Name :- SAKET SUMAN

Roll :- 1809169

Branch :- C.S.E

Sem :- 6th

Sub :- C.N

Sess :- 2018-2022

Module 1

I Data Communication

Data Communication are the exchange of data between two devices via some form of transformission medium such as a wire cable for data communication to occur, the communication devica must be part of a Communication System made up of a Combination of Hardware (physical equipment) and Software (program) The effectiveness of a data Communication System depends on four fundamental characteristics delivery, accuracy, timelenes and jitter

1) Delivery:-

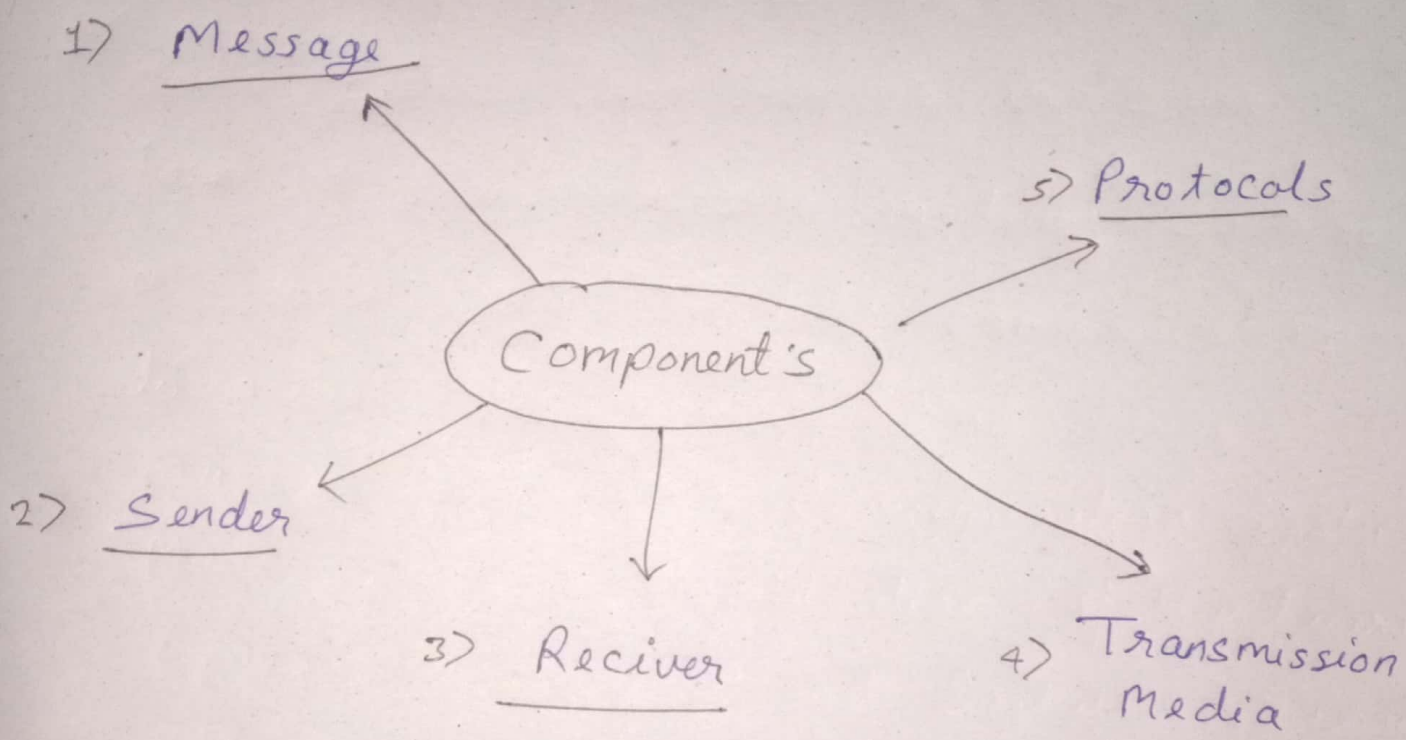
1) The System must deliver data is to corred destination. Data must be recived by the interded devica or uses

2) Accuracy - The System Must deliver the data accurately. Data must be recived by the intended deviver Been altred in transmission and left Uncorrected are Un Usable.

3 Timeliness :- The System Must delivered Data in a timely manner and in a Same way as it is produced in the Case of audio and video.
This is called time transmission.

4 Jitlers :- It reffers to the Variations in the packet arrival time. It is the Uneven delay in the delevery of audio or a Video packet.

Component's



1) Message :- The Message is the Information data to be Communicated popular form of Information include text, Number, picture, audio, & video, etc

2) Sender - Is the device that Send's the data Message. It Can be a Computer, Mobile, handset, video camera so on etc devices.

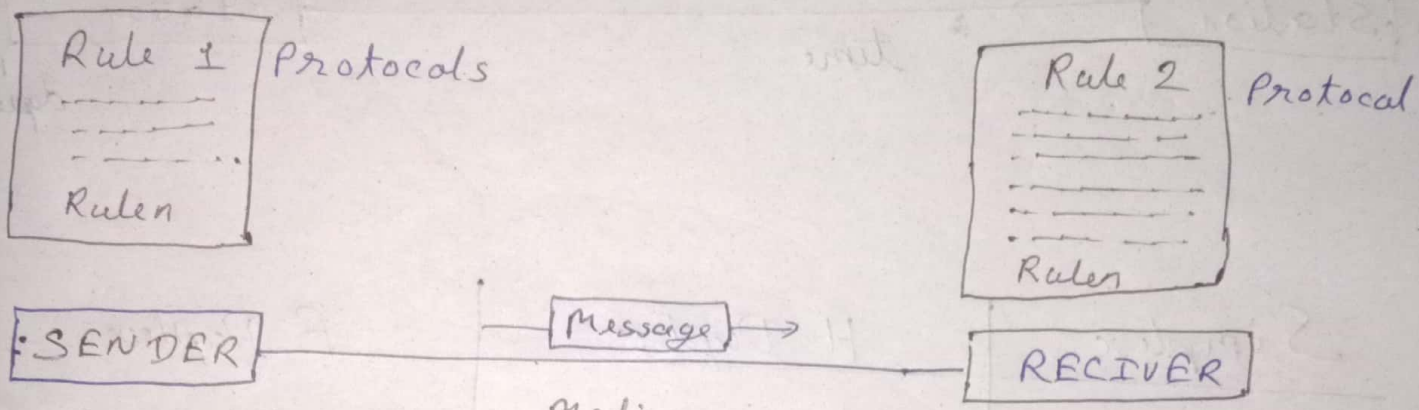
3) Reciver: - Is the device that receved the Message
Eg:- telephone handset, television etc

4) Transmission Media :- Is the physical path by which a message travel from Sender to reciver
Eg: twisted pair wire, Coaxial wire radio wave etc.

5) Protocals :- Is a set of rules that given data Communication. It repersent the agrement b/w Communication device. W/o prolocol a Network May be connected but it cant Communicate with each other

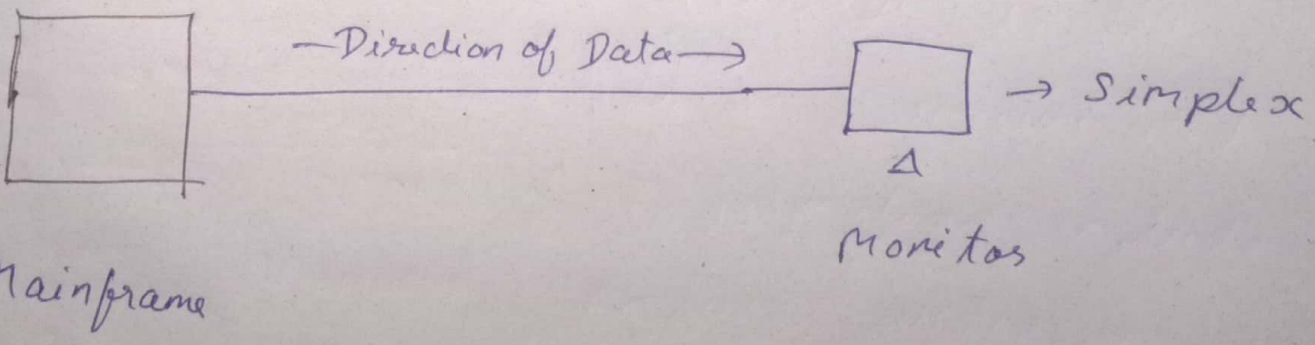
Data Repersentation

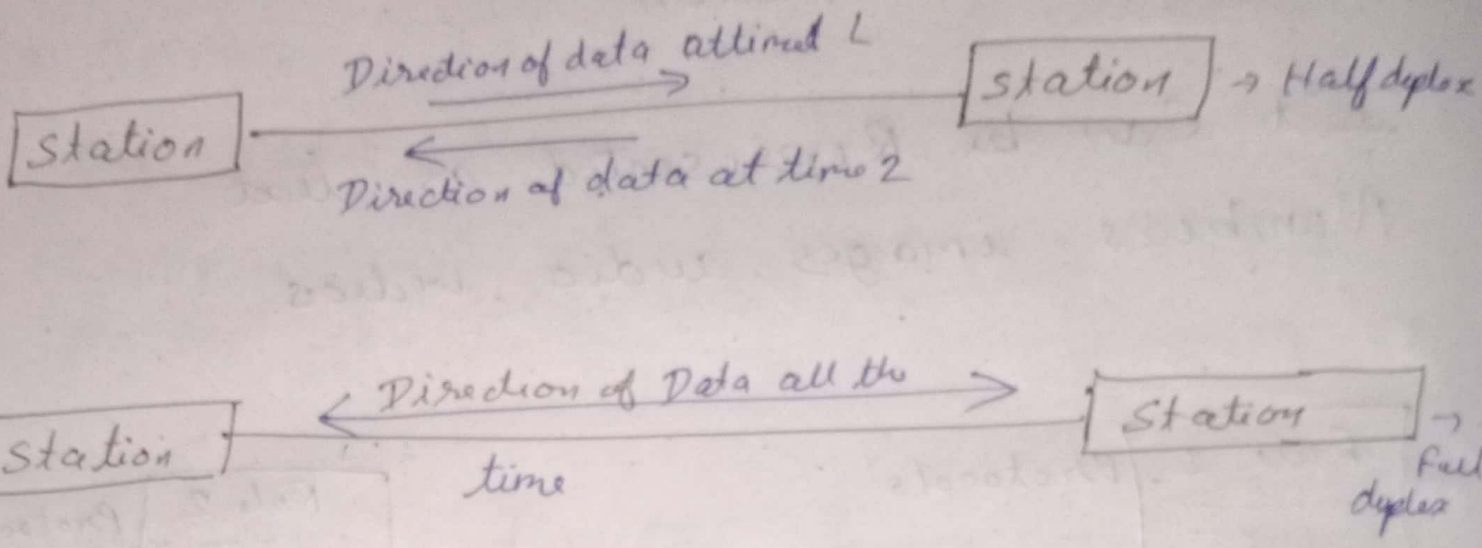
It Can be Represented as text Numberis, images, audio, videos.



Data Flow

Communication between two devices can be Simplex, half duplex or full duplex





Simplex	H. Duplex	F. Duplex
Key Board	Walki Talkies	Teliphone
Monitors	Radios	Network

Types of Topology

There are 5 types of topology in Computer Networks.

1) Mesh Topology
2) Star Toplogy
3) Bus Toplogy
4) Ring Topology
5) Hybrid Topology

1 Mesh Topology

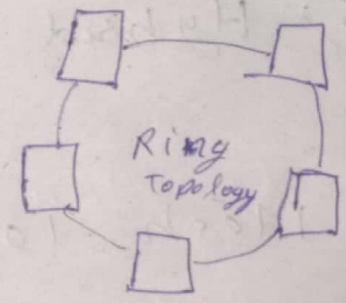
In Mesh topology each device is Connected to every other device on the Network through a dedicated point-to-point link.

Number of links in a Mesh topology of N devices would be

$$\frac{n(n-1)}{2}$$

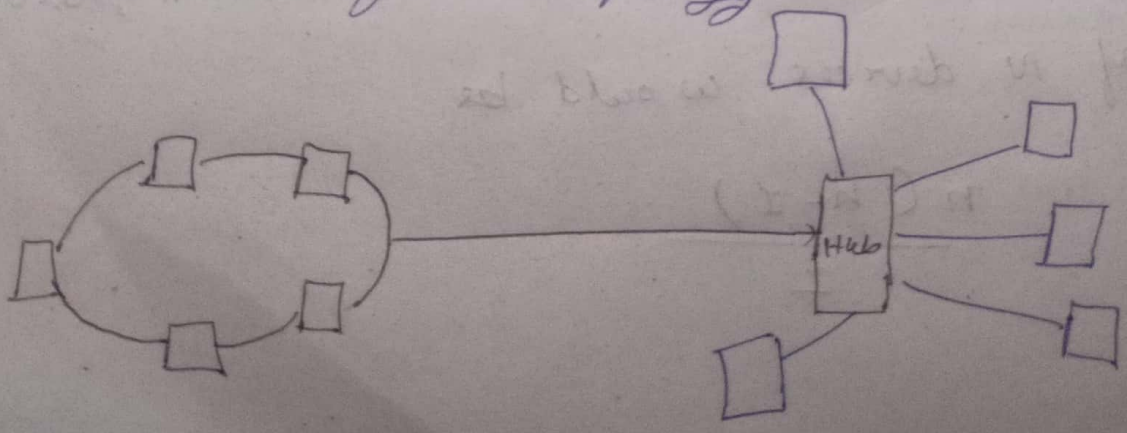
Ring Topology:

In Ring topology each device is connected with two devices on either side of it. There are two dedicated point to point links a device has with the devices on other side. This structure is known as Ring thus it is called Ring topology



Hybrid Topology

A combination of two or more Topology is known as Hybrid topology. For eg a Combination of Star and Mesh Topology is known as Hybrid Topology



Standard's

Standard's are the Set of Rules of Data Communication that are Needed for exchange of Information among devices.

It is important to follow Standard which are created by various Standard Organization like

IEEE, ISO, ANSI etc.

Standard are of Two types

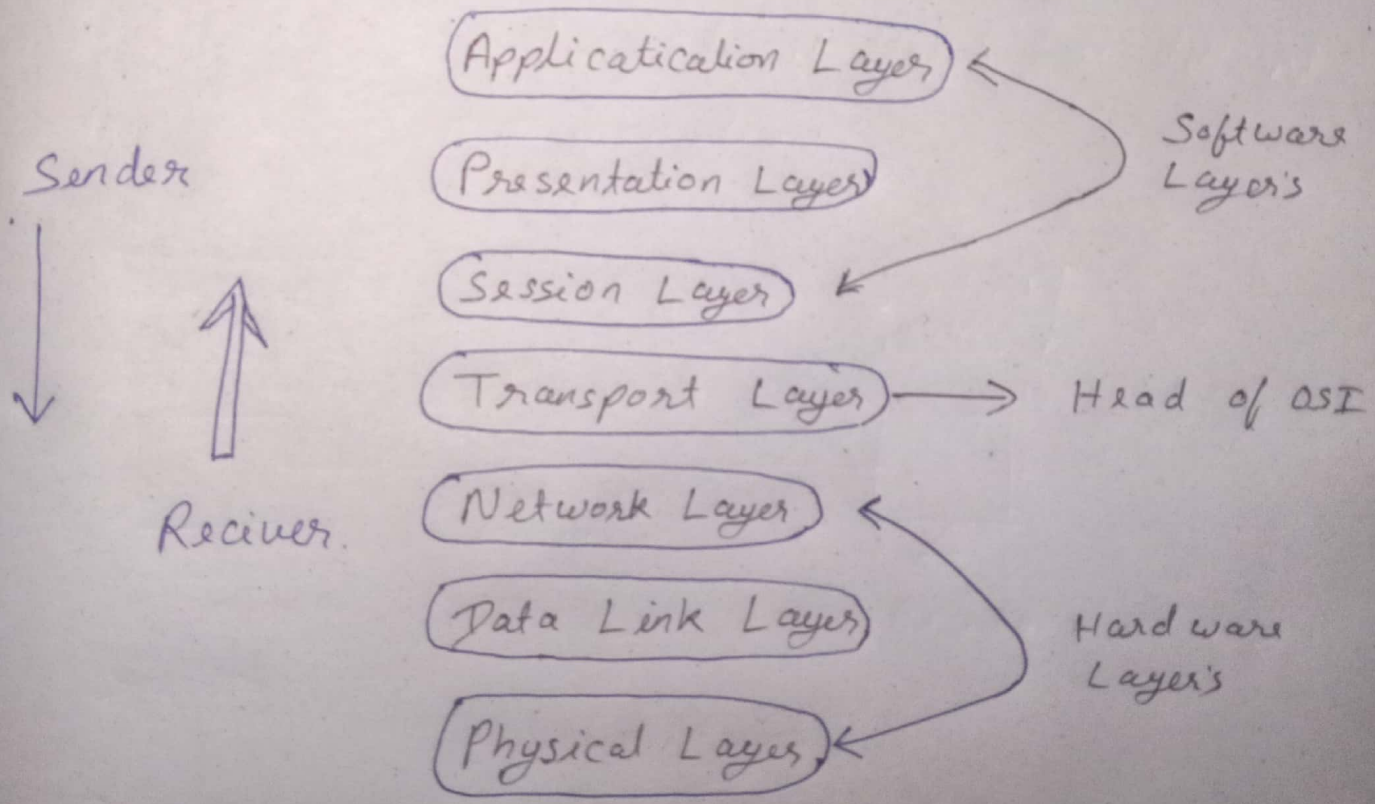
- De facto Standard
- De Jure Standard

OSI MODEL

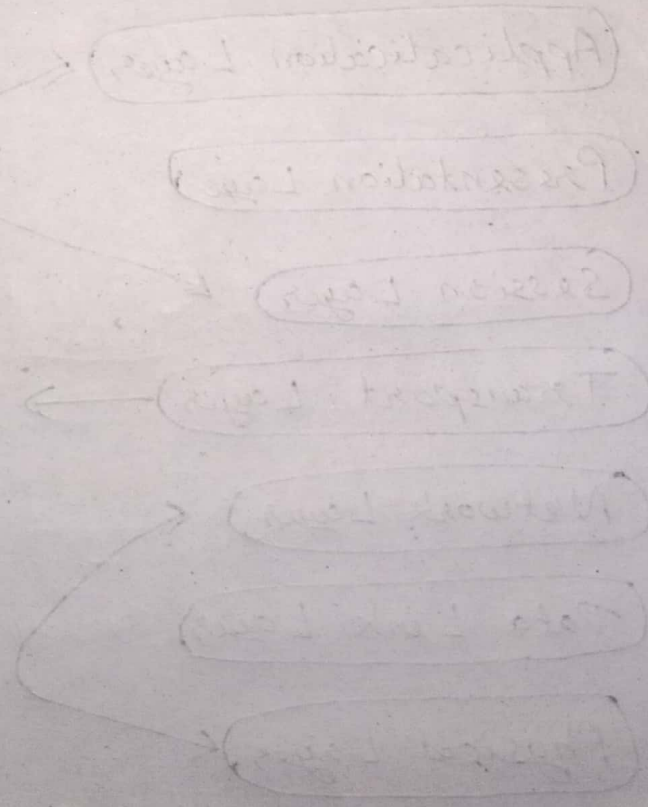
OSI Stands for Open System Inter-connection.

It has been developed by ISO

It is a 7 layer architecture with each layer Have Specific functionality to perform. All 7 layer's work Collaboratively to transmit the data from one person to another



- In OSI Model the transpart layer is only Connection Oriented
- In the OSI Model Dala link layer and physical are seprate layer's.
- Session and persentation layer's are a part of OSI Model
- The Min Size of OSI Model is 5 bytes.



TRANSMISSION MEDIA

It is a Communication Channel that Carrier the information from the Sender to the Reciver.

Two typer of Transmission Media

1 Guided

2 Unguided.

1) There are diffrent type of GUIDED MEDIA

a) Twisted pair Cable :-

Have been around for a long time They are inverted for Voice transmission It is widely Used transmission Medium In a Networking because its lighter Cheaper More flexiblity. easy to Install & provided greater speed than Coaxial cable.

b) Coaxial Cable:-

Have a Central copper Conductor Surrounded by an insulating Layer, a Conducting Shield the outer most Plastic Sheath.

- Mostly Used are RG-59, RG-6

c) Optical Fiber's

- Use light Waves for transmission Crosstalk, EMO & attenuation aren't issues with optical fibre These Cable are well suited for Voice data & video transmission
- Most Serve of all cable media

2) Wireless or Unguided

The features of Unguided Media are that the signals get broad cast w/o any guided Medium through air is less Secure.

There are 3 types of this

Radio waves

Infrared

Microwaves

Advantages:-

- They are Useful in wireless remote accessing Methods
- N/w Can be expanded w/o distribution the Current issues.

Disadv:-

- Potential Security issue
- They have limited Speed Compared to guided Transmission Media

MODULE - 2

Wired LAN:-

Local Area Network- Wired LAN. is a Computer Network that is designed for limited geographical area such as Building or Campus.

- Wired Lan has Six essential Components to function

- Cable Connectors In wired Network the most common form of connector is the RJ45

6 essential Components to Wired LAN

- Network Adapter :-

A Network Adapter is Usally the Only Component within a Compater for interfacing or Connecting with a Network. A Network Adapter for wired Network has an RJ-45 port that Uses twisted or Untwisted pair cable for Network Connectivity

- Network Medium

Wired Networks Need Cable. The Most Common form of Cable Used in Networks is called Unshielded Twisted Pair

- Cable Connection

In wired Networks the Most Common form of Connector is RJ45 Every computer with Networking

capabilities has an RJ45 port. This is sometimes called a Network port or an Ethernet port.

- Power Supply

Both wired and wireless Network's Need a power Supply. A wireless Network Use the Current to generate Radio Waves. A cabled Network Send's data interpreted as an elecdric pulse

- Hub / switch / Router - there are the connecting devices

Software :- Is the intelligence that Causes all of the Component's to function together. The Most popular

Network Software today Uses what is Known as the TCP/IP protocol Suite or Stack.

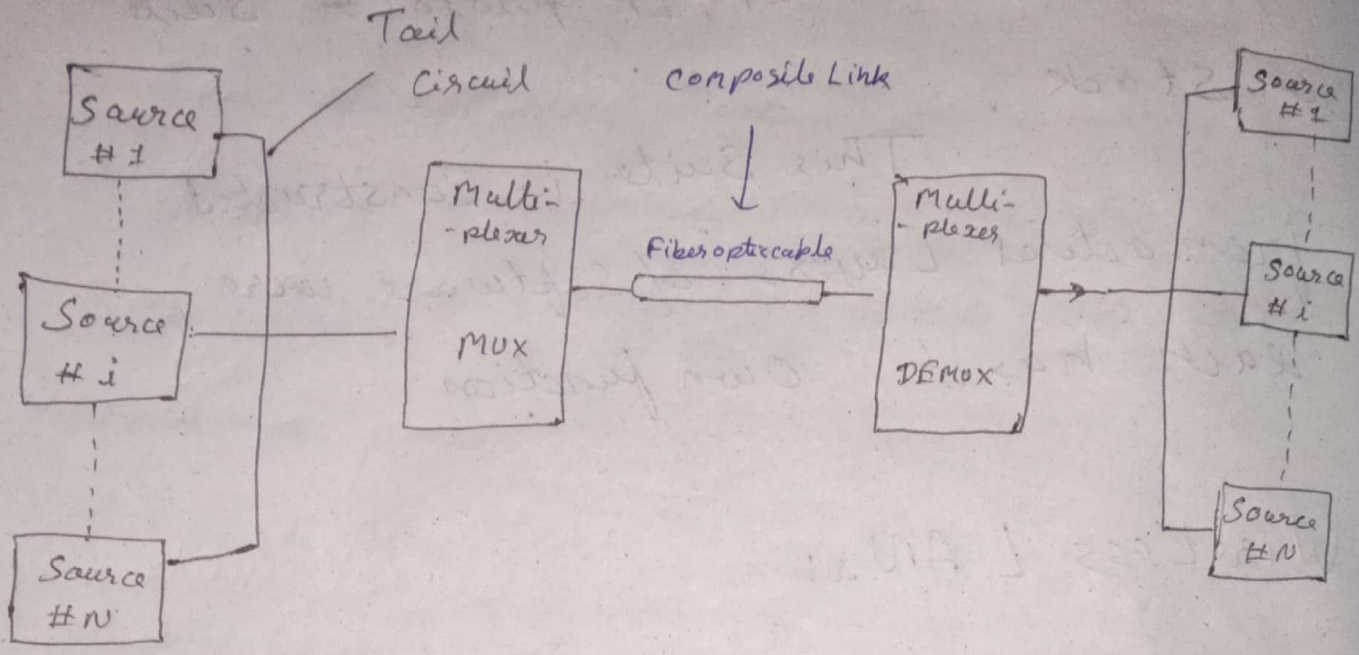
This Suite is Constructed from actual Layer's of Software, were each has its Own function

WireLess LAN's: -

These are the wireless Compatus Networks that use High frequency Ratio. Waves insted of Cables. for Connecting the devices within a limited area forming LAN (Local area Network) User's Connected by wireless LAN's Can Move around within the Limited area such as Home, School campus, office Building railway platform etc.

Most Lan Used are Based upon the Standard IEEE 802.11 Standard Wifi

Band with Utilization Multiplexing



Band width Utilization is the Use of avilable Band with to achieve goals. Efficiency Can be achived by Using Multiplexing Privacy and antijamming Can be achived By Using Spreading..

Mutliplexing is the set of techniques that allows the simultaneous transmission of multiple signal across a single data link In a multiplexed system, n lines share the Bandwidth of one link. The word link refers to the portion of a link that carries a transmission

There are three Basic Multiplexing Techniques:

(i) Frequency division multiplexing.
(ii) Wavelength division multiplexing
(iii) Time-division Multiplexing

The first two are techniques designed for analog signal, the third, for digital signal.

(i) Frequency div Multiplexing (FDM)

It is an analog technique that can be applied when the Bandwidth of a link (in Hertz) is greater than the combined bandwidth of the signal to be transmitted

(ii) Wave length-division Multiplexing (WDM)

Is designed to use the high bandwidth capability of optic-fiber cable WDM is an Analog multiplexing Technique to combine optical signals

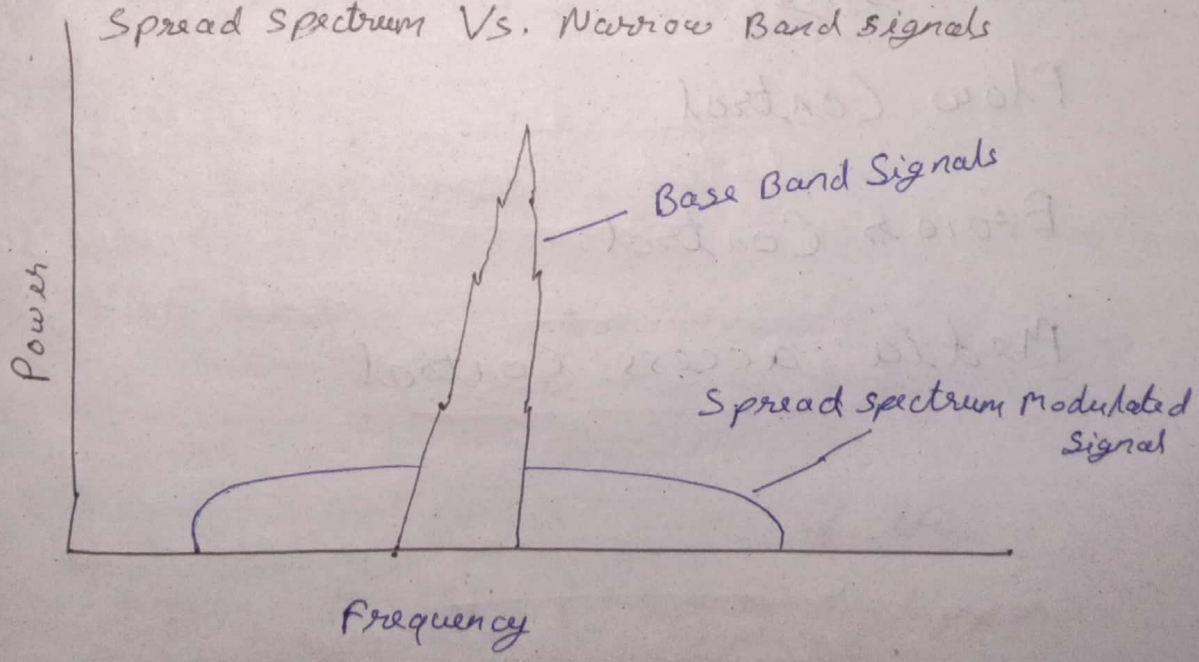
(iii) Time-division Multiplexing (TDM)

Is a digital process that allows several connections to share the high Bandwidth of a link. TDM is a digital Multiplexing Technique for Combining several Low-Rates Channels into one High-rate one.

Spread Spectrum

What is Spread spectrum.

Spread spectrum a means of Signal Modulation In which the Signal frequency is spread over a very wide Band width. The Band Spread is achived by means of a Code which is independent of data. A Code synchronized reception at the reciver is used for dispreading the Subsequnt data recovery.



Module - 3

Data link layer:

A data link layer, transform-layer a Raw transmission facility, to a line Responsible for Node-to-Node Communication

- Specific Responsibilities

framing

Addressing

Flow Control

Error Control

Media access Control

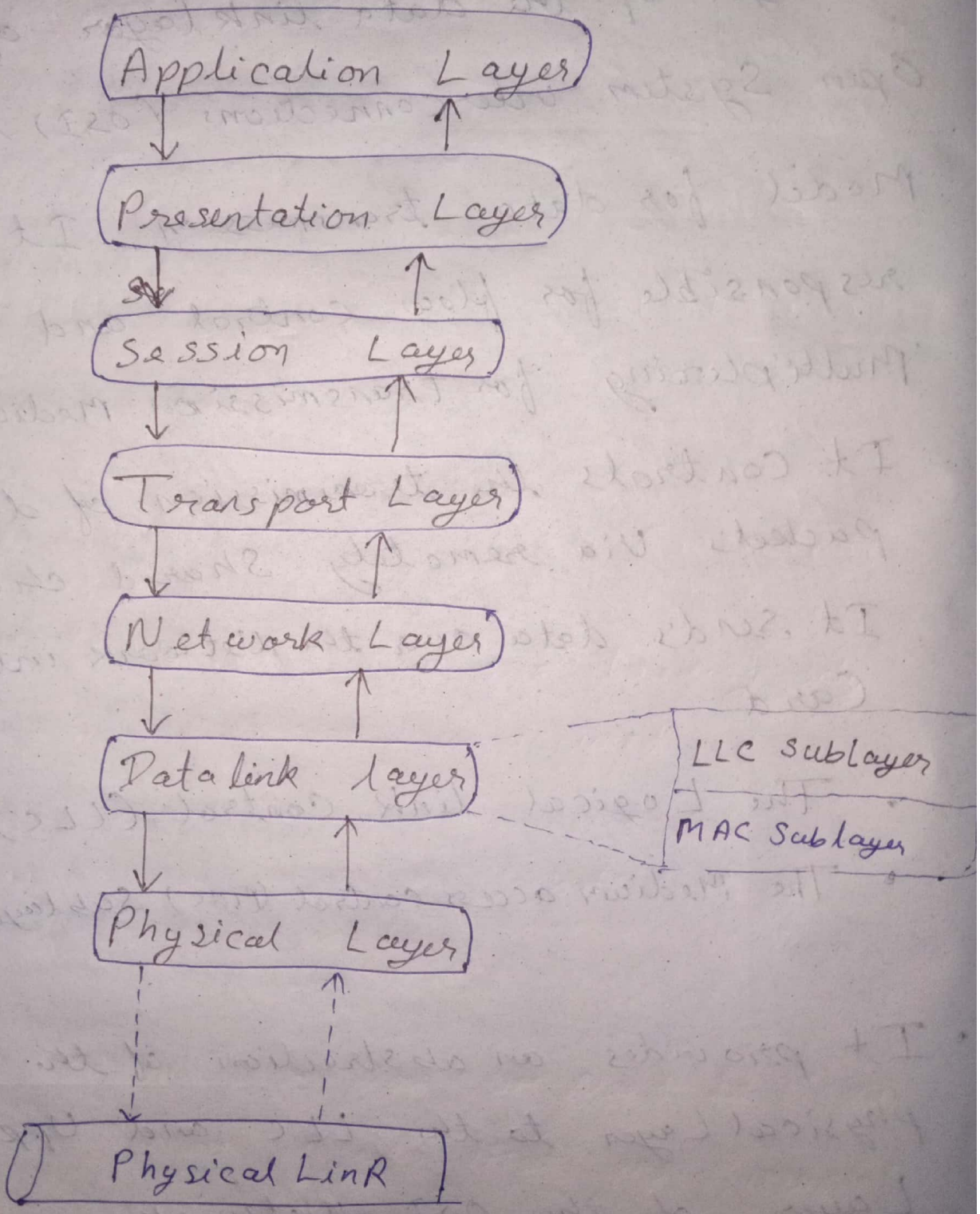
Medium Access Sub Layer:

The Medium access Control (MAC) is a Sub layer of the data link layer of the Open System interconnections (OSI) reference Model for data transmission. It is responsible for flow control and Multiplexing for transmission Medium It Controls the transmission of data packets via remotely Shared channels It Send's data over the Network interface Card

- The Logical link Control (LLC) sublayer
- The Medium access control (MAC) Sublayer

- It provides an abstraction of the physical Layer to the LLC and Upper Layer of the OSI Network
- It is Responsible for encapsulating frames

So that they are Suitable for transmission via the physical Medium



ERROR DETECTION AND CORRECTION

Data Can be Corrupted during Transmission Some application require that errors to be deteded and Corrected.

Types of error

Whenever bits flow from one point to another, they are subjected to Unpredictable changes because of interference.

a) Single Bit error

The term Single Bit error means that only 1 bit of given data Unit is changed from 1 to 0 or 0 to 1

Ex:-

0001010 ⟶ 0011010

Sender Reciver.

Brust error:-

It means two or more than two Bit's in one data Unit have changed

Eg:-

Sender	Reciver
0101101110	0100100111

Error Detection Vs Error Correction

- In error detection, we are looking only to see of any error has occured
- Eighter yes or No
- Instrested only in yes or No but Not is No of error's occured

- In Error Correction we Need to Know exact Number of bits that are corrupted and Most Importantly their Location in the msg.

BLOCK CODING

- In Block Coding, we divide msg into Block each of k bits called datawords We add redundant bits to each Block to make Length $n = k + r$
- The Resulting n-bits block are called Code words

Datawords → k Combination = 2^k

Code word → n " " = 2^n

Hamming Distance.

Hamming Distance is a metric for comparing Two binary bits data string While Comparing two binary bits string of equal length, Hamming distance is the Number of bit position in which the two Bits are different.

The hamming distance between two strings a and b is denoted as d(a, b) it perform XOR operation (a⊕b)

Module 4

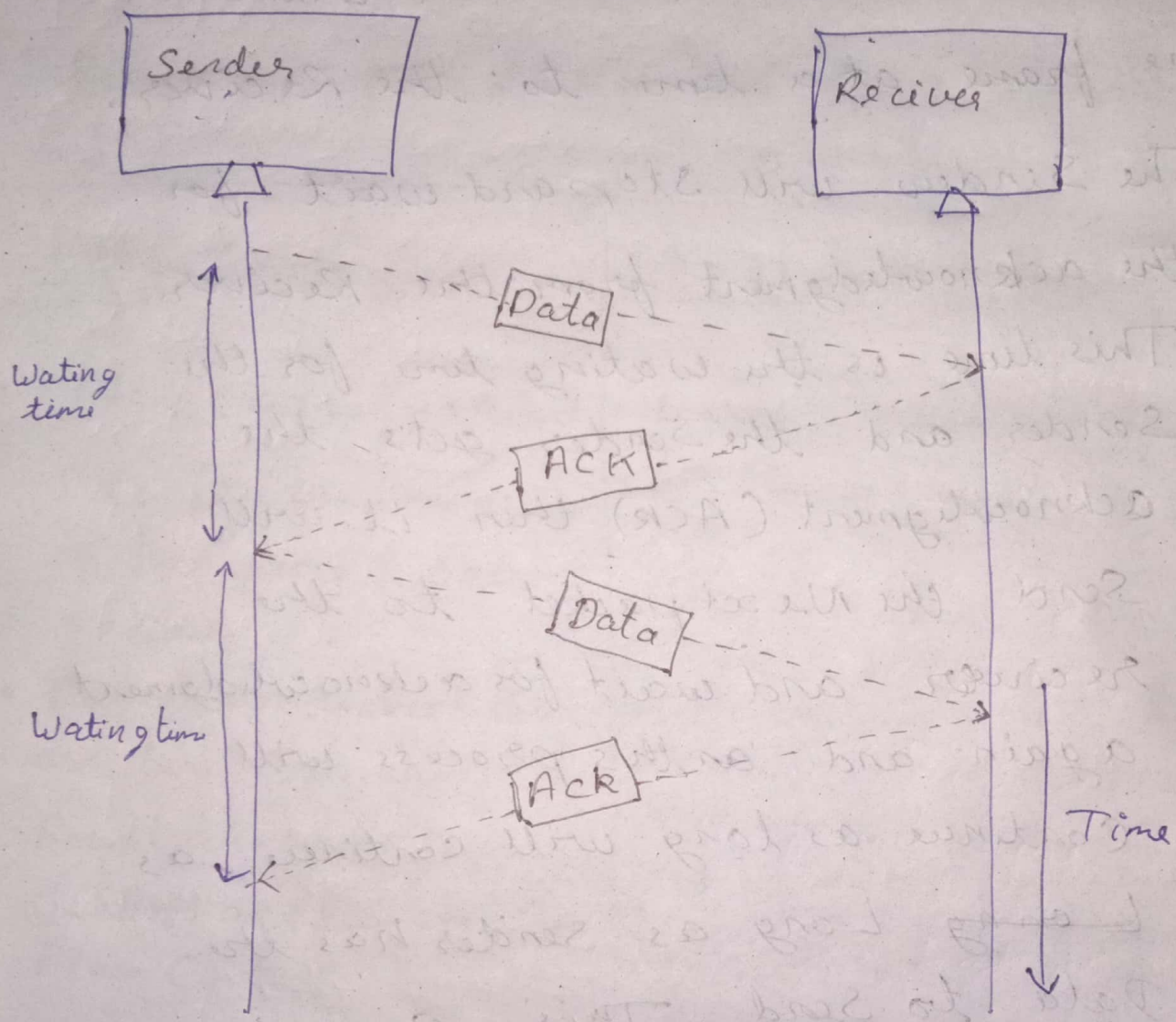
Flow Control and Error Control protocols

- Difference b/w Flow Control and Error Control

Flow Control	Error Control
• Flow Control is Meant only for the transmission of data from sender to Reciver • For Flow Control there are two Approches. Feedback-based flow Control and Rate-Based Flow Control • It prevents the loss of data and avoid over Running of recive buffers • Example for Flow Control Technique are:- Stop & Wait Protocol and sliding Window protocol	• Error Control is Meant for the transmission of error free data from Sender to Reciver • To detect error:- Approches are used CheckSum, Cyclic, Redundancy and parity checking • To Correct error in data the approches are:- Hamming Code, Binary Convolution Codes Reed-Solomon code, Low-Density parity Check Code • It is Used to detect and Carrect the error occured in the code Example:- of Error Control Technique are:- Stop & Wait ARQ and sliding window ARQ

Stop and Wait protocol

It is the Simplest flow control Method. In this the Sender will send one frame at a time to the Reciver. The Sender will stop and wait for the acknowledgment from the Reciver. This time is the wating time for the Sender and the Sender gets the acknowledgment (ACK) then it will Send the Next packet to the reciver and wait for acknowledgment again and on this process will continue as long will continue. as ~~Long~~ Long as Sender has the Data to Send. This can be Understood by the dig:-



Stop & wait protocol

Two types of Delay wile sending frame:..

- Transmission Delay

$$T_d = D/B$$

D — Dividing the data size

B — Bandwidth

- Propagation Delay

$$T_P = d/s;$$ were d = dist b/w sender and reciver

s = wave propagation speed

Efficiency:-

$$a = \frac{T_P}{T_d}$$

T_P — Useful time

T_d ⟶ total time

Throughput = $n * B$

2) Go Back N

It Uses the principle of protocal pipelining in which the multiple frames can be sent before receiving the acknowledgment of the first frame. If we have five frame and the Concept - Back 3 which means that the true frame can be sent frame No 1 frame No 2 Frame No 3 can be sent before expecting the acknowledgment of frame No 1

In go-back-N ARQ, the frame are Numbered Sequentially as go-back-N ARQ Sends the Multiple frames at a time that require the Numbering approach to distinguish the frame from another frame. fro and these Numbers are Known as the sequential Numbers

Efficiency :- $\frac{N}{(1+2a)}$

Window Size — Sender window size = N

Receiver Window size = 1

Min No. of seq Number required — N+1

Retransmission required if a packet is lost → The entire window is Retransmitted

Type of Transmission → Full duplex

Selective repeat

Selective Repeat ARQ (Automatic Repeat Request) is a data link layer protocol that Uses sliding window Method for Relible delivery of data frames

Here only the erroneous or lost frame are retransmitted, while the good frames are recived and buffered

It uses two windows of equal size: A sending window that stores the frames to sent and a reciving window that stores the frames.

For eg:- If the sequence Number from 0-15 the window size will be 8

Efficiency = $\frac{N}{1+2a}$

Window Size = Sender window size = N
Reciver window size = N

Min No of Seq No required = $2 \times N$

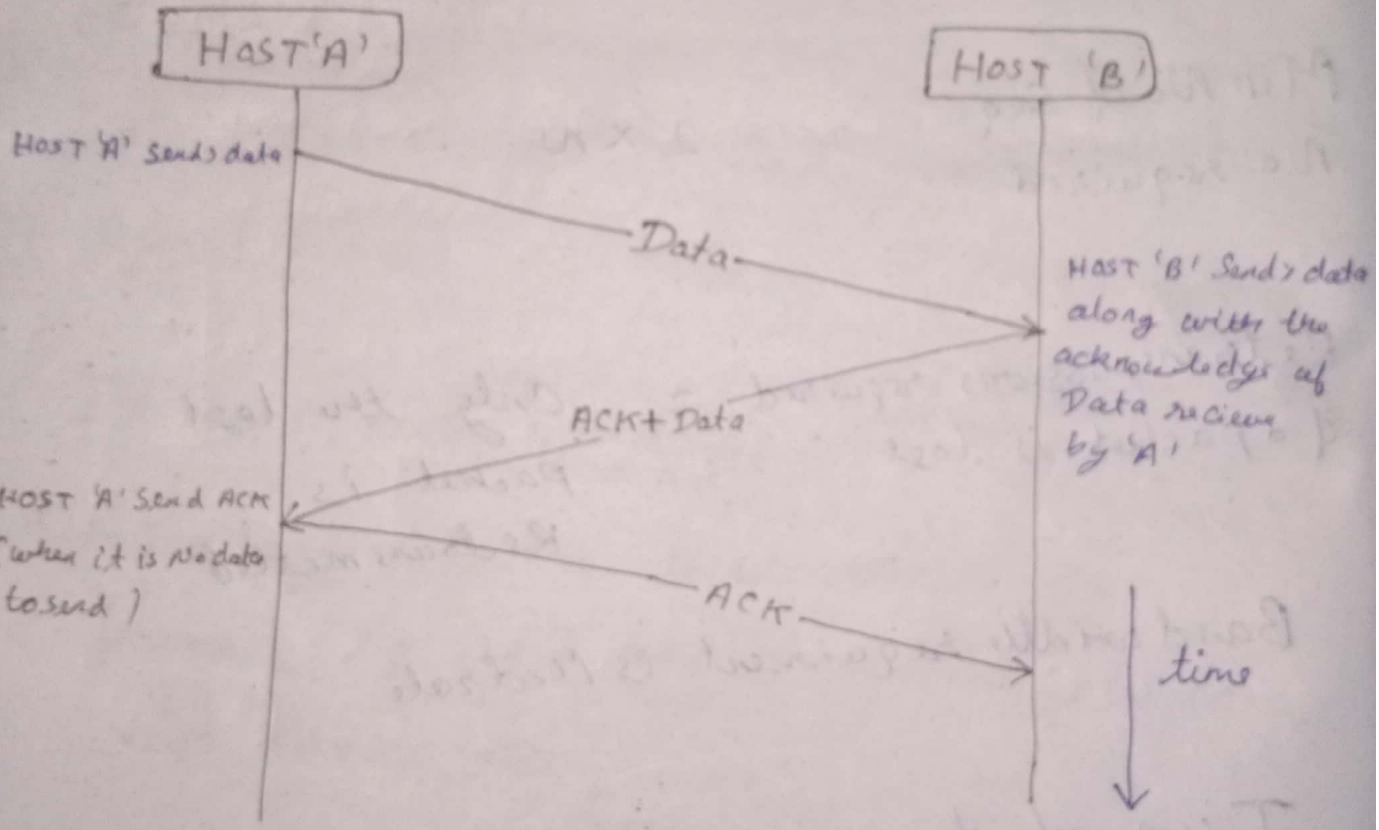
Retransmissions required if a packet is lost = Only the lost Packet is Retransmitted

Bandwidth requirment is Modrate

Type of transmission = Full Duplex

Piggybacking :

This technique in which the out going acknowledgment is delayed temprary is called piggybacking



As we can see in the fidure, we can see with Piggybacking, a single message (ACK + DATA) over the wire in place of two separate Message. Piggybacking improves the

efficiency of the bidirectional protocols

Advantages of piggybacking:

1) The Major Advantage of piggybacking is the better Use of available channel Band with. This happens Because Acknowledgment frame Need's Not to Besent Seperally

2) Usage Cost Reduction

3) Improves laterncy of data transfer.

Disadvantage of piggybacking:

1) the disadvantage of piggybacking is the additional Complexity.

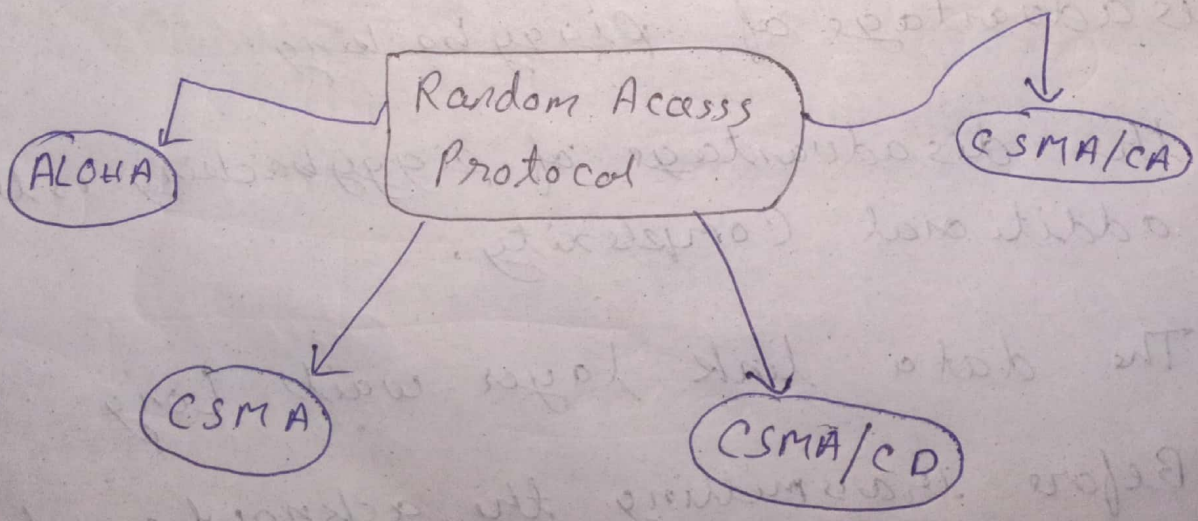
2) The data link layer wait's Long Before transmitting the acknowlegment (Block the ACK for some time), the frame will rebroadcast

The Random access protocols Consist of following Characterstic

The Random Access protocol consist of the following :-

1 There is No time restriction for sending the data
(you can talk to a friend without a timeRestriction)

2 There is a fixed sequnce of stations which are transmitting the data

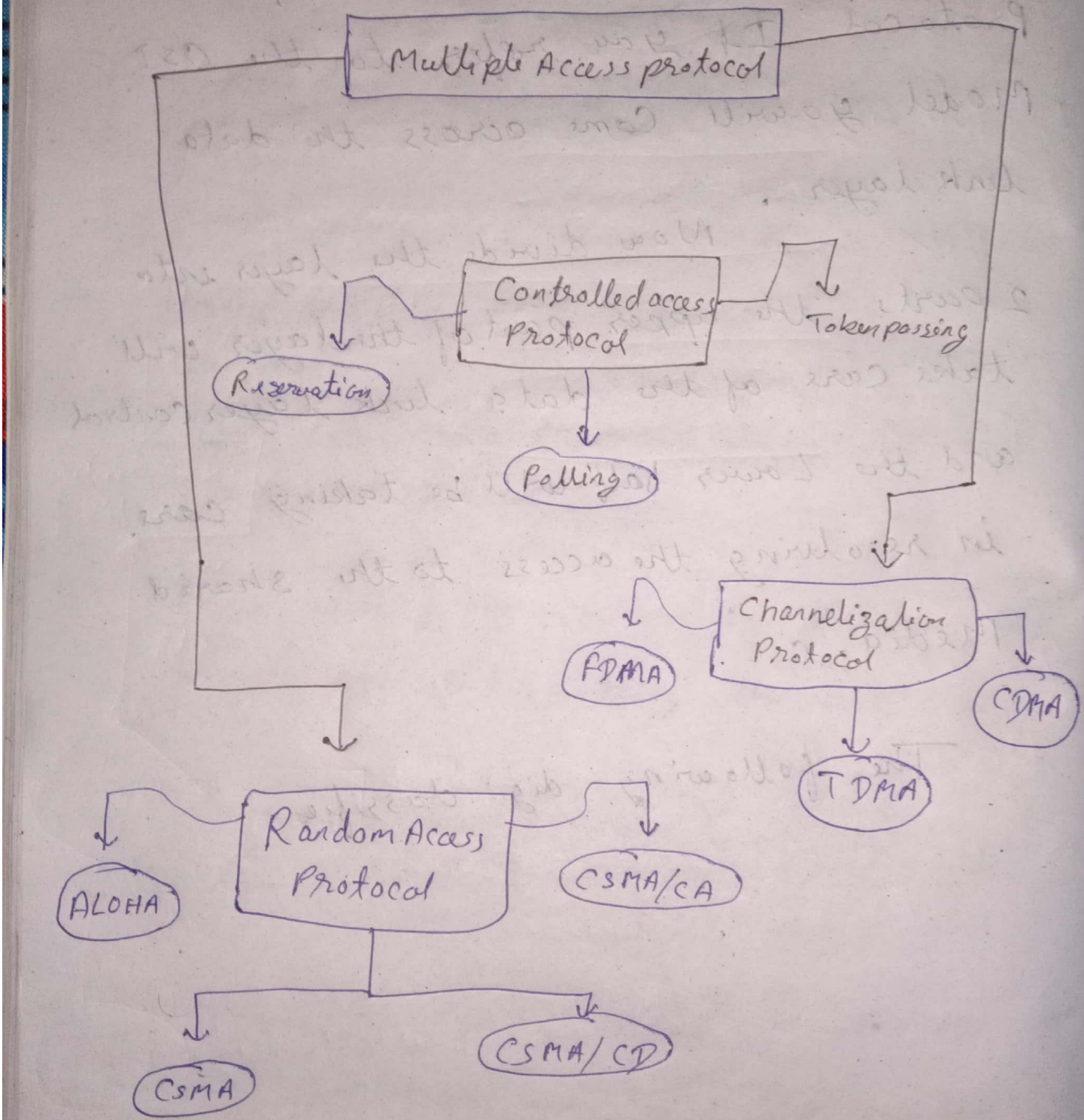


Multiple Access protocol

The Reson Behind this Multiple access Protocol If you refer to the OSI Model you will come across the data link layer.

Now divide the layer into 2 parts, the upper part of the layer will take care of the data link layer control and the Lower half will be taking care in resolving the access to the shared Media.

The following dig dassifies



PURE ALOHA

In Data transmission Stations Can transmit the data randomly i.e any Number of stations can transmit data at any time

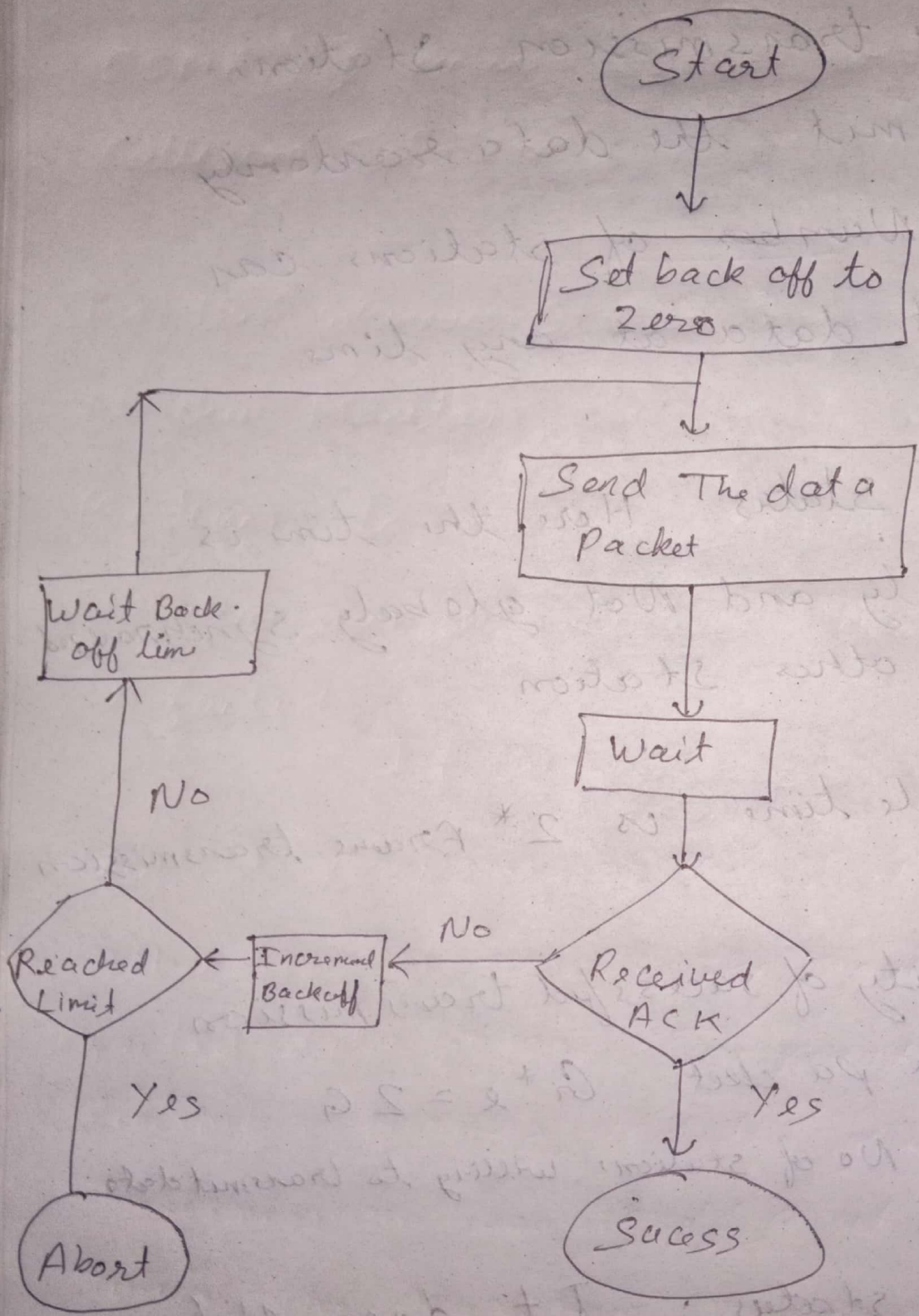
In time States Here the time is Continously and Not globaly synchronized with any other station

Vulnerable time is 2 * Frame transmission time

Probability of successful transmission of data packet $G * e = 2G$
were G = No of stations willing to transmit data

Collision states : It does Not Reduce the total Number of collision to Half

Flow chart Pure Aloha



Slotted ALOHA

The Slotted Aloha system Consist of the signals termed as becons which are at Precise time intervals are inform each Source when the channel is clear to send the frame.

Data transmission any Random Station Can transmit the data at the beginning of any Random time Slot

Time Status is discrete Unlike pure ALOHA and is also globally Synchonized

Probability of sucessful transmission of a data packed $G * e - G$

Collision Status it reduces the total No of collision to Half and double the efficiency of pure ALOHA

CSMA/CD Random Access protocol

CSMA/CD means CSMA with Collision Detection

In this whenever Station transmits data-frame it then Monitors the channel or the Medium to acknowledge the State of Transmission is successfully transmitted or failed

If the transmission Succeeds then it prepares for the Next frame Otherwise it resends the previously failed data frame. The point to Remember Here is that the frame Transmission time Should be at least twice the Maximum propagation time which can be deducted when the distance between the two Station involved in a collision is Maximum.

CSMA/CA

CSMA/CA means CSMA with collision avoidance

To detect the possible collisions, the sender Recives the acknowledgment and if there is only acknowledgment Present (its own) then this means that the data frame has been sent successfully But if there are 2 or More acknowledgement Signals then this indicate that the Collision has occured.

Method's avoid's collisions by :-

- Interframe Space
- Contention Window
- Acknowledgment

MODULE 5

SWITCHING

- When a User Accesses the internet or anothes Computer Network outside their immediate location, message are Sent through the Network of Transmission Media. This technique of transfering the information from One Computes Network to anothes Network is Known as Switching

- Switching in a Computer Network Isa achived by Using Switches A switch is a Small Harware device which is Used to Join

Multiple Computers together with One Local area Network (LAN)

- Network Switches operate at Layer 2 (Data link layer) in the OSI Model
- Switching is transparent to the User and does Not Require any configuration In home Network
- Switches are Used to forward the Packet based on MAC address
- It operated in full duplex Mode
- Packet collision is minimum as it directly Communicates b/w Source & destination
- It does Not Broadcast the Message as it works with limited Bandwidth.

IPv4

IPv4 is a Connectionless protocol Used for packet-switched Networks. It opretes on a best effort delivery Model, in which neither delivery is guaranteed, Nor proper Sequencing or avoidance of duplicate delivery assured. Internet protocol version 4 (IPV4) is the fourth revision of the Internet Protocol and a widely Used protocol in data Communication Over diffrent Kind of Network.

IPv4 is a Connectionless protocal Used in packet-switched layer Network Such as Ethernet, It provides a Logical Connection b/w Network device By providing identification of

each device. There are many ways to Configure IPv4 with all kinds of device - including Manual and Automatic Configuration - depending on the Network type

IPv4 used 32-bit address for Ethernet Communication in five classes A, B, C, D and E Class A, B and C Have diffrent bit length for addressing the Network Host. Class D addresses are Reserved for Milatory purpose and E class are reserved for future Use.

Ipv4 Uses 32-bit (4 byte) addressing which gives 2^{32} address.

IPv4 address are written in the dot-decimal Nolation;

- which Comparmises of four Octets of the address expressed individualy in decimal and Seprate by periods

for instance 192.168.1.5

- Size of Header 20 to 60 bytes

Type of service :- Low Delay, High Throughput Reliability (8 bits)

Totat length :- Length of Header + Data (16 bits) which is min value 20 bytes and max 65,535 byte

Flags :- 3 Flags of 1 bit each :
reserved bit (most be zero)
do Not fragment flag (same order)

Protocol :- Name of protocol to which the data is to be passed (8 bits)

16 bits Hetder checksum for checking errors in datagram Header.