Ayush Jain

Celebal Technologies

MAC Addressing

15 June 2025

MAC Addressing

To communicate or transfer data from one computer to another, we need an address. In computer networks, various types of addresses are introduced; each works at a different layer. A MAC address, which stands for Media Access Control Address, is a physical address that works at the Data Link Layer. In this article, we will discuss addressing a DLL, which is the MAC Address.

MAC Addresses are unique **48-bit** hardware numbers of a computer that are embedded into a network card (known as a **Network Interface Card**) during manufacturing. The MAC Address is also known as the **Physical Address** of a network device. In the IEEE 802 standard, the data link layer is divided into two sublayers:

1. Logical Link Control (LLC) Sublayer
2. Media Access Control (MAC) Sublayer

To understand what is MAC address is, it is very important that first you understand the format of the MAC Address. So a MAC Address is a 12-digit hexadecimal number (48-bit binary number), which is mostly represented by Colon-Hexadecimal notation.

The First 6 digits (say 00:40:96) of the MAC Address identify the manufacturer, called the OUI (**Organisational Unique Identifier**). IEEE Registration Authority Committee assigns these MAC prefixes to its registered vendors.

Types of MAC Address

1. Unicast: A Unicast-addressed frame is only sent out to the interface leading to a specific NIC. If the LSB (least significant bit) of the first octet of an address is set to zero, the frame is meant to reach only one receiving NIC. The MAC Address of the source machine is always Unicast.

2. Multicast: The multicast address allows the source to send a frame to a group of devices. In Layer-2 (Ethernet) Multicast address, the LSB (least significant bit) of the first octet of an address is set to one. IEEE has allocated the address block 01-80-C2-xx-xx-xx (01-80-C2-00-00-00 to 01-80-C2-FF-FF-FF) for group addresses for use by standard protocols.

3. Broadcast: Similar to Network Layer, Broadcast is also possible on the underlying layer(Data Link Layer). Ethernet frames with ones in all bits of the destination address (FF-FF-FF-FF-FF-FF) are referred to as the broadcast addresses. Frames that are destined with MAC address FF-FF-FF-FF-FF-FF will reach every computer belonging to that LAN segment.

Address Resolution Protocol

Address Resolution Protocol is a communication protocol used for discovering physical address associated with given network address. Typically, ARP is a network layer to data link layer mapping process, which is used to discover MAC address for given Internet Protocol Address. In order to send the data to destination, having IP address is necessary but not sufficient; we also need the physical address of the destination machine. ARP is used to get the physical address (MAC address) of destination machine.

Before sending the IP packet, the MAC address of destination must be known. If not so, then sender broadcasts the ARP-discovery packet requesting the MAC address of intended destination. Since ARP-discovery is broadcast, every host inside that network will get this message but the packet will be discarded by everyone except that intended receiver host whose IP is associated. Now, this receiver will send a unicast packet with its MAC address (ARP-reply) to the sender of ARP-discovery packet. After the original sender receives the ARP-reply, it updates ARP-cache and start sending unicast message to the destination.

Reverse Address Resolution Protocol

Reverse ARP is a networking protocol used by a client machine in a local area network to request its Internet Protocol address (IPv4) from the gateway-router's ARP table. The network administrator creates a table in gateway-router, which is used to map the MAC address to corresponding IP address. When a new machine is setup or any machine which don't have memory to store IP address, needs an IP address for its own use. So the machine sends a RARP broadcast packet which contains its own MAC address in both sender and receiver hardware address field.

A special host configured inside the local area network, called as RARP-server is responsible to reply for these kind of broadcast packets. Now the RARP server attempt to find out the entry in IP to MAC address mapping table. If any entry matches in table, RARP server send the response packet to the requesting device along with IP address.

- LAN technologies like Ethernet, Ethernet II, Token Ring and Fiber Distributed Data Interface (FDDI) support the Address Resolution Protocol.
- RARP is not being used in today's networks. Because we have much great featured protocols like BOOTP (Bootstrap Protocol) and DHCP(Dynamic Host Configuration Protocol).

How ARP Works?

Imagine a device that wants to communicate with others over the internet. What does ARP do? It broadcast a packet to all the devices of the source network. The devices of the network peel the header of the data link layer from the **Protocol Data Unit (PDU)** called frame and transfer the packet to the network layer (layer 3 of OSI) where the network ID of the packet is validated with the destination IP's network ID of the packet and if it's equal then it responds to the source with the MAC address of the destination, else the packet reaches the gateway of the network and broadcasts packet to the devices it is connected with and validates their network ID. The above process continues till the second last network device in the path reaches the destination where it gets validated and ARP, in turn, responds with the destination MAC address.

1. **ARP Cache:** After resolving the MAC address, the ARP sends it to the source where it is stored in a table for future reference. The subsequent communications can use the MAC address from the table.
2. **ARP Cache Timeout:** It indicates the time for which the MAC address in the ARP cache can reside.
3. **ARP request:** This is nothing but broadcasting a packet over the network to validate whether we came across the destination MAC address or not.
   - The physical address of the sender.
   - The IP address of the sender.

    - The physical address of the receiver is FF:FF:FF:FF:FF: FF or 1's.
    - The IP address of the receiver.

4. **ARP response/reply:** It is the MAC address response that the source receives from the destination which aids in further communication of the data.

- **CASE-1:**
    - The sender wants to send a packet to another host on the same network.
    - Use ARP to find another host's physical address.
- **CASE-2:**
    - The sender is a host and wants to send a packet to another host on another network.
    - The sender looks at its routing table.
    - Find the IP address of the next hop (router) for this destination.
    - Find the IP address of the next hop (router) for this destination.
- **CASE-3:**
    - The sender is a router and received a datagram.
    - The router checks its routing table.
    - Calculate the IP of the next router.
    - Use ARP to find the next router's physical address.
- **CASE-4:**
    - The sender is a router that has received a datagram destined for a host in the same network.
    - Use ARP to find this host's physical address.

How does RARP Work?

Reverse ARP (RARP) is a network protocol used by a client machine in a local area network (LAN) to obtain its Internet Protocol (IP) address from the gateway router's ARP (Address Resolution Protocol) table. When a machine doesn't have the memory to store its IP address, such as diskless machines or newly configured systems, it uses RARP to request an IP address.

1. RARP Request: A client machine that needs an IP address sends a broadcast message, known as a RARP request, to the network. This request contains the machine's unique MAC (Media Access Control) address in both the sender and receiver hardware address fields.

2. ARP Table in Gateway Router: The gateway router contains an ARP table that maps the MAC addresses to their corresponding IP addresses. This table is set up by the network administrator.

3. RARP Server Response: When a RARP request is received, the RARP server (which can be a regular computer in the network) checks its ARP table. If the MAC address in the RARP request matches one in its table, the server sends back the corresponding IP address to the requesting client.

4. Client Assignment: Upon receiving the IP address, the client machine configures itself with the new IP address. The RARP protocol facilitates the assignment of an IP address to the client that did not have a pre-configured one.

RESOURCES

1. https://www.geeksforgeeks.org/computer-networks/arp-reverse-arprarp-inverse-arp-inarp-proxy-arp-and-gratuitous-arp/
2. https://www.geeksforgeeks.org/how-address-resolution-protocol-arp-works/
3. https://www.geeksforgeeks.org/computer-networks/what-is-rarp/