

## What is MAC (Media Access Control) Address?

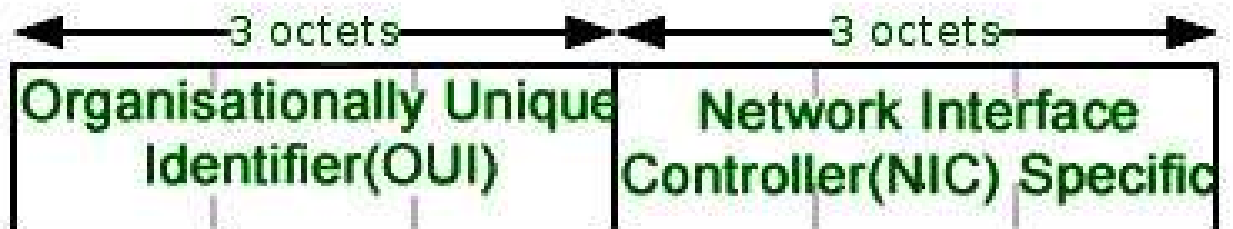
**MAC Addresses** are unique **48-bit** hardware numbers of a computer that are embedded into a network card (known as a [Network Interface Card](#)) during manufacturing. The MAC Address is also known as the [Physical Address](#) of a network device. In the IEEE 802 standard, the data link layer is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

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

**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.



or



0: Unicast  
1: Multicast

0: Globally unique  
1: Locally administered

## 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

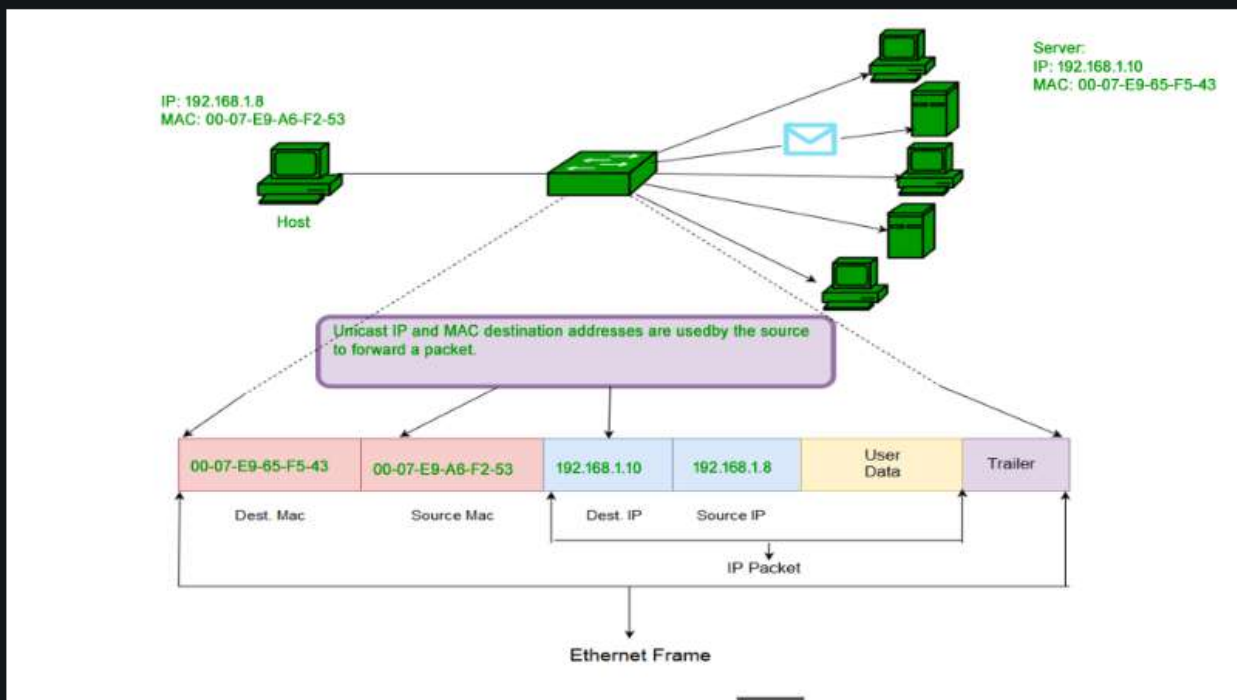
3C:5A:B4 - Google, Inc.

3C:D9:2B - Hewlett Packard

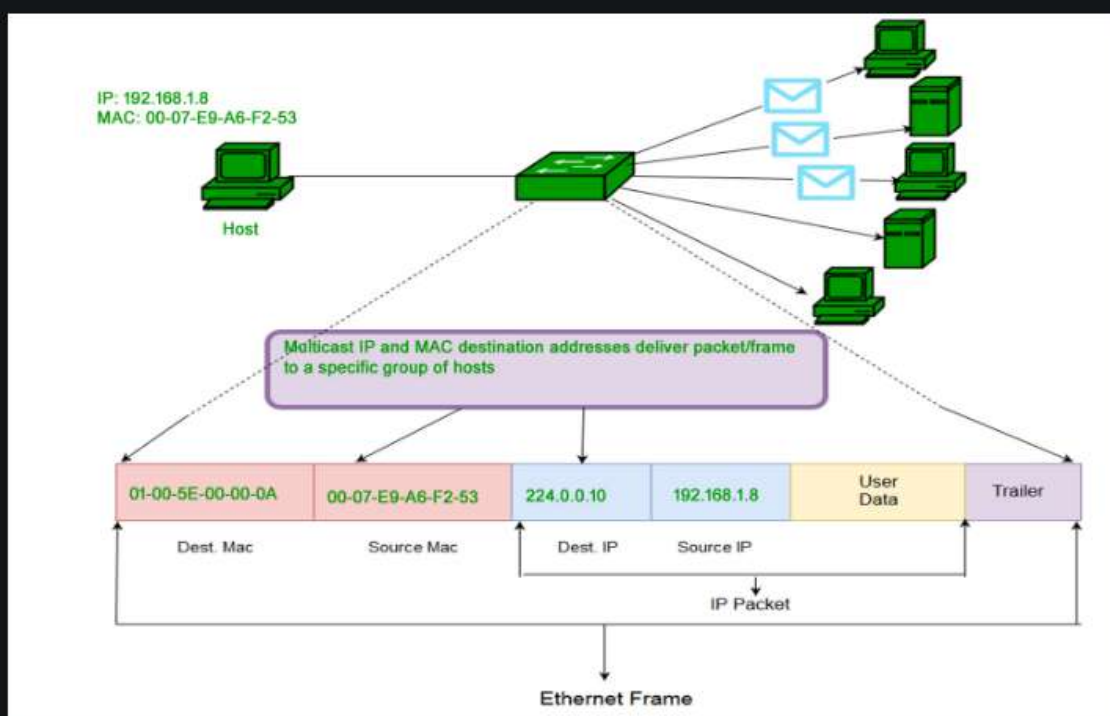
00:9A:CD - HUAWEI TECHNOLOGIES CO.,LTD

# Types of MAC Address

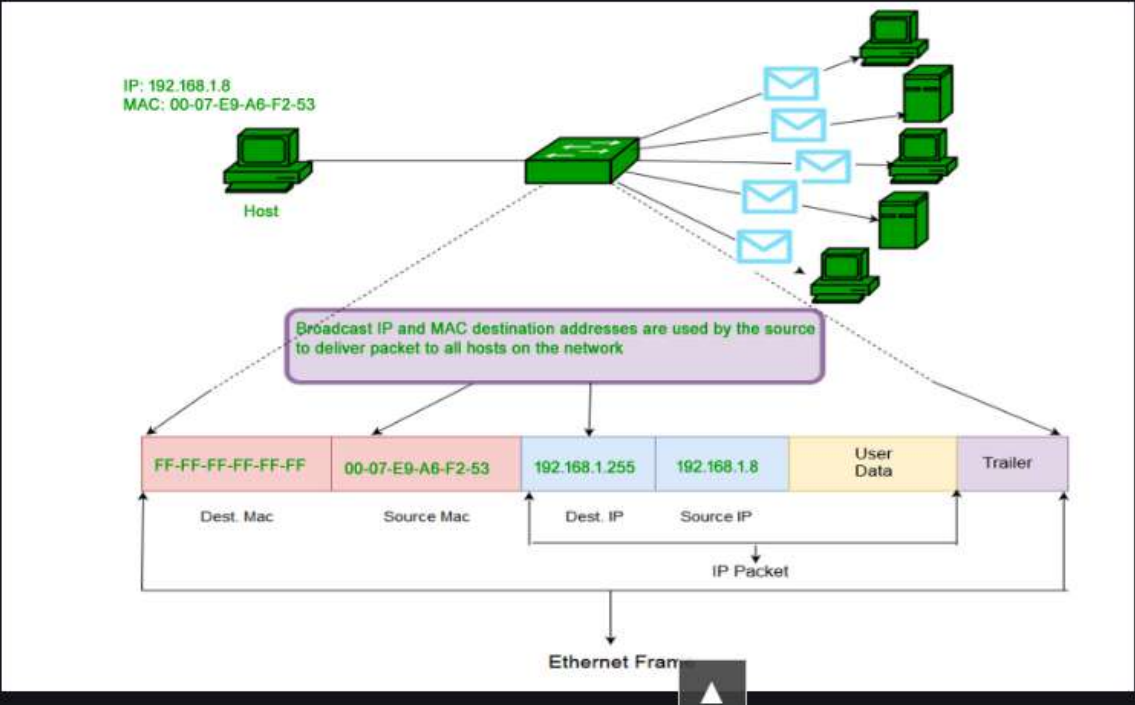
**1. Unicast:** A Unicast-addressed frame is only sent out to the interface leading to a specific NIC. If the LSB (least significant bit) of the first octet of an address is set to zero, the frame is meant to reach only one receiving NIC. The MAC Address of the source machine is always Unicast.



**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.





## Reason to Have Both IP and MAC Addresses.

The reason for having both IP and MAC addresses lies in the way the Internet works, specifically in the structure of the OSI Model. This model is a conceptual framework that describes how data is sent and received over a network. It's divided into seven layers, each performing specific functions.


- **Layer 2** uses **MAC addresses** and is responsible for packet delivery from **hop to hop** .
- **Layer 3** uses **IP addresses** and is responsible for packet delivery from **end to end** .

Layer 2 ([Data Link Layer](#)) uses a **MAC (Media Access Control) address**. These are unique identifiers assigned to network interfaces for communications at the data link layer. The primary function of MAC addresses is to manage how data is transported from one network node to another on a direct, physical basis – this is also referred to as “hop to hop” delivery.

On the other hand, Layer 3 ( [Network Layer](#) ) uses an **IP (Internet Protocol) address**. These IP addresses are used to identify devices on a network and to route traffic between networks. The IP addresses ensure that the data gets from its original source reaches its final destination and it is also called “end-to-end” delivery of data.

When a computer sends data, it first wraps it in an IP header, which includes the source and destination IP addresses. This IP header, along with the data, is then encapsulated in a MAC header, which includes the source and destination MAC addresses for the current “hop” in the path.

As the data travels from one router to the next, the MAC address header is stripped off and a new one is generated for the next hop. However, the IP header, which was generated by the original computer, remains intact until it reaches the final destination. This process illustrates how the IP header manages the “end to end” delivery, while the MAC headers handle the “hop to hop” delivery.





PORT	Service	Description	Transport Protocol
7	Echo	Port just echoes whatever is sent to it. This feature can be used in many attacks, such as Smurf/Fraggle.	TCP and UDP
20 /21	File Transfer Protocol (FTP)	Port used by FTP protocol to send data to the client	TCP
22	Secure Shell (SSH)	Used as secure replacement protocol for Telnet	TCP and UDP
23	Telnet	Port used by Telnet to remotely connect to a workstation or server(unsecured)	TCP

<b>25</b>	Simple Mail Transfer Protocol (SMTP)	Used to send E-Mail over internet	TCP
<b>53</b>	Domain Name System (DNS)	Port for DNS requests, network routing, and zone transfers	TCP and UDP
<b>67 /68</b>	Dynamic Host Configuration Protocol (DHCP)	Used on networks that do not use static IP address assignment.	UDP
<b>80</b>	Hypertext Transfer Protocol (HTTP)	Used for browsing web-pages on a browser	TCP
<b>110</b>	Post Office Protocol (POP3)	Port used to retrieve complete contents of a server mailbox	TCP