Network address :- 10.100.128.0/17

(1) Given subnet = 11

= (1011) 4 bit

Subnet
∴ ~~Host~~ $= 2^4 = 16$

∴ need to borrow 4 bits from Host bit address

Network bit = 17+4 host = 11

(2) Subnet mask

/17

17+4 = 21

11111111. 11111111. 11111000. 00000000

255 255 248 . 0

Subnet mask = 255.255.248.0

(3) 10.100.128.0 /21

11111111 . 11111111 . 11111000 . 00000000

11
Hostbit

octet = 3

subnet generaton
$= 2^3 = 8$

No. Host $= 2^{11}$
$= 2048$

usable $= 2048 - 2$
$= 2046$

Subnet 1 :- 10.100.128.0 / 21

∴ Host address range :-

10.100.128.1 — 10.100.135.254

First address :- 10.100.128.0

Broadcast address :- 10.100.135.255

Subnet 2 :- 10.100.136.0 /21

subnet 3 :- 10.100. .144. 0/21

Subnet 4 :- 10.100. 152.0/21

subnet 5 :- 10.100. 160.0 / 21

subnet 6 ⇒ 10.100.168.0/21

subnet 7 ⇒ 10.100.176.0/21

subnet 8 ⇒ 10.100.184.0/21

subnet 9 → 10.100.192.0/21

subnet 10 → 10.100.200.0/21

subnet 11 → 10.100.208.0/21

(3) ∴ CIDR notation 11th subnet network address

= 10.100.208.0/21

(5) ∴ Host address range

10.100.208.1 – 10.100.215.254

Before

10.100.128.0/17

∴ usable Host = $2^{32-17} - 2 = 32766$

After

10.100.128.0/21

∴ usable Host = $2^{32-21} - 2 = 2046$

∴ Host address lost for subnetting process = 32766 - 2046 = 30720

(5) 10.100.128.0 /21

No of host = 2

(10) 2bit

∴ Network bit = 32 - 2 = 30bit

New network address

= 10.100.128.0/30

11111111. 11111111. 11111111. 11111100

↳ $2^2 = 4$ host

∴ New subnetmask :-

255.255.255.252 /30

Two usable IP address are

1. 10.100.128.1
2. 10.100.128.2

10.100.128.0 → first address

10.100.128.3 → broadcast ,,

Port addressing :- is a mechanism used in computer networking to identify specific services/processes running on a device within a network.

why do we need ?

1. multiplexing
2. TCP/IP networking connection establishment
3. ~~Uniquely identify a process~~ help differentiate between various services/protocols running on device

---

1. Well-known port :- 0 – 1023
   - HTTP → 80
   - HTTPS → 443
   - FTP → 21
2. Registered port :- 1024 – 49151
3. Dynamic/private port :- 49151 – 65535

What is default gateway?

→ is a device that serves as the exit point for network traffic from a local network to other network. It acts as a router to connect local network to external network such as Internet

→ connect local network to other network

192.168.10.0/28

∴ default gateway :- 192.168.10.1

Features

1. Traffic Routing (forwarding traffic)
2. Internet Access (can route to other network)
3. Network Address Translation (NAT)
4. Firewall functionality
5. act DHCP services
6. supports QoS (Quality of service)

Host Forwanding Decision techinque :-

(local nouting)

→ is a method used by individual hosts to determine how to forward network traffic destined for different network.

① Packets are always created at source

② Routing Table :- each host device create their own nouting table

③ Destination IP :- a host can send packet to

④ Itself :- 127.0.0.1

② Local host :- (another host on same LAN)

③ Remote host :- not in same LAN

Next hop determination :-

④ Source device determine where the destination is Local on remote

For determination it use own IP address and subnetmask with destination IP address

⑤ Local traffic handled by host interface

Remote traffic " " by default gateway of LAN

Point to point

nefens to a communication link that connects two node dinectly with a dedicated link. without any intenmediang device

peen to peen

nefenes to netwonk anchitectune where all peens/node have equal cabcbilities and nesponsibility. each node can act as both client and senven, shanes nesounce dinectly.

what are the key elements of network protocol?

① Syntax :- define the structure and format of data being transmitted
Packet header, data field

② Semantics :- define the meaning and Interpetition of data exchanged between device

③ Timing :- condination & synchonization between devices.

what are functions provided by network protocol?

① Addressing & Identification
② Data encapsulation
③ packet forwanding - Routing
④ error detection - connection
⑤ flow control
⑥ Network management
⑦ Security & Encryption
⑧ Reliability (guaranteed delivery)
⑨ Sequencing

what are the network protocol requirements?

1. an identified senden - receiven
2. comman Language - gnammen
3. speed - timing of deliveny
4. Acknowledgementand confinmation of requinements.

what are the foun fondamental chanacteristic of data communication

1. Deliveny :- must deliven to connect destination
2. Accunacy :- must deliven accunate data
3. Timeliness :- timely mannen deliven
4. Jitten :- nefens to the vaniation in packet annival time.

(6) what are the foun chanactenistic of Reliable Netwonk?

(1) fault tolenance :- nefens to the ability of Netwonk to continue openating & pnoviding senvice even in the presence of failune

(2) scalibility

(3) Qos (Quality of senvice) :- pnionitize and manage netwonk, traffic to ensune specific level of penfonmance, nelsibility senvice, deliveny

(4) Netwonk secunity

what are the benifits of layened model?

1. Modulan Design :- divdie complex task into separate layen
2. Interopenability
3. Easien ~~Design~~ & simplified design implementation
4. Flexibility and Extensibility
5. Easy troubleshooting and debugging
6. standaridization value

—— o ——

Physical Layer

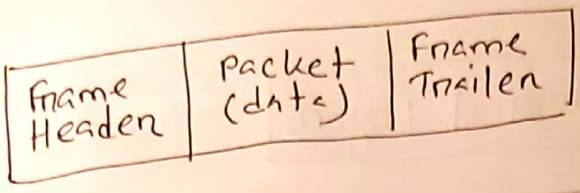
1. physical chanactenistic of intenface and tnansmission medium
2. Repnesentation of bits
3. Data / Bit nate
4. Synchnonization of bit
5. physical Topology
6. Line Configunation
7. Tnansmission mode
8. Signal encoding and modification

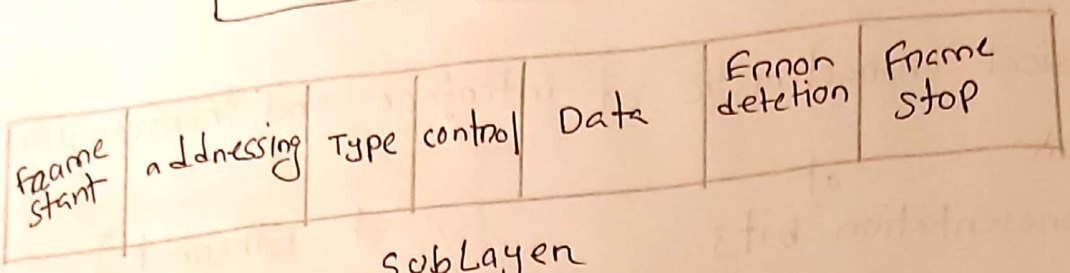
Ethennet
WLAN
SONET
SDH

bits

Data Link Layen

1. Framming & Defining bits
2. provide physical addness
3. Ennon detection
4. flow control
5. access control
6. hop to hop deliveny





SubLayer

LLC (Logical link control) sublayer

1. Framming
2. Error control
3. flow control
4. Sequencing
5. Link management

MAC (Media Access Control) Sublayer

1. Addressing
2. Medium access control
3. Frame transmission

Network Layer

IPv4
IPv6
Icmv4
Icmv6

1. Host to host packet deliveny
2. logical Addnessing
3. Routing (Route detenmination, selection)
4. pnovidies best effont senvice

Transpont Layen

1. TCP, UDP
2. Reliable pnocess to pnocess deliveny
3. pont addnessing
4. Ennon detection
5. flow contnol
6. connection contnol
7. Data segmentation and neassemble
8. Descnibe the fonmat of nequest/nesponse in between client-Senven
9. connection estoblishment and tenmination
10. Data multeplexing

Session Layer

1. Dialog control
2. synchronization
3. Login - logout
4. session establishment & manging

Presentation Layer

1. Translation, Formating
2. Compression
3. Encryption

PNG
JPG
GIF
MKV

Application Layer

1. providing service/access to user
2. file transfer, access, management
3. mail (email) and directory Services.

FTP, HTTP, HTTPS, DNS

CSE

192.168.40.0/21

11111111.11111111.11111000.00000000

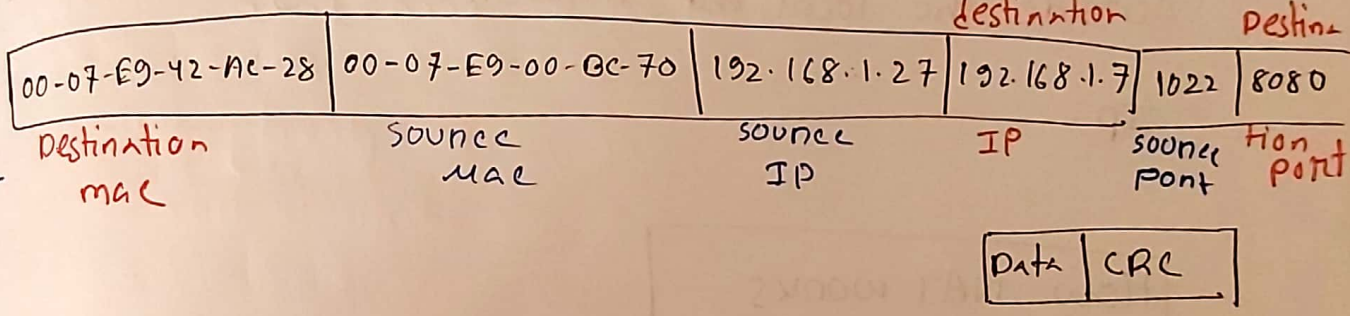
subnet mask :- 255.255.248.0

subnets :- 32

Host :- $2^{11} = 2048$

subnet -1 :- 192.168.40.0/21

192.168.40.1 — 192.168.47.254



Data Link Layer

Ethernet frame

Source socket :- IP + port

192.168.1.27:1022

what is NAT ?

NAT is Network address translation which works by translating IP (private) address used within a local network into a public IP address assigned by ISP (Internet Service provider).

→ allows device with private IP address to communicate with device outside the local Network using the public Ip.

How NAT works

(1) In local Network, device are assigned private IP address. (which are not routable in Internet)

(2) NAT act as gateway between local network and Internet.

(3) It has both private IP address with local network and a public IP assigned by ISP

The Nat router maintains a mapping table that keeps track of private IP address and their co-respond public IP address translation.

(4) when a device from local network wants to communicate with a device on Internet, NAT router modifies the source IP of outgoing packets to its own public IP

It allows multiple device within ~~a single~~ local network to connect internet using a single internet connection (public IP address)

Advantage

1. allows a single IP address for multiple device
2. Enhanced Security
3. simplified Network configuration

disadvantage

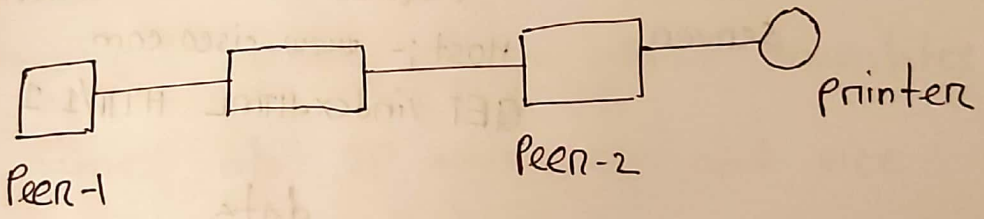
1. limited Peen-to-Peen connectivity
2. Increases complexity for Network adminstration
3. fully dependent on public IP availability.

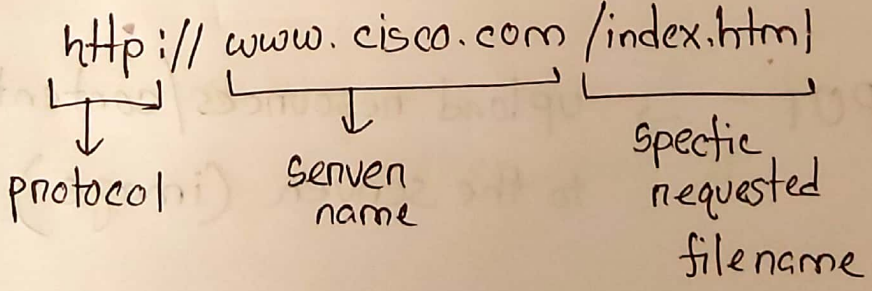
Application Layers protocols

1. HTTP
2. File Transfer Protocol (FTP)
3. DNS
4. IMAP (Internet Message Access)
5. DHCP

what is P2P?

→ Peer to peer network, two or more device connected via network and can share resources (printer, scanner, file) without having a dedicated server



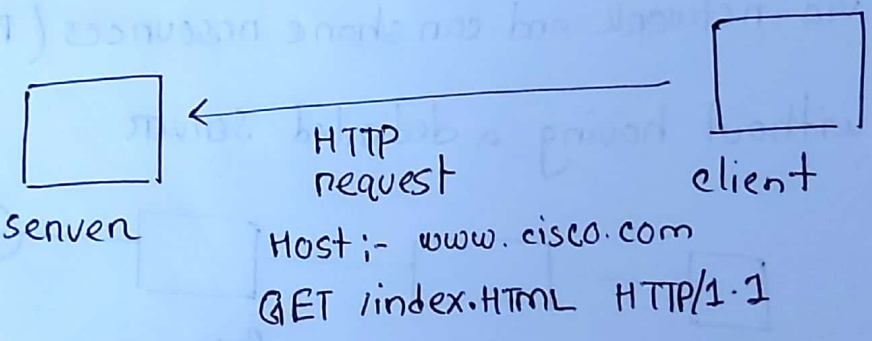


what is HTTP?

→ It is a protocol that specifies the message request/response type used for that communication.

3 common message type :-

① GET → a client (web browser) sends GET message to server to request for data on HTML pages.



② POST → uploads data file to the server (form data)

③ PUT → upload resources/content to the server (image)

Email protocol :-

(port:25) SMTP (simple Mail transfer protocol) → used to send email

(port:110) POP (post office protocol) & IMAP → receive mail

— o —

DNS (Domain Name service)

http://www.cisco.com → Domain Name

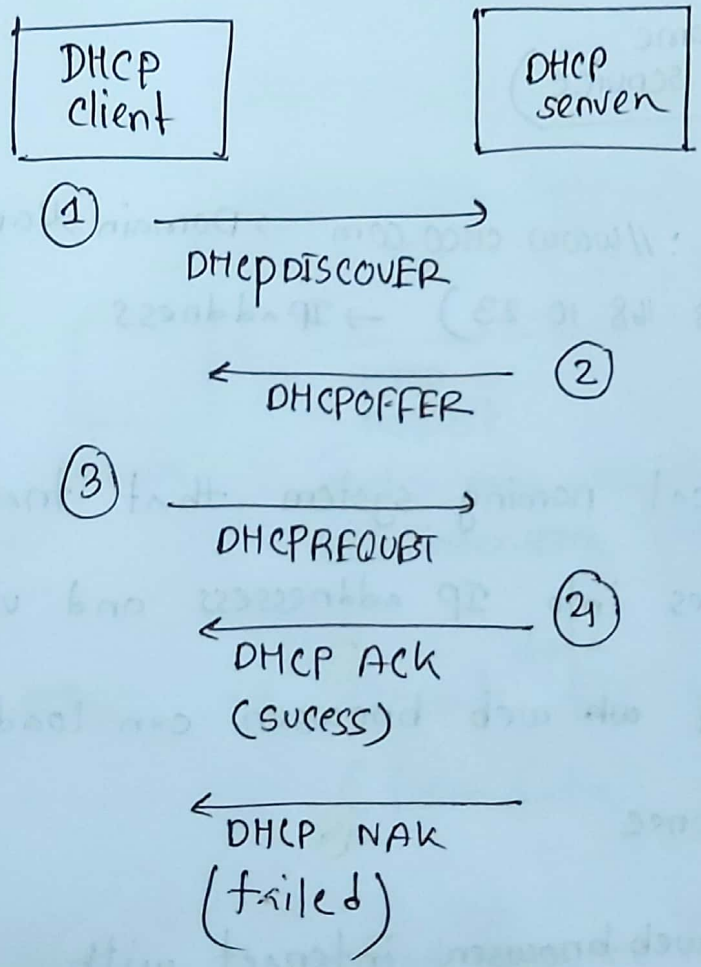
(198.168.10.23) → IP address

→ is hierarchical naming system that translates domain names into IP addressess and vice versa so that ~~wh~~ web browsen can load Internet resource

web browsen interact with eachothen using IP

DHCP (Dynamic Host configuration protocol)

→ is a dynamic addressing service which automates the assignment of IP addressing, subnet mask, gateway and other networking parameters



Types of Network Threats

1. Information Theft
2. Dataloss and manipulation
3. Identity Theft
4. DOS (~~Disproduct~~ Disruption of service)

Vulnerability → the degree of weakness in a network/device

1. Technological Vulnerability
2. Configuration "
3. Security Policy

Question

① what' are the components of data communication system? (5)

② what is protocol?

③ what are the network components? (6)

④ what are the criteria of efficient network(3)?

⑤ what is peer to peer network?

⑥ what is point to point network?

⑦ what is network topology?

Ans the following question for Mesh, star, RING, BUS

(i) connection type?
(point to point or multipoint)

(2) Defination

(3) cable no. / physical links

(4) number of port for each port

(5) what if a connection fail

(6) unplugging station

⑧ a Hybrid topology with Ring backbone and 2 bus network

(9) Difference LAN vs LWAN ?

(10) Difference Intranets vs Extranets?

(11) 7 Layers of OSI Model ?

(12) 4 Layers of TCP / IP Model?

(13) what is Multicasting?

(14) Difference between physical, Logical and port address?

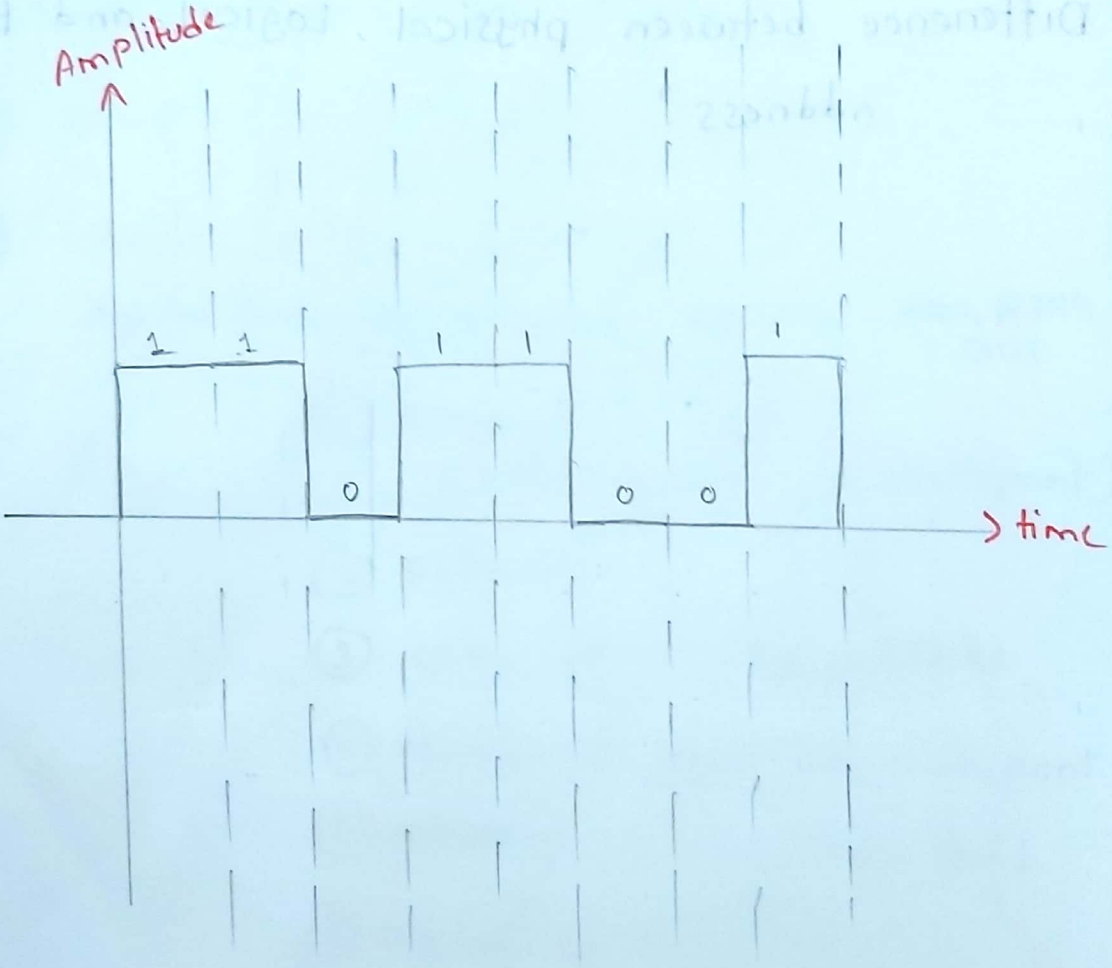
Line coding

Unipolar line coding

0 means zero voltage

1 means positive voltage — NRZ

Datastream:- 1101001



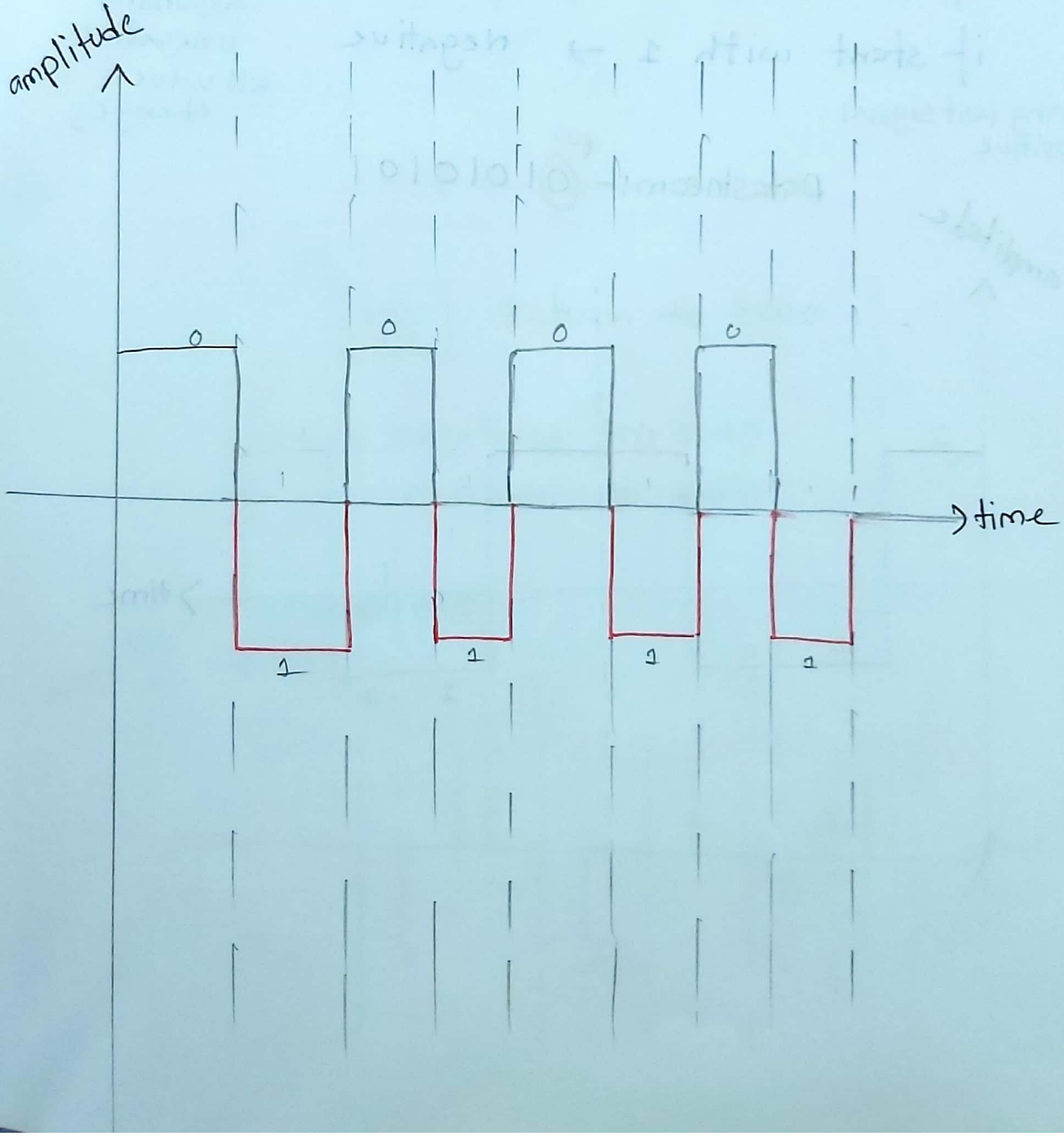
Polar Line coding

1. **NRZ-L** — Non return to zero level

'0' means positive

'1' means Negative not zero volt

Data schema :- 01010101



② NRZ-I

Non-return to zero Invented

if 0 ⟶ NO transition

1 ⟶ transition
pos ⟶ neg
neg ⟶ postive

Based on last signal

Careful

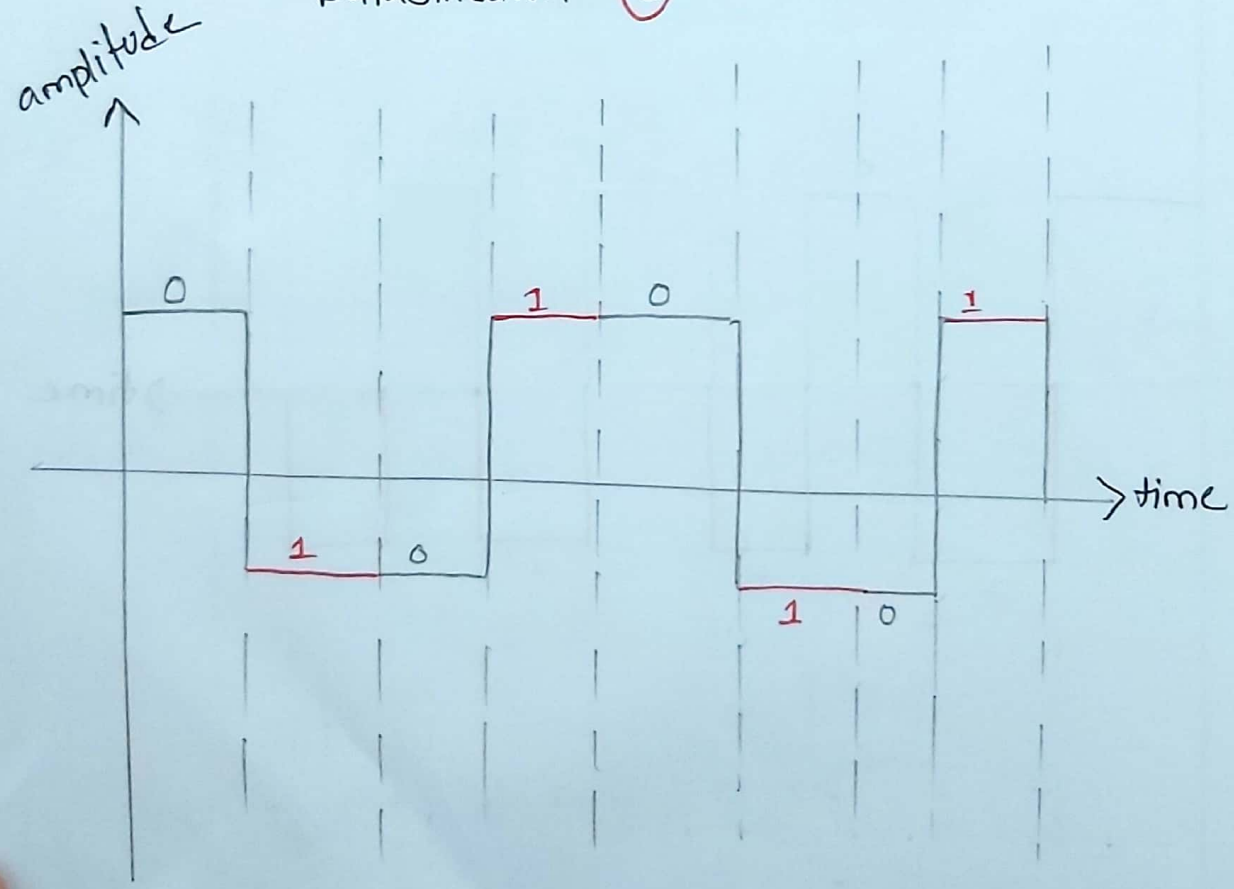
if stant with 0 → positive

if stant with 1 → Negative

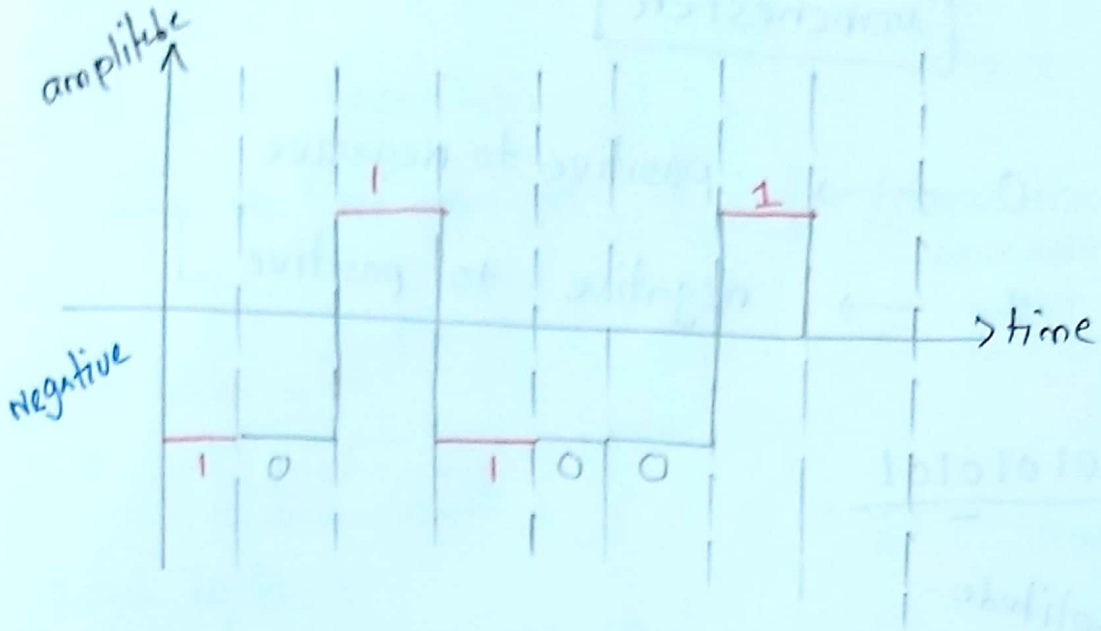
assuming last signal positive

* if last signal assuming is negative all value changes

Datastream:- (pos) 0 1 0 1 0 1



Datastream :- neg ① 011001



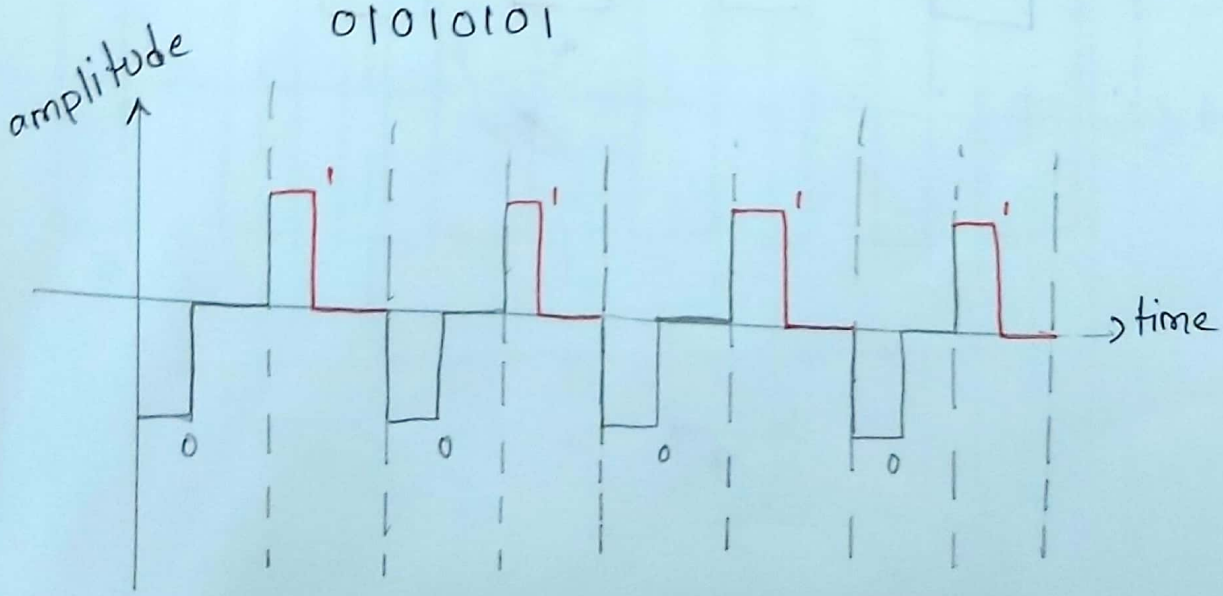
—— o ——

③ RZ Return to zero

0 ⟶ negative to zero

1 ⟶ positive to zero

01010101

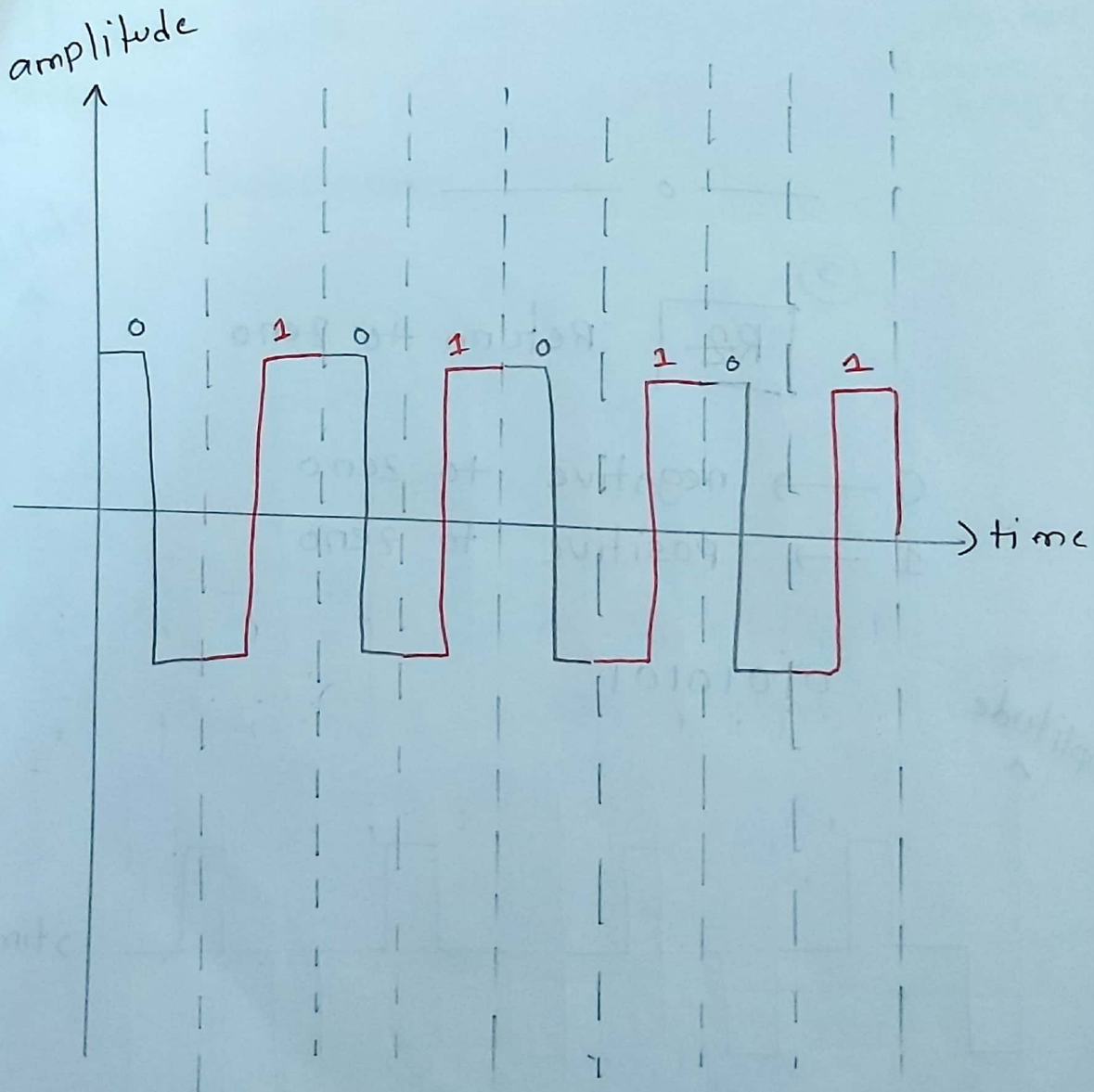


(4) **Manchester**

0 ⟶ positive to negative

1 ⟶ negative to positive

01010101



(5) Differential Manchester

0 ⟶ transition ⊓ . ⊓ (choose)

1 ⟶ No transition ⊐ ⌐ (choose form here according to last)

if stant with 0

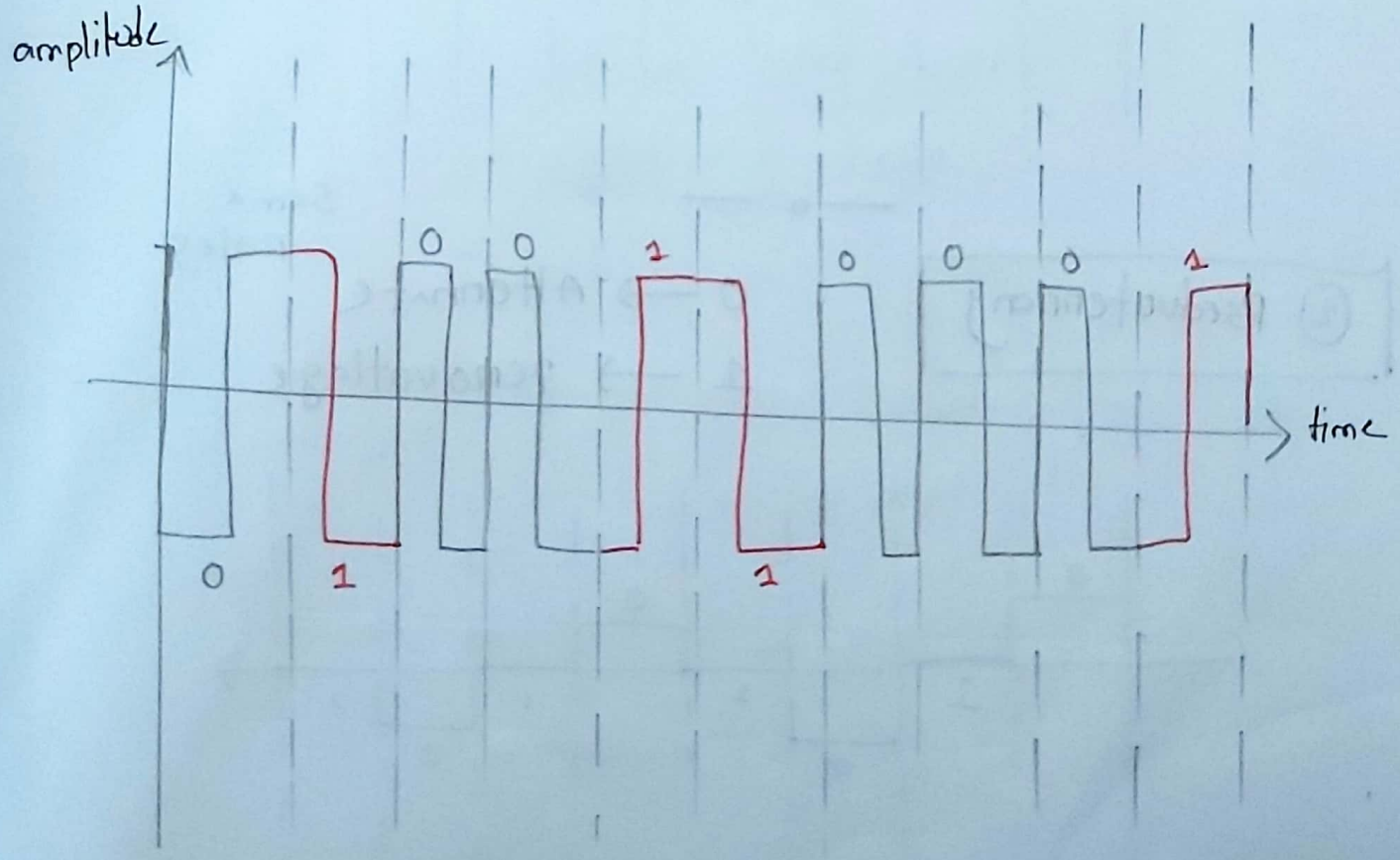
(low to high) ⊓

stant with 1

(post to neg) ⊐

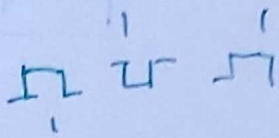
high to low

0100110001



Bipolar

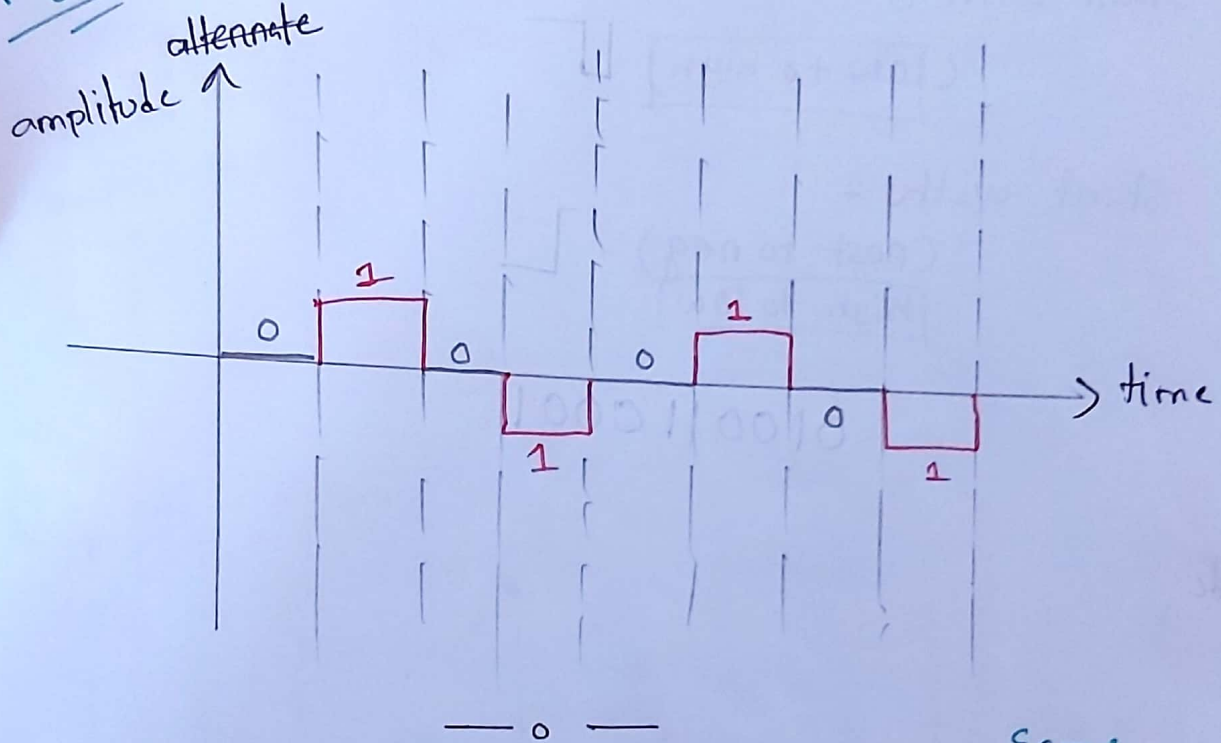
① AMI (Alternate Mark Inversion)



0 ⟶ zero voltage

1 ⟶ Alternate bit last 1 bit

assume Last bit negative : if starts with 1 (postive)



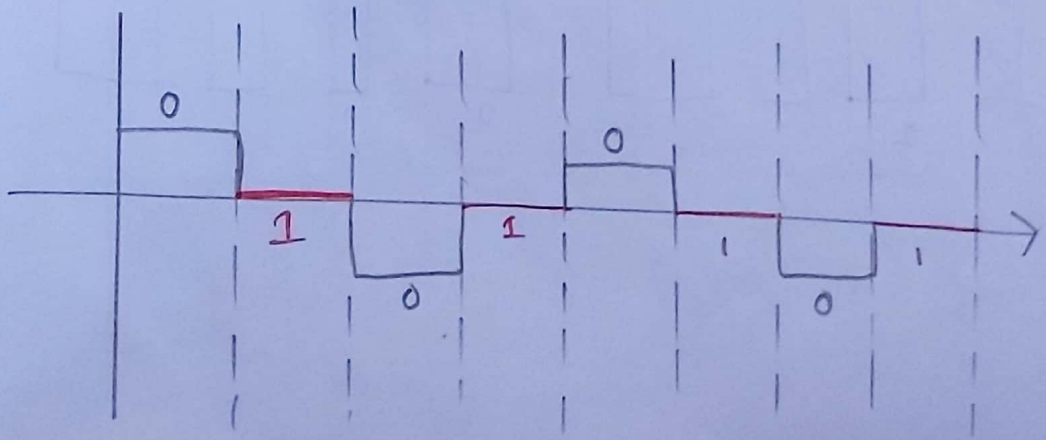
— o —

② Pseudoternary

Same Rules

0 ⟶ Alternate

1 ⟶ zero voltage



MULTiLine Transition

MLT-3

Focus on voltage (not bit)

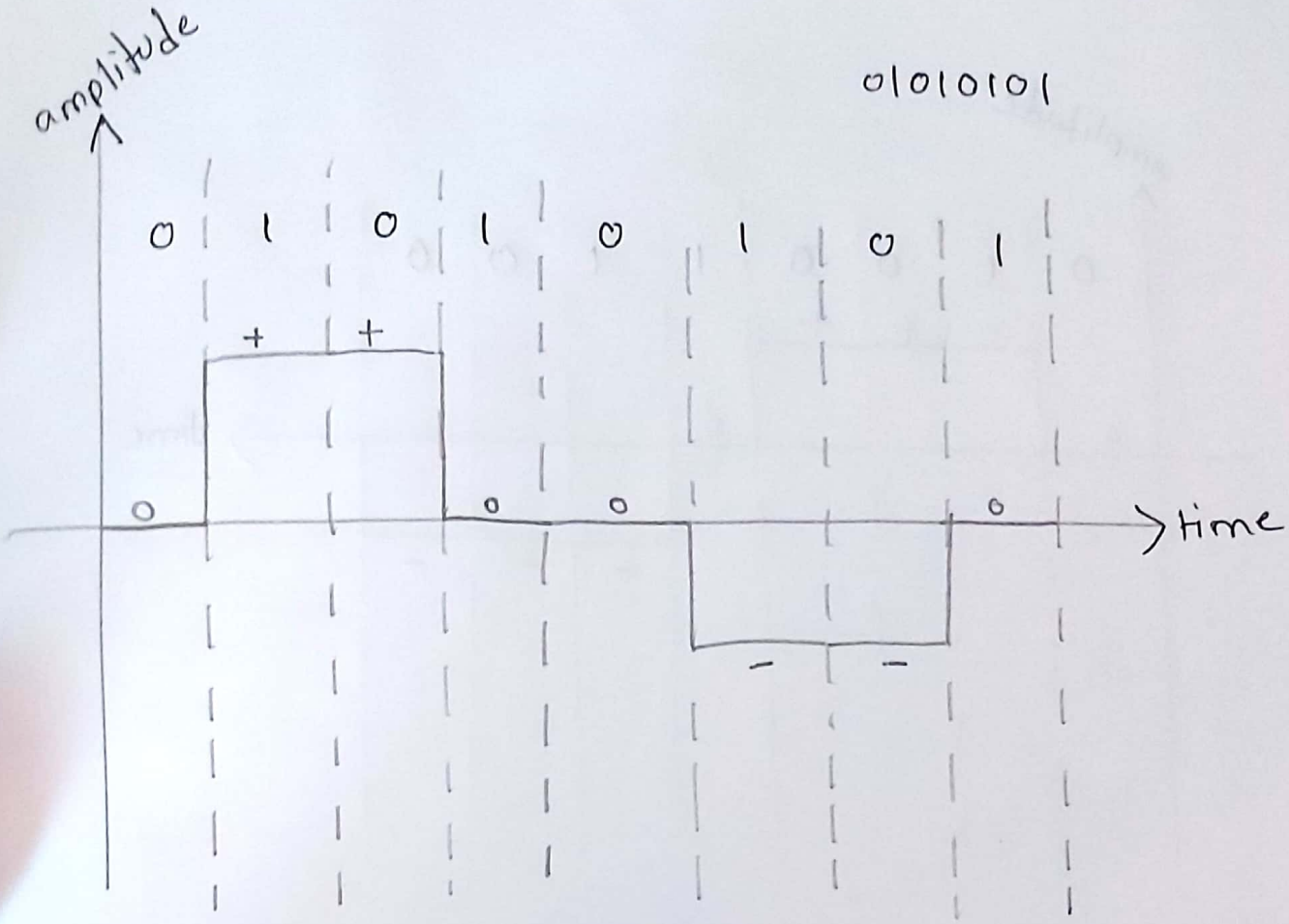
Rules:

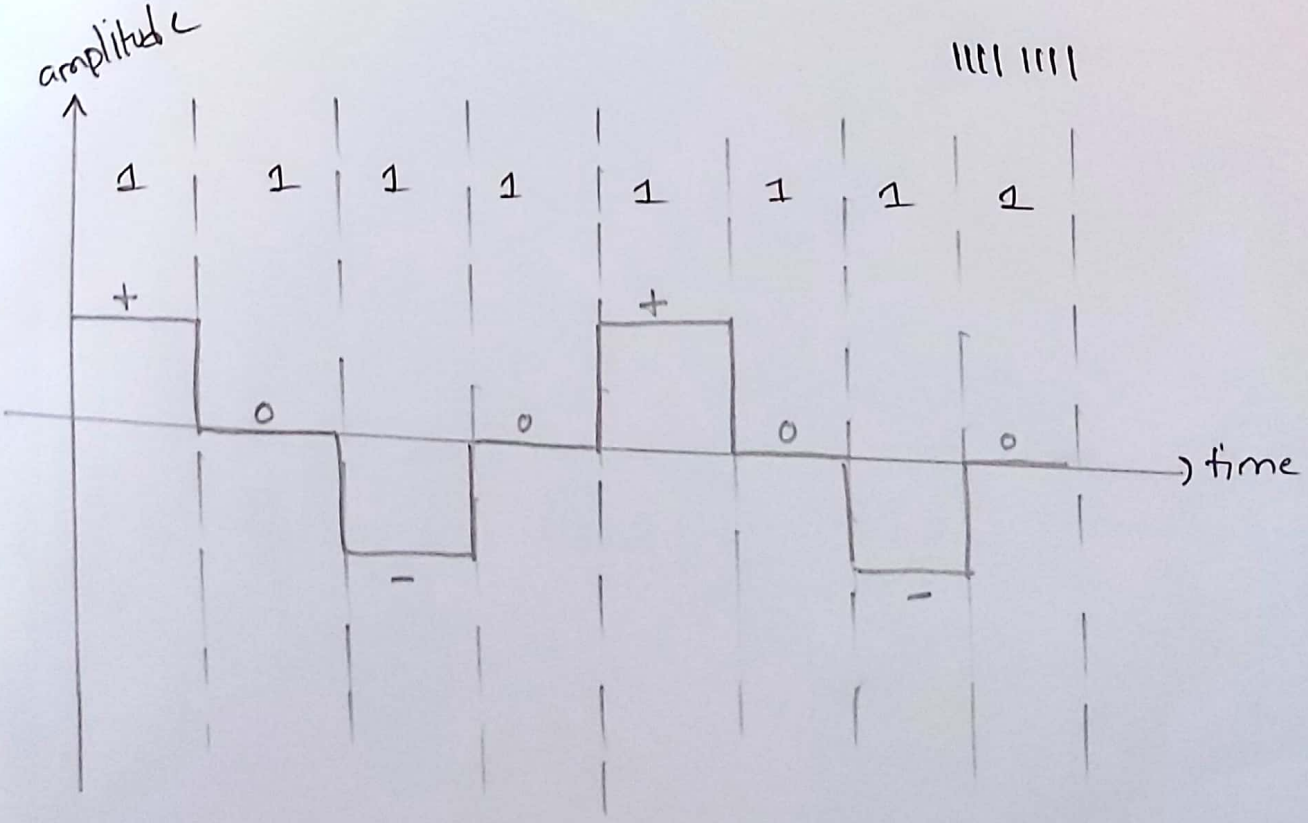
Assuming
last level = zero voltage
last non zero level = negative

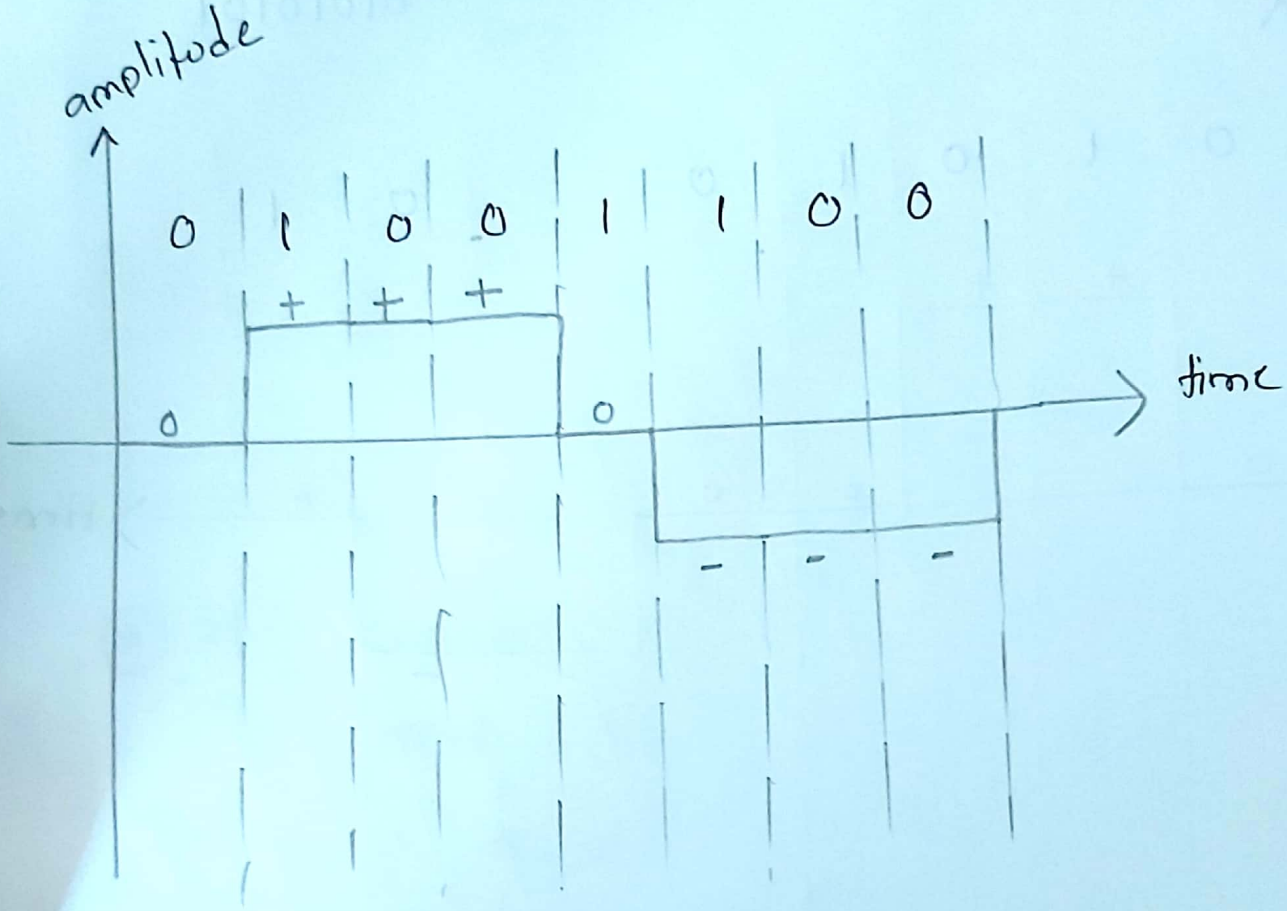
① if current level = zero, pos, neg
next bit = 0
∴ No transaction (same like last)

② if current level = zero volt
next bit = 1
∴
opposite of last non zero level

③ if current level = positive or negative
next bit = 1
∴
next zero voltage


amplitude
01010101
0 1 0 1 0 1 0 1
+ +
0 0 0 0
time
- -


amplitude
1111 1111
1 1 1 1 1 1 1 1
+ +
0 0 0 0
time
- -


amplitude
0 1 0 0 1 1 0 0
+ + +
0
0
time
- - -

connectionless, media Independent

Q IP/Network Layer provides best effort service.

properties of best effort service

1. IP will not guarantee the delivery of packet.
2. It is doesn't know other device has received the packet or not
3. IP doesn't expect acknowledgement
4. IP has reduced overhead cause It doesn't need to resend packet if not recived.

NT :- Transport Layer UDP also support best effort delivery service

TCP - 3 way Handshake

It is a inital handshake process by TCP to establish a neliable connection between two device client senven.

Control flags :- SYN → synenonize
ACK → Acknowledgement

3 steps :-

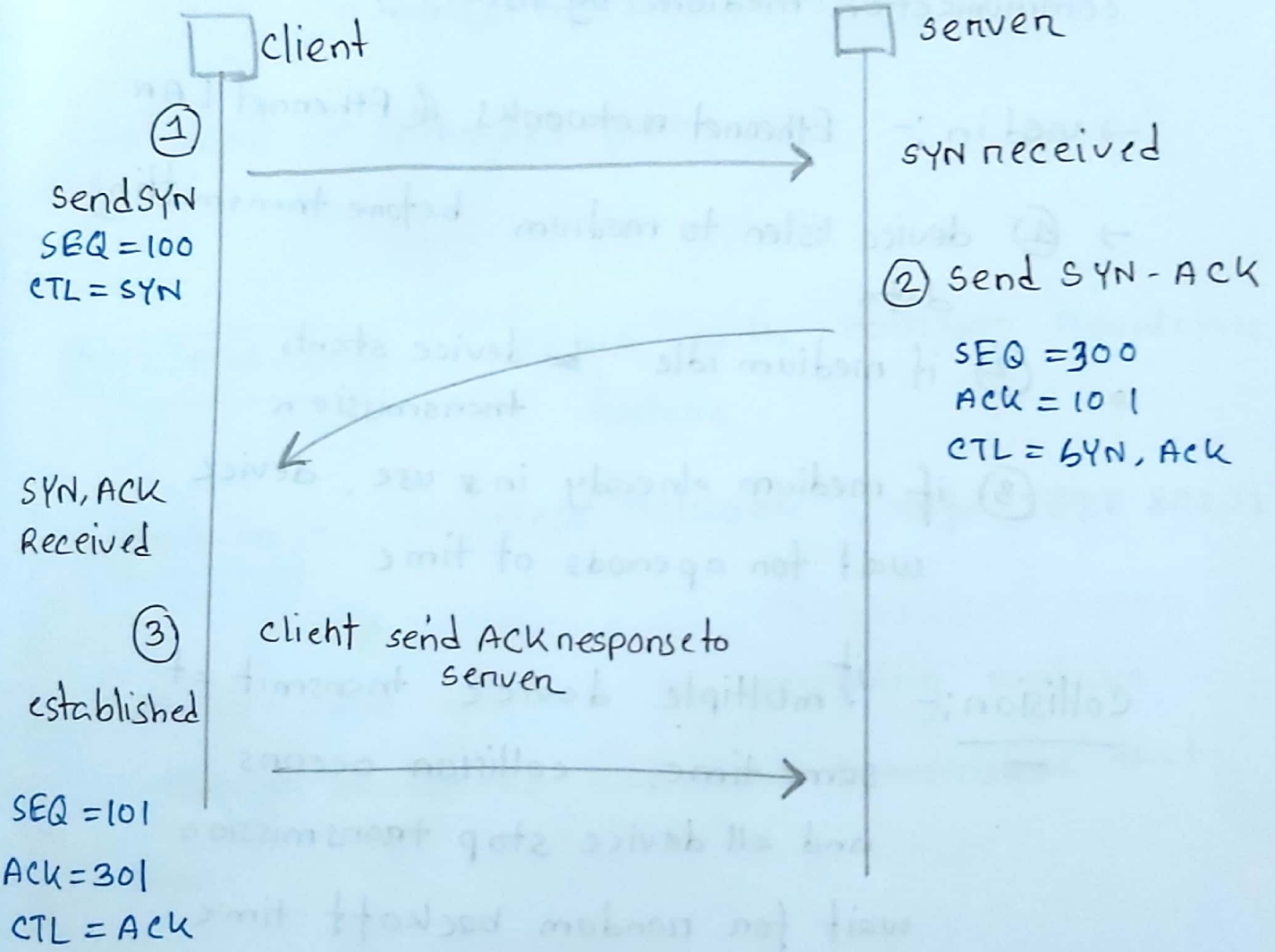
(1) client initates the connection with seven by sending TCP packets with SYN flag.

(2) Senven necives SYN packet. and nesponds to cliend by sending a TCP packet with control flag SYN & ACK

(3) client necives SYN - ACK packets and acknowlegde the senven by sending Packet with ACK flag.

(4) Server recives the ACK packet

∴ TCP connection is estcblished.



(*) **CSMA** (Cannien sense Multiple Access)

→ is a method (network access control) which allows multiple device to share the same communication medium by listening to medum.

→ used in :- Ethennet Networks & Ethennet LAN

→ (1) device listen to medium before transmitting data

(2) if medium idle, device starts transmission

(3) if medium already in use, device wait for aperiods of time

Collision :- if multiple device transmit at same time, collision occurs and all device stop transmission. wait for random backoff time for retying / retransmission

(1) **CSMA / CD** — CSMA with collision detection feature

→ detect collision as soon as they occur and minimize the time taken by collisions

→ used :- Ethernet LAN

(2) **CSMA / CA** — CSMA with collision Avoidance feature

used in :- wireless Network, wifi IEEE 802.11

minimize the collisions by reserving medium through handshake and avoid transmission that time.

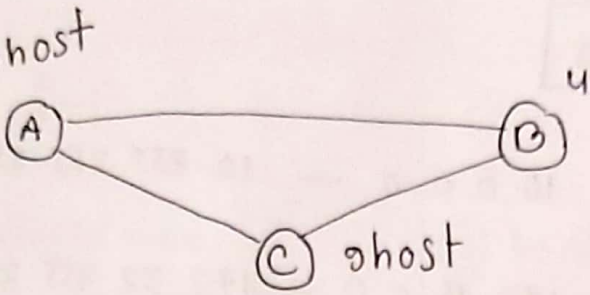
Layer	PDUs Protocol Data unit
Application Layer	→ Data
Session Layer	→ Data
presentation	→ Data
Transport	→ segment
Network	→ Packet
Data Link	→ Frame
Physical	→ bit

—o—

what is subnetting

is a method of dividing a single physical network into logical subnetworks on subnets.

1. reduce overall traffice, improve network speed and penfonmanc
2. subnet mask ensures the traffic remains in designated ~~traffic~~ subnet
3. boost network security
4. limit the Ip address usage to within fewdevice



120.124.80.0/24

High → Low

For (A)

host = 110 = (1101110) 7 bit

128

11111111. 11111111. 11111111. 1 0000000
7 Host bit

∴ subnest mask = 255.255.255.128

network = 120.124.80.0/25

For (B) Host = 40 = 101000 (6 bit)

11111111. 11111111. 11111111. 11 000000
6

∴ subnet mask : 255.255.255.192

network :- 120.124.80.128 / 26

For (C) Host = 9 = 1001 (4 bit)

64

11111111. 11111111. 11111111. 1111 0000
4

∴ subnet mask = 255.255.255.240

∴ network = 120.124.80.192 / 28

Private Ipaddness

10.0.0.0/8 → 10.0.0.0 — 10.255.255.255

172.16.0.0/12 → 172.16.0.0 — 172.32.255.255

192.168.0.0/16 → 192.168.0.0 — 192.168.255.255

Loopback addness

127.0.0.1

127.0.0.0 — 127.255.255.255

IPV6 :- ::1

Link Local addness

169.254.0.0/16

classful	classless
① IP address are allocated according to classes (A-E class)	① used to handle rapid exhaustation of IP address.
② Network and Host depends on class	② No restriction
③ do not support VLSM	③ support VLSM variable length subnetting mask
④ requires more bandwidth	④ require less bandwidth
⑤ don't support CIDR	⑤ support CIDR classless Inter Domain Routing
⑥ easy troubleshoot	⑥ Hard to troubleshoot

TCP (Transmission contro Protocol)

Features:-

1. TCP is connection-oriented and stateful protocol
2. Provides Relicbility (guncntee deliveny - acknowledgement, netnansmission if Data tails).
3. provide flow control
4. Acknowledgment of Data Recived
5. Divide data stneam into segments and tnack each segment tnansmitted to specific host fnom spectic Application
6. Sequence the data (ondening)
7. Fnnon detection
8. Send data at efficient nate acceptable by usen
9. Usecase :- system all data must cnnive with a pnopen sequence maintained.

Transmission Control Protocol	User Datagram Protocol
(1) connection - oriented	(1) connection-less
(2) provide Reliability of deliveny	(2) Doprovides neliability (support best effont)
(3) Acknowledgement of deliveny	(3) No acknowledgement
(4) support ~~odt~~ ordening	(4) X dont support
(5) support ennon control /detetion	(5) X " "
(6) steam-oriented message	(6) message-oriented
(7) support congestion control mechnism	(7) X
(8) Usecase :- used in webbnowsing, FTP, SSH email,	usecase (9) low-latency & Realtime communication VoIP, videstneaming, online gaming
(9) higen latency	(9) lowen latency higher thnoughtput

Internet Message Access

IMAP protocol

→ is an email retrival protocol that allows client to acesss and manage emails stored on mail server

function :-

1. Email Retrieval
2. Synchonization
3. Message status tracking

—— o ——

ARP address resolution protocol

It is a protocol used in computer network to map an IP address to a physical or MAC address.

Two functions

1. Resolve IP address to MAC address
2. Maintaining an ARP Table of mapping IP to Mac Address

same network → ARP table for destination IP address
different " → ARP Table for default gateway

3. NO ARP table found, device send an ARP request

~~Pur~~ purpose:- dynamically mapping the IP to MAC facilitating communication between device

disadvantage:-

1. Lack of - Authentication
2. " - vulnerability of ARP spoofing
3. " of scalibility
4. Limited Network scope

switching

store-forward switching	cut-through switching
(1) switch receive entire data frame before forwarding	(1) switch starts forwarding frame as soon as it is received in destination MAC.
(2) Higher Latency	(2) Minimal Latency
(3) has Error checking feature	(3) No error checking
(4) No frame size limitation	(4) has frame size limitation

switching

store-forward switching	cut-through switching
① switch receive entire data frame before forwarding	① switch starts forwarding frame as soon as it is received in destination MAC.
② Higher Latency	② Minimal Latency
③ has Error checking feature	③ No error checking
④ No frame size limitation	④ has frame size limitation