Prepare R&D Document on Basics of MAC Addressing and Functionality of ARP & RARP

Rudra Kadel

June 15, 2025

1. Introduction to MAC Addressing

In the realm of computer networking, devices need unique identifiers to communicate within a local network segment. This is where **MAC (Media Access Control) addresses** come into play. Unlike IP addresses, which are logical and can change depending on the network, MAC addresses are physical addresses that are typically hard-coded onto a network interface card (NIC) by the manufacturer. They are crucial for communication at the Data Link Layer (Layer 2) of the OSI model.

Think of a MAC address as the unique serial number of your network card. Just as each car has a unique Vehicle Identification Number (VIN), each network-enabled device has a distinct MAC address. This ensures that data frames transmitted within a local area network (LAN) can be delivered to the correct physical destination.

2. Structure and Types of a MAC Address

A MAC address is a 48-bit (6-byte) hexadecimal address, usually represented in one of the following formats:

- ‘MM:MM:MM:SS:SS:SS‘ (colon-separated)
- ‘MM-MM-MM-SS-SS-SS‘ (hyphen-separated)
- ‘MMM.MMM.SSS.SSS‘ (dot-separated, less common in general use, but found in some systems like Cisco)

Here, the first 24 bits (the first three octets, e.g., MM:MM:MM) represent the **Organizationally Unique Identifier (OUI)**, which identifies the manufacturer of the NIC. The last 24 bits (the last three octets, e.g., SS:SS:SS) are a serial number assigned by the manufacturer, ensuring the uniqueness of the MAC address within that manufacturer’s assigned OUI block.

2.1. OUI (Organizationally Unique Identifier)

The OUI is assigned by the Institute of Electrical and Electronics Engineers (IEEE). By looking up the OUI portion of a MAC address, one can determine the vendor of the network interface. This can be useful for inventory management, troubleshooting, and network security investigations.

2.2. Uniqueness and Address Types

The structure of MAC addresses, with the globally managed OUI and the manufacturer-assigned serial number, aims to guarantee the global uniqueness of every MAC address. This uniqueness is crucial for the proper functioning of Ethernet and other LAN technologies. However, it's possible for MAC addresses to be manually changed or "spoofed" in software, which has both legitimate (e.g., bypassing network restrictions, testing) and malicious (e.g., impersonation, evading detection) uses.

MAC addresses can be classified into different types based on their usage in a network:

- **Unicast MAC Address:** This is the most common type, assigned to a single, specific network interface. Data frames sent to a unicast MAC address are intended for and processed by only that specific device. The least significant bit of the first octet is '0' for unicast addresses (e.g., '00:1A:2B:3C:4D:5E').
- **Multicast MAC Address:** These addresses are used to send a single data frame to a specific group of devices on the network. Devices interested in receiving data for a particular multicast group will configure their NICs to listen for that multicast MAC address. The least significant bit of the first octet is '1' for multicast addresses (e.g., '01:00:5E:00:00:01' for IPv4 multicast, '33:33:00:00:00:01' for IPv6 multicast).
- **Broadcast MAC Address:** This is a special MAC address ('FF:FF:FF:FF:FF:FF') used to send a data frame to all devices within the same local network segment. All devices on the segment will receive and process frames addressed to the broadcast MAC address. Broadcasts are essential for many network discovery protocols.

2.3. Locally Administered vs. Universally Administered MAC Addresses

MAC addresses can also be categorized by how they are assigned:

- **Universally Administered Address (UAA):** This is the MAC address hard-coded into the NIC by the manufacturer. It's designed to be globally unique. The second least significant bit of the first octet is '0'.
- **Locally Administered Address (LAA):** This is a MAC address that can be manually configured by a network administrator or software. It overrides the burned-in UAA. The second least significant bit of the first octet is '1'. LAAs are used in scenarios like MAC address spoofing, virtual machine MAC assignment, or in some clustered environments.

3. MAC Address Tables (CAM Tables) on Switches

Network switches play a crucial role in forwarding Ethernet frames based on MAC addresses. They maintain a **MAC address table**, also known as a **Content Addressable Memory (CAM) table**.

- **Learning:** When a switch receives a frame, it inspects the source MAC address. If the MAC address is not in its table, or if it's on a different port than recorded, the switch adds (or updates) the MAC address and the port it was learned on to its CAM table.

- **Forwarding:** When a switch receives a frame with a destination MAC address, it looks up that address in its CAM table. If a match is found, the switch forwards the frame only out the specific port associated with that MAC address, minimizing unnecessary traffic.
- **Flooding:** If the destination MAC address is a broadcast address (‘FF:FF:FF:FF:FF:FF‘) or if the destination MAC address is not found in the CAM table (an "unknown unicast"), the switch will flood the frame out of all ports except the one it was received on.

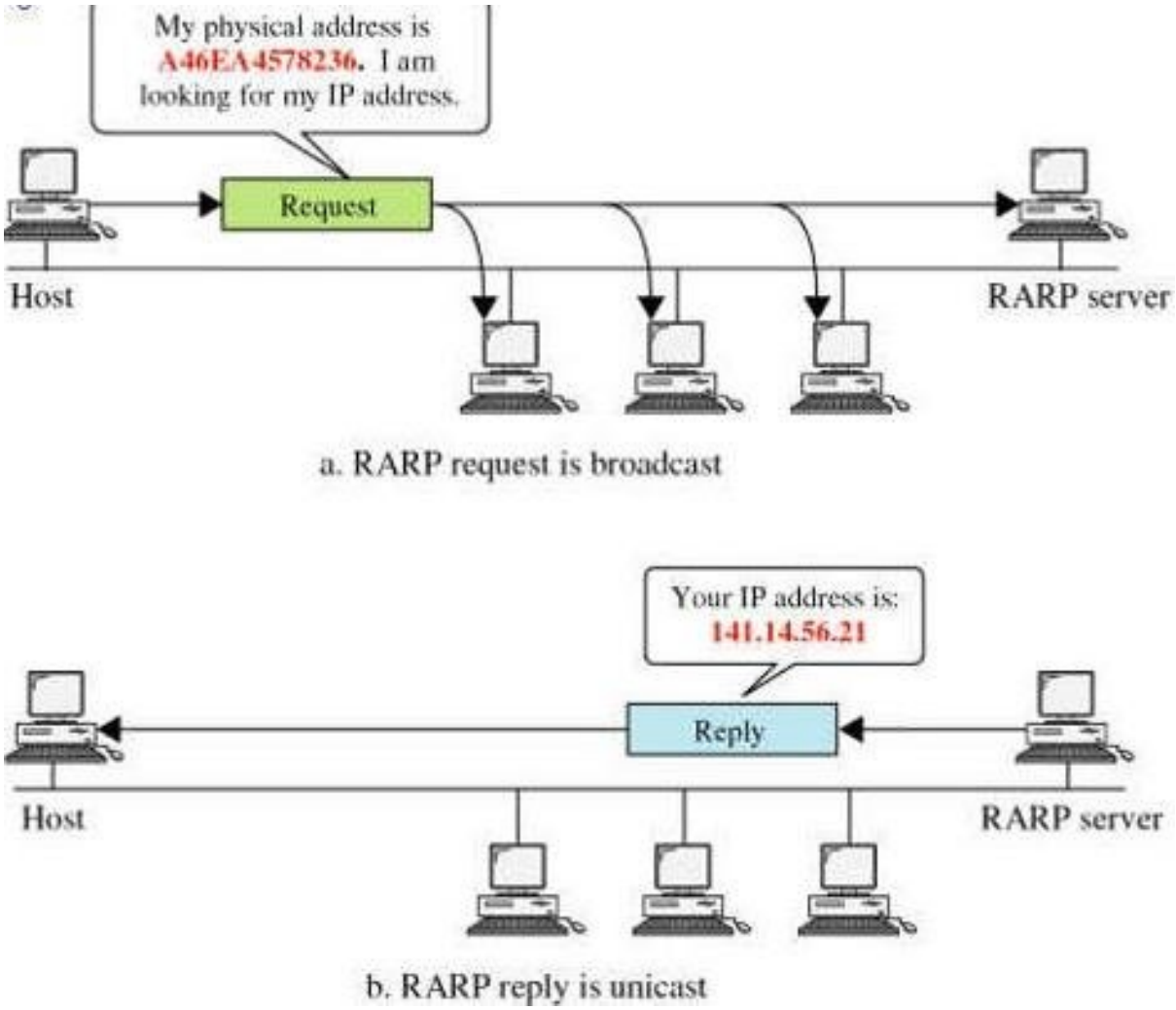

Figure 1: MAC Address Structure

4. Functionality of ARP (Address Resolution Protocol)

While MAC addresses handle local network communication, IP addresses are used for routing data across different networks. To send data to a device on the same local network, a device needs to know the destination’s MAC address. This is where the **Address Resolution Protocol (ARP)** comes into play.

ARP operates at the **Data Link Layer (Layer 2)** and translates Network Layer (Layer 3) IPv4 addresses into Data Link Layer (Layer 2) MAC addresses. It’s a critical component for IPv4 communication on Ethernet-based local area networks.

4.1. ARP Request

When a host wants to send a packet to another host on the same network and knows the destination's IP address but not its MAC address, it initiates an ARP process. The sending host broadcasts an **ARP request** packet to all devices on the network. This packet contains the following information:

- The sender's MAC address (Source Hardware Address)
- The sender's IP address (Source Protocol Address)
- The target's IP address (Target Protocol Address)

The target's MAC address (Target Hardware Address) is intentionally left blank (all zeros) in the request. The Ethernet header of an ARP request specifies a broadcast destination MAC address ('FF:FF:FF:FF:FF:FF').

4.2. ARP Reply

Every device on the local network receives the ARP request. They examine the target IP address in the request. If a device recognizes its own IP address as the target IP address, it responds with an **ARP reply** packet. This reply contains:

- The target's (now sender of the reply) MAC address (Source Hardware Address)
- The target's IP address (Source Protocol Address)
- The sender's (original requester) MAC address (Target Hardware Address)
- The sender's IP address (Target Protocol Address)

This ARP reply is sent directly to the MAC address of the requesting host (unicast).

4.3. ARP Cache Management

To optimize performance and reduce network traffic, the requesting host stores the IP-to-MAC address mapping in its **ARP cache**. This cache is a temporary table of recently resolved MAC addresses for corresponding IP addresses.

- **Aging (Timeout):** Entries in the ARP cache are typically dynamic and have a timeout period (e.g., a few minutes to several hours). After this period, the entry expires, and the host will need to perform another ARP request if it needs to communicate with that IP address again. This helps in managing changes to network topology or device MAC addresses.
- **Static Entries:** Network administrators can manually add static ARP entries to the cache. Static entries do not expire and are often used for critical servers or security purposes to prevent ARP spoofing.

Commands like 'arp -a' (Windows) or 'arp -n' (Linux/macOS) can be used to view the ARP cache.

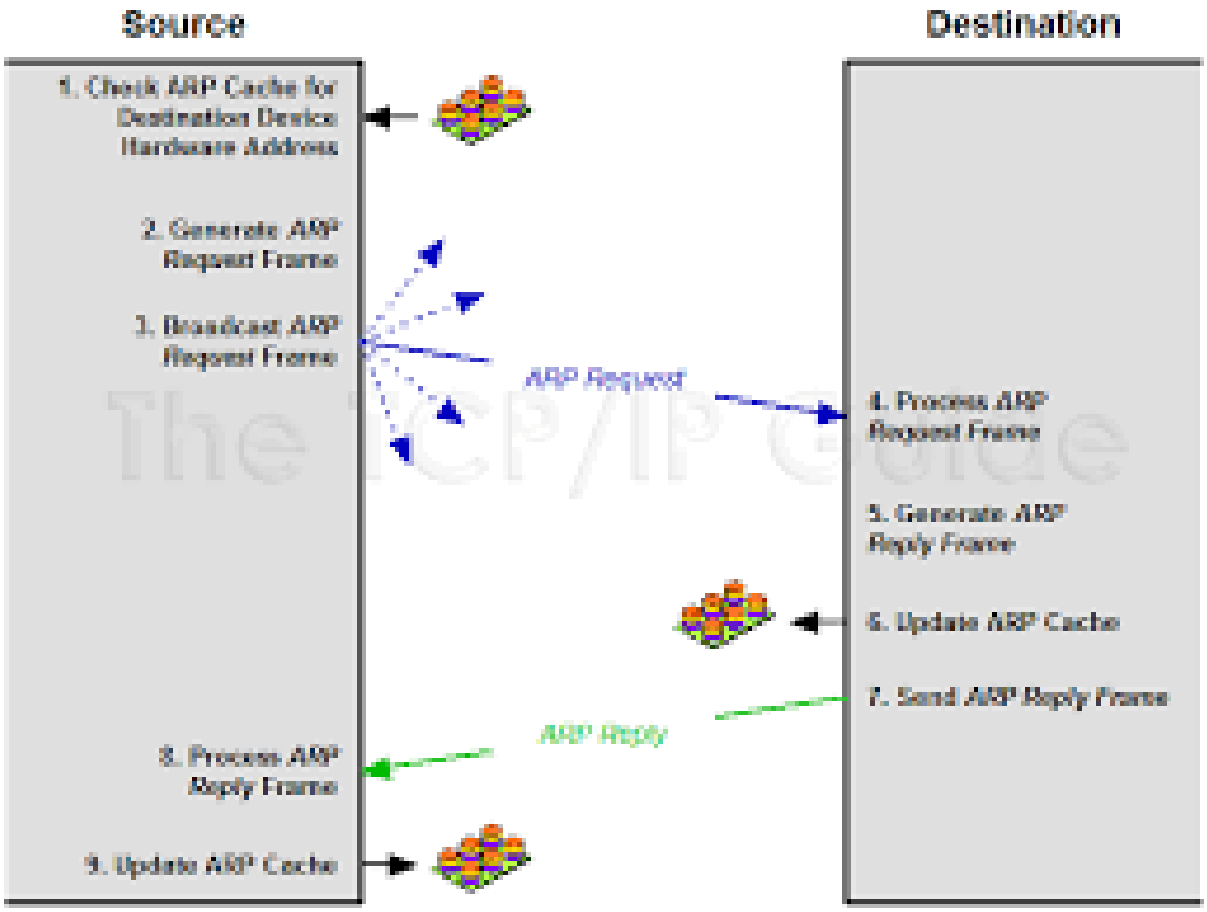

Figure 2: ARP Request and Reply Process

4.4. Advanced ARP Concepts

4.4.1. Proxy ARP

Proxy ARP is a technique where a router or a host on a network answers ARP requests for network addresses that are not on the local network segment but are reachable through that router/host. The router essentially "proxies" for the actual destination, making it appear that the destination is directly connected to the local network segment. This allows devices on one segment to communicate with devices on another segment without needing to know about the router. While it can simplify some small, unrouted networks, it can also lead to increased ARP traffic and potential security issues if not managed carefully.

4.4.2. Gratuitous ARP

A **Gratuitous ARP** is an ARP request broadcast by a device that is not expecting a reply. It's often sent when a device starts up, when its IP address changes, or when its NIC's state changes. Its primary purposes include:

- **Announcing its presence:** Informing other devices on the network about its IP-to-MAC address mapping, allowing them to update their ARP caches.

- **Detecting duplicate IP addresses:** If another device replies to a gratuitous ARP, it indicates an IP address conflict on the network.
- **Enhancing network redundancy/failover:** Used in High Availability protocols (like HSRP, VRRP, GLBP) to quickly update ARP caches on network devices after a failover event, ensuring traffic redirection to the newly active router.

4.5. ARP Security Implications

The stateless and trusting nature of ARP makes it vulnerable to attacks. **ARP spoofing** or **ARP poisoning** is a common attack where a malicious actor sends forged ARP messages to associate their MAC address with the IP address of another legitimate device (e.g., the default gateway or another host) on the local network. This can lead to:

- **Man-in-the-Middle (MitM) attacks:** Traffic intended for the legitimate device is redirected through the attacker's machine, allowing the attacker to intercept, inspect, or modify the data.
- **Denial of Service (DoS):** By associating an IP address with a non-existent or incorrect MAC address, traffic can be dropped, preventing legitimate communication.
- **Session Hijacking:** By intercepting traffic, an attacker might capture session cookies or credentials.

Defenses include static ARP entries (though not scalable for large networks), Dynamic ARP Inspection (DAI) features on managed switches, port security, and using network access control (NAC) solutions.

4.6. ARP in IPv6: Neighbor Discovery Protocol (NDP)

For IPv6, the functionality of ARP is replaced by the **Neighbor Discovery Protocol (NDP)**. NDP is part of ICMPv6 and provides broader functionality than ARP, including:

- Address resolution (mapping IPv6 addresses to MAC addresses)
- Router discovery
- Prefix discovery
- Parameter discovery
- Duplicate Address Detection (DAD)

NDP leverages multicast instead of broadcast, making it more efficient and scalable for IPv6 networks.

5. Functionality of RARP (Reverse Address Resolution Protocol)

Historically, in some specific network setups, a device might know its MAC address but not its IP address. This scenario was common with **diskless workstations** that boot from a network server and needed to obtain their IP configuration before they could load an operating system. The **Reverse Address Resolution Protocol (RARP)** was designed to address this situation.

RARP is a protocol by which a host on a local area network can discover its Internet Protocol address. It uses its physical address (MAC address) to ask a RARP server on the network for its IP address.

5.1. RARP Request and Reply

When a device boots up and needs to know its IP address, it broadcasts a **RARP request** packet on the local network. This packet contains the requesting device's MAC address. The IP address field in the request is typically left blank or set to zero, as the device doesn't know it yet.

A dedicated **RARP server** (if configured on the network) listens for RARP requests. When it receives a request, it looks up the MAC address in its pre-configured database of MAC-to-IP address mappings. If a corresponding IP address is found, the RARP server sends a **RARP reply** packet directly to the requesting device's MAC address (unicast). This reply contains the IP address assigned to that MAC address.

5.2. Why RARP Was Superseded

RARP suffered from several significant limitations that led to its obsolescence and replacement by more capable protocols:

- **Limited Information Provision:** RARP could only provide an IP address. It could not provide other crucial network configuration parameters such as the subnet mask, default gateway, DNS server addresses, or the location of a boot file (e.g., an operating system image). This meant that diskless clients still required manual configuration or additional protocols to get a full network setup.
- **Requirement for a Dedicated Server and Manual Configuration:** A specific RARP server was needed on the network to answer requests. This server required manual pre-configuration of MAC-to-IP address mappings for every client, which was cumbersome and prone to errors in large environments.
- **Broadcast Domain Limitation (Non-Routable):** RARP requests are broadcast within a single physical network segment (broadcast domain). A RARP server must reside on the same broadcast domain as the requesting client; RARP requests cannot be forwarded or routed across different network segments. This significantly limited scalability in larger or segmented networks.

These limitations led to the development and widespread adoption of more comprehensive protocols that operate at the application layer or higher, offering more flexibility and scalability:

- **BOOTP (Bootstrap Protocol):** Introduced as an improvement over RARP, BOOTP could provide an IP address, subnet mask, default gateway, and a boot file name, making it more suitable for diskless workstations. Importantly, BOOTP also supported relaying requests across routers, overcoming RARP's broadcast domain limitation.
- **DHCP (Dynamic Host Configuration Protocol):** DHCP is an extension of BOOTP and is the most widely used protocol today for dynamic IP address assignment. DHCP offers dynamic allocation, automatic renewal of leases, and can provide a wide range of network configuration parameters (IP address, subnet mask, gateway, DNS, NTP servers, etc.), making network management significantly easier, more robust, and highly scalable. Most modern networks rely heavily on DHCP for automated device configuration.

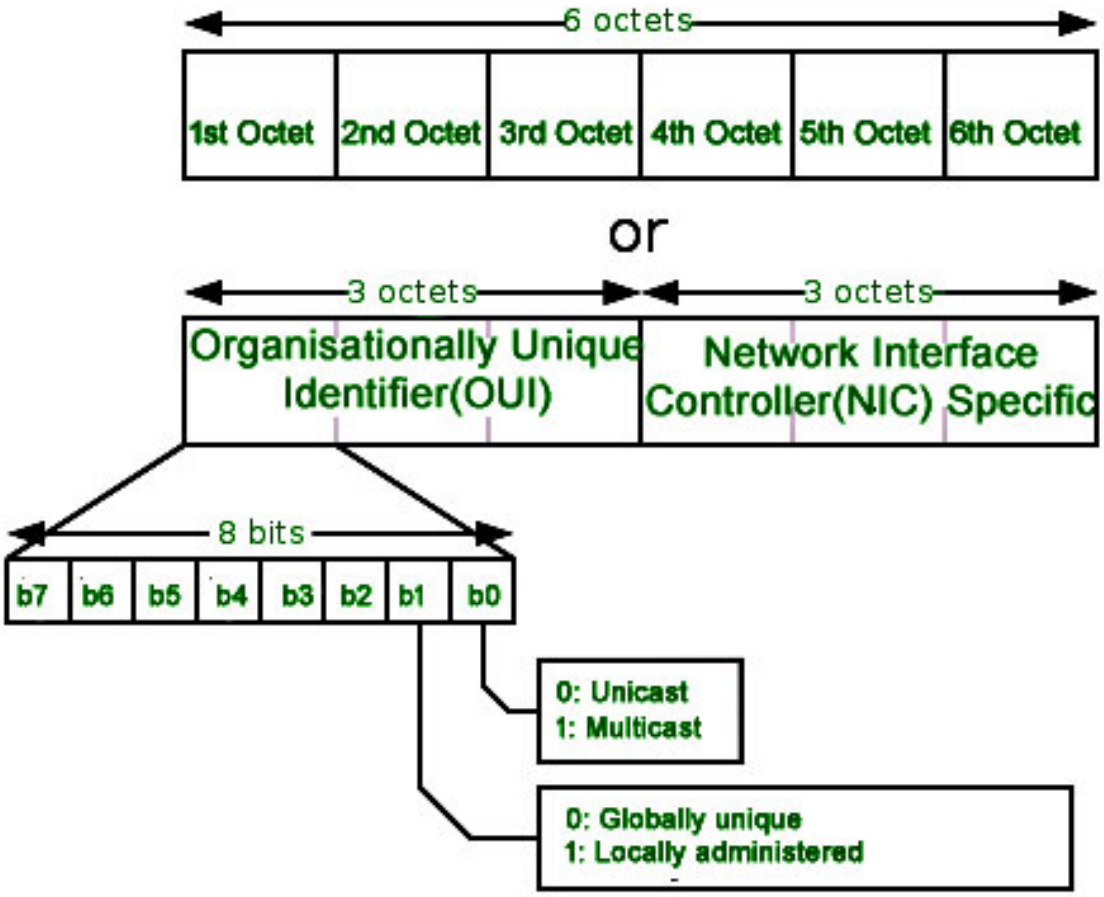

Figure 3: RARP Request and Reply Process

6. ARP vs. RARP: A Comparison Summary

Table 1: Comparison of ARP and RARP

Feature	ARP (Address Resolution Protocol)	RARP (Reverse Address Resolution Protocol)
Purpose	Resolves a Network Layer (IP) address to a Data Link Layer (MAC) address.	Resolves a Data Link Layer (MAC) address to a Network Layer (IP) address.
Question	"I have IP address X, what is its MAC address?"	"I have MAC address Y, what is my IP address?"
Layer	Data Link Layer (Layer 2) Protocol. Often considered part of the IP suite.	Data Link Layer (Layer 2) Protocol.
Request Type	Broadcast	Broadcast
Reply Type	Unicast	Unicast
Use Case	Essential for all IPv4 communication within a local network segment.	Used by diskless workstations to obtain their own IP address during boot-up.
Current Relevance	Still fundamental and widely used in all IPv4 networks.	Largely obsolete, replaced by BOOTP and primarily DHCP.
Security	Vulnerable to spoofing/poisoning attacks.	Less of a direct security concern today due to obsolescence, but relies on a trusted server.
IPv6 Equivalent	Neighbor Discovery Protocol (NDP)	Functionality integrated into NDP (Stateful/Stateless Autoconfiguration) and DHCPv6.

7. Conclusion

MAC addressing forms the physical foundation for communication within local area networks, providing unique identifiers for every network interface. The Address Resolution Protocol (ARP) is an indispensable component of IPv4 networks, efficiently translating logical IP addresses into physical MAC addresses, which is vital for delivering data frames to the correct destination within a local segment. Advanced ARP functionalities like Proxy ARP and Gratuitous ARP further illustrate its versatility, though they also highlight the importance of understanding associated security risks such as ARP spoofing.

Conversely, the Reverse Address Resolution Protocol (RARP), while historically significant for diskless clients to obtain their IP addresses, has been largely superseded by more comprehensive and flexible protocols like BOOTP and especially DHCP. DHCP's ability to dynamically assign not just IP addresses but also other critical network configurations has made it the industry standard for IP address management.

A thorough understanding of MAC addressing, ARP, and the historical context of RARP is crucial for anyone involved in designing, implementing, or troubleshooting modern computer networks. These foundational protocols ensure that data finds its way from one device to another, forming the invisible plumbing of the internet.

References

- GeeksforGeeks. (2023). *ARP, Reverse ARP/RARP, Inverse ARP/InARP, Proxy ARP, and Gratuitous ARP*. Available at: https://www.geeksforgeeks.org/computer-networks/arp-reverse-arprarp-inverse-arp-inarp-proxy-arp-and-gratuitous-arp/
- Kurose, J. F., Ross, K. W. (2017). *Computer Networking: A Top-Down Approach* (7th ed.). Pearson.
- Cisco Systems. (n.d.). *ARP - Address Resolution Protocol*. Available at: https://www.cisco.com/c/en/us/support/docs/ip/address-resolution-protocol-arp10123-1.html
- Wikipedia. (n.d.). *MAC address*. Available at: https://en.wikipedia.org/wiki/MAC_address
- Wikipedia. (n.d.). *Address Resolution Protocol*. Available at: https://en.wikipedia.org/wiki/Address_Resolution_Protocol
- Wikipedia. (n.d.). *Reverse Address Resolution Protocol*. Available at: https://en.wikipedia.org/wiki/Reverse_Address_Resolution_Protocol
- Odom, W. (2018). *CCNA 200-125 Official Cert Guide, Volume 1* (1st ed.). Cisco Press.
- Forouzan, B. A. (2010). *Data Communications and Networking* (5th ed.). McGraw-Hill Education.