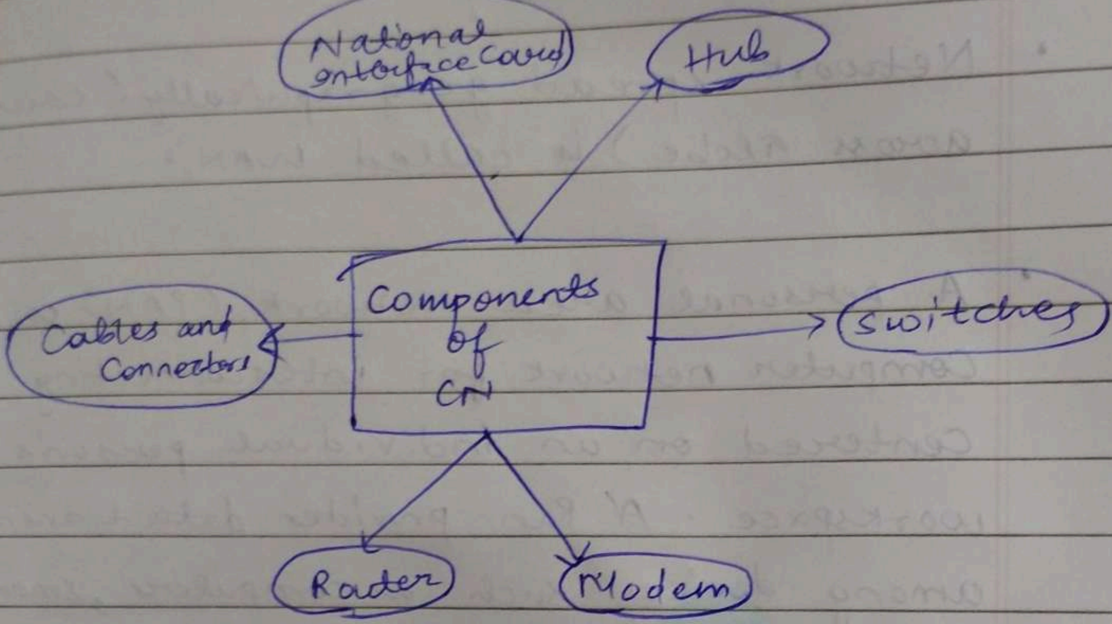
Computer Networks

· A collection of computing devices that are connected in various ways in order to communicate and share resources.



→ **Applications :-**

- E-mail
- Searchable Data (Web Series)
- E-Commerce
- News Groups.
- Internet Telephony (VoIP)

★ **Types of Computer Networks :-**

→ LAN (Local Area Network)

→ MAN (Metropolitan Area Network)

→ WAN (Wide Area Network)

→ PAN (Personal Area Network).

- Network in small geographical Area (Room, Building or a Campus) is called LAN.

- Network in a City is called MAN.

- Network spread geographically (country or across globe) is called WAN.

- A personal area Network (PAN) is a computer network for interconnecting devices centered on an individual person's workspace. A Pan provides data transmission among devices such as computers, smartphone, tablets and personal digital assistants.

Parameters	LAN	WAN	MAN
Ownership of network	Private	Private or Public	Private or Public
Geographical area covered	Small	Very large	Moderate
Design and Maintenance	Easy	Not easy	Not easy
Communication medium	coaxial Cable	PSTN or satellite links.	Coaxial cables, PSTN, optical fibre
Bandwidth	Low	High	moderate
Data ~~rates~~ (speed)	High	Low	moderate

* Internet :-

- A network of networks is called an internetwork, or simply the internet. It is the largest network in existence on this planet.

- The internet hugely connects all WAN's and it can have ~~a~~ connection to LAN's and Home networks.

- Internet uses TCP/IP protocol suite and uses IP as its addressing protocol.

→ Internet Backbone :-

- A set of high-speed networks that carry Internet traffic.
- These networks are provided by companies such as AT and T, GTE and IBM.

→ Internet Service Provider (ISP) :-

- A company that provides other companies or individuals with access to the Internet.

→ NIXI : National Internet Exchange.

★ Internet Connections :-

(1) Dial Up :-

- Establish a connection to an ISP by dialing a telephone number on a conventional telephone line.
- Uses the facility of public switched telephone networks (PSTN).
- Speed is slow more uses narrow band default speed is 56 kbps.

(2) Digital Subscriber line (DSL) :-

- Transmit data over telephone lines.
- DSL service can be delivered simultaneously with wired telephone service on the same telephone line.
- Assymetric DSL (ADSL), the most commonly used DSL technology for internet access.
- In symmetric DSL (SDSL) upstream and downstream data ~~rates~~ rates are same.

★ Integrated services digital network (ISDN) :-

- A set of communication standards for simultaneous digital transmission of voice, video, data and other network ~~se~~ service over the traditional circuits of the PSTN.

→ Broadband :- A connection in which transfer speeds are faster up-to 100 Mbps.

★ Computer Network Architecture :-

- It is a physical and logical design of the software, hardware, protocols, and media of the transmission of data.

Two types :-

- Peer to-Peer Network :- It is a network in ~~cli~~ which all the computers are linked together with equal privilege and responsibilities for processing the data.

→ Peer-To-Peer Network is useful for small environments, usually up to 10 computers.

- It has no dedicated server.

~~eg~~ Three such Architectures exist :

(i) Centralized Directory eg - Napster.
(ii) Query Flooding eg - Gnutella.
(iii) Exploiting Heterogeneity eg - KaZaA.

→ Advantages :-

- It is less costly as it does not contain any dedicated server.

- If one computer stops working but, other computers will not stop working.

- It is easy to set up and maintain as each computer manages itself.

→ Disadvantages :-

~~In the~~

- It does not contain the centralized system.

- It has a security issue as the device is managed itself.

★ Client/server Network

- HTTP and HTTPS.

- It contains the centralized system.
- ~~These~~ It has a dedicated server that improves the overall performance of the whole system.
- security is better.

Date
Page

* ~~Networki~~
* Networking devices:- ~~Prop~~ Modem, Router, NIC, Gateway.
- ~~Re~~

→ Repeaters :-

- Repeaters are networking devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it.

- Known as signal boosters.
- They can't connect dissimilar networks.

Prop:- 2 ports, Forwarding, No filtering, Collision domain.

→ Hub :-

- Hub is a centralized device that connects multiple devices in a single LAN network.
- Passive Hub (same format) fwd, Active Hub (amplifies)

Prop:- Multiport, Forwarding, No filtering, Collision domain

→ ~~Bridge:-~~

- ~~Used to connect two different networks. or LANs.~~

→ Switch :-

- It also works at the layer of LAN but you can say that ~~is~~ a switch is more intelligent than a hub.

- On receiving a packet, it checks the destination address and transmits the packet to the correct port.

Page

- Each switch has a dynamic table (called the MAC address table) that maps MAC addresses to ports.

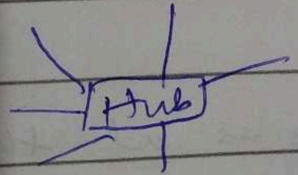
★ Network Topology :-

1. Bus Topology :-

- every computer and network device is connected to single cable. when it has exactly two endpoints, then it is called Linear Bus Topology.

2. Star Topology :-

- All the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node and all other nodes are connected to the central node.



3. Ring Topology :-

- It forms a ring as each computer is connected to another computer, with the last one connected to first.

4. Mesh Topology :-

- It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has $\frac{n(n-1)}{2}$ physical channels to link n devices.

5. Tree Topology :-

- It has a root node and all other nodes are connected to it forming.

6. Hybrid Topology :-

- Connects two or more topologies.

★ OSI Model :-

- OSI (Open System Interconnection) is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.

→ OSI consists of seven layers, and each layer performs a particular network function.

→ OSI model divides the whole task into seven smaller and manageable tasks.

→ Each layer is self-contained, so that task assigned to each layer can be peformed ...

- The upper layer ~~of the~~ ~~OSI layer~~ of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications.

- The lower layer of the OSI model deals with data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is ~~a~~ the lowest layer of the OSI model and is closest to the physical medium.

Layer	Application/eg	Common device/protocol		DOD 4 Model
Application	End use layer	User Applications SMTP	GATEWAY	
Presentation	Syntax layer	JPEG/ASCII EBCDIC TIFF		Process
Session	Sync and send to ports	Logical Ports SQL		
Transport	TCP	TCP/SPX/UDP		Host to host
Network	Packets	~~Pac~~ Routers		Internet
Datalink	Frames	Switch, Bridge	Land Based Layers	Network
Physical	Physical structure	Hub		

1. <u>Physical Layer</u> :-

- The physical layer is responsible for the movement of individual bits from one hop(node) to the next.
- It is the lowest layer of the OSI model.
- It specifies the mechanical, electrical and procedural network interface specification

→ <u>functions</u> :-

- Line Configuration
- Data Transmission
- Topology : how network devices are arranged.
- Signals : type of signal

2. Data Link Layer :-

- The Data Link layer is responsible for moving frames from one hop(node) to the next.

- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.

→ Two sublayers :-

(i) Logicallink control layer :-
- It is responsible for transfering the packets to the Network layer of the receiver that is receiving.

(ii) Media Access Control layer :-
- It is a link between the logical link control layer and the network's physical layer.

→ Functions :-
- Framing
- Physical Addressing
- Flow Control
- Error Control
- Access Control.

(3) Network layer :-

- It manages device addressing, tracks the location of devices on the network.

- The Network layer is responsible for routing and forwarding the packets.

- The protocols used to route the network traffic are known as Network layer protocols. eg - IP and IPv6.

→ Functions :-
- Internetworking
- Addressing
- Routing
- Packetizing.

(4) Transport Layer :-
- The Transport Layer is responsible for the delivery of a message from one process to another.
- It transfers the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.

The two protocols used in this layer are:-

(i) Transmission Control Protocol:
- It is a standard protocol that allows the systems to communicate over the internet.

(ii) User Datagram Protocol:-
- It is an unreliable transfer protocol.

→ Functions :-
- Service-point addressing
- Segmentation and reassembly.
- Connection control
- Flow Control
- Error Control

(5) Session Layer :-
- The session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

→ Functions :-
- Dialog Control
- Synchronization

(6) Presentation layer :-

- The Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network
- It is also known as the syntax layer.

→ Functions :-

- Translation
- Encryption
- Comp-ression

(7) Application layer :-

- Application layer interacts with application programs and is the highest level of OSI model
- It contains management functions to support distributed applications.
- It handles issues such as network transparency resource allocation, etc.

→ Functions :-

- File transfer, access, and management (FTAM).
- Mail Services
- Directory services.

★ TCP/IP Protocol stack:-

- The TCP/IP was developed, prior to the OSI Model and is exactly not ~~sm~~ similar to the OSI Model.

- The TCP/IP model consists of five layers:-

→ the application layer.
→ the transport layer.
→ the network layer.
→ the data link layer
→ the physical layer.

- The first four layers provide physical standards, network interface, internetworking and transport functions that correspond to the first four layers of the OSI model and top three layers are represented in TCP/IP model by a single layer called the application layer.

TCP/IP Model	OSI Model
Application layer	Application Layer Presentation Layer Session Layer
Transport layer	Transport Layer
Internet Layer	Network Layer
Network Access layer	Data Link Layer Physical Layer

(1) **Network Access layer** :-

- It is the lowest layer of the TCP/IP model.
- It is the combination of the Physical layer and Data Link layer in the OSI reference model.
- It defines how the data should be sent physically through a network.

(2) **Internet layer** :-

- It is the second layer of the TCP/IP model.
- It is also known as the network layer.
- The main responsibility is to send the packets from any network, and they arrive at the destination irrespective of the route they take.
- Protocols used : IP Protocol, …

(3) Transport Layer :-

- The transport layer is responsible for the reliability, flow control and correction of data which is being sent over the network.

- The two protocols used in the layer are:-

→ User Datagram Protocol.
→ Transmission Control Protocol.

(4) Application Layer :-

- Topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- There is an ambiguity in application layer. Every application cannot be placed inside the application layer except those who interact with the communication system.

- Protocols used : HTTP, SMTP, DNS, TELNET.

Date
Page

* Networking in different OS :- (NOS)

- Network Operating System (NOS), is the software that allows multiple computers to communicate, share files and hardware devices with one another.

- It is a specialized operating system for a network device such as a router, switch or firewall.

→ Features :-

- Basic ~~of~~ O.S. features support like protocol support, processor support, hardware detection and multiprocessing support for applications.

- Security features like authentication, restrictions, authorizations and access control.

- Features for file, web service.

- User management features.

- Internetworking features like routing and WAN ports.

→ Common tasks of NOS :-

- User administration
- System maintanance activities
- Tasks associated with file management
- Security monitoring on all resources in the network.
- Setting priority ~~f~~ to print jobs in the network.

Continue :-

★ Bridge :-

- It is used to connect two different networks or LANS.

Props :-

Connecting diff network architectures, Forwarding, Filtering, Collision domain, Bridge data unit protocol.

★ Router :-

- It is a physical ~~or~~ or virtual application that passes information between two or more packet switched ~~component~~ computer networks.

- It inspects a given data packet's destination IP address, calculates the best way for it to reach its destination and then forwards it accordingly.

- Routers are associated with Network Layer.

* **Gateway :-**
- It is a passage to connect two networks together that may work upon different networking models.

- They basically work as the messenger agents ~~lik~~ that take data from one system, interpret it, and transfer it to another system.

- Also called protocol convertors.
- More complex than switch or router.
- A gateway always has to be a router, but a router does not have to be a gateway.

* **Modem :-**
- A modem (modulator/ demodulator) is a hardware device that allows a computer to send and receive ~~it~~ information over telephone lines, cables, or satellite connection.

- It

formats in real time for two-way network communication.

eg- cable Modem, DSL modem.

* NIC :- Network Interface Card

- A NIC or Ethernet Card is a computer expansion card for ~~conne~~ connecting to a network using an Ethernet cable with an RJ-45 connector.

- It converts parallel data stream into serial data stream and the serial data stream to parallel data stream.

(1) Unipolar :-

- 1 pe upar
- 0 pe normal (0).

(2) NRZ-L :- Non-return to zero-level.

- 1 pe upar.
- 0 pe neeche.

(3) NRZ-I :- Non return zero Inverted.

- Transition → 1 [L → H, H → L]
- No Transition → 0

(4) RZ :- [Each bit → transition]

- ~~1 pe upar se neeche.~~
- 1 pe full transition upar.
- 0 pe full transition neeche.

(5) Manchester :- [Arrows]

- ~~Up.~~ Neeche se upar → 1
- Upar se neeche → 0

(6) Differential Manchester :-

0 → edge, dabba hona chahiye pehle.

1 → no edge.

(7) Bipolar AMI :-

- 1 pe +ve → -ve, -ve → po +ve [Alternati

- 0 pe normal (0).

(8) Pseudoternary :- [opp. of BAMI]

- 1 pe normal.
- 0 pe +ve → -ve, -ve → +ve.

(9) B8ZS :- [8 0's consecutive].

- Bipolar AMI.

Last pulse		
	+	000+-0-+
	-	000-+0+-

(10) HDB3 :- [4 0's consecutive] [Bipolar AMI]

Last pulse	No. of 1's since last substitution odd	even
-	000-	+00+
+	000+	-00-

* Transmission Media :-

- Guided (wired)
  - Twisted pair Cable
  - Coaxial Cable
  - Fibre-optic Cable
- Unguided (Wireless)
  - Air

(1) Twisted Pair Cable :-

. Pros and cons

→ Cheap; Easy to work with.

→ low data rate ; short distance <- bigger attenuation.

. Analog Signal : Amplifiers every 5 km to 6 km.

. Digital Transmission : repeater every 2 km or 2 km.

. Limited distance

. Limited ~~bra~~ bandwidth (1 MHz)

. Limited data rate (100 Mbp)

. Susceptible to interference and noise.

(2) Coaxial Cable :-

. Most versatile medium

⇒ LANs, Cable TV, Long-distance telephones, VCR-to-TV connections.

. Noise immunity is good.

. Very high channel capacity

⇒ few 100 ...

• Need repeater /amplifier every few kilometer or so.

~~• Has.~~
~~Both conduct~~

• Has an inner conductor surrounded by a braided mesh.
• Both conductors have a common center axial, hence the term "co-axial".

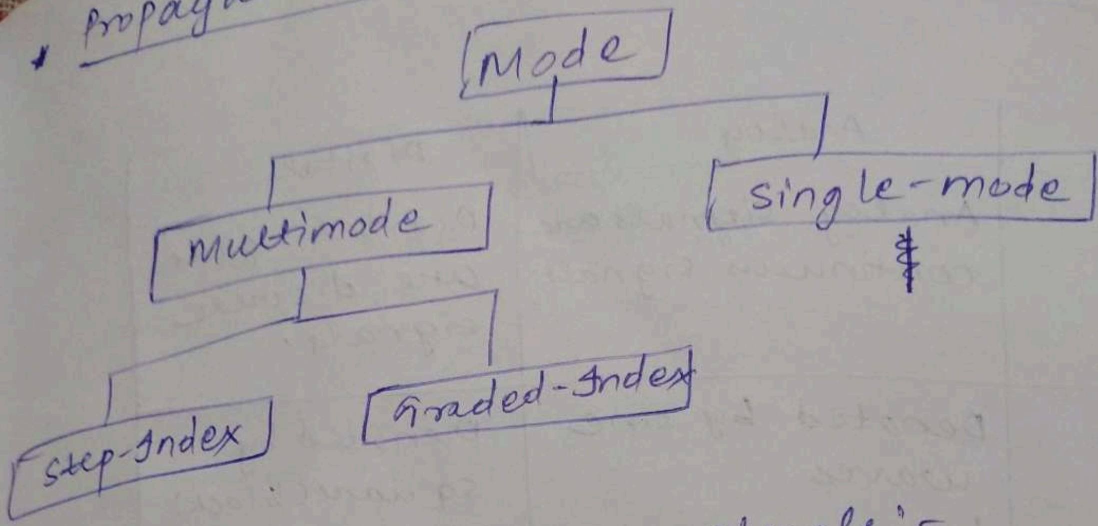
→ Properties:-

• Higher transfer rates
• Higher bandwidth
• Can be tapped easily
• Much less sus·ceptible to interference than twisted pair.
• High attenuation rate makes it expensive over long distance.

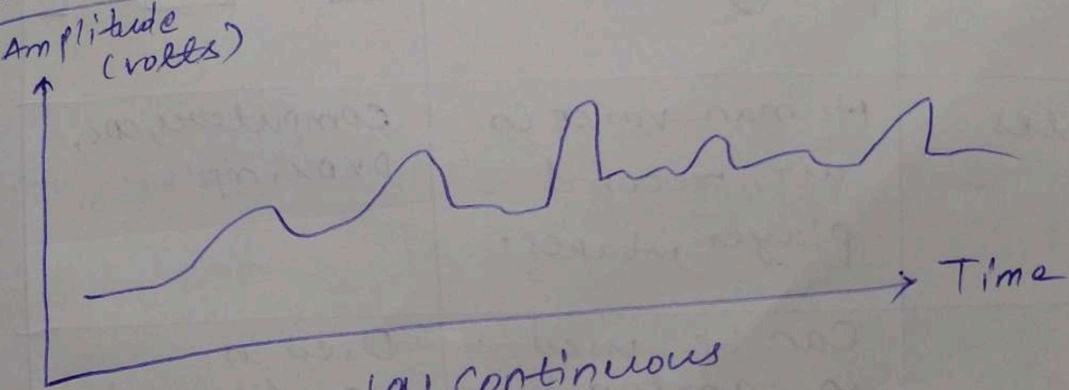
(3) Fibre - Optic Cable :-

• More expensive than copper cable.
• Much more difficult to install.
• Data rates in range of 100 Mbps to 2Gbps.
• Much lower attenuation than copper wires.
• Not subject to EMI.
• Need optical - electrical interface.

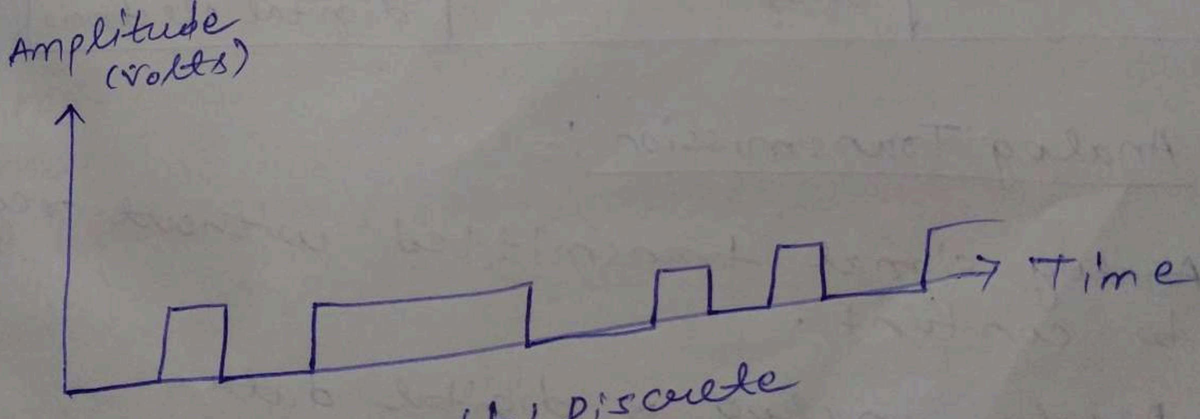
* Propagation Modes :-



* Continuous and Discrete signals :-

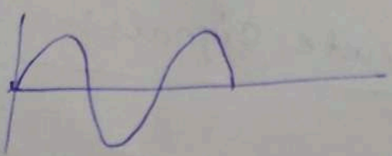
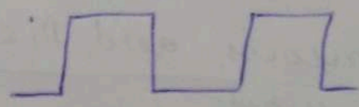


(a) Continuous



(b) Discrete

* Analog and Digital signals :-

~~Sign~~	Analog	Digital
signal	Analog signals are continuous signals.	Digital signals are discrete signals.
Waves	Denoted by sine waves 	Denoted by square (block) waves 
Examples	Human voice in air, record player, tapes.	computers, CDs, DVDs, mp3s.
Uses	Can be used in analog devices only.	Used in computing and digital electronics

→ Analog Transmission :-

- Analog signal transmitted without regard to content.
- Maybe analog or digital data.
- Attenuated over distance.
- Use amplifiers to boost signal.

→ Digital Transmission :-

- Repeaters receives signal
- Extracts bit pattern.
- Attenuation is overcome.

* Advantages:-

- low cost
- Longer distances over lower quality lines.
- High bandwidth.
- Encryption

* Transmission Impairments:-

- Attenuation
- Distortion
- Noise.

* Attenuation :-

- signal strength falls off with distance.
- Depends on medium.
- Received signal strength:

→ must be enough to be detected.
→ must be sufficiently higher than noise to be received without ~~error~~ error.

- Attenuation is an increasing function of frequency.
- Unit to measure strength: Decibel (DB)

  - Positive : amplified
  - Negative: Attenuated.

$$\boxed{dB = 10 \log_{10} (P_2/P_1)}$$

#

A signal travels through a transmission medium and its power is reduced to one half. Calculate the attenuation.

Ans-

Point 1 —— T.M. —— Point 2

$$dB = 10 \log_{10} (P_2/P_1)$$

Let $P_1 = P$

$P_2 = P/2$

$$dB = 10 \times \log_{10} \left(\frac{P}{2} \times \frac{1}{P} \right)$$

$$10 \times -0.30$$

$$\boxed{dB = -3\ dB}$$

2. $P_1 = P$

$P_2 = 20P$

Calculate the power gained.

$$dB = 10 \log_{10} \left(\frac{20P}{P} \right)$$

$$dB = 10 \times 1.30$$

$$\boxed{dB = 13\ dB}$$

Q) ~~A~~ Signal $P_1 \longrightarrow P_4$.

$P_2 \rightarrow -3\,dB$

Between P_2 and $P_3 \rightarrow 7\,dB$.

Between P_3 and $P_4 \rightarrow -3\,dB$.

Resultant decibel?

Ans - $-3 + 7 - 3 = +1$.

(Amplified).

Q) The loss in a cable is usually defined in decibels per km. (dB/km). If the signal at the beginning of a cable with -0.3 dB/km has a power of 2mW, what is the power of the signal at 5km?

Ans - ~~$dB = 10 \log_{10} \frac{P_2}{P_1}$~~

Ans - The loss in the cable in decibels is $5 \times (-0.3) = -1.5\,dB$

We can calculate the power as

$$dB = 10 \log_{10} \frac{P_2}{P_1} = -1.5$$

$$\frac{P_2}{P_1} = 10^{-0.15} = 0.71$$

$$P_2 = 0.71\,P_1 = 0.7 \times 2 = 1.4\,mW$$

★ Delay Distortion :-

- Only in guided media.
- Propagation velocity varies with frequency.
- Also called "Intersymbol Interference".

★ Noise :-

- Additional signals inserted between transmitter and receiver.
- Thermal : Due to thermal agitation of electrons.

→ Signal to Noise Ratio (SNR) :-

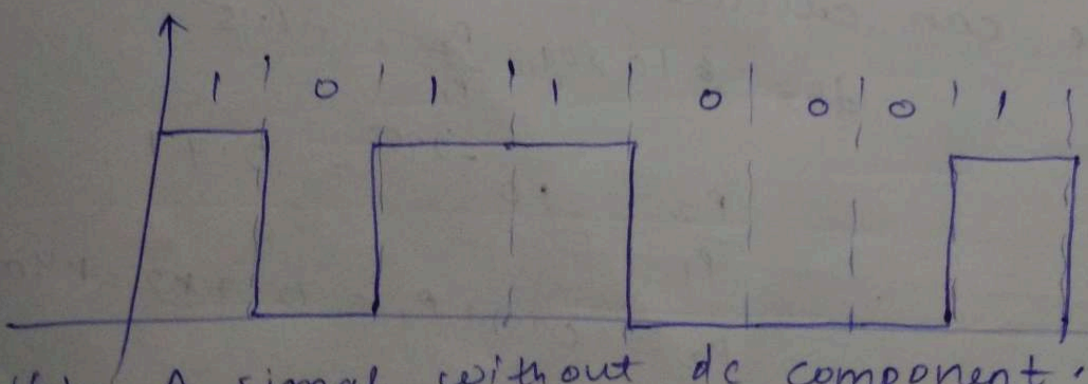
$$\boxed{SNR = \frac{\text{Average signal Power}}{\text{Average Noise Power}}}$$

$$\boxed{SNR_{dB} = 10 \log_{10} SNR}$$

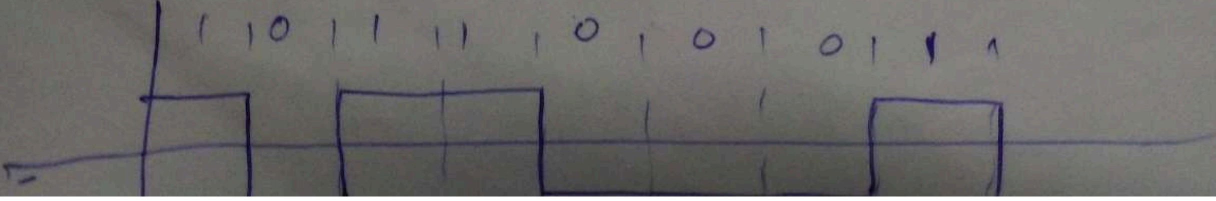
★ Encoding schemes :-

(a) A signal with dc component

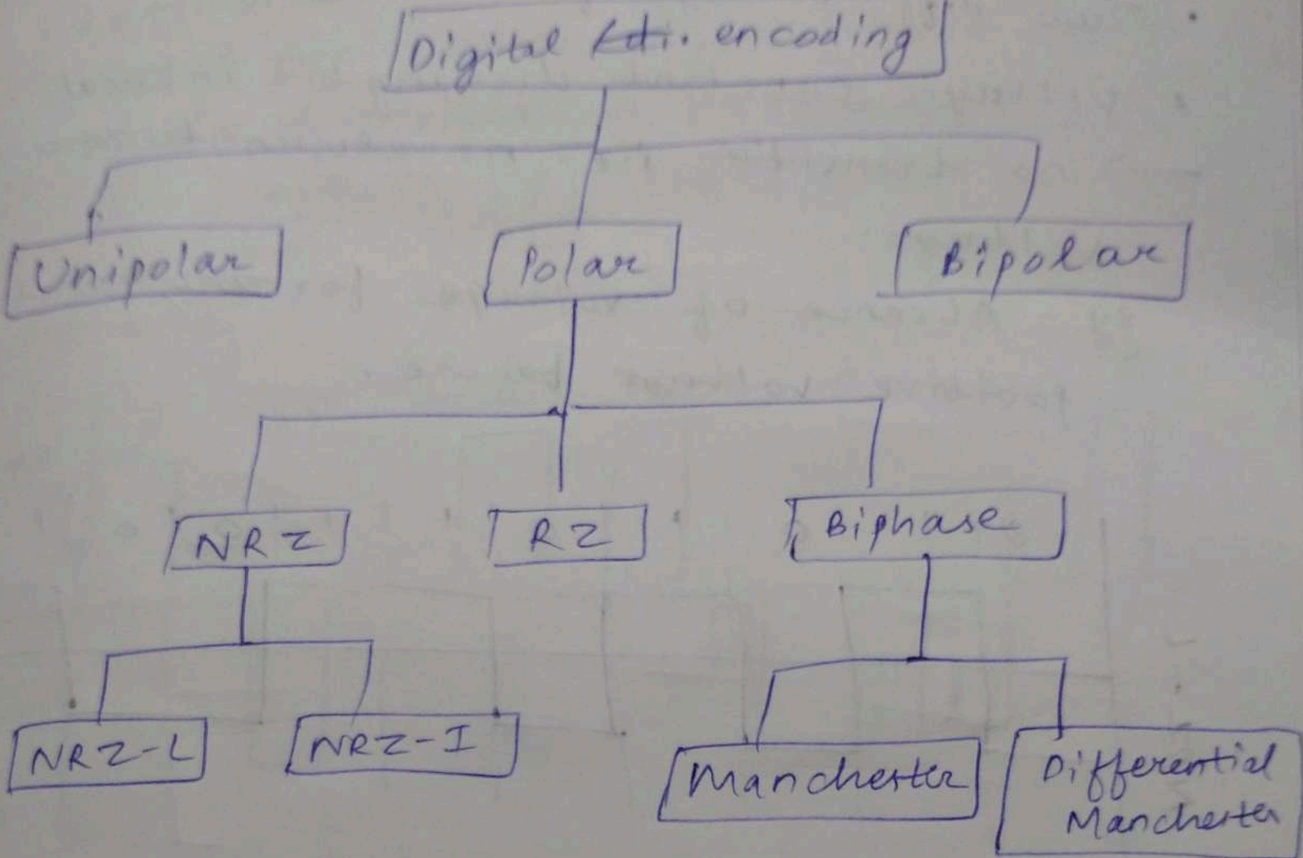
1 0 1 1 0 0 0 1



(b) A signal without dc component.

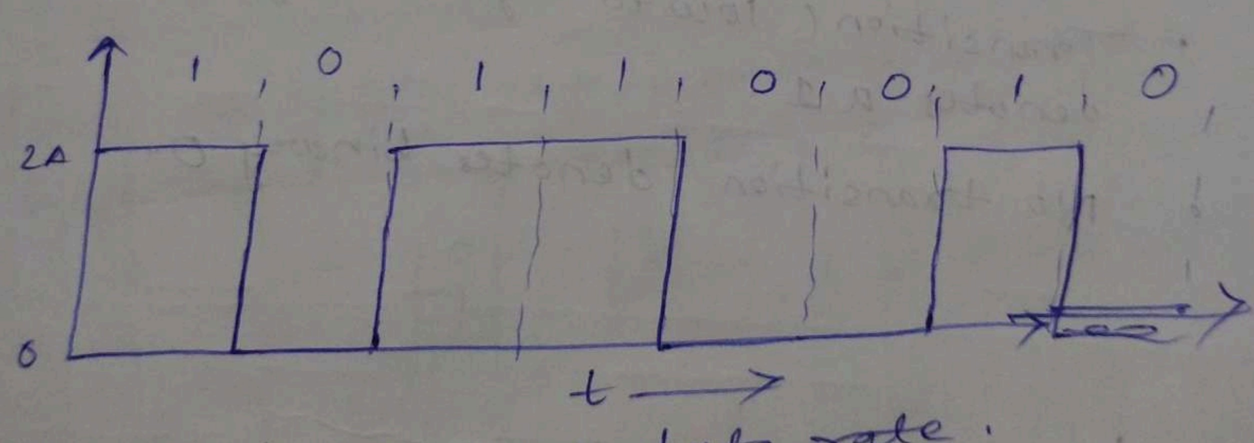


* Encoding schemes :-



* Unipolar Enchoding schemes :-

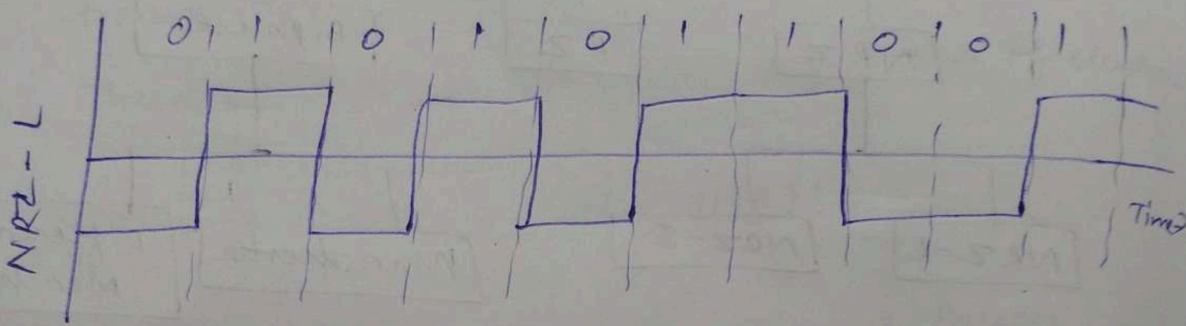
- Only two voltages levels are used.



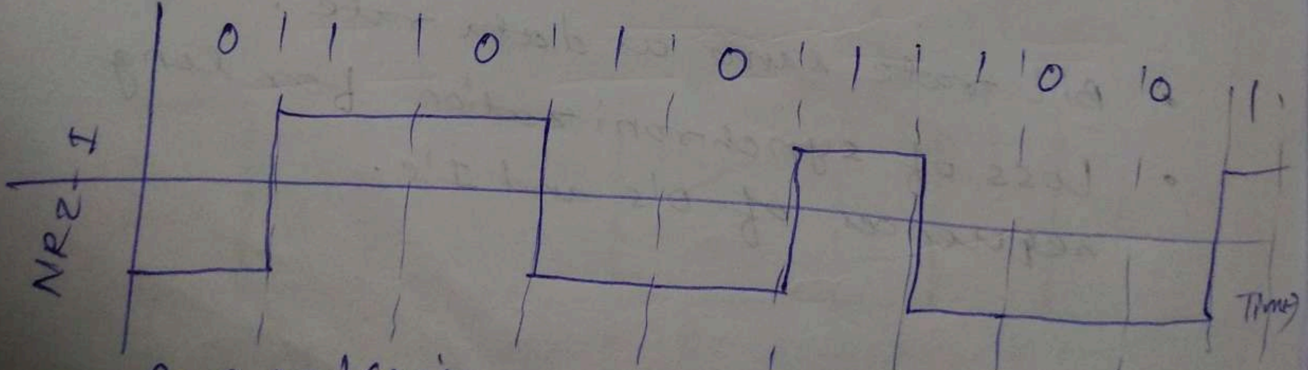
- Bit rate same as data rate.
- Loss of synchronization for long sequences of 0's and 1's.

* NRZ-L :- Nonreturn to zero Level.
- Two diff. voltages for 0 and 1 bits.
- Voltage constant during bit interval
→ no transition i.e. no return to zero voltage.

eg - Absence of voltage for zero, constant positive voltage for one.



* NRZ-I :- Non-return to Zero Inverted
- Nonreturn to zero inverted on ones.
- Transition (low to high or high to low) denotes a 1.
- No transition denotes binary 0.



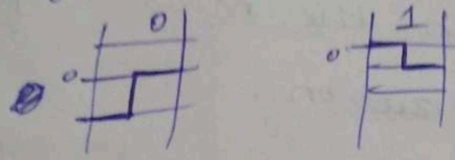
NRZ Pros and Cons-

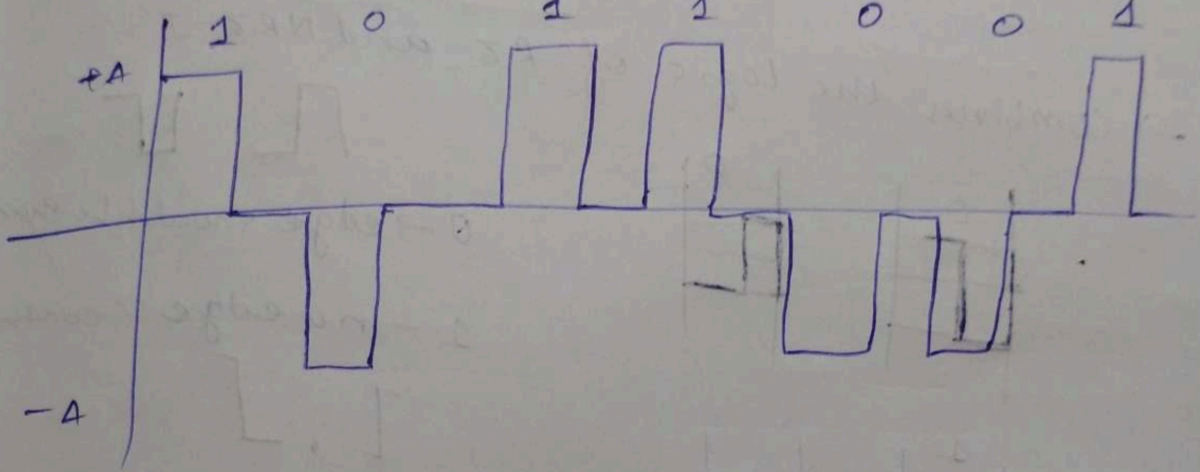
→ Pros → Two level, Make good use of bandwidth.

→ Cons → dc component, lack of synchronization capability.

* **RZ Enchoding scheme :-**

• Return to zero :- To ensure synchronization, there must be a single transition in each bit.



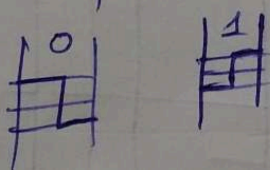


* **Biphase Encoding :-**

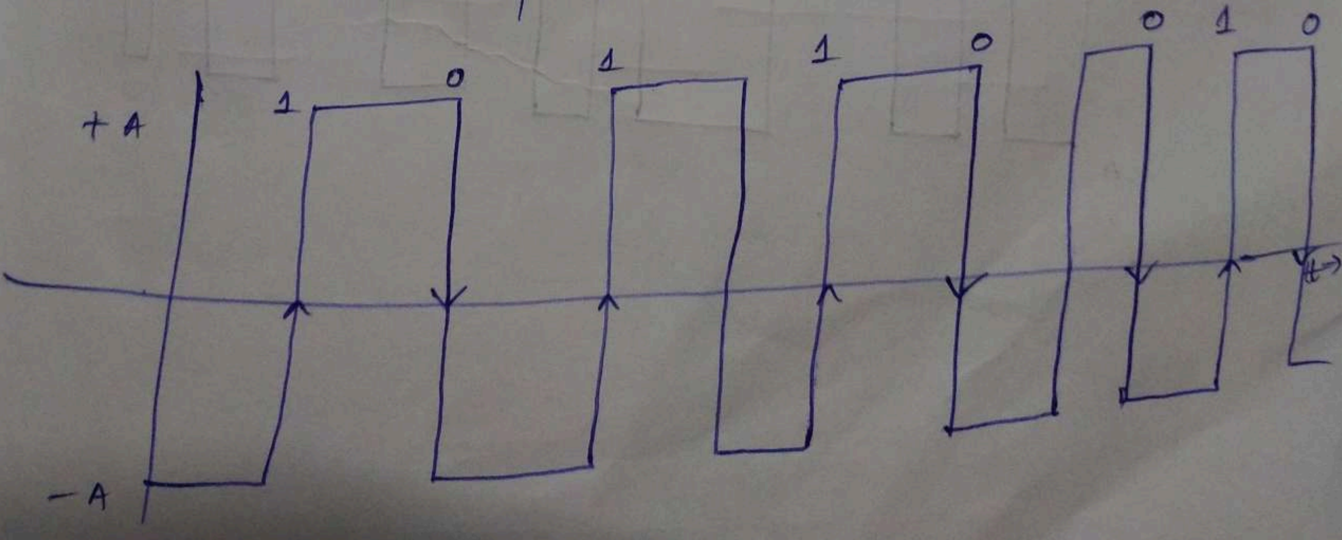
• ~~lor~~

→ **Manchester (Biphase) Encoding :-**

• low-to-high represents a 1 and high-to-low represents a 0.

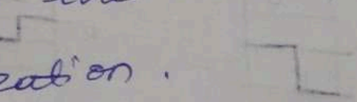


1 0 1 1 0 0 1 0

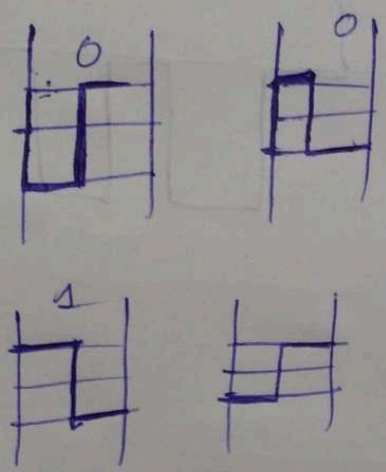


→ Differential Manchester (Biphase) Encoding :-

- Presence of transition in the beginning of a bit represents a 0.
- Uses a inversion in the middle of each bit for synchronization.

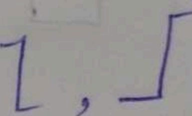


→ combines the logic of RZ and NRZ-I.



0 → edge should be there

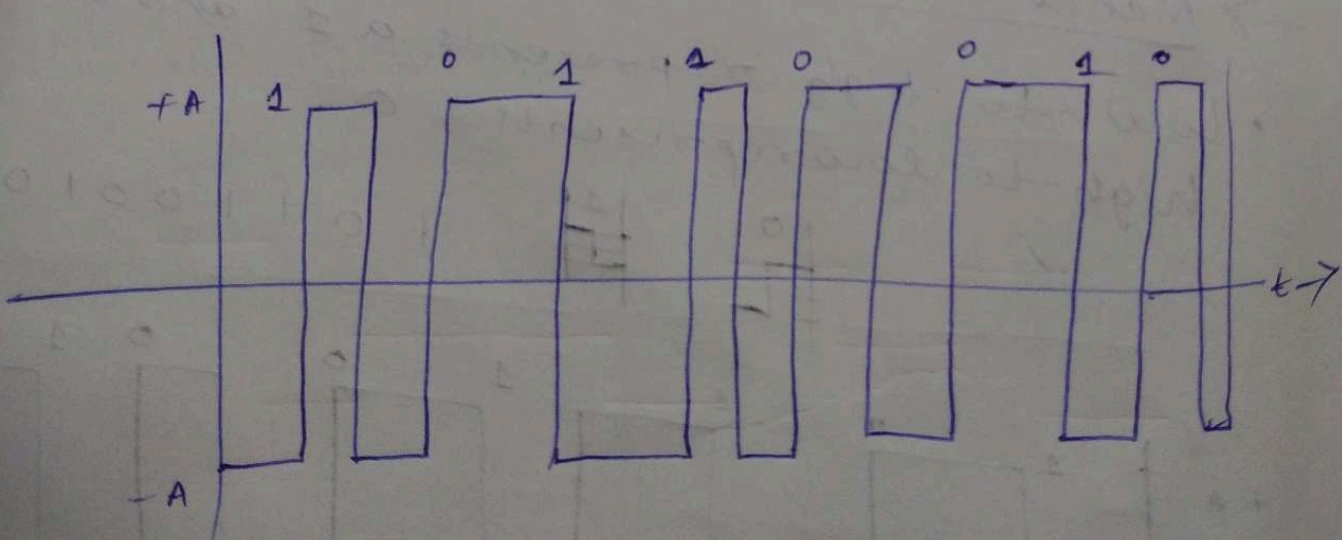
1 - no edge (continue).



0 → change

1 - cont. and draw

1 0 1 1 0 0 1 0



Biphase Pros and Cons -

Cons :-

- At least one transition per bit time and possibly two.
- Maximum modulation rate is ~~two~~ twice NRZ.
- Requires more bandwidth.

Pros :-

- synchronization on mid bit transition (self clocking)
- No dc component
- Error detection
  → Absence of expected transition.

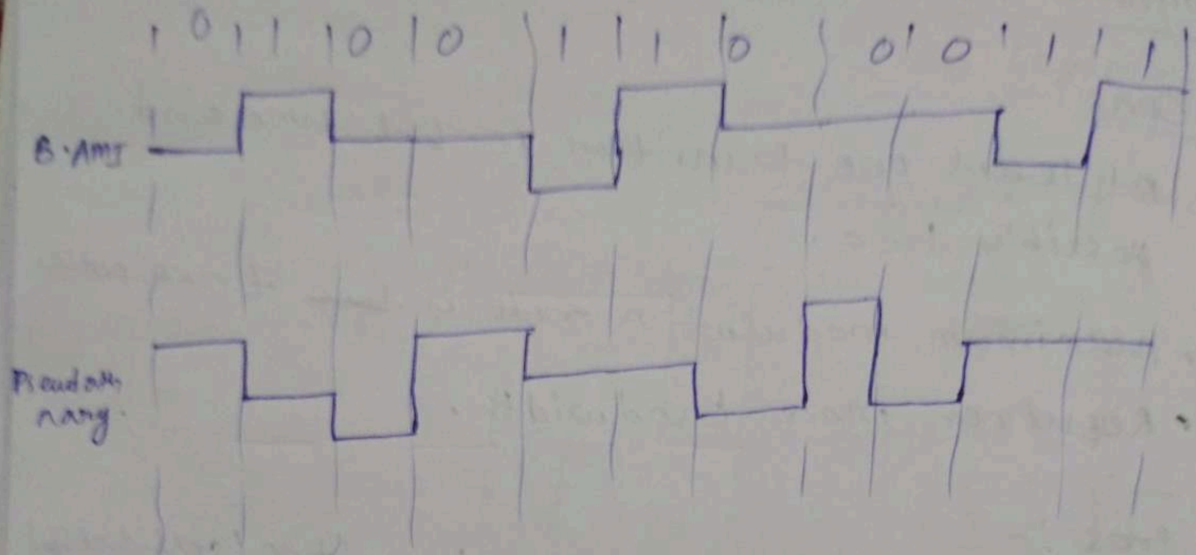
Bipolar encoding :-

- AMI
- B8ZS
- HDB3

- **Bipolar AMI (Amplitude Mark Inversion)**
  → zero represented by no line signal.
  → one represented by positive or -ve pulse. (Alternating)

- **Pseudoternary :-**
  → One represented by absence of line signal.
  → zero represented by alternating positive and negative.

Q) 01 0011000 11

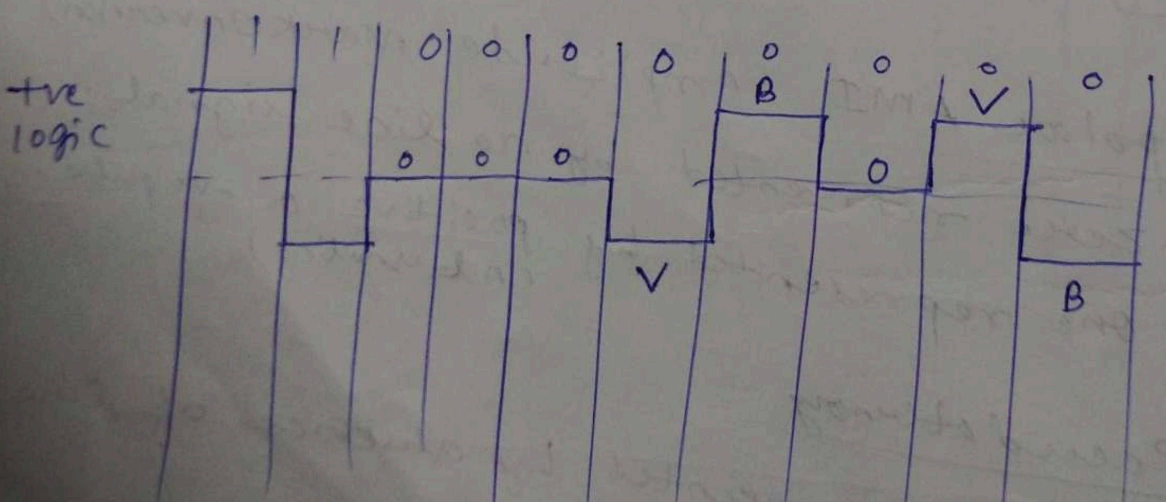


* Scrambling :-

- Bipolar AMI ; synchronization problem → scrambling.

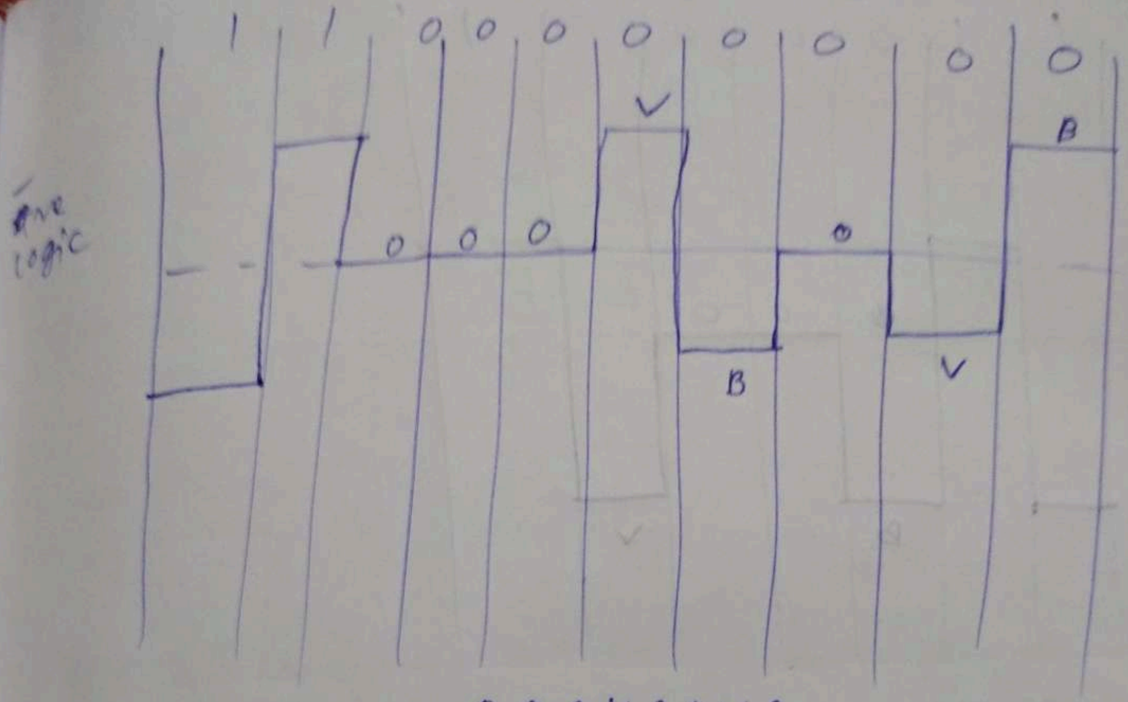
→ B8ZS :-
(Bipolar 8 0's substitution) :-
(There should be 8 consecutive B8ZS).

Q) 1100000000 (AMI)



000VB0VB

Last pulse		
	+	000+-0-+
	-	000-+0+-

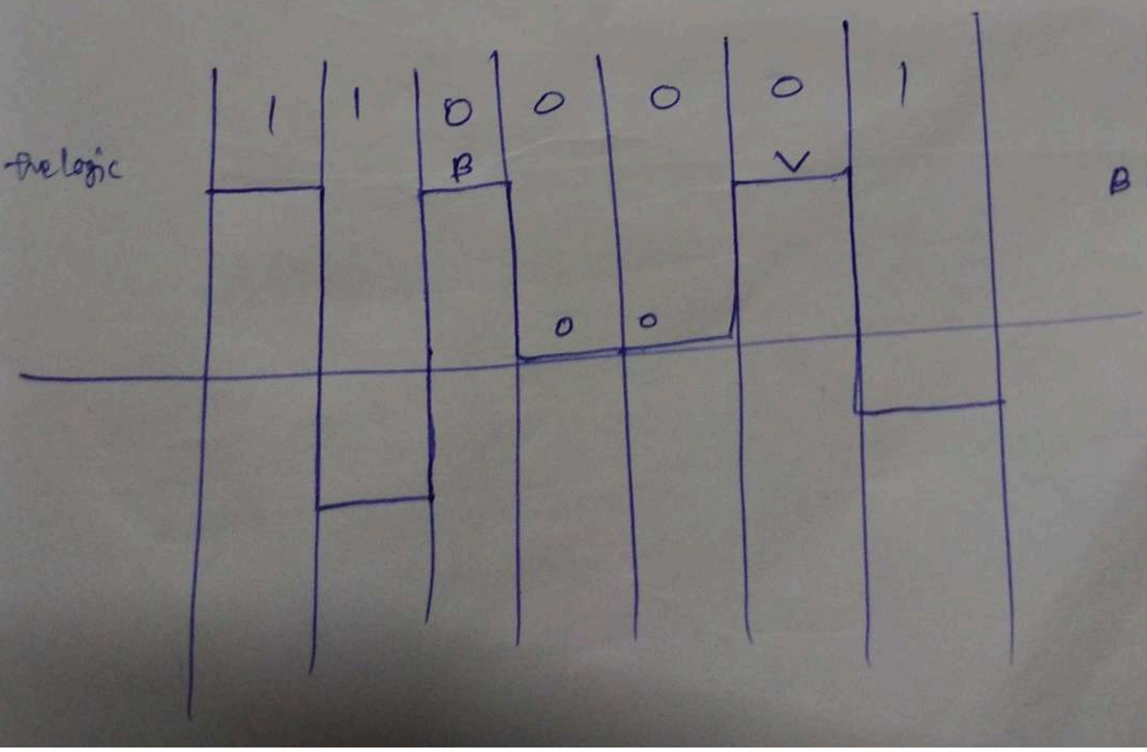


000VB0VB.

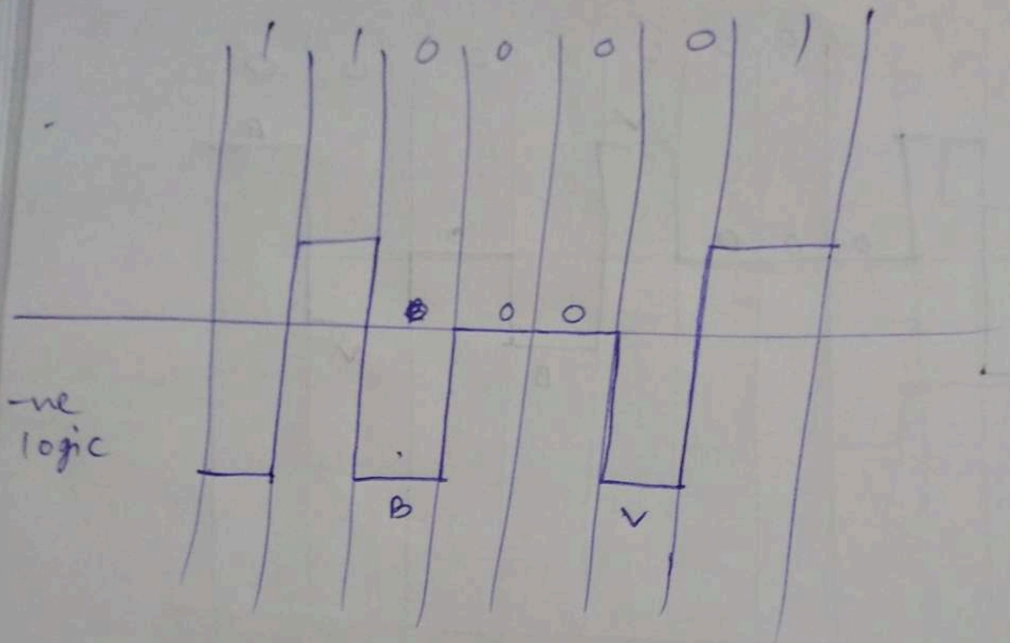
→ HDB3 :- (consecutive 4 0's substitution).

Last Pulse	No. of 1's since last substitution	
	odd	even
−	000−	+00+
+	000+	−00−

Q) 1100001



B00V.



BOOV

* Formulas :-

$\boxed{\text{No. of bits per level} = \log_2(\text{levels})}$

Q) A digital signal has 8 levels. How many bits are needed per level?

Ans - No. of bits per level = $\log_2 8 = 3$

* Nyquist Formula (noise free channel):-

$\boxed{R = 2B}$ → Bandwidth of the channel.

max. data rate

- Given binary signal (two voltage levels), the max. data rate supported by B Hz is 2B bps.
- One signal → one bit.
- If signal has 4 levels, then a signal can be used to represent two bits : 00, 01, 10, 11.
- With multilevel signalling,

$$\boxed{C = 2B \log_2 M}$$

M = no. of discrete signal levels.
B = given bandwidth.
C = channel capacity in bps.

• For a noiseless channel, the Nyquist bit rate formula defines :-

$$\boxed{\text{Bit rate } (R) = 2B \log_2 L}$$

$L \rightarrow$ no. of signal levels.

Q) $B = 3000 \text{ HZ}$

$L = 2$

$R = ?$

$R = 2B \log_2 L$

$= 2 \times 3000 \times \log_2 2 = 6000 \text{ bps}.$

Q) Bit rate $(R) = 265$ kbps [we need to send 265 kbps]...

$B = 20 \text{ kHZ}$

$L = ?$

$R = 2B \log_2 L$

$265,000 = 2 \times 20,000 \times \log_2 L$

$L = 2^{6.625} = 98.7$ levels.

★ Shannon Capacity Formula :- [White noisy channel]

$$\boxed{\text{Capacity} = B \times \log_2(1+SNR)}$$

B → Bandwitch

SNR → Signal to noise ratio

Q) If SNR = 0, what is the capacity?

$C = B \times \log_2(1+SNR)$

$C = B \times \log_2(1+0)$

$C = B \times \log_2 1$

$C = B \times 0$

$\boxed{C = 0}$.

Q) SNR = 3162, B = 3000 HZ

C = ?

$C = B \times \log_2(1+SNR)$

$= 3000 \log_2(1+3162)$

$= 3000 \times 11.62$

$\boxed{C = 34{,}860 \text{ bps}}$.

Q) $SNR_{dB} = 36$

$B = 2$ MHZ

$C = ?$

Ans- $SNR_{dB} = 10\log_{10} SNR \rightarrow SNR = 10^{SNR_{dB}/10}$

$= SNR = 10^{3.6} = 3981$

So, $C = 2 \times 10^6 \times \log_2 3982 = 24$ Mbps.

→ When SNR is too high, then SNR+1 = SNR.

So, $\boxed{C = B \times \left(\frac{SNR_{dB}}{3}\right)}$

★ Latency :-

Latency = Propagation time + transmission time + queuing time + processing delay.

★ Performance Measurements :-

$$\boxed{\text{Throughput, } T = \frac{\text{Amount of data transffered}}{\text{Time taken to transfer the data}}}$$

$$\boxed{\text{Propagation Time} = \frac{\text{Distance}}{\text{Propagation speed}}}$$

$$\boxed{\text{Transmission time} = \frac{\text{Message Size}}{\text{Bandwidth}}}$$

Q) $B = 10$ Mbps.
12,000 frames per minute
10,000 bits.
Througput ?

An - $T = \frac{\text{Amount transffered}}{\text{Time taken}}$

$$= \frac{12,000 \times 10,000}{60} = 2 \text{ Mbps.}$$

Q) distance b/n 2 points = 12,000 km.
Propagation speed = 2.4×10^8 m/s.

Propagation time $= \frac{12,000}{1000} / 2.4 \times 10^8$
$= 50$ms

Computer Networks
CAT-2

★ Data Link Layer Design Issues:-

- 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.

- It has two sub-layers:-

→ Logical Link Layer
→ Media Access Control.

- The main functions and the design issues of this layer are:-

(i) Services provided to the network layer:-

- There are 3 types of services:-

→ Unacknowledged connectionless service.
→ Acknowledged connectionless service
→ Acknowledged connection-oriented service.

(ii) Framing:-
- How to break a bit-stream into frames.

MAC Control	Destination MAC Address	Source MAC Address	LLC PDU	CRC

- MAC Control:- contains control info for the functioning of the MAC protocol, eg. priority level.
- Destination MAC address:- the destination physical attachment point on the LAN for this frame.

- Source MAC address : the source physical attachment point on the LAN for this frame.
- LLC : The LLC data from the next higher Layer.
- CRC : Cyclic Redundancy check field , used to check if a transmission error has occured.

→ Framing Methods :-

(1) Character Count :-

- $\boxed{\text{First field}}$ in the frame's header = $\boxed{\text{Length of frame}}$

character count

(a) Without errors

5	1	2	3	4	5	6	7	8	9	8	1	2	3	4	5	6	7

Frame 1 — 5 characters; F.2 — with 5 ch.; F3 — with 8 ch.

~~5 1 2 3 4 7 6 7 8 9 8 0 1 2 3 4 5 6 8 7~~

(b) With errors

5	1	2	3	4	7	6	7	8	9	8	1	1	2	3	4	5	6	7

F1; F2; single character (can't determine 1st and last character) so error.

(2) Character / Byte stuffing :- (Before)

- ~~Inserts $\boxed{ESC}$ whenever a~~
- It is the process of adding one extra byte whenever there is a flag or escape character in the payload.
- Inserts $\boxed{ESC}$ before a $\boxed{FLAG}$ or $\boxed{ESC}$ is encountered.

Original characters — After stuffing

$\boxed{A}$ $\boxed{FLAG}$ $\boxed{B}$ → $\boxed{A}$ $\boxed{ESC}$ $\boxed{FLAG}$ $\boxed{B}$

$\boxed{A}$ $\boxed{ESC}$ $\boxed{B}$ → $\boxed{A}$ $\boxed{ESC}$ $\boxed{ESC}$ $\boxed{B}$

$\boxed{A}$ $\boxed{ESC}$ $\boxed{FLAG}$ $\boxed{B}$ → $\boxed{A}$ $\boxed{ESC}$ $\boxed{ESC}$ $\boxed{ESC}$ $\boxed{FLAG}$ $\boxed{B}$

$\boxed{A}$ $\boxed{ESC}$ $\boxed{ESC}$ $\boxed{B}$ → $\boxed{A}$ $\boxed{ESC}$ $\boxed{ESC}$ $\boxed{ESC}$ $\boxed{ESC}$ $\boxed{B}$

(3) Bits stuffing :- (After)

- If 5 consecutive 1's → Add 0 after

11111 → 111110

(Original msg). eg- Original → 001111110111110110

(stuffs 0) Bit stuffing → 0011111$\underline{0}$1.011111$\underline{0}$0110

(Removes the extra bits) Destination → 00111111110111110110

(iii) ★ Error Control :-

- Deliver Frames without errors, in the proper order to network layer.

→ Error control Mechanisms :-

- Ack / Nak : Provide sender some feedback about other end.
- Time - out
- Sequence numbers

→ Two types of Error control :-

1. Error detection — Checksum, CRC, parity check
2. Error correction — Hamming code ✓

For both.

→ Error detection :-

(1) CRC (Cyclic Redundancy check) :-

Frame :- 1101 011011

Generator (divisor) :- 10011] size of generator − 1 = no. of zero

5 − 1 = 4 0's add to frame.

Subtraction:
diff bits → 1
same bits → 0

```
10011 | 11010110110000
        10011
        010011        msb≠0 discard
         10011
         00000        discard
             10110
             10011
             0010100

             10100
             10011
             00 1110
```

CRC = 1110

Receiver

```
10011 ) 1101011011110 (add the remainder)
        10011
        010011
         10011
        00000010111
              10011
              0010011
                10011
                00000
```

```
10011 ) 11010110111110 (add the remainder)
        10011
        0100111
dis.     10011
         0000010111
dis.          10011
              00100111
                10011
          1.    000000 } NO error.
```

Generator polynomial.

$x^3 + 1$

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

$1 \quad 0 \quad 0 \quad 1 \rightarrow 4 - 1 = 3$ 0's

$\rightarrow x^7 + x^5 + x^2 + x + 1$

$1 \; 0 \; 1 \; 0 \; 0 \; 1 \; 1 \; 1 \rightarrow 8 - 1 = 7$ 0's.

(2) Parity Check :-

- even parity → if no of 1's are even.
- odd parity - if no. of 1's are odd.

eg :- 101011~~1~~ size = 7 bits. Do in even parity.

↓

10101111 (even parity)

odd parity

eg - 1010 ~~send~~ {2 1's} Sender

↓

10101 {3 1's} Receiver.

→ Two dimensional parity check :- (Make it even on both row and column)

1100111 1011101 0111001 0101001

1	1	0	0	1	1	1	1	Row parity
1	0	1	1	1	0	1	1	~~Row parities~~
0	1	1	1	0	0	1	0	
0	1	0	1	0	0	1	1	
0	1	0	1	0	1	0	1	~~Column parities~~

1001111 10111011 01110010 01010011 01010101

(3) Checksum :-

Steps :-

(i) 'k' segments and 'm' bits.
(ii) Add all the segments.
(iii) If carry is 1, then add it to LSB of sum.
(iv) check sum → Complement of sum
(v) msg + checksum.

10110011 | 10101011 | 01011010 | 11010101

K = 4
m = 8

```
    10110011   [1st seg]
+   10101011   [2nd seg]
   ----------
   101011110
          →1
+  ----------
    01011111
+   01011010   [3rd seg]
   ----------
    10111001
+   11010101   [4th seg]
   ----------
   110001110
          →1
   ----------
    10001111   → Final sum.
```

Check sum = complement the sum
01110000 → It will become the 5th segment in receiver side.

Receiver's side :-

- If after complementing the checksum, ~~it~~ we get all zeroes then data is correct.

~~10010000~~

~~10001111~~ [~~Final sum~~]
~~10010000~~ [

10001111 [Final sum]
+ 01110000 [Checksum] [5th Seg.]

11111111

~~Complem~~ check sum = complement the ~~checksum~~ sum.

00000000 ✓ Accept data.

(4) Hamming Code :- (Even parity).

'm' · any no. of bits → 4 bits (1010)
↓
message (sdy).

parity bits (or) redundancy bits.

How many parity bits?

$$\boxed{2^r \geq m + r + 1}$$ [m = 4] [size of msg].

$r = 1 \Rightarrow 2 \geq 6$ ✗

$r = 2 \Rightarrow 4 \geq 7$ ✗

$r = 3 \Rightarrow 8 \geq 8$ ✓ ~~3 bits~~ ~~3 bits~~ $\boxed{\text{3 parity bits}}$

- Three parity bits → $2^0, 2^1, 2^2$
  1 2 4 → Position.

Original msg / Parity bits

7	6	5	4	3	2	1
1	0	1	P3	0	P2	P1

$3 \rightarrow 2^3 = 8$.

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

even parity.

P_1 – 1, 3, 5, 7. $P_1 = P_1, 0, 1, 1$ (0)
$P_1 = 0$.

$P_2 \rightarrow 2, 3, 6, 7$ $P_2 = P_2, 0, 0, 1$ (1)
$P_2 = 1$

$P_3 \rightarrow 4, 5, 6, 7$. $P_3 = P_3, 1, 0, 1$ (0)
$P_3 = 0$

Message = 1010010

Receiver side :-

P_1 = 0 0 1 1 → even → 0
P_2 = 1 0 0 1 → even → 0
P_3 = 0 1 0 1 → even → 0

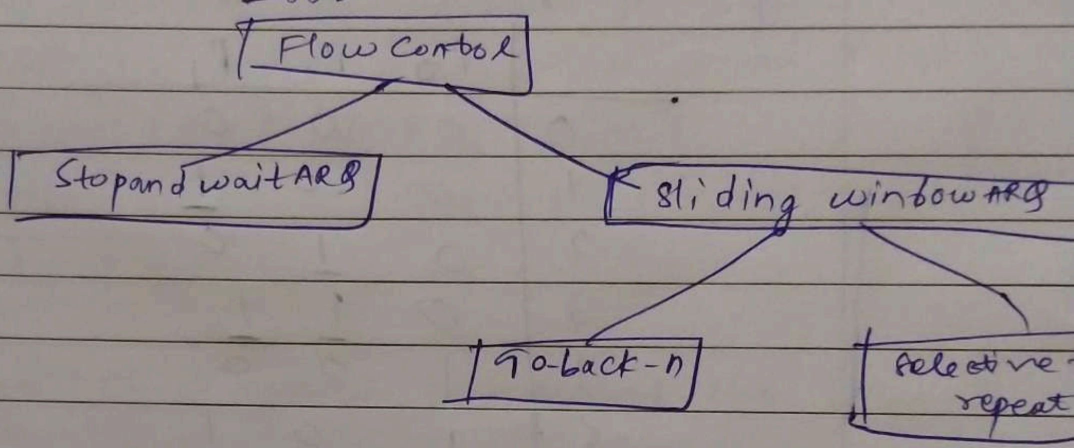
As all the values are 0, accept data.

(iv) Flow Control :-

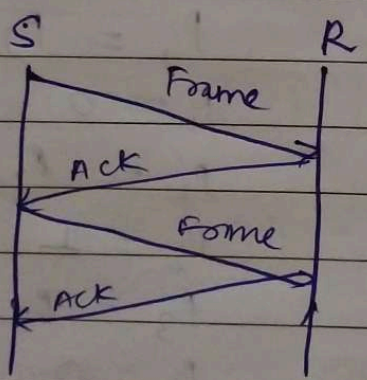
- Flow control coordinates the amount of data that can be sent before receiving acknowledgement.

~~Error~~.
~~Flow Control~~

~~Error~~



(1) Stop and Wait Protocol :-

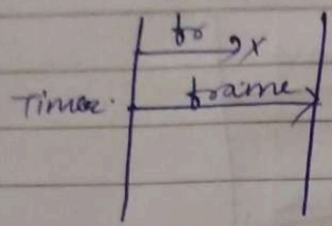


(i) Frame lost
(ii) Acknowledgement lost
(iii) Delayed Acknowledgement.

Stop and wait protocol ARQ = (All 3).

_/_/__

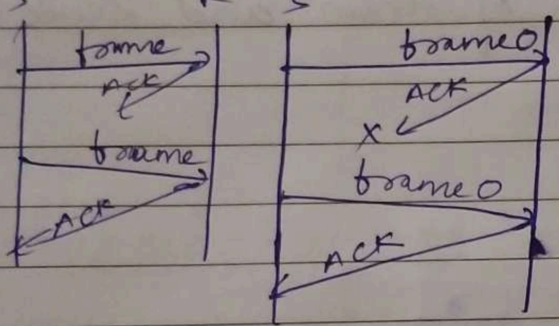
(i) Frame lost.



Stop and wait + timer → waits for the given ~~time and~~ then the frame reaches the receiver.

= Stop and Wait ARQ → Automatic Repeat Request.

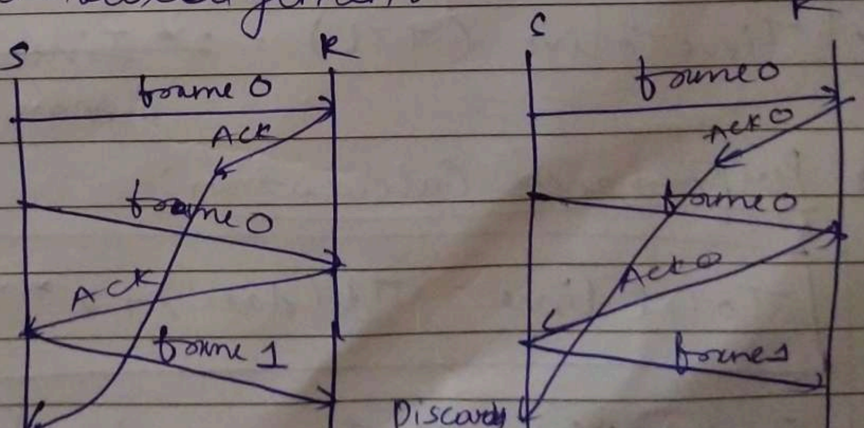
(ii) Acknowledgement lost.



Duplicate frame.
(Discard frame).

Add the sequence number to the frame so that the receiver can identify that it is the same old frame. Then discards the frame as it is duplicated and then sends the full acknowledgement.

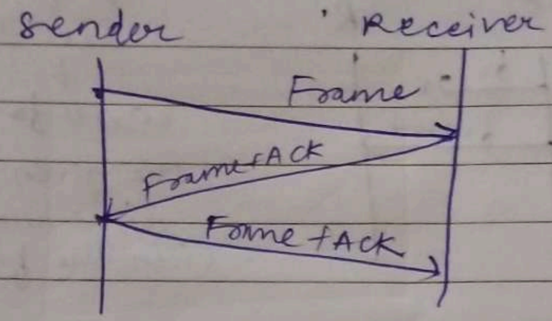
(iii) Delayed Acknowledgement.



Add sequence number to Acknowledgement so that ~~if it~~ it can identify then discard the old acknowledg acknowledgement

It saves bandwidth.

* **Piggybacking :-** ~~Methode~~.



- Instead of sending frames and acknowledgement, it combines both of them and sends them.

* **Useful Terms :-**

- Propagation Delay = $\frac{\text{Distance between routers}}{\text{velocity of Propagation}}$

- Round Trip Time (RTT) = 2 × Propagation Delay.

- Time Out (TO) = 2 * RTT.

- Time To Live (TTL) = ~~2* Time~~ 2 × Time out. (Max. TTL is 180 secs).

* **Performance Calculation :-**

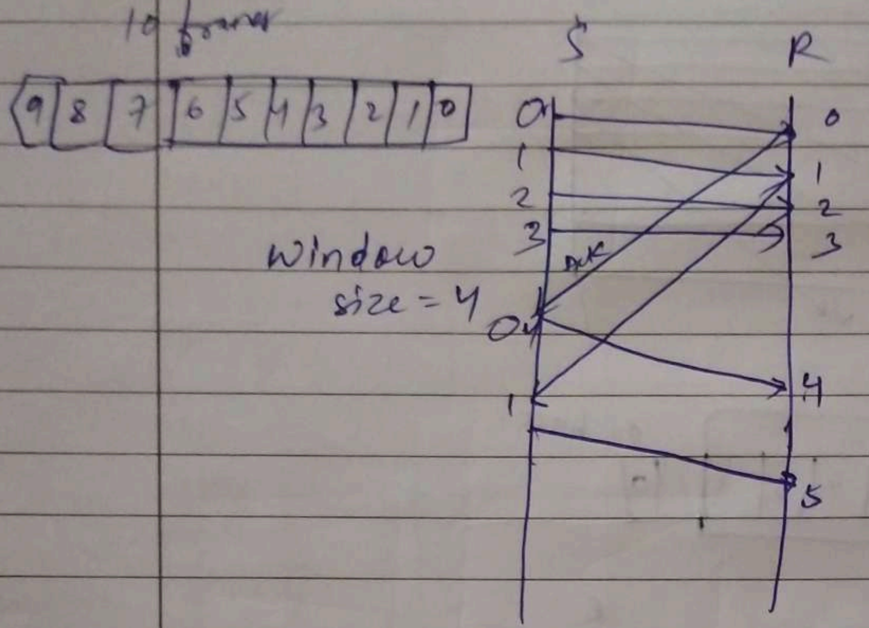
$$\boxed{\text{Total time} = T_t(\text{data}) + 2 * T_P}$$

~~Int~~ T_t(data) = Transmission delay for data packet

T_P = propagation ~~/ dea~~ delay for data packet / acknowledgment

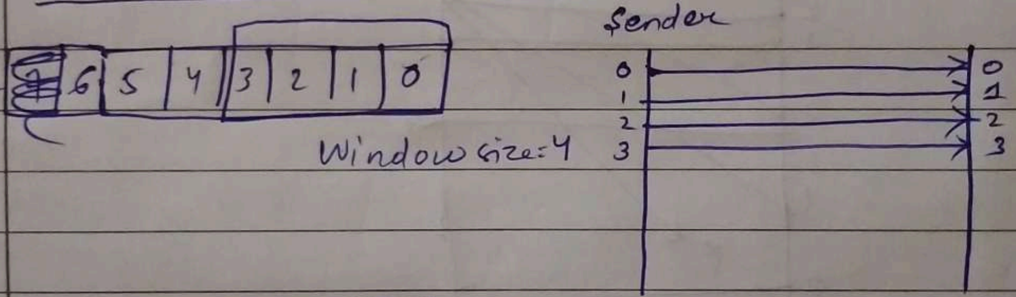
* Sliding Window Protocol :-

10 frames

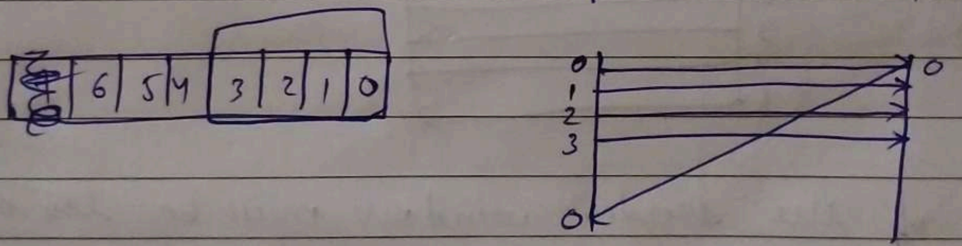


(1) GO-BACK - N ARQ Protocol :-

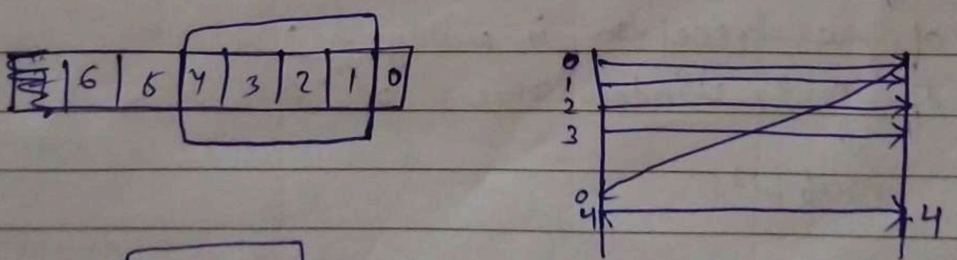
Step1 :-



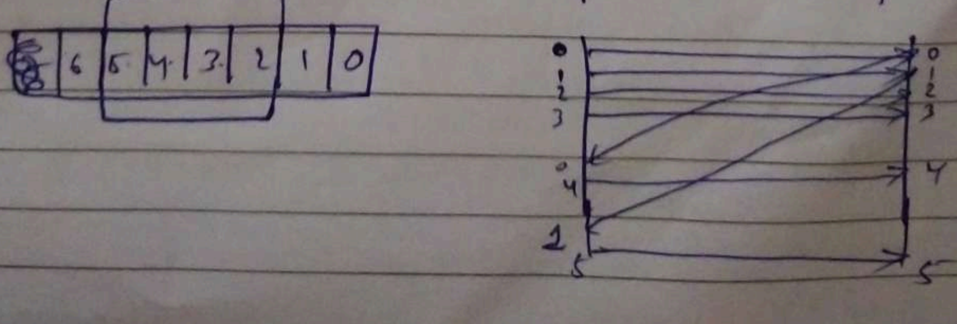
Step2 :-



Step3 :-



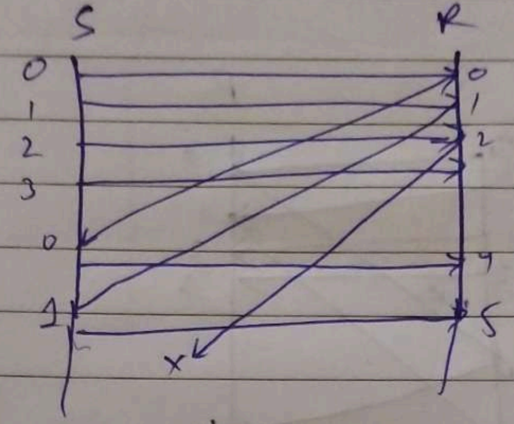
Step4 :-



Normal go back ~~arr~~ N ARQ will continue same wise till the last.

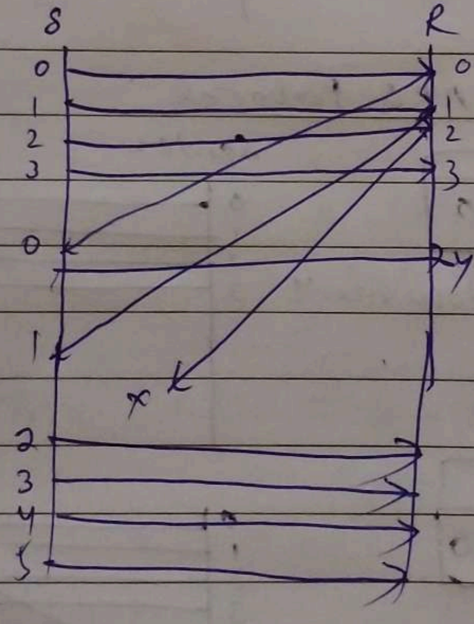
__/__/____

(Lost) Ack. **Step 5 :-** | 6 | 5 | 4 | 3 | 2 | 1 | 0 |



go back.

Step 6 :- | 6 | 5 | 4 | 3 | 2 | 1 | 0 |



- Size of the sender window must be less than 2^m.

Size of the receiver is always 1.

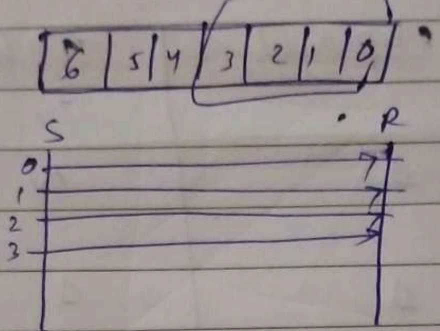
If $m = 2$, window size $= 2^m - 1 = 3$
↓
no. of bits.

(2) Selective Repeat ARQ protocol :-

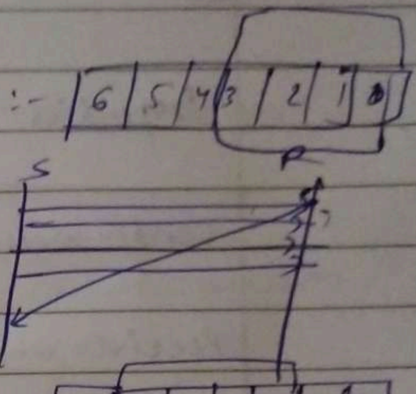
Lost frame :-

Step 1 :-

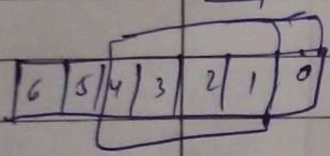
WS = 4

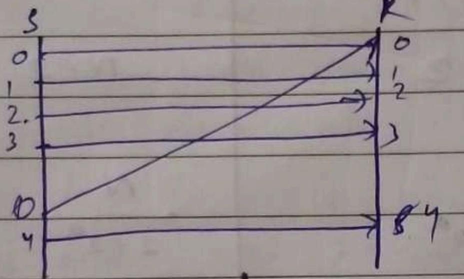


Step 2 :-

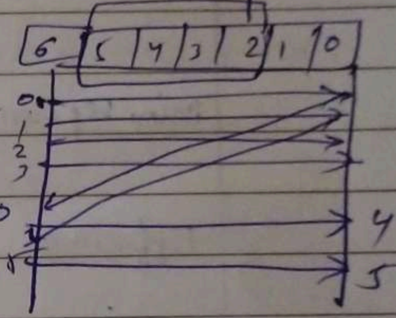


Step 3 :-

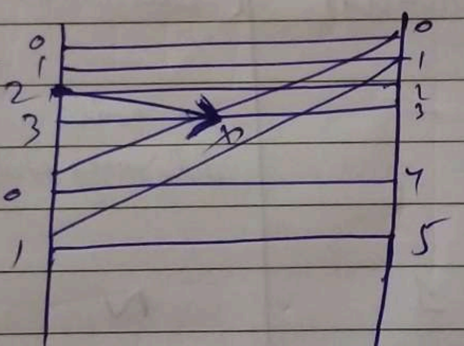


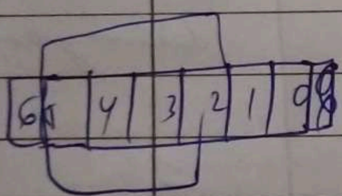


Step 4 :-

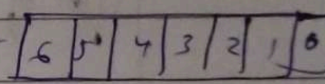


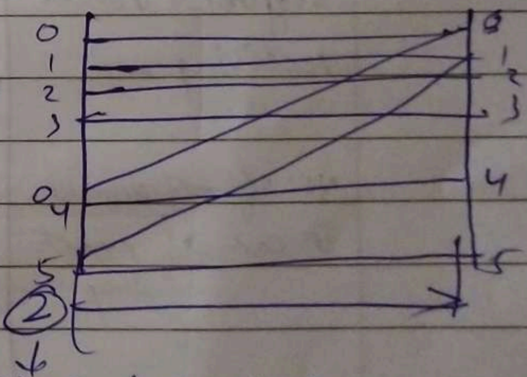
Step 5 :-





Step 6 :-





single frame.

- Size of sender and receiver windows must be at most one half of 2^m.

If $m = 2$, window size $= 2^m/2 = 2$.

_/_/_

* Comparision b/w Stop and wait, Go back N and Selective Repeat ARQ

Properties	Stop and wait	Go back N	Selective repeat
Sender window size	1	N	N
Receiver window size	1	1	N
Min. sequence no	2	N+1	2N
Efficiance	$\frac{1}{1+2a}$	$\frac{N}{1+2a}$	$\frac{N}{1+2a}$
Type of Ack.	Individual	Cumulative	Individual
Supported order at receiving end	-	In-order delivery only.	out-of-order delivery as well
No. of retransmission in case of packet drop.	1	N	1

* LAN Technologies :-

(1) Media Access :-

- Ethernet and Wi-fi are both "multi-access" technologies.

→ Broadcast medium, shared by many hosts.
→ Simultaneous transmissions will result in collision.

- Media Access Control (MAC) protocol required.

→ Rules on how to share medium.

- The Data link layer is divided into two parts :- MAC Sublayer and LLC (Logic Link Control) Sublayer

(2) Ethernet :-

- Bus Topology / Star.
- Carrier - Sense multiple access with collision detection (CSMA/CD).

→ ~~CS = C~~

- Base Ethernet ~~is~~ standard is 10 Mbps.

→ Ethernet Frame Format :-

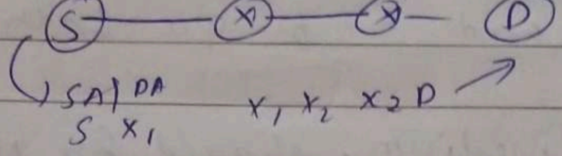
PREAMBLE	SFD	DA	SA	length	DATA	CRC
7B	1B	6B	6B	2B	46B-1500B	4B

- Preamble → 1010101
  SFD → 1 byte-11 → 1010101<u>1</u> } 56 Bits

_/_/_

- Destination Address :- 6B.
- Source Address - 6 B.

} 48 bits — frame is received by all adapters on a LAN and dropped if addresses does not match



- length → 2B → 16 bits, length of data field.

- Data : 46B - 1500 B. Max. 1500 bytes, min. 46 bytes. If data is less than 46 bytes, pad with zeroes to 46 bytes.
- CRC :- 4B. - 4 bytes generated using CR - 32, Checked at receiver; if error is detected, the frame is simply dropped.

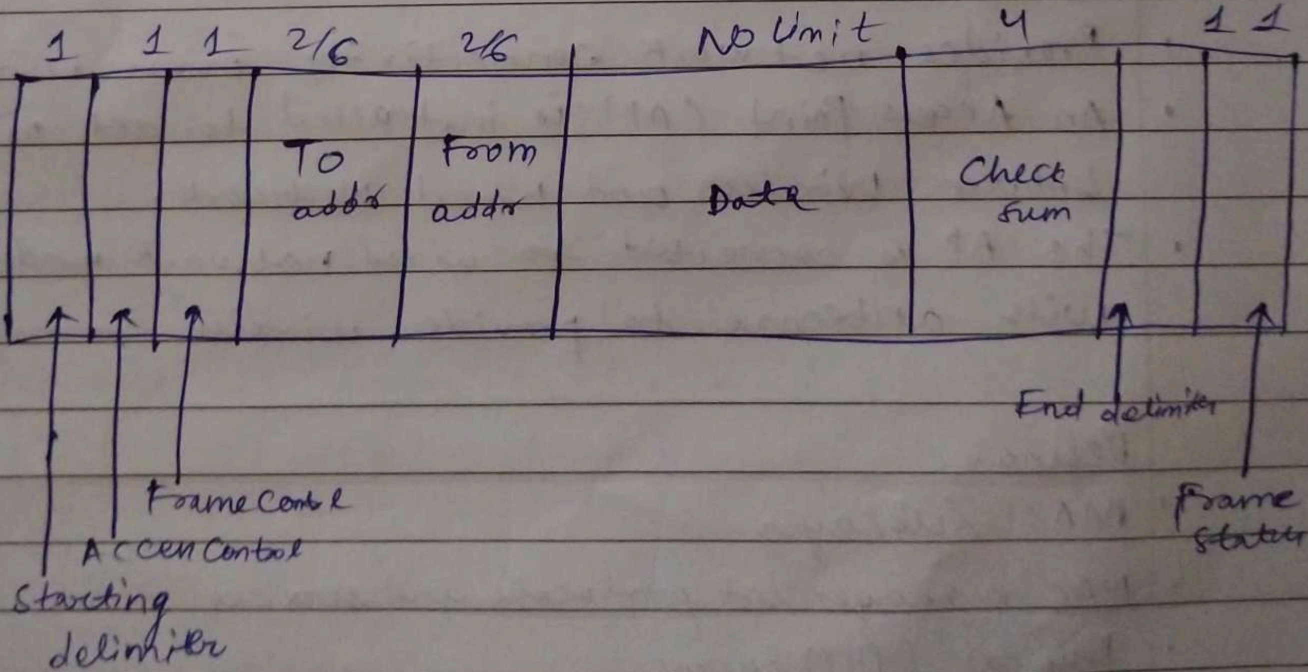
→ Fast / Gigabit Ethernet Outline :-

- Fast Ethernet
  - 100 Base T4
  - 8B/6T encoding
  - 100 Base TX
  - 100 Base FX
  - collision domains
-
- Gigabit Ethernet
  - 1000 Base SX
  - 8B/10B encoding
  - Fiber Channel

★ IEEE 802.5 (Token Ring) : Ring Topology :-

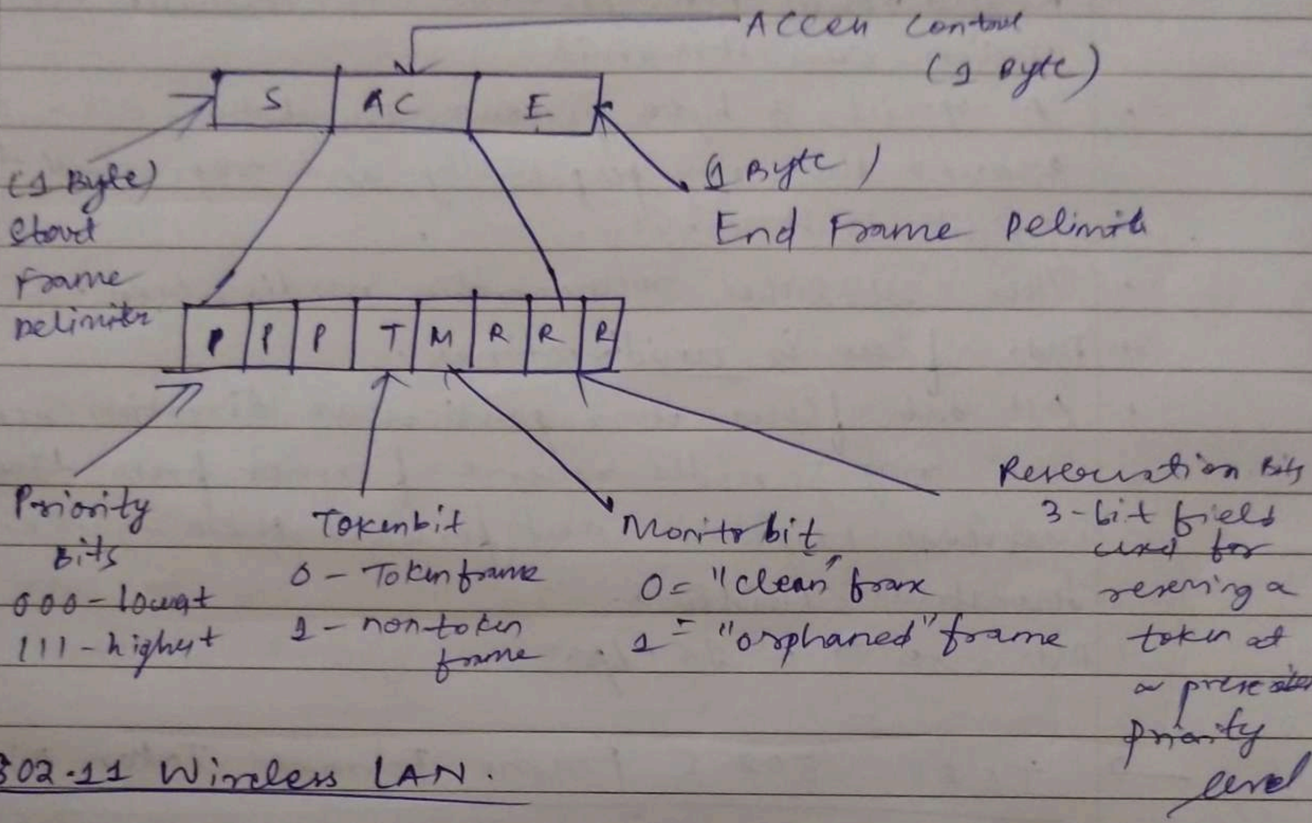
- Shared ring medium : all nodes see all frames.
- Round Robin MAC Protocol : determines which station can transmit.
- A special 3-byte pattern, the token, circulates around the ring perpetually and represents the "right to transmit".
- This establishes round-robin media access.
- Data flow is unidirectional.
- All data flows in a particular direction around the ring; nodes receive frames from their upstream neighbour and forward them to their downstream neighbour.
- Data rate :4 or 16 Mbps.

→ IEEE 802.5 Frame Format Token Ring :-



→ Token Frame Format

1	1	1
SD	AC	ED



★ 802.11 Wireless LAN.

- Provides network connectivity over wireless media.
- An Access Point (AP) is installed to act as Bridge between Wireless and Wired Network.
- The AP is connected to wired network and is equipped with antennae to provide wireless connectivity.

Defines

- MAC sublayer
- MAC management protocols and services.
- Physical (PHY) layers.

→ IR

→ FHSS

→ DSSS

- Station services:
  - authentication
  - de-authentication
  - privacy
  - delivery of data.
- Distribution services.
  - association
  - disassociation
  - reassociation
  - distribution

★ **HDLC :- High Level Data Link Control**

Features-

(i) Reliable protocol

→ selective repeat or go-back-N

(ii) Full-duplex communication

→ receive and transmit at the same time.

(iii) Bit-oriented protocol.

→ use bits to stuff flags occurring in data. i.e., it does not recognize or interpret byte value.

(iv) Flow control

- adjust window size based on receiver ~~capacity.~~ capability.

(v) Uses physical layer clocking and synchronization to send and receive frames.

→ Frame format of HDLC

1	1 or 2	1 or 2	Variable	2	1
Flag	Address	Control	Data	FCS	Flag

~~Information (I~~

→ Types of Frame :-

- I-Frame - I-frames or Information frames carry user data from the network layer. They also include flow and error control information that is piggybacked on user data. The first bit of I-frame is 0.

I-frame format

Receive sequence number	Poll final	Send sequence number	0

- S-Frame :- S-frames or supervisory frames do not contain information field. They are used for flow and control when piggybacking is not required. The first two bits of control field of S-frame is 10.

S-frame format

Receive sequence number	Poll final	Function code	0	1

- U-frame :- U-frames or Un-numbered frames are used for myriad miscellaneous functions, like link management. The first two bits are 11.

U-frame format.

Function Code	Poll final	Function code	1	1

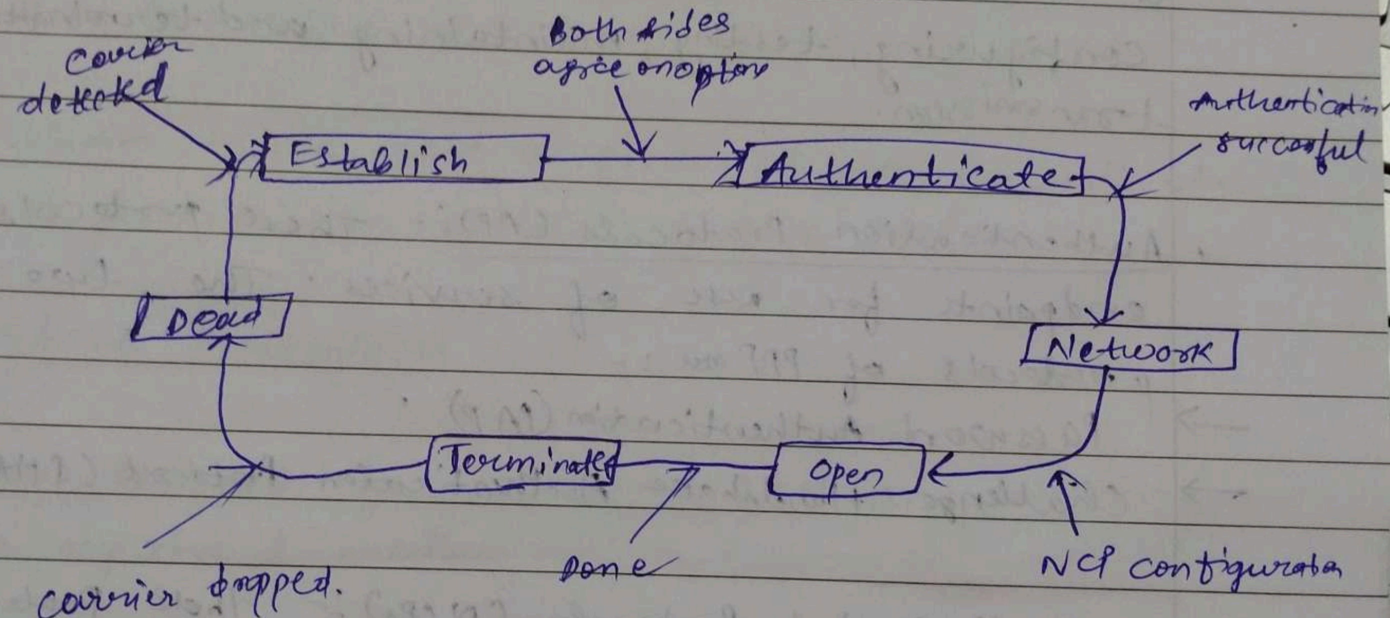
* PPP (Point-to-Point Protocol) :-

- Point-to-Point Protocol (PPP) is also data link ~~layer~~ protocol used on serial links just like HDLC.

- PPP ~~is~~ has more advanced features than HDLC :-

→ Link quality management features monitors the quality of the link. ~~of too~~

→ Supports PAP and CHAP authentication.



A simplified phase diagram for bring a line up and down.

→ PPP Frame :-

~~Flag~~

Flag	Address	Control	Protocol	Information	CRC	Flag
01111110	11111111	00000011				01111110

Address: All station are to accept the frame.

Control: Unnumbered frame

- PPP uses byte stuffing.
- Problems.

→ Components of PPP:-

- Encapsulation component:- It encapsulates the datagram so that it can be transmitted over the specified physical ~~by~~ layer.

- Link Control Protocol (LCP):- It is responsible for establishing, configuring, testing, maintaining and terminating links for transmission.

- Authentication Protocols (AP):- These protocols authenticate endpoints for use of services. The two authentication protocols of PPP are:-
→ Password Authentication (PAP).
→ Challenge Handshake Authentication Protocol (CHAP)

- Network Control Protocols (NCPs):- These protocols are used for negotiating the parameters and facilities for the network layer.

* ~~Multi~~ _/_/_

Multiple Access Protocols (MAC)

- Random Access Protocols
  - Aloha
  - CSMA
  - CSMA/CD, CSMA/CA
- Control Access
  - polling
  - Token Passing
- Channelization protocols
  - FDMA
  - TDMA

• **Problem :-** When two or more nodes transmit at the same time, their frames will collide and the link bandwidth is wasted during collision.

→ **Solution :-** We need a protocol to coordinate the transmission of the active nodes.

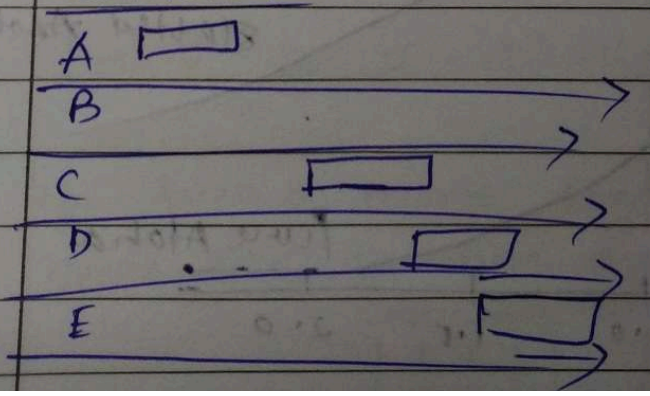
* Aloha Protocols:-

• was designed for wireless LAN and can be used for any shared medium.

(1) Pure Aloha :-

• Frame is resent after random amount of time which is known as back-off.

Collision



If the frame transmission time is $\boxed{T \text{ sec}}$, then the vulnerable time is $\boxed{2T \text{ sec}}$

- The throughput (S) for pure Aloha is

$$\boxed{\underbrace{S}_{\text{efficiency}} = G \times e^{-2G}}$$

G → avg. no. of frames generated by the system.

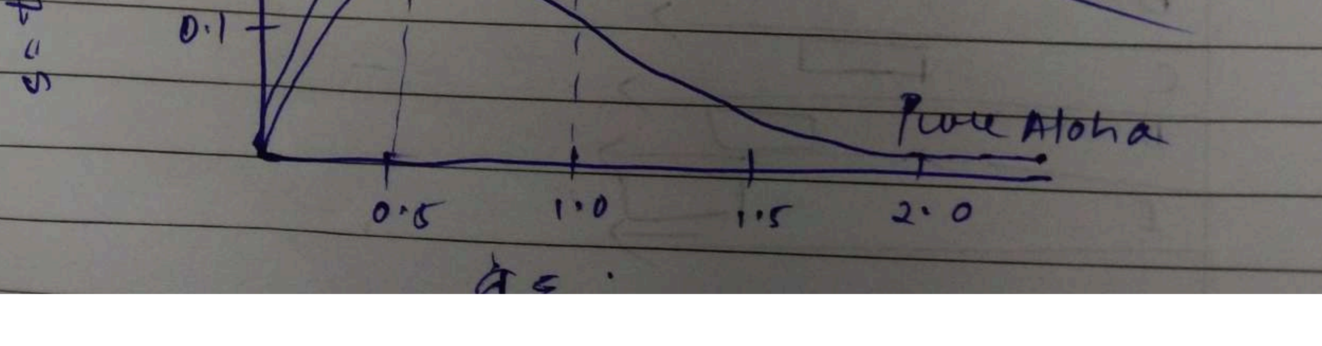
- The max. throughput, $\boxed{S_{max} = 0.184}$ when $\boxed{G = 1/2}$

(2) <u>Slotted Aloha:-</u>

- enhanced version of Pure Aloha.
- Max. channel utilization is 37%.
- The throughput for slotted Aloha is

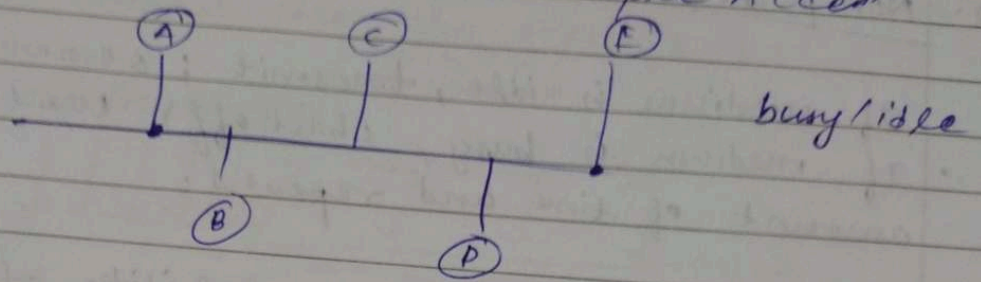
$$\boxed{S = G \times e^{-G}}$$

- The max. throughput, $\boxed{S_{max} = 0.368}$ when $\boxed{G = 1}$.



_/_/_

* CSMA (Carrier Sense Multiple Access).



- For a message to be sent, we check that the destination is busy/idle, if idle then it starts sending the msg. ~~other~~ If busy, it waits until it becomes idle.

- This reduces the possibility of collision but it can't eliminate it because of long propagation delay.

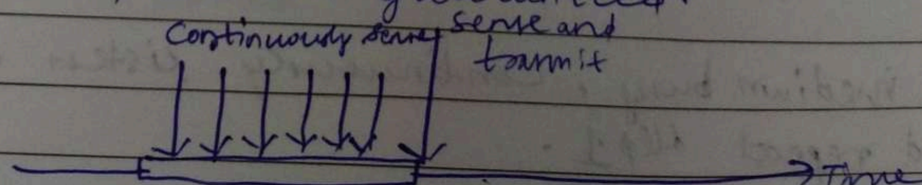
- Vulnerable time for CSMA is the maximum propagation time.

→ Types :-

1. 1-persistent CSMA

- To avoid idle channel time.
- If medium idle, transmit immediately.
- If medium busy, continuously listen until medium becomes idle; then transmit immediately with probability 1.

- If two or more stations become ready at the same time, collision guaranteed.

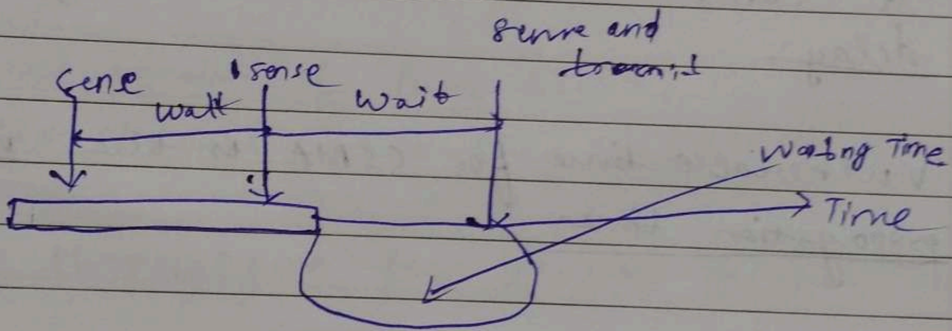


2. Non-persistent CSMA :-

- If medium is idle, transmit ; otherwise go to 2.
- If medium is busy, (back off), wait a random amount of time and repeat 1.

- Random delays reduces probability of collisions because two stations with data to be transmitted will wait for diff. amount of times.

- Bandwidth is wasted if waiting time (back off) is large because medium will remain ~~die~~ idle following end of transmission.



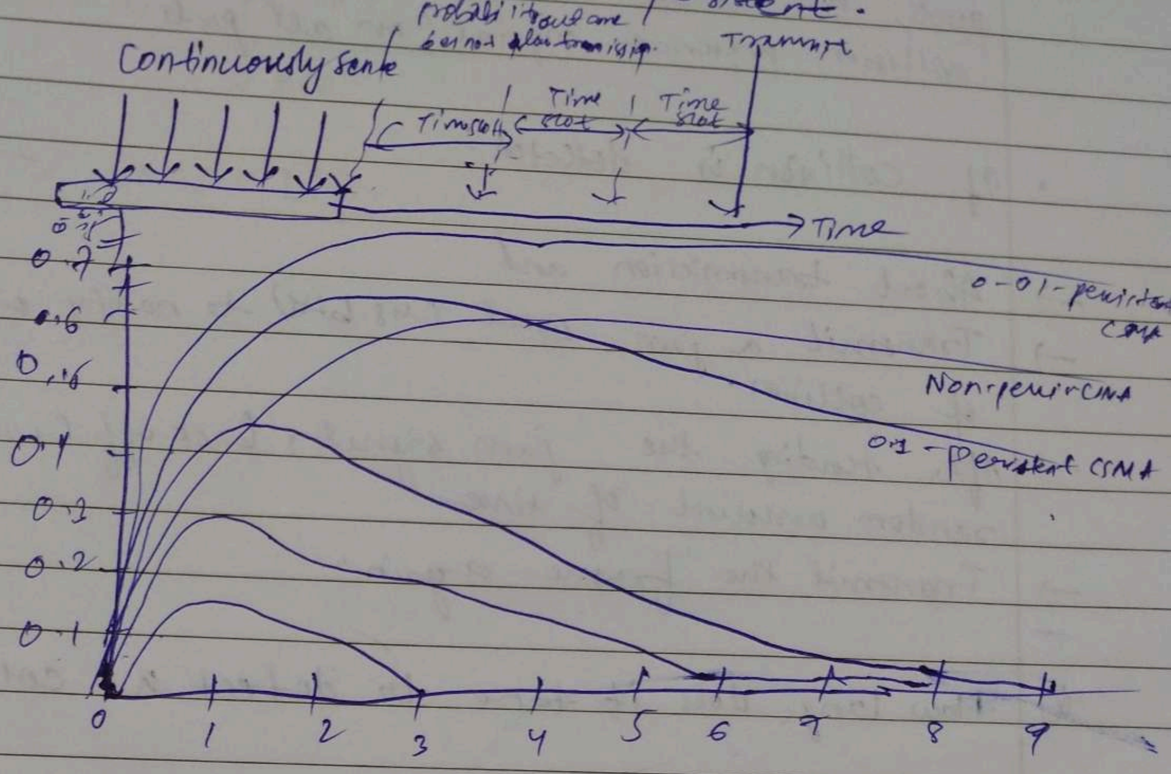
3. P-persistent CSMA :-

- Time is divided to slots where each Time unit (slot) typically equals maximum propagation delay.

- If medium idle,
→ transmit with probability (p), OR
→ wait one time unit (slot) with probability (1-p), then repeat 1.

- If medium busy, continuously listen until idle and repeat step 1.

- Reduces the possibility of collision like non-persistent.
- Reduces channel idle time 1-persistent.



* CSMA/CD Protocol:- (Collision Detection)

- While transmitting, the sender is listening to medium for collisions.
- Sender stops transmission if collision has occurred reducing channel wastage.
- Widely used for bus-topology LANs.

→ How does a node detect a collision?

- Transceiver:- A node monitors the media while transmitting. If the observed power is more than transmitted power of its own signal, it means collision occurred.

__/__/__

- Hub :- if input occur simultaneously on two ports, it indicates a collision. Hub send a collision presence signal on all ports.

- If collision is detected :-

→ Abort transmission and
→ Transmit a jam signal (48 bits) to notify other stations of collision.
→ After sending the jam signal, back off (wait) for a random amount of time
→ Transmit the frame again.

Q) How long does it take to detect a collision?

Ans- In the worst case, twice the max. propagation delay of the medium.

- Transmission time (T_t)
- Propagation time (T_p).

Frame size, Bandwidth

$$\boxed{S > \frac{2BL}{P}}$$

→ Length
→ Propagation speed.

$$\boxed{T_t >>= 2 * T_p}$$

To ensure tighter bound, to detect the collision completely.

Q) CSMA/CD protocol running at 1 Gbps over a 1 km with no repeaters. speed = 2×10^8 m/s.
Min. frame size?

Frame size $S > 2BL/P$

$L = 1 km = 1000 m$.

Propagation speed $P = 2 \times 10^8$ m/s.

Bandwidth = 1 Gbps = 10^9 bps.

$S >= 2 * bandwidth * T_p$ // $\left(T_p = \frac{L}{P}\right)$

$$S >= \frac{(2 * 10^9 * 1000)}{2 \times 10^8}$$

$S \geq 10000$ bits.

Module -4

Network Layer

_/_/___

★ **Duties of Network Layer :-**

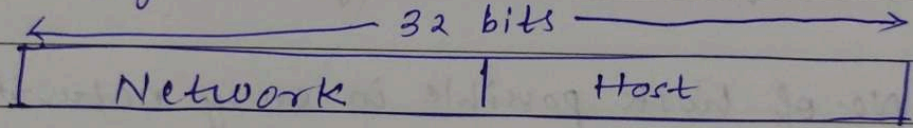
- Internetworking
- Adressing
- Routing
- Packetizing
- Fragmentation.

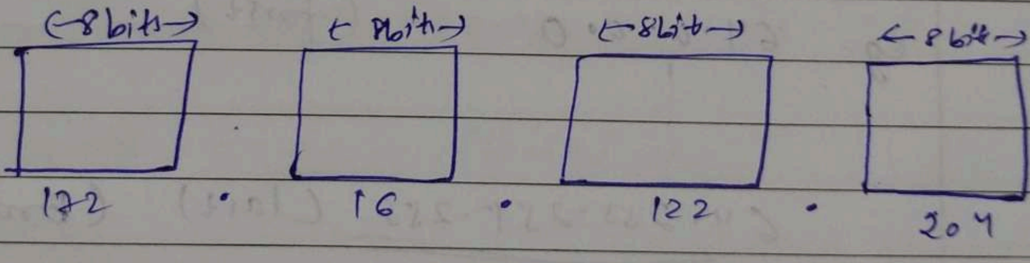
★ **IPV4 :- Internetnetworking Protocol**

- Connectionless
- Datagram service.

Header Size = 20-60 Bytes
Payload → 0-6 5515 Bytes.

★ **IPVP Adressing :-**





- Addresses 0.0.0.0, 127.0.0.1 and 255.255.255.255 carries special meaning.

Q) Binary notation to dotted.

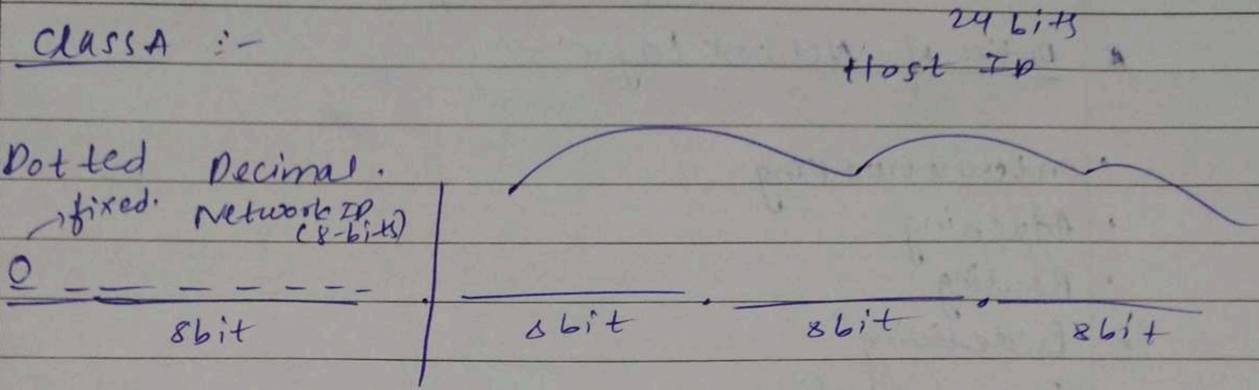
a. 10000001 00001011 00001011 11101111

A- 129 . 11 . 11 . 239 (8421).

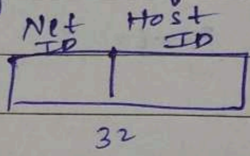
__/__/____

(1) <u>ClassA</u> :-

Dotted Decimal.



- $\boxed{2^{31}}$ → no. of IP Adresses in ClassA.



- 2^7 = 128 blocks
- $\boxed{\text{No. of networks in CA} = 2^7 = 128}$

~~Tot~~ Total usable 128-2 = 126

- Value from 0-127. (first value).
- No. of hosts possible in every network = $2^{24} - 2$

eg- 64.0.0.0 (first)

64.255.255.255 (last) (Broadcast Address)

- $\boxed{\text{Default Mask} = 255.0.0.0}$
- To find the host, do AND operation between the given ~~ad~~ IP address and the default address.

AND = 1 1 → 1
rest 0.

__/__/____

eg - 64.0.0.8

	01000000 . 0 . 0 . 00001000	→ Given.
AND	11111111 . 0 . 0 . 00000000	→ Default Mask
	01000000 . 0 . 0 . 0	

64.0.0.0 → Host.

(2) Class B :-

fixed. 8-bit 8bit 8-bit 8bit

10 _ _ _ _ _ _ . ____ . ____ . ____

- No. of networks in CB. = 2^{14} = 16,384 blocks.
- Value from 128 - 191 (first value)
- ~~eg~~- No. of addresses = 2^{30} = 25%.
- No. of hosts in each network = $2^{16} - 2$.

eg - 128.0.0.0 (first)

⋮

128.0.255.255 (last)

$\boxed{\text{Default mask} = 255.255.0.0}$

Q) 130.2.3.4 → CB.

To get host → AND with default mask.

(3) Class C :-

first 8 bits . 8 bits . 8-bits . 8-bits

1 1 0 _ _ _ _ _ . ____ . ____ . ____

- Range - 192 to 223
- No. of networks = 2^{21} = 2,097,152
- No. of hosts = $2^{8}-2$
- Default mask = 255.255.255.0
- No. of IP Address = 2^{29} (12.5%)

eg- 194.2.3.4 .

(4) Class D and class E :-

→ Class D

fixed 8-bits . 8-bits . 8-bits . 8-bits.

1 1 1 0 _ _ _ _ . ____ . ____ . ____

- Range - 224 - 239 .
- No. of IP addresses - 2^{28} (6.25%)

→ CLASS E :- fixed. (Reserved for future purpose)

1 1 1 1 _ _ _ _ . _ . _ . _

- Range - 240 - 255
- No. of IP address - 2^{28} = (6.25%)

	Class A	Class B	Class C	Class D	Class E
Range	0 - 127	128 - 191	192 to 223	224 - 239	240 - 255
No of network	$2^7 = 128$	$2^{14} = 16,384$	$2^{21} = 2,097,152$	—	—
Default mask	255.0.0.0	255.255.0.0	255.255.255.0	—	—
No of hosts	$2^{24} - 2$	$2^{16} - 2$	$2^8 - 2$	—	—
No of IP Address	2^{31} (50%)	2^{30} (25%)	2^{29} (12.5%)	2^{28} (6.25%)	2^{28} (6.25%)

CA | B |

★ Classful Addressing :-

Disadvantages :-

- Wastage of IP Addresses
- Maintenance is time consuming.
- More prone to errors.

★ Classless Addressing :-

- No classes
- Only Blocks

← 32 →

Block ID	Host ID

- Notation.

x · y · z · w/n ⟶ mask / no. of bits represent Block

no. of 1's

eg - 200·10·20·40 /28 → 28 no. of 1's.

→ For mask :-

32

28	4
B.ID	H.ID

No. of hosts = $2^4 = 16$

$\underbrace{11111111 . 11111111 . 11111111 . 1111}_{28 \text{ no of 1's}}0000$

255 · 255 · 255 · 240 (Mask of this network).

→ For network ID :-

200·10·20·40 /28

200·10·20· 00101000

8 8 8 ← 28 → 40

0000 } convert to 0000

__/__/__

200 · 10 · 20 · 32/28 → Network / Block ID

or

to get the network ID
AND operation of mask with given IP address.

→ Rules :

(i) Address should be contiguous.
(ii) No. of addresses in a block must be in power of 2.
(iii) First address of every block must be evenly divisible with size of block.

Q) Given the CIDR representation 20.10.30.35/27. Find the range of IP Addresses in the CIDR block.

Ans – 27 bits means 32 − 27 = 5 bits.

$\boxed{27 | 5}$ 27 no. of 1's

No. of hosts = 2^5 = 32

128 64 32 16 8 4 2 1

$\underbrace{11111111 \cdot 11111111 \cdot 11111111 \cdot 111}_{27 \text{ no. of 1's}}00000$

255 · 255 · 255 · 224 (mask of this network)

Network ID :-

~~20 · 10 · 30 · 35~~

~~20~~ 225 · 225 · 225 · 224
20 · 10 · 30 · 35

20 · 10 · 30 · 32 , [start]
⋮
20 · 10 · 30 · 63

} 32 addresses.

_/_/_

* Subnetting :-

- Dividing the big network into small networks.

eg - 200.10.20.0

No. of hosts = 256 → usable 256 - 2 = 254
in class C.

→ fix

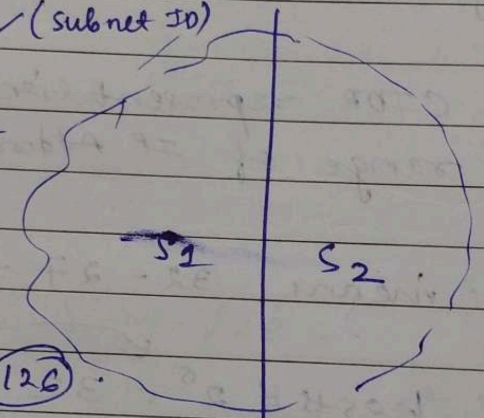
msb fix
S1 {
200.10.20. 0 0 0 0 0 0 0 0
200.10.20. 0 1 1 1 1 1 1 1
~~200.10.20. 1 _ _ _ _ _ _ _~~
} ~~One network.~~ Two ~~equal~~ networks

200.10.20.0 ✓ (subnet ID)

to

200.10.20.127
(Broadcast Address)

No. of hosts
= 0 - 127 = 128
- 2 = 126.



S2
200.10.20. 1 0 0 0 0 0 0 0

200.10.20. 1 1 1 1 1 1 1 1

Range
200.10.20.128 (subnet ID)

to

200.10.20.255 (Broadcast Addr)

No. of hosts - 128 - 255 ⇒ 128 - 2 = 126.

126 + 126 = 252.

→ For four subnets,

S_1 = Fix 00

S_2 = Fix 10.

S_3 = Fix 01

S_4 = Fix 11

Q) An address in a block is given as 73.22.17.25. Find the no. of addresses in the block, the first address and the last address.

An- No. of address in this blocks are.

$N = 2^{32-n} = 2^{24}$.

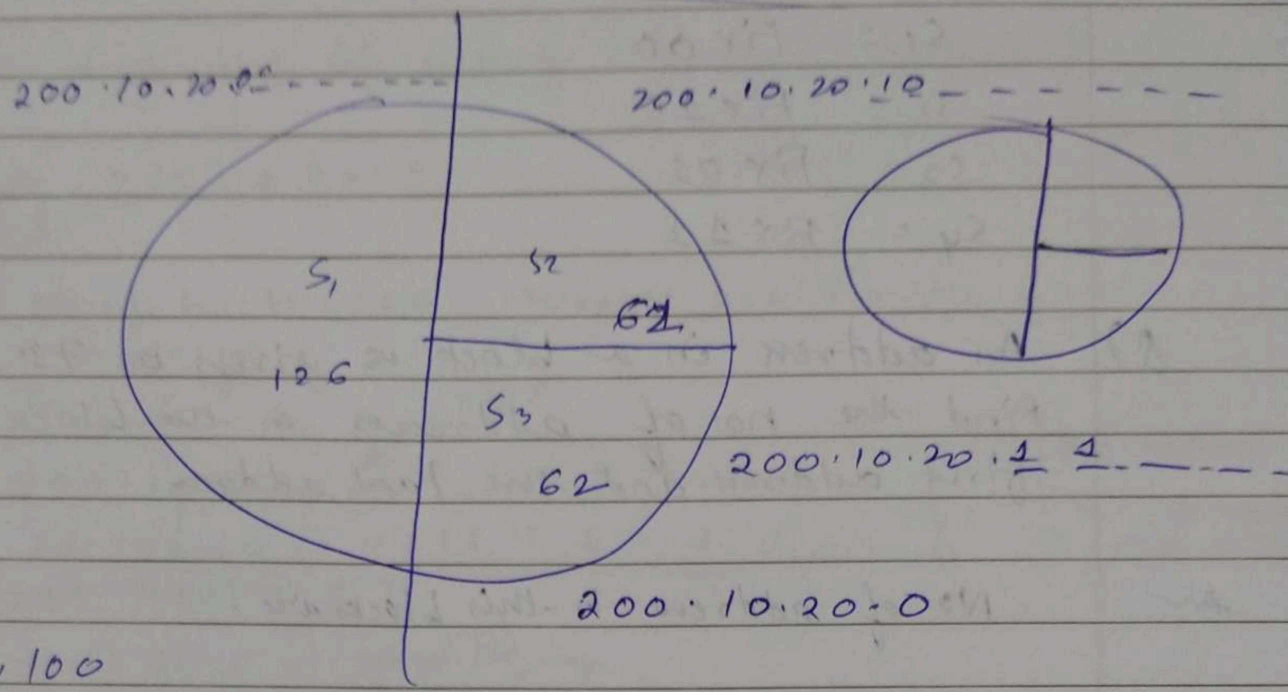
To find first address, left most bits 8 bits and set rightmost 24 bits to 0s.

~~2~~ 73.0.0.0

Last - rightmost 24 bits to 1s.

73.255.255.255

* Variable length subnet Marking :-



(i) 100

(ii) 50, 50

S1 → 200 . 10 . 20 . 0 _ _ _ _ _ _ _

fix

200 . 10 . 20 . 01111

200.10.20.0
to
200.10.20.127

128-2

S2 → 200.10.20.10000

200.10.20.1011111

200.10.20.128
to
200.10.20.191

64-2

$S_3 \rightarrow$ 200 · 10 · 20 · 11 0 0 0 0 0 0

⋮

200 · 10 · 20 · 11111111

200 · 10 · 20 · 192
to
200 · 10 · 20 · 255

64 − 2

- Subnet mask ?

$S_1 \rightarrow$ Fix 24 + 1 25 bits.

So, 255 · 255 · 255 · 128

$S_2 \rightarrow$ Fix 26 .

8421 .

255 · 255 · 255 · 192

$S_3 \rightarrow$ 255 · 255 · 255 · 192

Q) What is the max. no. of IP addresses that can be assigned to hosts on a local subnet that uses the 255 · 255 · 255 · 224 subnet mask?

Ans 255 · 255 · 255 · 11100000

27 are in use.

3 on 5 off

1's .

~~8 subnets~~.

32 − 27 = 5

Hosts = $2^5 - 2$. 30 .

$$\begin{array}{r} 128 \\ +64 \\ \hline 192 \end{array} \quad \begin{array}{r} 192 \\ +32 \\ \hline 224 \\ +16 \\ \hline 240 \end{array}$$

128 64 32 16 8 4 2 1

__/__/___

Q) You need to subnet a network that has 5 subnets, each with at least 16 host. Which classful subnet mask would you use?

Ans - A) 255.255.255.192
B) 255.255.255.224
C) 255.255.255.240
D) 255.255.255.248

192 - 1 1 0 0 0 0 0 0

6 subnet.

$24+2 = 26 = 32-26 = 6$ - 2 subnets.

$2^6 - 2 = 62$ hosts

240 - 1 1 1 1 0 0 0 0

$24+4 = 28 = 32-28 = 4$

$2^4 - 2 = 14$ hosts

224 - 1 1 1 0 0 0 0 0

$24+3 = 27 \quad 32-27 = 5$

$2^5 - 2 = 30$

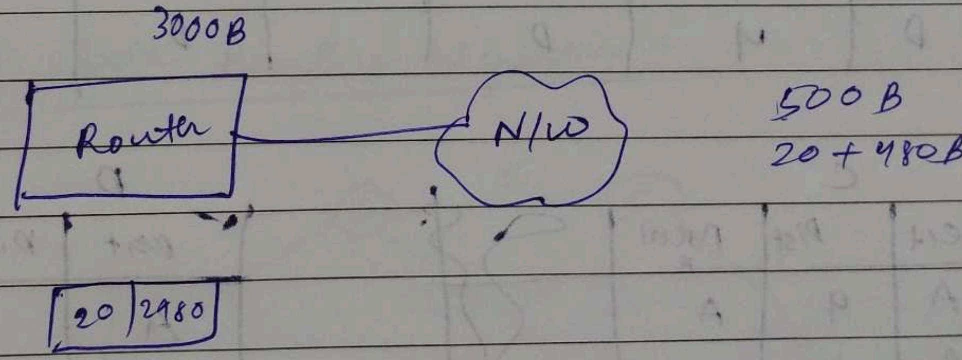
Q) Suppose a network with IP Address 192.16.0.0 is divided into 2 subnets, find no. hosts per subnet.

1. Subnet Address
2. First Host ID
3. second Host ID
4. Broadcast Addr

} As done previously

★ IPV4 Datagram ~~00~~ 0100 :-

Q) A datagram of 3000 B (20 B of IP header + 2980 B IP payload) reached at Router and must be forward to link with MTU of 500 B: How many fragments will be generated and also write MF, offset, Total length value for all.

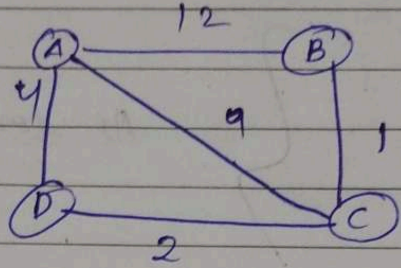


$$\frac{2980\,B}{480\,B} = 7.$$

__/__/____

* Routing Protocols :-

1) Distance Vector Routing



→ To determine best path to travel.

→ Routing table

Max steps = 4-1 [No. of routers - 1]

Step 1 :-

A

Dest	Distance	Next Router
A	0	A
B	12	B
C	9	C
D	4	D

B

Dest	Dist.	Next R
A	12	A
B	0	B
C	1	C
D	∞	–

C

Dest	Dist	Next R
A	9	A
B	1	B
C	0	C
D	2	D

D

Dest	Dist.	Next R
A	4	A
B	∞	–
C	2	C
D	0	D

_/_/_

Step 2 :- Find the shortest path through which it can reach the next dest.

A

Dist	Dist	Next
A	0	0
B	7	D, C, B
C	6	D, C
D	4	D

B

Des	Dist	next
A	7	C, D, A
B	0	0
C	1	C
D	3	C, D

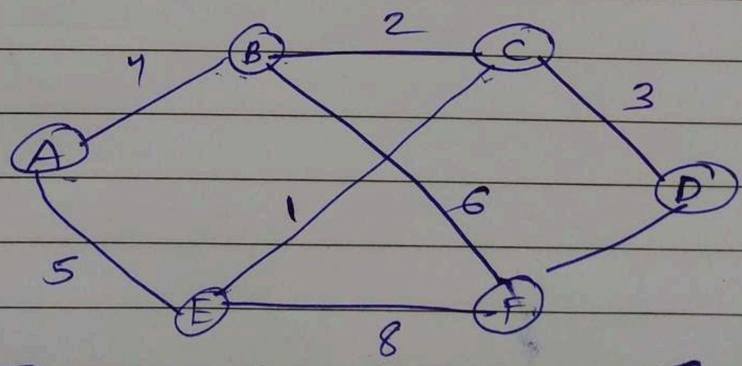
C

Dest	Dist	Next
A	6	D, A
B	1	B
C	0	0
D	2	D

D

Dest	Dist	Next
A	4	A
B	3	C, B
C	2	C
D	0	D

★ Link state Routing Algorithm :-



HELLO

Step 1 :- Write every neighbours distance

A	B	C	D	E	F
seq	seq	seq	seq	seq	seq
Age	Age	Age	Age	Age	Age
B 4	A 4	B 2	C 3	A 5	B 6
E 5	C 2	D 3	F 7	C 1	D 7
	F 6	E 1		F 8	E 8

Flooding

Dijkstra's .

	B	C	D	E	F
A	4	∞	∞	5	∞
AB	4 4	6	∞	5	10
ABE	4	6	∞	5	10