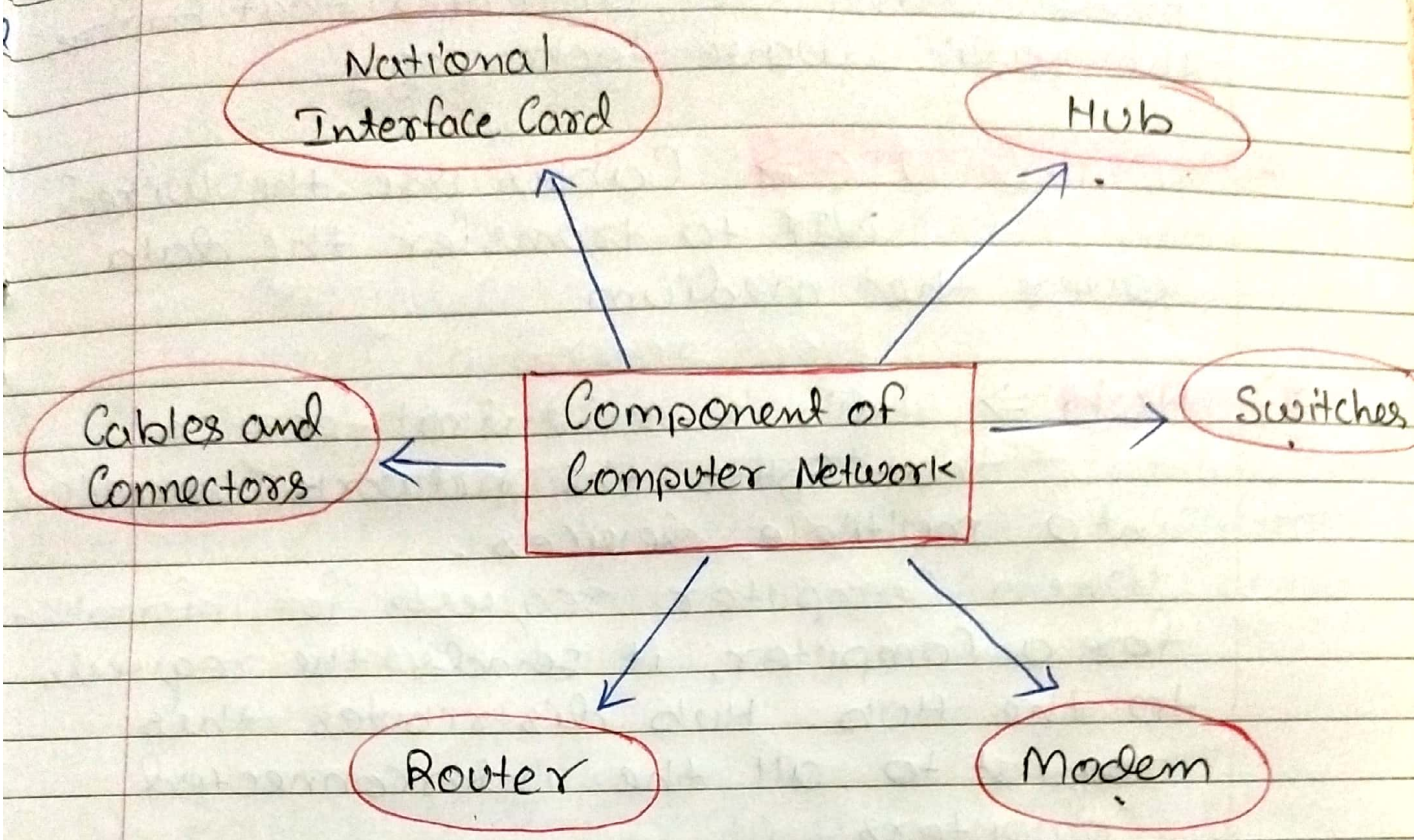
Computer Network

Computer Network ⇒ • Computer Network refers to interconnected Computing devices that can exchange data and share resources with each other.

- Computer Network is a group of Computers Connected with each other through wires, optical fibres or optical links so that various devices can interact with each other through a network.
- A Computer Network is a System in which multiple Computers are connected to each other to share information and resources.
- A Computer network is a set of Computers sharing resources located on or provided by Network nodes. The Computers use common Communication protocols over digital interconnections to Communicate with each other.
- A Computer Network is defined as a system that connets two or more Computing devices for transmitting and sharing information.

Components of Computer Network:



1) NIC (National Interface Card) ⇒

NIC is a device that helps the computer to communicate with another device.

The network interface card contains the hardware addresses, the data-link layer protocol use this address to identify the system on the network so that it transfers the data to the correct destination.

There are two types of NIC.

1) **Wireless NIC** ⇒ All the modern laptops use the wireless NIC.

in wireless NIC, a connection is made using the antenna that employs the radio wave technology.

2) **Wired NIC** ⇒ Cables use the wired NIC to transfer the data over the medium.

2) **Hub** ⇒ Hub is a central device that splits the network connection into multiple devices.
When computer requests for information for a computer, it sends the requests to the Hub. Hub distributes this request to all the interconnected computers.

3) **Switches** ⇒ Switch is a networking device that groups all the devices over the network to transfer the data to another device.
A switch is better than Hub as it does not broadcast the message over the network. Such as it sends the message to the device for which is belongs to.

4) **Cables and Connectors** ⇒ Cables is a transmission media that transmits the communication signals.

There are three types of cables:

1) Twisted pair cable ⇒ It is a high-speed cable that transmits the data over 1GbPS or more.

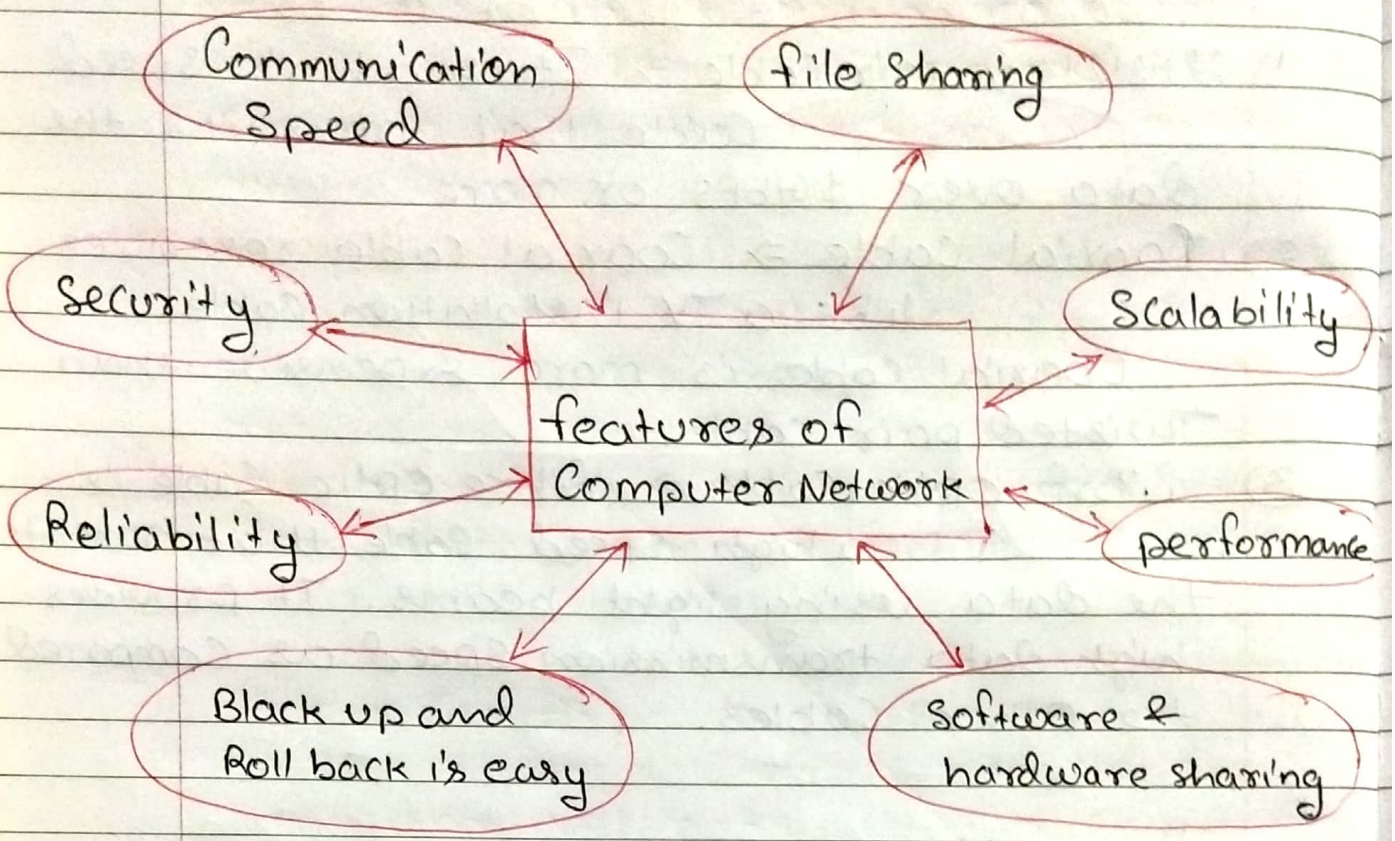
2) Coaxial cable ⇒ Coaxial cable resembles like a TV installation cable.
Coaxial cable is more expensive than Twisted pair cable.

3) fibre optic cable ⇒ fibre optic cable is a high-speed cable that transmits the data using light beams. It provides high data transmission speed as compared to other cables.

5) Router ⇒ Router is a device that connects the LAN to the internet. the router is mainly used to connect the distinct networks or connect the internet to multiple Computers.

6) Modem ⇒ Modem Connects the Computer to the internet over the Existing telephone line.
A modem is not integrated with the Computer motherboard.
A modem is a separate part on the PC Slot found on the motherboard.

features of Computer network



1) **Communication Speed** ⇒ Network provides us to Communicate over the network in a fast and efficient manner.
for Ex ⇒ we can do video Conferencing, email messaging etc. over the internet. The Computer network is a great way to share our knowledges and ideas.

2) **file sharing** ⇒ One of the most important features of a Computer Network is that with their help you can Easily share the files Between Different Systems that are Connected with Each other

through transmission media.

3) **Scalability** ⇒ The Scalability of a Computer network simply means that we can add new nodes or components of the network easily. Any computer network must be scalable so we can extend it easily by adding new nodes. After adding new nodes to the network the speed of connection decreases which leads to a decrease in the speed of transmission of data.

4) **Performance** ⇒ The performance of a Computer network is measured using response time and with the help of the speed of data transmission. For better performance the response time of sending and receiving data from one node to another should be minimum.

5) **Software and hardware sharing** ⇒ We can install the application on the main server, therefore the user can access the applications centrally. So, we do not need to install the software on every machine, similarly, hardware can also be shared.

6) **Back up and Roll back is easy** ⇒ Since the files

are stored in the main server which is centrally located. Therefore, it is easy to take the back up from the main server.

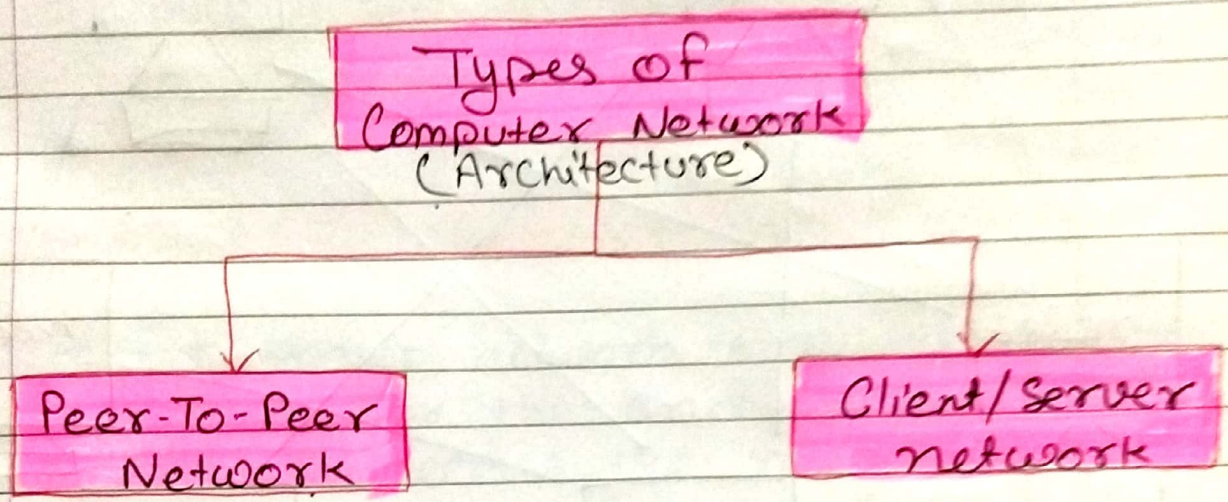
7) **Reliability** ⇒ With the help of Computer Networks there are fewer chances for the occurrence of failure and in case if there is any failure then recovery is fast.

8) **Security** ⇒ Security is one of the main characteristics of Computer Networks, Thus a computer network should be secure so that the data transmitting over the network should be safe from any unauthorized access, the data send by the sending node should be received as it is at the receiving node, which simply means there should be no loss of data during the transmission of the data.

Computer Network Architecture

Computer Network Architecture is defined as the physical and logical design of the Software, hardware, protocols and media of transmission of data.

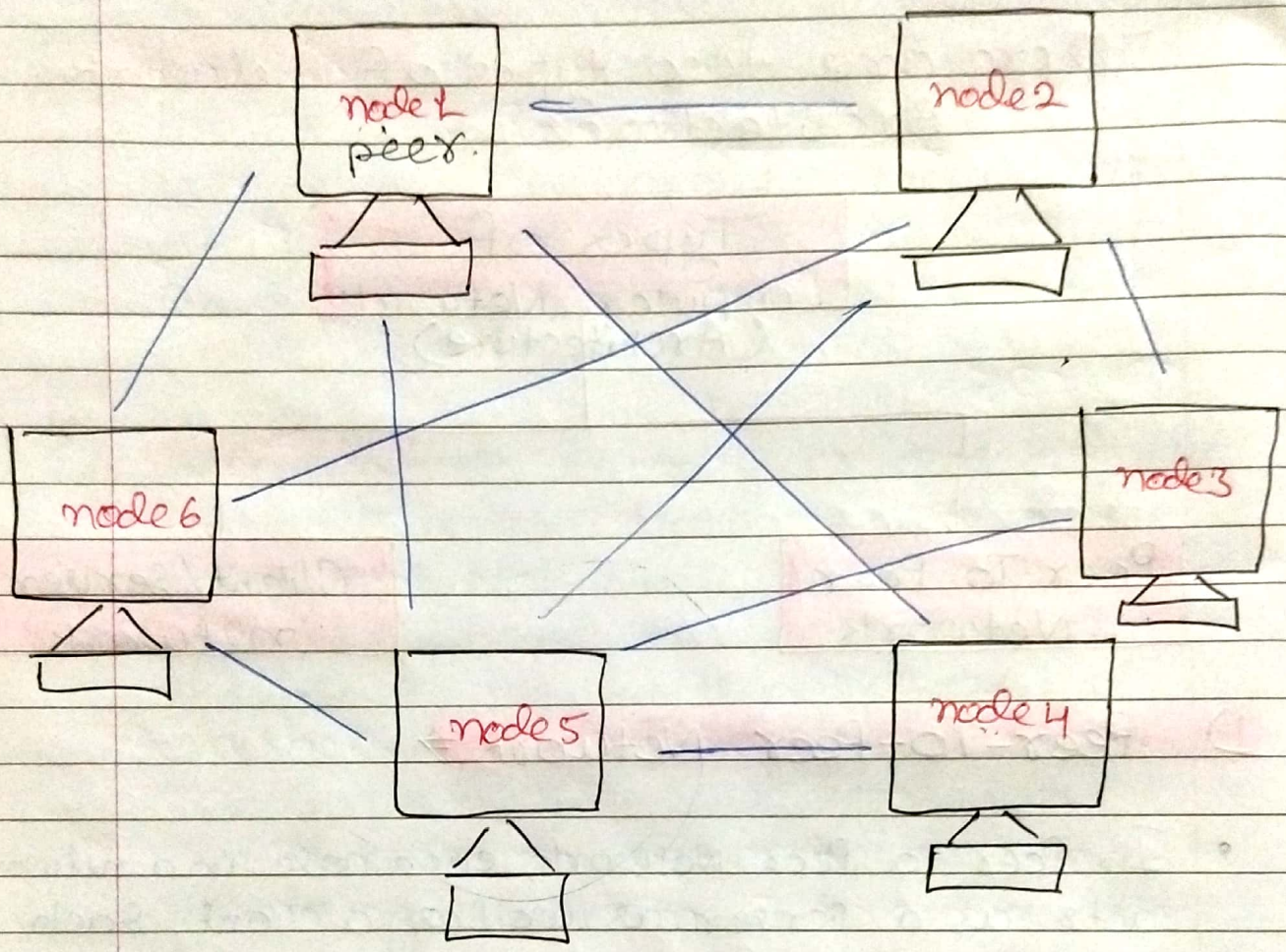
There are two types of network Architectures.



1) Peer-To-Peer Network ⇒

- In Peer to Peer Network, each node in a network acts as a server as well as a client Each node on network is known as a peer.
- There are no dedicated servers required to provide services to the clients.
- Peer-to-Peer network is useful for small environments, usually upto 10 Computers.
- 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.

- Each node is capable of requesting services and can also provide the server to other nodes.



Advantages of Peer-To-Peer Network:

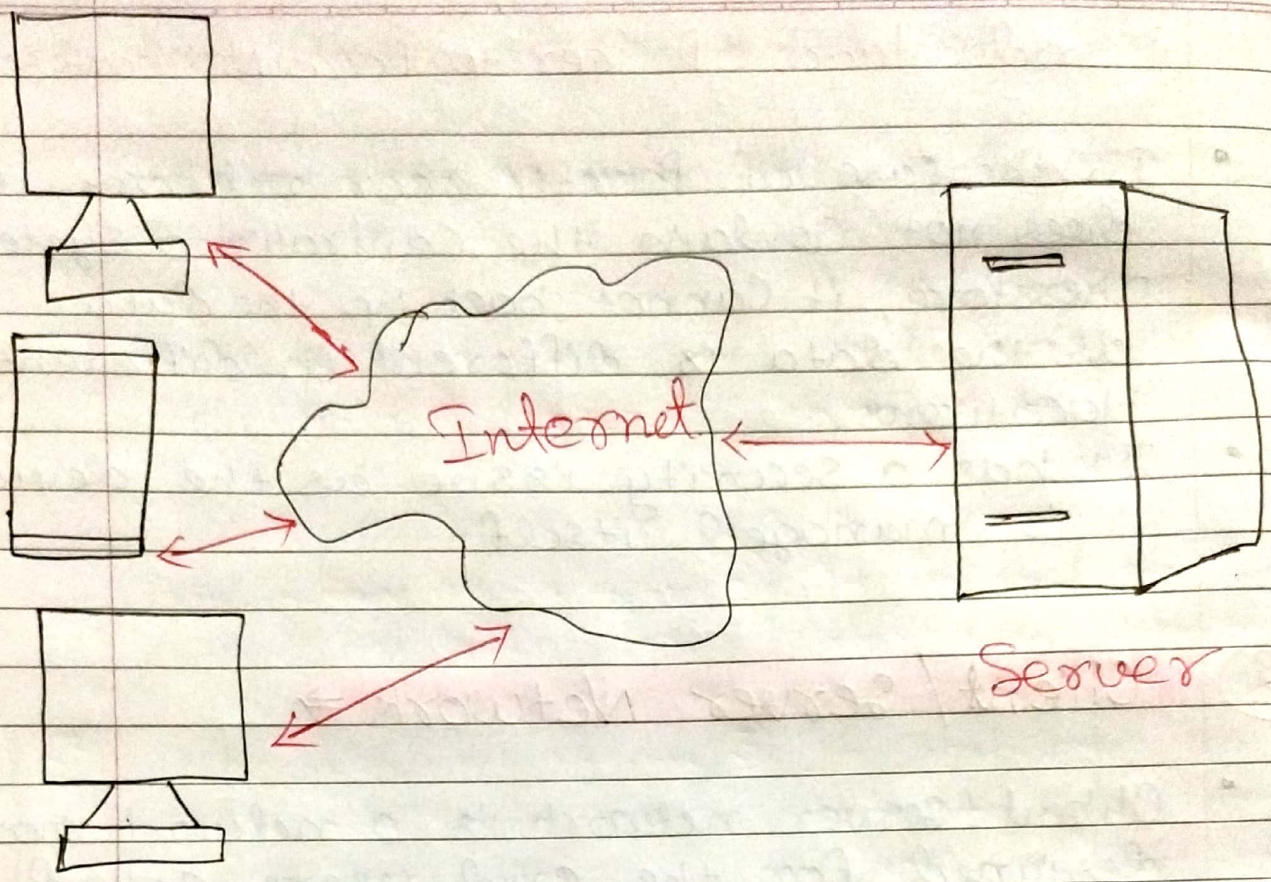
- It is less costly as it does not contain any dedicated server.
- if one computer stops working but, other computers will not stop working.
- It is easy to set up and maintain as each computer manages itself.

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.

2) 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.
- All the Clients Communicate with each other through a server.
- Suitable for a Larger network.



Advantages of Client/server network:

- A Client/server network Contains the Centralized System. Therefore we can backup 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:

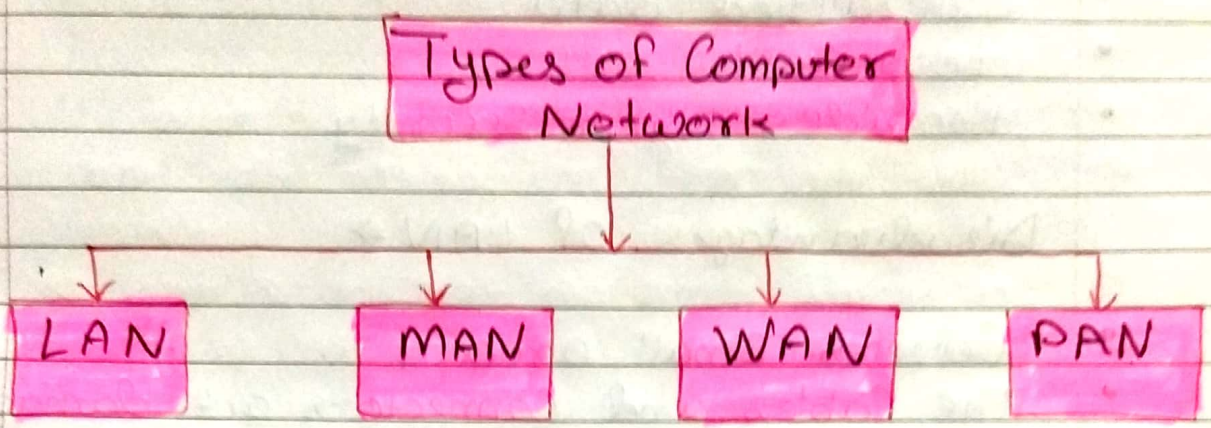
- Client/Server network is expensive as it requires the server with large memory.
- A server has a Network Operating System (NOS) to provide the resources to the clients, but the cost of NOS is very high.
- It requires a dedicated network administrator to manage all the resources

Difference between Peer-to-Peer and Client server network.

Peer-to-Peer Network	Client-server Network
1) The peer-to-peer network model is distributed and decentralized nature.	1) The Client-server network model is also distributed in nature but it is Centralized.
2) Peer-to-Peer Network focuses on Connectivity.	2) It focuses on information sharing.
3) In peer-to-peer Network, Clients and Server are not differentiated.	3) In Client-server Network, Clients and server are differentiated, Specific server and Clients are present.
4) Peer-to-Peer Network are less Stable if number of peer is increase.	4) Client-Server Network are more Stable than Peer-to-Peer Network.
5) Peer-to-Peer Network Each peer has its own data	5) Client-server Network, Centralized server is used to store the data.
6) Peer-to-Peer is less Expensive to implement	6) Client-Server network is more Expensive to implement.

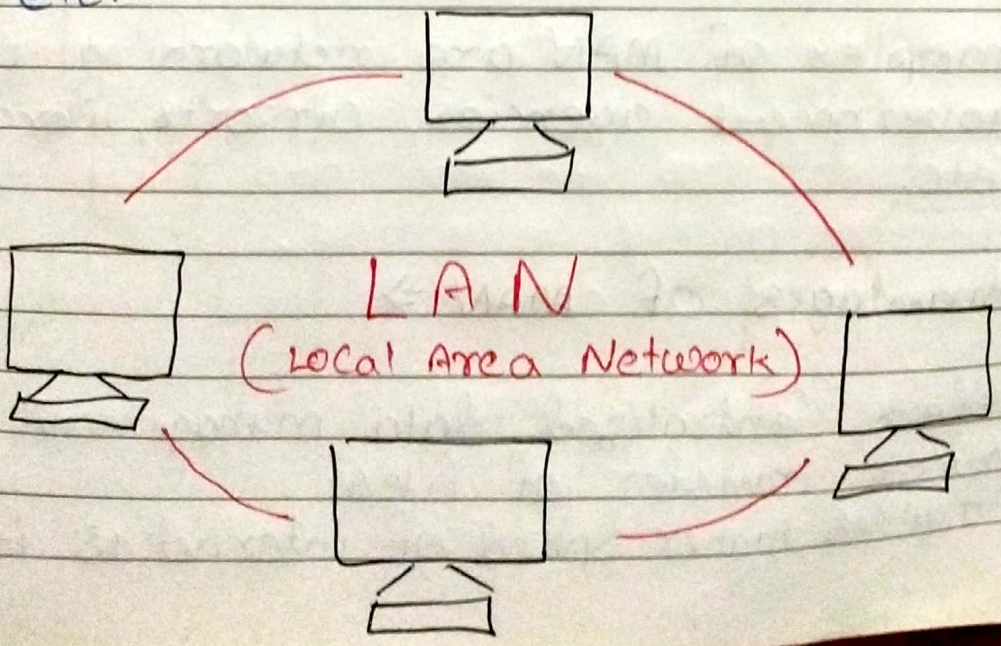
Types of Computer Network

A Computer network can be categorized by their size. A Computer Network is mainly of four types:



1) **LAN** (Local Area Network) ⇒

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



Advantages of LAN ⇒

- High data transfer rate
- Ease of setup
- Centralized data
- Low cost
- Provides higher security

Disadvantages of LAN ⇒

- Covers small area
- The cables and connectors get damaged easily.
- Requires administrative time.

2) MAN (Metropolitan Area Network) ⇒

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a large Network.

- Examples of MAN are networking in government agencies, airports, libraries etc.

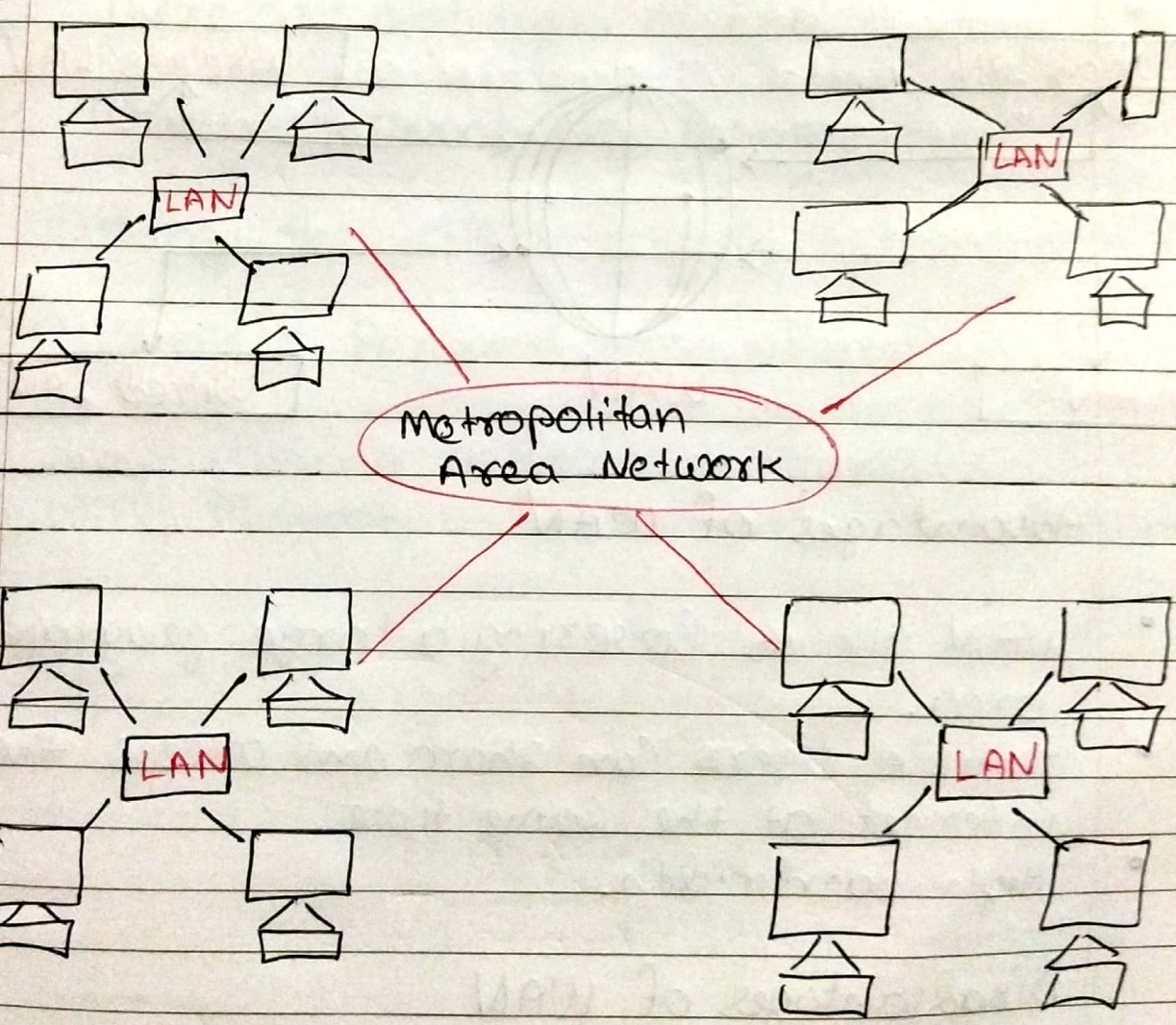
Advantages of MAN ⇒

- offers Centralized data management.
- Quick transfer of files
- Provides higher speed of internet as it

Uses fiber optics.

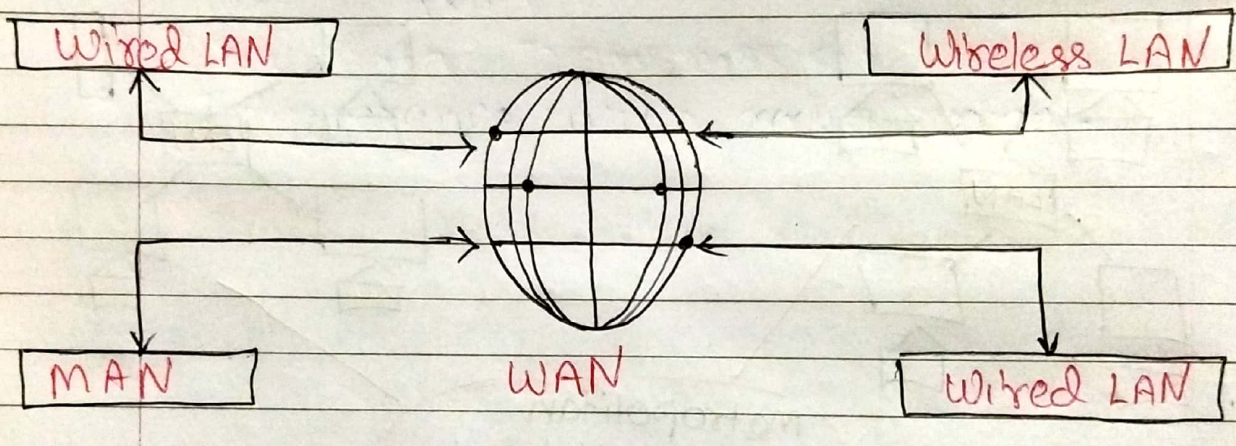
Disadvantages of MAN ⇒

- Difficult to handle due to large network size.
- Risk of hacking
- High installation cost as it requires fiber optics.



3) WAN (Wide Area Network) ⇒

- WAN is a types of Computer Network that Connects Computers over a Large geographical distance through a Shared Communication path.
- WAN Network Could be an interConnection between two or more LANs which are Connected through telephone lines or radio waves.



Advantages of WAN

- WAN allows Covering a Large geographical area.
- Multiple users Can share and access the internet at the Same time.
- High Bandwidth.

Disadvantages of WAN

- High initial investment Cost.

- Hard to handle as the network is vast and complex
- Less secure.

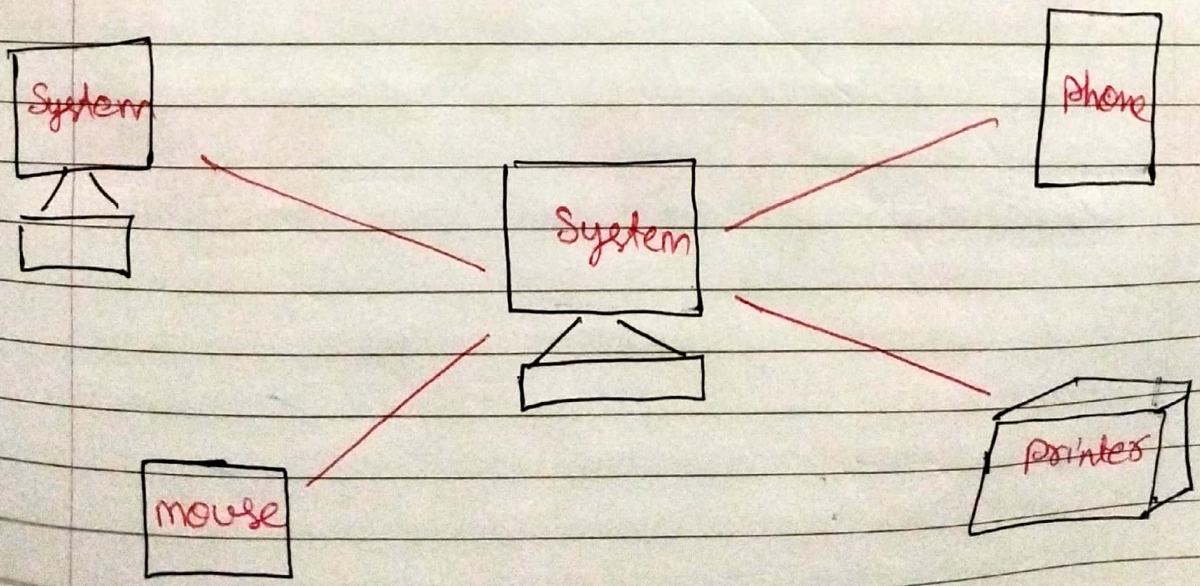
4) **PAN** (Personal Area Network) ⇒

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- It is the smallest and most basic type of computer network.

There are two types of PAN

1) Wired Personal Area Network :⇒ WPAN is created by using the USB.

2) Wireless Personal Area Network :⇒ WPAN is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.



Example of PAN are ⇒ USB, Computer, Bluetooth, etc.

Advantages of PAN are ⇒

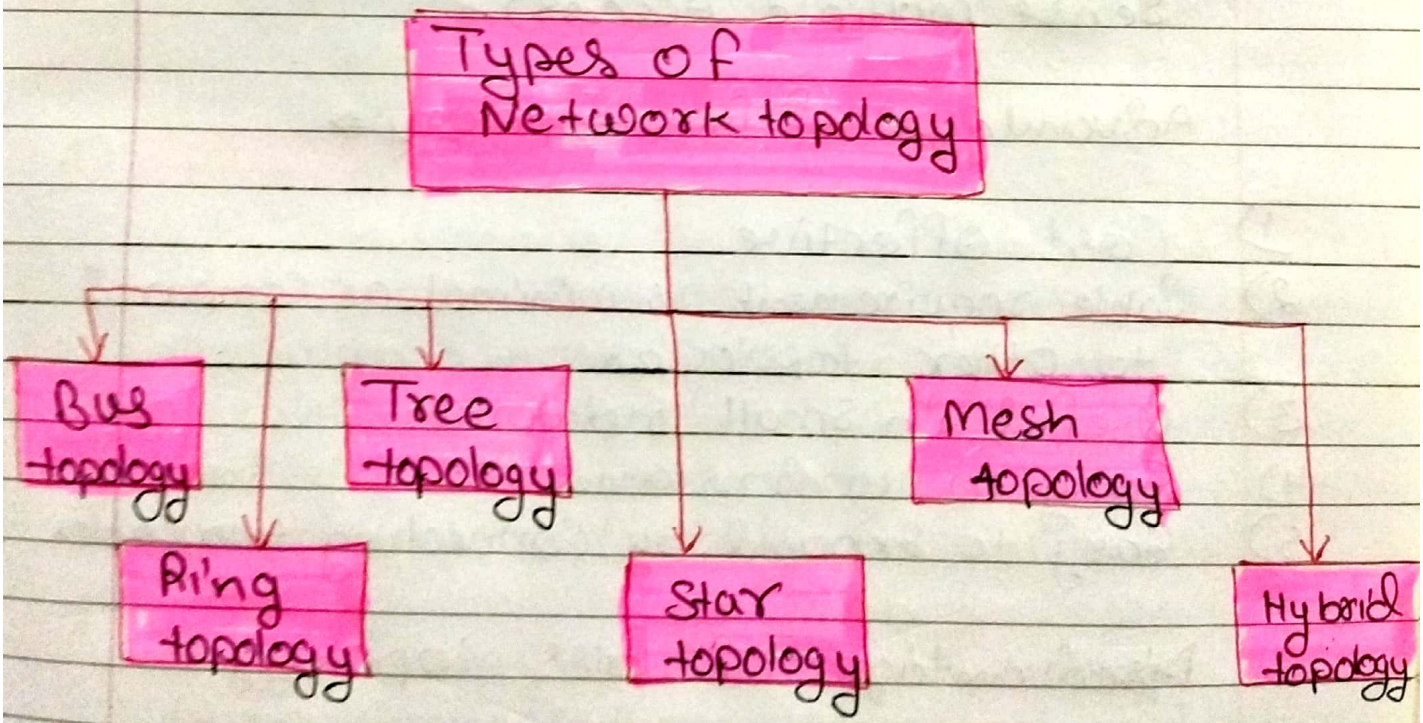
- Less Expensive
- Confined to a small space area.
- Links to multiple devices concurrently.

Disadvantages of PAN are ⇒

- Limited area
- Slow Data Transmission
- Interference with radio signal.

Network Topology

- A Network Topology is the arrangement with which Computer System or network devices are connected to each other.
- The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as network topology.
- Topologies may define both physical and logical aspect of the network.
  Both logical and physical topologies could be same or different in a same network.



1) Bus topology ⇒

- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- The backbone cable is considered as a "single lane" through which the message is broadcast to all the stations.
- The most common access method of the bus topologies is CSMA (carrier Sense multiple Access).

Advantage of Bus topology ⇒

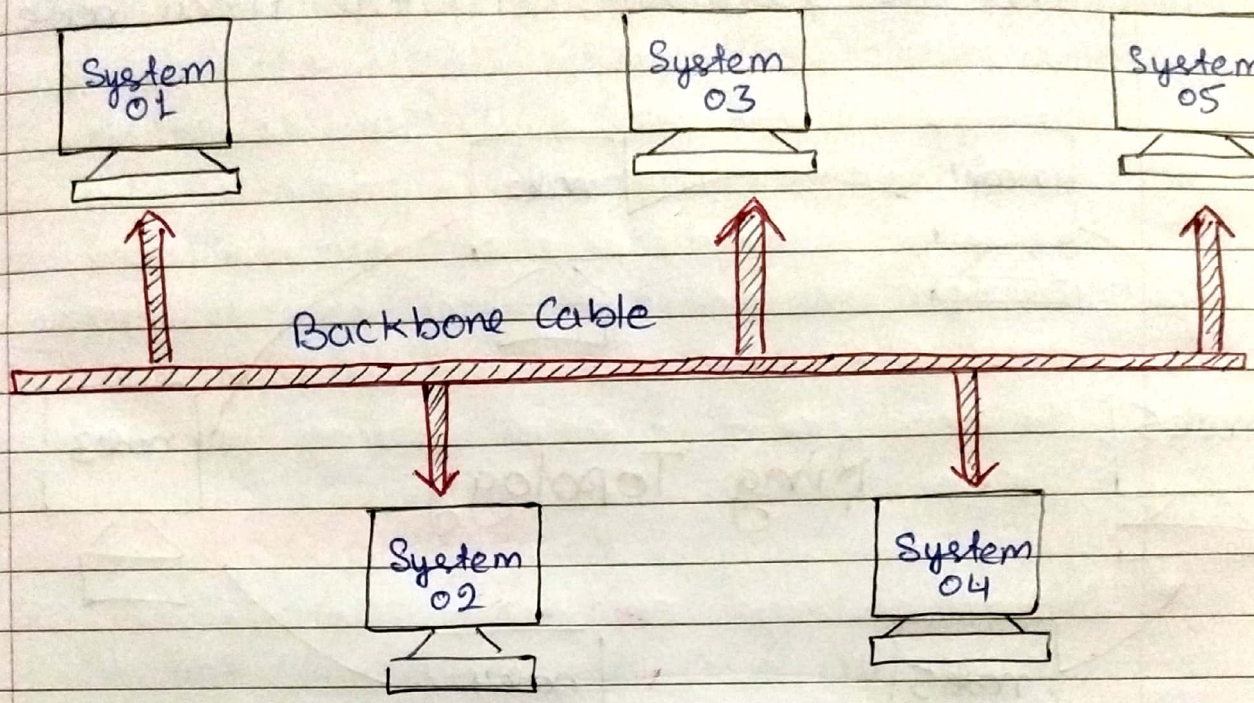
1) Cost-effective
2) Cable requirement is minimal as compared to other topologies
3) Useful in small networks
4) Easy to understand
5) Easy to Expand by Connecting two cables.

Disadvantage of Bus topology ⇒

1) The whole network fails if cables fail.
2) The performance of the network decreases in case network traffic is heavy or nodes are more or the cable has a

limited length.

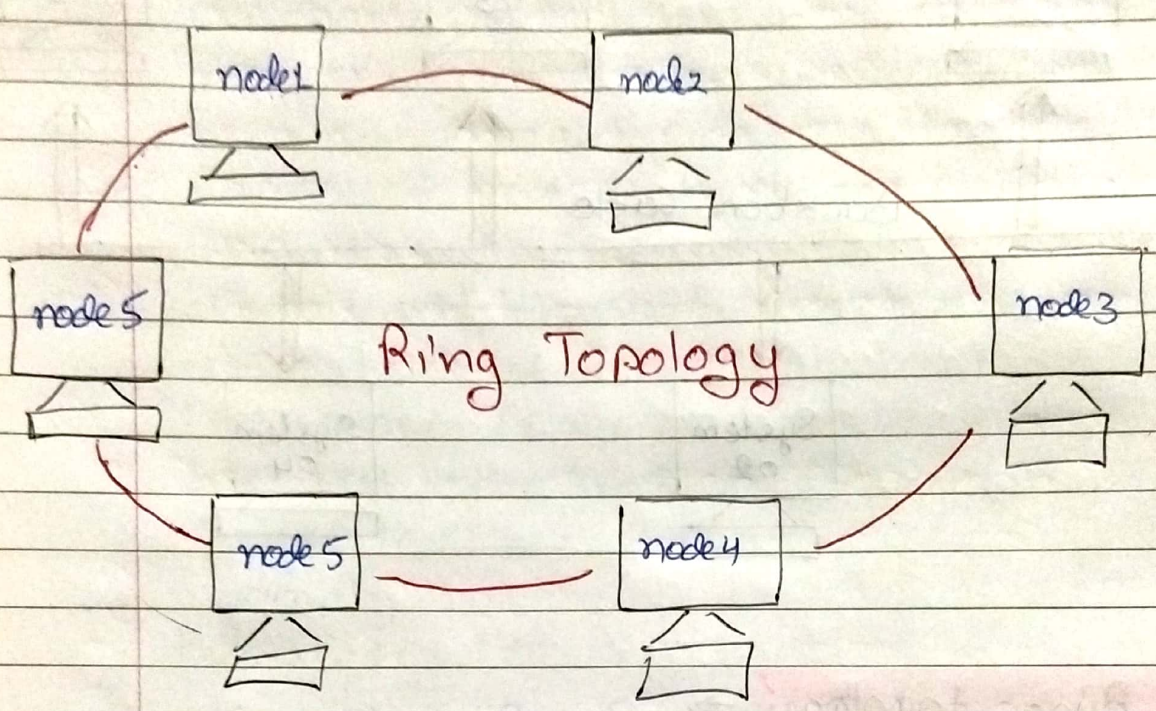
3) It works slower as compared to the ring topology.



2) Ring topology ⇒

- It is named ring topology because it creates a ring as each computer is linked to the neighbouring computer, with the last one linked to the first, there are exactly two neighbours for each computer.
- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.

- Data is transmitted in a sequential manner that is bit by bit. Data transmitted, has to go through each node linked in the network, till the final node.



Advantage of Ring Topology ⇒

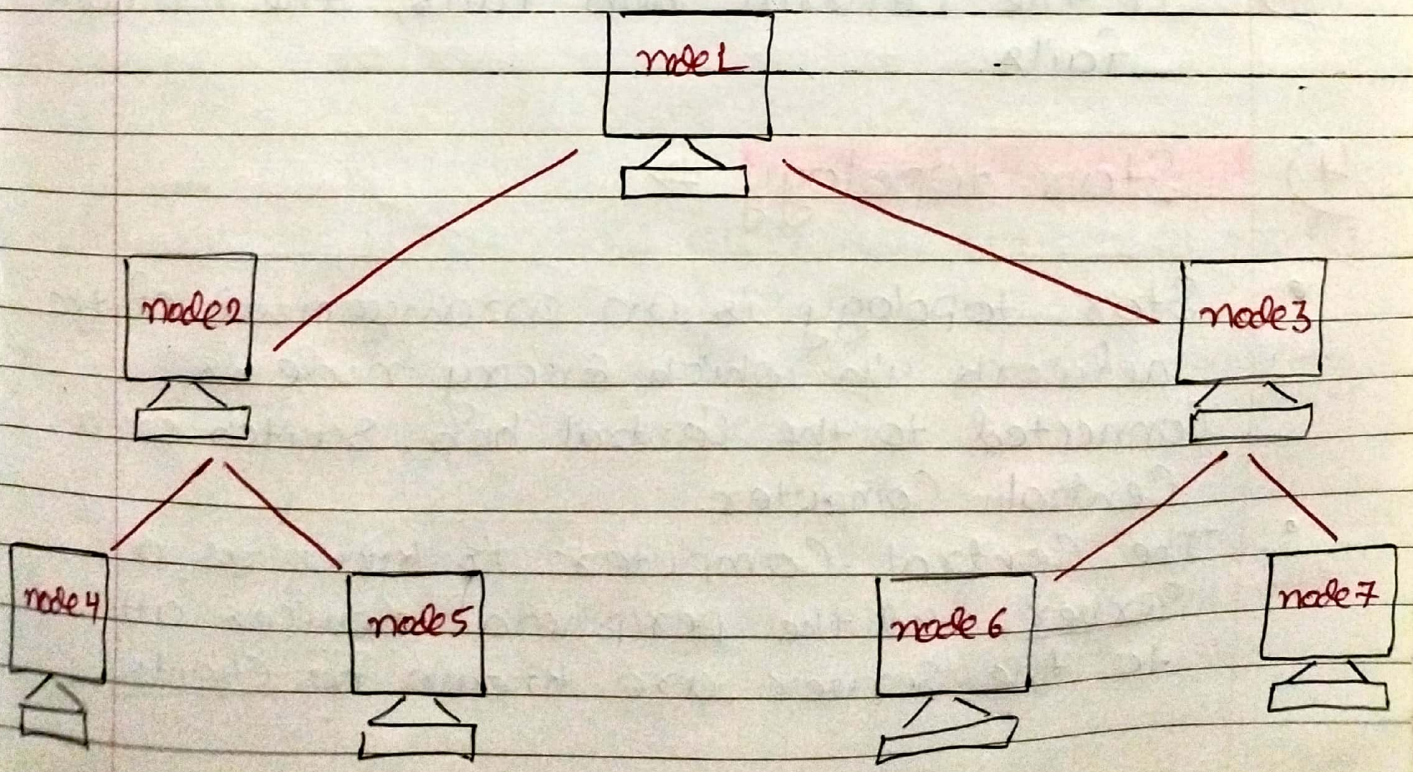
1) Transmitting network is not affected by huge traffic or by the addition of more nodes, as only the nodes having tokens (short message) are allowed to transmit data.
2) Low cost to install and Expand.
3) It is a more reliable network because the Communication System is not dependent on the single host Computer.
4) faulty devices can be removed from the network without bringing the network down.

Disadvantage of Ring topology ⇒

1) Troubleshooting is not simple in a ring topology.
2) The addition or removal of the computers interferes with the other nodes and network activity.
3) The crashing of one node affects the whole network.
4) Initial installation cost is high therefore not applied at low-density traffic.

3) Tree topology ⇒

- It has a root node and all other nodes are linked to it "creating a hierarchy."
- It is also called "hierarchical topology"
- It must have a minimum of three levels to the hierarchy.



- Ideal if workstations are situated in groups
- Useful in Wide Area Network.

Advantage of Tree topology

1) Extension of bus and star topologies.
2) Expansion of nodes is possible and easy Easily managed and maintained.
3) Error detection and Error Correction are very easy.
4) It has point-to-point wiring for individual segments.

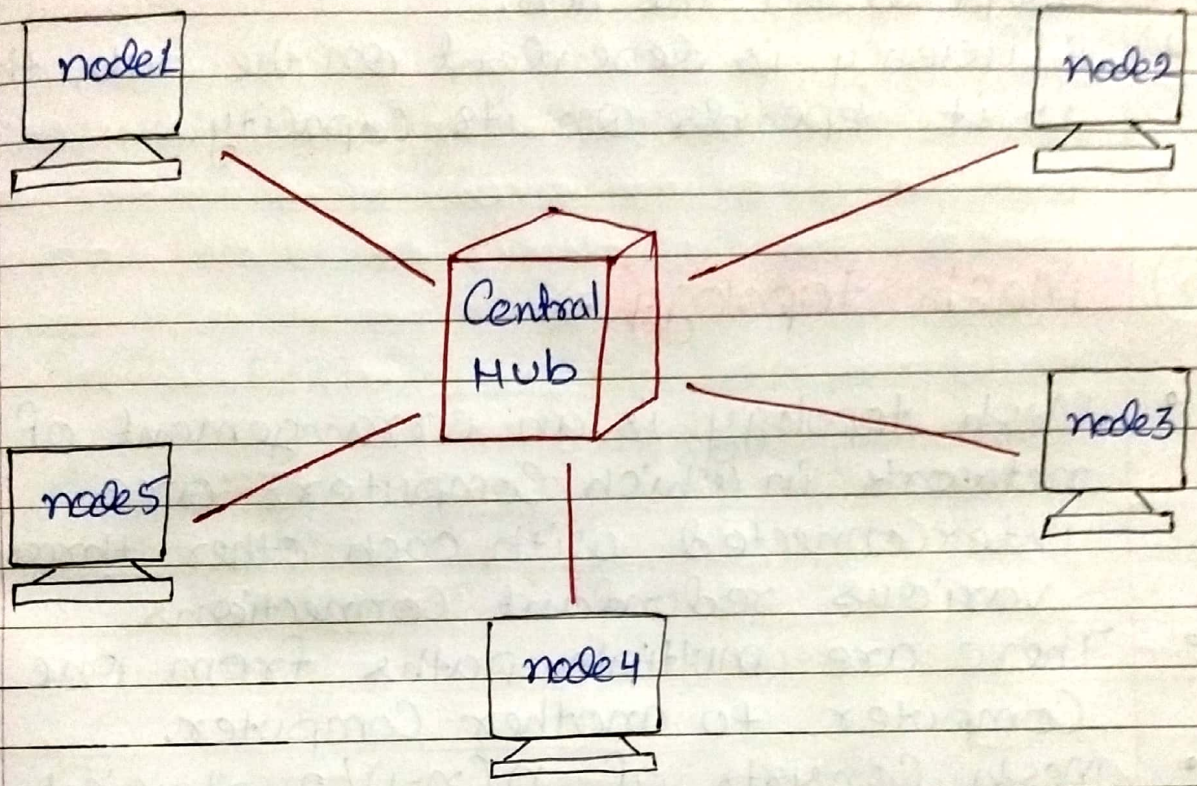
Disadvantage of tree topology

1) Heavily Cabled
2) Costly
3) If additional nodes are introduced, maintenance is difficult.
4) If the Central hub fails, the network fails.

4) Star topology ⇒

- Star topology is an arrangement of the network in which every node is Connected to the Central hub, Switch or a Central Computer.
- The Central Computer is known as a Server, and the peripheral devices attached to the Server are known as Clients.

- Coaxial Cable or RJ-45 Cables are used to Connect the Computers.
- Hubs or Switches are mainly used as Connection devices in a physical star topology.
- Star topology is the most popular topology in network implementation.



Advantage of Star topology

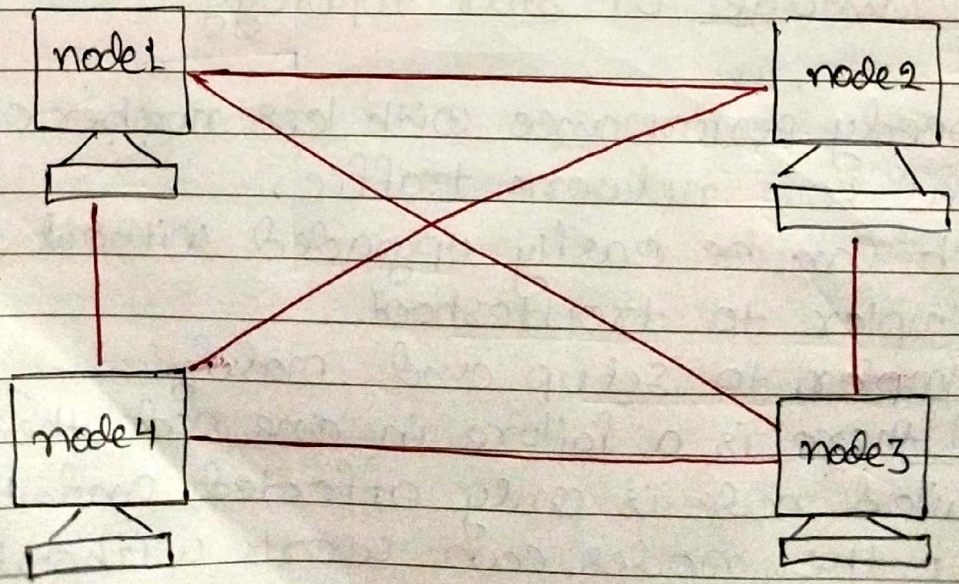
1) Speedy performance with less number of nodes and low network traffic.
2) Hub can be easily upgraded without difficulty.
3) Simpler to troubleshoot.
4) Simpler to setup and modify.
5) If there is a failure in one node then the failed node is only affected, and the rest of the nodes can work without any issues.

Disadvantage of Star Topology

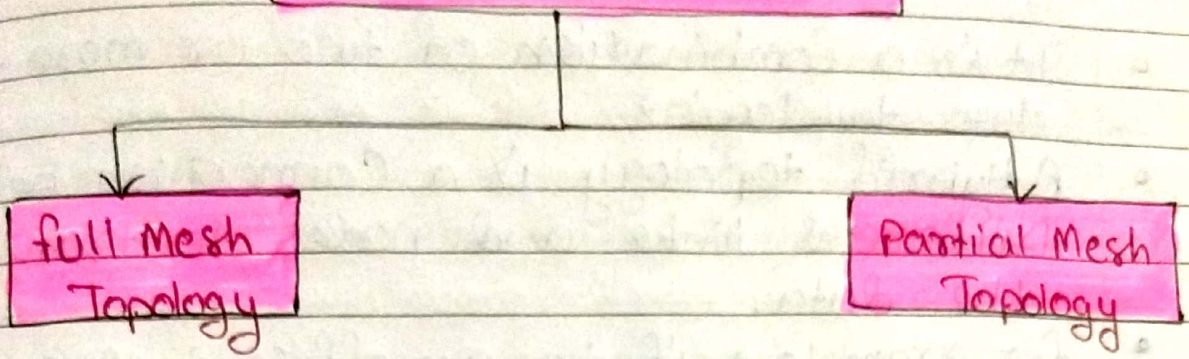
1) Expensive to install.
2) Expensive in usage.
3) If the hub crashes then the entire network is stopped because all linked nodes depend on the hub.
4) Efficiency is dependent on the hub, that is it depends on its capacity.

5) Mesh topology ⇒

- Mesh topology is an arrangement of the network in which Computers are interconnected with each other through various redundant connections.
- There are multiple paths from one Computer to another Computer.
- Mesh consists of $n(n-1)/2$ physical Channels to link n number of devices.



Types of Mesh topology



- full mesh Topology ⇒ In a full mesh topology, each Computer is connected to all the the Computers available in the network.

- Partial Mesh Topology ⇒ In a partial mesh topology, not all but certain Computers are connected to those Computers with which they Communicate frequently.

Advantage of mesh topology ⇒

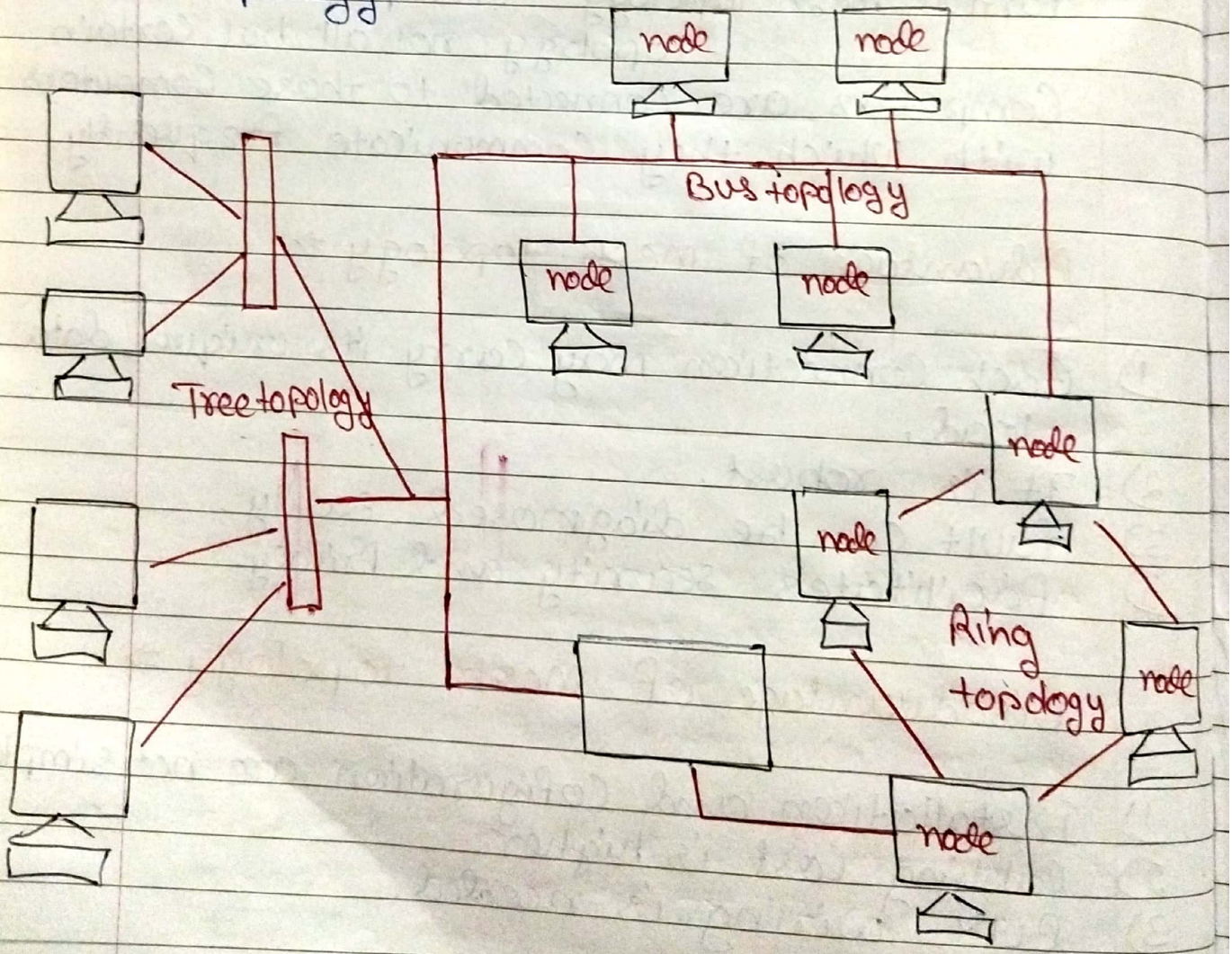
1) Each Connection may carry its unique data load.
2) It is robust.
3) fault can be diagnosed easily.
4) Facilitates security and Privacy.

Disadvantage of Mesh topology ⇒

1) Installation and Cofiguration are not simple.
2) Cabling Cost is higher.
3) Bulk wiring is needed.

6) Hybrid topology ⇒

- It is a Combination of two or more then two topologies.
- A Hybrid topology is a Connection between different links and nodes to transfer the data.
- for example ⇒ if in an office in some department ring topology is used and in another department in the same place, star topology is used, Connecting those topologies will form a Hybrid topology.



Advantage of Hybrid topology

1) Reliable because Error detecting and troubleshooting are Easy.
2) Effective
3) Scalable as size can be increased easily
4) flexible.

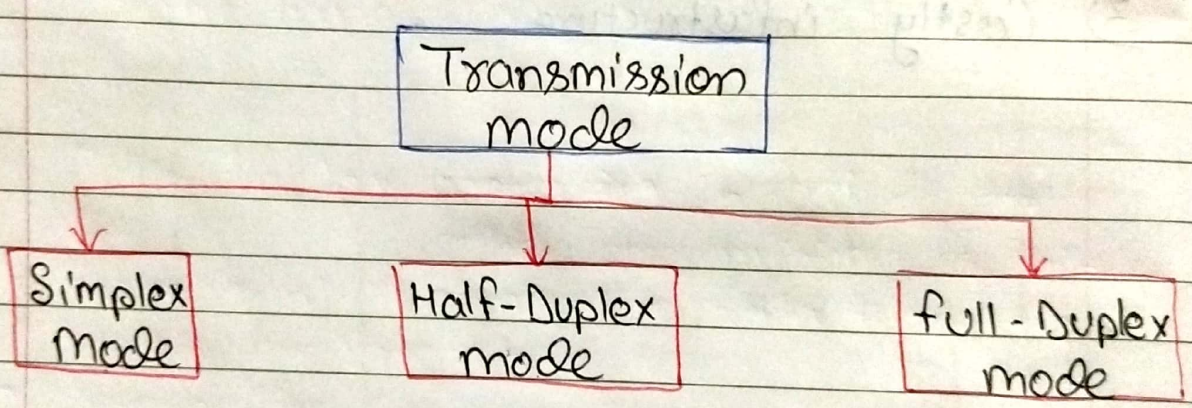
Disadvantage of Hybrid Topology.

1) Complex in design
2) Costly Hub
3) Costly infastructure

Transmission modes

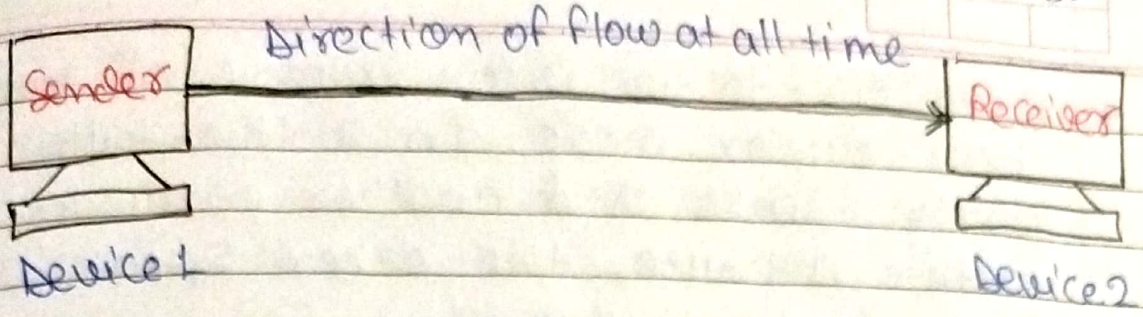
- The way in which data is transmitted from one device to another device is known as transmission mode.
- Data Tranmission mode defines the direction of the flow of information between two Communication devices.
- The transmission mode is also known as the Communication mode. These modes direct the direction of flow of information.
- The transmission mode is defined in the physical Layer.

The transmission mode is devided into three Categories:



Simplex Mode ⇒ • Simplex is the data transmission mode in which the data can flow only in one direction, i.e. the communication is unidirectional.

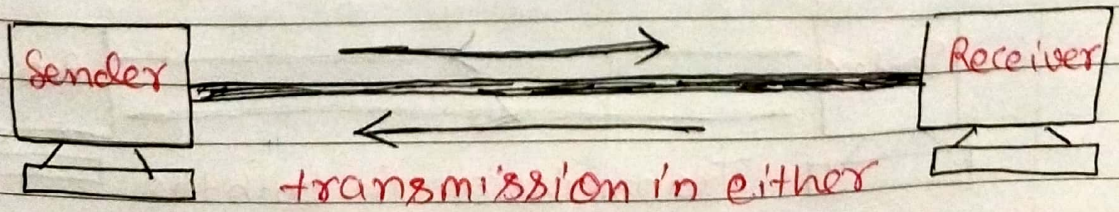
- A device can only send the data but cannot receive it or it can receive the data but cannot send the data.



- 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.
- The main advantage of the Simplex mode is that the full capacity of the communication channel can be utilized during transmission.
- Communication is unidirectional, so it has no inter-communication between devices.

Half-Duplex Mode ⇒ • In half duplex channel, direction can be reversed. such as the station can transmit and receive the data as well.

- Message flow in both the directions, but not at the same 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.

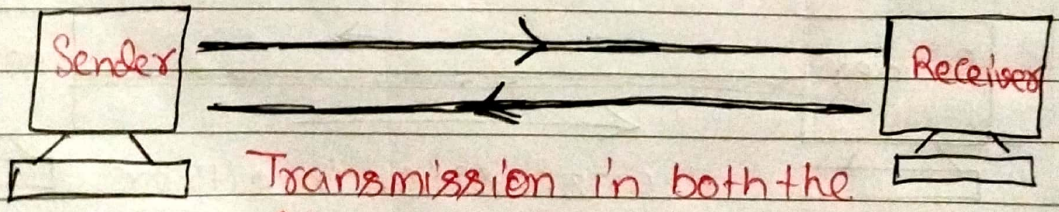


transmission in either direction, but not simultaneously.

- A Walkie-talkie is an example of the half-duplex mode. In walkie-talkie, one party speaks, and another party listen. After a pause, the other speaks and first party listens.
- main advantage of 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.
- One disadvantage of 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 such as 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.



Transmission in both the directions simultaneously

- The full-duplex mode is the fastest mode of communication between devices.
- The most common example of the full duplex mode is a telephone network. When two people are communicating with each other by a telephone line, both can talk and listen at the same time.
- Advantage of Both the stations can send and receive the data at the same time.
- Disadvantage of full-duplex if there is no dedicated path exists between the devices, then the capacity of the communication channel is divided into two parts.

Difference b/w Simplex, half duplex and full-duplex mode

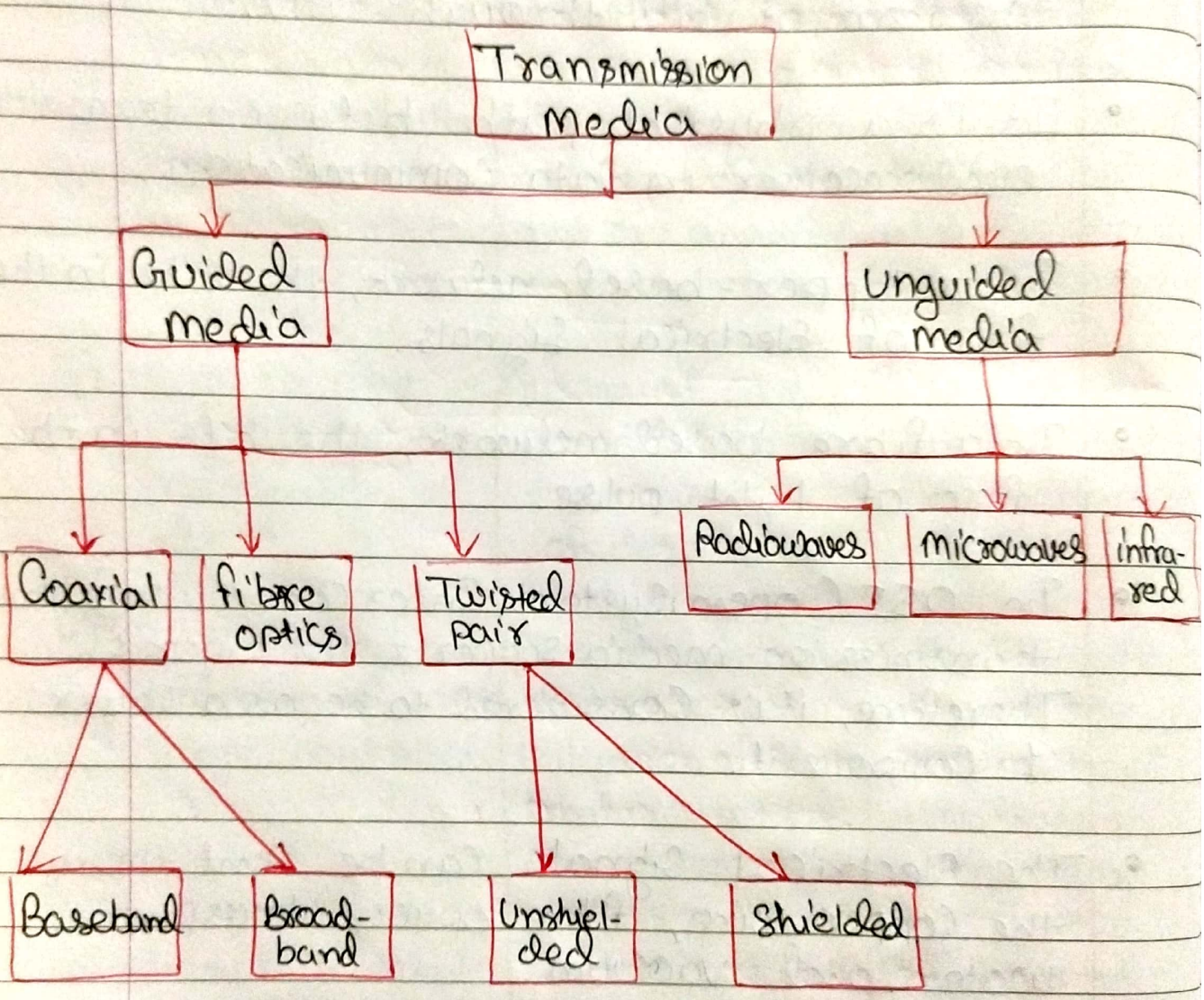
Simplex mode	Half-duplex mode	full-duplex mode
1) the Communication is undirectional	1) the Communication is bidirectional, but one at a time.	1) The Communication is bidirectional
2) Sender and Receiver in Simplex mode, Sender can Send the data but that Sender Cannot receive the data	2) Sender and Receiver in half duplex mode, Sender can send the data and also can receive the data but one at a time	2) Sender and Receiver in full duplex mode, Sender can send the data and also can receive the data Simultaneously
3) Usage of one Channel for the transmission of data	3) Usage of one channel for the transmission of data	3) Usage of two channels for the transmission of data.
4) Simplex utilize the maximum of a Single bandwidth	4) the half-duplex involves lesser utilization of Single bandwidth at the time of transmission	4) the full-duplex doubles the utilization of transmission bandwidth.
5) Example of Simplex mode are: keyboard and monitor	5) Example of half duple mode is Walkie-talkies	5) Example of full-duple mode is: Telephone.

Transmission media

- Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagenetic signals.
- The main functionality of the transmission media is to carry the information in the form of bits through LAN.
- It is a physical path between transmitter and receiver in data communication.
- In a copper-based network, the bits in the form of electrical signals.
- In a fibre based network, the bits in the form of light pulse.
- In OSI (open System Interconnection) phase transmission media supports the Layer 1. Therefore, it is considered to be as a Layer 1 Component.
- The Electrical signals can be sent through the copper wire, fibre optics, atmosphere, water and vaccum.
- 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 Physical Layer.

Classification of Transmission Media ⇒

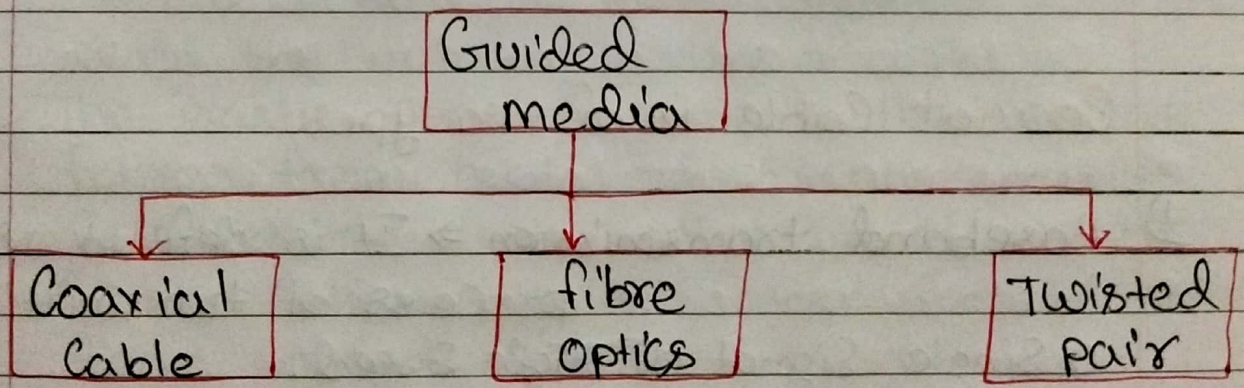


Guided Transmission Media

- Guided media are also known as wired or bounded media.
- It is defined as the physical medium through which the signals are transmitted.
- Signals being transmitted are directed and confined in a narrow pathway by using physical links.

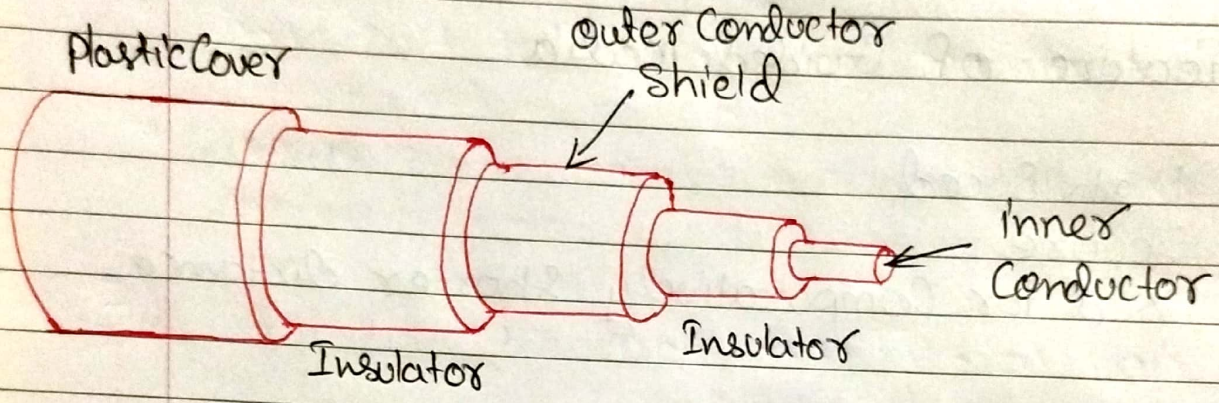
Feature of Guided media.

1) High Speed
2) Secure
3) Used for Comparatively shorter distance.



1) Coaxial Cable ⇒ • Coaxial Cable is very commonly used transmission media for example, TV wire is usually a Coaxial Cable.
- The name of the Cable is Coaxial as it Contains two Conductors parallel to each other.

- It has a higher frequency as compared to Twisted pair cable.
- the inner Conductor of the Coaxial Cable is made up of Copper, and the outer Conductor is made up of copper mesh. the middle core is made up of non-Conductive Cover that Separates the inner Conductor from the outer Conductor.



Coaxial Cable is of two types:

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 of Coaxial Cable ⇒

- The data can be transmitted at high Speed.

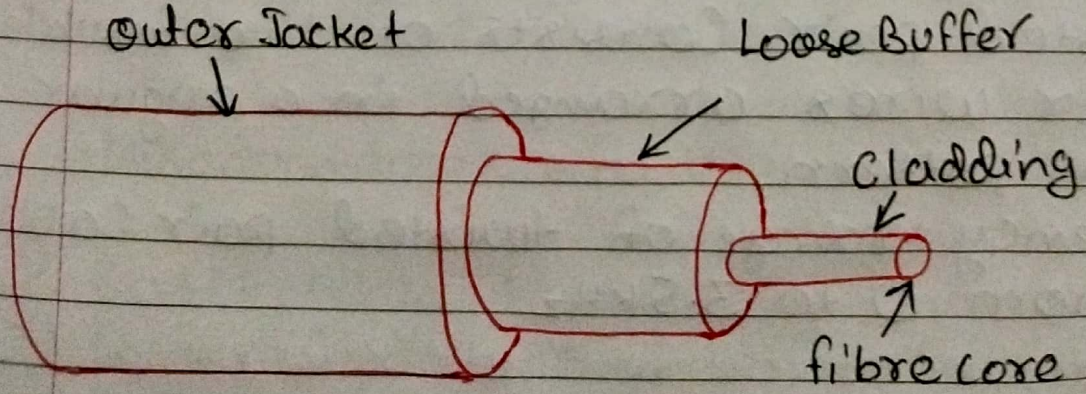
- It has better shielding as compared to twisted pair cable.
- It provides higher bandwidth.

Disadvantages of Coaxial Cable ⇒

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

2) Fibre Optics ⇒ • 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 type of wiring.
- fibre optics provide faster data transmission than copper wires.



Advantage of fibre optics ⇒

- Increased Capacity and bandwidth
- Lightweight
- Less Signal attenuation
- Immunity to Electromagnetic interference
- Resistance to Corrosive materials.

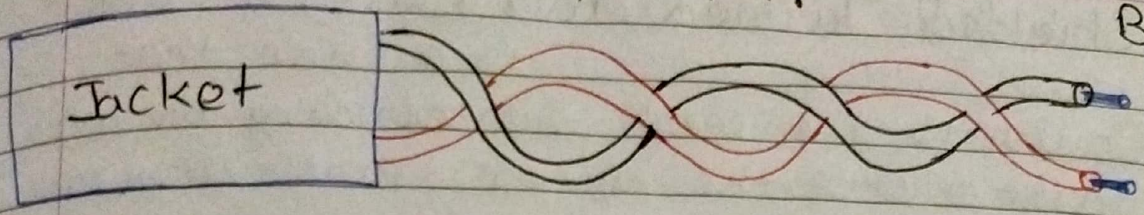
Disadvantage of fibre optics ⇒

- Difficult to install and maintain
- High Cost
- fragile.

3) 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.
- A wisted pair Consists of two insulated Copper wires arranged in a regular Spiral pattern.
- frequency range of twisted pair Cable is from 0 to 3.5KHz.

Twisted Pair



Types of Twisted Pair

- Unshielded Twisted Pair
- Shielded Twisted Pair

- **Unshielded twisted Pair (UTP) ⇒** • UTP Consists of two insulated copper wires twisted around one another.
- This type of cable has the ability to block interference and does not depend on a physical shield for this purpose.
- It is used for telephonic application.

Advantages of UTP ⇒

1) Least Expensive
2) Easy to install
3) High speed Capacity.

Disadvantages of UTP ⇒

1) Susceptible to External interference.
2) Lower Capacity and performance in comparison to STP.
3) Short distance transmission due to attenuation.

- Shielded Twisted Pair (STP) ⇒ • STP is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

Advantages of STP

1) Better performance at a higher data rate in comparison to UTP.
2) Eliminates crosstalk.
3) Comparatively faster.

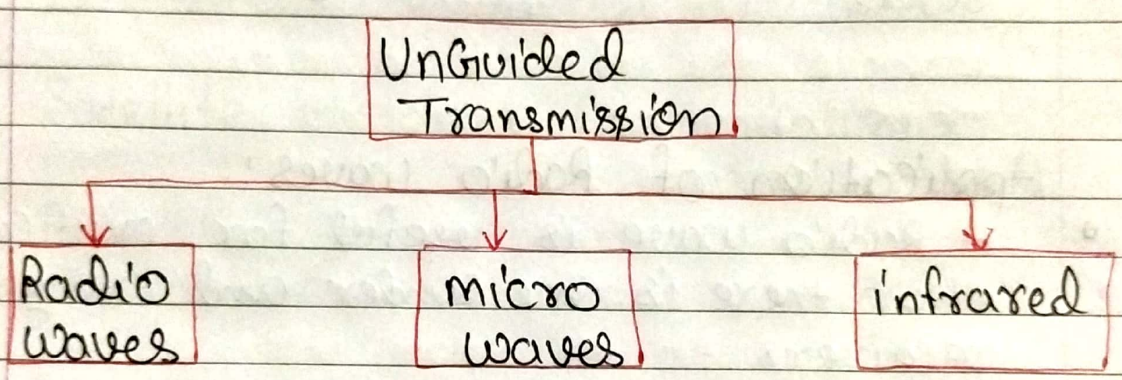
Disadvantages of STP

1) Comparatively difficult to install and manufacture.
2) More expensive
3) Bulky.

UnGuided Transmission Media

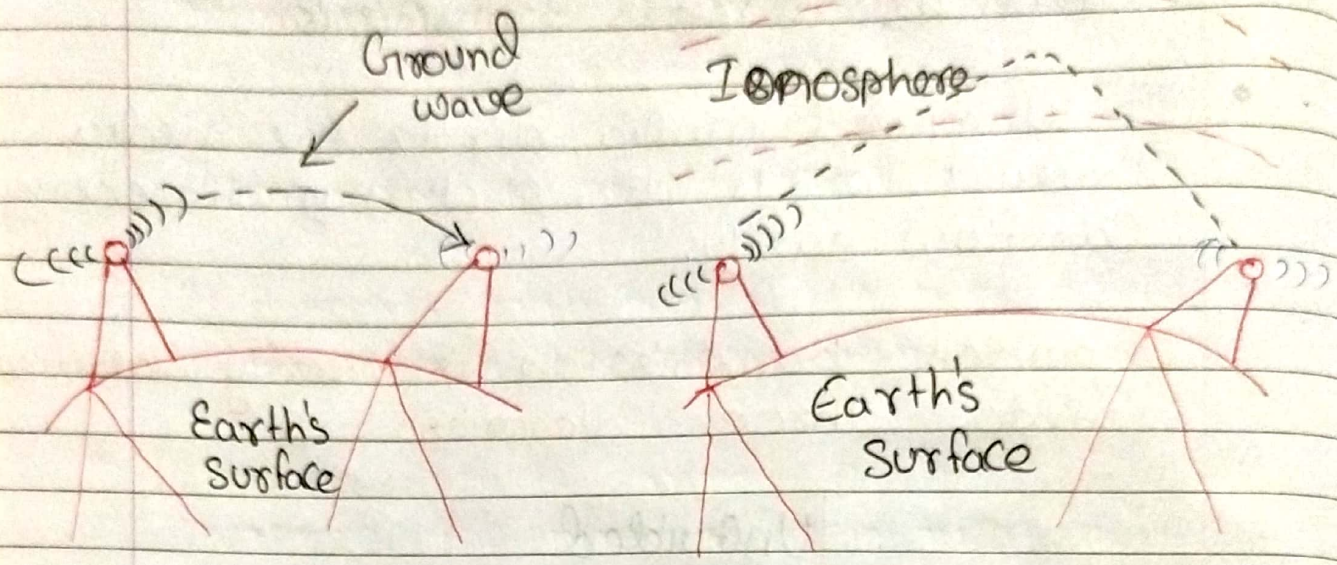
- An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as Wireless transmission.
- In unguided media, air is the media through which the electromagnetic energy can flow easily.

Unguided transmission is broadly classified into three categories:



Radio waves ⇒
- Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- Radio waves are omnidirectional such as 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 such that the wave sent by the sending antenna can be received by any receiving antenna.

- An example of the radio wave is FM radio.



Application of Radio waves:

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

Microwaves ⇒ There are two types of microwaves transmission.

1) Terrestrial microwaves
2) Satellite microwave Communication.

1) Terrestrial Microwave Transmission ⇒

- Terrestrial microwave transmission is a

- technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.

- Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 100GHz.

- Microwaves are unidirectional as the sending and receiving antenna is to be aligned such that the waves send by the sending antenna are narrowly focussed.

2) Satellite microwave Communication ⇒

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

- Satellite Communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems.

- We can Communicate with any point on the globe by using Satellite Communication.

Infrared ⇒ • An infrared transmission is a wireless technology used for Communication over short ranges.

- The frequency of the infrared in the range from 300GHz to 400THz

- It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Characteristics of infrared ⇒

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

OSI Model

- OSI stands for Open System Interconnection 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.

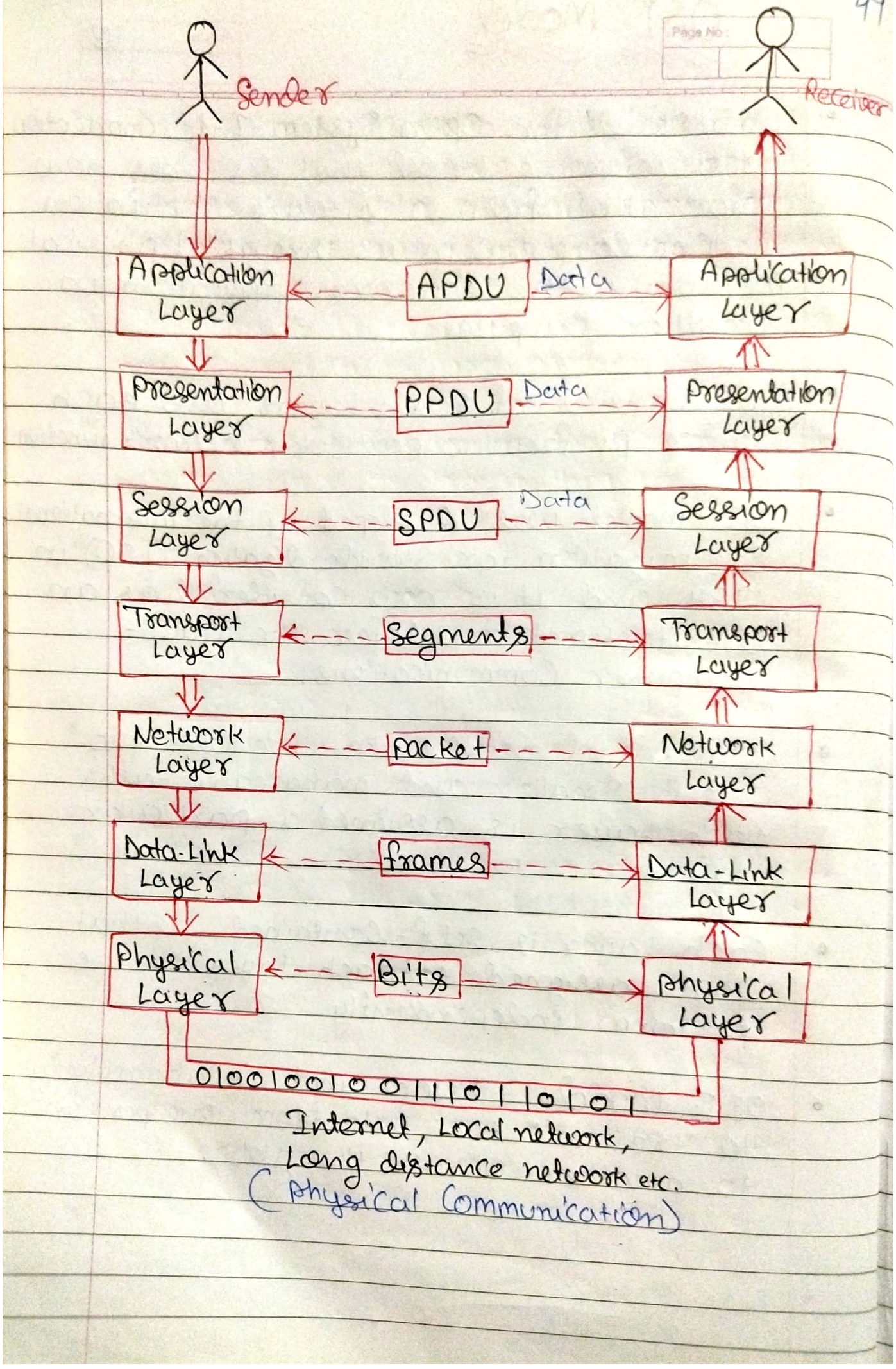
- OSI Consists of seven layers, and each layer perform a particular network function.

- 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.

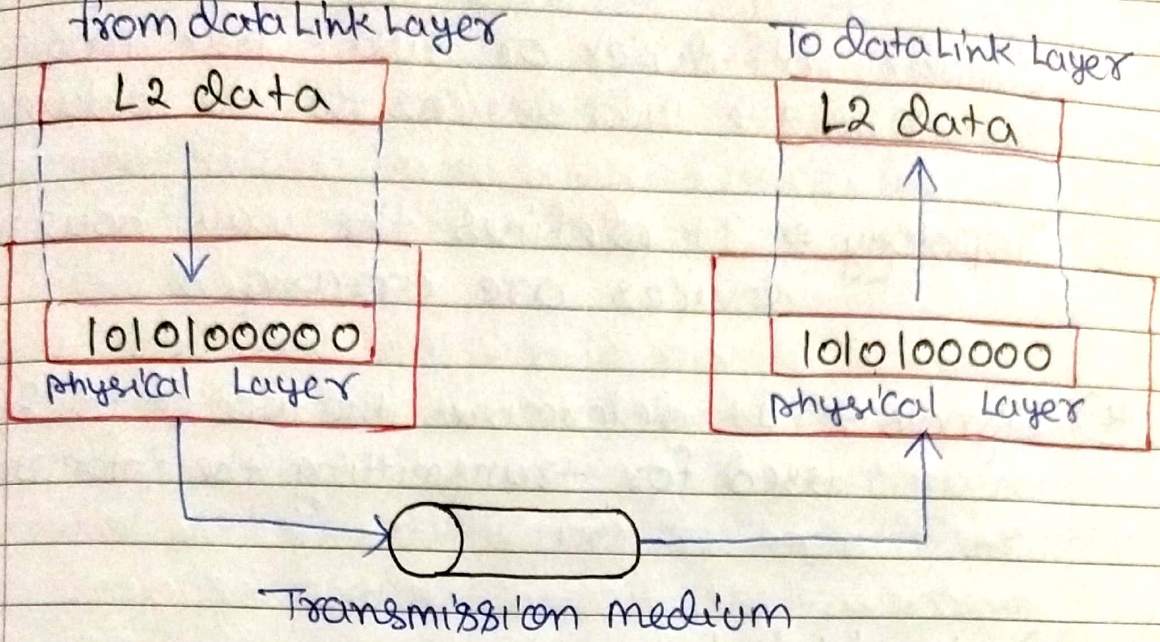
- Each layer is self-contained, so that task assigned to each layer can be perform independently.

- OSI model 7 layers work collaboratively to transmit the data from one person to another across the globe.



Page No :

1) Physical Layer ⇒



- The main functionality of the physical Layer is to transmit the individual bits from one node to another node.
- It is the Lowest Layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

functions of physical Layer ⇒

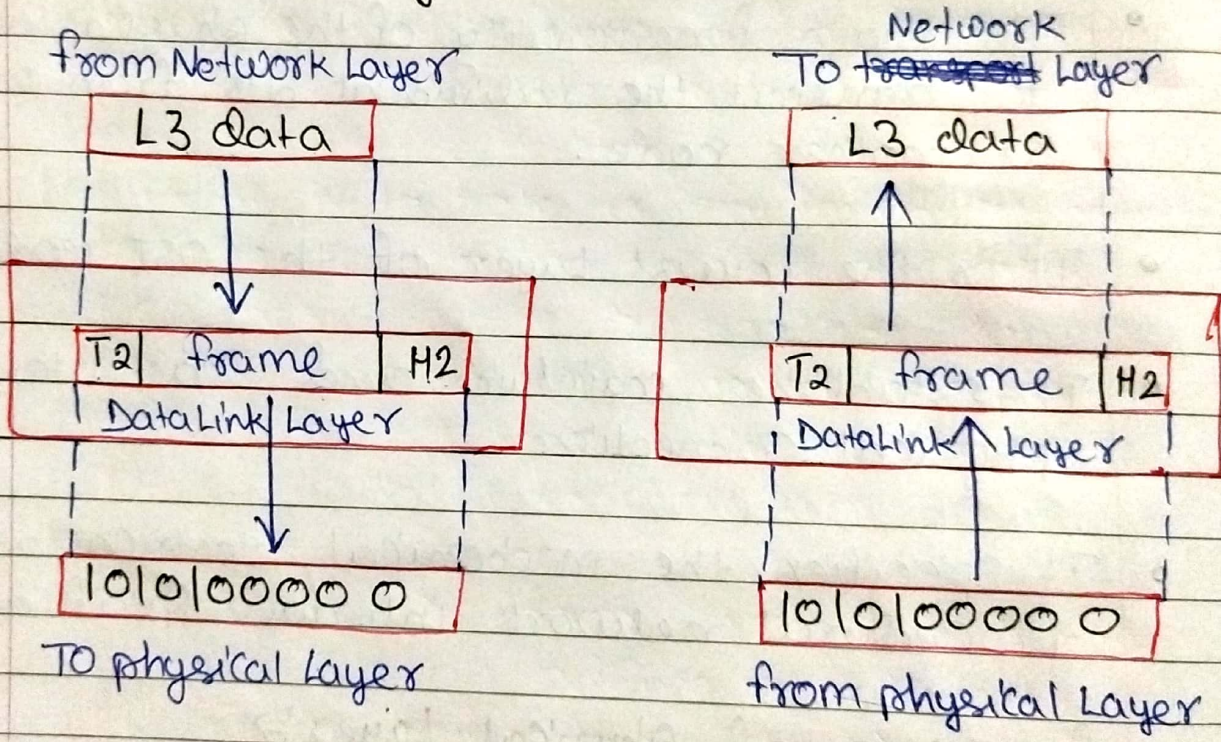
1) Line Configuration ⇒ It defines the way how two or more devices Can be Connected physically.

2) Data transmission ⇒ It defines the transmission mode whether it is simplex, half-duplex or full duplex mode between the two devices on the network.

3) Topology ⇒ It defines the way how network devices are arranged.

4) Signals ⇒ It determines the type of the signal used for transmitting the information.

2) Data-Link Layer ⇒



- This Layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.

Page No.

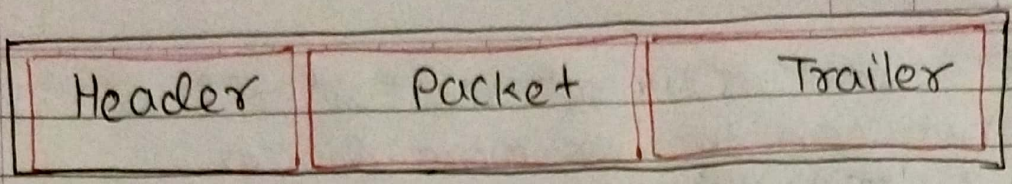
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a Local network.
- It Contains two Sub Layers:

1) Logical Link Control Layer ⇒ • It is responsible for transferring the packets to the Network Layer of the receiver that is receiving.
- It identifies the address of the network Layer protocol from the header
- It provides flow control.

2) Media Access Control Layer ⇒ • A media access control layer is a link between the Logical Link Control Layer and the network's physical layer
- It is used for transferring the packets over the network.

functions of the Data-Link Layer ⇒

1) framing ⇒ The data Link layer translates the physical's raw bit stream into packets known as frames. The data Link layer adds the header and trailer to the frame.



The header which is added to the frame Contains the hardware destination and source address.

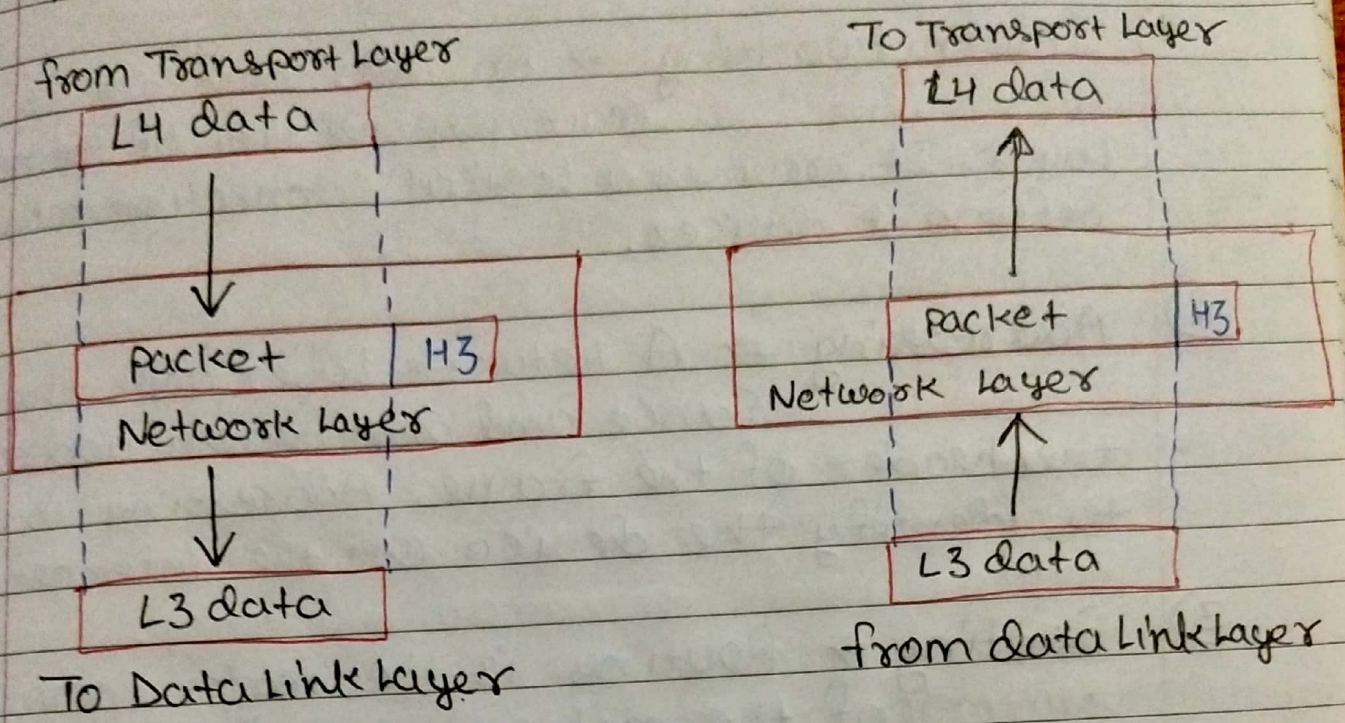
2) Physical Addressing ⇒ The data Link Layer adds a header to the frame that Contains a destination address. The frame is transmitted to the destination address mentioned in the header.

3) flow Control ⇒ flow Control is the main functionality of the Data-Link Layer. It is the technique through which the Constant data rate is maintained on both the Sides so that no data get ~~ge~~ Corrupted. It ensures that the transmitting station such as a server with higher processing Speed does not Exceed the receiving Station, with Lower processing Speed.

4) Error Control ⇒ Error Control is achieved by adding a calculated value CRC (Cyclic Redundancy check) that is placed to the Data link Layer's trailer which is added to the message frame before it is sent to the physical Layer.

5) Access Control ⇒ When two or more devices are connected to the same Communication Channel, then the data Link Layer protocols are used to determine which device has control over the link at a given time.

3) Network Layer ⇒



- It is a Layer 3 that manages device addressing, tracks the location of devices on the network.
- 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.
- Data Link Layer is responsible for routing and forwarding the packets.
- Routers are the Layer 3 devices, they are Specified in this Layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network Layer protocols. Example of protocols are IP and IPv6.

functions of Network Layer ⇒

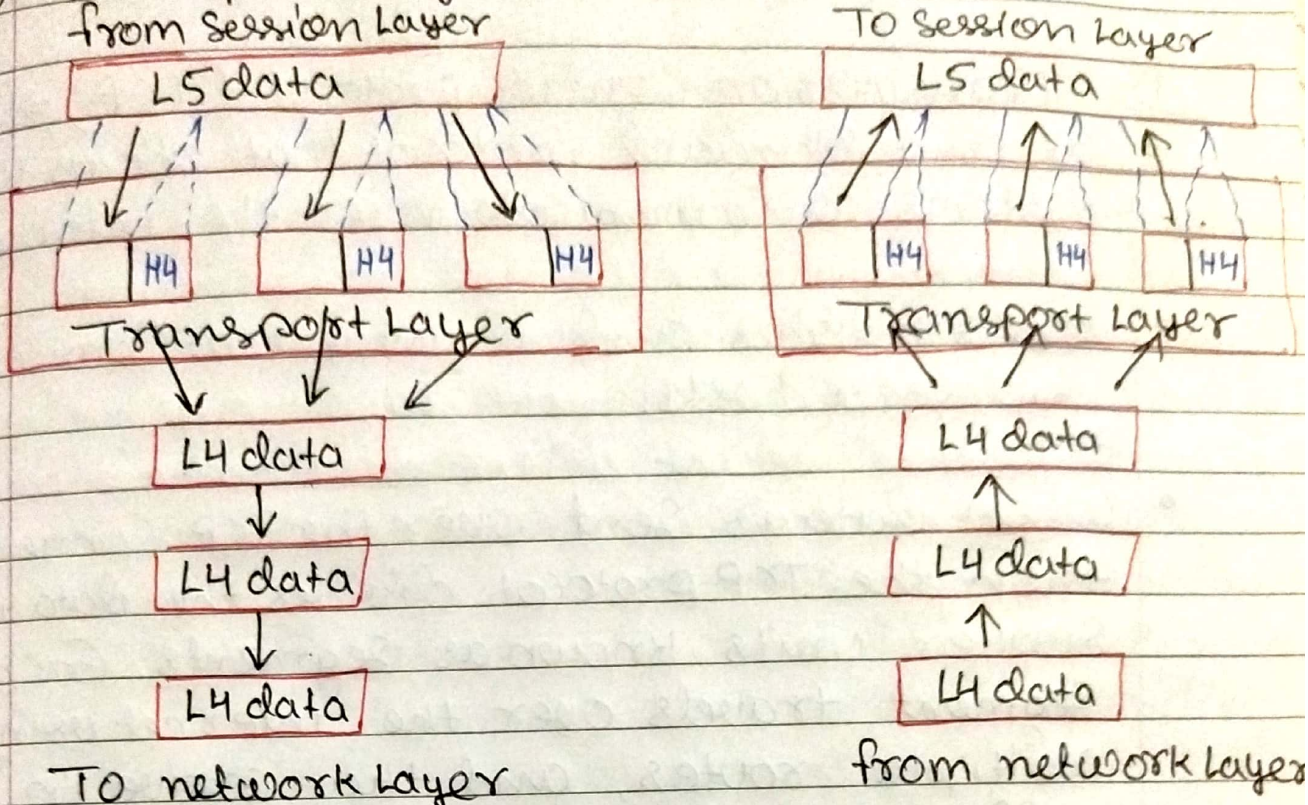
1) Internetworking ⇒ An internetworking is the main responsibility of the network Layer. It provides a Logical connection between different devices.

2) Addressing ⇒ A Network Layer adds the Source and destination address to the header of the frame. Addressing is used to identify the device on the internet.

3) Routing ⇒ Routing is the major component of the network Layer, and it determines the best optimal path out of the multiple path from source to destination.

4) Packetizing ⇒ A Network Layer receives the packets from the upper Layer and converts them into packets. This process is known as packetizing. It is achieved by internet protocol (IP).

4) Transport Layer ⇒



- The trasport Layer is a Layer 4 ensure that messages are transmitted in the order in which they are send and there is no duplication of data.
- The main responsibility of the transport Layer is to transfer the data completely.
- It receives the data from the upper Layer and Converts them into smaller units known as segments.
- This Layer Can be termeds as an end-to-end Layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are! ⇒

1) Transmission Control protocol (TCP) ⇒

- It is a standard protocol that allows the systems to communicate over the internet.
- It establishes and maintains a connection between hosts.
- When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The TCP reorders the packets in the correct order at the receiving end.

2) User Datagram Protocol (UDP) ⇒

- User Datagram protocol is a transport layer protocol.
- It is an unreliable transport protocol as in this case receiver does not send any acknowledgement when the packet is received, the sender does not wait for any Acknowledgement. Therefore, this makes a protocol unreliable.

functions of Transport Layer ⇒

1) Service-point addressing ⇒ Computer run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one Computer to another Computer but also from one process to another process. The trasport Layer adds the header that contains the address known as a Service-point address or port address. The responsibility of the network layer is to transmit the data from one Computer to another Computer and the responsibility of the transport Layer is to transmit the message to the Correct process.

2) Segmentation and reassembly ⇒ When the transport Layer receives the message from the upper Layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segments.

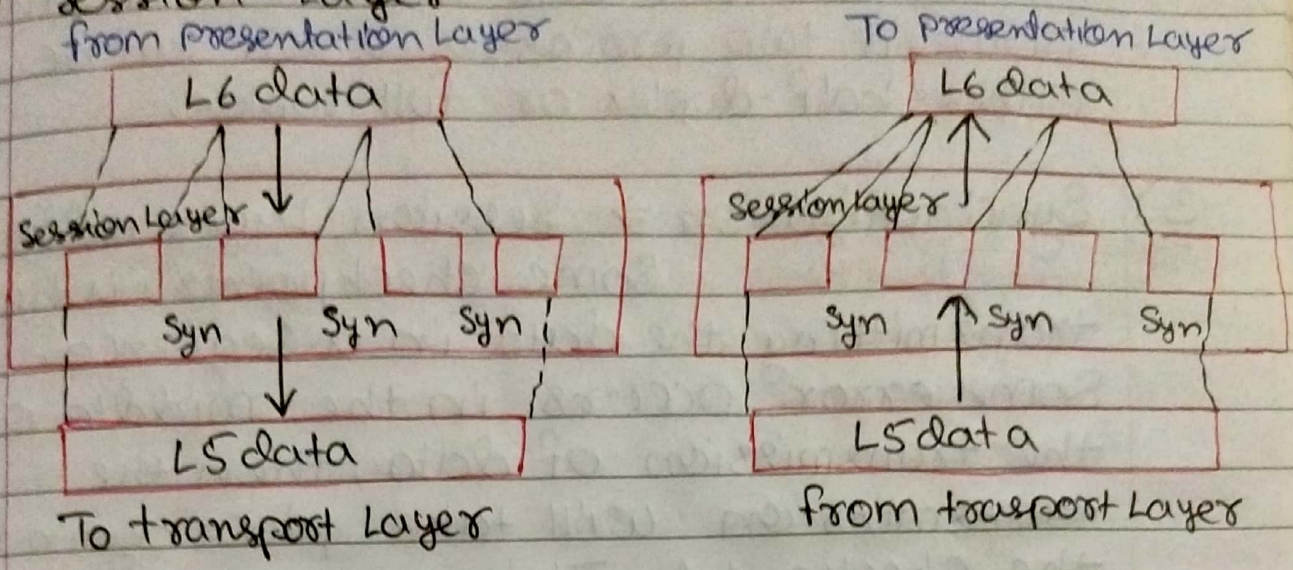
3) Connection Control ⇒ Transport Layer provides two Services Connection-oriented Service and Connectionless service. A Connectionless Service treats each segments as an individual packet, and they all travel in different routes to reach the destination.

4) flow Control ⇒ The transport Layer also reponsible for ~~error~~ flow Control.

but it is performed end-to-end rather than across a single link.

5) Error Control ⇒ The transport layer is also responsible for Error Control. Error Control is performed end-to-end rather than across the single link. The sender transport layer ensure that message reach at the destination without any error.

5) Session Layer



- It is a Layer 3 in the OSI model.
- The session Layer is used to establish, maintain and synchronizes the interaction between communicating devices.
- This Layer is responsible for the establishment of connection, maintenance of sessions, authentication, and also ensures security.

functions of session Layer:

1) Session establishment, maintenance and termination :⇒ The Layer allows the two processes to establish, use the terminate a connection.

2) 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.

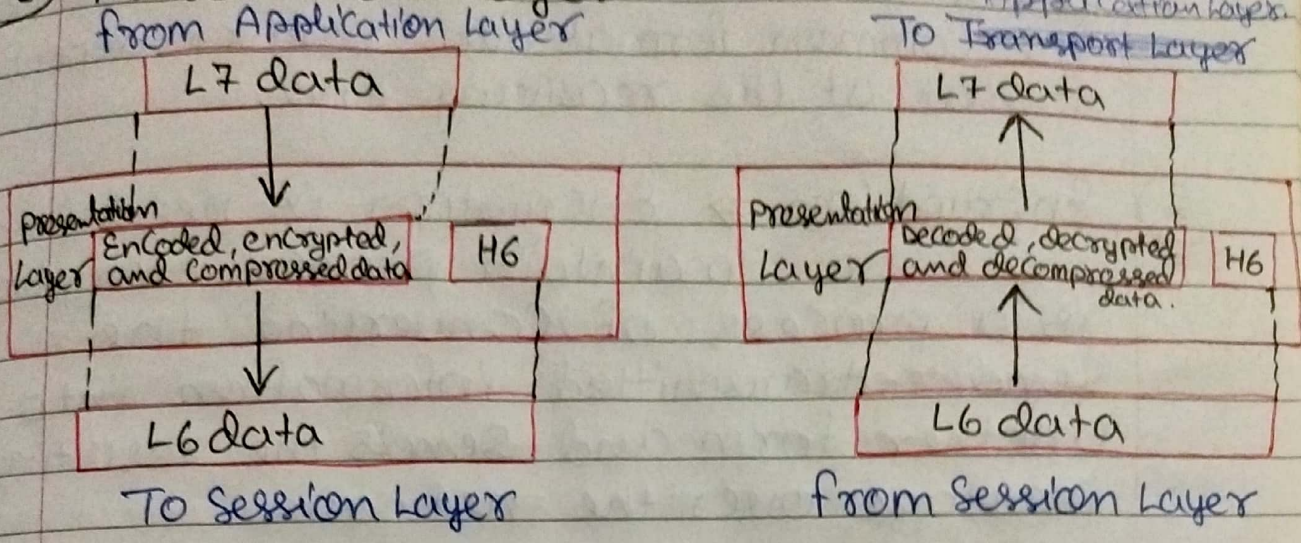
3) Synchronization ⇒ Session Layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

msg ⇒ Hello P.T

Key +3 KHOOR Encode C.T

-3 HELLO → P.T

6) Presentation Layer



- A Presentation Layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This Layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation Layer is also known as the Syntax Layer.

functions of Presentation Layer ⇒

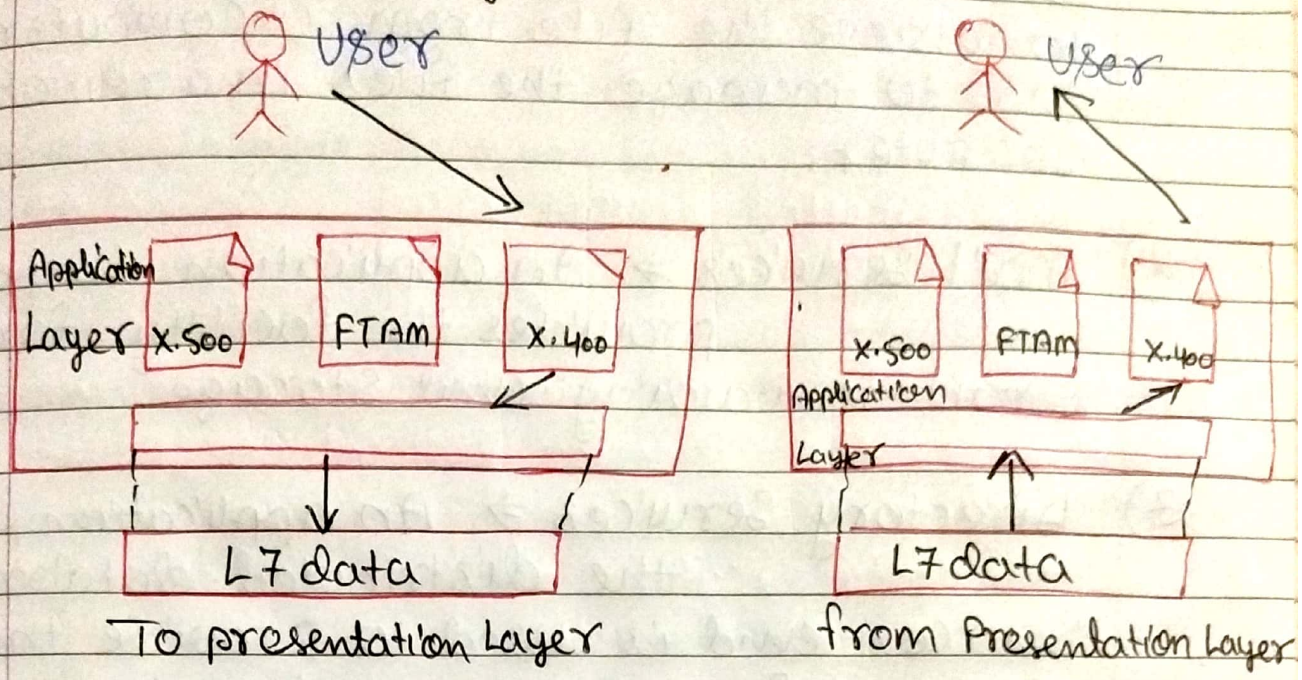
1) Translation ⇒ The processes in two systems exchange the information in the form of character string, number and so on.
It converts the data from sender-dependent

format into a common format and changes the common format into receiver-dependent format at the receiving end.

2) Encryption ⇒ Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.

3) Compression ⇒ Data compression is a process of compressing the data, such that it reduce the no. of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

7) Application Layer ⇒



- An application Layer Serves as a window for users and application process to acess network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application Layer is not an application, but it performs the application Layer function.
- This Layer provides the network services to the end-users.

function of Application Layer ⇒

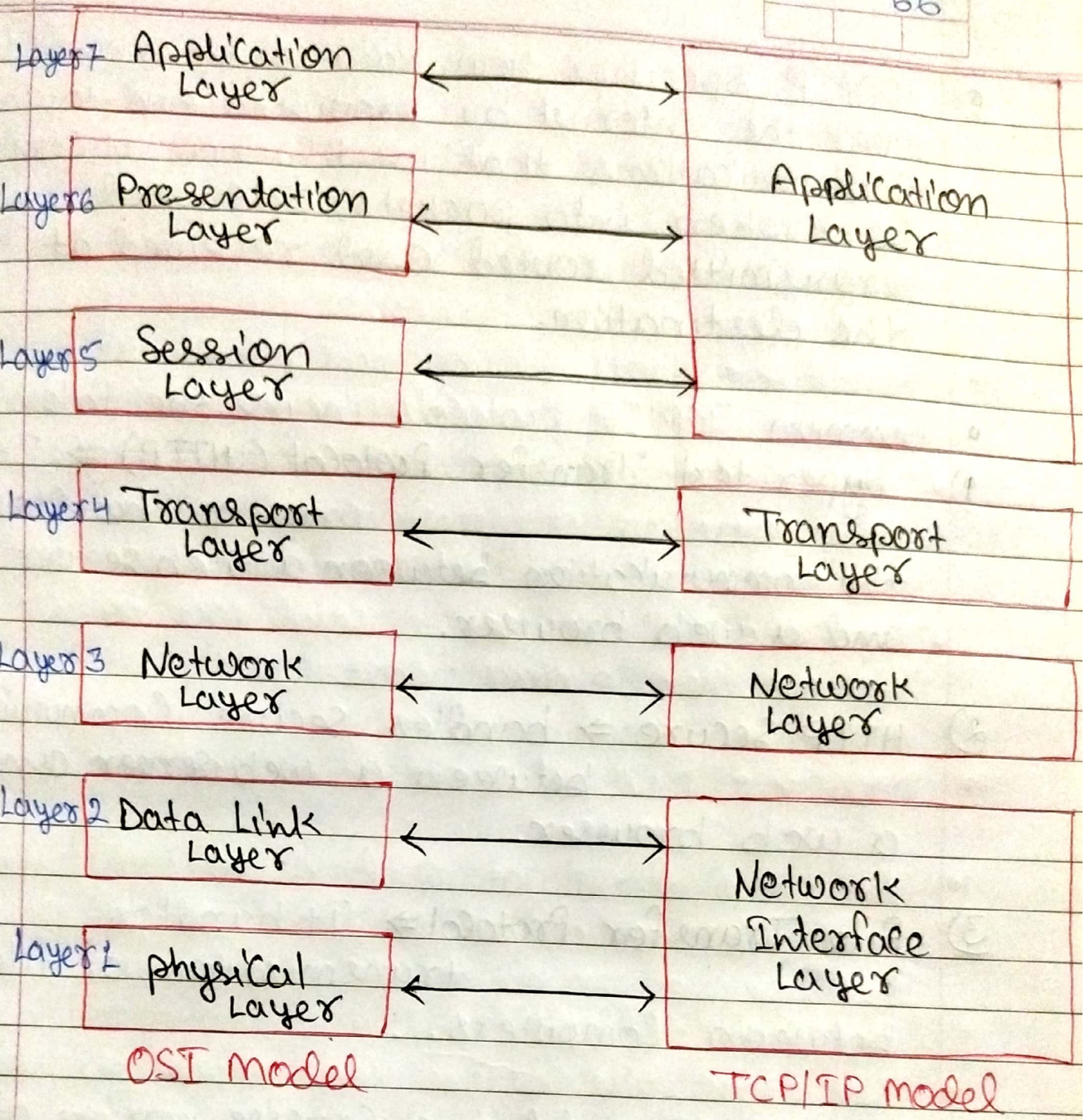
1) file transfer, access, and management (FTAM) ⇒ An application Layer allows a user,

to access the files in a remote Computer, to retrieve the file from a Computer and to manage the files in a remote Computer.

2) Mail services ⇒ An application Layer provides the facility for email forwarding and storage.

3) Directory services ⇒ An application provides the distributed database sources and is used to provide that global information about various objects.

TCP/IP Model



- TCP/IP Stands for Transmission Control Protocol / Internet Protocol and it's a suite of Communication protocols used to interconnect network devices on the internet.
- TCP/IP it's also used as a Communication protocol in a private Computer network (an internet and Extranet).

- TCP/IP Specifies how data is exchanged over the internet by providing end-to-end Communications that identify how it should be broken into packets, addressed, transmitted routed and received at the destination.

- Common TCP/IP protocols include the following:

1) Hyper text Transfer Protocol (HTTP) ⇒ It handles the communication between a web server and a web browser.

2) HTTP Secure ⇒ handles secure Communication between a web server and a web browser.

3) File Transfer Protocol ⇒ It handles transmission of files between Computers.

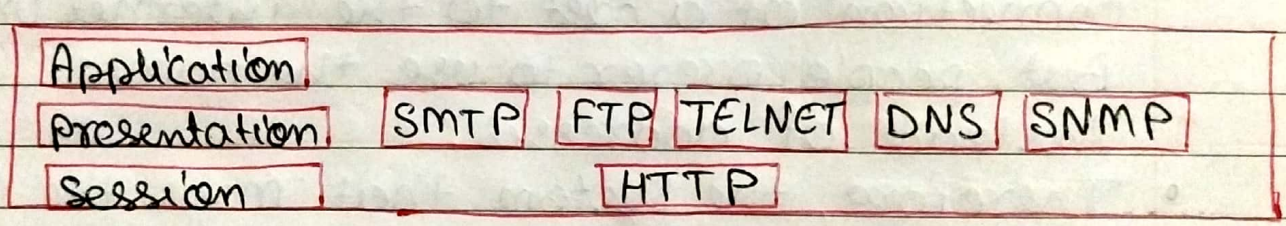
- The TCP/IP model is a Concise version of the OSI model. It Contains four layers, unlike seven layers in the OSI model. The layer are:

1) Application Layer / process
2) Transport Layer / Host-to-Host
3) Internet Layer / Network Layer
4) Network Interface / Link Layer

1) Application Layer ⇒

- 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.
- Example of the application Layer is an application such as file transfer, email, remote login etc.

function and protocols of Application Layer ⇒



- HTTP ⇒ • This protocol allows us to access the data over the world wide web.
- It transfer 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 support the e-mail is known as a Simple mail transfer protocol.
  - This protocol is used to send the data to another e-mail address.

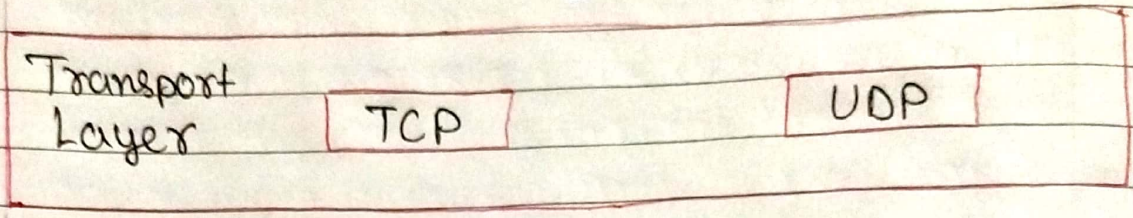
- DNS ⇒ • DNS stands for Domain Name System
  - An IP address is used to identify the Connection of a host to the internet uniquely But, people prefer to use the names instead of addresses.
  - Therefore, the system that maps the Name to the address is known as Domain Name System.

- TELNET ⇒ • It stands for Terminal Network or teletype Network Protocol.
  - 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.

2) 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.

User Datagram Protocol (UDP) ⇒

- It provides Connectionless service and end-to-end delivery of transmission.
- It is an unreliable protocol as it discovers the error but not Specify the error.
- User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.

ICMP (Internet Control message Protocol)

⇒ UDP Consists of the following fields:

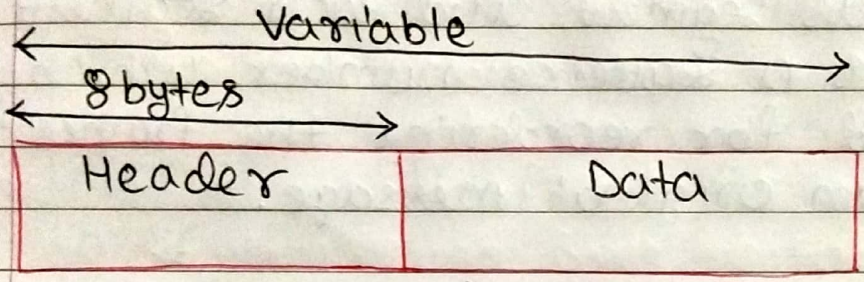
Source port address ⇒ The source port address is the address of the

application program that has Created the message.

Destination port address ⇒ The destination port address is the address of the application program that receives the message.

Total Length ⇒ It defines the total no. of bytes of the user datagram in bytes.

Checksum ⇒ The checksum is a 16-bit field used in Error detection.



Header format

Source port address 16 bit	Destination port address 16 bit
Total length 16 bits	Checksum 16 bits

Transmission Control Protocol (TCP) ⇒

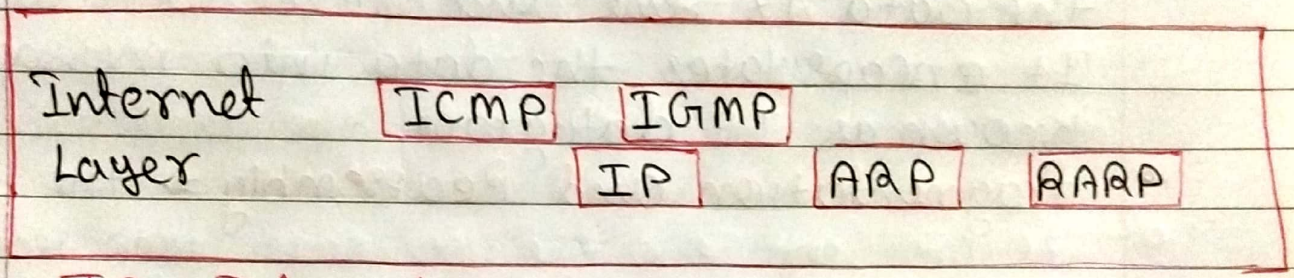
- It provides a full transport Layer services to applications.
- It Creates a virtual Circuit between the Sender and receiver, and it is active for

the duration of the transmission.

- TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
- At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
- At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

3) Internet Layer ⇒

- An 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.



IP ⇒ Internet protocol
ARP ⇒ Address Resolution protocol
ICMP ⇒ Internet Control Message protocol
IGMP ⇒ Internet Group Management Protocol
RARP ⇒ Reverse Address Resolution Protocol.

following are the protocols used in this Layer are: ⇒

1) IP Protocol ⇒ IP protocol is used in this Layer, and it is the most significant part of the entire TCP/IP suite.

following are the responsibilities of this protocol:

- IP addressing ⇒ this protocol implements Logical host addresses known as IP address.
- Host-to-host communication ⇒ It determines the path through which the data is to be transmitted.
- Data Encapsulation and formatting ⇒ An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, It encapsulates the data into message known as IP datagram.
- fragmentation and Reassembly ⇒ the limit imposed on the size of the IP datagram by data link Layer protocol is known as maximum Transmission unit (MTU).
  If the size of IP datagram is greater then the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the Local network.
- Routing ⇒ When IP datagram is sent over the same local network such as LAN, MAN, WAN, It is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly.

2) ARP Protocol ⇒

- ARP stands for Address Resolution Protocol.
- ARP is a network Layer protocol which is used to find the physical address from the IP address.

The two terms are mainly associated with the ARP protocol:

- ARP request ⇒ When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.

- ARP reply ⇒ Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply.

The recipient adds the physical address both to its cache memory and to the datagram header.

3) ICMP Protocol ⇒

- ICMP Stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.

- A datagram travels from router-to-router unit it reaches its destination.

- An ICMP protocol mainly uses two terms:
  ICMP test ⇒ ICMP test is used to test whether the destination is reachable or not.
  ICMP Reply ⇒ ICMP Reply is used to check whether the destination device is responding or not.

- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.

- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the address of the source and destination but not of the router that it is passed to.

4) Network Interface (Access) Layer ⇒

- A Network Layer is the lowest layer of the TCP/IP model.
- A Network 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 function carried out by this Layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP address into physical addresses.
- The protocols used by this Layer are ethernet, token ring, FDDI, X.25, frame relay.

Difference between OSI and TCP/IP Model

OSI Model	TCP/IP Model
1) OSI Stands for Open System Interconnection	1) TCP/IP implies Transmission Control Protocol / Internet Protocol.
2) The OSI model was developed by ISO (International Standard organization) in 1984.	2) The TCP/IP model was developed by ARPANET (Advanced Research Project Agency Network) in 1982.
3) It Consists of 7 Layers: Starting from the bottom they are the physical, data link, Network, Transport, session, Presentation and Application Layer.	3) It Consists of 4 Layers: Starting from the bottom they are the Network Interface, Internet, Transport and Application Layer.
4) The OSI model follows a vertical approach.	4) The TCP/IP model follows a horizontal approach.
5) In the OSI model, the transport Layer provides a guarantee for the delivery of the packets.	5) In TCP/IP transport Layer does not provide the surety for the delivery of packets. But still, we can say that It is a reliable model.

OSI model	TCP/IP model
6) In the OSI model, the Physical Layer and data Link Layer are Seprate Layer.	6) In TCP/IP, Physical and data Link Layers are merged as a single network Layer.
7) In OSI model, the Session and presentation Layers are seprated such as both the Layers are Different.	7) In this model, the Session and presentation Layer are not different Layers. Both Layers are included in the application Layer.

Computer Network Important Questions

Q01⇒ Define Computer networks. Discuss various types of network topologies in a Computer network. Also, discuss various advantages and disadvantages of each topology.

Q 02⇒ What are the applications of Computer networks?.

Q 03⇒ What is OSI Model?. Explain the functions and protocols and services of each Layer.

Q 04⇒ Explain the following :-
(a) LAN
(b) MAN
(c) WAN
(d) ARPANET

Q 05⇒ What is TCP/IP Model?. Explain the functions and protocols and services of each Layer. Compare it with OSI Model.

Q 06⇒ What is IP addressing?. How is it classified? How is subnet addressing performed?.

Q 07⇒ Explain the following :-
a) TCP
b) UDP

Q 08⇒ What are pure ALOHA and slotted ALOHA? Consider the delay of both at low load. Which one is less? Explain your answer.

Q 09⇒ Explain in detail CSMA Protocol in detail.

Q 10⇒ Explain in detail CSMA/CD protocol in detail, How it detects a collision.

Q 11⇒ What is IPV6? Explain its advantages over IPV4. Also, Explain its frame format.

Q 12⇒ Explain the following :-
a) firewall
b) IP address
c) Subnet mask
d) DNS
e) peer-to-peer network and served-based N/w.

Q 13⇒ What are the HTTP and HTTPS protocol?

Q 14⇒ What do you mean by ICMP protocol and DHCP protocol?

Q 15⇒ Compare hub, switch, router, Gateway.

Q 16⇒ What is the Difference between the ipcofig and the ifConfig?

Q 17⇒ What are Unicasting, Anycasting, multicasting, and Broadcasting?

Q 18⇒ What are Private and Special IP addresses?

Q 19 ⇒ What do you mean by Cryptography ? Explain Different types of Cryptography.

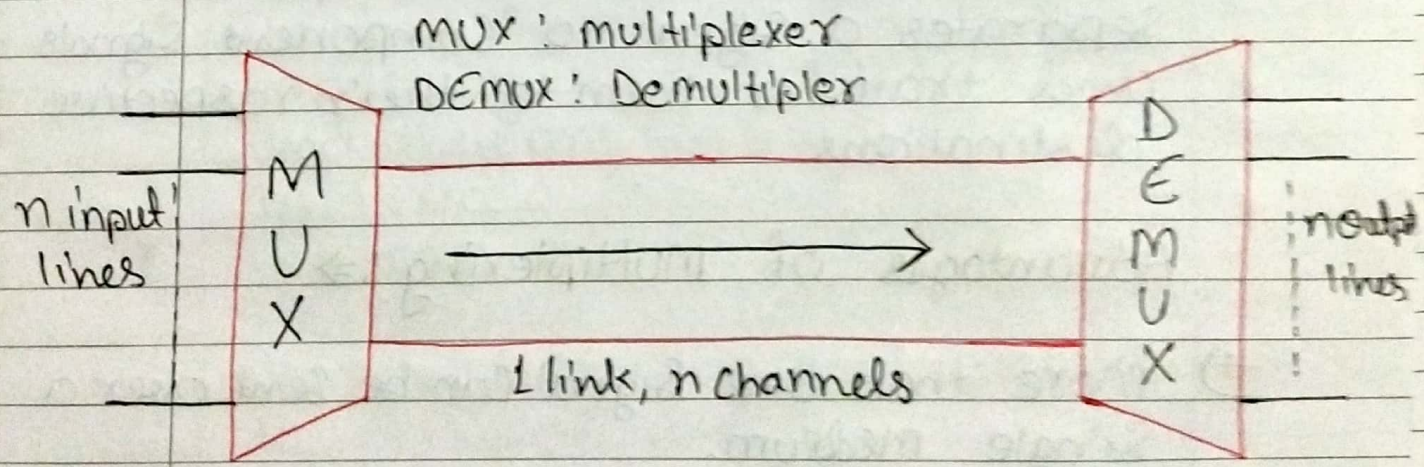
Q 20 ⇒ Consider building a CSMA/CD network running at 1 Gbps over a 1 km cable with no repeaters. The signal speed in the cable is 200,000 km/sec. What is the minimum frame size ?

OR

A Large FDDI ring has 100 stations & a token rotation time of 40msec. The token holding time is 10 msec. What is the maximum achievable efficiency of the ring ?

What is multiplexing

- Multiplexing is a technique used to combine and send the multiple data streams over a single medium.
- The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as multiplexer.
- Multiplexing is achieved by using a device called multiplexer (MUX) that combines n input lines to generate a single output line. Multiplexing follows many to one such as n input lines and one output line.
- Demutiplexing is achieved by using a device called Demultiplexer (DEMUX) available at the receiving end. DEMUX separates a signal into its component signals (one input and n outputs). Therefore we can say that demultiplexing follows the one-to-many approach.



History of Multiplexing ⇒

- Multiplexing technique is widely used in telecommunications in which several telephone calls are carried through a single wire.
- Multiplexing originated in telegraphy in the early 1870s and is now widely used in communication.

Concept of Multiplexing ⇒

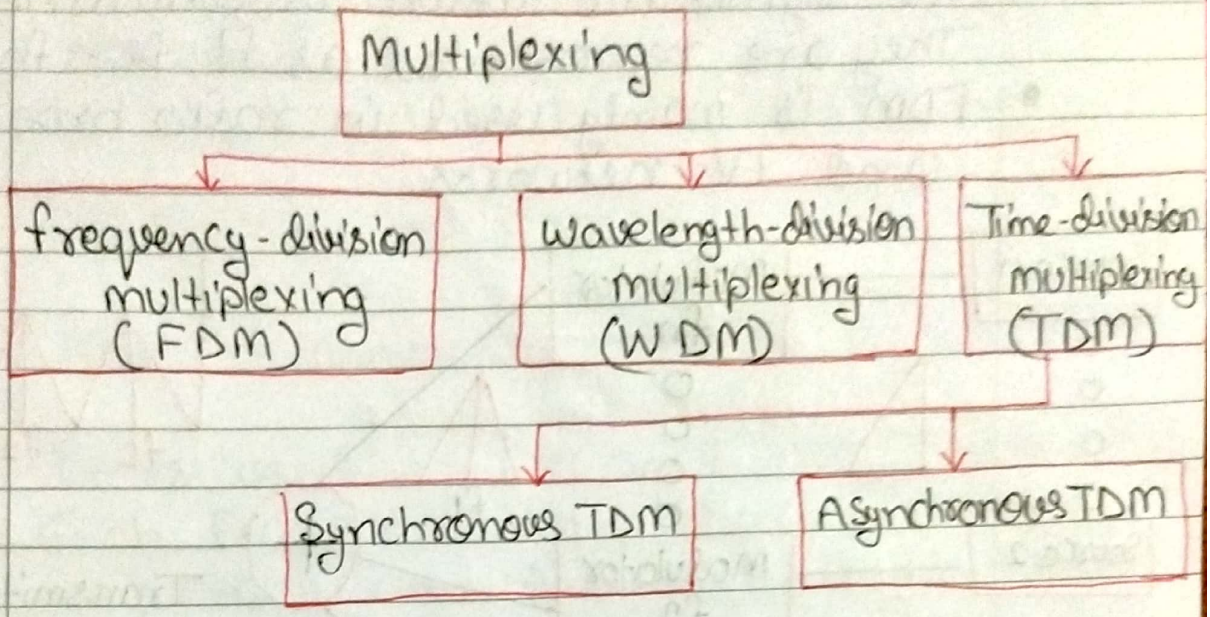
- The n input lines are transmitted through a multiplexer and mutiplexer combines the signals to form a composite signal.
- The composite signal is passed through a Demultiplexer and demultiplexer separates a signal to component signals and transfer them to their respective destinations.

Advantages of Multiplexing :⇒

1) more than one signal can be sent over a single medium.
2) The bandwidth of a medium can be utilized effectively.

Multiplexing Techniques

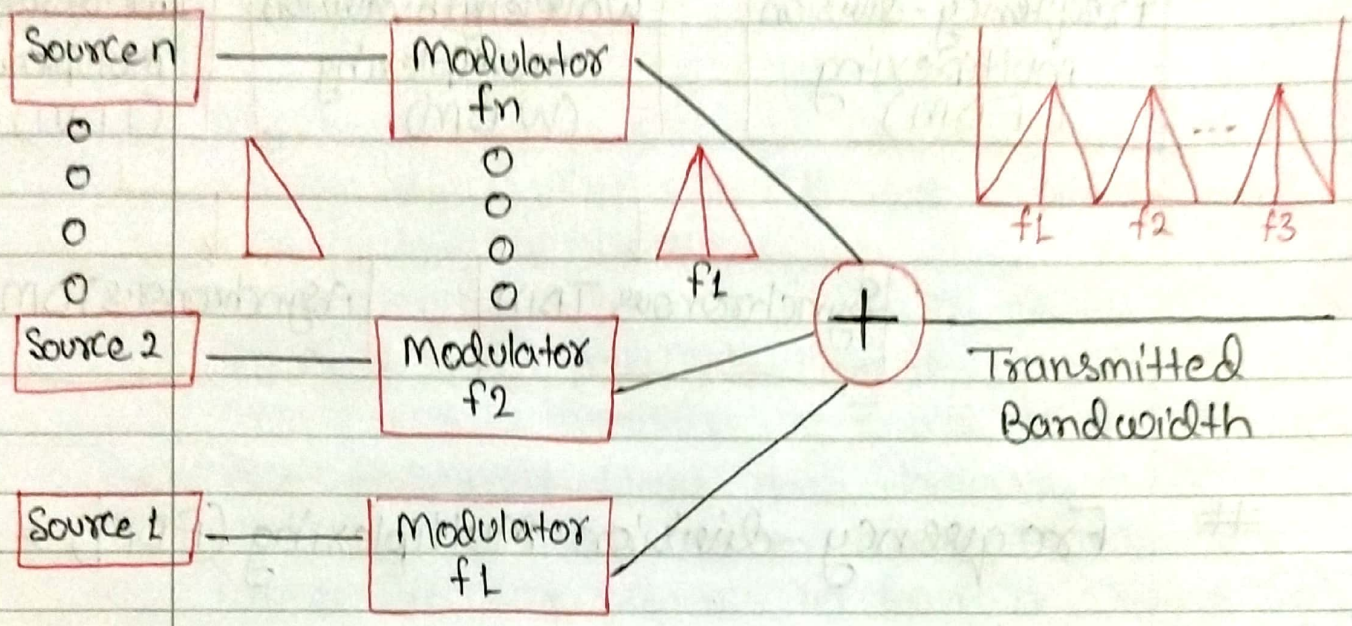
Types of multiplexing



Frequency-division Multiplexing (FDM) ⇒

- It is an analog technique.
- FDM is a technique in which the available bandwidth of a single transmission medium is subdivided into several channels.
- The input signals are translated into frequency bands by using modulation techniques, and they are combined by a multiplexer to form a composite signal.
- The main aim of the FDM is to subdivide the available bandwidth into different frequency channels and allocate them to different devices.
- Using the modulation technique, the input signals are transmitted into frequency bands and them combined to form a composite signal.

- The Carriers which are used for modulating the Signals are known as Sub-Carriers. They are represented as f1, f2, -- fn.
- FDM is mainly used in radio broadcasts and TV networks.



Advantages of FDM :⇒

- FDM is used for analog signals.
- FDM process is very simple and easy modulation.
- A Large number of signals can be sent through an FDM simultaneously.
- It does not require any synchronization between sender and receiver.

Disadvantages of FDM :⇒

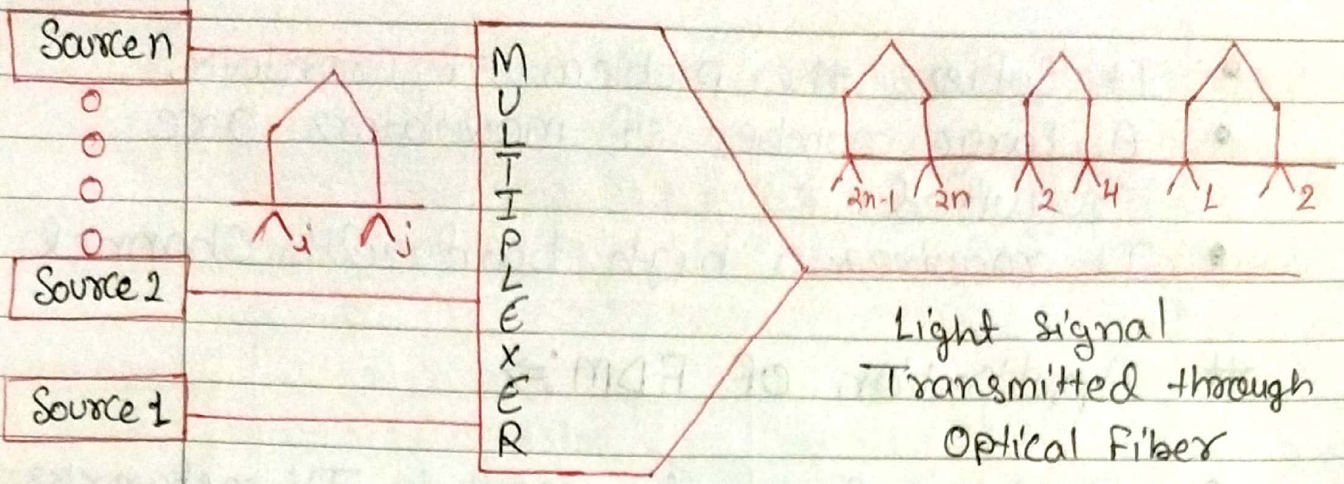
- FDM technique is used only when Low-Speed channels are required.

- It suffers the problem of crosstalk.
- A large number of modulators are required.
- It requires a high bandwidth channel.

Application of FDM :⇒

- FDM is commonly used in TV networks.
- It is used in FM and AM broadcasting. Each FM radio station has different frequencies, and they are multiplexed to form a composite signal. The mutiplexed signal is transmitted in the air.

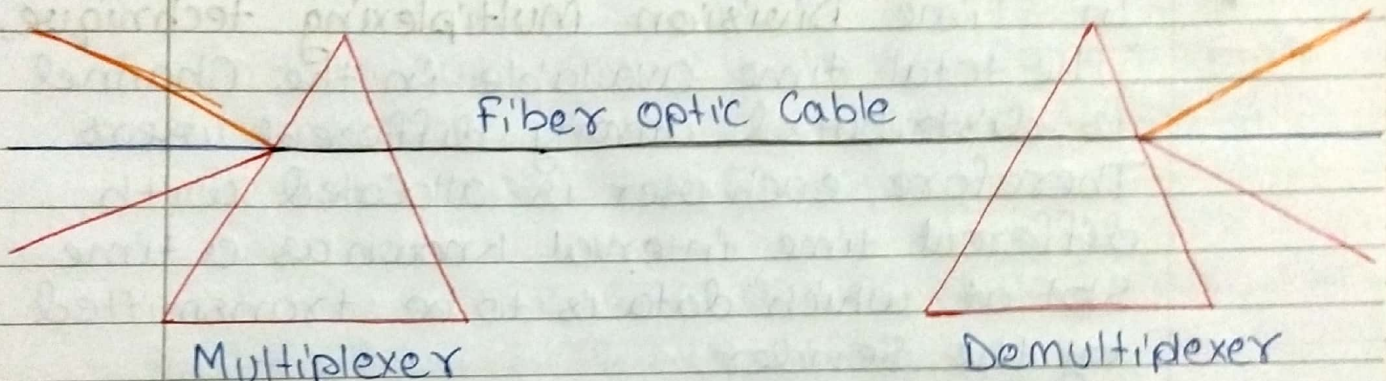
Wavelength Division Multiplexing (WDM)



WDM Transmitter

- Wavelength Division Multiplexing is same as FDM except that the optical signals are transmitted through the fibre optic cable.
- WDM is used on fibre optics to increase the capacity of a single fibre.
- It is used to utilize the high data rate capability of fibre optic cable.
- It is an analog multiplexing technique.
- Optical signals from different source are combined to form a wider band of light with the help of multiplexer.
- At the receiving end, demultiplexer separates the signals to transmit them to their respective destinations.
- Multiplexing and Demultiplexing can be achieved by using a prism.

- Prism can perform a role of multiplexer by combining the various optical signals to form a composite signal, and the composite signal is transmitted through a fibre optical cable.
- Prism also performs a reverse operation, such that demultiplexing the signal.



Time Division Multiplexing (TDM)

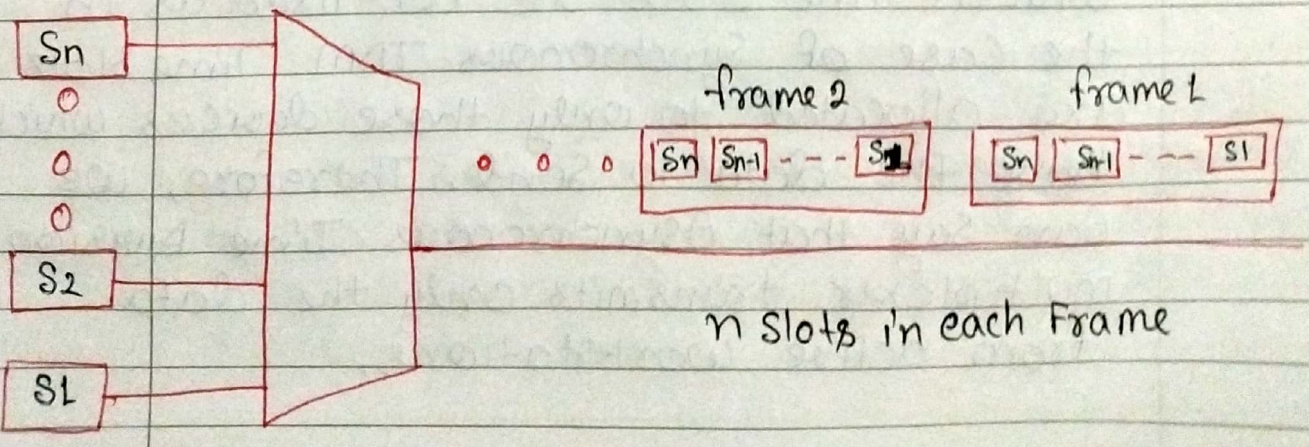
- It is a digital Technique.
- In frequency Division multiplexing Technique, all signals operate at the same time with different frequency, but in case of Time Division multiplexing technique, all signals operate at the same frequency with different time.
- In Time Division multiplexing technique, The total time available in the channel is distributed among different users. Therefore, each user is allocated with different time interval known as a time slot at which data is to be transmitted by the sender.
- A user takes control of the channel for a fixed amount of time.
- In time Division multiplexing technique, data is not transmitted simultaneously rather the data is transmitted one-by-one.
- In TDM, the signal is transmitted in the form of frames. Frames contain a cycle of time slots in which each frame contains one or more slots dedicated to each user.

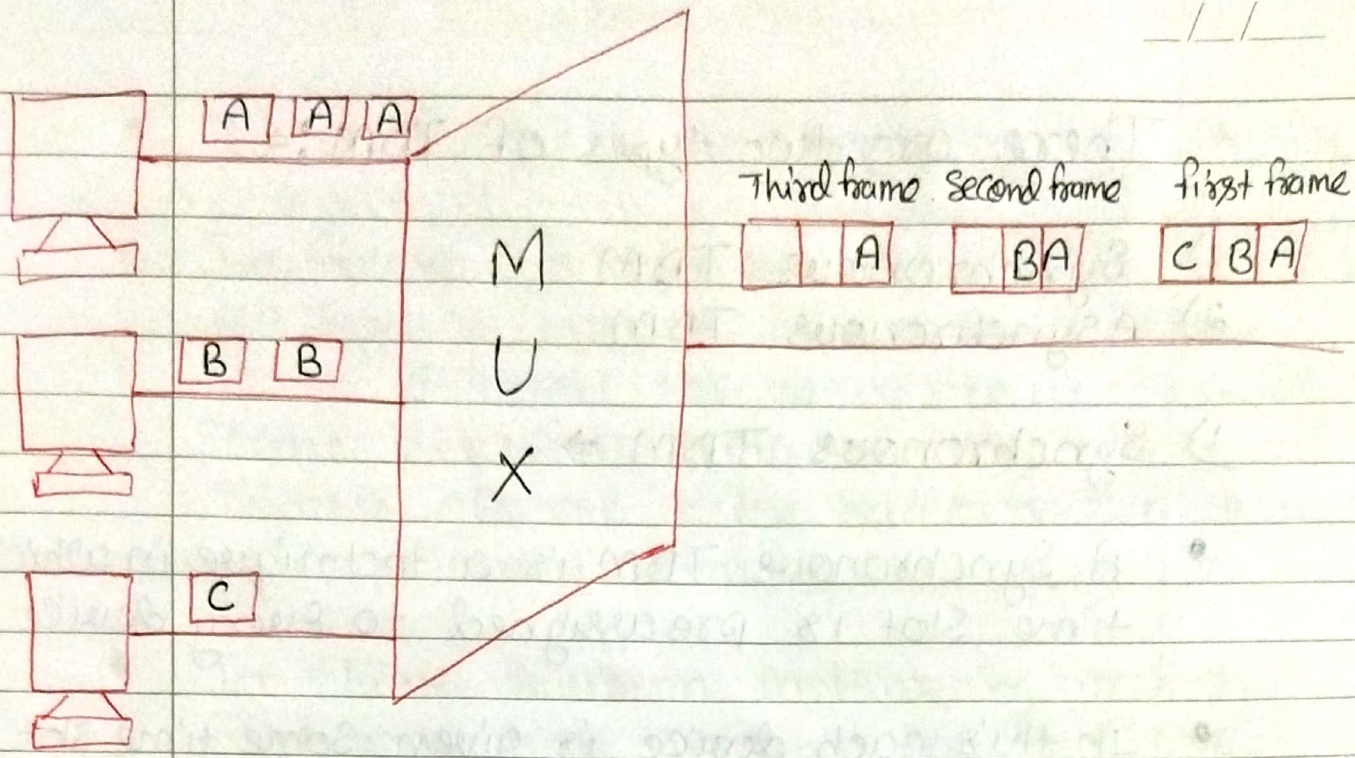
There are two types of TDM :→

1) Synchronous TDM
2) ASynchronous TDM

1) Synchronous TDM ⇒

- A Synchronous TDM is a technique in which time slot is pre-assigned to every device.
- In this each device is given some time slot irrespective of the fact that the device Contains the data or not.
- If the device does not have any data, then the slot will remain empty.
- In Synchronous TDM, signals are sent in the form of frames. Time slots are organized in the form of frames. if a device does not have data for a particular time slot, then the empty slot will be transmitted.
- If there are n devices, then there are n slots.



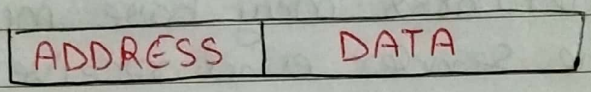


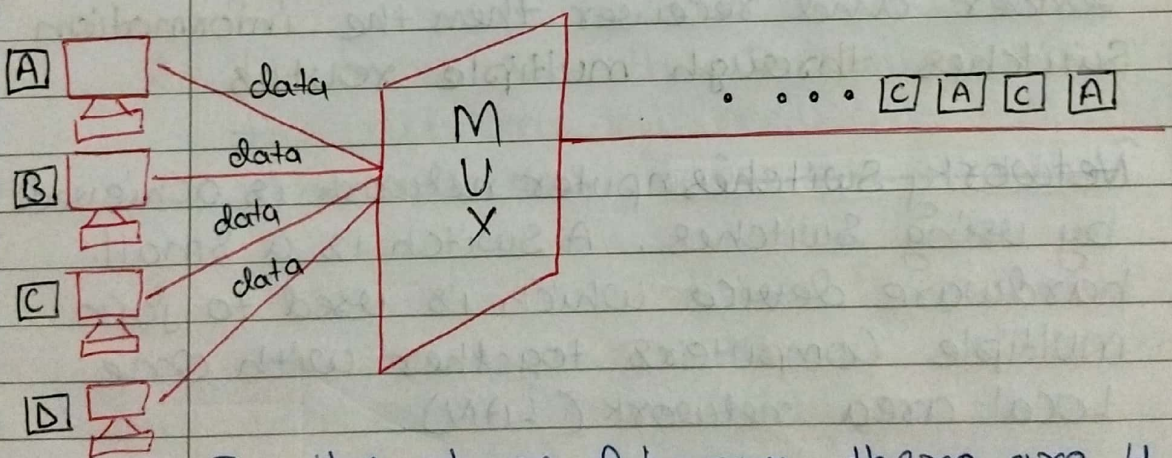
In the given figure, the Synchronous TDM technique is implemented. Each device is allocated with some time slot. The time slots are transmitted irrespective of whether the sender has data to send or not.

2) Asynchronous TDM ⇒

- An Asynchronous TDM is also known as Statistical TDM.
- An asynchronous TDM is a technique in which time slots are not fixed as in the case of Synchronous TDM. Time slots are allocated to only those devices which have the data to send. Therefore, we can say that Asynchronous Time Division multiplexer transmits only the data from active workstations.

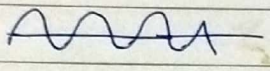
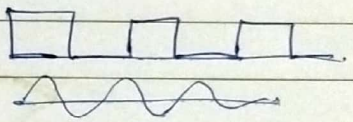
- An asynchronous TDM technique dynamically allocates the time slots to the device.
- In Asynchronous TDM, total speed of the input lines can be greater than the capacity of the channel.
- Asynchronous Time Division multiplexer accepts the incoming data streams and creates a frame that contains only data with no Empty slots.
- In Asynchronous TDM, each slot contains an address part that identifies the source of the data.





In the above diagram, there are 4 devices, but only two devices are sending the data such as A and C. Therefore, the data of A and C are only transmitted through the transmission line.

Difference between FDM TDM & WDM

FDM (frequency Division multiplexing)	TDM Time Division multiplexing	WDM Wavelength Division multiplexing
1) FDM has multiple data signals Combined for Simultaneous transmission via a Shared Communication medium. 	1) TDM allows multiple users to send signals over a Common Channel by allocating fixed time slot for each user. 	1) WDM modulates data streams, optical carrier signals of varying wavelength into a single light beams via a single optical fiber. 
2) FDM uses analog signals	2) TDM uses digital and analog signals	2) WDM uses optical signals.
3) FDM divides the bandwidth into smaller frequency ranges antransmitsser transmit data simultaneously through a Common Channel within their frequency range.	3) TDM allocates a fixed time slot for each user to send signals through a Common Channel. User gets the entire bandwidth within that time slot	3) WDM Combines multiple light beams from several channels and combine them to a single light bean and sends through a fibre optic strand similar to FDM.

Switching

- Switching refers to the process of directing a network traffic from one device or path to another.
- It is a important Component in Computer networking that enables data to be transmitted efficiently between multiple devices on a network.
- Switching is the mechanism in Computer network that helps in deciding the best route for data transmission if there are multiple paths in a Larger network.
- Larger networks may have multiple routes to link the sender and receiver. So whenever we send by information between the sender and receiver then the information Switches through multiple routes.
- 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).
- Network Switches operates at Layer 2 Data Link Layer in the OSI model.

- 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 model.
- 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 :⇒

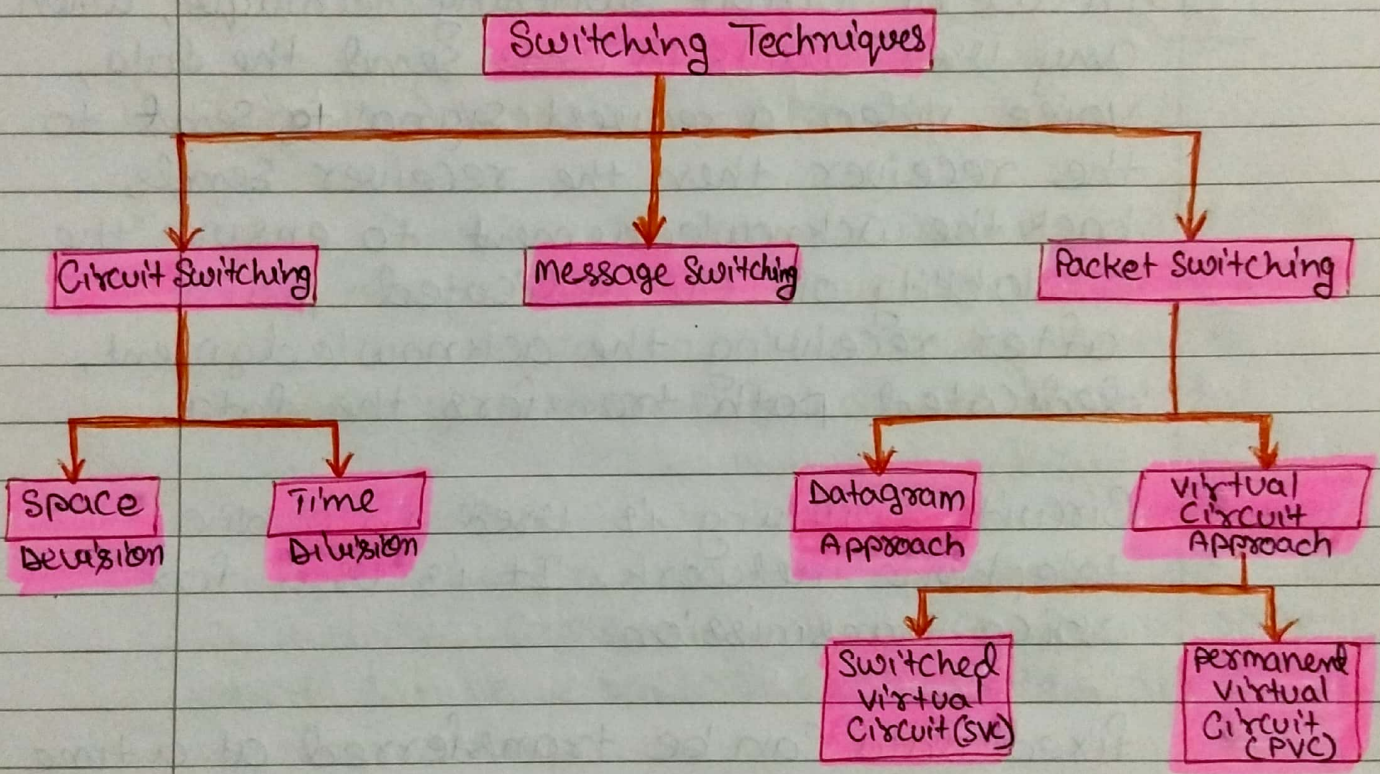
- A Switch is more expensive than network bridges.

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

Switching techniques

- In Large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.
- Switching technique is used to connect the systems for making one-to-one communication.

Classification of Switching Techniques



1) Circuit Switching ⇒

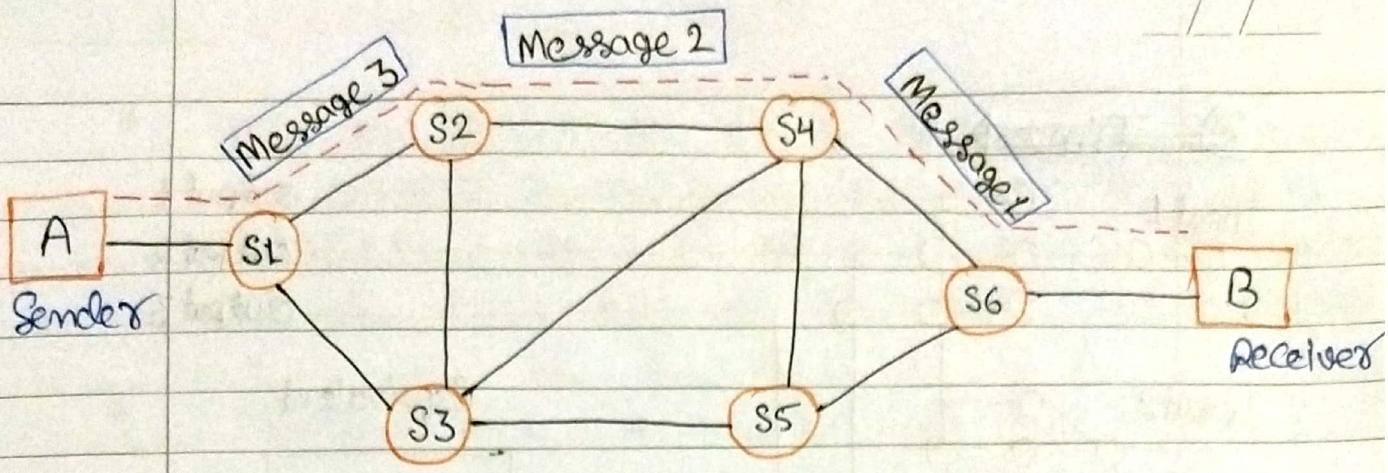
- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the

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 acknowledgement 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.

Communication through Circuit Switching has 3 phases:

1) Circuit establishment
2) Data transfer
3) Circuit Disconnect.



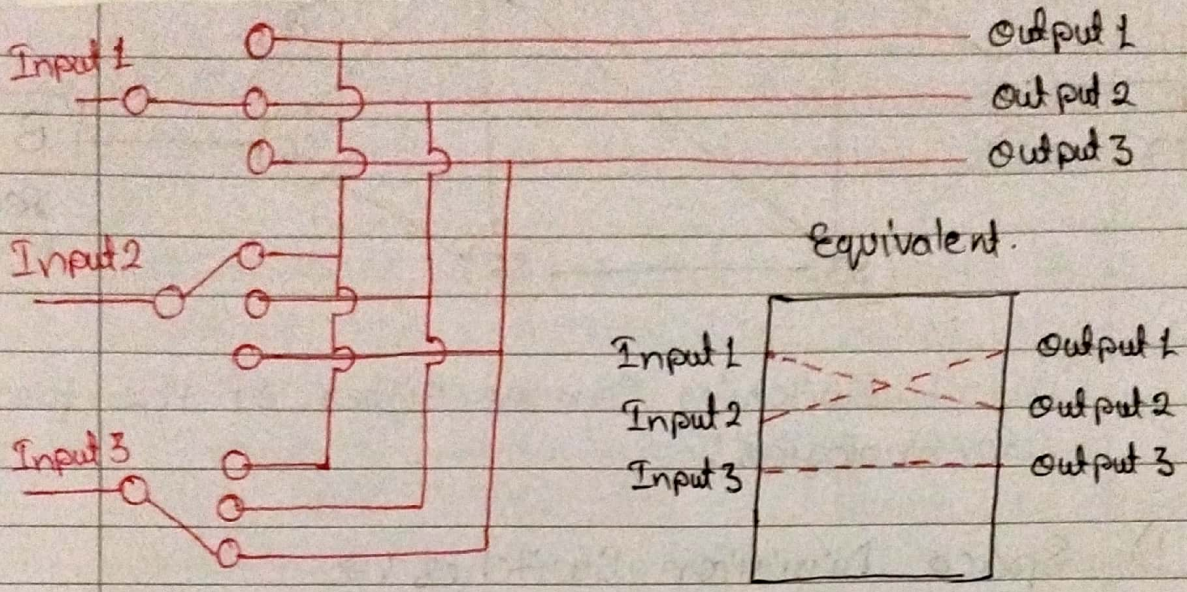
Circuit Switching can use either of the two technologies:

1) Space Division Switches :⇒

- Space Division switching is a circuit switching technology in which a single transmission path is accomplished in a switch by using a physically separate set of crosspoints.
- Space Division Switching can be achieved by using Crossbar Switch. A Crossbar Switch is a metallic crosspoint or semiconductor gate that can be enabled or disabled by a control unit.
- Space Division Switching has high speed, high capacity and nonblocking switches.

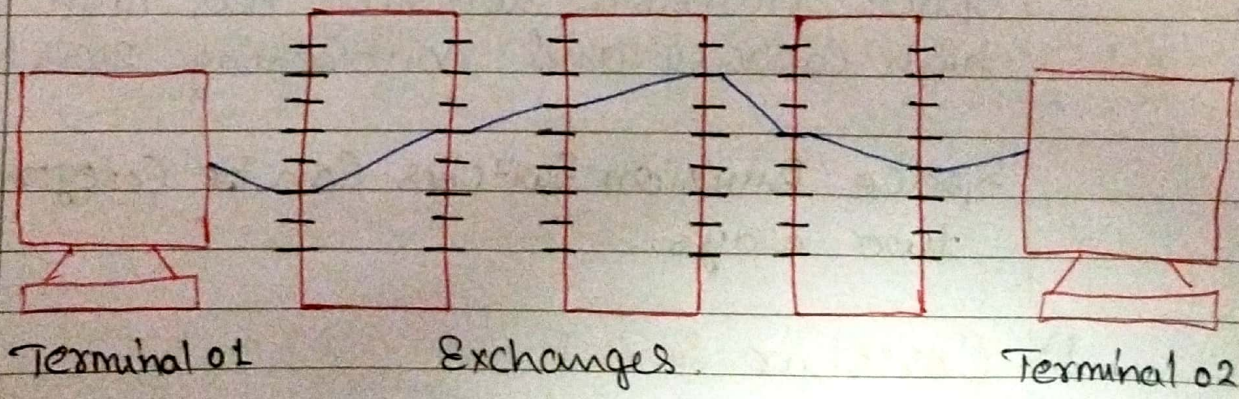
Space Division Switches can be categorized in two ways.

1) Crossbar Switch
2) multistage Switch



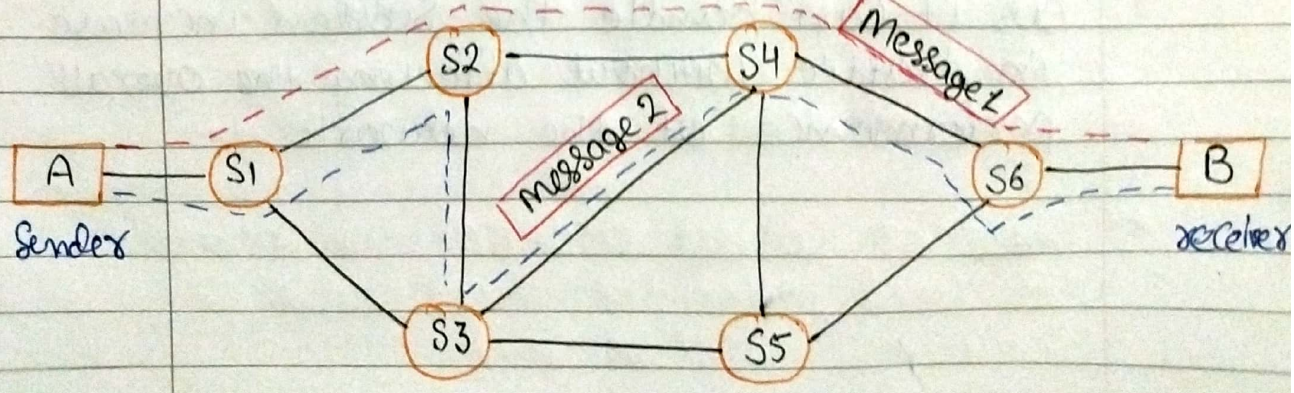
2) Time Division Switching ⇒

- Time division switching comes under digital switching techniques.
- The incoming and outgoing signals when received and re-transmitted in a different time slot, is called Time Division Switching.
- Time Division Switching is sharing of crosspoint.



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.
- There is no dedicated path established between the sender and receiver in message switching, as in Circuit switching.
- 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.



Advantages of Message Switching :⇒

1) Reliability ⇒ Message Switching is a reliable form of communication as it ensures the delivery of messages even if some packets are lost or delayed.

2) Scalability ⇒ The network can be easily Expanded as the number of users grows, making it ideal for Large -Scale Communication Systems.

3) Cost-Effectiveness ⇒ Message Switching is more Cost-Effective than other forms of Communication because it allows multiple messages to be transmitted simultaneously over the same Communication lines.

4) Flexibility ⇒ Message Switching allows for flexible Communication as it enables the transmission of messages of varying lengths and formats.

5) Robustness ⇒ Message Switching is a robust form of Communication as it can handle the sudden increase in traffic without affecting the overall performance of the network.

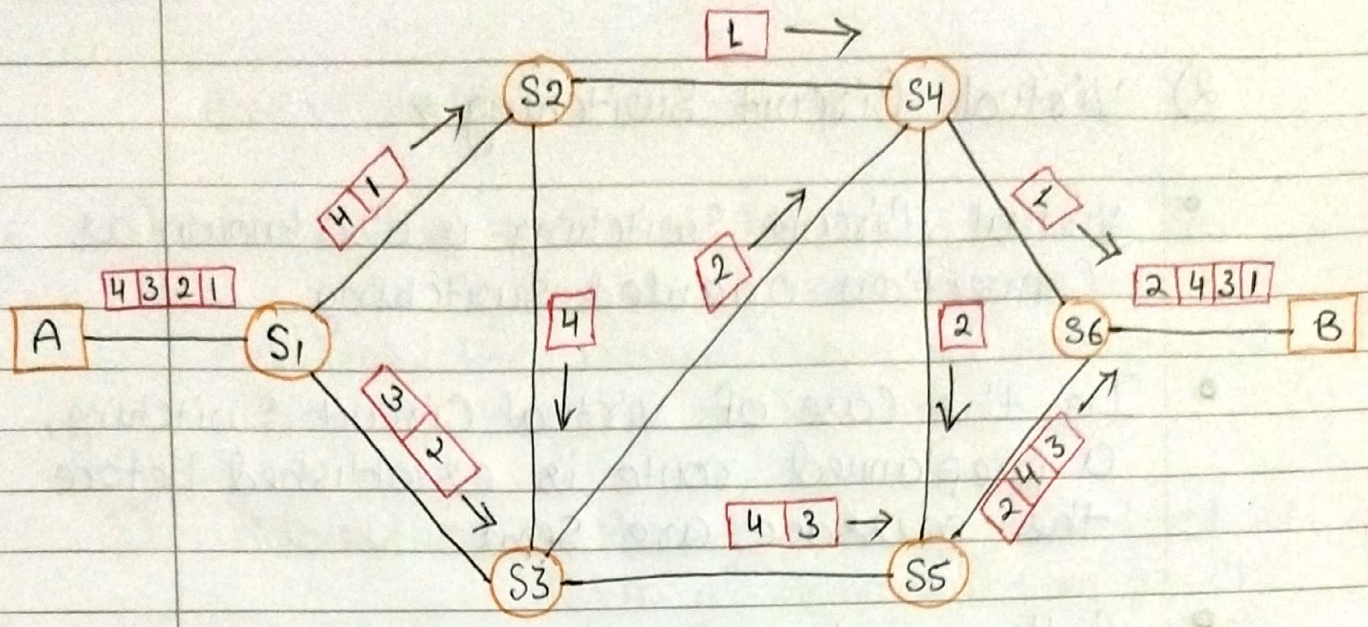
Disadvantages of Message Switching ⇒

1) The message switches must be equipped with sufficient storage to enable them to store the message until the message is forwarded.

2) The long delay can occur due to the storing and forwarding facility provided by the message switching technique.

Packet Switching

- In Packet Switching, when we send a message, then the whole message is divided into smaller pieces called packets. These pieces or packets travel across the network and take the shortest path possible.
- Every packet has a sequence number to identify its order at the receiving end.
- Each packet contains some information including a source address, a destination address, intermediate node address information, sequence number etc. so that individual packets can be routed through the internetwork independently. This method allows for more efficient use of network resources and enables multiple transmissions to occur simultaneously.
- Packet 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 acknowledgement message will be sent.



Approaches of Packet Switching :⇒

There are two approaches to Packet Switching:

1) 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 packet are reassembled at the receiving end in correct order.
- In Datagram Packet switching technique, the path is not fixed.
- It is also known as Connectionless Switching.

2) Virtual Circuit Switching ⇒

- Virtual Circuit Switching is also known as Connection-oriented switching.
- In the case of Virtual Circuit Switching, a preplanned route is established before the message 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.

Advantages of Packet Switching

1) Efficiency ⇒ Packet Switching allows for efficient use of network resources by breaking data into small packets and transmitting them individually.

2) Scalability ⇒ Packet Switching is scalable and can accommodate a growing number of users and devices.

3) Cost-effectiveness ⇒ Packet Switching is more Cost-effective than other forms of Communication because it allows multiple transmissions to occur simultaneously

over the same Communication Lines.

4) Flexibility ⇒ Packet Switching allows for flexible Communication as it enables the transmission of packets of varying lengths and formats.

5) Robustness ⇒ Packet Switching is a robust form of Communication as it can handle the sudden increase in traffic without affecting the overall performance of the network.

Difference Between Circuit Switching, Message Switching and Packet Switching

	Circuit Switching	Message Switching	Packet Switching
1)	There is physical Connection b/w transmitter and receiver	1) No physical path is set in advance b/w transmitter and receiver	1) No physical path is established b/w transmitter and receiver
2)	All the packet uses same path	2) Packet are stored and forward	2) Packet travels Independently.
3)	Need an end to end path before the data transmission	3) No need of end to end path before data transmission	3) No need of end to end path before data transmis
4)	There is one big entire data stream Called a message.	4) There is one big entire data stream Called a message	4) The big message is divided into a small number of Packets.
5)	Message arrives in sequence	5) Message arrives in sequence	5) Packets do not appear in sequence at the destination.
6)	Low Transmission Capacity	6) maximum transmission Capacity	6) maximum transmission Capacity.
7)	Waste of bandwidth is possible	7) No waste of bandwidth	7) No waste of bandwidth
8)	Not Suitable for handling interactive traffic	8) Suitable for handling interactive traffic	8) Suitable for handling interactive traffic

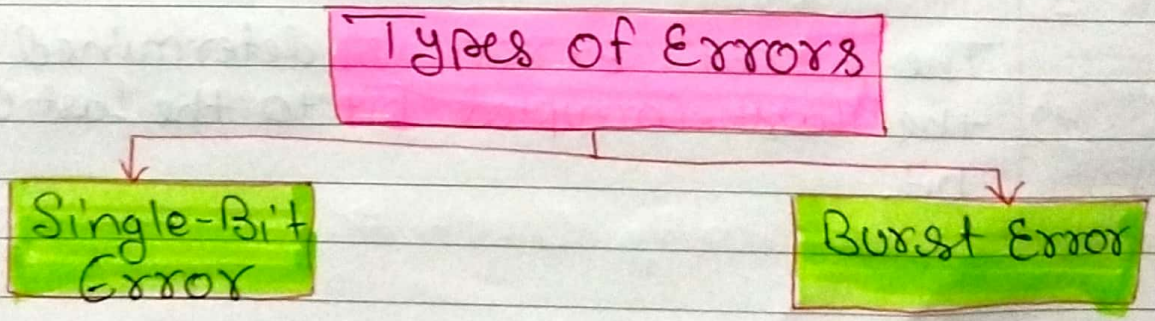
Error Detection

110101 → 00101

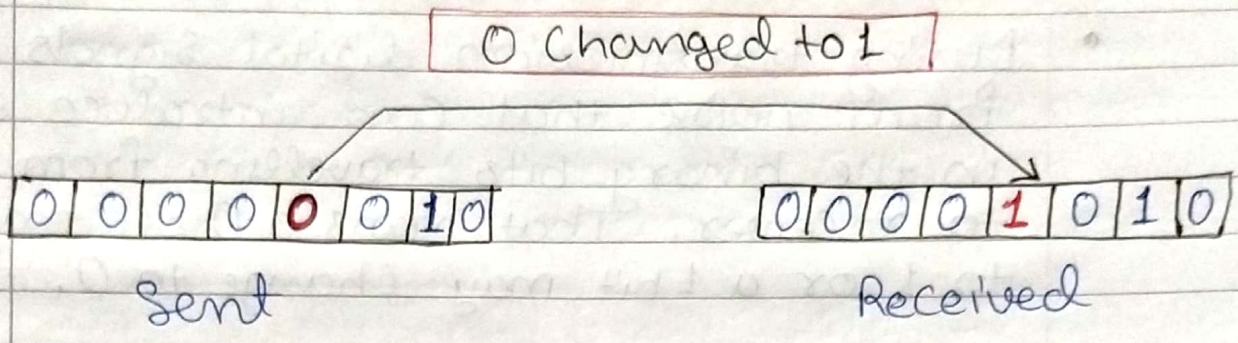
Error ⇒ • A condition when the receiver's information does not match with the sender's information.

- During transmission, digital signals suffer from noise that can introduce error in the binary bits travelling from sender to receiver. That means a 0 bit may change to 1 or a 1 bit may change to 0.
- When data is transmitted from one device to another device, the system does not guarantee whether the data received by the device is identical to the data transmitted by another device.
- An Error is a situation when the message received at the receiver end is not identical to the message transmitted.

Types of Errors.



Single-Bit Error:⇒ The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.



In the above example, the message which is sent is corrupted as single-bit such as 0 bit is changed to 1.

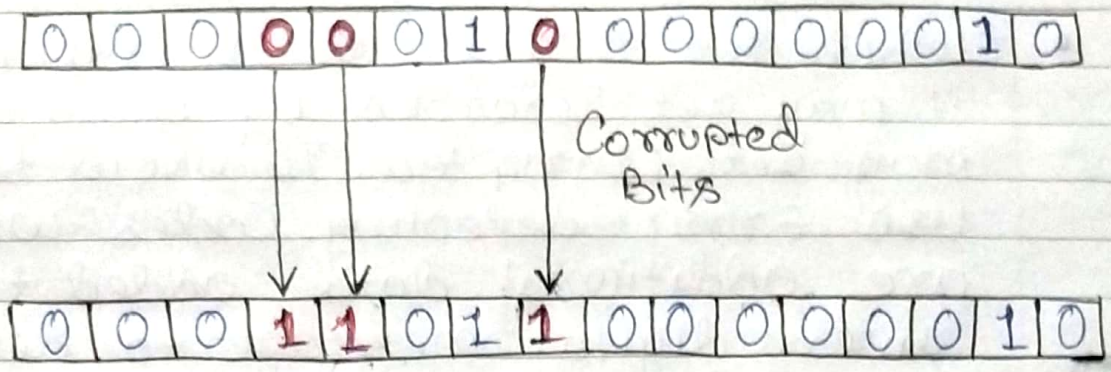
Single-Bit Error mainly occurs in Parallel Data Transmission.

Burst Error:⇒ The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.

The Burst error is determined from the first corrupted bit to the last corrupted bit.

Length of the Burst Error is 5

Sent



Received

- The duration of noise in Burst Error is more than the duration of noise in Single-Bit.
- Burst Errors are most likely to occurr in Serial Data Transmission.
- The number of affected bits depends on the duration of the noise and data rate.

Error Detection Codes

- Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if any error has occurred during transmission of the message.

- Basic approach used for error detection is the use of redundancy bits, where additional bits are added to facilitate detection of error.

Error Detecting Techniques :⇒

The most popular Error Detecting techniques are :⇒

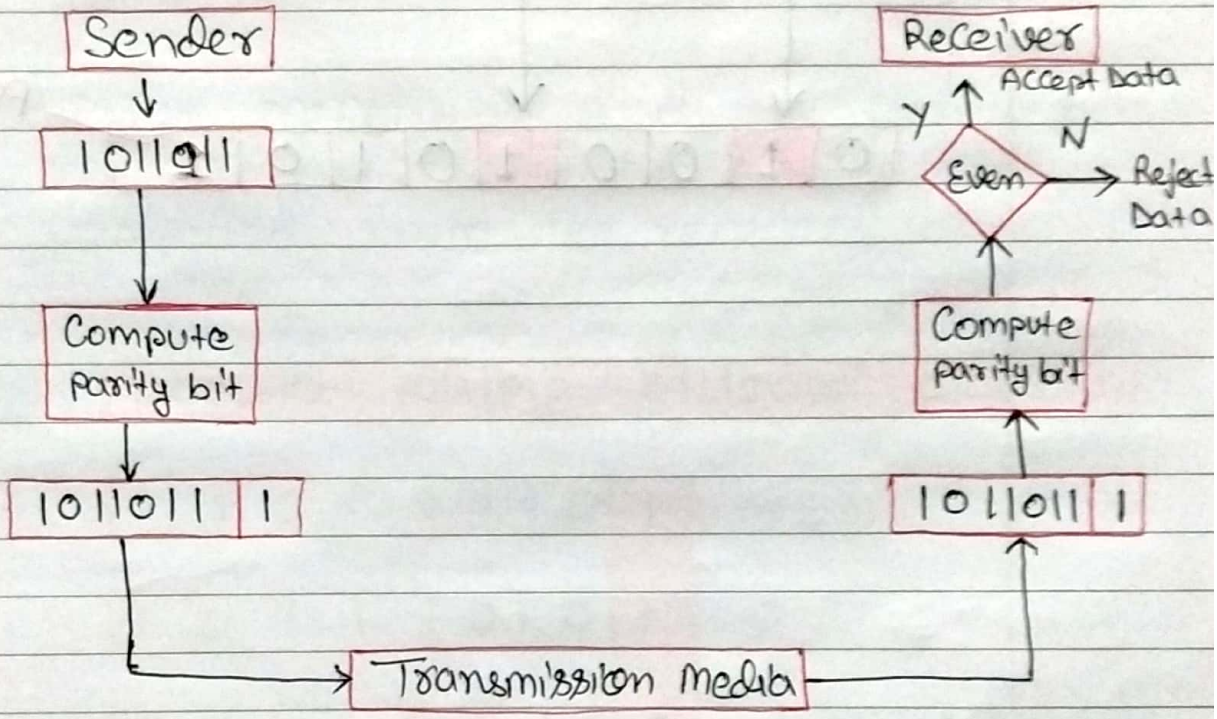
1) Single parity check
2) Two-dimensional parity check
3) Checksum
4) Cyclic redundancy check (CRC)

Single Parity Check ⇒

- Single Parity checking is the simple mechanism and inexpensive to detect the errors.

- In this technique, a redundant bit is also known as parity bit which is appended at the end of the data unit so that the number of 1s becomes even. Therefore, the total number of transmitted bits would be 9 bits.

- If the number of 1's bits is odd, then parity bit 1 is appended and if the number of 1s bits is even, then parity bit 0 is appended at the end of the data unit.

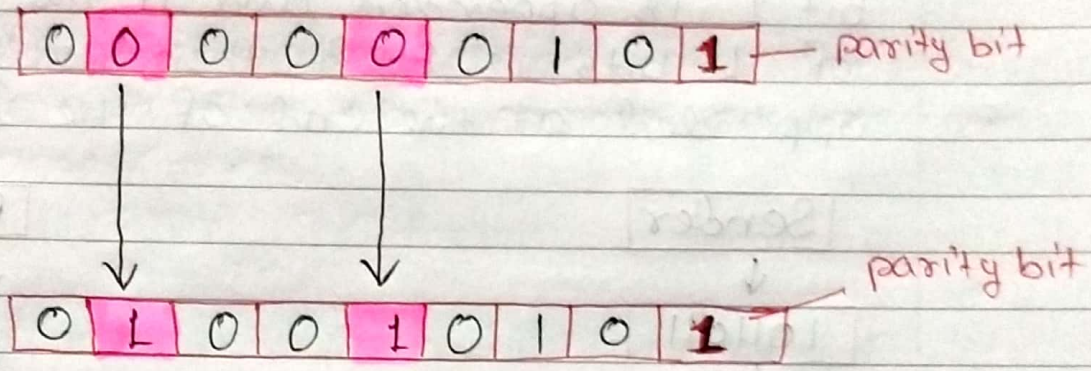


- At the receiving end, the parity bit is calculated from the received data bits and compared with the received parity bit.

- This technique generates the total number of 1s even, so it's known as even-parity checking.

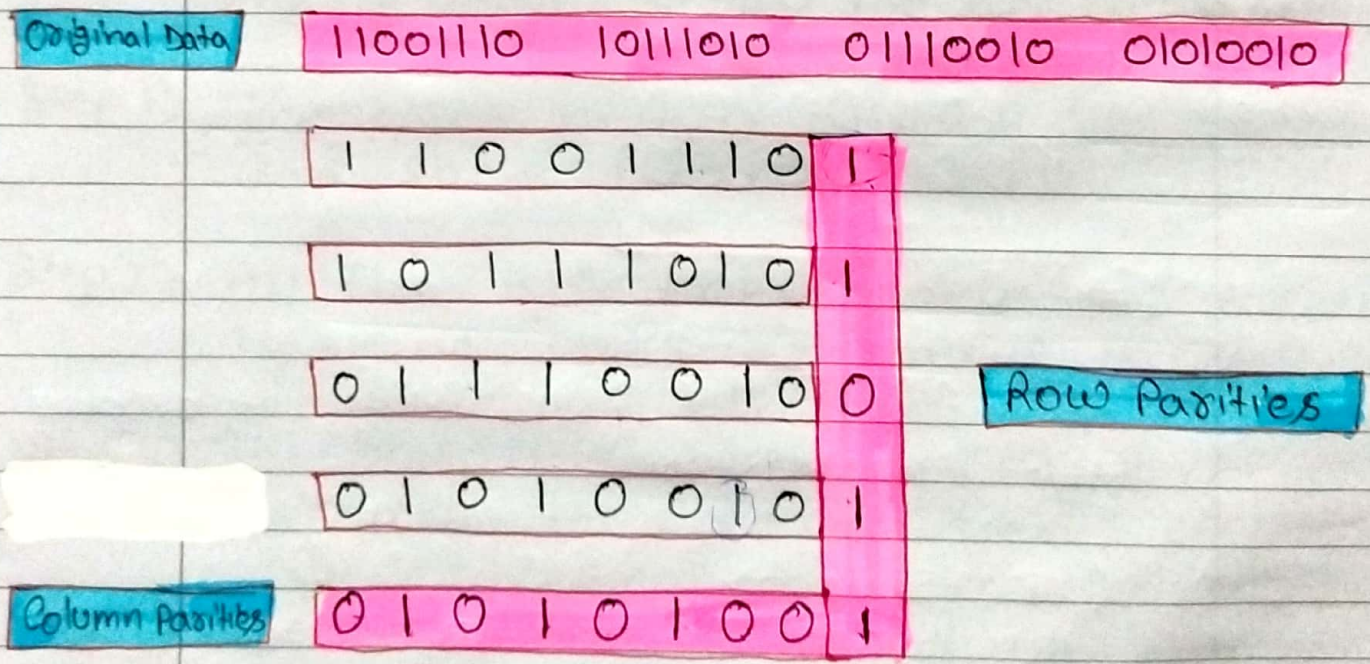
Drawbacks of Single Parity Checking ⇒

- It can only detect single-bit errors which are very rare.
- If two bits are interchanged, then it cannot detect the errors.



Two-Dimensional Parity check

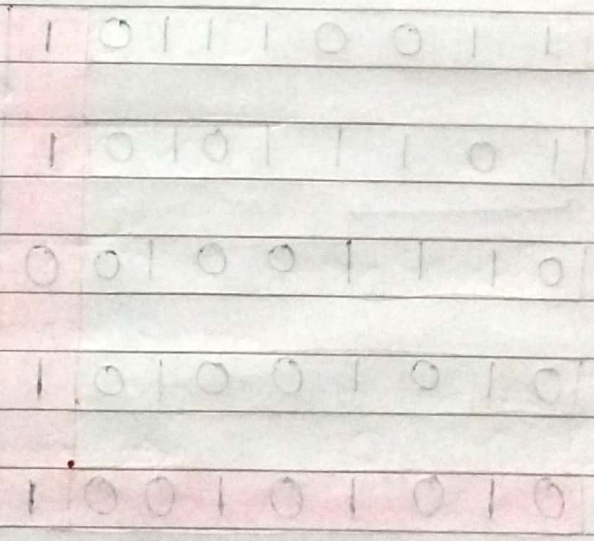
- Performance Can be improved by using Two-Dimensional Parity check which organizes the data in the form of a table.
- Parity Check bits are Computed for each row, which is Equivalent to the single-parity check.
- In Two-Dimensional Parity Check, a block of bits is devided into rows and the redundant row of bits is added to the whole block.
- At the receiving end, the parity bits are compared with the parity bits Computed from the received data.



Drawbacks of 2D Parity Check

- If two bits in one data unit are corrupted and two bits exactly the same position in another data unit are also corrupted, then 2D parity checker will not be able to detect the error.

- This technique cannot be used to detect the 4-bit errors or more in some cases.



Checksum

A Checksum is an Error detection technique based on the Concept of redundancy.

It is divided into two parts:

1) **Checksum Generator** ⇒ • A Checksum is generated at the Sending Side.
   - Checksum generator subdivides the data into equal segments of n bits each, and all these segments are added together by using one's Complement arithmetic.
   - The Sum is Complemented and appended to the original data, known as Checksum field. The Extended data is transmitted across the network.

The sender follows the given steps:

Step 1) The block unit is divided into k sections, and each of n bits.

Step 2) All the k sections are added together by using one's Complement to get the Sum

Step 3) The Sum is Complemented and it becomes the Checksum field.

Step 4) The original data and Checksum field are Send across the network.

Ex ⇒

original data

10011001	11100010	00100100	10000100
1	2	3	4

Step 1) ⇒

K = 4 , m = 8

divide the Block into K (K=4) section and each section m (m=8) bits.

Step 2) ⇒ All K section are added using 1's Complement.

Section 1 → 10011001

Section 2 ⇒ 11100010

(1) 01111011

→ 1

01111100

Section 3 ⇒ 00100100

10100000

Section 4 ⇒ 10000100

(1) 00100100

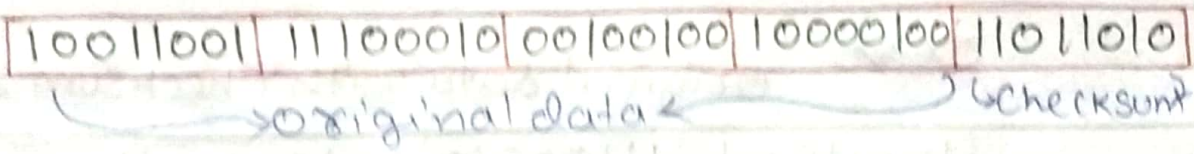
→ 1

Sum ⇒ 00100101

Step 3) Complement the Sum and it become the Check Sum.

Checksum ⇒ 11011010

Step 4) The original data with attached checksum send in network



These data send in network.

2) **Checksum Checker** ⇒ A Checksum is verified at the receiving side. The receiver subdivides the incoming data into equal segments of n bits each, and all these segments are added together, and then this sum is complemented. If the complement of the sum is zero, then the data is accepted otherwise data is rejected.

The Receiver follows the given steps:

Step1) The block unit is divided into k sections and each of n bits.

Step2) All the k section are added together by using one's complement algorithm to get the sum.

Step3) The sum is complemented.

Step4) If the result of the sum is zero, then the data is accepted otherwise the data is discarded.

Ex ⇒ original data with Checksum send by sender

10011001	11100010	00100100	10000100	11011010

← original data → Checksum

Step 1) The block unit is divided into k (k=5) section and each section m (m=8) bits.

k = 4 , m/n = 8

Step 2) All k section are added using 1's Complement

Section 1 → 10011001

Section 2 ⇒ 11100010

10111101 + 1 (carry)

01111100

Section 3 ⇒ 00100100

10100000

Section 4 ⇒ 10000100

10010010 + 1 (carry)

00100101

Section 5/Check Sum 11011010

11111111 → Sum

Step (3) ⇒ Sum is Complemented ⇒ 00000000

Step 4 ⇒ Complement of sum is all zero's so data is accepted.

Conclusion: Accept Data

Cyclic Redundancy Check (CRC)

CRC is a redundancy error technique used to determine the error.

Following are the steps used in CRC for error detection.

Step1⇒ In CRC technique, a string of n 0s is appended to the data unit, and this n number is less than the number of bits in a predetermined number, known as division which is n+1 bits.

Step 2⇒ Secondly, the newly extended data is divided by a divisor using a process is known as binary division. The remainder generated from this division is known as CRC remainder.

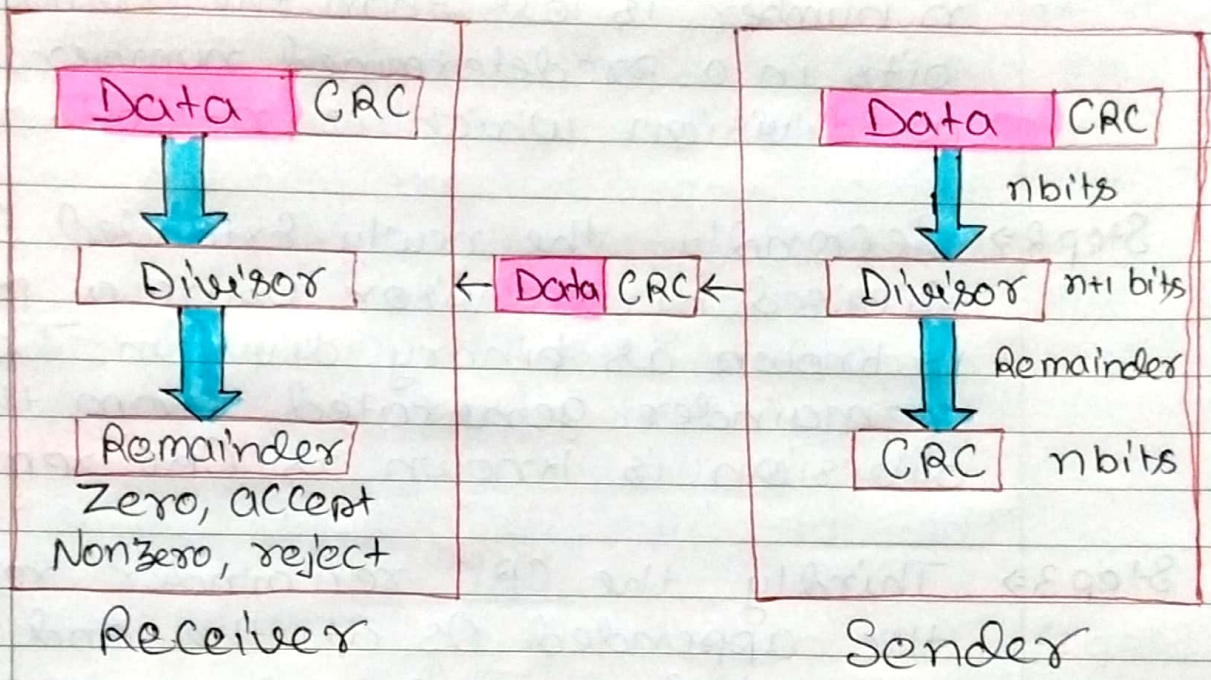
Step 3⇒ Thirdly, the CRC remainder replaces the appended 0s at the end of the original data. This newly generated unit is sent to the receiver.

Step4⇒ The receiver receives the data followed by the CRC remainder. The receiver will treat this whole unit as a single unit, and it is divided by the same divisor that was used to find the CRC remainder.

- If the resultant of this division is

Zero which means that it has no error and the data is accepted.

- If the resultant of this division is not zero which means that the data consists of an error. Therefore, the data is discarded.



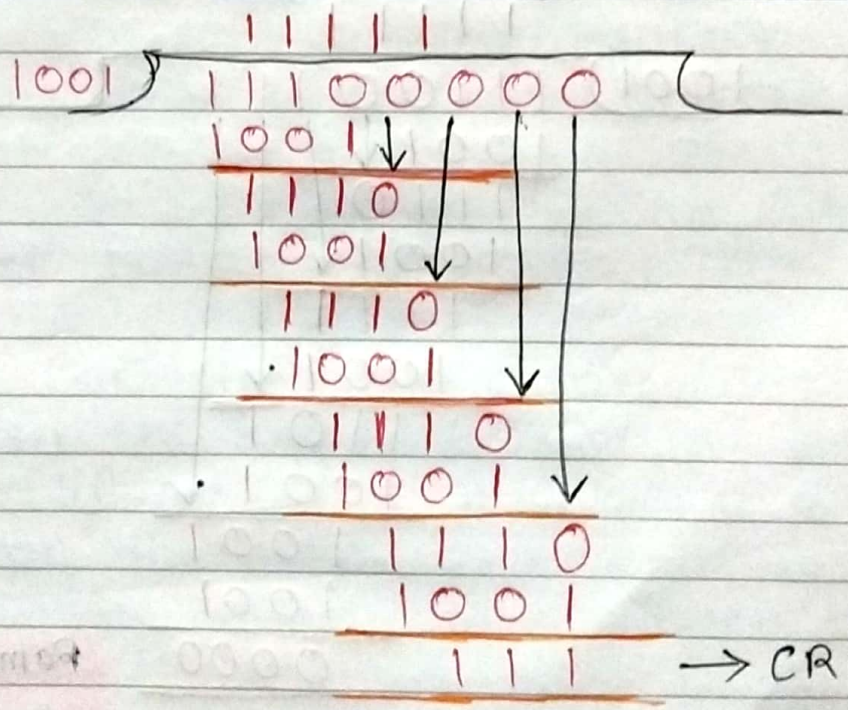
Ex: ⇒ Suppose the original data is 11100 and divisor is 1001.

CRC Generator ⇒

1) A CRC generator uses a modulo-2 division firstly, three zeroes are appended at the end of the data as the length of the divisor is 4 and we know that the length of

of the String 0s to be appended is always one less than the length of the divisor.

- Now, the String become 11100000, and the resultant String is divided by the divisor 1001.
- The remainder generated from the binary division is known as CRC remainder. The generated value of the CRC remainder is 111.
- CRC remainder replaces the appended string of 0s at the end of the data unit, and the final String would be 11100111 which is sent across the network.



CRC Checker ⇒

- The functionality of CRC checker is similar to CRC generator.
- When the string 11100111 is received at the receiving end, then CRC checker performs the modulo-2 division.
- A string is divided by the same divisor such as 1001.
- In this case, CRC checker generates the remainder of zero. Therefore, the data is accepted.

```
          1 1 1 1 1
      ┌──────────────
1001  | 1 1 1 0 0 1 1 1
        1 0 0 1
        ---------
          1 1 1 0
          1 0 0 1
          -------
            1 1 1 1
            1 0 0 1
            -------
              1 1 0 1
              1 0 0 1
              -------
                1 0 0 1
                1 0 0 1
                -------
                  0 0 0 0
```

Remainder is 0
data Accepted.

Error Correction

- Error Correction Codes are used to detect and correct the errors when data is transmitted from the sender to the receiver.

- Error Correction can be handled in two ways:

1) **Backword error Correction** ⇒ Once the error is discovered, the receiver requests the sender to retransmit the entire data unit.

2) **Forward error Correction** ⇒ In this case, the receiver uses the error-Correcting Code which automatically Corrects the errors.

A single additional bit can detect the error, but cannot correct it.

for Correcting the errors, one has to known the Exact position of error.
Ex ⇒ If we want to calculate a single-bit error, the error Correction Code will determine which one of seven bits is in error. To achieve this, we have to add some additional redundant bits.

Suppose r is the number of redundant bits and d is the total number of the data bits. The number of redundant bits r can be calculated by using the formula.

$$2^r >= d+r+1$$

where, r = redundant bit d = data bit.

The value of r is calculated by using the above formula.

for example, if the value of d is 4, then the possible smallest value that satisfies the above relation would be 3.

$$2^3 \geq 4+3+1$$

$$8 \geq 8$$

the redundant bits = 3.

Error Correction Techniques:

Hamming Code

Hamming Code is a set of error-Correction Codes that can be used to detect and correct the errors that can occur when the data is moved or stored from the sender to receiver.

Parity bits :⇒ The bit which is appended to the original data of binary bits so that the total number of 1s is even or odd.

Even parity :⇒ To check for Even parity, if the total no. of 1's is Even, then the value of the parity bit is 0. if the total no. of 1s occurrences is odd, then the value of the parity bit is 1.

Odd parity :⇒ To check for odd parity, if the total number of 1's is Even, then the value of parity bit is 0.

Algorithm of Hamming Code :

Step 1) An information of 'd' bits are added to the redundant bits 'r' to form d+r.

Step 2) The location of each of the (d+r) digits is assigned a decimal value.

Step 3) The 'r' bits are placed in the positions $1, 2, \ldots, 2^{k-1}$.

Step 4) At the receiving end, the parity bits are recalculated. The decimal value of the parity bits determines the position of an error.

Let understand the Concept of Hamming Code through an Example:⇒

Suppose the original data is 1010 which is to be sent.

Total number of data bits 'd' = 4

Number of redundant bits r: $2^r >= d+r+1$

$2^r >= 4+r+1$

Therefore, the value of r is 3 that Satisfies the above relation.
Total no. of bits = $d+r = 4+3 = 7$.

Determining the position of the redundant bits ⇒

The number of redundant bits is 3. The three bits are represented by r1, r2 r4. The position of the redundant bits is Calculated with Corresponds to the raised power of 2.
Therefore, their corresponding position are $1, 2^1, 2^2$.

The position of r1 = 1
the position of r2 = 2
the position of r4 = 4

Representation of Data on the addition of parity bits:

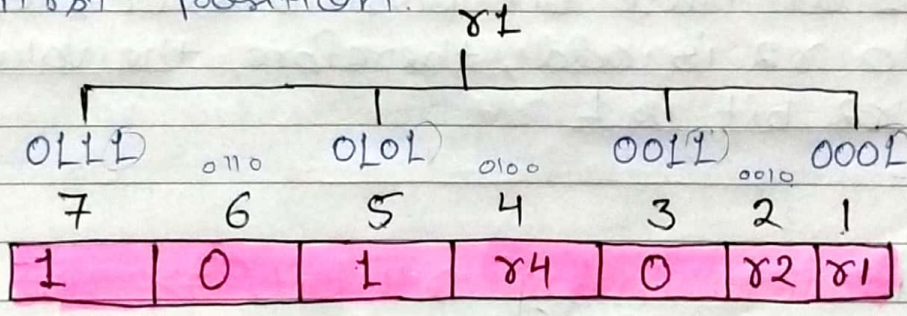
1010

7	6	5	4	3	2	1
1	0	1	r4	0	r2	r1

Determining the Parity bits:

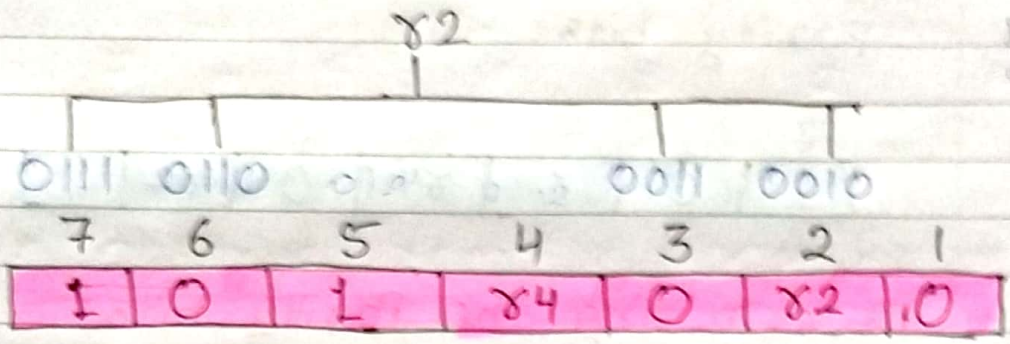
1) **Determining the r1 bit** ⇒

The r1 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the first position.



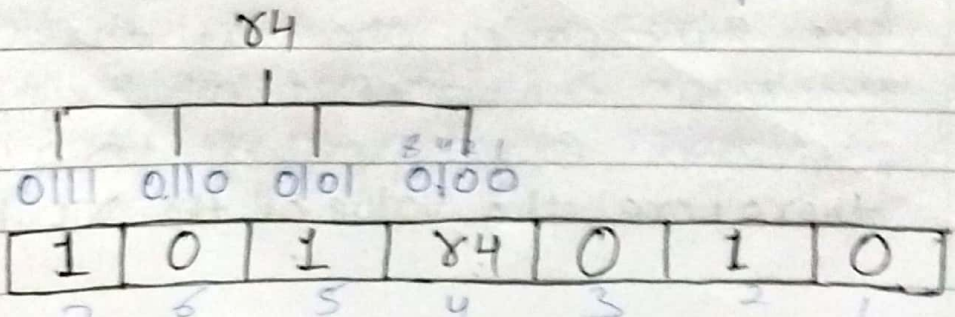
We observe from the above figure that the bit positions that includes 1 in the first position are 1, 3, 5, 7. Now, we perform the even-parity check at these bit positions. The total number of 1's at these bit positions corresponding to r1 is even therefore, the value of the r1 bit is 0.

2) **Determining r2 bit** ⇒ The r2 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the second position.



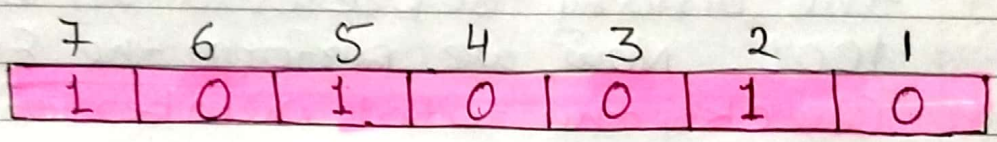
We observe from the above figure that the bit positions that includes 1 in the second position are 2, 3, 6, 7. Now, we perform the Even-parity check at these bit positions. The total no. of 1 at these bit positions corresponding to r2 is odd, therefore, the value of the r2 bit is 1

3) **Determining r4 bit** ⇒ The r4 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the third position.



We observe from the above figure that the bit positions that includes 1 in the third position are 4, 5, 6, 7. Now, we perform the Even-parity check at these bit positions. The total number of 1 at these bit position corresponding to r4 is even, therefore the value of the r4 bit is 0.

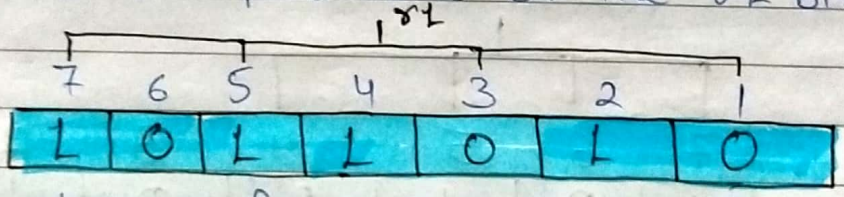
Data transferred is given below:



Suppose the 4th bit is changed from 0 to 1 at the receiving end, the parity bits are recalculated.

R1 bit

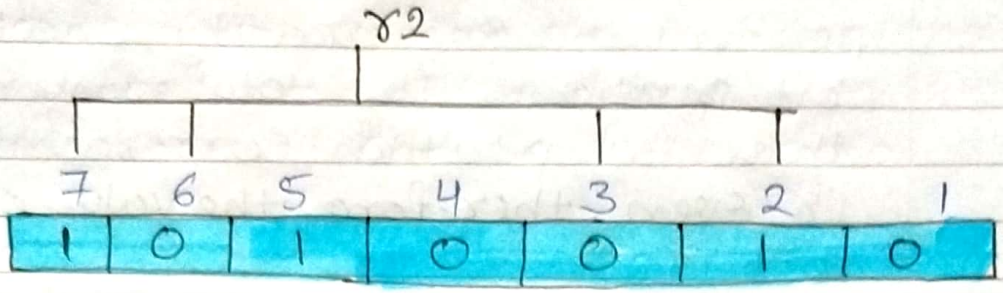
The bit positions of the r1 bit are 1, 3, 5, 7



We observe from the above figure that the binary representation of r1 is 1100. Now, we perform the Even-parity check, the total number of 1's appearing in the r1 bit is an Even number. Therefore, the value of r1 is 0.

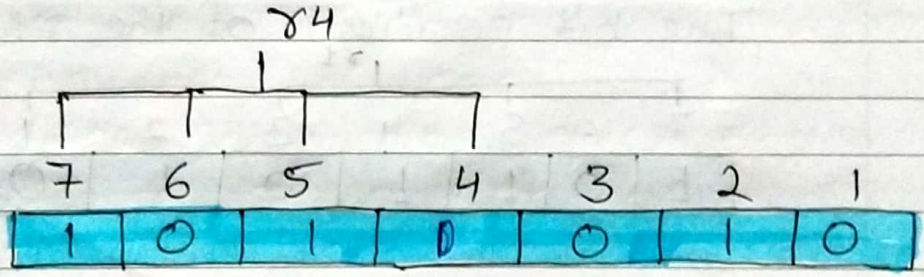
R2 bit ⇒

The bit position of r2 bit are 2, 3, 6, 7.



We observe from the above figure that the binary representation of r2 is '1001'. Now, we perform the Even-parity check, the total number of 1's appearing in the r2 bit is an Even number. Therefor, the value of r2 is 0.

R4 bit ⇒ The bit positions of r4 bit are 4, 5, 6, 7.

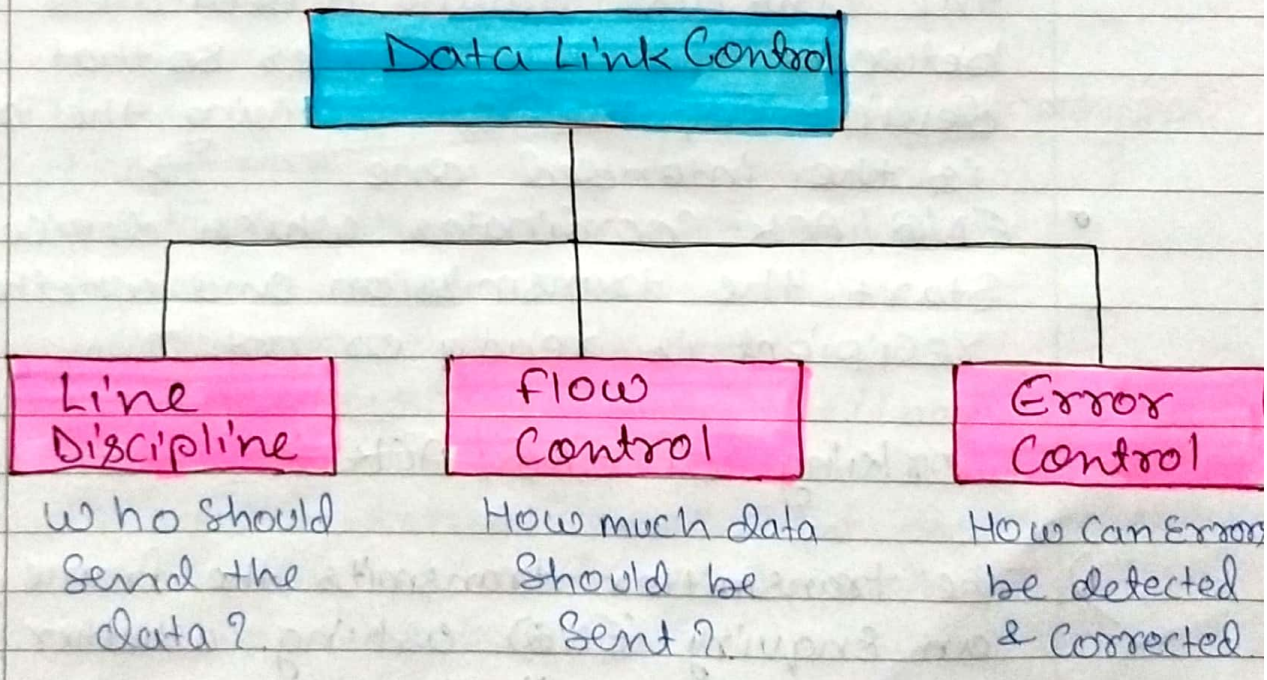


We observe from the above figure that the binary representation of r4 is 1010. Now, we perform the Even-parity check, the total no. of 1's appearing in the r4 bit is an odd no. Therefore, the value of r4 is 0.

Data Link Controls

- Data Link Control is the service provided by the Data Link Layer to provide reliable data transfer over the physical medium.
- For Example, In the half duplex transmission mode, one device can only transmit the data at a time. If both the devices at the end of the links transmit the data simultaneously, they will collide and leads to the Loss of the information.
- The data Link Layer provides the coordination among the devices so that no collision occurs.

The Data Link Layer provide three functions:



Line Discipline ⇒

- Line Discipline is a functionality of the Data Link layer that provides the coordination among the link systems. It determines which device can send, and when it can send the data.

Line Discipline can be achieved in two ways: ⇒

- ENQ / ACK
- Poll / Select

1) ENQ/ ACK ⇒
- ENQ / ACK stands for Enquiry/ Acknowledgement is used when there is no wrong receiver available on the link and having a dedicated path between the two devices so that the device capable of receiving the transmission is the intended one.
- ENQ / ACK coordinates which device will start the transmission and whether the recipient is ready or not.

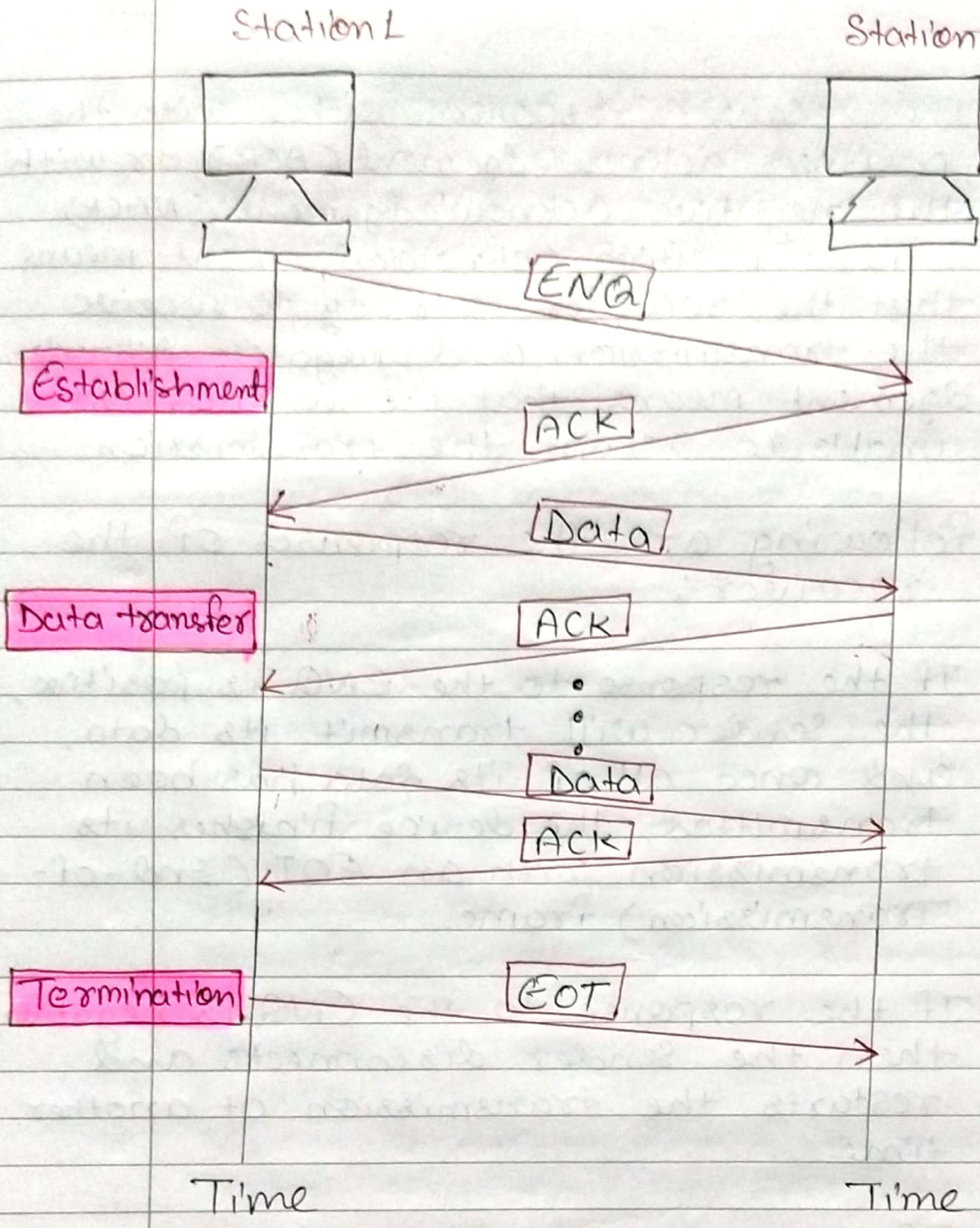
Working of ENQ/ ACK ⇒

1) The transmitter transmits the frame called an Enquiry (ENQ) asking whether the receiver is available to receive the data or not.

2) The receiver responses either with the positive acknowledgement (ACK) or with the negative acknowledgement (NACK) where positive acknowledgement means that the receiver is ready to receive the transmission and negative Acknowledgement means that the receiver is unable to accept the transmission.

following are the responses of the receiver:

- If the response to the ENQ is positive, the sender will transmit its data, and once all of its data has been transmitted, the device finishes its transmission with an EOT (End-of-Transmission) frame.
- If the response to the ENQ is negative, then the sender disconnects and restarts the transmission at another time.
- If the response is neither negative nor positive, the sender assumes that the ENQ frame was lost during the transmission and makes three attempts to establish a link before giving up.


Station 1
Station 2
ENQ
Establishment
ACK
Data
Data transfer
ACK
Data
ACK
Termination
EOT
Time
Time

2) Poll / select ⇒ The Poll/select method of line discipline works with those topologies where one device is designated as a primary station, and other devices are secondary stations.

Working of Poll / select ⇒

1) In this, the primary device and multiple secondary devices consist of a single transmission line, and all the exchanges are made through the primary device even though the destination is a secondary device.

2) The primary device has control over the communication link, and the secondary device follows the instructions of the primary device.

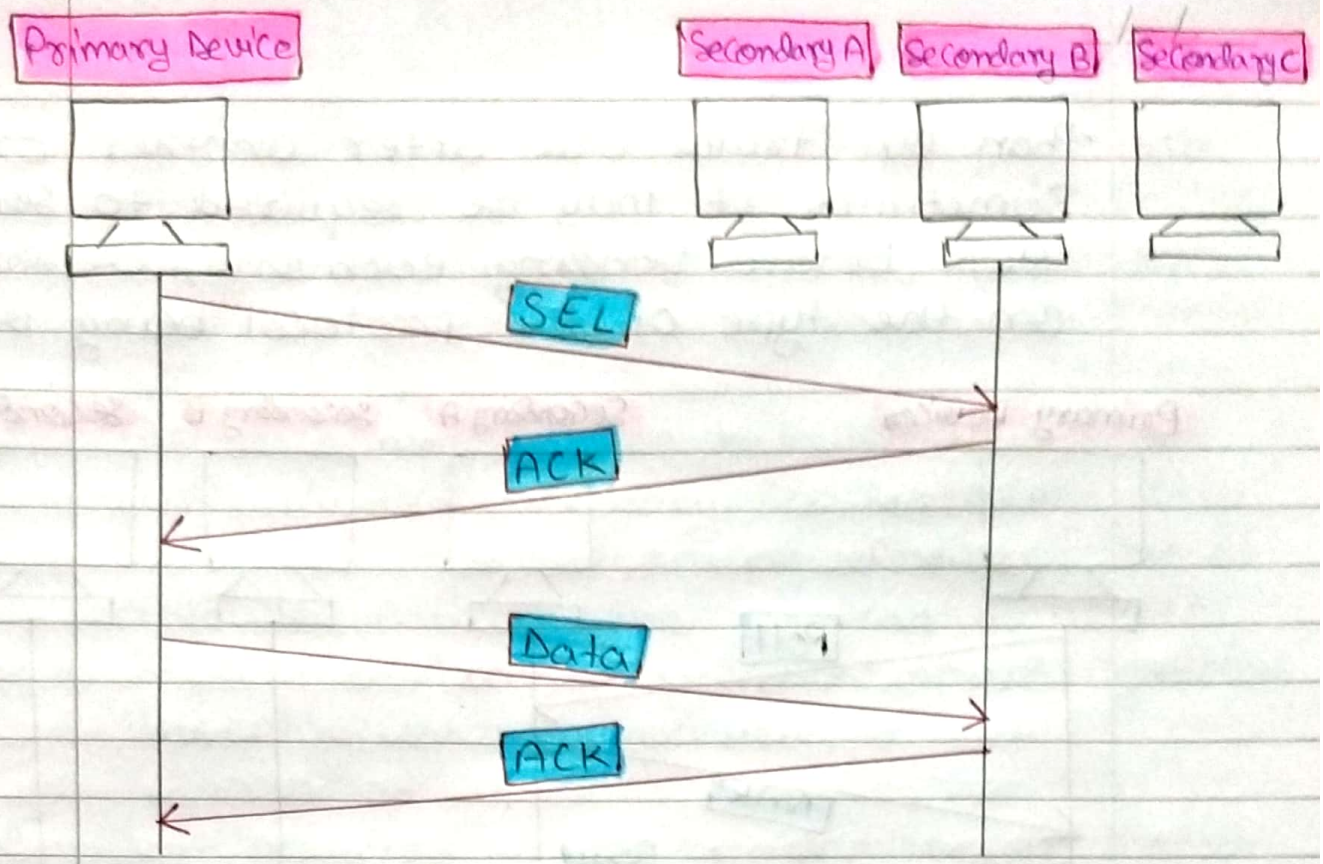
3) The primary device determines which device is allowed to use the communication channel. Therefore, we can say that it is an initiator of the session.

4) If the primary device wants to receive the data from the secondary device, it asks the secondary device that they anything to send, this process is known as polling.

5) If the primary device wants to send some data to the secondary device, then it tells the target secondary to get ready to receive the data, this process is known as selecting.

Select ⇒

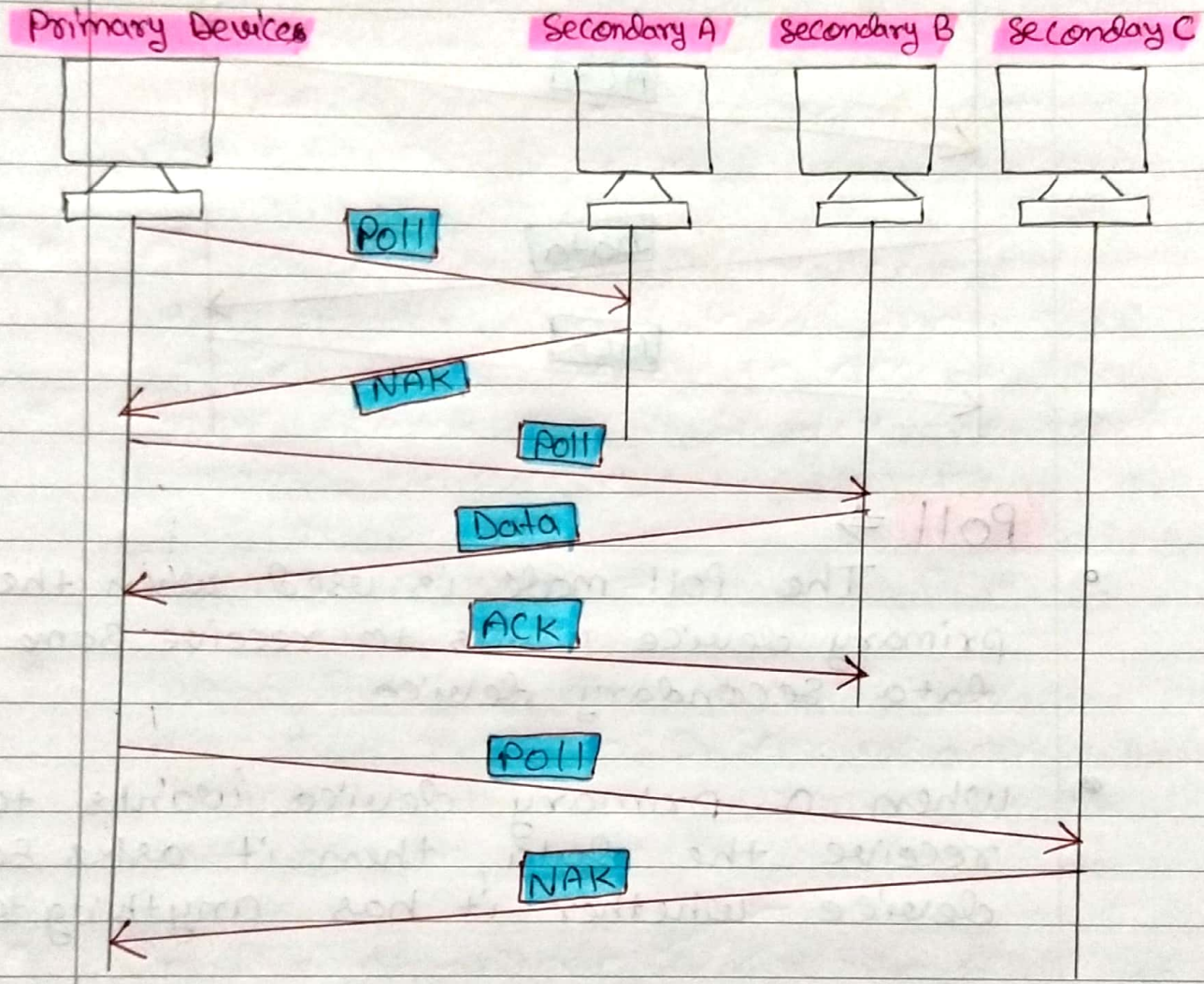
- The select mode is used when the primary device has something to send.
- When the primary device wants to send some data, then it alerts the secondary device for the upcoming transmission by transmitting a select (SEL) frame, one field of the frame includes the address of the intended secondary device.
- When the secondary device receives the SEL frame, it sends an acknowledgement that indicates the secondary ready status.
- If the secondary device is ready to accept the data, then the primary device sends two or more data frames to the intended secondary device. Once the data has been transmitted, the secondary sends an acknowledgement specifies that the data has been received.



Poll ⇒

- The Poll mode is used when the primary device wants to receive some data secondary device.
- When a primary device wants to receive the data, then it asks each device whether it has anything to send
- firstly, the primary ask (poll) the first secondary device, if it responds with the NACK (Negative Acknowledgement) means that it has nothing to send. Now, it approaches the second secondary device, it responds with the ACK means that it has the data to send.
- The secondary device can send more

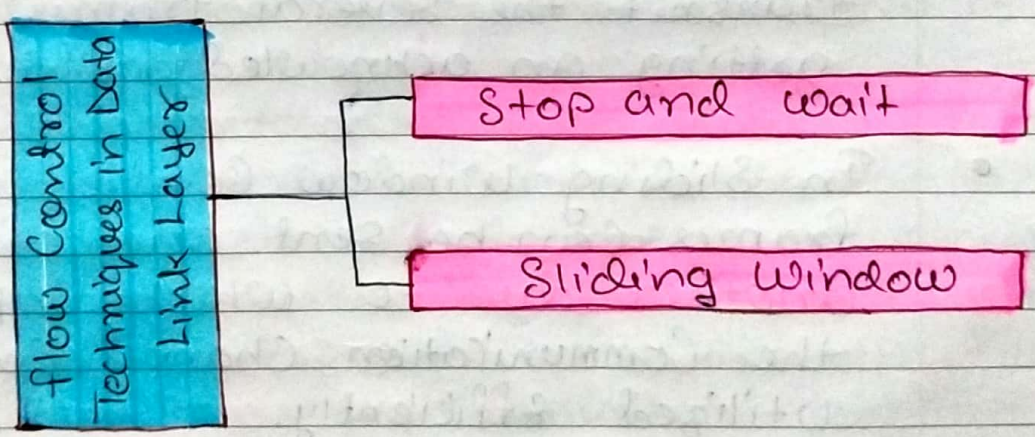
than on frame one after another or sometimes it may be required to send ACK before sending each one, depending on the type of the protocol being used.



Flow Control

- It is a set of procedures that tells the sender how much data it can transmit before the data overwhelms the receiver.
- The receiving device has limited speed and limited memory to store the data. Therefore, the receiving device must be able to inform the sending device to stop the transmission temporarily before the limits are reached.
- It requires a buffer, a block of memory for storing the information until they are processed.

Two methods have been developed to control the flow of data:



Stop and wait ⇒

- The sender sends a frame and waits for acknowledgment.
- Once the receiver receives the frame, it sends an acknowledgment frame back to the sender.
- On receiving the acknowledgment frame, the sender understands that the receiver is ready to accept the next frame. So it sender the next frame in queue.

Sliding window ⇒

- The Sliding window is a method of flow control in which a sender can transmit the several frames before getting an acknowledgement.
- In Sliding window control, multiple frames can be sent one after the another due to which capacity of the communication channel can be utilized efficiently.
- A single ACK acknowledge multiple frames.
- Sliding window refers to imaginary boxes at both the sender and receiver end.

- The window can hold the frames at either end, and it provides the upper limit on the number of frames that can be transmitted before the acknowledgement.
- frames can be acknowledged even when the window is not completely filled.
- The window has a specific size in which they are numbered as modulo-n means that they are numbered from 0 to n-1. for Example, if n=8, the frames are numbered from 0,1,2,3,4,5,6,7,0,1,2,3--
- The size of the window is represented as n-1. Therefore, maximum n-1 frames can be send before acknowledgement.
- When the receiver sends the ACK, it includes the number of the next frame that it want to receive.

for Example ⇒ to acknowledge the string of frames ending with frame number 4, the receiver will send the ACK containing the number 5. When the sender sees the ACK with the number 5, it got to know that the frames from 0 through 4 have been received.

Sender Window ⇒

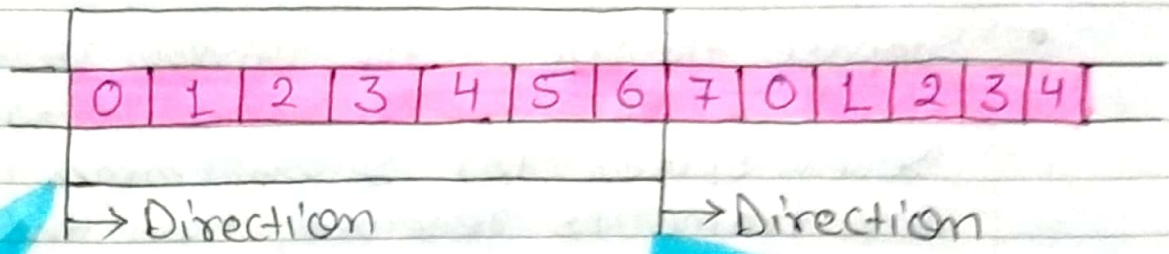
- At the beginning of a transmission, the sender window contains n-1 frames, and when they are sent out, the left boundary moves inward shrinking the size of the window.

for ex:⇒ if the size of the window is w if three frames are sent out, then the number of frames left out in the sender window is w-3.

- Once the ACK has arrived, then the sender window expands to the number which will be equal to the number of frames acknowledged by ACK.

- for example ⇒ The size of the window is 7, and if frames 0 through 4 have been sent out and no acknowledgement has arrived, then the sender window contains only two frames such as 5 and 6. Now, if ACK has arrived with a number 4 which means that 0 through 3 frames have arrived undamaged and the sender window is expanded to include the next four frames. Therefore the sender window contains six frames (5, 6, 7, 0, 1, 2).

Sender window



This wall move to the right when a frame is sent

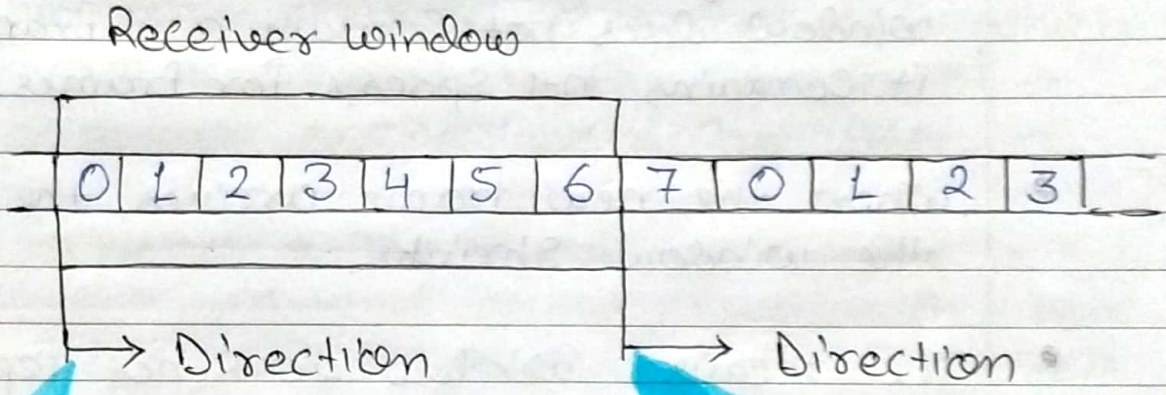
This wall moves to the right when an ACK is received

Receiver Window ⇒

- At the beginning of transmission, the receiver window does not contain n frames, but it contains n-1 spaces for frames.
- When the new frame arrives, the size of the window shrinks.
- The receiver window does not represent the number of frames received, but it represents the no. of frames that can be received before an ACK is sent.
  for ex ⇒ the size of the window is w, if three frames are received then the no. of spaces available in window is (w-3).
- Once the acknowledgement is sent, the receiver window expands by the no. equal to the no. of frames acknowledged.

- Suppose the size of the window is 7 means that the receiver window contains seven spaces for seven frames. If the one frame is received, then the receiver window shrinks and moving the boundary from 0 to 1.

  In this way, window shrinks one by one, so window now contains the six spaces. If frames from 0 through 4 have sent, then the window contains two space before an Acknowledgement is sent.



This wall moves to the right when a frame is received

This wall moves to the right when an ACK is sent

Error Control in Data Link Layer

- Error Control in data link Layer is the process of detecting and correcting data frames that has been corrupted or lost during transmission.
- In case of lost or corrupted frames, the receiver does not receive the correct data-frame and sender is ignorant about the loss.
- Data Link Layer follows a technique to detect transit errors and take necessary action, which is retransmission of frames whenever error is detected or frame is lost. The process is called Automatic Repeat Request (ARQ).

Phases in Error Control ⇒ The error control mechanism in data link layer involves the following phases-

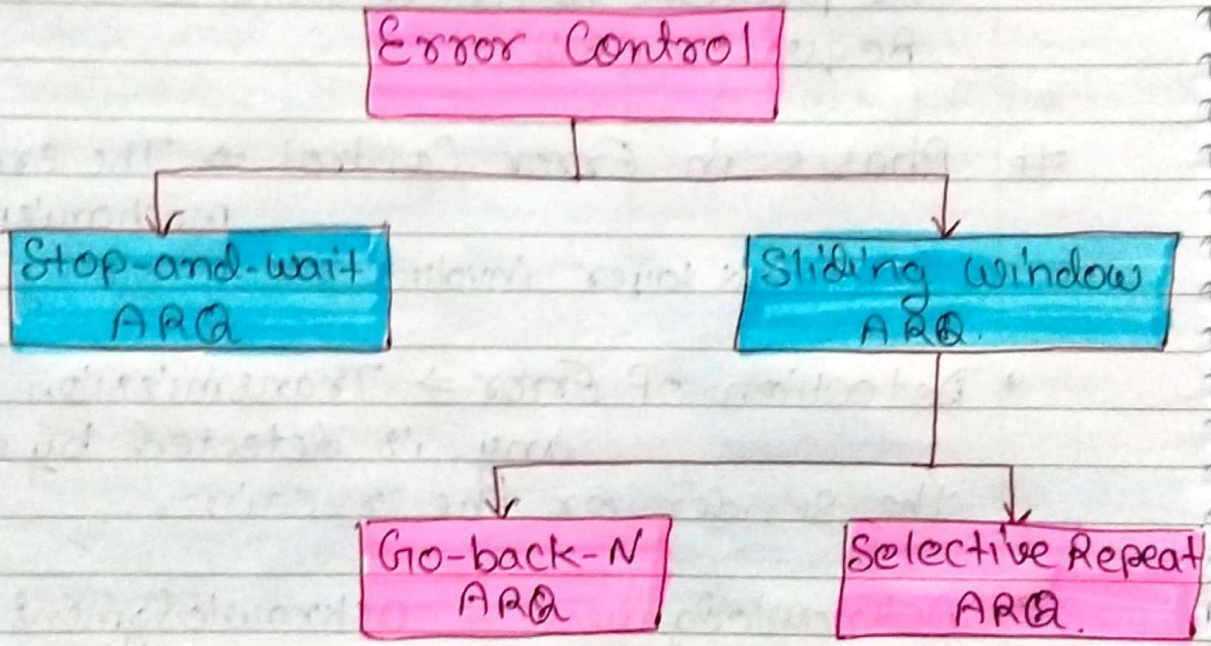
* Detection of Error ⇒ Transmission Error, if any, is detected by either the sender or the receiver.
* Acknowledgment ⇒ acknowledgment may be positive or negative.

1) Positive ACK ⇒ On receiving a correct frame, the receiver sends a positive Acknowledge.

3) Negative ACK ⇒ On receiving a damaged frame or a duplicate frame, the receiver sends a negative acknowledgment back to the sender.

* Retransmission ⇒ The sender maintain a Clock and sets a timeout period. If an acknowledgment of a data-frame previously transmitted does not arrive before the timeout, or a negative acknowledgement is received, the sender retransmits the frame.

Error Control Techniques.



Stop-and-Wait ARQ ⇒ This protocol involves the following transitions.

• A timeout Counter is maintained by the sender,

which is started when a frame is sent.

- If the sender receives acknowledgment of the sent frame with time, the sender is confirmed about successful delivery of the frame. It then transmits the next frame in queue.
- If the sender does not receive the acknowledgment within time, the sender assumes that either the frame or its acknowledgment is lost in transit. It then retransmits the frame.
- If the sender receives a negative acknowledgment, the sender retransmits the frame.

Go-Back-N ARQ ⇒ The working principle of this protocol is -

- The sender has buffer called sending window. Size, without receiving the acknowledgment of the previous ones.
- The receiver receives frames one by one. It keep track of incoming frame's sequence number and sends the corresponding acknowledgment frames.
- After the sender has sent all the frames in window, it checks up to what sequence number

it has received positive acknowledgment.

- If the sender has received positive acknowledgment for all the frames, it sends next set of frames.
- If sender receive NACK or has not receive any ACK for a particular frame, it retrasmits all the frames after which it does not receive any positive ACK.

Selective Repeat ARQ ⇒

- Both the sender and the receiver have buffers called sending window and receiving window respectively.
- The sender sends multiple frames based upon the sending-window size, without receiving the acknowledgment of the previous ones.
- The receiver also receives multiple frames within the receiving window size.
- The receiver keeps track of incoming frames sequence numbers, buffers the frames in memory.

- It sends ACK for all successfully received frames and sends NACK for only frames which are missing or damaged.
- The sender in this case, sends only packet for which NACK is received.

Network Layer

- The Network Layer is the third Layer of the OSI model.
- It handles the service requests from the transport Layer and further forwards the service request to the data link Layer.
- The network Layer translates the Logical addresses into physical addresses.
- It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the Congestion of data packets.
- The main role of the network Layer is to move the packets from sending host to the receiving host.

The main functions performed by the network Layer are: ⇒

1) Routing ⇒ When a packet reaches the router's input link, the router will move the packets to the router's output link. For Ex ⇒ A packet from S1 to R1 must be forwarded to the next router on the path to S2.

2) Logical Addressing ⇒ The data link Layer

implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system.

The network layer adds a header to the packet which includes the logical address of both the sender and the receiver.

3) Internetworking ⇒ This is the main role of the network layer that it provides the logical connection between different types of networks.

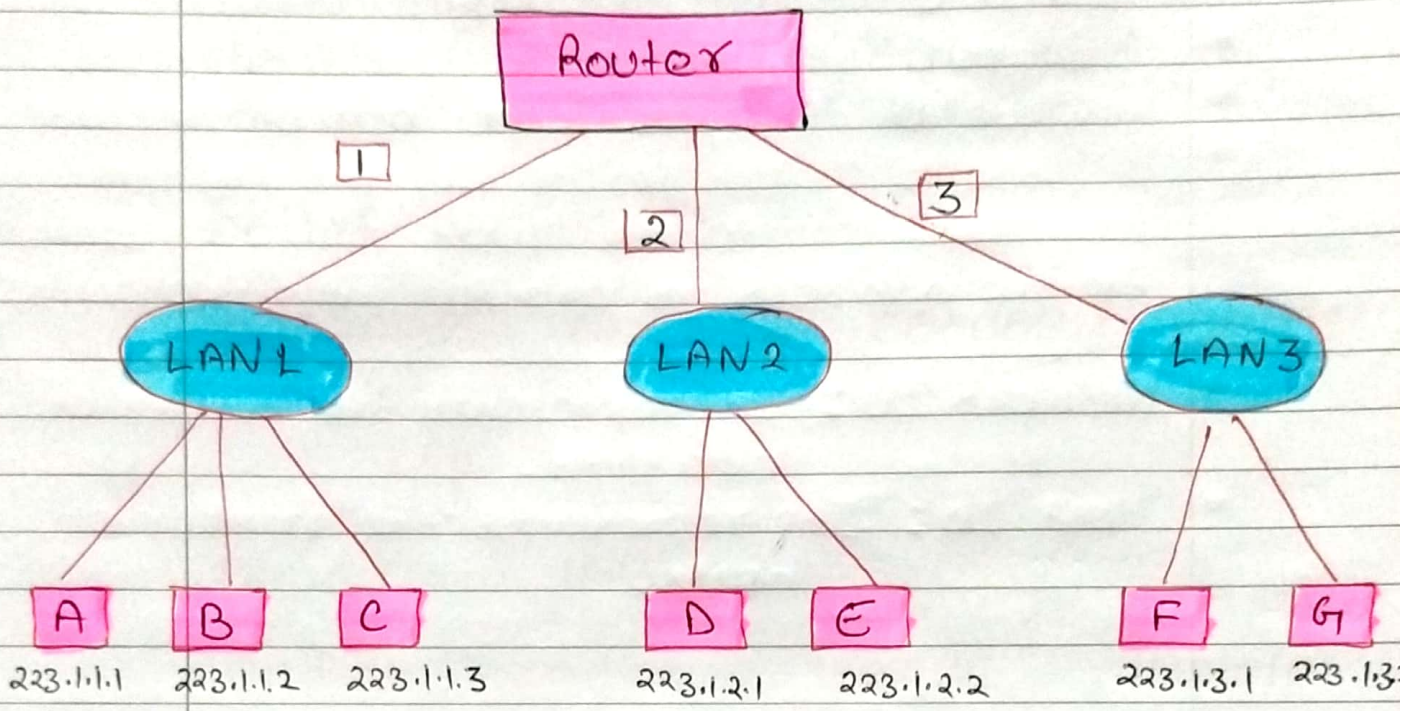
4) fragmentation ⇒ The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.

Network Addressing

- Network Addressing is one of the major responsibilities of the network Layer.
- Network addresses are always Logical such as Software-based addresses.
- A host is also known as end System that has one link to the network. The boundary between the host and link is known as an interface. Therefore, the host can have only one interface.
- A router is different form the host in that it has two or more links that connect to it. When a router forwards the datagram, then it forwards the packet to one of the links. The boundary between the router and link is known as an interface, and the router can have multiple interfaces, one for each of its links. Each interface is capable of sending and receiving the IP packets, so IP requires each interface to have an address.
- Each IP address is 32 bit long, and they are represented in the form of "dot decimal notation" where each byte is written in the decimal form, and they are separated by the period.
  An IP address would like 193.32.216.9 where 193 represents the decimal notation

of first 8 bits of an address, 32 represents the decimal notation of second 8 bits of an address.

Let's understand through a simple example ⇒



- In the above figure, a router has three interfaces labeled as 1, 2 & 3 and each router interface contains its own IP address.
- Each host contains its own interface and IP address.
- All the interfaces attached to the LAN1 is having an IP address in the form of 223.1.1.xxx, and the interfaces attached to the LAN2 and LAN3 have an IP address in the form of 223.1.2.xxx and 233.1.3.xxx.

- Each IP address consists of two parts. the first part (first three bytes in IP address) specifies the network and second part (last byte of an IP address) specifies the host in the network.

Classful IP Addressing

- IP address is an address having information about how to reach a specific host, especially outside the LAN.
- AN IP address is a 32 bit unique address having an address space of 2^{32}.
- Generally, there are two notations in which IP address is written, dotted decimal notation and hexadecimal notation.

Dotted Decimal Notation:

10000000 00001011 00000011 00011111

128. 11. 3. 31

Hexadecimal Notation:

01110101	00011101	10010101	11101010
75	1D	95	EA

0x751D95EA

NOTE⇒
- The value of any segment (byte) is between 0 and 255 (both included).
- There are no zeroes preceding the value in any segment (054 is wrong, 54 is correct)

255.255.255.255

~~054~~

54.

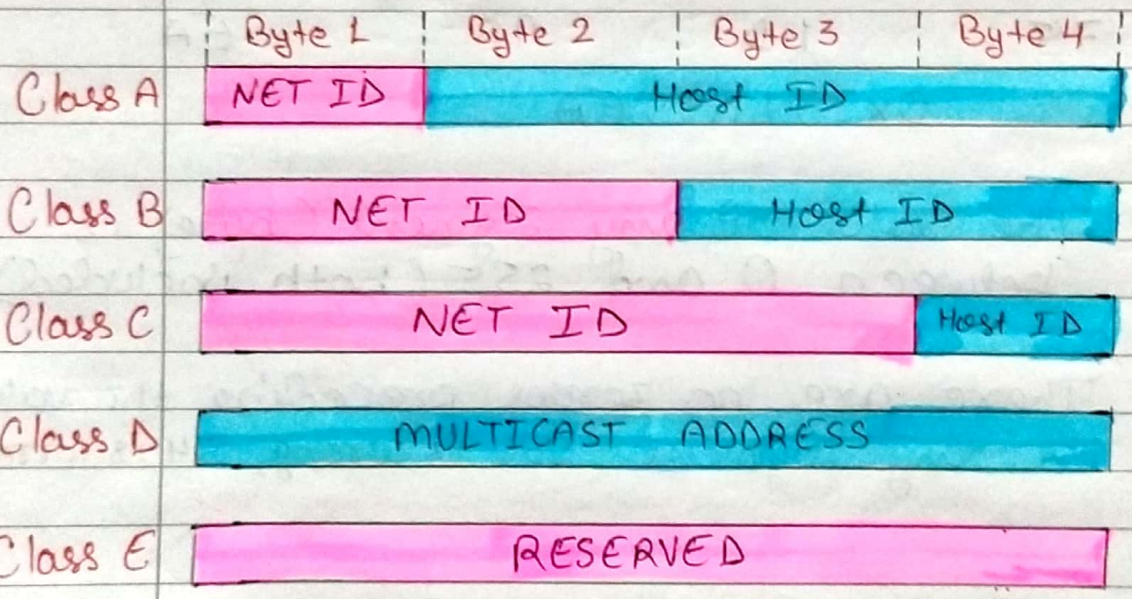
Classfull Addressing ⇒

The 32 bit IP address is divided into five sub-classes. These are:

- Class A
- Class B
- Class C
- Class D
- Class E

An ip address is divided into two parts:

- Network ID: It represents the number of networks.
- Host ID: It represents the number of hosts.



In the above diagram, we observe that each Class have a specific range of IP addresses.

The Class of IP address is used to determine the number of bits used in a class and number of networks and hosts available in the class.

Class A

In class A, an IP address is assigned to those network that contain a Large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

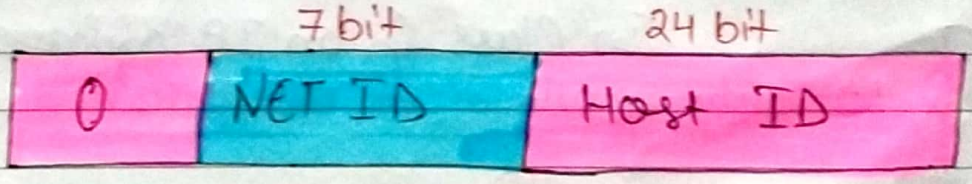
In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network.

The total number of networks in Class A =

$2^7 = 128$ network address

The total number of hosts in Class A =

$2^{24} - 2 = 16,777,214$ host address



Class B

In Class B, an IP address is assigned to those networks that range from small-sized to Large-sized networks.

- The Network ID is 16 bits long.
- The Host ID is 16 bits Long.

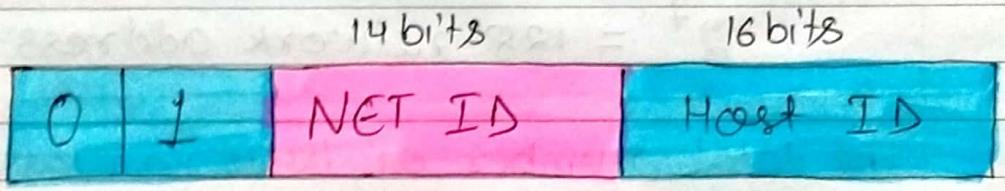
In Class B, the higher order bits of the first octet is always set to 10, and the remaining 14 bits determine the network ID. The other 16 bits determine the Host ID.

The total number of networks in Class B =

$$2^{14} = 16384 \text{ network address.}$$

The total number of hosts in Class B =

$$2^{16} - 2 = 65534 \text{ host address}$$



Class C

In Class C, an IP address is assigned to only small-sized networks.

- the Network ID is 24 bits long.
- the host ID is 8 bits long.

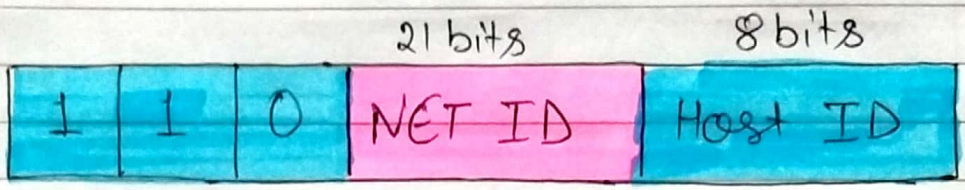
In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID. the 8 bits of the host ID determine the host in a network.

The total number of networks =

$$2^{21} = 2097152 \text{ network address}$$

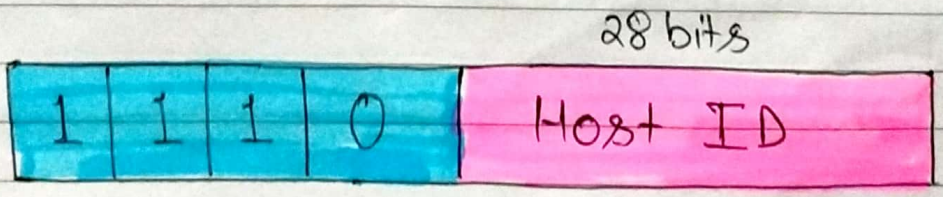
The total number of hosts =

$$2^8 - 2 = 254 \text{ host address}$$



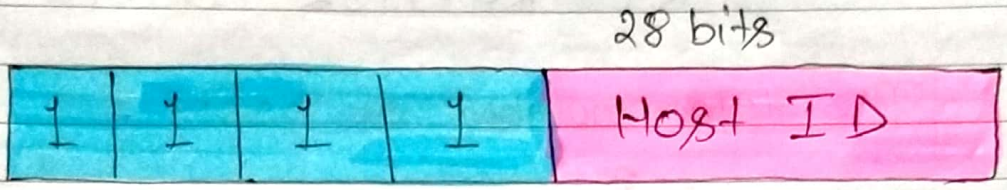
Class D

In Class D, an IP address is reserved for multicast addresses. It does not possess Subnetting. the higher order bits of the first octet is always set to 1110, and the remaining bits determines the host ID in any network.



Class E

In Class E, an IP address is used for the future use or for the research and development purpose. It does not possess any Subnetting. The higher order bits of the first octet is always set to 1111, and the remaining bits determines the host ID in any network.

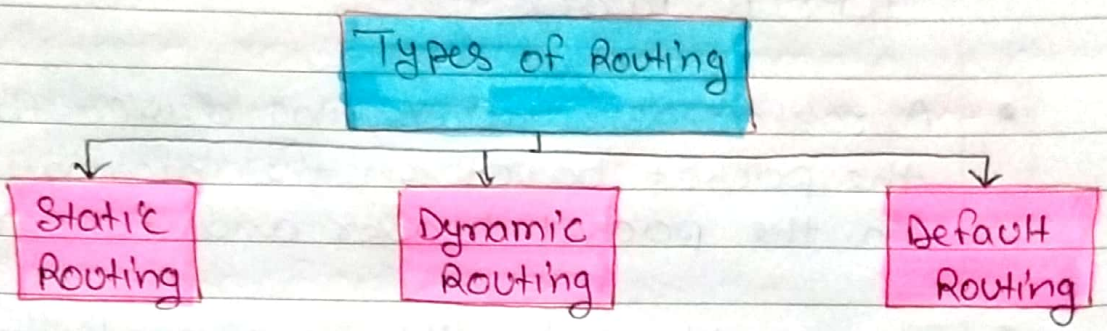


Routing in Computer Network

- A Router is a process of selecting path along with the data can be transferred from source to destination. Routing is performed by a special device known as a router.
- A Router works at the network Layer in the OSI model and internet Layer in TCP/IP model.
- A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.
- The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.
- The routing protocols use the metric to determine the best path for the packet delivery. The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path etc. used by the routing algorithm to determine the optimal path to the destination.
- The routing algorithm initializes and maintains the routing table for the process of path determination.

Types of Routing ⇒

- Static Routing
- Default Routing
- Dynamic Routing



Static Routing ⇒

- Static Routing is also known as Nonadaptive Routing.
- It is a technique in which the administrator manually adds the routes in a routing table.
- A Router can send the packets for the destination along the route defined by the administrator.
- In this technique, routing decisions are not made based on the Condition or topology of the networks.

Advantages of Static Routing ⇒

- No overhead ⇒ It has no overhead on

the CPU usage of the router. Therefore, the cheaper router can be used to obtain static routing.

- Bandwidth ⇒ It has not bandwidth usage between the routers.
- Security ⇒ It provides security as the system administrator is allowed only to have control over the routing to a particular network.

Disadvantages of Static Routing:

- for a large network, it becomes a very difficult task to add each route manually to the routing table.
- The system administrator should have a good knowledge of a topology as he has to add each route manually.

Default Routing ⇒

- Default Routing is a technique in which a router is configured to send all the packets to the same host device, and it doesnot matter whether it belongs to a particular network or not. A packet is transmitted to device for which it is configured in default routing.
- Default Routing is used when networks

deal with the single exit point.

- It is also useful when the bulk of transmission networks have to transmit the data to the same IP device.
- When a specific route is mentioned in the routing table, the router will choose the specific route rather than the default route. the default route is chosen only when a specific route is not mentioned in the routing table.

Dynamic Routing ⇒

- It is also known as Adaptive Routing.
- It is a technique in which a router adds a new route in the routing table for each packet in response to the changes in the condition or topology of the network.
- Dynamic protocols are used to discover the new routes to reach the destination.
- In Dynamic Routing, RIP and OSPF are the protocols used to discover the new routes.
- If any route goes down, then the automatic adjustment will be made to reach the destination.

Advantages of Dynamic Routing:

- It is easier to Configure
- It is more effective in selecting the best route in response to the changes in the condition or topology.

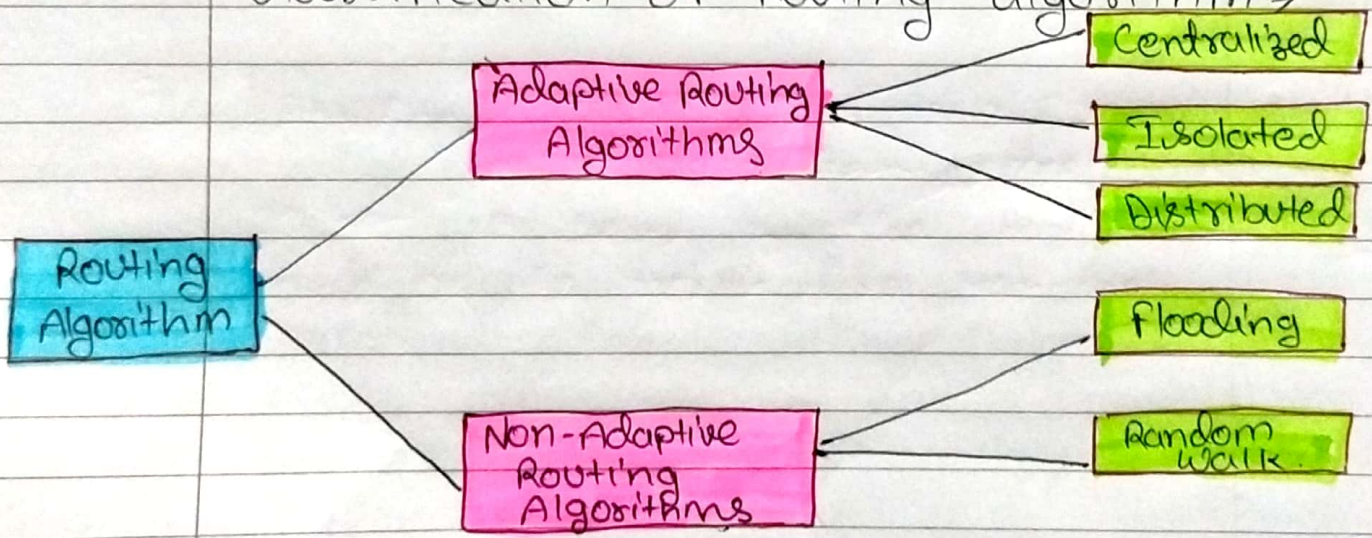
Disadvantages of Dynamic Routing:

- It is more expensive in terms of CPU and bandwidth usage.
- It is less secure as compared to default and static routing.

Routing Algorithms

- A routing algorithm is a procedure that lays down the route or path to transfer data packet from source to the destination.
- In order to transfer the packet from source to the destination, the network layer must determine the best route through which packets can be transmitted.
- The routing protocol is a routing algorithm that provides the best path from the source to the destination. The best path is the path that has the "least-cost path" from source to the destination.
- Routing is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm.

Classification of Routing algorithm ⇒



Adaptive Routing Algorithm ⇒

- An adaptive Routing algorithm is also known as dynamic routing algorithm.
- This algorithm makes the routing decision based on the topology and network traffic
- The main parameters related to this algorithm are hop count, distance and estimated transit time.

The three popular types of adaptive routing algorithms are -

1) Centralized algorithm ⇒ It finds the Least-Cost path between Source and destination node by using global knowledge about the network. So, it is also known as global routing algorithm

2) Isolated algorithm ⇒ This algorithm procures the routing information by using Local information instead of gathering information from other nodes.

3) Distributed algorithm ⇒ It is also known as decentralized algorithm as it computes the Least-Cost path between Source and destination in an iterative and distributed manner.

Non-Adaptive Routing Algorithm ⇒

- Non-adaptive Routing algorithm is also known as a static routing algorithm.
- When booting up the network, the routing information stores to the routers.
- Non adaptive routing algorithm do not take the routing decision based on the network topology or network traffic.

The two types of non-adaptive routing algorithms are -

1) Flooding ⇒ In flooding, when a data packet arrives at a router, it is sent to all the outgoing links except the one it has arrived on. Flooding may be uncontrolled controlled or selective flooding.

2) Random walks ⇒ This is a probabilistic algorithm where a data packet is sent by the router to any one of its neighbours randomly.

Distance Vector Routing Algorithm

- The Distance vector algorithm is a dynamic algorithm.
- A distance-vector routing (DVR) protocol requires that a router inform its neighbors of topology changes periodically.
- Historically it's known as the old ARPANET routing algorithm (or known as Bellman-Ford algorithm).

Bellman ford Basics ⇒ Each router maintains a Distance vector table containing the distance between itself and ALL possible destination nodes.
Distance, based on a chosen metric, are computed using information from the neighbors distance vectors.

Information kept by Distance Vector Router ⇒

- Each router has an ID.
- Associated with each link connected to a router, there is a link cost (static or dynamic).
- Intermediate hops.

Distance Vector Table Initialization ⇒

- Distance to itself = 0

- Distance to ALL other routers = infinity number

Distance Vector Algorithm ⇒

1) A router transmits its distance vector to each of its neighbors in a routing packet

2) Each router receives and saves the most recently received distance vector from each of its neighbors.

3) A router recalculates its distance vector when:

a) It receives a distance vector from a neighbor containing different information than before.
When a node x receives new DV estimate from any neighbor v, it saves v's distance vector and it update its own DV using B-F equations:

$D_x(y) = \min\{ C(x,y) + Dv(y), Dx(y)\}$ for each node $y \in N$.

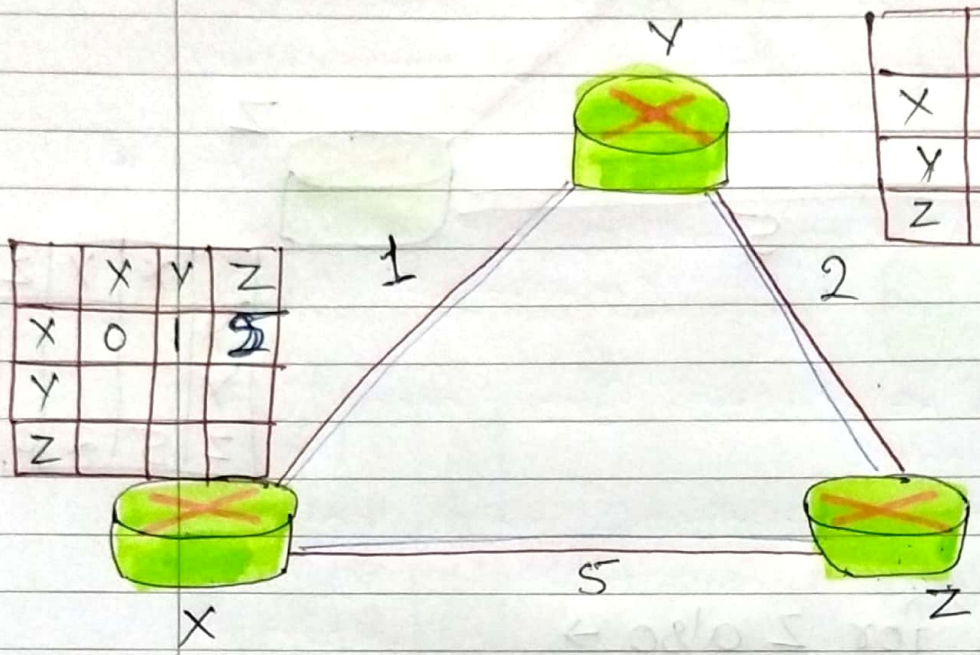
Where

$Dx(y)$ = Estimate of least cost from x to y.

$C(x,v)$ = Node x knows cost of each neighbor v.

$Dx = [Dx(y)\ y \in N]$ = node x maintains distance vector.

Example ⇒ Consider 3-routers X, Y and Z. Each router have their routing table. Every routing table will contain distance to the destination nodes.



	X	Y	Z
X			
Y	1	0	2
Z			

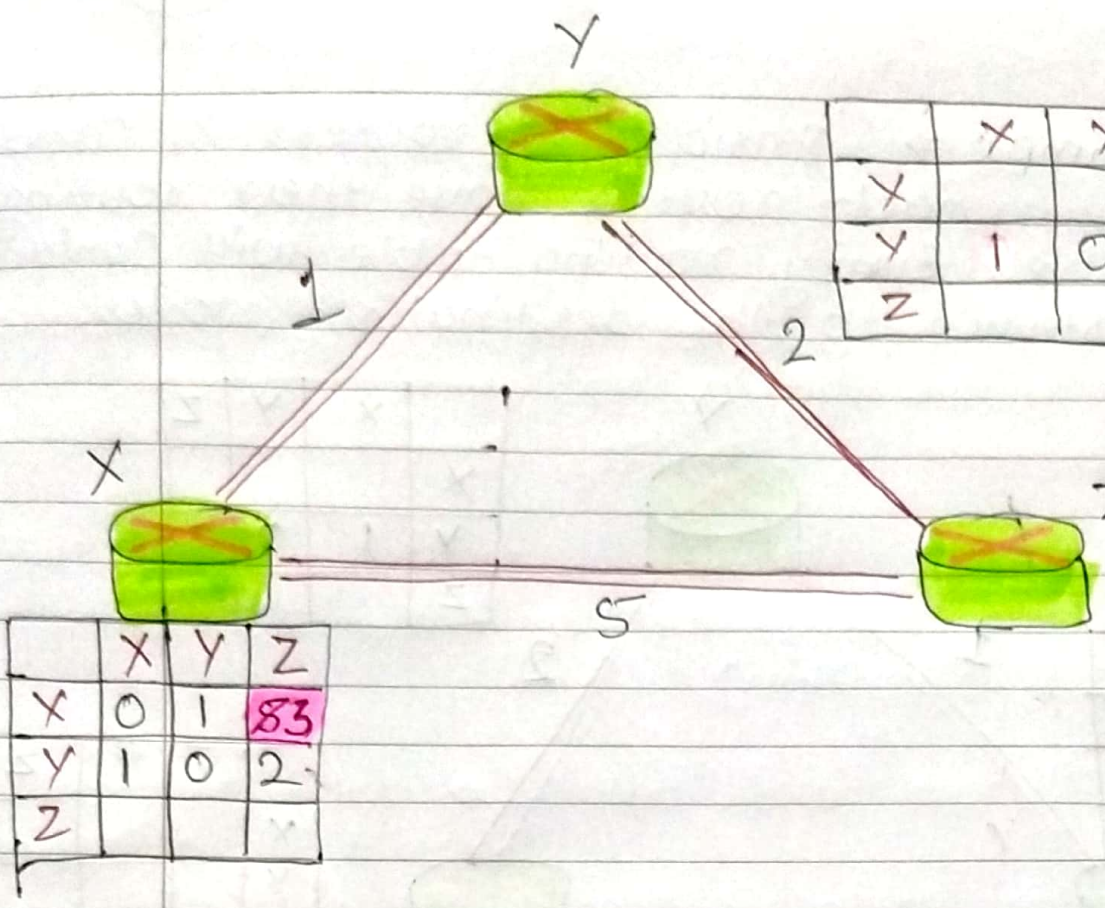
	X	Y	Z
X	0	1	5
Y			
Z			

	X	Y	Z
X			
Y			
Z	5	2	0

Consider router X, X will share it routing table to neighbors and neighbors will share it routing table to it to X and distance from node x to destination will be calculated using bellman-ford equation.

$$D_x(y) = \min_{y \in N} \{ C(x,y) + D_v(y) \} \text{ for each node}$$

As we can see that distance will be less going from X to Z when Y is intermediate node (hop) so it will be update in routing table X.

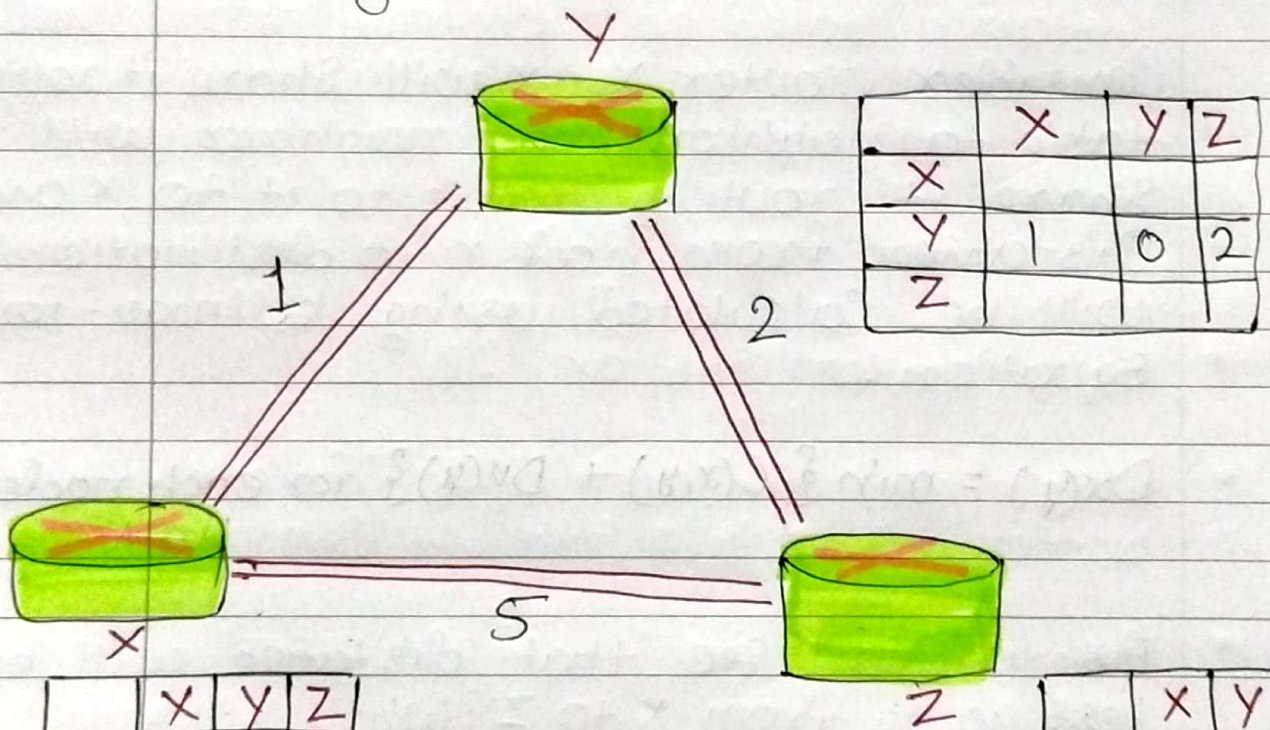


	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X	0	1	83
Y	1	0	2
Z			

	X	Y	Z
X			
Y			
Z	5	2	0

Similary for Z also →

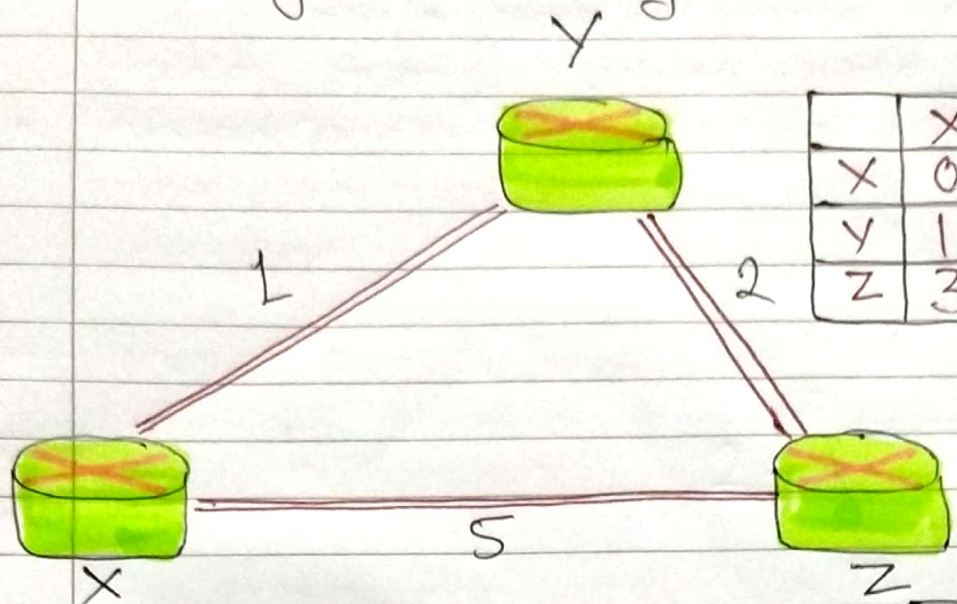


	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X	0	1	53
Y	1	0	2
Z	53	2	0

	X	Y	Z
X			
Y			
Z	5	2	0

finally the routing table for all ⇒



	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0