MAC Addressing and Functionality of ARP & RARP

1. Introduction to MAC Addressing

A **MAC (Media Access Control) address** is a hardware address assigned to the network interface card (NIC) of a device. It uniquely identifies a device at the **Data Link Layer (Layer 2)** of the OSI model.

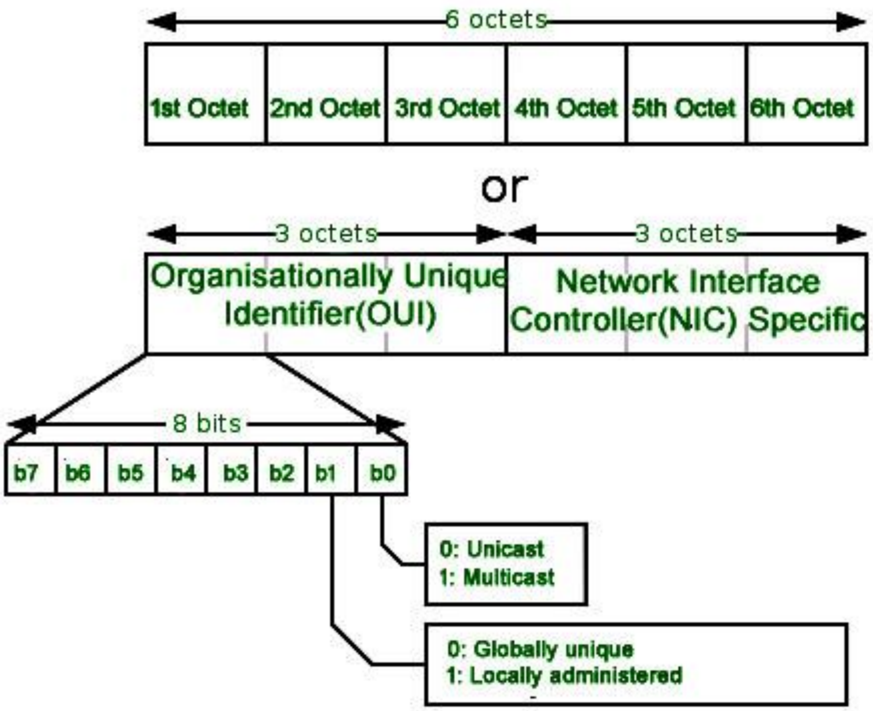
- MAC addresses are essential for communication **within a local network** (LAN).
- They are used in **Ethernet**, **Wi-Fi**, and other data-link protocols.

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

The MAC address is used by the Media Access Control (MAC) sublayer of the Data-Link Layer. MAC Address is worldwide unique since millions of network devices exist and we need to uniquely identify each.

A **MAC address** uniquely identifies network interfaces.



2. Structure and Types of MAC Addresses

2.1 Format

- **Length**: 48 bits (6 bytes)
- **Representation**: Hexadecimal, usually as XX:XX:XX:YY:YY:YY
- **Example**: 00:1A:2B:3C:4D:5E

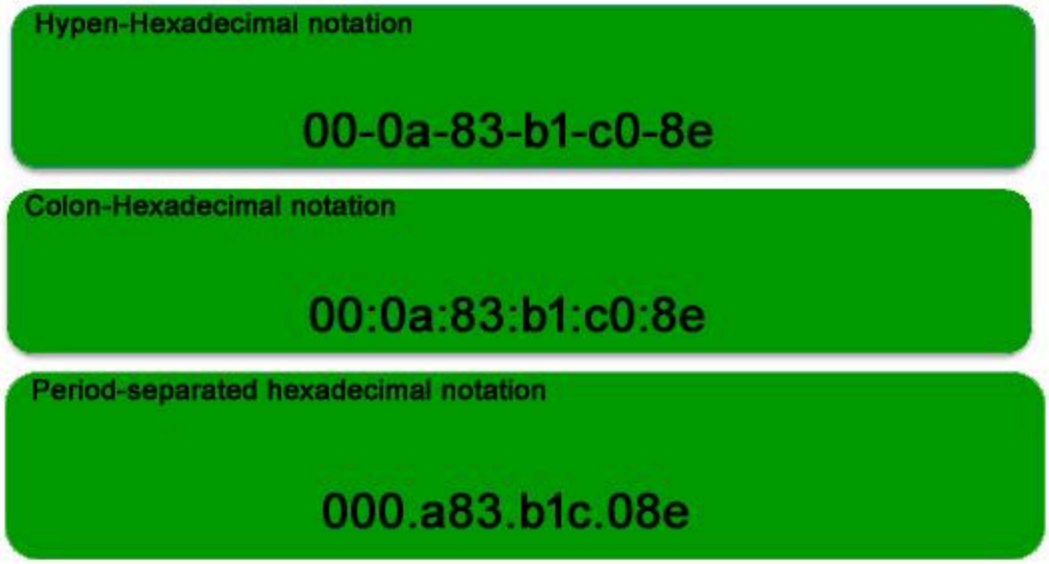
MAC Address is a 12-digit hexadecimal number (48-bit binary number), which is mostly represented by Colon-Hexadecimal notation.

The First 6 digits (say 00:40:96) of the MAC Address identify the manufacturer, called the OUI (**Organizational Unique Identifier**). IEEE Registration Authority Committee assigns these MAC prefixes to its registered vendors.
Here are some OUI of well-known manufacturers:
CC:46:D6 - Cisco
3C:5A:B4 - Google, Inc.

3C:D9:2B - Hewlett Packard
00:9A:CD - HUAWEI TECHNOLOGIES CO.,LTD

The rightmost six digits represent **Network Interface Controller**, which is assigned by the manufacturer.

As discussed above, the MAC address is represented by Colon-Hexadecimal notation. But this is just a conversion, not mandatory. MAC address can be represented using any of the following formats:


Hypen-Hexadecimal notation
00-0a-83-b1-c0-8e
Colon-Hexadecimal notation
00:0a:83:b1:c0:8e
Period-separated hexadecimal notation
000.a83.b1c.08e

2.2 Components

Section	Bits	Description
OUI	24	Organizationally Unique Identifier (Vendor-specific)
NIC-Specific	24	Unique per device (assigned by manufacturer)

2.3 Types of MAC Addresses

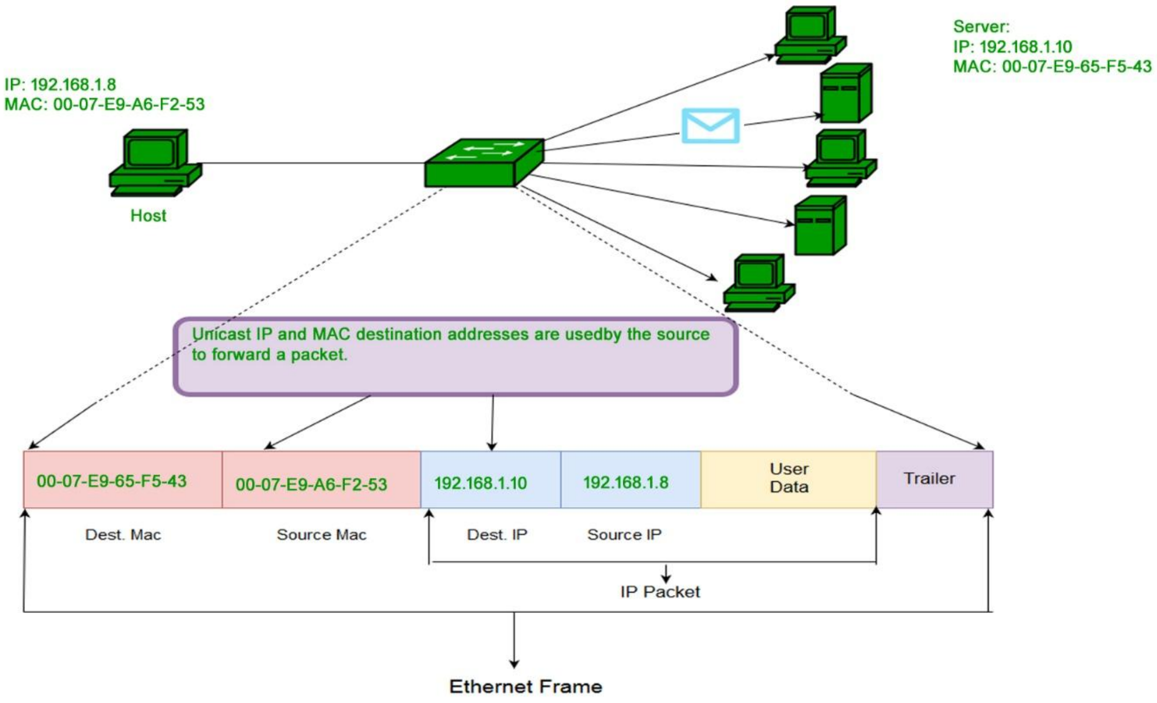
Type	Description
Unicast	Identifies a single network interface
Broadcast	Sent to all devices on the LAN (FF:FF:FF:FF:FF:FF)

Type	Description
Multicast	Sent to a group of devices sharing a multicast address

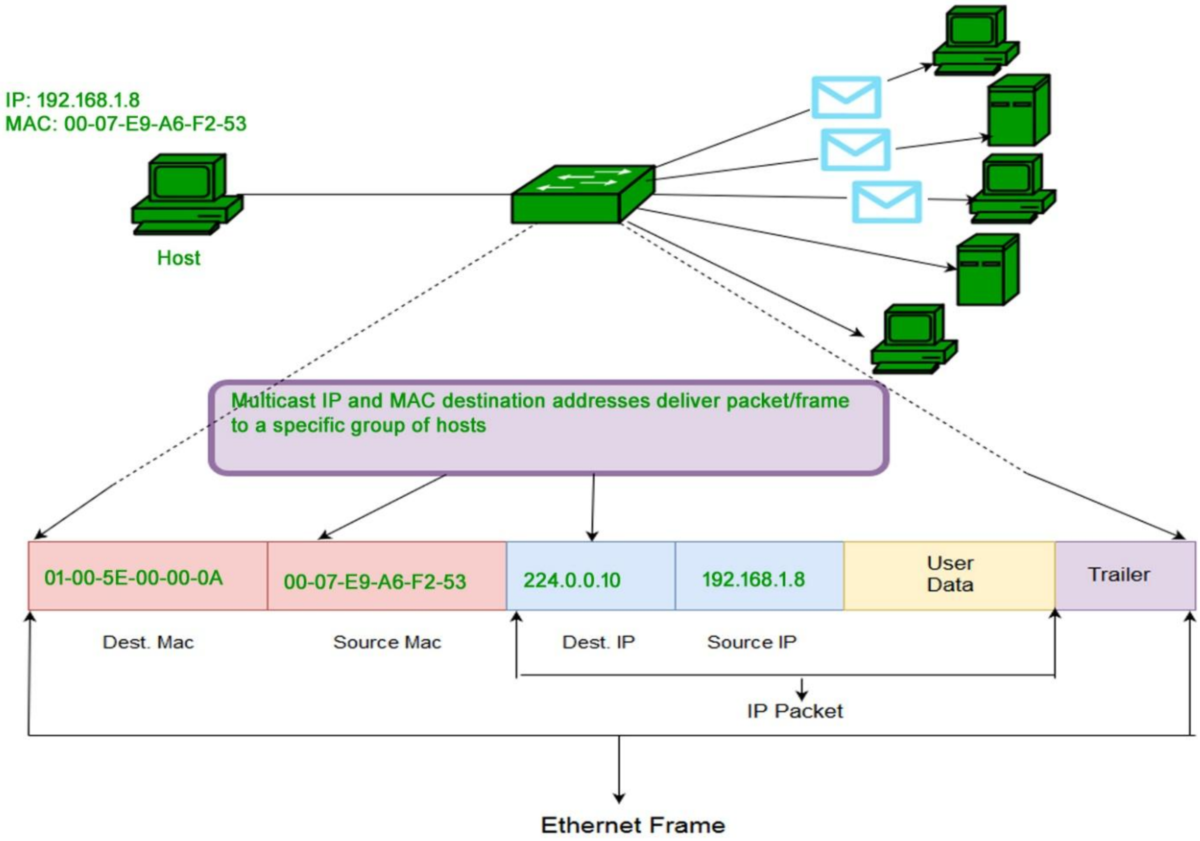
---

Types of MAC Address

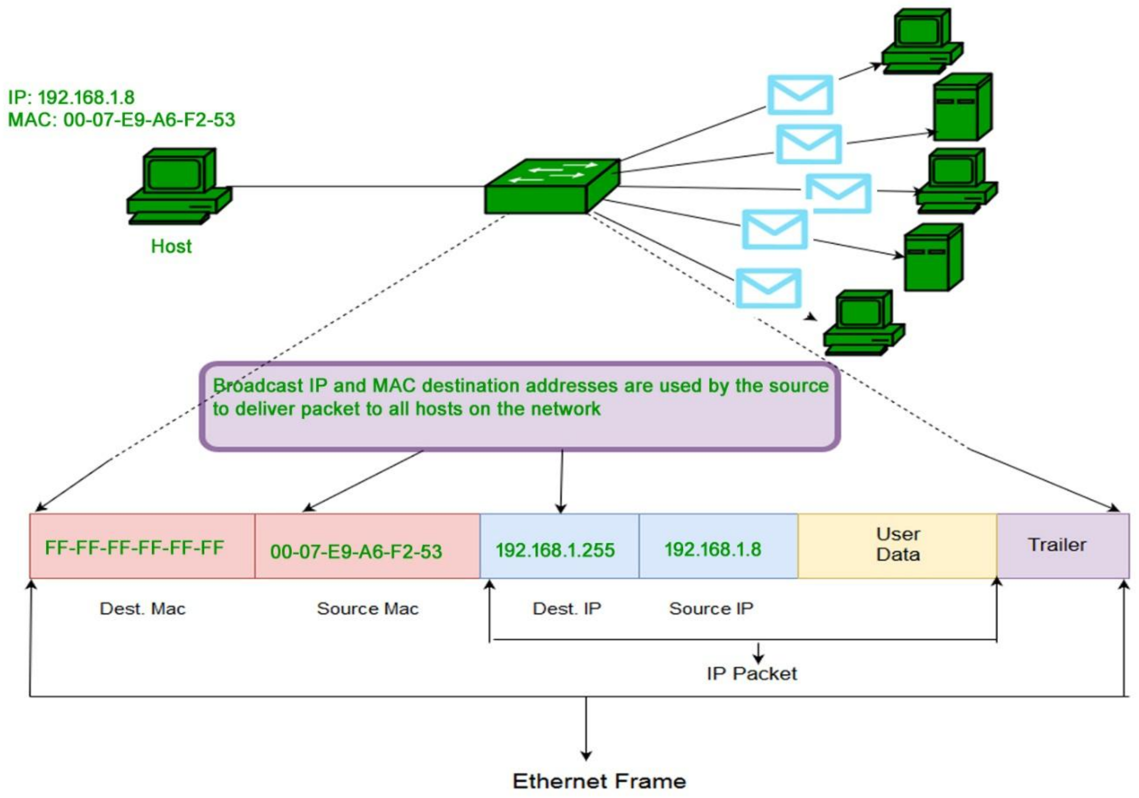
1. Unicast: A Unicast-addressed frame is only sent out to the interface leading to a specific NIC. If the LSB (least significant bit) of the first octet of an address is set to zero, the frame is meant to reach only one receiving NIC. The MAC Address of the source machine is always Unicast.



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.



---

3. Importance and Role in Networking

- MAC addresses operate at **Layer 2** of the OSI model.
- Switches use MAC addresses to **forward frames** within a LAN.
- Routers use **IP addresses** to route packets between networks.

---

4. Address Resolution Protocol (ARP)

4.1 Functionality

ARP maps a known **IPv4 address** to its corresponding **MAC address** within a local network.

- Operates in IPv4 environments
- Required when a device wants to send data to another device within the same LAN

4.2 ARP Packet Format (IPv4)

Field	Description
Hardware Type	1 for Ethernet
Protocol Type	0x0800 for IPv4
Opcode	1 = Request, 2 = Reply
Sender MAC	MAC address of sender
Sender IP	IP address of sender
Target MAC	MAC address of target (0 in request)
Target IP	IP address of target

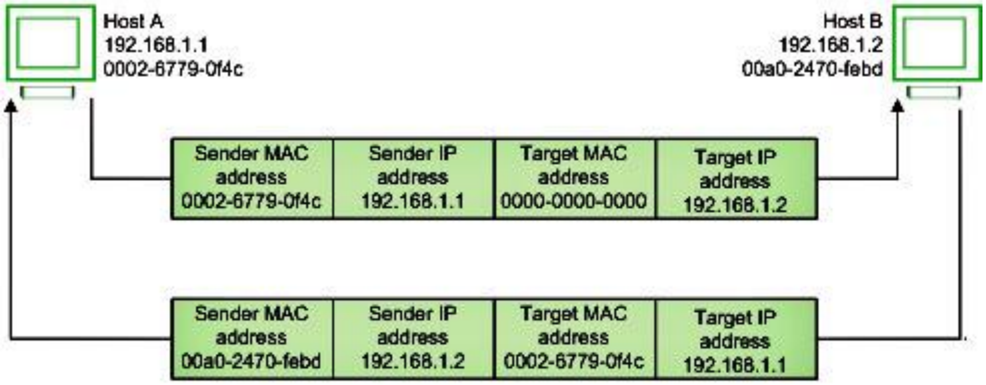
4.3 ARP Process

1. **Host A** wants to communicate with **Host B** (knows IP, not MAC).
2. Host A sends an **ARP Request**: "Who has IP 192.168.1.2?"
3. Host B responds with **ARP Reply**: "192.168.1.2 is at 00:1B:44:11:3A:B7"
4. Host A stores this mapping in its **ARP cache**.

ARP is **only used in local networks** (L2). For communication outside the LAN, it resolves the MAC of the **default gateway**.

4.4 Address Resolution Protocol (ARP) -

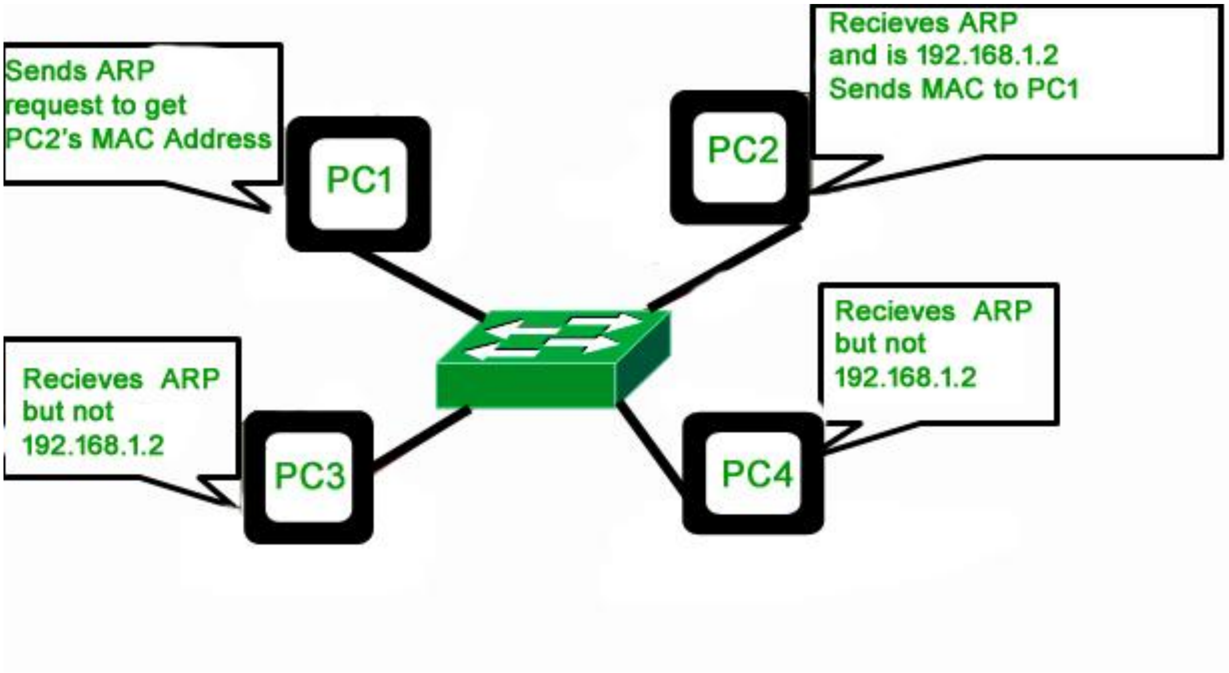
Address Resolution Protocol is a communication protocol used for discovering physical address associated with given network address. Typically, ARP is a network layer to data link layer mapping process, which is used to discover MAC address for given Internet Protocol Address. In order to send the data 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.



Sender MAC address	Sender IP address	Target MAC address	Target IP address
0002-6779-0f4c	192.168.1.1	0000-0000-0000	192.168.1.2

Sender MAC address	Sender IP address	Target MAC address	Target IP address
00a0-2470-febd	192.168.1.2	0002-6779-0f4c	192.168.1.1

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.


Sends ARP request to get PC2's MAC Address
PC1
PC2
Recieves ARP and is 192.168.1.2 Sends MAC to PC1
Recieves ARP but not 192.168.1.2
PC3
PC4
Recieves ARP but not 192.168.1.2

5. Reverse Address Resolution Protocol (RARP)

5.1 Functionality

RARP was used to map a **MAC address to an IP address**. It was primarily used by **diskless workstations** to discover their IP address from a central server at boot time.

5.2 How RARP Works

- A device sends a **RARP request**: "This is my MAC address, what is my IP?"
- A **RARP server** responds with the IP address mapped to that MAC address.

5.3 Limitations

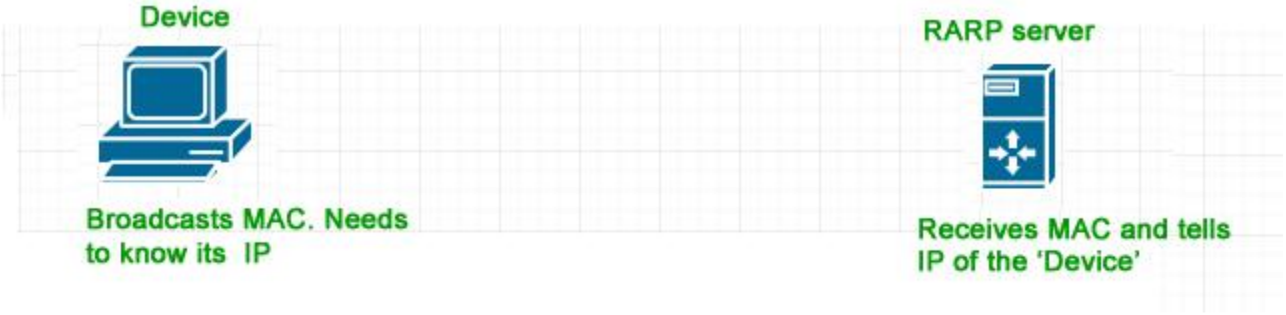
- RARP servers need to be **manually configured** with mappings.
- Only works for IPv4.

- Lacks flexibility and support for other settings (like subnet mask, gateway).

RARP has been deprecated and replaced by **BOOTP** and **DHCP**, which are more flexible and widely used.

5.4 Reverse Address Resolution Protocol (RARP) -

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.


Device
RARP server
Broadcasts MAC. Needs to know its IP
Receives MAC and tells IP of the 'Device'

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).

6. Comparison: ARP vs RARP

RARP	ARP
A protocol used to map a physical (MAC) address to an IP address	A protocol used to map an IP address to a physical (MAC) address
To obtain the IP address of a network device when only its MAC address is known	To obtain the MAC address of a network device when only its IP address is known
Client broadcasts its MAC address and requests an IP address, and the server responds with the corresponding IP address	Client broadcasts its IP address and requests a MAC address, and the server responds with the corresponding MAC address
MAC addresses	IP addresses
Rarely used in modern networks as most devices have a pre-assigned IP address	Widely used in modern networks to resolve IP addresses to MAC addresses
RFC 903 Standardization	RFC 826 Standardization

RARP	**ARP**
RARP stands for Reverse Address Resolution Protocol	ARP stands for Address Resolution Protocol
In RARP, we find our own IP address	In ARP, we find the IP address of a remote machine
The MAC address is known and the IP address is requested	The IP address is known, and the MAC address is being requested
It uses the value 3 for requests and 4 for responses	It uses the value 1 for requests and 2 for responses