DATA COMMUNICATION :-

The exchange of data between two computers (or) two devices (or) two persons through transmission medium.

(OR)

Data communication is the exchange of data (in the form of 0's & 1's between two devices via some form of transmission medium.

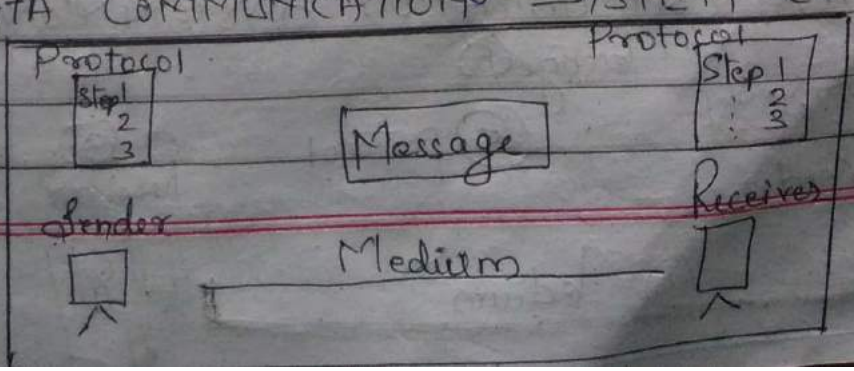
Characteristics of data communication :

1) DELIVERY :- System must deliver data to the correct destination. Data must be received by the device (or) User.

2) Accuracy :- System must deliver data accurately.

3) Time lines :- System must deliver data in a timely manner.

DATA COMMUNICATION SYSTEM COMPONENTS



COMPONENTS OF DATA COMMUNICATION SYSTEM

1) **Message** :- Message is an information to be communicatid. Eg:- text, picture, sound, video.

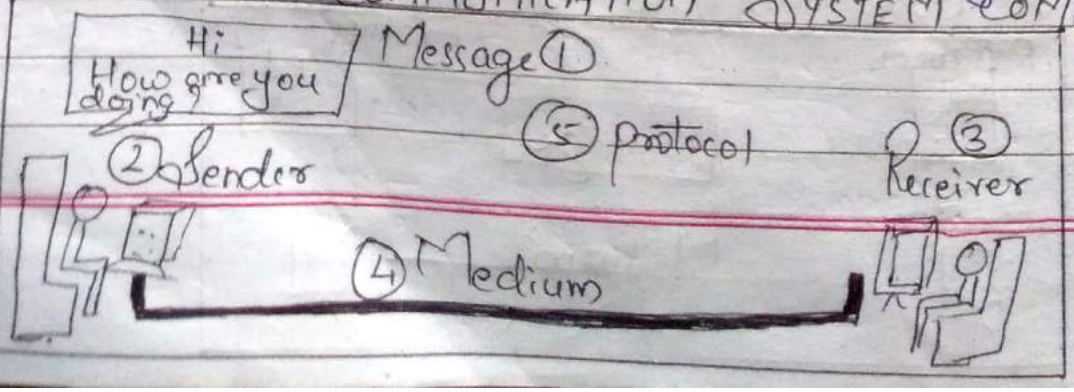
2) **Sender** :- Sender is a device that sends the data message. Eg:- computer, telephone, ~~Internet~~ handset etc.

3) **Receiver** :- A receiver is a device that receives the message.

4) **Medium** :- Physical path by which message travels from sender to receiver. Eg:- Twisted pair, coaxial cable, fibre optic etc.

5) **Protocol** :- Set of rules that govern data communication. Without protocol, two devices may be connected but not communication just as a person speaking french cannot be understood by a person who speake only japanese.

DATA COMMUNICATION SYSTEM COMPONENTS



NEED FOR DATA COMMUNICATION NETWORKING

1) Signal Generation :- Communication device must be able to generate and receive the signals.

2) Synchronization :- Receiver and transmitter must be synchronized, Receiver should know when the transmission of data starts and when the data ends.

3) Transmission System Utilization :- It refers to need to make efficient use of transmission channel by implementing various multiplying techniques.

4) Error Correction and Detection :- Transmitted signal getting distorted in transmission medium (or) error introduced by intermediate devices, In receiver end, the errors present in the signal are detected and corrected by error detection and correction method.

Error detection method → Parity checking, LRC, CRC, VRC etc.

Error Correction method → Hamming code, ARQ etc.

5) Flow of control of data -: Transmitter generate data faster than the receiver device, capable of handling to handle this.

6) Addressing -: When two or more devices share a transmitting facility, some identity or address is required for source and destination.

7) Routing -: Transmission system must ensure the data being sent (or) routed only to the destination system.

COMPUTER NETWORK AND ITS USE

1) Share Files -: LAN enables many users to share single copy of a file stored on a central file server.

2) Transfer files -: LAN enables to copy files quickly from machine to machine without having to exchange any peripheral devices.

3) Access Information and files -: LAN enables anyone to run applications.
ex - Banking software.

4) Share Application :- LAN enables two or more people to use the same copy of an application.

5) Simultaneously key Data into Application :- LAN application program allows two users to key data into it at once.

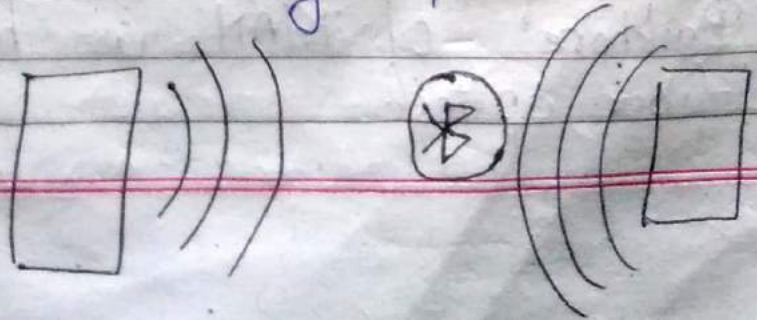
6) Share printers & other peripheral Devices.

7) Use Electronic mail :- LAN is used as a post office to send memos, reports and typed messages to other people sitting at computers in other building.

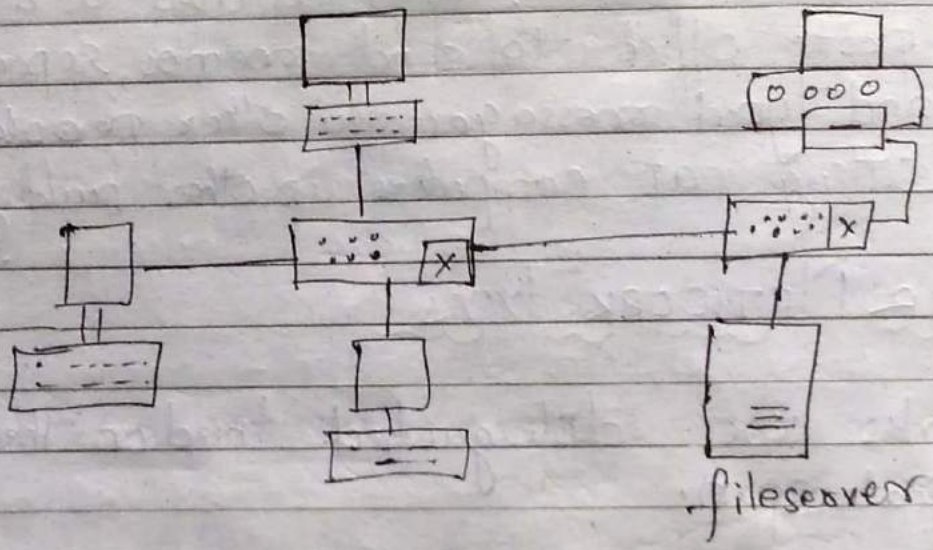
COMPUTER NETWORK TYPES

Networks are distinguished based on their geographical span.

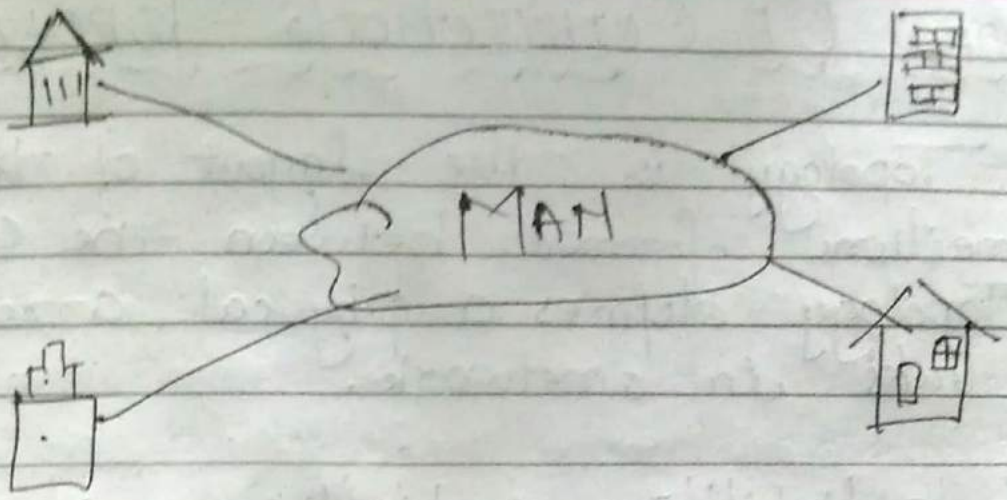
1) Personal Area Network :- Smallest n/w which is very personal to a user. This may include Bluetooth enabled devices. Range up to 10 meters.



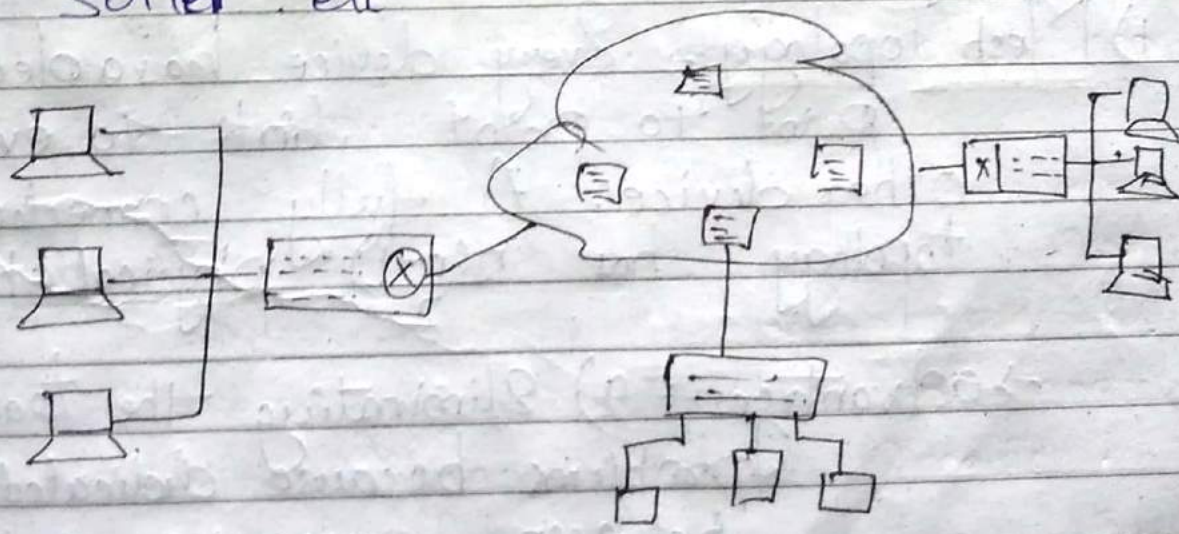
2) Local Area Network :- Computer network spanned inside a building and operated under single administrative system is generally termed as LAN. LAN provides an useful way of sharing the resources.
Ex- Organizational offices, colleges or universities.
LAN composed of inexpensive networking and routing equipment, contains local servers serving file storage.
LAN is wired and wireless both.



3) Metropolitan Area Network :- Generally expands throughout a city such as Cable TV network. It can be form of Ethernet, Token ring, ATM etc. Backbone of MAN is high-capacity fiber optics.



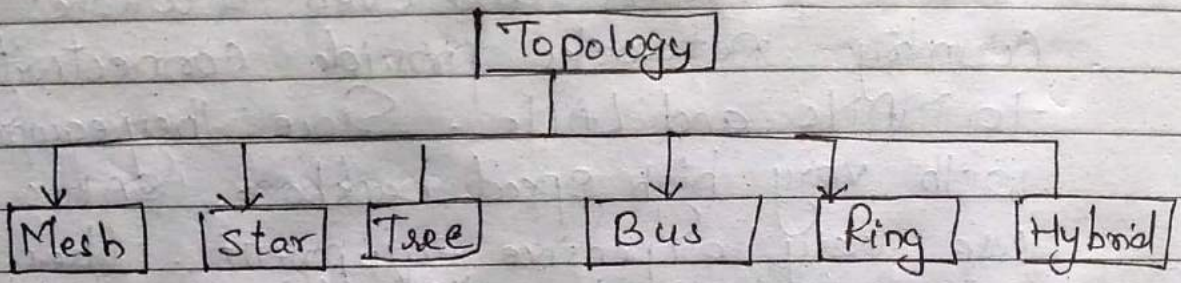
4) Wide Area Network :- WAN covers a wide area which may span across provinces and even a whole country. networks provide connectivity to MANs and LANs. Since they equipped with very high speed backbone, WANs use very expensive equipment. Uses Advance technology like frame relay SONET. etc.



TYPES OF CONNECTIONS - TOPOLOGY

Topology is the layout of the connections formed between the computers or Topology defines a physical arrangement of links in a network.

The reliability and efficiency of network is determined by structure. The topology is described how the devices in a network are interconnected.



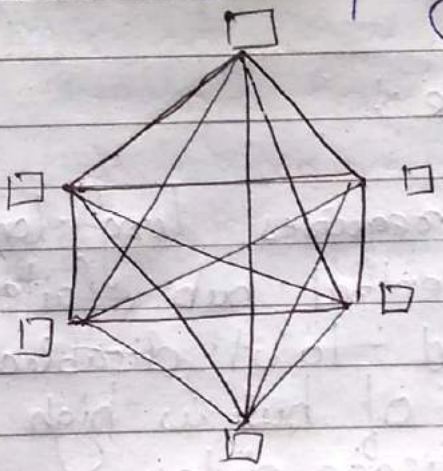
1) Mesh Topology :- Every device has a dedicated point to point link to every other device. A fully connected mesh topology has $\frac{n(n-1)}{2}$ physical channels.

→ advantages :- a) Eliminating the traffic problems because dedicated link between every two devices.

b) It is a robust because one link becomes fails, all other links

remain active.
c) fault identification easy.

→ Disadvantages:
a) Amount of required cabling is very large.
b) If large number of devices are used in network, the requirement of I/O ports are high.
c) Installation are reconfiguration are difficult.
d) This topology is expensive



2) Star Topology: Each devices has a dedicated link only through a central controller usually called a hub. Devices are not directly linked to each other. A star topology does not allow direct traffic between devices.
If one device wants to send

data to another, it sends the data to the controller, which then delivers the data to the appropriate destination.

→ Advantage :-

1) Less expensive than Mesh Topology
2) Device needs only one line and only one I/O port
3) Easy to Install and reconfigure
4) Less cabling is needed.
5) Robustness : If one link fails, only that link is effected.
6) fault identification is easy.

→ Disadvantage :-

1) It requires long length of cable.
2) If central hub failed the nodes attached to it disabled.
3) Cost of hub is high
4) Message delay.

3) Tree Topology

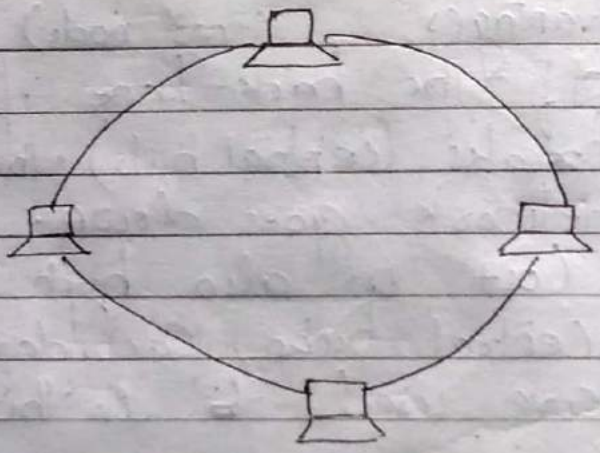
Advantages :-

1) It allows node devices to be attached to a single central hub.
2) It increases the distance a signal can travel between the devices.

Disadvantages (root node)

1) If the back-bone fails or breaks (central hub) the entire network goes down.
2) Cost is also high because central hubs, secondary hubs are used in this network.

4) Ring Topology :- Each device has a dedicated point to point line configuration. All devices are connected point to point in the shape of ring. A signal is passed along the ring in one direction from device to device until it reaches the destination. Each device in the ring can act as a repeater because each device in a ring receives the signal and regenerated the bits and then send to another device.



Advantages :- 1) Easy to install and reconfigure
2) Fault identification is easy.
3) A signal can travel long distance because each device a ring can act as a repeater.

Disadvantages :- 1) It is a unidirectional
2) If any one device fails in

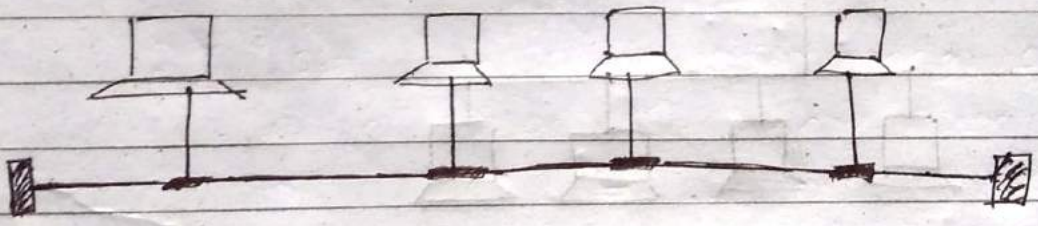
the ring topology the entire network fails.

3) Time delay of the signal is more.

5) Bus Topology :- One single and long cable (acts as a backbone) used to leave all other devices in the network.

Nodes are connected to the bus cable by droplines and taps. dropline is a connection between the device and the main cable.

In bus topology any computer can send data to any other computers because all computers attached to the main cable.



Advantages :- 1) Easy of Installation

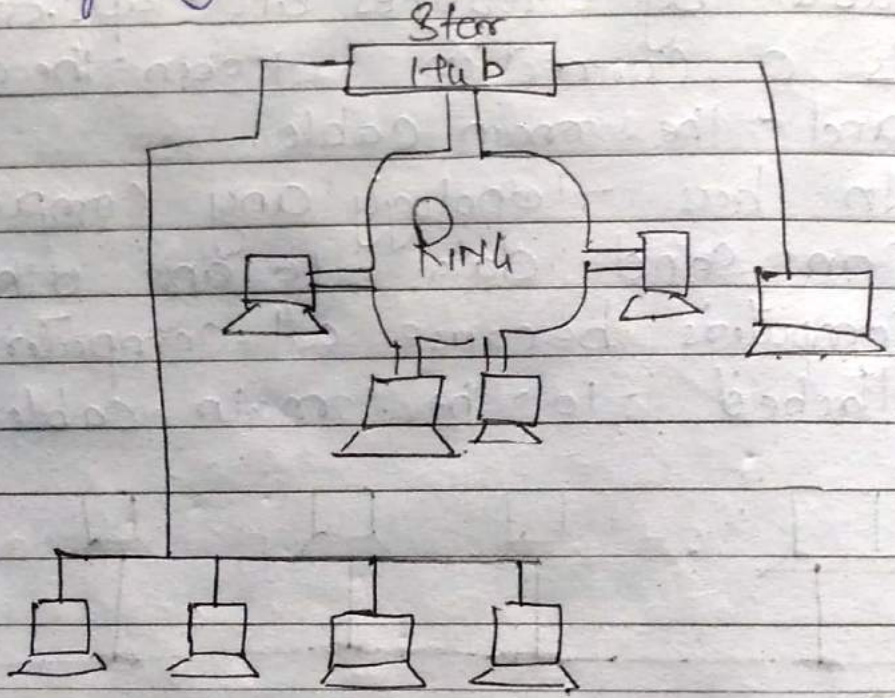
2) This topology requires least amount of cables to connect the computers and therefore less expensive.

Disadvantages :- 1) A fault or break in

the bus cable (Main Cable) stops transmission.

2) The speed of the bus is slow when heavy traffic.

6) Hybrid Topology :- Combination of various network topologies is called "Hybrid Topology". Different types of Hybrid topologies are.



WORKING OF TOKEN RING NETWORK

Token ring technique is based on the use of a small frame called a token, which circulates when all stations are idle. A Station wishing to transmit must wait until it detect a token passing by.

(1) At the start, a free Token is circulating on the ring. To use the network, a machine first has to capture the free Token and replace the data with its own message.

(2) Machine 1 wants to send some data to machine 4, so it first has to capture the free token. It then writes its data and the recipient's address onto the Token.

(3) The packet of data is then sent to machine 2 who reads the address, realizes it is not its own, so passes it onto machine 3. Machine 3 does the same and passes the Token on to machine 4.

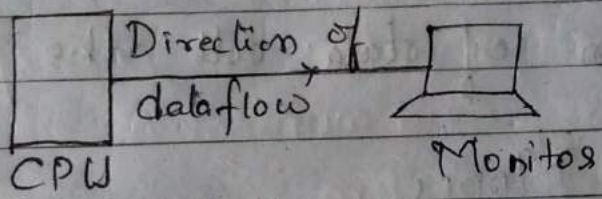
(4) This time it is the correct address and so number 4 reads the message. It cannot, however, release a free Token onto the ring, it must first send the frame back to number 1 with an acknowledgement to say that it has received the data.

(5) The receipt is then sent to machine

COMMUNICATION Modes

1) SIMPLEX MODE : A mode which provides transmission in only one direction. This is very limited in its application.

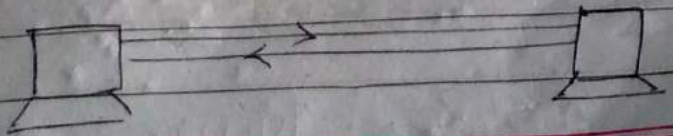
Only one of the two stations on a link can transmit the other can only receive.



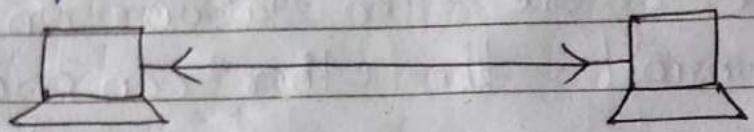
Eg → Tv transmission, key boards etc.

2) Half-duplex Mode - In half duplex mode each station can both transmit and receive data, but not at same time when one device is sending the other only receive and vice versa.

In half duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.



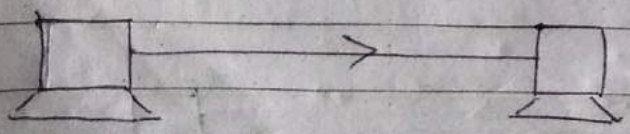
3) Full Duplex :- In full duplex mode both stations can transmit and receive simultaneously. Eg:- Cellphone, telephone In full duplex mode, signal going in either direction share the capacity of the link.



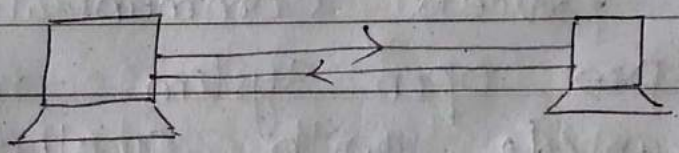
Direction of data all the time.

TRANSMISSION MODES

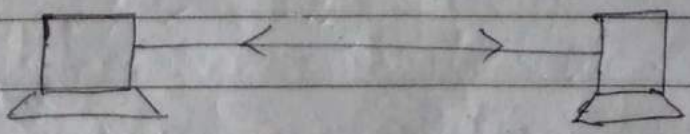
1) SIMPLEX :- In simplex communication mode, there is a one-way communication transmission. Television transmission is a very good exampl of simplex communication. The main transmitter sends out a signal (broadcast), but it does not expect a reply as the receiving units cannot issue a reply back to the transmitter



2) Half duplex :- In half-duplex mode, both units communicate over the same medium, but only one unit can send at a time. While one is in send mode, the other unit is in receive mode. It is like two polite people talking to each other - one talks, the other listens but neither one talks at the same time.



3) Full-duplex :- A full duplex system is used that allows information to flow simultaneously in both directions on the transmission path. Full-duplex lines improves efficiency as the line turn-around time required in a half-duplex arrangement is eliminated.



OSI - Open System Interconnection Model

OSI was developed by ISO (International Standard Organization) in 1983, for sending and receiving of data between two computers. It deals with connecting open system ie systems that follow a standards are open for communicating with other systems.

OSI represents a concept of inter process communication so that any open system may be able to communicate with another open system.

OSI Architecture decomposes the communication process into functional layers. Each layer is responsible for performing special functions. Therefore OSI architecture is reference model to all open system inter connections.

1) Application Layer :- The application layer enables the user, either human or software access the network. It provides end user for processing of data and supports for services such as e-mail, file transfers, Shared data base management, network software services and other types of distributed information services.
This layer acts as an interface between and user and network.
This layer mainly allows access to network resources.

2) Presentation Layer :- Presentation layer is concerned with the syntax and semantics of the information exchanged between two systems. It Translates the Application into network format and vice versa. It provides format and encrypt / decrypt data to be send across a network.

3) Session Layer :- It allows to establish, maintains and disconnected between Communicating Systems. It allows the communication between two devices

either in simplex or half duplex mode of transmission. It allows a process to add checkpoints (synchronization points) into a stream of data.

4) Transport Layer :- The transport layer is responsible for source to destination (end to end) delivery of the entire message. This layer converts data into smaller "segments" for sending and at the receiving end the segments are converted into original data. This layer is also responsible for error control and flow control.

5) Network Layer :- This layer converts data segments into packets and at the receiving end the ~~segments~~ packets are converted into data segments.
This layer determines path for transmitting data from source to destination.
It provide services like Routing, Internetworking, subnet, traffic control, Packet, Logical - physical address mapping (IP address)

6) Data Link Layer:- This layer converts data packets from network layer into frames and at the receiving end this layer converts frames into packet.

The data link layer divides the stream of bits received from the network layer into manageable data units called frames. If frames are to be distributed to different system on the network. The data link layer adds a header to the frame to define the physical address of the sender (source address) and receiver (destination address) of the frame.

Data link layer receives the data to be sent from the network layer. adds header and trailer to it which is now known as a frame. This frames then transmitted to the physical layer.

Data link layer can be devided into two sub-layers. They are

1) LLC (Logical link control)
2) MAC (Medium Access control)

7) Physical Layer :- Physical Layer is responsible for transmitting raw bits over a communication channel. It converts frames from the data link layer into bits and at the receiving end, bits from the physical layer is given to the data link layer.

The source and destination nodes have to agree on number of factors such as what voltage constitute a bit 0 & 1. Which communication modes etc. It also deals with the electrical specifications of cables, connectors and interface such as RS 232.

Functions of Physical layer.

a) Signal encoding
b) Medium
c) Bit Synchronization
d) Transmission Byte
e) Transmission mode
f) Multiplexing.

TRANSMISSION MEDIA

Transmission media is the physical path between the transmitter and receiver.

Types of transmission media:

a) Guided
b) Unguided

Guided Media, The waves are guided along a solid medium, such as copper

→ twisted pair
→ Coaxial cable
→ Optical fibre.

Unguided Media that provide a means of transmitting electromagnetic signals but do not guide them.

→ Radio frequency
→ Terrestial Microwave
→ Satellite communication
→ Cellular telephony

Transmission medium depends upon following factors:

→ Transmission rate
→ Distances
→ Cost and ease of Installations.
→ Resistance to environmental conditions

1) Twisted Pair :- Twisted pair is least expensive and most widely used. A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern. A wire pair acts as a single communication link.

Twisted Pair comes in two variables

→ Unshielded Twisted Pair
→ Shielded twisted pair.

Unshielded twisted pair is a set of twisted pairs of cable with in a plastic case.

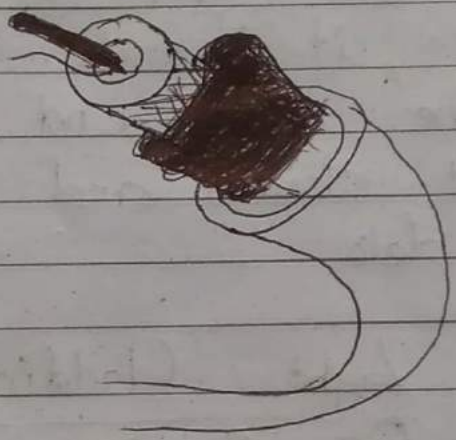
1) Twisted Pair :- Twisted pair is least expensive and most widely used. A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern. A wire pair acts as a single communication link.

Twisted Pair comes in two variables

→ Unshielded Twisted Pair
→ Shielded twisted pair.

Unshielded twisted pair is a set of twisted pairs of cable with in a plastic case.
It is the cheapest transmission media.
It is commonly used for LAN., its easy to work and install.
UTP is subject to external electromagnetic interference.
Category 3 and Category 5 UTP are commonly used in computer networks.
Difference between cat 3 and cat 5 Cable is the number of twists in the cable per unit distance

2) Coaxial Cable -: Coaxial cable has two wires of copper. The core wire lies in the center and it is made of solid conductor. The core is enclosed in an insulating sheath. The second wire is wrapped around over the sheath and that too in turn encased by insulator sheath. This all is covered by plastic.



→ Coaxial cable is capable of carrying high frequency signals than that of twisted pair cable.

→ Wrapped structure provides it a good shield against noise and cross talk.

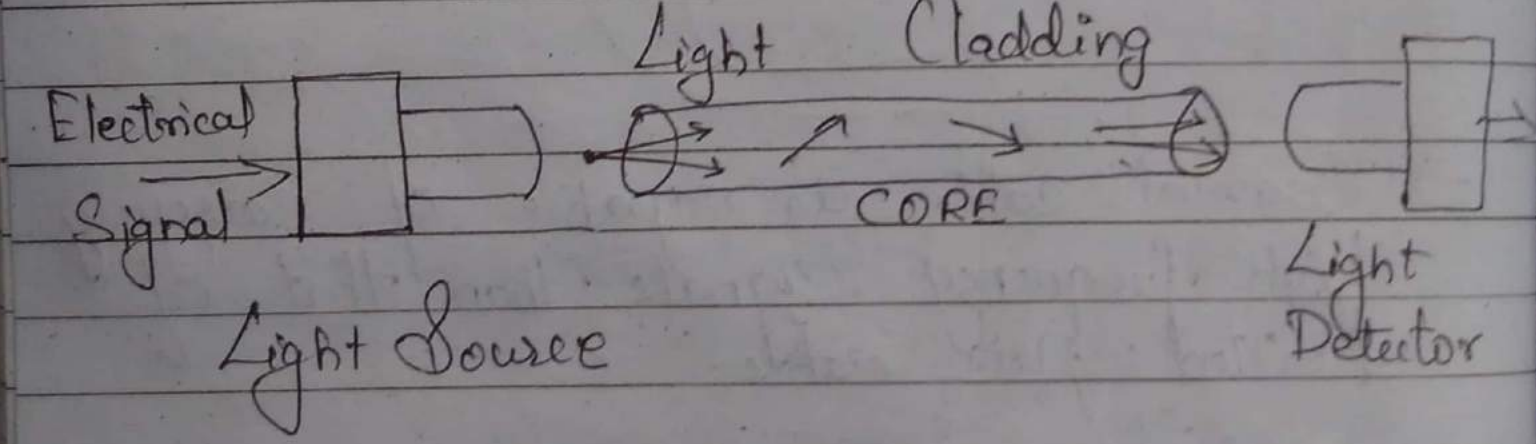
→ Coaxiable cables provide high bandwidth rate upto 450 mbps.

Example -:
RG-59 (TV cable) RG-58 (Thin Ethernet)
RG → Radio Government.

Cables are connected using BNC connector.

3) Fibre Optics :- Fibre Optics works on the properties of light. When light ray hits at critical angle it tends to refract at 90°. This property has been used in fibre optic. The core of fibre optic cable is made of high quality glass or plastic.

From one end of it light is emitted, it travels through it and at the other end light detector detects light stream and converts it to electric data.



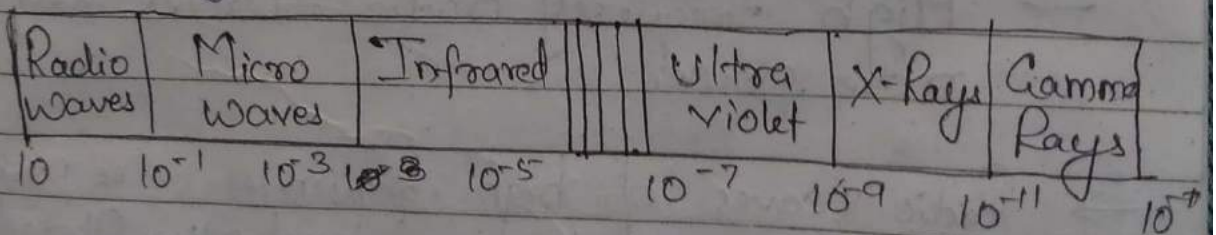
COAXIIAL	TWISTED PAIR	OPTIC FIBRE
→ It uses electric signal for transmission.	Uses electric signal for transmission	FOC uses optical form over a glass fiber.
→ Less affect by EMI	Affected by EMI	Not affected by EMI
→ Bandwidth is moderately high	Bandwidth is low	Bandwidth is very high
→ Supports moder-ately high data rates	Supports low data rates	Data rate is very high.
→ Moderately Costly.	Cheapest	Costly
→ Repeater Spacing is 1-10km	Repeater Spacing 2-10km	Repeater Spacing 10-100km
→ It Supports all radio frequencies	Supports all radio frequencies	Frequency range is 902 MHz to 928 MHz.

Media	Advantages	Disadvantage
Twisted Pair Cable.	1) Inexpensive 2) Easy Installation and use 3) Easy to add nodes	1) Sensitive to noise 2) Short Distances 3) Limited Bandwidth 4) No security. Signal can be easily tapped.
Coaxial Cable	1) High bandwidth 2) Long Distance 3) Noise Immunity	1) Physical dimensions 2) No security signal can be easily tapped.
Optic fiber cables	1) Very high bandwidth 2) Noise Immunity 3) Long distance 4) High security 5) Small Size	1) Special equipment needed for installation 2) Adding node is difficult 3) Very Expensive.

UNGUIDED TRANSMISSION

Wireless Transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless signals are spread over in the air and are received and interpreted by appropriate antennas.

When an antenna is attached to electrical circuit of a computer or wireless device, it converts the digital data into wireless signals and spread all over within its frequency range. The receptor on the other end receives these signals and convert them back to digital data.



1) Radio Transmission :-

Radio frequency is easier to generate and because of its large wavelength it can penetrate through

walls and structures alike. Radio waves can have wavelength from 1mm - 100000 km and have frequency from 3Hz to 300GHz.

→ Radio frequency is easier to generate and because of its large wavelength it can penetrate walls and structures alike.

→ Radio waves at lower frequencies can travel through walls whereas higher RF can travel in straight line and bounce back.

→ The power of low frequency waves decreases sharply as they cover long distance.

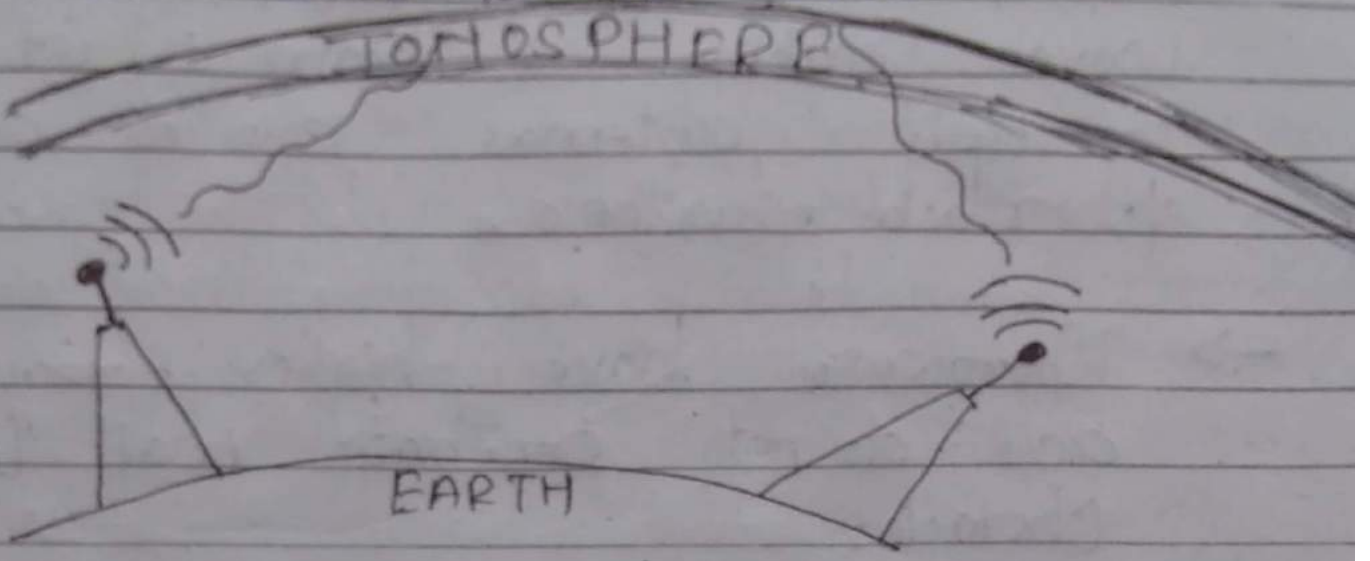
→ High frequency radio waves have more power.

→ Radio waves of high frequencies are prone to be absorbed by rain and other Obstacles

→ They use Ionosphere of earth atmosphere

→ When they reach Ionosphere, they are

re-fracted back to the earth.

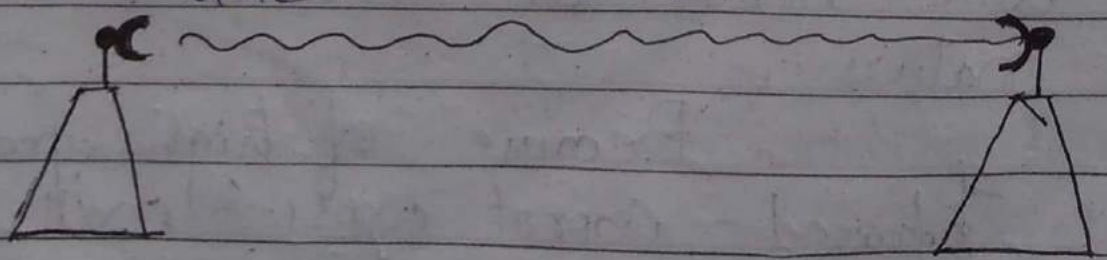


2) Microwaves Transmission -:

Electromagnetic waves above 100MHz tend to travel in a straight line and signals over them can be sent by beaming those waves towards one particular station.

Because Microwaves travels in straight lines, both sender and receiver must be aligned to be strictly in line of sight.

Microwave can have wavelength ranging from 1mm - 1meter and frequency ranging from 300MHz to 300GHz.



→ Microwave antennas concentrate the waves making a beam of it. multiple antennas can be aligned to reach further.

→ Microwave have higher frequencies and do not penetrate wall like obstacles

→ Microwave transmission depends highly upon the weather conditions and the frequency it is using.

3) Infrared Transmission:-

Infrared wave lies in between visible light spectrum and microwaves. It has wavelength of 700nm to 1mm and frequency ranges from 300GHz to 430THz.

Infrared wave is used for very short range communication purposes such as TV and its remote.

Infrared travels in a straight line hence it is directional by nature.

Because of high frequency, Infrared cannot cross wall like obstacles.

MULTIPLEXING

Multiplexing is a technique by which different analog and digital streams of transmission can be simultaneously processed over a shared link.

Multiplexing divides the high capacity medium into low capacity logical medium which is then shared by different streams.

Communication is possible over the air (radio-frequency) using a physical media (cable) and light (optical-fiber). All mediums are capable of multiplexing.

When multiple senders try to send over a single medium, a device called Multiplexer divides the physical channel and allocates one to each.

On the other ~~hand~~ end of communication, a De-multiplexer receives data from a single medium, identifies each and sends to different receivers.

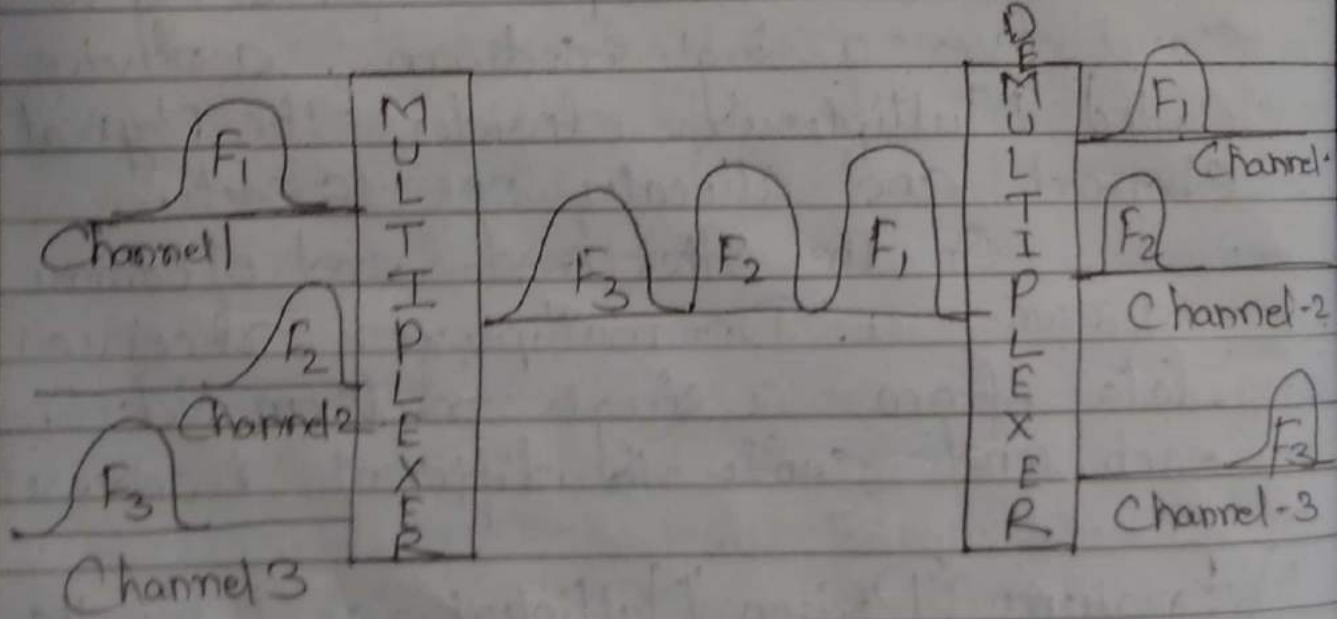
1) Frequency Divison Multiplexing : When the carrier is frequency, FDM is used. FDM is an analog technology.
   → FDM is an analog technology.
   → FDM divides the spectrum

or carrier bandwidth in logical channels and allocates one user to each channel.

→ Each user can use the channel frequency independently and has exclusive access of it.

→ All channels are divided in such a way that they do not overlap with each other, Channels are separated by guard space/bands.

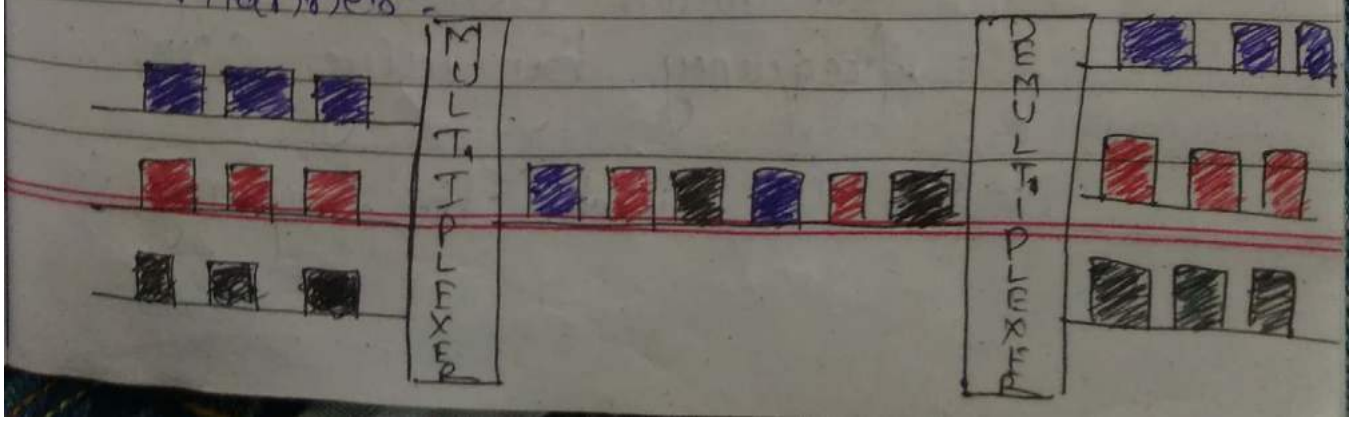
→ Guard band is a frequency which is not used by either channel.



2) Time Division Multiplexing :-

→ TDM is applied primarily on digital signals but can be

applied on analog signals as well. In
→ TDM the shared channel is divided
among its user by means of time slot.
→ Each user can transmit data within
the provided time slot only. Digital
→ signals are divided in frames, equivalent
to time slot ie frame of an optimal
size which can be transmitted in given
time slot.
→ TDM works in synchronized mode.
ie Multiplexer and Demultiplexer are
timely synchronized and both switch
to next channel simultaneously.
→ When channel A transmits its frame
at one end, the De-multiplexer
provides media to channel A on
the other end. As soon as the channel
A's time slot expires.
→ This side switches to channel B.
→ On the other end, the De-multiplexer
works in a synchronized manner
and provides media to channel B.
→ Signals from the different channels
travel the path in interleaved
manner.



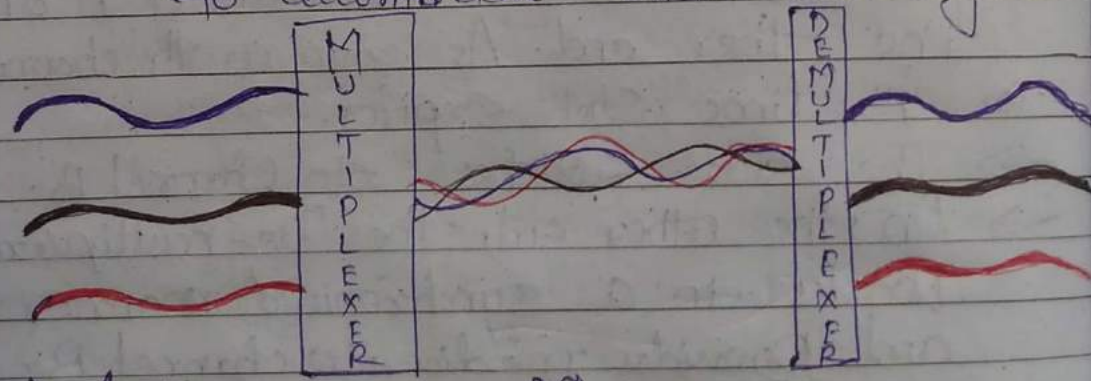
3) Wavelength Divison Multiplexing -

→ Light has different wavelength (Colors)

→ In fiber optic mode, multiple optical carrier signals are multiplexed into an optical fiber by using different wavelengths.

→ This is an analog multiplexing technique and is done conceptually in the same manner as FDM but uses light as signals.

→ On each wavelength time division multiplexing can be incorporated to accomodate more data signals.



4) Code Division Multiplexing -

→ Multiple data signals can be transmitted over a single frequency by using CDM.

→ FDM divides the frequency in

smaller channels but CDM allows its user to full bandwidth and transmit signals all the time using a unique code.

→ CDM uses orthogonal codes to spread signals.

→ Each station is assigned with a unique code called chip.

→ Signals travel with these codes independently inside the whole bandwidth

→ Receiver knows in advance the chip code signal it has to receive.

SWITCHING

Switching is process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called ingress and when data leaves a port or goes out it is called egress. A communication system may include number of switches and nodes. Switching is divided in two categories.

→ Connectionless :- The data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.

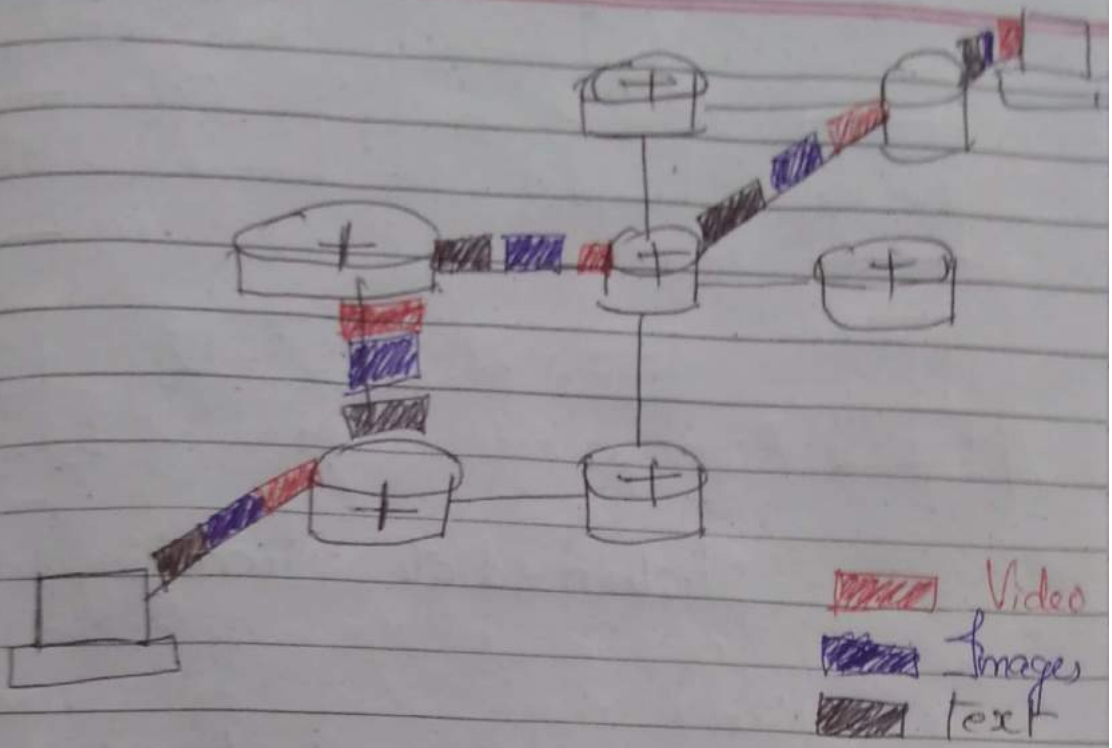
→ Connection Oriented :- Before switching data to be forwarded to destination, there is a need to pre-establish circuit along the path between both endpoints. Data is then forwarded on that circuit. After the transfer is completed circuits can be kept for future use or can be turned down immediately.

1) Circuit Switching :-

When two nodes communicate with each other over a dedicated communication path, it is called Circuit Switching. There is a need of pre-specified route from which data will travels and no other data is permitted. In circuit switching, to transfer the data, circuit must be established so that the data transfer can take place.

Circuits can be permanent or temporary. Applications which use circuit switching go through three phases

- Establish a circuit
- Transfer the data
- Disconnect the circuit.

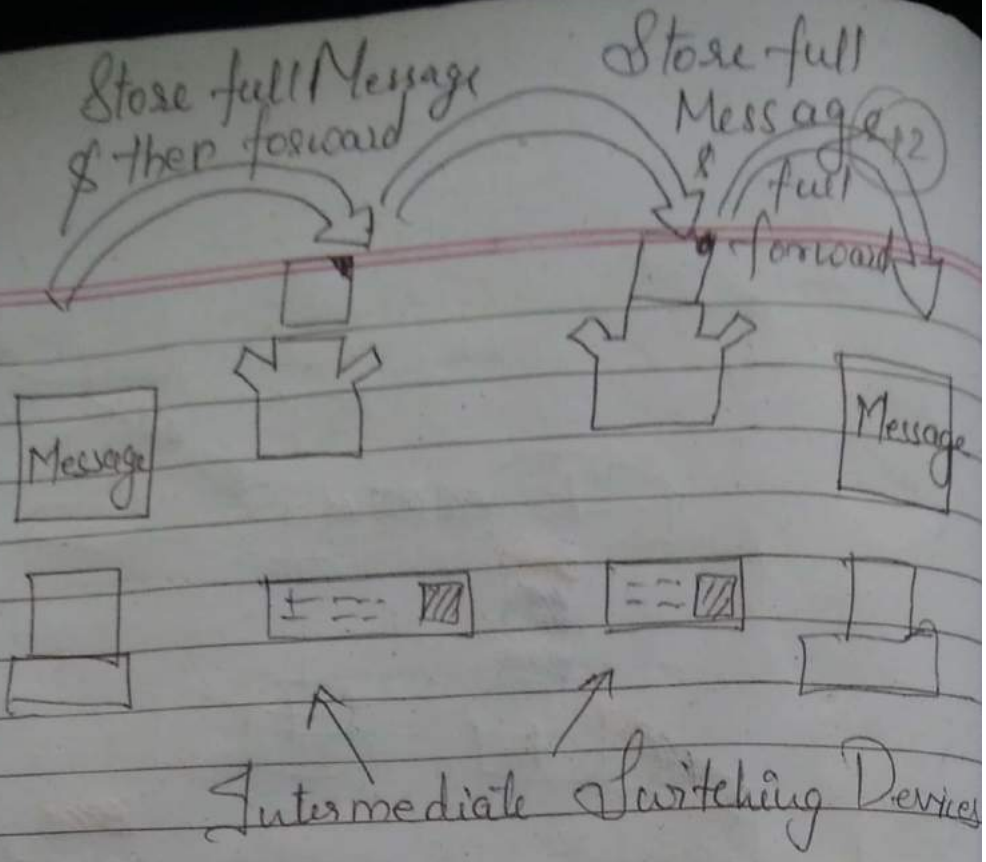


Circuit switching was designed for voice applications. Telephone is the best suitable example of circuit switching. Before a user can make a call, a virtual path between caller and callee is established over the network.

2) Message Switching :-

A switch working on message switching, first receives the whole message and buffers it until there are resources available to transfer it to the next hop.

If next hop is not having enough resource to accomodate large size message, the message is stored and switch waits.



This technique was considered substitute to circuit switching. As in circuit switching the whole path is blocked for two entities only.

Message switching has the following drawbacks:

→ Every switch in transit path needs enough storage to accomodate entire message

→ Because of store and forward technique and waits included until resources are available, message switching is very slow.

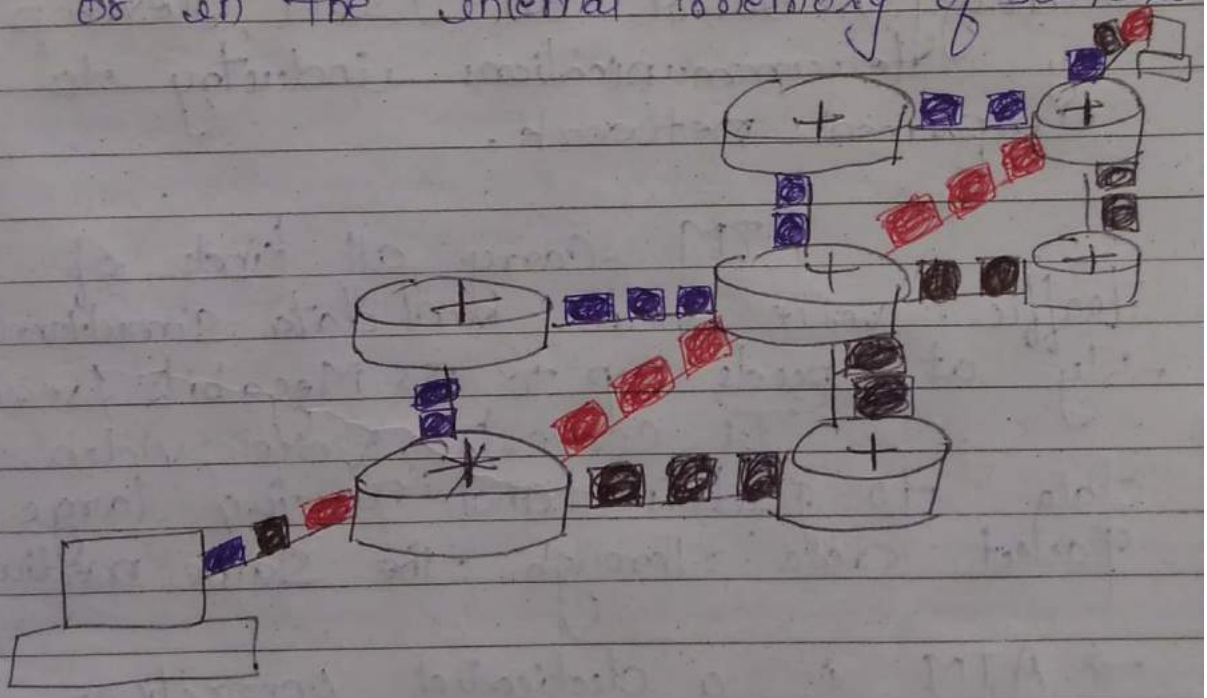
→ Message switching was not a solution for streaming media and real time applications.

3) Packet Switching :-

To overcome from Message Switching, Packet switching break down message into smaller chunks called packets.

Switching information is added in the header of each packet and transmi-tted independently.

It is easier for intermediate networking devices to store small size packets and they do not take much resources either on carrier path or in the internal memory of switches.



Packet Switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier.

Internet uses packet switching technique

Packet switching enables the user to differentiate data streams based on priorities. Packets are stored and forwarded according to their priority to provide quality of service.

ATM (Asynchronous Transfer Mode)

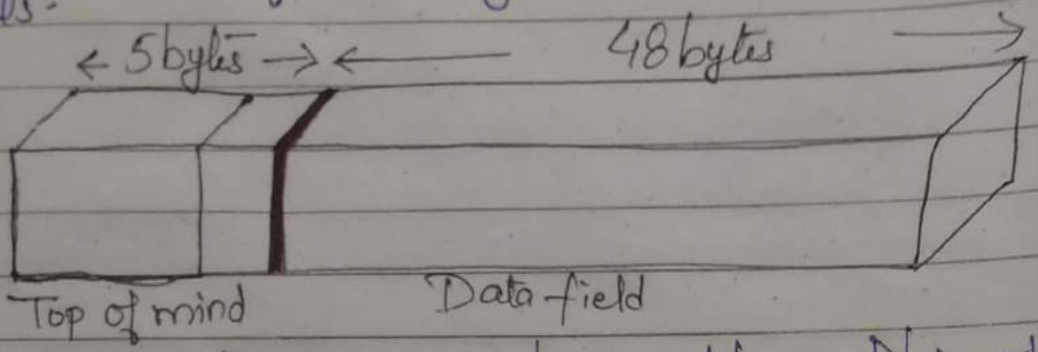
ATM also called cell relay that is operates at the data link layer of OSI Model over fibes or twisted pair cable, a high-speed switched n/w technology, based on ISDN, develop by telecommunications industry to implement network.

ATM carry all kinds of traffic: voice, video and data simultaneously at speeds up to 155 Megabits/second. It converts voice, video data to packets and passing large packet data through the same medium.

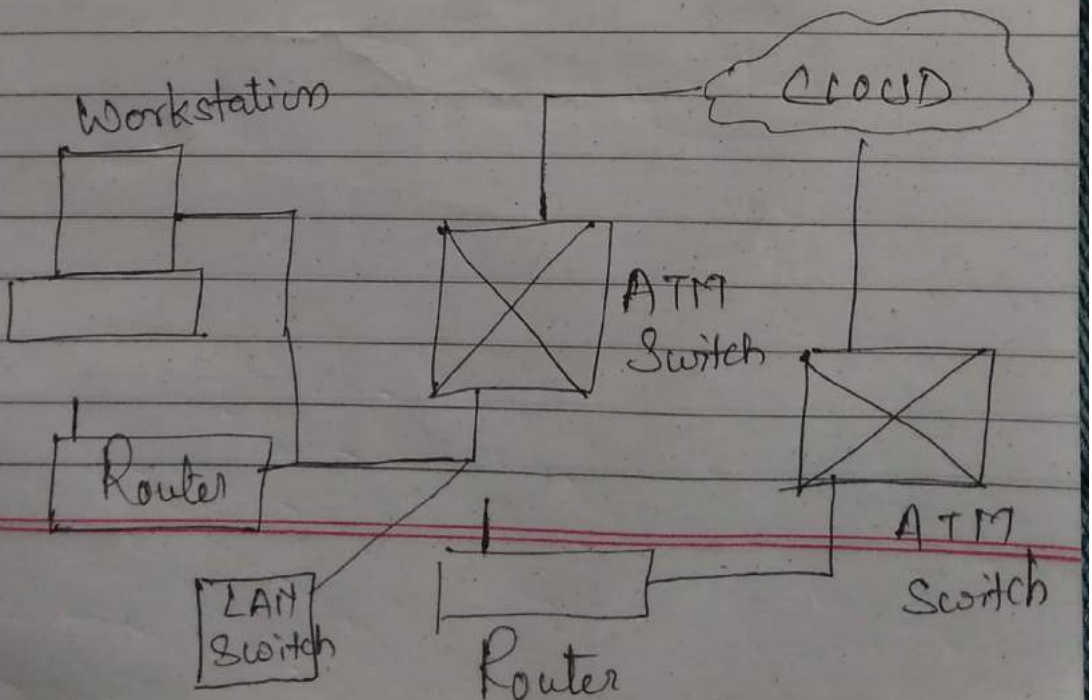
→ ATM is a dedicated connection-oriented switching technology, in which

→ In which switches create a virtual connection or virtual circuit between the

Sender and receiver of a call that permanent or switched for the duration of the call.
→ It is a small-packet switched system or similar to circuit-switched network which breaks down messages into very small, fixed length packets called cells.



An ATM header can have User-Network Interface (UNI) and Network-Node Interface (NNI) two formats.
→ User-Network Interface (UNI) used for communication between end systems.
→ Network-Node Interface (NNI) used for communication between switches.



UNIT-2

DATA LINK LAYER :-

Data link layer is second Layer of OSI Layered Model. This layer is one of the most complicated layers and has complex functionalities and liabilities. Data link layer hides the details of underlying hardware and represents itself to upper layer as the medium to communicate.

Data link layer works between two hosts which are directly connected in some sense. This direct connection could be point to point or broadcast. Systems on broadcast network are said to be on same link. The work of data link layer tends to get more complex when it is dealing with multiple hosts on single collision domain.

Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware. At the receiving end, Data link layer picks up data from hardware which are in the form of electrical signals, assembles them in a recognizable frame format, and hand over to upper layer.

Data link layer has two sub-layers

→ Logical link Control :- It deals with protocols, flow-control and error control.

→ Media Access Control : It deals with Actual control of media.

FUNCTIONALITY OF DATA-LINK LAYER

Data link layer does many tasks on behalf of upper layer. These are :-

→ Framing - Data-link layer takes packets from Network Layer and encapsulates them into frames. Then, it sends each frame bit by bit on the hardware. At receiver end, data link layer picks up signals from hard-ware and assembles them into frames.

→ Addressing - Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.

→ Synchronization – When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.

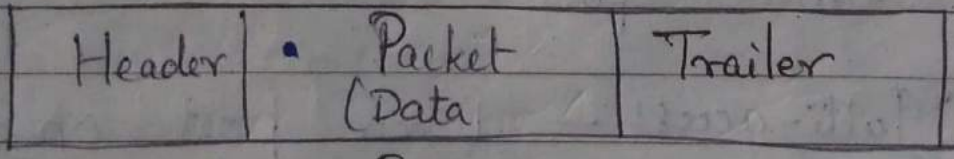
→ Error Control – Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.

→ Flow Control – Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machine to exchange data on same speed.

→ Multi-access – When host on the ~~when~~ shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple systems.

FRAMING IN DATA LINK LAYER

Framing is a Point-to-point connection between two computers or devices consists of a wire in which data is transmitted as a stream of bits. However, these bits must be framed into discernible blocks of information. Framing is a function of a the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. Ethernet, token ring, frame relay & other data link layer technologies have their own frame structures. Frames have headers that contain information such as error-checking codes.



FRAME

At data link layer, it extracts message from Sender and provide it to receiver by providing sender's and receiver's address. The advantage of using frames is that data is broken up into recoverable

chunks - that can easily be checked for corruption.

Problems in framing :-

→ Detecting start of the frame :- When a frame is transmitted, every station must be able to detect it. Station detect frames by looking out for special sequence of bits that marks the beginning of the frame ie SFD (Start Frame Delimiter)

→ How do station detect a frame :- Every station listen to link for SFD pattern through a sequential circuit. If SFD is detected, sequential circuit alerts station. Station checks destination address to accept or reject frame.

→ Detecting end of frame :- When to stop reading the frame.

Since the physical layer merely accepts and transmits a stream of bits without any regard to meaning or structure, it is upto the data link layer to create and recognize frame boundaries. This can be accomplished by attaching special bit patterns to the beginning and end of the frame. If these bit patterns can accidentally occur in data, special care must be taken to make sure these patterns are not incorrectly interpreted as frame delimiters.

four framing methods that are widely used are

(a) Character Count
(b) Starting and ending characters, with character stuffing.
(c) Starting and ending flags with bit stuffing
(d) Physical layer coding violations.

Charater Count :

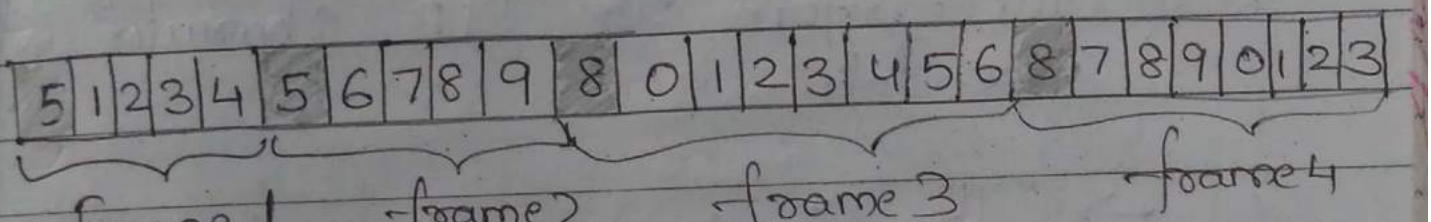
→ This method uses a field in the header to specify the number of characters in the frame

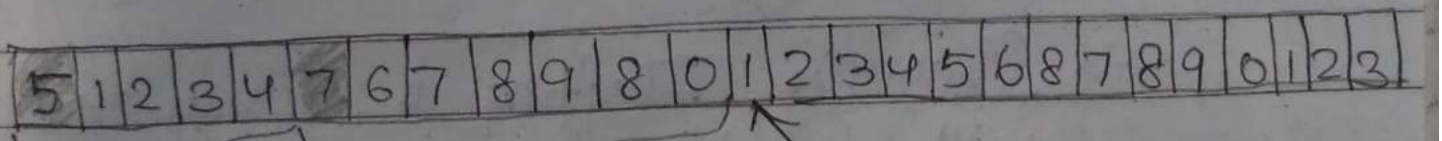
→ When the data link layer at the destination sees the character count, it knows how many characters follow and hence where the end of the frame is.

→ The disadvantage is that if the count is garbled by a transmission error, the destination will lose synchronization

→ is unable to locate the start of the next frame.

→ This method is rarely used.





Character Stuffing :

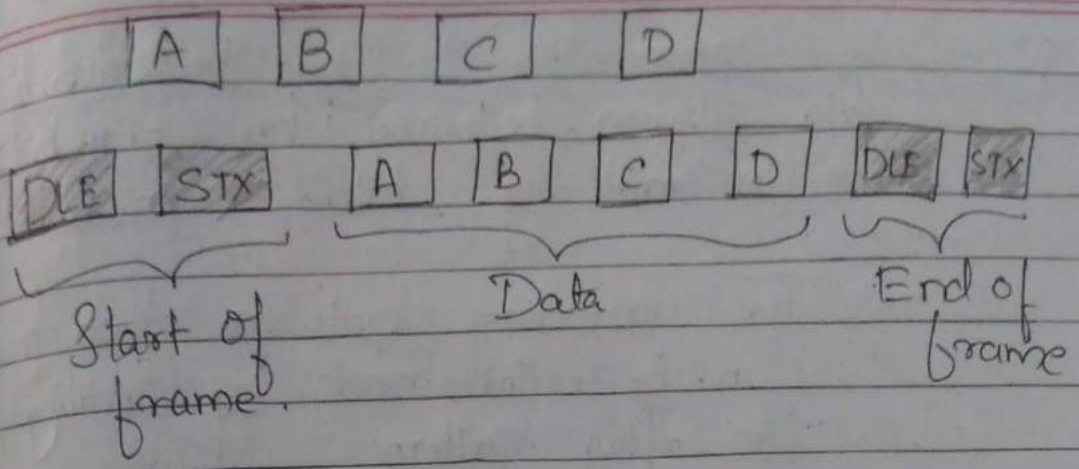
→ Each frame starts with the ASCII character sequence DLE STX and ends with the sequence DLE ETX.

→ This method overcomes the drawbacks of the character count method. If the destination ever loses synchronization it only has to look for DLE STX and DLE ETX characters.

→ The sender's data link layer inserts an ASCII DLE character just before the DLE character in the data.

→ The receiver's data link layer removes this DLE before this data is given to the N/w Layer.

→ Character stuffing is closely associated with 8-bit characters and this is a major hurdle in transmitting arbitary sized characters.



Bit Stuffing:-

→ Data frames to contain an arbitary number of bits and allow character codes with an arbitary number of bits per character.

→ At the start and end of each frame is a flag byte consisting of the special bit pattern '01111110'.

→ Whenever the sender's data link layer encounters five consecutive 1s in the data, it automatically stuffs a zero bit into the outgoing bit stream.

→ Whenever the receiver sees

five consecutive 1s in the incoming data stream, followed by a zero bit, it automatically destuffs the 0 bit.

→ The boundary between two frames can be determined by locating the flag pattern.

0 11111111 01111101
Char 1 Char 2

On the line we will send:

Start of frame. end of frame
01111011 01111001
Char 1 Char 2

Sender rule is - if 5 1's in data add (stuff) a zero.

Receiver strips start & end of frame and unstuffs.

011111-11 011111-01
Char 1 Char 2

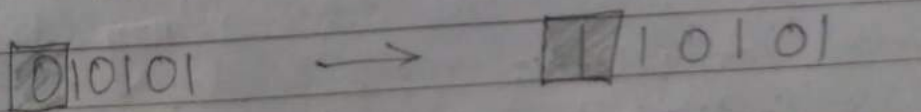
Receiver rule → If a zero occurs after 5 1's remove it.

ERROR DETECTION AND CORRECTION

ERROR :- Data can be corrupted during transmission. For reliable communication, errors must be detected and corrected. Signals flows one point to another. It is subjected to unpredictable interferences from heat, magnetism and other forms of electricity.

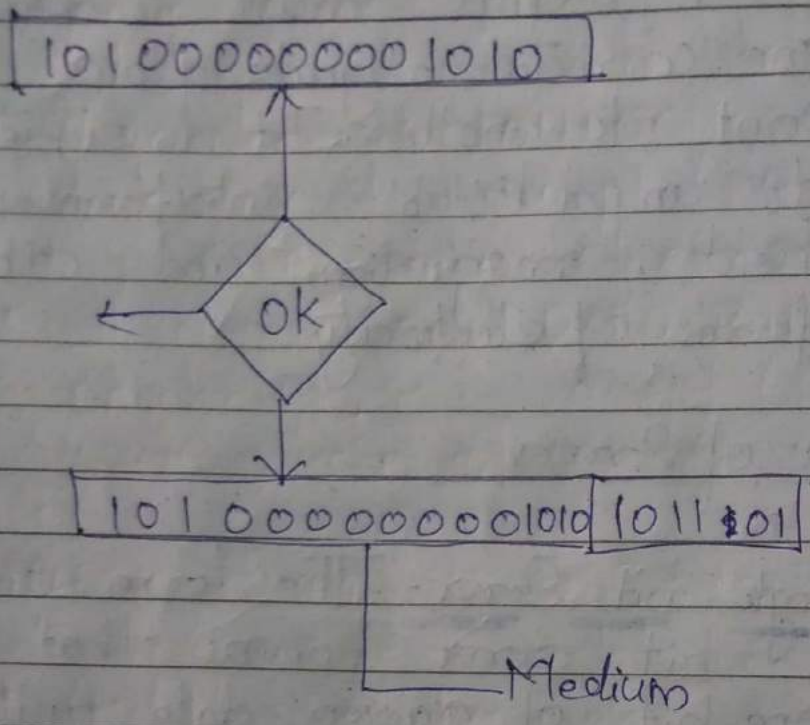
Types of Errors

→ Single bit Error - The term single bit error means that only one bit of a given data unit is changed from 1 to 0 or 0 to 1. 010101 is changed to 110101 here only one bit is changed by single bit error.



DETECTION :- 1) Redundancy - Error detection use the concept of redundancy, which means adding extra bits for detecting errors at the destination ie instead of repeating the entire

data stream, a shorter group of bits may be appended to the end of each unit.



1010000000001010 - data unit
1011101 — Redundancy unit

DETECTION METHODS

→ Parity checks
→ Cyclic redundancy check
→ Hamming code.

PARITY CHECK

A redundant bit called parity bit, is added to every data unit so that the total number of 1's in the unit become even (or odd).

even parity :- When count of 1's is even we keep parity as 0
When count of 1's is odd we keep parity as 1.

Odd parity → When count of 1's is Odd we keep parity as 0
When count of 1's is even we keep parity as 1

By default we will take Even parity.

Total data bit is then passed through parity checking function. If an error is detected the data is rejected.

Ex:- Data to be transmitted = 1011010 1

- 5 1's in the data
- parity bit is 1.

- Transmitted codeword = 10110101 1
- If receiver gets 10110101 1, parity check ok ---- accepted.
- If receiver gets with error 10110000 1 parity check fails ---- reject (ok) ask for frame to be retransmitted.
- If receiver gets 10111001 1 parity check ok ---- accept (Not ok: even number of errors undetected)
- If receiver gets 00110001 1, parity check ok ---- accept (Not ok: even number of errors undetected.

EXAMPLE 2: Data to be transmitted = 1011000

- 4 1's in the data.
- Parity bit is 0
- Transmitted codeword = 101100010

LRC — Longitudanal Redundancy Check.

Add single parity check bits to ~~each row and each column~~, ~~transmit row by row~~

Example data bit = 1110001 1000111
0011001

writing data bits in column.

Data bits

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

LRC

→ transmitted : 11100010100011100011001101011111.

Data to Receiver is —:

11100010100011100011001101011111

May be Receiver receive data with error

11000010100011100011001101011111

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

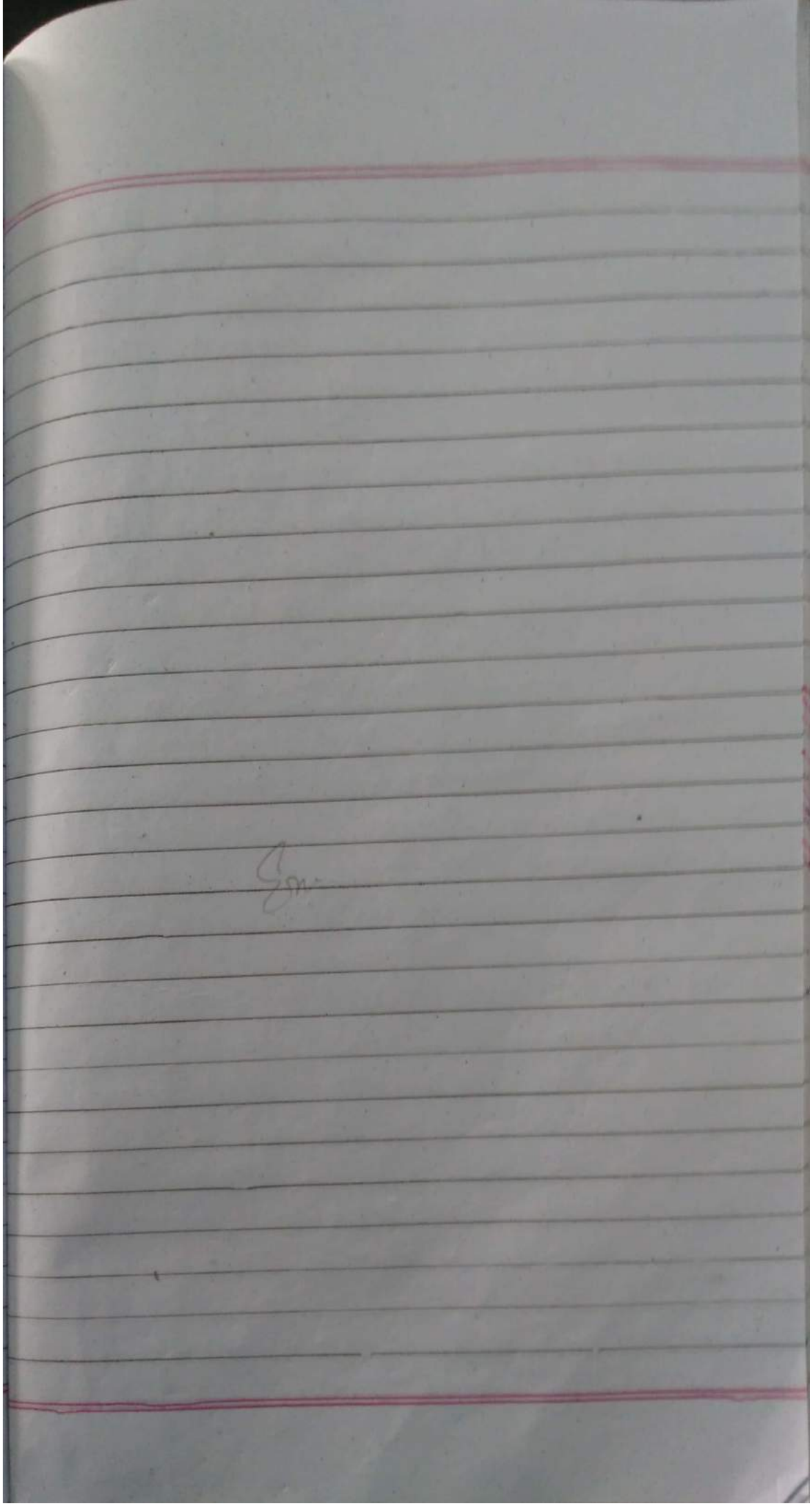
—— Wrong.

Column 3 parity is wrong. So, it detected but it's cannot correct them.

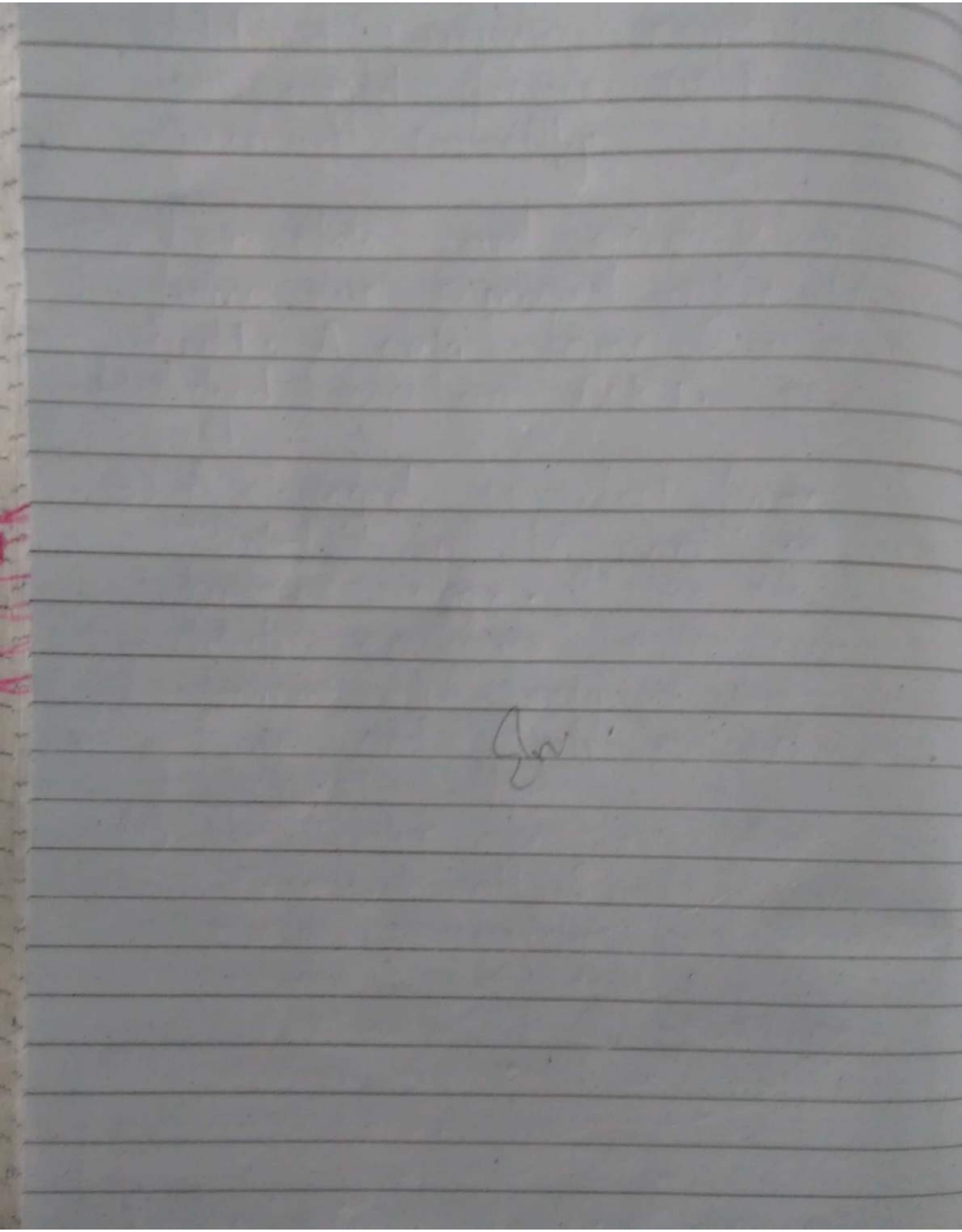
CYCLIC REDUNDANCY CHECK

CRC is based on binary division. In CRC instead of adding bits to achieve the desired parity, a sequence of redundant bits, called the CRC or the CRC remainder, is appended to the end of the data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.

At its destination the incoming data unit is assumed to be intact and is therefore accepted. A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.



$G_{\mathcal{R}}$



ERROR CONTROL

- Error control in the data link layer is based on ARQ (Automatic Repeat request), which is the retransmission of data.
- The term error control refers to methods of error detection and retransmission.
- Anytime an error is detected in an exchange, specified frames are retransmitted. This process is called ARQ.

Flow and Error Control Mechanisms

1) STOP AND WAIT ARQ
2) GO BACK N ARQ
3) SELECTIVE - REPEAT ARQ.

STOP AND WAIT ARQ

This is the simplest flow and error control mechanism. It has following features:

1) The sending device keeps the copy of the last frame transmitted until it receives transmit lost or damaged frames until they are received correctly.

2) Both data and acknowledgement frames are numbered alternately 0 and 1. A data frame 0 is acknowledged by an ACK 1.

3) A damaged or lost frame is treated in the same manner by the receiver. If the receiver detects an error in the received frame, it simply discards the frame and sends no acknowledgement.

4) The sender has a control variable which we call "S", that holds the number of recently sent frame. The receiver has a control variable, which we call "R" that holds the number of the next frame expected.

5) The sender starts a timer when it sends a frame. If an ACK is

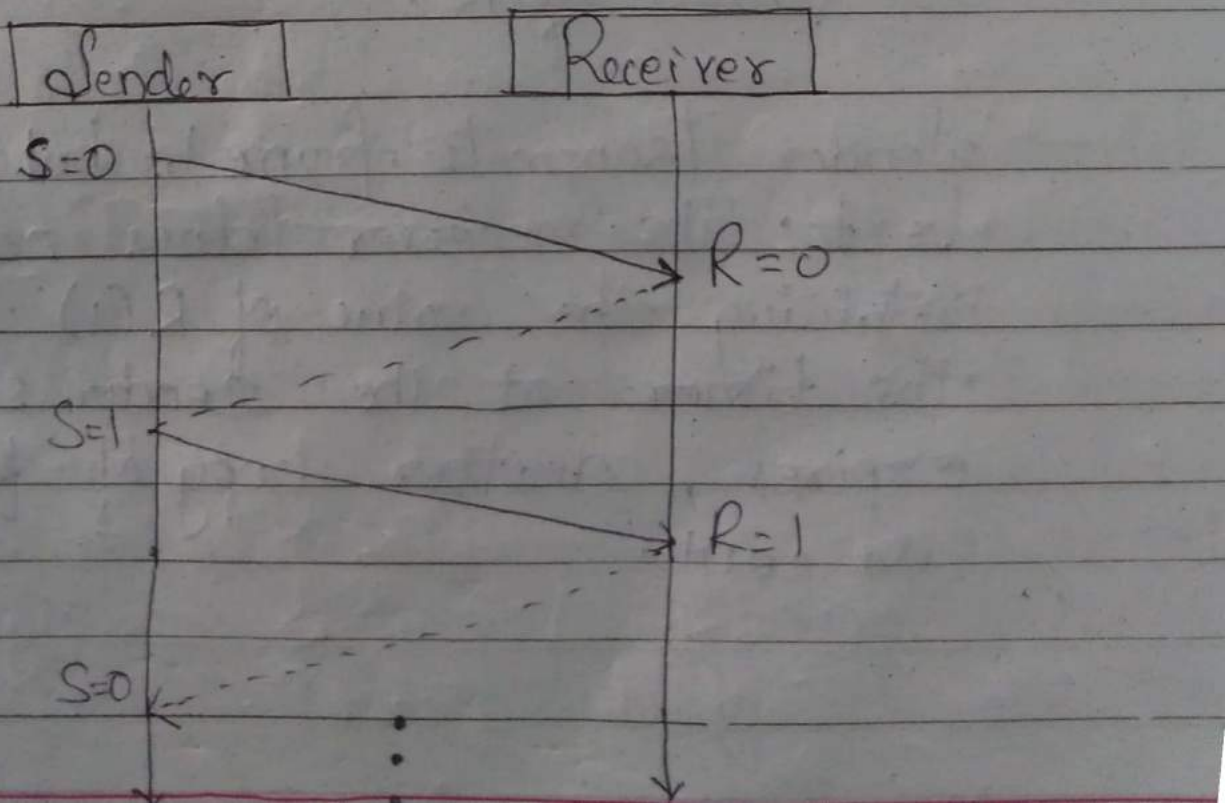
not received within an allotted time period - the sender assumes that the frame was lost or damaged and resends it.

6) The receivers send only positive ACK for frames received safe and sound; it is silent about the frames damaged or lost.

OPERATION :-

The possible operations are :-

a) Normal operation
b) Lost frame
c) ACK lost
d) Delayed ACK.



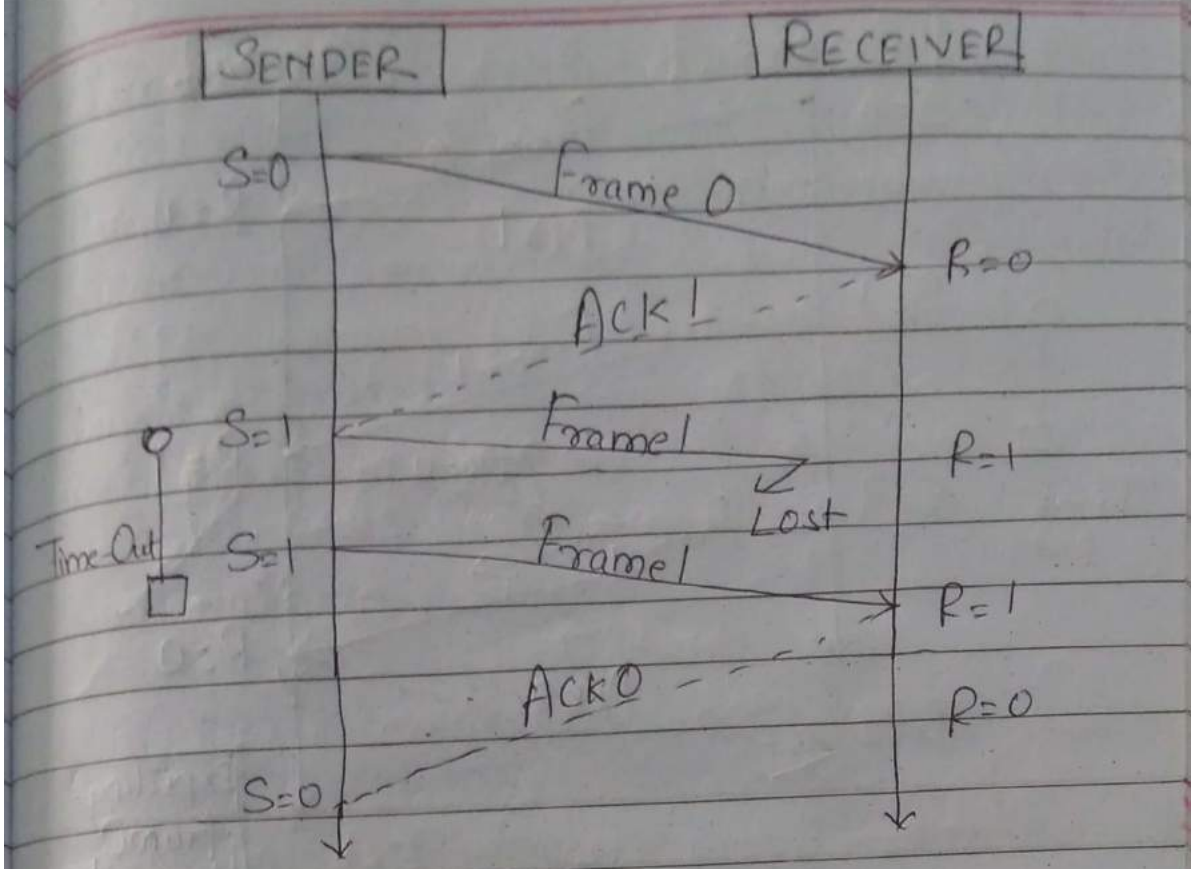
→ The Sender sends frame 0 and wait to receive ACK 1. When ACK 1 is received it sends frame 1 and then waits to receive ACK 0 and so on.

→ The ACK must be received before the time out that is set expires.

Lost or damaged Acknowledgement

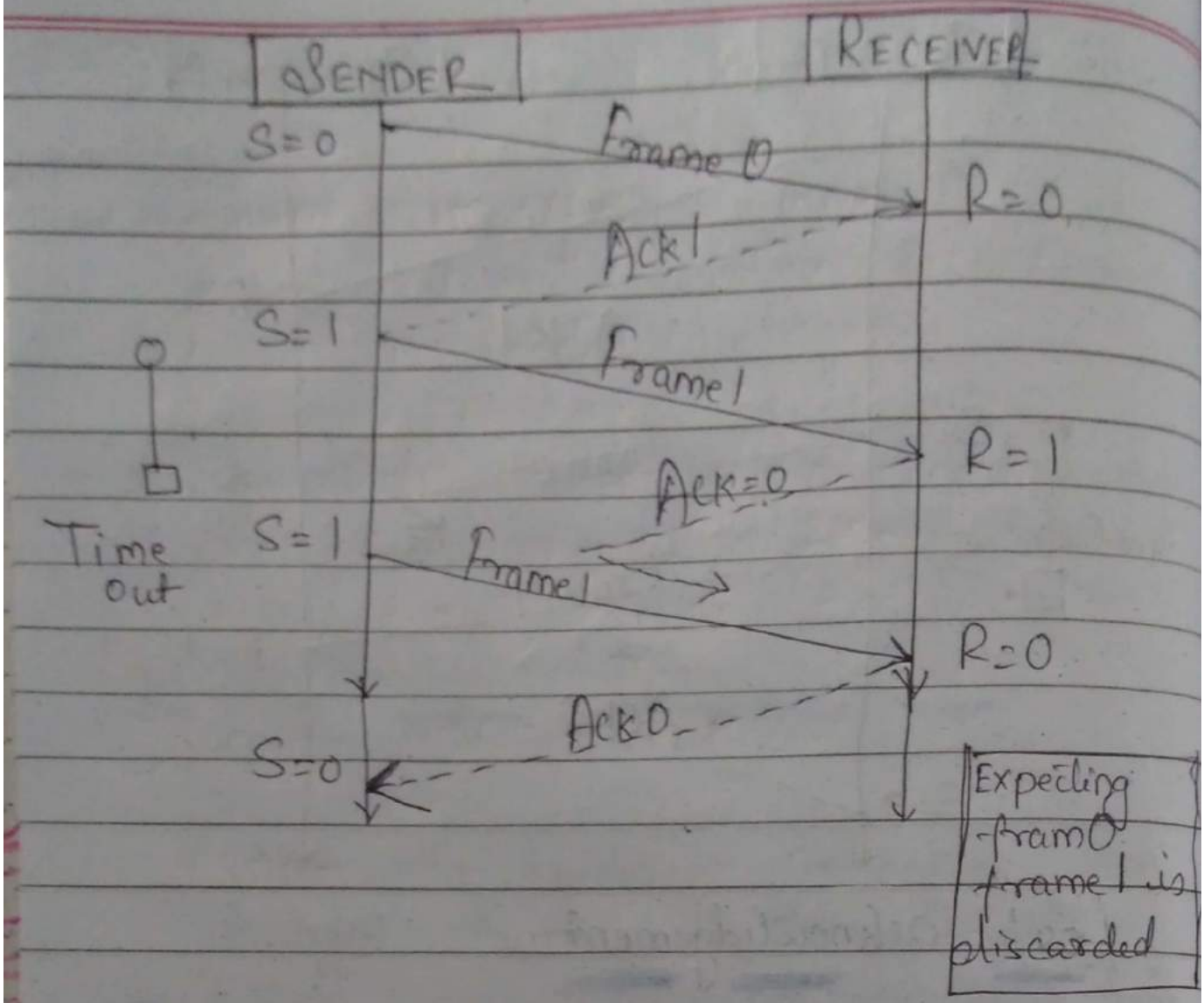
→ When the receiver receives the damaged frame it discards it, which essentially means the frame is lost. The receiver remains silent about a lost frame and keeps its value of "R".

→ Sender transmits frame 1, but it is lost. The receiver does nothing, retaining the value of R(1). After the timer at the Sender site expires, another copy of frame 1 is sent.



Lost acknowledgement

- A lost or damaged ACK is handle in the same by the Sender ; if the Sender receives a damaged Ack it discards it.
- A lost Ack 0. the waiting Sender does not know if frame 1 has been received. When the timer for frame 1 expires the sender retransmits frame 1.
- Receiver has already received frame 1 and is expecting to receive frame 0. Therefore, its silently discards the second copy of frame 1.

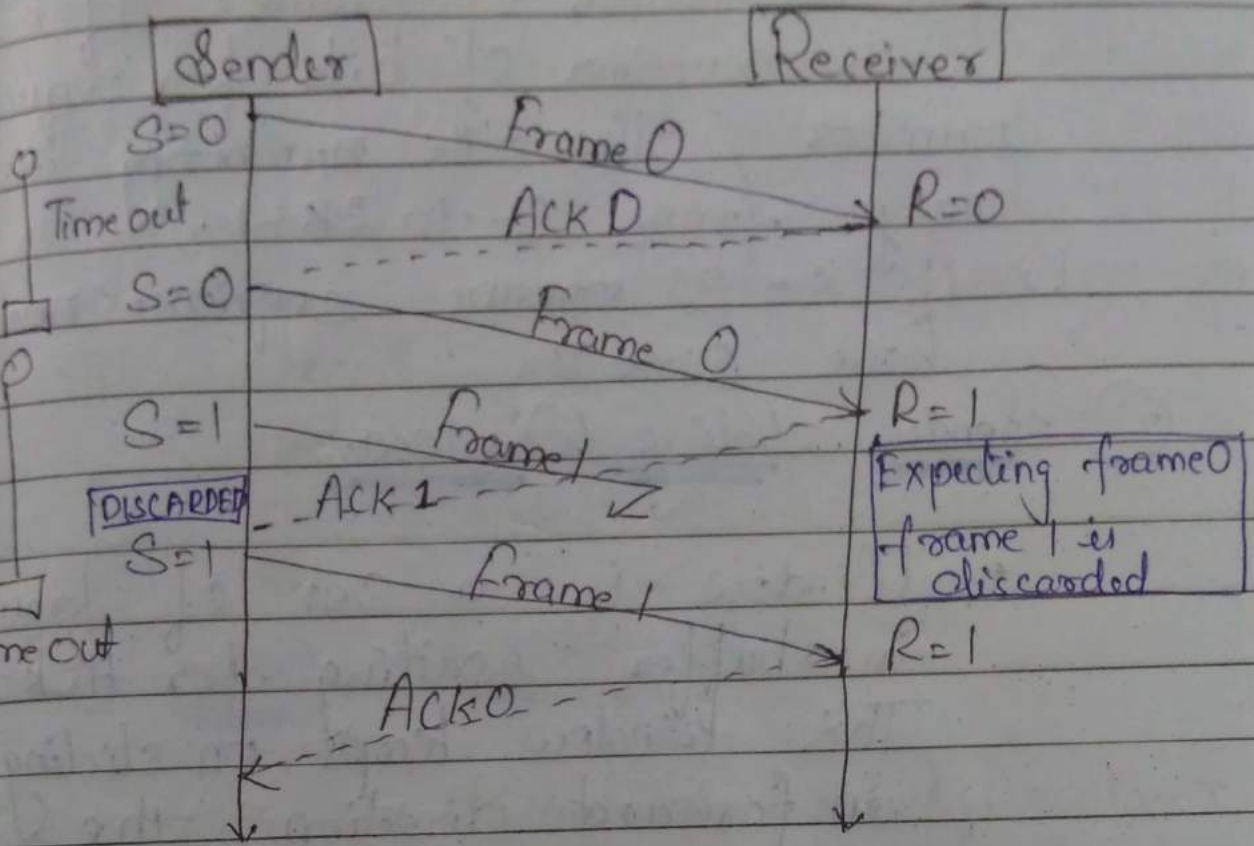


Delayed Acknowledgement

- An Ack can be delayed at the receiver or by some problem with the link. delay of Ack 1; it ids received after the timer for frame 0 as already expired.

- The sender has already retransmitted a copy of frame 0. The receiver expects frame 1 so its simply discard the duplicate frame 0.

- The sender has now received two ACK's one that was delayed and one that was sent after the duplicate frame0 arrived. The second ACK1 is discarded.



GO-BACK-N ARQ

- As in Stop-and-wait protocol senders has to wait for every Ack then next frame is transmitted. But in GO-BACK-N ARQ number of frames can be transmitted without waiting for Ack. A copy of each transmitted frame is maintained until the respective Ack is received.

Features of Go-Back-N ARQ

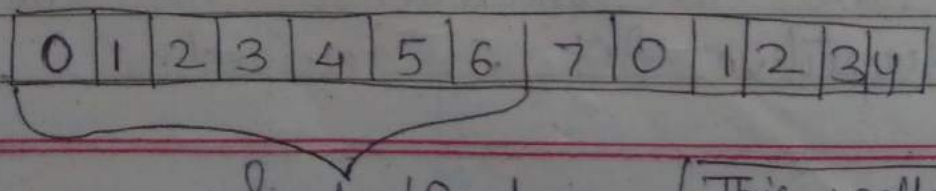
① Sequence numbers:- Sequence numbers of transmitted frames are maintained in the header of frame. If "k" is the number of bits for sequence number, then the numbering can range from 0 to $2^k - 1$.

Ex- if k = 3 means sequence no.s are 0 to 7.

② Sender sliding Window:-

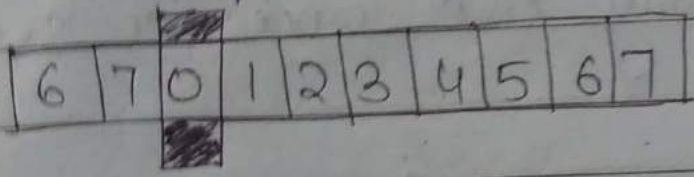
- Window is a set of frames in a buffer waiting for Ack. This window keeps on sliding in forward direction, the window size is fixed. As the Ack is received, the respective frame goes out of window and new frame to sent come into window.

- If sender receives, Ack 4, then it knows frames upto frame 3 were correctly received.



③ Receiver sliding Window:-

In the receiver side size of the window is always one. The receiver is expecting to arrive frame in specific sequence. Any other frame is received which is out of order is discarded. The receiver slides over after receiving the expected frame.



④ Control Variables :-

Sender variables and Receiver variables:

Sender deals with three different variables

S → Sequence number of recently sent frame.

S_F → Sequence number of first frame in the window.

S_L → Sequence number of last frame in the window.

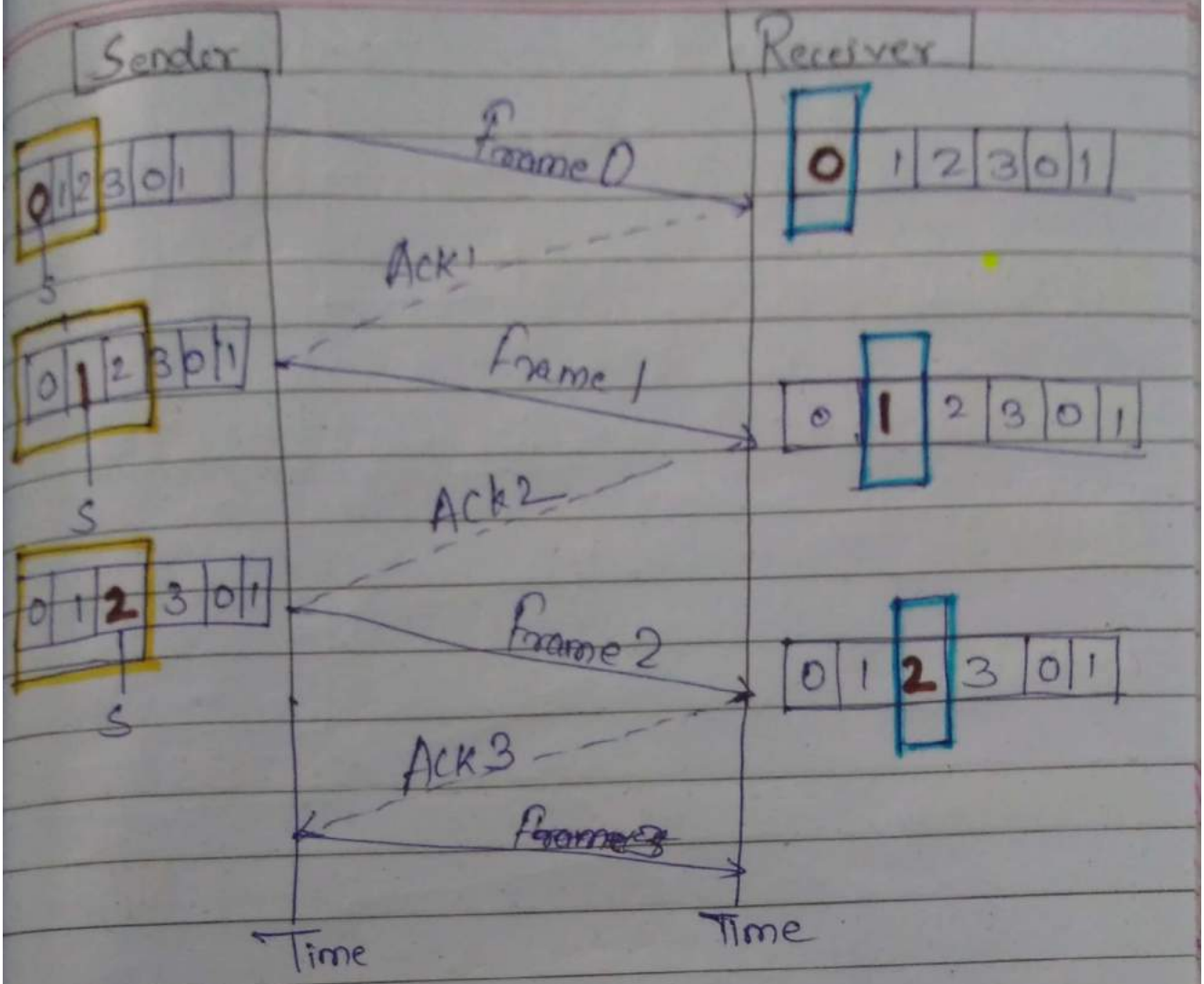
The receiver deals with only one variable R → sequence number of frame expected.

5. Timers :- The sender has a timer for each transmitted frame. The receivers don't have any timer.

6. Acknowledgement :- The receiver responds for frame arriving safely by positive ACK. For damaged or lost frames receiver doesn't reply, the sender has to retransmit it when timer of that frame elapsed. The receiver may ACK once for several frames.

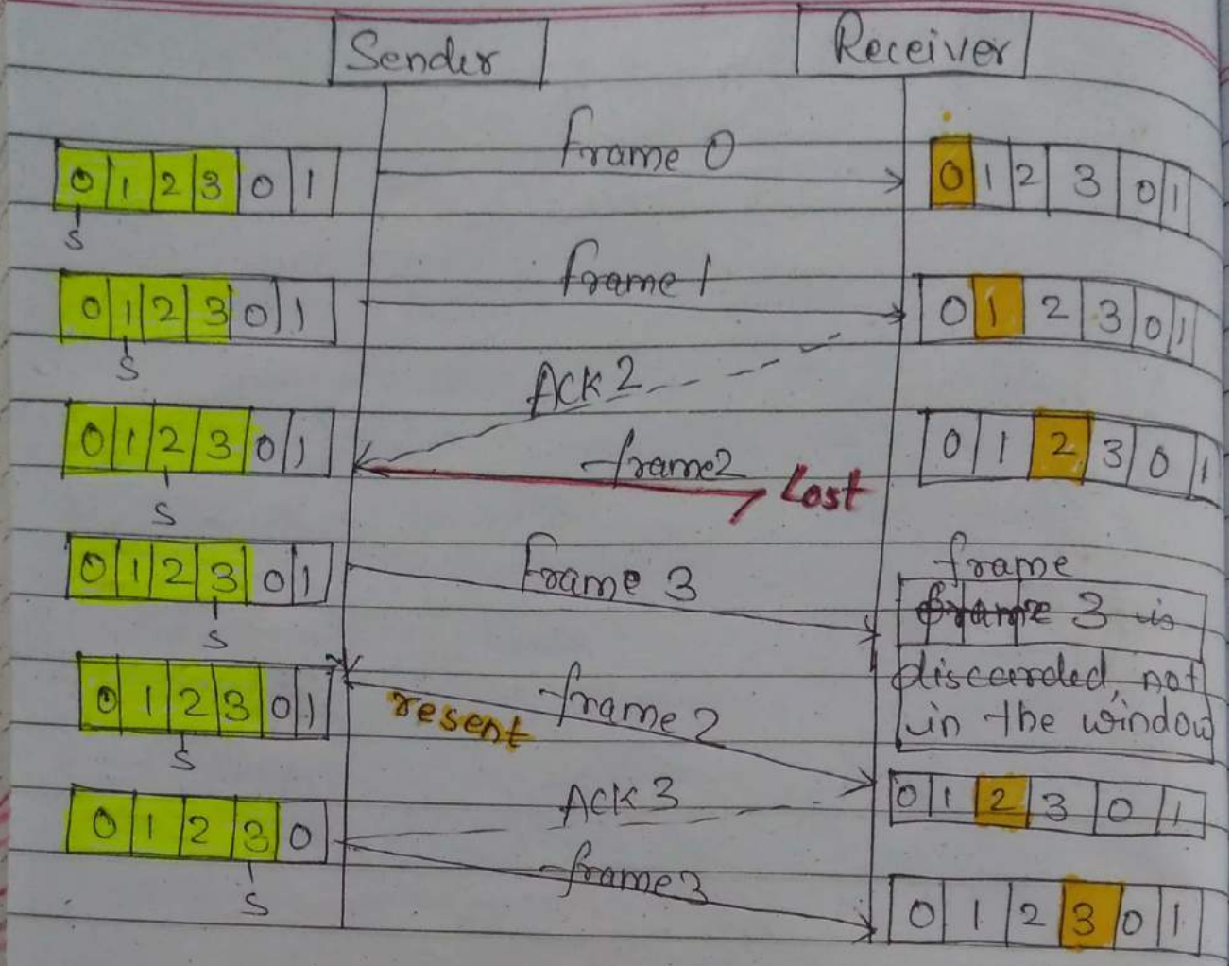
7) Resending frames :- If the timer for any frame expires, the sender has to resend the frame and the subsequent frame also., hence the protocol is called GO-BACK N ARQ.

8) Operation :- The sender keeps track of the outstanding frames and updates the variables and windows as acknowledgements arrive.



Damaged Or lost frame:

In following figure, frame 2 is lost. Note that when the receiver receives frame 3, it is discarded because the receiver is expecting frame 2, not frame 3. After the timer for frame 2 expires at the sender site, the sender sends frame 2 and frame 3.



Damaged or lost Acknowledgement

If an Ack is lost, we can have two situation If the next Ack arrives before the expiration of timer, there is no need for retransmission of frames because Ack are cumulative in this protocol. If the next Ack arrives after the time out, the frame and all the frames after that are resent. The receiver never resends an Acks.

Delayed Acknowledgement

A delayed ACK also triggers the resending of frames.

SELECTIVE REPEAT ARQ :-

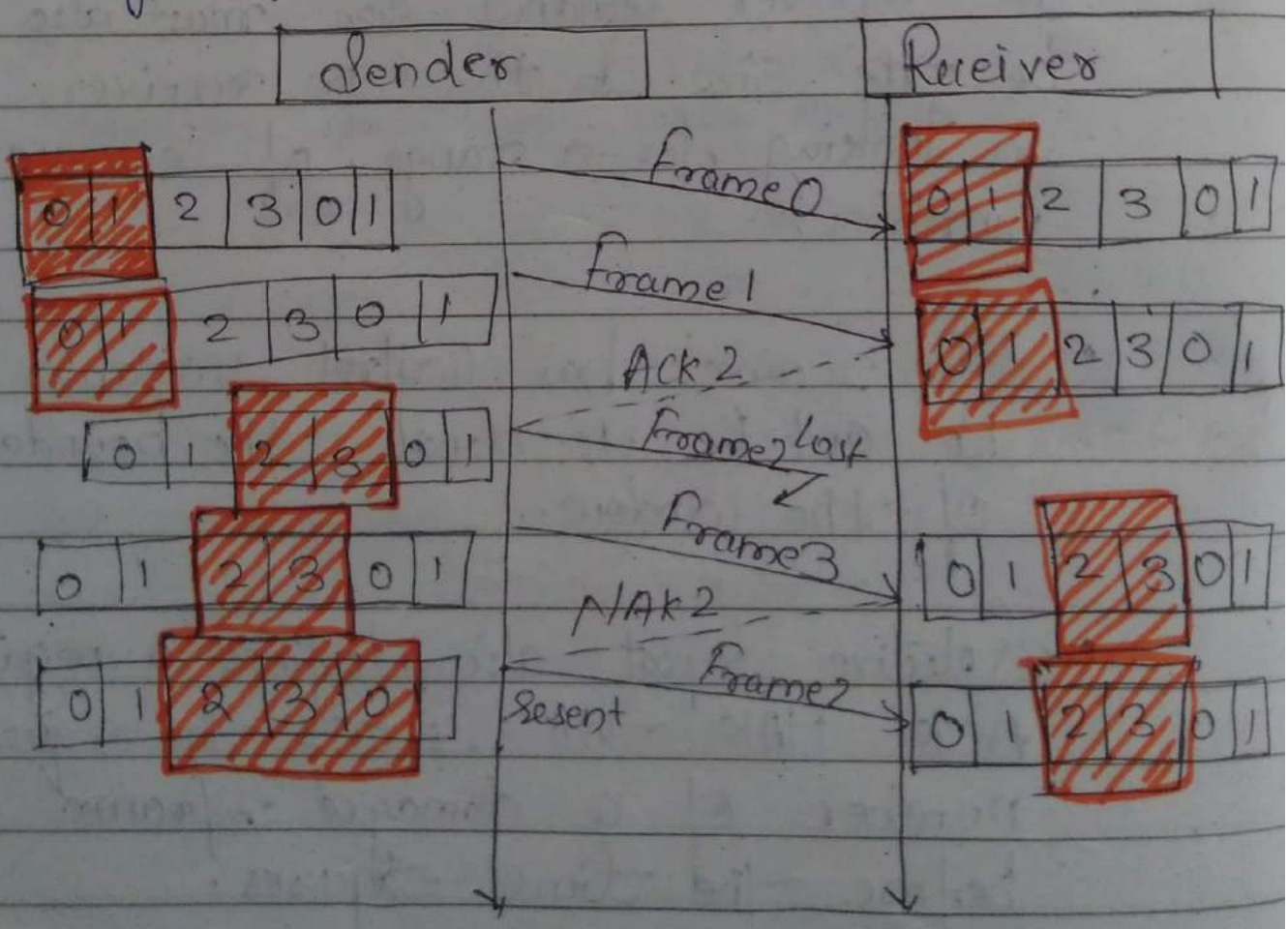
- The configuration and its control variables for this are same as those selective repeat ARQ
- The size of the window should be one half of the value 2^m.
- The receiver window size must also be the size. In this the receiver is looking for a range of sequence numbers.
- The receiver has control variables R_F and R_L to denote the boundaries of the window.
- Selective repeat also defines a negative ACK NAK that reports the sequence number of a damaged frame before the time expires.

Operation

Normal Operation:

Normal Operations of the mechanism with an example of a lost frame.

Frame 0 and 1 are accepted when received it is also accepted for the same reason. However the receiver sends a NAK 2 to show that frame 2 has not been received. When the sender receives the NAK2, it resends only frame 2, which is then accepted because it is in the range of the window.



Lost and delayed ACKs and NAKs

In this sender also sets a timer for each frame ~~out~~ sent. The remaining operation are same as GO-BACK-N ARQ.

~~High-level Data Link Control (HDLC)~~ Protocol

~~HDLC~~

COMPARISON CHART

COMPARISON BASIC	GO-BACK-N	SELECTIVE REPEAT
	Retransmits all the frames that sent after the frame which suspects to be damaged or lost.	Retransmits only those frames that are suspected to lost or damaged.
Bandwidth Utilization	If error rate is high, it wastes a lot of bandwidth.	Comparatively less bandwidth is wasted in retransmitting.
Complexity	Less Complicated	More complex as it require to apply extra logic and Sorting and storage

	N-1	N+1/2
Window size		
Sorting	Sorting is neither required at sender side not at receiver side.	Receiver must be able to sort as it has to maintain the sequence of the frames.
Searching	No searching of frame is required neither on sender side nor on receiver	The sender must be able to search and select only the requested frame.
ACK Numbers	NAK number refer to the next expected frame no.	NAK number refer to the frame last.
Use	It more often used.	It is less in practice because of its complexity

HDLC - High Level Data Link Control Protocol.

→ HDLC operates at layer-2 ie data link layer. It is also used for synchronous PPP connection.

→ It is bit oriented protocol.

→ On transmit side, HDLC receives data from application and delivers it to the receiver on the other side of link.

→ On receiver side, HDLC accepts data and delivers to high level application layer.

→ Both side of HDLC modules exchange control information, encoded into a frame.

→ HDLC protocol embeds information in a data frame that allows devices to control data flow and correct errors. HDLC is an ISO standard developed from SDLC

→

UNIT-4

PROCESS-TO-PROCESS DELIVERY

The Internet model has three protocols at the transport layer: UDP, TCP and SCTP.

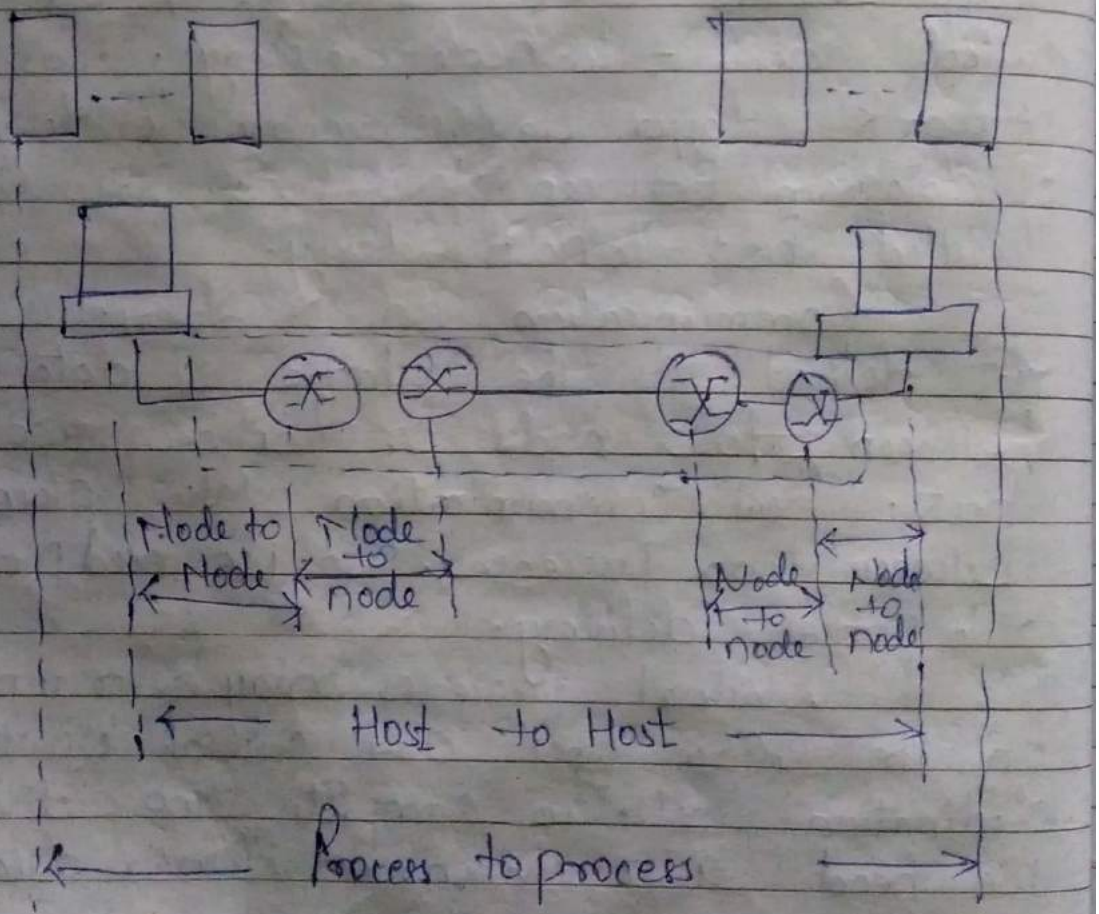
Data link layer is responsible for delivery of frames between two neighboring nodes over a link. This is called node-to-node delivery. The network layer is responsible for delivery of datagrams between two hosts. This is called host-to-host delivery.

Communication on the Internet is not defined as the exchange of data between two nodes or between two hosts. Real communication takes place between two processes. So, we need process-to-process delivery.

Several processes may be running on the source host and several on the destination host. To complete the delivery we need a mechanism to deliver data from one of these processes running on the source ~~host~~ host to the corresponding process running on the destination host.

The transport layer is responsible for process-to-process delivery the delivery of a packet, part of message, frame one process to another.

Node to Node : Data link layer
Host to Host : Network layer
Process to process : Transport layer



Services provided by Transport Layer are :-

1) Connection - oriented communication
2) Reliability
3) flow control
4) Congestion avoidance
5) Multiplexing
6) Process - to - process delivery.

Transport Layer is responsible for process - to - process delivery. Real communication takes place b/w two processes (application programs). The processes communicate in a client/server relationship.

To achieve process - to - process communi -cation, the client/server paradigm is used i.e A process on the local host is called client & process on the Remote host is called server. So for communication to happen, we need.

→ local host
→ local process
→ Remote host
→ Remote process

~~Addressing~~

ADDRESSING :

At data link layer, we need MAC address to choose one node among several nodes if the connection is not point-to-point. A frame in the data link layer needs a destination MAC address for delivery and a source address for the next node's reply.

At network layer we need an IP address to choose one host among millions. A datagram in the network layer needs a destination IP address for delivery and a source IP addresses for the destination's reply.

At transport layer, we need a transport layer address, called a port number, to choose among multiple processes running on the destination host. The destination port number is needed for delivery; the source port number is needed for the reply.

CLIENT - SERVER

Client program defines itself with a port number, chosen randomly by the transport layer software running on the client host. This is the ephemeral

Server process must define itself with a port number. This port number, however, cannot be chosen randomly. If computer at server site runs a server process and assigns a random number as the port number, the process at the client site that wants to access that server and use its service will not know the port number.

IANA → (Internet Assigned Number Authority) divided the port numbers into three ranges: well known, registered and dynamic (or private)

→ Well-known ports: The ports ranging from 0 to 1023 are assigned and controlled by IANA. These are well-known ports.

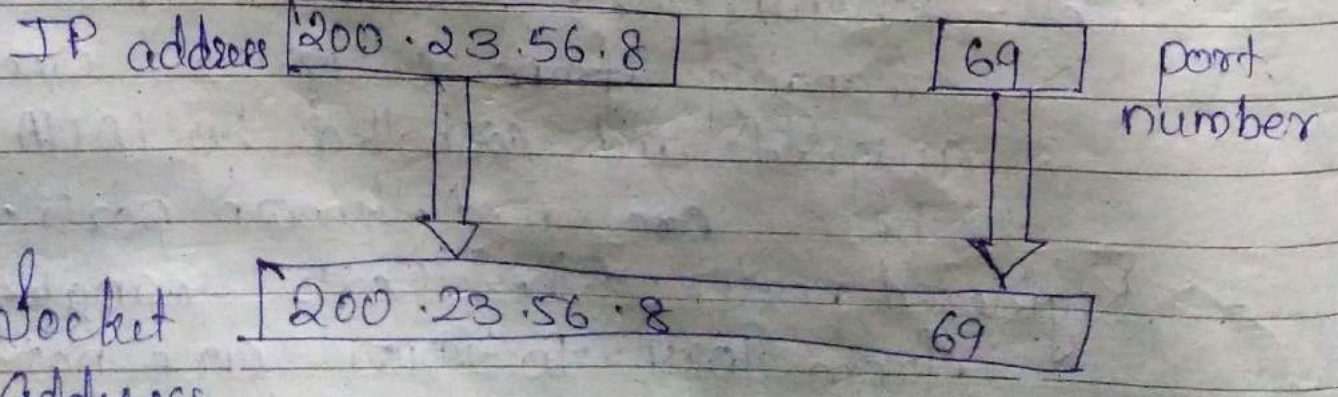
→ Registered ports: The ports ranging from 1024 to 49,151 are not assigned or controlled by IANA.

They can only be registered with IANA to prevent duplication.

→ Dynamic ports : The ports ranging from 49,152 to 65,535 are neither controlled nor registered. They can be used by any process.

Socket Addresses :-

Process-to-process delivery needs two identifiers, IP address and the port number at each end to make a connection. The combination of an IP address and a port number is called a socket address. The client socket address defines the client process uniquely just as the server socket address defines the server process uniquely just as the server socket address defines the server process



TCP (Transmission Control Protocol)

→ TCP is reliable, connection-oriented ordered & error-checked delivery of a station.

→ TCP resides in Transport layer.

→ TCP is a connection-oriented protocol because it first establishes an end-to-end communication session before any data may be send.

→ TCP is a protocol that make sure the data has been well delivered in the correct order.

→ There is also sequence number to assemble the Packets in the original order.

→ Packets may use different paths to reach the receipent, or a corrupted packets need to be resend.

→ ie the Recipient might get the pack in the wrong order, the sequence number make sure when resembling packets are in the correct order.

→ One other interesting feature of TCP is the windows handling the rate of data transmission between two devices is managed by a windowing system to prevent a fast sender from transmitting more data that can be supported by the receiving.

→ TCP is a connection-oriented service ie

1) The two TCP's establishes a connection between them
2) Data are exchanged in both directions
3) The connection is terminated.

→ TCP offers full-duplex service in which data can flow in both directions at the same time

→ Each TCP has a sending buffer & receiving buffers and segments move in both directions.

→ TCP is a reliable transport protocol It uses an acknowledgement mechanism to check the safe and sound arrival of data.

→ TCP uses Numbering system (sequence number & acknowledgement number) to keep track of the segments being transmitted or received in order.

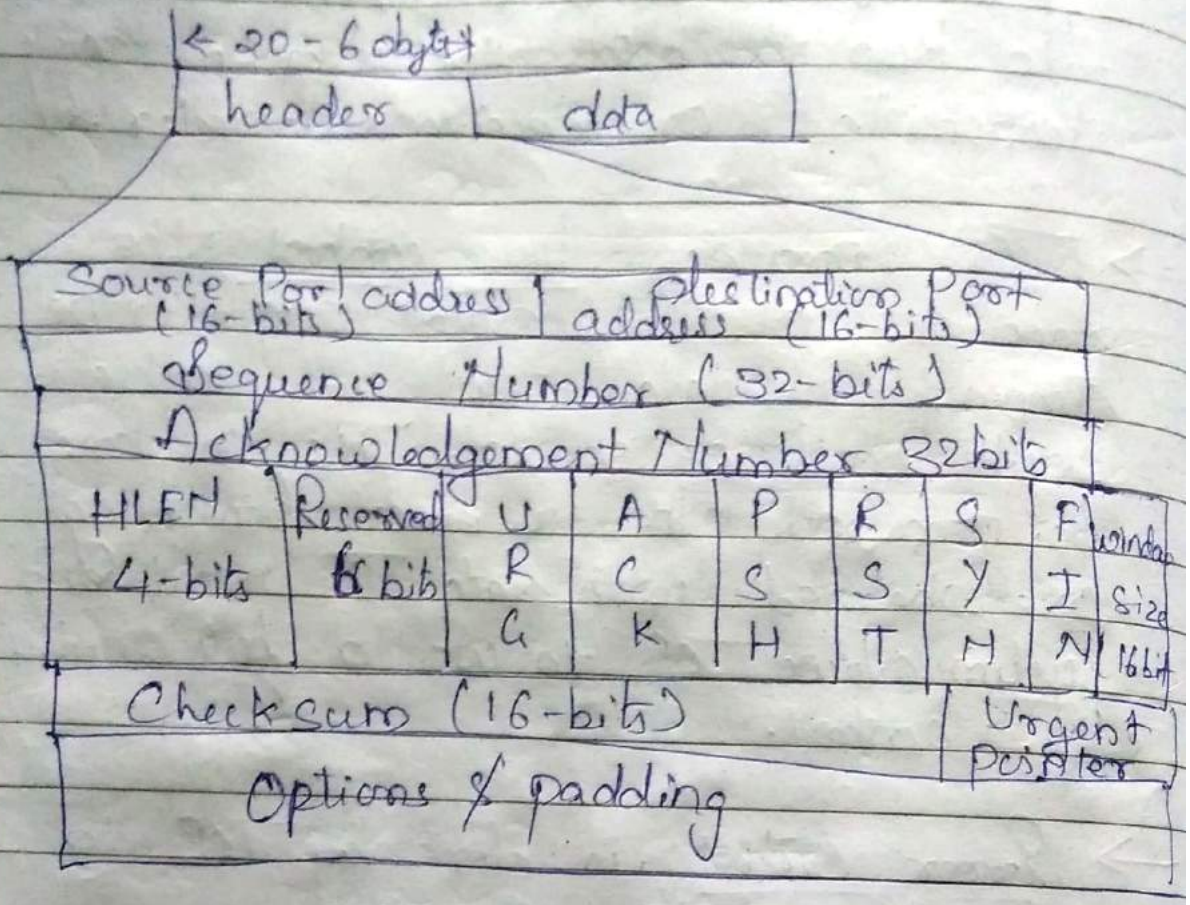
→ TCP provides flow control the receiver of the data controls the amount of data that are to be sent by the sender. This is done to prevent the receiver from being overwhelmed with data. The numbering system allows TCP to use a byte oriented flow control.

→ Error control is done by TCP to provide reliable services.

→ TCP does Congestion control in the N/w ie the amount of data sent by a sender is not only controlled by the receiver (flow control) but is also determined by the level of Congestion in the N/w.

→ The data in the Transport layer is known as segments.

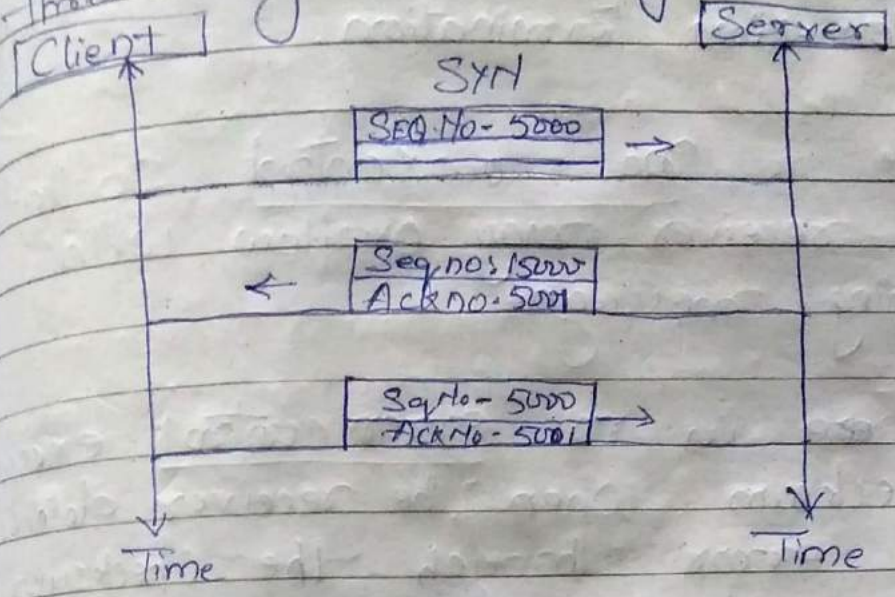
TCP segment format :-



Checksum — used for error control
Reserved — reserved for future use
Window size — Represents the size of the window in bytes
URgent pointer — ~~It~~ is field is valid only when URG bit is set to 1

ACK — Acknowledgement is valid
PSH → Request for push (push the data)
RST — Reset the connection
SYN — Synchronize Sequence Number
FIN — Terminates the connection.

TCP establish connection by using three way handshaking method



User Datagram Protocol (UDP)

UDP is called a connectionless, unreliable transport protocol.

→ UDP is very simple protocol using a minimum of overhead.
→ If a process want to send a small message & doesnot care much about reliability can then UDP

UDP Operations are :-
→ It provides a connectionless services ; here each user datagram sent by UDP is an independent datagram. (ie - the user datagrams

are not numbered) and also there is no connection establishment and no connection termination.

(2) There is no flow control so that the receiver may overflow with incoming messages

(3) There is no error control except checksum. When the receiver detects an error through the checksum, the user datagram is silently discarded.

Uses of UDP are:-

(1) UDP is suitable for a process that requires simple request response communication and with little flow and error control mechanism.

(2) UDP is suitable for multicasting
(3) UDP is used for management process such as SNMP.
(4) UDP is used for some route updating protocols, such as RIP (Routing information protocol)

~~SCAPE~~

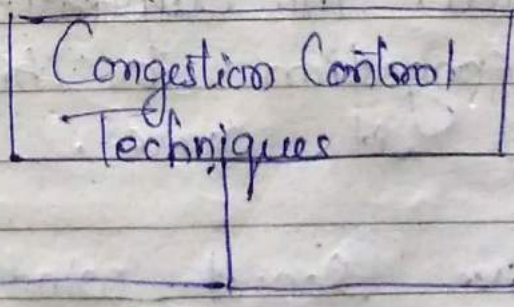
CONGESTION

A state occuring in network layer when the message traffic is so heavy that it slows down network response time.

Effects of Congestion

→ As delay increases, performance decreases
→ If delay increases, retransmission occurs making situation worse.

Congestion control refers to the techniques used to control or prevent congestion. Congestion techniques are broadly classified into two categories.



1) Retransmission Policy :- It is the policy in which retransmission of the packets are taken care. If the sender feels that a sent packet is lost or corrupted the packet needs to be retransmitted. This transmission may increase the Congestion in the n/w.
To prevent congestion, retransmission timers must be designed to prevent Congestion and also able to optimize efficiency.

2) Window Policy :- The type of window at the sender side may also affect the congestion. Several packets in Go-back-n window are resent, although some packets may be received successfully at the receiver end side. This duplication may increase the congestion in the network and making it worse.

Selective Sepeat window should be adopted as it sends the specific packet that may have been lost.

3) Discarding Policy :- discarding policy adopted by the routers is that the routers may prevent Congestion and at the same

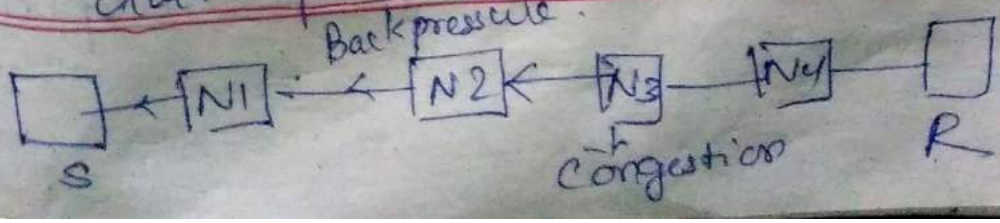
time partially discards the corrupted or less sensitive package and also able to maintain the quality of a message.

4) Acknowledgment Policy :- Acknowledgement policy imposed by the receiver may also affect congestion. Receiver should send acknowledgement for N packets rather than sending acknowledgement for a single packet.

5) Admission Policy :- In admission policy a mechanism should be used to prevent congestion. Switches in a flow should first check the resource requirement of a network flow before transmitting further.

CLOSED LOOP CONGESTION CONTROL

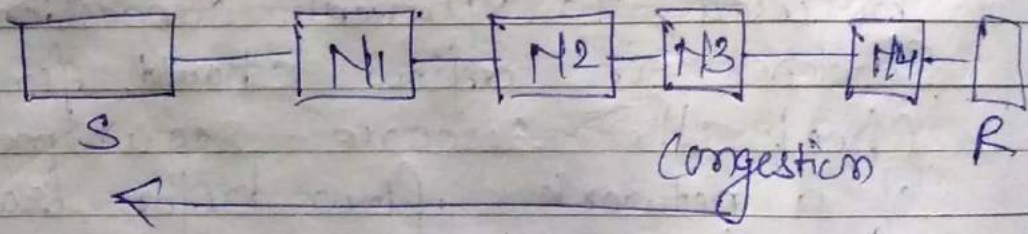
(1) Back pressure :- Back pressure is a technique which a congested node stop receiving packet from upstream node or nodes to become congested and rejects receiving data from above nodes.



In this 3rd node is congested and stop receiving packets as a result 2nd node may be get congested due to slowing down of the output data flows. Similarly 1st node get congested and informs the source to slow down.

2) Choke packet technique :-

Choke packet technique ~~is applicable to both~~ which packet is sent by a node to inform it of congestion. router directly send choke packet to the source giving it a feedback to reduce the traffic.



3) Implicit Signalling :-

When sender sends several packets and there is no acknowledgment for a while, source assume that there is a congestion.

4) Explicit Signalling :- Difference between Choke packet and ~~that~~ explicit

signalling is that it sends packet to the source or destination to inform about congestion.

Quality of Service (QOS)

→ QOS is the overall performance of a computer network, particularly the performance seen by the users of the network.

→ QOS considered, such as error rates, bit rate, throughput, transmission delay, reliability, jitter etc.

→ Reliability

Lack of reliability means losing a packet or acknowledgement, entails retransmission.

However sensitivity of all application Program not same. ie email, file transfer and internet access have reliable transmission than telephony and audio conferencing.

→ Delay

Source to destination delay is another flow characteristics.

For this case telephony, audio conferencing, video conferencing and remote login need

minimum delay while in file transfer or email is less importance.

→ Jitter

Jitter is variation in delay for packets belonging to the same flow. High jitter means the different between delays is large; low jitter means the variation is small.

→ Throughput

applications that can compensate for variations in bandwidth and delay with large receive buffers, which is often possible for example in video streaming.

TRAFFIC SHAPING

It is a mechanism to control the amount and the rate of the traffic sent to the network.
There are 2 types of traffic shaping algorithms:

1) ~~Leaky Bucket A~~

1) Leaky Bucket Algorithms

Suppose we have a bucket in which we are pouring water in a random order but we have to get water in fixed rate. for this we will make a hole at the bottom of the bucket. The input rate can vary but the output rate remains constant.

In networking a technique in which Burstly data are stored in the bucket and sent out at an average rate.

Algorithms

→ Leaky bucket algorithms used to control rate in a network.

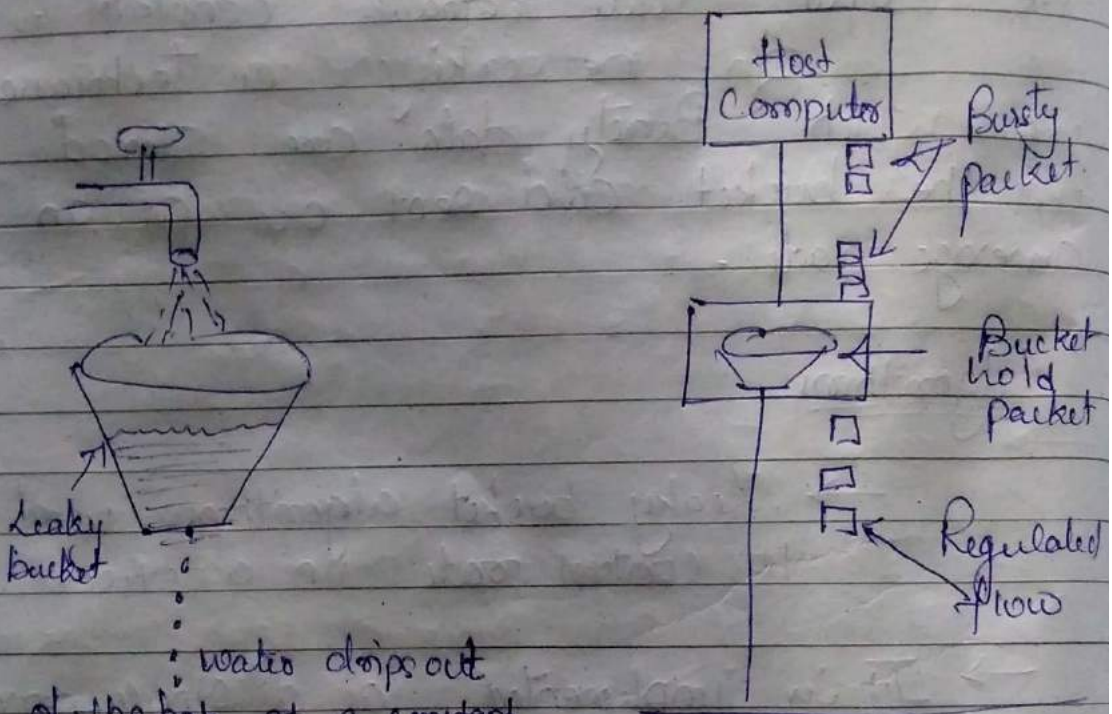
→ It is implemented as a single server queue with constant service time.
→ If the bucket (buffer) overflows then packets are discarded.
→ The input rate is vary but the output rate is fixed.

- Step 1: Initialize the counter to 'n' at every tick of clock.

Step 2: If 'n' is greater than the size of packet in the front of queue

Send the packet into the network and decrement the counter by size of packet. Repeat the step until "n" is less than the size of the packet.

Step3:- Reset the counter and goto step-1



Example:- Let n= 1000

Packet = | 200 | 700 | 500 | 450 | 400 | 200 |

Since n > front of Queue is

n > 200

∴ n = 1000 − 200 = 800

Packet size of 200 is sent to n/w

| 200 | 700 | 500 | 450 | 400 |

Now, n > front of queue ie n > 400

∴ n = 800 − 400 = 400

Packet Size 400 is sent to the N/w

200	700	520	450

Since n < front of queue

∴ the procedure is stop

and we initialize n = 100 on another tick of clock.

This procedure is repeated until all packet sent

Ex2. Consider a frame relay n/w having a capacity of 1Mb and data is input at the rate of 25 mbps. Calculate 1) time 2) if o/p rate is 2 mbps, time taken to empty bucket.

Ans2. C is capacity of bucket = 1mb

Data input rate = 25 mbps

output rate = 2 mbps

1) T = C/input rate = 1/25 = 40msec

2) T = C/output rate = 1/2 = 500msec.

HDLC - High Level Data Link Control Protocol.

→ HDLC operates at layer-2 ie data link layer. It is also used for synchronous PPP connection.

→ It is bit oriented protocol.

→ On transmit side, HDLC receives data from application and delivers it to the receiver on the other side of link.

→ On receiver side, HDLC accepts data and delivers to high level application layer.

→ Both side of HDLC modules exchange control information, encoded into a frame.

→ HDLC protocol embeds information in a data frame that allows devices to control data flow and correct errors. HDLC is an ISO standard developed from SDLC.

→ There are two transfer Mode.
1) Normal Response Mode
2) Asynchronous Balanced Mode.

Types of frames in HDLC

1) Information frames (I-frames)
2) Supervisory frames (S-frames)
3) Unnumbered frames (U-frames)

(1) Information frames :-

- I-frames carry user's data and control information about user's data.
- I-frame carries user data in the information field.
- The first bit of control field is always zero, ie the presence of zero at this place indicates

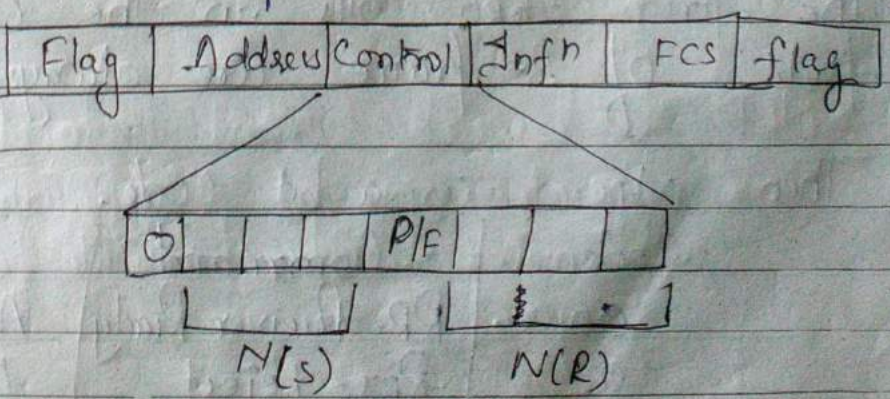
that it is I-frame.

- Bit number 2, 3 & 4 in control field is called N(s) that specifies the sequence number of the frame. Thus it specifies the number of the frame that is currently being sent. Since it is 3 bit field, Only eight sequence numbers are possible 0, 1, 2, 3, 4, 5, 6, 7.

- Bit number 5 in control field is P/F ie Poll/Final ~~and is used for these two purposes. It has meaning only when it is set ie when P/F = 1~~ ie Poll/final and is used for these two purposes It has meaning only when it is set ie P/F = 1

→ it means poll when frame ~~is~~ Sent Consist of receiver address

→ it means final when frame consist of Sender address.



Flag → Starting and ending of frame

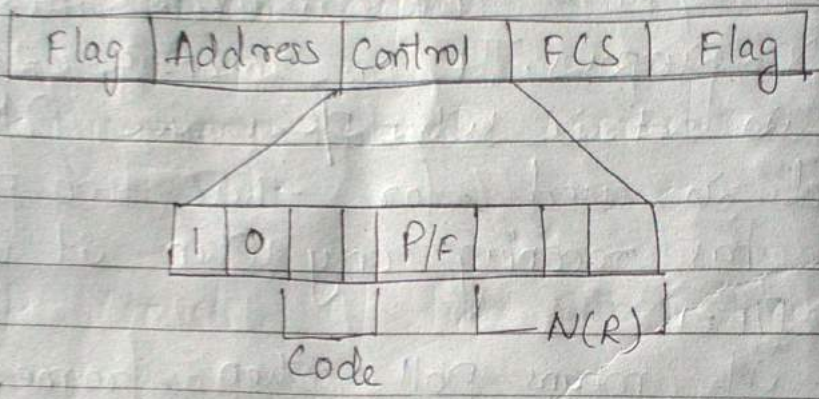
Address → Sender or Receiver address

FCS → CRC Error correction and detection

Information → Data field

(2) Supervisory frame :-

- S-frame carries control information primarily data link layer flow and error controls.
- It does not contain information field.
- The format is



- The first two bits in the control field of S-frame are always 10.
- Then there is a bit code.

Code	Command	
00	RR - Receiver Ready	Ack
01	REJ - Reject	NAK
10	RNR - Receiver Not Ready	used for flow control
11	SREJ - Selective Reject.	

SREJ - Selective Reject - Indicates to the Transmitter that it should retransmit the frame indicated in the N(R) subfield.

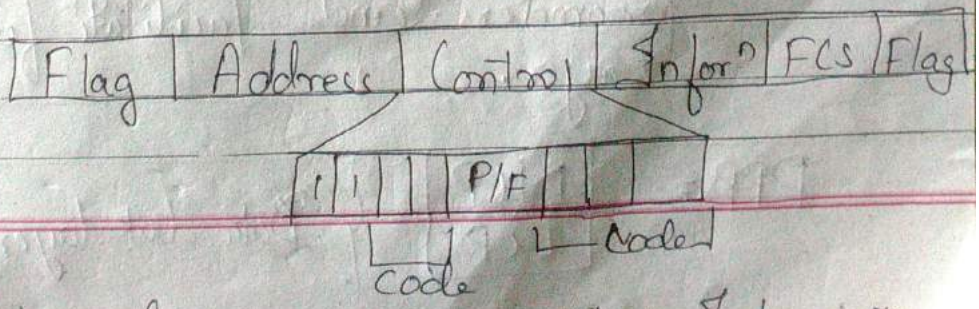
3) Un-numbered frame -

- U-frames are reserved for system management and information carried by them is used for managing the link.

- U-frames are used to exchange session management and control information both two connected devices.

- U-frame is identified by the presence of 11 in the first and second bit position in control field.

- i-frame doesn't contain any data so, no N(R) and N(S)



Inf^n - Session and Control Mgmt Information

Point To Point Protocol (PPP)

PPP is an open standard protocol that is mostly used to provide connection over point-to-point serial links. The main purpose of PPP is to transport layer 3 packets over a Data Link layer point-to-point link.

→ Asynchronous serial connection like plain old telephone service (POTS) dial-up.

→ Synchronous serial connection like ISDN.

PPP consists of two sub-protocols:-

→ LCP (Link Control Protocol):- set up and negotiate control options on DLL. After finishing setting up the link.

→ NCP (Network Control Protocol):- negotiate optional configuration parameters and facilitate for N/w Layer.

PPP = [NCP / LCP] } Data link layer

Establish a PPP session

Before a PPP connection is established the link must go through three phases of session establishment.

1) Link Establishment Phase: Each PPP device sends LCP packets to configure and test the data link.

2) Authentication Phase: If authentication is enabled, either PAP or CHAP will be used.

3) Network layer protocol phase: PPP sends NCP packets to choose and configure Network layer protocol to be encapsulate and sent over the PPP data link.

PAP → Very simple authentication protocol. The client who wants to access a server sends its username and password in clear text. The server checks the validity of the username and either accepts or denies Conn°.

CHAP → CHAP is an PPP authentication

Protocol which is far more secure. With CHAP, protocol begins with a random text sent from the server. After receiving challenge, client uses its password to perform hash algorithm. the result is sent back to server.

At the server side, the same algorithm is used to generate its own result. If two results match, the passwords must match too.

ALOHA :-

Aloha is a system for coordinating and arbitrating access to a shared communication Net channel. developed in 1970 by Norman Abramson at university of Hawaii.

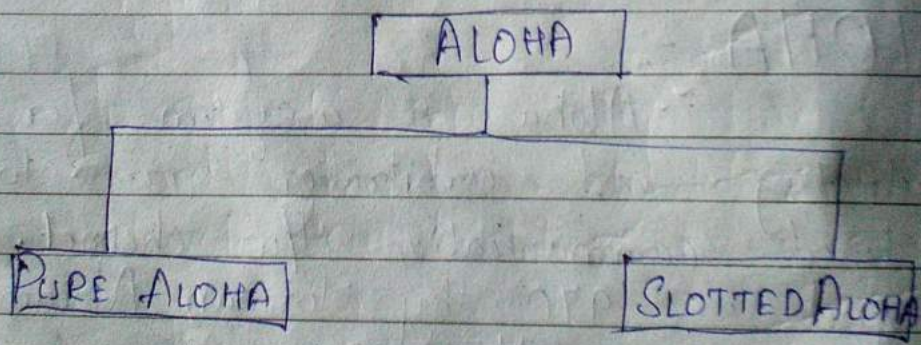
A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to

transmit on the channel at the same time.

Aloha means "Hello". Aloha is a multiple access protocol at the data-link layer and proposes how terminal access the ~~developed~~ medium without interference or collision.

A node transmit whenever data is available to send. If another node transmits at the same time, a collision occurs and the frames that were transmitted are lost.

There are two different versions of ALOHA



Pure Aloha :-

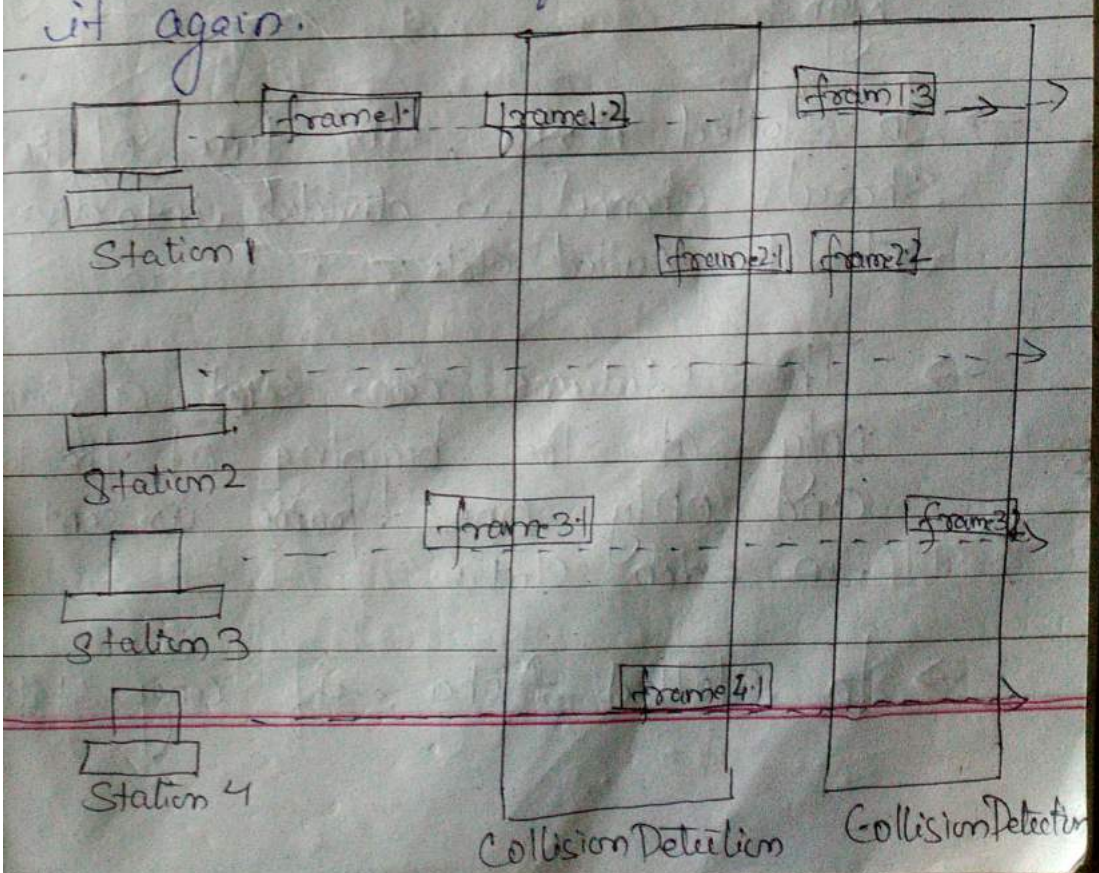
→ In pure ALOHA, the stations transmit frames whenever they have data to send.

→ When two or more stations transmit simultaneously, there is collision and the frames are destroyed

→ In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.

→ If acknowledgement is not received within specified time the station assumes that the frame (or acknowledgement) has been destroyed.

→ If the frame is destroyed because of collision the station waits for a random amount of time and sends it again.



→ Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be damaged.

→ If first bit of the new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be transmitted.

Slotted Aloha :-

→ Slotted Aloha is to improve the efficiency of pure Aloha as chances of collision in pure Aloha are very high.

→ In slotted Aloha, the time of the shared channel is divided into discrete intervals called slots.

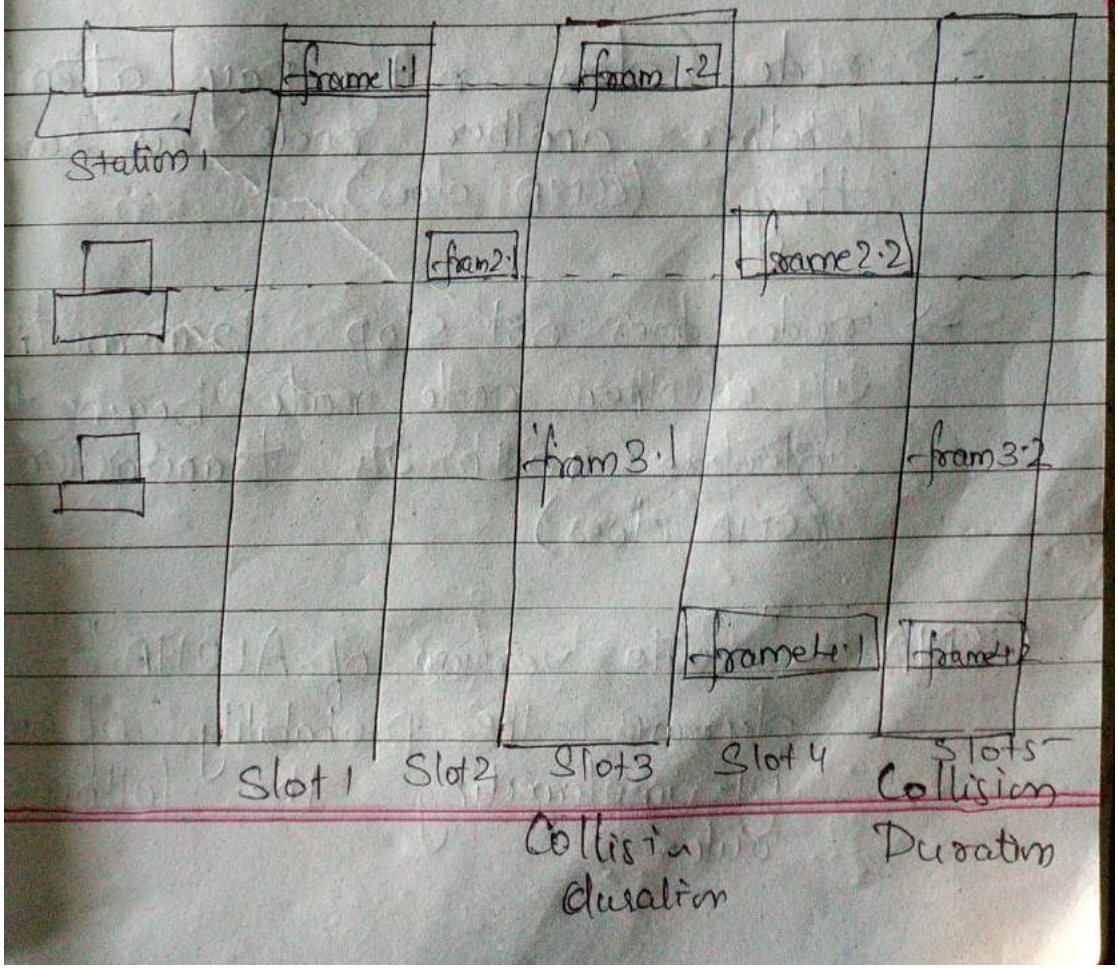
→ The stations can send a frame only at the begining of the slot and only one frame is sent in each slot.

→ In slotted Aloha, if any station

is not able to place the frame onto the Channel at the beginning of the slot ie It misses the time slot then the station has to wait until the beginning of the next time slot.

→ In slotted Aloha, there is still a possibility of collision if two stations try to send at the begining of the same time slots.

→ slotted Aloha still has an edge over pure Aloha as chances of collision are reduced to one-half.



CSMA/CD

To reduce the impact of collisions on the network performance, Ethernet uses an algorithm called CSMA with Collision Detection (CSMA/CD). CSMA/CD is protocol in which the station senses the carrier or channel before transmitting frame.

Aloha disadvantage :-

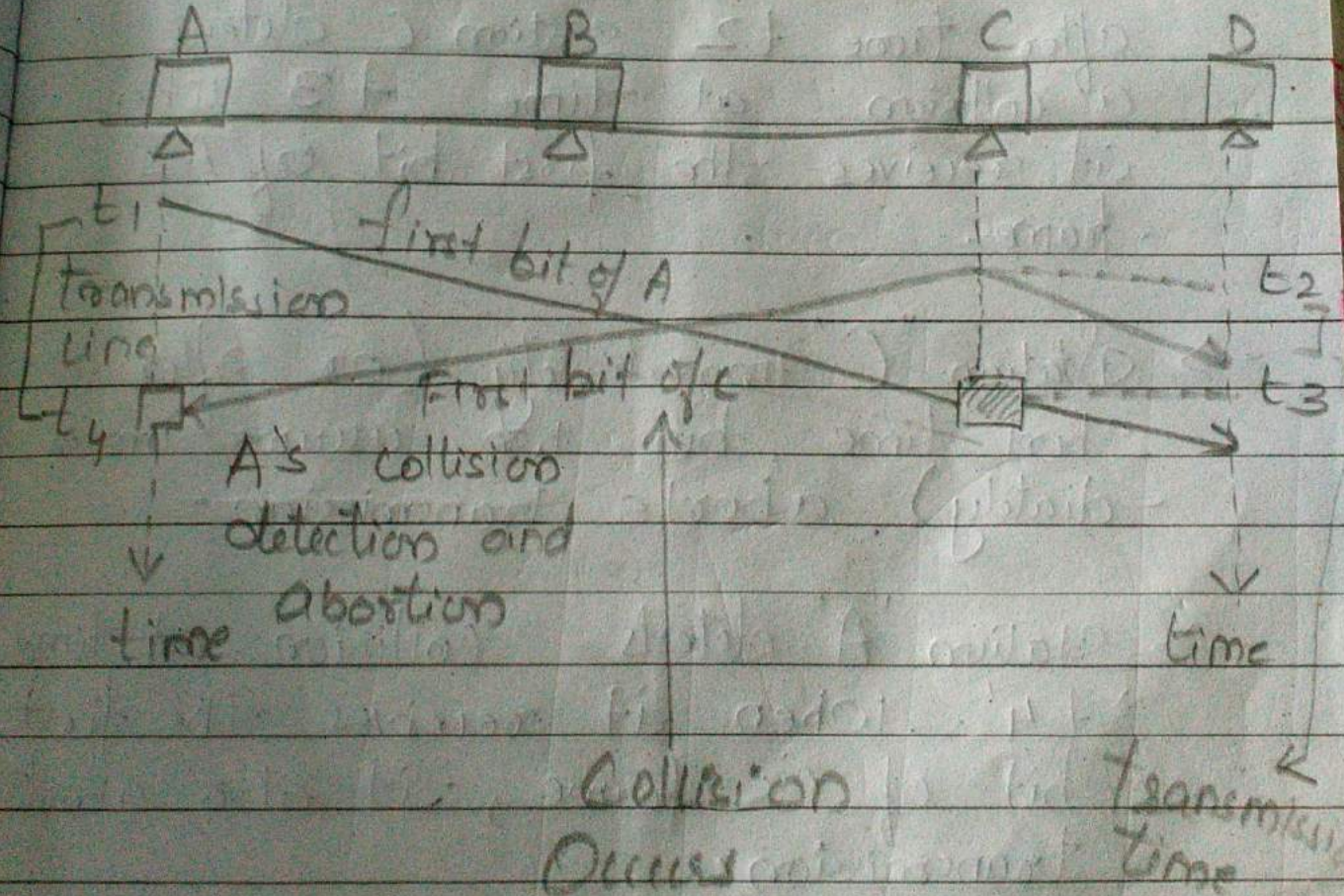
→ Node decides to transmit independently of other nodes attached to broadcast channel.

→ node does not pay attention whether another node is transmitting (CSMA does)

→ node does not stop transmitting if another node, node begins to interfere with its transmission (CSMA does)

CSMA - "Polite version of ALOHA" - decreases the probability of collision by implementing the following rule :-

- Carrier Sensing - node listens to the channel before transmitting
- if sensed channel idle ⇒ transmit entire frame
- if sensed channel busy ⇒ back-off (defer transmission) and keep sensing or sense the channel again after a random amount of time.



- → At time t1, station A has executed its persistence procedure and starts sending the bits of its frame.

→ At time t2, station C has not yet sensed the first bit sent by station "A".

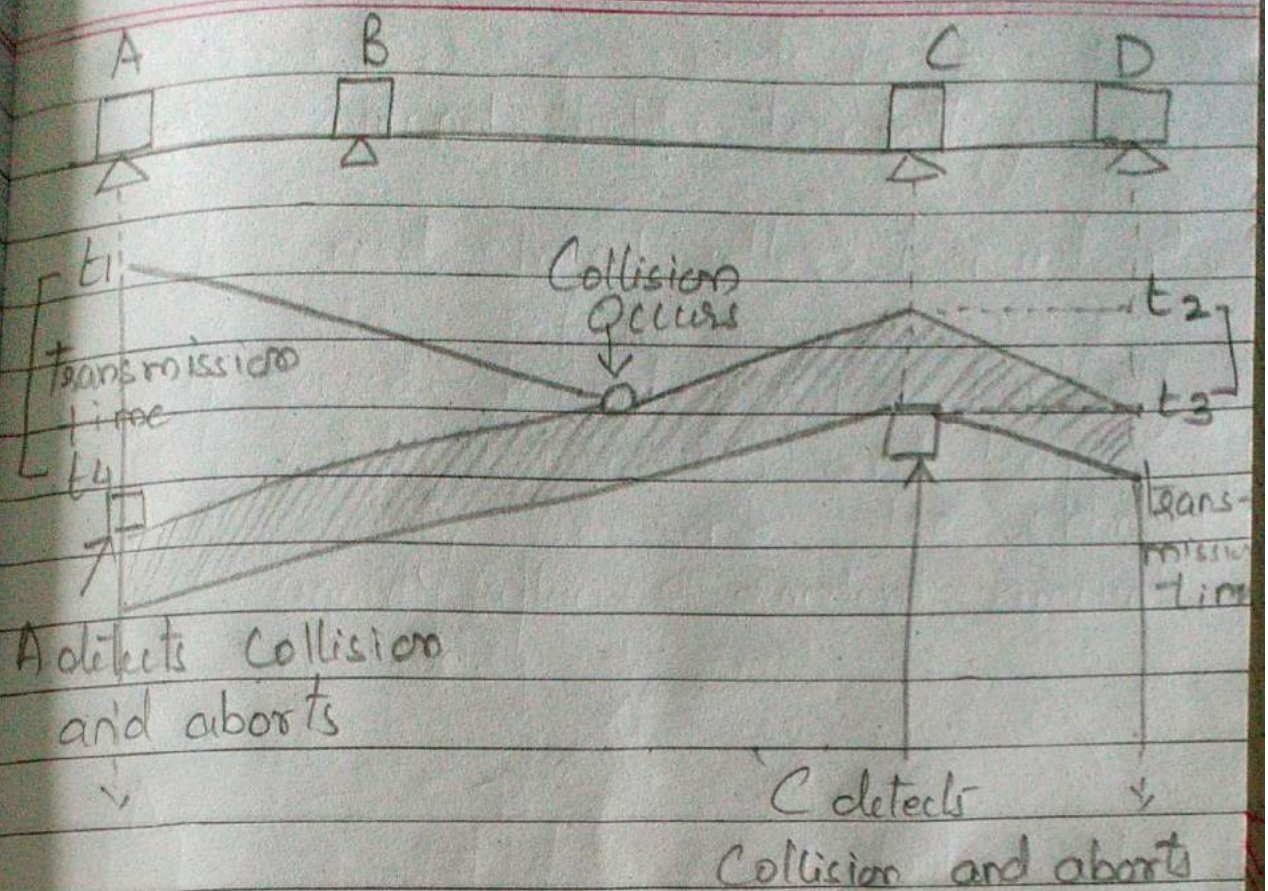
→ Station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right.

→ The collision occurs sometime after time t2 station C detects a collision at time t3 when it receives the first bit of A's frame.

→ Station "C" immediately (or after a short time, but we assume immediately) aborts transmission.

→ Station "A" detects collision at time 't4' when it receives the first bit of C's frame; it also aborts transmission.

→ 'A' transmit for the duration t4-t1; 'C' transmit for the duration t3-t2.



ETHERNET MAC SUBLAYER

MAC sub layer has two primary responsibilities :-

- Data encapsulation, including frame assembly before transmission and frame parsing / error detection during after reception.

UNIT – 5

SNMP → Simple Network Management Protocol.

1) SNMP is a framework for managing devices in an internet using the TCP/IP protocol suite.

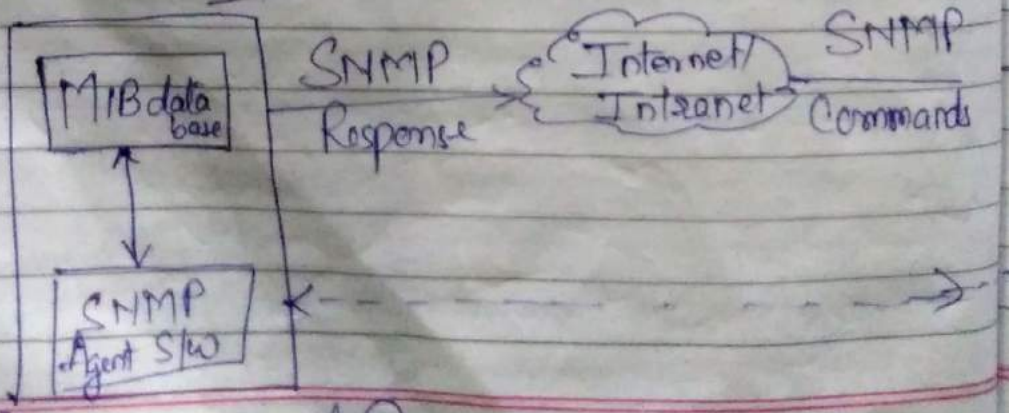
2) It is an Application Level protocol

3) It provides a set of fundamental operations for monitoring and maintaining an internet.

4) SNMP uses the concept of manager and agent.

5) That is, a manager, usually a host, controls and monitors a set of agents usually routers.

SNMP Architecture



Agent Device (Router, Switch, etc)

1) SNMP Manager:

→ A manager or management system is separate entity that is responsible to communicate with the SNMP agent implemented network devices.

→ This is typically a computer that is used to run one or more network management systems.

→ SNMP Manager's key functions:
(a) Queries agent
(b) Gets response from agents
(c) Sets variables in agents.
(d) Acknowledges asynchronous events from agents.

2) Managed devices:

→ A managed device or the network element is a part of the n/w that requires some form of monitoring and management.

→ Example: Routers Switches Servers, workstations etc printers

3) SNMP Agent :

→ The agent is a program that is packaged within the network element.

→ It makes information available to the SNMP managers, which is requested for.

→ These agents could be standard or specific to a vendor (eg HP insight agent)

→ SNMP agent's key function:

a. Collects management information about its local environment.

b. Stores and retrieves management information as defined in the MIB.

c Signals an event to the manager.

d Acts as a proxy for some non-SNMP manageable network node.

4) Management Information Base (MIB):

→ Every SNMP agent maintains an information database describing the managed device parameters.

→ The SNMP manager uses this database to request the agent for specific information and further translates the information as needed for the N/w management System (NMS).

→ This commonly shared database both the Agent and the Manager is called Manager Information Base (MIB)

→ MIB contains standard set of statistical and control values defined for hardware nodes on a network.

→ MIB files are the set of questions that a SNMP manager can ask the agent.

→ Agent collects these data locally and stores it as defined in the MIB.

DNS → (Domain Name System)

→ Domain Name System is an Internet service that translates domain names into IP addresses.

→ The DNS has a distributed database that resides on multiple machines on the Internet.

→ DNS has some protocols that allow the client and servers to communicate with each other.

→ When the Internet was small, mapping was done by using hosts.text file.

→ The host file was located at host's disk and updated periodically from a master host file.

→ When any program or any user wanted to map domain name to an address, the host consulted the host file and found the mapping.

→ Now Internet is not small, it is impossible to have only one host file to relate every address with a name and vice versa.

→ The solution used today is to divide the host file into smaller parts and store each part on a different computer.

→ In this method, the host that needs mapping can call the closest computer holding the needed information.

Name Space

→ The names assigned to the machine must be carefully selected from a name space with complete control over the binding between the names and IP addresses.

→ There are two types of name spaces: flat name space and Hierarchical name.

FLAT NAME SPACES

→ In a flat name space, an name

is a sequence of characters without structure.

→ A name in this space is assigned to an address.

→ The names were convenient and short.

→ A flat name space cannot be used in a large system such as the Internet because it must be centrally controlled to avoid ambiguity and duplication.

Hierarchical Name space

→ In hierarchical name space each name consists of several parts.

→ first part defines the nature of the organization, second part defines the name of an organization, third part defines a department of the organization and so on.

→ In hierarchical name space, the authority to assign and control the name spaces can be decentralized.

DNS on the Internet

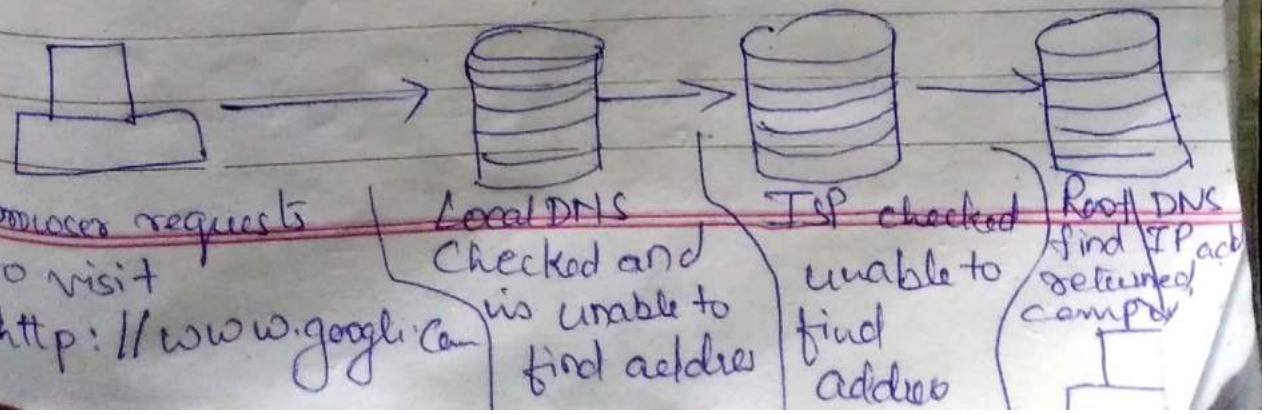
Working of DNS

→ When we type "www.gmail.com" into the browser, it asks the local DNS server for its IP address.

→ When the local DNS does not find the IP address of requested domain name, it forwards the request to the root DNS server and again enquires about IP address of it.

→ The root DNS server replies with delegation the "I don't know the IP address of www.gmail.com but know the IP address of DNS server.

→ The browser then ~~server~~ sends request to ~~IP address in~~ the DNS server and IP sends back to the browser.



LOGICAL ADDRESSING - Communication at N/w layer is host-to-host (computer - computer).

→ The sender computer should need to communicate with receiver computer, which is very far. So, the packet transmitted by the sender may pass through several LAN's or WAN's before reaching the destination computer.

→ For this level of communication we need a global addressing scheme called as logical addressing.

→ Logical address is known as I.P address (Internet protocol address).

→ There are 2 types of IP addresses : They are :

1. IPV4 (Version 4)
2. IPV6 (Version 6)

IPV4 (IP Version 4) address :- IPV4 is

a 32-bit address, which is unique (and provides connection of a device (router / computer) to the internet.

→ Two devices on the internet can never have the same address at the same time. ie IPV4 addresses are unique & universal.

→ The address space of IPV4 is 2^{32} = 4,294,967,296 (4 Billion approximately)

→ There are 2 types of notations used to represent the IPV4 address they are :

(1) Binary Notation (01110101 10010101 000 11101 000 00010)

(2) Dotted Notation (117.149.29.2

→ The Range of IPV4 addresses are from.

00 00000 . 00000000 . 00000000 . 00000000

to

11111111 . 11111111 . 111 11111 . 11111111

0.0.0.0 to 255.255.255.255

Addressing are of 2 types:

1) Classful addressing
2) Classless addressing.

In classful addressing, the address space is divided into five classes:

Class	Range	IP	Purpose
A	0-127	0.0.0.0 to 127.255.255.255	Whole signed - for large - scale of Organization
B	128-191	128.0.0.0 to 191.255.255.255	Mid-level Organizati
C	192-223	192.0.0.0 to 223.255.255.255	Small-scale Organizatio
D	224-239	224.0.0.0 to 239.255.255.255	Multicasting
E	240-255	240.0.0.0 (to) 255.255.255.255	Reserved.

→ On classful addressing, the large part of available address is wasted.

Class	FORMAT	PRIORITY BIT	No. OF N/w	No. OF Host
A	N·H·H·H	0	$2^{\text{No. of N/w bit} - \text{priority bit}} - 2$ $\Rightarrow 2^{8-1} - 2 = 2^7 - 2$ $= 128 - 2$ $= 126$ As 0 & 127 are the N/w ID so we have to Subtract that from the N/w as well as Host bit	$2^{\text{no. of host bit}} - 2$ $2^{24} - 2$ $= 16777216 - 2$ $= 16777214$ As 1st ~~N/w~~ IP address is 0.0.0.0 & last is 127.255.255.255 we have to remove it.
B	N·N·H·H	10	$2^{16} - 2$ $2^{14} = 16384$	$2^{16} - 2$ $65536 - 2$ 65534
C	N·N·N·H	110	$2^{24-3} = 2^{21}$ 2097152	$2^8 - 2$ $256 - 2$ 254

* Removing N/w ID &

Subnetting

→ Creating multiple Independent Networks from a single Network.

→ Converting Host bits into Network bits

Class	Subnet Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0
D	255.255.255.255

How Subnet Mask Works?

IP address : 192.168.1.1

Subnet Mask : 255.255.255.0

ANDING PROCESS :

192.168.1.1 = 11000000.10101000.00000001.00000001

255.255.255.0 11111111.11111111.11111111.00000000

11000000.10101000.00000001.00000000

Requirement of Hosts

Class C : 192 . 168 . 1 . 0
255 . 255 . 255 . 0

Host Required = 100

So, $2^h - 2 \geq$ Req. of Hosts

$2^h - 2 \geq 100$

$2^7 - 2 \geq 100$

$128 - 2 = 126$ hosts / Subnet

Customized subnet mask =

11111111 . 11111111 . 11111111 . 00000000

255 . 255 . 255 . 10000000

. 128

255 . 255 . 255 . 128 /25

CIDR = Class-less Interdomain Routing
it is notation (or) Slash notation
used in class-less address.

→ Classful addressing, is almost absolute & is replaced with class-less addressing

→ To overcome address depletion & give more to organizations access to the internet classless addressing was designed & implemented. In this scheme, there are no classes but the addresses are still granted in blocks.

→ In classless addressing, when a small or large organizations needs to be connected to the internet, it is granted a block of address.

→ The size of the block varies based on the nature & size of the entity.

→ An ISP (Internet service provider) may be given thousands (or) hundreds of addresses, based on the number of customer it may serve

→ To simplify the handling of addresses the internet authorities impose three restrictions on classless address Block.

① The address in a block must be contiguous, one after another.

(2) The no. of address in a block must be power of 2.

(3) The first address must be evenly divisible by the number of addresses

To find first address in a block when any address within a block is given:

Ex:- A block of addresses is granted to a small organization, we know that one of the addresses is 205.16.37.39/28 What is the first address in the Block.

Sol:- 205.16.37.39/28

= Binary representation is

11001101 00010000 00100101 00100111

The first address in the block can found by setting the right most (32-n) bits to 0's.

ie. 32-28; n=28 = 4 bits to 0's (right most)

ie. 11001101 00010000 00100101 ~~00100~~ 00100000

set to 0's

i.e, 32-28 = n=28 = 4 bits to 0's (right most)

ie 205.16.37.37 is the first address.

⇒ The last address in a block can be found by setting the right most (32-n) bits to 1's.

ex:- To find last address of 205.16.37.39/28 is

11001101 00010000 00100101 00100111

(32 - 28 = 4 bits)

So, last 4 bits to 1's.

ie ~~205.16~~

11001101 00010000 00100101 00101111

ie 205.16.37.47 (4 bits to 1's)

∴ The actual block is from

205.16.37.32
:
205.16.37.47

- Total No. of addresses = 2^{32-28}
= 16 addresses

Network addresses :—

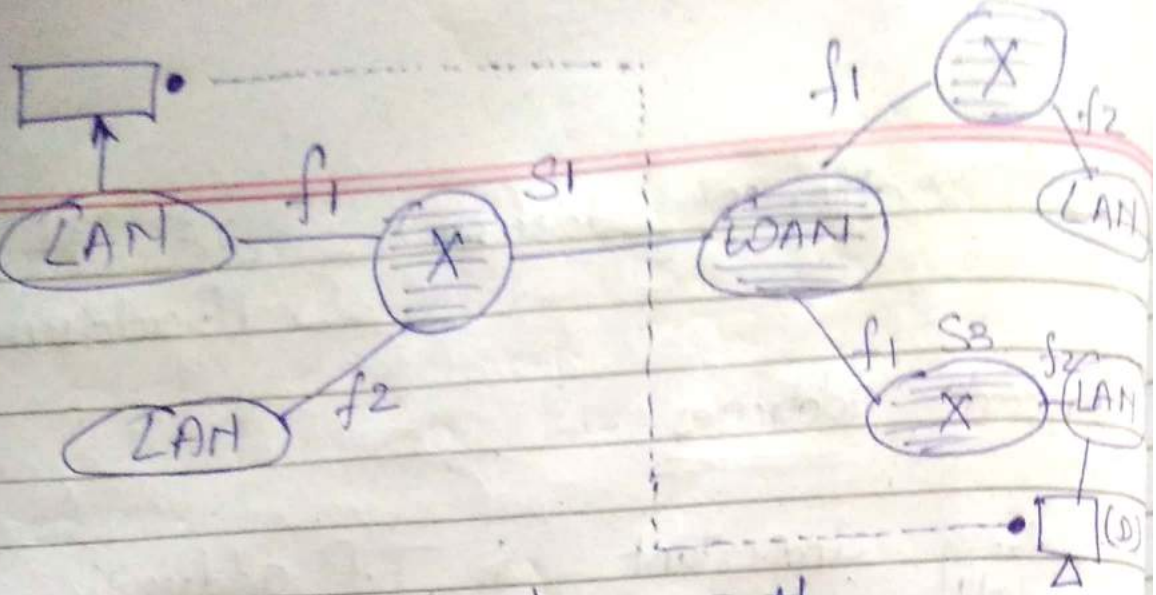
A very important in I.P addressing is the N/w address. When an organization is given a block of address, the Organization is free to allocate the address to the devices that need to be connected to the internet.

→ The first address, in a block is always treated as a special address (or) Network address, & it defines the Organization Network.

→ Network address defines the organization itself to the rest of the world.

INTERNETWORKING

N/w layer is responsible for host-to-host Communication / delivery. Internetworking routes the packet in the N/w to the proper destination.



host - n - host path

⇒ N/w Layer at the source, route & destination

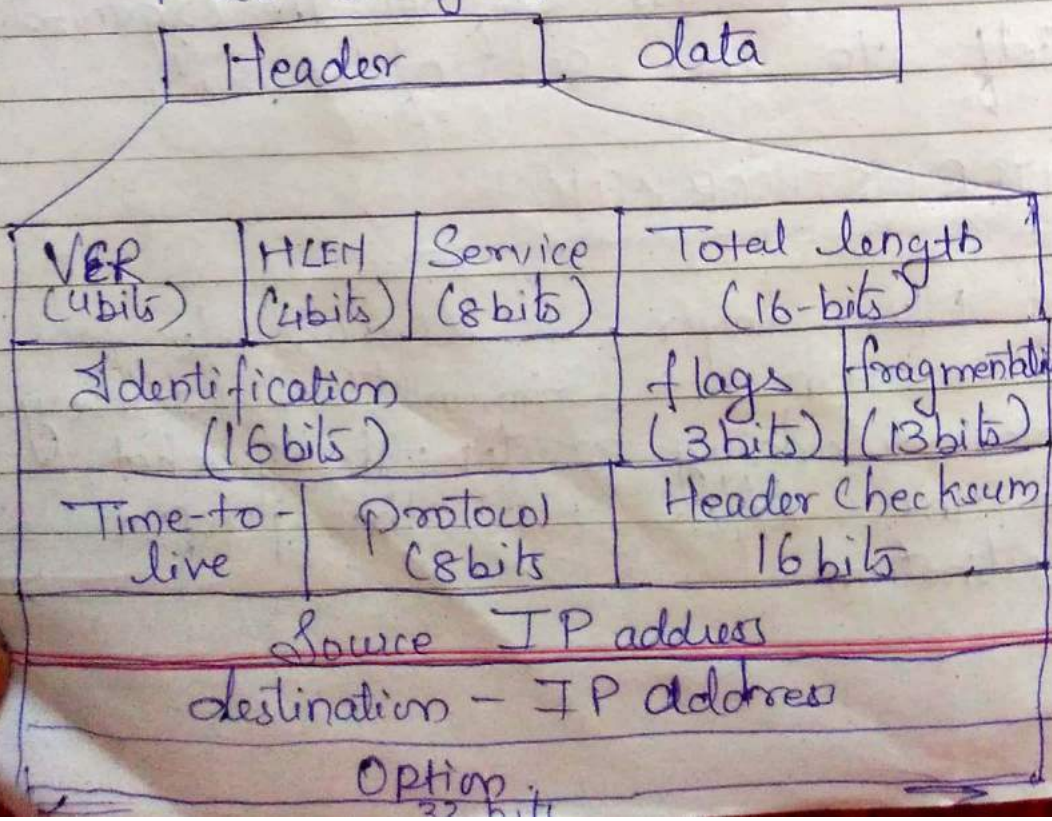
IPV4

→ IPV4 is used in N/w layer

→ IPV4 datagram format is

20 - 65536 bytes

20-60 bytes



1) VER (Version): (4bits)

It defines the version of IP, currently the version is 4. In future Version 6 totally replace version-4.

2) HLEN (Header length): (4bits)

The 4-bits defines the total length of the data-gram in 4-byte words.

3) Service (8 bits)

These bits defines the services & their types like delay Throughput Reliability etc.

4) Total length (16-bits)

It defines the total length of the data gram including Header (ie. 20 - 65,536 byte)

Identification (16bits):
flags (3-bits):
fragmentation offset:
} These fields are used in fragmentation. A datagram can travel through different H/w, each router decapsulates the IPV4 datagram from the frame it receives, Processes it & then encapsulates in another frame

(5) Time to live (8 bits): A datagram has a limited lifetime in its travel through an Internet. The datagram is discarded, when the value becomes zero.

(6) Protocol (8 bits) :-

An IPV4 datagram encapsulate data from several higher-level protocols (such as TCP, ICMP, IGMP)