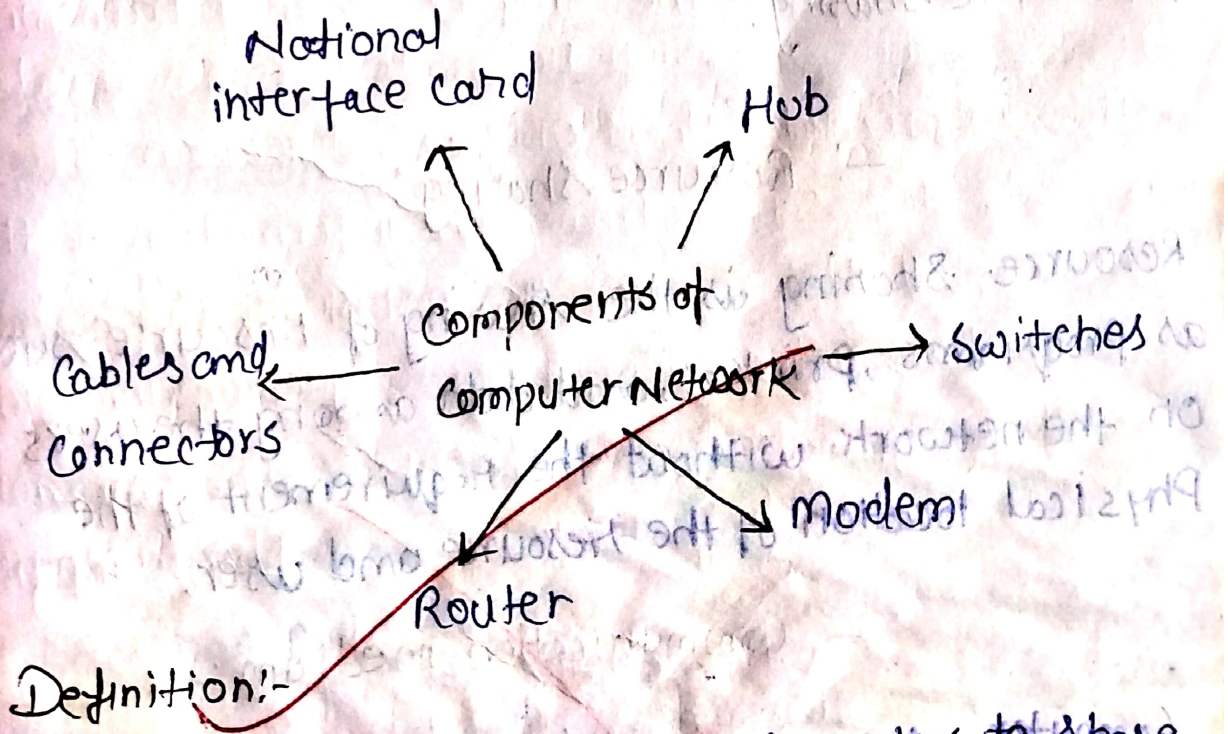
Introduction to Computer Network

Comuter Network :- Computer network is group of computers connected with each other through wires, optical fibers or optical links so that various devices can interact with each other through a network.

- The aim of computer network is the sharing of resources among various devices.
- In the case of computer network(is the)technology, there are several types of networks that vary from simple to complex level.

Components of Computer Network.



Definition:-

It's a group of interconnected computers to share resources, exchange file or allow communication.

In the Computer network resources can be in the form of hardware or software.

- In the hardware sharing user can share printer, scanner, CD Rom, Hardware etc.
- In software sharing user can share any type of file such as application software or system software.

Benifits of Computer Network.

1) Hardware sharing / Resource sharing.
2) Application sharing.
3) User communication
4) Network gamming.
5) Service clint model.
6) E-Commerce.
7) Resource sharing.

—: Resource sharing :-

Resource sharing is the sharing of resource such as programs, printers, and data among the users on the network without the requirement of the physical location of the resource and user.

—: Communication medium :-

Computer Network is also behaves as a communi-cation between as a communication medium among the users. for example, a company contains more

than one computer has an email system which the employees use for daily communication.

E-Commerce :-

Computer network is also important in businesse we can do the business over the internet. for example amazon.com is doing their business over the internet, i.e. they are doing their busines over the internet.

TYPES OF NETWORK

1: PAN (Person Area Network) :- It's a smalles network which is personal to uses, this may include (enab) blotooth enable devices or Infraray enable devices.

- PAN has collectivily range to aprox 10m
- PAN include wireless mouse, and wireless key-board, headphone etc.

2) LAN (Local Area Network) :-

- It's privetly own computer network.
- which cover a small geographical area.
- It's used in offices, schools etc.
- LAN has collectivily range to aprox 50m

3) MAN (Metropolitain Area Network) :-

- It's larger than LAN.
- Generally these network delives fast and

efficient communication by using fiber optics
- It's known as interconnected LAN.

4) WAN (Wide Area Network)

It's a telecommunication network which is used for communication between devices.
- It has a large geographical area between two contenents, in this area of network satalite systems are used.
- WAN contain multiple LAN and MAN.
- Internet is the largest WAN spaning the earth.

—: MODE OF TRANSMISSION :-

The term transmission mode define the flow of data between to communicating devices.

(1) Simplex mode :- The simplex mode of transmi-ssion refers to a communication method where data flows only one direction. In this mode, the sender transmits information to the receiver, but the receiver can not send any data back to the sender. It is a one way communication channel. A typical example of simplex transmission is radio broddcasting. mouse and key board inputting

(2) Duplex mode :- The duplex mode of transmission is a communication method where data can flow in both directions between two devices. There are two types of of duplex transmiss-ion.

(a) Full Duplex :- Both devices can send and receive data simultaneously. An example is telephone communication, where both parties can talk and listen at the same time

(b) Half Duplex :- Data can be sent in both directi-ons ; but not at the same time. An example is a walkie-talkie ; where one perso speaks while the other listnes, and they take turns to communication.

- Duplex modes enable more interactive communica-tion compared to simplex.

NETWORK TOPOLOGY

Network topology refers to the arrangement or layout of different elements (like nodes, links and devices) in computer network. It defines how the devices in the network are interconnected and how data flows between them. There are two primary types of network topologies.

(a) Physical topology.

(b) Logical topology.

(a) Physical Topology. :- The physical layout of devices and cables in a network. This refers to the actual physical connections, such as cables and devices.

- There are main five types of physical topology.

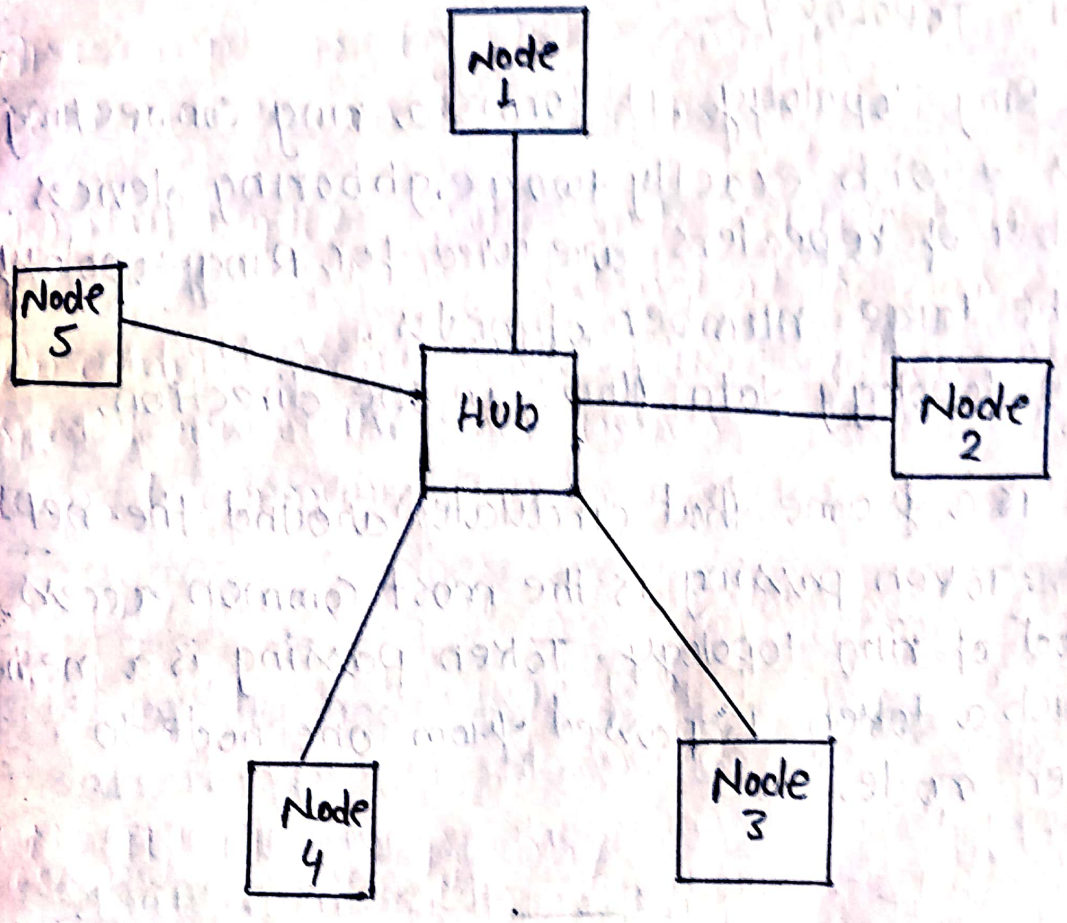
(1) BUS TOPOLOGY :- Bus topology is a type of network design in which all devices (nodes) are connected to a single central cable or backbone, know as bus. The communi-cation between devices in the network occurs over this shared bus.

Both ends of the shared channel (Bus) has line terminator ; the data is send in only one direction and as soon as it reaches the extreame end the transmer remove the data from the line.

- Andvantages
- Cost effective.
- It's used in small network.
- It requires less cable length in comparison to other topologies.
- Easy to understand.
- Disadvantages
- Limited cable length and number of devices.
- It's slow when more devices are attached in the network.

(2) STAR TOPOLOGY :- In this sort of topology every node is connected to the central node which is called hub or switch. The central node is server and other nodes are called client.

In this topology data from the source node is first delivered to the hub and transfered to the destination node.



- It's easy to add or remove new node in this topology. Star topology gives better performence than the bus topology.

- Advantages of star topology.
- Easy to fault identification and fault isolation.
- Star topology is cost-effective as it uses inexpensive coaxial cable.
- It is Robust. If one link fails only that link will affect and not other than that.

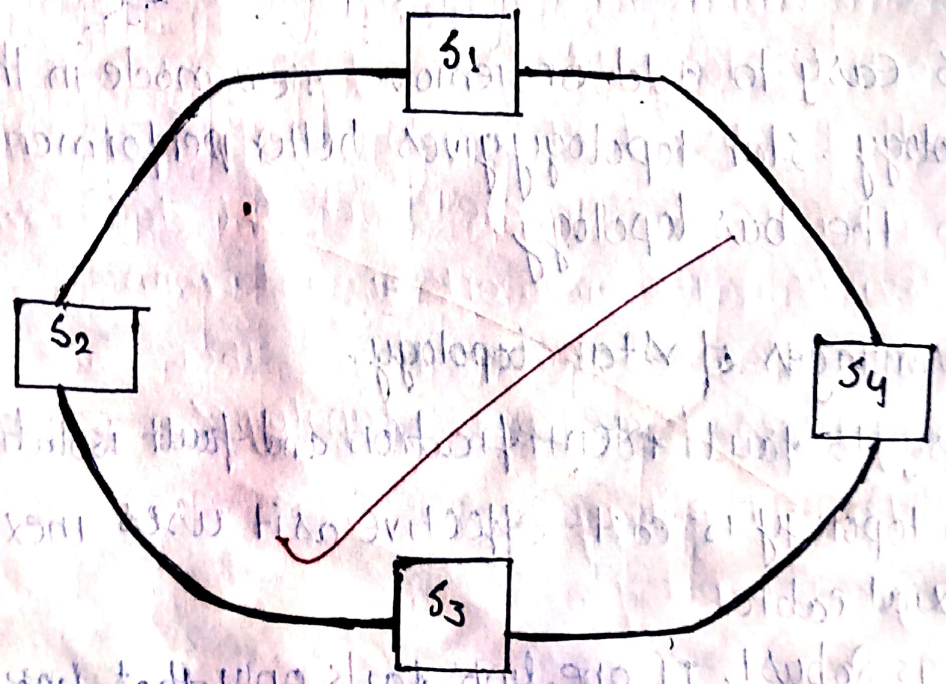
- Disadvantages:-
- If the hub on which the whole topology relies fails, the whole system will crash down.

- The cost of installation is high.

3) RING TOPOLOGY:-

In a Ring Topology, it forms a ring connecting devices with exactly two neighboring devices. A number of repeaters are used for Ring topology with the large number of nodes. In this topology data flows in one direction.

Token is a frame that circulates around the network. Token passing is the most common access method of ring topology. Token passing is a method in which a token is passed from one node to another node.



- Advantages.
- The data transmission is high speed.
- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.

Disadvantages

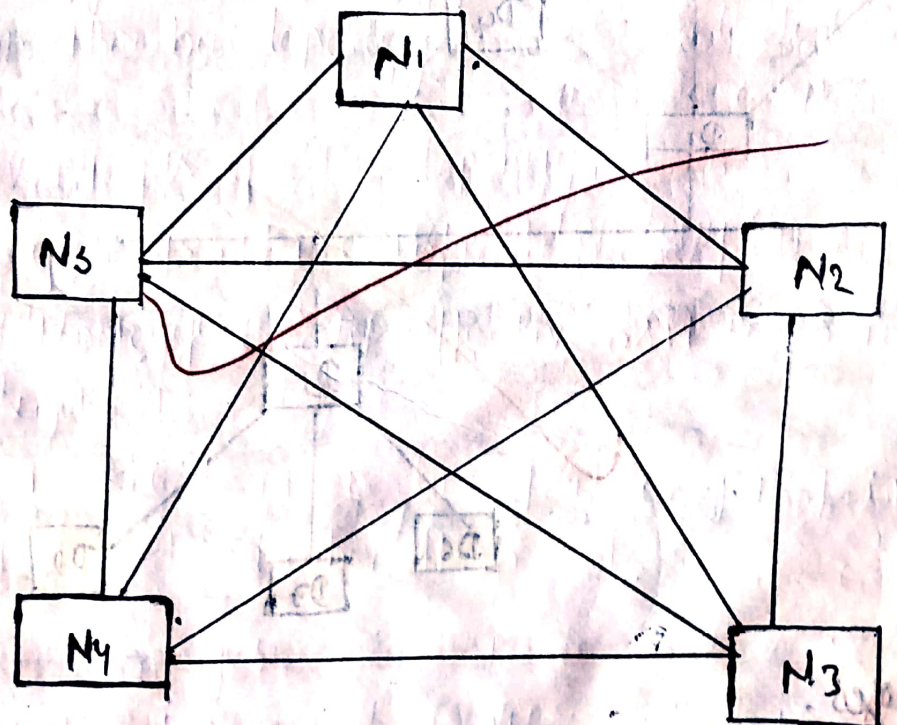
- The failure of a single node in the network can cause the entire network to fail.
- The addition of stations/node in between or the removal of station can disturb the whole topology.
- Less secure.

4) MESH TOPOLOGY :-

In a mesh topology every device is connected to another device via a particular channel. Every node sends it's own signal and data to the another nodes of the system.

Number of cable used = $\frac{n(n-1)}{2}$

where n = number of nodes



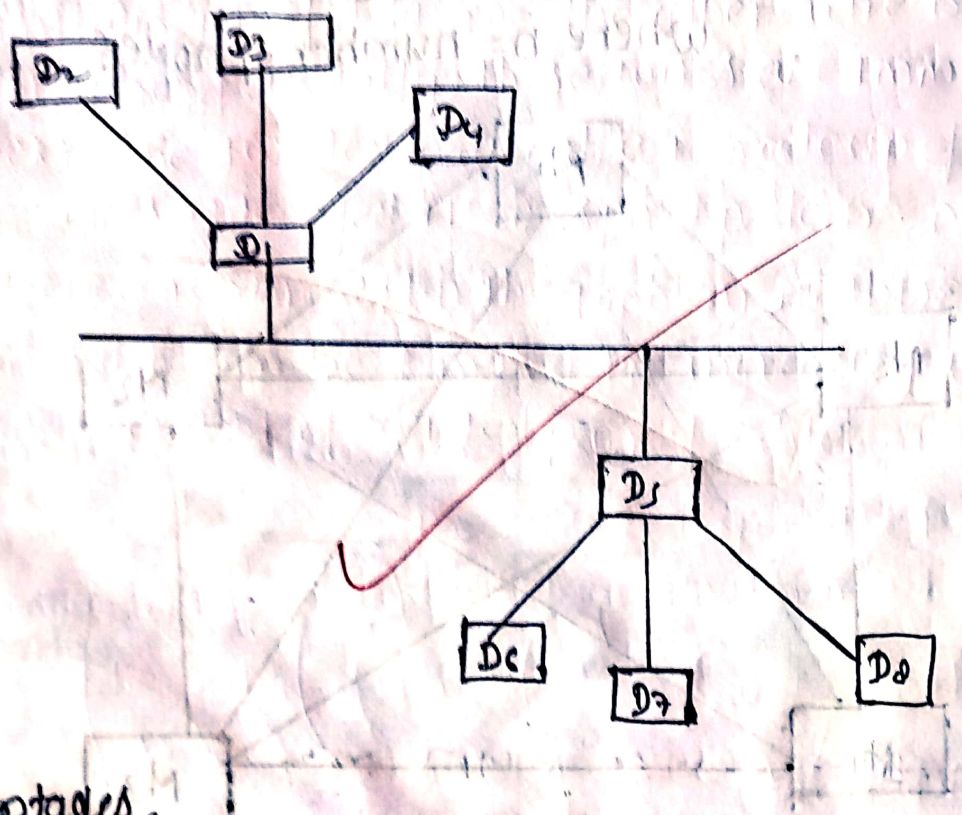
Advantages :-

- Communication is very fast between the nodes.

- Mesh topology is robust.
- The fault is diagnosed easily.
- Provides security and privacy.
- Disadvantages.
- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

5) TREE TOPOLOGY

It's a combination of Bus and Star topology. It is also known as Bus-star topology. In tree topology the whole network is divided into segments which can be easily managed and maintained.



- Advantages.
- It allows more devices to be attached to a single central hub thus it decreases the distance that

is travelled by the the signal to come to the devices.

- It allows the network to get isolated and and also prioritize from different computers.
- Error detection and erro correction is very easy in this topology.
- Disadvantages.
- If the central hub gets fail the entire system fails.
- The cos is high because of cabling.
- If the new devices are added. it becomes difficult to reconfigure.

Server AND Client :-

Server :- A server is a computer, device or program that provides services, resources, or data to other computers over a network. It listens for incoming requests from clients and responds them accordingly.

Client :- A client is a computer, device or program that requests services, resources or data from a server. It initiates communication with the server by sending a request and waits for the server respond.

DATA TRANSMISSION MEDIUM :-

A data transmission medium refers to the physical pathway or channel through which data is

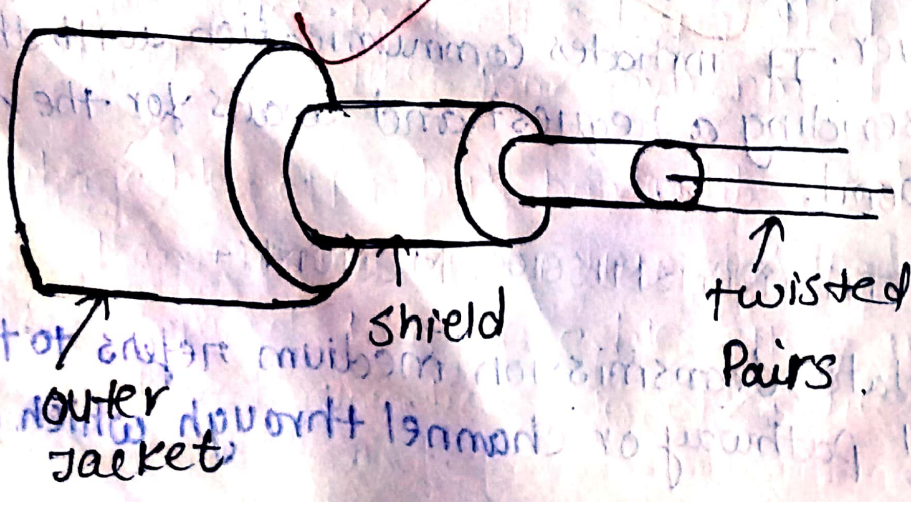
transmitted from one device or system to another. It can broadly classified into two categories.

1. Wired (guided) transmission media:-

Wired transmission media refers to physical cables or wires used to transmit data between devices in a network. This type of transmission is also called guided media because the signals are guided along a solid medium. There are several types of wired transmission of media.

(i) Twisted pair Cable:-

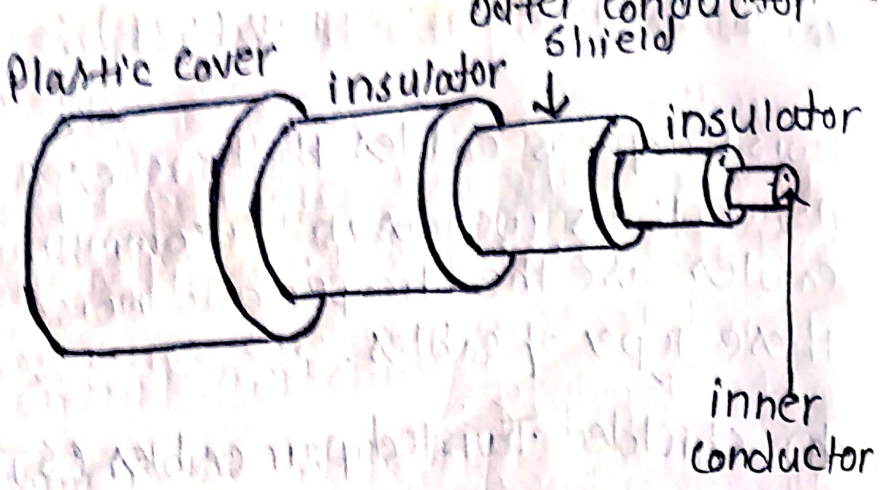
As the name suggests these are two twisted pairs of cables or wires made up of insulated copper. These are twisted togeather in such a way that they run parallelly, one wire is used for transmission of data and the other wire is used for ground. Usually, these wires are 1mm in diameter. The twisted-pair cable is made up of 2 copper wires arranged in a spiral pattern. Noise interference is more often the problem in these cables but it can be handled by increasing numbe of turns per foot of twisted pair of cable.



(a) Unshield twisted pair (UTP) :- UTP cables are the most common twisted pairs cables that are used in computer network as well as in telecommunication. These cables are the cheaper and noise is high in these type of cables.

(b) Shielded Twisted pair cables (STP) :- In comparison to UTP's, shielded twisted pair cables are costlier and consist of metal foil sometimes made up of insulated conductors. Metal foils help to improve the quality of the wire which otherwise will be affected by the noise. These cables are used to reduce cross-talk and the inteference caused due to electro-magamatic waves. In these types of cables transmission rate of data is fast.

(ii) Co-axial cable :- The most common type of transmission media that is used in various application like tv wires and ether-net connection setup also. This is a form of transmission media that consists of two conductors kept parallel to each other. It has a central core conductor of a solid copper wire enclosed in an insu-lating sheet and the middle core conductor is made up of copper mesh and lastly and outer metallic wrap that helps in noise cancellation. The whole cable is covered an protected by plastic cover. It is considered better than twisted-pair cables because of the higher frequency range.



(iii) optical fibers cables :-

optical fiber cable is a type of cable that uses light to transmit data over long distances. It consists of a core made of glass or plastic, surrounded by a cladding layer that reflects light back into the core, preventing signal loss. The core's diameter is very small, typically measured in micrometers.

Key components include:-

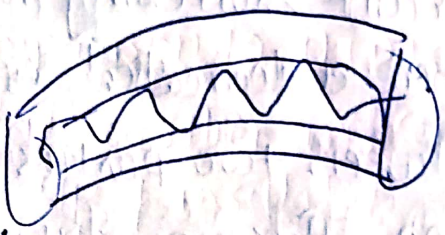
1) Core :- The central part where light travels.

2) Cladding :- A layer that keeps the light contained in the core through total internal reflection.

3) Jacket :- The outer protective layer that shields the fiber from environment damage

Optical fiber cables offer high bandwidth, enabling faster data transmission with minimal signal degradation compared to copper cables. They are widly used in telecommunications, internet services, and medical applications.

→ Core → made up of glass or plastic that is central part.
↳ Cladding layer - that reflects light back to core.



Wireless transmission Media :-

Wireless transmission media refers to methods of transmitting data over the air without physical cables. This includes various technologies and frequencies used for communication. such as :-

(i) Radio Waves :- Used in broadcasting, mobile networks and Wi-fi, suitable for long range transmission.

(ii) Microwaves :- Employed for point to point communication and satelite links, requiring line-of-sight.

(iii) Infrared :- Used for short-range communication, such as remote controls and some wireless peripherals.

These technologies enables flexible communication in various application, from mobile phones to satellite communication.

Switching :-

Switching generally refers to the process of changing of from one state, condition to another.

1) Circuit switching :-

Circuit switching is the method of communication where a dedicated communication path is established between two parties, for the duration of conversation. This means that once the connection is made, the entire bandwidth of the circuit is reserved exclusively for that session, ensuring a consistent and reliable flow of data.

This method is commonly used in traditional telephone network.

Advantages :-

- The dedicated circuit established between sender and receiver provides a guranteed data rate.
- Once the circuit is established data is transmitted without delay, there is no waiting time at each switch.
- Since a dedicated path is established the method is suitable for continious transmission.

- Disadvantages :-
- As the channel is dedicated it can not be used to transmit any other data even if the channel is free.

- It requires more bandwidth.
- Prior to the actual data transfer the time required to established a link between to station is to long.

2) —: Message switching :—

In message switching it is not necessary to established a dedicated path between transmitor and receiver. In message switching source node sends a message to the destination node or address is appended to the message. So in the message switching no need to established dedecated path between two communication nodes.

- for message sending there are many intermediatery message switching nodes which are responsible for transfering message. The message is transfered as a whole from source node to destination node.

for each message switching node receives the entire message and store it entirly on disk and then transmitted to the next node, if the next node does not have enough space the message is stored and switch waits.

"This type of network is called store and forward network".

- Advantages :-
- flexible routing :- message can be routed based on current network conditions, improving reliability and avoiding congested path.

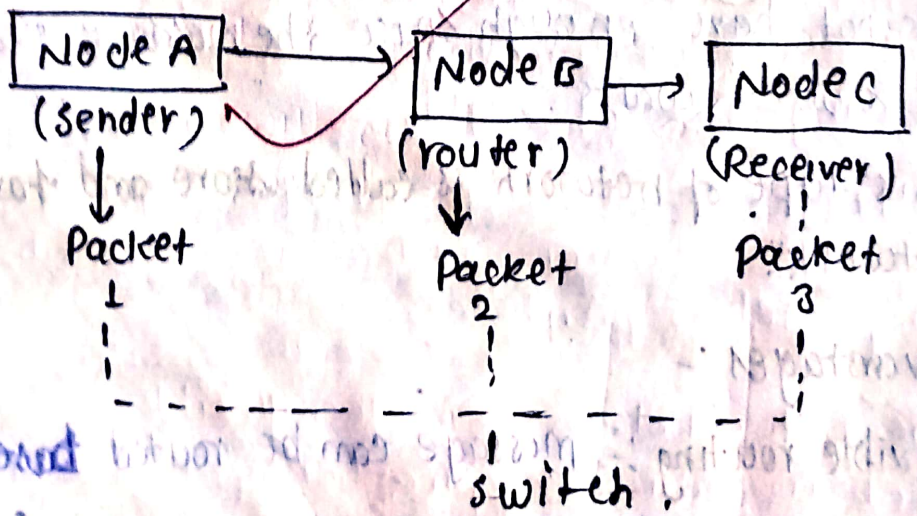
- It can handle message of different sizes without needing a pre-established path.
- Easily accommodates varying amounts of traffic without requiring dedicated circuits.

① Disadvantages :-

- message can experience delays due to the store-and forward process, which may not be suitable for real time communication.
- managing message storage and routing can be more complex than simpler switching methods.
- Unlike circuit switching, there's no dedicated path, which might lead to less predictable performance.

③ —: Packet Switching :—

Packet switching is a method of data transmission where data is broken into smaller packets, each sent independently over the network. Each packet may take different path to the destination, where they are reassembled and correct order.



- Node (A) is sender, or called source node where data is generated.
- Node B (Router): Intermediate node that route packet through the network.
- Node C (Receiver) :- The destination node where the data is reassambled.

- **Advantages :-**
- It utilizes network resources more effectively, allowing multiple communications to share the same bandwidth.
- If a rout fails, packet can be rerouted through the alternate path, enhancing reliability.
- It supports the different types of data (voice, video, text) in a mixed traffice environment.
- Each packet can include error-checking machanisms, allowing for retransmission of lost or corrupted packets.

- **Disadvantages :-**
- Packet can experience delays as they may take different routes to reach the destination.
- At the destination, packets must be reassembled in the correct order, which can complicate processing.
- Larger messages may need to be fragmented into smaller, which can lead to potential loss or errors during transmission.

Bandwidth :- Bandwidth refers to the maximum rate of data transfer across a network or communication channel in a given ammout of time, typically measured in bits per seconds (bps).

i) Network model :-

The network model is a data structure used to represent and manage complex relationship between various entities, typically in the context of databases and information system.

ii) Client-server network model :-

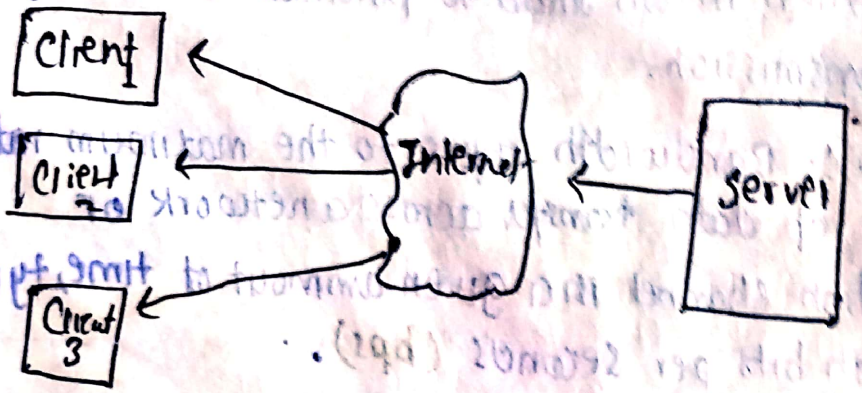
The client-server model is a network architecture where a server provides resources or services and client request them.

server :-

- A powerfull machine that stores, manages and processes data.
- Provides services like databases, file storage, web hosting etc.
- Typically always on and can handle multiple client requests simultaneously.

client :-

- Any device (PC, smartphone, etc) that accesses the server's resources.
- Sends requests to the server and waits for response
- Users intract with client to perform task that requires server resources.



(ii) Peer-to-Peer network model.

Peer-to-Peer (P2P) is a decentralized network model where each participant (or 'peer') can act as both a client and a server. In this model, peers can share resources, files, or information directly with one another without the need for a central server.

:- Key features :-

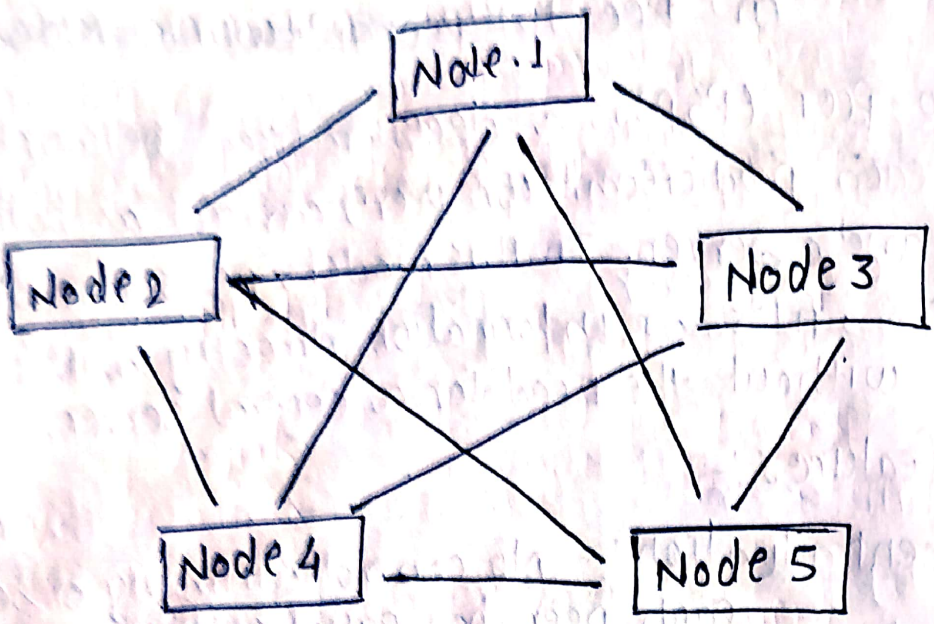
(i) Decentralization :- No control authority or server, each peer has equal status and can initiate or complete transaction.

(ii) Resource sharing :- Peers can share files, bandwidth, and processing power, making it efficient for distributing large amounts of data.

(iii) Scalability :- P2P networks can/share files easily expand as more peers join, improving overall capacity and redundancy.

(iv) Fault Tolerance :- Since there is no signal point of failure, the network can continue to function eveven if some peers go offline.

- Advantages :-
- Increased resilence and redundancy.
- Efficient resources utilization.
- Greater privacy for users.
- Disadvantages :-
- Potential security risks, such as exposure to malwa
- Difficulty in managing and controlling the network.
- Variable performance depending on the number of active peers.



-: P2P Architecture :-

-: NETWORK SOFTWARE :-

Network software contains a broad range of software used for design, impliments and operation and monitering of computer network.

Protocols :- A protocol is a set of rules and conventions agreed upon and followed by the Community entities for data Communication. A protocol outlines that, what and how and when of a Communication.

The three aspects of protocols are.

(i) Syntax :- It defines the format of the data that is to be sent or received.

(ii) Semantic :- It defines the meaning of each section of bit that are transfred

(iii) Timing :- It defines the time at what data

is transferred and at which speed data is transferred.

-: PROTOCOL HIERARCHIES :-

Generally, computer networks are comprised of or contain a large number of Hardware and Software. For network design, various networks are organized and arranged as a stack of layers of hardware and software, one on top of another. The number name, content and function of each layer might vary and can be different from one network to another. The main purpose of each layer is to provide services to higher layers that are present.

"A protocol Hierachy is a fixed set of rules and conventions that govern the communication between two or more computers. The hierarchical structure allows for modular design, interoperability, and ease of implementation in computer networks."

Example :-

Below is diagram representing a five-layer network. The diagram shows communication between Host 1 and Host 2. The data stream is passed through a number of layer from one host to other. Virtual Communication is represented using dotted lines (and) between peer layers. physical communication is represented using solid arrows between adjcent layers. Through physical medium actual communication occurs. The layer are same level commonly known as peers. The peers basically has a set of protocols. An

interface is present between each of layer that are used to explain services provided by layers to lower layer to higher layer.

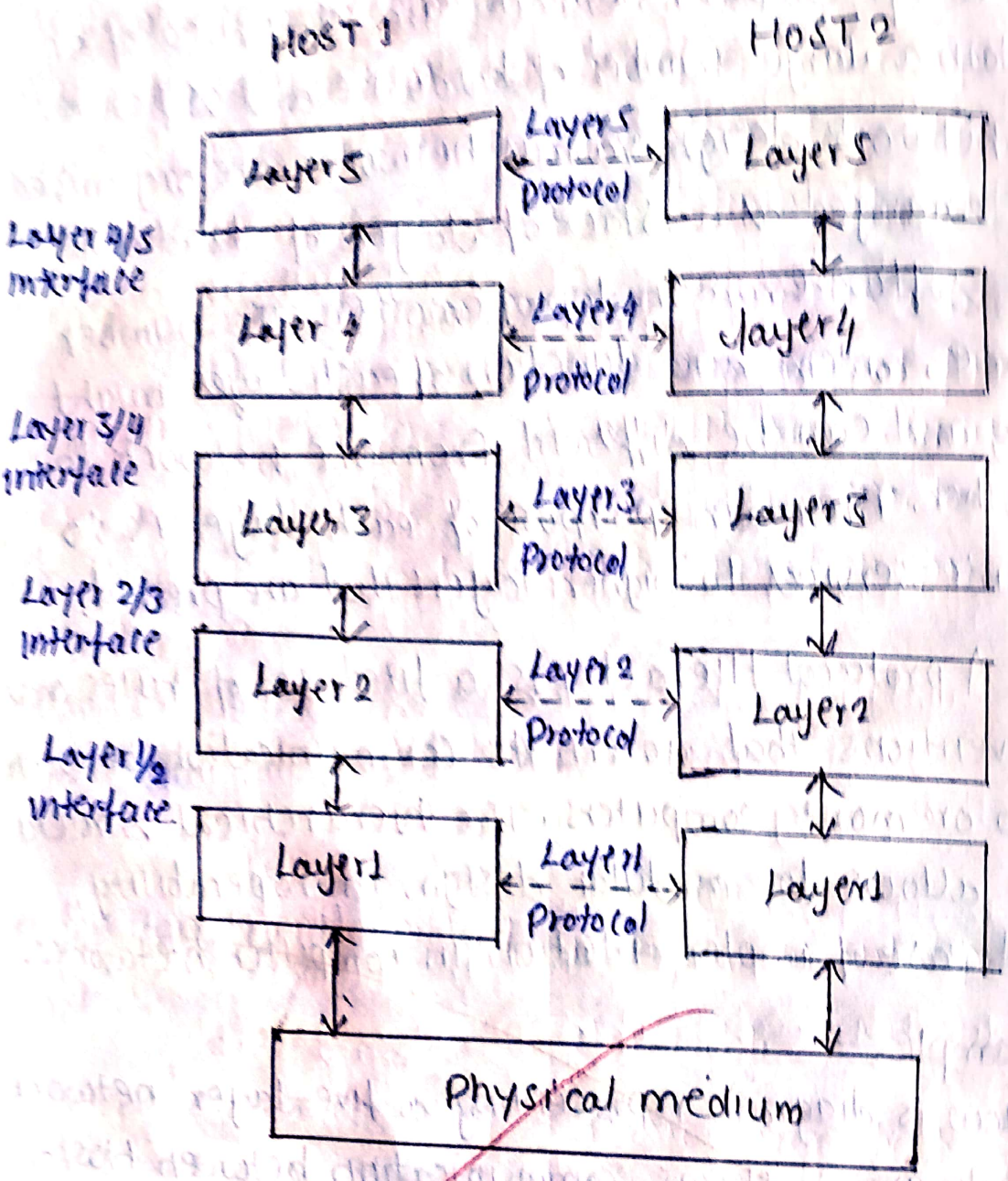


Fig:- PROTOCOL Hierarchies:-

- Advantages.
- The layers generally reduce complexity of communicati between networks.
- It increases network lifetime.
- It also uses energy efficiency.

• Disadvantages :-

• Implementation of protocol hierarchy is very costly.

• Protocol Hierarchy require a deep understanding of each layer of OSI model.

• protocol Hierarchy is not scalable for complex networks.

IPV4 :-

An internet protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the internet Protocol for communication. An IP address serves two main functions: host or network interface Indentification and location addressing.

Internet protocol version 4 (IPV4) defines an IP address as a 32-bit number. However because of the growth of the internet and the depletion of available IPv4 addresses, a new version of IP : using 128 bits. for IP address, was standardized in 1998. IPv6 deployment has been ongoing since the mid-2000s.

IPV6 :- Internet protocol version 6 (IPV6) is the most recent version of the internet protocol (IP), the communication protocol that provides and an identification and location system for computers on networks and routes traffic across the internet, it is 128 bit number.

• TCP :- Transmission control protocol is a standard that defines how to establish and maintain a network conversion through which application programs can exchange data. TCP works with the internet protocol (IP), which defines how computers send packets of data to each other, Together, TCP and IP are the basic rules defining the internet.

• UDP :- User datagram protocol (UDP) is a Transport layer protocol. UDP is a part of internet protocol suite, referred as UDP/IP suite. Unlike TCP, it is unreliable and connectionless protocol so. there is no needs to establish connection prior to data transfer.

TCP VS UDT

TCP	UDP
• Connection oriented protocol	Datagram oriented protocol
• Reliable	Unreliable.
• Extensive error checking mechanism.	Basic error checking.
• Sequencing of data.	No sequencing.
• Slower.	faster, simpler and efficie
• Retransmission is possible	Not possible.
• Heavy weight doesn't support broadcasting. Ex. HTTP, RTP etc	Light weigh support broadcasting. Ex. DNS, DHCP, etc

Some Important Full Forms :-

TCP - Transmission control protocol.

UDP - User datagram protocol.

FTP - File transfer Protocol.

SMTP - Simple mail transfer protocol.

TELNET - Telecommunication network.

ARP - Address resolution protocol.

RART - Reverse address resolution protocol.

Igmp - Internet group management protocol.

PoP_3 - Post office protocol.

SNMP - Simple network management protocol.

FTTP - Fibre to the premises.

ICMP - Internet control message protocol.

HTTP - Hyper text transfer protocol.

TCP/IP Model

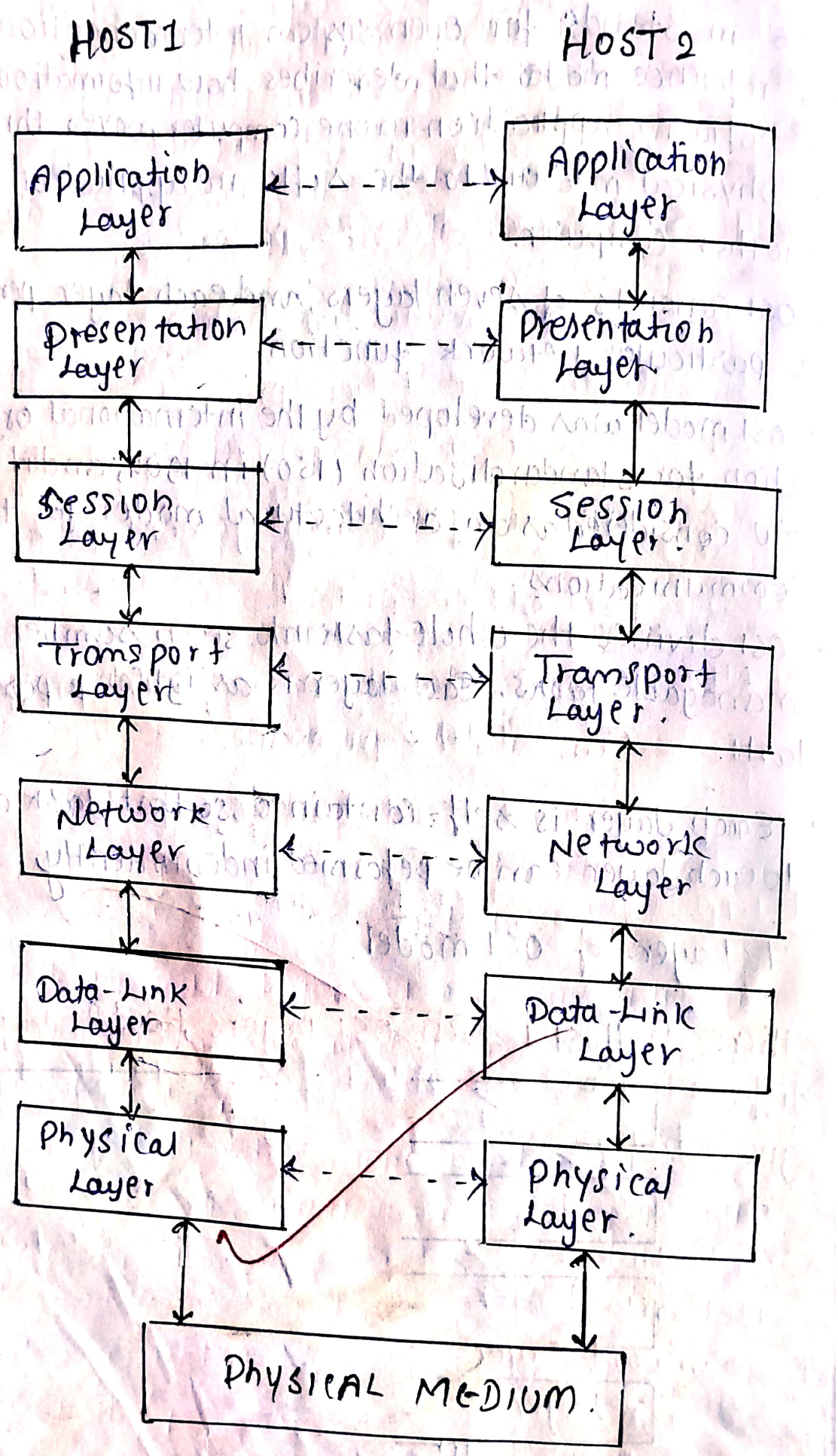
OSI MODEL

- 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 performs a particular network function.
- OSI model was developed by the international organiz-ation for standardization (ISO) in 1984; and it is now considered as an architectural model for the communications.
- OSI divides the whole task into seven smaller and managable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be peformed independently.

7 Layers of OSI model.

There are the seven OSI layers, Each layer has different functions. A list of seven layers are given below.

1. Physical Layer
2. Data-Link Layer.
3. Network Layer
4. Transport Layer.
5. Session Layer.
6. Presentation Layer.
7. Application Layer.


HOST 1
HOST 2
Application Layer
Application Layer
Presentation Layer
Presentation Layer
Session Layer
Session Layer
Transport Layer
Transport Layer
Network Layer
Network Layer
Data-Link Layer
Data-Link Layer
Physical Layer
Physical Layer
PHYSICAL MEDIUM

(1) Physical Layer

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data link layer, which will put the frame back together.

- The physical layer also defines the transmission rate. i.e. the number of bits sent per second.
- Physical layer also defines how the data flows between the two connected devices. The various transmission modes possible are simplex, half-duplex and full duplex.

(2) Data Link Layer (DLL)

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it's a responsibility of the DLL to transmit it to the Host using it's MAC address.

- The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frame.

(3) Network Layer

The network layer work for the transmi-ssion of data from one host to the other located in different networks. It also takes care of packet routing. i.e. selection of the shorte-st path to transmit the packet, from the number of routes available. The sender & receiver's IP addresses are placed in the header by the network layer.

(4) Transport layer.

Transport layer OSI model की चौथी layer है, इस Layer का प्रयोग Data को network के मध्य में से सही तरीके से transfer किया जाता है, इस Layer का कार्य दो computers के मध्य communication establish कराना भी है, इसे segment unit भी कहा जाता है,

function of transport Layer :-

- Transport layer का प्रमुख कार्य data को एक Computer से दूसरे Computer तक transmit करना है,
- जब यह layer अपरी layers से message को Receive करती है तो यह message को बहुत सारे segments में विभाजित कर देती है,
- प्रत्येक segmet का एक sequence number होता है जिससे प्रत्येक segment को आसानी से identify किया जाता है,
- यह दो प्रकार की service प्रदान करती है, connection oriented and connection less,
- यह flow control & error control दोनों प्रकार के कार्यों को करती है,

(5) Session Layer

Session layer OSI model की 5th layer है, जो कि बहुत सारे computers के मध्य connection को नियंत्रित करती है,

Session Layer दो Devices के मध्य Communication के लिए session उपलब्ध कराता है, अर्थात् जब भी कोई user कोई भी website खोलता है तो user के computer system तथा website के Server के मध्य तक session का निर्माण होता है,

Session Layer का मुख्य कार्य यह देखना है कि किस प्रकार connetion को establish, maintain & terminate किया जाता है,

:- Functions of Session layer :-

- Session Layer dailog controller की भाँति कार्य करती है, यह दो Process के मध्य dailog create करती है,
- यह synchronization के कार्य को पूरा करती है, अर्थात् जब भी transmission में कोई error आ जाता है तो transmission को दुबारा किया जाता है,

Protocal used :- Net BIOS, ZIP, APIS, Sokets, ASP etc.

(6) Presentation Layer :

इस Layer का उपयोग data का encryption तथा decryption के लिए किया जाता है, इसे data Compression के लिए भी प्रयोग किया जाता है, यह layer O.S. से संबंधित है,

It is responsible for preparing data for application layer.

Presentation layer is responsible for syntax, semantics, & Compression.

Function of Presentation Layer :-

- इस layer का कार्य encryption का होता है, privacy के लिए इसका use किया जाता है

इसका मुख्य कार्य compression का भी है। Compression बहुत जरूरी होता है क्योंकि data को compress करके इसके Size को कम कर सकते हैं।

- Protocol used :- ASCIII, NDR, XDR, EBCDIC, SSL, SSH, etc.

Encyption :- It is the process of protecting information or data by using mathematical models to scramable it is such a way that only the parties who have the key to unscrambe it can access it.

(7) Application Layer

This the only layer that only directly interact to Host. इसका मुख्य कार्य हमारी real application तथा अन्य Layers के बीच interface करती है, यह layer user के सबसे नजदीक होती है, यह layer यह नियंत्रित करती है कि कोई भी application किस प्रकार network से access कराती है।

:-Function of Application Layer:-

- Application Layer के द्वारा used remote computer से files को Access कर सकता है, और files को reliable करता है।
- यह email को forward और store करने की सुविधा देती है।
- इसे द्वारा हम Database से directory को access कर सकते हैं।

→ ① Difference Between OSI and TCP/IP model.

Parameters	OSI model	TCP/IP Model.
Full Form	OSI stands for open system Interconnection	TCP/IP stands for Transmission control protocol/ Internet protocol.
Layers	It has 7 layers	It has 4 layers.
Usage.	It is low in usage	It is mostly used.
Approach	It is vertically approached	It is horizontally approached.
Reliability	It is less reliable than TCP/IP model	It is more reliable than OSI model.
Protocol Example.	Not tied to specific protocols, But, example include. HTTP, SSL/TLS, TCP, etc.	HTTP, FTP, TCP UDP, IP, Internet.

UNIT-02 PHYSICAL

The physical layer is the first and lowest layer from the bottom of the 7 Layered osi model and delivers security to hardware. This layer is in charge of data transmission over the physical medium It is the most complex layer in the osi model.

The physical layer converts the data frame received from the data link layer into bits. i.e. interms of ones and zeros. It maintains the data quality by implementing the required protocols on different network modes and maintaining the bit rate through data transfer using a wired or wireless medium.

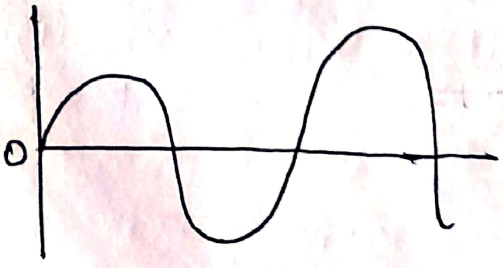
:- Attributes of the physical layer :-

The physical layer has several attributes that are implemented in the osi model.

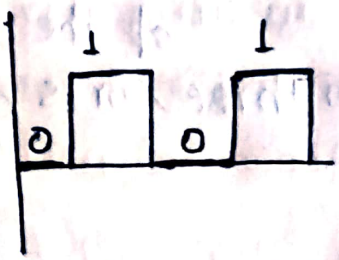
1. Signals : The data is first converted to a signal for efficient data transmission. There two kinds of signals.

(i) Analog Signals :- These signals are continuous waveform in nature and are represented by continuous electromagnetic waves for the transmission of data.

All the real life signals are analog signals ex : colours, heat, sound wave etc.



(ii) Digital signals: These signals are discrete in nature and are represented by continuous) e network pulses and digital data from the upper layers.



2) Transmission media:- Data is carried from source to destination with the help of transmission media. There are two sorts of transmission media.

(i) Wired media:- The connection is established with the help of cables. for example; fiber optic cables, coaxial cables, and twisted pair cables.

(ii) Wireless media:- The connection is established with the help of ~~(cables. for example fiber optic cables, coaxial cables, and twisted pair cables)~~ using wireless communication network. for example, Wifi. Bluetooth, etc.

3. Data flow:- It describes the rate of data flow and the transmission time frame. The factors affecting the data flow are as follows:

- Encoding: Encoding data for transmission on the channel.
- Error-rate: Receiving erroneous data due to noise in transmission.

Bandwidth:- The rate of transmission of data over the channel.

4. Transmission mode:- It determines the direction of the data which data can be transmitted in which form of transmission mode as follows.

- Simplex mode:- This mode of communication is one-way communication where a device can only send data. Examples are mouse, keyboards etc.
- Half-duplex mode:- This mode of communication supports one-way communication i.e. either data can be transmitted or received. An example is a walkie-talkie.
- Full duplex mode:- This mode of communication supports two-way communication. i.e. the device can send and receive data at the same time. An example is cellular communication.

5. Noise in transmission:- Transmitted data can get corrupted or damaged during data transmission due to many reasons. Some of the reasons are mentioned below.

- Attenuation:- It is a gradual deterioration of the network signal on the communication channel.
- Dispersion:- In the case of Dispersion, the

data is dispresed and overlapped during the transmission, which leads to the loss of the original data.

- Data Delay :- The transmission data reaches the destination system outside the specified frame time.

: The physical layer performs various functions and services :

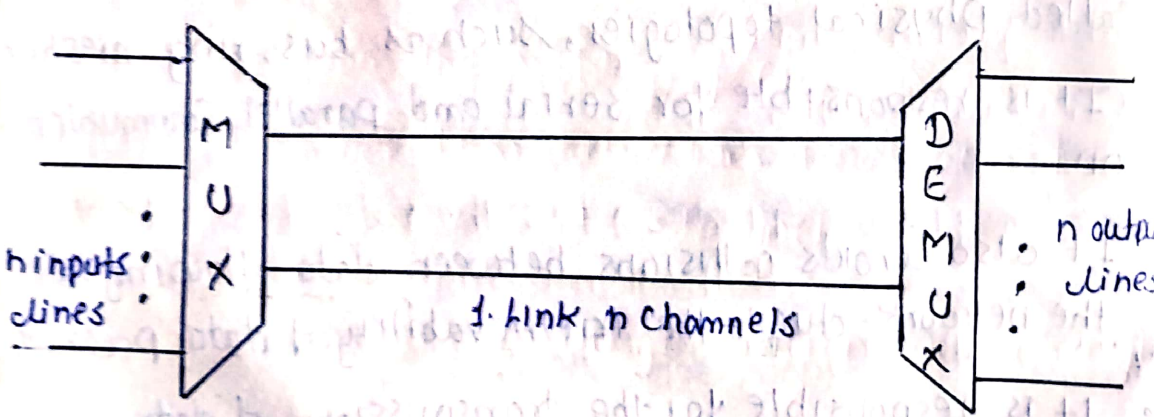
- It transfers data bit by bit or symbol by symbol.
- It performs bit synchronization, which means that only one bit needs to be transferred from one syste to another at a time. There should be no overlapping of bits during transmission.
- Bit rate control defines how many bits per second can be transmitted.
- The physical layer is responsible for knowing the arrangements made between devices in network called physical topologies, such as bus, ring, meshet
- It is responsible for serial and parallel Communicati -on.
- It also avoids collisions between data flowing in the network due to the irretrievability of data packets
- It is responsible for the transmission of data received from the data link layer for further transmission.

:- MULTIPLEXING :-

Multiplexing is a technique used to combine and send 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 inputs lines to generate a single output line. multiplexing follows many-to-one ie. n input lines and one output line.
- Demultiplexing 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.

:- Concept of multiplexing :-



MUX : multiplexer.
DEMUX - Demultiplexer.

- The 'n' input lines are transmitted through a multiplexer and multiplexing combines the signals to form a composite signal.

- plexer and demultiplexer separates a signal to component signal and transfers them to their respective destinations.

Advantages of Multiplexing :-

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

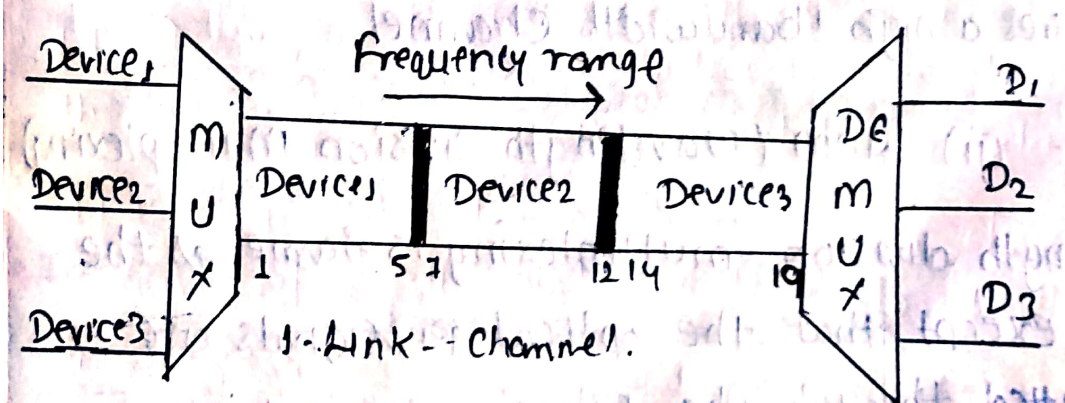
Multiplexing Techniques :-

Multiplexing techniques can be classified as :-

(1) Analog multiplexing
(2) Digital multiplexing

(i) FDM (Frequency Division multiplexing)

- It's an analog technique.
- Frequency division multiplexing is a technique in which the available bandwidth of a single transmission medium is subdivided into several channels.



- In the above diagram, a single transmission medium is subdevided into several frequency channels, and each frequency channel is given to different devices Device1

has the frequency channel from 1 to 5.

- 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.
- FDM is mainly used in radio broadcasts and TV networks.

Advantages :-

- 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.

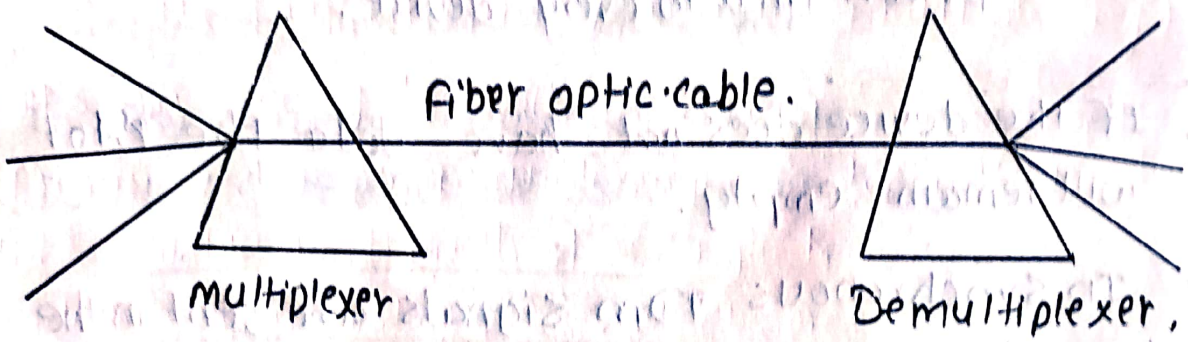
Disadvantages :-

- FDM technique is used only when low-speed channel are required.
- It suffers from the problem of crosstalk.
- A large number of modulators are required.
- It requires a high bandwidth channel.

(ii) WDM (Wavelength Division multiplexing)

- wavelength division multiplexing is same as the FDM execpt that the optical signals are transmitted through the fibre optic cable.
- WDM is used on fibre optics to increse the capacity of a single fibre.

• It is used to utilise the high ... 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 destination
• multiplexing and Demultiplexing can be achieved by a prism.
• Prism can perform a role of multiplexer by combining the various signals to form a composite signal; and the composite signal is transmitted through a fibre optical cable.



(iii) TDm (Time Division Multiplexing)

• It's a digital technique.
• In frequency Division multiplexing technique; all signals operate at the same time with different frequency, but it case of time division multiplexing technique, all signals operate at 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 time slot at which data is to be transmitted by the sender

- In this multiplexing technique data is transmitted one-by-one.

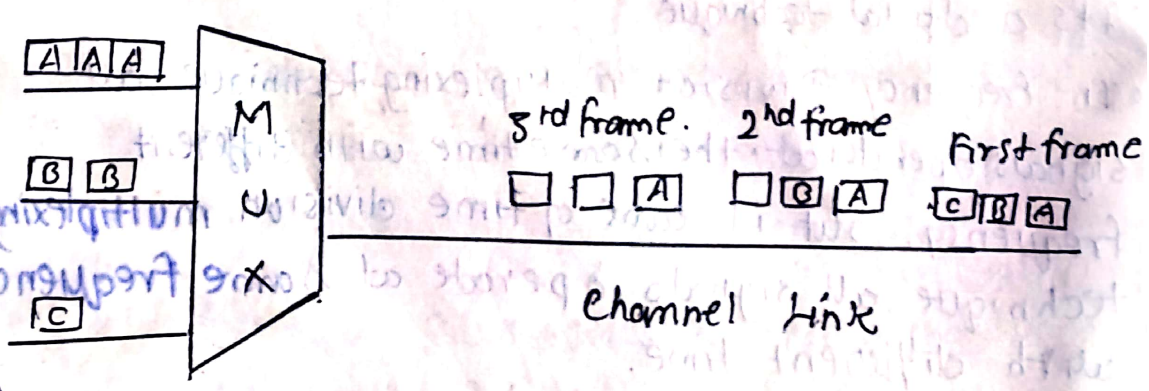
There are two types of TDM:

(i) Synchronous TDM.

(ii) Asynchronous TDM.

(i) Synchronous TDM

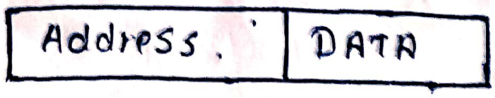
- A synchronous TDM is a technique in which time slot is preassigned to every device.
- If the device does not have data the slot will remain empty.
- In synchronous TDM signals are sent in the form of frames. If a device does not have data for a particular time slot, then the empty slot will be transmitted.

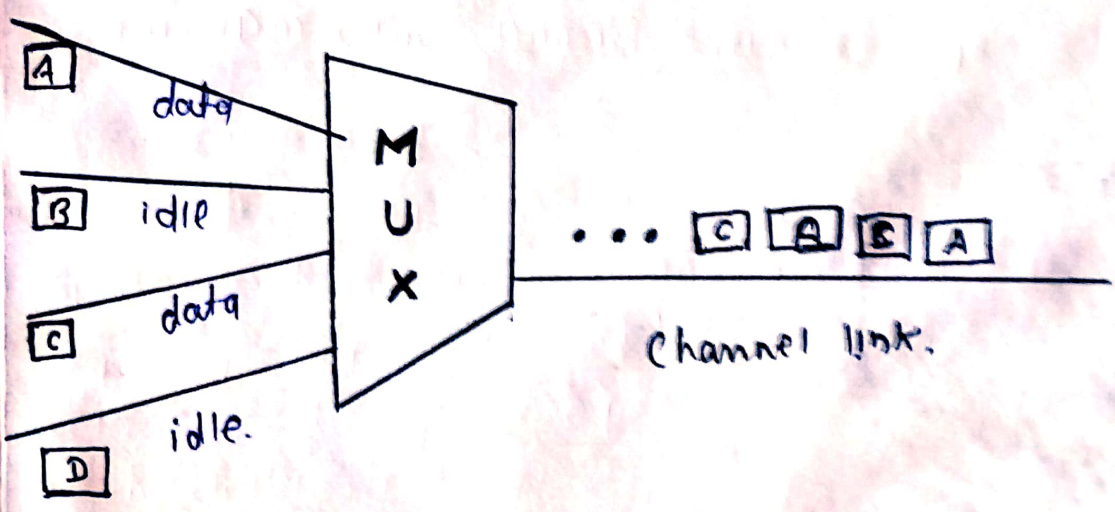


In the above figure, the synchronous TDM technique is implemented. Each device is allocated with some time slot. The time slots are transmitted irrespective of whether the sender has data to send or not.

Asynchronous TDM:-

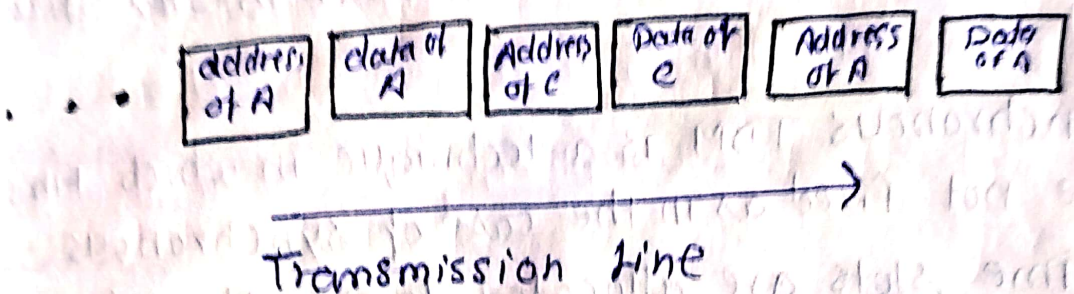
- As asynchronous TDM is also known as Statistical TDM.
- An Asynchronous TDM is a technique in which time slots are not fixed as in the case of synchronous TDM. Time slots are allocated to only those devices which have the data to send. Therefore we can say that Asynchronous Time Division multiplexer transmits the data from active workstations.
- An Asynchronous TDM technique dynamically allocates the time slots to the devices.
- 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, i.e. A and C. Therefore, the data of A and C are only transmitted through the transmission line.

Frame of above diagram can be represented as:-



The above figure shows that the data part contains the address to determine the source of the data.

UNIT- 03 DATA-LINK-LAYER

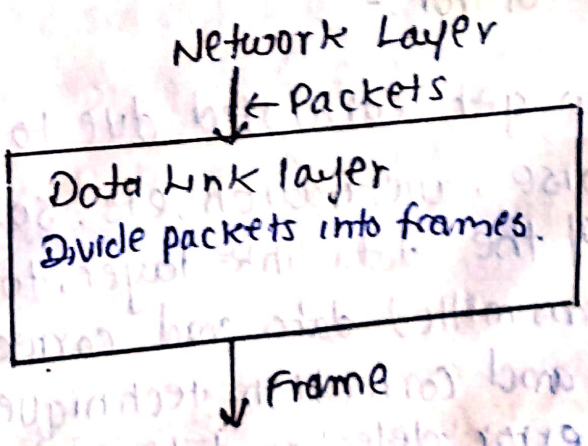
The Data Link layer is the second layer from the bottom in the OSI (open system interconnection) network architecture model. It is responsible for the node-to-node delivery of data. It's major role is to ensure error-free transmission of information. DLL is also responsible for encoding, decoding and organizing the outgoing and incoming data.

This is considered the most complex layer of the OSI model as it hides all the undelying complexities of the hardware from the other above layers.

- The data link layer receives the information in the form of packets from the Network layer, it divides packets into frames and sends those frames bit-by-bit to the uderlying physical layer.

FUNCTIONS OF THE DATA LINK LAYER :-

There are various benefits of data link layers.



(i) Framing :-

The packet received from the network layer is known as a frame in the data link layer at the sender's side. DLL receives packets from the Network layer and divides them into small frames, then, sends each frame bit-by-bit to the physical layer. It also attaches some special bits (for error control and addressing) at the header and end of the frame. At the receiver's end DLL takes bits from the physical layer organizes them into the frame, and sends them to the Network layer.

(ii) Addressing :-

The data link layer encapsulates the source and destination's MAC address / physical address in the header of each frame to ensure node-to-node delivery. MAC address is the unique hardware address that is assigned to the device while manufacturing.

(iii) Error Control :-

Data can get corrupted due to various reasons like noise, attenuation, etc. so it is the responsibility of the data link layer, to detect the error in the transmitted data and correct it using error detection and correction techniques respectively. DLL adds error detection bits into the frame's header so that receiver can check received data is correct or not. It adds reliability to physical layer.

damaged or lost frames.

(iv) Flow Control :-

If the receiver's receiving speed is lower than the sender's sending speed, then this can lead to an overflow in the receiver's buffer and some frames may get lost. So it's the responsibility of DLL to synchronize the sender's and receiver's speeds and establish flow control between them.

(v) Access Control :-

When multiple devices share the same Commu-nication channel there is a high probability of collisi-on, so it's the responsibility of DLL to check which device has control over the channel and CSMA/CD and CSMA/CA can be used to avoid collisions and loss of frames in the channel.

→ Line Discipline in Data link Layer :-

Line Discipline is function of Data link layer. It simply determines and identifies the direction of communication. It is simply process of coordinating half-duplex transmission. i.e. data can be transmitted in both directions on network of data can be trans-mitted in both directions on network of data

3. Line Discipline is done by two types :-

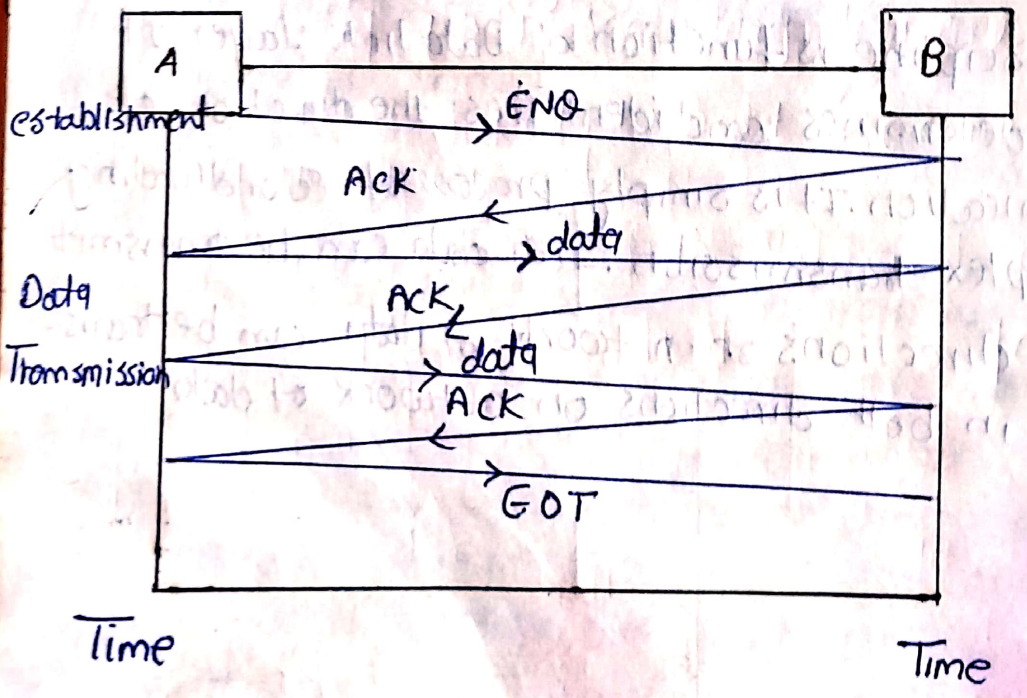
(i) ENQ/ ACK

(ii) Poll/ select

→ Enquery and Acknowledgement :-

ENQ/ACK is used in peer to peer (P2P) communication whenever there are two systems that it is working when two devices are connected to a dedicated link.

It Co-ordinate with the devices which start transmission and wether or not the receipent is ready or not.



EOT :- End of Transmission.

Sender transmit the ENQ frame asking the receiver is available or not. if receive will able it answers with Ack frame if it's ready. If receiver is not ready it will send NAK frame. If the system does not receive any Ack/NAK in specific time then it will assume that the frame is lost it. sender will resend the ENQ frame. It will be tried thrice. if still no response then the sender will disconnect and processed it will again next time.

If response is positive it means Ack, then sender will send the data. if response is negative for three time then sender will disconnect and sender will proceed it in next time.

After sending the data sender ends with the EOT frame.

→ Poll and select :-

It's a part of line discipline which is the part of DLL. It works where one device is primary and second is secondary. primary device control the line and secondary device follow the instructions, secondary device has not power to send instructions. here primary devices determine which device will use the channel and at which time.

Primary device is a initiator of the session. primary device control the link and knows which line is available multi point system guaranteed only one at time. because all control transmission in the primary device.

:- Address :-

- for point-to-point configuration there is no need of addressing because transmission by one will be other.
- for multipoint configuration there must be addressing because primary should identify the secondary devices. Address will appear in the specific part of each frame in Headder or address field/frame.

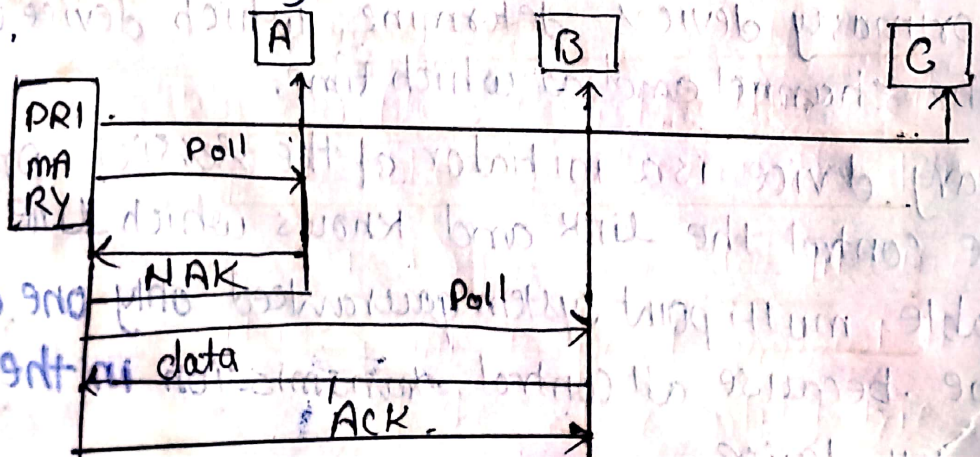
Poll and select is used in primary and secondary communication.

If primary want to receive data it will ask secondary device if they have anything to send.

Polling functions is used by primary to request transmission from secondary, secondary are not allowed to transmit until asked.

when primary is ready it sends poll frame to each device, if first secondary device responces NAK then primary poll, to next secondary if secondary response is data.

then primary will read the data and return the Ack.

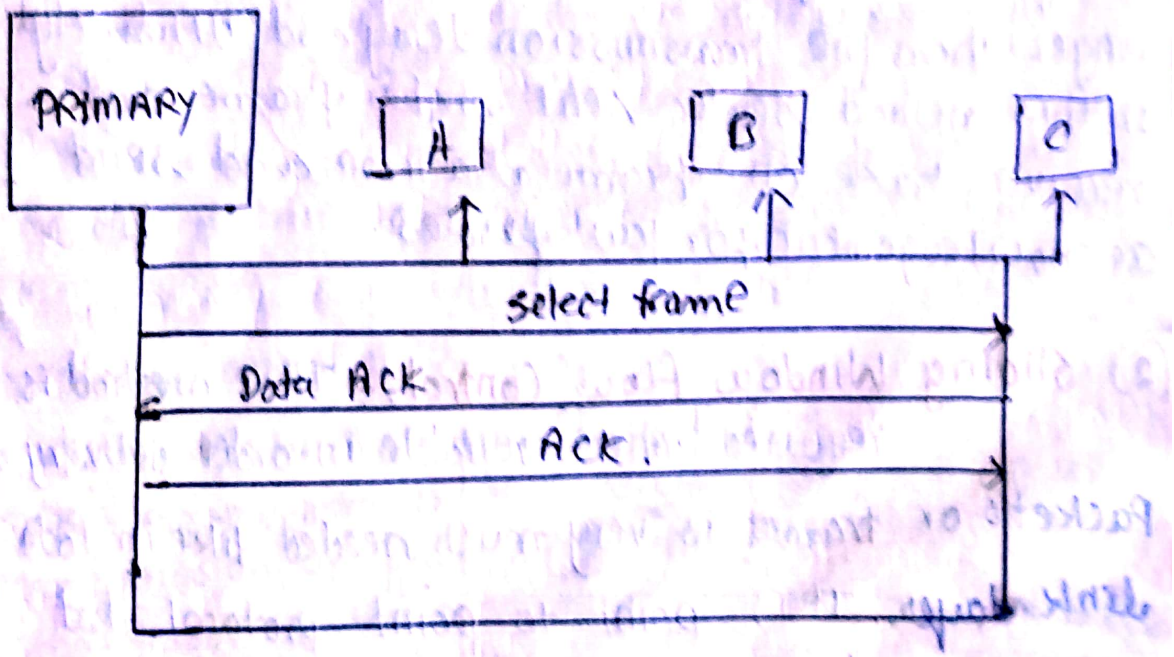


Two possibilities of the (transmitting the) terminating the exchange either secondary will send all data, and finish with EOT or primary say time is up.

If the primary want to send that data, it will send select frame.

It will tell secondary to get ready to receive this function is known select. It is used when primary has something to send. Primary select to to secondary by sele frame to know secondary is ready to receive or not.

One field of select frame contain address of the secondary frame is available for every device. Because in multipoint topology we use single link. Every secondary check address of select field if any device recognize, then it will open frame and read data.



FLOW CONTROL :-

Flow control is design issue at data Link Layer. It is a technique that generally observes the proper flow of data from the sender to receiver. It is very essential because it is possible for sender to transmit data or information at very fast rate and hence receiver can receive this information and process it.

Technique of flow control in Data Layer Link :-

(1) Stop and wait flow control: This method is the easiest and simplest form of flow control. In this method basically message or data is broken down into various multiple frames, and then receiver indicates its readiness to receive frame of data when acknowledgement is received, then only sender will send or transfer the next frame. This process is continued untill sender transmit EOT frame. In this method, only one of frames can be transmitted at a time. It leads to inefficiency i.e. less productivity if propagation delay is very much longer than the transmission delay and ultimately In this method sender sent single frame and receiver take one frame at a time and send acknowledgement for few frames.

(2) Sliding Window flow control :- This method is required where reliable in-order delivery of packets or frames is very much needed like in data link layer. It is point-to-point protocol that assumes that none of the other entity tries to communicate until current data or frame transfer

gets completed. In this method, sender transmits or sends various frames or packets before receiving any acknowledgement. In this method, sender transmits or sender and receiver agree upon total number of data frames after which acknowledgement is needed to be transmitted. Data Link Layer requires and uses this method that simply allows sender to have more that one unacknowledged packet "in-flight" at a time. This increases and improves network throughput, and ultimately In this method sender sent multiple frame but receiver take one by one and after completing one frame acknowledge for few frame.

:- ERROR CONTROL :-

In Error Control we see how can error be Corrected. It used to find out some data is corrupted while sending the data. It is used for error detection and retransmission of frame. It allows to receiver to inform sender about the lost or damaged frame. In the error control It also consider retransmission of lost and damaged frame by informing the sender.

whenever frame is lost frame is sent for retransmission.

STOP AND WAIT ARQ

whenever frame is lost it is sends for recompensation error control is based upon ARQ which means retransmission of frames. It three cases on the basis of that error control take decision that it has to retransmit to data.

(i) Damaged frame (2) lost frame.
(3) lost acknowledgement.

Any time error detected then NAK is returned and ARQ retransmit the specific frame.

One more thing done by ARQ if a frame is not recognised / damaged by the noise it is considered as lost frame. The lost frame is retransmitted to the receiver this is done by ARQ and ARQ perform automatic retransmission.

Stop and wait ARQ is a form of stop and wait flow control protocol which is extended to include retransmission of data frame in case of lost or damaged frame.

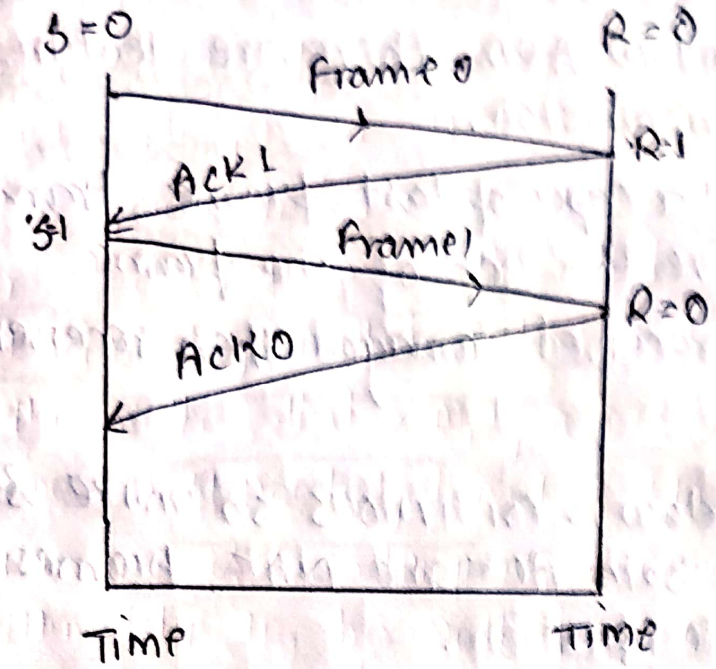
four features are added for retransmission.

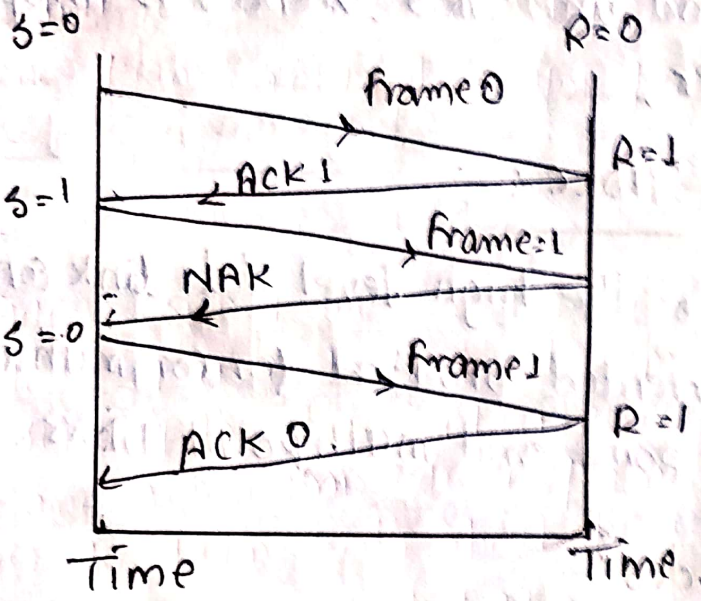
(i) Sender keeps a copy of last frame transmitted untill it receive Ack for that frame.

(ii) Both data and Ack are alternatively numbered as 0's and 1's for identification of duplicate transmission.

(iii) If error is discovered in data frame then it is considered as corrupted frame and NAK is returned from receive. This NAK is not numbe-red and till the sender to transmit the frame.

(iv) Sender is equipped with the timer if acknowledge-ment is not received at time then the sender assume that lost frame was lost, in transmit and send it again.





—; Lost frame case:-

—; Sliding Window ARQ:-

ARQ is a machanism which is used in retransmission. Sliding window ARQ is a part of error control and error control is the part of Link layer control.

It is continious transmission error can detected in this machanism. It's a form of sliding window flow control. machanism. which is extended to include retransmission of data in case of damaged

of lost frame.

In sliding window ARQ there are features are added for retransmission.

(i) sender keeps a copy of last frame transmitted untill it receive the ACK of the frame

(ii) If data is received damaged then receiver sends NAK.

As sliding window is continious so unlike stop and wait ARQ both ACK and NAK frames are numbered for identification.

(iii) Like sto and wait ARQ, sender is equipped with the timer,

:- HDLC :-

HDLC stands for the high level data link control. It is a bit oriented protocol for communication over point-to-point and multipoint links.

:- Transfer modes :-

1) Normal Response mode (NRm) - In this mode the configuration of the stations is unbalanced.

2) Asynchronous Balanced mode (ABm) : - In this mode configuration of the stations is balanced.

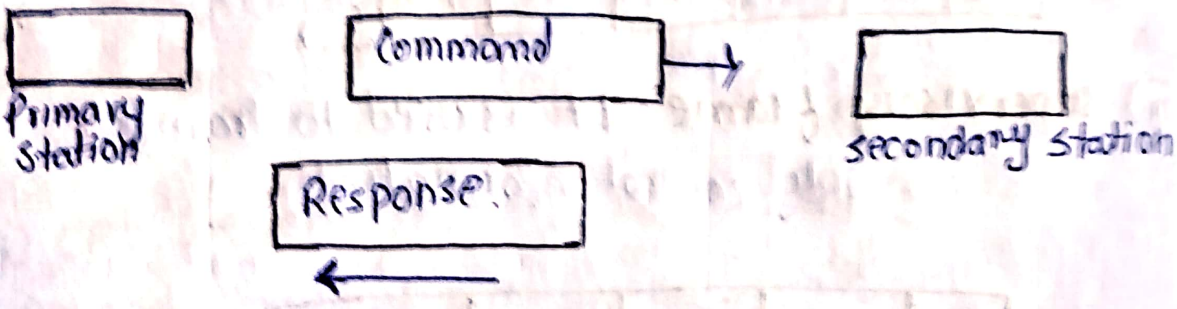
1) Primary stations :- In HDLC there is one primary stations that can send commands.

2) Secondary stations : There are multiple secondary stations, secondary stations

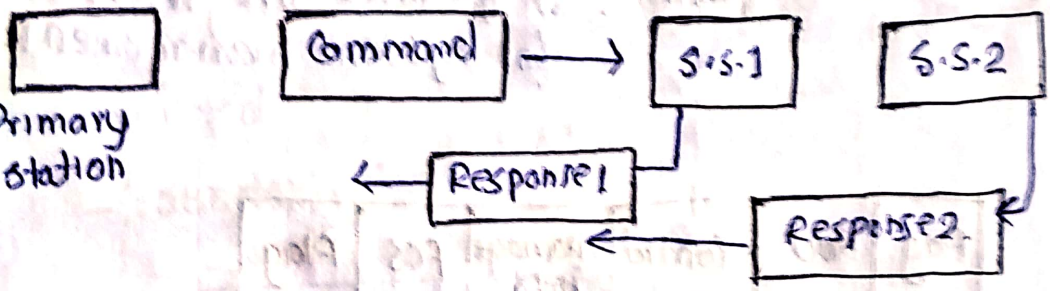
responds the commands send by primary station.

- Normal Response mode is used for point-to-point and multipoint too.

→ Point-to-point NRM

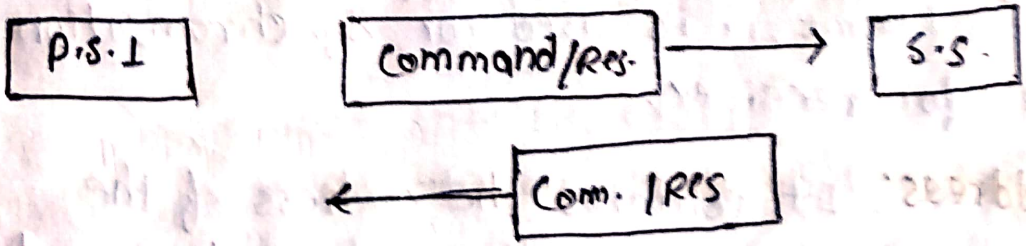


→ multipoint NRM.



- In Asynchronous, there is point to point communication.
- Each station can function as primary & secondary.

Point-to-point ABM

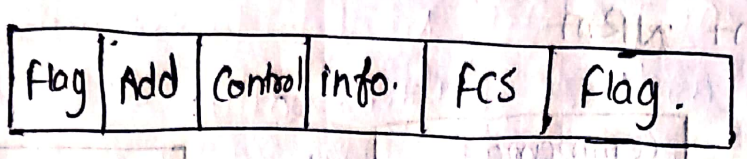


→ Types of frame in HDLC :-

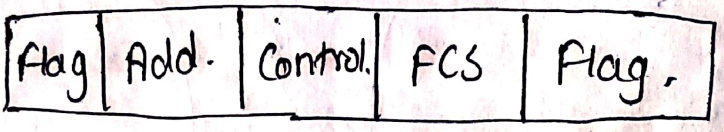
There are three types of frame in HDLC :

(i) Information frame (I-frame)
(ii) Supervisory frame (S-frame)
(iii) Unnumbered frame (U-frame).

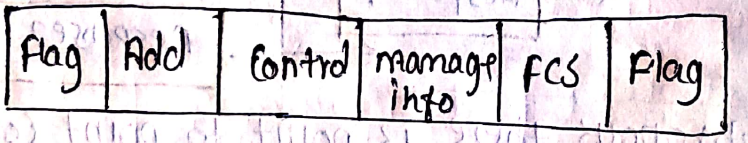
(i) Information frame :- It is used to transfer user data and control information.



(ii) supervisory frame : It is used to transfer only control information



(iii) Unnumbered frame : U-frames are reserved for system management.



Frames of format of HDLC :-

There are upto 6 layers of HDLC.

(i) Flag : It identifies beginning and ending of the frame, it is used for synchronization Pattern for receiver.

(ii) Address : It contains the address of the station (Generally address of secondary station).

(iii) Control field : It's used for error and flow control.

(iv) Information : User data, or management information.

(v) FCS: Frame check sequence, It's the error detection field of HDLC.

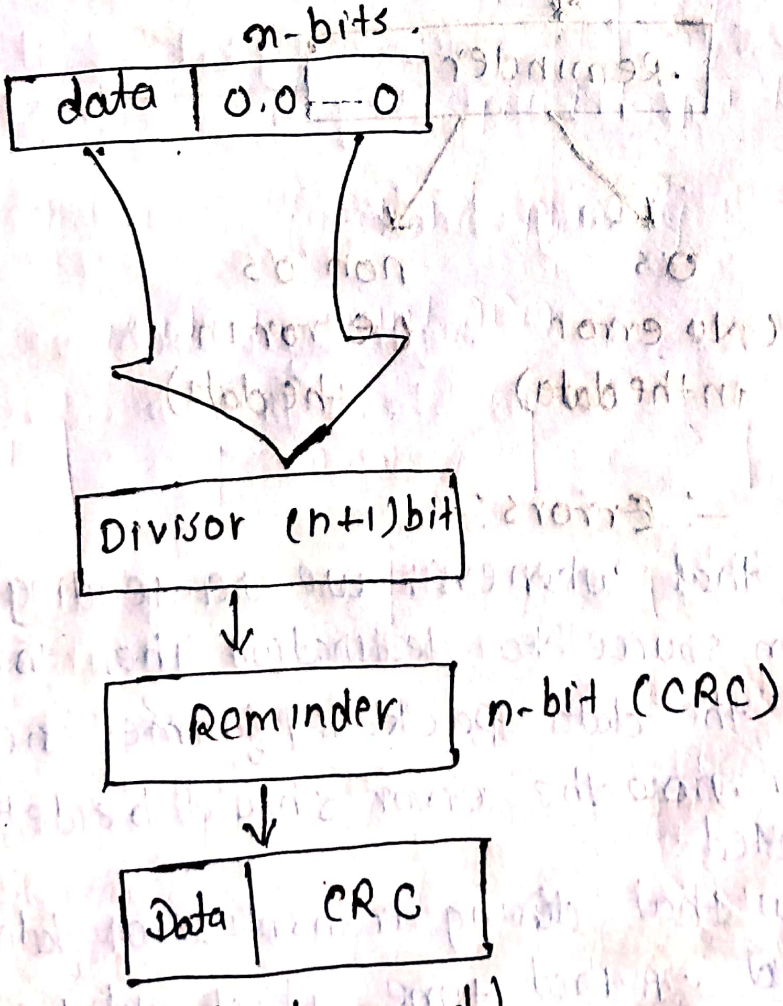
:- CRC :-

CRC stands for the Cyclic Redundancy check. It is based on the concept of the Binary division.

(i) CRC Generator.

- Append string of n 0's to the data unit.
- Divide newly generated data unit by the divisor.
- Reminder after division is n bit CRC.
- The CRC will replace n 0's to get code words to transmitted.

:- Sender's Side :-



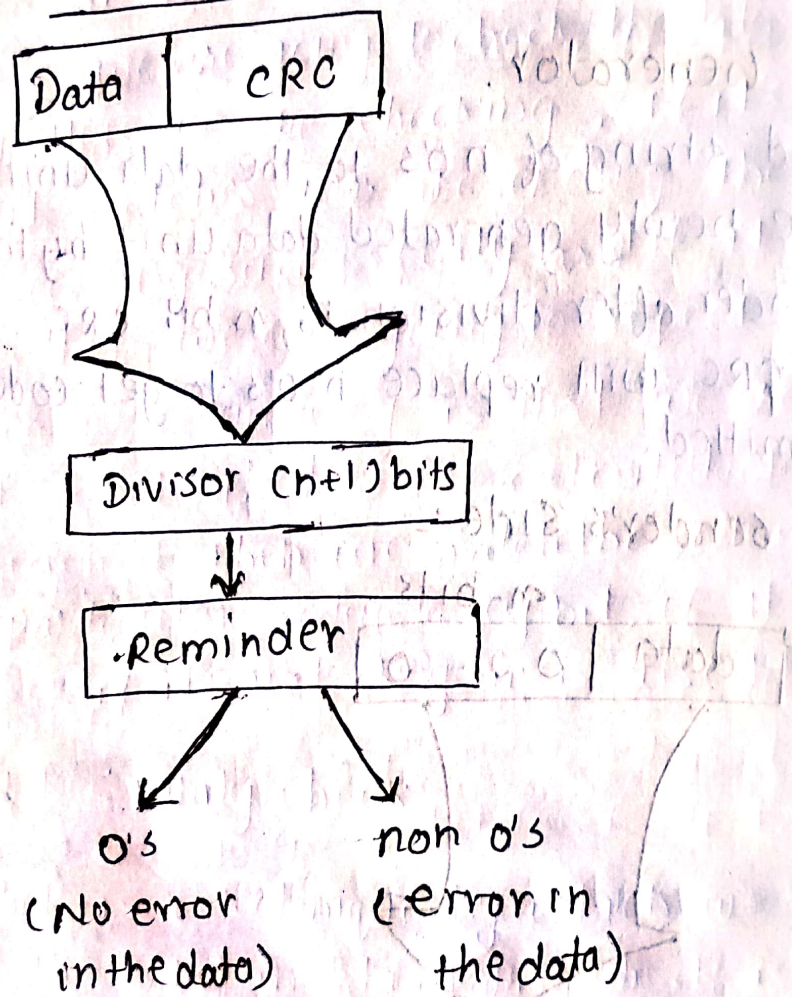
(Code word).

① Data checker will get the Data + CR

ii) CRC checker

Here the receiver divides the data unit by the same divisor which was used by the transmitter, The reminder of the division is then checked.

—: Receiver's side :—



—: Errors :—

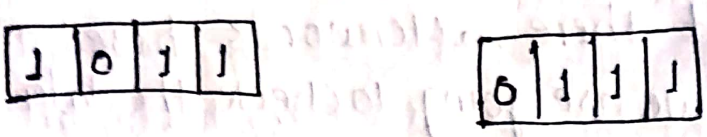
We know that whenever we are sending some data from source to destination then there sometimes the data packets / frames encounter with error, now the error should be detected and corrected.

We know that during transmission data can be corrected, & that time it should be corrected.

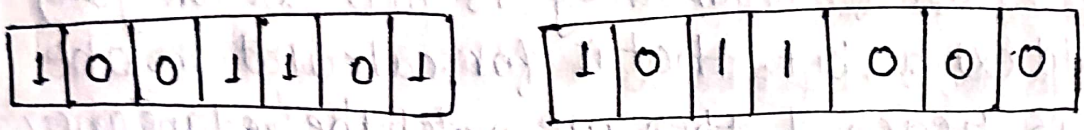
for a reliable communication error must be detected and corrected. There are basically two types of error.

(i) Single bit error - In the single bit error one bit only of data unit has been changed.

Ex:-



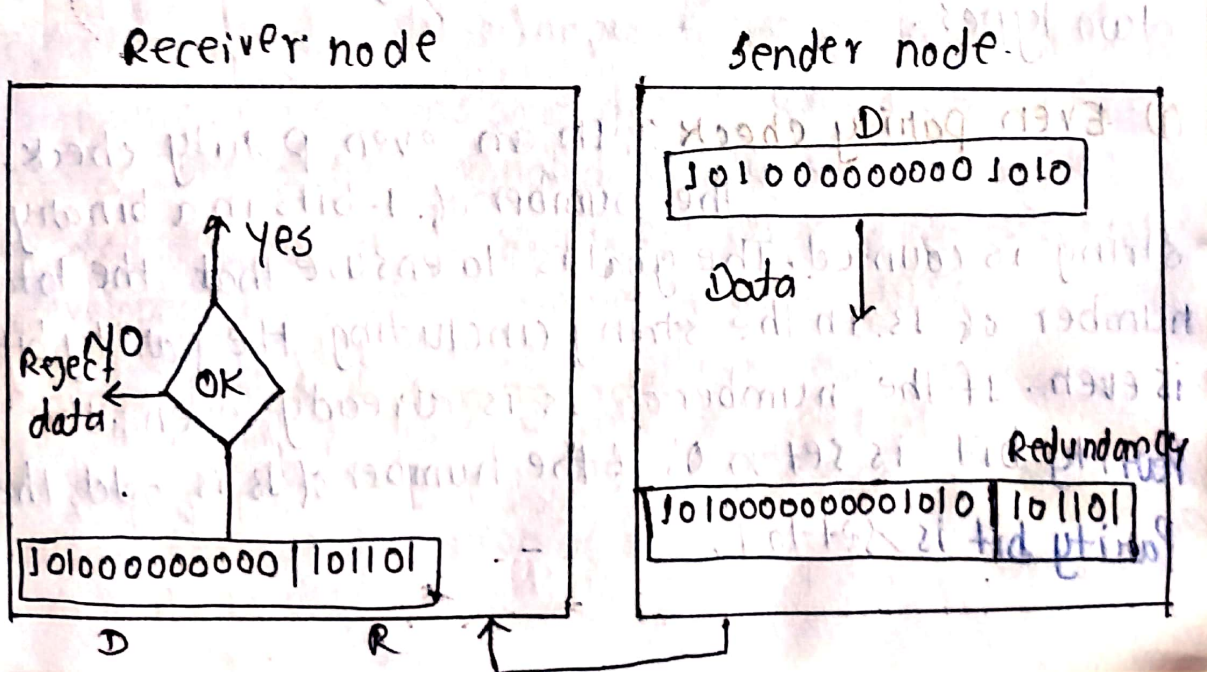
(ii) Burst error / multiple bit error :- whenever two or more bits of data are changed, length of burst error is from start to end, from starting where we have started error and till the where the last got changed.



* length of the burst error - 5 bit.

:- Redundancy :-

Redundancy is a error detection, technique which is used to find the error, in this, extra bit is added to detect the error.



we have a sender node : at sender's side we have some data in this, in this data we add some redundancy (bits), redundancy may be some code, some (1010) sequence, for checking purpose, these two data. Data and redundancy are sent via medium at receiver side and they are received at there, afterwords based on this redundancy, we are going to check the data, this is like a key, Here we are checking, if it's match or not. If it matches we are sending the data for the processing successfully and if it is not matching, then we are going to reject the data, idea of redundancy is that we are going to add extra bit that is for calculation, one data is reached, then we match the redundancy for that particular redundancy bit, if it's okey it's received if it's not okey it is discarded.

:- Parity Check :-

Parity chek is a technique by which we can find out the error in data. Parity check is of two types.

(i) Even parity check :- In an even parity check, the number of 1-bits in a binary string is counted. The goal is to ensure that the total number of 1s in the string (including the parity bit is even. If the number of 1s is already even, the Parity bit is set to 0; if the number of 1s is odd, the Parity bit is set to 1.

Example: For the data 1011001 ; the number of 1s is 4 (even). So, the parity bit would be 0 to maintain the parity.

*Odd parity check : In an odd parity check, the number of 1-bits in a binary string is also counted. The objective here is to ensure that the total number of 1s in the string (including the parity bit) is odd. If the number of 1s is already odd, the parity bit is set to 0, if the number of 1s is even, the parity bit is set to 1.

Example :- for the data 1011001, the number of 1s is 4 (even). To make it odd, the parity bit would be 1.

-: Hamming code :-

Hamming code is an error-correcting code used to ensure data accuracy during transmission or storge. Hamming code detects and corrects the error that can occur when the data is moved or stored from the sender to the receiver. This simple and effective method helps improve the reliability of communication systems and digited storage. It adds extra bits to the original data, allowing the system to detect and correct single bit error. It is a technique developed by Richard Hamming in the 1950s.

- Algorithm of Hamming Code.
- Hamming Code is simply the use of extra parity bits to allow the identification of an error.

Step-1 Write a bit positions starting from 1 in binary from (1, 10, 11, 100 etc).

Step2. All the bit position that are a power of 2 are marked as parity bit (1, 2, 4, 8 etc.)

step3. All the other bit positions are marked as data bit.

step4. Each data bit is included in a unique set of parity bits, are determined its bit position in binary form.

a. Parity bit 1 convers all the bits positions whose binary representation a 1 in the least significant Position (1, 3, 5, 7, 9, 11) etc.

b. Parity bit 2 covers all the bits positions whose binary representation includes a 1 in the second position from the least significant bit (2, 3, 6, 7, 10).

c. Parity bit 4 overs all the bits positions whose binary representation includes a 1 in the ~~fourth~~ third position from the least significant bit (8-15, 4-7, 12-15)

d. Parity bit 8 covers all the bits positions whose binary representation includes a 1 in the fourth Position from the least significant bit bits (8-15, 24-31, 40-47 etc)

e. In general, each parity bit covers all bits where bitwise AND of the parity position and the bit position in non-zero.

Step:5 Since we check for even parity set a parity bit to 1 if the total number of ones in the positions it checks is odd. set a parity bit to 0 if the total number of ones in the positions it check is even