Chapter - 4

Data Link Layer :

① Physical Addressing

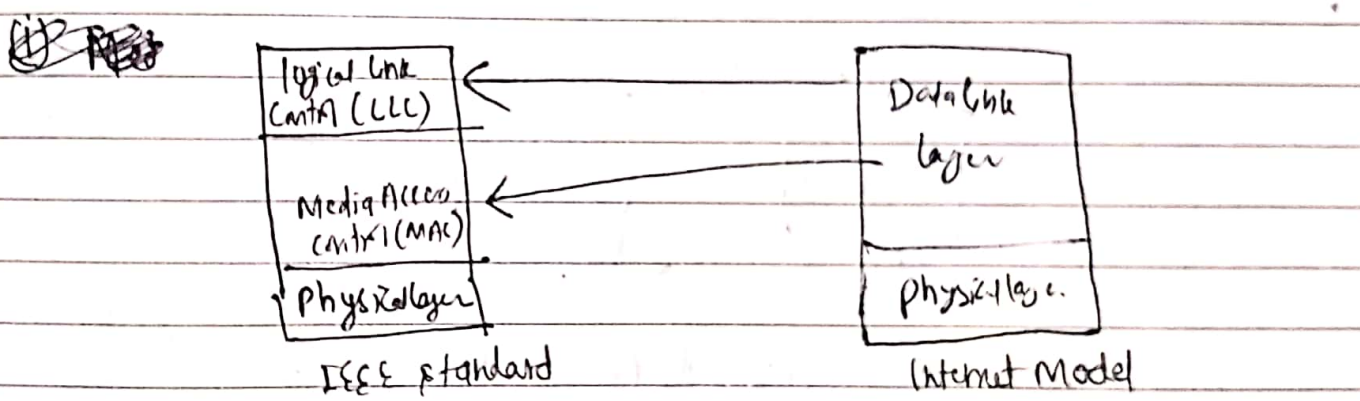
② Access Control ✓

③ Framing

④ Flow Control ✓

⑤ Error Control

Data link layer is further divided into two sublayers by IEEE.



(i) Media Access Control (MAC): It defines specific access method for each LAN. For example; it defines CSMA/CD as media access method for ethernet LANs. Take care of addressing at the level.

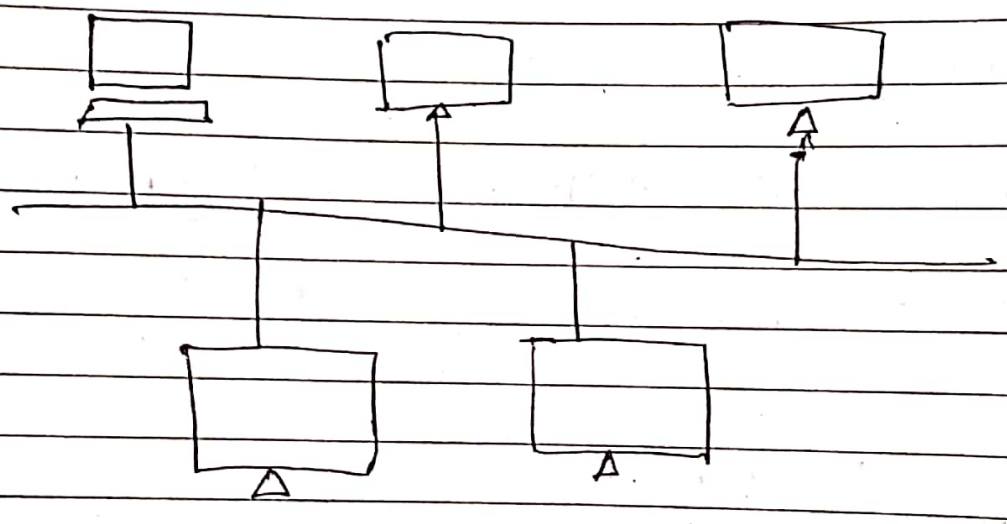
⇒ Flow control and Error control are handled by another sub layer logical link control (LLC).

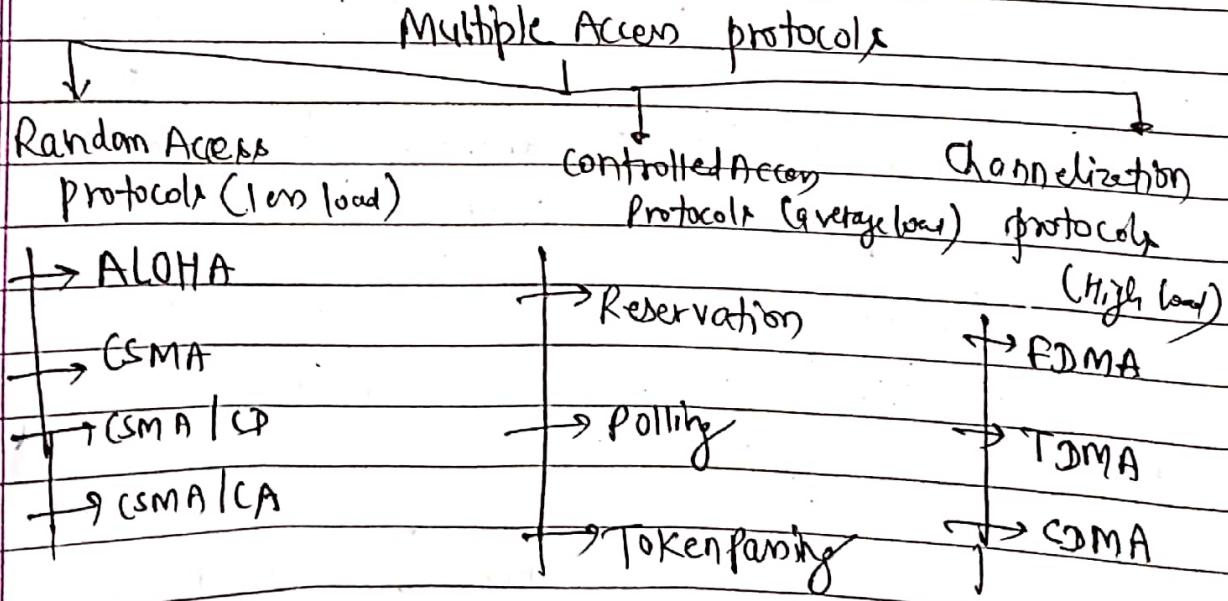
Framing is handled in both LLC sublayer and MAC sublayer.

Media Accen control :

⇒ When nodes or stations are connected and use a common link called multipoint or broadcast link, we need a multiple accen protocol to co-ordinate the accen to link.

⇒ Many protocols have been devised to handle accen to a shared link. All of these protocols belong to sublayer in data-link layer called Media Accen control (MAC).





Random Access Protocols:

→ All the stations / nodes have the same superiority that is no station has more priority than another station. It has two features:

→ ① There is no fixed time for sending data
② There is no fixed sequence of stations sending data.

The random access protocols are further subdivided as:

(1) ALOHA
(2) CSMA
- CSMA/CD (Detection is possible in wired not in wireless so we CA in wireless)
- CSMA/CA

~~① ALOHA~~:

→ However if more than one station tries to send, there is an access conflict - collision and frames will be either destroyed or modified.

→ All the protocols in Random Access Protocol approach will answer the following questions:

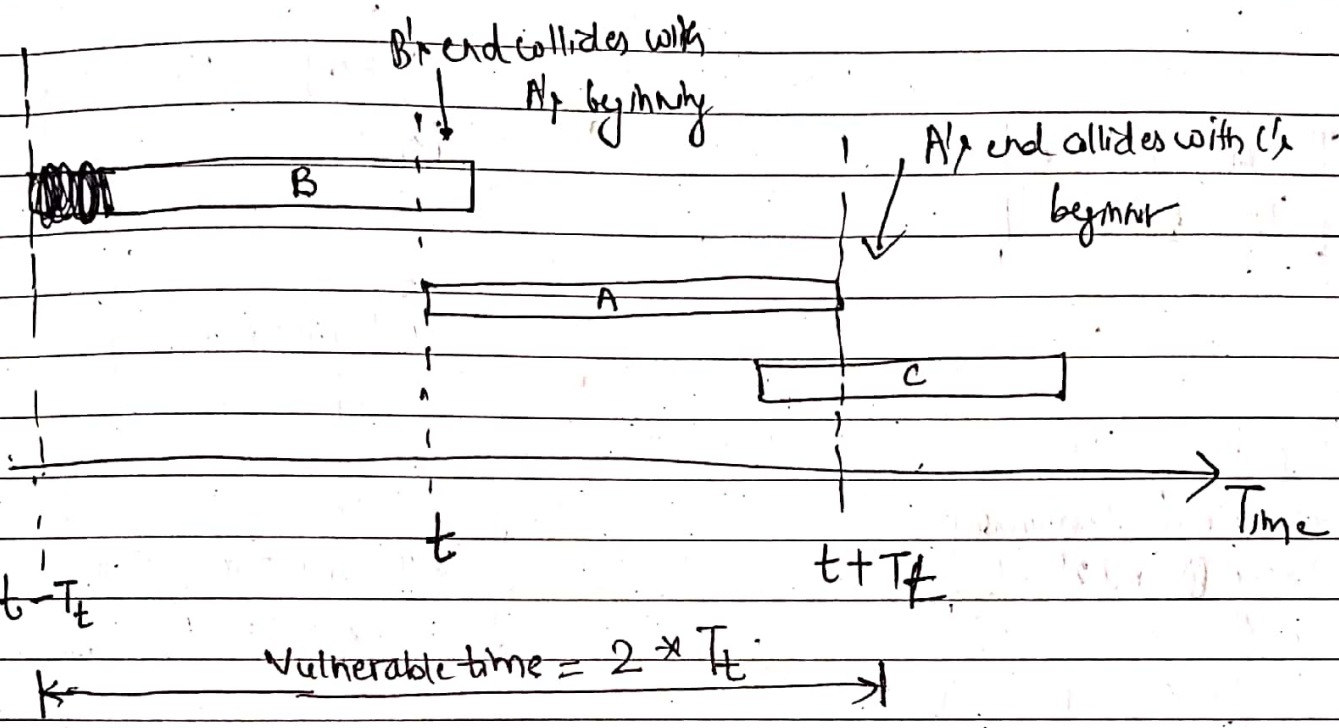
① When can the station access the medium?
② What can the station do if the medium is busy?
③ How can station determine the success or failure of transmission?
④ What can the station do if there is access conflict?

(1) ALOHA:

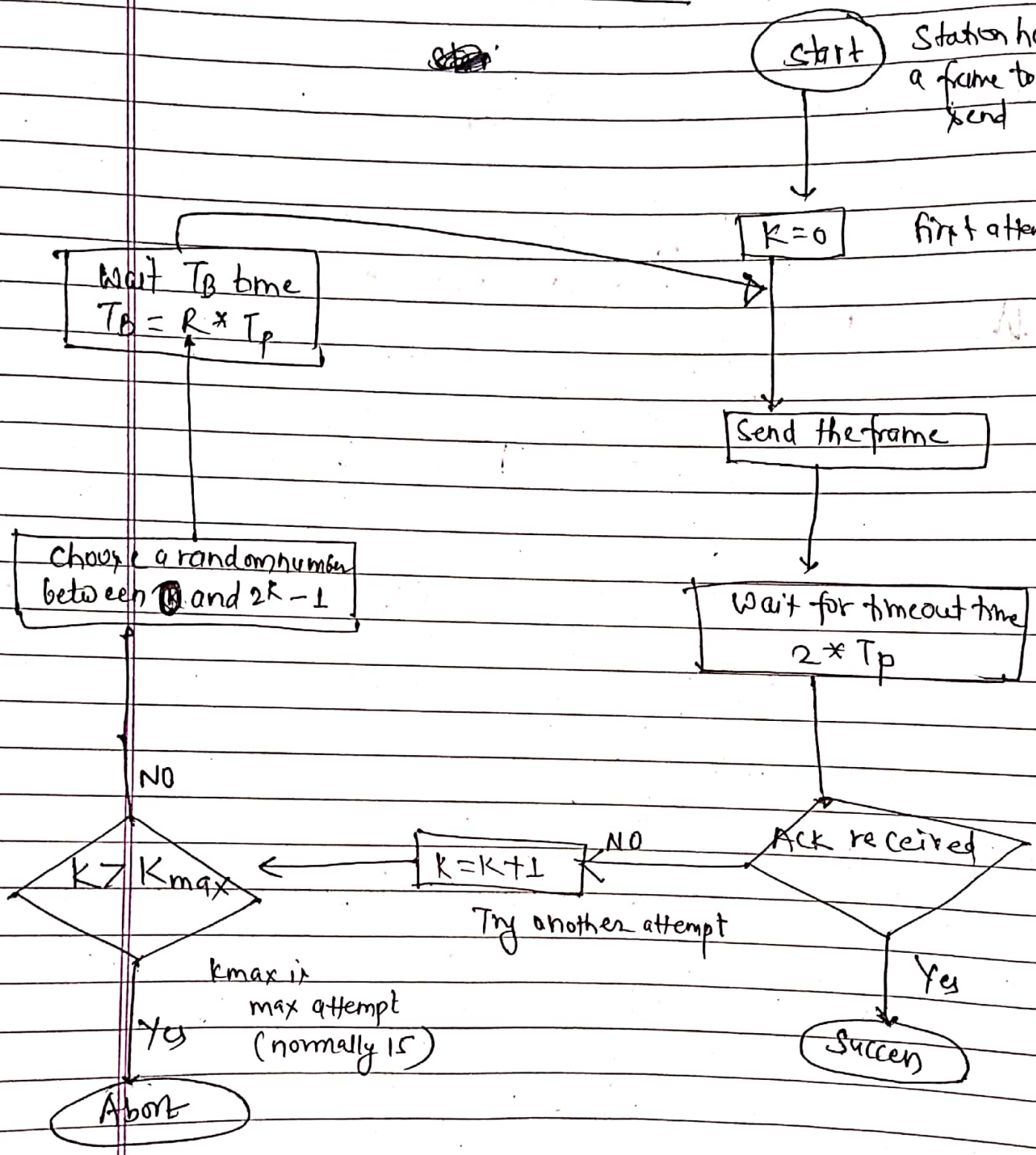
- Earliest random access method developed at the University of Hawaii around 1970.
- It was designed for radio (wireless) LAN, but can be used on any shared medium.
- The original ALOHA protocol is called pure ALOHA. This is a simple but elegant protocol.
- The idea is that each station sends a frame whenever it has a frame to send. However, there is possibility of collision between the frames from different stations.
- Vulnerable time in which there is possibility of collision. We assume that the stations send fixed-length frame with each frame taking T_{fb} to send.
- Station A sends a frame at time t. If station B already sent a frame between $t - T_{fb}$ and t, this leads to collision of frames of station A and station B. The end of B's frame collide with beginning of A's frame.
- On other hand, suppose station C sends a frame at t and $(t + T_{fb})$, the collision occurs between frames from station A and C. The beginning of C collides with end of A's frame.

→ We see that the vulnerable time during a collision in pure ALOHA is 2 times frame transmission time.

→ Pure ALOHA vulnerable time = $2 * T_t$



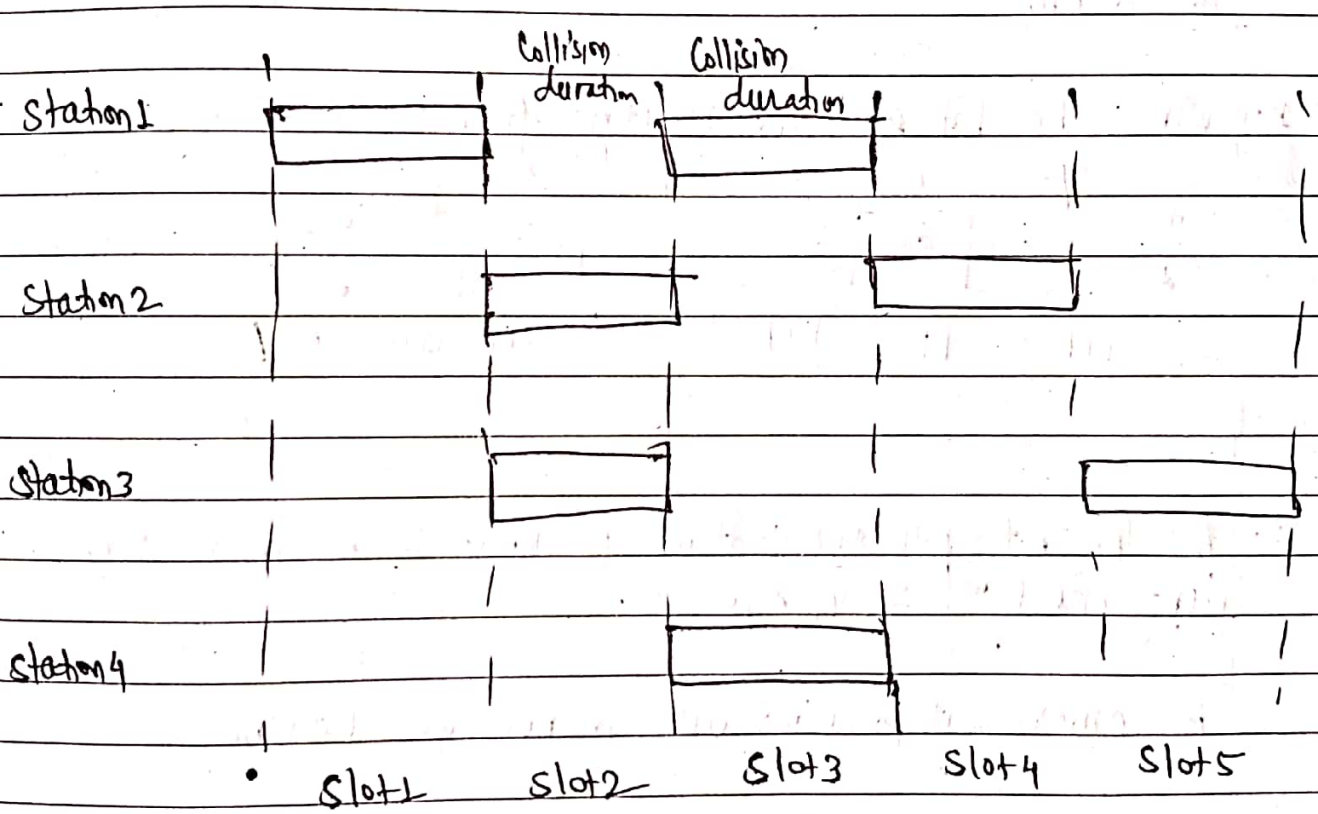
Procedure for pure ALOHA protocol:



(2) Slotted ALOHA:

→ Pure ALOHA has a vulnerable time of $2 * T_t$. This is because there is nonule that defines when the station can send. A station may send soon after another station has started or soon before another station has finished.

→ Slotted ALOHA was invented to improve the efficiency of pure ALOHA. In slotted ALOHA, we divide the time into slots of T_t & and force the station to send only at beginning of time slot.



[same slot मे two/more station के frame send होने collision]

[Flowchart same as ALOHA ; everything same as ALOHA]

Hamming code:

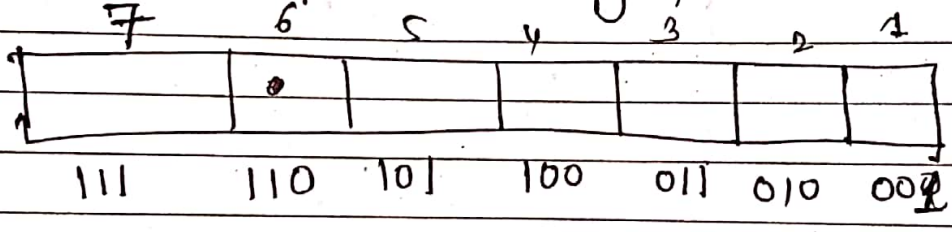
→ K- parity bits are added to n-data bits forming a new word of (n+k) bits.

→ The bit positions are numbered from 1 to (n+k).

→ Those positions with powers of two are reserved for parity bits. The remaining are data bits.

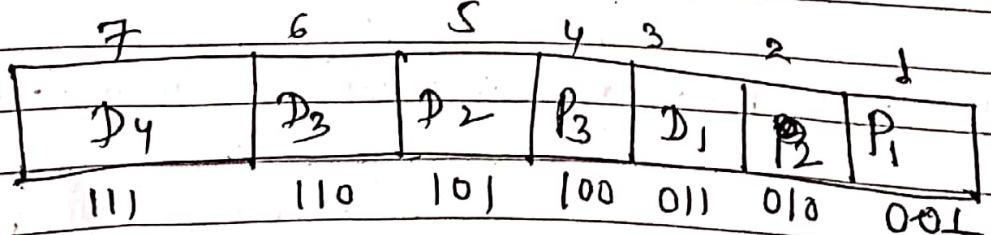
Algorithm:

1. Write the bit positions starting from 1 in binary form.



2. All the bit positions that are power of 2 are marked as parity bits (1, 2, 4, 8, etc.).

3. All other bit positions are marked as data bit.



4. Each data bit is included in a unique set of ~~priority~~ parity bits, as determined its bit position in binary form.

a. Parity bit 1 (P_1) covers all the bit positions with 1 in least significant portion (1, 3, 5, 7, etc.)

b. Parity bit 2 (P_2) covers all with 1 in second position from LSB (2, 3, 6, 7).

c. Parity bit 3 (P_3) covers all with 1 in third position from LSB (4, 5, 6, 7).

5. Since we check for even parity set parity bit to 1 if total number of ones in the positions it checks is odd.

6. Set a parity bit zero if total number of ones in the group of data bits it include is even.

Suppose the data to be transferred is 1011001.

11	10	9	8	7	6	5	4	3	2	1
1	0	1	P_4	1	0	0	P_3	1	P_2	P_1
1011	1010	1001	1000	0111	0110	0101	0100	0011	0010	0001

Groups: Positions (1, 3, 5, 7, 9, 11) = P_1, 1, 0, 1, 1, 1

$P_1 = 0$ (even)

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

$\Rightarrow (P_3, 4, 8, 6, 7, 11) = (P_3, 0, 0, 1, 1)$ $P_3 = 1$

$\Rightarrow (P_4, 9, 10, 11) = (P_4, 1, 0, 1)$ $P_4 = 0$

Thus, data transferred is:

11	10	9	8	7	6	5	4	3	2	1
1	0	1	0	1	0	0	1	1	1	0

Suppose, 6th bit is changed from 0 to 1 during transmission

0110

Classful Addresses:

Class A:

netId = 8 bits Host ID = 24

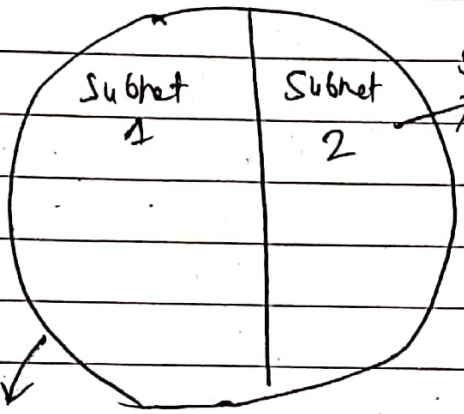
How to identify class A address:
- Range of 1st octet is [0, 127] in dotted decimal
- First bit is reserved to 0 in binary notation.

(Q) Consider the network having IP address 200.1.2.0. Divide this network into two subnets.

200.1.2.0 is class C network

→ First 3 Bytes are ~~Host Address~~ Network Id (Can't be manipulated)
→ Remaining 1 Byte (Host Id)

1 Byte = 2^8 = 256 hosts (0-255)



start: 200.1.2.1 0 0 0 0 0 0 0
200.1.2.128
End: 200.1.2.1 1 1 1 1 1 1 1
200.1.2.255

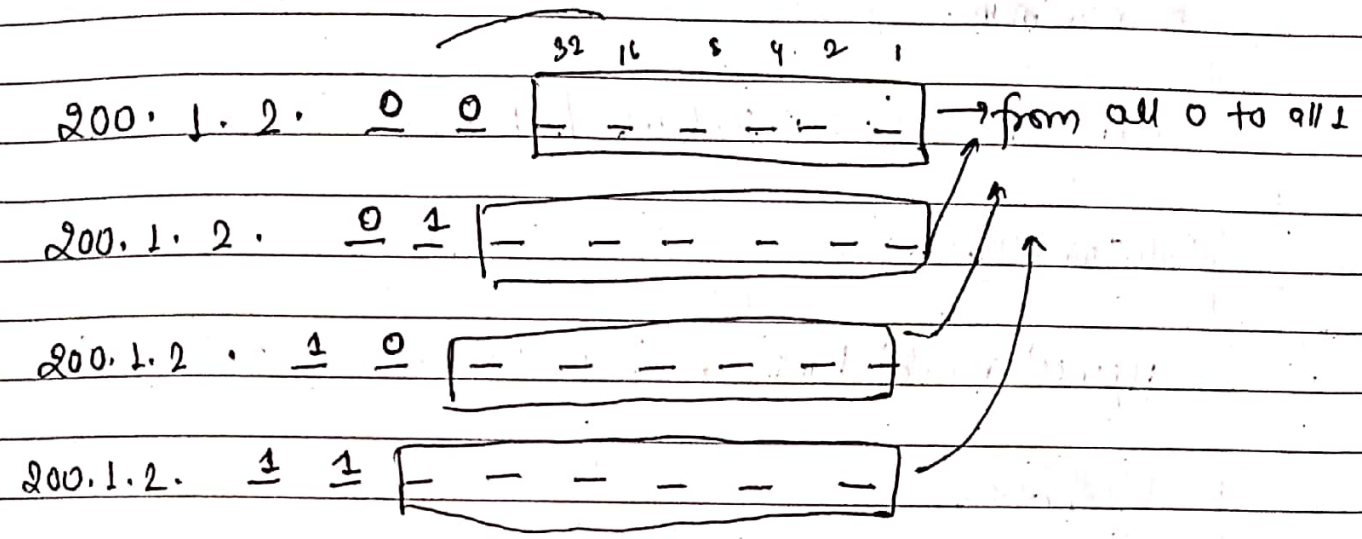
Start: 200.1.2.0 0 0 0 0 0 0 0 — 200.1.2.0
End: 200.1.2.0 1 1 1 1 1 1 1 — 200.1.2.127

Allocate MSB (of Host Id) 0 and 1 to start.

Start Address is subnet Id / IP Address of subnet.

[Bits are borrowed from host to network.

(Q) Consider we have a big single network of IP Addren 200.1.2.0. We want to do subneting and divide this network into 4 subnets.



Subnet 1: 200.1.2.0 to 200.1.2.63

subnet 2: 200.1.2.64 to 200.1.2.127

subnet 3: 200.1.2.128 to 200.1.2.191

subnet 4: 200.1.2.192 to 200.1.2.255

First IP is subnet Id,
Last IP (all 1's in host): Broadcast address

Both are non-allocatable to any hosts.

(Q) 4 departments A(23), B(16), C(28), D(13). Perform subnetting such a way that IP wastage in each subnet is minimum.

Given IP: 202.70.64.0 /24

Solution: Here:

Highest no. of host is in C (28).

We have:

202.70.64.0 /24 i.e.
Network bit = 24
Host bit = 8

let, n be no. of host bit for 28 then;

$2^n - 2 \geq 28$
or, $2^n \geq 30$
$\therefore \boxed{n = 5}$

Out of 8 Host bits, only 5 bits are sufficient. The remaining 3 bits can be given to Network. These 3 bits transfered from Host to Network are subnet bits.

No. of subnet possible $= 2^3 = 8$.

which are:

① 202.70.64.[000 00000]
② 202.70.64.[001 00000]
③ 202.70.64.[010 00000]
④ 202.70.64.[011 00000]
⑤ 202.70.64.[100 00000]
⑥ 202.70.64.[101 00000]
⑦ 202.70.64.[110 00000]
⑧ 202.70.64.[111 00000]

We assign following IP to C:

202.70.64.0 /27 (24 net + 3 subnet bit = 27) ← new net bits

① Network id [first IP of network]
= 202.70.64.0 /27

② Broadcast id [last IP with all host bit 1]
= 202.70.64.31/27

③ Usable range
= [202.70.64.1/27 , 202.70.64.30/27]

④ Subnet Mask:

128 64 32
255.255.255.[111 00000] = 255.255.255.224

⑤ Wildcard mask: (255 - each octet of subnet) mask:
= 0.0.0.31

(Q) Design a network of 5 departments containing 29, 14, 15, and 15 computers. Take a network example IP 202.83.54.92/25.

Soln : Here,

Given IP: 202.83.54.92/25

No. of Network Bits = 25

No. of Host Bit = 7

Highest no. of hosts in given problem is : 29

Let n be no. of host bit required.

$2^n - 2 \geq 29$

or, $2^n \geq 31$

$\therefore \boxed{n = 5}$

So only 5 bit for host is sufficient. 2 bits can be moved from host to network.

So, for 29 computers IP is:

Net IP: 202.83.54.0/27

~~Network IP: 202.83~~

Broadcast IP: 202.83.54.31/27

202.83.54.0 | 0 | 11011 |

00
01
10

11111
31

64
31
95

Usable Range: [202.83.54.1 – 202.83.54.30]

Subnet Mask: 255.255.255.224

Wildcard mask: 0.0.0.31

For 23 computers: n = 5

Network IP: 202.83.54.32/27
Broadcast IP: 202.83.54.63/27
Usable Range = [202.83.54.32/27 – 202.83.54.63/27]

For 15 Computers:

$2^n - 2 \geq 15$
$2^n \geq 17$
$n = 5$

Network IP: 202.83.54.64/27
Broadcast IP: 202.83.54.95/27

128
64
32
16
8
4
2
1

Date
Page

For 14 computers :

$2^n - 2 \geq 14$

$2^n \geq 16$

$n = 4$

202.83.54.0 | 00 0000

Subnet mask : 255.255.255.240 = (/28)

Network IP : 202.83.54.96

202.83.54.0 00 00000 ✓ (Gone)
01 00000 ✓ (Gone)
10 00000 ✓ (Gone
11 00000 (Remainy)

110 0000 — for 14 comp.
111 0000 — for 5 computer

Broadcast IP : 202.83.54.111

Usable = [202.83.54.97/28 – 202.83.54.110/28]

96
16
112
5
127

Date
Page

for 5 computers:

~~Network IP = 202.83.54.112~~
~~Broadcast IP:~~

$2^n - 2 \geq 5$

$2^n \geq 7$

$\boxed{n = 3}$

[202.83.54.01110] 000 (42,) Subnet Mask = 255.255.255.248

Network IP: 202.83.54.112 | 29
Broadcast IP: 202.83.54.119 | 29

2076 Bhadra

(14)

Ans: Four departments with 20, 32, 60 and 64 computers.

Let's suppose class C public network be:

200.10.10.0 /24 no. of network Bits = 24
no. of host bits = 8

① For 64 computer:

$2^n - 2 \geq 64$

$2^n \geq 66$

$\therefore n = 7$

(host)

So, 7 bits are sufficient for allocating 64 computers.
1 bit can be moved to network bits.

Subnet mask = 255.255.255.128 = /25

② For 60 computer:

$2^n - 2 \geq 60$

or, $2^n \geq 62$

$\therefore n = 6$

So, 6 host bits are sufficient.
2 bits can be transferred to network bits.

Subnet mask = 255.255.255.[11 000000] = 255.255.255.192
ie. /26

Network IP = 200.10.10.[00 000000] = 200.10.10.0 /26
Broadcast IP = 200.10.10.[00 111111] = 200.10.10.63 /26
Usable Host range = [200.10.10.1 - 200.10.10.62]

② For 32 computers:

$2^n - 2 \geq 32$
or, $2^n \geq 34$
$\therefore n = 6$

For 32 computers also, 6 bits are sufficient for host.
2 bits are transfered to network bits.

Subnet mask = 255.255.255.[11.000000] = 255.255.255.192
ie. /26
Network IP = 200.10.10.[01 000000] = 200.10.10.64 /26
Broadcast IP = 200.10.10.[01 111111] = 200.10.10.127 /26
Usable Range = [200.10.10.65 - 200.10.10.126]

③ For 24 computers:

$2^n - 2 \geq 24$
or, $2^n \geq 26$
$\therefore n = 5$ 3 bits are transfered to network bits.

Subnet mask = [255.255.255.111 00000] = 255.255.255.
i.e. /27

Network IP = 200.10.10.[100 00000] = 200.10.10.128

Broadcast IP = 200.10.10.[100 11111] = 200.10.10.159

Usable IP = [200.10.10.129 — 200.10.10.158]

(4) For 20 computer:

$2^h - 2 \geq 20$

or, $2^h \geq 22$

$\therefore \boxed{h = 5}$

3 bits can be transferred to network bits.

Subnet mask = [255.255.255.111 00000] = 255.255.255.22
i.e. /27

Network IP = 200.10.10.[101 00000] = 255.255.255.160

Broadcast IP = 200.10.10.[101 11111] = 255.255.255.191

Usable Range = [200.10.10.161 — 200.10.10.190]

Routing Algorithms:

Distance Vector:

Distance vector is the simplest routing algorithm, used by Routing Information Protocol (RIP).

→ Routers identify their neighbors through some sort of neighbour discovery mechanism.

→ Each router maintains a forwarding table consisting of <destination, next-hop, cost> of neighbouring networks only.

→ A router doesnot have the knowledge of entire path to a destination network. Instead the routers knows only:

① The direction in which packets should be forwarded
② The cost or distance to destination network.

→ Each router reports the <destination, cost> portion of its table to its neighbouring routers at ~~each~~ regular intervals. These portion are the "vectors" of algorithm name. It doesnot matter if neighbors exchange reports at the same time or even at same rate.

→ Each router also monitors its continued connectivity to each neighbour; if neighbour N becomes unreachable then its reachability cost is set to infinity.

→ In a real IP network, actual destinations would be subnets attached to routers; one router might be directly connected to several such destinations. In the following, however, we will identify all a router's directly connected with subnets with the router itself. That is, we will build forwarding tables to reach every router.

Distance-Vector update Rules: (Algorithm):

Let A be a router receiving a report $\langle D, C_D \rangle$ from neighbour N (ie. from N, D can be reached with cost CD). N is at cost C_N from A.

Now, A can reach D via N with cost $C = C_D + C_N$. A updates its own table accordingly to following rules:

① New destination: D is previously unknown destination.
A adds $\langle D, N, C \rangle$ to its forwarding table.

② lower cost: D is a known destination with entry $\langle D, M, C_{old} \rangle$ but the new total cost C is less than C_{old}. A switches to cheaper route, updating its entry for D to $\langle D, N, C \rangle$. ~~It is possible that M = N, meaning that N is~~ If $C = C_{old}$, A ignores the new report.

(neighbour को already exist path को cost increase गया)

(B) Next Hop Increase:

A has an existing entry $<D, N, C_{old}>$ and the new total cost c is greater than C_{old}. Because this is a cost increase from neighbour N that A is currently using to reach D, A must incorporate the increase in its table. A updates its entry for D to $<D, N, c>$.

The first two rules are for new destinations and shorter path to existing destinations.

The third rule introduces the possibility of instability, as a cost may also go up. It represents bad-news case, in that neighbor N has learned that some link failure has driven its own cost to reach D, and is now passing that bad news on to A which routes to D via N.

② Link State Routing Algorithm:

→ Alternative to Distance vector.

→ There are two specific link state protocols:
① Open Shortest Path First (OSPF)
② Intermediate Systems to Intermediate Systems (IS-IS)

→ In distance vector routing, each node knows a bare minimum of network topology; it knows nothing about links beyond ~~neighbors~~ immediate neighbours. In link state approach, each node keeps a maximum amount of network information; a full map of all nodes and all links. Routes are then computed locally from this map, using the shortest-path-first algorithm. The map also allows calculation of different routes for different quality-of-service requirements. The map also allows calculation of a new route as soon as news of failure of existing route arrives; distance-vector protocols on the other hand must wait for report of a new route after an existing route fails.

→ Link-state protocols distribute network map information through a modified form of broadcast of states of each individual link.

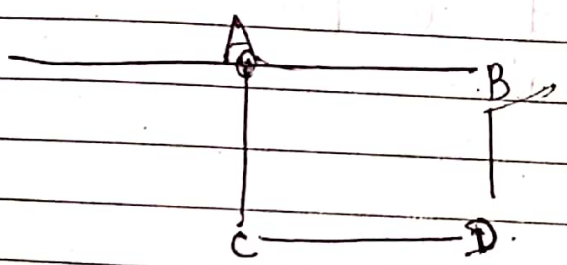
→ Whenever either side of a link notices that the link has died or if a node notices that a new link has become available, it sends out link-state packets (LSPs) that floods the network. This broadcast process is called reliable flooding.

→ The link-state flooding algorithm avoids the usual problems of broadcast in the presence of loops by having each node keep a distance of all LSP messages.

→ The originator of each LSP message includes its identity, information about the link that has changed status, and also a sequence number

→ other routers need only keep in their databases the LSP packet with the largest sequence number; older LSPs can be discarded.

→ When a router receives a LSP, it first checks its database to see if that LSP is old, or is current but has been received before; in these cases, no further action is taken.



Suppose, the A-E link status changes. A sends LSPs to C and B, Both these will forward LSPs to D;

Suppose B's arrives first. Then D will forward LSP to C. the LSP traveling C → D and LSP traveling D → C might even cross on wire. D will ignore the second LSP copy it receives from C and C will ignore the second copy it receive from D.

From network map next step is to compute shortest path using shortest path first algorithm.

Date
Page

Difference between Distance Vector and Link State Routing:

Distance Vector Routing	Link state Routing
(1) Each router has knowledge only about its neighbouring routers.	(1) Each router has full knowledge of network topology with all nodes and links.
(2) ~~Bandwith required is t~~ The router shares vector only to neighbour routers.	(2) The router floods packets to ~~all the nodes~~ the network.
(3) Bandwidth required is less due to local sharing of small packets and no flooding.	(3) Bandwidth required is more due to flooding.
(4) Based on local knowledge since it updates table based on information from neighbors.	(4) Based on global knowledge i.e. it have knowledge about entire network.
(5) Uses Bellman-ford algorithm	(5) Uses Dijkastra's algorithm
(6) Count to infinity problem.	(6) No count to infinity problem.

⑦ Persistent looping problem	⑦ No persistent looping prob
⑧ Practical implementation is RIP and IGRP.	⑧ Practical implementation is OSPF and ISIS.

Classful Routing:

→ It does not import subnet mask.

→ Subnet mask is same throughout the network; dont vary for all devices.

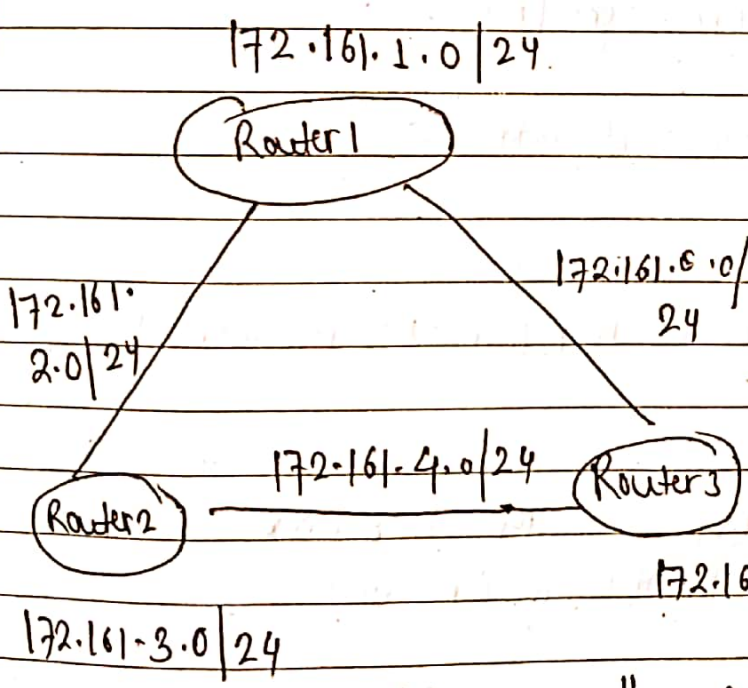


fig: Subnet is same throughout topology classful routing

Classless Routing

→ It imports subnet mask.

→ Subnet mask is not same throughout. varies for all devices.

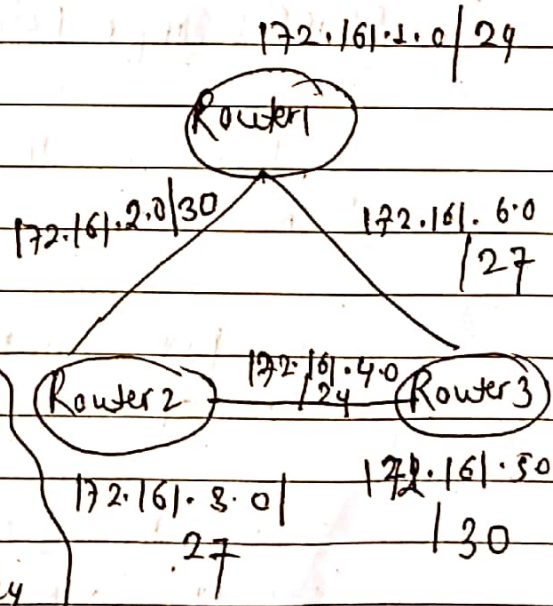


fig: Subnet can vary throughout topology in classless routing

Chapter-9 Network management and Security:

Network management is defined as all administrative actions such as monitoring, testing, configuring and troubleshooting network components to keep network running smoothly.

The network management has five areas of concern (FCAPS)

1. Fault Management
2. configuration Management
3. Accounting management
4. Performance Management
5. Security management.

SNMP (Simple Network Management Protocol):

→ It is an "Internet standard protocol" for managing devices on IP networks.

→ This protocol allows a device to report information about its current operational state.

→ Devices that typically support SNMP are routers, switches, servers, workstations, printers, modems, etc.

→ SNMP is by far the most popular protocol for supporting network device monitoring.

→ SNMP allows polling of individual designated device attributes such as the system name or the number of packets received via interface eth0.

→ Attributes may however be organized into records, sets and tables. Tables may be indexed contiguously, like an array - Eg: interface[1], interface[2], etc. or sparsely Eg: interface[1], interface[1236], etc.

→ SNMP node that replies to request for information is SNMP agent.

→ The network node doing SNMP querying is called manager.

3 Components of SNMP:

① SNMP manager:

It is a centralized system used to monitor network. It is node doing SNMP querying. It is also known as Network management ~~Network station (NMS)~~ (NMS).

② SNMP agent:

- It is a ~~software~~ management software installed on a managed device. Managed devices can be network devices like PC, routers, switches, servers etc.

③ Management Information Base (MIB):

MIB consists of information on resources that are to be managed. This information is organized hierarchically. It consists of objects instances which are essentially variables.

SNMP messages:

① GetRequest:

- Sends this message to request data from SNMP agent.
- SNMP agent responds with request value.

② GetNext Request:

③ GetBulkRequest (introduced in SNMP V2C)

④ Set Request: set value of an object on SNMP agent by manager

⑤ Response: It is a message sent from agent upon a request from manager.

⑥ Trap:

These are messages sent by agent without being requested by manager. It is sent when fault has occured.

⑦ Inform Request:

- used to identify if trap message has been received by the manager or not. The agents can be configured to

send trap message continuously until it receives an Inform Request.

SNMP security levels:

It defines type of security algorithm performed on SNMP packets. They are used only in SNMPV3 i.e There are 3 security levels namely:

1. noAuthnoPriv: (No authentication, no privacy)
2. auth NoPriv: uses md5 for authentication & no encryption for privacy
3. authPriv – HMAC with md5 or SHA for authentication
   – DES-56 for encryption.

Versions:

1. SNMP V_1 – uses community strings for authentication and uses UDP only
2. SNMP V_2c – uses community strings for authentication, uses UDP but can configured to TCP.
3. SNMP V_3 – uses HashBased MAC with MD5 or SHA for authentication & DES for privacy/encryption
   – uses TCP.

Higher the version of SNMP, more secure it will be.

Bandwidth:

→ Measure of how much data can be transfered from one point in a network to another within a specific amount of time
Eg: 100Mbps ie. 100 Mega bits per second.

A Higher bandwidth is better.

latency:

→ latency refers to how much time signal takes to travel to its destination and back.

→ A latency is better.

To test latency, we can send a small bit of data to remote server to measure round trip time.

We use ping command.

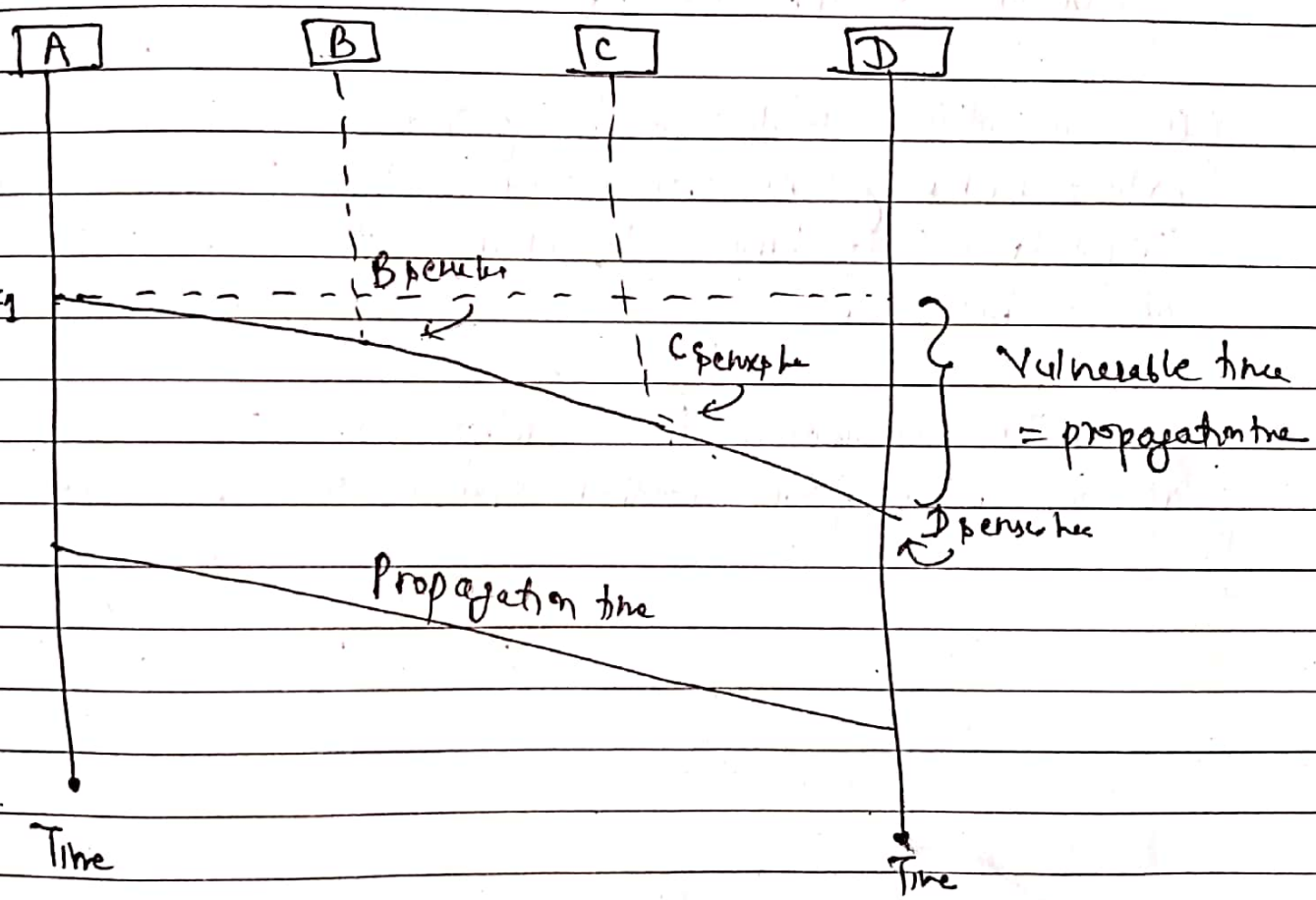
```
C:\> ping 4.4.8.8

$ ping 4.4.8.8
```

→ Carrier Sense Multiple Access (CSMA):

→ The station senses the medium before sending or using it.

→ It reduces chances of collision but it cannot eliminate it.

→ The possibility of collision exists because of propagation delay.



→ Each station checks the state of medium before sending.

Suppose A starts sending data at t_1. But data reaches to B at propagation time. During that interval, B may send data [Vulnerable period]

(detects collision / checks medium before sending but पहले से ही collision detect करने की CD चाहिए थी)

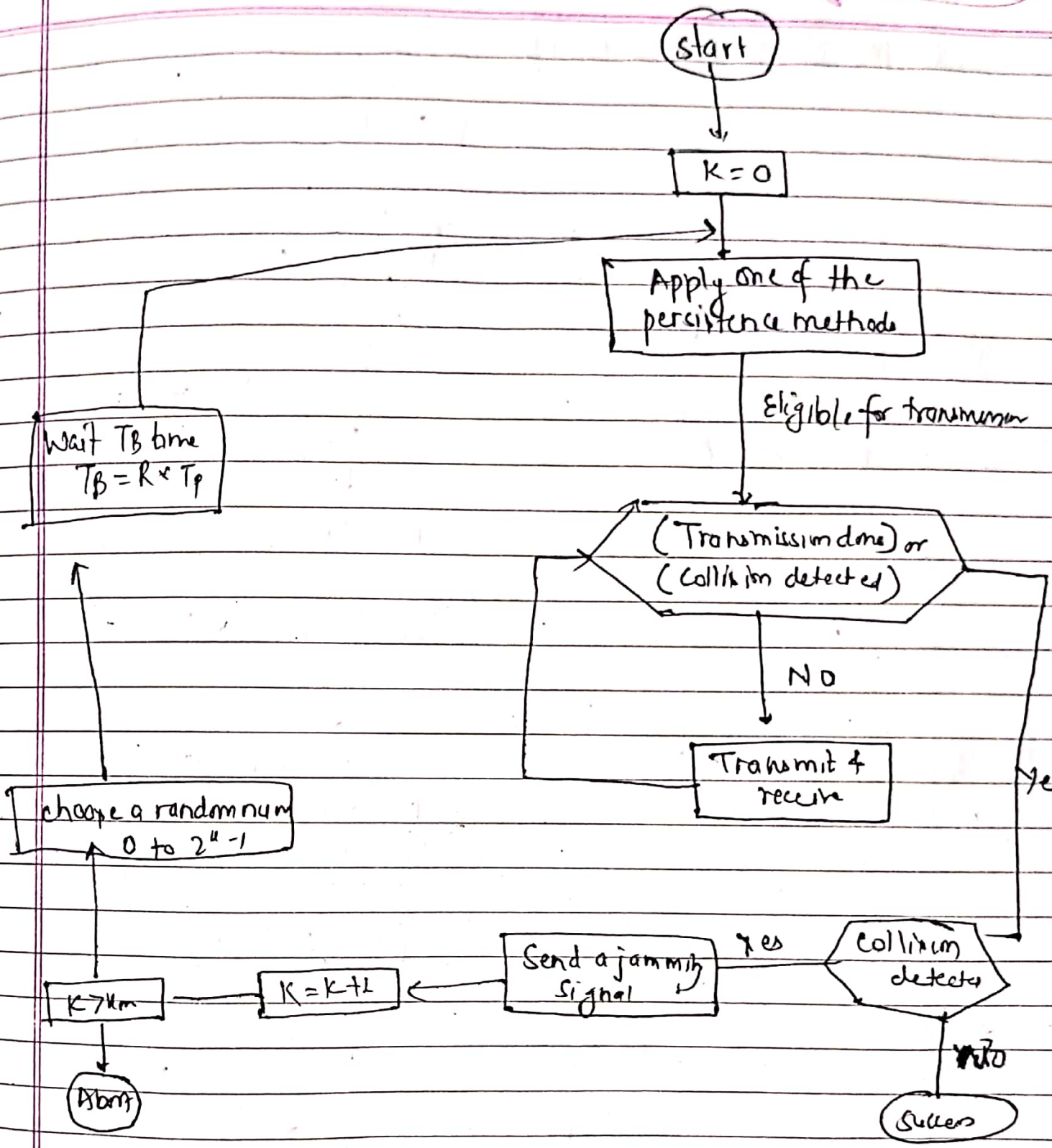
* CSMA/CD: [listen while Talk]

→ station monitors the medium after it sends a frame to see if it transmission was successful. If successful, transmittion is finished, if not, frame is sent again.

→ On top of CSMA, following rules are added to CSMA/CD:-

① If a collision is detected during transmission of a packet, the node immediately ceases transmission and it transmits jamming signal for a brief duration to ensure that all stations know that collision has occurred.

② After transmitting the jamming signal, the node waits for a random amount of time and then transmission is resumed.

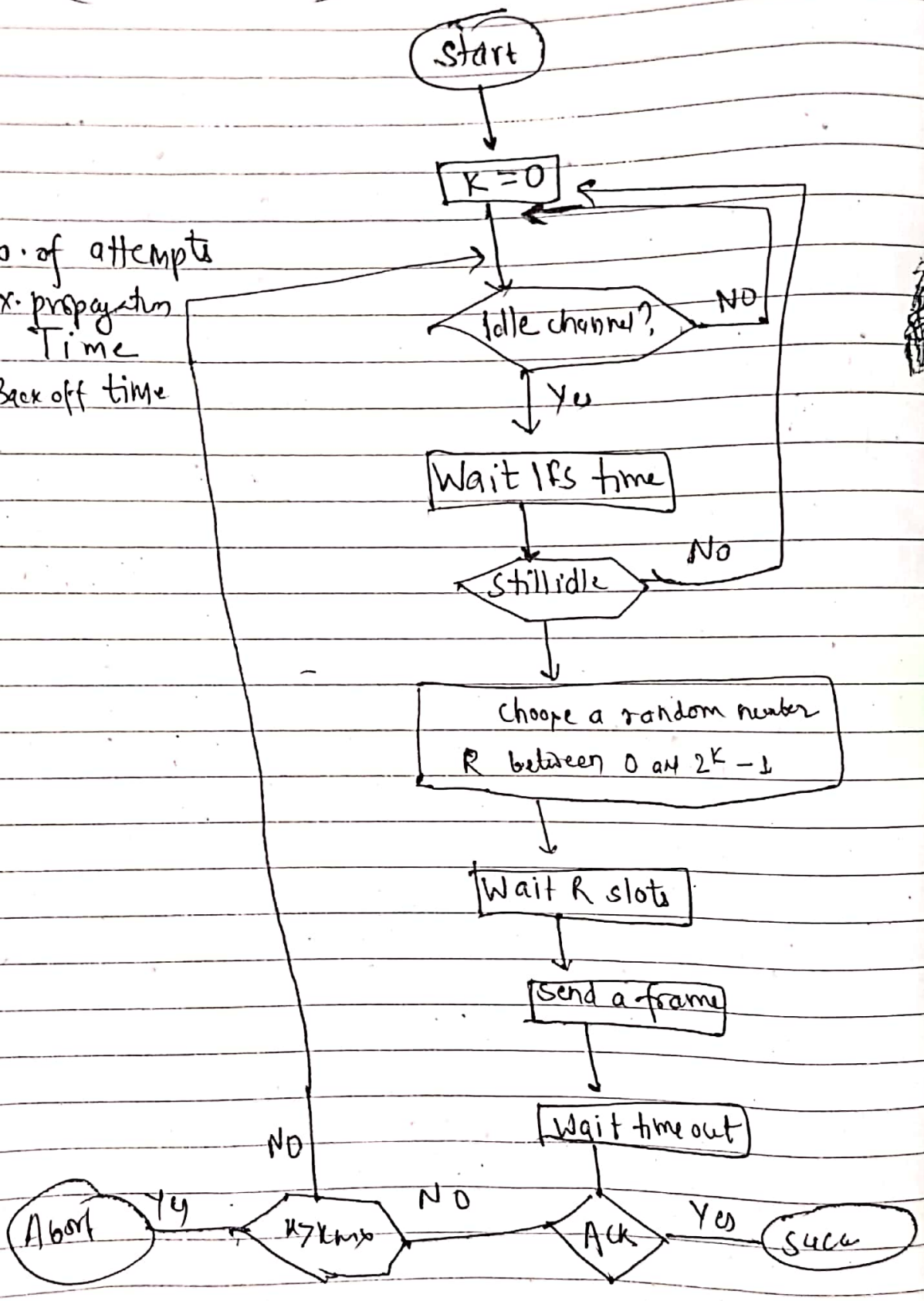

start
K=0
Apply one of the persistence methods
Eligible for transmission
(Transmission done) or (Collision detected)
NO
Transmit & receive
Yes
Collision detected
Yes
Send a jamming signal
K=K+1
K>Kmax
Abort
choose a random num 0 to 2^n - 1
Wait TB time TB = R * Tp
No
Success

CSMA CD :

→ P-persistence

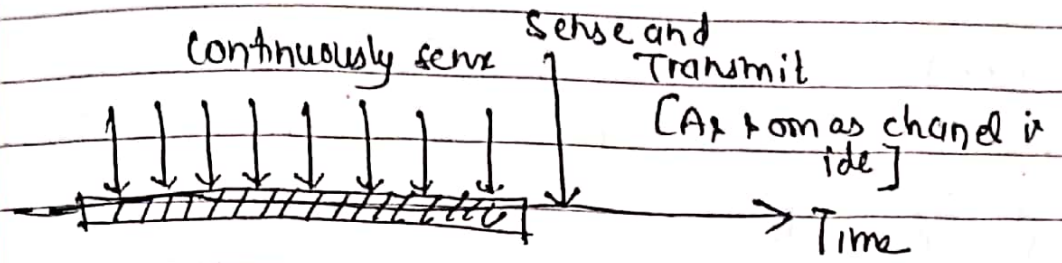
CSMA/CA (collision AVoidance)

K : No. of attempts
Tp : Max. propagation Time
T_B = Back off time

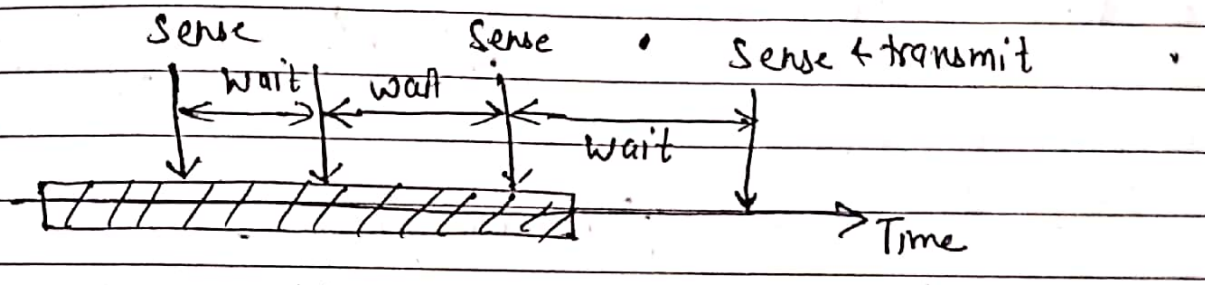


Persistant Methods:

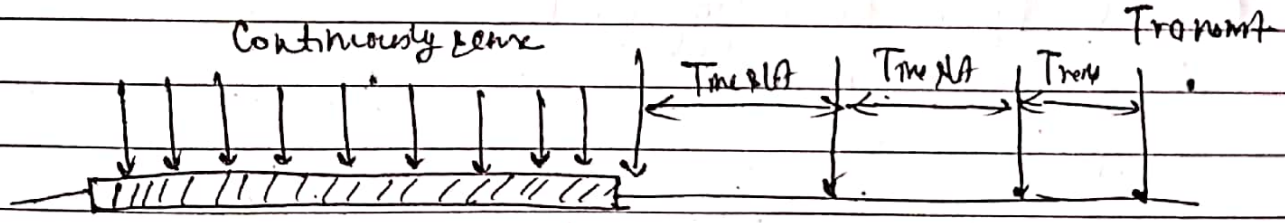
They describes what should a station do if channel is busy or idle.

(*) 

1- persistent

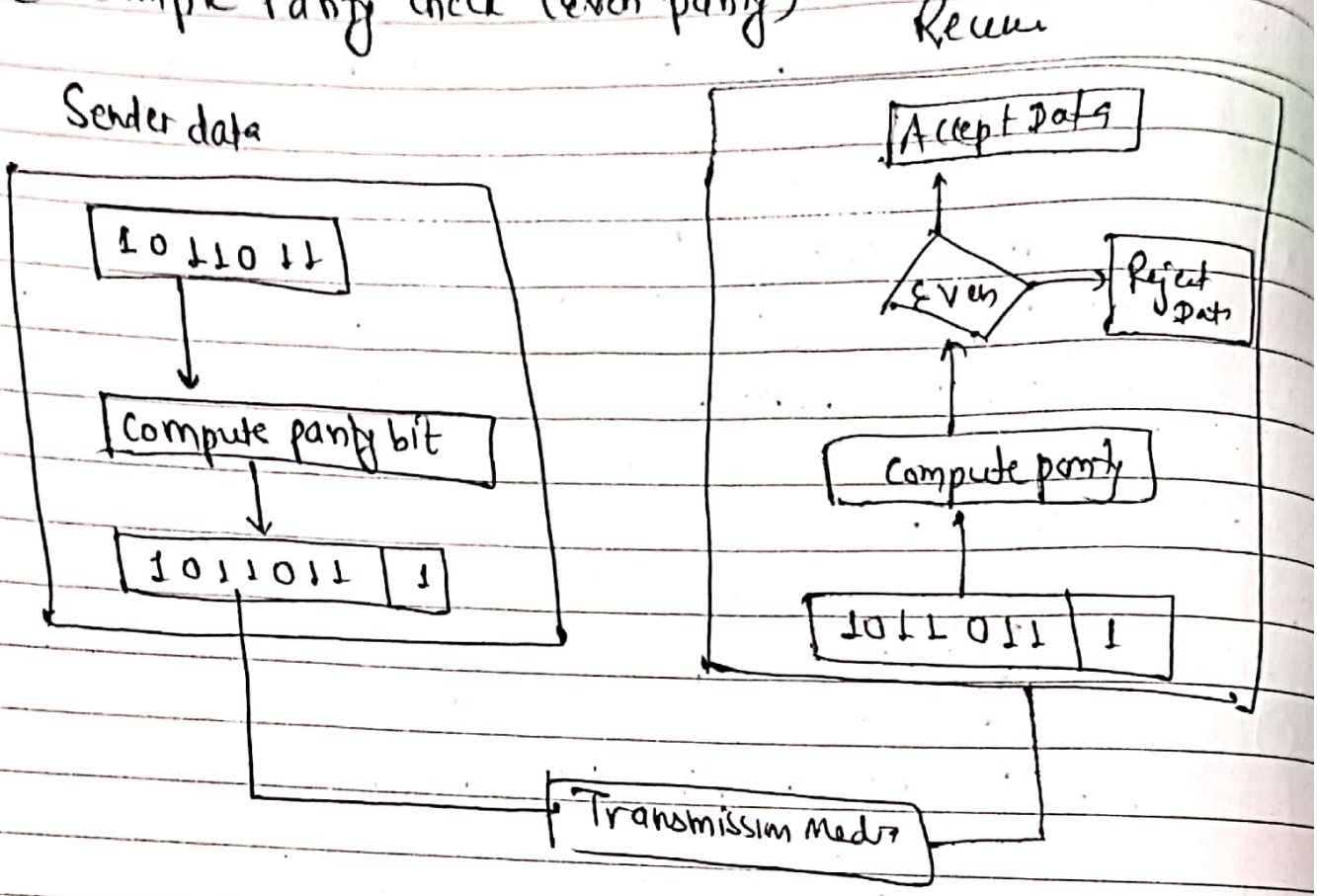
(*) 

Non-persistent

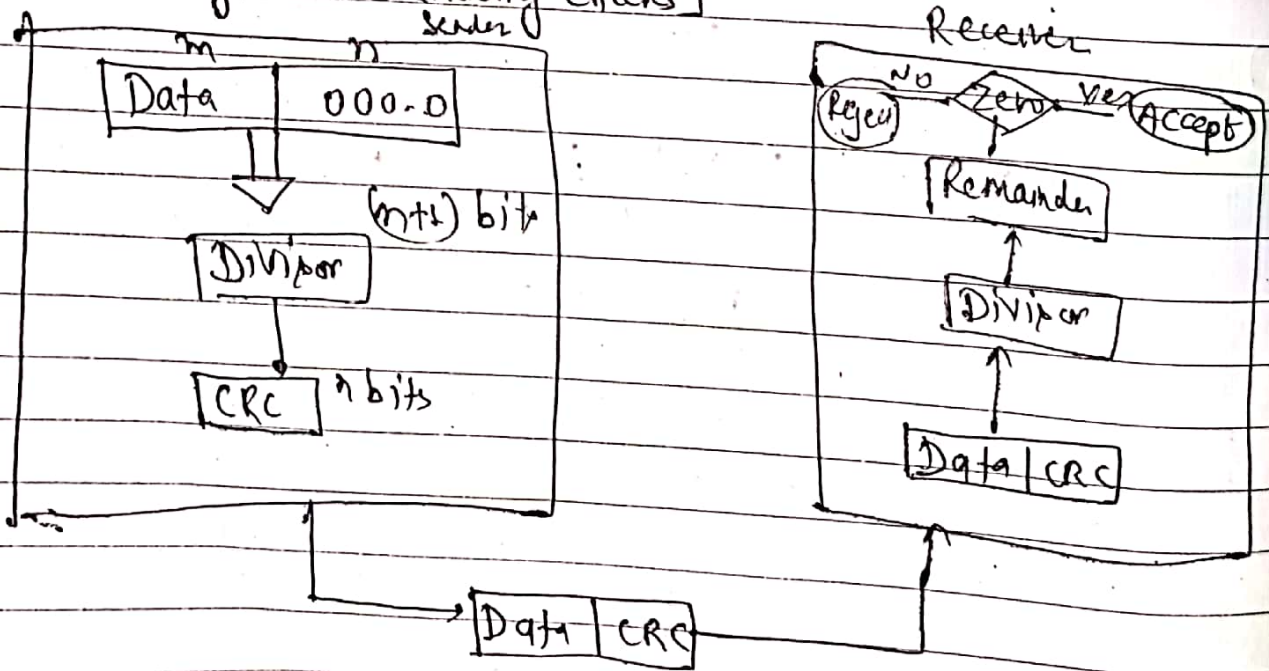
(*) 

p-persistent

① Simple Parity check (even parity)



② CRC [Cyclic Redundancy checks]



Eg: x^3+x+1 gives: 1011 (4 bits & no CRC = 3 bits)

Data is: 1101

```
        1111
     ┌─────────
1011 | 1101000
       1011↓
       ------
        1100
        1011↓
        ------
         1110
         1011↓
         ------
          1010
          1011
          ----
           001  ← CRC
```

So, data transmitted is 1101001.

Forward error Correction (FEC):

→ FEC is a digital signal procesing technique to enhance data realibility.

→ It does this by introducing redundant data, called error correction code, prior to data transmission.

→ FEC provides the receiver with ability to correct errors without a reverse channel to request retransmission of data.

→ The first FEC code is called Hamming code.

IPV4	IPV6
(1) It has 32-bit address length.	(1) It has 128-bit address length.
(2) IPV4 header includes checksum.	(2) It doesnot have header checksum.
(3) Header includes options.	(3) All the optional data is moved to IP V6 extension header.
(4) No identification of packet flow is available.	(4) Packet flow identification available using flow label within header.
(5) Broadcast addresses are available to send traffic to all nodes on a subnet.	(5) No broadcast address. Multicast and Anycast available.
(6) Both senders and routers fragment packets.	(6) only senders fragments packets, routers do not.
(7) Address representation is dotted decimal.	(7) Address representation is in hexadecimal separated by colon.
(8) The security feature is dependent on application.	(8) IPSEC is an inbuilt security feature in IPV6 protocol.
(9) Divided into five different classes (A, B, C, D, E)	(9) No any classes of IP address
(10) Eg:- 192.168.1.1	(10) Eg 2001:0000:3238:... 8 times

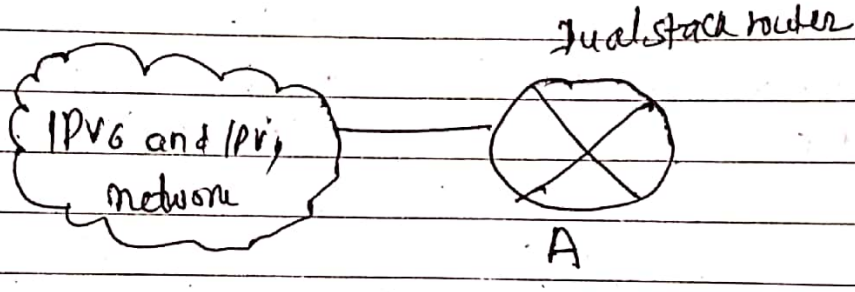
IPV6 transition mechanism: (sending request from IPV4 to IPV6)

1. Dual stack
2. Tunneling technique
3. Translation Technique

1. Dual stack:

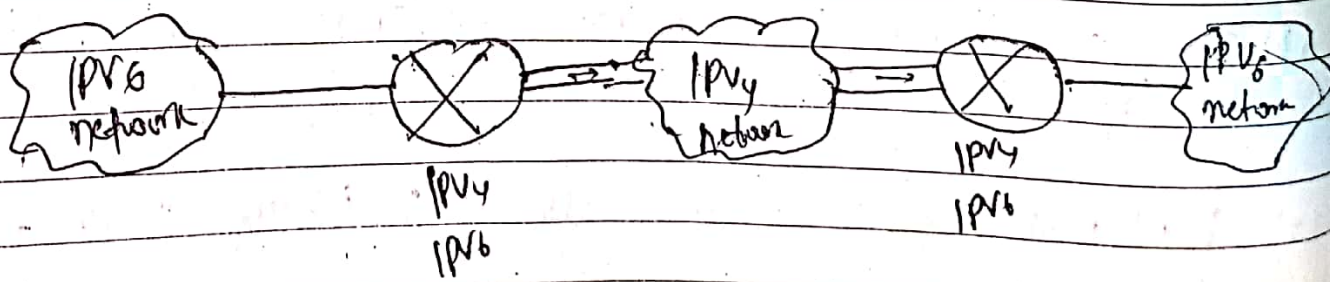
Dual stack is an integration method where a node has implementation and connectivity to both IPV4 and IPV6 network.

→ If both IPV4 and IPV6 are configured on an interface, this interface is dual stacked.



IPV4: 192.168.99.1
IPV6: 3ffe:b00:800:1::3

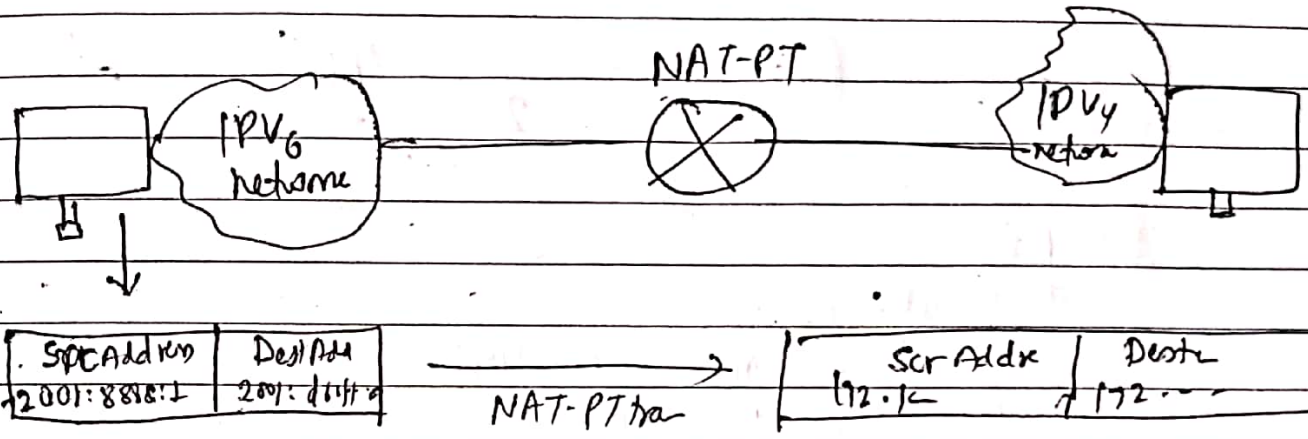
2. Tunneling Technique:



(Router/host at end of a tunnel should support both IPV4 & IPV6.)

(3) NAT - Protocol Translation (NAT-PT):

translates IPV4 packets to IPV6 & vice-versa.



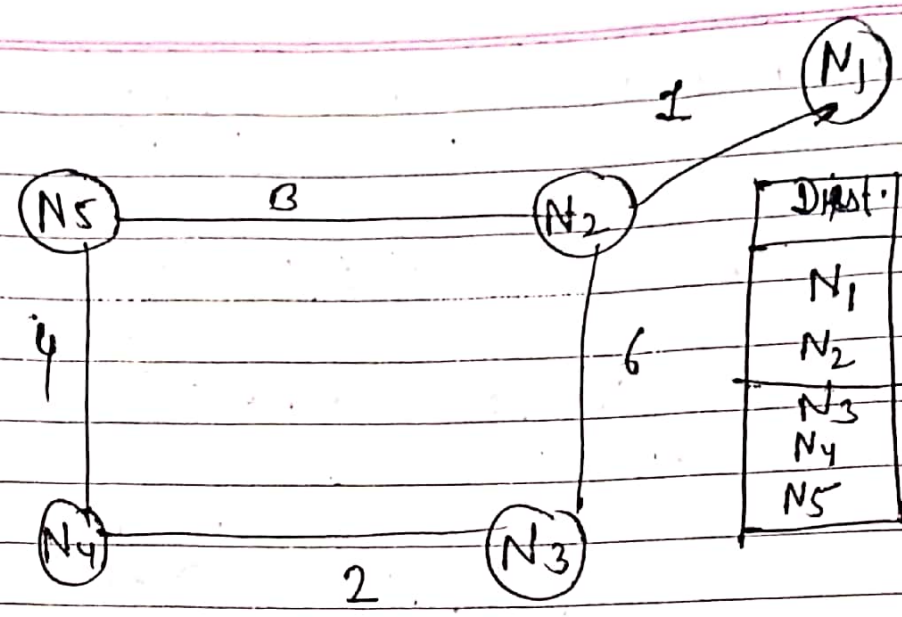
Router responsibility it to direct packets to destination by:

① Determining the best path to send packets
② forwarding packets towards their destination.

Distance Vector

N5

Dest.	Dist.	Next



Dest.	Cost	Next
N_1	0	N_1
N_2	1	N_1
N_3	∞	–
N_4	∞	–
N_5	∞	–

for N_2:

~~Distance~~

Destination	Cost	Next-Hop
N_1	1	N_1
N_2	0	N_2
N_3	6	N_3
N_4	∞	–
N_5	3	N_5

Now; N_2 shares distance vector <Dest, cost> with neighbor

At N_1: Update happens as:

~~Received~~:

Dest.	cost	Next-Hop
N_1	0	N_1
N_2	1	N_2
N_3	7	N_2
N_5	3	N_5

Border Gateway Protocol:

→ used to exchange routing information between ISP which are different autonomous systems.

→ This protocol can connect together any internetwork of autonomous system using an arbitary topology.

→ Only requirement is each Autonomous System have at least one router that is able to run BGP and that router is connected to least one other AS's BGP router.

Characteristics of BGP:

① → Inter-Autonomous System Communication

② Runs over TCP

③ Supports CIDR

④ Supports Security

BGP peers perform 3 functions, which are:

① The first function consist of initial peer acquisition and authentication. Both peers establish a TCP connection and perform message exchange that guarantees both sides have agreed to communicate.

(2) The second function mainly focus on sending negative or positive reachability information.

(3) The third function verifies that the peers and the network connection between them are functioning correctly.

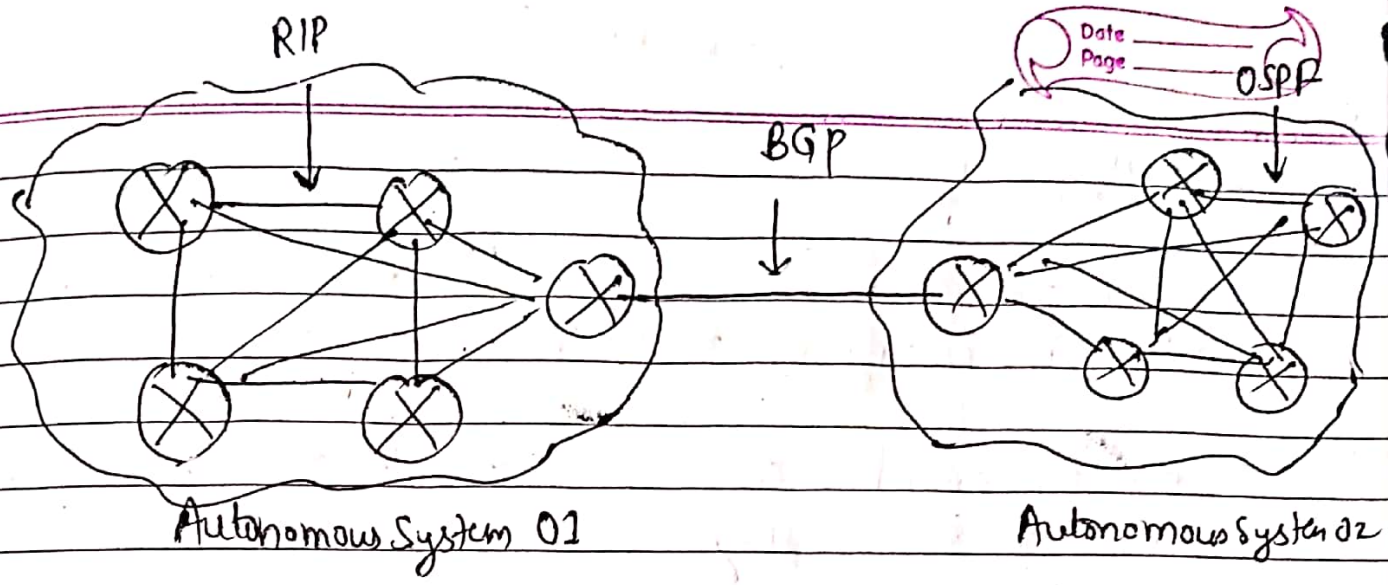
BGP Route Information Management functions:

(1) Route storage: → stores information about how to reach other networks.

(2) Route update: → special techniques are used to determine when and how to use the information received from peers to ~~peer~~ properly update routes.

(3) Route selection: which is the good routes to each network on internet.

(4) Route Advertisement: each BGP speaker regularly tells its peer what is known about various networks and method to reach them.



Ex: BGP

Causes → Bursty Traffic
→ Insufficient memory
→ Less Buffer Space
→ Less Processor

Congestion :

→ Condition which occurs when the load on a network is greater than the capacity of network (number of packets it can handle).

→ Congestion control refers to mechanisms to control the congestion and keep load below capacity.

- Congestion Control
  - Open-loop → Prevention
    - ① Retransmission policy
    - ② Window Policy
    - ③ Acknowledgement Policy
    - ④ Discarding policy (discard less sensitive packets)
    - ⑤ Admission Policy [check resource requirement of a flow before admitting it to network).
  - Closed loop - Removal
    - ① Back Pressure (to
    - ② Choke packet (to
    - ③ Implicit Signaling
    - ④ Explicit Signaling

Explicit Signaling → The congested node sends explicit signal to source or destination. In choke packets, separate packets is used but in explicit signaling, signal is included in the packets that carry data.

→ Backward Signaling → opposite direction of congestion → to source
→ forward Signaling → to destination that there is congestion slow it.

Traffic shaping :

→ mechanism to control amount and rate of data / traffic sent to network. Two techniques can shape traffic:

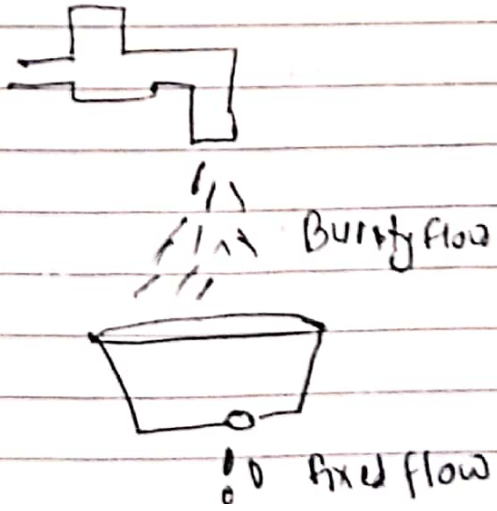
① Leaky bucket
② Token bucket

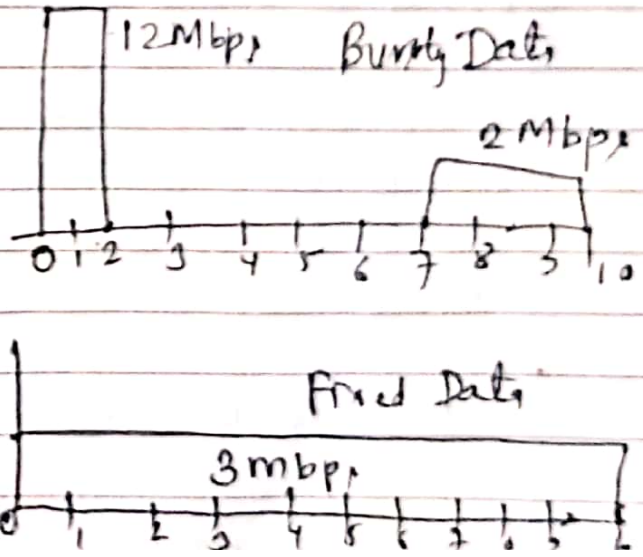
Traffic shaping is an approach to congestion management (prevention)

① Leaky Bucket

Suppose we have a bucket with a hole. The amount of water flowing out of the hole would be fixed irrespective of the flow input to the bucket as long as there is water in bucket. If there is bursty flow introduced to bucket, then also hole ensures the fixed rate.

The input rate can vary, but output rate remains constant. The leaky bucket can smooth out the bursty traffic. Bursty traffic data are stored in a bucket and sent out at an average rate.





We assume network has committed a bandwidth of 3 Mbps for a host. The use of leaky bucket shapes the input traffic to make it conform this commitment. In the above figure, the host sends a burst of data at a rate of 12 Mbps for 2s, for a total of 24 Mbits of data. The host is silent for 5s and then sends data at a rate of 2 Mbps for 3s, a total of 6 Mbits of data.

Without leaky bucket, the beginning burst may have hurt the network by consuming more bandwidth than is set aside for this host. We can also see that leaky bucket may prevent congestion.

Implementation:

→ A simple leaky leaky bucket algorithm can be implemented using FIFO queue. A FIFO queue holds the packets.

→ If the traffic consists of fixed-size packets (eg: cells in ATM network), the process removes a fixed number of packets from queue at each tick of clock.

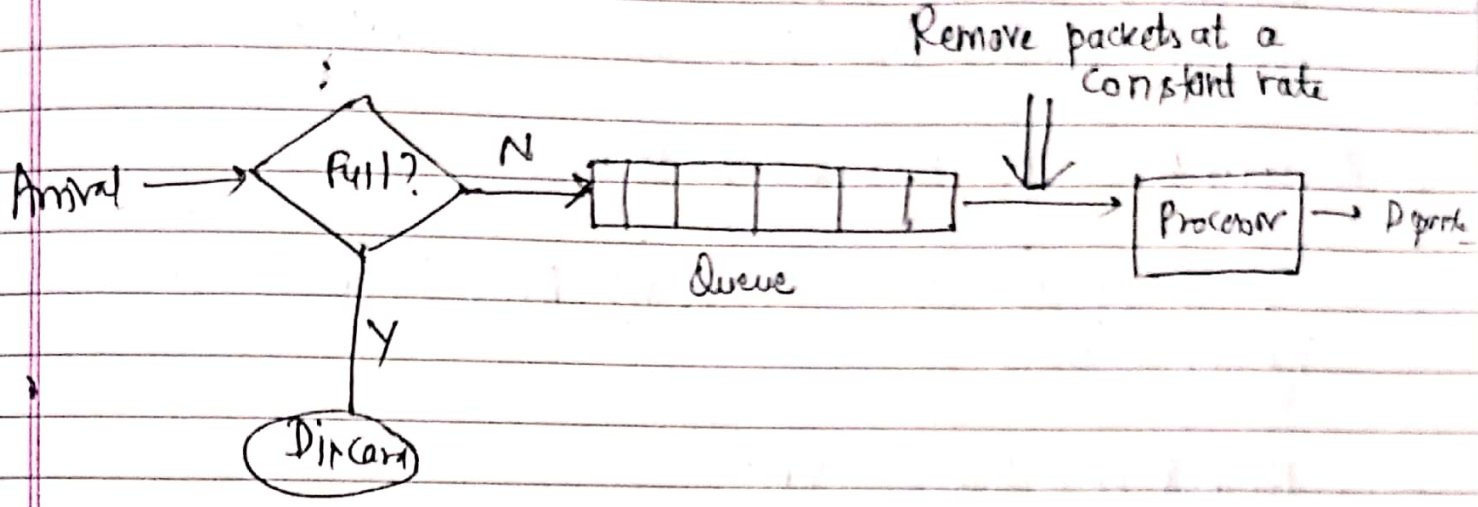
→ If the traffic consists of variable-length packets, the fixed output-rate must be based on the number of bytes or bits.

The following is an algorithm for variable length packets:

① Initialize a counter to n at tick of the clock.

② If ~~size of~~ n > size of packet, send the packet and decrement the counter by packet size. Repeat this step until n is smaller than the packet size.

③ Reset the counter and go to step 1.



A leaky bucket algorithm shapes bursty traffic into fixed rate traffic by averaging the data rate. It may drop the packets if bucket is full.

(2) Token Bucket :

→ The leaky bucket enforces a rigid pattern at output stream irrespective to pattern of input.

→ For many applications, it is better to allow the output to speed up somewhat when a larger burst arrives than to lose the data.

→ Token Bucket provides such a solution.

→ In token Bucket algorithm, leaky bucket holds token, generated at regular intervals.

Main steps of this algorithm:

(1) In regular intervals, tokens are thrown into the bucket.

(2) The bucket has a maximum capacity.

(3) If there is already a packet, a token is removed from bucket and packet is sent.

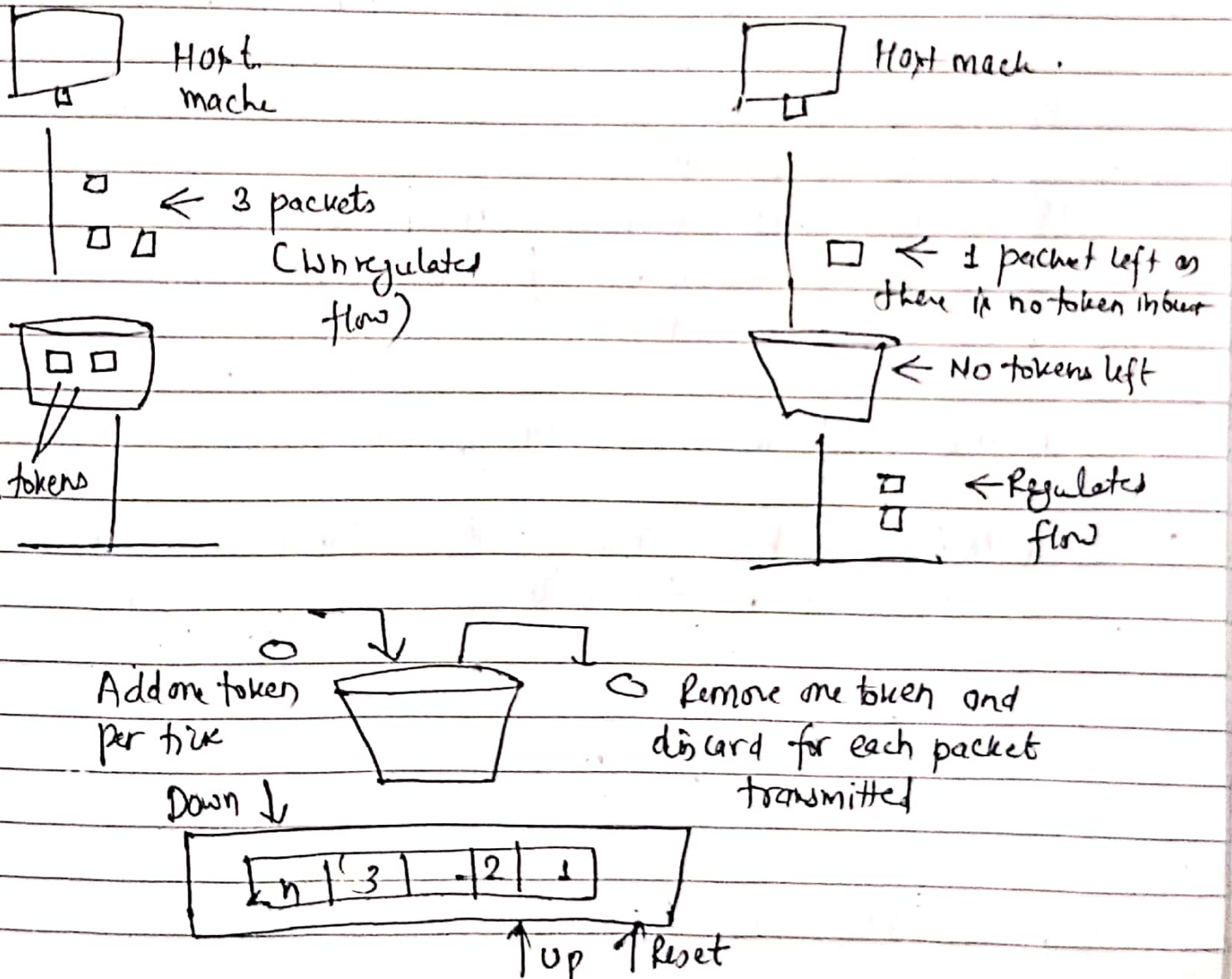
(4) If there is no token in the bucket, packet cannot be sent.

If a bucket has 2 tokens and 3 packets are waiting to be sent, two packets are sent out by consuming two tokens.

The token bucket is less restrictive than leaky bucket algorithm, in a sense, that it allows bursty traffic.

However, the limit of burst is restricted by number of tokens available in the bucket at a particular instant of time.

Implementation is simple. A variable is used just to count the tokens. This counter is incremented every t seconds and is decremented whenever a packet is sent. Whenever this counter is zero, no further packet is sent out.



TCP Congestion Control :

TCP uses a congestion window and a congestion policy that avoids congestion.

Congestion policy in TCP:

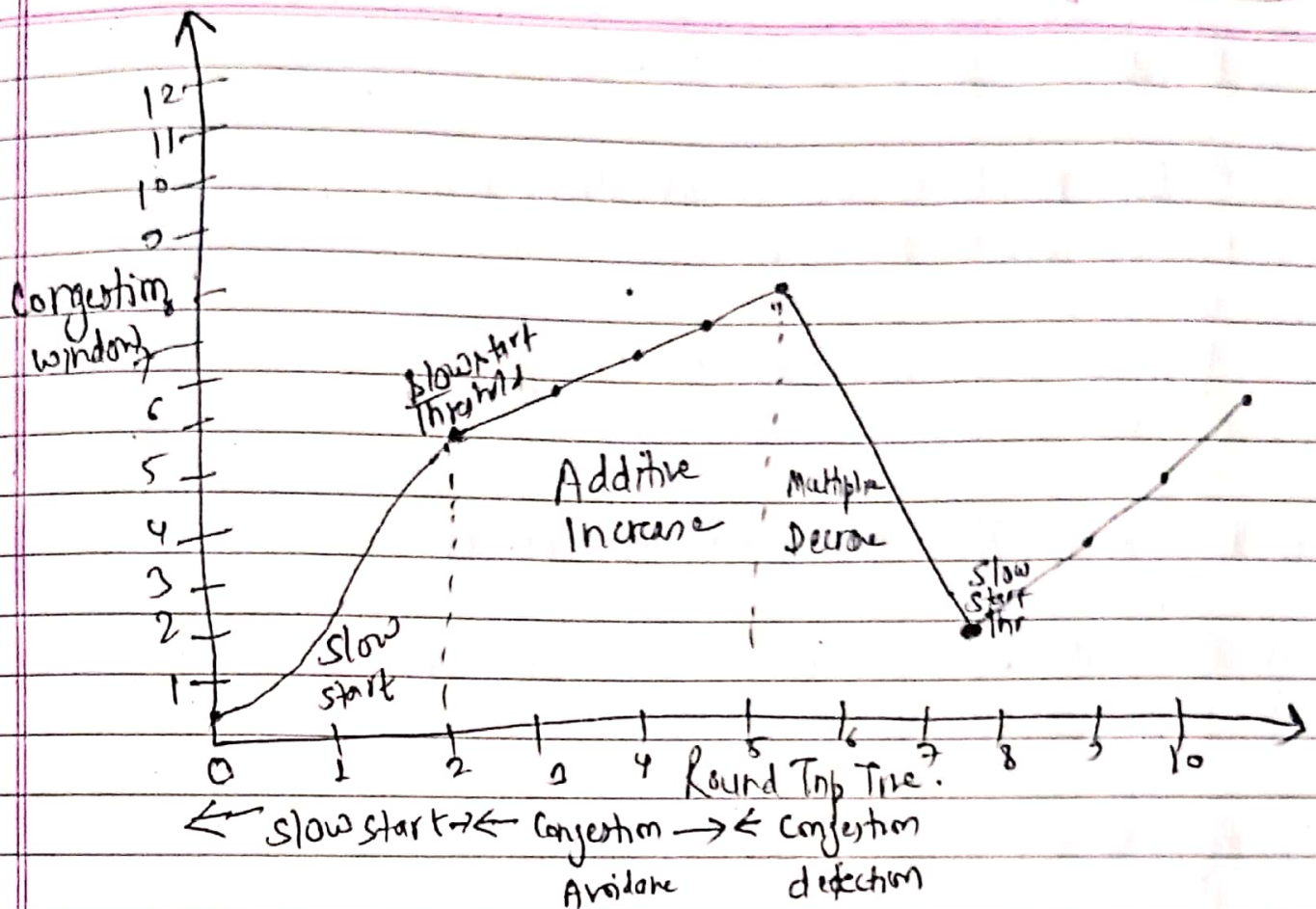
① Slow start phase = starts slowly increment is exponential to threshold

② Congestion avoidance phase: After reaching the threshold, window size is incremented by 1 (Additive increment)

③ Congestion ~~Avoidance~~ Detection Phase: Sender goes back to slow start phase or avoidance phase by multiplicative decrement.

AIMD – Additive increase multiplicative decrease

AIMD combines linear growth of congestion window with an exponential reduction when congestion takes place.



Congestion window $w(t+1) = \begin{cases} w(t) + a & \text{if congestion not detected} \\ w(t) * a & \text{if congestion detected} \end{cases}$

$a > 0$ & $0 < b < 1$.

Transport layer and Protocols :

→ Transport layer provides a logical connection between a source host and a destination host.

→ Primary duty is to provide end-to-end control and reliability as data travels through this.

→ The unit of data encapsulation in Transport layer is a segment.

→ End to end connection between hosts and preparing segments (Segmentation)

Protocols of Transport layer :

① TCP
② UDP

Services/ Responsibilities of Transport layer:

① End-to-End / Port-to-Port / Process-to-Process delivery:
Deliver data from port of source host to port of destination.

② Reliability:
(TCP) message are delivered to receiver as it as and in order. No loss of data

③ Error Control: checksum method (detect error)

④ Flow control (Stop & wait, Go back N, selective repeat)

⑤ Congestion control (AIMD)

→ TCP, UDP header format

→ TCP socket call for client & server

→ 3 tier architecture for distributed procesing in client/server. (Presentation Tier, Application Tier, Data Tier)

→ TCP Vs UDP with example

→ Definition of port & socket; UDP socket Vs TCP socket (port address)

→ Handshaking ; 4 way TCP handshaking

TCP :

→ Connection-oriented Transport layer protocol that provides reliable full duplex data transmission.

→ TCP breaks mesage into segments, reassembles them at destination and resends anything that is not received.

Key features :

→ TCP corresponds to Transport layer of OSI model.

→ Reliable and connection oriented.

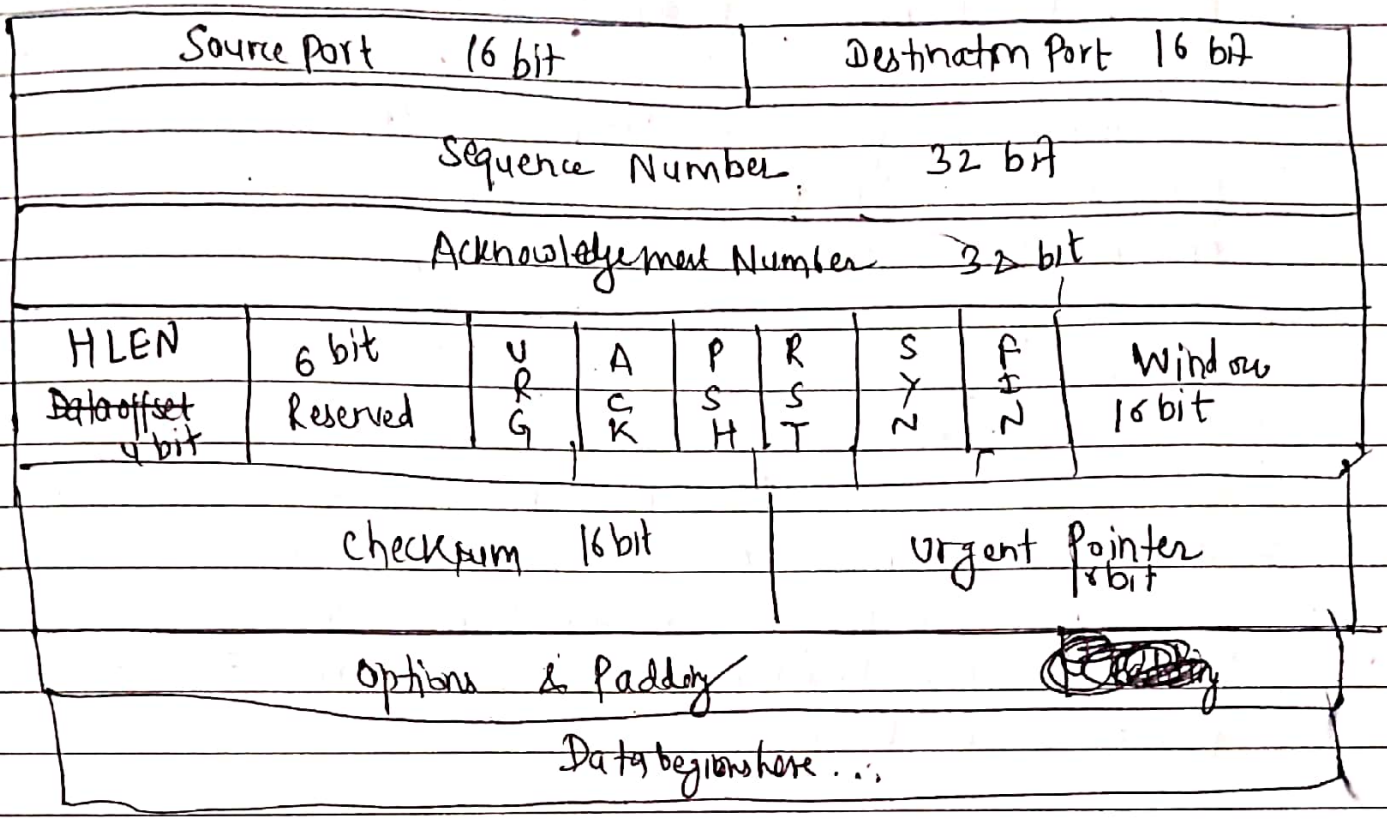
→ Efficient flow and congestion control

→ Acknowledgement and retransmits bytes not acknowledged.

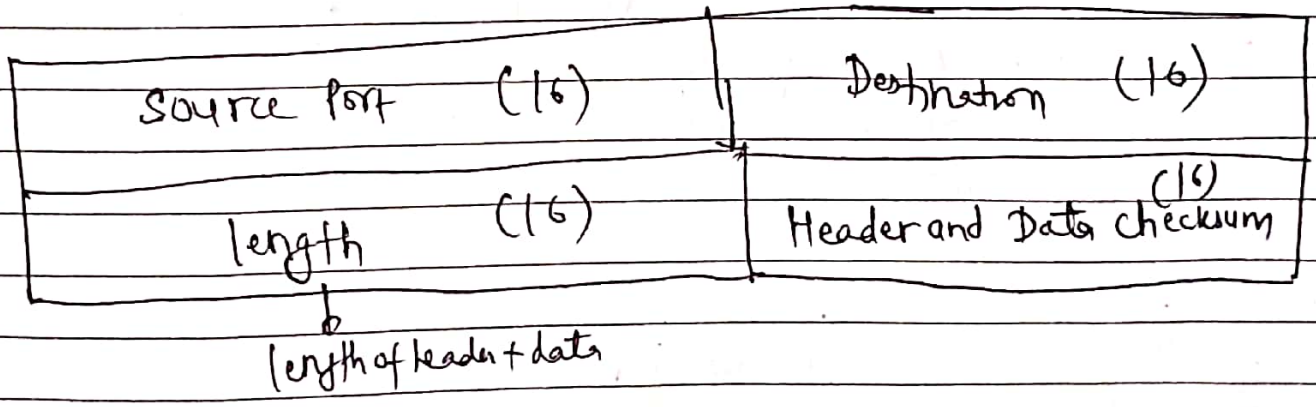
TCP services:

① Segmentation → Segment is a collection of bytes (Byte streaming)
② Connection Oriented Communication
③ Reliability
④ Full Duplex
⑤ Flow control
⑥ Congestion control.

TCP Header Format :



UDP Header Format :



TCP Handshake :

① 3 Way Handshake (Connection Establish)

Handshake procen is defined as the set of steps that take place in TCP for creating a secure and reliable communication link and also closing it.

Step 1 (SYN):

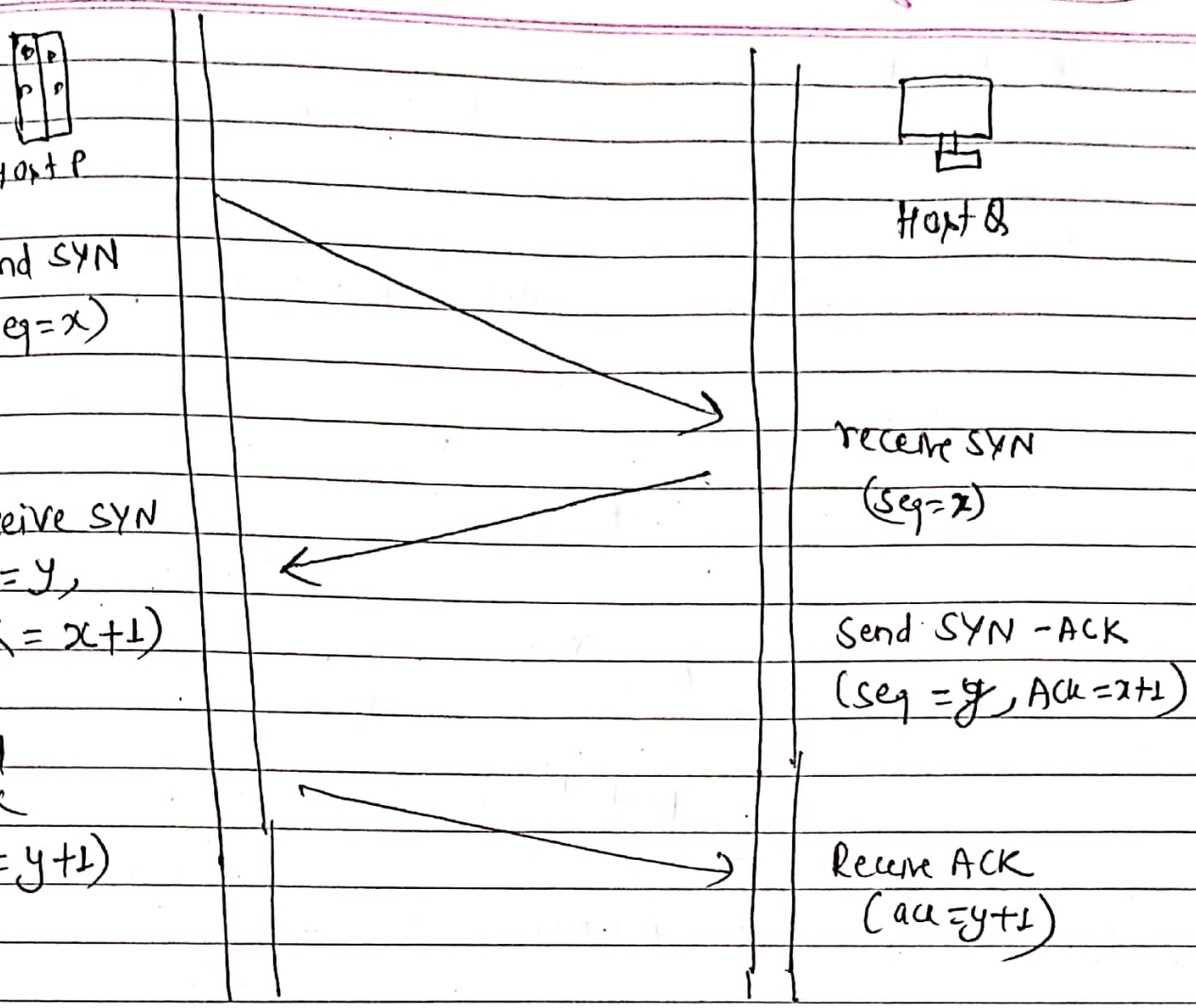
In first step, client wants to establish a connection with server, so it sends a segment with SYN (Synchronize Sequence number) which informs server that the client is likely to start communication and with what sequence number it starts segments with.

step2 (SYN + ACK):

Server responds to client with SYN-ACK signal. ACK signifies that response of segment it tereived and SYN signifies with what sequence number it is likely to start segments with.

step3 (ACK):

In final part client acknowledges the response of server and they both establish a reliable connection with which they start actual data transfer.



TCP Connection Termination (4 way Handshake):

① Suppose client want to close the connection.

① FIN M:

In first step, client sends a FIN flag indicating that it wants to terminate or close the connection

② ACK M+1 :

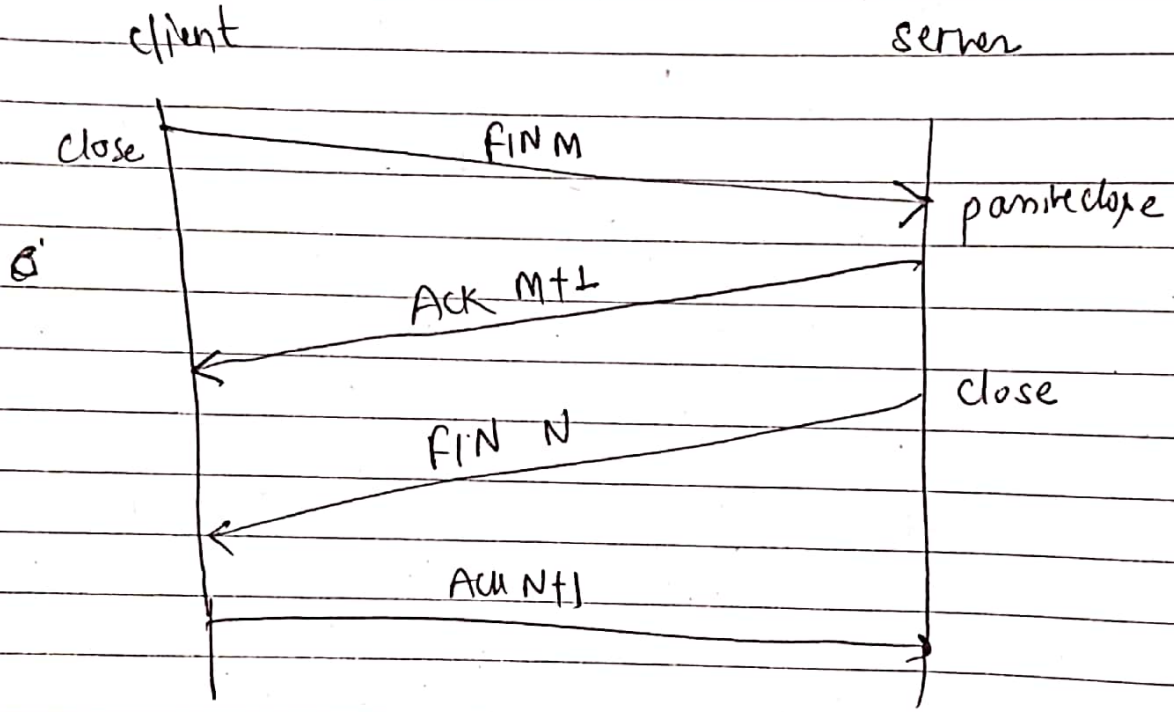
Server on receiving FIN performs passive close and sends an acknowledgment

③ FINN:

Server sends FIN signal to client

④ ACK N+1:

Client acknowledges FIN N with ACK N+1.



TCP VS UDP

TCP → Eg: HTTP/s, FTP, SMTP, Telnet

UDP → DNS, DHCP, RIP, VOIP

	TCP	UDP
①	TCP is a protocol of Transport layer that allows applications to send data reliably without worrying about network layer issues.	① UDP is a protocol of Transport layer that exchanges datagrams without guaranteed delivery.
②	Connection oriented; Connection must be setup prior to transmission.	② Connection less; data is sent without setup.
③	An acknowledgement segment is present.	③ No acknowledgement.
④	Sequencing of data so that packet arrives in order at the receiver.	④ No sequencing of data in UDP.
⑤	Comparatively slower.	⑤ Comparatively faster & simpler
⑥	Retransmission of lost packets	⑥ No retransmission of lost packet.
⑦	Uses handshakes (SYN, SYN-ACK, ACK)	⑦ It is connectionless so no handshake
⑧	No support for broadcasting.	⑧ Supports Broadcasting

Socket Programming:

→ Sockets are combination of IP address plus corresponding TCP/UDP ports.

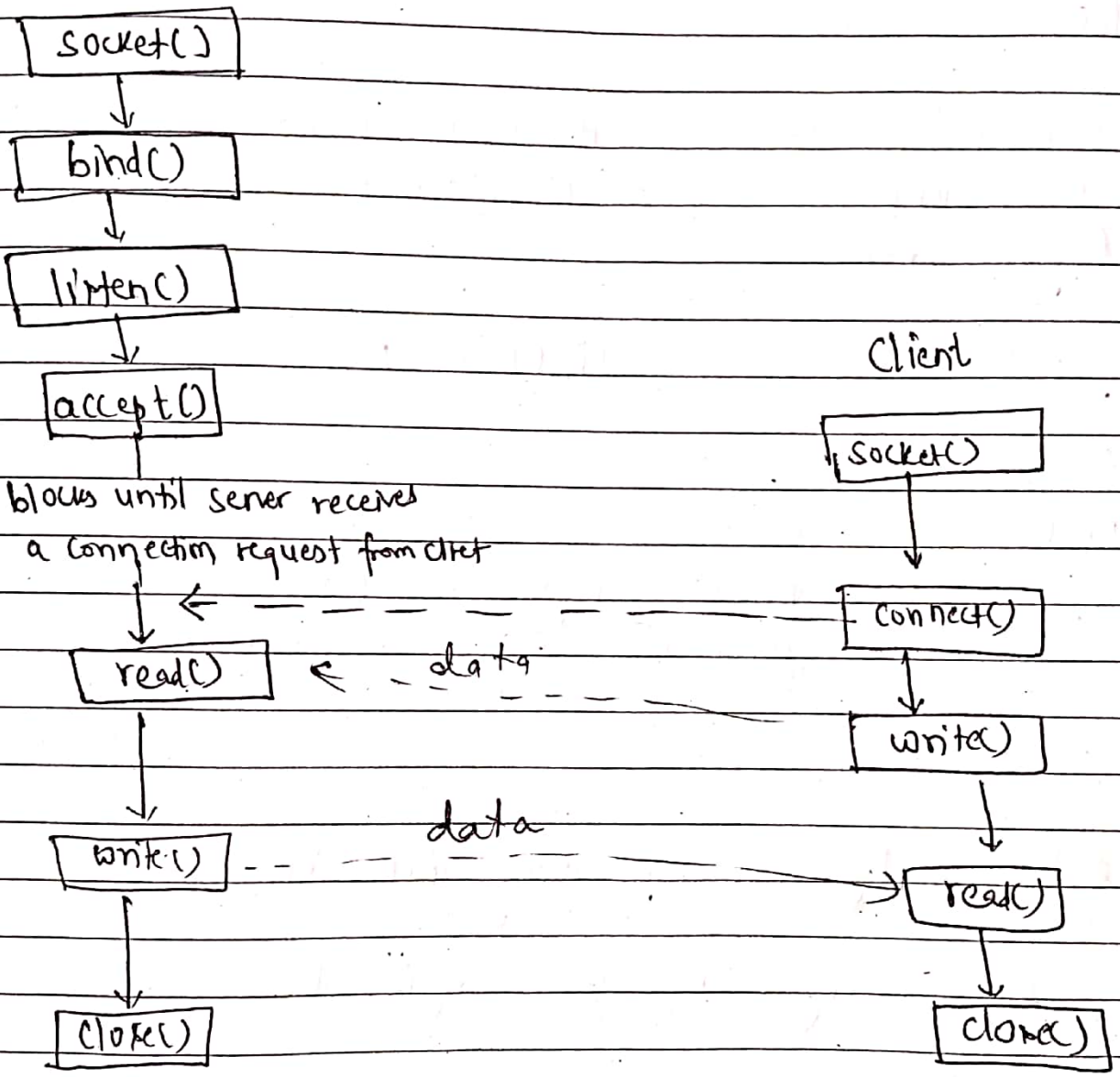
→ A socket is not a port. A socket is associated with a port through many-to-one relationship. ~~Each port can have a single~~ there can be only one listener socket for a given port.

Port is a service delivered by machine. Each and every service running will have a port number of 16 bit.

Types of sockets:

1. Stream sockets — TCP sockets [connection oriented, reliable]
2. Datagram sockets — UDP sockets [connectionless, no reliability]

TCP socket calls :



Application layer, Servers and Protocols:

① HTTP: port 80

→ Internet Protocol that specifies client/server interaction proces between web browsers such as Mozilla firefox and web servers such as Apache. Deliver resources.

- stateless GET, POST, PUT, PATCH, DELETE

HTTPs:

Secured version, encryption, HTTP over an encrypted secure sockets layer (SSL) - Prevents man in the middle attack.

② DHCP: (Dynamic Host Configuration Protocol)

The host in any network can be assigned IP address manually or dynamically.

for small networks, manual configuration is feasible.

But for large networks, manual configuration would be inefficient.

So, to resolve this DHCP is needed.

→ DHCP is needed to simplify the assignment of IP addresses on a network.

→ DHCP is a network management protocol that is used to dynamicly assign IP address and other information to each host on the network so they can communicate efficiently.

→ DHCP automates and centrally manages the assignment of IP address easily the work of network administration.

→ DHCP also assigns subnet masks, default gateway and Domain Name server (DNS) address, in addition to IP address.

How does DHCP works?

→ DHCP is a client server protocol that uses DHCP servers and DHCP clients.

→ A DHCP server is a machine that runs a service that can lease out IP addresses ~~and~~ to any clients that requests them. The DHCP server has a pool of IP addresses that is allowed to distribute to clients. and these clients lease an IP address from the pool for a specified period of time, usually several days. once the lease is ready to expire, the client contacts the server to arrange for renewal.

→ DHCP clients that are machines running special software that helps them to communicate with DHCP server.

Steps:

① DHCPDiscover:

clients broadcasts a request for DHCP server.

② DHCP offer:

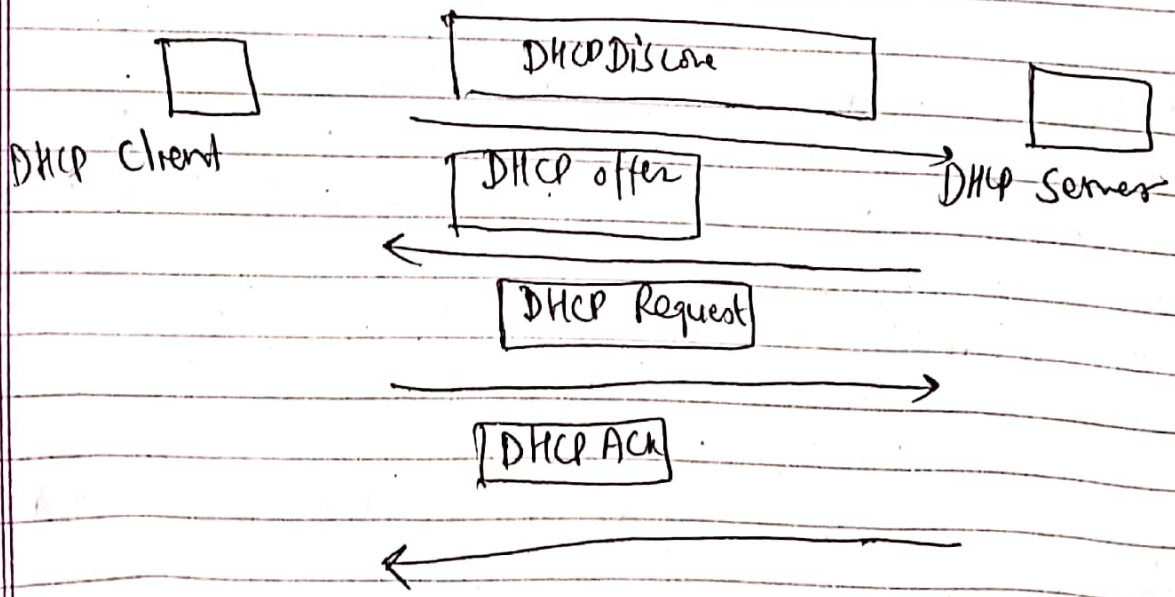
DHCP server on network offer an address to client

③ DHCPRequest:

client Broadcasts requesting configuration information sent in DHCP offer.

④ DHCPACK:

DHCP server acknowledge configuration information & begin lease.



Domain Name System (DNS) :

→ IP address are tough for human to remember. So, domain names such as py.edu.np are used. DNS are used to translate a host/Domain name (py.edu.np) to IP address (202.37.94.177).

DNS makes it possible to refer to IP based hosts in human friendly names (domain names).

Two Benefits of DNS:

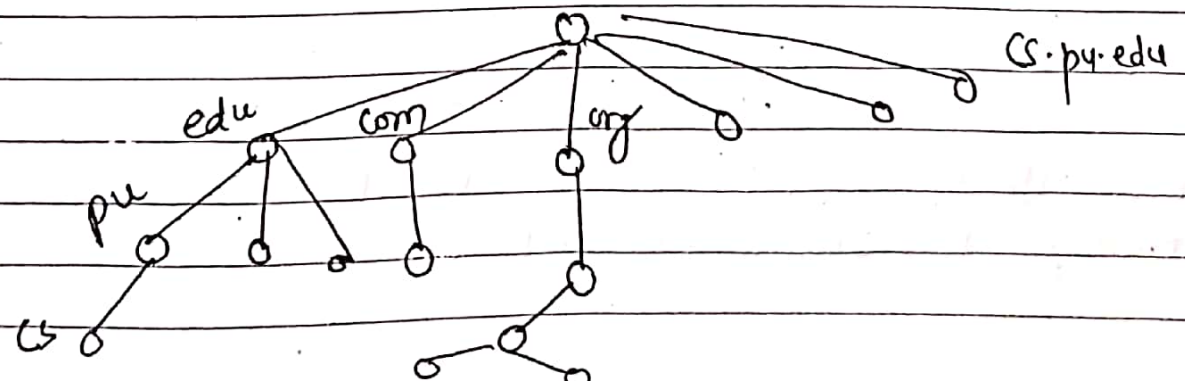
① Domain name can be logical and easily remembered.

② IP address of a host can change, domain name can still resolve transparently to users.

Domain Name Space:

To have hierarchial name space, domain name space was designed.

→ domain names are defined in inverted-tree structure with root at top. The tree can have only 128 levels: level 0 (root) to level (127)



A component called a DNS Resolver is responsible for checking if the hostname is available in local cache and if not contact a series of DNS name servers until it eventually receives the IP of service user is trying to reach and returns it to the browser or application.

3 types of DNS Query:

① Recursive:

→ DNS client provides a hostname and the DNS ~~component~~ Resolver must provide an answer - it responds with either a relevant resource record or an error message if it can't be found.

Resolver starts a recursive query process, starting from DNS Root Server, until it finds Authorative Name server that holds IP address for requested hostname.

② Iterative:

→ DNS client provides a hostname and DNS Resolver returns the best answer it can.

→ If in cache, returns them.

– If not, DNS resolver refers the DNS client to Root or another Authorative server which is nearest to required DNS zone.

→ The DNS client must then repeat the query directly against DNS server it was referred to.

③ Non-recursive Query:

→ A non-recursive query is a query in which DNS resolver already knows the answer.

→ It either immediately returns a DNS record because it already is in local cache or queries DNS Name server which is authrative for the record, to ensure that it holds correct data.

→ In both cases, there is no need for additional rounds of queries (like in recursive / iterative).

Types of DNS servers:

① DNS Resolver: (Recursive resolver):

Designed to receive recursive queries, which includes human readble hostname.

② DNS Root Server:

- rootserver is the first step in the journey from hostname to IP address.

- DNS extracts the top level domain from query eg: www.exam.com provides details for .com.

③ Authoritative DNS server:

→ They holds up the up-to-date information for a hostname.

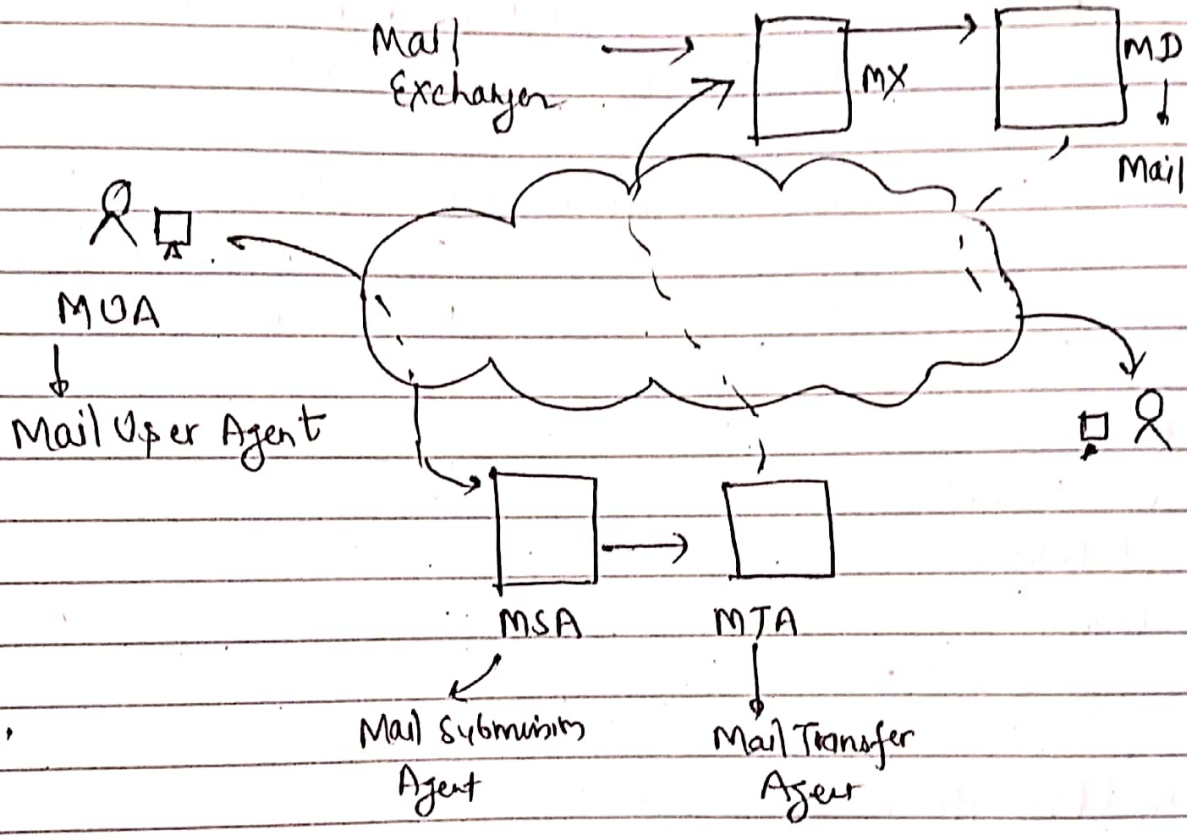
- They are the last stop in the name server query - it takes the hostname and returns correct IP address to DNS Resolver (or if it cannot find the domain name, returns NXDOMAIN message)

SMTP → Simple mail Transfer protocol

→ Sending mesage to one or more receipents

→ Sending mesage that includes texts, voices, videos or graphics.

→ SMTP support sending of email only. It cannot pull mesages from a remote server on demand (POP, IMAP can do that).



MTA uses DNS to look up mail exchanger for receipent's domain (part of address on right of @).

IMAP (Internet Mail Access Protocol) :→ Storing & retrieving messages from SMTP host.

→ SMTP provides underlying message transport for sending e-mail over Internet but it doesnot provide any facility for storing and retrieving messages.

→ IMAPv4 provides mechanisms for storing messages received by SMTP in a receptable called a mailbox.

→ IMAP server stores messages; IMAP server retrieves messages.

IMAPv4 includes a no. of features that are not supported in POP3.

① LIST (list of folders)
② Select
③ Fetch
④ Logout

POP (Post office Protocol)

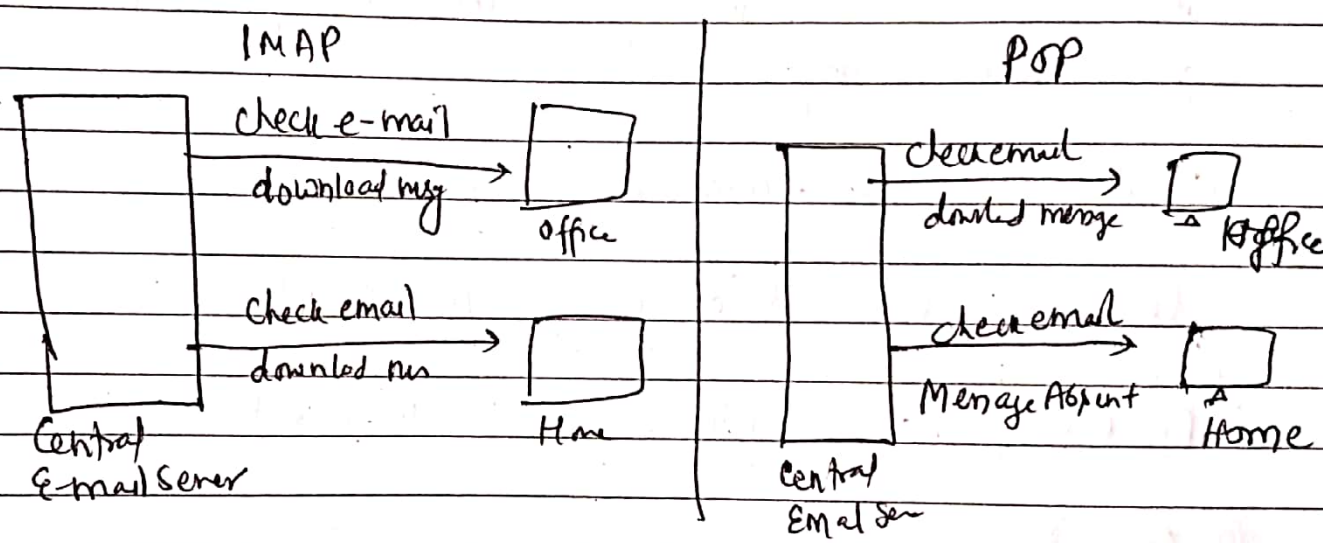
→ storing into mailbox.

① list (size of each message to be retrieved)
② retr
③ stat (no. of messages waiting to be retrieved)

POP vs IMAP

IMAP does not actually move/downloads messages on your computer. Messages remain in central mail server. It just displays them.

POP, does opposite. POP instead of just showing messages in mailbox, it downloads all the new messages in your inbox onto your computer and deletes them from server. Everytime we use POP to view new messages, they are no longer on central mail server.



VPN:

⇨ VPN is a technology that creates a safe and encrypted connection over less secure network such as Internet.

→ VPN is a way to create a private network over a public network infrastructure while maintaining confidentiality and security.

→ VPN uses cryptographic tunneling protocols to provide sender authentication, message integrity and confidentiality by protecting against packet sniffing.

→ VPN can be implemented at layer 2, 3 & 4 of OSI model.

* Components required to establish a VPN include:

① An existing network with servers and workstations

② Connection to Internet

③ VPN gateways that act as endpoints to establish, manage and control VPN connections (routers, PIX, ASA)

④ Software to create and manage tunnels.

Key to VPN is security.

→ Instead of using a dedicated, real world connection such as leased line, VPN uses virtual connections routed through Internet from company's private network to remote site.