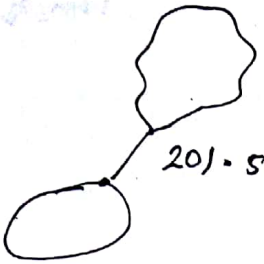
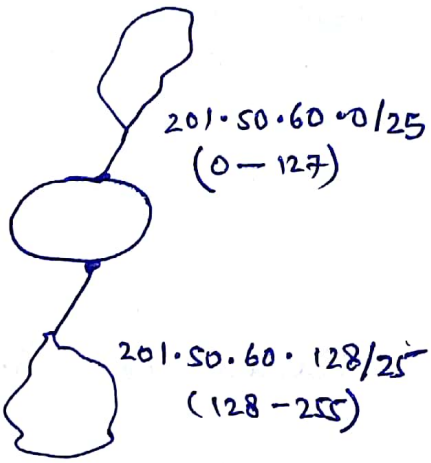
Equal length subnetting :-



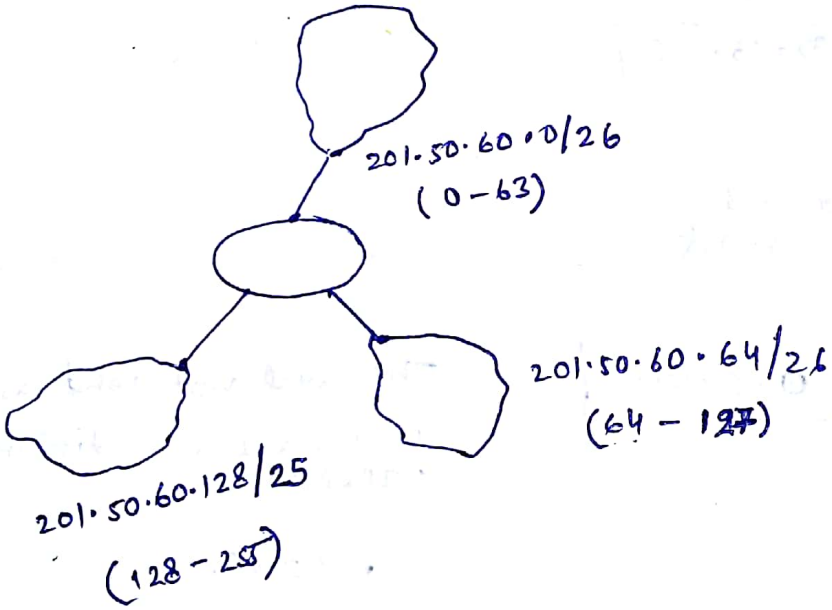
$\Rightarrow$

$2^{32-24} = 2^8 = 256$ addresses

$2^{32-25} = 2^7 = 128$ addresses



Variable length subnetting :-



* This is known as variable length subnet masking (VLSM).

Special cases :-

(i) IP_1 = 202.55.66.89, Calculate host on this network ?

IP belong to class C,

Mask = 255.255.255.0

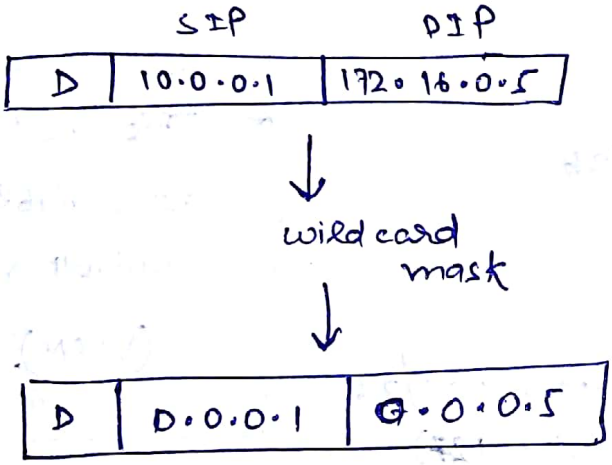
Wild card Mask = Complement of Mask

= 0.0.0.255

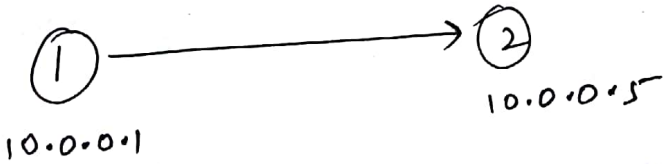
host on network = IP add ⊕ bitwise AND Wild card mask

= 0.0.0.89

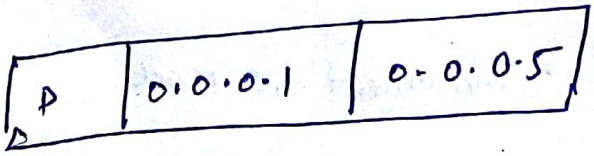
Usecase of "host on network":-



This will not send as both are on different (SIP & DIP) network.



Now here data packet is sending within same network so, we can use "host on network" method i.e



* This means we doesn't need to mention Net ID in a SIP and DIP when message is unicasting within the network.

(2) Which of the following IP can be used as source IP only?

(a) 10.0.0.5

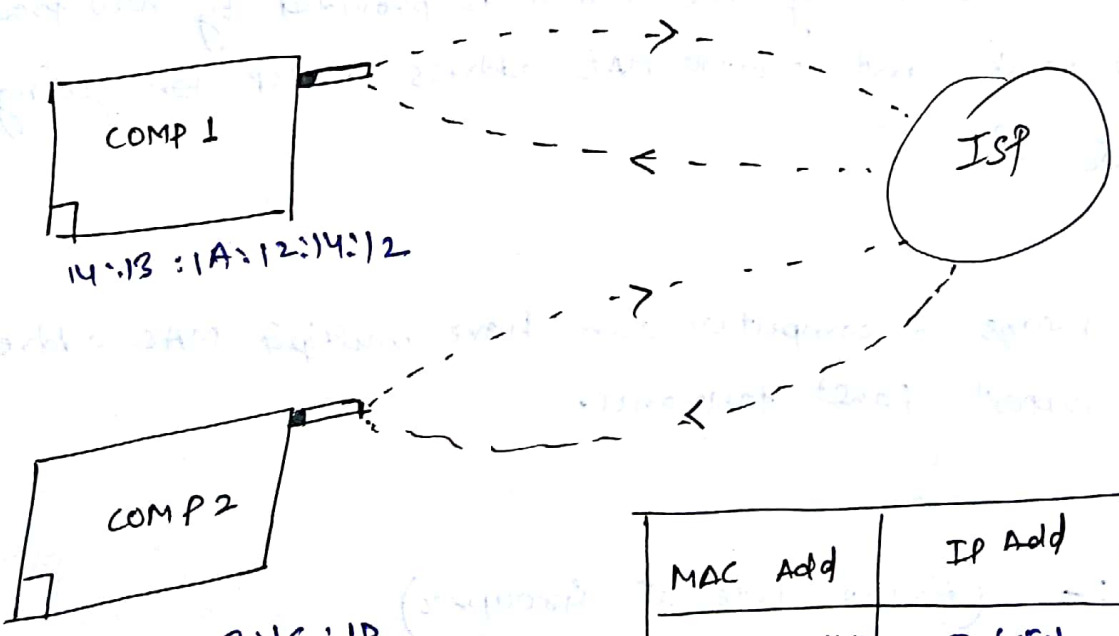
(b) 172.16.0.6

(c) 255.255.255.255

✓ (d) 0.0.0.0

* 0.0.0.0 is DHCP client request address which can only be used as SIP.

Dynamic assignment of IP by ISP:-

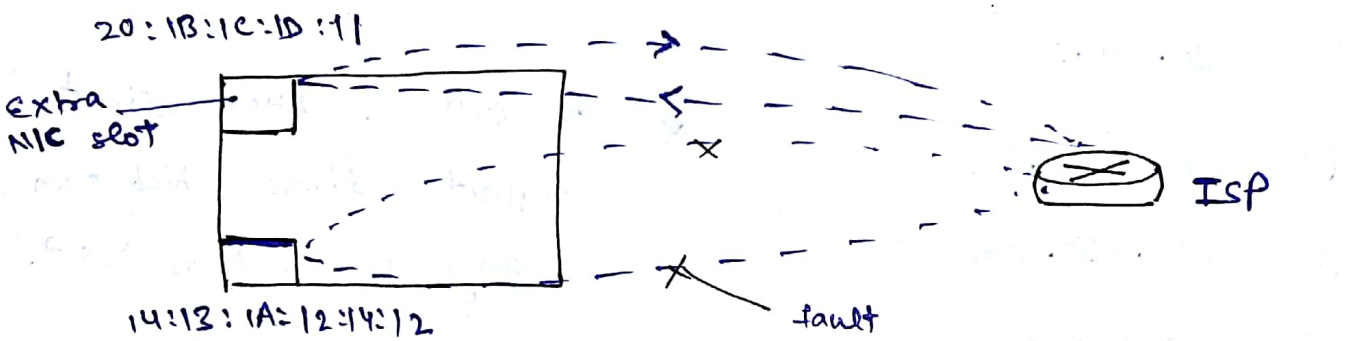


MAC Add	IP Add	Enabled
14:12:1A:12:14:12	7.6.5.1	✗
18:14:1A:1B:1C:1D	7.6.5.1	✓
14:13:1A:12:14:12	11.15.2.3	✓

* A computer can have multiple IP address at different instances of time.

* This concept is known as same MAC multiple IP address at different instances of time.

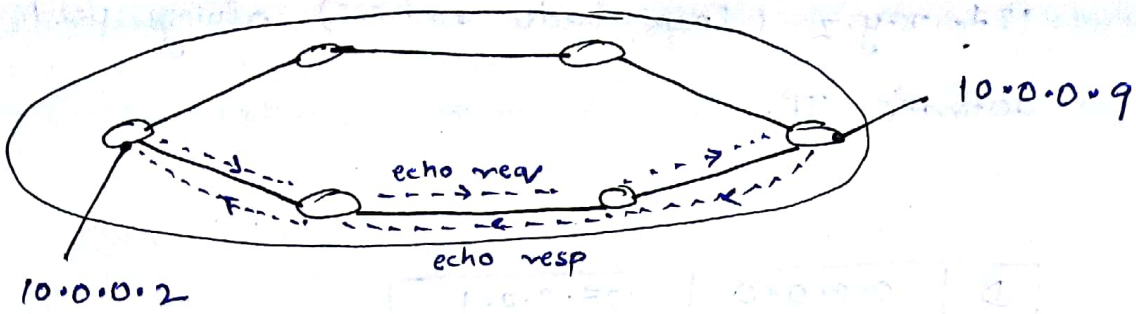
Fault tolerence :-



- when due to some malware script main NIC is dicabled then the secondary NIC which is provided by new processors will work and provide MAC address to ISP for getting public IP.

- This means a computer can have multiple MAC address to support Fault tolirance.

PING :- (Packet Internet Grouper)



C:\> Ping -t 10.0.0.9

> TTL = 2 ms , RTT = 4 ms (positive acknowledgment)

C:\> Ping -t 10.0.0.9

Destination unreachable or Request timeout (negative acknowledgment)

Ping command is used to troubleshoot the systems in the network. It is used to test the reachability of the system in the network.

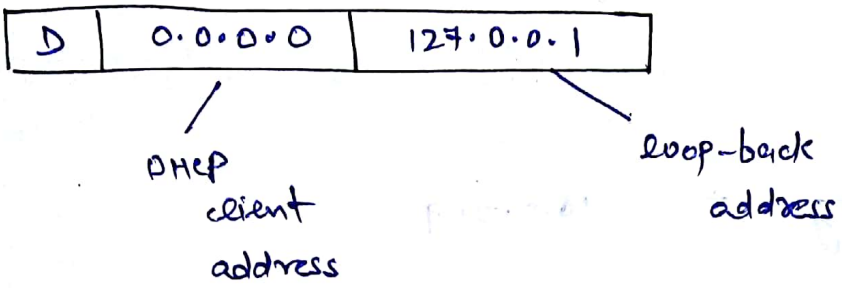
self-testing of network

C:\> Ping -t 127.0.0.1 — loop back address

TTL = 2ms , RTT = 4ms

i.e your computer is connected properly

* 127. x.y.z (loop-back address) always used as destination IP.

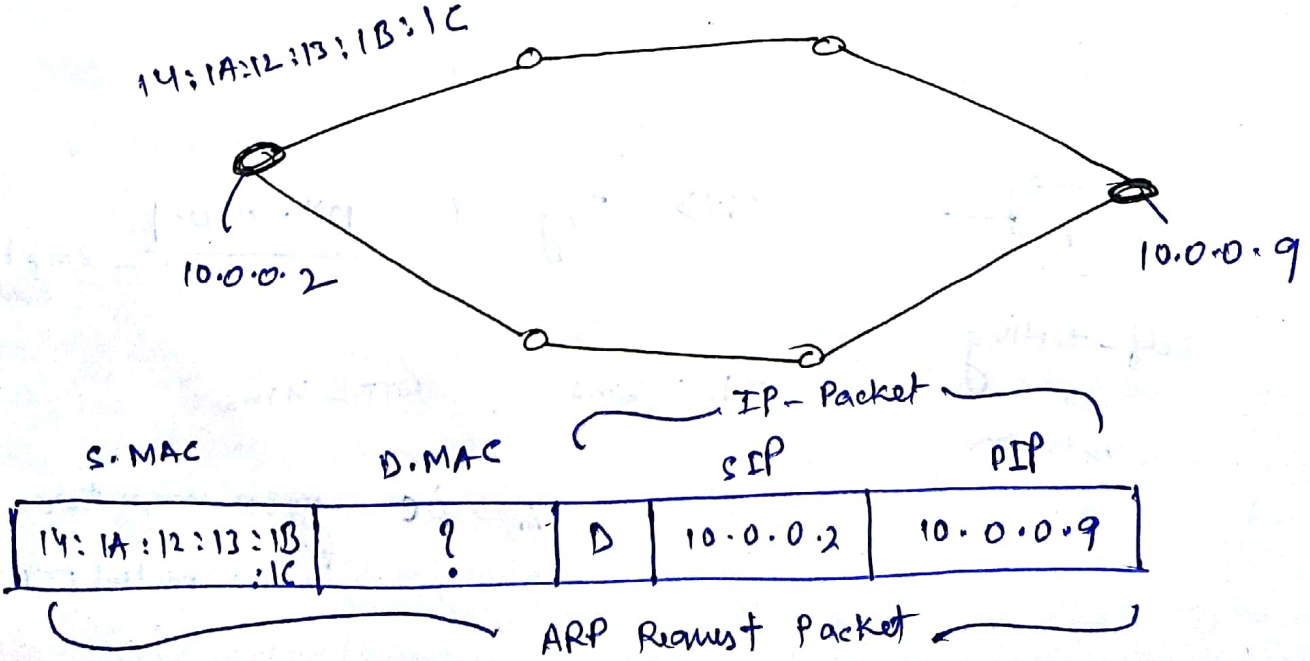


This packet showed that system performing loop-back testing without getting actual IP.

* Loop-back address will ~~not~~ never enter into the network.

* This loop-back address can be used as inter-process communication.

→ A. Address Resolution Protocol is used to get the physical address of the host on network.



- ARP request packet is a broadcast packet ie it contains soure MAC address, source IP, Destination IP, but it doesn't contains destination MAC.

- ARP reply packet is unicasted and reply with destination MAC address.

MAC address (48-bit) :-

- 14 : 18 : 1A : 12 : 13 : 14

  0001 0100 → eigth bit is 0, then it is unicast MAC address

- 19 : 1A : 1B : 1F : 1A : 12

  0001 1001 → eigth bit is 1, then it is mulicast MAC address.

- FF : FF : FF : FF : FF : FF

  this is broadcast MAC address.

*So in destination MAC address field of ARP request packet, broadcast MAC address is given.

Special case :- when network wishes to form subnet, or we can say no-network only subnets, then

no. of subnets $= 2^k$ where k is the no. of subnet bits.

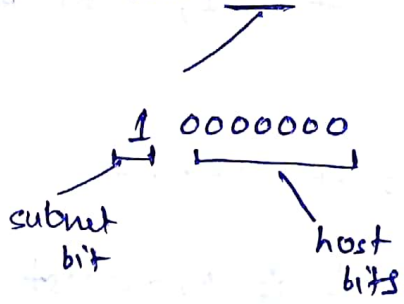
Sometime question also mentioned explicity configured zero subnet, OBA subnet.

for eg- IP = 199. 96. 89. 43 and subnetmask

= 255. 255. 255. 128.

(i) zero subnet ID :-

255. 255. 255. 128



so, for subnet ID all host bits are 0's and for zeroth subnet, subnet bit is 0.

i.e 0 0000000

199. 96. 89. 0

first host of zeroth subnet ID : 199.96.89.1

last " : 199.96.89.126

DBA of zeroth subnet ID : 199.96.89.127

(ii) DBA subnet ID :

for DBA subnet ID subnet-bit is 1 and all host bit is 0.

199.96.89.128

first host of DBA subnet : 199.96.89.129

last host of " : 199.96.89.254

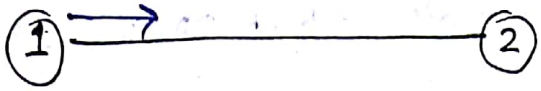
DBA of DBA subnet : 199.96.89.255

so, if subnet bits are 2

ie
- 00 — zero subnet
- 01 — 1st subnet
- 10 — last subnet
- 11 — DBA subnet

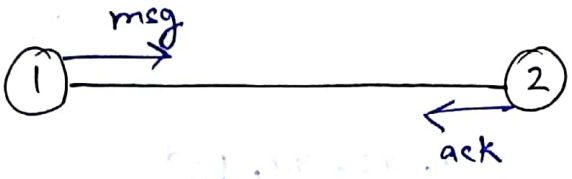
Types of transmission :-

(i)



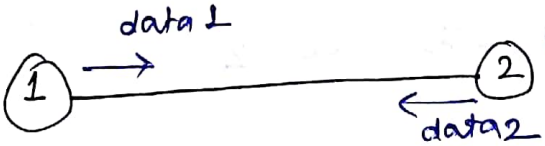
when only one system is transmitting then it is known as simplex transmission.

(ii)



when one party sending a msg and second party will send acknowledgement then it is known as half-duplex transmission. Both cannot transmit data at same time.

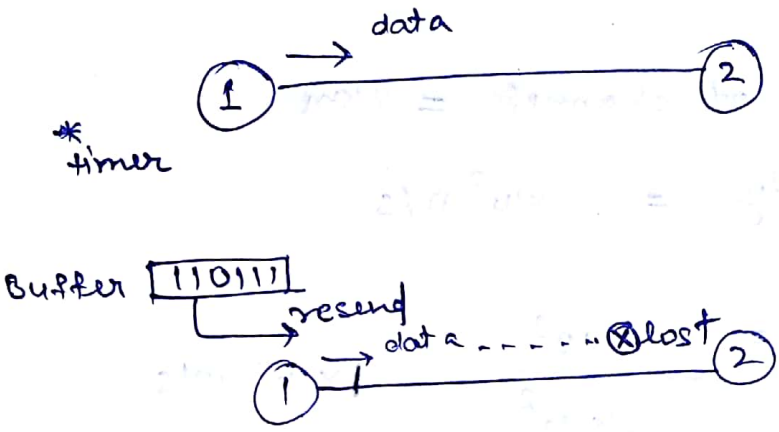
(iii)



when both system are able to transmit data at any instance of time, can be simultaneous. This transmission is known as full-duplex transmission.

- Timer is required because waiting time is finite.

- Unfortunately if data is lost, in order to resend the data we require buffer.



- The time taken by the system to put whole data on channel for transmission is known as transmission time.

$$\text{Transmission time} = \frac{\text{Data size (bits)}}{\text{Bandwidth (bps)}}$$

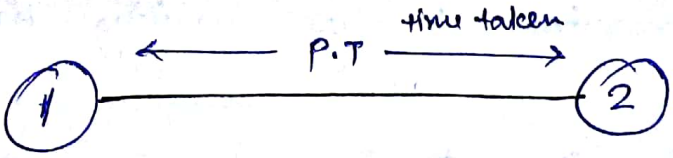
eg: datasize = 2Kb

Bandwidth = 10 Mbps

$$\text{So, } T.T = \frac{2\times10^{3}}{10\times10^{6}} = 2\times10^{-4}\ s$$

$$= 200\times10^{-6}\ s$$

$$= \boxed{200\ \mu s}$$



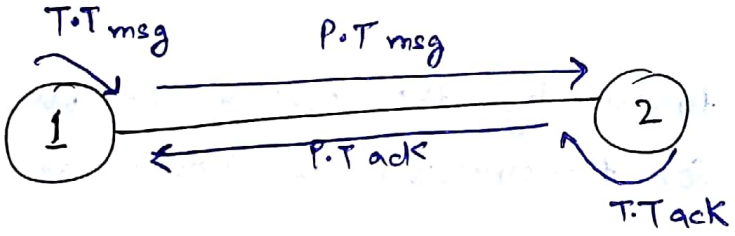
Propagation time = $\frac{\text{length of channel}}{\text{velocity of channel}}$

eg: length of channel = 2km

velocity = 2×10^8 m/s

P.T = $\frac{2 \times 10^3}{2 \times 10^8}$ = 1×10^{-5} m/s

= 10×10^{-6} m/s = 10 μs



since size(ack) <<< size(msg)

so, T.T (ack) <<< T.T (msg)

T.T ack is negligible.

but P.T msg = P.T ack

$$\left(\text{Total time}_T = T.T_{data} + P.T_{data} + T.T_{ack} + P.T_{ack}\right)$$

$$= TT + 2PT$$

$$\%\ \text{Link utilization of sender} = \frac{TT}{TT + 2PT} \times 100\ \%$$

eg. if $LU\% = 50\%$

then $\frac{TT}{TT+2PT} = \frac{1}{2}$

$\Rightarrow 2TT = TT + 2PT$

$\Rightarrow \boxed{TT = 2PT}$

Q. $LU\% = 50\%$ length of channel = 200m, velocity of channel = 2×10^8 m/s and bandwidth = 10Mbps. Calculate Data size = ?

$$\left(TT = 2PT\right)$$

$$\Rightarrow \frac{\text{Datasize}}{BW} = 2 \times \frac{\text{length}}{v}$$

$$\text{Data size} = \frac{2 \times 200 \times 10^6}{2 \times 10^8} = \boxed{20 \text{ bits}}$$

- Round trip time (RTT) = 2 × PT (double of propagation time).

Q: B.W = 10 Mbps, calculate 1-bit delay

1 sec = 10^7 bits

so, time taken by 1-bit = $\frac{1}{10^7} = 10^{-7}$

$= 0.1$ MS

** Q: B.W = 100 Mbps, $v = 2 \times 10^8$ m/s. Calculate 1-bit delay in meters of cable?

10^8 bits = 1 sec

1 bit = 10^{-8} sec

so, distance covered by that bit in 10^{-8} s

so, velocity of channel = 2×10^8 m/s

i.e 1 s = 2×10^8 m

so, in 10^{-8} s = $2 \times 10^8 \times 10^{-8}$ m

$= 2$m

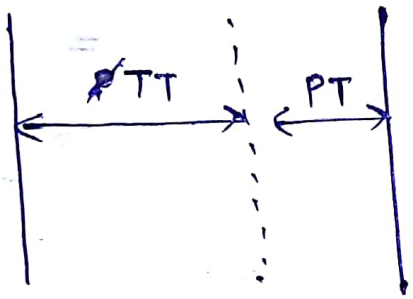
so, that mean two consecutive bits are seperated by distance of 2m.

Trade of PT and TT in LAN and WAN :-

in LAN length of channel is less (around few meters)

so, $PT = \frac{l}{v}$ ie PT↓

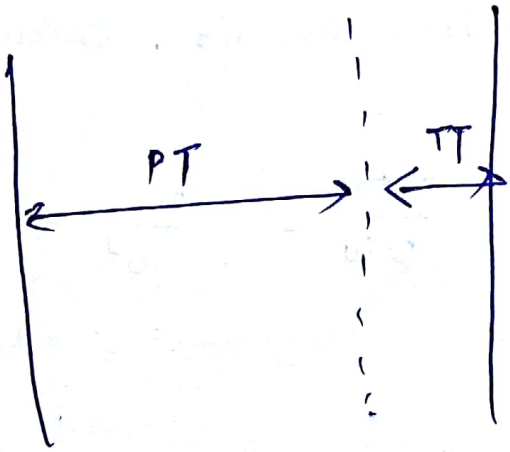
so, dominating factor will be TPT.



whereas in WAN length of channel is large (many km)

so, $PT \propto l$ thus PT ↑

Thus PT is dominant.



Q. B.W = 10Mbps, RTT = 50 μs. Calculate no. of bits that can be transmitted in RTT in LAN?

since $RTT = 2 \times PT$

since in LAN TT dominates

so, $(TT \sim RTT)$

thus no. of bits transmitted = RTT × BW

$= 50 \times 10^{-6} \times 10^{7}$

$= 500$ bits.

Throughput (transmission rate) $= \frac{\text{Datasize}}{\text{Total Time}} = \frac{\text{Datasize}}{TT + (2 \times PT)}$

Q. B.W = 10Mbps, $l = 200m$, $v = 2 \times 10^{8}$ m/s

Datasize = 200 bits. Calculate Throughput.

$T.T = \frac{\text{Data}}{B.W} = \frac{200}{10^{7}} = 20\,\mu s$

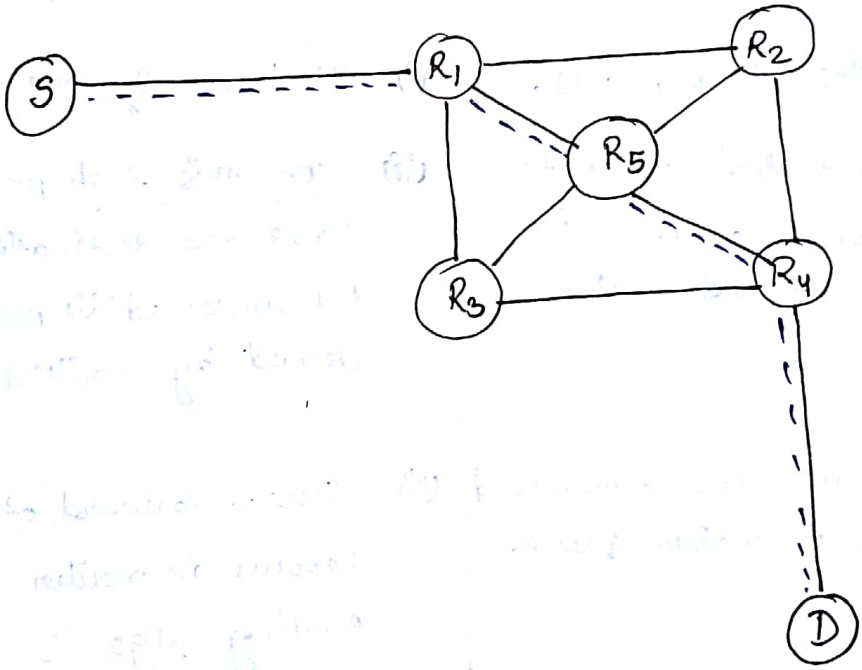
$$PT = \frac{l}{v} = \frac{200}{2 \times 10^8} = 1\,\mu s$$

so, $$\text{throughput} = \frac{200 \text{ bits}}{(20 + 2)\,\mu s} = \underline{9.09 \text{ Mbps}}$$

Thus, Throughput < Bandwidth.

$$\%.LU = \frac{\text{throughput}}{B.W} \times 100\%$$

Circuit Switching & Packet Switching :-

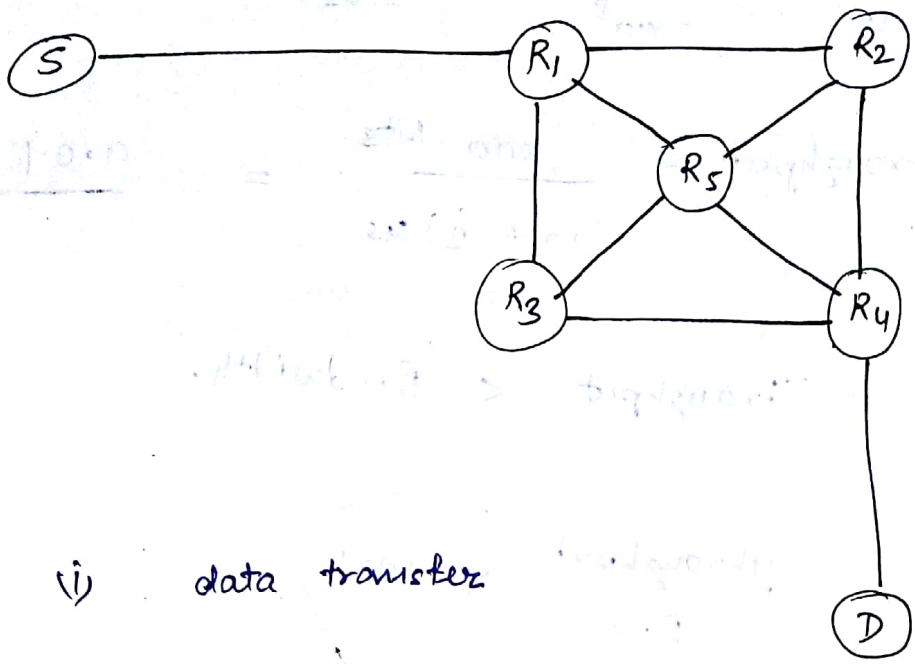


circuit switching

(i) connection establishment

(ii) Data Transfer

(iii) connection release



Packet switching

(i) data transfer

Circuit Switching	Packet switching
(i) It contains three phases.	(i) It has only one phase.
(ii) whole path from source to destination (address) is known to each data packet.	(ii) In this each packet will have the destination address, the intermediate path is decided by routers.
(iii) There is no store & forward operation in router queue.	(iii) Store & forward of data packets happens in router queue. Routing algo is applied and data-packets are forwarded on best path.
(iv) ~~The~~ The delay b/w the ~~packets~~ data is uniform. ~~whereas in packet switching~~	(iv) The delay b/w data packet is variable.

(v) Transmission of data is done by source only.	(v) Transmission of data is done by source as well as intermediate routers.
(vi) Resources are reserved in this as whole path is reserved for transmission of data for a particular source.	(vi) Resources are not reserved, it is shared among different sources.
(vii) Wastage of resource is more.	(vii) Wastage of resources is less.
(viii) Congestion can occur during connection establishment	(viii) Congestion occur during data transfer.
(ix) It is not fault-tolerant.	(ix) It is fault tolerant technique. Because packets can be diverted via other paths if links are broken.
(x) It is reliable as whole path is known.	(x) It is not reliable as there might be a loss of data.
(xi) Prefered for long messages.	(xi) Prefered for sending short messages.
(xii) It is a slow process	(xii) It is a fast process.

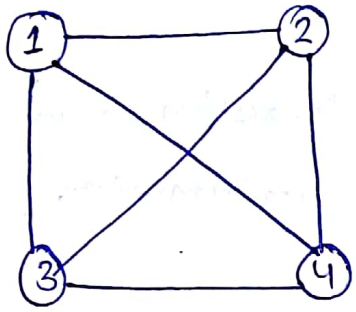
LAN Topologies :-

Physical topologies – Mesh, star, BUS

Logical topologies – IEEE 8023, IEEE 802.11

(i) MESH:

* every divice connected to each other devices.



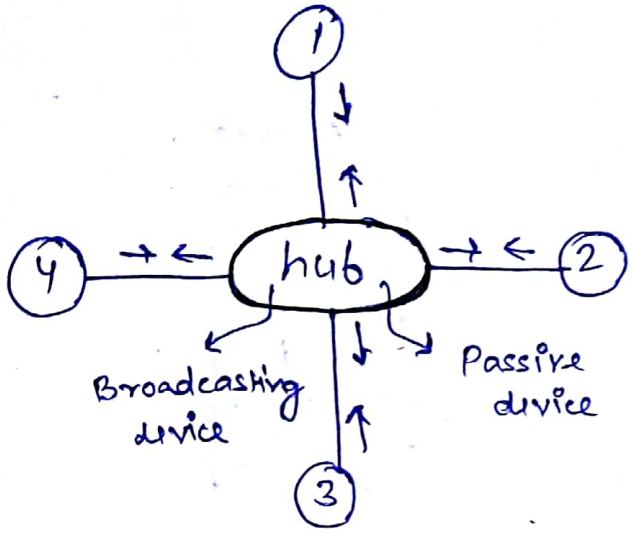
* for n devices ${}^{n}C_{2} = \frac{n(n-1)}{2}$ connecting cables are required.

Advantage :- ↳ Security is provided as each two devices has there seperate channel.

↳ Fault tolerance as alternative paths can be provided.

Disadvantage :- ↳ No. of cables are more, thus not economically efficient.

(ii) STAR :



(4-collision domain)

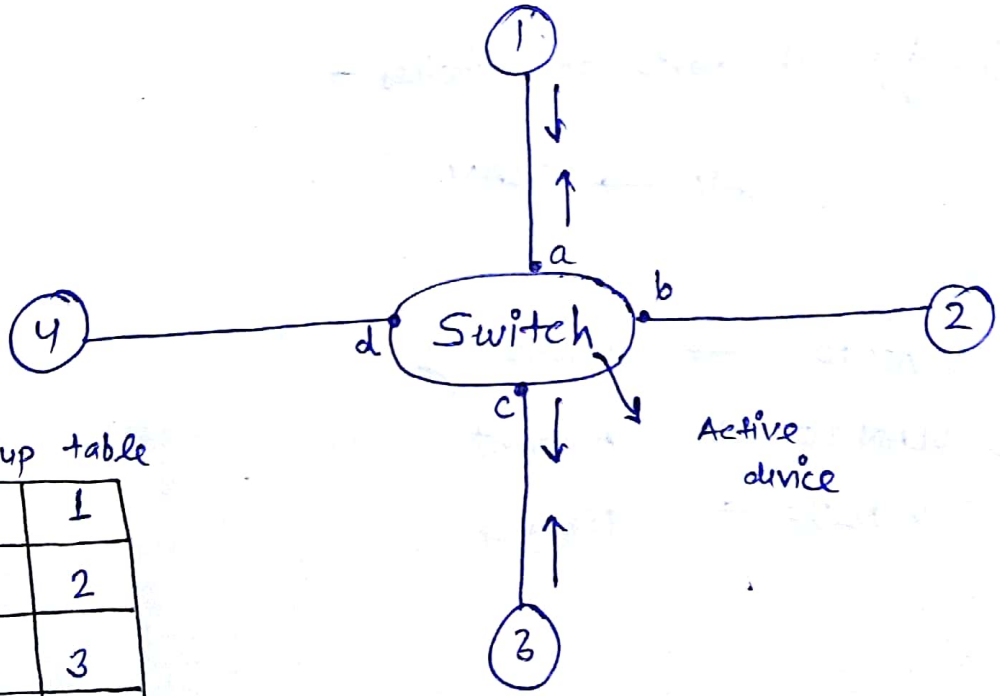
* all devices are connected to a single centric device (hub).

* n devices need n no. of cables.

* whenever a data packet is arrived at "hub", it broadcasted to each other devices.

- The place or area, where the collision are confined is known as collision domain.

- If HUB is used as a centric divice, then entire network has same collision domain. (HUB is not a collision domain seperator).

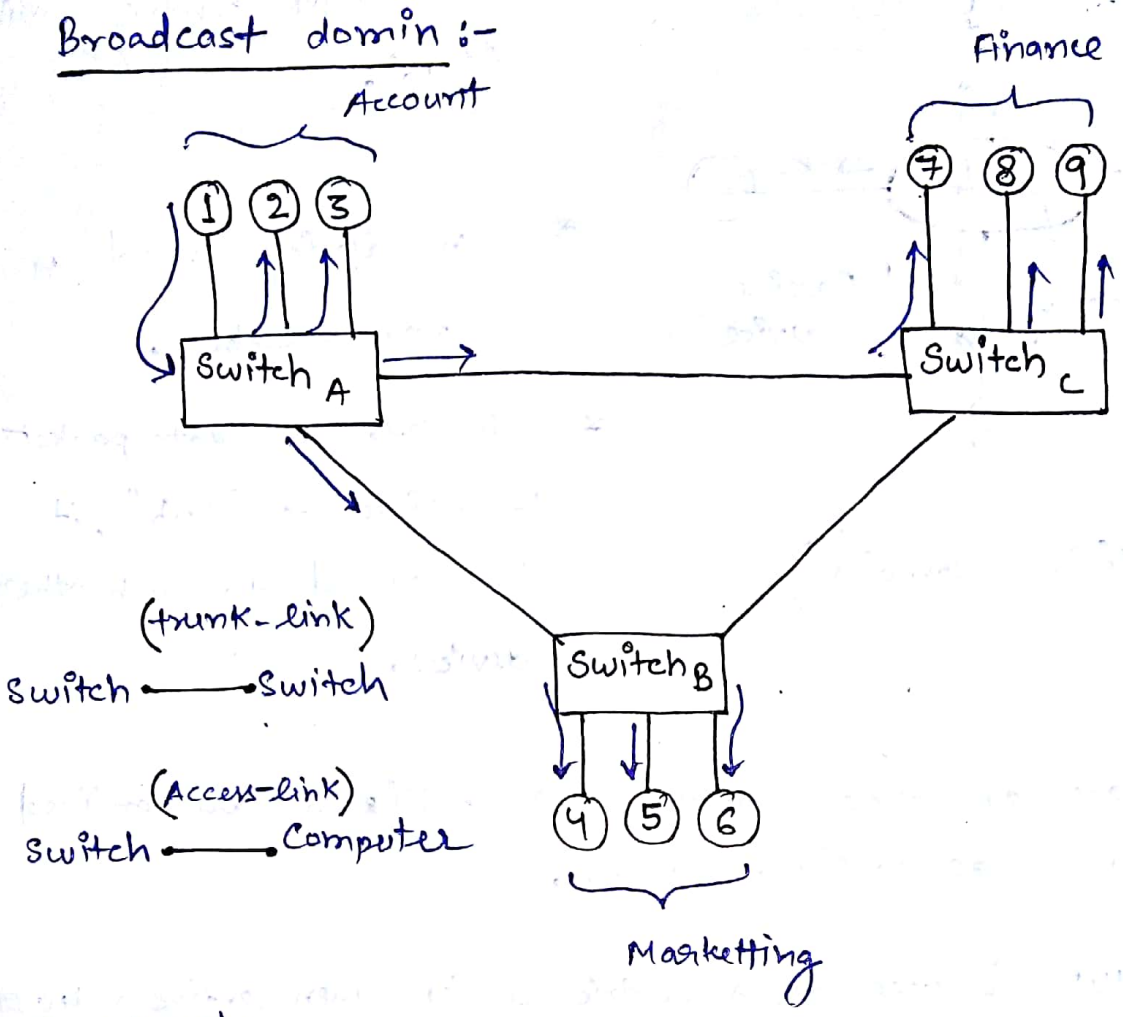


Lookup table

a	1
b	2
c	3
d	4

- Switch is a collision domain seperator device.

Broadcast domin :-



By default

* L Switch is not a Broadcast domain seperator.

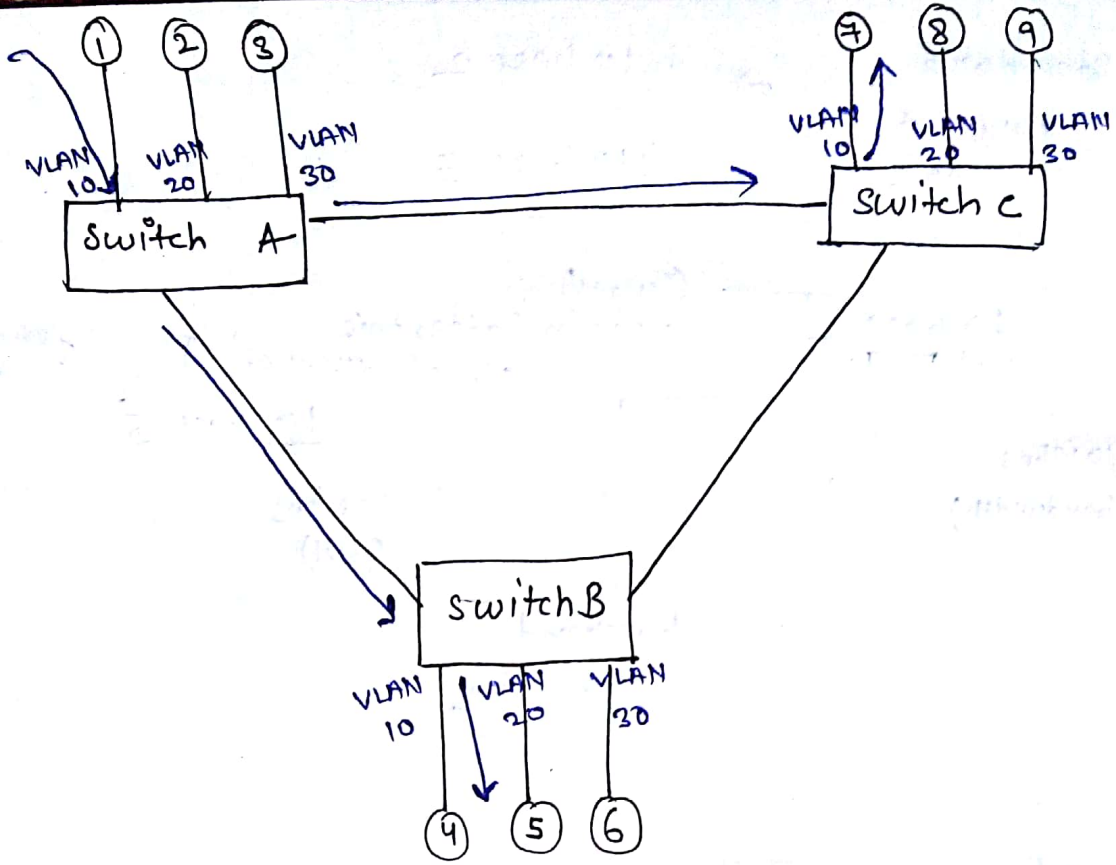
- By configuring the ports of switches -

LAN → VLAN

VLAN 10 → marketing

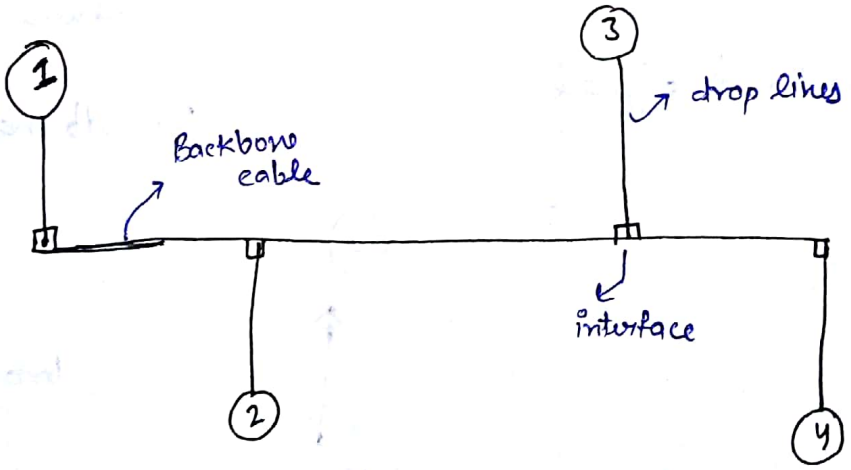
VLAN 20 → Account

VLAL30 → Finance



* if LAN is converted to VLAN then switch can perform as broadcast domain seperator.

(iii) BUS :



for n divices n drop cable + 1 backbone co-axial cable is required.

Standard ethernet cable ⇒ (i) 10 base 2

(ii) 10 base 5

so,

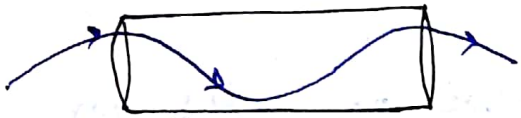
10 base 2 — (length) = 200 m (after this signal attenuation)

10 MBps (bandwidth)

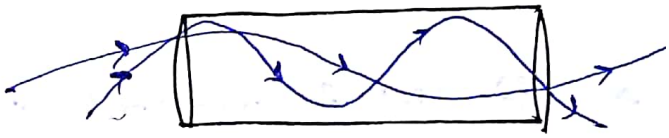
baseband signalling

10 base 5 — length = 500 m

10 MBps (BW)



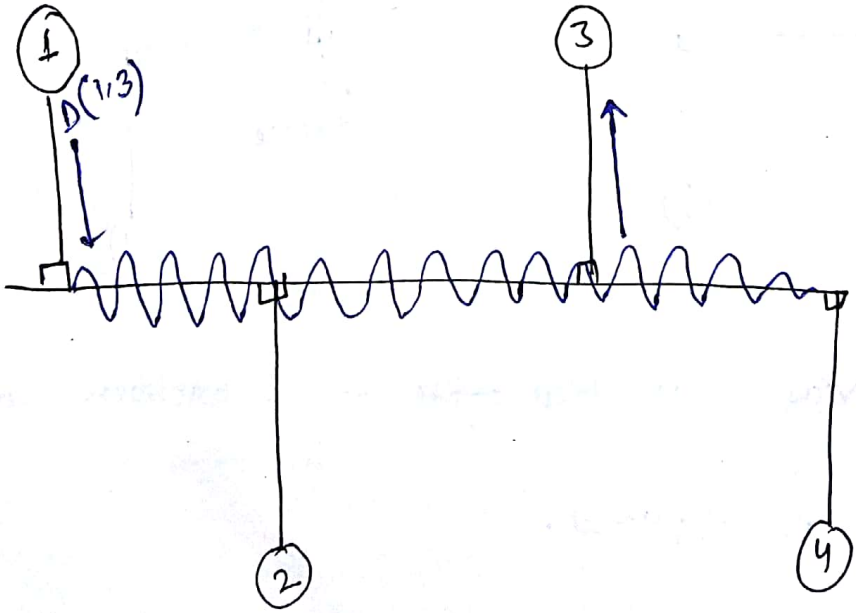
one - type of frequency or data is allowed at instance of data



more than one type of frequency or data is allowed at a instance of time.

Baseband signal

Broadband signal



broadcast channel and shared channel

* data-packet is broadcasted on backbone cable, only destination host will consume it.

Bell labs :

$$\text{signal to noise ratio} = \log_{10}\left(\frac{\text{signal power}}{\text{noise power}}\right) \text{ bells}$$

$$= 10 \times \log_{10}\left(\frac{S_p}{N_p}\right) \quad \underline{db}$$

eg:- signal power = 10 mW

noise power = 100 mW

$$\left(S/N\right)_{\text{ratio}} = 10 \log\left(S_p/S_n\right) = 10 \log\left(10/100\right)$$

$$= \underline{-10\,dB} \quad (-ve)$$

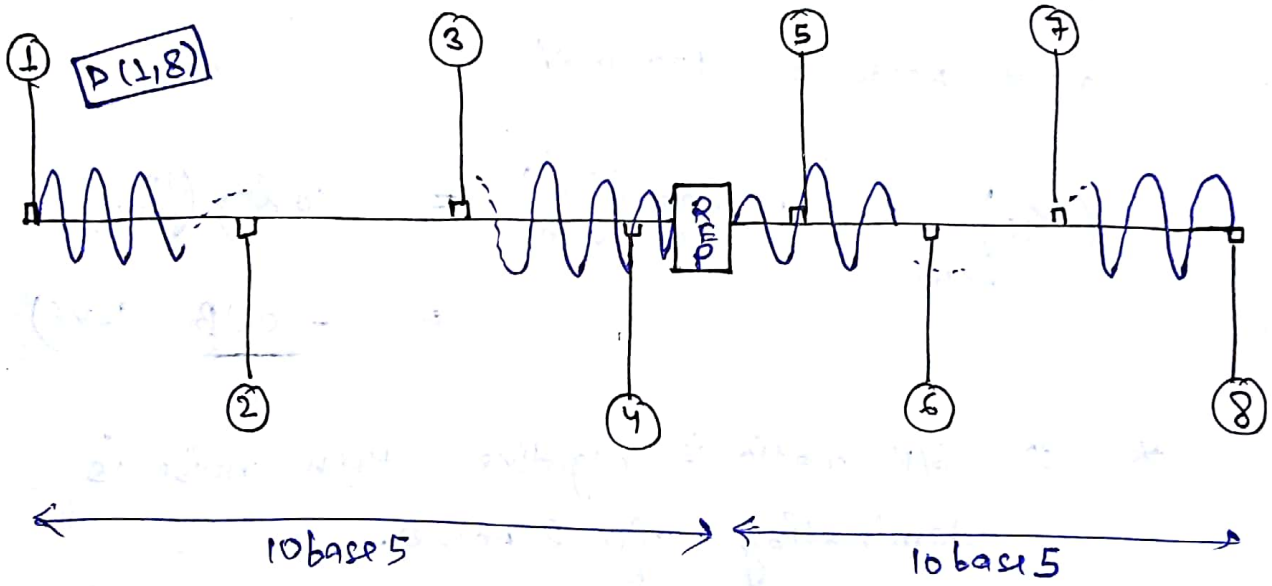
* if S/N ratio is negative then noise is dominating signal power.

* if S/N ratio is ~~+ve~~ +ve then n. signal power is dominating noise power.

Shannon experiment –

$$\text{max data rate} = (BW)\log_2\left(1 + S/N\right)$$

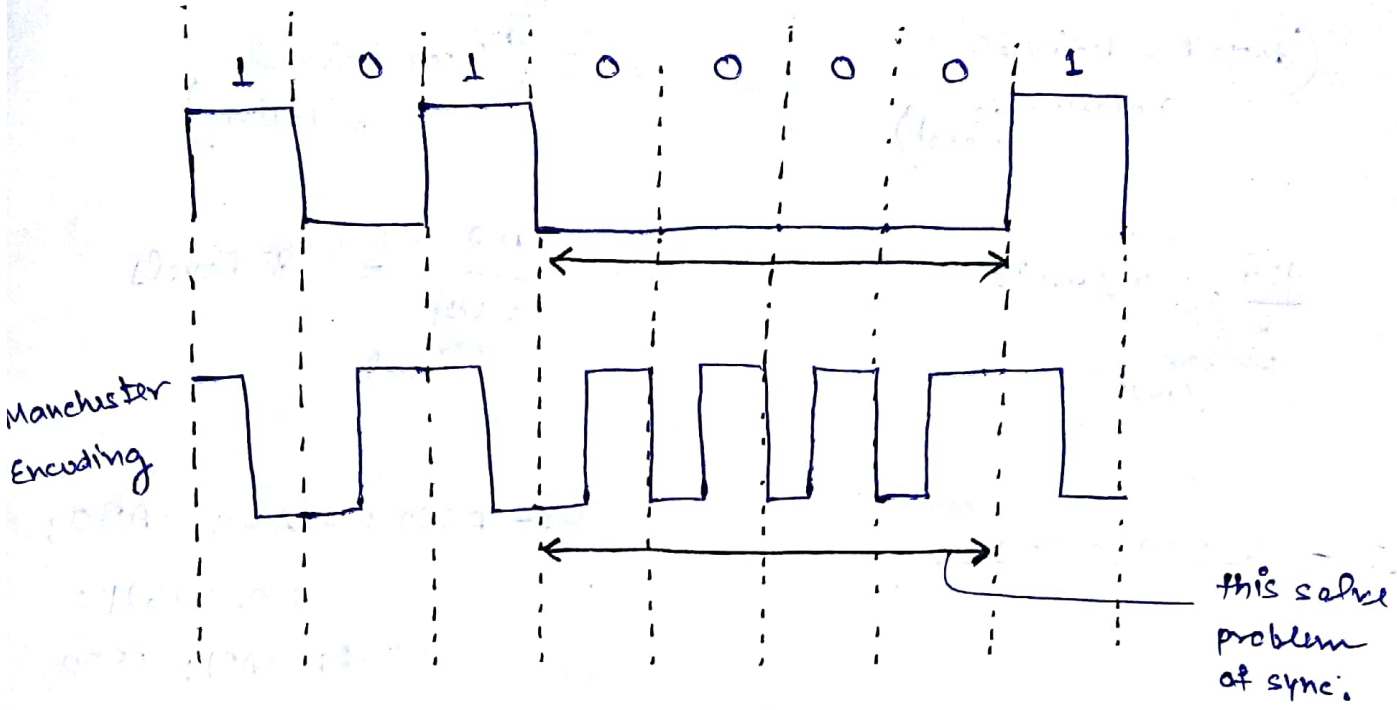
* In order to connect more devices by joining backbone -cable we need a device known as REPEATER. It regenerates signal to its original strength.



- REPEATER & HUB both are passive devices. REP is two port device whereas HUB is multiport-device.

Synchronization & encoding –

Data = 10100001



* Manchester encoding is used to eliminate problem of synchronization & high dc component.

* Manchester encoding assumption -

* As we can see encoder increases the frequency of waveform, whereas decoder decreases the frequency.

IPv4 (32-bit) → IPv6 (128-bit)

(dotted - decimal notation is used)

(hexa decimal notation)

$\frac{128}{8}$ = 4 levels (8 bits per level)

$\frac{128}{16\text{-bits per level}}$ = 8 levels

eg - 63 : 39 : 29 : 12

eg - F680 : 75A2 : 9AB0 : C532 : 7681 : 8432 : AAB1 : FF00

Q. IPv6 → FE80 : 0 : 1234 : 1A12 : 1B14 : 1C1E : 1D1F : 1A12

Compression technique:

FE80 : : 1234 : 1A12 : 1B14 : 1C1E : 1D1F : 1A12

substitute 0 value of level with :

(i) whenever a 0 is present in IPv6 address 0 can be replaced with '::'.

2001 : 1234 : 0 : 0 : 0 : 0 : 141A : 1B14

2001 : 1234 : : 141A : 1B14

(ii) whenever continuous 0 available in IPv6 address then all zeros can be replaced with "::"

– IPv6 → 2002 :0:0 : 1234 : 0:0:0 : 141A
(junc 1 = :0:0 ; junc 2 = 0:0:0)

→ 2002 ::1234 :0:0:0:141A

or

→ 2002 :0:0 :1234:: 141A

(iii) if 0's are present at discontinous places, then at only one junction 0 can replace with "::"

Q. IPv6 → ::

0:0:0:0:0:0:0:0 ⇒ unspecified address (similar to DHCP client in IPv4)

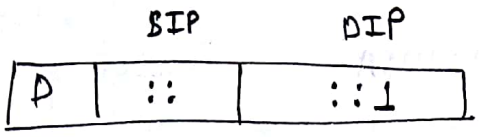
Q. IPv6 → ::1

0:0:0:0:0:0:0:1 ⇒ loop-back address (similar to 127.x.y.z IPv4)

* In IPv4 loop-back address 127.x.y.z, 2^{24} address are ~~wasted~~ used for loop-back testing whereas in IPv6 only one address is used as loop-back address.

Q. Check syntax of data-packet.

→



this means loop-back testing is performed by ~~an~~ host with unspecified address.

IPv6 Syntax :-

IPv6 address (128-bits) = Network prefix (64-bits) + Interface Id (Extended MAC) (64-bits)

Calculation of Extended MAC :-

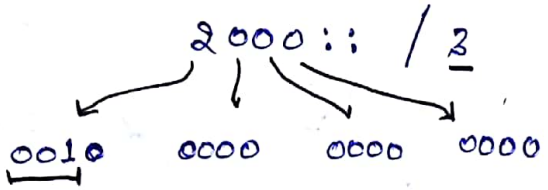
MAC address 48-bits = 16 : 1A : 1C : 1D : 1E : 12

FF : FE

= 16 : 1A : 1C : FF : FE : 1D : 1E : 12

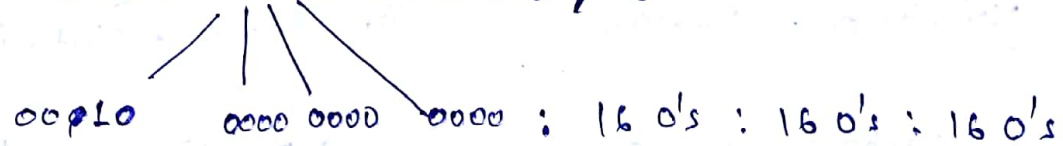
Extended MAC (64-bits) = 161A : 1CFF : FE1D : 1E12

Network prefix:- IPv6 Global unicast address (similar to public IP in IPv4)



* if first 3 bits is "001" then it is global unicast add

⇒ first add 2000:0:0:0/3



last add

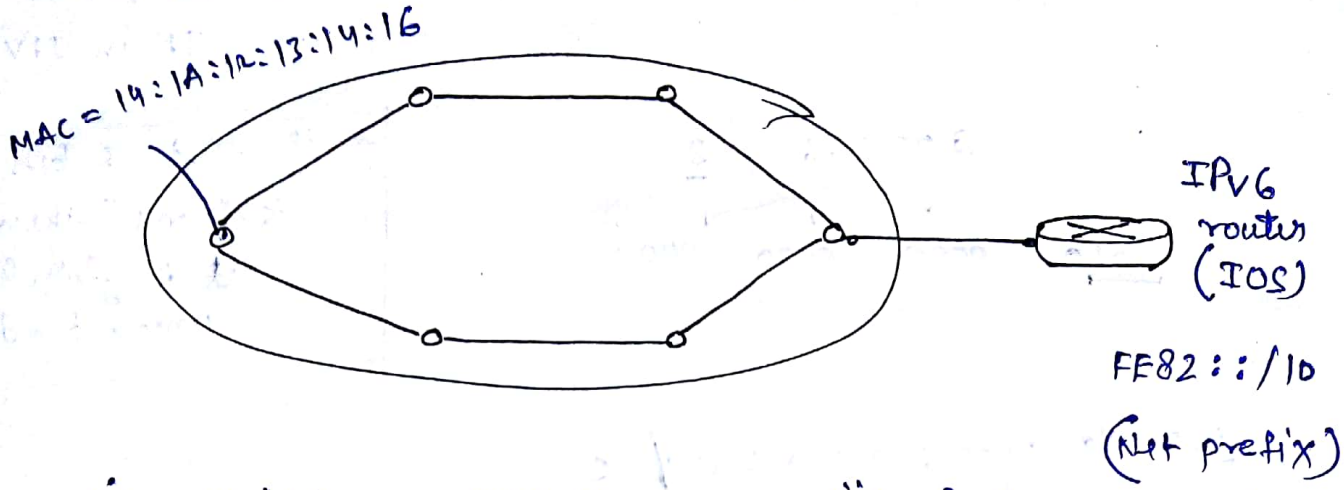
0011 1111 1111 1111 : 16 1's : 16 1's : 16 1's

3FFF : FFFF : FFFF : FFFF / 3

- These are the Network Prefix of IPv6 which are managed by ISP.
- when extended MAC address (at client side) are added to Network prefix then a complete IPv6 address is generated.

FE80::/10 → link local address
(similar to Private IP in IPv4)

IPv6 address assignment :-



(i) Neighbour solicitation

↳ Neighbour request

↳ Neighbour reply

(ii) Router solicitation

↳ Router request

↳ router reply

- In Neighbour request, client request other clients in LAN for there MAC address.

- In Neighbour reply, all clients will send there MAC addresses.

- Once the client get all MAC addresses, then it compare its MAC address with its neighbour. In its MAC add is unique then Extended MAC address is calculated.

Extended MAC add = 141A : 12FF : FE13 : 1416

- Router solicitation process is to ~~connect~~ collect the Network ID, which is then attached to Extended MAC.

FE82 :: 141A : 12FF : FE13 : 1416 /10

* IPv4 addressing is stateful as mapping table is maintained at server machine whereas IPv6 addressing is stateless as no table is maintained so there is no need to inform server for disconnecting.

* IPv6 addressing is fast as it doesn't need ARP protocol to findout the MAC address of destination as MAC is part of IPv6 address.

* IPv6 doesn't need DHCP server configuration.

* IPv6 can have ~~one~~ two address at same time. One is link local and other is global unicast.

- By default IPv6 doesn't required NAT configuration router because from the origin point it has the public IP address.

- IPv6 doesn't support broadcasting, it support only multicasting.

192.1.

Anycasting :-

↳ IPv6 support anycasting i.e all nodes will have the same address, but the service is provided by the nearest node.

- For mobile networks or cellular networks, IPv6 is suitable & as network overhead is less.