MAC addressing, ARP and RARP

# 

# ABSTRACT

This is a research and development document discussing the concepts and principles behind MAC (Media Access Control) addressing, the Address Resolution Protocol (ARP) and the Reverse Address Resolution Protocol (RARP). These protocols are much involved in the data link layer for network communication. Understanding about how they work, their formats and the interaction makes easier work of troubleshooting, networking design and clarity in practical implementation of LAN based systems.

# Introduction to MAC Addressing

MAC Address (Media Access Control Address) is a hardware identifier (unique) given to a network interface card (NIC) by the manufacturer. It works at the Media Access Control (MAC) sublayer of the Data link layer of the OSI model and is necessary to communicate locally over a LAN. In contrast to the IP addresses that can vary dynamically, MAC addresses are reserved to the hardware and are used to identify the devices on the same physical network.

# Structure of MAC Address

A MAC address is represented in hexadecimal format and it is of 48 bits. Therefore it is separated by colon or hyphens:

**EXAMPLE:** 00:1A:2B:3C:4D:5E

**FORMAT:**

Mac Address size = 48 bits(6 bytes).

**FIRST 3 bytes(24 bits):** OUI (Organizationally unique identifier), it identifies the manufacturer of the device.

**LAST 3 bytes(24 bits):** NIC specific (Device ID), it is assigned by the manufacturer to each Network interface Controller.

# Types of MAC Address

**UNICAST -** The MAC address is Unicast when the data is sent to one particular device on the network. Here, the frame is only transmitted to the destination device having the same MAC address. When the least significant bit (LSB) of the first octet in the address is 0, then the address is unicast. Also, the MAC address of the sending (source) device is a unicast address ,because it’s referring to only one device.

**MULTICAST -** The MAC address is Multicast when data is sent from one device to a group of devices on the network rather than a single device. On the Layer 2 (Ethernet) protocol, when the least significant bit (LSB) of the first octet is 1, then the frame is directed to multiple recipients. The IEEE has set aside the address range from 01-80-C2-00-00-00 to 01-80-C2-FF-FF-FF to be group-based (multicast) communications, as generally implemented by standard networking protocols.

**BROADCAST** - Broadcasting is also provided at the Data Link Layer like the Network layer. When a message needs to be delivered to each of the devices on a local network segment, i.e., on the same subnet then a Broadcast MAC address is used. In Ethernet, this is represented as a destination MAC address of FF-FF-FF-FF-FF-FF, i.e. all ones. Frames destined to this address will be sent to all the stations on that LAN.

# ARP

Address Resolution Protocol (ARP) is a protocol which is used to determine the MAC address (physical address) of a known IP address (network address) on a local network. It works in between Data Link Layer (Layer 2) and Network Layer (Layer 3). ARP is necessary since data delivery using Ethernet protocol requires a MAC address of a target and not only its IP. ARP also dynamically helps to detect the MAC address if the sender is not aware of it.

**Functionality of ARP:**

* The MAC address of the destination IP is then found by its ARP cache.
* Otherwise it transmits ARP Request on the local net:

Which computer takes this IP?

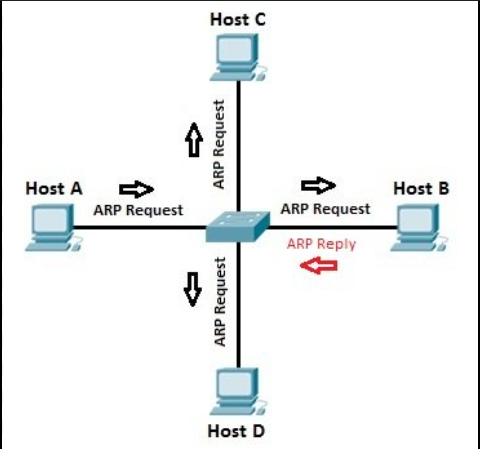
* All devices receive it and only the device with the same IP responds.
* Destination host then replies with its unicast ARP reply and its MAC address.
* The moment the sender gets the response, it updates its ARP cache after which data is directly transferred.

**Example:**

* If Host A with IP:192.168.1.10 wants to send any data to Host B with IP:192.168.1.20:
* Let host A not able to find MAC address for 192.168.1.20 in ARP cache
* So, then it broadcasts an ARP Request:

Who takes 192.168.1.20?

* Now host B receives and then reply via ARP reply:
* IP(192.168.1.20) is at MAC (AA:BB:CC:11:22:33) address
* So, host A now sends data to MAC and stores it in ARP cache.



Main types of ARP:

1. Reverse ARP- RARP (Reverse ARP) is a computer network protocol used by a device on a local area network to ask a gateway router to assign it an IPv4 address, given that the router already knows the MAC address of the device.
2. Proxy ARP- In proxy ARP router replies on behalf of another device which is on a different physical network but it's within the same IP subnet.
3. Inverse ARP- Here, the MAC address or Layer 2 identifier like DLCI in frame relay is already known and is used to discover device’s IP address.
4. Gratuitous ARP- When a device boots up it sends a broadcast to all other devices to announce its own IP and MAC address to the network.

# RARP

RARP(Reverse Address Resolution Protocol) is a computer network protocol used by a device on a local area network to ask a gateway router to assign it an IPv4 address, where the router already knows the device MAC address. The name reverse ARP is so because it maps MAC to IP instead of IP to MAC. It is usually useful for diskless workstations or the device that rely on a router or RARP server because they don’t have much storage to save IP addresses .

Functionality:

1. IP assignment: Devices without storage (e.g. diskless systems) can use RARP to get an IP address during the booting sequence.
2. Mapping IP to MAC: The RARP server or router must possess a static mapping table of MAC address to IP address, which is provided by a network administrator.
3. One-Time Resolution: RARP is normally needed only when booting or initialization of the network, once the IP gets assigned, the client does not need to request it again.
4. LAN works: The RARP packets are broadcast, and confined to the local network segment (just as ARP).

**Example:**

Working Model of RARP

Scenario:

A computer without a disk is switched on. It has a MAC address (e.g. AA:BB:CC:DD:EE:FF), and is unknown with its IP address.

RARP Steps:

Request:

* On the network, the computer broadcasts a RARP request packet.
* This is the MAC Address of source, (AA:BB:CC:DD:EE:FF).
* The MAC Address of target is FF:FF:FF:FF:FF:FF (broadcast).
* The IP address field's value is empty or 0.0.0.0.
* The request is passed to a router/RARP server on the network and consulted against the MAC-to-IP table.

IP Found:

* The RARP server then finds the matching entry for the MAC AA:BB:CC:DD:EE:FF that is mapped to IP 192.168.1.50.

RARP Reply:

* The server unicasts RARP Reply to the device whose IP is 192.168.1.50 and is directly transmitted to: AA:BB:CC:DD:EE:FF

IP Configures Client:

* As soon as it gets the reply, the client sets itself with the specified IP address.

Ready to Device:

* Now the device is ready to take part in network communication.

# 

# Conclusion

Local network communication requires the use of MAC addressing, ARP and RARP. Whereas MAC addresses make devices unique, ARP service translates IP addresses to MAC addresses for delivery of data. DHCP replaced RARP, but RARP was necessary in assigning IPs to non-storage devices. An insight into these protocols enhances network design, troubleshooting and implementation.