

What is a MAC Address?

MAC Address stands for **Media Access Control Address**.

It is a **unique physical address** given to every network device (like computers, smartphones, routers, etc.) by the **device manufacturer**.

It is used to **identify a device within a local network** (like your home or office Wi-Fi).

Format of MAC Address

A MAC address is a **48-bit** number written in **hexadecimal format**, usually like this:

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

- Divided into **6 pairs** of hexadecimal digits
- The first 3 pairs (24 bits) = **Organizationally Unique Identifier (OUI)** → identifies the manufacturer
- The last 3 pairs = **Device ID** (unique for each device)

Example:

MAC Address

Explanation

3C:5A:B4:12:34:56 3C:5A:B4 = Apple Inc. (OUI)

12:34:56 = Device serial section



Where is MAC Address Used?

- Inside Local Area Networks (LAN)
- In communication between devices on **same Wi-Fi or switch**
- Used by **routers, network switches, firewalls, and access points**

MAC Address vs IP Address

Feature	MAC Address	IP Address
Level	Hardware-level (Layer 2)	Software-level (Layer 3)
Assigned By	Device Manufacturer	ISP or Router
Format	Hexadecimal (00:1A:2B:3C:4D:5E)	Decimal (192.168.1.1)
Changes?	Usually permanent	Can change dynamically
Scope	Works within a local network	Works across the internet

How MAC Address Works?

When a device sends data:

1. It checks the **MAC address** of the destination device.
2. If the destination is in the **same network**, data goes directly using the MAC.
3. If not, data is forwarded using **IP routing**.

 Devices use a table called **ARP (Address Resolution Protocol)** to map **IP addresses to MAC addresses**.

Can MAC Address Be Changed?

Yes, this is called **MAC spoofing**. It can be done for:

- Privacy
- Testing security tools
- Bypassing MAC filtering in networks

Example on Windows:

bash

CopyEdit

```
netsh interface set interface name="Wi-Fi" newmac=XX:XX:XX:XX:XX:XX
```

MAC Address Filtering (Network Security Use)

Many routers allow **MAC filtering**, which means:

- Only **approved MAC addresses** can connect to Wi-Fi.
- Used to **restrict devices** from connecting.

However, **not a strong security measure** — attackers can spoof MAC addresses.