

Chapter 3: Communication and Networking

Computer Network

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.

Advantages of Computer Network

1. Sharing resources: 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. Faster and cheaper communication: communication in modern days has become very faster and cheaper to send information to a long distance through network.
3. 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.
4. Backup and recovery: server is used to keep data as backup. It maintains backup of all individual computers information.
5. 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.

Differences between analog and digital signal

Analog signal	Digital signal
Analog signal is a continuous signal which represents physical measurements.	Digital signals are discrete time signals generated by digital modulation.
Subjected to deterioration by noise during transmission and write/read cycle.	Can be noise-immune without deterioration during transmission and write/read cycle.

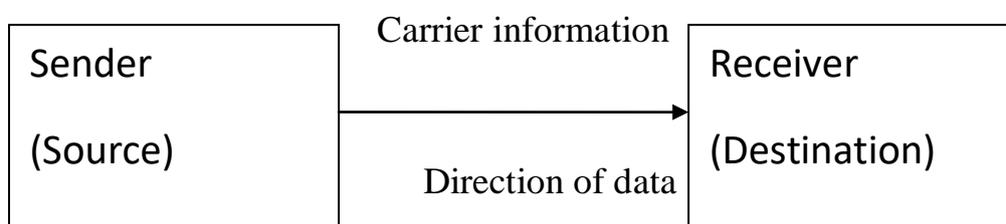
More likely to get affected reducing accuracy	Less affected since noise response are analog in nature
Stored in the form of wave signal	Stored in the form of binary bit
Low cost and portable	Cost is high and not easily portable
Example: Human voice in air, analog electronic devices.	Example: Computers, CDs, DVDs, and other digital electronic devices.

Data communication / Modes of data communication (transmission):

1. Simplex
2. Half-Duplex
3. Full-Duplex

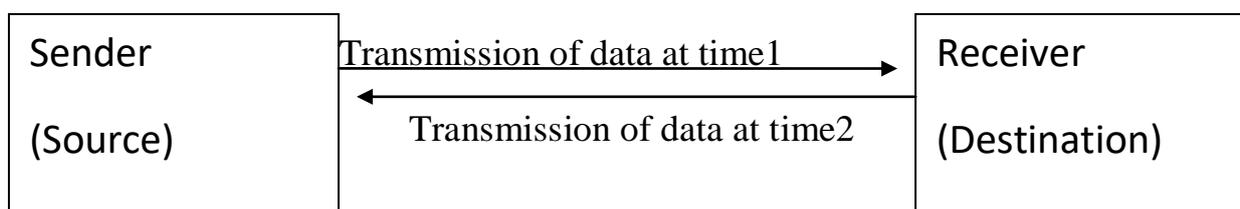
1) Simplex:

It means one way of communication system devices connection to such a circuit are either send only or receive only devices. For eg: sending a letter by mail, printer, fax, radio, newspaper, or books. Keyboard and traditional monitor are also the example of simplex devices. In simplex mode the communication is unidirectional.



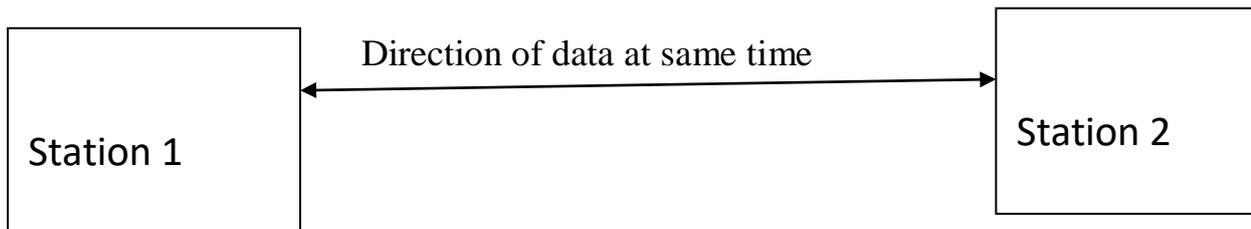
2) Half-Duplex:

It means transmission of data in both direction but only one at a time. A half-duplex line can alternate the send and receive data and requires two wires. In half –duplex when one device is sending the other can only receive and vice versa. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time for eg. Walkie-Talkie and citizen band radios (CB).



3) Full- Duplex:

In full duplex mode, both station can transmit and receive the data simultaneously. The full duplex mode is used when communication in both directions is required at a same time for eg. Telephone network. In telephone network when two people are communicating a telephone line both can talk and listen the same time. Audio chatting, video chatting are also full duplex mode.



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. Network architecture describes how network is organized and the computers on the network interact and communicate with each other. The major types of network architecture are:

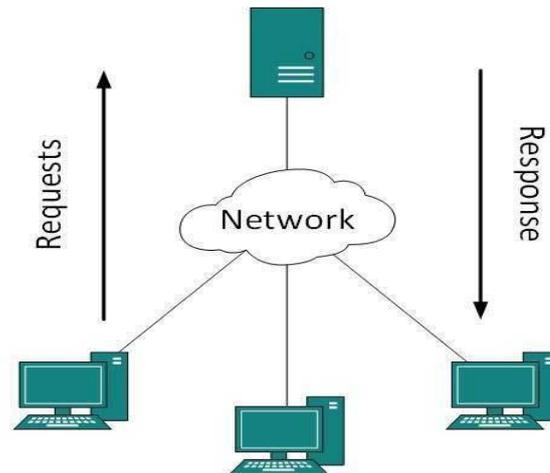
a) Client server network architecture

b) Peer to peer network architecture

a) Client server network architecture:

The client server network architecture consists at least one server and one or more client computer connected in the network. The server is a powerful computer with high processing, large memory and storage responsible for providing services to the workstation connected to the network. It provides easier network administration with secure and manageable access to the company data.

The client/server topology is the model for vertical scaling, where clients typically host a small subset of the data in the application process space and delegate to the server system for the rest. Compared to peer-to-peer by itself, the client/server architecture provides better data isolation, high fetch performance, and more scalability. If you expect data distribution to put a very heavy load on the network, client/server architecture usually gives better performance. In any client/server installation, the server system is itself a peer-to-peer system, with data distributed between servers. Client systems have a connection pool, which it uses to communicate with servers and other Gem Fire members. A client may also contain a local cache.



Advantages

- It covers larger geographical area.
- Its cabling structure may vary from simplex to complicated one.
- The network traffic is reduced in client server mode.
- The security management is centralized to the server.
- Backup of data is centralized.

Disadvantages:

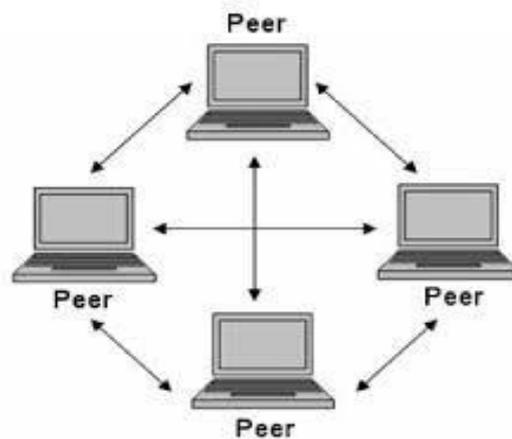
- Too many requests from the client may hang/breakdown the server.
- In this system if the server fails the whole network goes down.
- Initial setup of client server model is expensive.
- Professional technical IT person are needed to maintain the servers and other technical detail of networks.

b) Peer to peer network architecture:

The peer to peer network architecture consists of several computers connected together which functions both as server and client. In this architecture each computers has equal roles, responsibility, privileges and capabilities. Here the need of central server is removed and each computer interacts and share resources. This model is best fitted for small offices and home usages where data and other securities are not of big concern. This architecture is suitable for the networking environment where all nodes have the same capabilities and responsibilities.

The peer-to-peer distributed system is the building block for all Gem Fire installations. Peer-to-peer alone is the simplest topology. Each cache instance, or member, directly communicates with each every other member in the distributed system. This cache configuration is primarily designed for applications that want to embed a cache within the application process space

and participate in a cluster. A typical application example would be an application server cluster where the application and the cache are co-located and share the same heap.

**Advantages:**

- All resources are easily shared by all client computers.
- It is easy to install and configure.
- It's more reliable because central dependency is reduced.
- Failure of one client doesn't affect the network.
- Overall building and maintenance of this type of network is less than client server.
- No need of full time system administrator because each peer can control their resources.

Disadvantages:

- As whole system is decentralized, it is difficult to administrate.
- The network architecture is less secure.
- Data recovery and backup is very difficult since each client need its own backup.

Types of Computer Network:-

There are several types of computer networks. The classification of computer networks is done on the basis of the geographical location and the numbers of computer they have i.e. their size. The categories of computer network are:

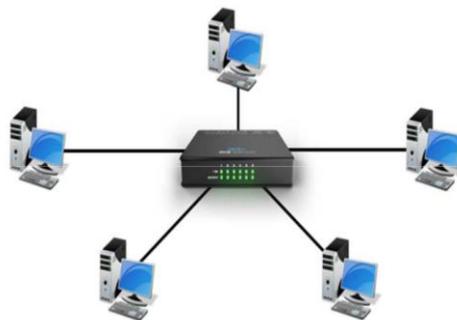
- a) **Local Area Network (LAN)**
- b) **Metropolitan Area Network(MAN)**
- c) **Wide Area Network (WAN)**

a) Local Area Network (LAN)

LAN is the computer network which relatively occupies small geographical area such as a single room or a building. The numbers of computers in LAN may vary from just two or three computers to hundreds of different kinds of computers. Computers in LAN are nearer to each other and are connected in a way that enables them to communicate by cables or wireless devices.

Along with the limited space or area, LANs are also typically owned, managed, controlled by the single organization or person. Networking done in computer lab is example of LAN.

A LAN is privately owned small size network. It spans only in small geographical area such as within a room, office, buildings or up to few kilometers (2 to 3 Km). it connects the network resources such as computers, faxes, printers and various networking devices.



Features of LAN

- It covers limited geographical area.
- It offers bandwidth of 10 to 100 Mbps (Megabits per second)
- It is owned and controlled by single organization.

Advantages of LAN

- It has higher bandwidth.

- Low cost
- Easy configuration
- Easy to manage

Disadvantages of LAN

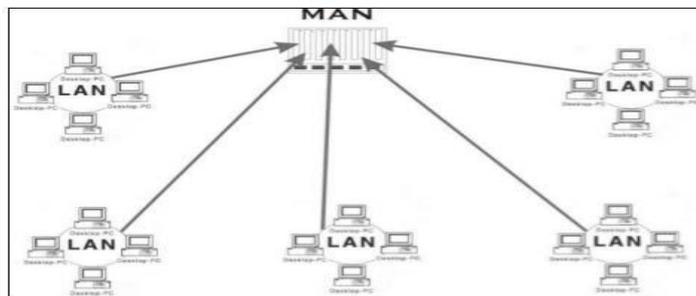
- It covers small geographical region.
- Limitation in exchanging information.
- Difficult to set up the network.

b) Metropolitan Area Network (MAN):

The computer network which is spread over the metropolitan area or city is called metropolitan area network. It is the medium sized network larger than LAN and smaller than WAN. Several LANs are connected together to form a MAN using different wires or wireless technologies. A MAN is typically owned and operated by a single entity such as a government body or large cooperation.

A MAN can be either public or privately owned network. Its size is bigger than LAN and smaller than WAN. It spans within one metropolitan city or larger geographical area. It can connect large number of computers and heterogeneous multiple LANs within a city maximum, up to 100Km.

METROPOLITAN AREA NETWORK (MAN)



Features of MAN

- It covers larger geographical area than LAN.
- The numbers of computers connected are also more than LAN.
- Multiple LANs are connected to form a MAN
- It is owned by single or multiple organizations.

Advantages of MAN

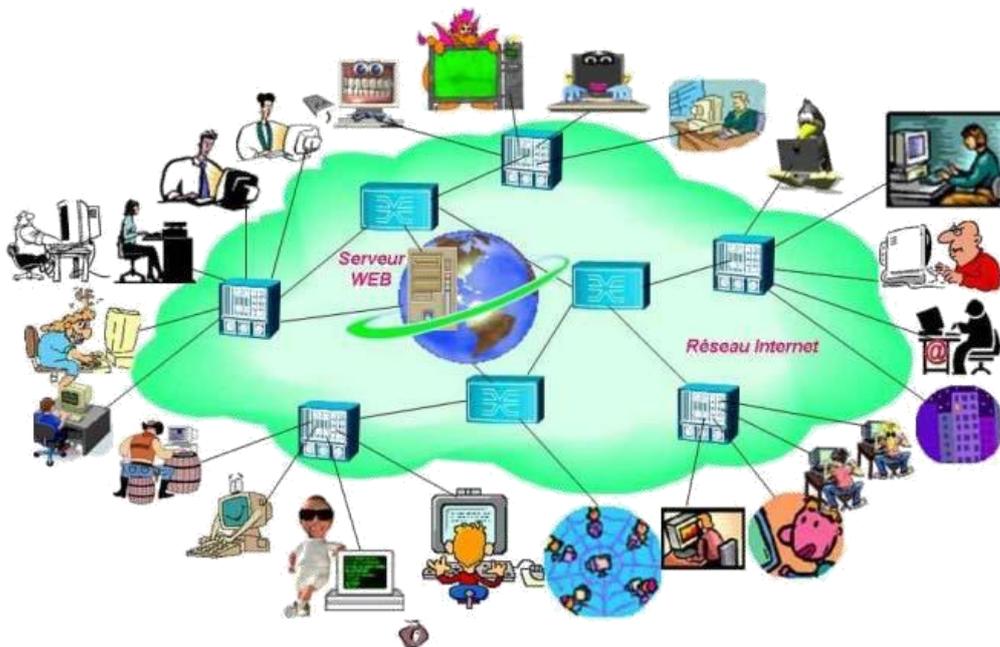
- It covers wider area than LAN.
- MAN requires fewer resources in comparison to WAN.
- Higher security.
- Increases the efficiency of handling data.

Disadvantages of MAN

- The large the network becomes difficult to manage.
- Difficult to make system secure from hackers.

c) **Wide Area Network (WAN):** The computer network which is spreads all over the world connecting hundreds thousands of computers. It is the largest network in the world where several LANs and MANs are connected through satellite links or microwave system. This network connects two or more computers generally across a wide geographical area such as cities, districts and countries. Internet is the example of WAN.

A WAN is basically public type heterogeneous network. It is the largest sized network and connects millions of computers, thousands of LANs, hundreds of MANs around the countries, continents and even the whole world.



Features of WAN:

- It is not restricted to a geographical locating; it is spreads all over the world.
- Satellites links and microwave system is used for connectivity.
- The technology is high speed and expensive.
- Data transmission is slower in comparison to LANs.

Advantages of WAN:

- It covers large geographical area.
- Ease update to the data and information.
- Scope of activities is not limited.

Disadvantages of WAN:

- The cost is higher.
- More associated errors occurs.
- Need to invest on good firewall system.
- High security challenges from hackers.

Difference between LAN and WAN

LAN	WAN
LAN (Local Area Network) is a computer network covering a small geographic area, like a home, office, school, or group of buildings.	WAN (Wide Area Network) is a computer network that covers a broad area (e.g., any network whose communications links cross metropolitan, regional, or national boundaries over a long distance).
High speed (1000 mbps)	Less speed (150 mbps)
Network in an organization can be a LAN	Internet is a good example of a WAN
If there is a need to set-up a couple of extra devices on the network, it is not very expensive to do that.	For WANs since networks in remote areas have to be connected the set-up costs are higher. However WANs using public networks can be setup very cheaply using just software (VPN etc).
LAN covers 100 m	WAN covers more than 100 m
Experiences fewer data transmission errors	Experiences more data transmission errors as compared to LAN

Typically owned, controlled, and managed by a single person or organization.	WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management over long distances.
--	---

Network topology and it's types: Short Description

Network topology refers to the physical layout of the network. It shows the geometrical representation of all links and linking devices, also called nodes. Its types are as:

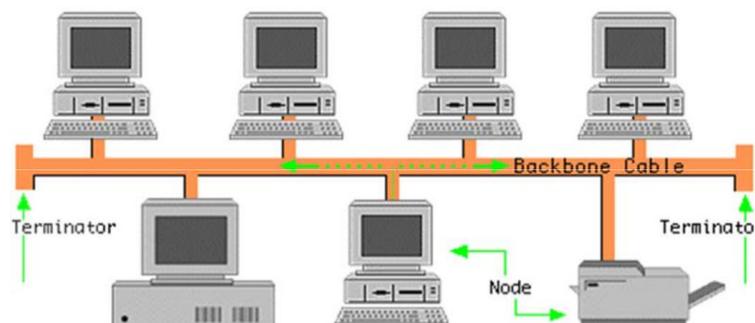
1. **Bus topology:** computers are connected to a single continuous cable that is called bus. A bus must be terminated on both sides to prevent signal bounce and computers are connected to the bus with the help of drop line and T-connector.
2. **Star topology:** Many home networks use the star topology. A star network features a central connection point called a "hub node" that may be a network hub, switch or router. Devices typically connect to the hub with Unshielded Twisted Pair (UTP) Ethernet.
3. **Ring topology:** In a ring network, every device has exactly two neighbors for communication purposes. All messages travel through a ring in the same direction (either "clockwise" or "counterclockwise"). A failure in any cable or device breaks the loop and can take down the entire network.
4. **Mesh topology:** Mesh topologies involve the concept of routes. Unlike each of the previous topologies, messages sent on a mesh network can take any of several possible paths from source to destination. (Recall that even in a ring, although two cable paths exist, messages can only travel in one direction.) Some WANs, most notably the Internet, employ mesh routing.
5. **Tree topology:** Tree topologies integrate multiple star topologies together onto a bus. In its simplest form, only hub devices connect directly to the tree bus, and each hub functions as the root of a tree of devices. This bus/star hybrid approach supports future expandability of the network much better than a bus (limited in the number of devices due to the broadcast traffic it generates) or a star (limited by the number of hub connection points) alone.
6. **Hybrid topology:** if two or more topologies are combined together then it is called hybrid topology. So it is very difficult to design and to implement the hybrid topology. It is expensive too.

Network Topology:-

Each device connected in the computer is called node. And the physical arrangement or the connection pattern of each device connected in the network is called network topology. It also refers to the cabling structure or geographical structure of the LAN. The basic network topologies are:

- a) **Bus or linear topology**
- b) **Star topology**
- c) **Ring topology**
- d) **Mesh Topology**
- e) **Tree Topology**
- f) **Hybrid Topology**

a) **Bus or linear topology:** It is the simplest of all network topology where all computers are arranged in linear format. In this topology all nodes of network are connected to the single cable by the help of connectors. The cable is backbone of the network and called bus. Data are transmitted on network through bus using the address of destination computers. The bus contains the terminator in each end and these terminator are responsible for stopping the flow of data out of the bus. This topology has maximum chance of data collision and if the backbone cable breaks then whole network gets jammed.



Features of Bus Topology:

- Data is transmitted in single direction.
- Every device is connected to a single cable.

Advantages of linear bus topology:

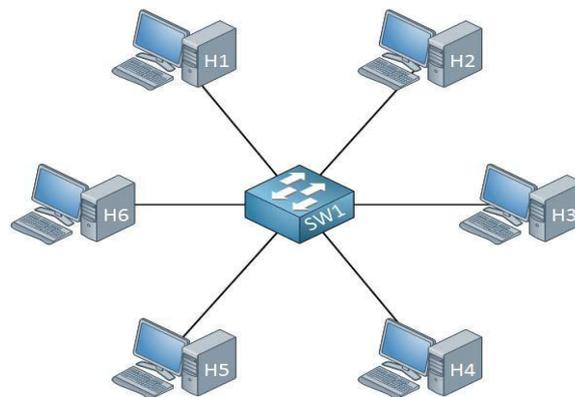
- It is easier to set up and extend.
- It requires fewer cables, so it is cheaper.
- New nodes can be easily added.

- It is mostly used in small networks

Disadvantages of linear bus technology

- Whole network stops functioning if backbone cable is damaged.
- Network slows down if additional computers or nodes are added.
- There is maximum chance of data collision.
- Cable has limited length.
- It is difficult to detect and troubleshoot the errors.

b) Star Topology: This is the most commonly used and popular network topology. In star topology all nodes or computers are connected through a central device called hub or switch. This is the most popular topology to connect nodes in the LAN. All devices are connected indirectly with each other with the help of hub or switch. If a device needs to communicate with another it needs to pass form the switch or hub before reaching to destination. Hub acts as a junction to connect different nodes, manages and controls entire network. Unshielded Twisted Pair (UTP), Ethernet cable is used to connect nodes to hub in star topology. If the central server or hub fails the whole network stops functioning but failures of single computer don't affect the whole network.



Features of Star Topology:

- Every node has its own connection to the hub.
- Hub acts as a repeater for data flow.
- Can be used with twisted pair, coaxial or fiber optical cable.

Advantages of star topology:

- It is easy to setup and configure.
- It provides better performance than bus topology.
- Easy to add and remove new nodes.
- Centralized management helps in monitoring the network.

- Failure of a single node doesn't affect functioning of the network.
- It is easy to detect the errors in this topology.

Disadvantages of star topology:

- It requires more cables in comparison to bus so, it is costlier.
- Failure of central switch/hub breaks down the whole network.
- Capacity of central device determines the numbers of nodes and performance of star topology.

c) Ring Topology: In ring topology all nodes are connected to each other in the shape of circle without the end point forming a closed circular loop. In this topology one computer is connected to other and so on to form a ring pattern. Each computer has two neighbors either side of it. There is no central controller in this type of topology and data are from one computer to another in circle passing through each computer on the network until destination computer is met.

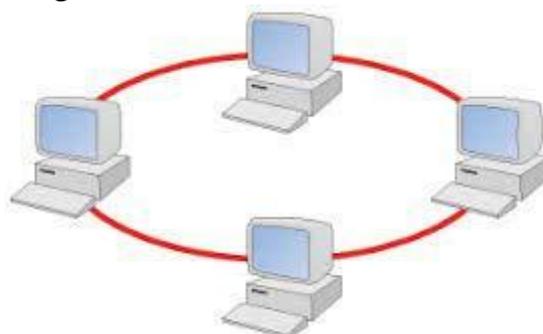
The TOKEN passing method is used to pass data from one computer to another in ring topology. Source computer generates the token containing data and destination address. Then the token is passed to the next node, which checks if the data is for it or not. If yes, it receives the data otherwise it passes the token to next node, the process continues until the destination computer is met.

Advantages of ring topology:

- Ring topology is easy to set up and configure.
- Each computer get equal opportunity to access the network resources.
- This topology helps to reduce chances of data collision.

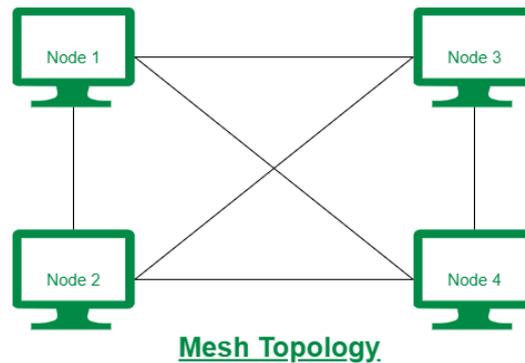
Disadvantages of ring topology:

- Data packet needs to pass through all nodes between source and destination.
- If one node or port goes down, the entire network gets affected.
- It is difficult to detect errors in this type of network.
- Adding or removing the devices affects the entire network.



d) Mesh Topology

In mesh topology each device is connected to every other device on the network through a dedicated point-to-point link. When we say dedicated it means that the link only carries data for the two connected devices only. Let's say we have n devices in the network then each device must be connected with $(n-1)$ devices of the network. Number of links in a mesh topology of n devices would be $n(n-1)/2$.



Advantages of Mesh topology

1. No data traffic issues as there is a dedicated link between two devices which means the link is only available for those two devices.
2. Mesh topology is reliable and robust as failure of one link doesn't affect other links and the communication between other devices on the network.
3. Mesh topology is secure because there is a point to point link thus unauthorized access is not possible.
4. Fault detection is easy.

Disadvantages of Mesh topology

1. Amount of wires required to connected each system is tedious and headache.
2. Since each device needs to be connected with other devices, number of I/O ports required must be huge.
3. Scalability issues because a device cannot be connected with large number of devices with a dedicated point to point link.

e) Tree or Expanded Star

A tree topology combines characteristics of linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable (See fig. 3). Tree topologies allow for the expansion of an existing network, and enable schools to configure a network to meet their needs.

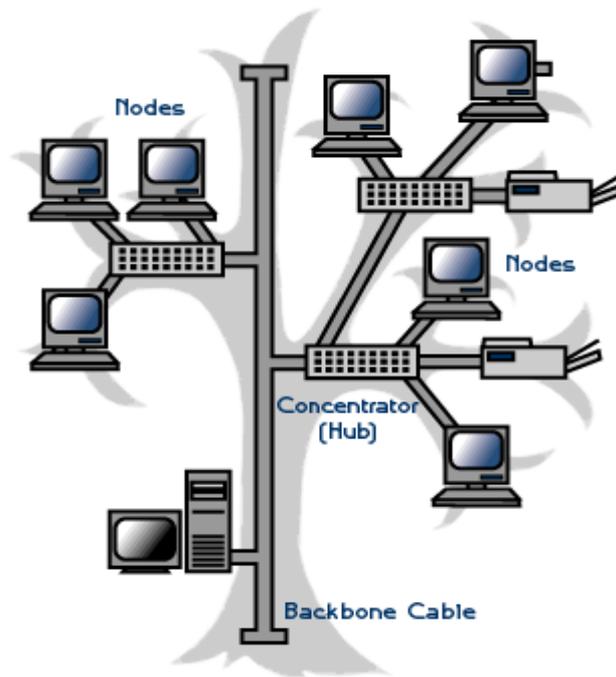


Fig. Tree topology

Advantages of a Tree Topology

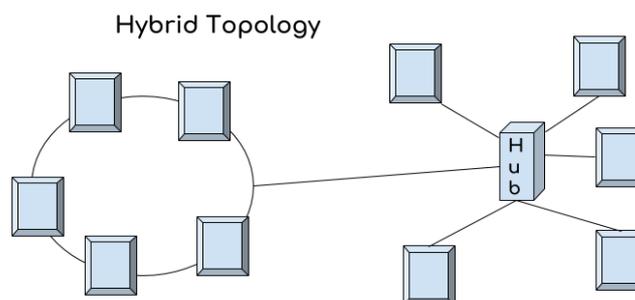
- Point-to-point wiring for individual segments.
- Supported by several hardware and software vendors.

Disadvantages of a Tree Topology

- Overall length of each segment is limited by the type of cabling used.
- If the backbone line breaks, the entire segment goes down.
- More difficult to configure and wire than other topologies.

f) Hybrid Topology

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



Advantages of Hybrid topology

1. We can choose the topology based on the requirement for example, scalability is our concern then we can use star topology instead of bus technology.
2. Scalable as we can further connect other computer networks with the existing networks with different topologies.

Disadvantages of Hybrid topology

1. Fault detection is difficult.
2. Installation is difficult.
3. Design is complex so maintenance is high thus expensive.

Difference between Internet and Intranet

Internet	Intranet
The Internet is a worldwide, publicly accessible series of interconnected computer networks transmit data by packet switching using the standard Internet Protocol	An intranet is a private computer network that uses Internet protocols, network connectivity to securely share part of an organization's information or operations
This is the base, independent of the World Wide Web	Independent of the internet; however, internet is also used parallel
The Internet allows computer users to connect to other computers & information stores easily across the world; it is also used in marketing, online chat, file transfer, etc.	Intranets are being used to deliver tools & applications, helps to improve the services provided to the users, increases employees' ability to perform their jobs faster, etc.
Internet is a public computer network	Intranet is a private computer network

Signal modulation

In electronics and telecommunications, modulation is the process of varying one or more properties of a periodic waveform, called the carrier signal (high frequency signal), with a modulating signal that typically contains information to be transmitted.

Three forms of modulations are possible. They are as:

1. **Amplitude Modulation (AM):** Amplitude modulation is an increase or decrease of the carrier voltage (E_c), with all other factors remaining constant.
2. **Frequency Modulation (FM):** Frequency modulation is a change in the carrier frequency (f_c) with all other factors remaining constant.
3. **Phase Modulation (PM):** Phase modulation is a change in the carrier phase angle (\hat{I}_s). The phase angle cannot change without also affecting a change in frequency. Therefore, phase modulation is in reality a second form of frequency modulation.

Components of Computer Network

Hardware: Mechanical parts used in the computer network refer to the hardware components which are listed below:

Computer: A well-functioning set of computer is a main element of the network. There may be just two or hundreds of computer connected in a single network.

Hub: The networking device used to connect the multiple computers in LAN. It broadcasts the information to all the ports and sends to all connected computers because it can't identify the destination computers.

Switch: An intelligent device that joins multiple computers together in the local area network (LAN) is switch. Unlike hub they identify the destination computer and forward the information to destination computer only.

Network Interface Card (NIC): It is the Ethernet card or Network adapter that enables a computer to connect to a network.



Repeater: The signals transmitted become weak when they need to travel longer distance. Repeater is a device that increases the length of network by amplifying the weak signals. It receives the weak signals, regenerates them and send them to the destination. So, it enables signals transfer the longer distance.



Bridge: The networking device used to connect two similar types of network is known as Bridge. It is used to connect two LANs or different segments of the same network.

Router: It is the device connecting two different networks having similar protocols. Along with this it is used to determine the best path for sending the data packets from source to destination. That means, routers are responsible for traffic management in computer network.



Gateway: Gateway are hardware or software responsible for connecting two different networks having dissimilar protocols. They make communication possible between different architecture and environment. They repackage and convert data going from one environment to another so that each environment can understand the other environment's data.

Difference between Hub and Switch.

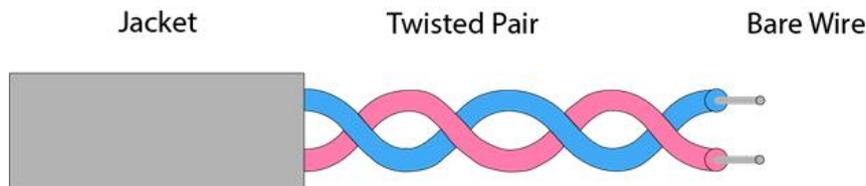
S N	HUB	SN	Switch
1	An electronic device that connects many network devices together so that devices can exchange data.	1	A switch is considered more advanced than a hub because a switch will only send message to device that needs or request it.
2	Hubs are classified in physical layer of OSI model.	2	Switch is classified in Data-link layer of OSI model.
3	Hubs are cheaper than switch.	3	Switch is expensive than hubs.
4	In hub data transmission is in the form of bits.	4	In switch data transmission is in the form of frames and packets.
5	Transmission rate of hubs are slower than switch.	5	Transmission rate of switch are slower than hub.

Difference between Routers and Repeaters.

SN	Routers	SN	Repeater
1	It is an internetworking device that forward packets between networks.	1	It is a device used to boost the signals uses its strength, while passing through a cable.
2	It normally connects LANs and WANs ,in the internet.	2	It connects two segment of same LAN.

Difference between Routers and Switch.

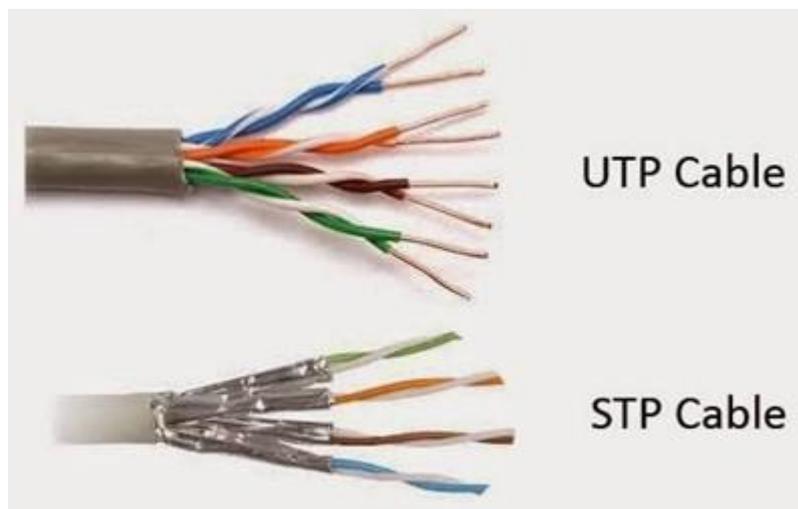
SN	Routers	SN	Switch
1	It is a WAN device .	1	It is a LAN device.
2	It connects two or more networks.	2	It connects two or more nodes in the same network.
3	It is Internetworking device.	3	It is networking device.
4	Routers is 3 layer devices for OSI model.	4	switch is 2 layer devices for OSI model.
5	It uses IP address.	5	It uses MAC address.
6	It is comparatively fast.	6	It is comparatively slow.



UTP Categories - Copper Cable				
UTP Category	Data Rate	Max. Length	Cable Type	Application
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Rink & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)



Types of Twisted pair:



i) Shielded Twisted Pair

A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

Characteristics of Shielded Twisted Pair:

- The cost of the shielded twisted pair cable is not very high and not very low.

- An installation of STP is easy.
- It has higher capacity as compared to unshielded twisted pair cable.
- It has a higher attenuation.
- It is shielded that provides the higher data transmission rate.

Disadvantages

- It is more expensive as compared to UTP and coaxial cable.
- It has a higher attenuation rate.

ii) Unshielded Twisted Pair

An unshielded twisted pair is widely used in telecommunication. Following are the categories of the unshielded twisted pair cable:

- **Category 1:** Category 1 is used for telephone lines that have low-speed data.
- **Category 2:** It can support up to 4Mbps.
- **Category 3:** It can support up to 10Mbps.
- **Category 4:** It can support up to 16Mbps. Therefore, it can be used for long-distance communication.
- **Category 5:** It can support up to 100Mbps.
- **Category 6:** It can support up to 10Gbps.

Advantages of Unshielded Twisted Pair:

- It is cheap.
- Installation of the unshielded twisted pair is easy.
- It can be used for high-speed LAN.

Disadvantage:

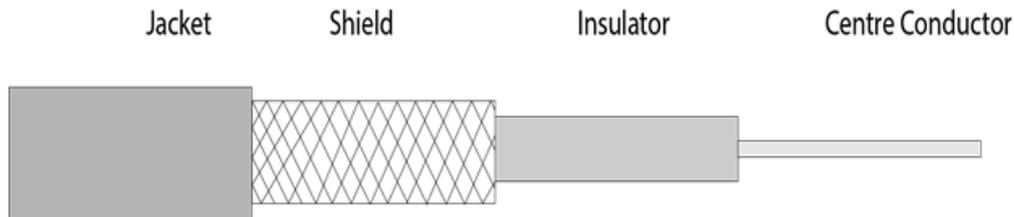
- This cable can only be used for shorter distances because of attenuation.

b. Coaxial Cable

- Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.
- The name of the cable is coaxial as it contains two conductors parallel to each other.
- It has a higher frequency as compared to Twisted pair cable.
- The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh. The middle core is made up

of non-conductive cover that separates the inner conductor from the outer conductor.

- The middle core is responsible for the data transferring whereas the copper mesh prevents from the EMI(Electromagnetic interference).



Coaxial cable is of two types:

- i. Baseband transmission:** It is defined as the process of transmitting a single signal at high speed.
- ii. Broadband transmission:** It is defined as the process of transmitting multiple signals simultaneously.

Advantages Of Coaxial cable:

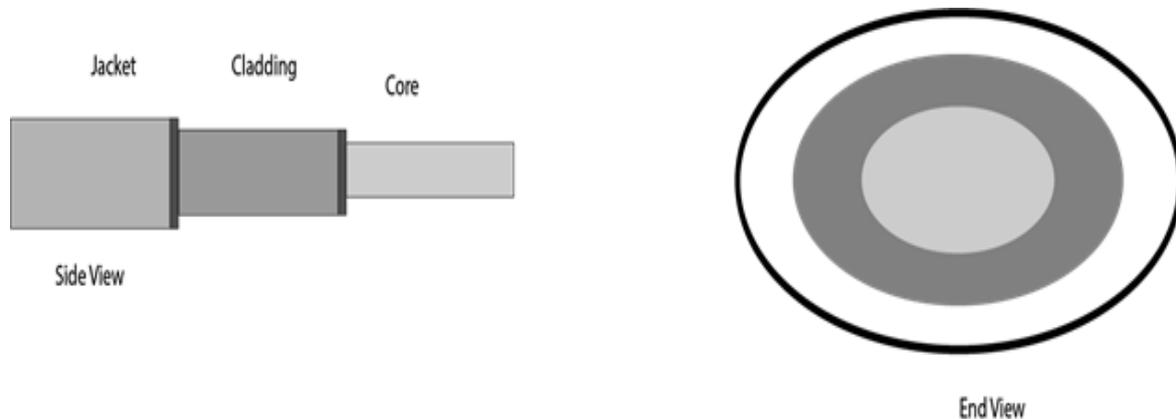
- The data can be transmitted at high speed.
- It has better shielding as compared to twisted pair cable.
- It provides higher bandwidth.

Disadvantages Of Coaxial cable:

- It is more expensive as compared to twisted pair cable.
- If any fault occurs in the cable causes the failure in the entire network.

c. Fibre Optical Cable

- Fibre optic cable is a cable that uses electrical signals for communication.
- Fibre optic is a cable that holds the optical fibres coated in plastic that are used to send the data by pulses of light.
- The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring.
- Fibre optics provide faster data transmission than copper wires.

Diagrammatic representation of fibre optic cable:**Basic elements of Fibre optic cable:**

- **Core:** The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of the core, the more light will be transmitted into the fibre.
- **Cladding:** The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.
- **Jacket:** The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

Following are the advantages of fibre optic cable over copper:

- **Greater Bandwidth:** The fibre optic cable provides more bandwidth as compared copper. Therefore, the fibre optic carries more data as compared to copper cable.
- **Faster speed:** Fibre optic cable carries the data in the form of light. This allows the fibre optic cable to carry the signals at a higher speed.
- **Longer distances:** The fibre optic cable carries the data at a longer distance as compared to copper cable.

- **Better reliability:** The fibre optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable.
- **Thinner and Sturdier:** Fibre optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

2. Wireless or Unguided Media or Unbound Transmission Media:

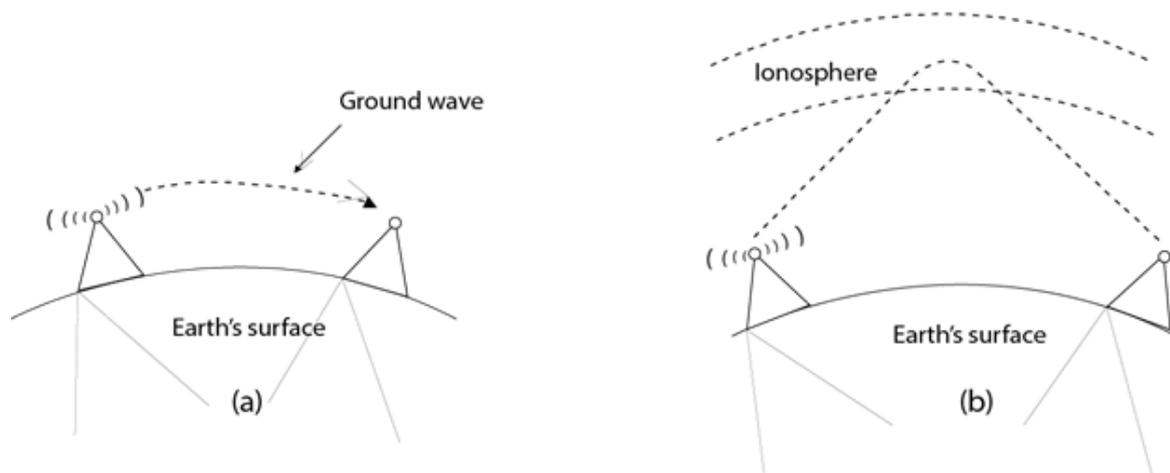
Unbound transmission media are the ways of transmitting data without using any cables. These media are not bounded by physical geography. This type of transmission is called Wireless communication. Nowadays wireless communication is becoming popular. Wireless LANs are being installed in office and college campuses. This transmission uses Microwave, Radio wave, Infra red are some of popular unbound transmission media.

- An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**.
- In unguided media, air is the media through which the electromagnetic energy can flow easily.

Unguided transmission is broadly classified into three categories:

a) Radio waves

- Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- Radio waves are omni-directional, i.e., the signals are propagated in all the directions.
- The range in frequencies of radio waves is from 3Khz to 1 khz.
- In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.
- An example of the radio wave is **FM radio**.



Applications of Radio waves:

- A Radio wave is useful for multicasting when there is one sender and many receivers.
- An FM radio, television, cordless phones are examples of a radio wave.

Advantages of Radio transmission:

- Radio transmission is mainly used for wide area networks and mobile cellular phones.
- Radio waves cover a large area, and they can penetrate the walls.
- Radio transmission provides a higher transmission rate.

b) Microwaves

Microwaves are of two types:

- Terrestrial microwave
- Satellite microwave communication.

i) Terrestrial Microwave Transmission

- Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.
- Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.
- Microwaves are unidirectional as the sending and receiving antenna is to be aligned, i.e., the waves sent by the sending antenna are narrowly focussed.

- In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.
- It works on the line of sight transmission, i.e., the antennas mounted on the towers are the direct sight of each other.

Characteristics of Microwave:

- Frequency range: The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
- Bandwidth: It supports the bandwidth from 1 to 10 Mbps.
- Short distance: It is inexpensive for short distance.
- Long distance: It is expensive as it requires a higher tower for a longer distance.
- Attenuation: Attenuation means loss of signal. It is affected by environmental conditions and antenna size.

Advantages Of Microwave:

- Microwave transmission is cheaper than using cables.
- It is free from land acquisition as it does not require any land for the installation of cables.
- Microwave transmission provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task.
- Communication over oceans can be achieved by using microwave transmission.

Disadvantages of Microwave transmission:

- Eavesdropping: An eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.
- Out of phase signal: A signal can be moved out of phase by using microwave transmission.
- Susceptible to weather condition: A microwave transmission is susceptible to weather condition. This means that any environmental change such as rain, wind can distort the signal.
- Bandwidth limited: Allocation of bandwidth is limited in the case of microwave transmission.

ii) Satellite Microwave Communication

- A satellite is a physical object that revolves around the earth at a known height.

- Satellite communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems.
- We can communicate with any point on the globe by using satellite communication.

How Does Satellite work?

The satellite accepts the signal that is transmitted from the earth station, and it amplifies the signal. The amplified signal is retransmitted to another earth station.

Advantages Of Satellite Microwave Communication:

- The coverage area of a satellite microwave is more than the terrestrial microwave.
- The transmission cost of the satellite is independent of the distance from the centre of the coverage area.
- Satellite communication is used in mobile and wireless communication applications.
- It is easy to install.
- It is used in a wide variety of applications such as weather forecasting, radio/TV signal broadcasting, mobile communication, etc.

Disadvantages Of Satellite Microwave Communication:

- Satellite designing and development requires more time and higher cost.
- The Satellite needs to be monitored and controlled on regular periods so that it remains in orbit.
- The life of the satellite is about 12-15 years. Due to this reason, another launch of the satellite has to be planned before it becomes non-functional.

c) Infrared

- An infrared transmission is a wireless technology used for communication over short ranges.
- The frequency of the infrared is in the range from 300 GHz to 400 THz.
- It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Characteristics of Infrared:

- It supports high bandwidth, and hence the data rate will be very high.

- Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
- An infrared communication provides better security with minimum interference.
- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

d) Wi-Fi:

Wi-Fi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. A common misconception is that the term Wi-Fi is short for "wireless fidelity," however this is not the case. Wi-Fi is simply a trademarked phrase that means IEEE 802.11x.

e) Bluetooth: -

It is a name of a wireless technology standard for connecting devices set to replace cables. It uses radio frequency in the 2.45 GHz ranges to transmit information over a short distance (10 meter or less). Bluetooth technology enable short range wireless connection between desktop and notebook computers, mobile phone, camera, printers, headsets, mouse, keyboard etc. A radio frequency technology enables to software in Bluetooth technology enables to transmit data from one to another devices. Bluetooth is a short-range wireless communication technology standard.

Switching system

It provides a path between the two devices in a network. The process of transferring data blocks from one node to another node is called data switching.

Types of switching system are as follows:

1. **Circuit switching:** It is the most familiar technique used to build a communication network. Used in ordinary telephone lines and it allows communications equipment and circuits to be shared among users. Each user has the sole access to a circuit during network use.

2. **Message switching:** Message switching is a network switching technique in which data is routed in its entirety from the source node to the destination node, one hop at a time. During message routing, every intermediate switch in the network stores the whole message. If the entire network's resources are engaged or the network becomes blocked, the message-switched network stores and delays the message until ample resources become available for effective transmission of the message.
3. **Packet switching:** A network technology that breaks up a message into small packets for transmission, unlike circuit switching, which requires the establishment of a dedicated point to point connections each packet in a packet switched network contains a destination address. Thus all packets in a single message do not have to follow the same path. Packet can arrive out of order. Destination computer reassembles the packets into their proper sequence.

OSI reference model

The Open Systems Interconnection (OSI) Model is a conceptual and logical layout that defines network communication used by systems open to interconnection and communication with other systems.

The model is broken into seven subcomponents, or layers, each of which represents a conceptual collection of services provided to the layers above and below it. The OSI Model defines a logical network and effectively describes computer packet transfer by using different layer protocols also referred to as the seven-layer OSI Model or the seven-layer model.

The OSI Model was developed by the International Organization for Standardization (ISO) in 1978. While working on a network framework, ISO decided to develop the seven-layer model.

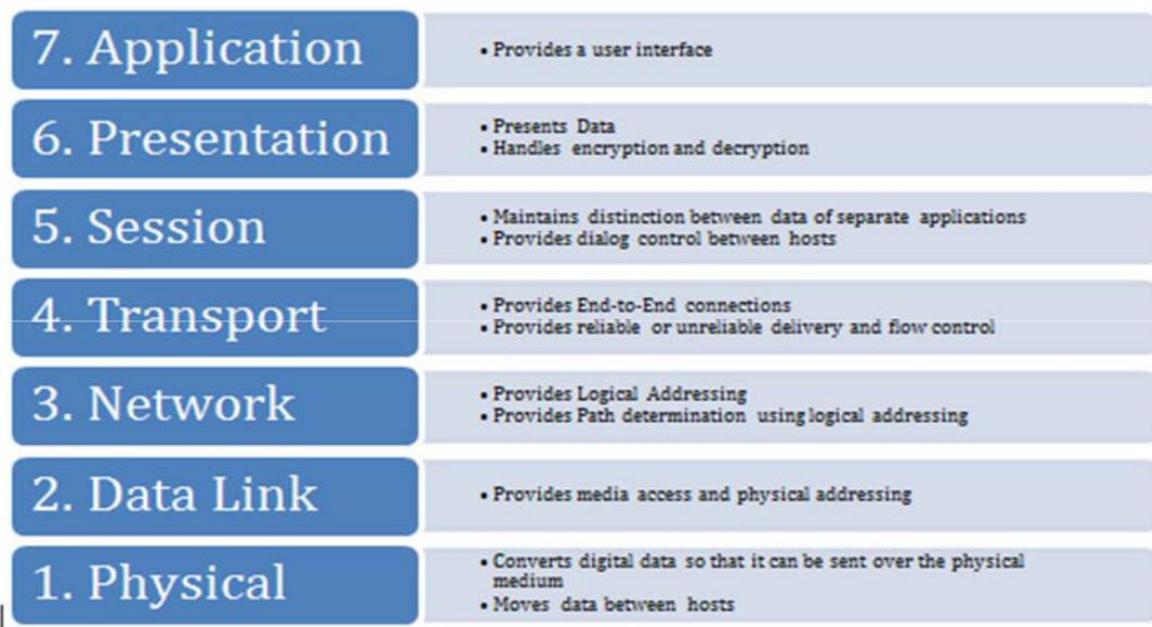
The OSI Model works in a hierarchy, assigning tasks to all seven layers. Each layer is responsible for performing assigned tasks and transferring completed tasks to the next layer for further processing. Today, many protocols are developed based on the OSI Model working mechanism.

Following are the same included in OSI reference model:

1. Physical layer
2. Data link layer
3. Network layer
4. Transport layer
5. Session layer

6. Presentation layer

7. Application layer



1. **Physical Layer:** This layer concerned with transmission of bit it determines voltage level for 0 & 1. It also determines the data rate of the system. This layer involves standardized protocol dealing with electrical & signaling interface.

2. **Data Link Layer:** It handles error in physical layer. This layer ensures the correct delivery of frame to the destination address. It consists of 2 parts or 2 sub-layers. i.e.

- i. Logic Link Control
- ii. Media Access Control

3. **Network Layer:** This layer is concerned with transmission of packet. N/w layer protocol chooses the best path to send a package called routing. Two protocols are widely used in n/w layer.

- i. X.25 Protocol
- ii. Internet Protocol

4. **Transport Layer:** It provides the mechanism for the exchange of data between end systems. It ensures that the data received is in fact in order. Following jobs are performed by this layer.

- i. Port Addressing
- ii. Segmentation & Reassemble
- iii. Connection Control

5. Session Layer: It is responsible for requesting logical connection to be established for communication process. This logical connection is termed as session. It also provides data synchronization between two communication terminals.

6. Presentation layer: This layer translates format data to adapt to the needs of the application layer & nodes at both receiving & sending end of communication process. It handles data communication, formatting, encryption, decryption, etc.

7. Application Layer: It is the top-most layer of OSI model & provides user access to the n/w. It provides services that support user application, such as database access, email & file transfer, etc.

IP Address:

This is a code made up of numbers separated by three dots that identifies a particular computer on the Internet. Every computer, whether it is a Web server or the computer you're using right now, requires an IP address to connect to the Internet. IP addresses consist of four sets of numbers from 0 to 255, separated by three dots.

For example "66.72.98.236" or "216.239.115.148". Your Internet Service Provider (ISP), will assign you either a static IP address (which is always the same) or a dynamic IP address, (which changes every time you log on).

MAC address: Stands for "Media Access Control Address," and no, it is not related Apple Macintosh computers. A MAC address is a hardware identification number that uniquely identifies each device on a network. The MAC address is manufactured into every network card, such as an Ethernet card or Wi-Fi card, and therefore cannot be changed.

Protocol: A standard set of regulations and requirements that allow two electronic items to connect to and exchange information with one another. Protocols regulate data transmission among devices as well as within a network of linked devices through both error control and specifying which data compression method to use. In particular, protocols decide: the method of error checking, how to compact data (if required), how the transmitting device signals that it has concluded sending data, and how the receiving device signals that it has completed receiving data.

The [TCP/IP](#) Internet protocols, a common example, consist of:

- Transmission Control Protocol (TCP), which uses a set of rules to exchange messages with other Internet points at the information packet level

- [Internet Protocol](#) (IP), which uses a set of rules to send and receive messages at the Internet address level
- Additional protocols that include the Hypertext Transfer Protocol (HTTP) and [File Transfer Protocol](#) (FTP), each with defined sets of rules to use with corresponding programs elsewhere on the Internet

There are many other Internet protocols, such as the Border Gateway Protocol ([BGP](#)) and the Dynamic Host Configuration Protocol ([DHCP](#)).