BIM

Semester: I

FOUNDATION OF INFORMATION TECHNOLOGY

Data Communication and Computer Network

REFERENCE NOTE

Unit-5: Data Communication and Computer Network

Data Communication

Communication:

The exchange of data and information between sender and receiver through any given medium following a common rule is known as communication.

Data communication:

It is the process of exchanging data among the computing devices. Data may be in different form like file, text, image, sound etc. These data are transmitted between a source and a destination. Source device is responsible for generating data and destination device is responsible for receiving the data generated by source. Communication like, email, IRC, VOIP etc. are examples of data communication.

Data communications *are the exchange of data between two devices via some form of transmission medium such as a wire cable.*

For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).

A data communications system has five components:

1. Message: The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

2. Sender: The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

3. Receiver: The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

4. Transmission medium: The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

5. Protocol: A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices.

Computer Network

A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users.

- It is defined as the collection of two or more autonomous computers which are interconnected together for sharing resources with the help of transmission media and set of protocols.
- A computer network is a logical or physical interconnection between two or more computers such that they could communicate with each other.
- A computer network is the group of two or more computers or computing devices interconnected together for communicating, sharing information, hardware, software and data.

Services provided by the computer network.

- Data sharing
- Print service
- File service
- Database service
- Application service

Importance of networks are used are:

- Facilitate communication via email, video conferencing, instant messaging, etc.
- Enable multiple users to share a single hardware device like a printer or scanner
- Enable file sharing across the network
- Allow for the sharing of software or operating programs on remote systems
- Make information easier to access and maintain among network users

Advantages of **Computer Network**

1. ***Sharing resources:*** Software and hardware resources such as processor, storage devices, printers, scanner, etc. can be shared among us using computer network. It helps to minimize the operational cost of an organization.
2. ***Saving Cost:*** Sharing of hardware and software resource avoids duplication, helps in optimal utilization of all types of resource like printer, disks, database etc.

3. ***Faster and cheaper communication:*** communication in modern days has become very faster and cheaper to send information to a long distance through network.
4. ***Centralized control:*** all network resources such as computers, printer file, database, etc. can be managed and controlled by a central connecting computer also known as the server.
5. ***Enterprises and chain organization developed:*** One office or head of the organization can easily visualize and monitor offices and staffs geographically located in different places through videoconference, CC camera etc.
6. ***Backup and recovery:*** server is used to keep data as backup. It maintains backup of all individual computer information.
7. ***Remote and mobile access:*** a remote user can access resources from the distance using computer network.

Disadvantages of **Computer Network**

1. ***Expensive:*** In order to install computer network, we require some extra cost to purchase networking devices such as hubs, switch, cables, etc.
2. ***Security problems:*** network security is the most challenging job for network administrator in order to protect network resources from authorized users and physical destructions.
3. ***Needs technical person:*** it is very difficult to install and operate good computer network.

Data Transmission Media

A transmission media is defined as the means of communication between two networking devices that helps to transfer data from sender to receiver and vice versa.

- Transmission channel is the path through which data are transmitted from source to destination.
- The path through which data transmit form source to destination is known as communication media.

Transmission media is broadly classified into two groups.

1) Bound (guided)/ Wired media

- Guided Media are those communication channel which directly link with each other through cables or other physical media.
- Data are transmitted in closed path through transmission media.
- Data gets transmitted through wires or cables in guided media.
- In guided media there is direct connection between source and destination nodes.
- Guided media has high bandwidth, low cost and high security.
- Data transmission is faster than wireless.
- The most commonly used guided media are: Twisted Pair cable, Coaxial Cable and Fiber Optics.

2) Unbound (unguided) / Wireless media

- The data transmitted in this medium is through electromagnetic waves so that any physical wire or cable is not required for the transmission.

- Unguided media transmission is bounded by geographical areas.
- Different types of unguided media are: Microwave, Radio wave, satellite communication, Bluetooth, Infrared, Wi-Fi, Li-Fi.

S.N.	Guided Transmission Medium	S.N.	Unguided Transmission Medium
1	Signal is directed and contained by the physical limits of the medium.	1	It has no physical medium for the transmission of electromagnetic signals.
2	It is called wired communication or bounded transmission media.	2	It is called wireless communication or unbounded transmission media.
3	The signal energy propagates through wires in guided media.	3	The signal energy propagates through air in unguided media.
4	It types are twisted pair cable, coaxial cable and fiber optic cable.	4	It types are radio wave, microwave and infrared.
5	Examples: Twisted pair cable, coaxial cable and fiber optic cables.	5	Examples: Microwave or radio links and infrared light.

1. ***Wired or Guided Media or Bound Transmission Media:*** The transmission of data and information from source to destination by using physical medium like wires are called bounded transmission media. Its types are as follows.
    1) Twisted pair cable
        i) Shielded Twisted pair cable (STP)
        ii) Unshielded Twisted pair cable (UTP)
    2) Coaxial Cable: 2.1. Thinnet 2.2 Thicnet
    3) Fiber optics

Twisted pair cable: A pair of copper wires is twisted to each other in a helical path making the same structure as a DNA molecule.

- The reason for twisting is to reduce electrical interference.
- It is the cheapest and easily available wire.
- It is mostly used in telephone systems.

Advantages

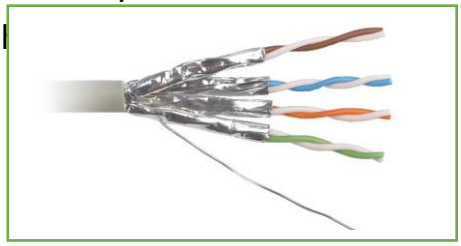
1. It is cheaper than other cables.
2. It is light and thin. So, it is flexible for LAN.
3. It can travel data in short distance with higher bandwidth.

Disadvantage

1. It is only used for short distance transmission.
2. It can be affected by electrical and magnetic field.
3. It is slower type of transmission media compared to other cables.

STP (Shielded Twisted Pair)

Shielded Twisted Pair cable is identical to UTP but it contains the extra shield covering the each pairs of cables. The installation of STP is comparatively difficult than UTP and they are more expensive than UTP but has high bandwidth.



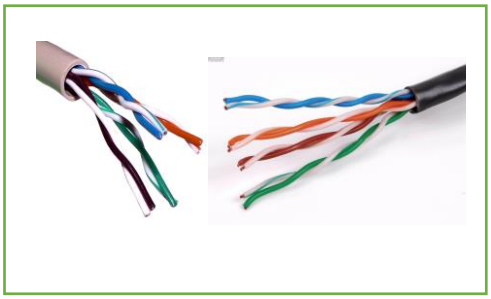
Features of STP Cable

» Better performance and high data transfer rate.
» Eliminates cross talk
» Faster than UTP
» More expensive

UTP (Unshielded Twisted Pair)

UTP is a commonly used cable because it is easy to install and is suitable for data and voice transmission. Unlike STP, UTP cable doesn't have the extra protection shield.

Features:



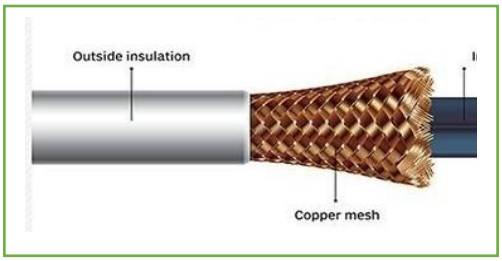
- Less expensive.
- Easy to install.
- High speed capacity.
- Susceptible to external interference.
- Lower capacity and performance than STP.
- Short distance transmission.

S.N.	UTP	S.N.	STP
1	Electromagnetic interference and noise is more in UTP	1	STP cable reduce electrical noise within the cable and from outside of the cable.
2	It offers speed or throughput of about 10 to 1000 Mbps.	2	It offers speed or throughput of about 10 to 100 Mbps.
3	It offers maximum cable length of about 100 meters.	3	It supports maximum segment of length about 100 meters.
4	UTP is widely used for data transmission within short distance and is very popular for home network connecting.	4	STP is mainly used for connection of enterprises over a long distance.
5	The cost of UTP is less when compared to that of STP.	5	STP is costlier than UTP.

Coaxial Cable:

Coaxial cable is a type of copper cable specially built with a metal shield and other components engineered to block signal interference. It is primarily used by cable TV companies to connect their satellite antenna facilities to customer homes and businesses.

Coaxial cable contains two conductors inner and outer, which are separated by an insulator. These two conductors lies parallel to each other. The inner conductor is made up of copper wire which is covered by an inner insulator. The inner insulator is again covered by outer conductor or metal foil. Outer metal wrapping is used as a protection against noise and as the second conductor which completes the circuit. The outer conductor is covered with an insulating cover.



Advantages:

1. It is faster and reliable than twisted pair cable.
2. It can transfer data over medium range of distance.

Disadvantages

1. It is not appropriate for relatively larger distance.
2. It is expensive than twisted pair cable.
3. It is rarely used in computer network.

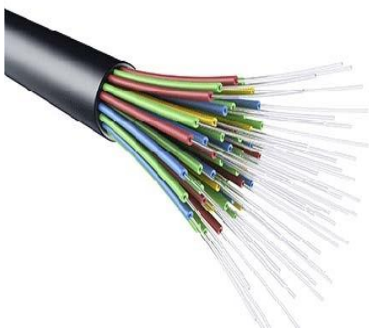
Coaxial cable is of two types:

(a) **Baseband transmission (Thin net):** It is defined as the process of transmitting a single signal at high speed.

(b) **Broadband transmission (Thick net):** It is defined as the process of transmitting multiple signals simultaneously.

Fiber Optics:

It is the most advanced media in communication, which uses light rather than electricity to transmit information. Optical fiber is very thin media, which is measured in microns and is very hard to identify with our necked eye. They're designed for long-distance, high-performance data networking, and telecommunications. Fiber optic cables support much of the world's internet, cable television, and telephone systems.



Features:

1. Data are transmitted in the form of light signals.
2. It is made up of glasses or plastics cover with fiber to protect.
3. It is difficult to install.
4. It has high bandwidth.
5. Data can transfer longer and faster than twisted pair and coax cable.

Advantages:

1. It has higher bandwidth that means it can handle large volume of data.
2. This medium can be used for long distance transmission.
3. It is the most secured and error free transmission medium.

Disadvantages

1. It is one of the expensive type of transmission media.
2. It is not used for short distance transmission.
3. Highly qualified and technical manpower are required to operate on fiber optics.
4. Difficult to install and Fragile in nature

Unguided/ Wireless Media

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them. Radio, microwave and satellite transmissions fall into this category.

1. Radio Transmission

The electromagnetic radio waves that operate at the audio frequency are also used to transmit computer data. This transmission is also known as Radio Frequency (RF) transmission. The computers using RF transmission do not require a direct physical connection like wires or cable. Each computer attaches to an antenna hat can both send and receive radio transmission.

When the antenna transmits the radio wave; they are propagated in all directions. Due to this the sending and receiving antenna doesn't need to be in line of sight position

Fig: Radio Transmission

2. Microwave Transmission

Microwave transmission refers to the technique of transmitting information over a microwave link. Microwaves have a higher frequency than radio waves. Microwave transmission can be aimed at a single direction, instead of broadcasting in all directions (like in radio waves). Microwaves can carry more information than radio waves but cannot penetrate metals. Microwaves are used where there is a clear path between the transmitter and the receiver.

- Microwave transmission is the line of sight transmission.
- The transmit station must be in visible contact with the receive station.
- The microwave is unidirectional.
- This sets the limit on the distance between stations depending on the local geography.
- The microwave is another type of electromagnetic waves that have a frequency range of 1 GHz to 300 GHz.

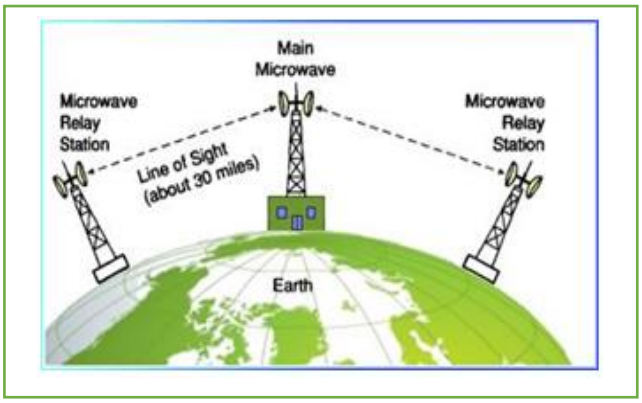


Fig: Microwave Transmission

Microwave transmission has the advantage of not requiring access to all contiguous land along the path of the system, since it does not need cables.

Disadvantages:

a) Needs expensive towers and repeaters, and

b) They are subject to interference from passing airplanes and rain.

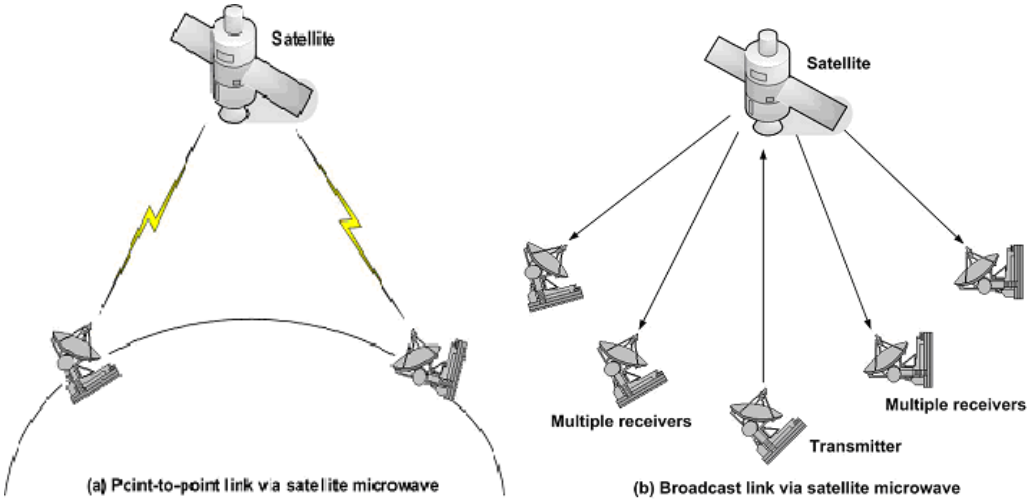
3. Infrared:

Infrared offers a great unbound photonic solution. Like fiber-optic cabling, infrared communications use light. So, they are not bound by the limitations of electricity. They

are normally used for short range communication such as in communication of remote and TV, Ac etc.

4. Satellite Transmission

These are the artificial satellites which are placed in the space for the purpose of communication between different antennas available of on the earth. These artificial satellites facilitate the transmission of signals between stations of the earth. They relays and amplifies radio telecommunication by creating communication channel between source transmitter and destination transmitter.



Bluetooth

Bluetooth *is a wireless technology that is designed and developed to transfer data and information between electronic devices.* This Bluetooth can transfer data within a range ranging from 10 meters to 50 meters. Therefore, as this is a wireless technology, they do not need cables and wires for communication between two or more devices. The Bluetooth device is a must in mobile devices which is used for sharing and transferring data and information like audio, video, files, documents, pictures, etc.

Bluetooth is used in Mobile phones, MP3 players, printers, digital cameras, laptops, personal computers, tablets, home music systems, etc. There is a limitation on the devices which can connect to Bluetooth, and the limit cannot be exceeded than 7 devices.

WIFI - Wireless Fidelity

We are all familiar with Wi-Fi, which is available on our mobile phones, laptops, or wherever Wi-Fi is supported. Wi-Fi is **a wireless networking technology that permits to connect wirelessly** to a network or to other computer or mobile device. A circular radio frequency range is used to transmit data in Wi-Fi.

Wireless Fidelity (Wi-Fi) is a generic term for the **wireless network in the communication norm**. Wi-Fi operates like a local area network without the use of a wire or cables.

Data Transmission across Media

Data Transmission

Data may be transferred from one device to another by means of some communication media. The electromagnetic or light waves that transfer data from one device to another device in encoded form are called **signals**. Data transmissions across the network can occur in two forms i.e.:

a. Analog signal
b. Digital signal

Fundamentals of Transmission

Telecommunication systems use electromagnetic waves to transfer information. A signal is a wave that is suitable for carrying information over a transmission medium. Information carrying signals are of two types:-

(a) Analog signal, and

(b) Digital signal

Analog Signal: An analog signal is a wave that continuously changes its information carrying properties over time. Analog signal has the potential for an infinite amount of signal resolution. The disadvantage of the analog signals is the noise which creates signal loss and distortion.

Digital Signal: A digital signal is wave that takes limited number of values at discrete intervals of time. Digital signals are non-continuous, they change in individual steps. They consist of pulses or digits with discrete levels or values. Digital signals have two amplitude levels called nodes. The value of which are specified as one of two possibilities such as 1 or 0, HIGH or LOW, TRUE or FALSE, and so on.

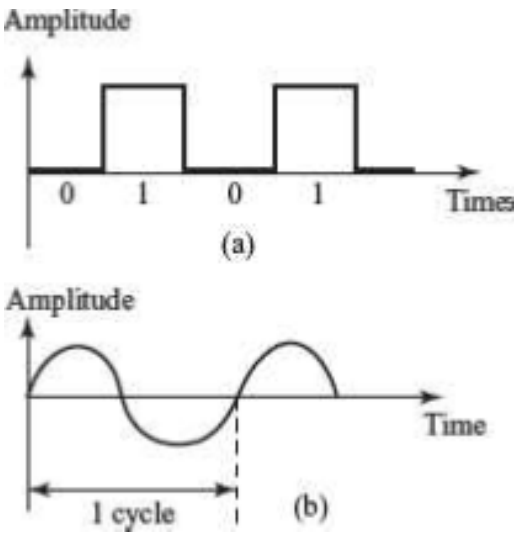


Fig: (a) Digital Signal (b) Analog Signal

Modulation and Demodulation

The process of changing some characteristics (Amplitude, Frequency or Phase) of a carrier wave in accordance with the intensity of the signal is known as **modulation**. The resultant wave is called the modulated wave or radio wave. For
Transmission purposes, a high frequency carrier wave is used to carry the audio signals.

Need for Modulation:-

- To make efficient use of the lines or media used for communication
- To make radio communications feasible
- To simplify signal processing

The process of segregating the data signal and the carrier signal from the modulated carrier wave is called **demodulation**. At the receiving end, the carrier wave is discarded after the data signal has been reconstructed.

Types of Modulation:

There are 3 types of analog modulation:

1. Amplitude Modulation (AM): When the amplitude of the high frequency carrier wave is changed in accordance with the intensity of the signal, it is called amplitude modulation. In amplitude modulation only the amplitude of the carrier wave is changed while the frequency of the modulated wave remains the same.

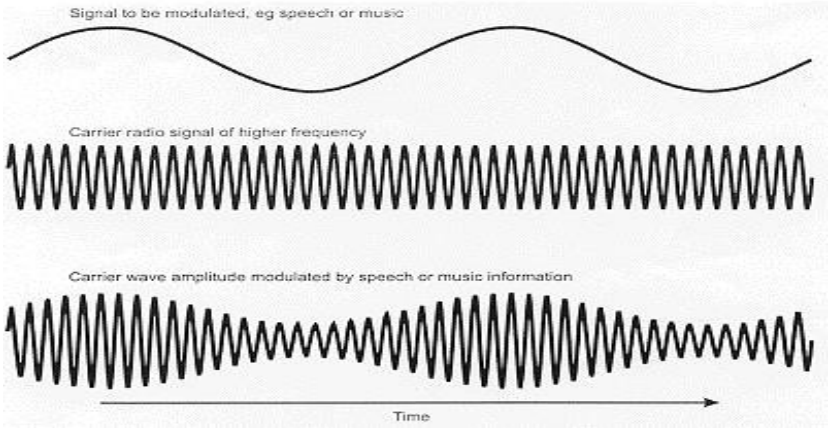


Fig: Amplitude Modulation

2. Frequency Modulation (FM): When the frequency of the carrier wave is changed in accordance with the intensity of the signal it is called frequency modulation. In FM, only the frequency of the carrier is changed while the amplitude of the modulated wave remains the same.

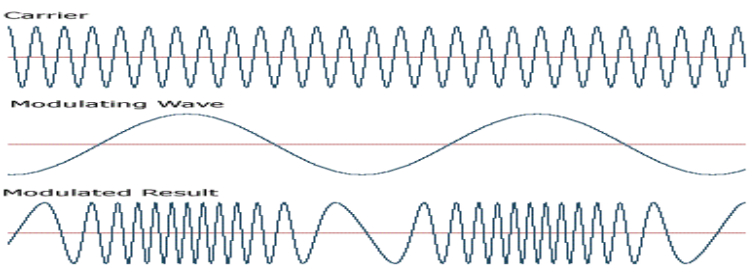


Fig: Frequency Modulation

3. Phase Modulation (PM): Phase modulation is change in the carrier phase angle, which cannot change without affecting a change in frequency. Therefore PM is in second form of frequency modulation (FM).

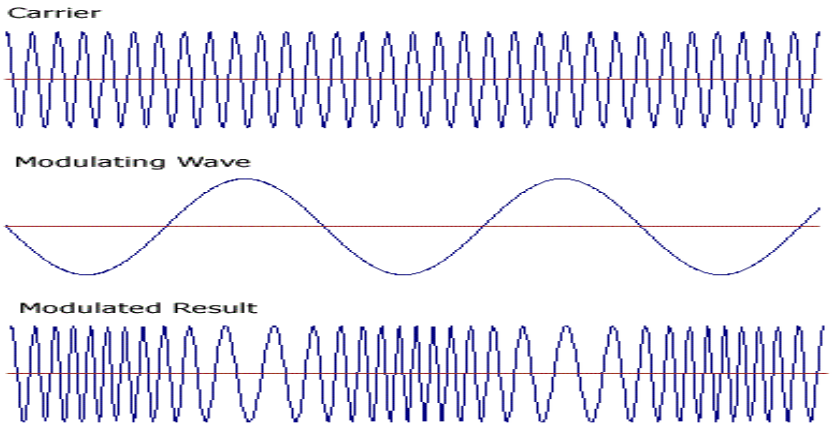


Fig: Phase Modulation

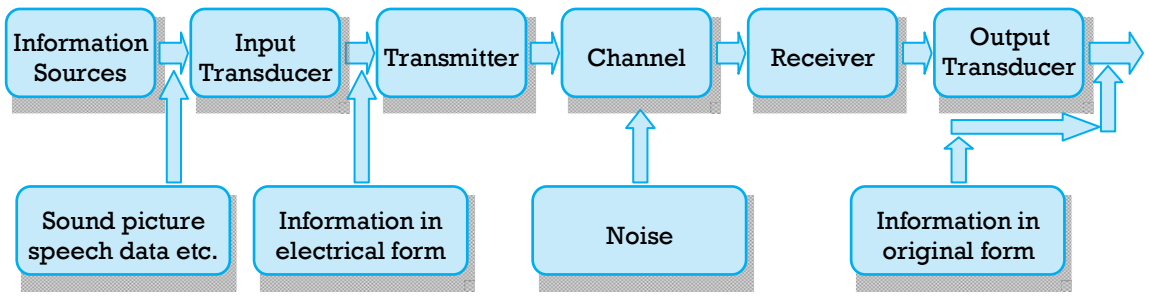
Modems

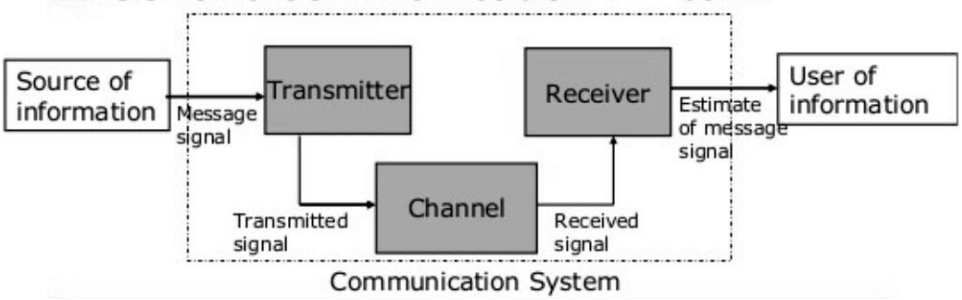
- Modem is a device that has both a modulator and a demodulator. Modulator accepts data signals from the computer and modulates the carrier wave accordingly. Demodulator accepts modulated carrier wave and regenerates the original data signal from it.
- During data communication, modem is attached to the computer, both at the sender and the receiver side. Modems are used with all transmission media like RF modem for RF transmission and optical modem for transmission through fiber.

Block diagram of Communication System

Exchanging of data, information and message is known as communication in simple term. The devices, equipment and other necessary things which play vital role in the communication of message form source to destination are known as communication equipment. These equipment may be computer, mobile, fax and other devices. When all these communication equipment combine together for exchanging the message, then they form the communication system. Line telephony, radio, television broadcast, mobile communication, computer communication etc. are the common examples of communication system.

In the communication, initially the message, data are originated from the information source and sent to destination passing several stages. The block diagram of general communication system is described below:





Elements of Communication System

A. Information Source:

Information source is the place or device which generates the information in communication system. The information may be in different forms such as text, data, speech, pictures, words etc. these information are send to the destination through the communication system. Main role of Information source is to generate the required message which has to be transmitted.

B. Input Transducer:

Input Transducer is important devices which convert one form of energy into another form. In some cases, the message generated form the information source may not be electrical in nature. At that time input transducer is responsible for converting such messages into electrical form. For instance, microphone converts analog sound in electrical signals.

C. Transmitter:

As the name suggests transmitter is responsible for transmitting and processing the electrical signals through the communication channel. In long distance radio communication, signal amplification is necessary for transferring data. Transmitter processes the signals such as restriction of range of audio frequencies, amplification and modulation of signals. All these processes are done just to ease the transmission of signals through the channel.

D. Transmission channel or channel:

Transmission channel is the transmission medium through data signals or information passes from source to destination. It is the medium through which the message travels from the transmitter to the receiver. It provides the connection between the sender / transmitter or receiver. Communication channel may be wired/ guided or wireless/unguided. Wired medium or also called point to point channels where devices are connected through the cables. Whereas wireless medium connect devices wirelessly through electromagnetic wave signals.

Sometime unwanted signal tend to interfere with the information that unwanted signal is called noise.

E. Receiver:

The main function of the receiver is to reproduce the message signal in electrical form from the distorted received signal. This reproduction of the original signal is accomplished by a process known as the demodulation or detection. Demodulation is the reverse process of modulation carried out in transmitter.

F. Output Transducer/Destination:

The transducer presented at output side of the communication system is called output transducer. It is responsible of converting electrical signals into non electrical signals like sound. It is also known as destination and is responsible for converting message signals into its original form from the electrical form. For instance, speaker is a destination or transducer in voice communication.

Mode of Data Transmission

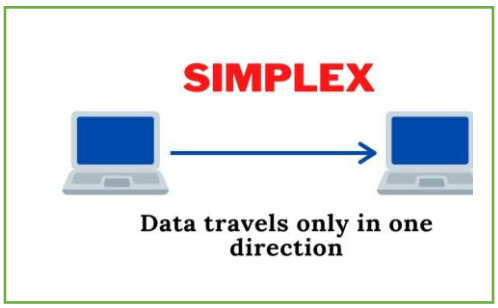
Mode of communication normally refers to the ways in which communication takes place or data gets transmitted between source and destination nodes. Modes of data transmission direct the direction, mechanism of data flow between devices.

1. **Simplex Communication:**

In this type of communication data transmission takes place only in one direction. It is also called a unidirectional communication mode.
Radio, Television, Newspaper and keyboard to CPU Communication are some of the most common example of simplex communication.

Features:

- Data are transmitted in only one direction.
- The sender sends data and receiver receives only.
- There is not bidirectional communication.
- Listeners cannot reply immediately.
- Radio and television broadcast are its examples.



2. **Duplex Communication:**

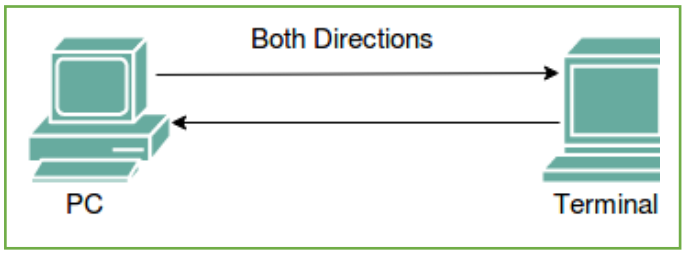
In duplex communication, mode data transmission is possible from both directions. The receiver can immediately respond to the sender. The duplex communication can be categorized into two groups.

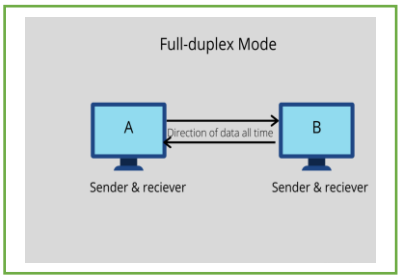
a. Half Duplex:

In this type of communication mode data can be transmitted in both directions, but only in one direction at a time. Both sender and receiver cannot transfer the data at a time. While sending data it cannot receive it and while receiving data it cannot send.

Features:

- Data are transmitted in both direction but single direction at one time.
- Receiving end acts as mere listener while sender sends data and vice versa.
- The communication is slower.
- Willkie Talkie used by the police man is the best example of half-duplex.





b. Full Duplex

Full Duplex communications allows data to flow the information at the same time. Speaking on telephone of full Duplex communication mode in which both the sender and receiver can speak simultaneously. Bidirectional communication at the same time is called full duplex communication mode.

Features:

- Data are transmitted in both direction at the same time.
- When one end sends data other end can receive as well as send data.
- Communication is faster.
- Telephone is an example of full duplex mode.

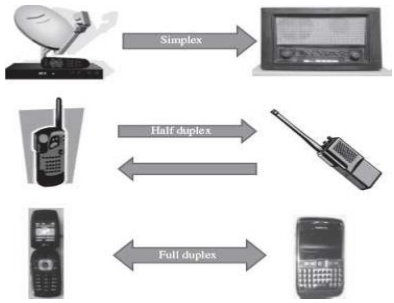


Fig: Transmission Modes

S.N.	Simplex	Half Duplex	Full Duplex
1	It is a uni-directional / One way communication	It is a two way directional communication but one at a time.	It is a two way directional communication simultaneously.
2	Sender can send the data but can't receive the data in it.	Sender can send the data and also can receive the data but one at time in it.	Sender can send the data and also can receive the data simultaneously in it.
3	It provides less performance than half duplex and full duplex.	It provides less performance than full duplex.	It providers better performance than simplex and half duplex mode.
4	Examples: radio and newspaper	Examples: Walky-talky and wireless handset	Examples: smart phone and land line phones.

Transmission Speed

When the signals are transmitted between two computers, two factors need to be considered:

(1) Bandwidth, and

(2) Distance.

Bandwidth is the amount of data that can be transferred through the underlying hardware i.e. the communication medium, in a fixed amount of time. Bandwidth is measured in *cycles per second (cps) or Hertz (Hz)*.

Throughput is the amount of data that is actually transmitted between the two computers. Throughput is specified in *bits per second (bps)*. Higher throughput is achieved by using a large part of the electromagnetic spectrum called broadband technology. Lower throughput uses small part of the electromagnetic spectrum is known as baseband technology.

The throughput is affected by the distance of communication between the connected computers or devices.

The bandwidth decreases with the increase in the distance between the connected devices. The gradual deterioration of signal strength across long distances is called *attenuation*.

Moreover, with increasing distance the external disturbance increases, which causes the signal to deteriorate and results in less amount of data to be transferred. The degradation of signal due to internal or external disturbances is called *distortion*.

Transmission and Data Networking

A network cannot allow or deny access to a shared communication facility. All computers attached to the network can use it to send and receive data. Networks allow sharing of communication medium using switching. Switching routes the traffic (data traffic) on the network. It sets up temporary connections between the network nodes to facilitate sending of data. Switching allows different users, fair access to the shared communication medium.

There are three kinds of switching techniques:

1) Circuit switching
2) Message switching
3) Packet switching

Switching

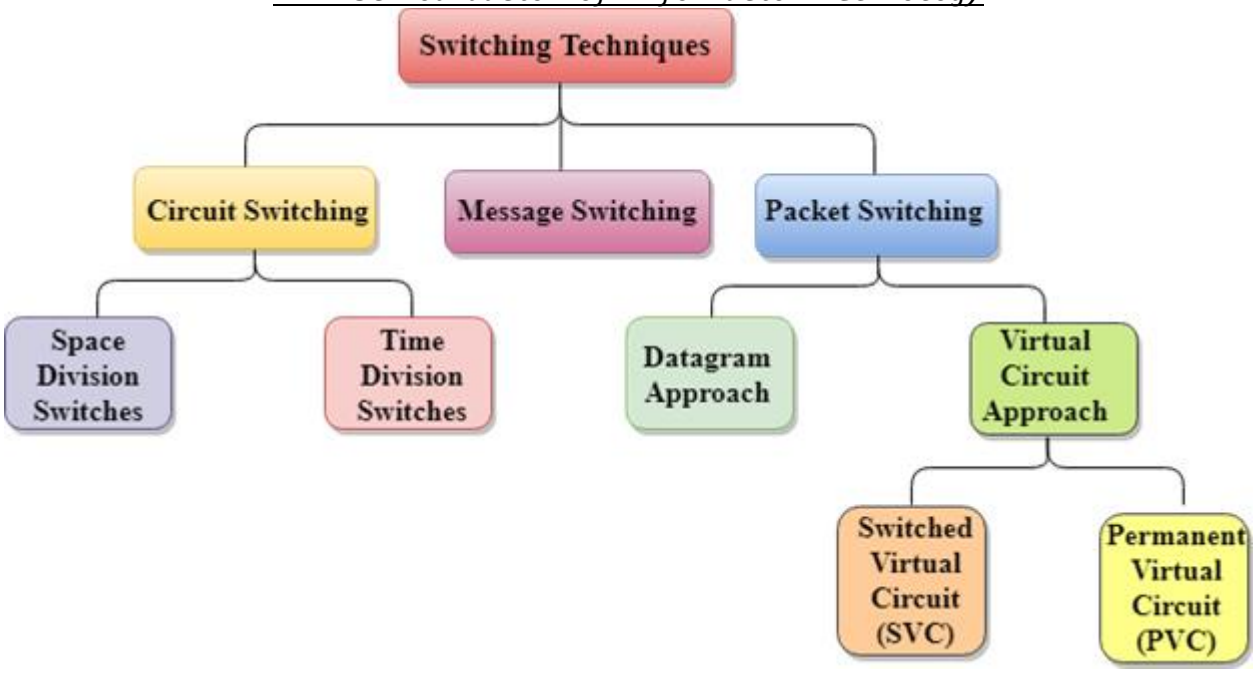
Switching is a mechanism by which data/information sent from source towards destination which are not directly connected. Networks have interconnecting devices, which receives data from directly connected sources, stores data, analyze it and then forwards to the next interconnecting device closest to the destination.

Switching technique

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-to-one communication.

Switching can be categorized as:



1. Circuit Switching

When two nodes communicate with each other over a dedicated communication path, it is called circuit switching.

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.

Advantages of Circuit Switching:

- In the case of Circuit Switching technique, the communication channel is dedicated.
- It has fixed bandwidth.

Disadvantages of Circuit Switching:

- Once the dedicated path is established, the only delay occurs in the speed of data transmission.
- It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.
- It is more expensive than other switching techniques as a dedicated path is required for each connection.

- It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.
- In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

Circuits can be permanent or temporary. Applications which use circuit switching may have to go through three phases:

i) Establish a circuit
ii) Transfer the data
iii) Disconnect the circuit

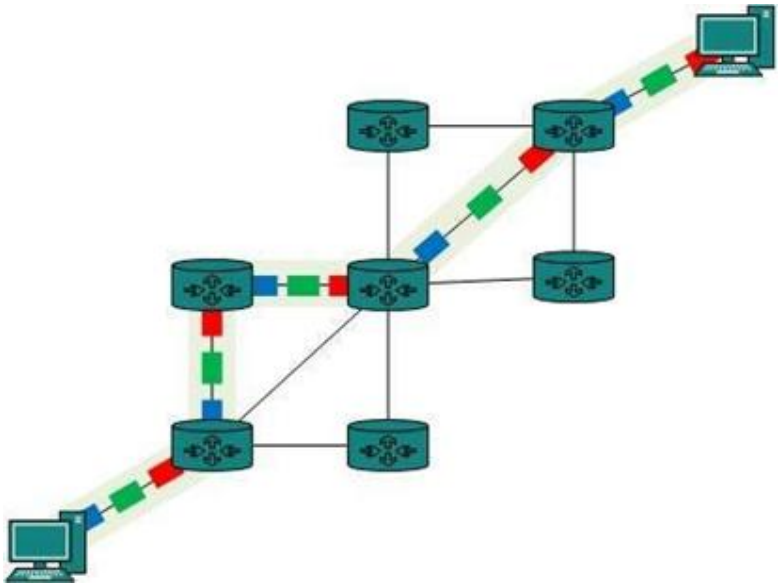


Fig: Circuit Switching

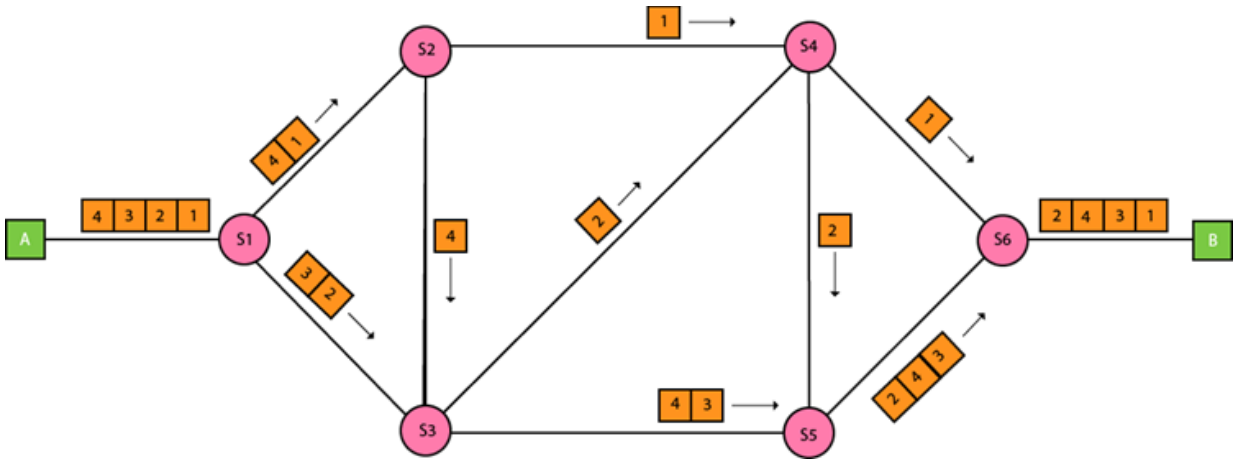
2.Packet Switching

Packet switching is the transfer of small pieces of data across various networks. These data chunks or "packets" allow for faster, more efficient data transfer.

Often, when a user sends a file across a network, it gets transferred in smaller data packets, not in one piece. For example, a 3MB file will be divided into packets, each with a packet header that includes the origin IP address, the destination IP address, the number of packets in the entire data file, and the sequence number.

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.

- If the correct order of the packets is reached, then the acknowledgment message will be sent.



Advantages of Packet Switching:

- **Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.
- **Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- **Efficient:** Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

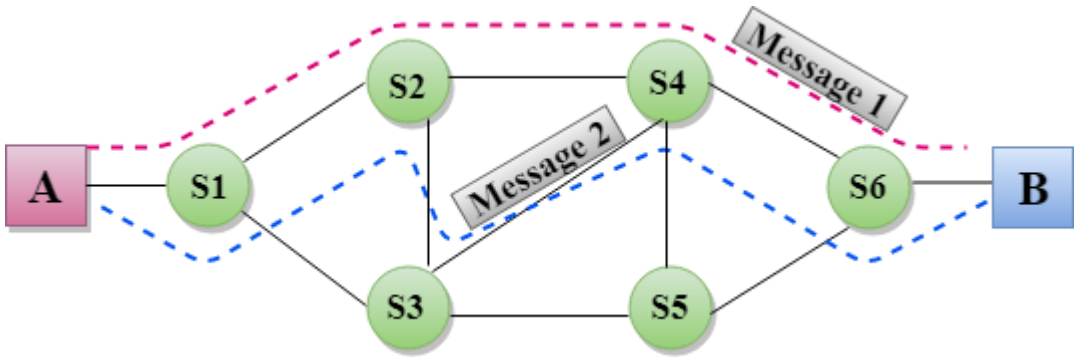
Disadvantages of Packet Switching:

- Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.
- The protocols used in a packet switching technique are very complex and requires high implementation cost.
- If the network is overloaded or corrupted, then it requires retransmission of lost packets. It cannot also lead to the loss of critical information if errors are nor recovered.

Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.

- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forwards it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.



Advantages of Message Switching

- Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.
- Traffic congestion can be reduced because the message is temporarily stored in the nodes.
- Message priority can be used to manage the network.
- The size of the message which is sent over the network can be varied. Therefore, it supports the data of unlimited size.

Disadvantages of Message Switching

- The message switches must be equipped with sufficient storage to enable them to store the messages until the message is forwarded.
- The Long delay can occur due to the storing and forwarding facility provided by the message switching technique.

S.N.	Parameter	Circuit switching Network	Packet switching Network
1	Path	In circuit switched network a dedicated path is created between two points by setting the switches.	In packet switched network no dedicated path is created between two points. Only the virtual circuit exists.
2	Store and forward transmission	In circuit switching there is no concept of store and forward transmission.	In virtual packet switched network, each node may store incoming packets and forward them after use.
3	Dedicated	The links that make a path in circuit switched network are dedicated and cannot be used for other connections.	In the virtual circuit network, links that make a route can be dedicated with other connections.
4	Availability of Bandwidth	In circuit switching, bandwidth is fixed because it is reserved in advance.	In the virtual circuit network, require bandwidth is dynamic because it can be released as it is needed.
5	The route followed by packets	The route followed by packets is always the same.	The route followed by packets is may or may not be different.

Types of Network

A computer network is a group of computers linked to each other through a transmission medium that enables the computer to communicate with another computer and share their resources, data, and applications.

There are mainly three types of computer networks based on their size:

1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide area network (WAN)

1. Local Area Network (LAN)

- A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as home, school, computer laboratory, office building, or closely positioned group of buildings.
- LAN's enable the sharing of resources such as files or hardware devices that may be needed by multiple users.
- It is limited in size, typically spanning a few hundred meters, and no more than a mile.
- It is fast, with speeds from 10 Mbps to 100 Mbps.
- LAN's can be either wired or wireless. Twisted pair coaxes or fiber optic cable can be used in wired LAN's.
- Nodes in a LAN are linked together with a certain topology. These topologies include: Bus ,Ring & Star

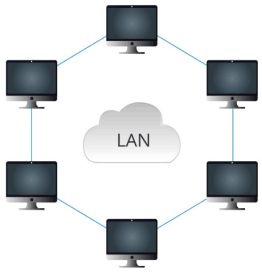


Fig: LAN

2. Metropolitan Area Network (MAN)

- A metropolitan area network (MAN) is a large computer network that usually spans a city or a large campus.
- A MAN is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities.
- A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations.
- A MAN often acts as a high speed network to allow sharing of regional resources.
- Examples of MAN: Telephone company network that provides a high speed DSL to customers and cable TV network.

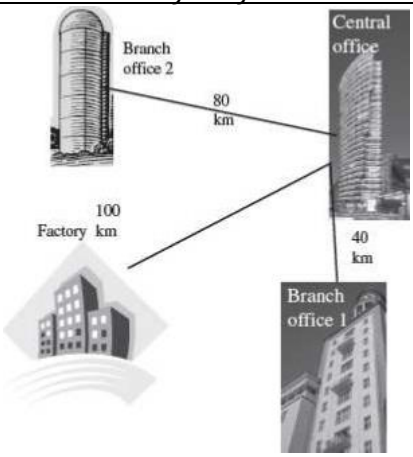


Fig: MAN

3. Wide area network (WAN)

- WAN covers a large geographic area such as country, continent or even whole of the world.
- A WAN is two or more LANs connected together. The LANs can be many miles apart.
- To cover great distances, WANs may transmit data over leased high-speed phone lines or wireless links such as satellites.
- Multiple LANs can be connected together using devices such as bridges, routers, or gateways, which enable them to share data.
- The world's most popular WAN is the Internet.

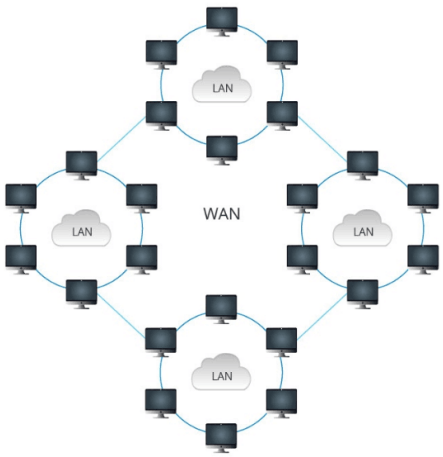


Fig: WAN

Network architecture:

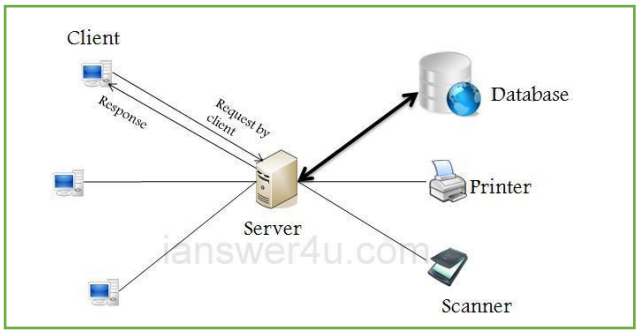
Network architecture refers to the various services provided by the network and it also deals with how data is transmitted from one computer to others.

1. **Client server network**: An arrangement of computers to resource sharing and communicate each other through a central device (server) to all workstations (clients) is called client server architecture one or more computers in the network act as server which provides services to other computers which are called clients.
   - The server is a high capacity high speed computer with a large memory.
   - Server contains the network operating system.

- The central server manages, organize, and coordinate all network clients on the network.
- The most common service is provided by different servers are file services, print services,
- Message services and database services.

Advantages

1. Centralized administration is possible through this network.
2. High security can be provided by suing appropriate server.
3. It is appropriate for large organization.
4. Data recovery and backup process is easier.



Disadvantages

1. If server fails whole network is affected.
2. It is expensive due to use of dedicated server.
3. It is complex to establish and manage.
4. Experienced administrator is required to operate.

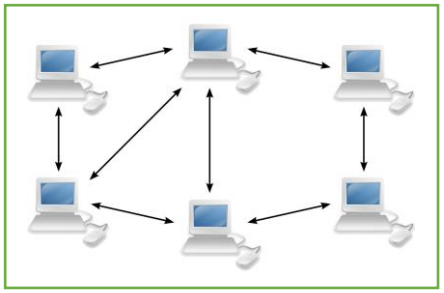
2. **Peer-peer network**: In peer-to-peer architecture computers are connected individually in pair (one-to-one connection). A peer-to-peer network is the type of network in which all computers in the network act both a client and a server i.e. all computers can both request and provide services.
   - Each workstations act as both a client and a server.
   - There is no central repository for information and no central server to maintain.
   - Peer to peer network are generally simpler and less expensive.
   - A peer to peer network is also known as a distributed network.
   - Peer to peer computing or networking is a distributed application architecture that partitions task or workstations between peers.
   - Peers are equally privileged and equal participants in the application.
   - Each node shares its sources with other nodes in the network.

Advantages

1. It is simple cheap and easier to set up.
2. Since there is no dedicated server, user can manage their own server.
3. Failure of a computer in a network doesn't affect the other computer in a network.

Disadvantages

1. Data security is very poor in this type of architecture.
2. Data recovery and backup is difficult.
3. It is not appropriate for large scale organization.



4. Network administration is difficult it without dedicated Server.

Difference between Client Server and Peer to Peer

Client Server	Peer to peer
➢ It is also known as centralized or server based network.	1. It is also known as distributed network
➢ It has central server computer.	2. There is no central server computer.
➢ The central server manages, organize, and coordinate all network clients on the network.	3. Peers are equally privileged and equal participants in the application.
➢ Client server network are more expensive.	4. Peer to peer network are generally simpler and less expensive.
➢ It has high security.	5. It is less security.
➢ If server crashes there is a chance of data loss.	6. Data and information is shared around the network, so less chance of data loss.
➢ Example, Google server, Yahoo server and Bank etc.	7. Example One to one computer and Bluetooth connectivity etc.

Network Topology

Network topology refers to the layout of connected devices, i.e. how the computers, cables, and other components within a data communications network are interconnected, both physically and logically. The physical topology describes how the network is actually laid out, and the logical topology describes how the data actually flow through the network.

The topologies commonly used are:-Bus topology, Star topology, and Ring topology. Other topologies are Tree topology, Mesh topology and Hybrid topology.

1. <u>Bus Topology</u>

- Each machine is connected to a single cable.
- Each computer or server is connected to the single bus cable through some kind of connector.
- A signal from the source travels in both directions to all machines connected on the bus cable until it finds the address on the network that is the intended recipient.
- If the machine address does not match the intended address for the data, the machine ignores the data.
- Alternatively, if the data does match the machine address, the data is accepted.

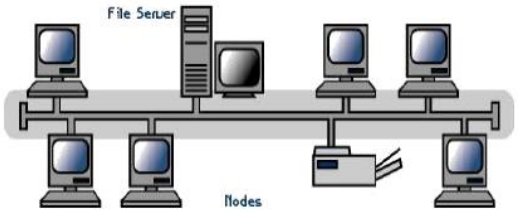


Fig: Bus Topology

Advantages:

- If any node or cable (except backbone) fails, it does not affect the whole network.
- They are relatively cheap and easy to install
- Don't require much cabling
- Easy to add and remove any node or cable except the backbone cable

Disadvantages:

- If the backbone cable fails, the entire network goes down
- Since all the data are transmitted through the backbone cable, data traffic is high
- Bus networks work best with a limited number of devices

2. Star Topology

- Each machine is connected to a central hub or switch.
- It allows each machine on the network to have a point to point connection to the central hub.
- All of the traffic which transverses the network passes through the central hub.
- The hub acts as a signal booster or repeater which in turn allows the signal to travel greater distances.
- Most widely implemented
- Hub is the single point of failure

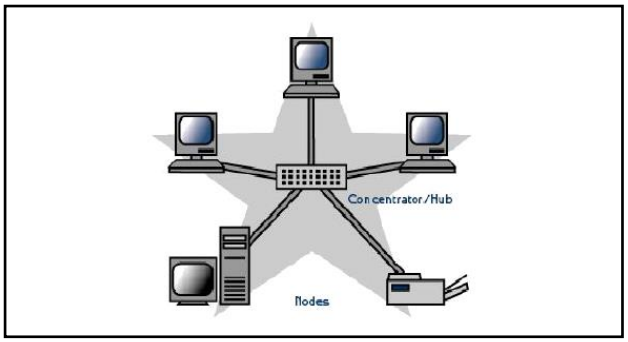


Fig: Star *Topology*

Advantages:

- A failure in any node or cable will only take down one computer's network access and not the entire LAN.
- Easy to diagnose the fault
- Easy to add and remove a node or cable

Disadvantages:

- Compared to the bus topology, a star network generally requires more cable
- If the hub fails, the entire network also fails.

3. Ring Topology

- Each computer is connected to the network in a closed loop or ring.
- Each machine or computer has a unique address that is used for identification purposes.
- The signal passes through each machine or computer connected to the ring in one direction.

- Ring topologies typically utilize a token passing scheme, used to control access to the network.
- By utilizing this scheme, only one machine can transmit on the network at a time.

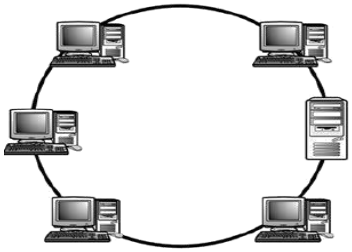


Fig: Ring Topology

Advantages:

- Short cables are required compared to other topologies
- It works where there is no central site computer system
- It is not dependent in a single cable or node

Disadvantages:

- A failure in any cable or device breaks the loop and can take down the entire network.
- It is rarely used in modern LAN
- It is difficult to find out the error
- Adding and removing any node or cable is difficult

4. Tree Topology

- Tree topology uses bus and star topology together to create a network. This topology combines many star topologies using the main cable.
- The whole network is divided into many chunks that can be easily managed and maintained.
- In this topology, all devices are connected to the main cable in the form of star topologies.
- Tree topology is similar to bus topology because all the devices are connected to the main cable. So the main cable acts as a backbone of the network.

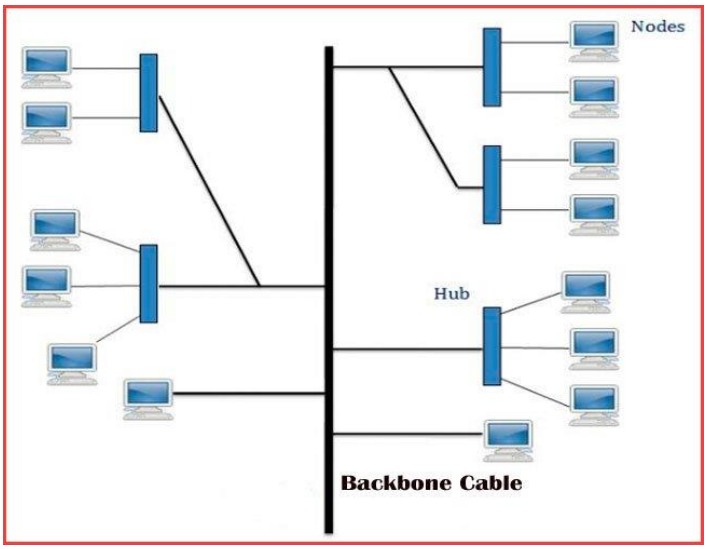


Fig: Tree Topology

Advantages:

- Expansion of nodes is possible and easy.
- If any devices damaged, other hierarchical networks are not affected.
- Other segments are not affected if any node or any segment gets damage.
- Easy to manage and maintain.

Disadvantages:

- If the main backbone line breaks then the entire network shut down.
- Huge amount of cable is needed.
- Maintenance is difficult if more devices are added.
- If the hub or concentrator fails, attached nodes are also disabled.

5. Mesh Topology

- In mesh topology, each computer on the network connects to every other, creating a point-to-point connection between every device on the network.
- Messages sent on a mesh network can take any of several possible paths from source to destination.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.

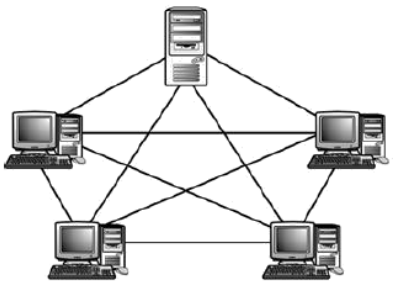


Fig: Mesh Topology

Advantages:

- Failure in any one wire or node does fail the entire network
- It is the most secure topology
- Faster communication because of point-to-point connection

Disadvantages:

- Most complicated network topology
- Expensive in comparison to other topologies.
- Difficult to find the error and trouble shoot.

6. Hybrid Topology

- This topology (sometimes called mixed topology) is simply combining various different topologies to form a larger, more complex topology.
- Main aim is being able to share the advantages of different topologies.

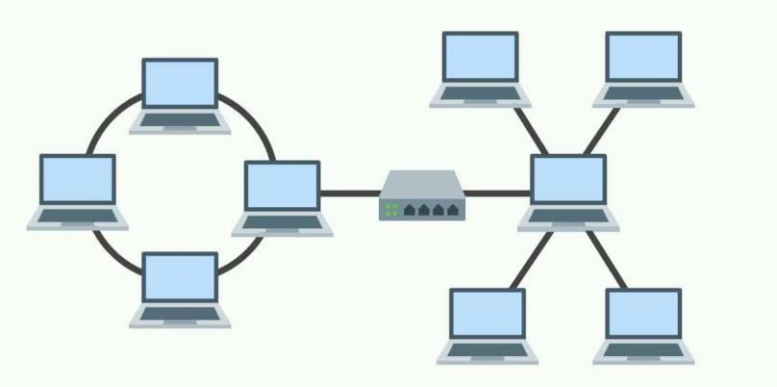


Fig: Hybrid Topology

Advantages:

- Easy network growth
- Manages troubleshooting

Disadvantages:

- Expensive network management.
- Loss of cabling.

Communication Protocol

A **protocol** is a set of rules that make communication on a network more efficient. For example, while flying an airplane, pilots obey very specific rules for communication with other airplanes and with air traffic control.

A **data communications protocol** is a set of rules or an agreement that determines the format and transmission of data.

The network communication protocol is organized as a stack of layers with one layer built upon the other. Each layer has a specific function and interacts with the layers above and below it. The outgoing data from a computer connected to the network passes down through each layer and the incoming data passes up through each layer. The corresponding layers on the different machines are called peers. The peers interact with each other using the protocol.

A communication protocol is a formal description of digital message formats and the rules for exchanging that message in between computer systems. Protocols define a set of formal rules describing how to transmit data especially across a network.

1. TCP/IP (Transmission Control Protocol/Internet Protocol): TCP/IP is a layered set of protocols TCP is reliable, but complex transport-layer protocol. It is stream connection-oriented and reliable transport protocol. TCP/IP is the protocol used by Internet. It adds connection-oriented and reliability features. TCP is responsible for making sure that the data is transmitted to other end. It keeps track of what is sent, and re transmits any data that has not reached its destination. The Internet Protocol (IP) is the principal communication protocol used for transmitting data packets across and network using the Internet Protocol Suite. Internet exist due to TCP/IP.

2. FTP (File Transfer Protocol): This protocol is used for transferring data between client and server over TCP/IP (Internet). Hence, it is responsible for uploading and downloading files to and from the server.

3. UDP (User Datagram Protocol): UDP is simple, connection less, unreliable transport protocol. It performs very limited error checking. It is mainly used for transmitting multimedia data, which requires faster transmission and error checking is not used.

4. SMTP (Simple Mail Transfer Protocol): SMTP is a standard protocol for transmitting electronic mail (email) by the internet. It is a Internet mail protocol. It is a TCP/IP protocol used to send emails

5. POP (Post Office Protocol): POP is also a protocol for transmitting email. It is simple but has limited functionality. It is an application layer Internet standard protocol used by clients to access e-mail from a server over a TCP/IP connection i.e. internet. POP3 (POP version 3) is used at present. POP3 is supported by most modern webmail services such as Gmail and Yahoomail.

6. HTTP (Hypertext Transfer Protocol): HTTP networking protocol for distributed, collaborative, hypermedia information systems. It is used transmitting hypertext or HTML based document. It is the foundation of data communication for the World Wide Web used by web browser to communication with respective servers.

7. HTTPS (Hypertext Transfer Protocol Secure): HTTPS is combination of Protocol with the SSL/TLS protocol to provide encrypted identification of a network. HTTPS connections are often used in World Wide Web for sensitive transactions. The main objective of HTTPS is to create a secure channel over an insecure network

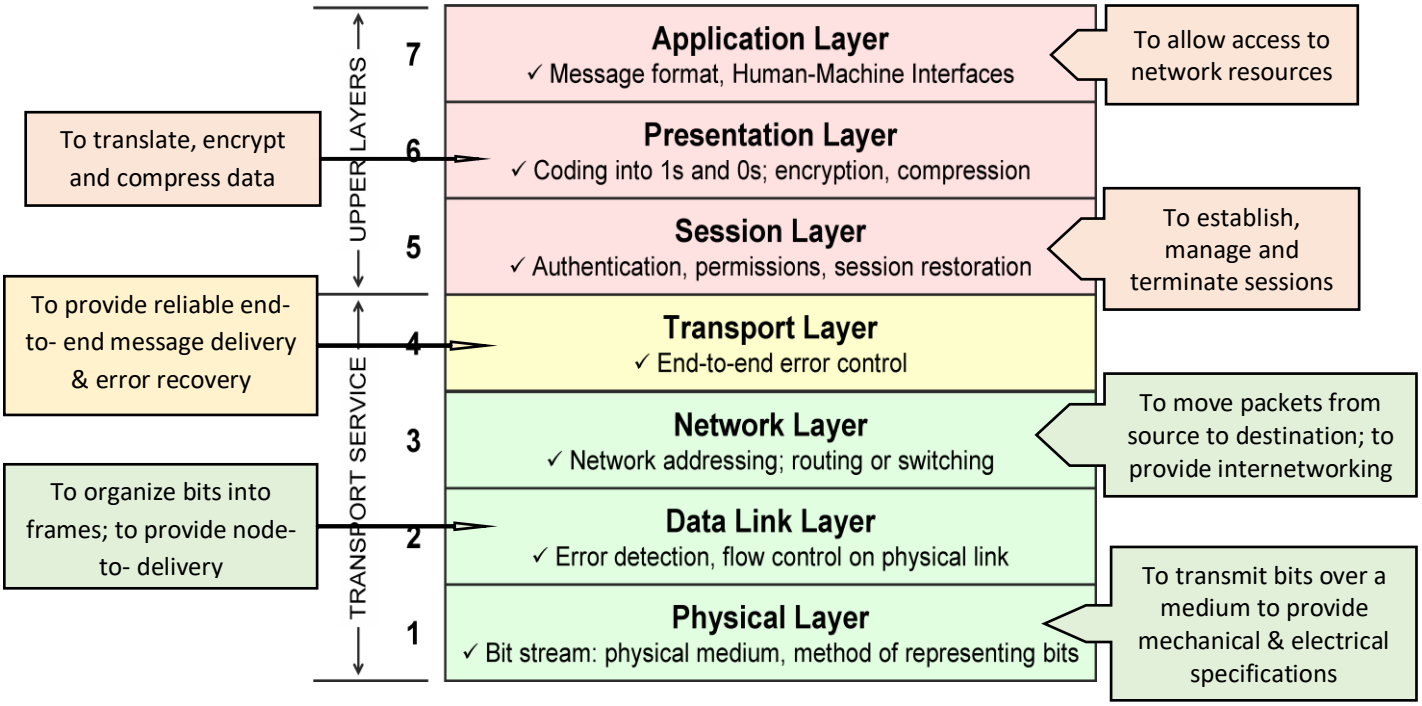
Layer	**Protocols**
Application	FTP, TFTP, Telnet, Gopher, HTTP
Presentation	SMTP, NFS
Session	Telnet, SNMP
Trasport	TCP, UDP
Network	IP
Data Link	ARP, RARP, RIP
Physical	Ethernet, Token Ring, FDDI

OSI Reference Model

The International Standards Organization (ISO) has developed a seven-layer reference model for data networks, known as OSI (Open System Interconnection) reference model.

- It is based on a proposal developed by the international organization for standardization (ISO).
- The model is called ISO OSI reference model, because it deals with connecting open system i.e. the system that are open for communication with other system. OSI consists of set of rules that represents a standard for physical connections, cabling, data formats, and transmission models. Each layer of the ISO model has its own protocols and functions.
- These layers works in hierarchical form, from physical layer to application layer. Data and information are received by each layer from an upper layer.

  The seven layers of the OSI model are:



1. Physical Layer:

This layer specifies the basic network hardware. Some of the characteristics defined in the specification are - interface between transmission media and device, encoding of bits, bit rate, error detection parameters, network topology, and the mode of transmission (duplex, half-duplex or simplex).

Layer 1 is anything that carries 1's and 0's between two nodes.

2. Data Link Layer:

This layer specifies the functions required for node-to-node transmission without errors. It specifies the organization of data into frames, error detection in frames during transmission, and how to transmit frames over a network. Data Link layer is to deliver packets from one NIC to another.

Layer 2 uses MAC addresses and is responsible for packet delivery from hop to hop.

3. Network Layer:

The network layer specifies the assignment of addresses (address structure, length of address etc.) to the packets and forwarding of packets to the destination i.e. routing.

Layer 3 uses IP addresses and is responsible for packet delivery from end to end.

4. Transport Layer:

It specifies the details to handle reliable transfer of data. It handles end-to-end error control and flow control, breaking up data into frames and reassembling the frames.

Layer 4 is responsible for service to service delivery.

5. Session Layer:

The session layer maintains a session between the communicating devices. It includes specifications for password and authentication, and maintaining synchronization between the sender and the receiver.

6. Presentation Layer:

This layer specifies the presentation and representation of data. Its functions include translation of the representation of the data into an identifiable format at the receiver end, encryption, and decryption of data etc.

7. Application Layer:

This layer specifies how an application uses a network. It deals with the services attached to the data. It contains the protocols used by users like HTTP, protocol for file transfer and electronic mail.

Network Devices

Network Devices are the devices that connects two or more LANS, or segments with each other or with the Internet. These connecting devices can operate in different layers of the Internet model. Some of them are:

1. Network Interface Card (NIC)

A Network Interface Card (NIC) is a hardware device through which the computer connects to a network. It works at both the data link layer and physical layer of the OSI reference model.

At the data link layer, NIC converts the data packets into data frames, adds the Media Access address (MAC address) to data frames.

At the physical layer, it converts the data into signals and transmits it across the communication medium.

2. Repeater

Repeaters are used to extend LAN. It has only two ports and can connect only two segments of the network. It retimes and regenerates the signals to proper amplitudes and sends them to the other segments. Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data. A repeater receives a signal and before it becomes too weak or corrupted, regenerates the

original bit pattern. The repeater then sends the refreshed signal. It can extend the physical length of a LAN.

Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay which can affect network communication when there are several repeaters in a row. Many network architectures limit the number of repeaters that can be used in a row. Repeaters work only at the physical layer of the OSI network model.

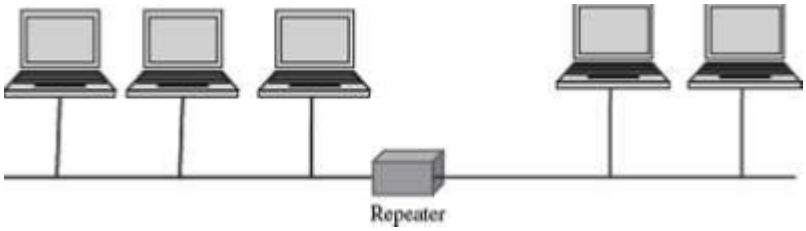


Fig: Repeater

3. Bridge

Bridge is used to connect two LAN segments like a repeater; it forwards complete and correct frames to the other segment. It works in both the physical and the data link layer. As a physical layer device, it regenerates the signal it receives. As a data link layer device, the bridge can check the physical (MAC) address contained in the frame. A bridge has a filtering capabilities i.e. it can check the destination address of a frame and decide if the frame should be forwarded or dropped.

A bridge reads the outermost section of data on the data packet, to tell where the message is going. It reduces the traffic on other network segments, since it does not send all packets. Bridges can be programmed to reject packets from particular networks. Bridges forward all broadcast messages. Only a special bridge called a translation bridge will allow two networks of different architectures to be connected. Bridges do not normally allow connection of networks with different architectures.

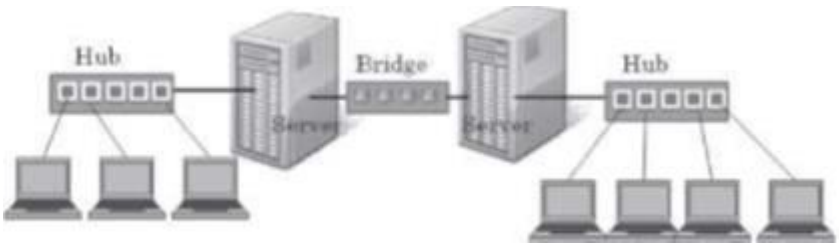


Fig: Bridge

4. Hub

It is a device that centrally connects devices in a computer network. There are two types of a hub i.e. active hub which is a multiport repeater that is used to create connections between stations in a physical star topology; and passive hub which is just a connector that connects the wires coming from different branches.

Every computer is directly connected with the hub. When data packets arrives at hub, it broadcast them to all the LAN cards in a network and the destined recipient picks them and all other computers discard the data packets. Hub has four, eight, sixteen and more

ports and one port is known as uplink port, which is used to connect with the next hub. Hubs work at the physical layer of the OSI (Open System Interconnection) model. The device is a form of multiport repeater. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision.

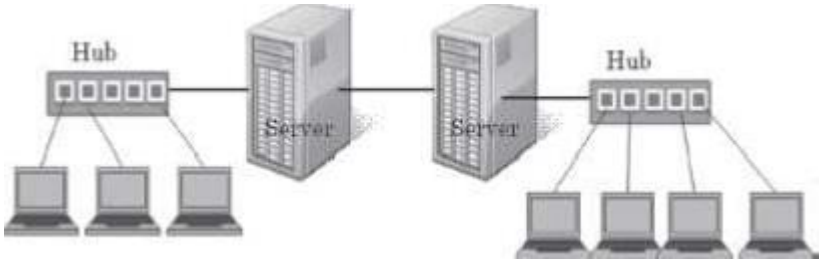


Fig: Hub

5. Switch

Like hub, switch also connects multiple computers in a network or different segments of the same network. Switches work at the Data Link Layer of the OSI reference model. Hence, switches consider data as frames and not as signals. Unlike the hubs, a switch does not broadcast the data to all the computers; it sends the data packets only to the destined computer.

A switch receives a signal as a data frame from a source computer on a port, checks the MAC address of the frame, forwards the frame to the port connected to the destination computer having the same MAC addresses, reconverts the frame back into signal and sends to the destination computer.

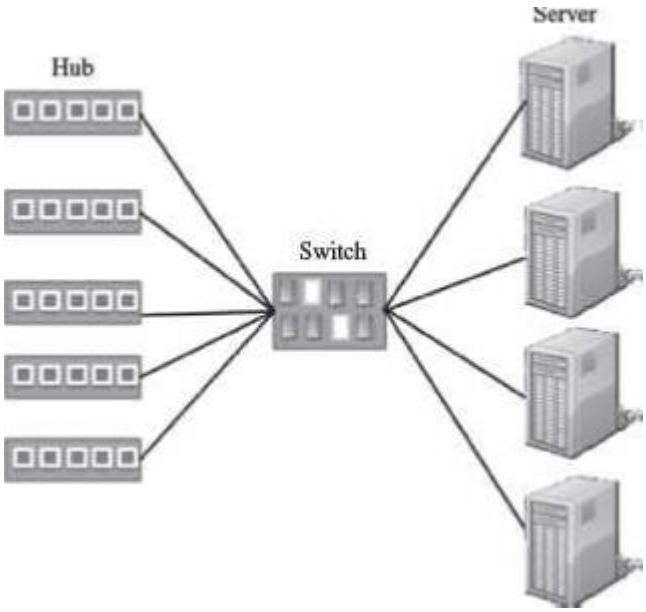


Fig: Switch

6. Router

A router is a communication device that is used to connect two logically and physically different networks, two LANs, two WANs and a LAN with WAN. The main function of the router is to sorting and the distribution (i.e. routing) of the data packets to their destinations based on their IP addresses. Routers provides the connectivity between the enterprise businesses, ISPs and in the internet infrastructure, router is a main

device. Every router has routing software, which is known as IOS. Router operates at the network layer of the OSI model. Router does not broadcast the data packets. Routers connect two or more logical subnets, each having a different network address.

A router determines which way is the shortest or fastest in a network, and routes packets accordingly based on the IP addresses.

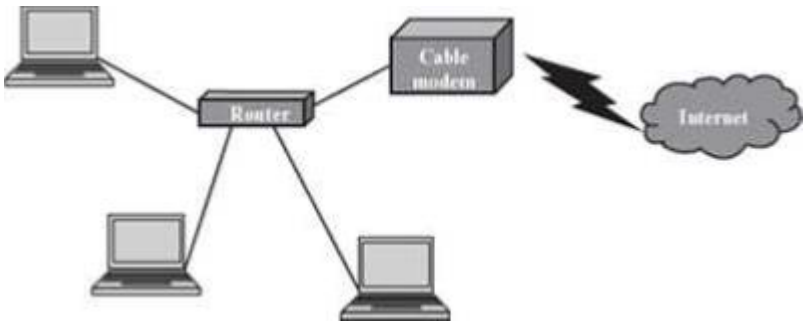


Fig: Router

7. Gateway

Gateway is a generic term used to represent devices that connect two dissimilar networks. A gateway at the transport layer converts protocols among communications networks. It can accept a packet formatted for one protocol and convert it to a packet formatted for another protocol. An application gateway can translate messages from one format to the other.

A gateway can be implemented in hardware, software, or in both hardware and software. Generally, gateway is implemented by software installed within a router.

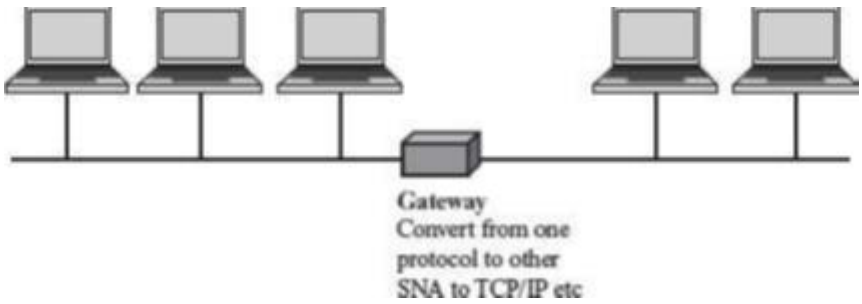


Fig: Gateway

Wireless Networking

Wireless network is a computer network connected wirelessly. The communication is done through a wireless media like radio waves, infrared or Bluetooth.

Uses of Wireless Networking

- Used for broadcasting in radio and television communication
- Used for communication using mobile phones and pagers,
- Used for connecting components of computers using Bluetooth technology, for Internet connection using Wi-Fi, Wireless LAN, PDA, and in remote controls for television, doors etc.

Bluetooth technology

Bluetooth technology is used to connect the different components of the computer in a room, a small office or home.

Wireless LAN

Wireless LAN is used to connect computers and devices wirelessly in a LAN, for example, different computers or devices in an office or campus.

Wireless WAN

Wireless WAN is used to connect wide area systems, for example access to Internet via mobile devices like cell phone, PDAs and laptops.

WIFI: Wireless Fidelity

WIFI also Spelled as Wi-Fi is *a local area wireless technology*. It allows an electronic device to transfer data or connect to the internet using ISM radio bands. It is an underlying technology of wireless local area network (WLAN). Wi-Fi allows computers and other devices to communicate over a wireless network.

Wi-Fi network components are based on the one of the 802.11 standards developed by the IEEE and adopted by Wi-Fi alliance. It provides a standard way to connect with wireless network. Wi-Fi is the trademark of the Wi-Fi alliance and used as a brand name for products using the IEEE 802.11 standards.

Wi-Fi can be used on several types of devices like personal computers, video game console, smart phones, digital camera, tablet computers etc. You can use Wi-Fi to create a hotspot within the range of 20 meters (66 feet). It is less secure than wired connection because the intruder does not need the physical connection to use the Wi-Fi.