UNIT I - INTRODUCTION AND PHYSICAL LAYER

Networks – Network Types – Protocol Layering – TCP/IP Protocol suite – OSI Model – Physical Layer : Performance – Transmission Media – Switching – Circuit Switched Networks – Packet Switching

INTRODUCTION TO NETWORKS

- A network is a set of devices (often referred to as nodes) connected by communication links.
- A node can be a computer, printer, or any other device capable of sending or receiving data generated by other nodes on the network.
- When we communicate, we are sharing information. This sharing can be local or remote.

CHARACTERISTICS OF A NETWORK

The effectiveness of a network depends on three characteristics.

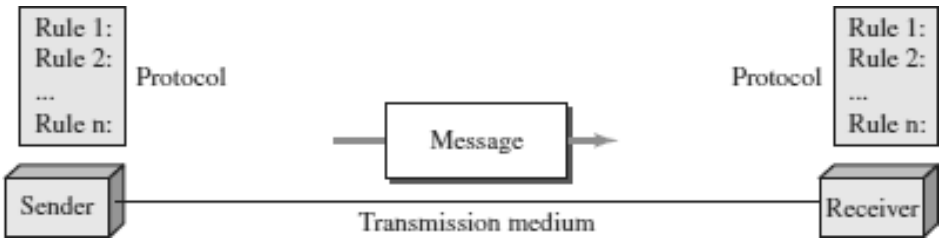
1. ***Delivery***: The system must deliver data to the correct destination.
2. ***Accuracy***: The system must deliver data accurately.
3. ***Timeliness***: The system must deliver data in a timely manner.

CRITERIA NECESSARY FOR AN EFFECTIVE AND EFFICIENT NETWORK

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

Factors that affect the Performance of a network:	***Factors that affect the Reliability of a network:***	***Factors that affect the Security of a network:***
1. Number of users 2. Type of transmission medium 3. Capabilities of the connected hardware	1. Efficiency of software. 2. Frequency of failure 3.Recovery time of a network after a failure	1.Protecting data from unauthorized access and viruses.

COMPONENTS INVOLVED IN A NETWORK PROCESS



The five components are:

1. **Message** - It is the information to be communicated. Popular forms of information include text, pictures, audio, video etc.
2. **Sender** - It is the device which sends the data messages. It can be a computer, workstation, telephone handset etc.
3. **Receiver** - It is the device which receives the data messages. It can be a computer, workstation, telephone handset etc.
4. **Transmission Medium** - It is the physical path by which a message travels from sender to receiver. Some examples include twisted-pair wire, coaxial cable, radiowaves etc.
5. **Protocol** - It is a set of rules that governs the data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating.

KEY ELEMENTS OF PROTOCOL

- ***Syntax***: Refers to the structure or format of the data, meaning the order in which they are presented.
- ***Semantics***: Refers to the meaning of each section of bits.
- ***Timing***: Refers to two characteristics. (1). When data should be sent and (2). How fast they can be sent.

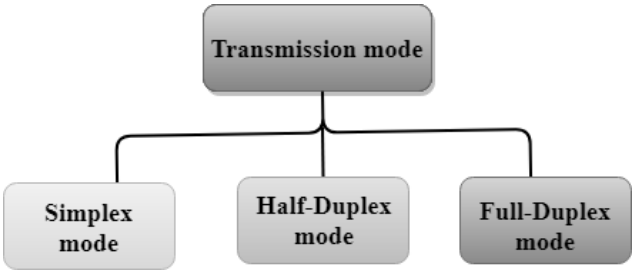
TRANSMISSION MODES

- The way in which data is transmitted from one device to another device is known as **transmission mode**.
- The transmission mode is also known as the communication mode.
- Each communication channel has a direction associated with it, and transmission media provide the direction. Therefore, the transmission mode is also known as a directional mode.
- The transmission mode is defined in the physical layer.

Types of Transmission mode

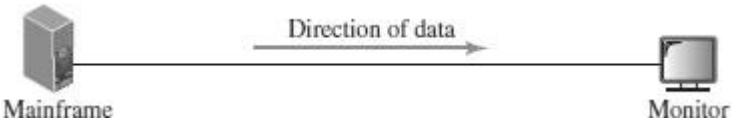
The Transmission mode is divided into three categories:

- Simplex Mode
- Half-duplex Mode
- Full-duplex mode (Duplex Mode)



SIMPLEX MODE

- In Simplex mode, the communication is unidirectional, i.e., the data flow in one direction.
- A device can only send the data but cannot receive it or it can receive the data but cannot send the data.
- This transmission mode is not very popular as mainly communications require the two-way exchange of data. The simplex mode is used in the business field as in sales that do not require any corresponding reply.
- The radio station is a simplex channel as it transmits the signal to the listeners but never allows them to transmit back.
- **Keyboard and Monitor** are the examples of the simplex mode as a keyboard can only accept the data from the user and monitor can only be used to display the data on the screen.
- The main advantage of the simplex mode is that the full capacity of the communication channel can be utilized during transmission.



Advantage of Simplex mode:

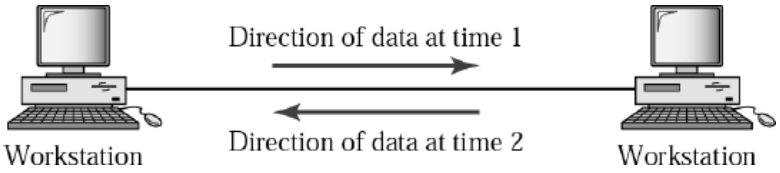
- In simplex mode, the station can utilize the entire bandwidth of the communication channel, so that more data can be transmitted at a time.

Disadvantage of Simplex mode:

- Communication is unidirectional, so it has no inter-communication between devices.

HALF-DUPLEX MODE

- In a Half-duplex channel, direction can be reversed, i.e., the station can transmit and receive the data as well.
- Messages flow in both the directions, but not at the same time.
- The entire bandwidth of the communication channel is utilized in one direction at a time.
- In half-duplex mode, it is possible to perform the error detection, and if any error occurs, then the receiver requests the sender to retransmit the data.
- A **Walkie-talkie** is an example of the Half-duplex mode.
- In Walkie-talkie, one party speaks, and another party listens. After a pause, the other speaks and first party listens. Speaking simultaneously will create the distorted sound which cannot be understood.



Advantage of Half-duplex mode:

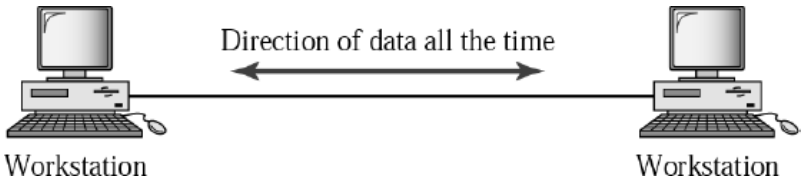
- In half-duplex mode, both the devices can send and receive the data and also can utilize the entire bandwidth of the communication channel during the transmission of data.

Disadvantage of Half-Duplex mode:

- In half-duplex mode, when one device is sending the data, then another has to wait, this causes the delay in sending the data at the right time.

FULL-DUPLEX MODE

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



Advantage of Full-duplex mode:

- Both the stations can send and receive the data at the same time.

Disadvantage of Full-duplex mode:

- If there is no dedicated path exists between the devices, then the capacity of the communication channel is divided into two parts.

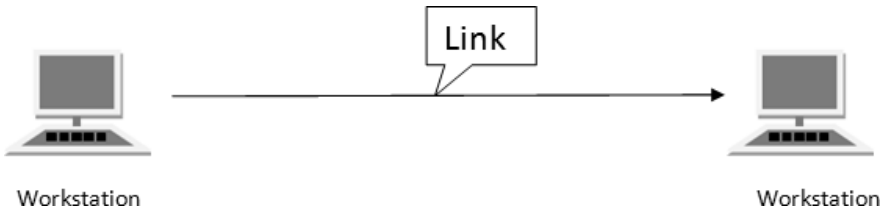
COMPARISON - SIMPLEX, HALF-DUPLEX AND FULL-DUPLEX MODE

BASIS FOR COMPARISON	SIMPLEX MODE	HALF-DUPLEX MODE	FULL-DUPLEX MODE
Direction of communication	Communication is unidirectional.	Communication is bidirectional, but one at a time.	Communication is bidirectional.
Send/Receive	A device can only send the data but cannot receive it or it can only receive the data but cannot send it.	Both the devices can send and receive the data, but one at a time.	Both the devices can send and receive the data simultaneously.
Example	Radio, Keyboard, and monitor.	Walkie-Talkie	Telephone network.

LINE CONFIGURATION / LINE CONNECTIVITY

Line configuration refers to the way two or more communication devices attach to a link. A link is a communications pathway that transfers data from one device to another. There are two possible line configurations:

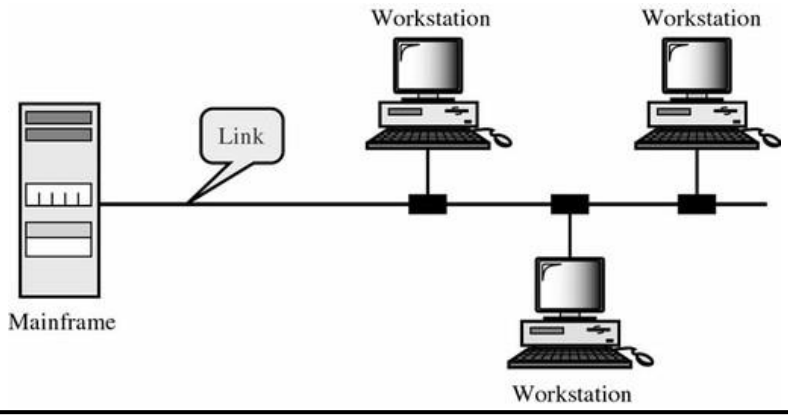
i. ***Point to Point*** **(PPP):** Provides a dedicated Communication link between two devices. It is simple to establish. The most common example for Point-to-Point connection is a computer connected by telephone line. We can connect the two devices by means of a pair of wires or using a microwave or satellite link.



ii. ***MultiPoint*** **:** It is also called ***Multidrop*** configuration. In this connection two or more devices share a single link.There are two kinds of Multipoint Connections.

- **Spatial Sharing**: If several devices can share the link simultaneously, it is called Spatially shared line configuration

- **Temporal (Time) Sharing**: If users must take turns using the link , then its called Temporally shared or Time Shared Line Configuration.

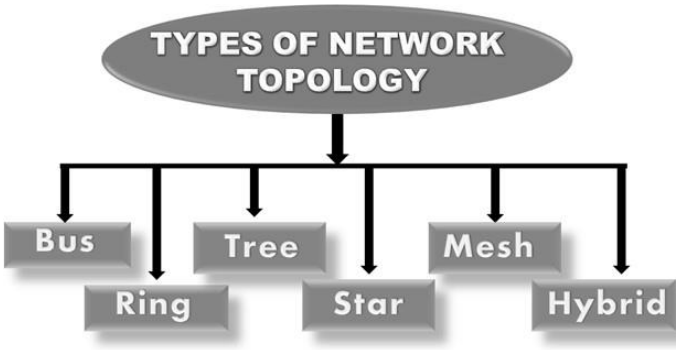


NETWORK TOPOLOGY

Two or more devices connect to a link. Two or more links form a topology.Topology is defined as

(1) The way in which a network is laid out physically.
(2)The geometric representation of the relationship of all the links and nodes to one-another.

The various types of topologies are : Bus, Ring, Tree, Star, Mesh and Hybrid.



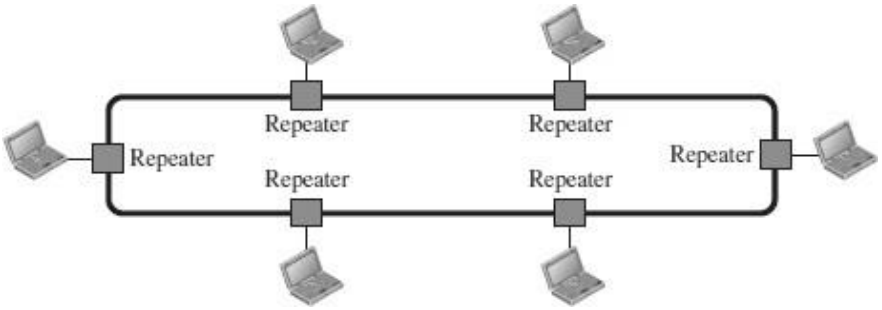
BUS TOPOLOGY

- Bus topology is a network type in which every computer and network device is connected to single cable.
- The long single cable acts as a backbone to link all the devices in a network.
- When it has exactly two endpoints, then it is called **Linear Bus topology.**
- It transmits data only in one direction.

Advantages of Bus Topology	***Disadvantages of Bus Topology***
1. It is cost effective. 2. Cable required is least compared to other network topology. 3. Used in small networks. 4. It is easy to understand. 5. Easy to expand joining two cables together	1. Cables fails then whole network fails. 2. If network traffic is heavy or nodes are more, the performance of the network decreases. 3. Cable has a limited length. 4. It is slower than the ring topology.

RING TOPOLOGY

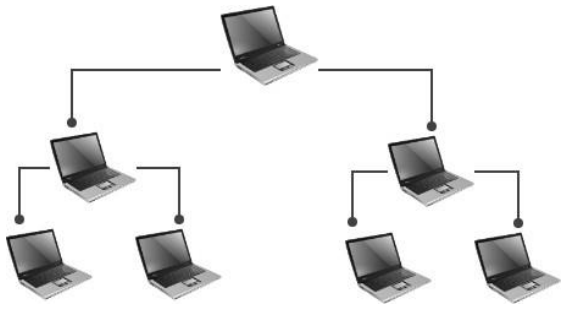
- In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction, from device to device, until it reaches its destination.
- Each device in the ring incorporates a repeater.
- When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.



Advantages of Ring Topology	***Disadvantages of Ring Topology***
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data. 2. Cheap to install and expand	1. Troubleshooting is difficult in ring topology. 2. Adding or deleting the computers disturbs the network activity. 3. Failure of one computer disturbs the whole network

TREE TOPOLOGY

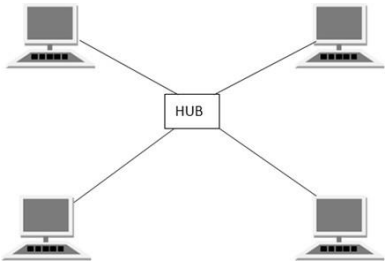
- It has a root node and all other nodes are connected to it forming a hierarchy.
- It is also called hierarchical topology.
- It should at least have three levels to the hierarchy.
- Tree topology is ideal if workstations are located in groups.
- They are used in Wide Area Network.

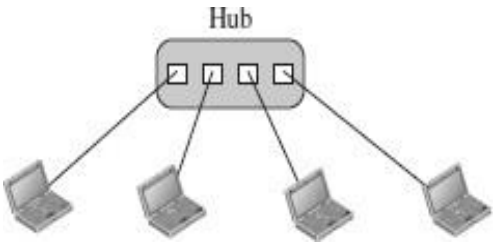


Advantages of Tree Topology	***Disadvantages of Tree Topology***
1. Extension of bus and star topologies. 2. Expansion of nodes is possible and easy. 3. Easily managed and maintained. 4. Error detection is easily done.	1. Heavily cabled. 2. Costly. 3. If more nodes are added maintenance is difficult. 4. Central hub fails, network fails.

STAR TOPOLOGY

- In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub.
- The devices are not directly linked to one another.
- The controller acts as an exchange.
- If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.

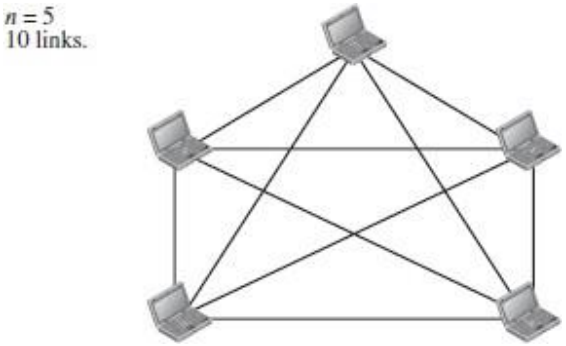




Advantages of Star Topology	***Disadvantages of Star Topology***
1. Fast performance with few nodes and low network traffic. 2. Hub can be upgraded easily. 3. Easy to troubleshoot. 4. Easy to setup and modify. 5. Only that node is affected which has failed, rest of the nodes can work smoothly	1. Cost of installation is high. 2. Expensive to use. 3. If the hub fails, then the whole network is stopped. 4. Performance is based on the hub that is it depends on its capacity

MESH TOPOLOGY

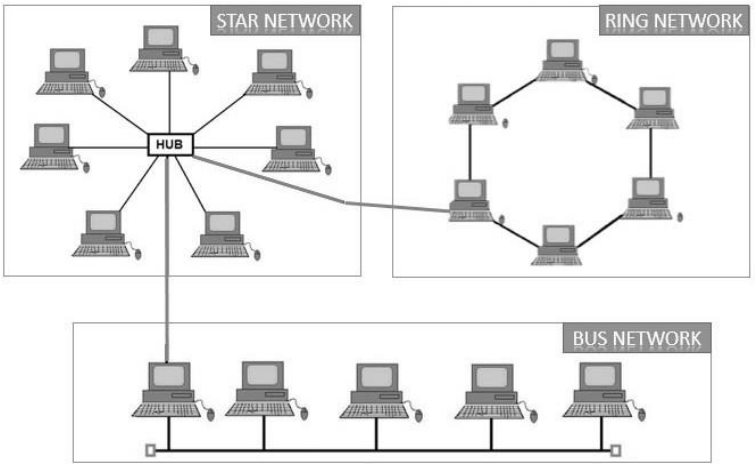
- In a mesh topology, every device has a dedicated point-to-point link to every other device.
- The term dedicated means that the link carries traffic only between the two devices it connects.
- The number of physical links in a fully connected mesh network with *n* nodes is given by $n(n-1)/2$.



Advantages of Mesh Topology	***Disadvantages of Mesh Topology***
1. Each connection can carry its own data load. 2. It is robust. 3. Fault is diagnosed easily. 4. Provides security and privacy.	1. Installation and configuration is difficult. 2. Cabling cost is more. 3. Bulk wiring is required.

HYBRID TOPOLOGY

- Hybrid Topology is a combination of one or more basic topologies.
- For example if one department in an office uses ring topology, the other departments uses star and bus topology, then connecting these topologies will result in Hybrid Topology.
- Hybrid Topology inherits the advantages and disadvantages of the topologies included.



Advantages of Hybrid Topology	***Disadvantages of Hybrid Topology***
1. Reliable as Error detecting and trouble shooting is easy. 2. Effective. 3. Scalable as size can be increased easily. 4. Flexible.	1. Complex in design. 2. Costly

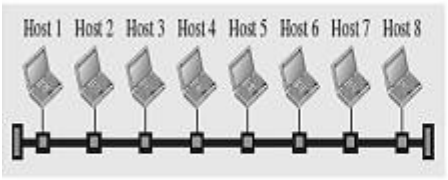
NETWORK TYPES

- A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.
- A computer network can be categorized by their size.
- A computer network is mainly of three types:
  1. Local Area Network (LAN)
  2. Wide Area Network (WAN)
  3. Metropolitan Area Network (MAN)

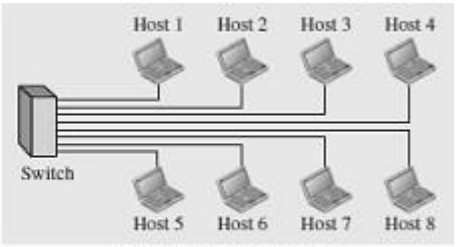
LOCAL AREA NETWORK (LAN)

- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.

- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- LAN can be connected using a common cable or a Switch.



a. LAN with a common cable (past)

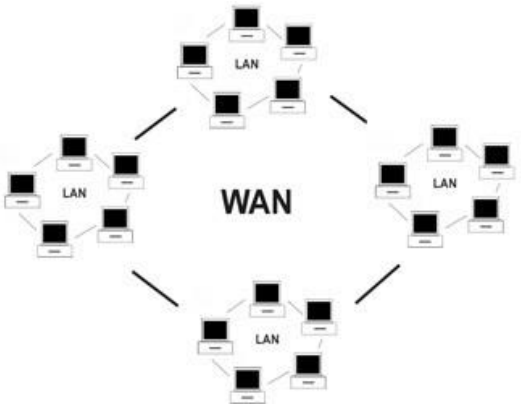


b. LAN with a switch (today)

Advantages of LAN	***Disadvantages of LAN***
•Resource Sharing •Software Applications Sharing. •Easy and Cheap Communication •Centralized Data. •Data Security •Internet Sharing	•High Setup Cost •Privacy Violations •Data Security Threat •LAN Maintenance Job •Covers Limited Area

WIDE AREA NETWORK (WAN)

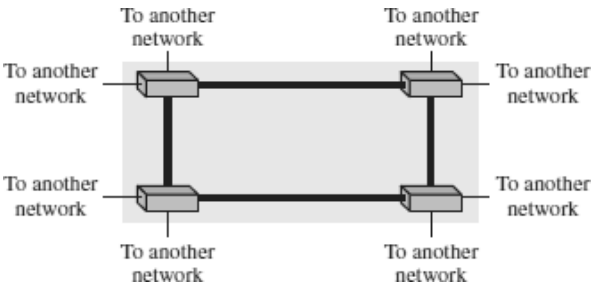
- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.



- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.
- WAN can be either a point-to-point WAN or Switched WAN.

Point-to-point WAN

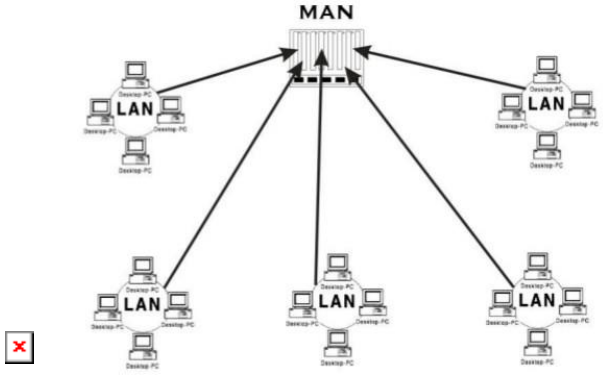
Switched WAN



***Advantages of Wide Area Network*:**	***Disadvantages of Wide Area Network*:**
○Large Geographical area ○Centralized data ○Exchange messages ○Sharing of software and resources ○High bandwidth	○Security issue ○Needs Firewall & antivirus software ○High Setup cost ○Troubleshooting problems

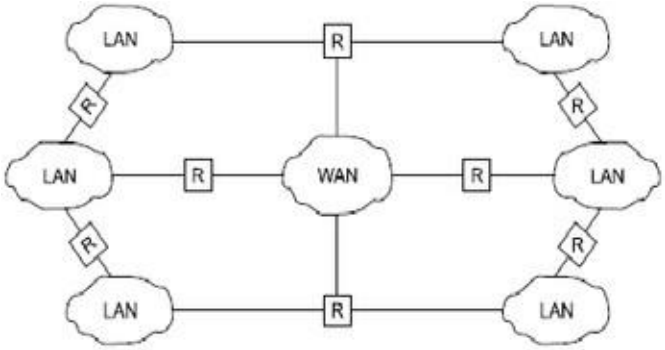
METROPOLITAN AREA NETWORK (MAN)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- It generally covers towns and cities (50 km)
- In MAN, various LANs are connected to each other through a telephone exchange line.
- Communication medium used for MAN are optical fibers, cables etc.
- It has a higher range than Local Area Network(LAN).It is adequate for distributed computing applications.



INTERNETWORK

- An internetwork is defined as two or more computer network LANs or WAN.
- An Internetwork can be formed by joining two or more individual networks by means of various devices such as routers, gateways and bridges.
- An interconnection between public, private, commercial, industrial, or government computer networks can also be defined as **internetworking**.



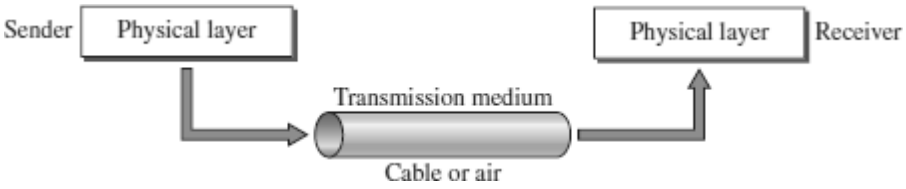
Types of Internetwork

Extranet	***Intranet***
An extranet is used for information sharing. The access to the extranet is restricted to only those users who have login credentials. An extranet is the lowest level of internetworking. It can be categorized as **MAN**, **WAN** or other computer networks. An extranet cannot have a single **LAN**, atleast it must have one connection to the **external network**.	An intranet belongs to an organization which is only accessible by the **organization's employee** or members. The main aim of the intranet is to share the information and resources among the organization employees. An intranet provides the facility to work in groups and for teleconferences.

TRANSMISSION MEDIA

- Transmission media is a communication channel that carries the information from the sender to the receiver.
- Data is transmitted through the electromagnetic signals.
- The main functionality of the transmission media is to carry the information in the form of bits (Either as Electrical signals or Light pulses).
- It is a physical path between transmitter and receiver in data communication.
- The characteristics and quality of data transmission are determined by the characteristics of medium and signal.
- Transmission media is of two types : Guided Media (Wired) and UnGuided Media (wireless).

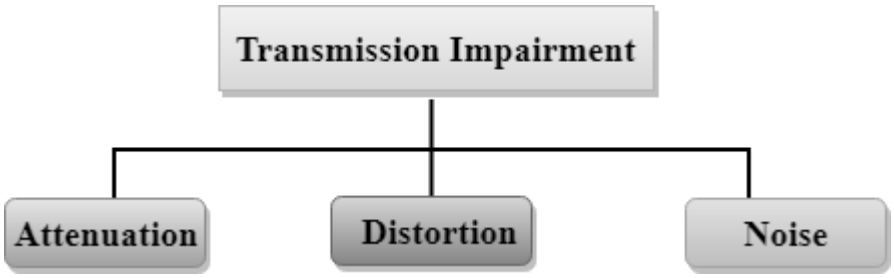
- In guided (wired) media, medium characteristics are more important whereas, in unguided (wireless) media, signal characteristics are more important.
- Different transmission media have different properties such as bandwidth, delay, cost and ease of installation and maintenance.
- The transmission media is available in the lowest layer of the OSI reference model, i.e., Physical layer.



FACTORS FOR DESIGNING THE TRANSMISSION MEDIA

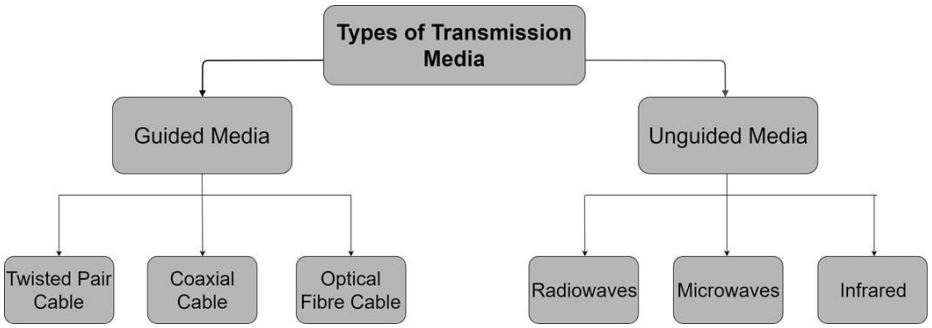
- **Bandwidth:** All the factors are remaining constant, the greater the bandwidth of a medium, the higher the data transmission rate of a signal.
- **Transmission impairment:** When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signals will get destroyed due to transmission impairment.
- **Interference:** An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.

CAUSES OF TRANSMISSION IMPAIRMENT



- **Attenuation:** Attenuation means the loss of energy, i.e., the strength of the signal decreases with increasing the distance which causes the loss of energy.
- **Distortion:** Distortion occurs when there is a change in the shape of the signal. This type of distortion is examined from different signals having different frequencies. Each frequency component has its own propagation speed, so they reach at a different time which leads to the delay distortion.
- **Noise:** When data is travelled over a transmission medium, some unwanted signal is added to it which creates the noise.

TYPES / CLASSES OF TRANSMISSION MEDIA

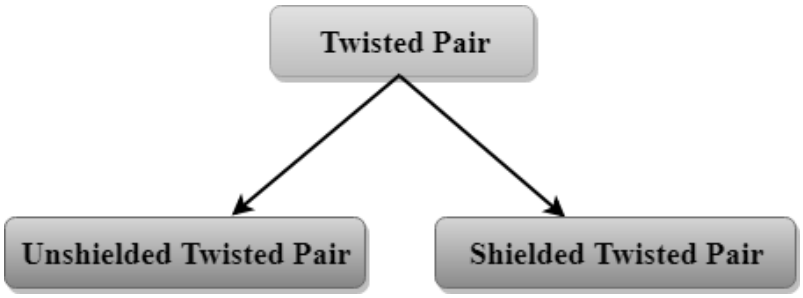


GUIDED MEDIA

- It is defined as the physical medium through which the signals are transmitted.
- It is also known as Bounded media.
- Types of Guided media: Twisted Pair Cable, Coaxial Cable , Fibre Optic Cable

TWISTED PAIR CABLE

- Twisted pair is a physical media made up of a pair of cables twisted with each other.
- A twisted pair cable is cheap as compared to other transmission media.
- Installation of the twisted pair cable is easy, and it is a lightweight cable.
- The frequency range for twisted pair cable is from 0 to 3.5KHz.
- A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.

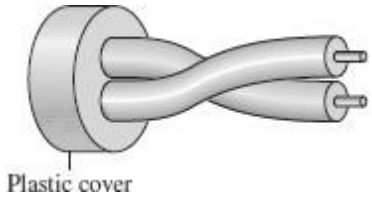


Unshielded Twisted Pair

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

- **Category 1:** Suports low-speed data.
- **Category 2:** It can support upto 4Mbps.

- **Category 3:** It can support upto 16Mbps.
- **Category 4:** It can support upto 20Mbps.
- **Category 5:** It can support upto 200Mbps.



Advantages :

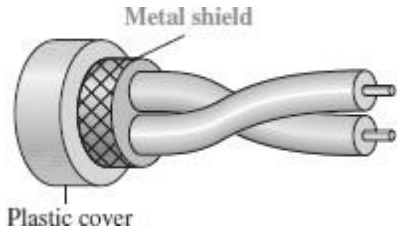
- It is cheap.
- Installation of the unshielded twisted pair is easy.
- It can be used for high-speed LAN.

Disadvantage:

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

Shielded Twisted Pair

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



Advantages :

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

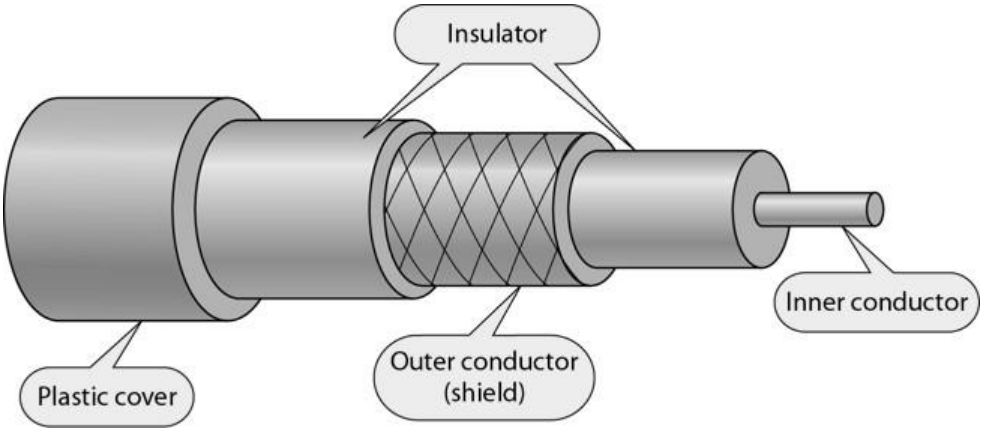
Disadvantages:

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

COAXIAL CABLE

- Coaxial cable(Coax) is a 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).
- Common applications of coaxial cable are Cable TV networks and traditional Ethernet LANs.



Coaxial Cable Standards

- Coaxial cables are categorized by their **Radio Government (RG)** ratings.
- Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and type of the inner insulator, the construction of the shield, and the size and type of the outer casing.
- Each cable defined by an RG rating is adapted for a specialized function.

Category	*Use*
RG-59	Cable TV
RG-58	Thin Ethernet
RG-11	Thick Ethernet

Types of Coaxial cable :

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

Advantages :

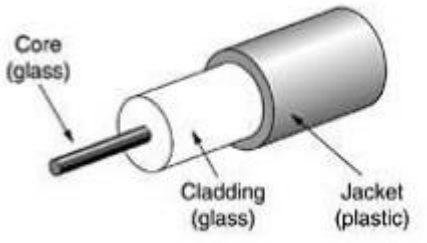
- The data can be transmitted at high speed.
- It has better shielding as compared to twisted pair cable.
- It provides higher bandwidth.

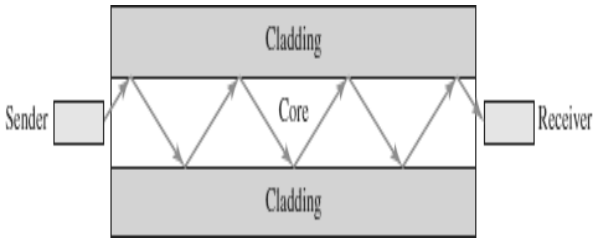
Disadvantages :

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

FIBRE OPTIC 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.





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.

Advantages:

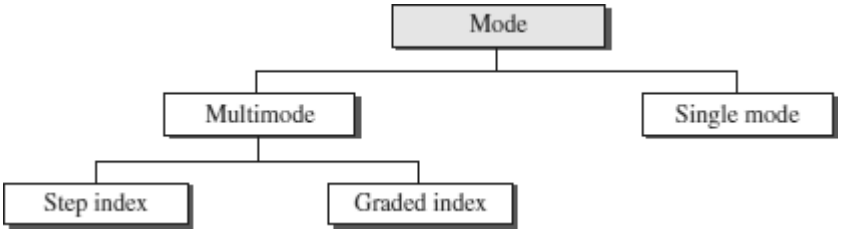
- Greater Bandwidth
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials
- Light weight
- Greater immunity to tapping

Disadvantages :

- Requires Expertise for Installation and maintenance
- Unidirectional light propagation.
- Higher Cost.

Propagation Modes of Fibre Optics

- Current technology supports two modes (multimode and single mode) for propagating light along optical channels, each requiring fiber with different physical characteristics.
- Multimode can be implemented in two forms: step-index or graded-index.



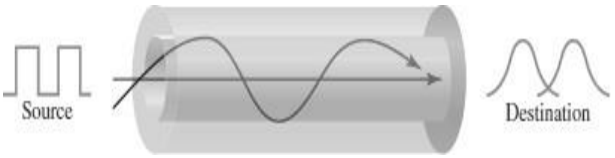
Multimode Propagation

- Multimode is so named because multiple beams from a light source move through the core in different paths.
- How these beams move within the cable depends on the structure of the core.

Multimode Step-index fiber

- In multimode step-index fiber**,** the density of the core remains constant from the center to the edges.
- A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding.
- At the interface, there is an abrupt change due to a lower density; this alters the angle of the beam's motion.
- The term *step-index* refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fiber.

Multimode Graded-index fiber



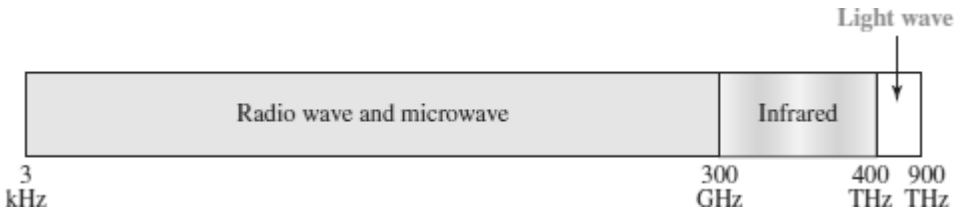
- The multimode graded-index fiber**,** decreases this distortion of the signal through the cable.
- The word *index* here refers to the index of refraction.
- The index of refraction is related to density.
- A graded index fiber, therefore, is one with varying densities.
- Density is highest at the center of the core and decreases gradually to its lowest at the edge.

Single-Mode Propagation

- Single-mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal.
- The single-mode fiber itself is manufactured with a much smaller diameter than that of multimode fiber, and with substantially lower density (index of refraction).
- The decrease in density results in a critical angle that is close enough to 90° to make the propagation of beams almost horizontal.
- In this case, propagation of different beams is almost identical, and delays are negligible. All the beams arrive at the destination "together" and can be recombined with little distortion to the signal.

UNGUIDED MEDIA

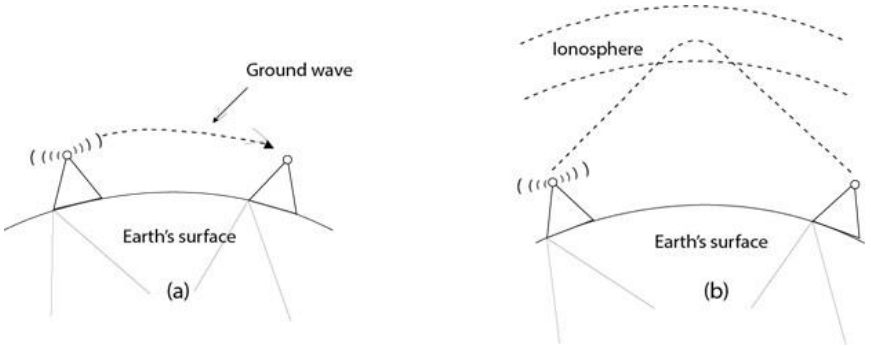
- An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**.
- In unguided media, air is the media through which the electromagnetic energy can flow easily.



- Unguided transmission is broadly classified into three categories :
  Radio Waves, Microwaves , Infrared

RADIO WAVES

- Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
- The range in frequencies of radio waves is from 3Khz to 1Khz.
- 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 waves*:**

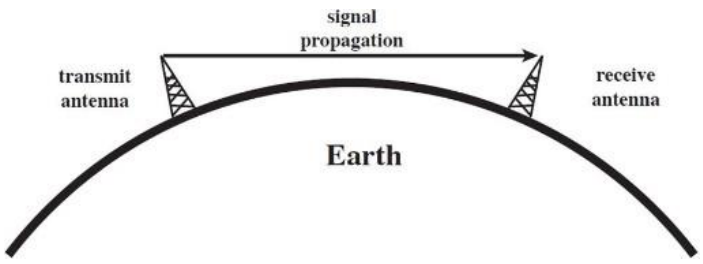
- Radio transmission is mainly used for wide area networks and mobile cellular phones.
- Radio waves cover a large area, and they can penetrate the walls.
- Radio transmission provides a higher transmission rate.

MICROWAVES

Microwaves are of two types - Terrestrial microwave & Satellite microwave

Terrestrial Microwave

- 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 focused.
- 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 at the direct sight of each other.



***Characteristics of Terrestrial 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 Terrestrial Microwave*:**

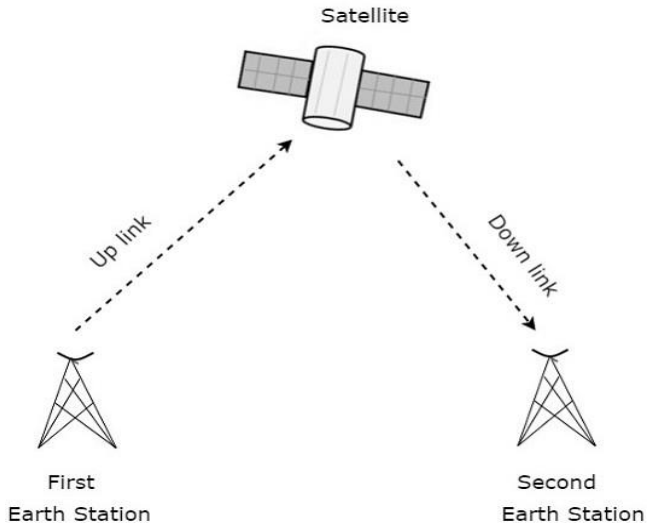
- Microwave transmission is cheaper than using cables.
- It is free from land acquisition as it does not require any land for the installation of cables.
- Microwave transmission provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task.
- Communication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

***Disadvantages of Terrestrial Microwave*:**

- Eavesdropping**.**
- Out of phase signal
- Susceptible to weather condition
- Bandwidth limited

Satellite Microwave

- 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.
- 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*:**

- 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:

- 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.

INFRARED WAVES

- An infrared transmission is a wireless technology used for communication over short ranges.
- The frequency of the infrared 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 and devices that resides in the same closed area.

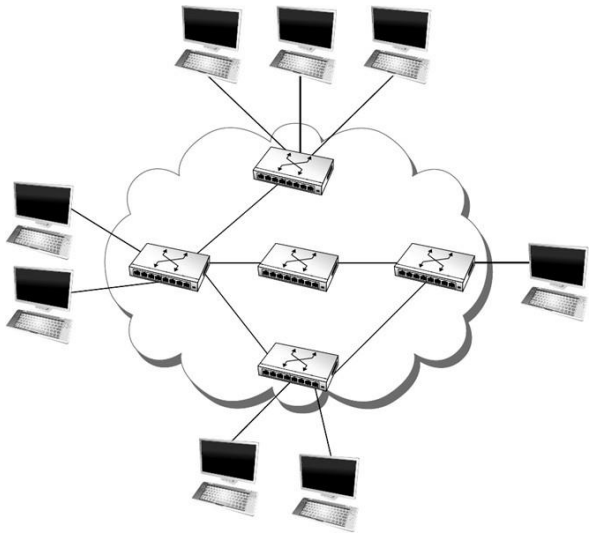
Characteristics of Infrared:

- 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.

SWITCHING

- The technique of transferring the information from one computer network to another network is known as **switching**.
- Switching in a computer network is achieved by using switches.
- A switch is a small hardware device which is used to join multiple computers together with one local area network (LAN).

- Switches are devices capable of creating temporary connections between two or more devices linked to the switch.
- Switches are used to forward the packets based on MAC addresses.
- A Switch is used to transfer the data only to the device that has been addressed. It verifies the destination address to route the packet appropriately.
- It is operated in full duplex mode.
- It does not broadcast the message as it works with limited bandwidth.



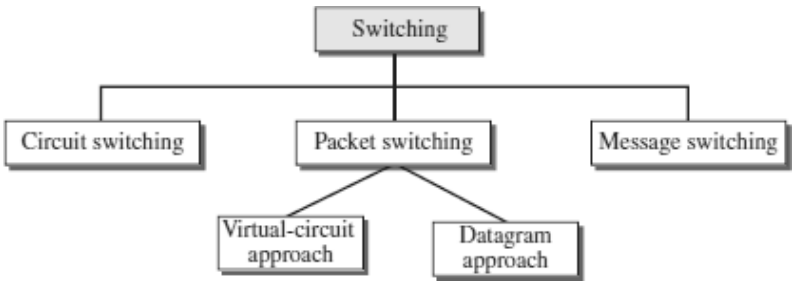
Advantages of Switching:

- Switch increases the bandwidth of the network.
- It reduces the workload on individual PCs as it sends the information to only that device which has been addressed.
- It increases the overall performance of the network by reducing the traffic on the network.
- There will be less frame collision as switch creates the collision domain for each connection.

Disadvantages of Switching:

- A Switch is more expensive than network bridges.
- A Switch cannot determine the network connectivity issues easily.
- Proper designing and configuration of the switch are required to handle multicast packets.

Types of Switching Techniques



CIRCUIT SWITCHING

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

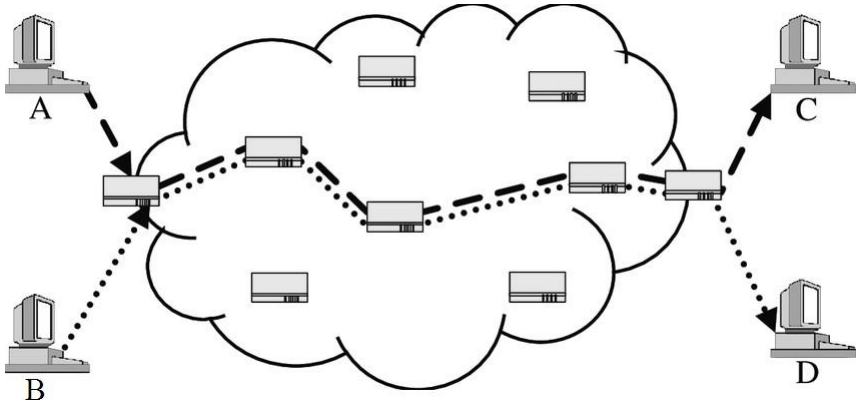
Phases in Circuit Switching

Communication through circuit switching has 3 phases:

1. ***Connection Setup / Establishment*** - In this phase, a dedicated circuit is established from the source to the destination through a number of intermediate switching centres. The sender and receiver transmits communication signals to request and acknowledge establishment of circuits.

2. ***Data transfer*** - Once the circuit has been established, data and voice are transferred from the source to the destination. The dedicated connection remains as long as the end parties communicate.

3. ***Connection teardown / Termination*** - When data transfer is complete, the connection is relinquished. The disconnection is initiated by any one of the user. Disconnection involves removal of all intermediate links from the sender to the receiver.



Advantages

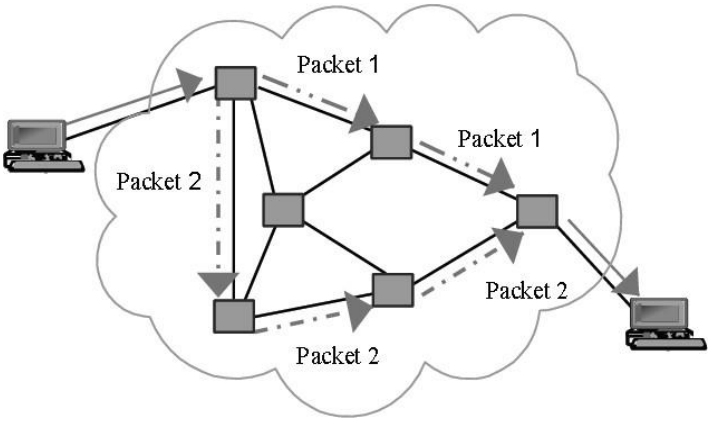
- It is suitable for long continuous transmission, since a continuous transmission route is established, that remains throughout the conversation.
- The dedicated path ensures a steady data rate of communication.
- No intermediate delays are found once the circuit is established. So, they are suitable for real time communication of both voice and data transmission.

Disadvantages

- Circuit switching establishes a dedicated connection between the end parties. This dedicated connection cannot be used for transmitting any other data, even if the data load is very low.
- Bandwidth requirement is high even in cases of low data volume.
- There is underutilization of system resources. Once resources are allocated to a particular connection, they cannot be used for other connections.
- Time required to establish connection may be high.
- It is more expensive than other switching techniques as a dedicated path is required for each connection.

PACKET SWITCHING

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



***Advantages of Packet Switching*:**

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

Disadvantages of Packet Switching:

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

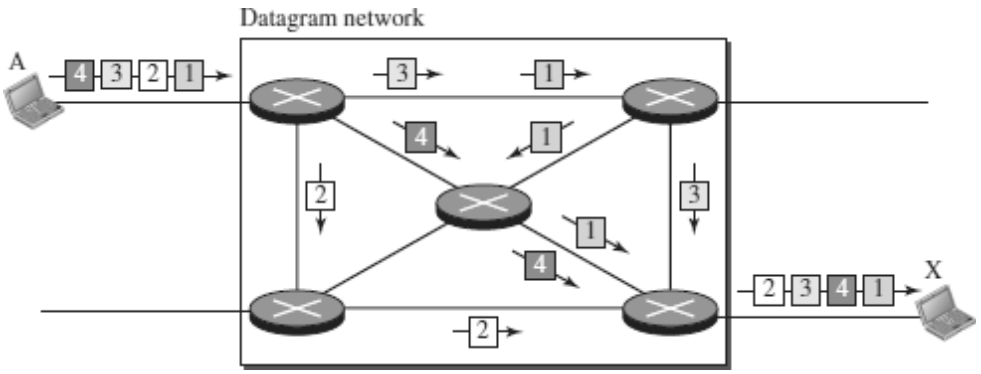
APPROACHES OF PACKET SWITCHING

There are two approaches to Packet Switching:

- Datagram Packet switching
- Virtual Circuit Switching

Datagram Packet switching

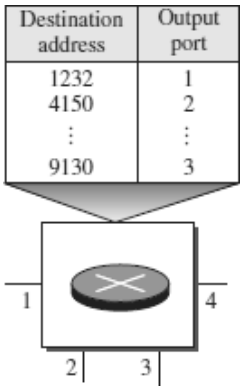
- It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity.
- Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
- The packets are reassembled at the receiving end in correct order.
- In Datagram Packet Switching technique, the path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.
- Datagram Packet Switching is also known as connectionless switching.
- There are no setup or teardown phases.
- Each packet is treated the same by a switch regardless of its source or destination.



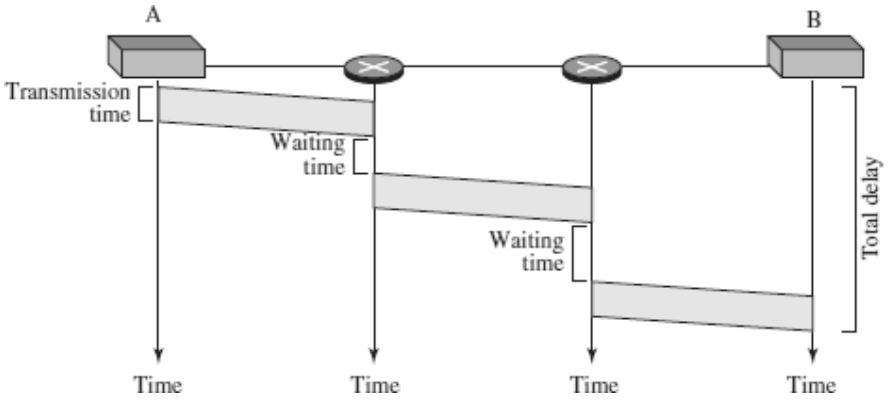
In this example, all four packets (or datagrams) belong to the same message, but may travel different paths to reach their destination.

Routing Table

In this type of network, each switch (or packet switch) has a routing table which is based on the destination address. The routing tables are dynamic and are updated periodically. The destination addresses and the corresponding forwarding output ports are recorded in the tables.



Delay in a datagram network



- The packet travels through two switches.
- There are three transmission times (3*T*),three propagation delays (slopes 3t of the lines), and two waiting times (*w*1 + *w*2).
- We ignore the processing time in each switch.

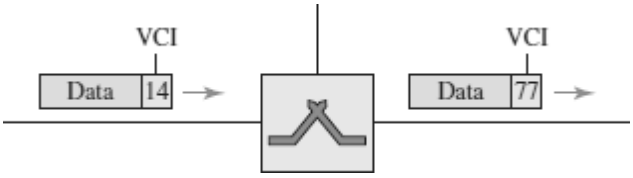
Total delay = 3*T* + 3t + *w*1 + *w*2

Virtual Circuit Switching

- Virtual Circuit Switching is also known as connection-oriented switching.
- In the case of Virtual circuit switching, a virtual connection is established before the messages are sent.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this case, the path is fixed for the duration of a logical connection.

Virtual Circuit Identifier (VCI)

A virtual circuit identifier (VCI) that uniquely identifies the connection at this switch. A VCI, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches. When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCI.



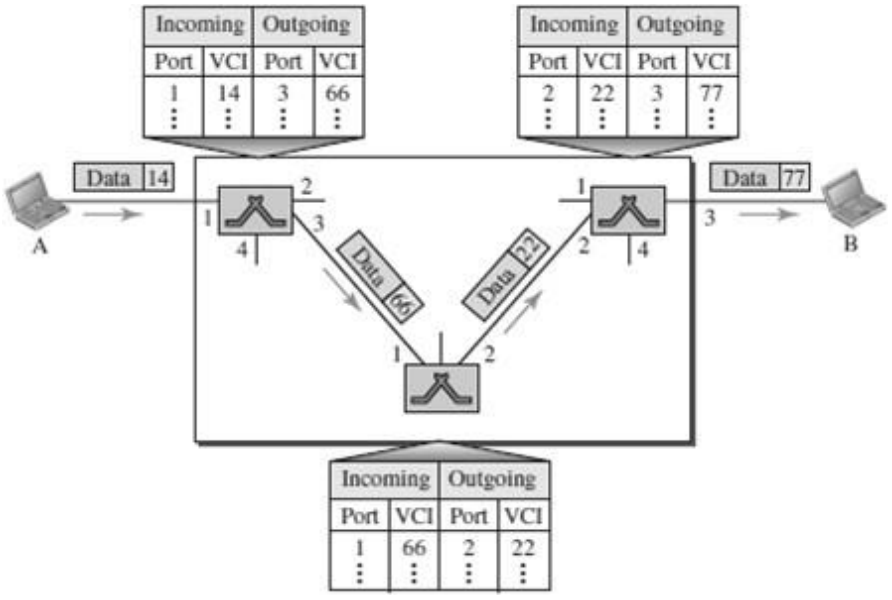
Virtual Circuit Table

Every Virtual Circuit (VC) maintains a table called Virtual Circuit table.
One entry in the VC table on a single switch contains the following :

- An incoming interface on which packets for this VC arrive at the switch
- An outgoing interface in which packets for this VC leave the switch
- A outgoing VCI that will be used for outgoing packets

Example :

Source A sends a frame to Source B through Switch 1, Switch 2 and Switch 3.



Types of Virtual Circuits

There are two broad classes of Virtual Circuits.
They are

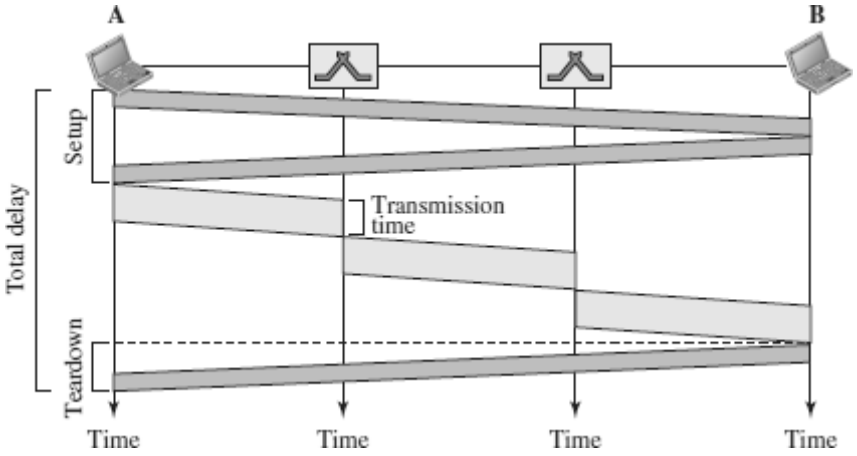
1. PVC – Permanent Virtual Circuit

- Network Administrator will configure the state
- The virtual circuit is permanent (PVC)

2. SVC – Switched Virtual Circuit

- A host can send messages into the network to cause the state to be established. This is referred as signaling.
- A host may set up and delete such a VC dynamically without the involvement of a network administrator

Delay in Virtual-Circuit Networks



- The packet is traveling through two switches (routers).
- There are three transmission times (3*T*), three propagation times (3t), data transfer depicted by the sloping lines, a setup delay (which includes transmission and propagation in two directions), and a teardown delay (which includes transmission and propagation in one direction).

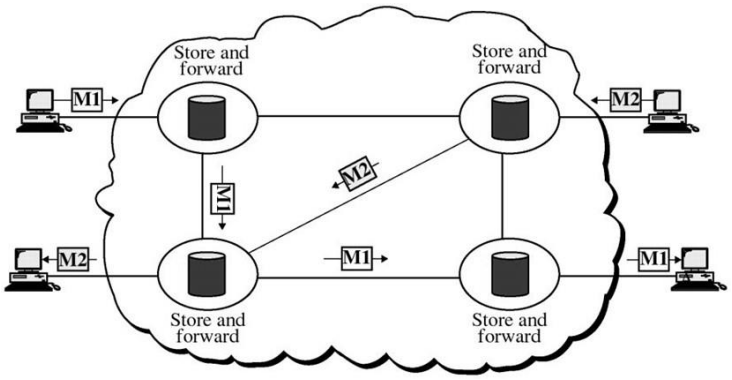
Total delay = 3*T* + 3t + Setup delay + Teardown delay

COMPARISON – CIRCUIT SWITCHING AND PACKET SWITCHING

CIRCUIT SWITCHING	PACKET SWITCHING	
	Virtual Circuit Switching	**Datagram Switching**
Connection oriented	Connection oriented	Connection less
Ensures in order delivery	Ensures in order delivery	Packets may be delivered out of order
No reordering is required	No reordering is required	Reordering is required
A dedicated path exists for data transfer	A dedicated path exists for data transfer	No dedicated path exists for data transfer
All the packets take the same path	All the packets take the same path	All the packets may not take the same path
Resources are allocated before data transfer	Resources are allocated on demand using 1st packet	No resources are allocated
Stream oriented	Packet oriented	Packet oriented
Fixed bandwidth	Dynamic Bandwidth	Dynamic bandwidth
Reliable	Reliable	Unreliable
No overheads	Less overheads	Higher overheads
Implemented at physical layer	Implemented at data link layer	Implemented at network layer
Inefficient in terms of resource utilization	Provides better efficiency than circuit switched systems	Provides better efficiency than message switched systems
Example- Telephone systems	Examples- X.25, Frame relay	Example- Internet

MESSAGE SWITCHING

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.



PROTOCOL LAYERING

- In networking, a protocol **defines the rules** that both the sender and receiver and all intermediate devices need to follow to be able **to communicate effectively**.
- A protocol provides a communication service that the process use to exchange messages.
- When communication is simple, we may need only one simple protocol.
- When the communication is complex, we may need to divide the task between different layers, in which case we need a protocol at each layer, or **protocol layering.**
- Protocol layering is that it allows us to separate the services from the implementation.
- A layer needs to be able to receive a set of services from the lower layer and to give the services to the upper layer.
- Any modification in one layer will not affect the other layers.

Basic Elements of Layered Architecture

- **Service:** It is a set of actions that a layer provides to the higher layer.
- **Protocol:** It defines a set of rules that a layer uses to exchange the information with peer entity. These rules mainly concern about both the contents and order of the messages used.
- **Interface:** It is a way through which the message is transferred from one layer to another layer.

Features of Protocol Layering

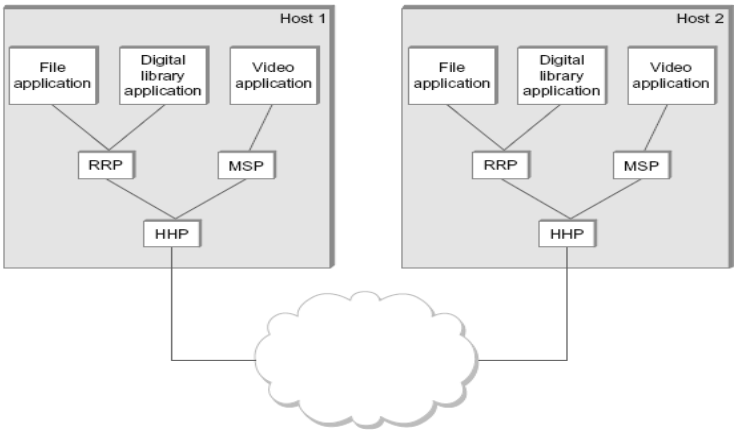
1. **It decomposes the problem of building a network** into more manageable components.
2. **It provides a more modular design**.

Principles of Protocol Layering

1. The first principle dictates that if we want bidirectional communication, we need to make each layer so that it is able to perform two opposite tasks, one in each direction.
2. The second principle that we need to follow in protocol layering is that the two objects under each layer at both sites should be identical.

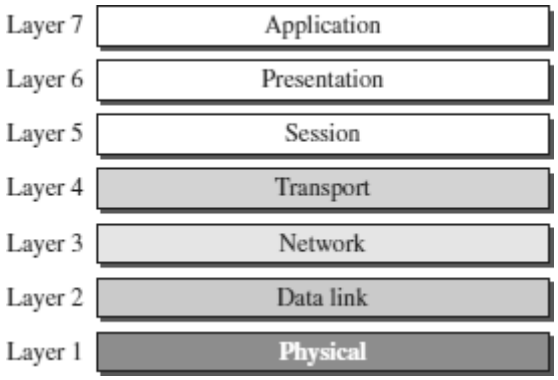
Protocol Graph

- The set of protocols that make up a network system is called a **protocol graph**.
- The nodes of the graph correspond to protocols, and the edges represent a dependence relation.
- For example, the Figure below illustrates a protocol graph consists of protocols ***RRP (Request/Reply Protocol)*** and ***MSP (Message Stream Protocol)*** implement two different types of process-to-process channels, and both depend on the ***HHP (Host-to- Host Protocol)*** which provides a host-to-host connectivity service



OSI MODEL

- OSI stands for **Open System Interconnection.**
- It is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.



ORGANIZATION OF THE OSI LAYERS

The OSI model is divided into two layers: **upper layers and lower layers**.

UPPER LAYERS

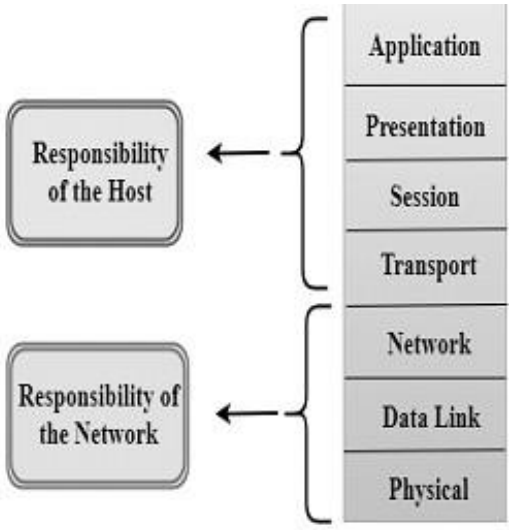
(Responsibility of the Host)

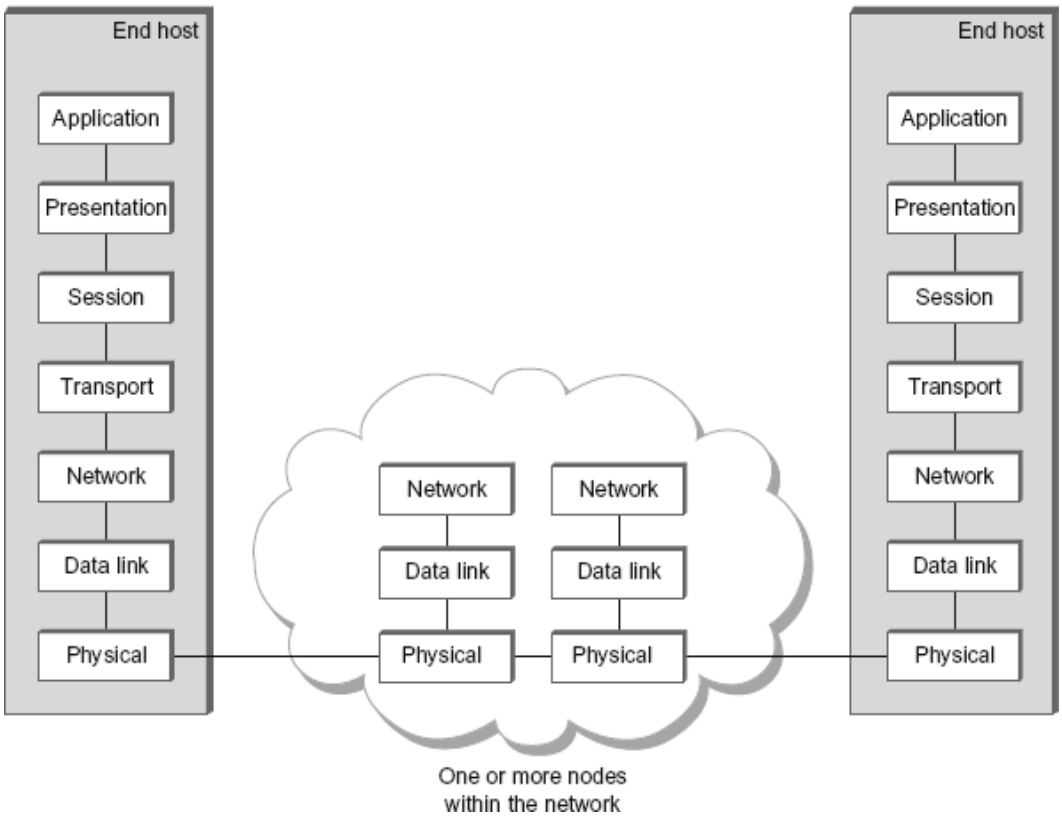
The upper layers of the OSI model mainly deals with the application related issues. They are implemented only in the software.

LOWER LAYERS

(Responsibility of the Network)

The lower layers of the OSI model deals with the data transport issues. They are implemented in hardware and software.





FUNCTIONS OF THE OSI LAYERS

1. PHYSICAL LAYER

The physical layer coordinates the functions required to **transmit a bit stream over a physical medium.**
The physical layer is concerned with the following functions:

- **Physical characteristics of interfaces and media -** The physical layer defines the characteristics of the interface between the devices and the transmission medium.
- **Representation of bits -** To transmit the stream of bits, it must be encoded to signals. The physical layer defines the type of encoding.
- **Signals:** It determines the type of the signal used for transmitting the information.
- **Data Rate or Transmission rate -** The number of bits sent each second –is also defined by the physical layer.
- **Synchronization of bits -** The sender and receiver must be synchronized at the bit level. Their clocks must be synchronized.
- **Line Configuration -** In a point-to-point configuration, two devices are connected together through a dedicated link. In a multipoint configuration, a link is shared between several devices.
- **Physical Topology -** The physical topology defines how devices are connected to make a network. Devices can be connected using a mesh, bus, star or ring topology.

- **Transmission Mode -** The physical layer also defines the direction of transmission between two devices: simplex, half-duplex or full-duplex.

2. DATA LINK LAYER

It is responsible for **transmitting frames from one node to the next node**.
The other responsibilities of this layer are

- **Framing -** Divides the stream of bits received into data units called frames.
- **Physical addressing** – If frames are to be distributed to different systems on the network , data link layer adds a header to the frame to define the sender and receiver.
- **Flow control**- If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender ,the Data link layer imposes a flow ctrl mechanism.
- **Error control**- Used for detecting and retransmitting damaged or lost frames and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.
- **Medium Access control** -Used to determine which device has control over the link at any given time.

3. NETWORK LAYER

This layer is responsible for the **delivery of packets from source to destination**.
It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
The other responsibilities of this layer are

- **Logical addressing -** If a packet passes the network boundary, we need another addressing system for source and destination called logical address. This addressing is used to identify the device on the internet.
- **Routing** – Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.

4. TRANSPORT LAYER

It is responsible for **Process to Process** delivery. That is responsible for source-to-destination (end-to-end) delivery of the entire message, It also ensures whether the message arrives in order or not.
The other responsibilities of this layer are

- **Port addressing / Service Point addressing** - The header includes an address called port address / service point address. This layer gets the entire message to the correct process on that computer.
- **Segmentation and reassembly** - The message is divided into segments and each segment is assigned a sequence number. These numbers are arranged correctly on the arrival side by this layer.

- **Connection control** - This can either be **connectionless or connection oriented.**
  - The connectionless treats each segment as an individual packet and delivers to the destination.
  - The connection-oriented makes connection on the destination side before the delivery. After the delivery the termination will be terminated.
- **Flow control** - The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error Control -** Error control is performed end-to-end rather than across the single link..

5. SESSION LAYER

This layer **establishes, manages and terminates connections between applications**. The other responsibilities of this layer are

- **Dialog control** - Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
- **Synchronization**- Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

6. PRESENTATION LAYER

It is concerned with the **syntax and semantics of information exchanged between two systems.**
The other responsibilities of this layer are

- **Translation** – Different computers use different encoding system, this layer is responsible for interoperability between these different encoding methods. It will change the message into some common format.
- **Encryption and decryption**-It means that sender transforms the original information to another form and sends the resulting message over the n/w. and vice versa.
- **Compression and expansion**-Compression reduces the number of bits contained in the information particularly in text, audio and video.

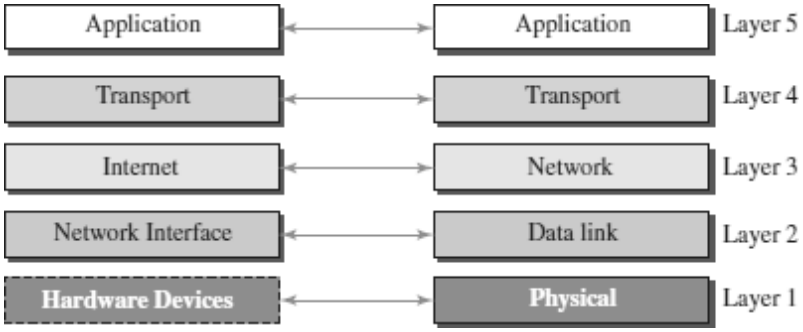
7. APPLICATION LAYER

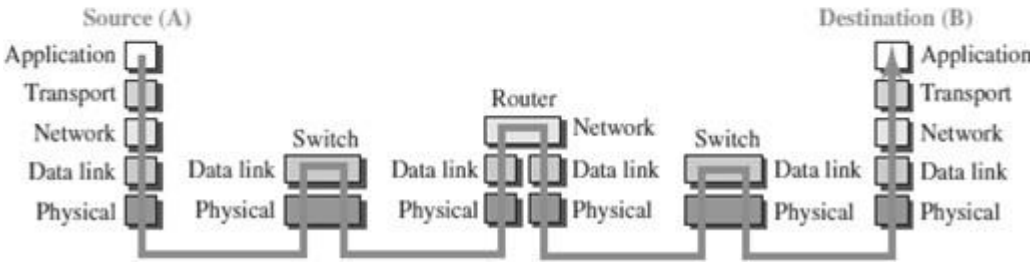
This layer **enables the user to access the network**. It handles issues such as network transparency, resource allocation, etc. This allows the user to log on to remote user.
The other responsibilities of this layer are

- **FTAM (File Transfer, Access, Management) -** Allows user to access files in a remote host.
- **Mail services** - Provides email forwarding and storage.
- **Directory services** - Provides database sources to access information about various sources and objects.

TCP / IP PROTOCOL SUITE

- The TCP/IP architecture is also called as Internet architecture.
- It is developed by the US Defense Advanced Research Project Agency (**DARPA**) for its packet switched network (**ARPANET**).
- TCP/IP is a protocol suite used in the Internet today.
- It is a 4-layer model. The layers of TCP/IP are
  1. **Application layer**
  2. **Transport Layer (TCP/UDP)**
  3. **Internet Layer**
  4. **Network Interface Layer**





APPLICATION LAYER

- An application layer incorporates the function of top three OSI layers. An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- Protocols such as FTP, HTTP, SMTP, POP3, etc running in the application layer provides service to other program running on top of application layer

TRANSPORT LAYER

- The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.
- The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.
  - **UDP** – UDP provides connectionless service and end-to-end delivery of transmission. It is an unreliable protocol as it discovers the errors but not specify the error.
  - **TCP** – TCP provides a full transport layer services to applications. TCP is a reliable protocol as it detects the error and retransmits the damaged frames.

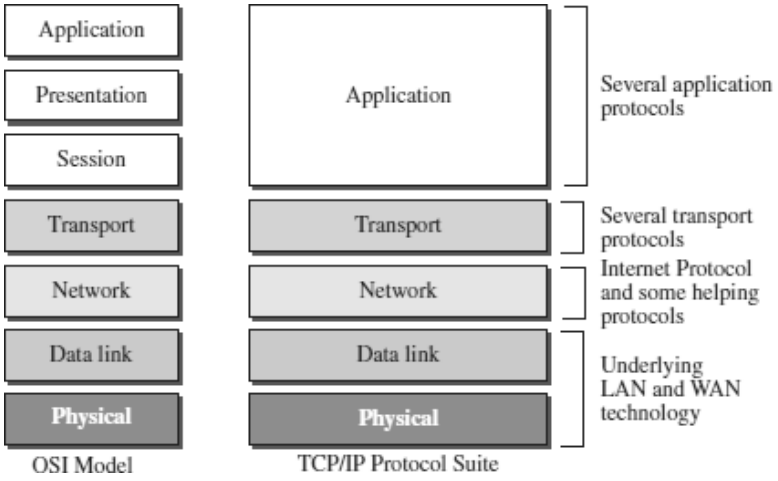
INTERNET LAYER

- The internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.
- Internet layer handle the transfer of information across multiple networks through router and gateway .
- IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

NETWORK INTERFACE LAYER

- The network interface layer is the lowest layer of the TCP/IP model.
- This layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are Ethernet, token ring, FDDI, X.25, frame relay.

COMPARISON - OSI MODEL AND TCP/IP MODEL



S.No	OSI MODEL	TCP/IP MODEL
1	Defined before advent of internet	Defined after the advent of Internet.
2	Service interface and protocols are clearly distinguished before	Service interface and protocols were not clearly distinguished before
3	Internetworking not supported	TCP/IP supports Internet working
4	Strict layering	Loosely layered
5	Protocol independent standard	Protocol Dependant standard
6	Less Credible	More Credible
7	All packets are reliably delivered	TCP reliably delivers packets, IP does not reliably deliver packets

NETWORK PERFORMANCE

Network performance is measured in using:

Bandwidth, Throughput, Latency, Jitter, RoundTrip Time

BANDWIDTH

- The bandwidth of a network is given by the number of bits that can be transmitted over the network in a certain period of time.
- Bandwidth can be measured in two different values: bandwidth in hertz and bandwidth in bits per second.

Bandwidth in Hertz

- Bandwidth in hertz refers to the range of frequencies contained in a composite signal or the range of frequencies a channel can pass.
- For example, we can say the bandwidth of a subscriber telephone line is 4 kHz.

Bandwidth in Bits per Seconds

- Bandwidth in Bits per Seconds refers to the number of bits transmitted per second.
- For example, the bandwidth of a network is a maximum of 100 Mbps. This means that this network can send 100 Mbps.

Relationship

- There is an explicit relationship between the bandwidth in hertz and bandwidth in bits per second.
- Basically, an increase in bandwidth in hertz means an increase in bandwidth in bits per second.

THROUGHPUT

- Throughput is a measure of how fast we can actually send data through a network.
- Bandwidth in bits per second and throughput may seem to be same, but they are different.
- A link may have a bandwidth of *B* bps, but we can only send *T* bps through this link. (*T* always less than *B).*
- In other words, the bandwidth is a potential measurement of a link; the throughput is an actual measurement of how fast we can send data.
- For example, we may have a link with a bandwidth of 1 Mbps, but the devices connected to the end of the link may handle only 200 kbps. This means that we cannot send more than 200 kbps through this link.

Problem :

A network with bandwidth of 10 Mbps can pass only an average of 12,000 frames per minute with each frame carrying an average of 10,000 bits. What is the throughput of this network?

Solution

We can calculate the throughput as

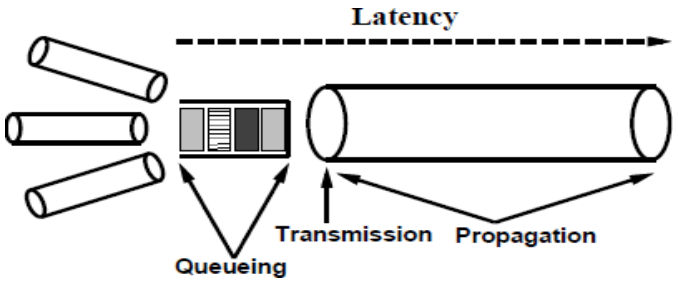
$$\text{Throughput} = (12{,}000 \times 10{,}000) / 60 = 2 \text{ Mbps}$$

The throughput is almost one-fifth of the bandwidth in this case.

LATENCY (DELAY)

- The latency or delay defines how long it takes for an entire message to travel from one end of a network to the other.
- Latency is made up of four components: Propagation time, Transmission time, Queuing time and Processing delay.

Latency = Propagation Time + Transmission time + Queuing time + Processing delay



Propagation Time

- Propagation time measures the time required for a bit to travel from the source to the destination.
- The propagation time is calculated by dividing the distance by the propagation speed.
- The propagation speed of electromagnetic signals depends on the medium and on the frequency of the signal.

$$Propagation\ time = Distance / Propagation\ Speed$$

Transmission Time

- In data communications we don't send just 1 bit, we send a message.
- The first bit may take a time equal to the propagation time to reach its destination.
- The last bit also may take the same amount of time.
- However, there is a time between the first bit leaving the sender and the last bit arriving at the receiver.
- The first bit leaves earlier and arrives earlier.
- The last bit leaves later and arrives later.
- The transmission time of a message depends on the size of the message and the bandwidth of the channel.

$$Transmission\ time = (Message\ size) / Bandwidth$$

Queuing Time

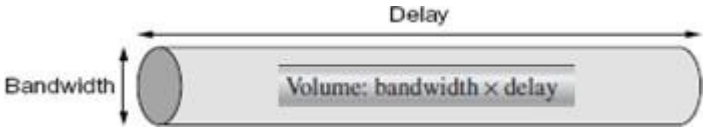
- Queuing time is the time needed for each intermediate or end device to hold the message before it can be processed.
- The queuing time is not a fixed factor. It changes with the load imposed on the network. When there is heavy traffic on the network, the queuing time increases.
- An intermediate device, such as a router, queues the arrived messages and processes them one by one.
- If there are many messages, each message will have to wait.

Processing Delay

- Processing delay is the time that the nodes take to process the packet header.
- Processing delay is a key component in network delay.
- During processing of a packet, nodes may check for bit-level errors in the packet that occurred during transmission as well as determining where the packet's next destination is.

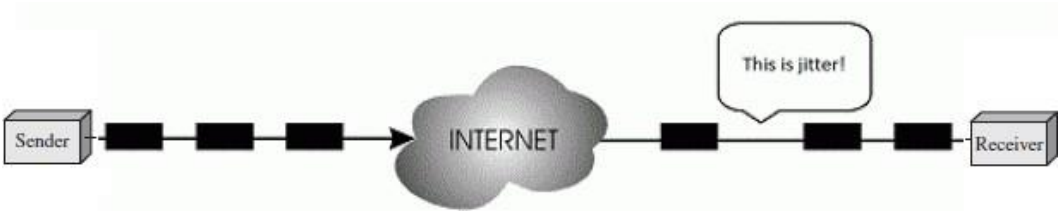
Bandwidth - Delay Product

- Bandwidth and delay are two performance metrics of a link.
- **The bandwidth-delay product defines the number of bits that can fill the link.**
- This measurement is important if we need to send data in bursts and wait for the acknowledgment of each burst before sending the next one.



JITTER

- Another performance issue that is related to delay is jitter**.**
- Jitter is a problem that if different packets of data encounter different delays and the application using the data at the receiver site is time-sensitive (audio and video data, for example).
- If the delay for the first packet is 20 ms, for the second is 45 ms, and for the third is 40 ms, then the real-time application that uses the packets endures jitter.



ROUND-TRIP TIME (RTT)

- RTT refers to how long it takes to send a message from one end of a network to the other and back, rather than the one-way latency. This is called as *round-trip time* (RTT) of the network.

SOLVED PROBLEMS – PERFORMANCE

Problem 1:

What is the propagation time if the distance between the two points is 12,000 km? Assume the propagation speed to be 2.4×10^8 m/s .

Solution :

Propagation time = (12000 * 1000) / (2.4×10^8) = 50 ms

Problem 2:

What are the propagation time and the transmission time for a 2.5-KB (kilobyte) message (an email) if the bandwidth of the network is 1 Gbps? Assume that the distance between the sender and the receiver is 12,000 km and that light travels at $2.4 * 10^8$ m/s.

Solution:

Propagation time = (12000 * 1000) / ($2.4 * 10^8$) = 50 ms
Transmission time = (2500 * 8) / 10^9 = 0.02 ms

Problem 3:

What are the propagation time and the transmission time for a 5-MB (megabyte) message (an image) if the bandwidth of the network is 1 Mbps? Assume that the distance between the sender and the receiver is 12,000 km and that light travels at $2.4 * 10^8$m/s.

Solution:

Propagation time = (12000 * 1000) / ($2.4 * 10^8$) = 50 ms
Transmission time = (5000000 * 8) / 10^6 = 40 s