Unit 3

Network Layer

IP ADDRESS → IPV4 → 32 bit
(Public globally unique)
→ IPV6 → 128 bit

Routing
IP ADDRESSING
IP
ARP
RARP

IP ADDRESSING / LOGICAL ADDRESSING

IPV4 → Binary → 11000111 ____ ____ ____
→ Dotted Decimal
Address space 2^{32} → 192 . 168 . 10 . 1

IPV4 classes

		I byte	II byte	III byte	IV byte
0	A	0-127	____	____	____
10	B	128-191	____	____	____
110	C	192-223	____	____	____
1110	D	224-239	____	____	____
11110	E	240-255	____	____	____

* Divide 32 bits in 4 octate

11110010 10101100 00010010 00000011

- Also divided in 4 octate, each bite is represented by a decimal number seperate by a 'dot (.).
→ 192.168.10.1

IPV4 is addresing is of 2 types
1. class full addresing
2. classless addresing

class full

IPV4 are divided into 4 classes, class A, B, C, D, E

Q Find the error if any in the following IPV4 Addresses
=
1) 111.56.045.78 => 111.56.45.78
2) 221.34.7.8.20 => Must have 4 octate
3) 75.45.301.14 => maximum number is 255
4) 11100010.23.14.67 => Either bitary or decimal

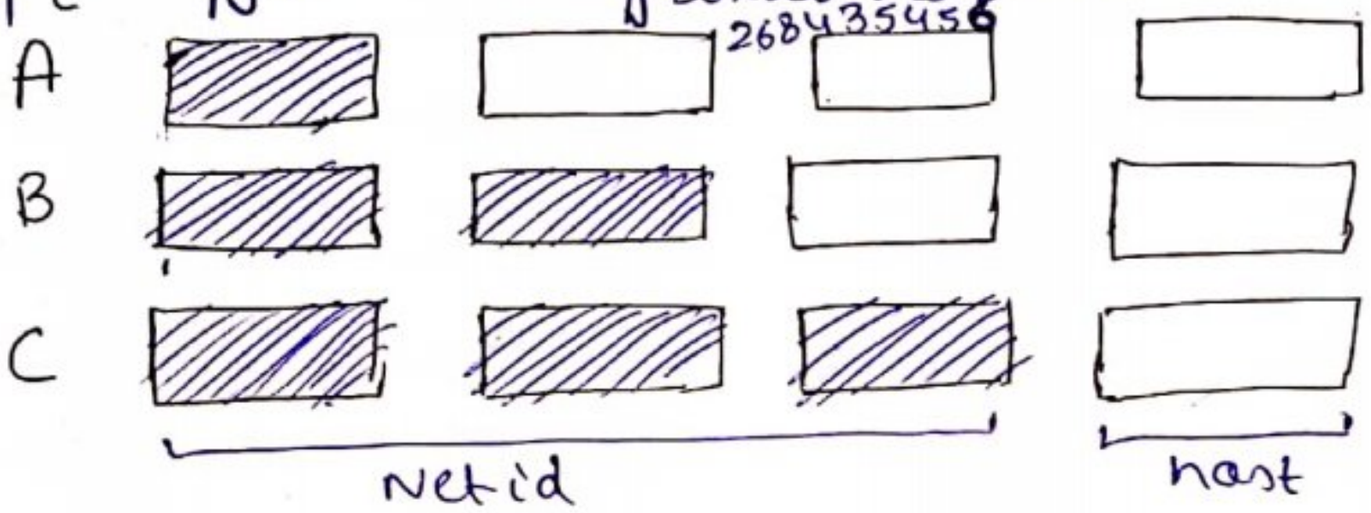
Net id & Host id

→ Net id

→ Host id

} only for class A, B, C

class	~~Net id~~ No of blocks	Block size	Application.
A	128	256×256×256 16777216	Unicast
B	64×256 16384	256×256 65536	Unicast unicast
C	32×256×256 2097152	256	multicast
D	1	16×256×256×256 268435456	Future use {Reserved}
E			



This is applied to class A, B, C only, net-Id defines network and host-id define the host

Q

192.168.10.1

Net id → 192.168.10

Host id → 1

Network address → 192.168.10.0

Host address → 192.168.10.1

185.68.65.29

Net id → 185.68

Host id → 65.29

Network address → 185.68.0.0

Host address → 185.68.65.29

Mask :- It is the combination of some continous 1 and some continous 0, it is 32 bit number, this concept doesnt apply to D and E. The mask can helps us to find netid and Hostid

A → /8 11111111 00000000 00000000 00000000 255.0.0.0
B → /16 " 11111111 " " 255.255.0.0
C → /24 " " 11111111 " 255.255.255.0

CIDR notation In Classless Addressing

In this scheme there is no class but addresses are still granted in blocks. In this addressing an organisation is granted a block of Addresses. The size of the block is based the nature and size of the organisation. Thes blocks are provided by ISP.

Restrictions

1. Contigious Address: The IP addresses in a block must be contigious one after another.
2. The number of IP addresses in a block must be power of 2 i.e 2^n.
3. The first address in a block must be evenly divisible by number of addresses in the block.

=> 205.16.37.32 } 16
⋮
.47

=> $205 \times 256^3 + 16 \times 256^2 + 37 \times 256 + 32 \times 28$
=> 3440387360 /16
=> 215024210 Seven

- Mask for classless

A betterway to define a block of addresses is to select any any address in the block and the mask.
In classless addressing the mask is any number between 0 & 32 and it is denoted in CIDR notation. In IPv4 Addressing any block can be defined as {x.y.z.t/n} where x.y.z.t is

any address of the block and n is the mask of that block

Q A block of address is grated to a small organisation and it is defined as 205.16.37.38/28 find the first address last address, of the block & no of addresses in the block

=> 205.16.37.38 /28

11111111.11111111 11111111 11110000

255.255.255.240

→ First address.

Replace last 32-n bits to 0

32-28

11111111 11111111 11111111 00100000

32

→ last address

→ Replace last 32-n bits to 1

11111111 11111111 11111111 00101111

47

→ no of address

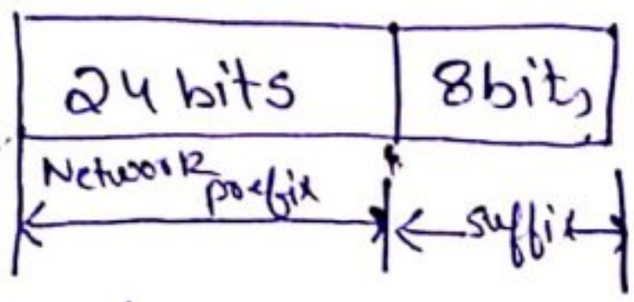
2^{32-n} $\Rightarrow 2^{32-28} = 2^4 = 16$

11110000
00100110
00100000

Subnet

If any organisation is granted a large block of addresses, it could be divide the addresses into several contgious group and assign each group to smaller networks, the smaller networks are called Subnet and this process is called Subnetting, Subnet is used in both classful and classless addressing

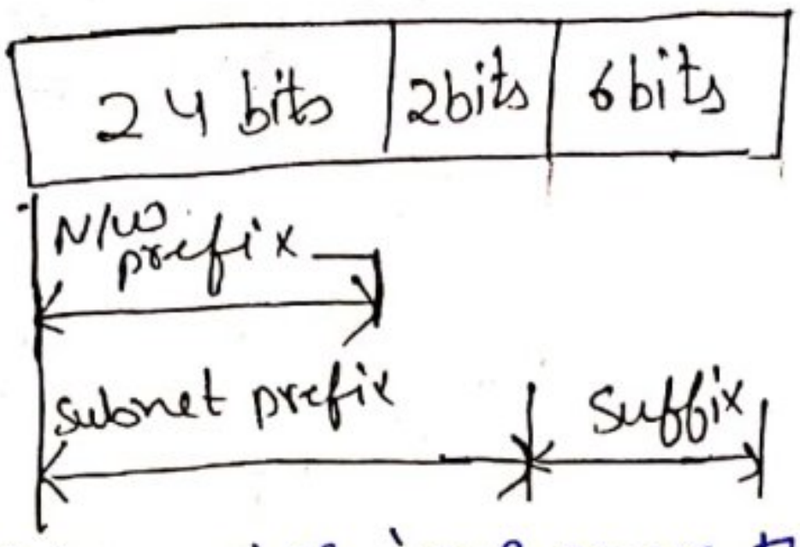
1. Two Level Hierarchy (No Subnetting)



Each address in a block can be considered as a 2 level Hierarchal structure the left most n bits define the network and rightmost 32-n bits define the host. The

prefix is common to all addresses in the network and the suffix changes from one device to another

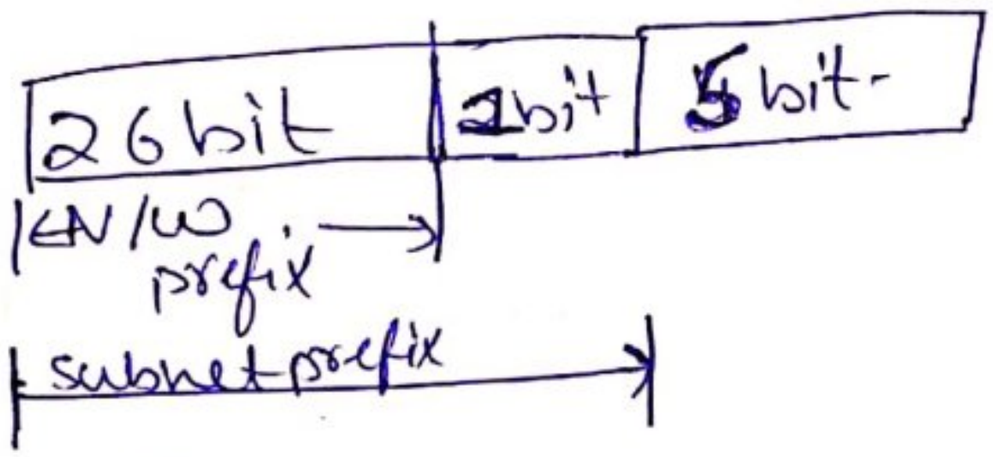
2o 3 level Hierarchy (Subnetting) 26-2--4



Subnetting will increase the number of continous '1' in network mask, in subnetting a large block of addresses is divided between different subnet but the rest of the work still sees the organization as one entity. All the messages are send to the router address that connects the organisation to rest of the internet. The router routes the message to the appropriate subnet

The organisation has its own mask and subnets have also its own mask.

Q A organisation has granted a block 17.12.40.0/26, the organisation want to create 3 offices which needs 32,16,16 address respectively design the subnet



$n_1\ n_2\ n_3$

$2^{32-n_1} = 32 = 2^5$

$n_1 = 27$

$2^{32-n_2} = 16 = 2^4$

$n_2 = 28$

$2^{32-n_3} = 16 = 2^4$

$n_3 = 28$

17.12.40.0 } Subnet 1 /22

17.12.40.31 }

17.12.40.32 } Subnet 2 /28

17.12.40.47 }

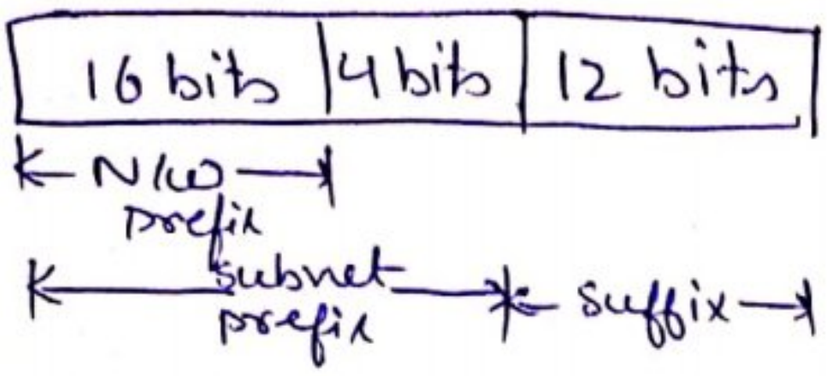
17.12.40.48 } Subnet 3 /28

17.12.40.63 }

Q A class B network has a subnet mask of 255.255.240.0 find the subnet number and host number

255.255.240.0

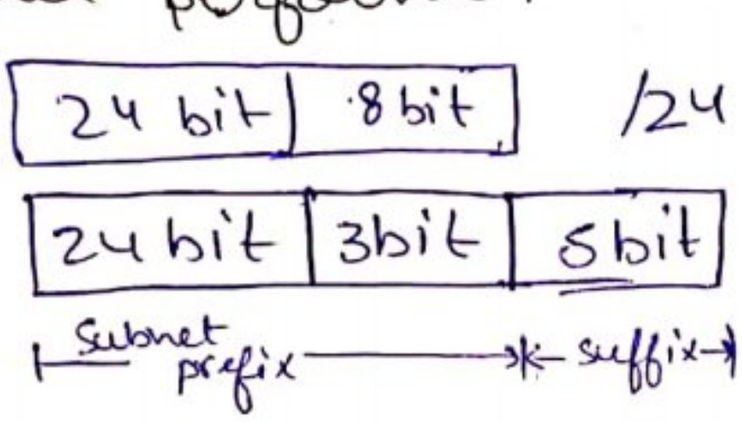
11111111.11111111 11110000 00000000



Subnet number $= 2^4 = 16$

Host number $= 2^{12} = 4096$

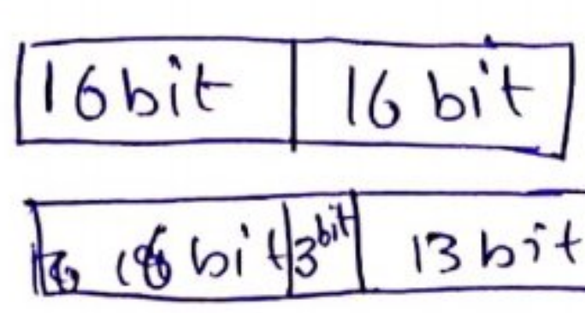
Q A company is granted a site address 201.70.64.0 the copay needs 6 subnet perform the subnetting.



000
001
010
011
100
101
110
111

1. 201.70.64.0 – 201.70.64.31
2. 201.70.64.32 – 201.70.64.63
3. 201.70.64.64 → 201.70.64.95
4. 201.70.64.96 → 201.70.64.127
5. 201.70.64.128 → 201.70.64.159
6. 201.70.64.160 → 201.70.64.191

Q Perform the subnetting of the following IP address 160.111.x.x
no of subnet = 6



000
001
010
011
100
101
110
111

160.111.64.0 – 160.111.95.255
160.111.96.0 → 160.111.127.255
160.111.128.0 → 160.111.159.255
160.111.160.0 → 160.111.191.255
160.111.192.0 160.111.223.255
160.111.224.0 160.111.255.255

— — 01000000.00000000 to — — 01011111.11111111

Q What is the Subnet address if destination address is
= 200.45.34.56 and subnet mask is 255.255.240.0

mask = /26

n=20

32-n=12

⇒ 12 right most bits to 0

200.45.001.00000.00000000

200.45.32.0 Ans.

⇒ 12 right most bit to 1

200.45.001 11111.11111111

200.45.63.255

Q. Show by calculation how many networks each IP class can have.

Q2 How many hosts per network in each IP class can exist
Show with example

		N/W	Host
Q1 = Class A	0	2^7	2^{24}
Class B	10	2^{14}	2^{16}
C	110	2^{21}	2^8
D	1110	1	2^{20}
E	1111	1	2^{20}

With Explanation

IPv6 Address (128 bits)

address space $= 2^{128}$

It can be denoted in 2 ways

1- binary notation (128 binary bits)

2. Hexadecimal colon notation

128 bits = 16 Byte

1 byte = 2 Hexadecimal digit

So 128 bits = 32 Hexa decimal digit,

In Hexadecimal colon notation, each 2 byte is written in Hexadecimal digit seperated by double colons.

Eg

FDEC:0074:0000:0000:0000:BOFF:0000:FFFF

=> First Abbreviation.

Drop out leading zeros

FDEC:74:0:0:0:BOFF:0:FFFF

=> Second Abbreviation

From left side remove continous zeros and put double colon in plac of zeros

This can only be done once from left side.

FDEC:74::BOFF:0:FFFF

Q Expand the address 0:15::1:12:1213

=> Opening 2nd Abbvt

0:15:0:0:0:1:12:1213

=> Opening 1st Abbvt

=> 0000:0015:0000:0000:0000:0001:0012:1213

NAT {Network Address Translation}

NAT Enables a user to have large set of address internally and one address or a small set of addresses eternally the traffic inside use the large set and traffic outside use the small set To seperate the addresses used inside the home or business and one used for internet, the internet authority has reserved 3 set of addresses as private addresses. Any organisation can use addresses out of these sets without permission from the internet authority (IANA). Everyone knows that these reserved addresses are for private networks. They are unique inside the organisation but they are not unique globally.

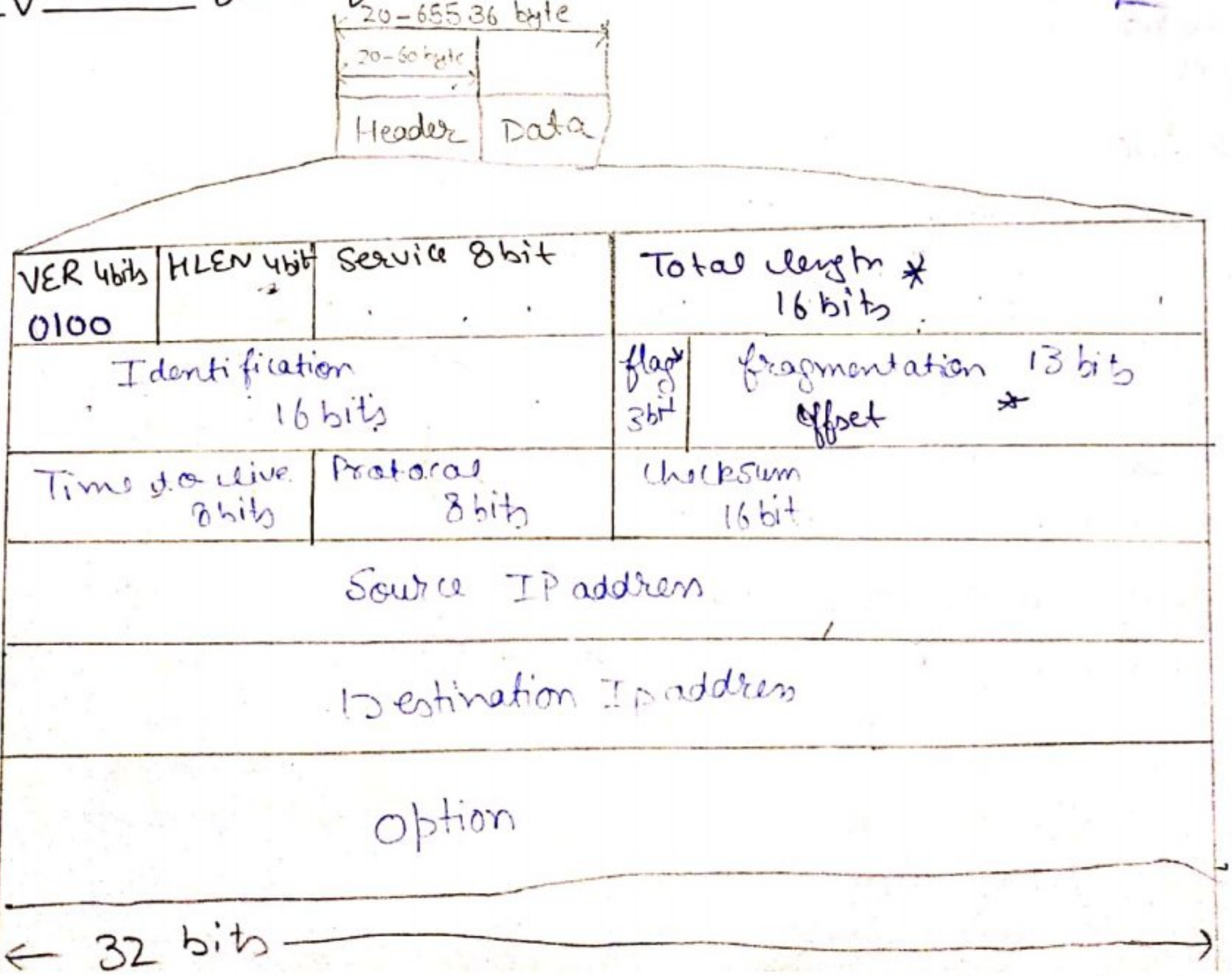
① 10.0.0.0 — 10.255.255.255
10.x.x.x 2^{24}

② 172.16.0.0 — 172.31.0.0 2^{20}

③ 192.168.0.0 — 192.168.255.255
192.168.x.x 2^{16}

IPv4 Protocal
→ It is connectionless
→ It is unreliable

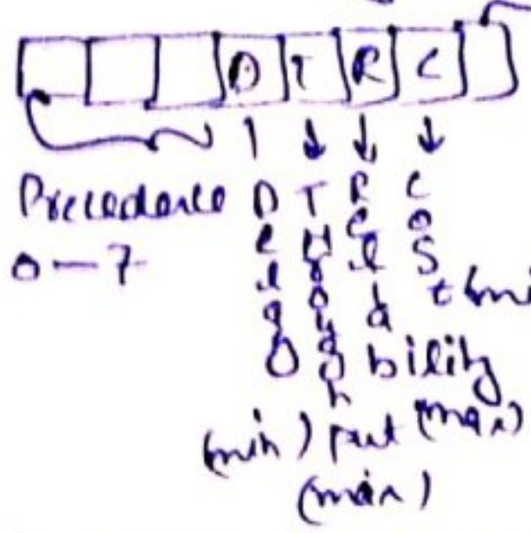
IPv4 datagram format



VER :- It define the version of the IP 0100

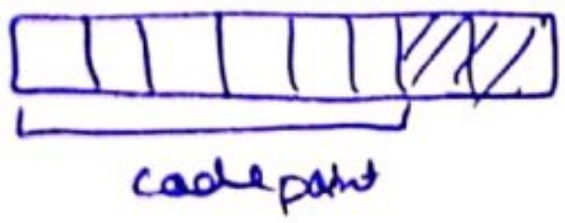
HLEN:- It define the length of the Header in 4 byte word. to obtain the header length multiply this by 4

Service bit :-



We have to set one for correspondig service, remaining bits will be zero.

differentiated service



Total length = Header length + data length

This 16 bit bit field define the total length of including header

Identification
flag
fragmentation
offset
} later related with fragmentation

Time-to-live :

It tells total life of IP datagram, this 8-bit field defines the maximum number of routers. A datagram can visit in a network before dropping out. A datagram has a limited life time in the internet this field hold a time stamps which was decremented by one by each visited router, if this value is being decremented to zero then the router discards the datagram.

Time Stamp = 2 x max no of routers in the network

If a packet is sent within a LAN then the value of this field is one.

Protocal: This 8 bit field defines which higher level protocal uses the services of the IPV4.

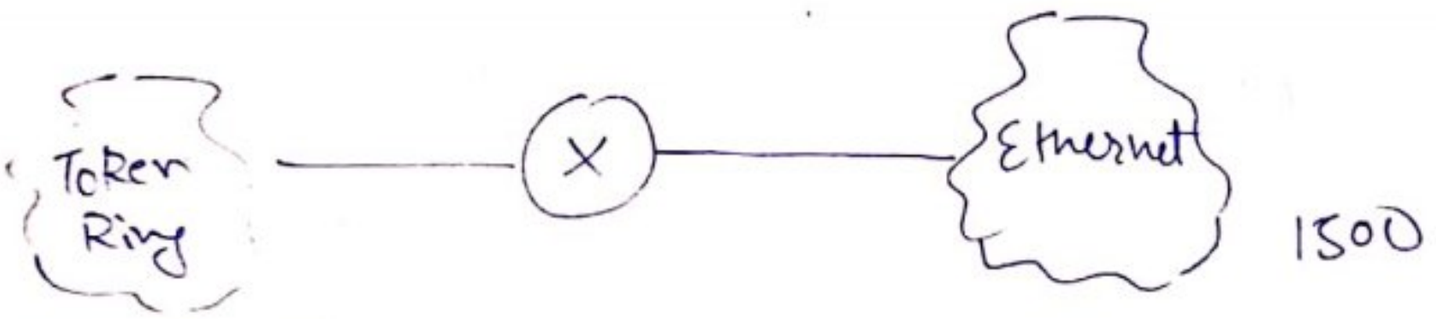
Protocal	value:
ICMP	1
IGMP	2
TCP	6
UDP	17

Header Checksum: (Internet checksum)
This 16-bit field is only for header errors and corruption checking

Source IP Address: (32 bit)
This is the IPv4 address of the source - This field must remain unchanged.

Destination IP Address:
This is the IPv4 address of the destination. This field must remain unchanged.

fragmentation:



Fragmentation is used because MTU (Maximum Transfer unit) is different of both networks.
Each data link layer protocal has its own frame format when a datagram is encapsulated in a frame. The total size of the datagram must be less than the maximum size of the frame. The value of MTU depends on the Physical network protocal.

Protocal	MTU
Hyperchannel	65535
Token Ring (6Mbps)	17940
(4Mbps)	4464
Ethernet	1500
PPP	296

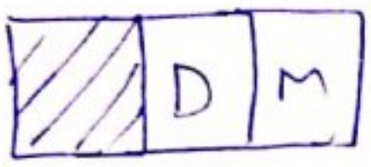
The host router that fragmen the datagram must change the value of 3 fields
→ Total length
→ flag
→ fragmentation offset and offcourse header checksum must be recalculated.

Identification: This 16 bit field identifies a datagram originating from the Source. The combination of the identification number and the Soure Ip address must uniquely define a datagram as it leave the source host.

To gurantee uniqueness the IP4 uses a counter to level the datagram. The counter is initialized to a positive number. When a IPV4 sends a datagram it copies the current value of the counter to the identification field and increment the counter by 1.

when a datagram is fragmented the value of identification field is copied to all fragments.

Flag: 3 bits

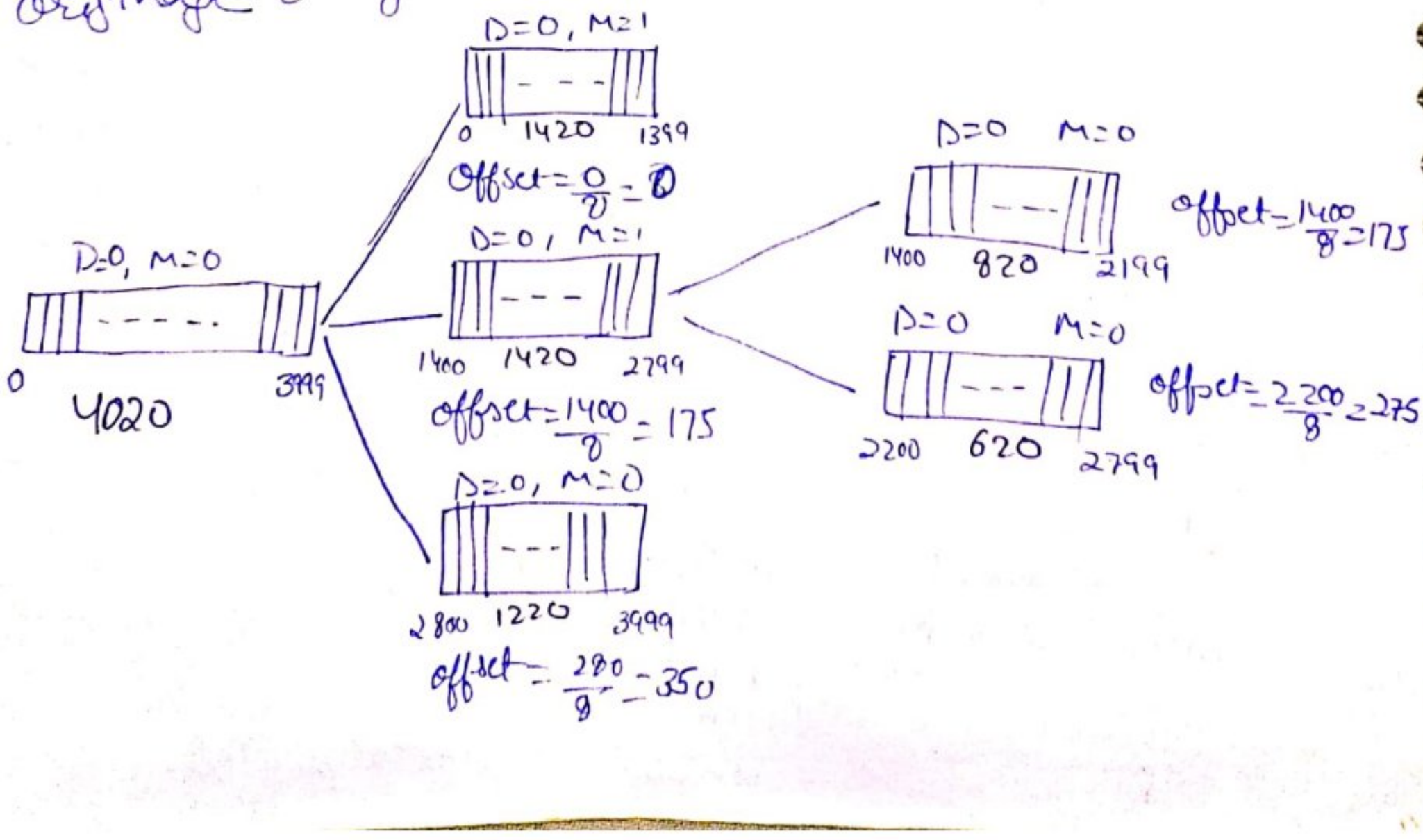


D → Dont fragment
1 – Dont fragment
~~0 → More fragments~~
0 → can be fragmented if needed

M → More fragments
1 → More fragments
0 → Single / only / last fragment.

Fragmentation offset

This 13 bits field shows the relative position of the fragment wrt the whole data gram. It is the offset value to the data of the orijinage datagram measures in unit of 8 bytes.



Q A IPV4 Packet has arrived with first 8 bits as shown 01000010 the packet is discarded by the receiver

HLEN = 0010 = 2 B

2x4 = 8 bytes minimum length = 20 bytes that why we discard it

Q The value of HLEN field is 1000 in binary how many bytes of options.

HLEN = $(1000)_2 = (8)_{10}$ = 8x4 = 32 bytes

options = 32-20 = 12 byte

IPv4 defines many options if there are more than 20 bytes rest are options

Q HLEN = $(5)_{10}$ = 20 bytes.

Total length = $0_x0028 = (40)_{10}$

How many bytes of data carried by the datagram.

Datalength = 40-20 = 20 bytes.

Q An IPv4 datagram has arrived with the following information in the header

0x45000054000035850200600007C4E0302B40E0F02

i, Is the packet corrupted -

ii, Are there any options -

iii, Is the packet fragmented -

iv, What is the size of the data -

v, How many more routers can the packet travels to

vi, what is type of service ~~what is the~~

vii, what is the identification no of the packet

i, Ver = 4 HLen = 5x4 = 20 Hence Not corrupt-

ii, No options -

iii, 0 1 0 1 hence not fragmented.

RDM

(iv) Total length = 0054

= 5x16+4 = 84 bytes.

Data length = 84-20 = 64 bytes

(v) TTL = $(20)_{16}$

= $(32)_{10}$ 32 more travel packet can travel

(vi) 0 → default

(vii) Identification no = $(0003)_{16}$

= $(0000\,0000\,0000\,0011)_2$

= $(3)_{10}$

IPv6 :- (IPng)

① IPv4 has some deficiencies that make it unsuitable for fast growing Internet. Despite all short terms sol^n like classless addressing, subnetting and NAT, addres depletion is still a long term problem.

② The Internet must accomodate the Real-time Audio-Video transmission which requires resource allocation. It is not provided in IPv4.

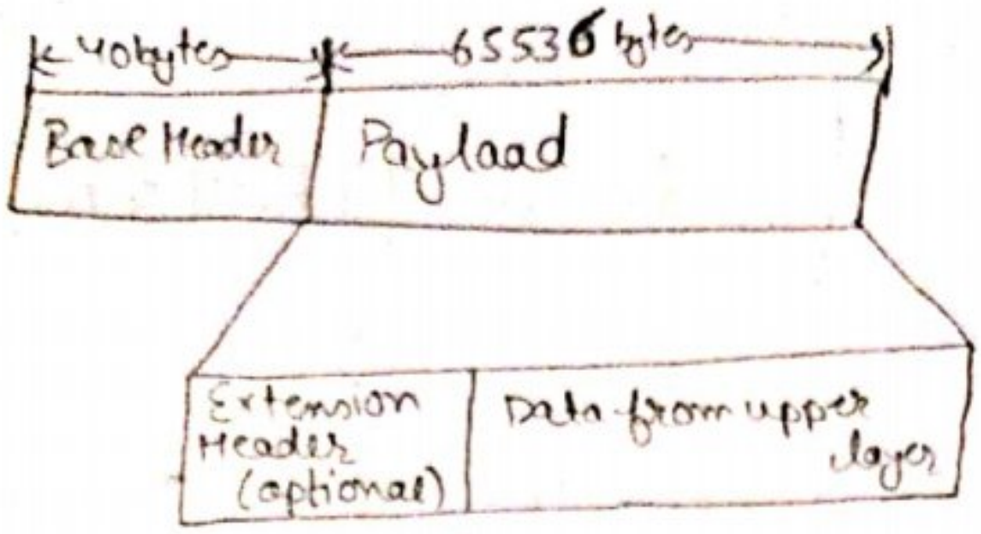
③ No encryption and authentication is provided in IPv4.

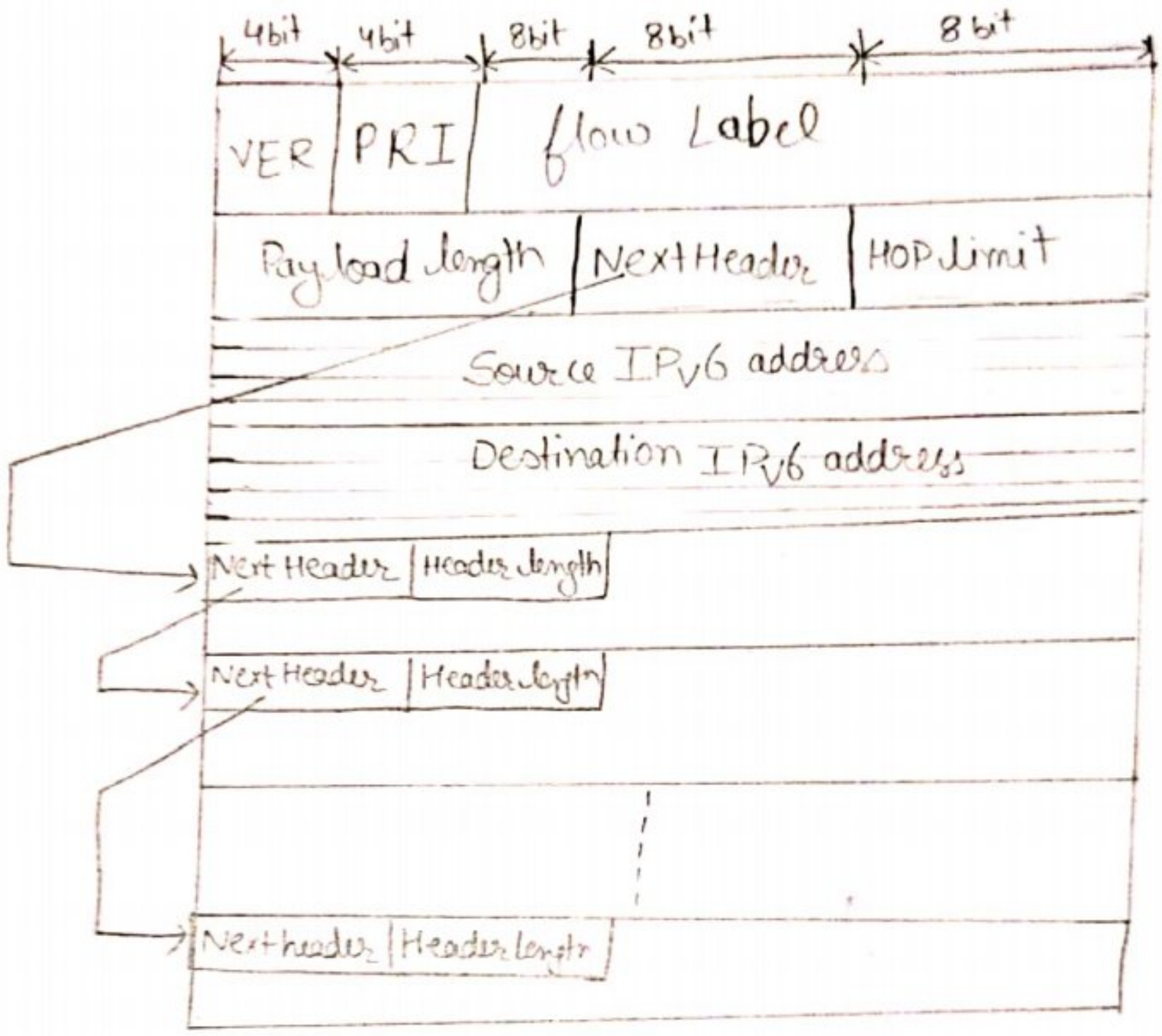
To overcome these deficiencies IPv6 or IPng (Next Gen.) has proposed and now it is a Standard.

Advantages

→ Larger address space (2^{128})
→ Better header format
→ In IPv6 options are separated from the base header and inserted when needed between the base header and the upper layer data thus IPv6 uses a new header format.
→ New options for better functionalities.
→ Support for resource allocation.
→ Support more security
→ Allowance for acceptance.

Packet Format





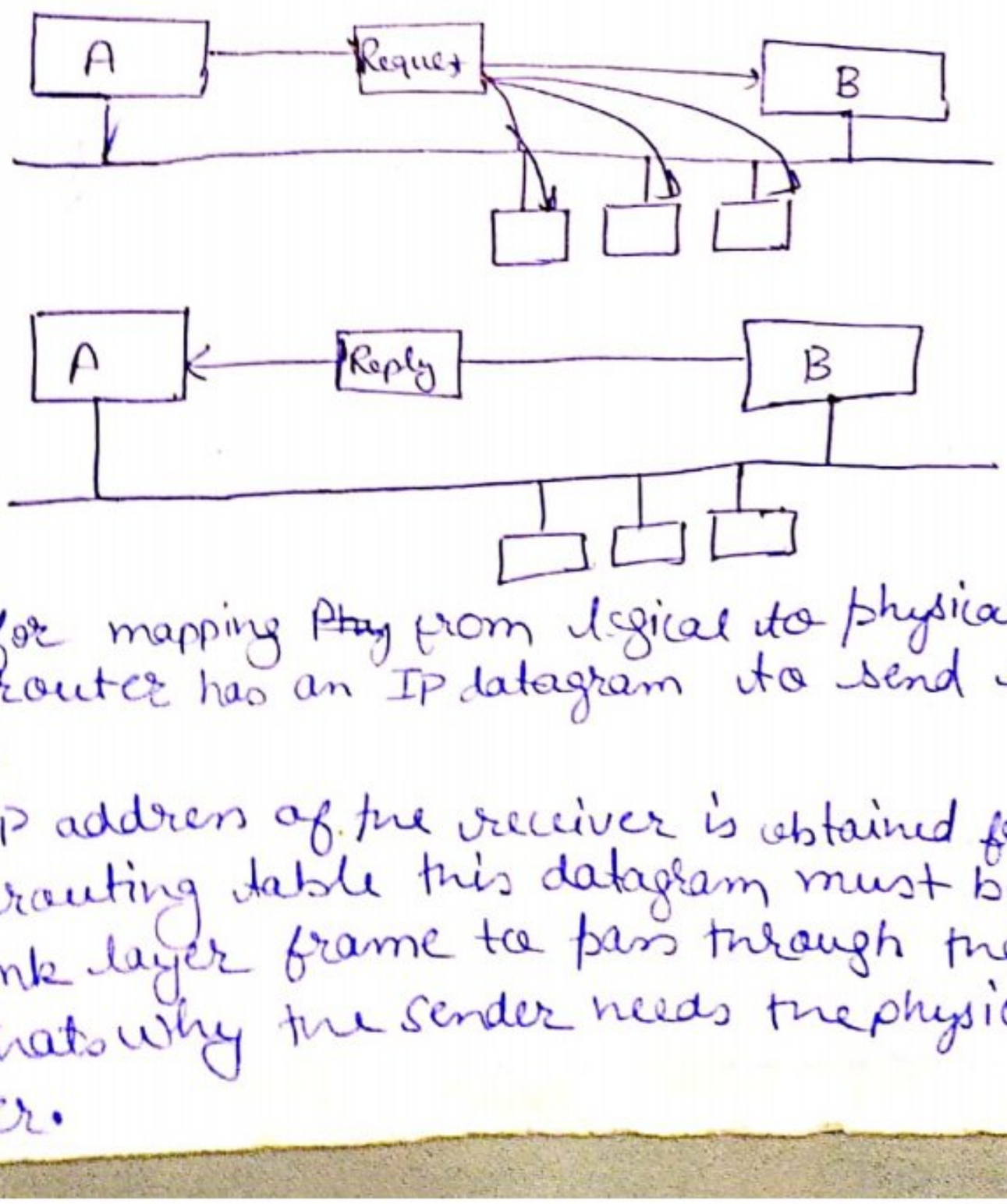
Next Header

Code	Next Header
0	HopbyHop option
2	ICMP
6	TCP
17	UDP
43	Source Routing
44	Fragmentation
59	None (No next header)

Difference between IPv4 and IPv6

1. The header length field HLEN is eliminated in IPv6 because the length of the header is fixed.
2. The service type field is eliminated in Ipv6 The priority and flow level take over together the function of service type field.
3. The total length field is eliminated in IPv6 and replaced with Payload length field.
4. Identification and offset field are eliminated from the base header in IPv6 and they are included in the fragmentation extension header.
5. The TTL field is called Hop limit in IPv6.
6. The protocal field is replaced by the next header
7. The header checksum is eliminated because the checksum is provided by the upperlayer protocal.
8. The option field of IPv4 is implemented as extension header in IPv6

ARP: (Address Resolution Protocal) & mapping logical to physical address



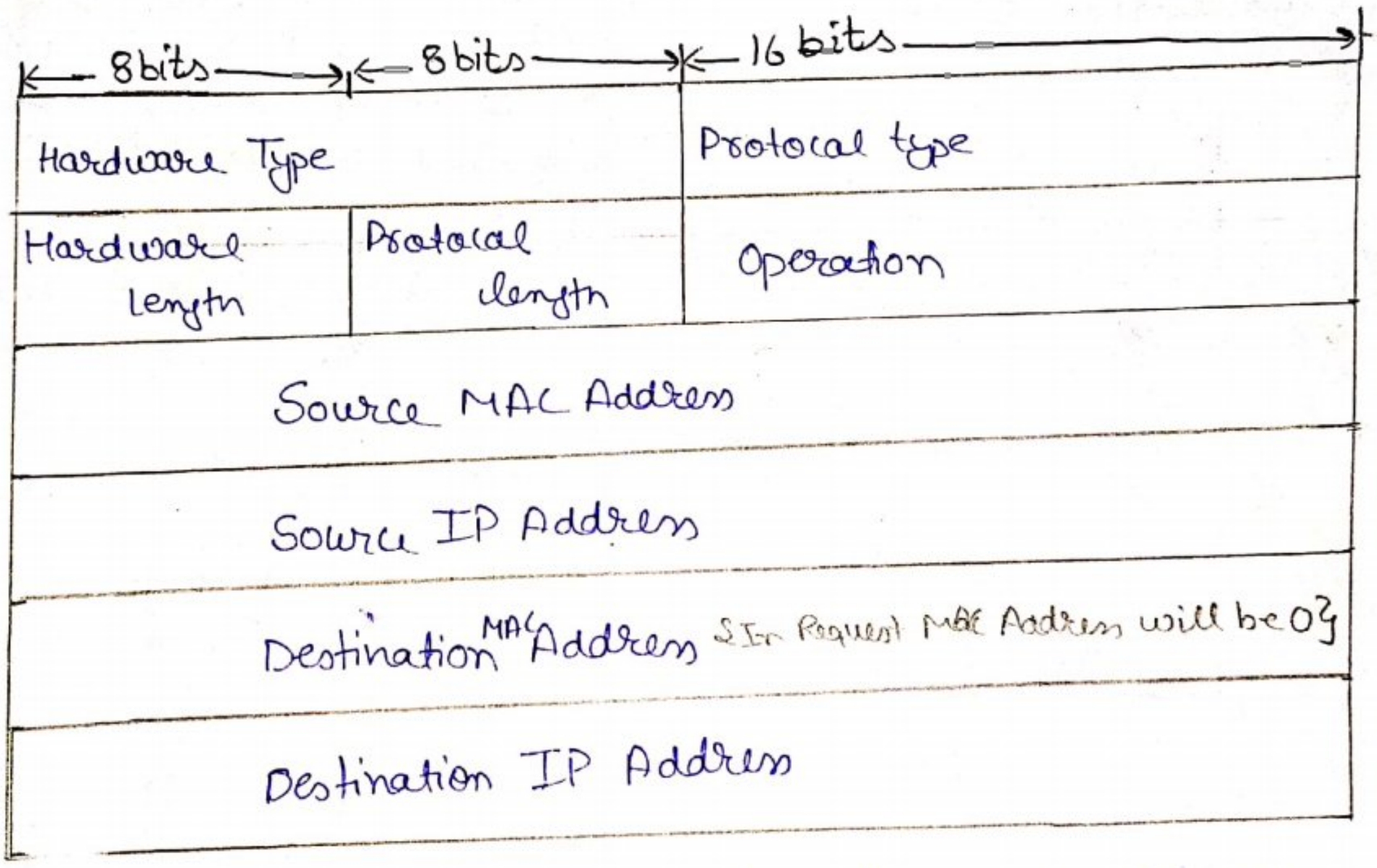
ARP is used for mapping ~~Phy~~ from logical to physical Address.
A host or router has an IP datagram to send to another host or router.

If the IP address of the receiver is obtained from the DNS or from the routing table this datagram must be encapsulated in a datalink layer frame to pass through the physical network. That's why the sender needs the physical address of the receiver.

The host or router sends an ARP query packet which includ the physical address & and IP address of the sender and the IP address of the receiver. The sender doesn't know the physical address of the receiver thats why the query is broadcasted over the network i.e. ARP request is broadcasted.

Each host in the network receives and processes the ARP query packet but the only intended receiver recognises its IP address and sends back an ARP response packet. ARP reply is unicasted

ARP packet format



Hardware Type: This 16 bit field defined physical network in used for ethernet its value is ~~0x0~~ '1'.

Protocal type: This field defines which type of protocal is used for networking. For IPv4 :- 0_x0800

Hard ware length: The length of the physical addres in bytes. for ethernet 0x06 b

Protocal length: This define the length of IP address in bytes. For IPv4 it is 0_x04

Operation: It is of two types

Request :- 1 (0_x0001)

Reply :- 2 (0_x0002)

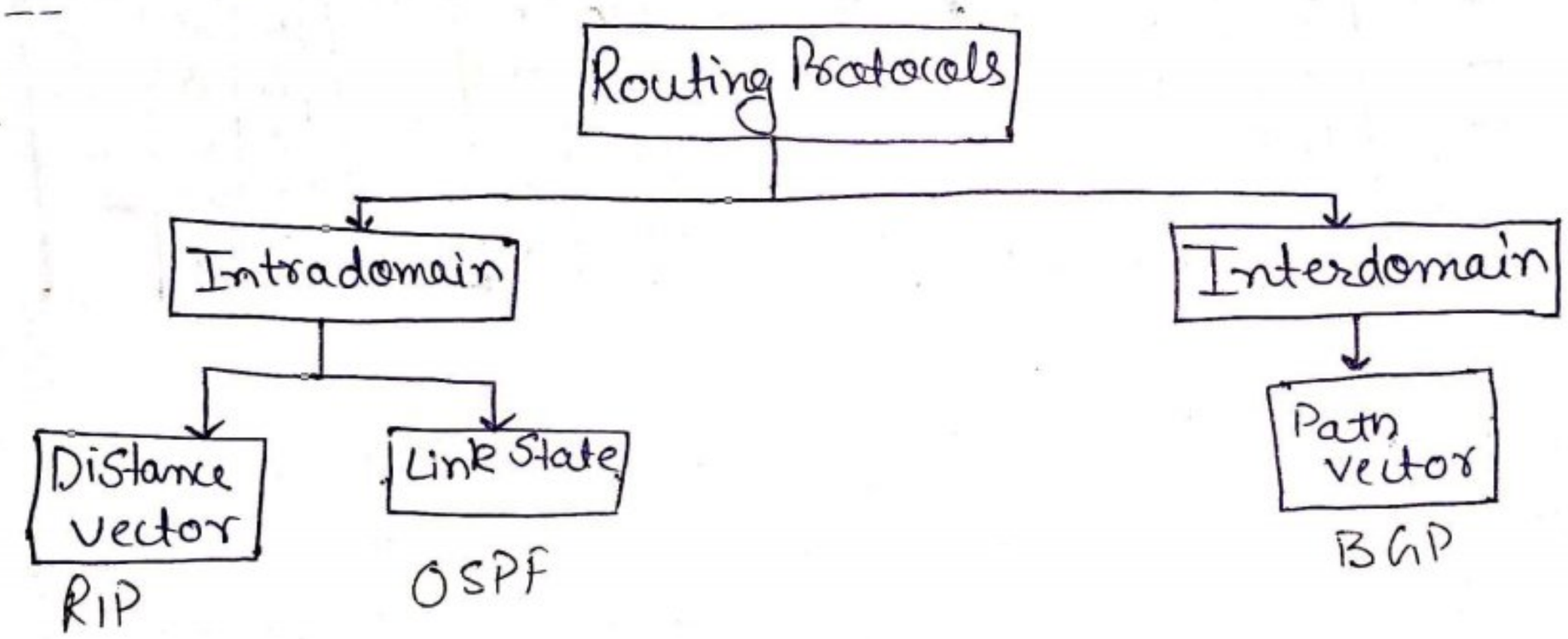
Routing:

Routing Algorithms are of 2 types
1. Non Adaptive (Static)
2. Adaptive (Dynamic)

Non Adaptive Algorithms
It uses static routing table which is one with manual entries. If there is a change in the network topology or any difference in the network the entries in the table will be filled manually.

Adaptive Algorithms
→ It maintains a dynamic Routing table which is updated automatically or Periodically when there is a change in the network.

Adaptive routing Protocals is a combination of rules and procedure that help ada routers in the internet to inform of changes about each other.

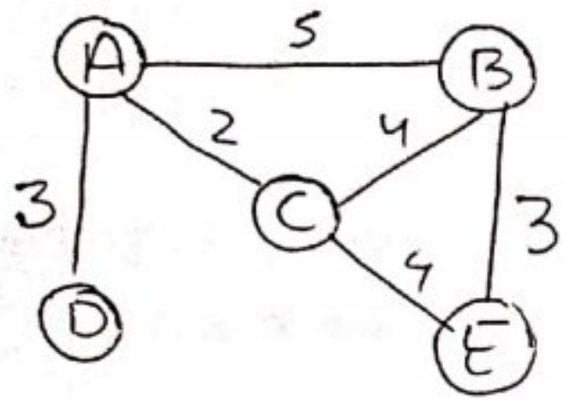


Distance vector is Dynamic
Link State is Static

Intradomain and Interdomain Routing Protocals.
Internet is divided into small groups called Autonomous Systems (called AS) and AS is a group of networks and routers under the authority of single administration.
Routing inside an AS is refers to as Intradomain routing & Routing between the AS is refers to as Inter domain routing.
Each AS can choose one or more Intradomain routing protocols to handel routing inside the autonomous system however only one interdomain routing protocal handels the routing between the AS.

Distance Vector Routing ~~Protocal~~ Protocol

Distance vector Routing uses the least cost route between the two nodes, and it is the route with min distance. In this protocal each node maintain a vector (table) of minimum distance to every node. The table at each node also guides the packets to the desired node by showing the next stop in the route.



I Initialization

For A

To	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	∞	

For B

To	Cost	Next
A	5	—
B	0	—
C	4	—
D	∞	—
E	3	—

For C

To	Cost	Next
A	2	—
B	4	—
C	0	—
D	∞	—
E	4	—

For D

To	Cost	Next
A	3	—
B	∞	
C	∞	
D	0	—
E	∞	

For E

To	Cost	Next
A	∞	—
B	3	—
C	4	—
D	∞	—
E	0	—

II Sharing

Sharing is done in 2 ways

→ Periodically :- After 30 min table automatically shared

→ Triggered :- when network have some change.

Every node shares its table with its immediate neighbour and only first two colums of the routing table will be shared

Here we need to share only C's table.

A	2
B	4
C	0
D	∞
E	4

III updation :- It has 3 steps

I) The receiving node needs to add cost between itself and Sending node to each value in the 2nd colun.

II) The receiving node needs to add the name of the Sending

node to each row as the 3rd column. The sending node is the next node in the Route. It is the modified table of the receiving node.

III.) The receiving node needs to compare each row of the old table with the corresponding row of the new table.

Now comparison is based on

① If the next node entries are different then receiving node chooses the row with the smaller cost. If there is a tie then keep old one.

② If the next node entries are same then receiving node chooses the new row entry.

A' modified table

To	cost	Next
A	4	C
B	6	C
C	2	C
D	20	C
E	0	C

compare

A's old table

To	cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E		

To	cost	Next
A	4 0	C —
B	6 5	C —
C	2 2	C —
D	20 3	C —
E	0 6	C E

Sharing

Modified A

To	cost
A	0
B	5
C	2
D	3
E	6

Updation

D'

To	cost	Next
A	3	A
B	8	D
C	5	D
D	6	A
E	9	A

comp

D old

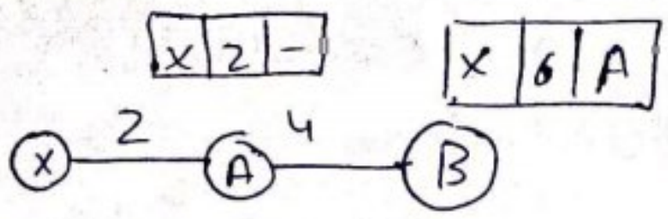
To	cost	Next
A	3	—
B	∞	
C	∞	
D	∞	—
E	∞	

To	cost	Next
A	3	—
B	8	A
C	5	A
D	6	—
E	9	A

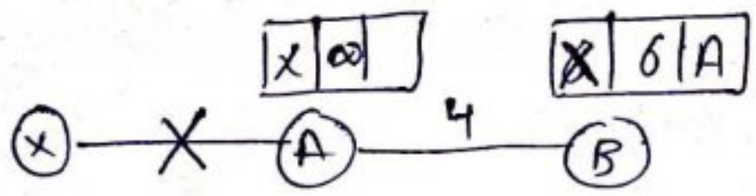
Two Node instability (count-to-infinity problem) while(1)

Problem with distance vector routing is instability this means that a network using this protocol can be instable. Let have a system with 3 nodes as shown in fig.

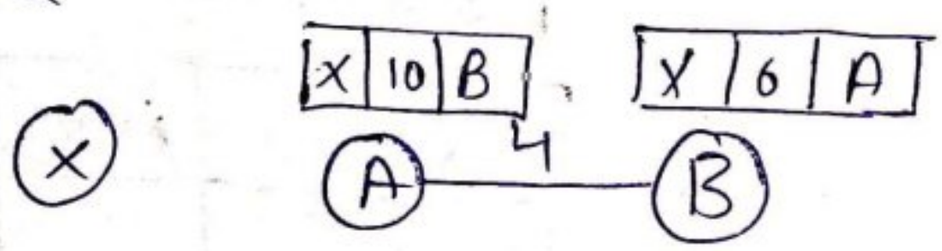
Before Failure



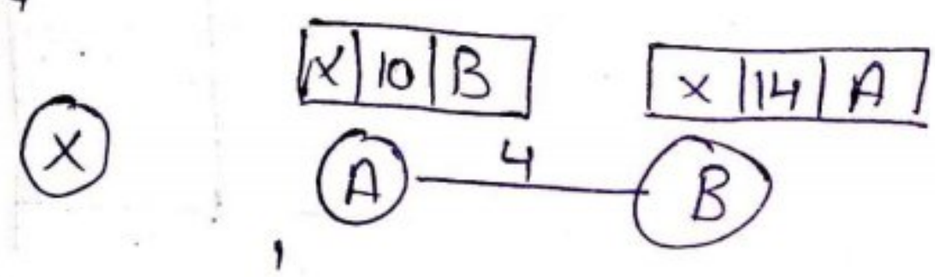
After Failure

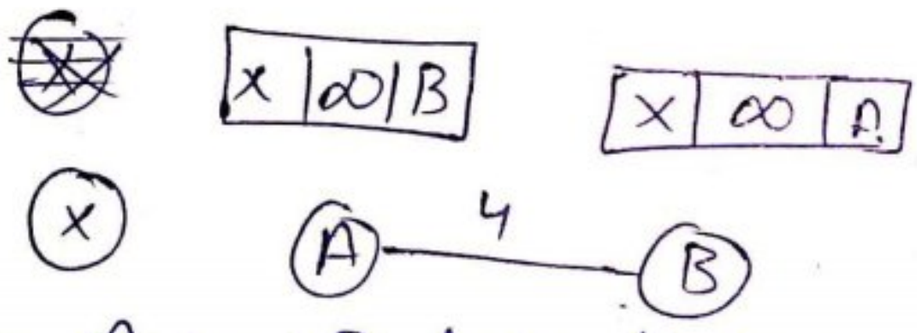


B shares its table with A



A shares its table with B





- At the begining A and B both knowns how to reach X
→ Suddenly the link between X and A breaks, and A update its table
* Complete from book *
→ But before A share its table with B, B shares its table with A
→ Now A thinks that there is a path to X from B, and B think that there a path to X from A
→ So both A and B will update each other's table constantly
→ This create count-to-infinity problem.

Solution:

1. Define Infinity: Most implementation of DBR define the distance between each node to be 'one' hop count. In DBR the distance 16 is defined as infinity.

2. Split Horizon: In this Strategy instead of sharing the table through each interface, each node sends only part of its table through some interfaces.
If according to its table node B thinks that optimum route to reach x is via A it doesnt need to advertise this piece of information to node A, because the information has come from A already. I.E.
Taking information from A, modifying it and Sending it back to A creates the confusion. Node B eleminates the last line of its routing table before it sends it a node A. In this ~~case~~ node A keeps the value of infinity as a distance to node X.

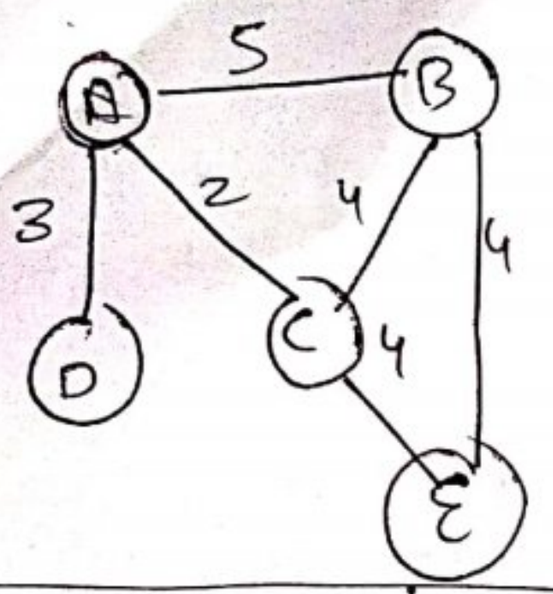
LINK STATE ROUTING

In LSR each node in the domain has the entire topology of the domain i.e. the list of nodes, links, how they are connected including the time type, cost and condition of the link, now the node can use Dijikstra algorithm to build a routing table.

Building Routing Table

In LSR 4 Sets of actions are required to ensure that each node has the routing table showing the least cost route to every other node

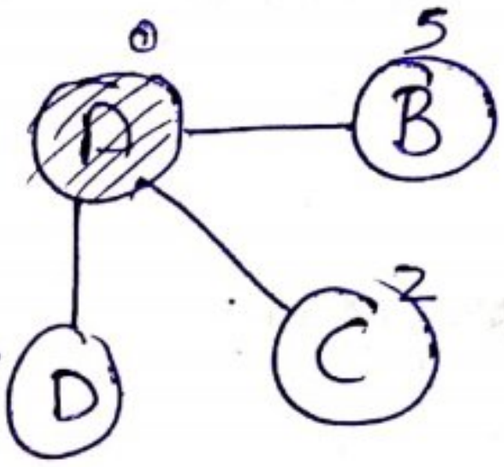
1. Creation of the States of the links by each node called LSP {Link State Packet}
2. Flooding: Sending of LSP's to every other router called flooding
3. Formation of shortest Path tree for each node.
4. Calculation of routing table based on the shortest path tree.



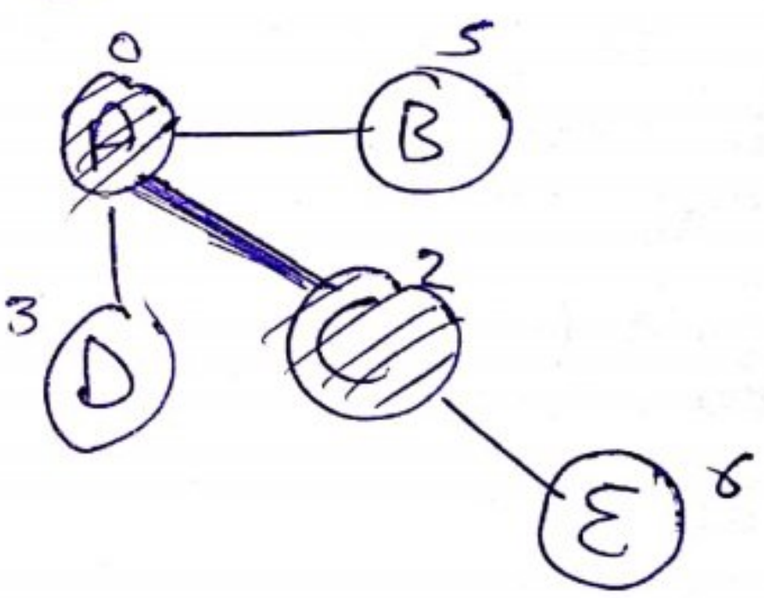
Permanent list	Temporary list
1. empty	A(0)
2. A(0)	B(5), C(2), D(3)
3 A(0), C(2)	B(5), D(3), E(6)

1.

2.



3.



Unit = 4 (Transport Layer)

Transport layer is responsible for delivery of message from one process to another process.

Client - server Paradigm :-

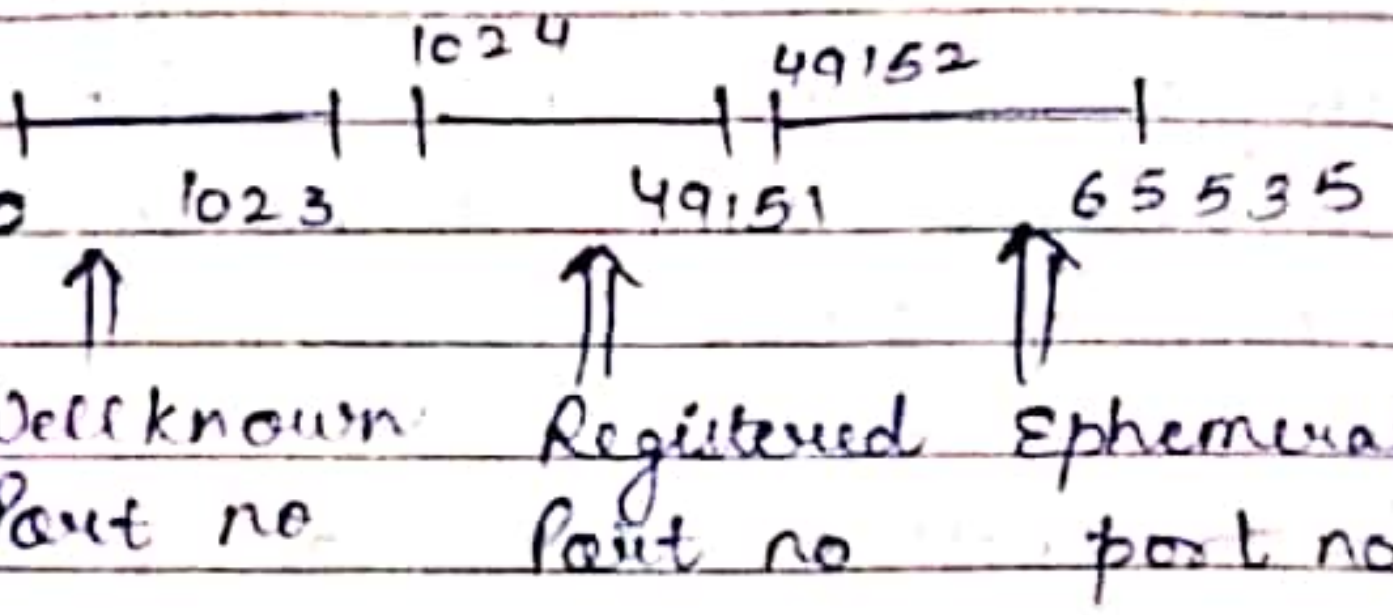
One of the way to achieve process to process communication is client server paradigm for comm^n. We must define the following

→ local host
→ local process
→ Remote host
→ Remote process

A process on the local host called a client needs services from a process usually on remote host called a server. Both processes has the same name.

Addressing :-

Port no : (16 bits) (0 to 65535)



Date 13-21

~~Addres~~ At the transport layer we need a port no. to chose among multiple processes running on the destinatione port. The destination port no. is needed for delivery & source port no. is needed for the reply. In TCP/IP model the port no's are 16 bit integers b/w zero & 65535. It is of 2 types -

(1) Ephemeral port no
(2.) Wellknown " "

1. Ephemeral port no - The client program defines itself with a port no. Chosen randomly by a transport layer s/w running on client host.

(2.) Wellknown Portno. - The internet has decided to use universal

port no is for servers. These are called wellknown port no. These are clients that are assigned well known port no., every client process knows the well known port no. of corresponding server process.

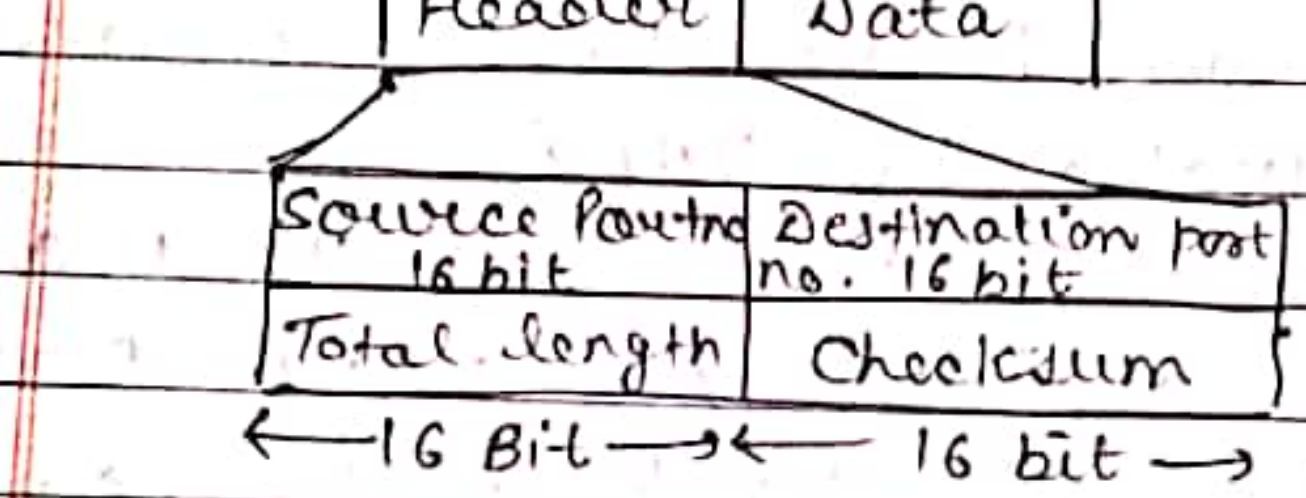
IANA Ranges :- Port no 0 to 1023 are wellknown portno. These are assigned & controled by IANA.
Registered Port no (1024-49151) are not assigned by IANA. These must be registered with IANA
Ephemeral (dynamic) port no (49152 - 65535) these are neither assigned nor controlled by IANA. These port no. can be used by any process.

Socket Address - Process to process delivery needs 2 identifiers, IP address & port no. at each end to make a connection. The combination of an IP address & a port no. is called a socket address.

Page No.

Date __/__/__

UDP (User Datagram Protocol) - It is a simple & small protocol. It is a connectionless protocol. It is unreliable because it has not mechanism of flow control & error control, It provides very limited error checking for header.



Source Port no - If source is client, then it is emphemerial portno. & if source is server then it is wellknown port no.

Destination port no - If source destination is client then it is emphemiral port no. & if destination is server then it is wellknown port no.

(well known) Port no	Process
9	Discard

Discard any data gram

13
20-21
69.
111

Application layer
TFTP (Trivial file transfer protocol)
RPC (Remote procedure call)

Total Length — This 16 bit field define the total length of the datagram (header + data). UDP total length is equal to ip length - ip header length.

Checksum — This field used to detect errors over the entire datagram.

Advantage of UDP w.r.t TCP —

1. UDP is a very simple protocol using minimum of overhead.
2. If a process wants to send a small message and does not care much about reliability then it can use UDP.
3. Sending a small message by using UDP takes much less interaction b/w sender & receiver rather than using TCP & STCP.

Use of UDP

→ UDP is suitable for a process that requires simple request response communication with little concern of flow and error control.
→ UDP is suitable for processes with internal flow and error control mechanism. Such as TFTP.
→ UDP is suitable for multitasking
→ UDP is suitable for management process and network debugging such as SNMP
→ UDP is used for some route updating protocals such as RIP

TCP:- Transmission Control Protocol

* Connection oriented
* Reliable.

It is a connection oriented protocal and reliable protocal It creates a virtual connection between two TCP to send the data.

Features:-

1. **Numbering System**:- In TCP Sender and Receiver contain a buffer which has divided in many number of bytes. A byte number is choosen randomly which is between "0 and $(2^{32}-1)$" and here segment uses a byte number

→ **Byte Number**: A byte number is a number between 0 & $2^{32}-1$ The type of data being transmitted in each connection are numbered by TCP.

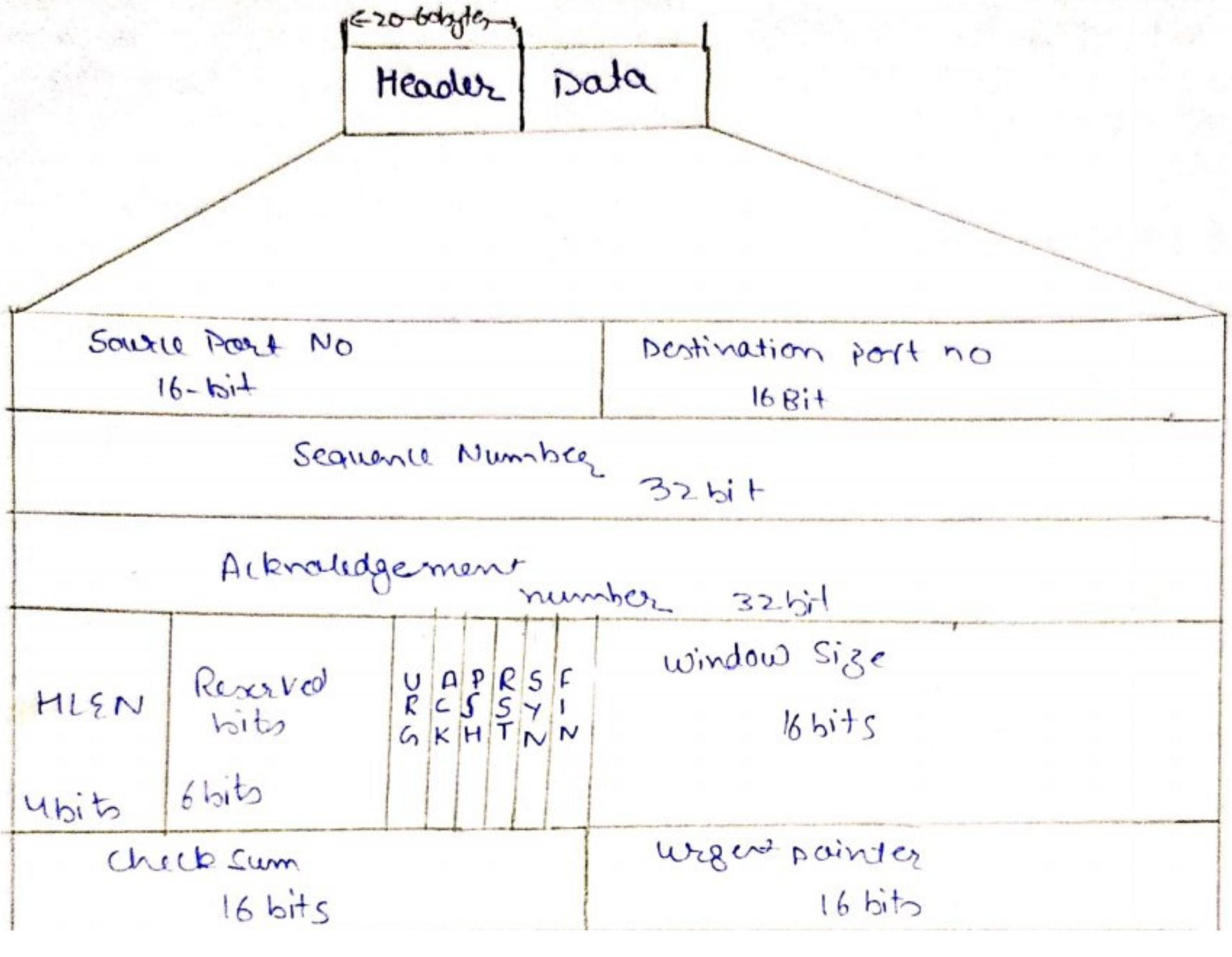
→ **Sequence number**: Sequence number is the number of segments the value in the sequence number field of the segment defines the number of first databyte contained in that segment.

Forex 5-segment of 1000 bytes.

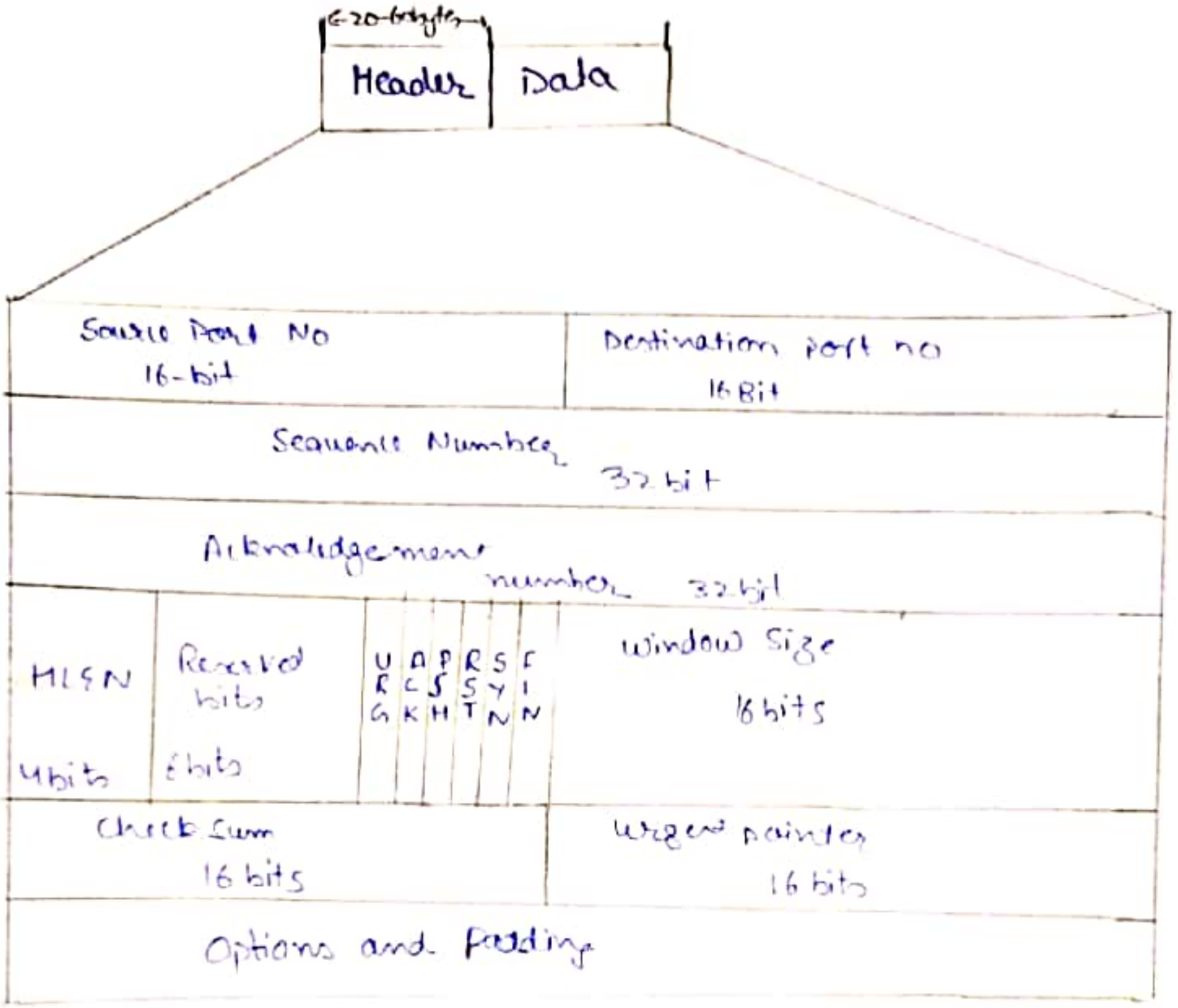
Seg1	(1001 — 2000)
Seg2	(2001 — 3000)
Seg3	(3001 — 4000)
Seg4	(4001 — 5000)
Seg5	(5001 — 6000)

SeqNO 1001 ← (choosen Radomly (0 to $2^{32}-1$)
2001
3001
4001
5001

Acknowledgement Number: The value of the acknowledgement field tells the number of next ~~number~~ bytes a party expects to receive
*The ack. number is cummulative.



Acknowledgement Number: The value of the acknowledgement field tells the number of next ~~number~~ bytes a party expects to receive
*. The ack. number is cummulative.



Flag/control field: This 6 bit control field defines 6 different flag flag have the meaning only when the corresponding bits is set to 1. One segment can contain more than one flag in control field.

1. URG :- The value of the urgent pointer field is valid.
2. ACK :- The value of the acknowledgement field is valid.
3. PSH :- Push the data
4. RST :- Reset the connection.
5. SYN :- Synchronized the sequence number during connection.
6. FIN :- Finish means terminate the connection

Window Size :-

$2^{16} = 65536$ bytes (0 - 65536 bit)

This 16 bit field defines the size of windows in bytes. That the other party must maintain. This value is normally refers to as receiving window. It is determined by

the receiver

Checksum: This 16 bit field is used for header checksum

Urgent Pointer: This 16 bit field is valid only when the urgent flag is set to 1 in control field. It is used when the segment contains the urgent data. It defines the number that must be added to the sequence number to obtain last urgent byte.

Option & padding: This 40 bytes field defines the option

The following is a dump of TCP Header in Hexadecimal

0x 0532 0017 00000001 00000000 5002 07FF 0000 0000

i, Source port no 0532

ii, Destination Port no 0017

iii, Sequence no 00000001

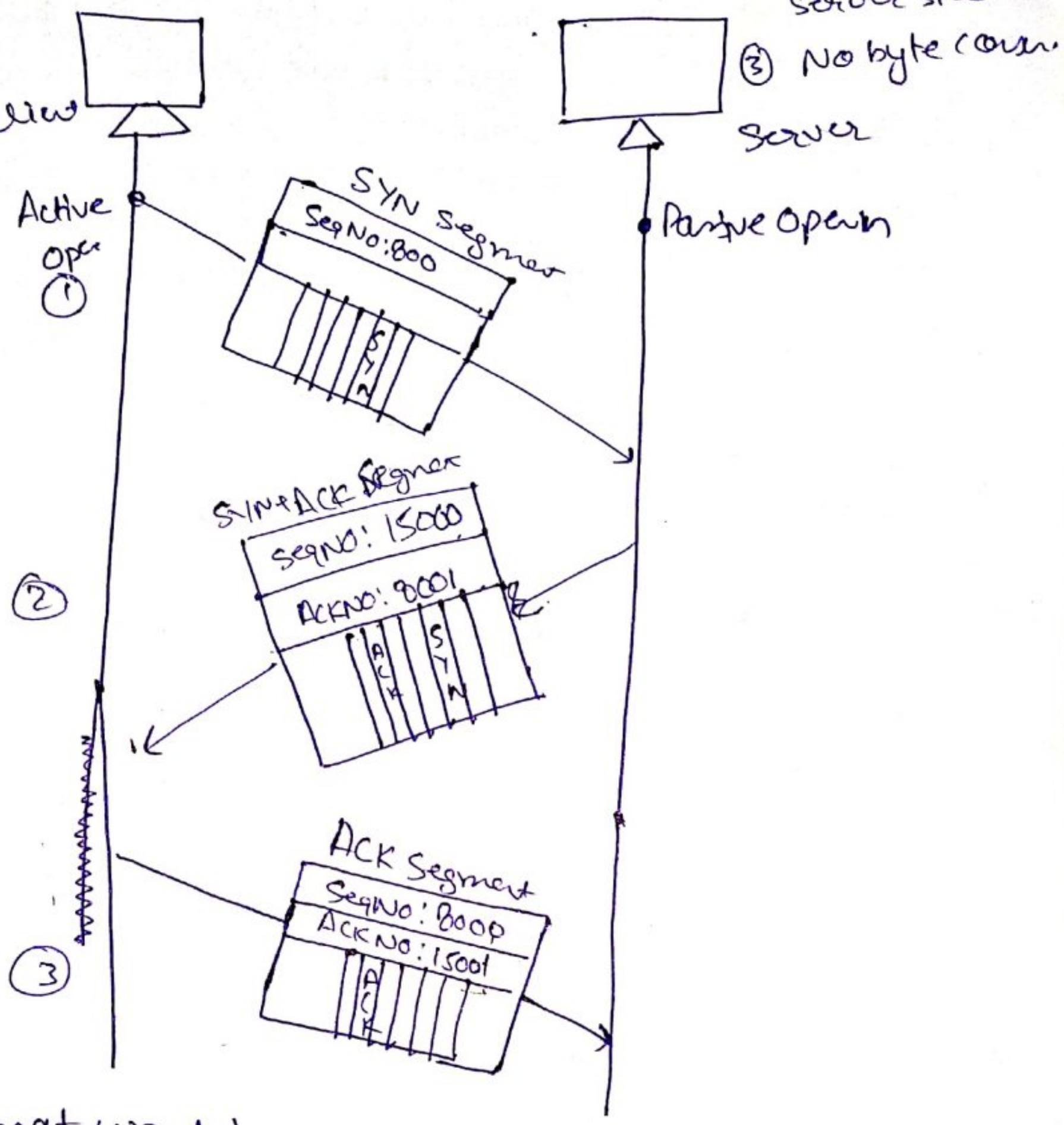
iv, Acknowledgement no 00000000

v, length of header 20 bytes

vi, Type of Segment. 000010 {Synchronized}

vii, window size 07FF = 2047 bytes.

TCP connection Establishment (3 way handshaking)



If client donot want to send then it will set SeqNo to initial

→ Client want to connect to server so this the connection is initiated by the client, before that server must be free to accept the connection. So server tells its TCP that he is ready, or he is free to establish a connection. This is called passive open.

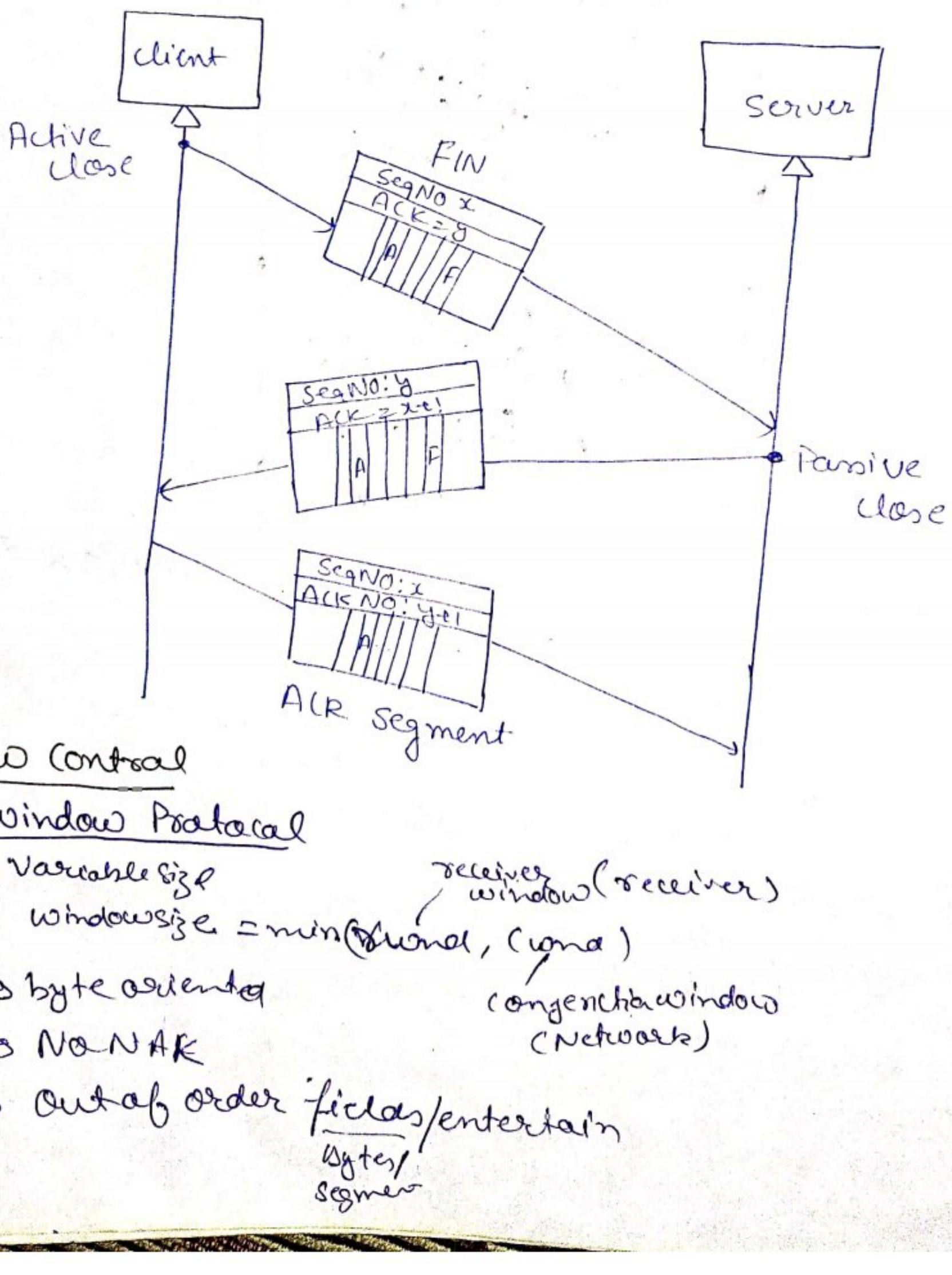
→ Now client tells its TCP to make a connection, and the connection is initiated it is called active open.

→ Now 3 way handshaking process begins

- 1. Client sends a syn segment SYN segment although not carrying the data consumes 1 byte number.
- 2. The SYN control field will be set to 1 in SYN segment.

2. SYN segment will be acknowledge if server also have the data to send then he will also choose a sequence number, this is called SYN + ACK segment & SYN & ACK control fields will be set to 1. This segment although does not carry any data but consumes 1 sequence number or byte number.
3. Previous segment will also being acknowledge and it will not consume any byte number, only ACK control field is set to 1 and acknowledgement segment will never be acknowledge.

TCP Connection Termination

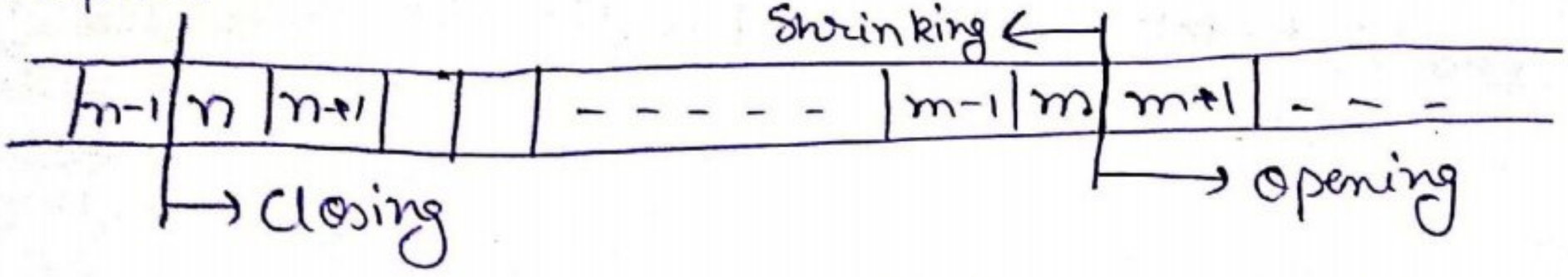


TCP Flow Control

Sliding window Protocol

→ Variable size
→ windowsize = min(Rwnd, Cwnd)
receiver window (receiver)
congenchia window (Network)
→ byte oriented
→ NO NAK
→ Out of order packets/entertain
bytes/segment

→ TCP window is of variable size and window size is min(rwnd,cwnd)
→ Size of rwnd is advertise by receiver and size of congection window is determined by Network. —
→ It is byte oriented
→ It doesn't use negative Acknowledgement (NAK)
→ It Support "out-of-order-segment" same as selective repeat.



Opening: Moving the right wall to the right, this allows new bytes in the buffer that are eligible for sending
closing: Moving the left wall to the right, this means some bytes have been ackrowledge and sender doesn't need to worry about them.
Shrinking: Moving the right wall to the left this is Strongly discouragious and now allowed in some implementation because it means revoking the eligibility of some bytes for sending, this is a serious problem if the sender has already send these bytes.

TCP Error Contral

In TCP Error means the segment is corrupted lost or duplicate. In TCP error contral can be done in 3 ways
1. checksum
2. Acknowledge
3. Retransmission

1. checksum: The checksum field in TCP header deals with the corrupted segment.
2. Acknowledgement: It is used for the data segments for some particular contral segments such as SYN or FIN segment but acknowledgement ~~segment~~ is not used for ACK segment. ACK segment doesn't consume any sequence number.
3. Retransmission: The heart of the TCP error contral

mechanism is retransmission. In TCP retransmission is done on 2 occasions.

1. Time out: when timer expires retransmission is done, Retransmission time out = RTT {Round trip Time}

$t = 2T_p$.

2. 3 duplicate ACK:- If 3 duplicate acknowledge is received.

Congestion Control

Congestion in a network occur if load on the network

of 3 duplicat ACK

Congestion Control :- Congestion in a n/w occurs if load of the n/w is greater than the capacity of n/w.
Congestion control refers to the mechanism & technique to control congestion & keep the load below the capacity.
Congestion can be prevented before it happens or can be removed after it happened.

Congestion Control Techniques

Openloop (Congestion prevention)
- Retransmission policy
- Window "
- Ack "
- Discarding "
- Admission "

Closedloop (Congestion avoida
- back pre
- Choke packet
- Implicit si
- Explicit "

Retransmission Policy — Retransmission sometime is unavoidable. In general it may increase the congestion in n/w. However a good retransmission policy can prevent congestion such as TCP retransmission policy.

Window Policy — The type of window at the sender side may also affect congestion. The selective repeat window is much better than goback-N window for congestion window.

3. Acknowledgement Policy — Ack policy imposed by receiver may also affect congestion. If the receiver does not Ack every packet it receives, it may slow down the sender & help to prevent congestion. The Ack are also part of the load of n/w so sending fewer acknowledgements means imposing less load on the n/w.

4. Discarding Policy :— A good

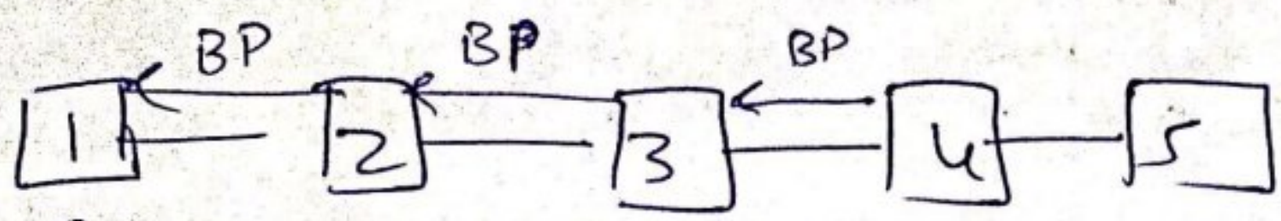
discarding policy by receiver may prevent congestion & at the same time may not harm the integrity of transmission.

e.g. The less sensitive packet in audio transmission can be discarded so that congestion is prevented & quality of sound is still preserved.

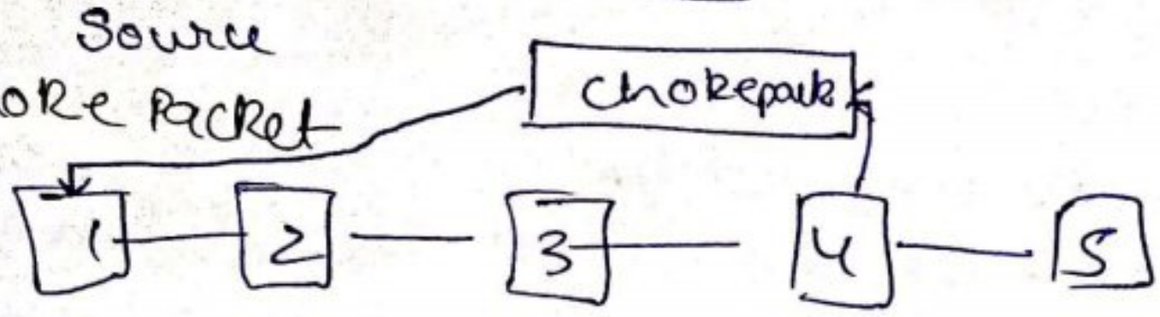
Admission Policy - It can also prevent congestion in virtual circuit n/w. Switches in a flow first check the resource requirement of a flow before admitting it to the n/w. A switch can deny to establish a virtual ckt if there is a congestion.

CLOSED LOOP & ~~ERROR~~ AVOIDANCE } Con
Congestion

1 Back pressure



2. Chore Packet



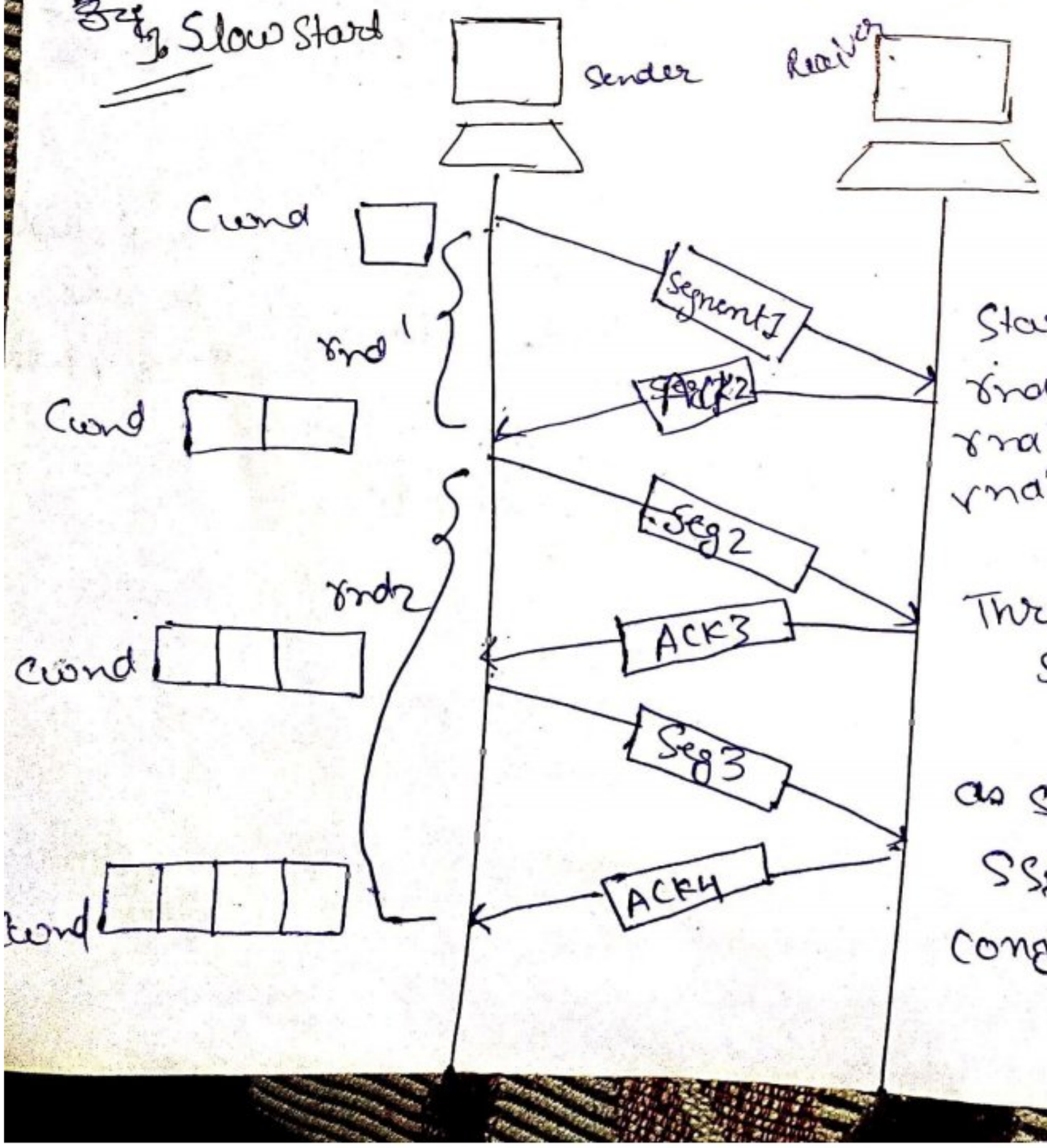
3. Implicit Signaling : Soure detect automatically from other symptom.

4. Explicit signaling → Forward { told ~~source~~ Destination to slow down }
→ Backward { told Source to slow down }.

TCP congestion control

1. Slow Start (Exponential Increase)
2. Congestion avaidance (Additive increase)
3. Congestion detection (multiplicative decrease)
→ Time out
→ 3, Ack's Receive (duplicate) } can be detected by

By Slow Start

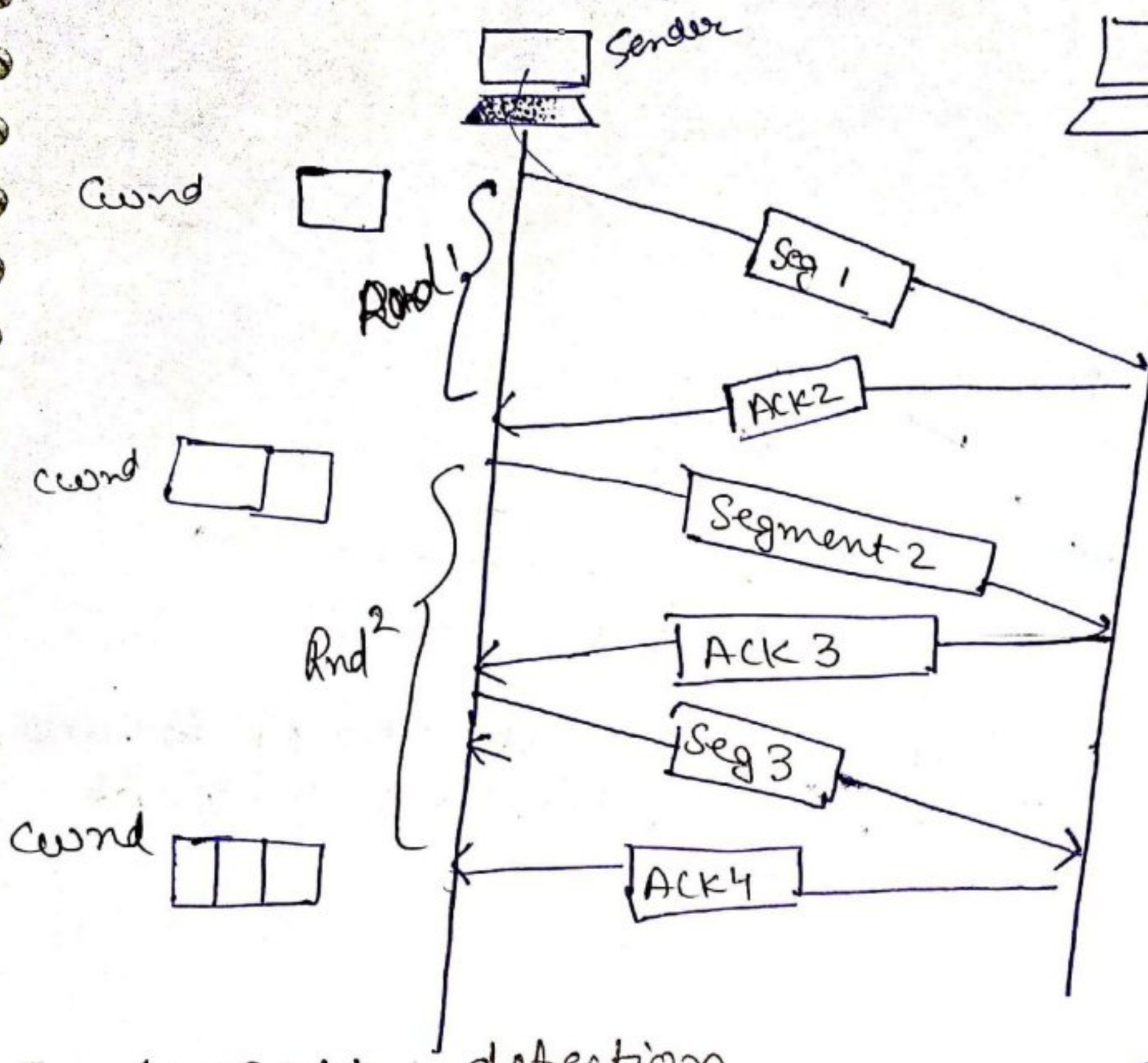


Assumption
Segment Size = 1 byte.

Start = cwnd = 2^0 = 1
rwnd 1 = cwnd = 2^1 = 2
rwnd 2 = cwnd = 2^2 = 4
rwnd 3 = cwnd = 2^3 = 8

Threshold value
SSthreshold
(65536)
as soon as we reach SSthreshold we start congestion avoidance

2. Congestion Avaidance
(Wnd size +1 only after end of round

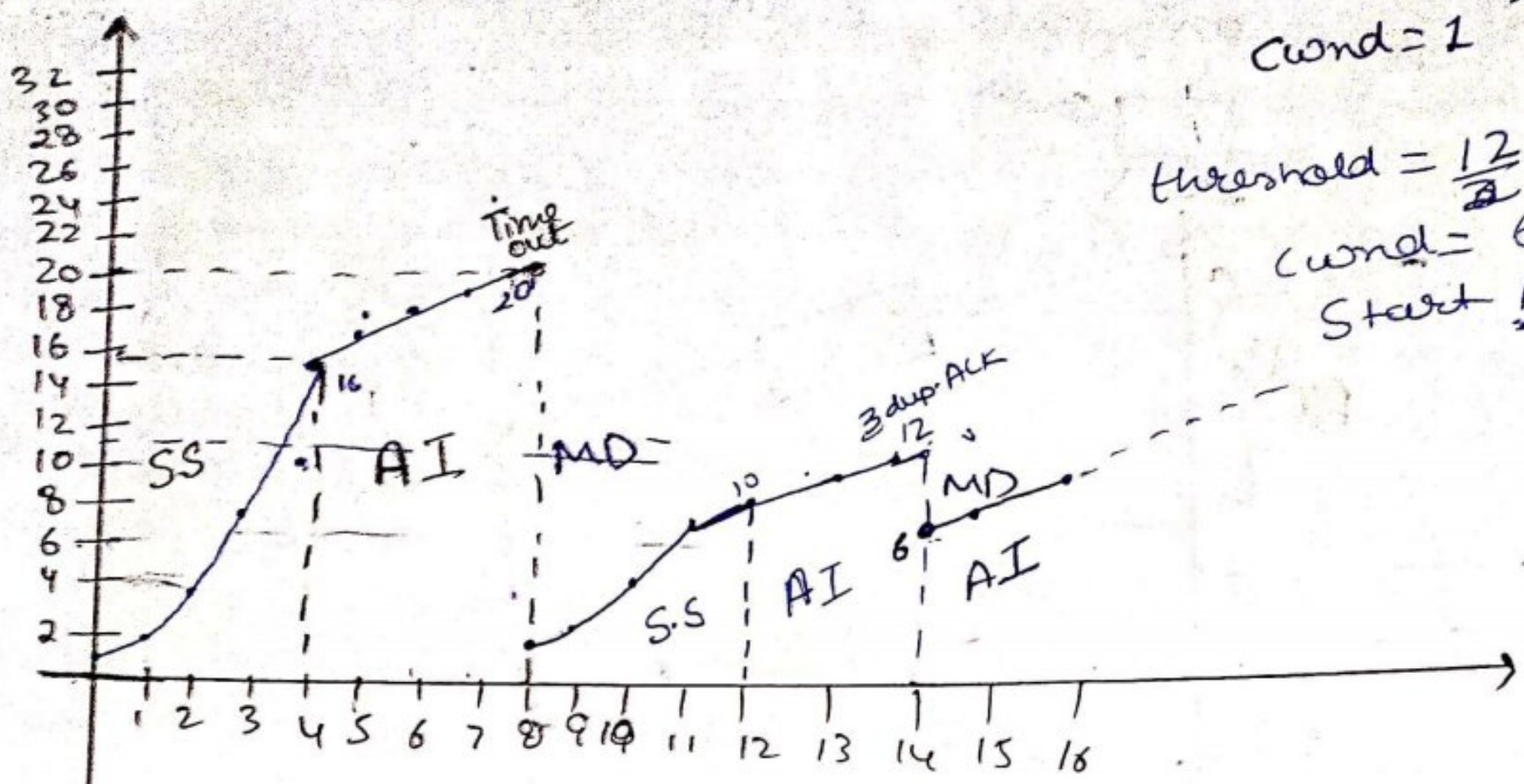


Start ⇒ cwnd = 1
rnd 1 ⇒ cwnd = 1+1 = 2
rnd 2 ⇒ cwnd = 2+1 = 3
rnd 3 ⇒ cwnd = 3+1 = 4

2. Congestion detection
Congestion ~~detection~~ can be detected in one of the following two ways
i) Time out: If it occurs then TCP will ~~react~~ react strongly
   a) Threshold value = $\frac{1}{2}$ current window size
   b) Cwnd = 1
   c) Start SS phase
ii) If congestion is detected by 3 duplicate ACK's received TCP reacts weakly
   a) Threshold value = $\frac{1}{2}$ current window size
   b) Cwnd = Threshold
   c) Start Congestion Avaidance phase

Q = Maximum window Size = 32 segments
Threshold value is set to 16 segments at 20 window Size Time out occurs and at 12 window 3 duplicat acknowledgement received.

Good Luck



Threshold val = $\frac{20}{2} = 10$

Cwnd = 1

Threshold = $\frac{12}{2} = 6$

Cwnd = 6

Start AI

QoS (Quality of Service)

A flow seeks to attempt is called QoS. There are 4 parameter of QoS

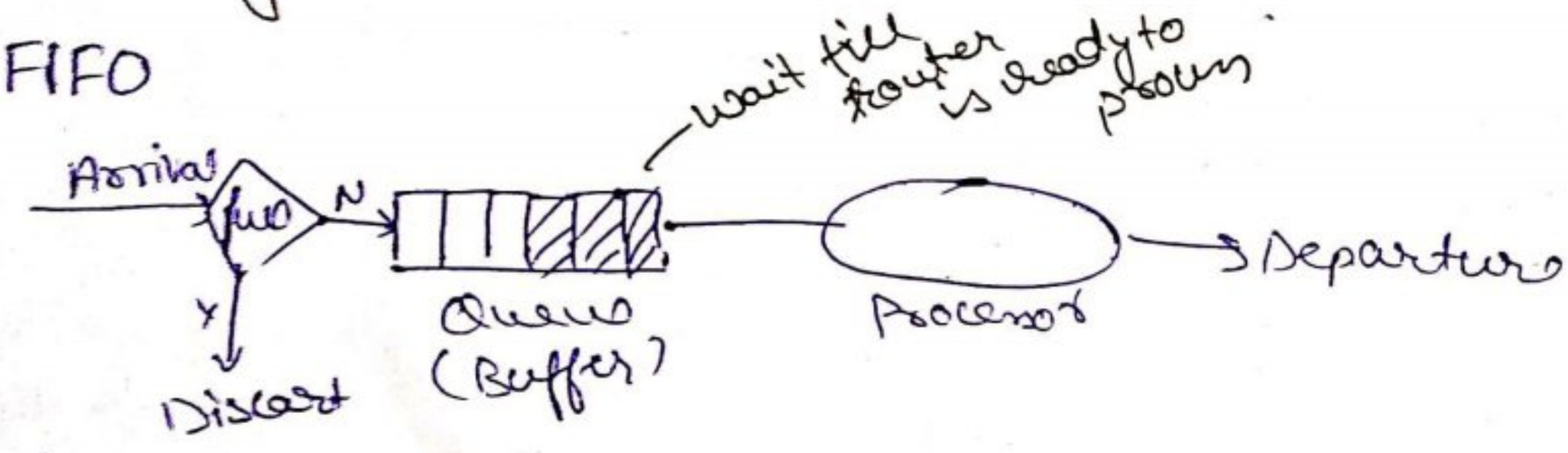
- → Reliability
- → Delay
- → Bandwidth
- → Jitter

Technique to improve QoS

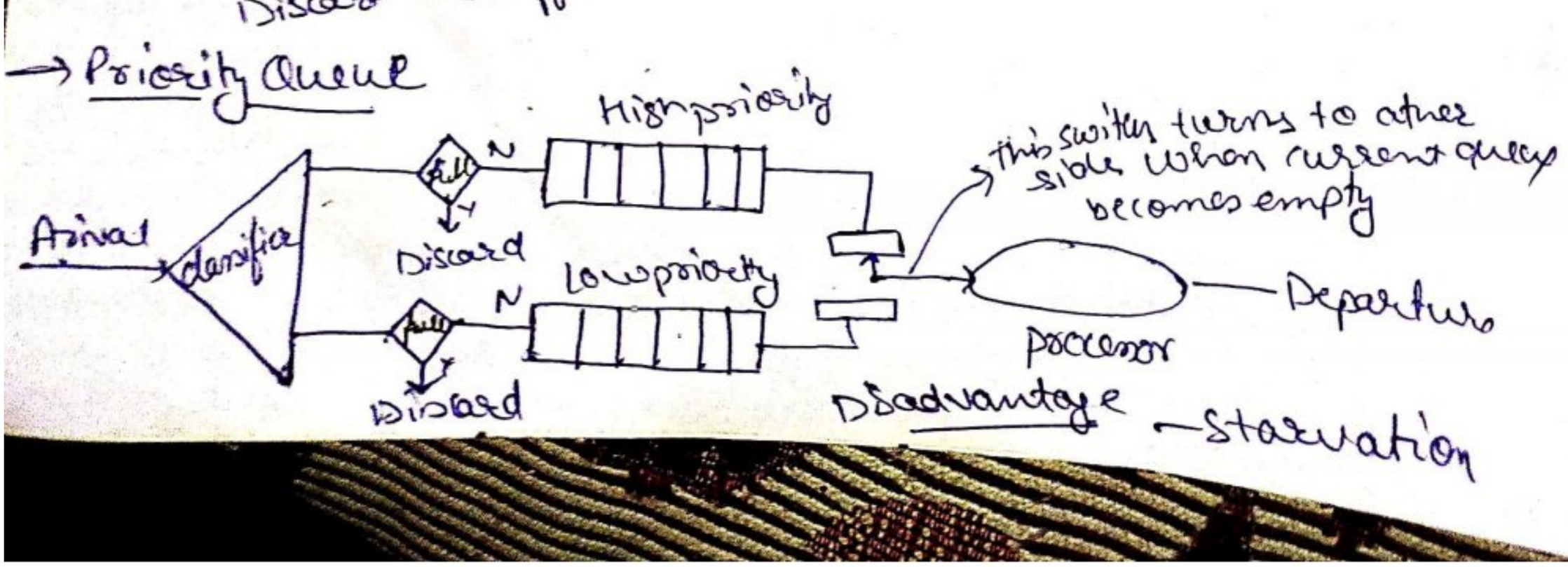
1. Scheduling
2. Traffic Shaping
3. Resource Reservation
4. Admition Control

Scheduling

→ FIFO

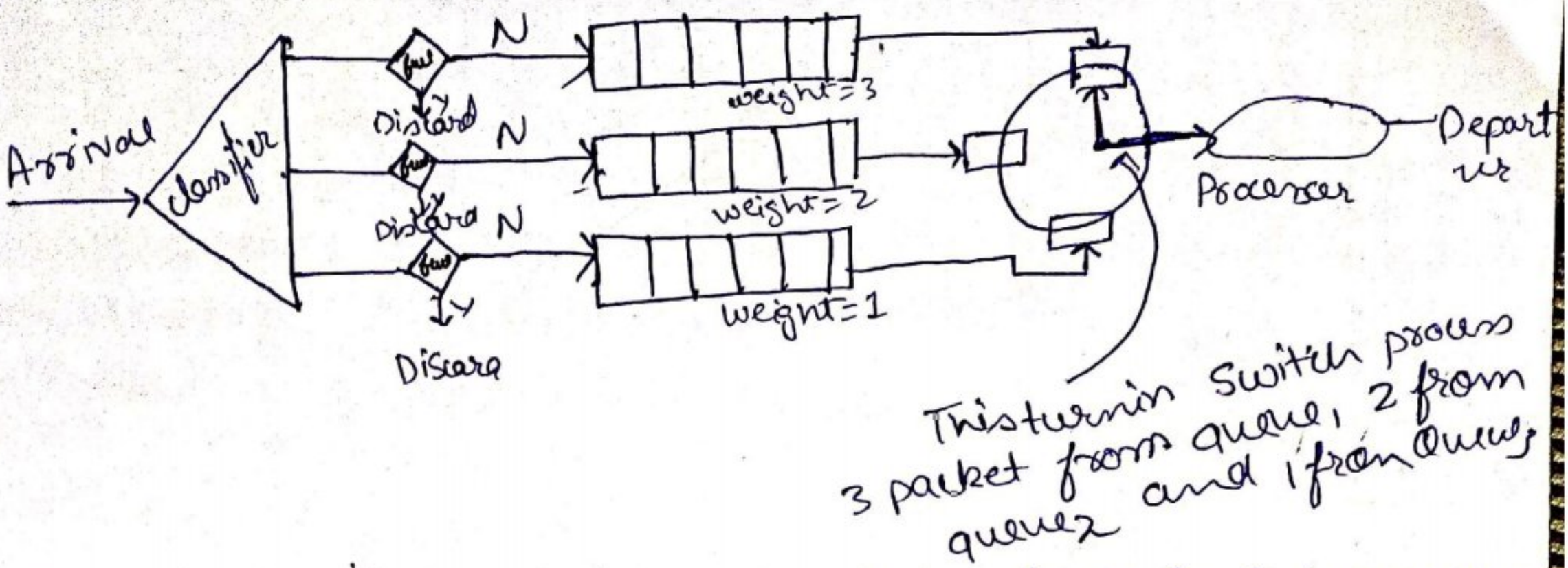


→ Priority Queue



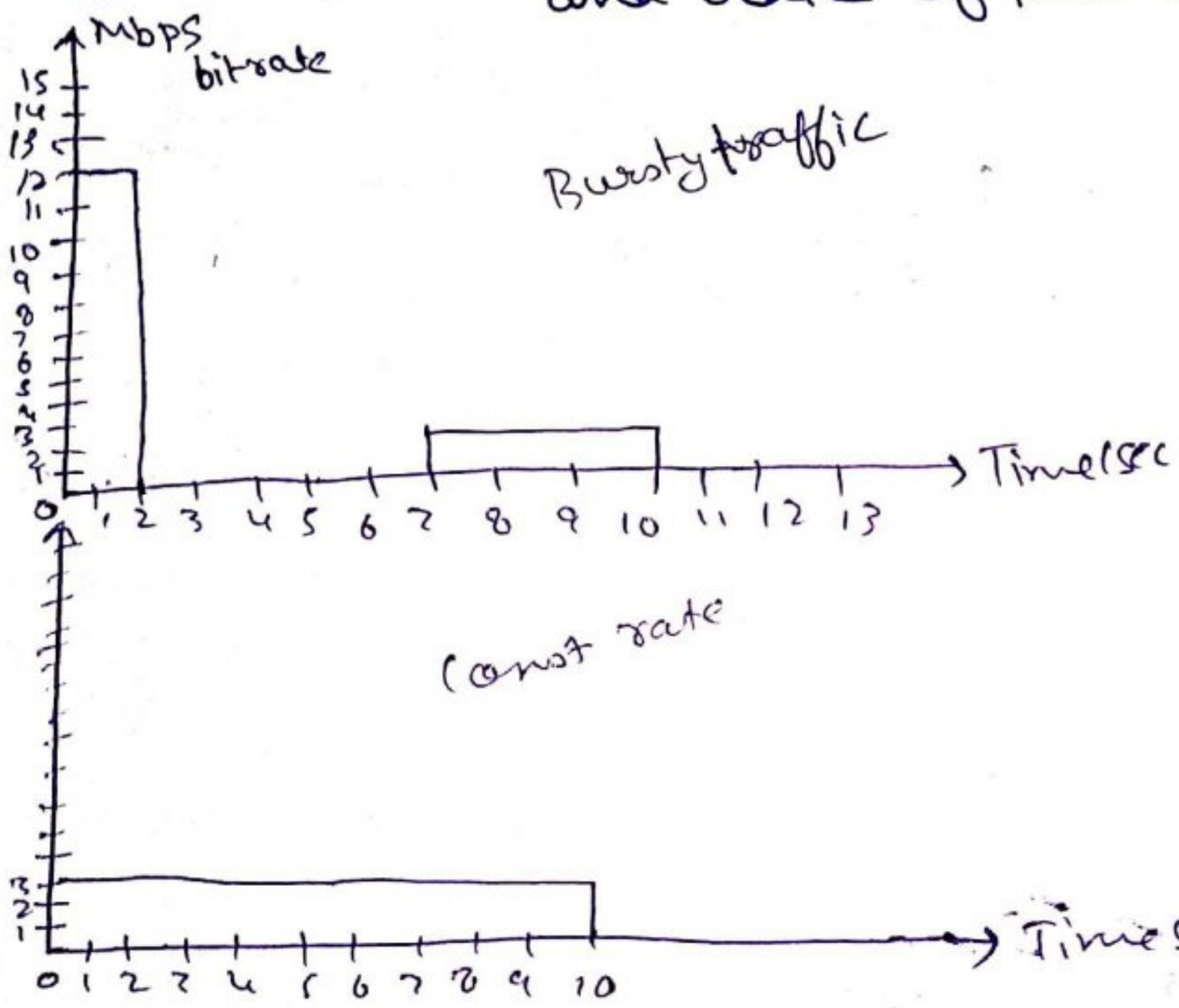
Disadvantage — Starvation

Weighted fair queue



Traffic Shaping

It is the mechanism to control the amount and rate of the traffic send to the network.



2×12 = 24 Mb
3×2 = 6
30 Mb

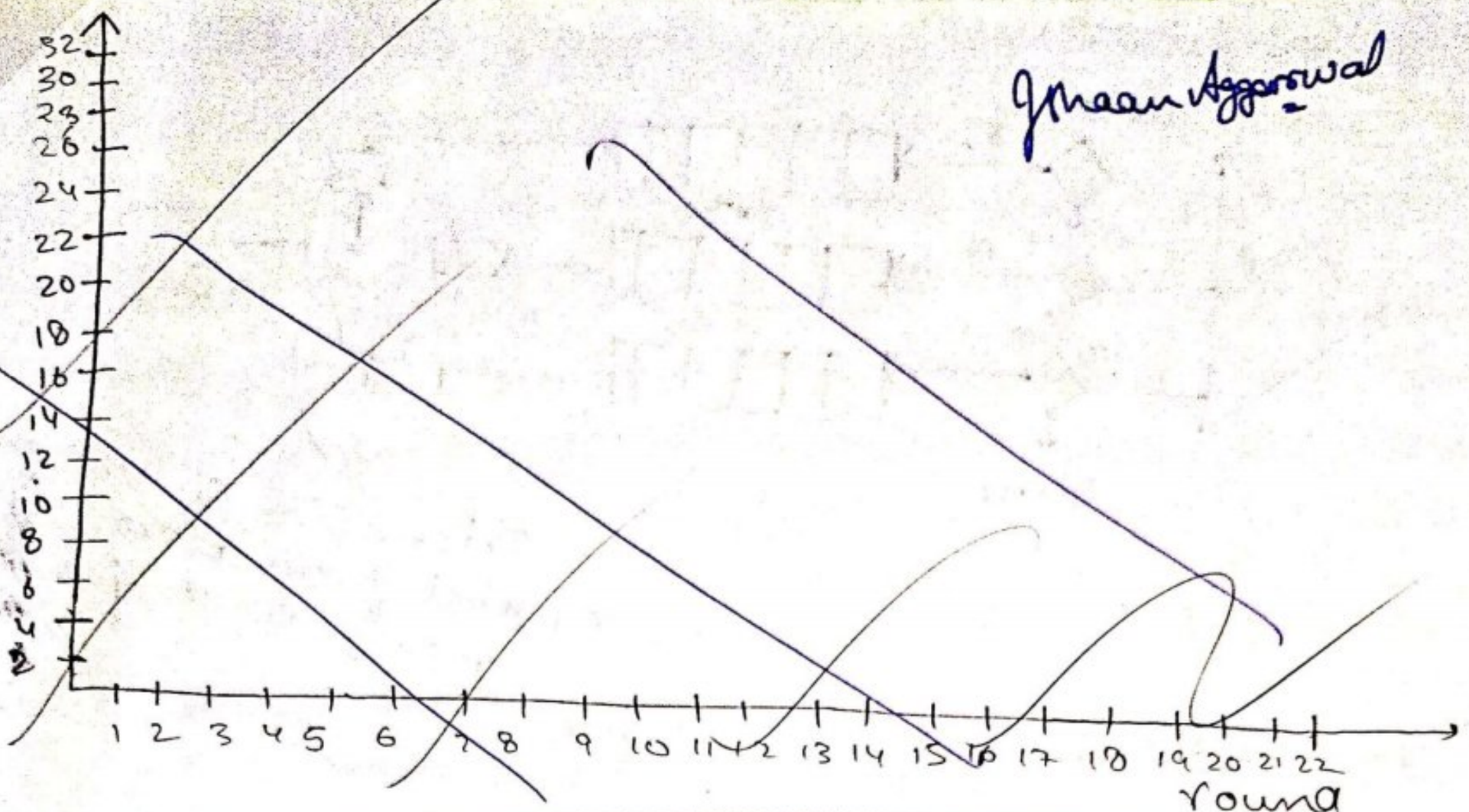
10×3 = 30 Mb

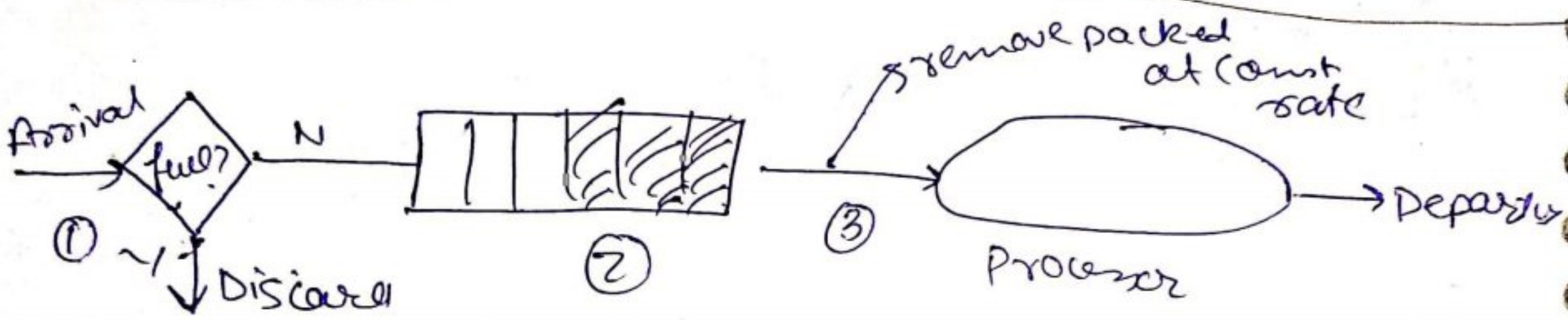
two techniques
→ Leaky bucket
→ Token bucket

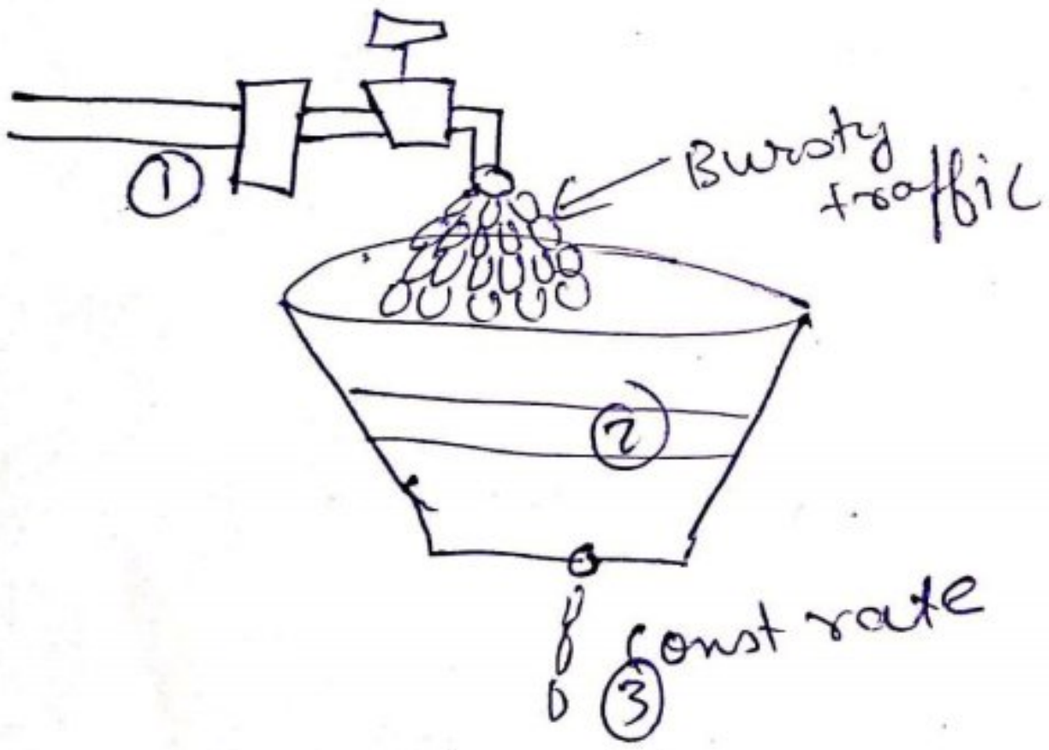
Leaky bucket

if fixed size no problem
if variable size problem → solution ① counter
② n > size of packet remove the packet
(Decrement the counter by size of packet)
③ n ≥ size of packet

Jhaan Aggarwal

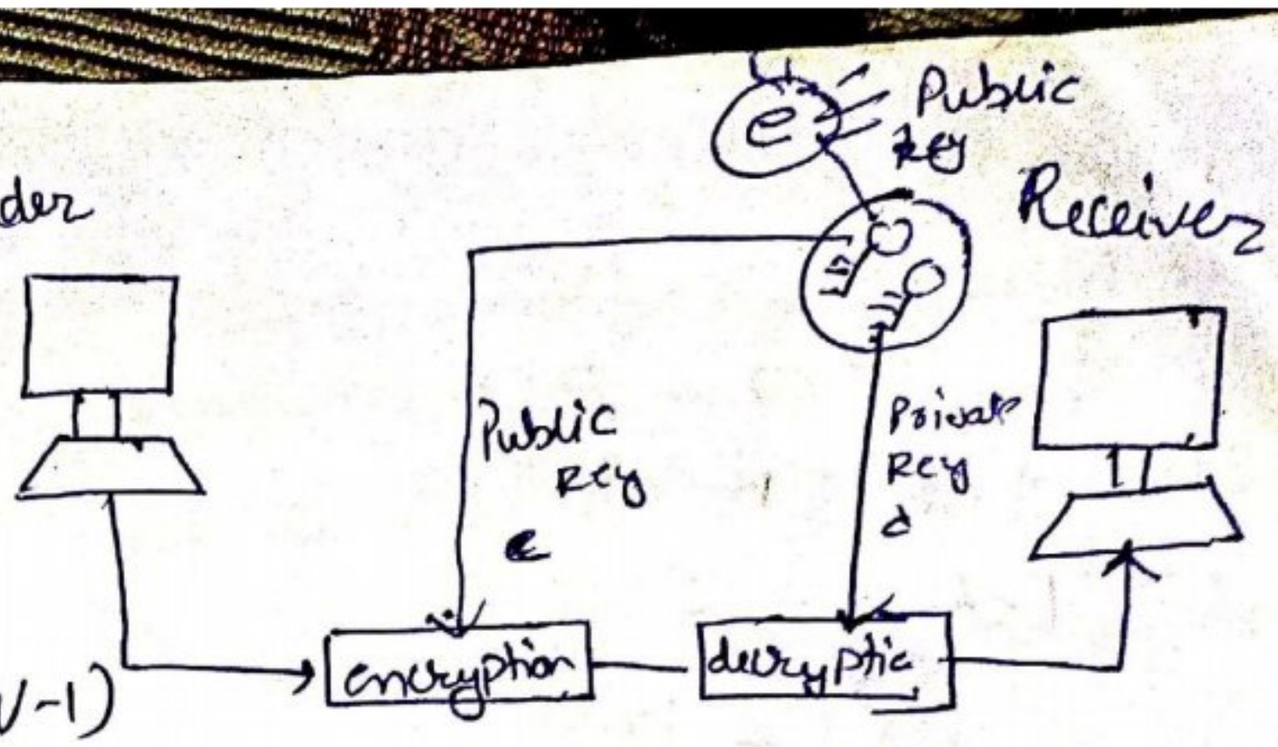






Token Bucket: when the tap is idle instead of making idle at each tick of clock add n token to the buffer which help in maintaining the data rate.

RSA Algorithm



1. Choose 2 large primeno p & q
2. Calculator $N = p \times q$
3. Calculate $\phi = (p-1) \times (q-1)$
4. Choose a random integer 'e' such that e & ϕ have no common factors. and Calculate d such that $d \times e \equiv 1 \bmod \phi$
5. Announce e and N to public and keep d & ϕ secret. Now encryption and Decryption will be as follows. Let P is plain text and C is Ciphertext

$a \equiv b \bmod \phi$
$(a-b)$ divisible by ϕ

6. Encryption:
$$C \equiv P^e \bmod N$$
7. Decryption:
$$P = C^d \bmod N$$

$d \times 7 \bmod \phi = 1$
$(d \times 7) - 1 \div 20 = 0$

Q Calculate public & Private key using RSA if $p=11$ & $q=3$ encrypt the message $P=5$ also decrypt it at receiver.

1. $p=11, q=3$
2. $N = 11 \times 3 = 33$
3. $\phi = 10 \times 2 = 20$
4. Let $e=7$
   $d \times 7 \equiv 1 \bmod 20$ } $(d \times 7) - 1 = 20m$ $(m=1,2,3)$
   $\Rightarrow d = 3$ } $d=3$
5. $e=7$ $N=33$ } Announce to public $d=3, \phi=20$ } secret.
6. $C = 5^7 \bmod 33 = 14$
7. $P = 14^3 \bmod 33 = 2744 \bmod 33 = 5$

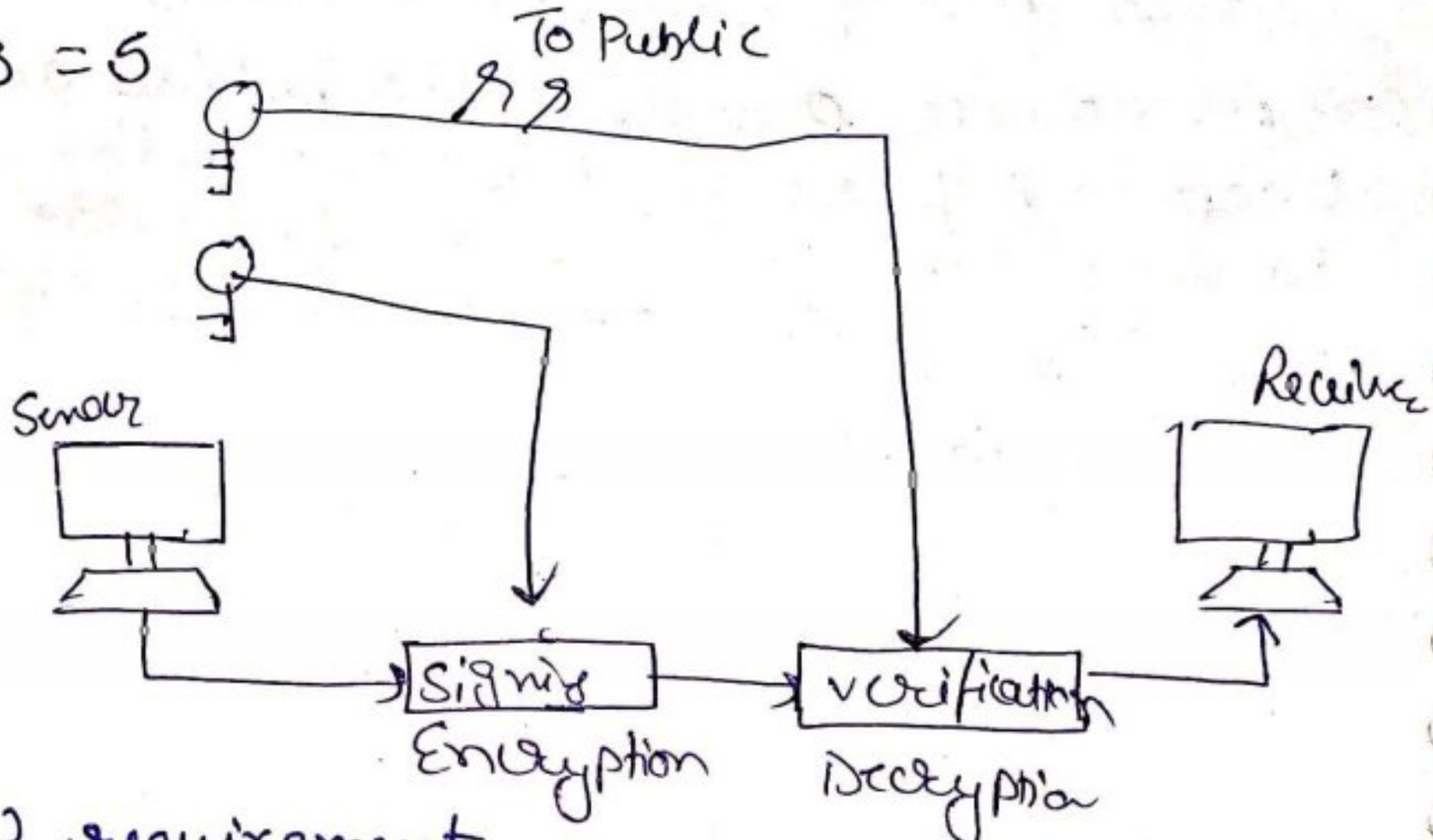
1. p = 11 q = 13
2. N = 11 x 13 = 143
3. ϕ = 10 x 12 = 120
4. d x e ≡ 1 mod ϕ
   Let e = 7
   d x 7 ≡ 1 mod 120
   d = 103
6. C = s^7 mod 143 = 47
7. P = 47^{103} mod 143 = 5

2, 5, 3, 4, ~~6~~, ~~12~~
&

(d x 7 − 1) = 120 m
d = 103

Digital Signature

→ signing
→ Relationship {one to one}
→ verification
→ Duplicity



Compression :-
It reduces b/w requirement
Encoder — Sender
Decoder — Receiver
} for efficient storage
Data transfer

It is of 2 types
→ Lossy
→ Lossless

Decompression
or
Reconstruction

In this the redundant bits (information) contained in the data are reduced due to removal of such information there is no loss of data of interest hence it is called lossless compression. It is also called data compaction

Lossy :- There is a loss of data but in a controlled manner This compression is therefore not completely reversible Lossy compression is used for digital data

Video compresion

Image compresion

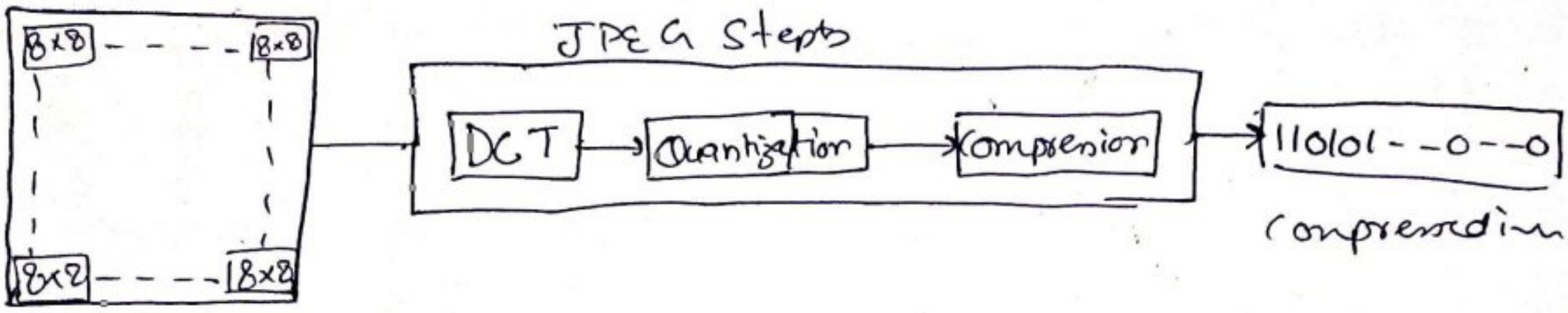
24bit = 2^{24} colours

8bits B/W = 2^8 colours

JPEG: Joint Photographic Expert Group

Image can be both B/W and coloured

JPEG divides the image into blocks in grayscale picture of 8x8 pixels (64 pixels)



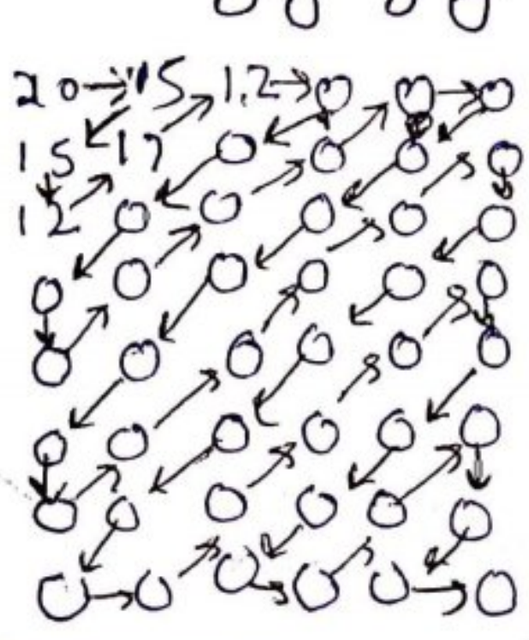
DCT {Discrete Cosine Transformation}

In this step each block of 64 pixels goes through a transformation called the discrete cosine transformation. The transformation changes the 64 values so that the relative relationship b/w the pixels are kept but the redundancies are revealed. DCT creates a table T(x,y) from table P.

Quantization: After the T table is created the values are quantized to reduce the number of bits needed for encoding. In quantization we divide a number by constants and drop the fractional part. This reduces required number of bits

Compresion: After the quantization the values are read from the table in a zig-zag manner and redundent zeros are removed

20
15



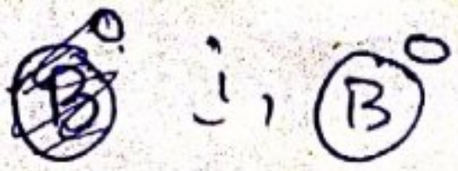
20-15-15-12-17-12-0-0

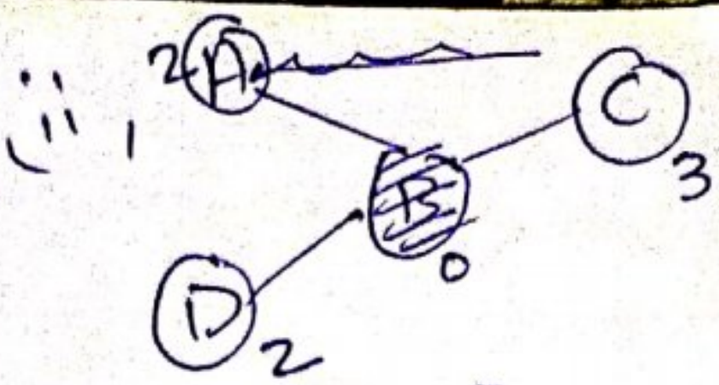
Ran.

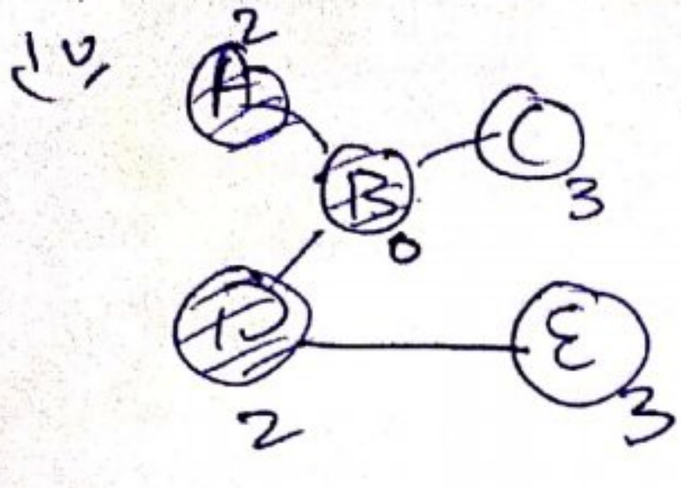
MPEG → Moving Pictures Expert Group

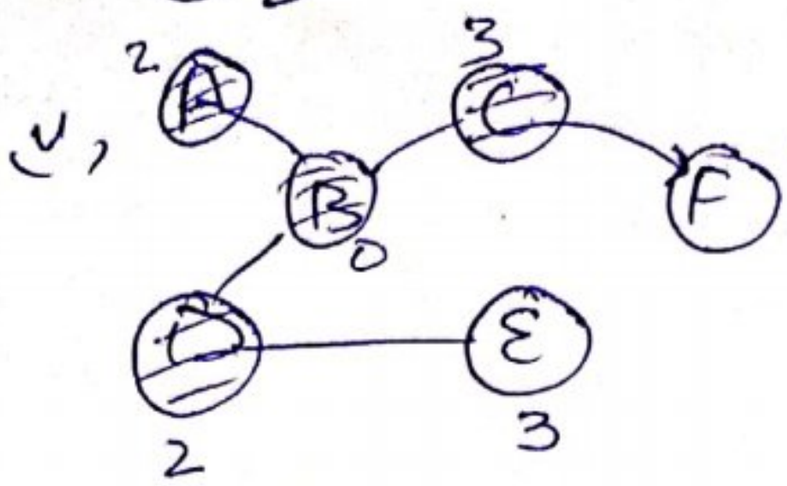
DNS (Domain Name System)
- → Generic — com, biz,
- → Country → in, UK, cn
- → inverse

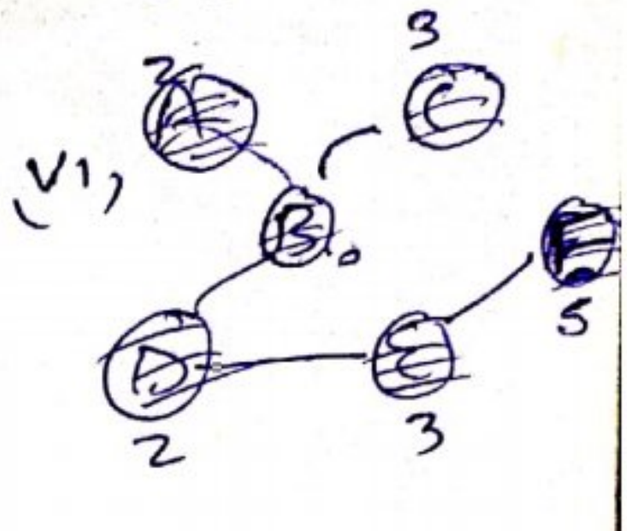
DNS client (resolver)
- Recursive
- Iterative

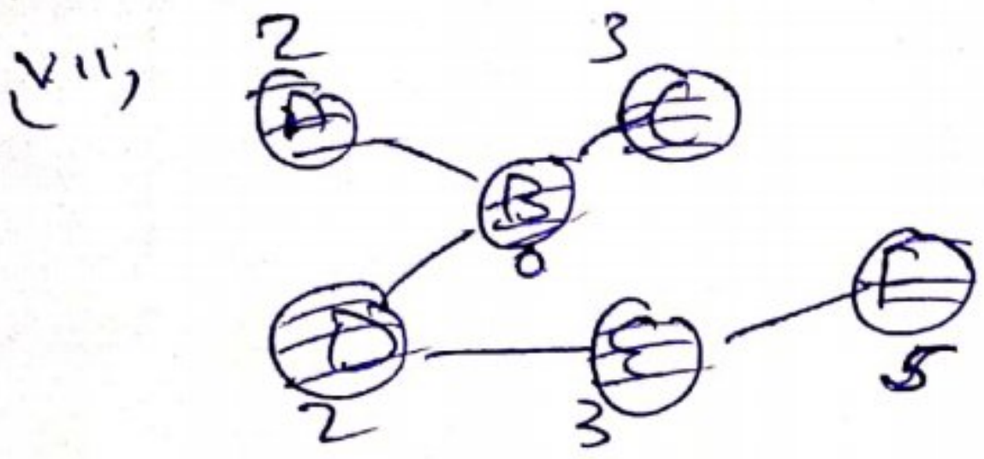












~~Roomer~~

To	Cost	Next
A	2	—
B	0	—
C	3	—
D	2	—
E	3	D
F	5	E

For C

Permanent	Tentative
1 Empty	C(0)
2 C(0)	A(5) B(3) F(5)
3 B(3) C(0)	A(5) D(5) F(5)
4 A(5) B(3) C(0)	D(5) E(6) F(5)
5 A(5) B(3) C(0) D(5)	E(6) F(5)
6 A(5) B(3) C(0) D(5) F(5)	E(6)
7 A(5) B(3) C(0) D(5) E(6) F(5)