

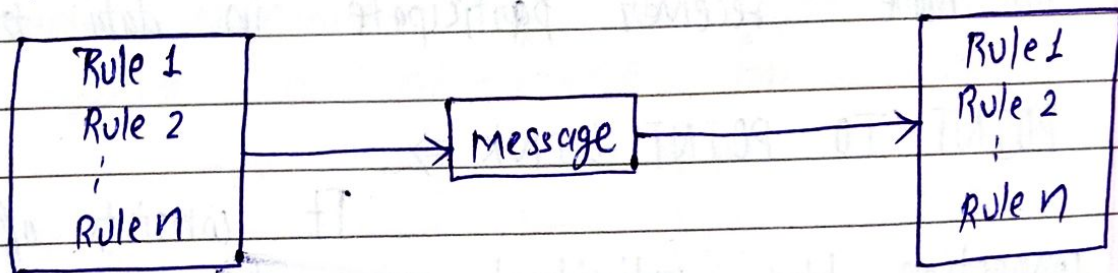
## Data Communication & Computer Network

- ✓ Data:- Raw facts & figures
- ✓ Communication:- Exchanging of info.
- ✓ Computer:- An electronic device that is design to work with one another.
- ✓ Network:- It consists of multiple devices that communicate with one another.
- ✓ Data Comm:- It refers to the transmission of this digital data b/w 2 or more computers.
- ✓ Computer network:- It is a tally comm. network that allows computer to exchange data.

### WHY TO LEARN DATA COMM. & COMPUTER NETWORK:-

- (i) Network basic understanding
- (ii) Network engg.
- (iii) Internet

Components of data comm. system:-



Major components of Data comm. system are -

- (i) Message
- (ii) Sender
- (iii) Receiver
- (iv) transmission medium
- (v) Protocols



Network HARDWARE  $\Rightarrow$  There is no generally accepted taxonomy into which all computer network fits, but 2D stand out as important

- (i) Transmission Technology
- (ii) Scale

Broadly speaking there are 2 types of transmission technology that are in wide spread used.

- (i) Broad Cast link
- (ii) Point to point link

(i) BROADCAST LINK  $\Rightarrow$

have a single comm. channel that is shared by all the machines on the network short messages called packets in certain contents sent by any machine are received by all the others.

In computer networking broadcasting refers to transmitting a packet that will be received by device on the network.

$\rightarrow$  Multicasting means one or more senders and one or more receiver participate in data transfer.

(ii) POINT TO POINT LINK  $\Rightarrow$

It consists of many connection b/w individual pairs of machine.

$\rightarrow$  Point to point transmission with one sender & one receiver is called unicasting.



## SOME NETWORK HARDWARE $\Rightarrow$

### (i) LAN (Local Area Network) :-

It is generally ~~used~~ called as LAN. These are privately owned network within a single building or campus of upto a few km in size. LAN provides a useful way of sharing the resource b/w end users. The resources such as printers, file servers, scanners & internet are easily sharable among computers.

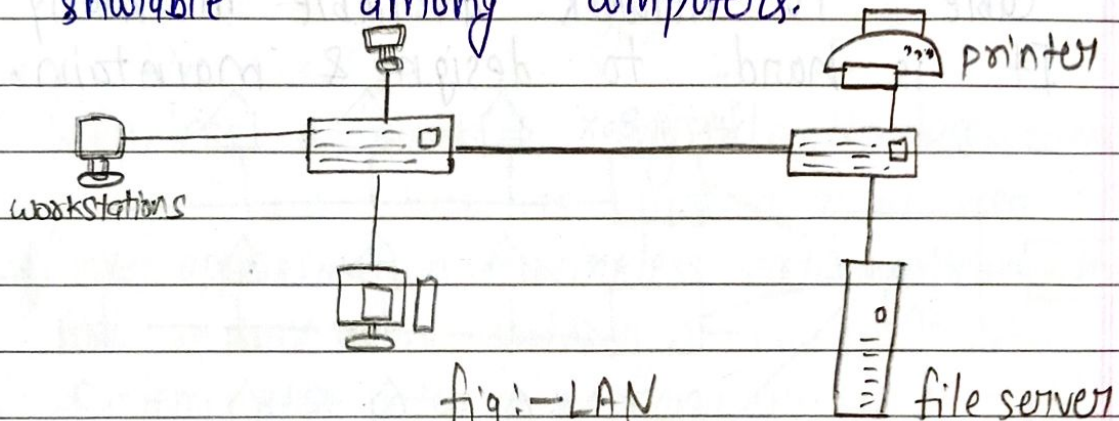
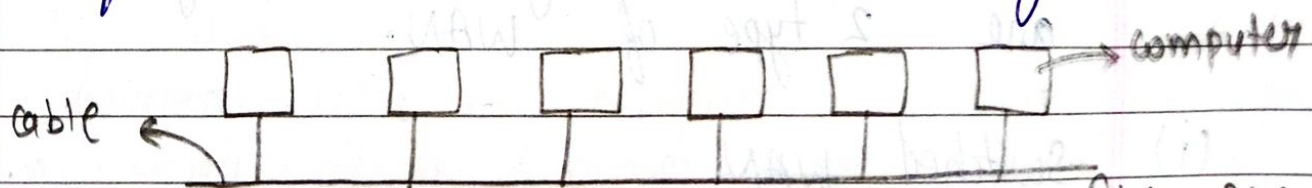


fig:-LAN

Various topology are possible for broadcast LAN. We show two of them i.e. BUS & RING. In a BUS network, at any instant atmost one machine is the master and is allow to permit / transmit and all other machine are required to re-frame for sending.



fig(9): BUS

In RING network, each bit propoget around on its own, not waiting for the rest of the packet to which it belong. Here all the nodes



are connected in closed figure. It can span large distances than other types of network.

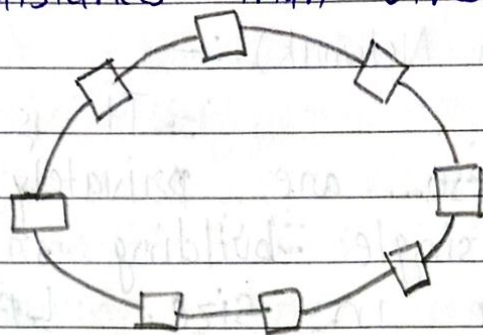
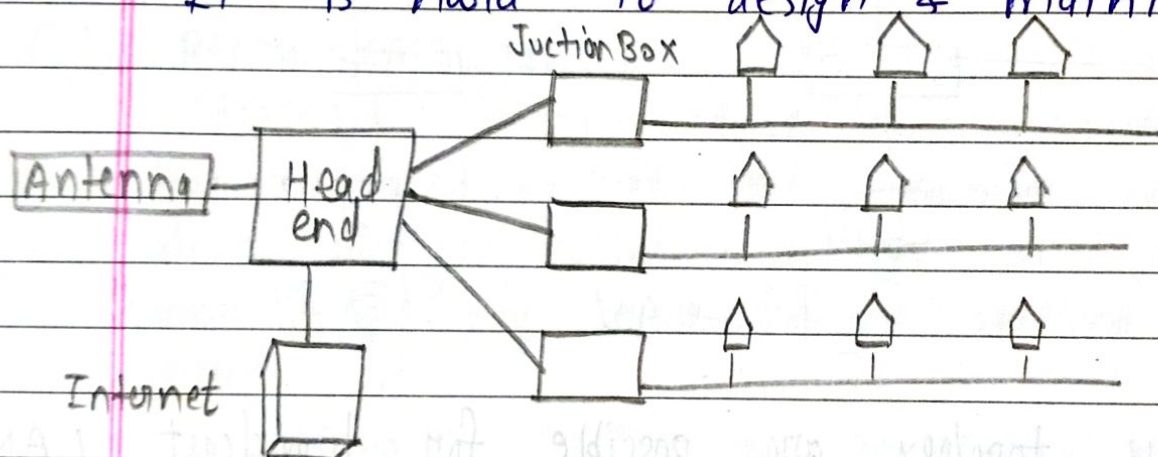


fig:- Ring

### (2.) MAN (Metropolitan Area Network):-

A MAN covers a city. The best known example of MAN is the cable TV network available in many cities. It is hard to design & maintain.

fig:- MAN  
Based on  
cable TV

### (3.) WAN (Wide Area Network):-

A WAN spans a large geographical area often a country or continent. It contains the collection of machine intended for running user programs. There are 2 type of WAN.

- (i) Switched WAN
- (ii) Point to point WAN

→ WAN is difficult to design & maintain is more congestion in network.



→ WAN data rate is slow.

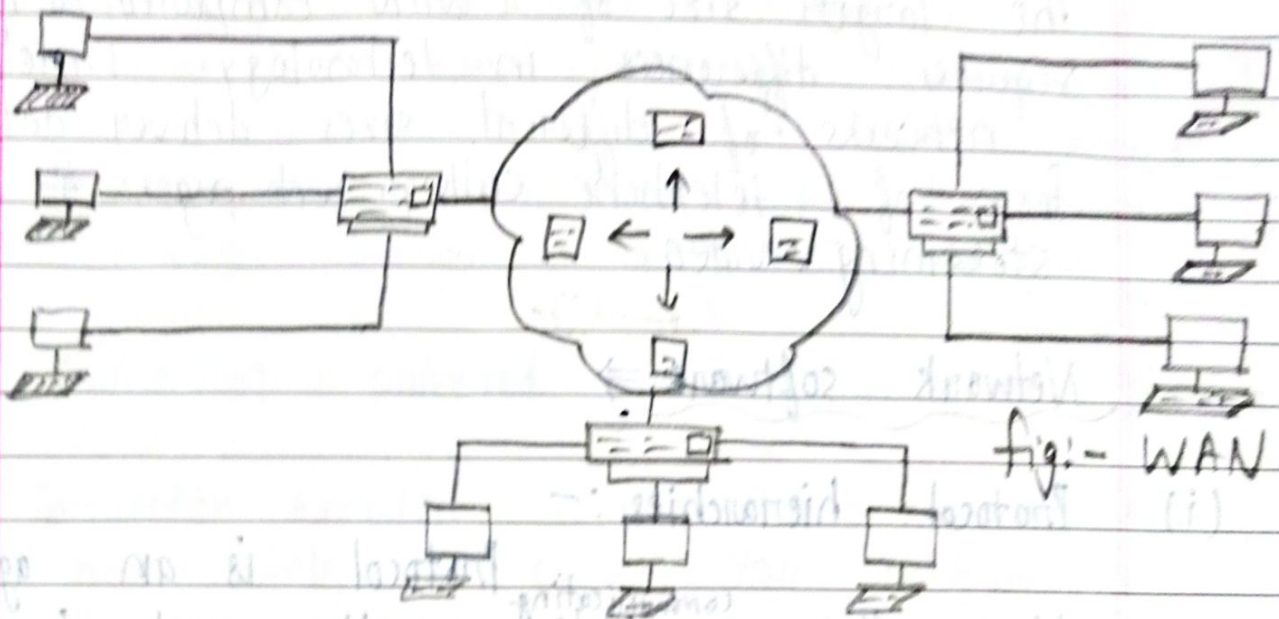


fig:- WAN

④ Wireless network  $\Rightarrow$  Digital wireless communication is not a new idea. To a first approximation wireless network can be divided into 3 main category:-

- (A) System ~~inter~~ inter connection
- (B) Wireless LAN
- (C) Wireless WAN

(A) System inter connection is all about inter connecting of a computer using short range radio. Almost every computer has a monitor, keyboard, mouse & printer connected to main unit by cables.

(B) Wireless LANs are becoming increasingly common in small offices & homes. Consequently some companies got together to design a short range wireless network called Bluetooth.



- (c) Wireless WAN, is a form of wireless network. The larger size of a WAN compared to LAN requires differences in technology. Wireless networks of different sizes deliver data in form of telephone calls, web pages & streaming video.

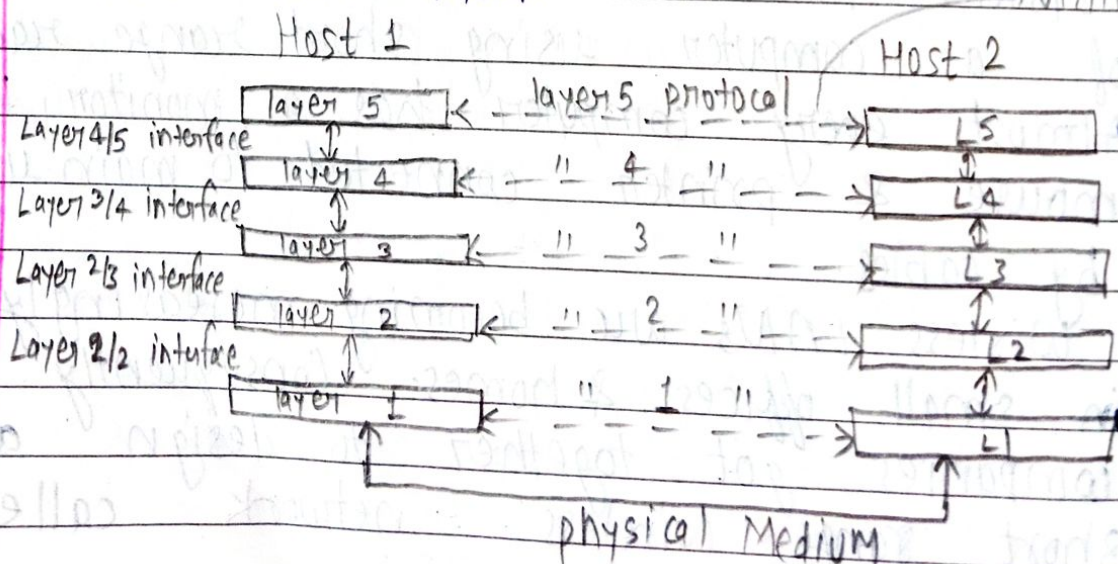
### Network software $\Rightarrow$

- (i) Protocol hierarchies :-

Protocol is an agreement blw the ~~communicating~~ <sup>communicating</sup> parties and how communication is proceed.

Protocol is the standard used to define a method per exchanging data over computer network such as land, internet etc.

The fundamental idea is that a particular piece of sw provides a service to its user but keep the details of its internal states and algorithm hidden from them.





Layer  $n$  carries a conversation with layer  $n$  on other machine. Rules in the conversation are known as layer  $n$  protocol. Here interface defines which primitive operation and services the lower layer make available for the upper one.

(ii) Connection oriented and Connection less services  $\Rightarrow$

Connection oriented service is modeled after the telephone system. You pick up the phone to talk someone, dial the number, take & Hang up. Similarly, to use a network you established the connection, use the connection & then release the connection.

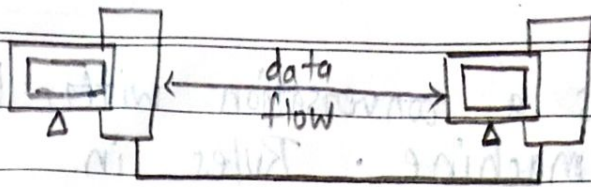
Whereas in connection less service, it is modeled after the postle system. Each message carry the full destination & Each one is routed through the system independent of all others.

Topologies  $\Rightarrow$

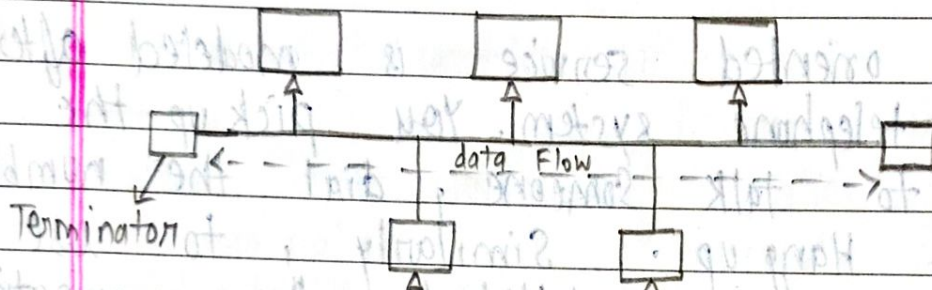
(A) Point to point Network:—

Point to point network contains exactly two hosts such as computer, switch, router & services connected back to back using a single piece of cable.

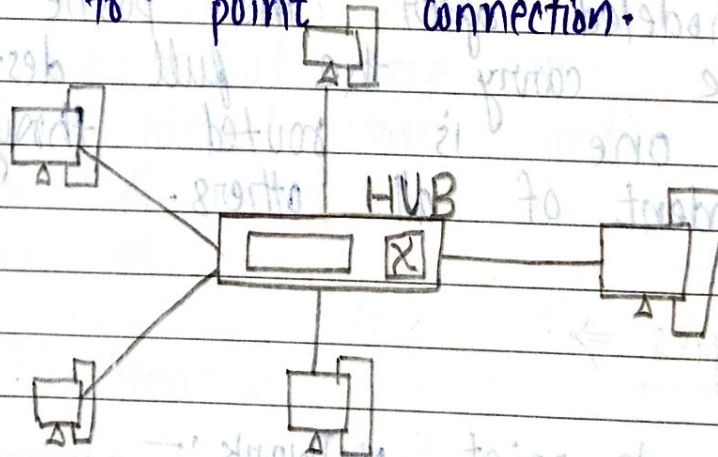




(ii) Bus topology:— In this, all devices share a single communication line or cable. Bus topology may have problem ~~when~~ while multiple host sending data at the same time.



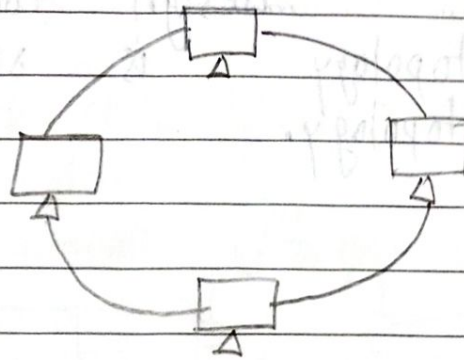
(iii) Star topology:— All host in star topology are connected to a central device known as hub devices using a point to point connection.



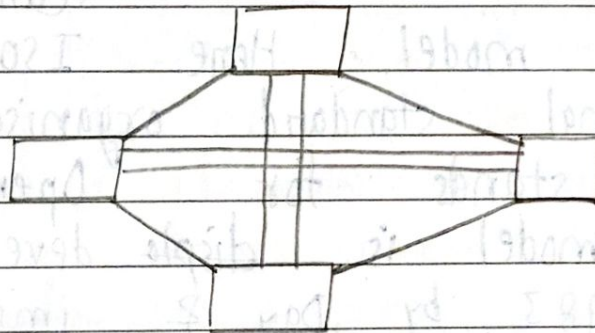
(iv) Ring topology ⇒ In Ring topology each host machine connects to exactly to other machines, creating a circular network structure, when one host tries to communicate or send message to a host which is not adjacent to it.



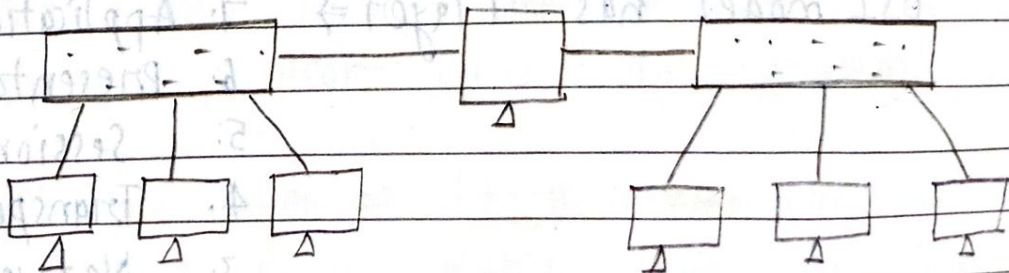
The data travels to the all intermediate Host.



(v) Mesh topology:- In this a host is connected to one or multiple host. This topology has host in point to point connection with every other host.

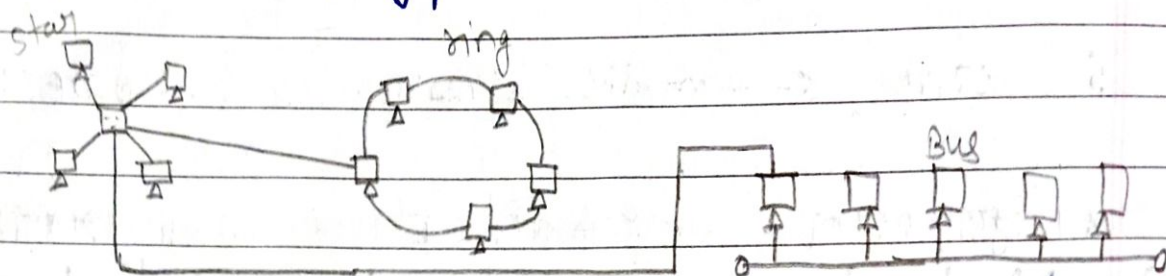


(vi) Tree topology:- It is also known as hierarchical topology. This is most common form of network. This topology implements or extended star topology and inherits properties of Bus topology.





(vii) Hybrid topology:- A network structure where design contains more than one topology is said to be as hybrid topology.



## Protocol & standard

OSI Reference Model  $\Rightarrow$  This model is also called ISO - OSI reference model. Here ISO stands for international standard organisation and OSI stands for Open System Interconnect. This model is developed by ISO in 1983 by Day & Immesman and it was revised in 1995.

It is open Systems interconnection model because it deals with connecting with open system i.e. the system that are open for communication with other system.

OSI model has 7 layers  $\Rightarrow$

7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. data link
1. Physical



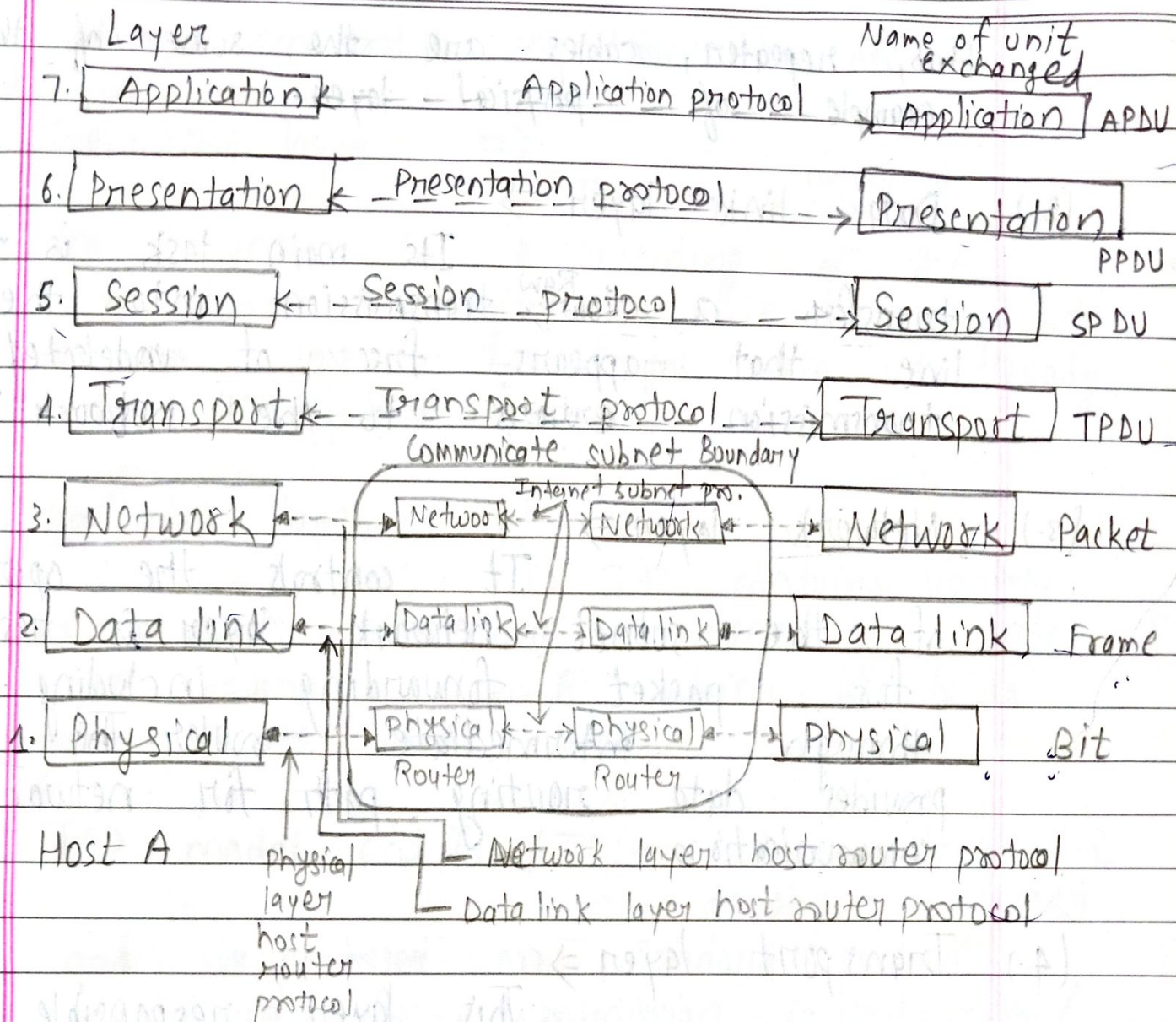


fig: OSI reference model

Broadcast networks have an additional issue in the data link layer: how to control access to the shared channel. A special sublayer of the data link layer, the medium access control sublayer, deals with this problem.

- (i) **Physical Layer**  $\Rightarrow$  It is responsible for the actual physical connection b/w devices. It contains information in the form of bits.



Hub, repeater, cables are the some of the example of physical layer.

(2.) Data link layer  $\Rightarrow$

Its main task is to transfer a ~~low~~<sup>raw</sup> transmission into the line that appears free of undetected transmission errors to the network layer.

(3.) Network layer  $\Rightarrow$

It controls the operation of the subnet network layer is responsible for packet forwarding including routing through intermediate router. This layer provides data routing path for network communication.

(4.) Transport layer  $\Rightarrow$

This layer responsible for n to n communication over a network. Its basic function is to accept data from network layer, split it into smaller units, pass these to the network layer & ensure that the pieces are arrive correctly and the other layer end.

(5.) Session Layer  $\Rightarrow$

It allows user on different machine to establish a session b/w them. Session offers various services including



dialogue control, synchronisation etc.

(6.) Presentation layer  $\Rightarrow$  This is concerned with the syntax & semantics of the information transmitted. While receiving data physical layer transforms data to ready for application layer.

(7.) Application layer  $\Rightarrow$  It contains variety of protocols that are needed by users for example HTTP which is basis for world wide web.

TCP model and TCP/IP:— It is designed & developed in 1960 and is based on standard protocol. It stands for transmission control protocol / Internet protocol.

It is concise version of OSI model.

It contains 4 layers that is

- (i) Process / Application Layer
- (ii) Host to Host / Transport Layer
- (iii) Internet Layer
- (iv) Network access or Link Layer

(i) Network access Layer  $\Rightarrow$  This layer correspond to the combination of data link layer & physical layer of OSI model.



Protocol presents in this Layer allows for the physical transmission of data. Protocol is used to connect the host so that the packets can be sent over it.

## (2.) Internet Layer $\Rightarrow$

This Layer parallels the function of OSI <sup>Network</sup> Layer. The main protocols residing at this layer are IP (Internet protocol) which is used in this layer. The various function performed by the internet layer are

- (a) Delivering packet
- (b) Performing Routing
- (c) Avoiding congestion

## (3.) Transport Layer $\Rightarrow$

It decides if data transmission should be on single path or parallel path. There are 2 and a + protocol have been defined on end transfer i.e.

- (a) Transmission control protocol (TCP)
- (b) User define protocol (UDP)

## (4.) Application / process Layer $\Rightarrow$

the higher level protocol. It contains all used in this layer. Some protocol are

- (i) ~~Internet~~ TELNET  $\Rightarrow$

It is the



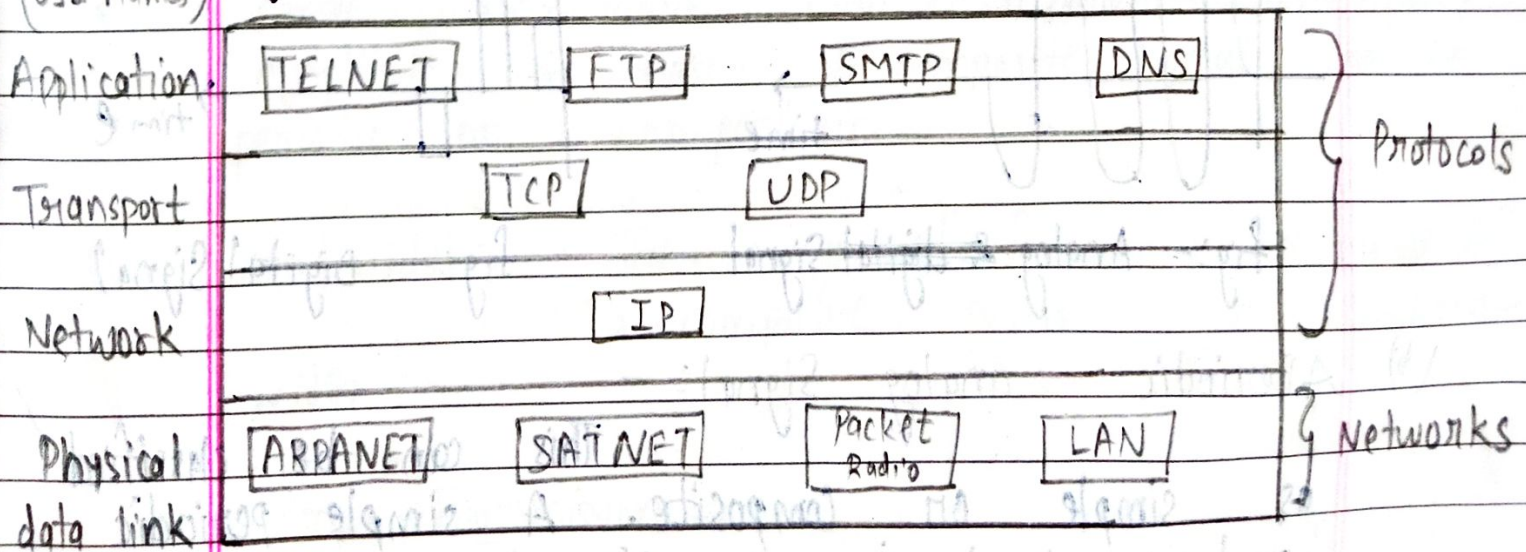
communication protocol which allow connecting to a remote machine and run application unit.

(ii) FTP  $\Rightarrow$  It is file transfer protocol which provides a way to move data from one machine to another.

(iii) SMTP  $\Rightarrow$  It is simple mail transfer protocol which is used to transport electronic mail b/w a source and destination directed via a route.

(iv) DNS  $\Rightarrow$  It is domain name server which resolves an IP address into a TELNET address for most connected over a network.

(Layer OSI names) fig:- Protocol & network in TCP/IP model





Physical Layer  $\Rightarrow$ 

## (a) Digital &amp; Analog Signal:—

Analog data refers to data i.e. of continuous format where as digital data is  $\pm$  which has discrete state so that analog data takes continuous value and digital data takes discrete value.

Similar to data the signal which represent this can also be digital or analog sign. Analog signal are known to have many levels of intensity over a given period of time. Digital signal rather have definite set of value and these are represented using a pair of perpendicular ~~axis~~ axis.

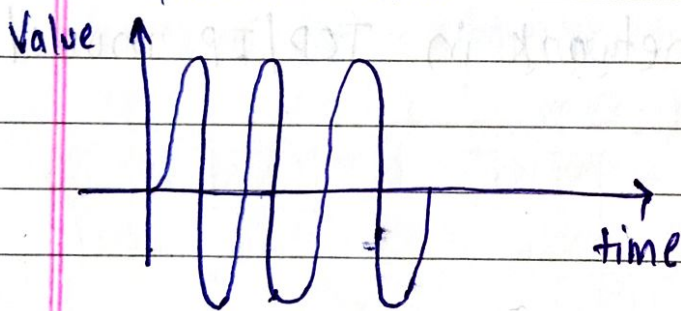


fig:- Analog &amp; digital Signal

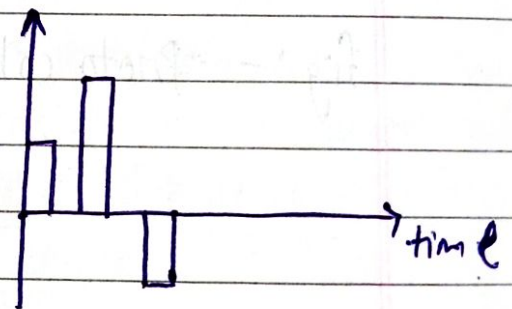


fig:- Digital Signal

## (b) Aperiodic analog Signal:—

This can be classified as simple or composite. A simple periodic analog signal is a ~~sig~~ sin wave which can not be decomposed into smaller signal. A composite periodic analog signal



is composed of multiple sin wave.  
The topic discuss in periodic analog signal are:-

(i) Sine wave :-

This can be represented by 3 parameters  
(A) Peak amplitude (B) frequency (C) Phase

(ii) Wavelength :- Wavelength is another signal travelling through a transmission medium. The wavelength is the distance, a simple signal can travel in one period.

(iii) Time & frequency domain :- To show the relationship blw amplitude & frequency we can use frequency domain block.

(iv) Composite Signal :- Any composite signal is actually a combination of simple sine wave with different frequency, amplitude & phase. A composite signal can be periodic or non-periodic.

(v) Band width :- The range of frequency contained in a composite signal is its band-width

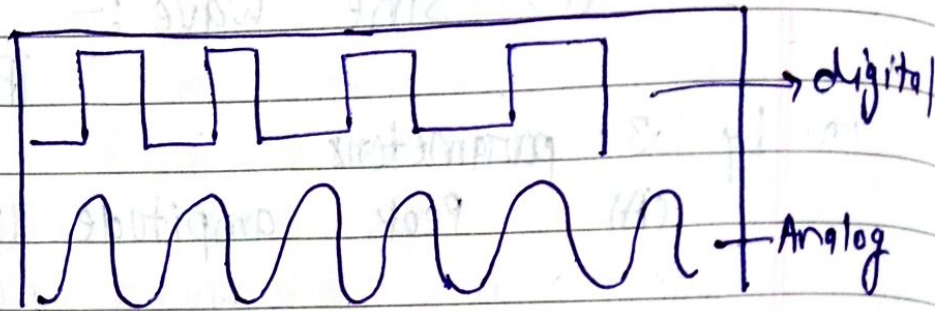
Signal Transmission  $\Rightarrow$

Signaling is a wave data which is transmitted across the medium.



It uses electrical energy to communicate.  
Basically there are two types of signaling

- (i) Digital
- (ii) Analog



- (i) Digital Signaling:— Most computer network use signaling. Encoding data in a digital signal is called encoding scheme. There are two main factors in DS i.e. (a) current state encoding (b) State transition encoding

### Advantages

- (a) Few errors from noise & interference.
- (b) Useless expensive equipment.
- (c) ~~See~~

### Disadvantages

- (a) Suffer from attenuation.
- (b) ~~See~~

(ii) Digital data transmission:—

A computer network design to send information from one point to another. This information needs to be converted to either digital signal



on analog signal for transmission.

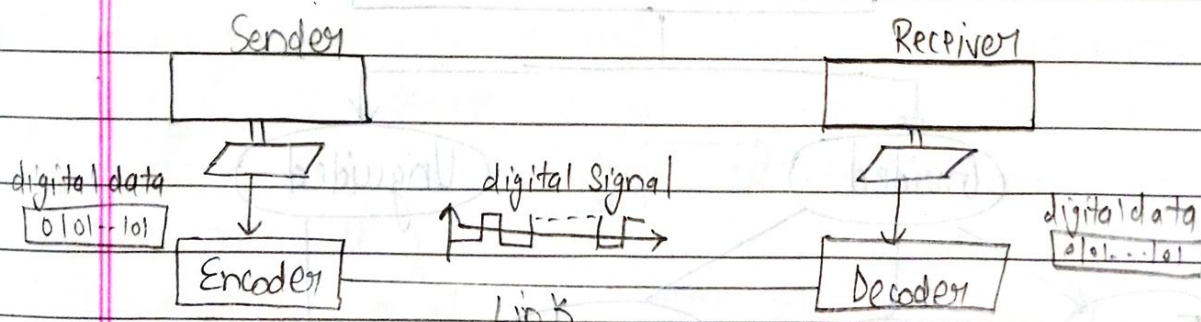
(9) Digital to Digital Conversion:—

This conversion involves 3 techniques i.e.

① Line coding, block coding and scrambling

Line coding is always needed but block coding scrambling may or may not be needed.

(I) Line coding is a process of converting digital data to digital signal. Line coding convert a sequence of bit to a digital signal. At the sender side, the data are encoded into digital signal whereas at receiver side the digital data are re-created by decoding the digital signal.



(II) Block coding helps in error detection and re-transmission of the signal. It is normally referred as mB/nB as it replaces each m bit data group with n bit data group.

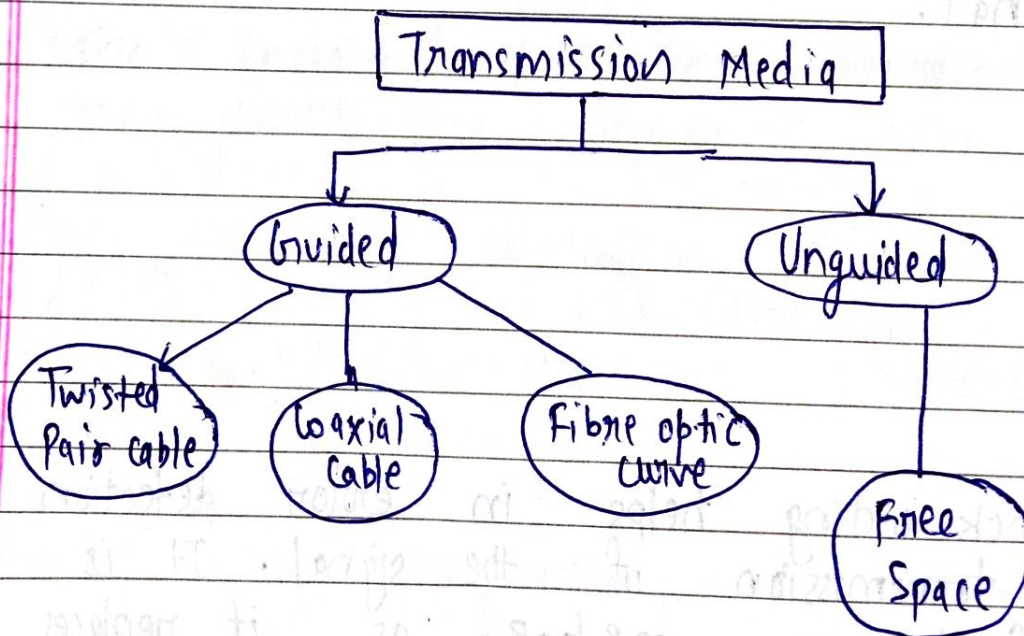


(III) Scrambling : — Scrambling is a technique that doesn't increase the number of bits and thus provide synchronisation.

Transmission Media  $\Rightarrow$

TM can be broadly defined as anything that can carry information from a source to destination. For example the transmission medium for two people having a dinner conversation in the air. The air can also be used to convey the message in the smoke signal or the semaphore. For a written message medium may be a mail, truck or airplane.

Classification of Transmission Media : —

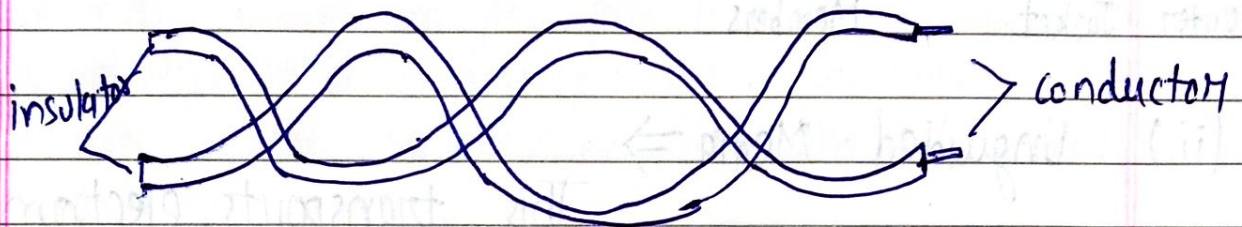


(i) Guided Media : — This provide a ~~condes~~ ~~accondi~~ from one device to another i.e. a signal travelling along



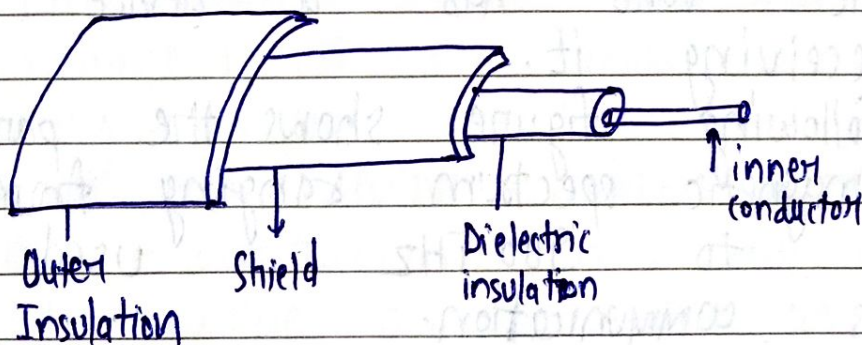
any of these media is distorted and content physical limits of the medium.

- (a) Twisted pair cable :— It uses metallic conductor that accepts & transport signals in the form of electric current. A twisted pair cable consist of two conductors each with its own plastic insulation twisted together.



- (b) Coaxial Cable :—

It is the type of cable that has an inner conductor surrounded by an insulating layer and conductive shielding.

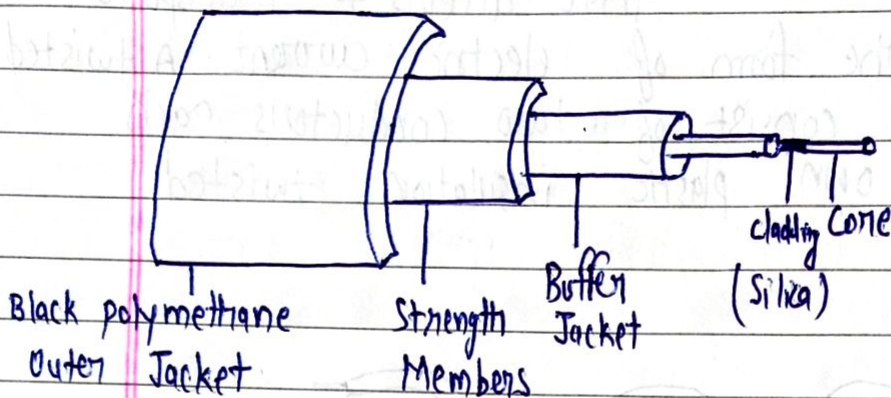


- (c) Fibre optic cable :—

It is an assembly similar to an electric cable but containing one or more optic fibres that are used to carry light. The optical fibre elements are typically



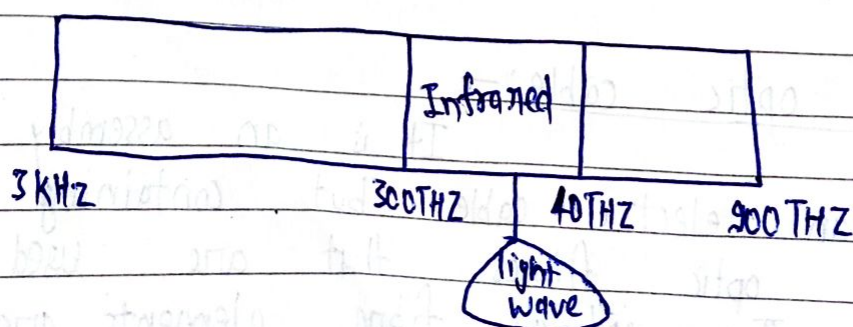
are individually coated with plastic layer & contained in a protective tube suitable for the environment where the cable will be deployed.



(ii) Unguided Media  $\Rightarrow$

This transports electromagnetic waves without using a physical conductor. This type of communication is often refers to wireless communication. Signals are normally broadcast through free space and thus are available to any one who has a device capable of receiving it.

The following figure shows the part of electromagnetic spectrum ranging from 3 kHz to 900 THz used for wireless communication.



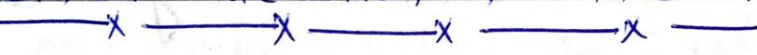


## Unit - ②

DATA LINK LAYER

- The data link layer is a second layer of 7 layer OSI model.
- This layer is the protocol layer that transfer data b/w adjacent network in a WAN or b/w nodes on the same LAN.
- The data link layer provides the functional & procedural means to transfer data b/w network entities and might provides the means to detect and possibly correct errors that may ~~be~~ occur in the physical layer.

Error detection & connection ⇒


 Decides framing, data link layer also include mechanism to detect and even recover from transmission errors. For a receiver to detect transmission error the centre must add redounded information as an error detection code to the frame set.

When the receiver obtain a frame with an error detection code, it recomputes and verifies whether the received error detection code matches the computer error detection code. If they match the frame is considered to be valid.



## Error correcting codes:-

Network Designers have developed a basic strategy for dealing with errors. One ~~base~~ way is to include enough redundant information along with each block of data send to enable the receiver to reduce what the transmitted data must have been, sent. Other way is to include only enough redundancy to allow the receiver to reduce that an error ~~reduce~~ occurred and have it request a re-transmission. The common former strategy uses error correcting code and ~~error~~ later uses error detecting code.

### Types of Error :-

#### (i) Single Bit Error $\Rightarrow$

It means only one bit of given data unit is changed from one to zero or 0 to 1. For example,  
 1 0000 1100  $\rightarrow$  1 0001 1100  
                     send                                      receiver

#### (ii) Multiple Bit Error $\Rightarrow$

In the receive frame more than one bit are corrupted. For example -

10011010  $\rightarrow$  10011010  
                     send                                      receiver



(iii) Burst Error  $\Rightarrow$

In the received frame, more than one ~~consecutive~~ <sup>consecutive</sup> ~~are~~ corrupted.

for example

1 0 0 1 1 0 1  $\longrightarrow$  1 0 0 0 0 0 1

Error detection Method :-

(A) VRC (Vertical Redundancy Check)  $\Rightarrow$

It is also called parity check. In this technique a redundant bit called a parity bit. One extra bit is sent along with the original bits to make no. of ones either even in case of even parity, or odd in case of odd parity.

1 0 0 1 0 0 1  $\longrightarrow$  1 0 0 1 0 0 1 1  
 Sent received  
 Data bits even parity form

(B) Longitudinal Redundancy Check (LRC)  $\Rightarrow$

In this a block of bits is organised in a table (rows & columns)

1	1	1	0	0	1	1	1	[ For odd we use 1 ] [ For even we use 0 ]
1	1	0	1	1	1	0	1	
0	0	1	1	1	0	0	1	
1	0	1	0	1	0	0	1	
1	0	1	0	1	0	1	0	



## 2 - Dimensional parity check : —

In this Both rows & columns are checked

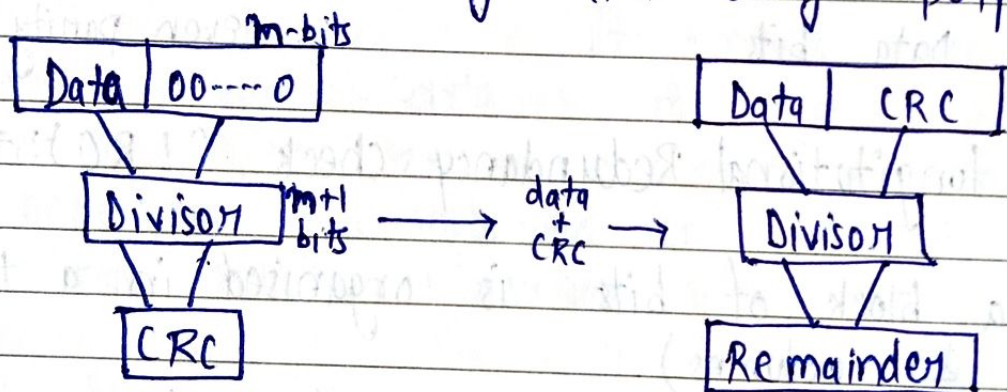
1	1	1	0	0	1	1	1	0
1	1	0	1	1	1	0	1	0
0	0	1	1	1	0	0	1	0
1	0	1	0	1	0	0	1	0
1	0	1	0	1	0	1	0	0

So final data we sent is

11100111011011101000111001010101001010101000

## (c) CRC (Cyclic Redundancy check) : —

CRC is different approach to detect if the receive frame contains valid data. This technique involves binary division of the bits are being sent. The divisor is generated using polynomials.



∴ zero = accepts

∴ Non-zero = not accepts

Algo : —

Step-1 Append n zero to the data unit, divisor is a n+1 bits.



Step-2 The newly data unit is divided by divisor using binary division. The remainder from division is the CRC.

Step-3 CRC of  $n$ -bits derived in step-2 replaces the appended zero at the end of data unit.

(D) ~~Step-4~~ Check sum :-

At sender side

(i) The data unit is divided into ~~two~~  $k$ -sections each of  $m$  bits

(ii) All sections are added together using once complement to get sum.

(iii) The sum is complemented and becomes the checksum.

(iv) The checksum is sent with the data.

At receiver site

(i) The data unit is divided into  $k$ -section each of  $n$  bits.

(ii) All sections are added together using once complement to get sum.

(iii) The sum is complemented

(iv) If the result is zero then data are accepted otherwise it will be rejected.

Block Coding:-

Block coding refers to the technique of adding extra bits to a digital word in order to improve the reliability of transmission. The word consists of a message bits plus code bits. It may also contain frame synchronisation bit.

✓ Sender

Dataword

↓  
Generator

↓  
Codeword

Receiver

Dataword

↑  
Checker

↑  
Codeword

← Block coding →



Example: —

$$K=2, n=3$$

Data word	Codeword
00	000
01	011
10	101
11	110

Here sender encodes the data 01 as 011 and send it to receiver. Receiver check the codeword, if codeword is valid then receiver extract from 011 other wise code word is corrupted or discarded.

Disadvantage: → If codeword is corrupted during transmission and 000 is received instead of 011 then the codeword is invalid and ~~code~~ data is destroyed.

# linear block coding: —

Linear code is an error correcting code for which any linear combination of code words is also a codeword. Linear codes are traditionally partitioned into block codes and convolution codes. Linear code allows for more efficient in coding & decoding algorithm than other code.



Linear codes are used in forward error correction and are applied in methods for transmitting symbol on a communication channel, so that if error occurs in the communication same error can be corrected or detected by the ~~repetition~~ of the message block. reception

A linear block code of  $n$  transmits block containing ~~an~~  $n$  symbols. For example (7,4) Hamming code is a linear binary code which represents 4-bit message using 7 bit codewords.

# Hamming Code: —

This can be applied to data units of any length and uses the relationship b/w data and redundancy bits. Hamming code is a set of error correction codes that can be used to detect and correct the error that can occur when the data is move or store from the ~~sen~~ sender to the receiver.

Flow control  $\Rightarrow$

In data communication flow control is the process of managing the rate of data transmission b/w two nodes to prevent a sender from overwhelming a slow receiver.



Flow control is important because it is possible for a sending computer to transmit information at a faster rate than the destination computer can receive and process it. Flow control is divided into 2 parts: —

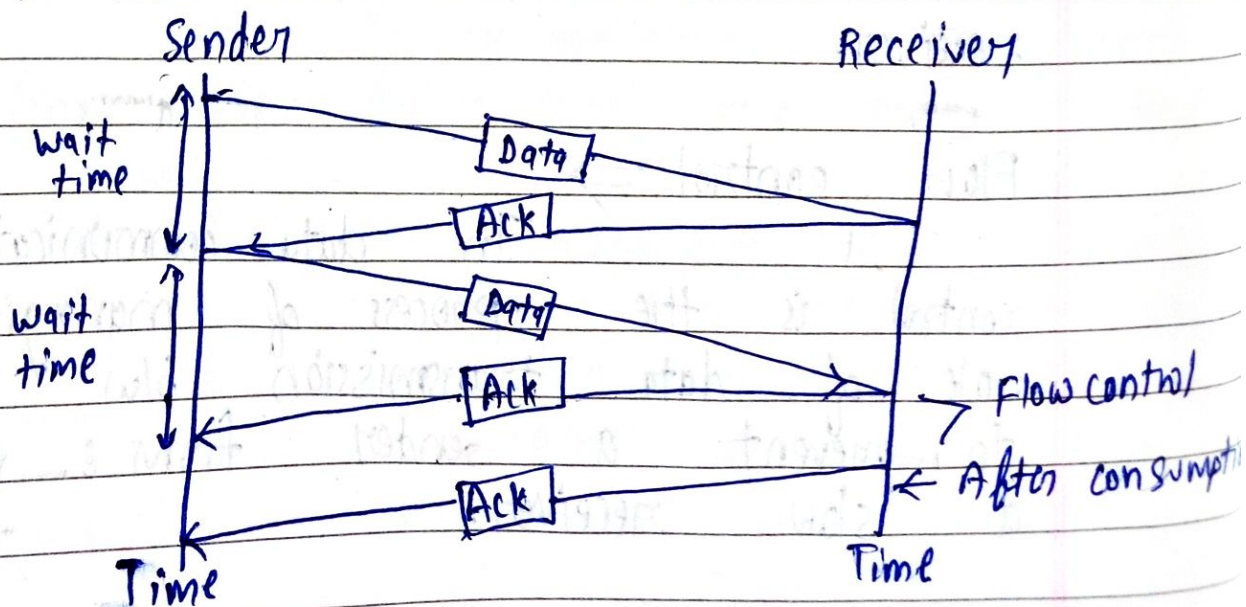
- (i) Stop & wait (Send one frame at a time)
- (ii) Sliding window (Send several frame at a time)

### (1) Stop and wait $\Rightarrow$

Stop and wait flow control is the simplest form of it. In this method the message is broken into multiple frames and receiver indicates the readiness to receive frame of data.

The sender waits for a receipt acknowledgement after every frame for a specified time.

The receiver sends the acknowledgement to let the sender know that the frame of data was received correctly. The sender will send to next frame only after the ack.





operation : —

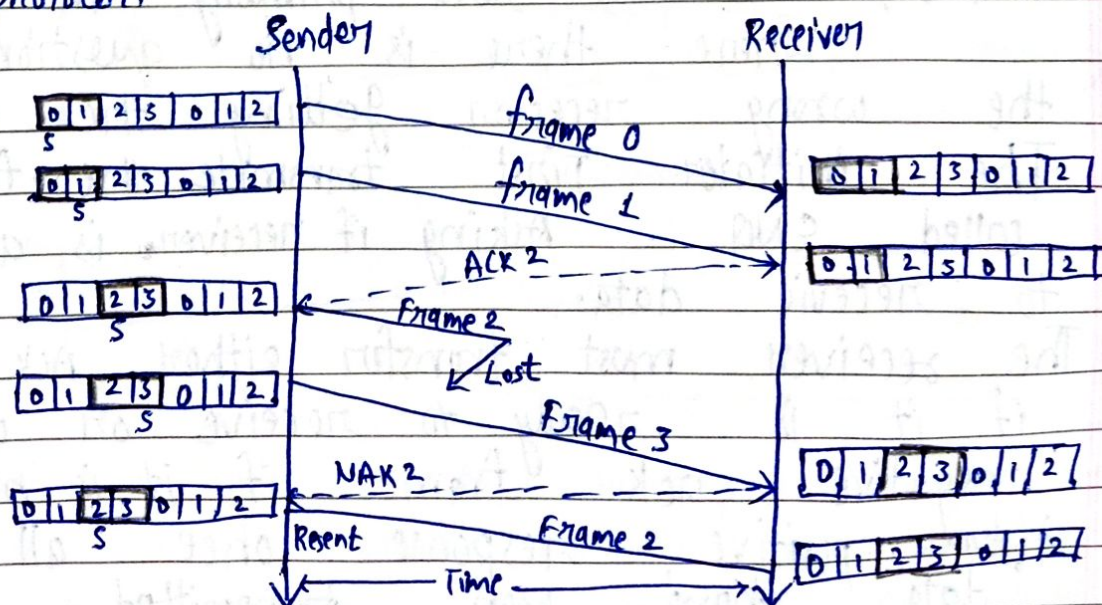
- (i) Sender:— It transmits the singal frame at a time.
- (ii) Sender waits to receive acknowledgement time out.
- (iii) Receiver:— Transmit ack. as it receives a frame.
- (iv) Go to step - 1 then ack. receive for time out is hit.

Problem is stop & wait :—

- (i) Lost data
- (ii) Lost acknowledgement
- (iii) ~~Delayed~~ ack. / data
- (iv) Delegated

(2) Sliding Window  $\Rightarrow$

In this, sender can transmit several frames before leading an ack. Sliding window refers to imaginary boxes at both sender & receiver side. Sliding window refer to packet based data transmission protocol.





Required sequence number:— Each sending frame has to be given a unique sequence number.

→ Maximum no. of frame that can be sent in the window is  $1+2A$ , same as minimum no. of sequence.

Note:- When min. no. of bits is asked we take the ceil. When max. no. of bit is asked we take the floor.

Implementation of Sliding window:—

There are 2 phase to implement:—

- ① Go Back N protocol.
- ② Selective repeat protocol.

Line discipline  $\Rightarrow$  It is of two type

- (i) ENQ [Enquiry or acknowledgement]
- (ii) Poll or select

(i) ENQ  $\Rightarrow$  It is used primarily in system where there is no question of the wrong receiver getting the transmission. The initiator first transmits the frame called ENQ. Asking if receiver is available to receive data. The receiver must transfer either Ack is frame if it is ready to receive or with a negative ack frame if it is not. After positive response once all of its data have been transmitted, the



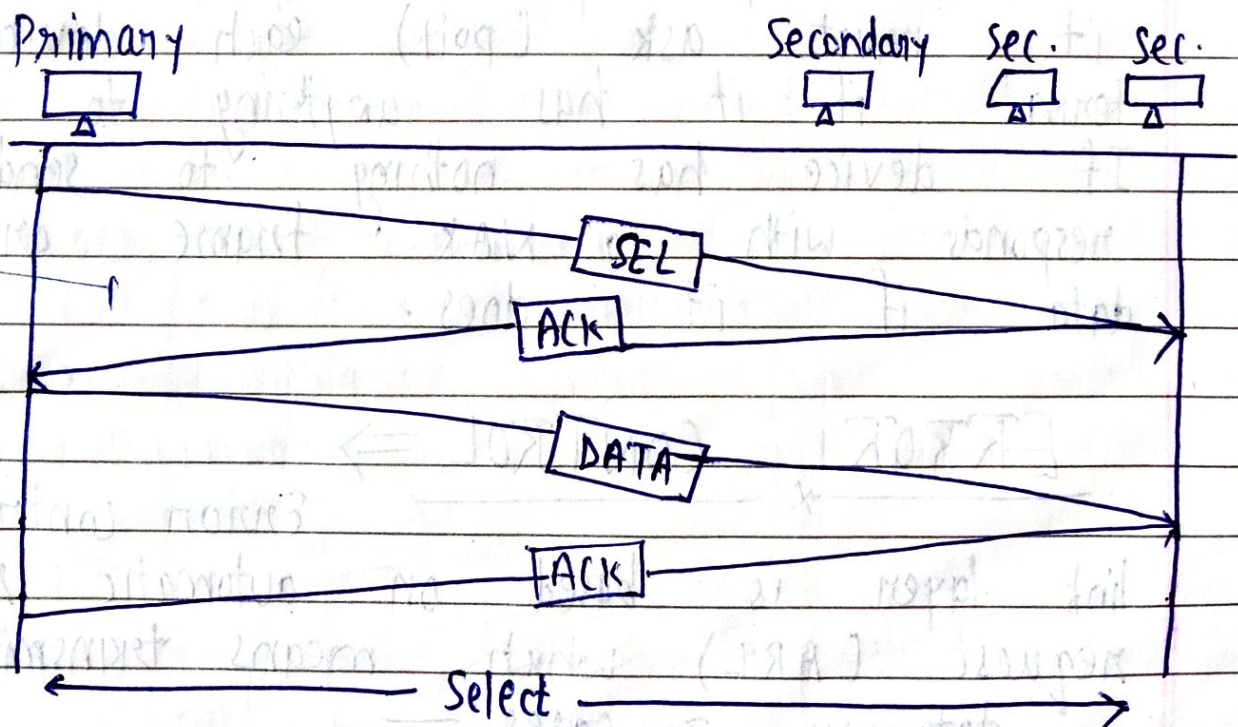
sending system finishes with an end of transmission frame.

(ii) Poll or select  $\Rightarrow$

This method works with topologies where one device is designated as primary station & others are secondary station. The primary device control the link and secondary device follow its instructions.

It is upto primary to determine which device is allowed to use the channel at a given time.

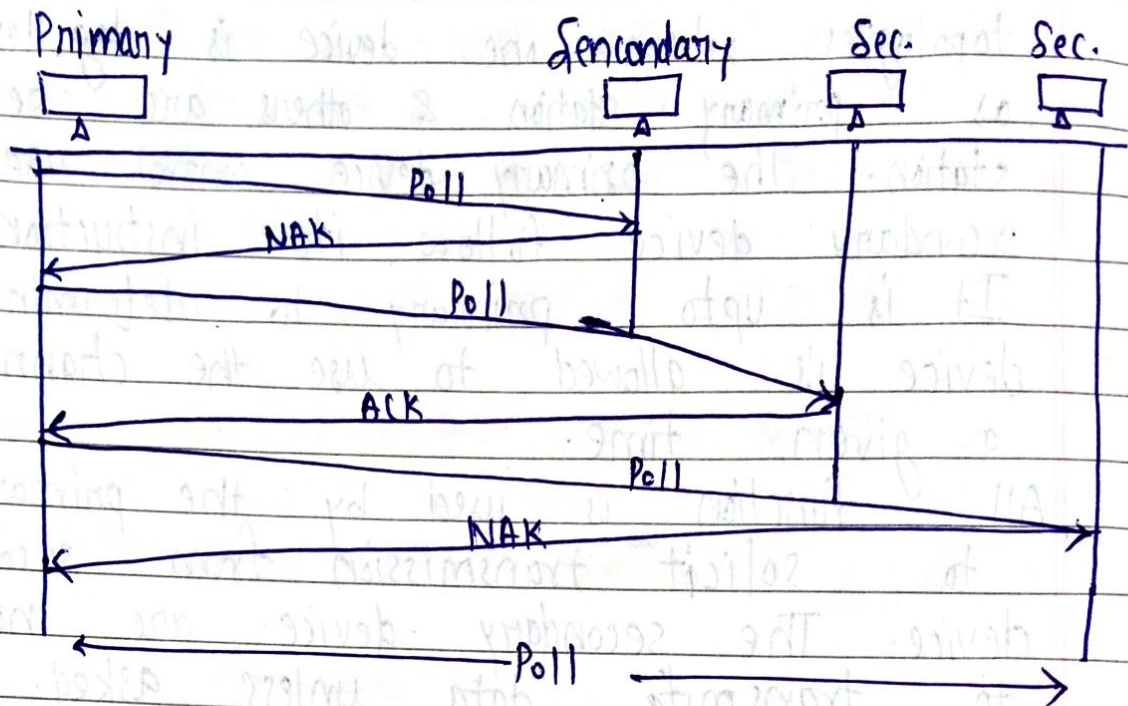
All function is used by the primary device to solicit transmission from secondary device. The secondary device are not allowed to transmit data unless asked.



Before sending data, primary creates and transmits a select frame. In the case of select frame, the enclosed data consist of an allot the



data are forth-coming. If the secondary is awake and running it returns ack. frame to primary. Primary then sends one or more data frames.



When the primary is ready to receive data it must ask (poll) each device in turn if it has anything to send. If device has nothing to send, it responds with a NAK frame or with data if it does.

### ERROR CONTROL ⇒

Error control in data link layer is based on automatic repeat request (ARQ) which means transmission of data in 3 cases:—

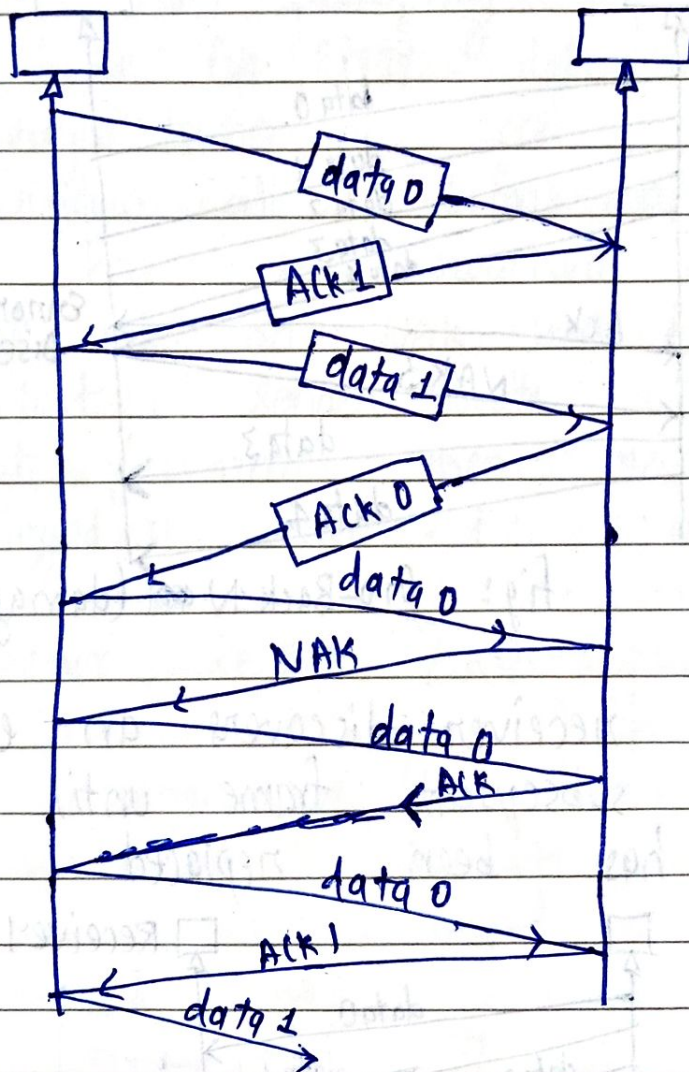
- (i) Damaged frame.
- (ii) Lost frame
- (iii) Lost ACK.



Error control is divided into 2 parts:—

- (i) Stop and wait ARQ
- (ii) Sliding window ARQ

(i) Stop and wait ARQ  $\Rightarrow$  Stop and wait flow control extended to include re-transmission of data in case of lost or damage frame.



- (ii) Sliding Window ARQ  $\Rightarrow$  There are 2 most popular protocol in this
- i.e. (i) go and back ARQ and
  - (ii) select, reject ARQ.
- The sending device keeps copies of all transmitted



frames until they have been ackd.  
 (a) Go-Back N ARQ:—

In this if one frame is lost or damaged, all frames sent since the last frame ack are transmitted.  
 If first ack. received is NAK3 it means frames 0, 1, 2 were all received in good shape. And only frame 3 must be re-sent.

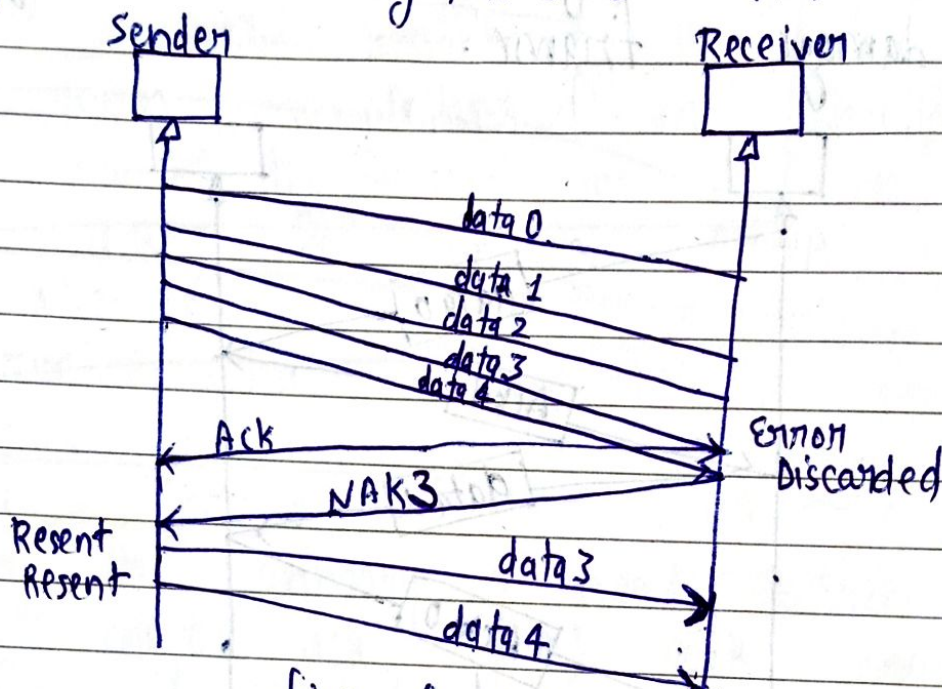


Fig: Go-Back N ARQ (damaged frame ARQ)

When the receiver discovers an error, it stops accepting subsequent frame until the damaged frame has been replaced correctly.

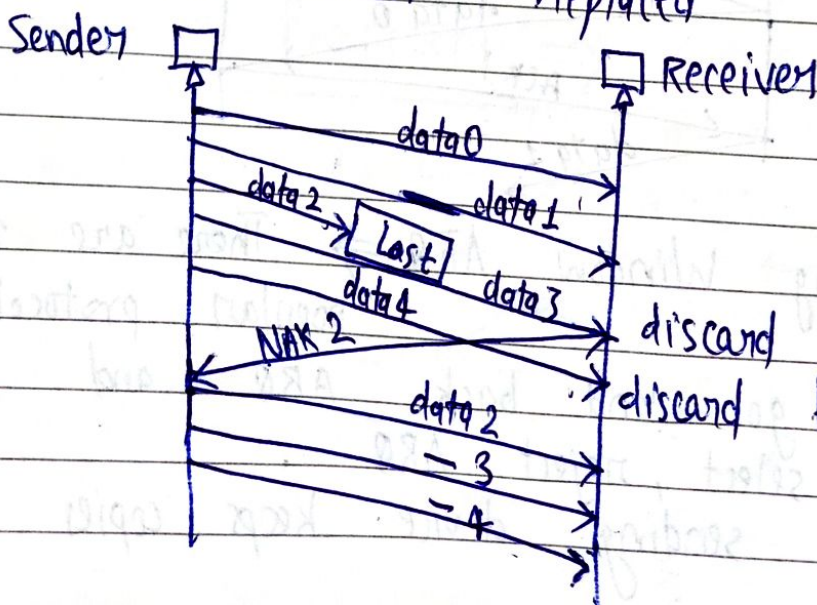


Fig: Go Back N ARQ (Lost Frame)



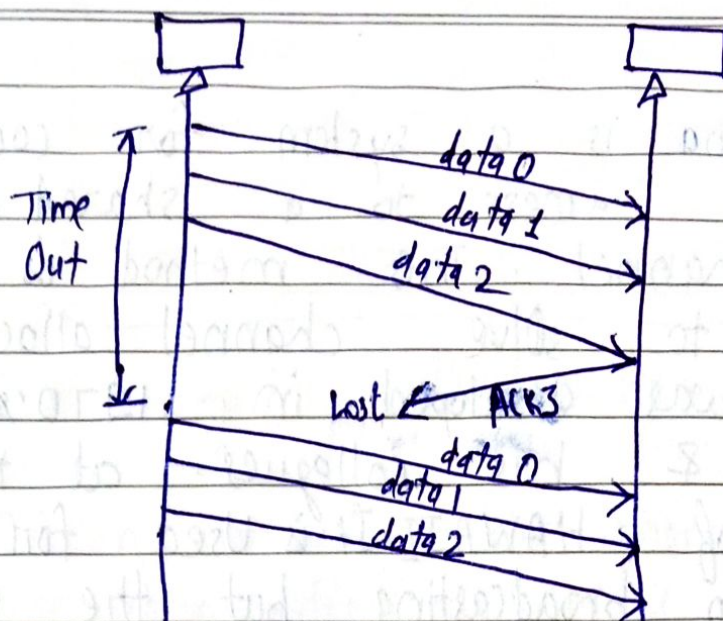


fig:- Go Back N  
ARQ (Lost Ack)

Sender is not ~~accepting~~ expecting to receive an ARQ frame for every data frame it sends. The sending device can send many frames, The window allows before waiting & ack. Once the limit has been reached it must wait. If the ack. or NAK sent by receiver has been lost, sender waits a predetermine amount of time then re-transmits the un-acknowledged frame.

(b) Selective - Reject ARQ:-

In this only the specific damage or lose frame is re-transmitted.

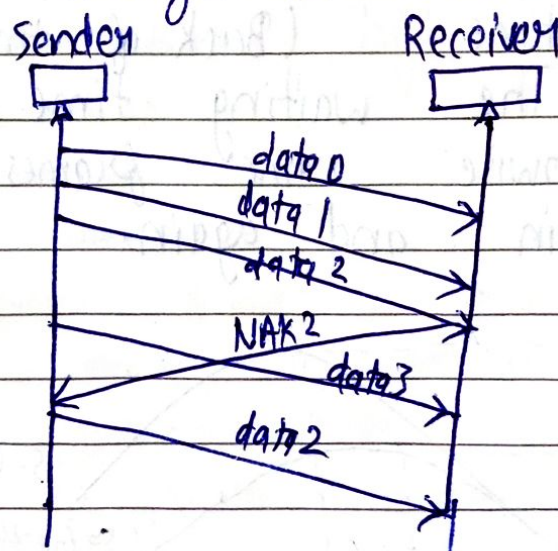


fig:- Selective  
Reject ARQ



## ALOHA :-

Aloha is a system for coordinating & arbitrating access to a shared common network channel. This method is used or developed to solve channel allocation problem. It was developed in 1970's by Norman & his colleagues at the university of HAWAII. It is used for ground based radio broadcasting but the system has been implemented in satellite comm<sup>n</sup> system.

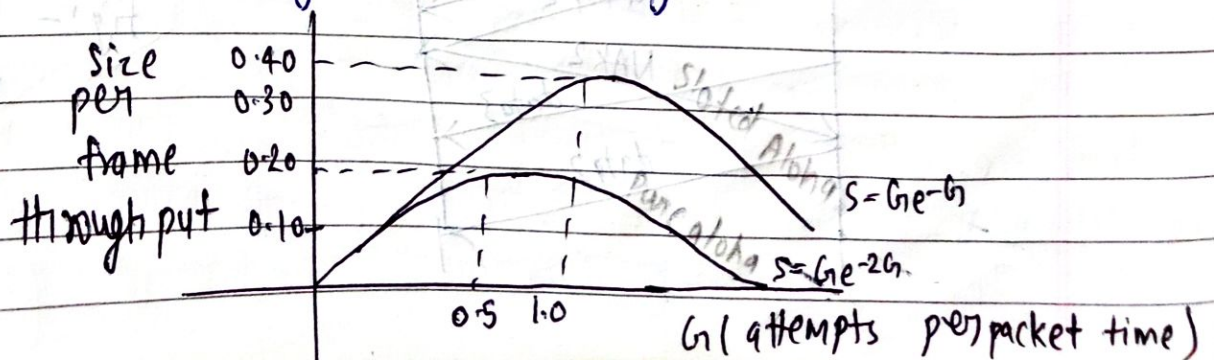
There are 2 types of ALOHA

(i) Pure Aloha

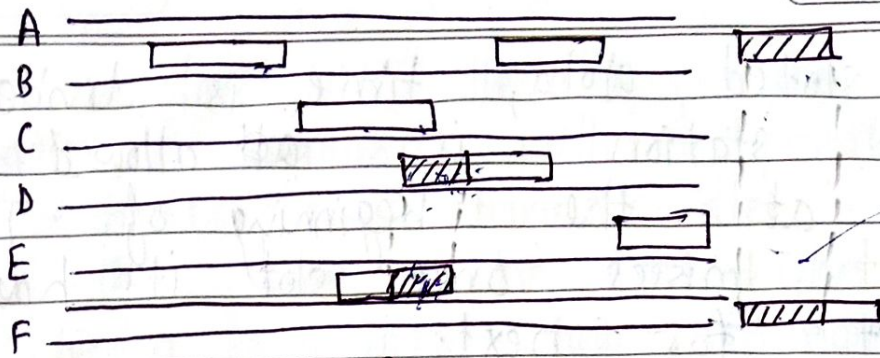
(ii) Slotted Aloha

### (i) Pure Aloha :-

The basic idea of an aloha system is simple i.e. let users transmit whenever they have data to be sent. When two or station transmit simultaneously there is collision and the frames are destroyed. The sender waits random amount of time (Back of times) and sends it again. The waiting time must be random otherwise same frames will collide again and again.







Pure Aloha

If a station starts transmitting data at any point of time, it is transmitted for  $2T$  time. During this time if any station starts transmitting data then there can be a collision.

Vulnerable time pure Aloha =  $2 \times T$ .

where  $T$  is vulnerable time.

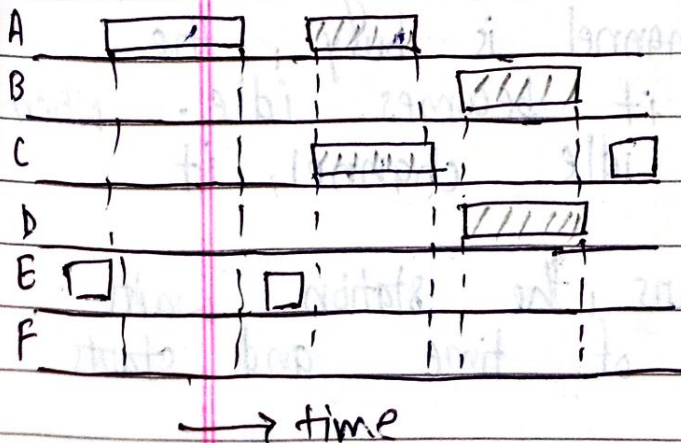
Efficiency in pure aloha =  $G \times e^{-2G}$

where  $G$  = no. of stations who wants to transmit in slot. Max. Utilization = 18%.

## (ii). Slotted Aloha:-

It is advance version of pure aloha. The slotted aloha was invented to improve ~~in~~ <sup>introduce</sup> the efficiency of pure aloha as chance of collision in pure aloha is very high.

Max utilization increased to 36%.





In slotted aloha, time is divided into slots. Each station is ~~not~~ allowed to transmit only at the beginning of TT slot, if it misses once slot it has to wait for next. Efficiency in slotted aloha is  $G \times e^{-G}$

CSMA  $\Rightarrow$  (Carrier Sense Multiple Access protocols)

CSMA was developed to overcome the problem found in Aloha i.e. to minimize the chances of collision.

With slotted aloha best utilization of channel that can be achieved is i.e. CSMA based on carrier sense protocols in which stations listen for a carrier (i.e. a transmission) and act accordingly are called "carrier sense protocols".

(1.) Persistent CSMA : —

When a station has data to send, it first listens to channel to see if anyone else is transmitting at that moment. If the channel is busy, the station waits until it becomes idle. When a station detects an idle channel, it transmits a frames.

If a collision occurs, the station waits a random amount of time and starts all over again.



The protocol is called 1-persistent because the station transmits with a probability of 1 when it finds the channel idle.

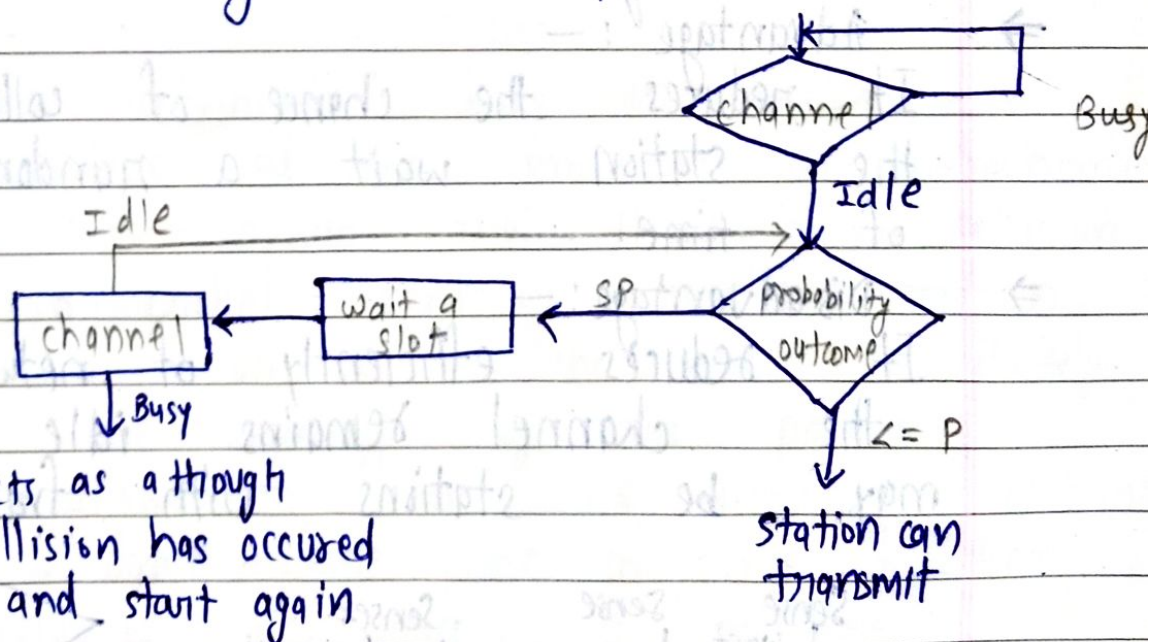
In this method has the highest chance of collusion because two or more stations may find channel to be idle at the same time and transmit their frames.

### (2.1) P-Persistent:-

It applies to slotted channels, When a station becomes ready to send, it senses the channel. If it is idle, it transmits with a probability  $P$ . If channel is busy station waits until next slot.

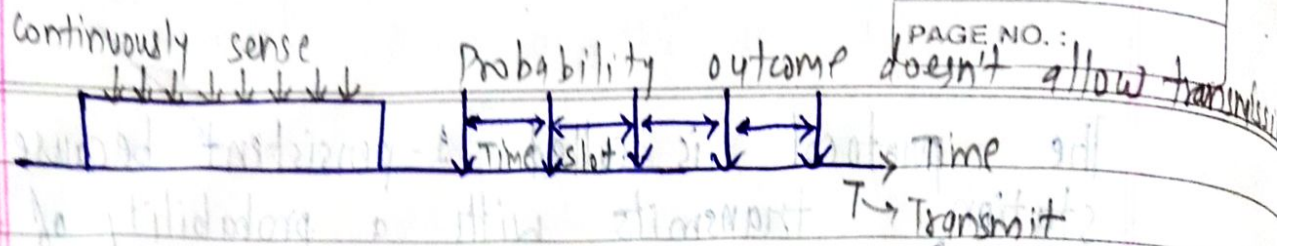
With probability  $2=1-P$ , the station then waits for the beginning of next time slot.

If next slot is also idle, it either transmits or waits again with probabilities  $2 \neq P$ .



It improves efficiency of n/w and reduces chance of collision.





### (3) Non-persistent : —

In this, if station wants to transmits a frame and it finds that channel is busy then it will wait for fixed interval of time.

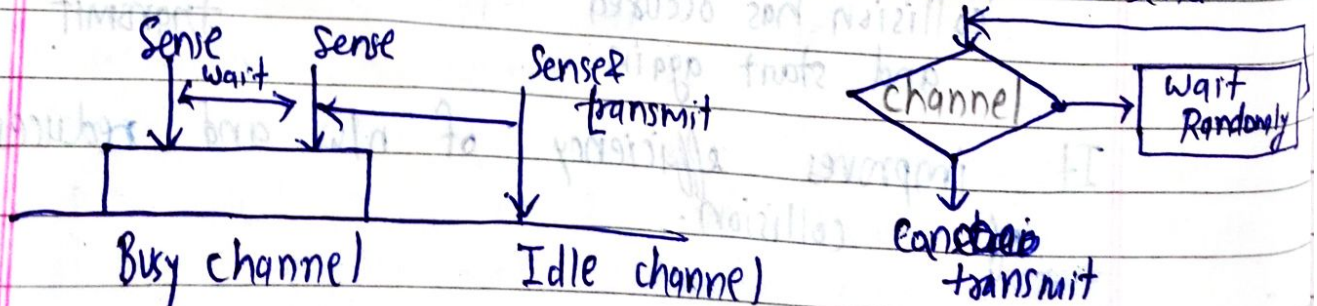
- After this time, it again checks the status of the channel and if the channel is free it will transmit.
- A station that has a frame to send senses the channel.
- If channel is idle, it sends immediately.
- If channel is busy, it waits a random amount of time & then senses the channel again.
- In non-persistent CSMA the station doesn't continuously sense the channel.

#### ⇒ Advantage : —

- It reduces the chance of collision because the station wait a random amount of time.

#### ⇒ Disadvantage : —

- It reduces efficiency of network because the channel remains idle when there may be stations with frame to send.





## Drawback of 1- Persistent:-

Propagation Delay time greatly affects this protocol. Suppose, just after the station 1 begins its transmission Station 2 also become ready to send its data and senses the channel. If station 1 signal has not yet reached station 2, Station 2 will sense the channel to be idle and will begin its transmission. This will result in collision.

## CSMA / CD [CSMA with collision Detection]

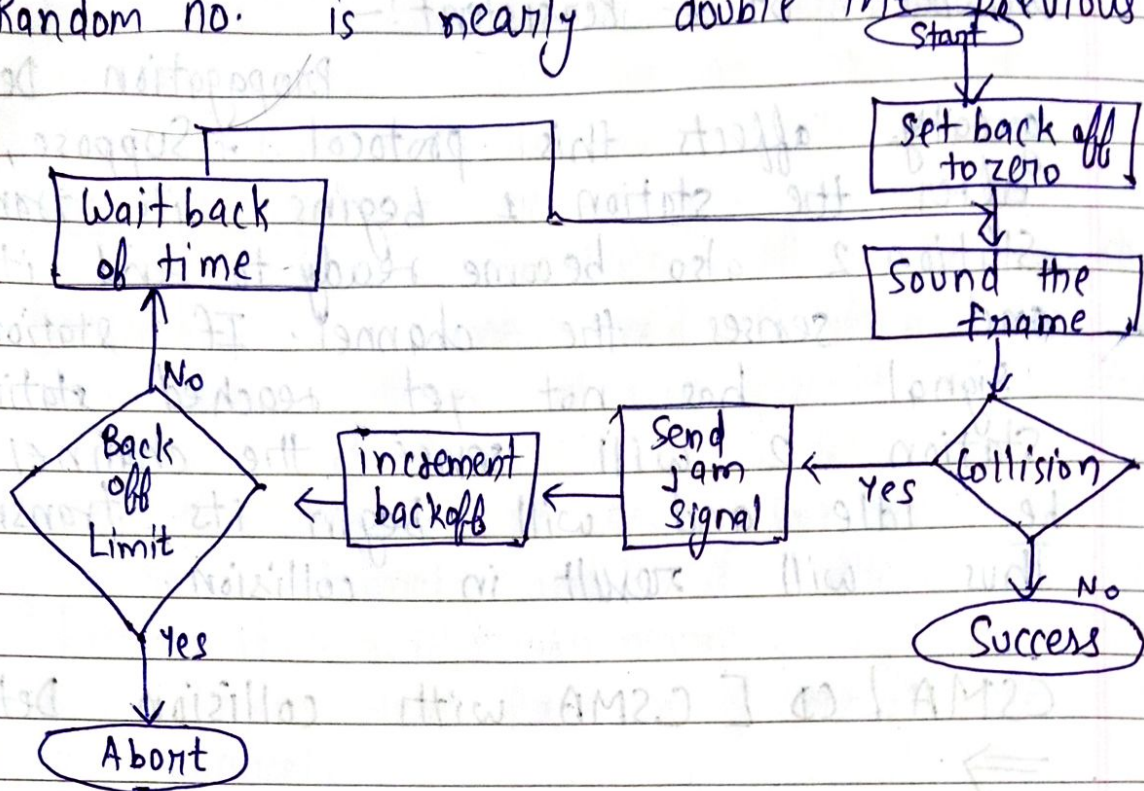


- It is a media access control method widely used in Ethernet technology / LANs.
- CSMA / CD is a protocol in which the ~~statement~~ station senses the carrier or channel before transmitting frame just as in persistent and non-persistent CSMA.
- If the channel is busy the station waits, it listens at the same time on communication media to ensure that there is no collision with a packet sent by another station.
- In a collision, the issuer immediately cancel the sending of the package.
- This allows to limit the duration of collisions: We don't waste time to send a packet complete if it detects a collision.
- After a collision, the transmitter waits again silence and again, he continued his hold for random no. but this time the



If collision is detected then, to ensure all stations are aware of the collision, the source station transmits a random bit pattern known as the jam sequence.

Random no. is nearly double the previous one.



CSMA/CA — Collision Avoidance :—

CSMA/CA protocol is used in wireless networks because they can't detect the collision so the only solution is Collision Avoidance.

CSMA avoids collisions using 3 basic techniques:-

① Interframe space (IFS) ⇒

Whenever the channel is found idle, the station doesn't transmit immediately. It waits for a period of time called IFS. When channel is sensed to be idle, it may be possible that some distant station may have already started transmitting and the signal of that distant station hasn't yet reached other stations.

Therefore purpose of IFS, the channel is still idle,



the station can send but it still needs to wait a time equal to contention time.

IFS variable can also be used to define the priority of a station or a frame.

## ② Contention window $\Rightarrow$

It is an amount of time divided into slots. A station that is ready to send chooses a Random no. of slot as its wait time.

- The no. of slots in window changes acc. to back off strategy. It means that it is set of one slot the first time & then doubles each time station can't detect an idle channel after the IFS time.

In contention window the station needs to sense the channel after each time slot.

If station finds the channel busy, it doesn't restart the process. It just stops the timer & restarts it when the channel is sensed as idle.

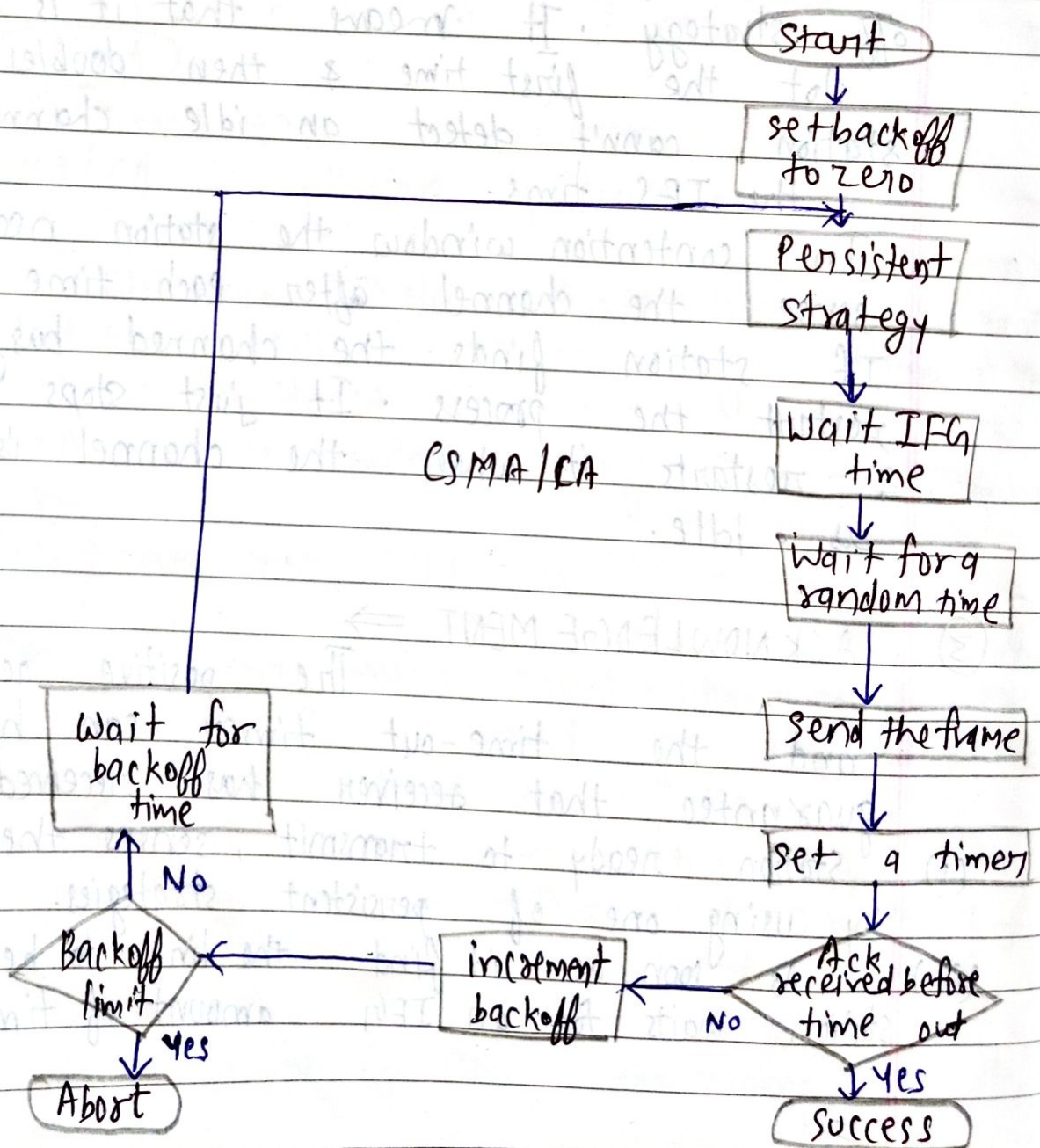
## ③ ACKNOWLEDGEMENT $\Rightarrow$

The positive acknowledgement and the time-out timer can help guarantee that receiver has received the frame.

- (i) Station ready to transmit, senses the line by line by using one of persistent strategies.
- (ii) As soon as it finds the line to be idle, the station waits for an IFS amount of time.

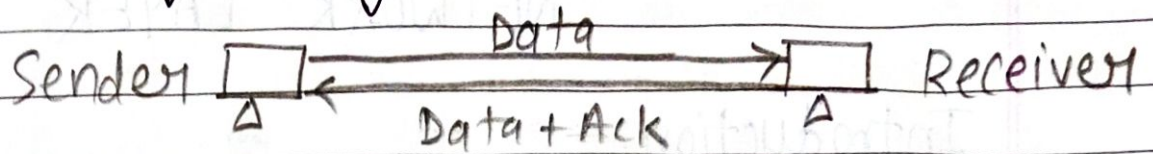


- (iii) If then waits for some random time & sends the frame.
- (iv) After sending the frame, it sets a timer and waits for the ack. from the receiver.
- (v) If the ack. is received before expiry of the timer, then the transmission is successful.
- (vi) But if transmitting station doesn't receive the expected ack. before the timer expiry then it increments the backoff parameter waits for the back off the time & resends the line.





Piggybacking Sliding window protocol  $\Rightarrow$



When a data frame arrives, instead of immediately sending a separate control frame, the receiver restrains itself and waits until the network layer passes it the next packet.

The ack. is attached to outgoing data frame (using ack field in frame header)

The technique of temporarily delaying outgoing ack. so that they can be attached with next outgoing data frame is known as piggybacking.

Advantage:—

It is better use of available channel bandwidth.

Control Token or Token passing  $\Rightarrow$  A station may transmit a

frame only when it has possession of the token and after it has transmitted the frame, it passes the token on, to allow station to access the transmission medium.

$\rightarrow$  It is a way of controlling access to a shared transmission medium.

$\rightarrow$  The techniques can be applied to both bus & ring network topologies.



## Chapter - ③ NETWORK LAYER

### Introduction:-

Layer 3 in the OSI model is called network layer. Network layer manages options ~~returning~~ ~~pretending~~ to host and network addressing, manages sub-networks and inter-networking. Network layer takes the responsibility for routing packets from source to destination within or outside a subnet. Two different subnet may have different addressing schemes or ~~and~~ non-compatible addressing types. Same with protocols, two different subnet may be operating on different protocols which are not compatible with each other. Network layer has the responsibility to route the packets from source to destination mapping different addressing schemes & protocols.

### Features of Network Layer ⇒

- (i) Quality of service management.
- (ii) Load balancing and link management.
- (iii) Security
- (iv) Inter-relation of different protocols & subnets with different schema.
- (v) Different logical network design over the physical network design.



- (vi) Layer 3 (VPN) and tunnels can be used to provide end to end dedicated connectivity.

### Functionalities of Network Layer $\Rightarrow$

- (i) Addressing Devices And Networks
- (ii) Populating Routing Tables OR Static Routes
- (iii) Inter-networking b/w two different Subnet
- (iv) Delivering Packets to destination with best efforts.
- (v) Provides connection oriented and connectionless mechanism.
- (vi) ~~De~~

### Design Issues in Network Layer $\Rightarrow$

- (i) Reliability :- Network channels and components may be unreliable, resulting in loss of bits while data transfer.
- (ii) Scalability :- The sizes of network are continuously increasing leading to congestion. Hence the design should be done so that the networks are scalable and can accommodate such additions and alterations.
- (iii) Addressing :-  
At the particular time ~~is~~ ~~no~~ innumerable message are re-transferred b/w large no. of computers. So a naming or addressing system should exist so that each layer can



identify a sender and receivers of each message

(iv) Error control:—

Layers need to agree upon common error detection & error correction methods. So as to protect data packets while they are transferred.

(v) Flow control:—

If the rate at which data is produced by the sender is higher than rate at which data is received by the receiver then there are chances of overflowing the receiver.

(vi) Security:—

A major factor of data comm is to depend it against threats like dropping and surprerititious alteration of messages.  
गुप्त सिस्टम

**Routing Algorithm:  $\Rightarrow$**

In order to transfer the packets from source to destination the network layer must determine the best route through which packets can be transmitted.

The routing protocol is a routing algorithm that provides the best path from source to destination. The best path is that path which has least cost path from source to destination.



## Classification of Routing algorithm:-

There are 2

type of algorithm

- (i) ~~Adapting~~ Routing Algorithm
- (ii) Non-adaptive Routing Algorithm

(i) Adaptive Routing Algorithm:-  $\rightarrow$  It is also known as dynamic Routing algorithm.

- $\rightarrow$  This algo. make the routing decision based on the topology and network traffic.
- $\rightarrow$  The main parameter related to this algorithm are hop, count, distance and estimated transit time.
- $\rightarrow$  An adaptive Routing algo. can be classified into 3 parts:-
  - (a) ~~See~~ Centralised Algorithm
  - (b) Isolation Algorithm
  - (c) Distributed Algorithm

(a) Centralised Algorithm:-

It is also known as global routing algorithm as it computes the least cost path b/w source & destination by using complete and global knowledge about the network. Link state algorithm is referred to as centralised algorithm since it is aware of cost of each link in the network.

(b) Isolation Algorithm:- It is an algo. that obtains the routing information by using local information rather than gathering info. from other nodes.



(c) Distributed Algorithm :- It is also known as decentralised algo. as it computes the least cost path b/w source & destination in an iterative and distributed manner.

(ii) Non-Adaptive Routing Algorithm  $\Rightarrow$

It is also known

as static routing algorithm.

When booting up the network the routing info. stores to the router.

This algorithm don't take the routing decision based on the network topology or network traffic.

The non-adaptive routing algorithm is of 2 types.

- (a) Flooding
- (b) Random walk.

(a) Flooding :- In case of flooding every incoming packet is sent to all the outgoing links except the one from it has been reached. The disadvantage of flooding is that node may contain several copies of a particular packet.

(b) Random walks :- In case of random walks, a packet sent by the node to one of its neighbors randomly. And advantage of using random walk is that it uses the alternative routes very efficiently.

A-3  
Q.1

Differentiate b/w adaptive & non-adaptive routing algorithms.



## IPv4 $\Rightarrow$

It is a connection less protocol used for packet switch network. It operates on a best effort delivery model in which neither delivery is guaranteed nor proper sequencing or avoidance of duplicate delivery is assured.

Internet protocol version 4 is the 4 revision of the internet protocol and a widely used protocol in data comm<sup>n</sup> over different kinds of network. IPv4 is basically used as ethernet. It provides a logical connection b/w network devices by providing identification for each device. There are many ways to configure IPv4 with all kind of devices including manual and automatic configuration depending on the network type.

IPv4 uses 32 bit 4 bytes addressing which gives  $2^{32}$  addresses. IPv4 addresses are written ~~return~~ in the dot decimal notation which comprises of 4 octets of the address expressed individually in decimal and separated by periods, for instance, ~~192~~ 192.168.105.

**IPv4 Datagram Header** :- Size of the header is 20 to 60 bytes



Version 4 bits	HLN 4 bits	Types of source 8 bits	Total length 16 bits			32bit=4bytes
Identification 16 bits			0 1bit	DF 1bit	DF 1bit	fragment offset 13 bits 4 byte
Time to leave 8 bits		Protocol 8 bits	Header checksum 16 bits			4 byte
Source IP 32 bits						4 byte
Destination IP 32 bits						4 byte
Option 0 to 40 bytes						
Data 32 bits						Data =
<div style="text-align: center;"> <span>←</span> <span style="margin: 0 10px;">32bits</span> <span>→</span> </div>						

Max Header  
= 60 bytes

Min Header  
= 20 bytes

## IPv6 ⇒

This was developed by internet engineering task force (IETF) to deal with the problem of IPv4 exhaustion. IPv6 is 128 bits address having an address space of  $2^{128}$  which is bigger than IPv4. In IPv6, we use colon hexa representation. There are 8 groups and each group represent 2 Bytes. IPv6 is better in terms of complexity and efficiency.

## IPv6 header format:-

Fixed Header	Version 4 Bits	Priority / Traffic class 8 bits	Flow Label (20 bits)	
	Payload length 16 bits	Next header 8 bits	Hop limit 8 bits	
	Source address (128 bits)			
	Destination (128 bits)			
	Extension headers !			



**Version :-** Indicates version of IP which contains bit sequence 0.110.

**Traffic class :-** It indicates class or priority of IPv6 packet which is similar to service field in IPv4 packet. It helps routers to handle the traffic based on priority of the packet.

Priority

Meaning

- |      |                               |
|------|-------------------------------|
| Zero | - No specific traffic.        |
| 1    | - Background data.            |
| 2    | - Unattended data traffic.    |
| 3    | - Reserved                    |
| 4    | - Attended bulk data traffic. |
| 5    | - Reserved                    |
| 6    | - Interactive traffic         |
| 7    | - Control Traffic             |

**Flow label :-** This field is used by source to label the packets belonging to the same flow in order to request special handling by intermediate IPv6 router such as non-default quality of service or real time service. While setting up flow label, source is also supposed to specify the life time of flow.

**Payload length :-** It is the 16 bits field indicates total size of the payload which tells routers about amount of information a particular packet can contain.



**Next Header:**— This indicates type of extension header immediately following the IPv6 header whereas in some cases it indicates the protocols contained within upper layer packet such as TCP & UDP.

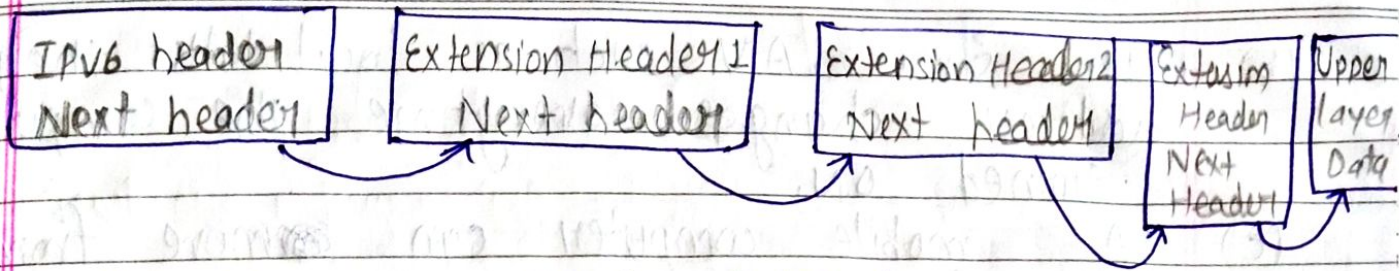
**Hop Limit:**— This is same as TTL in IPv4 packets. It indicates the max no. of intermediate nodes IPv6 packet is allowed to travel. Its value get decremented by 1 by each node that forwards the packet & packet is discarded if value decreament to 0.

**Source address:**— This is 128 bit IPv6 address of the original source of the packet.

**Destination Address:**— This indicates the IPv6 address of the final destination. All the intermediate nodes can use this information in order to correctly route the packet.

**Extension Headers:**— In order to rectifier the limitation of IPv4 option field, extension headers are introduced in IPv6. The Extension header mechanism is very important part of the IPv6 architecture. Next header field of IPv6 fixed header points to the first extension header and this points to the second extension header and so on.





A-3  
Q.2

Differentiate b/w IPv4 & IPv6

### Addressing Mapping $\Rightarrow$

An internet is made of a combination of physical network connected by inter-networking devices such as router. A packets starting from a source host may pass through several different physical network before finally reaching the destination host. The host and routers are recognised at the network level by their logic Ip address. However, packet pass through physical network to reach this host and routers. At the physical level the host & routers are recognised by their physical addresses.

A physical address is a local address it must be unique locally but it is not necessary to unique universally. It is called physical address because it is usually implemented in hardware. An example of a physical address is the 48 bit MAC address in the Ethernet protocol which is imprinted on the NIC installed in the host on Router.

### Limitation:-

- (1) A machine could change its NIC resulting in a new physical address.



- (b) In some LAN such as local talk the physical address changes everytime the computer is turned ON.
- (c) A mobile computer can ~~move~~ move from one physical network to another. Resulting in a change in its physical address.

### ARQ $\Rightarrow$ [Automatic Repeat ~~REQ~~uest]

It is the group of error control protocols for transmission of data over noisy or unreliable comm network. These protocol reside in the data link layer and in the transport layer of the OSI model. They are name so because they provide for automatic re-transmission of frames that are corrupted or lost during transmission. ARQ is also called +ve acknowledgement with pre-transmission (PAR). ARQ are used to provide reliable transmission over unreliable upper layer services. They are often used in global system for mobile comm.

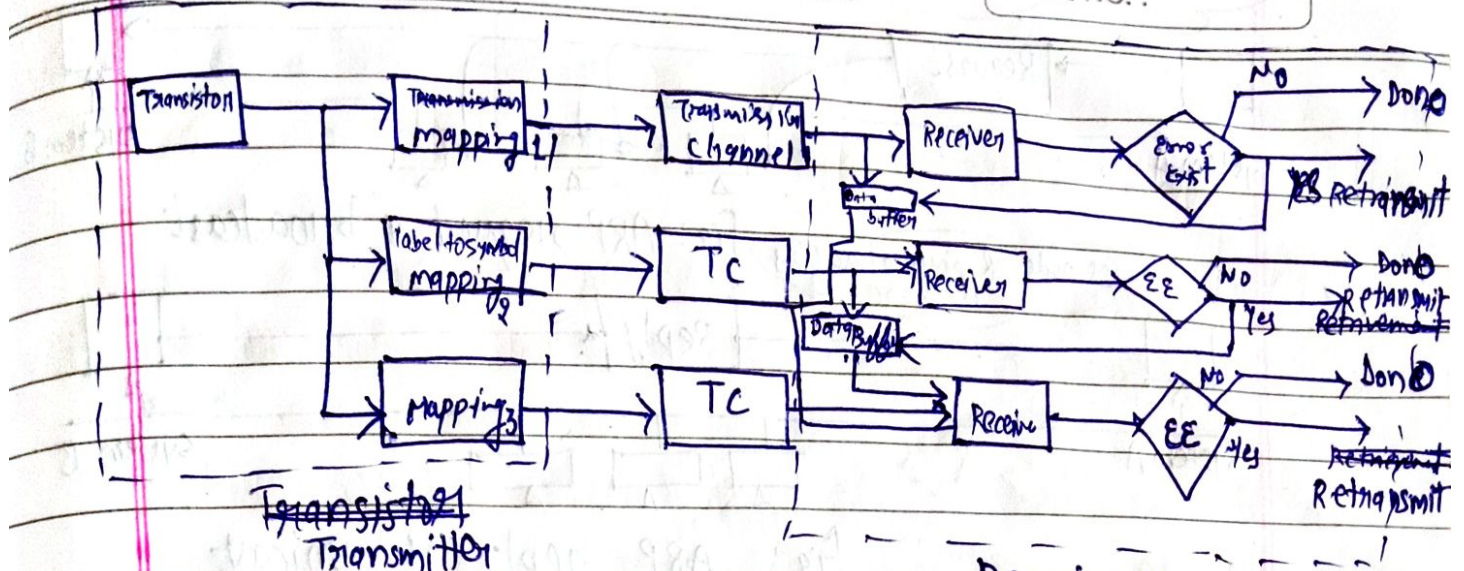
### Types of ARQ Protocol $\Rightarrow$

There are

3 type of ARQ in data link

- ① Stop wait ARQ
- ② Go-Back ARQ
- ③ Selective-repeat ARQ





Q-3 What is ARP and RARP in ~~addressing~~ addressing mapping.

ARP (Address Resolution Protocol)  $\Rightarrow$  It is a network layer protocol used to do address resolution or address mapping in TCP/IP protocols suite. The purpose of ARP is to point the MAC address of a device in a LAN for corresponding IP address which network application is trying to communicate.

Logical address/ IP address

$\downarrow$  (32 Bit)

ARP

$\downarrow$

Physical address/ MAC address  
(48 bit)

ARP associates an IP address with its physical address on a typical physical network such as LAN, each device on a link is identified by physical address i.e. usually imprinted on the NIC.



looking for physical address of a node

DATE : / /

PAGE NO. :

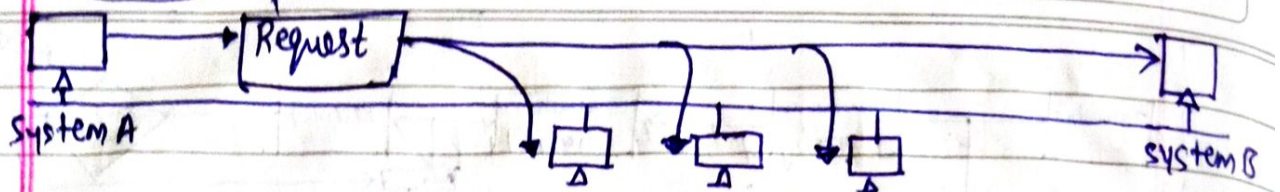


fig: ARP request a broadcast

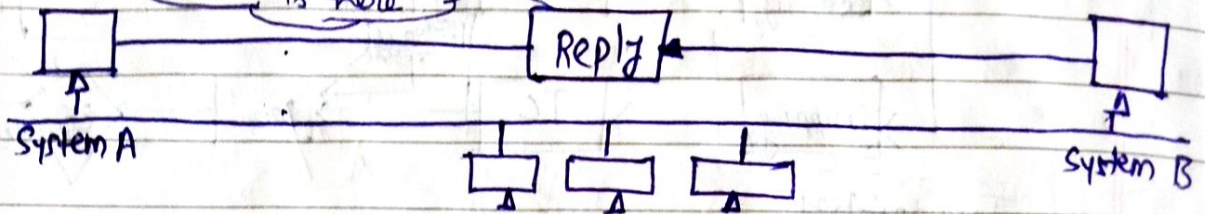


fig: ARP reply is unicast

## ARP Packet Format :-

- (i) H/w type [ 16 Bit ]  $\Rightarrow$  It defines type of network on which ARP is running
- (ii) Protocol type [ 16 Bit ]  $\Rightarrow$  It defines protocol using ARP.
- (iii) H/w length (8 Bit)  $\Rightarrow$  It defines length of physical address in bytes.
- (iv) Protocol length (8 Bit)  $\Rightarrow$  It defines length of IP address in bytes.
- (v) Operation (16 Bit)  $\Rightarrow$  It defines type of packet either it is request packet or reply packet.
- (vi) Sender hardware address (32 Bit)  $\Rightarrow$  It defines physical address of sender. [ for ethernet 6 Byte ]



logical address  
↓  
ARP  
↓  
physical address

logical address  
↑  
RARP  
↑  
physical address

DATE: / /

PAGE NO.:

(vii) Sender logical address (32 Bit)  $\Rightarrow$  It defines IP address of sender [For IPv4

It is 4 Bytes]

(viii) Target h/w address (32 Bit)  $\Rightarrow$  It defines physical address for target.

For ARP request message this field is all zeros because sender doesn't know physical address of target.

(ix) Target logical address (32 Bit)  $\Rightarrow$  It defines logical address of target

Hardware Type		Protocol Type
Hardware length	Protocol length	Operation
		Request 1, Reply 2
		Sender H/w address
		Sender logical Address
		Target H/w address
		Target logical Address

Congestion Control  $\Rightarrow$

Congestion:— A state occurring in network layer when the message traffic is so heavy that it slows down network response time.

Effect of Congestion  $\rightarrow$

(i) As delay increases, performance decreases.

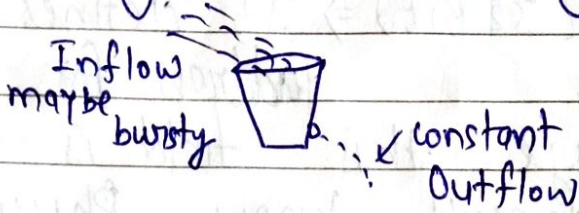
(ii) If delay increase, retransmission occurs & making situation



hose.

## ⇒ Congestion control algorithms:-

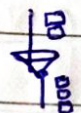
### ① Leaky Bucket Algorithm ⇒



Steps for algo:-

- (i) When host wants to send packet, packet is thrown into bucket.
- (ii) The bucket leaks at constant rate, meaning the network interface transmits packets at constant rate.
- (iii) Bursty traffic is converted to a uniform traffic by leaky bucket.
- (iv) In practice the bucket is finite queue that outputs at finite rate.

### ② Token Bucket Algorithm:-



after

traffic we need flexible algo. To deal with Bursty so that data is not lost.

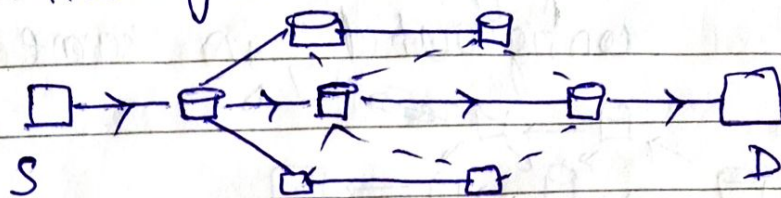
Steps for algo:-

- (i) In regular intervals tokens are thrown into bucket.
- (ii) The bucket has maximum capacity  $f$ .
- (iii) If there is ready packet, a token is removed from the bucket, and packet is sent.
- (iv) If there is no token in bucket, the packet can't be sent.



**Routing:**— When a device has multiple path to reach destination, it always selects one path by preferring it over others. This selection process is termed as Routing.

**Unicast Routing**  $\Rightarrow$



Most of traffic on internet & intranets known as unicast data. Routing unicast data over the internet is called unicast routing. It is simplest form of routing because the destination is known.

**Broadcast Routing**  $\Rightarrow$  By default, broadcast packets are not routed & forwarded by routers on network. Routers create broadcast domains. But it can be configured to forward broadcasts in some special cases. A broadcast message is destined to all network devices.

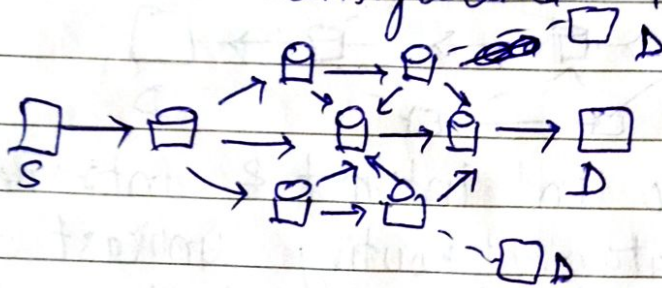
There are 2 ways (algorithms) for BC R  $\Rightarrow$

- (i) A router creates a data packet and then sends it to each host one by one. In this case, the router creates multiple copies of single data packet with different destination addresses. All packets are sent as unicast. But because they are sent to all, it simulates as if router is broadcasting.



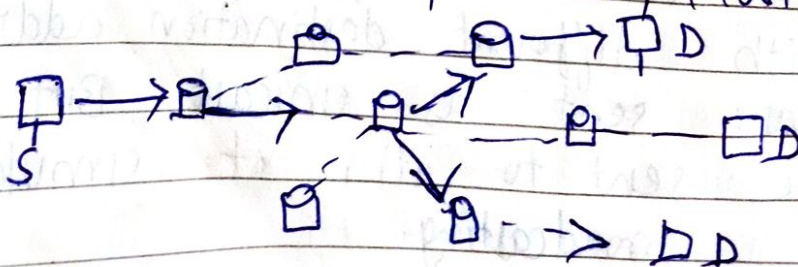
This method consumes lots of bandwidth & router must destination address of each node.

(2.) when router receive a packet that is to be broadcasted, it simply floods these packets out of all interfaces. All routers are configured in same way.



**Multicast Broadcasting:-** It is special case of broadcast routing with significance difference & challenges. The broadcast routing is used to send packet to all nodes even if they don't want it. But in multicast routing, the data is sent to only nodes which wants to receive the packets.

The routers must know that there are nodes, which wish to receive multicast packets then only it should forward. Multicast routing works spanning tree protocol to avoid looping. Multicast routing also uses reverse path forwarding technique, to detect & discard duplicates & loops.  
Eg - ICMP, PIM, DVMRP, MOSPF, MBGP. etc. protocols





Q.1 Define the element of Transport Layer protocol.

Ans- The elements of transport protocols are:

- (i) Addressing
- (ii) Connection Establishment
- (iii) Connection Release
- (iv) Error control & flow control
- (v) Multiplexing

(i) Addressing: - When an application process wishes to set up a connection to remote application process, it must satisfy which one to connect to. The method normally used is to define transport addresses to which processes can listen for connection requests. In internet, these endpoints are called ports.

There are two types of access points

(i) TSAP (Transport Service access point) to mean a specific endpoint in the transport layer.

(ii) The analogous endpoints in network layer are not surprisingly called NSAP. IP addresses are examples of NSAP.

(ii) Connection Establishment: - With packet lifetimes bounded, it is possible to devise a fool proof way to establish connection safely.

Packet lifetime can be bounded to known maximum using one of following techniques:

- Restricted subnet design
- Putting a hop counter in each packet.



→ Time stamping in each packet.  
Using a 3-way handshake, a connection can be established. This establishment protocol doesn't require both sides to begin sending with same sequence no.

### ③ Connection Release:—

A connection is released using either asymmetric or symmetric variant. But, the improved protocol for releasing a connection is a 3-way handshake protocol.

There are 2 styles of terminating a connection:

- (i) Asymmetric release
- (ii) Symmetric release

Asymmetric release is the way the telephone system work: when one party hang up, the connection is broken.

Symmetric release treats the connection as two separate unidirectional connections and requires each one to be released separately.

### ④ Flow control & Buffering:—

Flow control is done by having a sliding window on each connection to keep a fast transmitter from over running a slow receiver. Buffering must be done by the sender, if networks service is unreliable.



The sender buffers all the TPDU's sent to receiver.  
The buffer size varies for different TPDU's.

They are:

- (a) Chained Fixed size Buffers
- (b) Chained Variable size Buffers
- (c) One large circular Buffer per connection.

### (5) Multiplexing: -

In networks that use virtual circuits within the subnet, each open connection consumes some table space in routers for entire duration of connections. If buffers are dedicated to the virtual circuit in each router as well, a user who left a terminal logged into a remote machine, there is need for multiplexing.

There are 2 kind of multiplexing: -

- (i) UPWARD Multiplexing
- (ii) DOWNWARD Multiplexing



Q.1 What is FTP? Define FTP protocols.

Ans -

FTP stands for file transfer protocol. FTP is a standard IP provided by TCP/IP used to transmitted the file from one host to another. It is mainly used for transferring the web page files from their creator to the computer that act as a server for other computers on the internet. It is also used for downloading the files to computer from other servers.

As a user, we can use FTP with simple command line interface or with a commercial program that offers a graphical user interface.

Q.2 What is E-mail & Explain with help of example

Ans - The e-mail system consist of two subsystems. They are:-

- (i) User Agents, which allow people to read and send e-mail.
- (ii) Message Transfer Agents, which move messages from source to destination.

→ Email systems support 5 basic functions:-

- (a) Composition
- (b) Transfer
- (c) Reporting
- (d) Displaying
- (e) Disposition



Example of an e-mail is an happy birthday message a person . Sends from their Yahoo account to their mom at her gmail account.

Q.3) How many types of protocols used in Email?

A- The commonly used protocols are IMAP, POP3, SMTP and Exchange these are ~~four~~ 3 protocol types one would come across while accessing an e-mail client.

(i) IMAP:— [Internet mail Access protocol]

POP3 normally downloads all stored messages at each contact, the result is that the user's e-mail quickly gets spread over multiple machines, more or less at random; some of them not even the user's.

IMAP assumes that all e-mail will remain on the server indefinitely in multiple mailboxes. IMAP provides extensive mechanisms for reading message or even parts of messages, a feature useful when using a slow modem to read the text part of multipart message with large audio and video attachment.

(ii) POP3 :- POP3 begins when user starts the mail reader. The mail reader calls up the

ISP and establishes a TCP connection with message transfer agent at port 110.

Once the connection has been established, the POP3 protocol goes through 3 states in sequence:



- (i) Authorization
- (ii) Transactions
- (iii) Update

(iii) SMTP :- SMTP is simple ASCII protocol. After establishing the TCP connection to port 25, the sending machine, operating as the client, waits for the receiving machine, operating as the server, to talk first. The server starts by sending a line of text giving its identity & telling whether it is prepared to receive mail.

Q(4) What is WWW? Explain its working method.

Ans- The world wide web (WWW) is an architectural framework for accessing linked documents spread out over millions of machines all over the internet. WWW began in 1989 at CERN, the European center for nuclear research. WWW which is known as a web is collection of websites or web pages stored in web servers and connected to local computers through the internet.

Working method:-

The WWW commonly referred to as the web is a system of interlinked, hypertext document accessed through the internet.



It enable the retrieval & display of text and media to your computer. The WWW was developed by Tim Berners in 1991.

Q.5 what is DNS? define type of DNS and also define zones in DNS.

Ans - DNS [Domain Name System] :- This primarily used for mapping host and e-mail destinations to IP addresses but can also be used other purposes. DNS is defined in RFCs 1034 & 1035.

DNS defines a domain namespace which specifies top level domain (such as '.com'), second level domain (such as 'acme.com') and lower level domain also called subdomain (such as 'support.acme.com'). Each of these levels can be a DNS zone.

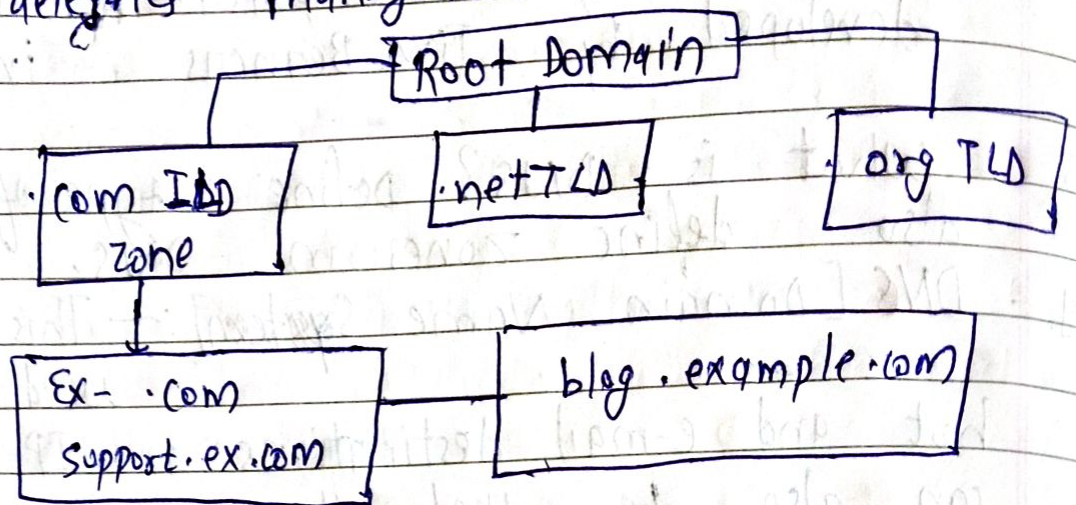
DNS Root Zone :- The root of DNS system represented by dot at end of the domain name.

TLD zone :- There is a DNS zone for each top level domain (such as '.com', '.org' or country code like '.co.uk'). There are currently over 1500 top level domain most top level domain are managed by IANA.

Domain zone - Second level domain like 'ns1.com' are defined as separate DNS zones, operated by individual or organisation.



Organization can run own DNS name server or delegates management to an external.



Secondary DNS zone:- DNS servers can be deployed in master/slave topology, where secondary DNS server holds a read only copy. primary DNS server holds the master zone file and secondary server constitutes an identical secondary zone.

DNS Zone Types  $\Rightarrow$  There are 2 types of zone files.

$\rightarrow$  DNS master file which authoritatively describes a zone

$\rightarrow$  DNS cache file which lists the contents of DNS cache - This is only a copy of the authoritative DNS zone.

DNS zone Records :-

In a zone file, each line represents a DNS resource record RR. A record is made up of the following fields



name	ttl	Records class	Record type	Record data
------	-----	------------------	----------------	----------------

- Name is a alphanumeric identities of DNS record
- Time to live (TTL) specifies how long the record should be kept in the local cache of DNS client.
- Record class ~~identi~~ indicates the namespace typically IN, which is the internet namespace.
- Record data has more ~~img~~ element, depending the record type, separated by a whitespace.

—————X—————

Subscribe

ER SAHIL KA GYAN