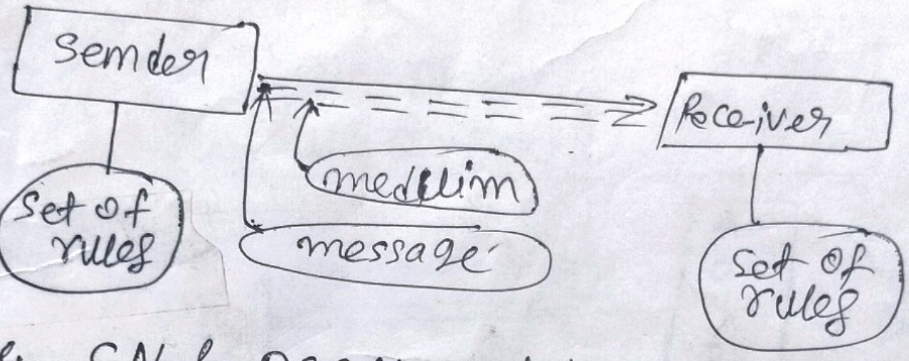
Computer Network = DCCN

Computer network refers to the interconnected 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.

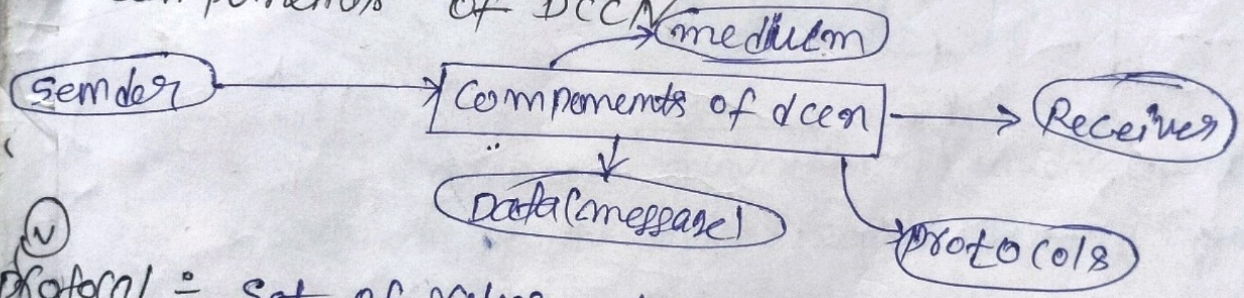
* DCCN devices are capable of sending & receiving the data over a communication medium.



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.

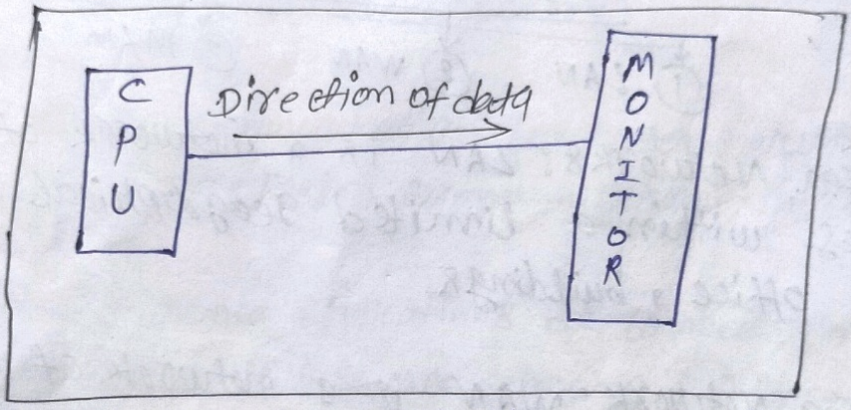
Define data flow or streamm processing or re-active progra & types of dataflow ~~and~~ ~~its goals with diagram~~ naming.

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

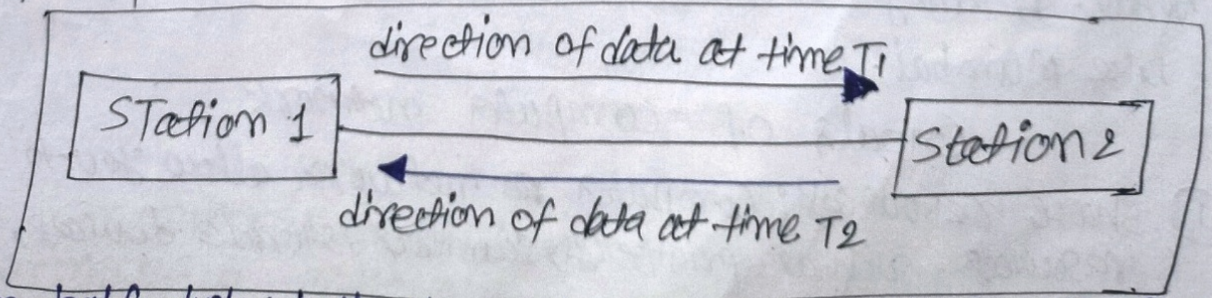
1. Simplex
2. Half Duplex
3. Full Duplex

(1) Simplex:



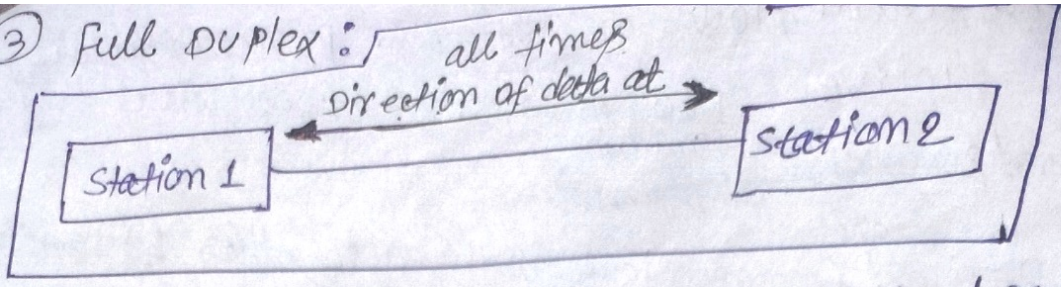
- In Simplex, communication is unidirectional
- only one of the devices sends the data and the other one only receives the data.
- Example: in ~~the~~ above diagram: a CPU send data while a monitor only receives data.

(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.

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.

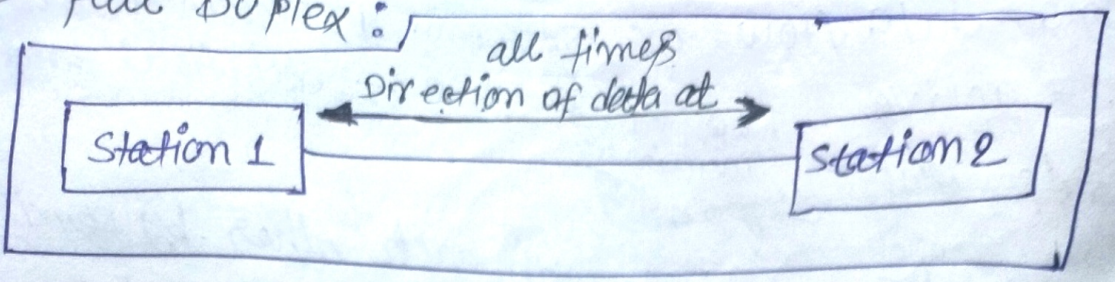
② Wide Area Network: WAN is a network of computers and devices that spans a large geographical area. The network in the entire state of Maharashtra could be a WAN.

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.

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.

~~diagram~~.

Types

(**) 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.

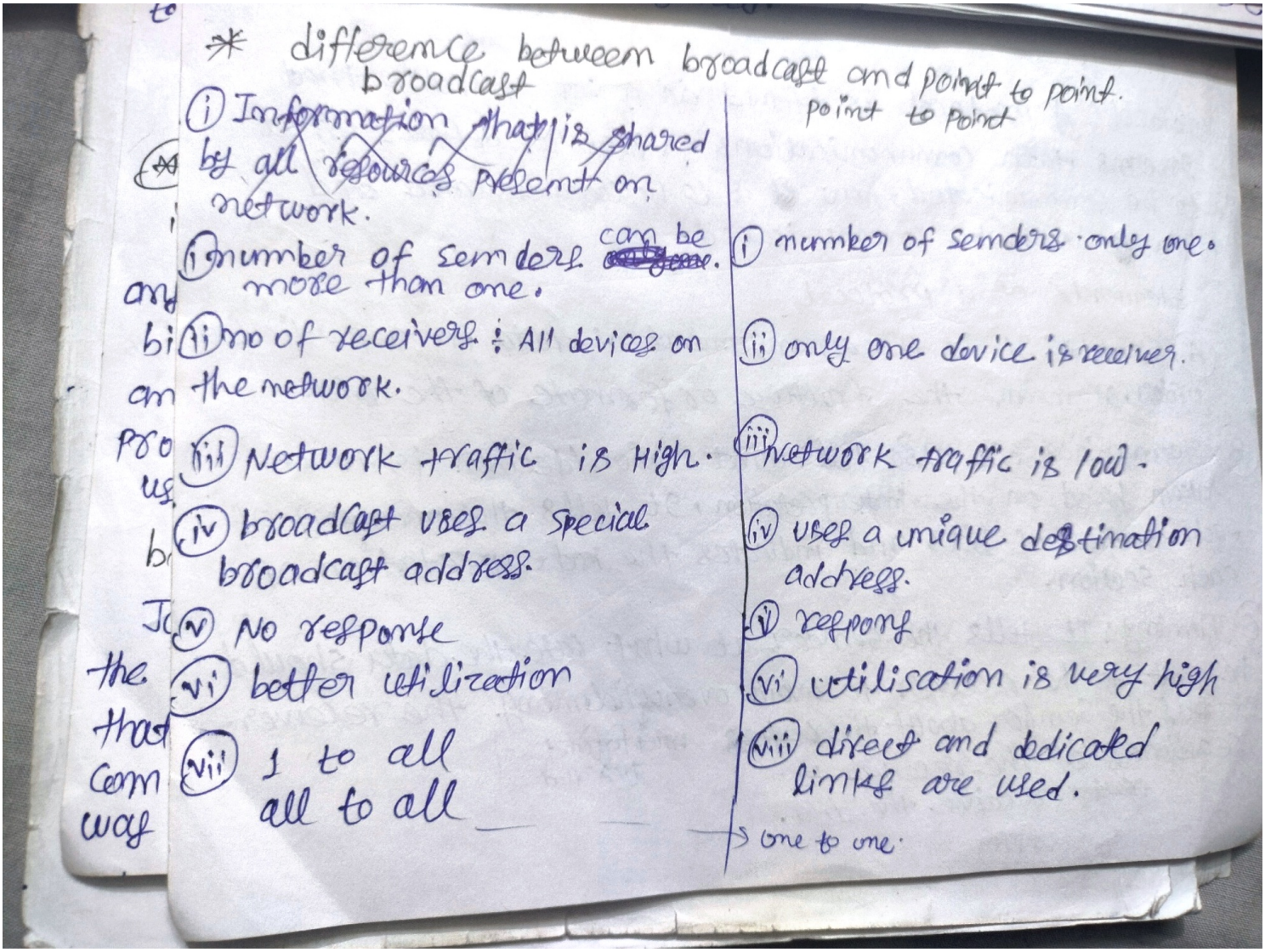
other words

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

receive the data.

* 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 ~~you 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 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.



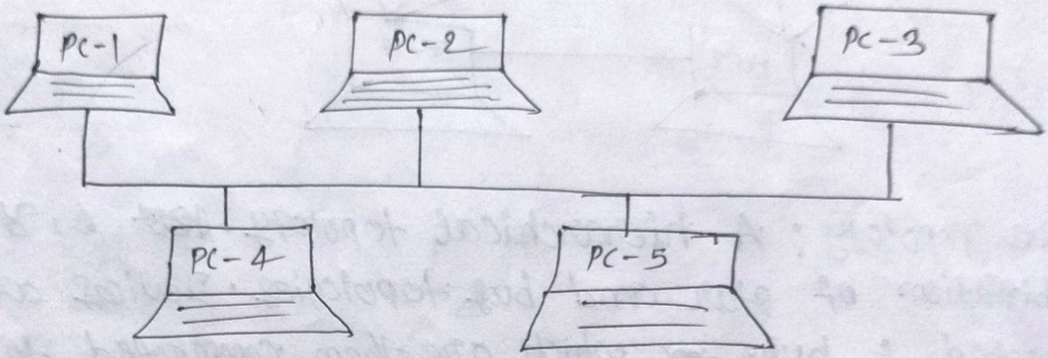
* difference between broadcast and point to point.

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.

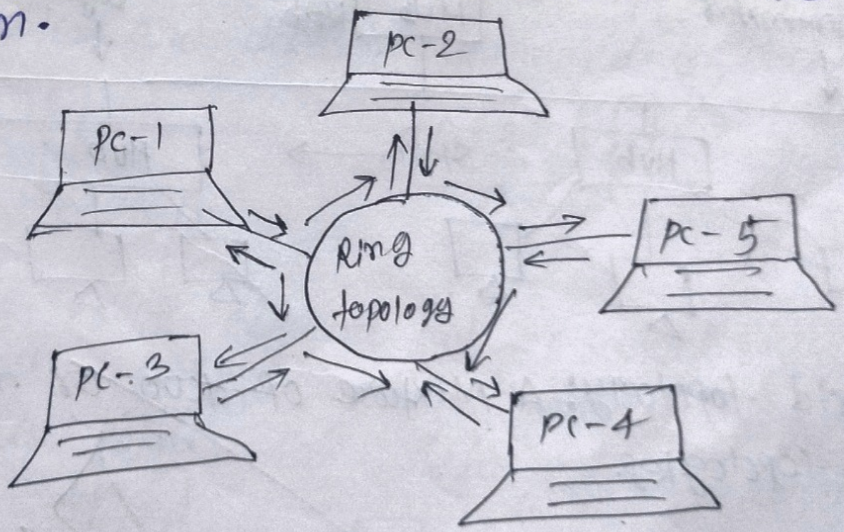
* Network topology: It is a logical & geometrical arrangement of nodes and connection of a network, nods can be switches, routers.

Types of Network topologies:

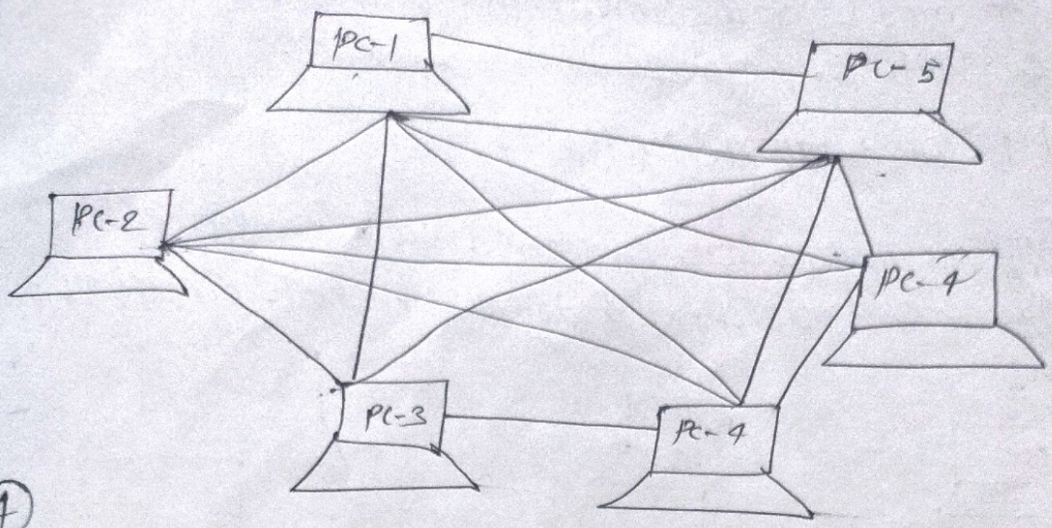
1. Bus topology: All devices are connected to a single cable, called the bus topology, data travels in both directions along the bus.



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

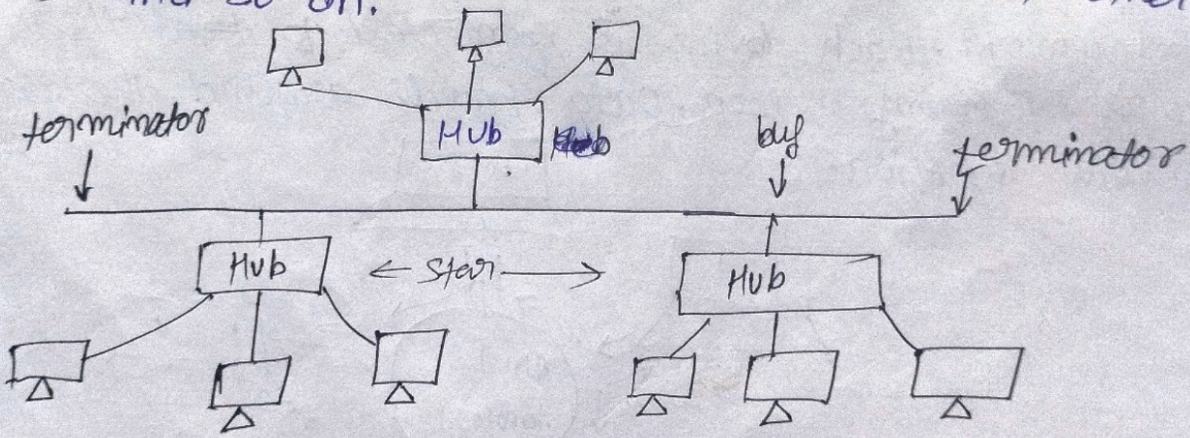


• Mesh topology: Every device is connected to every other device.



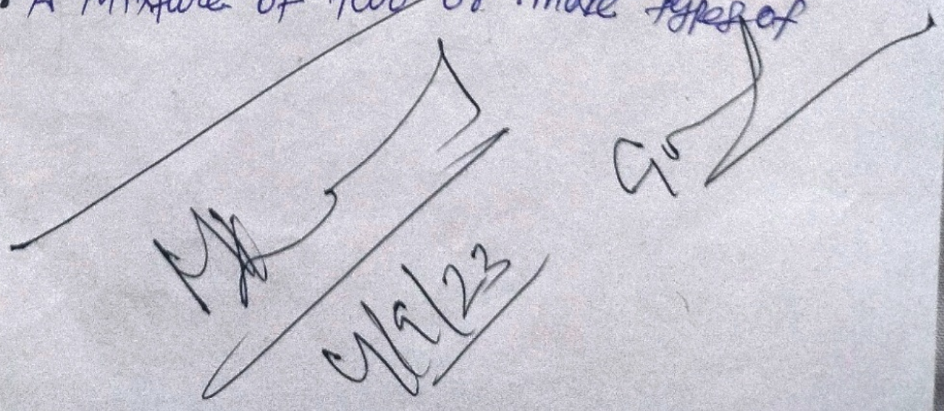
④

• 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.

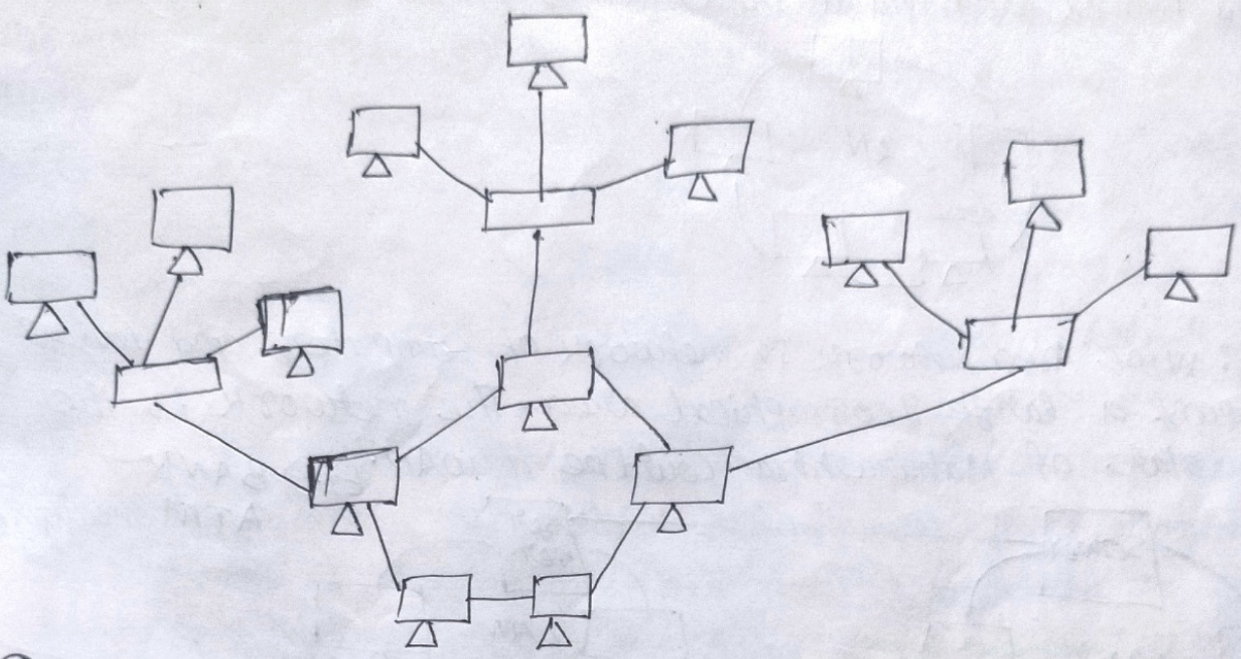


③

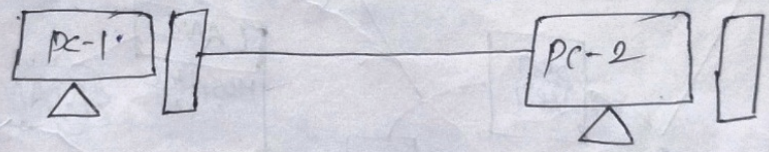
• Hybrid topology: A Mixture of two or more types of topologies.



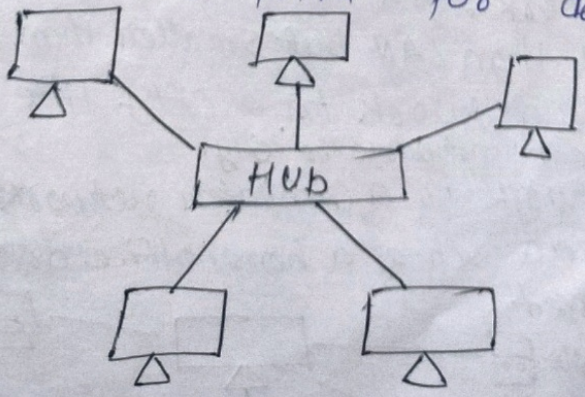
5) Hybrid topology: A hybrid topology is combination of two or more different types of topologies. It is created by interconnecting multiple smaller topologies to form a large, more complex network.



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



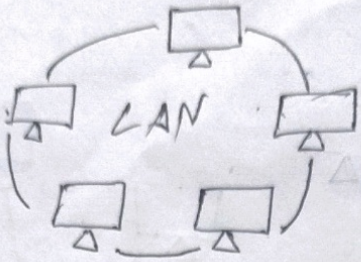
7) Star topology: It is a central hub or switch is connected to all devices in the network. The hub acts as a central point for data communication.



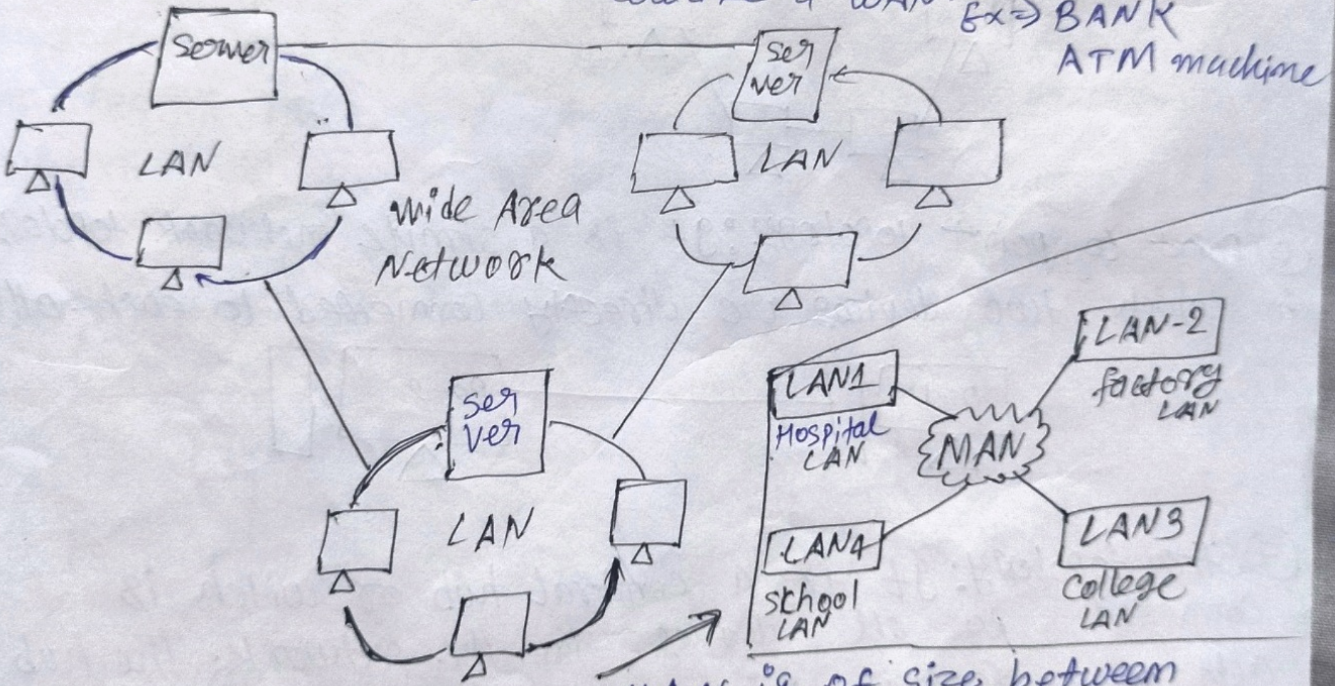
Types of Network

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.



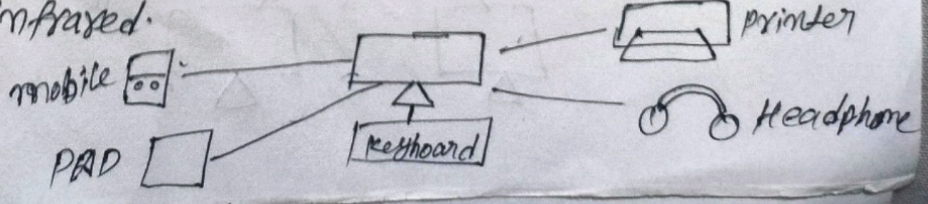
② WAN: Wide Area Network is network of computers and devices that spans a large geographical area. The network is the entire state of Maharashtra. could be a WAN. Ex ⇒ BANK ATM machine

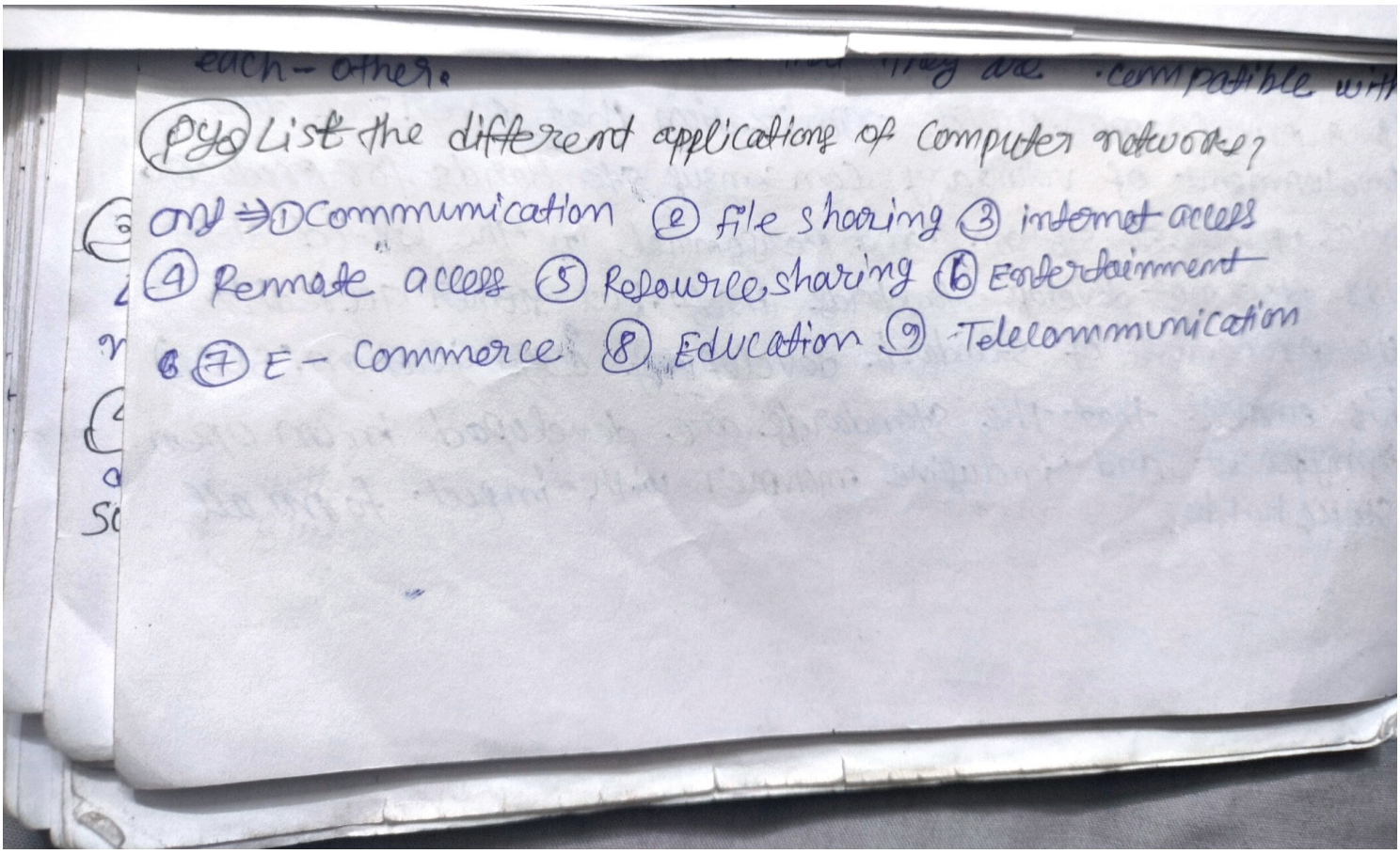


③ Metropolitan area network: MAN is of size between LAN & WAN. It is larger than LAN but smaller than WAN. It may comprise the entire network in a city like Mumbai.

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.





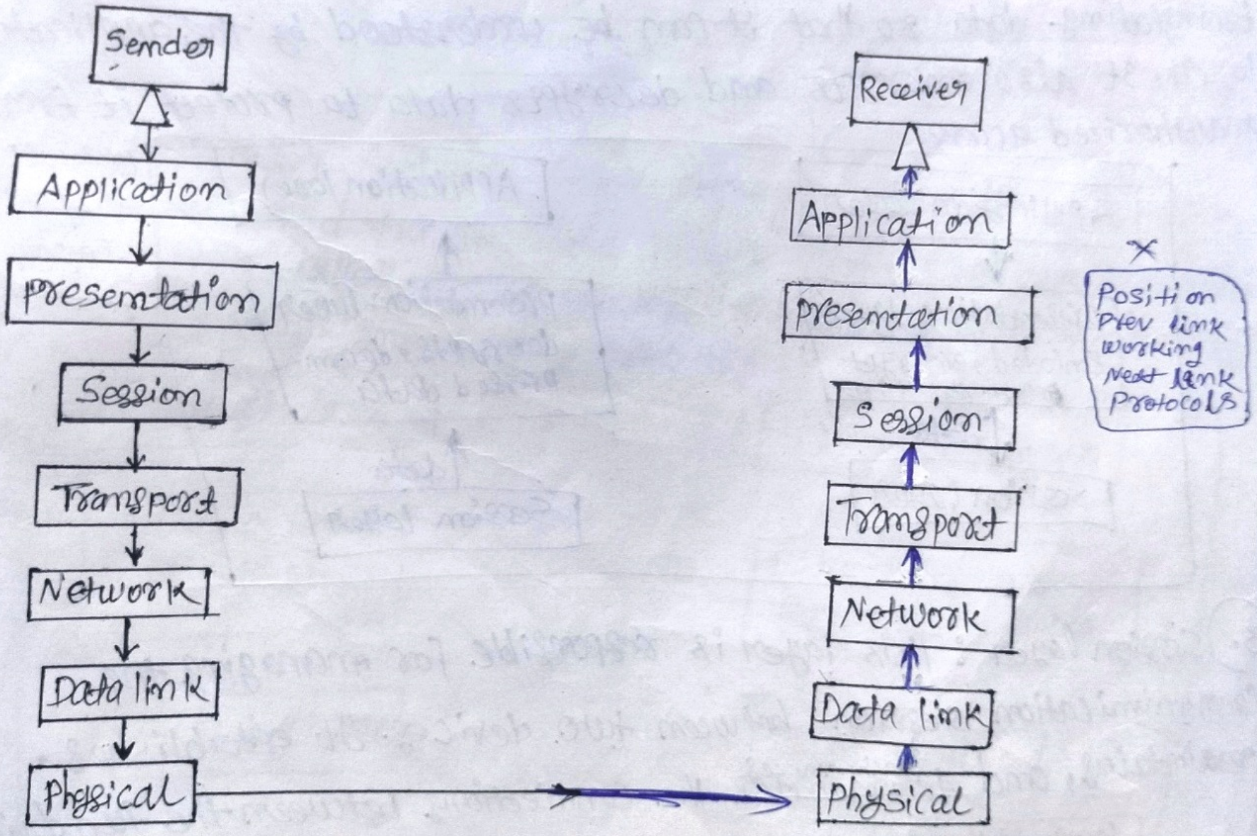
each - other.

(Pg) List the different applications of computer networks?

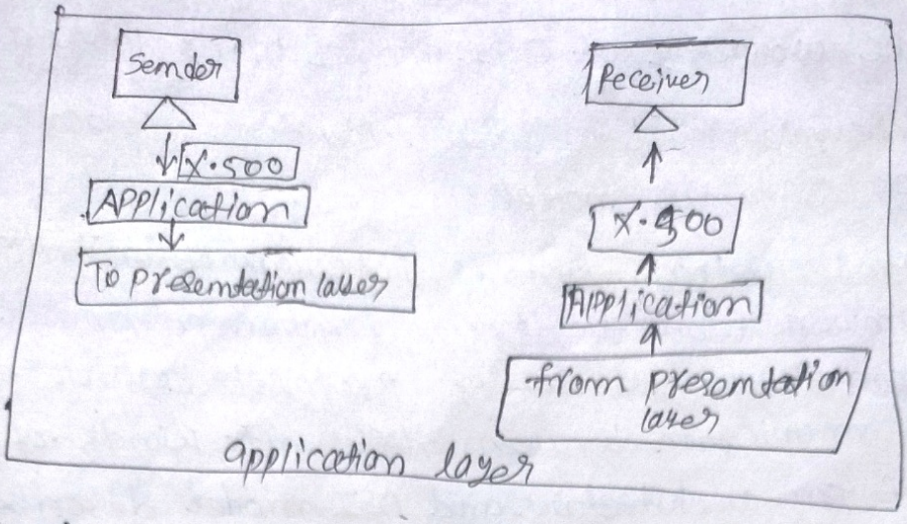
Ans ⇒ ① Communication ② file sharing ③ internet access ④ Remote access ⑤ Resource sharing ⑥ Entertainment ⑦ E - Commerce ⑧ Education ⑨ Telecommunication

Explain the working of OSI model using labeled diagram
or
Explain OSI Referemle model in detail. Mention protocols of each layer of OSI referemle model.

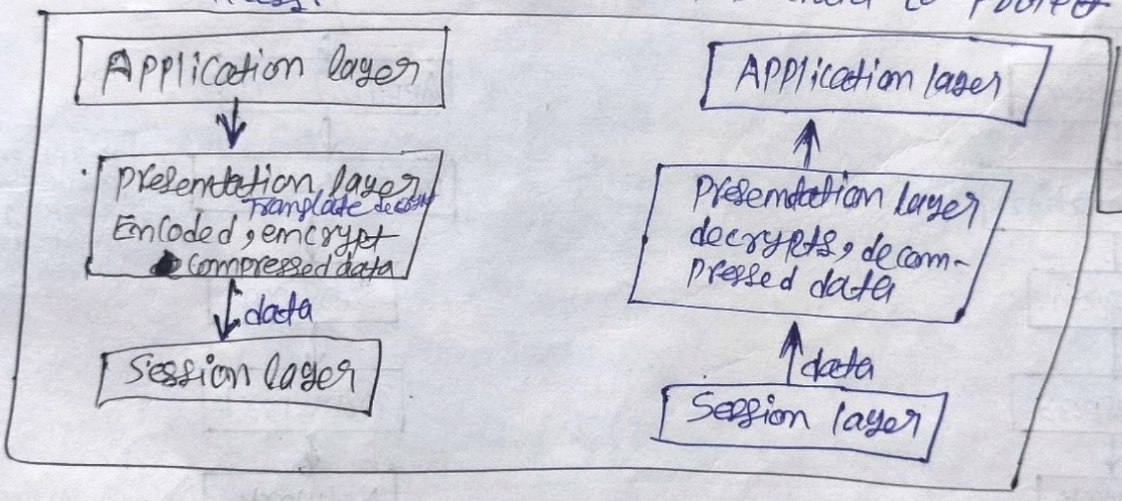
ans → OSI stands for(open systems interconnection) model. It is the framwork used to describe function performed in network system. It is a set of protocols which allows to use the communication between different kinds of system Regardless of an architecture and OSI model describe ~~the process of~~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



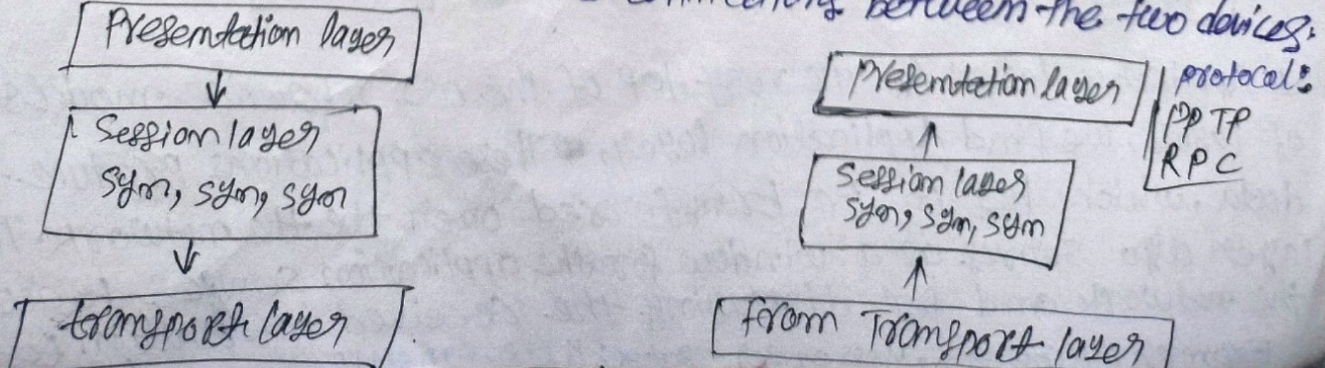
1. Application layer: At the very top of the OSI referemle model stack of layers, we find Application layer, These applications produce the data, which has to be transferred over the the network. This layer also serves as a window for the application sewices to access the network and for displaying the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



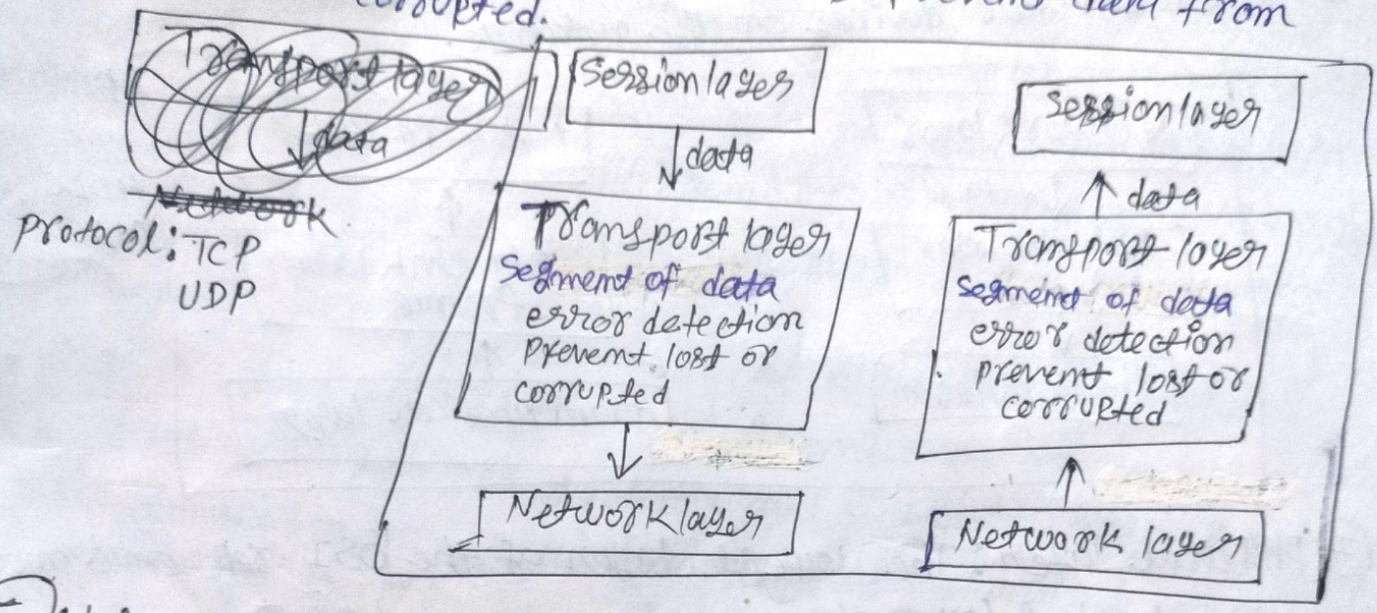
(2.) Presentation layer: The presentation layer is also called the Translation layer. This layer is responsible for formatting and translating data so that it can be understood by the application layer. It also encrypts and decrypts data to protect it from unauthorized access.



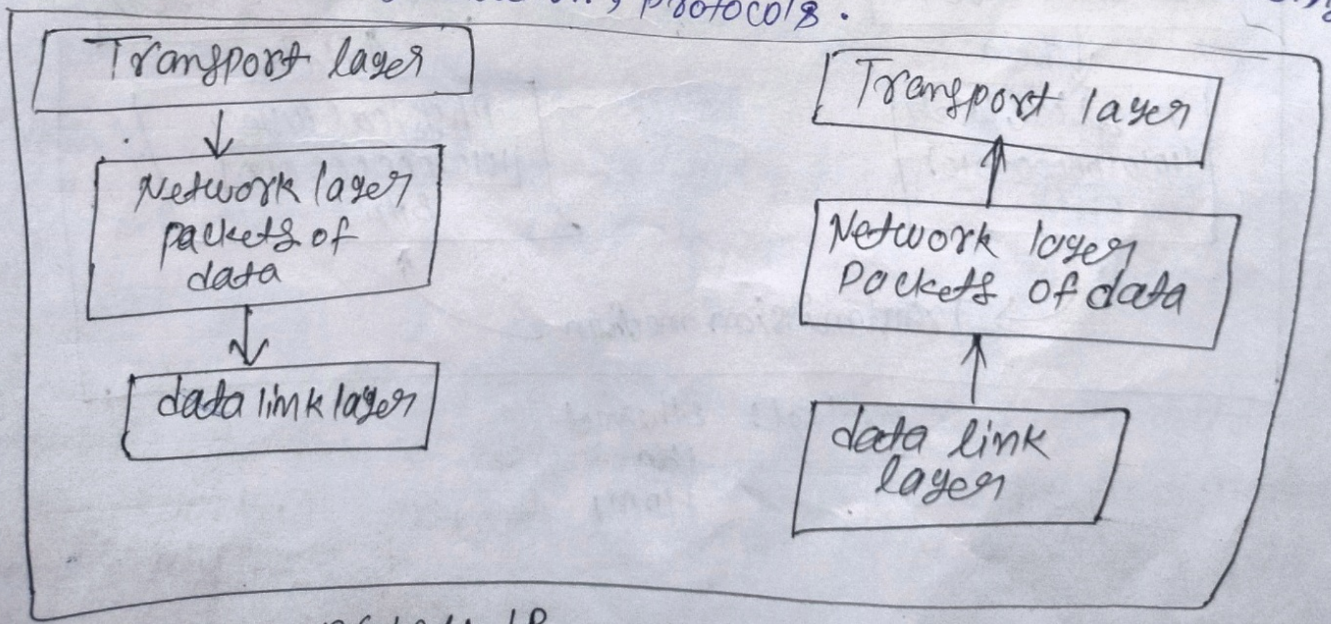
(3.) Session layer: This layer is responsible for managing the communication session between two devices. It establishes, maintains, and ~~terminates~~ synchronizes the connections between the two devices.



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.

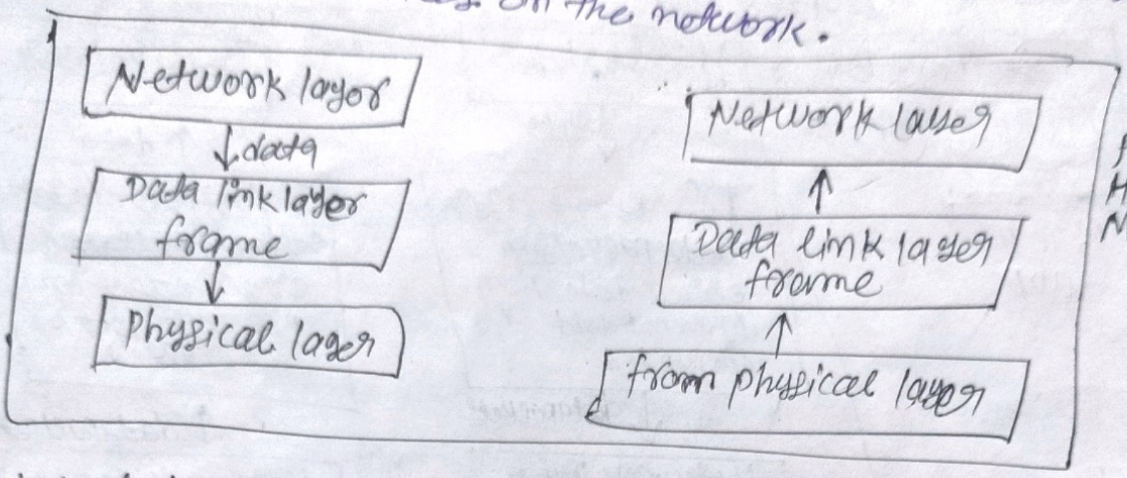


5. Network layer: Network layer convert segment of data to data packets and transfer data packets from network layer to data link layer. It stores IP addresses, logical addressing, Routing, packet fragmentation, protocols.

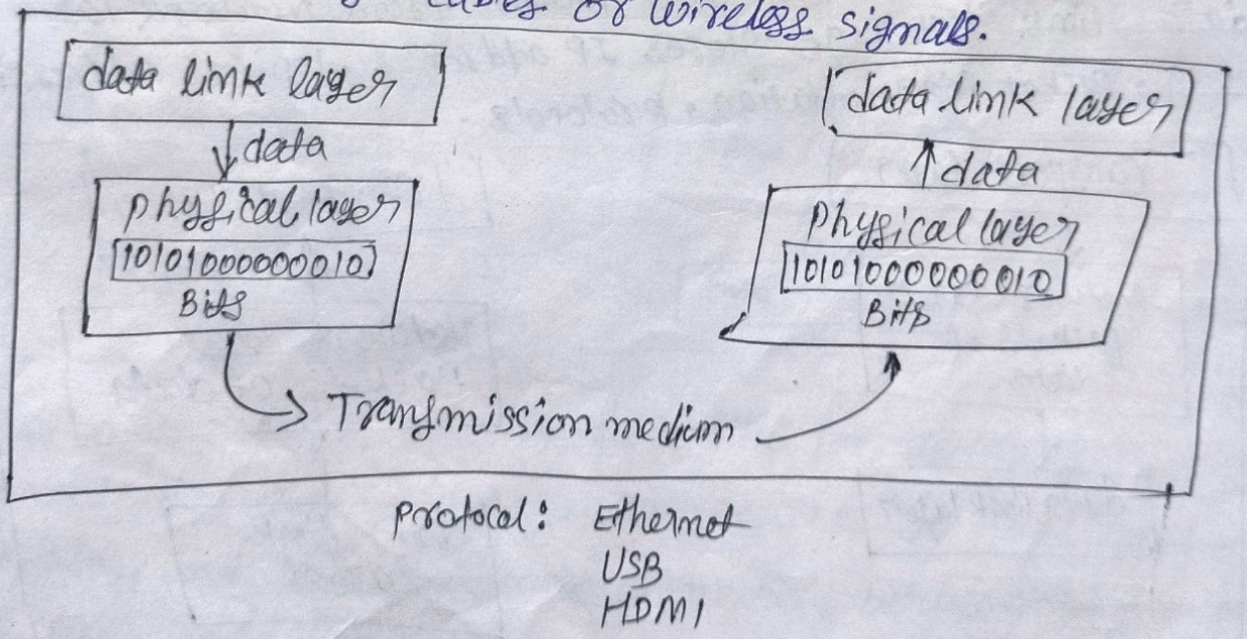


protocal: IP
ICMP

(6.) Data link layer: Data link layer further ~~divided~~ divided 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.



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 reliable protocol.	(iii) It is not reliable 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 bytes.	(vi) The header size of UDP is 8 bytes.
(vii) Retransmission of lost packet is possible	(vii) Not possible.
(viii) Secure.	(viii) unsecure.
(ix) flow control.	(ix) No flow control.

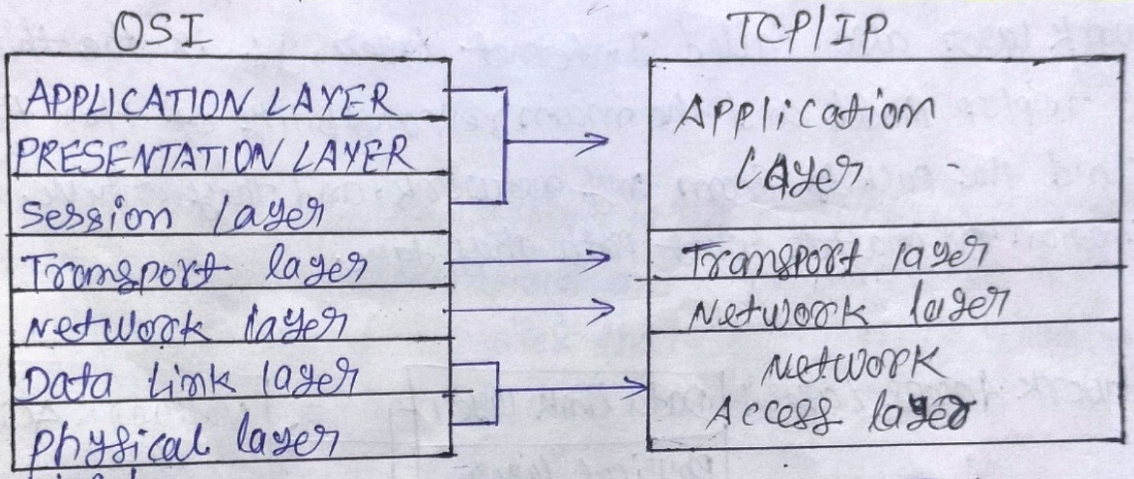
Explain the working of TCP/IP model using labled diagram.

Introduction:-

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

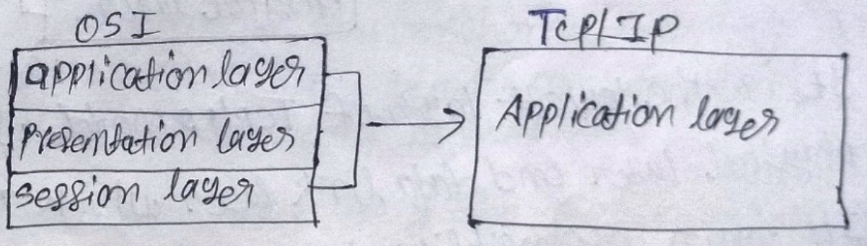
TCP/IP is also used as a communication protocol in computer network. TCP/IP specifies how data is exchanged over the internet by providing end-to-end communication that identify how it should be broken into packets, addressed, transmitted and received at destination. It consists four layers.

diagram:-



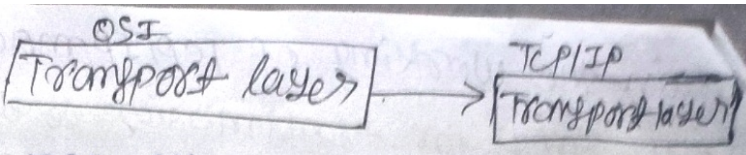
* working

① Application layer:



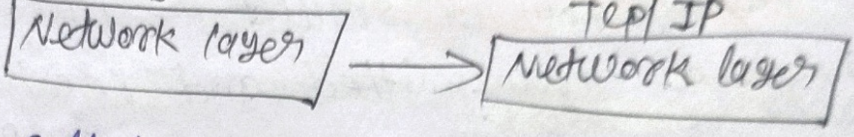
→ Application layer is the topmost layer in the TCP/IP model. It is responsible for handling high level protocols issue of presentation. This layer allows the user to interact with the application. When one application layer wants to communicate with another application layer, it forwards its data to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

② Transport layer:



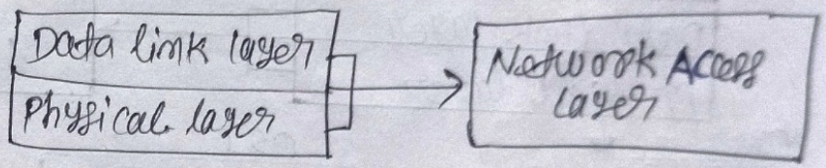
The transport layer is responsible for the reliability, flow control and, correction of data which is being send over the network. There are two protocols used in this layer (i) TCP (Transmission control protocol) (ii) UDP (User Datagram protocol): After that it forwards its data to Network layer.

③ Network layer:

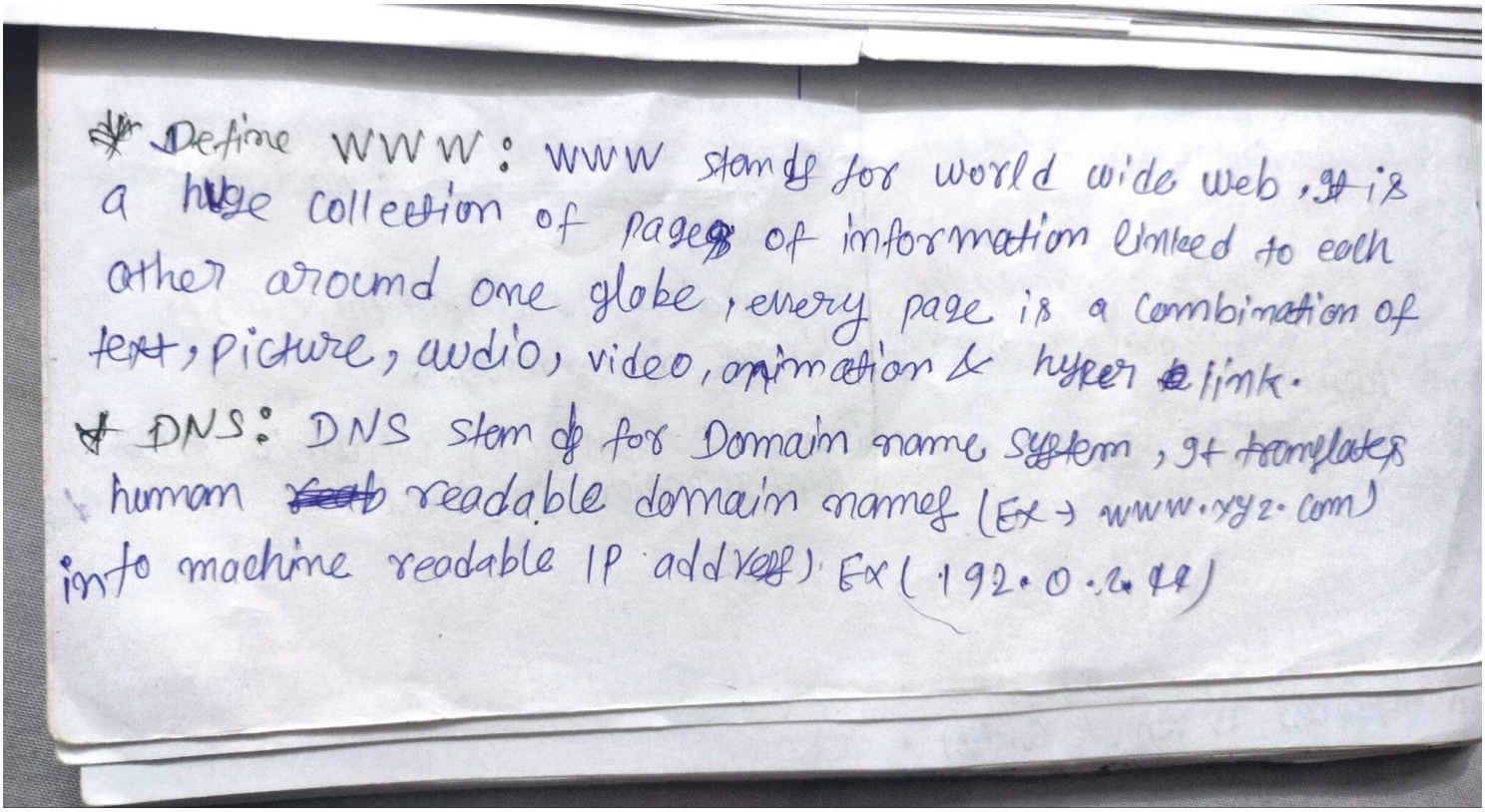


Network layer also called Internet layer, It is the third layer of the TCP/IP Model and the main responsibility of this layer is to send the packets from any network, and they arrive at the destination no matter what path they take.

④ Network Access Layer:



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. Its main responsibility is to the transmission of information or data between two devices over the same network.



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

system? ① Message ② Transmitter ③ Transmission medium ④ Receiver used in the data communication

(Pg8) A host communicates with another host using the TCP/IP protocal suite. what is the unit of data sent or received at network layer?

ans ⇒ the unit of data sent or received is called "packet".

(Pg8) 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.

(Q4) 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.

(Q5) 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.

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

* Differentiate among Twisted pair, Coaxial cable and fiber optics 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.

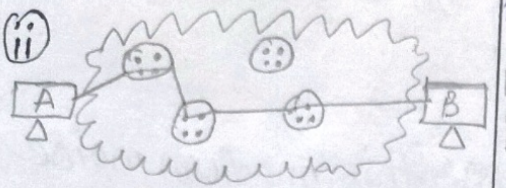
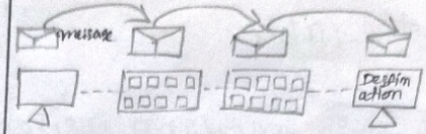
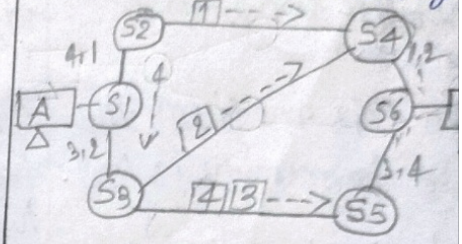
~~* Explain the shielded twisted pair (STP):~~

Q9) 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.

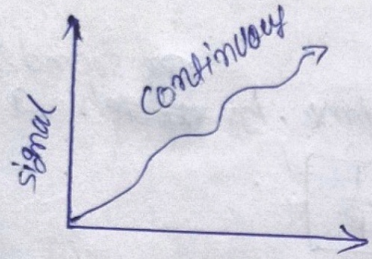
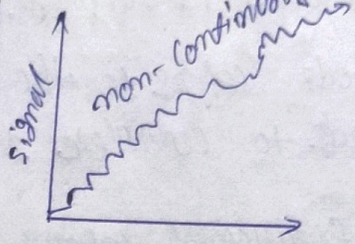
Q10) Explain Ethernet: Ethernet is the traditional technology for connecting devices in a wired local area network (LAN) It enables devices to communicate with each other via a protocal.

* 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 divided into smaller uni 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 en path before data transmission.
(v) waste of bandwidth is possible.	No waste of bandwidth	No waste of bandwidt
(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 differences between analog and digital signal.

Analog	digital
(1) 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.

* Data Rate limit: • 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~~ 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)
↳ how many signal levels we need.

② shannon capacity: (unit bps)

$\boxed{\text{Capacity} = \text{bandwidth} \times \log_2 (1 + \text{SNR})}$ 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 ⇒ $\text{Bitrate} = 2 \times \text{bandwidth} \times \log_2 L$

given: $b = 4000$ Hz, $L = 2$

$\text{Bitrate} = 2 \times 4000 \times \log_2 2$ (1)
$= 2 \times 4000$
$= 8000$ 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?

given: $b = 20 \times$ kHz
$br = 280$ kbps

Note: bandwidth unit → Hz

ans ⇒

$br = 2 \times b \times \log_2 L$

$280 = 2 \times 20 \times \log_2 L$

$7 = \log_2 L$

$\log_2 L = 7$

$L = 2^7$

$\boxed{L = 128 \text{ levels}}$

$\boxed{\log_e x = y}$

$\boxed{x = e^y}$

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 $B = 3000\ Hz$ $SNR = 3162$

$\boxed{B = 3\ kHz}$

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

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

$C = 3000 * \log_2(3163)$

$C = 3000 * 11.627$

$\boxed{C = 34881\ bps}$

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

FQ 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 Q

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

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

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

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

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

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

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

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

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

$C = 2392 \times 10^4$ bps

Approx $= 3978.6$

$\because \frac{11.96}{2} = 3988$

bit rate = $2 \times$ Bandwidth $\times \log_2 L$

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

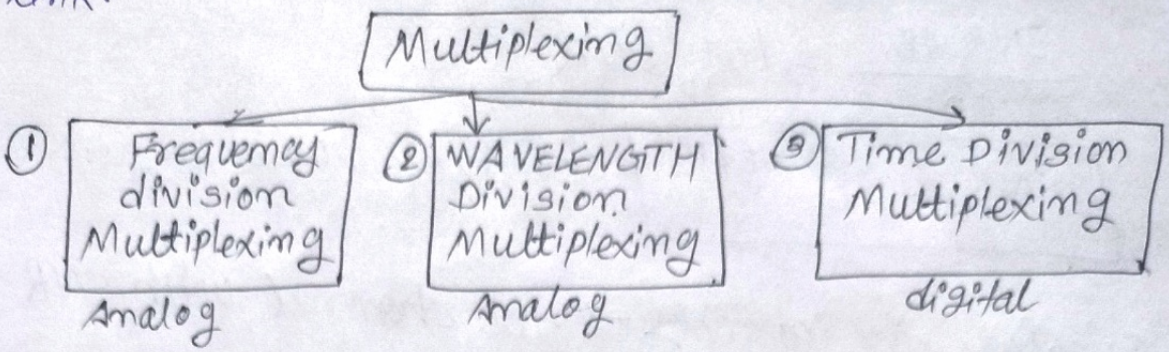
SNR = Avg signal power / Avg noise power

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

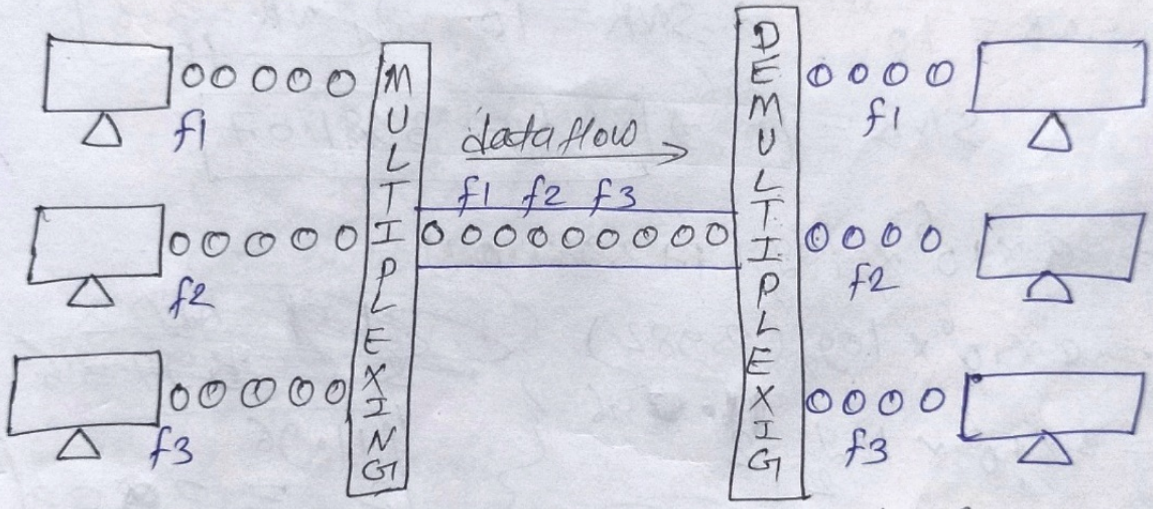
$SNR_{dB} = 10 \cdot \log_{10} SNR$

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

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

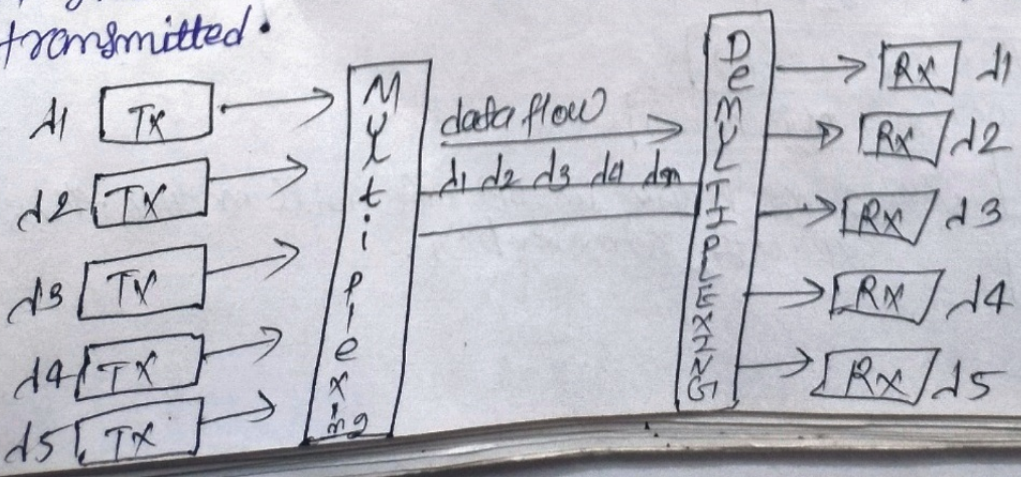


① Frequency-Division Multiplexing: Frequency-division multiplexing is an analog technique that combines analog signals, it can be applied when the bandwidth of a link is greater than the combined bandwidth of the signals to be transmitted.

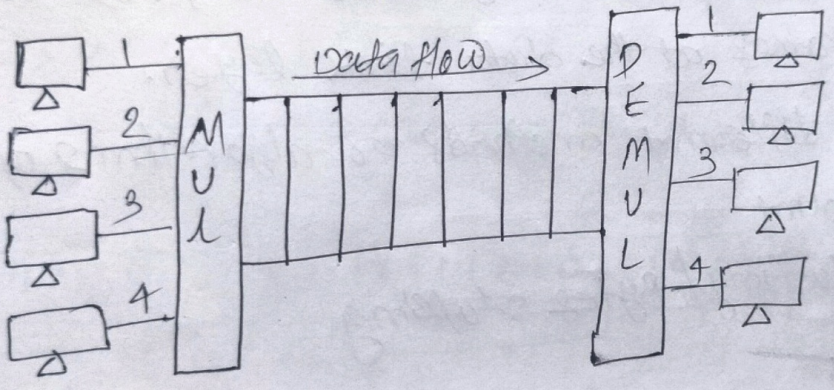


Frequency division Multiplexing

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.



channel

(*) 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 protocal 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 ~~and network configuration~~ 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 protocal.

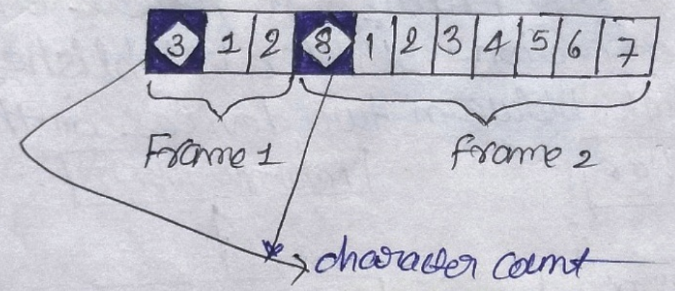
Q. Explain framing and different algorithms.

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.

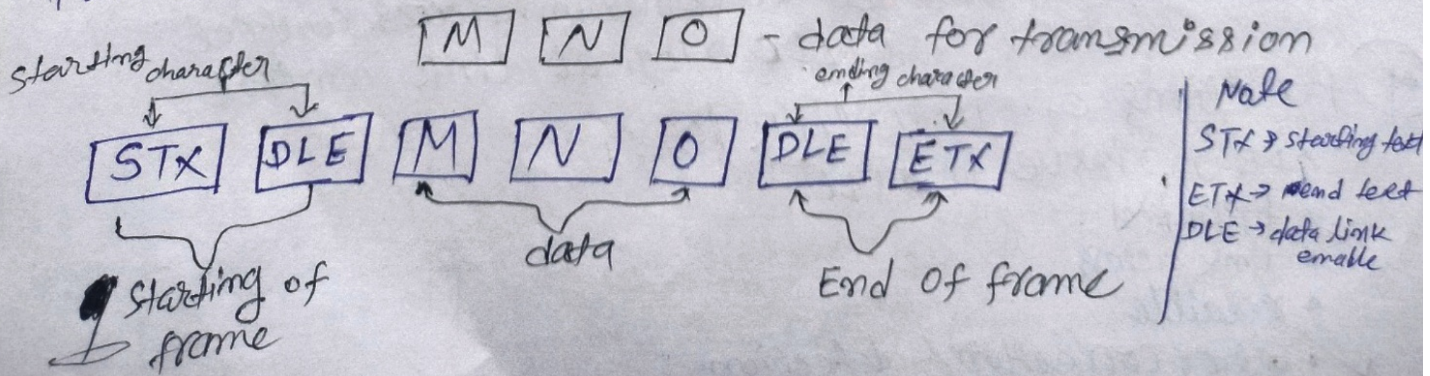
There are three different methods or algorithms of framing

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

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



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

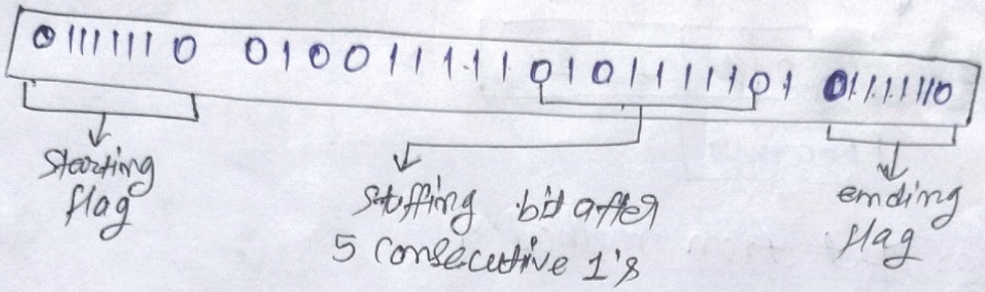


Bit stuffing: Bit stuffing is the inserting of non-information bits into data. It is called bit stuffing. the begining and end of each frame via a specific bit pattern 01111110 → flag byte.

original data: will have

→ 0 1 0 0 1 1 1 1 1 1 1 0 1 1 1 1 1 1

After 5 consecutive 1's insert (0)



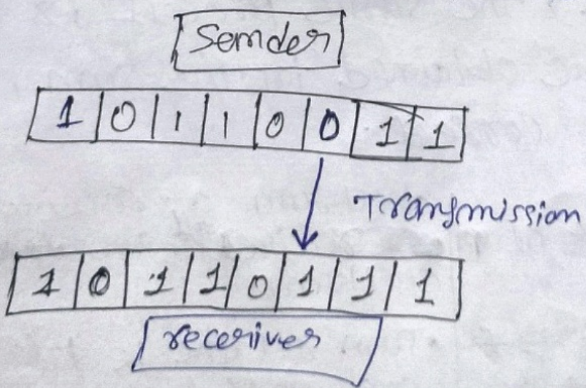
* Error detection and correction techniale.

What is error and its type.

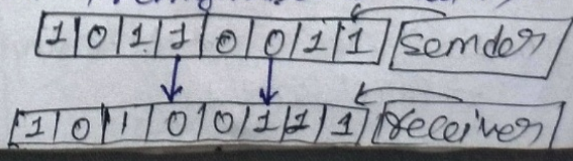
ans: Error is a condition when the receiver's information does not match the sender's information during the transmission. Types of error

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

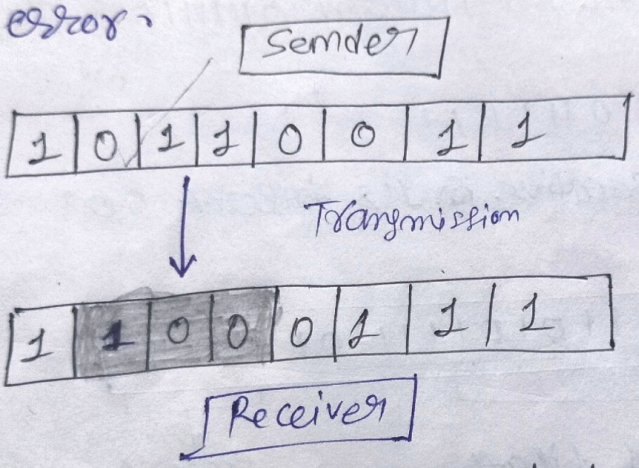
(i) single bit error: A single-bit error occurs when one bit of a transmitted data is changed during transmission.



(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 method's

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

Q1. ~~1001100111100010001001001000100~~

1001100111100010001001001000100

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
1 0
carry
  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
C +             1 0
  1 1 1 1 1 1 1 1
```

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 0 1

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

(2) 1's comp

```
  1 1 1 0 0
```

checksum

10110	11010	10001

block

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

at receiver side

```
  10110
  11010
  10001
  11100
  10 1 0 1
     1 0
  11111
```

received

CRC (cyclic 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 (L-1)
```

XOR operation same - 0 diff - 1

0 से start होगा तो XOR नहीं होगा divisor को

CRC : 110

Data transmitted : 1001110

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

1001 & 000 = 1001000

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

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? (1100 10)

```
1010 ) 1100 10 ( 111
       1010
       ----
        110 1
        1010
        ----
         111 0
         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.

$2^P \geq P+m+1$

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

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)]

FQ2m → Define flow and error control. (16)

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).

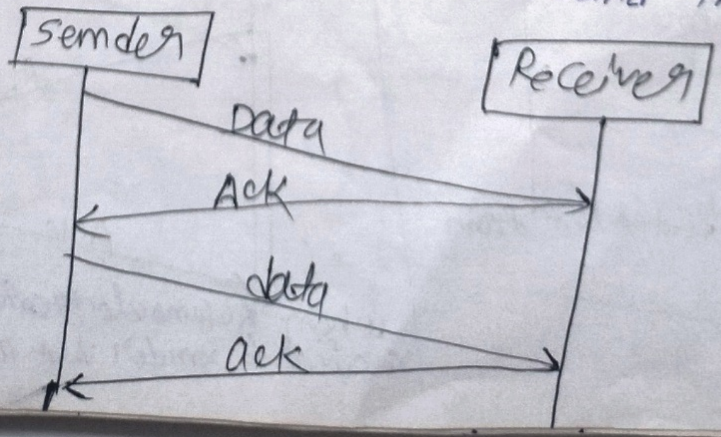
* Error control: Error control is basically process of detecting and re-transmitting data frames in data link layer, that might be lost or corrupted during transmission.

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

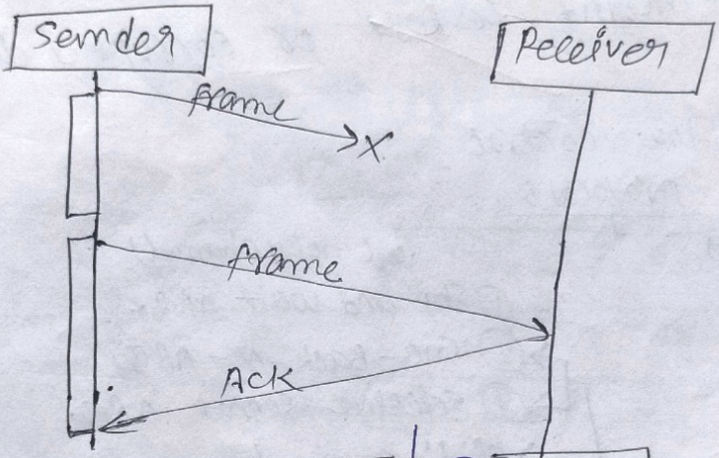
* Stop and wait: After the sender sends one data frame to receiver, one's the acknowledgement is received from the receiver then only the sender can send the next data frame.



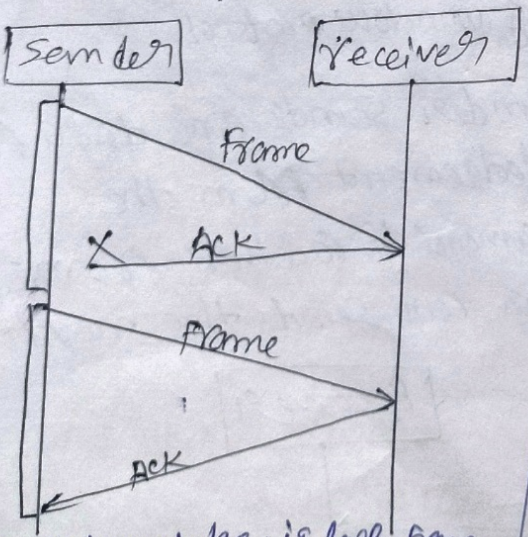
STOP and wait ARQ: After transmitting one frame, the sender waits for an acknowledgement before transmitting the next frame. If the acknowledgement does not arrive after a certain period of time, the sender timeout and retransmits the original frame. This retransmission is automatic that's why we called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

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

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

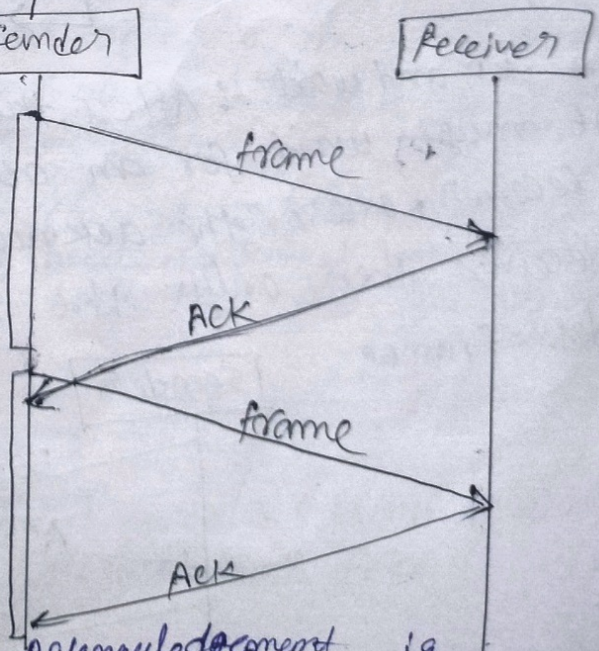


(b)



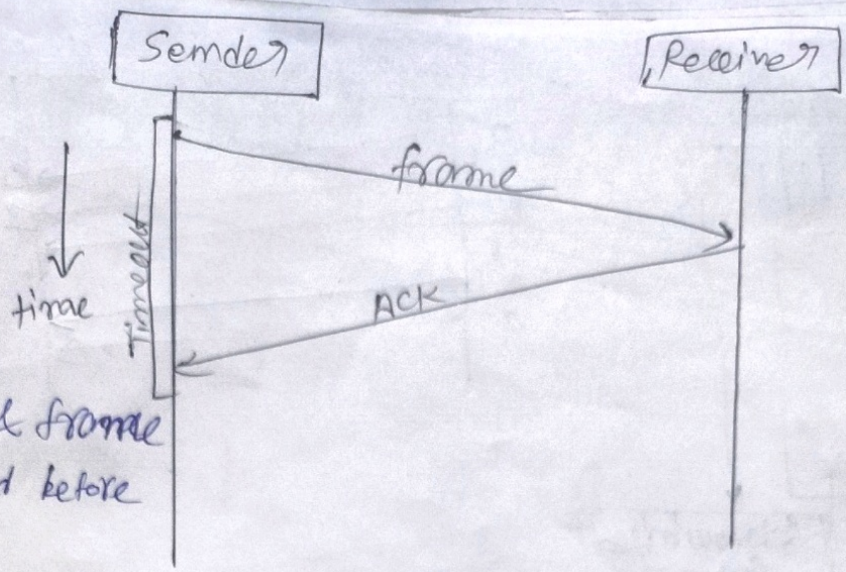
When Acknowledgement is lost from receiver side

(c)



When Acknowledgement is received to sender but after timeout

(d)



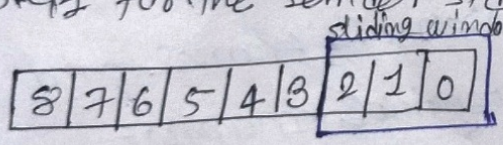
when data & frame both received before timeout.

Q9) Explain the working of sliding window flow control with the help of labeled diagram. or Explain sliding window protocol in detail. 12 marks.

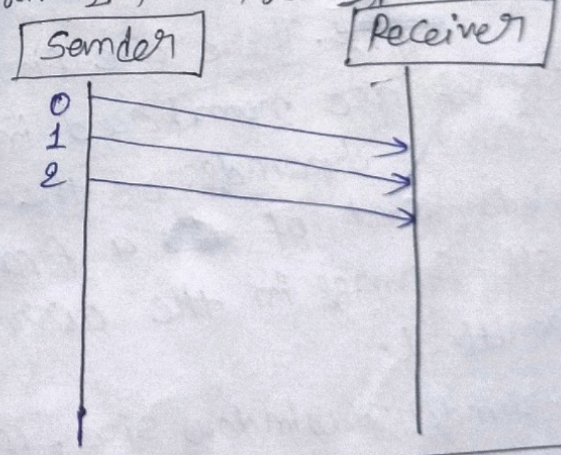
working: The working of the sliding window protocol can be divided into two steps sender steps, and the receiver steps and also some important steps.

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

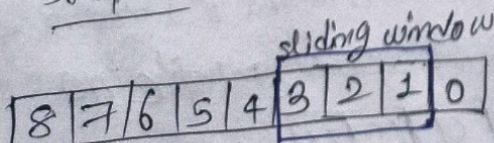
steps for the sender side



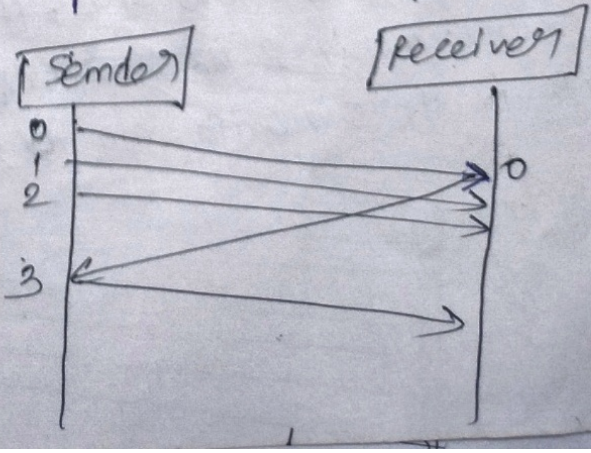
window size 3



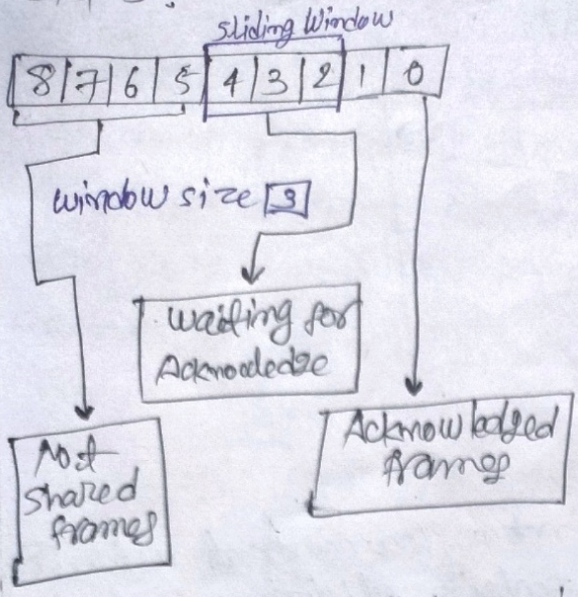
Step-2

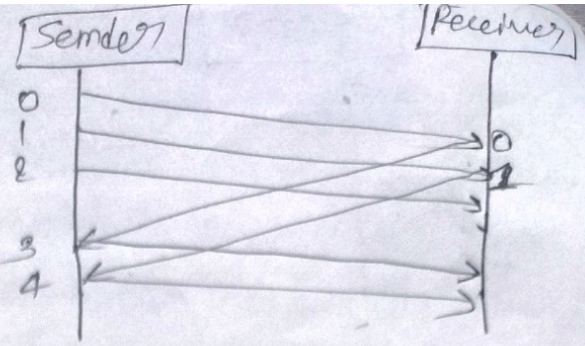


window size 3



Step 3:





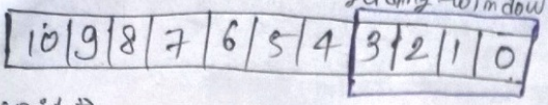
Sliding window protocol

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

* GO-BACK-N ARQ: GO-Back-N ARQ uses the concept of protocal 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.

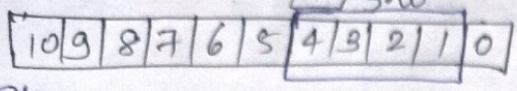
here → N - Sender's window size, if the window size = 4 (2^2) then the seaumce no is 2 [illegible] the no of bits in the sequmce no is 2 is 00 01 10 11

Working of GO-BACK-N-ARQ

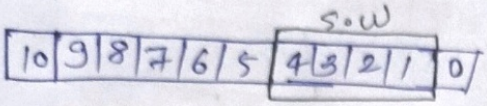


step:1 →

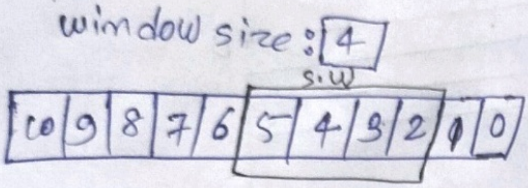
window size: 4



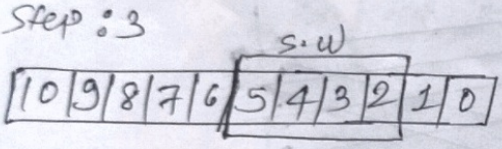
Step: 2



window size: 4

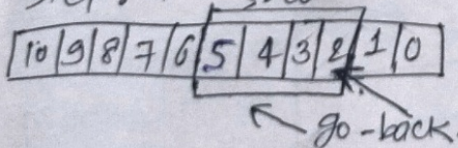


Step: 3



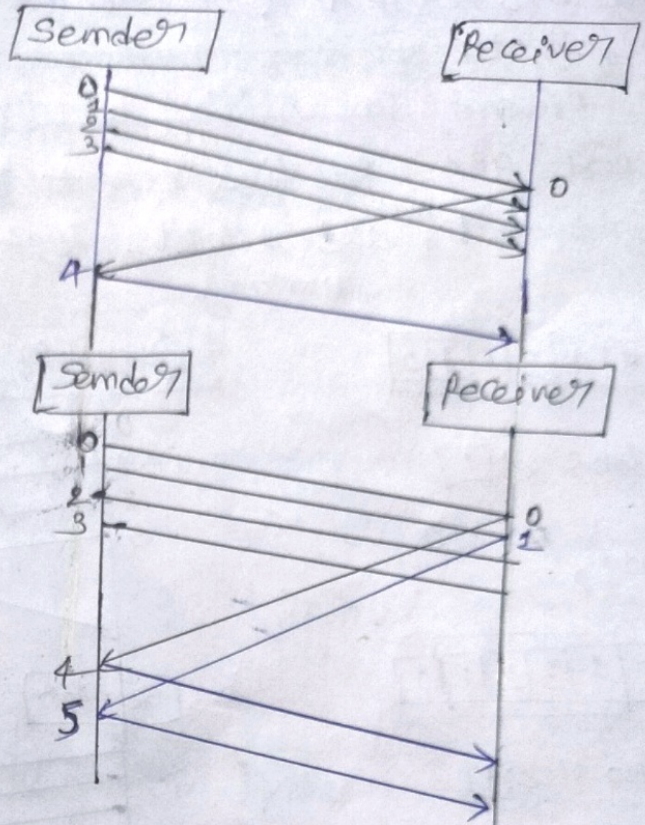
window size: 4

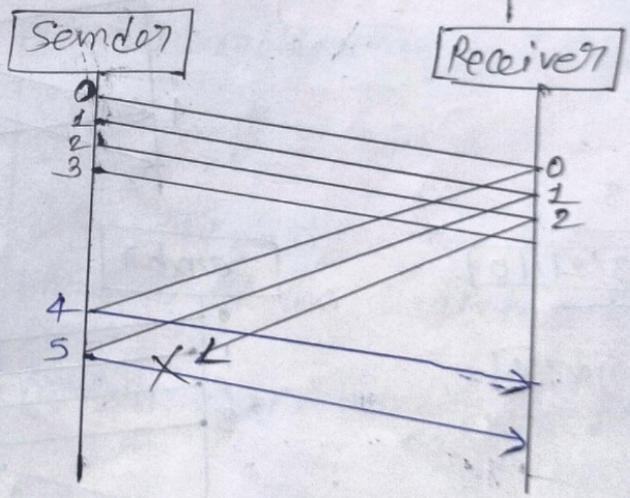
Step: 4

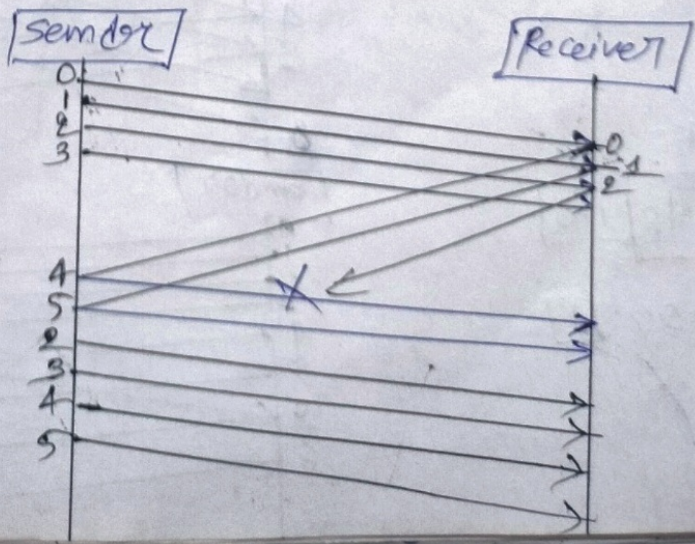


window size: 4

and so on.

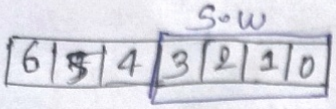




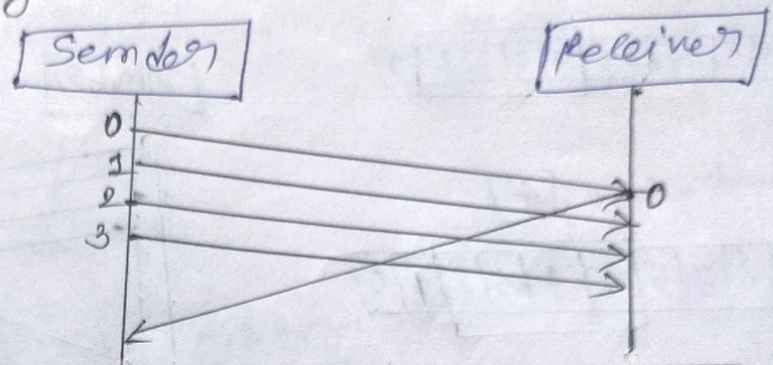


(ii) * Selective Repeat ARQ: In GO-BACK-N-ARQ if any one frame is lost the we have to retransmit all the frames which are present in sliding window but in case of selective repeat ARQ, selective repeat retransmit only those frame that are actually lost.

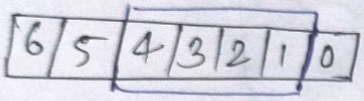
Working



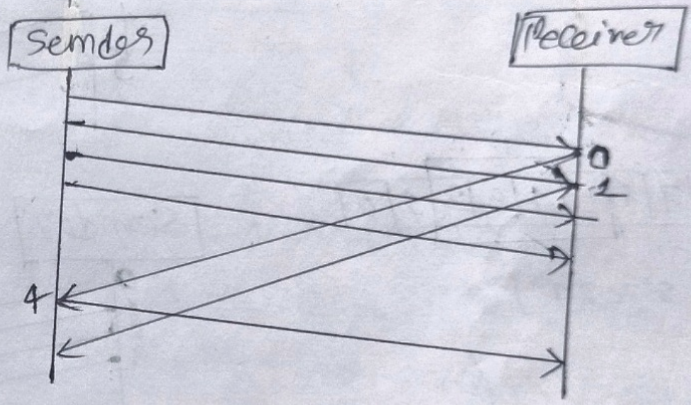
window size: 4



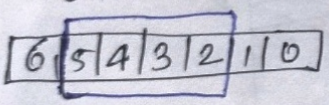
Step: 2



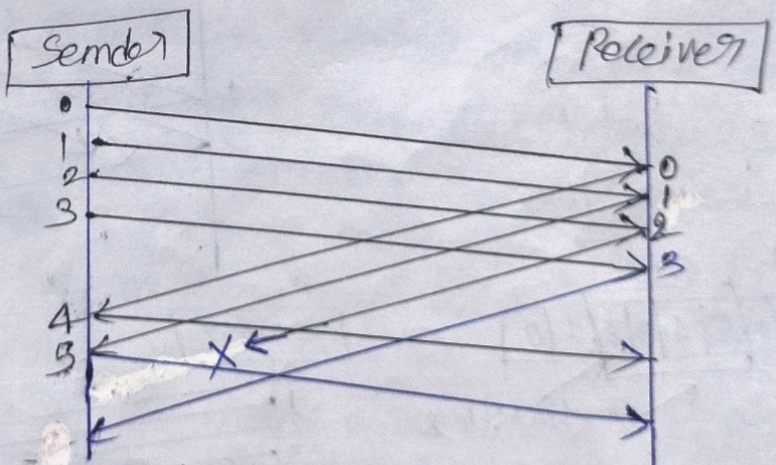
window size: 4



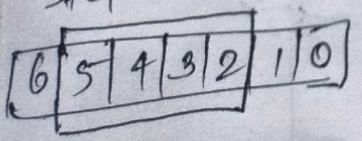
step: 3



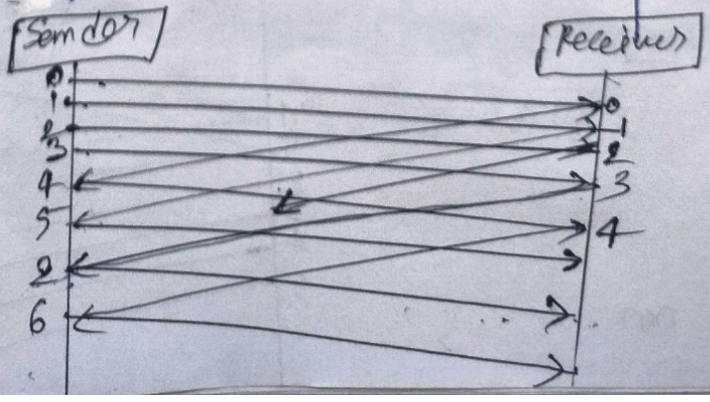
window side: 4



step: 4



Window size: 4



New-chap

Medium Access sub-layer

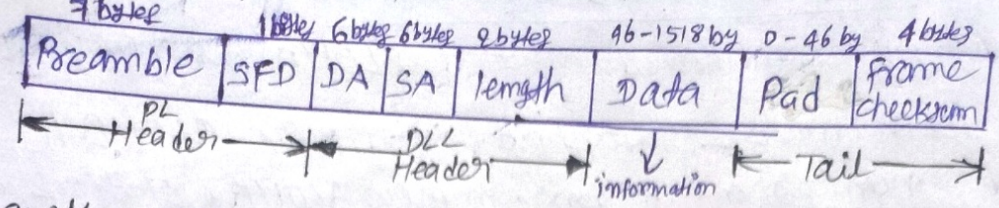
Ques: How throughput is improved in slotted ALOHA over pure ALOHA?

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 frame at the same time. but in case of it leads to collision Slotted ALOHA, Slotted ALOHA divides time into fixed intervals called slots so Stations can only transmit frame at the begining 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.

(Q2) 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 maximum 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.

(*) 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 state of the medium before sending.

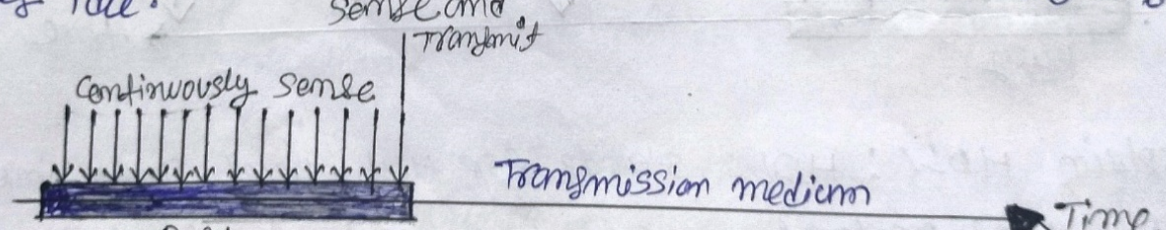
CSMA/CD: CSMA/CD stands for carrier sense multiple Access / Collision detection, CSMA/CD senses the channel first before transmitting the frame. ~~After that it sends a frame~~ if the channel is idle, it transmits a frame to check wheather the transmission was succeffful. If the frame is succeffully 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

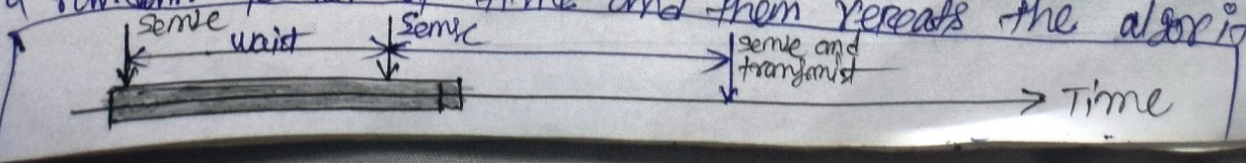
① 1-Persistent ② Non-Persistent ③ P-Persistent ④ O-Persistent

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 continously until it becomes idle.



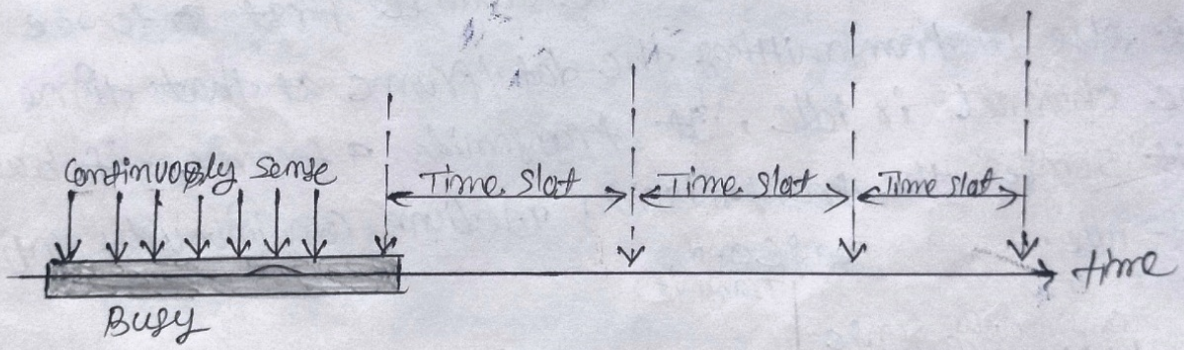
1-persistent

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 continously sense the transmission medium, it waits for a random period of time and then repeats the algorithm.

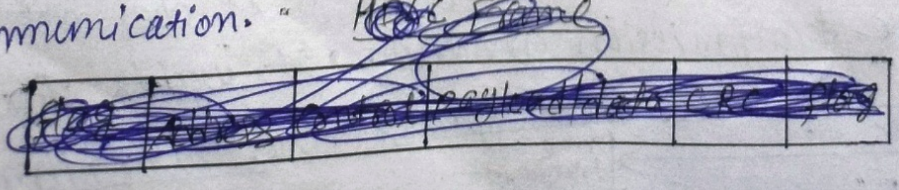


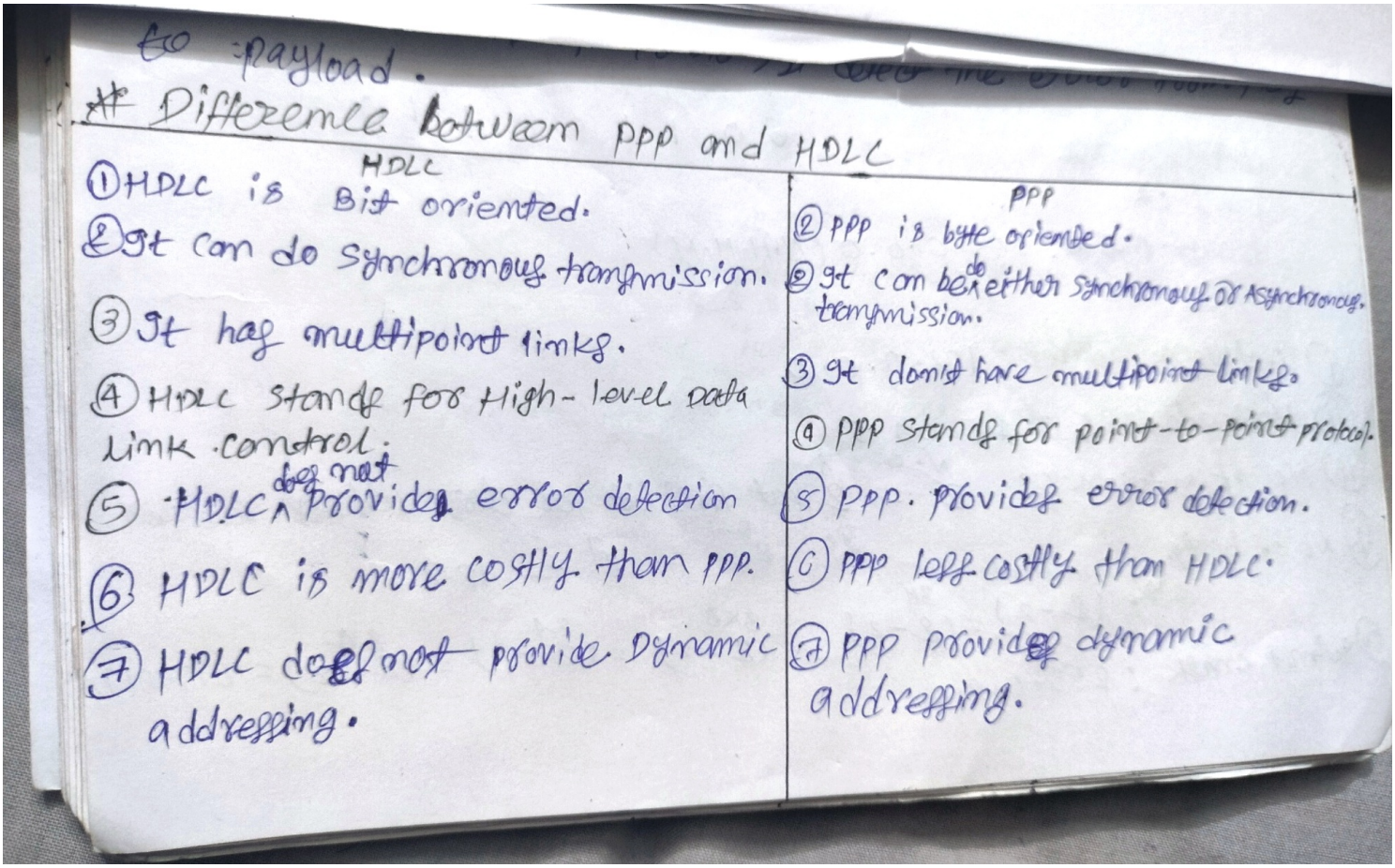
③ O-persistent: It defines the specialty of the channel before the transmission of the frame on the channel. if it is found that the channel is inactive then each station waits for its turn to retransmit the data.

④ P-Persistent: It is the combination of 1-persistent and Non-persistent. The P-persistent mode defines that each node senses a ~~frame~~ 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 co
It is a set of protocal or group of protocal of data link layer for transmitting the data between the network. It being Defined by ISO. It is a bit-oriented protocal th is applicable for both point to point and multipoint communication.





Eg :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 doesn't have multipoint links.
④ HDLC stands for High-level Data Link control.	④ PPP stands for point-to-point protocol.
⑤ HDLC doesn't 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 Oct of 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.

ans → 102.45.09.5

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

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: $2^{N-\text{default}} = 2^8$ 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

Pyq Calculate ⓐ Network address ⓑ host address ⓒ Number of Networks
ⓓ number of hosts ⓔ subnet mask for · ⓘ 102.45.09.5
ⓘⓘ 197.64.3.8

any → 102.45.09.5

class : A

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

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

ⓘ Network address : 102.0.0.0

ⓘⓘ Host address : 0.45.09.5

ⓘⓘⓘ No of networks : $2^{N-\text{class add}} = 2^8$ but first bit for class address reserve
so $2^{8-1} = 2^7 = 128$

ⓘⓥ No of hosts : $(2^{\text{no of hosts}} - 2) = (2^{3H} - 2) = (2^{3\times8} - 2) = (2^{24} - 2) = (2^{24} - 2) = 16777$

ⓥ 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

(ii) host address : 0.0.0.8

Class address → 110

(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 : $(2^h - 2) = 2^8 - 2 = 256 - 2 = 254$

* 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.

(97). 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 → n where n no of borrow bit

$2^6 = 64$

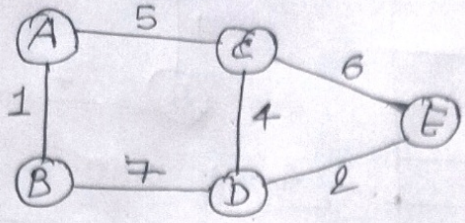
(2) No of ip address : 2^n = where n no of remaining bit

$2^2 = 4$

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

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

ans ⇒ 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

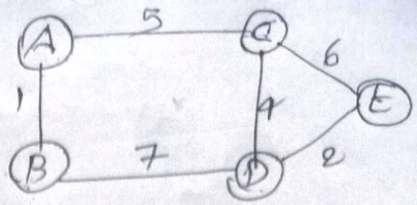
$$d_x(y) = \min_v \{c(x,v) + d_v(y)\}$$

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 + 7

A→C→E→D→B = 20
5 6 2 7

for (B)

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

A→C A→C = 5 ✓

A→B→D→C = 12
1 7 4

A→B→D→E→C = 16
1 7 2 6

for (C)

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

A→D A→C→D = 11
5 4

A→B→D = 8 ✓
1 7

A→C→E→D = 13
5 6 2

for (D)

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

A→E A→C→E = 11
5 6

A→B→D→E = 10 ✓
1 7 2

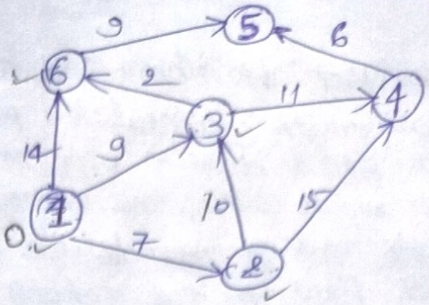
A→C→D→E = 11
5 4 2

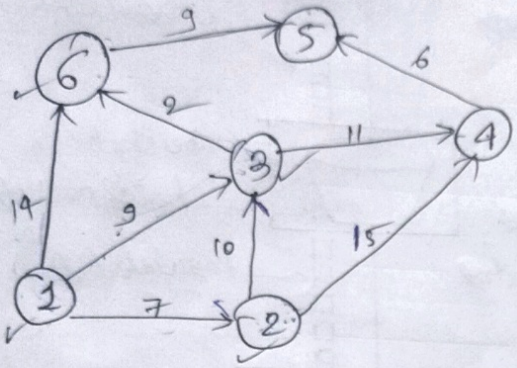
for (E)

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

and same process for each node

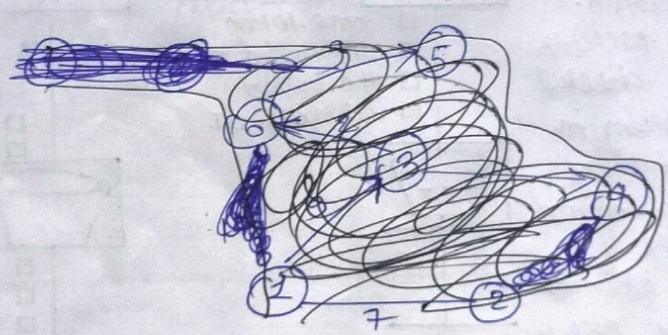
Prob Find shortest path from node 1 to all other nodes using Dijkstra's algorithm.

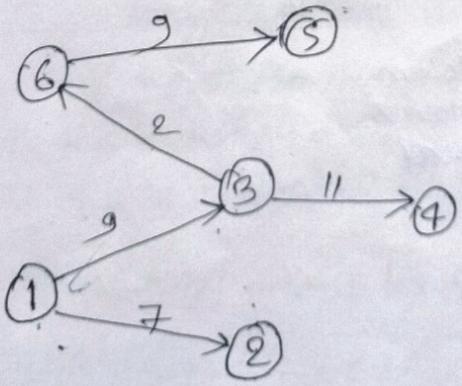




Source	Destination				
1	2	3	4	5	6
	∞	∞	∞	∞	∞
1,2	(7)	9	∞	∞	14
1,2,3	(7)	(9)	22	∞	14
1,2,3,6	(7)	(9)	20	∞	(11)
1,2,3,6,4	(7)	(9)	(20)	20	(11)
1,2,3,6,4,5	(7)	(9)	(20)	(20)	(11)

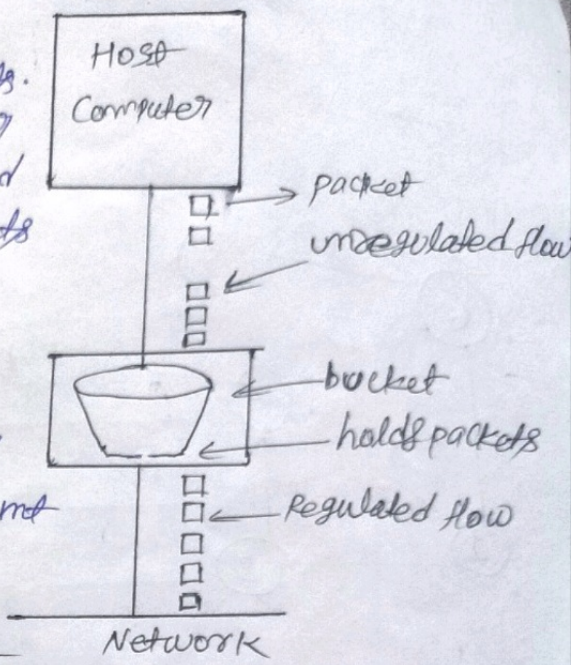
Shortest path is:





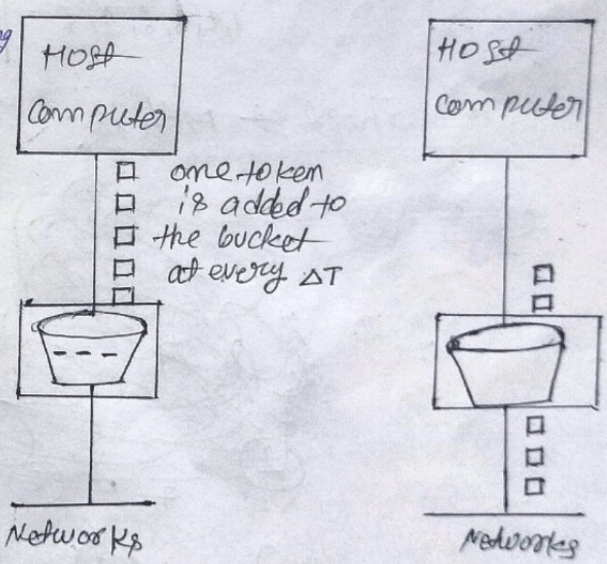
Q49) write short note on (a) Leaky bucket algorithm
(b) Token bucket algorithm

(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 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 halded and again when enough token will be there then tokens are added to the bucket at every ΔT time.



(Q5) Compare and contrast IPV4 and IPV6.

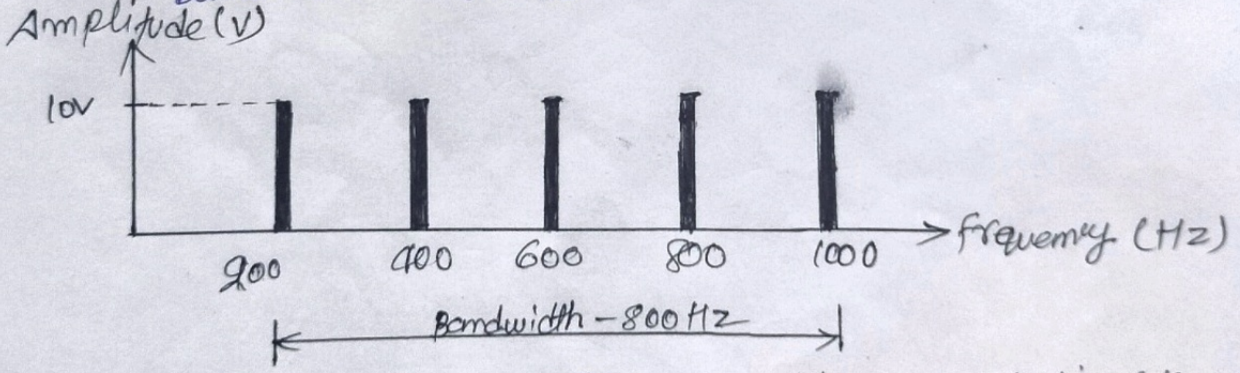
IPV4	IPV6
(i) Address size of IPV4 is 32 bits	Address size of IPV6 is 128 bits.
(ii) Address formate of IPV4 is dotted decimal	Address formate of IPV6 is Hexadecimal.
(iii) Header size of IPV4 is 20 - 60 bytes.	Header size of IPV6 is 40 bytes.
(iv) IPV4 is widely supported by all devices.	IPV6 is not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

(Q6) 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 $\frac{1}{6} \times 360 = 60$ $= \frac{60 \times \pi}{180} = \frac{\pi}{3}$

(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