Chapter 5

Data Communication and Computer Network

- communication is the process to send and receive information from source to destination.
- The communication process involves

➢ Sender of information

➢ Receiver of information

➢ Language used for communication

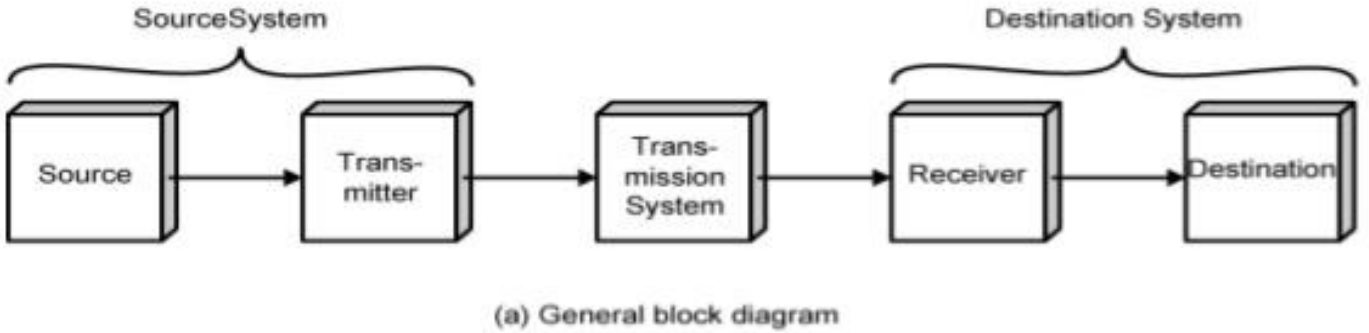
➢ And medium used to established the communication between the sender and receiver

Data Communication

- **Data communication** refers to the exchange of data between a source and a receiver via form of transmission media such as a wire cable. Data communication is said to be local if communicating devices are in the same building or a similarly restricted geographical area.
- The meanings of source and receiver are very simple. The device that transmits the data is known as source and the device that receives the transmitted data is known as receiver. Data communication aims at the transfer of data and maintenance of the data during the process but not the actual generation of the information at the source and receiver.
- **Datum** mean the facts information statistics or the like derived by calculation or experimentation. The facts and information so gathered are processed in accordance with defined systems of procedure. Data can exist in a variety of forms such as numbers, text, bits and bytes. The Figure is an illustration of a simple data communication system.

Data Communication Circuit

- Simplified block diagram of data communication network



(a) General block diagram

(b) Example

Components of data communication system

A Communication system has following components:
Message: It is the information or data to be communicated. It can consist of text, numbers, pictures, sound or video or any combination of these.

Sender/source: It is the device/computer that generates and sends that message.

Receiver: It is the device or computer that receives the message. The location of receiver computer is generally different from the sender computer. The distance between sender and receiver depends upon the types of network used in between.

Medium/transmitter: It is the channel or physical path through which the message is carried from sender to the receiver. The medium can be wired like twisted pair wire, coaxial cable, fiber-optic cable or wireless like laser, radio waves, and microwaves.

Protocol: It is a set of rules that govern the communication between the devices. Both sender and receiver follow same protocols to communicate with each other.

The effectiveness depends on four fundamental characteristics of data communications

1. **Delivery**: The data must be deliver in correct order with correct destination.
2. **Accuracy**: The data must be deliver accurately.
3. **Timeliness**: The data must be deliver in a timely manner. Late delivered Data useless.
4. **Jitter**: It is the uneven delay in the packet arrival time that cause uneven quality.

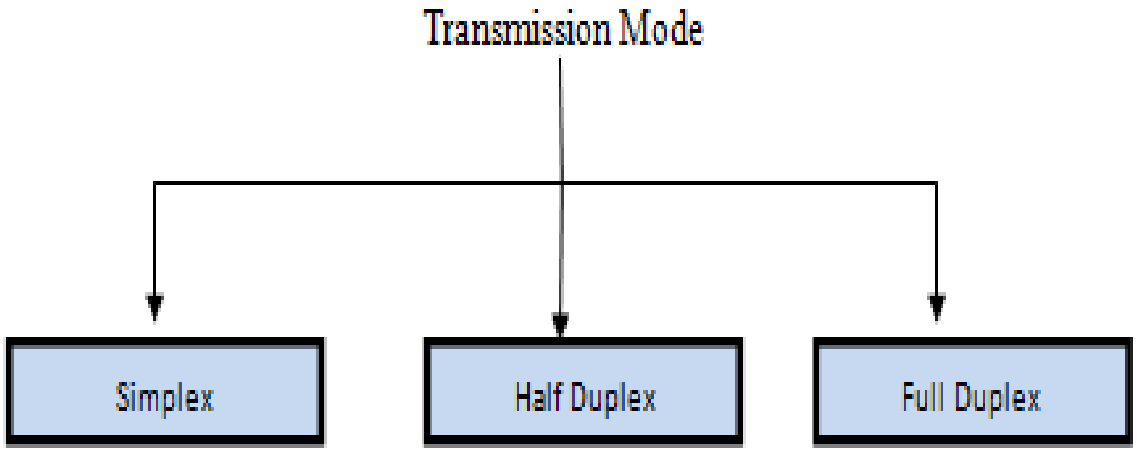
Data Communication vs. Voice Communication

Data Communication	Voice Communication
Requires connection set up time of about 1 sec or less	Requires connection set up time of about 1 sec to 1 minute.
one or two way communication based on application(FTP/browsing/VOIP)	mostly two way communication
data received is error free, in case of errors either retransmission is initiated or it is corrected using FEC techniques.	voice received is with noise and degradation in quality
transmission usually is in the form of bursts	transmission is continuous due to real time operation needed for voice
Data can be stored in database servers and tranmitted based on congestion and application(sms,email)	not tolerant of transmission delays and hence to be transmitted in real time
connection may be required for 24 hrs/day and 7 days/week in certain applications such as ATM cash machine	Connection duration is limited to several minutes
May require wide range of bandwidths	May require a fixed bandwidth of about 4KHz

Transmission Modes in Computer Networks

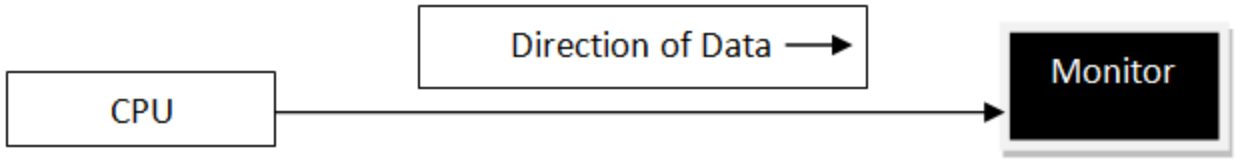
Transmission mode refers to the mechanism of transferring of data between two devices connected over a network. It is also called **Communication Mode**. These modes direct the direction of flow of information. There are three types of transmission modes. They are:

- Simplex Mode
- Half duplex Mode
- Full duplex Mode



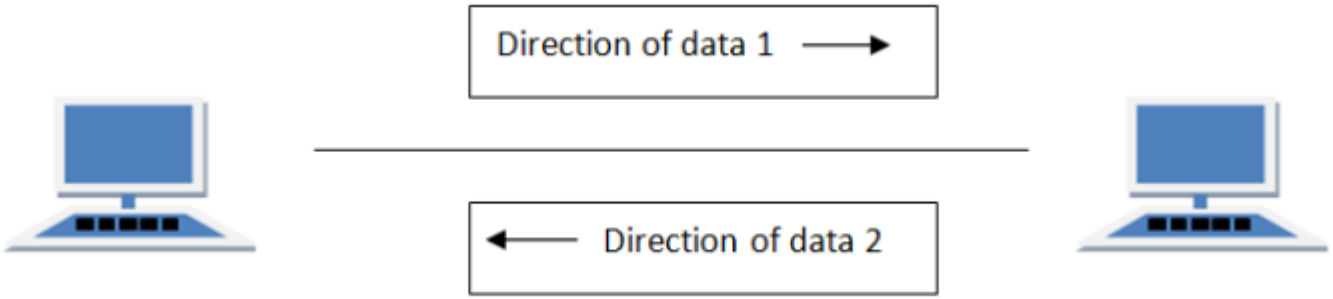
SIMPLEX Mode

- In this type of transmission mode, data can be sent only in one direction i.e. communication is unidirectional. We cannot send a message back to the sender. Unidirectional communication is done in Simplex Systems where we just need to send a command/signal, and do not expect any response back.
- Examples of simplex Mode are loudspeakers, television broadcasting, television and remote, keyboard and monitor etc.



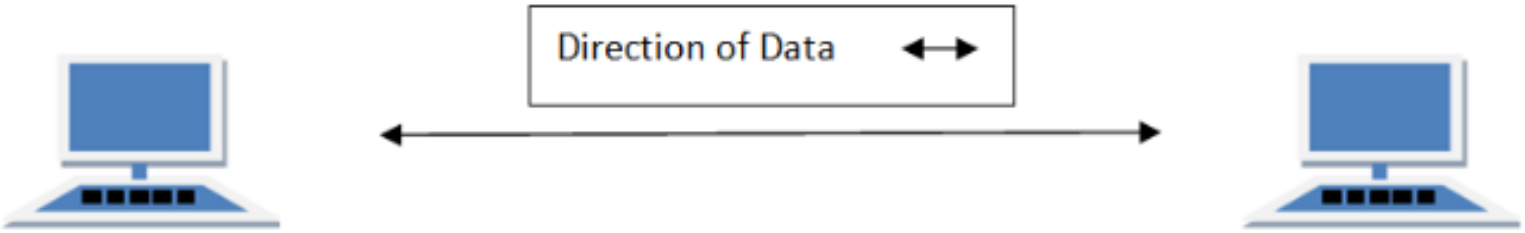
HALF DUPLEX Mode

- Half-duplex data transmission means that data can be transmitted in both directions on a signal carrier, but not at the same time.
- **For example**, on a local area network using a technology that has half-duplex transmission, one workstation can send data on the line and then immediately receive data on the line from the same direction in which data was just transmitted. Hence half-duplex transmission implies a bidirectional line (one that can carry data in both directions) but data can be sent in only one direction at a time.
- Example of half duplex is a Walkie- talkie in which message is sent one at a time but messages are sent in both the directions.

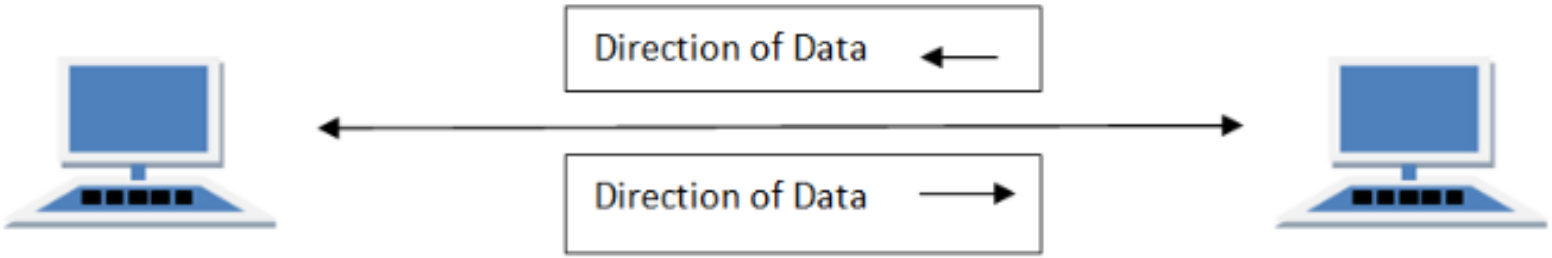


FULL DUPLEX Mode

- In full duplex system we can send data in both the directions as it is bidirectional at the same time in other words, data can be sent in both directions simultaneously. Example :Telephone network, mobile network, satellite communication system etc.
- Example of Full Duplex is a Telephone Network in which there is communication between two persons by a telephone line, using which both can talk and listen at the same time.



In full duplex system there can be two lines one for sending the data and the other for receiving data.



Comparison Chart

Basis for Comparison	Simplex	Half Duplex	Full Duplex
Direction of Communication	Communication is unidirectional.	Communication is two-directional but, one at a time.	Communication is two directional and done simultaneously.
Send/Receive	A sender can send data but, can not receive.	A sender can send as well as receive the data but one at a time.	A sender can send as well as receive the data simultaneously.
Performance	The half duplex and full duplex yields better performance than the Simplex.	The full duplex mode yields higher performance than half duplex.	Full duplex has better performance as it doubles the utilization of bandwidth.
Example	Keyboard and monitor.	Walkie-Talkies.	Telephone.

Transmission Speed

- The rate at which data are moved across a communications channel. Following are the transmission speeds of common LAN and WAN technologies
- Bandwidth of a communication system refers to its data transfer rate (amount of data that it can transfer per unit of time). It is analogous to a road's width. Wider a road, the more traffic it can handle in a given time. Similarly, higher the bandwidth of a communication system, the more data it can transfer in a given time.
- Bandwidth is measured in bits per second , also called baud. Generally, baud is identical to bits per second, hence a rate of 300 baud means 300bps. However, technically, baud refers to number of signal changes per second.

Based on data transmission speeds, there are three basic categories of communication channels (paths):

- **Narrow band:**

Narrow band or sub-voice grade channels have speed in the range of 45 to 300 baud. Low-speed devices and communication systems for low data volumes use narrow channels.

- **Voice-band:**

Voice-band channels have speed up to 9600 baud. Their major application is ordinary telephone voice communication, hence the name "voice-band". Communication systems for data transmission from slow I/O devices to CPU or vice versa use voice-band channels.

- **Broadband:**

Broadband channels have speed of 1 million baud or more. Communication systems for transmission of large volumes of data at high speed (such as high speed computer to computer communication or data transmission to several different devices simultaneously) use broadband channels.

Cost of data transmission service increases with speed. Hence, a thorough analysis of business needs and associated costs is necessary to make a proper choice of communication channel for an application.

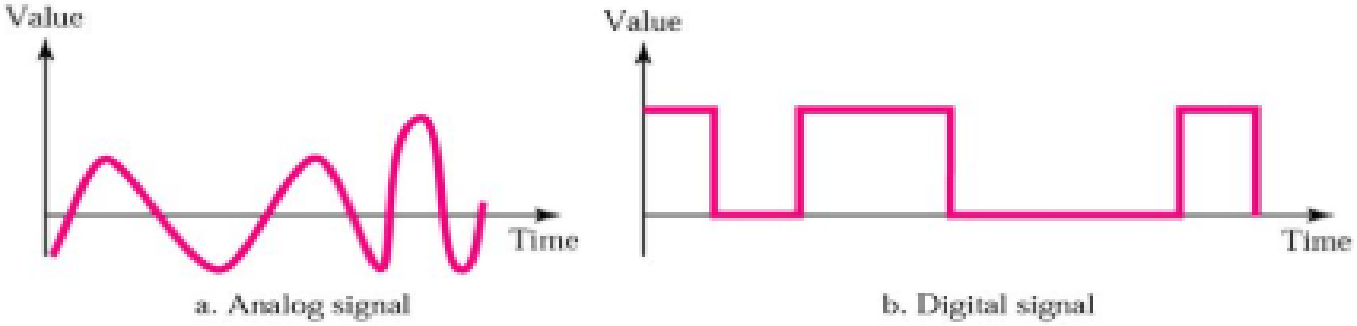
Concept of Signal

Analog Signal

A signal could be an analog quantity that means it is defined with respect to the time. It is a continuous signal. These signals are defined over continuous independent variables. They are difficult to analyze, as they carry a huge number of values. They are very much accurate due to a large sample of values. In order to store these signals, you require an infinite memory because it can achieve infinite values on a real line. Analog signals are denoted by sin waves.

Digital Signal

The word digital stands for discrete values and hence it means that they use specific values to represent any information. In digital signal, only two values are used to represent something i-e: 1 and 0 (binary values). Digital signals are less accurate then analog signals because they are the discrete samples of an analog signal taken over some period of time. However digital signals are not subject to noise. So they last long and are easy to interpret. Digital signals are denoted by square waves.



a. Analog signal

b. Digital signal

	Analog signal transmission	Digital signal transmission
signal	Analog signal is a continuous signal which represents physical measurements.	Digital signals are discrete time signals generated by digital modulation.
Waves	Denoted by sine waves	Denoted by square waves
Representation	Uses continuous range of values to represent information	Uses discrete or discontinuous values to represent information
Example	Human voice in air, analog electronic devices.	Computers, CDs, DVDs, and other digital electronic devices.
Technology	Analog technology records waveforms as they are.	Samples analog waveforms into a limited set of numbers and records them.
Data transmissions	Subjected to deterioration by noise during transmission and write/read cycle.	Can be noise-immune without deterioration during transmission and write/read cycle.
Response to Noise	More likely to get affected reducing accuracy	Less affected since noise response are analog in nature.

Characteristics of Signal

The signal can be represented with three parameters as follows:

The three main characteristics of signals are,

- **Amplitude.** This is the strength of the signal.
- **Frequency**. This is the rate of change the signal undergoes every second, expressed in Hertz (Hz), or cycles per second.
- **Phase**. This is the rate at which the signal changes its relationship to time, expressed as degrees.

Modulation

- The process of impressing low-frequency information to be transmitted on to a high-frequency wave, called the carrier wave, by changing the characteristics of its amplitude, frequency, or phase angle is called modulation.
- The process of altering the characteristics of the amplitude, frequency, or phase angle of the high-frequency signal in accordance with the instantaneous value of the modulating wave is called modulation.

Functions of the Carrier Wave

- The main function of the carrier wave is to carry the audio or video signal from the transmitter to the receiver. The wave that is resulted due to superimposition of audio signal and carrier wave is called the modulated wave.

Why Modulation is Necessary

- Modulation is a scheme under which the signal is first modified to suitable form and mixed with the carrier for transmission.
- To transfer the message signal from one site another site over a long distance without any interference and loss for that we are using modulation.

Modulation is important due to following basic reasons:

- Low frequency signals can't be transmitted for long distance. That's why we are modulating the information signals.
- Need of bandwidth: suppose many people are talking at the same time, we just cant make out the difference who is talking what, so bandwidth is provided to each wave and it is done over high frequency to save the quality of signal.

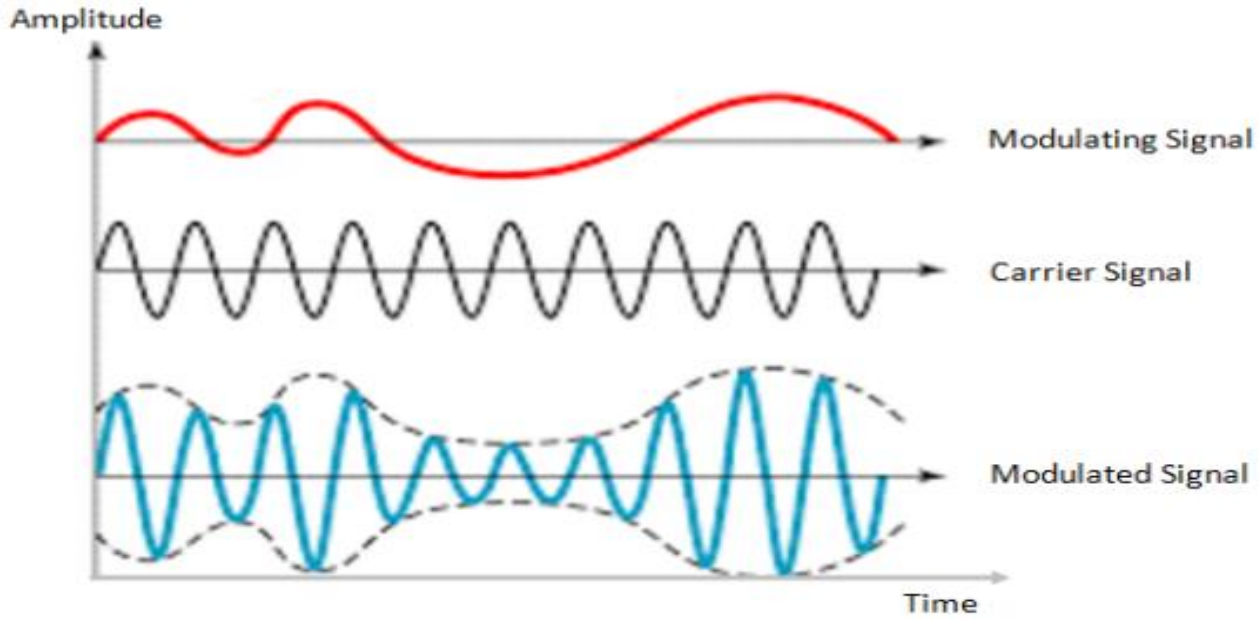
Modulation is necessary because of following advantages:

1. Reduction in height of antenna.
2. Avoids mixing of signals.
3. Increase the range of communication.
4. Multiplexing is possible.
5. Improves quality of reception

Types of modulation

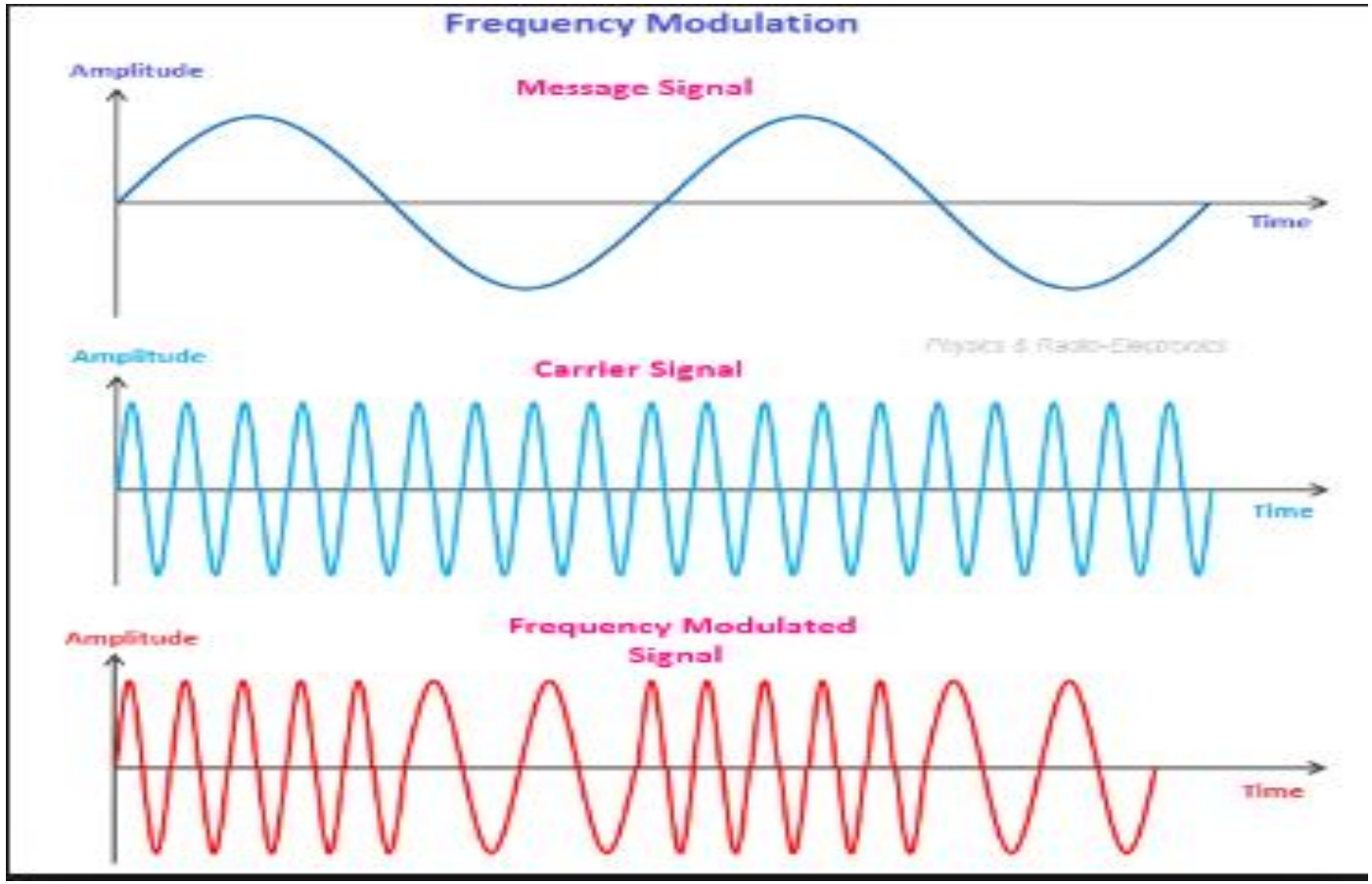
Amplitude modulation

- Amplitude modulation was developed in the beginning of the 20th century. It was the earliest modulation technique used to transmit voice by radio. This type of modulation technique is used in electronic communication.
- In this modulation, the amplitude of the carrier signal varies in accordance with the message signal, and other factors like phase and frequency remain constant.
- The modulated signal is shown in the below figure, and its spectrum consists of the lower frequency band, upper frequency band and carrier frequency components. This type of modulation requires more power and greater bandwidth; filtering is very difficult. Amplitude modulation is used in computer modems, VHF aircraft radio, and in portable two-way radio



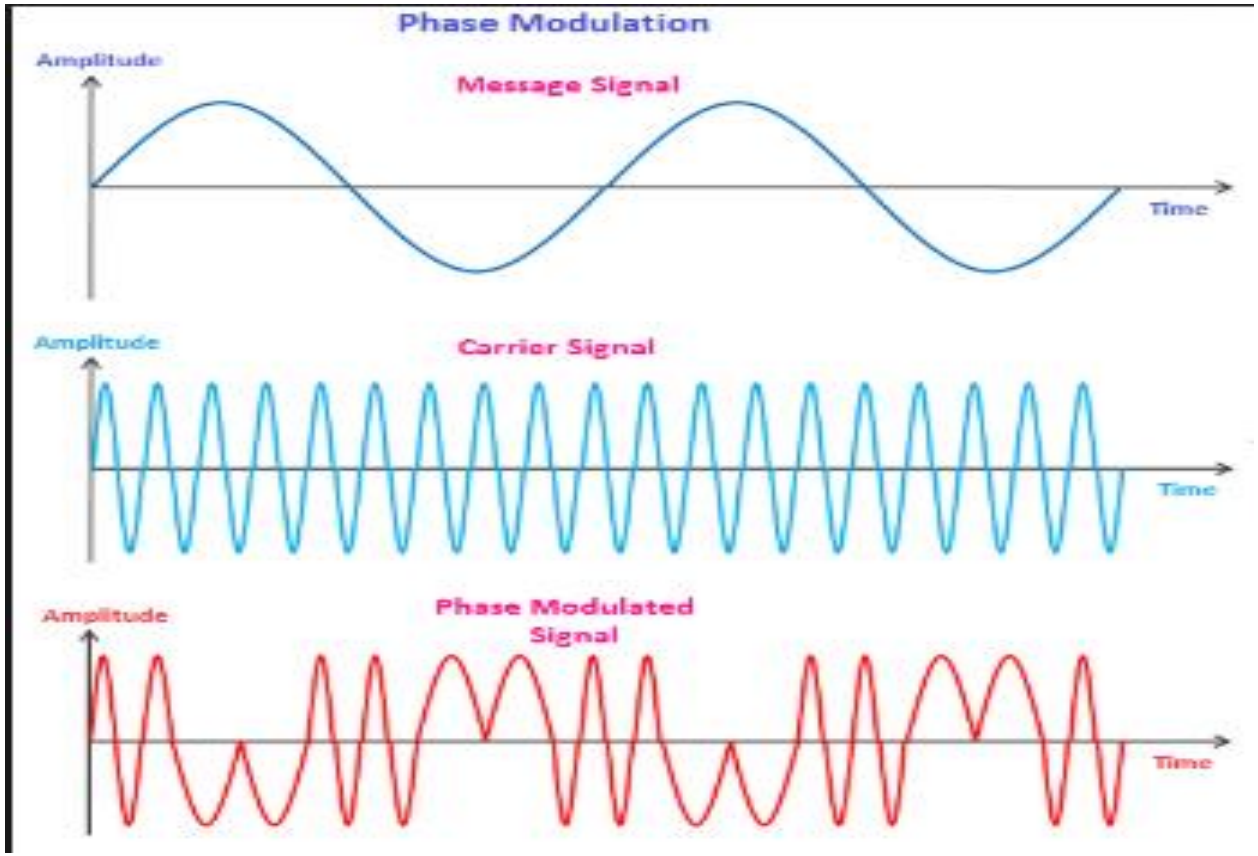
Frequency Modulation

- In this type of modulation, the frequency of the carrier signal varies in accordance with the message signal, and other parameters like amplitude and phase remain constant. Frequency modulation is used in different applications like radar, radio and telemetry, seismic prospecting and monitoring newborns for seizures via EEG, etc.
- This type of modulation is commonly used for broadcasting music and speech, magnetic tape recording systems, two way radio systems and video transmission systems. When noise occurs naturally in radio systems, frequency modulation with sufficient bandwidth provides an advantage in cancelling the noise.



Phase Modulation

- In this type of modulation, the phase of the carrier signal varies in accordance with the message signal. When the phase of the signal is changed, then it affects the frequency. So, for this reason, this modulation is also comes under the frequency modulation.
- Generally, phase modulation is used for transmitting waves. It is an essential part of many digital transmission coding schemes that underlie a wide range of technologies like GSM, WiFi, and satellite television. This type of modulation is used for signal generation in al synthesizers, such as the Yamaha DX7 to implement FM synthesis.



DIGITAL MODULATION TECHNIQUES

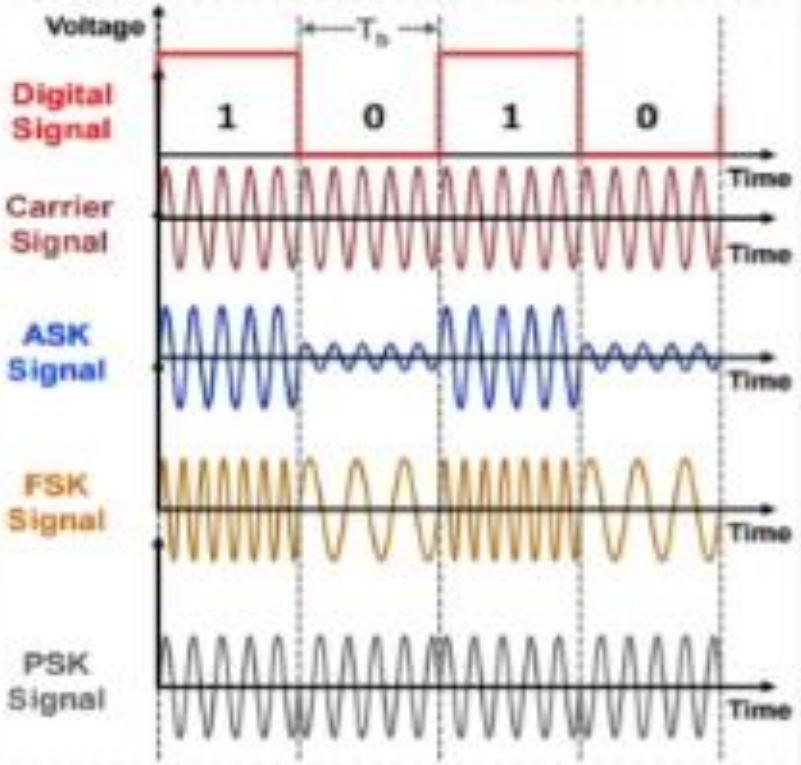
1. **Baseband digital message signal**: $m(t)$

2. **Analog sinusoidal carrier signal**
   A. Carrier signal: $A_c \cos(2\pi f_c t + \phi_c)$

3. **ASK: Amplitude Shift Keying**
   A. Message signal changes the carrier's **amplitude** : $A_i(t)$.

4. **FSK: Frequency Shift Keying.**
   A. Message signal changes the carrier's **frequency** : $f_i(t)$.

5. PSK: Phase Shift Keying.
   A. Message signal changes the carrier's phase : $\phi_i(t)$.



Computer Network

- A telecommunications network is a collection of terminal nodes;—links are connected so as to enable telecommunication between the terminals.
- Computer Network is a group of computer and associated peripherals connected by a communication channel capable of sharing files and other resources between the several users. It is the collection of hardware and software that enables a group of computers to communicate and share resources (resources may be data, software or hardware) with each other. Each computer or a device connected on the network is called node.
- **Example:** Instead of linking each computer to its own printer, all computers can be linked to a common printer for shared access by multiple users.

Advantages of Computer Networking

- Easy Communication and Speed
- Ability to Share Files, Data and Information
- Sharing Hardware
- Sharing Software
- Security
- Speed
- It is highly flexible.
- It increases cost efficiency.
- It boosts storage capacity.

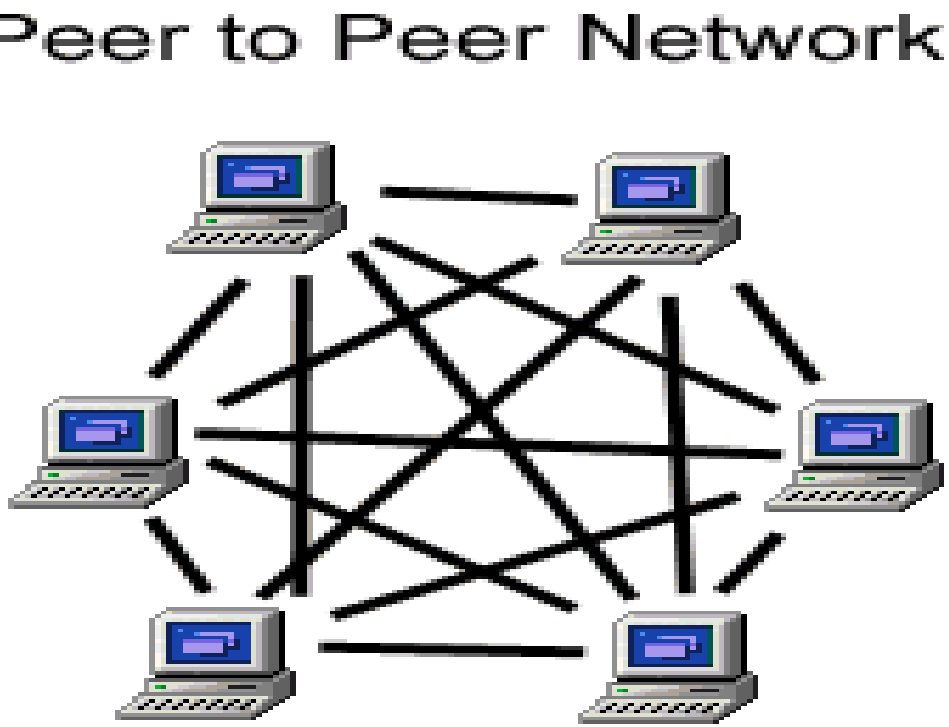
Disadvantages of Networking

- Breakdowns and Possible Loss of Resources
- Expensive to Build
- Security Threats
- Bandwidth Issues
- It lacks robustness
- It requires an efficient handler
- It allows for more presence of computer viruses and malware

Types of Network

On The Basis Of Network Architecture

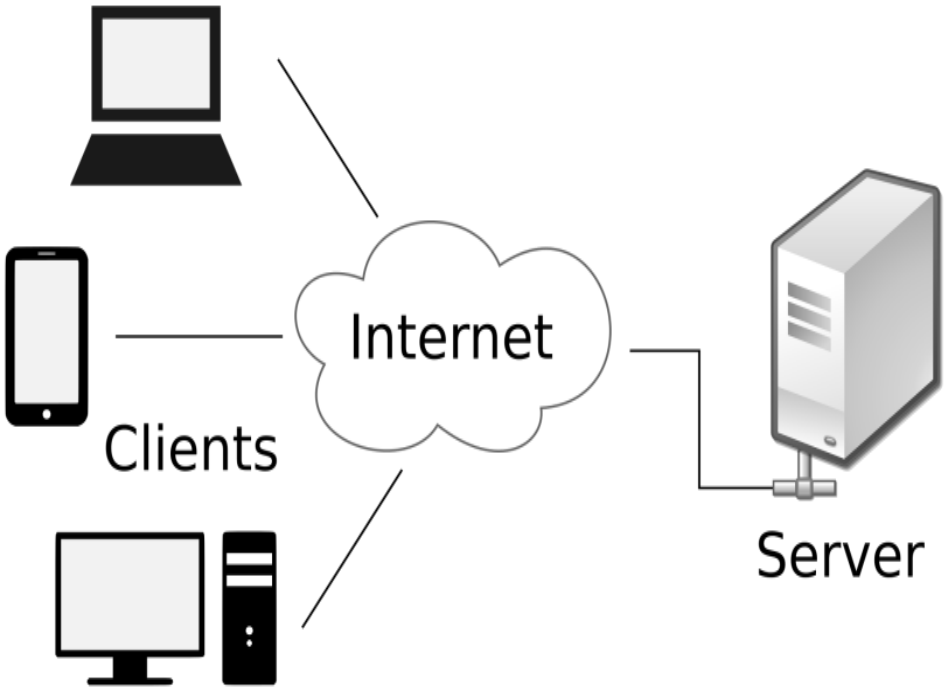
- **Peer-to-Peer Network (P2P)**



- **P2P Stands for "Peer to Peer." In a P2P network, the "peers" are computer systems which are connected to each other via the Internet.**
- **Files can be shared directly between systems on the network without the need of a central server.**
- **In other words, each computer on a P2P network becomes a file server as well as a client.**
- **The only requirements for a computer to join a peer-to-peer network are an Internet connection and P2P software.**
- **Common P2P software programs include Kazaa, Limewire, BearShare, Morpheus, and Acquisition.**
- **These programs connect to a P2P network, such as "Gnutella," which allows the computer to access thousands of other systems on the network.**
- **Once connected to the network, P2P software allows you to search for files on other people's computers.**
- **Meanwhile, other users on the network can search for files on your computer, but typically only within a single folder that you have designated to share.**
- **While P2P networking makes file sharing easy and convenient, is also has led to a lot of software piracy and illegal music downloads.**
- **Therefore, it is best to be on the safe side and only download software and music from legitimate websites.**

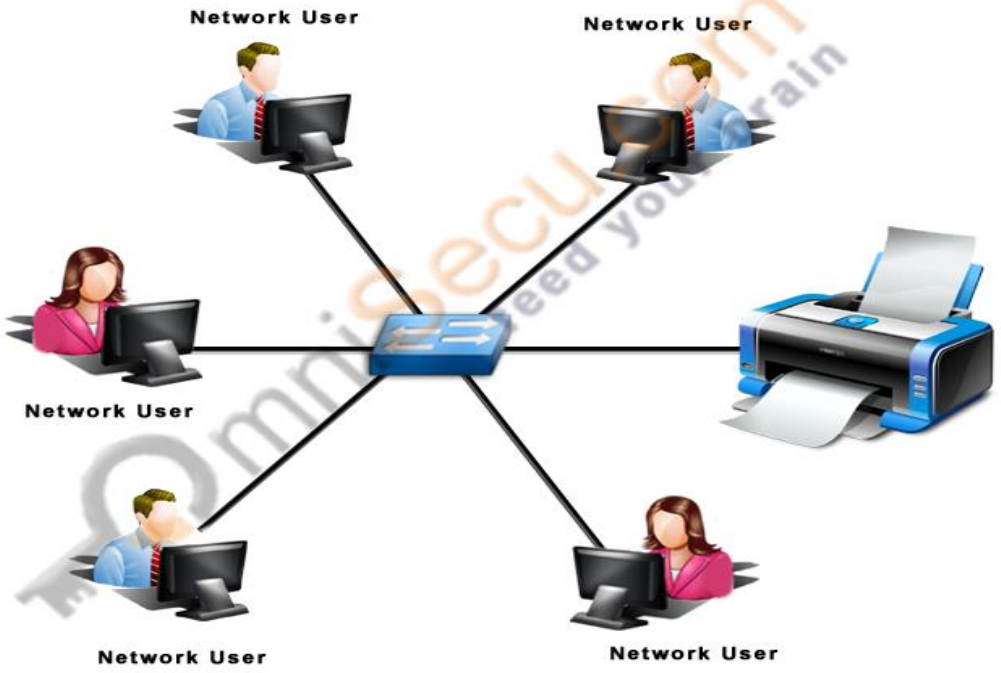
Client/Server Network

- A **client-server network** is designed for end-users, called **clients**, to access resources such as files, songs, video collections, or some other service from a central computer called a **server**.
- A server's sole purpose is to do what its name implies - serve its clients! You may have been using this configuration and not even have known it. Have you ever played Xbox Live or used the PlayStation Network? Your Xbox One is the client, and when it logs into the network, it contacts the Xbox Live servers to retrieve gaming resources like updates, video, and game demos.
- The client uses the **network** as a way to connect with and speak to the server. Just as the customer speaks to his server, the client uses the network to send and receive communications about its order, or request. The server will take the request and make sure that the request is valid. If everything checks out okay, then the server will fetch the request and serve the client.


Internet
Clients
Server

Depending upon the geographical area computer network can be classified into different types:

Local Area Network (LAN)



LOCAL AREA NETWORK (LAN)

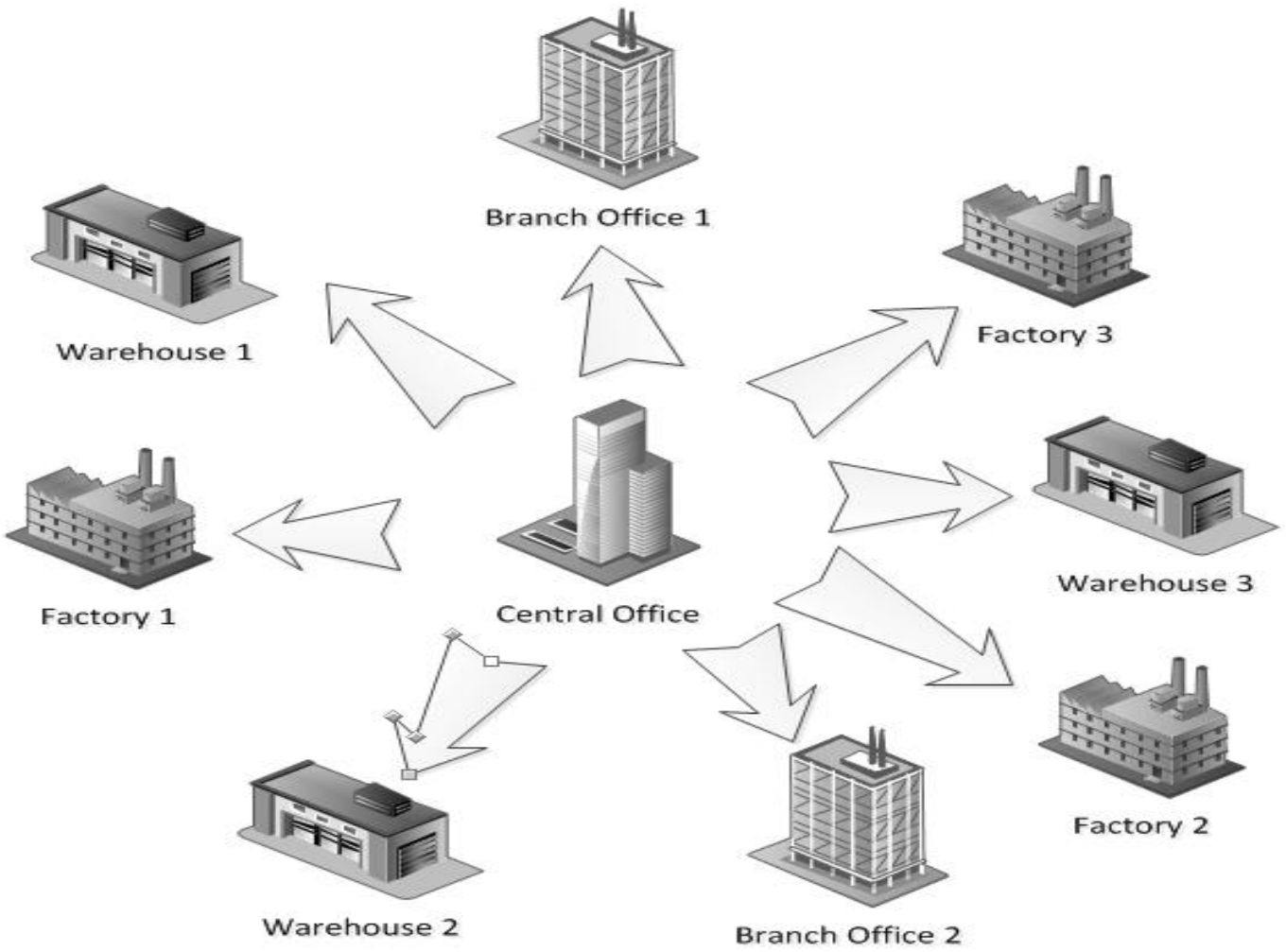
Features:

- It covers small geographical area.
- It uses guided transmission media.
- All the components share common protocol
- Communication cost is low.
- Speed is 1 mbps to 100 mbps.
- It is private network so, ownership is of single organization.
- No special security is needed.

LAN has the following characteristics:

- Coverage area is generally a few kilometers.
- Using different dedicated transmission medium you can achieve the transmission rate of 1 Mb/s to 100 Mbit / sec or higher, with the further development of LAN technology is currently being developed toward higher speed (e.g. 155Mbps, 655Mbps and 1000Mbps etc.).
- In LAN you can run the multiple devices to share a transmission medium.
- You can use the different topology mainly bus and ring in LAN.
- The communication quality is better IN LAN, the transmission error rate are low as compare to WAN.
- LAN support a variety of communications transmission medium such as a Ethernet cable (thin cable, thick cable, and twisted pair), fiber and wireless transmission.
- A LAN usually has low cost, installation, expansion and maintenance and LAN installation is relatively simple, good scalability.

Metropolitan Area Network (MAN)



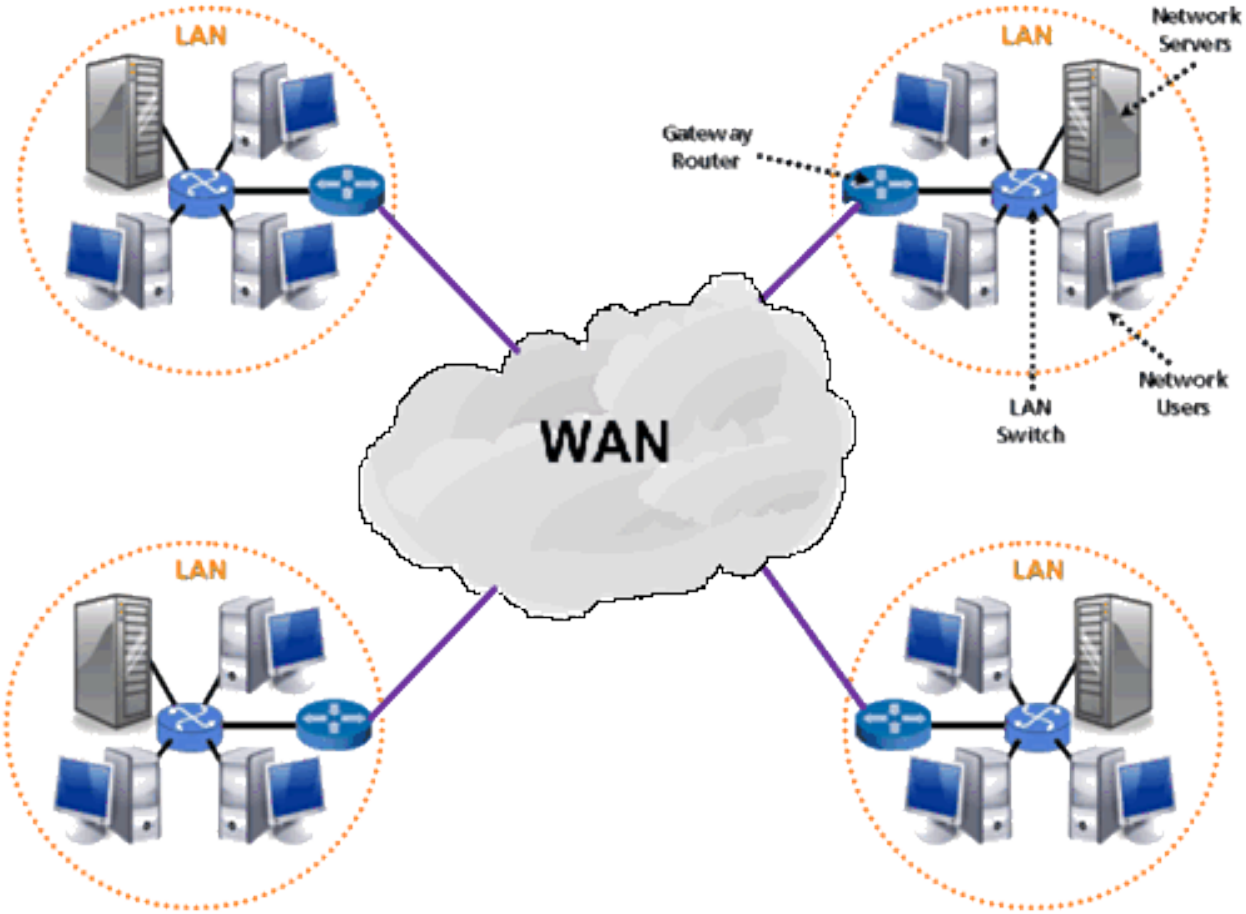
Features:

- It is larger than LAN.
- Different types of protocols can be used.
- Communication cost is high.
- Special security is needed.
- Speed is slower than LAN 1 to 10 mbps.
- Network size generally ranges from 5 to 50 km. It may be as small as a group of buildings in a campus to as large as covering the whole city.
- Data rates are moderate to high.
- In general, a MAN is either owned by a user group or by a network provider who sells service to users, rather than a single organization as in LAN.
- It facilitates sharing of regional resources.
- They provide uplinks for connecting LANs to WANs and Internet.

Example of MAN

- Cable TV network
- Telephone networks providing high-speed DSL lines
- IEEE 802.16 or WiMAX, that provides high-speed broadband access with Internet connectivity to customer

Wide Area Network (WAN)



Features:

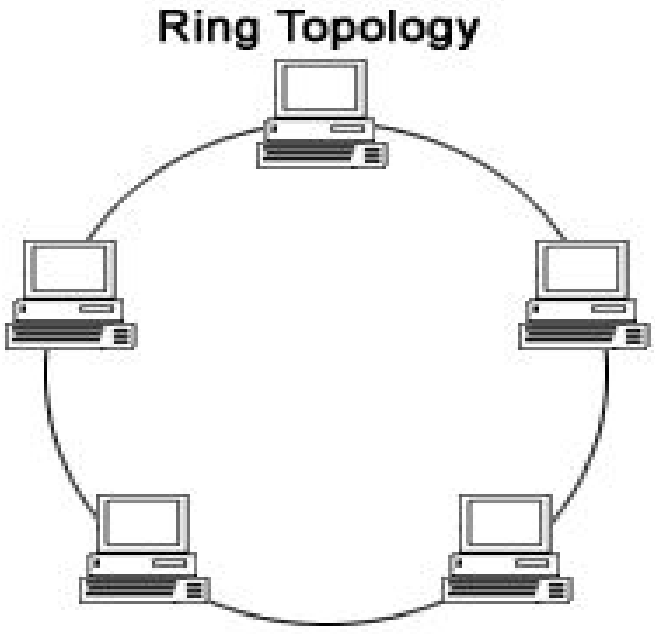
- It can support large geographical area.
- Wireless media, especially communication satellite is used.
- Communication cost is high.
- Speed is lower than LAN and MAN (1mbps).
- Multiple computers are connected together
- It connect devices that are separated by a broader geographical area than a LAN
- A WAN usually interconnects multiple LANs
- Communication links between computers are provided by telephone networks, public data networks, satellites etc.
- Links are of low capacity (that is low data rate)
- Bit error rate is higher (1 in 100,000) compared to that for a LAN.
- The data rates of WAN is low as compare to data transfer rate of local area network , and the signal propagation delay is much greater than the local area network. The typical data rates for WAN are 56kbps to 155Mbps, 622Mbps, 2.4 Gbps or higher speed WAN.

LAN Topologies

A *network topology* is the pattern in which *nodes* (i.e., computers, printers, routers or other devices) are connected to a local area network (LAN) or other network via links (e.g., twisted pair copper wire cable or optical fiber cable).

Ring Topology

In a ring topology each device is connected directly to two other devices, one on either side of it, to form a closed loop. This topology is relatively expensive and difficult to install, but it offers high bandwidth and can span large distances. A variation is the *token ring*, in which signals travel in only one direction around the loop, carried by a so-called *token* from node to node.



Advantages of Ring Topology

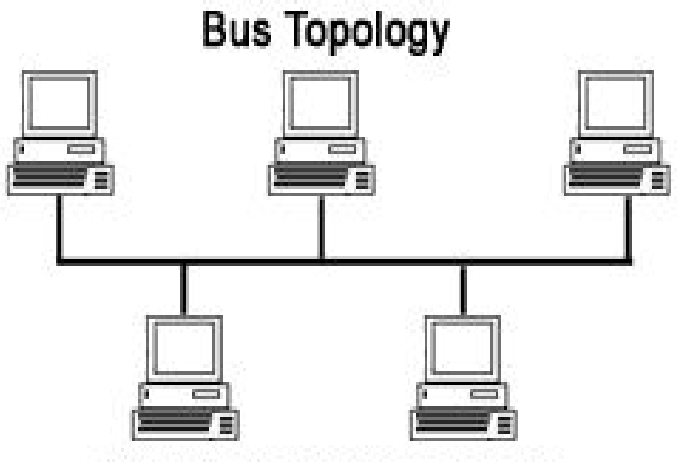
- Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
- Cheap to install and expand

Disadvantages of Ring Topology

- Troubleshooting is difficult in ring topology.
- Adding or deleting the computers disturbs the network activity.
- Failure of one computer disturbs the whole network.

Bus Topology

With the Bus topology, all workstations are connect directly to the main backbone that carries the data. Traffic generated by any computer will travel across the backbone and be received by all workstations. This works well in a small network of 2-5 computers, but as the number of computers increases so will the network traffic and this can greatly decrease the performance and available bandwidth of your network.



Advantages of Bus Topology

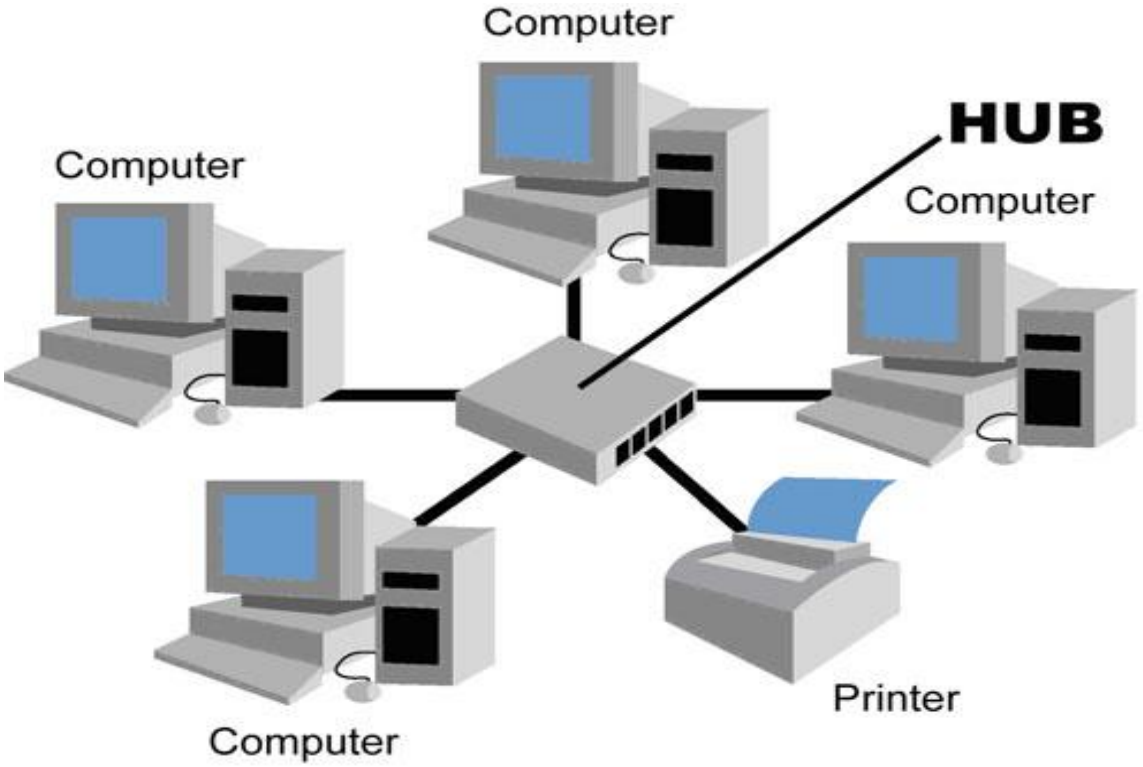
- It is cost effective.
- Cable required is least compared to other network topology.
- Used in small networks.
- It is easy to understand.
- Easy to expand joining two cables together.

Disadvantages of Bus Topology

- Cables fails then whole network fails.
- If network traffic is heavy or nodes are more the performance of the network decreases.
- Cable has a limited length.
- It is slower than the ring topology.

Star Topology

In a star topology all devices are connected directly to a central computer or server. Such networks are relatively easy to install and manage, but bottlenecks can occur because all data must pass through the central device.



Advantages of Star Topology

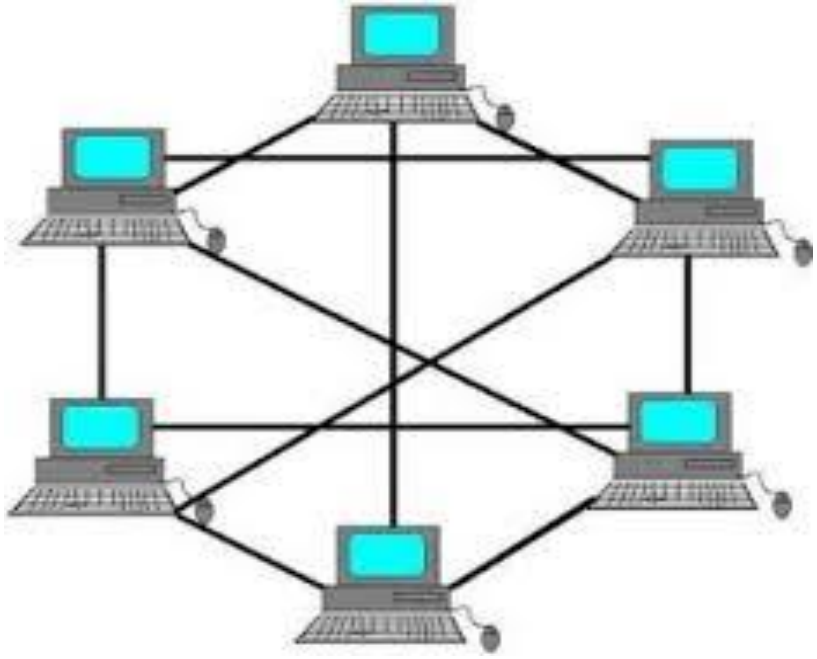
- Fast performance with few nodes and low network traffic.
- Hub can be upgraded easily.
- Easy to troubleshoot.
- Easy to setup and modify.
- Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

- Cost of installation is high.
- Expensive to use.
- If the hub fails then the whole network is stopped because all the nodes depend on the hub.
- Performance is based on the hub that is it depends on its capacity

Mesh Topology

In a mesh topology, each computer is connected to every other computer by a separate cable. This configuration provides redundant paths through the new work, so if one computer blows up, you don't lose the network :) On a large scale, you can connect multiple LANs using mesh topology with leased telephone lines, Thicknet coaxial cable or fiber optic cable.
Again, the big advantage of this topology is its backup capabilities by providing multiple paths through the network.



Advantages of Mesh Topology

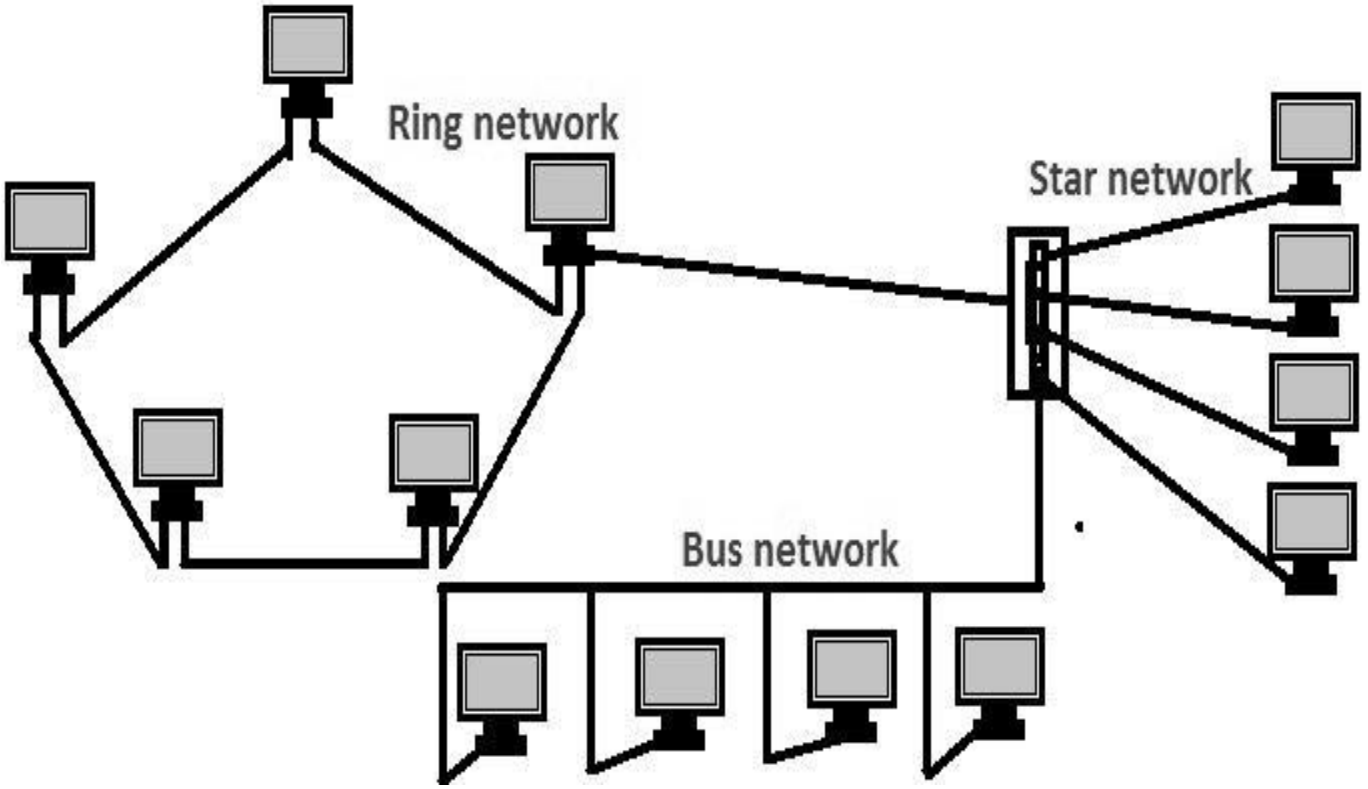
- Each connection can carry its own data load.
- It is robust.
- Fault is diagnosed easily.
- Provides security and privacy.

Disadvantages of Mesh Topology

- Installation and configuration is difficult.
- Cabling cost is more.
- Bulk wiring is required.

Hybrid Topology

With the hybrid topology, two or more topologies are combined to form a complete network. For example, a hybrid topology could be the combination of a star and bus topology. These are also the most common in use.



Advantages of Hybrid Topology

- Reliable as Error detecting and trouble shooting is easy.
- Effective.
- Scalable as size can be increased easily.
- Flexible.

Disadvantages of Hybrid Topology

- Complex in design.
- Costly.

Transmission media/communication media

- It is a pathway that carries the information from sender to receiver. We use different types of cables or waves to transmit data. Data is transmitted normally through electrical or electromagnetic signals.
- **Types of Transmission Media** Transmission media is broadly classified into two groups.

1. **Wired or Guided Media or Bounded Transmission Media**
2. **Wireless or Unguided Media or Unbounded Transmission Media**

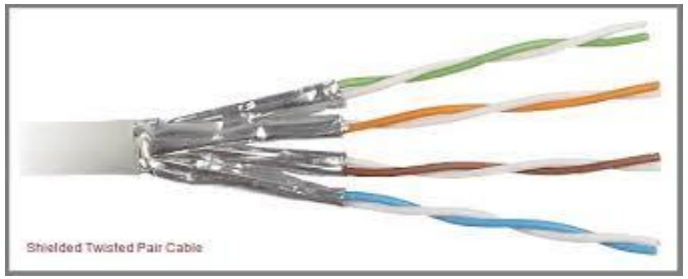
Wired or Guided Media or Bound Transmission Media

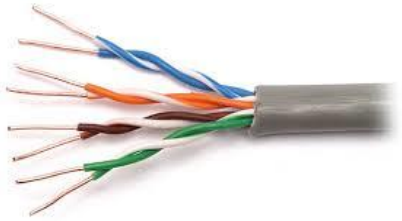
Twisted Pair Cable

- A type of cable that consists of two independently insulated wires twisted around one another. The use of two wires twisted together helps to reduce crosstalk and electromagnetic induction. While twisted-pair cable is used by older telephone networks and is the least expensive type of local-area network (LAN) cable.
- This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily.

Types of Twisted pair cable

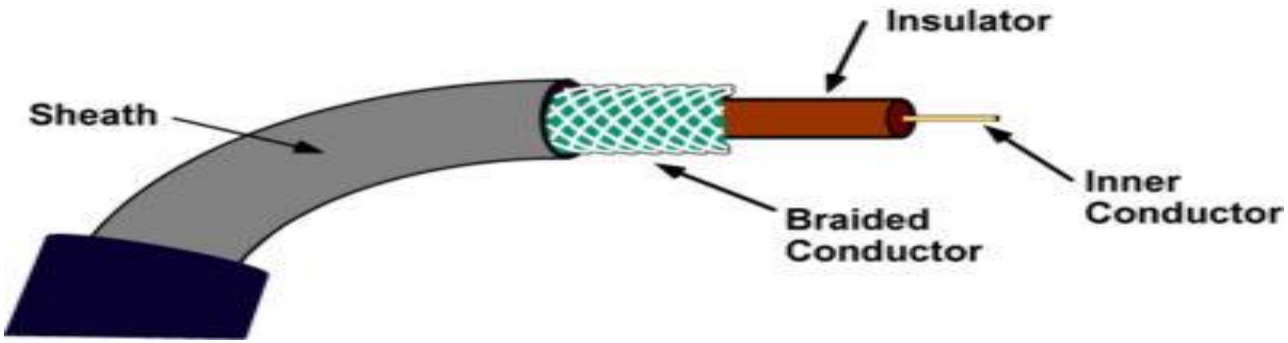
STP	UTP
STP cables are shielded.	UTP cables are unshielded.
STP cables are more immune to interference and noise than UTP cables	UTP cables are less immune to interference and noise than STP cables
STP cables are better at maximizing bandwidth compared to UTP cables	UTP cables are lower at maximizing bandwidth compared to STP cables
STP cables cost more per meter compared to UTP cables	UTP cables cost less per meter compared to STP cables
STP cables are heavier per meter compared to UTP cables	STP cables are lighter per meter compared to STP cables
STP is used in more high-end applications	UTP cables are more prevalent in small networks





Coaxial Cable

- Coaxial cable has the following layers (starting from the center): a metallic rod-shaped inner conductor, an insulator covering the rod, a metallic outer conductor (shield), an insulator covering the shield, and a plastic cover.
- Coaxial cable can carry signals of higher frequency ranges than twisted-pair cable.
- Coaxial cable is used in cable TV networks and traditional Ethernet LANs.



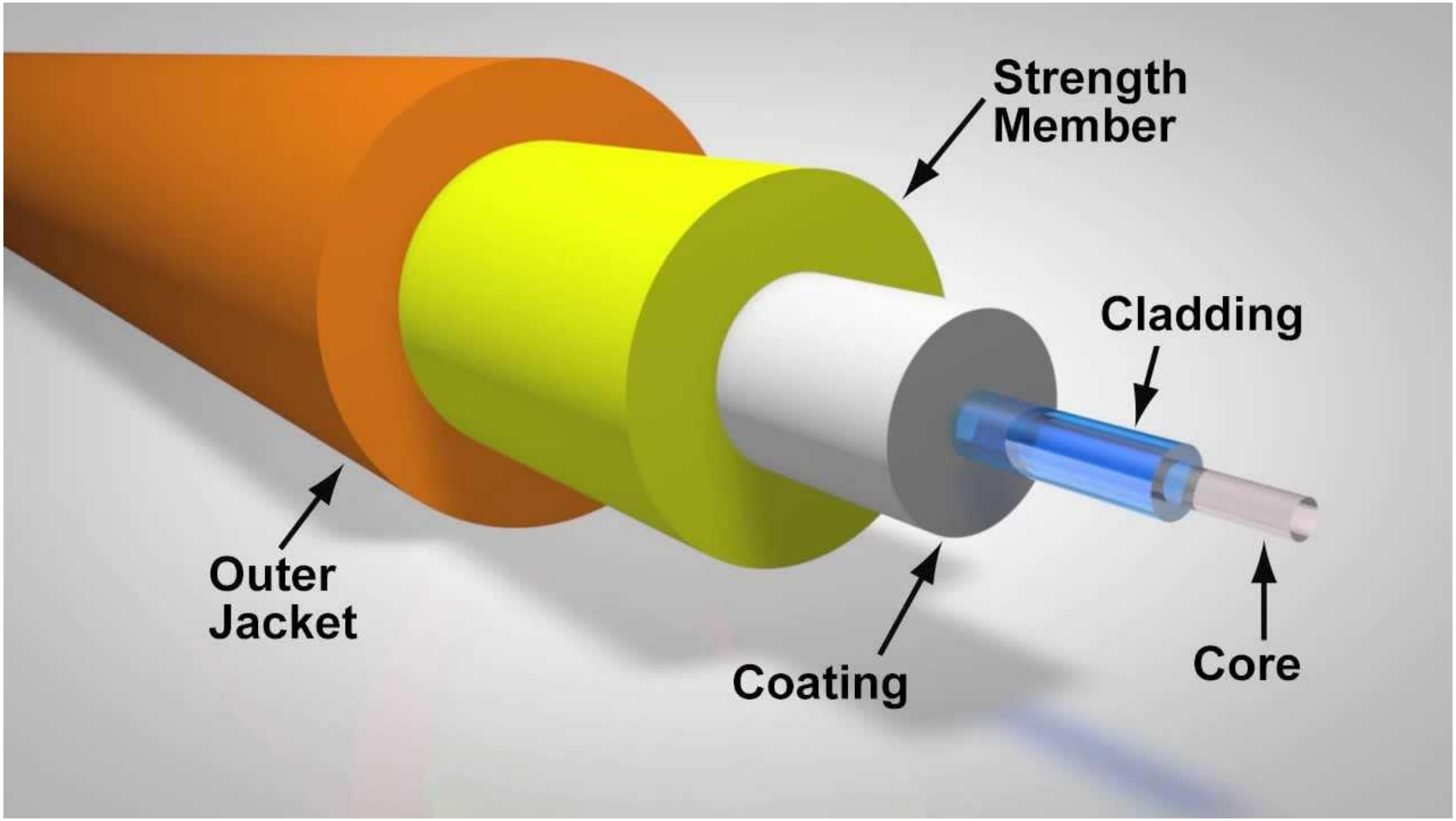
Advantages:

- Bandwidth is high
- Used in long distance telephone lines.
- Transmits digital signals at a very high rate of 10Mbps.
- Much higher noise immunity
- Data transmission without distortion.
- The can span to longer distance at higher speeds as they have better shielding when compared to twisted pair cable

Disadvantages:

- Single cable failure can fail the entire network.
- Difficult to install and expensive when compared with twisted pair.
- If the shield is imperfect, it can lead to grounded loop.

Fiber Optic Cable



Advantages :

- Provides high quality transmission of signals at very high speed.
- These are not affected by electromagnetic interference, so noise and distortion is very less.
- Used for both analog and digital signals.

Disadvantages :

- It is expensive
- Difficult to install.
- Maintenance is expensive and difficult.

Wireless/Unbounded/Unguided Transmission Media

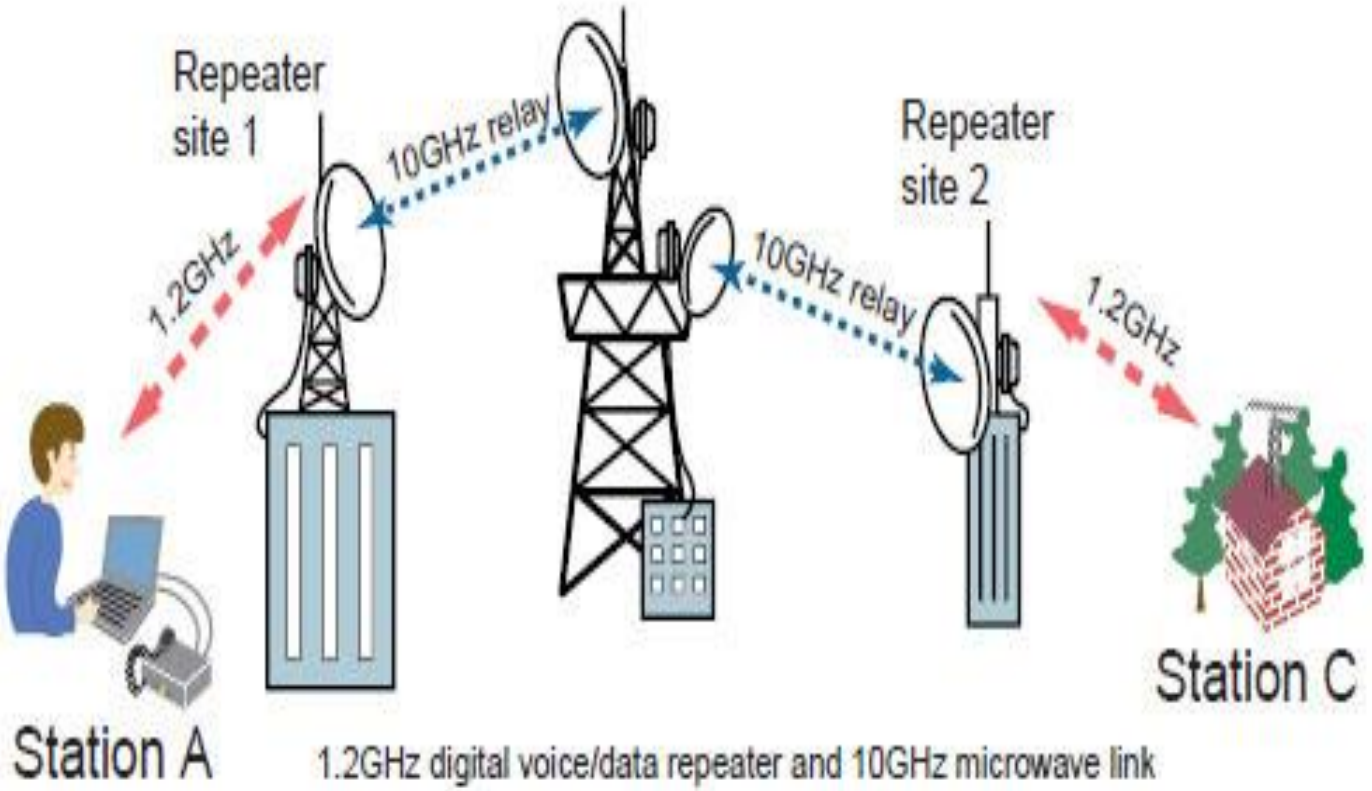
- Unguided media relates to data transmission through the air and is commonly referred to as wireless. The transmission and reception of data is carried out using antenna.

Types of unguided/ unbounded media

1. Microwave Communication
2. Satellite Communication
3. Radio Transmission

Microwave Communication

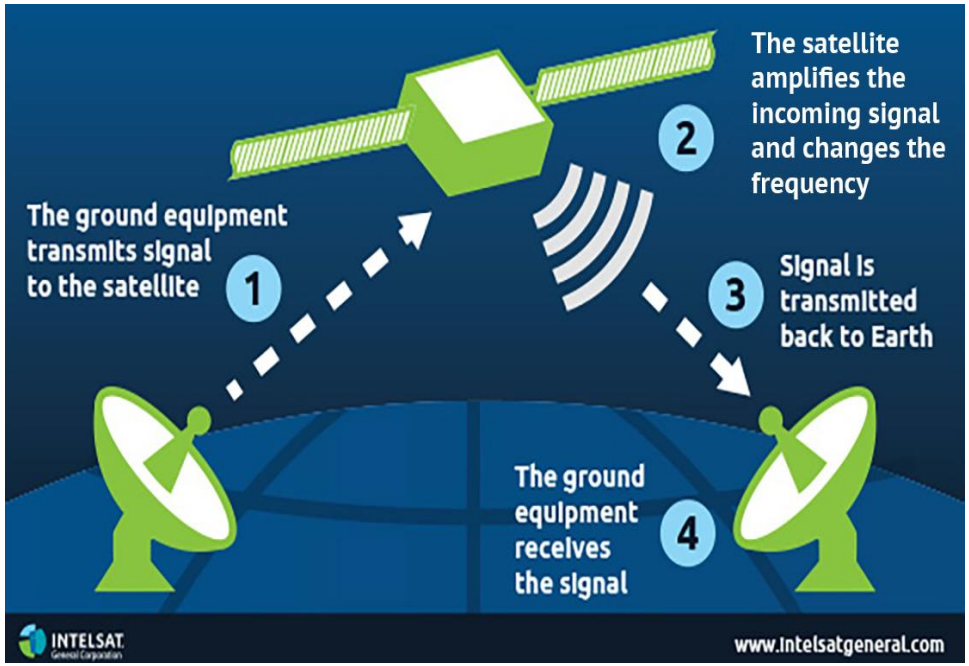
- In microwave transmission, data is transmitted through air or space, instead of through cables or wires. Microwaves are high frequency radio waves. Microwave uses line-of-sight transmission through space. The line-of-sight means that data signals (or waves) can only travel in straight lines and cannot bend.



1.2GHz digital voice/data repeater and 10GHz microwave link

Satellite Communication

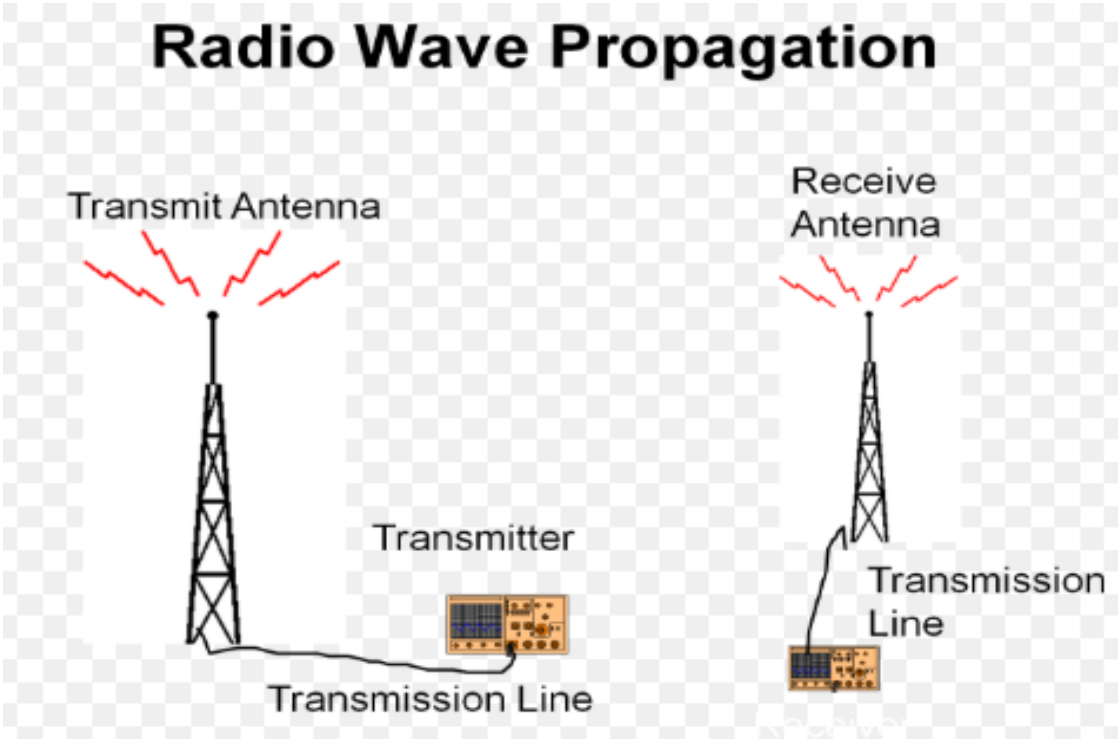
- A satellite receives microwave signals (or messages) from earth station. It amplifies the signals and sends them to another earth station. In this way, data is transferred from one location to another. Data transmission speed of satellite is very fast.
- It is approximately 22,300 miles above the earth. Each earth station consists of large dish antenna


The satellite amplifies the incoming signal and changes the frequency
2
The ground equipment transmits signal to the satellite
1
3
Signal is transmitted back to Earth
The ground equipment receives the signal
4
INTELSAT
www.Intelsatgeneral.com


Receiving signal
Transmitted signal
36000 km
Up-link
Down-link
Transmitting Antenna
Receiving Antenna
Earth

Radio transmission

Radio transmission works with or without line of sight. If line of sight is possible then transmission can take place between sending antenna and receiving antenna. The placement of antenna has to take into account the curvature of the Earth with antenna being built taller accordingly. This will also allow for greater transmission distances. If line of sight cannot be implemented then signals can be broadcast to the upper layers or the atmosphere or space and then transmitted back to Earth.

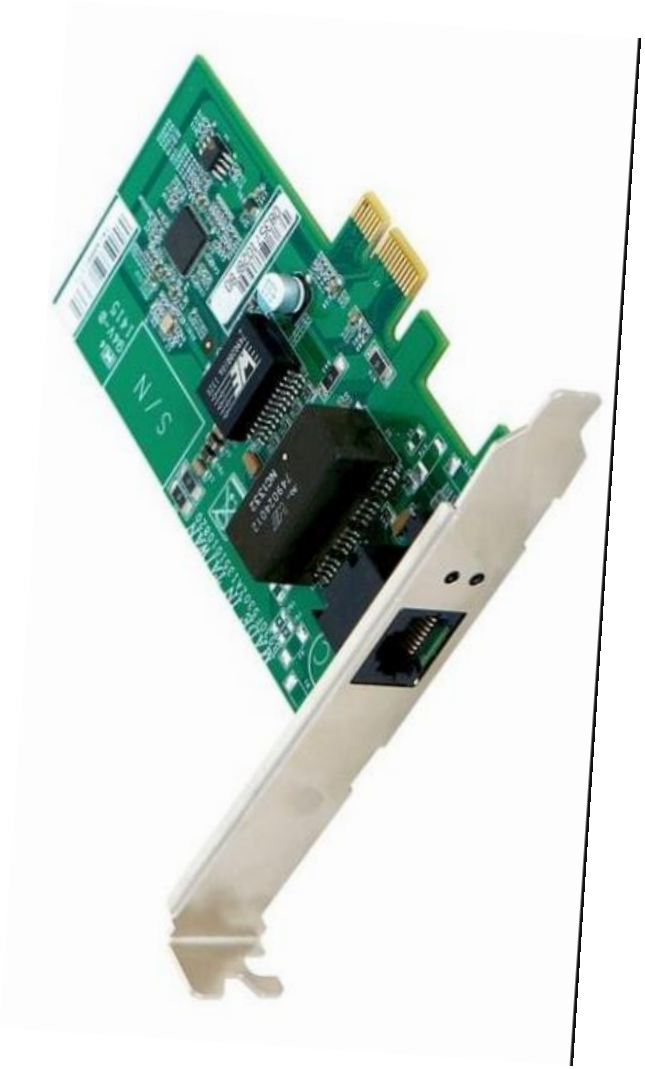


Network devices

- **Networking hardware**, also known as **network equipment** or **computer networking devices**, are physical devices which are required for communication and interaction between devices on a computer network. Specifically, they mediate data in a computer network. Units which are the last receiver or generate data are called hosts or data terminal equipment.
- Networking devices may include gateways, routers, network bridges, modems, wireless access points, networking cables, line drivers, switches, hubs, and repeaters; and may also include hybrid network devices such as multilayer switches, protocol converters, bridge routers, proxy servers, firewalls, network address translators, multiplexers, network interface controllers, wireless network interface controllers, ISDN terminal adapters and other related hardware.

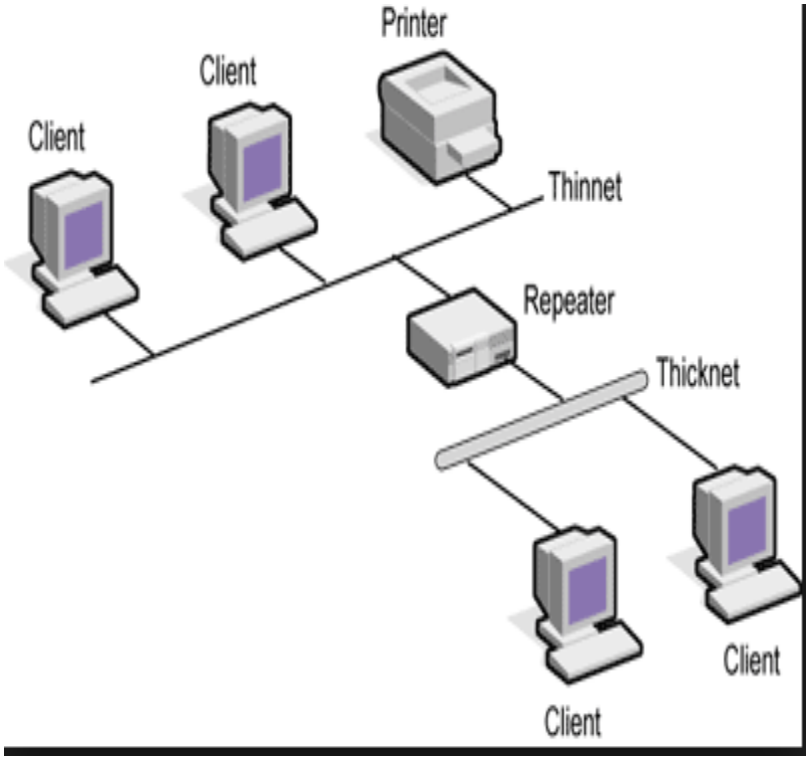
Network Interface Card (NIC)

- A network interface card (NIC) is a hardware component, typically a circuit board or chip, which is installed on a computer so that it can connect to a network. Modern NICs provide functionality to computers such as support for I/O interrupt, direct memory access (DMA) interfaces, data transmission, network traffic engineering and partitioning.
- A NIC provides a computer with a dedicated, full-time connection to a network by implementing the physical layer circuitry necessary for communicating with a data link layer standard, such as Ethernet or Wi-Fi. Each card represents a device and can prepare, transmit and control the flow of data on the network.
- The NIC uses the OSI model to send signals at the physical layer, transmit data packets at the network layer and operate as an interface at the TCP/IP layer.



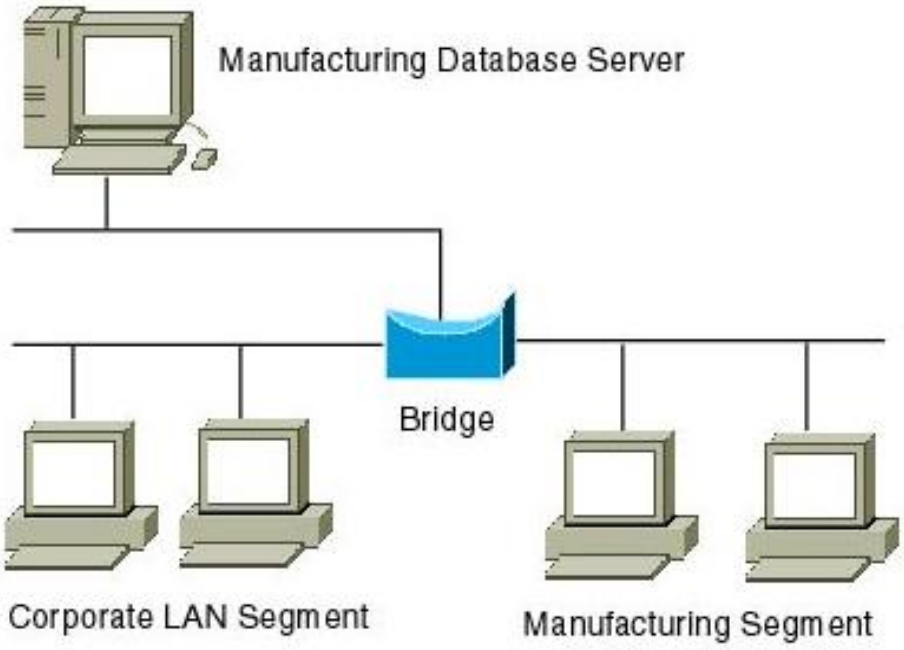
Repeater

- A repeater is a network device that retransmits a received signal with more power and to an extended geographical or topological network boundary than what would be capable with the original signal.
- A repeater is implemented in computer networks to expand the coverage area of the network, repropagate a weak or broken signal and or service remote nodes. Repeaters amplify the received/input signal to a higher frequency domain so that it is reusable, scalable and available.
- Repeaters were introduced in wired data communication networks due to the limitation of a signal in propagating over a longer distance and now are a common installation in wireless networks for expanding cell size.
- Repeaters are also known as signal boosters.



Bridge

- A bridge operates at data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.
- Bridge devices work at the data link layer of the Open System Interconnect (OSI) model, connecting two different networks together and providing communication between them. Bridges are similar to repeaters and hubs in that they broadcast data to every node. However, bridges maintain the media access control (MAC) address table as soon as they discover new segments, so subsequent transmissions are sent to only to the desired recipient.
- Bridges are also known as Layer 2 switches.



HUB

- A hub, also called a network hub, is a common connection point for devices in a network. Hubs are devices commonly used to connect segments of a LAN. The hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.
- A **hub** is the most basic networking device that connects multiple computers or other network devices together. Unlike a network switch or router, a network hub has no routing tables or intelligence on where to send information and broadcasts all network data across each connection. Most hubs can detect basic network errors such as collisions, but having all information broadcast to multiple ports can be a security risk and cause bottlenecks. In the past, network hubs were popular because they were cheaper than a switch or router. Today, switches do not cost much more than a hub and are a much better solution for any network.

Switch

- A **network switch** (also called **switching hub**, **bridging hub**, officially **MAC bridge**) is a computer networking device that connects devices on a computer network by using packet switching to receive, process, and forward data to the destination device.
- A network switch is a multiport network bridge that uses hardware addresses to process and forward data at the data link layer (layer 2) of the OSI model. Some switches can also process data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.
- A switch in an Ethernet-based LAN reads incoming TCP/IP data packets/frames containing destination information as they pass into one or more input ports. The destination information in the packets is used to determine which output ports will be used to send the data on to its intended destination.
- Switches are similar to hubs, only smarter. A hub simply connects all the nodes on the network -- communication is essentially in a haphazard manner with any device trying to communicate at any time, resulting in many collisions. A switch, on the other hand, creates an electronic tunnel between source and destination ports for a split second that no other traffic can enter. This results in communication without collisions.
- Switches are similar to routers as well, but a router has the additional ability to forward packets between different networks, whereas a switch is limited to node-to-node communication on the same network.

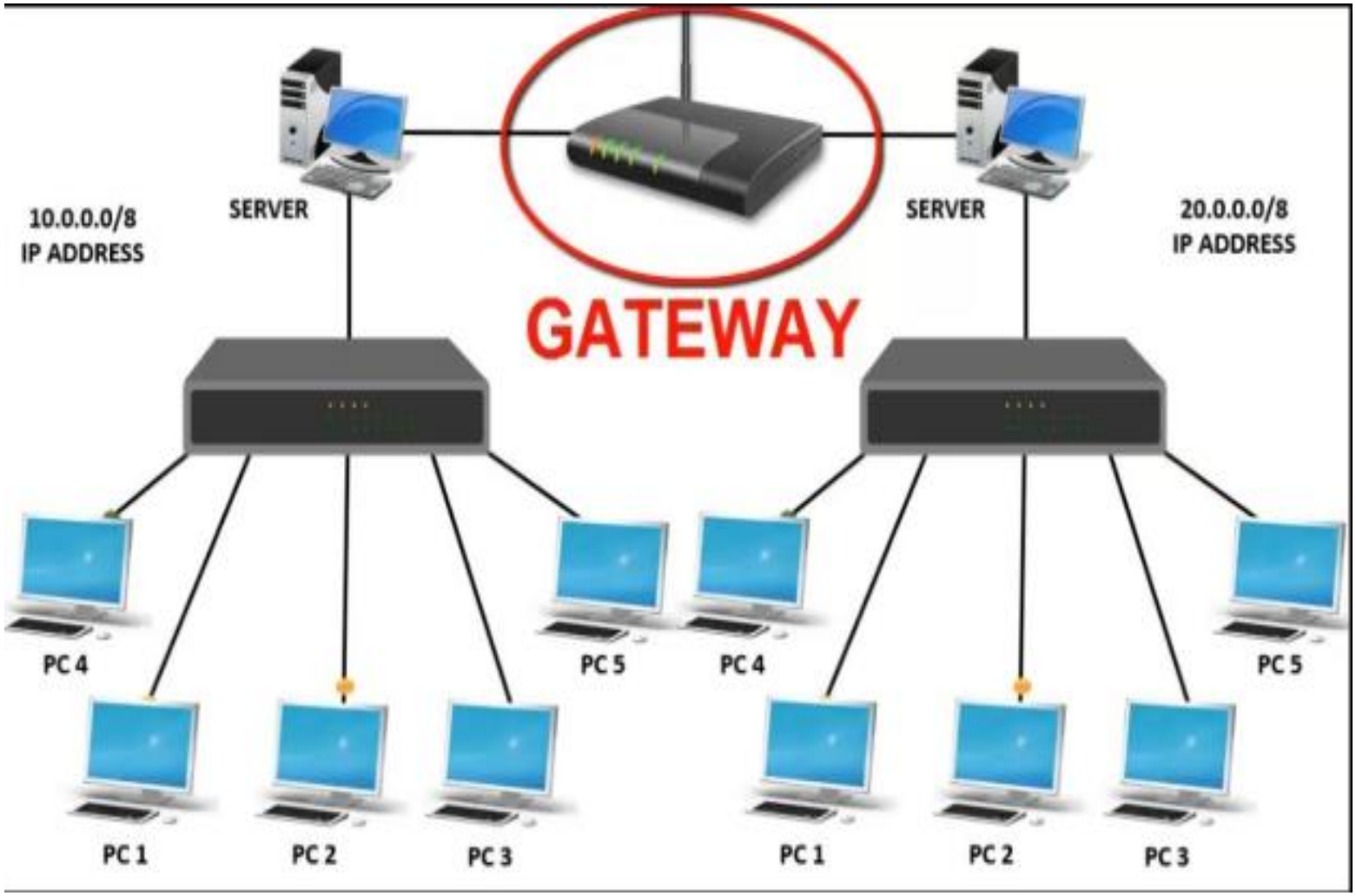
Network switches

Router

- A **router** is hardware device designed to receive, analyze and move incoming packets to another network. It may also be used to convert the packets to another network interface, drop them, and perform other actions relating to a network.
- It has the ability to connect dissimilar LANs on the same protocol.
- It also has the ability to limit the flow of broadcasts. A router primarily comprises of a hardware device or a system of the computer which has more than one network interface and routing software.
- A **router** has a lot more capabilities than other network devices, such as a hub or a switch that are only able to perform basic network functions. For example, a hub is often used to transfer data between computers or network devices, but does not analyze or do anything with the data it is transferring. By contrast, routers can analyze the data being sent over a network, change how it is packaged, and send it to another network or over a different network. For example, routers are commonly used in home networks to share a single Internet connection between multiple computers.

Gateway

- A gateway is a network node that connects two networks using different protocols together. While a bridge is used to join two similar types of networks, a gateway is used to join two dissimilar networks. A gateway is a hardware device that acts as a "gate" between two networks. It may be a router, firewall, server, or other device that enables traffic to flow in and out of the network.
- While a gateway protects the nodes within network, it also a node itself. The gateway node is considered to be on the "edge" of the network as all data must flow through it before coming in or going out of the network. It may also translate data received from outside networks into a format or protocol recognized by devices within the internal network.
- A router is a common type of gateway used in home networks. It allows computers within the local network to send and receive data over the Internet. A firewall is a more advanced type of gateway, which filters inbound and outbound traffic, disallowing incoming data from suspicious or unauthorized sources. A proxy server is another type of gateway that uses a combination of hardware and software to filter traffic between two networks. For example, a proxy server may only allow local computers to access a list of authorized websites.
- **NOTE:** Gateway is also the name of a computer hardware company founded in the United States in 1985. The company was acquired by Acer in 2007 but still sells computers under the Gateway name.

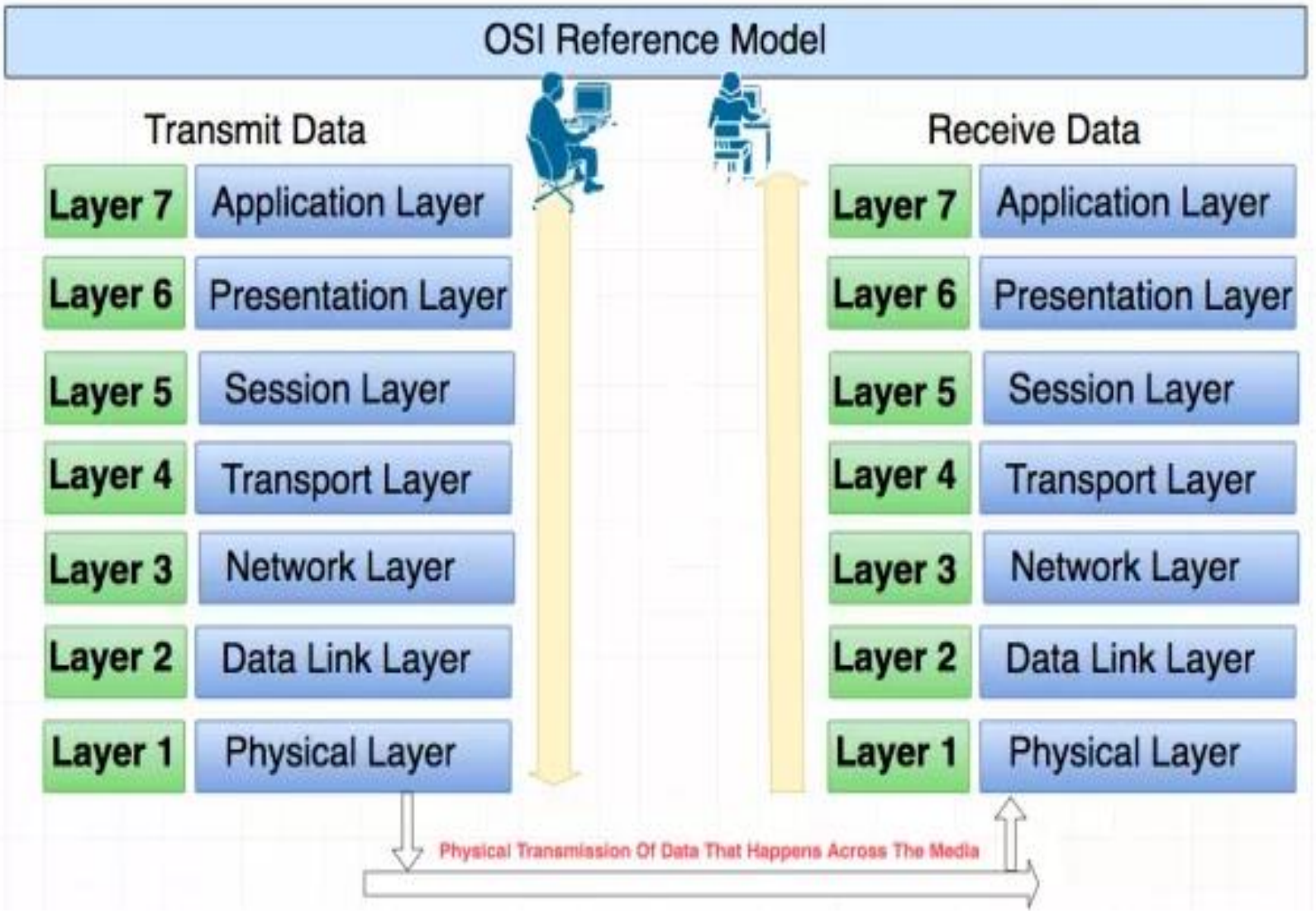

10.0.0.0/8
IP ADDRESS
SERVER
GATEWAY
SERVER
20.0.0.0/8
IP ADDRESS
PC 4
PC 5
PC 1
PC 2
PC 3
PC 4
PC 5
PC 1
PC 2
PC 3

Communication Protocol

- In telecommunication, a **communication protocol** is a system of rules that allow two or more entities of a communications system to transmit information via any kind of variation of a physical quantity. The protocol defines the rules, syntax, semantics and synchronization of communication and possible error recovery methods. Protocols may be implemented by hardware, software, or a combination of both.
- In computing, a **communication protocol** refers to the set of rules that computers use to communicate with each other. The protocol defines the signals that the computers will give each other, and other details such as how communication begins and/or ends.

OSI Reference Model

- OSI (Open Systems Interconnection) is a reference model for how applications communicate over a network.
- OSI or Open System Interconnection model was developed by International Standards Organization (ISO). It gives a layered networking framework that conceptualizes how communications should be done between heterogeneous systems. It has seven interconnected layers. The seven layers of the OSI Model are a physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer, as shown in the below diagram:
- The physical layer, data link layer and the network layer are the network support layers. The layers manage a physical transfer of data from one device to another. Session layer, presentation layer, and application layer are the user support layers. These layers allow communication among unrelated software in dissimilar environments. Transport layer links the two groups.

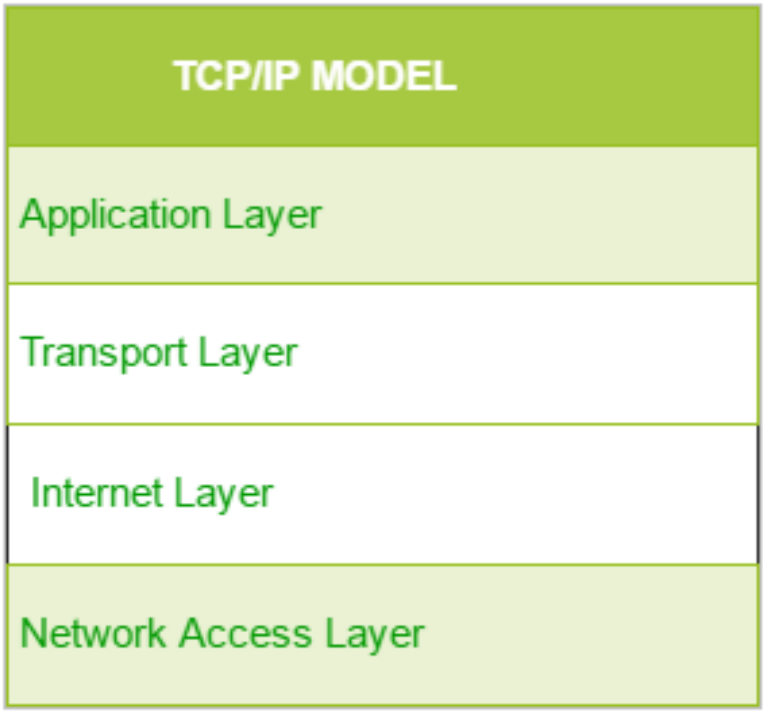

OSI Reference Model
Transmit Data
Receive Data
Layer 7
Application Layer
Layer 6
Presentation Layer
Layer 5
Session Layer
Layer 4
Transport Layer
Layer 3
Network Layer
Layer 2
Data Link Layer
Layer 1
Physical Layer
Layer 7
Application Layer
Layer 6
Presentation Layer
Layer 5
Session Layer
Layer 4
Transport Layer
Layer 3
Network Layer
Layer 2
Data Link Layer
Layer 1
Physical Layer
Physical Transmission Of Data That Happens Across The Media

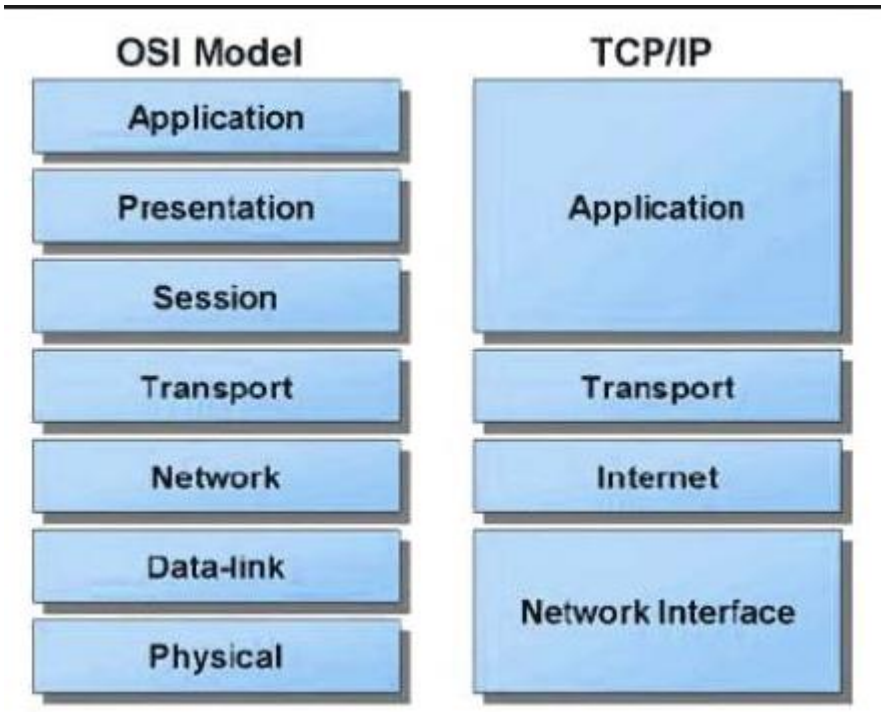
The main functions of each of the layers are as follows:

- **Physical Layer:** Its function is to transmit individual bits from one node to another over a physical medium.
- **Data Link Layer:** It is responsible for the reliable transfer of data frames from one node to another connected by the physical layer.
- **Network Layer:** It manages the delivery of individual data packets from source to destination through appropriate addressing and routing.
- **Transport Layer:** It is responsible for delivery of the entire message from the source host to destination host.
- **Session Layer:** It establishes sessions between users and offers services like dialog control and synchronization.
- **Presentation Layer:** It monitors syntax and semantics of transmitted information through translation, compression, and encryption.
- **Application Layer:** It provides high-level APIs (application program interface) to the users.

TCP/IP(Transmission Control Protocols/Internet Protocols)

- TCP/IP, or the Transmission Control Protocol/Internet Protocol, is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP can also be used as a communications protocol in a private network (an intranet or an extranet).
- TCP/IP specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into packets, addressed, transmitted, routed and received at the destination. TCP/IP requires little central management, and it is designed to make networks reliable, with the ability to recover automatically from the failure of any device on the network.
- The two main protocols in the internet protocol suite serve specific functions. TCP defines how applications can create channels of communication across a network. It also manages how a message is assembled into smaller packets before they are then transmitted over the internet and reassembled in the right order at the destination address.
- IP defines how to address and route each packet to make sure it reaches the right destination. Each gateway computer on the network checks this IP address to determine where to forward the message.





TCP/IP functionality is divided into four layers, each of which include specific protocols.

•*The application layer* provides applications with standardized data exchange. Its protocols include the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol 3 (POP3), Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP).

•***The transport layer*** is responsible for maintaining end-to-end communications across the network. TCP handles communications between hosts and provides flow control, multiplexing and reliability. The transport protocols include TCP and User Datagram Protocol (UDP), which is sometimes used instead of TCP for special purposes.

•***The network layer***, also called the internet layer, deals with packets and connects independent networks to transport the packets across network boundaries. The network layer protocols are the IP and the Internet Control Message Protocol (ICMP), which is used for error reporting.

•***The physical layer*** consists of protocols that operate only on a link -- the network component that interconnects nodes or hosts in the network. The protocols in this layer include Ethernet for local area networks (LANs) and the Address Resolution Protocol (ARP).

Merits of TCP/IP model

1.It operated independently.
2.It is scalable.
3.Client/server architecture.
4.Supports a number of routing protocols.
5.Can be used to establish a connection between two computers.

Demerits of TCP/IP

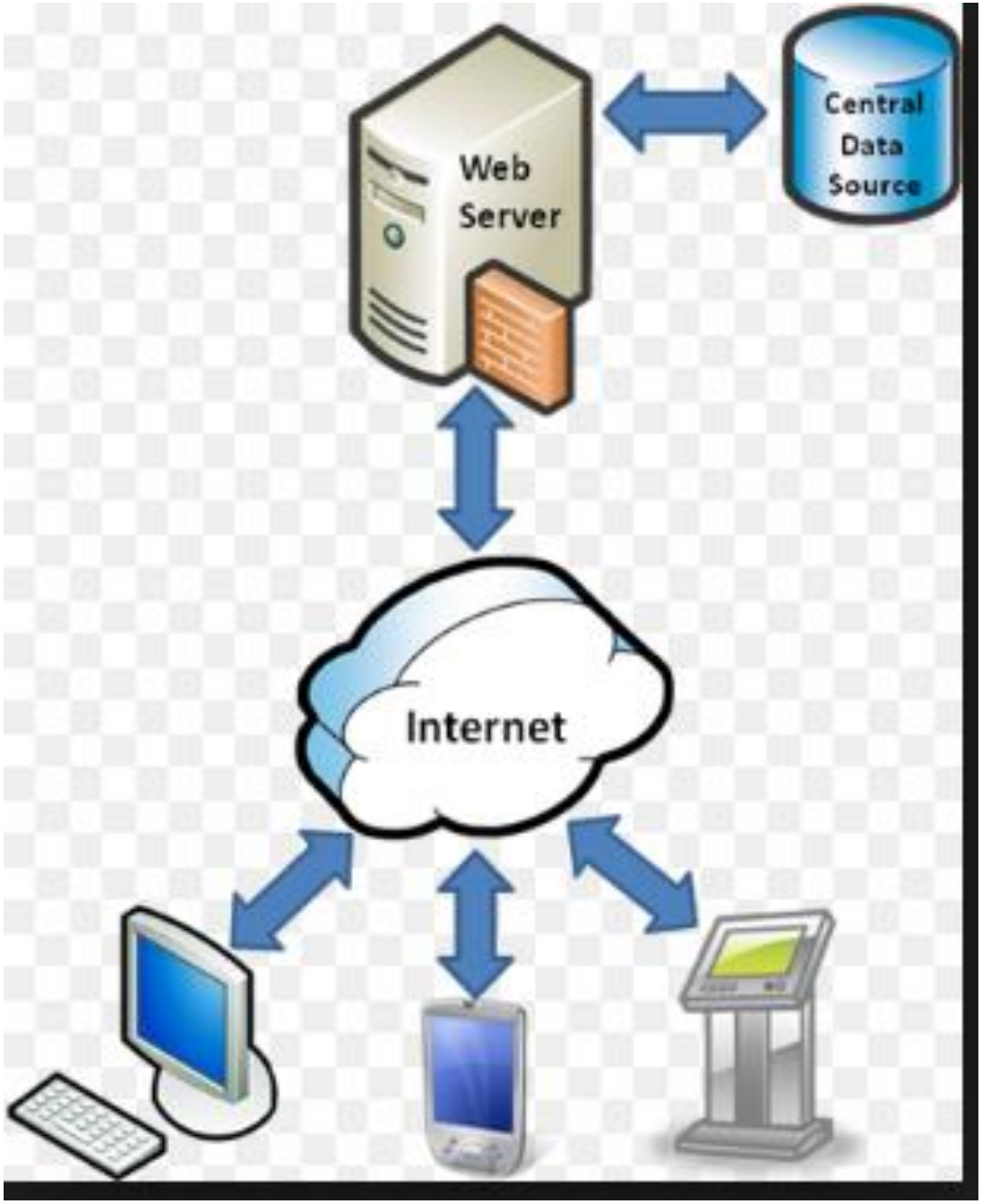
1.In this, the transport layer does not guarantee delivery of packets.
2.The model cannot be used in any other application.
3.Replacing protocol is not easy.
4.It has not clearly separated its services, interfaces and protocols.

TCP/IP	OSI
Implementation of OSI model	Reference model
Model around which Internet is developed	This is a theoretical model
Has only 4 layers	Has 7 layers
Considered more reliable	Considered a reference tool
Protocols are not strictly defined	Stricter boundaries for the protocols
Horizontal approach	Vertical approach
Combines the session and presentation layer in the application layer	Has separate session and presentation layer
Protocols were developed first and then the model was developed	Model was developed before the development of protocols
Supports only connectionless communication in the network layer	Supports connectionless and connection-oriented communication in the network layer
Protocol dependent standard	Protocol independent standard

Centralized Processing System

In this architecture all the data is collected to a single centralized storage area and processed upon completion by a single computer with often very large architectures in terms of memory, processor, and storage.

- Centralized computing is a type of computing architecture where all or most of the processing/computing is performed on a central server. Centralized computing enables the deployment of all of a central server's computing resources, administration and management.
- The central server, in turn, is responsible for delivering application logic, processing and providing computing resources (both basic and complex) to the attached client machines.
- Centralized processing architectures evolved with transaction processing and are well suited for small organizations with one location of service.
- Centralized processing requires minimal resources both from people and system perspectives.
- Centralized processing is very successful when the collection and consumption of data occurs at the same location.


Web
Server
Central
Data
Source
Internet

Centralized processing:

Centralized processing is the processing in which a centrally located computer system processes the data. A very powerful computer is needed for the centralized processing for gaining high speed and fast access. All the data get stored into the centralized data storage. The system administrator is responsible for protection level decisions and authorized access.

Advantages of the centralized processing:

1. Centralized processing helps in reducing the cost because it will not emphasize on more hardware and machines.

2. Centralized processing provides a better data security.

3. Processing is consistent in centralized processing systems.

4. The data and the program on each information system are independent to other information systems.

Disadvantages of centralized processing:

1. Large data storage is required at the central information system.

2. It will reduce the local accountability.

3. High traffic can cause input/output bottlenecks.

4. Ability to responds to the information request into a timely manner gets reduced.

5. Needs a high cost in transmitting transactions.

Distributed Processing System

- *Distributed processing*. In this architecture data and its processing are distributed across geographies or data centers, and processing of data is localized with the federation of the results into a centralized storage.
- Distributed architectures evolved to overcome the limitations of the centralized processing, where all the data needed to be collected to one central location and results were available in one central location. There are several architectures of distributed processing:

The key features of a distributed system are:

- Components in the system are concurrent. A distributed system allows resource sharing, including software by systems connected to the network at the same time.
- There can be multiple components, but they will generally be autonomous in nature.
- A global clock is not required in a distributed system. The systems can be spread across different geographies.
- Compared to other network models, there is greater fault tolerance in a distributed model.
- Price/performance ratio is much better.

Advantages:

–Scalability of systems and resources can be achieved based on isolated needs.

–Processing and management of information can be architected based on desired unit of operation.

–Parallel processing of data reducing time latencies.

Disadvantages:

–Data redundancy

–Process redundancy

–Resource overhead

–Volumes

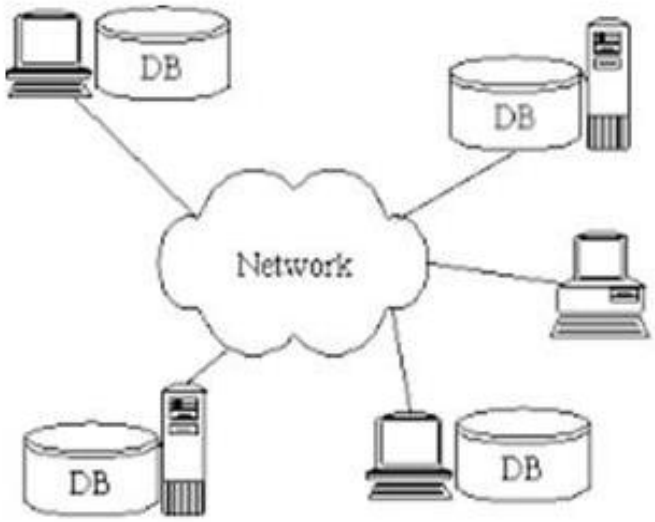


Figure. Distributed database System

The key goals of a distributed system include:

- Transparency: Achieving the image of a single system image without concealing the details of the location, access, migration, concurrency, failure, relocation, persistence and resources to the users
- Openness: Making the network easier to configure and modify
- Reliability: Compared to a single system, a distributed system should be highly capable of being secure, consistent and have a high capability of masking errors.
- Performance: Compared to other models, distributed models are expected to give a much-wanted boost to performance.
- Scalability: Distributed systems should be scalable with respect to geography, administration or size.

Challenges for distributed systems include:

- Security is a big challenge in a distributed environment, especially when using public networks.
- Fault tolerance could be tough when the distributed model is built based on unreliable components.
- Coordination and resource sharing can be difficult if proper protocols or policies are not in place.
- Process knowledge should be put in place for the administrators and users of the distributed model.

Centralized vs Distributed Systems

- **Centralized Systems**
  - Centralized systems have non-autonomous components
  - Centralized systems are often build using homogeneous technology
  - Multiple users share the resources of a centralized system at all times
  - Centralized systems have a single point of control and of failure
- **Distributed Systems**
  - Distributed systems have autonomous components
  - Distributed systems may be built using heterogeneous technology
  - Distributed system components may be used exclusively
  - Distributed systems are executed in concurrent processes
  - Distributed systems have multiple points of failure

Thank you