**Research and Development Document**

**ON**

**Basics of MAC Addressing & Functionality of ARP & RARP**

****

****

**By**

**Anirudh Sharma**

**(CT\_CSI\_CI\_66)**

**Under**

**Celebal Summer Internship**

**in**

**Cloud Infra & Security**

**Table of Contents**

[**MAC Addressing** 3](#_37j571eiwqbb)

[Types of MAC Address 4](#_y6stgd1hpq2j)

[MAC Cloning 4](#_vl7exia92vjq)

[Characteristics of MAC Address 4](#_3rt2fxot7y0q)

[Advantages of MAC Address 5](#_yowmo864d3mh)

[Disadvantages of MAC Address 5](#_pgmfah7ynsgl)

[**Address Resolution Protocol**:](#_bluihg29n2hv) 8

**Reverse** [**Address Resolution Protocol**](#_bluihg29n2hv)[:](#_m1uo7g69gwkk) 10

**References**………………………………………………………………………………………….12

**MAC Addressing**

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:

* **Logical Link Control (LLC) Sublayer**
* **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. 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

**Format of MAC Address**

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 (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

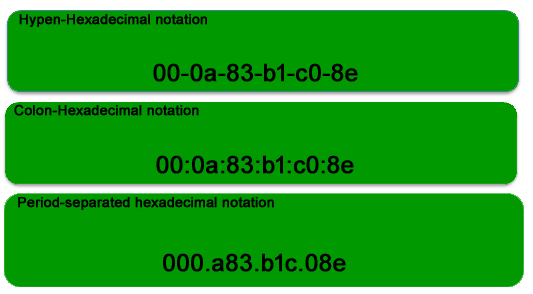
3C:5A:B4 - Google, Inc.

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.

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:



**Note: Colon-Hexadecimal notation is used by Linux OS and Period-separated Hexadecimal notation is used by Cisco Systems.**

## **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.

## **MAC Cloning**

Some ISPs use MAC addresses to assign an IP address to the gateway device. When a device connects to the ISP, the DHCP server records the MAC address and then assigns an IP address. Now the system will be identified through the MAC address. When the device gets disconnected, it loses the IP address.

If the user wants to reconnect, the DHCP server checks if the device is connected before. If so, then the server tries to assign the same IP address (in case the lease period has not expired). In case the user changed the router, the user has to inform the ISP about the new MAC address because the new MAC address is unknown to the ISP, so the connection cannot be established.

Or the other option is Cloning, users can simply clone the registered MAC address with ISP. Now the router keeps reporting the old MAC addresses to the ISP and there will be no connection issue.

## **Characteristics of MAC Address**

The Media Access Control address (MAC address) is a unique identifier assigned to most network adapters or network interface cards (NICs) by the manufacturer for identification and use in the Media Access Control protocol sub-layer.

An Ethernet MAC address is a 48-bit binary value expressed as 12 hexadecimal digits (4 bits per hexadecimal digit). MAC addresses are in a flat structure and thus they are not routable on the Internet. Serial interfaces do not use MAC addresses. It does NOT contain a network and host portion with the address. It is used to deliver the frame to the destination device.

* MAC addresses are used in LAN (Local Area Network) environments to identify devices and allow communication between them.
* MAC addresses are burned into the hardware of a network interface card (NIC) and cannot be changed, except in some rare cases where the manufacturer has provided a specific tool to do so.
* The first 3 bytes of a MAC address represent the manufacturer ID, while the last 3 bytes represent a unique identifier assigned by the manufacturer.
* MAC addresses are often used in conjunction with ARP (Address Resolution Protocol) to resolve IP addresses to MAC addresses for communication on a LAN.
* Some operating systems, such as Windows and Linux , allow you to view the MAC address of your network adapter through a command prompt or network settings.

## **Advantages of MAC Address**

1. **Uniqueness**: Each MAC address is unique, which means that devices on the network can be easily identified and managed.
2. **Simplicity**: MAC addresses are easy to configure and manage, and do not require any additional network infrastructure.
3. **Compatibility**: MAC addresses are widely used and supported by a variety of networking technologies and protocols, making them compatible with many different systems.
4. **Security**: MAC addresses can be used to restrict access to a network by only allowing devices with authorized MAC addresses to connect.
5. **Fault-tolerance**: In case of hardware or software failure, a device can be easily replaced without affecting the network, as long as the new device has the same MAC address as the old one.
6. **Multicasting**: MAC addresses can be used for multicasting, allowing a single packet to be sent to multiple devices at once.
7. **Efficiency**: MAC addresses allow for efficient communication on the network, as they enable devices to quickly and easily identify and communicate with each other.
8. **Lower network overhead**: MAC addresses reduce network overhead by allowing devices to communicate directly with each other without the need for additional routing or addressing.
9. **Ease of troubleshooting**: MAC addresses can be used to troubleshoot network issues by identifying the source of problems and tracking network activity.
10. **Flexibility**: MAC addresses can be used to support a variety of network configurations and topologies, including peer-to-peer, client-server, and hybrid models.

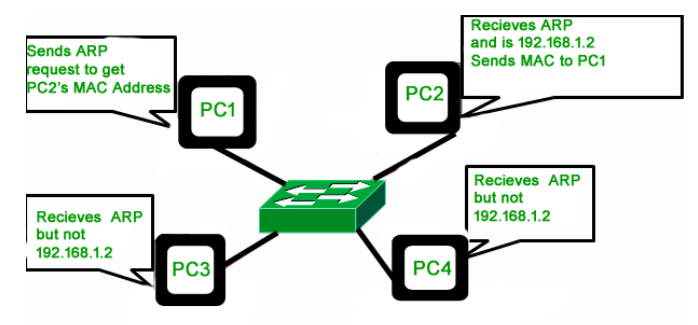
## **Disadvantages of MAC Address**

1. **Limited address space**: MAC addresses are 48-bit numbers, which means that there is a finite number of possible MAC addresses. This can lead to address conflicts if multiple devices have the same MAC address.
2. **Spoofing**: MAC addresses can be easily spoofed, allowing unauthorized devices to gain access to the network.
3. **Inefficiency**: MAC addresses are not hierarchical, which can make it difficult to efficiently manage large networks.
4. **Static addressing:** MAC addresses are typically assigned at the time of manufacture and cannot be easily changed. This can be a disadvantage in situations where devices need to be reconfigured or replaced.
5. **Limited scope:** MAC addresses are only used for identifying devices within a local network segment, and cannot be used to identify devices outside of this segment.
6. **Hardware-dependent**: MAC addresses are tied to the network interface card (NIC) of a device, which means that if the NIC fails or is replaced, the MAC address also changes.
7. **Lack of encryption:** MAC addresses are sent in plain text, which can make them vulnerable to interception and eavesdropping.
8. **No inherent security**: While MAC filtering can be used to restrict access to a network, MAC addresses themselves do not provide any inherent security features.
9. **MAC address collisions**: In rare cases, MAC addresses can collide, which can cause network disruptions and make it difficult to identify and manage devices on the network.

**Address Resolution Protocol**

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

Before sending the IP packet, the MAC address of the destination must be known. If not so, then the sender broadcasts the ARP-discovery packet requesting the MAC address of the 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 a unicast message to the destination.



**Working of ARP (Steps):**

1. Host A wants to send data to Host B (e.g., IP: 192.168.1.10)
2. It knows Host B’s IP address but needs the MAC address.
3. Host A sends an ARP request as a broadcast on the network:
4. All devices on the LAN receive this request, but only the device with IP 192.168.1.10 replies:
5. Host A now saves this mapping (IP ⇔ MAC) in its ARP table/cache.
6. Data can now be sent directly using the MAC address.

#### **Key Functionalities of ARP:**

1. **IP-to-MAC Address Resolution**
   * ARP translates known IP addresses into their corresponding MAC addresses so data can be transmitted on a local network.
2. **Broadcasting ARP Requests**
   * When a host doesn't know the MAC for a given IP, it sends a broadcast ARP request to all devices on the LAN.
3. **Receiving ARP Replies**
   * The device with the matching IP replies with its MAC address, allowing the sender to complete its Layer 2 frame.
4. **Maintaining ARP Cache (ARP Table)**
   * Devices store resolved IP-to-MAC mappings in memory for faster access in future communications.
5. **Supporting Efficient Local Communication**
   * Enables devices in the same subnet to communicate efficiently using their physical hardware addresses.
6. **Failover to Default Gateway**
   * If a host is not on the local network, ARP resolves the MAC of the default gateway/router to forward packets.

**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 set up or any machine which doesn't have memory to store an 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 the sender and receiver hardware address field.



A special host configured inside the local area network, called a RARP-server is responsible to reply for these kinds of broadcast packets. Now the RARP server attempts to find out the entry in IP to MAC address mapping table. If any entry matches in the table, the RARP server sends the response packet to the requesting device along with the 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 many great featured protocols like BOOTP (Bootstrap Protocol) and DHCP( Dynamic Host Configuration Protocol).

**Working of RARP (Steps):**

1. **Used by diskless computers or booting devices** that have no OS or IP configured.
2. The device sends a **RARP request** to a RARP server:
3. The **RARP server looks up** its configuration table.
4. Server replies with the IP address mapped to the MAC address.

#### **Key Functionalities of RARP:**

1. **MAC-to-IP Address Resolution**
   * RARP is used by a device to request its IP address by sending its MAC address to a RARP server.
2. **Enabling Bootstrapping in Diskless Devices**
   * Used in older or diskless workstations that booted from the network and needed to discover their IP address.
3. **Unicast Queries to RARP Server**
   * The request is directed specifically to a RARP server, which responds with the appropriate IP address.
4. **Static IP Mapping by Server**
   * The RARP server maintains a table with MAC-to-IP mappings that it uses to respond to client requests.

**References**

* **GeeksForGeeks**
* [**Cisco.com**](http://cisco.com)
* **AWS Documentation**
* **Youtube**