NAME: Marena Fernandes ROLL NO: 8669 CLASS: SEIT

CN ASSIGNMENT NO. 2

Q.1 Explain compression techniques in detail. Hence compress the given data using LZW compression.
WYS * WYGWYS * WYSWYSG.

Ans. COMPRESSION:

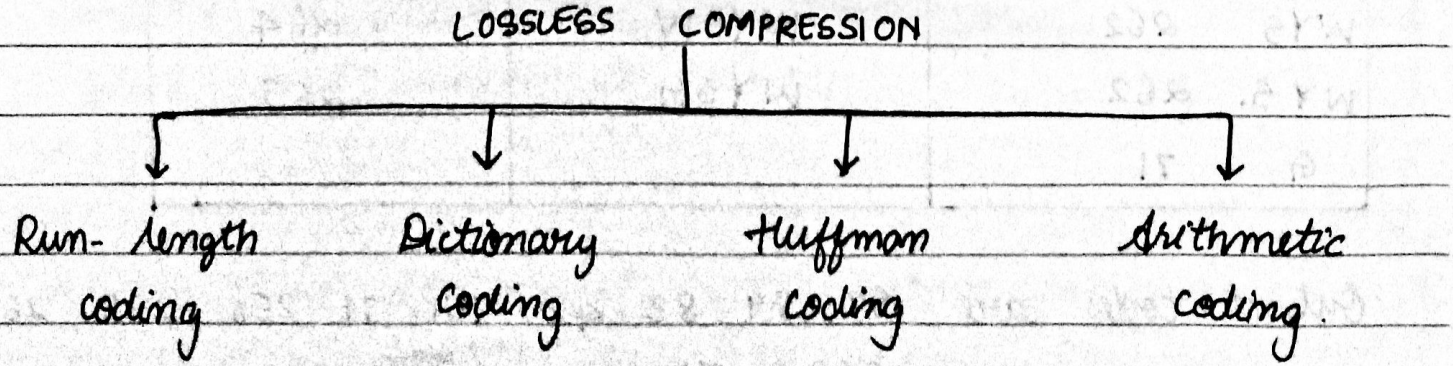
Due to large volume of data exchanged, compression plays an important role in multimedia communication

In compression, volume of data to be exchanged is reduced.

1) Lossless Compression:

In lossless compression, the redundant information contained in data is removed.

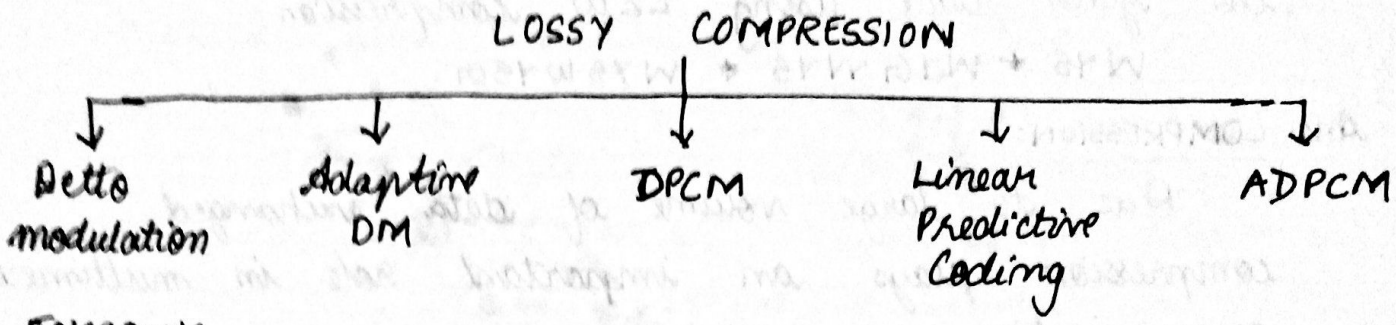
Due to such removal, there is no loss of data which contain information. Hence, it is called Lossless Compression.



2) Lossy Compression:

There is no limit on the amount of compression in lossy compression.

In this method there is loss of information in a controlled manner



ENCODING:

String		o/p Code	Addition
W	87	WY	256
Y	89	YS	257
S	83	S*	258
*	42	*W	259
WY	256	WYG	260
G	71	GW	261
WY	256	WYS	262
S*	258	S*W	263
WYS	262	WYSW	264
WYS	262	WYSG	265
G	71		

Output codes are 87 89 83 42 256 71 256 258 262 262 71

Q.2] Explain application layer protocols in details.

Ans: APPLICATION LAYER:

The application layer is present at top of the OSI model. It is ~~layer~~ layer through which user interacts.

1) Telnet:

Telnet stands for Telecommunications Network. It helps in terminal emulation. It allows telnet client to access resources of telnet server. It is used to managing files on the internet.

2) FTP:

FTP stands for File transfer Protocol. It is protocol that actually lets us transfer files. It can facilitate this between any 2 machines. But FTP is not just a protocol but it is also a program.

3) TFTP:

The trivial file transfer protocol is stripped down, stock version of FTP, but it is the protocol of choice if you know exactly what you want and where to find.

4) NFS:

It stands for network file system. It allows remote host to mount file systems over a network and interact with these as though they are mounted locally.

6) SMTP :

It stands for Simple Mail Transfer Protocol. It is part of TCP/IP protocol. Using method called store and forward, SMTP moves mail accross network.

6) LDP :

It stands for Line Printer Daemon : It is designed for printer sharing.

7) X Window :

It defines protocol for writing GUI based client / server applications. This idea allows a program, called a client, to run on one computer.

8) DNS :

It stands for domain Name Service. Every time on using domain name, a DNS server transcalates name to IP address.

Q.3] Differentiate between TCP and UDP. Hence find out following information from received TCP header.

E293 0017 00000001 00000000 5002 07FF

a. Source port no.
b. Destination port no.
c. Sequence no.
d. Acknowledgement no.
e. Length of header
f. Type of segment
g. Window size.

Ans.

TCP	UDP
• TCP stands for transmission control protocol	UDP stands for User Datagram Protocol.
• It is connection oriented.	It is connectionless protocol.
• TCP reads data in form of stream of bytes	UDP contains packets which are transmitted one by one.
• Header size is 20 bytes	Header size is 8 bytes.
• TCP is slower.	UDP is faster as error recovery is not attempted.
• TCP is heavier as 3 packets are required to setup connection.	UDP is lightweight. There is no tracking connections.
• Does error checking and recover.	Performs error checking but discards erroneous messages.
• Acknowledgement segments	No acknowledgement segments.

E293 0017 00000001 00000000 5007 07FF

TCP header contains following fields.

Source Port No. (2 bytes)	Dest. Port No. (2 bytes)		
Seq. No (4 bytes)			
Acknowledgement No. (4 bytes)			
HLEN (4 bits)	Reserved (6 bits)	Control flags (6 bits)	Window size (2 bytes)
Check sum (2 bytes)	Urgent pointer (2 bytes)		
optional data (0-40 bytes)			

a. Source Port No. $= (E293)_{16} = 58003$

b. Dest. Port No. $= (0017)_{16} = 23$

c. Sequence No. $= (00000001)_{16} = 1$

d. Acknowledgement No. $= (00000000)_{16} = 0$

e. Length of header = 5 i.e header $= 5 \times 4 = 20$ bytes.

f. Type of segment : Combination of reserved field and control field is $(002)_{16}$. The rightmost 6 bits in binary are 0000 0 which means only SYN bit is set which is used to establish connection.

g. Window size $= (07FF)_{16} = 2047$ bytes

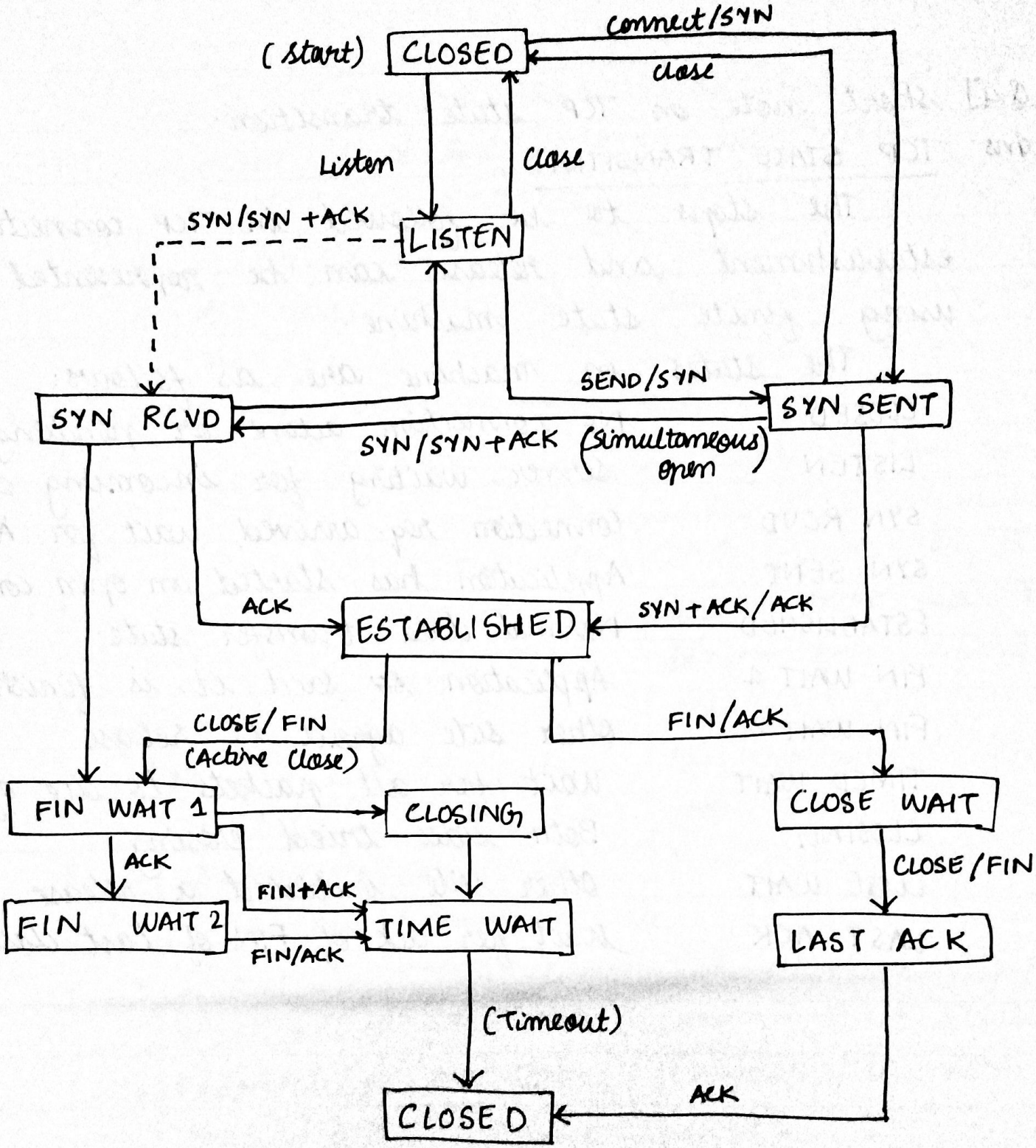
Q.4] Short note on TCP state transition.

Ans: TCP STATE TRANSITION

The steps to be followed in TCP connection establishment and release can be represented using finite state machine.

The states in machine are as follows:

CLOSED	No connection active or pending.
LISTEN	Server waiting for incoming call
SYN RCVD	Connection req. arrived, wait for ACK
SYN SENT	Application has started an open conn.
ESTABLISHED	Normal data transfer state.
FIN WAIT 1	Application ~~to~~ said it is finished
FIN WAIT 2	Other side agreed to release
TIMED WAIT	Wait for all packets to die off
CLOSING	Both sides tried closing
CLOSE WAIT	Other side initiated a release
LAST ACK	Wait for ack of FIN of last close


(start)
CLOSED
connect/SYN
close
Listen
close
SYN/SYN+ACK
LISTEN
SEND/SYN
SYN RCVD
SYN SENT
SYN/SYN+ACK
(simultaneous open)
ACK
ESTABLISHED
SYN+ACK/ACK
CLOSE/FIN
(Active close)
FIN/ACK
FIN WAIT 1
CLOSING
CLOSE WAIT
ACK
CLOSE/FIN
FIN+ACK
FIN WAIT 2
TIME WAIT
LAST ACK
FIN/ACK
(Timeout)
ACK
CLOSED

Q.5] Compare IPv4 and IPv6. Hence for given IP Datagram find out following information.

45000054 00030000 2006.....

a. header size
b. Are there any options in packet?
c. Size of data.
d. Is packet fragmented?
e. No of routers packet can travel.

Ans:

IPv4	IPv6
• IPv4 is 32 bit IP address.	IPv6 is 128 bit IP address
• Numeric address with bits separated by dot (.)	Alphanumeric address whose binary bits separated by colan (:)
• No. of header fields is 12.	No. of header fields is 8.
• It has checksum fields.	Does not has checksum fields.
• It supports for virtual length subnet Mask (VLSM)	Does not support VLSM.
• IPv4 offers different classes of IP address. Class A to E.	IPv6 allows storing unlimited number of IP addresses.
• Fragmentation done by sending and forwarding routes.	Fragmentation done by sender.
• eg. 192.168.0.1	eg. 2001:0bd8:0000:0000:0000:ff00:0047:7879

45 00 00 54 00 03 00 00 20 06

a. Header size = 5 × 4 = 20 bytes.

b. Since length of header is 20 bytes, there are no options.

c. Size of data = 84 - 20 = 64 bytes ∴ total length is 84.

d. D = 0, M = 0 offset = 0 packet is not fragmated.

e. Since value of time to live = 32
packet can travel 32 more routes.

Q.6] An organization is granted the block 130.56.0.0/16. The administrator wants to create 1024 subnet.

a. Find no. of addresses in each prefix

b. Find subnet prefix

c. Find first and last address in first subnet

d. Find first and last address in last subnet.

Ans: Organization granted block 130.56.0.0/16.

a. No. of valid addresses in each subnet = 62

b. Subnet prefix = 130.56

c. First address in 1st subnet = 130.56.0.1
Last address in 1st subnet = 130.56.0.62

d. First address in last subnet = 130.56.255.193
Last address in last subnet = 130.56.255.254

Q.7] The routing table of a router is shown below. Find out on which interfaces will the router forward packets addressed to destinations 128.75.43.16 and 192.12.17.10 respectively?

Destination	Sub net mask	Interface
128.75.43.0	255.255.255.0	Eth 0
128.75.43.0	256.255.255.128	Eth 1
192.12.17.5	255.255.255.255	Eth 3
default		Eth 2

Ans: Packet 1: 128.75.43.16

(128.75.43.16) and (128.75.43.0) = (128.75.43.0)

(128.75.43.16) and (255.255.255.128) = (128.75.43.0)

Since both of the masks are producing same ~~net~~ network ID, one with greater numbers of one will selected.

i.e. $(10000000)_2 > (0)_2$

128 in binary has more number of 1s than that of 0.

∴ Eth 1 will be selected.

Packet 2: 198.12.17.10

(192.12.17.10) and (255.255.255.0) = (192.12.17.0)

(192.12.17.10) and (255.255.255.128) = (192.12.17.0)

(192.12.17.10) and (255.255.255.255) = (192.12.17.10)

as it does not match with any network id, it will be forwarded to default.

∴ Eth 2 will be selected.

Q.8] An IP packet with 2500 bytes of data plus header passes through IP network with MTU 500 bytes. How many additional bytes will be delivered at destination?

Ans. Given that,

Header + Data = 2500 bytes.

Let size of IP header = 20 bytes.

∴ data = 2480 bytes.

MTU = 500 bytes.

Here 20 bytes for header of each fragment of data.

∴ 480 bytes of data.

fragments = 2480 / 480

≈ 6 fragments.

∴ 6 × 20 = 120 bytes of header will be delivered.

∴ Extra data = (2480 + 120) - 2500

= 100 bytes

100 bytes of extra data will be received at receiver end.

Q.9] IP packet, value of HLEN is 5, and value of total length field is 1000 in decimal, how many data bytes that packet carriers?

Ans: HLEN = 5

Total length field = 1000

Header size = 5 × 4 = 20 bytes

$(1000)_{10} = (1111101000)_2$

∴ No. of bits = 10

∴ Size of packet allowed = $2^{10} - 1$

= 1023 bytes.

Out of 1023 bytes, 20 bytes will be header

∴ Data bytes = 1023 - 20

= 1003 bytes

Packet contains 1003 bytes.

Q.10] A message is made up entirely of characters from the set X = {P, Q, R, S, T}. The table of probabilities of each character is shown below:

Character	Probability
P	0.22
Q	0.34
R	0.17
S	0.19
T	0.08
Total	1.0

A message of 100 characters over X is encoded using Huffman coding. Then the expected length of the encoded message in bits is _____.

Ans:

P	0.22
Q	0.34
R	0.17
S	0.19
T	0.08

R, S, T → RT (0.25)

Q	0.34
RT	0.25
P	0.22
S	0.19

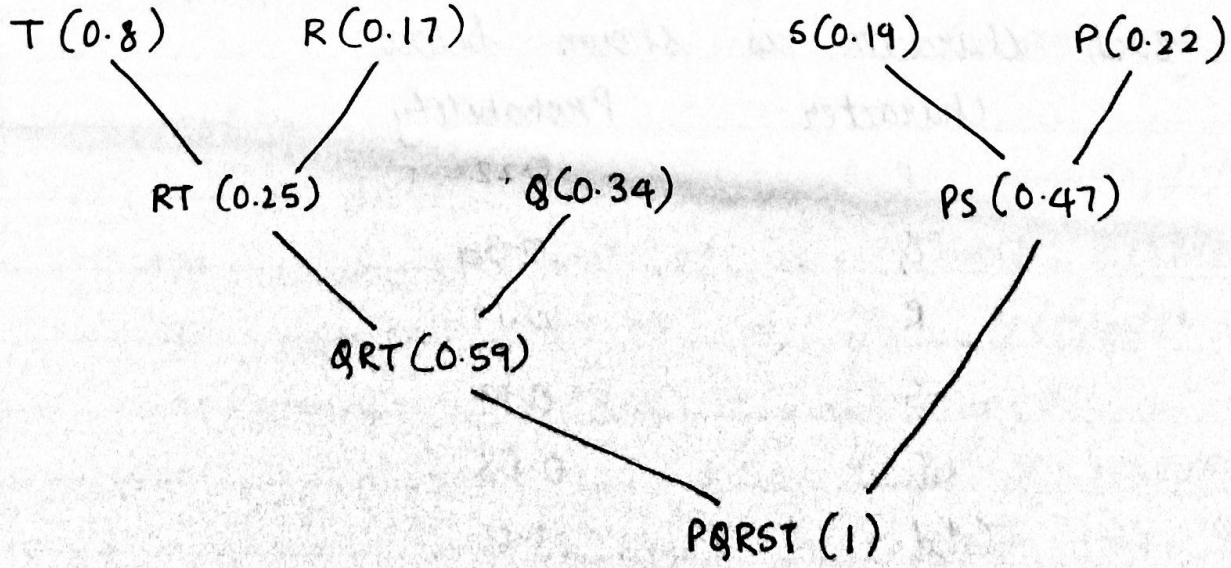
P, S → PS (0.41)

PS	0.41
Q	0.34
RT	0.25

Q, RT → QRT (0.59)

QRT	0.59
PS	0.41

QRT, PS → PSQRT ≡ 1.00



here, no. of bits by each P = 2

Q = 2

R = 3

S = 2

T = 3

∴ Expected length of encoded message

= 3(0.8) + 3(0.17) + 2(0.19) + 2(0.22) + 2(0.34)

= 2.25

For 100 characters message = 2.25 × 100

= 225 bits

Q.11] Short notes on:

a. Berkleys socket :-

Ans: Berkleys socket is an Application Programming Interface (API) for internal sockets and Unix domain sockets, used for inter process communication (IPC)

It is commonly used as library of linkable modules.

A socket is an abstract representation for the local endpoint of a network. Berkley socket API represent it as a file descriptor.

Common functions of library are:

Socket — Creates a new socket of certain socket type.

bind — Typically used on server side to associate socket with address.

listen	Used on server side and cause TCP socket to enter listening state.
connect	Used on client side to connect to server
close	Used to close socket connection.
send	Used to send message.
recv	Used to receive message.

b. Piggybacking.

Piggybacking is networking is a technique to utilize available bandwidth more efficiently.

The host does not send acknowledgement immediately but waits for some time and sends it with outgoing packet.

Consider 2 way communication b/w A & B:

A sends some data to B

B has to send to A.

B waits and sends ack with packet in which it contains message for A.

This approach is called piggybacking.

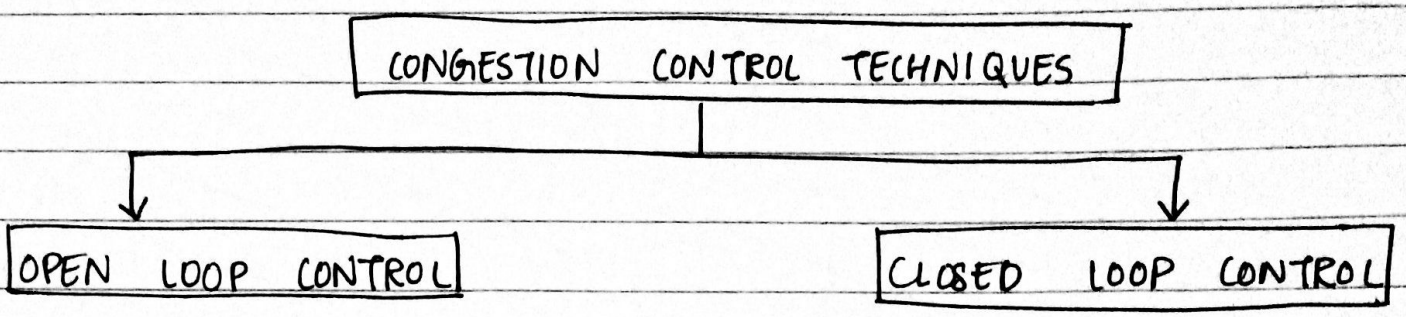
- Advantage:

  Better Utilization of network bandwidth.

- Disadvantage:

  While waiting to send for ack, transmitter may retransmit packet.

c. Congestion control Techniques :-



Congestion control techniques used to control or prevent congestion.

1) Open Loop Control:

In this method congestion ~~prog~~ prevented before it happens. Congestion handeled either by source or destination.

Policies Adopted:

- Retrasmision policy.
- Window Policy.
- discarding policy.
- Acknowledgement policy.
- Admission policy.

2) Closed Loop Control:

This technique is used to treat congestion ~~of~~ after it happens.

Techniques used are.

- Backpressure.
- Choke packet technique.
- Implicit Signaling.
- Explicit Signaling.

Many of these methods handeled by protocols.