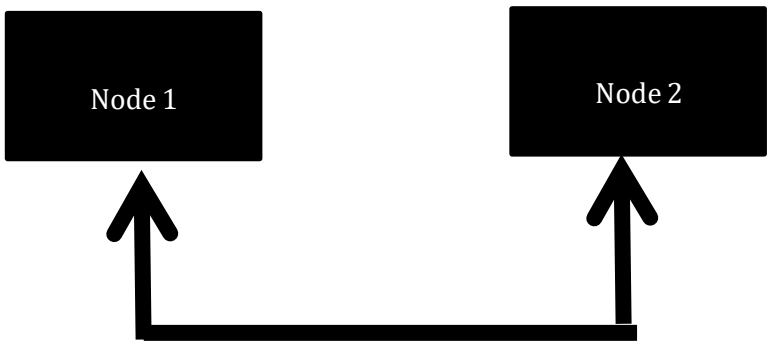
Table of Contents

Networking

When two or more communication devices are interconnected with each other through a transmission medium — such as cables, optical fibers, or wireless signals — they form a **network**. A network enables these devices to exchange data, share resources (like files, printers, or internet connections), and communicate efficiently regardless of their physical location. Depending on its size and scope, a network can be classified into types such as **LAN (Local Area Network)**, **MAN (Metropolitan Area Network)**, and **WAN (Wide Area Network)**. The medium of connection can be **wired** (e.g., Ethernet cables) or **wireless** (e.g., Wi-Fi, Bluetooth, cellular). Networks are the backbone of modern communication, supporting everything from simple email exchanges to complex real-time applications like video conferencing and cloud computing.



A node in a computer network is any device capable of sending, receiving, or forwarding information. Common examples include personal computers, printers, modems, switches, hubs, bridges, servers, and other devices connected via Wi-Fi or Ethernet. Nodes are essential components that make up a network, and they must have some form of identification, such as an IP address or MAC address, to be recognized by other network devices.

Need of network

1. Information Sharing (Data communication)
2. Resource sharing e.g web server.

Components of data server communication.

There are five components of data communications

1. Message: It can be a text, picture, audio, video etc.
2. Sender: It can be a mobile phone, laptop, computer, walky-talky etc.
3. Receiver: It can be a mobile phone, laptop, Computer, Walkie-Talkie etc.
4. Medium: It can be a cable, Radio, Waves Microwaves etc.
5. Protocol: It is set of rules that determine how data is sent and received over a network.

Modes of communication:

There are three modes of communication in networking.

1. Simple mode
2. Half-duplex mode
3. Full-duplex mode

1. **Simplex mode**: In simplex transmission mode, the communication between sender and receiver occurs in only one direction. The sender can only send the data and the receiver can only receive the data e.g., radio, television etc.
2. **Half-duplex mode**: In half-duplex mode, both devices can transmit signals but one at a time. If node 2 sends data at time and node 2 can only receive and vice versa. E.g. Walky-Talky.
3. **Full-duplex mode**: In full duplex mode, communication is capable of network data transmission at the same time e.g. mobile phones, laptops, computers etc.

Topologies

Topology is the geographical representation of our network. There are five types of topologies.

1. Mesh topology
2. Star topology
3. Bus topology
4. Ring topology
5. Tree topology

Mesh Topology

In this topology every device is connected to another device with a particular link.

Advantages

1. If one link become unreachable it does not harm the entire system.
2. It is easy trouble shot.

Disadvantage:

1. A full mesh network can be very expensive
2. It is difficult to install and reconfigure

Star topology

The star topology with a central device called. Hub and the sharing of data is only possible through

Hub.

Advantages:

1. It proadcast the message.
2. It is less expensive due to less cabeling.
3. Easy to connect new modes without effecting rest of modes.

Disadvantage

1. In star topology we must require a network device like hub or switch like.
2. If two modes went to share the data sharing is only possible through.
3. If hub is failed entire network will be fail .
4. We cant send private data .

Bus topology

The bus topology is designed in such a way that all the station are connected through a single cable each mode is either connected to backbone cable by drop cable or directly connected to the backbone cable . when a node was send to message our the network.

Advantages

1. Low cost cables : In bus topology modes are directly connect to the backbone cable without passing through a hub or switch.
2. Moderate data speed : co axil or turned pair cables are mainly used in the link topology that support upto 10 mbps .

Disadvantage

1. There are huge threat of traffic jam
2. Attention is a loss of signal leads to communicate issues. Repeats are used to regenerate the signals.

Ring topology

1. Ring topology is a network topology in which each mode connects to exactly two other immediate nodes forming a signal continuous path way for signal through each mode called as ring topology.

Advantages

1. All data flows in one direction reducing the chances of packets
2. A network server is not needed to controls network connectivity between work stations.

Disadvantages

1. All data being transferred our the network must pass through each work station on the network which can make it slower and dangerous.
2. The entire network will be impacted if one work station shut down.

Tree topology

A tree network or star bus network is hybrid network topology in which star network are interconnected via link network.

Tree network are heirachal in nature and each node can have an arbiratary no. of child nodes.

Mediums of network

We have two types of medium through which we can create a network.

1. Guided medium
2. Un-Guided medium

Guided medium/physical/wired

Guided Media is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

E.g. Optical fibre cable, Co-axial cable, Twisted pair cable, Two wire open line.

Features:

- High Speed
- Secure
- Used for comparatively shorter distances

Un-Guided medium/Wireless Technology

Unguided media is a type of Transmission Media. A transmission medium is a physical path between the transmitter and the receiver. Unguided media transport electromagnetic waves without using a physical conductor. It is also known as unbounded or wireless media, and does not rely on physical pathways to transmit signals.

e.g. Radio waves, Microwaves, Infrared, Bluetooth

Types of network

There are 4 types of network

1. LAN (Local Area Network)
2. MAN (Metropolitian Area Network)
3. WAN (Wide Area Network)
4. PAN (Personal Area Network)

1. **Local Area Network (LAN)**
   LAN is the most frequently used network. A LAN is a computer network that connects computers through a common communication path, contained within a limited area, that is, locally. A LAN encompasses two or more computers connected over a server. The two important technologies involved in this network are Ethernet and Wi-fi. It ranges up to 2km & transmission speed is very high with easy maintenance and low cost. Examples of LAN are networking in a home, school, library, laboratory, college, office, etc.

2. **Metropolitan Area Network (MAN)**
   A MAN is larger than a LAN but smaller than a WAN. This is the type of computer network that connects computers over a geographical distance through a shared communication path over a city, town, or metropolitan area. This network mainly uses FDDI, CDDI, and ATM as the technology with a range from 5km to 50km. Its transmission speed is average. It is difficult to maintain and it comes with a high cost. Examples of MAN are networking in towns, cities, a single large city, a large area within multiple buildings, etc.
3. **Wide Area Network (WAN)**
   WAN is a type of computer network that connects computers over a large geographical distance through a shared communication path. It is not restrained to a single location but extends over many locations. WAN can also be defined as a group of local area networks that communicate with each other with a range above 50km. Here we use Leased-Line & Dial-up technology. Its transmission speed is very low and it comes with very high maintenance and very high cost. The most common example of WAN is the Internet.
4. **PAN (Personal Area Network)**
   PAN is the most basic type of computer network. It is a type of network designed to connect devices within a short range, typically around one person. It allows your personal devices, like smartphones, tablets, laptops, and wearables, to communicate and share data with each other. PAN offers a network range of 1 to 100 meters from person to device providing communication. Its transmission speed is very high with very easy maintenance and very low cost. This uses Bluetooth, IrDA, and Zigbee as technology. Examples of PAN are USB, computer, phone, tablet, printer, PDA, etc.

Networking Device

Network devices are physical devices that allow hardware on a computer network to communicate and interact with each other. Network devices like hubs, repeaters, bridges, switches, routers, gateways, and brouters help manage and direct data flow in a network. They ensure efficient communication between connected devices by controlling data transfer, boosting signals, and linking different networks.

Below are some common network devices used in modern networks:

- Access Point
- Modems
- Firewalls
- Repeater
- Hub
- Bridge
- Switch
- Routers
- Gateway
- Brouter
- NIC

1. **Access Point (AP)** A device that allows wireless devices (like laptops, smartphones) to connect to a wired network using Wi-Fi. It acts as a bridge between wireless clients and the wired LAN.
2. **Modem** Short for *Modulator–Demodulator*. Converts digital signals from a computer into analog signals for transmission over telephone lines (or vice versa), enabling internet access. Modern modems can also work with cable or fiber connections.
3. **Firewall** A hardware device or software system that monitors and controls incoming and outgoing network traffic based on security rules. It acts as a barrier between a trusted internal network and untrusted external networks (like the internet).
4. **Repeater** A device that receives a network signal, amplifies it, and retransmits it to extend the range of the network. Used to overcome signal loss over long distances.
5. **Hub** A basic networking device that connects multiple computers in a LAN and broadcasts incoming data to all connected devices. It works at the physical layer (Layer 1) of the OSI model and does not filter traffic.
6. **Bridge** A device that connects and filters traffic between two network segments, reducing collisions. Works at the data link layer (Layer 2) and uses MAC addresses to forward data.
7. **Switch** An intelligent device that connects multiple devices in a LAN and forwards data only to the specific device (port) it is intended for. Works at the data link layer (Layer 2) and improves network efficiency compared to hubs.
8. **Router** A device that connects different networks together (e.g., a home network to the internet) and directs data packets based on IP addresses. Works at the network layer (Layer 3).

9. **Gateway** A device that connects networks using different protocols and translates data between them. It can operate at any OSI layer depending on its function.
10. **Brouter** Short for *Bridge Router*. A device that can function both as a bridge (forwarding data based on MAC addresses) and as a router (forwarding data based on IP addresses).
11. **NIC (Network Interface Card)** A hardware component inside a computer or device that allows it to connect to a network. It can be wired (Ethernet) or wireless (Wi-Fi).

Or

1. **Access Point** – Lets wireless devices (like phones or laptops) connect to a wired network using Wi-Fi.
2. **Modem** – Connects your home or office to the internet by changing signals from your provider into a form your devices can use.
3. **Firewall** – Protects a network by blocking unwanted or unsafe connections.
4. **Repeater** – Boosts a weak network signal so it can travel farther.
5. **Hub** – Connects several devices in a network and sends data to all of them.
6. **Bridge** – Connects two separate networks so they can work as one.
7. **Switch** – Connects devices in a network and sends data only to the device that needs it.
8. **Router** – Connects different networks (like your home network to the internet) and directs data to the right place.
9. **Gateway** – Links two networks that use different rules so they can share data.
10. **Brouter** – Works as both a bridge and a router.
11. **NIC (Network Interface Card)** – A part inside a computer or device that lets it connect to a network (wired or wireless).

Networking Address

A network address is a logical or physical identifier that uniquely identifies a device or host within a telecommunication network. These addresses are essential for the communication and identification of devices in a network. Common examples of network addresses include IP addresses, MAC addresses, and telephone numbers.

Types of Network Addresses

IP Addresses

An IP address is a 32-bit numeric address used to identify a node in an IP network. It is represented in dot-decimal notation, such as 192.168.1.1. IP addresses are divided into two parts: the network ID and the host ID. The network ID identifies the network, while the host ID identifies the specific device within that network.

- Think of it like a **house address** on the internet.

- It's a number (like `192.168.1.1`) that tells other devices **where** your device is so they can send data to it.

- It has two parts:

  - **Network ID** → like the street name (tells which network you're on).
  - **Host ID** → like the house number (tells which device on that network).

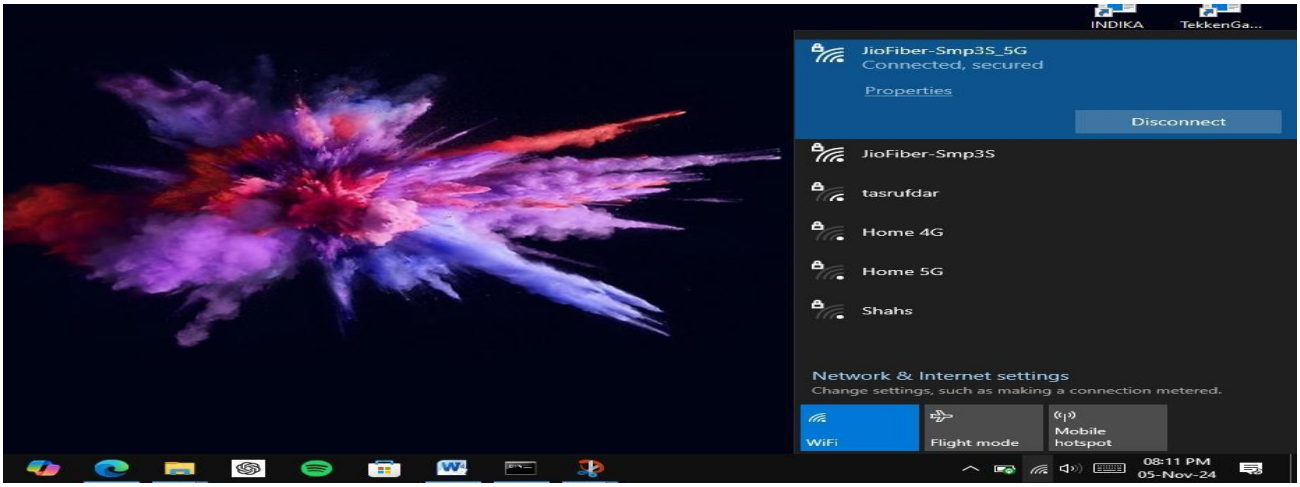
MAC Addresses

A MAC address is a unique identifier assigned to network interfaces for communications at the data link layer of a network segment. It is used to ensure that data packets are delivered to the correct device on a local network.

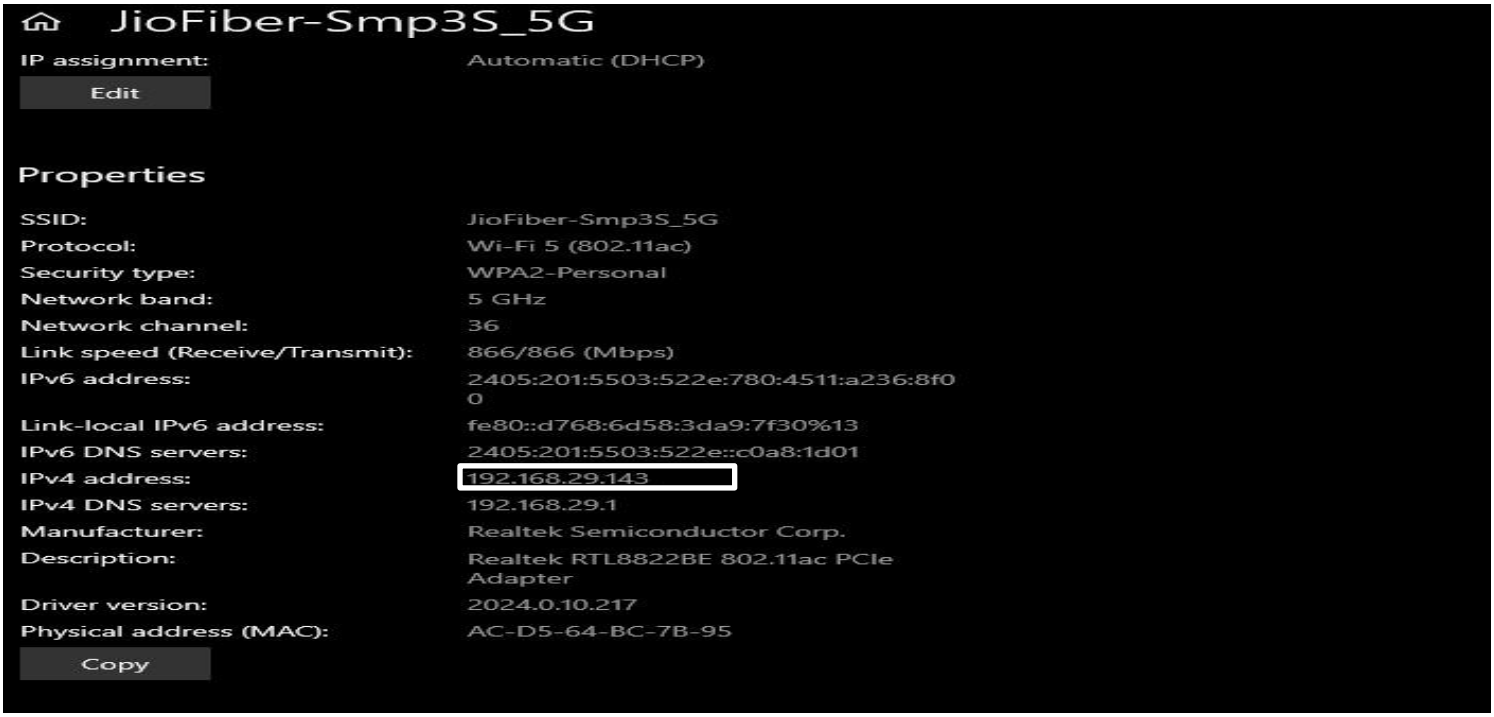
- Think of it like your device's **fingerprint** — it's unique and built into your network card.
- It's used inside a local network (like inside your home or office) to make sure data goes to the **exact** device it's meant for.
- Even if two devices are on the same network, their MAC addresses will always be different.

How to find IP Address in Windows 10 for wifi

1. On the taskbar, select **Wi-Fi network** > the Wi-Fi network you're connected to > **Properties**.



2. Under **Properties**, look for your IP address listed next to **IPv4 address**.



Or

You can open CMD (Command Prompt) and type Ipconfig in it.