ANNAMACHARYA UNIVERSITY, RAJAMPET

(ESTD UNDER AP PRIVATE UNIVERSITIES (ESTABLISHMENT AND REGULATION) ACT, 2016
RAJAMPET, Annamayya District, AP, INDIA

Course : **Computer Networks**

Course Code : **24FMCA24T**

Branch : **MCA**

Prepared by : **S. Mastan**

Designation : **Assistant Professor**

Department : **MCA**

ANNAMACHARYA UNIVERSITY, RAJAMPET

(ESTD UNDER AP PRIVATE UNIVERSITIES (ESTABLISHMENT AND REGULATION) ACT, 2016
RAJAMPET, Annamayya District, AP, INDIA

Title of the Course: Computer Networks
Category : PC
Course Code : 24FMCA24T
Year : I
Semester : II
Branch : **MCA**

Lecture Hours	Tutorial Hours	Practice Hours	Credits
3	1	0	3

Course Objectives:

- To know the concepts of the Reference Models and understand the fundamentals of Computer Networks.
- To understand various techniques of data link layer.
- To know various issues of routing, quality of service and congestion control.
- To understand various transport protocols.
- To know various security issues of computer networks.

Unit 1 **INTRODUCTION** **12**

Uses of Computer Networks, Network Topologies, Network Hardware, Network Software, and Reference Models- The OSI Reference model, The TCP/IP Reference Model. THE PHYSICAL LAYER: Multiplexing- Frequency Division Multiplexing, Synchronous Time Division Multiplexing, Code Division Multiplexing, Switching-Packet Switching, Circuit Switching.

Unit 2 **THE DATA LINK LAYER** **11**

Data Link layer design issues-Framing, Error Control, Flow Control, Error Detection and Correction, Elementary Data Link Protocols, Sliding Window Protocols. THE MEDIUM ACCESS CONTROLSUB-LAYER: The Channel Allocation Problem, Multiple Access Protocols-ALOHA, Carrier Sense Multiple Access Protocols (CSMA), Collision-Free Protocols, Limited-Contention Protocols, Wireless LAN Protocols.

Unit 3 THE NETWORK LAYER **10**

Network layer design issues; Routing Algorithms-The Optimality Principle, Shortest path Algorithm, Flooding, Distance Vector Routing, Link State Routing, Hierarchical Routing, Broadcasting routing. Internetworking-How Networks Differ, Tunneling, Internetwork Routing, Packet Fragmentation.

Unit 4 THE TRANSPORT LAYER **10**

The Transport Service, The Internet Transport Protocols: UDP, The Internet Transport Protocols: TCP. THE APPLICATION LAYER: The Domain Name System(DNS), Electronic Mail.

Unit 5 NETWORK SECURITY **10**

Cryptography, Symmetric-Key Cryptography algorithms- Data Encryption Standard (DES), Advanced Encryption Standard (AES); Asymmetric-Key Cryptography algorithms- Rivest, Shamir, and Adleman (RSA); Digital Signature, Entity Authentication.

Prescribed Text Books:

1. Andrew S. Tanenbaum, David J. Wetherall, Computer Networks, Pearson Education, 6th Edition, 2022.

References Books:

1. Behrouz A. Forouzan, Data Communications and Networking, McGraw-Hill. 6th Edition, 2022.
2. James F. Kurose, Keith W. Rose. Computer Networks- A Top-Down Approach Featuring the internet, Pearson Education., Standard Edition, 2023
3. Larry L. Peterson, Computer Networks: A Systems Approach, Morgan Kaufmann, 6th Edition 2021.

Course Outcomes:

At the end of the course, the student will be able to

1. Summarize the concepts of computer networks.
2. Apply the different data link layer techniques.
3. Apply various routing algorithms.
4. Analyze various transport protocols.
5. Comprehend the cryptography and network security techniques.

CO-PO Mapping:

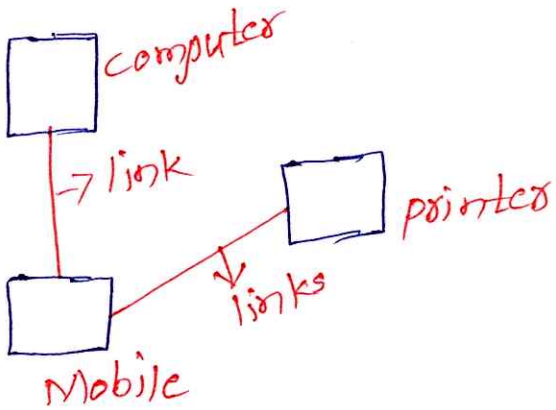
Course Outcomes	Foundation Knowledge	Problem Analysis	Development of Solutions	Modern Tool Usage	Individual and Teamwork	Project Management and Finance	Ethics	Life-long Learning
24FMCA24T.1	2	2	1	-	-	-	-	-
24FMCA24T.2	3	2	1	-	-	-	-	-
24FMCA24T.3	3	2	1	-	-	-	-	-
24FMCA24T.4	3	3	2	-	-	-	-	-
24FMCA24T.5	2	2	1	-	-	-	-	-

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 peppl to sell products online and execute secure payments.

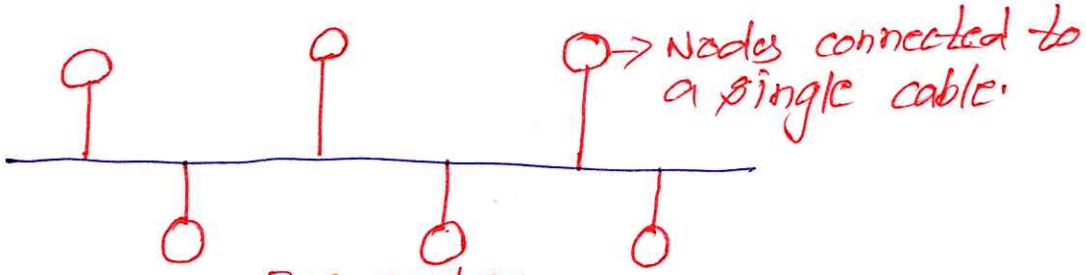
* Education:- computer Networks provides a platform for distance learning, access to resources of higher education and give opportunity for collaboration among students and teachers.

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.

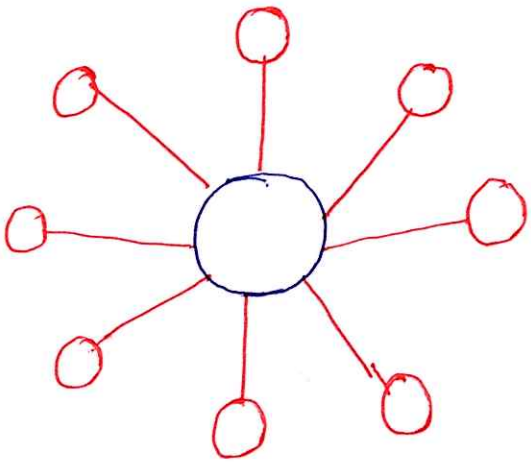
Types of Network Topologies:-

* **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.



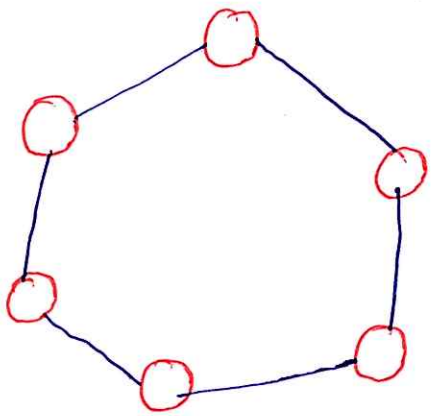
Bus Topology

* **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.



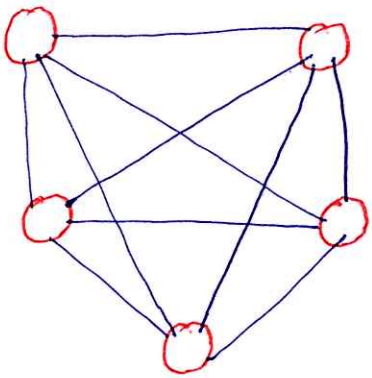
Star Topology

* 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.



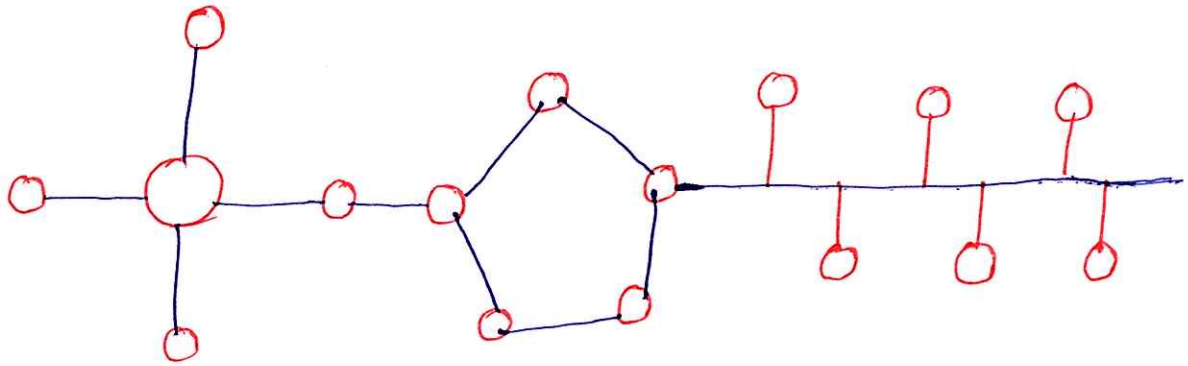
Ring Topology

* 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

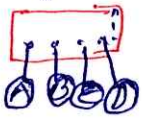
➡ Network Hardware (or) Hardware Components

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 10 Base FX

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.

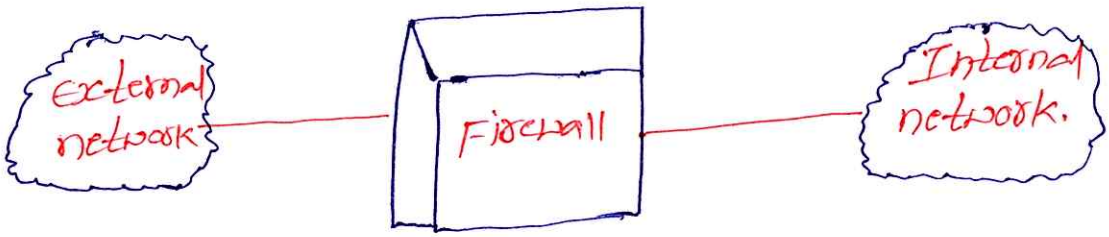
5. Bridge:- Bridge is a device that connects two or more LAN's which works on the same protocal.

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.

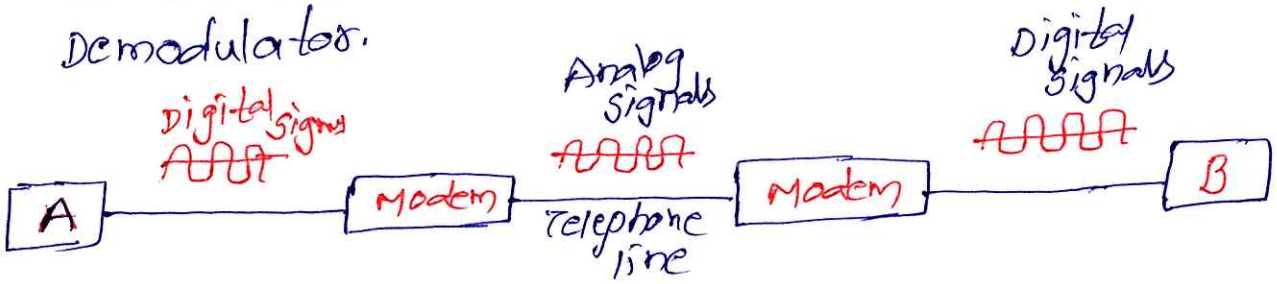
8. IDS:- IDS means an Intrusion Detection System is a network security tool that monitors network traffic for suspicious activity.

Intruder → Intrusion → IDS

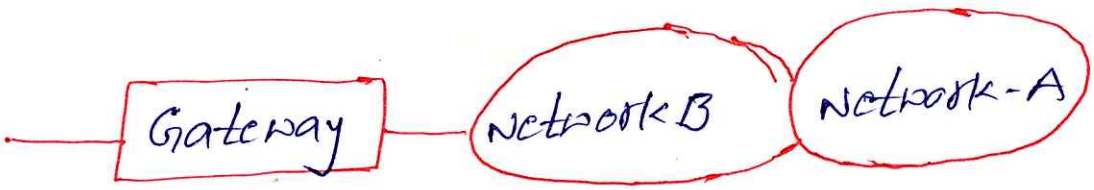
9. Firewall:- A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on configurable ~~network~~ ~~traf~~ security rules.



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



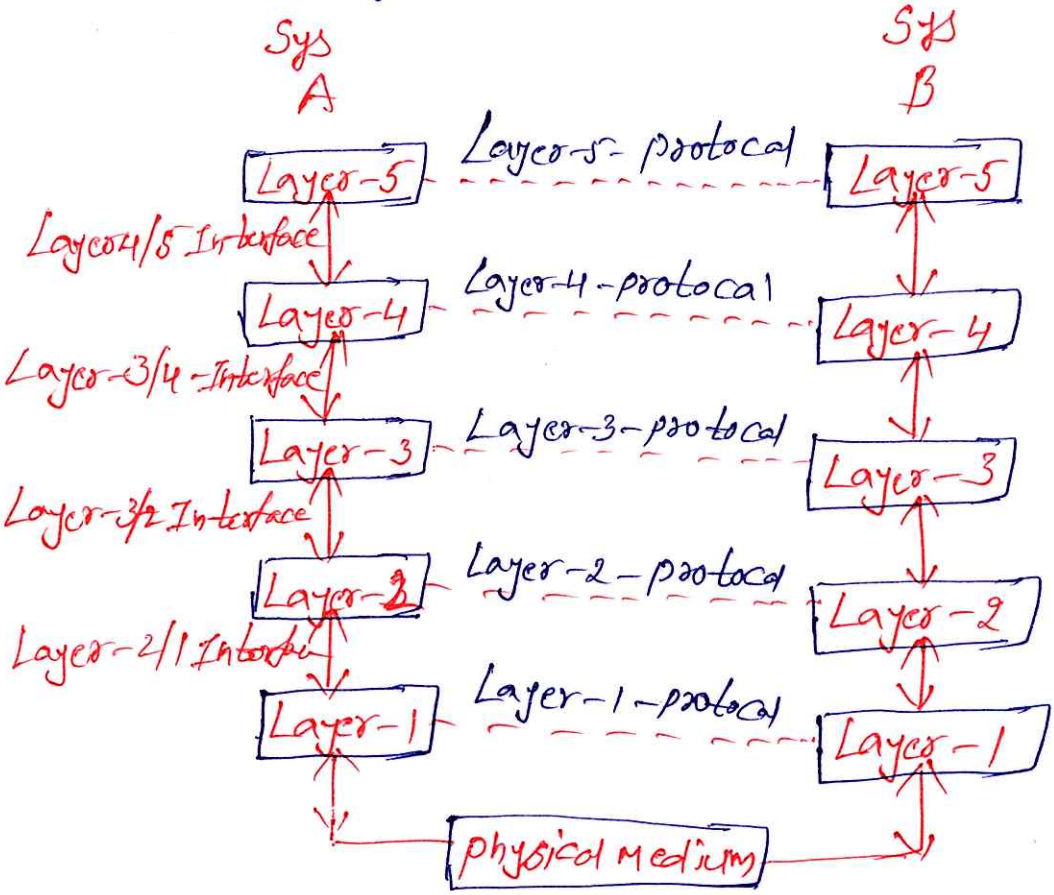
Network Software:-

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.

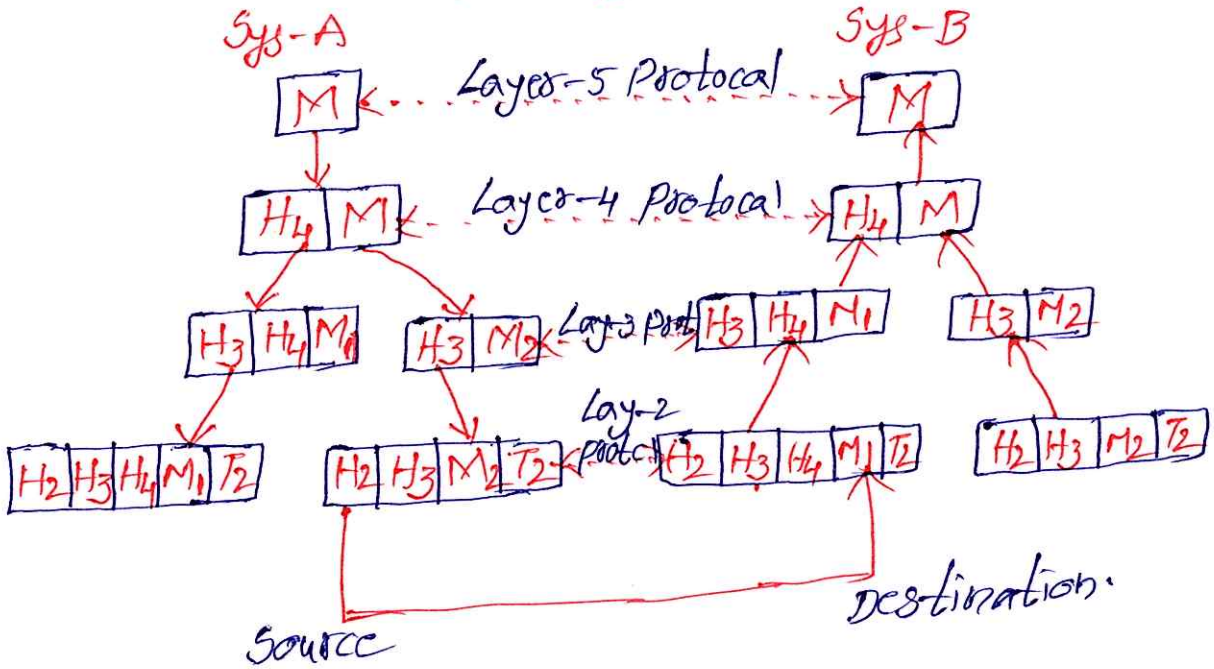
Q. 1. Protocal Hierarchies:- Most Networks are organized as a stack of layers or labels each one build upon and one below it.



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.

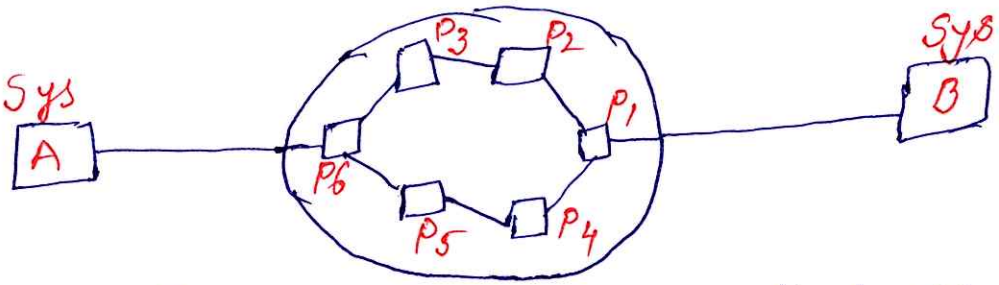


2. Design issues for the layers:-

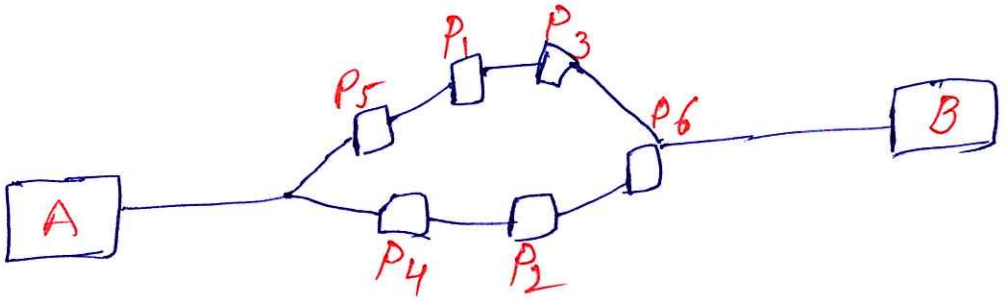
* Reliability:- Error detection & correction and routing.
* Evaluation of Network:- Addressing or Naming Scalable.
* Resource Allocation:- Transmission line, Real time delivery, quality of services.
* Network security:- confidentality, Authentication Integrity.
* Direction of Transmission:-
  * simplex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

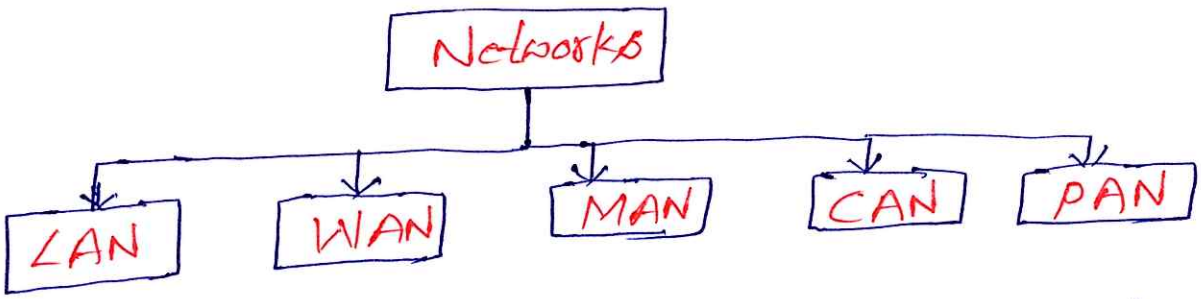


4. Service primitives:- A service is basically defined as a set of operations available to user process to access the services.

5. The relationship of services to protocals:-

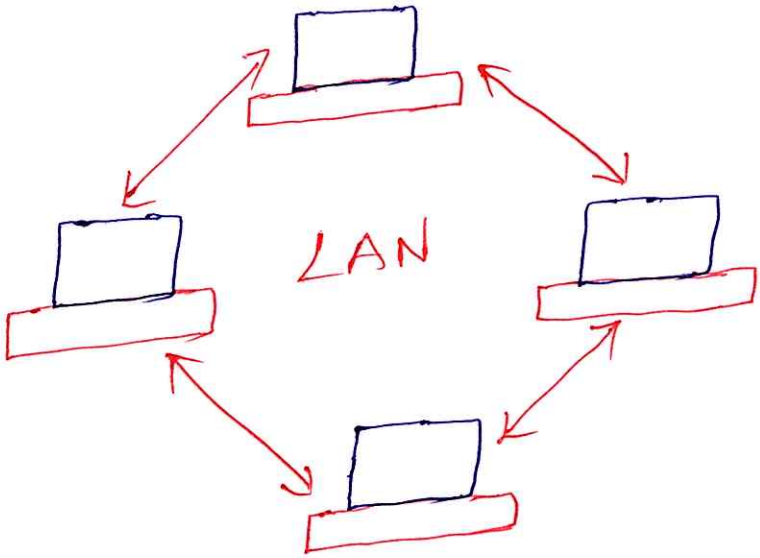
* The service defines ~~that~~ relates to an interface bth two layers, with the lower layer being the service provider and the upper layer being the service user.
* A protocal is a set of rules where the data is transfered bth. two devices within a layer.

Types of Networks



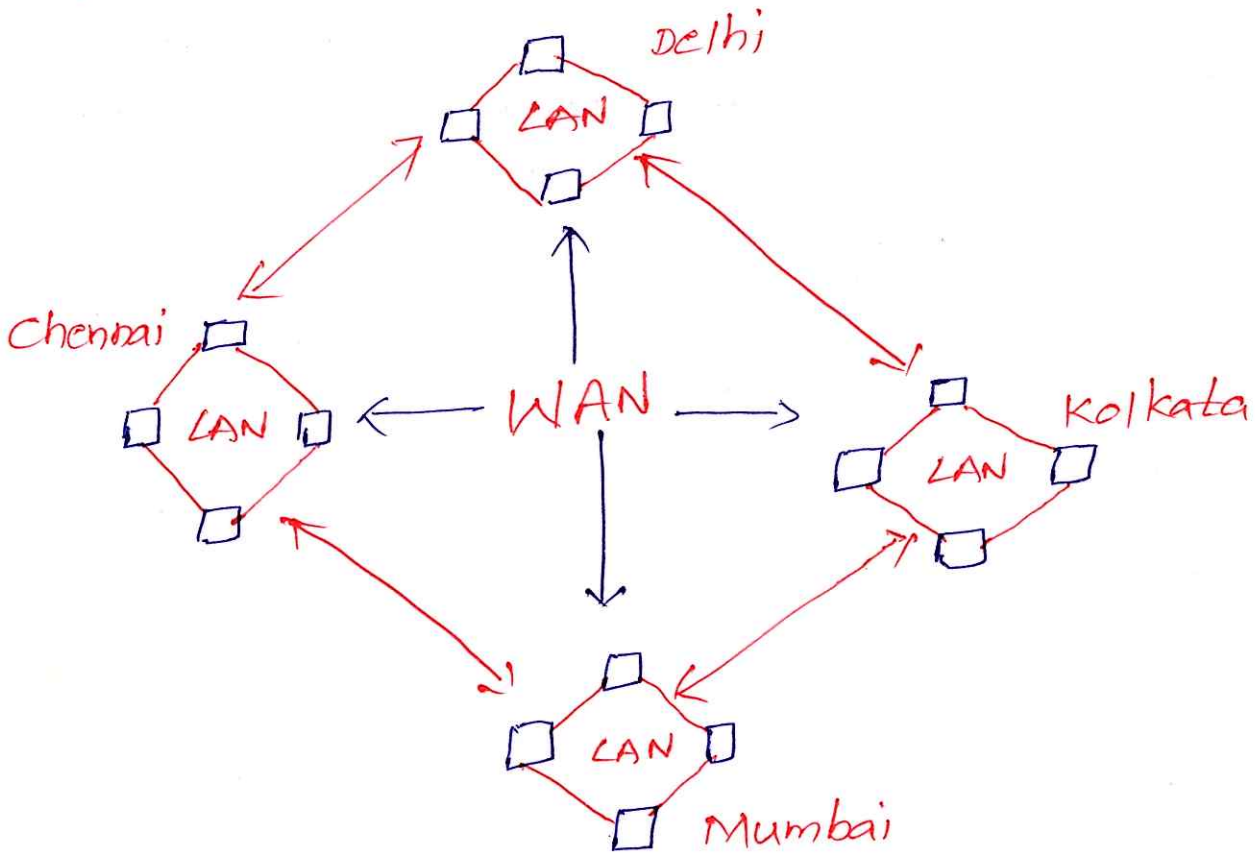
Networks are mainly classified into Five types widely used in both homes and business. The networks are categorised based on their scale and scope, historical reasons, preferences for networking industries and their design.

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.

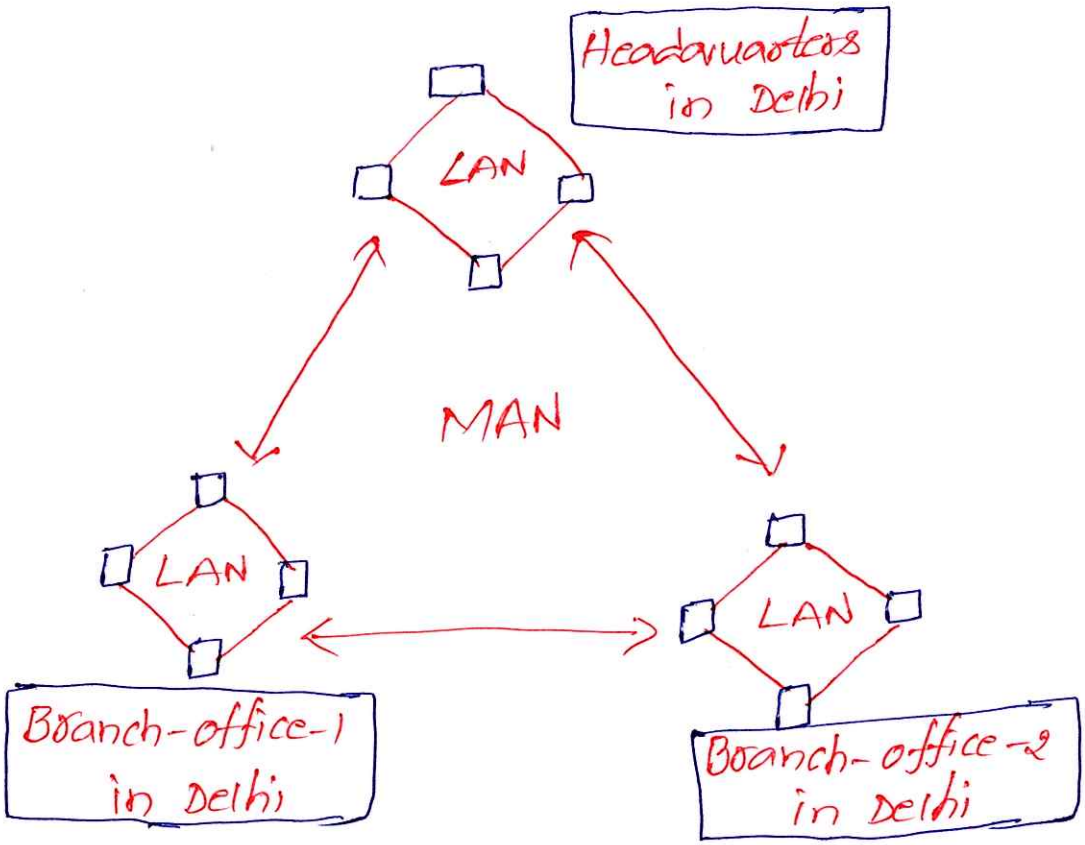


2. WAN :- WAN means Wide Area Network. As indicated by name it spreads a large geographical area such as city, country or even intercontinental distances using a communication channel that combines many types of media such as telephone lines, cables and air waves.

~~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.

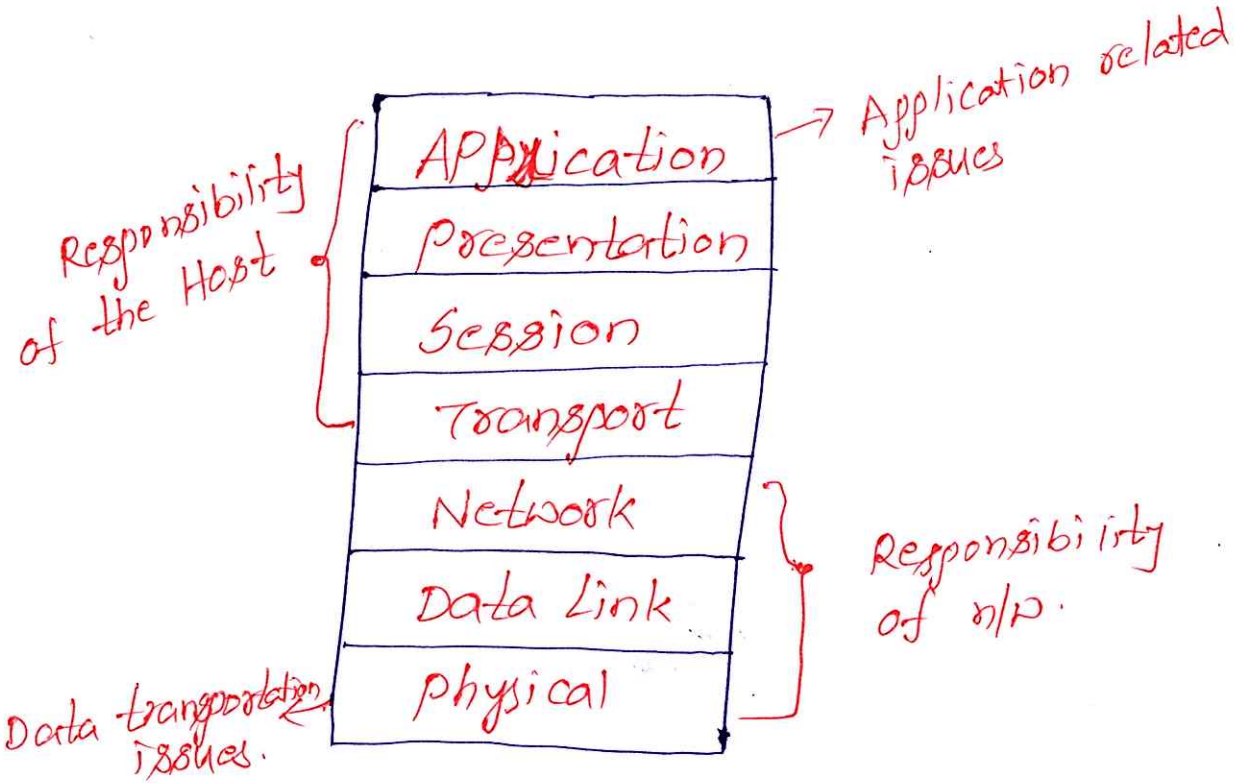
OSI Reference Model

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.

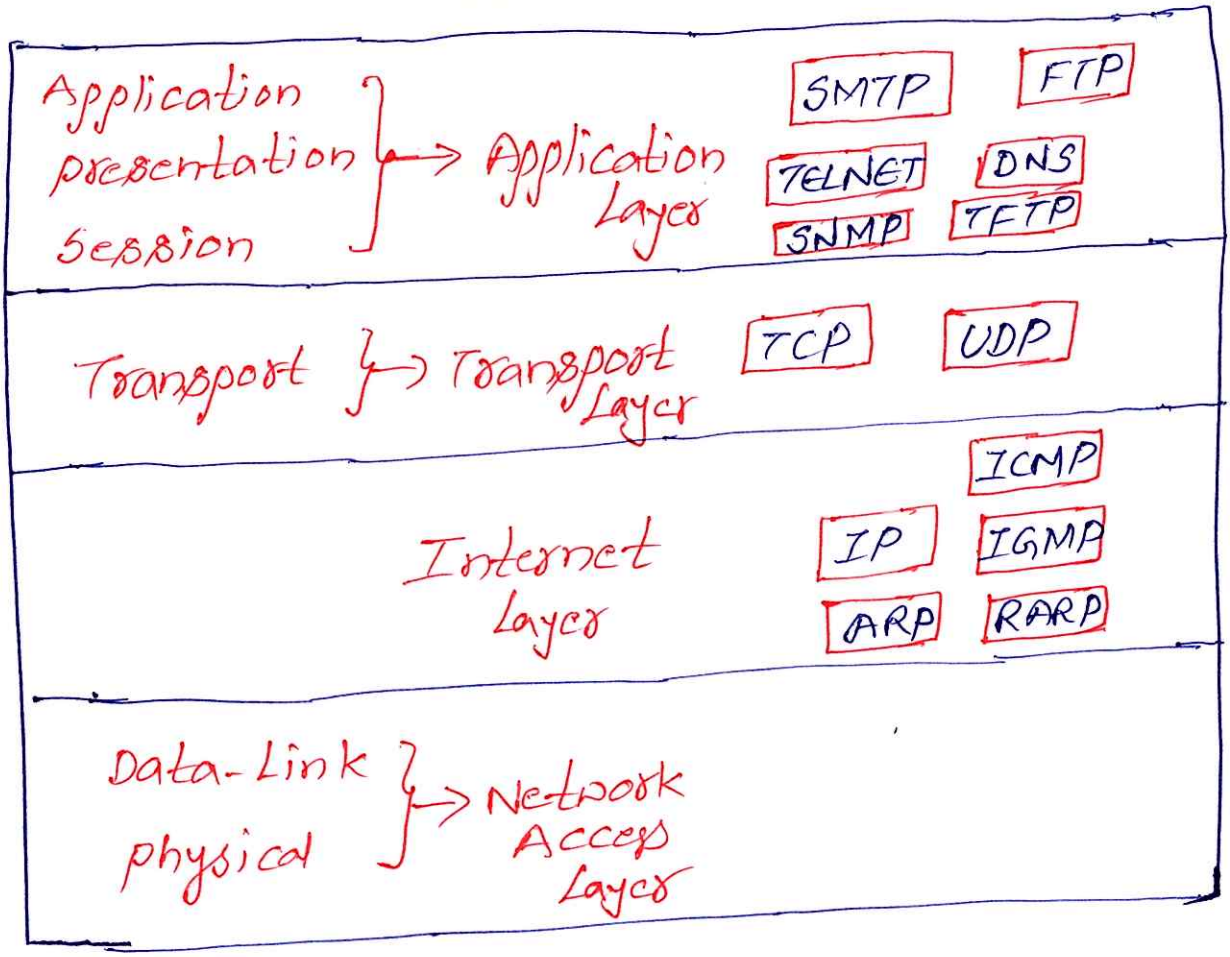
* OSI model consists of seven layers, each layer performs a particular task.



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.

* 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.

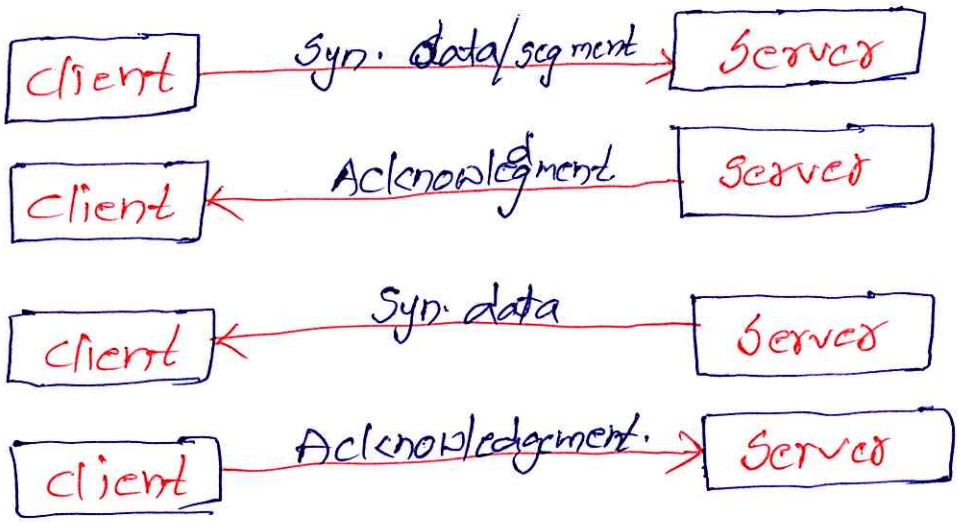
1. Decides transmission should be single/parallel, 2. Multiplexing & Splitting, 3. Quality of service, 4. converting msg to segments 5. End to end delivery

* 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.

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.

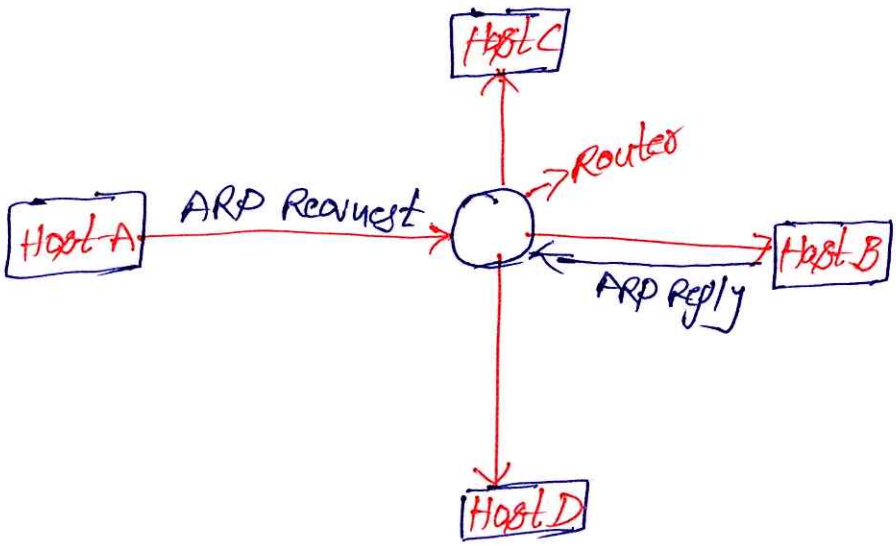


* Message or data is divided into segments and each segment having some sequence number.

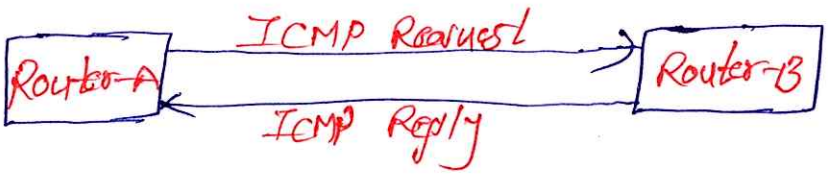
* **UDP:-** UDP means User Datagram Protocol. UDP is a communication protocol that sends data packets directly to a destination computer. UDP sends messages called datagrams, which are units of data transmission. UDP is faster than TCP, but less reliable.

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.

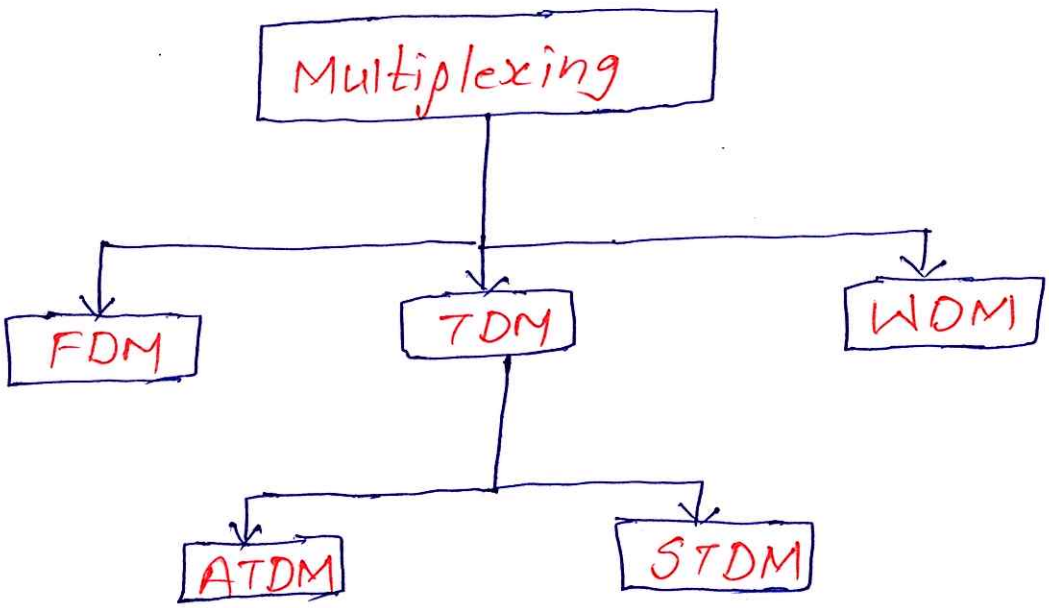
* **IP:-** IP means Internet Protocol. IP is a set of rules that how data is sent and received on the internet. Some functionalities of IP are:
  * IP Addressing
  * Host-to-Host communication
  * Data Encapsulation
  * Reassembling
  * Routing.

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 bth. devices on a network and ensures data is properly received and transmitted accross that connection.

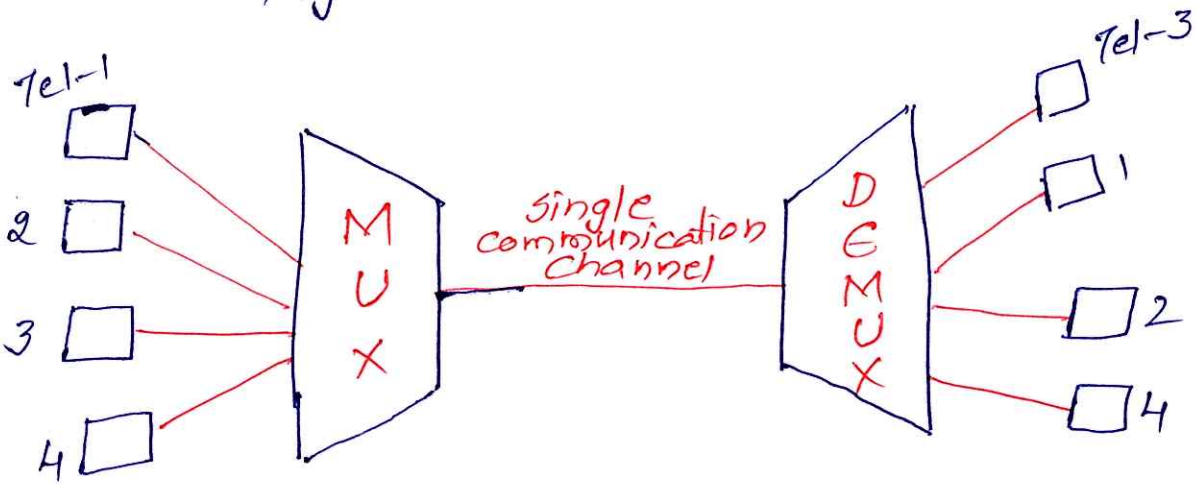
Multiplexing / Data Multiplexing:-

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:-

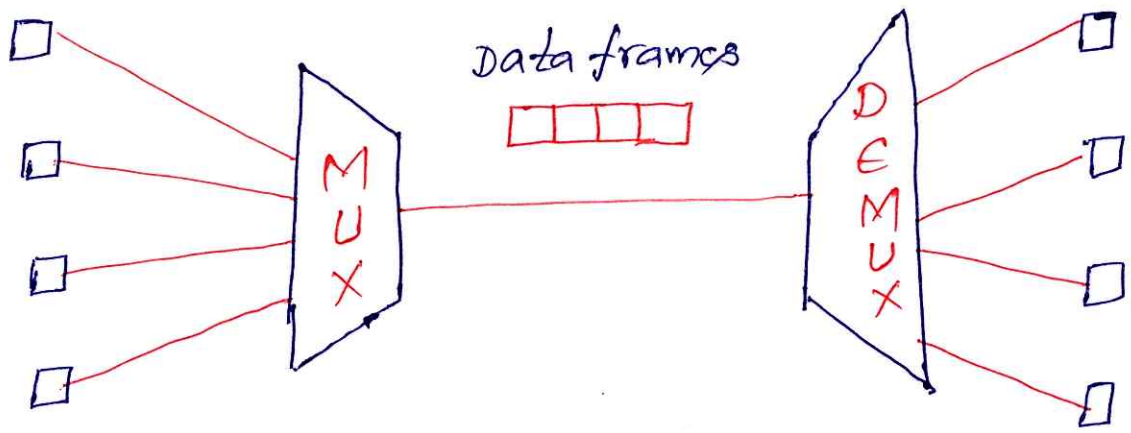


* FDM:- FDM means Frequency Division Multiplexing. FDM is a networking technique that allows multiple signals to be transmitted ~~over a signals to be transmitted~~ over a single communications channel. The FDM is widely used in television and radio transmitters to broadcast several channels simultaneously.

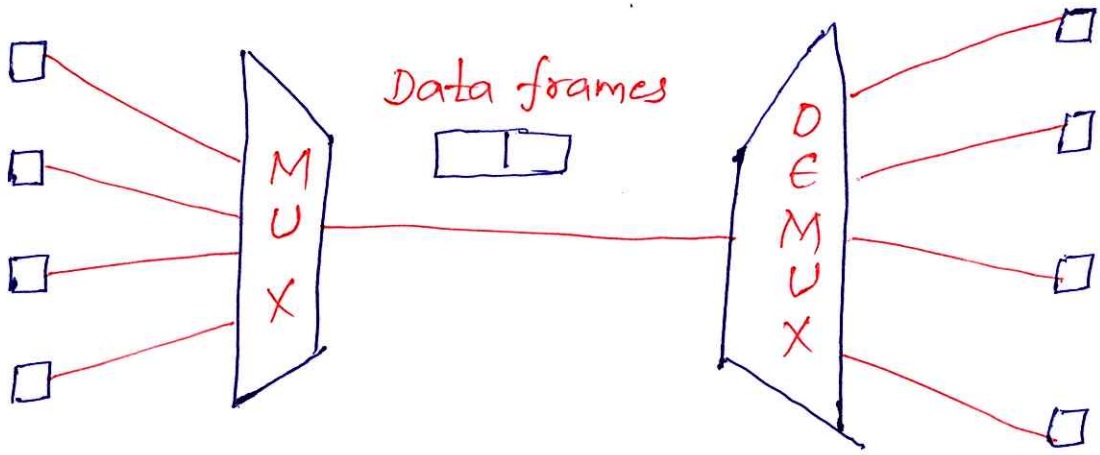


* TDM:- TDM means Time Division Multiplexing. TDM is a digital/Analogue multiplexing technology that seperates data streams based on time, instead of frequency. The channel is divided into time slots. Each signal is assigned a time slot. signals take turns transmitting data during their allocation time. There are two ways for implementing TDM. i.e ATDM and STDM.

* **STDM:-** STDM means Synchronous TDM. In STDM the MUX gives equal time to each device connected to it. If any device has some data to transmit, then it waits for its turn. When its turn comes the device can transmit for a predetermined time.

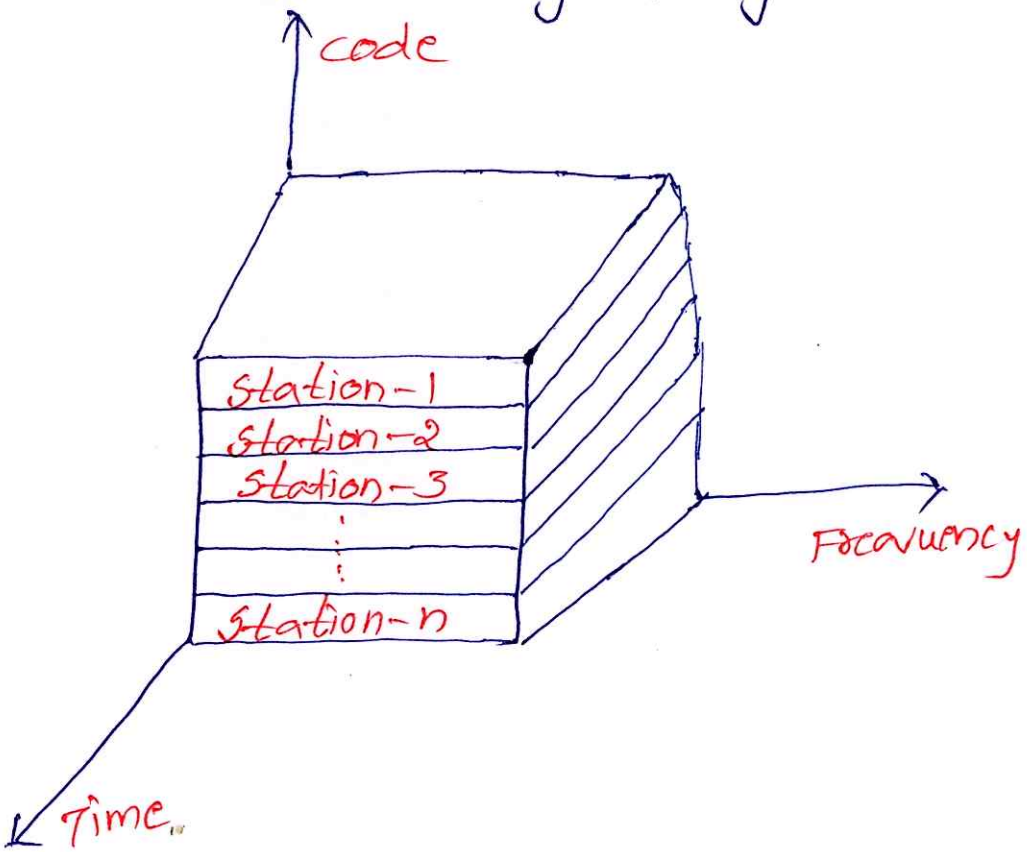


* **ASTDM:-** Asynchronous TDM. In ASTDM timeslots are allocated to devices that have some data to transfer. This technique allocate slots dynamically to achieve more efficiency, and maximum line usage and to improve bandwith efficiency. In ASTDM the no. of slots in each frame is less than the no. of sending devices.



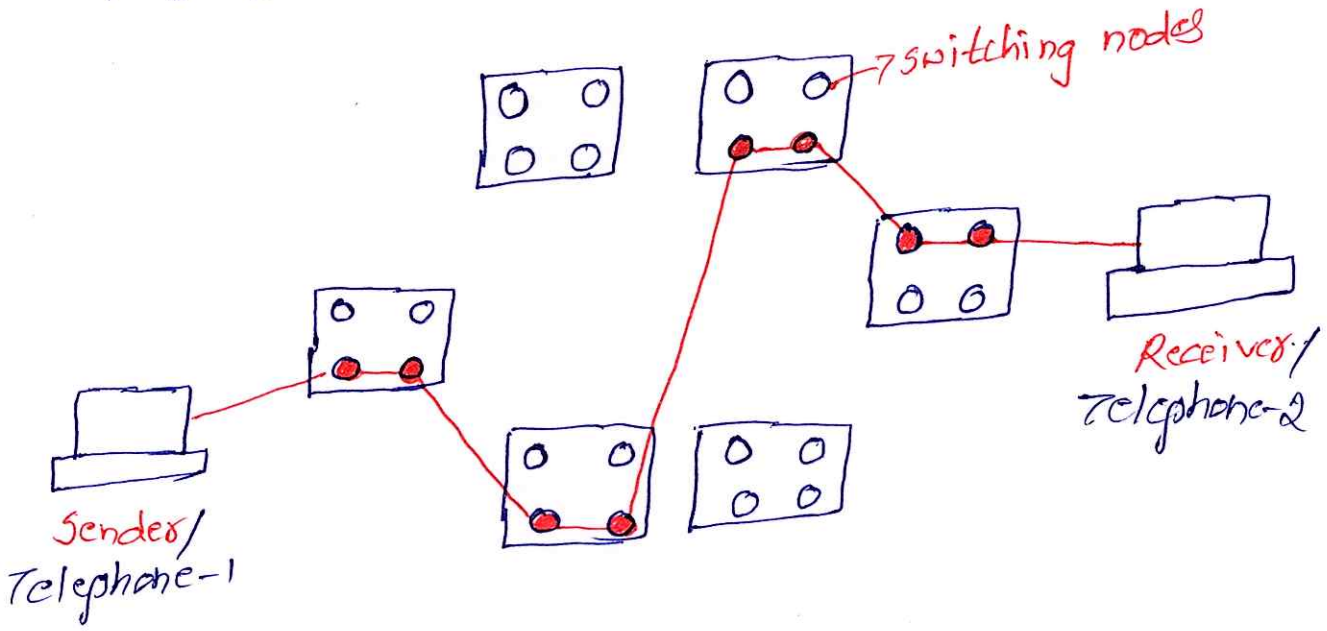
* WDM :- WDM means Wavelength Division Multiplexing. WDM is an analogue multiplexing technique that is quite similar to FDM. WDM fully utilizes the high data rate capability of Fiber-optic cables. When we use a Fiber-optic cable for one single line, the entire bandwidth is used by a single line. Therefore WDM combines the inputs from several optical cables into one.

* CDM:- CDM means code Division Multiplexing. CDM is a technique that allows multiple users to share the same frequency spectrum by assigning each user a unique digital code. A unique code is assigned to each signal. The code is combined with the original signal to create an encoded stream of data. The encoded data is transmitted on a shared medium. At the receiving end the encoded data is combined with the same code to retrieve the original signal.

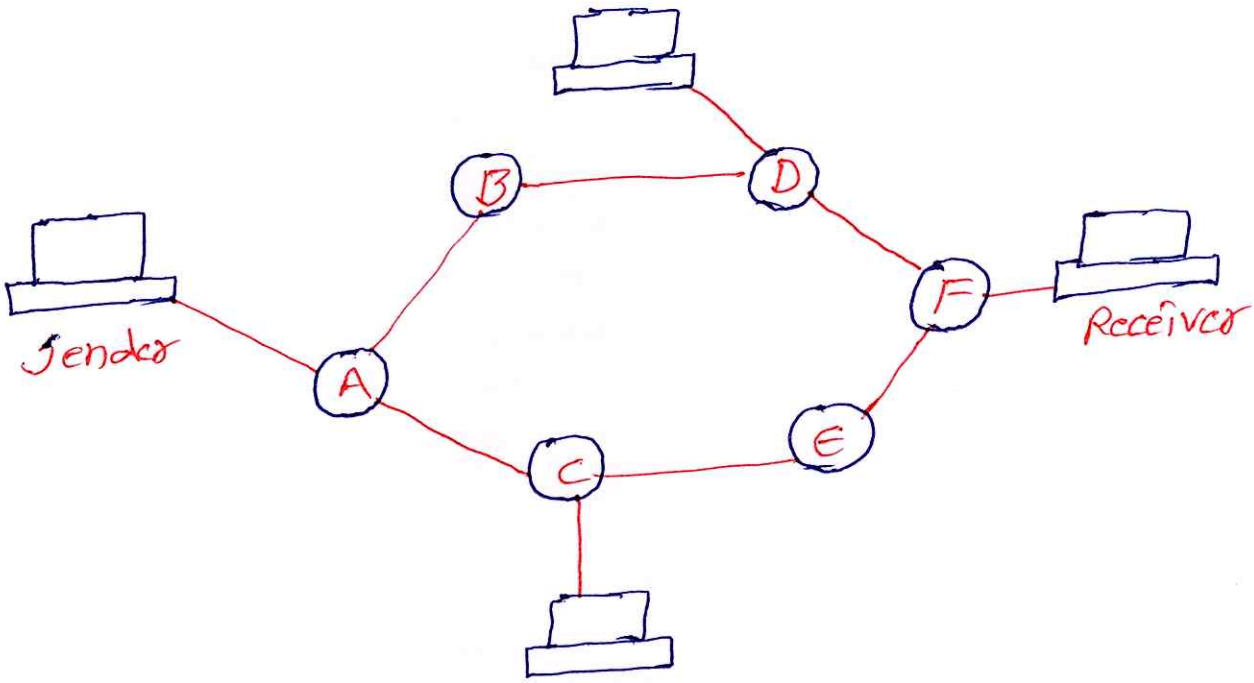


Data Switching:- Data switching is the process of transferring data packets btn. devices on a network. In data switching we are having three types.

1. **circuit Switching:-** when we make a phone call to a friend, a circuit is established btn. our phone and friends phone. This circuit may pass through a no. of telephone exchanges. Once the call has been setup, the dedicated path will continue to exist until the call is finished.

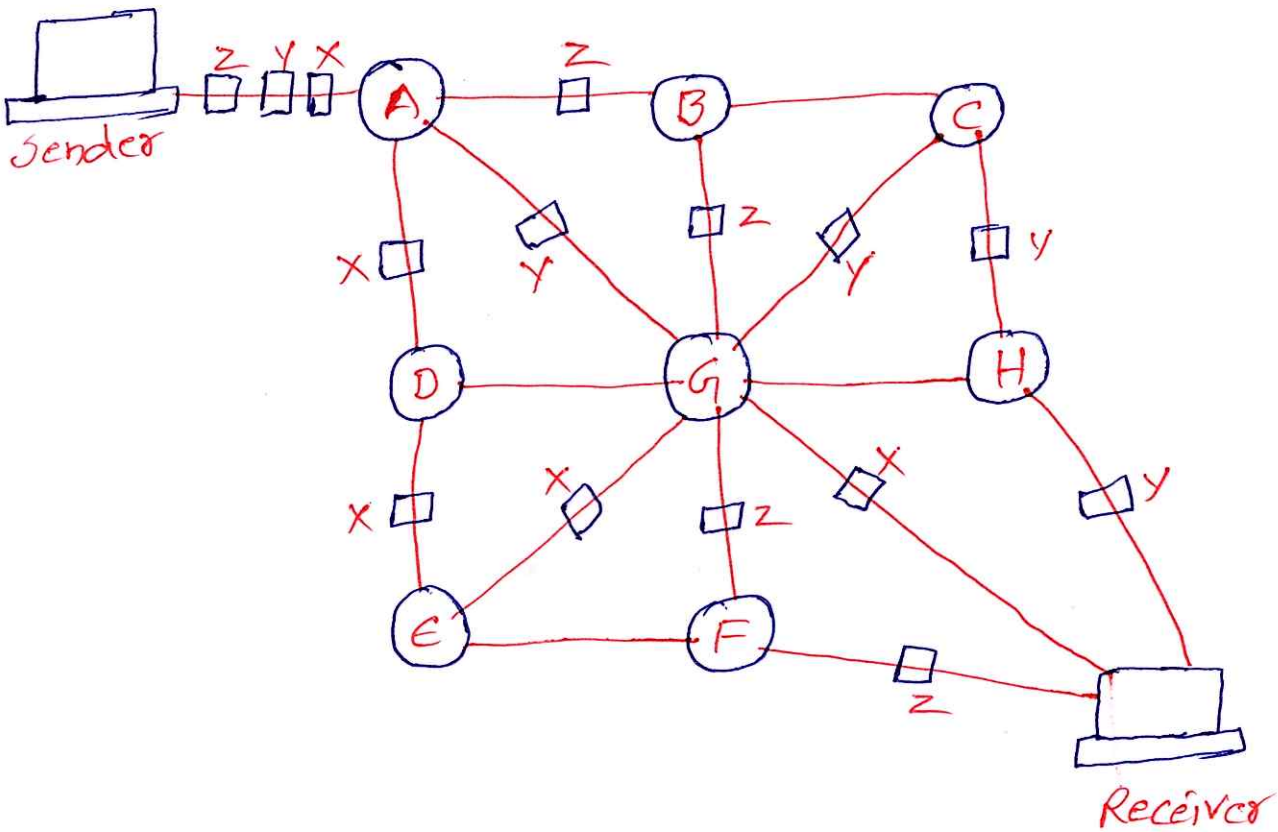


2. Message ~~Packet~~ Switching :- A message is a logical unit of information that can be of any length. In message switching if a device/sender wants to transmit data, it attaches the destination address i.e address of the receiver to the message. Between the sender and the receiver there may be a no. of intermediate nodes. These intermediate nodes accept the data store it temporarily, checks for any errors and then transmits it to one of its directly connected device. This process of transmitting data to intermediate nodes continuous until the message reaches its destination.



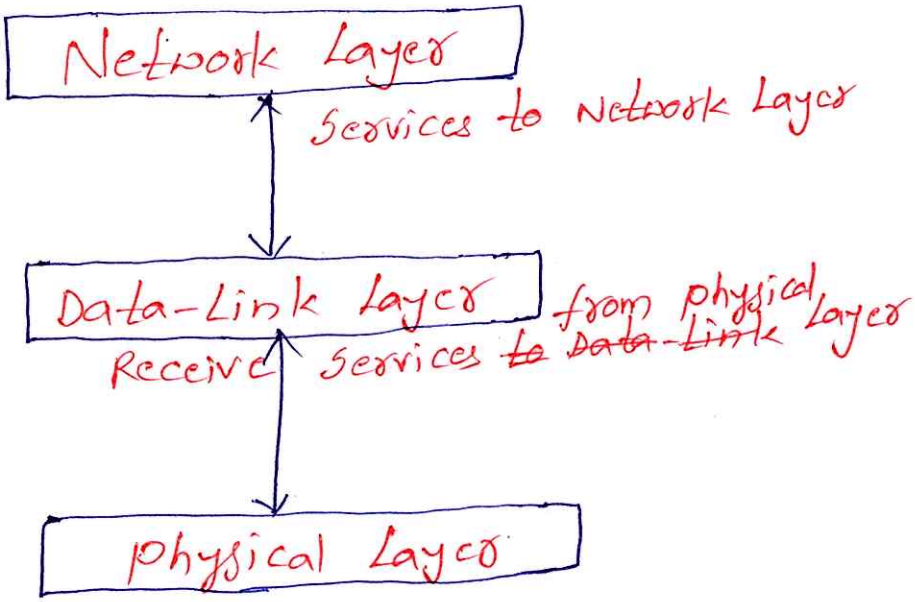
3. Packet Switching:- Packet switching is similar to Message switching. However in Message switching the message can have unlimited length, whereas in packet switching a message is split into packets of fixed size.

A packet consists of a header part that stores the address of the receiver, control information, packet number, and so on. A data packet that stores the information and a trailer at the end that contains error checking information.



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

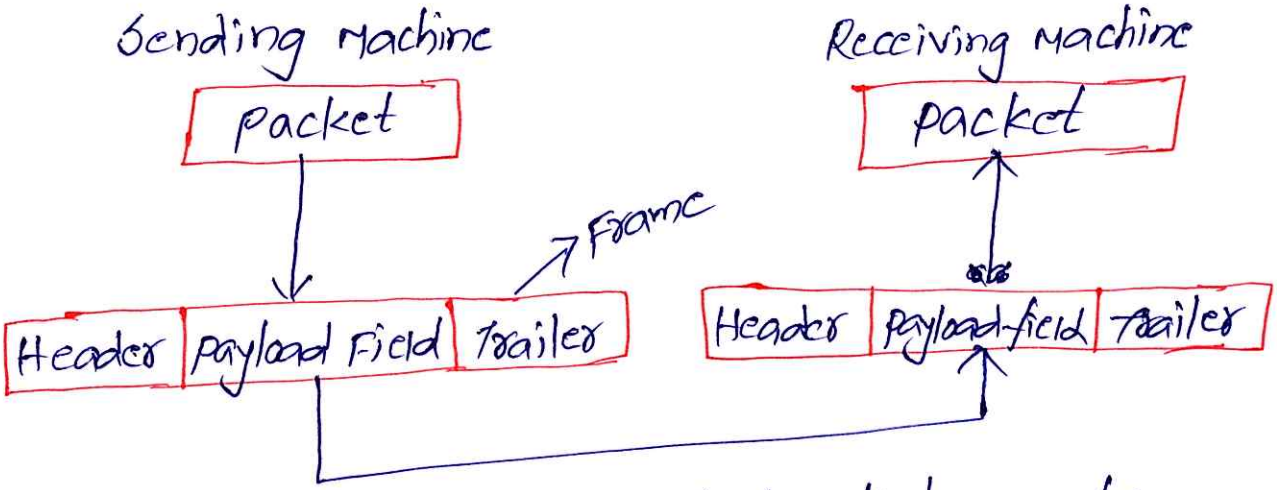
1. Fixed-Size Framing
2. Variable Size Framing.

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.

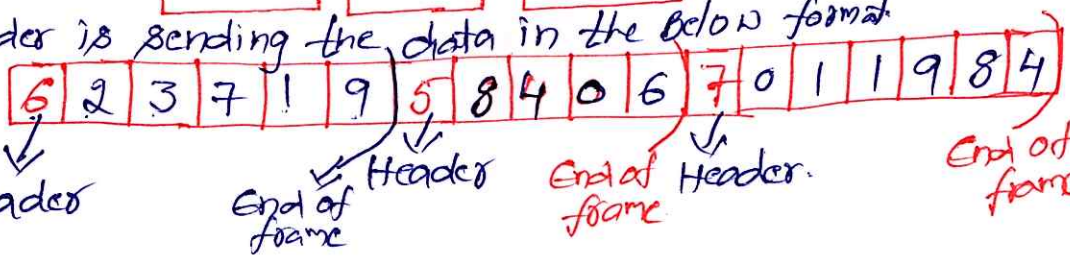
* Character count/Byte count
* Flag bytes with byte stuffing
* Flag bits with bit stuffing
* Physical layer coding violations.

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

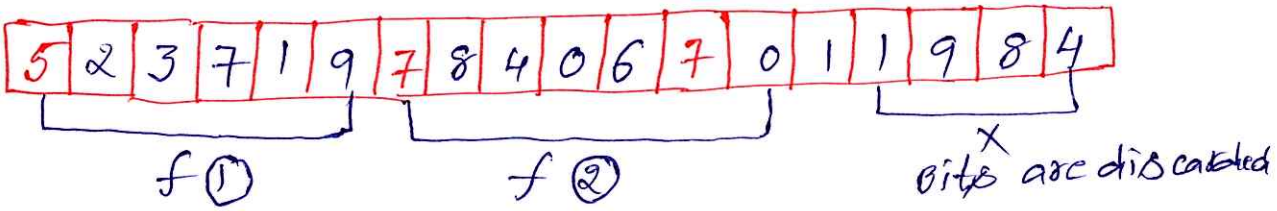
Ex:- 2 3 7 1 9 8 4 0 6 0 1 1 9 8 4

Message without Error.

Sender is sending the data in the below format



Message with errors

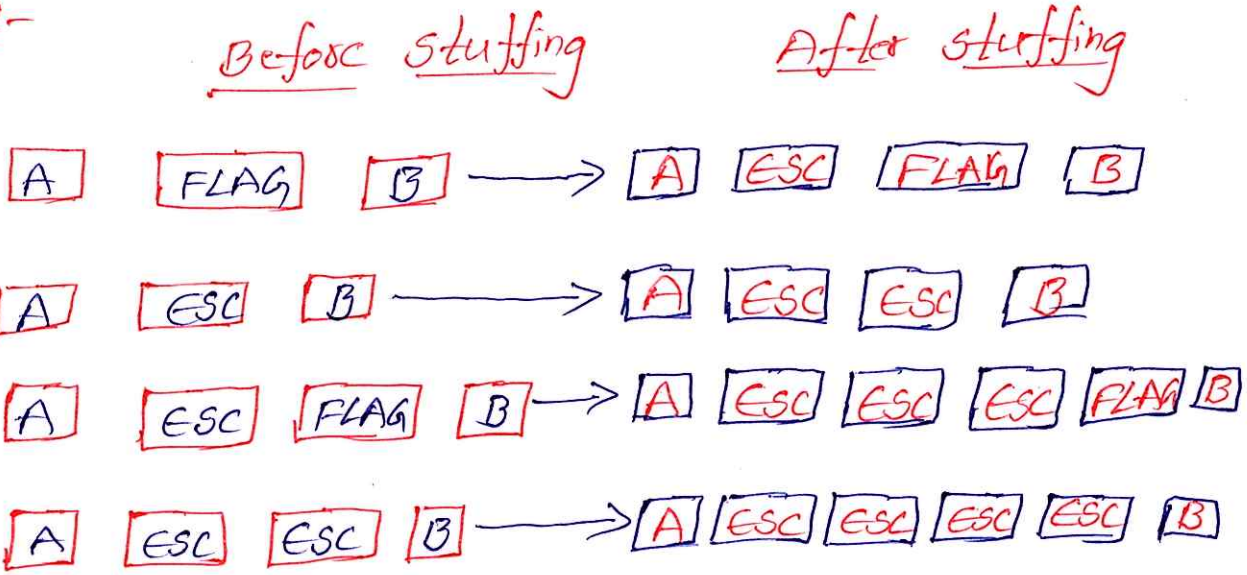


* **Flag bytes with byte stuffing:-** This method is used in point to point protocol. In this method each frame start & end with special bytes, called FLAG byte. If the FLAG byte occurs in the frame then we have to stuff the frame with an extra escape byte (ESC).

Ex:- A frame with flag bytes

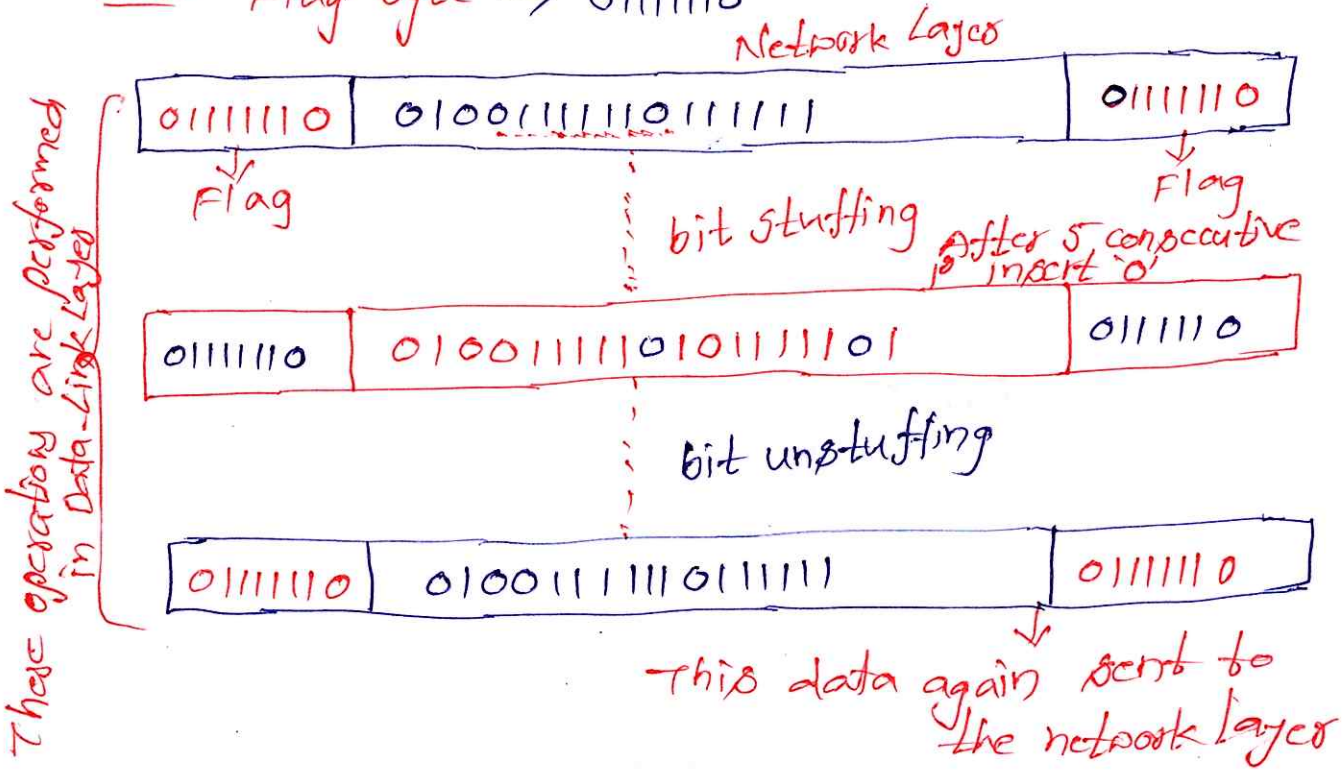
* FLAG → A bit patern that defines the begining and end bits in a frame.
* Header → It contains the source and destination address of the frame.
* payload → It contains the actual message.
* Trailer → It contains the error detection and error correction bits.

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

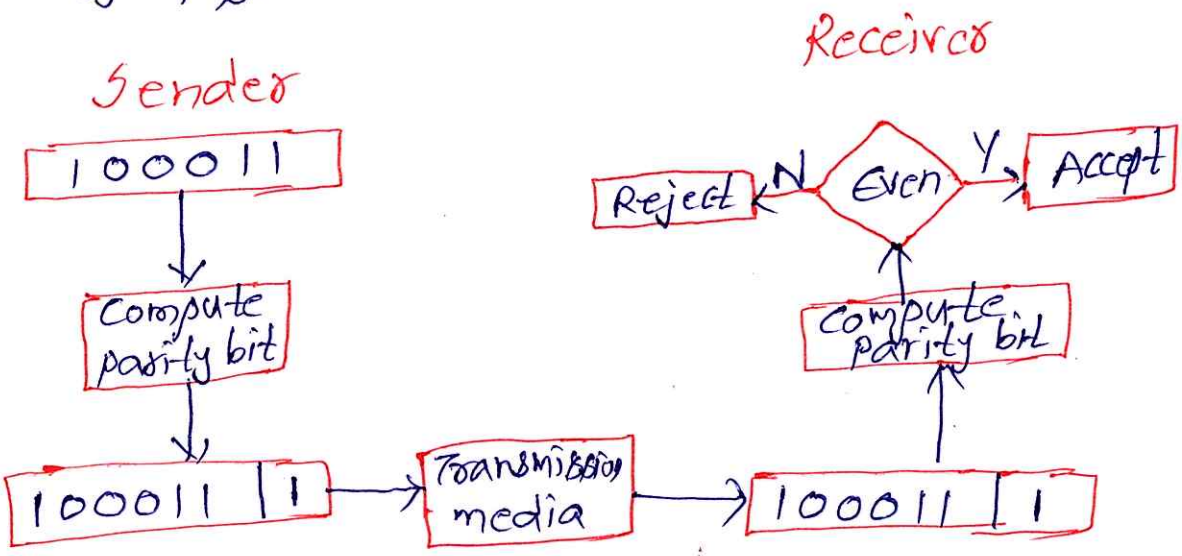
* Error Detection Techniques:-

To detect errors a common techniaue is to indroducc redundancy bits that provide additional information. There are four types of error detection. They aoc

* Simple parity check/single P.C
* Two-Dimensional Parity check
* checksum
* Cyclic Redundancy check (CRC)

* Simple/single parity check:-

* In this method '1' is added to the block if it contains an odd number of '1's (or)
* '0' is added if it contains an even no. of '1's.



* **Two-Dimensional parity check:-** In this method parity check bits are calculated for both rows and columns. Then these both parity bits are sent along with the data.

Ex:- 0100 10, 1100 01, 1001 11, 0001 11

	Row parity
0100 10	0
1100 01	1
1001 11	0
0001 11	1
column parity 0000 11	0

Data to be sent

0100100	1100011	1001110	0001111

* **checksum:-** This technique is based on redundancy. In this process the data is divided into equally sized segments and using a 1's complement to calculate the sum of these segments.

Sending

* Divide into 'n' segments with m bits.
* Add all the segments
* If carry is '1' add it to the LSB of sum.
* Complement the sum to get checksum.
* Msg + checksum sent to receiver.

Receiving

* Divide into sections.
* Add all the segments.
* If carry is '1' add it to the LSB of sum.
* Add checksum received from sender.
* Complement the sum to get checksum.
* If result is '0' accept the msg. otherwise discard.

- Ex:- original Data.

10011001	11100010	00100100	10000100

K=4, m=8

Sender

1. 10011001
2. 11100010
   01111011
   0111 1100
3. 00100100
   10100000
4. 10000100
   00100100
   Sum → 00100101
   Checksum → 11011010

Receiver

1. 10011001
2. 11100010
   01111011
   0111 1100
3. 00100100
   10100000
4. 10000100
   00100100
   ~~Sum~~ → 00100101
   complement → Checksum 11011010
   Sum → 11111111
   complement → 00000000
   Accept data

* Cyclic Redundancy Check:-

In CRC a sequence of redundant bits called cyclic redundancy check bits are appended to the end of the data. Then we perform modulo 2 division on the data. This process is also done in the receiver side. Finally if the remainder is '0' the the data is accepted otherwise rejected.

Sender side

Ex:- original message $M(x) = 11010111$

Generator polynomial $G(x) = x^4 + x + 1$

$= 1.x^4 + 0.x^3 + 0.x^2 + 1.x^1 + 1.x^0$

$G(x) = 10011 \therefore n = 5$ bits

Now $n-1$ no. of zeros are appended to the $M(x)$ at the LSB side. i.e $n-1 = 5-1 = 4$ bits

$\therefore M(x) = 11010111110000$

$G(x) = 10011$

XOR Gate operation

i.e $0\,0 \rightarrow 0$

$1\,1 \rightarrow 0$

$0\,1 \rightarrow 1$

$1\,0 \rightarrow 1$

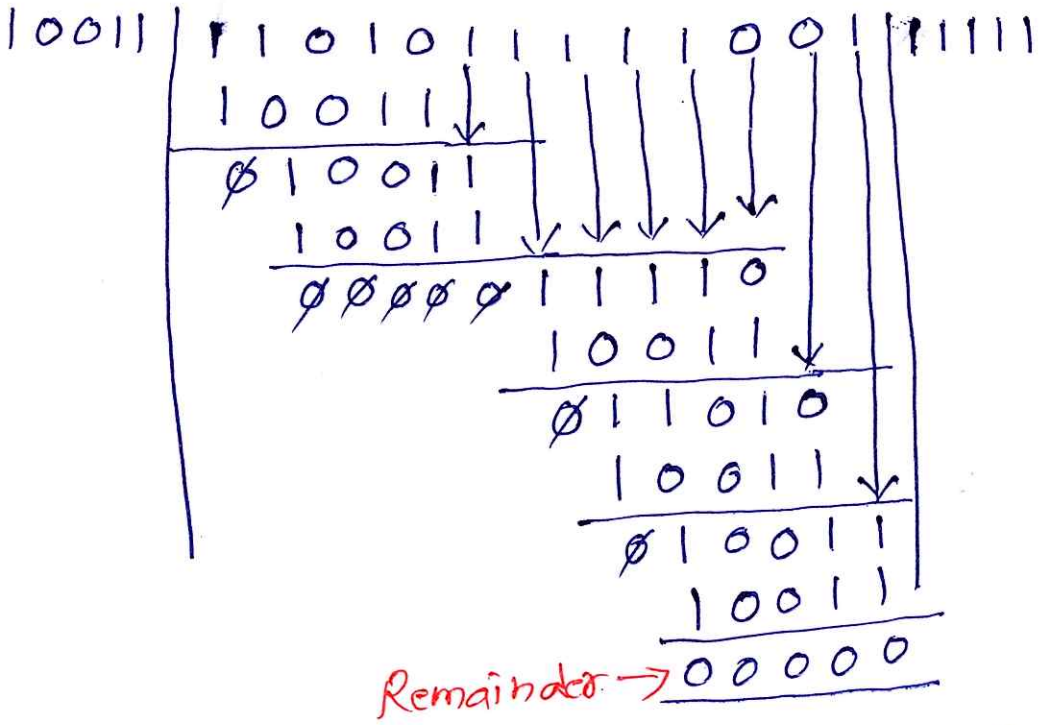
```
10011 | 11010111110000
        10011
        -----
        01001
         10011
         -----
        00000 11100
              10011
              -----
              01111 0
               10011
               -----
               01100 0
                 10011
                 -----
                 0100 1  -> Remainder
```

This remainder can be taken as CRC.

Now original message + CRC = 11010111110011

Receiver Side

Now message M(x) = 11010111111001



If the remainder is '0' no error in the message. So the receiver accepts the data.

* Error correction:- Error correction codes are used to detect and correct the errors. Error corrections can be done in two ways.
* Backward error correction:- once the error is found the receiver requests the sender to retransmit the entire data.
* Forward error correction:- In this case the receiver uses the error-correcting code which automatically corrects the errors.

* What is Hamming Code?

Hamming code is used to detect and correct the errors that can occur when the data is moved from sender to receiver. This technique was developed by Richard Hamming in 1950's. This method is the most effective method to detect single-data bit errors in the original data at the receiver end.

For encoding a message using Hamming code includes the following steps:

* calculating the total no. of parity bits:-

Let us consider that the message contains

m = no. of message bits
p = no. of parity bits

No. of parity bits can be calculated by using the formula.

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

Total no. of bits = m+p

* placing the parity bits in their correct position:-

For example : m=4

then p=3

$2^3 \geq 4+p+1$ p=1 ✗
$2^3 \geq 5+p$ p=2 ✗
$8 \geq 8$ ✓ p=3 ✓

∴ p - parity bits are placed at bit positions of power of 2.

P_1	P_2		P_3				
1	2	3	4	5	6	7	8
2^0	2^1		2^2				

* Calculating the values of parity Bits:-

The parity bits may be even or odd.

Odd parity:- The total no. of 1's are odd then it is odd parity.

Even parity:- The total no. of 1's are even then it is even parity.

Ex:- message m = 0 1 1 0, p = 3 ∴ Messag = 4+3 = 7

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

$2^p \geq 4+p+1$

$2^p \geq 5+p$

$2^3 \geq 5+3$

$8 \geq 8$ ✓

∴ p=1 ✗

p=2 ✗

p=3 ✓

P_1	P_2	m_1	P_3	m_2	m_3	m_4
1	2	3	4	5	6	7
1	1	0	0	1	1	0

P_3	P_2	P_1	
C_1	C_2	C_3	
0	0	0	✓
0	0	1	-1
0	1	0	-2
0	1	1	-3
1	0	0	-4
1	0	1	-5
1	1	0	-6
1	1	1	-7

∴ Now parity bits P_1, P_2, P_3 are calculated as:

$P_1 = 1, 3, 5, 7$

$= P_1, 0, 1, 0$

$= 1010 \quad \therefore P_1 = 1$

$P_2 = 2, 3, 6, 7$

$= P_2\ 0, 1, 0$

$= 1010 \quad \therefore P_2 = 1$

$P_3 = 4, 5, 6, 7$

$= P_3\ 1\ 1\ 0$

$= 0110 \quad \therefore P_3 = 0$

Identify the error position = $P_1\ P_2\ P_3$

$1\ 1\ 0 \rightarrow 6$

∴ Final message : $\overset{1\ 2\ 3\ 4\ 5\ 6\ 7}{1\ 1\ 0\ 0\ 1\ 1\ 0}$

For example receiver receive message as 1100110.

$C_1 = 4, 5, 6, 7 \quad C_1 \rightarrow 1$

$C_2 = 2, 3, 6, 7 \quad C_2 \rightarrow 0 \quad \therefore$ pattern is: $100 = 4$

$C_3 = 1, 3, 5, 7 \quad C_3 \Rightarrow 0$

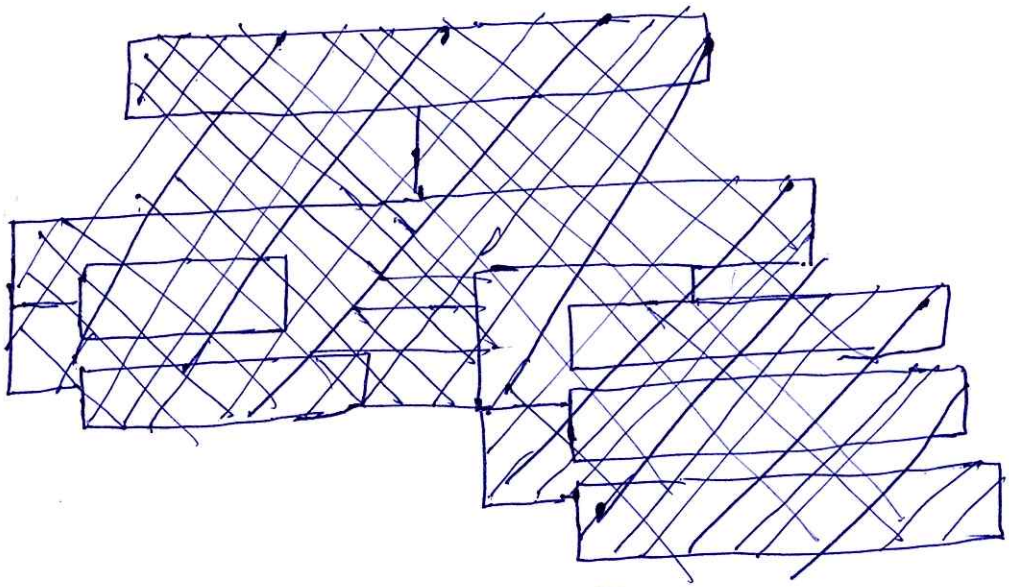
∴ the fourth bit is corrupted.

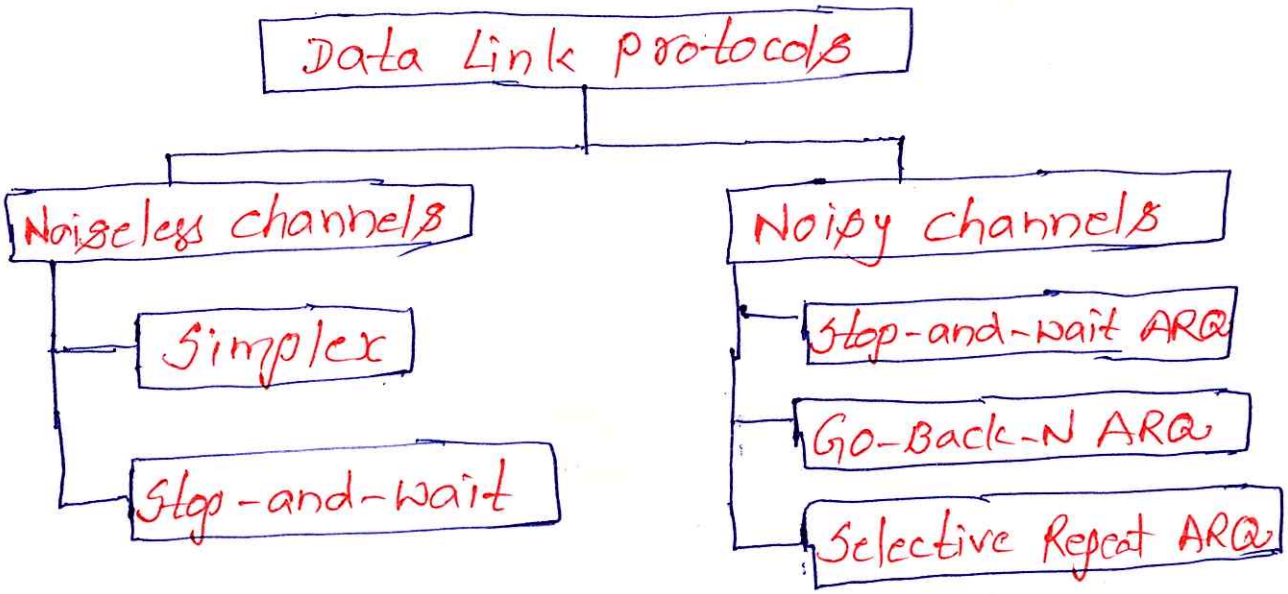
∴ It will correct the message & corrected message is 1100110.

→ 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.



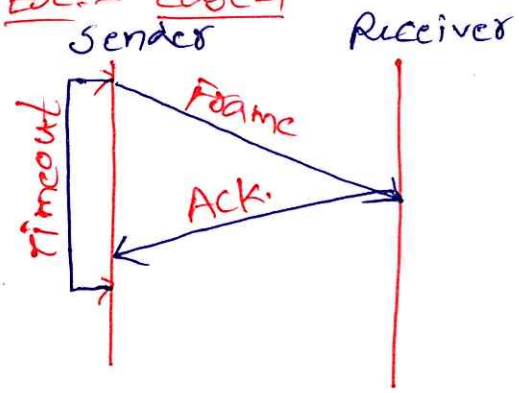


* **Simplex protocol:-** This is a unrestricted simplex protocol. This protocol works on assumption. i.e It can send any amount of data and the data does not have any errors. There is no any acknowledgement from receiver side. It is only one way transmission. The ~~receiver~~ sender can send the data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

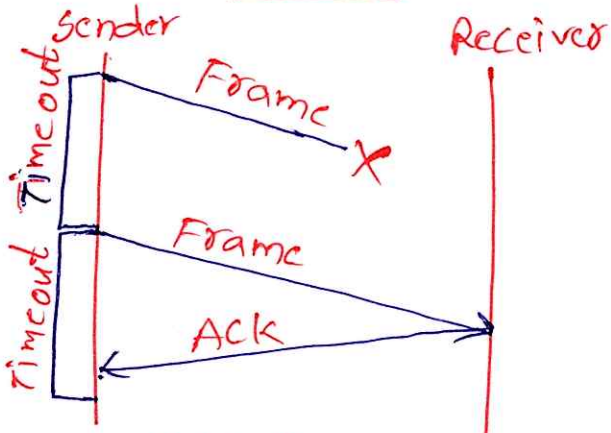
* **Stop-and-wait protocol:-** It is a noiseless protocol or error free protocol. In this protocol the sender sends the message and the message stops and waits ~~for~~ the receivers acknowledgement and then transmits the data. Even though it is a simple stop-and-wait protocal the receiver can have capability 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.

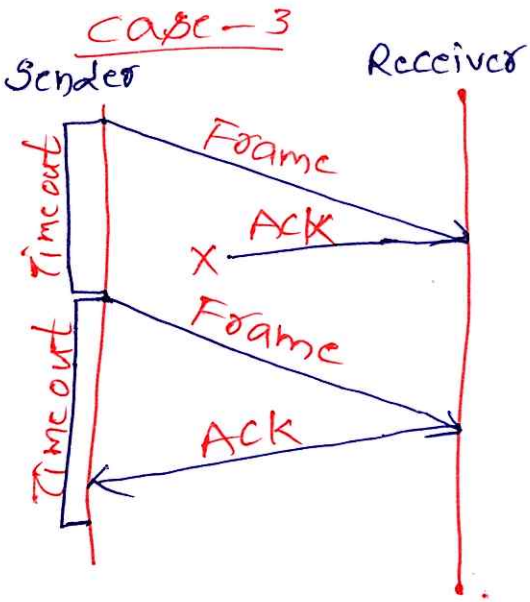
Ex:- case-1



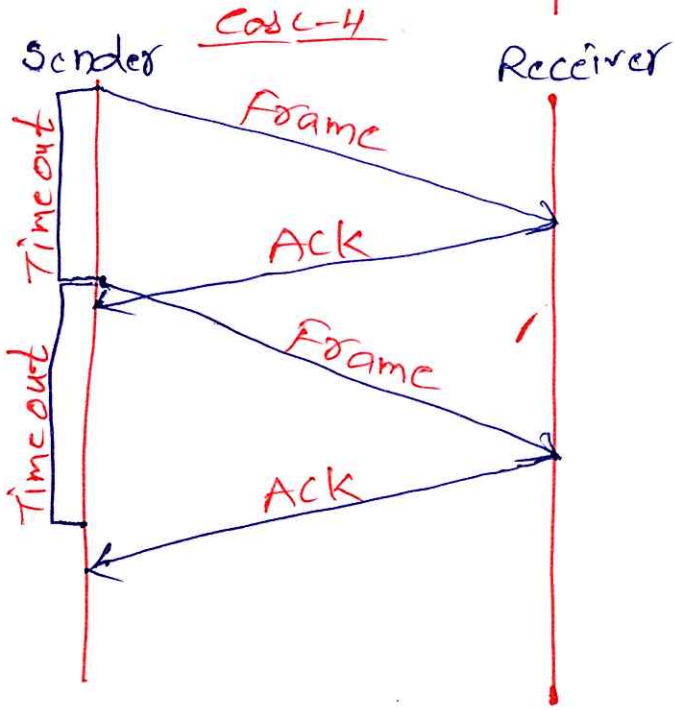
case-2



case-3

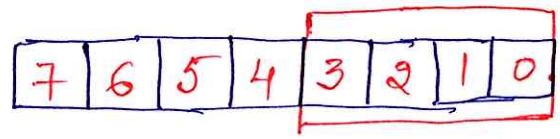


case-4

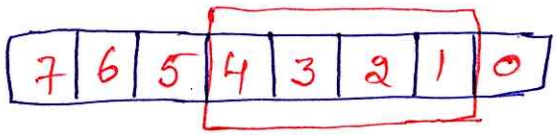


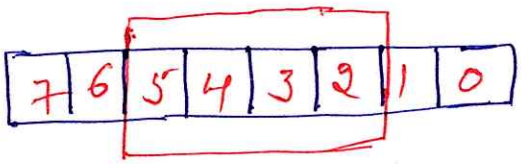
* **Go-Back-N ARQ:-** Go-Back-N ARQ is a sliding window protocol. Here 'N' is the window size. If N=4 the ~~sender~~ Receiver can send 4-frames ~~wit~~ at a time without expecting any Ack.

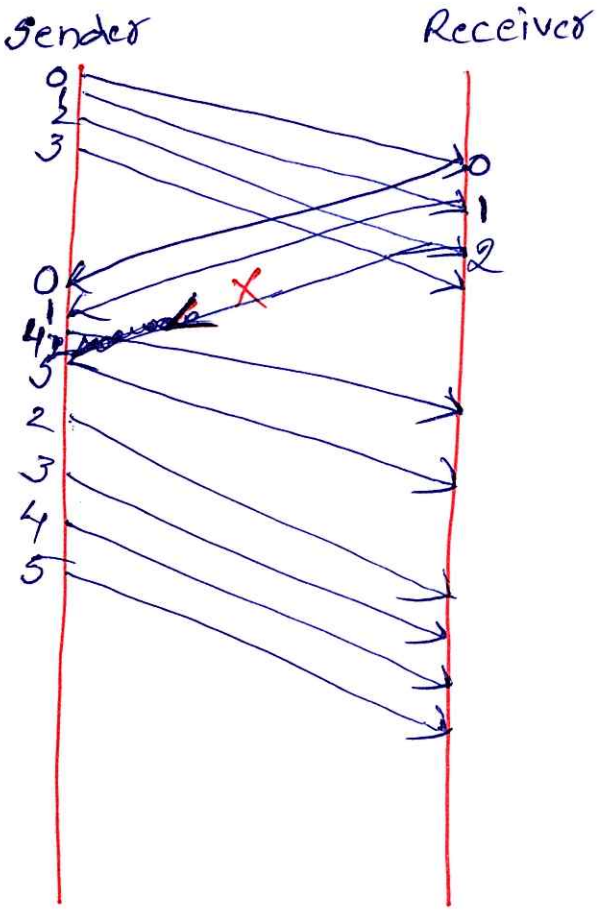
Go-Back-N ARQ uses the concept of pipelining i.e the sender can send multiple frames before receiving the Ack. for the first frame. If the Ack. of a frame is not received within a time period, all frames in the current window are retransmitted.



N=4



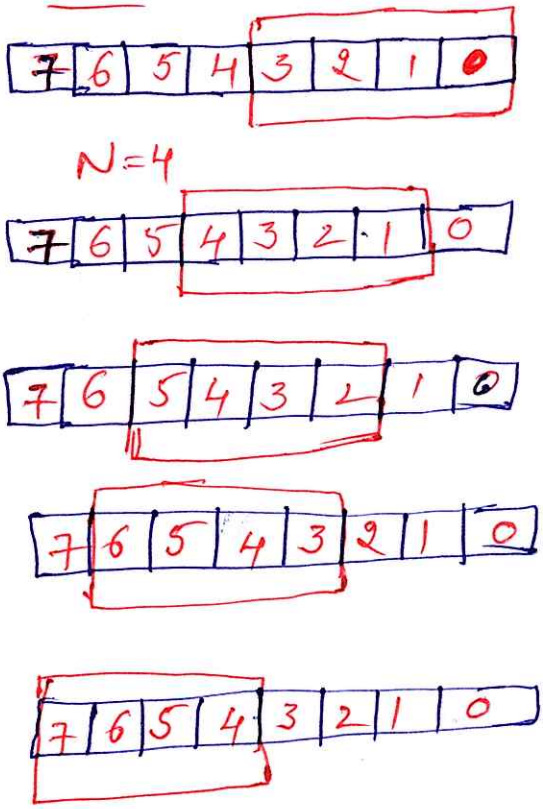


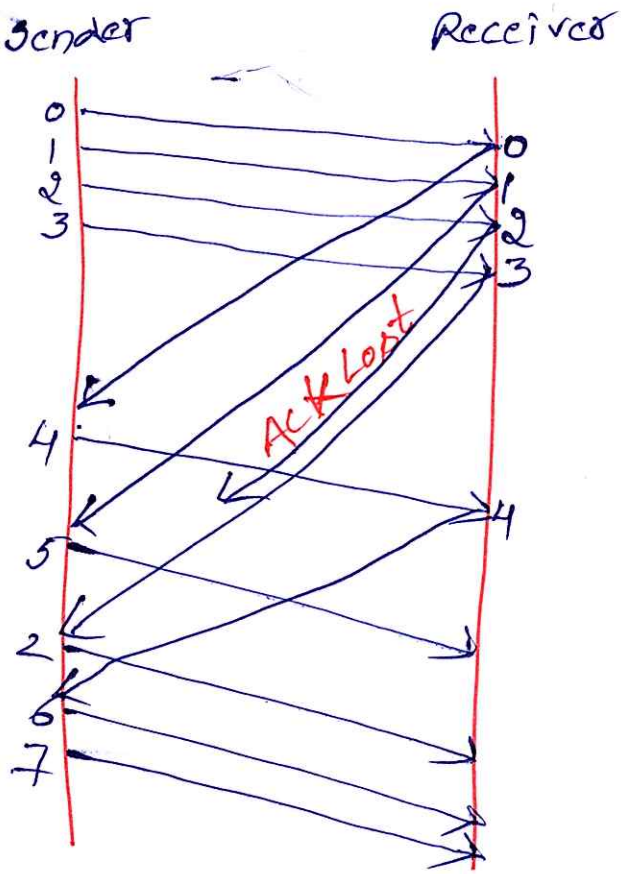


* Selective Repeat ARQ:- It is also a sliding window protocol. In selective Repeat ARQ only the lost frames are retransmitted. while correct frames are received and buffered.

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.

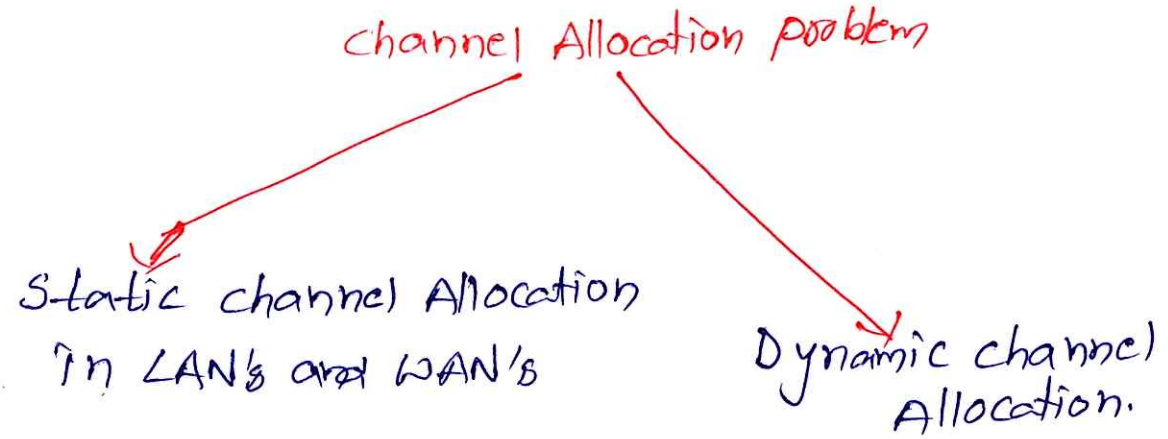
Ex:-





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.

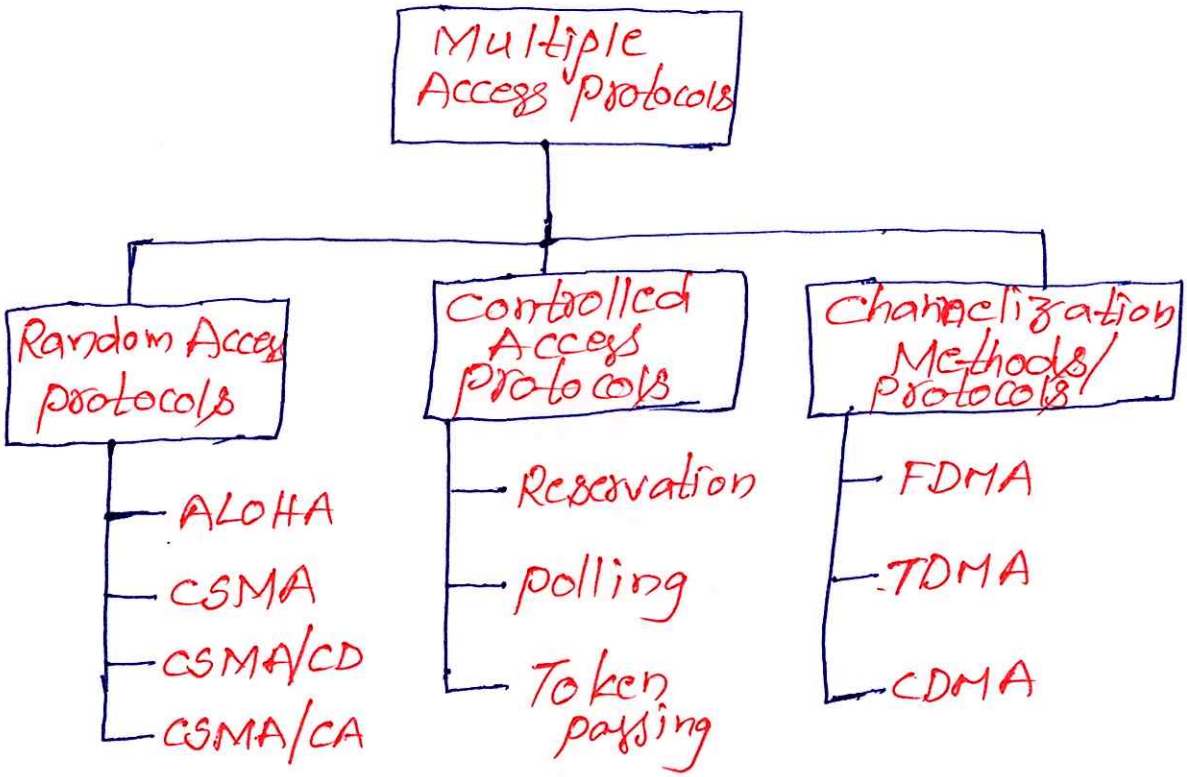
Single channel Assumption: In this allocation all stations are equivalent and can send and receive on that channel.

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.

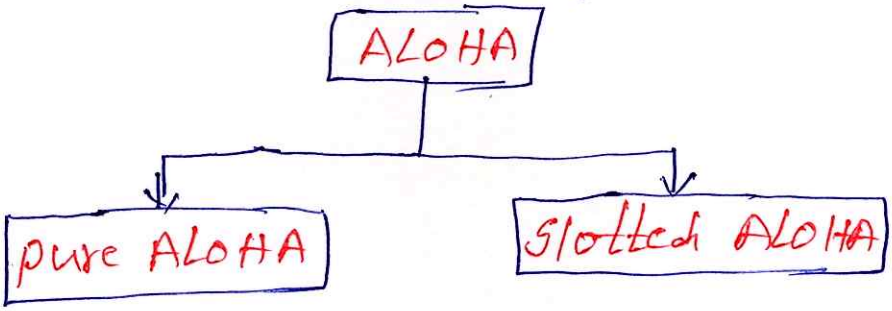
Multiple Access protocols are mainly classified into three types.



→ 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).

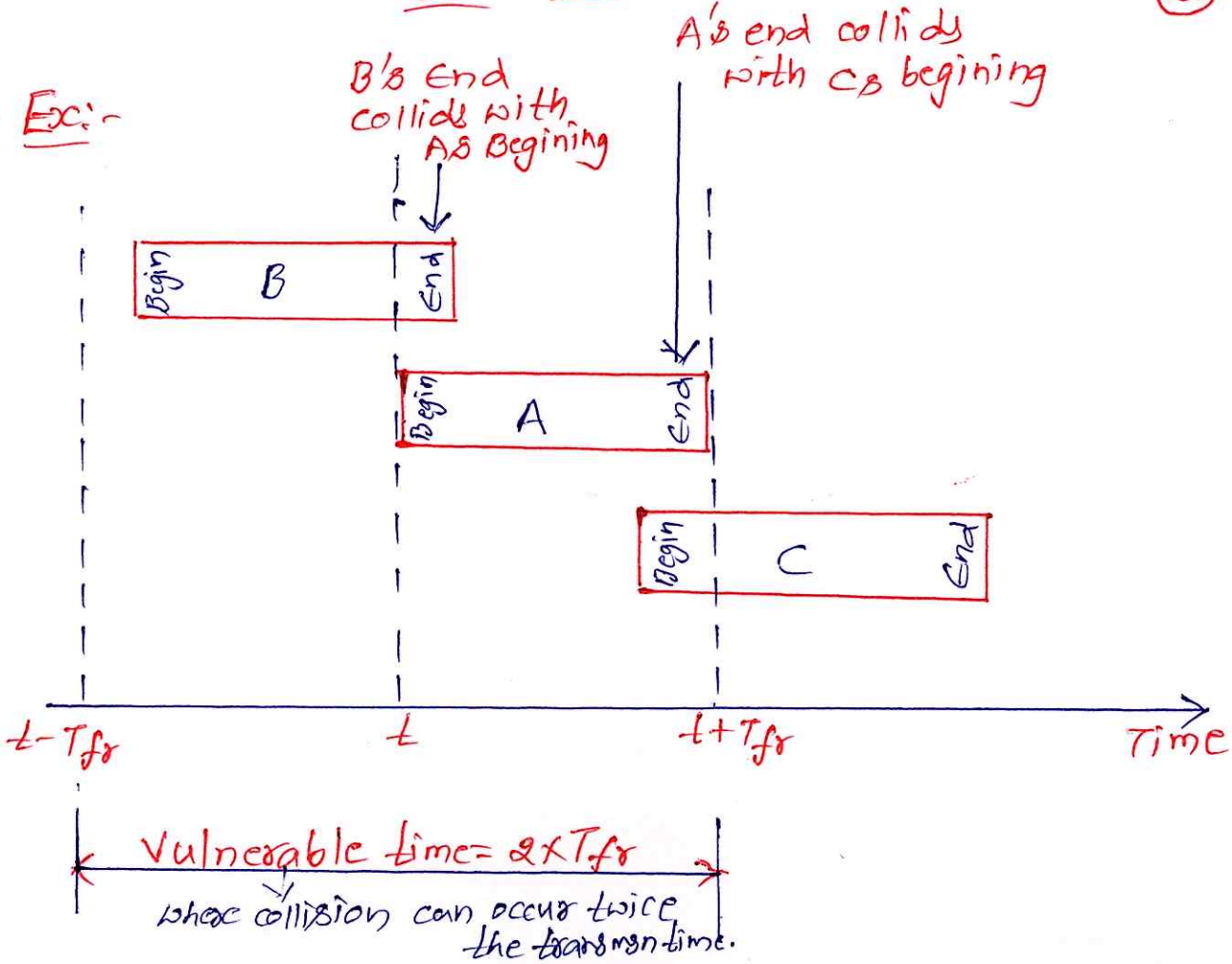
These are two types of ALOHA.



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.

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

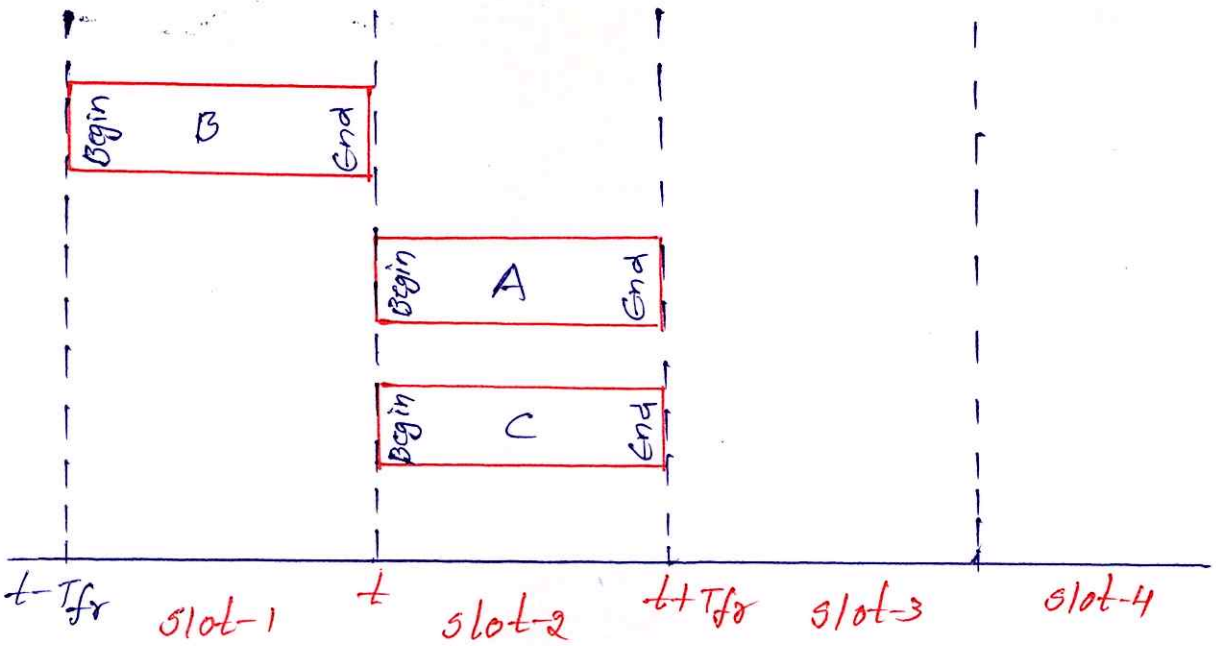
$$S = \frac{1}{2} \times e^{-1}$$

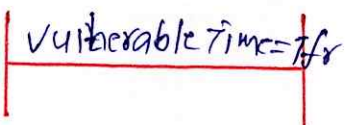
$$S = 0.184$$

$$\therefore S = 18.4$$

* **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 $= T_{fr}$

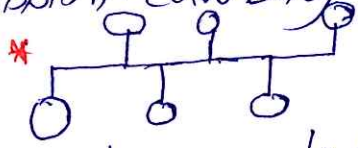
Throughput $S = G \times e^{-G}$

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

$= 0.368$

$S = 36.8$

* 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.



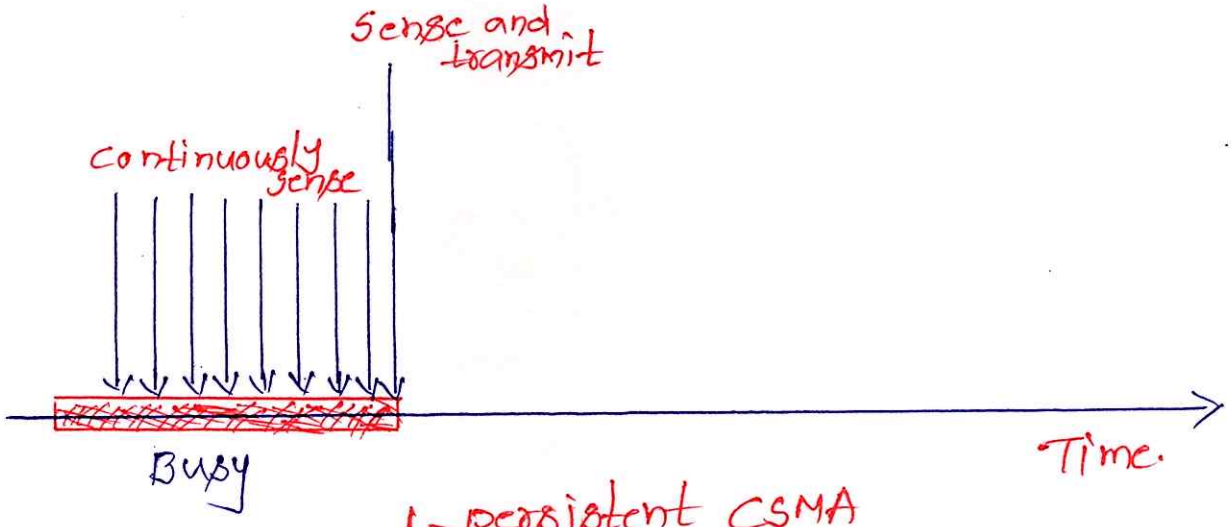
* The possibility of collision still exists because of propagation delay, a station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received.

Types of CSMA:-

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

*a. 1-persistent CSMA:-

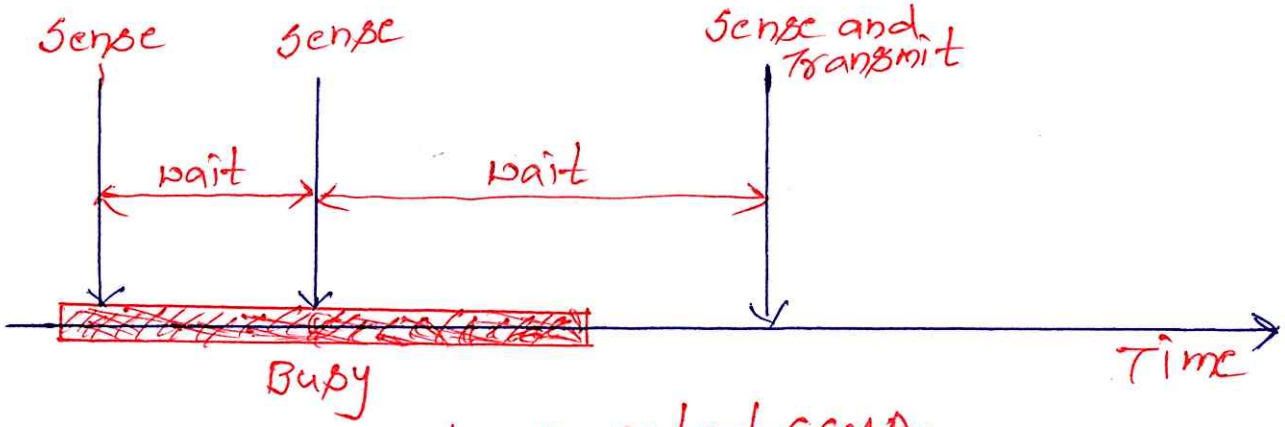
* Before sending the data, the station first listens to the channel to see if anyone else is transmitting the data at that time.
* If the channel is idle, the station transmits a frame.
* If busy, then it senses the transmission medium continuously until it becomes idle.
* Since the station transmits 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:-

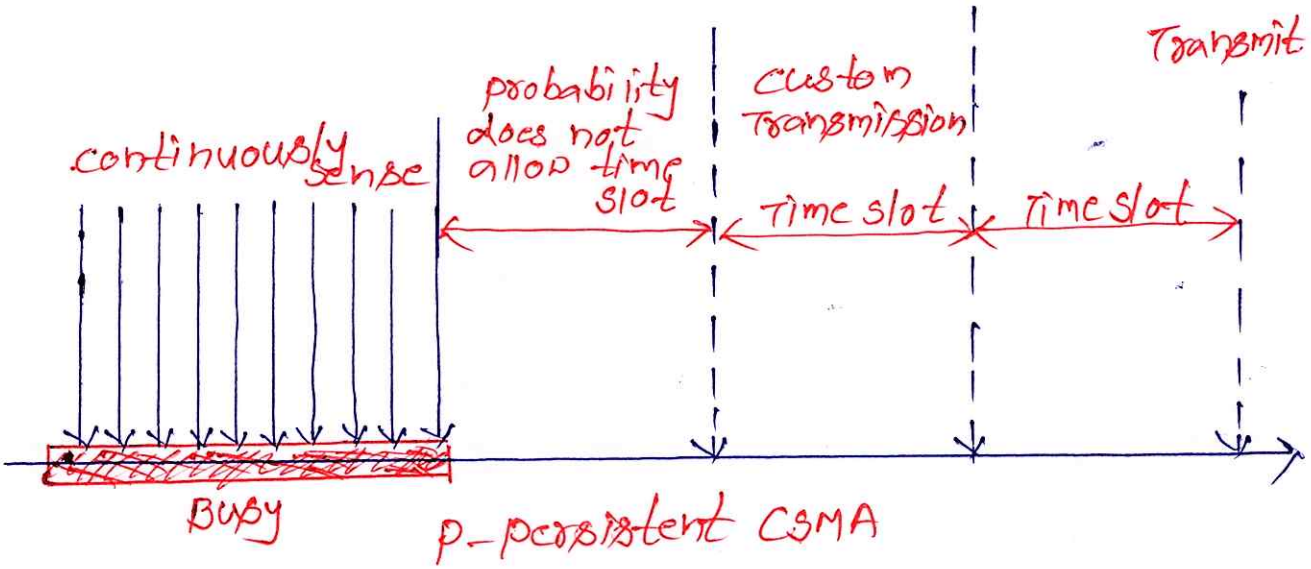
* Before sending a station senses the channel. If no one else is sending the station begins doing so itself.
* However, if the channel is already in use, the station does not continuously senses it for the purpose of seizing it immediately upon detecting the end of the previous transmission.
* Instead, 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.

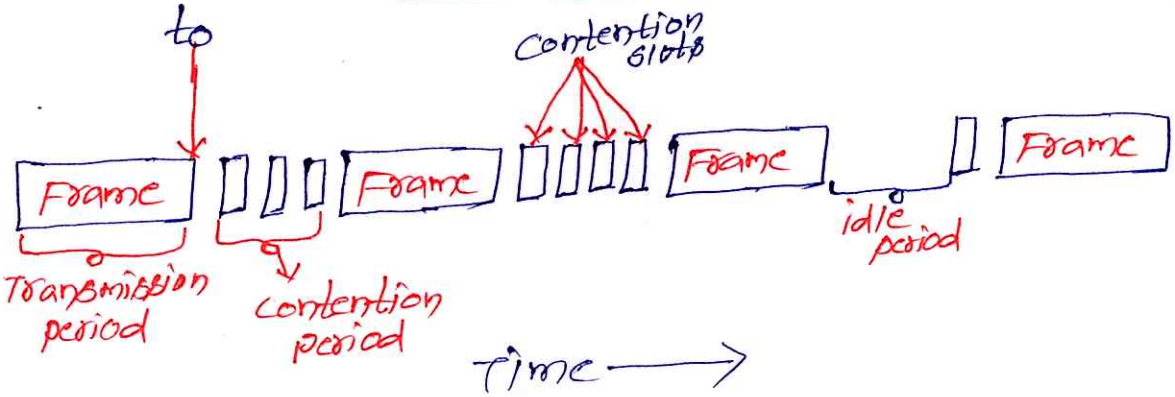
* p-persistent CSMA :-

* 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.

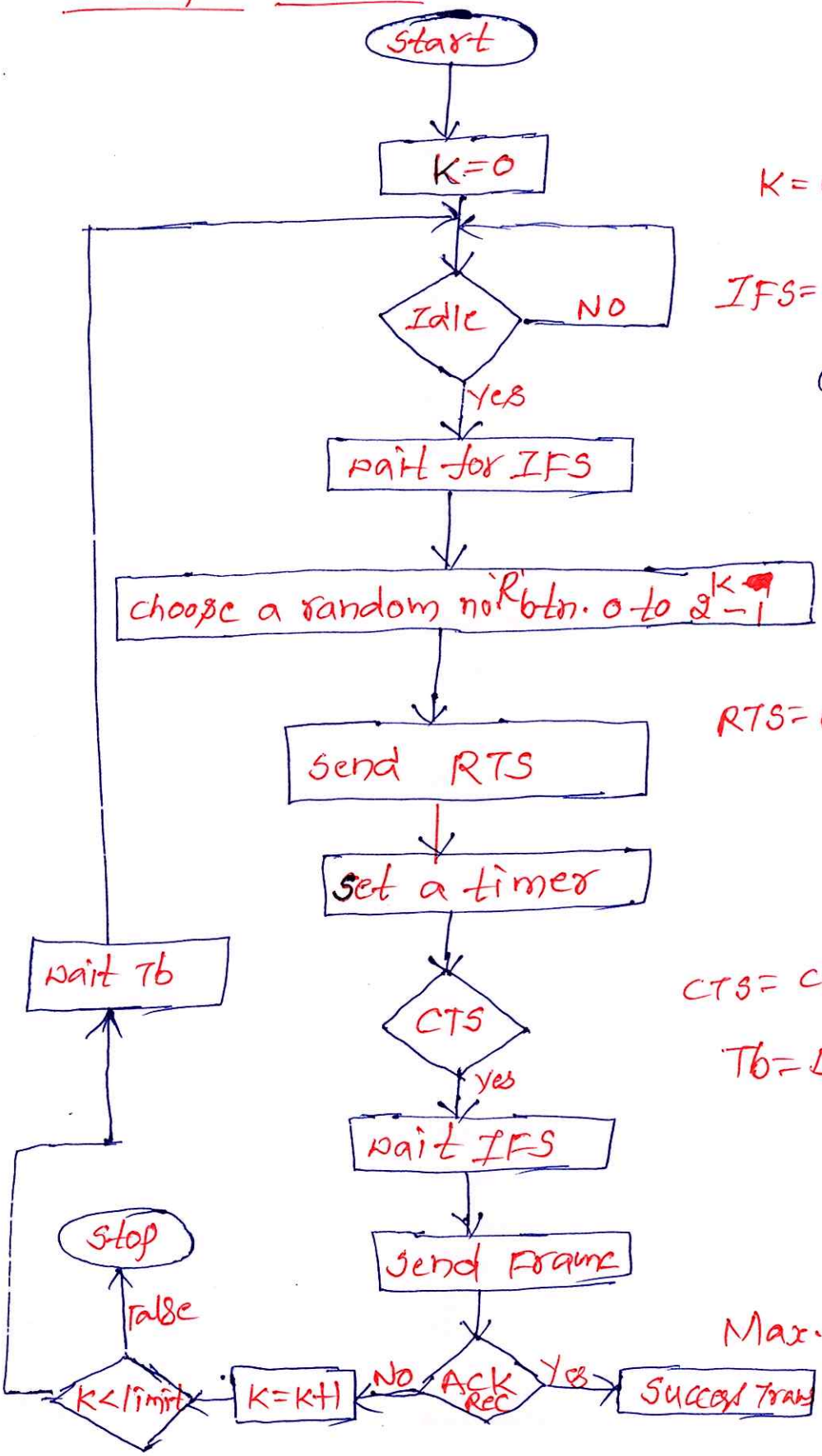
* **CSMA/CD:-** CSMA/CD means Carrier Sense Multiple Access Collision Detection.
  * If two stations sense the channel to be idle and begin transmitting simultaneously, they both detect collision almost immediately.
  * The frames are not transmitted, which are garbled anyway, they should stop transmitting 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

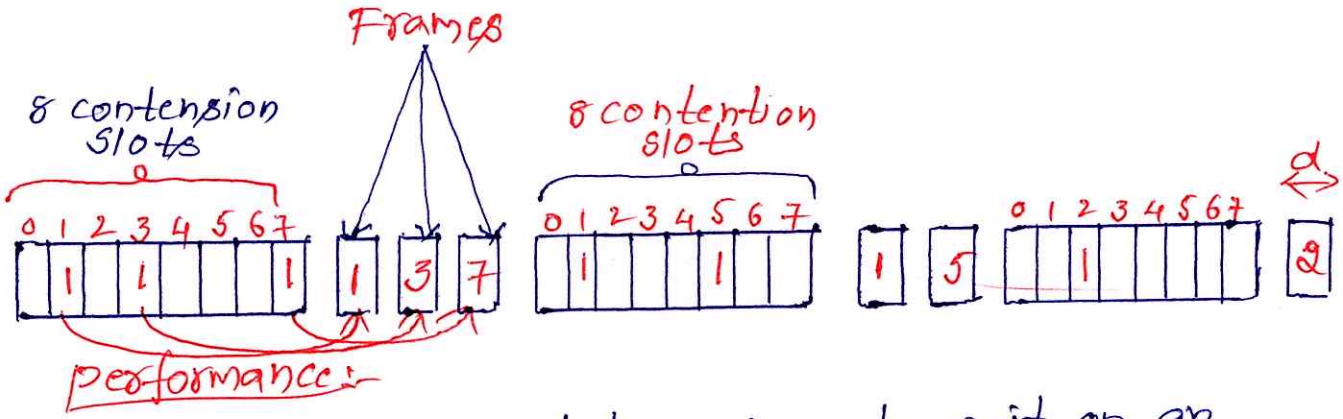
Max. no. of attempts = 14

Collision Free Protocols:-

Almost all collisions can be avoided in CSMA/CD & CSMA/CA, but they can still occur during the contention period. Here are some collision free protocols that resolve the collision during the contention period.

* Bit-map protocol
* Binary countdown pro.
* Limited contention prot.
* The Adaptive Tree Walk protocols.

* **Bit-map protocol:-** Bit-map protocol is a collision free protocol. In bitmap protocol each contension period consists of exactly 'N' slots. i.e (0 to N-1). If any slot has to send a frame then it transmits '1' bit in the corresponding slot. For example if station '2' has a frame to send, it transmits '1' bit to the 2nd slot. In this way each station has complete knowledge of which station wishes to transmit. There will be no collisions because everyone knows which stations wants to transmit. This type of protocols are called "Reservation protocols."



* Low numbered stations have to wait on an average of 1.5 N slots.
* High numbered stations have to wait on an average of 0.5 N slots.

$$\text{Avg. delay} = \frac{1.5N + 0.5N}{2}$$

$$= \frac{2N}{2}$$

$$\text{Avg. delay} = N \text{ slots.}$$

* efficiency on low load $= \frac{d}{d+N}$ $\because d$ = frame size.

* efficiency on high load $= \frac{N \cdot d}{d \cdot N + N}$

$$= \frac{N \cdot d}{N(d+1)}$$

$$= \frac{d}{d+1} //$$

* Binary Countdown:-

Binary countdown protocol is used to overcome the overhead 1 bit per binary station. In binary countdown, binary station addresses are used. A station wants to use the channel broadcast its address as binary bit string starting with the higher order bit. (*)

In this method different station addresses are read together who decide the priority of transmitting. (*) All addresses are of same length. The bits in each addres position of the hosts are boolean ored by the channel.

Ex:- For example 4 stations are wish to transmit. Their addresses are 0010, 0100, 1001, 1010.

					Countdown			
					0	1	2	3
A →	0	0	1	0	0	–	–	–
B →	0	1	0	0	0	–	–	–
C →	1	0	0	1	1	0	0	–
D →	1	0	1	0	1	0	1	0
					1	0	1	

∴ station 'D' transmits the frame

* Limited Contention Protocols:-

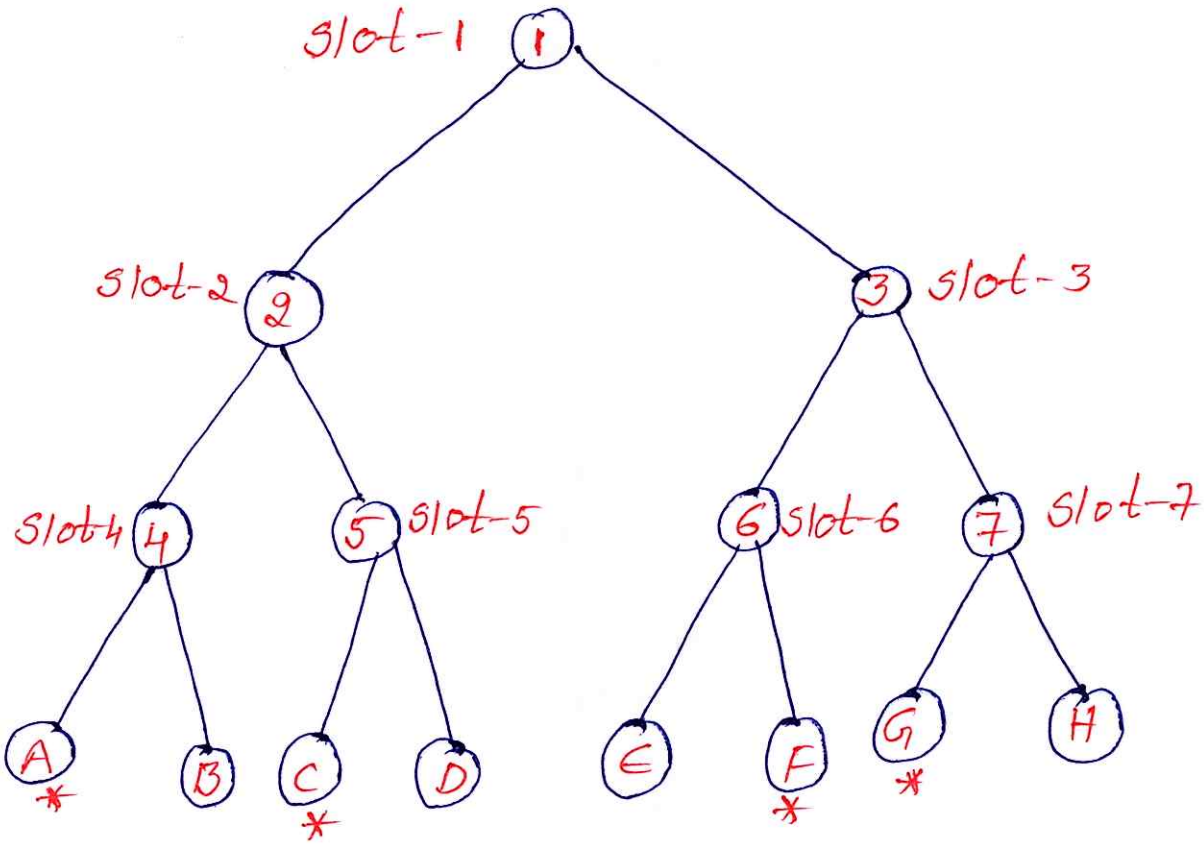
It combines both collision based protocols i.e pure Aloha, slotted Aloha & CSMA/CD are good when the network load is low. Collision free protocols like Bitmap, Binary countdown are good when load is high.

* Behaves like ALOHA scheme under light load.
* Behaves like Bitmap scheme under heavy load.

* Adaptive Tree walk Protocol:-

In Adaptive Tree walk protocols ~~or groups of~~ the stations are partitioned into groups. The stations are arranged in the form of a Binary Tree structure. All the stations are treated as leaf nodes.

In this structure each node has assigned a slot. In each slot whenever collision occurred, the Adaptive tree walk protocol applies depth first search in the tree structure to resolve collision. Each time slot corresponds to a node of the tree.



In the above tree structure there are 8 stations which are placed as leaf nodes of binary tree. out of 8-stations only 4-stations wishes to transmit data i.e A, C, F, G. In the slot-1 all the four stations can transmit data then collision occurs. Then it comes to slot-2, in slot-2 only A, C can transmit data. Again collision occurs then it comes to slot-4, now only 'A' can transmit data, here no collision. In the remaining slots all the stations transmit their frames without collision.

Wireless LAN Protocols:-

WLAN protocols are also known as WiFi protocols. WLAN protocols uses the IEEE 802.11 standard to enable wireless communication bth. devices within a limited area such as a home or office. WLAN's uses high frequency radio waves instead of cables for connecting the devices. WLAN uses CSMA/CA protocol.

* Types of WLAN protocols:-

IEEE 802.11 or WiFi has a number of variants, the main among them are.

* **802.11a protocol:-** This protocol supports very high transmission speed of 54 Mbps. It has a high frequency of 5GHz range. This protocol employs orthogonal Frequency Division Multiplexing (OFDM) which is well suited for the office environment.
* **802.11b protocol:-** This protocol operates within the frequency range of 2.4GHz and supports 11Mbps speed. It uses Multiple Access method known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with Ethernet

protocol. Even though this bandwith is low compared to 802.11a protocol but it greatly facilitates path sharing. Implementation of this protocol is low-cost with good data transmission signal.

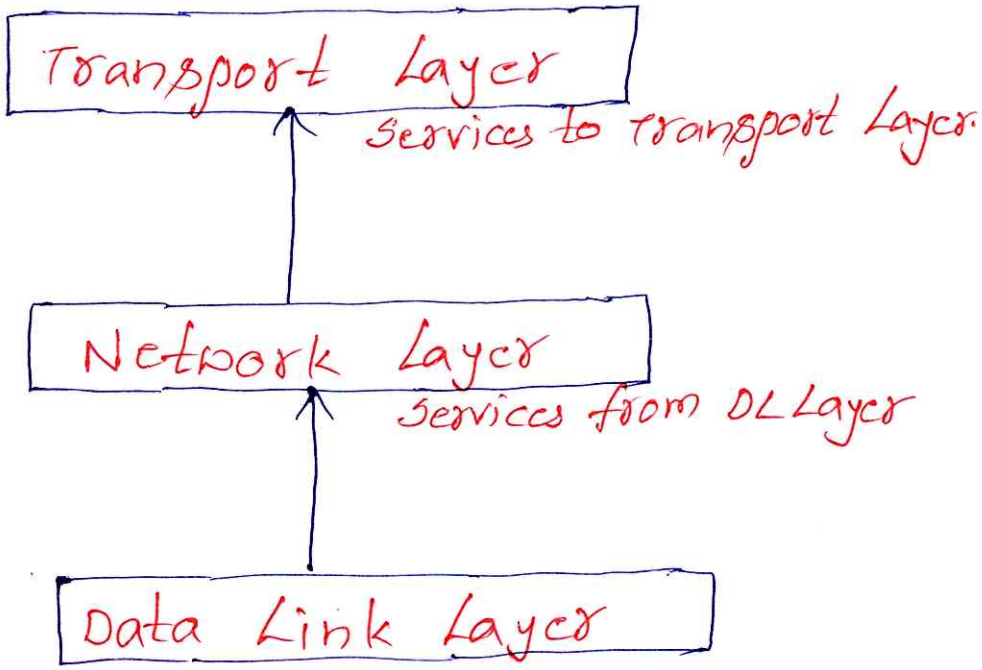
* 802.11g protocol:- This protocol combines the features of 802.11a and 802.11b protocols. It supports both frequency ranges 5 GHz as in 802.11a and 2.4 GHz as in 802.11b protocol. 802.11g is backward compatible with 802.11b devices. That means it can work interchangeably with their access points and network adaptors. This protocol is more expensive for implementation.

* 802.11n protocol:- It is popularly known as Wireless N protocol. This is an upgraded version of 802.11g. It provides very high bandwidth upto 600 Mbps. It uses Multiple Input/Multiple output (MIMO) having multiple antennas at both the transmitter end and receiver end. If there is any signal obstruction it uses alternative routes for data transmission. This protocol is highly expensive for implementation.

Computer Network UNIT-3

➡ Network Layer Design Issues :-

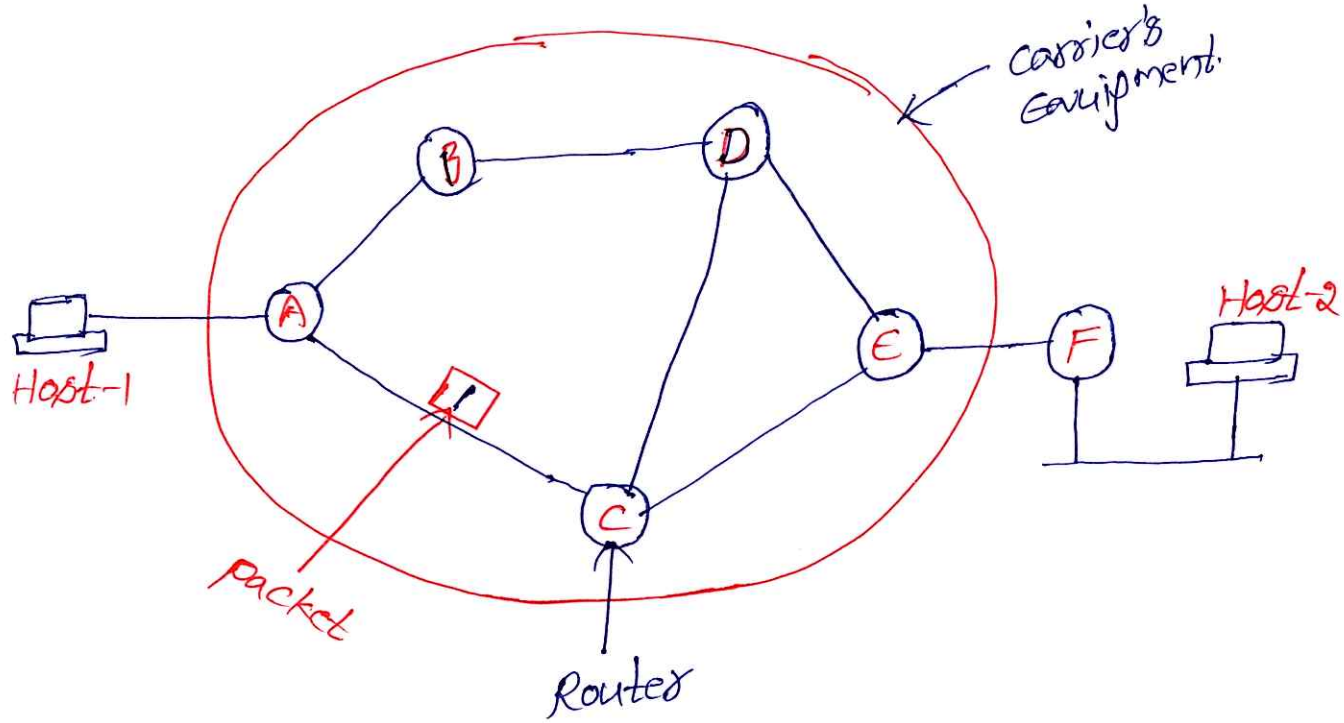
The Network Layer is located between Data Link Layer and Transport Layer. It receives services from Data Link Layer and provides services to the Transport Layer.



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:-

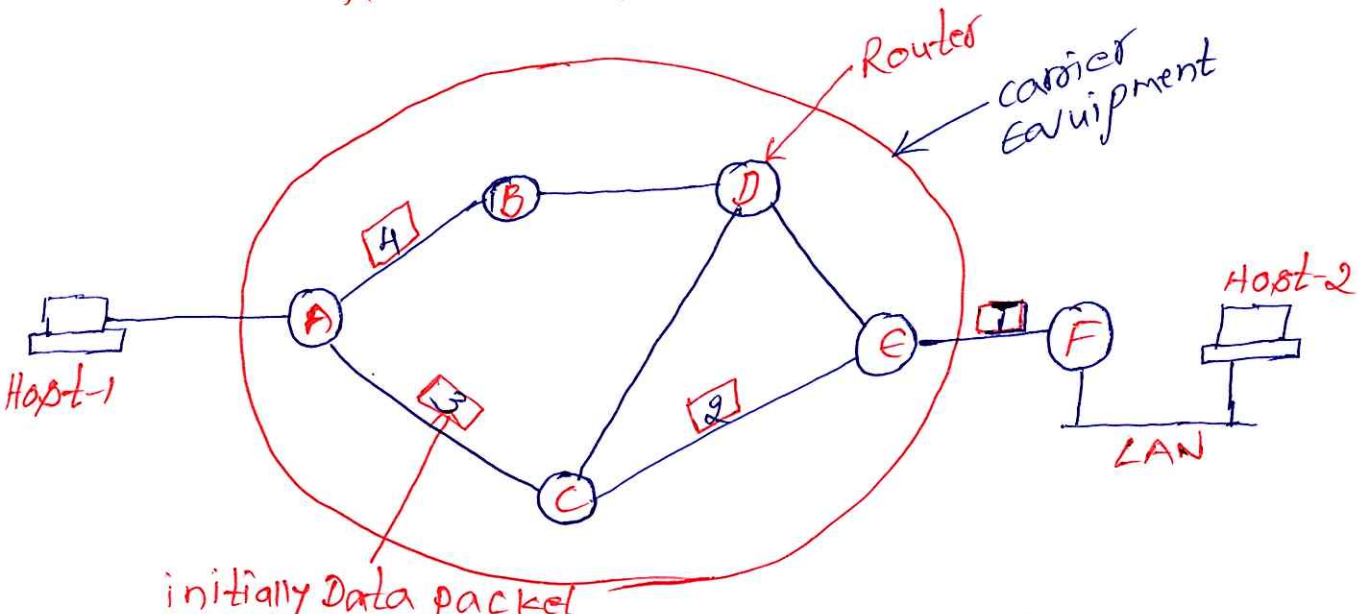


* A host with a packet to send, transmits it to the nearest router either on its own LAN or over a point-to-point link to the carrier (ISP).
* The router waits for the packet until it has fully arrived then the checksum can be verified.
* Then it is forwarded to the next nearest router along the path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

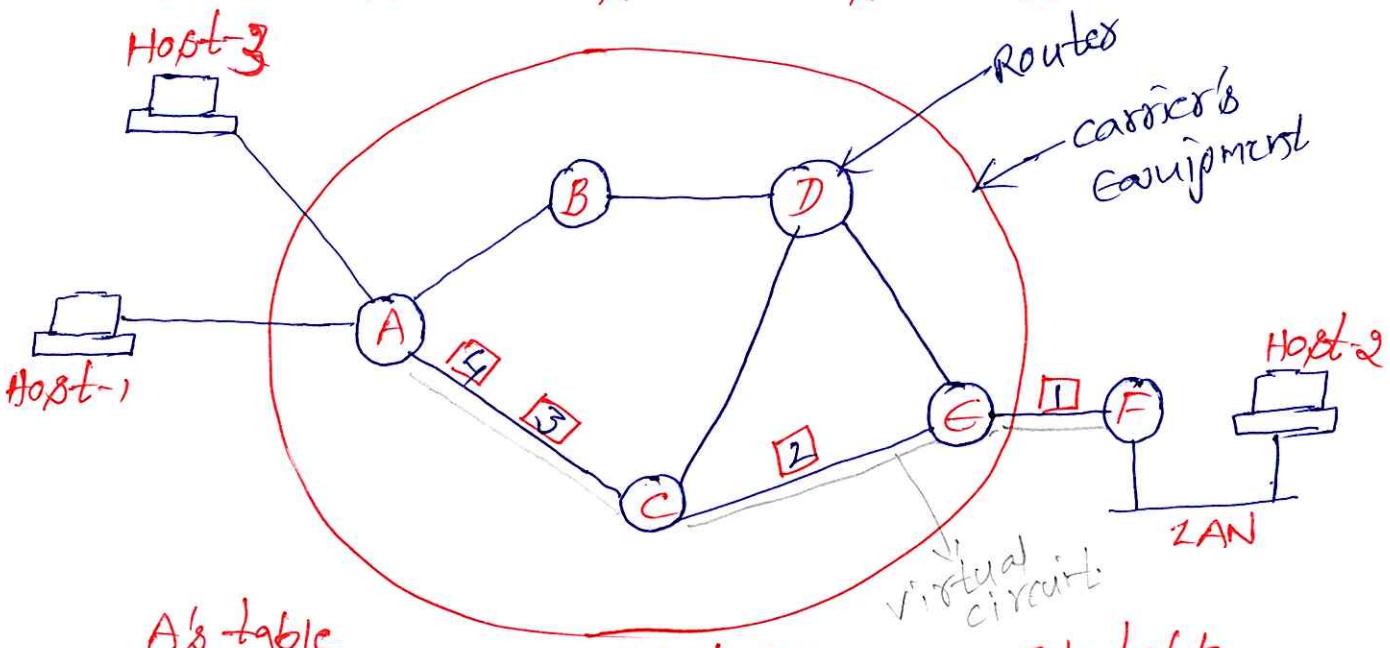
A	A
B	A
C	–
D	D
E	E
F	E

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.

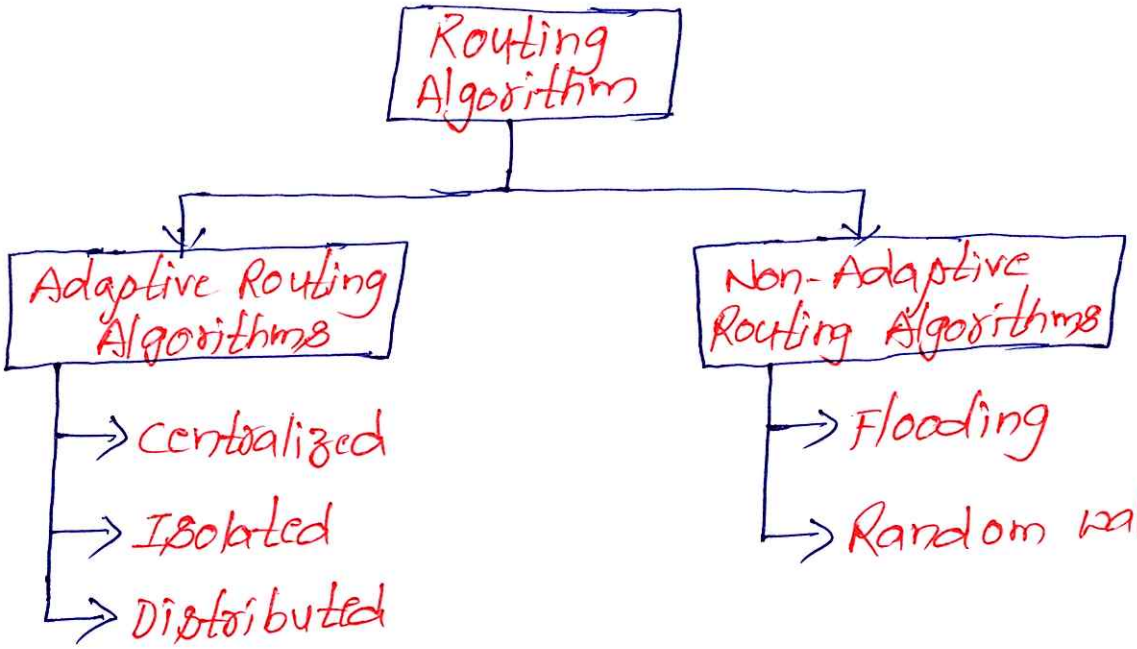
* comparison of virtual circuit Vs Datagram network:-

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.

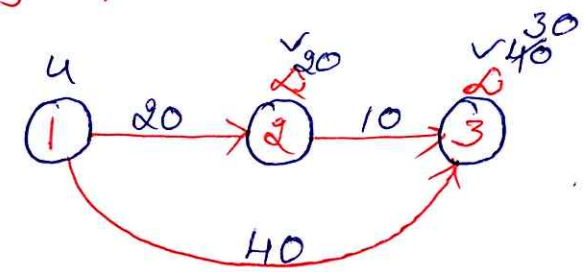
* **Single-source shortest path Algo:-** In single-source shortest path Algo. we will consider any one node as a source, and we have to find the shortest path from the source node to all the remaining nodes in the given graph. we have two types of single-source shortest path Algo. They are → Dijkstra's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

$0 + 40 < \infty$

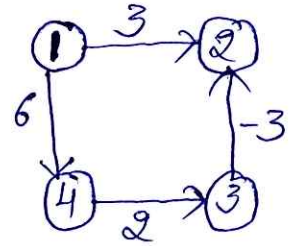
$d(v) = 0 + 40 = 40$

From 2 to 3

$20 + 10 < 40$

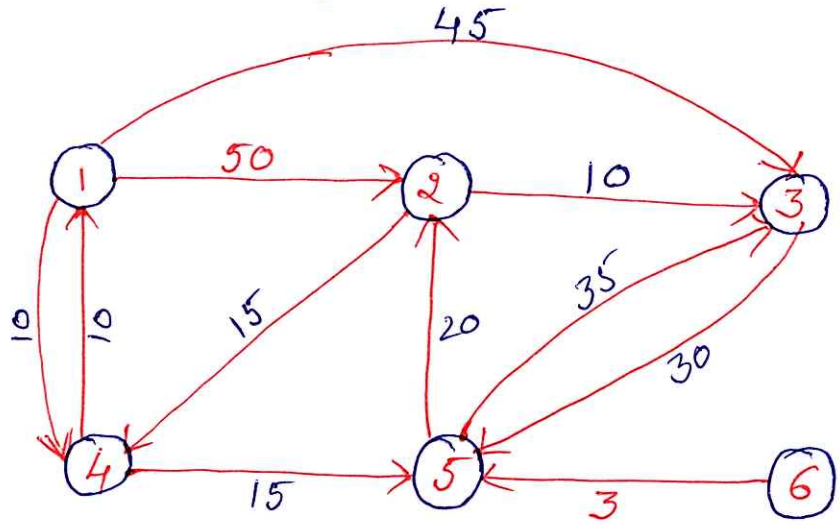
$30 < 40$

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

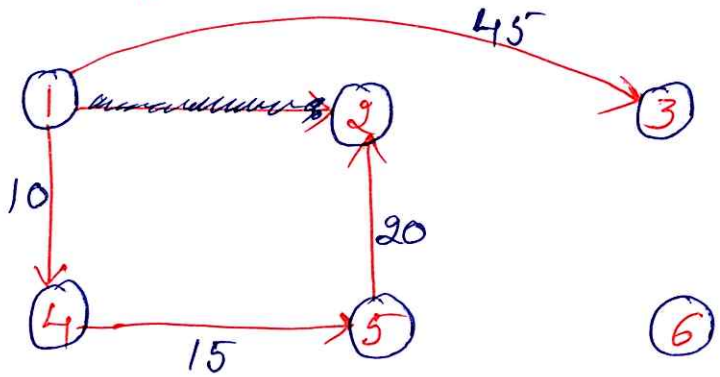


* Dijkstra's Algo. using Directed Graph:-

Eg:-

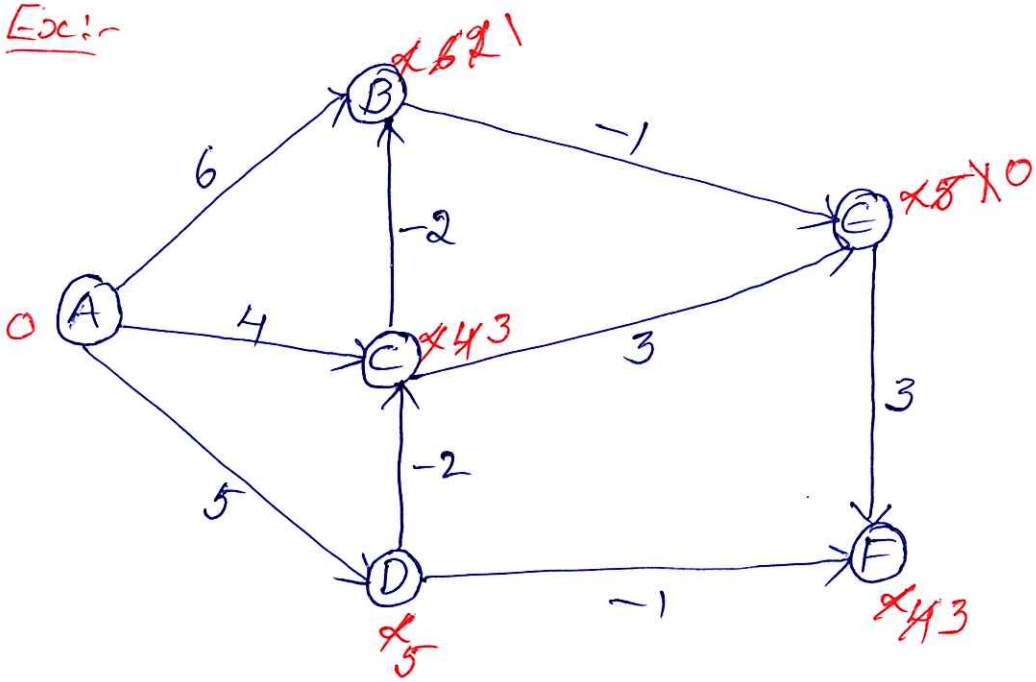


source	Destination				
1	2	3	4	5	6
1	∞	∞	∞	∞	∞
1	50	45	10	∞	∞
1, 4	50	45	10	25	∞
1, 4, 5	45	45	10	25	∞
1, 4, 5, 3	45	45	10	25	∞
1, 4, 5, 3, 2	45	45	10	25	∞



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

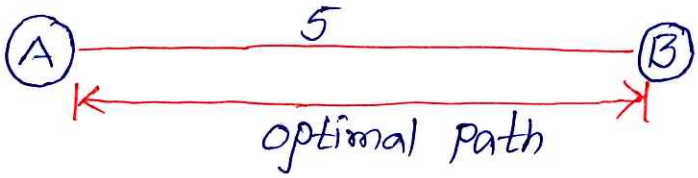
Itr-1

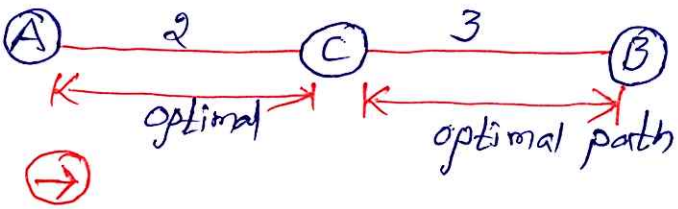
A-B → 6
A-C → 4
A-D → 5
B-E → 5
C-B → 2
C-E → 5
D-C → 3
D-F → 4
E-F → 4

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:- (*)





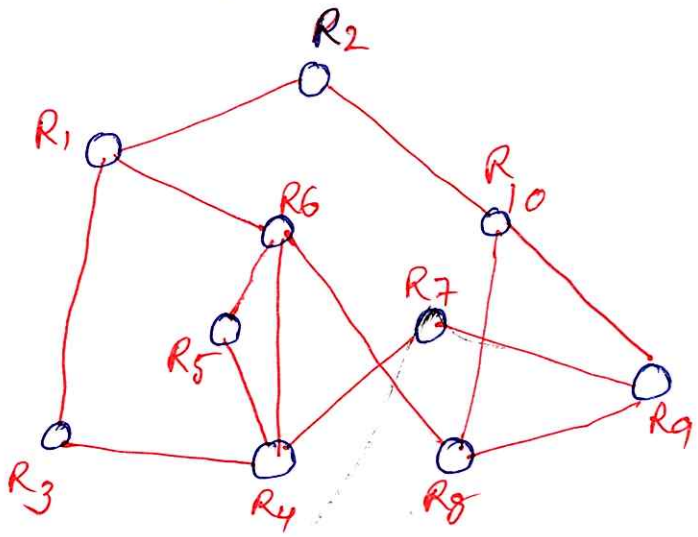
(→)

(*) It is necessary to find the optimal path from source to destination to send packets regardless of network traffic or topology. The router creates a routing table, lists the optimal routes, and selects the best optimal path to send the packets.

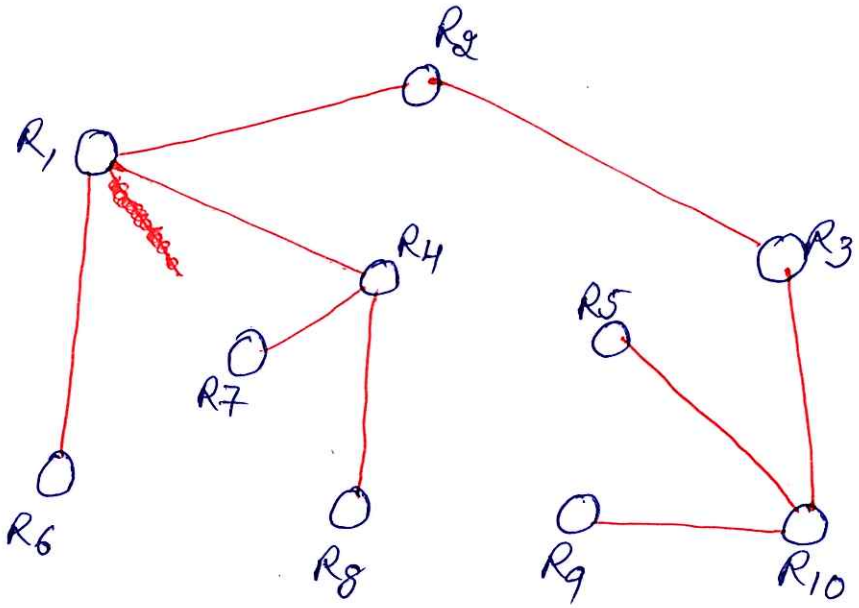
(⇒) In the above figure, If the path from Router-A to Router-B is optimal then if any router-C appears in the middle of this path then the path from Router-A to Router-C and Router-C to Router-B will also be optimal.

The tree is formed when there exists a set of optimal routes from multiple sources to a given destination. This tree is known as the sink tree, in which the distance metric is the number of hops.

Ex:-



Network.



Sink Tree of Router-2.

As shown in the above figure, there are 10 Routers on a network. The topology of the router on the left is cyclic, while the sink tree for router-2 is shown on the right.

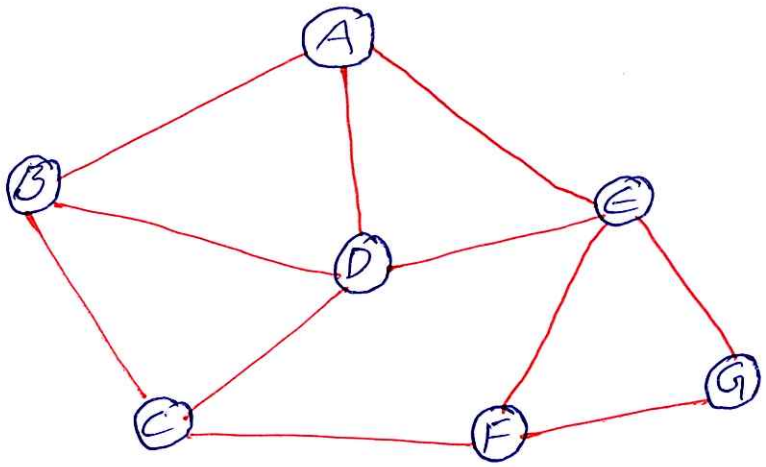
The structure of the sink tree is acyclic graph in which the graph has no loops.

In the sink tree no loops exists, so packets sent by the sender will be distributed within a limited number of routers.

The sink tree is not necessarily unique. It may be possible that there exist other trees with similar path lengths.

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.

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.

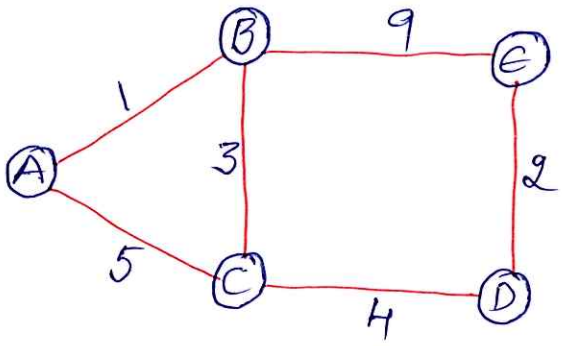
The Distance Vector Routing Algo. shares the information of routing table with the neighbouring routers and keeps the information up-to-date to select an optimal path from source to destination.

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

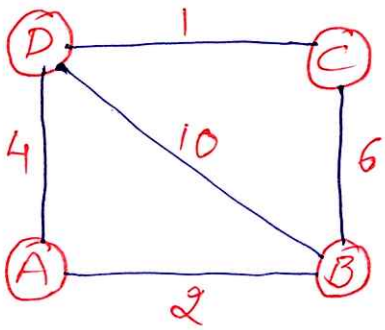
E-B-A-C-4 → 19

* 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

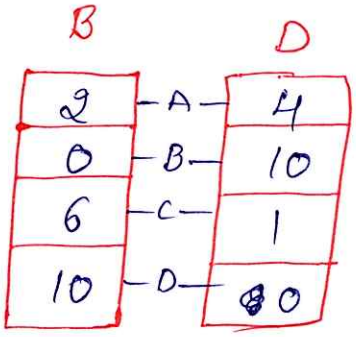
D's

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	∞	4
2	6	10
∞	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

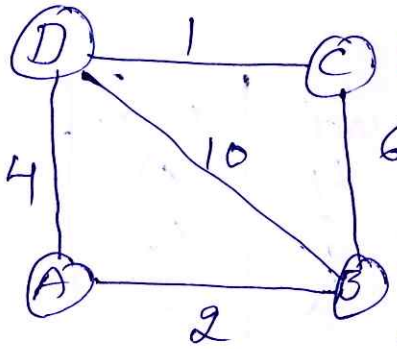
$$d(D-B) = \min \begin{cases} c(D-B) + d(B-B) \\ c(D-A) + d(A-B) \\ c(D-C) + d(C-B) \end{cases}$$

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

* 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

Link State Routing Algo:-

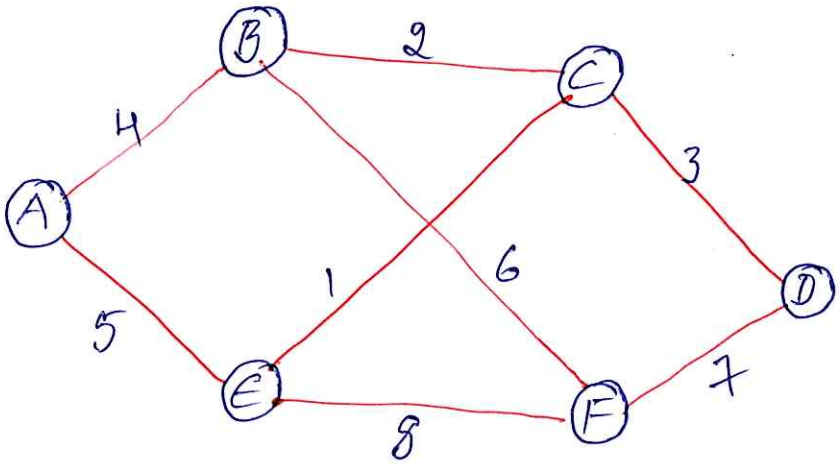
Link state Routing Algo. is a dynamic routing Algo. Link means the edges connected to nodes and state means whether the link is up or down. That means if the link is running or not.

In Link state routing Algo. each router builds a map of the entire network including all links and their costs, and uses this map to calculate the shortest path to every destination.

* Steps in LSR:-

1. At initial stage each router prepares its Link state tables by sending HELLO message packets to its directly connected neighbours and measures the cost of each link.
2. In the second stage the router shares its information using the Flooding technique. By using this Flooding technique each router knows the entire information of entire network.
3. In this stage every router uses the shortest path calculation algorithm like Dijkstras Algo. to calculate the shortest path from a single source to all the destinations.

Ex:-



Step-1:-

A	
Seq	
Age	TTL
B	4
E	5

B	
Seq	
Age	TTL
A	4
C	2
F	6

C	
Seq	
Age	TTL
B	2
E	1
D	3

D	
Seq	
Age	TTL
C	3
F	7

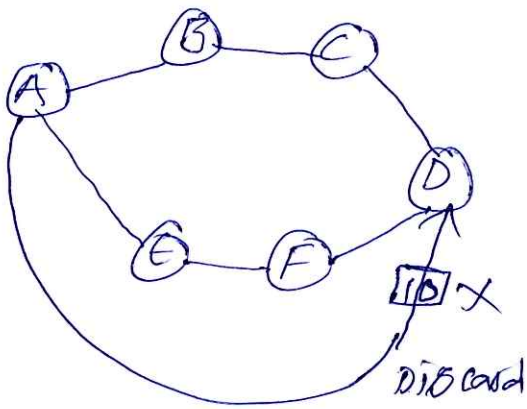
E	
Seq	
Age	TTL
A	5
C	1
F	8

F	
Seq	
Age	TTL
B	6
E	8
D	7

* Sequence number is used to discard older packets from the network.
* Sequence number also reduces the effect of flooding.

Ex:-

Router	Seq. no
A	15
B	20
C	35
D	40

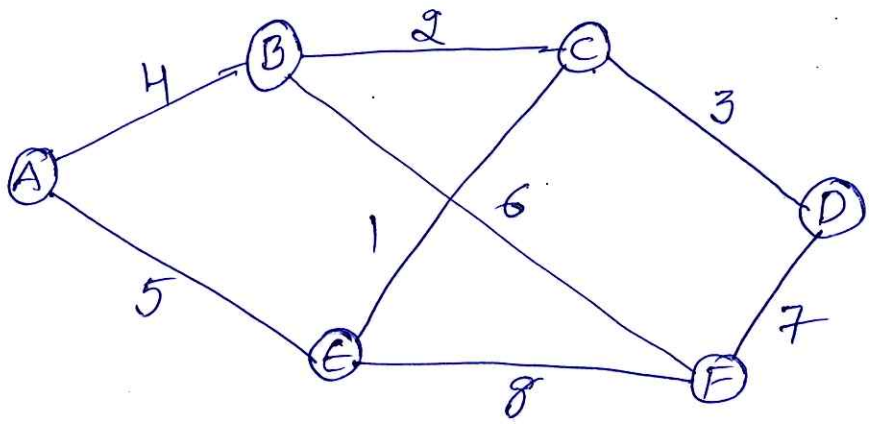


* TTL is used to avoid infinite loops in the network.
* Age is used to avoid issues of network updation.

Ex:-

Router	Seq. NO	Age/Life time
A	15	60
B	20	60
C	38	60
D	40	60

Step-2:- Flooding



* In this stage every router has to prepare a database, to store the every routers information.
* Now every router having the global knowledge of entire network.

Step-3:- Using Dijkstras Algo. finding the shortest path.

source A	destination B	C	D	E	F
A	∝	∝	∝	∝	∝
A	4	∝	∝	5	∝
A, B	4	6	∝	5	10
A, B, E	4	6	∝	5	10
A, B, E, C	4	6	9	5	10
A, B, E, C, D	4	6	9	5	10

Sol:-

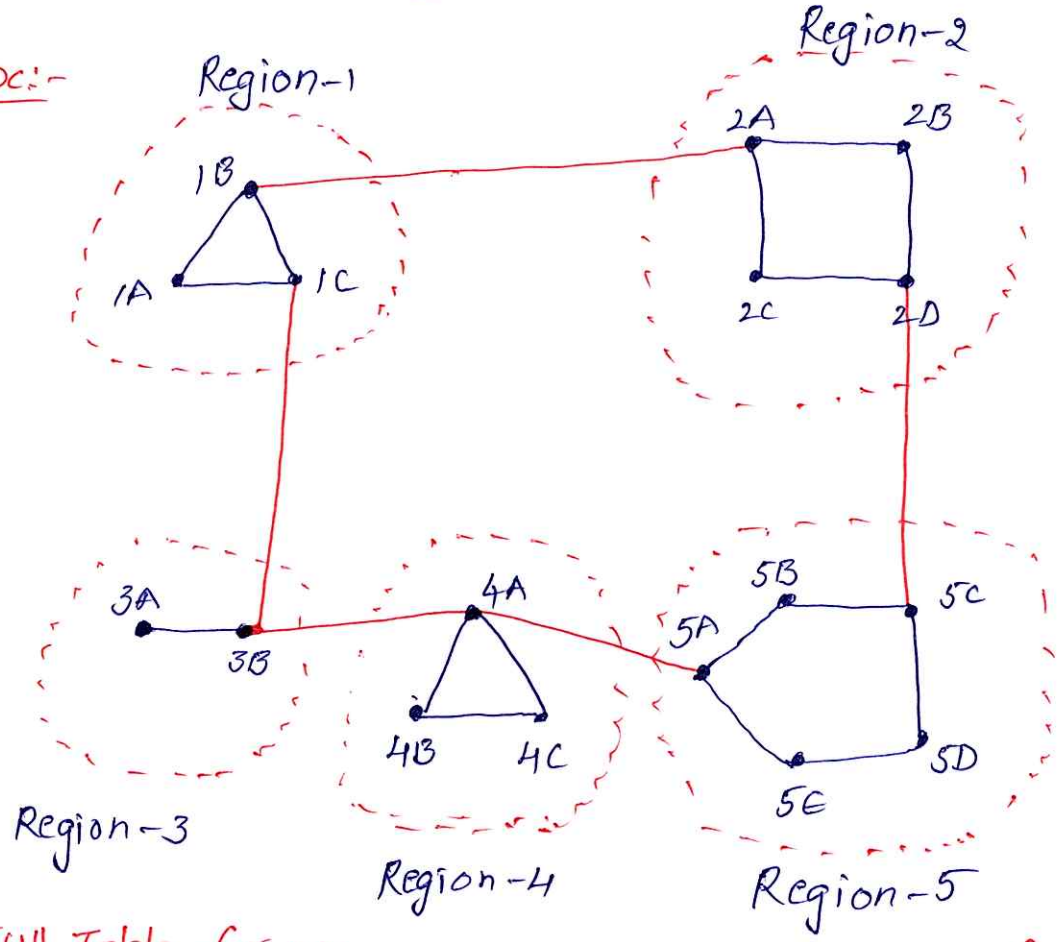
source	dest	cost	Next
A	B	4	B
	C	6	B, E
	D	9	B, E
	E	5	E
	F	10	B

In the same way all the routers build their own routing tables.

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.

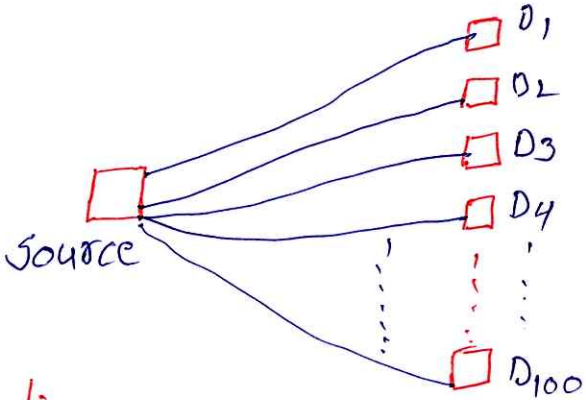
In Broadcasting Routing Algo. the data or signals are transmitted from one source to all the destinations within a network. Unlike routing (one-to-one communication) or multicasting routing (one-to-many communication) broadcast routing ensures that information reaches all devices or nodes within the 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.

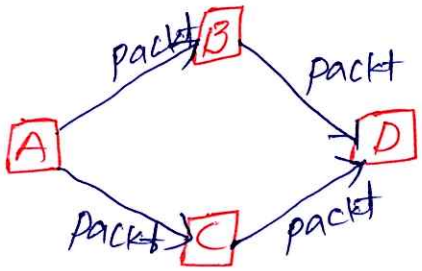
1. **Point-to-point Transmission:-** In this point-to-point transmission the source router will transmit the data packet to all the destination nodes separately. To do this the source router has to store all the destination addresses. Therefore the bandwidth of the router increases.

Ex:-



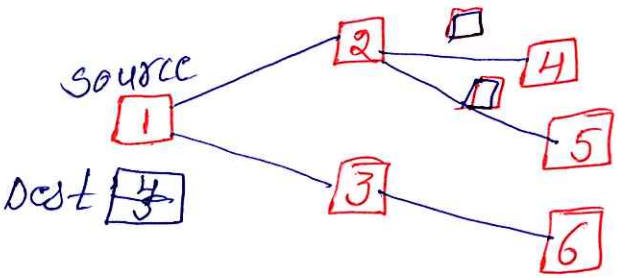
2. Flooding:- In Flooding when a data packet arrives at a router, it is sent to all the outgoing links except the one it has arrived first.

Ex:-



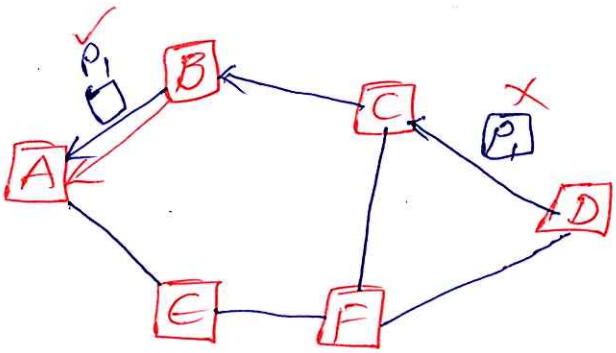
3. Multi Destination Routing:- In Multi Destination Routing the router will send the packets to multiple destinations by storing the address of multiple destination routers.

Ex:-



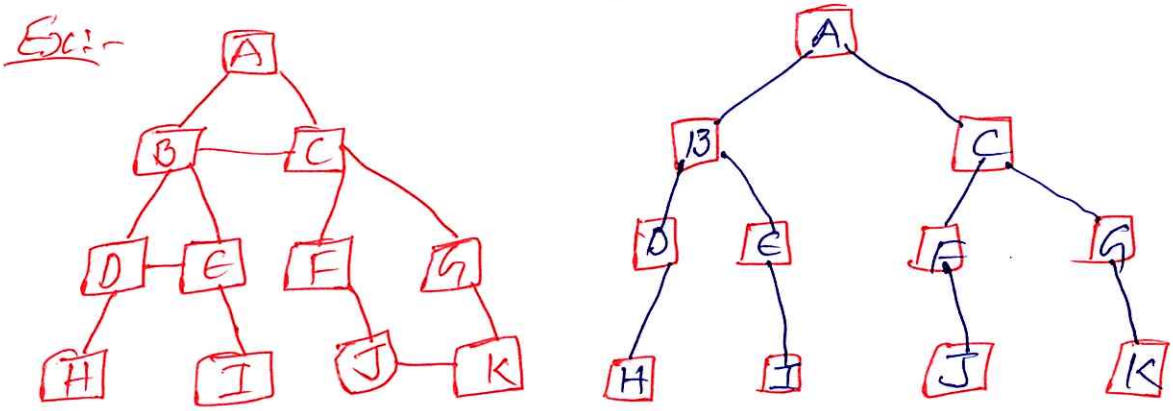
4. Reverse path forwarding:- In Reverse path Forwarding the concept of Flooding is also used. In Reverse path forwarding the routers will accept the packets from the shortest paths. If it receive packets from largest path the router will simply retransmits the packt to the source.

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:-

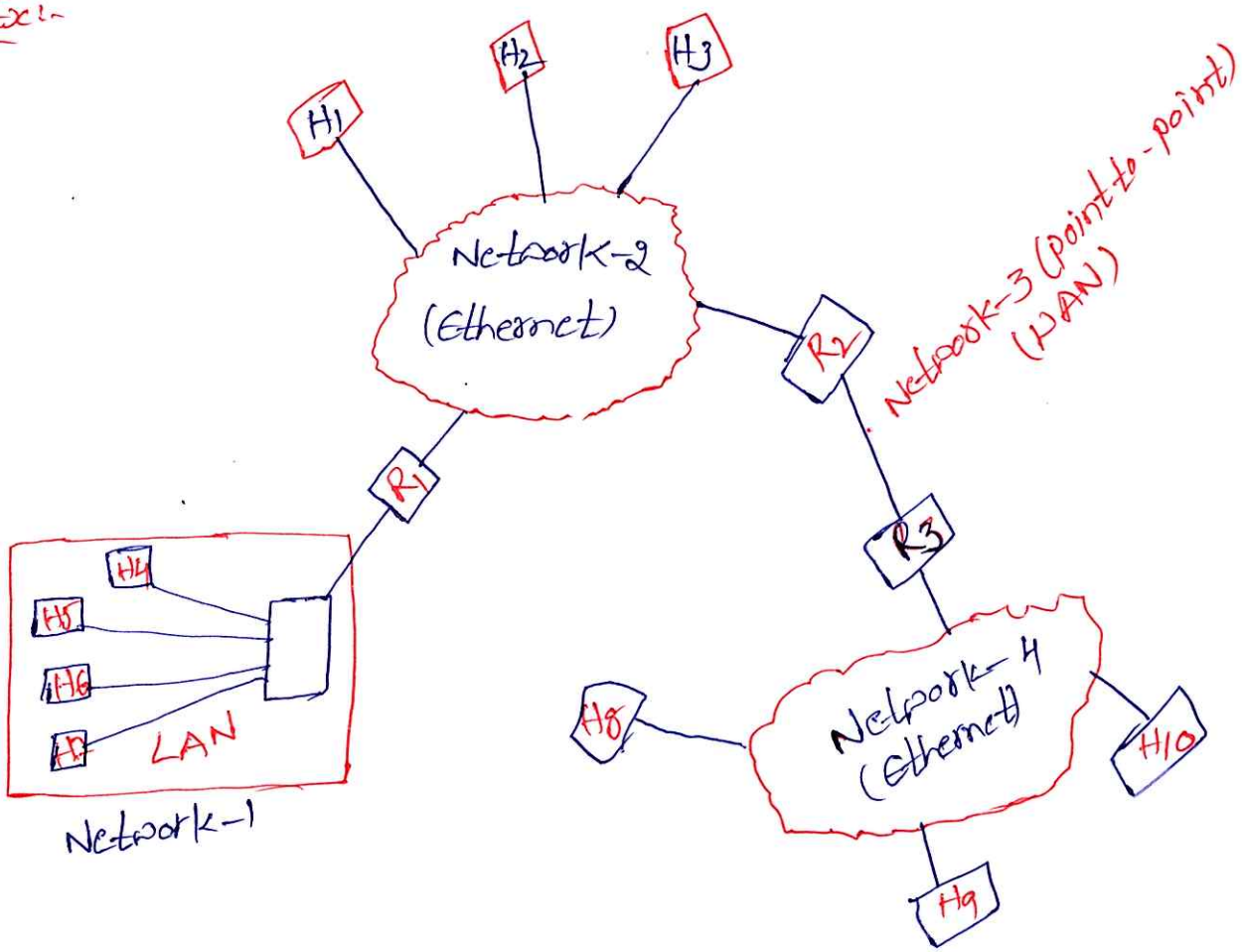


Internetworking:-

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.

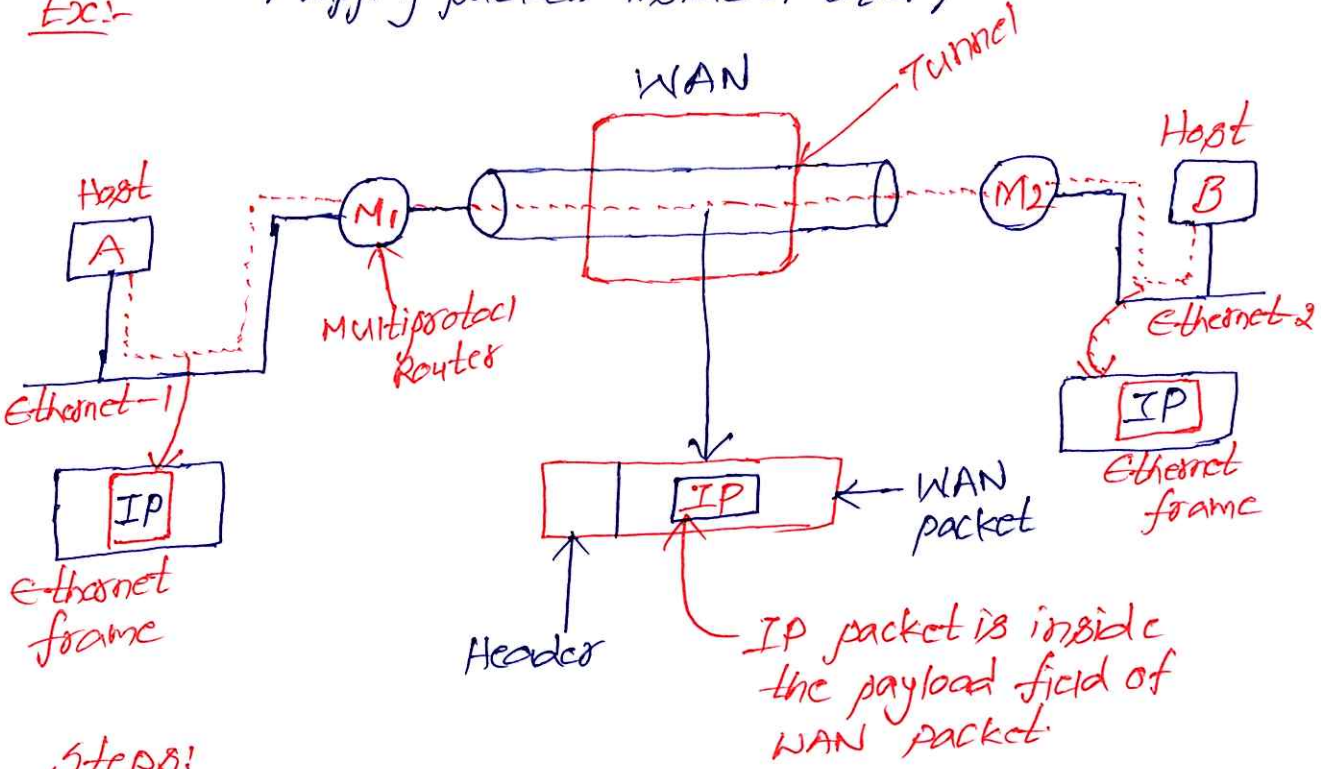
* components or Principles of Internetworking:-

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

Tunneling:-

A technique of inter-networking called Tunneling is used when source and destination networks of the same type are to be connected through a network of different types. Tunneling uses a layered protocol model such as OSI or TCP/IP protocol. Tunneling works by encapsulating packets i.e wrapping packets inside of other packets.

Ex:-



Steps:

* Host-A constructs a packet that contains the IP address of Host-B.
* Host-A then inserts this IP packet into an Ethernet frame.
* Now this frame is addressed to the Multiprotocol router M1.

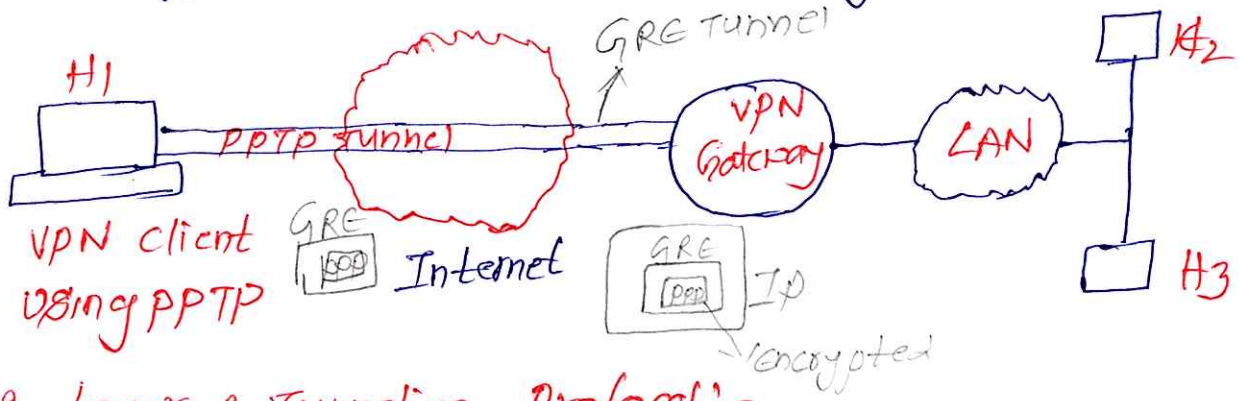
* When M1 receives this frame, it removes the IP packet and inserts it in the payload packet of the LAN network layer packet.
* Now the LAN payload packet is addressed to Multiprotocol Router M2.
* The Multiprotocol router M2. removes the IP packet and sends it to Host-B in an Ethernet frame.

Some tunneling protocols are:

1. Point-to-Point Tunneling Protocol:-

* The PPTP is an obsolete method for implementing VPNs (virtual private Networks).
* The PPTP creates an encrypted tunnel btn. two points.
* once authenticated, a Generic Routing Encapsulation (GRE) tunnel is established btn the client and server.
* PPP (Point-to-point protocol) frames are encapsulated within GRE packets which are then encapsulated within IP packets for transmission over the internet.
* Microsoft point-to-point encryption (MPPE) is applied to encrypt the data with in the PPP frames.

* The encrypted and encapsulated data is transmitted over the internet through the established (GRE) tunnel.
* When reaches the destination GRE tunnel is terminated and the data is decapsulated and decrypted to retrieve the original information.



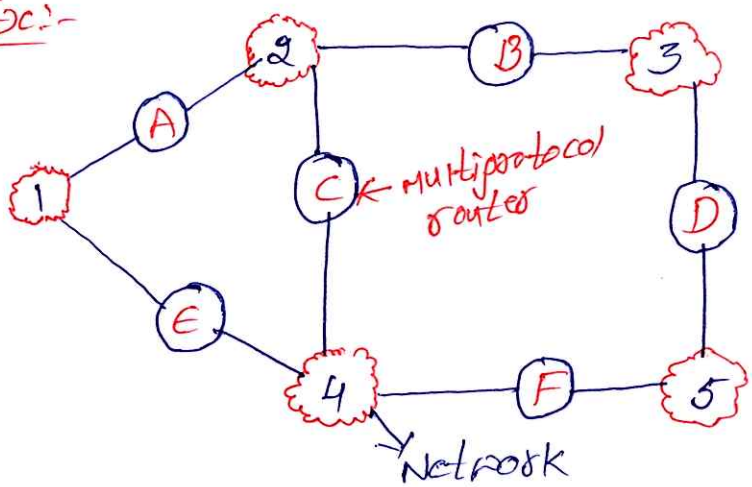
2. Layer-2 Tunneling Protocol :-

* L2TP is a Tunneling protocol that was designed to support VPN connections used by an Internet Service provider (ISP) to enable VPN operations over the Internet
* It operates at the data link layer of the OSI model.
* It encapsulates PPP frames to transmit over Internet protocol (IP).
* L2TP combines the best features of two other Tunneling protocols – PPTP and L2F (Layer-2 Forwarding)

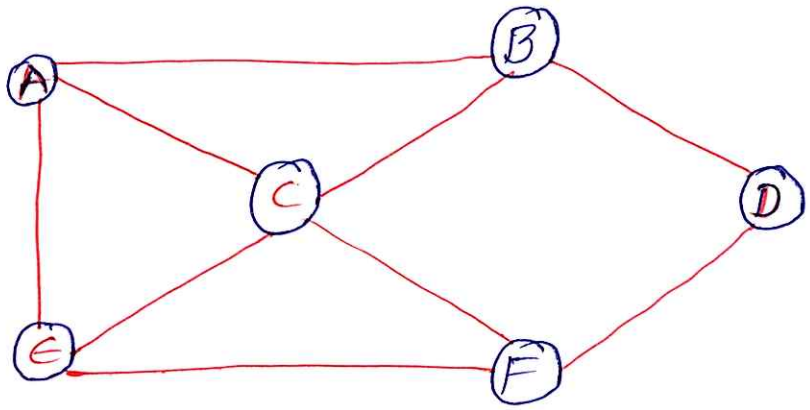
Internetwork Routing :-

Internetwork Routing is the process of selecting paths in a network along which to send data packets from a source to a destination across multiple interconnected networks.

Ex:-



a. An internetwork.



b. A graph of the internetwork.

* Once the graph has been constructed, Distance vector Algo. or Link State Routing Algo. can be applied to set of multiprotocol routers.
* This gives a two level routing Algo.
  1. Within each network an interior gateway protocol is used.
  2. But between networks an exterior gateway protocol is used.
* Routers use routing tables to store information about different networks and the best path to reach them.
* These tables are typically updated using routing protocols, which allow routers to exchange information about network connectivity and topology.
* When a router receives a packet, it looks up the destination IP address in its routing table and selects the next-hop router on the path to the destination.
* This process is repeated at each router along the path until the packet reaches its final destination.

Packet Fragmentation:-

Fragmentation is the process of breaking down large packets into smaller fragments. These fragments are transmitted accross networks with size limitations. This is necessary when a packet exceeds the Maximum Transmission Unit (MTU) of a network segment.

Fragmentation occurs at the Network Layer of OSI model. Fragmentation allows data to be transmitted accross networks where the MTU is smaller than the original packet size.

Fragmentation

Identification 16-Bits	Flag 3-Bits	Fragmentation Offset 13-bits

* Identification field is used to identify the corresponding fragment belongs to which packet.

* In Flag we have 3-bits

  Bit-0 -> It is reserved and always set to '0'

  Bit-1 -> DF (Dont Fragment)

    * If DF is set to '0' the packet should be fragmented.

* If DF is set to '1' the packet should not be fragmented.

Bit-2 → MF (More Fragments)

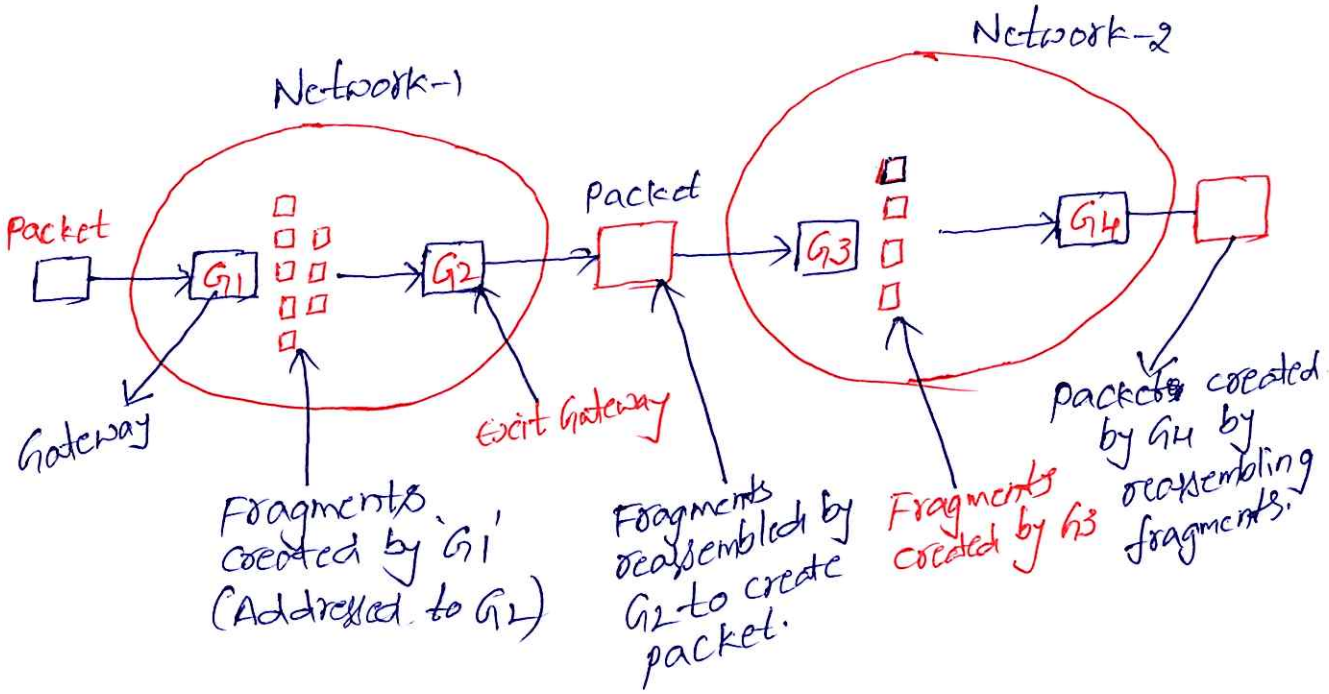
* If MF is set to '0' that means there is no more fragments.
* If MF is set to '1' there are more fragments appear.

* Fragment offset specifies the position of the fragment.

There are two different types of fragmentation. They are

1. Transparent Fragmentation.
2. Non-Transparent Fragmentation.

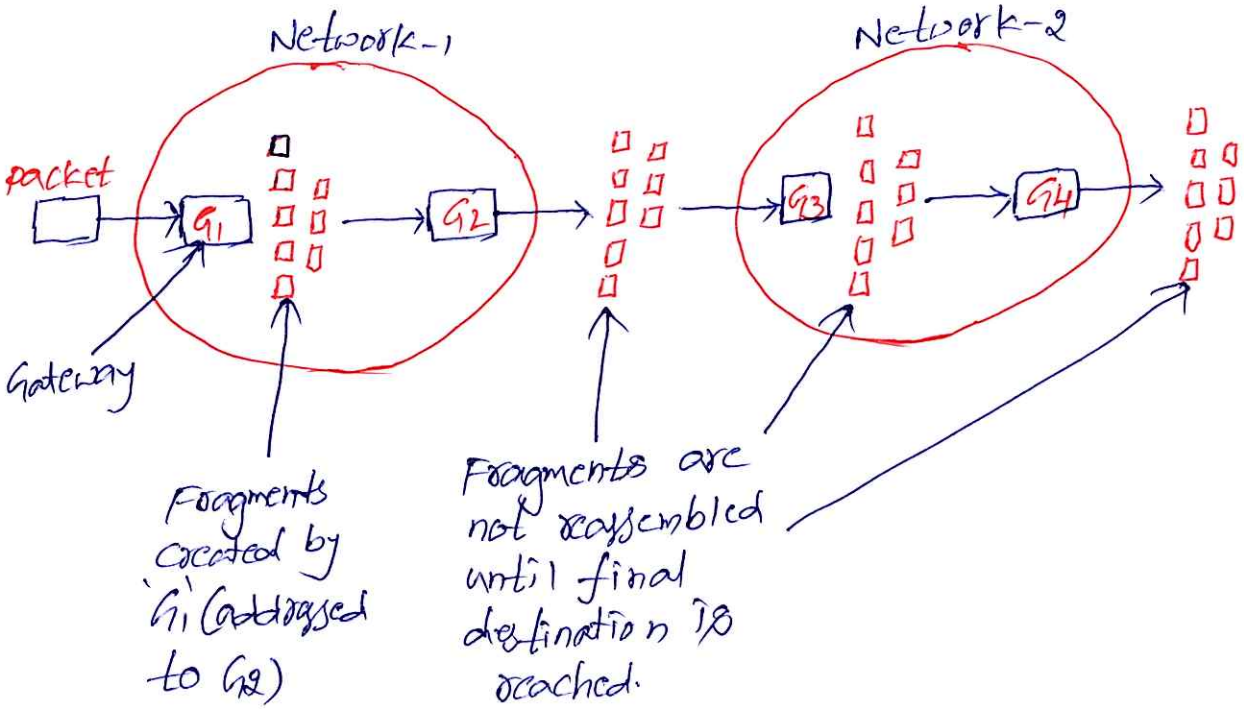
1. Transparent Fragmentation:-



This fragmentation is done by one network is made transparent to all other subsequent networks which packet will pass.

As shown in the above figure when a large packet arrives at a gateway it breaks the packet into small fragments. After this each fragment is addressed to some exit gateway. The exit gateway 'G2' reassembles the fragments ~~into~~ created by 'G1' before passing them to Network-2. Thus subsequent network is not aware that fragmentation has occurred.

2. Non-Transparent Fragmentation:-



This fragmentation is done by one network is non-transparent to the subsequent networks through which a packet passes.

As shown in the above figure the packet fragmented by a gateway 'G1' of a network-1 is not recombined by exit gateway 'G2' of same network-1.

once a packet is fragmented, each fragment is treated as a original packet. All fragments of a packet are passed through exit gateway and recombination of these fragments is done at the destination host.

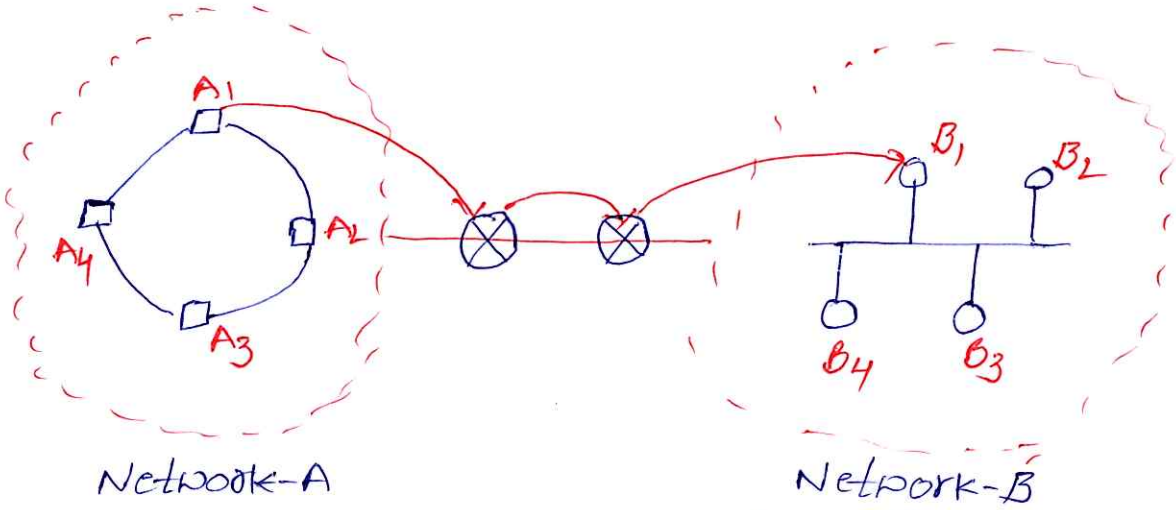
Computer Networks
UNIT - IV

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.

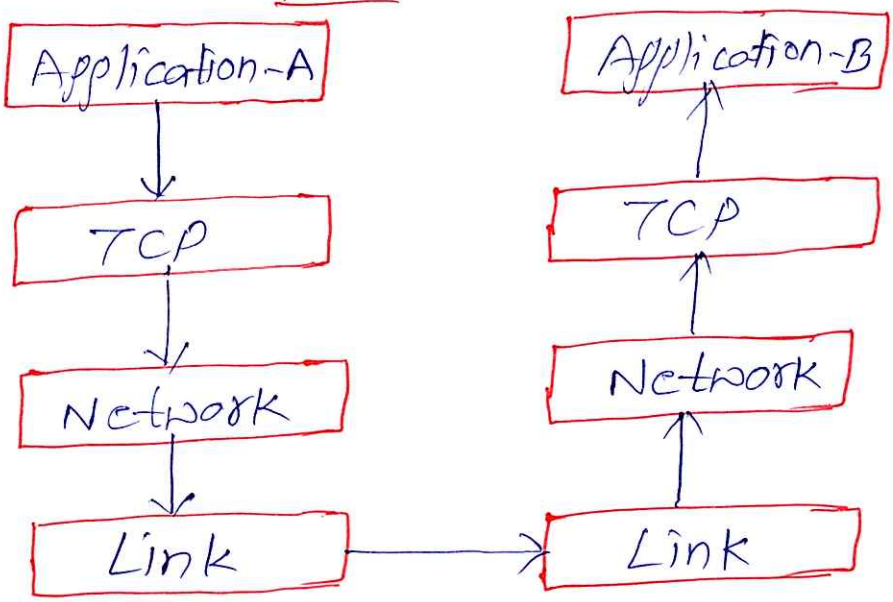
* **End-to-end connection:-** The Transport Layer is also responsible for creating the end-to-end or port-to-port connection btn. hosts. It uses two protocols mainly TCP and UDP. TCP is a secure connection-~~proto~~ oriented protocol that uses a handshake protocol to establish a robust connection btn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



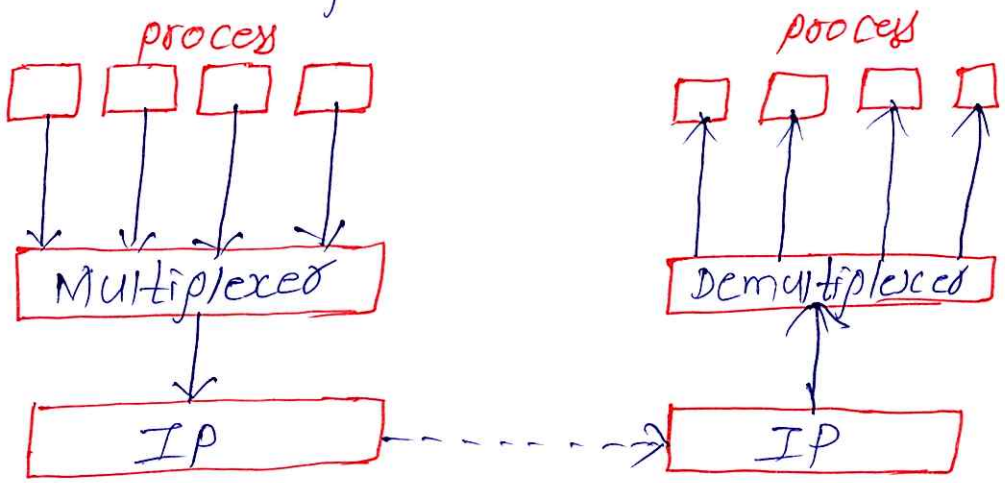
End-to-end/port-to-port comm.

* 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.

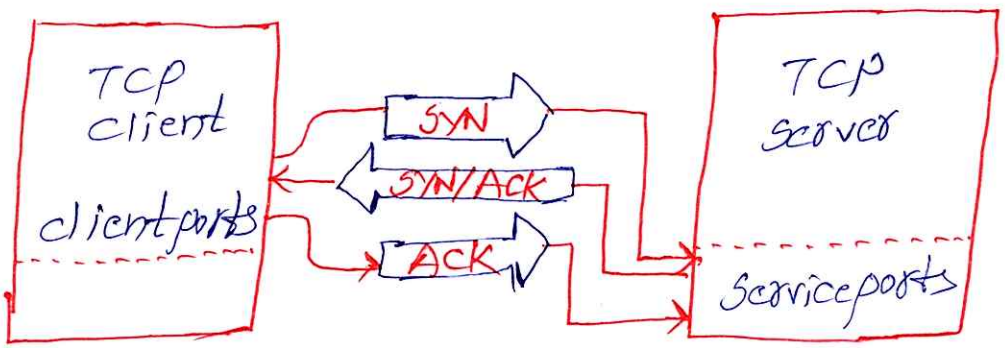
Flow control



* **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.

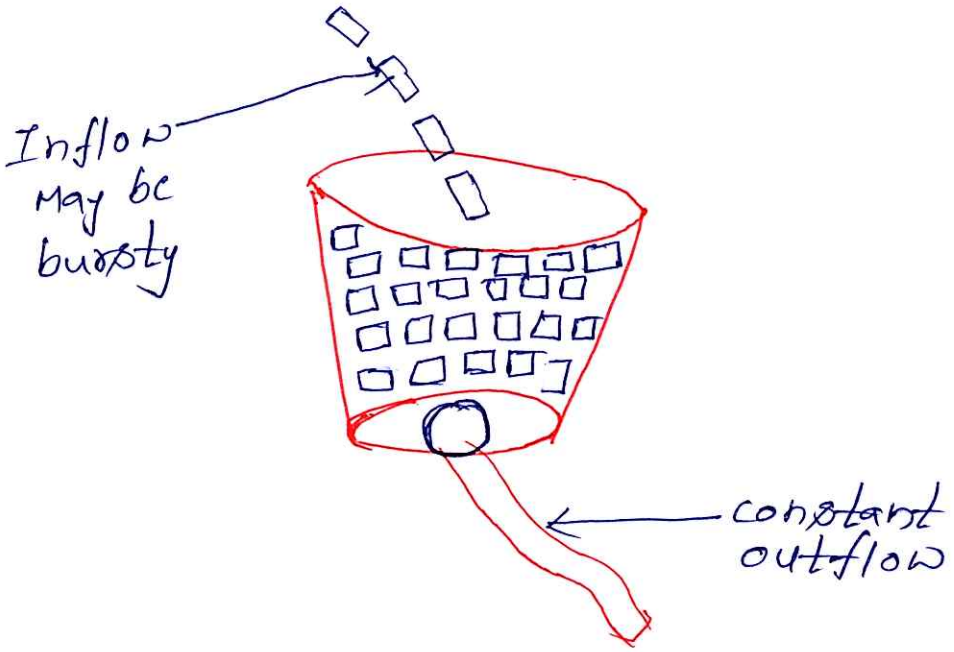
* In the Graceful connection release, the connection is open until both parties have closed their sides of the connection.

* 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.

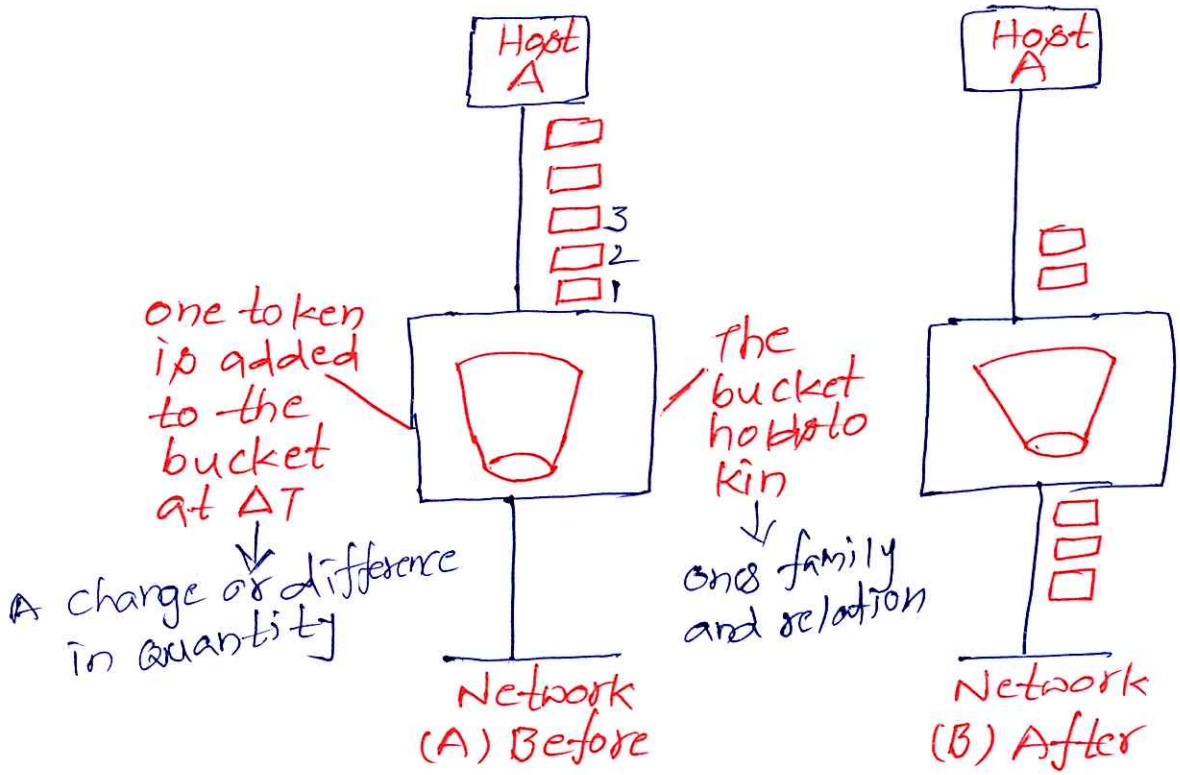
* Congestion control:- Congestion in a computer network happens when there is toomuch data being sent at the same time, causing the network to slow down. Congestion control technique helps to manage the traffic, so all users can enjoy a stable and efficient network connection. There are two methods for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

* Token Bucket Algo:-



In the above figure-A we see a bucket holding three tokens, with five packets waiting to be transmitted. For a packet to be transmitted, it must capture and destroy one token. In figure-B we see that three of the five packets have gotten/processed/transmitted through, but the other two are stuck and waiting for more tokens to be generated.

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.

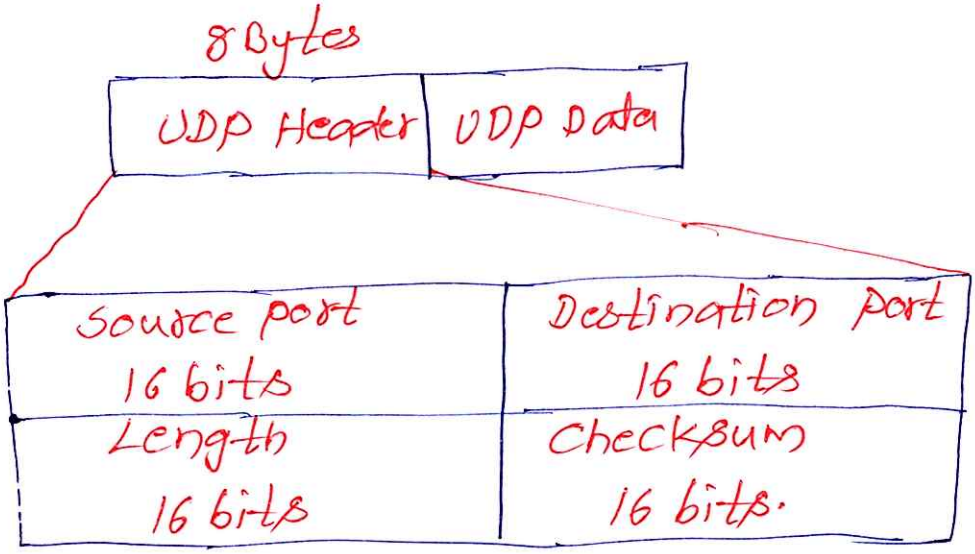
* Unreliable:- while the network does its best to deliver packets, there is no guarantee that they will all arive in the correct order or not.

* 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.

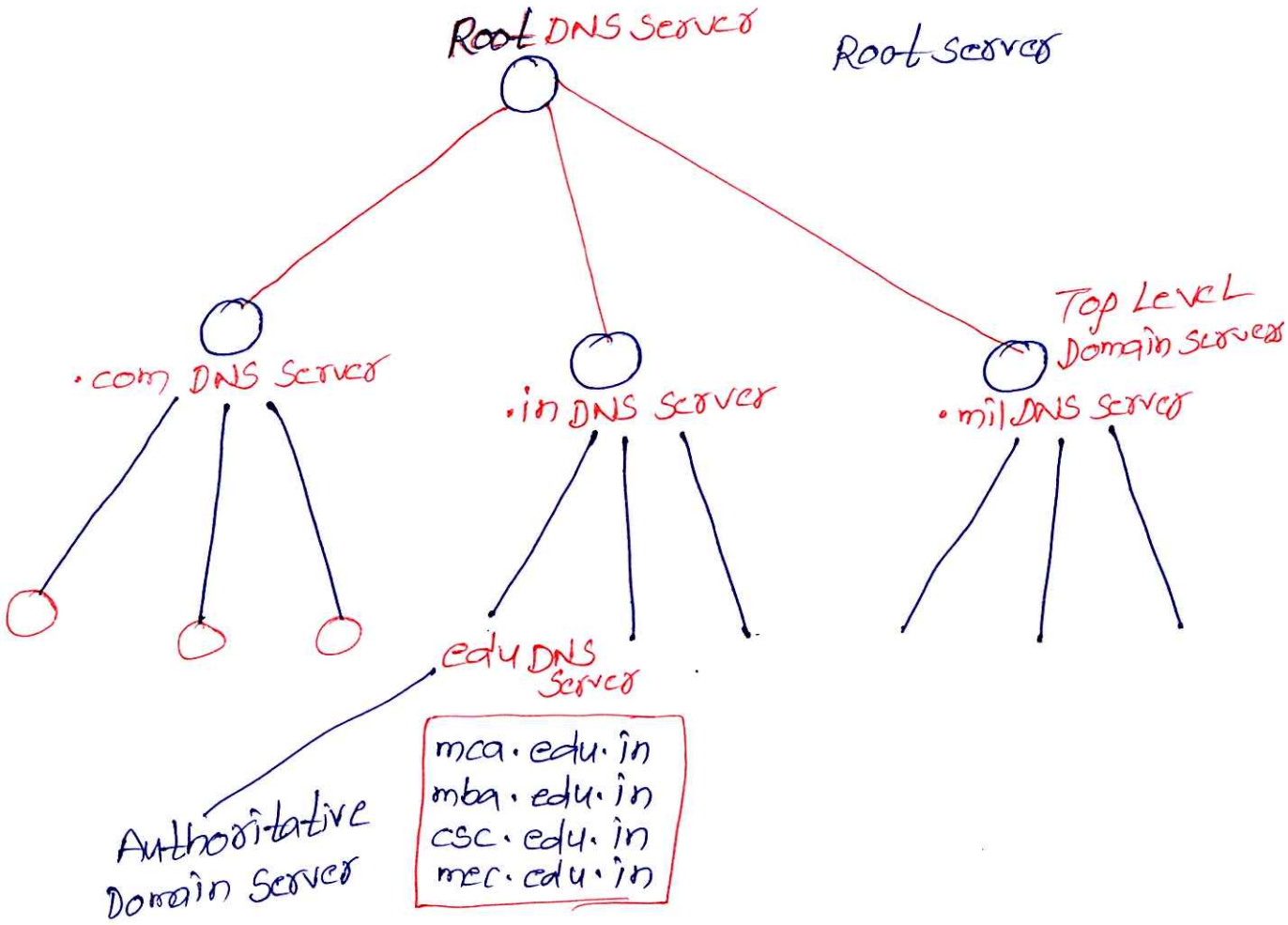
The Domain Name System:-

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.

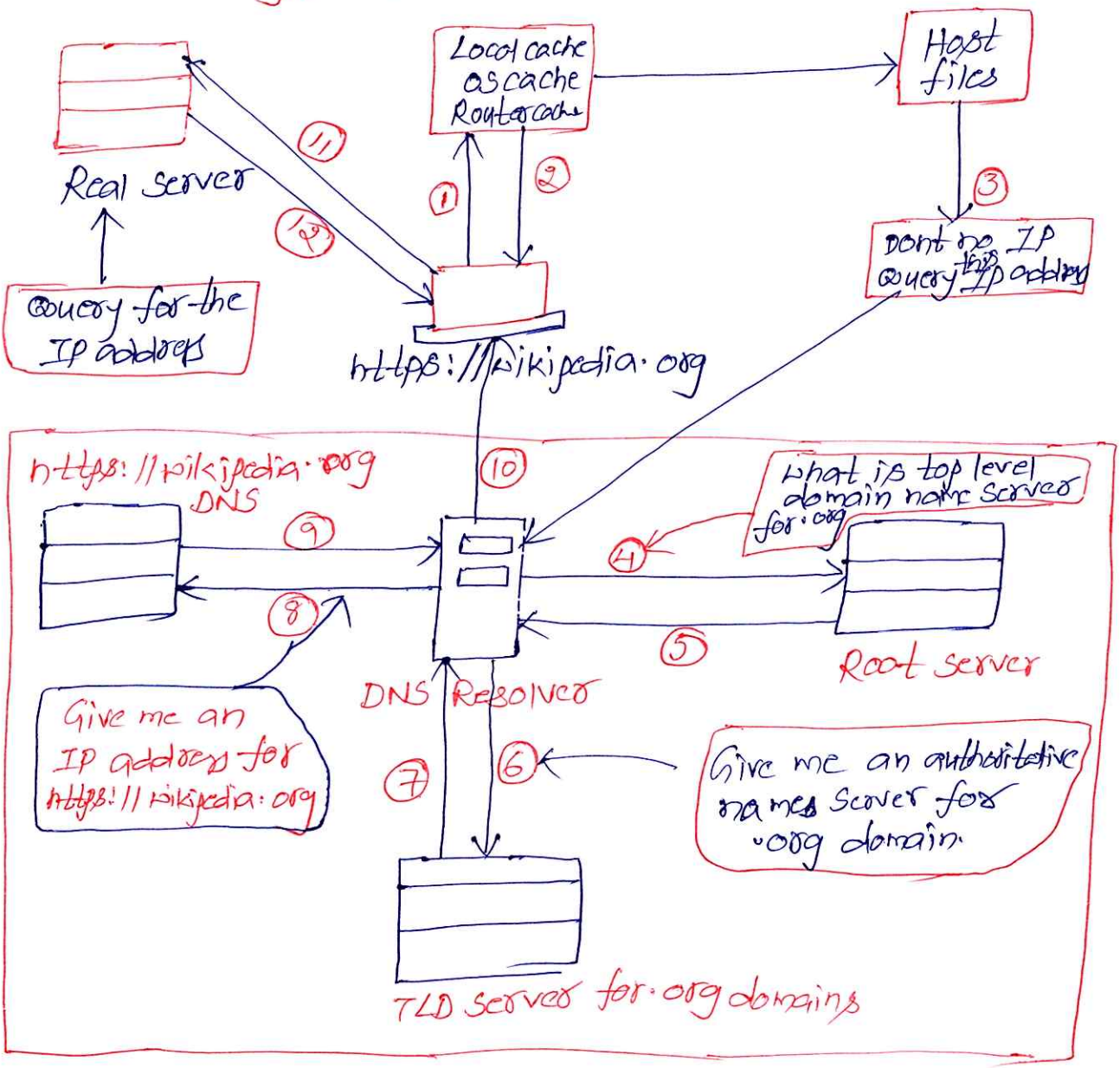
* Authoritative DNS Servers:- These are the servers that store the actual DNS records for domain names. These servers are responsible for providing the correct IP address to allow users to reach websites.

* 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.

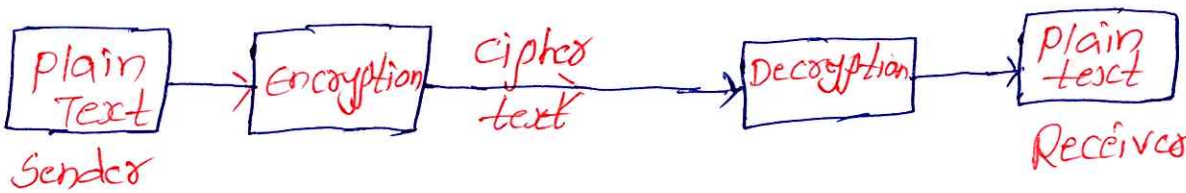
* How to send an email :-

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.

Cryptography :-

Cryptography is a techniaue of securing information and communications using codes to ensure confidentiality, integrity and authentication. The prefix "crypt" means "Hidden" and suffix "graphy" means writting. That means "Hidden writing".

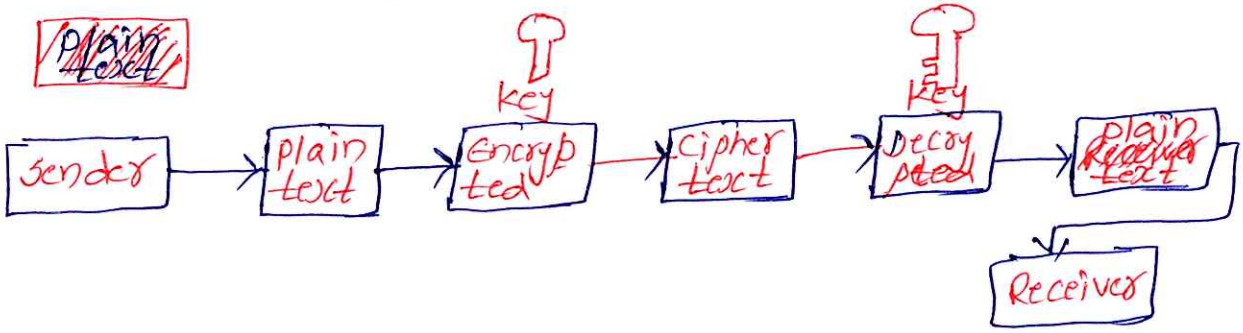
In cryptography the techniaues that are obtained from mathematical concepts and a set of rule-based calculations known as algorithms to convert messages in the way that make it hard to decode them.



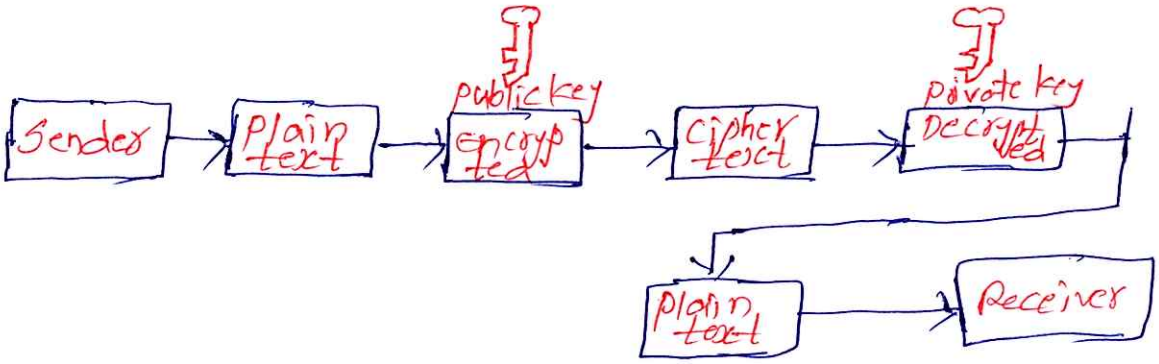
* Types of cryptography :- There are three types of cryptography. They are:

1. Symmetric key cryptography
2. Asymmetric key "
3. Hash Functions.

1. Symmetric key cryptography:- Symmetric key cryptography is an encryption system where the sender and receiver of a message use a single common key to encrypt and decrypt messages. Symmetric key cryptography is faster and simple, but the problem is that the sender and receiver has to exchange the key securely. the most popula SKC systems are DES (Data Encryption System), and AES (Advanced ES).



2. Asymmetric key cryptography:- In Asymmetric key cryptography a pair of keys is used to encrypt and decrypt information. A senders public key is used for encryption and a receivers private key is used for decryption. public keys and private keys are different. Even if the public key is known by everyone the intended receiver can only decode it because he holds his private key. The most popular AKC algorithm is RSA Algo.



3. Hash Functions:- There is no key required in Hash function cryptography, as it uses mathematical equations to generate a hash message for any length of message and the output will be of fixed length. Some of the famous Hash functions are:

* SHA-256 → Secure Hash Algorithm
* MD5 → Message Digest
* MD6

➡ Symmetric Key Cryptography Algorithms:-

The most popular Symmetric key cryptography Algos. are:

* DES → Data Encryption ~~System Standard~~
* AES → Advanced Encryption Standard

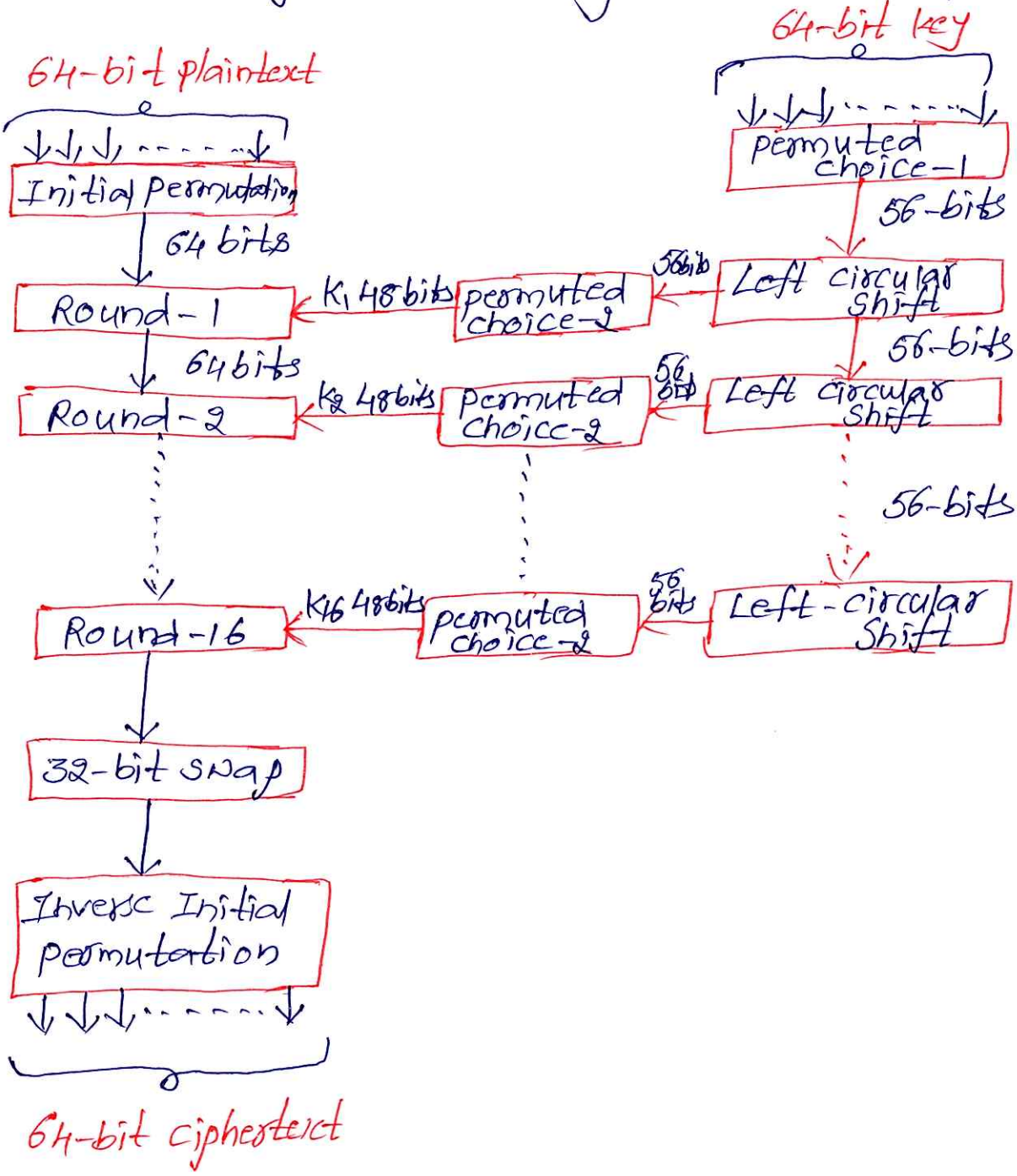
* DES:- Data Encryption Standard is an older encryption algo. that is used to convert 64-bit plaintext into 48-bit encrypted cipher-text. It uses Symmetric keys for encry. & decry.

It is old by today's standard but can be used as a basic building block for learning newer encryption algos.

DES is a "symmetric" block cipher. By "symmetric" we mean that the size of input text and output text is same. Here "block" means that it takes group of bits (64 bits) together as input instead of encrypting the text bit by bit. Some basic points of DES.

* It is a block cipher that encrypts data in 64-bit blocks.
* It takes a 64-bit plain-text as input and generates a corresponding 64-bit ciphertext as output.
* The main key length is 64-bit which is transformed into 56 bits by skipping every 8th bit in the key.
* It encrypts the text in 16-rounds, where each round uses 48-bit subkey.
* This 48-bit subkey is generated from the 56-bit effictive key.
* The same algo. & keys are used for both encry. & decry. with minor changes.

* Working of DES:- DES consists of 16 steps each of which is called a round. Each round performs the steps of substitution and transposition along with other operations.



* In the first step the 64-bit plaintext is handedover to the Initial permutation.
* The initial permutation is performed on the plaintext.
* Now the initial permutation produces two halfs i.e Left plain Text and Right plain Text.
* Now each LPT and RPT go through 16 rounds of the encryption process.
* After 16-rounds the two halfs are swapped.
* In the end the Inverse Initial permutation is performed on LPT & RPT.
* The result of this process produces 64-bit ciphertext.

* Initial Permutation:- The 64-bits plain-text blocks is input into an Initial permutation function that rearranges the orders of bits. The order of bits is changed using predefined table. The IP table is a 8x8 matrix (64-entries) where each entry specifies the new position of a bit from the original plaintext.

Ex:-

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

→

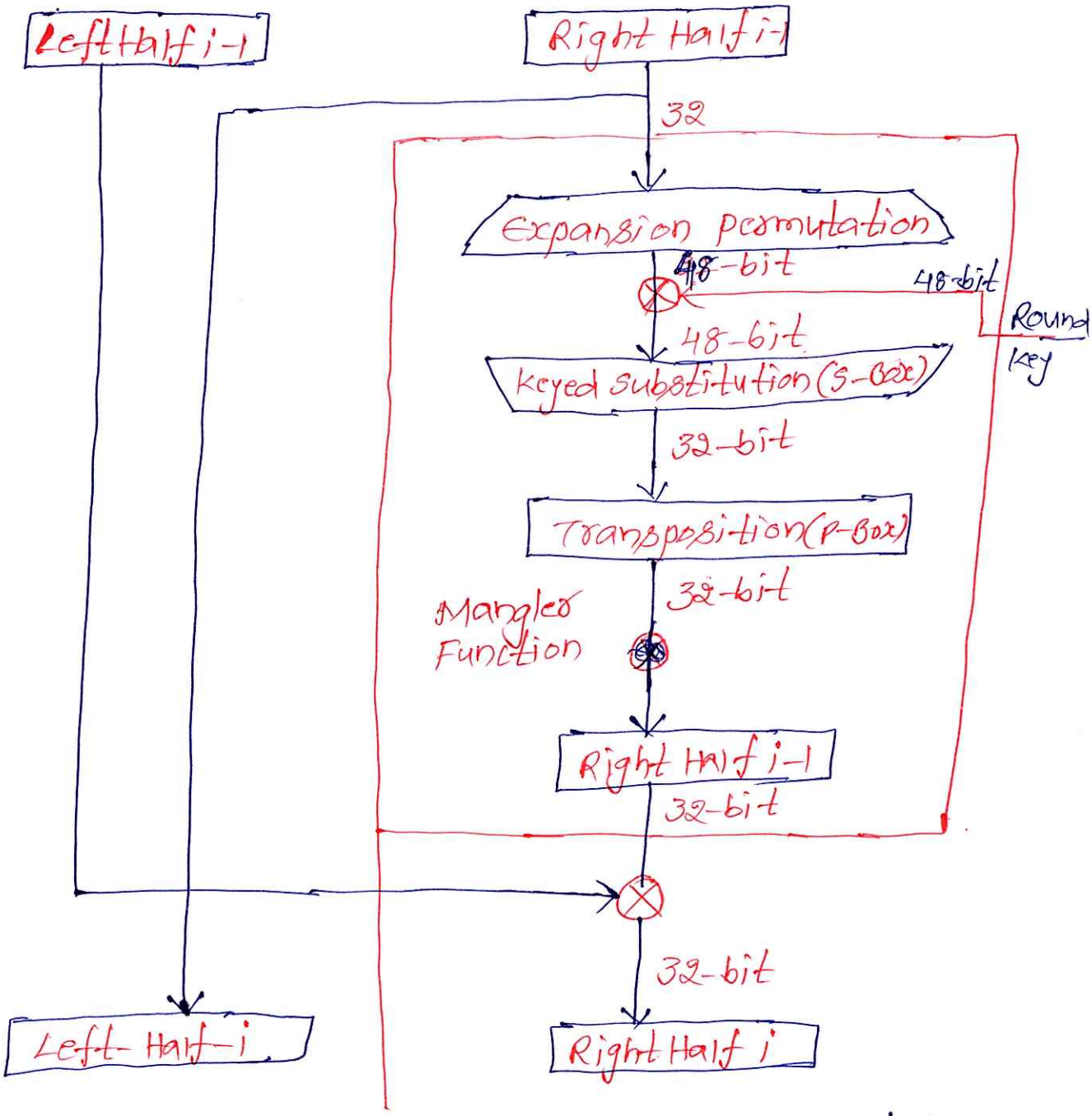
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

* Inverse Initial permutation:- After 16-rounds we get two blocks (Left & Right) of 32-bit each. The two 32-bit halves are again swapped back, resulting in a 64-bit block. This step is called 32-bit swap in DES encryp. Algo. Finally the block undergoes an Inverse Initial permutation. This is essentialy the Inverse permutation applied at the begining.

Ex:-

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

* Single Round of DES:- / single Feistel Round in DES:-



* Every round receives 64-bits permuted plaintext from the Initial permutation function and 48-bit transformed subkey (k_i).
* The permuted 64-bit plaintext is divided into two halves called as LPT & RPT. Both of these halves are 32-bit in size.

* The right half is processed using Mangler f^n. Mangler f^n involves expansion, key mixing, substitution (S-boxes), and permutation (P-box) of RPT.
* The RPT first go through expansion permutation. In this permutation 32-bit RPT is expanded into 48-bits using expansion box or E-box Table.

Ex:-

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

* This expanded block is XORed with the 48-bit round sub-key.
* After XOR is performed, the resulting 48-bit block is split into 8 chunks of 6-bit size each.
* The 6-bits chunks will be converted into 4-bits using S-boxes.
* This process is called substitution.

* Now we combine 4-bit chunks to get 32-bit block as output.
* This 32-bit again get permuted using P-Box permutation.
* The mangler function finishes here.
* The 32-bit Right halfe is XORed with the 32-bit Left plain Text.
* The output of this XOR operation serves as Right plain Text for next round.
* The initial Right plain Text will serve as Left half for the next round.
* The same operations are performed for 16-rounds.

32-bit Swap:-

* After these 16-rounds we get two blocks LPT & RPT of 32-bit each.
* The two 32-bit halves are again swapped back, resulting in a 64-bit block.
* This step is called 32-bit Swap in DES encryption Algo.

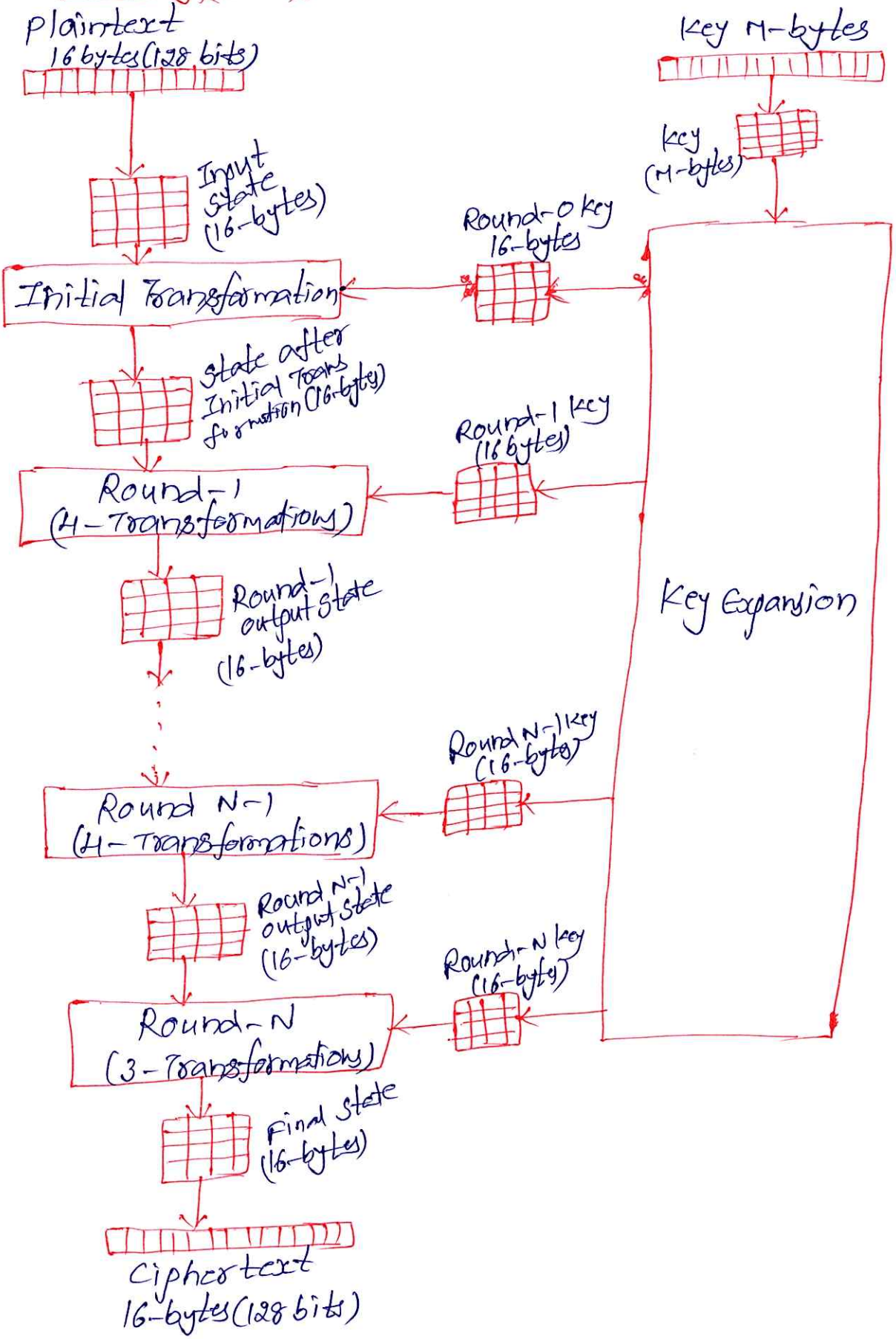
Advanced Encryption Standard: (AES):-

* Advanced encryption standard (AES) is a highly trusted encryption Algo.
* It is used to secure data by converting it into an unreadable format without the proper key.
* It is widely used today as it is much stronger than DES.
* AES encryption uses various length keys (128, 192 or 256 bits) to provide strong protection against unauthorised access.
* This data security is widely implemented in securing sensitive data and encrypting files over internet.

Some of the points to remember in AES is:

* AES is a Block cipher.
* It takes 128 bits as input and outputs 128 bits of encrypted cipher text.
* The key size can be of different sizes of bits such as 128, 192 and 256 bits.

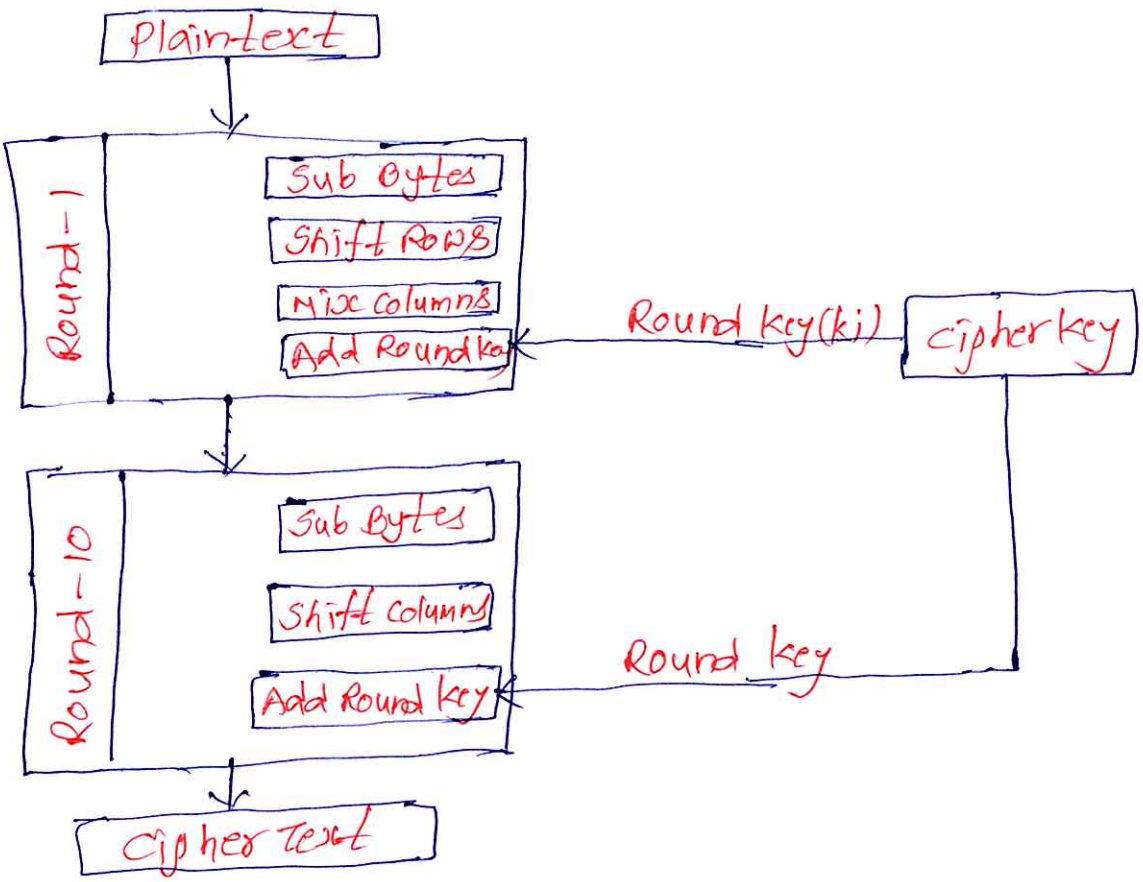
Working of AES:-



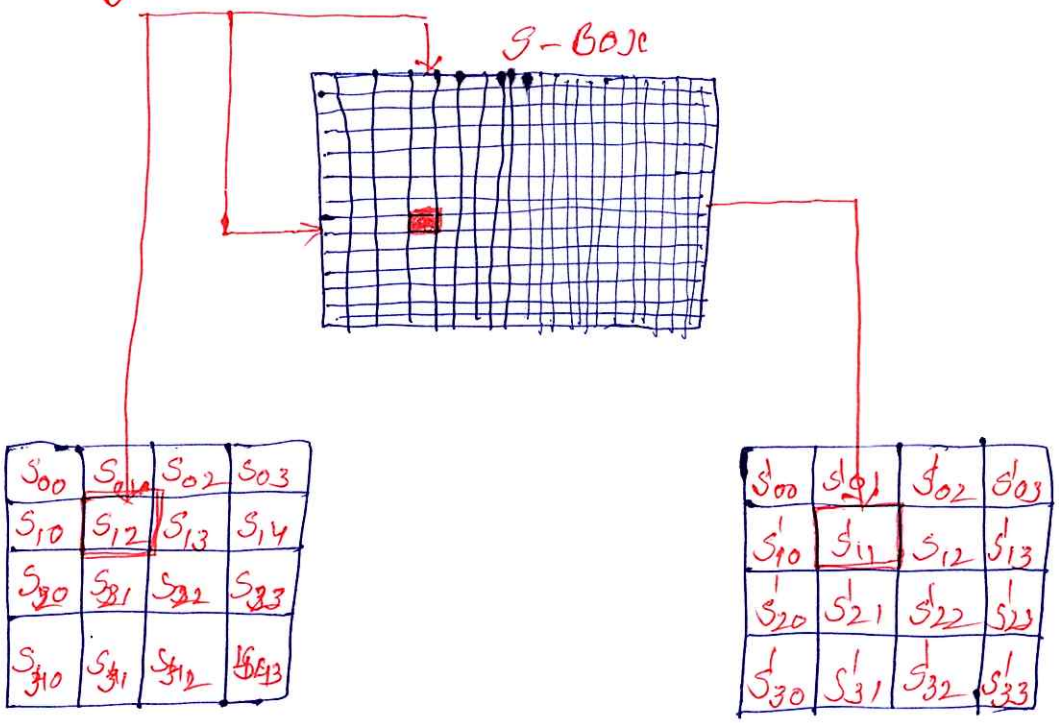
* AES performs operations on bytes of data rather than in bits.
* Since the block size is 128 bits, the cipher processes 128 bits or 16-bytes of input data at a time.
* The no. of rounds depends on the key length as follows.

No. of Rounds	Key size in bits
10	128
12	192
14	256

* AES Encryption & Decryption:-

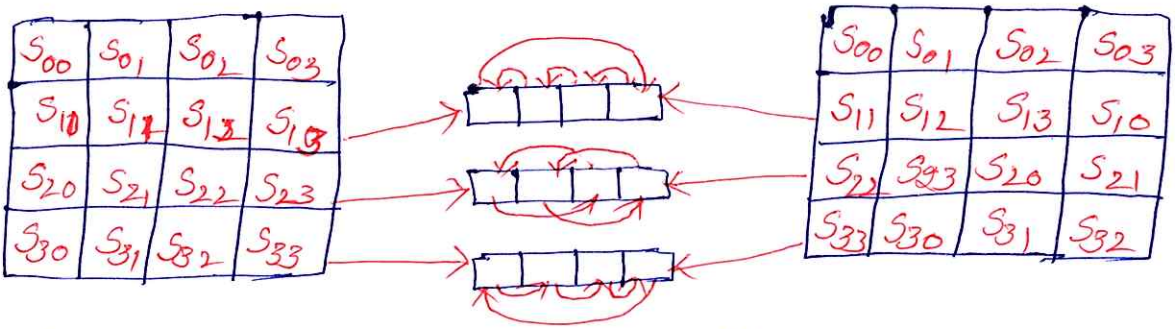


* Sub-Bytes:-



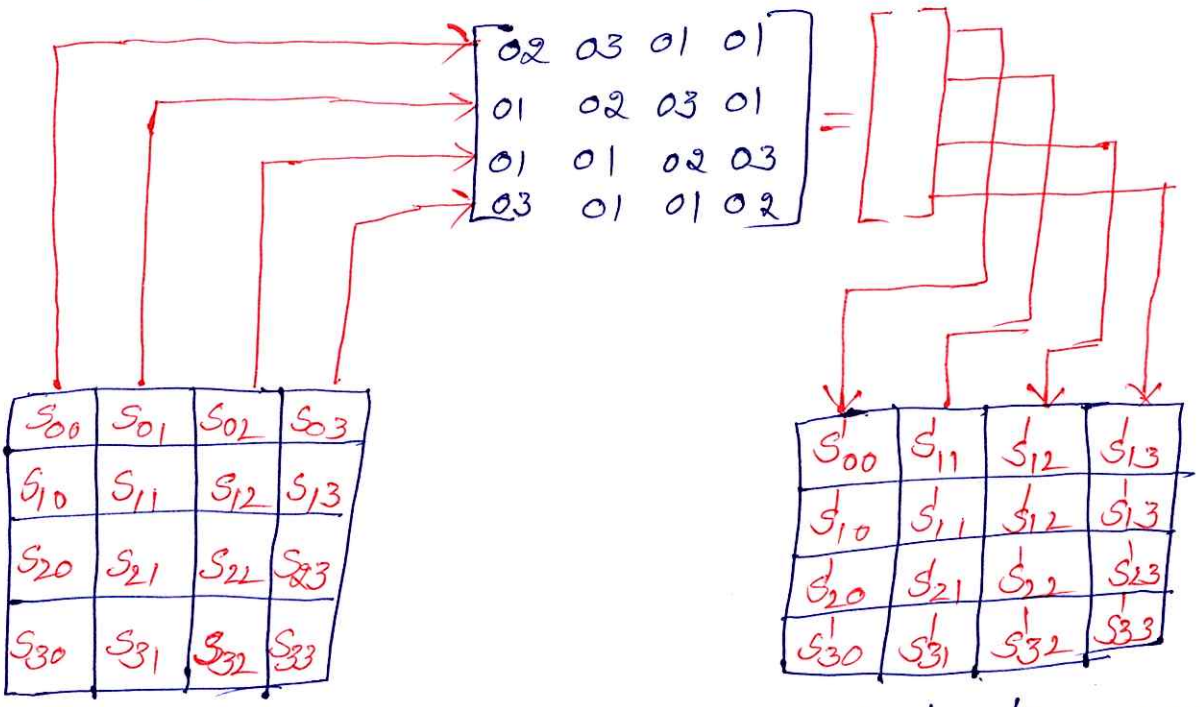
In this step each byte is substituted by another byte. It is performed using a lookup table also called the S-Box.

* Shift Rows:-



* The first row is not shifted
* The second row is shifted once to the left.
* The third row is shifted twice to the left.
* The fourth row is shifted once to the right.

* MixColumns:-



This step is a mix multiplication. Each column is multiplied with a specific matrix and thus the position of each byte in the column is changed as a result.

* this step is skipped in the last round.

* Add Round keys:-

* Now the resultant output of the previous stage is xORed with the corresponding round key.
* Here the 16-bytes are not considered as a grid but just as 128 bits of data.
* Now this encrypted data is given to the 2nd round.
* After completion of all rounds we get the encrypted data called ciphertext.

RSA (Rivest, Shamir, Adleman) Algo:-

* RSA is an ~~Asymmetric~~ or public key ~~encryption~~ cryptography Algo.
* It works on two different keys i.e public key and Private key.
* The public key is used for encryption and is known to every-one.
* The private key is used for decryption and must be kept secret by the receiver.
* If a person 'A' wants to send a message securely to person-'B'. person 'A' encrypts the message using person 'B' public key and person 'B' decrypts the message using their private key.

RSA Encryption & Decryption:-

* Consider two large prime numbers p and q.
* Calculate $n = p * q$
* Calculate Euler Totient Function $\phi(n) = (p-1)*(q-1)$
* Assume a public key 'e' such that $1 < e < \phi(n)$ and $\gcd(e, \phi n) = 1$ ('e' is coprime to $\phi(n)$)
* Assume a private key 'd' such that $d \equiv e^{-1} \bmod \phi(n)$ (congruent)

$\Rightarrow d * e \equiv 1 \bmod \phi(n)$

$d * e \bmod \phi(n) \equiv 1 \bmod \phi(n)$

$de \bmod \phi(n) = 1$

* Public key = $\{e, n\}$
* Private key = $\{d, n\}$
* **Encryption:-** ciphertext $M < n$

$$\Rightarrow C = M^e \bmod n$$

* **Decryption:-** $M = C^d \bmod n$

Ex:- 1

→ $p = 5$ & $q = 11$

→ $n = 5 \times 11 = 55$

→ $\phi(n) = 4 \times 10 = 40$

→ $1 < e < \phi(n)$

→ $1 < 3 < 40$ & $\gcd(3, 40) = 1$

→ public key = $\{e, n\} = \{3, 55\}$

→ private key = $\{d, n\} = \{1, 55\}$

3)40(13
30
10
9
1

9)55(6
54
1

$d \cdot e \bmod \phi(n) = 1$

$d \cdot 3 \bmod 40 = 1$

$1 \cdot 3 \bmod 40 = 1$

$\therefore d = 1$ //

Euclid's Algo

$GCD(m, n) = GCD(n, m \bmod n)$ $\quad m > n$

$GCD(40, 3) = GCD(3, 40 \bmod 3)$

$= GCD(3, 1)$

$= (1, 0) = 1$

$\Rightarrow C = M^e \bmod n$

$= M^3 \bmod 55$

$= 3^3 \bmod 55$

$= 9 \bmod 55$

$= 1$ //

$\Rightarrow M = C^d \bmod n$

$M = 1^1 \bmod 55$

$M = 1$ //

Exc:-2 → p=3 & q=11

→ n=3×11=33

→ $\phi(n)=2\times10=20$

→ $1<e<20 \Rightarrow 1<13<20$

→ gcd(13, 20)=1

13)20(1
13
7

13)120(81
104
16
13
(3)

→ p=13, q=11

→ n=13*11=143

→ $\phi(n)=12\times10=120$

→ $1<e<120 \Rightarrow 1<13<120$

→ gcd(13, 120)=1

4^{17} = 17, 179, 869, 184

3^{17} = 129, 140, 168 ≈ 140

(13, 3)

(4, 3)

→ the public key = {e, n} = {13, 33}

→ private key = {d, n} = {17, 33}

$d \cdot e \bmod \phi(n)=1$ or $d(\phi(n)*i+1)/e$

$d \cdot 13 \bmod 20=1$

$17 \cdot 13 \bmod 20=1$

$221 \bmod 20=1$

Encryption:- M<n

$C = M^e \bmod n$

$= M^{13} \bmod 33$

$\equiv 4^{13} \bmod 33$

$= 67,108,864 \bmod 33$

$C = 31$

→ Decryption: $M = C^d \bmod n$

$M = 3^{17} \bmod 33$

$= 31^{17} \bmod 33$

$M = 4$

Exc:- 3. → $p = 13 \quad q = 17$

→ $n = p * q \Rightarrow n = 13 \times 17 = 221$

→ $\phi(n) = (p-1) * (q-1)$

$= (13-1) * (17-1)$

$= (12) * 16)$

$\phi(n) = 192$

→ $1 < e < \phi(n) \Rightarrow 1 < 17 < 192$

→ $\gcd(17, 192) = 1$

$\Rightarrow GCD(17, 192 \bmod 17)$

$\Rightarrow GCD(17, 5)$

$\Rightarrow GCD(5, 17 \bmod 5)$

$\Rightarrow GCD(5, 2)$

$\Rightarrow GCD(2, 5 \bmod 2)$

$\Rightarrow GCD(2, 1)$

$\Rightarrow GCD(1, 2 \bmod 1)$

$\Rightarrow GCD(1, 0)$

$\Rightarrow 1$

17)192(11
17
22
17
5

5)17(3
15
2

2)5(2
4
1

* public key $= \{e, n\} = \{17, 221\}$

* private key $= \{d, n\} = \{159, 221\}$

$\Rightarrow d \cdot e \bmod \phi(n) = 1$

$\Rightarrow d \cdot 17 \bmod 192 = 1$

$\Rightarrow d = (\phi(n) * i + 1)/e$

$\Rightarrow d = (192 * 1 + 1)/17$

$\Rightarrow d = (193)/17 = 11.25$

$\Rightarrow d = (193 \times 2 + 1)/17$

$\Rightarrow d = (387)/17 = 22.76$

$\Rightarrow d = (193 * 3 + 1)/17$

$\Rightarrow d = (580)/17 = 34.11$

~~$\Rightarrow d = (580 * 4$~~

$\Rightarrow d = (193 * 4 + 1)/17$

$\Rightarrow d = (773)/17 = 45.47$

$\Rightarrow d = (193 * 5 + 1)/17$

$\Rightarrow d = (966)/17 = 56.82$

$\Rightarrow d = (193 * 6 + 1)/17$

$\Rightarrow d = (1159)/17 = 68.17$

$\Rightarrow d = (193 \times 7 + 1)/17$

$\Rightarrow d = (1352)/17 = 79.52$

$\Rightarrow d(193\times8+1)/17$

$\Rightarrow d(1545)/17 = 90.88$

$\Rightarrow d(193\times9+1)/17$

$\Rightarrow d(1738)/17 = 102.23$

$\Rightarrow d(193\times10+1)/17$

$\Rightarrow d(1931)/17 = 113.58$

$\Rightarrow d(193\times11+1)/17$

$\Rightarrow d(2124)/17 = 124.94$

$\Rightarrow d(193\times12+1)/17$

$\Rightarrow d(2317)/17 = 136.29$

$\Rightarrow d(193\times13+1)/17$

$\Rightarrow d(2510)/17 = 147.64$

$\Rightarrow d(193\times14+1)/17$

$\Rightarrow d(2703)/17 = 159$

$\therefore 159 \cdot 17 \bmod 192 = 1$

* Encryption:- $M < n$

$\Rightarrow C = M^e \bmod n$

$\Rightarrow C = 4^{17} \bmod 221$ $\quad C = 1^{17} \bmod 221$

$C = 17,179,869,184 \bmod 221$ $\quad C = 1$

$C = 140.$ $\quad C = 2^{17} \bmod 221$

$= 131072 \bmod 221$

$C = 19$

$\Rightarrow$ Decryption:-

$M = c^d \bmod n$

$M = 140^{159} \bmod 221$

$M =$

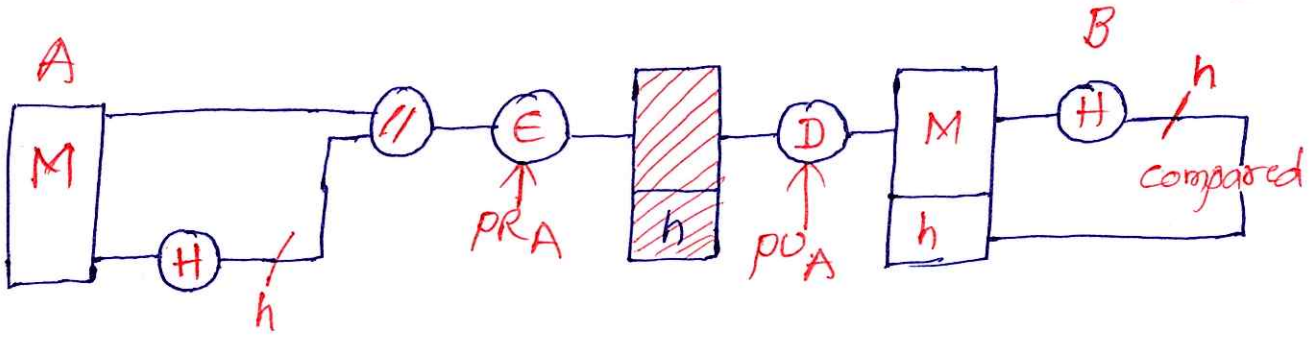
$M = 1^{159} \bmod 221$

$M = 1 \bmod 221$

$M = 1$

Digital Signature Algo:-

* A digital signature in cryptography is a mathematical scheme that provides authentication and non-repudiation, for digital messages or documents.
* If the encryption is done using "sender's" private key then it is called as Digital Signature.
* It works by using a private key to encrypt a hash of the message, and the corresponding public key is then used to verify the signature.



* consider the plaintext message 'M'.
* Apply the Hash Functions (SHA-1)256), so that we get Hash code.
* Now the message and Hash code is aperoded.
* The appended data is encrypted by using private key of 'A'.
* Then we get the encrypted data, and at the receiver side the data is first decrypted using public key of 'A'.
* After decryption we get the plaintext and hash code.
* Now we apply Hash function on the plaintext, we get a Hash code.
* Now the appended Hash code is compared with the decrypted Hash code.
* If both the Hash codes are same, the plaintext is accepted otherwise rejected.

Entity Authentication:-

* Entity Authentication is a crucial aspect of cryptography that ensures the identity of entities involved in a communication or transaction.
* Entity Authentication is defined as the process of verfying the identity of an entity, such as a user, device or system
* The importance of entity authentication is to prevent unauthorised access to sensitive information and protect against various types of attacks.

* Techniques for Entity Authentication:-

Several techniques are used for entity authentication such as

* Password-Based Authentication:-

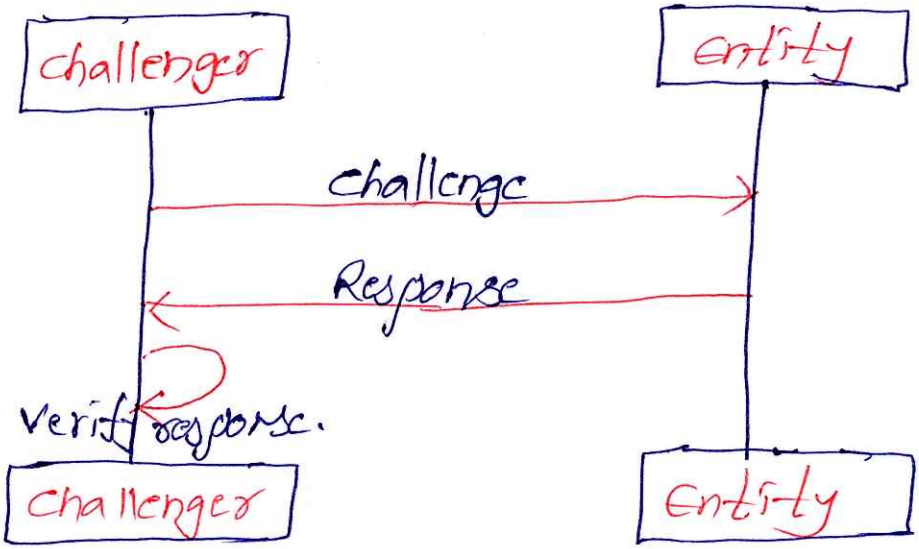
Password-based authentication involves the use of secret password to verify an entity's identity. The technique is widely used, but it has some limitations, such as password guessing attacks and password cracking.

* **Biometric Authentication:-** Biometric authentication involves the use of unique physical or behavioral characteristics such as fingerprints, facial recognition or voice recognition to verify an entity's identity. Biometric authentication provides a higher level of security compared to password-based authentication.

* **Entity Authentication Protocols:-**

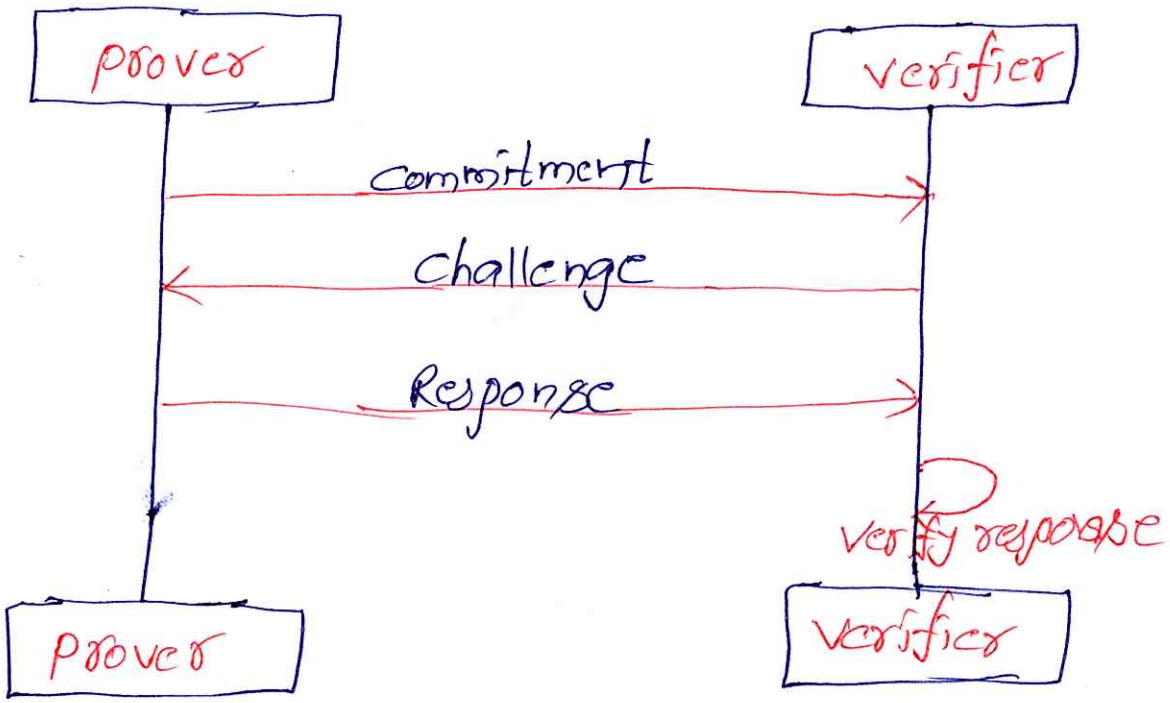
Several entity authentication protocols are used to provide secure entity verification such as:

* **Challenge-Response Protocol:-**



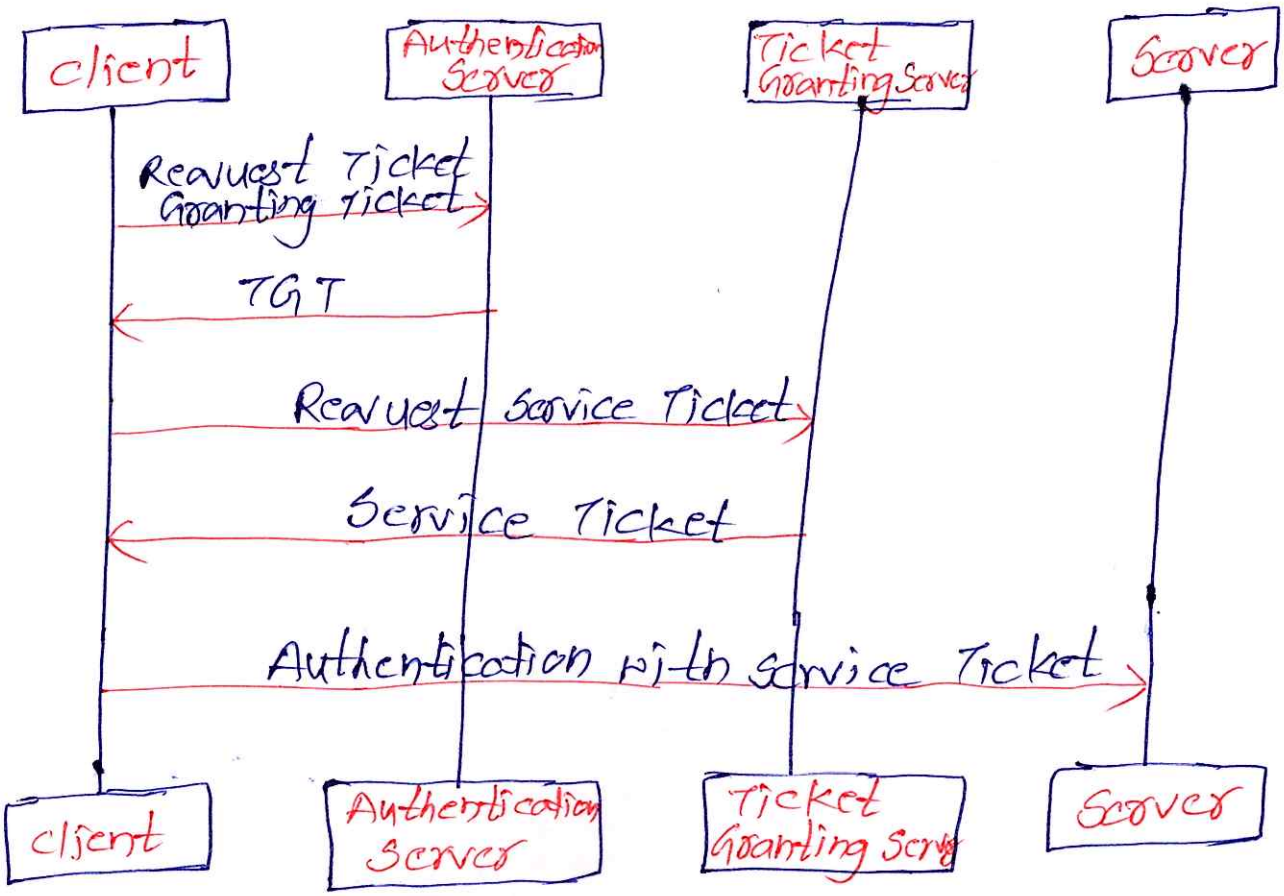
The challenge-response protol involves a challenge is being sent to the entity, the entity responds with a response, the response is verified by the challenger. This protocol is used to prevent reply attacks and ensure that the entity is genuine.

* Zero-knowledge proofs:-



Zero-knowledge proofs (ZKPs) are cryptographic protocols that enable an entity to prove its identity without revealing any sensitive information. ZKPs are used in various applications, including authentication and identity verification.

* Kerberos Authentication Protocol:-



Kerberos is a widely used authentication protocol that provides secure authentication for client-server architectures. Kerberos uses a ~~ticket~~ based system, where a client requests a ticket from a trusted third-party authentication server, which is then used to authenticate the client to the server.