Data Communication is defined as exchange of data between two devices via some form of transmission media such as a cable, wire or it can be air also. For occurrence of data communication, communicating devices must be a part of a communication system made up of a combination of hardware or software devices and programs.

The effectiveness of a data communication depends upon the 4 fundamental characteristics:

1. *Delivery: The system must deliver the data to the correct destination.*
2. *Accuracy: The system must deliver the data accurately.*
3. *Timeliness: The system must deliver the data in a timely manner.*
4. *Jitter: Jitter refers to the variation in the packet arrival time. It is the uneven delay in the arrival of audio or video packets.*

Data Communication System Components:

There are mainly five components of a data communication system:

1. Message
2. Sender
3. Receiver
4. Transmission Medium **5.** Set of rules (Protocol)

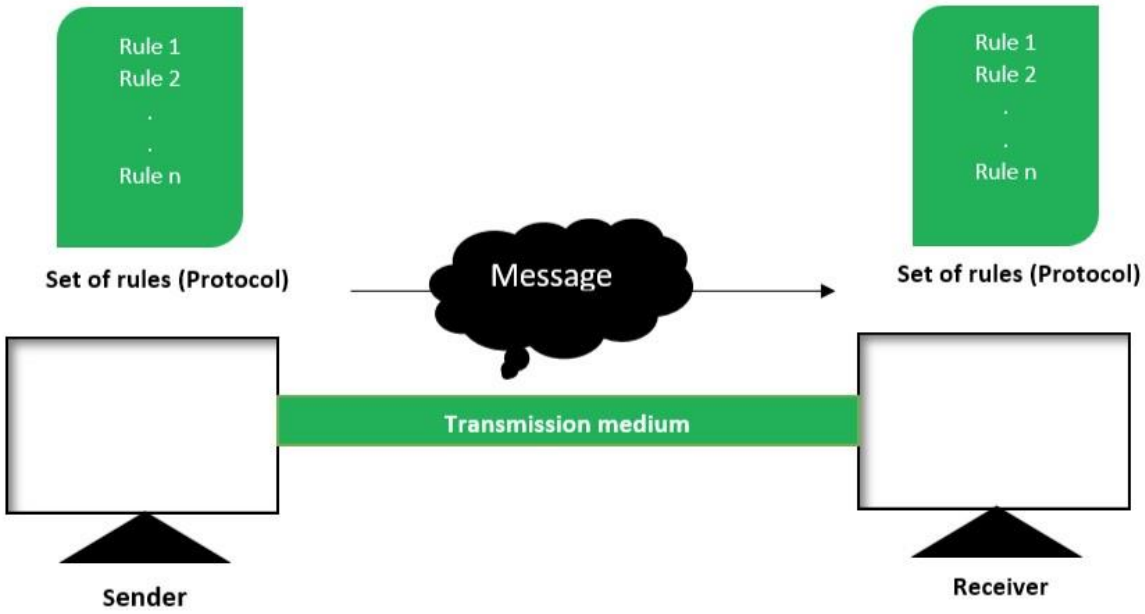


Figure – Components of Data Communication System

Message:

This is the most useful asset of a data communication system. The message simply refers to data or piece of information which is to be communicated. A message could be in any form, it may be in the form of a text file, an audio file, a video file, etc.

Sender:

To transfer a message from source to destination, someone must be there who will play the role of a source. Sender plays part of a source in a data communication system. It is simply a

device that sends data messages. The device could be in the form of a computer, mobile, telephone, laptop, video camera, or a workstation, etc.

Receiver:
It is the destination where the final message sent by source has arrived. It is a device that receives messages. Same as sender, receiver can also be in the form of a computer, telephone mobile, workstation, etc

Transmission medium:
In the entire process of data communication, there must be something which could act as a bridge between sender and receiver, Transmission medium plays that part. It is the physical path by which data or message travels from sender to receiver. Transmission mediums could be guided (with wires) or unguided (without wires), for example, twisted pair cable, fiber optic cable, radio waves, microwaves, etc.

Set of rules (Protocol):
To govern data communications, various sets of rules had been already designed by the designers of the communication systems, which represent a kind of agreement between communicating devices. These are defined as protocol. In simple terms, the protocol is a set of rules that govern data communication. If two different devices are connected but there is no protocol among them, there would not be any kind of communication between those two devices. Thus the protocol is necessary for data communication to take place.

Example:-
A typical example of a data communication system is sending an e-mail. The user which send email act as sender, message is data which user wants to send, receiver is one whom user wants to send message, there are many protocols involved in this entire process, one of them is Simple Mail Transfer Protocol (SMTP), both sender and receiver must have an internet connection which uses a wireless medium to send and receive email.

Computer Network:

A **computer network** is a set of connected computers. Computers on a network are called **nodes**. The connection between computers can be done via cabling, most commonly the Ethernet cable, or fiber optic cable. Computer network is defined as the interconnection of two or more computers or networking devices with the help of transmission media and set of protocols.

Purpose of Networking (Advantages)

1. **Sharing resources**
2. **Faster and cheaper communication**
3. **Centralized control**
4. **Backup and Recovery**
5. **Remote and Mobile access**

Disadvantages of Networking

1. Expensive to install

2. Security Breach problem
3. Needs Technical person
4. Virus attacks
5. Extreme dependency on server

Block Diagram of a Communication system/model

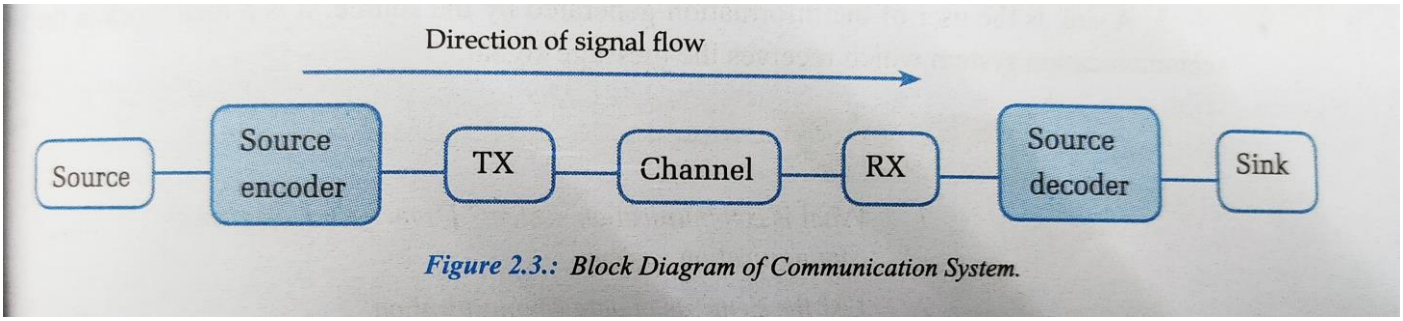


Figure 2.3.: Block Diagram of Communication System.

Communication system is the system of communicating from one point to another point. The elements of data communication are **Source, Source encoder, Transmitter, channel, Receiver, source decoder and sink.**

Source: A source generates the information. Information represents anything that we want to transmit such as voice, message, data, picture etc.

Source encoder/Input Transducer: A source encoder is a translator that converts the information into an electrical form called message signal.

Transmitter: It is used to convert the message signal into a form acceptable to the channel. It contains electronic devices such as amplifiers, mixers, oscillators and power amplifiers.

Channel: The channel is the path or a link that connects the transmitter and receiver. It can be wired or wireless.

Receiver: A receiver performs an inverse function of that of the transmitter to recover message signal. The receiver receives the incoming modified version of the message signal from the channel. Then processes it to recreate the original form of the message signal. It can be loudspeaker, video display unit, computer, radar, and antenna.

Source Decoder/Output Transducer: A source decoder converts the electrical signal back to a form acceptable by the receiver. For example: loudspeaker converts electrical signals into sound.

Sink/Destination: A sink is the user of the information generated by the source or it is the place or point where we want to send the signal. In audio transmission, human ear is the destination**.**

Types of Computer Networks

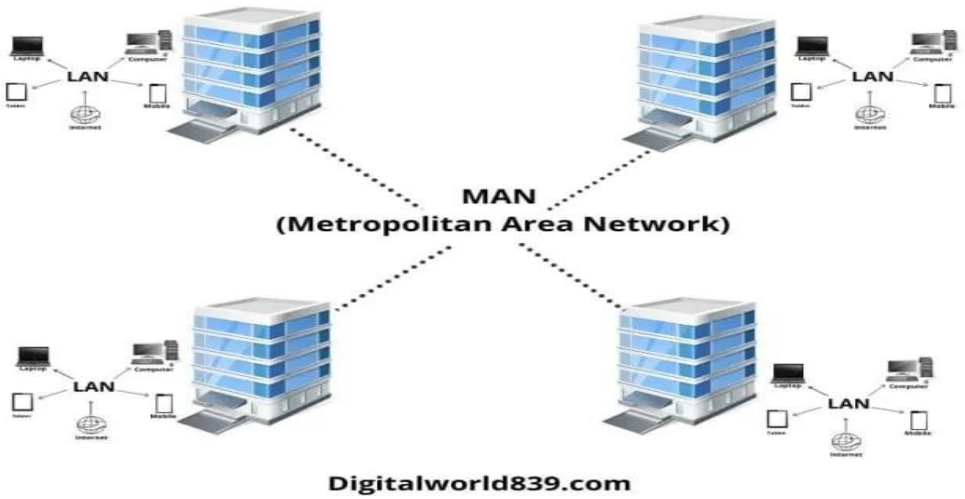
The **Network** allows computers to **connect and communicate** with different computers via any medium. LAN, MAN and WAN are the three major types of the network designed to operate over the area they cover. There are some similarities and dissimilarities between them. One of the major differences is the geographical area they cover, i.e. **LAN** covers the smallest area; **MAN** covers an area larger than LAN and **WAN** comprises the largest of all.

1. Local Area Network (LAN)

1. Local area network is a group of computers connected with each other in small places such as school, hospital, apartment etc.
2. LAN is secure because there is no outside connection with the local area network thus the data which is shared is safe on the local area network and can't be accessed outside.

LAN or Local Area Network connects network devices in such a way that personal computers and workstations can share data, tools and programs. The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol.
It can cover only a few kilometers. (Usually up to 3 km)

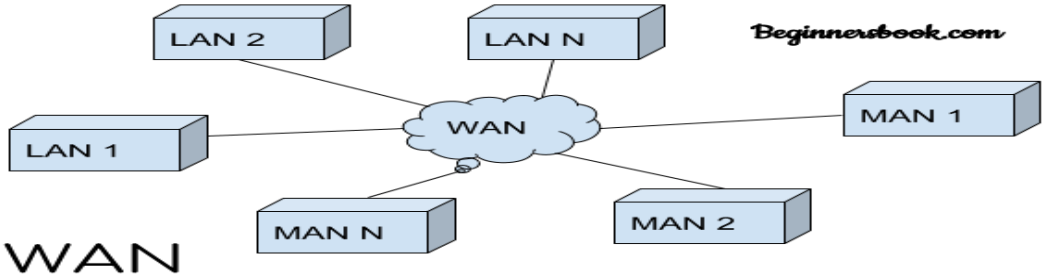
2. Metropolitan Area Network (MAN)



It connects two or more computers that are apart but reside in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider).
MAN network covers a larger area by connecting LANs to a larger network of computers. In the Metropolitan area network various Local area networks are connected with each other through optical cables or telephone lines. The size of the Metropolitan area network is larger

than LANs and smaller than WANs (wide area networks), a MANs covers the larger area of a city or town.

3. Wide area network (WAN)



Wide area network provides long distance transmission of data. The size of the WAN is larger than LAN and MAN.

It is a largest sized network and connects millions of computers, thousands of LANS, hundreds of Mans around the countries, continents and even the whole world.

Slightly more complex than a LAN, a WAN connects computers together across longer physical distances.

A WAN can cover a country, continent or even a whole world.

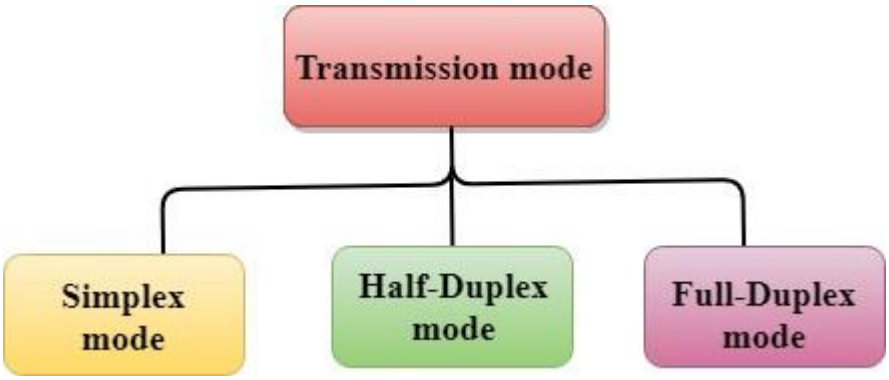
Internet connection is an example of WAN. Other examples of WAN are mobile broadband connections such as 3G, 4G etc.

CLASSWORK +HOMEWORK

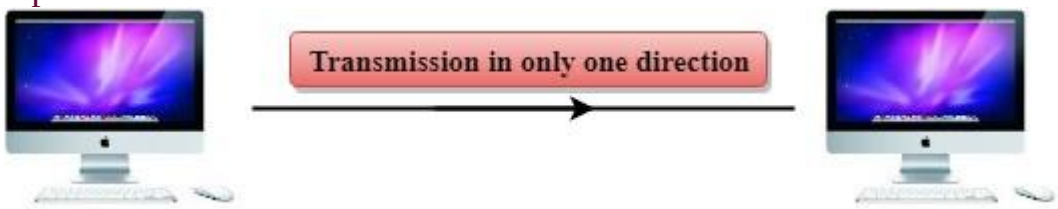
1. **Write down 3-3 advantages and disadvantages of LAN, WAN AND MAN.**
2. **Write down the 5 differences between LAN and WAN.**

Transmission modes:

The way in which data is transmitted from one device to another device is known as **transmission mode**. The transmission mode is also known as the communication mode. The Transmission mode is divided into three categories:

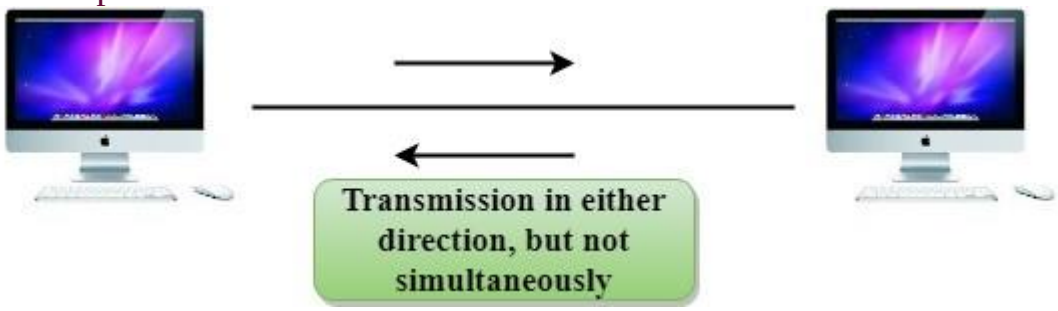


Simplex mode



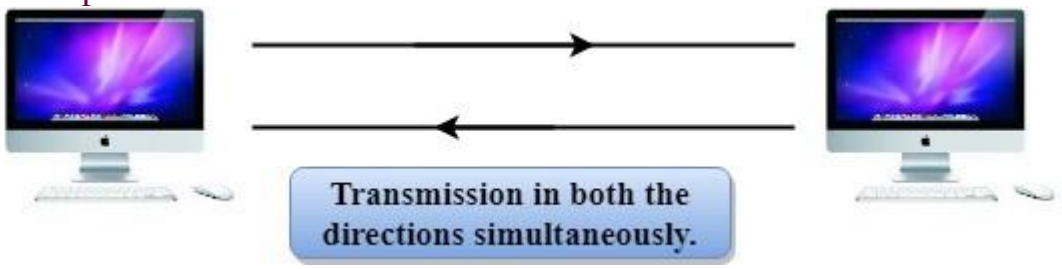
- In Simplex mode, the communication is unidirectional, i.e., the data flow in One direction.
- A device can only send the data but cannot receive it or it can receive the data but cannot send the data.
  The radio station is a simplex channel as it transmits the signal to the Listeners but never allows them to transmit back.

Half-Duplex mode



- In a Half-duplex channel, direction can be reversed, i.e., the station can Transmit and receive the data as well.
- Messages flow in both directions, but not at the same time.
- A **Walkie-talkie** is an example of the Half-duplex mode. In Walkie-talkie, One party speaks, and another party listens. After a pause, the other speaks and the first party listens. Speaking simultaneously will create a distorted sound which cannot be understood.

Full-duplex mode



In Full duplex mode, the communication is bi-directional, i.e., the data flow in both the directions.

- Both the stations can send and receive the message simultaneously.
- Full-duplex mode has two simplex channels. One channel has traffic moving in one direction, and another channel has traffic flowing in the opposite direction.
- The Full-duplex mode is the fastest mode of communication between devices.
- The most common example of the full-duplex mode is a telephone network. When two people are communicating with each other by a telephone line, both can talk and listen at the same time.

Network Models

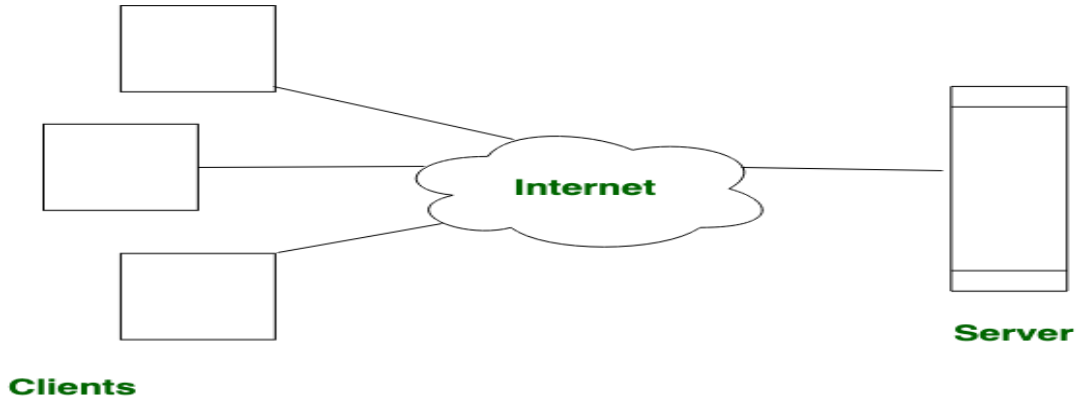
Client-Server Network:

This model is a broadly used network model. In Client-Server Network, Clients and servers are differentiated, specific server and clients are present. In Client-Server Network, Centralized server is used to store the data because its management is centralized. In Client-Server Network, Server responds to the services which are requested by Client.

Advantages:

All files are stored in a central location.
Backups and network security is controlled centrally
All users are allow to share the resources
Centralized backup and recovery.

Disadvantages:
Single point of failure.
Maximum data traffic at server so chance of data collision.
The server is expensive to purchase.
Network operating system and network manager is needed.



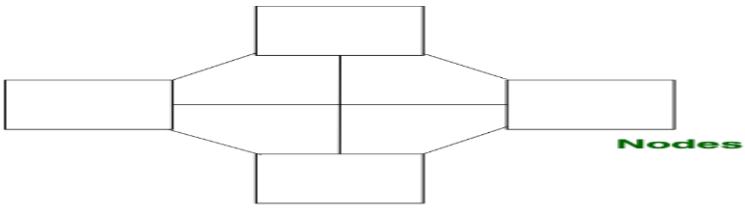
Client-Server Network Model

Peer-to-Peer Network:

A peer to peer network is a kind of computer network where two or more computer systems are connected together without using a separate server. Files can be directly shared between the systems on the network without the need of a central server.
In other words, each computer on the P2P network becomes a file server as well as a client.

This model does not differentiate the clients and the servers, in this each and every node is itself client and server. In Peer-to-Peer Network, Each and every node can do both request and respond for the services.

Each workstation or computer connected in the network has unique address for its identification. When a message is to be sent from one computer to another computer in the network, the address of source computer and destination computer are sent along with the message.



Peer-to-Peer Network Model

Advantages:

All workstations can access files or share files

No single point of failure
All users have own permission to share any file over the network.

Disadvantages:
Too much slow performance because every computer is accessed by other users.
Every computer system contains a unique password over the whole network
Network security has to be applied on each computer separately.

Classwork + Homework

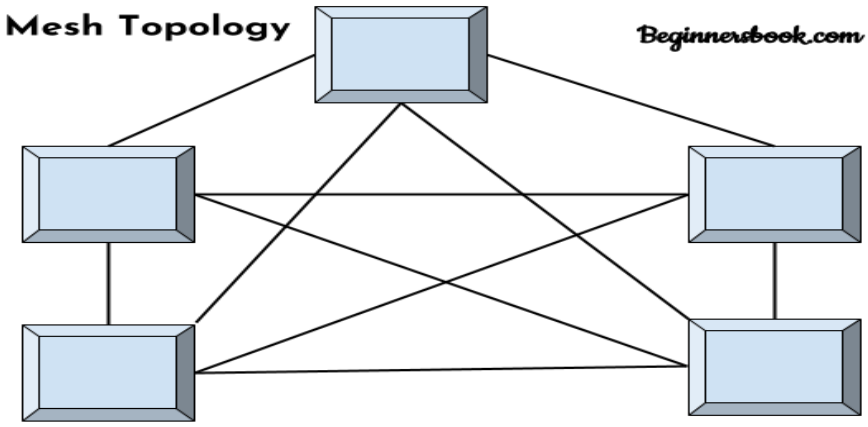
1. Write down the 10 differences between client-server model and peer to peer network model architecture.

Network Topology

Network topology refers to how various nodes, devices, and connections on your network are physically or logically arranged in relation to each other. Think of your network as a city, and the topology as the road map.

Types:

Mesh Topology



In mesh topology each device is connected to every other device on the network through a dedicated point-to-point link. When we say dedicated it means that the link only carries data for the two connected devices only.

Let's say we have n devices in the network then each device must be connected with (n-1) devices of the network. Number of links in a mesh topology of n devices would be n(n-1)/2.

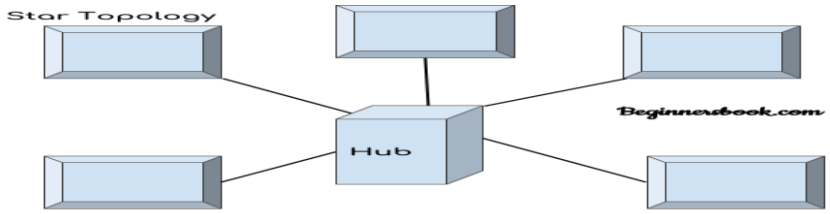
Advantages of Mesh Topology

1. Each connection can carry its own data load.
2. It is robust (even one component fails there is an alternative present)

Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.

Star Topology



In star topology each device in the network is connected to a central device called a hub. Unlike Mesh topology, star topology doesn't allow direct communication between devices, a device must have to communicate through a hub. If one device wants to send data to other device, it has to first send the data to hub and then the hub transmit that data to the designated device.
Hub or switch acts like a server and other nodes as clients

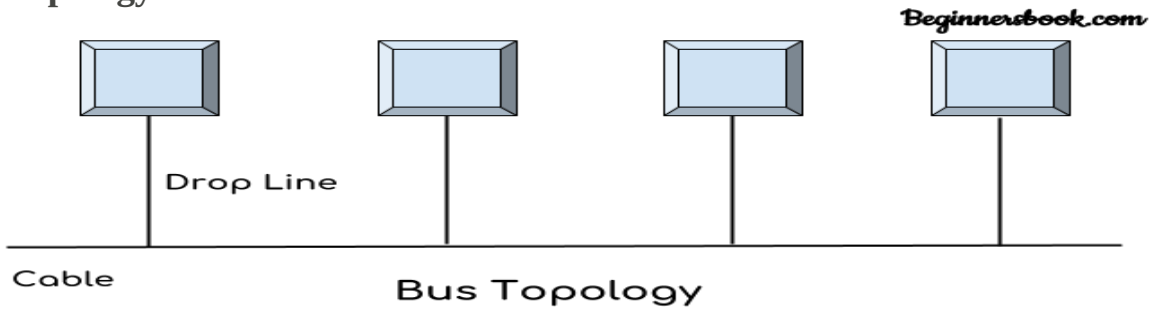
Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hubs can be upgraded easily.
3. Number of nodes can be expanded without affecting others.

Disadvantages of Star Topology

1. Cost of installation is high.
2. If a hub fails, Whole network will go down.

Bus Topology



In bus topology there is a main cable and all the devices are connected to this main cable through drop lines. There is a device called tap that connects the drop line to the main cable. Since all the data is transmitted over the main cable, there is a limit of drop lines and the distance a main cable can have.

A special device terminator is used at both ends of series to absorb the signals or to prevent signal bounce.

In Bus topology, when node A is sending a signal to node B, the signal goes to bus and every node attached to the bus gets the copy. But only B gets the message and all others simply ignores it.

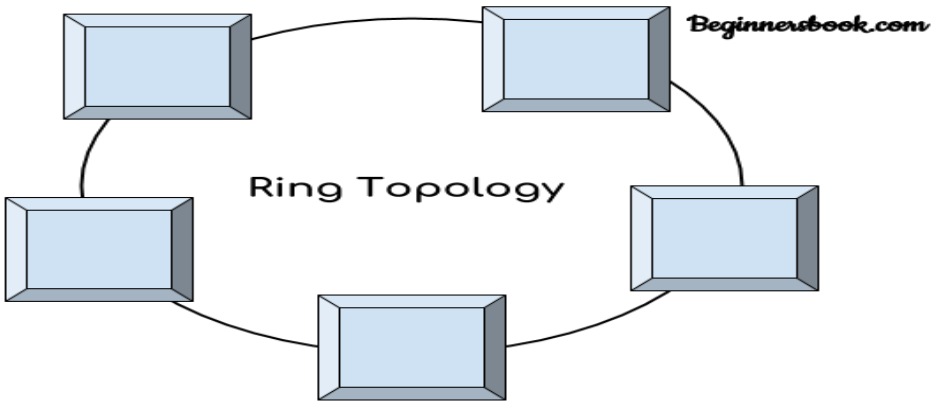
Advantages of Bus Topology

1. It is cost effective.
2. Cable required is least compared to other network topology.
3. If any node fails, it won't affect other nodes.

Disadvantages of Bus Topology

1. If Cables fail then the whole network fails.
2. If data traffic high, chance of data collision.
3. If network traffic is heavy or nodes are more the performance of the network decreases.
4. Length of the bus should be small otherwise performance decreases.

Ring Topology



It is based on peer to peer architecture. In ring topology each device is connected with the two devices on either side of it. There are two dedicated point to point links a device has with the devices on either side of it.
This structure forms a ring thus it is known as ring topology. If a device wants to send data to another device then it sends the data in one direction, each device in ring topology has a repeater, if the received data is intended for another device then repeater forwards this data until the intended device receives it.

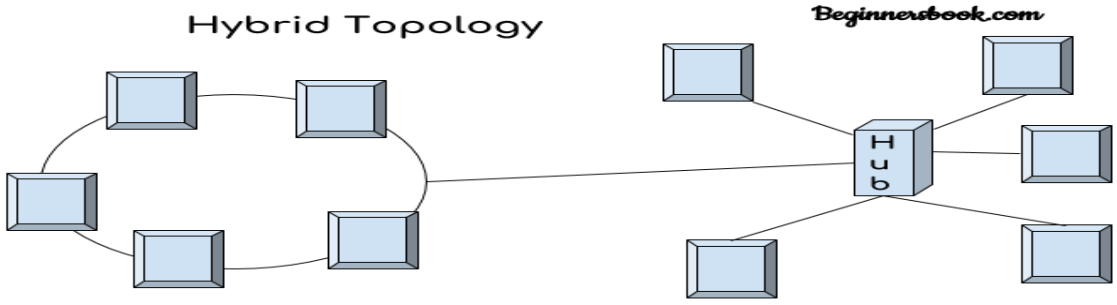
Advantages of Ring Topology

1. Cheap to install and expand
2. Less chance of data collision because of unidirectional concept
3. No server so each computer has equal facilities to the resources.

Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer in the ring can affect whole network.

Hybrid topology



A combination of two or more topologies is known as hybrid topology. For example a combination of star and mesh topology is known as hybrid topology.

Advantages of Hybrid Topology

1. Reliable as Error detecting and troubleshooting is easy.
2. Effective as it uses multiple topologies.

Disadvantages of Hybrid Topology

1. Complex in design.
2. Costly.
3. Difficult to install and configure.

Transmission Media/Communication Media (Very IMP LONG QUESTION)

Transmission medium refers to the physical connection through which data are transmitted between sender and receiver devices.

Transmission can be classified as

1. **Guided (bounded or wired) medium**
2. **unguided (unbounded or wireless)**

In guided transmission, there is a physical link made of wire/cable through which data in terms of signals are propagated between the nodes. These are usually twisted-pair cable, co-axial cable fiber-optic cable, etc. They are also known as wired media.

In unguided transmission, data travels in air in terms of electromagnetic waves using an antenna. They are also known as wireless media. Some examples are radio waves, microwaves, satellite communication, mobile communication etc.

Some factors need to be considered for designing the transmission media:

- **Bandwidth:** *It is defined as the maximum rate of data transfer across a given path. The greater the Bandwidth of a medium, the higher the data transmission rate of a signal. Bandwidth is expressed as a bit rate and measured in bits per second (bps).*
- **Transmission impairment:** *When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the Signals will get destroyed due to transmission impairment.*

- **Interference:** *An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.*

Causes of Transmission Impairment:

Transmission impairments means the signals that are transmitted at the beginning of the medium are not the same as the signals that are received at the end of the medium i.e what is sent is not what is received.

Causes:

Attenuation: It is the loss of signal strength in networking cables or connections. It is typically measured in decibels (db.) or voltage and can occur due to variety of factors. Attenuation means the loss of energy, i.e., the strength of the signal decreases with increasing the distance which causes the loss of energy.

Distortion: Distortion occurs when there is a change in the shape or frequency of the signal. It is also an unintentional change in the message. This type of distortion is examined from different signals having different frequencies. Each frequency component has its own propagation speed when travelling through a medium, so they reach at a different time which leads to the delay distortion.
Alteration of waveform of an information-bearing signal such as an audio signal representing sound or a video signal representing images.

Noise: *When data is travelled over a transmission medium, some unwanted Signal is added to it which creates the noise. It interferes with the original message signal and corrupts the parameter of the message signal. In communications, noise can be created by radio waves, power lines, lightning and bad connections.*

Several types of noise such as thermal noise, induced noise, crosstalk and impulse noise.

Thermal Noise is the random motion of electrons in a wire which creates and extra signal not originally sent by the transmitter.
Induced Noise is the noise that comes from the motor and other appliances.
Crosstalk Noise is the noise when one wire affects the other wire because of Electromagnetic Interference. It occurs when cables run too closely to each other. So some cables use shielding to help reduce the impact of crosstalk.
Impulse Noise is a signal with high energy in a very short time that comes from lightning or power lines.

Jitter: It is the disturbance in the normal sequence of sending data packets. It is also called fluctuation in delay as packets are being transferred over a network. It is measured in milliseconds. It is especially seen in IP telephony and video-audio conferencing. The longer data packets take to transmit, the more jitter affects audio quality.

Echo: Echo is a sound that is repeated because the sound waves are reflected back. It is the returning of reflection of a signal to its initiator.

Number of receivers: It is concerned with the number of users or destination points where data are received.

Bounded or Guided Transmission Media

It is defined as the physical medium through which the signals are transmitted in wires/cables. It is also known as Bounded media.

Twisted pair:

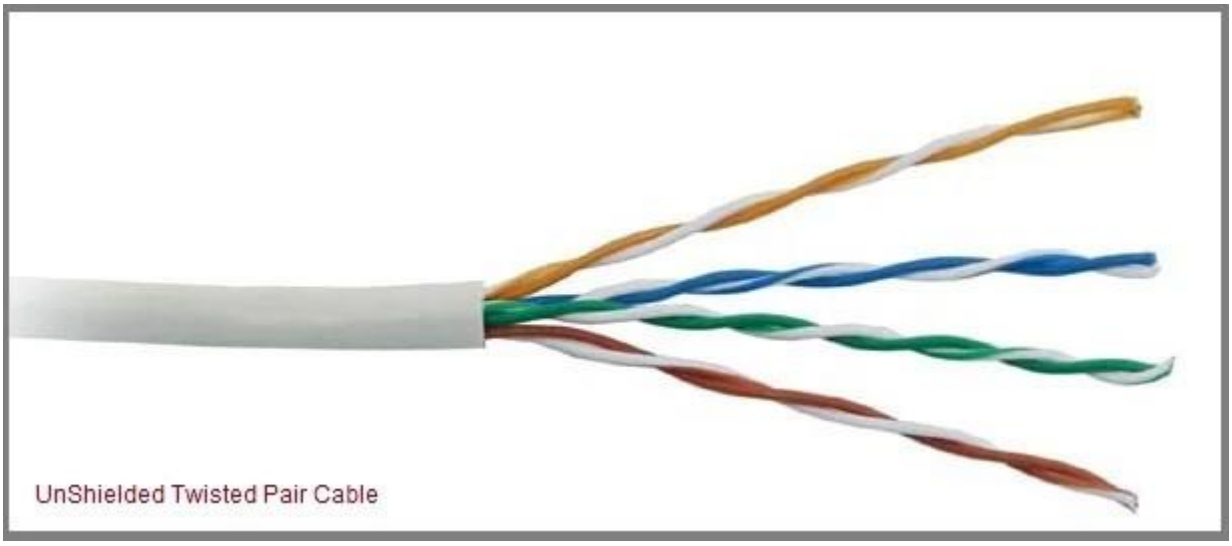
Twisted pair is a physical media made up of a pair of copper wires twisted with each other and finally surrounded by outer insulating jacket.
One wire of the pair is used for receiving data signal and the other wire is used for transmitting data.
The wires are twisted in order to reduce unwanted noise and interference from external sources.
It is available in different categories such as category 1,2,3,4,5,6,7 depending upon the bandwidth of the cables.
It is mainly used in telephone lines in order to provide voice transmission.

Twisted Pair is of two types:

- **Unshielded Twisted Pair (UTP)**
- **Shielded Twisted Pair (STP)**

Unshielded Twisted Pair Cable
It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own color plastic insulator.

It has lower bandwidth and it may interfere by external sources. It is mainly used in telephone connections.
It has lower bandwidth maximum up to 10 Mbps.

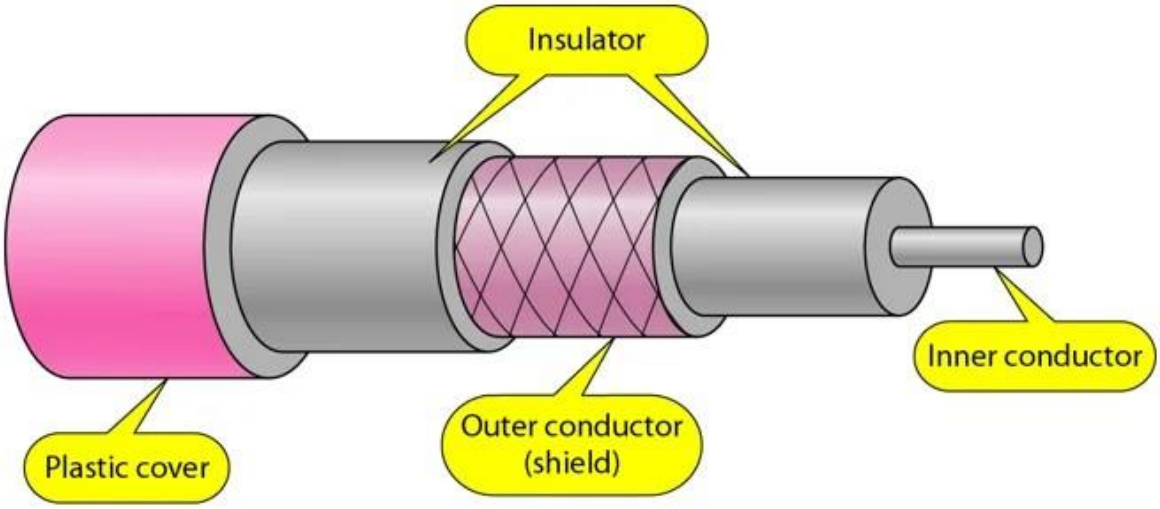


Shielded Twisted Pair Cable

This cable has a metal foil or braided-mesh covering (also called outer PVC jacket) which encases each pair of copper wires that are twisted together. Electromagnetic noise penetration is prevented by metal casing. Shielding also eliminates crosstalk and gives better performance than UTP. More used in LAN for digital data transmission. It has more bandwidth 100Mbps up to 1000Mbps.

Coaxial Cable

- Coaxial cable is a very commonly used transmission media by TV companies.
- The name of the cable is coaxial as it contains two conductors parallel to each other.
- The inner copper conductor is surrounded by an insulator over which a sleeve of copper wire is wrapped around and is used to protect from EMI and this all is covered by a protective plastic covering to protect inner layers from physical damage such as fir or water.
- It has a higher bandwidth as compared to twisted pair cable.



Fiber Optic Cable

A fiber-optic cable is made of high quality of thin glass or plastic and transmits signals in the form of light up to distance of thousands of miles.
In Fiber optics, Noise and distortion is less.

- Fiber optic is a cable that carry communication signals using pulses of light generated by small lasers or light emitting diodes.
- Fiber optics provide faster data transmission than copper wires.
- It consists of 3 parts:
    - Core: The center of the fiber optic cable is the core which provides the pathway for light to travel.
    - Cladding: The core is surrounded by a layer of glass called cladding that reflects the light back to the core.

- Protective coating: The cladding is further protected by a plastic coating called jacket which prevent the cable from EMI.