks.

2.3 Structure and Format

- **Length:** 48 bits (6 bytes), represented as 12 hexadecimal digits.
- **Format:** Expressed as six pairs of hexadecimal digits separated by colons or hyphens (e.g., 00:1A:2B:3C:4D:5E or 00-1A-2B-3C-4D-5E).
- **Components:**

- **OUI (Organisationally Unique Identifier):** First 24 bits (3 bytes), assigned by IEEE to the manufacturer (e.g., 00:1A:2B might identify Cisco).
- **Device-Specific Portion:** Last 24 bits (3 bytes), assigned by the manufacturer to uniquely identify the device.

- **Example:** In 00:1A:2B:3C:4D:5E, 00:1A:2B is the OUI, and 3C:4D:5E is the device identifier.

2.4 Types of MAC Addresses

- **Unicast:** Targets a single device (first bit of first byte is 0, e.g., 00:1A:2B:3C:4D:5E).
- **Multicast:** Targets a group of devices (first bit of first byte is 1, e.g., 01:00:5E:xx:xx:xx for IPv4 multicast).
- **Broadcast**: Targets all devices in the network (all bits set to 1, e.g., FF:FF:FF:FF:FF:FF).

3. ARP (Address Resolution Protocol)

3.1 Purpose

ARP maps an IPv4 address (Layer 3) to a MAC address (Layer 2) within a local network, enabling devices to communicate over Ethernet or similar protocols.

3.2 Functionality

- **Process:**
  1. A device (e.g., Device A) needs to send data to an IP address (e.g., 192.168.1.5).
  2. Device A checks its ARP cache (table) for the corresponding MAC address.
  3. If not found, Device A broadcasts an ARP Request to the network, asking, "Who has IP 192.168.1.5?"
  4. The device with that IP (Device B) responds with an ARP Reply containing its MAC address.
  5. Device A updates its ARP cache and uses the MAC address to send the data.
- **ARP Cache:** Stores IP-to-MAC mappings temporarily to reduce network traffic. Entries expire after a set time (e.g., 5–20 minutes, depending on the system).

3.3 ARP Packet Structure

An ARP packet includes:

- **Hardware Type:** Specifies the network type (e.g., Ethernet = 1).
- **Protocol Type:** Specifies the protocol (e.g., IPv4 = 0x0800).
- **Operation Code:** Indicates Request (1) or Reply (2).

- **Sender/Target Addresses:** Includes sender and target IP and MAC addresses.

3.4 Types of ARP

Type	Description
Standard ARP	Maps an IP address to a MAC address within a local network.
Proxy ARP	A router responds to an ARP request on behalf of a device in a different subnet, facilitating communication across subnets without changing device configurations.
Gratuitous ARP	A device sends an unsolicited ARP request for its own IP to detect IP conflicts or update other devices' ARP caches (e.g., during failover in high-availability systems).
Inverse ARP (InARP)	Used in Frame Relay/ATM networks to map a known MAC address to an IP address.

3.5 Practical Example

Scenario: Device A (192.168.1.10) wants to ping Device B (192.168.1.5).

1. Device A checks its ARP cache for 192.168.1.5's MAC address.
2. If absent, Device A broadcasts an ARP Request: "Who has 192.168.1.5?"
3. Device B responds with its MAC address (e.g., 00:1A:2B:3C:4D:5E).
4. Device A updates its ARP cache and sends the ping packet to Device B's MAC address.

4. RARP (Reverse Address Resolution Protocol)

4.1 Purpose

RARP enables a device (typically diskless workstations or thin clients) to discover its own IP address using its known MAC address.

4.2 Functionality

- **Process:**
  1. A device broadcasts a RARP request containing its MAC address.
  2. A RARP server (preconfigured with MAC-to-IP mappings) responds with the device's IP address.
  3. The device configures its network interface with the received IP.

- **Use Case:** Common in the 1980s for diskless workstations or embedded systems that lacked storage to maintain IP configurations.

4.3 Limitations and Obsolescence

- **Limitations:**
  - Requires a dedicated RARP server with static MAC-to-IP mappings, which is unscalable.
  - Limited to local network segments (non-routable).
  - Supports only IPv4 and lacks advanced features.
- **Obsolescence:** Replaced by BOOTP (Bootstrap Protocol) and DHCP (Dynamic Host Configuration Protocol), which offer dynamic IP assignment and additional configuration options (e.g., gateway, DNS).

5. Comparison Table: ARP vs RARP

Feature	ARP	RARP
Purpose	Maps IP to MAC address	Maps MAC to IP address
Direction	Forward resolution	Reverse resolution
Used By	All hosts and routers	Diskless workstations
Operation	Broadcast request, unicast reply	Broadcast request, unicast reply
Protocol Layer	Data Link/Network Layer	Data Link/Network Layer
Current Usage	Widely used in IPv4 networks	Obsolete, replaced by DHCP/ BOOTP
Scalability	Highly scalable (dynamic cache)	Poor (requires static server mappings)
RFC	RFC 826	RFC 903

6. Related Protocols and Concepts

6.1 BOOTP and DHCP

- **BOOTP:** Replaced RARP by providing dynamic IP address assignment and additional configuration (e.g., gateway, boot file). Still used in some legacy systems.
- **DHCP:** Extends BOOTP with features like lease times, automatic IP allocation, and support for larger networks. DHCP is the modern standard for IP address assignment.
-

6.2 NDP (Neighbor Discovery Protocol) in IPv6

- **Purpose:** Replaces ARP in IPv6 networks, as ARP is not compatible with IPv6's 128-bit addresses.
- **Functionality:**
  - Uses ICMPv6 messages for neighbor discovery, address resolution, and router discovery.
  - Operates via multicast (e.g., Neighbor Solicitation and Advertisement) instead of broadcasts.
  - **Example:** A device sends a Neighbor Solicitation to resolve an IPv6 address to a MAC address.
- **Advantages:** More efficient, supports IPv6 features like Stateless Address Autoconfiguration (SLAAC).

7. Real-World Applications

- **Network Troubleshooting:** ARP cache inspection (e.g., arp -a command) helps diagnose connectivity issues or IP conflicts.
- **Security:** ARP spoofing (poisoning) attacks manipulate ARP tables to intercept traffic. Mitigation includes static ARP entries or ARP monitoring tools.
- **High Availability:** Gratuitous ARP is used in failover scenarios (e.g., VRRP, HSRP) to update network devices with new MAC addresses for virtual IPs.
- **IoT and Embedded Systems:** Legacy systems may still use RARP-like mechanisms, though DHCP is preferred for modern IoT devices.
- **IPv6 Transition:** Understanding ARP is critical for IPv4 networks, while NDP knowledge is essential for IPv6 adoption in modern enterprises.

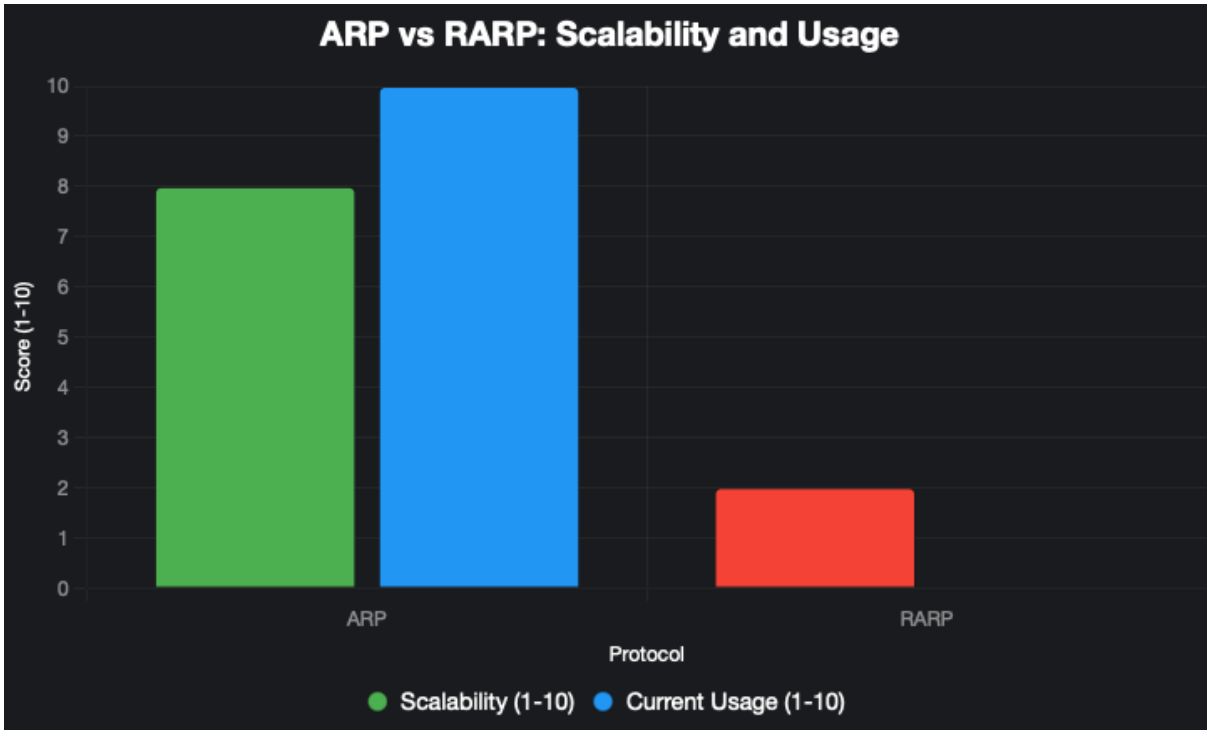
8. Best Practices

- **Monitor ARP Traffic:** Use tools like Wireshark to detect unusual ARP activity (e.g., spoofing attempts).
- **Secure ARP:** Implement static ARP entries or Dynamic ARP Inspection (DAI) on switches to prevent ARP spoofing.
- **Clear ARP Cache:** Periodically clear stale ARP entries to avoid communication issues (e.g., arp -d on Windows or ip -s -s neigh flush all on Linux).
- **Transition to IPv6:** Adopt NDP for IPv6 networks to leverage its efficiency and security features.

- **Document MAC Assignments:** Maintain a record of MAC-to-device mappings for troubleshooting and inventory management.

9. Visualizing ARP vs. RARP

To illustrate the differences between ARP and RARP, the following chart compares their key functionalities. (Confirm with your supervisor if a visual chart is desired for inclusion in the document.)



This chart highlights ARP's high scalability and continued relevance compared to RARP's obsolescence and limited scalability.

10. Conclusion

MAC addressing provides the foundation for device identification at the Data Link Layer, while ARP and RARP historically facilitated IP-to-MAC and MAC-to-IP mappings, respectively. ARP remains critical for IPv4 networks, with variants like Proxy ARP and Gratuitous ARP supporting advanced networking scenarios. RARP, though obsolete, laid the groundwork for modern protocols like DHCP. Understanding these concepts, along with their replacements (e.g., DHCP, NDP), is essential for network configuration, troubleshooting, and

transitioning to IPv6. This document equips network administrators with the knowledge to manage Layer 2 and Layer 3 interactions effectively.

11. References

- GeeksforGeeks: https://www.geeksforgeeks.org/computer-networks/arp-reverse-arprarp-inverse-arp-inarp-proxy-arp-and-gratuitous-arp/
- Cisco Networking Academy: https://www.cisco.com/c/en/us/support/docs/ip/address-resolution-protocol-arp/13718-5.html
- IETF RFC 826: https://tools.ietf.org/html/rfc826
- IETF RFC 903: https://tools.ietf.org/html/rfc903
- IETF RFC 4861: https://tools.ietf.org/html/rfc4861
- IEEE 802.3 Standards: https://standards.ieee.org/products-services/regauth/oui/