Unit-1

Data communication :-

Data communication is the process of transferring data from one place to another is called data communication.

Network :-

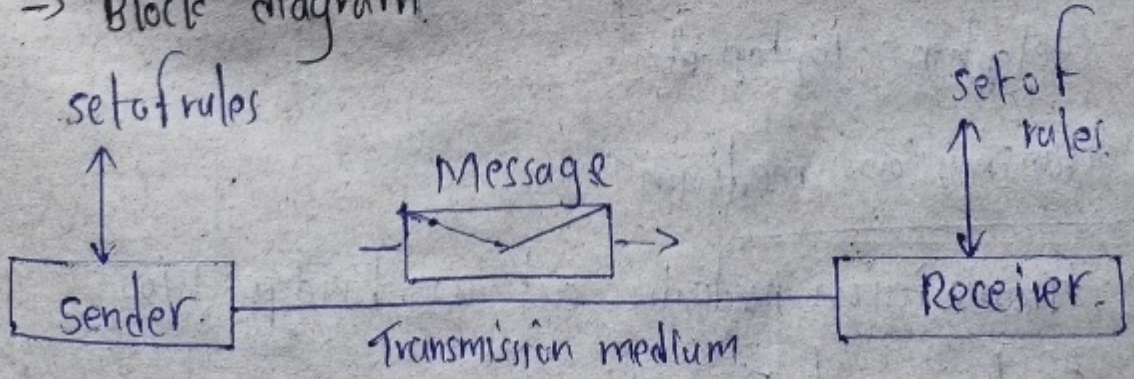
A network is a group of two or more computers or other electronic devices that are interconnected for exchanging data or sharing data is Network.

Data communication components :-

-> There are mainly five components in data communication system.

1. Message 2. sender 3. Receiver.
4. Transmission medium 4. set of rules.

-> Block diagram



1. Message

-> This is the most useful asset of data communication system.
-> message refers to data or information.
-> A message could be in any form such as, audio, video, text etc.

2. Sender:

-> sender sends the message from source to destination.
-> sender plays role of source.
-> It is a simple device may be computer, mobile, telephone, laptop, etc.

3. Receiver:

-> It is a destination, where message comes finally send by sender.
-> It is a device that receives message.
-> It is a device, may be computer, mobile, telephone, laptop etc.

4. Transmission medium:

-> Transmission medium act as bridge b/w sender and Receiver.
-> It is a physical path, message travells from sender to receiver.
-> Transmission medium could be guided or unguided.

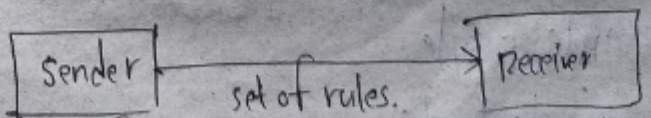
5. set of rules

-> set of rules defined as protocals.
-> protocol is a set of rules that governs data communication.
-> set of rules are necessary for data communication.

* protocols

-> protocol is a set of rules that governs data communication.

Def: protocol is a "set of rules" which is used in digital communication to connect network devices and exchange information b/w them.



Types of protocols

1. TCP/IP, 2. HTTP, 3. SMTP, 4. POP, 5. IMAP, 6. UDP, 7. PPP, 8. FTP. etc.

-> key elements of protocol
  a. syntax.
  b. semantics.
  c. timing.

Standards

Def: standards are the set of rules for data communication.

-> standards are needed for data exchanging.

-> standart organizations - ISO, IEEE, ANSI etc.

-> Types of standards

1. De-facto standards

-> The meaning of DeFacto is "Fact on By convention".

-> These are standards but not approved by any organizations.

-> Established by manfacturers.

Ex: Apple, google.

2. De-jure standard:

-> The meaning of the word is De-jure is "By law".

-> These are standards that have been approved by organizations like, ISO, IEE, ANSI etc.

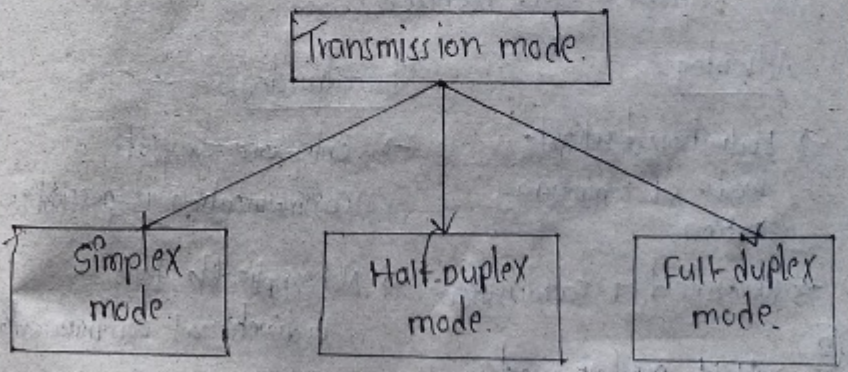
-> Ex: i SMTP
  ii UDP.

Transmission modes

Def: Transmission mode means transferring data b/w two devices. is called Transmission mode.

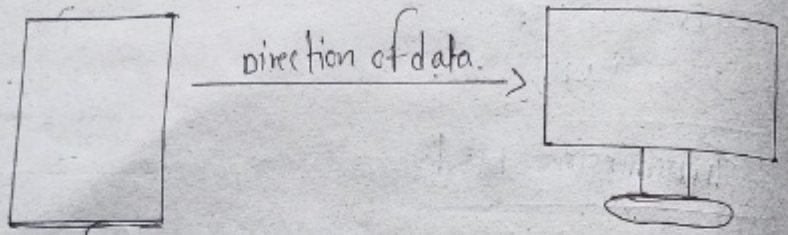
-> It is also called as communication mode.

Types of Transmission modes:



① Simplex mode

-> Block diagram.



-> In simplex mode, the communication is unidirectional.
-> only one way of communication
-> only one of two devices can transmit and other can receive only.

Ex: keyboard and moniter.

Advantages

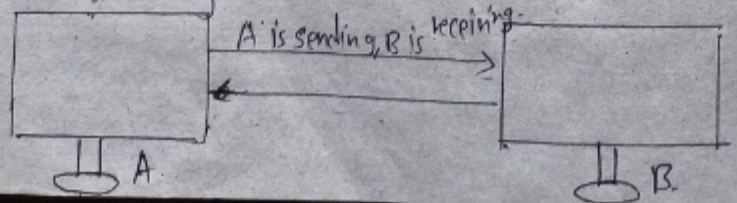
-> Earliest and reliable mode of communication.
-> No need of coordination

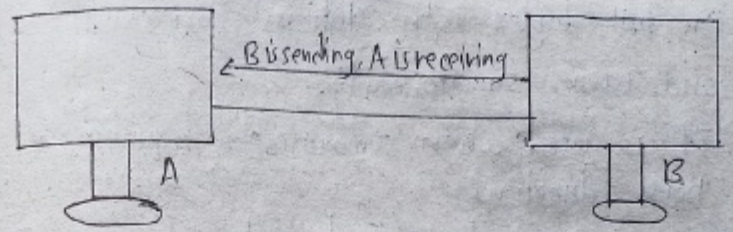
Disadvantages

-> only one way of communication is possible.
-> Not applicable for bidirectional communication

② Half-duplex mode

-> Block diagram.





-> In half-duplex mode, the communication is bi-directional but not at same time
-> when one device is sending, the other can only receive and vice versa.
-> It is used when there is no need of communication in both directions at same time.

Ex: Walkie-Talkie.

Advantages

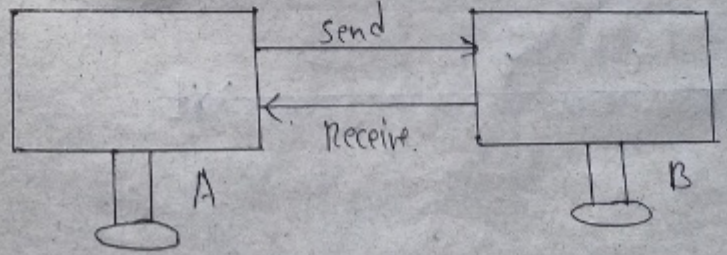
-> Bidirectional communication.
-> less expensive

Disadvantages

-> less reliable.
-> Delay occur.

③ Full duplex mode:

-> Block diagram.



-> In full duplex both stations can send and receive simultaneously.
-> It is used when communication required in both directions.
-> Full-duplex mode is fast mode of communication

Advantages

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

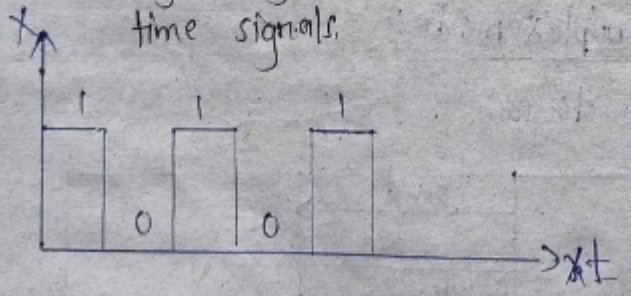
Disadvantages

-> Expensive
-> complex.

* Digital signals

Def: digital signal is a type of signal that represents the data at discrete instants of time is called digital signal.

-> Digital signals are also called discrete time signals.

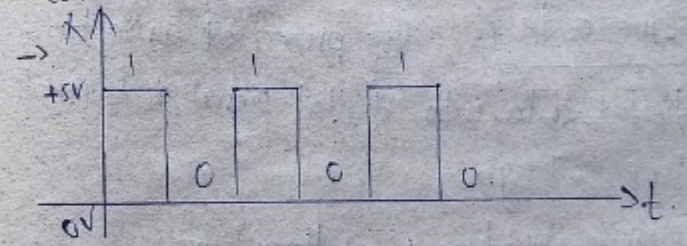


-> Types of digital signals

-> digital signals are classified into two types namely.

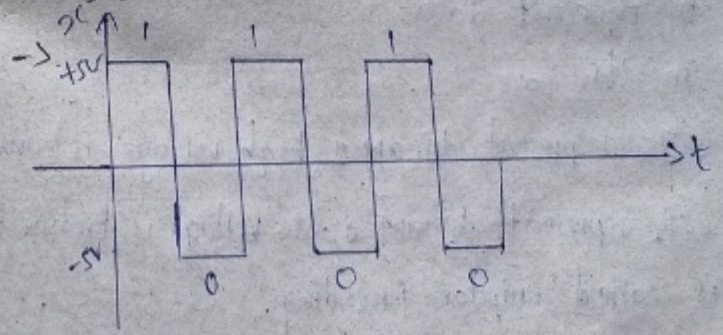
(1) unipolar digital signal:

-> It is a type of digital signal, in which binary states 0 and 1 are used to positive voltage level (or) negative voltage level called UDS.



(2) Bipolar digital signal:

-> It is a type of digital signal in which binary states 0 and 1 are used to +ve voltage level (or) -ve voltage level is called BOS.



* Digital to digital Encoding

-> Def: Digital to digital Encoding is the representation of digital information by digital signal.

-> It can be done in two ways they are
1. line encoding.
2. Block coding.

① Line coding: The process of converting digital data into digital signal is called line coding.

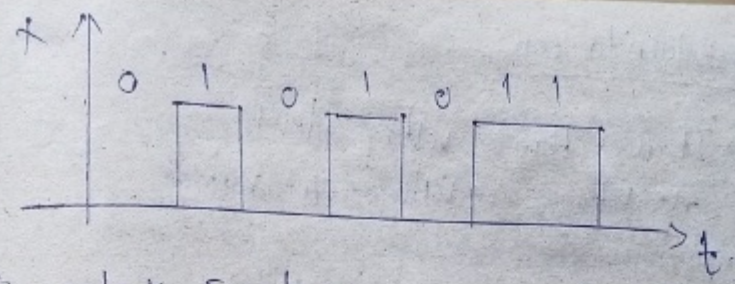
-> Line encoding is of three types
1. unipolar. 2. polar. 3. Bipolar.

1. Unipolar Encoding

-> unipolar encoding uses single voltage level to represent data.

-> In this case,
- To represent binary 1, high voltage is transmitted
- To represent binary 0, No voltage is transmitted

is called unipolar Encoding.



②. polar. Encoding

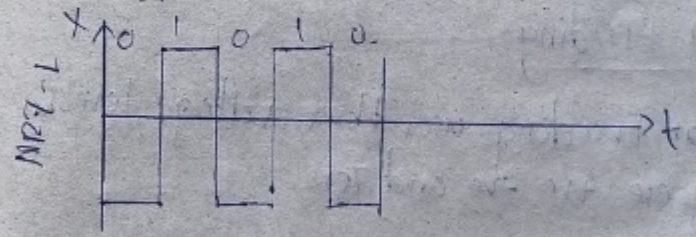
-> polar encoding uses multiple voltage levels to represent binary values. is called polar encoding.

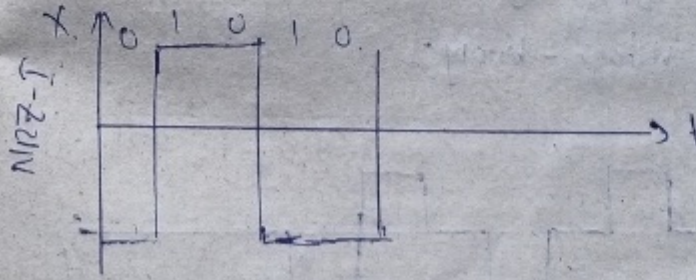
-> polar encoding is of four types

i polar Non-return to zero (NRZ):-

-> It wes two diffrent voltage levels.

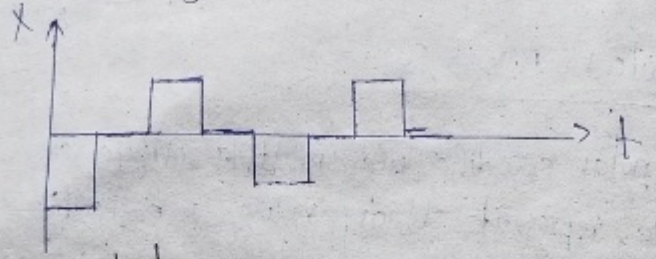
-> It has two variants NRZ-L, NRZ-I.





ii. Return to Zero

-> It uses three voltage levels, +ve voltage, -ve voltage, Zero voltage.



iii. Manchester

-> It is combination of RZ and NRZ-L.

iv. Differential manchester

-> It is combination of RZ and NRZ-I.

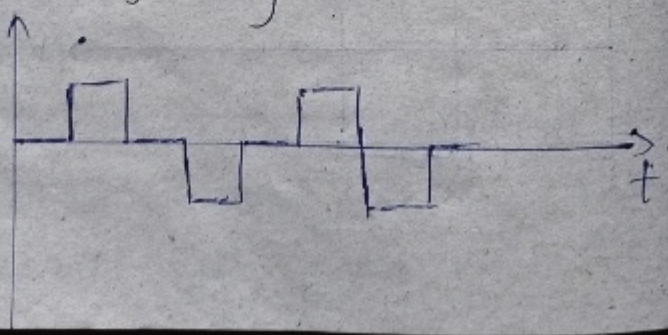
3. Bipolar Encoding

-> Bipolar Encoding uses three voltage levels, they are +ve, -ve, and zero.

Zero voltage - binary '0'

+ve & -ve voltage - binary '1'

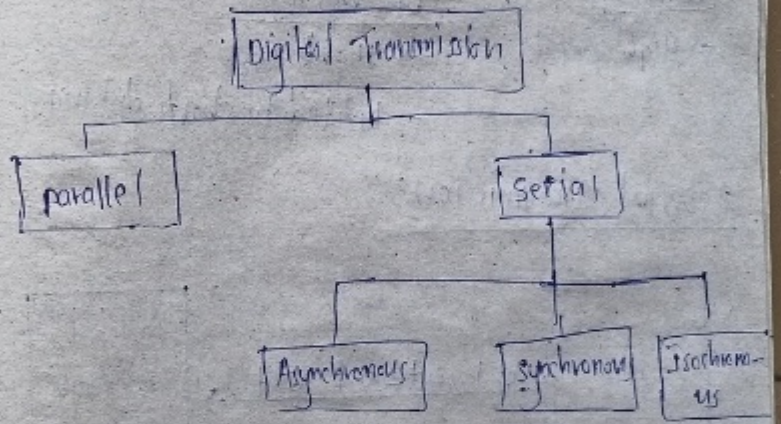
->



Digital data Transmission

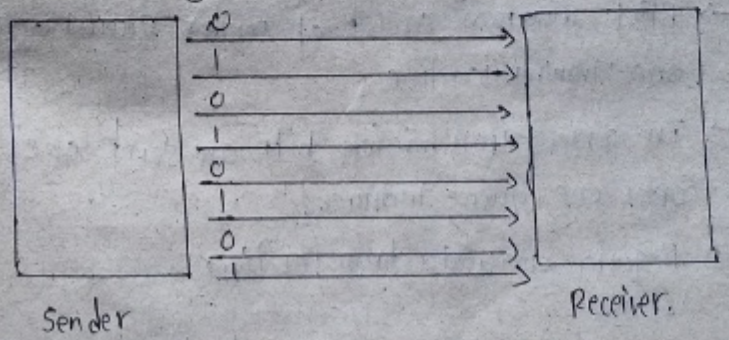
Def: Digital Transmission is the transfer of data from one point to another is called digital data Transmission

-> digital Transmission is called as digital communication.



parallel Transmission

-> Block diagram

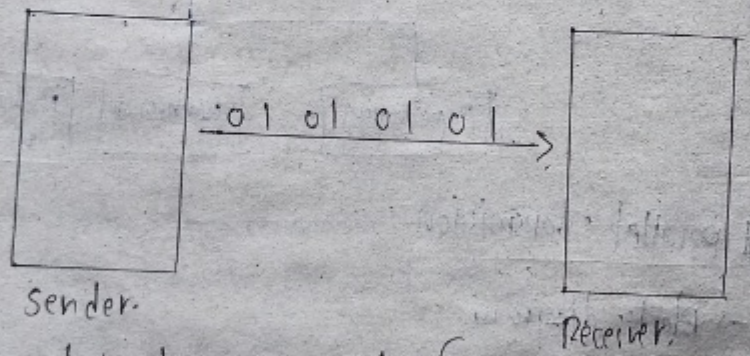


-> Block diagram consist of sender and Receiver with 8 transfer lines.
-> multiple bits are sent at a time.
-> To transfer 8-bits 8- seperate transfer lines are required.
-> 8-bits are sent together.

Advantage
-> High speed.

Disadvantage
-> High cost.
-> limited to short distances.

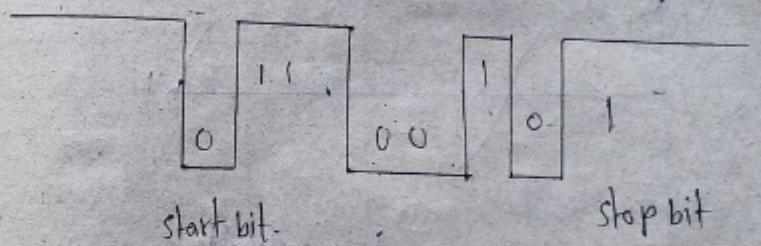
2. Serial Transmission:



-> Block diagram consist of sender, Receiver and one Transmission line.
-> In series Transmission bits are sent one after one (queue manner).
-> Requires one data transfer line.

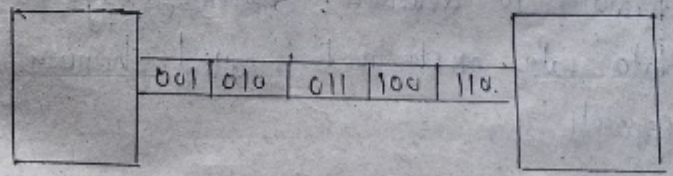
(i) Asychronous serial Transmission

-> Asynchronous serial Transmission is in which the signals are not synchronized to each other.
-> It works on start and stop bits.



(ii) Asynchronous serial Transmission:

-> synchronous serial Transmission is a serial Transmission protocol, in which data sent in continuous manner is called SST.



(iii) Isochronous:

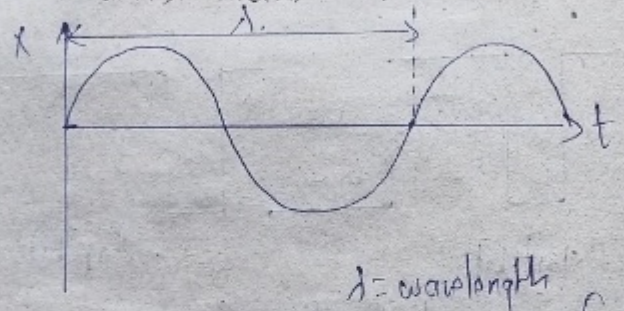
-> An Isochronous serial Transmission is a combination of Asynchronous and synchrous Transmission.

* wavelength

Def: wavelength is a measure of distance. A signal can travel in a period.

-> It is the distance b/w corresponding points.

-> units = meter, centimeters.



λ = wavelength

-> wavelength depends on medium & frequency.

* Shannon capacity:

-> In 1944, Claude shannon introduced formula to determine theoritical highest data rate of channel is called shannon capacity.

$$C = B \log_2 \left(1 + \frac{S}{N}\right)$$

C = shannon capacity

B = Bandwidth

S/N = signal to noise ratio.

* Review of Error detection and Error correction codes

-> Error detection & Error coriection codes plays an important role in transfer of data from sender to receiver.

Error detection: This codes are used for detecting errors in the received data bit-stream.

-> Error detection code encodes message before sending it over noisy channels.

-> Error detection code, detects the errors in message.

-> Error detection techniques
- i parity code
- ii checksum,
- iii CRC

(i) parity code: In parity code, we add one parity bit to right of LSB or left of MSB to bitstream.

-> parity is of two types.

- Even parity
- odd parity.

o Even parity code

Binary code	Even parity bit	Even parity code
000	0	0000
001	1	0011
010	1	0101
011	0	0110
100	1	1001
101	0	1010
110	0	1100
111	1	1111

o odd parity code

odd parity	odd parity bit	odd parity code
000	1	0001
001	0	0010
010	0	0100
011	1	0111
100	0	1000
101	1	1011
110	1	1101
111	0	1110

Error correction code

-> Error correction codes are generated by using specific algorithm used for removing (or) correcting errors from message is called Error correction code.

(i) Block codes

-> In block codes, in fixed blocks of bits, the message is contained.

-> Redundant bits are added for correcting errors

(ii) convolution codes

-> It is a type of error correcting code that generates parity symbol.

-> symbols are encoded in serial form.

* Networks

A Network is a group of two or more computers or other electric devices inter-connected to exchange information is called Network.

-> classification of Networks

1. LAN.
2. MAN.
3. WAN.

* Comparision of Networks

LAN	MAN	WAN
-> stands for local Area Network	-> stands for metropolitan Area Network.	-> stands for wide Area Network.
-> It is a network, that connects group of computers in a small Area.	-> It is a network, that connects group of computer in large areas (Towns)	-> It is a network, that connects group of computers, over countries.
-> ownership is private.	-> owner is private or) public	-> private or) public
-> Easy to design.	-> difficult	-> difficult.
-> speed is high.	-> moderate	-> low.
-> High Tolerant.	-> less	-> less
-> less congestion.	-> more	-> more
-> used for college, school etc.	-> For small towns, city etc	-> For. countries

* protocols :

-> A protocol is synonymous with rule.
-> It consist of communication.
-> protocol determines, what is communicated, how and when it's communicated
-> key elements of protocol

a. Syntax
-> structure of the data
-> field delineation

a. Semantics
-> Interpret the meaning of bits.

a. Timing
-> when and what data should be sended

* standards

-> A standard is a formalized protocol accepted by most of the parties that implement it.
-> Not all protocols are standards.
-> And Not all standards are protocols.

-> standards are mainly used to provide guidelines to manfacturers, vendors etc.

-> standards are two types.

① de-facto:

-> de-facto means "by fact".

-> The de-facto are standards that have not been approved by any organization.

-> It is widely used.

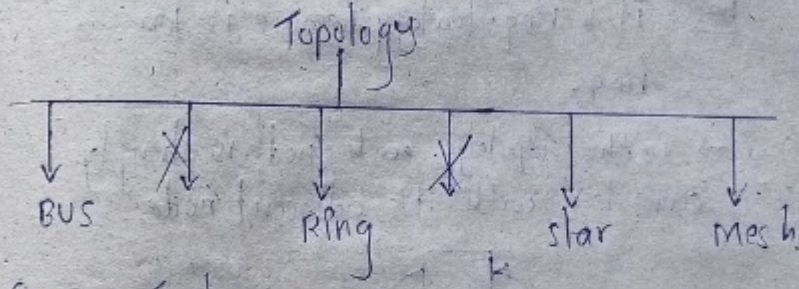
② de-jure:

-> de-jure means "by law".

-> The-jure is a standard that have been approved by organisation.

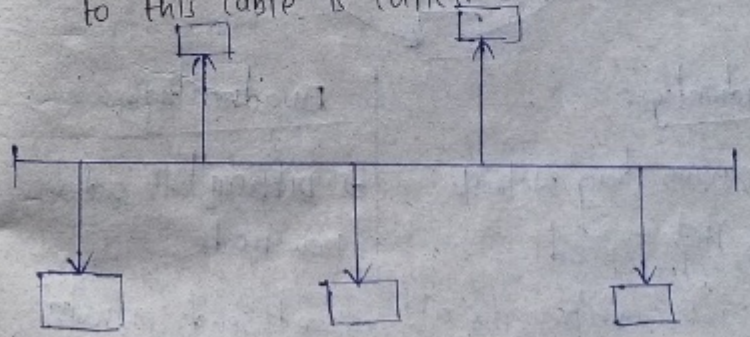
* Topology

Def: It is defined as physical arrangement of the computers/node, which is connected to each other via communication medium is called Topology.



① Bus Topology

-> In bus Topology, one long communication channel & all the devices are connected to this cable is called B.T.



Advantages

-> Easy to add & remove nodes in network.

-> Required only cable.

-> less expensive.

-> Easy to maintain

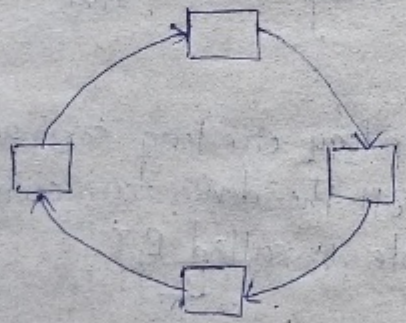
Disadvantage

-> If cable is failed, then entire network will fail.
-> The length of cable is limited.

2. Ring Topology

Def: It is ring topology, because it forms a ring.

-> In this topology each node is strongly connected with it's adjacent node.



Advantages

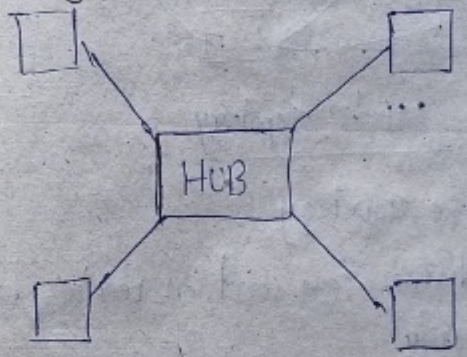
-> Forms strong network
-> High speed
-> Interconnection b/w all nodes.

Disadvantages

-> Difficult to add new node.
-> can't send private messages.

3. STAR Topology

-> In star topology all nodes are connected with central device called HUB.
-> sharing of data possible through HUB.



Advantages

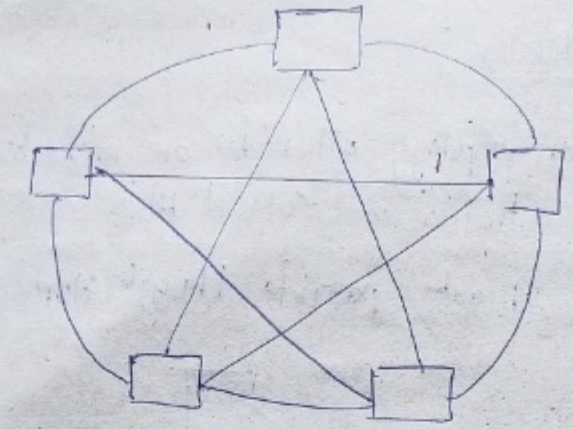
-> less expensive.
-> Easy to connect new nodes.

Disadvantages

-> We can't sent private data.
-> If HUB fails, entire network will fails.

4. MESh Topology

-> In this topology each and every computer is directly connected to each other.



Mesh Topology

Advantages

-> good & safe Topology.

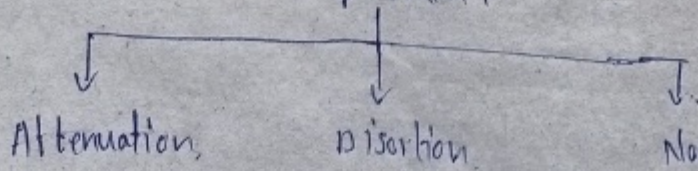
-> multiple devices can sent or receive data simultaneously.

Disadvantages

-> Difficult to add new node.

* Transmission Impairment

-> It is defined as signal quality is compromised due to imperfection in the medium. is called Transmission impairment.



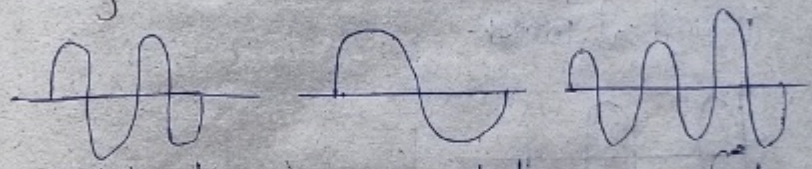
Attenuation:

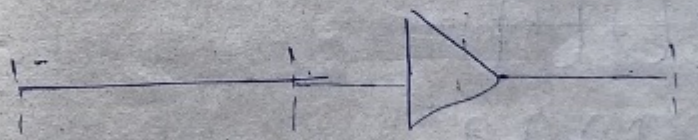
-> Attenuation means of loss of energy.

-> The strength of signal decreases with increasing distance, this cause loss of energy.

-> This signal is called attenuated signal.

-> Amplifiers are used to amplify attenuated signal.





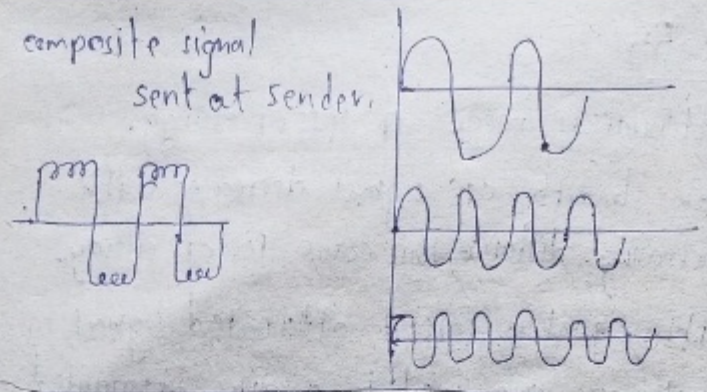
Attenuation(dB) = $10\log_{10}(P_2/P_1)$

Attenuation(dB) = $20\log\log(V_2/V_1)$

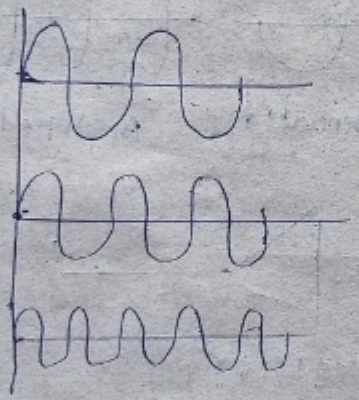
Distortion:

-> Distortion means change in the form of signal

composite signal
sent at sender.

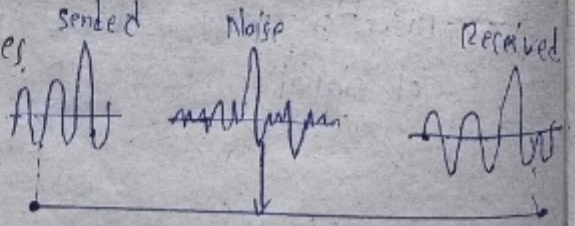


composite signal
Received at receiver.



③ Noise: The random or unwanted signal that mix up with the original signal is called Noise.

-> Types of Noises



- o. Induced Noise
- o. Crosstalk Noise
- o. Thermal Noise
- o. Impulse Noise

Transmission performance:

-> The performance of Transmission medium can be measured with

- o. Throughput
- o. propagation speed
- o propagation time

o. Throughput: It is the measure of how many bits pass through a point in one second is called Throughput.

o. propagation speed

-> The distance a signal travells through a transmission medium is called P.S.

o. propagation Time:

-> The time required for a signal to travel from one point to another is called P.T.

* DTE-DCE Interface :-

i Data Terminal equipment (DTE)

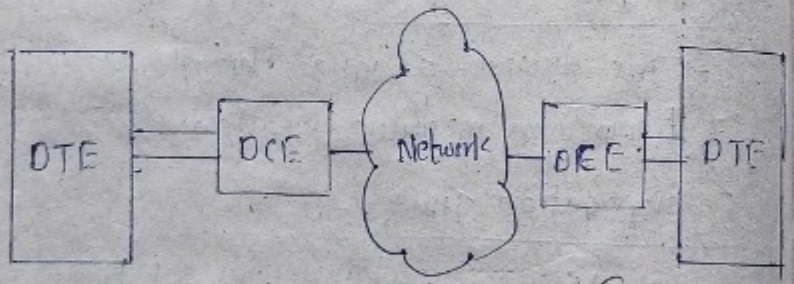
-> DTE stands for Data terminal Equipment.

-> The function of DTE is either source or destination.

-> Examples of DTE includes computers, printers etc.

-> DTEs do not communicate directly each other, they require, intermediate as DCE.

-> Block diagram.



-> Block diagram shows working of DTE, by using DCEs.

-> DTE generates data and pass that to DCE.

-> DCE converts signal to a format and passes to Network.

-> when signal arrives at the end, this process reversed.

ii Data circuit-Terminating Equipment (DCE)

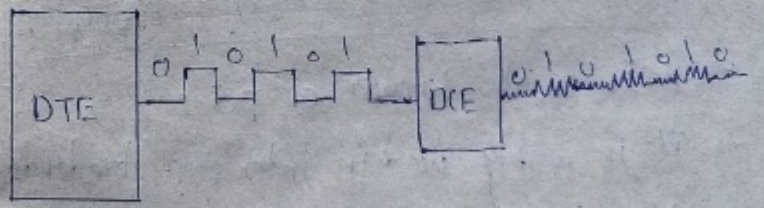
-> DCE - stands for data circuit-Terminating Equipment.

-> ~~DCE is a~~ The function of DCE is either source or destination.

-> DCE takes signal sent by DTE and converts that into appropriate signal.

-> This appropriate signal DCE sends to Network again network sent to DCE and at last DTE receives the signal.

-> Block diagram.



* DTE- DCE standards

-> Interface standards play a crucial role in various domain & seamless communication.

-> key contexts in.

1. Telecommunication interface standards

~~-> In the realm of telecommunications,~~

-> In telecommunications, an interface standard is a standard that describle one or more functional concepts.

-> Functional concepts - code conversion, line assignments, etc.

-> physical concepts - Electrical, mechanical etc

2. peripheral component interface Express (PCIe) :-

-> PCIe is also known as PCI-e.

-> It is widely used in interface standards.

-> It have high speed data transfer.

-> key features

o. High speed.

o. various configurations.

* Modems :-

-> Modem stands for modulator/demodulator.

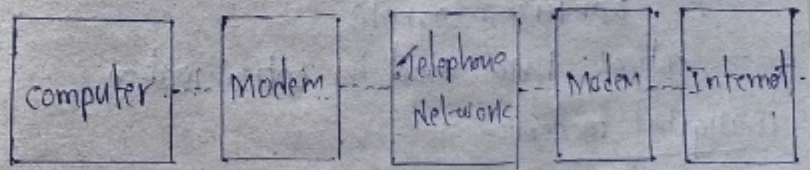
-> The modem is defined as "The device used to connect the network with Internet is called modem.

-> The function of modem is converting analog signal into digital signal.

-> Modem can perform modulation and demodulation processes.

working of modem

-> Block diagram



-> Block diagram shows working of modem.

step 1 : data generation :

-> The computer system generates data which is in digital form.

step 2 : Modulation :

-> modulation means converting digital data into analog data.

step3 Transmission

-> The modulated analog data transmitted through transmission line.

step4 - Demodulation

-> Demodulation means converting di-analog data in digital data.

step5 Decoding

-> Demodulated data, decodes by the computer for further use.

Types of modems

i optical modem

-> In optical modem optical cables are used to transfering signals.

-> optical fibre used in optical modem.

ii Digital modem

-> digital modem is used to converting digital data into digital signals.

iii cable modem

-> cable modem used to establish high speed communication b/w computer & Internet.

Advantages

-> connects LAN to internet.

-> performs both modulation & Demodulation.

Disadvantages

-> High cost.

-> just interface b/w LAN & Internet.

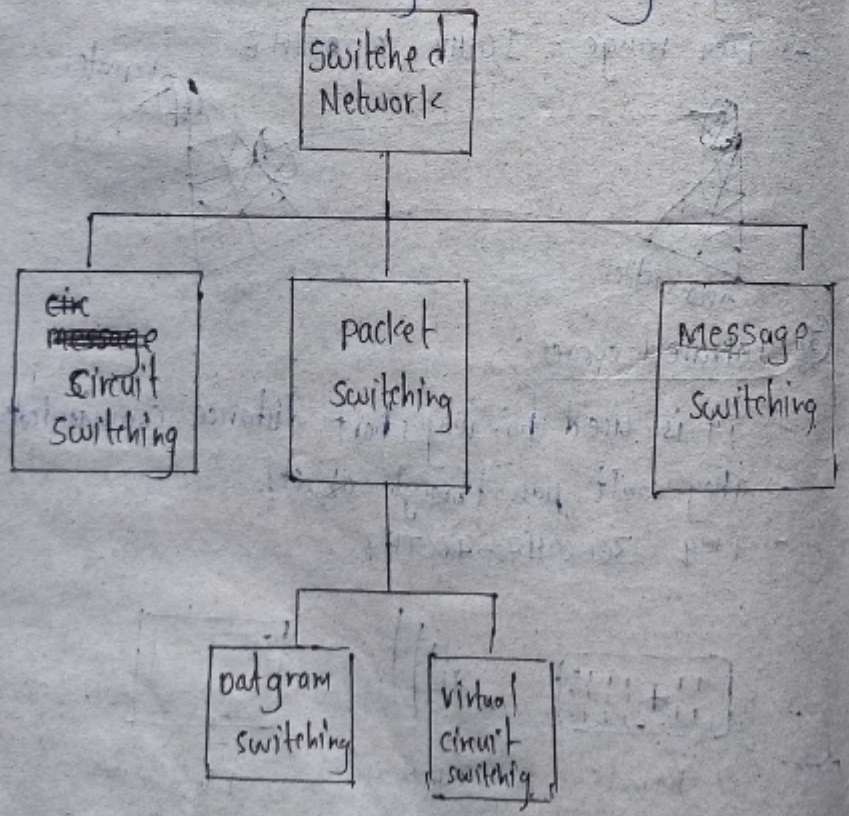
* Switching Networks

Switching :- In computer networking, switching is the process of transferring data packets from one ~~place~~ device to another device is called switching

-> The specific devices used for switching is called Switches

-> Types of switching

-> There are three types of switching networks



1. Circuit switching

-> In this type of switching, a connection is established between the source and destination beforehand.

-> circuit switching is better than message switching.

-> Example Telephone network

-> It is designed for voice applications

2. Message Switching

-> Message switching is an older switching technique.

-> In message switching, the entire data block(or) message is passes through entire network

-> It is high inefficient

③. packet switching

~~This~~ packet switching requires the data to be broken into small packets.

-> These data packets transferred to their destinations at particular time.

-> This switching is used in modern computers

-> It is of two types.

i Data gram switching

-> In data gram switching each data packet is taken as individual entity..

-> Here no connection, before transmitting data.

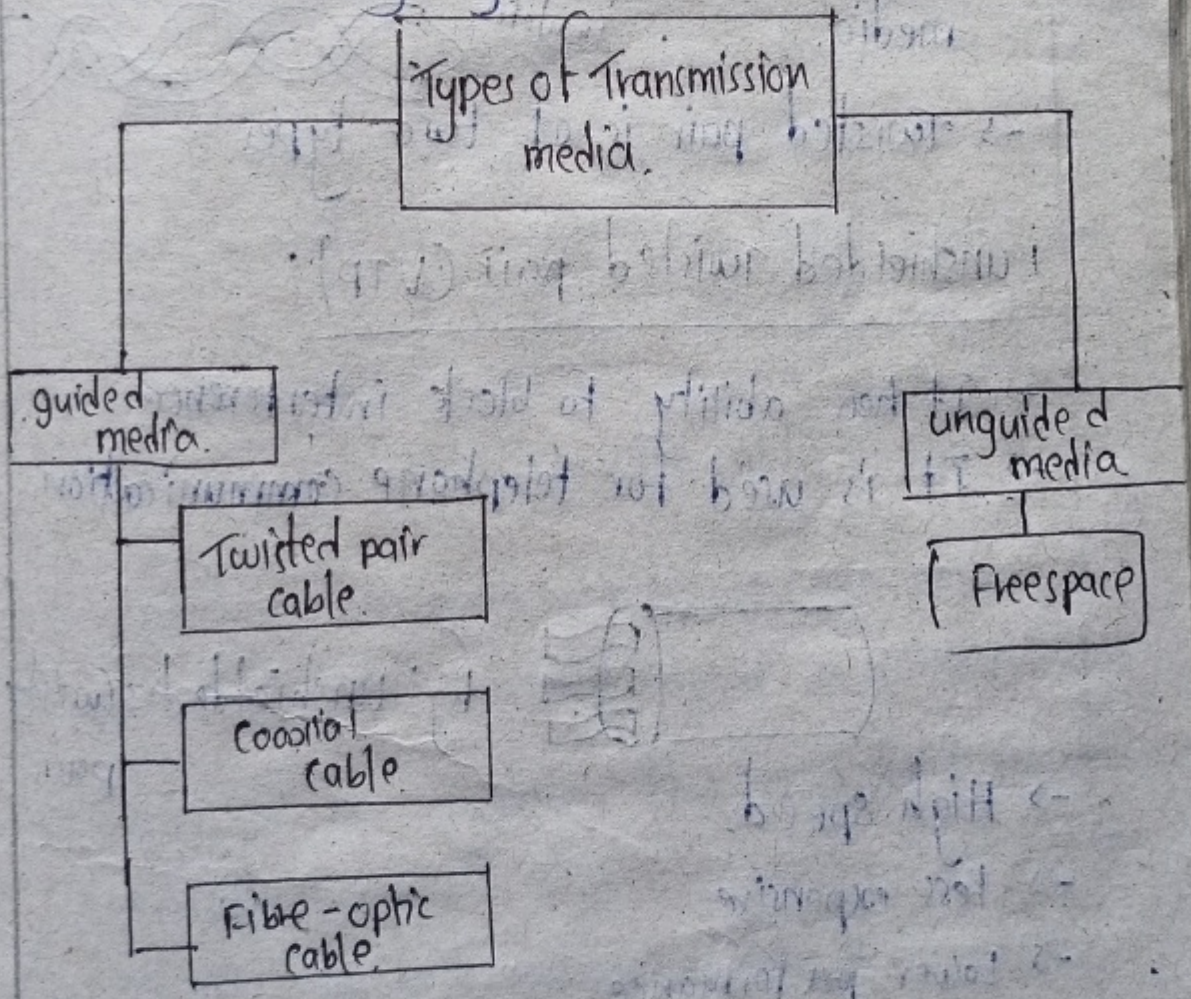
ii virtual circuit switching

-> In this switching, there is a connection b/w source and destination before transmitting data.

* Transmission media guided and unguided

Transmission medium: In data communication network, transmission medium is a physical path between the transmitter and receiver. is called

-> Transmission medium broadly classified into the following types.



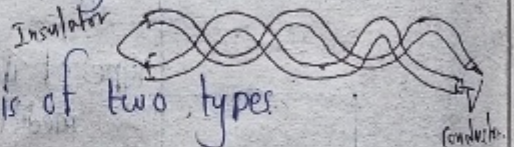
1. Guided media: It is also referred as wired or) Bounded transmisson media.

-> Signals being transmitted in a narrow path by using physical links

-> High speed
-> used for short distances

1. Twisted pair cable :

-> It consists of two seperately insulated conductor wires wound about each other.
-> They are most widely used in Transmission media.



-> Twisted pair is of two types

i unshielded Twisted pair (UTP):

-> It has ability to block interference
-> It is used for telephone communication.

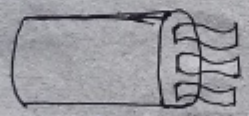


fig: unshielded Twisted pair

-> High speed.
-> less expensive
-> Lower performance

ii sheilded Twisted pair (STP)

-> This type of cable consist of special Jacet.
-> It is used for telephone communication.

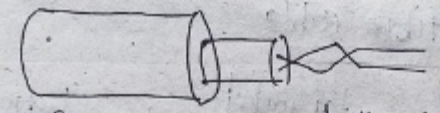


fig: sheilded Twisted pair

-> High speed
-> more expensive
-> High performance

2 Coaxial cable

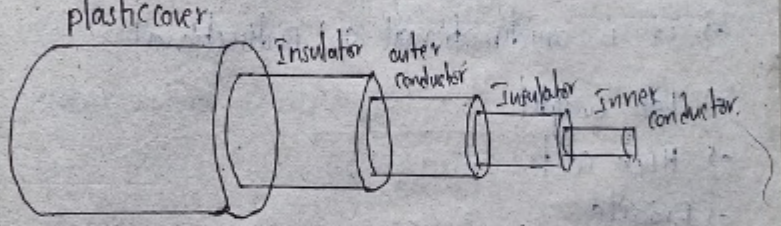
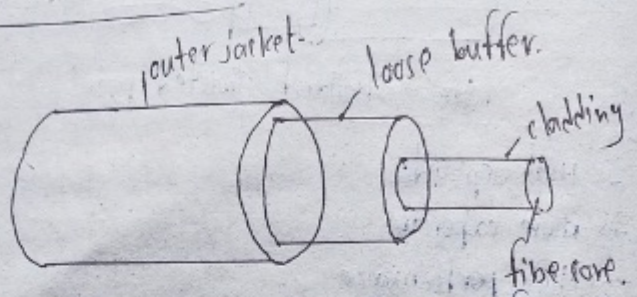


Fig: coaxial cable

-> It has an outer plastic to cover and containing an insulator made of precon Teflon
-> There is an insulator blw outer and inner conductors
-> It can transmit information in two modes
  - Baseband mode
  - Broadband mode
-> less expensive
-> High bandwidth
-> one cable failure disturb entire networks.

③. optical fibre cable



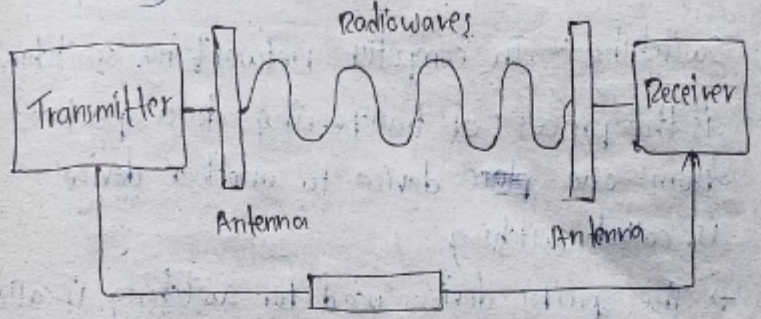
-> It used the concept refraction of light.
-> core is made up of glass (or) plastic
-> It is unidirectional (or) Bidirectional
-> Less weight
-> High cost
-> Fragile

② unguided media

-> It is also referred as wireless (or) unbounded Transmission media.
-> Signals are Transmits through air.
-> used for large distances
-> There are three types of unguided media.

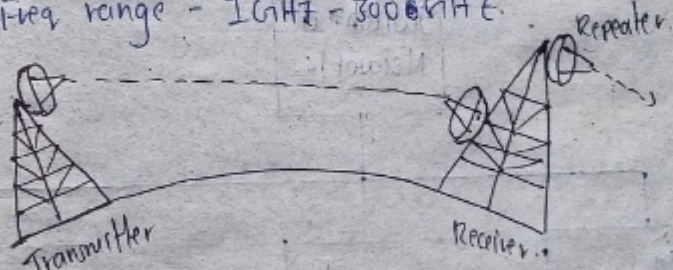
i Radia waves.

-> These are easy to generate and passes through buildings.
-> Frequency range - 3KHZ - 1GHZ



2 Microwaves

-> The sending and receiving antennas needs to be aligned each other.
-> Freq range - 1GHZ - 300GHZ



③ Infrared waves:

-> It is used for very short distance communication
-> They can't pass through objects.
-> Freq 300GHZ - 400THZ

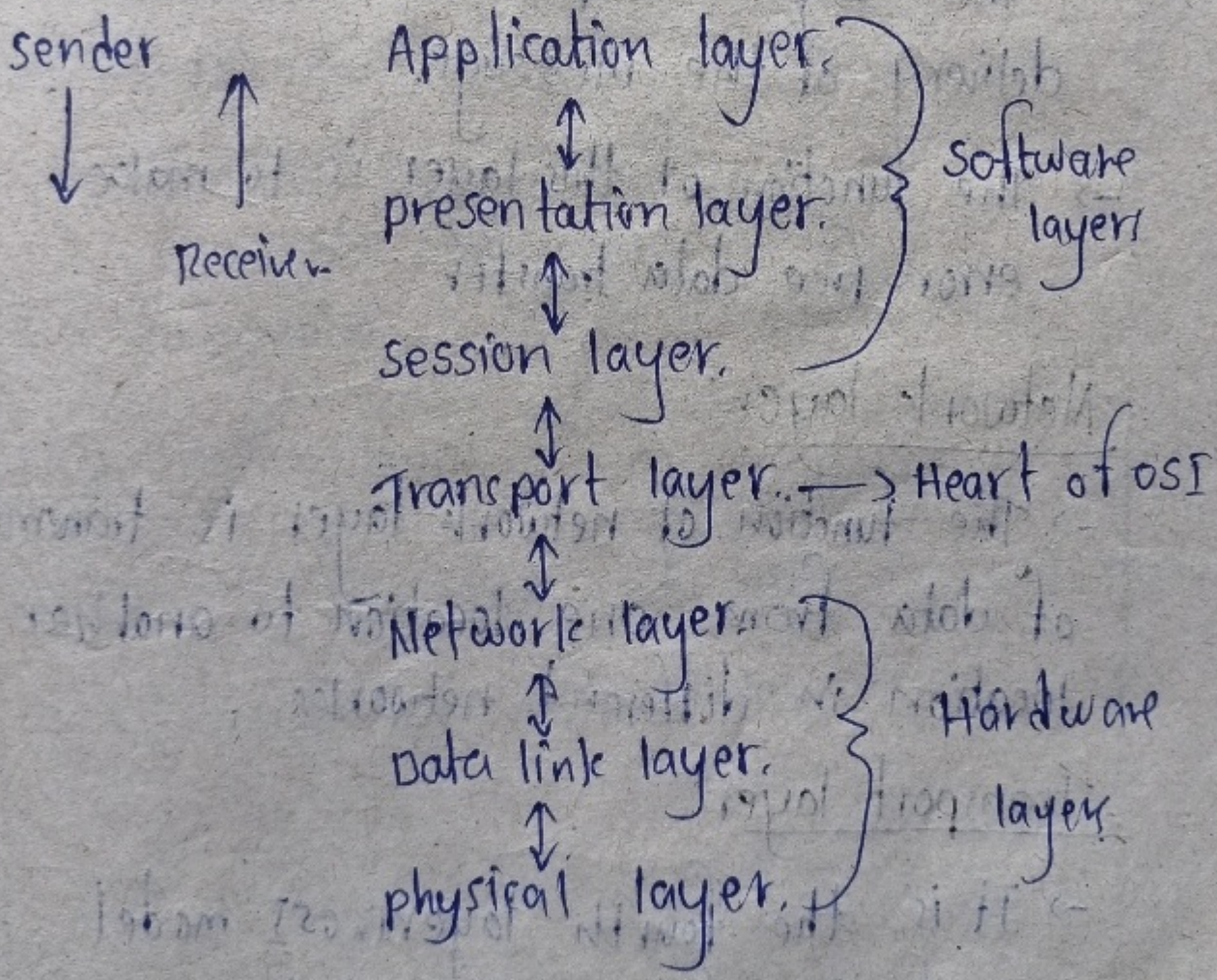
OSI Model :-

-> The word OSI stands for open systems interconnection.

-> It has been developed by ISO- International standardization of organisation in 1974.

-> It is 7 layer architecture, each layer having specific functionality.

Structure of OSI



-> Functionality of each layer.

physical layer:

-> physical layer is the lowest layer of the OSI reference model.
-> It is responsible for physical connection b/w devices.
-> This layer converts receive d signal binarys and send them to data link layer.

Data link layer

-> This layer is responsible for node-to-node delivery of the message.
-> The function of this layer is to make error-free data transfer.

Network layer:

-> The function of network layer is transmission of data from one location to another location in different networks.

Transport layer:

-> It is the fourth layer in OSI model
-> The function of transport layer is, takes services from Application layer and provides to Network layer.
-> It is the heart of OSI.

Session layer:

-> It is the 5th layer in OSI model
-> It is this layer is responsible establishing as well as maintaining a safe and secure connection.

presentation layer:

-> It is the 6th layer in OSI model.
-> It extracts the data from application layer and changes it's format, transmit over network.
-> Functions:
  a. Translation
  b. Encryption / decryption
  c. Compression

Application layer:

-> It is the top most layer in OSI model
-> It works on mail services.

* Types of computer Networks:

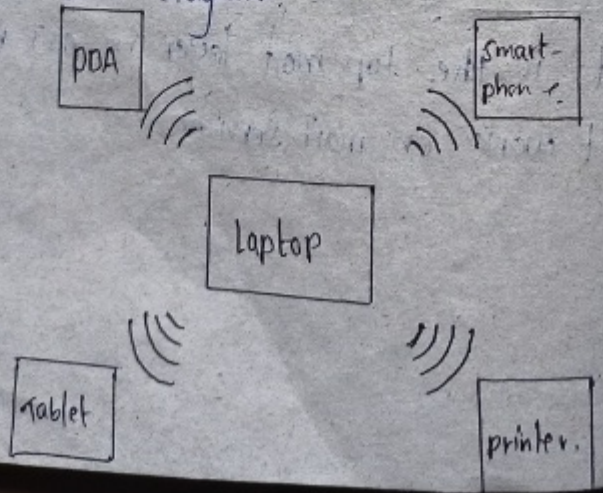
Network: A network consist of two or more computers that are linked to share resources.

-> The computer on Network may be linked through, cables, satellites etc.

Types of Networks

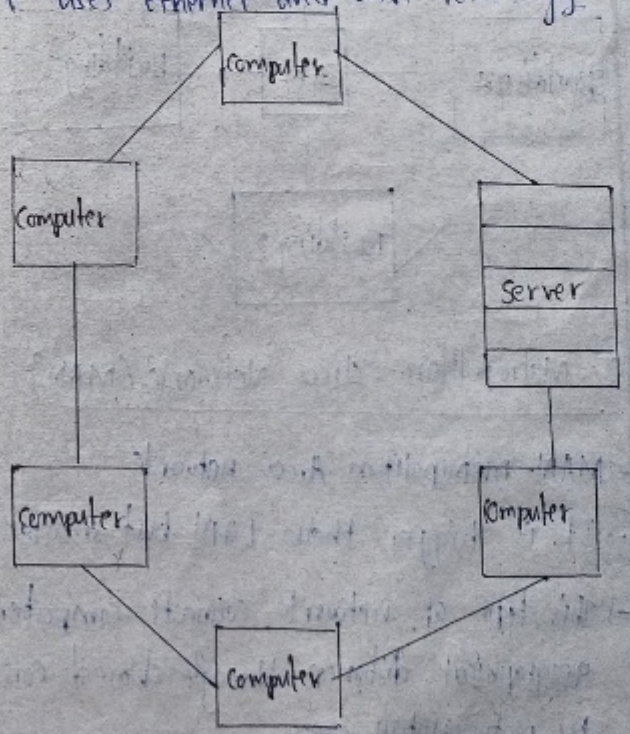
1. personal Area Network (PAN):

-> PAN- personal Area Network.
-> PAN is the most basic type of Network
-> This network is restricted to single person
-> PAN Network range is 1 to 100 meters
-> This uses bluetooth, zigbee technology
-> Block diagram



2. Local Area Network (LAN):

-> LAN- Local Area Network
-> LAN- is most frequently used network
-> LAN is a computer network that connects computer through common path from server.
-> This network doesn't restricted to single person
-> LAN network range is 2KM.
-> It uses ethernet and wifi Technology.



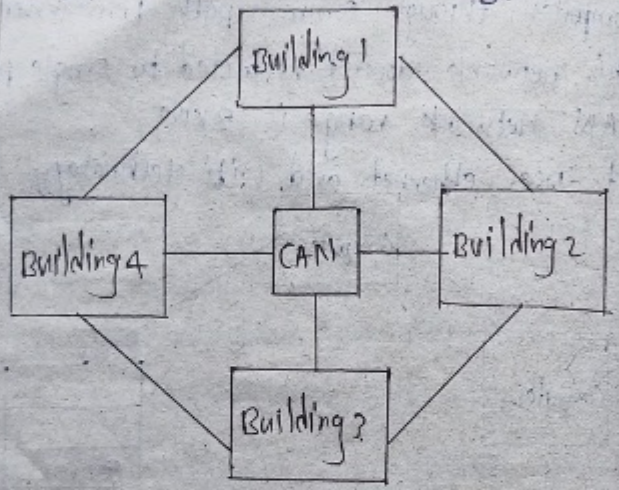
(3). Campus Area Network (CAN):

-> CAN- Campus Area Network
-> CAN is bigger than LAN but smaller than MAN

-> This type of network usually used in schools, colleges etc.

-> This CAN network range is limited area within the buildings and campus.

-> It uses ethernet technology.



④ Metropolitan Area Network (MAN)

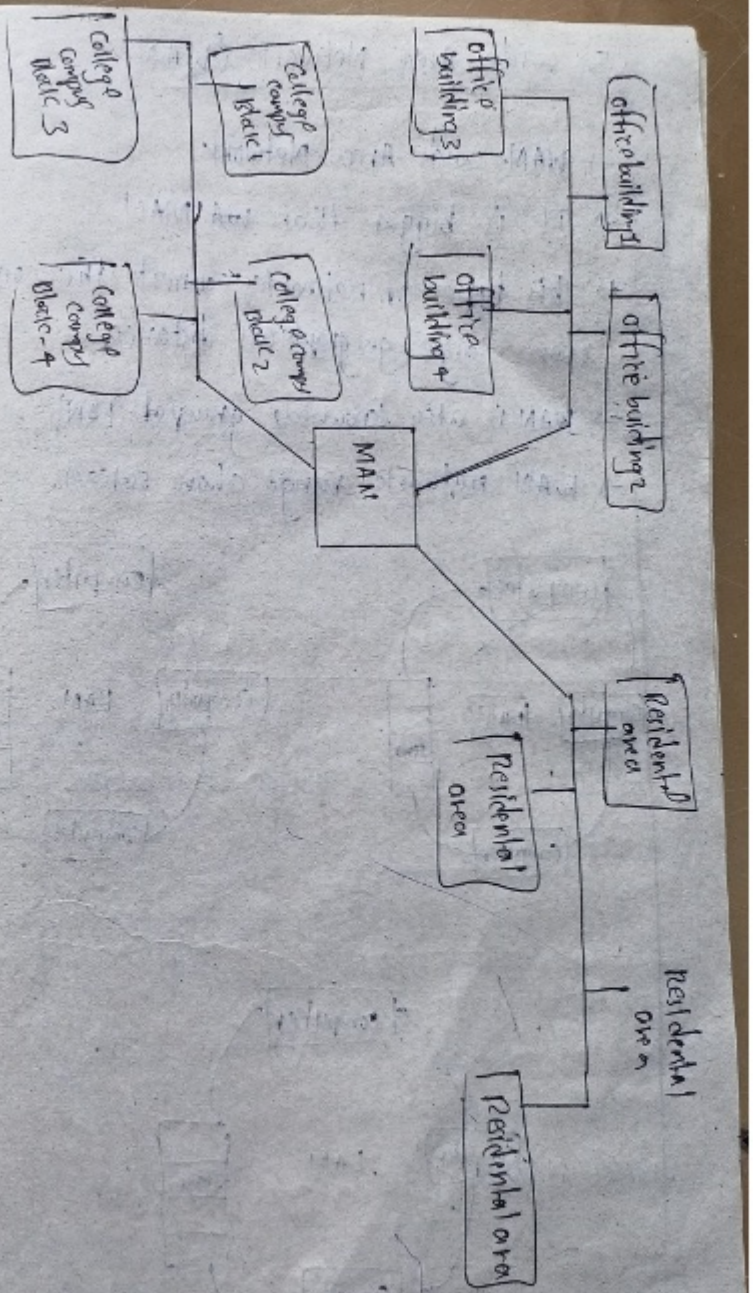
-> MAN - metropolitan Area network.

-> It is bigger than LAN but smaller than WAN.

-> This type of network, connects computer over a geographical distance through shared communication by metropolitan area.

-> MAN network range - 5 - 50 km

-> It uses FDDI, CDDI & ATM Technology



(5). Wide Area Network (WAN)

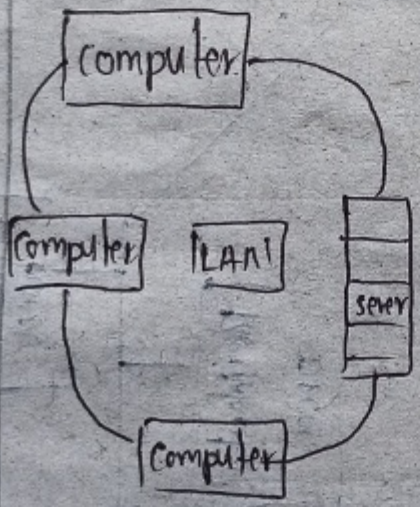
-> WAN- wide Area Network.

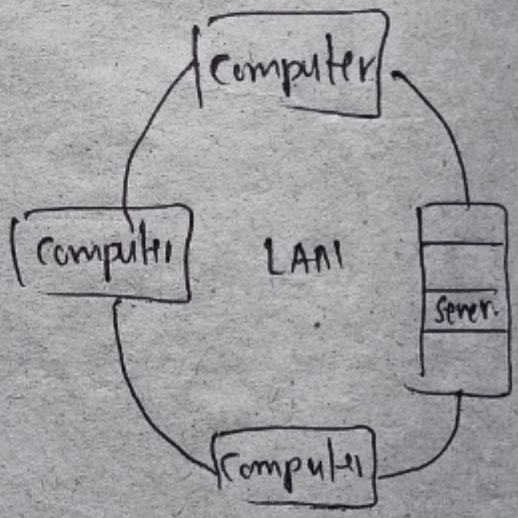
-> It is bigger than WA MAN!

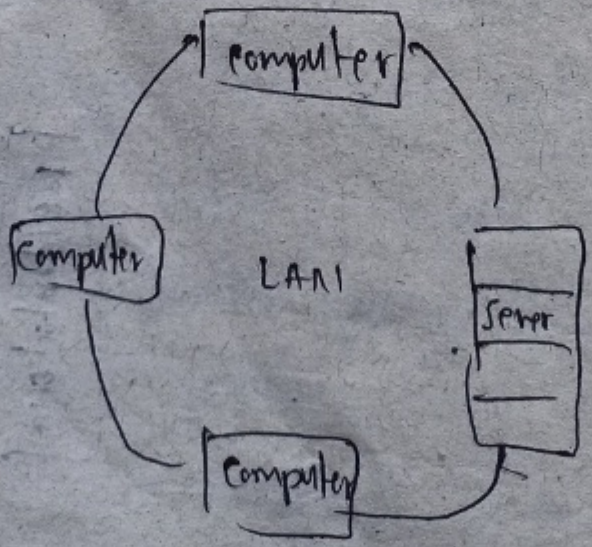
-> This type of network connects the computers over large geographical distance.

-> WAN is also known as group of LAN's

-> WAN network range above 50KM.







Unit-2

Data-link layer:

Def: Data link layer is the second layer after the physical layer.

-> Data link layer is responsible for maintaing the data link b/w two nodes is called data link layer.

-> Data-link layer is divided into two-sub layers

(i) logic link control (LLC) sublayer:

-> provides the logic for the data link.

-> Functions - Error recovery, user addressing, flow control operations.

(ii) Media Access control (MAC) sublayer:

-> It is the second sublayer of data link layer.

-> Functions - control of access, Direction of errors.

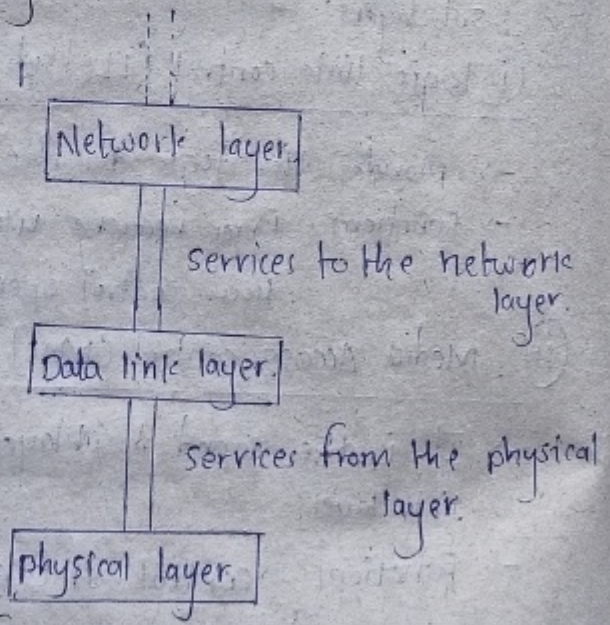
* Design Issues

1. servicer provided to the network layer:

-> The data link layer act as service interface to the network layer.

-> The primary function of this layer is providing a well-defined service interface to ~~na~~ network layer.

-> Block diagram.



-> Types of servicer provided

a. Unacknowledged connectionless service.
a. Acknowledged connectionless service.
a. Acknowledged connection.

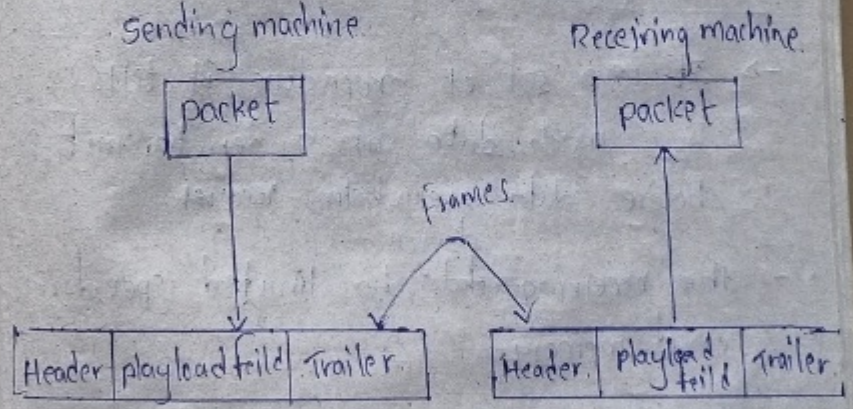
2. Framing

-> The source machine sends a data in the form of blocks called frames

-> Frame has three parts, namely -

a. Frame header.
a. playload feild
a. Trailer

-> Block diagram



(3) Error control:

-> Error control is used to prevent duplication of frames

-> Dealing with transmission errors.

-> Retransmitting lost frames

-> Identifying duplicate frames and deleting them

④ Flow control

-> Flow control is done to prevent the flow of data frame at receiver end.

-> Flow control generally observes proper flow of data from sender to Receiver.

* Data link control and protocols

Flow control

-> It is a set of procedures, it tells how much data can sender transmit before data overwhelms receiver.

-> The receiving device has limited speed and memory.

-> The receiving device informs that stop transmitting data after limit reached.

-> Two methods have been developed to control flow of data.

o. Stop-and-wait.

o. Sliding window.

o Stop-and-wait

-> In stop-and-wait method, the sender waits for acknowledgement, after every frame it sends.

-> when acknowledgment is received, then only next frame is sent.

-> End of transmission frame [EOT]

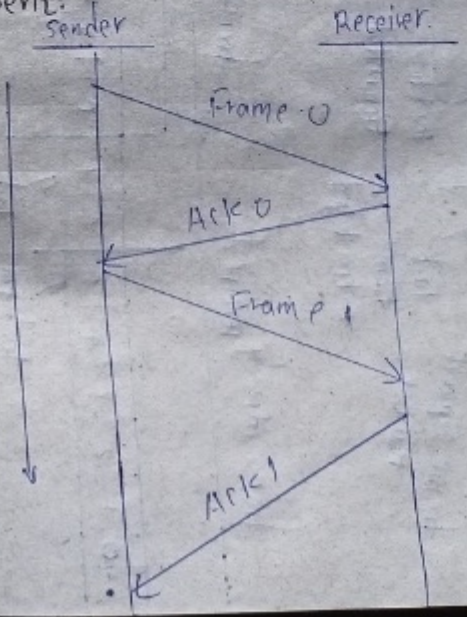
Advantages

-> stop-and-wait method is simple.

-> Each frame checked before next frame sent.

Disadvantages

-> Inefficient.



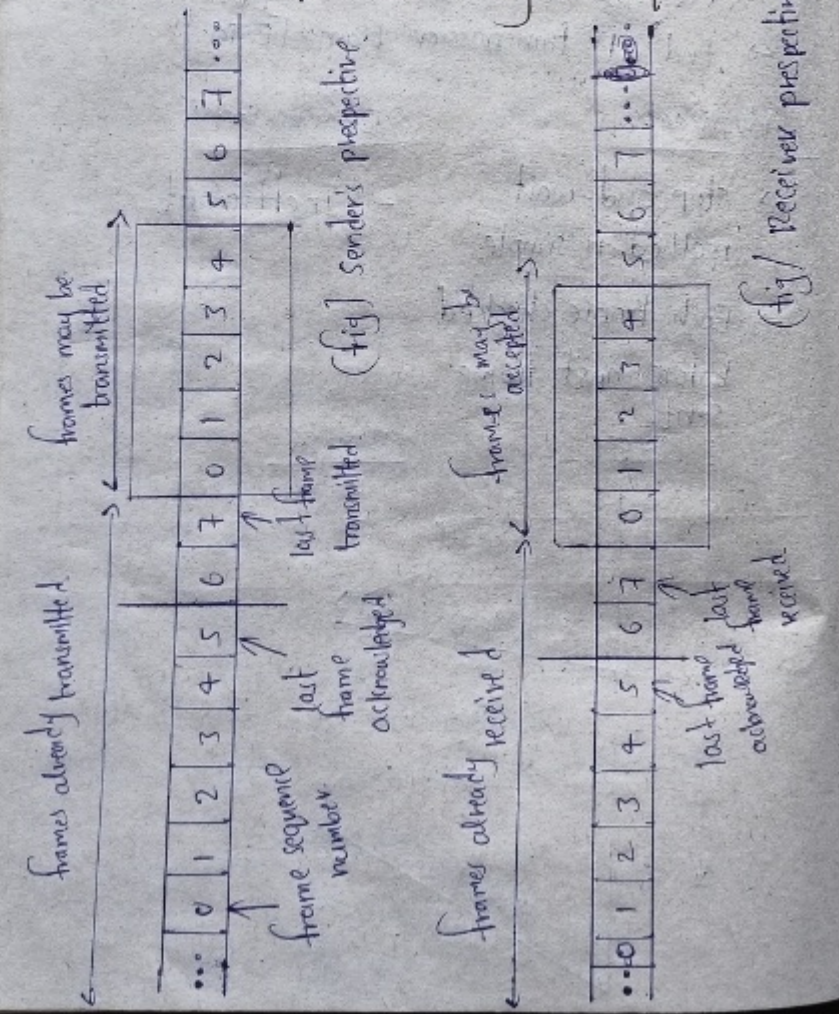
Sliding window:-

-> It is a flow control mechanism.

-> It is also known as windowing.

-> It is a method for controlling sending data packets b/w network devices

-> It is a problem solving technique.



(fig) Sender's prespective (fig) Receiver prespective

-> limitations of stop and wait can be overcomed by sliding window.

Error control

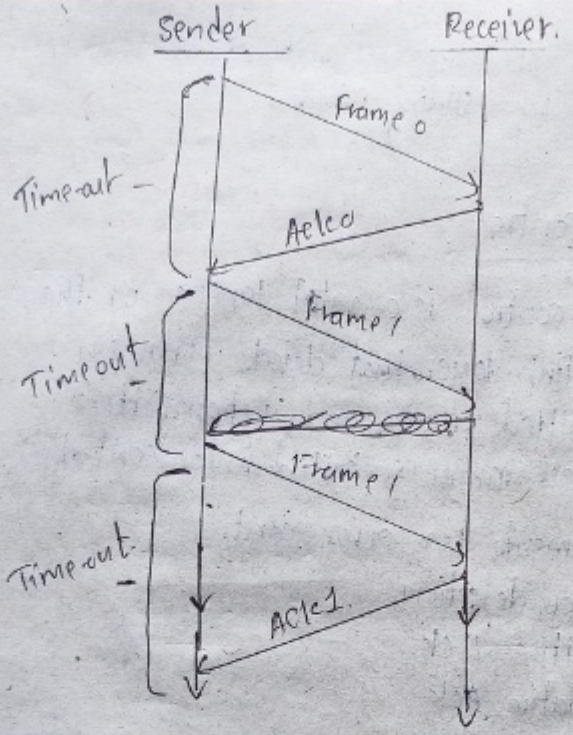
-> Error control is a vital function of the data link layer, that detects error in transmitted frames and retransmitts errorless frames is called Error control.

-> Requirements for error control.
- Error detection.
- positive Ack
- Negative Ack
- Retransmission.

-> In error control three types of techniques are available they are:

1. Stop-and-wait ARQ

-> Stop and wait ARQ block diagram shown in below figure.



-> The above transmission occur in stop-and wait ARQ.

-> The sender maintains a timout counter.

-> when a frame is sent, the sender starts timeout counter.

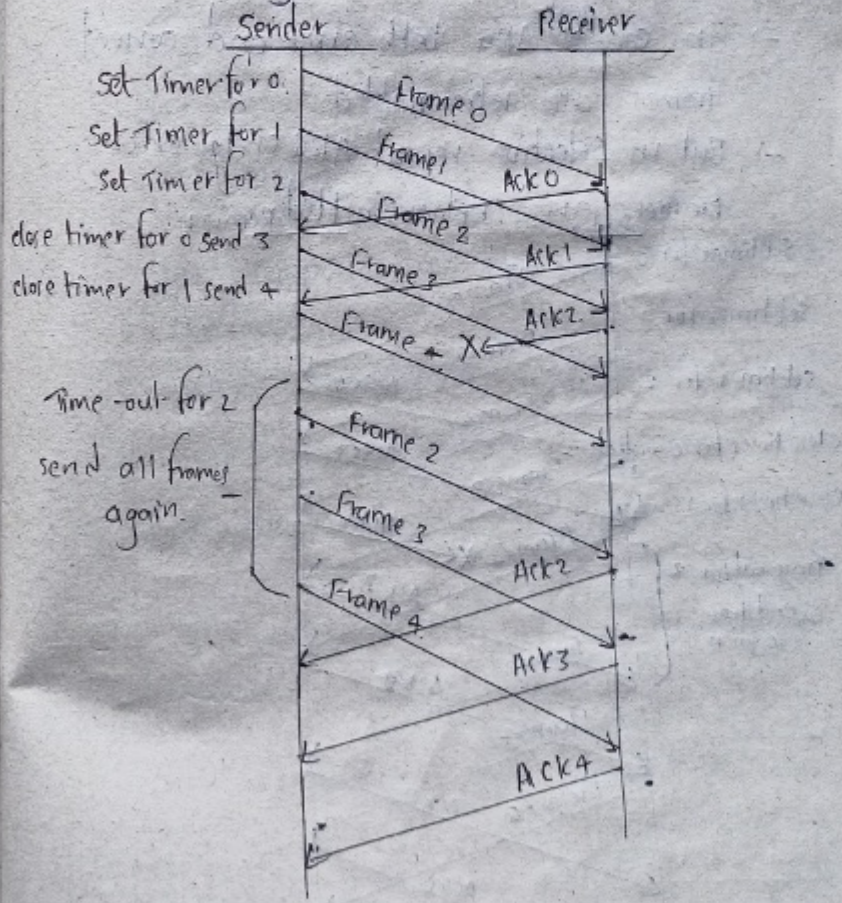
-> If -ve acknowledgement is received, the sender retransmits the frame.

Go-Back-N ARQ.

-> Go-Back-N ARQ is a error control technique.

-> Go-Back-N ARQ both sender and Receiver maintain a window.

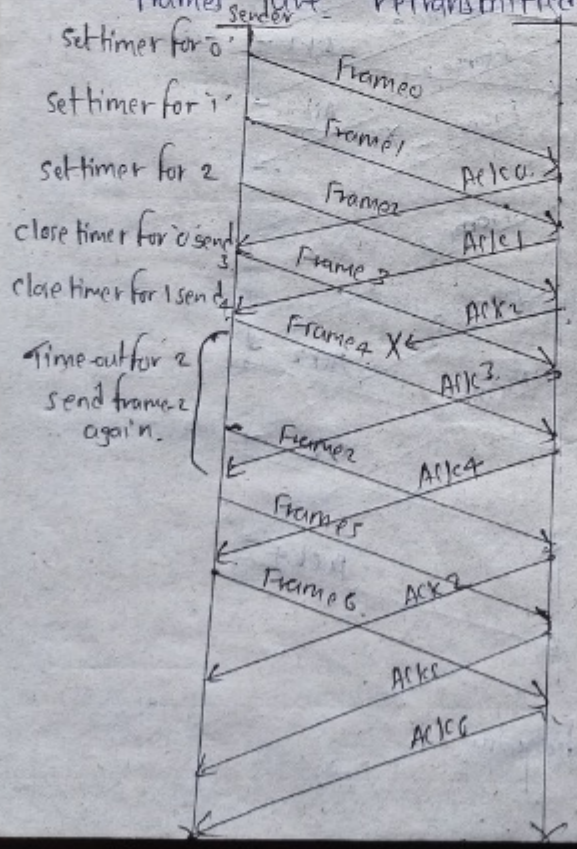
-> Block diagram of Go-Back-N ARQ.



-> Explain diagram.

Selective Repeat ARQ:

-> Selective Repeat ARQ is a Error control technique.
-> It is also known as sliding window technique.
-> It is used for error detection.
-> In Go-Back N- ARQ both error and correct frames are retransmitted.
-> But in selective repeat ARQ only error frames are retransmitted.



* HDLC:

-> HDLC stands for High level DAta Link control.
-> Def: HDLC is a group of communication protocols of the data link layer for transmitting data b/w the nodes.
-> HDLC is a data link protocol, data is in the form of frames.

-> HDLC Transfer modes:

-> HDLC supports two types of transfer modes, they are:
o Normal response mode o asynchronous balanced mode.

o Normal response mode

-> Block diagram

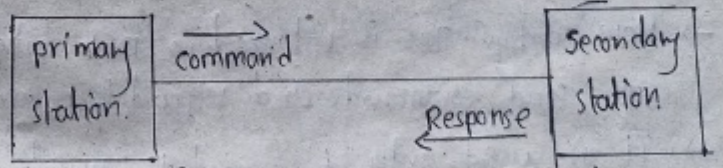


fig1. point-to-point communication

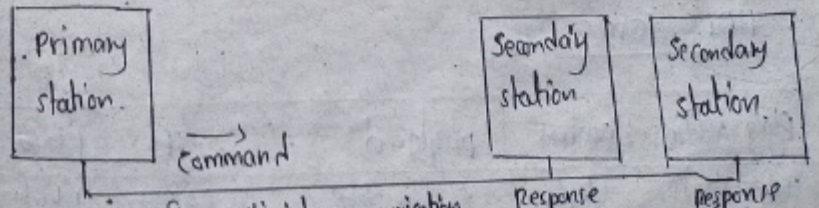
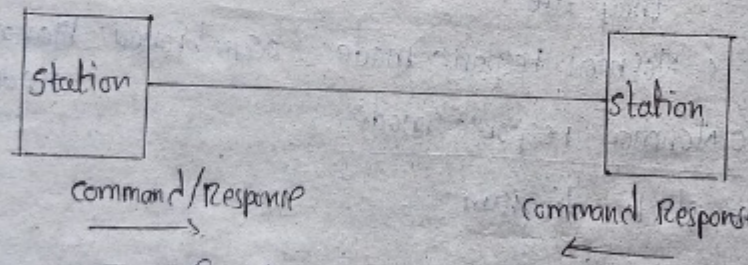


fig2. multipoint communication

-> Fig 1 shows the point-to point communiation
-> In point-to point communication, two types of stations are there, they are
a. primary station b. secondary station.
-> primary station given commands and secondary station gives response for that commands.
-> Fig 2 shows multipoint communication.
-> It is similar to point-to-point but two secondary stations are there

a. Asynchronous Balanced mode

-> Block diagram



-> Here configuration is Balanced i.e. both stations can send commands and respond to commands
-> It is used only for point-to-point communication.

HDLC fame

Flag	Address	control	payload	FCS	Flag
1byte	1byte	1byte	variable	2or4 bytes	1byte

-> Types of HDLC frames

-> There are three types of HDLC frames

(1). I-fame

-> I-frame is also known as Information frame
-> I-frame carry user data from network layer
-> First bit of I frame is 0

Flag	Address	control	user data from upper layers	FCS	Flag.

(2). S-frame

-> S-frame is also known as Supervisory frame
-> Do not contain information feild.
-> First two bits of S-frame is 10.

Flag	Address	control	FCS	Flag.

(3). U frame

-> U-frame is also known as unnumbered frame
-> It contain information feild, if required
-> First two bits of U-frame is 11.

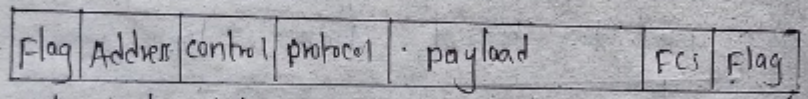
Flag	Address	control	Management Information	FCS	Flag

* point-to-point protocol (PPP)

-> PPP - point-to-point protocol
-> ppp is a data link layer protocol
-> ppp is a WAN protocol, commonly run over internet links.
-> It is widely used in broadband communication
-> It is used to transmit multiprotocol data b/w two directly connected computers
-> It is also known as RFC 1661.

-> PPP frame format

-> PPP frame.



-> PPP is a byte oriented protocol
-> The fields of ppp frame are-

Flag: Flag is at the begining and end of the frame and bit pattern 01111110.

Address: Address is of 1 byte which is set to 11111111.

control: control is of 1 byte which is set to 11000000

protocol: protocol is of 1(or) 2 bytes, that defines type of data.

payload: -> This carrys data from network layer.
-> length is 1500 bytes

FCS: FCS is of 2(or) 4 bytes.

Byte stuffing in ppp frame

-> Byte stuffing is used in ppp payload feild
-> The escape byte 01111101.
-> It is also known as character stuffing

* PPP stack

-> PPPstack - point-to-point stack.
-> In pppstack, there are three set of protocols
1. link control protocol (LCP.
2. Authentication protocol. (PAP, CHAP)
3. Network control protocol

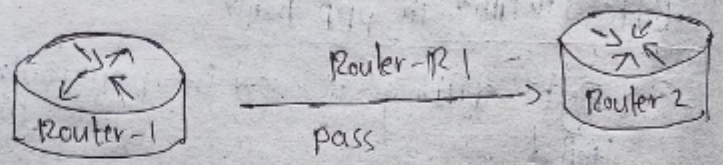
① link control protocol (LCP):

-> The role of LCP is to establish, maintain configure, and terminate the links.
-> It provides negation mechanism

② Authentication protocols:

→ There are two types of authentication protocols

(i) password Authentication protols (PAP):

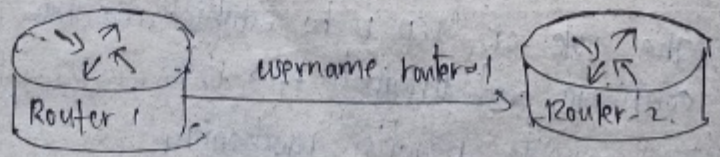


→ PAP is less secure as compared to CHAP.
→ It is a two step process.
→ The password is sent in the form of clear text.

Authentication	database
username	Router2
password	xyz

Authentication database	
username	Router1
password	xyz

(ii) challenged Handshake authentication protocal



→ CHAP is more secure than PAP.
→ It is a three step process.

Authentication database	
username	Router2
password	xyz

Authentication database	
username	Router1
password	xyz

③ Network control protocol (NCP):

→ After the establishment of the link and authentication, the next step is to connect the network layer.
→ Now PPP uses another protocol called as NCP.
→ NCP is a set of protocols.

Unit-3

Medium access sublayer:

Def: medium access sublayer provides control for accessing the transmission medium

-> It is responsible for moving data packets from one NIC to another NIC.

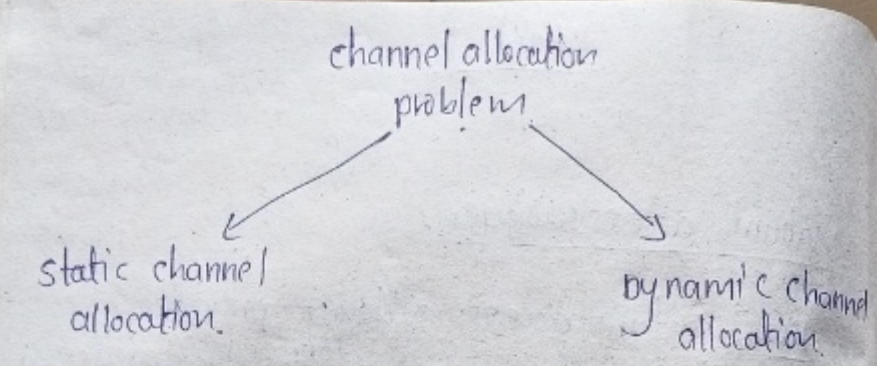
Channel allocation problem:

Def: channel allocation is a problem in which a single channel is divided and allotted to multiple users.

-> There are user's quantity may increase ~~in~~ every time.

-> channel allocation problem can be solved by two methods:

1. static channel allocation
2. Dynamic channel allocation.



① Static channel allocation :

-> In static channel allocation, allocating a single channel among multiple users using Frequency division multiplexing

-> If there is N users, the channel is divided into N-equal parts.

-> Each user assigned to one part only

-> There is no interface b/w users.

② Dynamic channel allocation

-> In dynamic channel allocations, frequency bands are not assigned permanently to users.

-> This allocation optimises bandwidth usage and result is faster.

-> dynamic channel allocation further divided into two types

(i) centralized allocation

(ii) distributed allocation

MID-II

① Multiple Access protocols

ⓐ

Def: multiple access protocols are a set of protocols operating in the medium access sublayer of osi model is called 'MAP'

→ multiple Access protocols are broadly classified into three types, they are
1 Random Access protocols
2. controlled " "
3. channelization methods

1. Random Access protocols

→ Random Access protocols assign uniform priority to all connected nodes.
→ Any node can send data, if channel is idle.
→ There is no fixed time
→ If more than one node tries to send data, collision will occur.

→ four random access protocols
- ALOHA. (It was designed for wireless LAN)
  → In this multiple stations can send data at same time
- CSMA (carrier sense multiple Access)
- CSMA/CD (carrier sense multiple Access with collision detection)
- CSMA/CA (carrier sense multiple Access with collision Avoidance

② controlled Access protocols:

→ controlled Access protocols allow only one node to send data at a given time
→ Before initiation, a node seeks information from another node.
→ This avoids collision of messages
→ This is advanced version of RAR.
→ CAP methods
  - Reservation
  - polling.
  - Token passing.

③ channelization methods.

→ channelization, access all nodes at the

same time to send the data is called channelization.

- It is characterization protocol.
- channelization methods.
  - a. FDMA (Freq Division multiple access)
  - b. TDMA (Time Division " ")
  - c. CDMA (code " " "

unit-3

* Multiple Access protocols

-> A group of protocols is known as multiple access protocols

* IEEE standards 802.3 and 802.11 for LANs

-> IEEE - stands for Institute of Electrical and Electronics Engineers.

-> IEEE composed of engineers, scientists, professionals, etc.

-> IEEE mainly focuses on Electrical Engineering, Electronics engineering, computer engineering, IT etc.

IEE standard.	Description.
-> IEEE 802.3	standards for CSMA/CD.
-> IEEE 802.11	standards for wifi(or) wireless Networking.

-> characteristics of IEEE standards.

- Good performance (or) compatability.
- Technical societies
- Fast speed.
- Topology implemented by using IEEE LAN.

Advantages

-> Speed is fast.
-> works for benifit of Humanity.

Disadvantages

-> security required.
-> requires periodic maintenance.

* High speed LANs

-> LAN stands for Local Area Network.

-> A Local Area Network is a connected environment, including one (or) more buildings typically in a one-kilometer radius is called LAN.

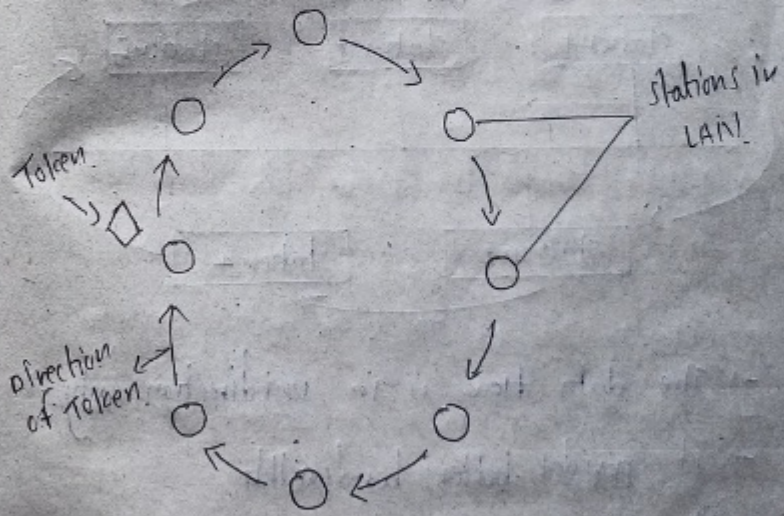
-> High speed LANs
- Token Ring LAN
- Token Bus LAN
- Fi wireless LAN
- FDDI LAN.

1. Token Ring LAN

-> Token Ring is a communication protocol in local Area Networks, where all stations are connected in Ring topology is called Token Ring LAN.

-> Token Ring is IEEE standard (802.5).

-> Block diagram



-> The data flow is unidirection i.e token passing.

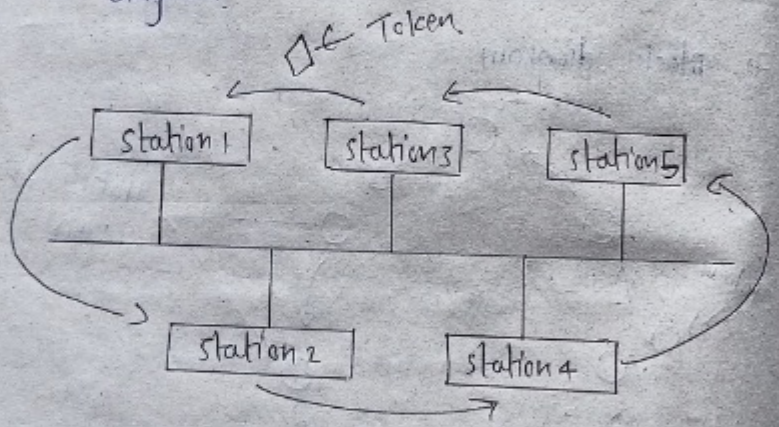
-> The above diagram shows working of Token Ring LAN.

2. Token Bus LAN:

-> Token Bus LAN is communication protocol in Local Area Networks, where all stations are connected in virtual Ring (or) coaxial cable called Token Bus LAN.

-> Token Bus LAN is IEEE standard (802.4)

-> Diagram



-> The data flow is in unidirection only.

-> It provides better bandwidth.

-> It uses Bus topology.

* WLAN

-> WLAN stands for wireless LAN.

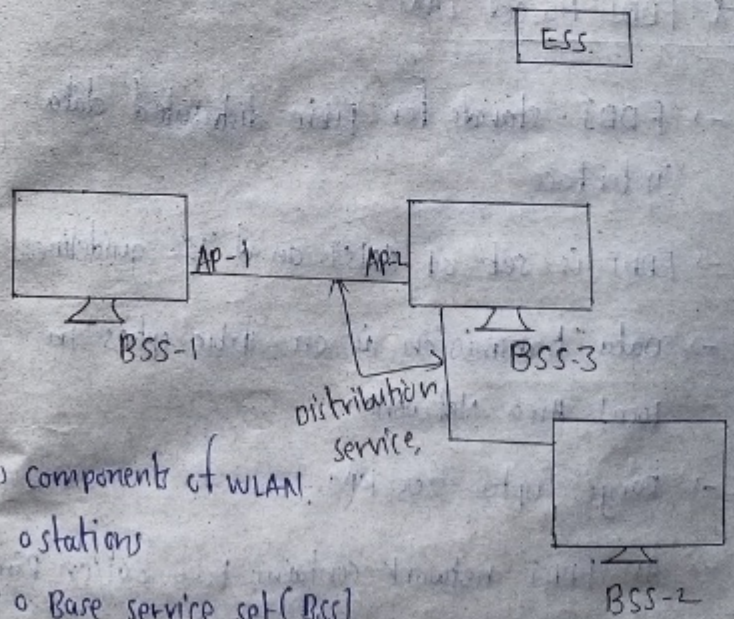
-> WLAN is a Local Area Area Networks that uses radio communication.

-> The performance of WLAN is high compared with other wireless Networks.

-> WLAN covers within campus (or) Building.

-> WLAN standards IEEE 802.11, wi-Fi, etc.

-> Diagram



-> Components of WLAN.

- o stations
- o Base service set (BSS)
- o Ens Extended service set (ESS)
- o. Distribution service

o Types of WLAN's

- o Infrastructure mode
- o Ad-Hoc mode.

Advantages

- -> High speed.
- -> flexibility
- -> Reliability
- -> mobility

Disadvantages

- -> slower Bandwidth
- -> less capacity.

* FDDI Based LAN :-

-> FDDI - stands for Fibre distributed data interface.

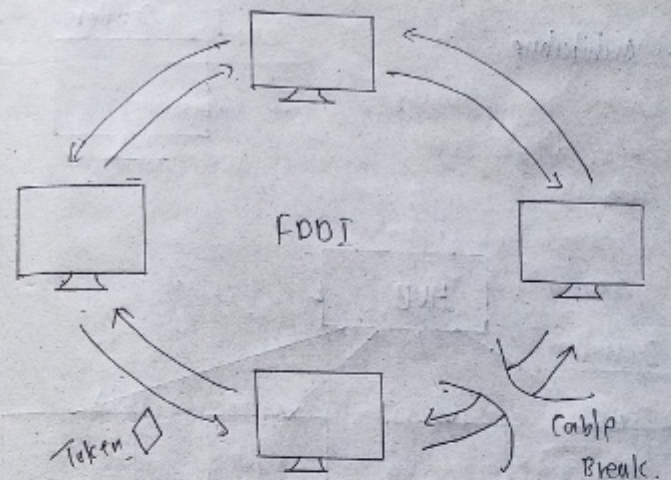
-> FDDI is set of ANSI and Iso guidelines.

-> Data transmission is on fibre optics in Local Area Network.

-> Range upto 200 km.

-> An FDDI network contains two token Rings.

-> An FDDI is a Ring Network.



-> FDDI gives 100 mbps of Information.

Advantages

- -> Range 200km.
- -> High transmission capacity

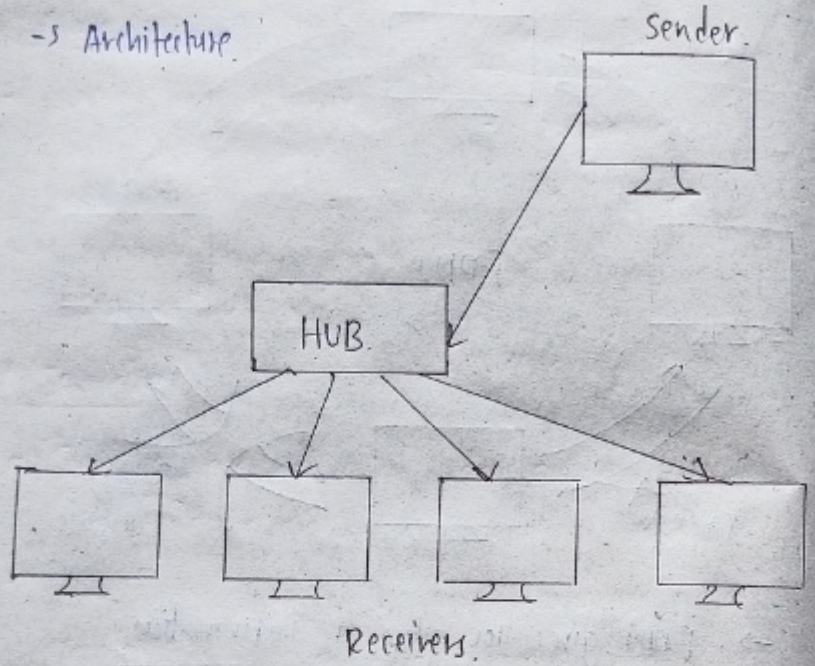
Disadvantages

- -> complex
- -> expensive

* Hubs : A Hub is a device that connects multiple computers and devices together. is called Hub.

- -> Hub is also called as repeater.
- -> Hub is used in LANs.
- -> A hub has many ports in it.

-> Architecture



-> A Hub is half duplex.
-> A hub operates in physical layer of the OSI model.
-> A hub is a passive device.
-> Types of hubs

o passive hubs: It is configred in star topology.
-> It includes connectors and connected to LANs.

o ~~passive hub~~ Active hubs: As compared to passive hub, active hub includes some additional features.
-> It plays important role.

o Intelligent hub: It is smarter than passive and active hubs.
-> Better performance offers.

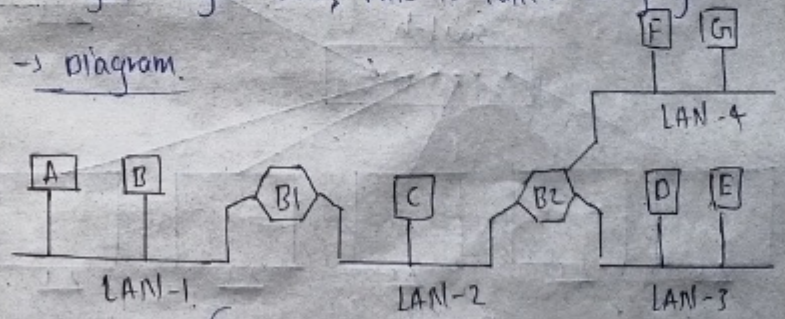
Advantages
-> less expensive.
-> good performance

Disadvantage
-> Find shortest path
-> No mechanism for traffic detection.

* Bridges

-> A bridge is a network that connects multiple subnetworks to create a single network.
-> Bridge provide interconnection with other computer.
-> Bridge is used to connect multiple LANs to get larger LAN, this is called bridging.

-> Diagram



-> working of bridge.
o Receiving data
o Transmitting data
o Building a table
o Filtering data.

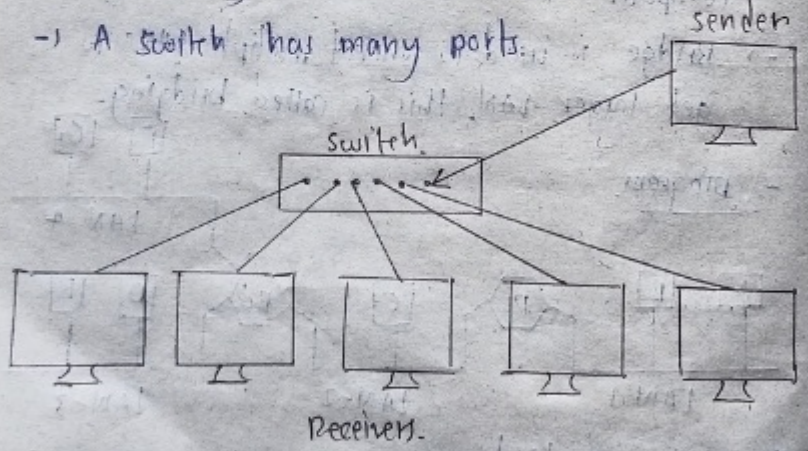
Advantages	Disadvantage
-> Divides large networks into multiple small networks	-> Expensive.
-> Increases the physical size of network.	-> slow speed.

* Switches

-> Switches are networking devices operating at data link layer of OSI model is called switches.

-> Switches connects the devices and use packet switching to send (or) receive data.

-> A switch has many ports.



-> Switch uses physical address and packet switching.

-> It supports unicast, multicast, and broadcast.

-> Types of switches.

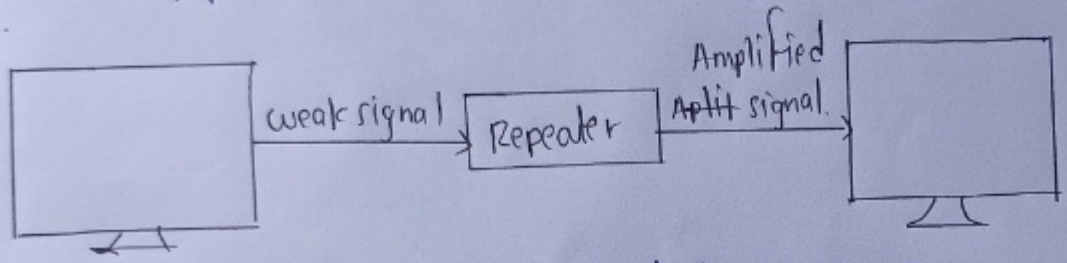
- o unmanaged switch.
- o Managed switch
- o LAN switch.
- o PoE switch.

* Token Bus	Token Ring
-> Token Bus is a protocol in LAN.	-> Token ring is protocol in LAN.
-> It uses Bus Topology.	-> Token Ring uses star Topology.
-> It provider high bandwidth	-> It provides less bandwidth.
-> It's IEEE standart 802.4	-> It's IEEE standard 802.5.
-> It is used large industries.	-> It is used in workplaces.
-> coaxial cable is used.	-> Fibre optics is used.
-> cable length 200m to 500m.	-> cable length 50m to 100m.
-> Not reliable	-> Reliable.
-> less expensive.	-> More expensive.

* Repeaters

Def: A repeater is a networking device i.e used to amplify and generate incoming signal.

-> Repeaters work at physical layer of osi model.
-> Repeater increases the networking distance.
-> In LANs and WANs repeaters are used.
-> Repeater transfers data securely to long distances.



-> Repeaters used in Analog and digital circuits.
-> Repeaters extend range of networks.
-> Repeater reduces the errors.

Types of Repeater

0 Based on signals
-> Analog repeater.
-> Digital repeater.

0. Domain of Network.
-> local repeater.
-> Remote repeater.

0. Based on connected Network.
-> wired repeater.
-> wireless repeater.

0. Based on Technology
-> microwave repeater.
-> Radio repeater.

Advantages.

-> Better performance
-> More expensive.

Disadvantages

-> Limited no. of repeaters
-> collision.

Unit - 4

* Design Issues

* Network layer

Def. The Network layer is the part of the Internet communications process, where packets of data sending back and forth between different networks called Network layer.

* Design Issues of Network layer

-> The Network layer is majorly focused on getting packets from the source to destination

-> The Network layer have some design issues

o store and forward packet switching:-

-> The network layer operates in environment that uses store and forward packet switching.

-> The node sends the data packet to the nearest router.

-> This data packet after verifying the checksum then it is forwarded to next router.

-> This mechanism is called "store and forward packet switching.

◎ Services to Transport layer :

-> The network layer provide services to transport layer through network.

-> Two types of services are there

○ ● connection-oriented service :- In this service a path is setup blw source and destination.

-> There is connection blw source and destination
-> This path (or route called virtual circuit.

○ Connection less service :- In this service, there is no path setup blw source and destination.

-> Data is individually routed from source to destination.

-> The network uses datagram for transmission is called datagram networks.

* Routing Algorithms :-

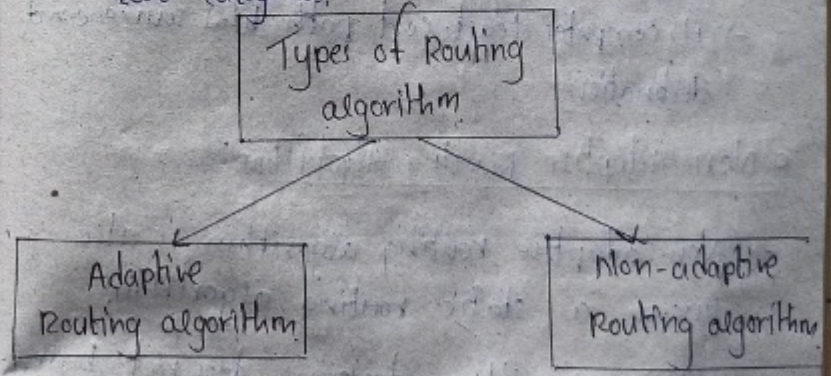
-> Routing Algorithm in Computer Network, determines the optimal path for data packets to travel from source to destination.

-> Routing is of four types.

- ○ unicast routing.
- ○ Broadcast routing
- ○ multicast routing
- ○ Anycast routing

○ classification of Routing algorithms :

-> The Routing algorithm is divided into two categories.



○ Adaptive routing Algorithm :

-> An adaptive routing algorithm is also known as dynamic routing algorithm.

-> In this algorithm decisions is based on topology and network traffic.

-> Again adaptive Routing algorithm can be divided into three types.

o Centralized Routing algorithm :-

-> It is also known as global routing algorithm.

-> Least-cost path b/w source and destination.

o Isolation Algorithm :-

-> It is an algorithm, that obtains routing information by using local information.

o Distributed Algorithm :-

-> It is also known as decentralized algorithm.

-> It computes least-cost path b/w source and destination.

o Non-Adaptive Routing Algorithm :-

-> Non-adaptive routing algorithm is also known as static routing algorithm.

-> In this algorithm decisions does not based topology and network traffic.

-> Non-Adaptive routing algorithm is of two types.

o Flooding :- In flooding, every incoming packet is sent to all the outgoing links.

o Random walks :- Random walks, uses the alternative routes very efficiently.

* Congestion control Algorithm :-

-> Congestion control algorithm is a mechanism that controls the entry of data packets into the network.

-> Congestive avoidance Algorithms avoid congestive collapse in a work.

-> Congestion control Algorithm is of two types.

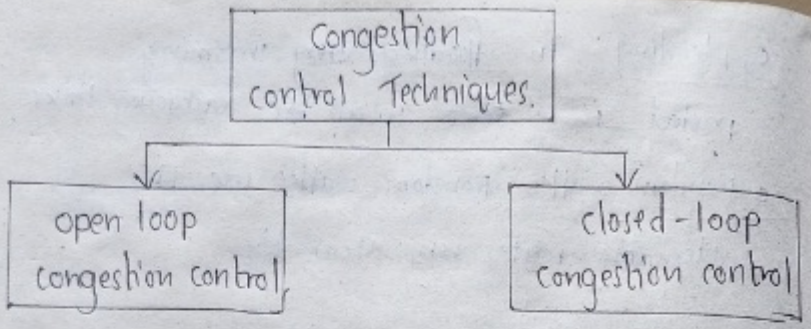
o Leaky Bucket Algorithm.

o Token Bucket Algorithm.

o Congestion control techniques :-

-> Congestion control techniques used to control or prevent congestion.

-> Congestion control techniques can be classified into two types.



o open-loop congestion control :

-> open loop congestion control policies are applied to prevent congestion.

-> The congestion control is handled by either source (or) destination.

-> policies by open-loop congestion control.

o Retransmission policy

-> It is the policy, in which retransmission of packets are take care of it.

-> If sender sent a packet, i.e lost (or) corrupted then that pacle need to be retransmitted.

o window policy :-

-> To implement window policy, selective reject method is used.

-> selective reject method, sends only specific (or) damaged packets.

o Discarding policy :-

-> Discarding policy may prevent congestion at the same time may transmission.

o Acknowledgement policy :

-> The acknowledgement policy imposed by the receiver also affect congestion.

-> It prevents the congestion.

o closed-loop ~~control~~ congestion control :-

-> closed-loop congestion control mechanism used to remove congestion.

o Backpressure

-> Backpressure is a technique in which congested node stops receiving packets from upstream node.

-> Back pressure is a node-to-node congestion control technique, that propagate opposite direction of data flow.

o choke packet technique :-

-> choke packet technique is applicable to both virtual network and datagram subnets.

-> It removes the congestion.

o Implict signaling

-> In implict signaling there is no communication between congested node and source.

-> This is congestion removal policy, used by Tcp.

o Explict signaling :

-> In explict signaling, there is communication between ~~cong~~ source and destination.

-> Explict signaling may occur in either forward (or) backward direction.

-> This is congestion removal policy.

* Host-to-Host Delivery

* Internetworking Internetworking is the practice of interconnecting multiple computers networks and exchange messages is called internetworking.

-> The resulting system of interconnected network is called internetwork (or) internet.

-> The term internetworking is a combination of inter and networking.

-> In past internet is called as catenet.

-> Internetworking is between public, private, commerical, industrial (or) governmental networks.

-> There is one minute difference blw extending network and internetworking.

-> Internetworking is of three types they are:-

o Extranet o Intranet o Internet.

o Extranet :

-> It is a network, that is restricted to an organisation (or) entity.

-> It is very lowest level of Internetworking.

-> It is used in personal area.

-> Extranet may additionally classified as MAN, WAN and LAN.

-> It is used for medium distances.

o ~~Intranet~~ :

-> Features

o Data security

o Faster communication

o Flexibility

o Intranet

-> An intranet is a private network, i.e belongs to particular organization.
-> It is designed for using personal organization
-> It is more secure.
-> It is based on, TCP/IP protocol
-> It is cheap and easy to implement.
-> It is more safe than Extranet and internet.
-> Types of Inbanets
  o corporate intranet
  o departmetal Intranet
  o could-Based Intranet

o Internet

-> The internet is a global network of interconnected computers, servers, phones, smart appliances, using TCP.
-> The intenet is foremost tool.
-> Internet connects millions of computers, webserver, websites etc.
-> By using internet we can send E-mails, photos videous, and audious to whom we want to send.
-> The internet working with medium like LAN, WAN, MAN. etc
-> with requires physical cable to access internet
-> The internet uses IP address.
-> The internet can be considered as library.
-> The internet is hard-ware oriented.
-> Advantages
  o online Banking and Transaction
  o Education
  o Best communication medium

* IP Addressing

-> An Internet protocol addressing is a unique identifying number assigned to every device connected to the internet is called IP addresing.

o working of IP addres

-> The working of IP is similar to other languages.
-> It can also use some set of rules.

-> using IP address we can easily send or receive data.

-> classification of IP address.

o. public IP address

-> public address is of two types. they are

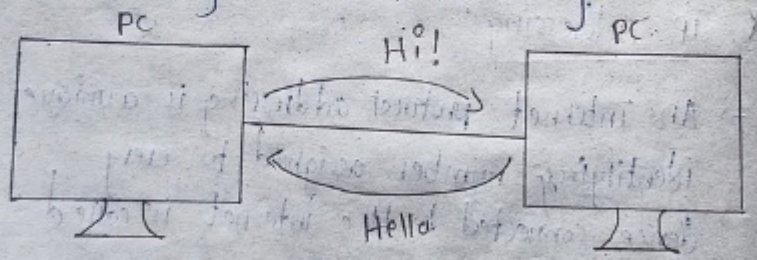
- o Dynamic IP address
- o static IP address

o private IP address.

o shared IP address.

o dedicated IP address

-> Block diagram of IP Addressing.



* classful and classless Addressing

classfull Addressing An IPv4 addressing architecture is known as classfull addressing and split addresses into five classes is called classful addressing.

-> classfull addressing is divided into 5 types.

1. class A - class A IP address assigned to the networks that contain large no. of hosts.
   - -> The network ID is 8 bits long.
   - -> The host ID is 24 bits long.
   - -> IP address range 0.0.0.0 - 127.255.255.255

2. class B - class B IP address assigned to networks that range from medium sized to large sized networks
   - -> The network ID 16 bits long.
   - -> The host ID 16 bits long.
   - -> Range - 128.0.0.0 - 191.255.255.255

3. class C - class C IP address at assigned to small-sized networks
   - -> The network ID 24 bits long
   - -> The host IP 8 bits long
   - -> Range 192.0.0.0 - 223.255.255.255

4. Class D: Class D IP address is assigned to multicasting.

-> Range - 224.0.0.0 - 239.255.255.255.

5. Class E: Class E IP address is assigned to experimental and research purpose.

-> Host ID is 28 bits long.

-> Range - 240.0.0.0 - 255.255.255.255

Classless Addressing

-> classless addressing is an IPv4 addressing architecture that uses variable-length subnet masking is called classless addressing.

-> The most common use of classless addressing is to combine two (or) more class C networks.

-> For example the class C networks 192.168.32.0 and 192.168.33.0 are combined we get 192.168.32.0/23

Classfull	Classless
-> Classfull addressing is less practical	-> classless addressing is more practical
-> It does not supports the VLSM.	-> It supports the VLSM.
-> It requires more Bandwidth.	-> It requires less Bandwidth.
-> It is more expensive.	-> It is less expensive.
-> It is slower.	-> It is faster.
-> It does not support CIDR.	-> It supports CIDR.
-> Division of address. o Network o Host o subnet.	-> Division of address. o Host o subnet.

* Routing : Routing is the process of path selection in any network.

-> Types of Routing

-> There are three types of Routing they are:-

1. Static Routing : static routing is a process in which we have to add routes to the routing table.

~~Ad~~ -> It is also known as Non-adaptive Routing.

Advantages

-> good security
-> No overhead
-> No Bandwidth

Disadvantages

-> For large networks, difficult to add routes.

2. Dynamic Routing : Dynamic routing is a process in which router adds a new route to the routing table.

-> It is also known as adaptive routing.

Advantages

-> Easy to design.
-> More effective.

Disadvantages

-> More expensive
-> less secure.

③. Default Routing Default routing is a process in which router send all packets towards single router.

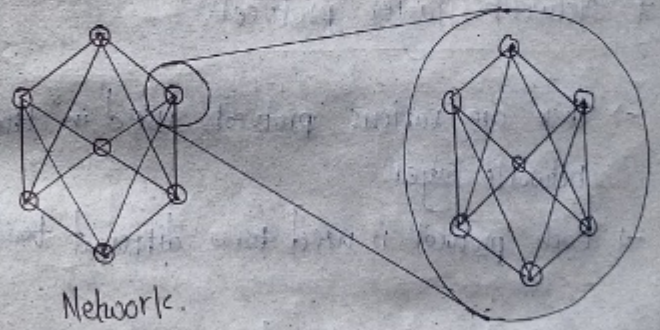
-> Design is same as static Routing.

* Subnet :

Def A Subnet (or) subnetwork, is a network inside a network.

-> subnets make networks more efficient.

-> Diagramatic representation.



-> organizations use a subnet to subdivide large networks into smaller.

-> Goal of subnet is to divide large networks into small networks.

-> Each subnet allows connected devices to communicate each other.

Subnetting

when a bigger network is divided into smaller networks, to maintain security, then it is called subnetting.

- -> subnetting is used to increasing network security.
- -> subnetting provides security to one network from another network.
- -> Maintenance is easy.

* Network layer protocols:

-> There are various protocols used in the network layer.

-> Each protocol is used for a different task.

1. IP (Internet protocol)

-> IP stands for Internet protocol

-> Internet protocol is responsible for transfering the data from one node to another node in network.

-> IP is connectionless protocol

-> The Internet protocol is divided into two types:

* IPV4

-> Internet protocol V4 or is with a 32 bit address scheme.

-> IPv4 has four numeric feilds and seperated by dot.

-> IPV4 can be configured either ~~DHPC~~ DHCP or manually.

-> IPv4 does not provide security.

-> IPv4 is divided into five clases they are class A, class B, class C, class D, class E.

* IPV6:

-> Internet protocol V6 is the most recent version of IP.

-> It provides 128 bit address scheme.

-> IPV6 has eight numeric feilds, that are seperated by colon.

-> IPV6 provides more security.

-> IPV6 has more address range than IPV4.

* ARP :

-> ARP - stands for Address resolution protocol

-> ARP is used to convert IP address into physical address.

-> By using ARP. el physical address can be changed easily.

-> If the host wants to know the physical address of another host the ARP can be used.

-> The ARP ~~cam~~ cache is used to make network more efficient.

-> There are two types of ARP entries

o dynamic entry :

-> It is an entry which is created automatically.

-> dynamic entries are not permanent and they are removed periodically.

o static entry :

-> It is an entry where someone manually enters the IP to physical address.

* ICMP :

-> ICMP stands for Internet control message protocol.

-> ICMP is network layer protocol used by hosts and routers.

-> ICMP uses echo test/reply to check whether destination is reachable (or) not.

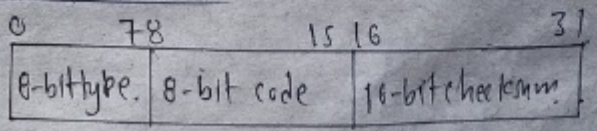
-> ICMP handls both control and error messages.

-> ICMP messages are divided into two types.

o Error message : (It states issues (or) problems that are faced by host.

o query message : (It is used ~~to~~ by host inorder to get information from host (or) router.

-> ICMP formats



* ICMPV6

-> ICMPV6 - Internet control message protocol V6.

-> ICMPV6 is modified version of ICMP protocol.

-> ICMPV6 is a TCP/IP protocol.

-> ICMPV6 is combination of ARP and ICMP.

-> ICMPV6 can perform error reporting and diagnostic functions.

-> ICMPV6 supports Neighbour discovery protocol.

-> ICMPV6 messages are usually sent as ICMPV6 packet.

-> ICMPV6 messages are related to MLD or NDISC.

Unit-5

* Transport Layer

Transport layer takes services from the application layer and provides services to the network layer is called transport layer.

-> At senders end - Transport layer receives data from Application layer and transfers data to the Network layer.

-> At receivers end - The transport layer receives data from network layer and transfers data to the application layer.

* process to process Delivery

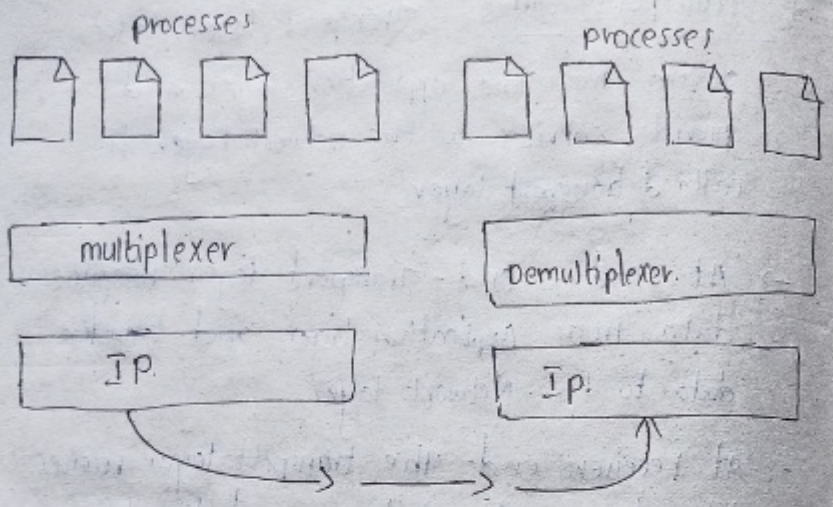
-> The transport layer is responsible for process to process delivery.

-> process to process delivery is also called as node-no to-node delivery.

-> The network layer is responsible for delivery of datagrams b/w two hosts.

-> This is called host-to-host delivery.

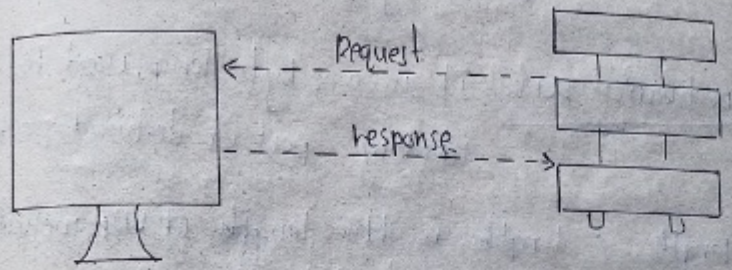
-> Real communication takes place between two processes



* UDP (user datagram protocol):

-> UDP - stands for user datagram protocol.
-> UDP is a transport layer protocol.
-> UDP enables process-to-process communication.
-> UDP is a part of internet protocol i.e UDP/IP.
-> UDP is a standard protocol.
-> UDP is the alternative protocol to the to the TCP protocol.

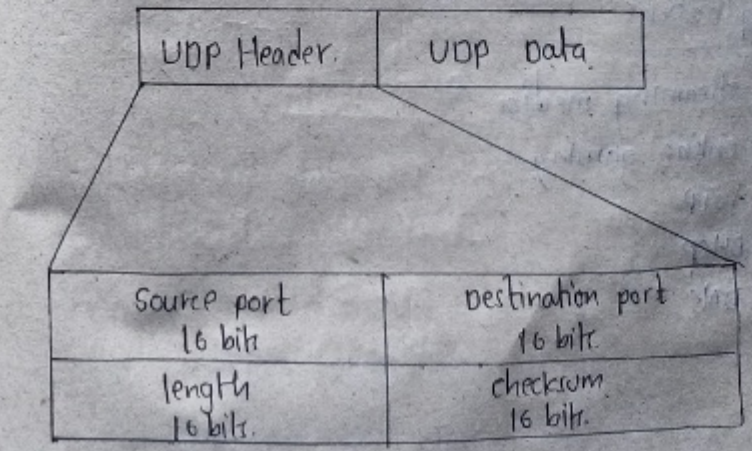
-> Block diagram.



-> There is no error checking in UDP.

-> UDP Header

-> UDP header is an 8-byte simple and fixed header.
-> The first 8-bytes contains necessary header info and remaining contains data.
-> UDP is 16 bits long.



Source port: source port is a 2-byte long, used to identify port no. of the source.

Destination port: It is a 2-byte long, used to identify port of destined packet.

length: length is the length of UDP, including header and data. (16 bits)

checksum: checksum is 2 byte long feild. (16 bits) It's calculation is not mandatory.

Advantages

-> speed is fast.
-> simplicity.
-> smaller packet size.

Disadvantages

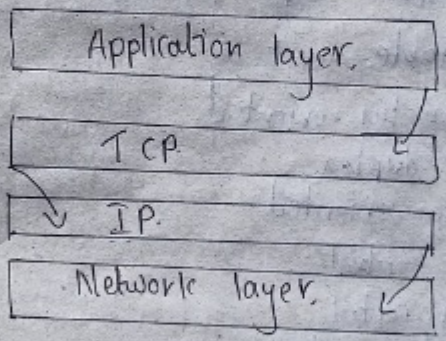
-> No reliability
-> No flow control.
-> No congestion control.

Applications

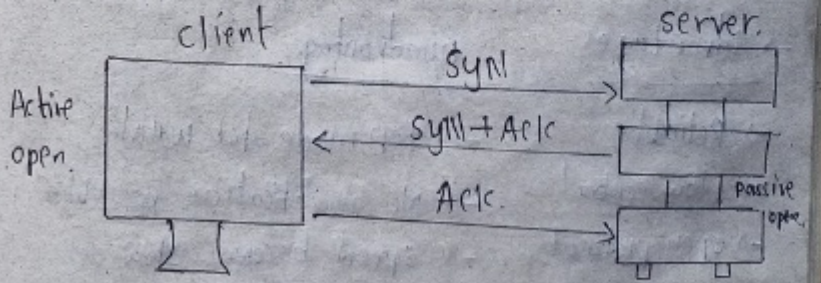
-> streaming media.
-> online gaming
-> VoIP.
-> DHCP.
-> DNS.

* TCP (Transmission control protocol)

-> TCP - stands for Transmission control protocol
-> TCP is the one of the main protocol in Internet protocol (TCP/IP)
-> TCP lies between application layer and network layer.
-> TCP - is a connected-oriented protocol for communication.



-> TCP



-> In TCP/IP, data breaks down into small bundles, and afterward reassembles the bundles into original data on opp end.

-> The main function of Tcp is to take data from application layer.

-> In Tcp data exchange is between client and server.

-> client end is called Active open.

-> server end is called pasive ope.

o Features of Tcp

-> Transport layer protocol.

-> Reliable.

-> connection-oriented.

-> Full-duplex

-> Stream oriented.

-> Flow control

-> Error control.

-> congestion control.

-> Advantages

-> Reliable.

-> Flow control.

-> open protocol.

Disadvantages

-> Tcp made for WANs.

-> No modification possible.

-> speed becomes slow as time increases.

* Congestion control

-> congestion control is a mechanism that controls, the entry of data packets into the network, is called congestion control.

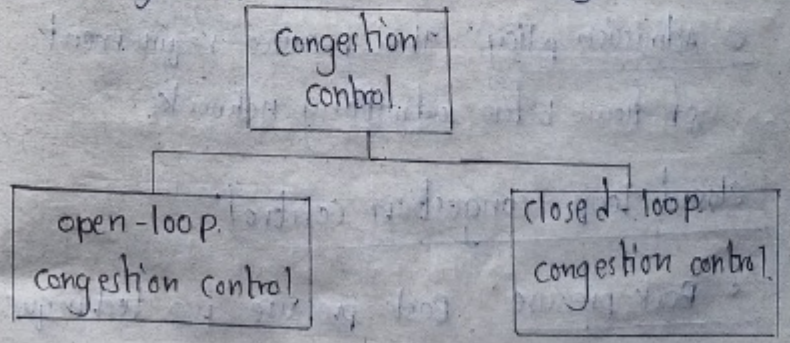
-> To avoid congestive collapse, congestive-avoidance algorithms are used.

-> There are two congestion control algorithms.

- o Leaky Bucket algorithm.
- o Token Bucket Algorithm.

-> congestion control refers techniques and mechanisms.

-> Congestion control is of two types.



Open-loop congestion control:

-> It is used to prevent congestion before it happens.

-> It is handled by either source or destination.

- Retransmission : It is designed to optimize efficiency and preventing congestion.
- window : selection Repeat is better than Go-back-N.
- Acknowledgement : Does not Ack every packet.
- Discard policy : It prevent congestion and at the same time may not harm the integrity of the transmission.
- Admission policy : The resource requirement of flow before admitting network.

Closed-loop congestion control:

- Back pressure : Back pressure is a technique in which a congested nodes stops receiving ~~from~~ packets from upstream node.

-> It is nod-to-node control technique.

- choke packet technique

choke packet technique is applicable to both virtual networks as well as datagram subnets.

- Implict signaling : In this there is no communication between the congestion node and the source.
- ~~Expliit~~ Explicit signaling : In this the node can ~~expiit~~ explicitly send a signal to source or destination.

* Quality of services

-> Quality of service refers to traffic control mechanisms.

-> Quality of services is a set of technologies that works on network.

-> In quality of service, we try to create appropriate environment for the traffic.

- QoS specification

~~-> Delay~~ -> Reliability
~~-> Delay variation~~ -> Delay
~~-> Through put~~ -> Jitter
~~-> Error Rate~~ -> Bandwidth

-> There are two types of QoS solutions

- stateless solutions
- stateful solutions

- stateless solution

-> It is scalable and robust.

-> In this server and client are loosely coupled and can act.

- stateful solution

-> It is less scalable and robust

-> In this server and client are tightly coupled.

- quality of services parameters

-> Reliability : It is one of the main parameter, flow needs.

-> If reliability is low, packet loss will occur.

-> Delay : Another parameter of flow is the delay.

-> Here transmission is b/w source and destination.

Jitter : Jitter is basically the variation in the packet delay.

-> If jitter is high then delay is large.

-> If jitter is low then delay is low.

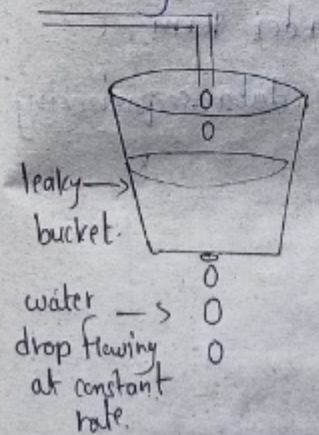
-> Bandwidth : The different application need different bandwidth

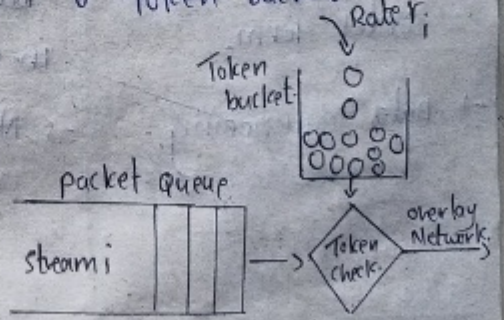
- Techniques involved in QoS

- FIFO ~~queing~~ queuing
- priority queuing
- weighted fair queuing.

- Traffic shaping

- Leaky bucket
- Token Bucket





* TCP Vs UDP

TCP	UDP
-> TCP - Transmission control protocol.	-> user datagram protocol.
-> It is connection-oriented protocol.	-> It is connection-less protocol.
-> It supports full duplex	-> It doesn't support full duplex.
-> It provides error and flow control.	-> It doesn't provide error and flow control.
-> It is relatively slow.	-> It is relatively fast.
-> It have state memory.	-> It have stateless memory.
-> It is reliable.	-> It is not reliable.
-> Data packets are in order form.	-> Data packets are in in-order form.
-> Data sequenceing.	-> No data sequenceing.

* Application layer

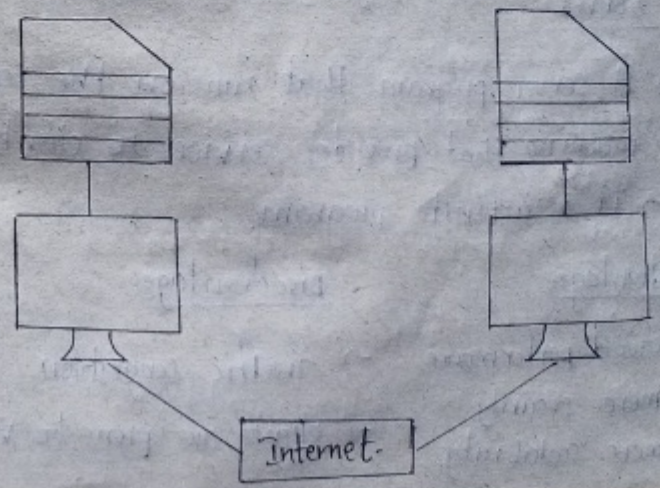
Def: An application layer is an abstraction layer, that is used by end-user software such as web browsers and Email clients in network is called Application layer.

* Client-Server Model

Def: A client-server model is a networking computing system design, that gives a relationship between two (or) more computers.

-> Here client computer requests the services from server computer.

-> Block diagram of client-server Model



-> An application program is known as client program.

-> An service from application program is known as server program.

-> A client program runs only when it requests for service.

-> A server program will run all the time.

-> A server provides service for many clients, like many-to-one relationship.

o client

-> A client is a program that runs on local machine i.e requests service from server.

-> It is finite program.

o. Server

-> A server program that runs on the remote machine, that provides services to clients.

-> It is infinite program.

Advantages

-> Good performance.
-> more security.
-> more scalability.

Disadvantages

-> Traffic congestion.
-> clients are prone to viruses.

* Socket Interface

Socket: A socket is one end-point of two-way communication link b/w two programs running on the network is called socket.

-> The socket mechanism provides inter-process communication (IPC).

-> The socket provides bidirectional FIFO communication.

-> Each socket has a specific address.

-> Sockets are generally used in client-server applications.

o Types of sockets

-> There are two types of sockets.
  o Datagram socket.
  o Stream socket.

o Datagram socket: This is a type of network which has connection less point-for-sending and receiving packets.

-> It is similar to mail box

o Stream socket: This is a type of network socket, which is connection-oriented, sequenced for sending and receiving data packets is called stream socket.

-> It is similar to phone.

o Advantages

-> Data storing and sharing
-> Flexible Access.
-> Services.

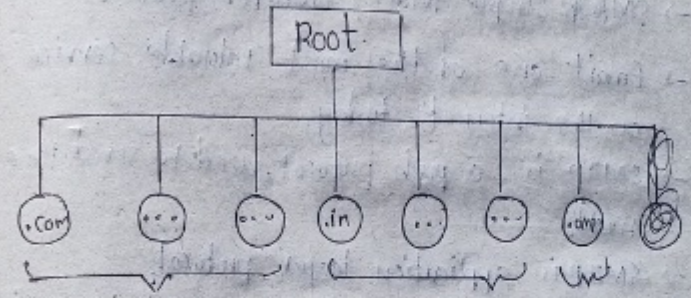
o Disadvantages

-> Failure of server.
-> cable braking issue
-> Set cost is high.

*. DNS (Domain Name system)

-> DNS - stands for Domain Name system
-> DNS - is a host name of IP address.
-> DNS is a application layer protocol for exchanging message between client and server.
-> DNS is required for working of Internet.
-> DNS is a TCP/IP protocol.
-> DNS used in different platforms.

-> The Domain Name space is divided into three categories



o Generic Domain: com (commercial), edu (educational), mil (military), org (organisation) etc.

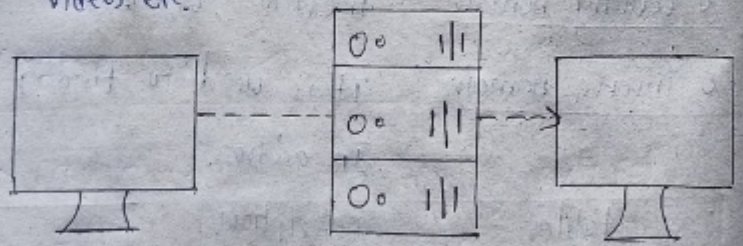
o country domain: in (india), us, uk etc

o Inverse Domain: It is used to finding Ip address.

lable	Description
com.	Commercial organization
edu	education institutions
gov.	government institutions
mil.	Military
int.	International organizations
biz	Business.
name	personal names.

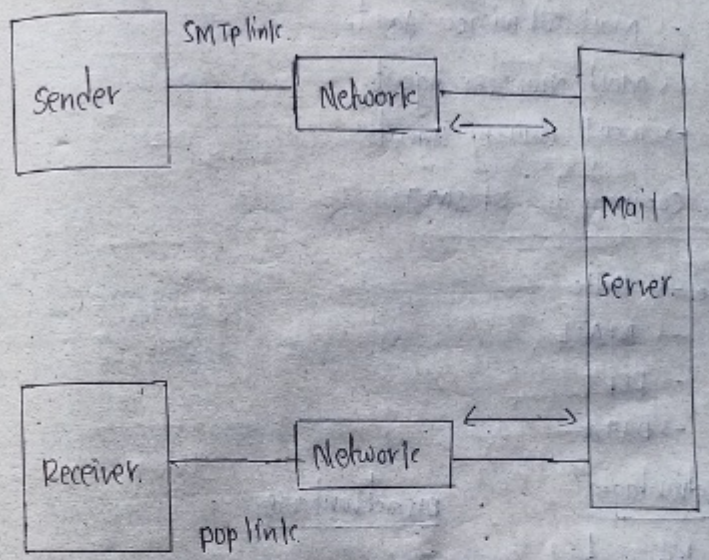
* SMTP :-

-> SMTP Simple Mail Transfer protocol.
-> Email one of the most valuable service on the internet today.
-> SMTP is a push protocol, used to send the mail.
-> SMTP is application layer protocol.
-> SMTP server is an always on listening mode
-> SMTP is a set of communication guide lines.
-> SMPT is program used for sending messages to other computer based on e-mail address.
-> sending messages can include voice, text, videos etc.



-> SMTP protocol is of two types
  o End-to-End method.
  o. Store and Forward method.

-> working of SMTP



-> Communication blw sender and Receiver. :- Sender Sends the messages to network through SMTP ~~net~~ link, network forwards to mail server.
-> Mail server sends message to network, again network sends to receiver.
-> Sending E-mail :- After completing E-mail, the mail client submits to e-mail to server by using SMTP.
-> Receiving E-mails :- client sends e-mail to Receiver, i.e. username for example manoj@g.mail.com. message forwards to this username.

o Components of SMTP

-> Mail user Agent
-> Mail submission Agent
-> Mail Transfer Agent
-> mail delivery Agent

o Commands of SMTP

-> Hello
-> MAIL
-> RCPT
-> DATA

Advantages	Disadvantages
-> low cost	-> less security
-> Reliable	-> Just 7-bit Ascii used

X FTP (File Transfer protocol)

-> FTP stands for file transfer protocol.

-> FTP is a standard network protocol, used to transfer files from one host to another over a TCP based network is called FTP.

-> FTP is a application layer protocol

-> In FTP data (or) file transfers efficiently and reliably.

-> FTP can transfer data including, images, audio and video.

-> In FTP transfering of files is simple.

o Types of FTP

-> Anonymous FTP: The user can access these files without having any username (or) password.

-> password protected FTP: This is similar to Anonymous FTP.

-> FTP secure: It is more secure version of FTP data transfer.

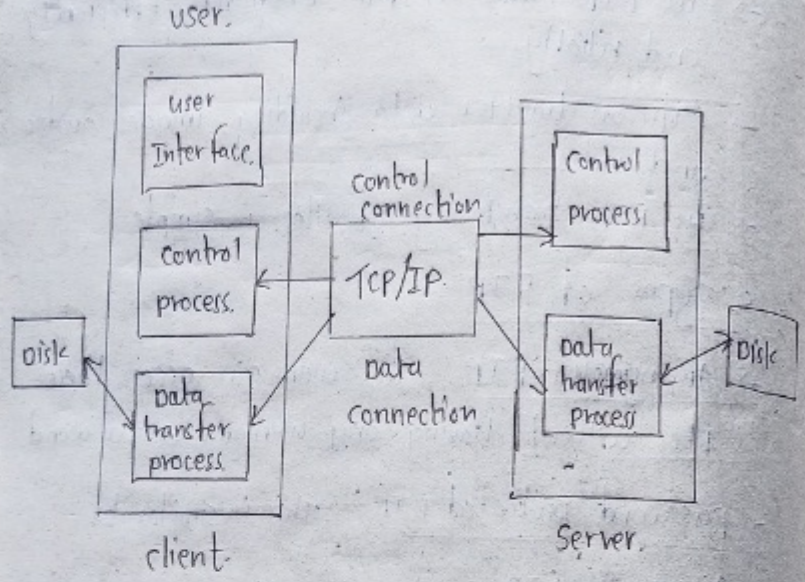
-> Secure FTP: Secure FTP is not a FTP protocol. it works on port 22.

o working:

-> FTP is a client-server protocol,

-> A client can start a conversation with server by client request

-> The user can start different functions like upload, delete, copy, etc.



- Types of connections
  - control connection.
  - Data connection.
  - control connection

-> It uses very simple rules for communication.
-> The control connection is made blw the control processes.

- Data connection

-> It uses very complex rules for communication.
-> The data connection is made between the data transfer processes.

Advantages

-> High speed.
-> more efficient.
-> Back and forth movement.

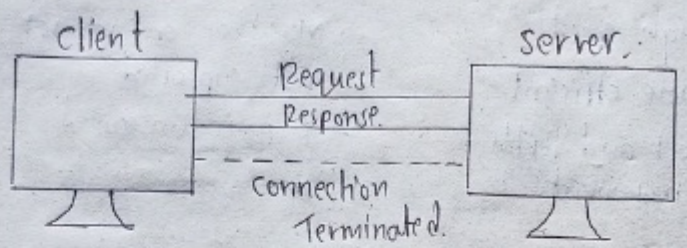
Disadvantages

-> More than one receiver not supported.
-> FTP is unsecured.

* HTTP (Hyper Text Transfer protocol)

-> HTTP stands for Hyper Text Transfer protocol.
-> Hyper text is sperially coded with standard coding language called Hyper Text markup language.
-> HTTP/2 is new version of HTTP and HTTP/3 is lastest version of HTTP.
-> The protocol used to transfer Hyper Text blw two computers is called HTTP.
-> HTTP is a set of rules for transfering data from one computer to another.
-> data included images, audio and video.
-> HTTP is similar to FTP.

-> HTTP



-> Above figure shows HTTP transcation b/w client and server.
-> The client initiates a transaction by sending a request to server.
-> The server replies to client by sending response to client.

o Features of HTTP

-> connection less protocol.
-> Independent.
-> stateless.

o Messages

-> HTTP messages are of two types namely
  o Request (sendy by client to server)
  o Response (send by server to client)

-> HTTP is a HTTP/IP based protocol.

o Advantages

-> Low memory usage.
-> less congestion.

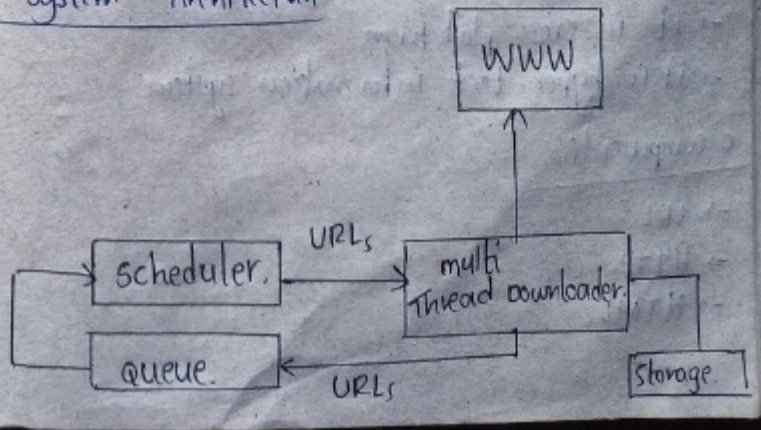
o disadvantages

-> High power required
-> less secure.

* www (world wide web)

-> www stands for world wide web.
-> www is commonly known as web
-> www is defined as collection of different websites around the world, containing different information via servers called www.
-> web pages are linked together using hyperlinks.
-> The data in the web may be text, audio, video and images.

o System Architecture



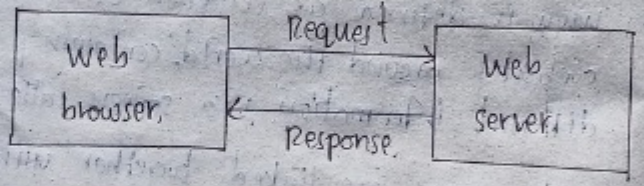
-> www Architechire consist of scheduler, queue, Multi thread downloader, www, storage etc.

-> The basic model of how web works shown in above figure.

-> A web browser is used to access the web pages.

-> web browser consist of text, data, pictures, audio, video.

-> working of www shown in below figure.



-> www operates similarly as client-server operation.

o Features

-> www is open source.
-> It is cross-platform.
-> It is hyper-text information system.

o components

-> URL
-> HTTP.
-> HTML.

o Advantages

-> Accessibility
-> communication and collaboration.

o Disadvantages

-> Information overload.
-> privacy and security.