What is a Computer Networks?

A computer network is a collection of interconnected devices (computers, servers, routers, etc.) that communicate with each other to share data, resources, and services.

Uses of Computer Networks

- Communicating using email, video, instant messaging, etc.
- Sharing devices such as printers, scanners, etc.
- Sharing files.
- Sharing software and operating programs on remote systems.
- Allowing network users to easily access and maintain information.

Advantages of Computer Network

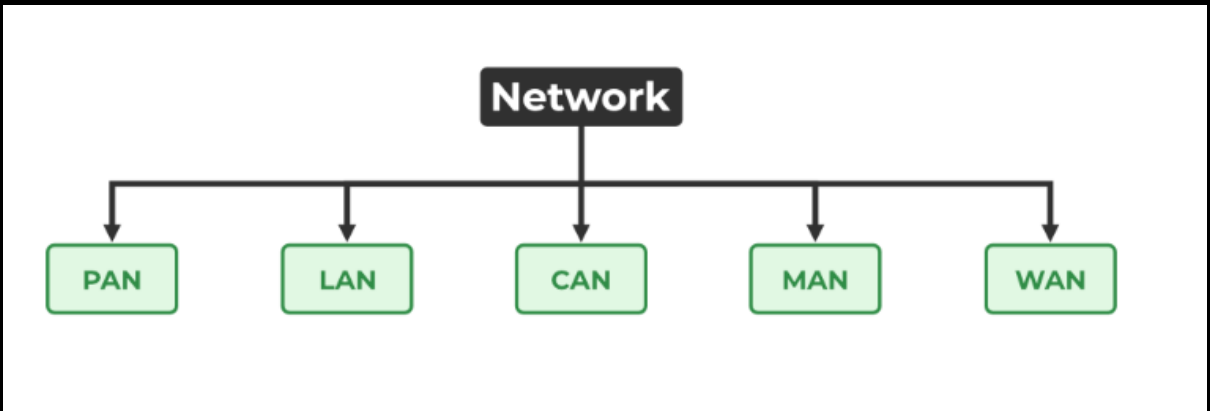
- **Central Storage of Data:** Files are stored on a central storage database which helps to easily access and available to everyone.
- **Connectivity:** A single connection can be routed to connect multiple computing devices.
- **Sharing of Files:** Files and data can be easily shared among multiple devices which helps in easily communicating among the organization.
- **Security through Authorization:** Computer Networking provides additional security and protection of information in the system.

Disadvantages of Computer Network

- **Virus and Malware:** A virus is a program that can infect other programs by modifying them. Viruses and Malware can corrupt the whole network.
- **High Cost of Setup:** The initial setup of Computer Networking is expensive because it consists of a lot of wires and cables along with the device.
- **loss of Information:** In case of a System Failure, might lead to some loss of data.
- **Management of Network:** Management of a Network is somehow complex for a person, it requires training for its proper use.

Types / Classification of Networks:

https://www.geeksforgeeks.org/types-of-computer-networks/



- Range, Examples, Technologies involved
- Types of PAN
- Advantages of PAN
- Disadvantages of PAN
- Applications of PAN

Parameters	PAN	LAN	CAN	MAN	WAN
Full Name	Personal Area Network	Local Area Network	Campus Area Network	Metropolitan Area Network	Wide Area Network
Technology	Bluetooth, IrDA,Zigbee	Ethernet & Wifi	Ethernet	FDDI, CDDi. ATM	Leased Line, Dial-Up
Range	1-100 m	Upto 2km	1 – 5 km	5-50 km	Above 50 km
Transmission Speed	Very High	Very High	High	Average	Low
Ownership	Private	Private	Private	Private or Public	Private or Public
Maintenance	Very Easy	Easy	Moderate	Difficult	Very Difficult
Cost	Very Low	Low	Moderate	High	Very High

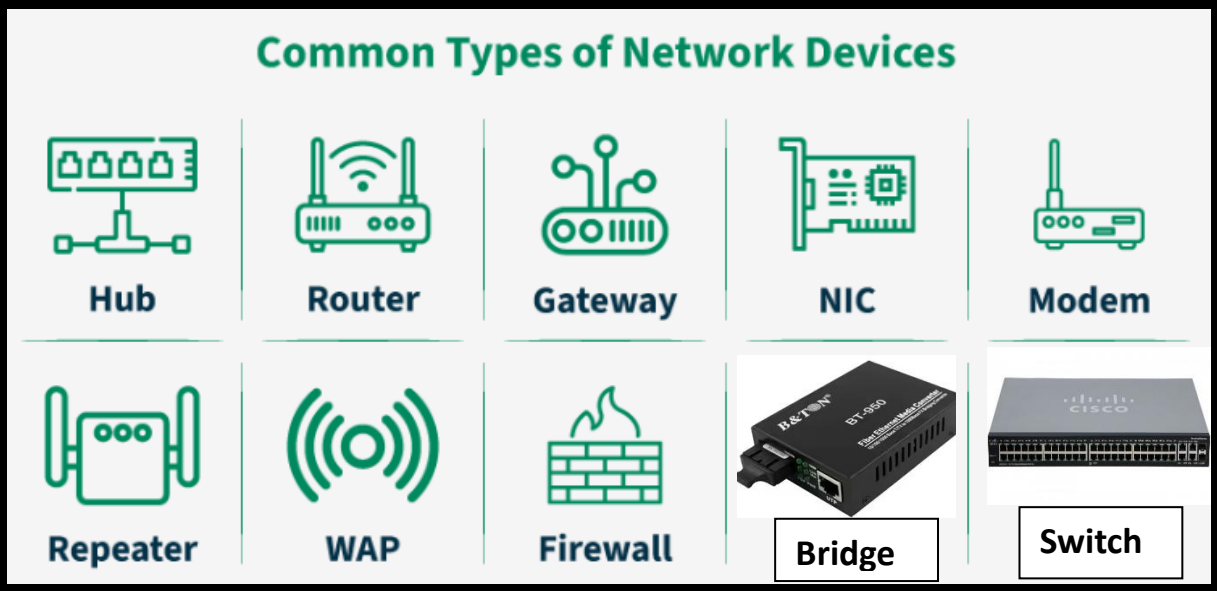
Networking is everywhere:

- ✓ Networks support the way we learn.
- ✓ Networks support the way we communicate.
- ✓ Networks support the way we work.
- ✓ Networks support the way we play.

Network Devices:

https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/

Network devices are physical devices that allow hardware on a computer network to communicate and interact with each other. These devices enable communication, data transfer, and efficient management of network traffic. Below are the main network devices:



Functions of Network Devices

- Network devices help to send and receive data between different devices.
- Network devices allow devices to connect to the network efficiently and securely.
- Network devices Improve network speed and manage data flow better.
- It protect the network by controlling access and preventing threats.
- Expand the network range and solve signal problems.

1. Hub

A hub is a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. Layer 2 (DLL) Device.

- **Function**:
  - Acts as a basic connection point for devices in a LAN.
  - Broadcasts data packets to all devices connected to it.

- **Types**:

1. **Active Hub**: Amplifies signals before broadcasting.
2. **Passive Hub**: Simply forwards signals without amplification.

- **Disadvantages**:
  - Inefficient due to broadcasting data to all devices.
  - Causes network congestion in larger networks.

- **Use Case**:
  - Rarely used today due to inefficiency; replaced by switches.

2. Router

A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.

Function:

- Connects multiple networks (e.g., a LAN to the Internet).
- Routes data packets between devices using IP addresses.
- Supports features like Network Address Translation (NAT) and Dynamic Host Configuration Protocol (DHCP).

- NAT is a process in which one or more local IP addresses are translated into one or more Global IP addresses and vice versa to provide Internet access to the local hosts.
- DHCP automates the process of assigning IP addresses, which can be especially useful for large networks
- DHCP makes it easier for network administrators to add or move devices

Applications:

- Home Internet connectivity.
- Enterprise-level routing and traffic control.

3. Gateway

A gateway is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer of the OSI model. Gateways are generally more complex than switches or routers.

Function:

- Acts as an entry and exit point between two different networks.
- Converts data formats, protocols, or addresses to ensure compatibility.
- They can be unidirectional or bidirectional, meaning data can only pass in one direction or in both directions.

Examples:

- Connecting an enterprise network to the Internet.
- Translating communication between IPv4 and IPv6 networks.

4. NIC

NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and the router or modem. NIC card is a layer 2 device which means that it works on both the physical and data link layers of the network model.

Function:

- NIC allows both wired and wireless communications.

Role:

- Each NIC has its own unique MAC address, which is used to identify a device on a network
- Transmits and receives data packets over the network.

5. Modems (Modulation -> Transmission -> Demodulation)

Modems is also known as modulator/demodulator, is a network device that is used to convert digital signal into analog signal of different frequencies and transmits these signal to a modem at the receiving location. These converted signals can be transmitted over the cable systems, telephone lines, and other communication mediums. A modem is also used to convert analog signal back into digital signal. Modems are generally used to access internet by customers of an Internet Service Provider (ISP).

Function:

- This allows devices to send and receive data over telephone lines or cable networks.
- It convert the analog signals that come from telephone wire into a digital form. In digital form, these converted signals are stored in the form of 0s and 1s.

Applications:

- Accessing the Internet in homes and businesses.

6. Repeater

A repeater operates at the physical layer. Its main function is to amplify (i.e., regenerate) the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device.

Function:

- Boosts signals in a network to extend the distance of data transmission.

Applications:

- Used in large networks to ensure reliable communication.
- Extends the range of Wi-Fi or wired networks.

7. WAP

WAP can stand for Wireless Application Protocol or Wireless Access Point.

It is a protocol designed for micro-browsers and it enables access to the internet in mobile devices. It uses the markup language WML (Wireless Markup Language and not HTML), WML is defined as an XML 1.0 application. It enables the creation of web applications for mobile devices in 1998.

Wireless Access Point (WAP) is used to create the WLAN (Wireless Local Area Network), it is commonly used in large offices and buildings which have expanded businesses.

It is easier and simpler to understand and implant the device. It can be fixed, mobile or hybrid proliferated in the 21st century. The availability, confidentiality, and integrity of the communication and network are a responsibility and to be ensured about that.

Application of Wireless Access Point:

1. It is a device that creates a WLAN (Wireless Local Area Network) in large enterprises.
2. It is used to extend the coverage area of the network so that it can’t disconnect which allows more users to connect to the network easily.
3. LANs can also be provided in public places such as coffee shops, restaurants, airports, etc.
4. Wireless Printing: Wireless printers can be connected to the network and then users can print anywhere within the range of the access point.

5. Cloud services: Wireless access points can be used to connect devices to cloud services, allowing for data backup and synchronization across multiple devices.

8. Firewalls

A firewall is a network security device that monitors and controls the flow of data between your computer or network and the internet. It acts as a barrier, blocking unauthorized access while allowing trusted data to pass through. Firewalls help protect your network from hackers, viruses, and other online threats by filtering traffic based on security rules. Firewalls can be physical devices (hardware), programs (software), or even cloud-based services, which can be offered as SaaS, through public clouds, or private virtual clouds.

Function:

- Protects the network by monitoring and controlling incoming and outgoing traffic based on predefined security rules.

Types:

1. **Hardware Firewall**: Dedicated device placed between the network and the Internet.
2. **Software Firewall**: Installed on individual devices to protect them.

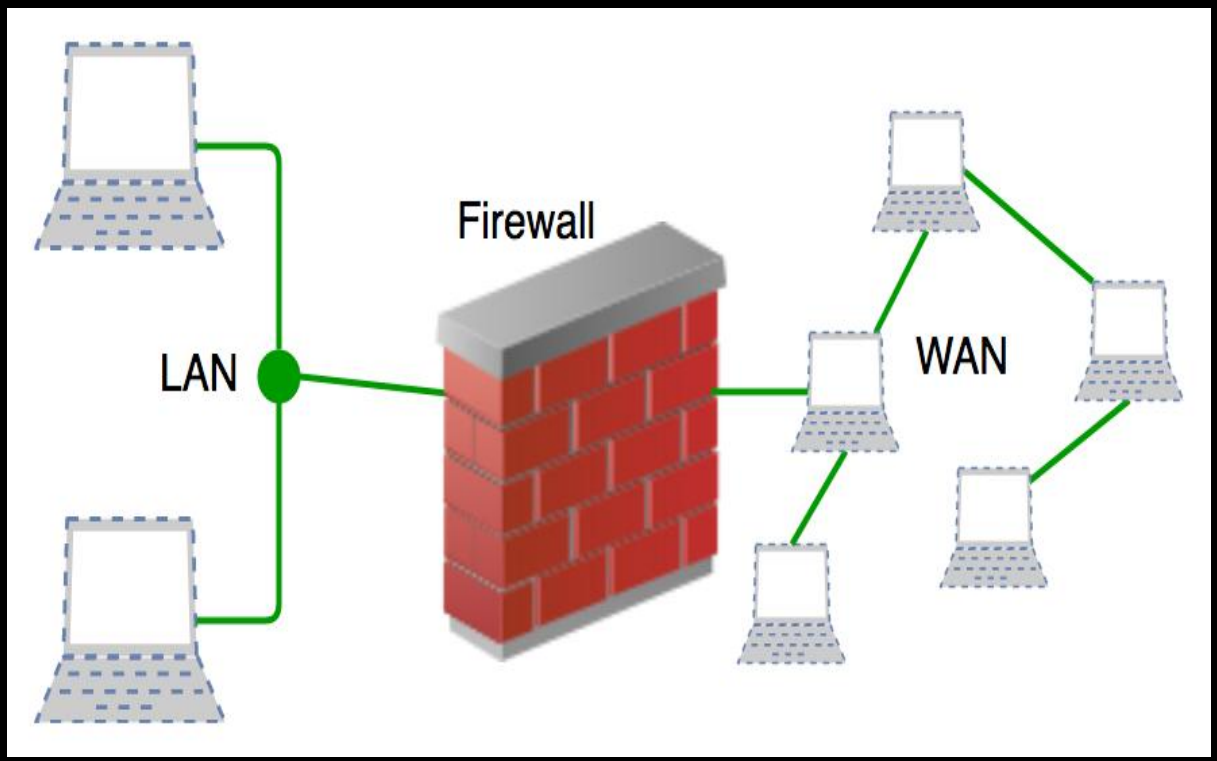
Features:

- Packet filtering, stateful inspection, proxy services.

Applications:

- Safeguarding networks from external threats like hackers and malware.


DC12V
LAN-I
LAN-II
LAN-III
LAN-IV
LAN-V
LAN-VI


Firewall
LAN
WAN

9. Bridge

A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It typically connects multiple network segments and each port is connected to different segment. A bridge is not strictly limited to two ports, it can have multiple ports to connect and manage multiple network segments. Modern multi-port bridges are often called Layer 2 switches because they perform similar functions.

Function:

- Connects two or more network segments within the same network to operate as a single LAN.

Advantages:

- Reduces traffic by dividing networks into smaller segments.
- Improves overall network performance.

10. Switch:

A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

Function:

- Connects devices within a Local Area Network (LAN).
- Uses MAC addresses to forward data only to the intended recipient, making it efficient.

Advantages:

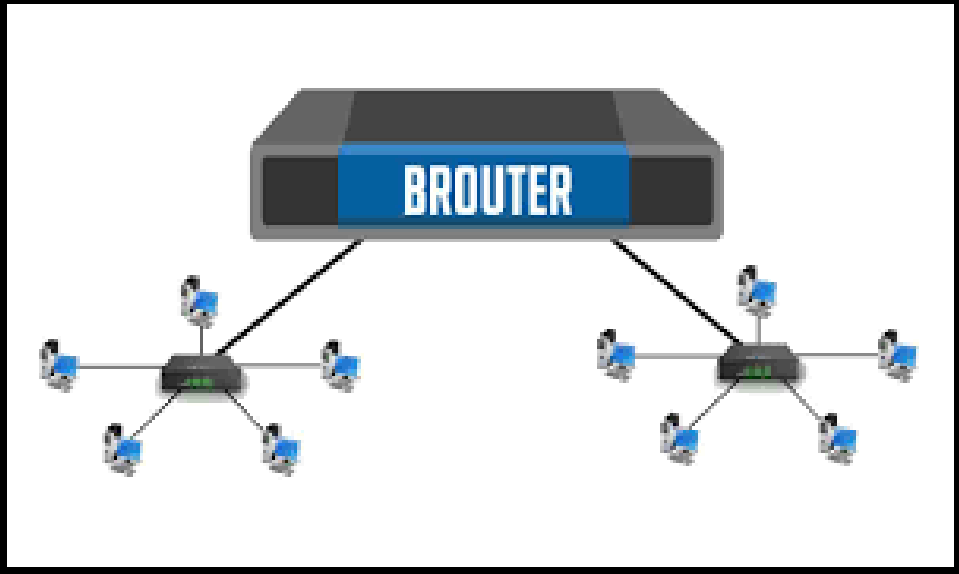
- Faster than hubs due to intelligent data forwarding.
- Reduces network congestion by isolating data traffic.

11. Brouter

A **Brouter** is a hybrid networking device that combines the functionalities of both a **bridge** and a **router**. It can operate at both the **data link layer** (Layer 2) and the **network layer** (Layer 3) of the OSI model.

Applications of a Brouter:

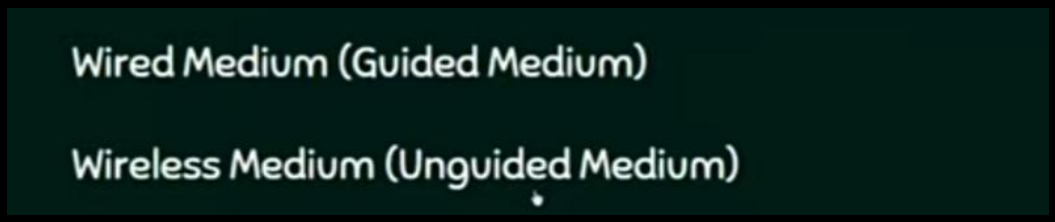
1. **Mixed Network Environments**:
    - Used in networks where both bridging and routing capabilities are needed.
2. **Legacy Systems**:
    - Suitable for older networks that require compatibility with both bridged and routed traffic.
3. **Protocol-Specific Scenarios**:
    - Helpful in environments with unsupported or proprietary protocols that need bridging.

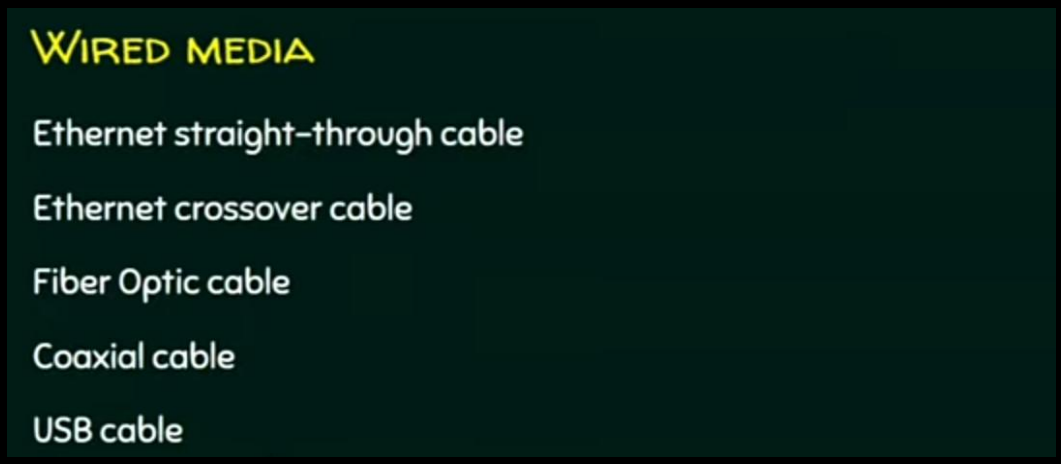


Device	Function	Types	Advantages/Disadvantages	Applications
Hub	Basic connection for LAN, broadcasts data to all devices	Active Hub: Amplifies signals Passive Hub: Forwards without amplification	**Advantages:** Simple **Disadvantages:** Inefficient, network congestion	Rarely used, replaced by switches
Router	Connects networks, routes data using IP addresses	Wired Router, Wireless Router, Edge Router, Core Router	**Advantages:** Enables internet access, traffic control **Disadvantages:** Can be expensive	Home/enterprise internet connectivity, traffic management
Gateway	Connects networks with different protocols, acts as a translator	-	**Advantages:** Enables compatibility between networks **Disadvantages:** More complex than switches/routers	Connecting enterprise networks, IPv4/IPv6 translation
NIC	Connects a computer to a network	Ethernet NIC: Wired connections Wireless NIC: Wi-Fi	**Advantages:** Assigns MAC address **Disadvantages:** Limited to device-specific installations	Enables wired/wireless device connectivity

Modem	Converts digital signals to analog and vice versa	DSL Modem, Cable Modem, Fiber Optic Modem	**Advantages:** Internet access **Disadvantages:** Limited to ISP and medium	Internet connectivity at homes/businesses
Repeater	Amplifies and regenerates network signals	-	**Advantages:** Extends transmission range **Disadvantages:** Doesn't filter data	Large networks, Wi-Fi signal extension
WAP	Creates Wireless LANs, extends network coverage	-	**Advantages:** Wireless connectivity, mobility **Disadvantages:** Security concerns in unmanaged environments	Large enterprises, public spaces, cloud services
Firewall	Monitors and controls network traffic for security	Hardware Firewall, Software Firewall	**Advantages:** Blocks threats **Disadvantages:** May reduce performance	Safeguards networks from hackers, viruses
Bridge	Connects and filters network segments	Transparent Bridge, Source Routing Bridge	**Advantages:** Reduces traffic, improves performance **Disadvantages:** Limited to same network protocol	Connecting LAN segments
Switch	Intelligent data forwarding within LAN	Unmanaged Switch, Managed Switch, Layer 3 Switch	**Advantages:** Efficient traffic control **Disadvantages:** Higher cost for managed switches	High-performance LANs
Brouter	Combines bridging and routing functionalities	-	**Advantages:** Handles mixed traffic **Disadvantages:** More complex, not widely used	Mixed protocol environments, legacy systems

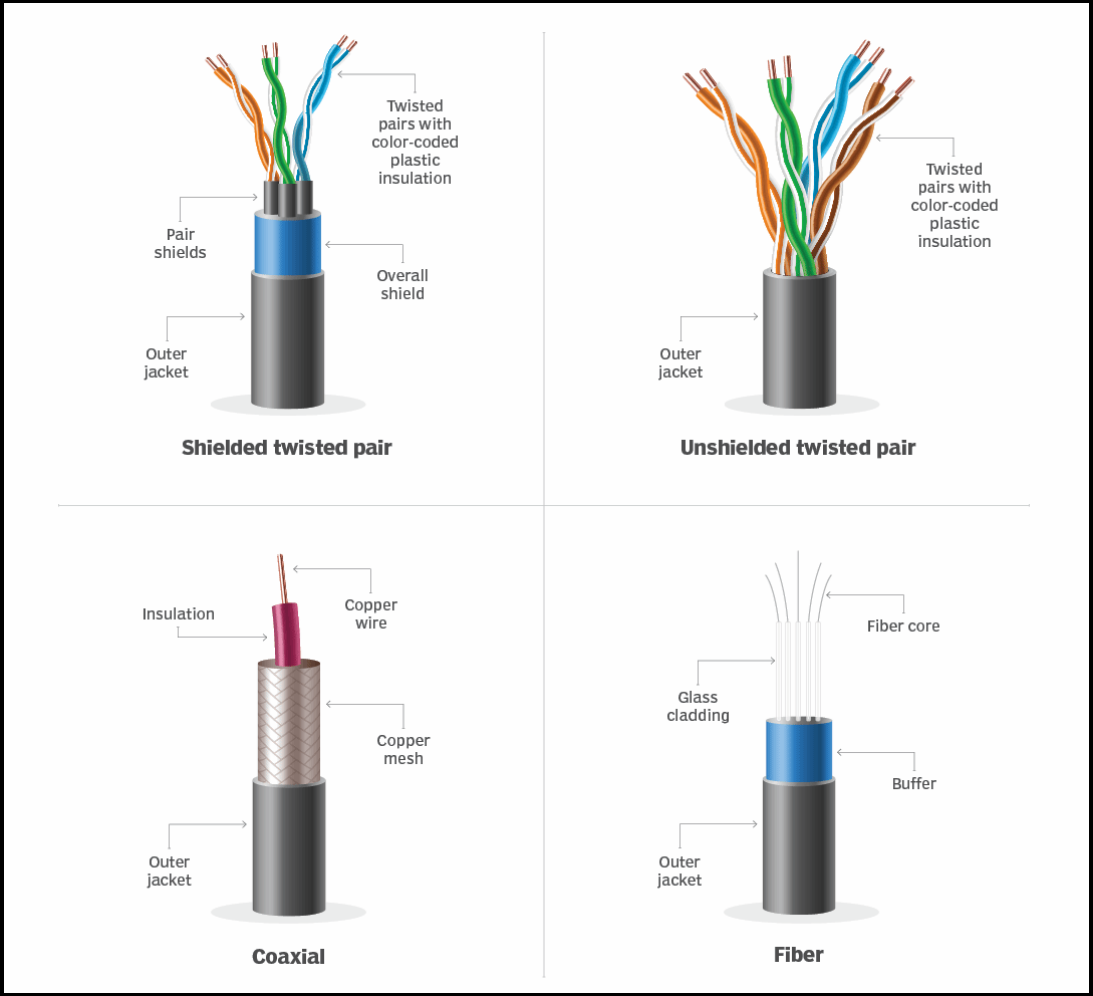
Media:





The Four Main Types of Network Cables

Network cables are essential components of any communication system and are categorized into four main types: coaxial, shielded twisted pair (STP), unshielded twisted pair (UTP), and fiber optic cables.



1. Coaxial Cables

Coaxial cables are designed with a central conductor surrounded by an insulating plastic layer, a metal shield, and an outer protective sheath. This layered structure minimizes external interference and safeguards the conductor, which transmits electromagnetic signals.

- **Core Structure**: The central conductor (core) can be single-core or multi-core, depending on the number of wires.
- **Protection**: The metal shield prevents external interference, while the plastic insulation protects the core from physical damage.

- **Usage**: Coaxial cables were widely used in early computer networks but have since been replaced by more advanced options.

2. Shielded Twisted Pair (STP) Cables

STP cables, commonly used in business networks, are specifically designed to minimize interference and allow for extended cable distances.

- **Structure**: These cables consist of four color-coded wire pairs, twisted and shielded with a metal layer, and encased in a durable plastic sheath.
- **Applications**: Ideal for environments with high levels of electromagnetic interference (EMI), STP cables provide reliable performance in complex installations.

3. Unshielded Twisted Pair (UTP) Cables

UTP cables are widely used in industrial computing and telecommunications due to their affordability and effectiveness in minimizing EMI.

- **Structure**: Similar to STP cables, UTP cables feature twisted wire pairs encased in a plastic sheath, but they lack the additional metal shielding.
- **Advantages**: While less resistant to interference than STP cables, UTP cables are cost-effective and sufficient for most standard applications.

4. Fiber Optic Cables

Fiber optic cables are advanced networking cables with a core made of glass or plastic, surrounded by cladding, buffer layers, and an outer jacket for durability and protection.

- **Features**: These cables are highly resistant to external interference and capable of transmitting data over long distances at high speeds.

- **Types**:
    - **Single-Mode Fiber (SMF)**: Optimized for long-distance data transmission.
    - **Multi-Mode Fiber (MMF)**: Supports higher data volumes over shorter distances.

- **Applications**: Fiber optic cables are the standard choice for connecting networks across distant locations, offering unmatched speed and reliability.

Derivations from analogy

Reaching our city = Reaching our network. (IP Address)

Reaching our Apartment = Reaching the host. (MAC Address)

Reaching the right person = Reaching the right process. (Port Address)

IP Address

IP stands for Internet Protocol.

Every node in the computer network is identified with the help of IP address.

IP Address (IPV4)

- ★ Every node in the computer network is identified with the help of IP address.
- ★ Logical address.
- ★ Can change based on the location of the device.
- ★ Assigned by manually or dynamically.
- ★ Represented in decimal and it has 4 octets (x.x.x.x).
- ★ 0.0.0.0 to 255.255.255.255 (32 bits).

MAC Address

MAC stands for Media Access Control.

Every node in the LAN is identified with the help of MAC address.

IP Address = Location of a person.

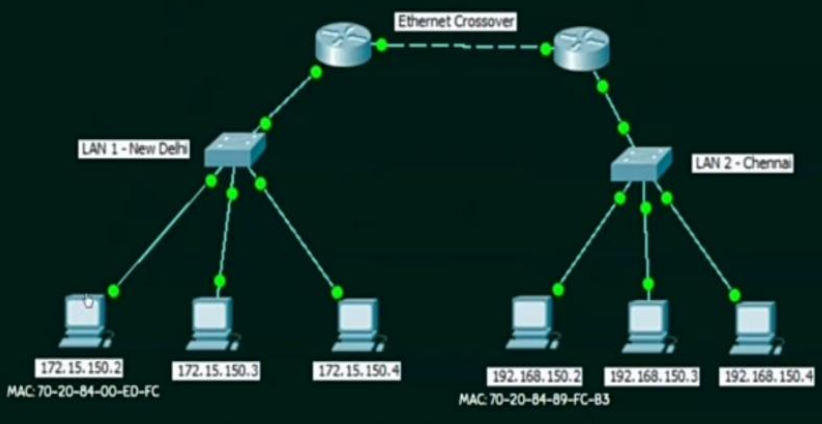
MAC Address = Name of the person.

MAC Address

- ★ Every node in the LAN is identified with the help of MAC address.
- ★ Physical address or Hardware Address.
- ★ Unique.
- ★ Cannot be changed.
- ★ Assigned by the manufacturer.
- ★ Represented in hexadecimal.
- ★ Example: 70-20-84-00-ED-FC (48 bits).
- ★ Separator: hyphen(-), period(.), and colon(:).

MAC Address

- ★ Every node in the LAN is identified with the help of MAC address.



IP Address Vs MAC Address

IP Address	MAC Address
Needed for communication.	Needed for communication.
32 bits.	48 bits.
Represented in Decimal.	Represented in hexadecimal.
Router needs IP Address to forward data.	Switch needs MAC address to forward data
Example: 10.10.23.56	Example: 70-20-84-00-ED-FC

Activity Time

Identify the valid and invalid IP addresses in the following set and place the options in the appropriate columns.

a. 24.25.26.8
b. 10.3.156.256
c. 0.0.0.0
d. 255.255.255.255
e. 100.2.6.345.456
f. 16.2e.45.67

Valid IP Addresses	Invalid IP Addresses

Port Address or Port Number

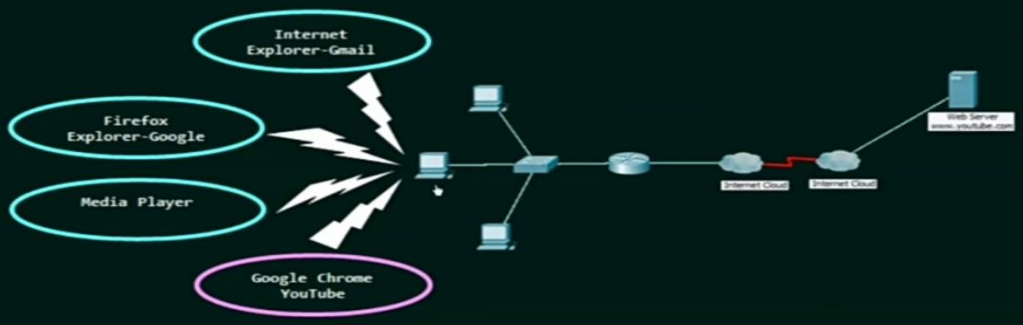
- ★ In a node, many processes will be running.
- ★ Data which are sent/received must reach the right process.
- ★ Every process in a node is uniquely identified using port numbers.
- ★ Port = Communication endpoint.
- ★ Fixed port numbers and dynamic port numbers (0 – 65535)

Example:

Fixed port numbers : 25, 80 etc.,

OS assigned dynamic port numbers : 62414.

Port Address or Port Numbers



Port Address or Port Numbers