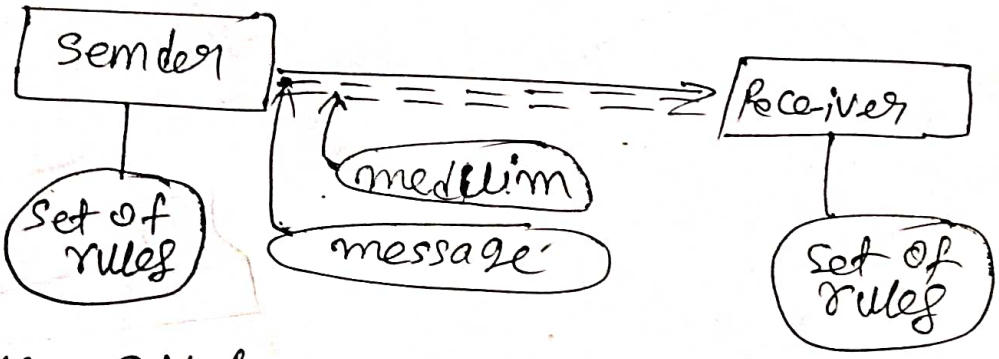
Computer Network = DCCN

Computer Network refers to the interconnected computer devices to exchange the data and to share the resources with each-other, connection can be a wireless or a wired, hardware and softwares are used to connect the computers.

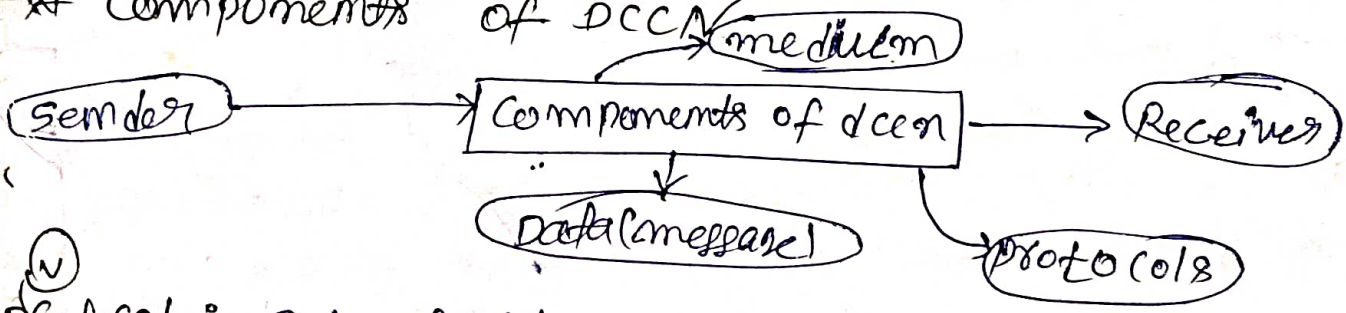
* DCCN devices are capable of sending & receiving the data over a communication medium.



imp Q.

* Define CN & DCCN, explain the components of dccn.

* Components of DCCN



(v) Protocol : Set of rules which we have to follow while communication, by using proper protocol communication becomes easy and more flexible.

(i) Message.
(ii) Sender.
(iii) receiver.
(iv) Transmission medium.
(v) protocols.

(1) Message: It is the information to be communicated by the sender to the receiver.

(ii) Sender: The sender is any device that is capable of sending the data.

(iii) Receiver: It is the device that the sender wants to communicate the data, and receiver receives the data.

(iv) Transmission Medium: It is the path by which the message travels from sender to receiver.

Define data flow or stream processing or re-active progra & types of dataflow ~~and~~ naming.

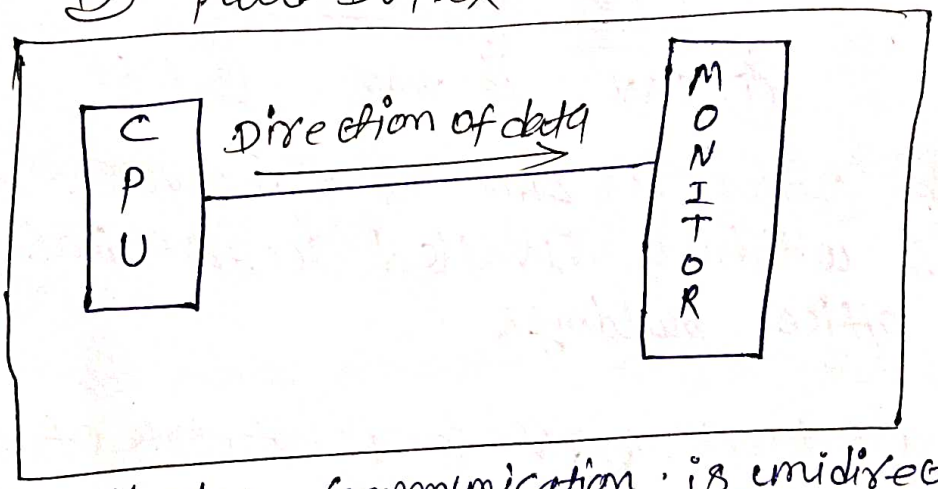
~~its goals with diagram~~.

ans ⇒ The Devices are Communicate with each other by sending and receiving data, this flow of data between two devices are called data flow.

Types of data flow

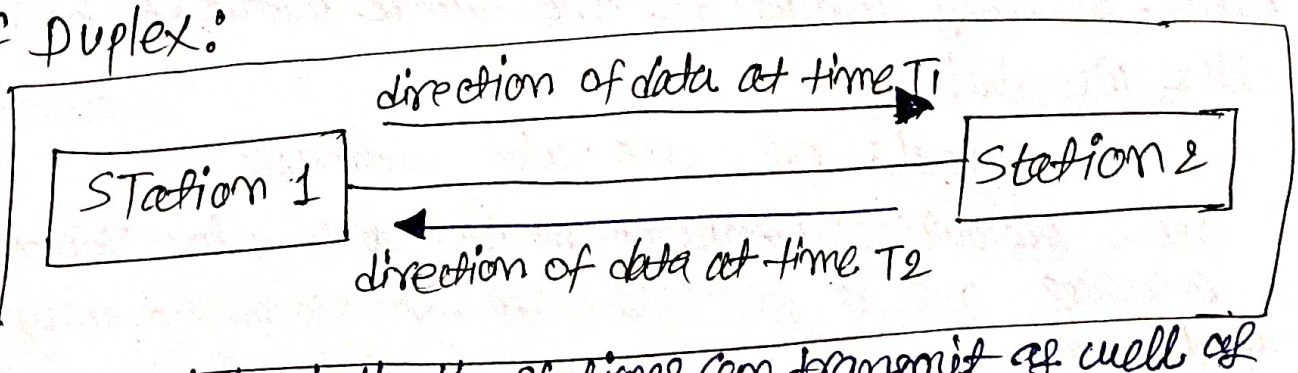
1. simplex
2. Half Duplex
3. full Duplex

(1) Simplex :



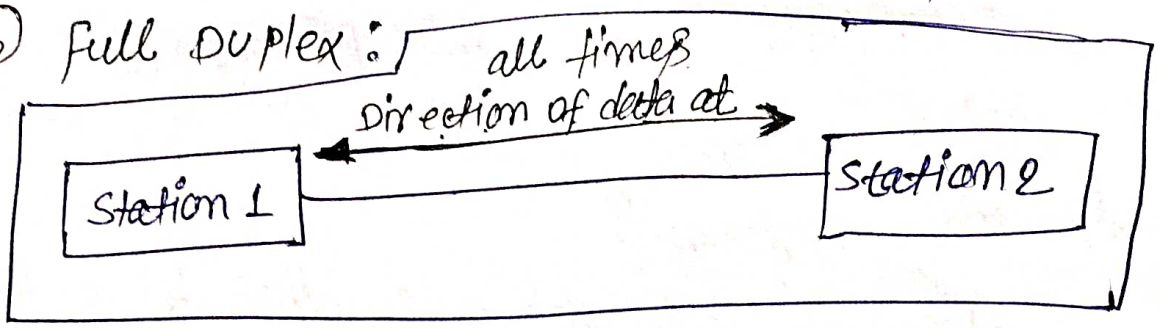
- In Simplex, communication is unidirectional
- only one of the devices sends the data and the other one only receives the data.
- Example: in ~~the~~ above diagram: a CPU send data while a monitor only receives data.

(2) Half Duplex:



- In half duplex both the stations can transmit as well as receive data but not at the same time.
- when one device is sending other can only receive and vice-versa
- A Walkie-talkie.

③ Full Duplex:



- In full duplex, both stations can transmit and receive data at the same time.
- Example: mobile phones.

* Explain the types of Network and its goals with ~~diagram~~ & with diagram.

Types of Networks

① LAN ② WAN ③ MAN

① Local Area Networks: LAN is a network of computers and devices within a limited geographical area, such as office, buildings.

② Wide Area Network: WAN is a network of computers and devices that spans a large geographical area. The network in the entire state of Maharashtra could be a WAN.

③ Metropolitan Area Network: MAN is of size between LAN & WAN. It is larger than LAN but smaller than WAN. It may comprise the entire network in a city like Mumbai.

Goals of computer network

① Share resources: Computer network allow you to share resources such as printers, scanners, storage devices, software application.

communication medium: Computer networks provide a plateform for communication and collaboration among users.

(iii) Be secure: Computer networks must be secure in order to protect user's data and privacy.

(iv). Remote access: Computer network allows users to access the data and application remotely.

(v) Person to person communication: Computer network can be used for person to-person communication through email, chat, and video.

(vi) ● List the difference applications of computer networks?
ans ⇒ (i) Communication (ii) Resource sharing (iii) Remote access (iv) Education (v) Healthcare (vi) Business (vii) Government (viii) [redacted] Research. (RRR) 3RBEGCH

(vii) Define Multiplexing: Multiplexing in computer networks is the technique of combining multiple signals from multiple sources into a single signal that can be transmitted over a single communication medium.

other words

Multiplexing is a way of sending multiple signals over a communication medium at the same time in the form of a single signal.

* Difference between interconnection and intraconnection networks.

Interconnection	Intraconnection
(i) A network that connects two or more separate networks.	(i) A network that connects different parts of the same network.
(ii) It allow ~~[illegible]~~ to communication and data sharing between different networks.	(ii) It allow communication and data sharing between different parts of the same network.
(iii) The internet is an example of an interconnection network.	(iii) A company's a internet is an example of an intraconnection network
(iv) Interconnection network can be complex and expensive to set up and maintain.	(iv) Intraconnection network can be difficult to manage and secure.

(*) What is an internet? write a brief history about internet & what do you consider an internet in todays life.

ans ⇒ Internet is a global network that connects billions of computers across the world with each other and to the world wide web. It uses standard internet protocol suite (TCP/IP) to connects billions of computer users worldwide.

brief history about internet

January 1, 1983 is considered the official birthday of the internet. In 1960s department of defense project that aimed to connects computers for research and communication. In the 1980s, the TCP/IP protocol suite was established, The world ~~wide~~ wide web invented

by Tim Berners-Lee in 1989, enabled the easy sharing of information through hypertext links. throughout the 1990s, the internet expanded globally. The 2000s saw the rise of social media, search engines, and e-commerce giants. Today, the internet is an integral part of modern life, connecting billions of devices and people worldwide.

Yes, I do consider the internet to be a basic necessity in today's life. It is used for so many different things from communication to education to entertainment. It is also becoming increasingly important for work and business.

* protocol

protocol: A protocol is defined as a set of rules that governs data communications. A protocol defines what is to be communicated, how it is to be communicated and when it is to be communicated.

Elements of a protocol

(A) Syntax: It is the arrangement of data in a particular order, it means the structure or formate of the data.

(B) Semantics: It also tells what action/decison is to be taken based on the interpretation, It tells the meaning of each section of bits and indicates the interpretation of each section.

(C) Timing: It tells the sender at what rate the data should be sent to the receiver to avoid overwhelming the receiver. It tells the sender about the readiness of the receiver to receive the data.

* Standards in network : Standards provide guidlines to product manufacturers and vendors to ensure national and international interconnectivity.

Classification of standards

(1) De facto standard : • These are the standards that have been traditionally used and mean by fact or by convention
• These standards are not approved by any organized body but are adopted by widespread use.

(2) De jure standard : • It means by law or by regulation.
• These standards are legislated and approved by an body that is officially recognized.

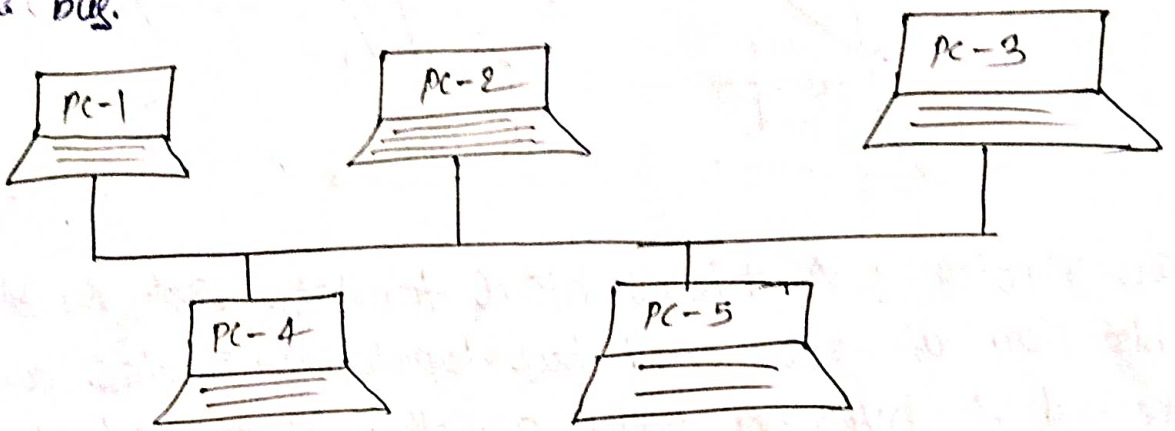
* difference between broadcast and point to point.

broadcast	point to point
(i) Information that is shared by all resources present on network.	
(i) number of senders can be more than one.	(i) number of senders only one.
(ii) no of receivers : All devices on the network.	(ii) only one device is receiver.
(iii) Network traffic is High.	(iii) Network traffic is low.
(iv) broadcast uses a special broadcast address.	(iv) uses a unique destination address.
(v) No response	(v) response
(vi) better utilization	(vi) utilisation is very high
(vii) 1 to all all to all	(viii) direct and dedicated links are used. → one to one.

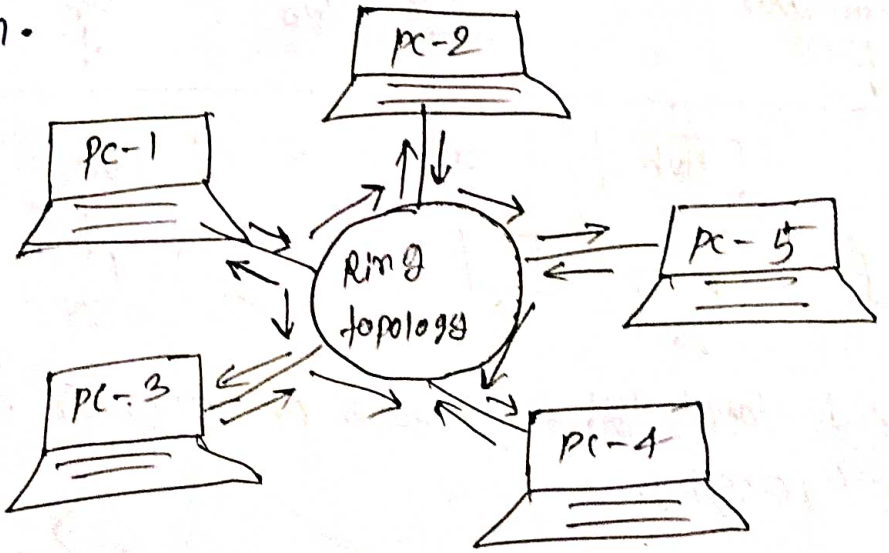
* Network topology: It is the physical & logical arrangement of nodes and connections in a network, nods can be switches, routers.

Types of Network topologies:

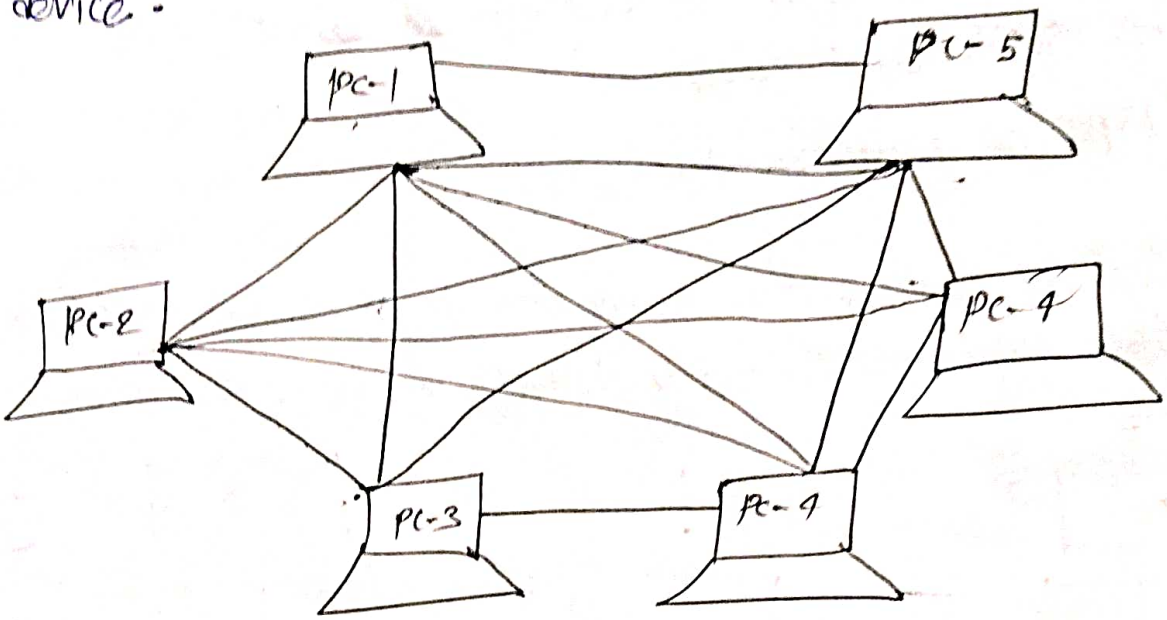
1. Bus topology: All devices are connected to a single cable, called the bus topology, data travels in both directions along the bus.



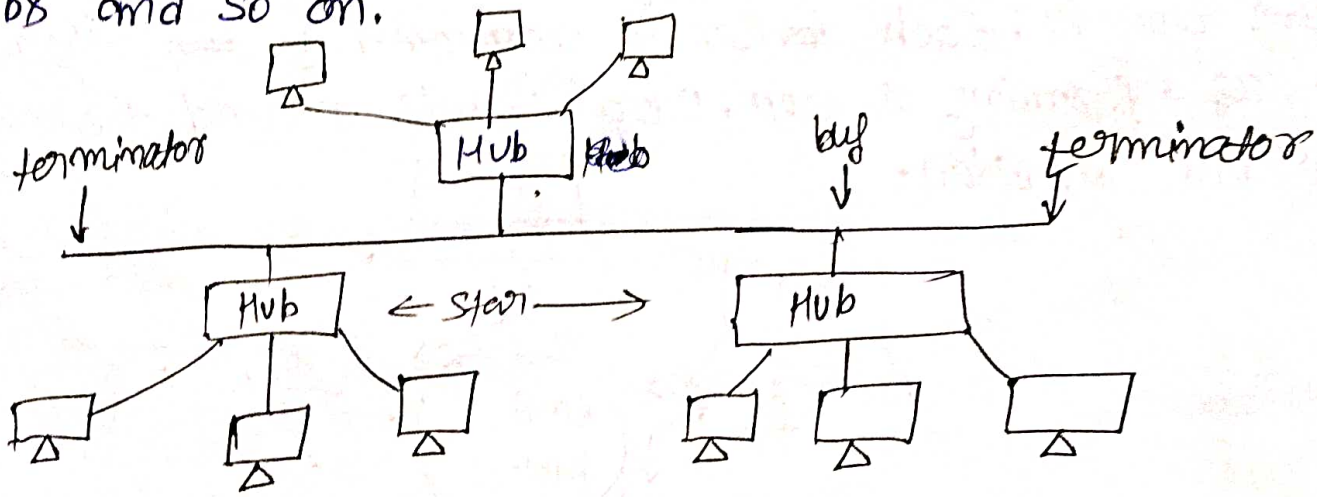
2. Ring topology: Each device is connected ~~to~~ ~~two~~ other devices, forming a loop, Data travels around the ring in one direction.



(3) • Mesh topology: Every device is connected to every other device.

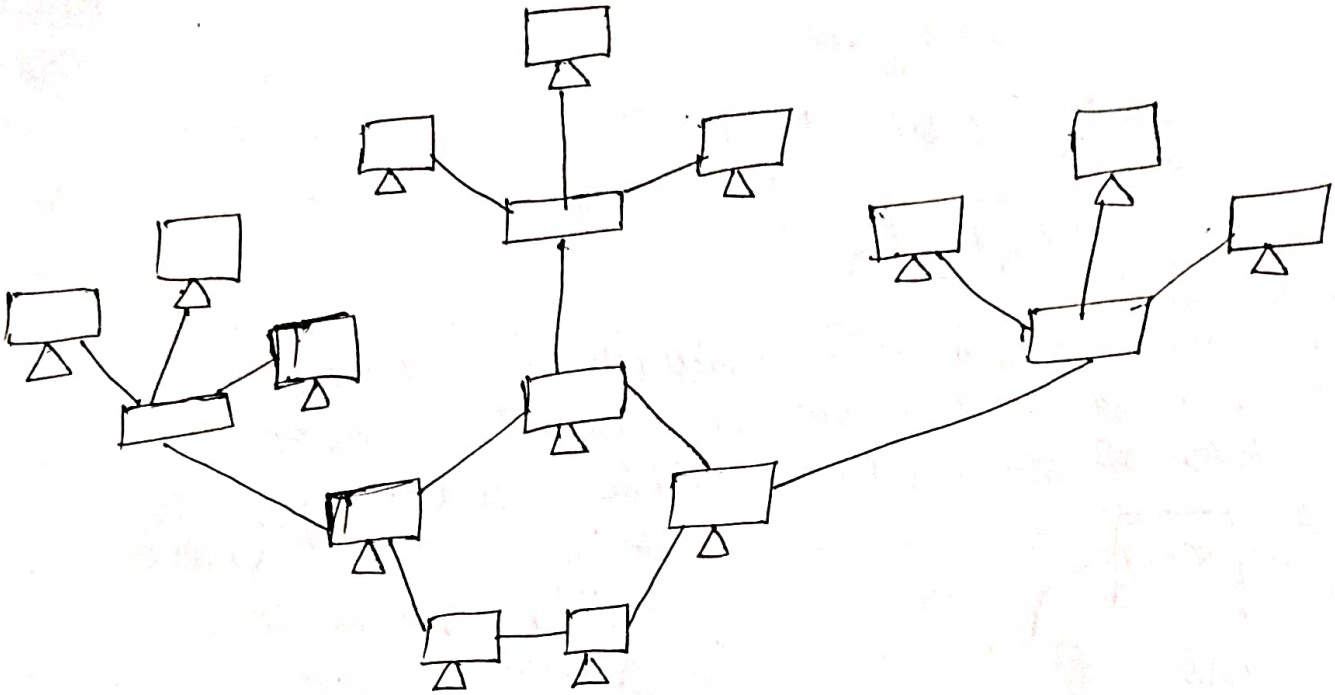


(4) • Tree Topology: A hierarchical topology ~~that~~. It is combination of star and bus topologies. Devices are connected to hubs ~~or~~ which are them connected to other hubs and so on.



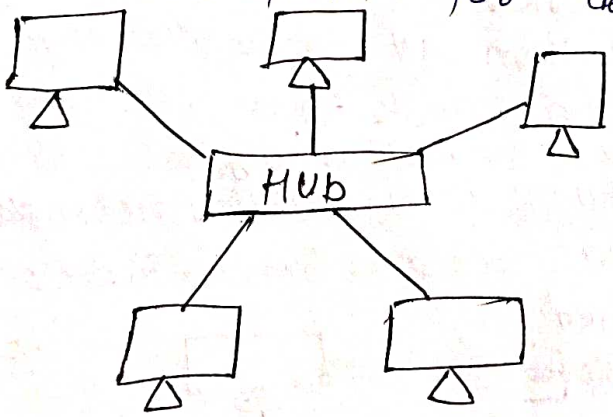
(5) • Hybrid topology: A Mixture of two or more types of topologies.

(5) Hybrid topology: A hybrid topology is combination of two or more different types of topologies. It is created by interconnecting multiple smaller topologies to form a large, more complex network.



(6) Point to point topology: It is a simple network topology in which two devices are directly connected to each-other.

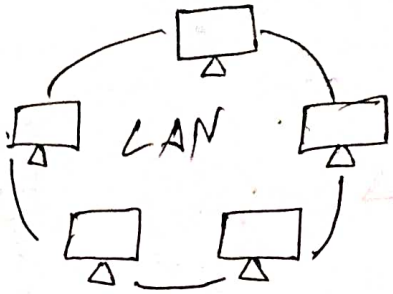
(7) Star topology: It is a central hub or switch is connected to all devices in the network. The hub acts as a central point for data communication.



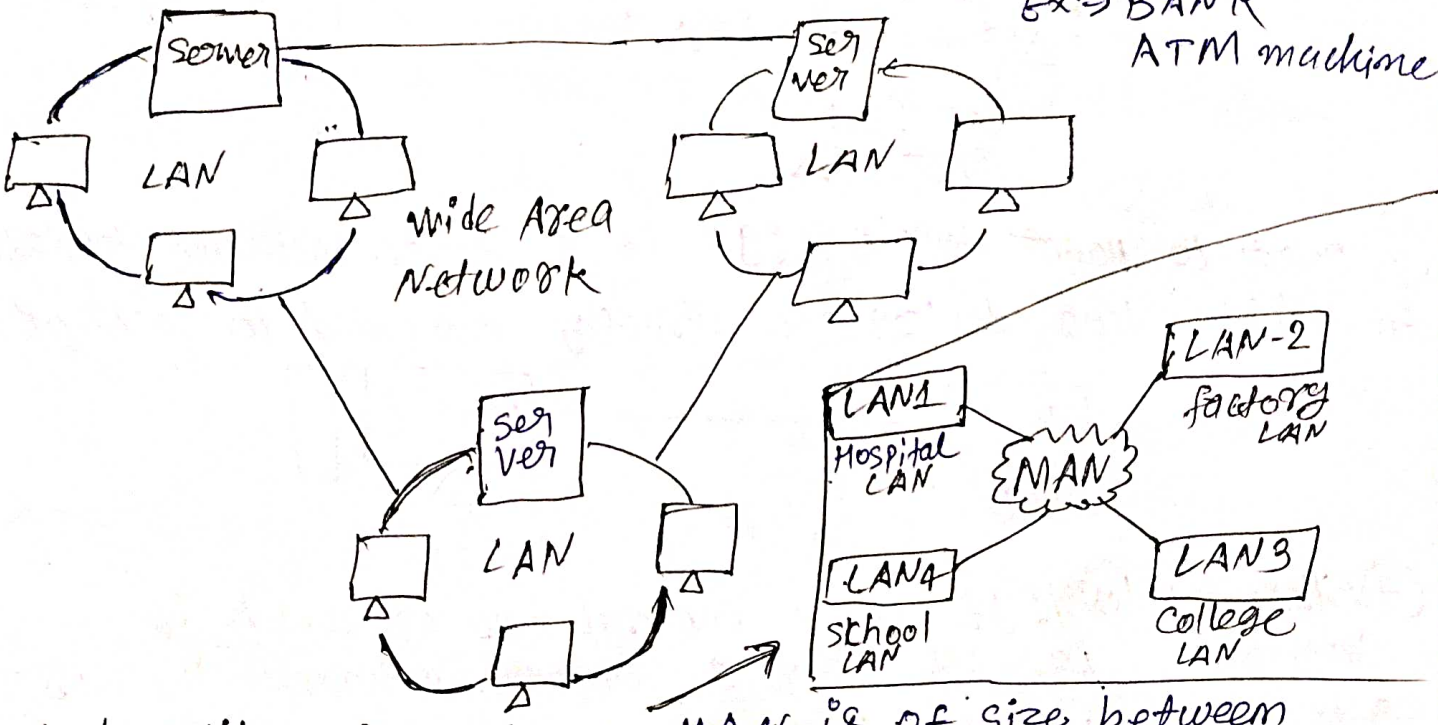
Types of Network

LAN MAN WAN PAN

① LAN: Local area network is a network of computers and devices within a limited geographical area, such as office, buildings.

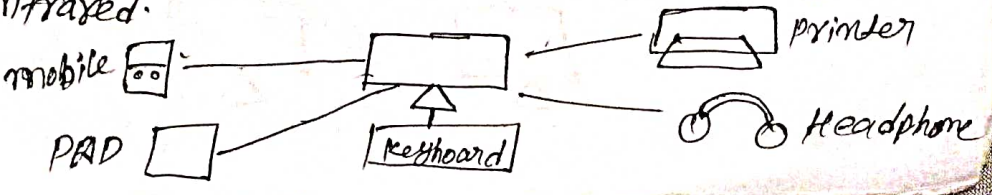


② WAN: Wide Area Network is network of computers and devices that spans a large geographical area. The network is the entire state of Maharashtra. Could be a WAN. Ex ⇒ BANK ATM machine



③ Metropolitan area network: MAN is of size between LAN & WAN. It is larger than LAN but smaller than WAN. It may comprise the entire network in a city like Mumbai.
Ex ⇒ cable TV network in city.

④ PAN: Personal area network is a computer network that connects devices within a limited area such as a home, office or vehicle. Such as Bluetooth, NFC, infrared.



Explain all the standards of the organization

ans →

ISO: Stands for "International organization for standardization". It is an organization to verify the quality of a product ~~the~~ during the development of the product. ISO 9001 specifie the quality management system means if you want to check a quality of a software product them you should use ISO 9001. ISO implicitly use the TQM (total quality management) technology to provide certificate for our organization based on quality of product.

IEEE: IEEE stands for Institute of electrical and electronics engineers. It is a non profit organization. It is world largest technical professional organization dedicated to advancing technology for the Benefit of himanity. IEEE purpose is to develops technological innovation and excellence for the benefit of humanity. IEEE is a trusted source of information and expertise in the field of technology.

ANSI: ANSI stands for American National Standards Institute is a private, non-profit organization that oversees the development of voluntary Consensus Standards for products, services, processes, system, and personnel in the united states. ANSI does not develop standards itself, but rather accredits the procedures of standards developing organization (SDOs) This ensures that the standards are developed in an open, transparent and inclusive manner with input form all stakeholders.

EIA: EIA stands for Electronic industries Alliance (EIA) was a trade association that developed standards for the electronics industry. It was is a nonprofit organization devoted to the promotion of electronics manufacturing concerns. EIA ~~stan~~ help to ensure that electronic products are compatible with each other and that they meet certain safety and performance requirements.

ITU-T: ITU-T stands for International Telecommunication union Telecommunication is a standards development organization that develops and publishes international standards for telecommunications and information ~~that~~ and Communications technologies.

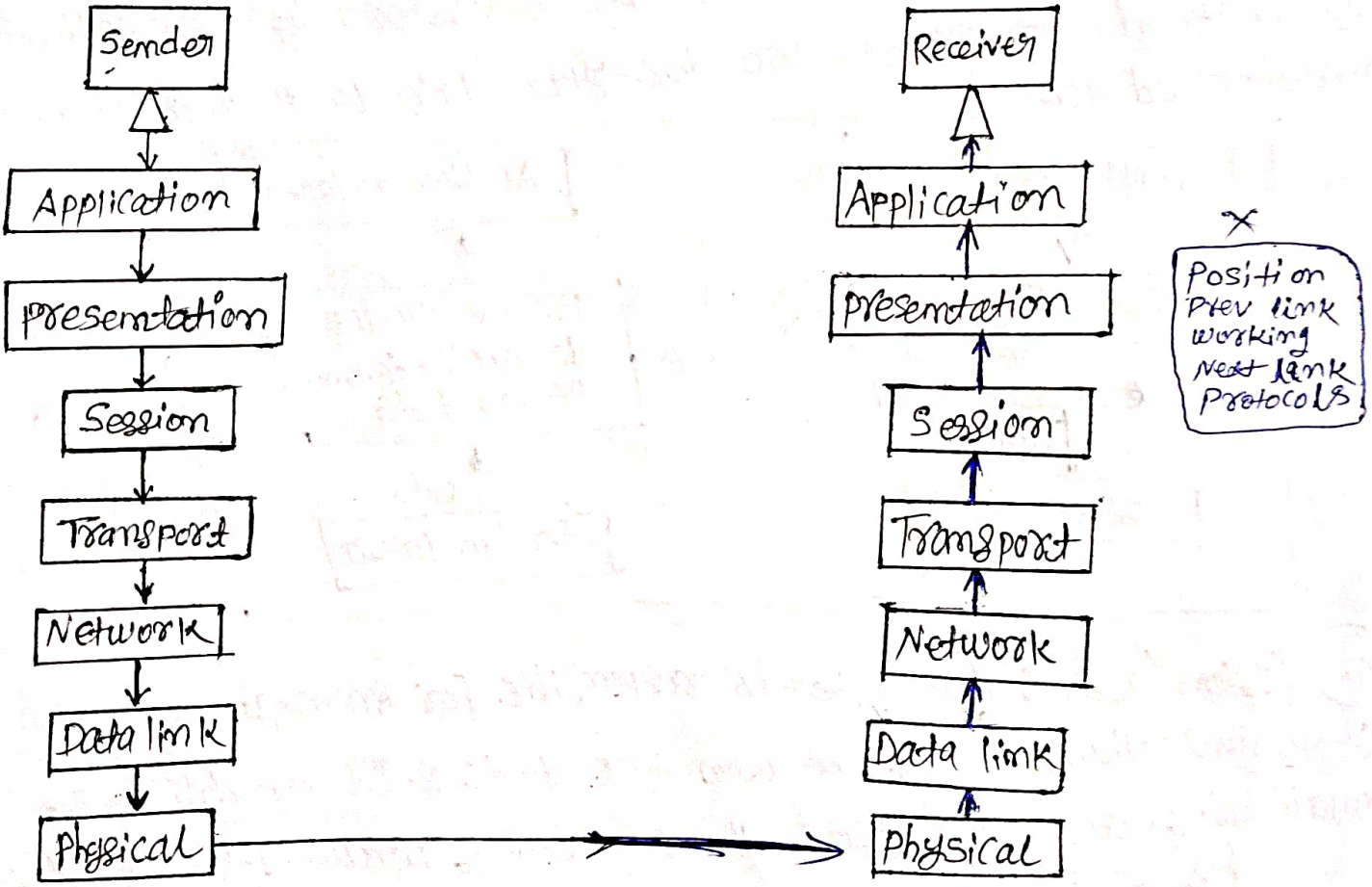
* Define Standards: A standard is a set of rules, guidelines or specifications that are used to measure or compare things. Standards can be used to ensure that products, services or processes are of a certain quality or to make sure that they are compatible with each-other.

(Pyq) List the different applications of computer networks?

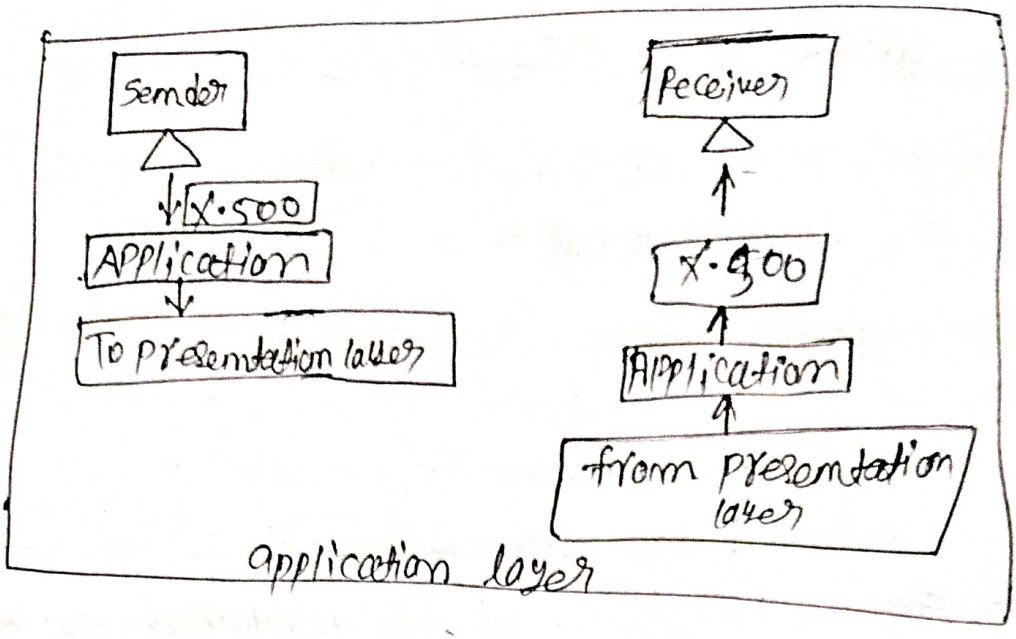
Ans ⇒ ① Communication ② file sharing ③ internet access ④ Remote access ⑤ Resource sharing ⑥ Entertainment ⑦ E-Commerce ⑧ Education ⑨ Telecommunication

Q Explain the working of OSI model using labeled diagram
or
Explain OSI Reference model in detail. Mention protocols of each layer of OSI reference model.

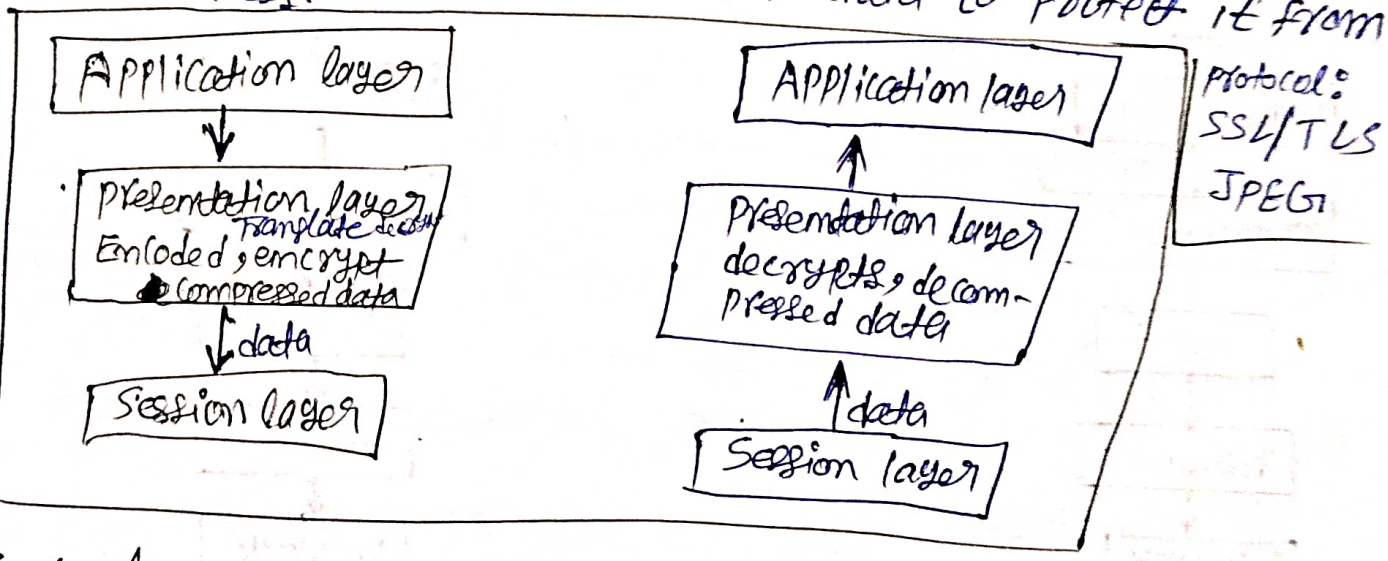
ans ⇒ OSI stands for (open systems interconnection) model. It is the framwork used to describe function performed in network system. It is a set of protocols which allows to use the communication between different kinds of system Regardless of an architecture and OSI model describe ~~the~~ how data moves between computers on a network. It devides the process into seven layers. OSI developed by ISO in 1984.



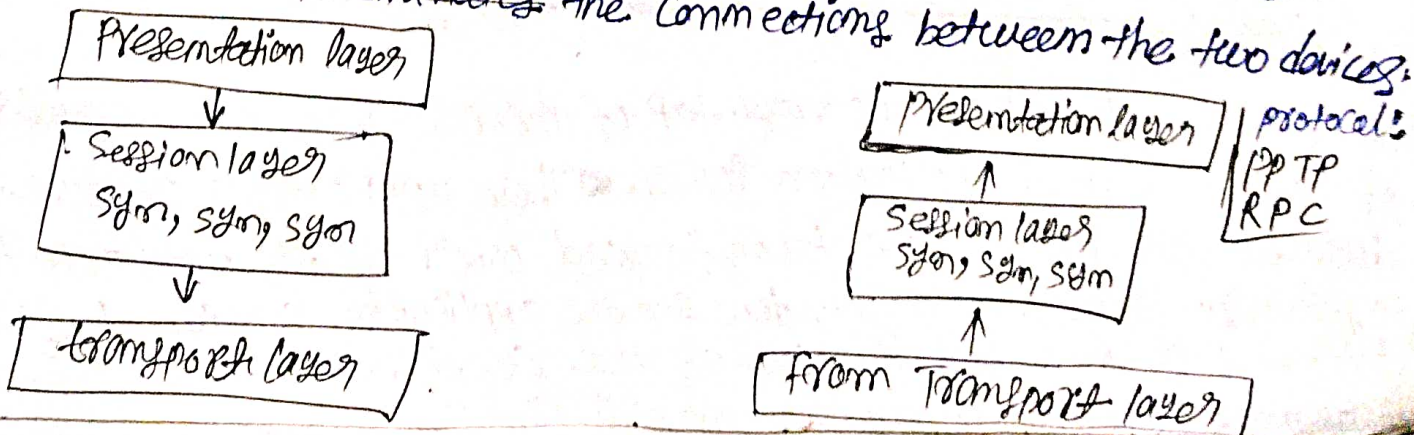
1. Application layer: At the very top of the OSI reference model stack of layers, we find Application layer, ● These applications produce the data, which has to be transferred over the the network. This layer also serves as a window for the application sewices to access the network and for displaying the received information to the user.
Example: Browers, Messenger. Protocol: HTTP, FTP, SMTP



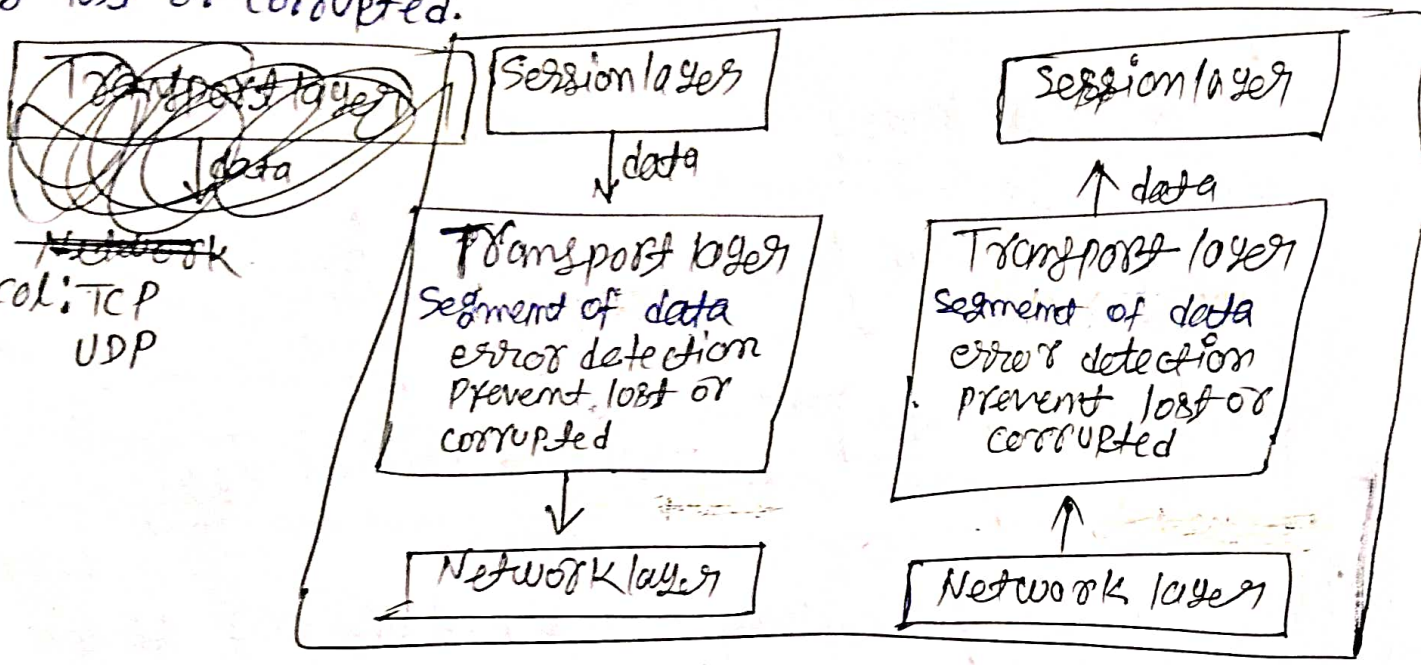
2. Presentation layer: The presentation layer is also called the Translation layer. This layer is responsible for formatting and translating data so that it can be understood by the application layer. It also encrypts and decrypts data to protect it from unauthorized access.



3. Session layer: This layer is responsible for managing the communication session between two devices. It establishes, maintains, and ~~terminates~~ synchronizes the connections between the two devices.

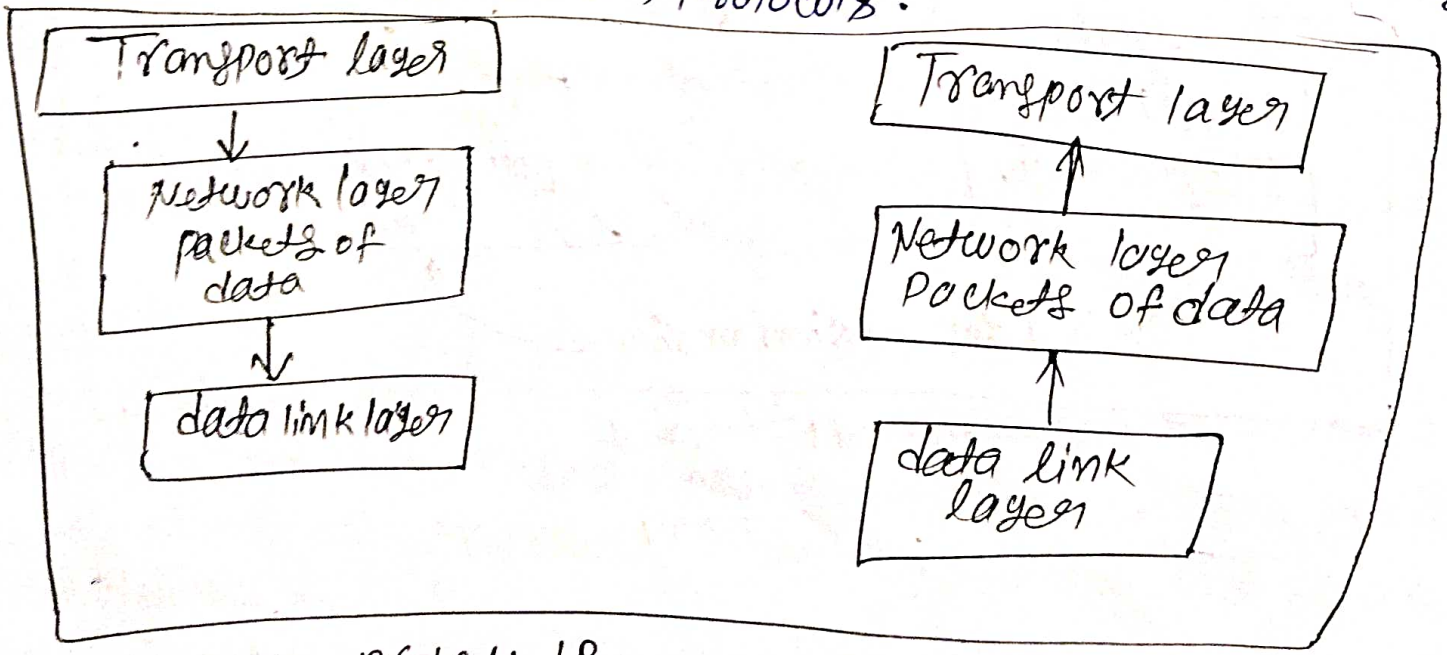


4. Transport layer: This layer is responsible for ensuring the reliable delivery of Segment of data, it provides error detection and correction as well as flow control to prevent data from being lost or corrupted.



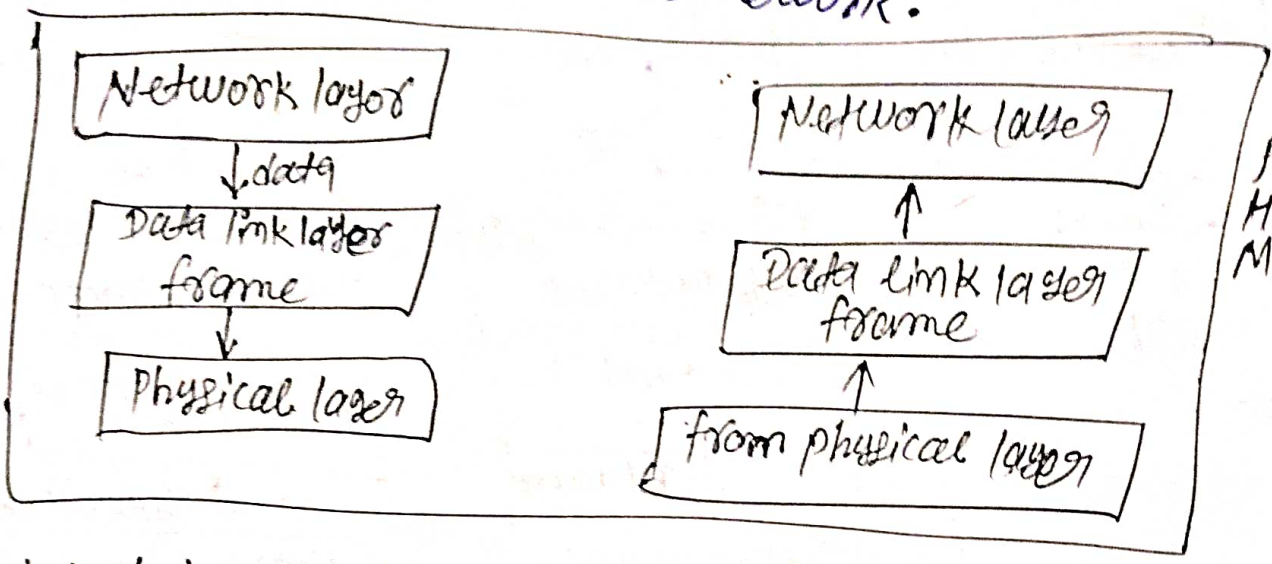
Protocol: TCP
UDP

5. Network layer: Network layer convert segment of data to data packets and transfer data packets from network layer to data link layer. It stores IP addresses, logical addressing, Routing, packet fragmentation, protocols.

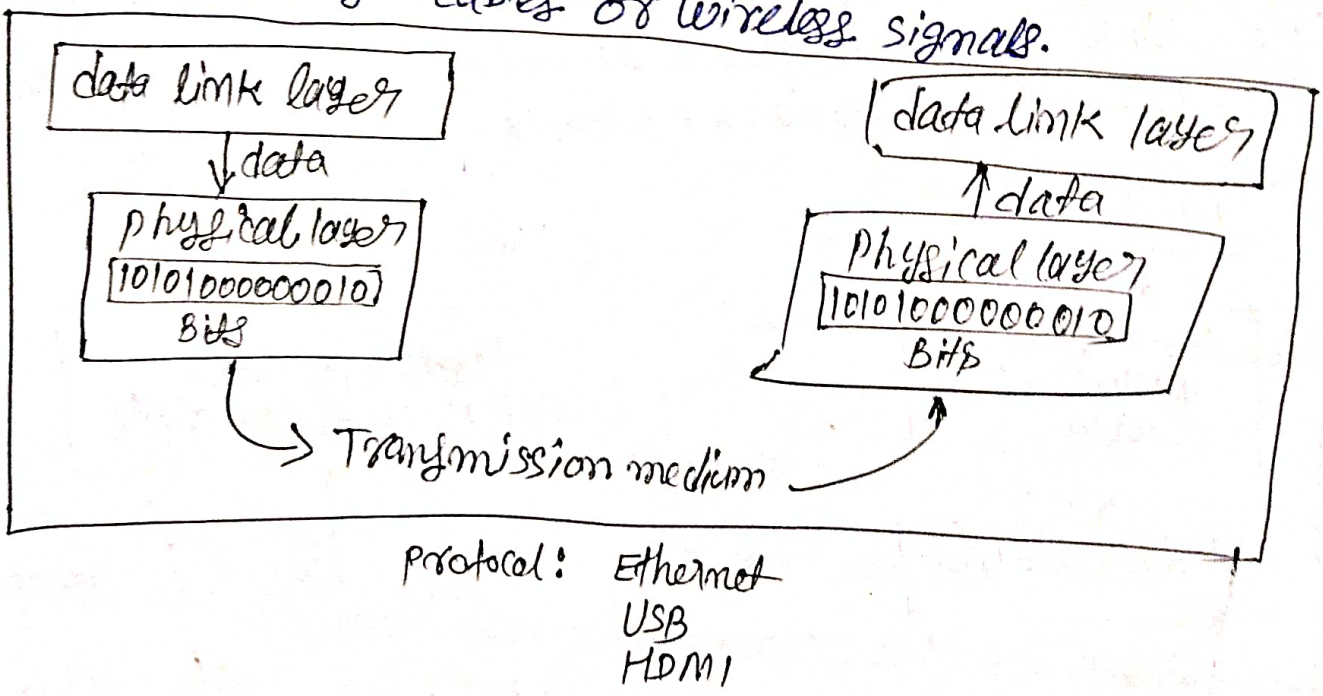


Protocal: IP
ICMP

(6.) Data link layer: Data link layer further ~~divided~~ divided the received ~~data~~ packets into frames. It handles error detection and correction. It also establishes and maintains the logical link between two devices on the network.



(7) Physical layer: The lowest layer of the OSI reference model is the physical layer. Physical layer converts data into bits. It responsible for transmitting individual bits from one node to the next node through cables or wireless signals.



Q. Why OSI is a reference modal.

ans ⇒ OSI model is considered a reference model because it provides a conceptual framework for understanding and standardizing the function of a telecommunication or networking system. It serves as a reference point to help people understand how different networking protocols and technologies interact within a networked environment.

→ in summary

OSI model is a reference model because, the OSI model provides a common language and framework for discussing and designing network protocols and systems, making it easier to develop and maintain complex networked environment.

* frame: frames can be a unit of communication, manageble data units are also frame.

* packets: A packet is a small unit of data that is transferred over a network. Packets are used to send data between computers, devices.

* define routing: Routing is the process of determining the best path for a packet to take from its source to its destination.

* define flow control: flow control is a mechanism that regulates the rate of data transmission between two nodes in a network. It prevents the sender from sending data too quickly.

* define error control: Error control is a machanism that detects and corrects errors in data transmission

* what do you mean by synchronisation of bits.

ans ⇒ Synchronization of bits is the process of enfuring that the sender and receiver of data are in sync with each other.

in other words:

The process of aligning the timing of the bits in a digital communication system.

* protocols: set of rules which we have to follow while communication, by using proper protocol Communication become easy and more flexible.

Types of protocol

(1) TCP/IP (2) HTTP (3) SMTP (4) POP (5) IMAP (6) UDP (7) PPP (8) FTP

Q. difference between TCP and UDP protocol.

TCP protocol	UDP protocol
(i) TCP is connection-oriented.	(i) UDP is connectionless.
(ii) TCP stands for: transmission control protocol.	(ii) UDP stands for User datagram protocol.
(iii) It is reliebe protocol.	(iii) It is not relieble protocol.
(iv) It is slower than UDP.	(iv) It is faster than TCP.
(v) It is used over long distance.	(v) It is used over short-distance.
(vi) The header size of TCP is 20 byte	(vi) The header size of UDP is 8 byteg.
(vii) Retransmission of lost packet is possible	(vii) Not possible.
(viii) Secure.	(viii) unsecure.
(ix) flow control.	(ix) No flow control.

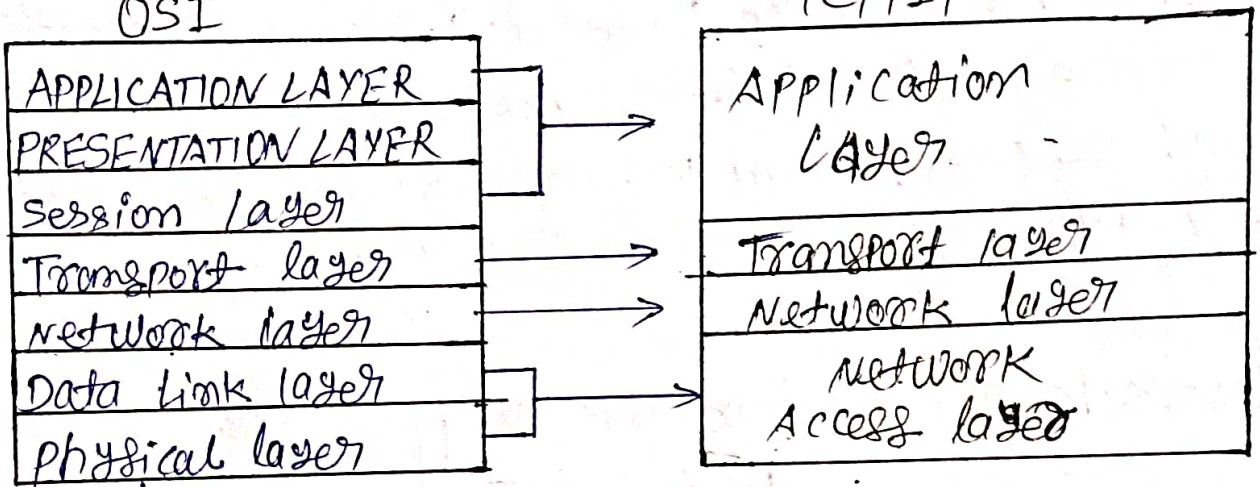
* Explain the working of TCP/IP model using labled diagram.

Introduction:-

ny→ TCP/IP stands for transmission control protocol/ Internet protocol, It is a communication protocols used to interconnect network devices on the internet.

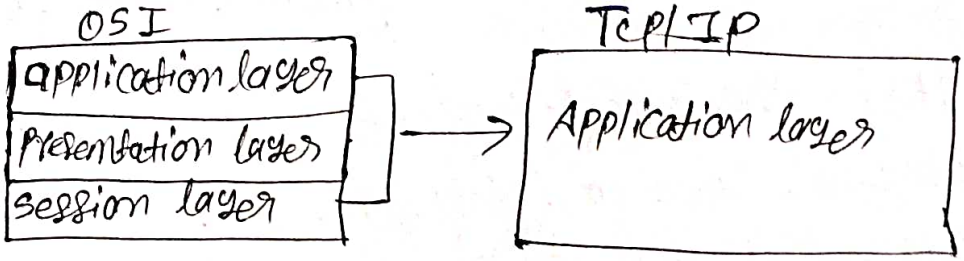
TCP/IP is also used as a communication protocal in computer network. TCP/IP specifies how data is exchanged over the internet by providing end-to-end communication that identify how it should be broken into packets, addressed, transmitted and received at destination. It consists four layers.

diagram:-



* Working

① Application layer:



→ Application layer is the topmost layer in the TCP/IP model. It is responsible for handling high level protocols issue of presentation. This layer allows the user to interact with the application. When one application layer wants to communicate with another application layer, it forwards its data to the transport layer.

② Transport layer: OSI [Transport layer] → TCP/IP [Transport layer]

* The transport layer is responsible for the reliability, flow
ng and, correction of data which is being sent over the netwo
or There are two protocols used in this layer (i) UDP (User Datagram) protocol (ii) TCP (Transmission control protocol). After that it forwards its data to Network layer.

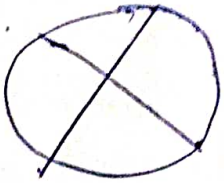
③ Network layer: OSI [Network layer] → TCP/IP [Network layer]

* Network layer also called Internet layer, It is the third layer of the TCP/IP Model and the main responsibility of this layer is to send the packets from any network, and they arrive at the destination no matter what path they take.

Q. ④ Network Access Layer: [Data link layer / Physical layer] → [Network Access layer]

(i) It is the lowest layer of TCP/IP Model. It is the combination of physical layer and data link layer which present in the OSI Model.
(ii) Co
(iii) Its main responsibility is to the transmission of information or data between two devices over the same network.
(iv)
(v)
(vi)
(vi)

Name – RAUSHAN KUMAR
CRN – 2221139
URN – 2203751
BRANCH – IT-B2



DCCN Assignment

Q1. Explain about application layer

ans ⇒ The application layer is the topmost layer in the OSI model and TCP/IP protocol suite. It provides interface between software applications.

1. User Interface: The application layer enables communication between software applications and end-users. It includes various protocols and services that allow application to interact with users, such as web browsers.

2. Data Exchange: This layer handles data exchange, formatting and presentation. It ensures that data sent or received by applications is properly structured and interpreted.

3. Error handling: The application layer may also include error handling and recovery mechanisms to ensure the reliable delivery of data between applications.

4. Interoperability: The applications layer ensure that different software applications running on different platforms and devices can communicate with each other.

5. Security: Security measures like encryption and authentication are often implemented at the application layer to protect the data exchanged between applications.

Q2. Define WWW

ans⇒ The world wide web (WWW), also known as the web, is an information system that uses the internet to link documents and other resources together. The WWW allows users to access and share information across the globe.

Q3 Define DNS

ans:- DNS stands for Domain Name System. It is a fundamental technology used on the internet that translates human-friendly domain names, like "example.com", into numerical IP (Internet Protocol) addresses, which computers use to identify each other on the network.

4Q Explain the protocols which are being used by email communication. (SMTP, POP3, IMAP, MIME)

ans⇒ Email communication relies on several protocols to work effectively.

1. SMTP (Simple Mail Transfer Protocol): SMTP is responsible for sending outgoing email messages from ~~server~~ a client to a mail ~~sever~~ server or between mail servers. It defines how mail clients communicate with email servers to send messages.

2. POP3 (Post Office Protocol version 3): POP3 is an email retrieval protocol. It allows email clients to download messages from a mail server to a local device such as a computer or smartphone.

3. IMAP (Internet Message Access Protocol): IMAP is another email ~~retrieve~~ retrieval protocol. Unlike POP3, IMAP allows email clients to access messages on the mail server without downloading them. This means you can access your email multiple devices and changes (read, delete, move) are synchronized across devices.

MIME (Multipurpose Internet mail Extensions): MIME is not a communication protocol itself, but rather a set of extensions to email protocols of multimedia content, such as images, audio, and video, within email message. MIME defines the structure and formatting of email messages.

Q5 Explain difference between OSI reference model and TCP/IP reference model.

OSI reference model	TCP/IP reference model
(i) It has 7 layers	It has 4 layers.
(ii) It is protocol-independent.	It is protocol-dependent.
(iii) It is more theoretical.	It is more practical.
(iv) Not widely used.	widely used.
(v) focuses on the functions of each layer.	focuses on the interaction between layers.
(vi) Designed for general-purpose networking.	Designed for the internet.

* Define WWW: WWW stands for world wide web, it is a huge collection of pages of information linked to each other around one globe, every page is a combination of text, picture, audio, video, animation & hyper link.

* DNS: DNS stand for Domain name system, it translates human readable domain names (Ex → www.xyz.com) into machine readable IP address. Ex (192.0.2.44)

(*) Differences between TDM and FDM.

TDM	FDM
(i) TDM stands for time division multiplexing.	FDM stands for frequency division multiplexing.
(ii) TDM works with digital signals as well as analog signals.	FDM works with only analog signals.
(iii) TDM has low conflict.	FDM has high conflict.
(iv) It is efficient	It is not efficient.
(v) in this time sharing takes place	In this frequency sharing take place.

(Pys) identify any four components used in the data communication system? ① Message ② Transmitter ③ Transmission medium ④ Receiver

(Pys) A host communicates with another host using the TCP/IP protocol suite. what is the unit of data sent or received at network layer?
ans ⇒ the unit of data sent or received is called "packet".

(Pys) List two differences in DNS and DHCP?

DNS	DHCP
(i) It assigns domain names to IP addresses, translating user-friendly domain name.	Dynamically assigns IP address and network configuration information to devices on a network.
(ii) It's responsibility to manages the mapping between domain names and IP addresses.	It handles the allocation of IP addresses dynamically.
(iii) DNS stands for Domain name system	(iv) DHCP stands for Dynamic Host configuration protocol.

Pyq When a party makes a local call to another party, is this a point to point or multiple connections? Comment and justify.

ans⇒ When a party makes a local call to another party, it tipically involves a point to point connection. In point to point connection there is a direct link between the calling and receiving parties. Creating a dedicated communication channel for the duration of the call.

Pyq Define connection oriented and connection less services. Give two computer applications of connections services.

ans⇒ • Connection oriented service: Connection-oriented service involve establishing a dedicated communication path before data transfer, ensuring a reliable and ordered delivery of the data.

Connection less service: Connectionless services transmit data without establishing a dedicated communication path, offering less reliability but often faster transmission.

Two Computer applications of connection oriented service.

① File Transfer protocal (FTP)

② Hypertext Transfer protocol (HTTP)

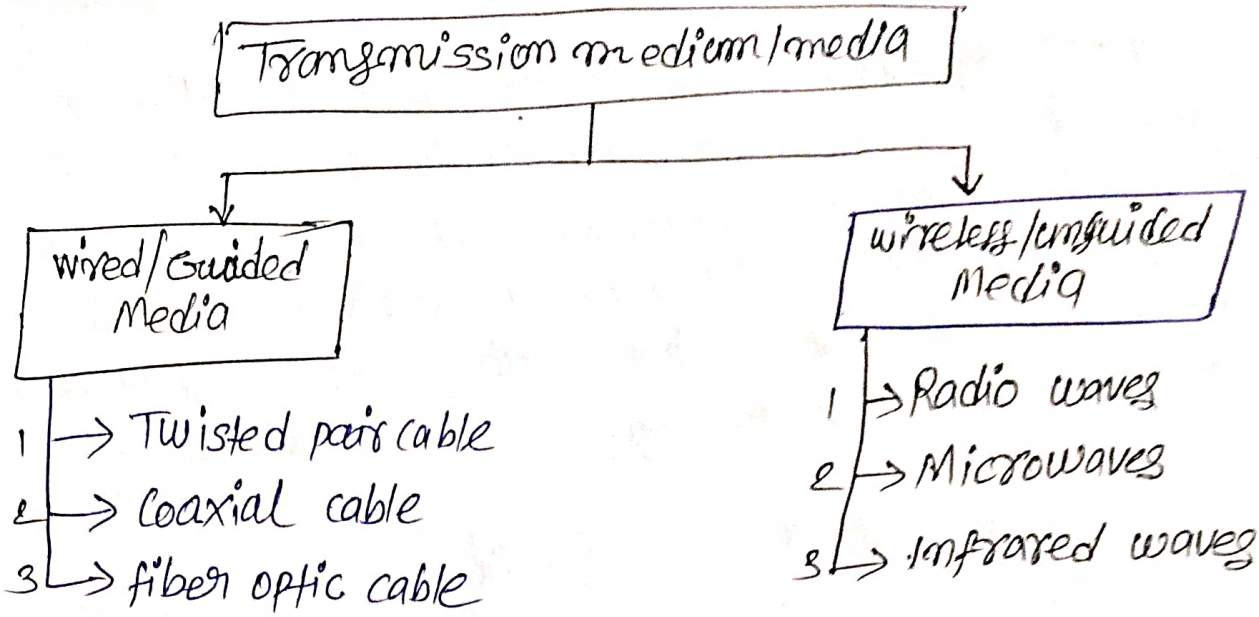
Two application of connectionless service

① voice over internet protocal ② online Gramming ③ Video streaming

(Pyq) Explain shielded Twisted Pair and un-shielded twisted pair.

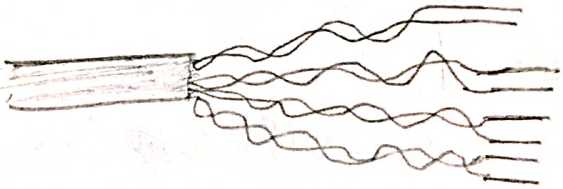
Shielded twisted pair	un-shielded Twisted pair
(i) STP has a metal foil covering	(i) UTP does not have a metal foil covering.
(ii) STP gives better resistance to electromagnetic interference.	(ii) UTP does not provide better resistance to electromagnetic interference.
(iii) STP is little expensive than UTP	(iii) UTP is less expensive than STP.
(iv) Grounding is possible.	(iv) Grounding is not possible.
(v) Distance travelled is large	(v) Distance travelled is less
(vi) It can be used in MAN.	(vi) It can be used in LAN.

(Pyq) Explain Ethernet: Ethernet is a technology for connecting devices in a wired local area network (LAN). It enables devices to communicate with each other via a protocal.

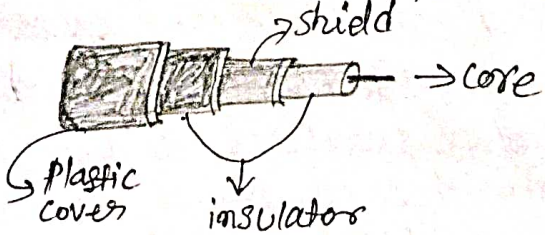


* Transmission media: Transmission medium is the way in which data is transmitted from one place to another place. It provide a path over which the message in form of binary digits can travel from sender - receiver.

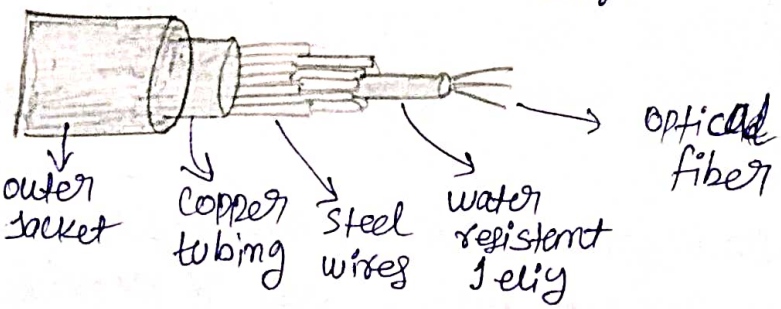
*(1) Twisted pair cable: A twisted pair cable is a pair of copper wires which are most common wires used for transmitting signals because of good performance at low costs. A twisted pair cable consists of two conductors, each with its own plastic insulation, twisted together to form a single media, these cables are color coated.



(2) Coaxical cable: Coaxical cables are copper cables with better shielding than twisted pair cables, so that transmitted signals may travel longer distances at higher speeds. It is the primary types of cabling used by the cable television industry and it is also widely used for computer networks such as ethernet.



(iii) Fiber optics cable: A fiber optic cable is made of high quality of thin glass or plastic used to transfer digital data signals in form of light up to distance of thousand of miles. Fiber optic cables have a much high bandwidth than metal cables. This means that they can carry more data. It is thiner than human hair.



(iv) Radio waves: Radio waves are electromagnetic waves that have wavelengths between 1 millimetre to 100 kilometer. Radio waves are generated by radio transmitters and received by radio receivers. It can penetrate walls easily so these waves are widely used for communication both indoors and outdoors. It is used in mobile, FM radio, television.

(v) Micro waves Transmission:

Microwaves are a type of radio waves with high frequencies. It can be classified as a subclass of radio waves. microwaves are unidirectional, in which the sending and receiving antennas need to be aligned. Microwaves are widely used for point-to-point communication.

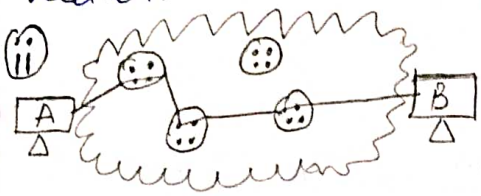
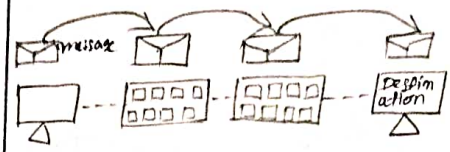
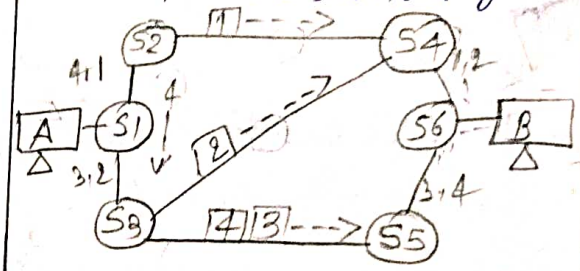
(vi) Infrared ~~signals~~ waves: Infrared signals have frequencies between 300 GHz to 400THz. They are used for short-range communication. Like TV remote, wireless speakers, Automatic doors due to short range communication, the use of an infrared communication system in one room will not be affected by the use of another system in the next room. This is why using an infrared TV remote control.

* Differentiate among Twisted pair, Coaxial cable and fiber optices transmission media.

Twisted pair cable	Coaxial cable	fiber optics cable
(i) Transmission of signals over the metallic conducting wires.	Transmission of signals over the inner conductor of the cable.	Transmission of a signal over a glass fiber
(ii) In this medium the noise immunity is low.	In this medium noise immunity is higher.	At this medium noise immunity is higher.
(iii) cheapest cable.	Moderate cable.	Expensive cable.
(iv) low bandwidth.	Moderately high bandwidth.	very high bandwidth.
(v) Attenuation is very high.	Attenuation is low.	Attenuation is very low.
(vi) Installation is easy.	Installation is fairly easy.	Installation is difficult.
(vii) It can be affected due to external magnetic field.	It can be less affected due to external magnetic field.	Not affected by the external magnetic field.

~~* Explain the shielded twisted pair (STP).~~

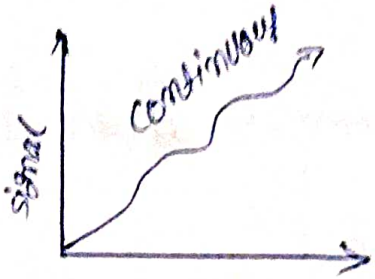
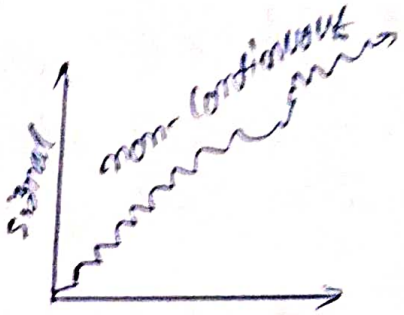
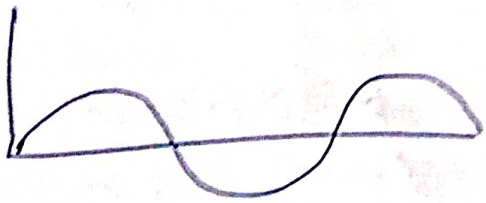
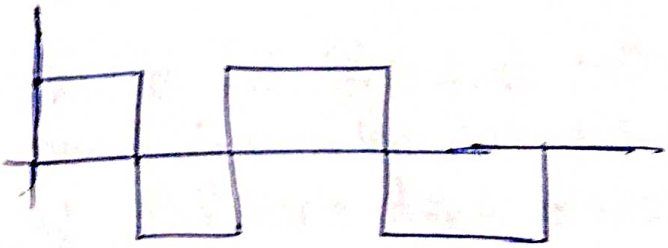
* Difference among circuit switching, Message Switching and packet switching. *

circuit switching	Message switching	packet switching
(i) circuit switching is a method of transmitting data in which a dedicated path is established b/w sender & receiver.	Message switching is a method of transmitting data in which messages are sent as complete units from one node to another.	packet switching is a method of transmitting data in which message are divided into smaller units called packets switching.
(ii) 		
(iii) There is Physical connection b/w transmitter and receiver.	No Physical path in set advance b/w transmitter and receiver.	No Physical path is established b/w transmitter and receiver.
(iv) Need of end to end path before the data transmission.	No need of end to end path before data transmission.	No need of end to end path before data transmission.
(v) waste of bandwidth is possible.	No waste of bandwidth	No waste of bandwidth
(vi) It cannot support store and forward transmission.	It support store and forward transmission.	It support store and forward transmission.
(vii) Not suitable for handling interactive traffic.	Suitable for handling interactive trafic	Suitable for handling interactive trafic

Explain Unshielded twisted pair (UTP):

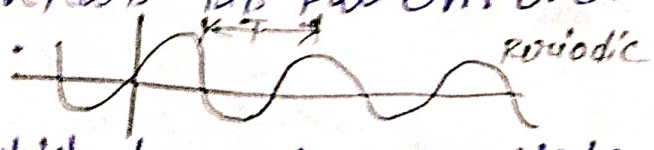
*

* 5 difference between analog and digital signal.

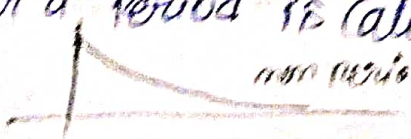
Analog	digital
(i) Continious signals.	Discrete time signals.
(ii) It represent physical measurement.	They are being generated by digital modulation.
(iii) They have continuous electrical signal.	It have non-continuous signal.
(4) 	
(5) It is used in only analog device.	It is used in computers, mobiles & many more.
(6) Analog data & signals	digital data & signals.
(7) Infinite value.	limited values
(8) It has sine wave. 	It has square wave. 

* Define periodic signal & Non-periodic signals:

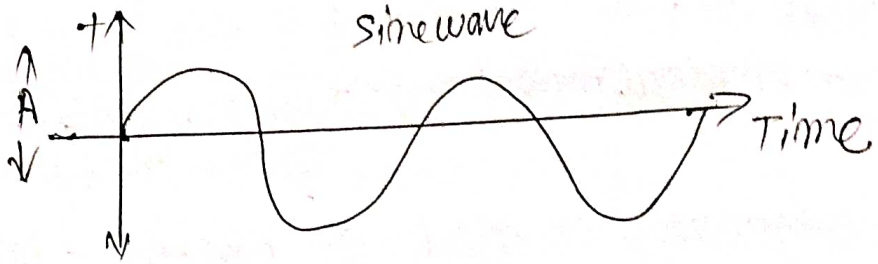
Periodic signal: A signal which repeats itself after a specific interval of time and it repeats its pattern over a period is called periodic signal.



* Non periodic signals: A signal which does not repeat itself after a specific interval of time and it does not repeats its pattern over a period is called non periodic signal.



* Define Sinewave: A sinewave is a geomatic waveform that oscillates (up & down, or side to side) periodically, and it is defined by the function $y = \sin x$

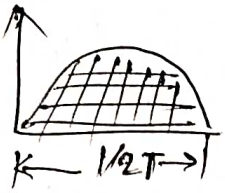


* Define Period and frequency:

Period: Periods refers to the amount of time, in seconds, a signal needs to complete 1 cycle. $T = \frac{1}{f}$

frequency: frequency refers to the number of cycles completed by the wave in one second. $f = \frac{1}{T}$

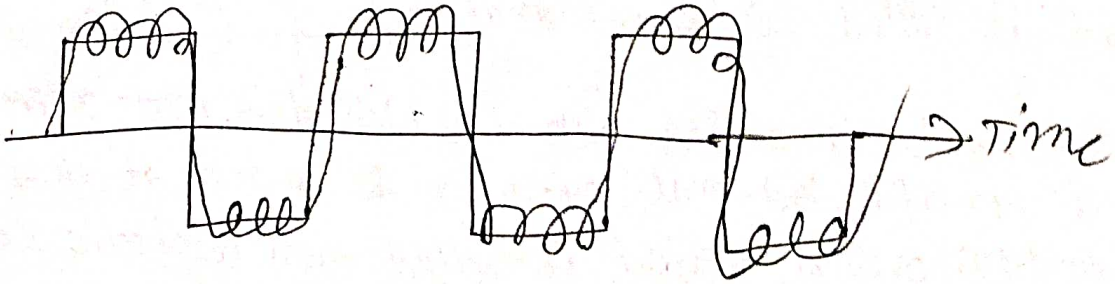
* Define phase: Phase describes the position of the waveform with respect to time.



* Define wavelength: The wavelength of a signal refers to the relationship between frequency and propagation speed of the wave through a medium.

$$\text{Wavelength } (\lambda) = \text{propagation speed} \times \frac{1}{\text{frequency}}$$

* Define composite signal: A composite signal is combination of two or more simple sine waves with different frequency.



Define bandwidth: Bandwidth refers to the maximum data transfer rate or capacity of a network communication channel is called bandwidth, it is typically measured in bits per second (bps).

in other words:

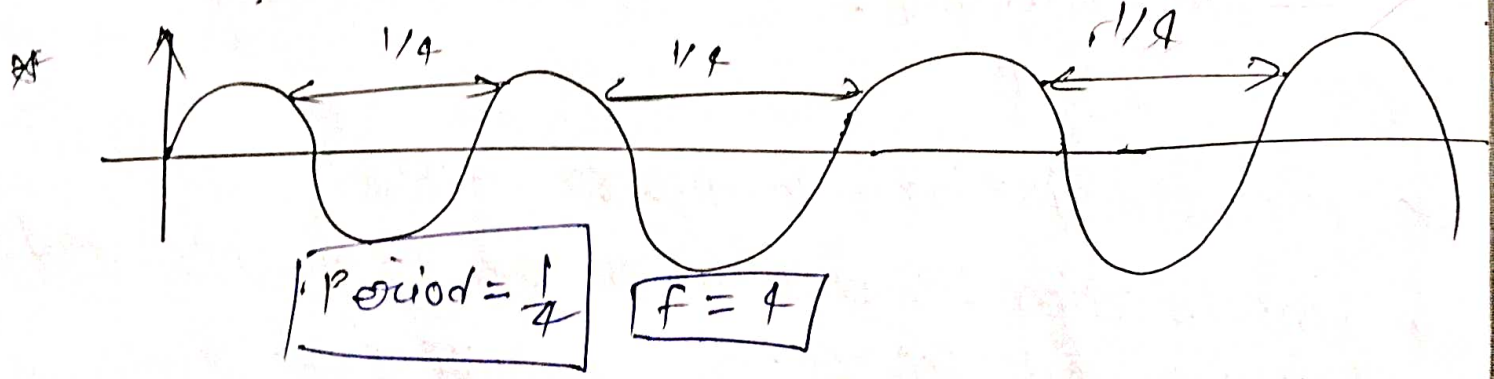
Bandwidth is difference between two numbers:

Note = Capacity = bandwidth $\times \log_2(1+SNR)$

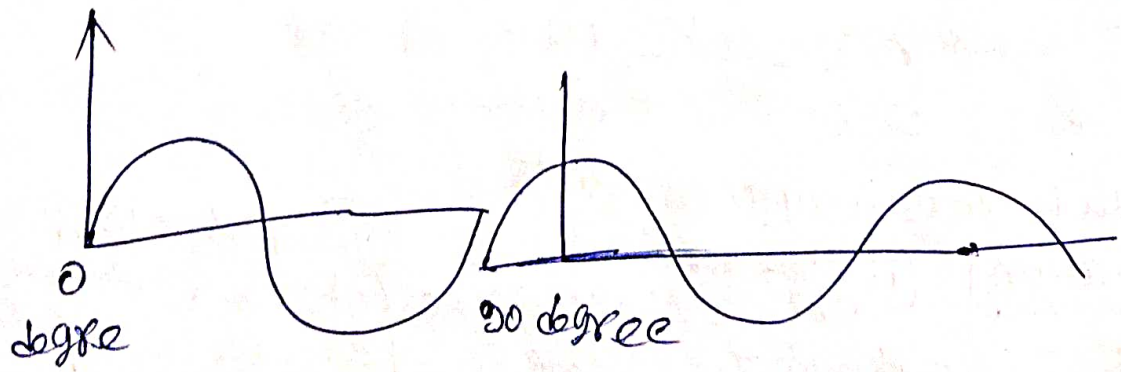
BitRate = $2 \times$ bandwidth $\times \log_2 L$

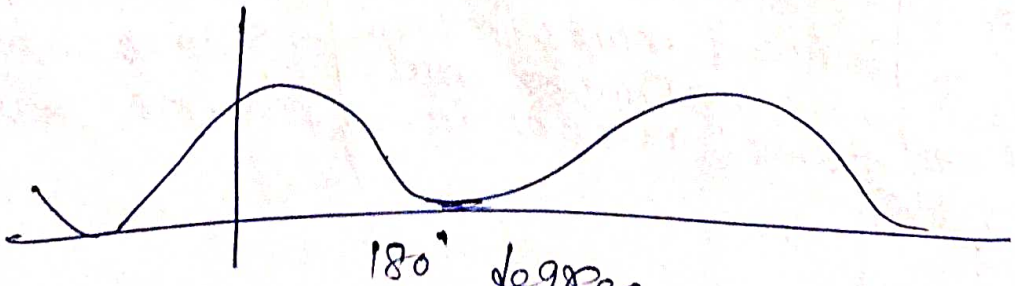
* The power we use 60Hz the period of sinewave can be determine.

$T = \frac{1}{F}$ $T = \frac{1}{60}$ $T = 0.01s$



Period = $\frac{1}{4}$ $f = 4$





* A sinewave width 1/6 cycle with respect to time what is the phase in degree & radian.

ans ⇒ $P = \frac{1}{6} \times 360$ $\boxed{P = 60^\circ}$

in radian

$\frac{60 \times 2\pi}{360} = \frac{\pi}{3}$ radian.

* Time domain, freaumy domain

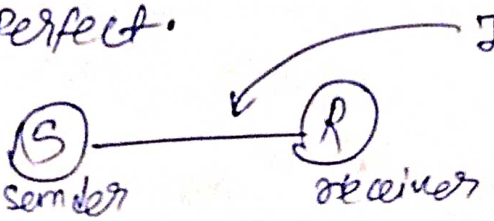
Time domain can be used to analyze a wide range of signals, including audio signals, video signal and even biological signals.

freaumy domain refers to the analysis to freaumy, rather than time.

* New

* Transmission impairment.

* imperfection: signal which are travelling and which are not perfect.



Three causes for impairment

(i) Attenuation → loss of energy

Electrical → Heat

when a signal travels through a medium, it loses of its energy in overcoming the resistance of the medium.

(ii) ~~loss of energy~~ noise: Noise can be a thermal noise or induced noise, induced noise is of motor and thermal noise of electrical

(iii) distortion

change of form or shape.

→ signal changes its form or shape.

* Data Ratelimit: • There are three factors of DRL.

① Bandwidth
② Level of signals
③ channel quality (the level of noise)

formula to calculate the data rate.

① • Nyquist for a noiseless channel
② • Shannon for noisy channel.

① $\boxed{\text{BitRate} = 2 \times \text{Bandwidth} \times \log_2 L}$ for noise channel (Nyquist)
(unit bps) ↳ how many signal levels we need.

② Shannon capacity: $\boxed{\text{capacity} = \text{bandwidth} \times \log_2 (1 + \text{SNR})}$ upper limit
unit → bps

$\boxed{\text{SNR} = \text{Avg signal power} / \text{avg noise power}}$

Note: ① A noiseless channel has a bandwidth of 4000 Hz and its transmitting a signal with two signal levels. calculate the maximum bit rate.

ans → formula ⇒ Bitrate = 2 × bandwidth × $\log_2 L$
given: b = 4000 Hz, L = 2
Bitrate = 2 × 4000 × $\log_2 2$ (1)
= 2 × 4000
= 8000 bps.

② Consider a noiseless channel with a bandwidth of 20 KHz, we need to send 280 Kbps over a channel. How many signal levels are required?

ans ⇒ given: b = 20 × KHz
Br = 280 Kbps

Note bandwidth unit → Hz

$br = 2 \times b \times \log_2 L$
$280 = 2 \times 20 \times \log_2 L$
$7 = \log_2 L$
$\log_2 L = 7$
$L = 2^7$
$\boxed{L = 128 \text{ levels}}$

$\boxed{\log_e x = y}$
$\boxed{x = e^y}$

Q1. Consider a extremely noisy channel in which signal to noise ratio is almost zero. calculate the capacity of the channel.

$C = B \times \log_2(1+SNR)$ { given $\therefore SNR = 0$

$C = B \times \log_2(1+0)$ { $\log_2 1 = 0$

$C = B \times 0$

$\boxed{C = 0}$

Note → Highest bitrate → capacity
Appropriate bitrate → capacity

Q2. Calculate the highest bit rate (capacity of channel) if the bandwidth is 3000Hz and signal to noise ratio (SNR) is 3162

ans: given $B = 3000\ Hz$ $SNR = 3162$

$\boxed{B = 3\ KHz}$

$C = B * \log_2(1+SNR)$

$C = 3000 * \log_2(1+3162)$

$C = 3000 * \log_2(3163)$

$C = 3000 * 11.627$

$\boxed{C = 34881\ bps}$

$\log_2(3163) = \frac{\log(3163)}{\log 2} = \frac{3.50}{0.30} = 11.627$

F.Q we have a channel with a 1-MHz bandwidth. The SNR for this channel is 63. what is the appropriate bit rate and signal level?

ans ⇒ given ⇒ $B = 1 \times 10^6\ Hz$

$SNR = 63$

$C = B * \log_2(1+SNR)$

$C = 10^6 \times \log_2(1+63)$

$C = 10^6 \times \log_2(64)$

$C = 10^6 \times \log_2 2^6$

$C = 10^6 \times 6 \times \log_2 2$ — 1

BR → $\boxed{C = 6 \times 10^6\ bps}$

level is

$BR = 2 \times B \times \log_2 L$

$6 \times 10^6 = 2 \times 10^6 \times \log_2 L$

$\frac{6 \times 10^6}{2 \times 10^6} = \log_2 L$

$3 = \log_2 L$

$\log_2 L = 3$

$L = 2^3$

$\boxed{L = 8\ levels}$

Note: $SNR_{dB} = 10 \log_{10} SNR$ decibal

$$\frac{SNR_{dB}}{10} = \log_{10} SNR$$

$$SNR = 10^{SNR_{dB}/10}$$ ← this will use in ℙ

F.ℙ → Calculate the capacity of the channel with SNR of 36dB and bandwidth of 2 MHz.

given: $SNR_{dB} = 36$ $B = 2 \times 10^6$ Hz . $C = ?$

$$C = B * \log_2 (1 + SNR)$$

$$\because SNR = 10^{SNR_{dB}/10} \Rightarrow SNR = 10^{36/10} \Rightarrow SNR = 10^{3.6}$$

$$SNR = 10^{3.6} \Rightarrow SNR = 3981.07$$

$$C = 2 \times 10^6 \times \log_2 (1 + 3981.07)$$

$$C = 2 \times 10^6 \times \log_2 (3982)$$

$$C = 2 \times 10^6 \times \log_2 2^{11.96}$$

$$C = 2 \times 10^6 \times 11.96 \times \log_2 2$$

$$C = 2392 \times 10^4 \text{ bps}$$

~~Approx = 3978.6~~

$$\because 2^{11.96} = 3985$$

bit rate = 2 × Bandwidth × $\log_2 L$

capacity = Bandwidth × $\log_2 (1 + SNR)$

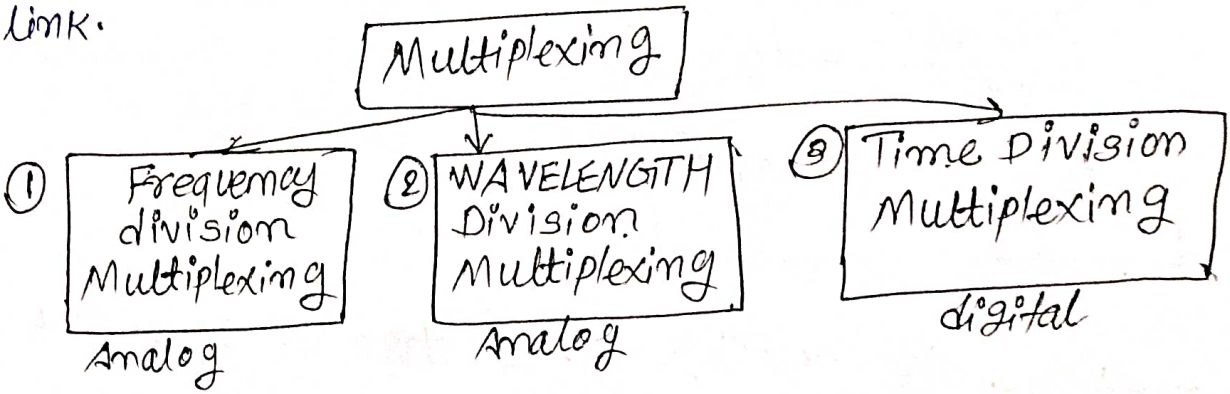
SNR = Avg signal power / Avg noise power

$\log_e x = y = x = e^y$

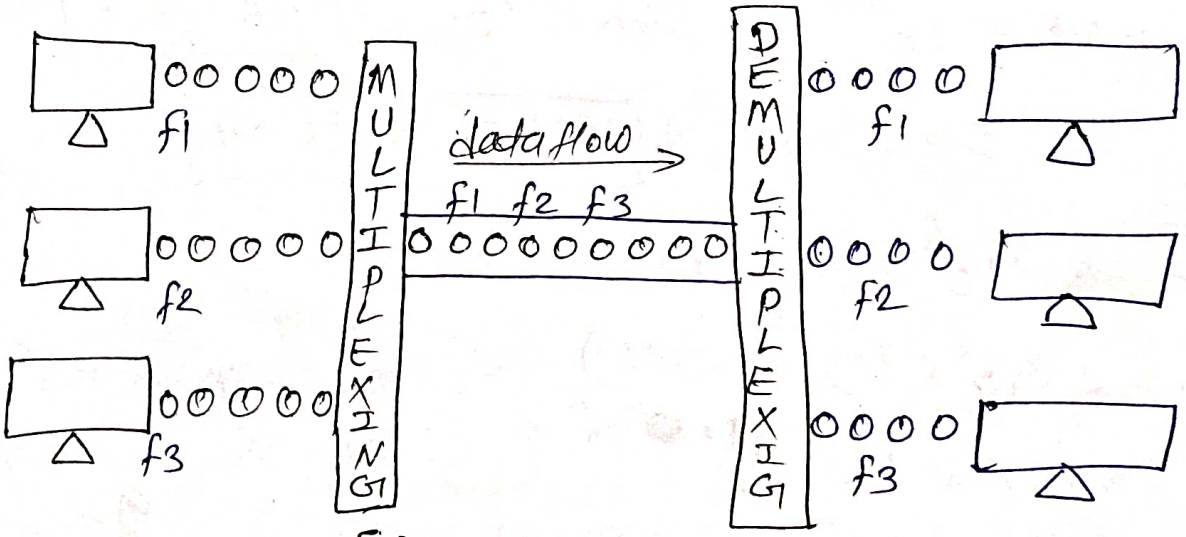
$SNR_{dB} = 10 . \log_{10} SNR$

Note: any prefix in bit rate will make this capacity → remember.

* Multiplexing: Multiplexing is a technique which allows transmission of multiple signal at the same time across one link.

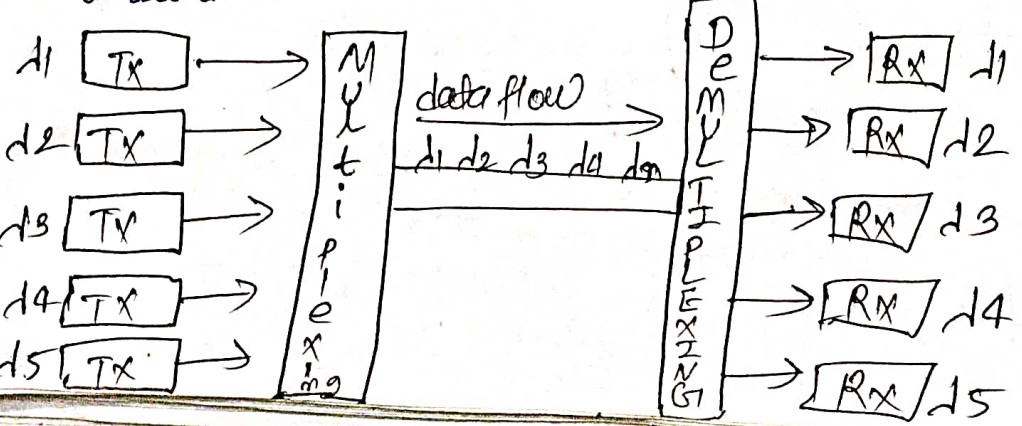


① Frequency-Division Multiplexing: Frequency-division multiplexing is an analog technique that combines analog signals, it can be applied when the bandwidth of a link is greater than the combined bandwidth of the signals to be transmitted.

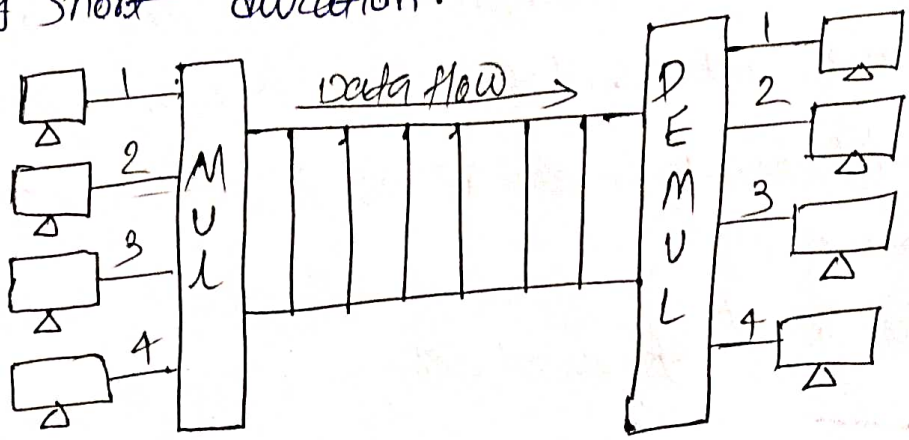


Frequency division Multiplexing

② Wavelength-Division Multiplexing: Wavelength division Multiplexing is an analog technique to combine optical signals. It can be applied when the bandwidth of a link is greater than the combined bandwidth of the signals to be transmitted.

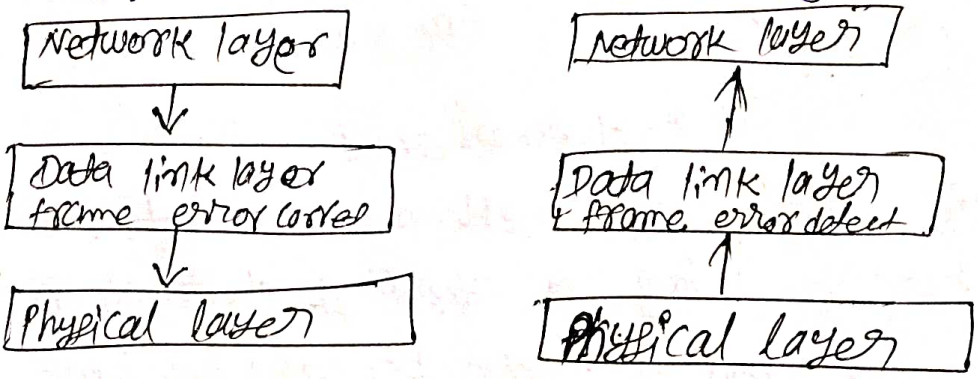


Time division multiplexing: Time division technique is a digital technique, it can be combined multiple low-rate channels into one high-rate channel each having a very short duration.



Chapter -

Data link layer: Data link layer devided received data packets into frams. It handle error detection and error correction. It also establishes and maintains the logical link between two devices on the network



DLL has two sublayers ① Mac → medium access control.
② LLC → logical link control

(*) functions of Data link layer:

- Design issue in DLL
- framing
- link access
- relaible
- error correction & detection
- frame formating
- freqauencing
- flow control

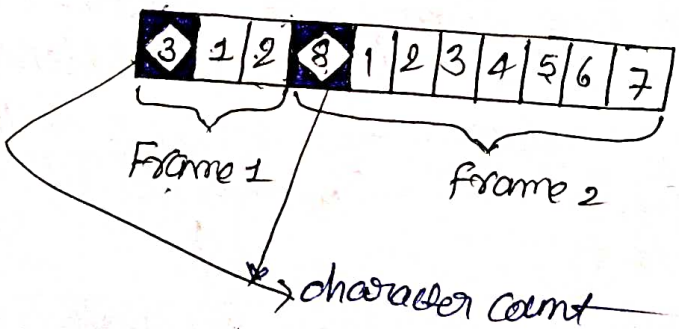
pQ. Explain framing and different algorithms.

ans⇒ Breaking the bit stream into frames is called framing. The bits to be transmitted is first broken into discrete frames at the data link layer.

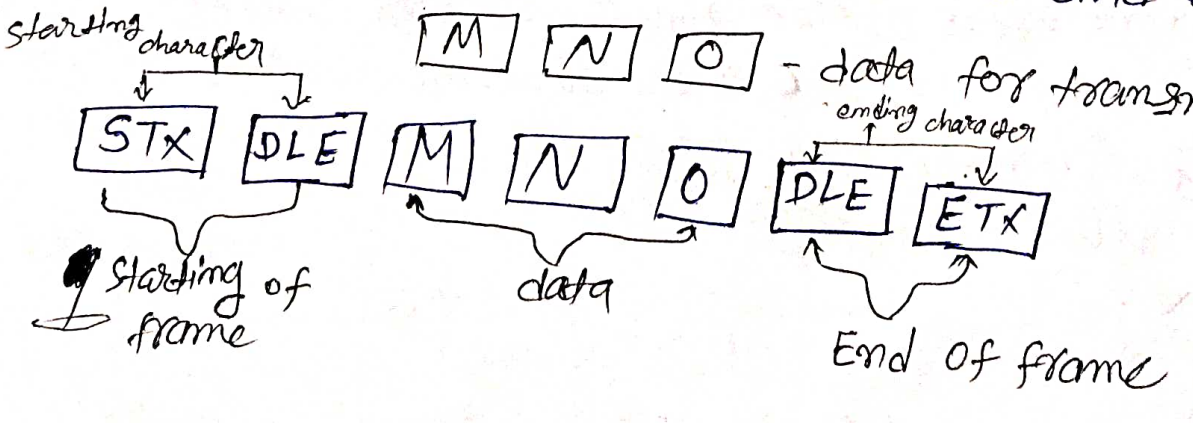
There are three different methods or algorithms of framing

(i) character count
(ii) Character stuffing / Bytes stuffing
(iii) Bit stuffing.

(i) Character count : In this method, a field is used in header to count the numbers of characters in the frame.



(ii) Character stuffing: The problem of character count method is sloved here by using a starting character before each frame and ending character at the end of each frame.



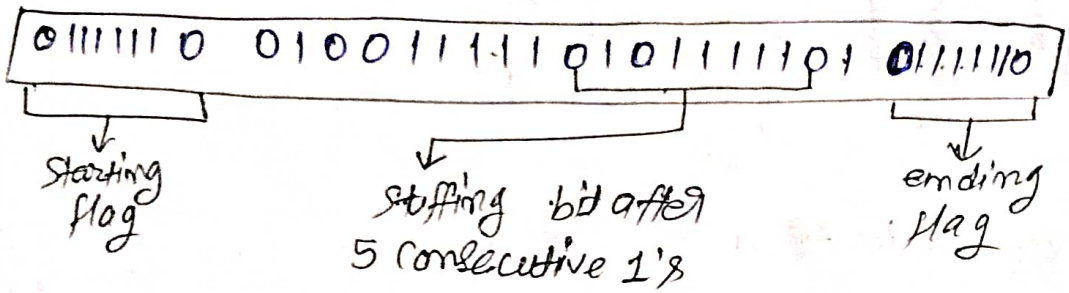
Note
STX → starting text
ETX → end text
DLE → data link escape

Bit stuffing: Bit stuffing is the inserting of non-information bits into data. It is called bit stuffing. the begining and end of each frame via a specific bit pattern 01111110 → flag byte.

original data: will have

↳ 0 1 0 0 1 1 1 1 1 0 1 1 1 1 1 1

After 5 consecutive 1's insert (0)



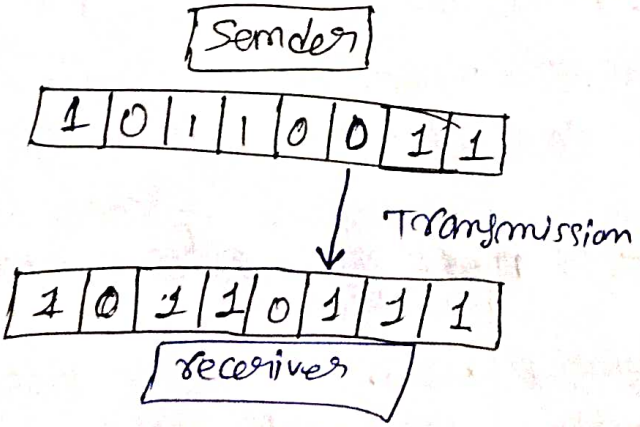
* Error detection and correction techniques.

• What is error and its type.

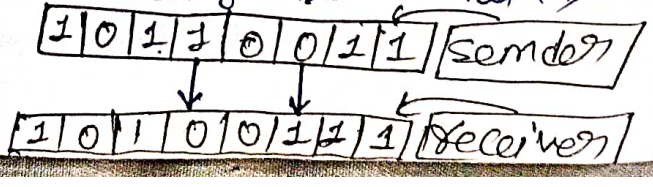
ans: Error is a condition when the receiver's information does not match the sender's information during the transmission. Types of error

(i) single-Bit error (ii) Multiple Bit error (iii) Burst error

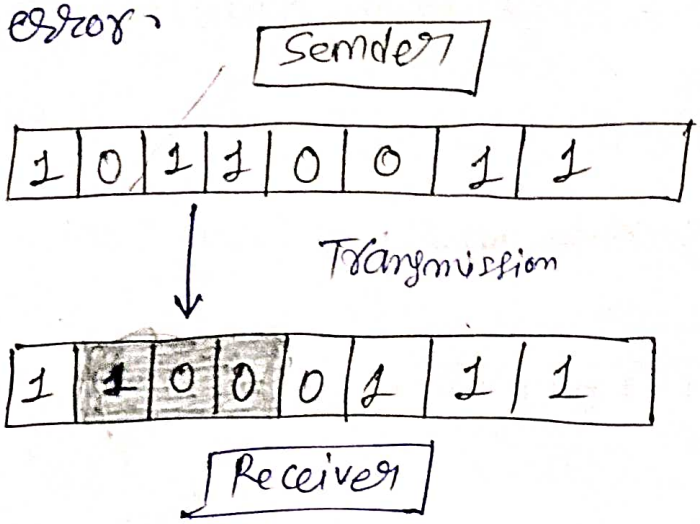
(i) single Bit error: A single-bit error occurs when one bit of a transmitted data is changed during transmission.



(ii) Multiple-Bit error: Multiple-Bit occurs when more than one data bit of a transmitted data is changed during transmission.



(iii) Burst error: When several consecutive bits are flipped mistakenly in digital transmission, it creates a burst error.



Error Detection methods

(i) Checksum
(ii) CRC (Cycle Redundancy check)
(iii) Hamming code

Checksum: checksum error detection is method used to identify errors in transmitted data. The process involves dividing the data into equally sized segments and using 1's complement to calculate the sum of these segments. The calculated sum is sent along the data to the receivers. At the receiver's end, the same process is repeated and if all ones are obtained in the sum, it means that the data is correct.

Checksum at sender side
- divide data into k segments of m bits in each block.
- sum all the k data blocks
- Add the carry to the sum, if any
- DO 1's complement to the sum = Checksum

Checksum at receiver side
- receive all segments along with checksum.
- sum all the k data blocks and checksum.
- After this if the result is all 1's, accept else reject.

Q1. ~~100111001111000100010010010000100~~

100111001111000100010010010000100

at the sender side

10011001	11100010	00100100	10000100

```
  1 0 0 1 1 0 0 1
  1 1 1 0 0 0 1 0
+ 0 0 1 0 0 1 0 0
  1 0 0 0 0 1 0 0
```

(100)

carry 1 0

```
  0 0 1 0 0 0 1 1
+           1 0
  0 0 1 0 0 1 0 1
```

1's com

1 1 0 1 1 0 1 0

checksum

at the receiver side

11011010	10011001	11100010	00100100	10000100

```
  1 1 0 1 1 0 1 0
  1 0 0 1 1 0 0 1
  1 1 1 0 0 0 1 0
  0 0 1 0 0 1 0 0
  1 0 0 0 0 1 0 0
1 0 1 1 1 1 1 0 1
+               1 0
  1 1 1 1 1 1 1 1
```

1's C

receiver accepted

(Q) Calculate the checksum for the following packets

10110 11010 10001.

at sender side

```
  1 0 1 1 0
+ 1 1 0 1 0
  1 0 0 0 1
carry 1 0 0 0 0 1
        + 1 0
  0 0 0 1 1   checksum
```

(2) 1's comp

```
  1 1 1 0 0
```

10110 | 11010 | 10001

block

```
  1 1 1 6
1 1 1 1 c
  0 1 0 0 0
```

at receiver side

```
  1 0 1 1 0
  1 1 0 1 0
  1 0 0 0 1
  1 1 1 0 0
1 0 1 0 1 0
      1 0
  1 1 1 1 1
```

received

CRC (cycle Redundancy check)

CRC generation at sender side

1. Find the length of the divisor (L).
2. Append (L-1) bits to the original message.
3. Perform binary division operation.
4. Remainder of the division = CRC.

CRC must be of L-1 bit

Q- Generate the CRC code for the following.

Message : 1001

Divisor : 1011

① L = 4 ② 3 bit of 0's to the message

```
1011 ) 1 0 0 1 0 0 0 ( 1010
       1 0 1 1
     x 0 1 0 0
       0 0 0 0
     x 1 0 0 0
       1 0 1 1
     x 0 1 1 0
       0 0 0 0
     x 1 1 0   remainder = CRC of (4-1)
```

XOR operation same - 0 diff - 1

0 से start होगा तो 0 x कुछ भी का हो divisor का

CRC : 110

Data transmitted : 1001 & 000 = 1001000

```
  1 0 0 1 1 0
+       1 1 0
  1 0 0 1 1 1 0
```

Data transmitted & message + L-1 times zero + remainder

Data transmitted : 1001110

CRC at receiver side

① Perform binary division operation.
② if the remainder is zero the data received otherwise not correct.

Eg. Use CRC method to check whether the received data correct or not where G = 1010? (110010)

```
1010 ) 110010 ( 111
       1010
       ----
        1110
        1010
        ----
         100
```

the received data is not correct because all remainder are not zero.

---

③ Hamming code ÷ a formula $2^P \geq P+m+1$ where P → parity bits, m → message bits.

Eg. Generate the Hamming code for 1110.

ans → $2^P \geq P+m+1$

$2^P \geq P+4+1$ $2^P \geq P+5 \Rightarrow 2^3 \geq 3+5 \Rightarrow 2^3 \geq 8, P=3$

For even

digits = mess + parity = 4+3 = 7

2^0 2^1 2^2

1(001) 2(010) 3(011) 4(100) 5(101) 6(110) 7(111)

P1 P2 m1 P3 m2 m3 m4

P1 P2 1 P3 1 1 0

0 0 1 0 1 1 1 ↓ hamming code.

P1 → (1, 3, 5, 7)
P2 → (2, 3, 6, 7)
P3 → (4, 5, 6, 7)

P1 → 1 3 5 7 (0)
P1 1 1 0 [even (P1=0)]

P2 = 2 3 6 7 (0)
P2 1 1 0 [even (P2=0)]

P3 = 4 5 6 7 (0)
P3 1 1 0 [even (P3=0)]

for odd

P1 → (1, 3, 5, 7)
P2 → (2, 3, 6, 7)
P3 → (4, 5, 6, 7)

P1 = 1 3 5 7

P1 1 1 0

for odd P1 = 1 [No of one = 3 odd]

P = 1

P2 = 2 3 6 7

P2 1 1 0

for odd P2 = 1 [No of one = 3 odd]

P2 = 1

P3 = 4 5 6 7

P3 1 1 0

for odd P3 = 1 [No of one = 3 odd]

P3 = 1

P1	P2	m1	P3	m2	m3	m4
1	1	1	1	1	1	0

Hamming code.

* Detection V/S correction of errors.

① Detection is always easier than correction.	correction is always difficult than detection.
• In case of error detection we dont need of know exact no of bit that are corrupted.	• In case of error correction we need to know exact no of bit that are corrupted.

* forward error correction V/S retransmission

• receiver tries to guess the message use redendency.	sender transmits again and again till error gets free.

FQ2m → Define flow and error control.

Flow control: It control the amount of data that a sender can send. It makes the wait until an acknowledgement is not received from the receiver's end.

* Error control: In data link layer it is based on automatic repeat request, which is the retransmission of data. This process is called Automatic Repeat Request (ARQ).

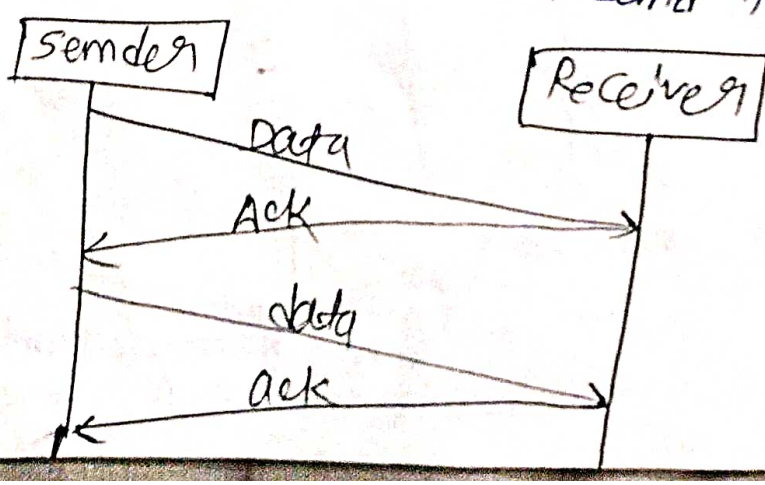
* Error control: Error control is basically process of detecting and re-transmitting data frames in data link layer, that might be lost or corrupted during transmission.

Flow control protocols

(Noiseless channel)
- ① simplest
- ② stop and wait

(noisy channel)
- ① Stop and wait ARQ.
- ② Go-Back-N-ARQ.
- ③ selective Repeat ARQ.
- Sliding window protocol

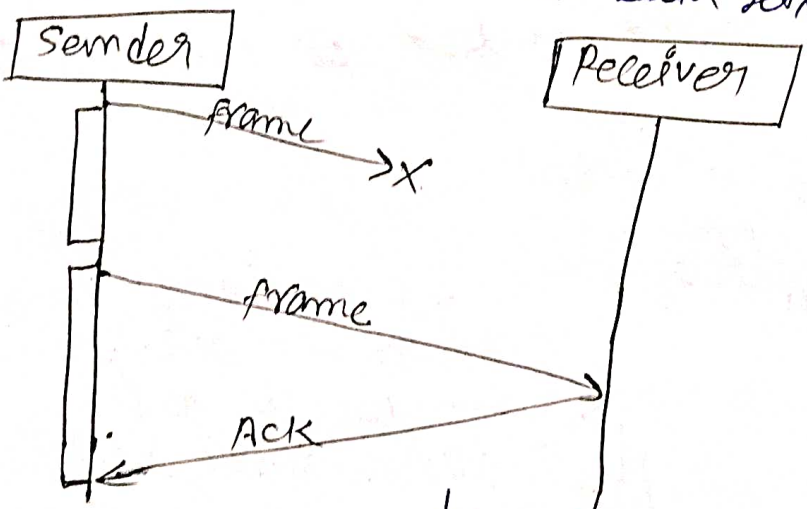
* Stop and wait: After the sender sends one data frame it must wait for an acknowledgement from the receiver, once it the acknowledgement is received from the receiver then only the sender can send the next data frame.



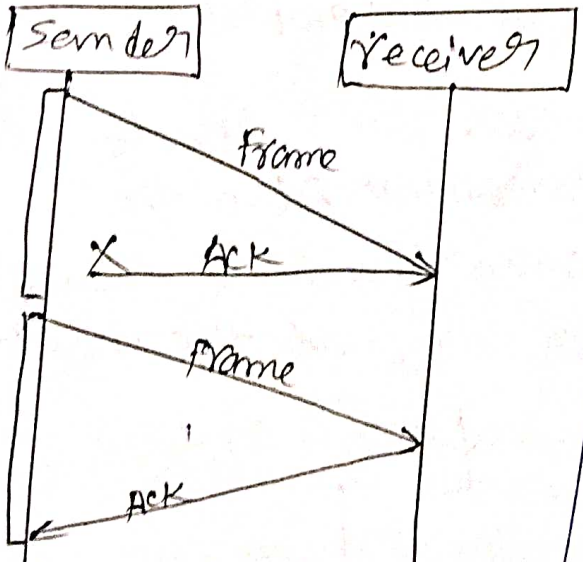
STOP and wait ARQ: After transmitting one frame, the sender waits for an acknowledgement before transmitting the next frame. If the acknowledgement does not arrive after a certain period of time, the sender timeout and retransmits the original frame. This retransmission is automatic that's why we called this as automatic ~~repeated~~ repeat request protocol.

Stop-and-wait ARQ = Stop-and-wait + Timeout timer + Sequence no

(a) When sender send data but ~~data~~ data gets lost from sender side.

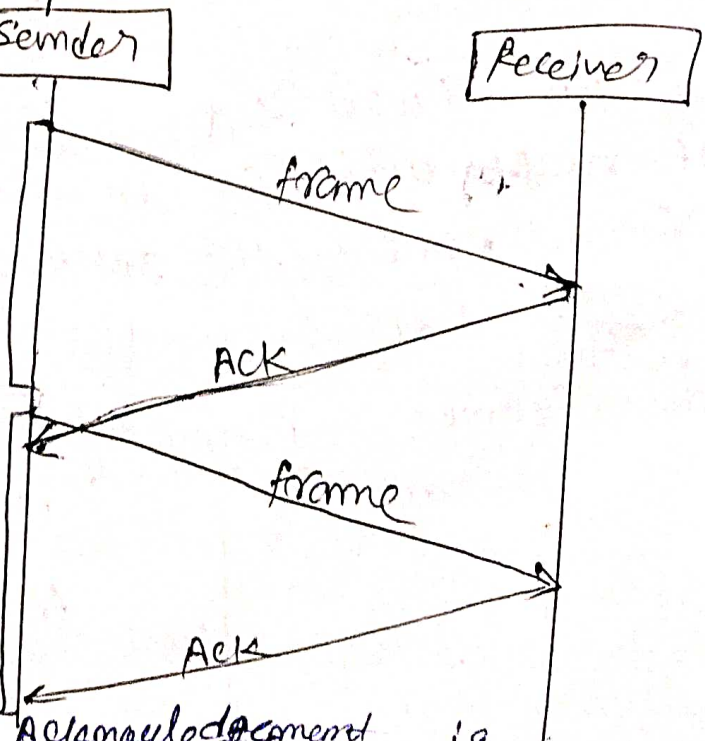


(b)



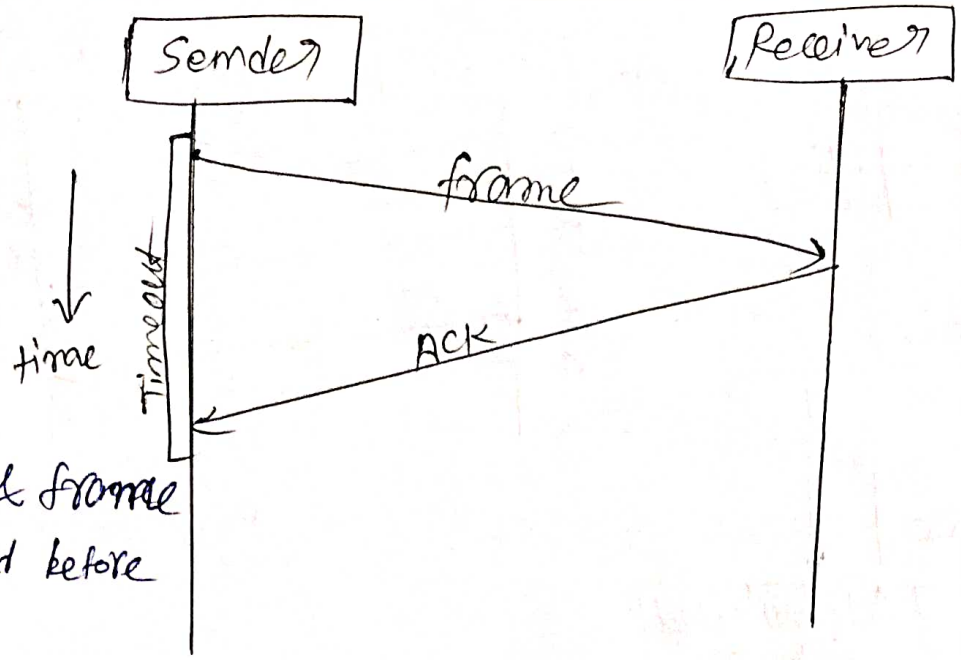
When Acknowledgement is lost from receiver side

(c)



When Acknowledgement is received to sender but after timeout

(d)



when data & frame both received before timeout.

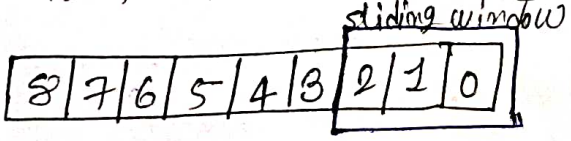
12 marks.

(Q9) Explain the working of sliding window flow control with the help of labeled diagram. or Explain sliding window protocol in detail.

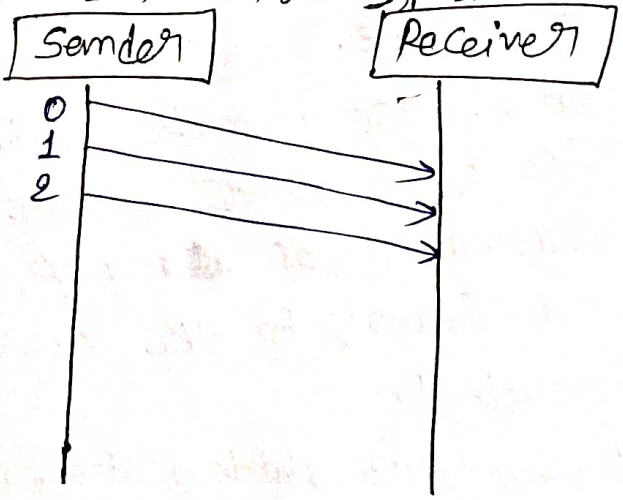
Working: The working of the sliding window protocol can be divided into two steps sender steps, and the receiver steps and also some important steps.

- sender and the receiver side
- window size
- the total data frames to be transmitted.

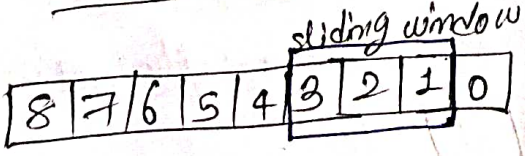
Steps for the sender side



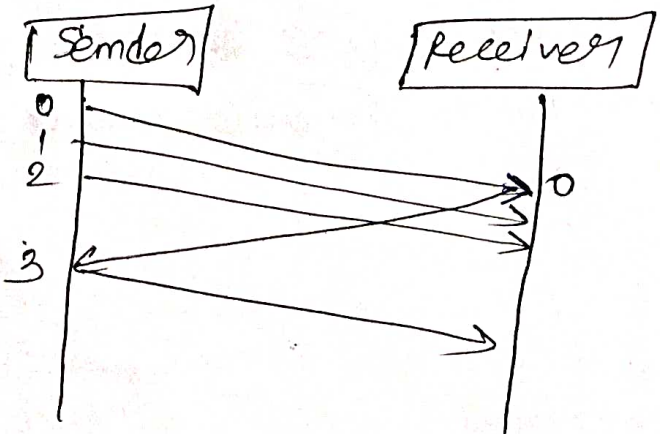
window size 3



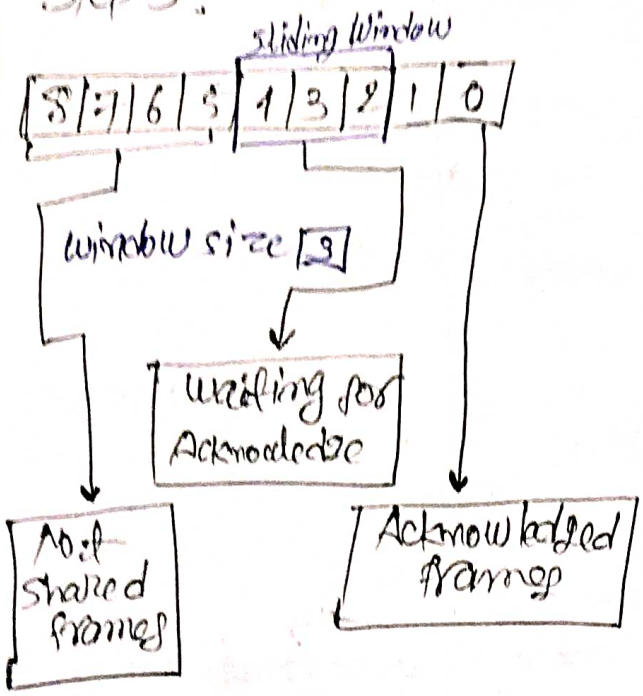
Step-2

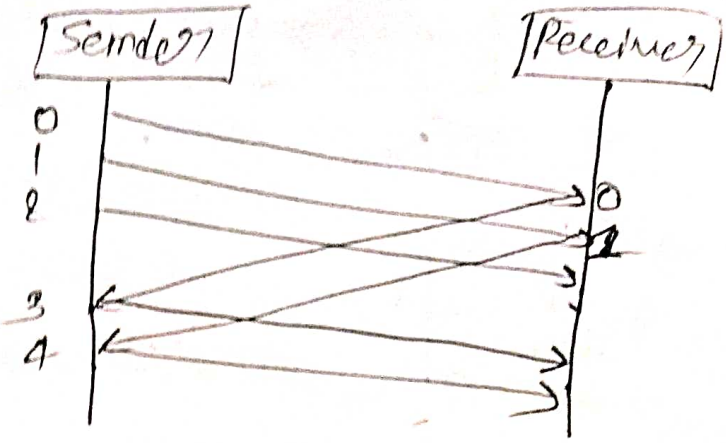


window size 3



Step 3:





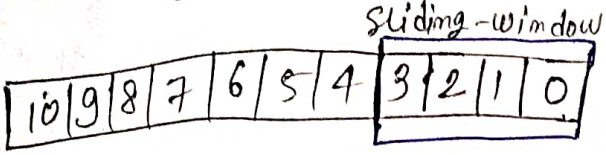
Sliding window protocol

- GO-BACK-N-ARQ
- Selective Repeat ARQ

* GO-BACK-N ARQ: GO-Back-N ARQ uses the concept of protocol pipelining that is the sender can send multiple frames before receiving the acknowledge for the first Time. There are finite number of frames and the frames are numbered in a sequential manner. and frames depends on the window size. If the acknowledgement of a frame not received in time then all frames in the current window are retransmitted.

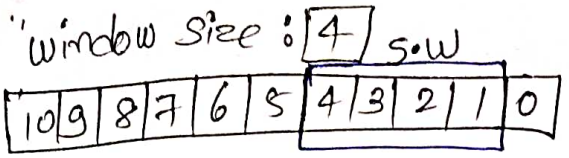
here → N - Sender's window size, if the window size = $4 (2^2)$ then the seaumce no i.s 2 [illegible] the no of bi.ts in the seaumce no 2 i.s 00 01 10 11

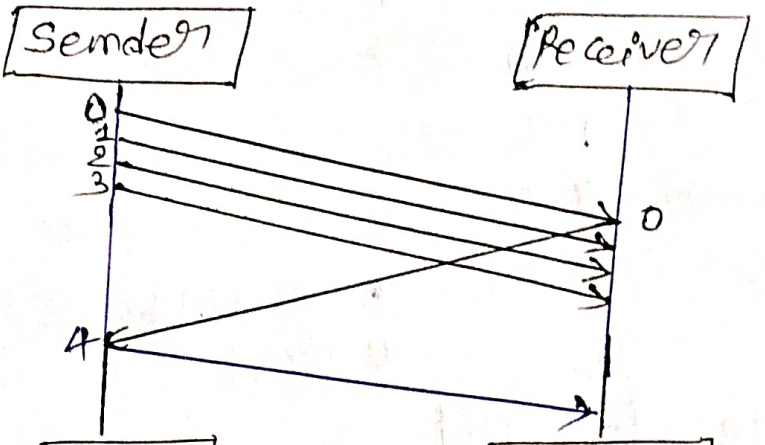
Working of GO-BACK-N-ARQ



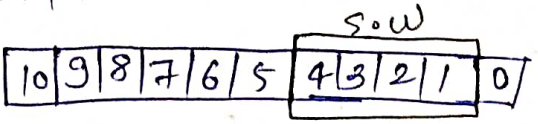
step:1 →

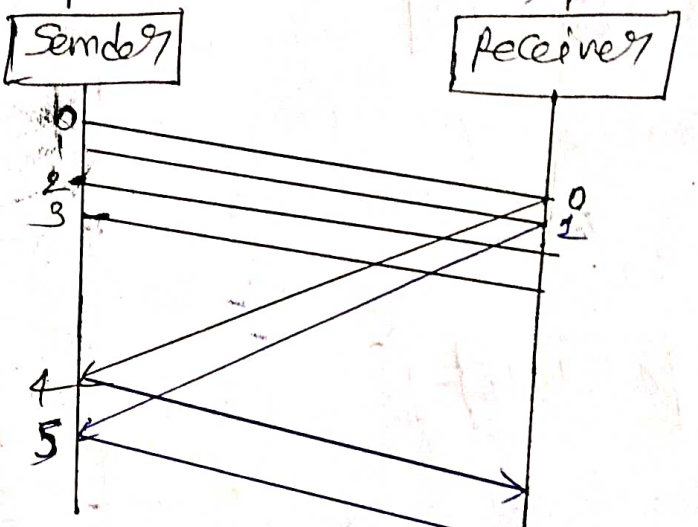
window size: 4



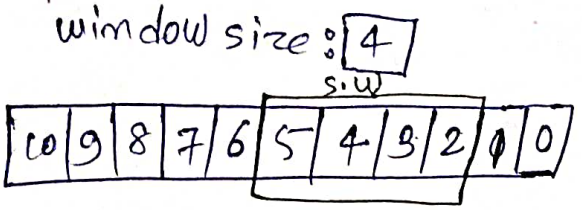


Step: 2

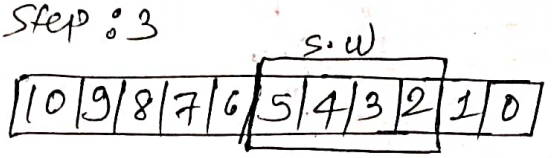




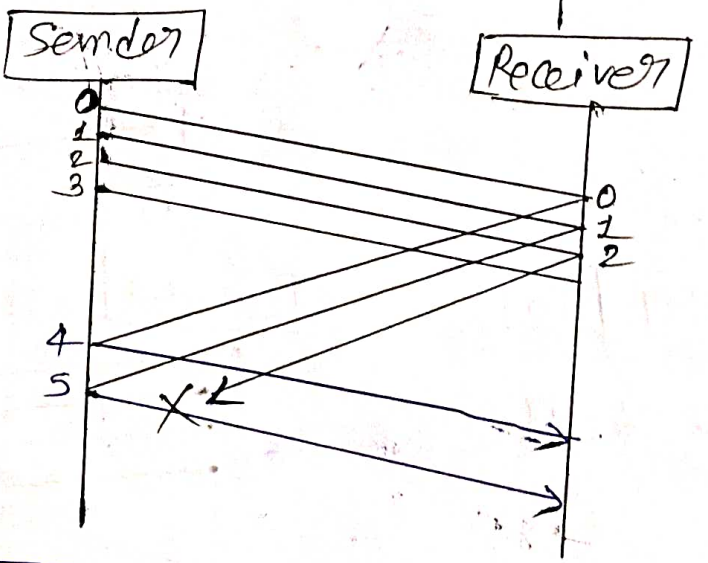
window size: 4



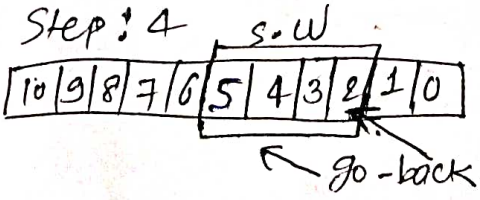
Step: 3



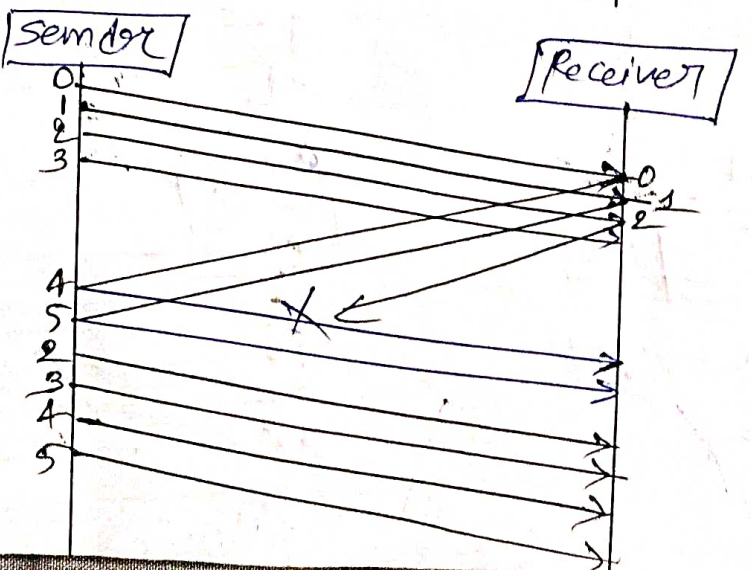
window size: 4



Step: 4



window size: 4

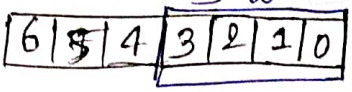


and so on.

(11) Selective Repeat ARQ: In GO-BACK-N-ARQ if any one frame is lost then we have to retransmit all the frames which are present in sliding window but in case of selective repeat ARQ, selective repeat retransmit only those frame that are actually lost.

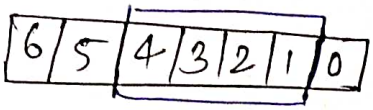
working

S.W



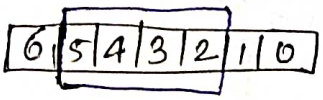
window size: 4

Step: 2



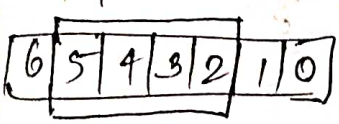
window size: 4

step: 3

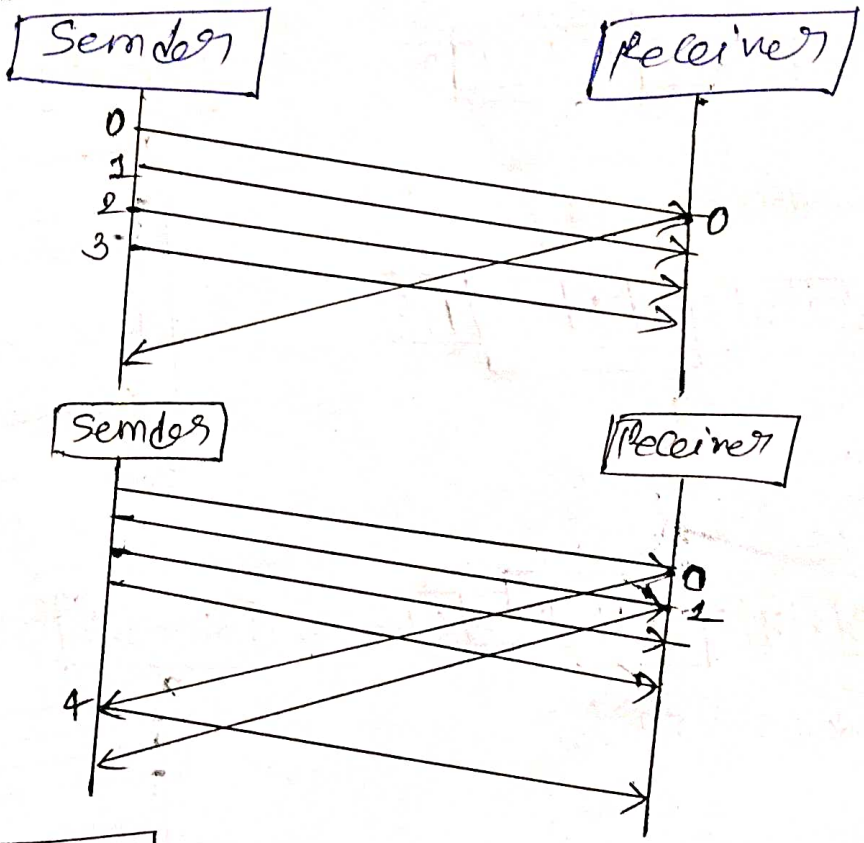


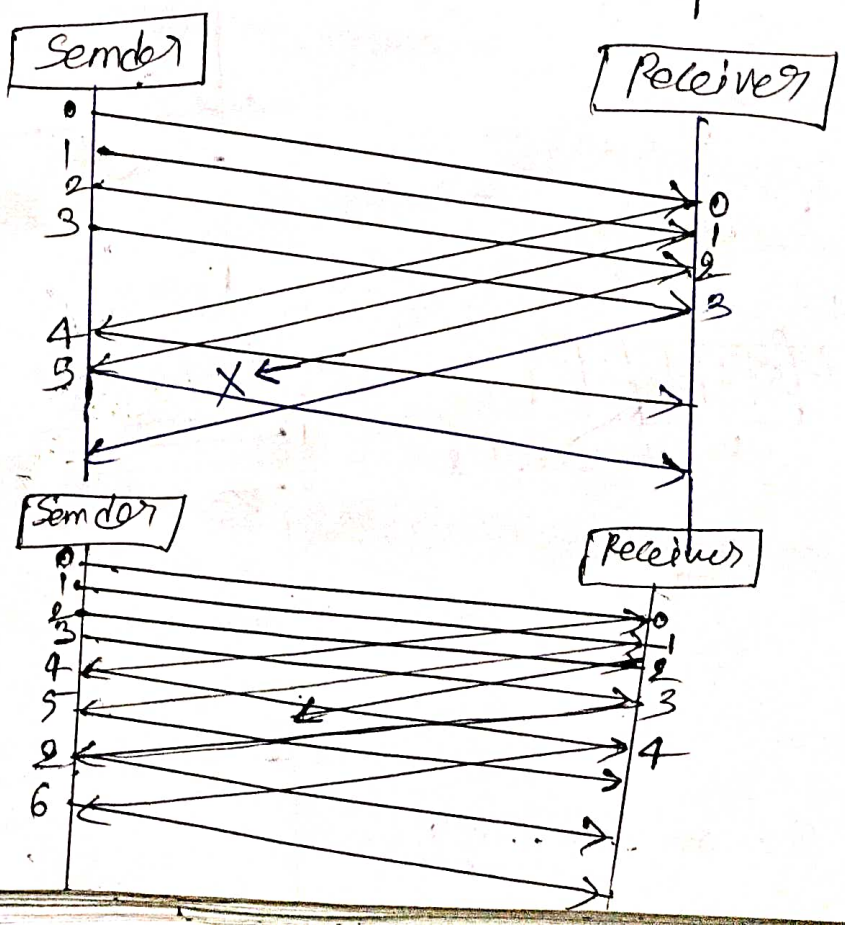
window side: 4

step: 4



Window size: 4





New-Chap

Medium Access sub-layer

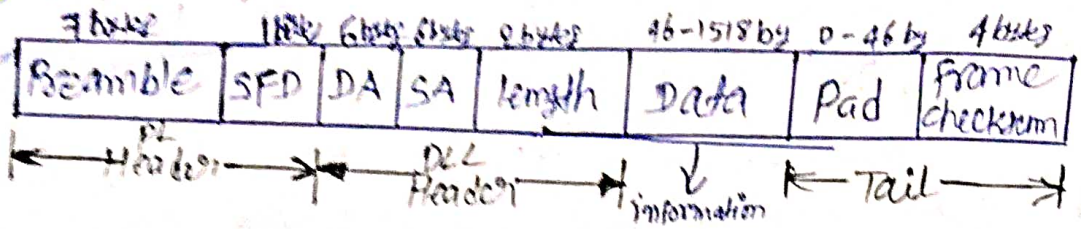
Qs: How throughput is improved in slotted ALOHA over pure ALOHA?

Ans: Slotted ALOHA improves throughput over pure ALOHA by reducing the number of collsions. in pure ALOHA, stations can transmit at any time, which can lead to collisions because when two or more stations transmit a frame at the same time. it may lead to collision but in case of Slotted ALOHA, Slotted ALOHA divides time into fixed intervals called slots so Stations can only transmit a frame at the beginning of a slot. This reduces the chance of collisions because two stations can only collide if they transmit in the same slot.

Pure ALOHA	Slotted ALOHA
① Random Access protocol.	① Random Access Protocol.
② Vulnerable time = $2 \times T_t$	② Vulnerable time = T_t
③ Efficiency = 18.4 %	③ Efficiency = 36.8 %
④ In this, stations can transmit at any time.	④ In this, Stations can only transmit at the begining of a slot.
⑤ Collision probability is High.	⑤ Collision probability is low.
⑥ Transmission time continuous.	⑥ Transmission time Slotted.

Q5 Describe frame formate of IEEE 802.3.

Ans:



Preamble: This field is 7 bytes (56 bits) long with a sequence of alternate 0 and 1 that is 10101010. This pattern helps to identify that it is beigining of frame.

SFD: Starting frame delimeter this field is 1 byte (8 bit) long has pattern 10101011. It also indicates beginning of a frame and ensures that the next field will be a destination address.

DA: Destination Address ; this field is 6 byte (48 bits) long. It Contains the physical address of the destination.

SA: Source Address ; This field is 6 byte (48 bits) long. It Contains the physical address of the sender.

length: It is 2 byte (16 bits) long. It indicate the number of bytes in the data field. The length allowable value can be 1518 bytes.

Data: This field will be a minimum of 46 bytes and maximume of 1500 bytes. This field contains actual information.

Pad: This field can be 0 to 46 bytes long. It is required if, the data size is less than 46 bytes as a 802.3 frame must be atleast 64 bytes long.

frame checksum: This field is 4 bytes (32 bit) long. It contains information about error detection, this is also part of Tail of frame formate.

* static and dynamic channel allocation:

Static channel allocation: (FCA) is a channel allocation technique in which channels are permanently assigned to users or cells. This is the simplest and most efficient way to allocate channels, but it can lead to underutilization of resources if the traffic load is not evenly distributed.

Dynamic channel allocation (DCA): Dynamic channel allocation technique in which channels are assigned to users or cells on a temporary basis, as needed. This allows for more efficient use of resources, but it can be more complex to implement and manage.

FCA	DCA
(i) channel assignment is permanent.	channel assignment is Temporary.
(ii) simple and efficient	More efficient. but it can be more complex.
(iii) distributed traffic load	.uneven traffic load.
(iv) Cellular networks	wifi networks.

* Controlled Access: polling, Token passing.

polling: In polling, a central device, called the primary station, polls each of the other devices on the network in a predetermined order. if a device has data to transmit, it indicates this to the primary station then grants permission to the device to transmit its data. if a device has no data to transmit, it simply responds

to the poll with a negative acknowledgement.

Polling: polling is a simple and efficient protocol, but it has two main drawbacks. first, it can be show if there are many devices on the network, because the primary station has to poll each device individually. second it is not very fair because devices that are polled earlier in the polling order have more opportunities to transmit data than devices that are polled later in the order.

Token passing: Token passing is a more fair protocol than polling, because all devices have an equal opportunity to transmit data. It is also more efficient than polling for networks with a large number of devices, because the token can be passed around the network very quickly.

Ethernet Cabling: Ethernet cabling is a type of network cabling that uses Ethernet technology to connect devices to a local area network (LAN). Ethernet cables are typically made of copper or fiber optic materials, and they come in a variety of categories, each with its own maximum speed and bandwidth.

Manchester encoding: Manchester encoding is a line code in which a data bit is represented by a transition from one voltage level to another at the middle of the bit period. this is in contrast to other line codes such as non-return to-zero (NRZ), where the voltage level itself represents the data bit.

* Collsion detection in 802.3 : Collision detection in 802.3 is a mechanism used to detect collisions between Ethernet that are being transmitting stations stop transmitting and wait for a random amount of time before retransmitting. This helps to reduce the number of collisions and improve the overall performance of the network.

Collision detection is implemented in the media Access Control (MAC) layer of the 802.3 standard. When a station wants to transmit to see if it is busy. if the medium is idle, the station begins transmitting, it also monitors the medium for the station detects another signal. It knows that a collision has occurred. if a collision is detected, the station immediately stops transmitting and sends a jam signal to inform all other stations on the network of the collision. The stations then wait for a random time before attempting to transmit again.

* Binary exponential back off algorithm: Binary exponential backoff algorithm is a collision resolution mechanism used in computer networks, it is a technique to reduce the probability of collisions by delaying retransmissions after a collision.

The algorithm works by doubling the amount of time a device waits before retransmitting after each collision.

This means that the device will wait a random amount of time between 0 and 1 slot times after the first collision, between 0 and 3 slot times after the second collision, and so on.

The binary exponential backoff algorithms is used in a variety of networking protocols, including Ethernet and wi-fi. It is also used in other systems, such as distributed databases and peer-to-peer networks.

(*) Explain the CSMA protocol in detail.

ans: CSMA stands for carrier sense Multiple Access. This method was developed to decrease the chances of collisions when two or more stations start sending their signals over the data link layer. CSMA requires that each station first check the states of the medium before sending.

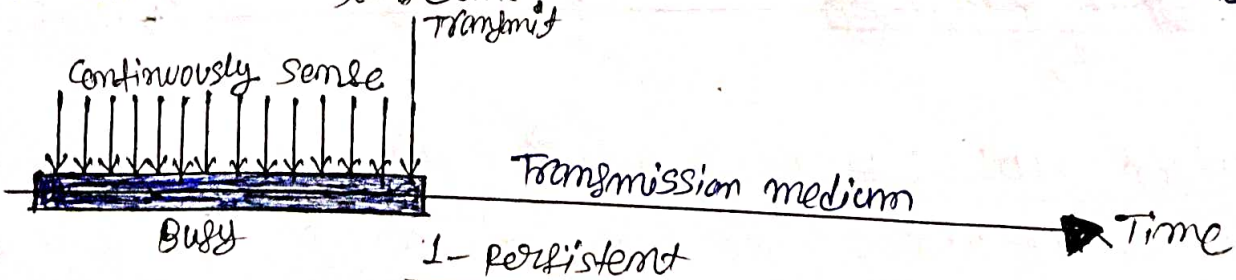
CSMA/CD: CSMA/CD stands for carrier sense multiple Access / collision detection, CSMA/CD senses the channel first before transmitting the frame. After that it sends a frame if the channel is idle, it transmits a frame to check wheather the transmission was succeffful. If the frame is Sucessfully received the station sends another frame. If any collision is detected the station sends a jam/stop signal to the channels to stop data transmission After that, it waits for a random time before sending a frame to a channel.

CSMA/CA: CSMA/CA stands for carrier sense multiple access/collision avoidance. When a data frame is sent to a channel, it receives an acknowledgement to check whether the channel is idle. if the station receives only one single acknowledgment, that means the data frame has been successfully transmitted to the receiver. But if it gets two signals that means a collision of the frame occurs in the channel. So it detects the collision of the frame when a sender receives an acknowledgement signal.

Types of CSMA

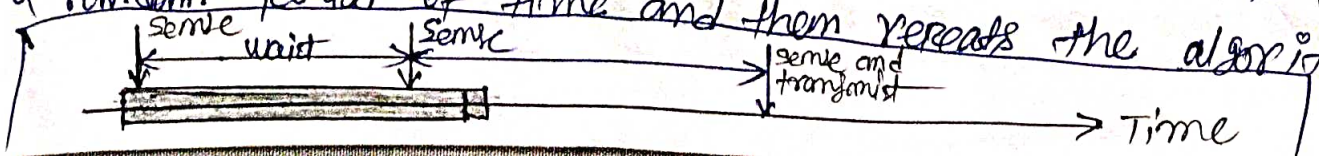
① 1-Persistent ② Non-Persistent ③ P-Persistent ④ O-Persistent

① 1-persistent: It sense the channel first to see if anyone else is transmitting the data/frame at that time. if the channel is idle, it transmits a frame, if busy then it senses the transmission medium continuously until it becomes idle.



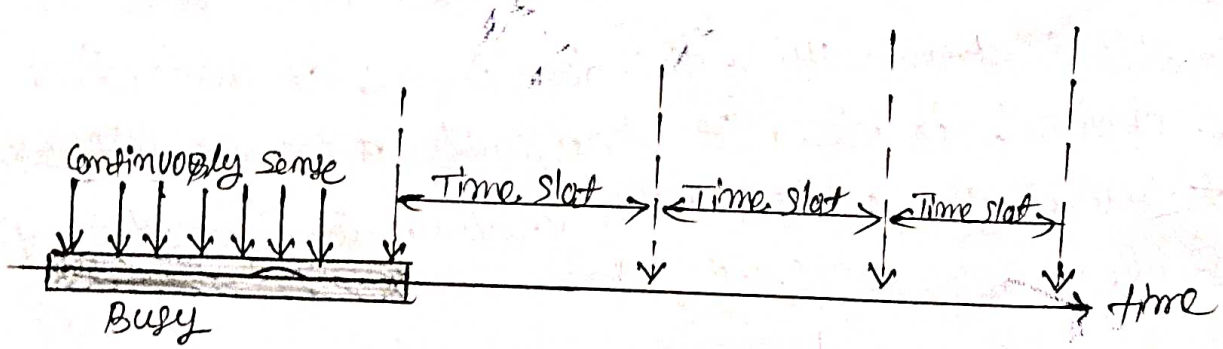
1-persistent

② Non-Persistent: It sense the channel first to see if anyone else is transmitting the data/frame at that time, if the channel is idle, it transmits a frame, if busy then it does not continuously sense the transmission medium, it waits for a random period of time and then repeats the algorithm.

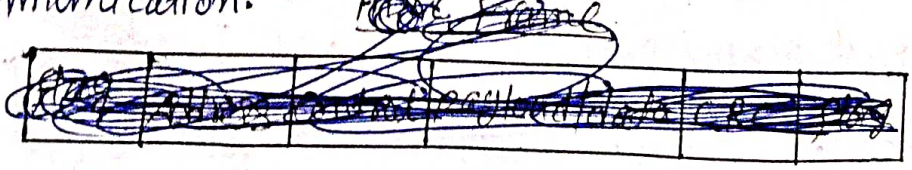


③ O-persistent: It defines the specialty of the channel before the transmission of the frame on the channel. if it is found that the channel is inactive then each station waits for its turn to retransmit the data.

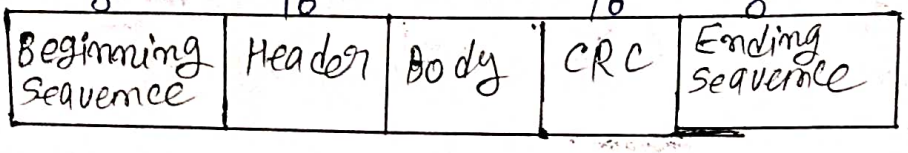
④ P-Persistent: It is the combination of 1-persistent and Non-persistent. The P-persistent mode defines that each node senses a channel and if the channel is idle it transmits the frame with a probability P. if the data is not transmitted, it waits for a (Q=1-P probability) random time and resumes the frame with the next time slot.



*Explain HDLC: HDLC stands for High-level Data Link control. It is a set of protocal or group of protocal of data link layer for transmitting the data between the network. It is being Defined by ISO. It is a bit-oriented protocal that is applicable for both point to point and multipoint communication.



HDLC - Frame format



Begining Seaveence: It is an 8 bit seaveence that defines the beginning of the frame. The bit pattern of the Begining Seaveence is 01111110.

Header: Header field containg Address and Control field. It is of 16 bit, it contains the address of the receiver. if the frame is semt by the primary station and so on.
Control → It is 1 or 2 bytes containing flow and error control information.

Body: This carries the data from the network layer. its length may vary from one network to another.

CRC: Cyclic Redundancy check - It detects the error from beiginning to Body. It is of 16 bit

Ending Seaveence: It is of 8 bit seaveence that defines the ending of the frame. The bit pattern of the Ending seaveence is 01111110.

Types of HDLC frames

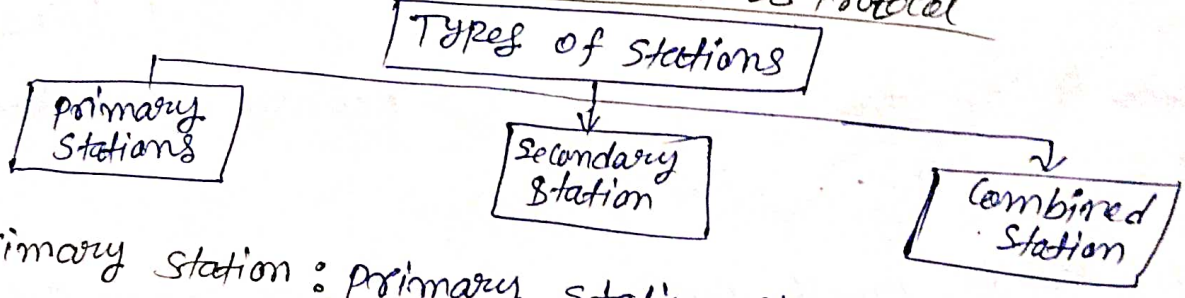
1. I-frame: Information frame (carries information)
2. S-frame: supervisory frame (carries flow error control)
3. U-frame: Un-numbered frame

I - frame: Information frame carry user data from the network layer. They also include flow HDLC control & error [illegible]. The first bit of control field of I-frame is 0.

S-frame: Supervisory frames do not contain information Field. They are used for flow and error control. The first two bits of control field of S-frame is 10.

U-frame: Un-numbered frames are used for [illegible] unclountable. miscellaneous functions, like link management, The first two bits of control field of U-frame is 11.

Types of Stations of HDLC protocol



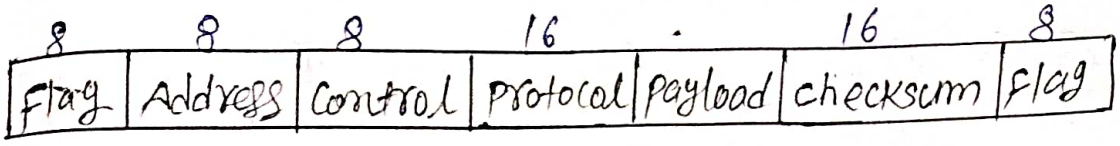
1. primary station: primary station simply takes care of data link management. The main responsibility of primary station is to control operation of all other station on links.

2. secondary station: Secondary stations generally give responses to commands that are sent from primary station.

(3) Combined station: Combined station as the name suggests generally acts as combination of both primary and secondary stations.

* point-to-point Protocol: Point to-point protocol (PPP) is a communication protocal of the data link layer that is used to transmit multiprotocal data between two directly connected (Point-to-point) computers. It is a byte-oriented protocol that is widely used in broadband communication having heavy load and high speed.

Frame format



*flag: It is of 8 bit sequence that defines the begining and ending of the frome. The bit pattern of the Begining sequence is 01111110.

*Address: It is of 8 bit sequence, The bit pattern of the Address is 11111111 in case of broadcast.

*Control: It is of 8 bit sequence, The bit pattern of the control is 11000000 which is a constant value.

*protocol: It is of 16 bit sequence that define the type of data contained in the payload field.

* payload: This carries the data from the network layer. The maximum length of the payload field is 1500 byteg. However this may be negotiated between the endpoints of communication.

*checksum: It is of 16 bit, It detect the error from flag to payload.

Difference between PPP and HDLC

HDLC	PPP
① HDLC is Bit oriented.	② PPP is byte oriented.
② It can do synchronous transmission.	② It can be either synchronous or Asynchronous transmission.
③ It has multipoint links.	③ It don't have multipoint links.
④ HDLC stands for High-level data Link control.	④ PPP stands for point-to-point protocol.
⑤ HDLC does not provides error detection	⑤ PPP provides error detection.
⑥ HDLC is more costly than PPP.	⑥ PPP less costly than HDLC.
⑦ HDLC does not provide Dynamic addressing.	⑦ PPP provides dynamic addressing.

(12 marks) Classes of IPV4 Address

Network layer

Address class	1st Octet range in decimal	1st Octet bits range in dotted notation	Network (N) and HOST (H) portion	Default Mask (Decimal) & Example	No of possible networks and hosts Per networks
A	0-127	00000000 - 01111111	N.H.H.H	255.0.0.0 Ex: 10.0.0.0	128 Nets (2^7) hosts ($2^{24}-2$)
B	128-191	10000000 - 10111111	N.N.H.H	255.255.0.0 Ex: 128.16.0.0	(2^{14}) Nets ($2^{16}-2$) hosts
C	192-223	11000000 - 11011111	N.N.N.H	255.255.255.0 Ex: 192.168.1.	(2^{21}) Nets (2^8-2) hosts
D	224-239	11100000 - 11101111	NA (Multicast)	Ex: 224.0.0.0 —	—
E	240-255	11110000 - 11111111	NA (Experimental)	Ex: 240.0.0.0 —	—

classful addressing: classful addressing is a method of organizing ipv4 addresses into five classes A, B, C, D and E, each class is assigned a different range of addresses and the class of an address can be determined by the value of the first octet.

(Pg 20) Calculate (a) Network address (b) host address (c) number of networks (d) number of hosts (e) subnet mask for (i) 102.45.09.5
(ii) 197.64.3.8

ans → 102.45.09.5

[redacted]

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0
0 1 1 0 0 1 1 0

class : A

default Mask : 255.0.0.0 (N.H.H.H)
8 8 8 8

(i) Network address : 102.0.0.0

(ii) Host address : 0.45.09.5

(iii) No of networks : $2^{N-\text{desired}} 8 = 2^8$ but first bit for class address reserved so $2^{8-1} = 2^7 = 128$.

(iv) No of hosts : $(2^{\text{no of hosts}} - 2) = (2^{3H} - 2) = (2^{3\times8} - 2) = (2^{24} - 2) = (2^{24} - 2) = 16777214$

(v) Subnet mask : 255.0.0.0

(ii) 197.64.3.8

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0
1 1 0 0 0 1 0 1

class : C

default Mask : 255.255.255.0 (N.N.N.H)

(i) Network address : 197.64.3.0

class address → 110

(ii) host address : 0.0.0.8

(iii) No of networks : $(2^{N-\text{class address}})$

$: (2^{3N-3}) = 2^{3\times8-3} = 2^{24-3} = 2^{21} = 2097152$

(iv) No of hosts : $(2^h - 2) = (2^8 - 2)$ — 256 − 2 = 254

(v) Subnet mask : 255.255.255.0 (N.N.N.H)

(Pyq) you have been allocated a class c network address of 211.1.1.0 and are using the default subnet mask of 255.255.255.0.
N N N H
How ~~many~~ hosts you have?

ans ⇒ no of hosts : $(2^h - 2) = 2^8 - 2 = 256 - 2 = 254$

for classless

* Subnetting : ① How to find the no of network :

2^n : n is total no of bits borrowed from host.

② How to find no of IP address on each network

2^n → n is no of remaining host bits

③ How To find the no of hosts in each network.

$(2^n - 2)$ → n is no of remaining host bits.

(Q7). Subnet the class c ip address 205.11.2.0 so that you have 30 subnets.

(a) what is the subnet mask for the maximum no of hosts?

(b) How many hosts can each subnet have?

(c) what is the ip address of host 3 on subnet 2?

ip add : 205.11.2.0

class : c

255.255.255.0

Subnet = 30

11111111 11111111 11111111 11111100 | 30

$2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$

255 255 255 128+64+32+16+8+4

↓

252

(a) Subnet mask → 255.255.255.252

(b) No of hosts : $(2^n - 2)$ n → no of remaining bit

$= 2^2 - 2 = 4 - 2 = 2$

Extra: (1) no of network

2^n → where n no of borrow bit

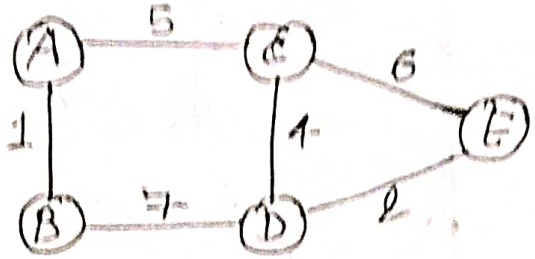
$2^6 = 64$

(2) No of ip address : 2^n = where n no of remaining bit

$2^2 = 4$

(*) Define subnetting: Subnetting is the process of dividing a large network into smaller network. It helps to optimize network performance and efficiently allocate IP addresses.

(P20) Evaluate the distance vector routing algorithm using suitable example.



(1) Routing table for each node

Routing table for (A)

Destination	Distance	hop
A ✓	0	A
B	1	B
C	5	C
D	∞	—
E	∞	—

Routing table for (C)

Destination	Distance	hop
A	5	A
B	∞	—
C ✓	0	C
D	4	D
E	6	E

Routing table for (B)

Destination	Distance	hop
A	1	A
B ✓	0	B
C	∞	—
D	7	D
E	∞	—

Routing table for (D)

Destination	Distance	hop
A	∞	—
B	7	B
C	4	C
D ✓	0	D
E	2	E

Routing table for (E)

Destination	Distance	hop
A	∞	—
B	∞	—
C	6	C
D	2	D
E ✓	0	E

(2) After exchanging the distance vectors, each router prepare a new routing table.

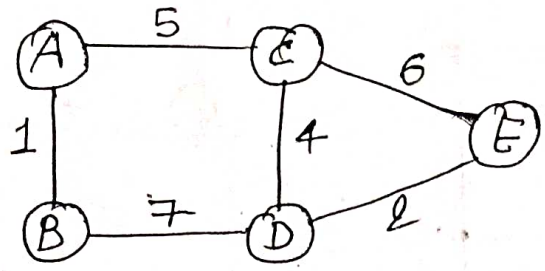
Bellman ford equation: from node x to node y

$$d_x(y) = \min_v \{c(x,v) + d_v(y)\}$$

x → source, y → destination
v → intermediate

(PYQ) Evaluate the distance vector routing algorithm using suitable example.

one ⇒ Ex ⇒



(1) Routing table for each node

Routing table for (A)

Destination	Distance	hop
A ✓	0	A
B	1	B
C	5	C
D	∞	—
E	∞	—

Routing table for (C)

Destination	Distance	hop
A	5	A
B	∞	—
C ✓	0	C
D	4	D
E	6	E

Routing table for (B)

Destination	Distance	hop
A	1	A
B ✓	0	B
C	∞	—
D	7	D
E	∞	—

Routing table for (D)

Destination	Distance	hop
A	∞	—
B	7	B
C	4	C
D ✓	0	D
E	2	E

Routing table for (E)

Destination	Distance	hop
A	∞	—
B	∞	—
C	6	C
D	2	D
E ✓	0	E

(2) After exchanging the distance vectors, each router prepare a new routing table.

Bellman ford equation: from node x to node y

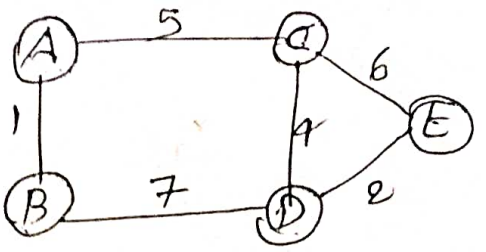
$$d_x(y) = \min_v \{c(x,v) + d_v(y)\}$$

x → source, y → destination
v → intermediate

New routing table for each node

for (A)

Destination	Distance	hop
A ✓	0	A
B	1	B
C	5	C
D	8	B
E	10	B



A→A D=0 h=A ✓

A→B A→B, 1, B ✓

A→C→D→B = 16
5 4 7

A→C→E→D→B = 20
5 6 2 7

A→C A→C = 5 ✓

A→B→D→C = 12
1 7 4

A→B→D→E→C = 16
1 7 2 6

A→D A→C→D = 11
5 4

A→B→D = 8 ✓
1 7

A→C→E→D = 13
5 6 2

A→E A→C→E = 11
5 6

A→B→D→E = 10 ✓
1 7 2

A→C→D→E = 11
5 4 2

and same process for each node

for (B)

Destination	Distance	hop
A	1	A
B ✓	0	B
C	6	A
D	7	D
E	9	D

for (C)

Destination	Distance	hop
A	5	A
B	6	A
C ✓	0	C
D	4	D
E	6	E

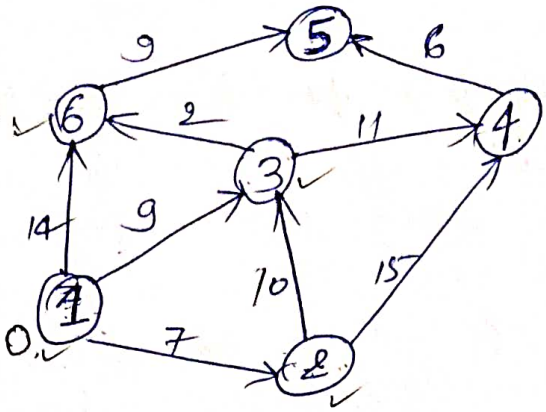
for (D)

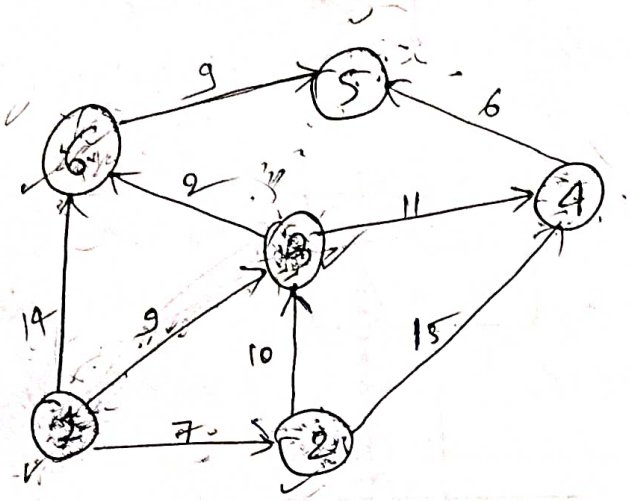
Destination	Distance	hop
A	8	B
B	7	B
C	4	C
D ✓	0	D
E	2	E

for (E)

Destination	Distance	hop
A	10	D
B	9	D
C	6	C
D	2	D
E ✓	0	E

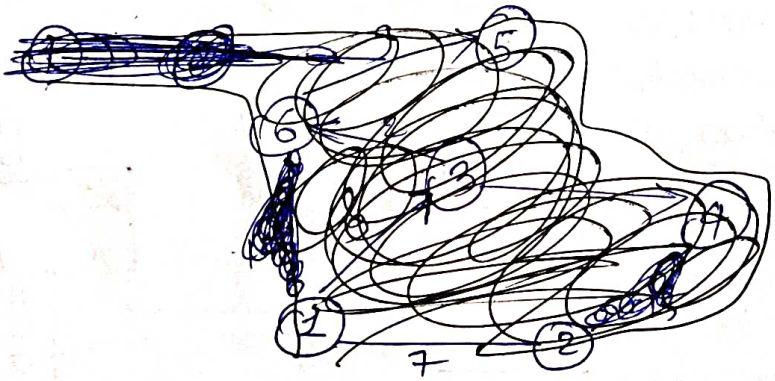
Q10 Find shortest path from node 1 to all other nodes using Dijkstra's algorithm.

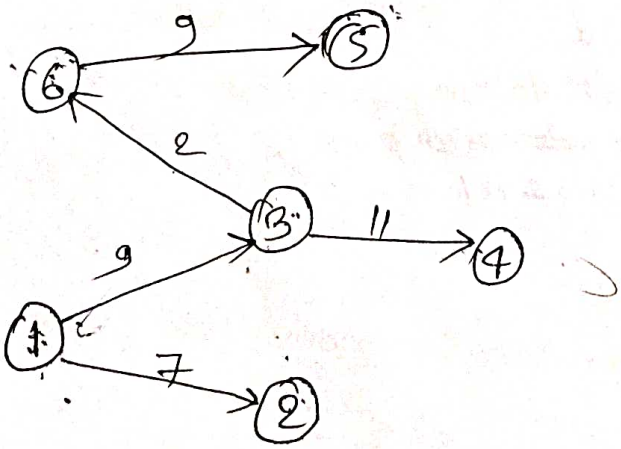




Source	Destination				
1	2	3	4	5	6
	∞	∞	∞	∞	∞
1,2	7	9	∞	∞	14
1,2,3	7	9	22	∞	14
1,2,3,6	7	9	20	∞	17
1,2,3,6,4	7	9	20	20	11
1,2,3,6,4,5	7	9	20	20	11

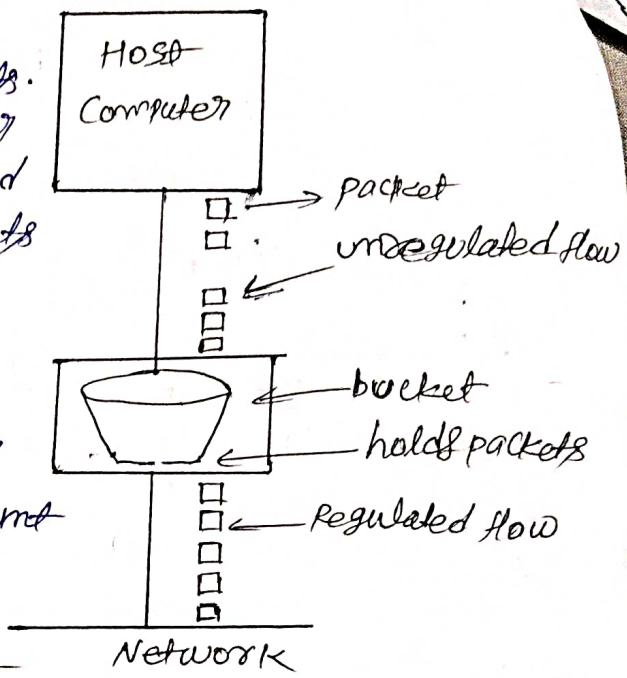
Shortest path is:





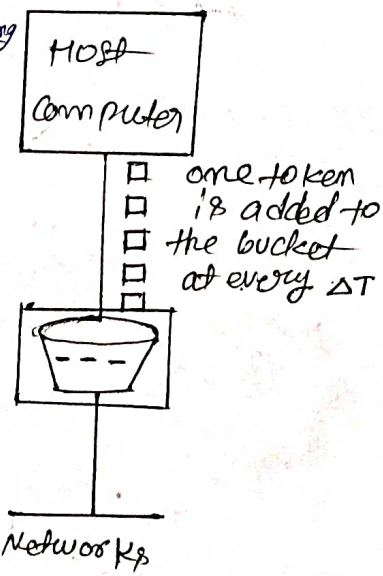
(Dec 19) write short note on (a) Leaky bucket algorithm
(b) Token bucket algorithm

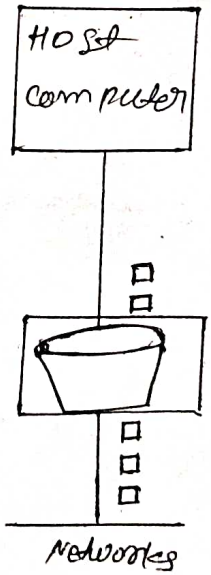
(a) Leaky bucket algorithm : A Host computer transmits unregulated packets. A bucket is placed between host computer and network which stores the unregulated flow of packets and it release the packets in regulated flow to the network. this analogy called leaky bucket algorithm.



This algorithm has two main parameters
(i) Bucket size: The maximum amount of data that bucket can be stored.
(ii) Token rate: The rate at which data/packet is released from the bucket.

(b) Token bucket algorithm:
In Leaky bucket algorithm when bucket is full then remaining upcoming packets are discarded to overcome this problem token bucket algorithm is developed. It uses tokens, when packets arrives the algorithm checks if there are enough token in the bucket or not, if there are enough token then tokens are consumed and packets are transmitted, if there are not enough tokens then the packets are ~~discarded~~ holded and again when enough token will be there then packets core added to the bucket at every ΔT time.





(pg9) Compare and contrast IPV4 and IPV6.

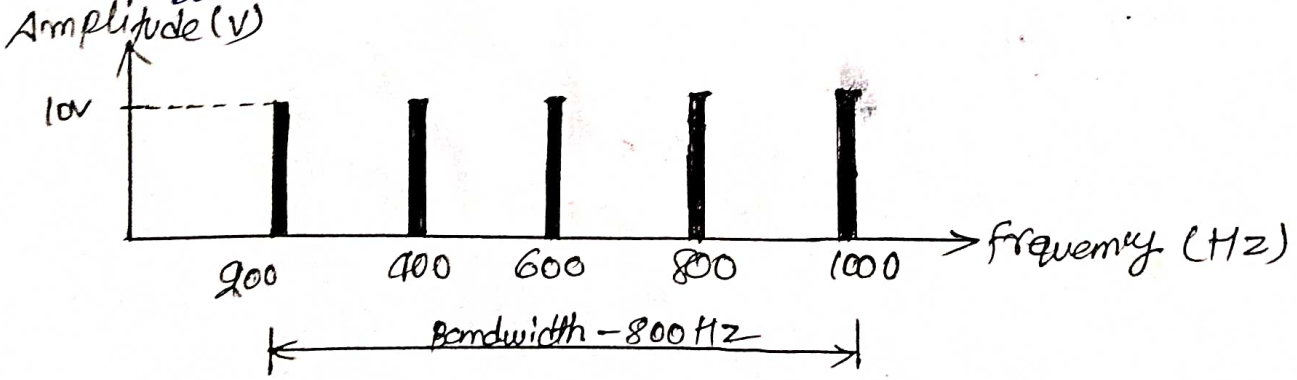
IPV4	IPV6
(i) Address size of IPV4 is 32 bits.	Address size of IPV6 is 128 bits.
(ii) Address formate of IPV4 is dotted decimal	Address formate of IPV6 is Hexadecimal.
(iii) Header size of IPV4 is 20 - 60 bytes.	Header size of IPV6 is 40 bytes.
(iv) IPV4 is widely supported by all devices.	IPV6 is not widely supported as IPV4.
(v) checksumfield is available in IPV4.	checksumfield is not available in IPV6.

(pg8) If a periodic signal is decomposed into five sine waves with the frequencies of 200, 400, 600, 800 and 1000 Hz, what is its bandwidth? Draw the spectrum assuming all components have a maximum amplitude of 10v.

∵ bandwidth = highest frequency − lowest frequency

bandwidth = 1000 − 200 = 800 Hz

bandwidth is 800 Hz.



(ii) A sine wave is having 1/6 cycle with respect to time 0. what is phase in degrees and radians.

ans → $\frac{1}{6}$ cycle that is $\frac{1}{6} \times 360 = 60$ $= \frac{60 \times 2\pi}{360} = \frac{\pi}{3}$

(iii) The Period of a signal is 100 ms. what is its frequency in kilohertz.

ans → time = 100 ms $100 \times 10^{-3} = \frac{100}{1000} = 0.1$ s $f = \frac{1}{T}$ $f = \frac{1}{0.1}$ $f = 10$ Hz

in kilohertz $= \frac{10}{1000} = 0.01$ kHz