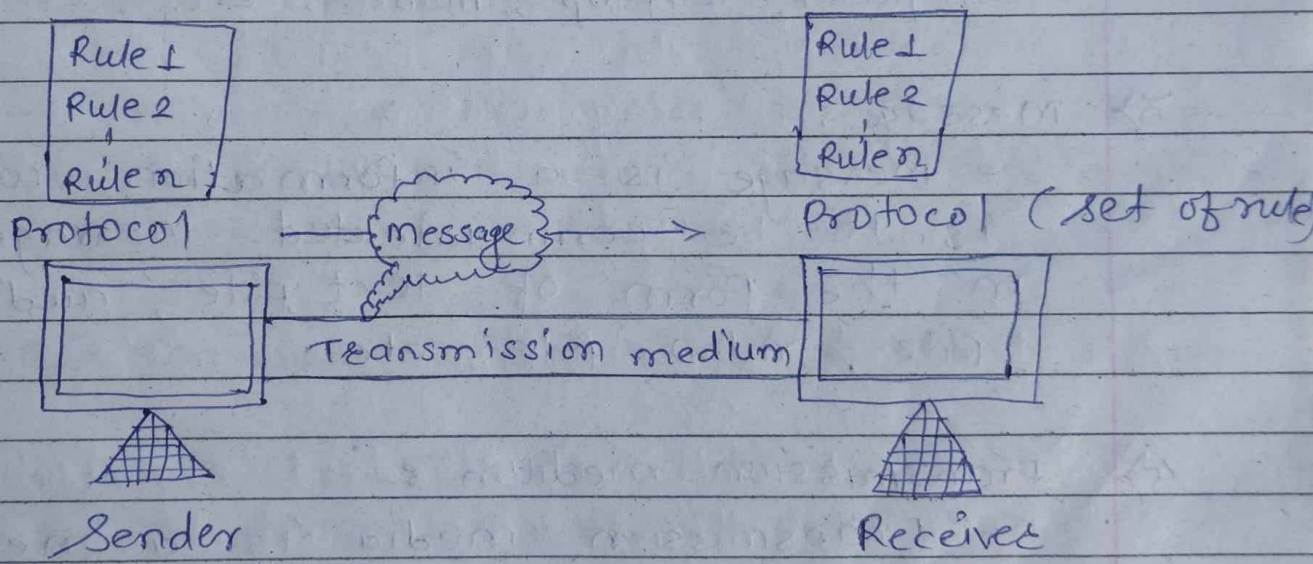
1. Fundamentals of Data Communication and Computer Network

- **Data communication :-** Data communication is the exchange of data between two devices via some transmission media, such as cable, wire or air, vaccum.

- **Components of data communication**

1) Sender
2) Receiver
3) Message
4) Transmission medium
5) Protocol (set of rule)



SMTP :- Simple mail Transfer protocol

1) Message

1) Sender
- It is a device that sends the data message. It should be a computer, Laptop, mobile, etc. Sender plays the role of source in data communication

2)

2) Receiver
- It is destination where message sent by source has arrived. It is a device that receives the message or data that is sended by sender. It should be Computer, Laptop, mobile, etc.

3) Message :-
- Message is a information which is to be communicated. Message is in the form of text file, audio file, video file, etc

4) Transmission medium :-
- Transmission media is a medium of data Transmission. It is a physical path in which data or message travels from sender to receiver. It should be a guided or unguided
(wired) (wireless)
ex :- Twisted pair cable, radio wave, micro wave, etc

5) protocols
protocol is nothing but the set of rules and regulation.

* Example of data communication.

1) Sending the email :- User with sending a e-mail acts as a sender. Message is a data which is to be send and receiver is one that accepts the message. In these entire process there are many protocols which plays important role.

• Network Standard

- It defines the rules for data communication that are needed for interoperatability of networking technology and process

- The commonly used standards at ~~eak~~ each layer.

1) Application layer
- HTTP (Hypertext transfer protocol)
- HTML (Hypertext markup language)

2) Transport layer
- TCP (Transmission Control protocol)

3) Network layer :-
- Ip (Internet protocol)

* Types of standards.

1) D-facto :- These are the standards that are followed without any formal plan or approval by any organization.
ex :- HTTP

2) De-jure :- These standards are one which have been adapted through legislation by any oficially recognize standard organization
ex :- Communication standard available nowdays.

* standard organization

1) ISO (International standards organizations
2) ITU (International Telecommunication Union)
3) IEEE (Institute of electronics and electrical engineers)
4) ANSI (American National Standard Institute)
5) IETF (Internet Research Task Force
6) EIA (Electronic Industries Association)

- Bandwidth :- -It is a data carrying capicity of network. It generally measured in bits per second (~~bits/s~~) (bps)
  - For example if bandwidth is 100 mbps it means maximum 100 mb data can be transffered per second on that channel.

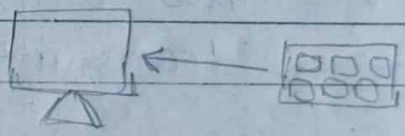
- Data Rate :-
  - Data rate is a amount of the data that is to be transmitted during a specifying time period over a network.
  - For example, if bandwidth is 100 mbps but data rate is 50 mbps, it means maximum 100 mb data can be transferred but channel is transmitting only 50 Mb data per second.

Bit rate	Baud rate
- It is defined as the transmission of number of bits per second	- It is defined as the number of signal units per second
- It defines as per second travel number of bits	- It defines as per second number of changes in sign
- Bit rate emphasized on computer efficiency	- While baud rate emphasized on data transmission.
- formula :- baud rate x n. of bps	- formula :- bit rate / n. of ~~bits~~ bits pe band

- (Modes of data communication)

- Transmission mode (communication mode) :-
  - The way in which data is transmitted from one device to another device is known as transmission mode
  - Transmission mode is also known as communication mode
  - It works on the physical layer.
  - There are three types of T.M.
    1) Simplex Mode
    2) Half-duplex Mode
    3) full-duplex Mode

1) Simplex mode



- In simplex mode communication is unidirectional
- A device can send data but cannot receive it or it can receive the data but cannot send the data.
- The radio station is a simplex channel as it transmits the signal to the listeners but never allows them to transmit back.
- example :- radio, monitor, keyboard, etc.

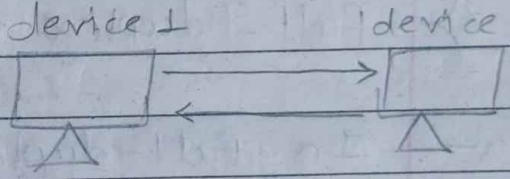
• Advantages •

1) Cost effective
2) Reduced complexity
3) Low latency
4) predictable performance

• Disadvantages •

1) It is ~~uno~~ unidirectional
2) No error correction
3) Limited flexibility
4) Limited use
5) Not suitable for real time

2) Half duplex mode



- In half duplex message flows in both direction the direction but not at the same time
- In half duplex direction can be reversed
- while device 1 sending data then device 2 can ~~not~~ only receive data it cannot be send.
- and another case device 2 is sending data then device 1 can only reciere the data it cannot be send
- In half duplex every device se can send or receive data but not simultaneously
- ex :- walky - Talkie

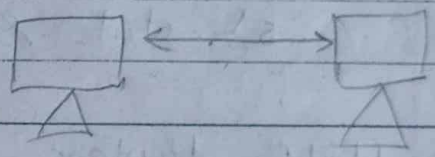
• Advantages •

1) Two-way communication
2) cost effective
3) Efficient bandwidth
4) Reduced collision Risk

• Disadvantages •

1) slower communication
2) Limited use
3) missed message
4) Complex control logic

3) Full-duplex mode



- In full-duplex mode, the communication is bi-directional.
- The data flow in both the directions.
- Both devices can send or receive data simultaneously.
- It is a fastest ~~device~~ mode ~~in~~ of Communication between devices
- example :- Telephone, mobile phone

• Advantages •

1) Simultaneous Communication
2) Faster Data Transfer
3) Real- Time Interaction
4) Improved performance
5) Enhanced User experienced

• Disadvantages •

1) Complexity
2) Higher Cost
3) Network managment
4) Increased resource Usage

Basis	Simplex	Half - Duplex	Full- Duplex
Direction of communi	Unidirectional	Bidirectional but not simultaneously	Completely birectional
Send or receive	Either only send data or receive data	Send or receive data but one at a time	Send and receive data simultaneously
performance	Better in half duplex	Better in Full- duplex	Already better than Simplex & Half duplex
Example	Radio, monitor, keyboard	walkie, Talkie	Telephone net network

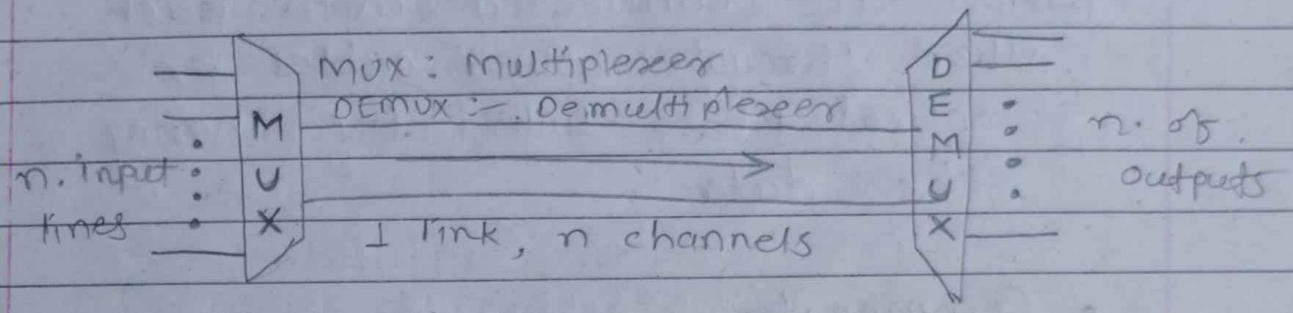
☆ Multiplexing

- It is a technique used to combine and send the multiple data stream over a single medium.
- The process of combining the data stream is known as multiplexing.
- Multiplexing follows many to one approach
- The device used for multiplexing is called MUX → multiplexer that combines n input lines to generate single output line.

☆ Demultiplexing

- Demultiplexing is achieved by using device DEMUX. (de-multiplexer)
- DEMUX seperates the signal into its component signals (one input and n outputs).
- Demultiplexing follows one to many approach.

✱ Concept of multiplexing



- The 'n' input lines are transmitted through a multiplexer and multiplexer combines the signals to form a composite signal
- The composite signal is passed through a Demultiplexer and demultiplexer saperates a signal to component signals and transfers them to their respective destinations

- Computer Network
  - It is a group of computers which are connected with each other through wires cables or optical fibers links for sharing the data.

- Components

  1) Hub
  2) modem
  3) router
  4) switch
  5) NIC
  6) cable

- Uses of Computer Networks

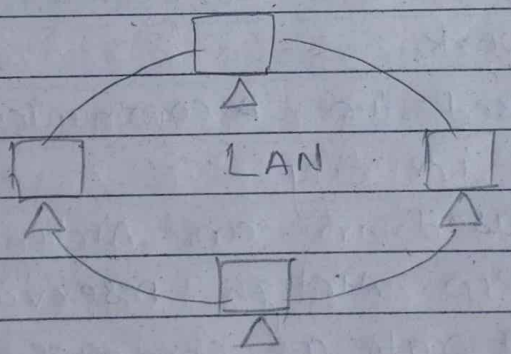
  1) Resources sharing
  2) client - server model
  3) Communication media
  4) e-commerce

- features of Computer Network

1) Communication Speed
2) File sharing
3) Back up and roll back
4) Security
5) Scalability
6) Reliability
7) Software sharing.

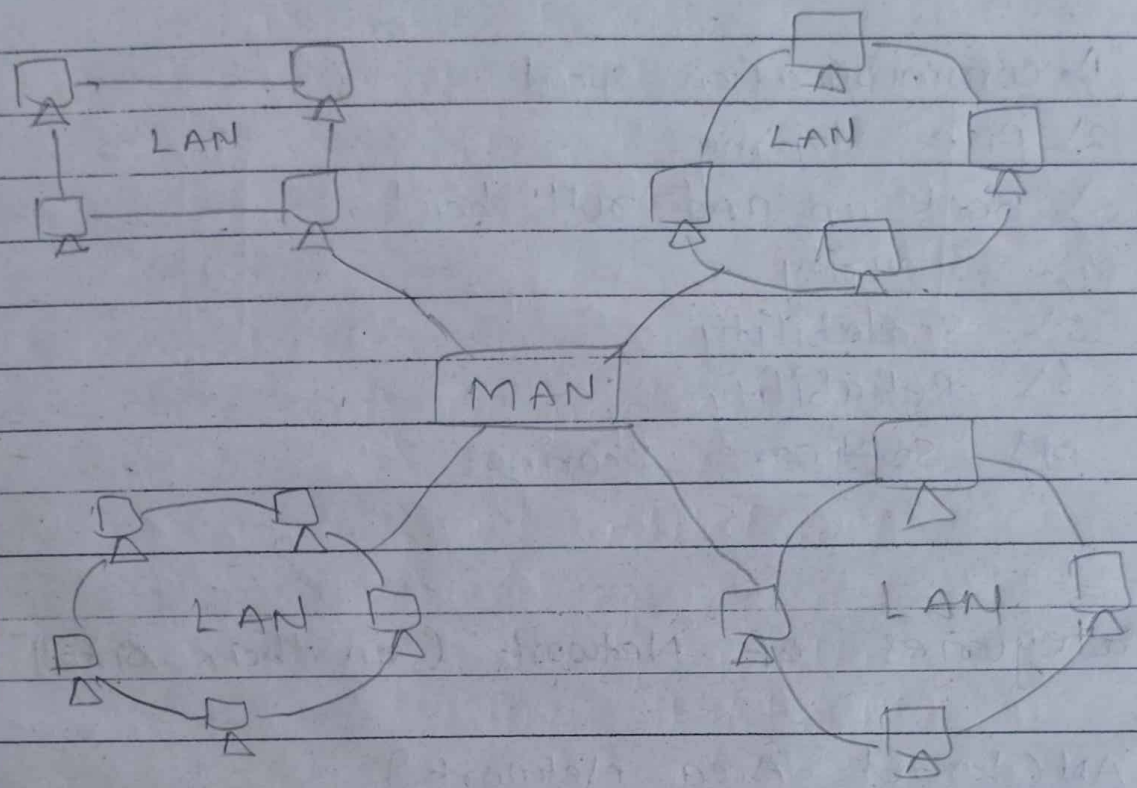
* Categories of Network (on their size)

1) LAN (Local Area Network)



- LAN is a group of computers connected to each other in small area such as building
- It is limited in small area
- It is used for connecting two or more personal computers through communication medium such as twisted pair, coaxial cable
- It is expensive - faster data rate

o) MAN (Metropolitan Area Network)



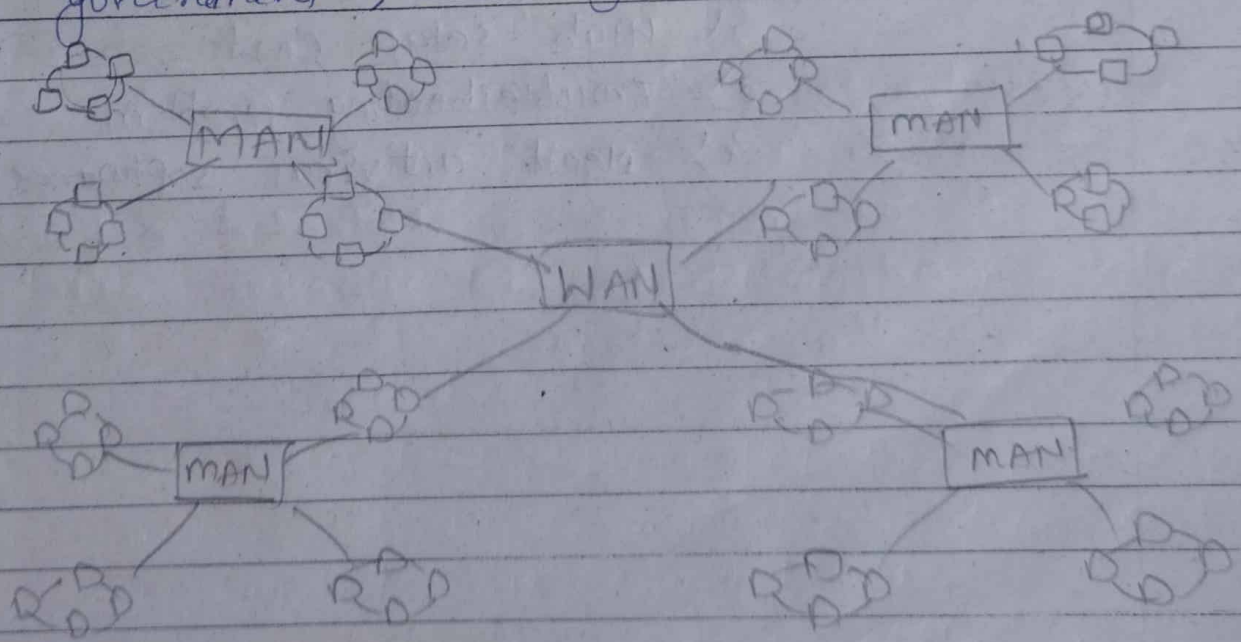
- multiple LAN's are connected to form MAN Network
- MAN is used in communication between the banks in city
- It can be used in an Airline Reservation
- It is used in Airlign reservation System
- Faster data rate as compare to LAN
- It has higher range than LAN.
- Goverenment agencies use MAN to connect to the citizens and private industries
- MAN covers large geographical area

• uses •

- MAN is used in communication between the banks in a city
- It can be used in an Airline Reservation
- It can be used in a collage within a city
- It can also be used for communication in the military

3) WAN (Wide Area Network)

- It coress large geographical Area such as contri
- A wide Area network is bigger network than the LAN
- WAN network is not limited to single location
- the internet is a example of WAN
- A WAN is widely used in field of buisness, goreenment, and edjucation



- Examples :-
  1) mobile broadband
  2) Last mile
  3) private network

- Advantages :-
  1) Geographical Area
  2) centralized Data
  3) Get updated files
  4) exchange messages
  5) sharing of softwares & resources
  6) High bandwidth

- Disadvantages :-
  1) Security issue
  2) High setup cost
  3) Troubleshooting problem
  4) Need antivirus softwares

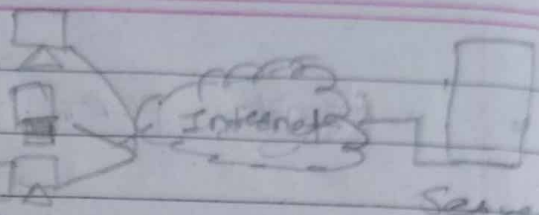
- peer to peer network

- It is a network in which all computers are connected to each other with equal privilliages and responcibilities
- peer-to peer network is useful for small enviornment
- In peer to peer special permissions are assign to each computer for sharing resources.

- Advantages
  1) It is less costly.
  2) If one computer stop working then other computer will not stop working.
  3) It is easy to setup

- Disadvantages
  1) In the case of peer to peer network it does not contain the centralized system
  2) It has security issue

- client - seerer Network



- client / seerer network is network
- The central controller is known as the seerer, while all other computers in the network is called client
- seerer manages ~~the~~ all the resources
- client - seerer model follows the request response type of operation

- Advantages
  1) It contains centralized system
  2) client - seerer has dedicated seerer that improves overall performance of whole system
  3) It also increase the speed of sharing resources

- Disadvantages
  1) It is expensive
  2) It requires a dedicated network administrator to manage all the resources

- Features of Computer Network

1) Communication Speed
2) File sharing
3) backup
4) Hardware & software sharing
5) Security
6) Scalability → Increase the size of network
7) reliability

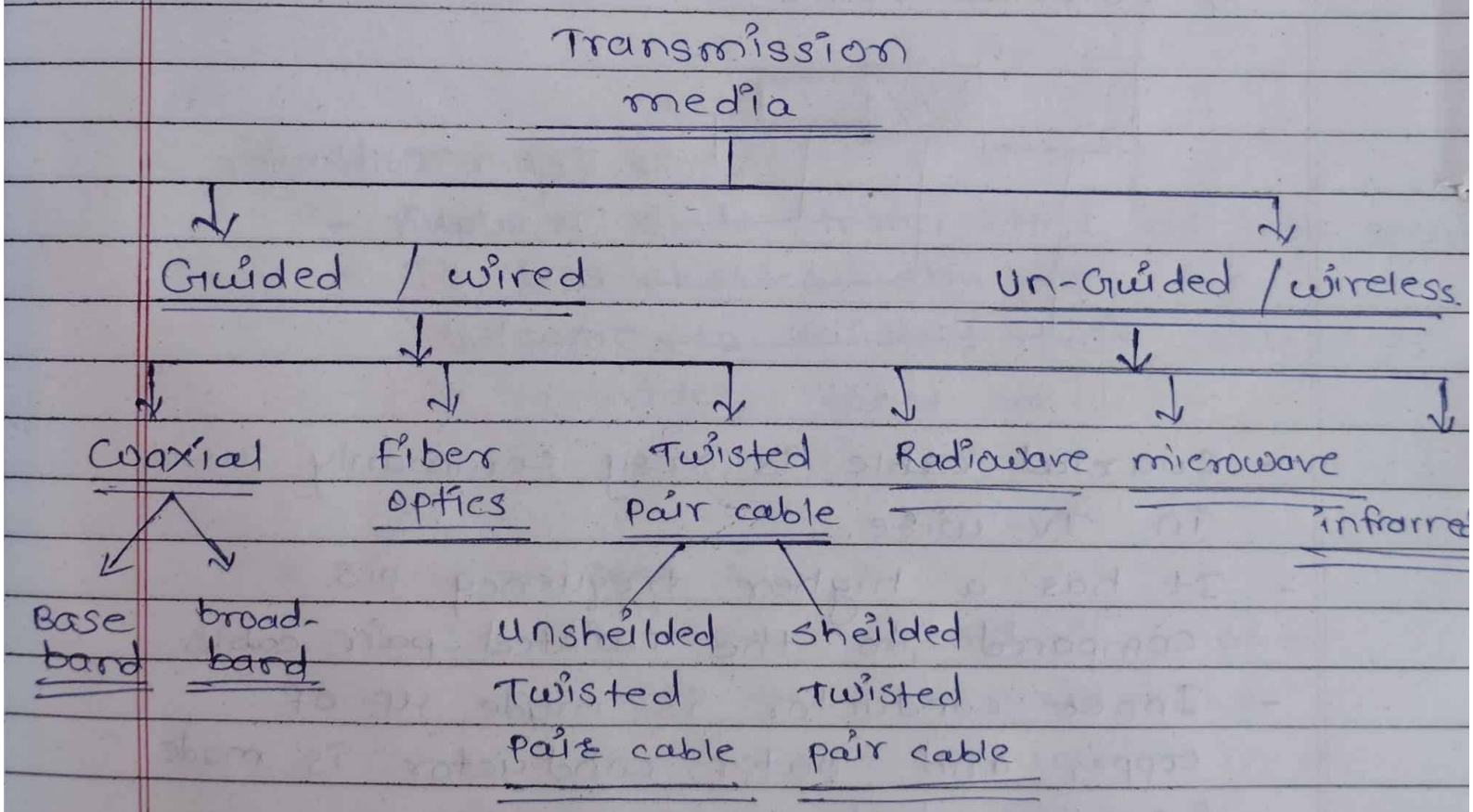
peer to peer	client server
- less costly	- more costly / High C.
- Limited security features	- Enhanced security features
- Easy setup and manage.	- more complex setup and managment
- Direct communication between peers	- clients communicate with a central server
- De-centralized	- centralized
- All devices have equal roles	- Distinct roles for clients and servers
- Suitable for small networks	- scalable for large networks

2. Transmission media & switching

PAGE NO.:
DATE: / /

- **Transmission media :-**
  Transmission media is a channel that carries the information from sender to receiver.
  Data is transmitted through the electromagnetic signal.

- classification of transmission media.



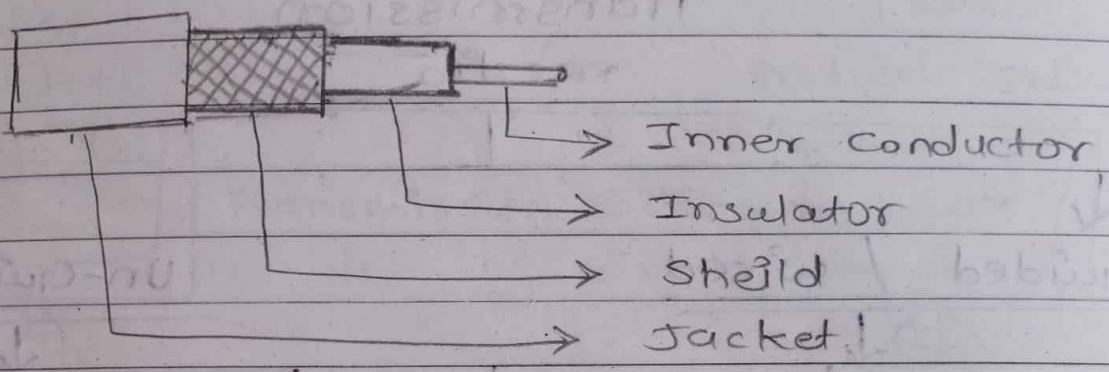
* classification of transmission media *

PAGE NO.:
DATE: / /

- Guided media :- It is defined as the physical medium through which the signals are transmitted. It is also known as bounded media.

- Types of guided media :-

1) Coaxial cable



- Coaxial cable is very commonly used in TV wire.
- It has a higher frequency as compared to the Twisted pair cable.
- Inner conductor is made up of copper and outer conductor is made up of copper mesh.
  Middle ~~cord~~ core is made up of non-conductive cover that saperates the inner conductor from the outer conductor.
- Middle core actual carries the data. there are the copper mesh prevents from EMI

PAGE NO.:
DATE: / /

- Types of coaxial cable :-

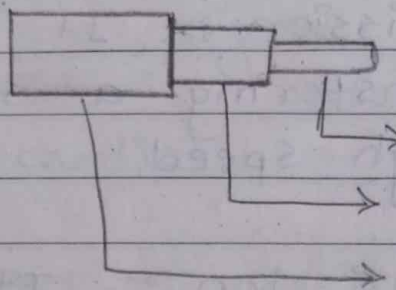
1) Baseband transmission :- It is a process of transfering a single signal at high speed.

2) Broadband transmission :- It is a process of transfeeing multiple signals simultaneously.

* Advantages *
- Data can be transmitted at high speed
- It has better shielding as compare to twisted pair cable
- It provides higher bandwidth.

* Disadvantages *
- It is more expensive compared to the twisted pair cable
- If any fault occurs ~~th~~ in the cable causes the failure in the entire network

2) fiber optics.



- It is a cable that uses data in the form of ~~pulse~~ light pulse
- It uses electrical signals for communicat^n
- plastic coating protects the cable from the heat, cold, EMI.
- It provides fastes data transmission than copper wires.
- Elements / components of fiber optic cable :-

1) core :- A core is a light transmission area of the fiber.

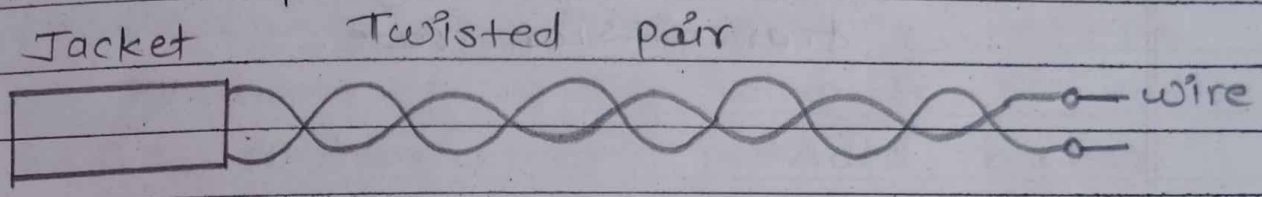
2) cladding :- It is a layer of glass called as cladding. It provides the refractive index.

3) Jacket :- It is the protective covering of plastic over the fiber optic cable called as Jacket. It absorb the shock and provide extra protection.

PAGE NO.:
DATE: / /

* Advantages *
- Greater Bandwidth
- faster speed
- Longer distance
- Thinner
- Better reliability.

3) Twisted pair.



- It consist of pair of cable twisted with each other.
- Installation of twisted pair cable is easy.
- The frequency range of twisted pair cable is 0 to 3.5 kHz.
- There are two types of twisted pair cable :- 1) unshelded Twisted pair (UTP)
  2) shelded Twisted pair (STP)

1) UTP :- UTP cables is used in telecommunication.
- following are the categories of UTP.
  1) category 1 :- used in telephone service that carries low speed data
  2) category 2 :- It supports upto 4 mbps.
  3) category 3 :- It supports upto 16 mbps.

4) category 4 :- It supports upto 20 mbps.

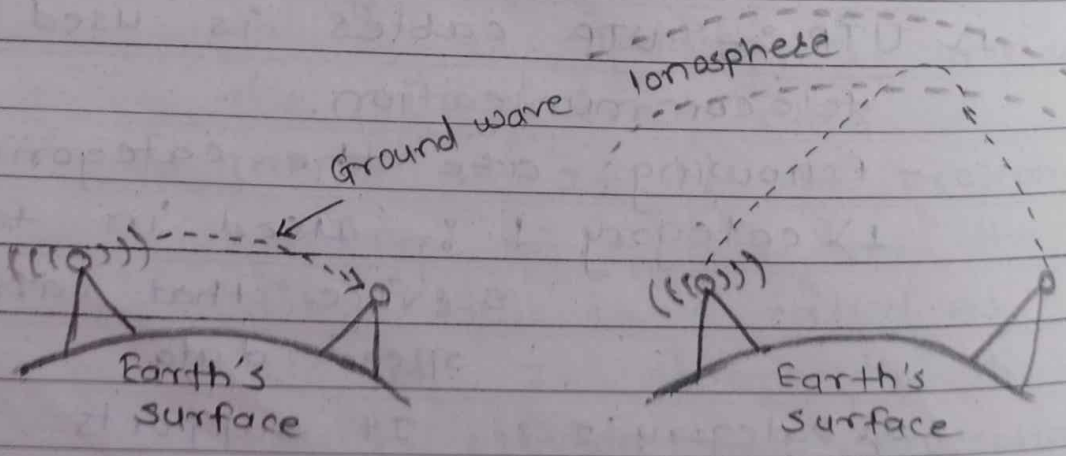
5) category 5 :- It supports upto 200 mbps.

2) STP :- STP cable contains the mesh surrounding the wire that allow high data transmission rate.

- Un-guided Transmission :- An un-guided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as wireless Transmission.

- Types of un-guided media :-

1) Radio waves :-



(a) (b)

- Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- Radio waves are omnidirectional
- The range of radio waves
- In the case of radio waves, the sending and receiving antenna are not alligned. i.e., the wave sent by the sending antenna can be received by any receiving antenna.
- An example of radio wave is FM radio.
- Radio transmission provides higher transmission rate.
- It covers large area, and they can penetrate the walls.

2) Micro waves :-
- Types of micro-wave Transmission :-
  i) Terrestrial microwave transmission
  ii) satellite microwave transmission.

i) Terrestrial microwave transmission.
- Terrestrial microwave transmission is a technology that transmits the radio signals from one ground-based microware transmission antenna to another
- Terrestrial microwaves are unidirectional as the sending and receiving antenna is to be aligned.
- It works on line of sight transmission
- Bandwidth supports 1 to 10 mbps
- Frequency :- 1 ghzs to 1000 ghzs
- It is preferred to short distance

2) Satellite / Microwave transmission :-

- A satellite is a physical object that revolves around the earth at a known height
- The satellite accepts the signals that is transmitted from earth's station and it amplyfies the signal. The amplified signals is retransmitted to another earth station
- It covers large area
- Independant of the distance
- It requires to the monitored
- life of satellite is 12 to 15 years so launch of another satellite is to be planned
- we can communicate globaly.

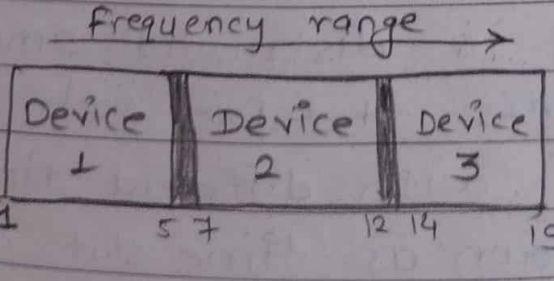
3) Infrared Transmission :-

- An infrared transmission is wireless technology used for communication over short range
- It cannot penetrate the walls.
- It supports high bandwidth, hence the data rate will be very high.
- It is used for short-range communication such as data transfer between two cell phones.

- An infrared communication provides better security with minimum interference.
- Infrared communication is unreliable outside the building because the sunrays will interfere with the infrared waves.

• Frequency Division Multiplexing (FDM)

- In frequency division multiplexing technique, all signals operates at the same time with different frequency.
- It is an analog technique
- In FDM the number of signals are transmitted at the same time and each source transfers its signals in the alloted frequency range.
- The available bandwidth of a transmission media is divided into several channels.
- The input signals are translated into frequency band by using modulation technique and they are combined by multiplexer to form composite signal.
- This technique is used in TV network and radio.



* Advantages *
- FDM is used for Analog signals
- FDM process is very simple and easy modulation
- A large number of signals can be sent through FDM simultaneously
- It does not require any synchronization between sender & receiver.

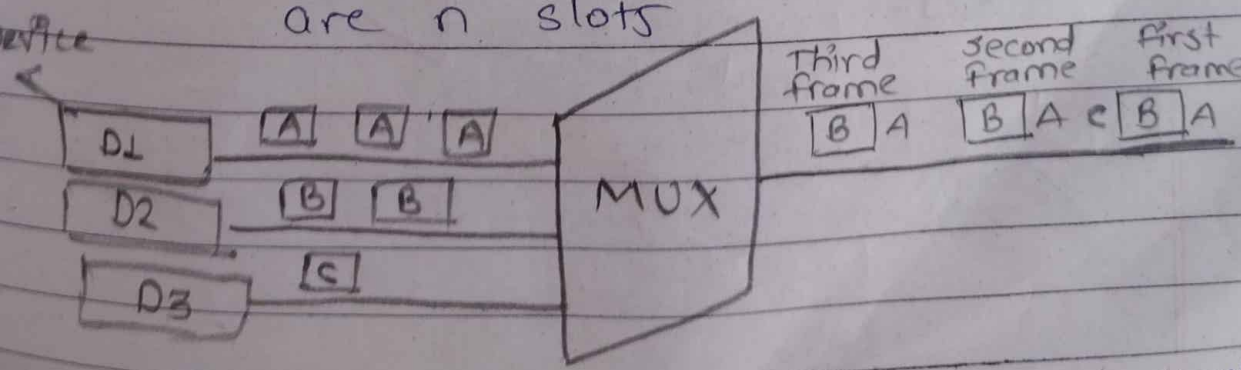
* Disadvantages *
- FDM technique is used only when low-speed channel is required
- A large number of modulators are required
- It requires a high bandwidth channel.

• Time Division multiplexing (TDM)

- It is a digital technique
- In FDM signals are operates at same time but different frequency but in TDM signals are operate at the same frequency with different time
- In TDM 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 sender.
- There are two types of TDM :-
  i) Synchronous TDM
  ii) Asynchronous TDM
- In TDM Data is transmitted one by one
- In TDM, the signal is transmitted in the form of frames.

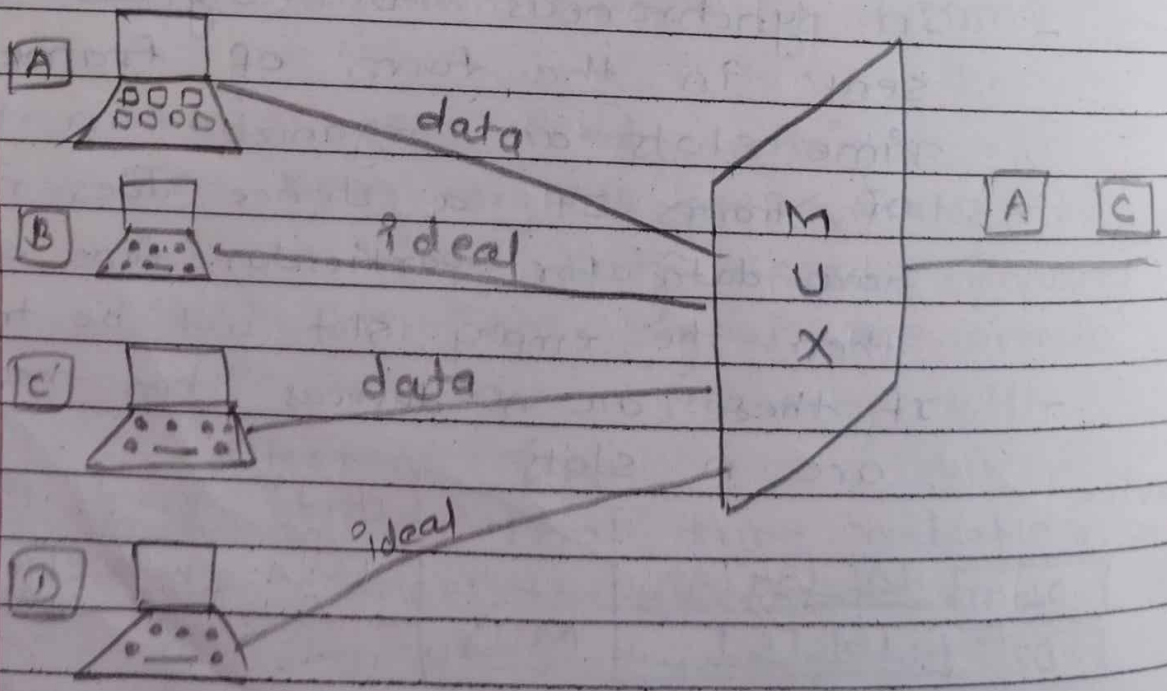
i) Synchronous TDM.
- A synchronous TDM is a technique in which time slot is preassigned to every device.
- In synchronous TDM, each device is given some time slot, it tells the device contains data or not
- If the device does not have any data then the slot will remain empty.
- In synchronous TDM signals are sent in the form of frames. Time slots are organized in the form of frames. If a device does not have data for particular time slot then the empty slot will be transmitted
- If these are n devices then there are n slots



- In synchronous TDM many slots are unutilized

99) Asynchronous TDM.

- An asynchronous TDM is a technique in which time slots are not fixed
- 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
- It accepts the incoming data streams and creates a frame that contains only data with no empty slots
- In Asynchronous TDM slots are fully utilized.



• switching. *

Transformation of data in a one device to another device in a network is known as switching.

* Circuit switching :-

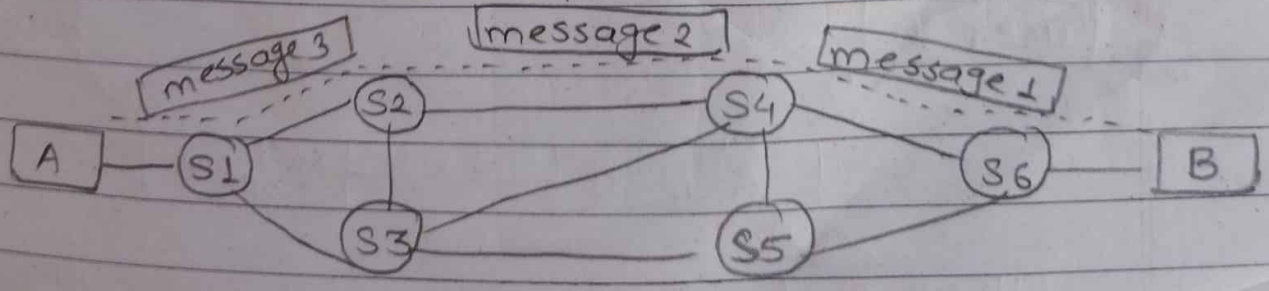
- Circuit switching is a connection oriented service
- It provides dedicated path from sender to receiver
- It has very less chances of data loss due to dedicated circuit.
- but bandwidth is wasted because another sender cannot use the same path for transmission of data
- circuit switching is completely transparent.

• phases of circuit switching :-

1) circuit establishment :- A dedicated circuit between the source and destination is constructed.

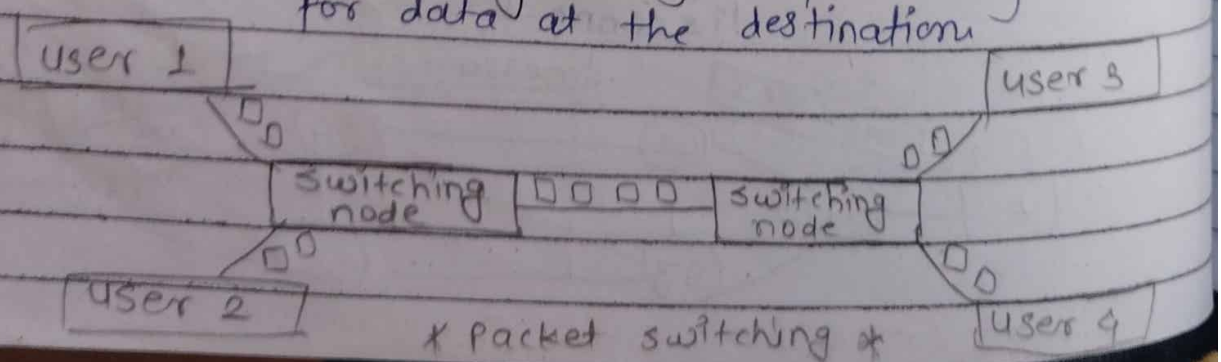
2) Data transfer :- Data can be transferred between the source and destination once the circuit has been established

3) circuit disconnection :- Disconnection in the circuit occurs when one of the users initiates the disconnect.



* packet switching

- packet switching is a connection less service.
- It does not required dedicated path between the sender and receiver.
- It has more chances of data loss and error.; The packets may arrive in the wrong order.
- packet switching is a method of transferring data to a network in the form of packets.
- packet switching uses store and forward technique
- Types of delay in packet switching :-
  - Transmission delay :- Time required for the source station to transmit the data
  - propagation delay :- Time of data propagation through the link
  - queing delay :- Time spent by the packet at the destination's queue
  - processing delay :- processing time for data at the destination



* Packet switching *

PAGE NO.:
DATE: / /

- Difference between circuit switching and packet switching.

circuit switching	packet switching
i) It requires dedicated path from sender to receiver	i) It does not require dedicated path from sender to receiver.
ii) less chances of dataloss	ii) more chances of data loss
iii) Each packet follows the same route	iii) A packet can follow any route
iv) call setup is required	iv) No call setup is required
v) Bandwidth wastage	v) No bandwidth wastage
vi) No store and forward transmission	vi) It supports store and forward transmissio

3. Error detection, Correction and Wireless Comm

- Error detection :- When data is transmitted from one device to another device. system doesn't guarantee whether data received by device is identical to data transmitted by another device

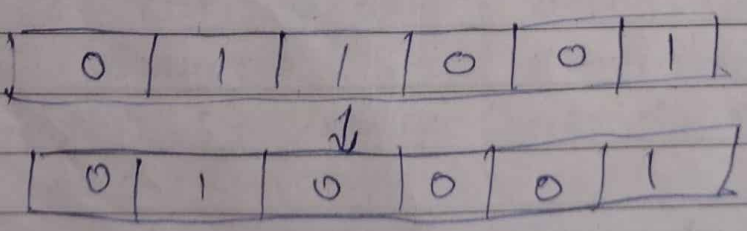
- Error :- It is a situation when the message received at the receiver end is as not same the message transmitted.

- Types of error :- 1) Single ~~bit~~ bit error
  2) Burst error.

- Single parity check

① While transmitting the data some redundant data is to be sent.

② for even parity :
- if there is even no of ones in data then add '0' redundant in it
- if there is odd no of one's in data then add '1' redundant in it

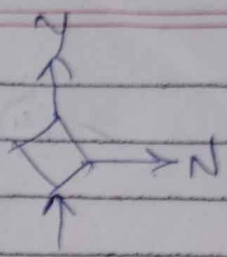


conversion of polynomial to Binary.

If $x^4 + x^3 + 1$ or $x^4 + x^3 + 0x^2 + 0x + 1$

1 1 0 0 1 1 1 0 0 0

PAGE NO:
DATE: / /



Sender

1011011

↓

Compute even parity bit

↓

1011011 [1]

→ Transmission media → Compute parity bit

↑

1011011 [1]

~~Single parity check~~ / VRC

- CRC (cyclic Redundancy check) Remainder

① In CRC technique a string of n zeroes is appended in a data unit This 'n' is less than the no of bits in a predetermined number (by 1 only)

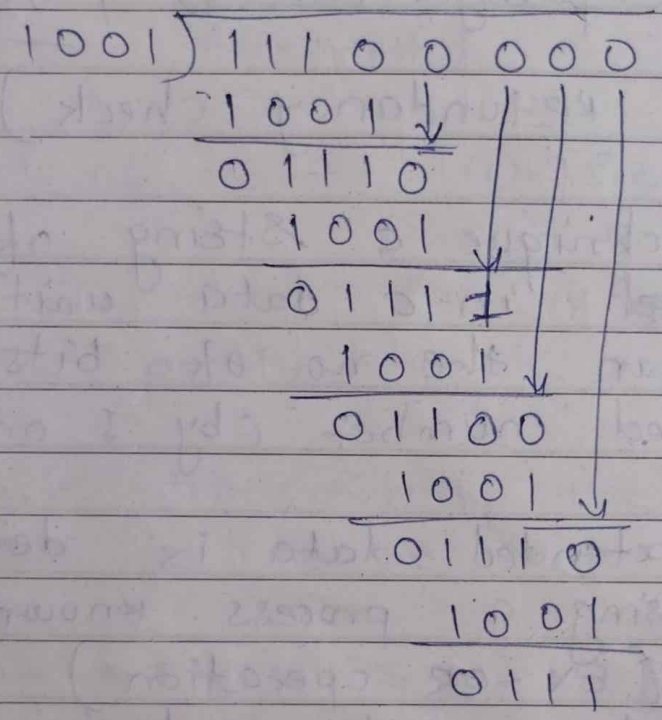
② Newely extended data is devided by devisor using a process known as binary devision. (EX-OR operation) Remainder generated from this devision is known as CRC Remainder.

③ The CRC Remainder replaces the appended zeroes at the end of original data. This newely generated data is send to the receiver. At the receiver side again the same procedure is follows and find at the out the CRC remainder

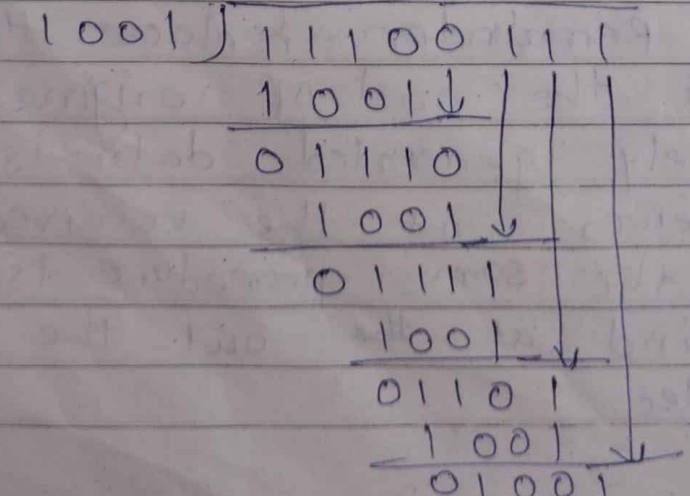
PAGE NO.:
DATE: / /

④ If remainder of this derision is zero means no error (data is accepted) otherwise there is an error (data is discussed)

- original data :- 11100
  Divisor :- 1001



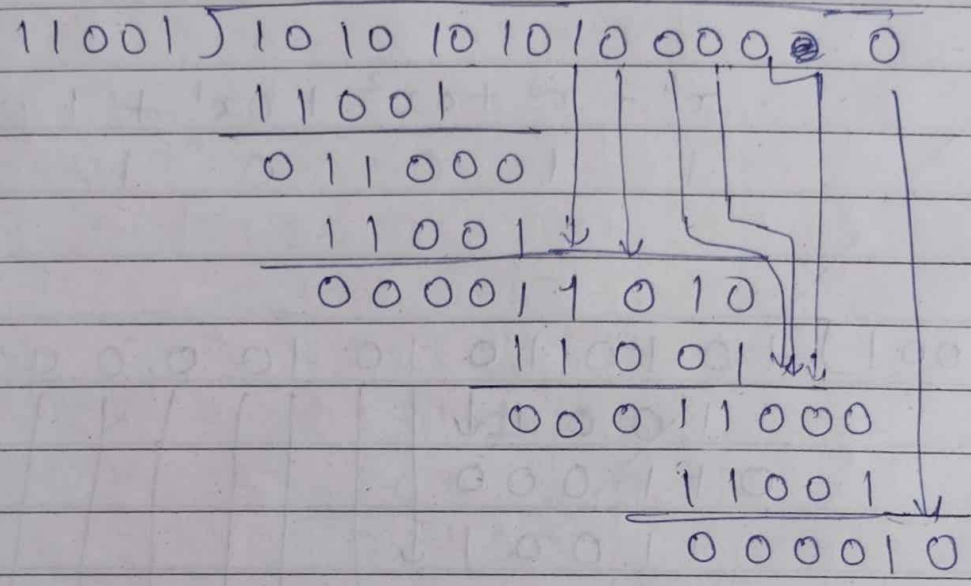
- Receiver side



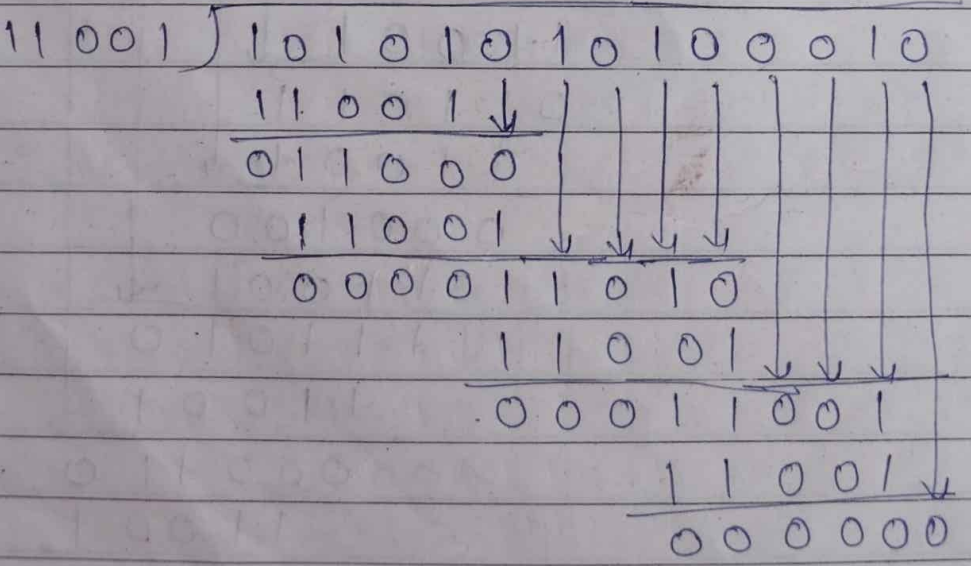
PAGE NO. :
DATE : / /

Q Data word :- 1010101010
Divisor :- $x^4 + x^3 + 1$, i.e.

$x^4 + x^3 + 0x^2 + 0x^1 + 1$
1 1 0 0 1



- Receiver side.



PAGE NO.:
DATE: / /

Q Word length :- 1 1 0 1 0 1 1 0 1 1
Divisor :- $x^4 + x + 1$
1 0 0 1 1

```
10011 ) 1 1 0 1 0 1 1 0 1 1 0 0 0 0
        1 0 0 1 1 ↓
        0 1 0 0 1 1
          1 0 0 1 1 ↓ ↓ ↓ ↓ ↓
          0 0 0 0 0 1 0 1 1 0
                1 0 0 1 1 ↓ ↓
                0 0 1 0 1 0 0
                  1 0 0 1 1 ↓
                  0 0 1 1 1 0
```

• Receiver Side

```
10011 ) 1 1 0 1 0 1 1 0 1 1 1 1 1 0
        1 0 0 1 1 ↓
        0 1 0 0 1 1
          1 0 0 1 1 ↓ ↓ ↓ ↓ ↓
          0 0 0 0 0 1 0 1 1 1
                1 0 0 1 1 ↓ ↓
                0 0 1 0 0 1 1
                  1 0 0 1 1 ↓
                  0 0 0 0 0 0
```

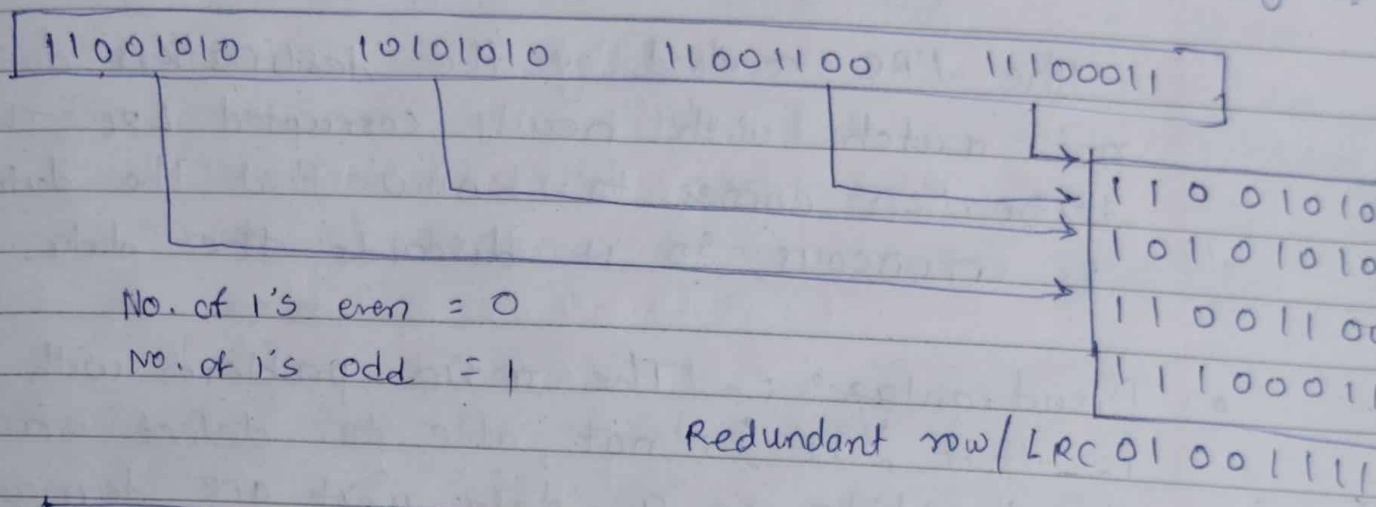
Longitudinal Redundancy check (LRC) or 2-D parity check

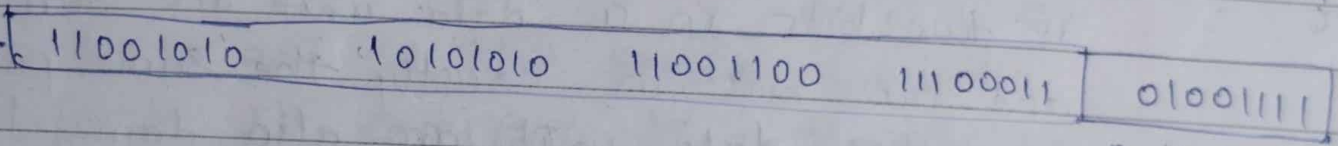
In this method, data which the user want to send is organized into tables in the form of rows and columns. A block of bit is divided into table or matrix of rows and columns. In order to detect an error a redundant bit is added to the whole block and this block is transmitted to receiver. The receiver uses this redundant row to detect error. After checking the data for errors, receivers accepts the data and discards the redundant row of bits.

PAGE NO.:
DATE: / /

Example :-

If a block of 32 bits is to be transmitted it is divided into matrix of four rows and eight columns which as shown in the figure.

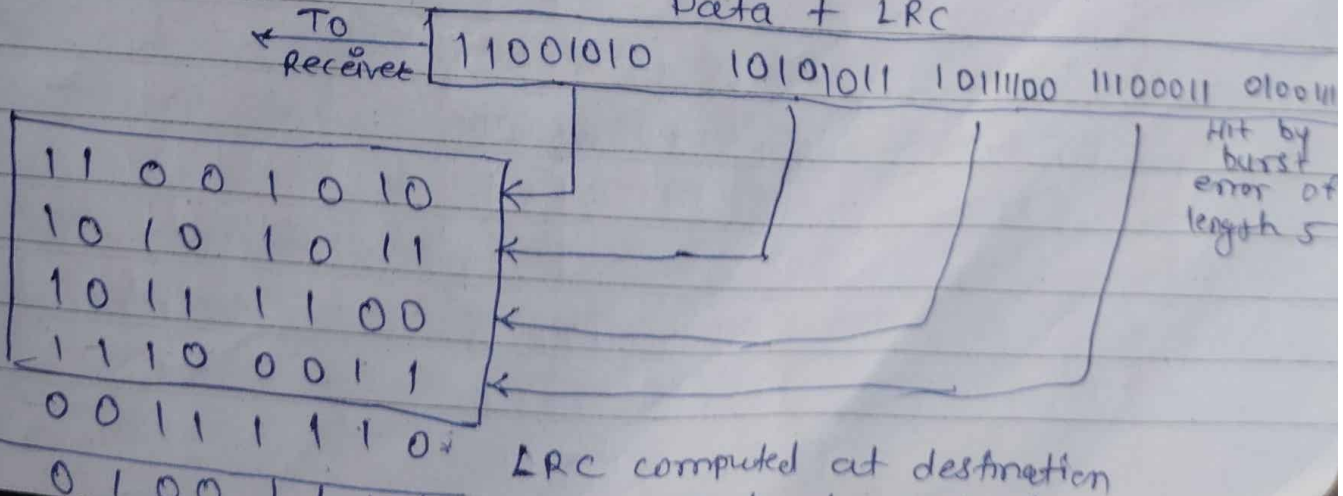




In this matrix of bits, a parity bit is calculated for each column. It means 32 bits data plus 8 redundant bits are transmitted to receiver. Whenever data reaches at the destination receiver uses LRC to detect error in data.

- Advantages :-

LRC is used to detect burst errors.



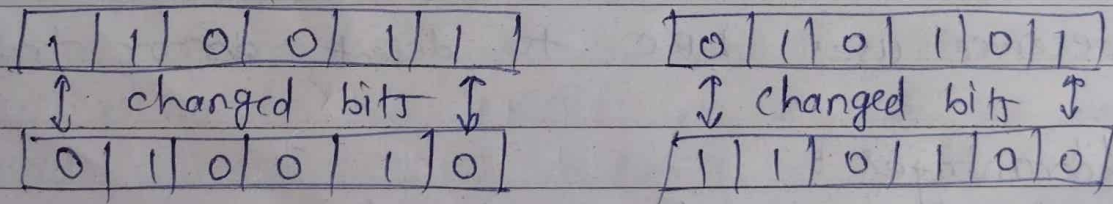
PAGE NO.:
DATE: / /

Example:- Suppose 32 bit data plus LRC that was being transmitted is hit by a burst error of length 5 and some bits are corrupted as shown in the following figure: ⤵

The LRC received by the destination does not match with newly corrupted LRC. The destination comes to know that the data is erroneous, so it discards the data.

- Disadvantages :- The main problem with LRC is that, it is not able to detect error if two bits in a data unit are damaged and two bits in exactly the same position in other data unit are also damaged.

Example:- If data 11001| 01010| is changed to 01001|0110100



PAGE NO.:
DATE: / /

Checksum

This is a block code method where a checksum is created based on the data values in the data blocks to be transmitted using some algorithm and appended to the data. When the receivers receive the data a new checksum is calculated and compared with the existing checksum. A non-match indicates an error

- Error detection by checksum

- Sender's end :- The sender adds the segment using 1's complement arithmetic to get the sum. It then complements the sum to get the checksum and sends it along with the data frames

- Receivers end :- The receivers adds incoming segments along with the checksum using 1's Complement arithmetic to get the sum and the complements it

If the result is zero, the received frames are accepted; otherwise they are discarded

{ This method ~~is~~ makes the use of checksum generator on sender side and checksum checker on receiver side }

Ex

Sender side

Frame 1 : 11001100
Frame 2 : +10101010
partial sum : 101110110
+1
01110111
Frame 3 : +11110000
partial sum : 101100111
+1
01101000
Frame 4 : +11000011
partial sum : 100101011
+1
Sum : 00101100
checksum : 11010011

Receiver side

Frame 1 : 11001100
Frame 2 : +10101010
partial sum : 101110110
+1
01110111
Frame 3 : +11110000
partial sum : 101100111
+1
01101000
Frame 4 : +11000011
100101011

PAGE NO.:
DATE: / /

```
  10010111
+        1
----------
Sum:    00101100
checksum: 11010011

Sum:    11111111
Complement: 00000000
```

Hence frames are accepted.

ARQ (Automatic Repeat Request)

ARQ is an error control strategy used in a two-way communication system. It is a group of error-control protocols to acheive reliable data transmission over an unreliable source or service. These protocols reside in the Transport layer or Data Link layer of OSI model.

Working principle of ARQ

The main function of this protocol is that the sender receives an acknoledgment from the receiver end implying that the frame or packet is received currectly before a timeout occurs, timeout is a specific period within acknoladgment is send by receiver to the sender If the timeout occurs, then the sender

does not receive the acknoledgment before the specified time, it is implied that the frame or packet has been corrupt or lost during the transmission

- Types of ARQ

- Stop And Wait ARQ

Stop and wait ARQ is also referred to as the alternating protocol is a method used in two-way communication systems to send information between two connected devices. It is reffered to as stop and wait ARQ because the function of this protocol is to send one frame at a time. After sending a frame or packet, the sender doesn't send any further packets until it's receives an acknoladgment from the receiver. If the acknoledgment does not reach the sender before the specified time, known as the timed out

- Go-Back-N ARQ

Go Back-N ARQ is a type of ARQ protocol, in which sending process continues to send several frames or packets even without receiving an acknoledgment packet

from the receiver. The receiver will remove any packet that does not have the desired sequence number it ~~excepts~~ accepts and will resend acknoledgment for the last correct frame. The only drawback of this type of system is that it results in sending packets multiple times, if any frame was lost or found to be currupted., then the frame and all following frames in the send window will be transmitted. . This protocol is more efficient than Stop and wait ARQ as there is no waiting time

- Selective Repeat ARQ / Selective Reject ARQ

Selective Repeat ARQ protocol mechanism is similar to the Go-Back-N protocol mechanism but in selective Repeat ARQ the sending process continues even after a frame is found to be currupted or lost. If a frame is not received at the receivers end, the sender continues to send the succeding frames until it has emptied its window. once this error-correction process has been done, the process continues where it left off. Unlike, GO back-N protocol this does not send a packet multiple times

PAGE NO.:
DATE: / /

★ IEEE Networking

IEEE 802 is a family of IEEE standards dealing with local area networks and metropolitan area networks.
More specially, the IEEE 802 standards are restricted to networks carrying variable-size packets. By contrast, in cell relay network data is transmitted in short, uniformly sized units called cells.

The services and protocols specified in IEEE 802 map to the lower two layers (Data link and physical) of the seven-layer of OSI model.
The sub layers can listed like this:

- Data link layer.
  - LLC Sublayer (logical link control)
  - MAC Sublayer (media access control)
- physical layer
  - LMSC (LAN/MAN standards Committee)

★ 802.2

802.2 is ~~the~~ specifies the general interface between the network layer and data link layer.
Basically the 802.2 is the translator for the Data link layer. 802.2 is concerned with ~~may~~ managing traffic over the physical Network. It is responsible for

flow and error control. The Data link layer wants to send some data over the network. 802.2 logical link control helps make this possible. It also helps by identifying the line protocol, like NetBIOS, or Netware.

* 802.3

802.3 is the standard which Ethernet operates by. It is the standard for CSMA/CD. This standard encompasses both the MAC and physical Layer standards.

CSMA/CD is what Ethernet uses to control access to the network medium (network cable). If there is no data, any node may attempt to transmitt, if the nodes detect a collision, both stop transmitting and wait a random amount of time before retransmitting the data.

The original ~~80.2~~ 802.3 standard is 10 mbps. (mega bits per second) 802.3u defined the 100 mbps (fast ethernet) standard, 802.3z / 802.3ab defined 1000 mbps Gigabit Ethernet, and 802.3ae define 10 Gigabit ethernet.

Commonly, Ethernet networks transmit data in packets, or small bits of information. A packet can be a minimum size of 72 bytes or a maximum of 1518 bytes.

The most common topology for Ethernet is the star topology

PAGE NO.:
DATE: / /

802.5

The token is a special frame which is designed to travel from node to node around the ring.

The token ring network is designed in such a way that each node on the network is guaranteed access to the token at some point. This equalizes the data transfer on the Network. This is different from an Ethernet network where each workstation has equal access to grab the available bandwidth, with the possible of a node using more bandwidth than other nodes

Originally, token ring operated at a speed of about 4 Mbps and 16 Mbps. 802.5t allows for 100 mbps speeds and 802.5v provides for 1 Gbps over fibber.

Token ring can be run over a star topology as well as the ring topology.

There are three major cable types for token ring: Unshield Twisted pair ~~table~~ (UTP), (STP) and fibber.

Token ring utilizes a multi-station Access unit (MAU) as a central wiring hub.

PAGE NO.:
DATE: / /

- IEEE 002.11 standard.
  - It's commonly known as wifi that defines the Map and mac-map physical layer specification for wireless lan
  - It uses radiowares instead of cables for connecting the devices

- Terminologies of 802.11

1> station.
2> Access point (AP) or (WAP) → wireless AP
3> Client
4> Distribution system
5> Frame
6> SDU (service data unit)
7> PDU (protocol data unit)
8> NIC (Network interface card)
9> portal

- 802.11 architecture provides some basic services W-LAN (wireless LAN)
  (1) Basic services (BSS) :- It consist of group of stations and relise on access point in which station from different BSS interact through the AP which link multiple W-LAN cells.

PAGE NO.:
DATE: / /

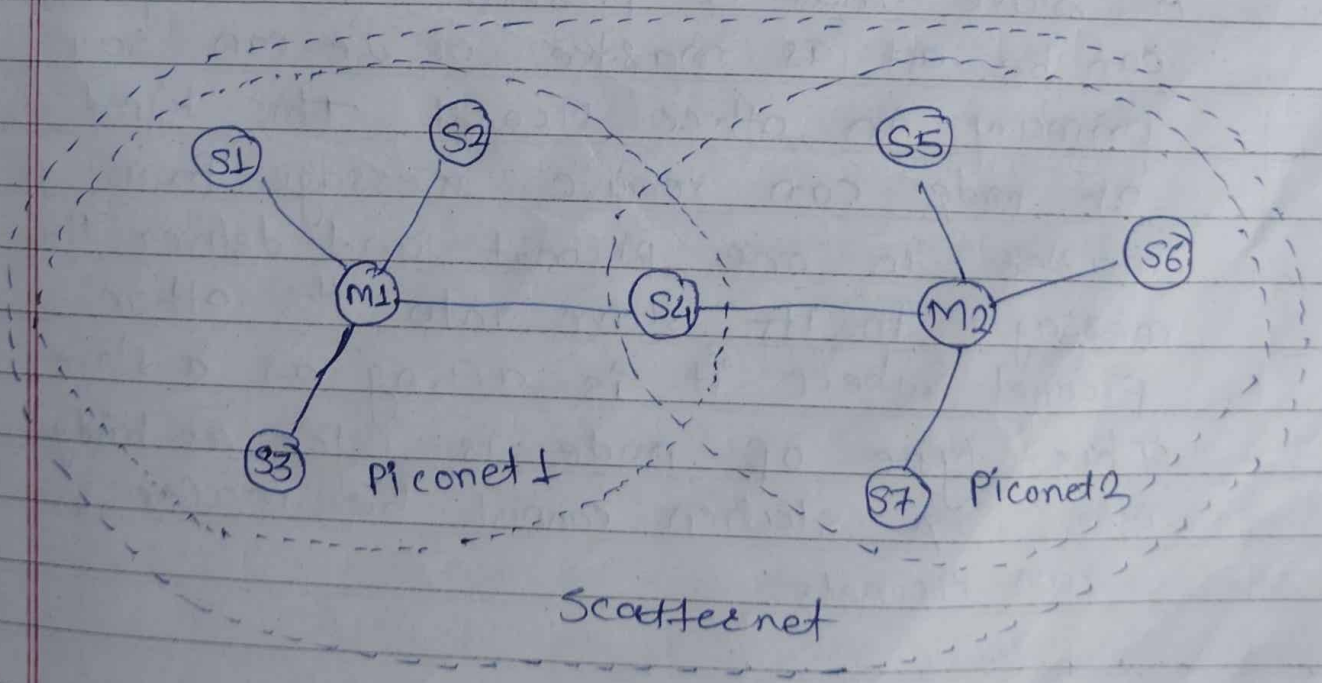
- **Bluetooth**

It is a wireless pessonal Area Network (WPAN) technology and is used for exchanging data over smaller distance. This technology was invented by Ericson in 1994. Maximum device that can be connected at the same time are 7. Bluetooth ranges upto 10 meters. It provides data rates upto 1 Mbps or 3 Mbps depending upon its version. A bluetooth network is called piconet and a collection of interconnected piconet is called Scatternet

- **Bluetooth Architecture**

The Bluetooth Architecture ~~of but~~ defines two types of networks:

1) Pickonet
2) Scatternet.



Advantages

1. Low cost
2. Easy to use
3. It can also penetrate through walls
4. It is used for voice and data transfer.

Disadvantage

1. It can be hacked and hence, less secure
2. It has low data transfer rate : 3 mbps
3. It has smaller range : 10 meters

★ Piconet :-

Piconet is a type of bluetooth network that contains one primary node called master node and seven active secondary nodes called as slaves slave nodes. Thus we can say that there are total of 8 active nodes which are present at a distance of 10 meters. The communication between the primary and secondary node can be one-to-one or one-to-many. Possible communication is only between the master and slave ; slave to slave communication is not possible. The secondary nodes cannot be participate in communication.

★ Scatternet :

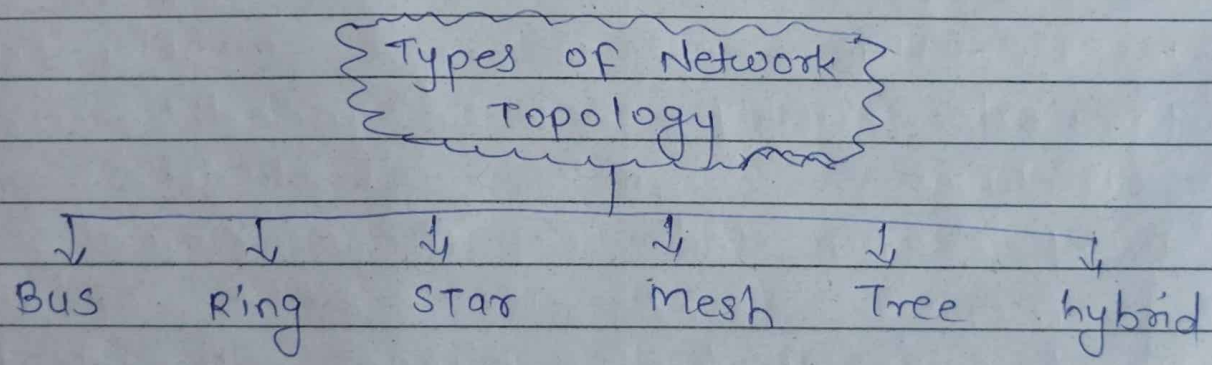
It is formed by using various piconets. A slave that is present in one piconet can be act as master or we can say primary in other piconet. This kind of node can receive message from master in one piconet and deliver the message to its slave into the other piconet where it is acting as a slave. This type of node is refer as bridge node. A station cannot be master in two piconets.

4. Network Topologies and Network devices

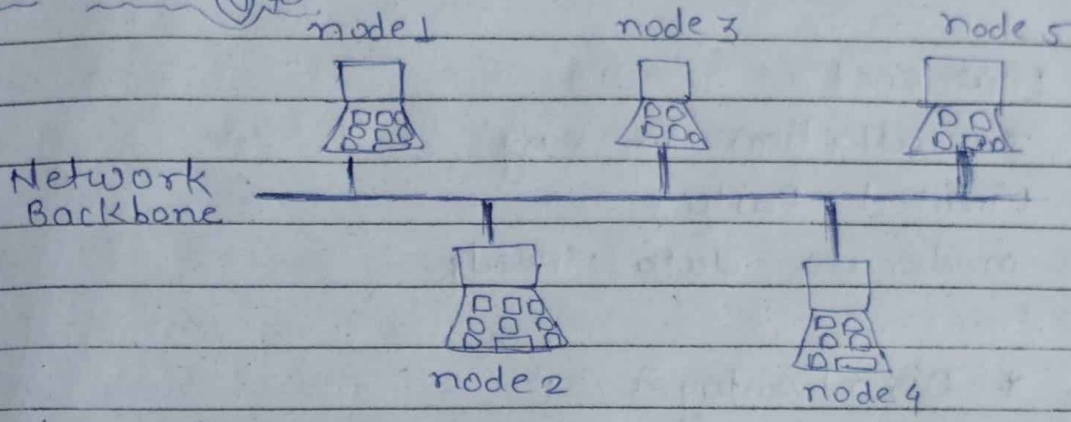
- Topology :- Topology defines the structure of the network of how all the components are interconnected to each other.

- There are two types of topology
  1. physical Topology.
  2. Logical Topology

Note:- [physical topology is the geometeic representation of all nodes in a network]



1) Bus Topology



- It's main purpose is to avoid data loss
- In bus topology all nodes are connects to the backbone cable
- Data transfer in both direction.
- Data receive by each and every node
- The most common access method of the bus topology is CSMA (carrier sense multiple Access)
  { CSMA :- It is a media access control used to control the data flow. }
- There of Two techniques of CSMA
  - CSMA CD (Collision detection) :- CSMA CD is an access method used to detect the collision.
  - CSMA CA (Collision Avoidance) :- CSMA CA is an access method used to detect the collision.
- The bus topology is mainly used in 802.3 and 802.4 networks.

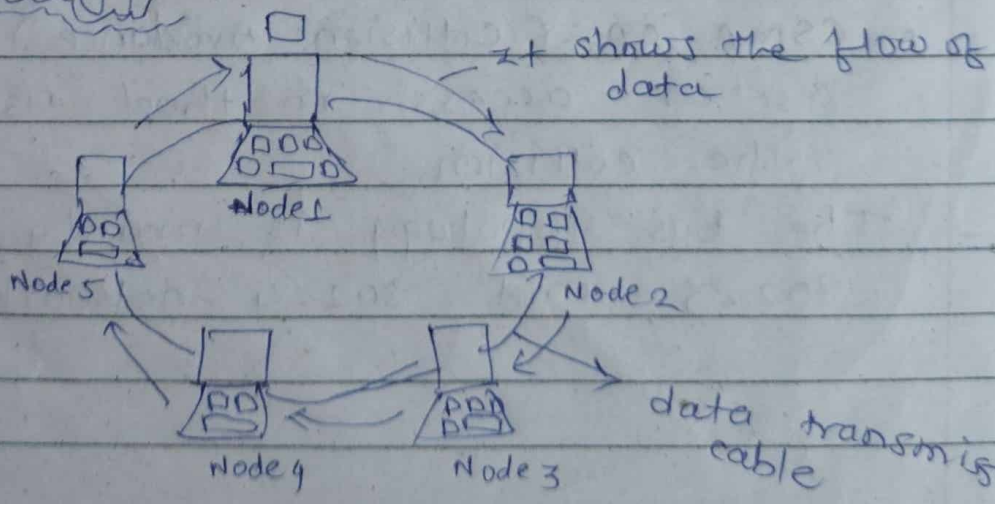
* Advantages *

- Low cost
- Installation is easy
- Limited failure
- Moderate data speeds

* Disadvantages *

- Difficult Troubleshooting
- expensive cabeling
- If main cable get currupt then all network get collapse
- Signal Interference :(If two nodes send the message simultaneously, then the signals of both the nodes will collide with each other)
- Reconfiguration is difficult

2) Ring Topology



- Ring Topology is like a bus topology, but connected ends
- Every node is connected with neighbour node
- Data flows in one direction
- It is unidirectional
- The data flows in a single loop continously, known as endless loop
- ~~The~~ data will be flow in a clockwise direction
- The most common access method of the ring topology is Token passing

- Token passing :- It is a network access method in which token is passed from one node to another node
- Token :- It is a frame that circulates around the network

- Working of Token passing.

- A token moves around the network, and it is passed from computer to computer until it reaches the destination
- The sender modifies the token by putting the address along with the data.
- The data is passed from one device to another device until the destination address matches. ~~Once~~

Once the token received by the destination device, then it sends the acknoledgment to the sender.

- In a ring topology, a token is used as a carrier.

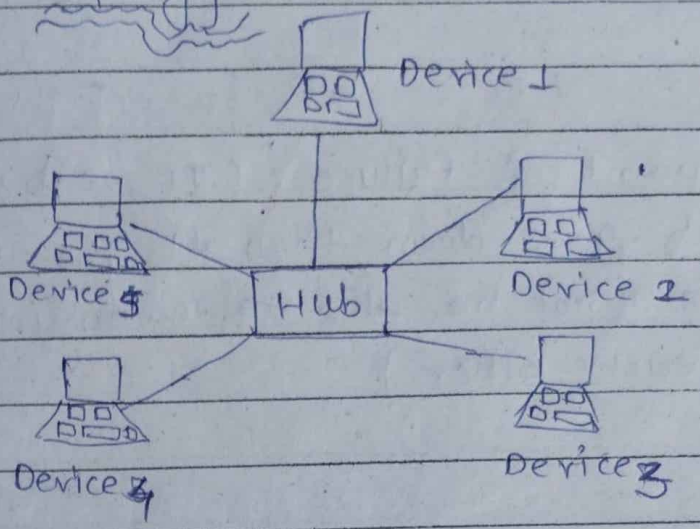
* Advantages *

- Easy Installation
- Low cast
- Reliable.
- Network managment
- Product availability

* Disadvantages *

- Difficult Troubleshooting
- Failure
- Reconfiguration difficult
- Delay (It is directly protorticnal to the no. of nodes)

3) Star Topology



- Star topology is an arrangment of the network in which every node is connected to the central hub device like hub, switch a central computer
- The central computer is known as Server and the pheripheral 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.

* Advantages *

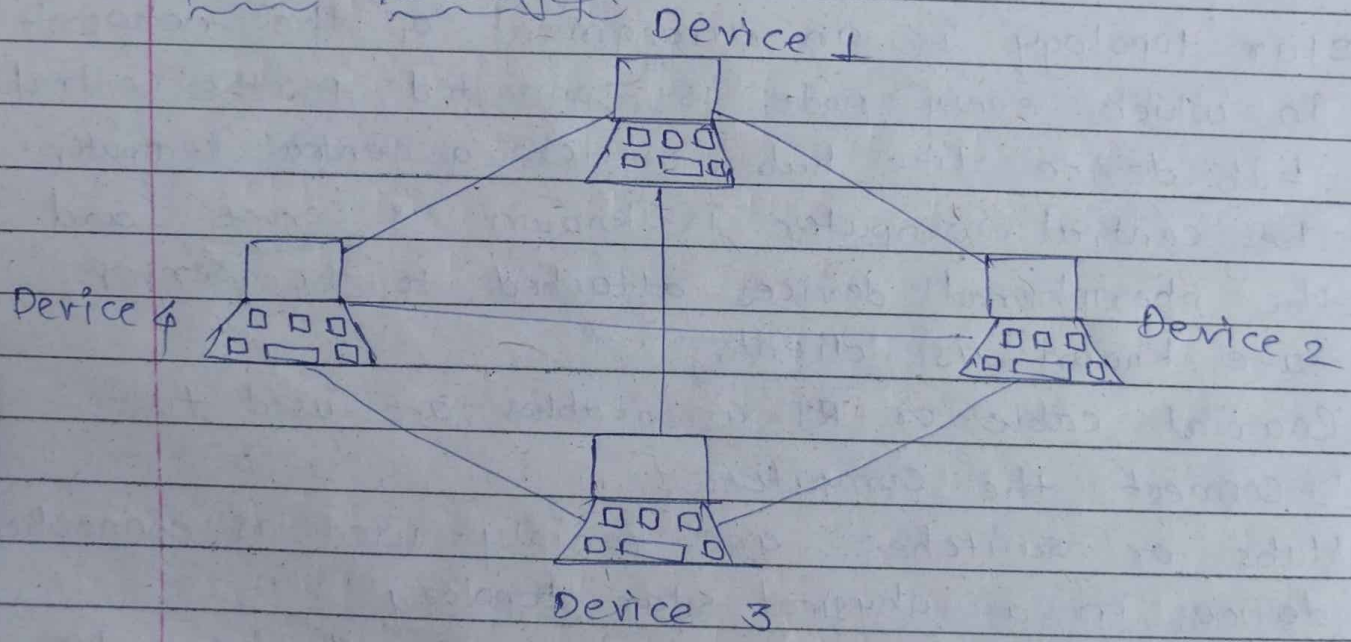
- Limited failure
- Easily expandable
- less expensive / cost effective
- Familiar Technology
- High data speeds
- Network Control

* Disadvantages *

~~If the~~

- A central point of failure :-(If central hub or switch goes down, then all the connected nodes will not be able to communicate with each other)
- Cables

4) Mesh Topology

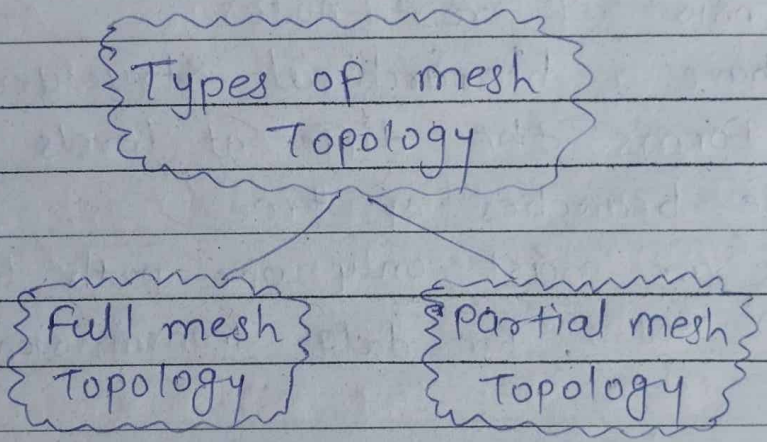


- All computer are connected with each other
- multiple paths are available
- There is no central point like switch or hub
- Internet is an example of mesh Topology
- It is a wireless network.

- This Topology divided into 2 parts :
  1) Fully connected
  2) partial connected

1) Fully connected :- Every node connected with each other

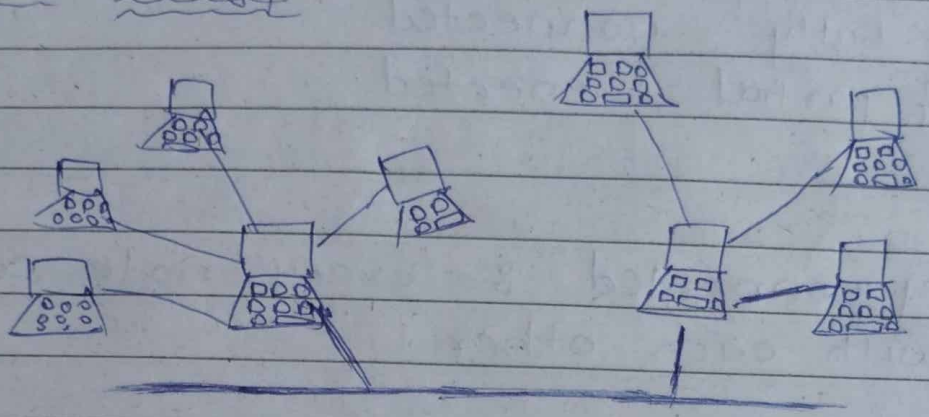
2) partial connected :- Not every computer, but those computes communicate frequently are connected



* Advantages
  - Communication is fast
  - It is Reliable
  - Easier reconfiguration (Scalable)

* Disadvantages
  - High Cost
  - Difficult to manage
  - Efficiency

5) Tree Topology

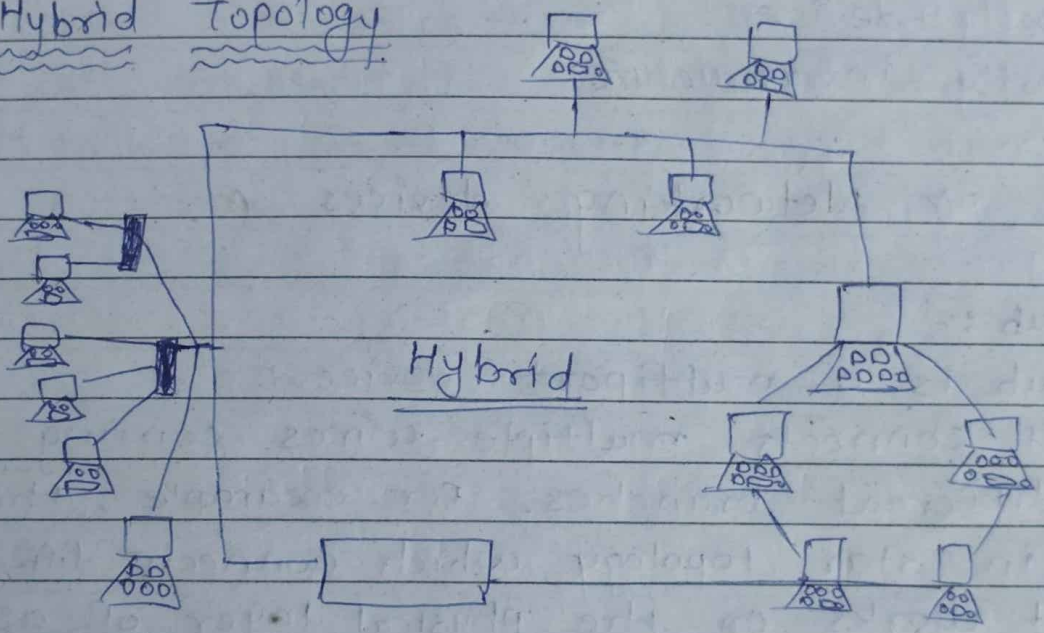


- Tree topology is a combination of bus and Star Topology
- It consist of root nodes
- It have a hierarchical structure
- It forms the different levels which are the branches of tree
- These are exist only one path between two nodes for data transmission.

* Advantages *
- Easily managable
- Easily expandable / scalable
- Limited failure
- point to point wiring
- Error detection

* Disadvantages *
- Difficult troubleshooting
- High cost
- Failure (If the base have problem then complete topology will stop)
- Reconfiguration difficult.

6) Hybrid Topology



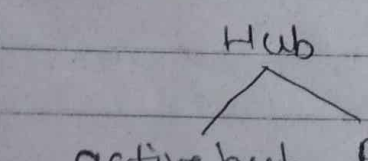
- The combination of various different topologies is known as Hybrid topology
- It is a combination of more than one topology
- It consist of different links between the nodes to transfer the data.

* Advantages *
- Reliable
- Flexible
- Scalable / expandable
- Effective

* Disadvantages *
- Complex design
- Costly devices
- Costly infrastructure

☆ Networking devices ☆

1) Hub :-
- Hub is a multiport device.
- It connects multiple wires coming from different branches. for example, the connector in star topology which connects different stations
- It works on the physical layer of OSI model.
- It having one collision domain and brodcast domain
- It generally used for Local area network (LAN
* - Hub cannot filter data, so data packet are sent to all connected devices.
* - Hub is not an 'intelligent device because it cannot find out best path for data packets.



2) Router

- A router is a device that routes data packets based on their IP addresses.
- Router operates on the Network layer.
- There is no collision of data.
- Router normally connect LANs and WANs together
- Router is responsible for eecieving, analyzi and forwarding data packets.
- It brodcast data to all the devices
- It have static routing cable and dynamic routing cable.
- Types of router :- i) wireless Router
  ii) Brodband Router
  iii) Core Router
  iv) Edge Router
  v) B-router.

3) Gateway

- It forms a passive between two networks co-orprating with different transfer protocol.
- It can be ~~exit~~ ~~or~~ entry, exit point of netwo
- It works on any layer of OSI model depending on the Functionality.
- It acts as a protocol conveeter.
- It also store routing path.
- It uses packet switching technique
- Types :- 1) Unidirectional gate way
  2) Bidirectional gate way.

4) Repeater

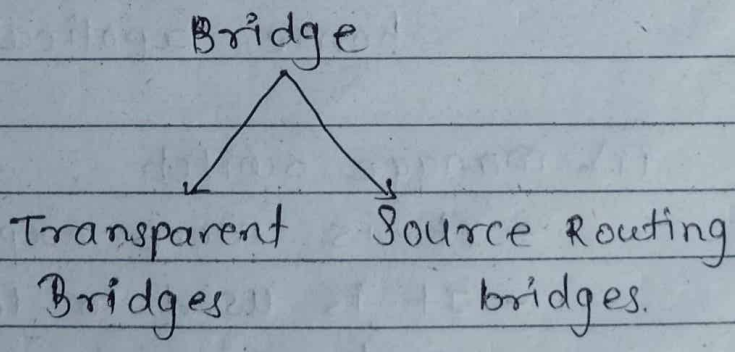
- Repeater works on a physical layer
- It is a two port device
- It is used to ~~amplify and~~ regenerate the signal over the same network
- Repeater do not amplify the signal
- When the signal becomes, weak, they copy the signal bit by bit and regenerate it at the original strength.
- Within a network install repeater, at every particular distance to regenerate the strength of signal
- Types :- i) Depending on signal
  analog and digital
  ii) Type of network
  wired or wireless
  iii) Domain of LAN
  local repeater & remote repeater

• Disadvantages

i) can't differentiate between signal & noise
ii) can't connect to two different network
iii) It can not reduce the network traffic

5> Bridge (layer to switch)

- It operates on data link layer of OSI model
- It connects the LAN that has a similar protoco
- It is a Two port device in which ~~one is~~ single input or single output port, thus making it a 2 port device
- Through bridge multiple LAN's can be connected together to form large WAN network
- A bridge is a repeater, with add on a functionality of filtering content by reading the MAC addresses of source and destinatio
- If the destination MAC address could not available, it brodcast the data to all the nodes.



6) Switch

- switches connects multiple devices within a local area network (LAN), allowing them to communicate with each other.
- It is a layer 2 device
- It works on a data link layer of OSI model
- switch is a multiport network bridge
- It uses packet switching technique
- It use full duplex transmission mode
- It also perform the error checking before forwarding the data
- maximum 48 ports are available
- types of switches :-

i) unmanage switch
- It is less expensive
- It is used to small buisness, home applications

ii) manage switch
- It is more expensive
- It is used to large organization and companies
- It provides advanced features

iii) LAN switch
- It is also known as ethernet switch
- It is used to reduce Traffic

iv) POE (power over ethernet)

7) Modem

- Modem is used to connect to ISP (Internet service Provide
- It is used in a home network
- The main function is to convert analog signal into digital signal
- Modem perform both modulation and demodulati
- It also called as signal Translator
- Working :-

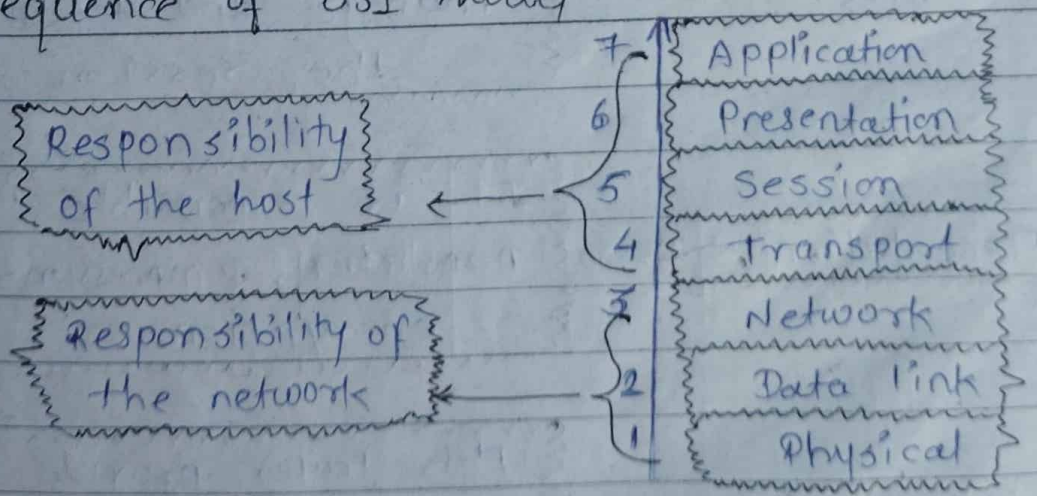
step 1 : Data generation
step 2 : Modulation
step 3 : Transmission
step 4 : Demodulation
step 5 : Decoding (It is a process of maintaining the privacy

5. Network reference model.

OSI model

- OSI stands for open system Interconnection
- It deals with how the information from software application in one computer moves through physical medium to the software application of another computer.
- The mode is developed in 1984 for international organization for standardization
- OSI consist of seven layers, and each layer performs a particular network functions
- OSI model divided into 2 Types
  - i) upper layer
  - ii) Lower layer

- characteristic of OSI model. and
- Sequence of OSI model



* Layers of OSI Model
* Function of the OSI Layers.

1) Physical → It provides a physical medium through which bits are transmitted

2) Data link → It is used for error free transfer of data frames

3) Network → It is responsible for moving the packets from source to the destination

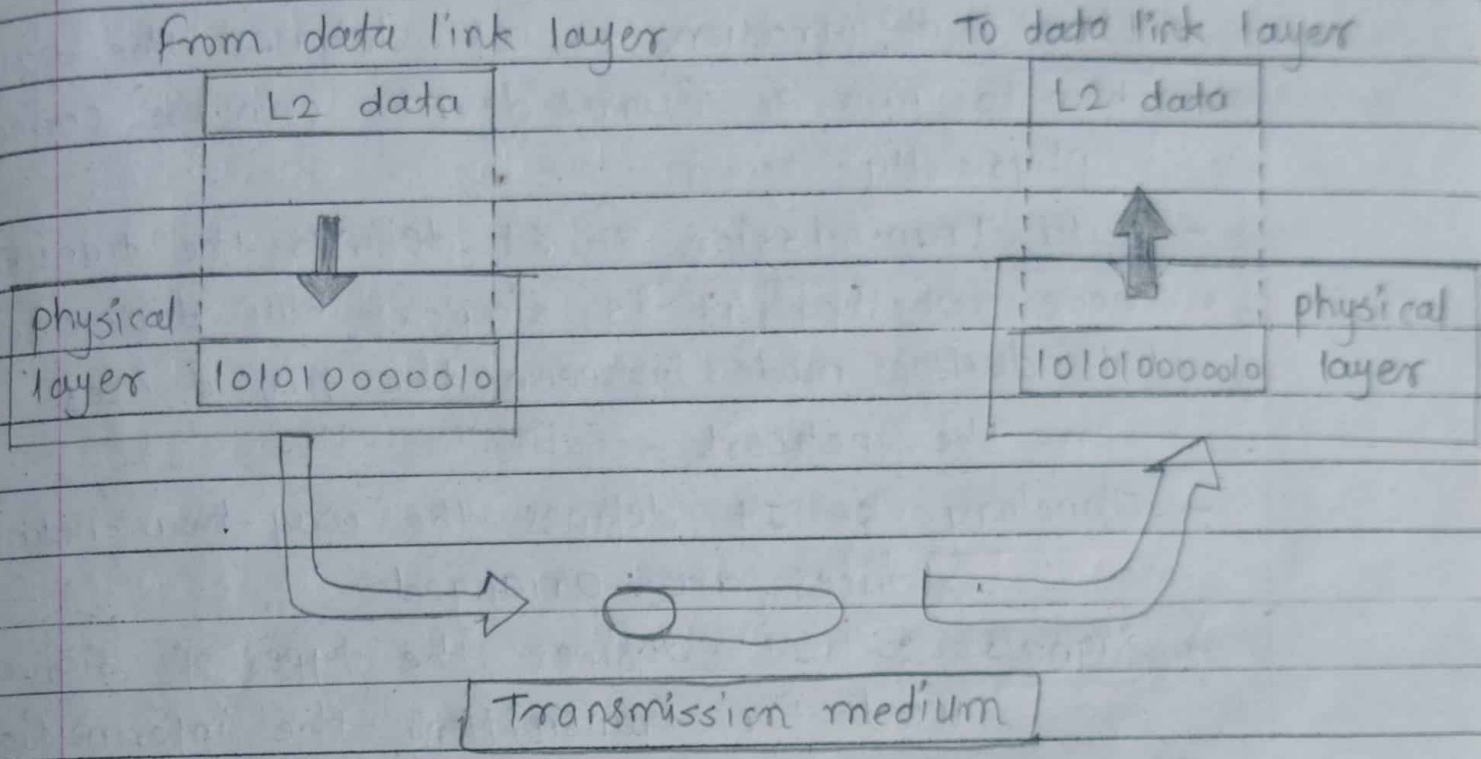
4) Transport → It provides reliable message delivery from process to process

5) Session → It is used to establish, manage and terminate the session

6) Presentation → It is responsible for translation, compressions encryption

7) Application → This layer proride the service to the user

1) physical layer

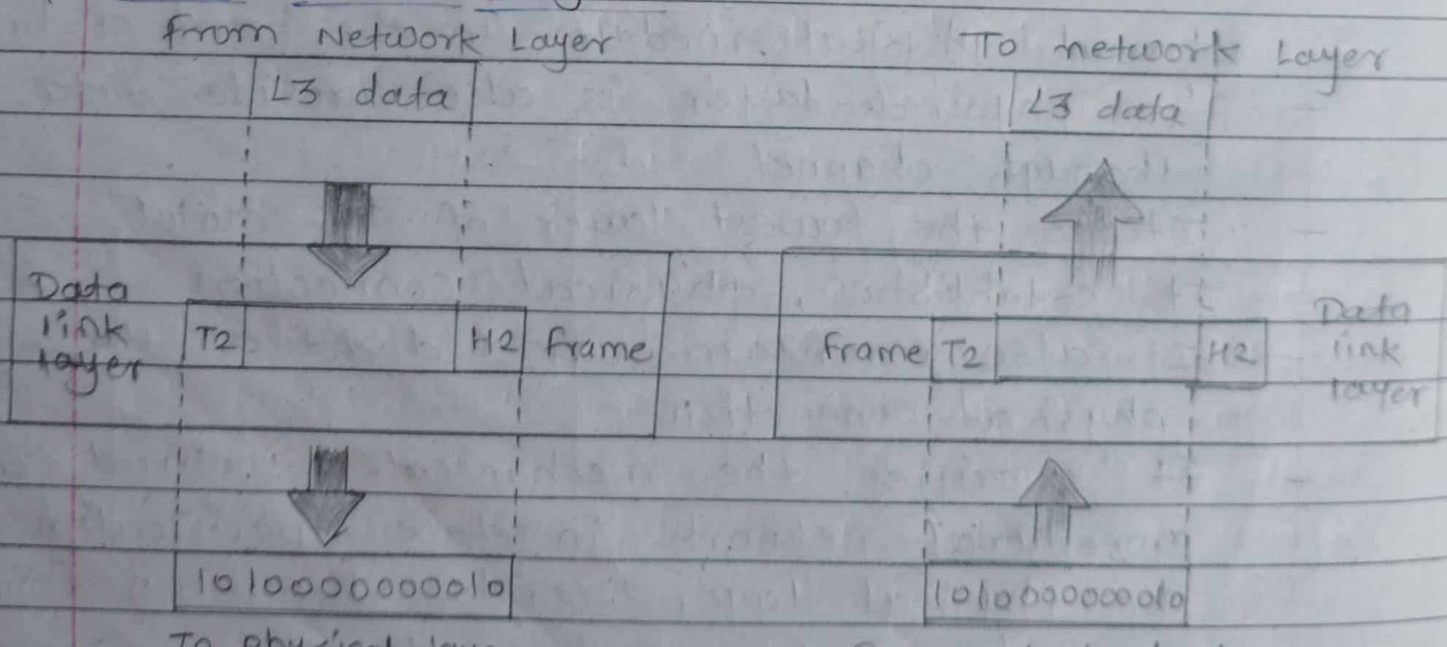


- The main function is to transmit the data through physical medium in the form of bits.
- The physical layer is also provide data through channel.
- It is the lowest layer of OSI model
- It establishes, physical connection
- It also maintain and deactives the physical connection
- It specifies the mechanical, electrical and procedural network interface specification
- The physical layer sends data bits from one device to another device

~ Functions

- Line configuration :- It defines the way how to two or more devices can be connected physically
- Data Transmission :- It defines the transmission mode whether it is simplex, half duplex or full duplex mode between the two devices on the network
- Topology :- It defines the way how network devices are arranged
- Signals :- It defines the types of signal used for transmitting the information.

2) Data - Link Layer

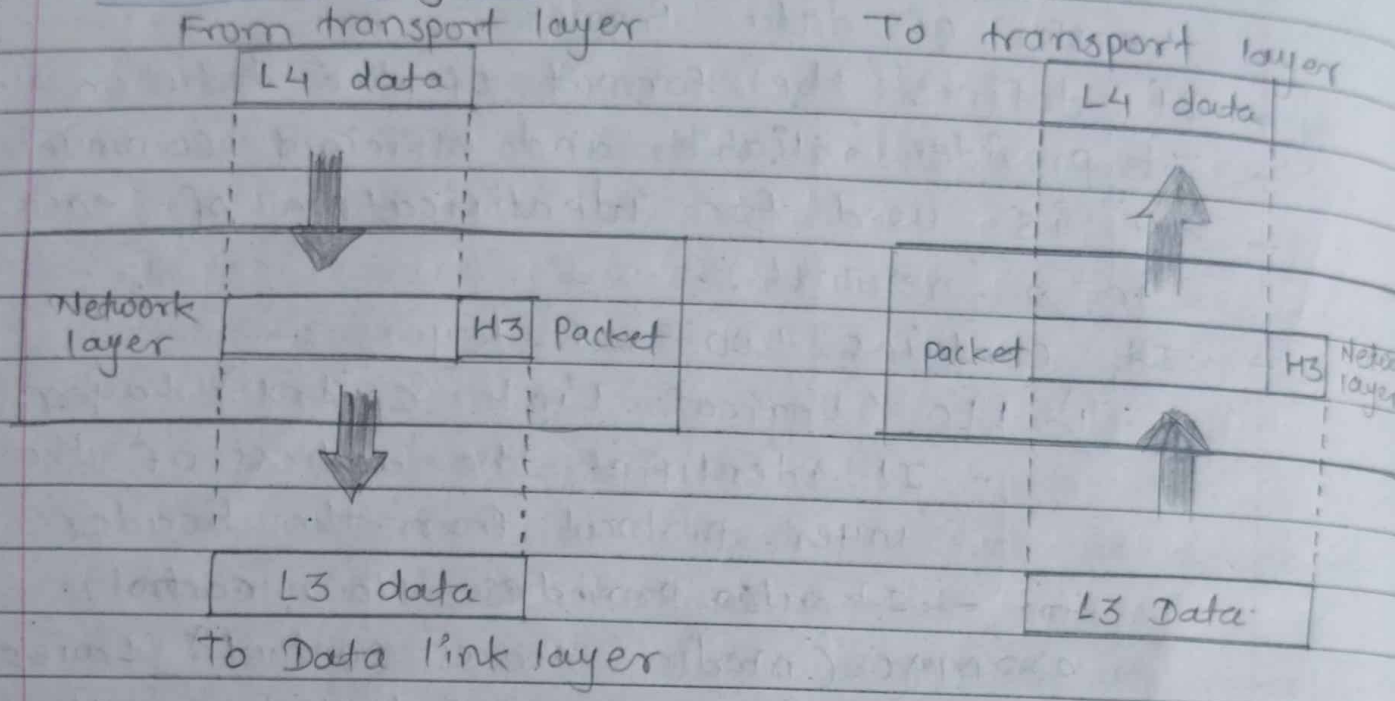


- Error detection is done by using CRC method
- Data-link layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network
- It provides reliable and efficient communication.
- It is used for identification of each devices in a network.
- It contains two sub-layers :-
  1) LLC (Logical Link control) Layer
     - It identifies the address of the network layer protocol from the header
     - It also provides flow control.
  2) MAC (Media Access control) Layer
     - A MAC is a link between the logical link control layer and the network's physical layer
     - It is used for transferring the packets over a network

functions

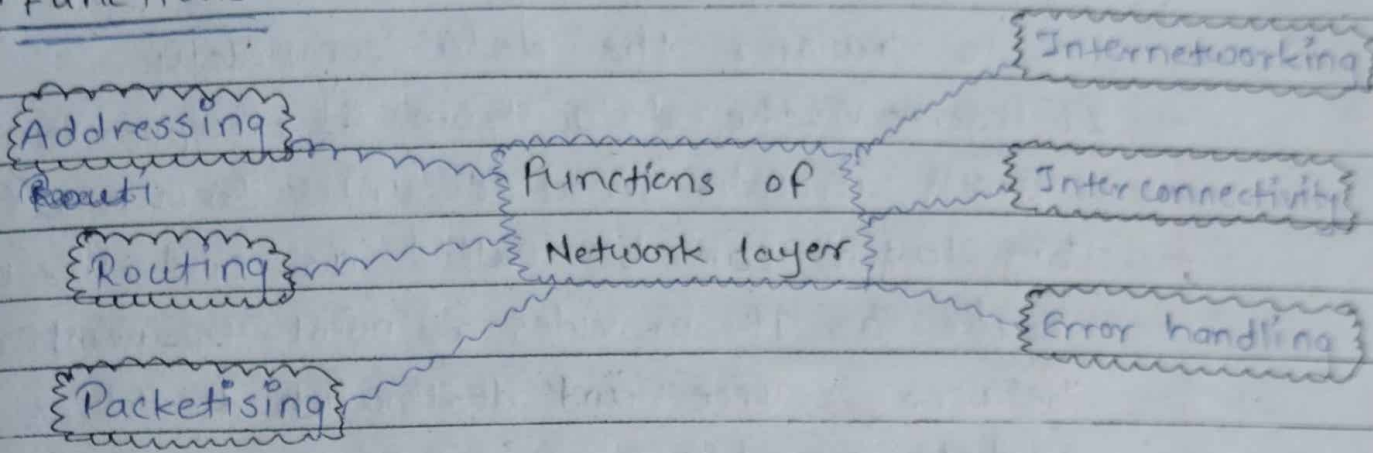
- framing
- physical Addressing
- flow control
- Error control
- Access control

3) Network layer

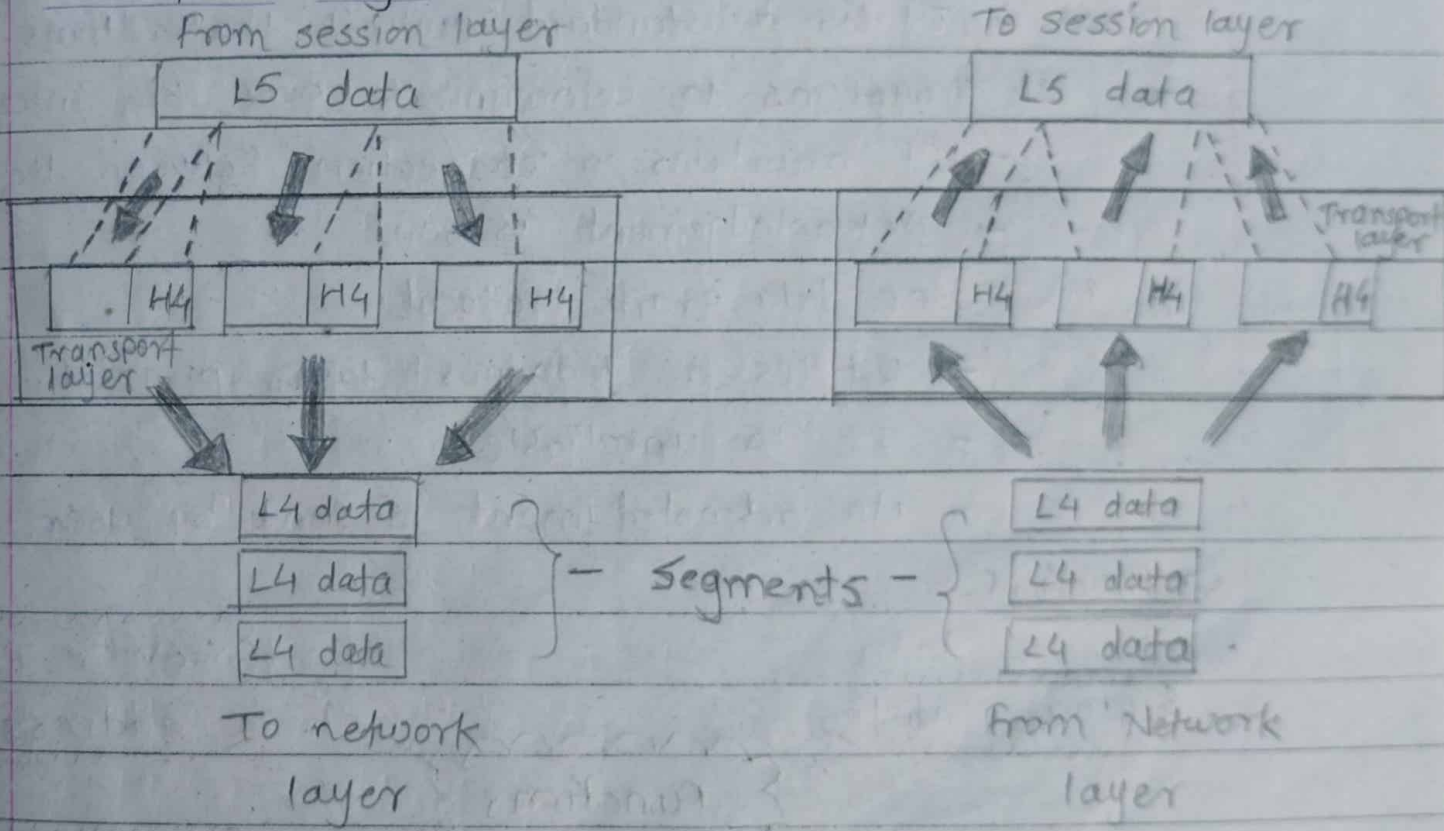


- It is a layer 3 that manages devices addressing, tracks the location of devices on the network.
- It determines the best path to move the data from source to destination.
- Router is a device which works on this layer.
- Routers are the layer 3 device
- (IP) Internet protocol is work on this layer.
- The protocols used to route the network traffic are known as Network layer protocols.
- The main function of network layer is to maintain the quality of data and transmit it from source to destination.
- Data is transmitted in the form of packets. Via various logical network pathways between various devices.

- Functions



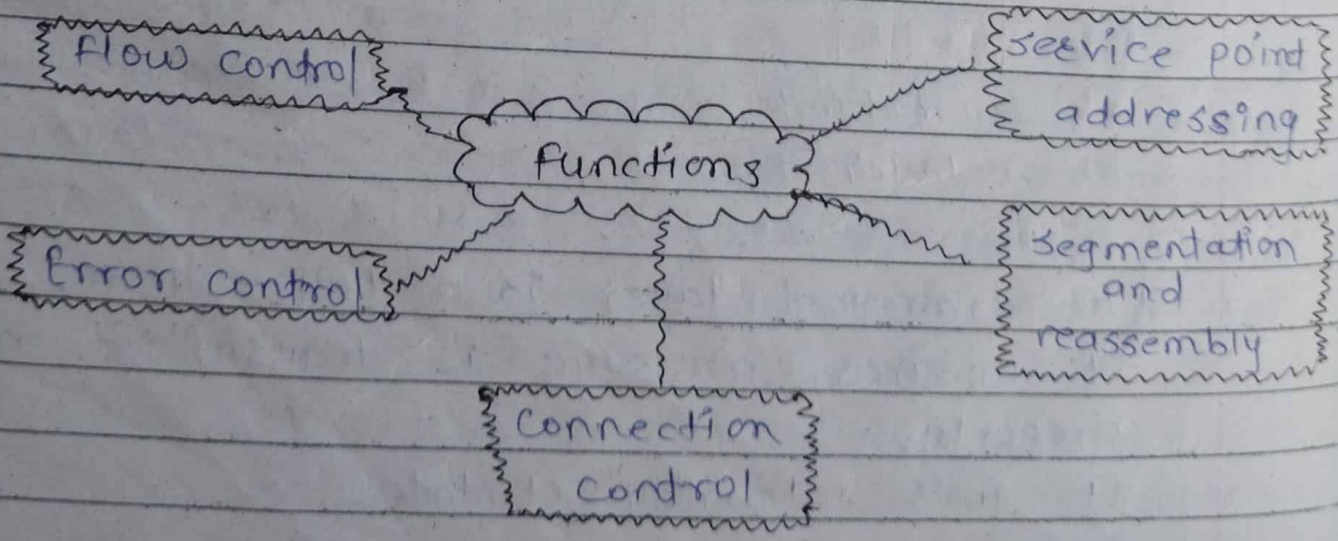
4) Transport Layer



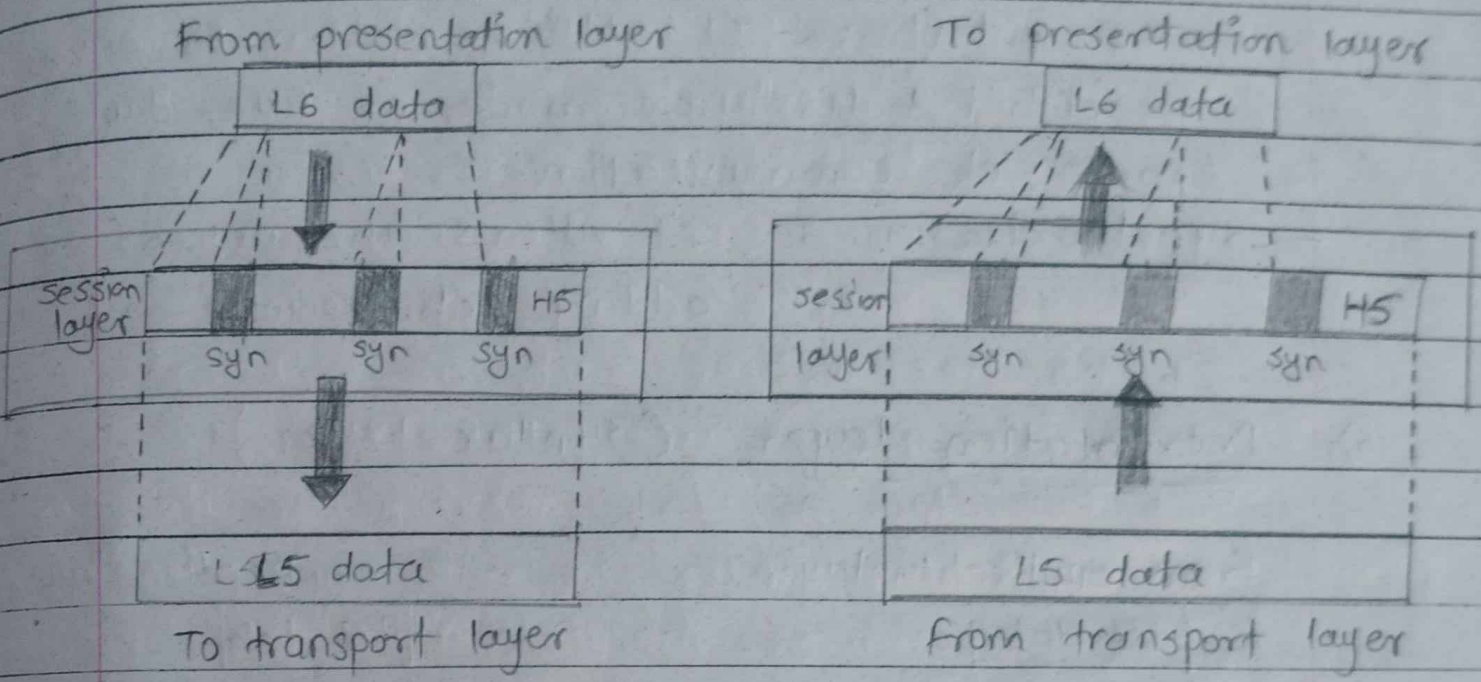
- The transport layer is a Layer 4 en.
- It ensures message is transmitted and receive properly.
- It gives reliability of data.

- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts it into smaller units known as segments
- This layer can be called as end-to-end layer as it provides a point-to-point connection between source and destination to delivers the data reliably.
- It consist of two protocols.
  i) TCP (transmission control protocol)
     - It is a standard protocol that allows the systems to communicate over the internet
     - It maintains a connection between hosts.
     - Acknoledgement is sent
  ii) User data gram protocol
     - It is a transport layer protocol
     - It is unreliable
     - No acknoledgment is sent by user.

↳ Functions



5) Session layer

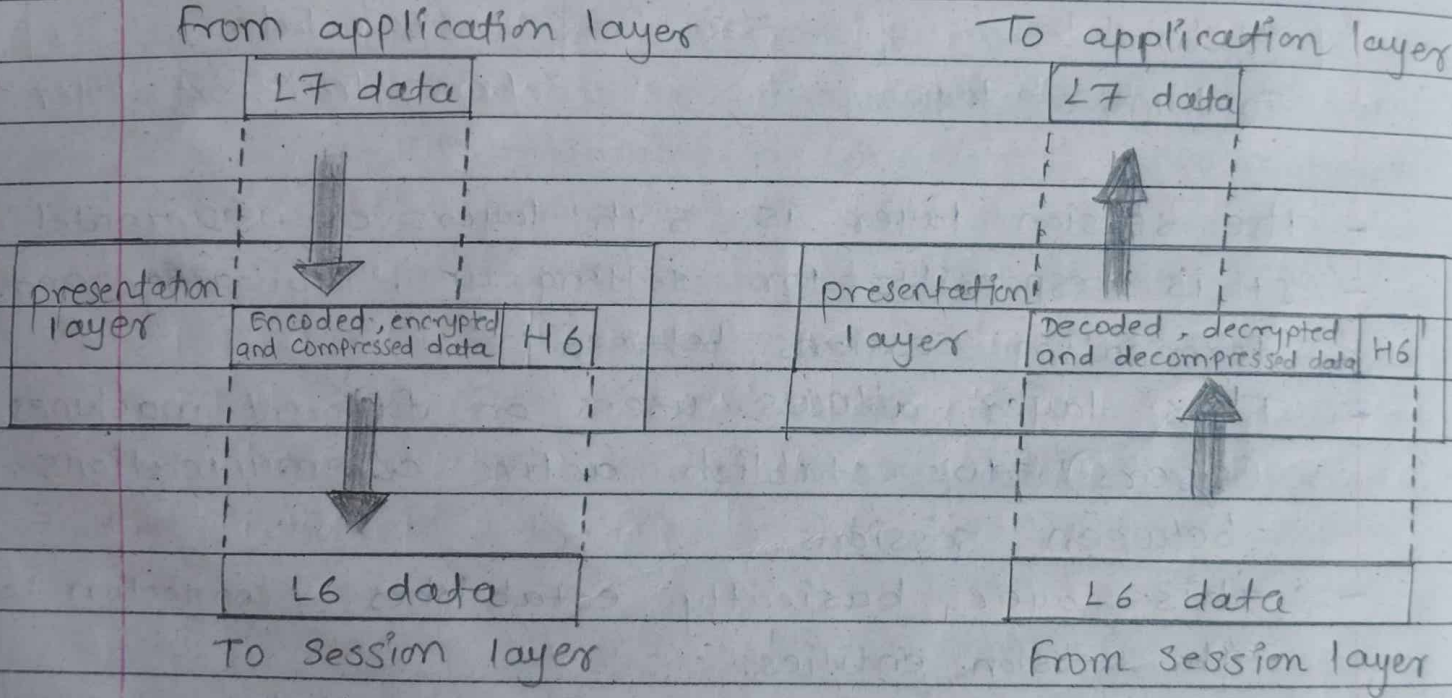


- The session layer is 5th layer of OSI model
- It is responsible for setting up, managing and terminating sessions ~~between~~ p
- This layer allows users on different machines (users) to establish active communications between sessions.
- This layer basically establishes a connection between the session entities.
- This layer handles and manipulates data which it receives from the session layer as well as from the presentation layer.

Functions

- Dialog control :- It allows system to communicate in either half-duplex mode or full-duplex mode of communication
- synchronization :- It allows the process of adding checkpoints.

6) Presentation layer (syntax layer)



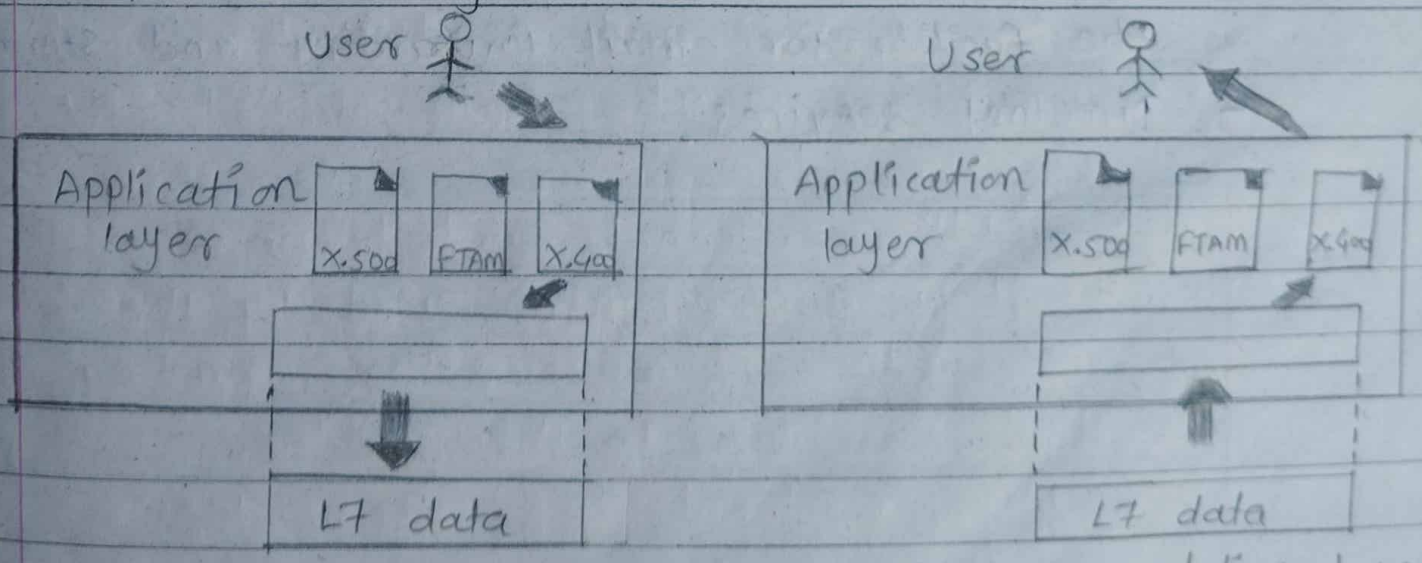
- A presentation layer deals with syntax and symantics of the information exchange between the two systems.
- It acts as a data translator for a network.

- 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 syntax layer.

Functions

- **Translation** :- The processes in two systems exchange the information in the form of characters strings, numbers and so on.
- **Encryption** :- Encryption is needed to maintain privacy.
- **Compression** :- Data compression is a process of compressing the data.

Application layer



- The application layer provides the functionality to send and receive data from users.
- It acts as the interface between user and the application.
- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transperency, resource allocation, etc.
- It provides network service to the user.
- An application layer is not an application, but it performs the application layer functions.

Functions

- FTAM (File transfer, access and managment)
- Mail service :- An application layer provides the facility for email forwarding and storage.
- Directory services.

TCP/IP reference model

- TCP/IP stands for Transfer control protocol / Internet ~~control~~ protocol., which are core protocols of the internet.
- This model defines the how data is teansmitted over networks.
- This model is similar to OSI model consisting of 5 layers. Application layer, Transport layer, Network layer, Data-link layer, physical layer.

Network 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 data between two devices on the same network.

≈ protocols

1) IP (Internet protocol)
- IP addressing
- Host to Host communication
- Data encapsulation and formatting
- fragmentation and reassembly
{It consist of limit of IP datagram known as MTU (maximum transmission unit)
- Routing

2) ARP (Address Resolution protocol)
- ARP request and ARP reply.
- When sender wants to know the address of device it brodcast ARP request
- Every device attach to network accept the ARP request but only recieptent recognize it and send back its physical address in the form of ARP reply.

3) ICMP (Internet control message protocol)
- It is a mechanism used by the hosts or routers to send notification regarding datagram problems back to the sender.
- this protocol uses two teams:
  i) ICMP test
  ii) ICMP reply.

i) ICMP Test :- ICMP test is used to whether the destination is reachable or not

ii) ICMP Reply :- ICMP Reply is used to check whether the destination device is responding or not.

2) Transport layer.

- The transport layer is responsible for the reliability, flow control and correction of data which is being sent over the network.

protocols

1) UDP (User Datagram protocol)
   - Connectionless
   - Unreliable
   - It consist of fields, like :-
     - Source port address
     - Destination port address
     - checksum - 16 bit limit
     - Total lengths.

2) Tcp (Transmission Control protocol)
   - Connection oriented service
   - Reliable
   - Segmentation and reassembling

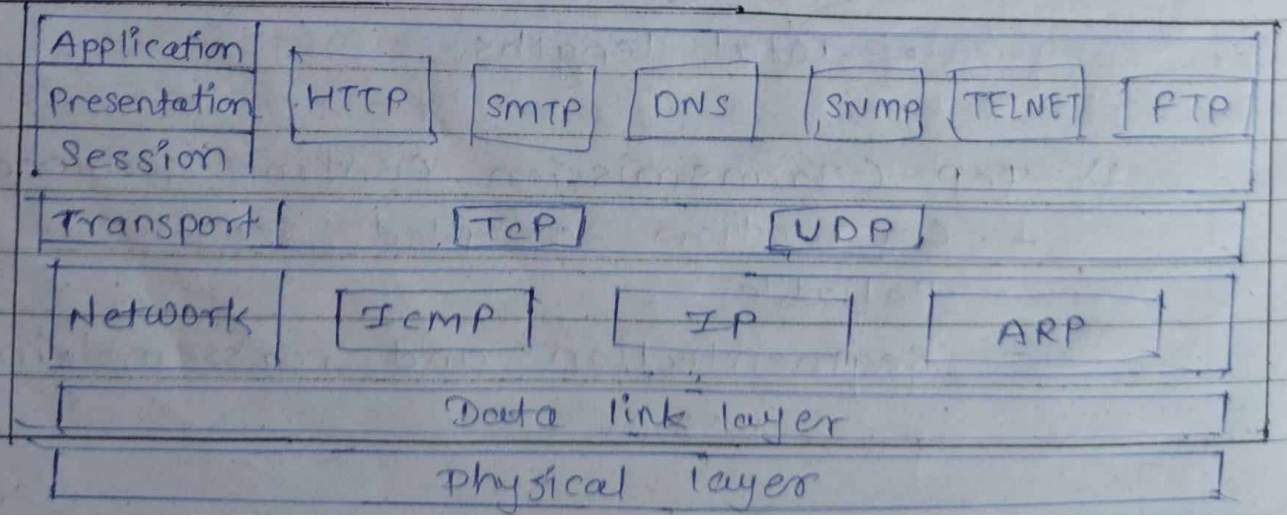
3) Application layer

- 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 applications.

protocols

- HTTP (Hypertext Transfer protocol)
- SNMP (Simple Network managment protocol)
- SMTP (simple mail ~~pr~~ Transfer protocol)
- DNS (Domain Name system).
- FTP (File Transfer protocol)
- TELNET (Terminal Network)

Functions of TCP/IP layers



* Comparison of OSI and TCP/IP reference model

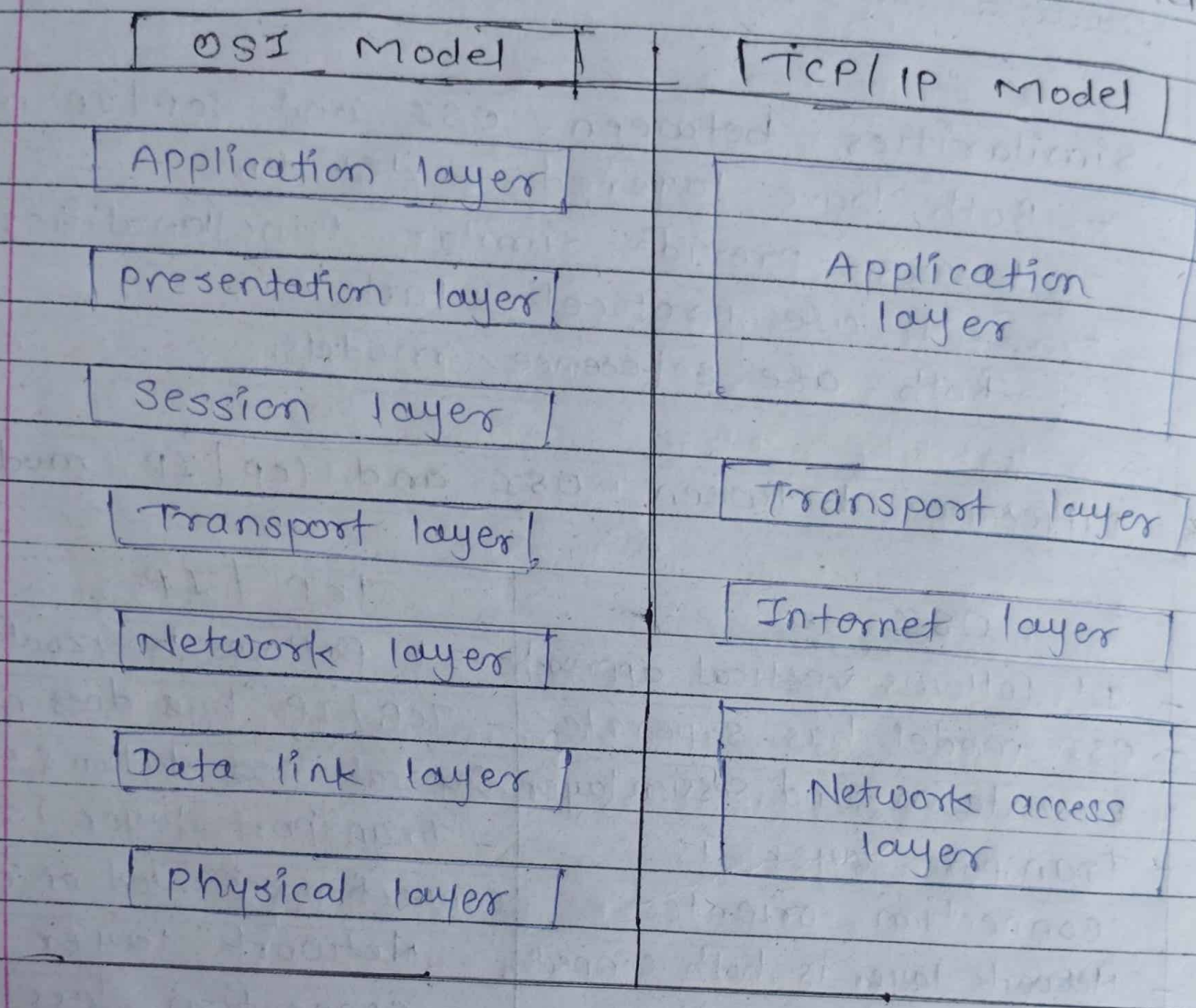
Similarities between OSI and TCP/IP model

- Both have layered architecture
- Layers provide similar functionalities.
- Both are protocol stack
- Both are reference models.

* Difference between OSI and TCP/IP model

OSI	TCP/IP
- It follows vertical approach	- It follows horizontal approach
- OSI model has saperate Presentation and session layer	- TCP/IP has does not have saperate presentation & session layer
- Transport layer is connection oriented	- Transport layer is both connection oriented or connectionless
- Network layer is both connection oriented and connection less	- Network layer is connection less
- It has 7 layers	- It has 4 layers
- OSI model has a problem of fitting the protocols into the model	- TCP/IP model does not fit any protocol
- protocols are hidden In OSI model and are easily replaced as the technology changes	- In TCP/IP replacing protocol is not easy

Diagramic comparison between OSI and TCP/IP



DCN

Unit : 6 TCP / IP Fundamentals

Date
Page No.

6.1 TCP / IP Protocols : is a collection of communication protocols that connect network devices on the internet.

(1) SLIP (serial line internet protocol)

- It is IP that allows users to gain internet access using computer modem.
- It was used on dedicated serial links.
- It is usually used with line speed bet^n 1200bps and 19.2 kdps. It is allowing mixes of hosts and routers to communicate with one another.
- It does not provide addressing, error detection and Packet type identification.

- Problems of SLIP

1) Standard Datagram size specification
2) Error detection / correction mechanism
3) control messaging
4) Type Identification
5) Address Discovery method
6) support for compression
7) security features

(2) PPP (Point - to - Point) Protocol

- It is a layer two protocol i.e. data-link.
- It defines the format of frames.

L&W

- It defines the link establishment process.
- It defines exchange process.
- The main feature of PPP protocol is the encapsulation.
- It defines the authentication process between the two devices.
- It is used in broadband communications having heavy loads and high speed.
- It is used to transmit the multi protocol data betⁿ the two connected (point - to - point) computers.

Flag	Address	control	Protocol	data & Padding	FCS	Flag.
1 Byte	1 Byte	1 Byte	1 to 2	variable	2 to 4	1 Byte.

③ DHCP (Dynamic Host configuration protocol)
- It is a ~~Dynamic~~ network management protocol wed to dynamic assign an Ip address to any device, or node, on a network. so they can communicate wing Ip.

• DHCP does following:
- It manages provision of all the nodes or devices added or dropped from network.
- It maintains unique Ip address of host using a DHCP server.
- It send request to DHCP server whenever a client which is to be works DNCP

connected to network.
- The server acknowledges by providing an IP address to the client / node / device.

- How DHCP works:
- It works on application layer of TCP/IP model. To dyamically assign IP address to DHCP client and allocated TCP / IP configuration information. to DHCP client.
- It is based on client server protocol in which server manages pull of unique IP addresses. and assign. addresses out of thos address pools.

- DHCP lease process works as follows:
- Client must be connected to internet.
- DHCP clients request for IP address.
- DHCP server responds to the client by providing IP server address.
- while refreshing an assignment, client requesting same parameter, but server may assign a new IP address.

- Components of DHCP:
i) DHCP server
ii) DHCP client
iii) subnet mask
iv) IP address pool
v) DNCP Relay
vi) lease.

Date
Page No.

- Benifits of DHCP :

i) Centralized administration of IP configuration.
ii) Dynamic host configuration
iii) seamless IP host configuration.
iv) Flexibility and scalability.

(4) NAT (Network address translation)

→ It is a process to assigng unique public IP address to represent an entire grop of computer.
- In NAT router assign public address to one or more device connected through private network.
- object of NAT is to reduce NAT is to reduce no. of public IP. addresses in use per security reason.

- How does it works ?
- Request term at the port and NAT directed to the proper location without this closing the destination private IP address.
- It translate the privat IP of maching into a unique IP address to allow communication of local network in the internet.

Q. 6 a) Describe the process of DHCP server configuration.

→ To configure a DHCP (Dynamic Host configuration Protocol) server, follow these basic steps:

1. Install DHCP server software : If not already installed, add the DHCP server role or install DHCP software on your server (on windows server, use the server manager).
2. Create a New scope : Define a scope (range of IP addresses) that the DHCP server will assign to devices on the network. set the starting and ending IP addresses with in this range.
3. set scope options : Configure additional settings like subnet mask, default gateway, and DNS servers that devices will use when they receive an IP addrss.
4. Activate the scope : Enable or activate the scope so the DHCP server starts assigning IP addresses to devices automatically.

L&W

5. test the configuration: Connect a device to the network and confirm it receives an IP address from the DHCP server within the defined range.

Q. 6 b) Describe the process of installation of TCP/IP protocol suite.

→ To install the TCP/IP protocol suite on a computer, follow these basic steps:

1. open Network settings: In windows, goto "control panel," open "Network and sharing center," then click "change adapter settings."
2. select your connection: Right click your network connection (like wifi and Ethernet) and choose "properties."
3. look for TCP/IP protocols: In the list, look for "Internet protocol version 4" (TCP/IPV4) and "Internet protocol version 6" (TCP/IPv6).
4. Install if Not listed: If TCP/IP is not listed, click on "Install," then select "Protocol" and add TCP/IP.
5. set up TCP/IP: once installed, you can set IP address, subnet mask, and DNS under the TCP/IPV4 or TCP/IP V6 Properties if needed.
6. save changes: click "ok" to save your settings and restart the computer if asked.

Q. 6 c) Different betⁿ IPV4 & IPV6 with respect to following parameters.

→

Parameters.	IPV4	IPV6
i) Address length	32 bits (4 bytes)	128 bits (16 bytes)
ii) Classes	uses address classes (A, B, C, D, E)	No classes, uses hierarchical addressing.
iii) Checksum field	contains a checksum field	No checksum field;
iv) Address Representation	Dotted decimal format (e.g. 192.168.1.1)	Hexadecimal format (e.g. 2001:0db8::1)
v) Security features	security optional, relies on external protocols	security builtin, with IPsec support as standard
vi) Packet Flow Identification	No flow Identification for QoS	Flow label field for faster packet flow & quality of service (QoS)