DATE ___/___/___

Frames — data link layer
Packets — Network layer
process to process — Transport layer

Addressing

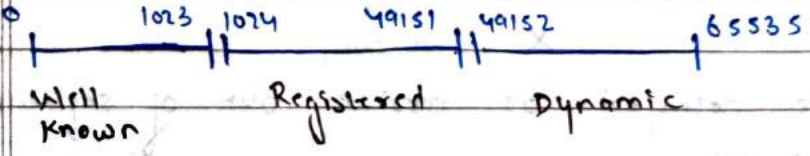
physical — MAC address:- (Data link layer) Unique identifier of Network
logical — IP address:- (Network layer) Assigned to each device on network.
Port Number:- (16 bit) (0-65535)

Types of Port Number:

(i) Ephemeral port No. (temporary)
(ii) Well known port No. (universal)
Server side port no. is universal
client side port no. is temporary

IANA Ranges (Internet Assigned Number Authority)

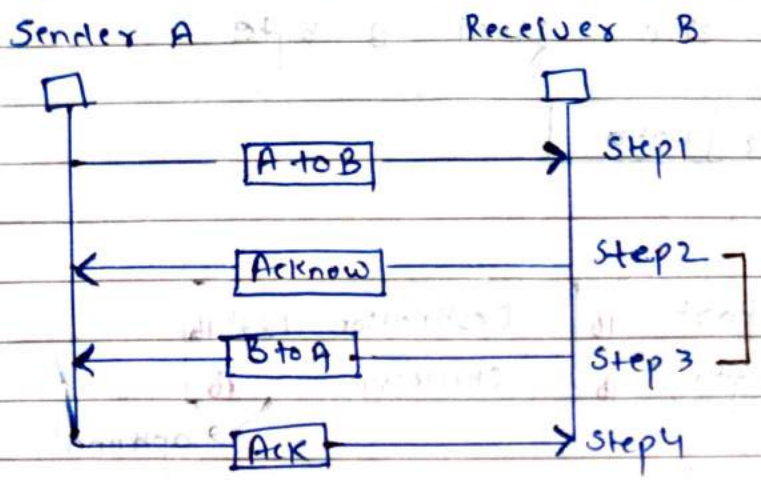
(i) Well known ports (0-1023)
Assigned & controlled by IANA
(ii) Registered (1024-49151)
not assigned or controlled by IANA (registered ✓) to prevent dyplication
(iii) Dynamic / private:- (49152-65535)
neither controlled or registered by IANA
These are ephemeral port no.



DATE ___/___/___

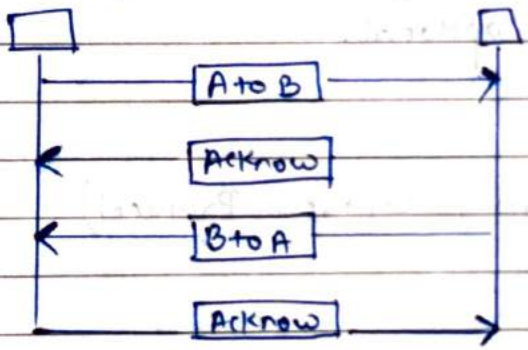
Connection - oriented Service

Connection establishment



4-way Process
Can be 3-way Process

Connection Termination



4-way Process cannot be reduced to 3-way

UDP (User Datagram Protocol)

- Connection less
- Unreliable
- For small messages
- No flow and error control

	Port No.
Echo	7
Discard	9
Daytime	13
SNMP	161

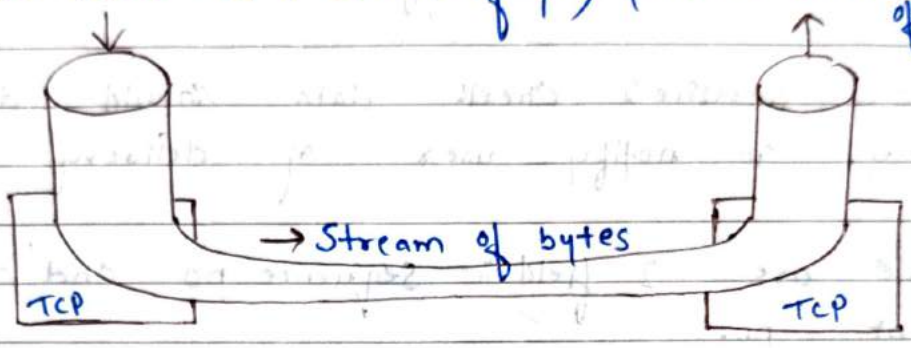
For simplicity divide sending buffer into 20 parts.

DATE / /

TCP Services

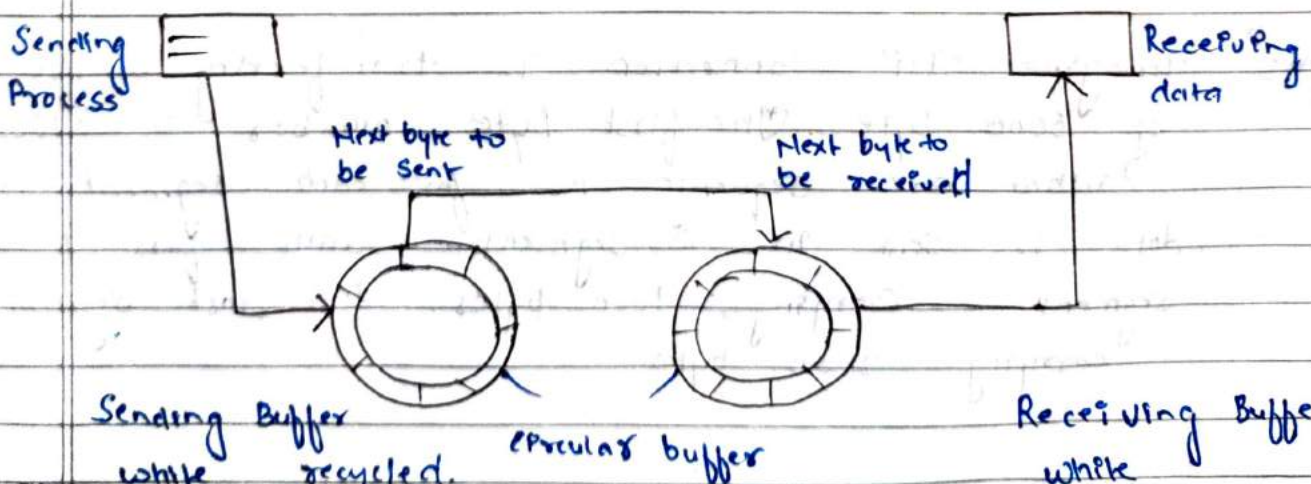
Stream delivery Service.

Sending Process (deliver data as a stream of bytes) | Receiving process (Obtain data as a stream of bytes)



Because sending and receiving process, not produce and consume data at same speed, we need buffer.
Sending Buffer
Receiving Buffer.

At transport layer TCP, group no. of bytes together into ~~bytes~~ packets. TCP add. Header to each segment and delivers segment of IP for transmission.



Be Positive...

DATE ___/___/___

Full Duplex Service :- Data can flow in both direction at the same time.

Half Duplex Service :- Data can flow in both direction but at different time.

Reliable Service :- Check data should deliver safely, if notify user if delivery fails.

There are 2 field :- Sequence no and acknowledgement no.

Sequence no :-

Acknowledgement :- Confirm the byte has received

Sequence no. range :- $0 \rightarrow 2^{32}-1$

eg :- 1057 and total data to be sent are 6000
1057 to 7056

Acknowledgment no = 7056 + 1 = 7057

Sequence no. to each segment | --- | --- | 1059 | 1058 | 1057 | →

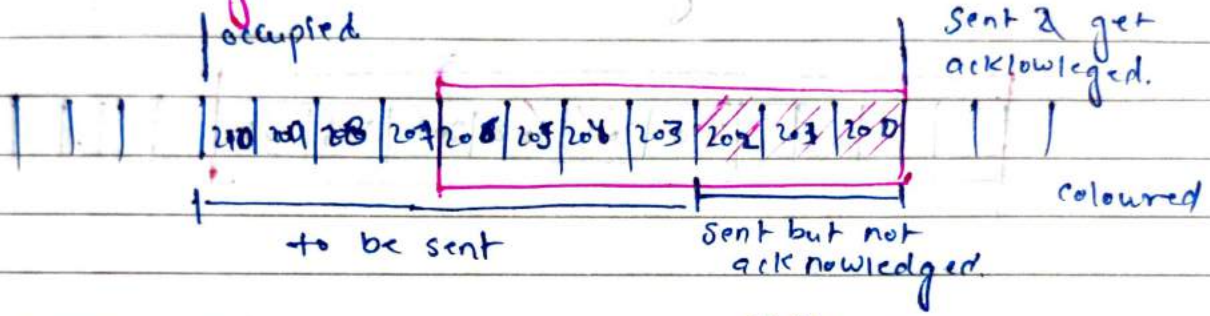
Ques Imagine TCP connection is transferring a file of 6000 byte. The first byte number is 10010 what are sequence no. for each segment if data is sent in 5 segments with first 4 segment carrying 1000 bytes and last segment carrying 2000 bytes.

DATE / /

	Sequence No.	Range.
Segment 1	10010	10010 – 11009
Segment 2	11010	11010 – 12009
Segment 3	12010	12010 – 13009
Segment 4	13010	13010 – 14009
Segment 5	14010	14010 – 16009

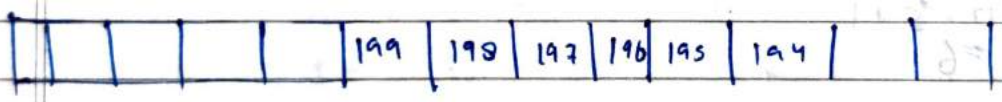
Sliding Window Protocol

Sender window
Sender side buffer



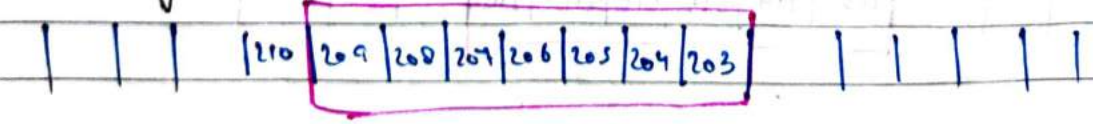
Size - 7

Receiver window



N = 13
M = 6
13 - 6 = 7 free space.

Suppose the sender sends two more 6 and acknowledgement is received i.e 203 with no change in window size.



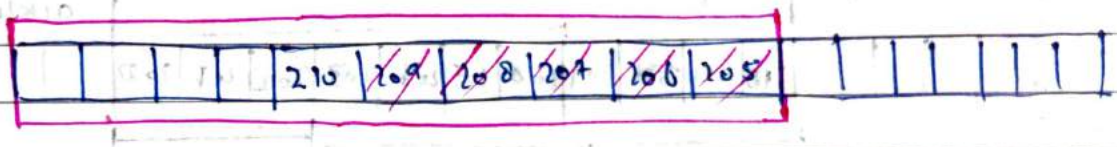
DATE / /

Sliding the sender window

Expanding the sender window

Ack. expecting. 205
At the same time increase the value of reciever window size to.

And the sending TCP has send 5 bytes.



Shrinking the Sender window

Send. → received
10 - 5 + 1
= 6

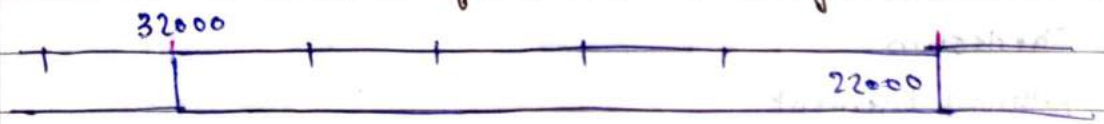
The receiver has received 5 bytes. However the receiving
which means free space is reduced to 6
and ack is 210.
TCP sends two more bytes.

Be Positive...

DATE ___/___/___

Ques A TCP connⁿ is using a window size of 10,000 bytes and the previous ack no was 22,001 It receives a segment with ack no. 24,001 draw a diagram to show the situation of window before and after.

Before Acknowledgment



After:

Ques OSI Model
Circuit Switching | Packet Switching.
LAN | MAN | WAN
Selective Repeat | Go Back N
Network Devices

DATE ___/___/___

Error Control

Error control includes mechanism for detecting corrupted segment, lost segments, out of order segments, duplicate segments.
TCP uses 3 simple tools.

1- Checksum
2- Acknowledgement
3- Time Out

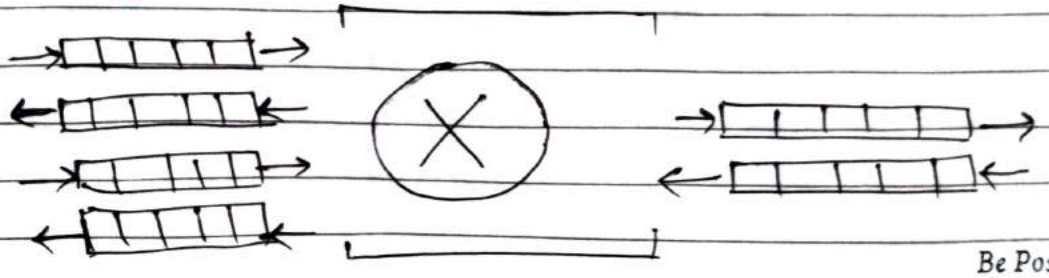
Each segment includes the checksum field which is used to check for a corrupted segment. If the segment is currpted it is discarded by ~~TCP~~ destination.

TCP uses the ack. method to confirm the of those segment that have reached the destination uncurrpted. +ve ack is used in TCP.

If a segment is not ack. before the timeout it is considered to be either currpted or lost.

Congestion Control & Quality of service

Congestion.



DATE / /

Congestion in a network may occur if the load of the network (no. of packets sent to network) is greater than the capacity of the network (no. of packets the network can handle)

Congestion control refers to mechanism & technique to control the congestion & keep the load below the capacity.

Congestion in a network or inter-network occurs because routers and switches have queues. (buffers that hold packets before & after processing)
When a packet arrives at the incoming interface it undergoes 3-steps before departing.

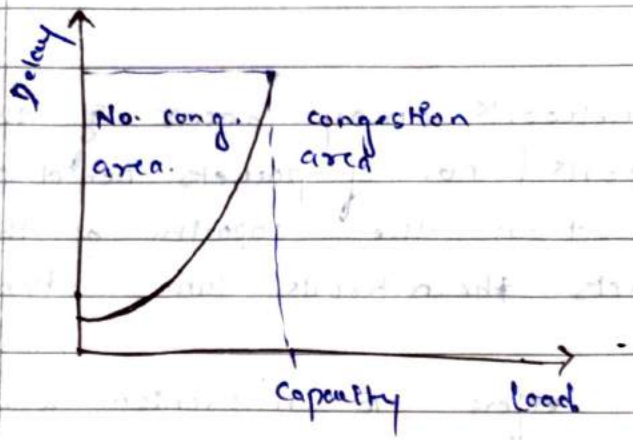
Step1- The packet is put at the end of the input queue while waiting to be checked.

Step 2- The processing module of the router removes the packet from the input queue once it reaches the front of the queue and uses its routing table and the destination addr to find the route.

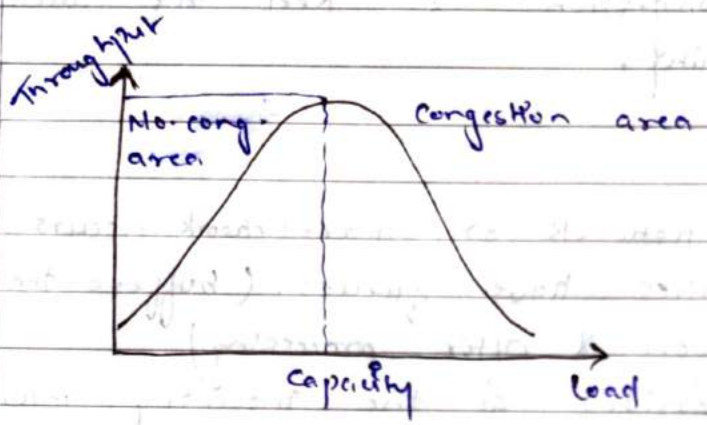
Step-3 The packet is put in the appropriate output queue and waits for its turn to be sent.

we can define throughput as the no. of packet passing through the network in a unit of time.

DATE / /



Note that the delay becomes infinite when load > capacity



1. Open loop congestion control
2. Closed loop congestion control

1 a- Retransmission policy
b- Acknowledgement policy
c- Discarding policy
d- Window policy

Selective repeat window is better than go back-N window.

c- In audio transmission if the policy is to discard less sensitive packets when congestion is likely to happen. The quality of sound is still preserved & congestion is prevented.

DATE / /

e Admission Policy

It is quality of service mechanism, can also prevent congestion in virtual circuit networks. Switches in a flow first check the resource requirement of a flow before admitting it to the network.

Closed loop congestion control

Try to elevate congestion after it happens.

a. Back pressure :-

b- Choke point :- A choke point is a packet sent by a router to the source to inform it of congestion

c- Implicit Signalling :- Sender feels itself that congestion has occured.

d- Explicit Signalling :- backward signalling (congestion ki opposite direc") informs sender
Forward signalling (congestion ki direc") informs receiver

The routers that experience congestion can send an explicit signal, the setting of a bit in a packet. to inform the sender or receiver of congestion.

Bursty or not constant 

DATE ___/___/___

Congestion in TCP

Actual window size = min (receiver window size, congestion window size)

→ In TCP the senders window size is determined not only by the receiver but also by congestion in the network.

→ The sender has two piece of information: the receiver advertised window size & the congestion window size.
The actual size of window is the min of these two.

Congestion Avoidance

To avoid congestion the sender TCP has two strategies, one is called slow start and additive increase. Second is multiplicative decrease.

Congestion Control in Frame relay

Congestion in frame relay network decreases in throughput and increase delay

→ A high throughput and low delay are the main goal of the frame relay protocol.

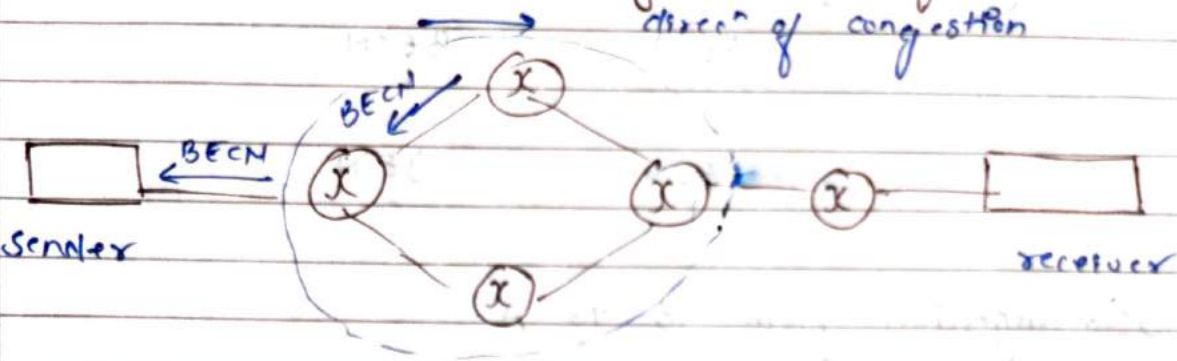
→ It does not have flow control in addition frame relay allow users to transmit bursty data.

DATE ___/___/___

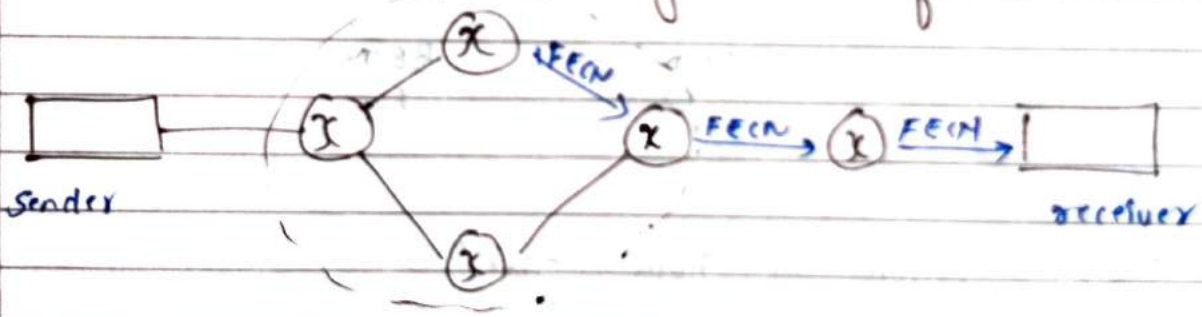
This means that a frame relay network has potential to be really congested through traffic. So requires congestion control.

Congestion Avoidance.

BECN (Backward explicit congestion notification)



FECN (Forward explicit congestion notification



When 2 end points are communicating using a frame relay network, 4 situation may occur with regard to congestion.

DATE / /

Quality of service

It is an internetworking issue which can be defined as flow which is required for communication.

Flow characteristics.

Reliability Delay Jitter Bandwidth.

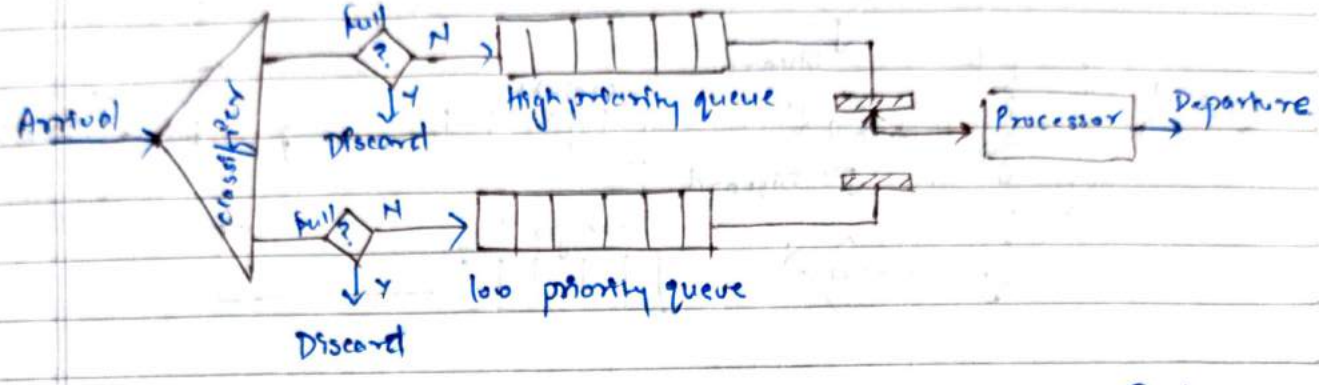
Reliability :-
No packet loss.
Ack. received on time
characteristic that a flow needs. lack of reliability means loosing a packet or acknowledgement. which retransmission. Ex:- It is more important that electronic mail, file transfer & internet access have reliable transmission than telephony or audio transmission.

Delay :-
Source to destination delay is another characteristic Applications can tolerate delay in different degrees. In this case telephony, audio/video conferencing & remote login need min. delay. while delay in file transfer or e-mail is less important.

Jitter :
Variation in delay for packets belonging to the same flow.

DATE ___/___/___

Priority Queuing.



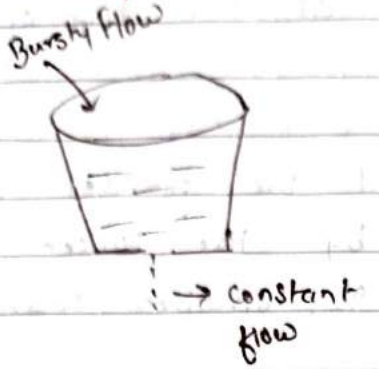
Packets are first assigned to a priority class. Each priority class has its own queue. The packets in the highest priority queue process first & packets in lowest priority queue are processed last.

A priority queue can provide better QoS than the FIFO because high priority traffic such as multimedia can reach the destination with less delay.

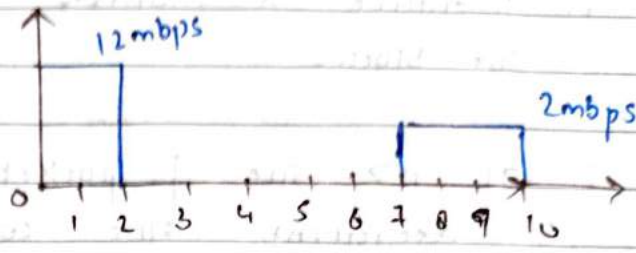
If there is continuous flow of high priority queue the packets in the lower priority queue will never have chance to be processed this condⁿ is called Starvation

DATE / /

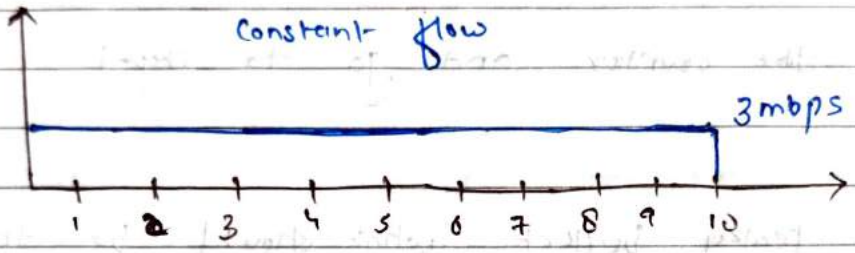
Leaky bucket



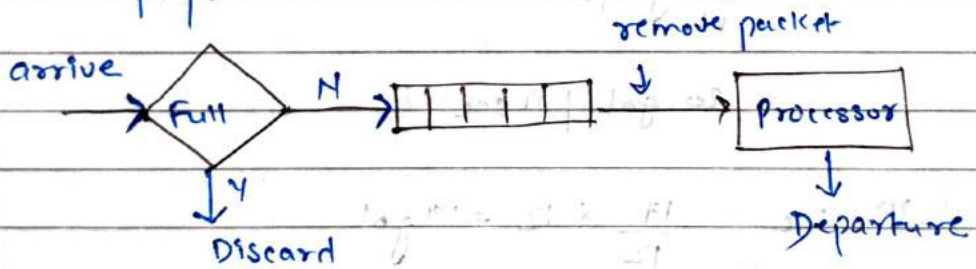
bursty flow



24 + 6 = 30mbps for 10sec



Rate at which water exists doesnot depends on rate at which water is entering until the bucket is empty.



The following algorithm for variable length packets.

If the traffic consist of fixed size packets the process removes fixed no of packets from the queue at each

If traffic consists of variable length packet the fixed output rate must be based on no. of bits / bits.

DATE / /

Algorithm

1- Initialize a counter to n at the tip of the block.

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

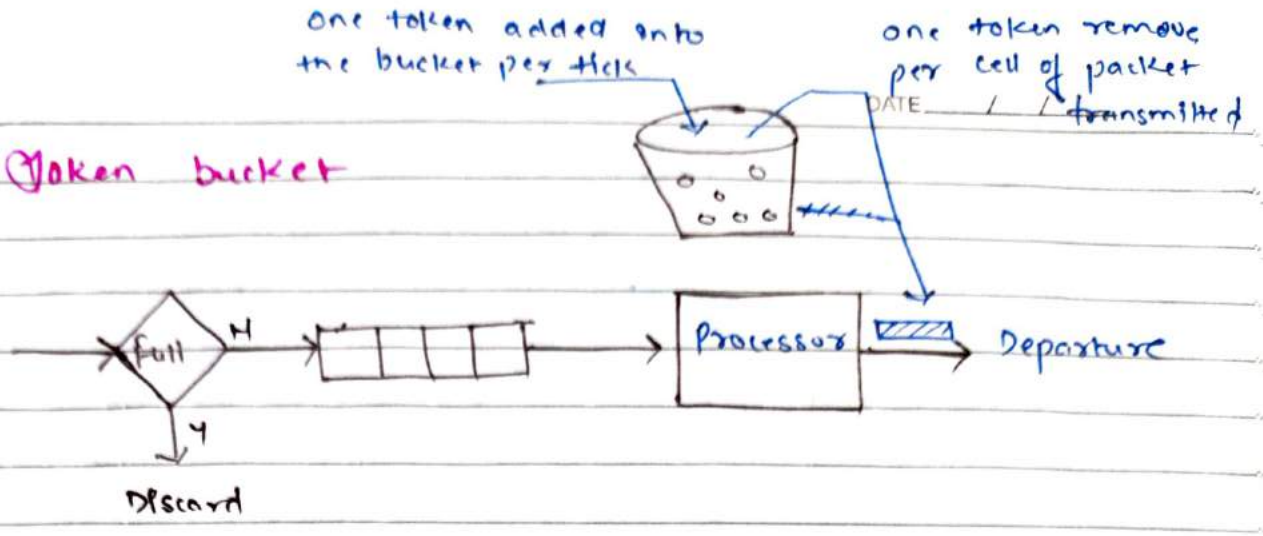
3- Reset the counter and go to step-1

Qu^r → In a leaky bucket what should be the capacity of bucket if the output rate is 5 gallon ~~/sec~~ min and there is an input burst of 100 gallon / min for 12 sec and there is no input for 48 sec.

out $\frac{1}{12}$ gal/sec

in 20 gal / 12 sec

at 12th sec $\frac{19}{12} \times 12 = 19$ gal



Token bucket

The token bucket allows bursty traffic
The token bucket can be easily implemented with counter.
The token is initialized to zero. each time token is added
Each time a unit of data is sent, counter is decremented by one.
When counter is zero, the host cannot send data.

Difference b/w leaky bucket and token bucket

Token bucket	Leaky bucket
→ Token dependent	Token independent
→ If bucket is full token is discarded but not the packet	If bucket is full, packets are discarded.
→ Packets can only transmit when there are enough tokens.	Packets are transmitted at constant rate
→ Allow large bursts to be send at faster rate	Sends packet at constant rate

DATE / /

Attacks

Passive attack

Release of message contents

traffic analysis

Active attack

Masquerade

Modification

replay attack

alteration

Denial of Service

Passive attack donot involve any modification to the content of original message.
Release of message content is quite simple to understand when we send a confidential e-mail message to our friend and our desire that only he be able to access it but the content of message are released against our wishes to someone else.
Traffic analysis:- If many messages are passing through a passive attacker could try to figure out similarities b/w them to come up with some sort of pattern that provides some clues regarding the communication that is taking place. Such attempts of analysis of messages to come-up with likely patterns are the works of traffic analysis attacks.

Denial of service make an attempt to prevent legitimate users from accessing some services which they are eligible for. For instance an unauthorized user might send too many login request to a server using random user ids in quik succession

virus, worm, trojen balls, Sniffing & Spoofing, fishing & farming

DATE ___/___/___

so as to flood the network and deny other legitimate users to use the network facilities.

Cryptographic Techniques.

Substitution

Ceaser cipher Key → 3 places down
A L O K → plain text
D O R N → cipher text

modified version of Ceaser cipher

cipher text K W U M P M Z M

An attack on cipher text message wherein the attacker attempts to use all possible permutations and combinations is called a brute force attack

The process of trying to break any cipher text message to obtain the original plain text message itself is called crypt analysis and a person attempting a crypt analysis is called crypt analyst

Mono-alphabetic cipher substitution
In mono alphabetic cipher, rather than using a uniform scheme for all the alphabets in a given plain text message we decide
this means that in a given plain text message each a can be replaced by any alphabet (b — z)
and b can also " " " " " (A, c-z)
And so on.

DATE / /

Homophonic substitution cipher

It is very similar to monoalphabetic the diff b/w the two techniques is that where the replacement alphabet set in case of simple substitution is fixed but in case of homophonic substitution cipher one plain text alphabet can map more than one cipher text alphabet.

example A → can be replaced by (T, M, P, R)
B → by (P, I, Q, S) etc

Polygram substitution cipher

HELLO → YQEEV
HELL → ZXYT

Rather than replacing one plain text alphabet with one cipher text alphabet at a time, a block of alphabet is replaced by a totally different cipher text block.

Play fair cipher

Playfair example

P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

MY NA ME IS KH AN
XF OL IX MK SB LO

(If odd. add Z at last)

DATE

My name is Khan

My NA ME IS KH AN

XF OL IX MK SB LO

Keyword Harsh plain text:- My name is JUI kahate. I am harshu's sister

H	A	R	S	B
C	D	E	F	G
I	K	L	M	N
O	P	Q	T	U
V	W	X	Y	Z

My NA ME IS JU IK AH AT EJ AM
TS KB LF MH OM KL RA PS LC SK
NO

HA RS HU SS IS TE RX
AR SB OB HM QE ER

SX SI ST ER
RY HM FY LE

Be Positive...

DATE ___/___/___

Hill Ciphers

Step 1:- Treat every letter in the plain text message as a number i.e a=0, b=1 .. z=25

CAT C=2 A=0 T=19

$$\begin{bmatrix} 2 \\ 0 \\ 19 \end{bmatrix}$$

Now plain text matrix is multiplied by a matrix of randomly chosen keys. The matrix consist of size $n \times m$

$n \rightarrow$ no. of rows.

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

Now multiply the two matrix

Now compute %26 value of above matrix

$$\begin{bmatrix} 31 \\ 216 \\ 325 \end{bmatrix} \bmod 26 = \begin{bmatrix} 5 \\ 8 \\ 13 \end{bmatrix} \quad \begin{matrix} F \\ I \\ N \end{matrix}$$

For decryption.

Take cipher text matrix and multiply it by the inverse of the original key matrix.

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \times \begin{bmatrix} 5 \\ 8 \\ 13 \end{bmatrix} = \begin{bmatrix} 210 \\ 442 \\ 325 \end{bmatrix} \bmod 26 \begin{bmatrix} 2 \\ 0 \\ 19 \end{bmatrix}$$

DATE / /

$C = K.P \mod 26$

$P = K^{-1}.C \mod 26$

$$K^{-1} = \frac{adj(K)}{|K|}$$

Transposition Technique

Rail Fence Technique

Write down plain text message as a sequence of diagonals.

Read the plain-text written in Step 1 as a sequence of rows

Come Home Tomorr

C M H M T M R

O E O E O O R

COMHMTMROEOEOOR

DATE ___/___/___

Simple columnar Transposition Technique.

Write the plain text message row by row in a rectangle of a predefined size
Read the message column by column however it need not be in the order of column 1,2,3 etc It can be any random order such as 2,3,1
The message obtained is the ciphor text message.

C1	C2	C3	C4	C5	C6
C	O	M	E	N	O
M	E	T	O	M	O
R	R	O	W		

CMROERMTOEOWNMOO

Vernam Ciphor (one Time pad)

A=0 B=1 C=2 .... Z=25

Plain text :-

H	O	W	A	R	E	Y	O	U
7	14	22	0	17	4	24	14	20

One Time Pad :-

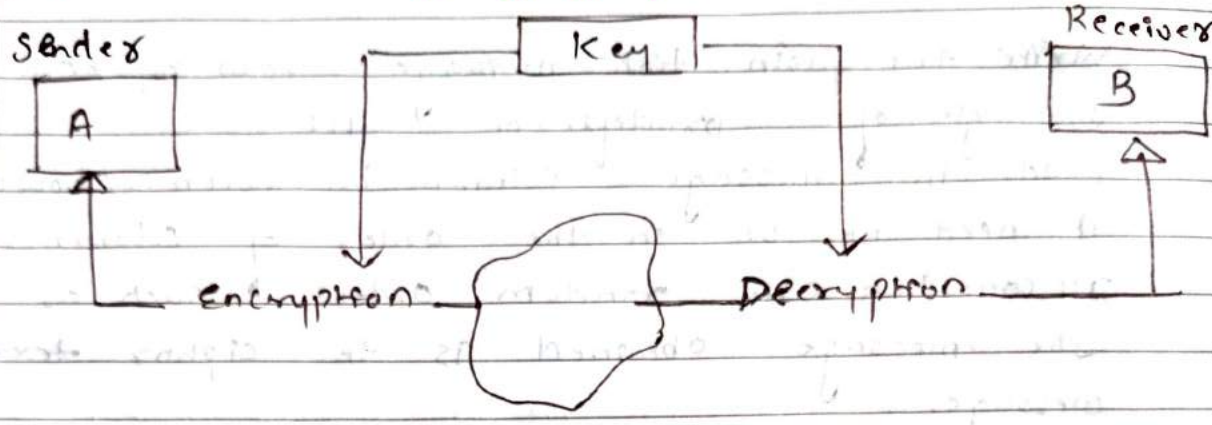
N	C	B	T	Z	Q	A	R	X
13	2	1	19	25	16	0	17	23

Sum

20	16	23	19	42	20	24	31	43	% 26
Ciphor text				16			5	17	
U	Q	X	T	Q	U	Y	F	R	

DATE ___/___/___

Symmetric Cryptography



Key Exchange Algorithm

A	B
$n = 11$ $g = 7$	$n = 11$ $g = 7$
$x = 3$	$y = 6$
$A = g^x \bmod n$	$B = g^y \bmod n$
$= 7^3 \bmod 11$	$= 7^6 \bmod 11$
$A = 2$	$B = 4$
$B = 4$	$A = 2$
$K_1 = B^x \bmod n$	$K_2 = A^y \bmod n$
$= 4^3 \bmod 11$	$= 2^6 \bmod 11$
$= 9$	$= 9$

Key pairs needed $= {}^nC_2 = \frac{n(n-1)}{2}$

Asymmetric Cryptography

A — public
A — private

B — public
B — private

public key — encrypt
private key — decrypt

DATE ___/___/___

Authenticity is not maintained ✗
Confidentiality ✓

Digital Signature.

A

public :- decrypt
private :- encrypt

A sends message by using his private key to encrypt
B decrypts the message using public key of A.

Authenticity ✓
confidentiality ✗