COMPUTER NETWORKS

(MODULE 1)

PART 1: INTRODUCTION CONCEPTS

COMPUTER NETWORK: DEFINITION

A computer network is a set of computers connected together for the purpose of sharing resources. The most common resource shared today is connection to the Internet. Other shared resources can include a printer or a file server.

GOALS OF COMPUTER NETWORKS:

The following are some important goals of computer networks:

1. **Resource Sharing** –

Many organizations have a substantial number of computers in operations, which are located apart.
Example- A group of office workers can share a common printer, fax, modem, scanner, etc.

2. **High Reliability** –

If there are alternate sources of supply, all files could be replicated on two or more machines. If one of them is not available, due to hardware failure, the other copies could be used.

3. **Inter-process Communication** –

Network users, located geographically apart, may converse in an interactive session through the network. In order to permit this, the network must provide almost error-free communications.

4. **Flexible access** –

Files can be accessed from any computer in the network. The project can be begun on one computer and finished on another.
Other goals include Distribution of processing functions, Centralized management, and allocation of network resources, Compatibility of dissimilar equipment and software, Good network performance, Scalability, Saving money, Access to remote information, Person to person communication, etc.

GOALS:

- Several machines can share printers, tape drives, etc.
- Reduced cost
- Resource and loadsharing
- Programs do not need to run on a single machine
- High reliability
- If a machine goes down, another can take over
- Mail andcommunication

APPLICATIONS OF COMPUTER NETWORKS:

- Shared resource
- Communication
- Remote access
- Storage capacity
- Business Applications
- Data security and management
- Data sharing
- Entertainment
- Software sharing
- Directory services
- Educational applications
- Financial services
- Flexibility
- Media center server
- Network management
- Social media
- Software Management

COMPONENTS OF COMPUTER NETWORKS:

1. Server: A server is a computer that serves the data to other computers and users. The network components can be in the form of a computer, a hardware device, or a computer program that is loaded so that it can send data and any information to other computers.

The term "server" usually refers to a computer system that receives a request for a web document and sends the request information to the client.

2. Client: The device that receives requests, and responses from the server, is called a client. When the server and its clients work together on the computer, we call it the client/server network.

3. Transmission media: Transmission media are the medium through which data is transferred from one device to another in a network. Transmission media can be used either in a physical transmission medium or wireless transmission medium.

Physical transmission medium includes the use of wires and cables like fiber optic cables, coaxial cable, etc.; and wireless transmission medium includes the use of unguided media like infra-red waves, electromagnetic, microwaves, etc.

4. NIC (Network Interface cards): Network Interface cards (NICs) are also called Network Interface Controller, Network adapter, LAN adapter, and Physical Network interface. NIC cards are hardware components used to connect computers with networks. Without NIC a

computer cannot be connected to the network

It is installed in a computer circuit board that provides a network connection to the computer. Due to the popularity and low cost of Ethernet standards, the network interface is built directly into the motherboard in almost all new computers.

5. **Hub:**
    - Hubs are those devices that are used to link several computers together. Hubs repeat one signal that comes in on one port and then copies it to other ports.
    - A network hub is basically a centralized distribution point for all the data transmission in a network.
    - Hub is a passive device.
    - The hub receives the data and then rebroadcasts the data to other computers that are connected to it. Hub mainly does not know the destination of a received data packet. Thus it is required to send copies of data packets to all the hub connections.
    - Also, Hubs consumes more bandwidth on the network and thus limits the amount of communication.
    - One disadvantage of using hubs is that they do not have the intelligence to find out the best path for the data packets which then leads to inefficiencies and wastage.

Types of Hub:

- **Active Hub:** Active Hubs make use of electronics in order to amplify and clean up the signals before they are broadcast to other ports. Active Hubs are mainly used to extend the maximum distance between nodes. It works both as a wiring center as well as a repeater.

- **Passive Hub:** Passive Hubs are those hubs that connect only to Active Hubs. Passive Hubs are simply used to connect all ports together electrically and these are usually not powered. These hubs are cheaper than Passive hub. Passive hubs neither amplify the signal nor regenerate the signal.

- **Intelligent Hub:** Intelligent hubs give better performance than active and passive hubs. Nowadays Intelligent hubs are widely used and are in more demand than active and passive hubs. These hubs are mainly used to connect various devices. It supports amplification and regeneration of signals at any point of incoming signals. Intelligent hub sustains the network along with the selection path. The tasks of both passive and active are manageable by the intelligent hub. With the help of an intelligent hub, the Speed and efficiency of the whole network increases which helps to gain the fast and efficient performance of the network.

6. **Switch:**

- Switch mainly resembles a Hub. It is a layer-2 device and it is used for the intelligent forwarding of messages. By intelligent we mean the decision-making ability of the switch. As hub works in the way by sending data to all ports on the device, whereas the switch sends the data to only that port that is connected with the destination device.
- The switch is a network component and is mainly used to connect the segments of the network.

- The switch is more intelligent than the network hub.
- Mainly Switches are capable of inspecting the data packets as soon as they are received, then determine the source and destination of that packet, and then forward it appropriately.
- Switch differs from the hub as it also contains ports of different speeds.
- Before forwarding the data to the ports switch performs the error checking and this feature makes the switch efficient.
- As the switch delivers the message to the connected device it was intended for, thus it conserves the bandwidth of the network and offers better performance than the hub.
- The most important feature of the switch is that it supports unicast (one to one), multicast (one to many), and broadcast (one to all) communications.
- The switch makes use of MAC address in order to send data packets to the selected destination ports.

7. Repeater:

- The repeater is a Physical layer device. As the name suggests, the repeater is mainly used to regenerate the signal over the same network and it mainly regenerates before the signal gets corrupted or weak.
- They are incorporated into the networks in order to extend the coverage area. Repeaters can connect signals by making the use of diffrent types of cables.
- Repeaters are cost-effective.
- Repeaters are very easy o install, and after their installation, they can easily extend the coverage area of the network.
- But there is a problem with repeaters and it is they cannot those networks that are not of the same type.
- Repeaters do not help to reduce the traffic in the network.

8. Router:

- The router is a network component that is mainly used to send or receive data on the computer network. The process of forwarding data packets from the source to the destination is referred to as Routing.
- The router is a Network Layer (i.e. Layer 3) device.
- The main responsibilities of the router are receiving data packets, analyzing them, and then forwarding the data packets among the connected computer networks.
- Whenever any data packet arrives, then first of all the router inspects the destination address and then consults with its routing tables in order to decide the optimal route and then transfers the packet along this route towards the destination.
- Routers are mainly used to provide protection against broadcast storms.
- Routers are expensive than a hub, switches, repeaters, and bridges.
- Routers can also connect different networks together and thus data packets can also be sent from one network to another network.
- Routers are used in both LAN as well as in WAN (wide area network).
- Routers share data with each other in order to prepare and refresh the routing tables.

9. Modem:

- The modem is basically a hardware component that mainly allows a computer or any other device like a router, switch to connect to the Internet.
- A modem is basically a shorthand form of Modulator-Demodulator.
- One of the most important functions of the modem is to convert analog signals into

digital signals and vice versa. Also, this device is a combination of two devices: modulator and demodulator. The modulator mainly converts the analog data into digital data at the time when the data is being received by the computer.

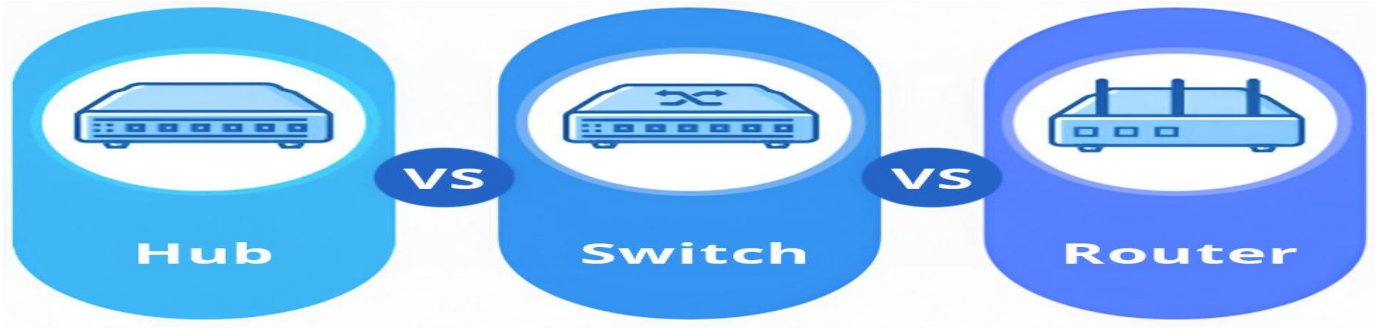
- The demodulator basically converts the digital data signals into analog data at the time when it is being sent by the computer.

10. Bridges:

- This bridge is a device that has such functionality that it filters the content, for which it reads MAC addresses of both source and destination. The bridge connects two LANs (Local Area Network) using the same protocol. This device operates in the data link layer of the OSI Model.
- These network components are very useful for filtering the data load of traffic, for which they divide them into segments or packets. The bridge controls the data traffic of LANs or other networks. These bridges are actually passive devices, as there is no interaction between bridged and paths of bridging.

11. Gateway:

- This gateway is a hardware device that acts as a "gate" within two networks. It can also be a router, firewall, server, or any other device that enables traffic to flow in and out of the network. Gateways are used to connect networks based on different protocols. As a bridge is used to join two similar types of networks, similarly, the gateway is used to join two dissimilar networks.
- This gateway node is located at the edge of the network and all the data flows through it which enters or exits the network. In addition, it can also translate received data that is received from outside networks, into a format or protocol that can be identified by devices within the internal network.

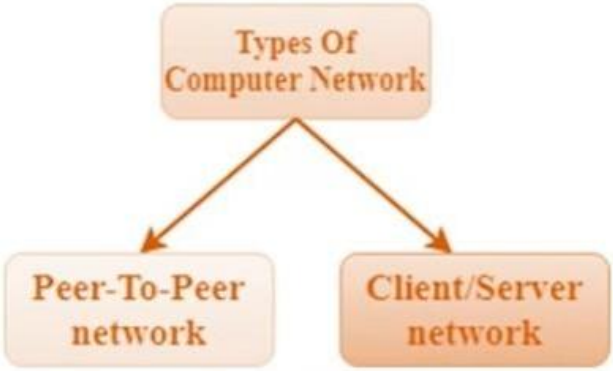


Hub	Switch	Router
Broadcast device	Multicast device	Routing device
Connects devices in the same network	Connects devices in the same network	Connects devices from different networks
Only one device can send data at a time	Multiple devices can send data at the same time	Multiple devices can send data at the same time
Does not store any device information	Stores and uses MAC addresses to transfer data	Uses IP addresses to transfer data

COMPUTER NETWORKS STRUCTURE AND ARCHITECTURE:

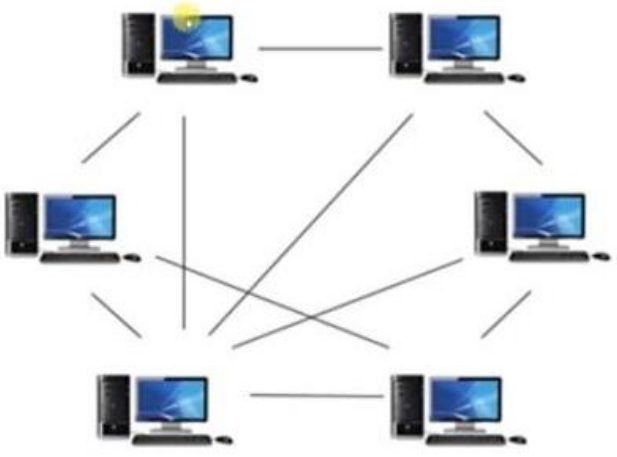
The two types of network architectures are used

- Peer-To-Peer network or client-to-client network
- Client/Server network



Peer-To-Peer network

- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.



Advantages Of Peer-To-Peer Network

- It is less costly as it does not contain any dedicated server.
- If one computer stops working but, other computers will not stop working.
- It is easy to set up and maintain as each computer manages itself.

Disadvantages Of Peer-To-Peer Network

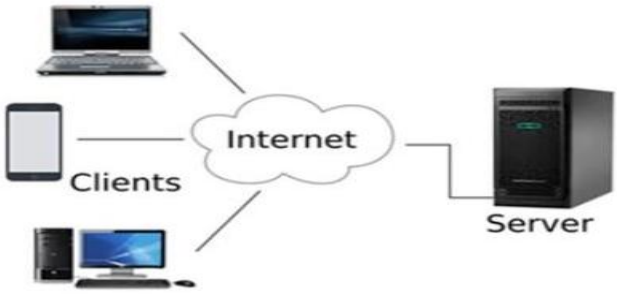
- In the case of Peer-To-Peer network, it does not contain the centralized system . Therefore, it cannot back up the data as the data is different in different locations.
- It has a security issue as the device is managed itself.

Client/Server Network

- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- The central controller is known as a server while all other computers in the network are called clients.
- A server performs all the major operations such as security and network management.

Client/Server Network

- A server is responsible for managing all the resources such as files, directories, printer, etc.
- All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.



Advantages Of Client/Server network

- A Client/Server network contains the centralized system. Therefore we can back up the data easily.
- A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- Security is better in Client/Server network as a single server administers the shared resources.
- It also increases the speed of the sharing resources.

Disadvantages Of Client/Server network

- Client/Server network is expensive as it requires the server with large memory.
- A server has a Network Operating System(NOS) to provide the resources to the clients, but the cost of NOS is very high.
- It requires a dedicated network administrator to manage all the resources.

CLASSIFICATION AND TYPES: PAN, LAN, MAN, WAN:

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

There are other types of Computer Networks also, like:

1) **PAN** stands for personal area network. It is a new type of network that connects computers/devices within the range of an individual person. A perfect example of a PAN is a cell phone connecting to a Bluetooth headset or mobile computer connecting to a portable Bluetooth thermal printer.
    - **Range:** 10 meters (30 feet)
    - **Use:** Around person, home

2) **LAN** stands for local area network. It is a group of network devices that allow communication between various connected devices. Private ownership has control over the local area network rather than the public. LAN has a short propagation delay than MAN as well as WAN. It covers smaller areas such as colleges, schools, hospitals, and so on. Example: Wi-Fi, Ethernet.
    - **Range:** 100m to 1000m (1km)
    - **Use:** Buildings, schools, colleges etc.

3) **MAN** stands for metropolitan area network. It covers a larger area than LAN such as small towns, cities, etc. MAN connects two or more computers that reside within the same or completely different cities. MAN is expensive and should or might not be owned by one organization.
    - **Range:** 5km to 50km
    - **Use:** city

4) **WAN** stands for wide area network. It covers a large area than LAN as well as a MAN such as country/continent etc. WAN is expensive and should or might not be owned by one organization. PSTN or satellite medium is used for wide area networks.
    - **Range:** 100km to 10,000km
    - **Use:** country, continent

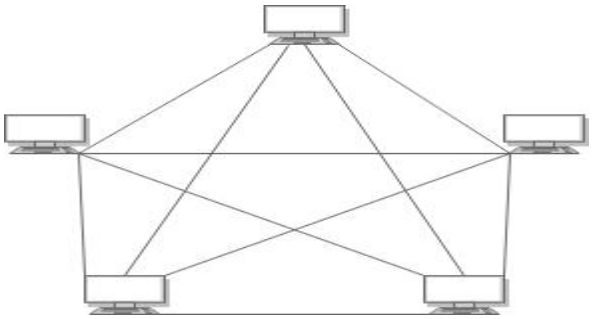
TOPOLOGY:

The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as network topology. The various network topologies are:

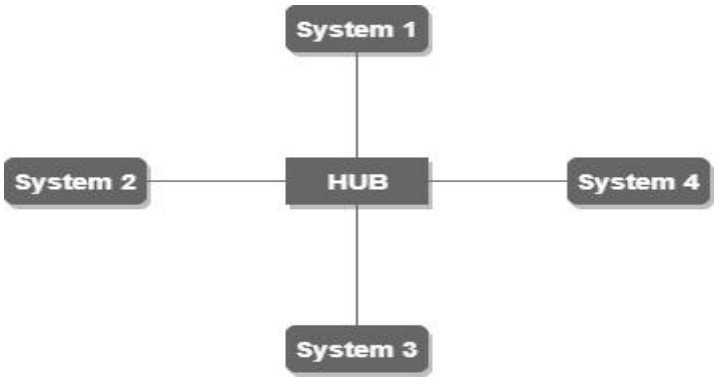
a) Point-to-Point
b) Mesh Topology
c) Star Topology
d) Bus Topology
e) Ring Topology
f) Tree Topology
g) Hybrid Topology

Point-to-Point: Point to Point topology is the simplest topology that connects two nodes directly together with a common link.

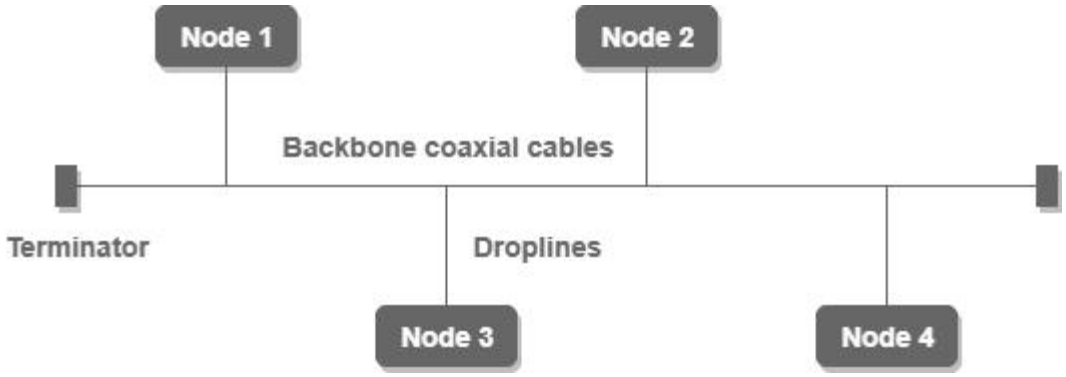
Mesh Topology: In a mesh topology, every device is connected to another device via a particular channel.



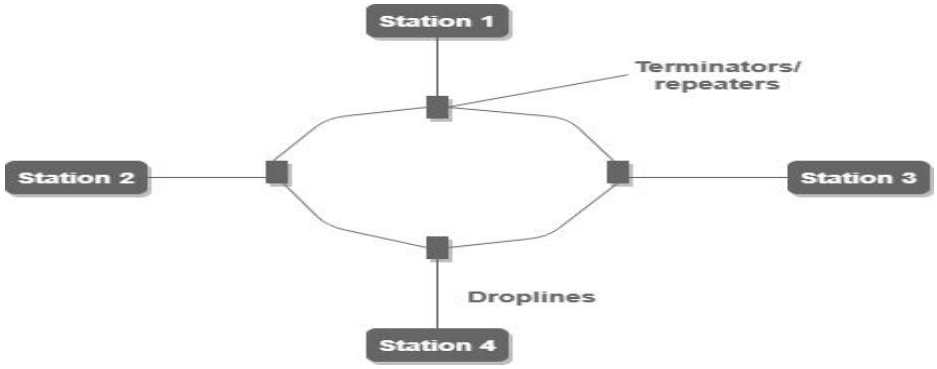
Star Topology: In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them.



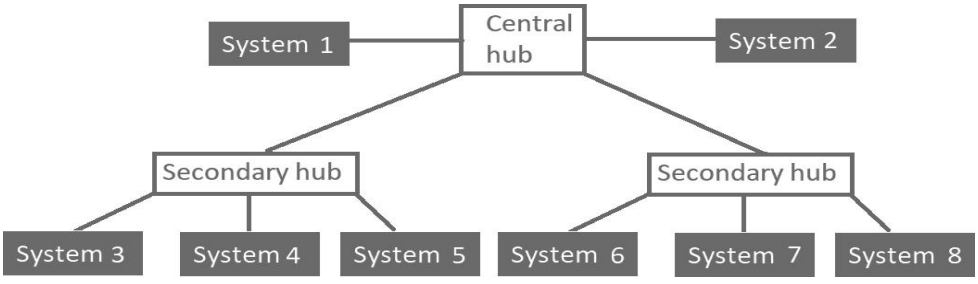
Bus Topology: Bus topology is a network type in which every computer and network device is connected to a single cable. It transmits the data from one end to another in a single direction. No bi-directional feature is in bus topology. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.



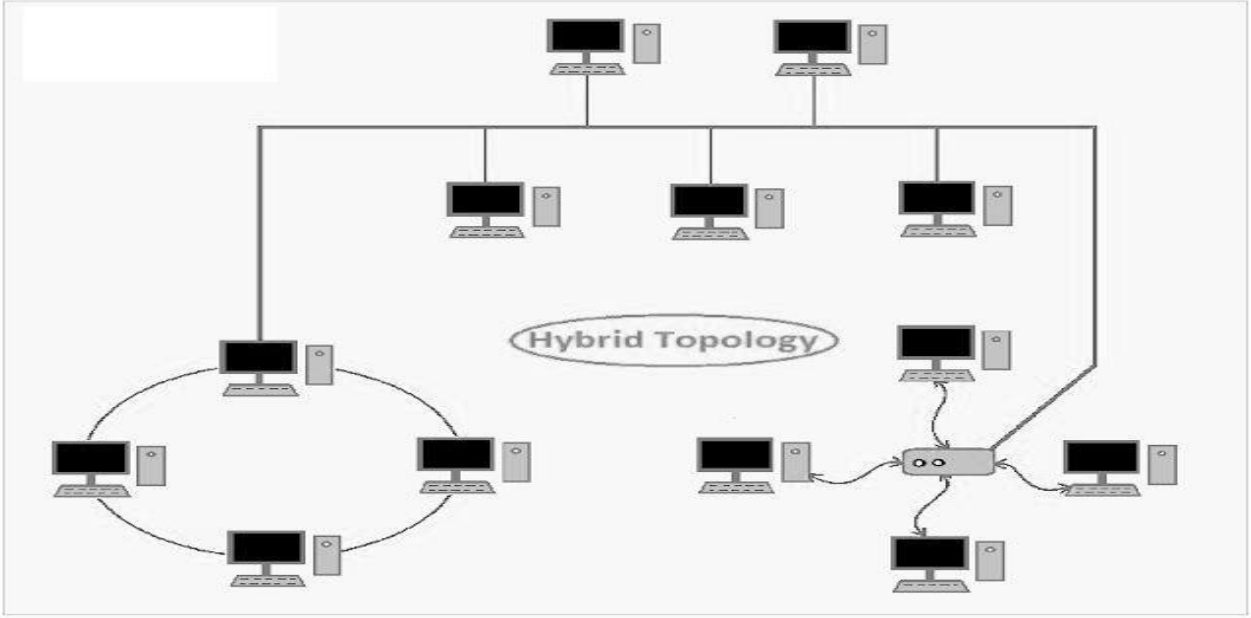
Ring Topology: In this topology, it forms a ring connecting devices with its exactly two neighboring devices. A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.



Tree Topology: This topology is the variation of Star topology. This topology has a hierarchical flow of data.



Hybrid Topology: A hybrid network is any computer network that uses more than one type of connecting technology or topology. Hybrid network combines the benefits of different types of topologies. It can be modified as per the requirement. It is extremely flexible. It is very reliable. It is easily scalable.



CONNECTION ORIENTED & CONNECTIONLESS SERVICES, SERVICE PRIMITIVES, DESIGN ISSUES & ITS FUNCTIONALITY

- **Connection-oriented:**

There is a sequence of operation to be followed by the users of connection-oriented service. They are:

1. Connection is established
2. Information is sent
3. Connection is released

In connection-oriented service we must establish a connection before starting the communication. When connection is established we send the message or the information. Then we release the connection.

Connection oriented service is more reliable than connectionless service. Example of connection oriented is TCP (Transmission Control Protocol) protocol.

- **Connectionless:**

It is similar to postal services, as it carries the full address where the message (letter) is to be carried. Each message is routed independently from source to destination. The order of message sent can be different from the order received.

In connectionless the data is transferred in one direction from source to destination without checking that destination is still there or not or if it prepared to accept the message.

Authentication is not needed in this. Example of Connectionless service is UDP (User Datagram Protocol) protocol.

DIFFERENCE BETWEEN CONNECTION-ORIENTED SERVICE AND CONNECTION-LESS SERVICE

Connection Oriented Service	Connection Less Service
Connection-oriented service is related to the telephone system.	Connection-less service is related to the postal system.
Connection-oriented service is preferred by long and steady communication.	Connection-less Service is preferred by busty communication.
Connection-oriented Service is necessary.	Connection-less Service is not compulsory.
Connection-oriented Service is feasible.	Connection-less Service is not feasible.
In connection-oriented Service, Congestion is not possible.	In connection-less Service, Congestion is possible.
Connection-oriented Service gives the guarantee of reliability.	Connection-less Service does not give the guarantee of reliability.
In connection-oriented Service, Packets follow the same route.	In connection-less Service, Packets do not follow the same route.
Connection-oriented Services requires a bandwidth of high range.	Connection-less Service requires a bandwidth of low range.

ISO OSI REFERENCE MODEL: PRINCIPLE, MODEL, DESCRIPTIONS OF VARIOUS LAYERS AND ITS COMPARISON WITH TCP/IP.

ISO stands for International Organization of Standardization. This is called a model for Open System Interconnection (OSI) and is commonly known as OSI model. The ISO-OSI model is a seven layer architecture. It defines seven layers or levels in a complete communication system.

PRINCIPLES OF OSI REFERENCE MODEL:

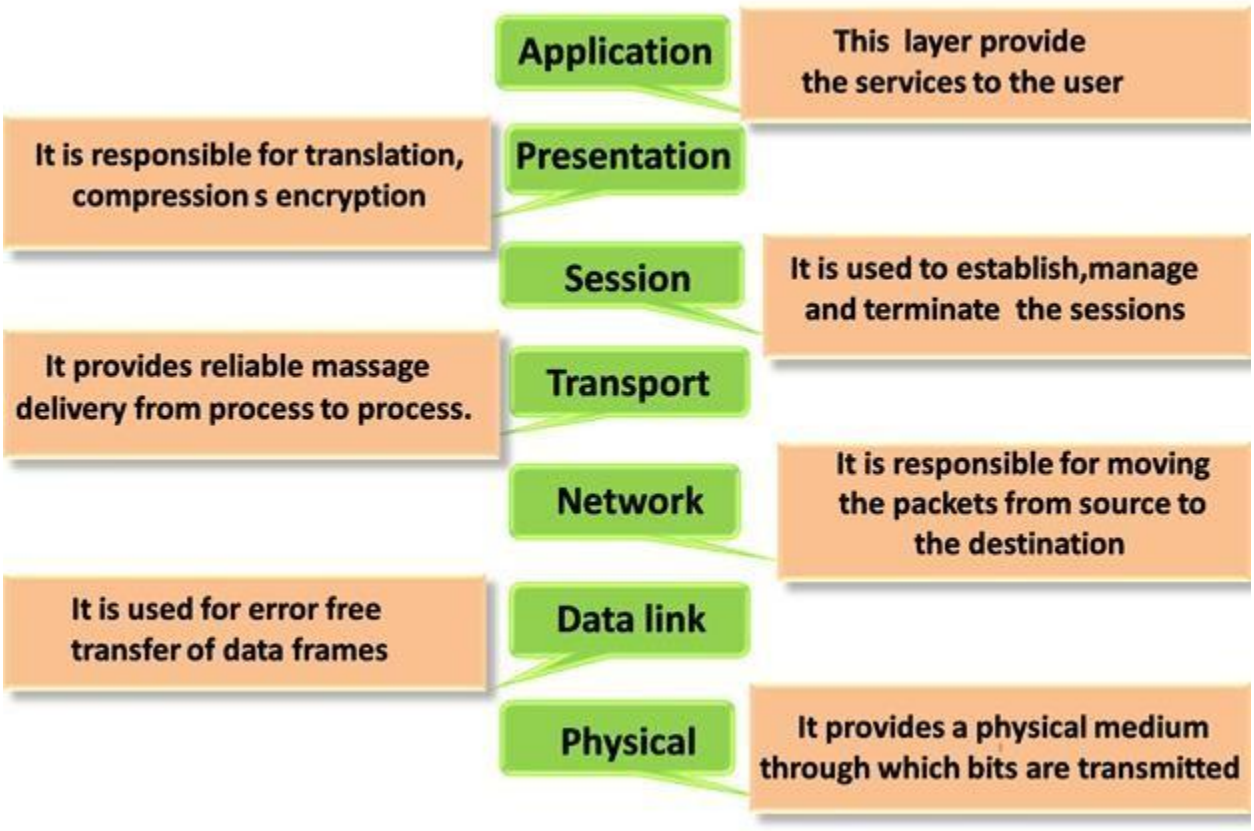
The OSI reference model has 7 layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

1. A layer should be created where a different abstraction is needed.
2. Each layer should perform a well-defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that architecture does not become unwieldy.

FEATURES OF OSI MODEL:

1. Big picture of communication over network is understandable through this OSI model.
2. We see how hardware and software work together.
3. We can understand new technologies as they are developed.
4. Troubleshooting is easier by separate networks.
5. Can be used to compare basic functional relationships on different networks.

DESCRIPTION OF DIFFERENT LAYERS IN OSI:



Layer 1: The Physical Layer:

- It is the lowest layer of the OSI Model.
- It activates, maintains and deactivates the physical connection.
- It is responsible for transmissionand reception of the unstructured raw data overnetwork.
- Voltages and data rates needed for transmission is defined in the physical layer.
- It converts the digital/ analog bits into electrical signal or optical signals.
- Data encoding is also done in this layer.
- Contain **stream of bits.**

Layer 2: Data Link Layer:

- Data link layer synchronizes the information which is to be transmitted over the physical layer.
- The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
- Transmitting and receiving **data frames** sequentially is managed by this layer.
- This layer sends and expects acknowledgements for frames received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.
- This layer establishes a logical layer between two nodes and also manages the Frame traffic control over the network. It signals the transmitting node to stop, when the frame buffers are full.
- Error control and flow control at local level.

- Node-to-Node or Hop-to-Hop.
- MAC addresses function at the data link layer.

Layer 3: Network Layer:

- It routes the signal through different channels from one node to other.
- It acts as a network controller. It manages the Subnet traffic.
- It decides by which route data should take.
- It divides the outgoing messages into packets and assembles the incoming packets into messages for higher levels.
- Fragmentation, Routing is done at this layer.
- Host-to-Host communication.
- Data in the form of **Packets/ Datagram.**

Layer 4: Transport Layer:

- It decides if data transmission should be on parallel path or single path.
- Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer
- It receives messages from the Session layer above it, converts the message into smaller units and passes it on to the Network layer.
- Transport layer can be very complex, depending upon the network requirements.
- End-to-End communication.
- Flow control and error control at global level.

Layer 5: Session Layer:

- Session layer manages and synchronize the conversation between two different applications.
- Transfer of data from source to destination session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely, and data loss is avoided.
- Dialog control, Synchronization, checkpoints maintain etc.

Layer 6: Presentation Layer

- Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data.
- While receiving the data, presentation layer transforms the data to be ready for the application layer.
- Languages (syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.
- It performs Data compression, Data encryption and decryption, Data conversion etc.
- Also a syntax layer.

Layer 7: Application Layer

- It is the topmost layer. It is the End user layer.

- It handles user request.
- Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc. are services provided by application layer.
- This layer mainly holds application programs to act upon the received and to be sent data.

Merits of OSI reference model:

- OSI model distinguishes well between the services, interfaces and protocols.
- Protocols of OSI model are very well hidden.
- Protocols can be replaced by new protocols as technology changes.
- Supports connection-oriented services as well as connectionless service.

Demerits of OSI reference model:

- Model was devised before the invention of protocols.
- Fitting of protocols is tedious task.
- It is just used as a reference model.

TCP/IP REFERENCE MODEL:

The TCP/IP reference model was developed prior to OSI model. The major design goals of this model were,

1. To connect multiple networks together so that they appear as a single network.
2. To survive after partial subnet hardware failures.
3. To provide a flexible architecture.

Unlike OSI reference model, TCP/IP reference model has only 4 layers. They are,

1. Network Interface Layer or Host-to-Network Layer
2. Network Layer
3. Transport Layer
4. Application Layer

Layer 1: Network Interface Layer or Host-to-Network Layer

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network.

Layer 2: Network Layer

1. Selection of a packet switching network which is based on a connectionless inter network layeris called a internetlayer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.
6. The various functions performed by the Internet Layer are:
    - Delivering IP packets

- Performing routing
- Avoiding congestion

Layer 3: Transport Layer

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the networklayer.
6. Transport layer also arrange the packets to be sent, in sequence.

Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

Merits of TCP/IP model:

1. It operated independently.

2. It is scalable.

3. Client/server architecture.

4. Supports 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.

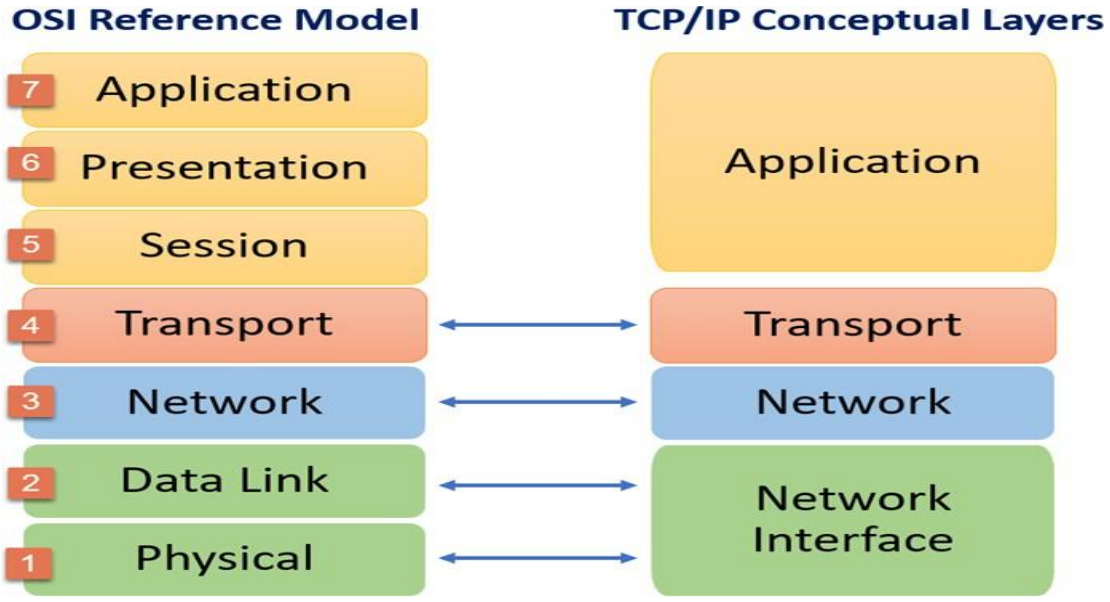


Fig: OSI 7 LAYERS AND TCP/IP 4 LAYERS

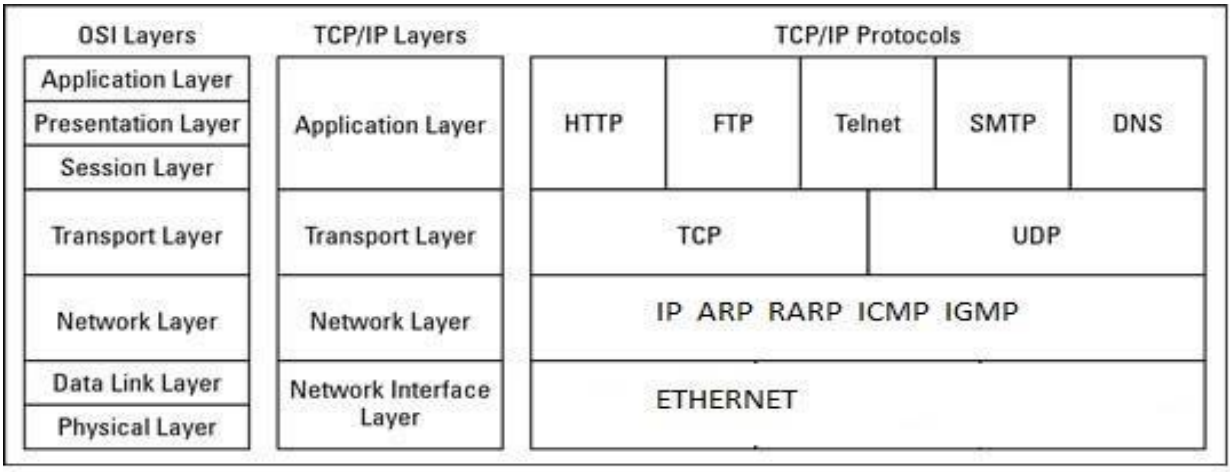


Fig: PROTOCOLS USED IN EACH LAYER OF TCP/IP

Following are the main protocols used in the Application Layer of TCP/IP:

HTTP: HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the World Wide Web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.

SNMP: SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.

SMTP: SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.

DNS: DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.

TELNET: It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.

FTP: FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

Following are the main protocols used in the Transport Layer of TCP/IP:

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

TCP	UDP
TCP is a connection oriented protocol.	UDP is a connection less protocol.
It is reliable.	It is not reliable.
It is slower than UDP.	It is faster than TCP.
The header size of TCP is 20 bytes.	The header size of UDP is 8 bytes.
Retransmission of lost packet is possible.	Retransmission of lost packet is not possible.
Error checking and error recovery.	Simply error checking but no error recovery.
Handshake	No handshake
Acknowledgements	No Acknowledgements
Rearrangement of packets in order.	No inherent order.

Following are the main protocols used in the Network Layer of TCP/IP:

IP: An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol". IP address is of 32-bits. It is also called a logical address.

ARP: ARP stands for Address Resolution Protocol. ARP is a network layer protocol which is used to find the physical address (MAC) from the IP address.

ARP: IP ⟶ MAC

RARP: RARP stands for Reverse Address Resolution Protocol. RARP is a network layer protocol which is used to find the IP address from the physical address (MAC).

RARP: MAC ⟶ IP

ICMP: ICMP stands for Internet Control Message Protocol. The Internet Control Message Protocol (ICMP) is a network layer protocol used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner.

IGMP: The Internet Group Management Protocol (IGMP) is a protocol that allows several devices to share one IP address so they can all receive the same data.

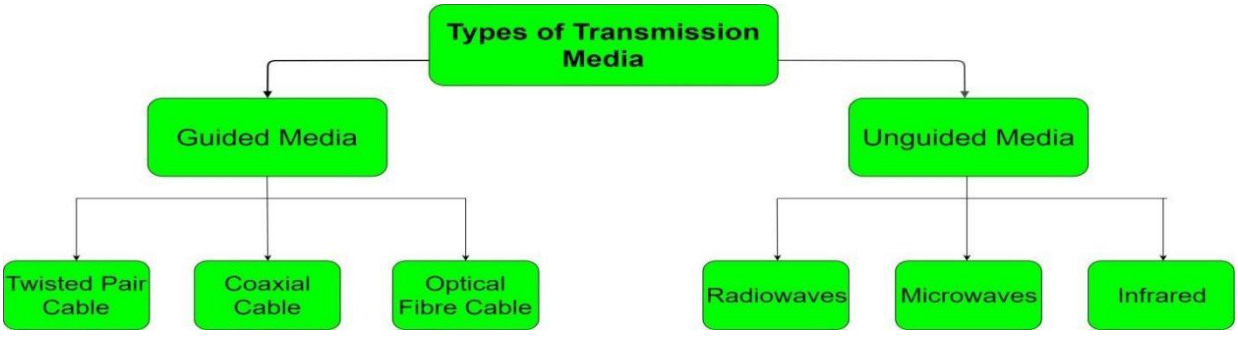
DIFFRENCE BETWEEN OSI AND TCP/IP:

OSI	TCP/IP
OSI refers to Open Systems Interconnection.	TCP/IP refers to Transmission Control Protocol.
OSI has 7 layers	TCP/IP has 4 layers
The OSI Model is a logical and conceptual model that defines network communication used by systems. Hence, a theoretical model.	TCP/IP helps you to determine how a specific computer should be connected to the internet and how you can be transmitted between them. Hence, a practical model.
OSI follows a vertical approach.	TCP/IP follows a horizontal approach.
OSI model is developed by ISO (International Standard Organization)	TCP Model is developed by ARPANET (Advanced Research Project Agency Network).
OSI is a reference model around which the networks are built. Generally, it is used as a guidance tool.	TCP/IP model is, in a way implementation of the OSI model.
Have separate application, presentation and session layer.	Have combined presentation and session layer with the application layer.
Protocols are hidden in OSI model and are easily replaced as the technology changes.	In TCP/IP replacing protocol is not easy.
OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
Network Layer is both Connection Oriented and Connection less.	Network Layer is Connection less
Transport Layer is Connection Oriented.	Transport Layer is both Connection Oriented and Connection less.

Principals of Physical Layer:

Physical Layer is the bottom-most layer in the Open System Interconnection (OSI) Model which is a physical and electrical representation of the system. It consists of various network components such as power plugs, connectors, hubs, receivers, cable types, etc. Physical Layer sends data bits from one device(s) (like a computer) to another device(s). Physical Layer defines the types of encoding (that is how the 0's and 1's are encoded in a signal). Physical Layer is responsible for the communication of the unstructured raw data streams over a physical medium. It contains Streams of bits and performs synchronization of bits.

Physical Layer Transmisson Media:



Two types of transmission media are:

1. **Guided Media:** It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links/ medium. Features: High Speed, Secure, Used for comparatively shorter distances
    - **Twisted Pair Cable:** A twisted pair cable is a type of cable made by putting two separate insulated wires together in a twisted pattern and running them parallel to each other. This type of cable is widely used in different kinds of data and voice infrastructures.
    - **Coaxial Cable:** Coaxial cable is a type of transmission line, used to carry high-frequency electrical signals with low losses. It is used in such applications as telephone trunk lines, broadband internet networking cables, high-speed computer data busses, cable television signals, and connecting radio transmitters and receivers to their antennas.
    - **Fiber Optics Cable:** It uses the concept of reflection of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for the transmission of large volumes of data.

2. **Unguided Media:** It is referred to as Wireless or Unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals. Features: The signal is broadcasted through air, Less Secure, Used for larger distances. Ex- In Space.
    - **Radio waves:** Radio waves are a type of electromagnetic radiation best-known for their use in communication technologies, such as television, mobile phones and radios.
    - **Micro waves:** Microwave is a form of high frequency radio signal (operating at thousands of MHz) in which the signal is not broadcast but is transmitted in a straight line through the air. Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications.
    - **Infrared:** Infrared (IR) radiation, sometimes called infrared light. Infrared (IR) radiation is a type of electromagnetic radiation (a wave with electricity). The wave is longer than light which humans can see and shorter than microwaves.

Bandwidth: Bandwidth is defined as the potential of the data that is to be transferred in a specific period of time. It is the data carrying **capacity** of the network or transmission medium. In simple words, it is the maximum amount of data that can be transferred per second on a link. It is generally measured in bits per second (bps), mega bits per second (Mbps) or Giga bits per second (Gbps).

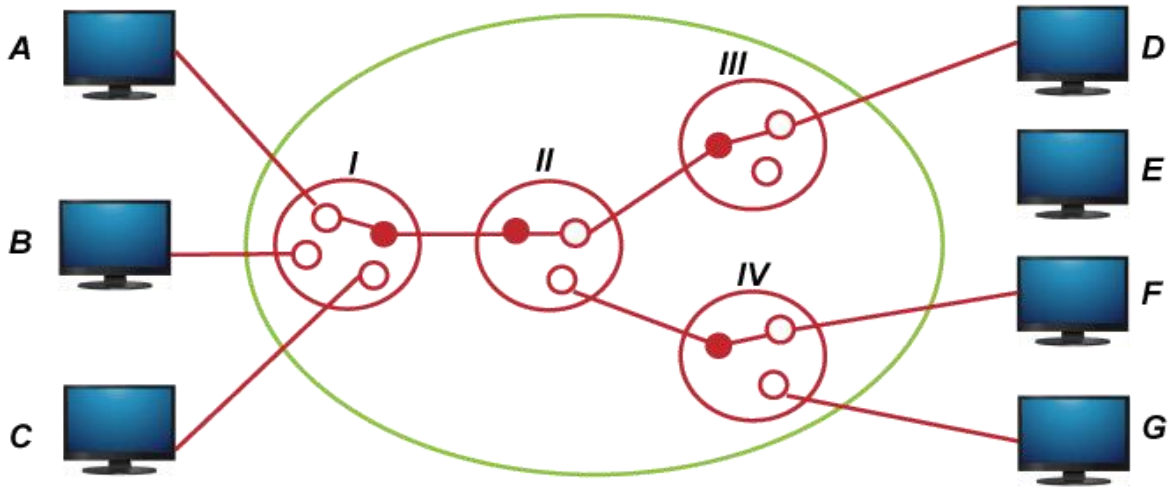
Data Rate: Data Rate is defined as the amount of data transmitted during a specified time period over a network. It is the **speed** at which data is transferred from one device to another or between a peripheral device and the computer. It is generally measured in mega bits per second (Mbps) or Mega Bytes per second (MBps).

Modulations: Modulation is the process by which information is encoded into electrical signals for transmission over a medium. Binary information, as represented by a series of 1s and 0s, must be converted to analog or digital electrical signals for transmission.

SWITCHING METHODS: CIRCUIT SWITCHING & PACKET SWITCHING

Circuit Switching Network:

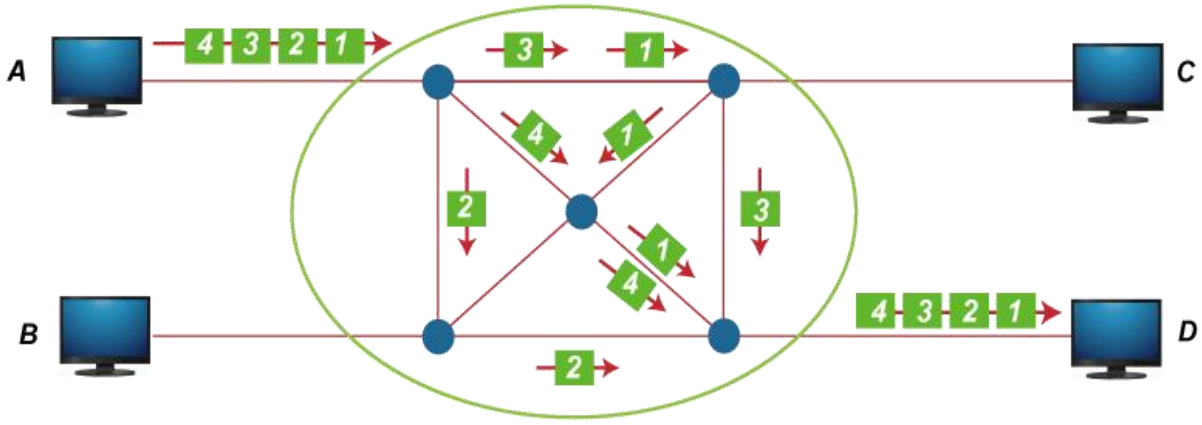
A circuit-switched network is one of the simplest data communication methods in which a dedicated path is established between the sending and receiving device. In this physical links connect via a set of switches. In the figure, it shows a circuit switched network in which computer connect via 4 switches with a point to point connections.



Circuit Switched Network

Packet Switching Network:

In the Packet switching Network, the message is divide into packets. Each packet contains a header which includes the source address, destination address, and control information. In the figure, it shows how a datagram (packet) approach is used to deliver four packets from station A to station D.



Packet Switched Network

S.No	Parameter	Circuit switching Network	Packet switching Network
1	Path	In circuit switched network a dedicated path is created between two points by setting the switches.	In packet switched network no dedicated path is created between two points. Only the virtual circuit exists.
2	Store and forward transmission	In circuit switching there is no concept of store and forward transmission.	In virtual packet switched network, each node may store incoming packets and forward them after use.
3	Dedicated	The links that make a path in circuit switched network are dedicated and cannot be used for other connections.	In the virtual circuit network, links that make a route can be dedicated with other connections.
4	Availability of Bandwidth	In circuit switching, bandwidth is fixed because it is reserved in advance.	In the virtual circuit network, require bandwidth is dynamic because it can be released as it is needed.
5	The route followed by packets	The route followed by packets is always the same.	The route followed by packets is may or may not be different.
6	Call setup	An in-circuit switching call setup is required.	In packet switching, call setup is not required.
7	Congestion	In circuit switching, congestion can occur at set up time.	In packet switching, congestion can occur on every packet.
8	Wastage of Bandwidth	In circuit switching, bandwidth is fixed, unused bandwidth on an allocated circuit is wasted.	Other packets from an unrelated source may utilize unused bandwidth.
9	Charging	In circuit switching, users are charged based on time and the basis of distance.	In packet switching, users are charged based on time and number of bytes carried & not based on distance.
10	Application	Telephone network for bidirectional, real time transfer of voice signal.	Internet for datagram and reliable stream service between computers.
11	Layers	Circuit-switched network is implemented at the physical layer.	A virtual circuit network is implemented at the data link and a network layer.
12	Reliability	Circuit-switched is highly reliable.	In packet switching, low reliability, subject to congestion.
13	Overhead bits	In Circuit-switched network, no overhead bits after call setup.	In packet switching, Overhead bits in each packet.
14	Technologies or types	Circuit switching using two technologies ○ Time Division Switching ○ Space Division Switching	Packet Switching using two technologies ○ Datagram circuit approach ○ Virtual circuit Approach
15	Installation Cost	Circuit switching's initial cost is low.	Packet switching networks have high installation costs.

16	Protocols	Circuit switching requires simple protocols for delivery.	Packet switching requires complex protocols for delivery.
17	Addressing scheme	In Circuit switching, Hierarchical numbering plan scheme is used.	In Packet switching, Hierarchical address space is used.
18	End Terminal	In this telephone and modem is used as end terminal.	In this computer is used as end terminal.
19	Information type	In this information type is Analog voice or PCM digital voices.	In this information type is binary information.
20	Multiplexing scheme	In circuit switching, circuit multiplexing is used.	In packet switching, packet multiplexing shared media access network in used.
21	Routing Scheme	In circuit switching, route selecting during set up.	In packet switching, each packet is routed independently.

TIME DIVISION MULTIPLEXING (TDM)

- TDM is a method that allows multiple signals to share a single communication channel/resource by dividing it into time slots so that each signal can use the channel.
- In TDM, the channel is divided into several time slots, and each signal is transmitted during its allocated time slot. As a result, several signals share the channel without interfering with each other.
- TDM is commonly used in telecommunications, broadcasting, and computer networking to increase data transmission efficiency.

Some of the simple examples of time division multiplexing are:

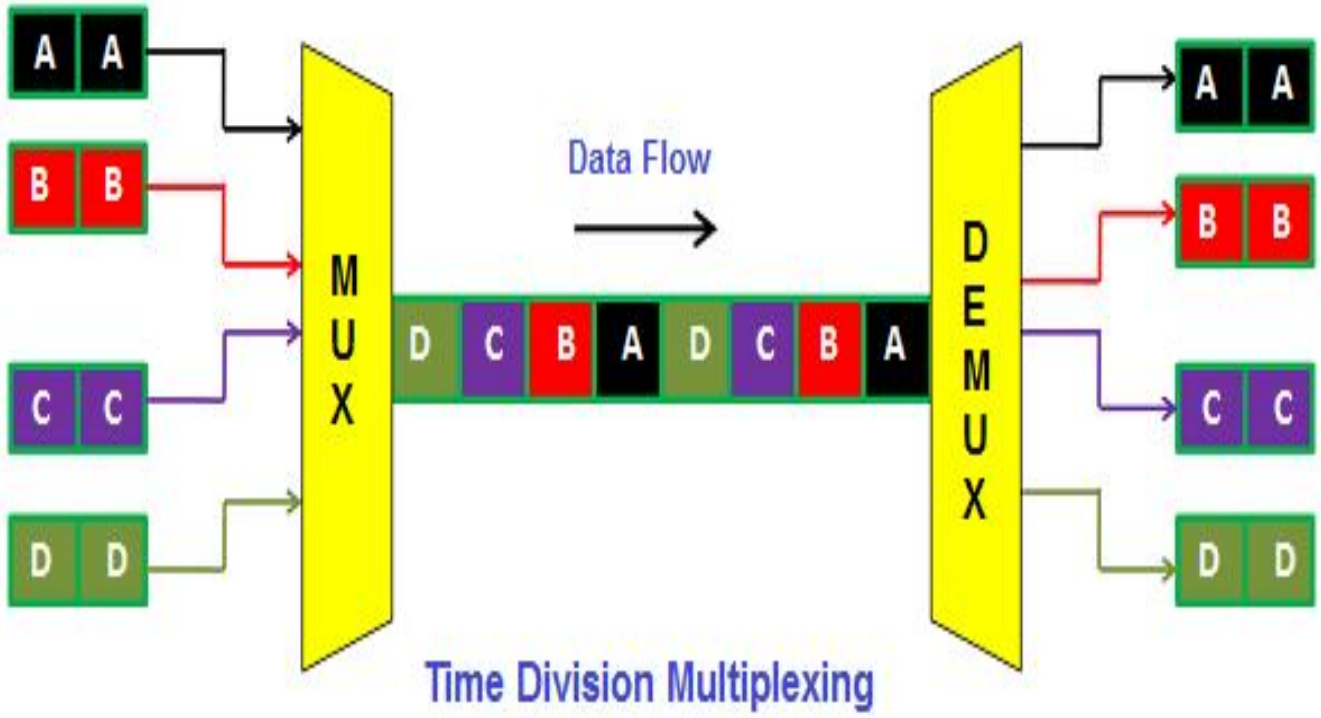
- Multiple users sharing a printer
- Traffic lights to manage the flow of traffic
- Digital TV broadcasting of TV channels

In all these examples, time division multiplexing is used to allow multiple users or signals to share a single resource without interfering with one another. Conflicts are avoided by allocating specific time slots for each user or signal, and the resource can be used more efficiently.

TDM is broadly divided into three types:

1) **Synchronous TDM:** In Synchronous TDM, each signal is transmitted in fixed time slots synchronized with the transmitter's clock. Synchronous TDM is commonly used in digital telecommunications networks, allowing multiple voice or data signals to be transmitted over a single communication line. (Clock)
2) **Asynchronous TDM:** In Asynchronous TDM, each signal is assigned a time slot, and these slots are transmitted asynchronously; they are not synchronized to a common clock signal. This allows signals with different data rates to be transmitted over the same channel. ATDM is widely used in telecommunications and computer networks to improve bandwidth utilization and reduce transmission delays. (No Clock)
3) **Statistical TDM:** In Statistical TDM, the time slots are not fixed but vary depending on how much data is transmitted. Statistical TDM is often used in computer networks and broadband services where data traffic is highly variable and unpredictable.

TDM's workflow is represented as:



ANALOG - TO - DIGITAL CONVERTOR

DIGITAL - TO - ANALOG CONVERTOR

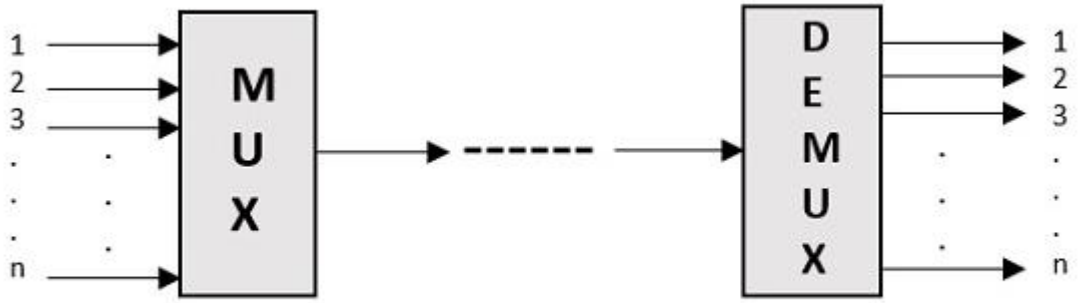
MUX: convert multiple signals into single signal

DMUX: convert single signal into multiple signals

BASIC IDEA OF MULTIPLEXING:

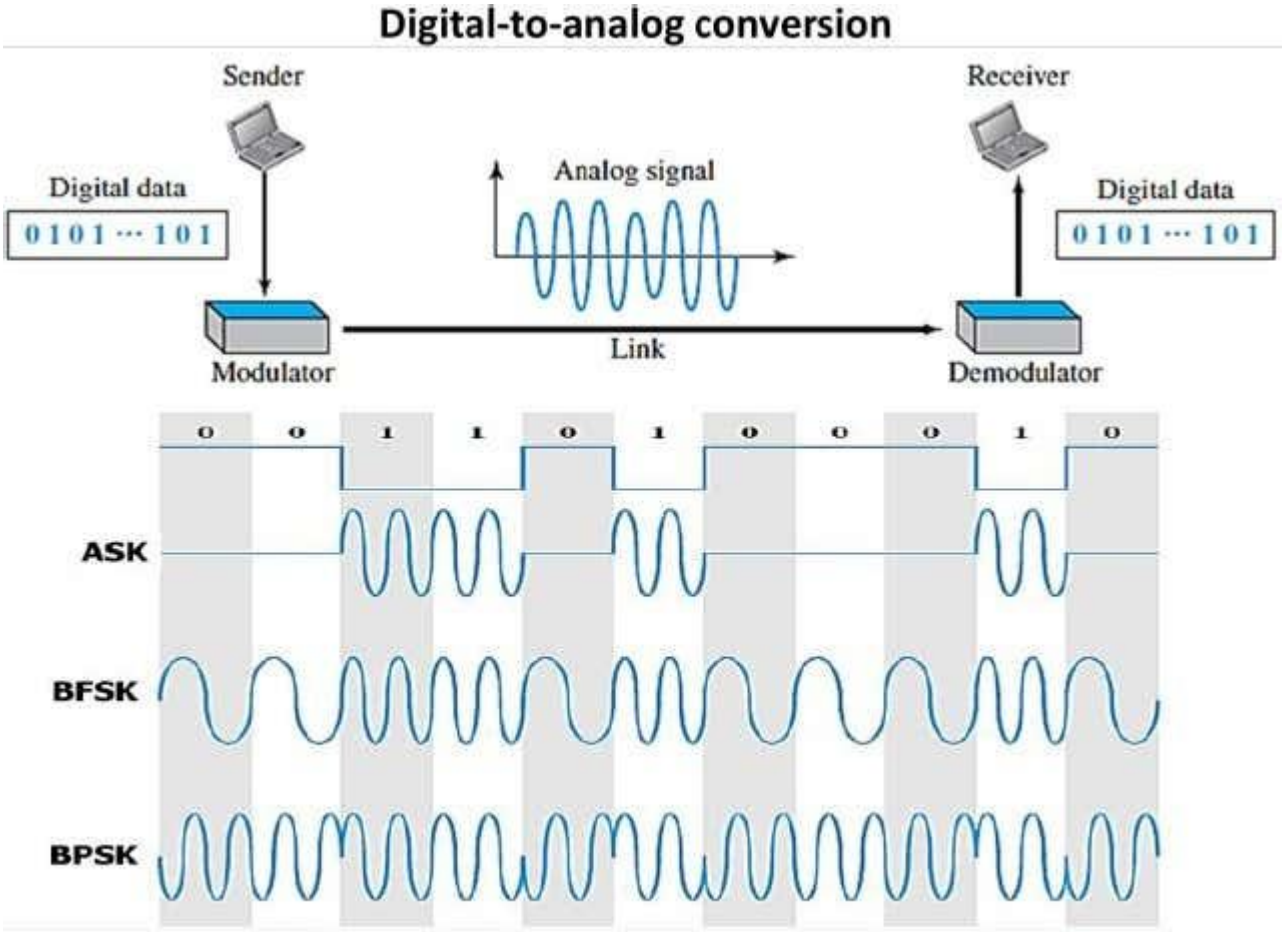
MUX: Multiplexing is the process of combining multiple signals into one signal, over a shared medium.

DMUX: Demultiplexing is the process of converting one signal into multiple signals, over a shared medium.

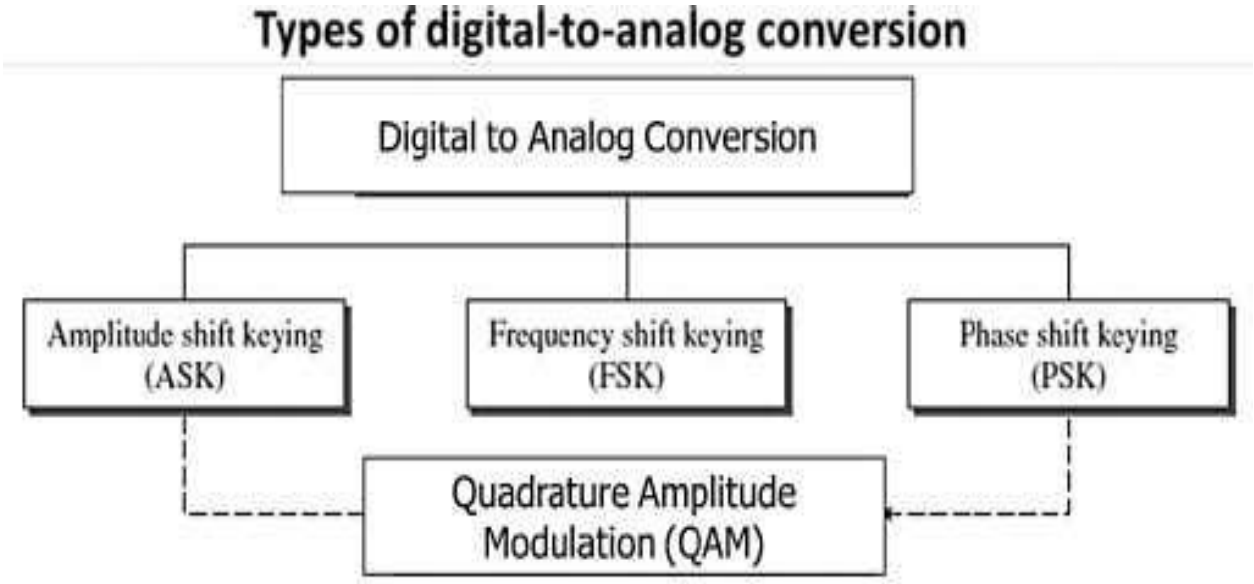


Multiplexing and Demultiplexing

BASIC IDEA OF MODULATION (ASK, FSK, PSK):



Modulation of Analog Signals for Digital Data



S. No.	Parameters	ASK	FSK	PSK
1	Stands For	Amplitude Shift Key	Frequency Shift Key	Phase Shift Key
2	Modulation Technique	Digital Modulation Technique	Digital Modulation Technique	Digital Modulation Technique
3	Variable Characteristics	Varies Amplitude	Varies Frequency	Varies Phase
4	Bandwidth Requirement	2 fb	4 fb	2 fb
5	Noise Immunity	Low	High	High
6	Error Probablity	High	Low	Low
7	Complexity	Simple	Moderately Complex	Very Complex
8	Performance in Presence of NOISE	Poor	Better than ASK	Better than FSK

TRANSMISSION IMPAIRMENT:

TRANSMISSION IMPAIREMENT

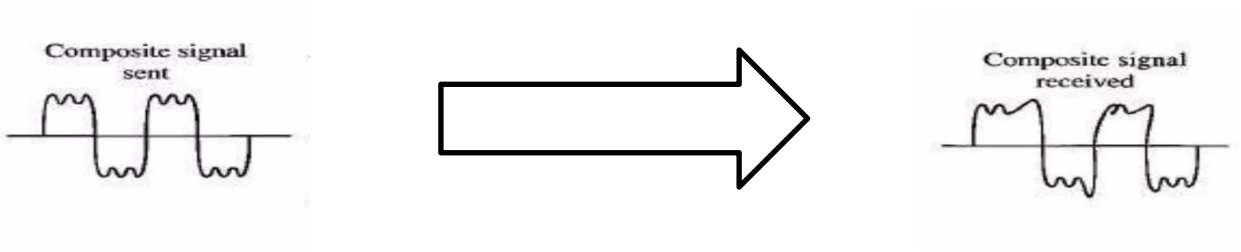
- When a signal transmit from one transmission medium to other, the signal that is received may differ from the signal that is transmitted, due to various transmission impairments.
- Consequences:
  - For analog signals: degradation of signal quality
  - For digital signals: bit errors
- The most significant impairments include
  - **Attenuation**
  - **Distortion**
  - **Noise**

Attenuation

- Attenuation refers to lose of energy by a signal time.
- When a signal, simple or composite , travels through a medium ,it loses some of its energy in overcoming the resistance of the medium.
- It compensate for this lose, amplifier are used.

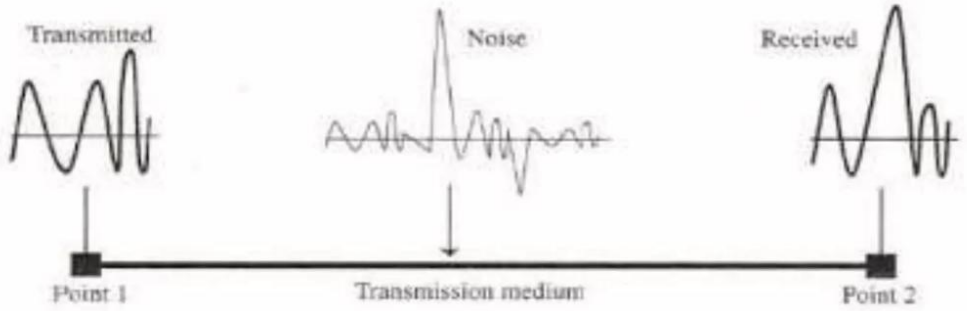
Distortion

- Distortion means signal changes its form or shape.
- Distortion can occur in a composite signal made of different frequency. Each signal component have its own propogation spped through a medium and therefore its own delay in arriving at the final signal.



Noise

- Several type of noise as thermal noise, induced noise ,crosstalk noise, impule noise may corrrupt the signal.



LINE CODING SCHEME:

Signals that represents the **data** can either be in the form of **digital or analog signals. Line coding** is the process of converting **digital data** to **digital signals.** By this technique we converts a **sequence of bits/ binary data** to a **digital signal/ discrete signal**. At the sender side digital data are encoded into a digital signal and at the receiver side the digital data are recreated by decoding the digital signal.

We can roughly divide line coding schemes into five categories:

1) Unipolar (NRZ, RZ).

2) Polar (NRZ-L, NRZ-I, RZ, Manchester and Differential Manchester).

3) Bipolar (AMI and Pseudoternary).