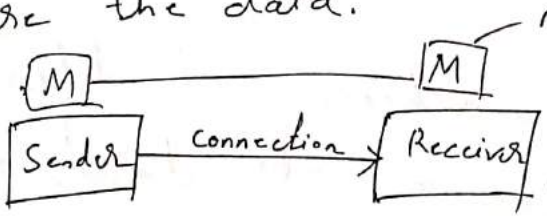
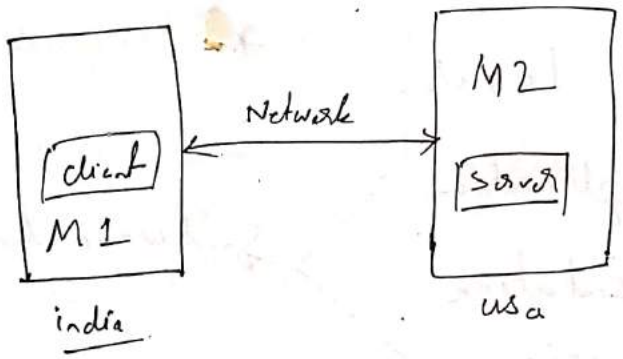
Computer Networks

Collection of various computing devices to share the data.



To read the data which Receiver received from Sender, there must be some protocal (set of instruction) in both machine. So that both machine can understand each other.

Proper communication = connection + proper protocal



computer network make used that both are on same machine. like in facebook accessing data is very fast.

Functionalities —

Mandatary:
(i) Error control (catching error)
(ii) Flow control (amount of data send)
(iii) Multiplexing & demultiplexing (lot of processes are going on & which process sending data)

etc.

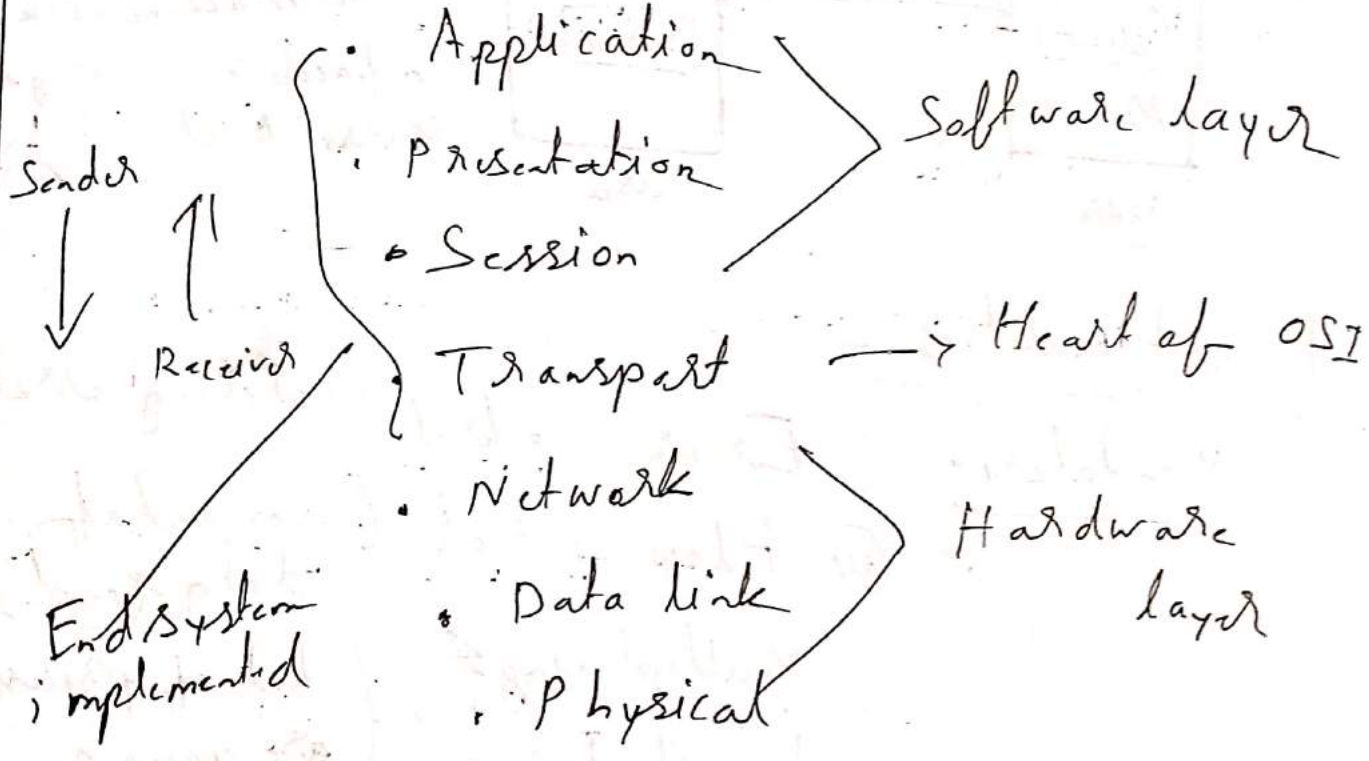
Optional:
(i) Encryption (banking app, valuable data need)
(ii) checkpaint (big files is split into

Several checkpoint. like if we downloading a file of 500 mb, there is checkpoint in every 100 mb & if fails at 350 mb. Then downloading will start from 300 mb again).

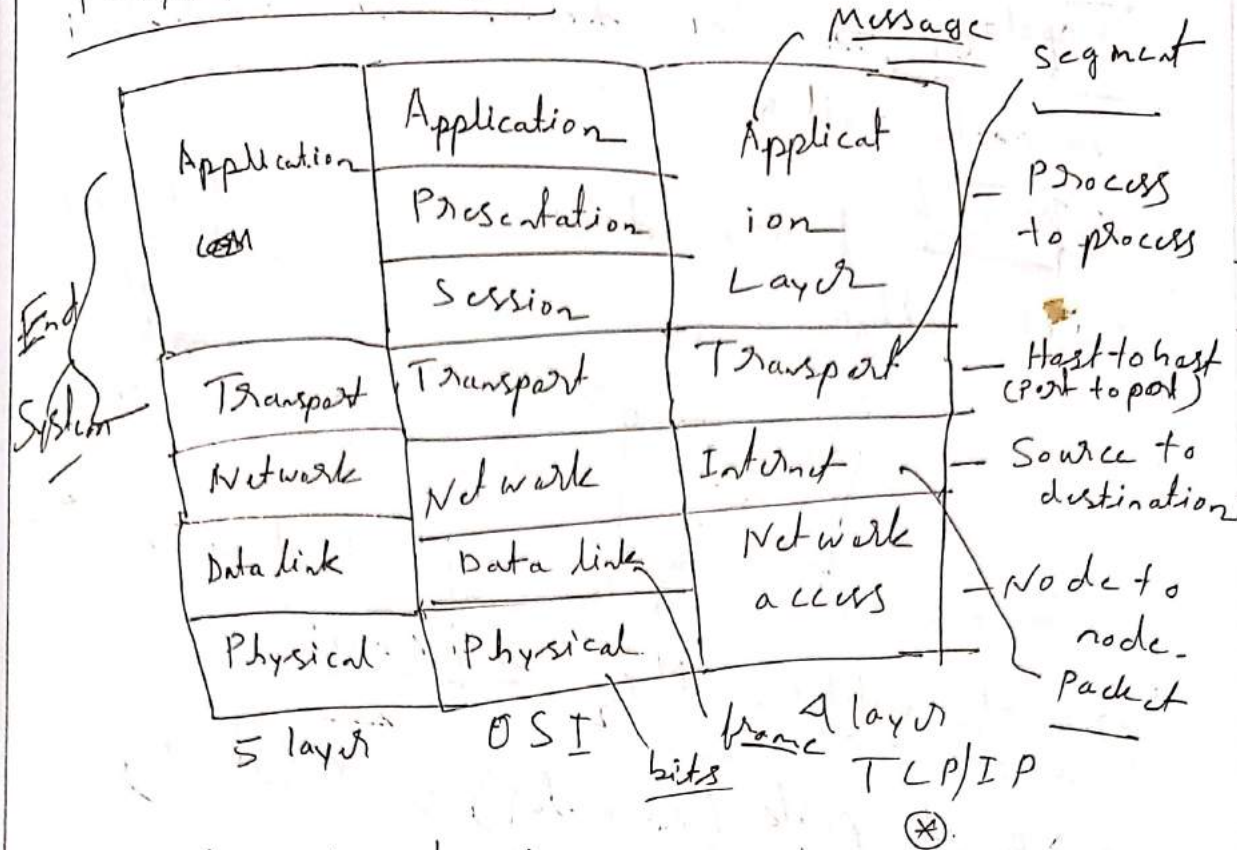
In order to achieve all this functionalities we follow a standard model (OSI or TCP/IP ...) Transmission control protocol.

- OSI (open System interconnection) Model is a conceptual framework used to describe the function of a network System.

There are 7 layers



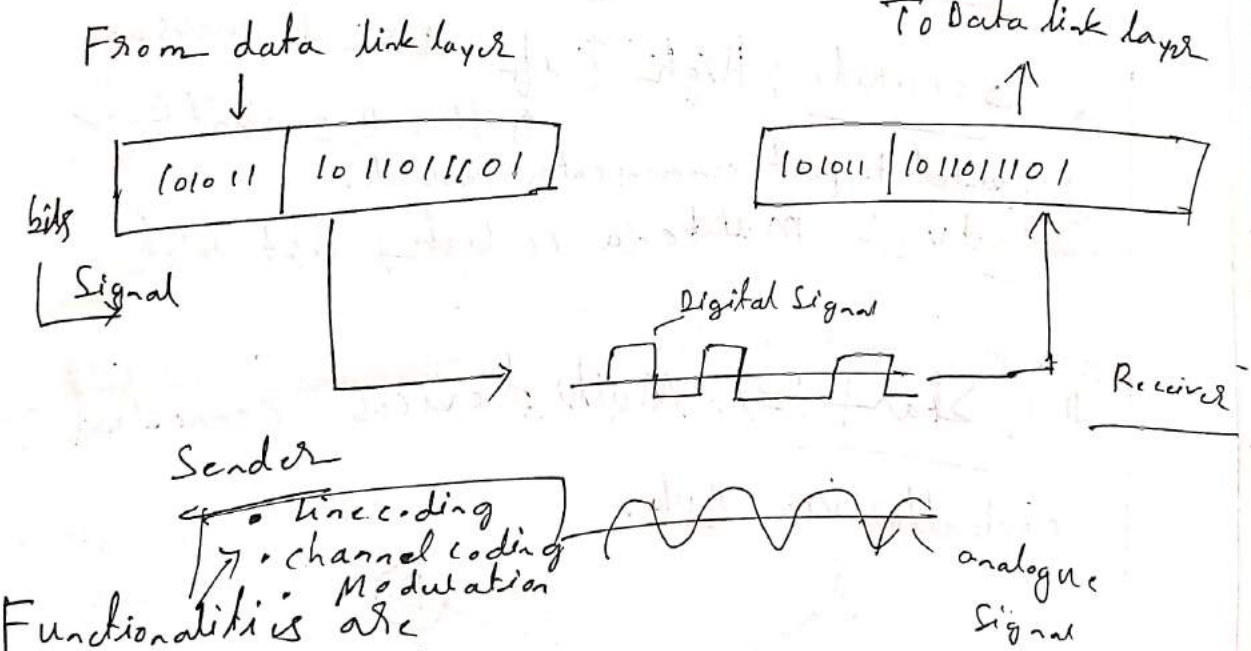
TCP/IP Vs OSI



TCP/IP is developed by ARPANET

- Support client server and Peer to peer

Physical Layer Functionalities ⇒

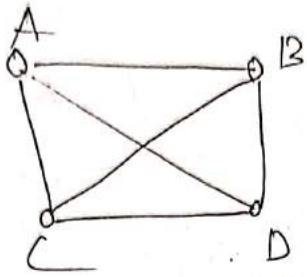


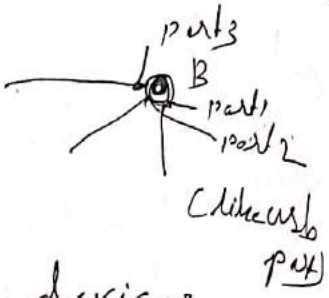
Functionalities are

- Cable, Connectors
- Physical Topologies
- Hardware (Repeater, hub)
- Transmission mode (simplex, duplex, Half duplex)
- Multiplexing (multiple signal in one time)
- Encoding (Fm use analogue signal)

Topology :⇒ How devices are connected to each other

(i) Mesh : Every device is connected with each other

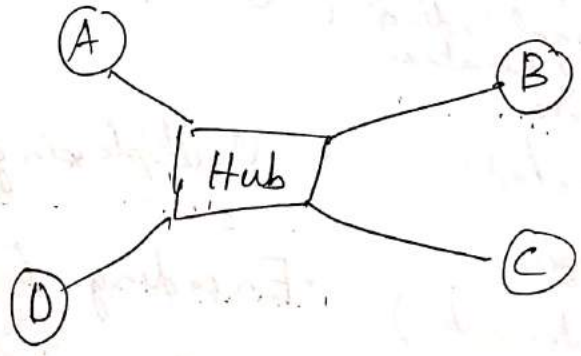




- No of cables = $^{n}C_2 = \frac{n(n-1)}{2}$ (n = number of devices)
- No of ports (connector) = $n(n-1)$
- Reliability : High (if one cable fail still we can send message via other way)
- Cost : High (a large number of cable)
- Security : High (if A send message to D then B, C can't know)
- Point to point communication possible.

Disadv :- Maintenance high, cost high

(ii) Star :⇒ Multi devices connected to each other via Hub.



. No of cables = n

. No of ports = n

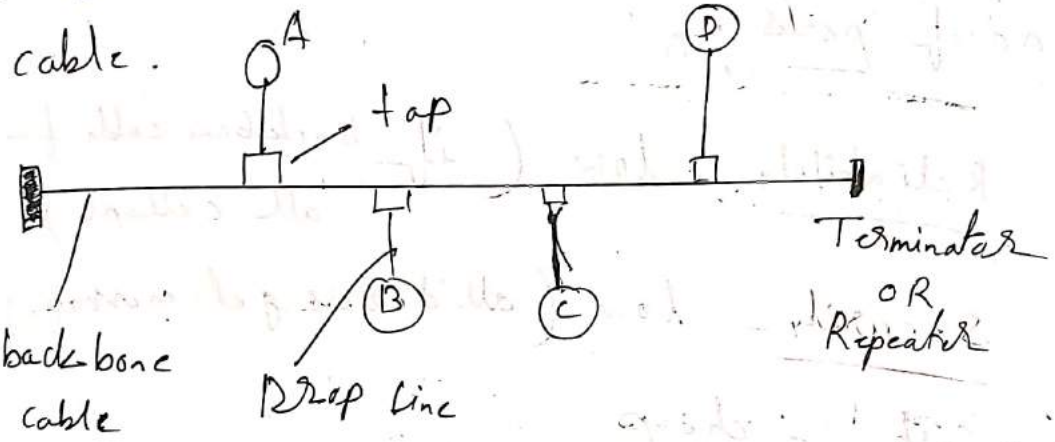
. Reliability :- Low (if hub fails then whole communication lost) Single point failure

. cost : comparatively low than Mesh

. Security : Low (Hub send message to every device)

. Point to point communication possible

(iii) Bus :⇒ Multidevice connected to a single cable.



tap Connect to device with backbone table.

Drop line ~~connect to~~ is a cable which connect tap & device

. No of cables = n+1

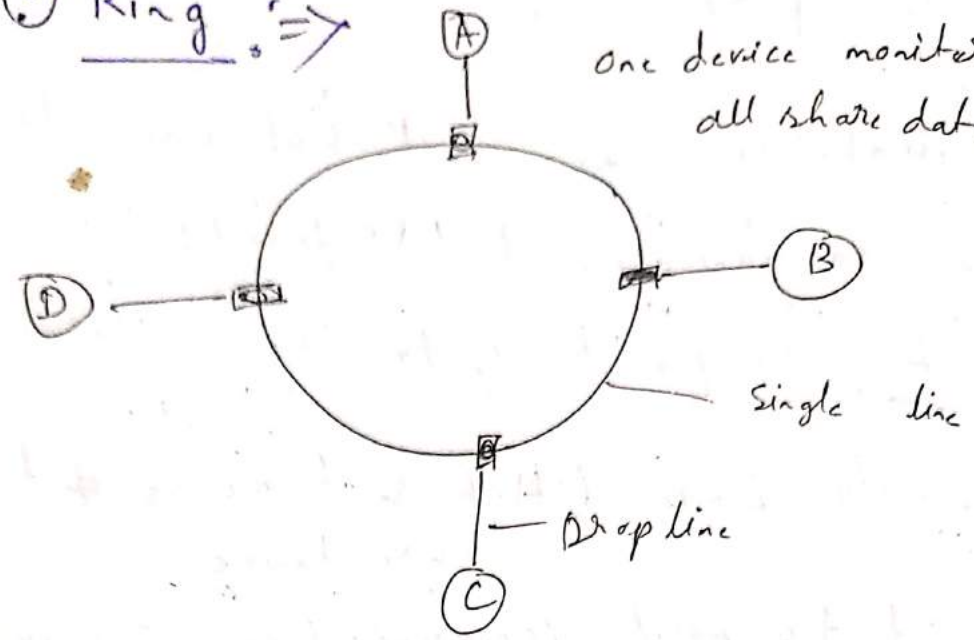
. No of ports = n

. Reliability :- low (if backbone cable fail full system collapse)

. Security :- Low (if A send to D, other device will also get the message)

- Cost :- cheap (cables is few)
- multipoint so callison happen (if every device send sign at a time it called)

(iv) Ring :- =>



one device monitor, rest all share data

No of cables : n+1

no of ports : n

Reliability :- low (if backbone cable fail all collapse)

Security - low (all devices get message)

Cost :- cheap

Here also callison happen

. we use Token ring to avoid callison.

Token Ring :- => A token is a frame of data transmitted between network points. Only a host that holds a token can send data and token are released when receipt of data is confirmed.

• It is used in Ring and Star topology to prevent collison.

Manchester Encoding & Differential Manchester :⇒

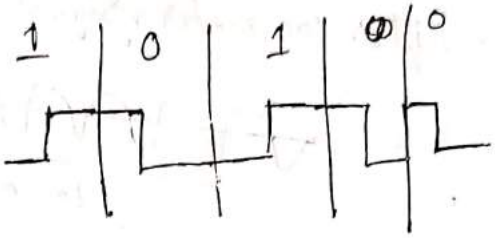
We use Manchester & Differential Manchester Encoding to transfer digital → digital

2 convention - (i) IEEE (default)
(ii) Dr Thomas ← opposite

IEEE

0 -

1 -



Devices :⇒

(i) Cables
(ii) Repeater
(iii) Hub
— Hardware

(iv) Bridges
(v) Switches
(vi) Router
— Hardware + Software

(vii) Gateway - tsm

(viii) IDS
(ix) Firewall
— Security

(x) Modem (Modulator & Demodulator)

(physical layer)

Cables: Cable is medium for transfering data.

(i) **Unshielded twisted pair cable**: electrical signal

Base band – at a time only one signal can move

Broad band –, at a time multiple signal

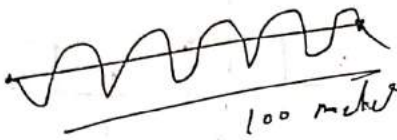
10 Base T → 100 meter

100 Base T → 100 meter, 100 mbps

10 → 10 Mbps (megabits)

Base → base band

- it is used in Ethernet, LAN
- After 100 meter signal strength very low



(ii) **Coaxial cable**: electrical signal

10 Base 2 → 10 mbps, 200 meter

10 Base 5 → 500 meter

(iii) **Fibre optic**:- light signal speed

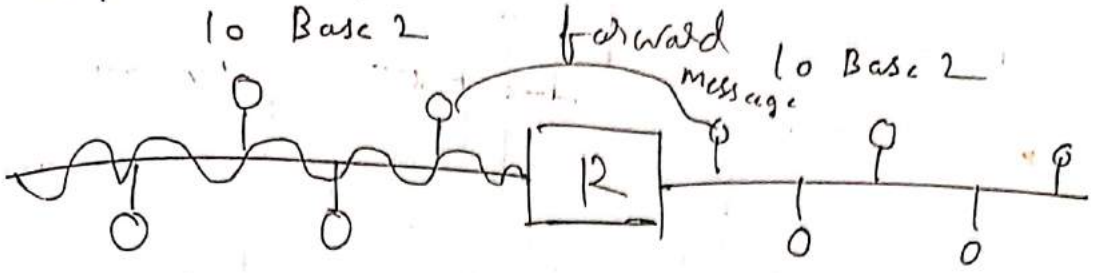
100 Base Fx → 100 MBPS (megabits), ~2 km

(*) If there is n device then n devices participate in collison

(*) Cables are used in physical layer

(*) it does not support filters (it two lan connect then

Repeater ⇒ (Hardware) it works only on physical layer
Layer 1



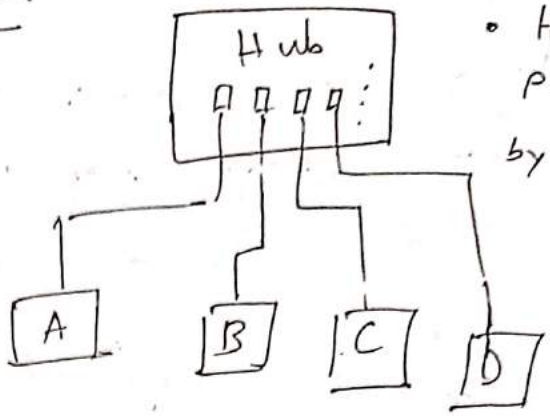
Repeater Regenerate the strength original (X → X)

Amplifier increase strength (X → 2X, X → 3X)

- We increase distance of signal with the help of Repeater
  - It is a 2-port device
  - Repeater forward the message.
  - It can't filter (as its hardware device, it can't know whether the destination of a signal already passed)
  - Max collision n (number of devices attached) (as Repeater has no buffer)

Hub :=> It is part of physical layer. It has no software.

Layer 1



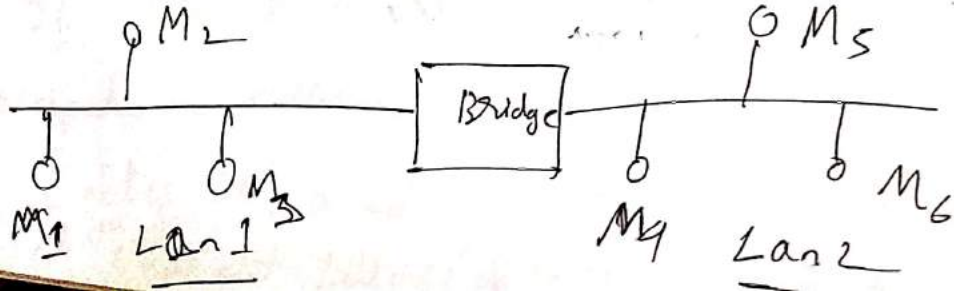
- Hub can say which port has problem by blinking which repeater can.

- multiport device
- It Forward the message
- It does not support Filtering (as it has no software, it can't filter message)
- Max collision - N (number of device)

Bridges :=> it works Physical & Data link Layer

Layer 2

- Used to connect two different LAN
- Bridge can check Mac address
- It support Forwarding of message
- It support Filtering. (It checks whether destination is right side or left side. if it is in left side it does not forward)



- Collison is very low as Bridge has a dedicated buffer to store & forward.
- Bridge make spanning tree to avoid loop with the help of data unit protocal.

Bridge has 2 type

(i) Static : Packet has source & destination mac address. Bridge check the static box and decide whether destination address is on which side & whether to send or not.

MAC	Port
M_1	P_1
M_2	P_1
M_3	P_1
M_4	P_2
M_5	P_2
M_6	P_2

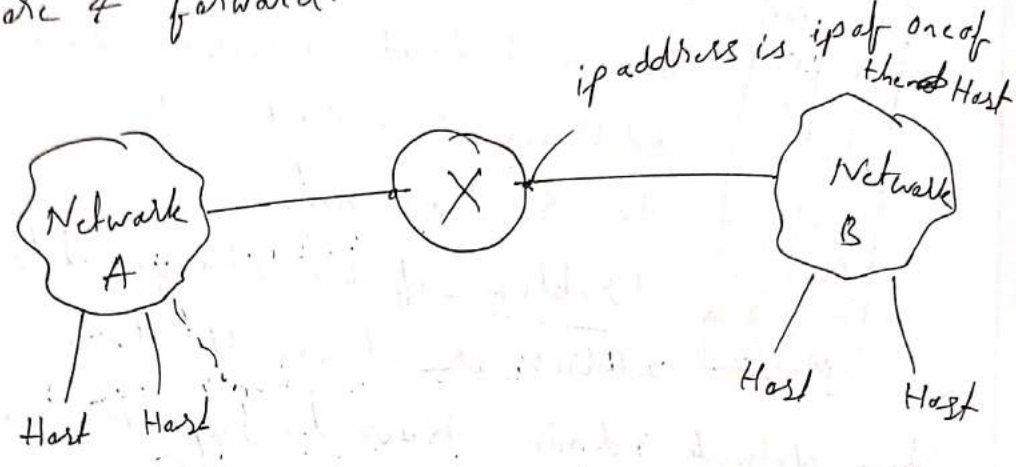
Problem - if we change the Mac address or change the device location then Network admin have to type manually on the bridge.

(ii) Dynamic : First Mac & port table is empty then bridge itself learn and entry the values.

Suppose a packet came with $\boxed{\overset{S}{M_1}\,\overset{D}{M_2}}$ So bridge entry M_1 & M_5 and in port column it first entry P_1 (in the M_1 side) then as it has no. port value of M_2 it just forward the packet. After acknowledging data the destination send a reply and bridge did entry according to it.

Router :=> It works on Physical, data link layer, (Mac) Layer 3 Network Layer - (ip address)

- It support Forwarding
- It support Filtering using Routing table
- Collison less as Router uses buffer to store & forward.



Circuit Switching :=> Developed for Telephone Connection. (Physical layer)

We use circuit switching for physically connect the telephone

- First we setup the connection by dialling number & make a dedicated path
- We send data in contiguous flow. (we speak continuously).
- it does not use any headers (it does not need any ip/mac as it use direct connection).
- Efficiency less (Connection is on if you did not disconnect & path is reserved)

- Delay less (there is no extra device for store & forward, Process)

Total time = Setup time + transmission time (TT) + Propagation Delay (PD) + teardown time

Resource deallocation

Message / Bandwidth

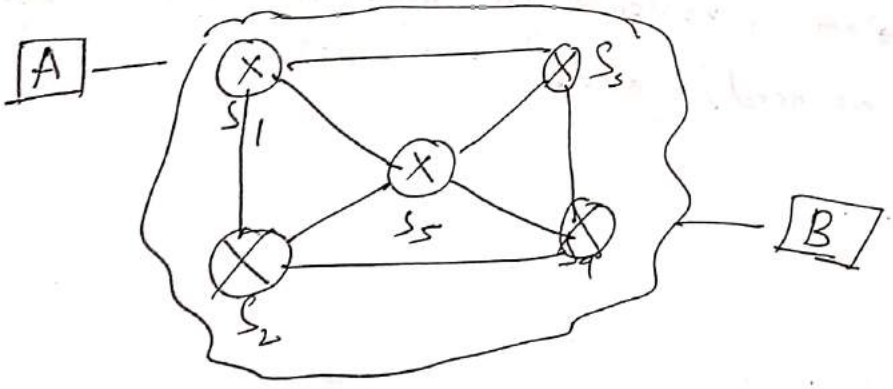
Distance / Velocity

⊖ We cant use this in gmail, whatsapp etc as its efficiency less.

Packet Switching :⇒ • Works on data link & Network Layer.

- There is different switches in network which use store & forward system (in buffer)
- Efficiency is high (as no direct communication is established)
- Delay also high (as there is switch which use buffer to store & forward)
- Pipline used (Partial packet is transmitted

⊕ Data is converted into different packets & transmitted



Total time = n (TT) + PD)

number of switch

Packet Switching is categorized into 2 type

Datagram Switching	virtual circuit
• Connection less	• connection oriented
• No reservation	• Reservation (Routing table)
• out of order	• Same order
• High overhead	• Less overhead
• Packet lost high (Different route)	• Packet lost low
• Delay high	• Delay less
• used in internet	• used in Asynchronous Transfer mode.
• Efficiency high + cost less	• Efficiency Less + cost high

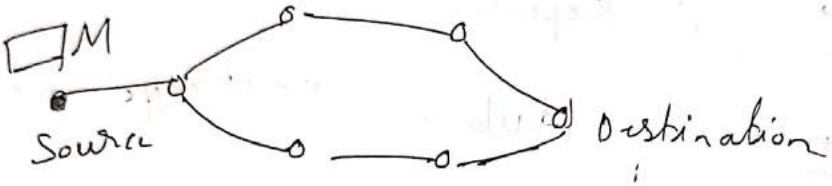
(*) In virtual circuit before sending data packet, a global packet is send to B & it reserves all the switch, buffer in this way so that data packet can follow same path

(*) overload depends on header (ip address, mac etc) In datagram overload is needed but in virtual circuit no need to add.

Message Switching :=> 1960

After circuit switching came then message switching then modified version is Packet switching. CS → MS – PS

- In message switching whole message is send to a hop & then it stored and forwarded to another hop. Finally destination.
- no Reservation



Switch :=> Physical & Data link layer
Layer 2

- multi port bridge. (bridge has only 2 port)
- Full duplex Link (if A send message to B it use a circuit & if B send to A it use other circuit)
- collision is 0
- Traffic is minimum (as it send only data to the destination device according to Mac),

Collison Domain & Broadcast Domain ⇒

Domain means territory / area.

Collison domains means how much data (Message) collide with each other

Broadcast Domain means how many devices got the broadcasted message. (message for all in the network)

Layer	Device	Collison	Broadcast
1	Repeater	no change	no change
1	Hub	no change	no change
2	Bridge	Reduce	no change
2	Switch	Reduce	no change
3	Router	Reduce	Reduce
4	Gateway	Reduce	Reduce

* Repeater & Hub do not use buffer to store & forward so collison same
* Bridge, Switch, Router, Gateway use buffer to store & forward so collison less
* Router has power to determine the broad cast type. (Whether for all or limited to a specific network)

Unicast, broadcast, Multicast :=>

cast – how many devices will get the data

Uni – one to one

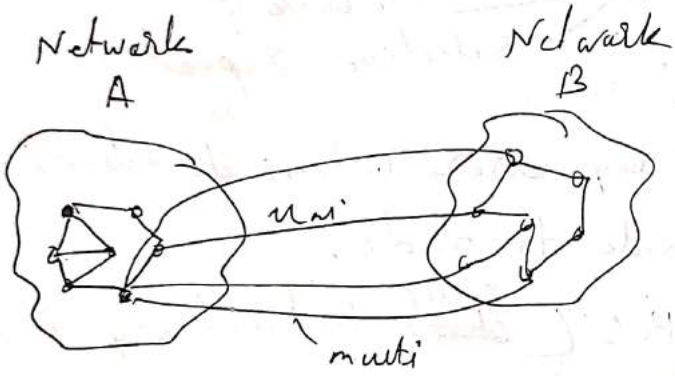
broad – Send to all

Multi – Send to group (more than one)

Broadcast has 2 type :

(i) Limited – Send all devices of same network

(ii) Direct – Send all devices of other network

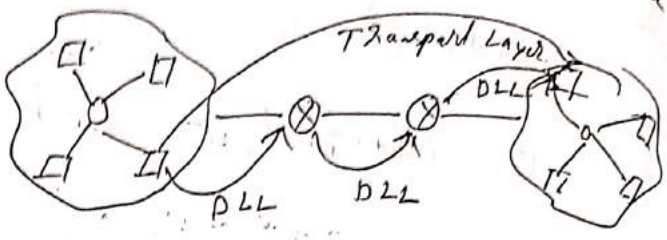


Data Link Layer :=>

Network
Datalink
Physical
Receiving

main function of data link layer is

(i) Hop to Hop / Node to Node delivery of packet (We can transmit data within network with the help of data link itself. But to transfer to different network, we need different Network Layer)



(ii) Flow control :

Speed of sending data to avoid overflow (buffer full & data lost)

We use 3 algo — Stop & wait, Go back N, Selective Repeat

(iii) Error control :

if there occurs any error in time of delivery of packet from node to node.

We use CRC (Cyclic ~~Check~~ Redundancy check)

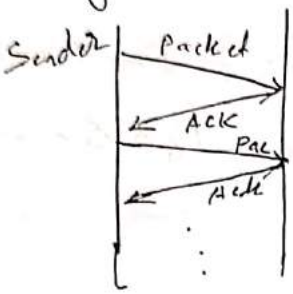
* We also check error in destination but if we check error in node to node then we can mark the error & solve in early stage, so efficiency increase.

(iv) Access controll : When host on shared network tries to transfer data, it has a probability of collison. We use CSMA/CD (Carrier Sense multiple access with collison detection) → Aloha, Token ring to avoid collison.

(v) Framing : Data link layer takes packet from Network Layer and encapsulate into frame. Then it sends each frame bit by bit on the hardware. At receiver end data link layer picks signal from hardware & assemble into frame

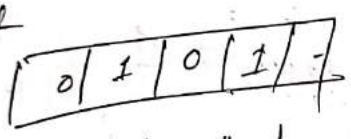
Stop & Wait :=>

- Sender sends data / frame to the receiver & waits until it get acknowledgement of receiving data.

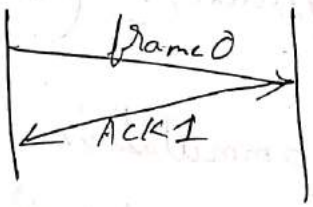


⊗ if acknowledgement is not received then after Timeout we again send the frame.

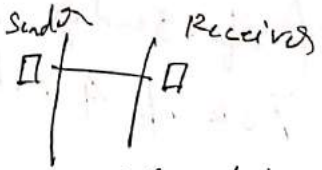
- We use sequence number so that we can determine whether any duplicate packet received or not



⊗ We send Acknowledgement of Next expected frame



- Only 1 frame transmit.
- Sender window = 1
- Receiver window = 1 (in order transmission only)
- Waiting time very High & Efficiency less
- Retransmission = 1



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

$$a = \frac{\text{Propagation delay}}{\text{Transmission time}}$$

$$\left(\frac{\text{transmission time}}{\text{TT} + 2 * \text{PD}_{\text{TO}}}\right)$$

Terms:

Propagation delay: Amount of time taken by a packet to make a physical journey from one router to another router

$$PD = \frac{\text{Distance between routers}}{\text{Velocity of propagation}}$$

Round Trip Time (RTT) = $2 * PD$

Timeout (TO) = $2 * RTT$

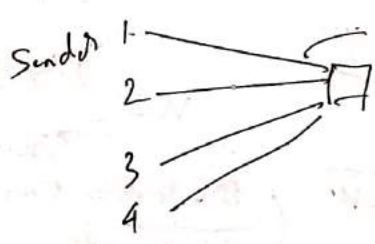
Time To Live (TTL) = $2 *$ Timeout
(Max 180 Second)

Go Back N ⇒

- Multiple frames are transmitted of a window
- Sender Window $2^k - 1$ (k = number of bits required to represent window)
- Receiver Window = 1 (inorder transmission only)
- efficiency = $(2^k - 1) \times \frac{1}{1+2a}$
- Commulative Acknowledgement

(if Sender does not recive Ack of 2 but received Ack of 4 it means 1, 2, 3 is received)

- Retransmission = $2^k - 1$



is lost then we again Retransmit all.

Selective Repeat ⇒

- multiple frames are transmitted of a window
- Sender window size $= 2^{k-1}$
- Receiver window size $= 2^{k-1}$ (out of order is possible as it has complete data)
- Efficiency $= 2^{k-1} * \frac{1}{1+2a}$
- Commulative & independent Acknowledgement
- Retransmission = 1

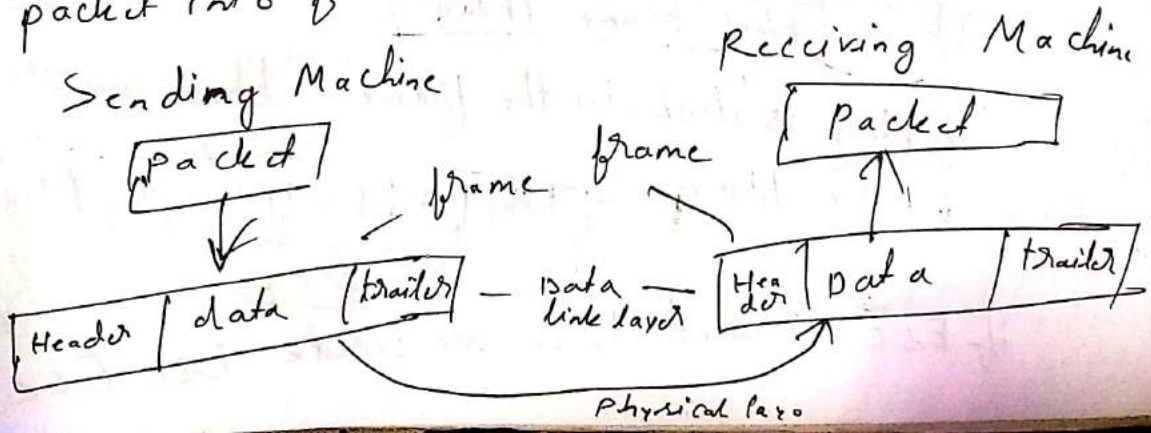
(e) Suppose $k = 3$ bit then Sender window size $= 2^{3-1} = 4$

0	1	2	3

if 1, 2, 3 is received & it does not receive 0 then in order to receive from 0 it send NAK 0 (Negative Acknowledgement). Thus waiting Time is less)

Framing in Data link Layer ⇒

To transmit the data between connected device we use framing. primary function of data link Layer is to split packet into frame.



In a frame there is

Flag — marks beginning & ending of the frame

Header — Source & destination address

Payload field — data / message delivered

Trailer — error detection and error correction bits

Types :=>

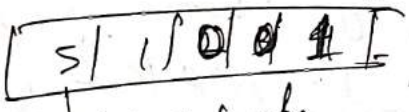
(i) Fixed Size : frame has fixed size.

no need to define boundaries ex — ATM Cells

Drawback — internal fragmentation solution — Padding

(ii) Variable size : no fixed frame size

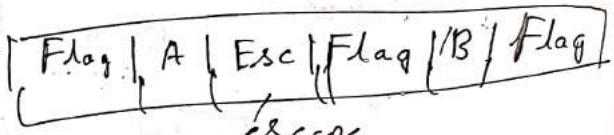
(a) Length Field : (Byte count) length of data is maintained, used in Ethernet frame



(b) End delimeter : a pattern is used as a delimeter to determine beginning & end of the frame

Byte stuffing : Flag byte is added as beginning & end of the frame data.

if flag is itself in the frame then we use Esc before flag —



if Esc is used then we write Esc Esc

* Bit stuffing: if it encounter the flag pattern in data it automatically stuff a bit in between Later at receiver end it is deleted.

ex- in HDLC (High level data link control)
01111111 is used as flag So for every consecutive 5 1s it add 0
→ 01111101
Stuffed.

Error detection & correction :⇒

if sender send the data & receiver receives different data then there is error

Sender: 011. → 001 receive (error)

There is 2 type of error
(i) Single bit error
(ii) Burst error (more than one bit is wrong)

Length of error is bits between two error bit including both 1011 — 1001
length = 4

Detection:
(i) Single parity (Even, odd)
(ii) 2D parity check
(iii) checksum (in transport layer)
(iv) CRC (Cyclic Redundancy check) (in datalink layer)

Correction:
* Hamming Code

Single Parity :⇒ Parity means number of 1 message bit
(Vertical Redundancy check)

- Total bits Send: $m+1$
- mainly even parity is used (number of 1 is even in the frame)
- Least expansive (as we only Send one bit extra)
- Can detect single bit error or odd number of bit error
- Can not detect even number of bit error

ex - Like in 4 bit data

	parity bit
0000	0
0010	1 — as number of 1s is 1 then to make even we add 1
1101	1 — number of 1s is 3 So we add one 1
1110	0 — number of 1s is 4 So we will add 0 as it is even already.

Hamming distance is number of bits different we can get by XOR operation

```
 0000
 0011
------
 0011   distance 2
```

Minimum Haming distance in single Parity is 2

```
 00000
 00101
-------
 00101
```

Cyclic Redundancy check (CRC) =>

error detection method based on binary division. (Most widely used method)

- total bit $(n+r)$ → reduded bit appended
- Can detect all single bit error
- can detect odd number of error if divisor is factor of $(X+1)$
- detect all double bit error if it contain at least three 1's in divisor
- detect burst error of length equal to polynomial degree

(*) if CRC generator polynomial is $X^4 + X^3 + 1$ then its binary equivalent will be $1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x^1 + 1 \cdot x^0$

Max degree

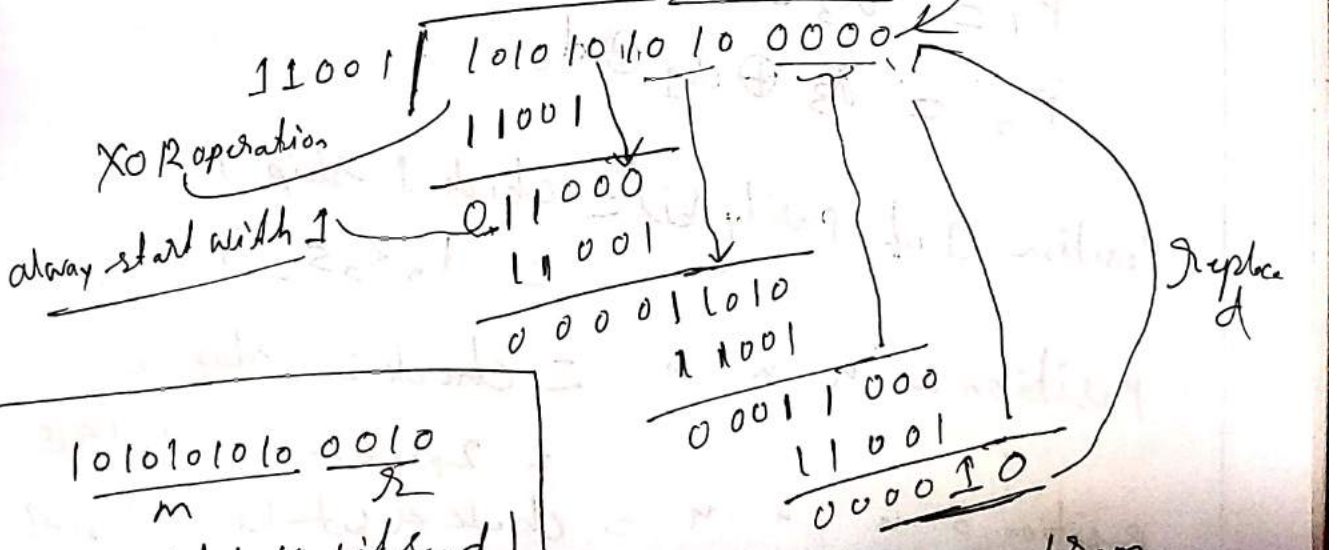
$\downarrow$

$1\ 1\ 0\ 0\ 1$ (divisor bit = 5)

total number of bits append with data = 4

Suppose- Data is 1010101010

We have to perform binary division



$\frac{1010101010}{m}\ \frac{0010}{r}$

(total 14 bit send)

Receiver Receives the 14 bit frame & will do the same if the Remainder is 0 then no error occured

```
10001 | 10101010100010
```

Hamming code For Detection & Correction :⇒

Set of error correction code for detecting error & correction purpose

Total number of frames bits $N = M + R$

M for data, R redundant bit

R will be such that

$$2^R \geq M + R + 1$$

if total bit 7 then $M = 4$ $R = 3$

bit is 13 then $M = 8$ $R = 4$

position –	7	6	5	4	3	2	1
bit –	d_3	d_2	d_1	P_2	d_0	P_1	P_0

$P_2 = d_1 \oplus d_2 \oplus d_3$

$P_1 = d_3 \oplus d_2 \oplus d_0$

$P_0 = d_3 \oplus d_1 \oplus d_0$

Position 1 of parity bit = check 1 skip 1

= 1, 3, 5, 7 ...

Position 2 " " " = check 2 skip 2

= 2, 3, 6, 7, 10, 11, 14, 15

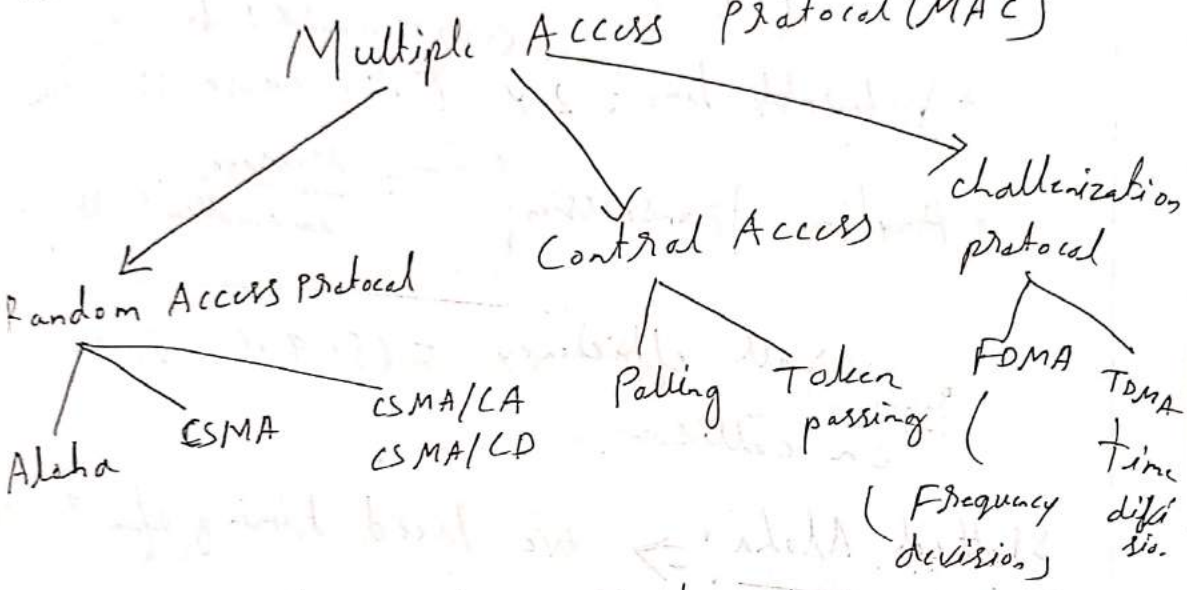
Position 3 " " " = check 4 bit then skip 4

= 4, 5, 6, 7, 12, 13, 14, 15

⊛ Data link layer has two sublayer

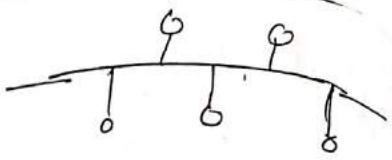
(i) Logical link control (LLC): It deals with protocols flow control, error control

(ii) Media/ access control (MAC): It deals with actual control of Media through multiple common link



⊛ MAC is not possible in Mesh but possible in bus as bus topology multiple devices try to send data on single link.

Pure Aloha :=>



- Random Access protocol
- Collison possible as randomly devices send data in link
- Acknowledgement needed
- LAN based
- Only transmission time
- No propagation time (Router – Router) (Fiber transmit 41 km/sec)
- Vulnerable time = 2 × TT (Transmission time)
- Anytime transmission

$$TT = \frac{\text{Message}}{\text{Bandwidth}}$$

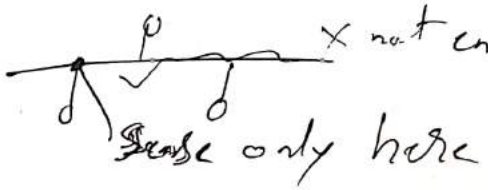
- overall efficiency = 18.9 % Restart on collison.

Slotted Aloha :=> We fixed timing of transmission by some slot

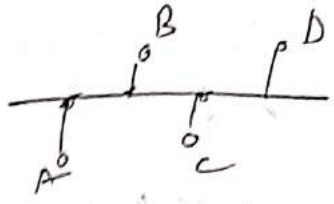
- Vunerable time = TT (Transmission time)
- overall efficiency = 36.8 %.

Carrier Sensor Multiple Access (CSMA) :=>

- Before transmission a node check the carrier (linkcable).
- it does not check whole channel it just sense its area



CSMA
- 1 persistant
- 0 persistant
- P-persistant



1 persistant: Continuously check whether any data is being sent. If no data is transmitting then the device will send the data to link

Disad → if A is sending to D & stop. B, C check and realize no data is being transmitted then both will send & collison happen

. used in Ethernet

Checking in our house front car/bike

0 persistant: check after random amount of time. collison is less

Disadv → too much waiting time (if link is free & no one is sending

P persistant: — continuously check but immediately it will not transmit data. It will transmit according to probability

. used in wifi

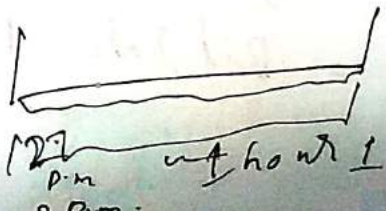
CSMA/CD ⇒ Collison detection

We dont use Ack as it will make collison more

We detect collison by the help of collison signal if $TT \geq 2 * PD$

or $\frac{L}{BW} \geq 2 * PD$ (L - message length)

or $L \geq 2 * PD * BW$



if data sending last greater than $2 * P_D$ then we can get the collison signal else we cant

CSMA/CA :=> Collison avaidance

three strategy —

(i) Inter frame space (IFS): When a station find channel busy, it wait for a period of time

(ii) Contention Windos :— amount of time divided into slots

(iii) Acknowledge :— Positive Acknowledgement and time out timer can help guarantee transmition.

Ethernet: used in data link 1983
LAN protocol.

- use CSMA/CD

10 Base 2 — Thin ethernet

10 Base 5 — Thick

100 Base Fx — Fast

10G Base Y — gigabit

Topology — Bus*, star

- Bit rate 1 Mbits/s — 400 Gbits/sec

Structure

Destination Address

Preamble 7B	SFD 1B	DA 6B	SA 6B	Length 2B	Data 46-1500B	CRC 4B

Physical layer add for alerting Receiver that data is coming

Source Address

SA	DA
S	X address

Physical address

Minimum frame size - 72B

Maximum frame size = 1526

Token Ring

- Ring Topology is used
- Access control method used is token passing (Who will get the power to send)
- Unidirectional
- Data rate used is 4 Mbps, 16 Mbps
- Piggybacking Acknowledgement is used (Ack send with Data)
- Differential manchester encoding used
- Variable size framing
- Monitor station is used.

SD	AC	ED

total – 3 byte (token)

Start delimiter, Acknowledgement, End delimiter

Polling :⇒ Controller grant access to the station to send data giving its address to all station (device)

too much overhead & high dependency on controller.

FDMA :⇒ Frequency Division multiple Access

- overall bandwidth is shared among number of station

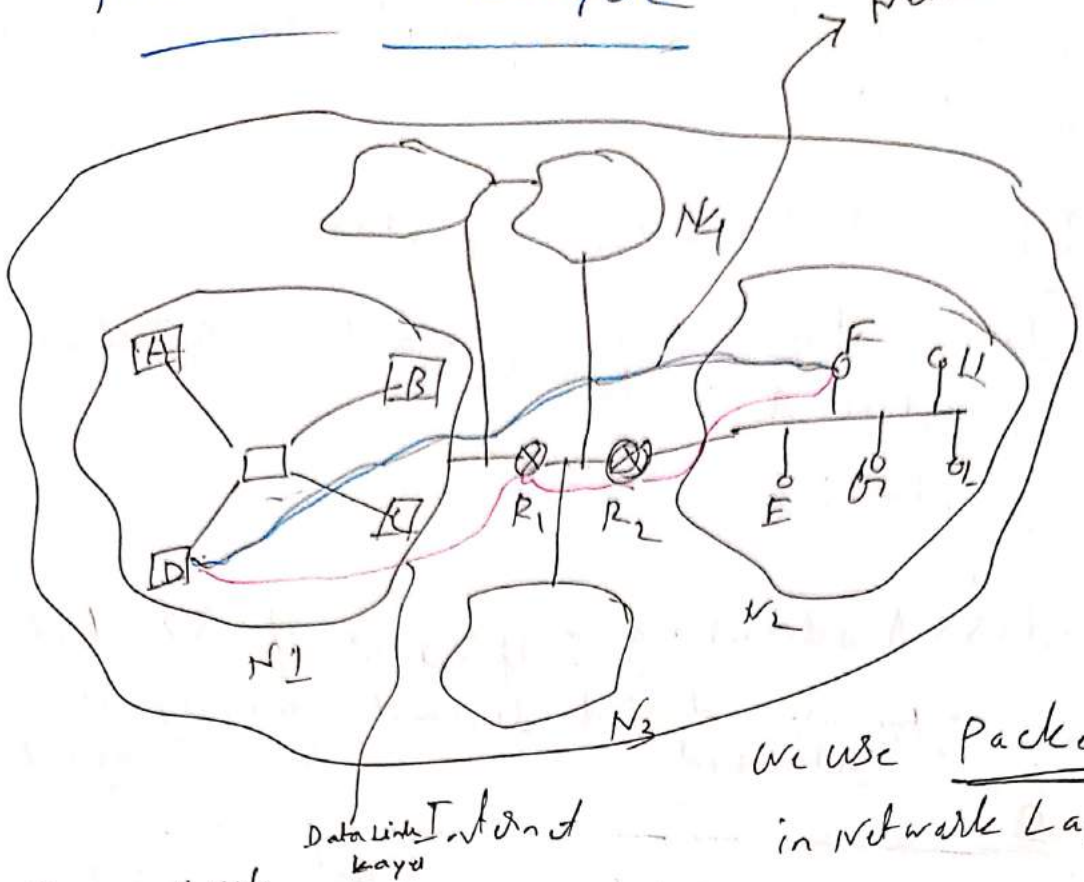
guard band needed for adjacent channel

TDMA :⇒ Time division Multiple Access

Time slot given to each station for transmit.

- guard time between adjacent slot is necessary.

Network Layer



We use Packet in Network Layer.

Responsibility

(i) Host to host / source - destination / Machine to Machine → a device of a network is connected to a device of other network

(ii) It uses Logical address for transferring data which is called Internet protocol address (Connection less)
- Network ID (Which network)
- Host ID (Which machine in that network)

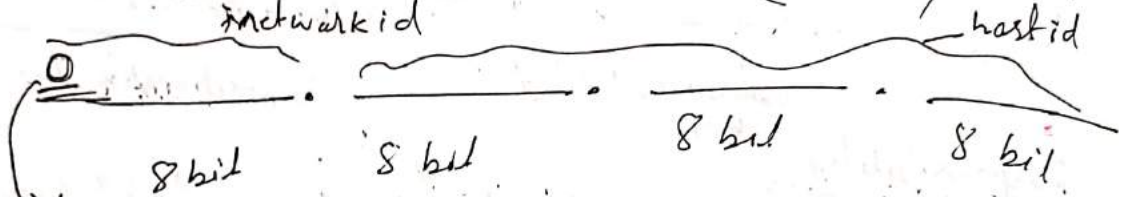
(iii) Routing → deciding path to arrive at the destination (nearest Router)

(iv) Fragmentation :- if any Router has limited buffer So we have to send packet into frames.

(v) Congestion control :- Controlling the capacity of a network. (how many packet come in a network at a time)

IP addressing :⇒ Ip address is classified into 5 type
(i) class A (ii) class B (iii) class C (iv) class D
(v) class E

Class A addressing : ipv4 is of 32 bits
- we use dotted decimal (widely used



→ fixed (first bit is fixed to determine that it is a class A ip address

- Total ip address is possible $= 2^{31}$
- The first 8 bits represent Network Ip
- The other 24 bits represent Host ID of that network
- Total number of networks $= 2^7 = 128 - 2 = 126$
  (The first & last address is not use as ip address)
- Total number of Hosts in every network $= 2^{24} - 2$

(Suppose network id of google 64.
64.000.0 ——— represent whole network
64.255.255.255 — broadcast address
(send packet to every host)

- Range of network id = 0 – 127

(X) ip address = 64.0.0.8

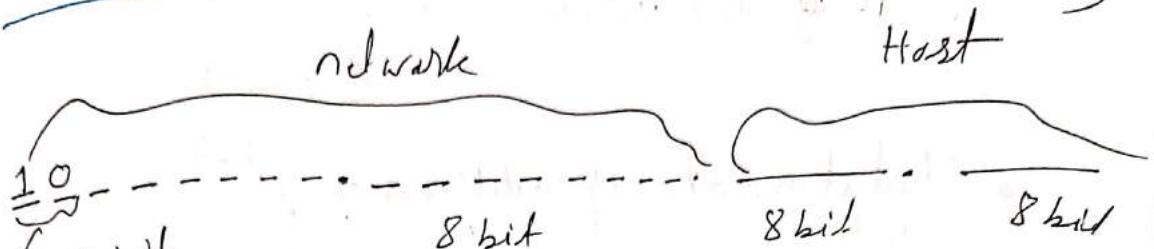
Default mask = 255.0.0.0 and operation

network address = 64.0.0.8 & 255.0.0.0

= 64.0.0.0

Class B addressing

- total 32 bit (8bit x4)



→ fixed prefix (helps to recognize that it is class B)

10000000 (128)
10 000001 (129)
10 000010
...
10 111111 (191)

- Range of network in first octate → 128 – 191 (total 64)
- Total no of ip address = 2^{30}
- Total no of networks = 2^{14} = 16384
- Total no of host in a network

= 2^{16} = 65536 – 2

= 65534

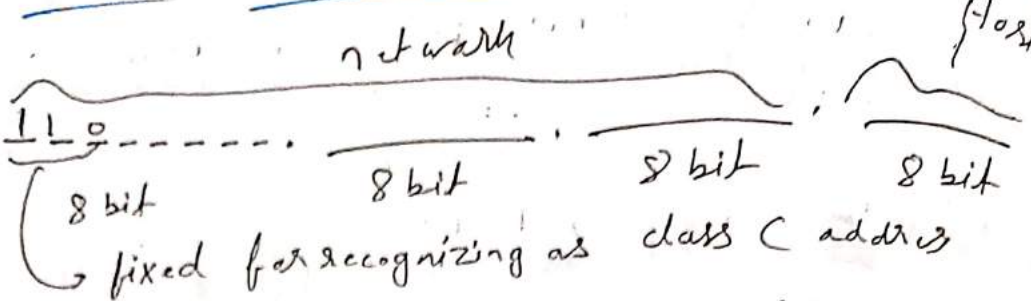
(0.0 - represent whole network, 255.255 - broadcast address } excluded)

(X) ip address 130.2.3.4

Mask address = 255.255.0.0

∴ Network address = 130.2.0.0

Class C addressing:

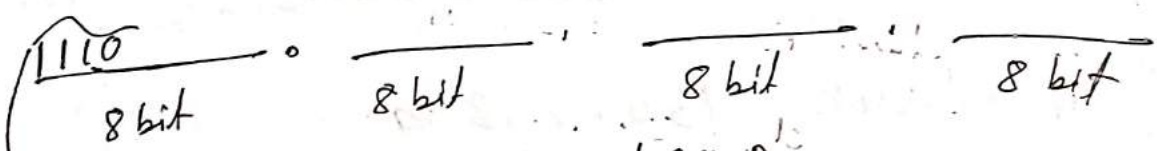


8 bit
↳ fixed for recognizing as class C addrs

- Range of 1st octate = 192 – 223 (32)
- Total no of ip addresses = 2^{29}
- Total no of networks = 2^{21}
- Total no of hosts in a network = $2^8 = 256 - 2$ (0 – network address, 255 – broadcast address excluded) = 254

(X) ip address 194.2.3.4
Mask addrss 255.255.255.0
network address - 194.2.3.0

Class D :⇒



↳ fixed for recognizing class D

- Range of first octate - 224 – 239 (16)
- Total no of ip address = 2^{28}
- Total no of networks & host not possible

as this address is not given to common people.

- This addresses used for Multicasting, group email or broadcast

Dis → too much waste of ip address

class E:

1111 . ____ . ____ . ____

→ Reserved for Recognizing class D

- Range of first octate = 240-255 (16)
- Total no of ip address = 2^{28}
- All ip address is reserved for military purpose.

Dis → too much wastage.

Q) ip address = 201.20.30.40

⇒ As 201 is in between 193 & 223 So it is a class C ip address

∴ Network id = 201.20.30.0

4th host id = 201.20.30.4 (as 0 is not any host)

Last host id = 201.20.30.254

Broadcast address → Limited (Send broadcast in own network)

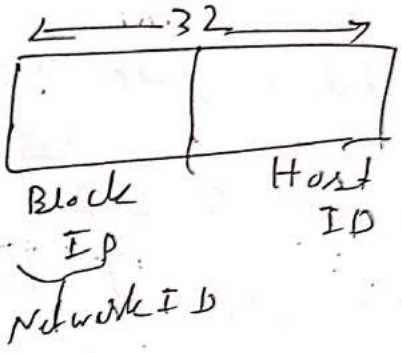
Direct → 201.20.30.255

Disadvantage of classful addressing.

- Wastage of ip address (Cl A - 1 crore, Cl B - 65k, Cl C = 256)
- Maintenance is time consuming
- More prone to error

Classless Addressing (1993) => (CIDR)

- No concept of classes
- We will use only blocks

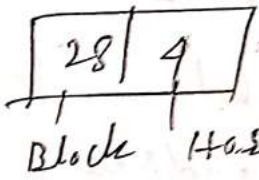


- Notation

X.Y.Z.W / n (n = mask call it / no of bits representing block internally)

ex — 200.10.20.40/28

it means



- No of hosts = 2^{32-n} (Here 2^4)

- 200.10.20.00101000
  & 255.255.255.11110000 — mask address
  200.10.20.00100000

= 200.10.20.32/28 — Network id

Rules — (i) address should be contiguous

(ii) No of address in a block must be in power of 2

(iii) First address of every block must be evenly divisible with size of block

---

Subnetting :=> Dividing the big networks into small network

- we use for securing whole network & lower the maintenance.

Subnetting in classful :=> network ID

- Suppose ip address = 200.10.20.0 (class C address)
- there can be possible 254 host. (256-2 excluded)
- Now if we want to subnet we should not change network id but will use last octate (Host id)
- We reserve 1st bit of host & it will divided into two part

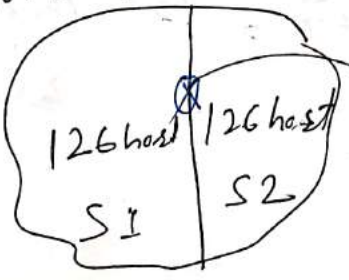
(i) 200.10.20.0 _ _ _ _ _ _ _ _

=> 200.10.20.0 → 200.10.20.127

subnet id — direct broadcast id

(ii) 200.10.20.1 _ _ _ _ _ _ _

=> 200.10.20.128 — 200.10.20 — 255



Subnet mask (number of bits in network)

= 255.255.255.128

Dis → computation is higher (as there we also calculate in which subnet the packet should go).

Subnetting in classless :: ⇒ (Subnetting in CIDR)

host/network

Suppose IP address is = 195.10.20.128/26

26	6	Host bit

network bit

195.10.20.10000000

26

to subnet in 2 part we will reserve 1 bit MSB

(i) 195.10.20.10 0 00000

⇒ 195.10.20.128 → 195.10.20.159

no of host = 32 but useful - 30

195.10.20.128/27 (subnet id) . 195.10.20.159/27 (broadcast id)

(ii) 195.10.20.10 1 00000

⇒ 195.10.20.160 → 195.10.20.191

no of hos = 32 but useful 30

195.10.20.160/27 → 195.10.20.191/27

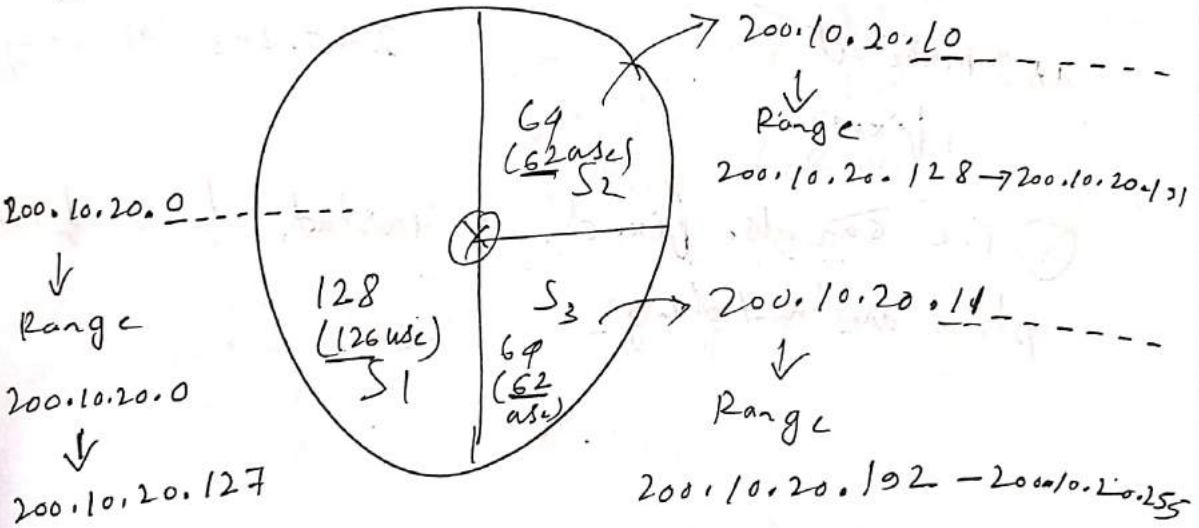
subnet id → broadcast id

Variable length Subnetting mask (VLSM)

To achieve flexibility we want to create subnets of ~~var~~ different range.
earlier we were doing same range subnet

VLSM in classful addressing:

network ip address = 200.10.20.0
it is class C address means first 24 bit is of network
. Total number of host = $2^8 = 256$ out of which 254 is useful



Subnet mask for S1 - 255.255.255.128
" " " S2&S3 - 255.255.255.192

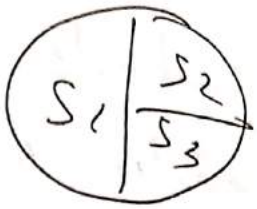
VLSM in classless (CIDR)

ip address - 245.248.128/20

So we can say -

20	12

network bit | Host bit



network bit

Host

245.248.1000 0000.0000000

Reserved

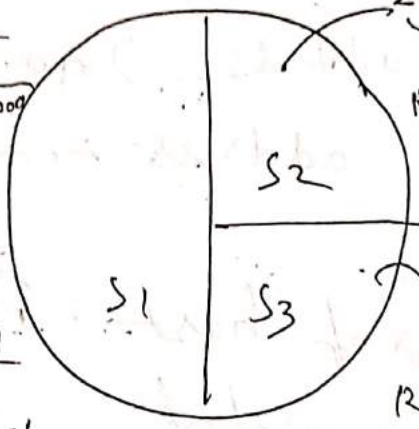
Range will be

245.248.128.0/21

to

245.248.135.255/21

as 1 more bit fixed



245.248.1000 10 .....

Reserved

Range - 245.248.136.0/22 to 245.248.139.255/22

245.248.1000 11 .....

Reserved

Range →

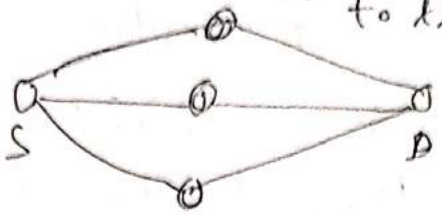
245.248.140.0 to /22

245.248.143.255/22

(*) We can also fixed 1 instead of 0 if no option are matching..

IPV4 Header :⇒ Internet Protocol Version 4

- Connection less (no connection established)
- Datagram Service (any route can be followed to transfer packet)



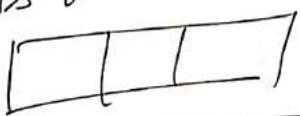
- Datagram — Header size 20–60 byte (min header size)
  - Payload = 0 – 65515 Byte (data)

. Header say where to data send, how to data send & any error check (like overlaps)

- in Header there is
  - source ip (4 byte)
  - destination ip (4 byte)
  - Protocal (1 byte)
  - Header checksum (2 byte)
  - TTL (Time to live) (1 byte) — how many switch it can traverse, always decrement by 1 after each traverse
  - Flag etc.

Fragmentation in IP v4 :⇒

Datagram is divided into fragments



identification bit 16 bit	Flag 3 bit	Fragment offset 13 bit

Flag: RS | DF | MF
- 0 0 — Do not fragment
- 0 1 — Flag
- 1 0
- 1 1 — Fragment

Option / padding in IPV4 :⇒ S → x → x → x → D

- For recording Route → Strict source routing
  Loose source routing
- Padding – IPV4 header is multiple of 4. If header size is 23 bit then we will add 1 byte extra pad. Then it will be 24

IPV6 Header :⇒ IPV4 was of 32 bits but now IPV6 is of 128 bit

total ip address possible $= 2^{128}$

in IPV6 there is

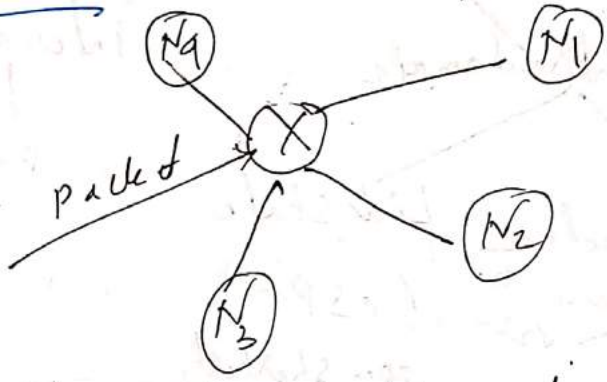
(i) version (4 bit)
(ii) priority (8 bit)
(iii) Source address (128 bit)
(iv) Distination address (128 bit)
(v) Hop limit

Base Header (min size) = 40 byte (320 bit)

Routing Protocol ⇒

. Routing is a process in which the layer 3 devices (router or layer 3 switches) find the optimal path to deliver a packet from one network to another.

. Routing protocol are the set of defined rules used by routers to communicate between source & destination. They do not move information from source–destination but only update routing table that contains the information.



Routing table has cost, metrics hop count

There is mainly two type of routing protocol

(i) Static (ii) Dynamic

(i) Static: Admin manually assign path from source to destination

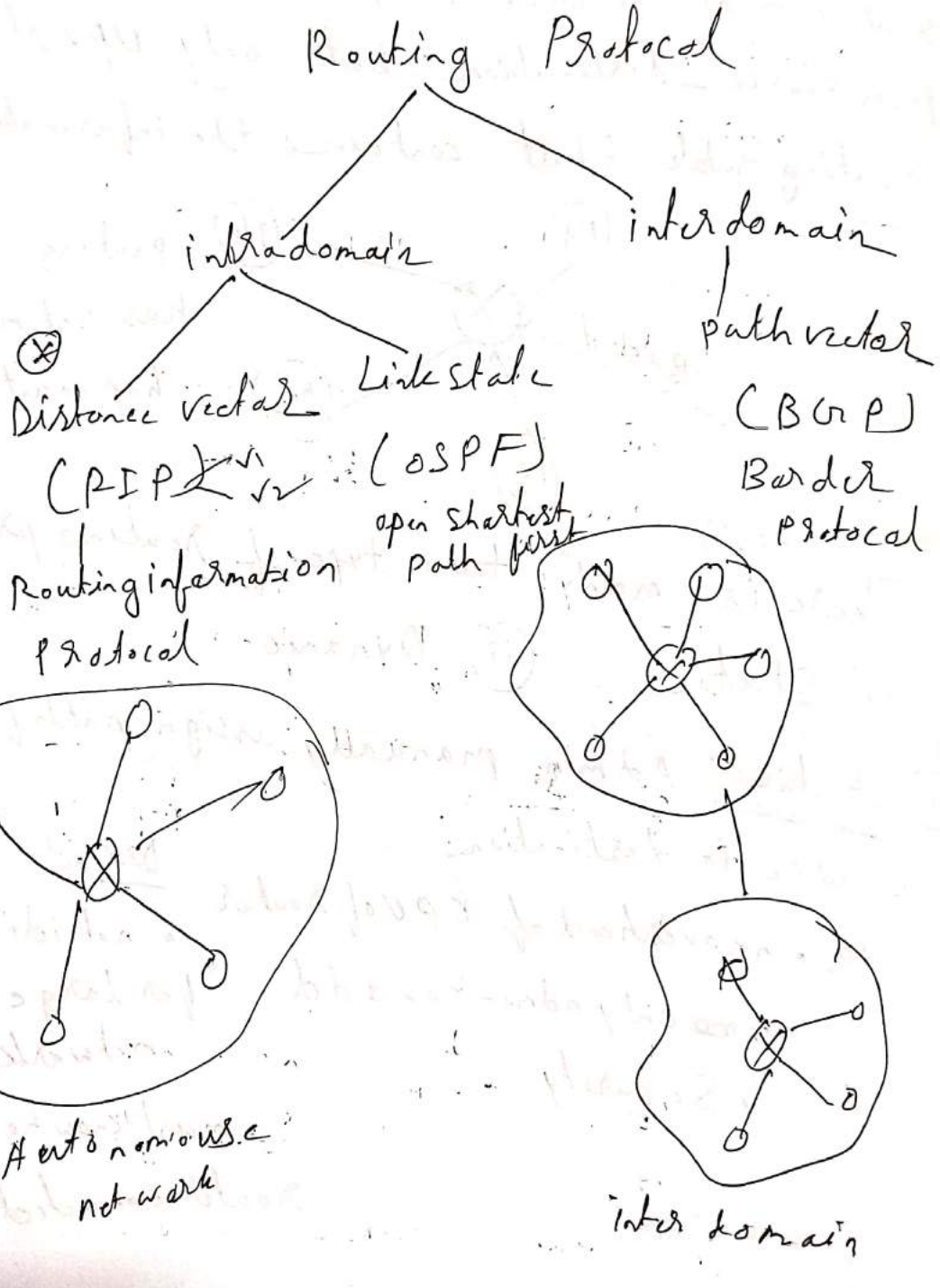
adv
. no overhead of CPU of router
. only admin can add
. Security

Disadvan
. not ideal for large network
. must know how router connected.

(ii) Dynamic :- routers add information automatically on routing table.

Adv –
- easier to configure on large network
- load balancing between multiple links

Dis. – - additional load on router CPU
- updates are shared between routers

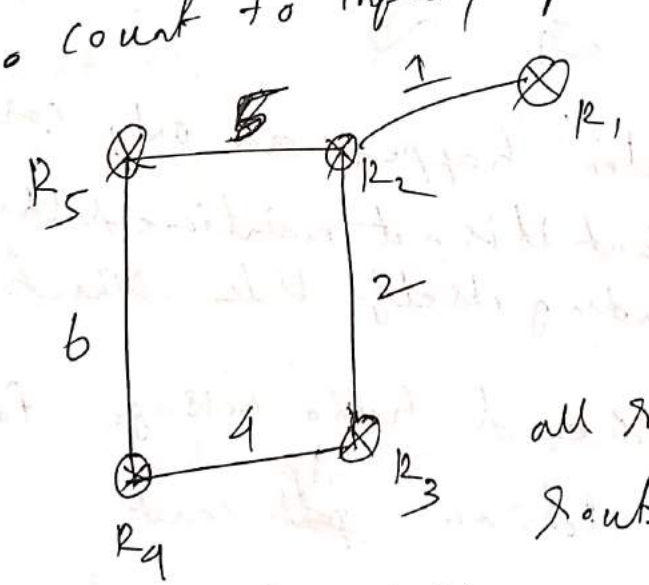


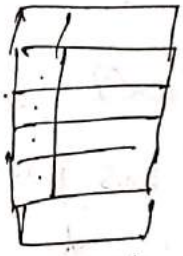
Distance Vector Routing (DVR)

Select the best path on the basis of hop count to reach destination. The path with the least hop will be choosen as the best path.

- It uses hop count / distance as the metric value which is shared between the neighbouring routers.
- updates of the network are exchanged periodically.
- routing table distance value is shared only with the neighbours
- Routers always trust information of its neighbours

Dis ⇒ • Unneccessary traffic occur & bandwidth wasted for sharing routing table
- Security issue
- count to infinity problem occured





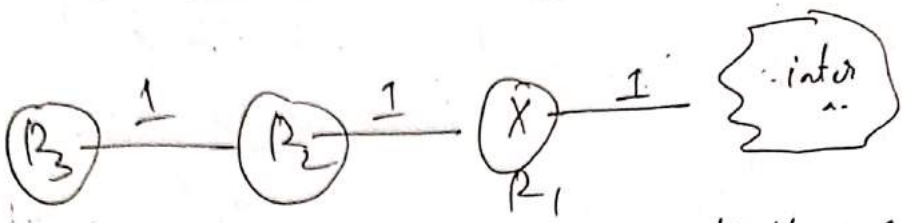
routing table

all routers has routing table

Frequently routing table is exchanged between neighbour if any link broken then

it choose other optimal path

Count to infinity problem :-



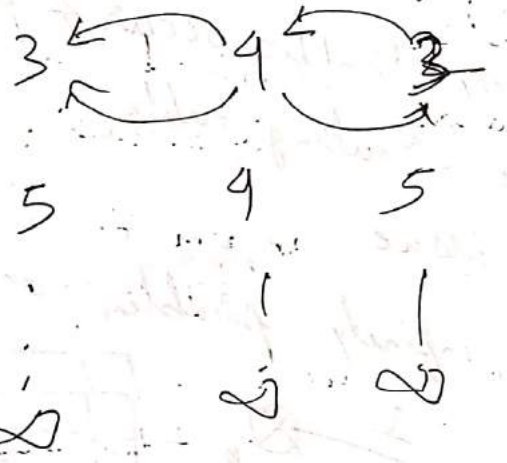
∞ ∞ 1 initially cost / hop count

∞ 2 1 } after interchanging routing table.

3 2 1 } metric (cost)

if link broken

it send ∞ to R_2 but R_2 also get 3 from R_3 So it update to 3+1

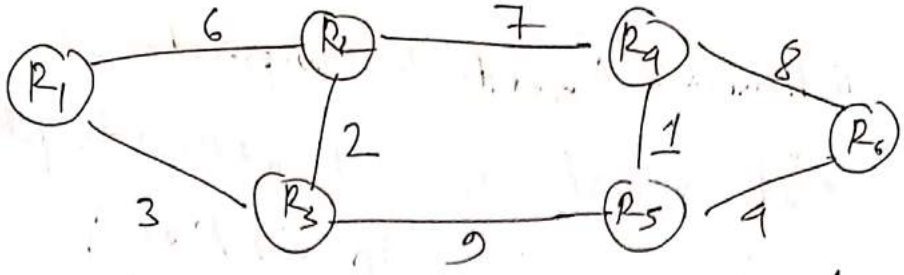


This problem happen as only cost metric is send but it is not maintained that it is taking route including itself link which is broken.

(*) Router send hello message to neighbour router to determine ~~path~~ hop count

Ex- Routing information protocol

Link State Routing :⇒



- every router has link state table which has neighbour distance. Then it is flooded to all router
- Hello message used for neighbour discovery
- concept of triggered update
- only that update are shared that needed by neighbour

It maintain 3 table

(i) neighbour table → neighbour of router information

(ii) Topology table → information about whole topology (contain both best & backup route.

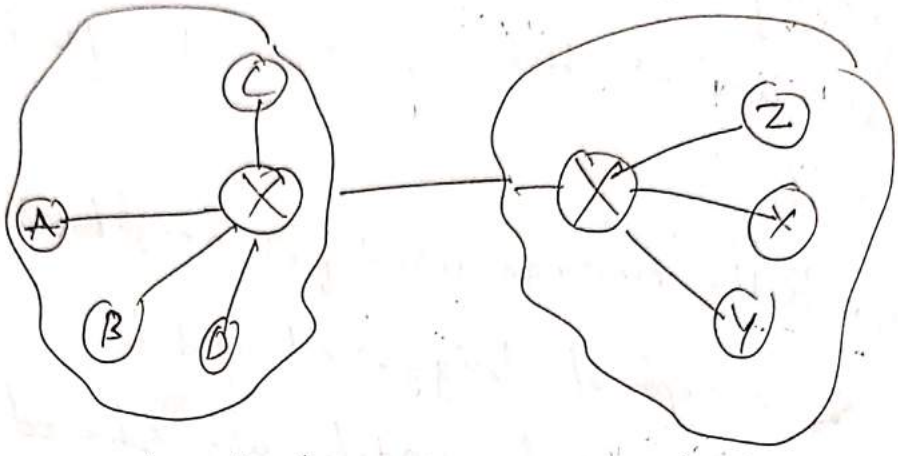
(iii) Routing table → all the best route

Adv
- contain backup route
- concept of triggered update
- use of less bandwidth

ex- Shortest Path first

Address Resolution protocol (ARP)

- Layer 3 (network) protocol
- It convert logical address to physical address (ip → Mac)



Network 1

IP_S	MAC_S	IP_{R2}	MAC_{R2}

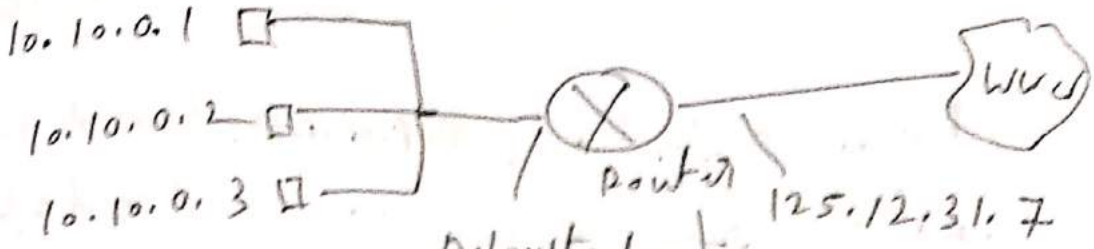
if we does not know MAC of receiving we simply broadcast it with FFFFFF

FFFFFF

48 bit MAC address

Network Address Translation (NAT) :=>

- it translate private ip → public ip
  public ip → private ip
- Range of private ips in ipv4
  - 10.0.0.0 → 10.255.255.255 2^{24}
  - 172.16.0.0 → 172.31.255.255 2^{20}
  - 192.168.0.0 → 192.168.255.255 2^{16}



NAT translation table

Private	Public
10.10.0.2	

Transport Layer ⇒

Responsibilities :-

(i) End to End (port to port) :- Like in chrome there is different tab opened from which tab it requested, it will get response. Different application has different request. Port no given by OS

(ii) Reliability & inorder delivery : We use different protocol (TCP) which ensure reliability (all message will be must received in receiver) : inorder delivery (same order message will be soon. No Loss of data.

- UDP does not give Reliability
- TCP first make connection Then send data

(iii) Error control :- TCP use checksum for error detection

(iv) Congestion control ⇒ AIMD is used

(v) Flow control :→ Receiver send its capacity of message size to sender we use Stop & wait, Gobackn, selective Repeat

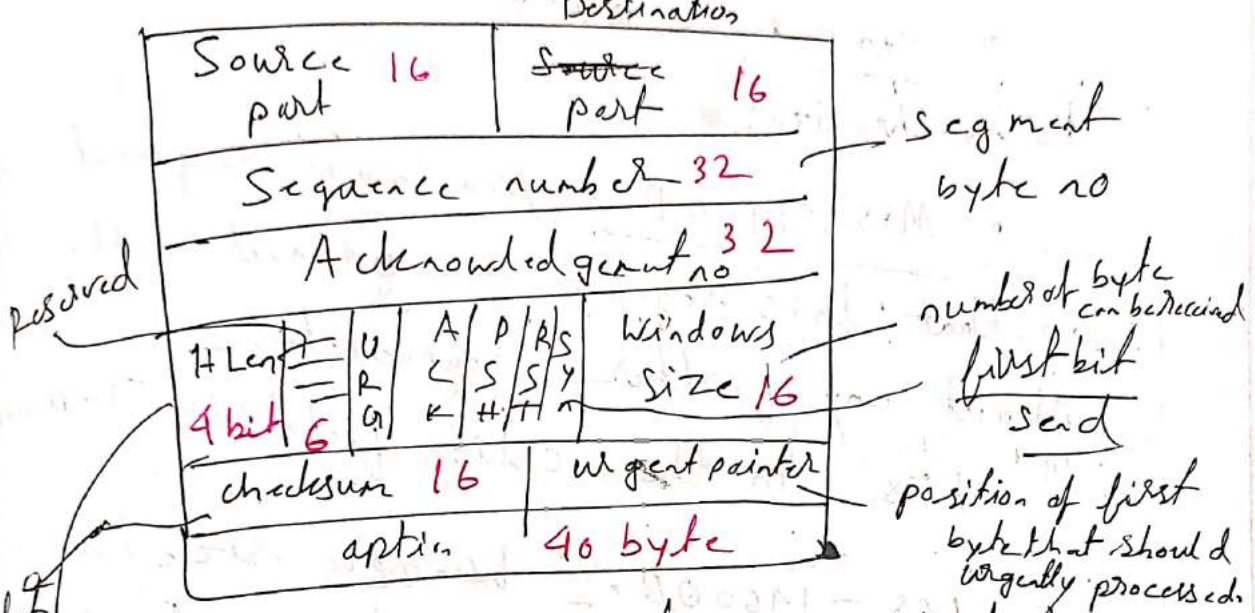
(*) From application layer messages come in form of bit continuously. We make (collection of byte) Segment with header with help of TCP, UDP & send to network Layer.

(vi) multiplexing / demultiplexing :⇒ multiple application are sending data to transport layer, it then multiplex it & send to the channel.
on receiver end different messages are demultiplexed.

TCP (Transmission control Protocol)

- used in transport layer
- it is Byte Streaming (a lot of bits come from application layer came & TCP convert into segment in which there is lot of Bytes)
- Connection oriented (3 way handshaking
  (i) make connection
  (ii) Acknowledge
  (iii) Send data)

- Full duplex (S ⟷ R)
- Piggybacking (We can send data along with Acknowledgement)
- Error control (checksum is used
- Flow control (to maintain the capacity of
- Congestion control Receiver properly)



TCP Header (20 - 60 Byte)

Min

if 15 then header is 15 × 4 = 60

8 → 32 byte Scale of 4

- There is 6 single bit flag

(i) URG :- Payload data must be processed immediately

(ii) ACK :- Receipt of TCP packet.

(iii) PSH :- Push flag ensure TCP segment immediately pushed without sending to buffer

(iv) RST :- if there is error in transmission, A TCP packet with RST set (1) can reset the connection.

(v) Syn :- initiating the connection. (first step of 3 way connection)

(vi) Fin :- Sender is ending the transmission.

TCP Connection Establish :=>

- It is called 3 way Connection Establishment

1. Sender start the process with the following

- Seq = 521 : contain random initial sequence generated in sender side
- Syn = 1 : => Requested the receiver to synchronize.
- MSS = 1460 B : Maximum segment size so that this segment can travel in the network without any further segmentation.

it is in the option field in TCP header.

- WS = 14600 B :- Window size / sender tells about its buffer capacity in which he has to store message from receiver

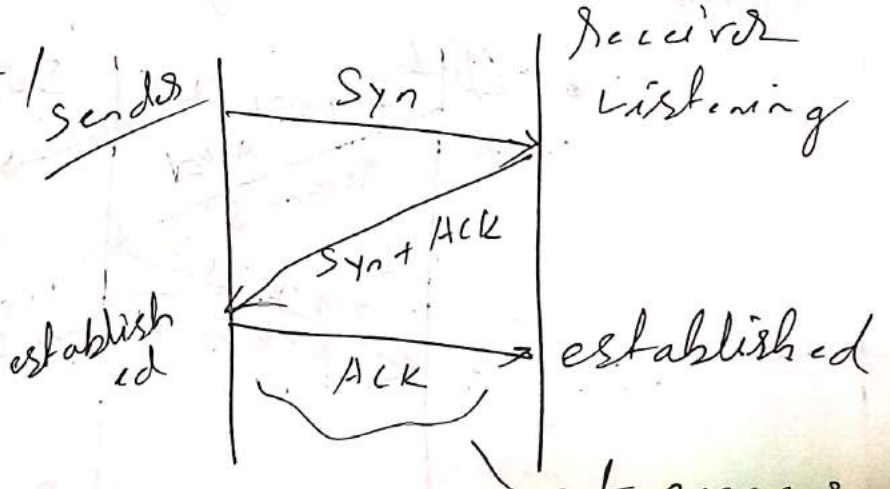
2. TCP is full duplex protocol so both Sender & Receiver require a window for receiving messages from one another.

- Seq = 2000 : contains the random initial sequence number generated at the receiver side
- Syn = 1 : Request the Sender to synchronize its Sequest number.

- MSS = 500 B: Sender tells its maximum segment size, so that receiver send datagram which won't require any fragmentation.
- WS = 10000 B: Window size / Receiver tells about his buffer capacity in which he has to store messages from the sender.
- Ack no = 522: Ack no is always be the next sequence no. Sender is acknowledging SYN = 1 packet from the receiver with sequence number 521.
- Ack = 1 — Ack no field contain next sequence expected by receiver

3. Sender makes the final reply for connection establishment

- Seq = 522
- Ack no = 2001
- Ack = 1 sends



TCP Data Transfer :⇒

TCP data transfer is full duplex

it uses

(i) Piggy backing :⇒ We send acknowledgement while we in time of transferring the data.

Data + Acknowledgement = Piggy backing

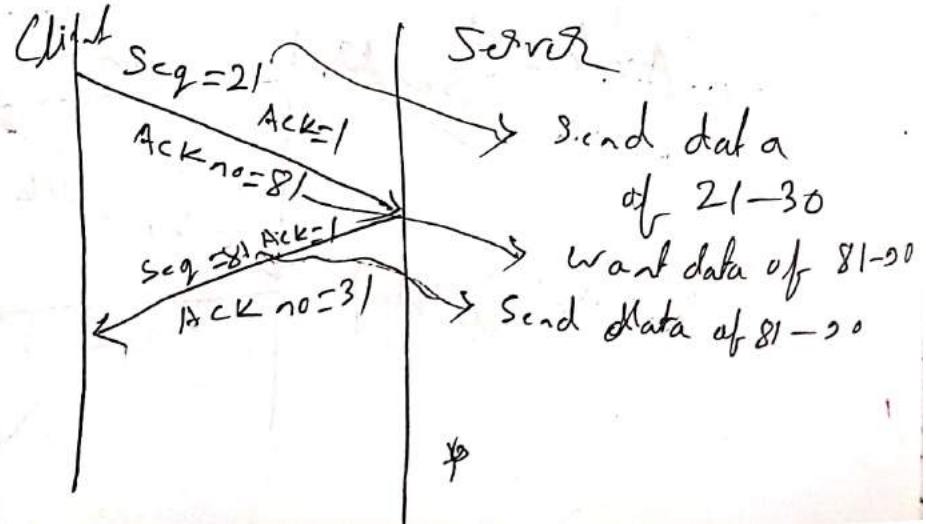
adv → Network load reduce.

(if we send differently one by one it will enhance the network traffic.)

(ii) Pure Acknowledgement :⇒ When data & acknowledgement is ~~sent~~ sent in a differently.

- When there is no data to be sent then we send only acknowledgement

ex- We wait for payment gateway acknowledgement while submitting otp.



TCP Connection Terminator

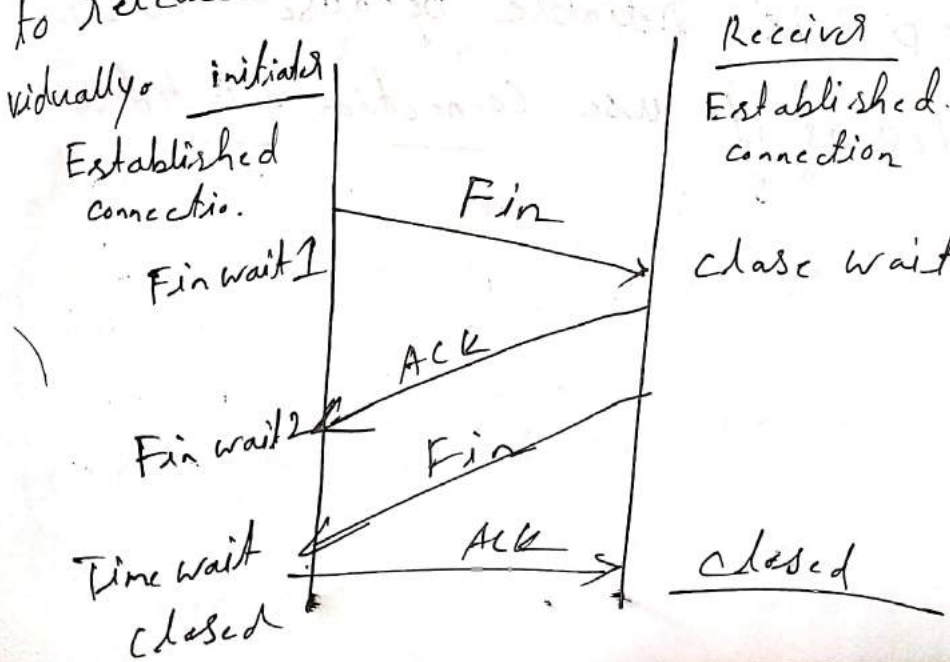
. Fin : The finish flag signals to the other party that a sender is ending the transmission.

TCP support two type of connection release

(i) Abrupt connection release
(ii) Graceful connection release

(i) Abrupt :⇒ When both client & server forced to close the connection.
. It is done by RST flag set(1)
⊗ When non Syn segment receipt
⊗ When a segment with an invalid header is received.

(ii) Graceful :⇒ it is done by using the TCP header's Fin flag. it allows each host to release its own side of the connection individually.



- When client decides to close the connection it send (server) Fin bit set to 1 and Sender enter in Finwait_1 state

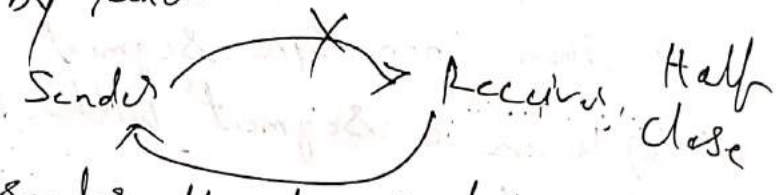
- After getting Ack From server of receiving Fin Sender entered in Fin wait 2 state.

- If there is no data to be sent by Server then it send Fin to sender.

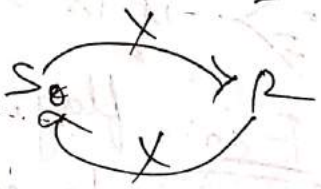
- Sender enter in Time_wait state and Send the Ack to server

All the resources released of client.

(*) Fin sent by Sender to receiver



(*) Fin send by Sender then fin sent by receiver



(*) TCP is reliable because there is no packet loss as it use Connection oriented.

UDP :=> User Datagram Protocol

- It is connection less (non-Reliable)

payload = Pure data

Source port 16	Destination port 16
Length 16	Checksum 16

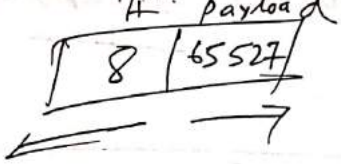
16 bit used to represent ports 0-65535

used for error control

8 Byte fixed (UDP Header)

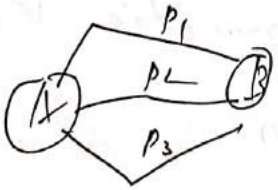
- order of data is not maintained

→ Max size of Segment 65535 in which header is of 8 Byte so Pure data will be 65527 Byte.



- Checksum = UDP header + UDP data + Pseudo header of IP

{ Hash value at side of sending & Hash value at side of receiving



packet goes to different path

(*) In IPv4 checksum is optional but in V6 it is mandatory.

UDP Application : UDP has no overhead (extra header value)

- Query Response Protocol (One request one reply)
  ex- DNS, DHCP
  We need not any connection to just get the ip of a website
- Speed (online games, voice over IP)
  Where we need high speed we use UDP for doing things fast without overhead.
- Broadcasting / Multicasting (RIP)
  after every some second a node share its routing table to others.
  we should not make connection that will take so much time.
- Continuous Streaming (Skype, Youtube)

Q2 type Protocol

- Stateful — When connection value is saved ex- amazon save what you clicked, what you saw etc.
- Stateless — Connection value is not saved. ex- UDP is stateless.

(X) TCP	UDP
• Connection oriented	• Connectionless
• Reliable	• non Reliable
• Error control mandatory	• Error control is optional. (only V_6 modality)
• Slow transmission	• Fast transmission
• More overhead (20B–60B)	• Less overhead (8B)
• Flow control, Congestion control	• No Flow control Congestion control

→ Too much header

it takes different route So fast.

(Y) HTTP is not Reliable So it use TCP to ensure Reliability

• DNS use UDP

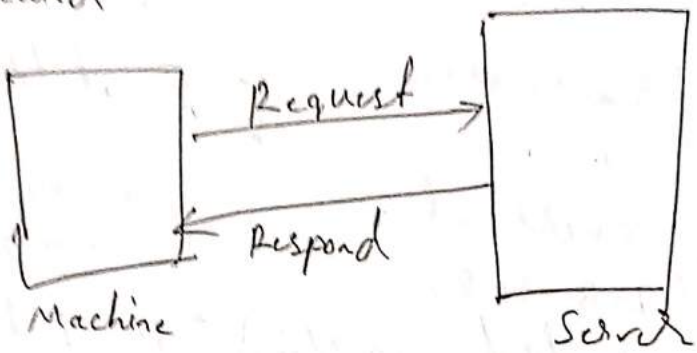
• FTP (File Transfer protocal) use TCP.

TCP	UDP
HTTP	DNS
FTP	BootP
	DHCP
	RIP

Session Layer :- create a session

Responsibilities are

- Authentication : When we give user id & password. Server do authenticate and give us authorization (set of previllage). & session is created



- Session restoration (checkpoint) :⇒ We can save the state of Session with the help of session bin

Banking website does not provide it due to security issue.

- Webinar :- provide Synchronization of audio & video (flow control)

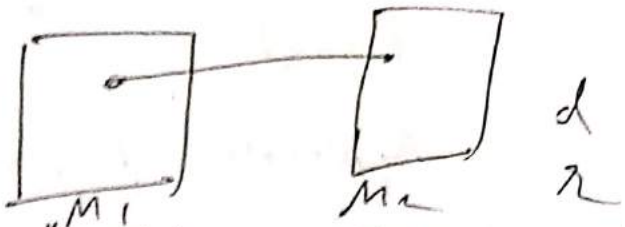
(X) Session & presentation layer is not the responsibility of O.S. It is responsibility of the application:

- Synchronizable of data exchange provided by Session Layer

Presentation Layer :=>

Responsibilities are

- Code conversion
- Encryption/Decryption
- Compression



Data can't be read by unknown person

Application Layer :=>

protocol name	port no	Transport protocol
Echo	7	TCP/UDP
FTP	20/21 (data, connection)	TCP
Secure shell (SSH)	22	TCP
Telnet	23	TCP
SMTP	25	TCP
DNS	53	UDP
DHCP	67/68	UDP
TFTP	69	UDP
HTTP	80	TCP
POP	110	TCP
NTP	123	UDP
HTTPS	443	TCP
	520	UDP

- It is the top most layer of OSI model
- User can interact through which user can interact.

Application layer program are based on client server model.

Functionalities

- Identifying communicating partner to transmit the data
- Determining resource availability. (checks whether sufficient network resources are available)
- Synchronizing communication.

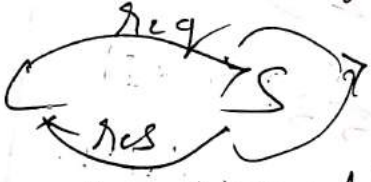
Services

- File transfer
- mail service
- Directory services.

(x) (x) Port no is of 16 bit so total no of port no 0 — 65535

0 — 1023 → well defined port no

Echo:



total time = round trip time

echo tells the total time

FTP: File transfer Protocal

20 (Data transfer)

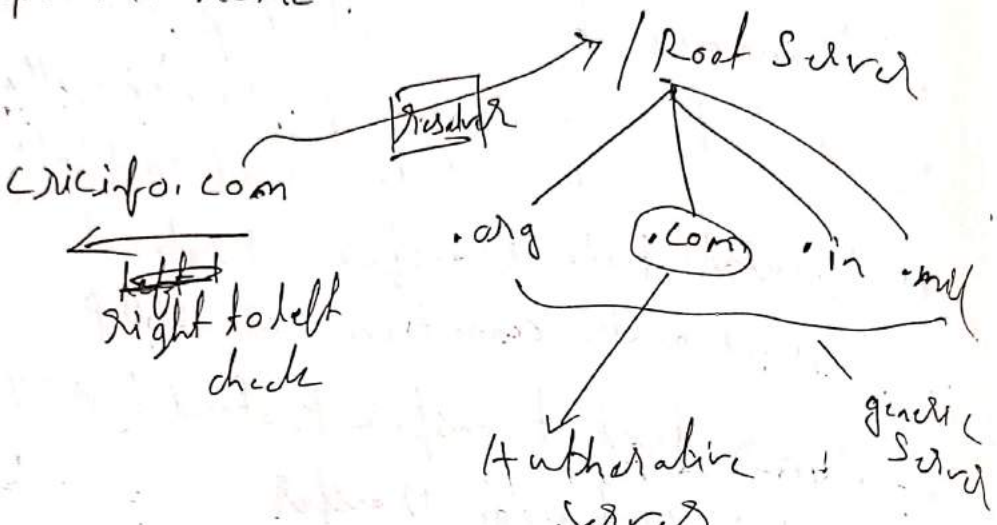
21 (control transfer)

- Secure Shell is used in cryptography use tunnelling
- Telnet is used for Remote log in
- Simple mail transfer Protocal (Smtp) used to send mail to server
- Domain name System (DNS) use UDP as it just give name & get ip
- Dynamic Host control protocal (DHCP) is used for assigning ip dynamically 67 (data) 68 (control)
- Trivial File transfer protocal (TFTP) it dosnot make connection use UDP
- Hyper text transfer Protocal (HTTP) is used in web page transfer
- Post office protocal (Pop) is used from server to system.
- Network time protocal (NTP) used for Synchronize the time
- HTTP Secure (HTTPS) - it used with secure Socket Layer (SSL)
- Routing information Protocal (RIP) - it just send the distance.

Domain Name System use UDP

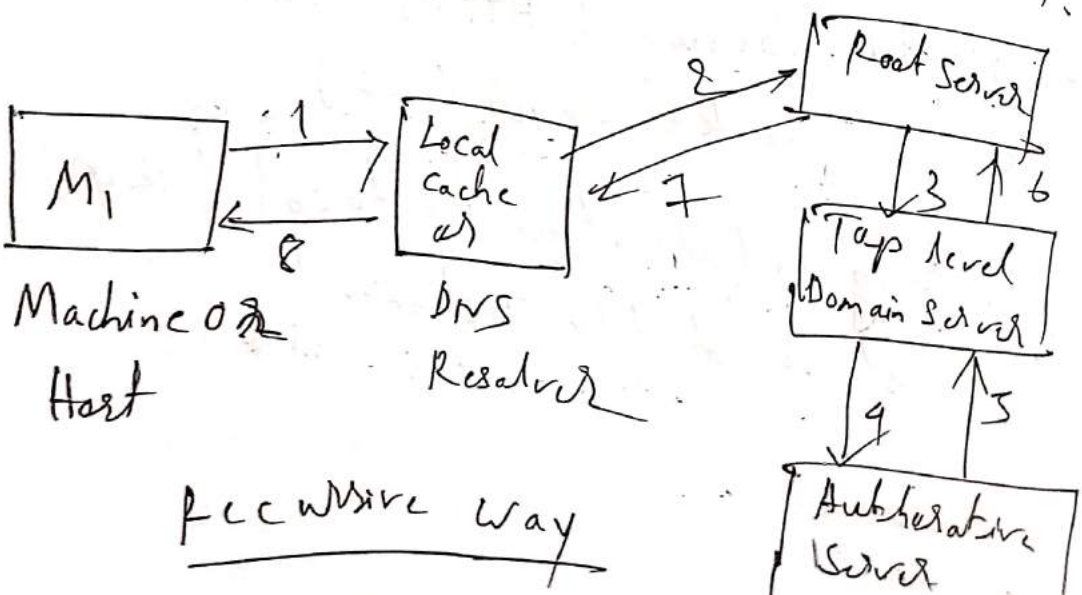
- Used for mapping domain name with ip address

Used for
- simplicity for remembering
- changed ip address automatically mapped to name.



it stored ip address & name

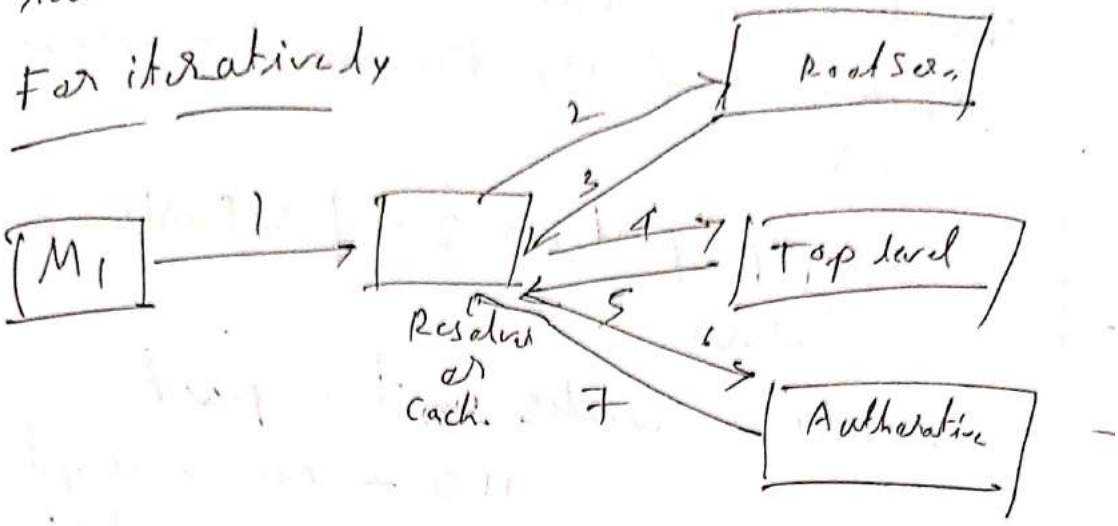
- Resolver first go to Root server then Resolver go to .com - server then it goes to Authoritative server
- It uses both recursive & iteratively.



Recursive way

@ Isp's Local cache store famous ip addresses so that every time it has not to go to root server.

- For iteratively



HTTP :=> used in webpage

- Port no 80
- not reliable but use TCP to achieve reliability
- inband Protocol (Command & Data go from the same port)
- stateless (does not store information of user)

amazon, flipkart etc use cookies to get information

FTP :=>

- 20 (Data) 21 (Control) port
- Data connection is non persistant
- Control connection is persistant
- not inband
- Reliable
- e.t.c

SMTP & POP :=>

FTP is synchronous (both sender & receiver should online) but SMTP & POP is both synchronous & asynchronous (need not to be online)

- SMTP port no 25 for Pushing mail in server
- POP3 works on two part
  - 110 — non encrypted
  - 995 — encrypted
- MIME (Multipurpose internet mail extension) used for — video, photo.

Persistant HTTP vs Non Persistant HTTP :=>

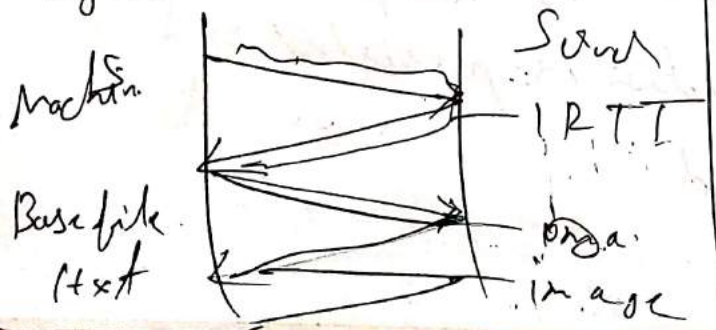
HTTP by default used — (1.1) persistant HTTP. (1.0)

persistant:

Server leaves connection open after sending Response

1 RTT for all Reference object

- Less overhead as it does not need to be connect again

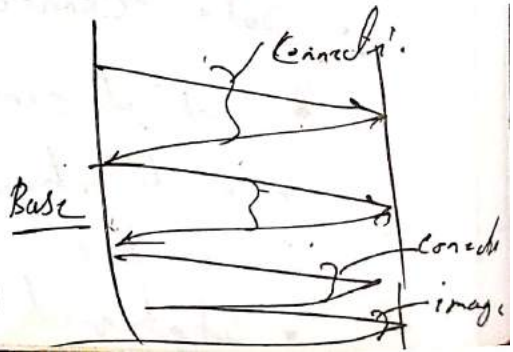


non persistant:

Connection closed after Sending Response

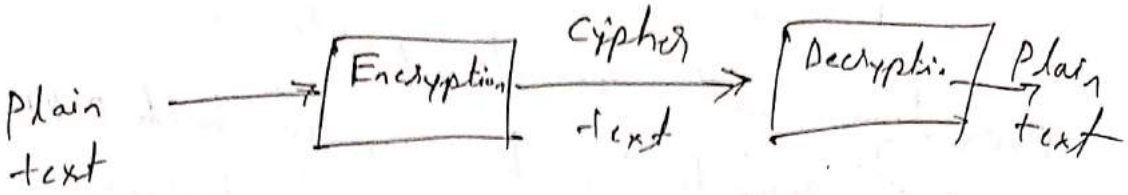
It requires 2 RTT per object (1 for connection + 1 for object)

- More overhead



Cryptography :-> "To achieve confidentiality"

Plain text is converted into cipher text
& again cipher text is converted into plain text

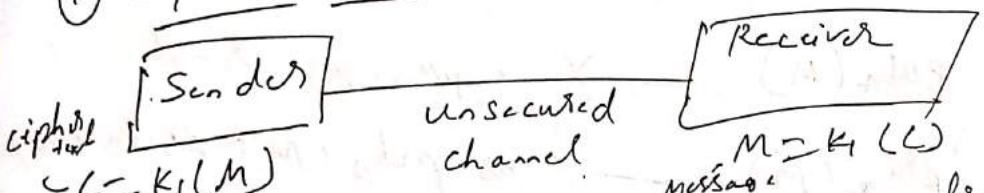


Sender Receiver

(x) Cipher text can be read but not understand by anyone.

(*) Cryptography use two types of key

(1) Symetric key: Same key in both Sender & Receiver

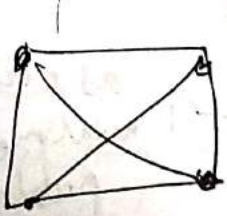


message

There is different algo for Symetric key

- DES (Data Encryption key) - 56 bits
- 3DES
- AES

Main challenge is sending key to receiver
(key can not be given with data else it will be stolen)



4 devices
Total key needed = $^nC_2$

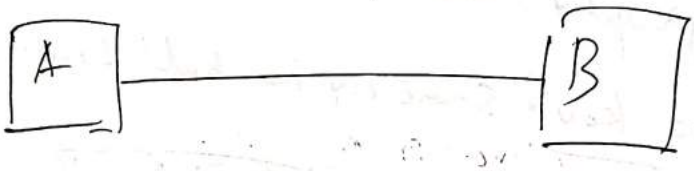
(Receiver can use same key to send data to sender)

(ii) Asymetric Key / public key :=> Different key is used for encryption & decryption.

Every device will generate public & private key

public ⇄ privat :=> if encrypted with public key of A then it can be decrypted with private key of A

- if encrypted with private key then decrypted with public key of same device



$Pub_A(M)$ — X as $pri_A(M)$ is not in B

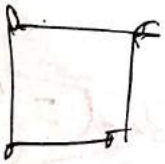
$pri_B(M)$ — X as $pub_A(M)$ is in every device as it broadcasted

$pri_B(M)$ → X as pri_B is not in A

$Pub_B(M)$ — ✓ as pri_B is in B and pub is sharable

(X) We use RSA Algorithm

(Rivest, Samer, Aldemai)



total 4 node

Key needed = 2n as every node will make public + private key

RSA Algo

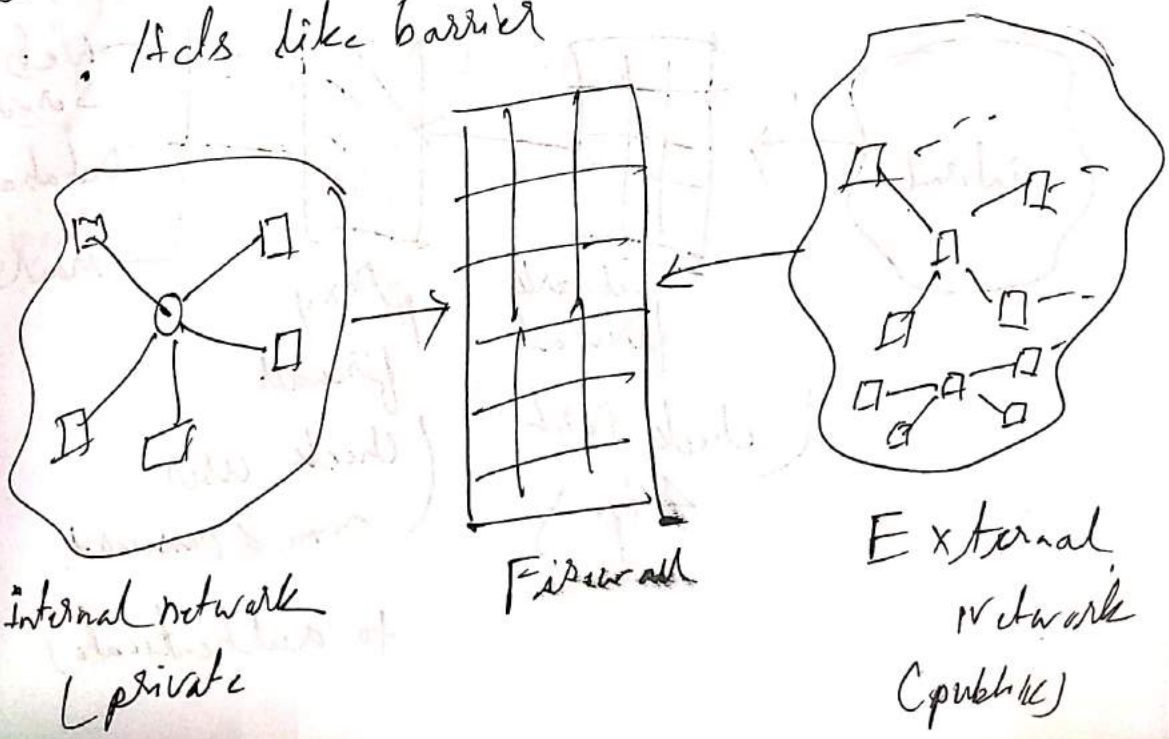
- Choose two different large random prime no
- Calculate $n = p * q$
- Calculate $\phi(n) = (p-1) * (q-1)$
- Choose e such that $1 < e < \phi(n)$
  e is coprime to $\phi(n)$ $\gcd(e, \phi(n)) = 1$
- Calculate d, such that $de \equiv 1 \bmod \phi(n)$
- public key e, private key d

$de = (1 + k\phi(n))$

$k = 0, 1, 2 \ldots n$

Firewall ⇒ (Network Security)

- A device mixture of software hardware
- Monitor and control incoming & outgoing data based on predefined rules
- Acts like barrier

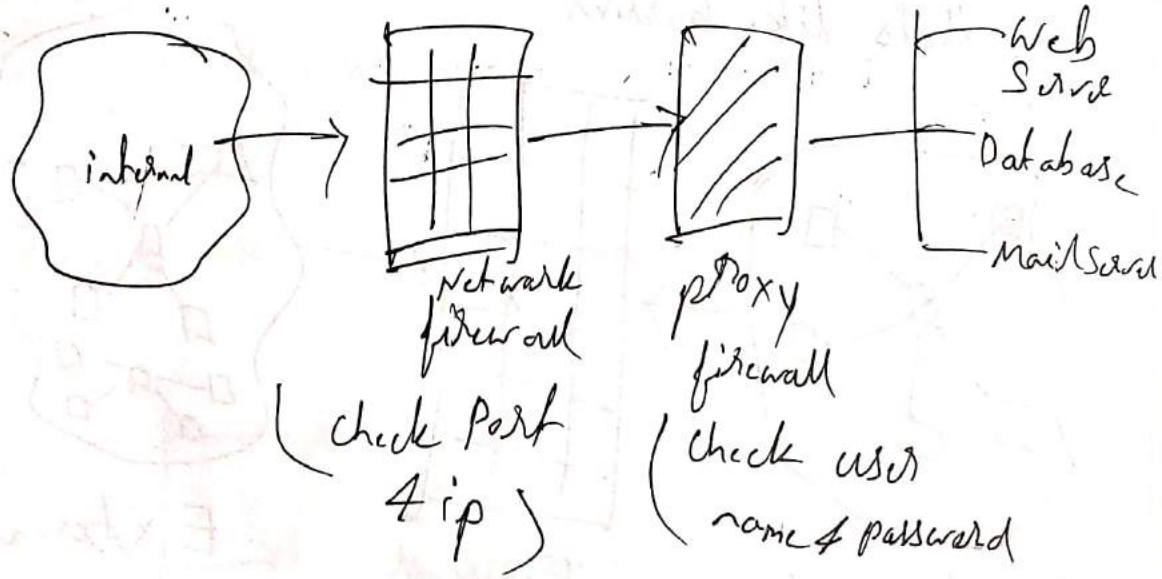


- There is host based (Software in PC) & network based (Hardware in organization) firewall

- 2 category
  (i) Packet filtering firewall
  (ii) Application (proxy) filtering firewall

(i) Packet filtering firewall : (Layer 4 upto transport)
- check ip header (ip address), TCP header (port number)
- works on network & Transport layer
- can block ip address / full network
- Can block a service (http (ftp)

(ii) Application (Proxy) firewall : (Layer 5 upto application layer)



Q. ip = 194.122.14.5 Mask = 255.255.255.0

(i) Host id is 14.5

(ii) Network id 194.122.14

(iii) 0.0.0.100 may be host of this network

(iv) ~~0.0.0.~~ Network consist of $2^8 - 2$ host, 0 subnets

(v) 1 bit is borrowed from host id

⇒ there is no slash then it is classful addressing

it is class C as it is in range of 192-223

- Network id 192.122.14.0

Host id 14.5 ✗ 0.5 ✓

network id 192.122.14 ✓

0.0.0.100 may be host ✓ (0-255)

- Network consists of $2^8 - 2$ host ✓

- 1 bit borrowed from host id ✗ (we borrow when we do subnet.

Q| Connect following

1. HTTP
2. FTP
3. DNS
4. SMTP
5. POP3

(i) uses both TCP, UDP
(ii) uses two ports for its operation
(iii) Mime to deal with non Ascii data
(iv) used to get mail
(v) Trace Method loop back request message.

⇒ 1 → v, 2 → ii
3 → (i)
4 → iii
5 → iv

(x) DNS use TCP / UDP but UDP is best

---

a| RSA algo is used P = 17 q = 11
public pair (e, n) = (7, 187) Secret key d = ?
(a) 11 (b) 15 (c) 10 (d) 23

⇒ $\phi(n) = 16 \times 10 = 160$
$de = 1 + k\phi(n)$ → (d) ✓
or, $d \cdot 7 = 1 + 1 \cdot 160$
or, $d = \frac{161}{7} = 23$

Need of IPV6 => (ip nxt) next generation

- Limitation in ipV4 addresses
  2^{32} ipV4 addresses
  2^{128} ipV6 addresses
- Realtime data transmission (ipV4 doesn't support)
- Authentication
- Encryption
- Fast processing at routers
  (Base header 40B)

Ip Security (ipsec) Protocol =>

- Network layer Protocol (used both by IPV4 & IPV6)
- IETF standard
- collection of protocols
  (i) Encapsulating Security payload (ESP)
  (ii) Authentication Header
  (iii) internet key exchange (Ike
- Use of Ipsec
  (i) confidentiality
  (ii) Authenticatio.
- Modes
  - Transport mode
  - Tunnel mode

(*) Socket address = ip address + Port no

Socket address used for uniquely identify specific connection.

- only port number is not sufficient for connecting to server as there is chance that more than one device is assigned same port no of a server

port no is of 16 bits

Total possibilities $0 - 2^{16}$

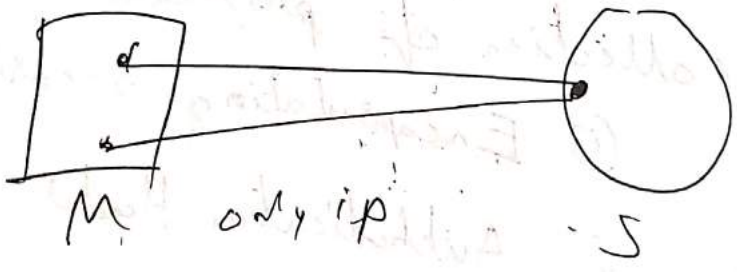
0 - 1023 well defined

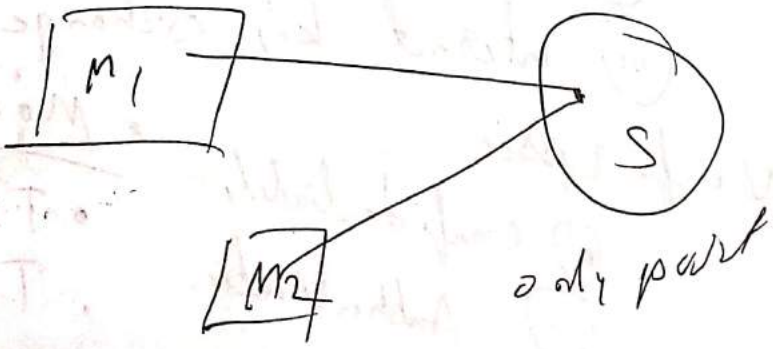
1024 - 49151 - Reserved for comp.,

49152 - 65535 - Randomly given

⊕ Possibility of same port

- only ip address is not sufficient as multiple processes of a machine has same ipaddress & if it communicate with the same server then it will create problem





- Each layer add. its own header to the data (from upper to lower)
- structure/format of data is called Syntax
- Message travel from Sender to receiver via a physical path called medium

wired (guided) wireless (unguided)

- Network edge device = host system (PC, Server, Smartphone)
- distributed system same like network but difference - whole collection seems to single system (writer)
- Overlay network built on another network (VPN or P2P)
- Bluetooth is an ex of Personal area network
- Network congestion = traffic overloading
- DSL (Digital Subscriber Line) provide both wire phone + ISP

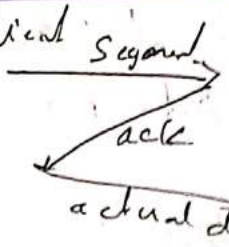
DSLAM (Multiplexer) (convert analogue → Digital

application, presentation, session — user support layer

transport layer — linker

network, data link, physical — network support

- ICMP (Internet Control Message Protocol) is a network Layer protocol used for error & diagnostic function.
- Socket is endpoint of an inter process communication flow across a network.
- Multiplexing used in circuit switching (telephone)
- TDM (Time division Multiplexing) used for transmit digital signal
- FileServer (FTP) helps Lan user to share data & program.
- STP cable (Rj-45 connector use) — Max length 100 m, Max speed 100 Mbps
- Sniffer prevented by Switched network.
- Firewall often block UDP traffic as it is more vulnerable to attack.
- Resource Reservation Protocol is used in transport Layer.



(HTTP) 3 way handshake

- HTTP Request -

Request line (Get, Post, Head)
Header line
Status line

Get method — client request data from server
post method - client submit data to server
Head method — only request smaller amount of data (document size not the entire document)
faster

- Web cache has its own disk size in storage.
- Conditional Get helps to keep the cache data of requested site.
- FTP built on client server architecture
- FTP has 2 modes
  - (a) active: client initiate control connection & server initiate data connection
  - (b) passive — client initiate both
- FTP is out of band connection (as data & control connection is done separately.)
- FTP has different mode
  - Stream mode (data → Segment fragmenting)
  - Block mode
  - compressed mode

PASS → for Password.

- SMTP works on client server architecture
It only support 7 bit ASCII code transmission

RCPT TO → Mail address of Receiver

It is push protocol as it sends mail to server

UA (user agent) is responsible for writing, reading & Replying Message

MTA (Message transfer agent) is responsible for routing message.

ODMR (On demand mail relay) is an extension of SMTP (which give mail after authentication)

DNS

- Hostname can Max of 255 char
- DNS client is called DNS resolver
- Server no clue about hostname - ask to root server
- Wildcard domain start with *

SSH | Port 22

- can be used in any OS
- It use Public key Cryptography / host based / password
- used for Secure communication + Remote
- SSH 2 does not contain physical layer

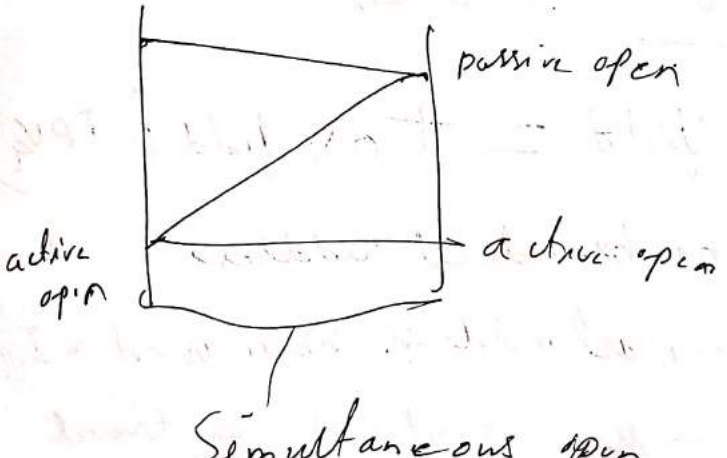
DHCP

67 (data) 68 (connection) UDP

- It gives ip address to each & every device
- used in both ipV4 & ipV6
- ip is assigned for a limited period
- It use Dynamic, automatic, Static } allocation
- DHCP Snooping = technique to ensure security
  if established then specific mac/ip can access network.

TCP

- In Segment header, Sequence number + ack number = Byte number
- Sequence number = first byte number of Segment
- value of ack field is next byte to be received Sequence no.
- header is 20–60 Byte



Source & destination Port both of 16 bit

UDP

- It also provide Demultiplexing & error checking.
- Low overhead fast
- Header 8 byte
- Ephemeral Port = client port (1025 – 5000)
- encapsulate in ip datagram so

UDP Length = ip Length – ip header's length

IPV4 32 bit

TTL → Time to live (max number of routers it can pass)

Protocol field – 6 – TCP
17 – UDP

- Offset helps for arrangement of fragments.

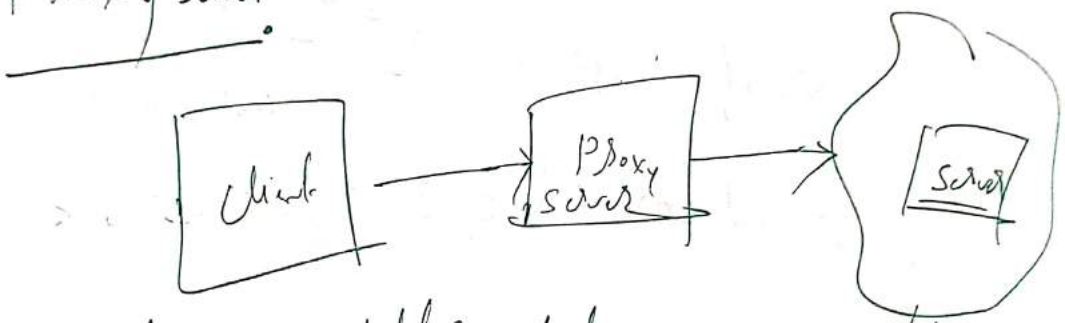
IPV6 128 bit

- Traffic field = TOS field (IPV4)
- There is no broadcast address
- There is anycast address which is not in IPV4
- Hop limit → Max router it can travel
- Dual stack = both ipv4 & ipv6

total Network layer 4

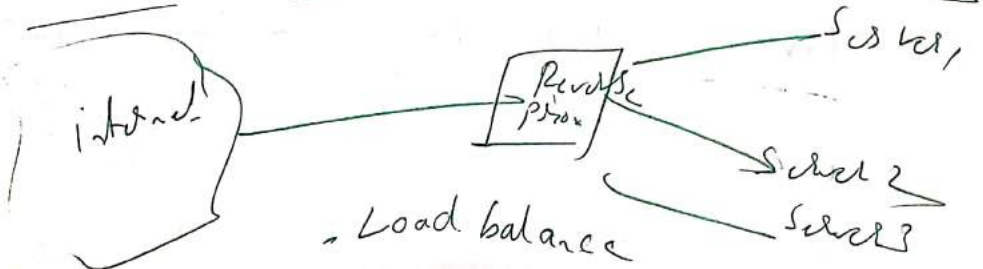
total data link layer 6

Proxy server



- acts as a filter between client & server
- Better Management
- protects client from attacks
- Security

Reverse Proxy :- Protect Server



- Load balance

Subnet

• ex 205.105.65.0/26

⇒ it is class C so 24 bit is for Network but here 26 bit for Network

∴ 2 extra bit

∴ No of subnet = $2^2 = 4$ (U29-tag)

0 0
0 1
1 0
1 1

Subnet mask = 255.255.255.192

∴ Network id = 205.105.65.0
255.255.255.192
205.105.65.0

∴ No of host = $2^6 - 2 = 62$
(Network id + broadcast id)

∴ Broadcast id = 205.105.65.63

Host range = 205.105.65.1 — 205.105.65.62

(*) Private ips

Class A - 10.0.0.0 - 10.255.255.255

Class B 172.16.0.0 - 172.31.255.255

Class C - 192.168.0.0 - 192.168.255.255

(X) VLAN = Break up broadcast domain in layer 2 switch internetwork

(X) Stub network :- A network that has only one entry & exit point

(X) Hardware address of a local device = ARP
(Address Resolution protocol) ✓MAC

(X) Internet control Message protocol (ICMP) is a network layer protocol to diagnosis network communication issue.

(X) DNS use both TCP / UDP

(X)