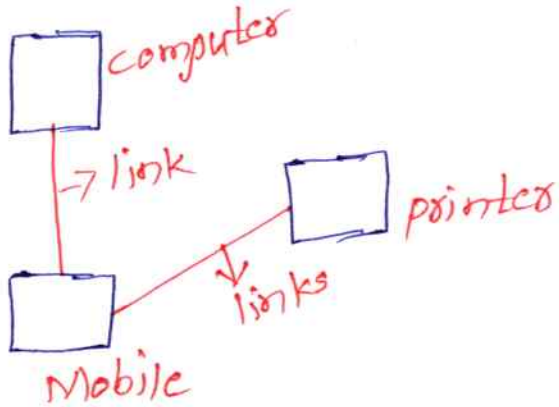
# Computer Networks

## UNIT-I

### What is a computer Network?

A computer Network is a group of communication elements or computing devices connected by some communication links or cables that exchange data and resources with each other.




Communication devices: computers, Mobiles, routers, printers, Laptops etc.

communication Links: copper wires, Twisted pair cables, coaxial cables, Fiber optic cables, Wireless Links: microwaves infrared waves.

### Uses of computer Network:-

* Communication:- Through computer Networks individuals and organizations can communicate collaborate using communication channels that may include email, chatting, video conferencing.
* Resource Sharing:- Computer Networks allows us to share resources like printers, files, Software etc. Instead of everyone needing their printer, Multiple people can use one printer through the network.

* Data Access:- We can quickly access and retrieve data from different places. For example you can lookup information on the internet or access your work files from home.

* Entertainment:- Networks let us watch movies, play online games, listen to music.

* collaboration:- A team of people can work together more easily using computer Networks. Tools like Google docs. and Microsoft Teams let people work on the same document simultaneously.

* E-commerce:- online sales and payments processing are empowered with the computer networks, that enable people to sell products online and execute secure payments.

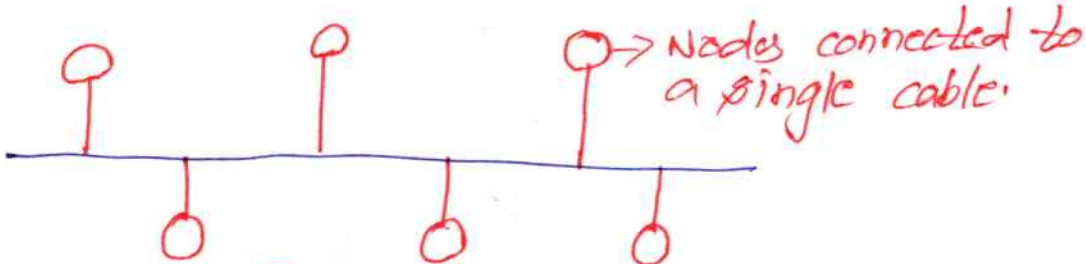
* Education:- computer Networks provides a platform for distance learning, access to resources of higher education and give opportunity for collaboration among students and teachers.

## Network Topologies:-

* **Topology:-** Topology refers to the systematic description of the arrangement of a network.
* **Network Topology:-** Network topology refers to the actual geometric layout of computers and other devices connected to the network.

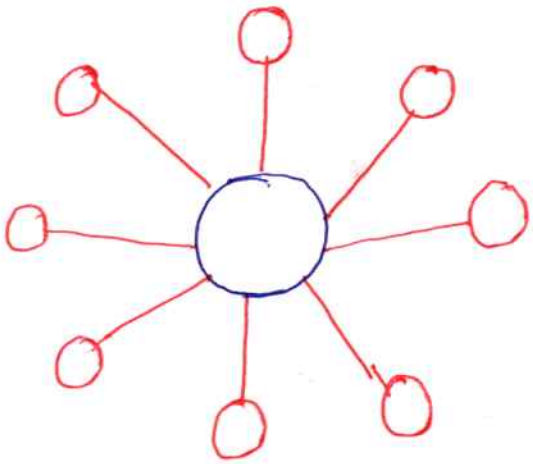
### Types of Network Topologies:-

* **Bus Topology:-** In a Bus Topology each computer or server is connected to a single cable. Hence all the nodes (computers and other devices) share the same communication channel.



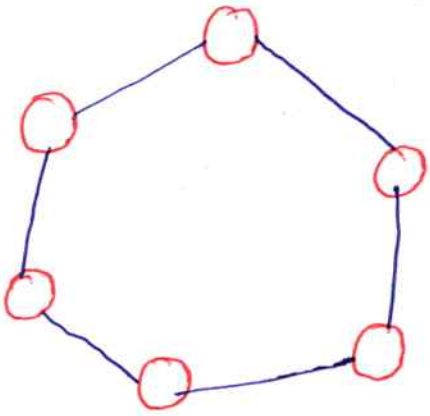

Bus Topology

* **Star Topology:-** The star Topology is considered as the easiest topology to design and implement. In this topology each node is connected to a central Hub or Server with a point-to-point connection. All resources that traverses the network passes through the central Hub.



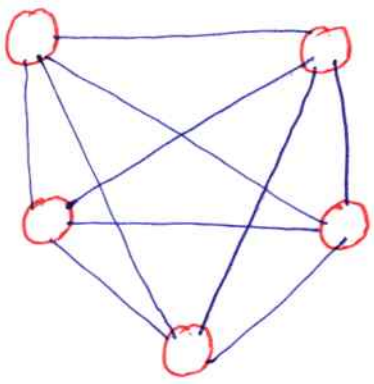
Star Topology

* Ring Topology:- In a Ring Topology all the nodes are connected to each other in the shape of a closed loop. So that every node is connected directly to two other nodes, one on either side of it. In a ring network messages travel in ~~the same~~ one direction either in clock-wise or anti-clockwise.



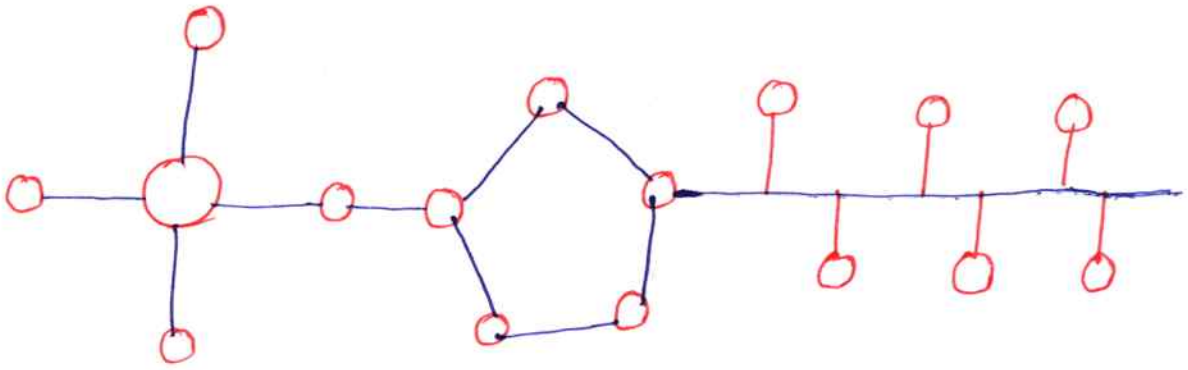
Ring Topology

* Mesh Topology:- Mesh Topology is also known as a completely network, every node is connected to every other node on the network using a separate physical link. Mesh topology involves the concept of routes. Unlike other topologies in a Mesh topology, a message can take any of the several possible paths from source to the destination.



Mesh Topology

* Hybrid Topology:- We have studied the star, ring, bus, mesh topologies. Each of these has its own advantages and disadvantages. Hence in the real world a pure star, pure ring, pure bus is rarely used. Hence Hybrid network topology uses a combination of any two or more topologies.



Hybrid Topology

---

## ➡ Network Hardware (or) Hardware Components

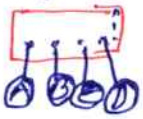
Network Hardware is nothing but Hardware components or Network devices. Some of the Network devices are.

1. **Network cables:-** Network cables are the transmission media to transfer data from one device to another device. A commonly used network cable is RJ-45 connector. Ex:- Twisted pair cables → 1G Base T, 100 mbps, 100 Base T
   Coaxial → 10 Base2, 10 Base5 10 Mbps
   Fiber optic → In form of light 1000 Base FX Speed = 3x10^8, 2KM

2. **Repeater:-** Network repeaters are electronic devices that regenerates incoming electrical, signals, wireless or optical signals. without a repeater the data can only span a limited distance before the quality of the signals degrades.



3. Hub:- A Hub is a device which is used to transfer the data in the form of packets to all the connected devices.



4. Switch:- Switch is a device that can be used in all places where a hub is used. In switch error checking is done. It sends the good data packets to the correct devices.

5. Bridge:- Bridge is a device that connects two or more LAN's which works on the same protocal.

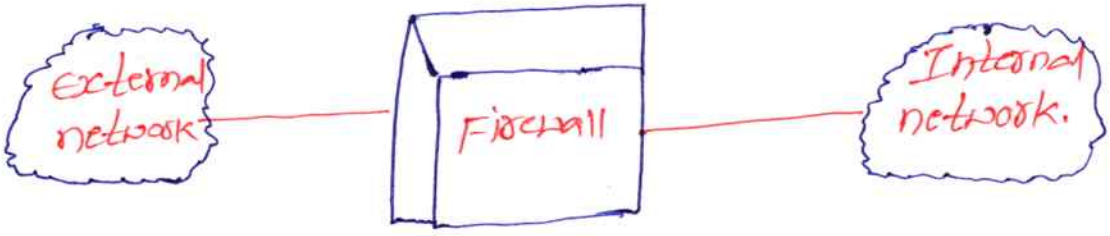



6. Router:- A router is an intelligent device that routes data to the destination computers. It is basically used to connect two logically and physically different networks two LANs, two WANs and a LAN with WAN. The routers use special software known as routing table that stores the address of devices connected to the network.

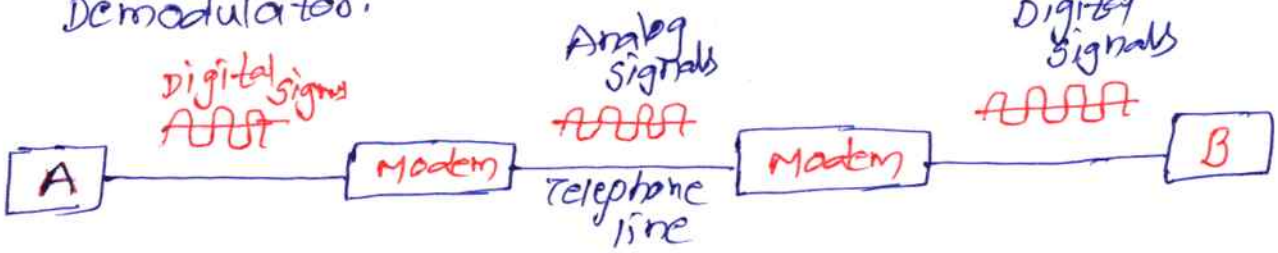
8. **IDS:-** IDS means an Intrusion detection system is a network security tool that monitors network traffic for suspicious activity.

Intruder ⟶ Intrusion ⟶ IDS

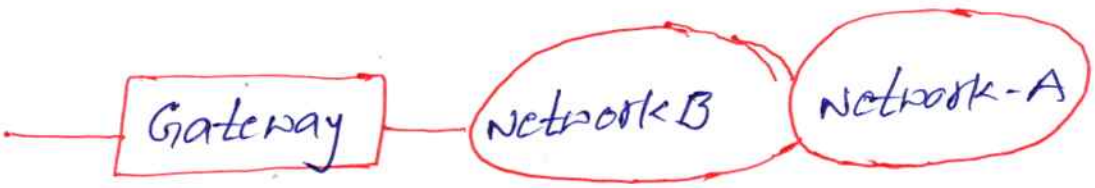
9. **Firewall:-** A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on configurable ~~network traf~~ security rules.




10. **Modem:-** A modem is a network device that allows computers and other devices to connect to the internet. It is a Modulator and Demodulator.



7. Gateway:- A Gateway is a very complicated networking device that is used to pass data to the different networks which are using different networking models or different protocols



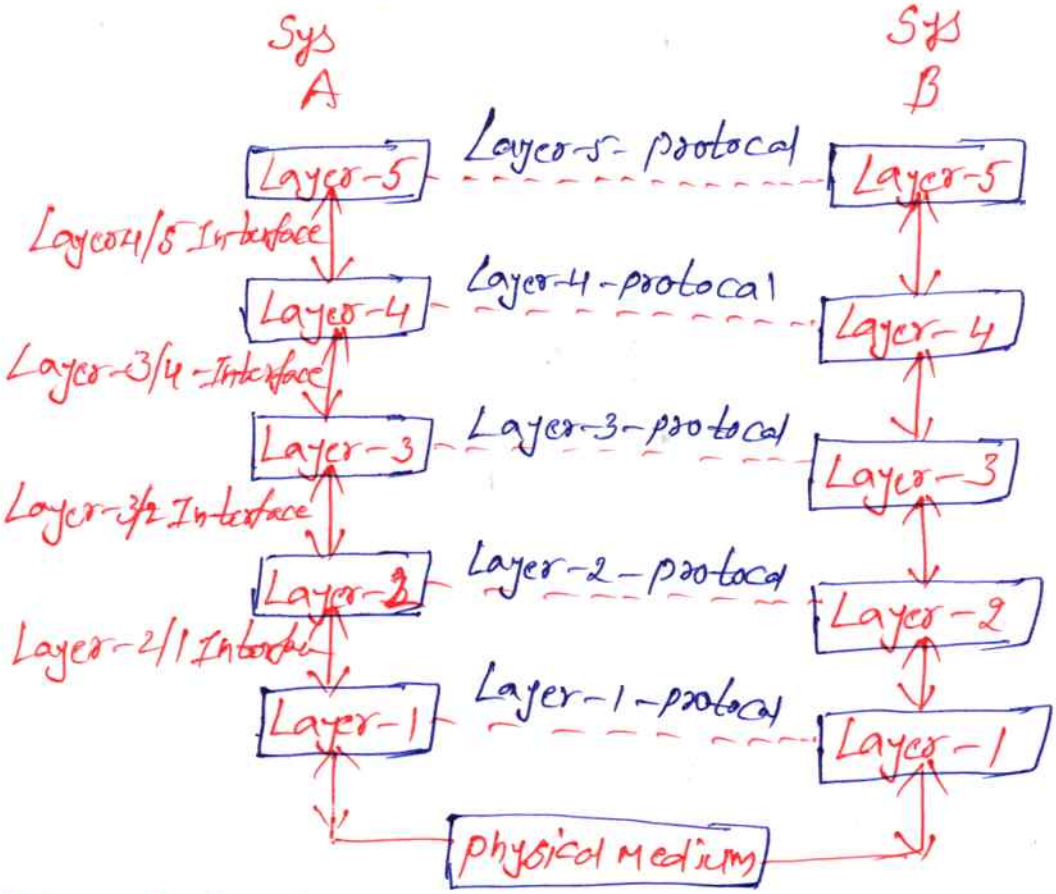

## Network Software:-

Network software is defined as a wide range of software that streamlines the operations, design, monitoring and implementation of computer networks.

Most networks are organized as a stack of layers, one on the top of another. The no. of layers or levels. Each layer has a specified function and specified protocols.

1. protocal Hierarchies
2. Design issues for the Layers
3. connection-oriented versus connectionless Service
4. Service primitives.
5. The relationship of Services to protocals.

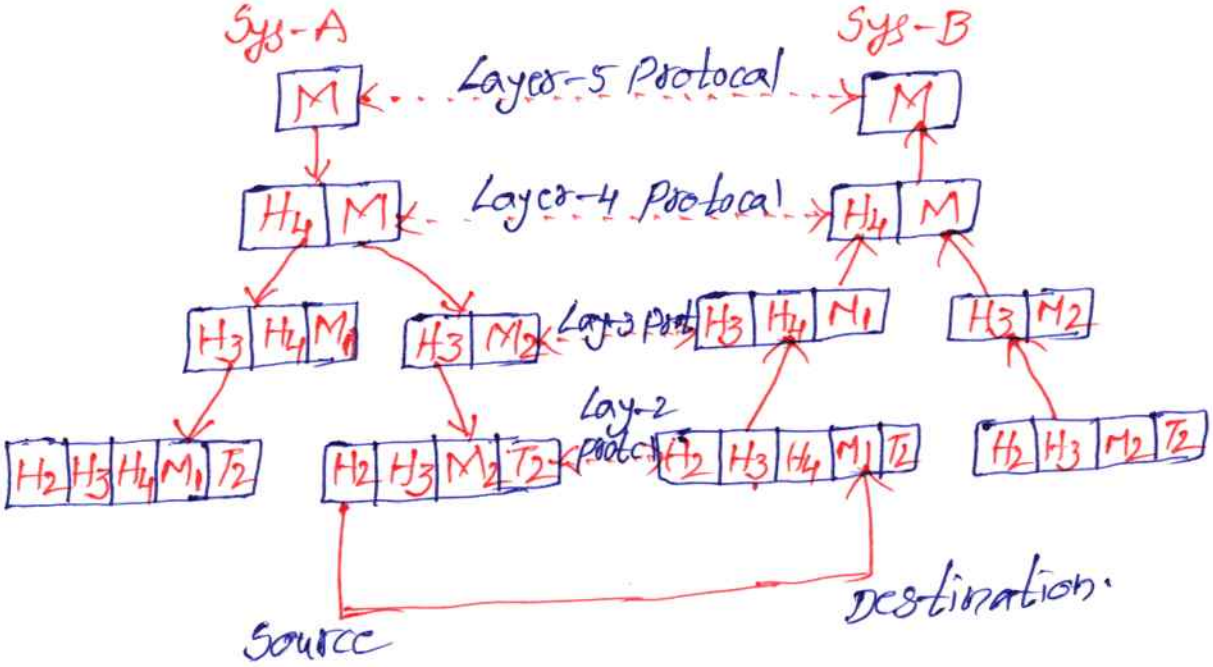
Q. 1. Protocal Hierarchies:- Most Networks are organized as a stack of layers or labels each one build upon and one below it.




Q. 2. Network Architecture:- A set of layers and protocals is called Network architecture. A list of protocal used by certain system is called protocal stack.

Header-H:- Identification of message, address, seaunce no., size.

Trailer-T:- one packet end and next begining.

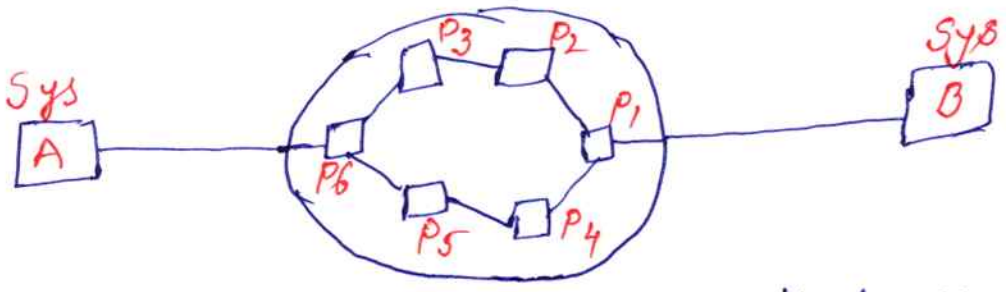



2. Design issues for the layers:-

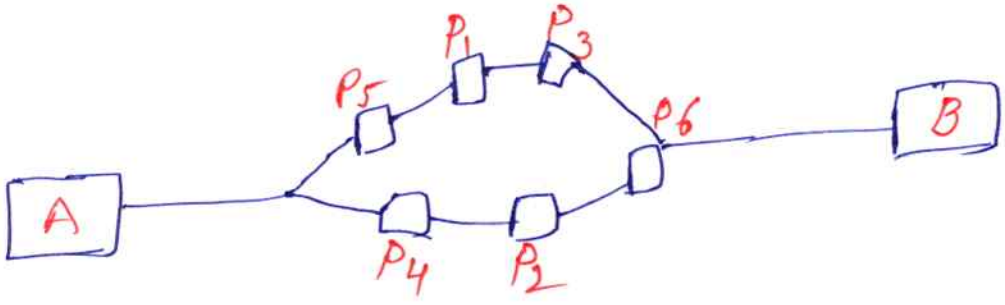
* Reliability:- Error detection & correction and routing.
* Evaluation of Network:- Addressing or Naming Scalable.
* Resource Allocation:- Transmission line, Real time delivery, quality of services.
* Network security:- confidentality, Authentication Integrity.
* Direction of Transmission:-
  * simplex – Tv, Radio
  * Half-duplex – walkitaki
  * Full Duplex – Mobile

## 3. Connection oriented versus connection-less services:-

* **Connection oriented:-** It is similar to telephone system. It can be established in same n/w or different n/w. It provides end-to-end connection b/w sender & Receiver.




* **Connection-less:-** In this method no any connection is provided. For example in postal system the sender sends the data and reaches the destination and no any connection is there while sending the data. In this method the data packets are not sent in the same order.



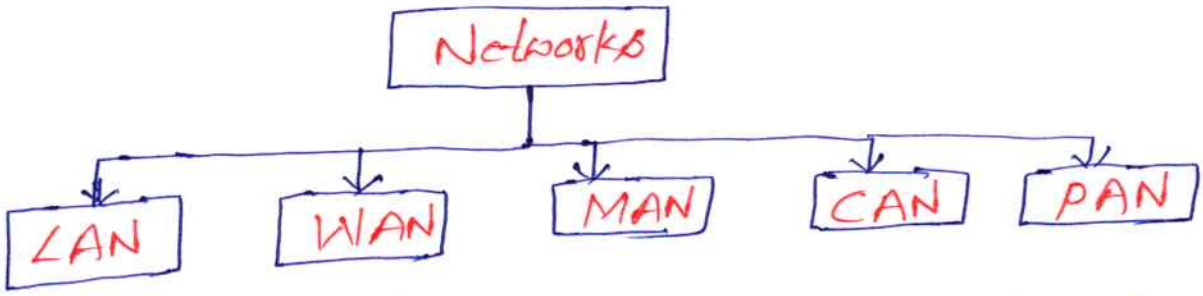
4. Service primitives:- A service is basically defined as a set of operations available to user process to access the services.

5. The relationship of services to protocals:-

* The service defines ~~what~~ relates to an interface bth two layers, with the lower layer being the service provider and the upper layer being the service user.
* A protocal is a set of rules where the data is transfered bth. two devices within a layer.

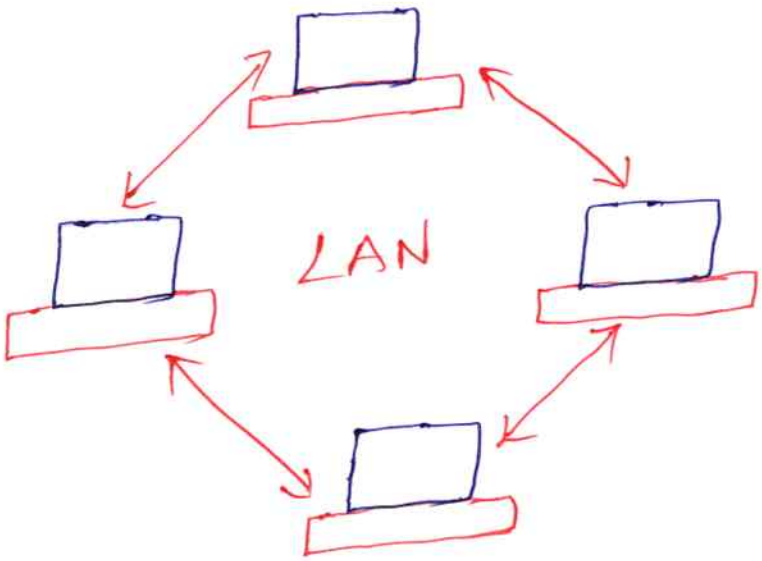
---

## Types of Networks



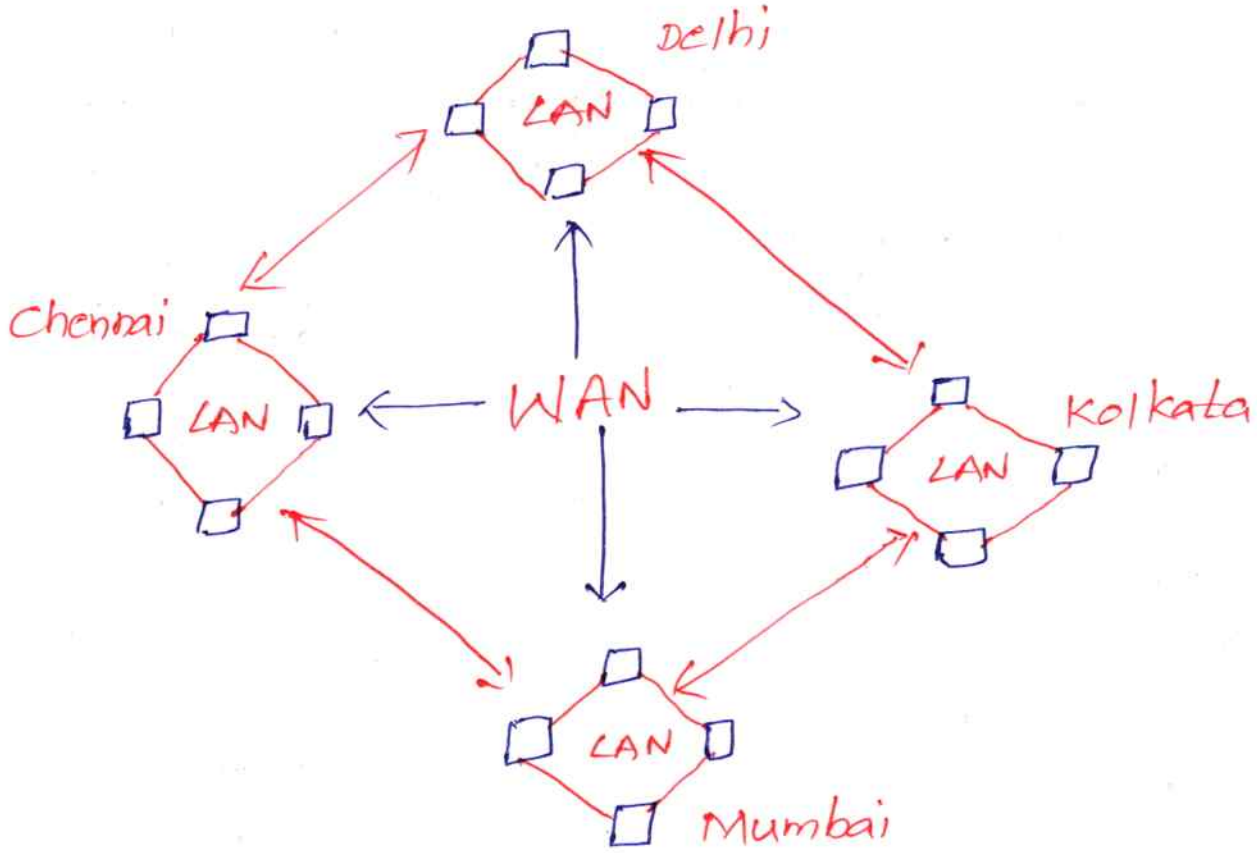

Networks are mainly classified into Five types widely used in both homes and business. The networks are categorised based on their scale and scope, historical reasons, preferences for networking industries and their design.

1. LAN :- LAN means Local Area Network. LAN was first invented for communication btn. two computers. However later with growth in technology, it was used to connect computers and devices in a limited area such as home, school, computer laboratory.

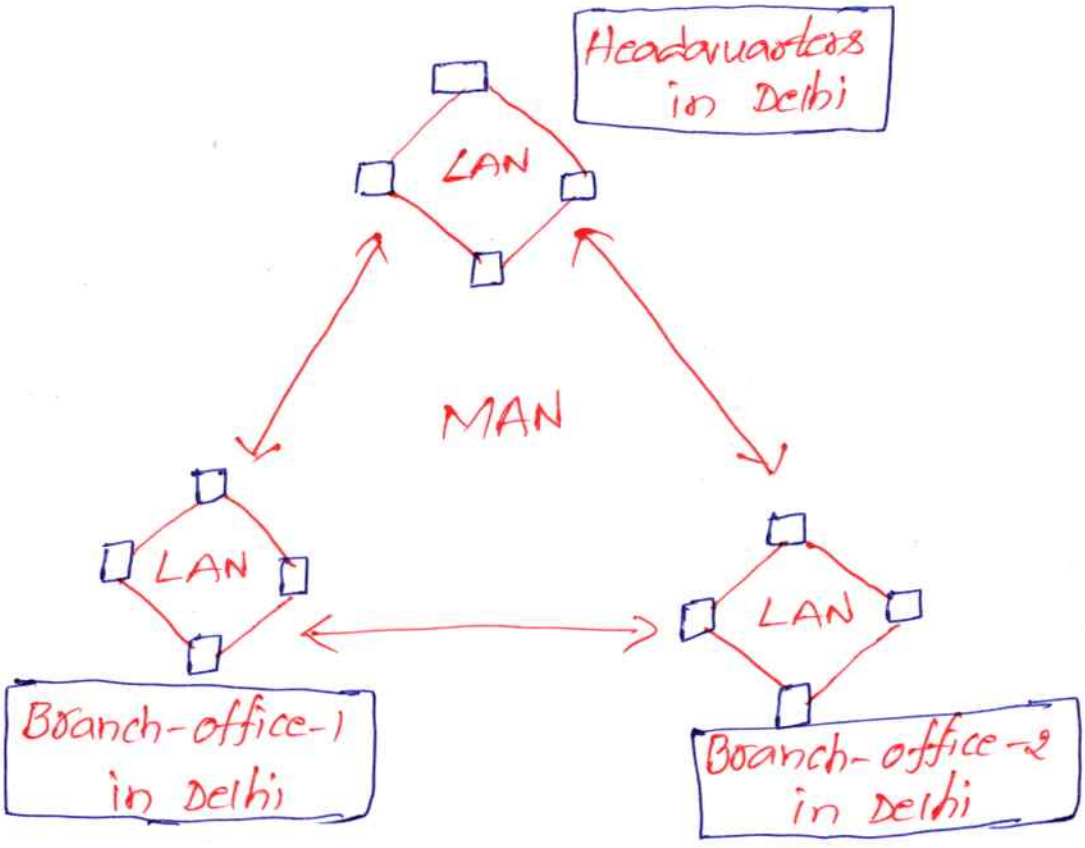



2. WAN :- WAN means Wide Area Network. As indicated by name it spreads a large geographical area such as city, country or even intercontinental distances using a communication channel that combines many types of media such as telephone lines, cables and air waves.

~~3. MAN:- MAN means Metropo~~




3. MAN:- MAN means Metropolitan Area Network. MAN is a network that interconnects computers and other devices in a geographical area or region larger than that covered by even a large LAN, but smaller than the area covered by a WAN. A MAN may interconnect networks in a city, ~~a campus~~ or a community to form a single larger network.




4. CAN:- CAN means campus/corporate Area Network. CAN is a computer network created by interconnecting LANs within a limited geographical area. The network is almost entirely owned by the campus of an enterprice, University, government, military bases etc. The size of the area that CANs cover is larger than that of LANs and smaller than that of MANs or WANs.

5. PAN:- PAN means Personal Area Network. PAN is a computer network designed for communication btn. computer devices such as mobile computers, cell phones, personal Digital Assistants that are close to one person. The range of a PAN is few meters i.e 10 meters.

---

## OSI Reference Model

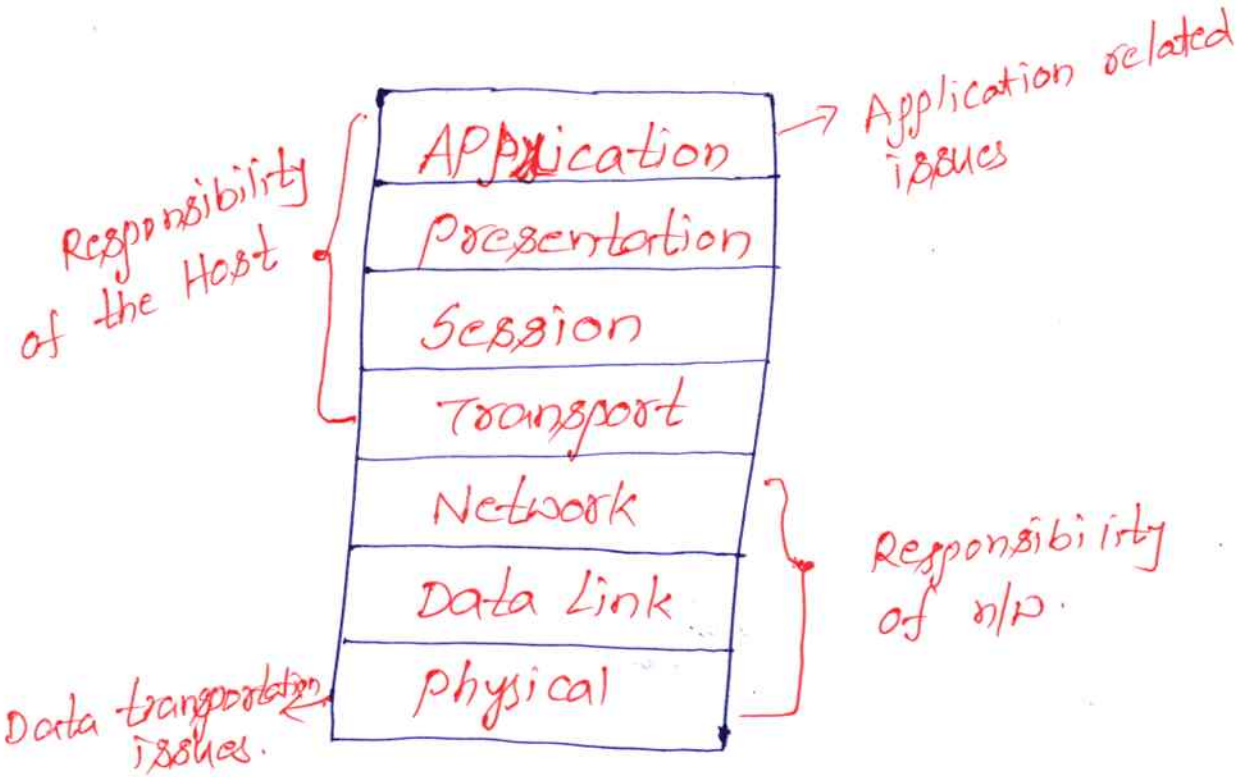
OSI stands for open System Interconnection

OSI is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.

* OSI model was developed by the International Organization for Standardization (ISO) in 1984.

* OSI model divides the whole task into smaller and manageable tasks. Each layer is assigned a particular task.

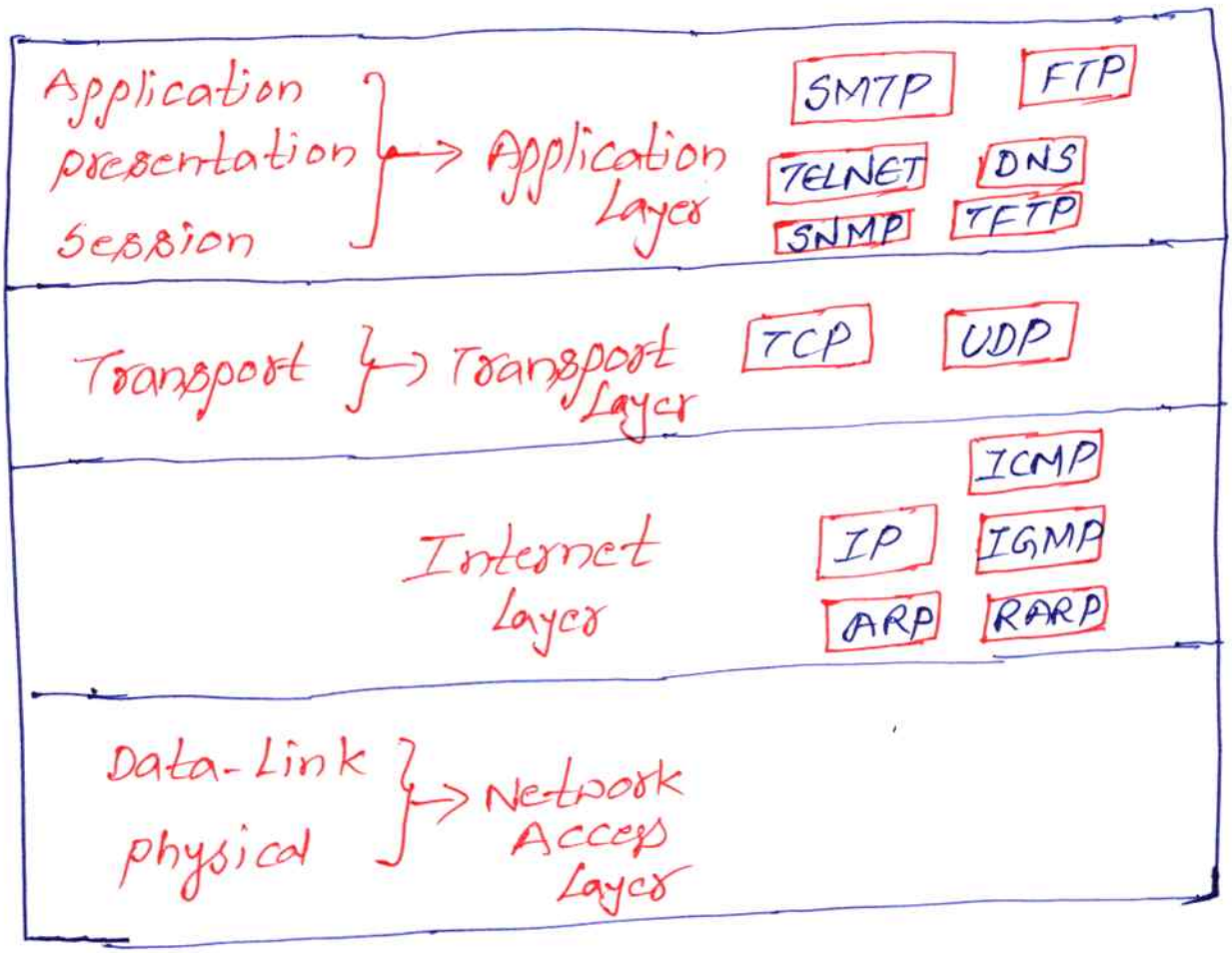
* OSI model consists of seven layers, each layer performs a particular task.




1. Application Layer:- It provides the services to the user.
2. Presentation Layer:- It is responsible for translation, compression, encryption.
3. Session Layer:- It is used to establish, manage and terminate the sessions.
4. Transport Layer:- It provides reliable message delivery from process to process.
5. Network Layer:- It is responsible for moving the packets from Source to Destination.
6. Data Link Layer:- It is used for error free transfer of data frames.
7. Physical Layer:- It provides a physical medium through which bits are transmitted.

## TCP/IP Reference Model

TCP means Transmission Control protocol/Internet protocol. It was designed to describe the functions of the communication system. this model was developed by Department of Defense (DOD).




1. Application Layer:-

* SMTP:- SMTP means Simple Mail Transfer protocol. It is used to send the data to another E-mail address.

* FTP :- FTP means File Transfer protocol. It is used to transfer files from one p.c to another p.c.

* TELNET :- TELNET means Terminal Network. It is used to establish the communication btn the Local computer to Remote computer. accessed & controlled from a separate, distinct location using SSH or a network connection.

* DNS :- DNS means Domain name System. Domain names are nothing but website names.

* SNMP :- SNMP means Simple Network Management protocol. It is used to manage the devices in the internet.

* TFTP :- Trivial File Transfer protocol. It allows the users to store and access their files from the remote host.

2. Transport Layer :- This Layer protocols exchange data receipt acknowledgements and retransmit missing packets to arrive in order & without error.

* It is heart of OSI Model. The responsibility of Transport Layer is Reliability, Flow control & correction of data. The protocols in Transport Layer are:

* The role of Transport Layer is End to End delivery or port to port delivery.

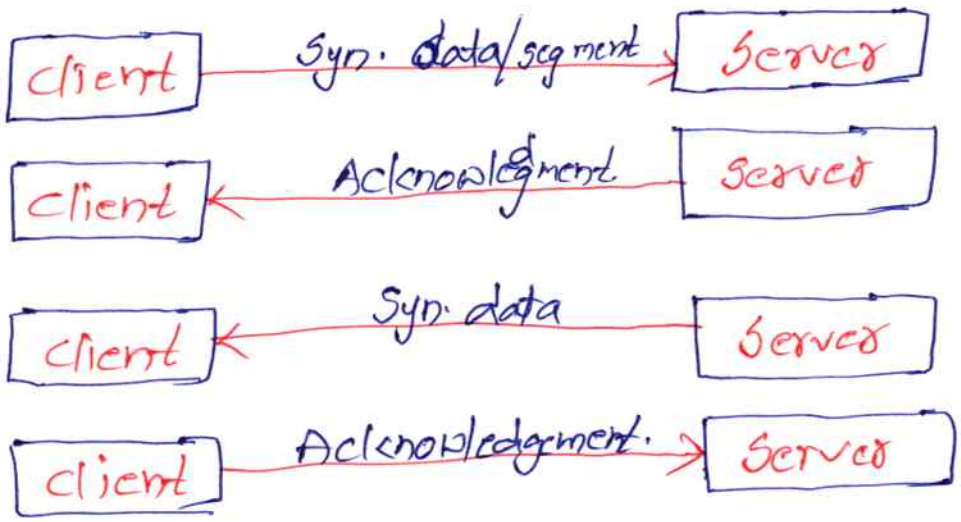
1. Decides transmission should be single/parallel, 2. Multiplexing & Splitting, 3. Quality of service, 4. converting msg to segments 5. End to End delivery

* TCP * UDP.

* **TCP:-** TCP means Transaction Control protocol. In TCP Applications can interact with one another using TCP & physically connected by a circuit. That physical circuit is like Virtual circuit btn. Sender and Receiver.

Virtual circuit → logical pathway that enables data transmission btn. devices on a network.

By using TCP, it transfer all segments to receiver then it receives an acknowledgement. In this process any data damage will occur, again retransmit the damaged frames.

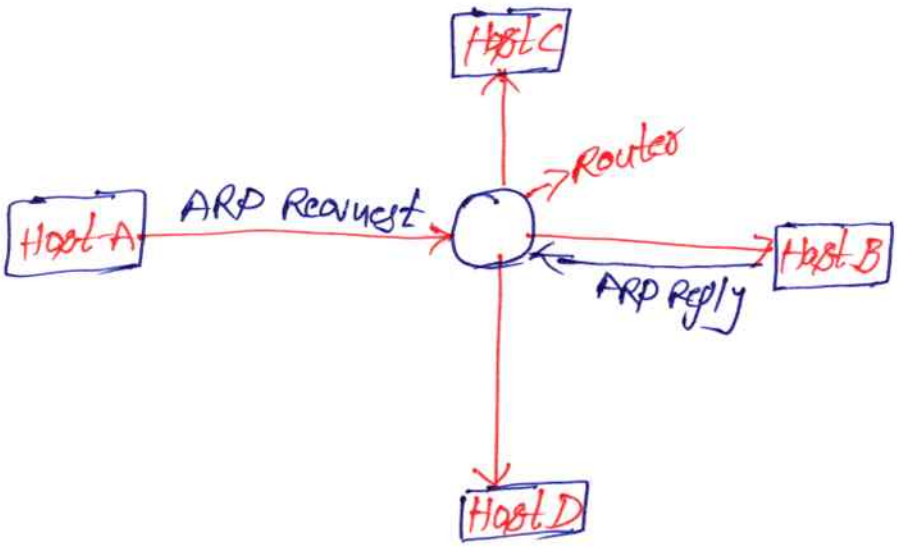



* Message or data is divided into segments and each segment having some sequence number.

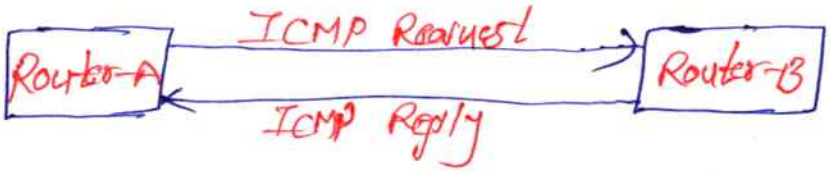
* **UDP:-** UDP means User Datagram Protocol. UDP is a communication protocol that sends data packets directly to a destination computers. UDP sends messages called datagrams, which are units of data transmission. UDP is faster than TCP, but less reliable.

**3. Internet Layer:-** It performs the Logical Transmission of data over the entire network. i.e sends the packets to any network and they arrive to the destination.

* **ARP:-** ARP means Address Resolution Protocol. ARP is a network protocol used to find out the MAC (Media Access control) address or hardware address of a device from an IP address. ARP has two protocols. i.e ARP Request & ARP Reply.



* ICMP:- ICMP means Internet Control Message Protocol. ICMP sends error messages from the receiver to sender when data doesn't arrive as expected. It is used to test for network delay and packet loss.




* IGMP:- IGMP means Internet Group Management protocol. This protocol allows several devices to share one IP address so they can all receive the same data. It is used for Multicasting communication with IP networks. Multicasting means a group of devices receives the same messages or packets.

* IP:- IP means Internet Protocol. IP is a set of rules that how data is sent and received on the internet. Some functionalities of IP are:

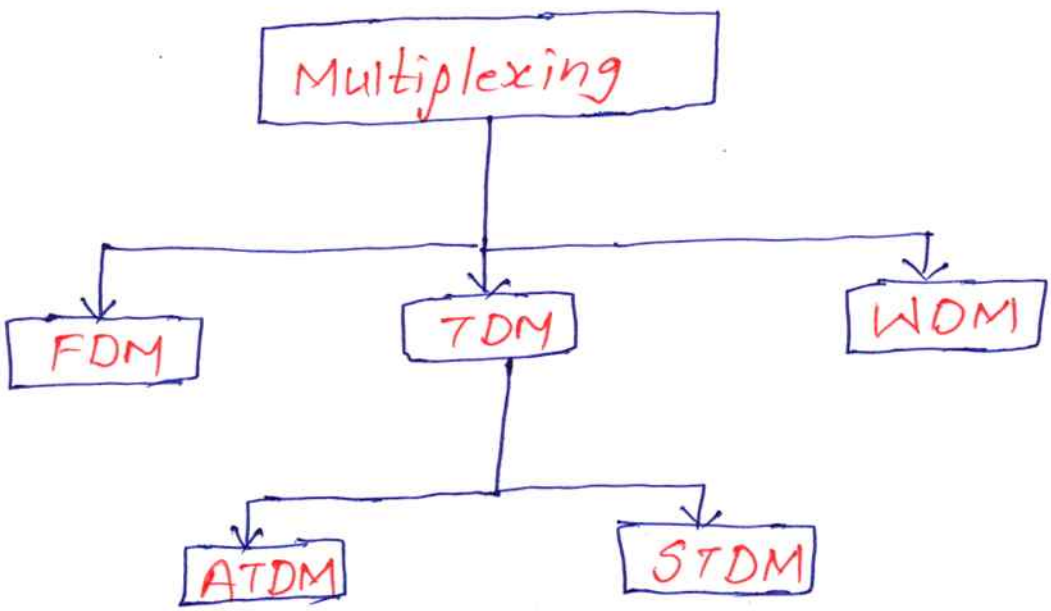
* IP Addressing
* Host-to-Host communication
* Data Encapsulation
* Reassembling
* Routing.

4. Network Access Layer:- This Layer manages the physical aspects of data transmission including how bits are sent over the network. It deals with the physical connection btn. devices on a network and ensures data is properly received and transmitted accross that connection.

## Multiplexing / Data Multiplexing:-

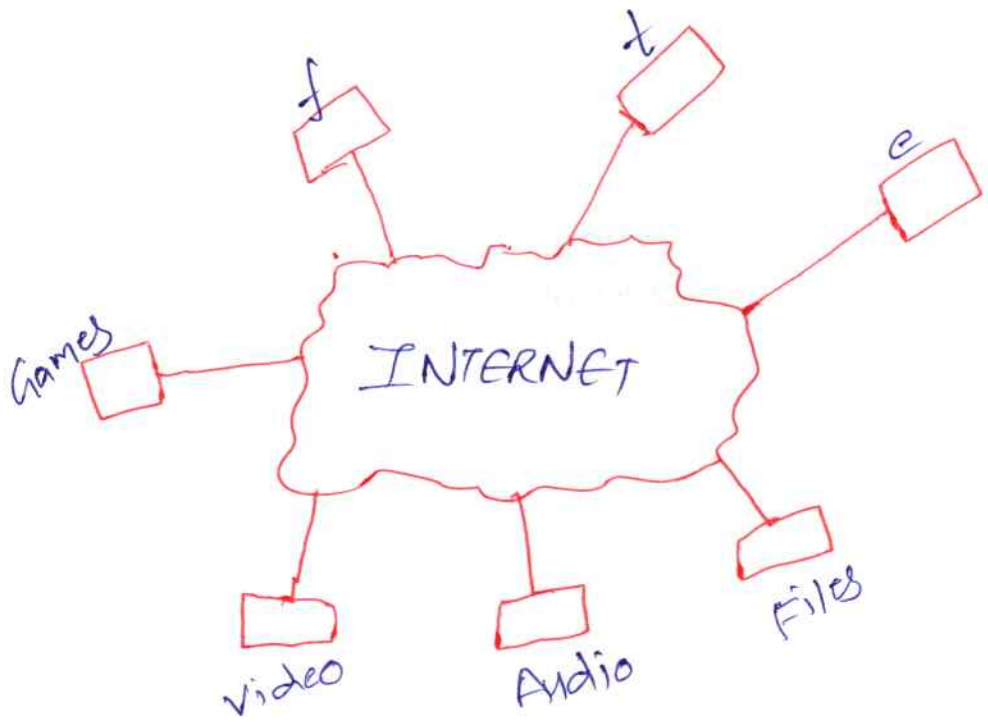
Data Multiplexing is a technique that combines multiple Analogue message signals or digital data streams into one signal for transmission over a shared medium. It is widely used in everyday devices such as telephone and television.

### Types of Multiplexing:-



## Internet:-

* The Internet came in the year 1960 with the creation of the first working model called "ARPANET".
* It allowed multiple computers to work on a single network which was their biggest achievement at that time.
* In oct, 1969 using ARPANET first message was transferred from one computer to another.
* Now-a-days Internet is a global network of interconnected computers and devices that allows users to access and share information.
* It enables users to access a wide range of services like websites, emails, social media, online applications etc.
* The Internet facilitates the sharing of information, resources and media accross vast distances making it essential for education, Business, entertainment and personal communication.



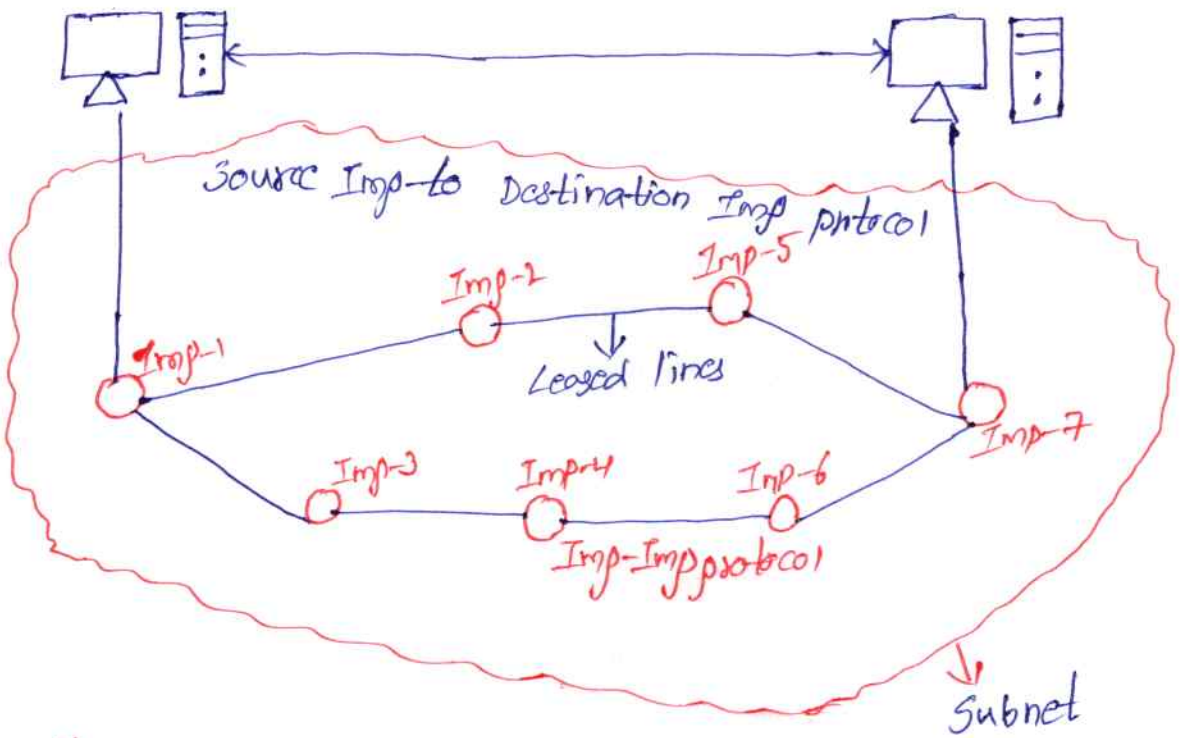

* The internet is setup with the help of physical optical fiber data transmission cables or copper wires and various other networking mediums like LAN, WAN, MAN etc.
* For accessing the internet even 2G, 3G, 4G and 5G services and the wifi requires these physical cable setups to access the internet.
* The Domain Name System (DNS) and protocols that ensure the smooth functioning and global connectivity of the internet.

## ARPANET:-

* ARPANET stands for Advanced Research Projects Agency Network.
* ARPANET was introduced in the year 1969 by the Advanced Research Projects Agency of the US Department of Defense.
* It was the first to implement TCP/IP protocols.
* It was basically the begining of the internet with the use of these technologies.
* It was the first operational network to use packet switching.
* Packet switching means breaking down the data into smaller packets for transmission.
* This network became the foundation for the modern day internet.
* Before ARPANET, computers used circuit switching like telephone networks.
* In circuit switching a dedicated line was needed for communication.
* In this circuit switching method only one person could communicate with another at a time.

* If the line failed, the entire connection was lost.

ARPANET Architecture:-



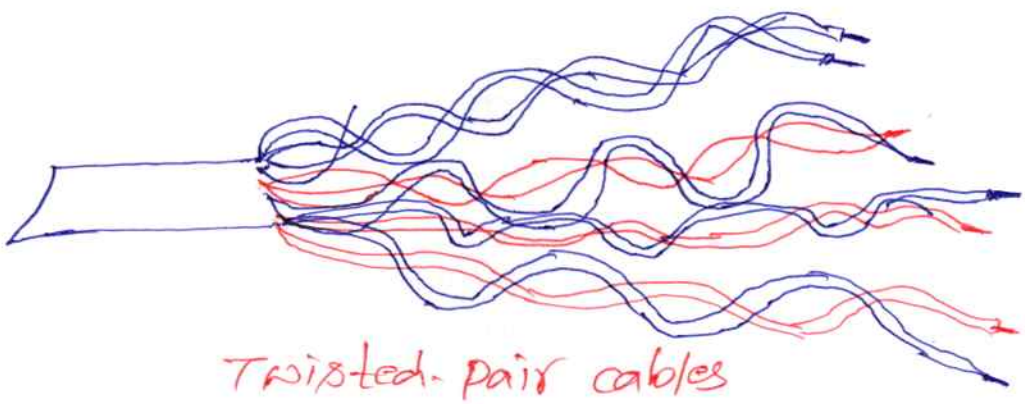

* ARPANET has two main parts
  * Host:- Hosts are nothing but computers that need to communicate.
  * Subnets:- Subnets are the networks that are connected the hosts.
* The subnet contained some special mini devices called IMP's (Interface Message processors), that connected the hosts using leased lines.
* To ensure reliability each IMP was connected to atleast two other IMP's.

* So if a connection failed data could take another path and reaches the destination Host.
* In ARPANET the subnet was the entire network infrastructure that connected computers.
* It includes → 1. IMP's → Interface Message processors These are the actual mini devices that acts like routers.
  2. Leased Lines:- These are the cables which connects the IMP's.
* Each IMP was responsible for
  1. Receiving data from one host
  2. Breaking it into packets
  3. Sending those packets to the correct destination IMP.

## Guided Transmission Media:

* computers and other computing devices are connected by different types of media such as Twisted-pair cables, coaxial cables, optical fiber cables and various wireless technologies.

## Twisted-Pair Cables:-

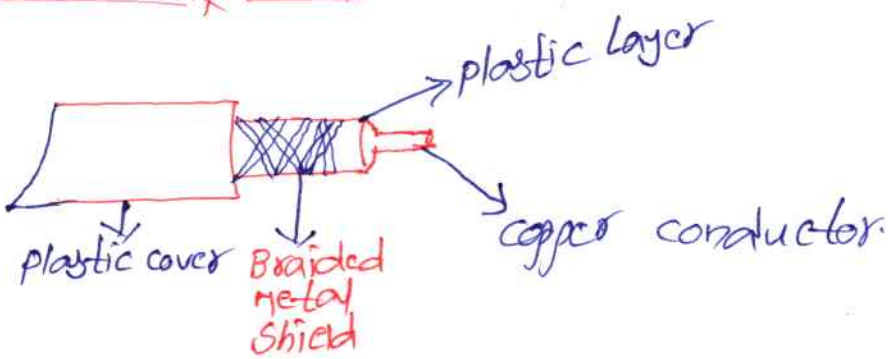


Twisted-pair cables

* Twisted pair cables which consists of copper wires that are twisted into pairs.
* These are the most widely used medium for telecommunications.
* As shown in above figure a bunch of twisted pair cables are enclosed in a plastic insulation.
* In ordinary telephone wires consists of two insulated copper wires twisted into pairs.
* The computer network cables consists of four pairs of copper cabling that can be utilized for both voice and data transmission.

* The transmission speed of twisted pair cable varies from 2 million bits per second to 100 million bps.
* They are cheap and easy to install and use.

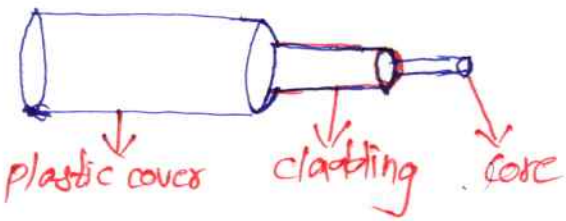
## Coaxial Cables:-




* Coaxial cables are highly preferred connecting media for cable television systems and for connecting the computers within an office building or within short distances to form a network.
* The coaxial cable consists of a single copper conductor at its centre, encapsulated inside a plastic layer that provides insulation btn. the conductor and a braided metal shield.
* The metal shield blocks any interface from the outside environment and is again protected by an outer shield of plastic material.
* The coaxial cable is highly resistant and can support greater cable lengths ~~btn~~ than twisted pair cables.

* The transmission speed varies from 200 million to more than 500 million bps.

## Fiber Optic Cables:-



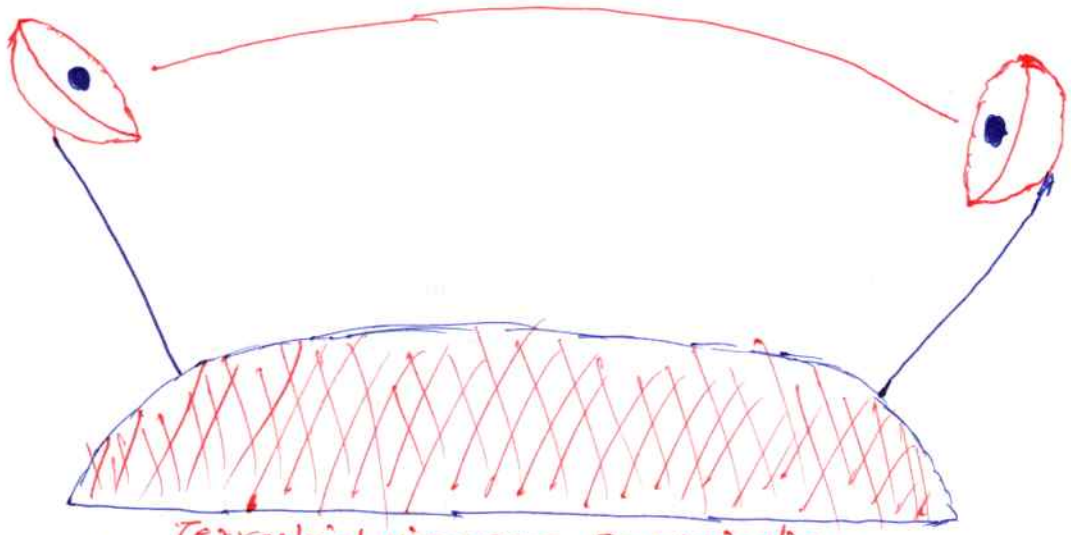

* The fiber optic cable is constructed in several layers.
* The core is the actual glass or fiber conductor, which is covered with a refractive coating called cladding, that causes the light to travel in a controlled path along the entire length of the glass core.
* The next layer is a protective covering or an insulating jacket made of teflon or polyvinyl chloride (PVC) to protect the core and coating from any kind of sustaining damage.
* optical fiber cables carry data as pulses of light. They transmit light that can travel over extended distances.
* The transmission speed of an optical fiber cable is hundreds of times more than that of coaxial cables and thousands of times more than that of twisted pair cables.

## → Wireless Transmission:-

The wireless technology that connect computers and other devices to form a network include Terrestrial Microwave, Satellite communication

### * Terrestrial Microwaves:-

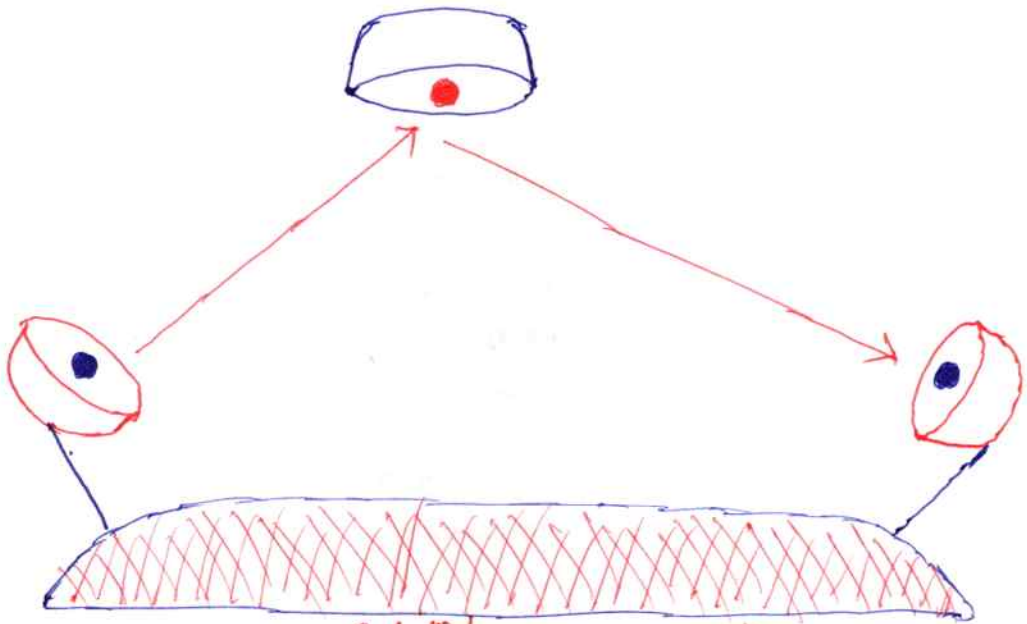
* Terrestrial microwaves use earth-based transmitters and receivers.
* Microwave antennas are usually placed on the top of buildings, towers, hills, and mountain peaks and resembles satellite dishes.
  ↓ look like somebody
*



Terrestrial Microwave communication.

* Terrestrial microwaves use the low-gigahertz range which limits all communications to the line-of-sight.
* Two relay stations are seperated by approximately 40 km.

## * Satellite Communication:-



Satellite communication.

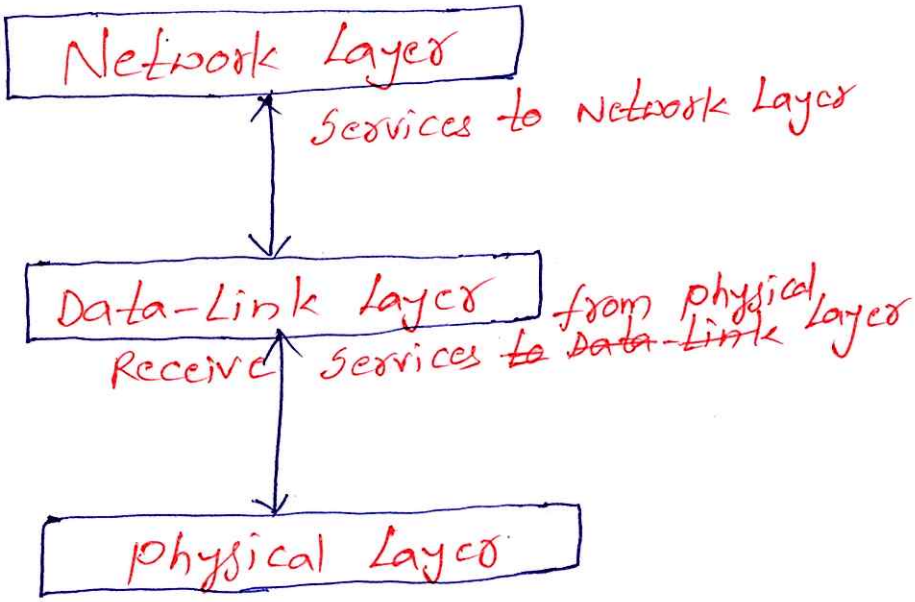
* In satellite communication signals are transferred b-tn. the sender and the receiver using a satellite that is stationed in space.
* The satellite is typically at 35,400 km above the equator.
* In this process the signal which is basically a beam of modulated microwaves is sent towards the satellite.
* The satellite amplifies the received signal and transmits it back to the receiver's antenna present on the earth's surface.
* This means that all the transfer of signal happens in space.

## * Infrared Communication :-

* Infrared light is widely used by TV and video cassette recorder (VCR).
* Infrared wireless communication uses infrared light to transmit data over short distances.
* Infrared technology enables computing devices to communicate via short-range wireless signals.
* This communication technology is commonly used in remote controls and other devices where a direct line of sight is possible.
* Mobile phones are also equipped with ~~each other~~ infrared ports to enable them to be connected to a computer for dial-up networking connections.
* It is characterized by low cost, low power consumption and high security for close-range data transmission.
* The common applications include remote controls for TV's, DVD players and other home entertainment devices.

## Data-Link Layer Design Issues:-

The Data Link Layer is located between physical and Network Layer. It provides services to the Network Layer and it receives services from the physical Layer.




The following are the design issues in the Data Link Layer.

* Services that are provided to the Network-Layer.
* Framing
* Error control
* Flow control.

## * Services to the Network-Layer:-

In OSI each layer uses the services of the bottom layer and provides services to the upper layer. The main function of this layer is to provide a well defined service ~~to the~~ interface over the network layer. There are three types of services.

* Unacknowledged connectionless services:- In this type of services the sender sends the message to the receiver and the sender doesnot get any acknowledgement.

* Acknowledged connectionless services:- In this type of service the sender sends the message to the receiver and the receiver sends the acknowledgement to the sender.

* Acknowledged connection-oriented services:- In this type both the sender & Receiver are connected. sender sends the message through a connected media and the receiver sends the acknowledgement through that connected media.

* **Framing:-** Framing is a point-to-point connection b/n. two computers or devices consisting of a wire in which data is transmitted as a stream of bits. There are two types of Framing

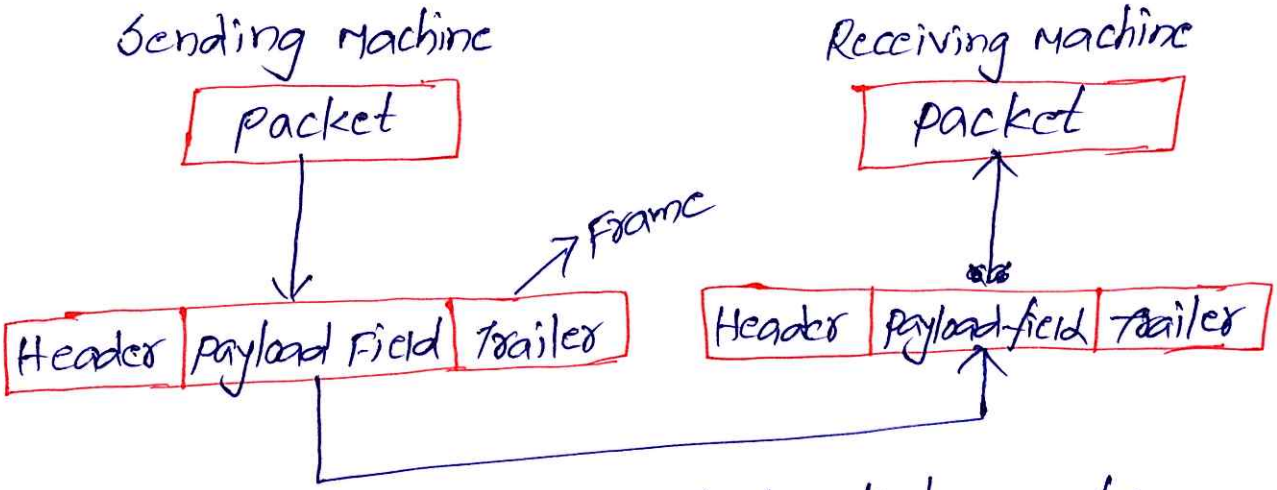
1. Fixed-Size Framing
2. Variable Size Framing.

1. **Fixed Size Framing:-** In this type of framing the size ~~is~~ of the frame is fixed. For example if a device is sending 200 bits of data to the other device. The Receiving device receives 50 bits of frame size first, then ~~it~~ ~~sent~~ the receiver will automatically knows that the next 50 bits are of frame 2 and so on.

2. **Variable Size Framing:-** In this type of framing the size of the frames are different. So additional mechanism has to be implemented to mark the end of one frame and the begining of the another frame. For example the receiver receives the first frame of size 100 bits, the second may be 25 bits and the last frame may be remaining bits.

A frame contains the following parts:

* Frame Header
* payload Field for holding packet
* Frame Trailer.




There are 4 methods that can be used to find the start & end of each frame.

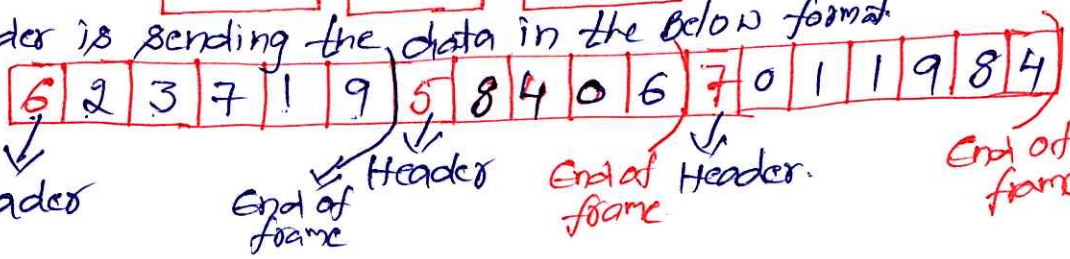
* Character count/Byte count
* Flag bytes with byte stuffing
* Flag bits with bit stuffing
* Physical layer coding violations.

* Character count:- This method uses a field in the header to specify the no. of bytes in the frame.

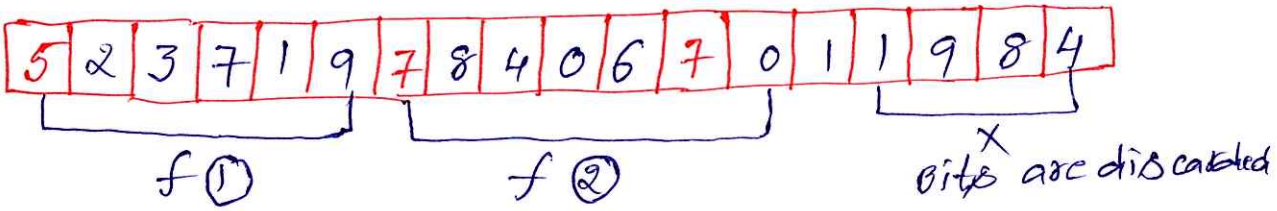
Ex:- 2 3 7 1 9 8 4 0 6 0 1 1 9 8 4

Message without Error.

Sender is sending the data in the below format



## Message with errors



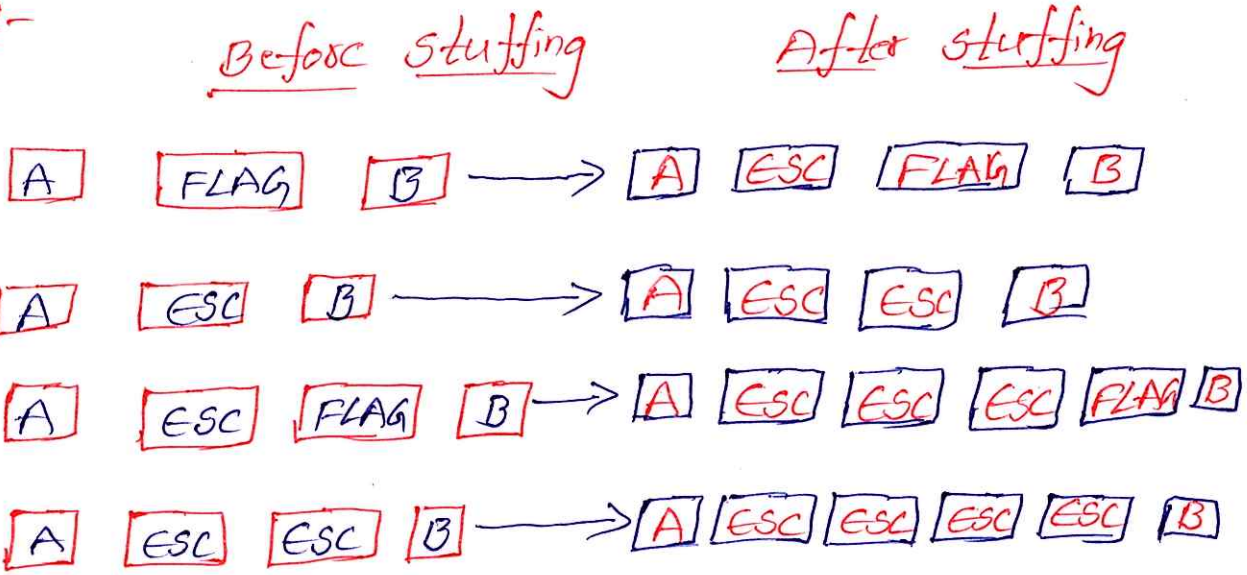

* **Flag bytes with byte stuffing:-** This method is used in point to point protocol. In this method each frame start & end with special bytes, called FLAG byte. If the FLAG byte occurs in the frame then we have to stuff the frame with an extra escape byte (ESC).

Ex:- A frame with flag bytes



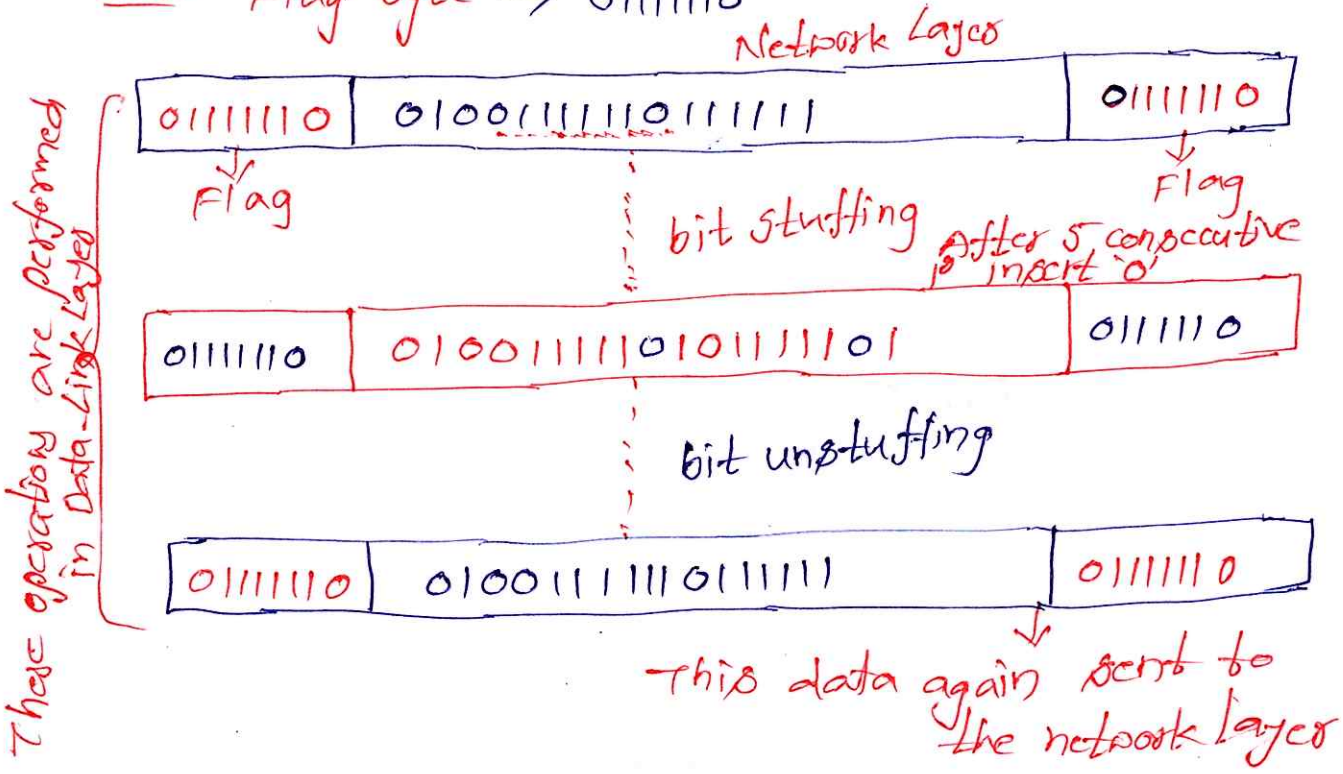

* FLAG → A bit patern that defines the begining and end bits in a frame.
* Header → It contains the source and destination address of the frame.
* payload → It contains the actual message.
* Trailer → It contains the error detection and error correction bits.

Ex:-




* Flag Bits with Bit Stuffing:- In this framing technique the begining & end of each frame a specific bit pattern is added.

Ex:- Flag byte → 01111110



# CN II

* **physical Layer coding violations** :- this method is used in networks where the physical medium's encoding has redundancy.

Ex:-

LAN's encoding → each bit of data is represented by two physical bits.

In Manchester encoding:- 1 → 10 → high-low
0 → 01 → low-high

For example if low-low, high-high } not used for data may be used for frame boundaries

∴ In order to create a division b/n frames in DLL this approach exploits the redundancy.

* **Error control**:- The DLL ensures error free link free for data transmission.
  * It deals with transmission errors
  * Sending acknowledgement frame in reliable connections.
  * Retransmitting lost frames
  * Identifying duplicate frames and deleting them.

* **Flow control:-** The data link Layer controls the flow control. When the sender sends frames at very high speed, a slow receiver may not be able to handle it. There may be loss of frames even if the transmission is error free.

---

## ➡ Error Detection and Correction

Detecting the errors while sending the data from Sender to Receiver is called Error detection. i.e some of the bits of data in the frame are corrupted i-e changed. correcting those bits by some methods is called correction.

There are 3 types of Errors.

* **Single bit Error:-** only one bit is changed during the transmission from sender to Receiver.

Exc:- Sender Receiver

0 1 0 1 1 0 ⟶ 0 1 0 1 0 0

* **Multiple bit error:-** when two or more bits are changed during the transmission.

Exc:- Sender Receiver

1 0 1 1 0 1 1 0 1 ⟶ 1 1 1 1 0 1 0 0 1

* **Burst Error:-** When several consecutive bits are changed.

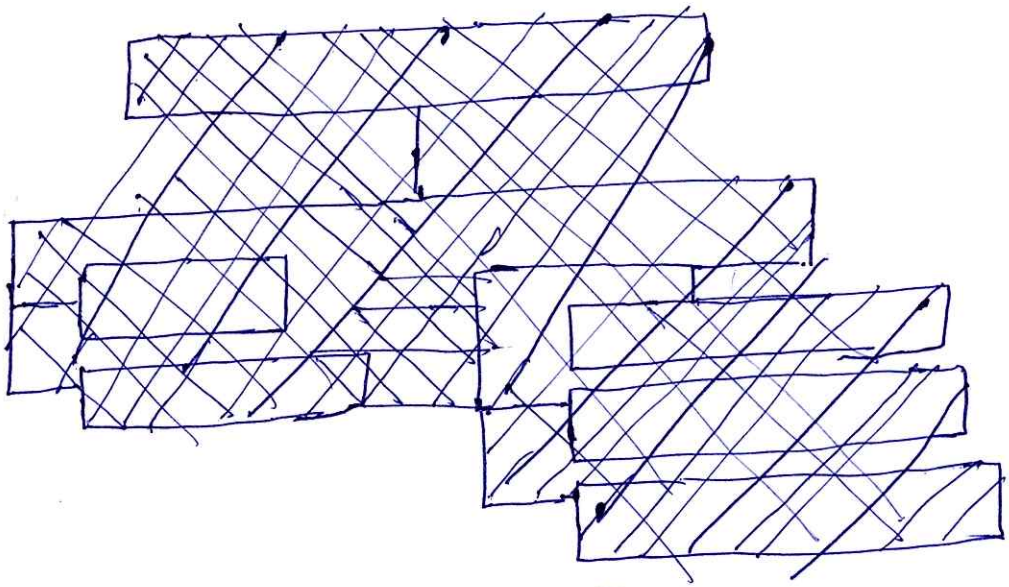
Exc:- Sender Receiver

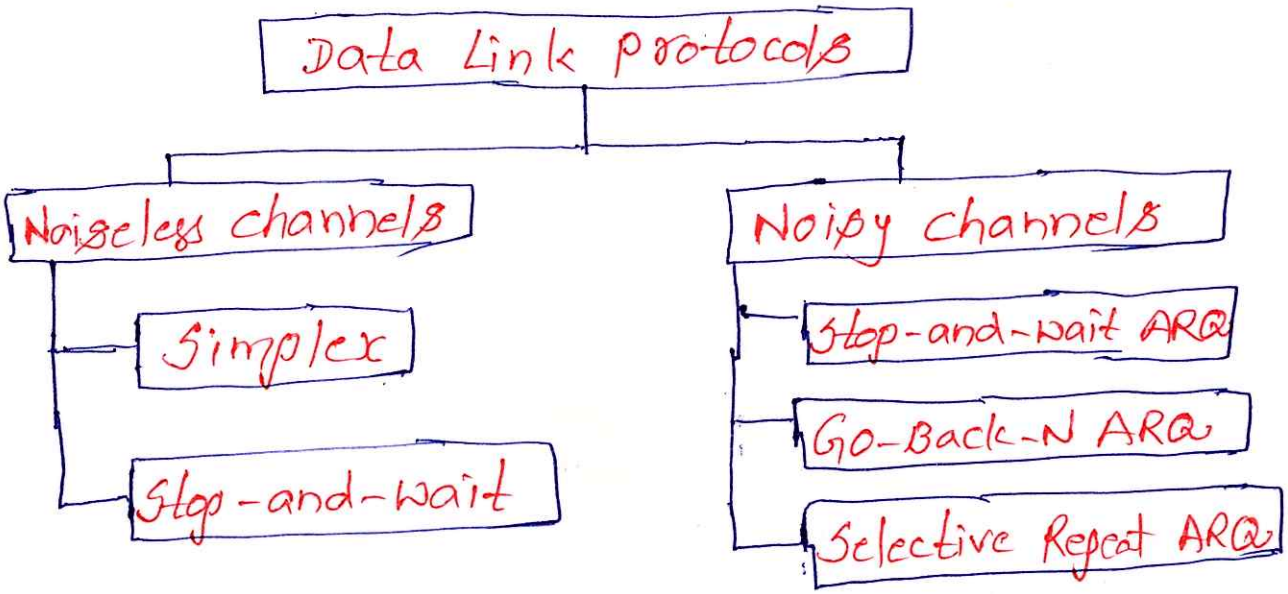
1 0 1 1 0 1 1 0 1 1 ⟶ 1 0 0 0 1 0 1 0 1

## → Elementary Data Link Protocols:-

Data Link layer protocols are designed to perform some basic functions like Framing, Error control and Flow control.

Data link layers can be broadly divided into two categories depending on whether the transmission is noiseless or noisy.



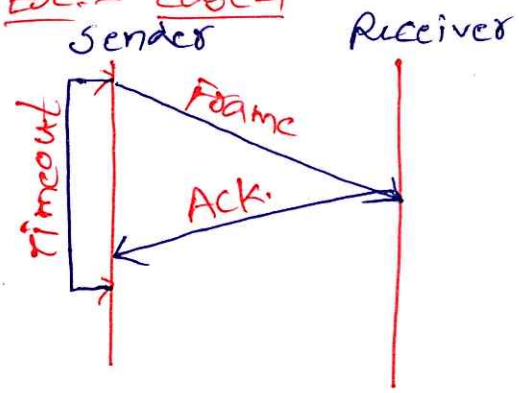


* **Simplex protocol:-** This is a unrestricted simplex protocol. This protocol works on assumption. i.e It can send any amount of data and the data does not have any errors. There is no any acknowledgement from receiver side. It is only one way transmission. The ~~receiver~~ sender can send the data any time. Receiver has infinite Buffer space to receive infinite amt. of data.

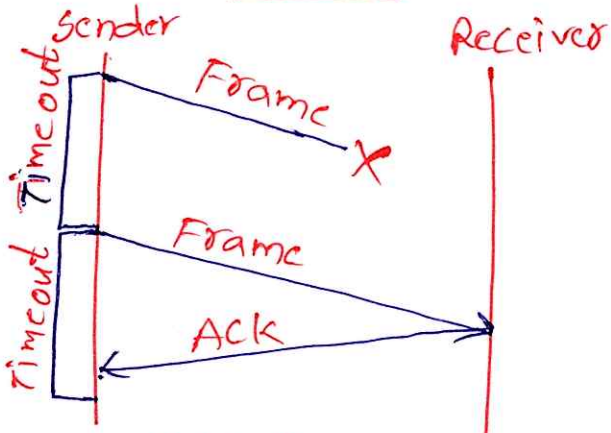
* **Stop-and-wait protocol:-** It is a noiseless protocol or error free protocol. In this protocol the sender sends the message and the message stops and waits ~~for~~ the receivers acknowledgement and then transmits the data. Even though it is a simple stop-and-wait protocal the receiver can have capability of sending the acknowledgement to the sender. Here the communication channel is error-free. There is no flow contol in this protocol.

* Stop-and-wait ARQ:- Stop-and-wait Automatic Repeat Request is a straightforward protocol. After sending one frame, the sender waits for an Ack. before transmitting the next frame. If the Ack. does not received by the receiver after a certain period of time, the sender times out and retransmits the original frame.

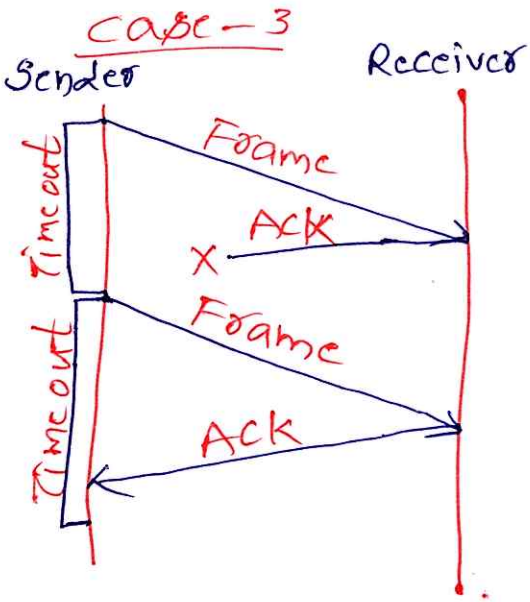
Ex:- case-1



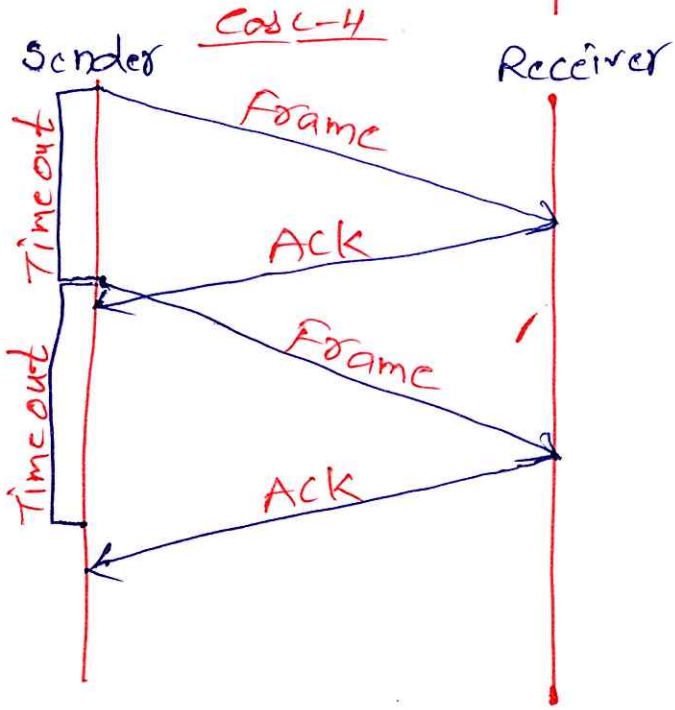

case-2




case-3

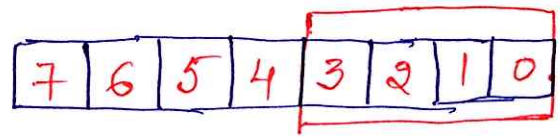



case-4

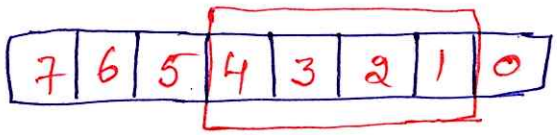


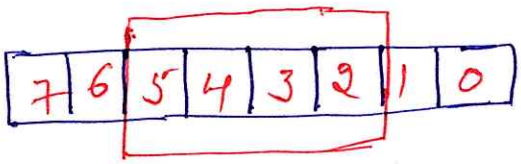
* **Go-Back-N ARQ:-** Go-Back-N ARQ is a sliding window protocol. Here 'N' is the window size. If N=4 the ~~sender~~ Receiver can send 4-frames ~~wit~~ at a time without expecting any Ack.

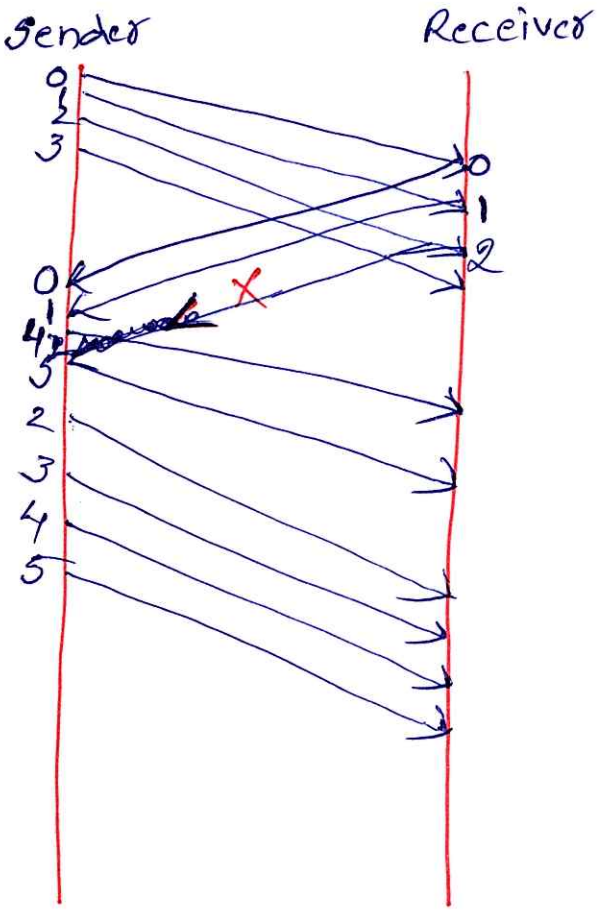
Go-Back-N ARQ uses the concept of pipelining i.e the sender can send multiple frames before receiving the Ack. for the first frame. If the Ack. of a frame is not received within a time period, all frames in the current window are retransmitted.




N=4



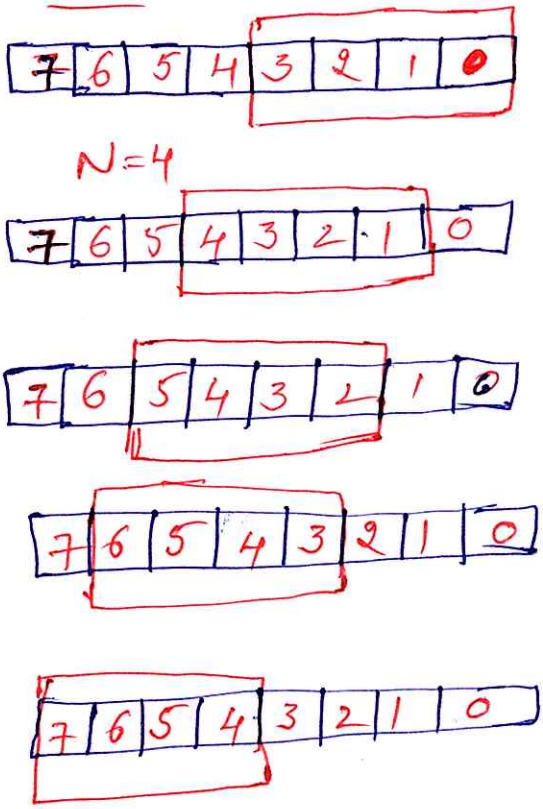



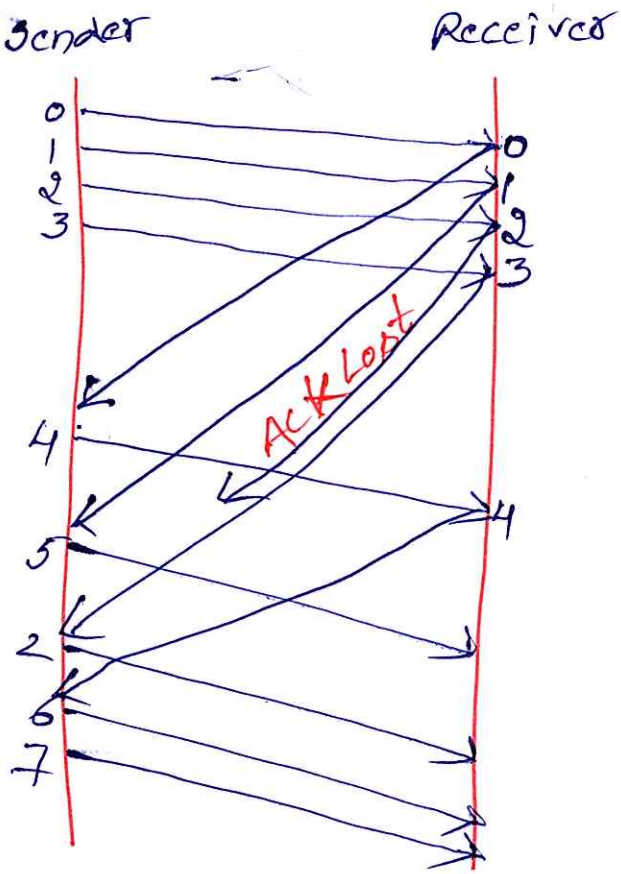



* Selective Repeat ARQ:- It is also a sliding window protocol. In selective Repeat ARQ only the lost frames are retransmitted. while correct frames are received and buffered.

The receiver while keeping track of sequence numbers, buffers the frames in memory and sends -ve Ack for only frames which is missing or damaged. The sender will retransmit data packets for which -ve Ack is received.

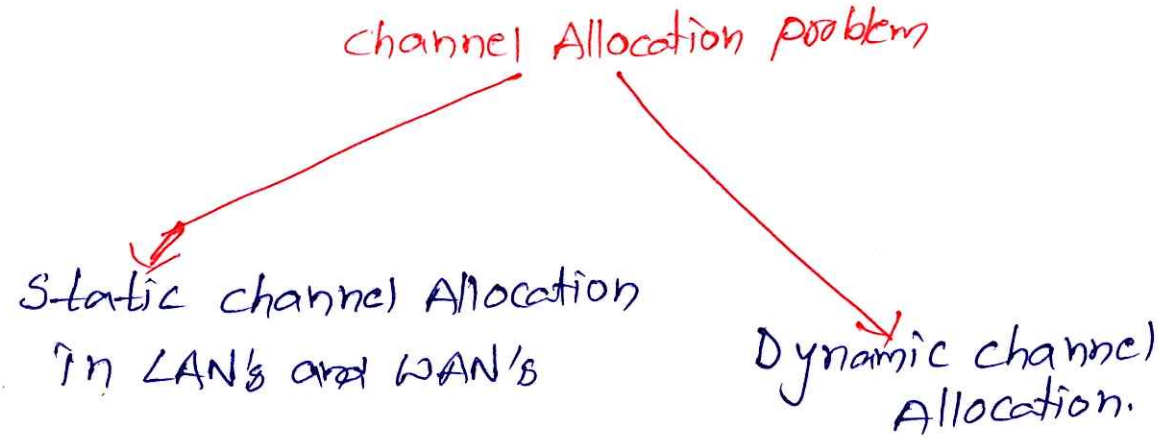
Ex:-



## The Channel Allocation Problem:-

Channel Allocation is a process in which a single network channel is divided and allotted to multiple users to carry users tasks. If there are 'N' no. of users and the channels are divided into 'N' equal-sized sub channels. Each user is assigned one sub-channel.




### * Static channel Allocation:-

A single channel is allocated among multiple competing users using FDM. Since each user has a private frequency band there is no interference b/n users. If there are 'N' users the bandwidth is divided into 'N' equal sized portions each user being assigned one portion.

## * Dynamic channel Allocation:-

The possible assumptions may include:

Station Model: Assumes that each of 'N' stations independently produce frames.

Single channel Assumption: In this allocation all stations are equivalent and can send and receive on that channel.

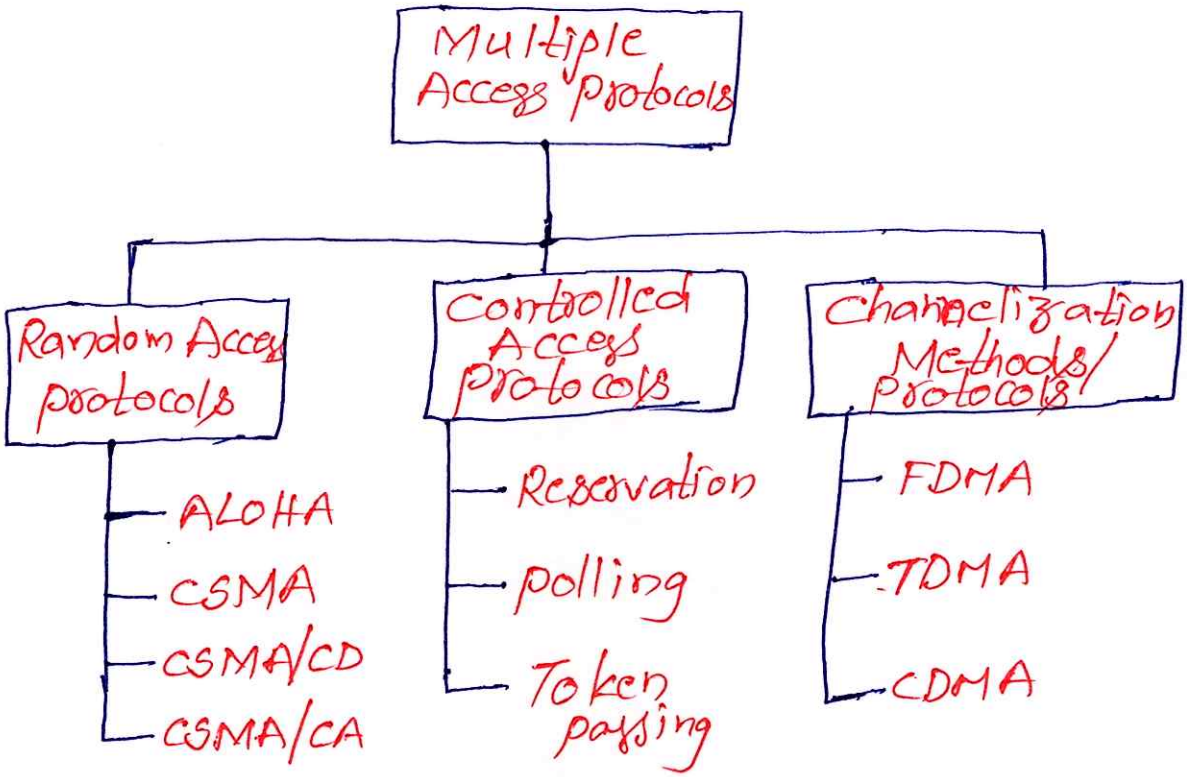
Collision Assumption: If two frames are overlaped in time, then that is collision. Any collision is an error and both the frames must be retransmitted. Stations can sense the channel before transmitting the data.

---

## → Multiple Access Protocols

Multiple Access Protocols are methods used in computer networks to control how data is transmitted when multiple devices are trying to communicate the same network. These protocols ensures that data packets are sent and received efficiently without collisions.

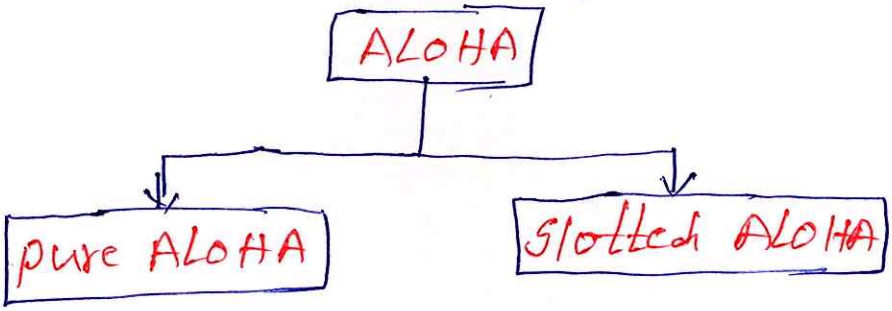
Multiple Access protocols are mainly classified into three types.




→ Rando Access Protocols:- Random Access protocols assign uniform priority to all connected nodes. Any node can send data if the transmission channel is idle. No fixed time or fixed sequence is given for data transmission. The four random access protocols are: ALOHA, CSMA, CSMA/CD & CSMA/CA.

* ALOHA:- Aloha is a random access protocol. It was actually designed for PLAN, but it is also applicable for shared medium. In this protocol multiple stations can transmit data at the same time and can lead to collision and data being garbled (damaged/corrupted).

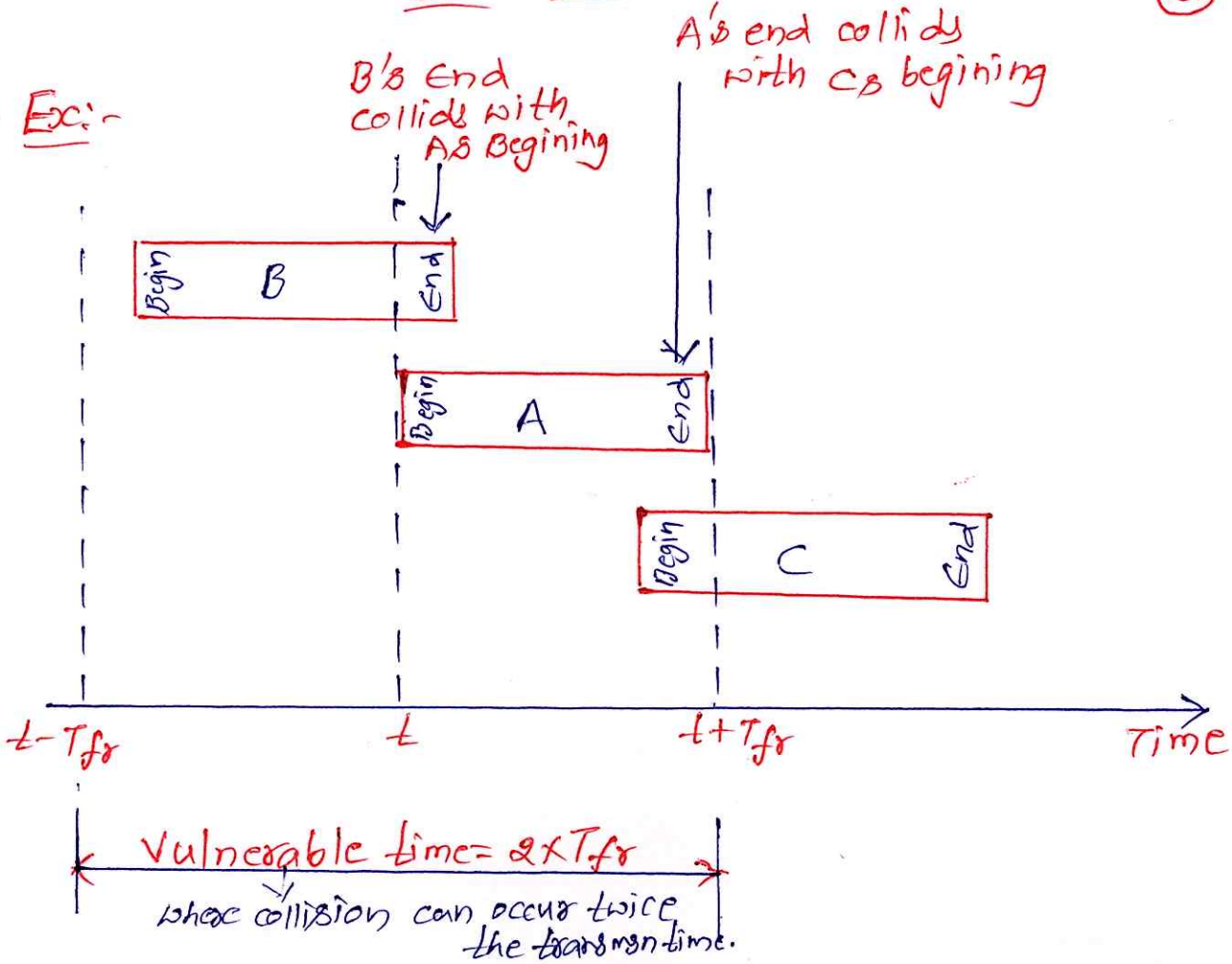
These are two types of ALOHA.




Pure Aloha:- whenever data is available for sending over a channel at stations, we we pure Aloha. When the multiple stations transmits data without knowing the channel is idle or not then the collision occurs and data may be lost. The sender may waits for the acknowledgement if he does not receive any Ack. he assumes that data packet is lost or corrupted. The sender waits for a random amount of time called back-off time (Tb) then re-transmits the data upto the receiver receives the data.

The throughput of pure Aloha is maximized when waves are of same length. If the first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted later.

Ex:-




Vulnerable time = 2×Tfr

where collision can occur twice the transmn time.

∴ Vulnerable time = 2×Tfr

← Throughput $S = G \times e^{-2G}$ ∴ where 'G' is the no. of stations wish to transmit in the same time.

The actual amt of data succesfly transmtd with a specific period.

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

For good efficiency we are transmitting one packet out of two.

$$\therefore S = \frac{1}{2} \times e^{-2 \times \frac{1}{2}}$$

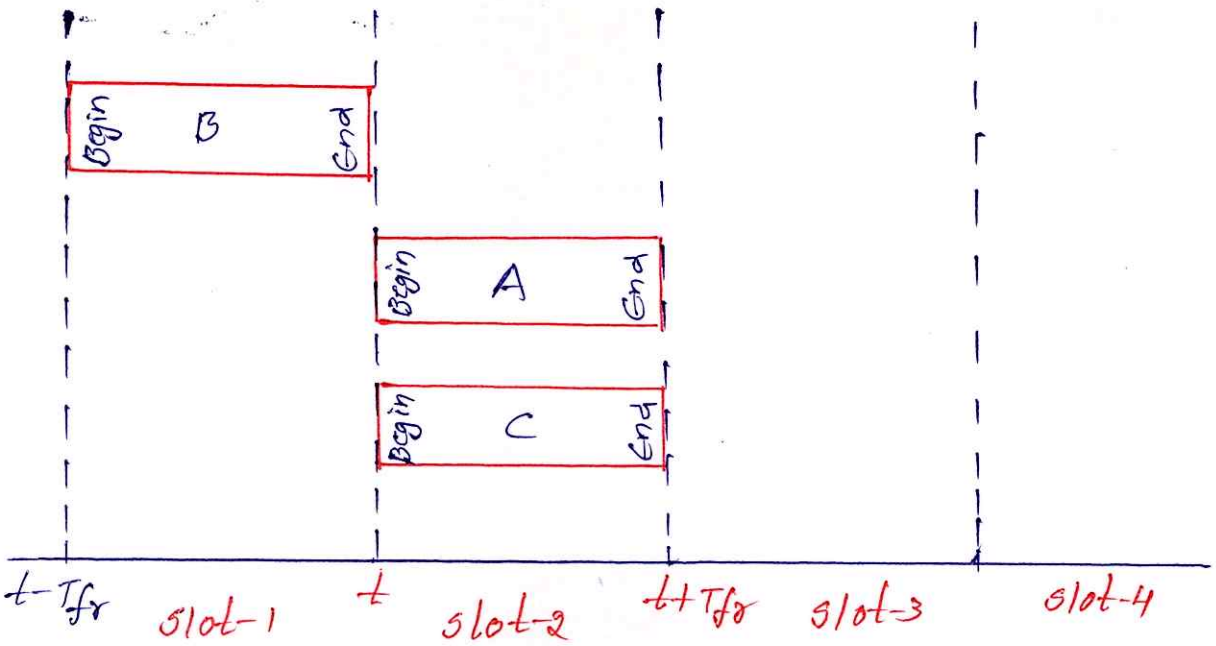
$$S = \frac{1}{2} \times e^{-1}$$

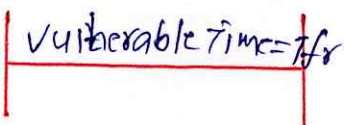
$$S = 0.184$$

$$\therefore S = 18.4$$

* **Slotted ALOHA:-** It was developed just to improve the efficiency of pure ALOHA as the chances for collision in pure aloha are high. The time of the shared channel is divided into discrete time intervals called slots. Sending of data is allowed only at the begining of these slots. If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.

Ex:-




∴ Vulnerable time $= T_{fr}$

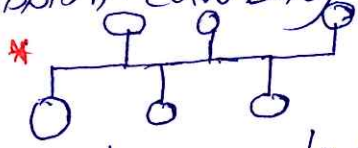
Throughput $S = G \times e^{-G}$

$= 1 \times e^{-1}$

$= 0.368$

$S = 36.8$

* CSMA:- CSMA means Carrier Sense Multiple Access protocol.
* carrier sense protocol
* To minimize the chances of collision and therefore, increase the performance, the CSMA method was developed.
* principle of CSMA: "sense before transmit" or "Listen before talk".
* Carrier busy = Transmission is taking place.
* carrier idle = No transmission is currently taking place.



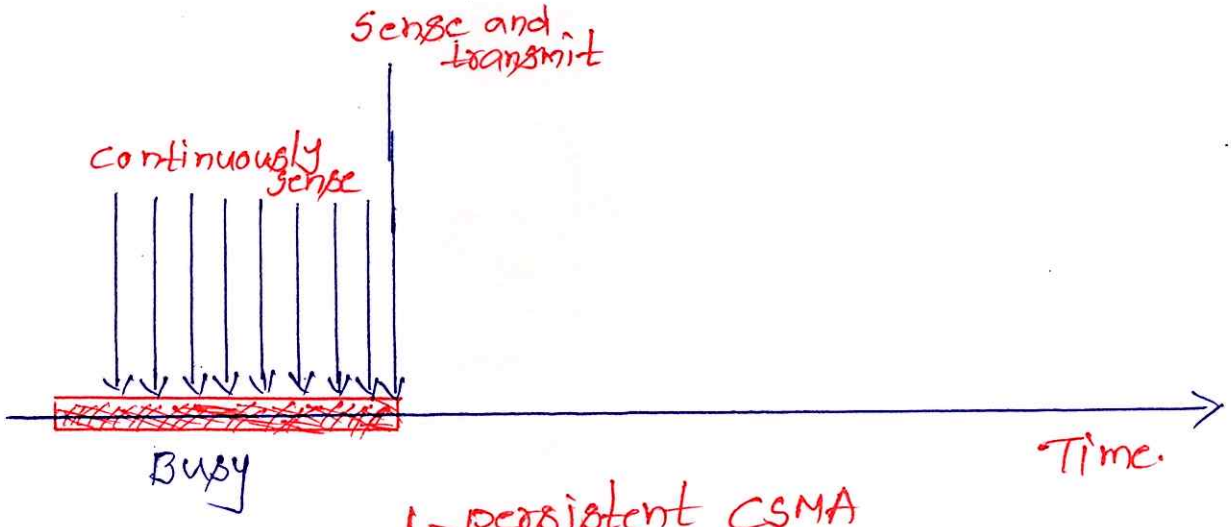
* The possibility of collision still exists because of propagation delay, a station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received.

Types of CSMA:-

* 1-persistent CSMA
* p-persistent CSMA
* Non-Persistent CSMA
* O-persistent CSMA

## *a. 1-persistent CSMA:-

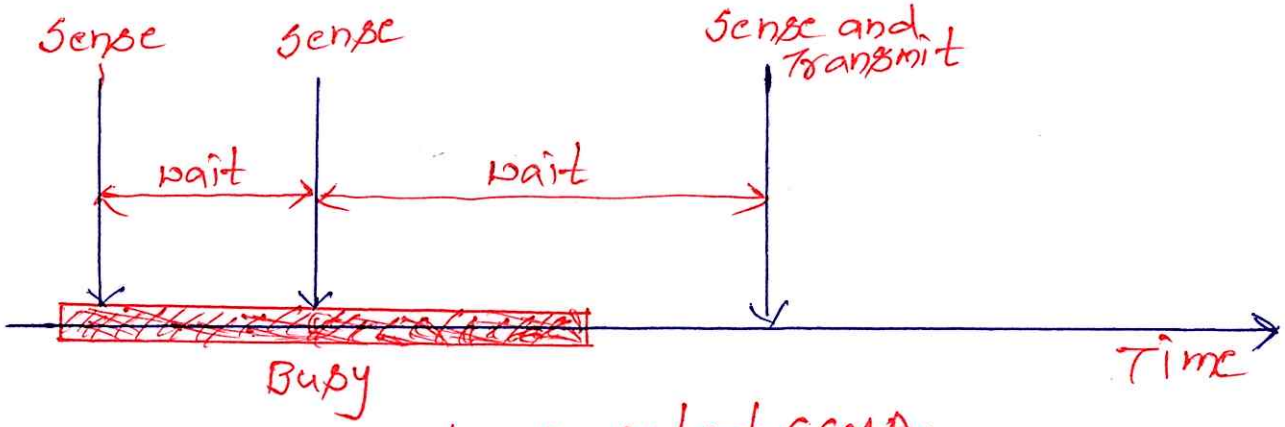
* Before sending the data, the station first listens to the channel to see if anyone else is transmitting the data at that time.
* If the channel is idle, the station transmits a frame.
* If busy, then it senses the transmission medium continuously until it becomes idle.
* Since the station transmits the frame with the probability of '1' when the carrier or channel is idle, this scheme of CSMA is called as 1-persistent CSMA.
* The longer the propagation delay, the more important this effect becomes, and the worse the performance of the protocol.




1-persistent CSMA

## * Non P-Persistent CSMA:-

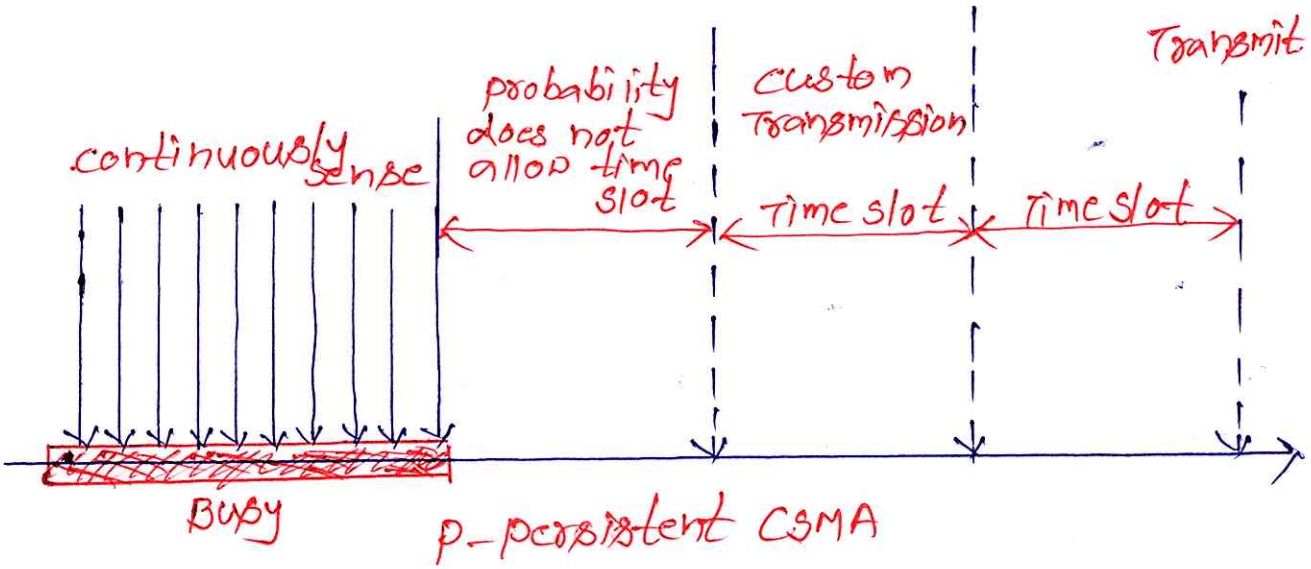
* Before sending a station senses the channel. If no one else is sending the station begins doing so itself.
* However, if the channel is already in use, the station does not continuously senses it for the purpose of seizing it immediately upon detecting the end of the previous transmission.
* Instead, it waits a random period of time and then repeats the algorithm consequently, this algorithm leads to better channel utilization but longer delays than 1-persistent CSMA.




Non-persistent CSMA.

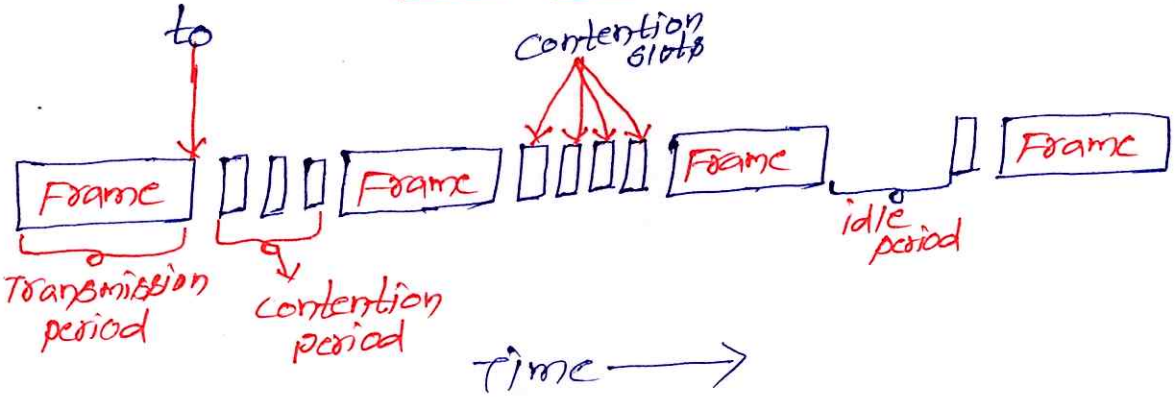
## * p-persistent CSMA :-

* It is applied for slotted channels.
* When a station becomes ready to send, it senses the channel.
* If it is idle, it transmits with a probability p.
* With a probability q = 1-p, it ~~defers~~ defers until to transmit or not until a later time.
  the next slot.
* If that slot is also idle, it either transmits or defers again, with probabilities p & q.
* This process is repeated until either the frame has been transmitted or another station has begun transmitting.
* In the later ~~time~~ case, the unlucky station acts as if there had been a collision. (i.e, it waits a random time and starts again).
* If the station initially senses the channel busy it waits until the next slot and applies the above algorithm.



* **0-Persistent CSMA:-** In 0-Persistent CSMA each node is assigned a transmission order by a supervisory node. It does not checkes the channel if it is busy, but waits a random period before retrying. If the channel is idle the station immediately transmits with a probability of 0, meaning it does not transmit immediately but waits a random period before retrying.

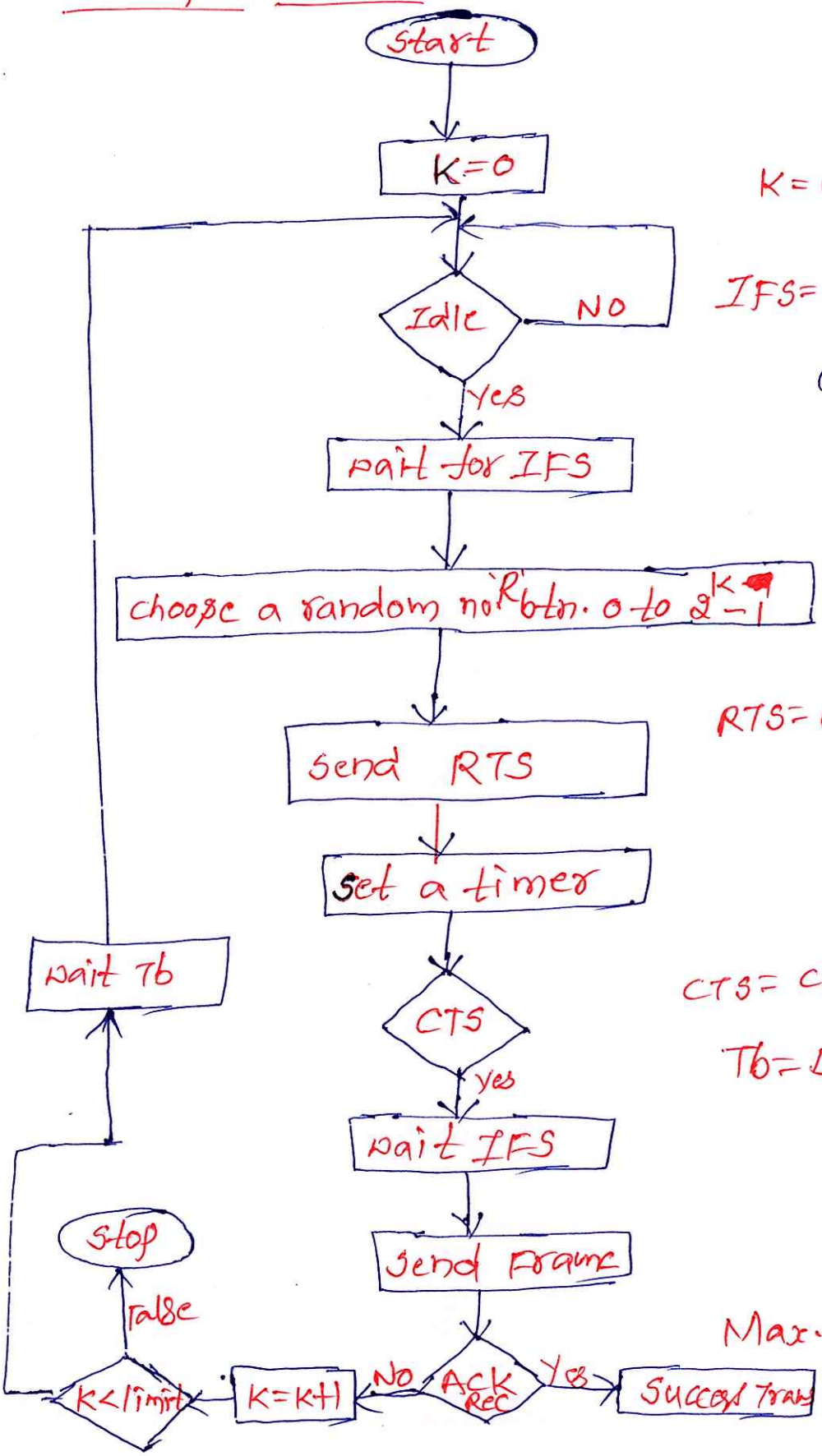
* **CSMA/CD:-** CSMA/CD means Carrier Sense Multiple Access Collision Detection.
  * If two stations sense the channel to be idle and begin transmitting simultaneously, they both detect collision almost immediately.
  * The frames are not transmitted, which are garbled anyway, they should stop transmitting the collision is detected.
  * Quickly terminating damaged frames saves time and bandwith.
  * This protocol is known as CSMA/CD is widely used on LAN's in the MAC sub-layer.
  * This Access method used by Ethernet: CSMA/CD




* At the point marked to a station has finished transmitting its frame.
* Any other station having a frame to send may now attempt to do so. If two or more stations decide to transmit simultaneously, there will be collision.
* collision can be detected by looking at the power or pulse width of the received signal and comparing it to the transmitted signal.
* Therefore CSMA/CD will consist of alternating contention and transmission periods, with idle periods occuring when all stations are quiet.

* **CSMA/CA:-** CSMA/CA means Carrier Sense Multiple Access collision Avoidance
  * CSMA/CA is a network multiple access method in which carrier sensing is used but nodes attempt to avoid collisions by begining transmission only after the channel is sensed to be idle.
  * CSMA/CA is used in wireless networks, like Wi-Fi that aims to prevent collision by having devices check if the channel is clear before transmitting.

# CSMA/CA Flow chart:-




K = No. of Attempts

IFS = Inter Frame Space (A random period of time)

RTS = Ready to send

CTS = clear to send

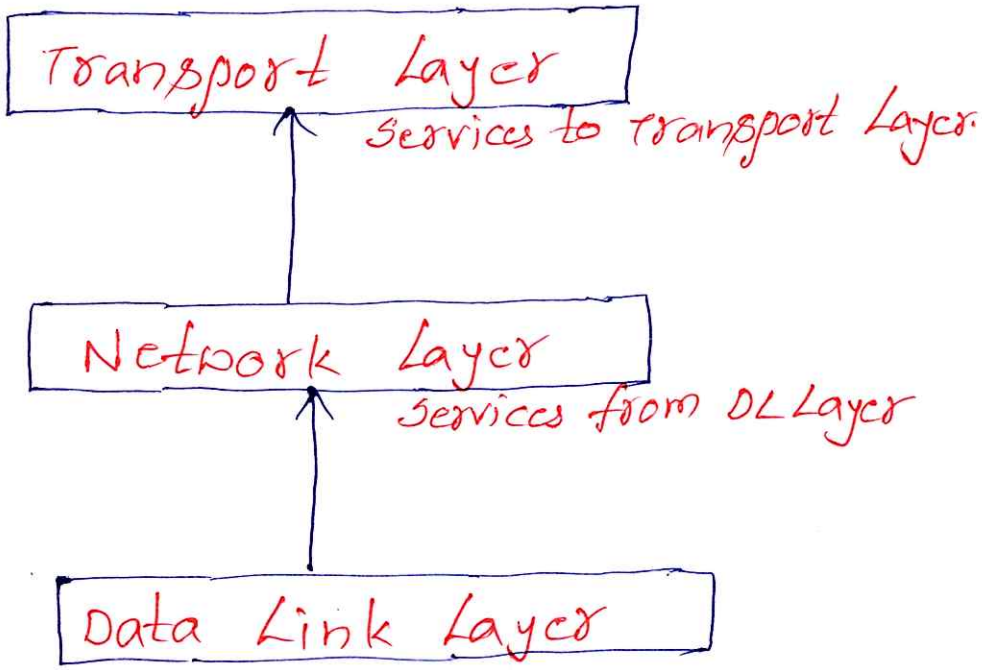
Tb = Backoff time

Max. no. of attempts = 14

# Computer Network UNIT-3

## ➡ Network Layer Design Issues :-

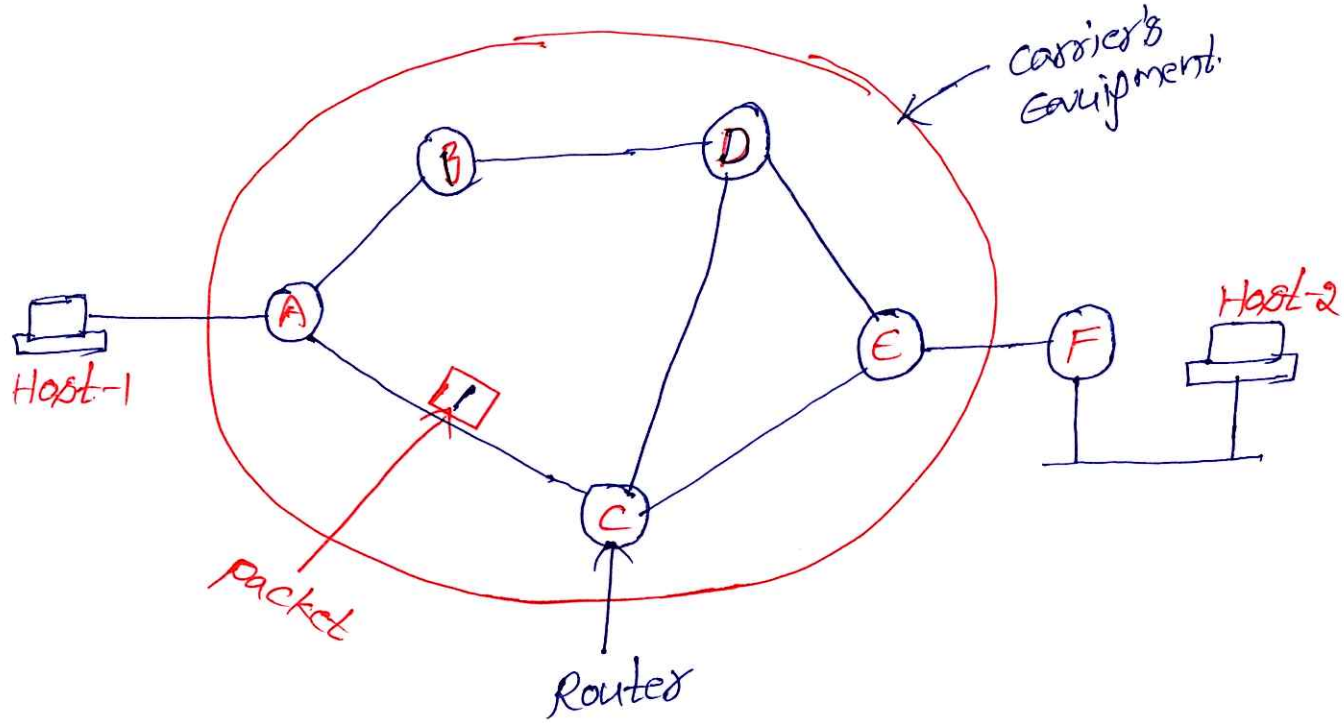
The Network Layer is located between Data Link Layer and Transport Layer. It receives services from Data Link Layer and provides services to the Transport Layer.




The following are the design issues in the Network Layer.

* Store-and-forward Packet Switching
* Services provided to Transport Layer
* Implementation of connectionless service
* Implementation of connection-oriented Service.
* Comparison of virtual-circuit and datagram networks.

## * Store-and-forward Packet Switching:-

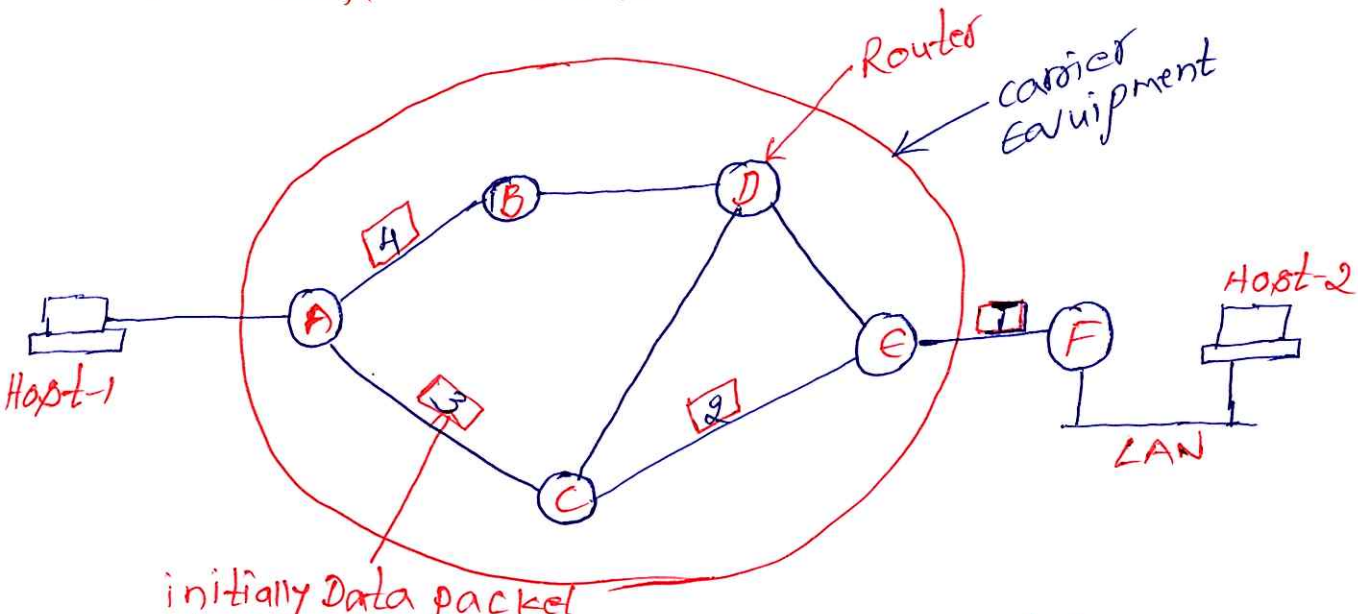



* A host with a packet to send, transmits it to the nearest router either on its own LAN or over a point-to-point link to the carrier (ISP).
* The router waits for the packet until it has fully arrived then the checksum can be verified.
* Then it is forwarded to the next nearest router along the path until it reaches the destination host, where it is delivered.
* This mechanism is called store-and-forward packet switching.

## * Services provided to Transport Layer:-

* The services should be independent of the router technology.
* The transport layer should be shielded (Hidden) from the number, type, and topology of the routers present.
* The network addresses made available to the transport layer should use a uniform numbering plan, even across LAN's and WAN's.

## * Implementation of connectionless Service:-




A's table

| | |
|---|---|
| A | – |
| B | B |
| C | C |
| D | B |
| E | C |
| F | C |

Later

| | |
|---|---|
| A | – |
| B | B |
| C | C |
| D | B |
| E | B |
| F | B |

C's Initially

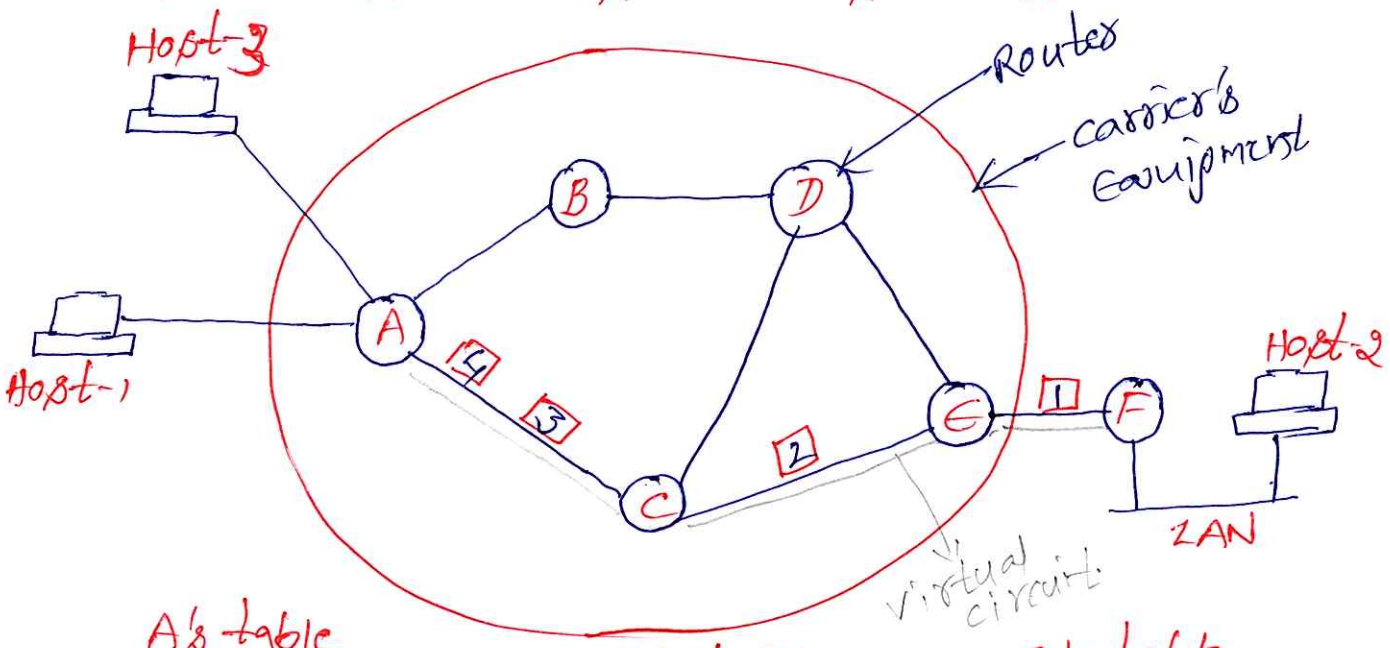
| | |
|---|---|
| A | A |
| B | A |
| C | – |
| D | D |
| E | E |
| F | E |

E's table

| | |
|---|---|
| A | C |
| B | D |
| C | C |
| D | D |
| E | – |
| F | F |

* For example out message is very long in size. So we have broken that message into 4 packets and sends each packet to router 'A' using some point-to-point protocol.
* After receiving the packets to the router-A the carrier takes over the responsibility that where the packets has to transfer to the nearest routers where the routers having the router tables. Each table entry is a pair consisting of a destination and the outgoing line to use for that destination. only directly connected lines can be used.
* However the router sent the packet-4 via router-B. The router-A assumes that already three packets 1, 2, 3 are sent via router-C. So it desided that the path ACE is busy or traffic jam may occur. So the router-A sent the packet-4 via router-B. The router table is also updated.
* The algorithm that manages the tables and makes the routing decisions is called the routing algorithm.

## * Implementation of connection-oriented services:-




A's table

| | |
|---|---|
| H1 | 1 |
| H3 | 1 |

In

| | |
|---|---|
| C | 1 |
| C | 2 |

out

C's table

| | |
|---|---|
| A | 1 |
| A | 2 |

In

| | |
|---|---|
| E | 1 |
| E | 2 |

out

E's table

| | |
|---|---|
| C | 1 |
| C | 2 |

In

| | |
|---|---|
| F | 1 |
| F | 2 |

out

* In connection-oriented service the virtual circuits avoid choosing a new route for every packet
* When a connection is established b/n the source host to destination host, the connection setup is stored in tables inside the routers.
* once the path have been established, the path will continue for data transmission where the same way that the telephone system works.
* When the connection is released, the virtual circuit is also terminated. In virtual circuit, each packet carries an identifier tells that which virtual circuit it belongs to.

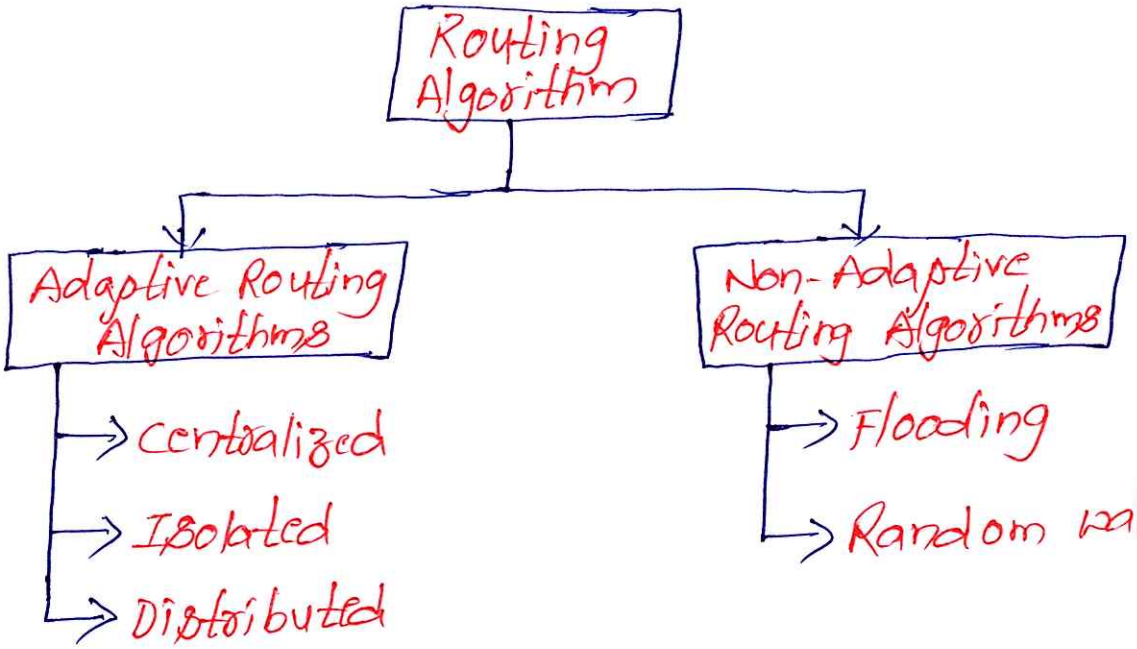
## * comparison of virtual circuit Vs Datagram network:-

| Issue | Datagram Network | Virtual-circuit Network. |
|---|---|---|
| circuit setup | Not Needed | Reavuired |
| Addressing | Each packet contains the full source and destination address. | Each packet contains a short VC number. |
| State Information | Routers do not hold state information about connections. | Each VC reavuires router table space per connection. |
| Routing | Each packet is routed independently | Route choosen when VC is set up all packets follow it. |
| Effect of router failure | None, except for packets lost during the crash. | All VCs that passed through the failed router are terminated. |
| Quality of service | Difficult | Easy if enough resource can be allocated in advanced for each VC. |
| congestion control | Difficult | Easy if enough resource can beallocted in advance for each VC |

## ⇒ Routing Algorithms :-

Routing means sending the data packets from source to destination in a desired path.

Routing Algorithms can be broadly classified into two types.




1. **Adaptive Routing Algorithms :-** Adaptive Routing Algorithm is also known as Dynamic Routing Algo. The routing decisions dynamicaly depending on the network conditions. It constructs the routing table depending upon the network traffic & Topology. The parameters of routing depends upon the hop count, transmit time and distance.

* Isolated:- This Algo. makes routing decision by using the local information. It does not depends on any other nodes information.

* centralized:- It finds the Least-cost path btn. source and destination nodes by using global knowledge about the network. So it is also known as Global routing Algo.

* Distributed:- It is a decentralized Algo. It computes Least-cost path btn. source and destination. It takes information from neighbours and makes routing decision.

2. Non-Adaptive Routing Algorithms:- Non-Adaptive Routing Algo. are also known as static Routing Algo. It constructs a static routing table to determine the path through which packets to be sent. the static routing table is constructed based upon the routing information stored in the routers when the network is booted up. It does not based on traffic or topology.

* **Flooding:-** In Flooding when a datapacket arrives at a router, it is sent to all the outgoing links except the one it has arrived first. The main problem in Flooding is that a node may contains several copies of a particular packet.

* **Random walk:-** This is a probabilistic Algo. where a data packet is sent by the router to any one of its neighbours randomly.

**Different Routing Algorithms:-**

* Shortest path Algorithm
* optimality principle
* Flooding
* Distance vector Routing
* Link state Routing
* Hierarchical Routing
* Broadcasting Routing.

* **Shortest path Algorithm:-** In shortest path Algo. we have two types.
  * Single-source shortest path Algo.
  * All-pair shortest path Algo.

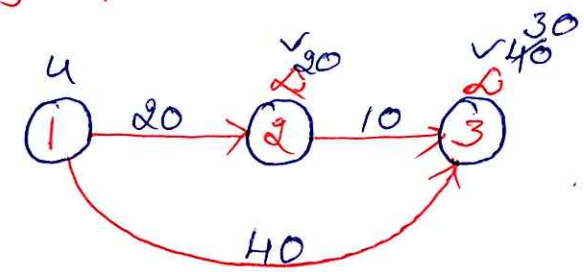
* **Single-source shortest path Algo:-** In single-source shortest path Algo. we will consider any one node as a source, and we have to find the shortest path from the source node to all the remaining nodes in the given graph. we have two types of single-source shortest path Algo. They are → Dijkstra's Algo.
  → Bellman-Ford Algo.

* ~~Dijkstras~~ **All-pair shortest path Algo:-** In All-pair shortest path Algo. we have to find the shortest path between a pair of vertices in the given graph. we have two types of All-pair shortest path Algo. They are → Floyd-warshall Algo.
  → Johnson's Algo.

## * Single-Source Shortest path Algo:-

1. **Dijkstras Algo:-** Dijkstras Algo. is a popular Algo. used to find the shortest paths from a starting node to all other reachable nodes in a weighted graph. this algorithm is particularly useful for finding the shortest routes in road networks.

### Working of Dijkstras Algo:-




**Relaxation**

$d(u) + c(u,v) < d(v)$

$d(v) = d(u) + c(u,v)$

**From 1 to 2:-**

$d(u) + c(u,v) < d(v)$

$0 + 20 < \infty$

$d(v) = 0 + 20 = 20$

**From 1 to 3**

$0 + 40 < \infty$

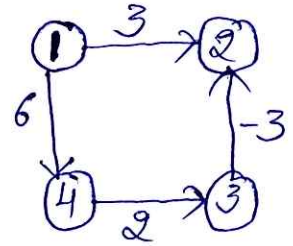
$d(v) = 0 + 40 = 40$

**From 2 to 3**

$20 + 10 < 40$

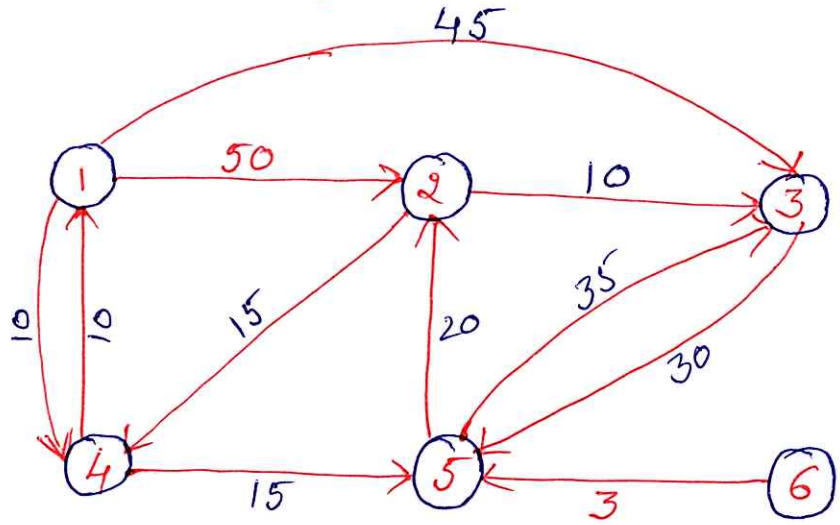
$30 < 40$

| source | destination | | |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 1 | ∞ | ∞ | ∞ |
| 1 | (3) | ∞ | 6 |
| 1, 2 | (3) | ∞ | (6) |
| 1, 2, 4 | (3) | (8) | (6) |

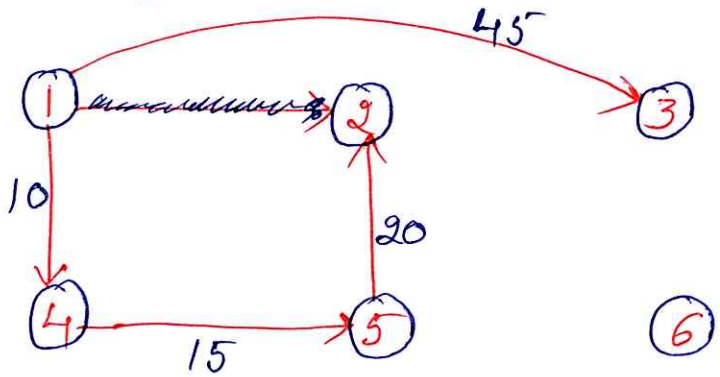


## * Dijkstra's Algo. using Directed Graph:-

Eg:-

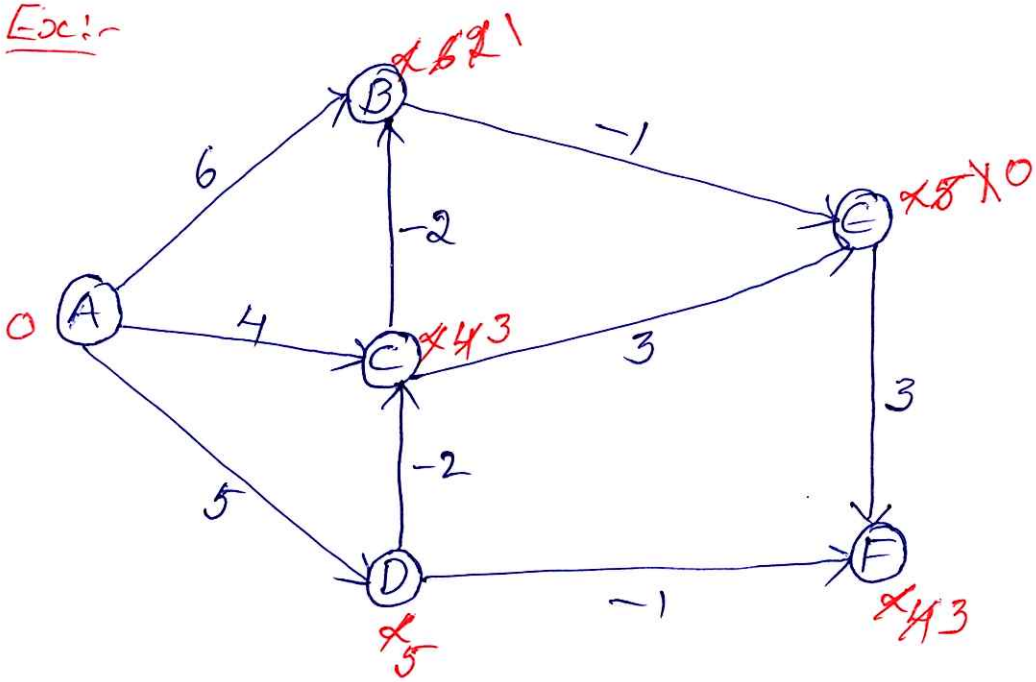



| source | Destination | | | | |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | ∞ | ∞ | ∞ | ∞ | ∞ |
| 1 | 50 | 45 | 10 | ∞ | ∞ |
| 1, 4 | 50 | 45 | 10 | 25 | ∞ |
| 1, 4, 5 | 45 | 45 | 10 | 25 | ∞ |
| 1, 4, 5, 3 | 45 | 45 | 10 | 25 | ∞ |
| 1, 4, 5, 3, 2 | 45 | 45 | 10 | 25 | ∞ |



2. **Bellman Ford Algo:-** It is a single source shortest path Algo. It works on negative edge weights for finding the shortest path from a single source. But it does not works in case of negative weight cycles. Bellman Ford Algo. is slower than Dijkstra's Algo. It works on relaxing all the edges in the given graph for "n-1" times where n = no of edges.

Ex:-




(A-B)(A-C)(A-D), (B,D), (C,E) (D,C), (D,F) (E,F) (C,B)

**Itr-2**

A-B → 2
A-C → 3
A-D → 5
B-E → 1
C-B → 1
C-E → 1
D-C → 3
D-F → 4
E-F → 4

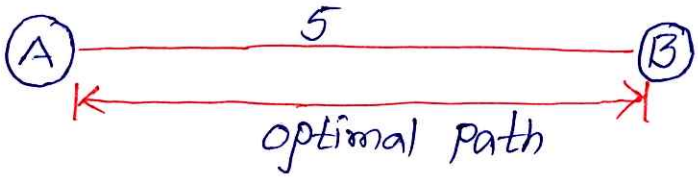
**Itr-1**

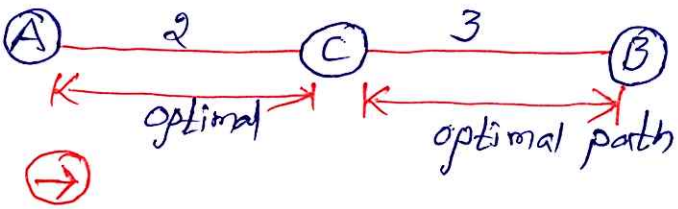
A-B → 6
A-C → 4
A-D → 5
B-E → 5
C-B → 2
C-E → 5
D-C → 3
D-F → 4
E-F → 4

| Itr-3 | Itr-4 | Itr-5 | Sol |
|---|---|---|---|
| A-B → 1 | A-B → 1 | A-B → 1 | A → 0 |
| A-C → 3 | A-C → 3 | A-C → 3 | B → 1 |
| A-D → 5 | A-D → 5 | A-D → 5 | C → 3 |
| B-E → 6 | B-E → 6 | B-E → 6 | D → 5 |
| C-B → 1 | C-B → 1 | C-B → 1 | E → 6 |
| C-E → 6 | C-E → 6 | C-E → 6 | F → 3 |
| D-C → 3 | D-C → 3 | D-C → 3 | |
| D-F → 4 | D-F → 3 | D-F → 3 | |
| E-F → 3 | E-F → 3 | E-F → 3 | |

After 5th iteration there is no any change in 4th & 5th iteration. Therefore there is no need to perform the 6th iteration. We can stop at 5th iteration and we can write the final solution.

➡ Optimality Principle:- (*)

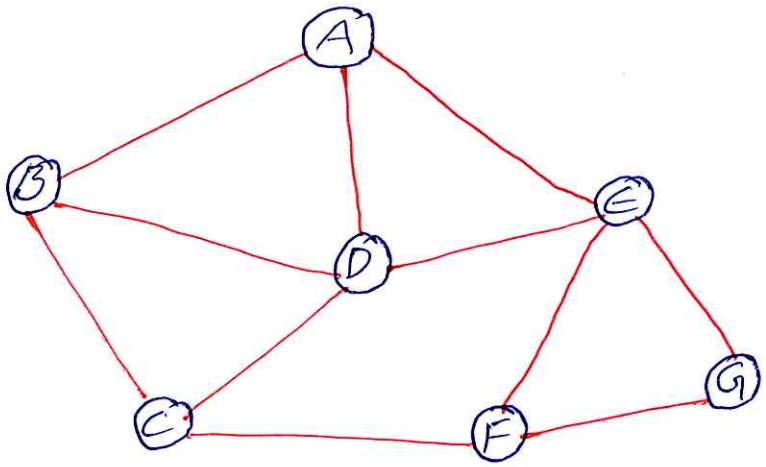



(→)

## Flooding:-

Flooding is a routing method where every incoming data packet is forwarded to every outgoing link except the one it arrived on. This ensures that the packet is delivered to every connected node on the network.




* An incoming packet to A, will sent to B, D, E
* B will send the packet to C and D
* C will send the packet to D, and F
* D will send the packet to ~~B, E and~~ E
* E will send the packet to F & G
* F will send the packet to G.
* Finally the packet is delivered to the destination G.

Types of Flooding:- There are three types of Flooding.
* controlled Flooding
* Uncontrolled Flooding
* Selective Flooding.

* Controlled Flooding:- In controlled Flooding they use some methods to transmit packets to the neighbouring nodes. The two popular Algos for controlled flooding are Seaquence Number controlled Flooding and Reverse path Forwarding.

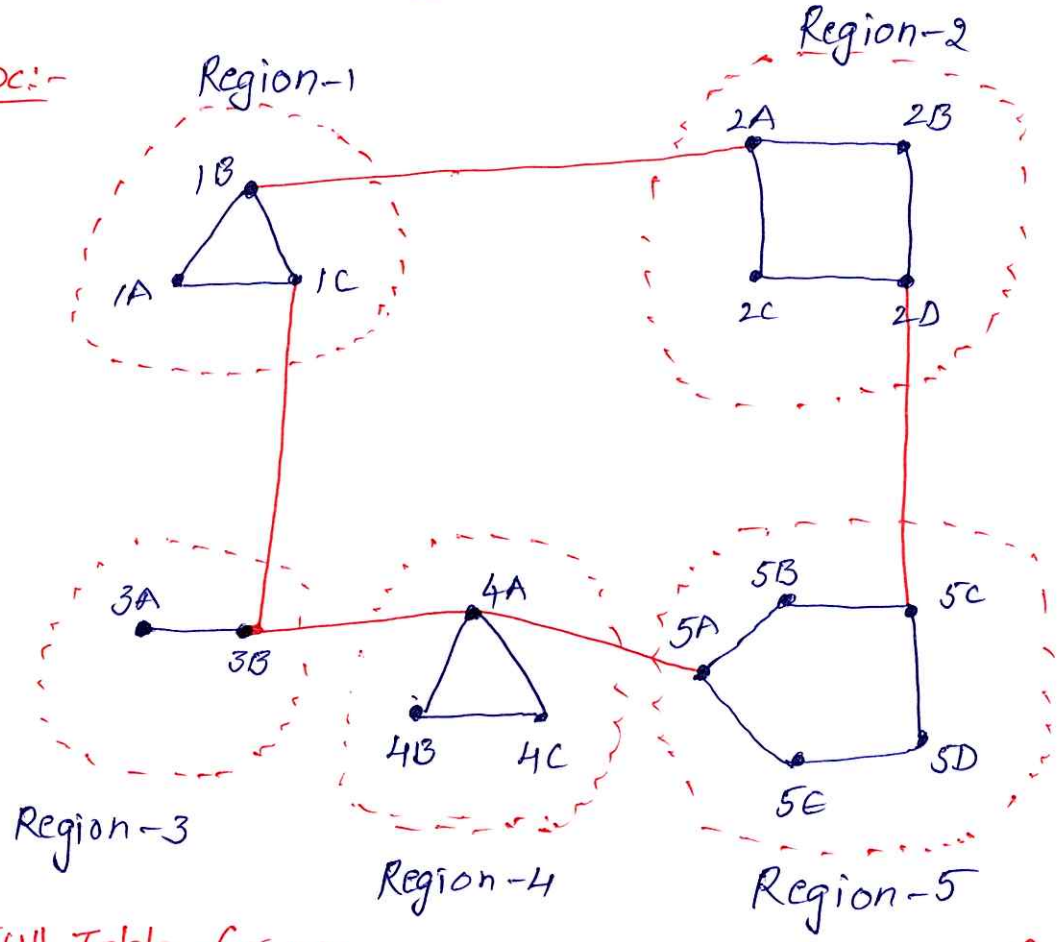
* Uncontrolled Flooding:- In Uncontrolled Flooding each router unconditionally transmits the incoming data packets to all its neighbours.

* Selective Flooding:- In selective Flooding the routers dont transmit the incoming packets to its neighbour routers. The routers will transmit data packets only along those paths which are heading towards approximately in the right direction instead of every available paths.

## Hierarchical Routing Algo:

* When the network size increases the no. of routers will also increase.
* We know that every router has a routing table which contains the details of all other ~~details~~ in routers.
* Therefore the routing table size increases. When the size of the router increases the routers can not handle the traffic efficiently.
* So we require large amount of memory and more band width.
* To overcome this problem we use Hierarchical routing. In Hierarchical routing the routers are divided into regions.
* Each router has complete details about how to route packets to destination with in its own region.
* But it does not have any idea about the internal structure of other region.
* So we use a Gateway router. The Gateway router knows the information about another region.

Ex:-




Full Table for 1A

| Dest | Line | Hops |
|---|---|---|
| 1A | — | — |
| 1B | 1B | 1 |
| 1C | 1C | 1 |
| 2A | 1B | 2 |
| 2B | 1B | 3 |
| 2C | 1B | 3 |
| 2D | 1B | 4 |
| 3A | 1C | 3 |
| 3B | 1C | 2 |
| 4A | 1C | 3 |
| 4B | 1C | 4 |
| 4C | 1C | 4 |
| 5A | 1C | 4 |
| 5B | 1C | 5 |
| 5C | 1B | 5 |
| 5D | 1C | 6 |
| 5E | 1C | 5 |

Hierarchical Table for 1A

| Dest | Line | Hops |
|---|---|---|
| 1A | — | — |
| 1B | 1B | 1 |
| 1C | 1C | 1 |
| 2 | 1B | 2 |
| 3 | 1C | 2 |
| 4 | 1C | 3 |
| 5 | 1C | 4 |

## Broadcasting Routing Algo.

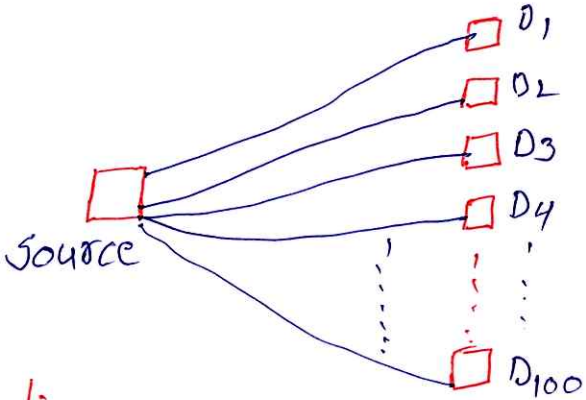
In Broadcasting Routing Algo. the data or signals are transmitted from one source to all the destinations within a network. Unlike routing (one-to-one communication) or multicasting routing (one-to-many communication) broadcast routing ensures that information reaches all devices or nodes within the network. Broadcasting routing is mainly used in radio, weather and Television communication.

Broadcasting routing can be implemented by using five methods.

1. point-to-point transmission.
2. Flooding.
3. Multi Destination Routing.
4. Reverse path Forwarding.
5. Spanning Trees.

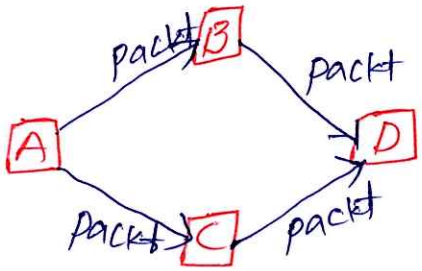
1. **Point-to-point Transmission:-** In this point-to-point transmission the source router will transmit the data packet to all the destination nodes separately. To do this the source router has to store all the destination addresses. Therefore the bandwidth of the router increases.

Ex:-



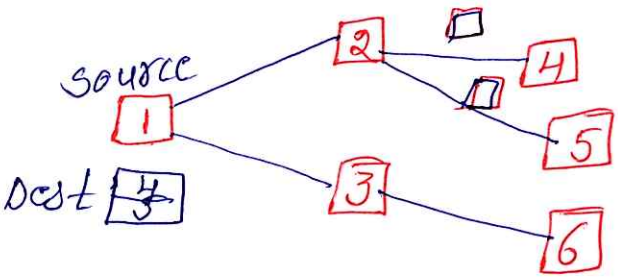

2. Flooding:- In Flooding when a data packet arrives at a router, it is sent to all the outgoing links except the one it has arrived first.

Ex:-



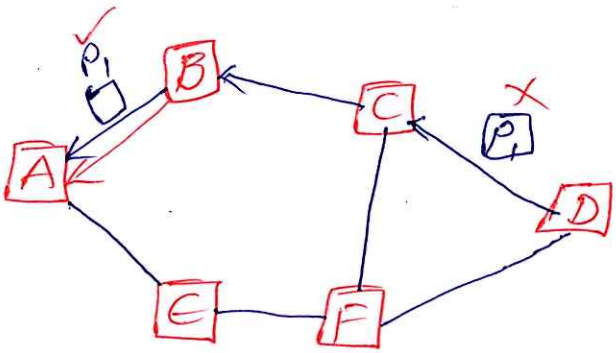

3. Multi Destination Routing:- In Multi Destination Routing the router will send the packets to multiple destinations by storing the address of multiple destination routers.

Ex:-



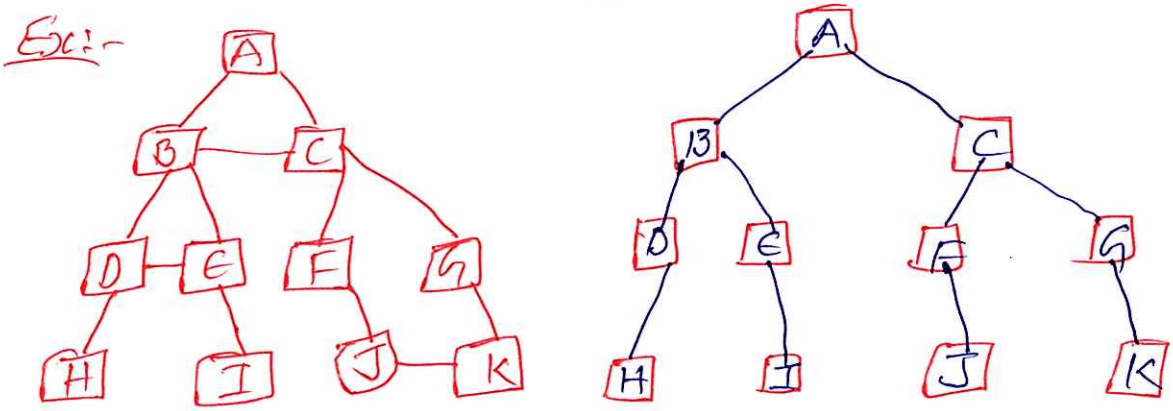
4. Reverse path forwarding:- In Reverse path Forwarding the concept of Flooding is also used. In Reverse path forwarding the routers will accept the packets from the shortest paths. If it receive packets from largest path the router will simply retransmits the packt to the source.

Ex:-




5. Spanning Tree:- A spanning tree is a tree structure where the routers are connected in a network will form a spanning tree network where 'n' routers are there the spanning tree is constructed with n-1 no. of links with out forming loops in the network.

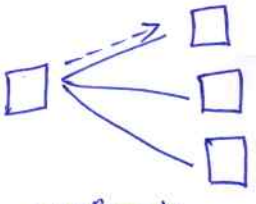
Ex:-



## Multicast Routing:

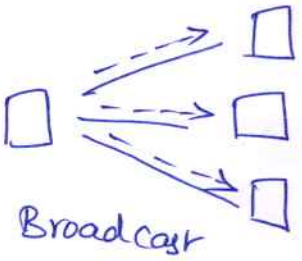
Multicast routing is a networking technique used to deliver data packets to multiple recipients simultaneously, often referred to as a multicast group. This approach is more efficient than sending individual packets to each recipient, especially when the number of recipients is large.

Unicast : The packet is sent from one sender to one receiver, i.e., it is one-to-one communication



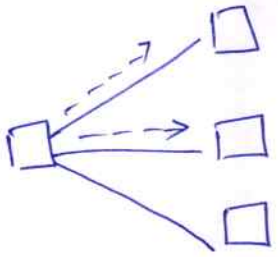
Unicast

Broadcast : The message is sent from one sender to all the connected and possible receivers. i.e., it is one to all communication



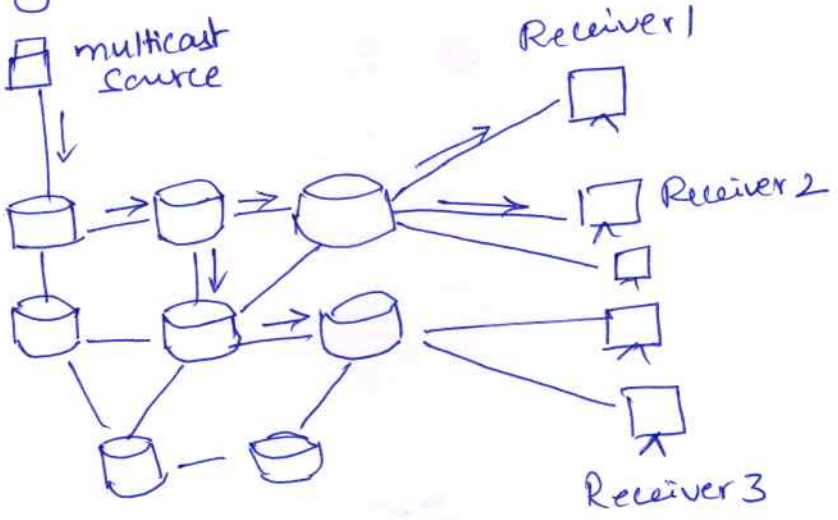
Broadcast

Multicast : The message is sent from one sender to all the receivers who are interested to receive that particular traffic, i.e., it is one-to-many communication.



multicast

It helps to reduce consumption, network load, and processing overhead on the sources.




The primary objective of multicast routing is to optimize the delivery of data to multiple receivers within the network. By sending one copy of data to each group of receivers, multicast routing conserves bandwidth and reduces network congestion.

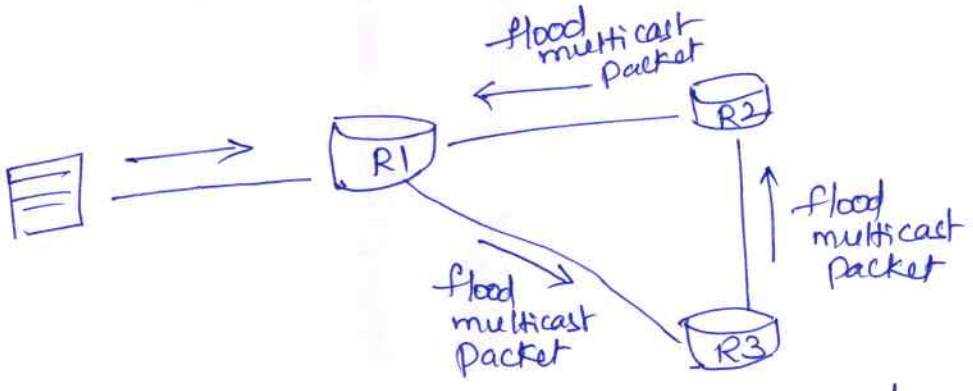
## Multicast Routing Protocols

Multicast routing protocols are classified into two categories.

1. Dense mode
2. sparse mode

1. Dense mode : Dense mode protocols assume that there are many receivers in the network and use flooding to

send data packets to all nodes. Then, nodes that are not interested in receiving the data prune themselves from the multicast tree by sending messages to upstream routers.




The following are the dense mode protocols.

Distance vector multicast Routing Protocol (DVMRP):

It is based on a distance vector routing algorithm and makes use of hop count as the metric. It floods multicast packets throughout the network and uses pruning messages to stop forwarding packets to unwanted branches.

Multicat open shortest path First (mospf)

It makes the use of the existing OSPF (Open Shortest path First) topology database in order to build multicast trees.

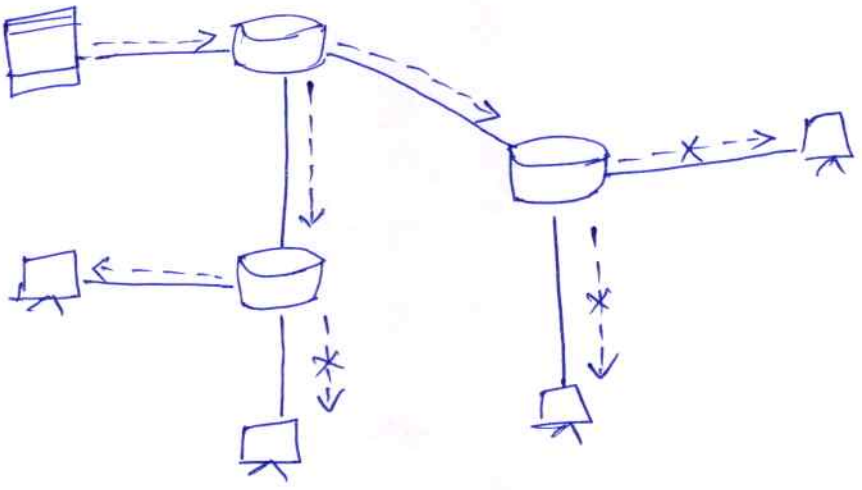
PIM Dense mode (PIM-DM)

PIM-DM protocol suitable for multicast receivers and Encess bandwidth. PIM-DM operates using a shared tree model, where all routers share the root for each multicast group.

2. Sparse mode

Sparse mode protocols assume that there are few receivers in the network. and use Explicit join messages to build multicast trees. They use a rendezvous point (RP) as a central node and connects that into

Sources and receivers. Receivers send join messages to the RP, which then forwards them to the sources.



PIM Sparse mode:

PIM Sparse mode is also a multicast routing protocol that operates, all network routers do not need transmitted multicast traffic.

In this, first joined router send the join message to a DR (Designated Router), which connects to the source of the multicast stream. then DR builds an SPT (Shortest Path Tree) to the source in order to forward the multicast packets.

Multicast Routing algorithms

1. Shortest path Tree (SPT) algorithm:

It builds a tree where the shortest path is calculated from to source to all receivers. It ensures minimal delay in data delivery.

2. Reverse path forwarding (RPF)

It prevents loops and ensures that multicast packets follow the correct path.

## Distance Vector Routing:-

Distance Vector Routing Algo. is also called as Bellman-Ford Algo. This Algo. is used to find the shortest route from one node to another node in the network.

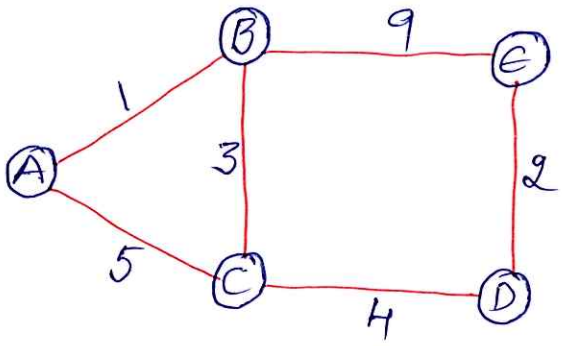
The Distance Vector Routing Algo. shares the information of routing table with the neighbouring routers and keeps the information up-to-date to select an optimal path from source to destination.

### Steps in DVR:-

* Each router prepares its routing table by their Local knowledge.
* Each router knows about the routers present in the network and distance to their neighbouring routers.
* Each router exchanges its distance vector with its neighbouring routers.
* Each router prepares a new routing table using the distance vectors obtained from its neighbours.
* This step is repeated for n-1 times. where n = no. of routers.

* DVR Algo: Direct Method

Ex:-




considerations

* Min. cost
* Min. Intermediate nodes.

* A to B

A - B → 1 ✓

A - C - B → 8

A - C - D - E - B → 20

* A to C

A - C → 5

A - B - C → 4 ✓

A - B - E - D → 16

* A to D

A - C - D → 9

A - B - C - D → 8 ✓

A - B - E - D → 12

* A to E

A - B - E → 10 ✓

A - C - B - E → 17

A - C - D - E → 11

A's table

| Destination | cost | Next Hop |
|---|---|---|
| A | 0 | A |
| B | 1 | B |
| C | 4 | B |
| D | 8 | B |
| E | 10 | B |

* B to A

B-A → 1 ✓

B-C-A → 8

B-E-D-C-A → 20

* B to C

B-C → 3 ✓

B-A-C → 6

B-E-D-C → 15

* B to D

B-E-D → 11

B-C-D → 7 ✓

B-A-C-D → 10

* B to E

B-E → 9 ✓

B-C-D-E → 9

B-A-C-D-E → 12

B's table

| Dest. | cost | Next Hop |
|---|---|---|
| A | 1 | A |
| B | 0 | B |
| C | 3 | C |
| D | 7 | C |
| E | 9 | E |

* C to A

C-A → 5

C-B-A → 4 ✓

C-D-E-B-A → 16

* C to B

C-B → 3 ✓

C-A-B → 6

C-D-E-B → 15

* C to D

C-D → 4 ✓

C-B-E-D → 14

C-A-B-E-D → 17

* C to E

C-D-E → 6 ✓

C-B-E → 12

C-A-B-E → 15

C's table

| Dest. | cost | Next Hop |
|---|---|---|
| A | 4 | B |
| B | 3 | B |
| C | 0 | C |
| D | 4 | D |
| E | 6 | D |

* DtoA

D-C-A → 9

D-C-B-A → 8 ✓

D-E-B-A → 12

* DtoB

D-C-B → 7 ✓

D-E-B → 11

D-C-A-B → 10

* DtoC

D-C → 4 ✓

D-E-B-C → 14

D-E-B-A-C → 17

D's table

| Dest. | cost | Next Hop |
|---|---|---|
| A | 8 | C |
| B | 7 | C |
| C | 4 | C |
| D | 0 | D |
| E | 2 | E |

DtoE

D-E → 2 ✓

D-C-B-E → 16

D-C-A-B-E → 19

---

* EtoA

E-B-A → 10 ✓

E-D-C-A → 11

E-D-C-B-A → 10

* EtoB

E-B → 9 ✓

E-D-C-B → 9

E-D-C-A-B → 12

E's table

| Dest. | cost | Next hop |
|---|---|---|
| A | 10 | B |
| B | 9 | B |
| C | 6 | D |
| D | 2 | D |
| E | 0 | E |

* EtoC

E-B-C → 12

E-D-C → 6 ✓

E-B-A-C → 15

* EtoD

E-D → 2 ✓

E-B-C-D → 16

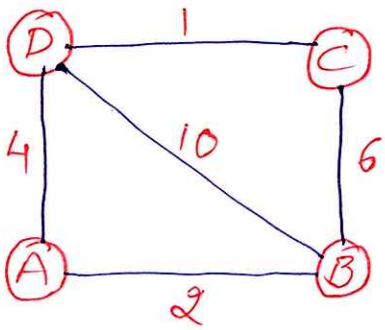
E-B-A-C-4 → 19

## * DVR Alg. Using Formula:-

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

where x = source node
y = Destination node
c = cost
v = Intermediate node
d = Distance.

Ex:-




### Iter-1

A's

| Dest | cost | Next |
|---|---|---|
| A | 0 | A |
| B | 2 | B |
| C | ∞ | — |
| D | 4 | D |

B's

| Dest | cost | Next |
|---|---|---|
| A | 2 | A |
| B | 0 | B |
| C | 6 | C |
| D | 10 | D |

C's

| Dest | cost | Next |
|---|---|---|
| A | ∞ | — |
| B | 6 | B |
| C | 0 | C |
| D | 1 | D |

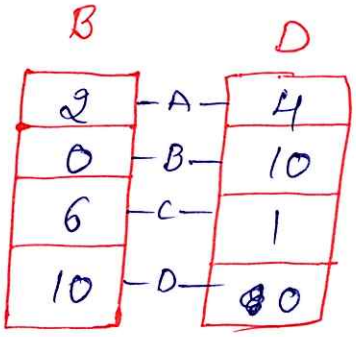
D's

| Dest | cost | Next |
|---|---|---|
| A | 4 | A |
| B | 10 | B |
| C | 1 | C |
| D | 0 | D |

### Iter-2

A's

| Dest | cost | Next |
|---|---|---|
| A | 0 | A |
| B | 2 | B |
| C | 5 | D |
| D | 4 | D |



* A to B

$$d(A-B) = \min \begin{cases} c(A-B)+d(B-B) \\ c(A-D)+d(D-B) \end{cases}$$

$$= \min \begin{cases} 2+0=2 \checkmark \\ 4+10=14 \end{cases}$$

* A to C

$$d(A-C) = \min \begin{cases} c(A-B)+d(B-C) \\ c(A-D)+d(D-C) \end{cases}$$

$$= \min \begin{cases} 2+6=8 \\ 4+1=5 \checkmark \end{cases}$$

* A to D

$$d(A-D) = \min \begin{cases} c(A-D)+d(D-D) \\ c(A-B)+d(B-D) \end{cases}$$

$$= \min \begin{cases} 4+0=4 \checkmark \\ 2+10=12 \end{cases}$$

B's

| Dest | cost | Next |
|---|---|---|
| A | 2 | A |
| B | 0 | B |
| C | 6 | C |
| D | 6 | A |

| A | C | D |
|---|---|---|
| 0 | $\infty$ | 4 |
| 2 | 6 | 10 |
| $\infty$ | 0 | 1 |
| 4 | 1 | 0 |

* B to A

$$d(B-A) = \min \begin{cases} c(B-A) + d(A-A) \\ c(B-D) + d(D-A) \\ c(B-C) + d(C-A) \end{cases}$$

$$= \min \begin{cases} 2+0 = 2 \checkmark \\ 10+4 = 14 \\ 6+\infty = \infty \end{cases}$$

* B to C

$$d(B-C) = \min \begin{cases} c(B-C) + d(C-C) \\ c(B-D) + d(D-C) \\ c(B-A) + d(A-C) \end{cases}$$

$$= \min \begin{cases} 6+0 = 6 \checkmark \\ 10+1 = 11 \\ 2+\infty = \infty \end{cases}$$

* B to D

$$d(B-D) = \min \begin{cases} c(B-D) + d(B-B) \\ c(B-A) + d(A-D) \\ c(B-C) + d(C-D) \end{cases}$$

$$= \min \begin{cases} 10+0 = 10 \\ 2+4 = 6 \checkmark \\ 6+1 = 7 \end{cases}$$

C's

| Dest. | cost | Next. |
|---|---|---|
| A | 5 | D |
| B | 6 | B |
| C | 0 | C |
| D | 1 | D |

B

| 2 |
|---|
| 0 |
| 6 |
| 10 |

D

| 4 |
|---|
| 10 |
| 1 |
| 0 |

* C to A

$$d(C-A) = \min \begin{cases} c(C-B) + d(B-A) \\ c(C-D) + d(D-A) \end{cases}$$

$$= \min \begin{cases} 6+2=8 \\ 1+4=5 \checkmark \end{cases}$$

* C to B

$$d(C-B) = \min \begin{cases} c(C-B) + d(B-B) \\ c(C-D) + d(D-B) \end{cases}$$

$$= \min \begin{cases} 6+0=6 \checkmark \\ 1+10=11 \end{cases}$$

* C to D

$$d(C-D) = \min \begin{cases} c(C-D) + d(D-D) \\ c(C-B) + d(B-D) \end{cases}$$

$$= \min \begin{cases} 1+0=1 \checkmark \\ 6+10=16 \end{cases}$$

D's

| Dest. | cost | Next Hop |
|---|---|---|
| A | 4 | A |
| B | 6 | A |
| C | 1 | C |
| D | 0 | D |

| A |
|---|
| 0 |
| 2 |
| ∝ |
| 4 |

| B |
|---|
| 2 |
| 0 |
| 6 |
| 10 |

| C |
|---|
| ∝ |
| 6 |
| 0 |
| 1 |

* D to A

$$d(D-A) = \min \begin{cases} C(D-A) + d(A-A) \\ C(D-B) + d(B-A) \\ C(D-C) + d(C-A) \end{cases}$$

$$= \min \begin{cases} 4+0 = 4 \checkmark \\ 10+2 = 12 \\ 1+\infty = \infty \end{cases}$$

* D to B

$$d(D-B) = \min \begin{cases} C(D-B) + d(B-B) \\ C(D-C) + d(C-B) \\ C(D-A) + d(A-B) \end{cases}$$

$$= \min \begin{cases} 10+0 = 10 \\ 1+6 = 7 \\ 4+2 = 6 \checkmark \end{cases}$$

* D to C:

$$d(D-C) = \min \begin{cases} C(D-C) + d(C-C) \\ C(D-B) + d(B-C) \\ C(D-A) + d(A-C) \end{cases}$$

$$= \min \begin{cases} 1+0 = 1 \\ 10+6 = 16 \\ 4+\infty = \infty \end{cases}$$

Iter-3

A's

| Dest | cost | Next |
|---|---|---|
| A | 0 | A |
| B | 2 | B |
| C | 5 | D |
| D | 4 | D |

B

| |
|---|
| 2 |
| 0 |
| 6 |
| 6 |

D

| |
|---|
| 4 |
| 6 |
| 1 |
| 0 |

* AtoB

$$d(A-B) = \min \begin{cases} C(A-B)+d(B-B) \\ C(A-D)+d(D-B) \end{cases}$$

$$= \min \begin{cases} 2+0=2 \checkmark \\ 4+6=10 \end{cases}$$

* AtoC

$$d(A-C) = \min \begin{cases} C(A-B)+d(B-C) \\ C(A-D)+d(D-C) \end{cases}$$

$$= \min \begin{cases} 2+6=8 \\ 4+1=5 \checkmark \end{cases}$$

* AtoD:

$$d(A-D) = \min \begin{cases} C(A-D)+d(D-D) \\ C(A-B)+d(B-D) \end{cases}$$

$$= \min \begin{cases} 4+0=4 \checkmark \\ 2+6=8 \end{cases}$$

B's

| Dest | cost | Next |
|---|---|---|
| A | 2 | A |
| B | 0 | B |
| C | 6 | C |
| D | 6 | A |

| A | C |
|---|---|
| 0 | 5 |
| 2 | 6 |
| 5 | 0 |
| 4 | 1 |

* B to A

$$d(B-A) = \min \begin{cases} c(B-A)+d(A-A) \\ c(B-C)+d(C-A) \end{cases}$$

$$= \min \begin{cases} 2+0=2 \checkmark \\ 6+5=11 \end{cases}$$

* B to C

$$d(B-C) = \min \begin{cases} c(B-C)+d(C-C) \\ c(B-A)+d(A-C) \end{cases}$$

$$= \min \begin{cases} 6+0=6 \checkmark \\ 2+5=7 \end{cases}$$

* B to D:

$$d(B-D) = \min \begin{cases} c(B-D)+d(D-D) \\ c(B-A)+d(A-D) \\ c(B-C)+d(C-D) \end{cases}$$

$$= \min \begin{cases} 10+0=10 \\ 2+4=6 \checkmark \\ 6+1=7 \end{cases}$$

C's

| Dest | cost | Next |
|---|---|---|
| A | 5 | D |
| B | 6 | B |
| C | 0 | C |
| D | 1 | D |

B

| 2 |
|---|
| 0 |
| 6 |
| 6 |

D

| 4 |
|---|
| 6 |
| 1 |
| 0 |

* C to A

$$d(C-A) = \min \begin{cases} c(C-B) + d(B-A) \\ c(C-D) + d(D-A) \end{cases}$$

$$= \min \begin{cases} 6+2=8 \\ 1+4=5 \checkmark \end{cases}$$

* C to B

$$d(C-B) = \min \begin{cases} c(C-D) + d(D-B) \\ c(C-D) + d(D-B) \end{cases}$$

$$= \min \begin{cases} 6+0=6 \checkmark \\ 1+6=7 \end{cases}$$

* C to D

$$d(C-D) = \min \begin{cases} c(C-D) + d(D-D) \\ c(C-B) + d(B-D) \end{cases}$$

$$= \min \begin{cases} 1+0=1 \checkmark \\ 6+6=12 \end{cases}$$

D's

| Dest | cost | Next |
|---|---|---|
| A | 4 | A |
| B | 6 | A |
| C | 1 | C |
| D | 0 | D |

| A | B | C |
|---|---|---|
| 0 | 2 | 5 |
| 2 | 0 | 6 |
| 5 | 6 | 0 |
| 4 | 6 | 1 |

* D to A:

$$d(D-A) = \min \begin{cases} c(D-A) + d(A-A) \\ c(D-B) + d(B-A) \\ c(D-C) + d(C-A) \end{cases}$$

$$= \min \begin{cases} 4+0=4 \checkmark \\ 10+2=12 \\ 1+5=6 \end{cases}$$

* D to B

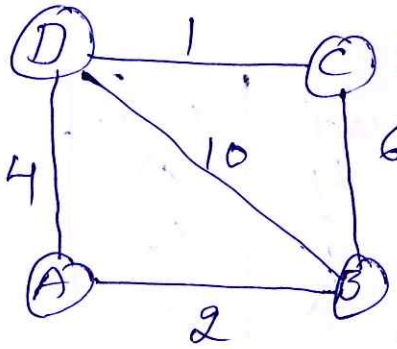
$$d(D-B) = \min \begin{cases} c(D-B) + d(B-B) \\ c(D-A) + d(A-B) \\ c(D-C) + d(C-B) \end{cases}$$

$$= \min \begin{cases} 10+0=10 \\ 4+2=6 \checkmark \\ 1+5=6 \end{cases}$$

* D to C

$$d(D-C) = \min \begin{cases} c(D-D) + d(C-C) \\ c(D-A) + d(A-C) \\ c(D-B) + d(B-C) \end{cases}$$

$$= \min \begin{cases} 1+0=1 \checkmark \\ 4+5=9 \\ 10+6=16 \end{cases}$$




A's

| Dst | cost | Next |
|---|---|---|
| A | 0 | A |
| B | 2 | B |
| C | 5 | D |
| D | 4 | D |

A to B

A-B → 2 ✓

A-D-B → 14

A-D-C-B → 11

A to C

A-B-C → 8

A-D-C → 5 ✓

A-B-D-C → 13

A-D-B-C → 20

A to D

A-D → 4 ✓

A-B-D → 12

A-B-C-D → 9

~~A to B~~

B to A

B-A → 2 ✓

B-D-A → 14

B-C-D-A → 11

B to C

B-C → 6 ✓

B-D-C → 11

B-A-D-C → 7

B to D

B-D → 10

B-A-D → 6 ✓

B-C-D → 7

B's

| Dst | cost | Next |
|---|---|---|
| A | 2 | A |
| B | 0 | B |
| C | 6 | C |
| D | 6 | A |

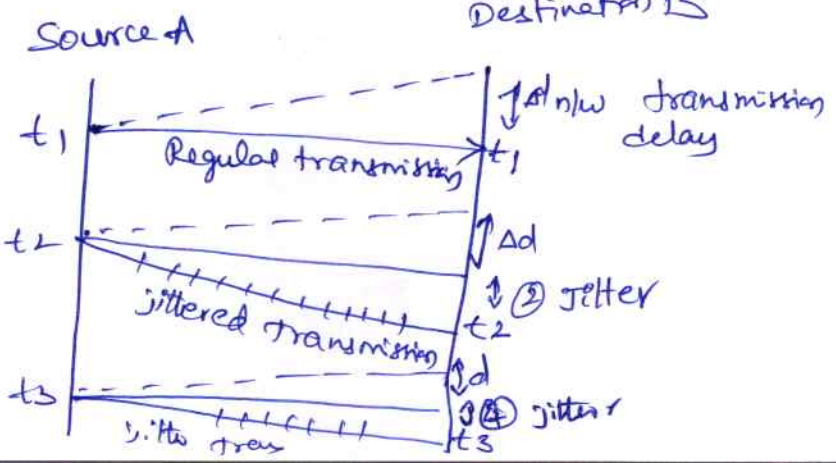
# Quality of Service

It measures the capability of a n/w to provide high quality services to an end user. It designates the mechanisms and technologies for managing data traffic and controlling n/w resources.

* The primary goal of QoS is to prioritize critical applications and specific types of data.
* QoS technologies seek to increase throughput, lower latency and reduce packet loss.

A n/w flow is a sequence of packets going from one device to another. To quantify the QoS on a n/w, we need to measure the flow by several metrics.

1. **Reliability**: Reliability is the degree to which a n/w guarantees delivering data packets.
   * The bit error rate (BER) is the ratio of the number of erroneous bits and total no of received bits.
2. **Delay or latency**: It shows how much time a data packet needs to travel from its source to destination.
3. **Jitter**: The jitter refers to the scenario when packets are not delivered at regular interval of time.
   * It is the change in the amount of latency for a set of packets delivering a singular service.



Band width :

The band width refers to the transmission capasity of the network. i.e., how much data we can transfer at a given time.

Techniques to improve the QoS :

we have several mechanisms to improve the QoS in a n/w.

1. Classification and marking :

we label each packet with the appropriate class by changing a field in the packet header. This process is called marking.

Classification is sorting the packets for labeling.

Both are implemented within a router or a switch.

2. Queuing and Scheduling

when a router receives packets from different flows, it stores them in different buffers we call queues. Differentiate the traffic in queues by order of priority. packets belongs to the same type of class from a singular queue. Based on the result of classification, each traffic receives a specific type of techniques.

3. Policing and shaping

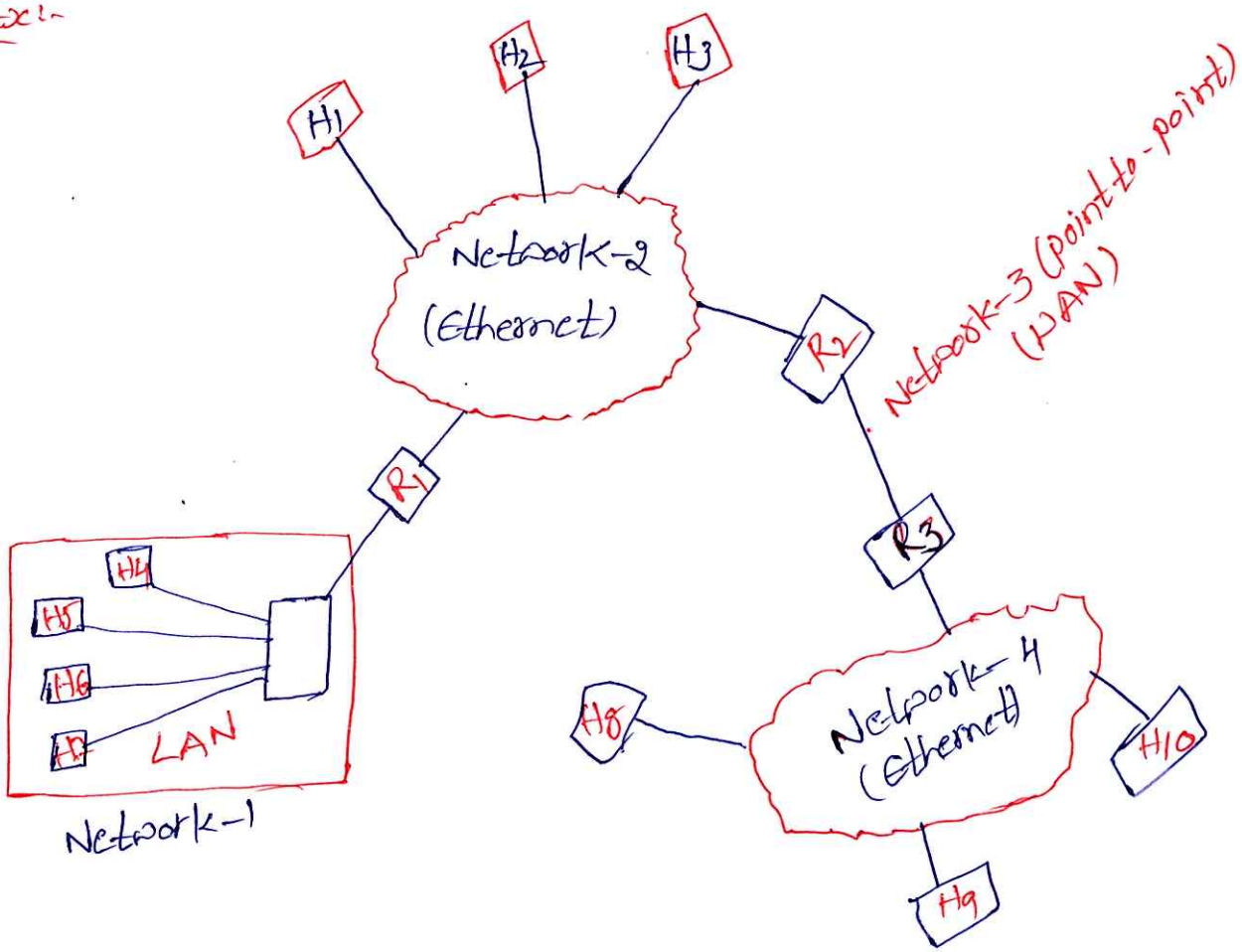
policing and shaping are bandwidth-modeling techniques to manage the amount and rate of traffic.

## Internetworking:-

Internetworking is the word which combines the words "Inter" and "networking" which denotes a connection btn. completely distinct nodes.

Internetworking is the process or technique of connecting different networks by using some intermediary devices such as routers or gateways. It is a technique of connecting computer devices with different operating systems and protocols of a network to another different network.

Ex:-



* Internet:- The internet is a public and global communication network that provides direct connectivity to anyone.

* Intranet:- An Intranet is a corporate LAN or WAN that uses Internet technology and is secured behind company's firewalls. The internet services can be accessed only the authorised persons of that organization.

* Extranet:- An extranet is a private network similar to an internet, but typically open to external parties such as business partners, suppliers, key customers etc.

* How Network can be connected:- Networks can be interconnected by different devices. In the physical layer networks are connected by different network devices.

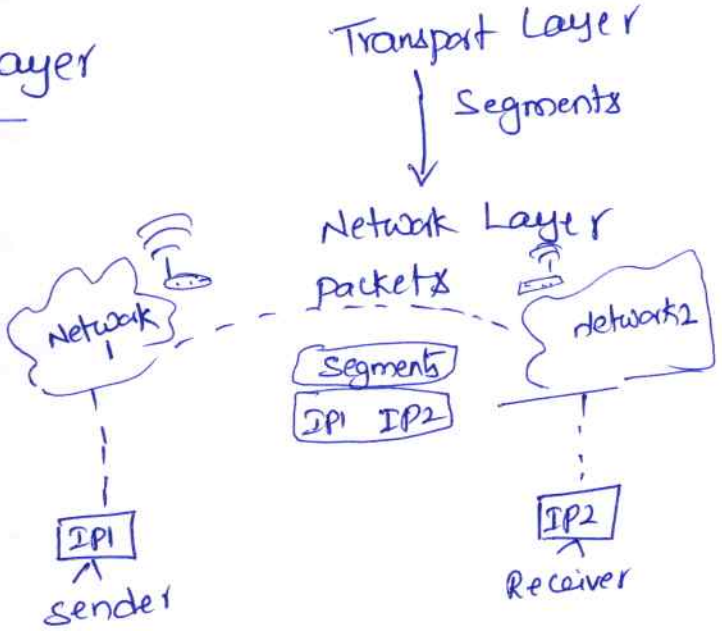
* components or Principles of Internetworking:-

1. Routers:-
2. Switches:-
3. protocols:- It supports two protocols such as OSI & TCP/IP model.
4. Gateways:-
5. Modems:-
6. Bridges:-

# The network layer in the internet

The network layer, also known as Layer 3 of the OSI model or the Internet layer in the TCP/IP model, is responsible for routing and transferring data packets between devices across interconnected networks. It makes the internet possible by connecting different types of networks into one global system.

## Functions of the Network Layer




* **Local Addressing:** Assigns unique IP addresses to devices, ensures each has an identifiable location on the network. This is fundamental for data transmission between hosts.

* **Routing:** Determines the optimal path for data packets through routers, from the source to the destination, based on routing tables and network algorithms like OSPF, RIP or BGP.

* **Packet forwarding:** Moves packets through routers hop-by-hop using destination IP addresses.

* **Fragmentation and Reassembly:** Splits large packets into smaller fragments to match a network's maximum transmission unit (MTU) and reassembles them at the destination.

Error Reporting and Control: Utilizes protocols to report network issues such as unreachable destinations.

Subnetting and Network Addren Translation (NAT): Allows efficient IP addren management and enables private networks to connect to the Internet security.

Protocols operating at this layer:

- IP (Internet protocol - IPV4/IPV6): Core protocol for addressing and routing data packets across networks.
- ICMP (Internet Control Message protocol): manages error reporting and network diagnostics.
- ARP/RARP (Addren Resolution/Reverse ARP): Translates addresses between IP and MAC formats.
- NAT and IPSec: Enhance security and manage network addressing.

Importance of Network Layer in the Internet

- connects multiple diverse networks into one large internetwork (Internet).
- Supports end-to-end data transmission regardless of physical or data link technologies.
- provide scalable communication through hierarchical addressing and dynamic routing.
- Enables interoperability, allowing devices worldwide to communicate seamlessly.

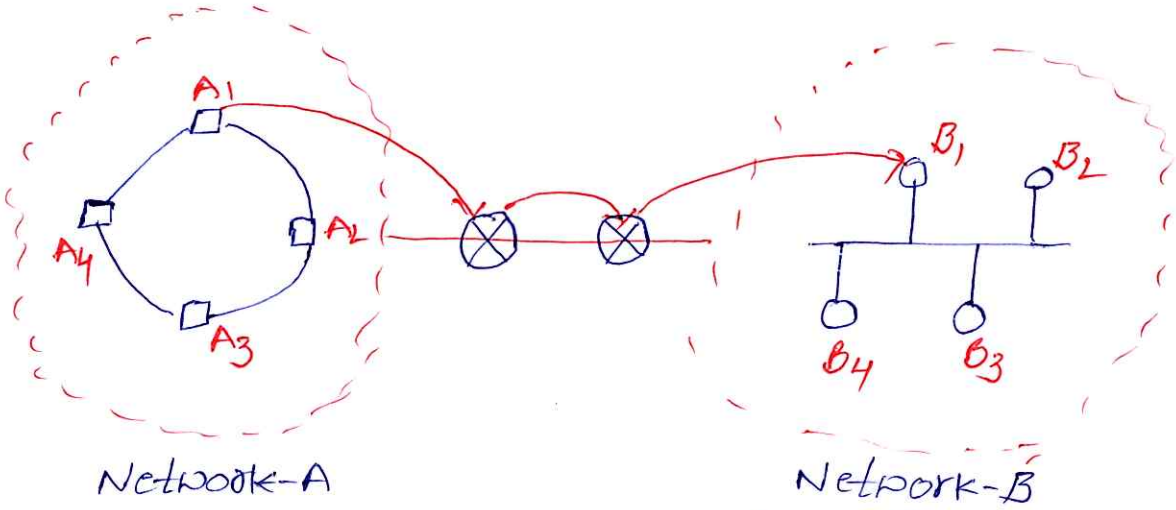
# Computer Networks
## UNIT - IV

### Services Provided by Transport Layer:-

The Transport Layer is the second layer in the TCP/IP model and fourth layer in the OSI model. It is an end-to-end layer used to deliver messages to a host. It also delivers data as port-to-port. Transport layer services are.

* End-to-end connection
* Flow-control
* Multiplexing and Demultiplexing
* connection establishment
* connection termination
* Reliable Data delivery.
* congestion control.

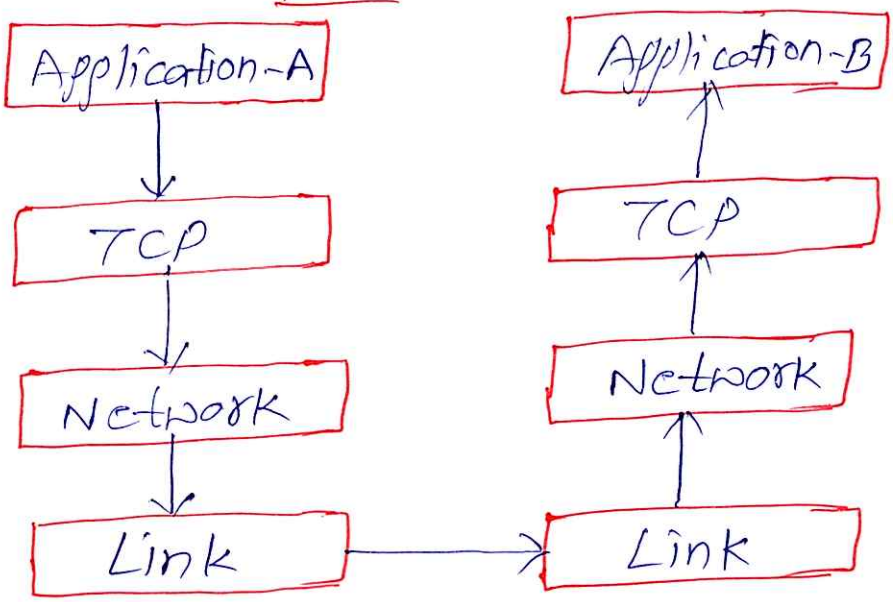
* **End-to-end connection:-** The Transport Layer is also responsible for creating the end-to-end or port-to-port connection btn. hosts. It uses two protocols mainly TCP and UDP. TCP is a secure connection-~~proto~~ oriented protocol that uses a handshake protocol to establish a robust connection btn two end hosts. UDP is unreliable protocol that ensures best-effort delivery.



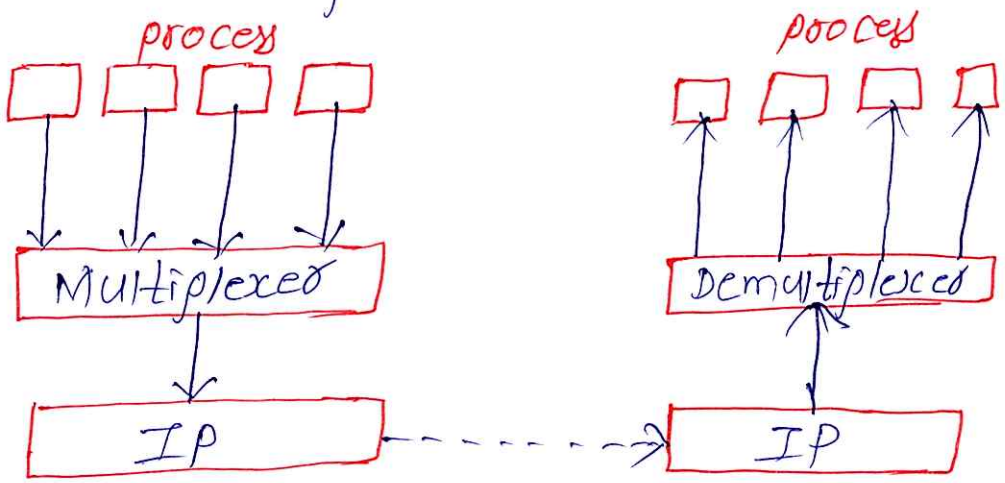

End-to-end/port-to-port comm.

* Flow-control:- The Transport layer provides a flow control mechanism bth. the adjacent layers of the TCP/IP model. TCP prevents data loss due to faster sender and slow receiver by implementing some flow control techniques. It uses the sliding window protocol for flow control.

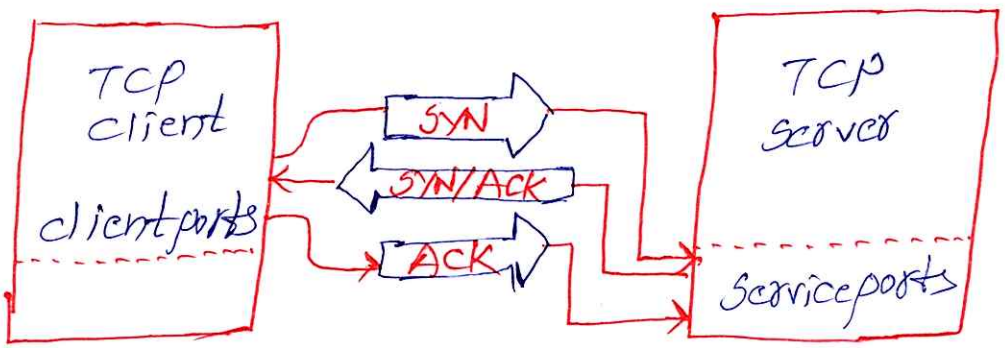
Flow control



* **Multiplexing & Demultiplexing:-** Multiplexing means when data is received from several processes, then these processes are merged into one packet along with header and sent as a single packet. Demultiplexer is required at the receiver side when the message has to distribute for different processes.




* **Connection Establishment:-** When two devices in a network wants to establish a connection using TCP, it is done through a 3-way handshake process



* the first computer connects to the second computer by sending a SYN packet to a specified port number.
* If the second computer is listening it will respond with a SYN/ACK.
* When the first computer receives the SYN/ACK it replies with an ACK packet.
* After this the two devices can communicate normally.

* **Connection Termination:-** In a TCP connection we have two types of terminations.

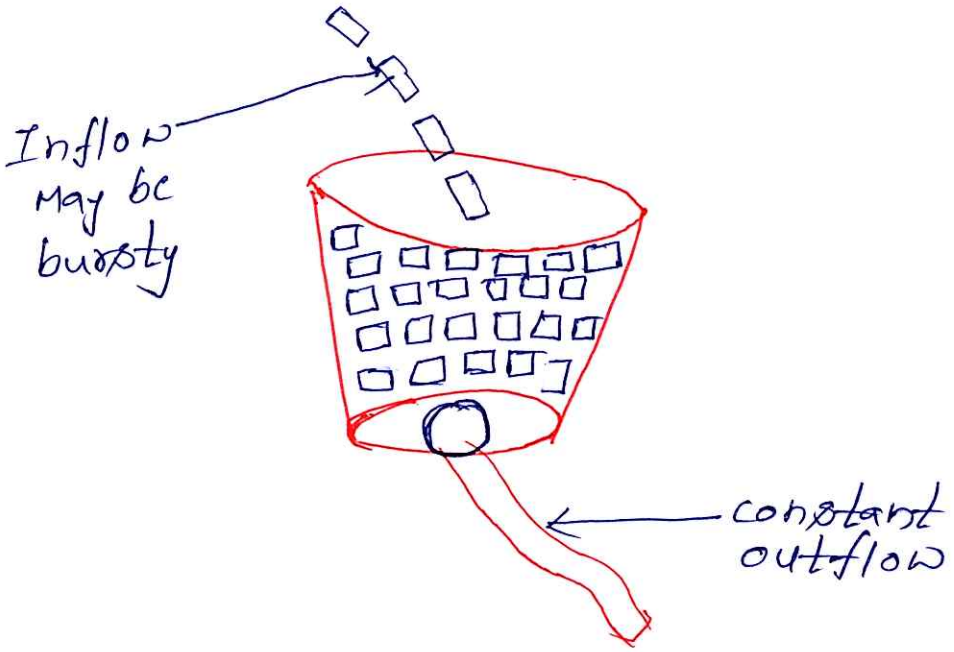
* In the Graceful connection release, the connection is open until both parties have closed their sides of the connection.

* In an Abrupt connection release, either one TCP entity is forced to close the connection or one user closes both directions of data transfer.

* **Reliable Data Delivery:-** The Transport layer checks for errors in the messages coming from the application layer by using error detection codes and computing checksums, it checks whether the received data is not corrupted and uses the ACK and NACK services to inform the sender if the data has arrived or not and checks for the integrity of data.

* Congestion control:- Congestion in a computer network happens when there is toomuch data being sent at the same time, causing the network to slow down. Congestion control technique helps to manage the traffic, so all users can enjoy a stable and efficient network connection. There are two methods for congestion control.

* Leaky Bucket Algo:-




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

## Connection Management

Connection management refers to establishing, maintaining and terminating network connections between devices or systems to enable reliable data transfer. In protocols like TCP, it manages logical associations using a three-way handshake for connection establishment, ensuring synchronization of sequence numbers. It handles flow control via sliding windows, error connection through checksums and acknowledgments and congestion control. Connection states (Eg. SYN, ESTABLISHED, FIN-WAIT) are tracked along with resource allocation, efficient communication and mitigating issues like packet loss or retransmission.

## Process of Connection management

* Connection Establishment :- The process begins with initiating a request from source to destination.
  * This typically involve protocols such as TCP or UDP (User Datagram protocol)
* Handshake : Once the connection request received, the server validates the request and responds with a message to acknowledge and establish the connection.
* Data Transfer : with the connection established, data can be transmitted between the source and destination.
* Data Transmission monitoring :
  The life span of the connection, both parties monitors its status to ensure continued reliability and performance.

Scanned with OKEN Scanner

* Connection Termination: This involves sending a termination request or notification, followed by the Ack: acknowledgement of closure.
* Resource mgnt: efficient allocation and utilization of resources such as n/w bandwidth, memory and processing power to support multiple concurrent connections without compromising performance.
* Error handling and Recovery:

Communication protocols and networking software implement error detection, correction and recovery mechanism to handle various issues.

## Connection management on the Transport Layer

Connection management on the transport layer is a critical function that ensures reliable data transfer between devices over a n/w. This procen includes establishing, maintaining and terminating data transfers, primarily handled by the Transmission Control protocol (TCP).

1. Connection Establishment

Three-way Handshake: The procen of establishing a connection in TCP and other communication protocols involves a three-way handshake:

1. SYN (Synchronize): The client sends a SYN packet to the (Server) Receiver to initiate a connection. This packet includes an initial Sequence Number (ISN) chosen by sender.
2. SYN-ACK (Synchronize-Acknowledge): The Server responds with a SYN-ACK packet. The SYN - Contains Receivers Sequence no.
   ACK - acknowledges the client's SYN packet.

Scanned with OKEN Scanner

3. Ack (Acknowledge) : The client sends an acknowledgement Ack packet back to the server. This acknowledges the server's SYN-ACK by incrementing the servers ISN by one.

2. Data Transfer procedures

* Sequencing - TCP assigns sequence numbers to each byte of data to ensure correct order delivery.
* Acknowledgements (ACKs) - The receiver acknowledges received data by sending ACKs back to the sender.
* Flow Control - TCP uses a sliding window protocol to manage the amount of data that can be sent before receiving an acknowledgement
* Error Detection and Retransmission - If a segment is lost or corrupted, the sender transmits the data after a timeout or upon receiving duplicate Ack's.
* Congestion Control - TCP implements algorithms like to manage network congestion and optimize throughput.

3. Connection ~~Transmi~~ Termination

The process of terminating a TCP connection involves a four-way hand-shake:

1. FIN (Finish) - The sender or receiver sends a FIN packet to terminate its side of the connection
2. ACK (Acknowledge) - The receiving end acknowledges the FIN packet with an ACK packet
3. FIN (Finish) - The receiver sends a FIN packet to close its side of the connection.
4. Ack (Acknowledge) - The initiator of the termination acknowledges the receiver's FIN packet with an Ack.

Scanned with OKEN Scanner

4. Resetting Connections

RST (Reset command) - A TCP connection can be reset using the RST packet, which immediately terminates the packet.

Scanned with OKEN Scanner

## The Internet Transport Protocol: UDP:-

UDP means User Datagram Protocol. UDP is one of the core protocol of the Internet protocol. It is a communication protocol used across the Internet for data transmission. Unlike Transmission control protocol (TCP), UDP is connectionless and does not guarantee delivery, order or error checking, efficient option for certain types of data transmission. Some of the features of UDP are:

* connectionless services
* unreliable
* No-Guarantee Delivery
* Less overhead
* No Flow control

* **connectionless services:-** A connectionless service is also known as a datagram service. It transmits data packets independently, without establishing a connection. Each packet is treated individually and may follow different paths through the network. It is just like sending letter in the postal System.

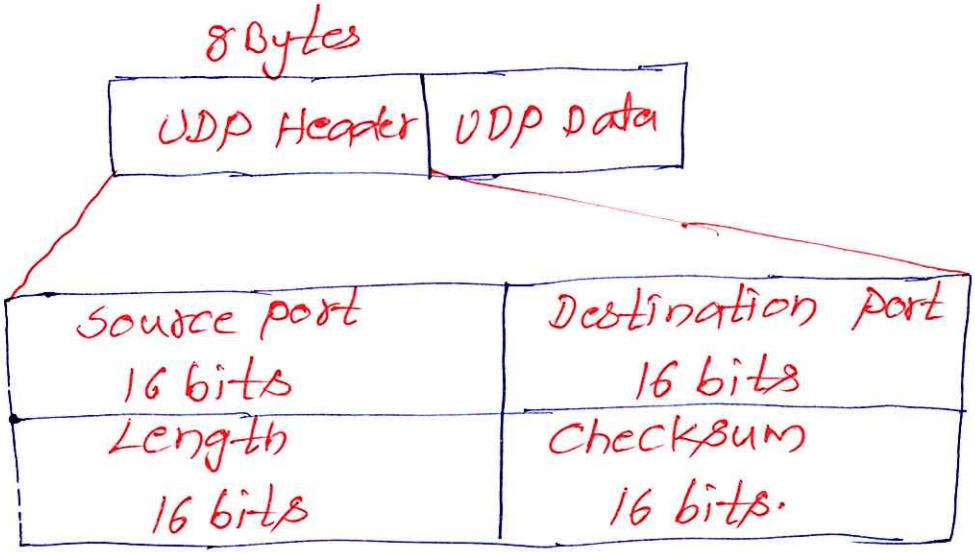
* Unreliable:- while the network does its best to deliver packets, there is no guarantee that they will all arive in the correct order or not.

* No-Guarantee Delivery:- while the sender sends the data to the destination, there is not guarantee that the data sent by the sender will reach the destination or not.

* Less overhead:- when the sender sends the data to the receiver, the sender does not receives any acknowledgement from the receiver. If the data has any errors, or the data is lost, the sender no need to worry about the transmission.

* NO Flow-control:- There is no data flow control in UDP. Because if the sender sends the data of a high speed, and the receiver has no capacity of receiving the data sent by the sender, then the data may lost or corrupted.

## * UDP Header:-




UDP Header is an 8-byte fixed, while for TCP it may vary from 20 bytes to 60 bytes. The first 8 bytes contain all necessary header information and the remaining part consists of data.

* UDP port number fields are each 16 bits long. Therefore the range for port numbers is defined from 0 to 65535 i.e $2^{16}-1$ bits = 65536-1 = 65535.
* **Source port:-** Source port is a 2 Byte long field used to identify the port number of the source.
* **Destination port:-** It is a 2 byte long field used to identify the port of the destination packet.

* **Length:-** Length of UDP including the header and the data. It is a 16 bits field.

* **checksum:-** Checksum is 2 Bytes long field. It is the 16-bit one's complement sum of the UDP header, the pseudo-header of information from the IP header, and the data, padded with zero at the end to make a multiple of two octets.

---

## ➡ The Internet Transport Protocol: TCP:-

TCP means Transmission Control protocol. TCP is a connection-oriented Protocol for communications that helps in the exchange of messages bth. different devices over a network. It is one of the main protocols of the TCP/IP. In OSI model, it operates at the Transport layer (Layer-4). It lies bth. the Application and Network Layers which are used in providing reliable delivery services. Some of the features of TCP are:

* Segment Numbering System
* congestion control.
* connection oriented
* Full Duplex
* Flow control
* Error control

* Segment Numbering System:- TCP keeps track of the segments being transmitted or received by assigning numbers to each and every single one of them.
* connection oriented:- It means sender and receiver are connected to each other till the completion of the process.
* Full Duplex:- In TCP data can be transmitted from receiver to the sender or vice-versa at the same time.
* Flow control:- Flow control limits the rate at which a sender transfers data. This is done to ensure reliable delivery.
* Error control:- TCP implements an error control mechanism for reliable data transfer. Segments are checked for error detection.
* Congestion control:- TCP takes into account the level of congestion in the network. Congestion level is determined by the amount of data sent by a sender.

## * TCP Header:-

<table>
<tr><td colspan="4">Source port 16-bit</td><td colspan="4">Destination port 16-bit</td></tr>
<tr><td colspan="8">Sequence Number 32-bit</td></tr>
<tr><td colspan="8">Acknowledge Number 32-bit</td></tr>
<tr><td>HLEN 4-bit</td><td>Reserved 6bit</td><td>U R G</td><td>A C K</td><td>P S H</td><td>R S T</td><td>S Y N</td><td>F I N</td><td>Window Size 16-bit</td></tr>
<tr><td colspan="4">Checksum 16-bit</td><td colspan="4">Urgent Pointer 16-bit</td></tr>
<tr><td colspan="8">options and padding 40-bytes</td></tr>
</table>

The length of TCP header is min. 20 bytes long and max. 60 bytes.

* Source port:- (16-bit) It identifies source port of the application process on the sending device.
* Destination port:- (16-bit) It identifies destination port of the application process on the receiving device.
* Sequence Number (32-bit):- Sequence number of data bytes of a segment in a session.

* Acknowledgement Number: (32-bit):- When ACK flag is set this number contains the next sequence no. of the data byte expected and works as acknowledgement of the previous data received.

* Header Length/Data offset: (4-bits):- This field implies both, the size of TCP header and the offset of data in current packet in the whole TCP segment.

* Reserved (6-bits):- Reserved for future use and all are set zero by default.

* Flag bits:-

  * URG:- It indicates that urgent pointer field has significant data and should be processed.

  * ACK:- It indicates that Acknowledgement field has significance. If ACK is set to '0', it indicates that packet does not contain any ACK.

  * PSH:- This flag push the data as soon as it receives the data without buffering it.

  * RST:- This flag is used to refuse an incoming connection, or reject a segment or restart a connection.

* SYN :- This flag is used to set-up a connection btn hosts.

* FIN :- This flag is used to release a connection and no more data is exchanged thereafter.

* Window Size (16-bits) :- This field is used for flow control btn. two stations and indicates the amt. of buffer the receiver has allocated for a segment.

* Checksum (16-bits) :- This field contains the checksum of Header, data and pseudo headers.

* Urgent Pointer (16-bits) :- It points to the urgent data byte if URG flag is set to '1'.

* Options (40-bytes) :- It facilitates additional options which are not covered by the regular header. option field is always described in 32-bit words. If this field contains data less than 32-bit, padding is used to cover the remaining bits to reach 32-bit boundary.

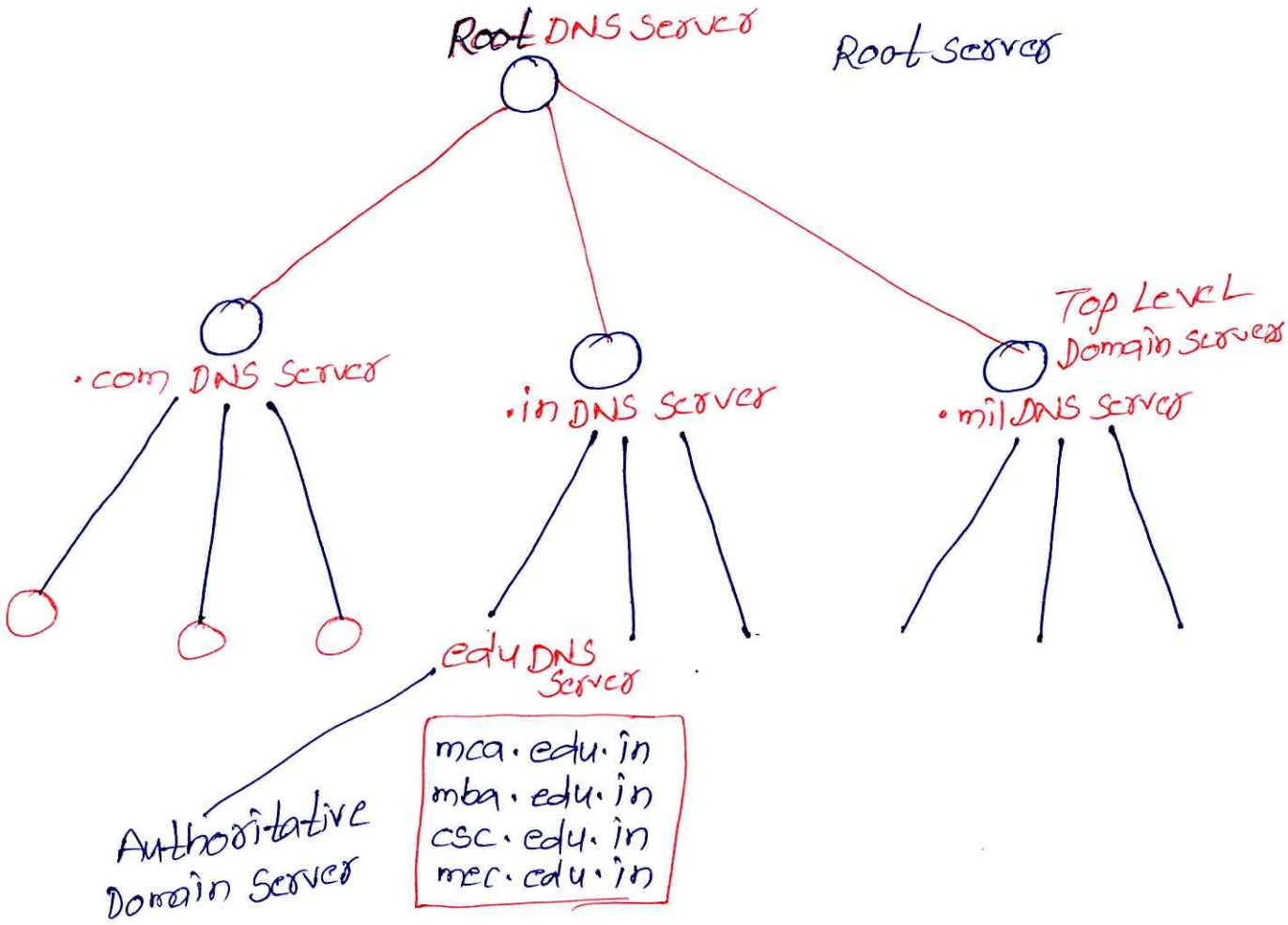
## The Domain Name System:-

The Domain Name System (DNS) translates human readable domain names (like google.com) into numerical IP addresses that computers use to communicate. This allows users to easily access websites by typing in domain names instead of complex IP addresses.

DNS is the Internet's "Phone Book!" It translates domain names like www.google.com in to IP addresses like 192.168.2.1, which are the numerical addresses that computers use to identify each other.

When you type a domain name into your browser, your computer first checks its own cache for the IP address. If not found it queries a DNS server which in turn consults other DNS servers until the IP address is located.

* **Structure of DNS:-** DNS operates through a hierarchical structure which ensures scalability and reliability across the global internet infrastructure.




* Root DNS Server:- These are the highest-level DNS servers and know where to find the TLD servers. They are crucial for directing DNS queries to the correct locations.

* TLD Servers:- These servers manage domain extensions like .com, .org, .net, .edu, .gov and others.

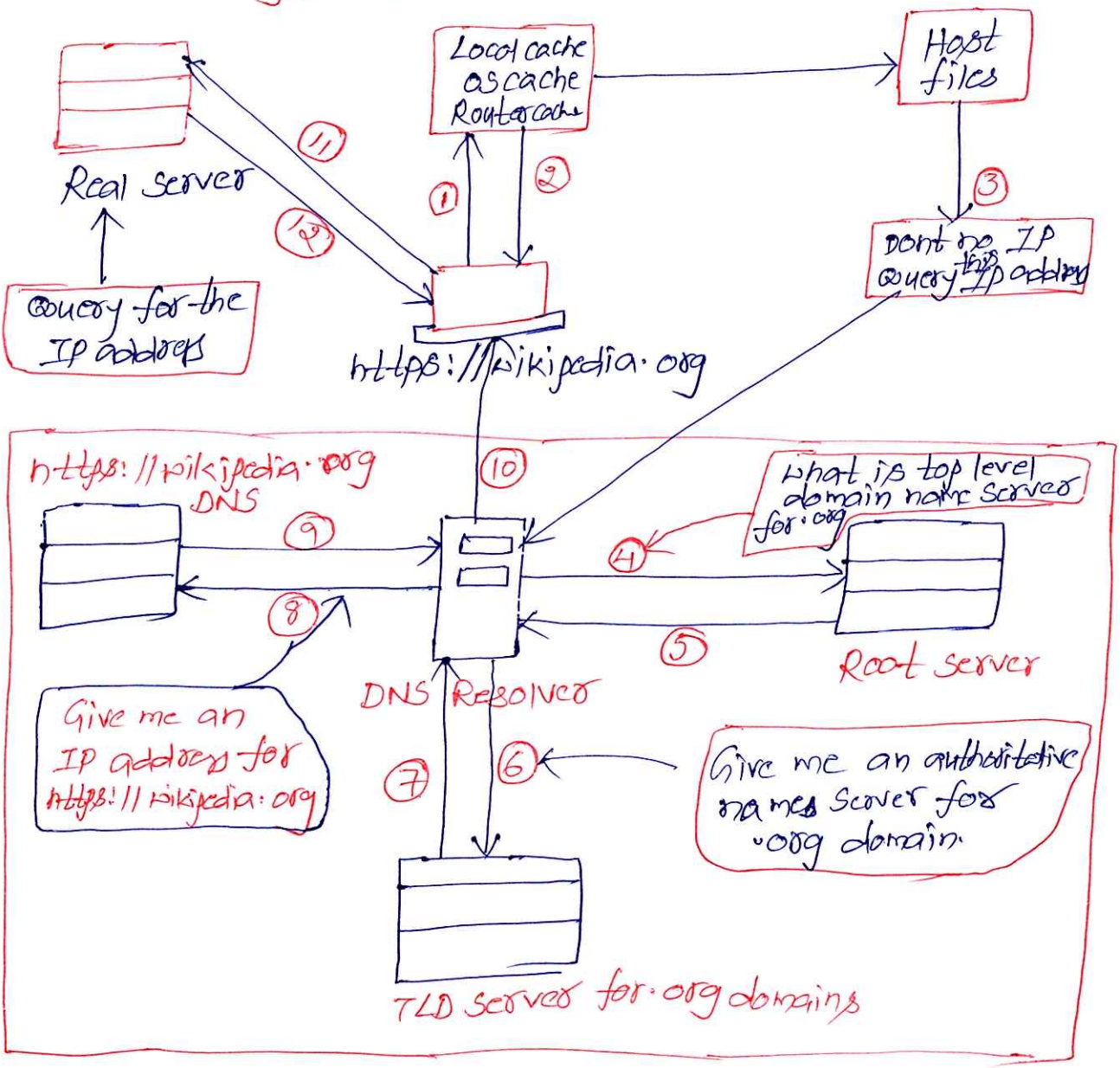
* Authoritative DNS Servers:- These are the servers that store the actual DNS records for domain names. These servers are responsible for providing the correct IP address to allow users to reach websites.

* Types of Domains:- Some of the primary domains are:

* Generic Domains:- These include top-level domains like .com, .org, .net and .edu.

* country code Domains:- These domains represent specific countries or regions such as .in, for India, .us for the united states, .jp for japan etc.

* working of DNS:-



1 * User Input:- For example you entered a website address such as "www.wikipedia.org" in your web browser.

2 * Local cache check:- Your browser first checks its local cache to see if it has recently looked up the domain. If it finds the corresponding IP address, it uses that directly without querying external servers.

3 * DNS Resolver query:- If the IP address isn't in the local cache, your computer sends a request to a DNS resolver.

4 * Root DNS Server:- The resolver sends the request to a root DNS server. The root server doesn't know the exact IP address for "www.wikipedia.org" but knows which top-Level Domain (TLD) server to query based on the domains extension.

5 * TLD Server:- The TLD server for .org directs the resolver to the authoritative DNS server for "www.wikipedia.org".

6* Authoritative DNS Server:- This server holds the actual DNS records for "wikipedia.org", including the IP address of the website's server. It sends this IP address back to the resolver.

7* Final Response:- The DNS resolver sends the IP address to your computer, allowing it to connect to the website's server and load the page.

---

## Electronic Mail:-

Electronic mail, commonly known as email. It is a method of exchanging messages over the internet. Some of the basics of e-mail are:

* An email address:- This is unique identifier for each user, typically in the format of name@domain.com.
* An email client:- This is software program used to, receive and manage emails, such as gmail, outlook, Yahoo etc.
* An email server:- This is computer system responsible for storing and forwarding emails to their intended recipients.

* How to send an email :-

1. Compose a new message in your email client.
2. Enter the receipients email address in the "TO" field.
3. Add a subject line to summarize the content of the message.
4. Write the body of the message.
5. Attach any relevant files if needed.
6. Click "Send" to deliver the message to the recipients email server
7. Emails can also include features such as cc (carbon copy) bcc (blind carbon copy) to send copies of the messages to multiple recipients, and reply, reply all, and forward options to manage the conversation.
8. Message in mail not only contains text, but it is also contains images, audio and videos data also.

## SNMP

Simple Network Management protocol (SNMP) is widely used protocol for n/w management that provides a standardized framework for monitoring and managing n/w devices such as routers, switches, servers, firewalls and load balancer. It operates within the application layer of the Internet protocol suite and allows n/w administrators to manage n/w performance.

SNMP is an Internet standard protocol used for managing and monitoring n/w connected devices in IP n/w's. SNMP is an application layer protocol that uses UDP port no. 161/162.

SNMP used for monitor the n/w detect n/w faults, and sometimes even to configure remote devices.

## Architechture of SNMP

There are mainly 3 main components in SNMP architechture:

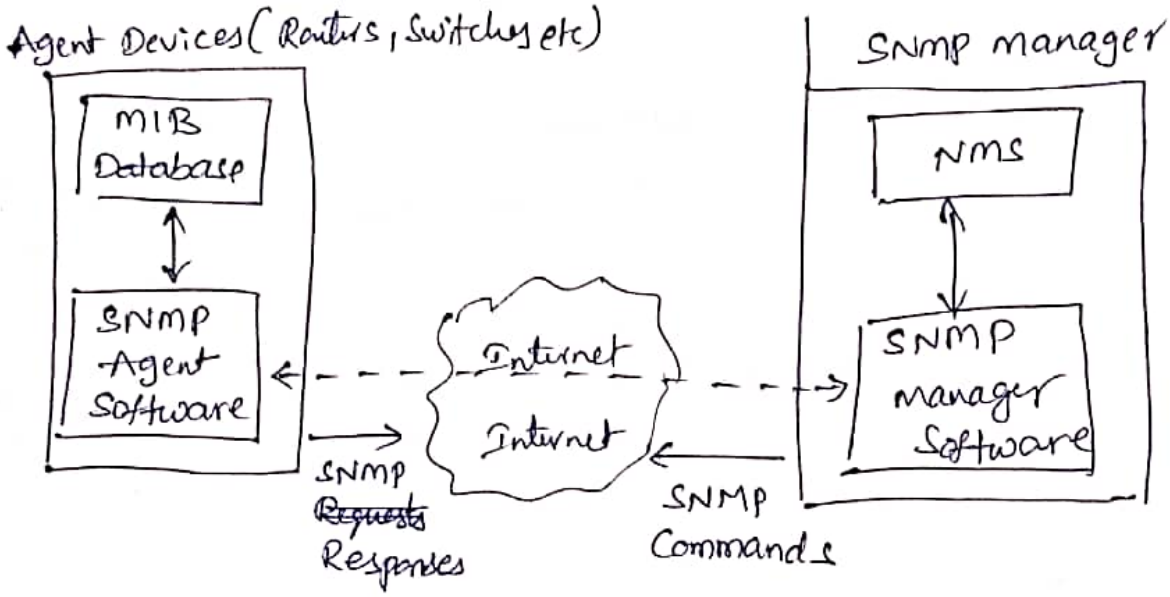
- **SNMP manager**: It is a Centralized system used to monitor the n/w. It is also known as a Network Management Station (NMS). A Router that runs the SNMP Server program is called agent, while a host that runs the SNMP client program is called a manager.
- **SNMP agent**: It is a s/w mgnt s/w module installed on a managed device. The manager accesses the values stored in the database, where as the agent maintains the info in db. (database)

Scanned with OKEN Scanner

For Example, manager examine the variables that a router stores, quantity of packets received and transmitted.

- Management Information Base : MIB Consists of info on resources that are to be managed. This info is organized hierarchically.

A MIB or a collection of all the objects under managment by the manager, is unique to Each agent. System, interface, address translation, IP, UDP and EGP, ICMP, TCP are the Eight categories that make up MIB.




## SNMP messages

- ~~Get~~
- Get Request : To retrive data from SNMP agents. In response to this, the SNMP agent responds with the requested value through a response message.
- GetNextRequest : the manager sends the agent the GetNextRequest message. It is used to define an object in certain circumstances.

Scanned with OKEN Scanner

- Set Request : It is used by the SNMP manager to set the value of an object instance on the SNMP agent.
- Response : when sent in response to the set message, it will contain the newly set values as confirmation that the value hasbeen sent.
- Trap : These are the messages sent by the agent without being requested by the manager. It is sent when a fault has occured.
- InformRequest : It was added to SNMPv2c and is used to determine if the manager has received the trap message or not. It is same as the trap but adds an acknowledgement that the trap doesn't provide.

SNMP Security levels

- noAuthNoPriv : This (no authentication, no privacy) security level uses a community string for authentication and no encryption for privacy.
- authNopriv : This security level (authentication, no privacy) uses HMAC with MD5 for authentication and no encryption is used for privacy.
- authpriv : This security level (authentication, privacy) uses HMAC with MD5 or SHA for authentication and Encryption uses the DES-56 algorithm.

Versions of SNMP

- SNMPv1 : It uses Community strings for authentication and uses UDP only. SNMPv1 is the first version of the Protocol.
- SNMPv2c : It uses Community strings for authentication. It uses UDP but can be Configured to use TCP. Improved MIB structure elements, transport mapping and protocol

Scanned with OKEN Scanner

Packet types are all included in this updated version.

- SNMPv3 : It uses Hash-based MAC with MD5 or SHA for authentication and DES-56 for privacy. This version uses TCP. that's way it provide more security.

## Characteristics of SNMP

- SNMP is used for monitor n/w.
- It detects any n/w faults
- It can also be used to configure remote devices
- It allows a standardized way of collecting information about all kinds of devices from various manufacturers among the n/w industry.

## Advantages of SNMP

- It is Easy to implement
- Agents are widely implemented
- Agent level overhead is minimal
- It is robust and extensible
- It offers the best direct manager agent and interface.

## Limitations of SNMP

- It doesnot scale well.
- There is no object oriented data view.
- It has no standard control definition
- It has many implementation specific extentions.
- It has high communication overhead due to polling.

# The World Wide Web [WWW]

The world wide web often called the web, is a system of interconnected webpages and information that you can access using the Internet. It was created to help people share and find information Easily, using links that connect different pages together. The web allows us to browse websites, videos,

Scanned with OKEN Scanner

shop online and connect with others around the world. The data may present in text, picture, audio or video formats on the internet.

## Key parts of web (or) building blocks

* URL [Uniform Resource Locator]: This is the address of a webpage, like. https://google.com/ - It tells your browser exactly where to find the page.
* HTTP (Hypertext Transfer Protocol): This is the set of rules that lets your browser and the server talk to each other to send and receive webpages.
* HTML (Hypertext Markup Language): This is the code that tells browsers how to display a webpage, including where to put text, pictures and links.

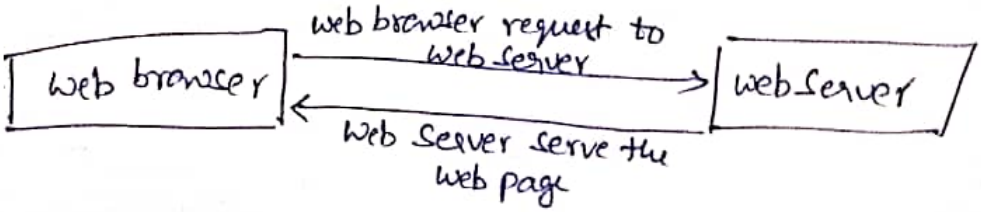
## Working principle

A browser is used to access webpages.

web browser - programs which display text, data, pictures, animation and video on the internet.

Initially, web browsers were used only for surfing the web but now they become more universal.

World wide web operates like client - server architecture of the internet. when users request web pages or other information, then the web browser of your system request to the server for the information and then the web server provide requested services to web browser back and finally the requested service is utilized by the user who made the request.




Scanned with OKEN Scanner

## Challenges of the web

* Privacy : Some websites collect info about you, like what you search for, and might share it without asking.
* Safety : Hackers can try to steal your information or send viruses through fake links or ads
* False Information : Not everything on the web is true, so you need to check if a website is trustworthy
* Too much screen time : Spending too much time online can make it hard to focus on school or sleep well.
* Access Issues : Not everyone has fast internet, especially in some countries, which makes it harder to use the web.

## History of WWW

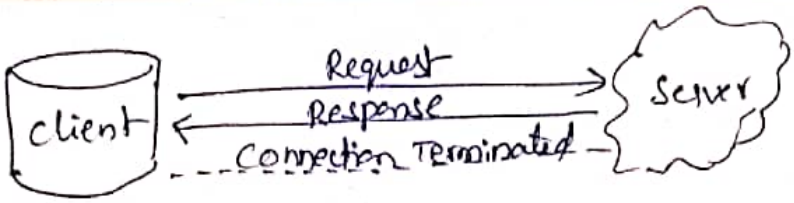
In 1989 Tim Berner Lee was created a project for researches to work together effectively at CERN. at world wide web (W3C) Consortium.

- web 1.0 (1990-2000) - Introduced static websites
- web2.0 (2000-2010) - Interactive and social platforms
- web3.0 (2010-2020) - the semantic web, enabling machines to understand and data
- web 4.0 (2020-2030) - A fully intelligent web ecosystem powered by AI and integrated web operating systems.

## HTTP

HTTP (Hyper Text Transfer Protocol) is a fundamental protocol of the internet, enabling the transfer of data between a client and a server. It is the foundation of data communication for the world wide web. HTTP provides a standard between a web browser and a web server to establish communication.

Scanned with OKEN Scanner




HTTP Connection

## Methods of HTTP

- GET : Used to retrive data from a specified resource. It should have no side effects and is commonly used for fetching web pages, images etc.
- POST : Used to submit data to be processed by a specified resource. It is suitable for form submissions, file uploads and creating new resources.
- PUT : Used to update or Create a resource on the server. It replaces the entire resource with the data provided in the request body
- PATCH : Similar to PUT but used for partial modifications to a resource.
- DELETE : Used to remove a specified resource from the server.
- HEAD : Similar to GET but retrieves only the response headers, useful for checking resource properties.
- OPTIONS : Used to retrive the communication options available for a resource, including supported methods and headers.
- TRACE : Used for debugging purposes to echo the received request back to the client.
- CONNECT : Used to establish a tunnel to the server through a HTTP proxy.

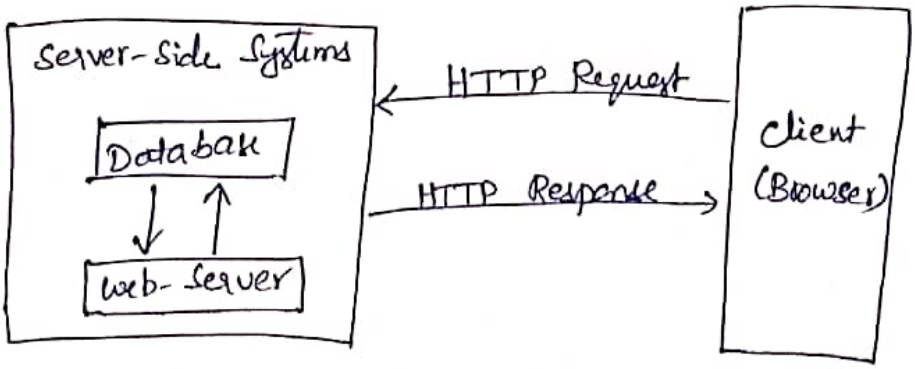
## HTTP Request/Response :

HTTP is a request-response protocol, which means that for every request sent by a client, the server responds with a corresponding response.

The basic flow of an HTTP request-response cycle is as follows

Scanned with OKEN Scanner

- Client sends an HTTP request : The client initiates the process by sending an HTTP request to the server. This request includes a request method ( GET, POST, PUT, DELETE ), the target URI ( Uniform Resource Identifier ), headers and an optional request body.
- Server processes the request : The server receives the request and processes it based on the requested method and resource.
- Server sends an HTTP response : After processing the request, the server sends an HTTP response back to the client. The response includes the status code, headers and an optional response body.
- Client processes the response : The client receives the server's response and processes it accordingly.




Scanned with OKEN Scanner