Date.....

Computer Networks (BCS603)

Unit-1 :- Introductory Concepts :- Goals and applications of Networks, Categories of networks, Organization of the Internet, ISP, Network analysis structure and architecture (layering principles, services, protocols and standards), The OSI refrence model, TCP/IP protocal suite, Network devices and components.

Physical Layer :- Network topology design, Types of ~~Correction, flow control (Elementary Data link, Protocols, Sliding Window protocols).~~
Connections, Transmission media, Signal transmission and encoding, Network performance and transmission impairments, switching techniques and multiplexing.

Unit-2 :- **Link Layer :-** Framing, Error Detection and Correction, flow control (Elementary Data Link Protocols, Sliding Window protocols).

Medium Access Control and Local Area Networks : Channel allocation, Multiple access protocols, LAN stardards, Link layer switches & bridges (learning bridge and spanning tree algorithms).

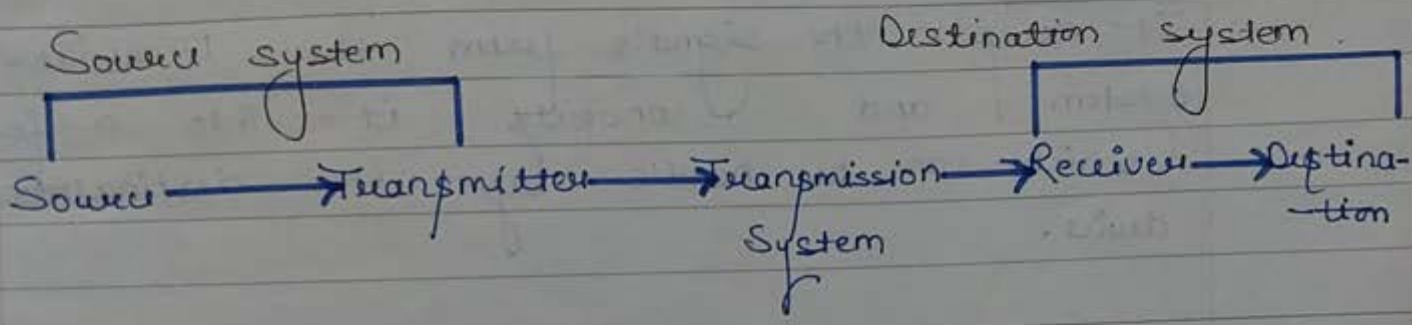
Date.....

Unit-3 :- Network Layer :- Point-to-point networks, Logical addressing, Basic internetworking CIP, CIDR, ARP, RARP, DHCP, ICMP), Routing, forwarding and delivery, Static and dynamic routing, Routing algorithms and protocols, Congestion ~~and~~ control algorithm, IPV6.

Unit-4 :- Transport Layer :- Process-to-Process delivery, Transport layer protocols (UDP and TCP), Multiplexing, Connection management, Flow control and retransmission, ~~Data compression~~, ~~Cryptography - basic concepts~~. Window management, TCP Congestion Control, Quality of service.

Unit-5 :- Domain Name System, World Wide Web and Hyper Test Transfer Protocol, Electronic mail, File Transfer Protocol, Remote Login, Network management, Data Compression Cryptography - basic concepts.

Basic Communication Model :-



Introduction.

A network is a set of devices often referred to as nodes, a node can be a computer, printer or any other devices compatible of sending and receiving all data.

Source.

Having data to be transmitted.

Transmitter

Data is not directly transmitted in the form they are generated, it is transferred and encoded the information in such a manner to produce electromagnetic signals these are transmitted across some part of transmission system.

Transmission system
It can be a single transmission line or a complex network connecting source & destinations.

Receiver.
It accepts the signals from the Transmission system and converts it into a form which can be handle by the destination devic.

Distination.
It takes incoming data from the receiver.

The old communication model in which a single computer used to safe all the computational requirements of an oreganisation has bun replaced by a new one in which a large numbers of separate but interconnected computers perform the job. Such system are called computer networks.

Computer Networks Criteria.

Network is a communication system which supports many users a. network must be able to most contain criteria :-

1) Performance:
We can measure it in terms of transmit & response time.

* Transit time.
It is the amount of time required for a message to travel from one device to the other.

* Response time
It is the time elapsed b/w transmitter & response

Other factors deciding the performance are as follows:-

Number of users, capability of connected network, Types of transmission & efficiency of software.

ii) Reliability
It decides the frequency at which network failure take place.

iii) Security.
It refers to the protection of data from the unauthorized users access.

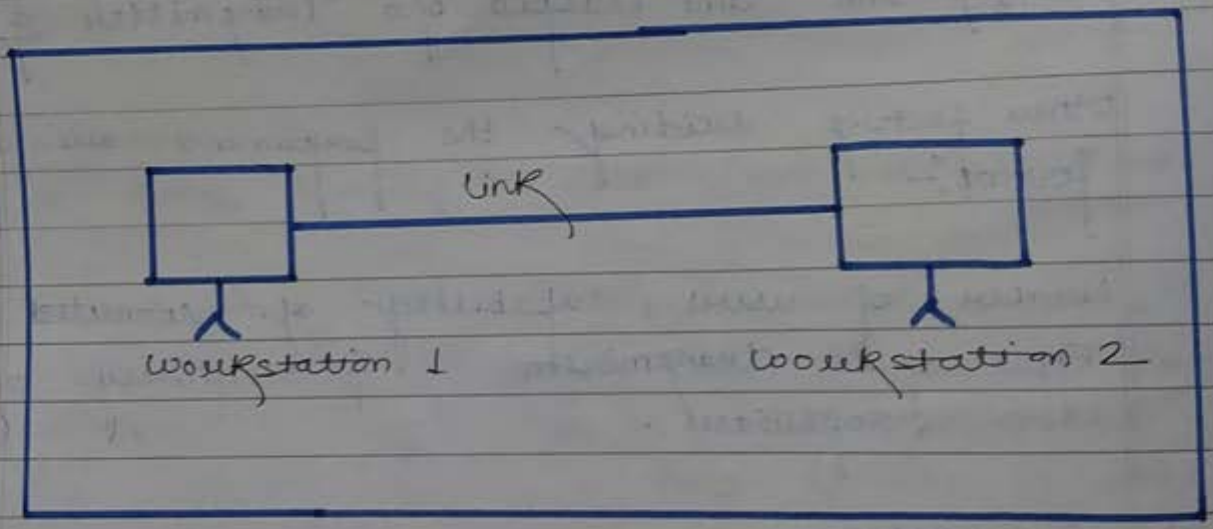
Types of connections

A network is two or more devices connected to each other through connecting links.

There are two possible ways to connect the devices they are as under.

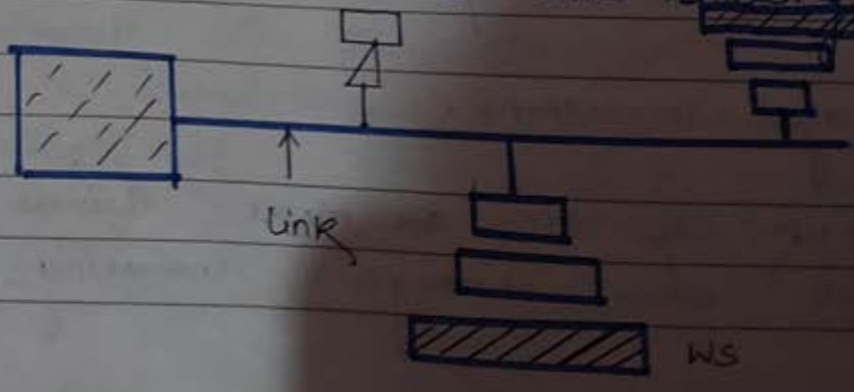
* Point to point connection

It provides a dedicated link b/w two devices entire capacity of the link is reserved for transmission between two devices.



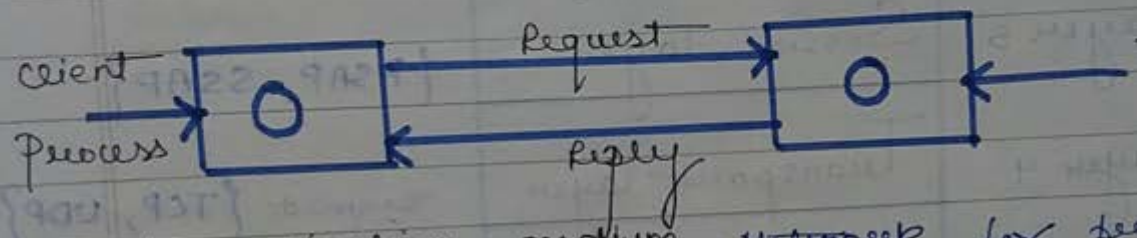
* Multi point connection.

It is also called a multidrop connection. The multipoint connection the capacity is shared but it share it turn by turn then it is time sharing network



Goals & applications of computer network :-

Services provided by the network for companies resource sharing, providing high reliability, save money, provide a powerful communication medium, provides high reliability by having alternative sources of data for example - All files could be replicated on more than one devices so that if it is unavailable due to hardware failure the other copies can be used.

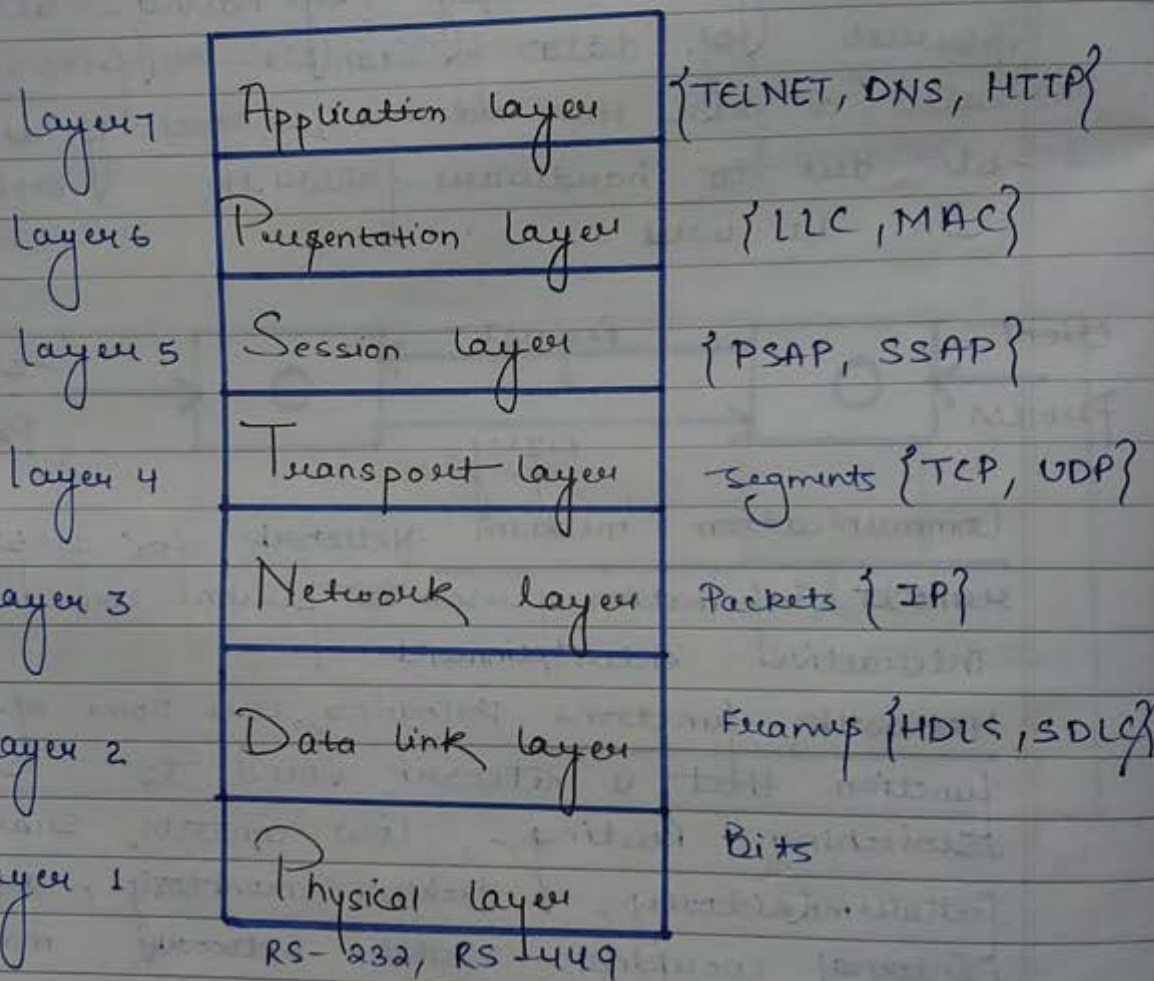


Network for people, access to remote information person to person communication interactive entertainment

Network functions Following are some of the input function that a network need to perform!
Switching, Routing, flow control, security, Backup, failure monitoring, traffic monitory, accounting, Internal working and network management.
Network structure and architecture

* Protocol Hierarchies (Layer architecture) To reduce the design complexity network are organized as a series of layer or the no. of layers, the name of each layer, contents of each layer & function of each layer differs from network. Layer N on one machine (source) carries on a conversation with layer N on another machine (destination)

OSI Model



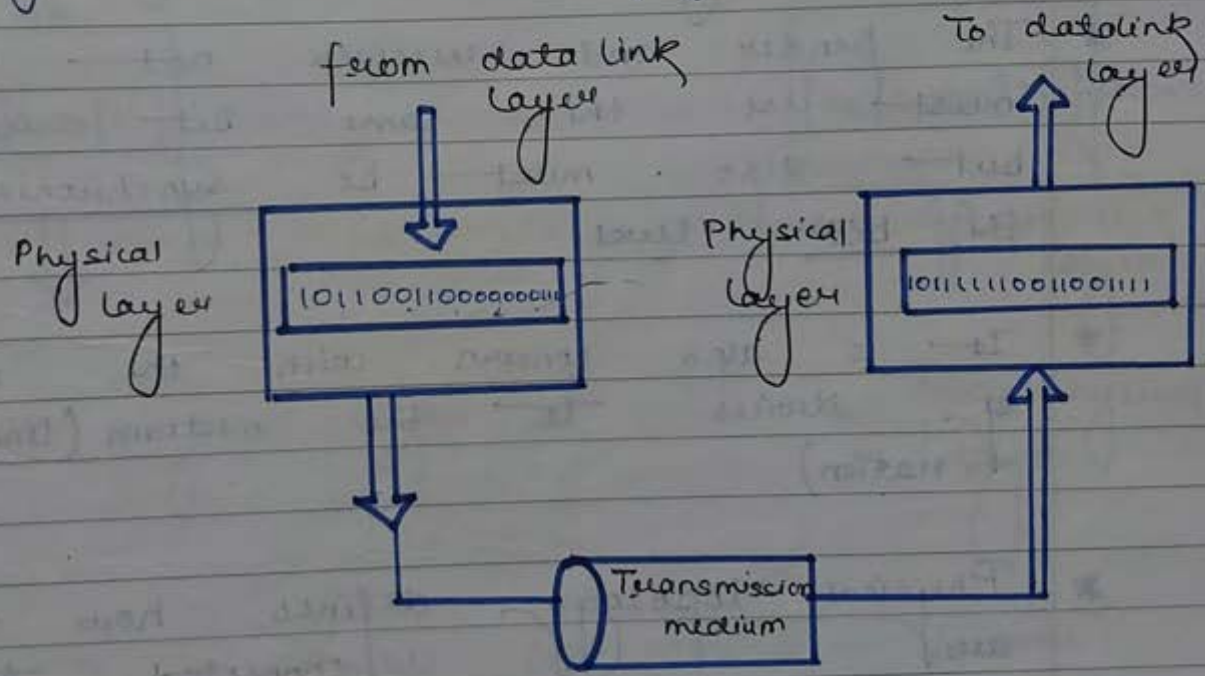
7 Layers of OSI model.

This model is a layer framework for the design of network system that allows communication b/w all types of computer system.

It consist of several separate but related layers. Each of which defines a part of the process of moving of information accross a network.

Physical Layer.

It coordinates the function require to carry a big stream over a physical medium.



* It is responsible for movement of individual bit from one node to another.

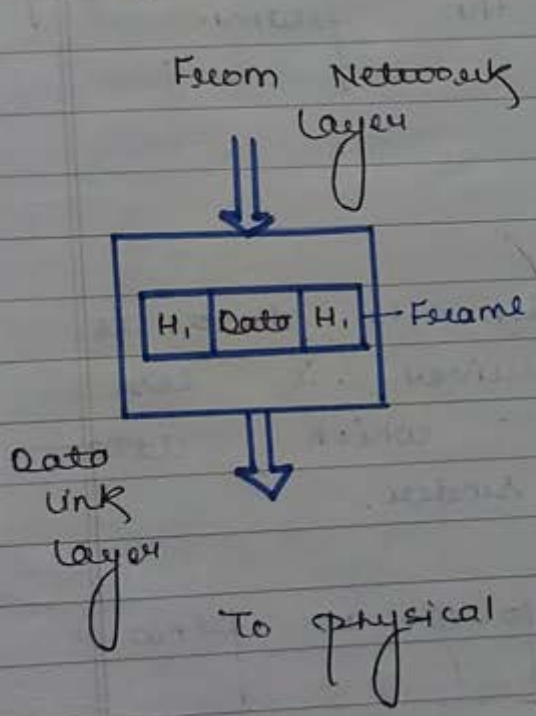
* Physical characteristics of interfaces & medium.

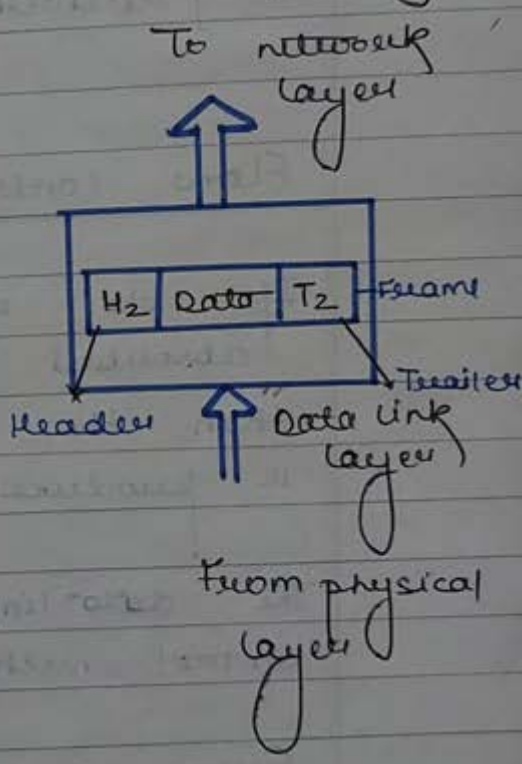
It also defines the types of transmission medium

* It defines the type of encoding of bits (how zero's & one's are change into signals)
* The transmission rate (no. of bits send each second) is also defined by the physical layer.
* The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level.
* It is also concern with the connection of devices to the medium (line configuration)
* Physical topology defines how devices are connected to make the network.
* Transmission mode is also define by physical layer.

Data link layer.

It transforms the physical layer, a raw transmission facility to a reliable link. It makes the physical layer link appear error free to the upper layer (network layer)





* It is responsible for moving frames from one node to the next.

Framing

It divides the stream of bits into manageable data units called frames.

Physical addressing

If frames are to be distributed to the different systems on the network then the data link layer adds a header to the frame to define the sender & receiver of the frame.

Flow control

If the rate at which the data is absorbed by the receiver is less than the rate at which data is produced by the sender.

The data link layer imposes a flow control mechanisms.

Error control

It adds reliability to the physical layer by adding mechanism to detect & retransmit, damage or loss frames.

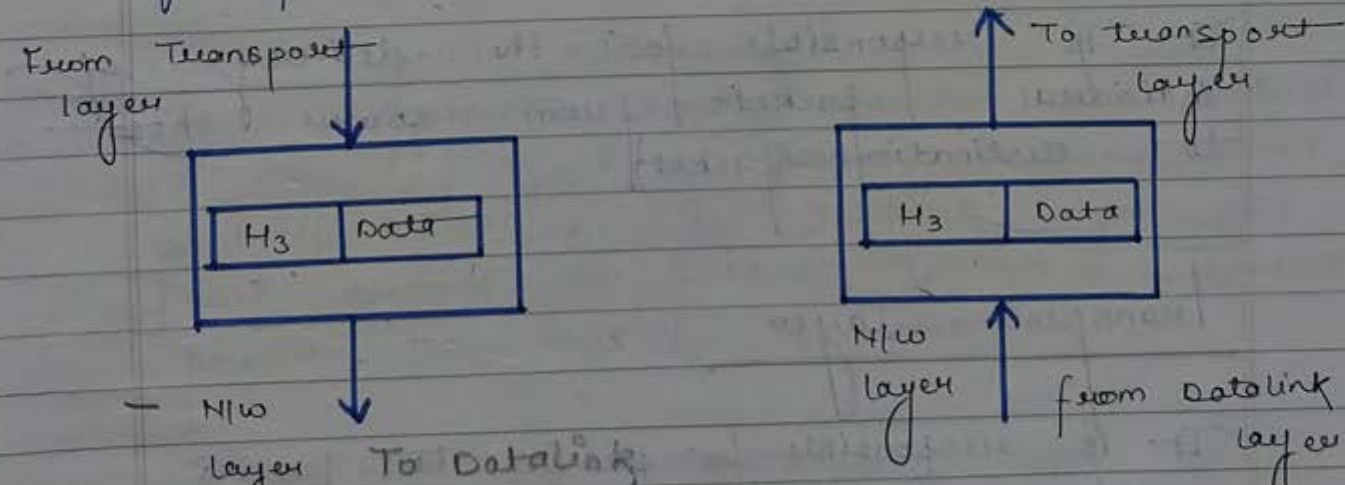
It also uses a mechanism to recognize duplicate frames.

Error control is normally achieved through a trailer added to the end of the frame.

Access control when two or more devices are connected to the same link, the data link layer protocol is necessary to determine which device has control over the link at any given time.

Network layer

It is responsible for source to destination delivery of a packet possibly across multiple networks



Functions / Responsibilities of Network layer

Logical addressing

The physical addressing is implemented

by the data link layer if a packet passes the network boundary we need another addressing system to help to distinguish the source & destination system.

Routing

When independent networks or links are connected to create internetworks (network of networks) or a large network the connecting devices are called routers or switches.

(Route or switch) the packets to their final destination)

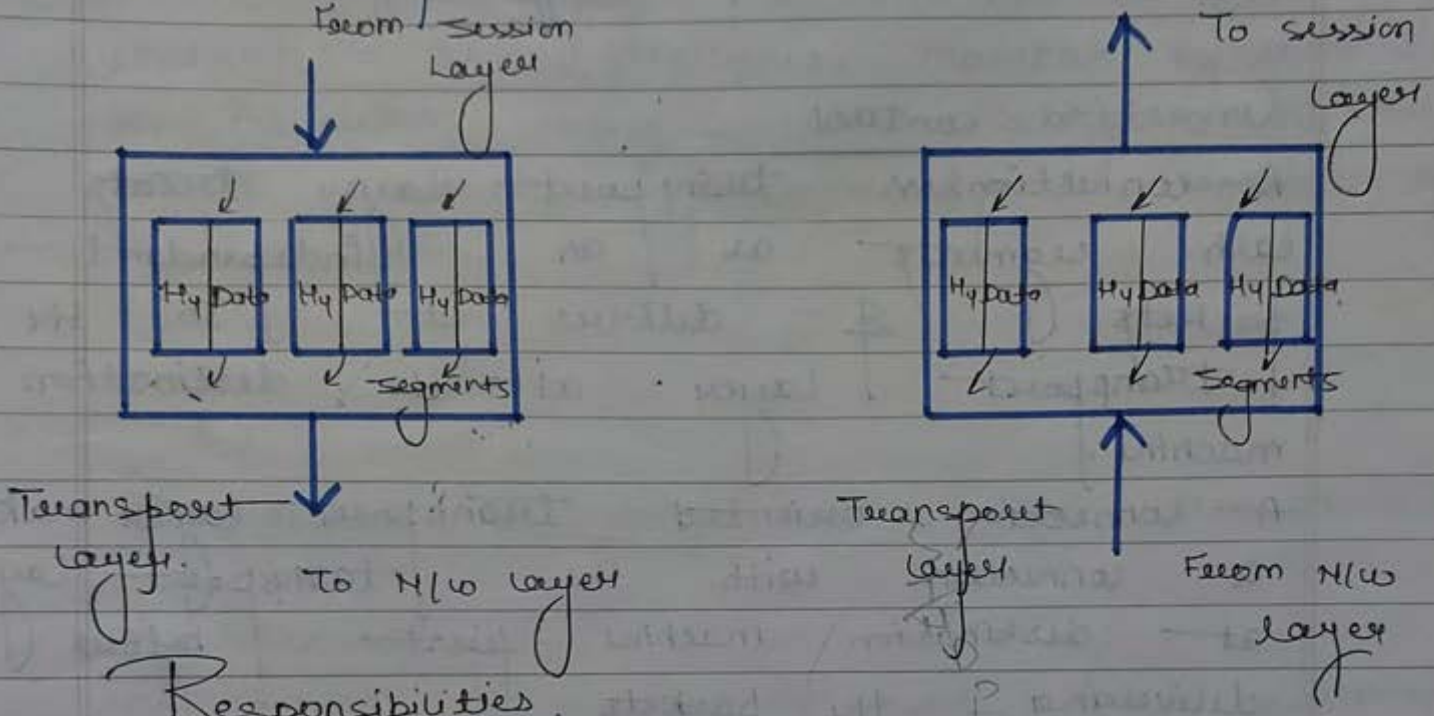
It is responsible for the delivery of individual packets from source host to destination host (packet).

Transport layer

It is responsible for process to process delivery of the entire message.

A process is an application program running on a host, whereas the n/w layer oversees source to

destination delivery of individual packets. It does not recognize any relationship b/w those packets.



Responsibilities.

Service point addressing

The transport layer header must include a type of address called service point address. The network layer gets each packet to the correct process on that computer.

Segmentation & reassembly

A message is divided into transmitable segments, with a segment containing a sequence number which helps the transport layer reassemble

the message correctly upon arriving at the destination point & to identify & replace packets that were lost in transmission

Connection control

A connectionless transport layer treats each segments as an independent packets & delivers it to the transport layer at the destination machine.

A connection oriented transport layer makes a connection with the transport layer at destination machine first before delivering the packets

Flow control

It is also responsible for flow control however flow control at this layer is perform end to end rather than across single link.

Error control

It is also responsible for error control however error control at this layer error control is perform process to process across a single. Error control is usually achieved through retransmission

Session layer

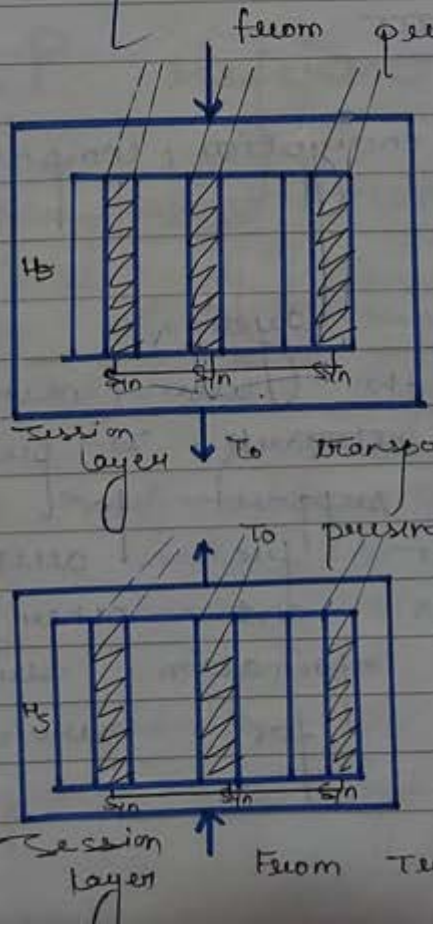
The services provided by the first three layers are not sufficient for some processes. the session layer is the network dialogue controller. It establishes, maintain synchronizes the interaction among communicating system. It is responsible for dialogue controller & synchronization.

Dialogue control

It allows the communication b/w two process

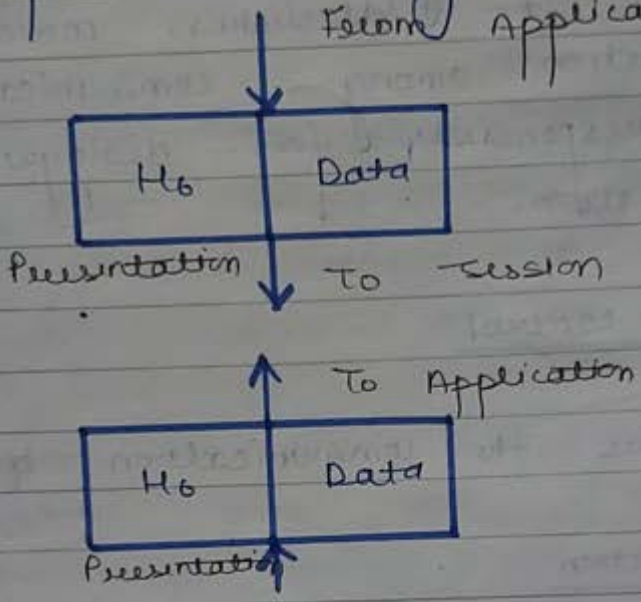
Synchronization

It allows the process to add check point or synchronization point to a stream of data.



Presentation Layer.

It is concern with the syntax & semantics of the information exchange b/w two systems.



Responsibilities

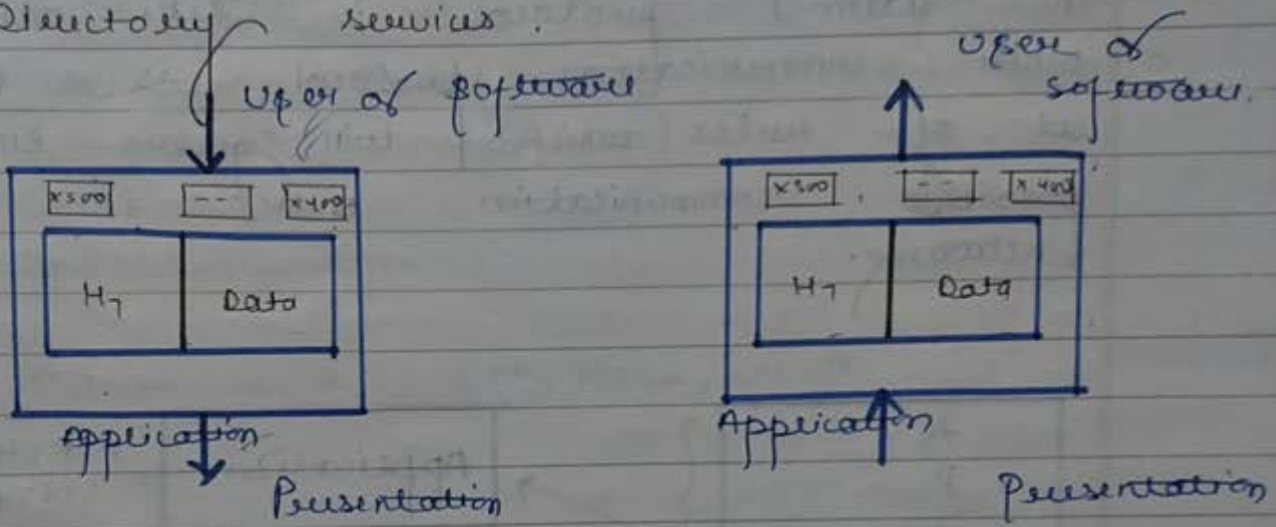
Translation, encryption, compression

Application Layer.

It enables the user (whether human or software) to access the network. It provides user interface & support for services such as email, remote file access and transfer, shared DBMS and other types of distributed information services. It is responsible for services to the user.

Specific services provided by this layer —

Network virtual terminal
File transfer, access and management
Mail services
Directory services.



TCP/IP reference model

It was originally developed by the department of defence project research agency (arpa later DARPA) to connect military networks together

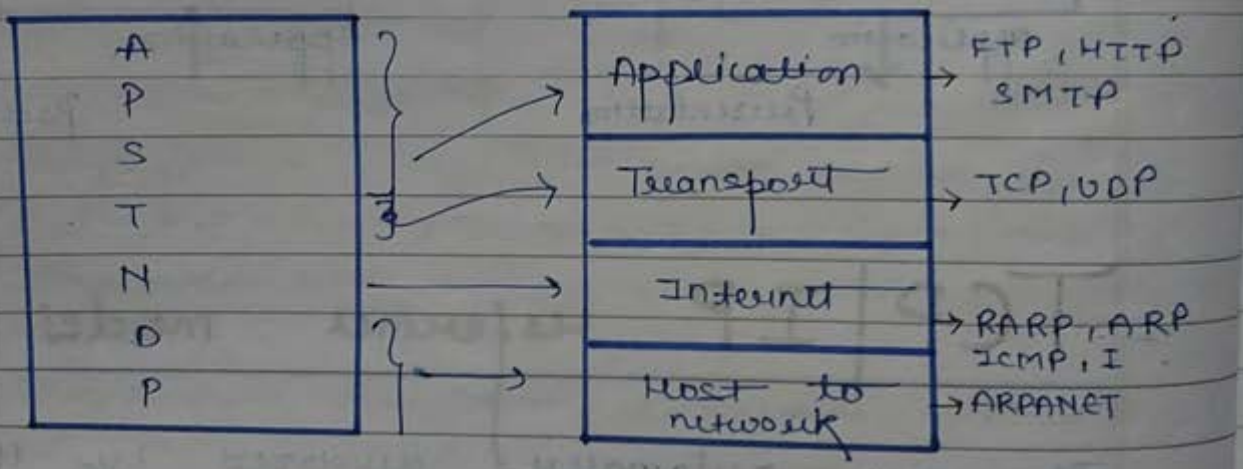
It was used by ARPANET and then it is being used in the internet

Transmission control protocol

It became standards for interoperating unix computer, specially in military

& university environment. These protocols describe the movement of data b/w the host computers on Internet.

The internet protocol is like any other communication protocol is a set of rules which will govern every possible communication over the network.



Switching Methods

Host to network

Host has to connect to network using some protocol so that it can send IP packet over it.

Internet layer.

Main task is to allow host to inject packets into any n/w & then make them

modes of communication flow {Simplex, Half Duplex, Full Duplex}

travel Independently.

Transport layer

This allows the peer entities of the source & destination machine to converse with each other. Protocols used are TCP (connection oriented and reliable) & UDP {unreliable connectionless}

Application layer

Protocol used FTP, HTTP, SMTP

Switching methods.

It defines how data connections are made & movements are handled in WAN

1. Circuit switching

The telephone network provides telephone service with two way real time transmission of electrical current and voice signals to flow b/w two users. The end to end connection is maintained for the duration of call. The transfer mode of a network that involves setting up a dedicated end to end connection called circuit switching. In circuit switching the sending PC establishes a link with a

→ Reduces traffic network congestion.
→ Provide asynchronous communication.
→ Network device share data channels.

receiving PC after the data flow stops the link is released.

Provide guaranteed data rate.

There is no delay in data flow because of the dedicated path.

2. Message switching.

In telegraphy, the text message is encoded using the morse code into sequences of dots and dashes. In telegraph networks, the text message is transmitted from source to the telegraph switching station. Then the operator takes the decision of routing the message.

In message switching, a dedicated path b/w two communicating devices is not established. Each intermediate device receives the message, stores it, until the next device is ready to receive it and then forwards it to the next device.

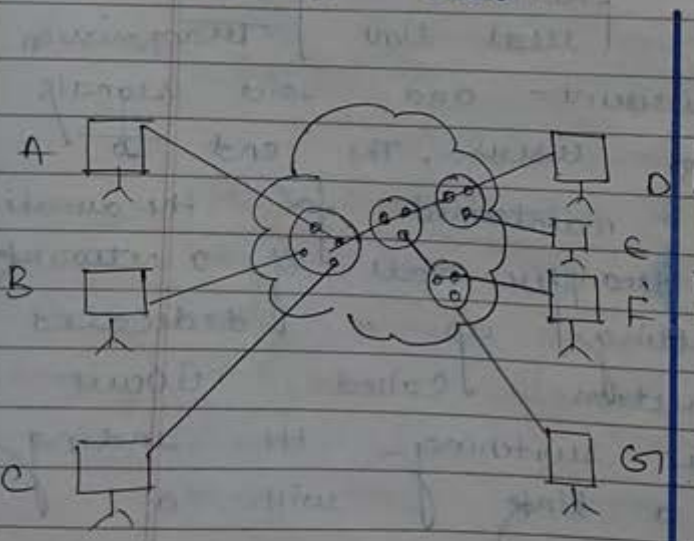


Fig: Circuit Switching network

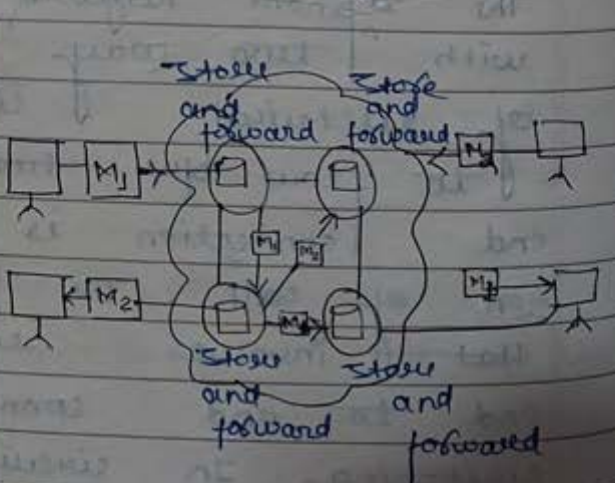


Fig: Message Switching network

ASSIGNMENT-1

Ques. Short note on LAN, MAN, WAN

Ans LAN

It stands for (local area network).

A local area network is a group of computers and associated devices that share a common communications line or wireless link to a server.

Typically, a LAN encompasses computers and peripherals connected to a server within a distinct geographic area such as an office or a commercial establishment.

MAN

It stands for metropolitan area network.

A metropolitan area network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN).

WAN

It stands for wide area network.

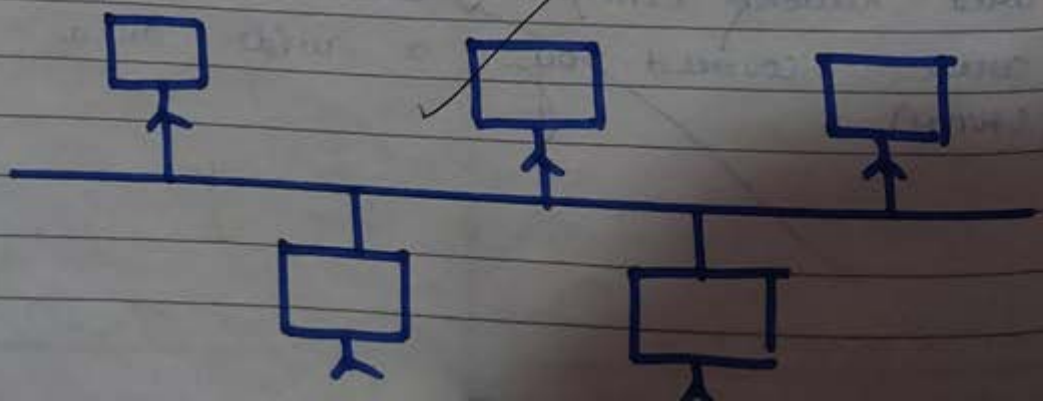
A wide area network (WAN) is a telecommunications network or computer network that extends over a large geographical distance / place. Wide area networks are often established with leased telecommunication circuits.

Ques 2. What are different network topologies explain each with proper diagram.

Ans. Network topology is the schematic description of a network arrangement, connecting various nodes (sender and receiver) through lines of connection.

* Bus Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called Linear Bus topology.



Features of bus topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable.

Advantages of Bus topology

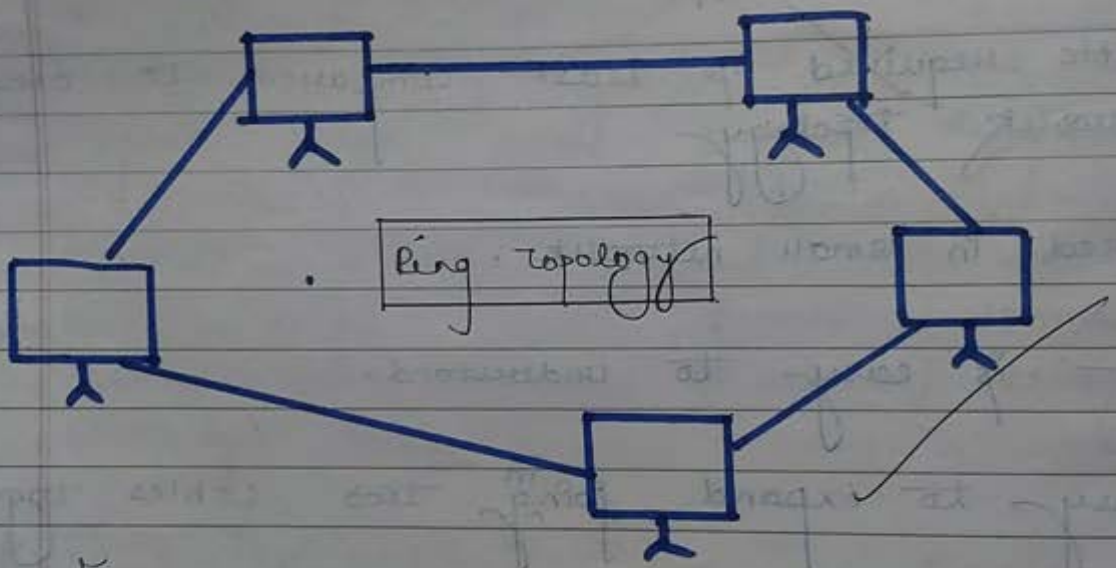
1. It is cost effective.
2. Cable required is least compared to other network topology
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

Disadvantages of Bus Topology

1. Cable fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of network decreases.
3. Cable has a limited length
4. It is slower than the ring topology

* Ring Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.



Features of Ring topology

Data is transferred in a sequential manner that is bit by bit. Data, transmitted, has to pass through each node of the network, till the destination node.

Advantages of ring topology

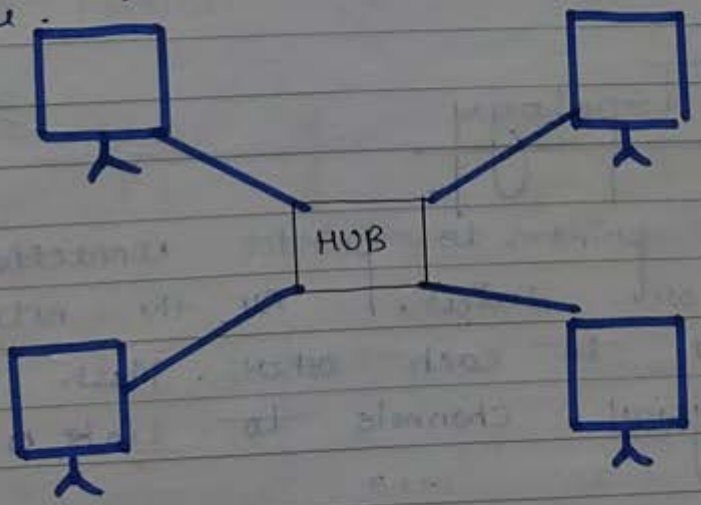
1. Cheap to install and expand

Disadvantages of ring topology.

1. Adding or deleting the computers disturbs the network activity
2. Failure of one computer disturbs the whole network

* Star Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



Features of Star Topology

Every node has its own dedicated connection to the hub.

Advantages of Star topology

1. Hub can be upgraded easily.
2. Fast performance with few nodes and low network traffic.

Disadvantages of Star Topology

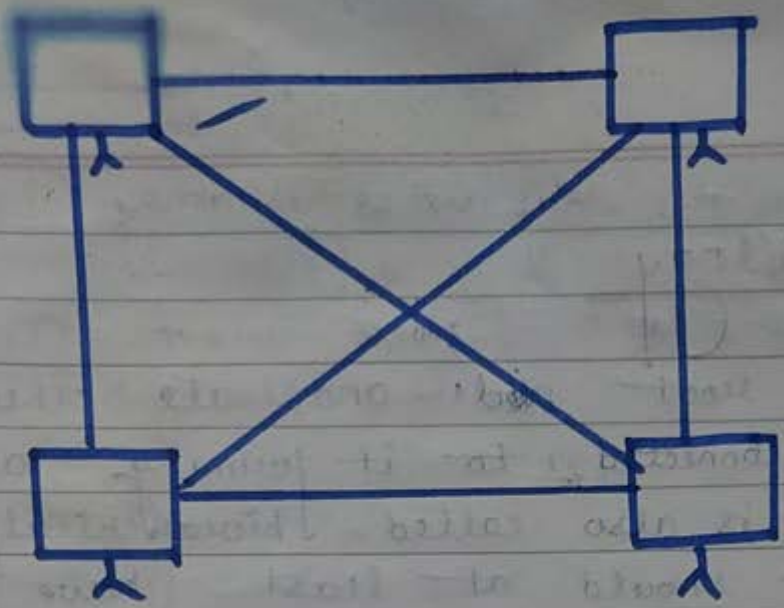
1. Expensive to use.
2. Cost of installation is high.

* Mesh Topology

It is a point-to-point connection to other nodes or devices. All the network are connected to each other. Mesh has $n(n-1)/2$ physical channels to link n devices

There are two techniques to transmit data over the Mesh topology, they are.

1. Routing
2. Flooding



Features of Mesh topology

1. Fully connected
2. Robust
3. Not Flexible.

Advantages of Mesh Topology:

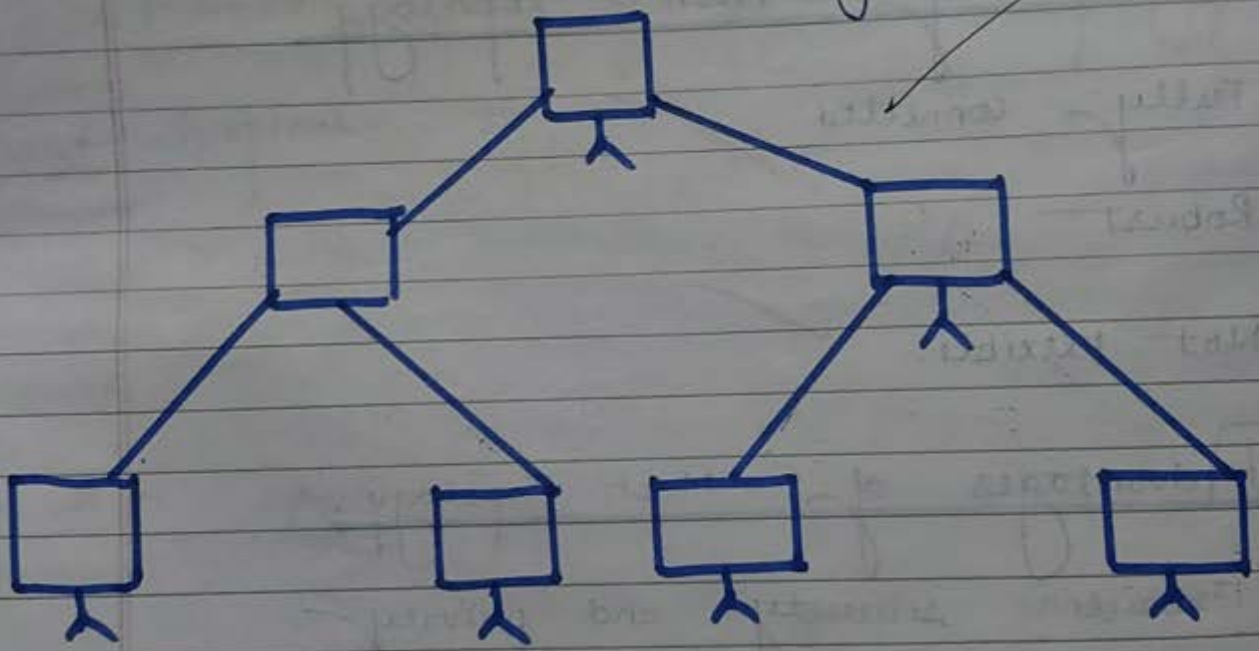
1. Provide security and privacy
2. It is robust

Disadvantages of Mesh Topology

1. Bulk wiring is required.
2. Cabling cost is more.

* Tree topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.



Features of Tree Topology

Used in wide area network.

Advantages of Tree Topology.

1. Error detection is easily done.
2. Easily managed and maintained.

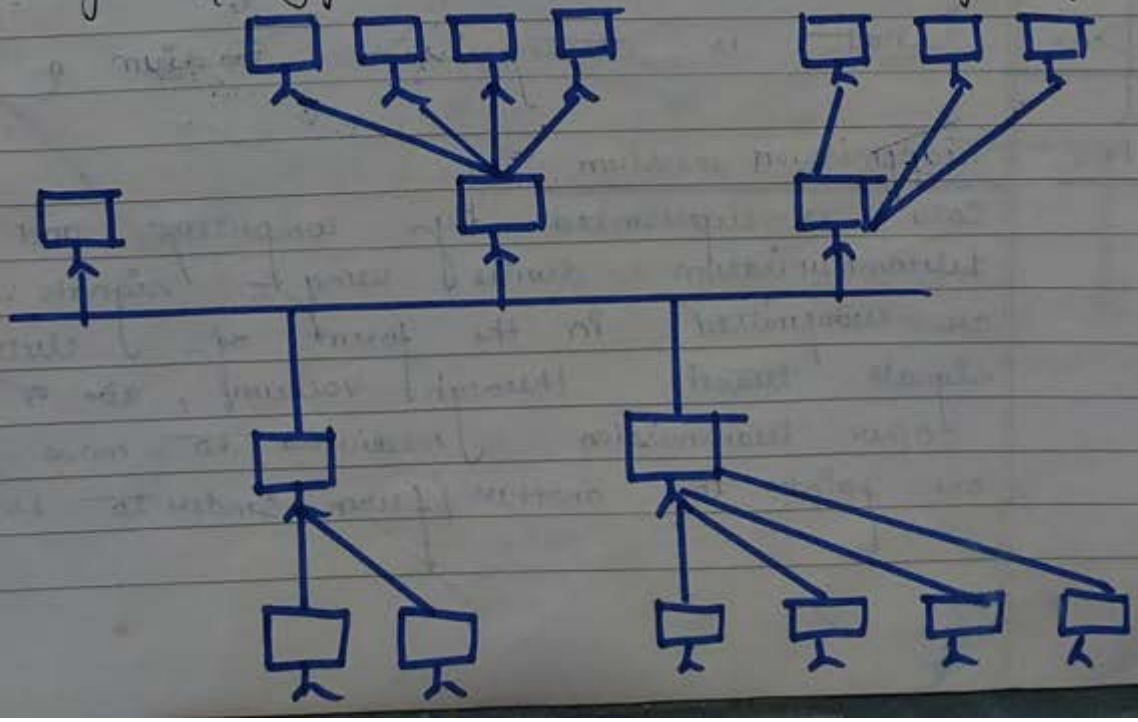
Disadvantages of tree topology.

1. If more nodes are added maintenance is difficult
2. Costly.

* Hybrid topology

It is of two different types of topologies which is a mixture of two or more topologies.

For example if in an office in one department ring topology is used in another star topology is used, connecting these topologies will result in Hybrid Topology {ring topology and star topology}



Features of Hybrid Topology

1. It is combination of two or more topologies.

Advantages of Hybrid Topology

1. Effective
2. Flexible

Disadvantages of Hybrid Topology

1. Complex in design.
2. Costly.

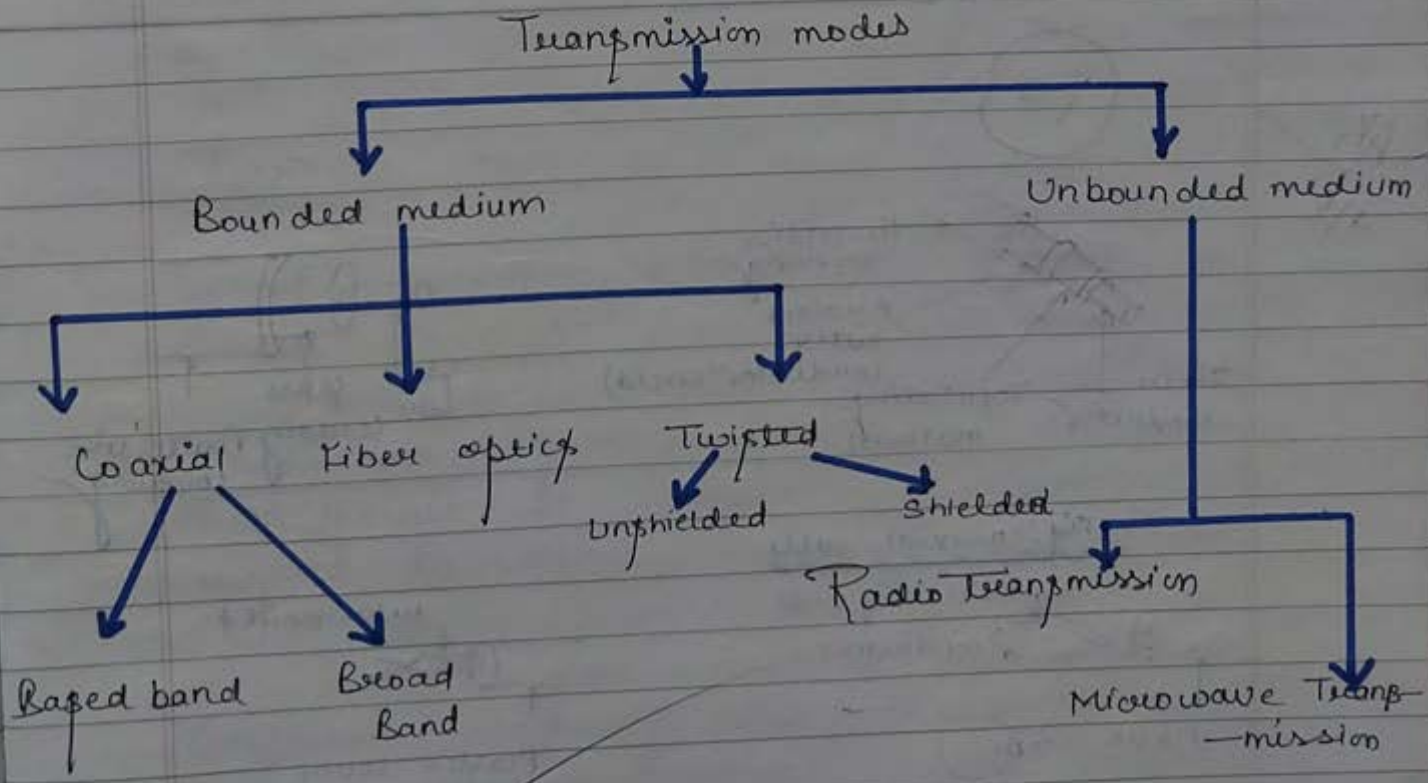
Ques 3. What is transmission medium ?

Ans. **Transmission medium**

Data is represented by computers and other telecommunication devices using signals. Signals are transmitted in the form of electromagnetic signals travel through vacuum, air or other transmission mediums to move from one point to another (from sender to receiver)

Electromagnetic energy (includes electrical and magnetic fields) consists of power, voice, visible light, radio waves, ultraviolet light, gamma rays etc.

Transmission medium is the means through which we send our data from one place to another. The first layer (physical layer) of communication Networks OSI Level layer model is dedicated to the transmi-ssion media.



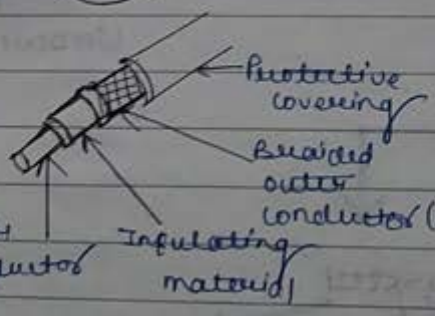
Factors to be considered while selecting a Transmission Medium.

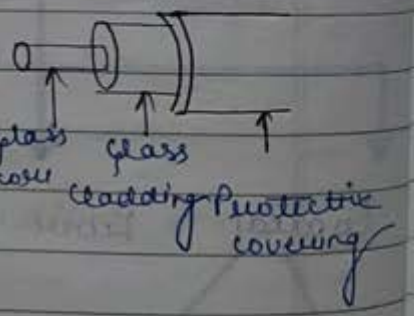
1. Transmission Rate.
2. Cost and Ease of installation.
3. Resistance to Environmental conditions.
4. Distances.

V. good

10

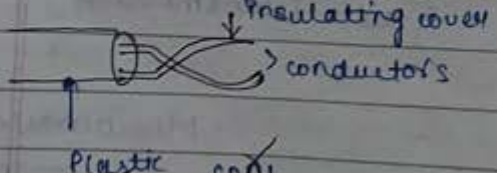
AK
+12

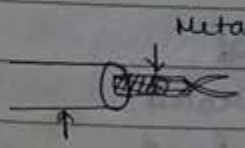




b)

Fig: Co-axial cable.

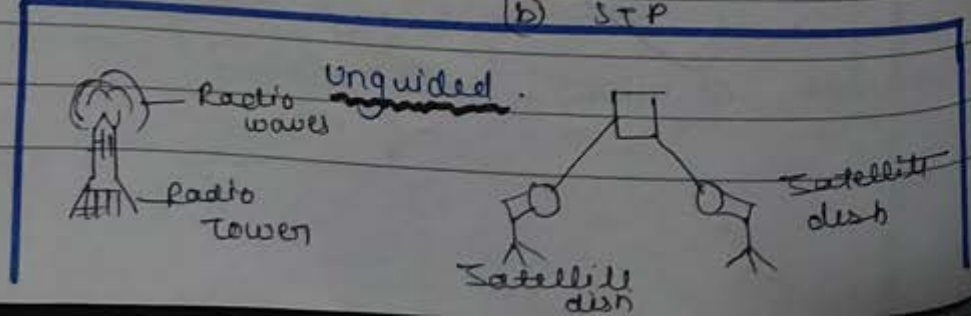




(a) UTP

(b) STP

Unguided.



3. Packet Switching

It is a method of grouping data which is transmitted over a digital network into packets which are made of header and trailer.

A message is divided into a stream of packets and is addressed independently. It establishes a logical connection b/w sending and receiving devices.

Types of packet switching

a) **Virtual circuit packet switching**

A single route is choosen b/w the sender & receiver and all the packets are send through this route.

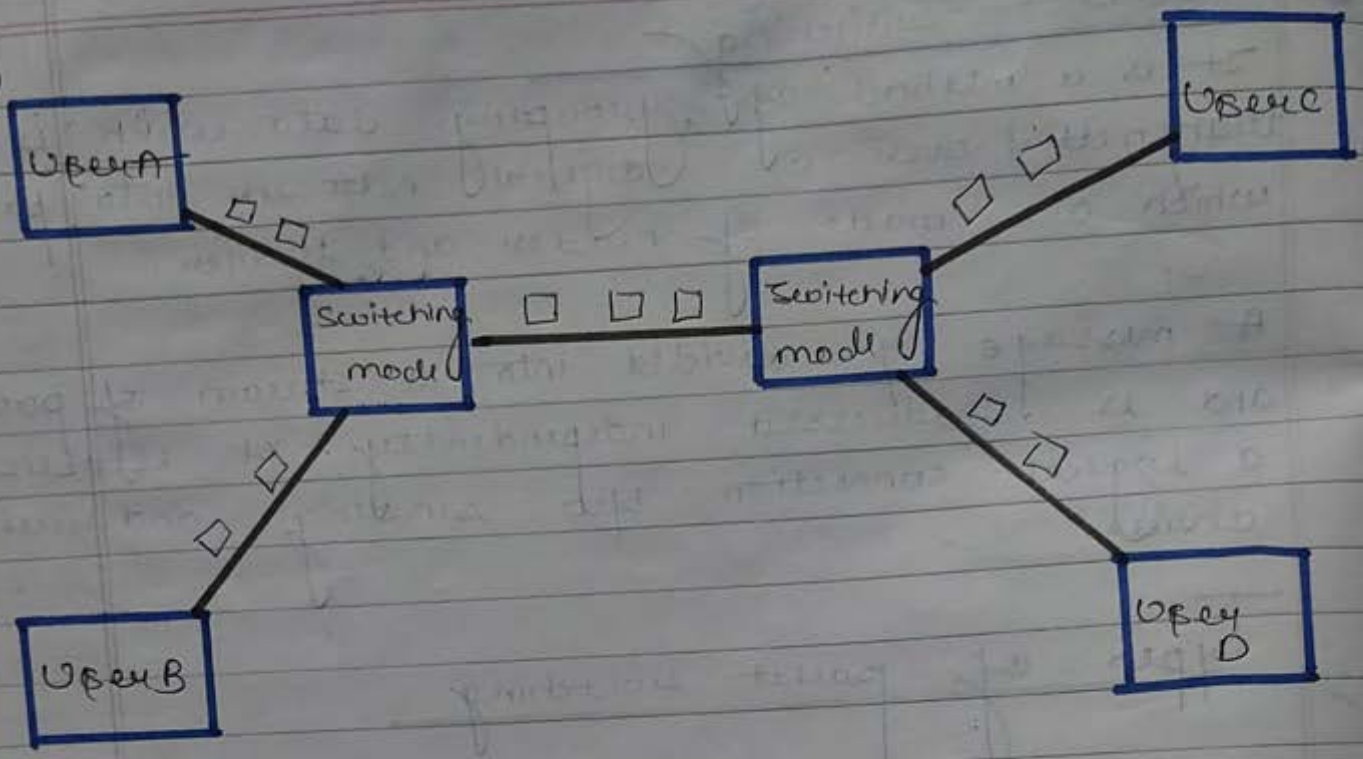
Every packet contains a virtual circuit number.

b) **Datagram packet switching**

Each packet is transmitted without any regard to other packets, Every packet contain.

Datagram switching done at network layer the source & destination address are used by routers to decide the routes for the packets.

c)



INTEGRATED SERVICES DIGITAL NETWORK {ISDN}

DSL (latest tech) Skywire

ISDN is an all digital communication line that allows for the transmission of voice, data, video & graphics at very high speed over standard communication lines. It provides a single common interface with which to access digital communication services that are required by varying devices by ~~transparent~~ to the remaining user

1000 m long coil & amplify signal

Problem in digital communication

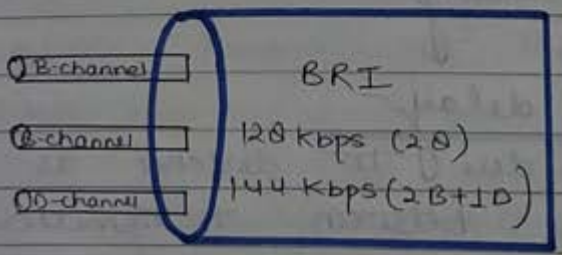
It is not restricted to public telephone network it may be transmitted via packet switched n/w.

It is circuit switched telephone n/w which also provide access to packet switched n/w design to allow digital transmission of voice & data over ordinary telephone copper wire.

It was created as a communication standard for transmission of digital data, video facts etc. along with voice signal over circuit switches (PSTN) Public switch telephone network.

TYPES OF ISDN

BRI {Basic rate interface} B channel
It consist of two 64 kbps, and one D channel for transmiting control information.

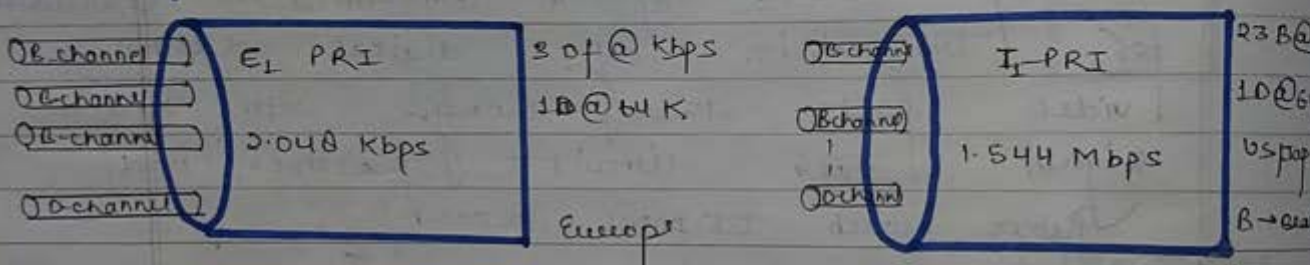


Data/voice
↑
B- Bearer
D- Delta and operates at 16 kbps

PRI {Primary rate interface}

It consist of 23 B channels and 1 D channel (US) or 30 B channels and 1 D channel (Europe).

BRI gives a total usable bandwidth of 128 Kbps whereas PRI gives a bandwidth of 144 Mbps.



Delay

In network terminology delay refers to total time consumed during message transferring from sender to receiver.

Types of Delay

Propagation delay

It occurs due to distance as it depends upon distance between transmitter and receiver and velocity of signal.

$$T_p = \frac{d}{V}$$

It cannot be reduced.

Transmission delay

Time taken by frame to come out from transmitter. It can be reduced by increasing the data rate of the line also by limiting the size of frame.

$$T_t = \frac{l}{v}$$

l → frame size
v → data rate

Node delay or Processing delay

Time taken at each node. It can be reduced by more dedicated paths i.e., in circuit switching. Call setup time increase here.

T_n = time consume at each node for processing

Delay = considerating in topological design

Backbone design

A network containing a high capacity connectivity infrastructure that forms the main link or backbone through to the different parts of the network.

Network consist of various LAN's WAN's and sub networks.

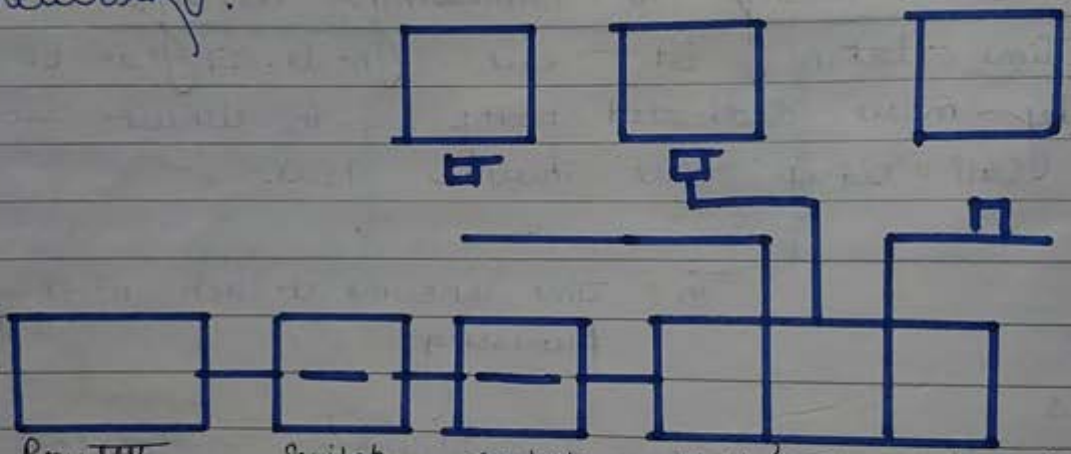
It normally consist of cableing, switches

bridges, routers and gateways in varying segment

Types of backbone design

Serial

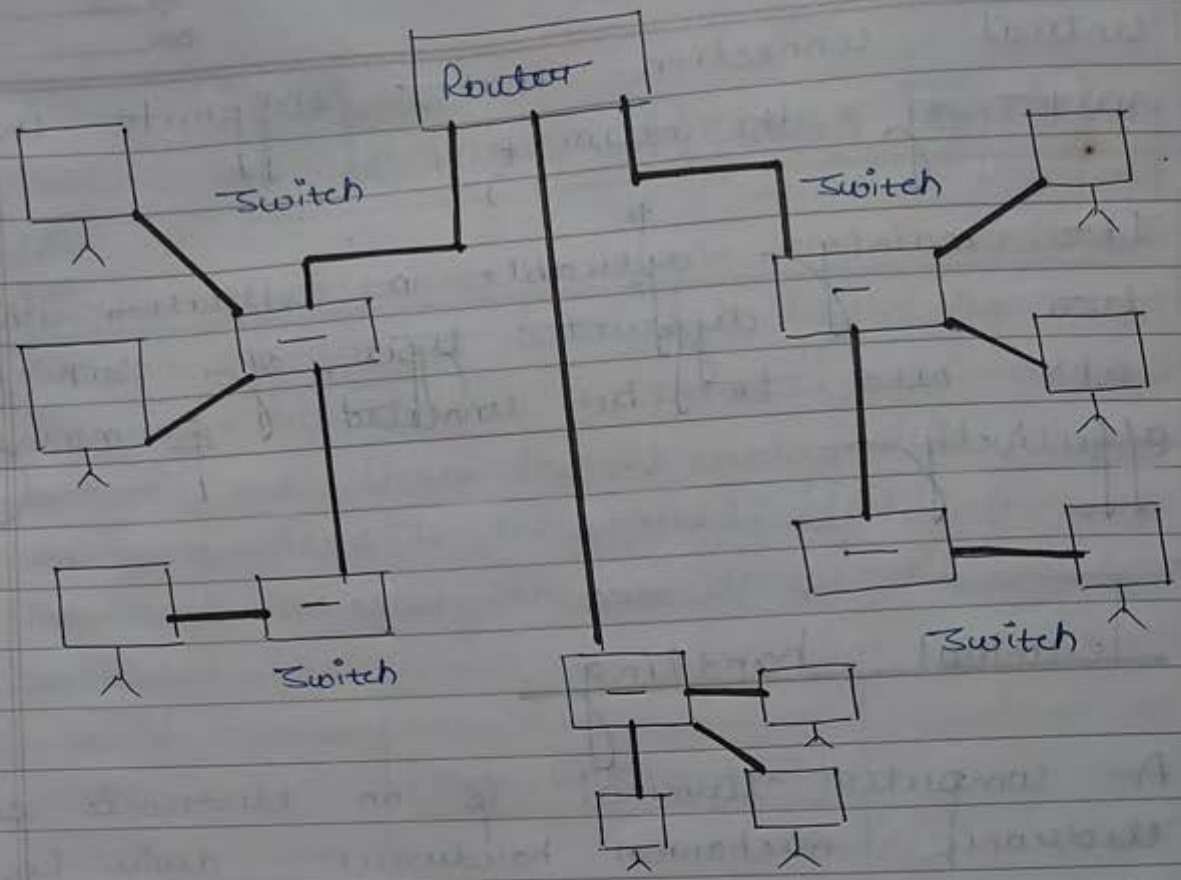
It consist of two or more nodes linked to each other via singal cable in series connecting to an extension to the network.



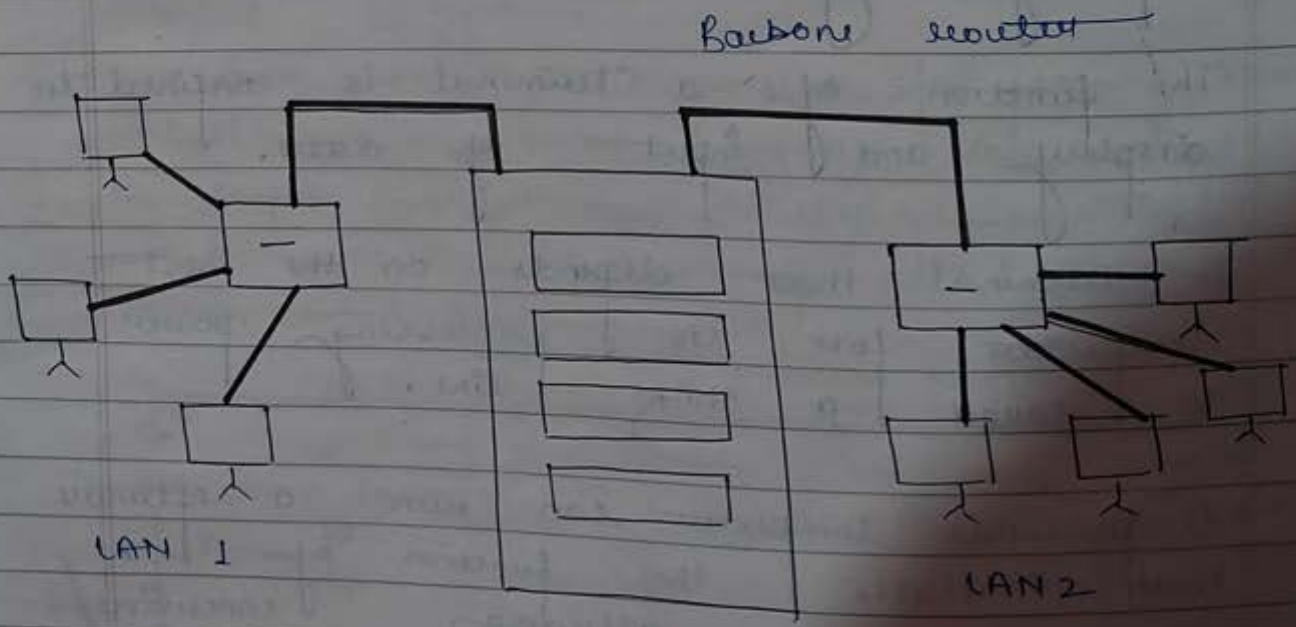
Rarely used for Enterprise level n/w topology.

Distributed -

It comprises of hierarchical formation of multiple devices are connected to switches. It is well suited for enterprise wide connectivity.



Collapsed



It makes use of a single but high specification router that serves as the actual backbone of

central connection that supports the rest of the network.

It mainly aplicable in situation where two different types of sub-networks need to be connected & managed effectively.

Terminal handling:

A computer terminal is an electronic or electronic mechanical hardware device i.e. used by entering data into and displaying data from a computer or a computing system.

The function of a terminal is confined to display and input of data.

A terminal that depends on the host computer for its processing power is called a thick line.

A personal computer can run a software that emulates the function of a terminal sometimes allowing concurrent use of local programs & access to a distant terminal host system.

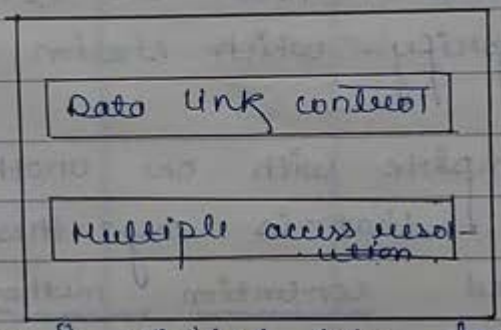
5/02/19

UNIT-II

Medium Access Sublayer

[MAC] Medium access control / Multiple access control

We can consider the data link layer as two sublayers. The upper sublayer is responsible for data link control and the lower sublayer is responsible for resolving access to the shared medium. If the channel is dedicated then we don't need the lower sublayer.



Data link layer is divided into two functionality oriented system.

1. The upper sublayer is responsible for flow & error control and is called logical link control.
2. The lower sublayer i.e., mostly responsible for multiple access resolution & is called media access control layer.

Multiple access protocols

- Random access Protocols
  - Aloha
  - CSMA
  - CSMA/CD
  - CSMA/CA
- Controlled access Protocols
  - Reservation
  - Polling
  - Token Passing
- Channelisation Protocols
  - FDMA
  - TDMA
  - CDMA

Random access protocols.

In random access / contention methods no station is superior over an other station and none is assigned the control over another. No station permits or does not permit another station to send.

Features

1) There is no scheduled time for a station to transmit.
2) Transmission is random among the station that is why these methods are called random access.
3) No rules specify which station should send next.

Stations complete with on another to access the medium that is why these methods are also called contention method.

* Aloha.

It is the earliest random method developed at the university of Hawaii in early 1970's. It was designed for a radio / wireless LAN but it can be used on any shared medium. The medium is shared b/w the stations when a station sends to data another station may attend to do some time. The data from the two stations collide and become garbled.

Pure Aloha :

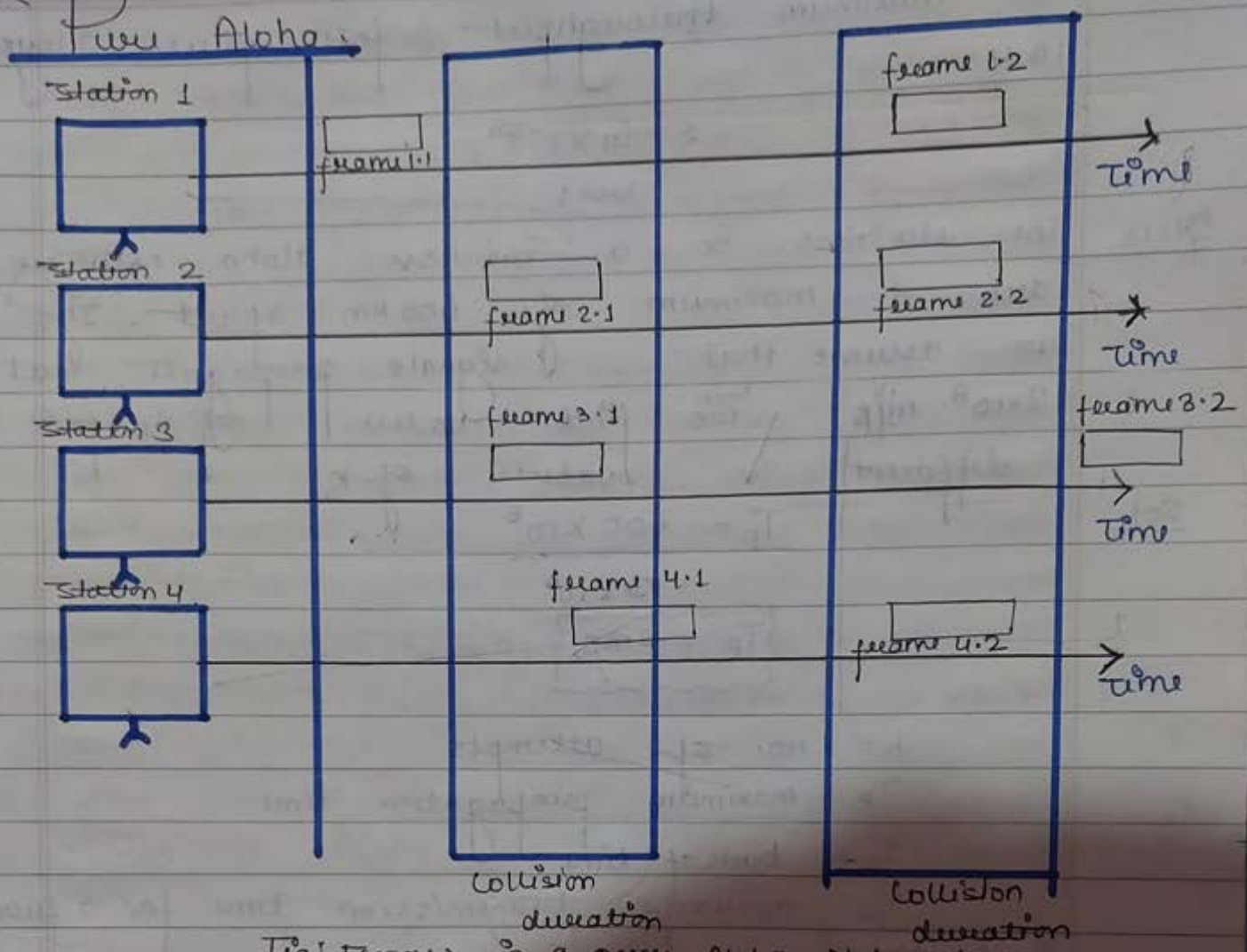


Fig: Frames in a pure Aloha Network

The original aloha protocol is called pure aloha. This is a simple but elegant (favourable condition) protocol. The idea is that each station sends a frame whenever it has a frame to send. However since there is only one channel to share there is the possibility of collision between frames of different stations.

1) In pure aloha, vulnerable time is two times the frame transmission time.

The maximum throughput for pure alloys 18.4%.

$$S = G \times e^{-2G}$$

$$G = \frac{1}{2}$$

Ques The stations on a wireless aloha network are a maximum of 600 km apart. If we assume that signals propagate at 3×10^8 m/s Now we find value of T_B for different values of K.

Sol

$$T_p = \frac{600 \times 10^6}{3 \times 10^8}$$

$$T_p = 2 ms$$

T_p =

K = no. of attempts

T_p = maximum propagation time

T_B = back off time

T_{fr} = average transmission time for a frame

Backoff time

The backoff time T_B is a random value that normally depends on K {no. of attempted unsuccessful transmission}. For each retransmission a multiplier in the range 0 to $2^K - 1$ is randomly chosen & multiplied by T_p or T_{fr} to find T_B.

Range value 0-1s

$$T_B = RV * T_p \mid T_{fr}$$

0 to $2^K - 1$

for K=1

0 to $2^1 - 1 = \{0, 1\}$

$T_B = \{0, 1\} \times T_p$

$= \{0, 2\}$

$K=2 \Rightarrow 0 \text{ to } 2^2-1 \Rightarrow \{0, 3\}$

$T_B = \{0, 1, 2, 3\} \times T_p$

$T_B = \{0, 2, 4, 6\}$

$K=3$

$0 \text{ to } 7 \Rightarrow \{0, 1, 2, 3, 4, 5, 6, 7\}$

$= \{0, 2, 4, 6, 8, 10, 12, 14\}$

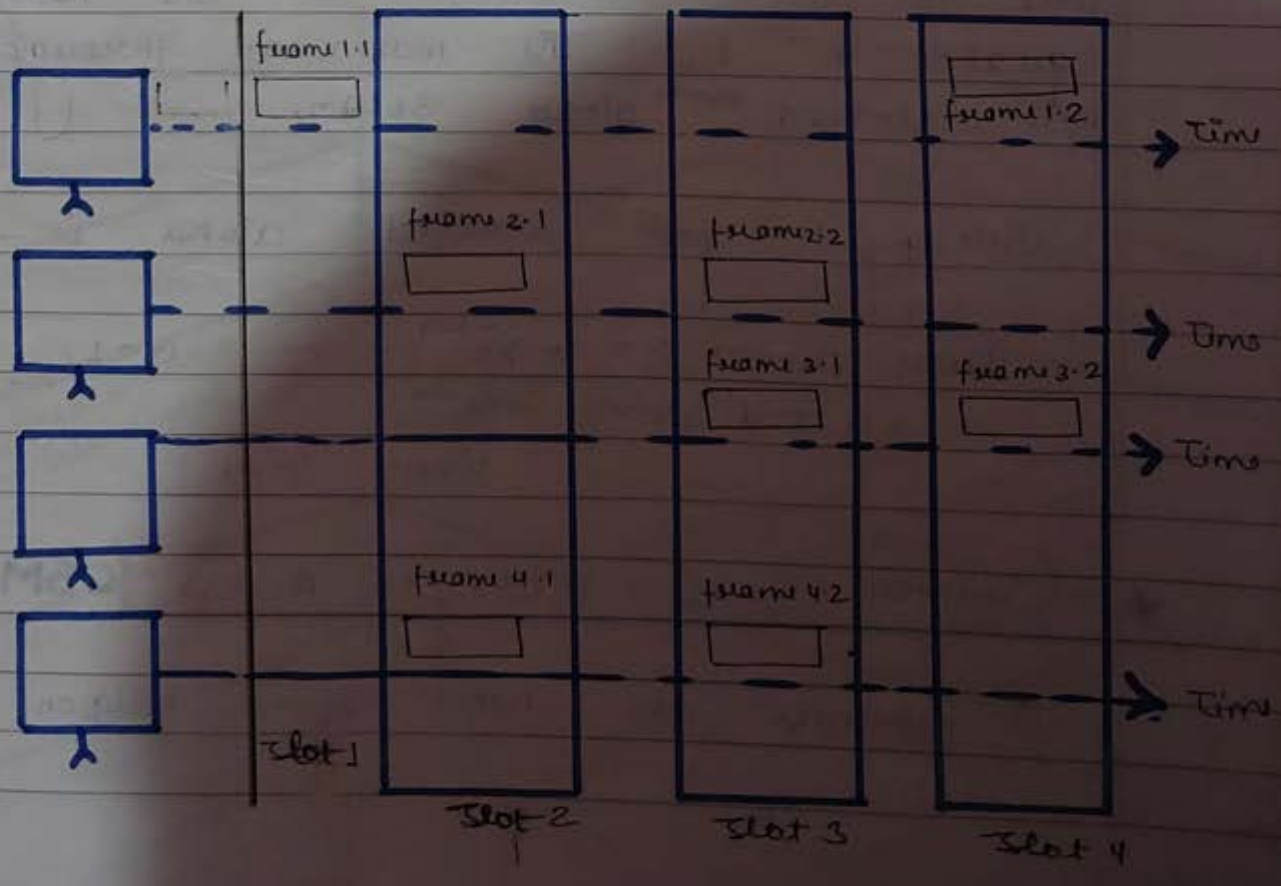
$K=4$

$0 \text{ to } 2^4-1$

$= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$

$= \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30\}$

Slotted Aloha.



It was invented to improve the efficiency of pure aloha in this we divide the time into slots & force the station to send only at the beginning of the time slot because a station is allow to send only at the beginning of the synchronized time slot. If a station misss this moment, it must wait until the beginning of the next time slot. This means that the station which started at the beginning of this slot has already finish sending its frame. There is still the posibility of collision if two station try to send at the beginning of the same slot however the vulnerable time is now reduced to one half equal to t_{fr}. The maximum throughput for slotted aloha 36.8%.

Throughput for slotted aloha is -

Pure aloha → $S = G \times e^{-2G}$ $G = 1/2$

Slotted aloha = $G \times e^{-G}$

where $G = 1$

Area where a signal exist

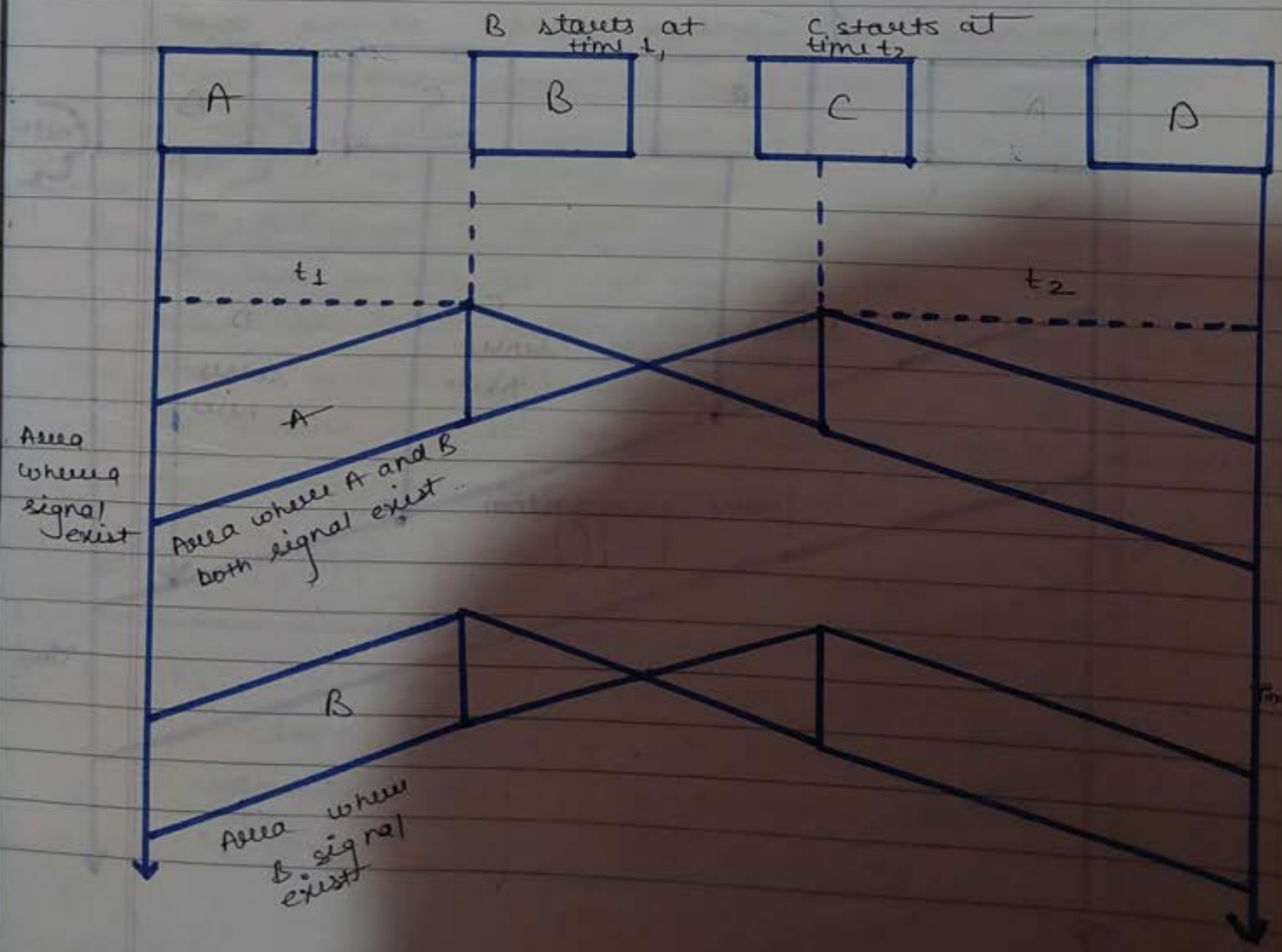
* Carrier Sense Multiple Access {CSMA}

To minimize the chance of collison

And therefore increase the performance the CSMA method was developed. The chance of collision can be reduced if a station ceapes a medium before time to use it.

CSMA requires that each station first listen to the medium or check the state of the medium before sending. In other words it is based on the principle "sense before transmit or listen before talk."

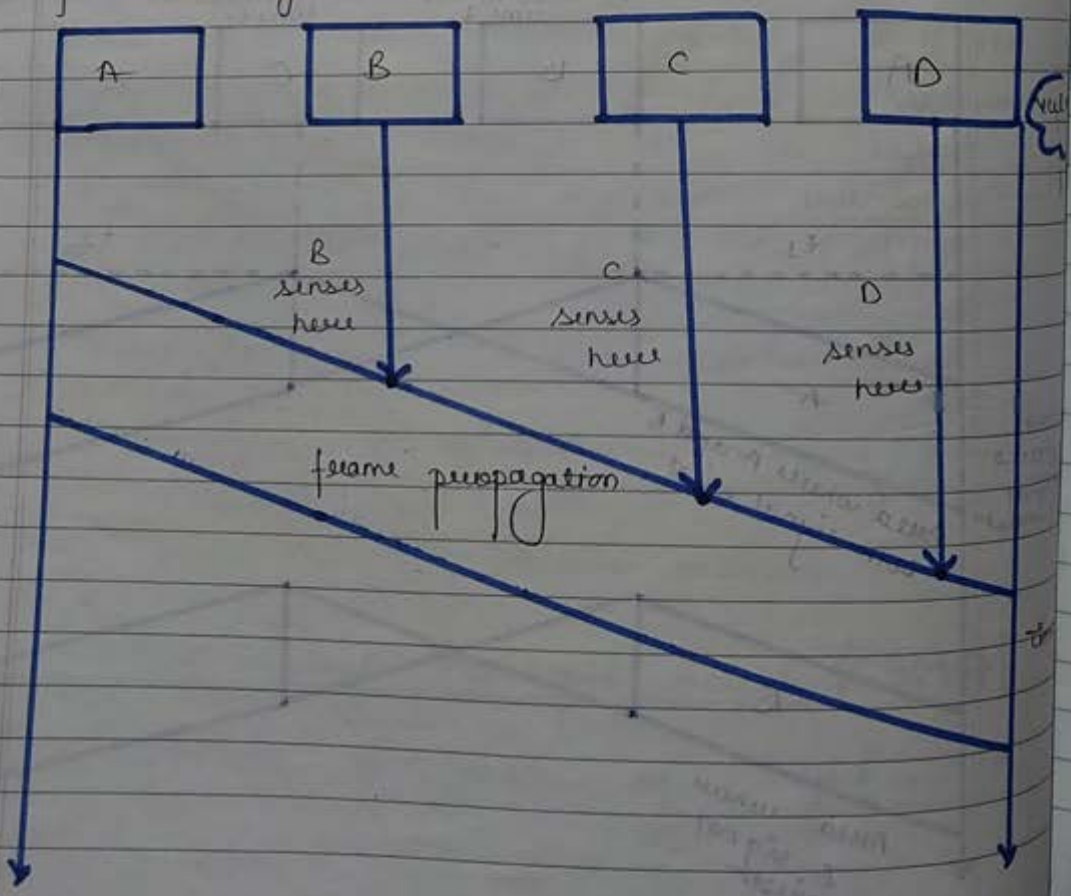
It can reduce the possibility of collision but it cannot eliminate it.



The vulnerable time for CSMA is same as the propagation time.

Vulnerable time

This is a time needed for a signal to propagate from one end of medium to the other when a station sends a frame & other station tries to send a frame during this time a collision will occur but if the first bit of the frame reaches the end of the medium. Every station will already have heard the bit & will refrain from sending.



Vulnerable time = propagation time

1. Non-

If a st
that
fixed int
clocks.
is free

2. On-pers

In this
continuous
and then
this ste
If two
-sion st
channel

3. P- Pers

In this
allow to
channel b
The stati
P.

* CSM

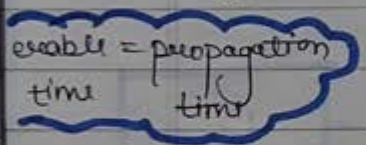
The CSM
procedure
augment
Coll

1. Non-persistant CSMA

If a station wants to transmit a frame and it finds that channel is busy then it has to wait for fixed interval of time. After this time it again checks the status of the channel & if the channel is free then transmit.

2. One-persistant CSMA

In this case the station which wants to transmit continuously monitors the channel until it become idle and then transmits immediately. The disadvantage of this strategy is that -
If two stations transmits simultaneously retransmission starts after finding the chances of channel free.



3. P-persistant CSMA

In this scheme all the waiting station are not allow to transmit simultaneously as soon as the channel becomes idle.
The station is to be transmitting with a probability p.

* CSMA/CD {CSMA with Collision detection}

The CSMA method does not specify the procedure following a collision. CSMA/CD augments the algorithm to handle the collision.

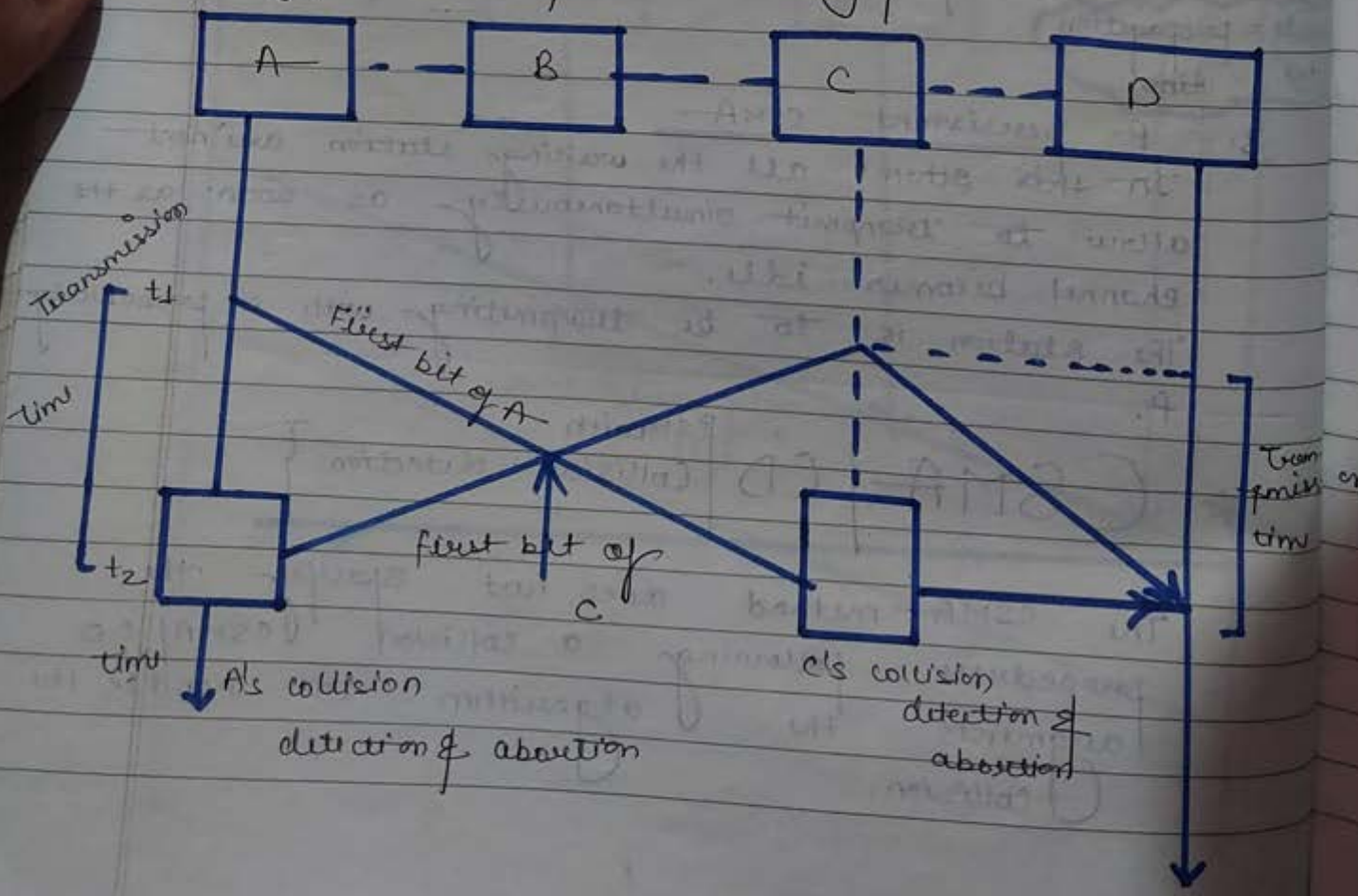
In this method a station monitores the medium after it sends a frame to see if the transmission was successful. If so the station is finished. If however there is a collision the frame is sind again.

Ex.

Let us look at the first bit transmitted by the two stations involved in the collision.

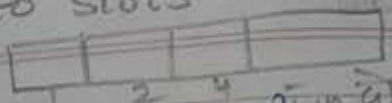
Although each station continues to sind bits in the frame until it detects collision.

It includes minimum frame size, procedures, energy level & throughput.



wireless NW

contention window
Amount of time divided into slots



* CSMA/CA (Collision Avoidance)

IFS → Interframe space

The station ready to transmit senses the medium by using one of the persistent strategy. As soon as it finds the line to be idle. The station waits for an interframe gap amount of time. It then waits for some random time & sends the frame. After sending the frame it sets the timer & wait for the acknowledgement from the receiver. If the acknowledgement is received before expiry of the timer then the transmission is successful. But if the transmitting station doesn't receive the expected acknowledgement before the timer expiry then it implements the backoff parameter. Waits for the backoff time & resumes the line.

In this collisions are avoided through the use of three strategies -

The Interframe space, the contention window, the acknowledgement.

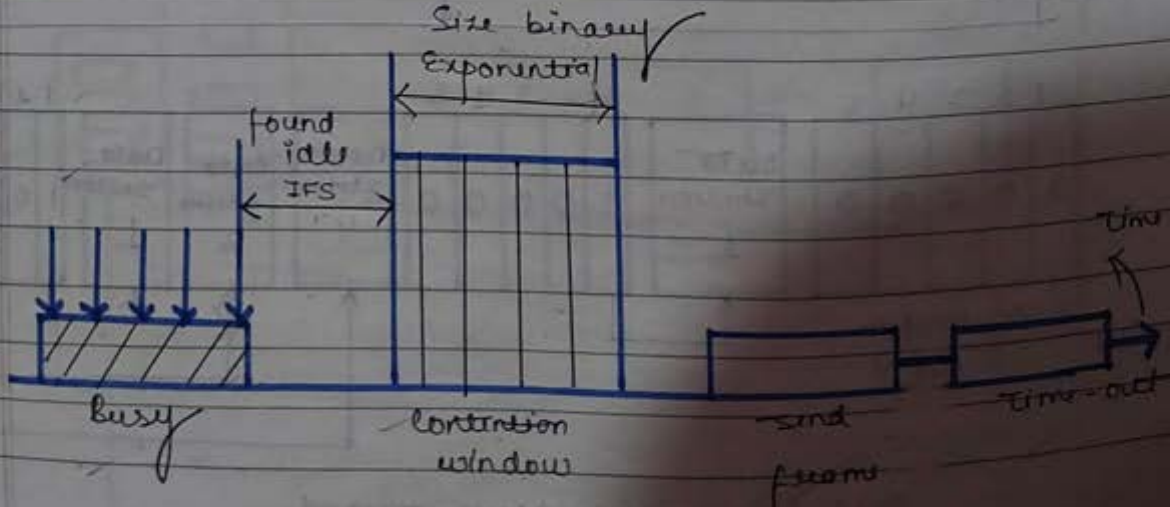


Fig: Timing in CSMA/CA

* Controlled access protocol

In this the stations concern one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations.

a) Reservation.

In this method a station needs to make a reservation before sending data. Time is divided into intervals. In each interval a reservation frame precedes the data frame sends in that interval. If there are n-stations in the system there are exactly n-reservation minislots in the reservation frame. Each slot belongs to a station when a station needs to send a data frame it makes a reservation in its own mini slot. The station that have made reservation can send their data frame after the reservation frame.

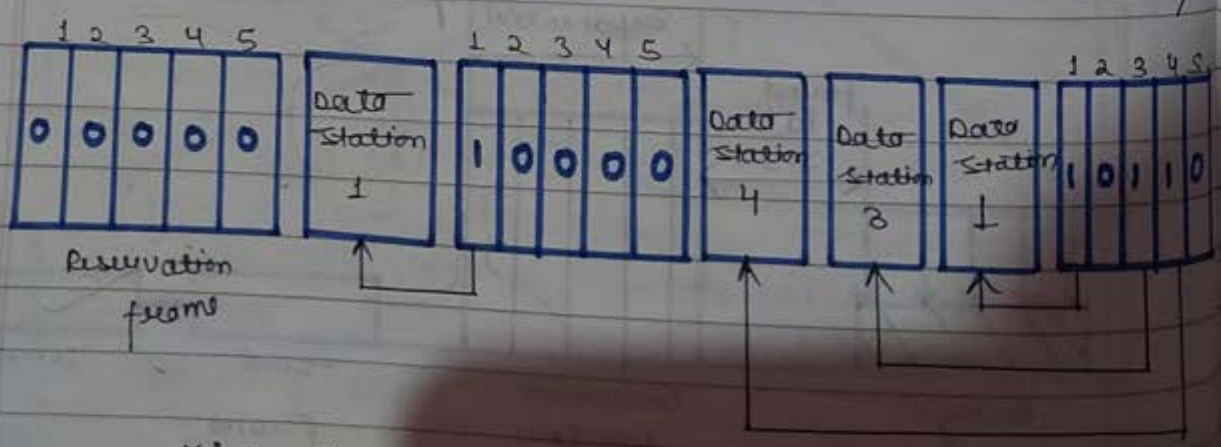


Fig: Reservation access method.

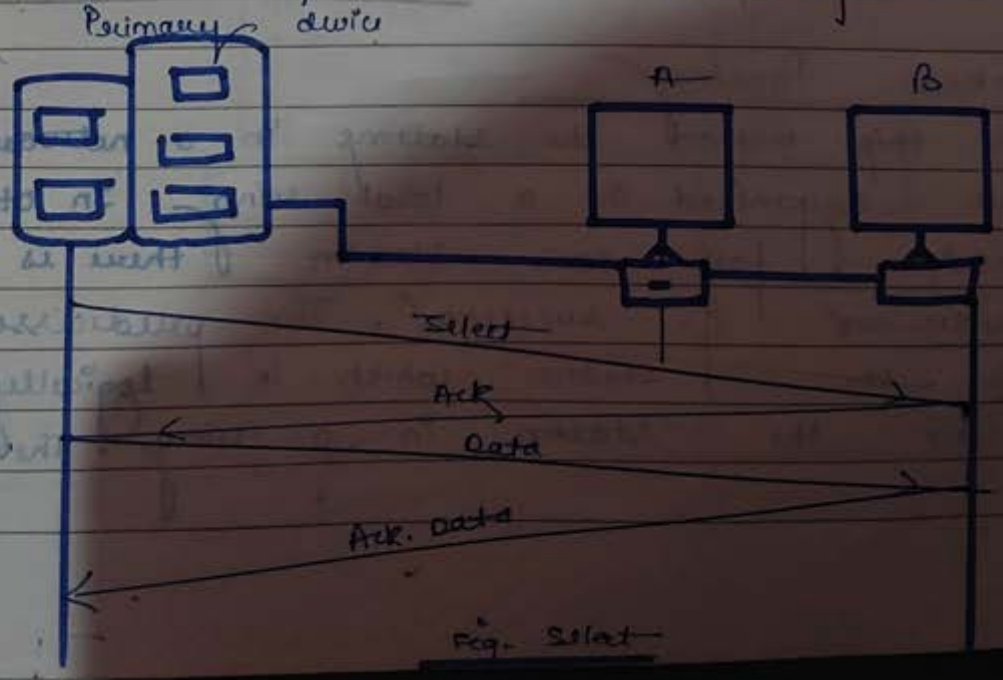
b) Polling

It works with topology in which one device is designated as a primary device / station & the other devices are secondary stations. All data exchange must be made through the primary device even when the ultimate destination is secondary device. The primary device controls the link, the secondary devices follow its instructions. It is up to the primary device to determine which device is allow to use a channel at a given time.

The primary device therefore is always the initiator of a session.

If the primary device wants to receive data it asks the secondary device, if they have anything to send.

If the primary device wants to send data it tells the secondary to get ready to receive this is called select function



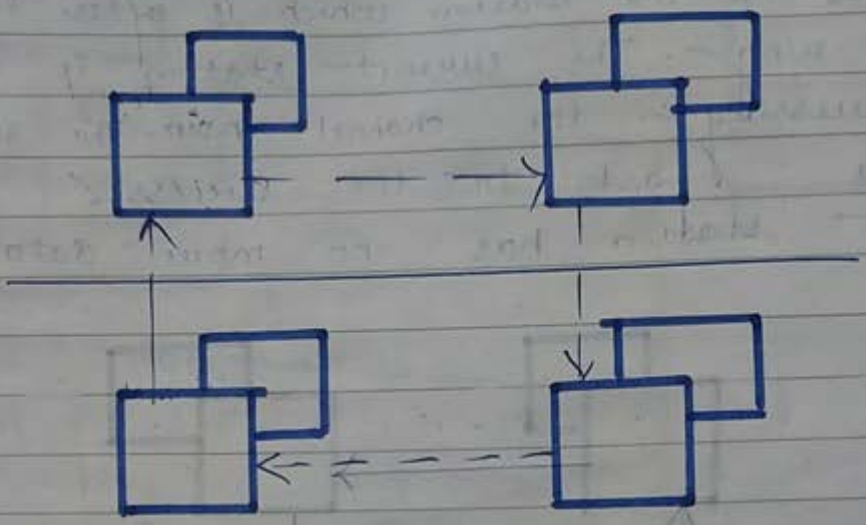


Fig: Bus ring

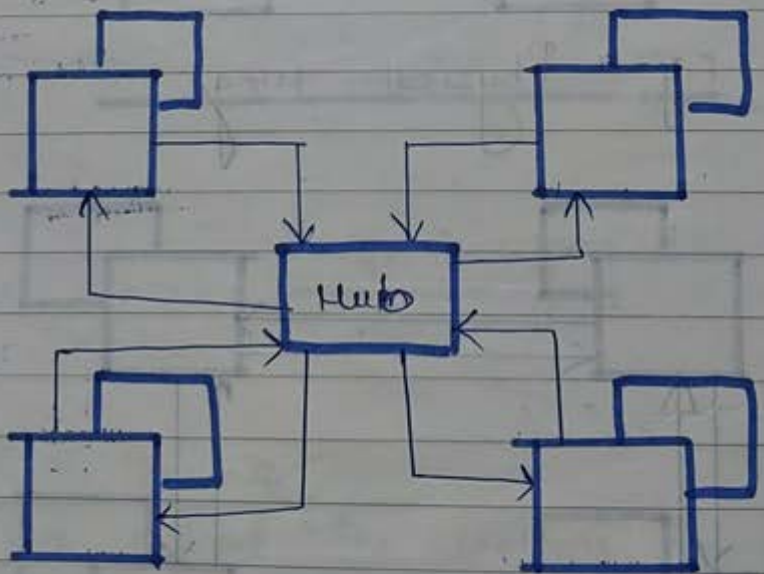


Fig: Star ring

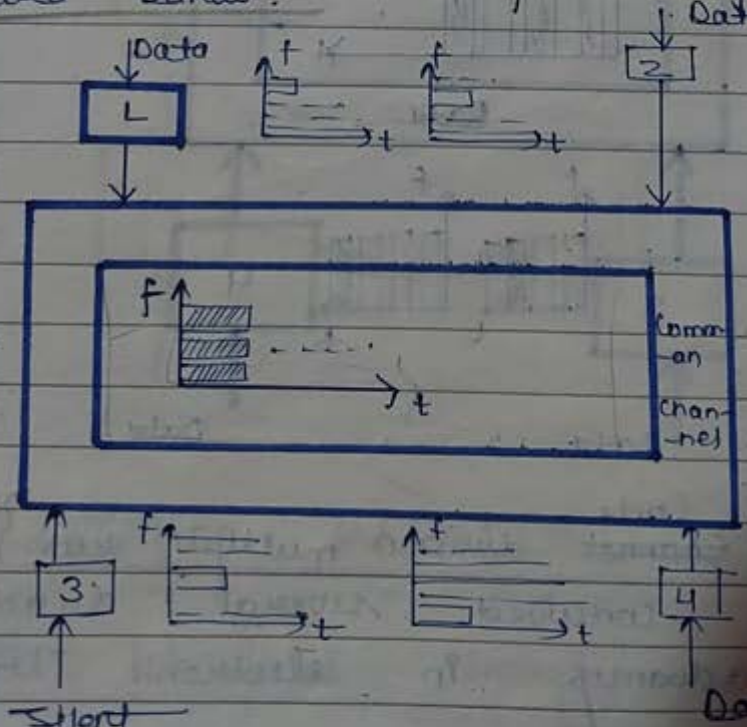
* Channelization

It is a multiple access method in which the available bandwidth of a link is shared in time, frequency or code b/w different stations.

FDMA (frequency division multiple access)

In this the available bandwidth is into frequency bands. Each station is allocated a band to send its data.

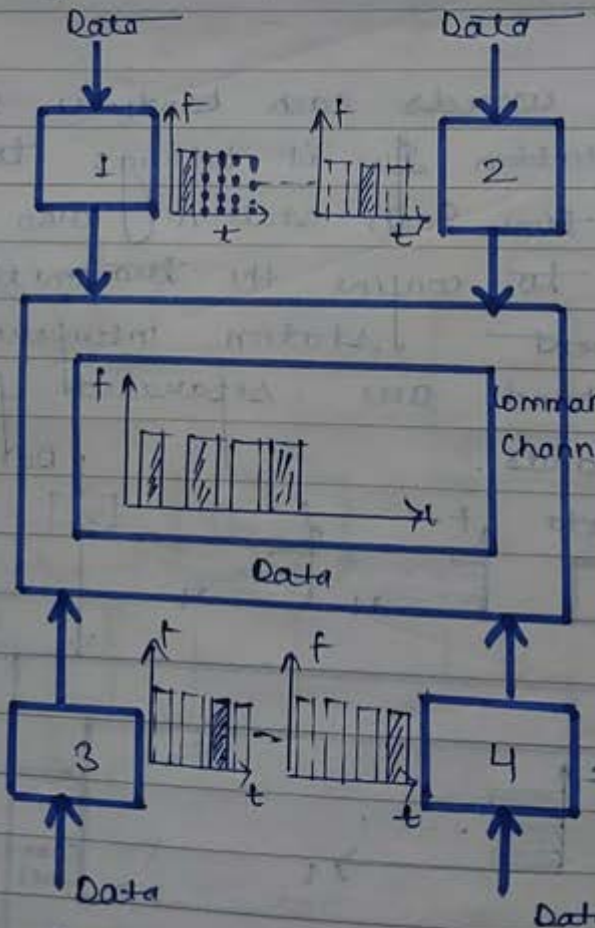
In other words each band is reserved for a specific station & it belongs to the station all the time. Each station also uses a band pass filter to confine the transmitted frequency. To prevent station interferences the allocated band are separated from one another guard bands.



Eg.: FDMA (Frequency division multiple access)

TDMA {Time division multiple access}

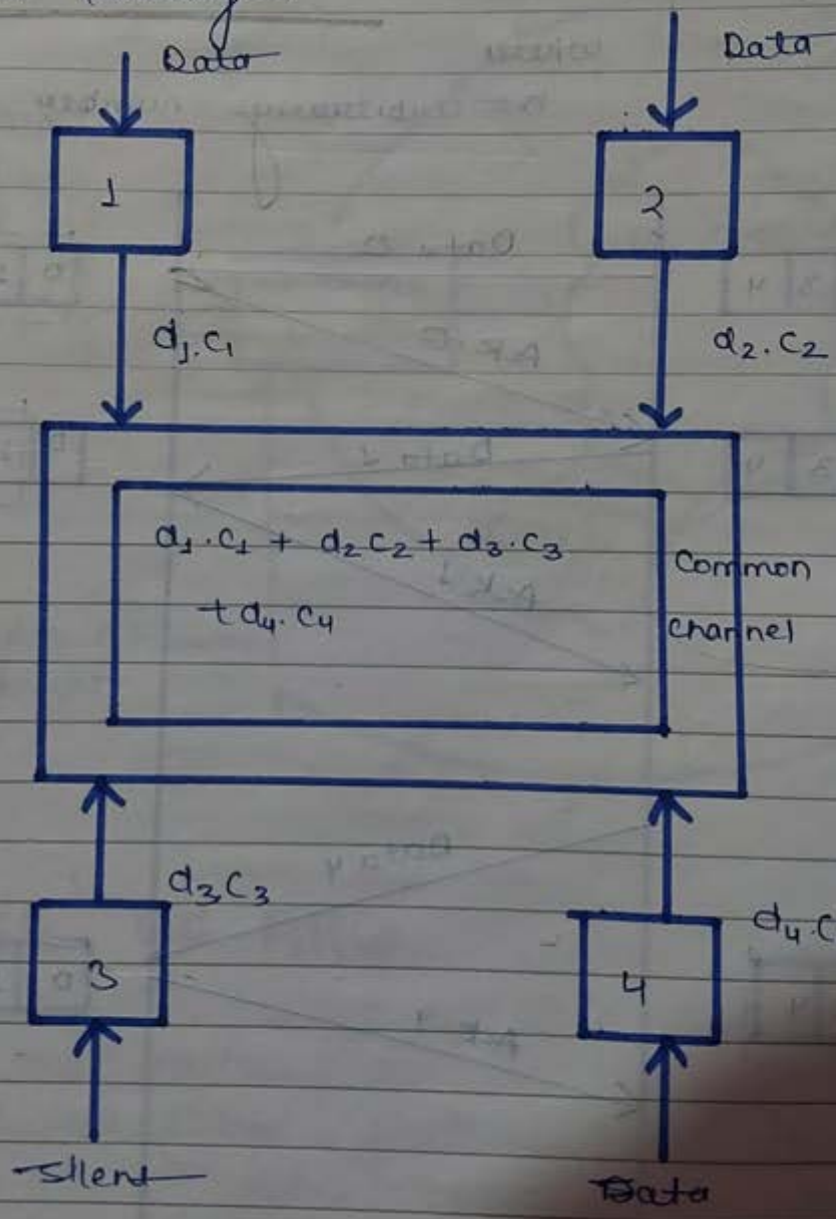
In this the stations share the bandwidth of the channel in time each station is allocated a time slot during which it can send data. Each station transmits its data in assign time slot. The main problem with TDMA lies in achieving synchronization b/w the different stations. Each station needs to know the beginning of its slot & the location of the slot



CDMA {Code ~~Channel~~ division multiple access}

It was conceived several decades ago. Present advances in electronic technology

have made its implementation possible. It differs from FDMA because only one channel occupy the entire bandwidth of link. It differs from TDMA because all stations can send data simultaneously there is no time sharing.



* SLIDING WINDOW PROTOCOLS

- **Sliding Window** Imaginary boxes at

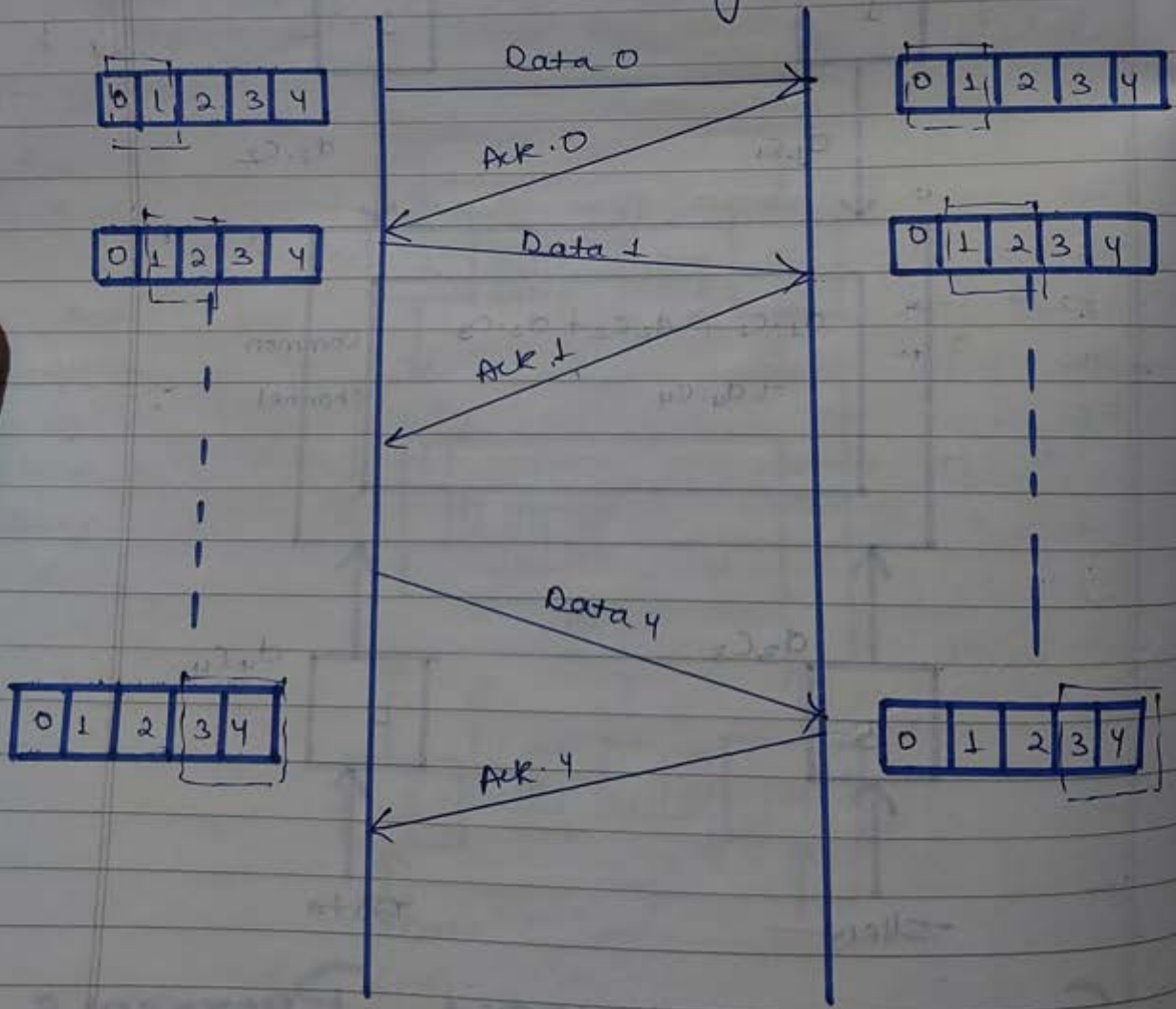
transmitter & receiver {temporary buffer storage area}.

- **Sequence no.**

Number given to each out bound frame {0 to 2^n}.

where

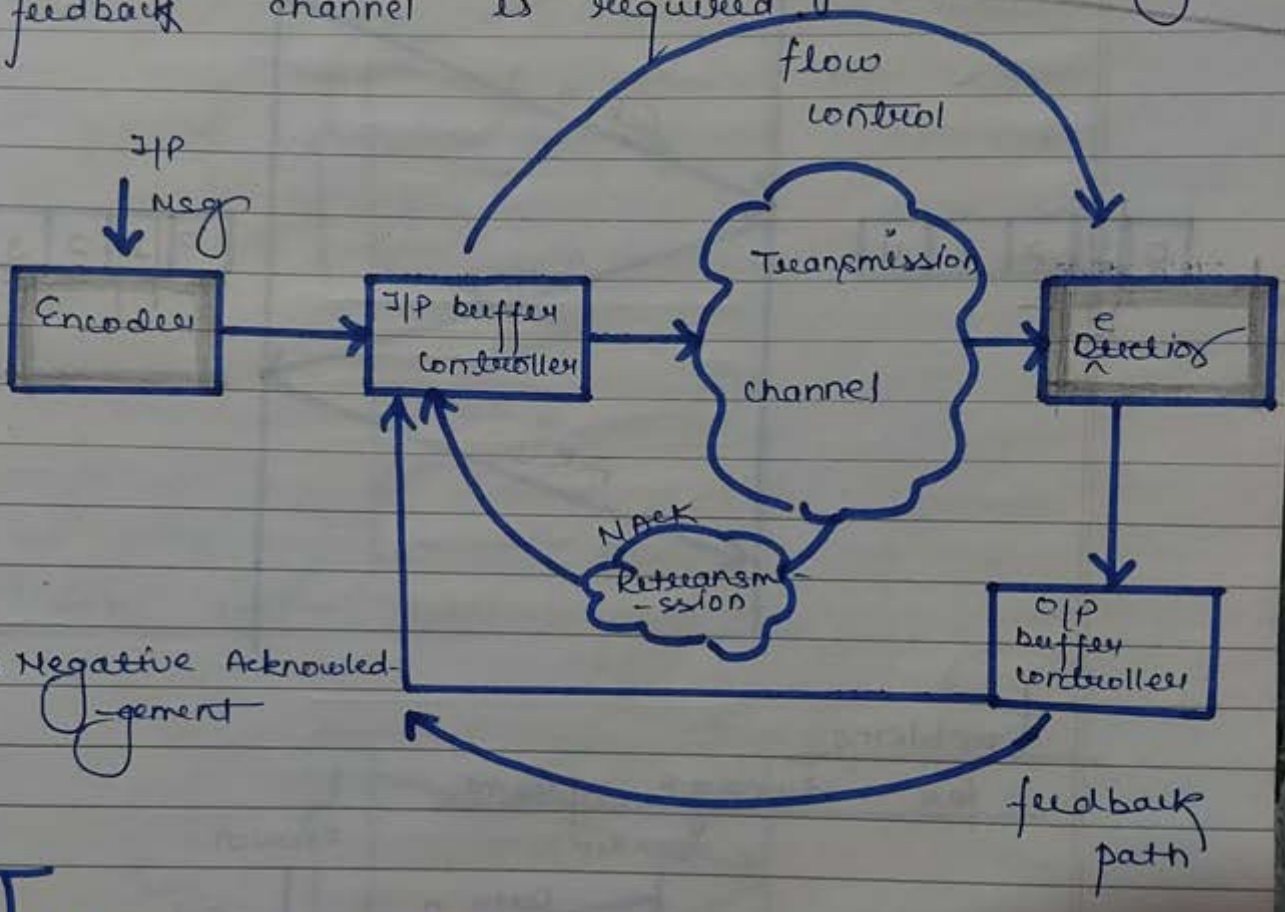
n = arbitrary number



Types

ARQ {Automatic review request}

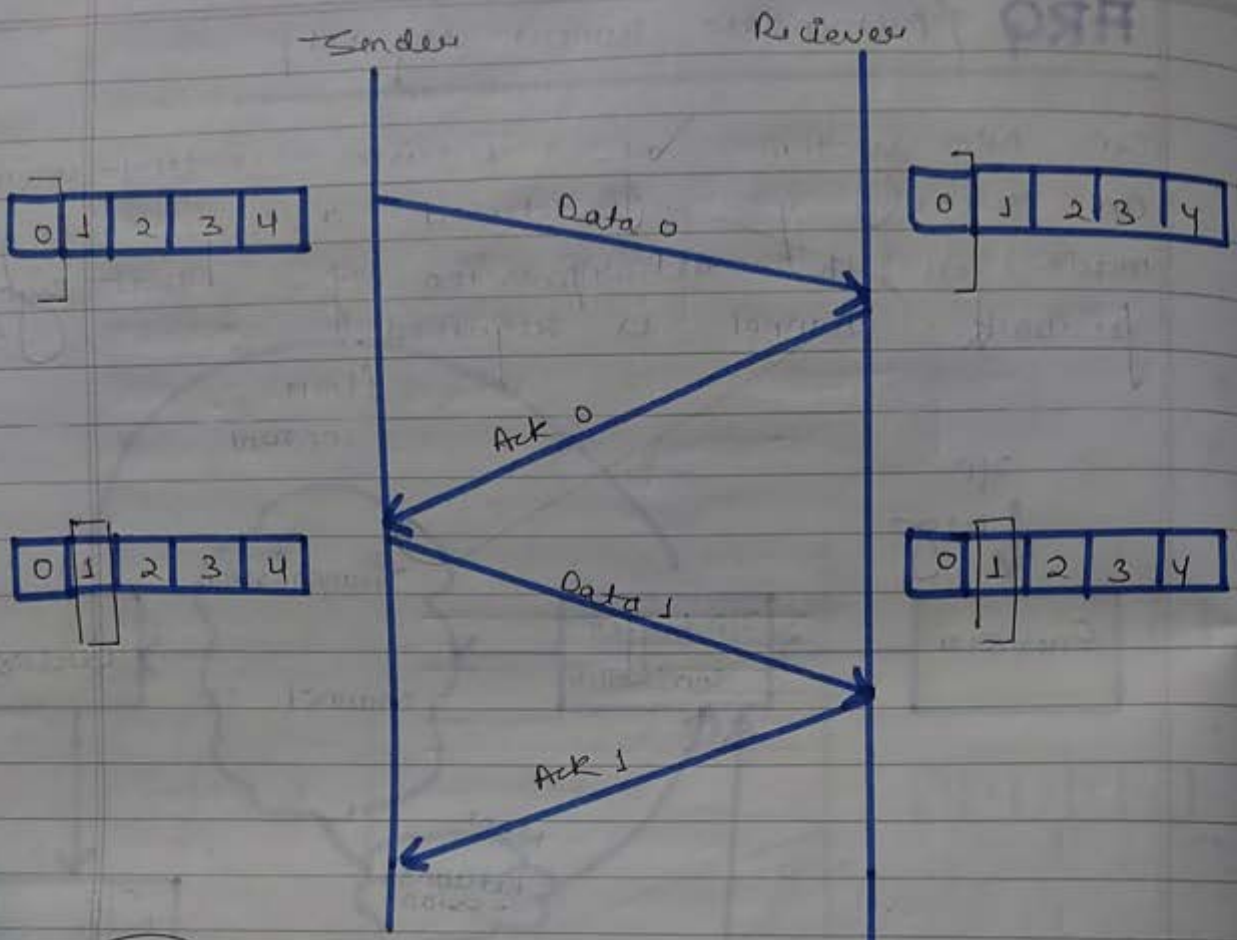
In ARQ system of error control when an error is detected a request is made for the retransmission of that signal feedback channel is required.



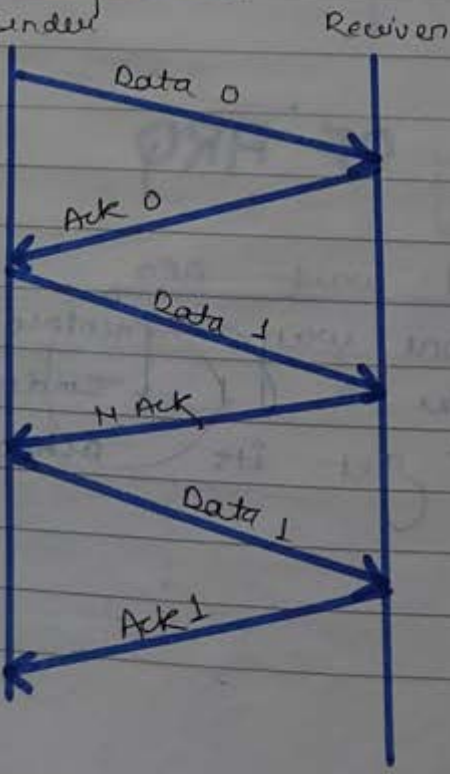
TYPES OF ARQ

1. Stop and wait ARQ

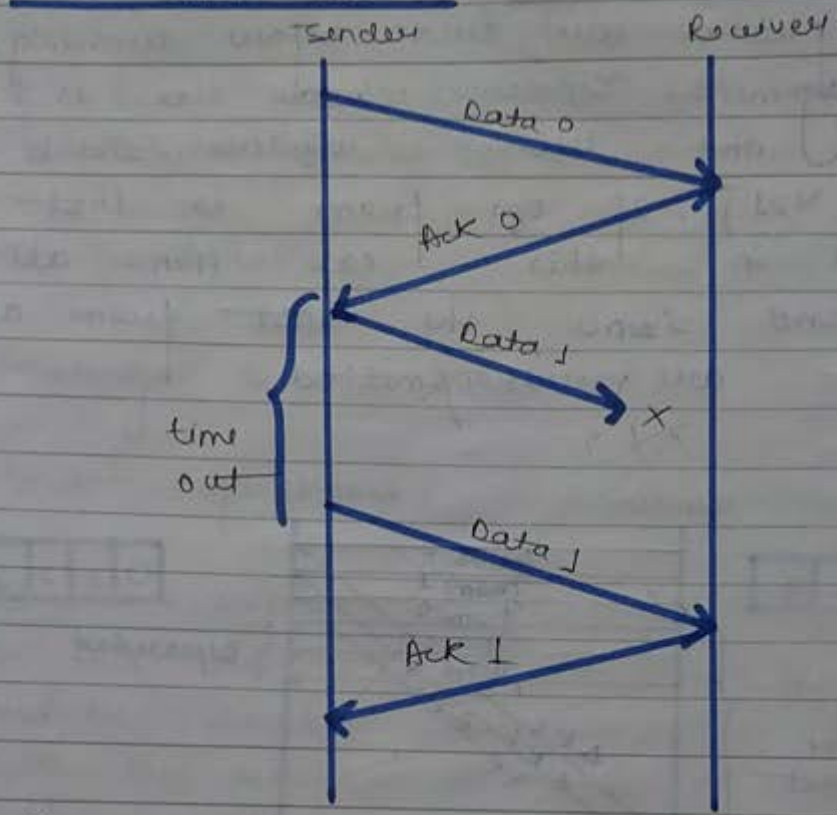
It is one way protocol that if the maximum window size is 1 Sender sends one frame & waits to get its acknowledgement



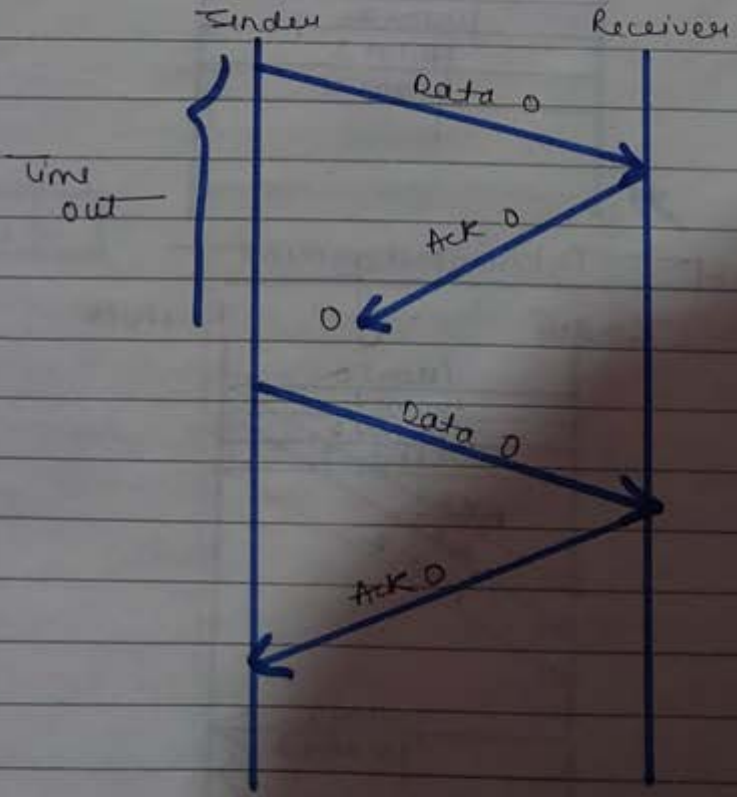
Problems for damage frame.



For lost data



For lost acknowledgement

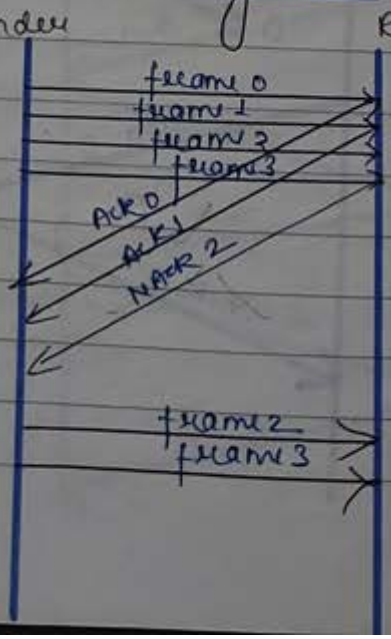


2. Go Back NARQ

Several frames are send before receiving acknowledgement. Sender window size is equal to N and receiver window size is equal to 1 (N>1). If one frame is lost or damaged in this case then all frames are send since the last frame acknowledgement are retransmitted.

for lost Acknowledgement

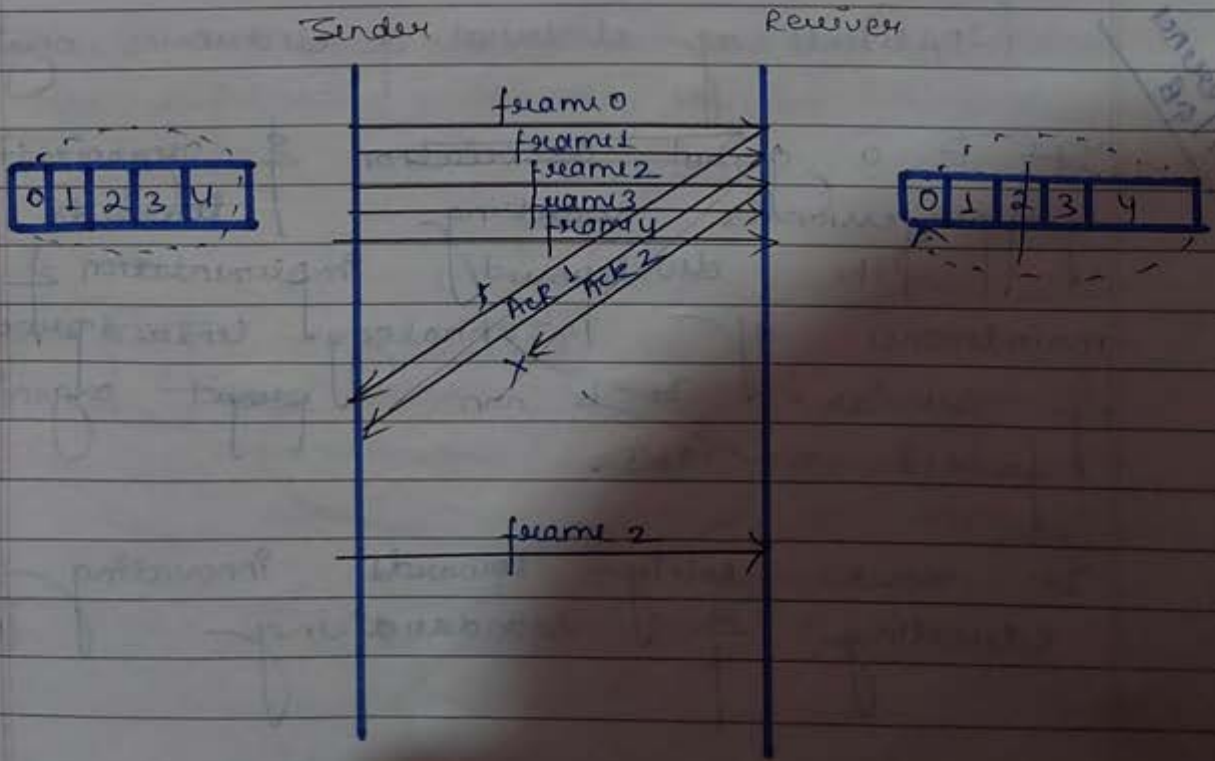
for lost data



1. Retransmits N [No. of frames) in case of any error.
2. If error rate is high it waste lost of bandwidth
3. Less complicated.
4. Sorting is not required
5. Most often used.

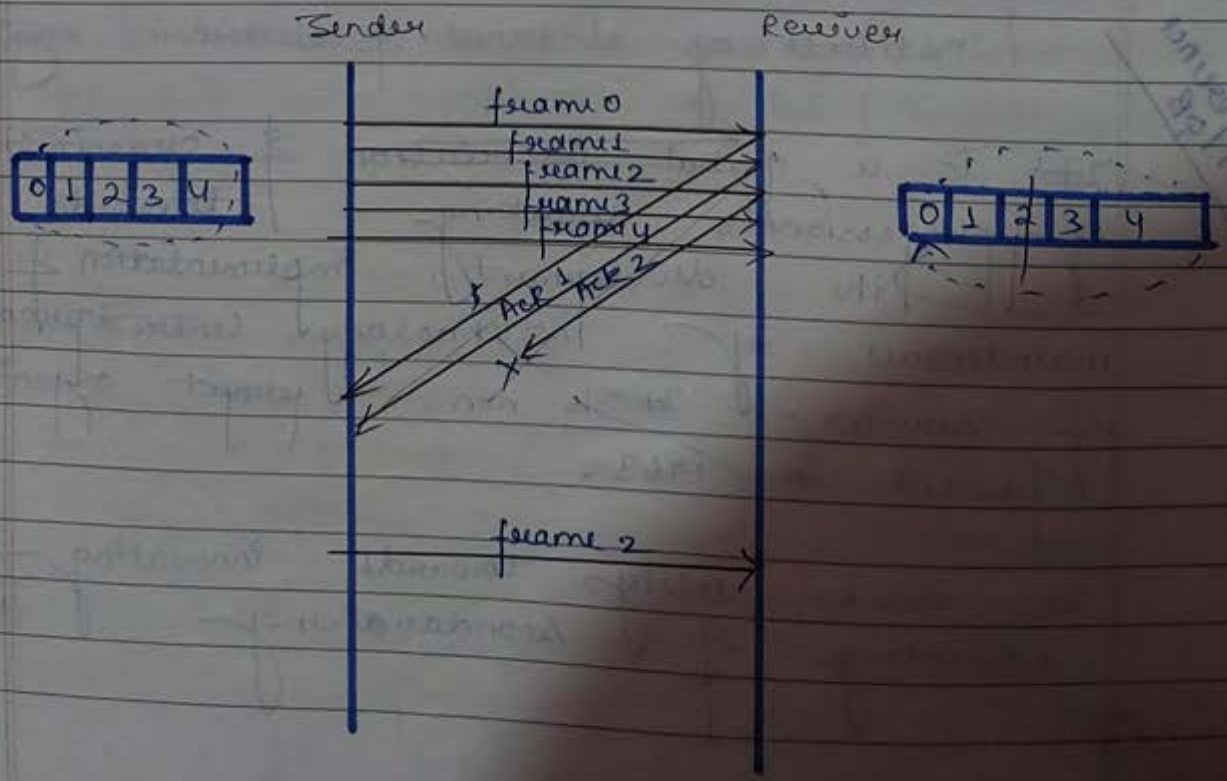
Selective repeat ARQ : (Automatic review request)

In this the sender window size is equal to receiver window size which is greater than 1. Only the specific damaged or lost frame is retransmitted.



1. Retransmits N [No. of frames] in case of any error.
2. If error rate is high it waste lost of bandwidth
3. Less complicated
4. Sorting is not required
5. Most often used.

Selective repeat ARQ : [Automatic review request]
In this the sender window size is equal to receiver window size which is greater than 1. Only the specific damaged or lost frame is retransmitted.



1. Retransmits only those frames that have problems.
2. less wastage of Bandwidth.
3. More complex.
   - Sorting
   - Storage
4. Sorting is requised
5. less use due to high complexity.

* IEEE Standards.

Difference QB

[Institute of electrical & electronics engineering]

It is a global association & organization of professionals working towards the development, implementation & maintenance of technology centered products & services. It is non profit organization founded in 1963.

It works solely towards innovating, educating & standardizing the

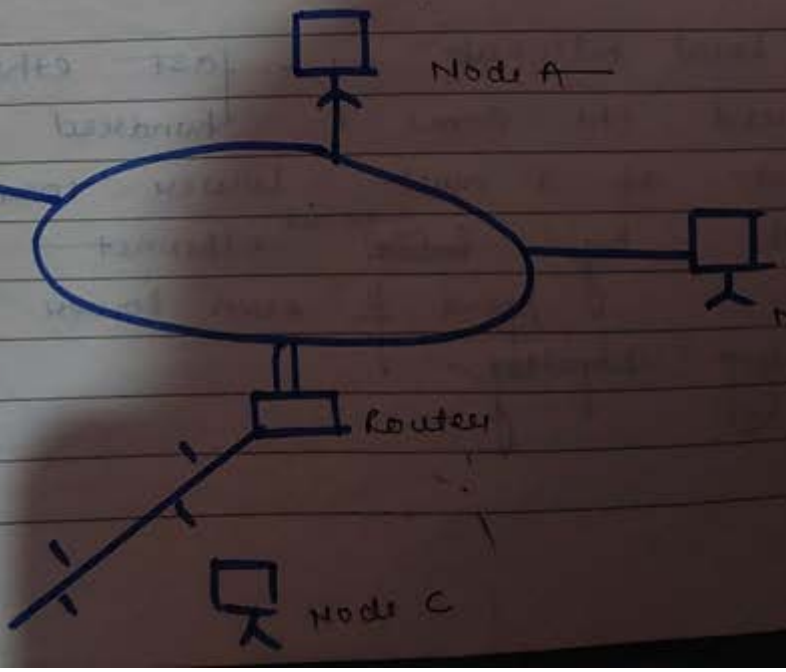
electrical & electronic development industry. It is best known for its development of standards such as - IEEE 802.11 [Wifi] LAN, Bluetooth.

The prime area of focus are electrical, electronics, computer engineering, CS, IT & most of them related disciplines.

Imp* FDDI [Fibre distributed data interface]

Quantum

It is a standard for data transmission in a LAN. It uses optical fibre as its standard underline physical medium, although it was also later specified to use copper cable in which case it may be call CDDI [Copper distributed data interface], standardized as TP_PMD [Twisted pair physical medium dependent] also referred to as TP_DDI [Twisted pair distributed data interface].



Topology

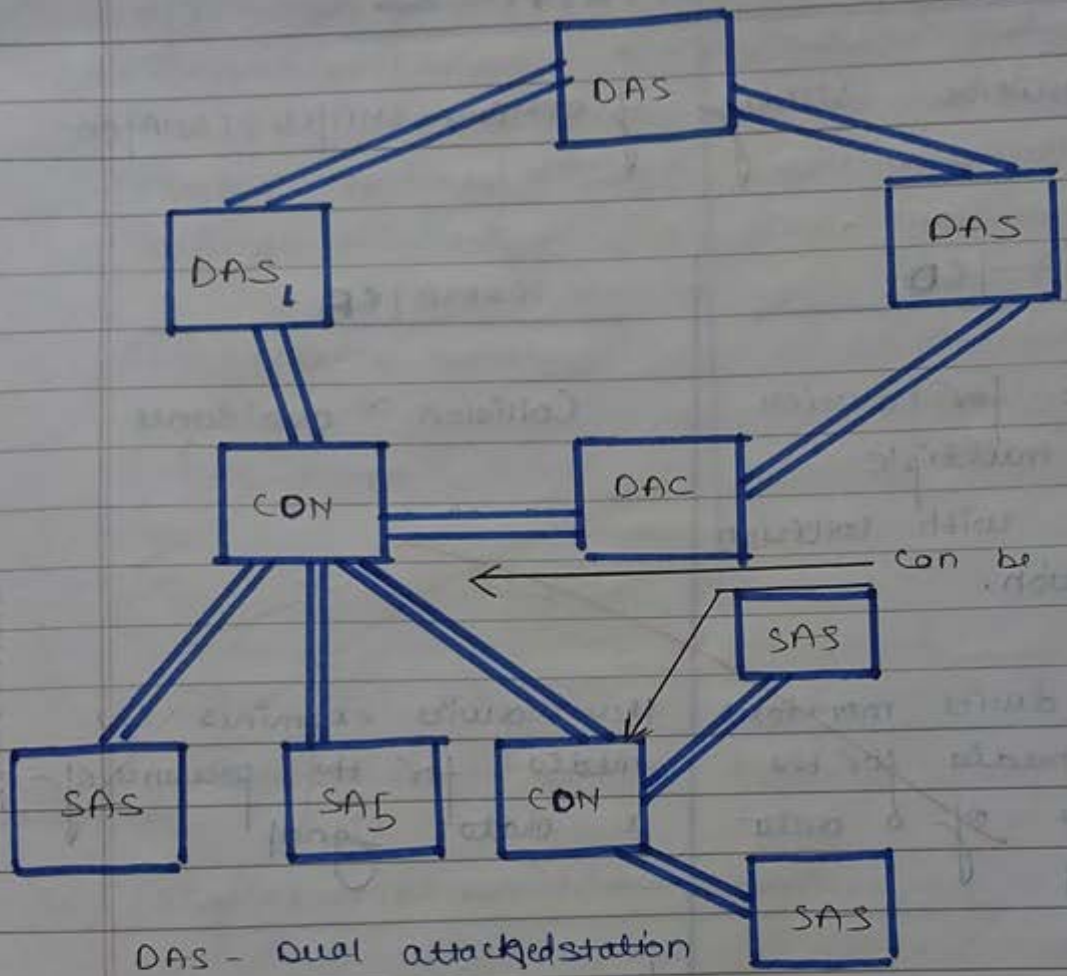
Designers normally constructed FDDI rings in a n/w topology such as a dual ring of trees. A small no. of devices, typically infrastructure devices such as routers & concentrators rather than host computers were dual attached to both the rings.

Host computers then connect as single attached devices to the routers or concentrators.

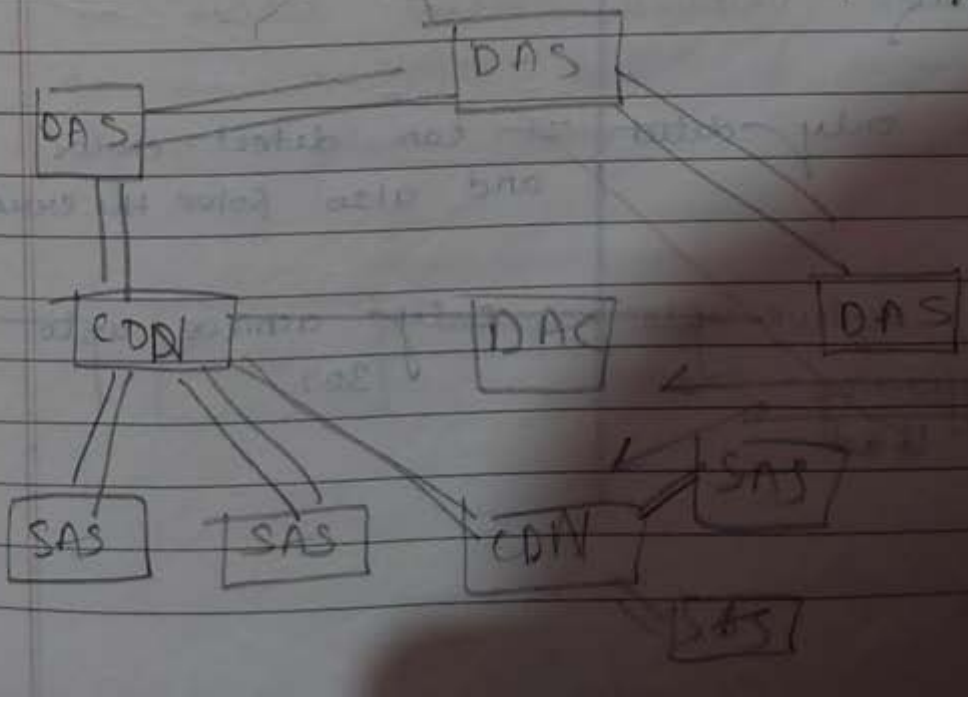
FDDI requires this network topology because the dual ring actually passes through each connected device & requires each such device to remain continuously operational.

FDDI was effectively make obsolete [अपने आप को इतना कर लेना]

In local network by fast ethernet which offered the same hundred Mbid/s speed but at a much lower cost & since 1998 by gigabit ethernet due to its speed & even lower cost & ubiquity.



DAS - Dual attached station
SAS - Single attached station
CDN - Concentrated attached Content delivery network



12/02/19

ASSIGNMENT-2

Quest. Comparitive study of ~~CSMA~~, CSMA/CD, CSMA/CA

Ans.

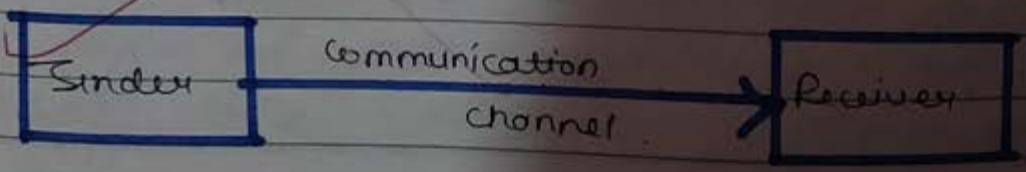
CSMA/CD	CSMA/CA
Stands for carrier sense multiple access with collision detection.	Collision avoidance
Here, device monitores the media for the presence of a data signal	Here, device examines the media for the presence of a data signal
This method is used by 802.3 Ethernet network.	This method is used by 802.11 Ethernet network.
It can only detect error	It can detect error and also solve the error.
It can achieve upto 70% efficiency and heavy load	Only achieve upto 30%.

It does not take any often to prevent collision	can take .
CSMA/CD is used at wired network	wireless
CSMA/CD is more popular than CSMA/CA	CSMA/CA is less popular than CSMA/CD .

Ques 2. Write short note on –

→ Simplex communication channel.

A simplex communication channel only sends information in one direction. For example, a radio station usually sends signals to the audience but never receives signals from them.



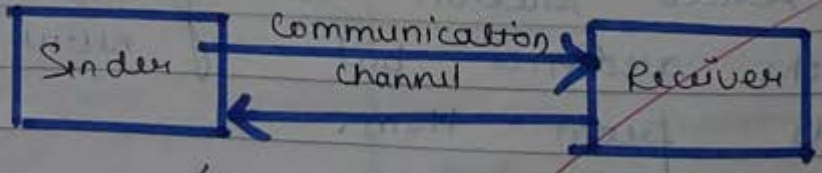
→ Half duplex.

In half duplex mode, data can be transmitted in both directions on a signal carrier but not at the same time.

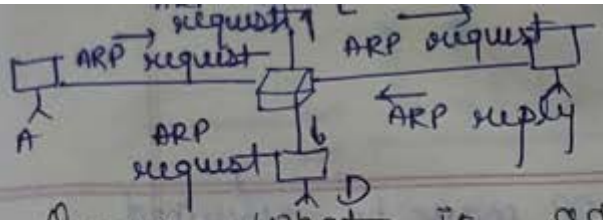
(one process done at a time) sending or receiving not both.

→ Full duplex.

A full duplex communication channel is able to transmit data in both directions on a signal carrier at the same time.



(transmission can be done at same time)

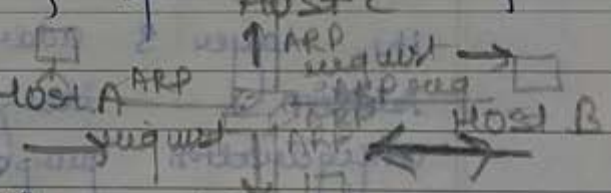


Ques 3. What is address resolution protocol and reverse address resolution protocol?

Ans Address resolution protocol.

The address resolution protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address typically an IPv4 address.

ARP has been implemented with many combinations of network & data link layer technologies.

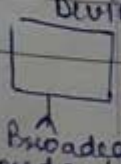


Reverse address resolution protocol

It is used to obtain Network Layer addresses (for example, IP addresses) of other nodes from Data Link Layer (layer 2) addresses.

It is primarily used in Frame Relay (DLCI) and ATM networks, in which Layer 2 addresses of virtual circuits are sometimes obtained from Layer 2 signaling & corresponding layer 3 addresses must be available before those virtual circuits can be used.

Since ARP translates Layer 3 addresses to



Broadcast MAC needs to know the IP

Receives MAC and tells IP of the device.

Layer 2 addresses. InARP may be described as its inverse. In addition, InARP is implemented as a protocol extension to ARP; it uses the same packet format as ARP, but different operation codes.

The Reverse address resolution protocol (Reverse ARP or RARP), like InARP translates Layer 2 addresses to Layer 3 addresses.

However, in InARP the requesting station queries the Layer 3 address of another node, whereas RARP is used to obtain the Layer 3 address of the requesting station itself for address configuration purposes. RARP is obsolete; it was replaced by BOOTP, which was later superseded by the Dynamic Host Configuration Protocol (DHCP).

UNIT 3

NETWORK LAYER

1. Point-to-Point N/W's

It refers to a communication connection b/w two communication end points or nodes. An example is a telephone call in which one telephone is connected with other & what is said by one caller can only be heared by the other.

This is contrasted with a point to multipoint or broadcast connection in which many nodes can receive information transmitted by one node

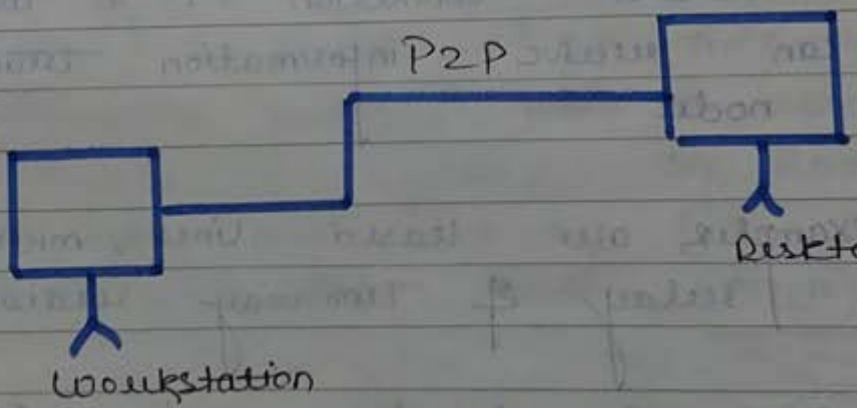
Other examples are leased lines, microwave radio relay & two-way radio.

It is also referred to a wire or other connection that links only two computers or circuits as opposed to other n/w topologies such as Buses or cross-bar switches which can connect many communication devices. Usage of point-to-point is differ from peer-to-peer n/w in the context of file sharing n/w.

Point-to-point n/w are mainly used for locations that need to securely send sensitive or confidential data b/w each location.

It provides high performance due to the low latency of the n/w.

For confidentiality purpose this service does not require data traffic to be routed over the public Internet.



Routing

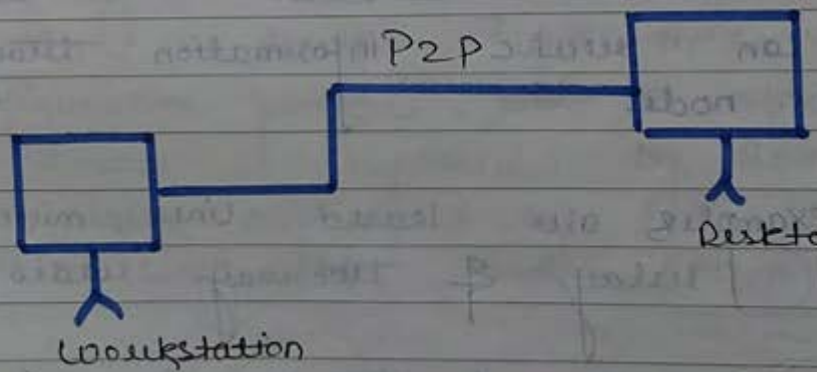
It is the process of selecting a path for traffic in a n/w or across multiple n/w's.

It is preferred in many types of n/w

Point-to-point n/w are mainly used for securely send sensitive or confidential data b/w each location. locations that need to

It provides high performance due to the low latency of the n/w.

For confidentiality purpose this service does not require data traffic to be routed over the public internet.



Routing

It is the process of selecting a path for traffic in a n/w or across multiple n/ws.

It is preferred in many types of n/w

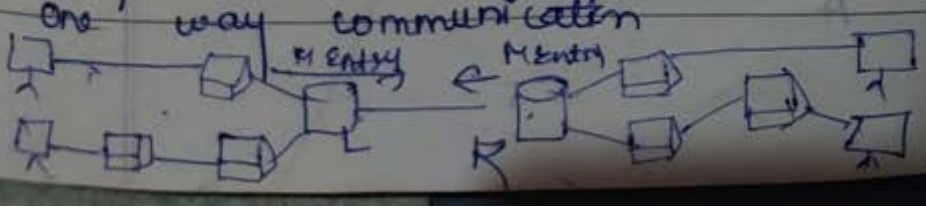
including circuit switched n/w such as PSTN and CN such as Internet).

The routing process usually directs forwarding on the basis of routing tables which maintain a record of the routes to various n/w destination.

Routing tables may be specified by an administrator, learned by observing n/w traffic or built with the assistance of routing protocols. It has become the dominant form of addressing over the Internet.

TYPES OF ROUTING

- Static routing
  - Manually entry of router's in routing table
  - Ideal for small organization
  - One way communication
- Adaptive routing / Dynamic routing
  - Distance Vector
  - Link state
  - Hybridized convergence



Static routing

The simplest form of routing is preprogram & consequently static routes. The task of discovering routes and propogating them throughout a network are left to the internetworks administrators. A router programmed for static routing forward packets out of predetermined ports. There are many benefits to using static routes. For instance, statically program routes can make for a more secure network. It is more resource efficient. It uses for less bandwidth across the transmission facilities does not waste any router CPU cycles try to calculate routes & requires for less memory. In some networks you might even be able to use smaller, less expensive routers by using static routes.

Dynamic routing.

a) Distance vector routing: Distance vector routing is also sometimes called Bellmann ford algorithm. The algorithm passes copies of their routing tables to their immediate network neighbours. Each recipient adds a

distance vector ie., its own distance value to the table & forwards it onto its immediate neighbours. This step by step process results each router learning about other routers & developing a cummulative perspective network distances. This cummulative table then used to update each routers routing table.

Example.

(i) Each router prepares routing table by their local knowledge each routers know about.

All the routers present in the network a distance to its neighbouring routers.

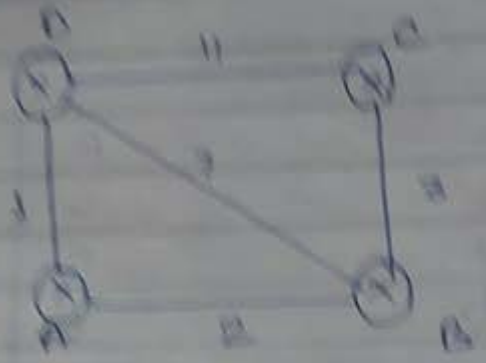
Each router exhanges its distance vector with neighbouring routers.

Each router prepares a new routing table using the distance vector. It has obtained from its neighbours.

This step is repeated for (N-2) times if there are N routers in the Network.

After routing tables converge & become stable.

Example



Step 1

→ Router A

Destination	Distance	Next Node
A	0	A
B	2	B
C	∞	-
D	1	D

→ Router B

A	2	A
B	0	B
C	3	C
D	7	D

→ Router C

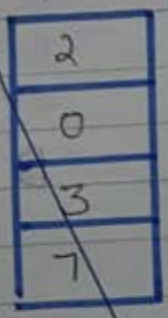
A	∞	-
B	3	B
C	0	C
D	11	D

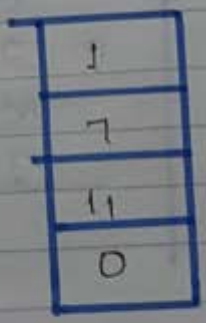
Router D

A	1	A
B	7	B
C	11	C
D	0	D

Step 2

Router A





Cost (A → B) = 2

Cost (A → D) = 1

Cost of reaching destination B from router A) min (

Cost of reaching destination C from router

Cost of reaching destination D from router

B

New table of D

A	1	A
B	9	A
C	10	B
D	0	D

These will be the final

Step 2.

Router A

2
0
3
7

1
7
11
0

Cost of reaching B from router A = min(2+0, 1+7) = 2

" " " C " " A = min(2+3, 1+11) = 5

" " " D " " A = min(2+7, 1+0) = 1

Updated table of A.

A	0	A
B	2	B
C	5	B
D	1	D

Router B.

0	∞	1
2	3	7
∞	0	11
1	11	0

Cost of reaching A from router B = min(2+0, 3+∞, 7+1) = 2

" " " C " " " = min(2+∞, 3+0, 7+11) = 3

" " " D " " " = min(2+1, 3+11, 7+0) = 3

Updated table

A	2	A
B	0	B
C	3	C
D	3	A

Router C

2	1
0	7
3	11
7	0

Cost of reaching A = min (3+2, 11+1) = 5

" " " B = min (3+0, 7+11) = 3

" " " D = min (3+7, 11+0) = 10

Updated table of Router C

A	B	C
A	5	B
B	3	B
C	0	C
D	11	B

Router D

0	2	∞
2	0	3
∞	3	0
1	7	11

A → 1
B → 3
C → 10

Updated table of D

A	1	A
B	3	A
C	10	B
D	0	D

Step 3.

Router A

B	D
2	1
0	3
3	10
3	0

Cost of reaching B from router A = min(2+0, 1+3) = 2

" " " C " " " = min(2+3, 1+10) = 5

" " " D " " " = min(2+3, 1+0) = 1

Updated table of router A

A	0	A
B	2	B
C	5	B
D	1	D

Router B.

0	5	1
2	3	3
∞	0	10
1	10	0

Cost of reaching A from router B = min(2+0, 3+5, 3+1) = 2

" " " C " " " = min(2+∞, 3+0, 3+10) = 3

" " " D " " " = min(3+1, 3+10, 3+0) = 2

Updated table of router B

A	2	A
B	0	B
C	3	C
D	3	A

BA ← BC

Router C

2	1
0	3
3	10
3	0

Cost of reaching A = min(3+2, 10+1) = 5
" " " B = min(3+0, 10+3) = 3
" " " D = min(3+3, 10+0) = 6

Updated table of C

A	5	B
B	3	B
C	0	C
D	6	B

CB

Router D

A	B	C
0	2	5
2	0	3
5	3	0
1	3	10

A → 1
B → 3
C → 6

Updated table

A	1	A
B	3	A
C	6	A
D	0	D

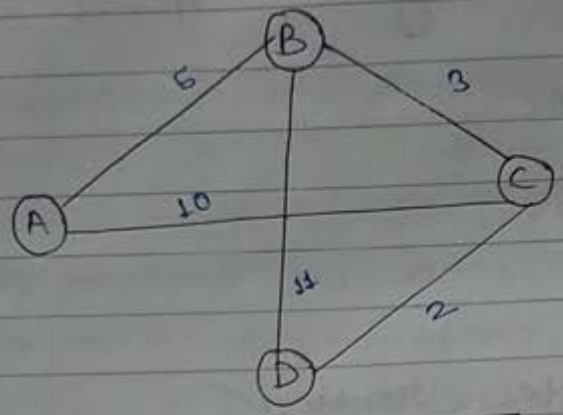
1. Value of next hop in the final routing table of router A suggest that only edges A B & A D are used.
2. B A & B C
3. C B
4. D A

b) Link State routing

Also known as shortest path first algorithm maintain a complete database of the n/w's topology. Unlike distance vector protocols link state protocols develop & maintain a full knowledge of the n/w's routers as well as how they interconnect. This is achieved via exchange of link state advertisements with other routers in a network. Each router that has exchanged LSA {link state advertisement} constructs a topological database using all received LSAs.

An SPF algorithm is then used to compute reachability to networked destinations. This information is used to update the routing table. This process can discover changes in the network topology caused by component failure or

network growth. It is both memory & processor intensive.



A
B/5
C/10

B
A/5
C/3
D/11

C
A/10
B/3
D/2

D
B/11
C/2

Link state DB in router D

c) Hybridized routing — It is third classification of routing algorithm. It uses distance vector to select more accurate matrix for selecting path & support routing information when there is change in n/w topology. This form of routing use distance vector matrix but emphasize more accurate matrix than conventional distance vector protocols. They also converge more rapidly than distance vector protocols but avoid the overheads of link state updates. A protocol enhanced Interior gateway routing protocol was designed to combine the best aspects of distance vector & link state routing

protocols with ensuring any of their performance limitations

d) **Convergence** - जब सारे सभी routers को network के द्वारे सभी routers तक पहुंचने की information हो जाए called converge n/w called converged network.

One of the most facinating aspects of routing is a concept known as convergence convergence. Convergence takes place whenever a change occurs in a n/w topology of shape all the routers in that n/w must develop a new understanding of what the n/w topology is.

(when there is change in n/w)

This process is both colaborative & independent; the routers share information with each other but most independently calculate the impacts of the topology change on there own routes.

(• change in n/w topology)

Convergence is necessary because routers are devices that can make their own routing decisions.

(• Link up, down; • n/w new router introduce हो; • old खराब हो जाए)

There are many types of routing

Protocols { Routing information protocol are dynamic routing protocol based on Bellman-Ford algorithm. }

1. **Routing information protocol**

The rip messages can be broadly

{ These protocols are used to decide where to send the datagram }

Classified into two types.

a) Messages that deliver routing information.

b) Messages that request routing information.

Both consist of fixed header followed by an optional list of manual & distance pair.

RIP version 1.

Command	Version	All zeroes
Address	Family	All zeroes
IP Address		
All zeroes		
All zeroes		
Metric		
Repeat of last 20 bytes		

20 bytes = 1 Network

Fig: RIP message Format

Command.

It indicates whether the packet is a request or a response. The request ask that a router sends a path of its routing table. The response can be unsolicited routing. Multiple rip packets are used to convey information from a large routing tables.

Version number.

It specifies a rip version used.

All zeros

This field was added solely to provide backward compatibility pre-standard variety of RIP. Its name come from its default value zero.

Address family identifier.

It specifies the address used. RIP is designed to carry routing information for several different protocols

Each entry has address family identifier indicate the type of address being specified.

Metric

Indicate how many network HOP (routers) have been traversed in the trip to the destination. This value is b/w 1 & 15

for a value hoot of 16. for an unreachable hoot.

2. Interior gateway routing protocol

It is distance vector IGRP make believe by CISCO. Router used to exchange routing data within an independent system.

IGRP created in part to cyeat each route as well as reliability, delay load & bandwidth.

The maximum HOP of ~~exterior~~ Enhanced IGRP is 255 & routing updates are transmiting 90 sec.

It measured in classful routing protocol but it is less popular because of wasteful of IP address spac.

Open shortest path first (OSPF)

It is an active routing protocol used in internet protocol. Particularly it is a link state routing

protocol & includes into a group of interior gatway protocol.

OSPF operating inside a distinct autonomous system.

The version 2 of OSPF defined in 1998 for IP version 4 than the OSPF version 3 in RFC 5340 in 2008. It is most widely used in the n/w of big business companies.

Exterior gatway protocol.

The absolute routing protocol for internet is exterior gatway protocol which is specified in 1982 by ERIC C.

EGP initialy expressed in RFC 827 & properly specified in RFC 904 in 1984. The EGP is unlike distance vector & path vector protocol. It is a topology just like tree.

Enhanced interior gatway routing protocol.

EIGRP based on three original IGRP while it is a CISCO proprietary

routing protocol. It is a distance vector routing protocol.

In advance within the optimization. lessen both the routing unsteadyness incurred after topology & attenuation + the users in bandwidth & processing power the router which support EIGRP will automatically allocate route information to IGRP neighbours by exchanging the 32-bit EIGRP metric to the 24-bit IGRP metric

Border gateway protocol.

These are the core routing protocol of the Internet & responsible to maintain a table of Internet protocol n/w's which authorized network reaching capability.

BGP expressed as path vector protocol. It does not employ conventional IGP metrics but making routing judgement based on path, network policies.

It is created to replace EGP routing protocol to permit completely decentralized routing.

The fourth version of BGP has been in use since 1994.

The fourth version RFC 4271 has many features such as it covers a lots of previous errors & brought it much nearer to industry practice.

Intermediate system to Intermediate System (IS-IS)

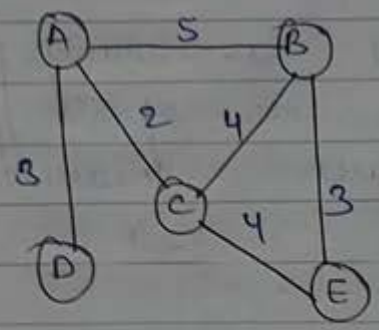
IS-IS is a great protocol used by network devices to determine the best way to promoted datagram from side to side a packet switched network & this process is called routing.

It was defined in ISO/IEC 10589/2002 within the OSI reference design.

IS-IS differentiate among levels such as level 1 & level 2. The routing protocol can be changes without contacting the intra area routing protocol.

IS-IS was designed to move data efficiently within a computer n/w or physically connated devices or similar devices.

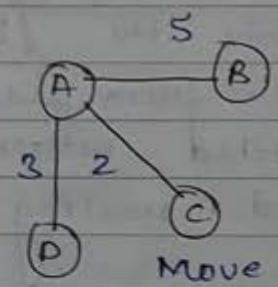
Example of Link state



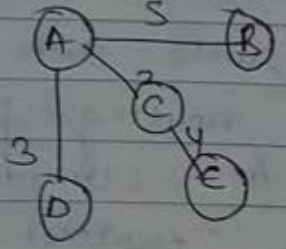
Node	Cost	Next. Router
A	0	-
B	5	-
C	2	-
D	3	-
E	6	E

1) (A) Root

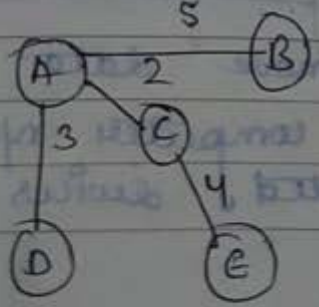
Set root to A & move A to tentative list.

2) 

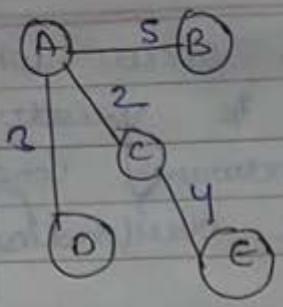
Move A to permanent list & add B, C, D to tentative list.

3) 

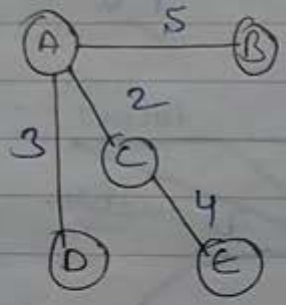
Move C to permanet list & add E to tentative list.

4) 

Move D to permanent list

5) 

Move B to permanent list.

6. 

Move E to permanent list

Permanent list : A(0), B(5), C(2), D(3), E(6)

Tentative list : Empty.

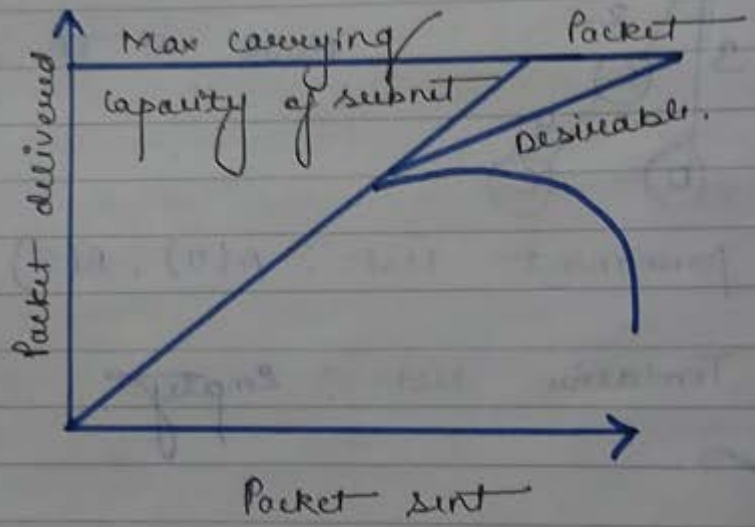
Congestion.

Congestion is an important issue that can arise in packet switched network. Congestion is a situation in computer networks in which too many packets are present in a part of the subnet, performance degrades.

Congestion takes place when network node or link is carrying more data than it can handle. This may result in packet loss.

Congestion in a n/w may occur when the load on the n/w is greater than the capacity of the n/w. Network congestion occurs in case of traffic overloading.

In other words when too much traffic is offered congestion sets in & performance degrades sharply.



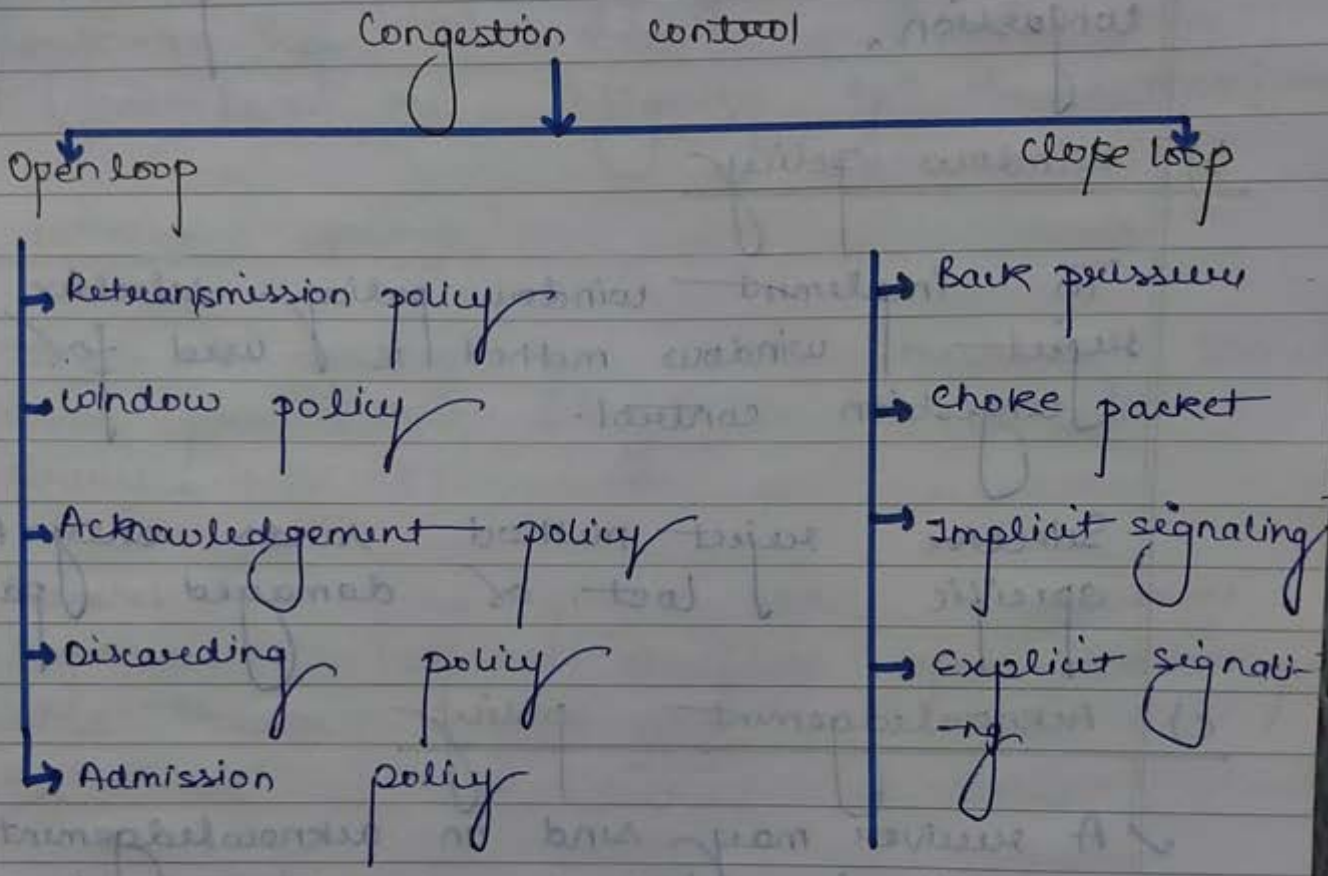
Congestion Control.

It refers to the mechanism & techniques to control the congestion & keep the load below the capacity.

OR

It refers to the mechanism that can either prevent congestion before it happens or

remove congestion after it happens.



* Openloop.

These policies are applied to prevent congestion before it happens. In these mechanism congestion control is handled by either the source or the destination.

Following are the policies -

a) Retransmission policy

The good retransmission policy to prevent

congestion & the retransmission timers need to be design to optimize efficiency & at the same time prevent the congestion.

b) Window policy

To implement window policy selective reject window method is used for congestion control.

Selective reject method sends only the specific lost or damaged packets.

c) Acknowledgement policy

✓ A receiver may send an acknowledgement only if it has a packet to be send.

✓ A receiver may send an acknowledgement when a timer expires.

A receiver may also decide to acknowledge only end packets at a time.

If the receiver does not acknowledge every packet it receives it may slow down the sender & help prevent congestion.

d) Discarding policy

✓ A router may discard less sensitive packets when congestion is

likely to happen.

Such a discarding policy may prevent congestion & at the same time not harm the integrity of the transmission.

e) Admission policy

It is a quality of servic mechanism can also prevent congestion in virtual circuit networks.

Switches in a flow first check the resource requirement of a flow before admitting it to the n/w.

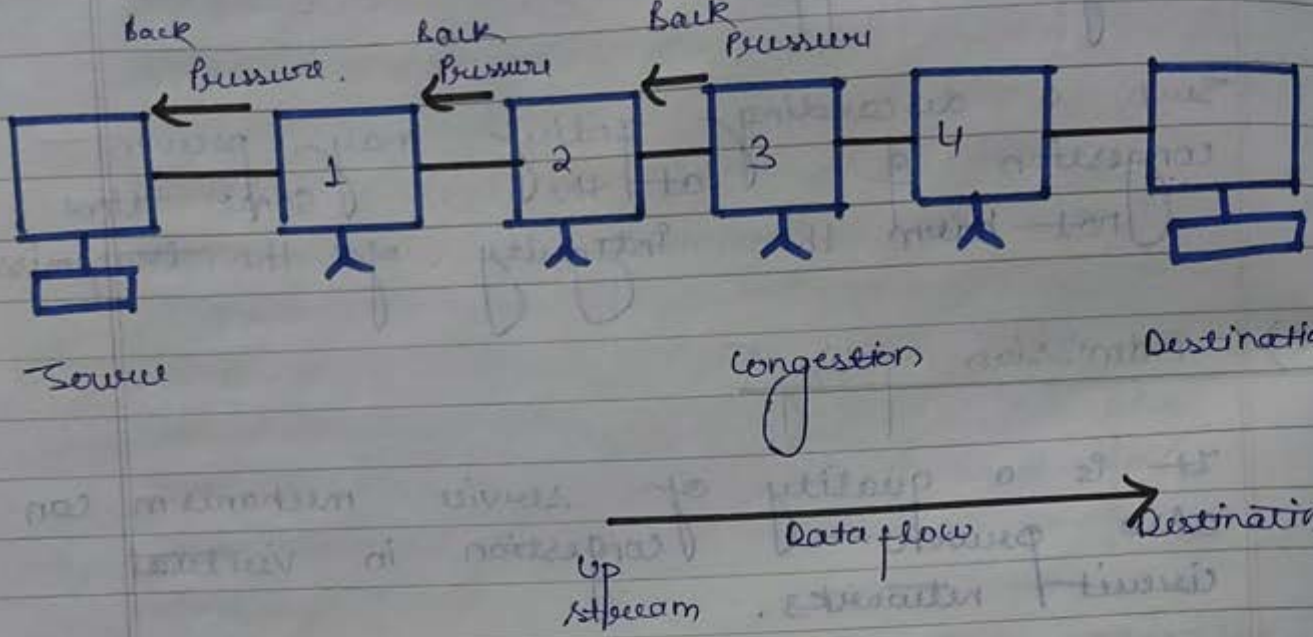
* Closcloop

It try to remove the congestion after it happing.

a) Back pressure.

It is a node to node congestion control that starts with a node & propagates in the opposite direction of data flow.

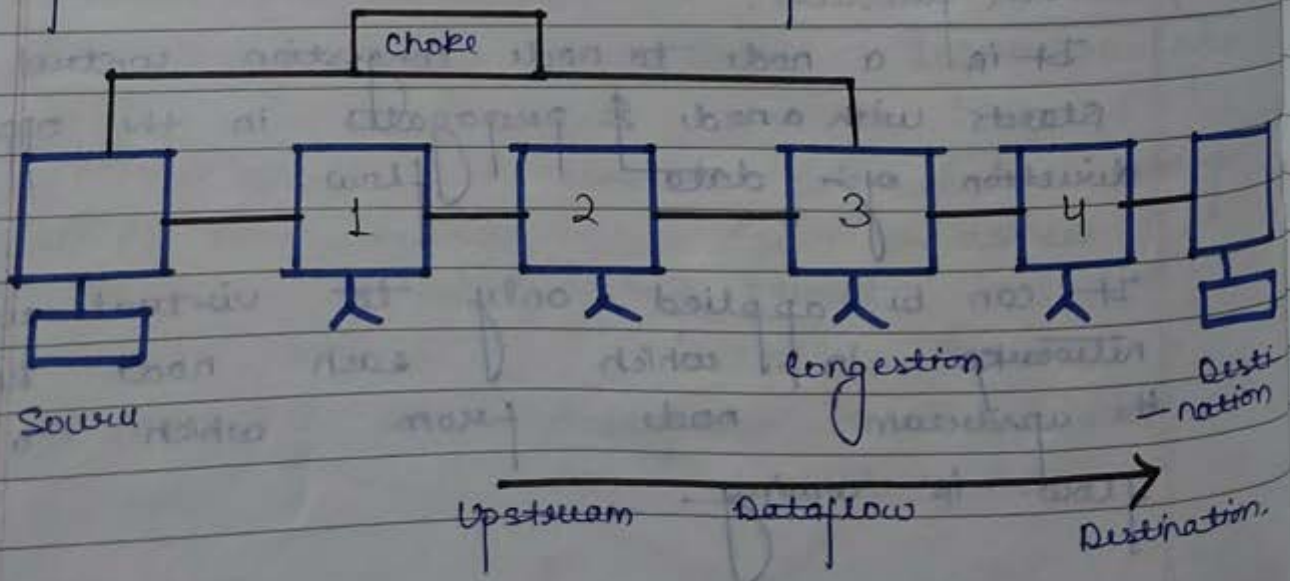
It can be applied only to virtual circuit networks in which each node knows the upstream node from which a data flow is coming.



b) Choke packet

In this congested router or node sends a special type of packet called choke packet, to the source to inform it about the congestion.

In this congested node sends a warning directly to the source station not its upstream node as in back pressure method.



Implicit signaling

In this there is no communication b/w the congested node or node and the source.

The source guesses that there is congestion somewhere in the network when it does not receive any acknowledgement. Therefore the delay in receiving an acknowledgement is interpreted as congestion in the network.

On sensing this congestion the source slows down.

This type of congestion control policy is used by TCP.

Explicit Signaling.

In this method the congested nodes explicitly send a signal to the source or destination to inform about the congestion

It is different from choke packet in which a separate packet is used for this purpose whereas in this method

the signal is included in the packets that carry data.

Explicit signaling can occur in either the forward direction or backward direction.

IP Version 4. Address.

(It is a 32-bit address that uniquely and universally defines the connection of a device)

Ex.
A computer or a router to the Internet.
IP version 4 addresses are unique as each address defines one and only one connection to the Internet.

Two devices on the Internet can never have the same address at the same time

IP version 4 addressing & its inception used the concepts of classes.

This architecture is called classful addressing.

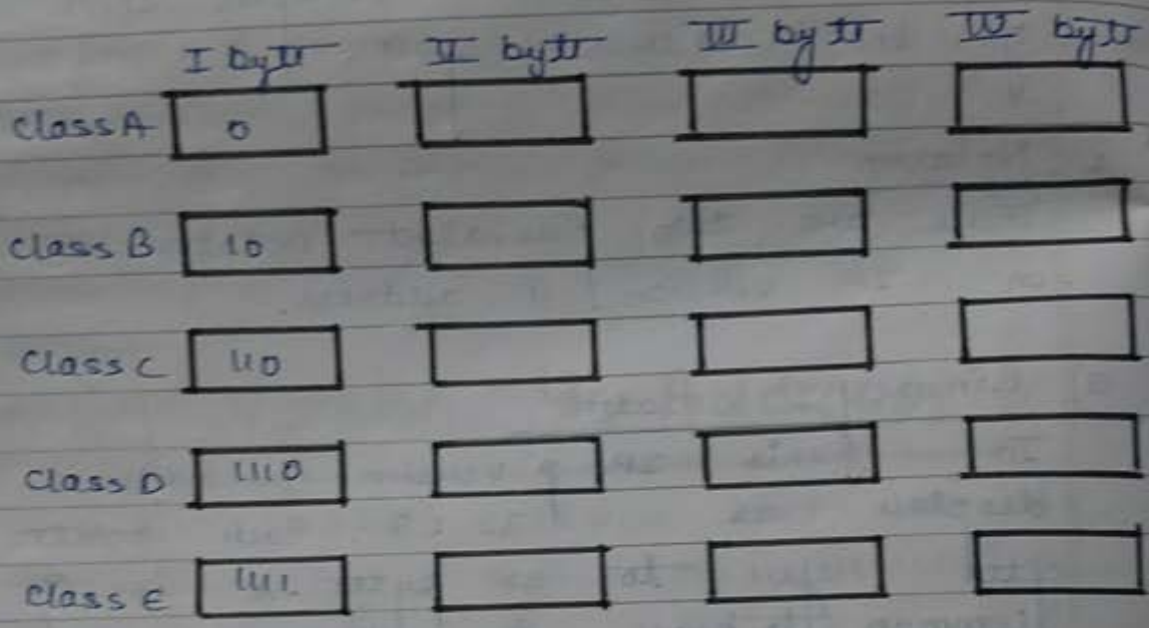
In classful addressing the address space is divided into 5 classes A, B, C, D & E. Each class occupies some part of the address space.

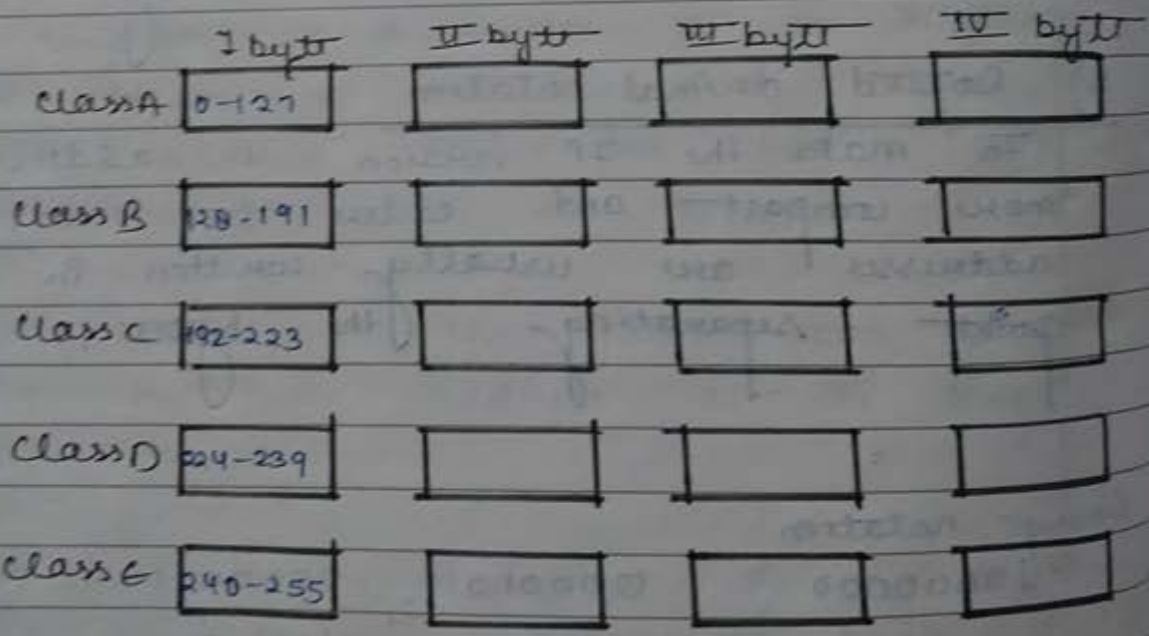
* Notation.
There are two prevalent notation to show an IP version 4 address.

a) Binary notation
In this IP version 4 address is displace as 32-bit. Each octate is often refer to as bytes so it is comman to hear an IP version 4 address as 32-bit address or 4 byte address.

b) Dotted decimal notation
To make the IP version 4 address more compact and easier to read, ethernet addresses are usually written in decimal point separating the bytes.

Binary notation
10000000 00001011 00000011 00011111
→ 128 . 11 . 3 . 31
Dotted decimal notation


I byte
II byte
III byte
IV byte
Class A
0
Class B
10
Class C
110
Class D
1110
Class E
1111


I byte
II byte
III byte
IV byte
Class A
0-127
Class B
128-191
Class C
192-223
Class D
224-239
Class E
240-255

Format of IP Version -4.

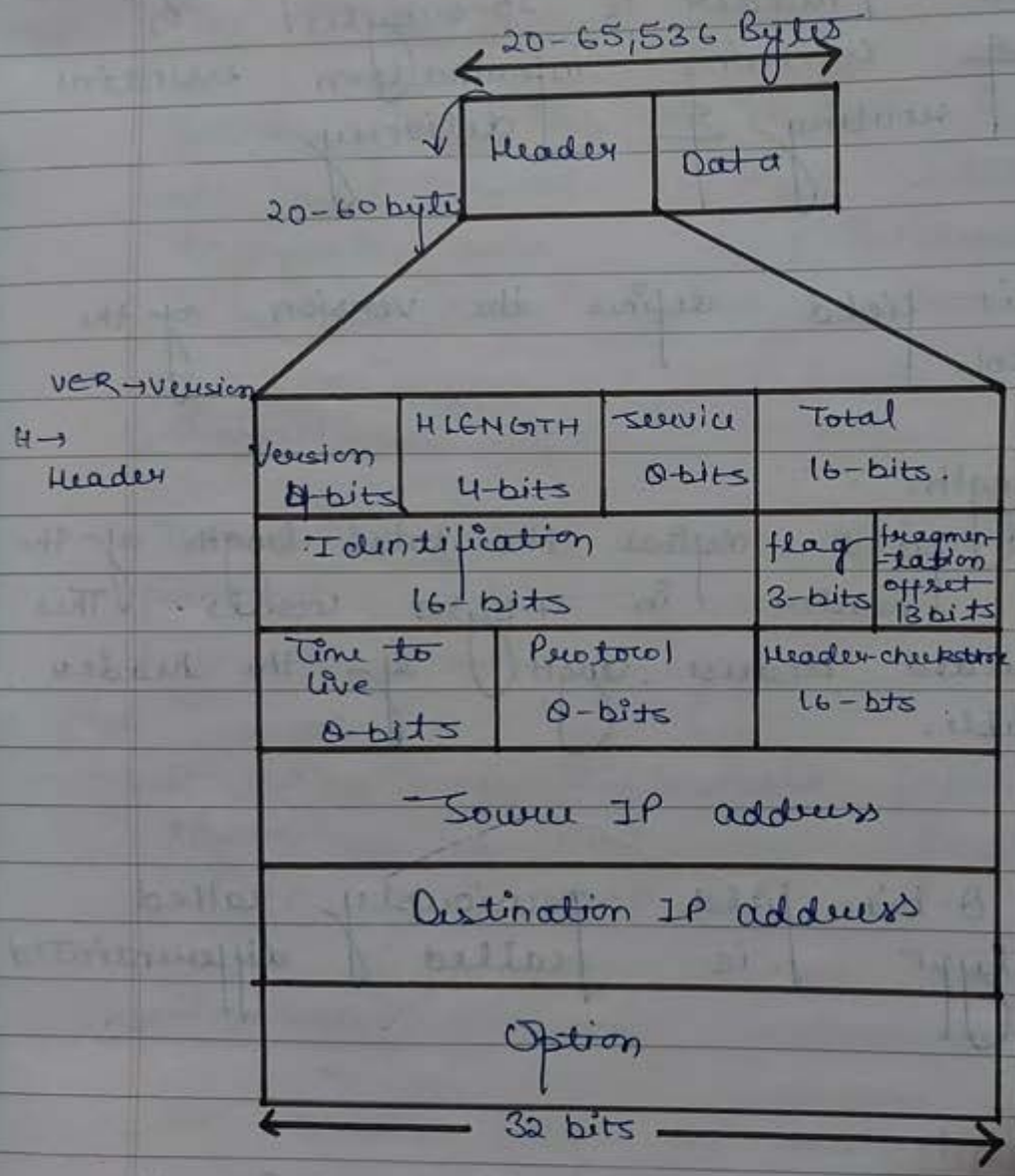


Fig: IP Version 4 datagram format

IP Version 4 is the delivery mechanism of TCP/IP protocol. It is an unliable and connectionless datagram protocol

Packets in IP-Version 4 are called datagram. A datagram is a variable length packet consisting of two parts header & data. The header is 20-60 bytes in length & contains information essential to routing & delivery.

Version

This 4-bit field defines the version of the IP protocol.

Header length.

This 4-bit field defines the total length of the datagram header in 4-byte words. This field is needed because length of the header is variable.

Services.

This is 8-bit field previously called servic type is called differentiated services.

Total length.

This is a 16-bit field that defines the total length of the IP version 4 datagram in bytes.

Length of data = Total length - header length.

Identification, flag, fragmentation offset

These fields are used in fragmentation.

Time to live.

A datagram has a limited life time during its travel through internet. The datagram was discarded when the value becomes zero.

Protocol.

This 8-bit field defines the higher level protocol that uses the services of the IP version 4-layer.

It can encapsulate data from several higher level protocol as TCP, UDP, ICMP etc.

Checksum.

It covers only the header not the data.

Source address

This field defines the address of the source.

It must remain unchange during its life time.

Destination address.

It defines the address of the destination.

option.

It can be used for n/w testing & debugging.

IP- Version 6

IP version 4 has some deficiency that make it unsuitable for the fast growing internet.

1. The internet must accomodate real time audio and vedio transmission, which is not provided in IP version 4 design.
2. The internet must accomodate encryption & authentication of data for some application which is not provided by IP version 4.

To overcome these defiviencies IP version

6 was proposed & is now a standard

3. The format & the length of the IP address were changed along with packet format.

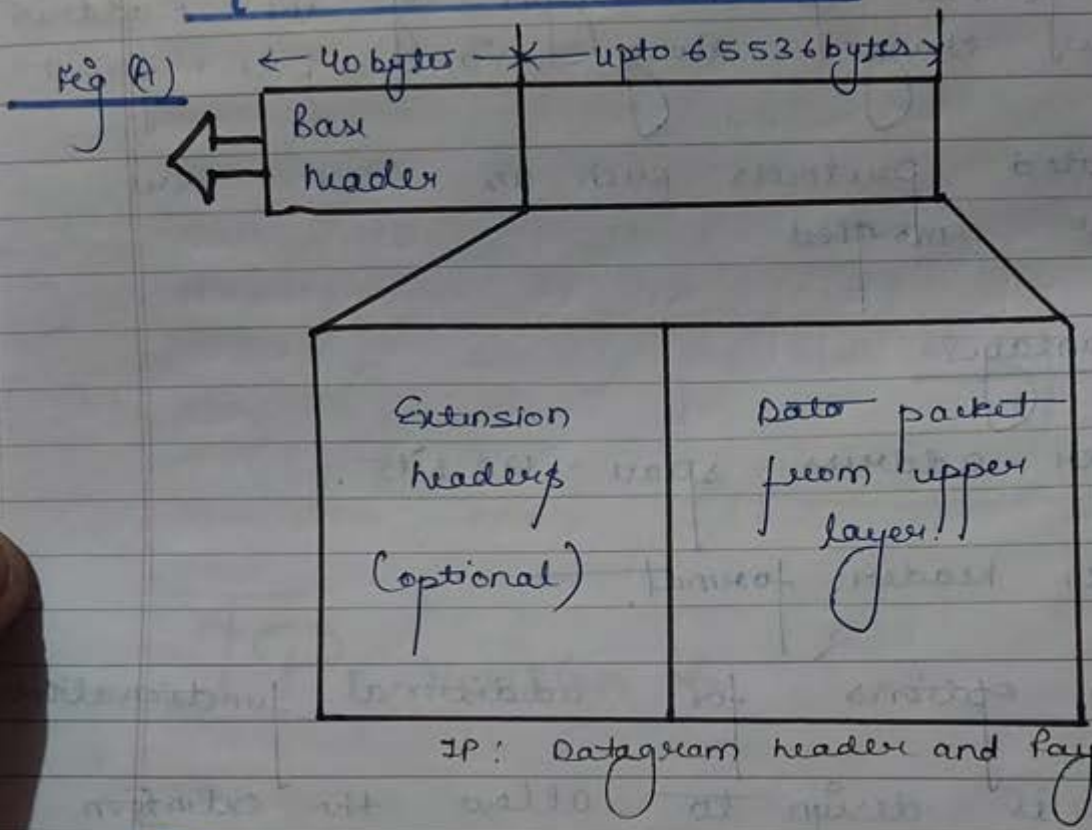
4. Related protocols such as ICMP were also modified.

Advantages

1. Larger address space : 128 bits.
2. Better header format.
3. New options for additional functionalities.
4. It is design to allow the extention of the protocol required by new technologies or application.
5. In IP version the type of service field have been removed but a mechanism called flow label has been added to enable the source to request special handling of packet.
6. The encryption & authentication options in IP version 6 provide confidentiality & integrity of the packets.

PACKET FORMAT

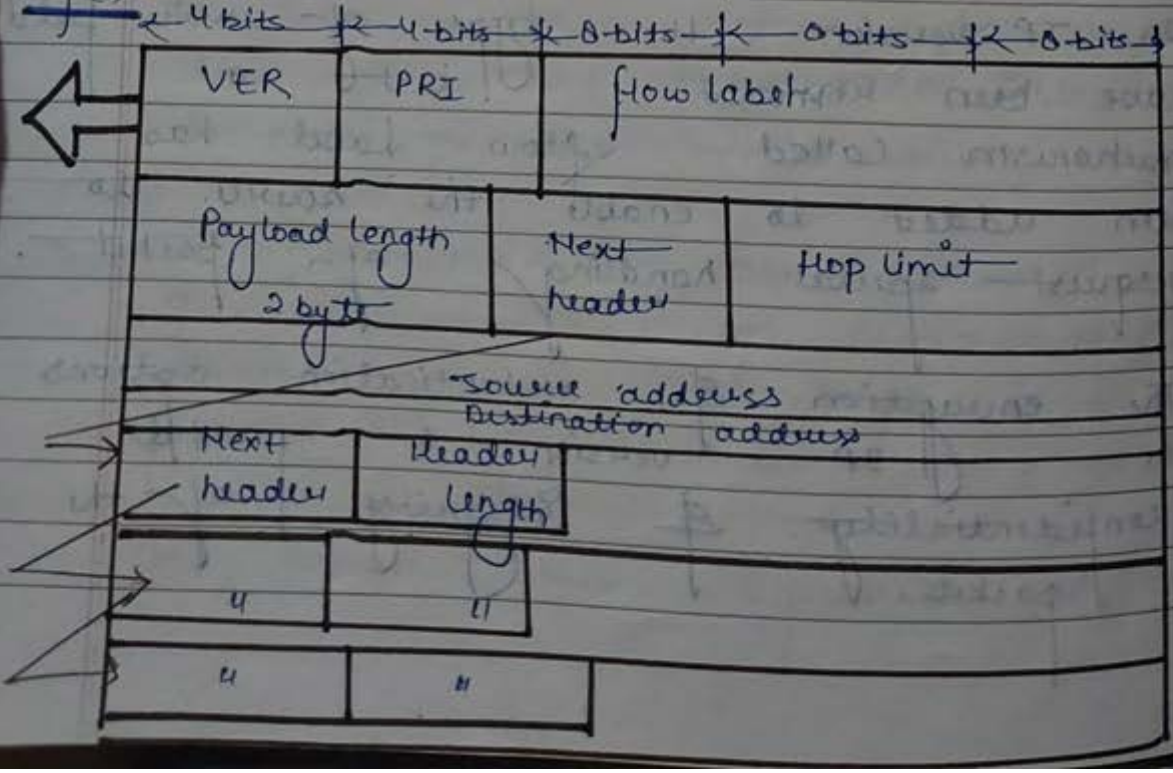
Fig (A)



IP : Datagram header and Payload.

DATAGRAM FORMAT

Fig (B)



Packet format

Each packet is composed of a mandatory based address followed by the payload which consist of two parts - optional extension header.

Data from an upper layer

Datagram format

Datagram format is shown in figure (B)

Version ~~Fig (A)~~ VER

It defines the version of IP

Priority (PRI)

It defines the priority of packet w.r.to traffic congestion

Flow label designed

It is ~~defined to~~ provide special handling for a particular flow of data

Payload length

It defines the length of the IP datagram excluding the base header

Next header.

It defines the header that follows the base header in the datagram. This field in version 4 called protocol.

HOP limit

This field serves the same purpose as the (TTL) Time to live field in IP version 4.

Source address
Destination address } Same as IP version-4

IP Version 6 addresses

* **Structure**

An IP version 6 address consist of 16 byte (octates) it is 128 bits long.

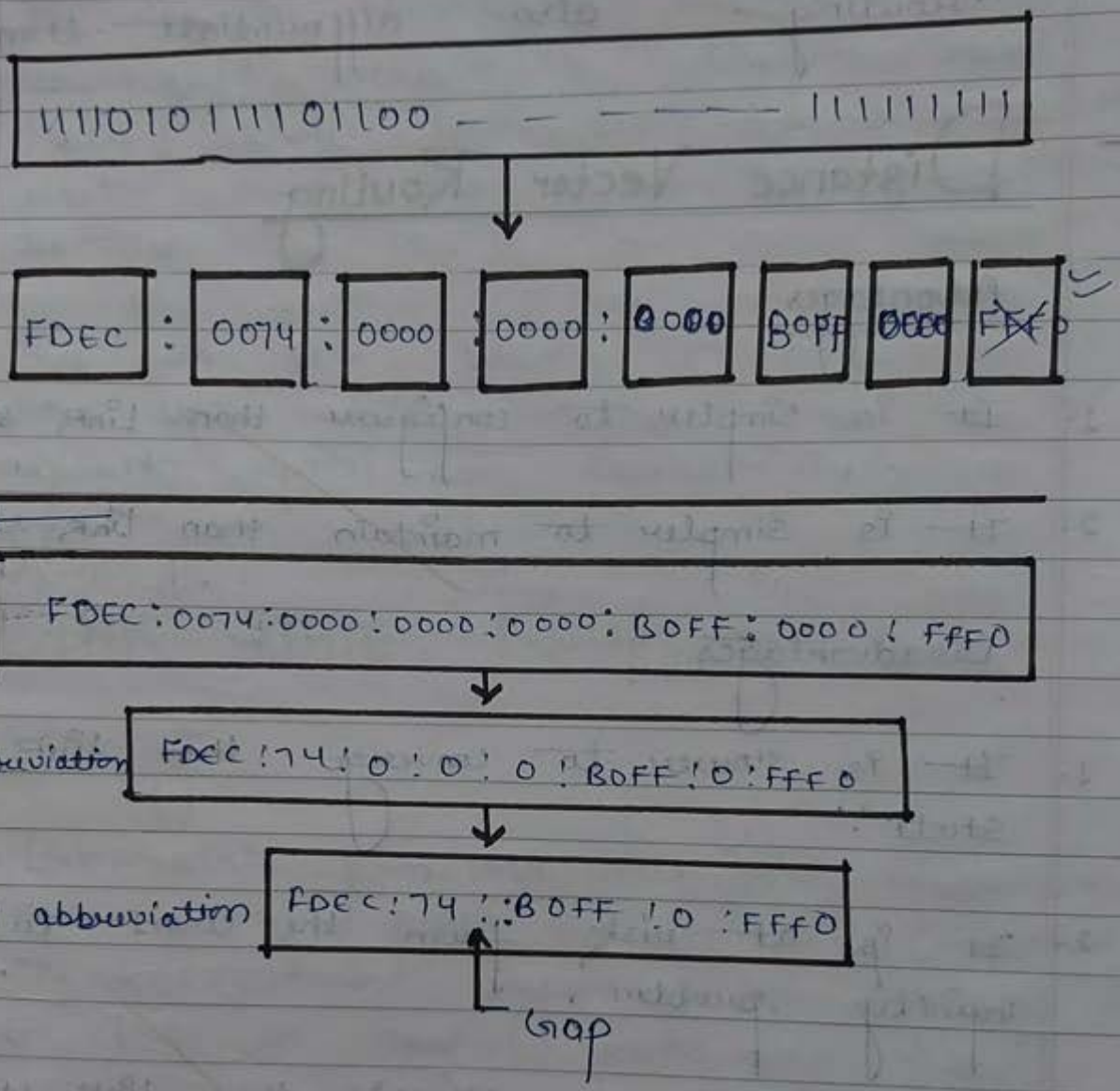
* **Hexadecimal colon notation**

To make more readable IP version 6 specifies hexadecimal colon notation.

In this notation 128 bits divided into 8 sections each 2 bytes in length. 2byte in hexadecimal notation requires 4 hexadecimal digits.

UNIT-3

Abbreviation



ASSIGNMENT-3

Ques 1. What are the advantages and disadvantages of distance vector and link state routing also differentiate them.

Ans.

Distance Vector Routing.

Advantages

1. It is simpler to configure than Link state.
2. It is simpler to maintain than link state.

Disadvantages

1. It is slower to converge than Link state.
2. It is at risk from the count-to-infinity problem.
3. It creates more traffic than link state since a hop count change must be propagated to all routers and processed on each router. Hop count updates takes place on a periodic basis, even if there are no changes in the network topology, so bandwidth wasting.

broadcasts still occur.

4. For larger networks distance vector routing results in larger routing tables than link state since each router must know about all other routers.

5. This can also lead to congestion on WAN links. RIP announces host or default routes by default.

LINK STATE ROUTING

Advantages

1. Link-state protocols use cost metrics to choose paths through the network. The cost metric reflects the capacity of the links on those paths.

2. Link-state protocols use triggered updates and LSA floods to immediately report changes in the network topology to all routers in the network. This leads to fast convergence times.

Each router has a complete and synchronized picture of the network.

Therefore, it is very difficult for routing loops to occur.

3. Routers use the latest information to make the best routing decisions.

4. The link state database sizes can be minimized with careful network design.

5. Link state protocol supports CIDR and VLSM.

Disadvantages

1. They require more memory and processor power than distance vector protocols. This makes it expensive to use for organizations with small budgets and legacy hardware.

2. They require strict hierarchical network design, so that a network can be broken into smaller areas to reduce the size of the topology tables.

They require an administrator who understand -s the protocol well.

They flood the network with LSAs during the initial discovery process. This process can significantly decrease the capability of the network to transport data. It can noticeably degrade the network performance.

Difference b/w distance vector and link state routing.

Basis for comparison	Distance Vector routing	Link-state routing
* Algorithm	Bellman Ford	Dijkstra
* Network View	Topology information	Complete information
* Best path Calculation	Based on the least number of hops	Based on the cost

* Updates	Full routing table	Link state updates
* Updates frequency	Periodic updates	Triggered updates
* CPU and memory	Low utilisation	Intensive
* Simplicity	High simplicity	Requires a trained network administrator.
* Convergence time	Moderate	Fast
* Updates	On broadcast	On multicast
Hierarchical structure	No	Yes.
Intermediate nodes	No	Yes

Ques 2. What are the different congestion control algorithms.

Ans. **Congestion Control algorithms.**

1. Leaky Bucket algorithm.

Let us consider an example to understand

Imagine a bucket with a small hole in the bottom. No matter at what rate water enters the bucket, the outflow is at constant rate. When the bucket is full with water additional water entering spills over the sides and is lost.

Similarly, each network interface contains a leaky bucket and the following steps are involved in leaky bucket algorithm:

a) When host wants to send packet, packet is thrown into the bucket.

b) The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.

c) Bursty traffic is converted to a uniform traffic by a leaky bucket.

d) In practice the bucket is a finite queue that outputs at a finite rate.

2. Token bucket algorithm.

Need of token bucket algorithm -

The leaky bucket algorithm enforces output pattern at the average rate, no matter how matter how bursty the traffic is. So in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

Steps of this algorithm can be described as follows:

a) In regular intervals tokens are thrown into the bucket.f

b) The bucket has a maximum capacity.f

c) If there is a ready packet, a token is removed from the bucket and the packet is send.

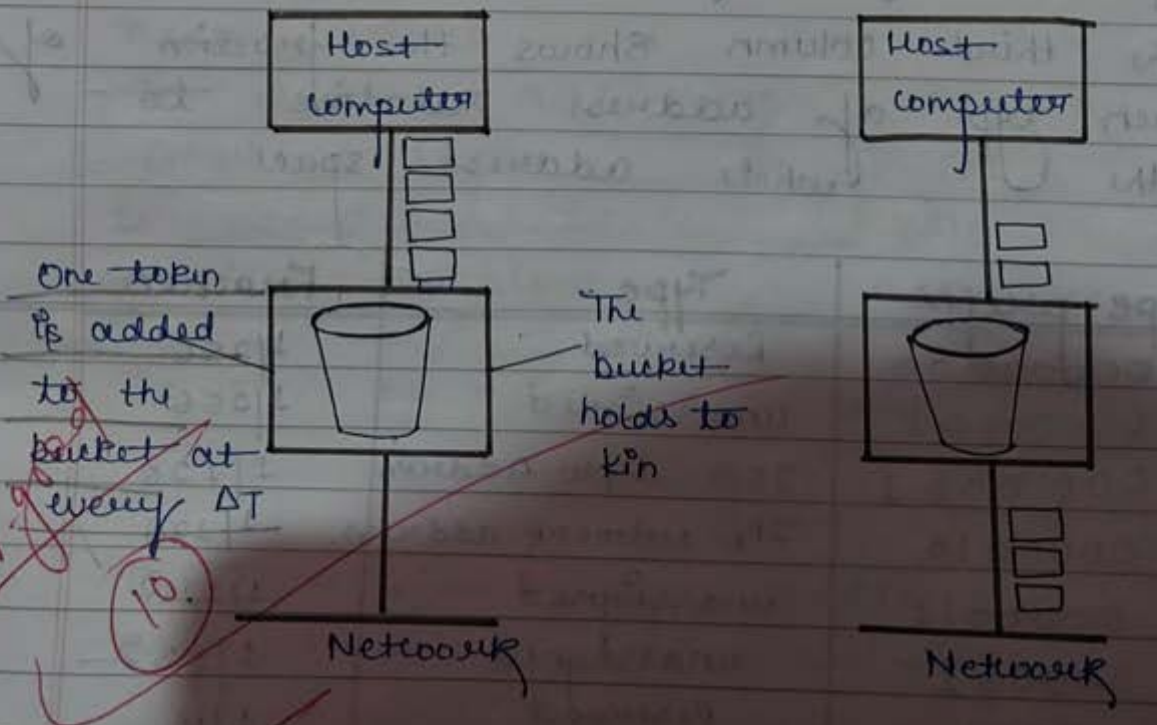
d) If there is no token in the bucket, the packet cannot be send.

Let's understand with an example,

In figure (A) we see a bucket holding three tokens, with five packets waiting to be transmitted. For a packet to be transmitted, it must capture and destroy one token.

In figure (B) we see that three of the five packets have gotten through, but the other two are stuck waiting for more tokens to be generated.

Let's understand with an example,



a) Before

b) After

ADDRESS SPACE

IP version 6 has much larger address space that 2^{128} addresses are available. The designers of IP version 6 divided the address into several categories. A few left most bits called the type prefix in each address define its category.

The type prefix is variable in length but it is design such that no code is identical to the first part of any other code.

The third column shows the fraction of each type of address relative to the whole address space.

Type prefix	Type	Fraction
00000000	Reserved	1/256
00000001	unassigned	1/256
0000 001	ISO NW to Address	1/128
0000010	IPx Network address	1/128
0000011	unassigned	1/128
0001	unassigned	1/32
001	Reserved	1/16
010	Reserved	1/8
	Private based Unicast address	1/8

It includes → multicast addresses
unicast addresses
local addresses
reserved addresses
Anycast addresses

CLASSLESS ADDRESSING

It was developed in 1993 to overcome the address depletion and give more organizations access to the Internet. In this scheme there are no classes but the addresses are still granted in blocks.

Address blocks.

In classless addressing when an entity, small or large organization needs to be connected to the Internet. It is granted a block of addresses.

The size of the block varies based on the nature and size of the entity.

This type of entity handled by internet assigned number authority.

Rules.

Addresses should be contiguous

Number of addresses in a block must be in power of 2.

First address of every block must be evenly divisible with size of blocks

Notation

$x.y.z.w/n$ — mask; number of bits represent blocks n/w.

Unicast, Multicast, Broadcast Addresses.

A source address is always a unicast address. The frame come from only one station, destination address however may be unicast, multicast and broadcast.

Unicast = 0 Multicast = 1

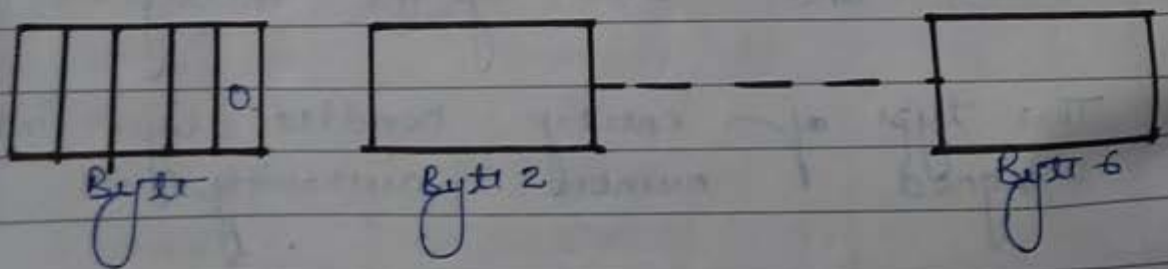


Fig.: Unicast and multicast addresses

The above figure shows how to distinguish a unicast addresses from multicast address. If the least significant of the first byte in a destination address is zero, the address is called unicast otherwise multicast.

The relationship b/w the sender & receiver is 1 to 1.

A multicast destination address defines the group of addresses & the relationship b/w the sender and the receiver is 1 to many.

The broadcast address is a special case of multicast addresses.

The recipient of all the station is on the LAN.

CLASSES AND BLOCKS

Class	No. of blocks	Block-size	App.ⁿ
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved.

One problem with classful addressing is that each class is divided into fixed number of blocks. Class A addresses were designed for large organizations with a large no. of routers or host attached. Class B address were designed for mid-size addresses with tens of thousand of attached host or routers.

Class C addresses were designed for small organizations.

Subneting in IP

Dividing a large network into multiple small network is called subnetting.

A subnetwork or subnet is a logical subdivision of an IP network the practice of dividing a network into two or more networks is called subnetting.

Computers that bllong to a subnet are addressed with identical most

significant bit grouped in there IP addresses.

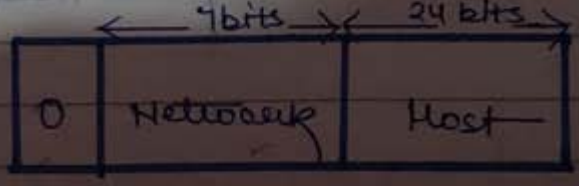
Each IP class is equiped with its own default subnet mask which bounds that IP class to have prefixed number of n/w and prefixed number of host per network.

Classful IP addressing doesnot provide any flexibility of having less number of host per n/w or more n/w per IP class.

CIDR { Classless interdomain routing }
Provides flexibility of borrowing bits of host part of IP address & using them as network in network called subnet.

By using subnetting one single class A IP address can be used to hack smaller sub networks which provides better n/w management capabilities.

Class A

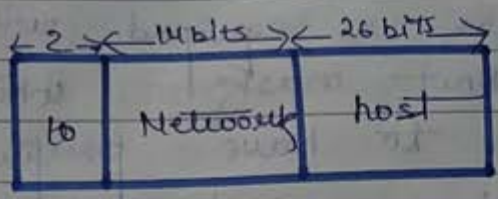


CIDR = 18

Default mask = 255.0.0.0

No. of network = 27, host = $2^{24}-2$

Class B



CIDR = 16

Default mask = 255.255.0.0

No. of network = 2^{14}

Host = $2^{16}-2$

Class C

CIDR = 24

Default mask = 255.255.255.0

No. of network = 2^{21}

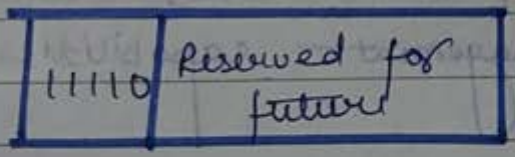
host = $2^{8}-2$

Class D

~~Default mask =~~

~~No. of network =~~

Class E



~~No. of network =~~

~~Default mask =~~

IP Addresses

Every host and router on the Internet has unique IP address.

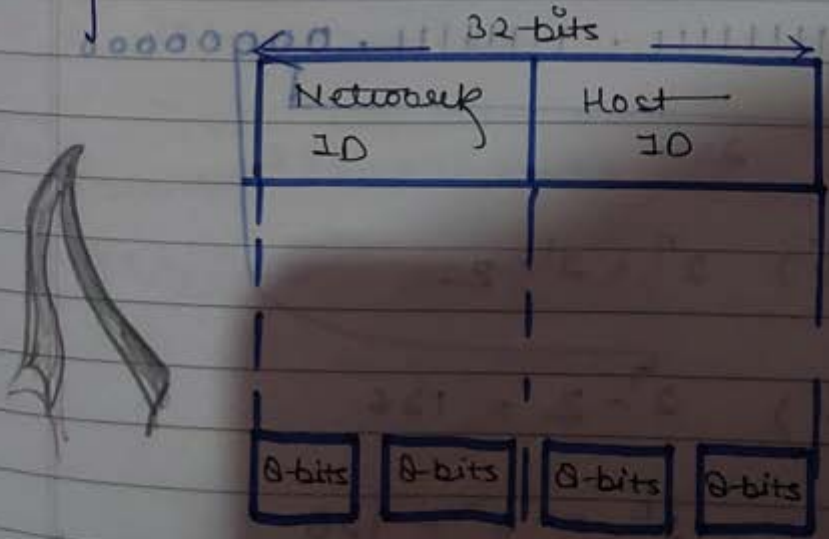
All the IP addresses are 32-bit long they are used in source and destination address.

It consist of two fields network ID and host ID.

IP address format

The 32-bit IP address is grouped into group of 8-bits separated by dots.

Each 8-bit group is then converted into its equivalent binary number thus octate can take value from 0-255.



IP Address format

10010001.00001010.00100010.00000011 is denoted in dotted decimal as 145.10.34.3

Dotted Decimal Notation

Ques 192.168.10.0/24 find no. of n/w, host & IP address.

Solution CIDR = 24, 25'

Class C

Host → 0

N/w → 1

255.255.255.0

11111111.11111111.11111111.00000000

24-bits 8 bits

(i) $= 2^n$ → borrow bit

$= 2^0 = 1$

(ii) $2^7 - 2 = 126$ $2^8 - 2 = 254$

2^{8-2}

(iii) 2^n → no. of host bit

$2^8 = 256$ IP address

for 25.

11111111.11111111.11111111.00000000

25-

(i) $2^n = 2^1 = 2$

(ii) $2^7 - 2 = 126$

(iii) $2^n = 2^7 = 128$

IP address

Network divide

1 → 0 – 126
1 – 125 ✓
2 - 127 - 255
128 - 254 ✓

Ques. IP address = 201. 20. 30. 40

Calculate

(i) N/w Id
(ii) 4th host Id
(iii) last host Id
(iv) Broadcast Id.

(i) Default Mask

201. 20. 30. 40 — binary
AND
255. 255. 255. 0 (+)

201.20.30.0 ✓

(ii) 201. 20.30.4

(iii) 201.20.30.254

(iv) Direct 255. 255. 255. 255 broadcast

limited 201.20.30.255

Ques. IP address 200.10.20.40/20
find.

(i) No. of host

(ii) Mask value.

(iii) Network Id | Block Id.

Sol)

255.255.255.0

11111111.11111111.11111111.00000000

(i) $2^7 = 2^4 \Leftarrow 16 = 14$

(ii) 255.255.255.0

11111111.11111111.11111111.00000000

$2^8 2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$

(iii) 255.255.255.240

$$\begin{bmatrix} 255.255.255.240 \\ 200.10.20.40 \end{bmatrix}$$ AND operator

200.10.20.00100000 (32)

2	240	0
2	120	0
2	60	0
2	30	0
2	15	1
2	7	1
2	3	1
	1	1

11110000 – 240
00101000 – 40
00100000 (32)

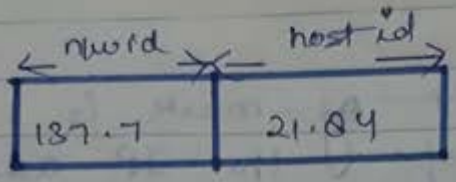
Ques For the address 24.46.0.95 identify the type of network and find the network address

net id	host id
24	46.0.95

(i) Class A

(ii) 24.0.0.0 (255.0.0.0)

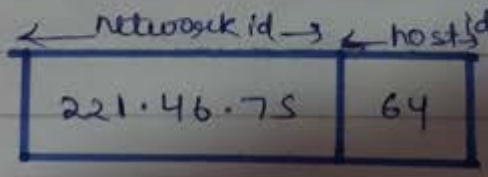
Ques 2 for the address 137.7.21.04 find type of network and network address



(i) Class B

(iii) 137.7.0.0

Ques 3. For the IP address 221.46.75.64 find the class of the network.



(i) class C

(ii) 221.46.75.0 (Nlw address)

16 +
32
64 ~
118
10

Address Mask

An address mask determines which portion of an IP address identifies the network and which portion identifies the host.

If a given bit of mask is 1 the corresponding bit of the IP address is in network portion of the address and if a given bit of the mask is zero the corresponding bit of the IP address is in the host portion.

14/03/19

UNIT-4

TRANSPORT LAYER

Processes Node2Node! Data Link Layer / MAC address

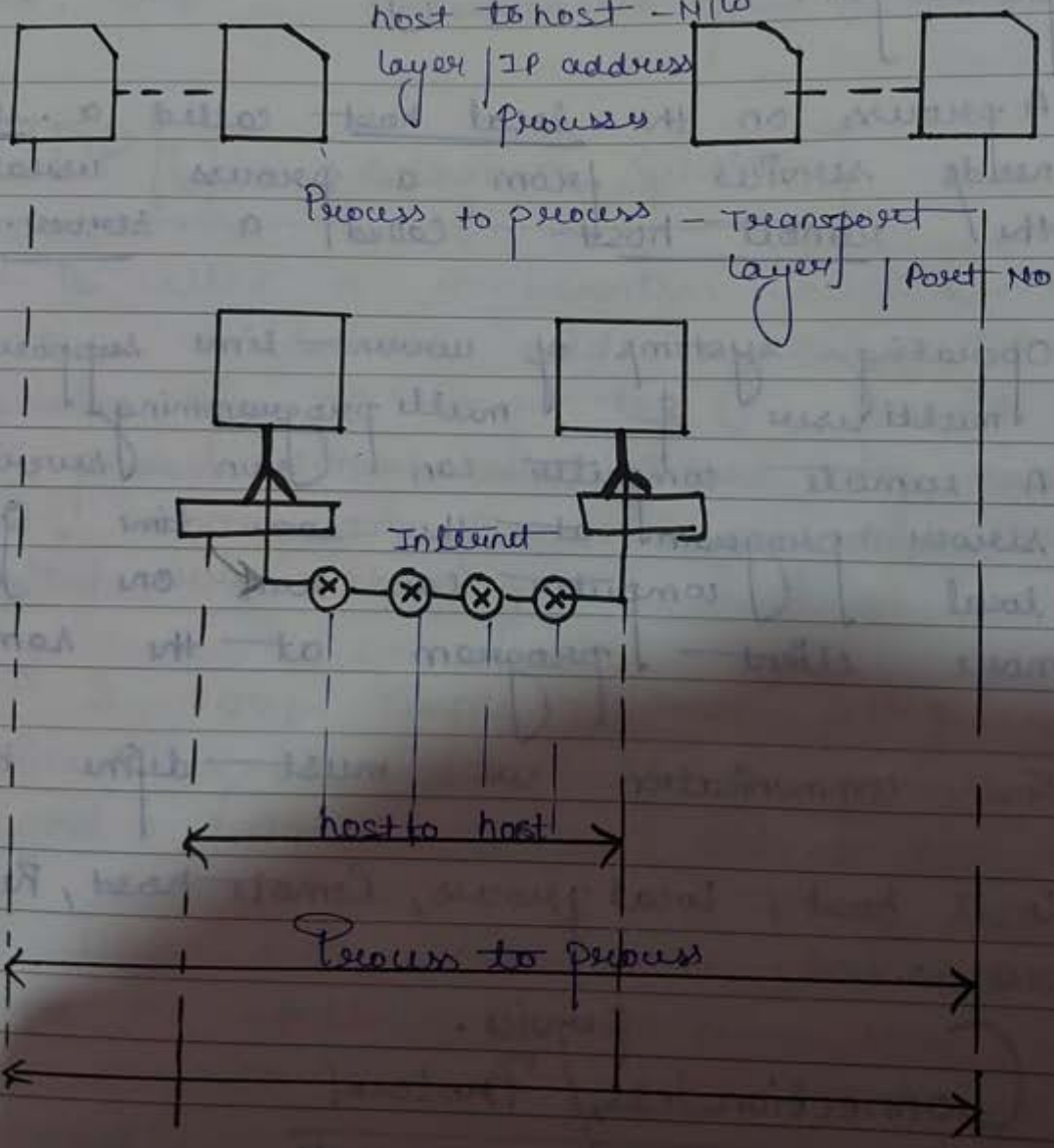


Fig: Types of data delivery

The transport layer is responsible for process to process delivery, that delivery of packets, part of a message from one process to another process.
Two processes communicate in a client server relation. Although there are several ways to achieve process to process communication. The most common one is through the client server paradigm.

A process on the local host called a client, needs services from a process usually on the remote host called a server.

Operating systems of current time supports both multiuser & multiprogramming environment. A remote computer can run several server program at the same time just as local computer can run one or more client program at the same time.

For communication we must define the following.

Local host, Local process, Remote host, Remote process.

Connectionless service. Protocol

In this service the packets are send

from one party to another with no need for connection establishment or connection release.

The packets are not numbered they may be delayed or lost or may arise out of sequence, There is no acknowledgement either.

Ex. UDP is connectionless protocol.

UDP {User datagram protocol}

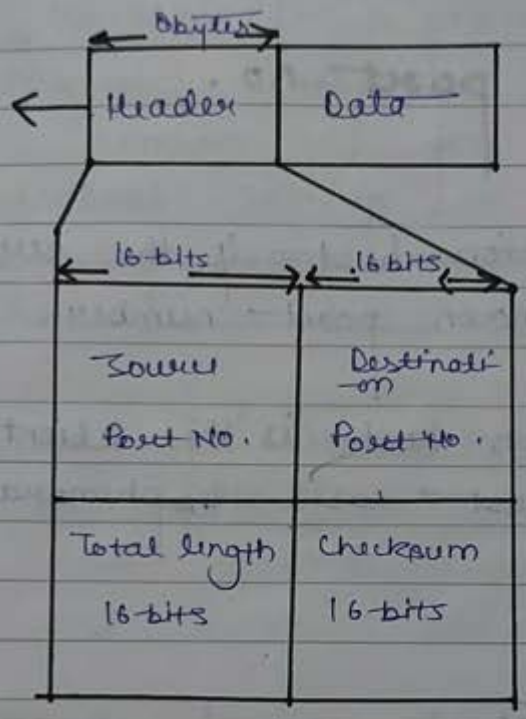
It is called a connectionless unreliable transport protocol. It does not add anything to the services of IP except to provide process to process communication instead of host to host communication. Also it perforums very limited error checking.

UDP is very simple protocol using a minimum of overhead. If a process wants to send a small message and does not care much about reliability. It can use UDP. UDP takes much less interaction between the sender and receiver than using TCP or SCTP {stream control transmission protocol}.

* Well Known ports for UDP

Port	Protocol	Description
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram i.e, received.
11	Users	Active Users.
13	Day time	Return the data and the time.
17	Quote	Return a quote of the day
19	Charger	Returns a string of characters.
53	Nameserver	Domain name service
67	BOOTPs	Server port to download. bootstrap Information
68	BOOTPc	Client port to download bootstrap information.
69	TFTP	Trivial file transfer protocall
111	RPC	Remote procedure call
123	NTP	Network Time protocol
161	SNMP	Simple network management protocol
162	SNMP	Simple n/w management protocol (Trap)

User Datagram Format



UDP packets called user datagram have a fixed size header of 8 bytes.

Souce Port number

This is the port number used by the process running on the source host. If the source host is the client the source host in most cases is an ephemeral. Port number request by the process and choosin by the UDP software running on the source host. If the source host is

the server the port no. is well known port number.

Destination port no.

If the destination host is the server the port no. is well known port number.

If the destination host is the client the port number in most cases ephemeral port no.

Total length

Total length = header + data

The need of total length is to be because a UDP is stored in an IP datagram.

UDP length = IP length − IP header's length.

Checksum

This field is used to detect errors over the entire datagram.

Uses of UDP

It is suitable for a process that requiring simple request response communication with little concern for flow and error control. It is suitable for multi-casting capability which is embedded in UDP software but not in TCP.

It is used for some route updating protocol such as routing information protocol.

Transport layer design issues

The transport layer is a conceptual division of methods in the layered architecture of protocols in the network stack, in the Internet internet protocol suit and OSI model.

The best known transport protocol of TCP/IP is the transmission control protocol. It is used for connection oriented transmissions.

Transport layer is responsible for following issues:

1. Transport delivers the message process to process running on two different host thus it has to perform no. of functions to ensure the accurate delivery of messages.

2. Accepting message segments from the application layer and to divide into packets.

3. End to end delivery of the packets.

4. Combining packets into message segment and at receiver side.

5. Connection management

In other words, transport layer is responsible for two tasks.

Transport and regulate the flow of information from source to destination reliably and accurately.

6. End to End control.

7. Sliding windows.

8. Sequencing numbers.

9. Acknowledgements.

10. Segmentation.

11. Establishing, maintaining and releasing connection.

12. Addressing.

13. Congenstion control.

Three way handshake method / Protocol.

It is a method used in a TCP/IP network to create a connection between local host/client and server.

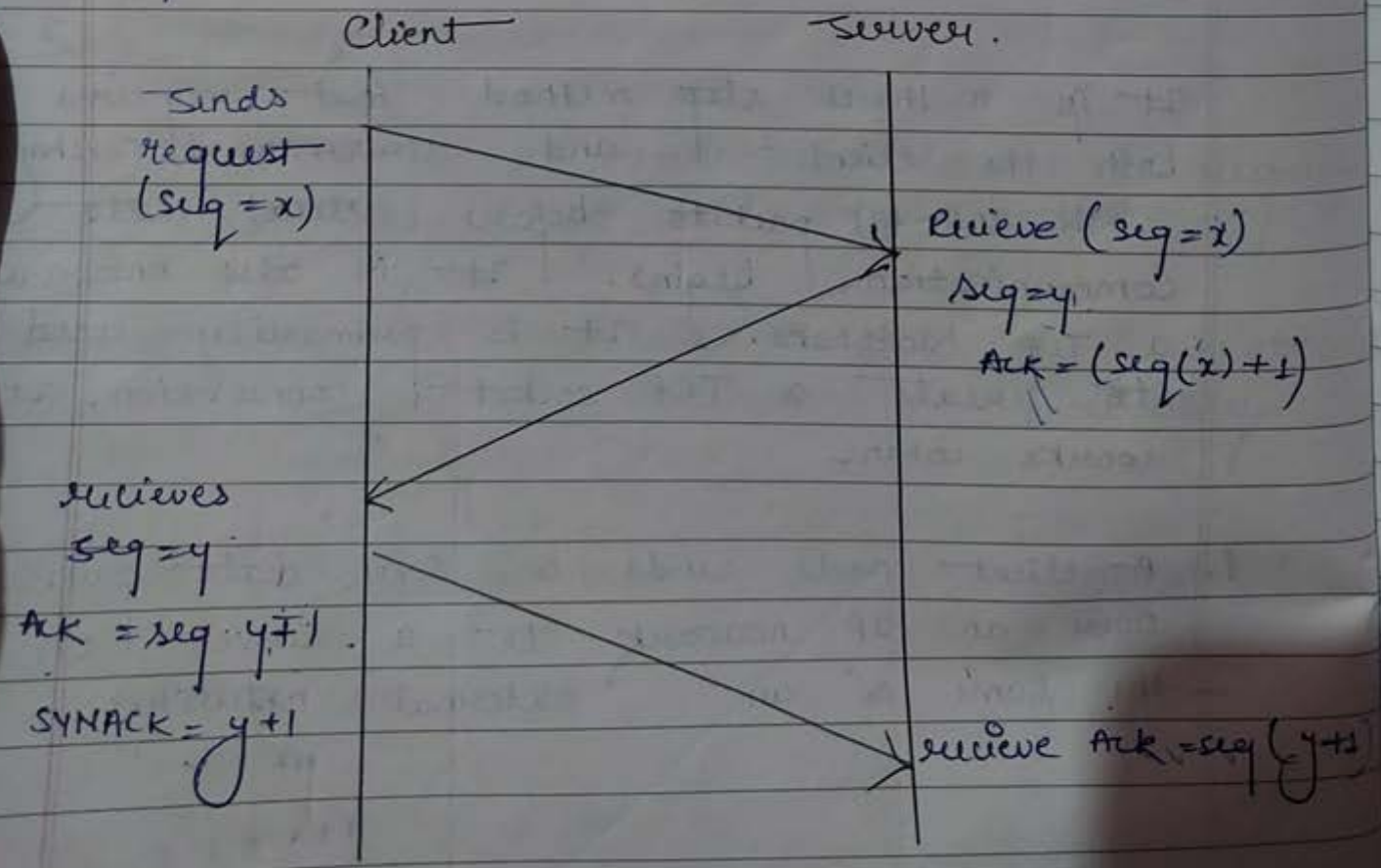
It is a three step method that requires both the client and server to exchange SYN and ACK packets before actual data communication begins. It is also known as a TCP handshake. It is primarily used to create a TCP socket connection. It works when -

1. A client node sends a SYN data packet over an IP network to a server on the same or an external network.

The objective of this packet is to ask if the server is open for new connections.

2. The target server must have open ports that can accept and initiate new connections.
When the server receives the SYN packet from client node it responds and returns a confirmation receive the ACK packet or SYN/ACK packet.

3. The client node receive the SYN/ACK from server & response with an ACK packet.



upon completion of this process the connection is created and the host and the server can communicate. The TCP 3 way handshake in TCP is the method used by TCP setup.

A TCP/IP connection over an Internal protocol based N/W. This 3-way handshake process is also designed so that both ends can initiate and negotiate separate TCP socket connections at the same time.

Event

* Host A sends a TCP Synchronize packet to host B
* Host B receives A's synchronize host b sends synchronize ACK
* Host A sends acknowledge Host B recieves ACK TCP socket connection is established.

Diagram

TCP 3-way handshake (SYN, SYN-ACK, SYN)

Step 1. SYN

In the first step client wants to establish a connection with the server so it sends a segment with SYN (Synchronize sequence number.) which informs server

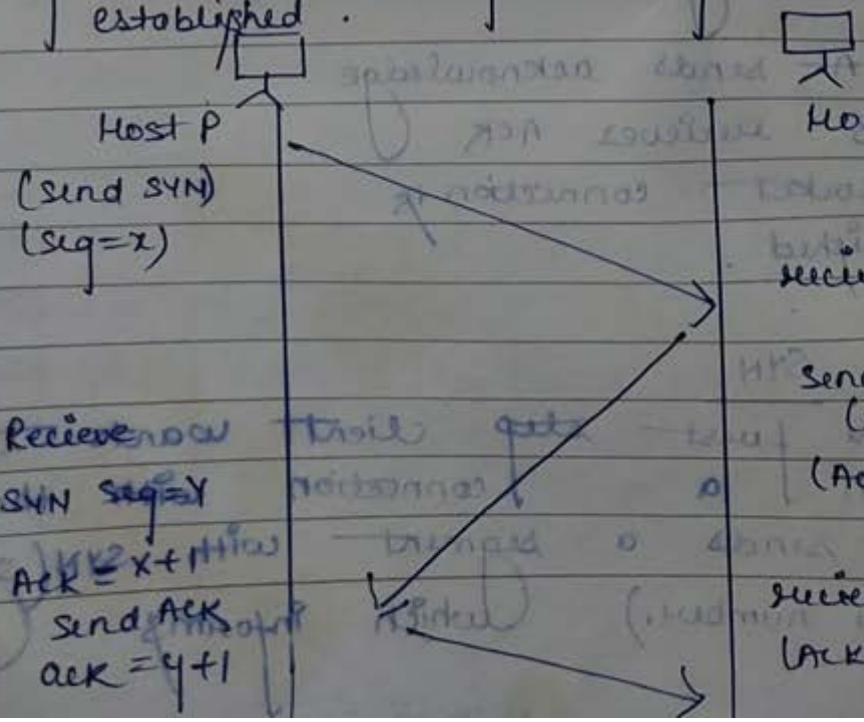
that client is likely to start communicat on and with what sequence it starts segment with.

Step 2. SYN+ACK

Server responds to client request with SYN-ACK signal bits set. Ack signifies the response of segment. It received an SYN signifies with what sequence no. It is likely to start the segment with.

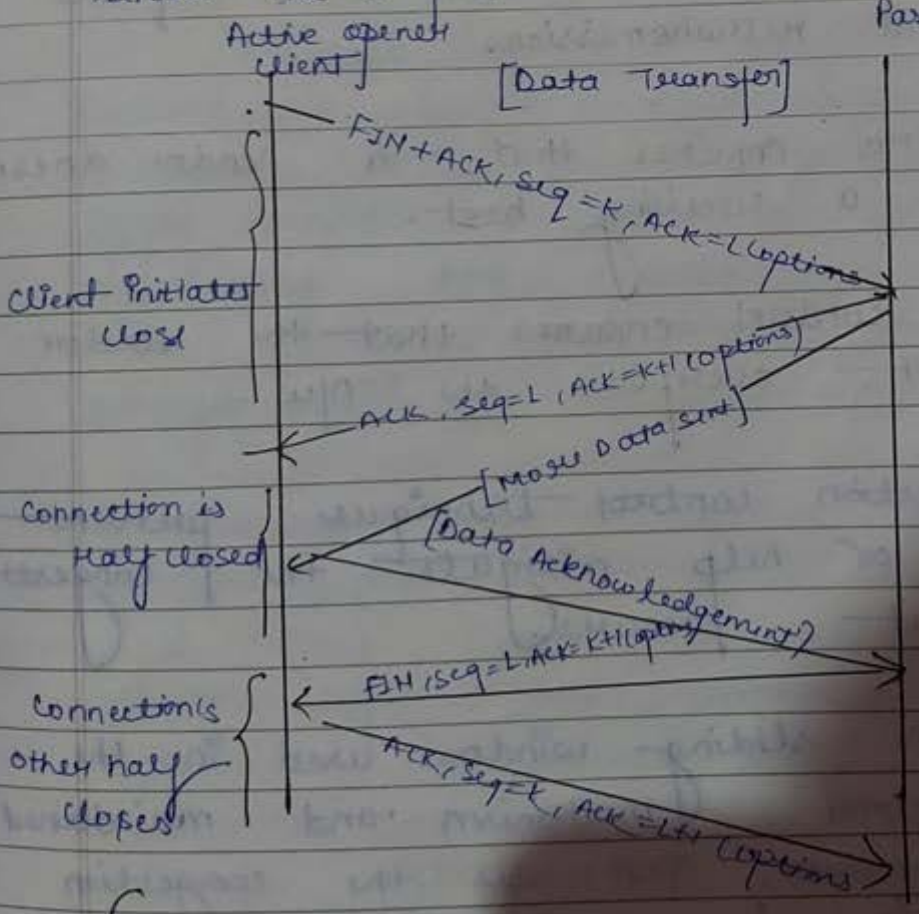
Step 3. ACK

In the final part client acknowledges the response of server and they both establish a reliable connection with which they will start the actual data transfer. Now a full duplex communication is established.



TCP HALF CLOSE

TCP supports a half close operation. Few applications require this capability so it is not common. To use this feature the API must provide a way for this application -on to say; I am done sending data so send a fin to the other end, but I still want to receive data from the other end until it sends me a fin.



Congestion

Network congestion may occure when a sender overflows the network with too many packets. The function of TCP is to control

The transfer of data so that it is reliable. The main TCP features are connection management, flow control and congestion control.

1. Connection management includes connection initialization (three way handshake) and its termination.
2. A reliable point to point transfer between host is achieved with the sequence number and retransmission.
3. Flow control ensures that a sender does not overflow a receiving host.
4. Congestion control ensures that the sender does not overflow the n/w.

TCP congestion control technique prevent congestion or help mitigate the congestion after it occurs.

Unlike the sliding window used in the flow control mechanism and maintained by receiver, TCP uses the congestion window (CWND) maintained by the sender while sliding window (RWND) is present in the TCP header.

CWND is known only to the sender & is not send over the links.
CWND is maintained for each TCP session & represents maximum amount of data that can be send into the N/w without being acknowledged. In fact different variants of TCP use different approaches to calculate CWND based on the amount of congestion on the link.

Design Issues of Session layer.

It responds to service request from the presentation layer and issues service request to the transport layer. This layer provides the mechanism for opening, closing and managing a session b/w end user application processes. i.e, a semi-permanent dialogue.

Communication sessions consist of request and responses that occur b/w application.

Session layers are commonly used in application environment that make use of remote procedure calls (RPC).
Ex of RPC Session layer protocol —
ISO 8237 X.225.
In case of connection loss this protocol may try to recover the connection.

If a connection is not used for a long period the session layer protocol may close it and reopen it.

It provides for either full duplex or half duplex operation.

Session layer services.

Authentication, permission, session restoration {check pointing} and recovery}.

Remote procedure call

{RPC is a protocol which works in a session layer of the OSI model & in the aggregate application layer of TCP/IP model. It is useful in developing n/w applications which need services from a remote computer in the network}

Working

It is working as a client server model.

It uses different authentication methods to validate

It is independent of transport layer protocols.

RPC request can use both UDP & TCP but prefer UDP format.

The major RPC authentication methods are -

* Null authentication

often calls must be made where the caller does not know who he is or the server does not care who the caller is.

* Unix authentication

The caller of remote procedure may wish to identify himself as he is identify on a unique system

DES {Data encryption standard}.

It is the advanced form of unix authentication.

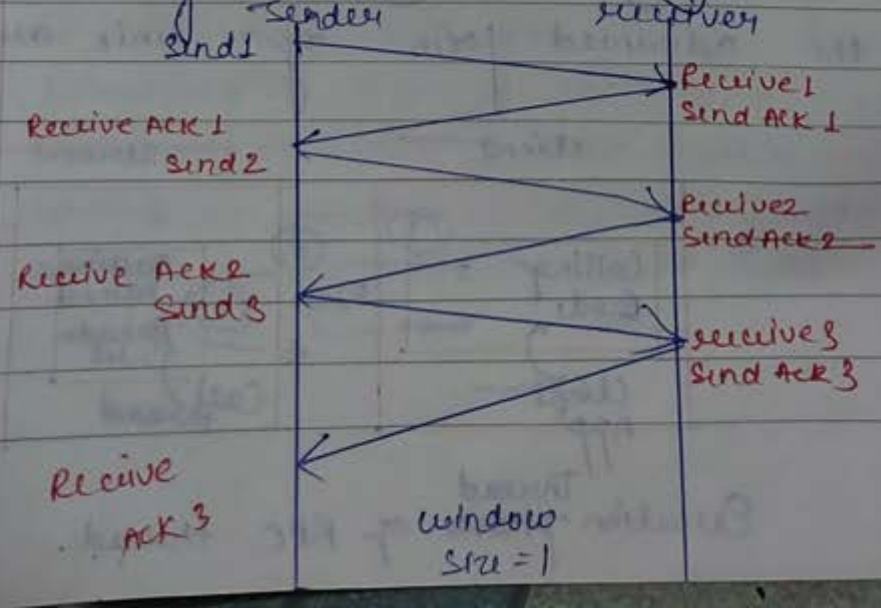
Thread Execution phases of RPC thread.

Window Management in TCP.

It is an important concept that ensures reliability in packet delivery as well as reduce the wastage of time in waiting for the acknowledge after each packet.
Sliding windows, a technique also known as windowing is used by the internet's TCP as a method of controlling the flow of packets b/w two computers or network host. The buffer allows TCP to receive & process data independently of the upper application.

Window size. It determines the amount of data that you can transmit before receiving an acknowledgement.

Sliding window refers to the fact that the window size is negotiated dynamically during the TCP session.



Design issues with presentation layer

To manage & maintain the syntax & semantics of the information transmitted.

Encoding data in a standard agreed upon way.
Ex. String, double, data etc.

Perform standard encoding on wire.

Data compression.

to optimize disk space when saving data
There are two general types of compression algorithms -

1. Lossless compression.
It compresses the data in such a way that when data is decompressed it is exactly the same as it was before compression i.e., there is no loss of data. It is used to compress file data such as executable code,

text files & numeric data because programs that process such file data cannot tolerate mistakes in the data. It will typically not compress file as much as lossy compression techniques & may take more processing power to accomplish the compression. The various algorithms used to implement lossless data compression.

1) Run length encoding
It replaces the consecutive occurrence of a given symbol with only one copy of the symbol along with a count of how many times that symbol occurs. Hence called run length.
Ex.
AAAABBCDDEE
The string ↑ would be encoded as 4A2B1C2D2E

2) ~~Differ~~ Differential pulse code modulation
In this method first a reference symbol is placed then for each symbol in the data we place the difference between that symbol & a reference symbol used.

Ex,
Using symbol A as reference symbol the string would be encoded as

AAABBCDDDD
A0011233333

c) Dictionary based encoding
One of the best known dictionary based algorithm is Lempel-Ziv (LZ). Also known as substitution coder.

In this method a dictionary [table of variable length strings is built. This dictionary contains almost every string that is expected to occur in data when any of these strings occur in the data then they are replace with the corresponding index to the dictionary.

Let us say the word dictionary has a index 3240 in one particular dictionary.

To compress a body of text each time the string dictionary appears it could be replaced by 3240

*) Lossy compression
It is the one that does not

promise that the data receive is exactly the same as data send i.e., the data may be lost. This is because a lossy algorithm removes information that it cannot later restore

They are used to compress still images video & audio. It typically achieve much better compression ratio than lossless algorithm

Audio compression

1. It is used for speech or music
2. For speech we need to compress a 64KHz digitized signal, for music we need to compress 1.411 megaHz(MHz) signal.
3. Two types of techniques are used
   a) Predictive encoding

In this the differences b/w the samples are encoded instead of encoding all the sample values.

It is normally used for speech.

Several standards have been defined such as GSM {13 Kbps}, G.729 {8 Kbps} & G.723.3 {6.4 or 5.3 Kbps}

b) Perceptual encoding
It is used to a CD quality audio that requires a transmission bandwidth of 1.414 Mbps.

Mp3 a part of MPEG standard use this perception encoding.

It is based on the study of psychoacoustics {a study of how people perceives sound}.

Mp3
Mp3 these two phenomenon i.e., frequency masking.
{The ability of a loud sound in one frequency band to high the softer sound in another frequency band that would have been audible in the absence of loud sound} & temporal masking to compress audio signals

A small no. of bits are allocated to the frequency ranges that are partially masked & a larger number of bits are allocated to the frequency ranges that are not masked.

Assignment 4.

Reliable VS Unreliable.

Reliable.

End stations running reliable protocols will work together to verify the transmission of data to ensure accuracy & integrity of the data.

A reliable system will set up a connection & verify that all data transmitted is controlled in an orderly fashion is received in the correct order & is intact.

Reliable protocols work best over physical medium that loses data & is prone to errors. The error correction ordering & verification mechanisms require overhead in the data packets & increase the total amount of bandwidth required to transmit data.

TCP is a typical reliable protocol TCP often usually adds an average of 42-63 bytes of overhead to datagram.

Unreliabl.

Unreliabl protocols make no effort to set up a connection, they don't check to see if the data was received & usually don't make any provision for recovering from errors or lost data.

Unreliabl protocols work best with physical medium with low loss & low error rates. UDP is an example of Unreliabl protocol.

UDP makes no provision for verifying whether data arrived or is intact.

Difference between symmetric and Asymmetric cryptosystem.

Comparison factor	Symmetric Cryptosystem	Asymmetric cryptosystem
Number of cryptographic keys	Symmetric encryption incorporates only one key for encryption as well as decryption	Assymmetric encryption consist of two keys. These key known as Public key and Private key.

Complexity	Symmetric encryption is a simple technique compared to asymmetric encryption as only one key is employed to carry out both the operations	Contribution from separate keys for encryption and decryption makes it a rather complex process
Swiftness of Execution	Due to its simplistic nature both the operation can be carried out pretty quickly	Because of encryption & decryption by two separate keys and the process of comparing them make it a tad slow procedure.
Algorithm Employed	• RC4 • AES • DES • 3DES • QUAD	• RSA • Diffie-Hellman • ECC • El Gamal • DSA

Ques3. Voice over IP

VoIP is short of voice over internet protocol.

VoIP is category of hardware and softw - are that enables people to use the internet as the transmission medium for telphon calls by sending voice data in packets using IP rather than by traditional circuits transmission of the PSTN

Advantages of VoIP

One advantage of VoIP is that the telephone calls over the Internet do not incur a surcharge beyond what the user is paying for internet access, much in the same way that the user doesn't pay for sending individual emails over the internet.

(06)

There are many internet telphony applications available. Some, like CoolTalk and NetMeeting, come bundled with popular web browsers. Others are standalone products.

VoIP also referred as internet telephony, IP telphony of Voice over the Internet [VoI]

Assignment 5.

Internet

The Internet is a global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide.

It is a network of networks ~~of local to global scope~~ that consists of private, public, academic, business & government networks of local to global scope, linked by a broad array of electronic, wireless & optical networking topologies.

The Internet carries a vast range of information resources & services such as the inter-linked hypertext documents & applications of the WWW, electronic mail, telephony & file sharing. Some publications no longer capitalize "Internet".

Email.

Email is short of electronic mail, mail you can send or receive directly to your computer, & you can turn on your computer & go pick up your mail whenever it's convenient. Many people use email

Ques3 Voice over IP

VoIP is short for Voice over Internet Protocol.

VOIP is a category of hardware and software for sharing their personal data.

Although basically a method of passing message from one computer to another, email is becoming increasingly popular, in part because those computers sending messages to each other could be in adjacent offices or on opposite sides of the world.

In fact the ability to send the letter or memo halfway across the world at the speed of electricity instead of more traditional postal services is one of the strengths of the internet. Because of email even the remotest office can maintain practically instant communication with headquarters, or even another remote office.

Public network

A public network is a type of network wherein anyone, namely the general public has access and through it can connect to other networks or the Internet. This is in contrast to a private network, where restrictions and access rules are established in order to segregate access to a select few. Since a public network has few or no restrictions, users need to be wary of possible security risks when accessing it.

A public network is a usage designation rather than a topology or other technically related principle.

There is no technical difference between private and public network in terms of hardware and infrastructure, except for the security, addressing & authentication systems in place.

UNIT-5.

Application layer.

It is the layer in OSI model and in the TCP/IP protocol suite.

It consists of protocol that focus on process to process communication across an IP N/w and provide communication interface & end user services.

Services.

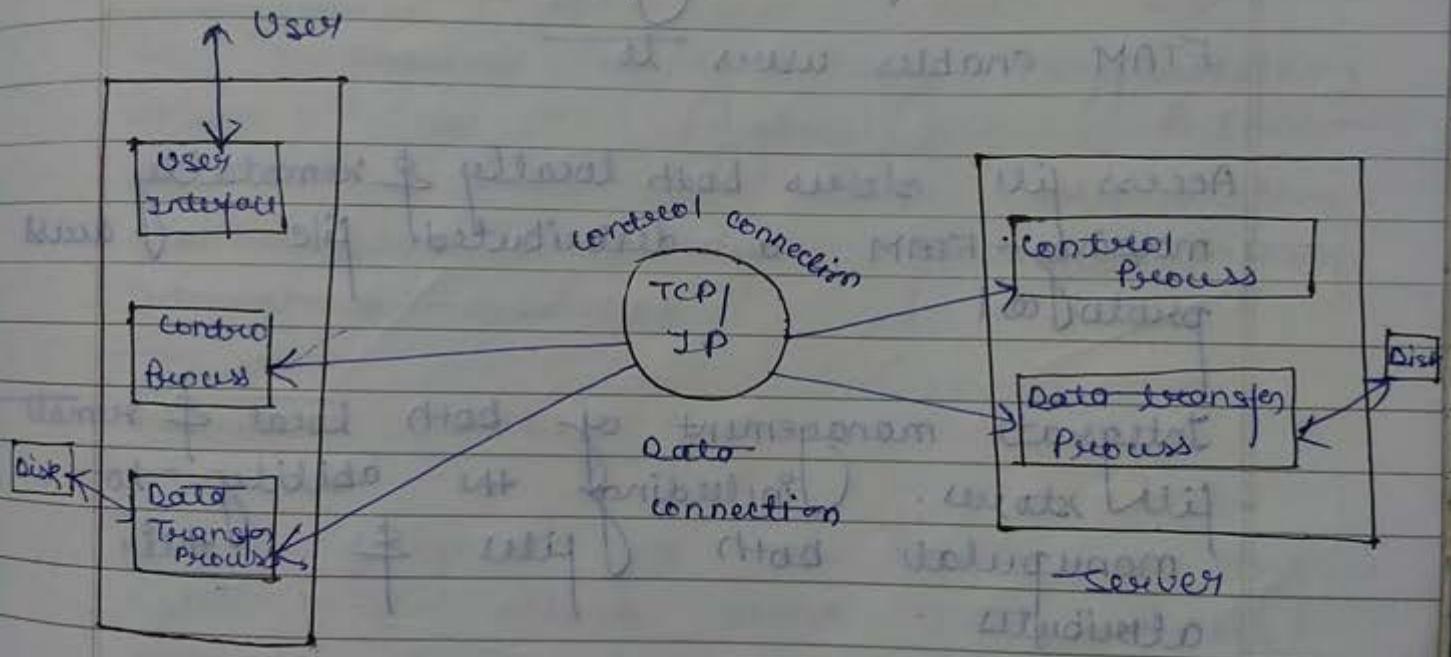
1. Simple mail transfer protocol (SMTP)
2. File transfer protocol (FTP)
3. Web surfing
4. Web chat
5. Email client
6. N/w data sharing
7. Virtual terminals
8. Various file & data operation.

File transfer protocol.

FTP is an application layer protocol which moves files b/w local & remote file systems. It runs on the top of TCP like http. To transfer file to TCP connections are used by FTP in parallel control connection & data connection.

For sending control information like user identification, password, commands to change the remote directory, commands to retrieve & store file etc are initiated on port number : 21

For sending the actual file, data connection is used, initiated on port number 20.



When a FTP session is started b/w a client & server the client initiates a controlled TCP connection with the server side. The client sends the controlled information over this. When the server receive this it initiates a data connection to the client side. Only one file can send over one data connection but the controlled connection remain active throughout the user session unlike http FTP needs to maintain a

state about its user throughout the session.

File transfer access & management (FTAM)

It specifies a standard mechanism for access & management of a distributed network file system.

FTAM enables users to

Access file stores both locally & remotely making FTAM a distributed file access protocol

Integrate management of both local & remote file stores. including the ability to manipulate both files & their attributes.

Access files stores on different kinds of machin that have different types of file system.

Transfer files both synchroniously & asynchroniously.

This model defines the architecture of a hierarchical, virtual file store

In terms of file structure, file attributes & kinds of operations that can be performed on files & their attributes.

It simply specify the underline architecture of the system.

VPN

It is popular among large organizations which use global Internet for both intra and inter organization communication but require privacy in their internal communication.

Private network.

It is designed for use inside an organization. It allows access to Shared resources & at the same time provide privacy. To achieve privacy organization use one of the following strategies - private n/w, hybrid n/w and VPN.

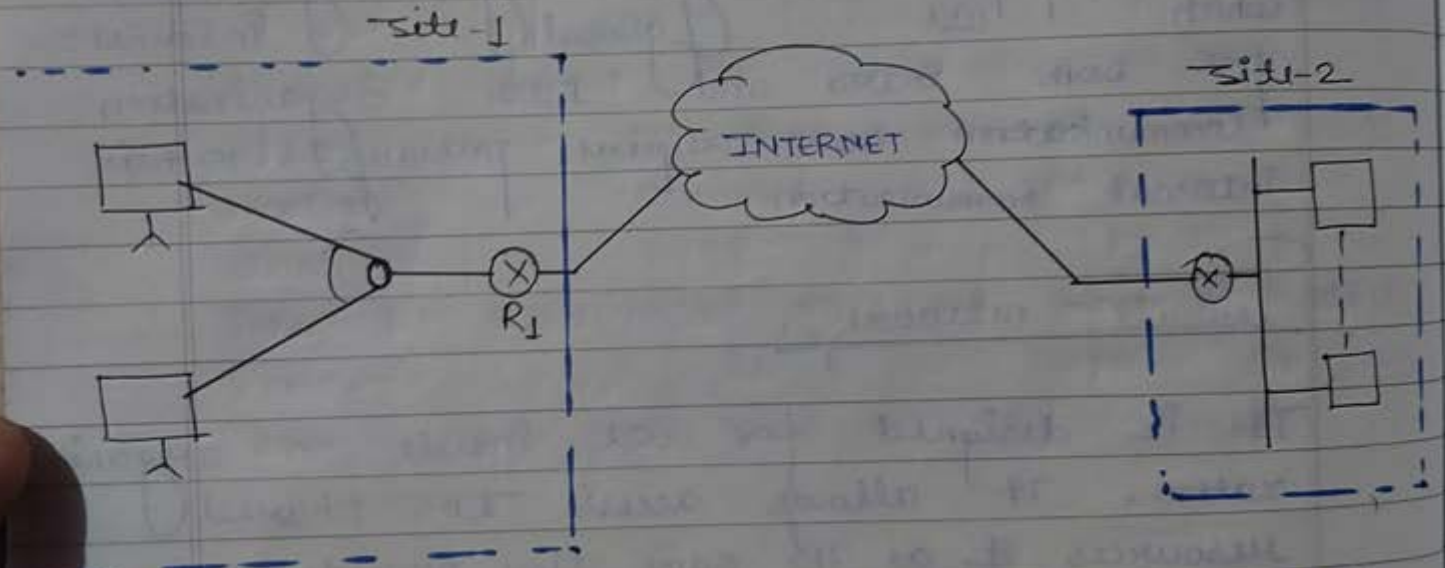
Private and hybrid n/w have a major drawback i.e./ cost private WANs are expensive

One soln is to use global Internet in public and private communication.

A technology called VPN allows the organization to use global internet for both purposes.

It creates a n/w i.e., private but virtual.

It guaranties privacy inside organization and it is virtual because it does not use real private WAN.



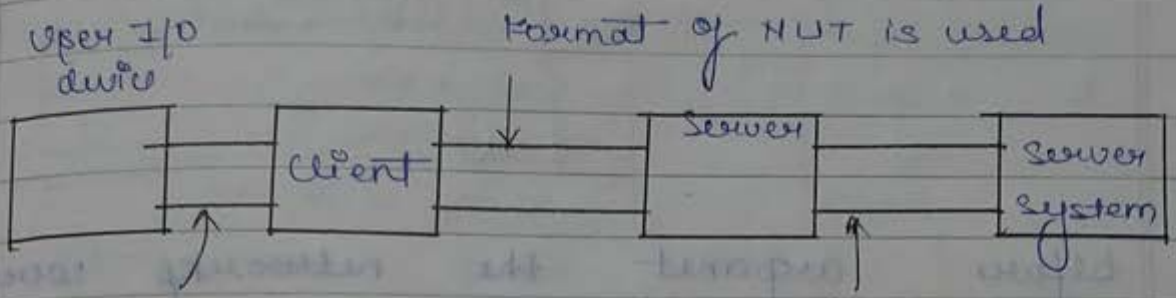
VPN uses IP security in the tunnel mode to provide authentication, integrity and privacy.

Virtual terminal

Network virtual terminal NVT is a device used by telnet. It enables a local computer to communicate with a remote machine.

It is bidirectional device. It has a Keyboard and a printer

NVT {Network virtual terminal} uses client server architecture.



NVT uses the seven bit standared ~~ascii~~ {ASCII} representation of data.

Example of network

Network can be classified in-

1. Public n/w
2. Research n/w
3. Cooperative n/w
4. Commercial network
5. Coorporate network

Novell network

This is most popular network in PC world. Specially designed to be used by a n/w of PCs. It is based on the client server model looks more

It looks more like TCP/IP model.

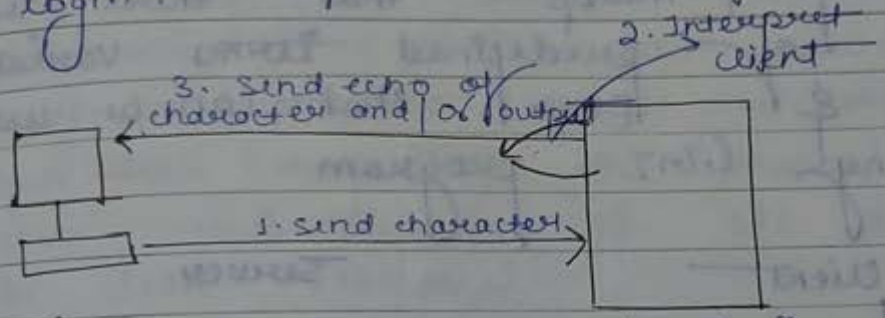
Before arpanet the networks were basically the telephone n/w which operated on the circuit switching so domain naming system was created for organizing machines into domains & map host names into IP addresses later arpanet was handed over to the defense communication agency.

Remote login.

In a system if all users login to the central server computer and uses its resources it is known as local login, but sometimes a user may have to access an application program i.e., located on remote computer for this user logon to the remote computer in a process called

remote login.

Telnet is a protocol used for remote login.



CGI (Comman Gateway Interface)

It is a technology that handles and creates dynamic documents. It is a set of standards that defines how a dynamic document is written, How data are input to the program and hocols the output result is used.

The term comman in CGI indicates that the standard defines the set of rules that is comman to any language or platform.

The term gateway here means that a

CGI program can be used to access other resources such as database, graphical packages & soon. The term interface means that there is a set of predefined terms variables, calls & soon that can be used in any CGI program

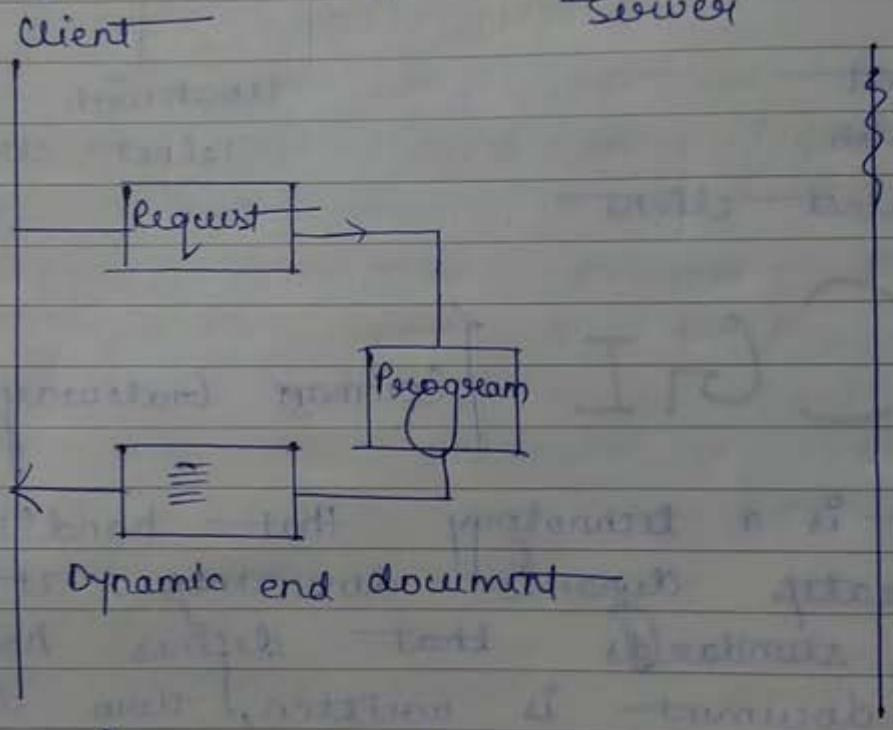


Fig Dynamic document using CGI

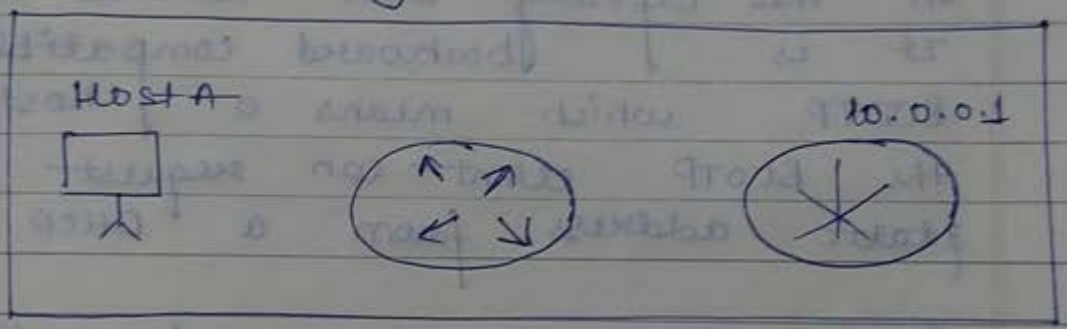
TFMP (Trivial file management protocol)

It is a network protocol used to transfer file between host in a TCP/IP network. It is a simpler version of FTP and it does not have all

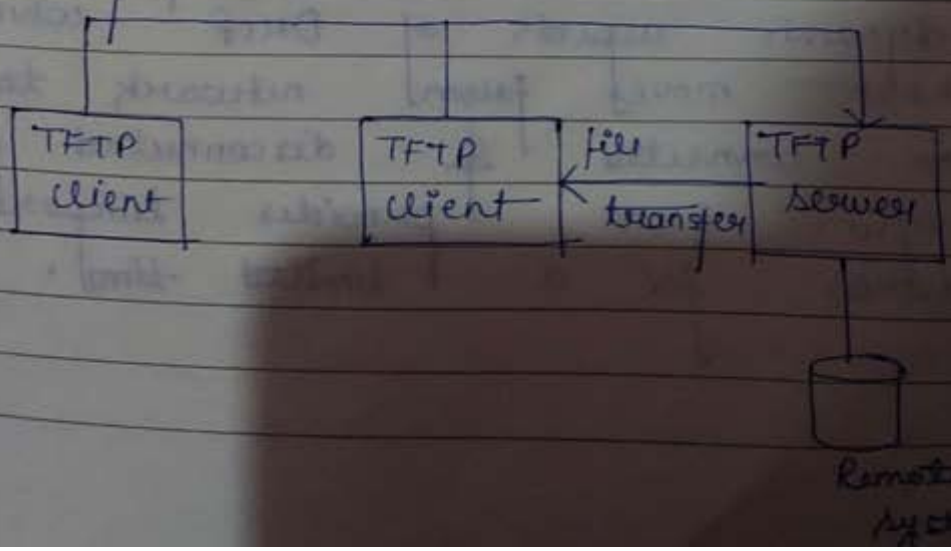
of its functions.

Ex.

You cannot list, delete or rename files or directories on a remote server. It can only be used to send and receive files b/w two computers. It doesnot support user authentication & all data sent in clear text eg.



A user wants to transfer files from host A to the router R_1. R_1 is a CISCO device and it has a TFTP server installed the user will have to start an TFTP client program & initiate a data transfer. It uses a well known UDP port 69



Dynamic host configuration protocol

It has been devised to provide static & dynamic address allocation that can be manual or automated. DHCP provides

Static address allocation.

In this capacity DHCP act as BOOTP does. It is backward compatible with BOOTP which means a host running the BOOTP client can request a static address from a DHCP server.

A DHCP server has a database that statistically binds physical address to IP address.

Dynamic address allocation. DHCP has a second database with a pool of available IP address. This second database makes DHCP dynamic. The dynamic aspects of DHCP when a host moves from network to network or connected & disconnected from a n/w. DHCP provides temporary IP address for a limited time.

It allows both manual and automatic configuration. ~~Static~~ addresses are created manually & dynamic addresses are created automatically.

Delay	It is slower than connectionless service. Before sending a packet as it create virtual connection.	It is faster than connection oriented service.
Packet Travel	All the packets b/w sender & destination follows same path.	Not necessary all packets follows same path.
Protocol Example.	TCP protocol	UDP protocal.

Ques 10. what are the number of cable links required for n service connected in mesh, ring, bus and star topology?

Ans. Cable link required for mesh topology $= n(n-1)/2$
" " " " bus " $= n-1$
" " " " ring " $= n$
" " " " star " $= n$

Comparison chart — b/w Connection oriented protocol services and Connectionless protocol services

Characteristics	Connection oriented services	Connectionless services.
Definition	It is the communication service in which virtual connections is created before sending the packet over the Internet	In this communication service no virtual connections is created before sending the packet over the Internet.
Authentication	It needs authentication of the distination node before transferring data	It transfers data without any authentication.
Reliability	This is a more reliable connection as it makes the virtual connection before sending packets and ensures delivery to the distination	This connection does not ensures reliability
Handshaking	The handshaking is carried out to ensure both sender and receiver agree with this connection	There is no handshaking process

Difference b/w TCP/IP model and OSI model

Basis for Comparison	TCP/IP model	OSI model
Expands to	TCP/IP Transmission control protocol/Internet protocol	Open system Interconnect
Meaning	It is a client server model which is used for data transmission over Internet.	It is theoritical model which is used for computing systems.
Number of layers	4 layers	7 layers
Tangible	Yes	No
Usage	Mostly used model	Never used model