Theorems are —

1). Nyquist Theorem :-
↳ for Noiseless channel.

2). Shannon's Theorem :-
↳ for Noisy channel.

1). Nyquist Theorem :-

Two important characteristics of a transmission channel are —

(i) Signal to Noise ratio (SNR)
(ii) Bandwidth

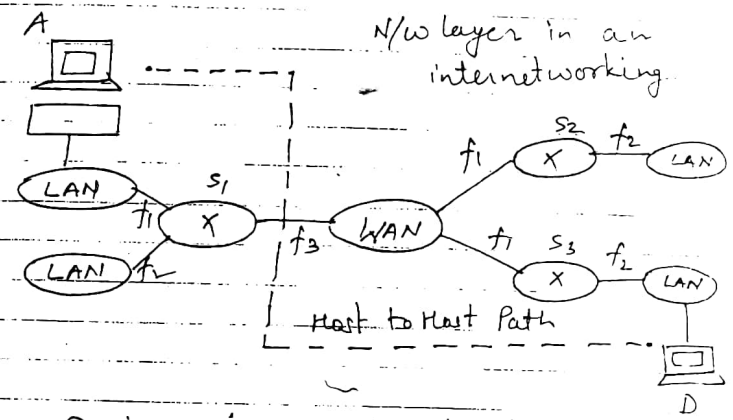
Nyquist theorem states that — "If the Bandwidth of channel is 'B' which carry a signal having 'L' no. of levels then the max. data rate 'R' on this channel —

$$R = 2B \log_2 L$$

As max. datarate for reliable transmission is defined as channel capicity 'C'. The above expression gets modified as —

$$C = 2B \log_2 L$$

NETWORK LAYER



Design issues of Network layer :-

(i) services provided to the transport layer.
(ii) internal organisation of the network layer.
(a) To use the connection oriented services.
(b) To use the connectionless services.

(a) To use the connection oriented service :-

it is called virtual ckt connection it is similar to the physical connection.
- establish the connection
- uses the connection
- release the connection

(b) To use connectionless service:

- it is also called datagram ckt.
- Packets move independently

Difference b/w virtual CKT & Datagram CKT

S.No	Parameter	Virtual CKT Subnet	Datagram Subnet
1.	CKT setup	Required	Not Required.
2.	Addressing.	each packets contains a virtual CKT number	each packet contains source as well as Destination Address
3.	Repair	Harder to Repair	easy to Repair
4.	State info.	A table is needed to hold the state info.	Subnet does not hold state info.
5.	Routing	Each packets of the message follow the same route. This is also called static Routing.	each packet is route independently This is called Dynamic Routing.
6.	conjection Control	easy to control	Difficult
7.	effect of Router failure	All virtual CKTs which passed through failed Router are terminated	No other effect except for the packet at the time of crash.

Router :→

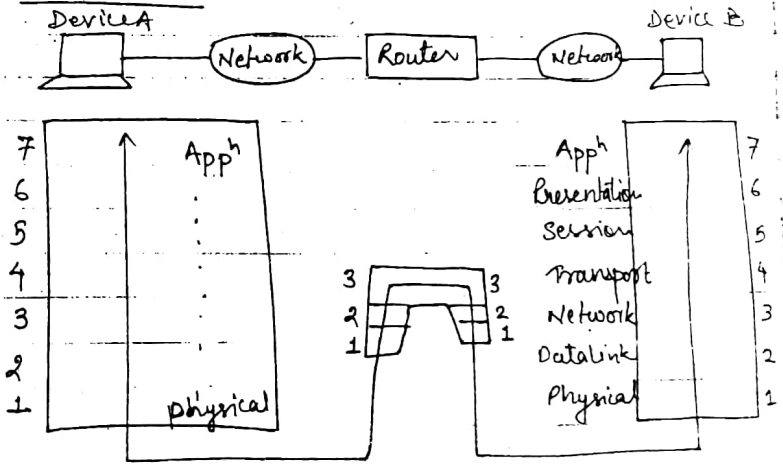


fig: A router in OSI Model.

- Router are the devices that connects two or more networks which is shown in figure.

- they consist of a combination of hardware & software.
- The hardware can be a network server, a separate computer, or a special device.
- The softwares in the Router are operating system of Router protocols, Management software can also be used.
- The Routers use logical & physical addressing to connect two or more logically separate networks.
- Route discovery is the process of finding the possible routes through the internetwork & then building routing tables to store that information.
- The two methods of Route discovery are —
  - (i) Distance Vector Routing.
  - (ii) Link State Routing.

dynamic algo

- Router works at the network layer of the OSI Model.

Imp

Routing Algorithms :→

static → Dijkstra
dynamic

- it is used to provide the best path from source to destination.
- it is responsible for deciding the output line on which a packet is to be send.
- such a decision is dependent on the robustness on the virtual ckt. it is a datagram ckt.

Properties of Routing Algorithms :→

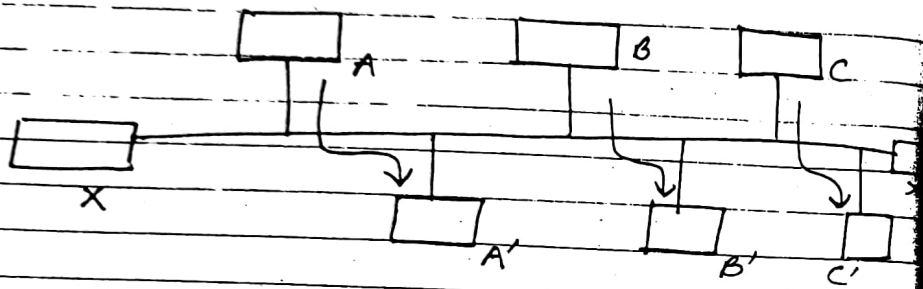
- Correctness & Simplicity :→
- Stability :-
- Robustness :-

it should be able to coperate with the changes in the topology & traffic without requiring all jobs in all host (PC) to be about it and the network to be rebooted every time some router crashes.

- fairness & optimality :→

↳ fair if No one approach.
↳ enough traffic between A & A', to saturate the horizontal link.

↳ to maximize the total flow, prevent traffic b/w x to x'



↳ Some compromize is necessary b/w global efficiency & fairness to individual connection is needed.

↳ Minimizing the packet delay.

↳ Maximizing the total n/w throughput.

Types of Routing Algorithms:-

(1) Non-adopted or static Routing Algo:-

↳ Choice of root is done in advance

↳ Routing decision is not based on current traffic & topology. e.g. shortest path Algorith is bit Strapping, flooding, flow based Routing

* Dijkstra

* Flooding :→

↳ every incoming packet is send out in every out going packet except the line on which it have arrive.

↳ Disadvantage :- large no. of duplicate packets.

↳ To prevent endless copies of packet we use the Hop Counter.

↳ destination must always prepared to receive multiple copies of the incoming packets.

↳ there are various defrading techniques such as -

- using the hop counter.
- to keep a track of which packet have been flooding.

Selective flooding :→

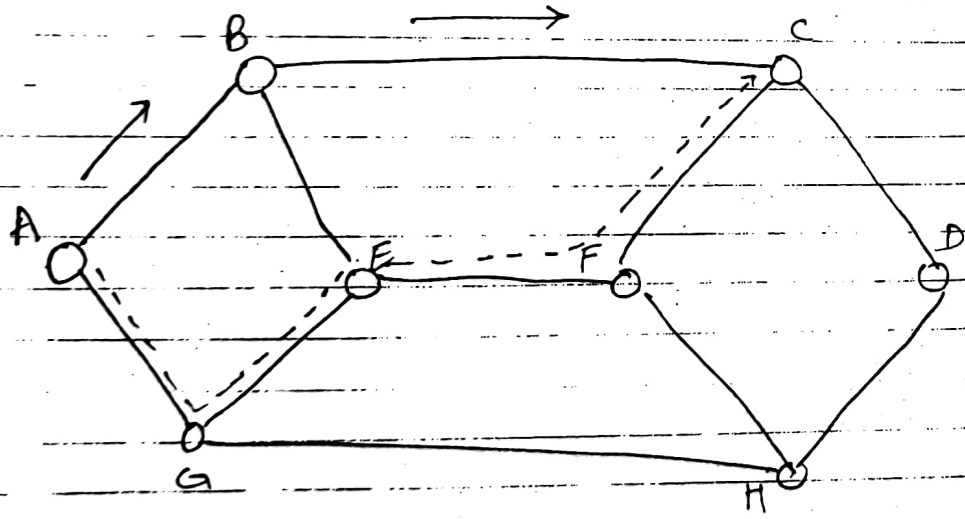
In this algorithm every incoming packet is not send out on every o/p lines.

↳ Infact, packet is sent only those lines which are approximately going in the right direction.

Application Of flooding :→

(1) Milit̄ry app^ns
(2) Robustness of flodding is very much desirable.
(3) used in distributed database applications.
(4) it always select the shortest path so it produces the shortest possible delay.

Flow based Routing :→



(2) Dynamic Routing Algorithm (or Adoplive)

In this algorithm, routing decision can be changed, if there are any changes in the topology of traffic. this is called dynamic routing.

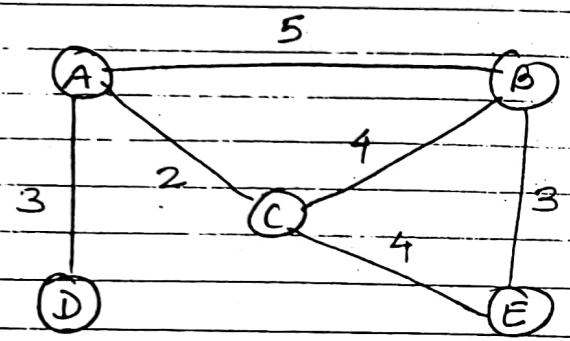
↳ Distance Vector,
↳ Link state Routing,
↳ Count to infinity problem

(i) Distance Vector Routing :→

In this algorithm, each router maintain a table called vector such a table gives the best known distance to each destination & the information about the lines to be used to reach there.

↳ This algorithm some times called by the other means (or Distributed Bellmanford Routing algorithm.
(b) Ford-Fulkerson Algorithm

Initialization :-



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

A's table

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

B's table

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

C's table

To	Cost	Next
A	~~∞~~	
B	~~∞~~	–
C	~~∞~~	–
D	0	
E	∞	–

D's table

To	Cost	Next
A	0	–
B	5	–
C	2	–
D	3	–
E	6	C

A's table

To	Cost	Next
A	5	–
B	0	–
C	4	–
D	8	A
E	3	–

B's table

To	Cost	Next
A	2	–
B	4	–
C	0	–
D	5	A
E	4	–

C's table

To	Cost	Next
A	3	–
B	8	A
C	5	A
D	0	–
E	9	A

D's table

To	Cost	Next
A	6	C
B	3	–
C	4	–
D	9	C
E	0	–

E's table

↳ **Sharing :-** If Node A shares its routing table with the Node C, Node C also knows how to reach to Node E. This is called the sharing.

In the Distance vector Routing each node share its routing table with its immediate neighbours periodically & when there is a change.

(ii) Link state Routing :→

Distance vector Routing was used in the ARPANET upto 1979. After that it was replaced by Link state Routing.

Link state Routing is simple & each router has to perform the following five op's :—

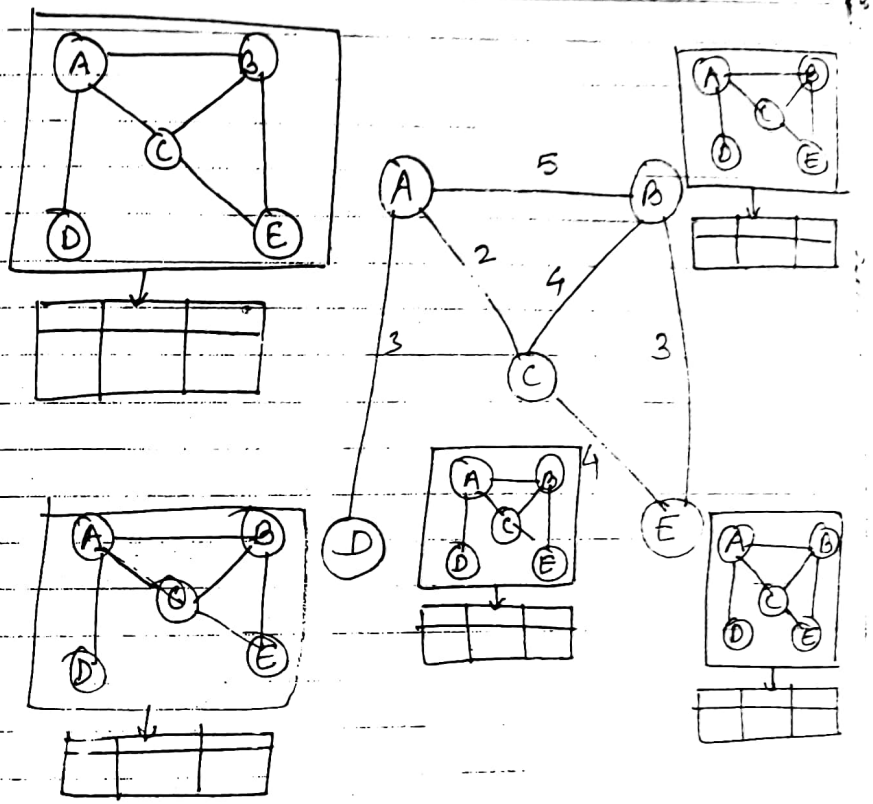
(a) each router should discover its neighbour & obtain there network address.

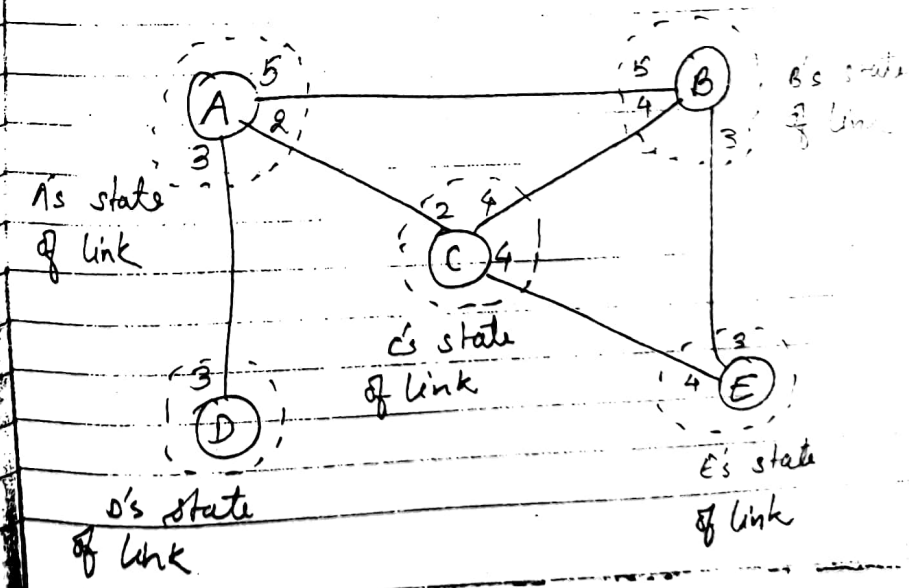
(b) Then it should return when the delay or cost to each of their neighbour.

(c) It should construct a packet containing the network address & the delays of all the Neighbours

(d) Send this packet to all the Routers.

(e) Compute a shortest path to every other Routers by the Dijkstra Algorithm.

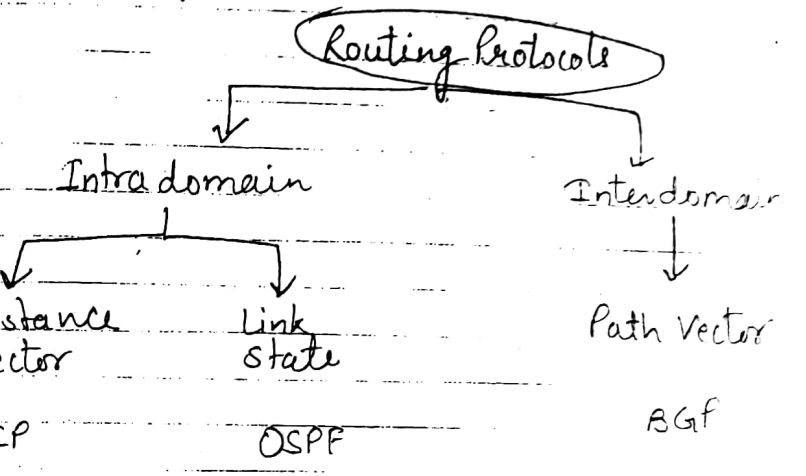


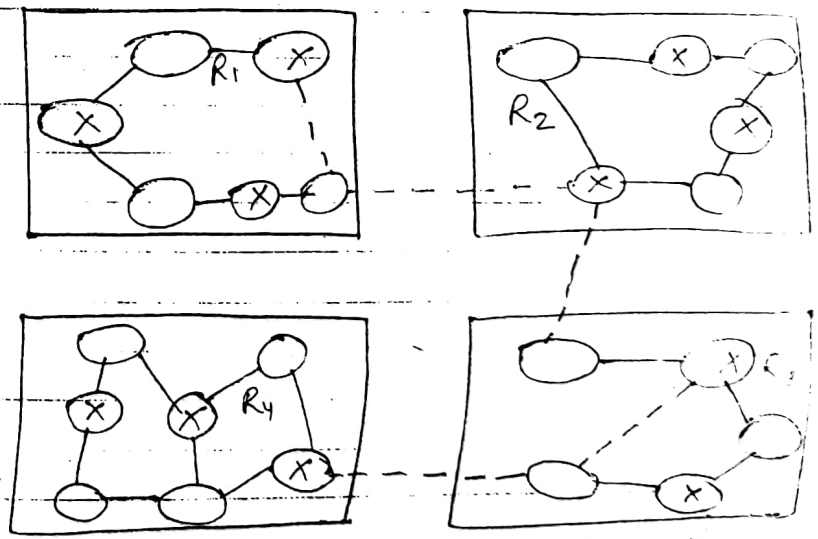


Difference b/w Distance Vector & Link State:-

Distance Vector	Link State
1. Each Router maintain routing table indexed containing one entry for each routers.	1. it is the advanced version of Distance vector Routing.
2. Bandwidth is less	2. Bandwidth is High
3. Routers measure delay directly with special packet	3. All delays measured & distributed to every routers.
4. it does not take line bandwidth into account when selecting the roots.	4. it considers the line bandwidth into account when selecting the roots.
5. Algorithms takes too long to converge. ~~Algorithm is~~	5. Algorithm is faster.

Routing Protocols :→





Autonomous System

Intradomain :- Routing Inside Autonomous system.

Interdomain :- Routing b/w Autonomous System

unicast → one to one
multicast → one to many

RIP: Routing Info. Protocol

OSPF: open shortest path first.

BGP: Border Gateway protocol.

Autonomous System:-

" " is a group of networks & the Routers.

Interdomain Routing :-

Routing b/w Autonomous System is called interdomain Routing.

Intradomain Routing :-

Routing inside the autonomous System is called Intradomain Routing.

RIP:→

↳ Routing Info. Protocol
↳ it is an intradomain routing protocol used inside an autonomous system.
↳ it is an implementation of distance vector protocol.

OSPF:-

↳ open shortest path first.
↳ it is intradomain Routing protocol based on link state Routing
↳ its domain is also an autonomous System

BGP:-

↳ Border Gateway Protocol.
↳ it is an interdomain Routing protocol using path vector Routing.
↳ it first appeared in 1989.

★ **Broadcast Routing :→**

↳ one to all.

sending a packet to all the destination simultaneously is called Broadcasting. (various method of Broadcasting is as follows:-

(i) **Simple Broadcasting :-** The source will simply send a distinct packet to each destination.
↳ This method has two drawback
(a) it waste the bandwidth
(b) The source has to a complete list of all destination.

(ii) Flooding :-

it is another method used for broadcasting.

↳ The problem with the flooding is that it has a point to point routing algorithm.

↳ it consume a lots of bandwidth & generates to many packets.

(iii) Multi Destination Routing :-

In this algo, each packet contains a list of destination, which indicates the desired destination. When such a packet arrive at router, the router first checks all the destination & decides the set of output lines that will be required.

↳ The Router Generate a new copy of the received packets for each output lines to be used.

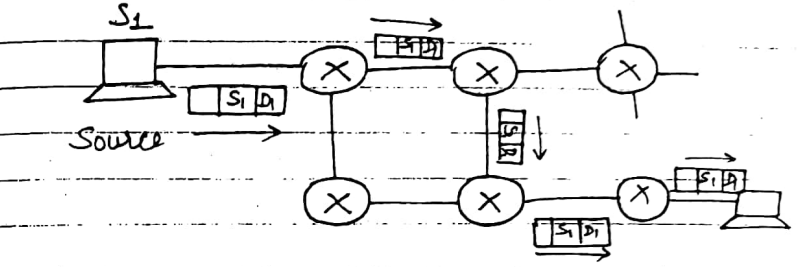
↳ it includes a list of only those destination that are to used the line in each packet going out on that line.

Multicasting Routing Protocol :-

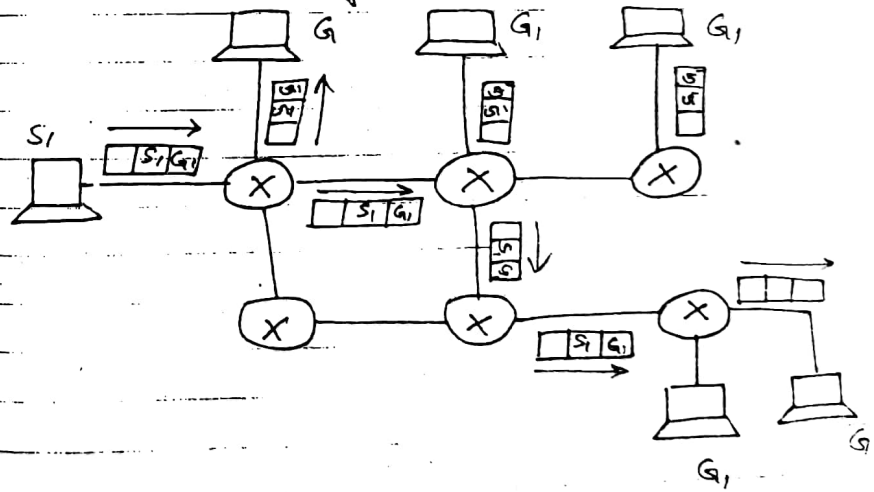
↳

29/3/11

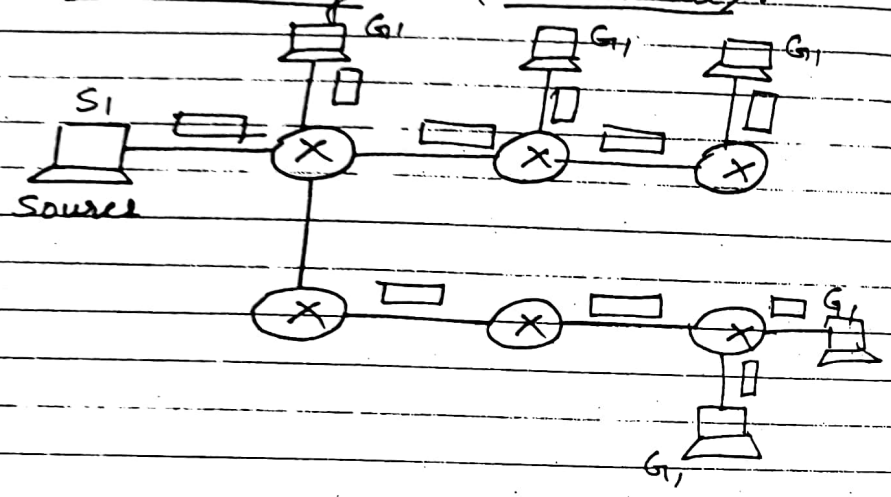
↳ ① unicasting (one to one) :-



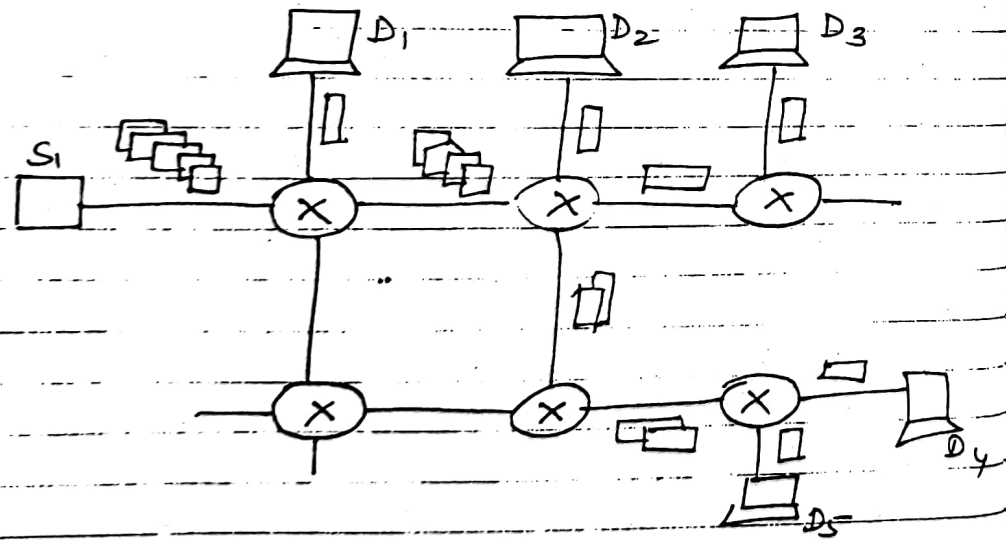
② Multicasting (one to many) :-



③ Broadcasting :→ (one to all) :-

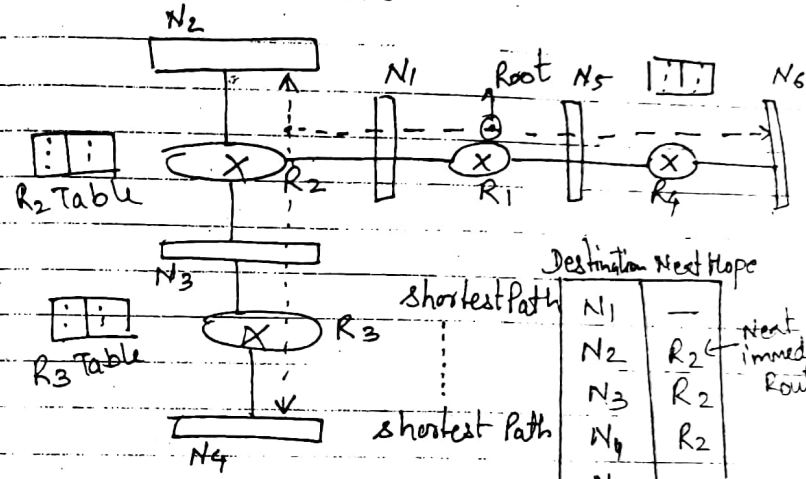


(4) Multiple Unicasting :→



Multicast Routing :-

↳ unicast Routing :-

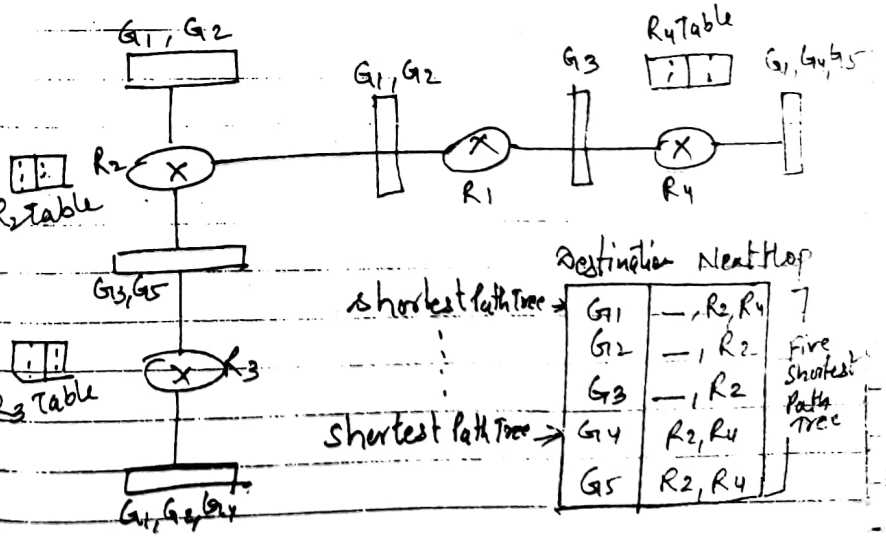


Destination	Next Hope
N1	—
N2	R2 ← Next immediate Router
N3	R2
N4	R2
N5	—
N6	R4

R1 Table

↳ Multicast Routing

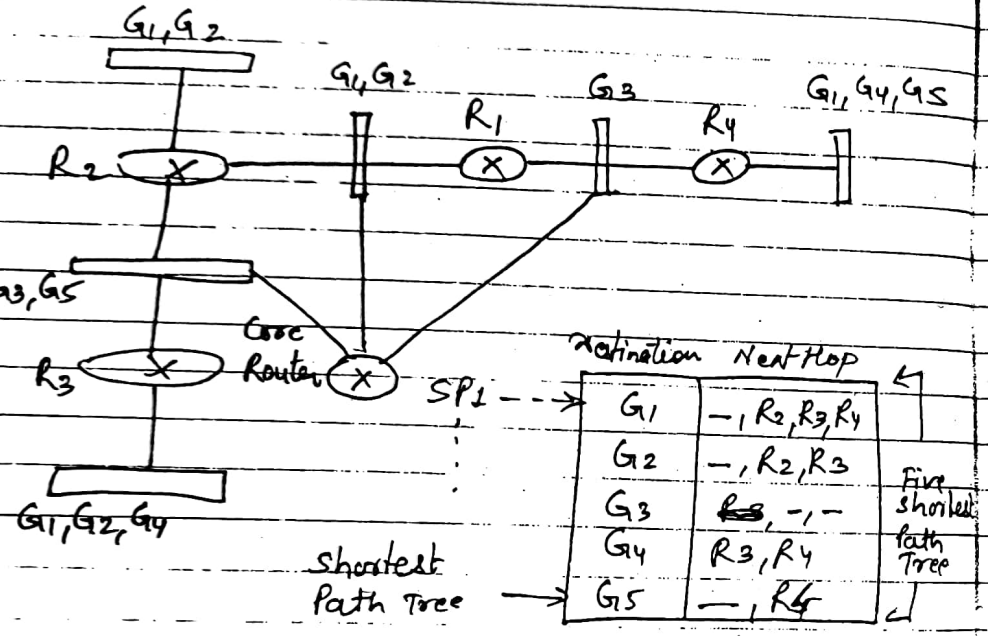
↳(i) Source Based Tree :-



Destination	Next Hop
G1	—, R2, R4
G2	—, R2
G3	—, R2
G4	R2, R4
G5	R2, R4

Five Shortest Path Tree

(ii) Group Shared Tree :-



Core Router Table

unit-2

Elementry Data Protocol :-

for Noiseless Channel

① unrestricted Simplex Protocol :-

(↳ one direction flow of data)

↳ Transmission of data take place in only in one direction.

↳ So it is Simplex or unidirectional protocol.

↳ The Commu^n channel imagine noise free.

↳ So it does not damage or lost any frame

↳ This protocol consists of two destinct protocol namely sender & Receiver.

↳ No sequence or acknowlegement no:s used.

② A Simplex Stop & wait protocol :-

↳ Like the first protocol commu^n channel is assumed to be noise free & commu^n is simplex (i.e only in one direction).

↳ The Transmitter sends one frame & then wait for the damy frame (i.e ack).

↳ One's the ack. is received, it sends the next frame then it is also called stop & wait.

③ A Simplex protocol for Noisy Channel :-

↳ Normal operation

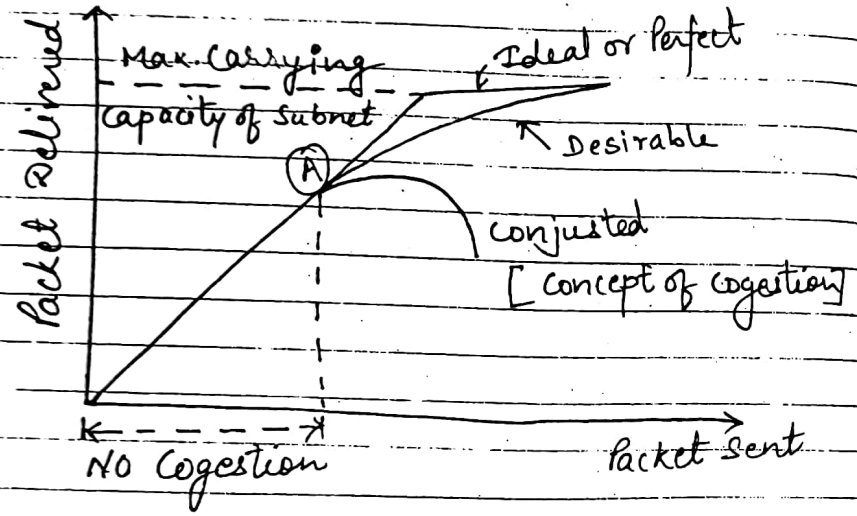
↳ Time out

↳ Lost frame

↳ Piggy (packing) protocol

30/3/11

Congestion Control :→



- An imp. issue in a packet switching is congestion.
- When too many packets are present in a part of subnet the performance degrades. This situation is called congestion.
- Congestion in the n/w may occure when traffic load on the network.

e.g.

The no. of packet sents to the network is greater than the capacity of the network from the figure

↳ The no. of packet delives is proportional to the no. of packet sent. then no congestion takeplace.

↳ But after point 'A' the traffic increasing too large.

→ The Router can not cope (सामना) with the Increase traffic & they begin to the loss of packets.

↳

As the traffic increases the performance degrades.

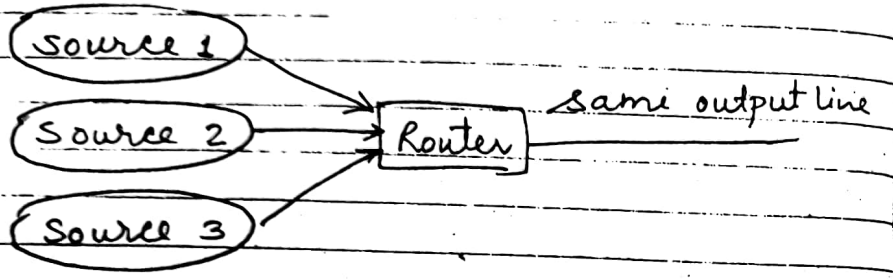
Need of Congestion Control :→

* Congestion Control is neccessary to ensure that the user gets the quality of service.

* Congestion will lead used to a large queue length which results in buffer overflow & loss of packets.

* it is not possible completely avoid the congestion but it is necessary to control it.

Causes of congestion :→



↳ When multiple user access the same output line simultaneously then it will lead to the congestion

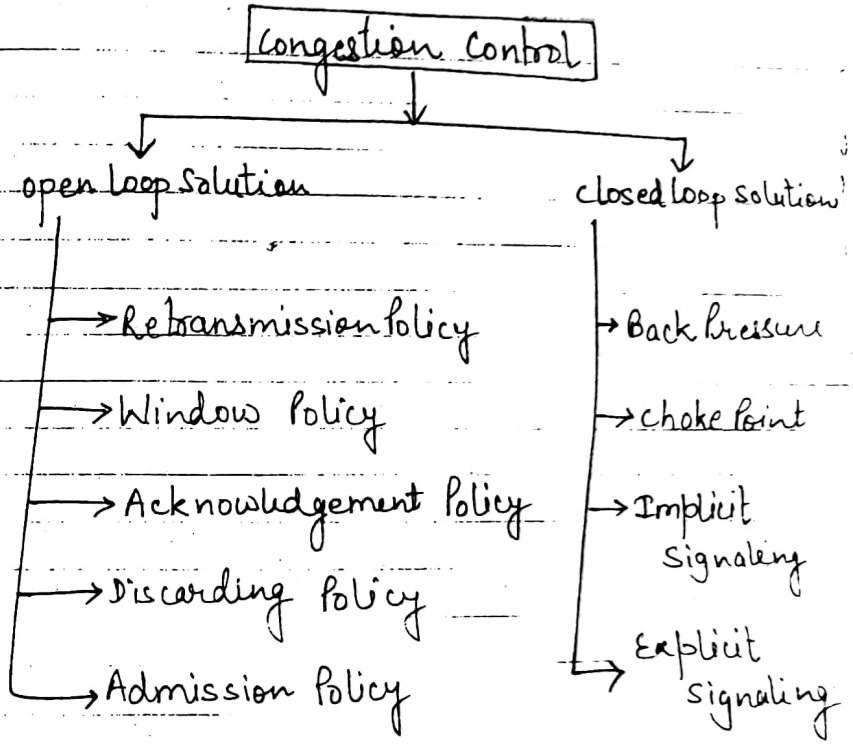
↳ Low Bandwidth lines can also the cause of congestion.

↳ Slow processor.

↳ Congestion is caused by slow link.

Diff^n b/w Flow Control & Congestion Control book.

Classification of congestion control :→



4/4/11

open loop solutions :-

↳ Excellent design to prevent the congestion from happening

↳ it is used for when to accept the new packets & when to discard the packet

closed loop solution :-

↳ Detect the congestion & locate it
↳ Action can be taken
↳ Adjust the system operation to correct the congestion

e.g. TCP - flow control.

⇒ open loop solution for the Data link layer policies :-

Retransmission :-

↳ Based on the sender time out.
↳ if sender time out then it will retransmit.

Out of order caching :-

↳ Receiver discard all the packets which are out of order.

then retransmission of these packets will take place.

↳ This will increase the load & result in congestion.

Acknowledgement Policies:-

↳ if the acknowledgement is delay then the possibility of time out & retransmission of the packets.

↳ if each packet is acknowledged immediately then the acknowledge packet will increase the ~~packet~~ congestion.

Window Policiy:-

↳ Selective Repeat is the better or efficient than go-back

Admission Control:-

↳ One's the congestion has been detected donot setup any more virtual circuits until the congestion is cleared.

open loop Solution for the Network layer policies:-

choice blw virtual circuit & datagram

↳ affect on congestion

↳ Many Congestion algo use virtual ckt subnet.

↳ Service may be used for virtual ckt subnet or datagram subnet

Packet Queuing:-

↳ Priority based order e.g. Round Robin

↳

Packet Discard Policiy:-

↳ Policy tells the router which packet is to be discarded.

Routing Algorithms:-

Packet life time management:-

↳ This policy define the time for which a packet may live before being discarded.

open loop solution for the transport layer policies:-

↳ The fun^ality of transport layer is same as in Data link layer.

Traffic shaping :- (uniform data flow).

↳ The Reason of the congestion is due to the brusting natur of the traffic.

↳ if the traffic has a uniform data rate then congestion could be less common.

↳ iet is the open loop contol.

↳ it will regulate the avg rate of the brusteingness of the data transmission.

↳ Monitoring a data traffic flow is called as traffic policy.

↳ check if a packet stream obey its discripter, & if it violates its discripter give panalty will be

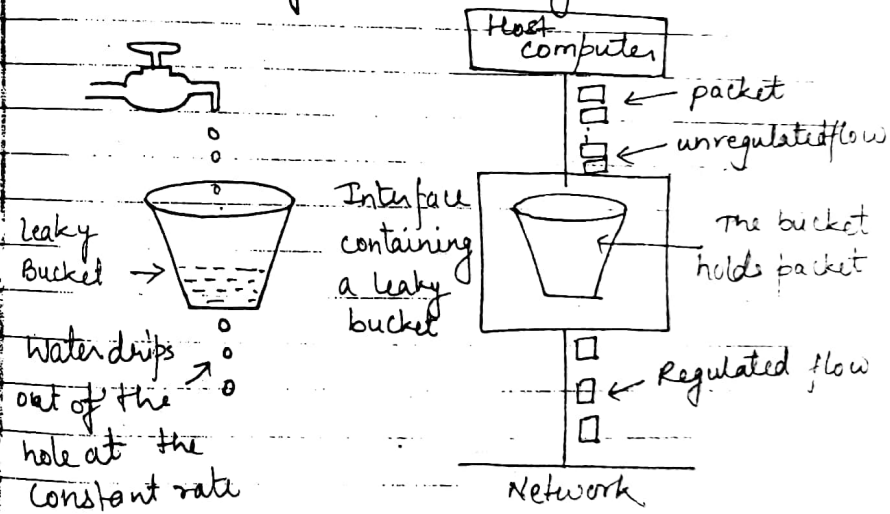
test 5/4/11

* Drop packets that violate the discripter.
* Give the low priority of the ...

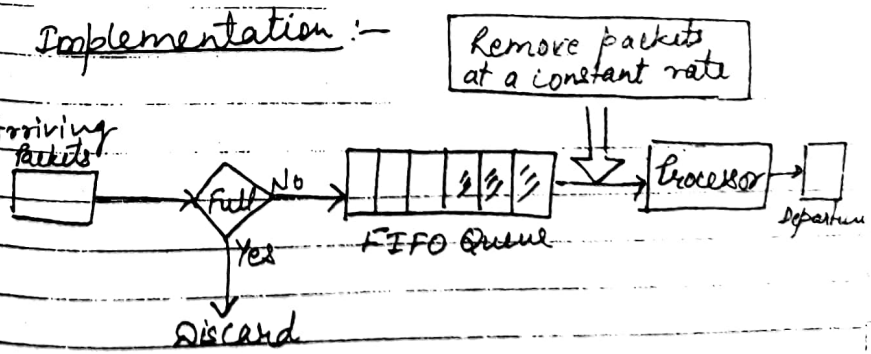
These are two types of algorithm in traffic shaping :-

(i) leaky Bucket Algo. (var o/p rate)
(ii) Token Bucket Algo. (avg rate)

Imp (i) Leaky Bucket Algo :-



Implementation :-



- A leaky bucket algorithm shapes the bursty traffic into a fixed rate traffic.
- it does by averaging the data rate.
- it drops the packet, if the bucket is full.
- A FIFO Queue is used for holding the packets
- The implementation can be discussed under two different operating condition -

condition 1:- for the packet of fixed size

if the arriving packets are of the fixed size, then the purpose of above figure removes a fixed no. of packets from the queue at each tick of the clock.

condition 2:- Packets of variable size :→

if the arriving packets are of different size then the fixed output rate will not be based on the no. of departing packets.

instead it will be based on the no. of departing bytes

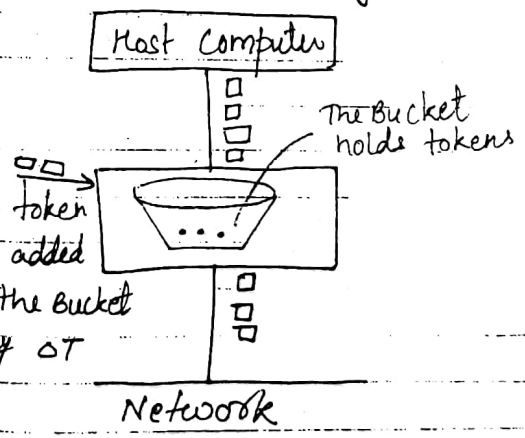
Algorithm:-

step 1:- initialize a counter to n at the tick of the clock.

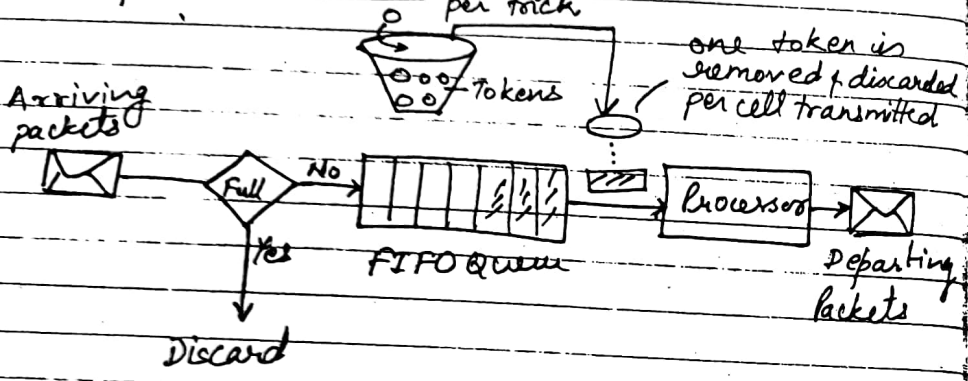
step 2:- if n > the packet size then ~~(the packet of)~~ decrement the counter by the packet size.

step 3:- Repeat step-2 until n becomes smaller than packet size

(ii) **Token Based algo :→**



Implementation :- one token is added per tick



↳ This algorithm is similar to leaky bucket but it allows for varying the output rates.

Steps:-

↳ This is useful when larger burst of traffic arrive.

↳ it enforce a long term average transmission rate.

↳ In this approach, a token bucket is used to manage the queue regulator that controls the rate at which packets flow into the network.

Steps:-

↳ The token buckets can be easily implemented with a counter. The token is initilize to zero.

↳ each time, a token is added, the counter is incremented by 1 & each time a unit of data is dispatched, the counter is decremented by numeric one.

↳ If the counter contains zero, the host can not send any data.

Note :- The token bucket allows the bursty traffic at the max. possible rate.

Congestion Control in the Datagram subnet :->

There are 3 techniques which are —

(i) choke packets. ← var-u for utilizing channel $0 \le u \le 1$
(ii) Load shedding. ($u > t$) ↳ mild warning ↳ stern warning ↳ ultimately warn
(iii) jitter control.

(i) Choke Packets :->

- In this technique, each router associates a real variable with each of its output line.
- This real variable say 'u' has a value b/w 0 & 1 and it indicates percent utilization of that line.

if the value of 'μ' goes above the threshold then the output line is in the warning state.

- The Router will check each new arriving packet to see if its output line is in the warning state.
- If it is in the warning state then the router send back a choke packet signal to the sending host.
- The ~~center~~ sender host will not generate any more packets.
- Depending on the threshold value the choke packets can contain a —
  - → mile warning
  - → stern warning
  - → ultimatum warning

Disadvantage:-

The problem with the choke packet technique is that the action to be taken by the source host.

On receiving a choke packet is voluntary & not compulsory

(ii.) Load shedding :→

congestion control technique :→ (in datagram subnet)

(ii) Load shedding :-

→ The principle of load shedding states that when the routers are being inundated by the packets that they can not handle then they should simply throughout the packets away.

→ A router which is flooding (overflow) with the packets due to congestion can drop any packets at random but there are better ways of doing this.

→ The policy for droping a packet depends on the type of packet e.g.

for file transfer, an old packet is more imp. then new packet but on the other hand, for multimedia a new packet is more imp. then an old one.

So the policy for file transfer called wine (old is better then new). & for the multimedia is called milk (new is better then old).

→ An intelligent discard policy can be decided on the depending of application.

(iii) Jitter control :→

↳ variation in delay.

Jitter :-

Jitter is defined as the variation in delay for the packets belonging to the same flow.

→ For the audio & video transmission if the packet takes 20 ms to 30ms (delay) to reach the destination, it does not matter the delay remain constant.

→ The Quality of the sound & video will be hampered, if the delays associated with different packets have different values.

Jitter Control :→

When a packet arrive at a router, the router will check its sec

or a head (advanced) & by a what time.

This info. is stored in the packet & updated at every hop (host).

→ if the packet ahead of the schedule (early) then the router will hold it, for a slightly longer time.

→ if the packet is behind of the schedule (late) then the router will try to send it out as quickly as possible.

This will help in keeping the avg. delay per packet constant & will avoid time jitter.

(iv) Quality of Service :→

Some characteristics of quality of service is given -

(i) Reliability :-

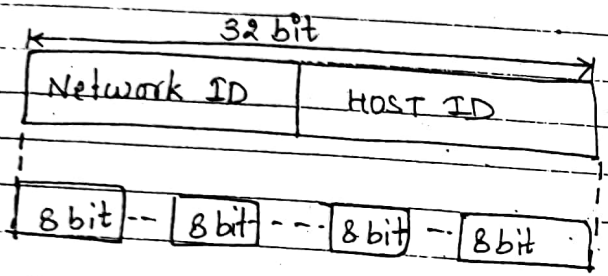
→ it is a characteristic that a flow needs

→ lack of reliability means losing the packet which entails retransmission.

e.g. it is more important that

14 | 11

IP-address format :-



10010001.00001010.00100010.00000011

$2^7 00 2^4 000 2^0 . 000 0 2^3 0 2^1 0 . 00 2^5 000 2^1 0 . 000000 2^1 2^0$

128+0+0+16+0+0+0+1 . 0+0. +8+0+2 . 0+32+0+2+0 . 0+ -+2+1

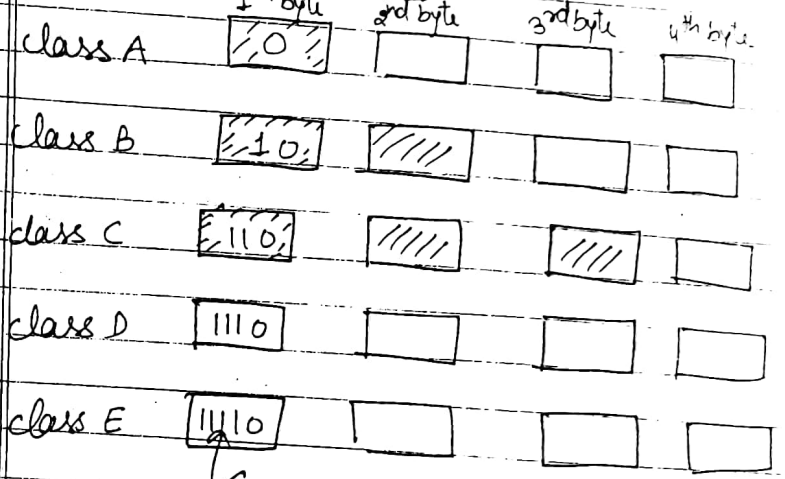
↓ ↓ ↓ ↓

145 . 10 . 34 . 3

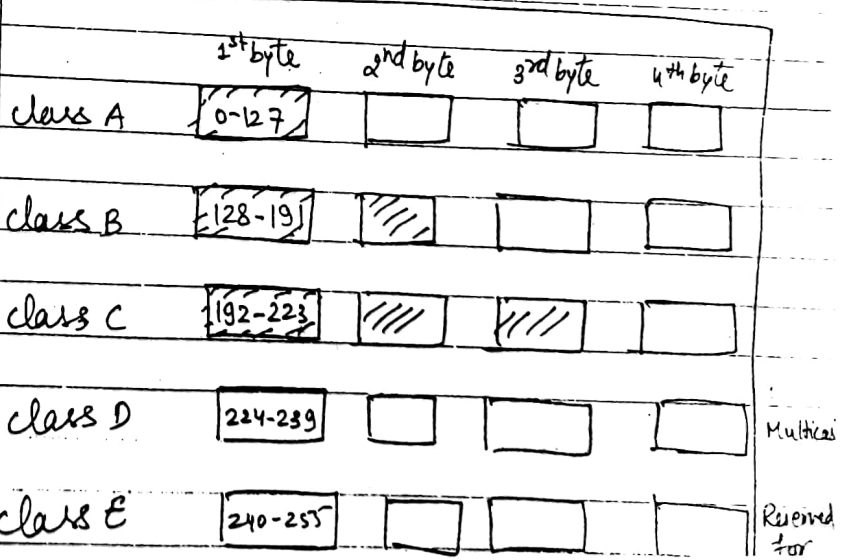
IP Address ⇒ 145.10.34.3 (in decimal)

IP address classes :-

(a) Binary Notation :-



(b) Dotted Decimal Notation :-



No. of blocks & block size useful in IP4 Addressing :-

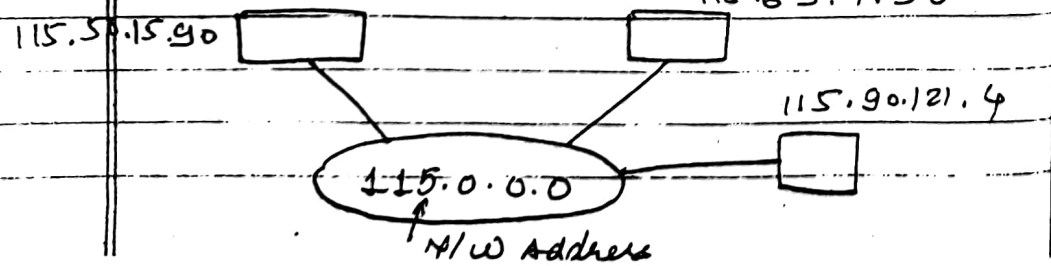
class	No. of blocks	Block size	App^n
A	128 (2^7)	16,777,216 (2^{24})	unicast
B	16,384 (2^{14})	65,536 (2^{16})	unicast
C	2,097,152 (2^{21})	256 (2^8)	unicast
D	1	268,435,456 (2^{28})	Multicast
E	1	268,435,456 (2^{28})	Reserved

for Network bits — host bits

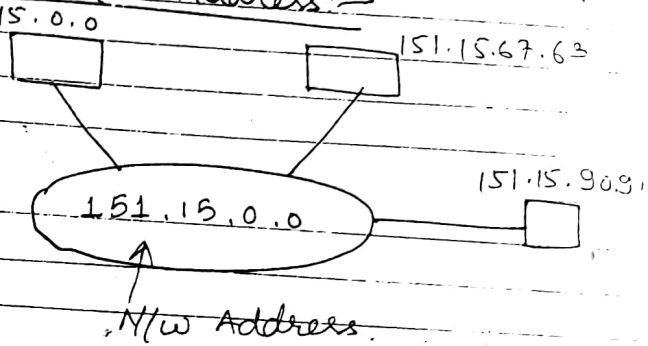
Network Address :-

The network address is an address that defines network itself. it can not be assigned to a host.

class A N/W Address :-



class B N/W Address :-



14/9/11

Address Mask (default mask)

* An address mask determines w/c portion of an IP address identifies the n/w & w/c portion identified the host. like an IP address, the mask is represented by 4 octate. equivalent to a decimal no. in the range 0-255

* If a given bit of the mask is numeric (1) the corresponding bit of the IP address is in the n/w address.

0000 or 0 — Host Address
255 or 1 — N/W Address
244 ⇒ Mix

* if a given bit of the mask is zero, the corresponding bit of the IP address is in the host portion.

Add. class		Add. mask (N/w | Host)
A	⇒	255.0.0.0
B	⇒	255.255.0.0
C	⇒	255.255.255.0

Element	Network	Host
Mask	255.255.255	0
	11111111.11111111.11111111	00000000
IP address	192.15.28	16
	11000000.00001111.00011100	00010000

M.2nd

Subnetting :→

* (Small part of the n/w called the subnetting)

Like = Hierarchical or tree topology in this the parent node that take the responsibility of the child node. But outside org. that takes it as only one n/w but it internally break.

* Smaller part of n/w is called subnet.
* All the host in a n/w must have the same network no. but this property of the IP addressing can be problematic as the n/w size increases.
* with increases in the no. of distinct local n/w these management become a problem.
* Every time a new gets installed, the system administrator has to contact N/C to get a new n/w & then this no. is to be announced to the world.
* The sol^n to this problem is that, the n/w is split into several smaller networks internally but it acts like a single n/w to the outside world

⇒

e.g. Suppose Total no. of host = 30

255 = 128 64 32 16 8 4 2 1

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

Address ⇒ 192.168.1.000 00000
3 extra bit

h = 3 (extra bit)
no. of subnet $2^h = 2^3 = 8$
(000 - 111) ⇒ subnet.

e.g ⇒ 128 64 32 | 16 8 4 2 1
N/w | Host

Class C :→ 192.168.1.000 00000 ← N/w
192.168.1.111 11111 ← Broadcast
255.255.255.224 — Subnet mask identify the n/w & host part

Processing ⇒
192.168.1.000 00001 ⇒ 1st host
192.168.1.000 00010 ⇒ IInd "
192.168.1.000 11111 ⇒ last "
192.168.1.001 00000 ⇒ broadcast

Q: A block of addresses is granted to a small org., we know that one of the address is 205.16.37.39/28
A 1 - 127
B 128 - 191 N/w address bit
C 192 - 223 must be 28.
What is the first address in the block?

101111
$= 32 + 8 + 4 + 2 + 1$

Ans- 205 - 16 - 37 - 39
11001101.00010000.00100101.00100111

39 → binary no. ⇒ 4 after that the 4 bit of the 39 make as 0000 because we firstly take the host bit 0000 & last bit 1111.

32 — 0010 0000 first address
47 — 0010 1111 last address

205.16.37.32 first address
205.16.37.47 last address

N/w address bits in class-C is 24 bits it takes the 4 bit from the host address.

Q. Perform the Subnetting of the following IP address ⇒ 160.11.x.x
original subnet mask 255.255.0.0
no. of subnet = 6.

Sol ⇒ Here are class B IP address.

11111111	11111111	111	00000	00000000
255	255	3 bits		13 bits

255.255.31.0

Subnet 1 — 255.255.63.0
Subnet 2 — 255.255.95.0
Subnet 3 — 255.255.127.0
Subnet 4 — 255.255.139.0
Subnet 5 — 255.255.191.0
Subnet 6 — 255.255.223.0

⇒ Add = 32.

255.255.255.0

TM.Imp

Q. A class B network on internet has a subnet mask 255.255.240.0 what will the max. no. of host per subnet.

Ans:→

255.255.240.0

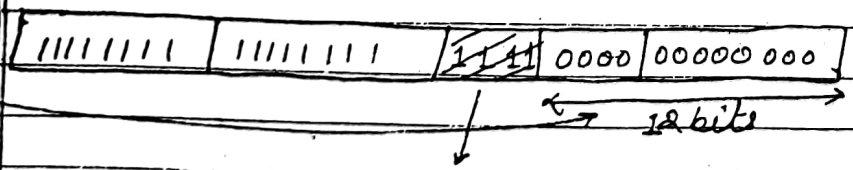
$2^7 2^6 2^5 2^4$

$n = 4$

Total no. of subnet $= 2^4 = 16$

⇒ 12 bits

we have subnet mask = 255.255.240.0



each subnet can have $= 2^n - 2$ Host

$= 2^{12} - 2$

$= 4094$

$n = 12$ (Host bits)

because 1 bit for N/w address
1 bit for Broadcast Address.

Class-less Addressing

* The no. of device on the internet is much less than the 2^{32} address space.
* We have runout of class A, class B addresses & class C block is too small.
* For the most mid size organisation, one solution to this problem is the idea of class less addressing.
* In this scheme, there are no classes.

e.g. ⇒ ↳ A household may be given only two addresses.

↳ A large organisation may be given thousand of addresses

Restriction :⇒

* To simplified handling of addresses, the internet authorities impose three restrictions.

1. The addresses in the block must be contiguous. one after another.
2. The no. of addresses in a block must be a power of 2 (1, 2, 4, 8, 16, ...) ($16 = 2^4$)
3. The first address must be evenly divisible by the no. of addresses.

3,440,387,360 / 16 = 215,024,210

205. 16. 37. 32
205. 16. 37. 33
⋮ ⋮ ⋮ ⋮
205. 16. 37. 47

X

	Block	Block
1 →	205. 16. 37. 32	11001101 00010000 00100101 00100000
	205. 16. 37. 33	11001101 00010000 00100101 00100001
	⋮ ⋮ ⋮ ⋮	⋮ ⋮ ⋮ ⋮
Last →	205. 16. 37. 47	11001101 00010000 00100101 00101111

16 addresses

Process ⇒ address ⇒ port number
device " " ⇒ IP address

13/4/11

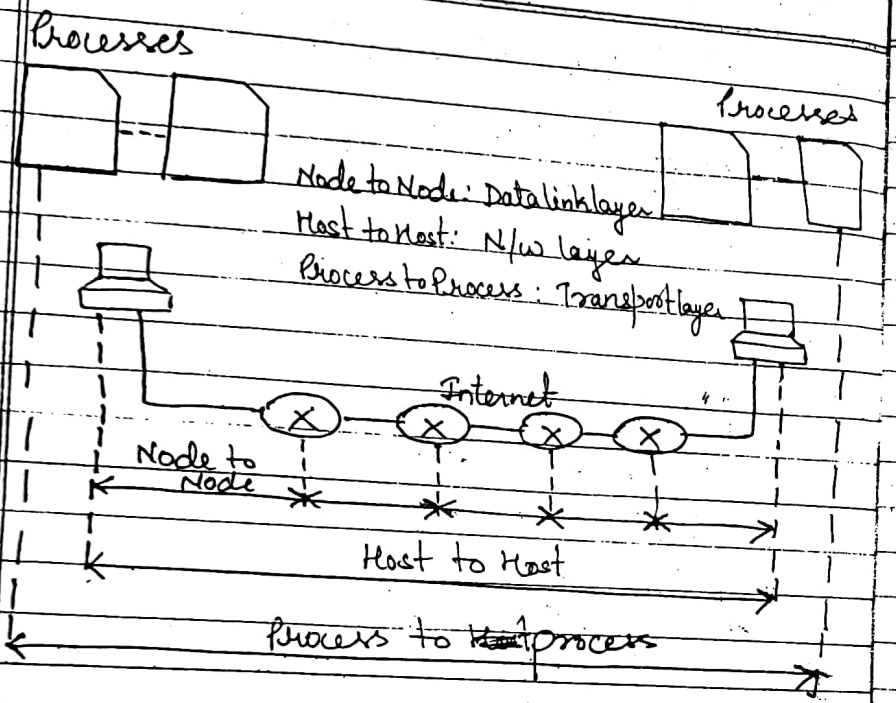
UNIT-4

Transport, session & Presentation layer

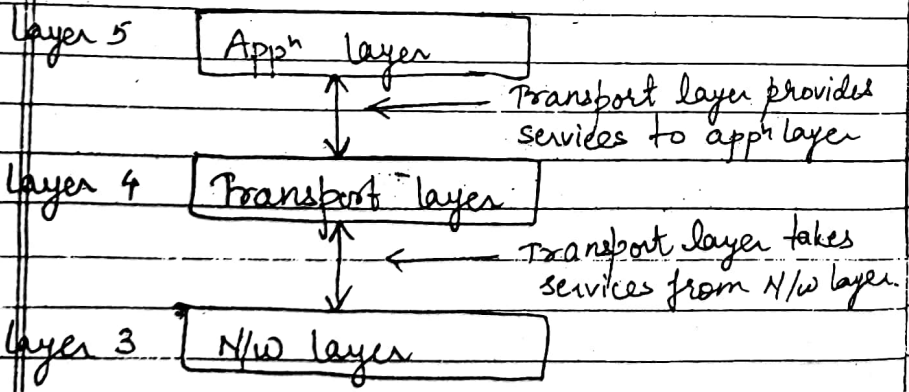
// Responsibilities :⇒ of transport
↳ ~~source to destination delivery of data~~
↳ Packetization.
↳ Process to process delivery of data

Transport layer :⇒

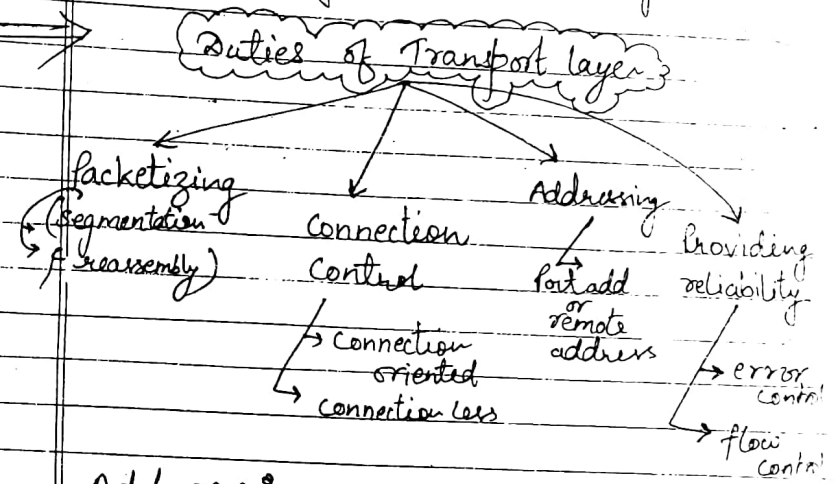
* The transport layer is responsible for process to process delivery of data or delivery of the entire message.
* A process is an app^n program running on a host.
* segmentation & reassembly
* whereas the n/w layer oversees source to destination delivery of individual packet.
* On the other hand the transport layer ensures that the whole message arrives intact (unbroken) & in order overseeing both error control & flow control at the source to destination level.



Position of transport layer:→



Transport layer provide service to the appⁿ layer & takes the services from N/w layer.



Addressing:→

The client needs the address of the remote computer it wants to communicate with such a remote computer have a unique address so that it can be distinguish from all the computers.

The transport hacker must therefore include a type of address called a service point address or the port address.

Transport layer Services:→

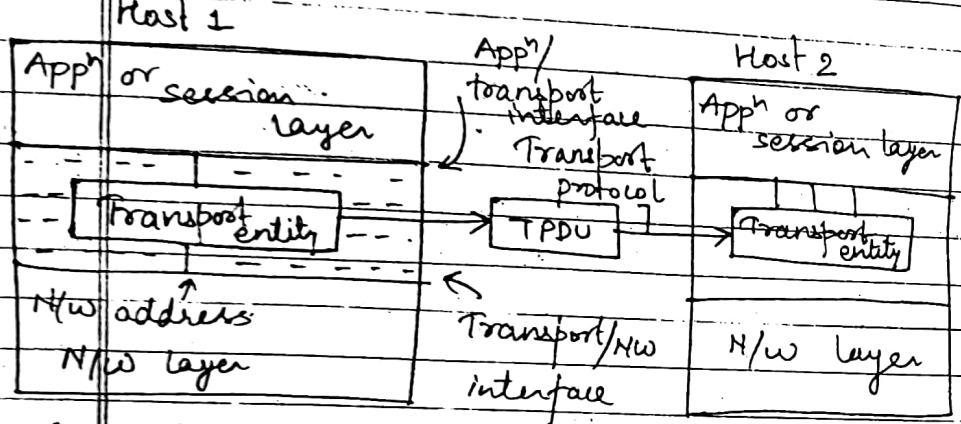


fig:- Relⁿship b/w N/w, transport & applⁿ layer.

TPDU:-

↳ Transport protocol data unit

↳ The message sent from transport entity to transport entity is called TPDU.

⇒ The task of the transport layer is to provide reliable cost effective transport of the data from source machine to the destination m/c.

⇒ To achieve this goal, the transport layer makes use of the services provided by the n/w layer.

Transport Entity:→

⇒ The hardware & the software with in the transport layer which does the work of making use of the services provided by the n/w layer is called the transport entity.

⇒ Transport layer services are of 2 types
↳ connection oriented
↳ connection less

⇒ Layer 1st to 4, form the 1st group called transport service provider.

⇒ Layers above 4 are in the 2nd group called transport service users.

14/4/11

Congestion Control & Quality of Service:→

Typical Quality of Service parameters are given below:-

1) Connection Establishment Delay. ← Request & confirmation
2) Connection establishment failure probability ← due to congestion,
3) Throughput.
4) Transit Delay.
5) Protection
6) Residual Error Ratio:→

7). Priority
8). Resilience

Transport layer Primitives :→

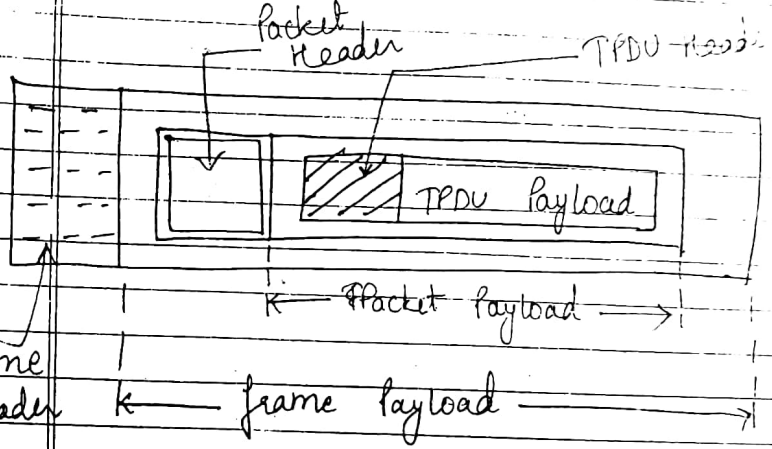
S.No.	Primitive	TPDU sent	Meaning
1.	Listen	None	Block until some process tries to connect.
2.	Connect	Connection Request	Activity attempt to establish a connection.
3.	Send	Data	send data.
4.	Receive	None	Block until a data TPDU arrives.
5.	Disconnect	Disconnect Request	Release the connection

↳ The transport layer primitives allows the transport user such as appⁿ program to access the transport service.

↳ each transport service has its own primitives.

↳

Nesting of TPDU's packets & frames :-



Socket :→

it is the combination of port address & IP address.

Note → Diffⁿ b/w port address & IP address :→

(i) The IP address & port number play different roles in selecting the final destination of the data.

(ii) The destination IP address defines the host among the millions of

host in the world.

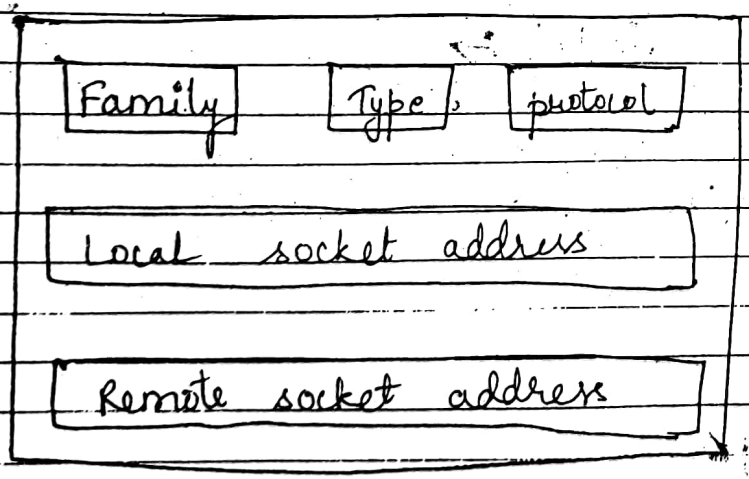
(iii) After a particular host is selected, the port no. defines one of the process on this selected host.

Socket

⇒ Two processes can communicate if & only if these have a socket at ~~end~~ each end point.

⇒ A socket x has an end point.

structure of socket :→



15/4/11

family → define the group of protocol such as IPv4, IPv6, unix domain protocol.

Type → define the type of socket such as stream socket, packet socket or raw socket.

✗ Local socket address → combination of port add & IP address

✗ Remote socket add → combination of Remote IP address & port address

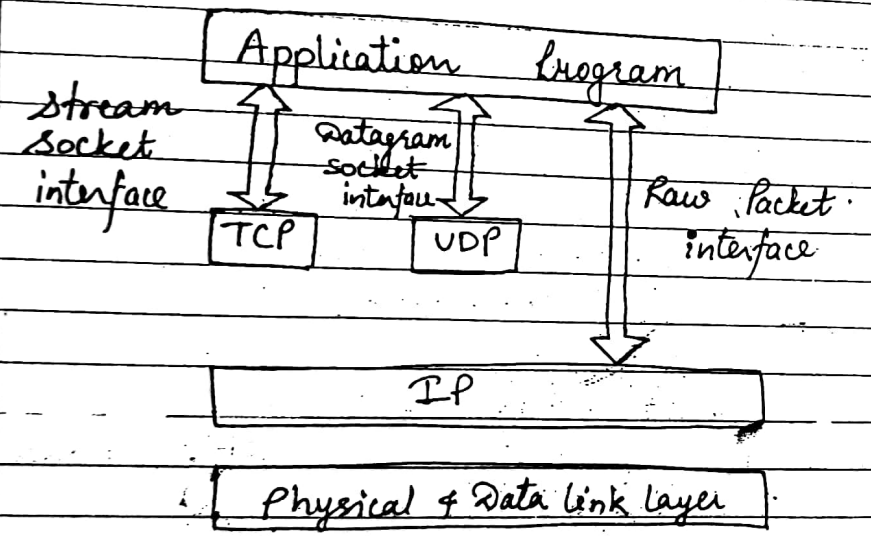
Protocol :- This field is usualy for TCP & UDP.

Local socket address :-
it is used for defining the local socket address.
↳ it is the combination of local IP address & port address.

Remote socket address :→
it is used for defining the remote socket address
↳ it is a combination of remote IP address + port address.

Types of socket :→

↳ Stream socket (for connection oriented TCP)
↳ packet or datagram socket (connectionless)
↳ Raw socket (for IP)



Imp **Berkeley Sockets :→**

Socket functional calls :-

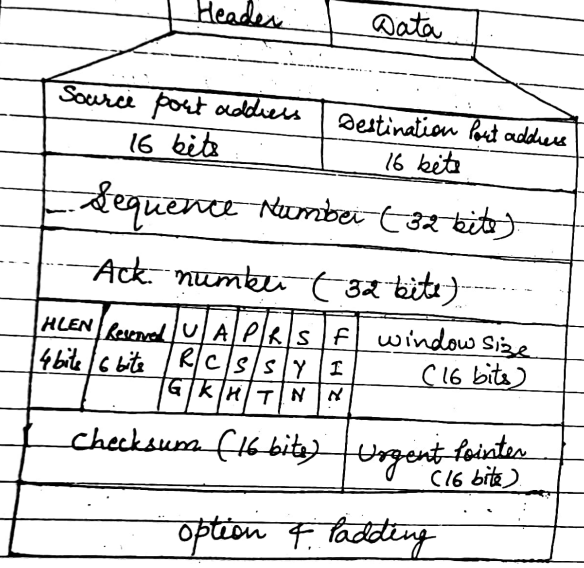
Socket() :- create a socket
bind() :- bind a socket to a local IP address & port #
Listen() :- passively waiting for connections.

Connect() :- initiating connection to another socket.
accept() :- accept a new connection.
Write() :- write data to a socket.
Read() :- Read data from a socket.
Send to() :- Send a datagram to another UDP socket.
recvfrom() :- Read a datagram from a UDP socket.
close() :- close a socket tear down the connection.

V.Imp **TCP Segment Header :→**

Flag	Description
URG:	Urgent pointer is valid
ACK:	acknowledgement field
PSH:	Push the data.
RST:	Reset the connection
SYN:	Synchronize sequence No. during connection
FIN:	Terminate the connection.

Format:-

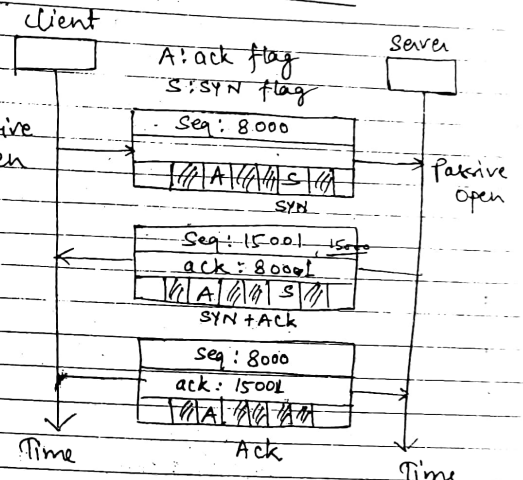


19/4/11

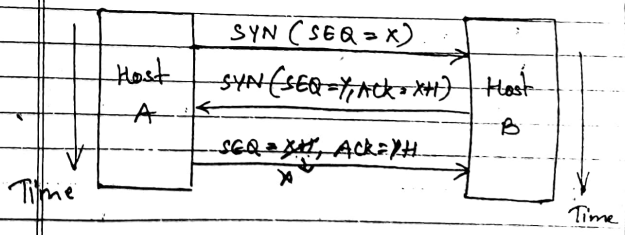
(3-way Handshaking)

TCP Connection / TCP connection Mgt →

* connection establishment:→



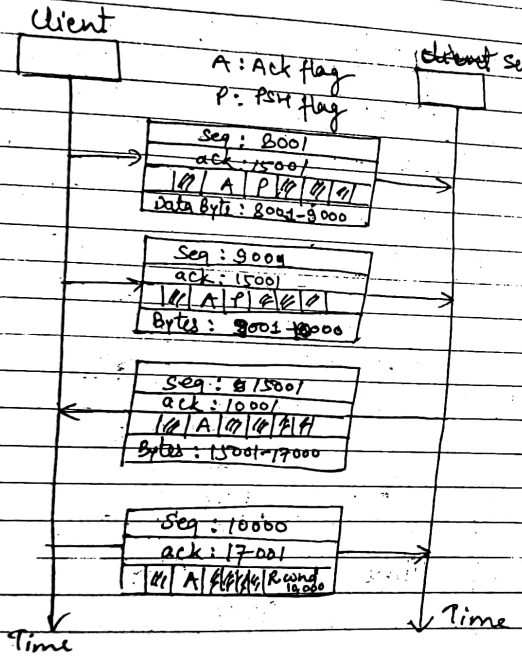
→ fig (i)



R.wnd : Receiving window.

(ii) → Data Transfer :—

fig (ii)



From fig (i) :—

So in the TCP, connection oriented transmission requires 3-phases —

connection establishment

Data Transfer

(iii) Connection Termination

(i) connection establisment :—

TCP transmit data in full duplex mode. When 2 TCP into m/c are connected. They are able to send segments to each other simultaneously.

3-way Handshaking :→

The connection establishment in the TCP is called 3-way Handshaking.

Note :— 3-steps are involve in 3-way handshaking.

(i) a SYN segment can't carry data. but it consume one sequence no. e.g. sequence no = 8000 in figure.

(ii) a SYN + ACK, can't carry data but does consume one sequence no.

(iii) The ACK segment does not consume any sequence no.

is established, bidirectional data transfer can take place. The client & server can both send data & ack. from the time, the client sends 2000 bytes of data in one segment to the server, then sends 2000 bytes in one segment. The data segment sends by the client have PSH flag set.

(ii) Data Transfer :-

fig (ii).

R.wnd : Receiver Window, 10,000, it is the number of Bytes, the other end can accept before its buffer overflows & data are discarded.

C.wnd :- Congestion window,
↳ it is a value determined by the network to avoid the congestion.

Q.1. what is the size of the window for Host A if the value of receiver window is 3000 bytes & the value of congestion window is 3,500 bytes.

size of window for Host A = 3000 bytes

Q.2. What is the value of receiver window for Host A, if the receiver Host B has a Buffer size of 5000 bytes, & 1000 bytes of received & unprocessed data.

value of receiving window = 5000 - 1000
= 4000 bytes.

(iii) Connection Termination :-

24/4/11

Pushing the data :-

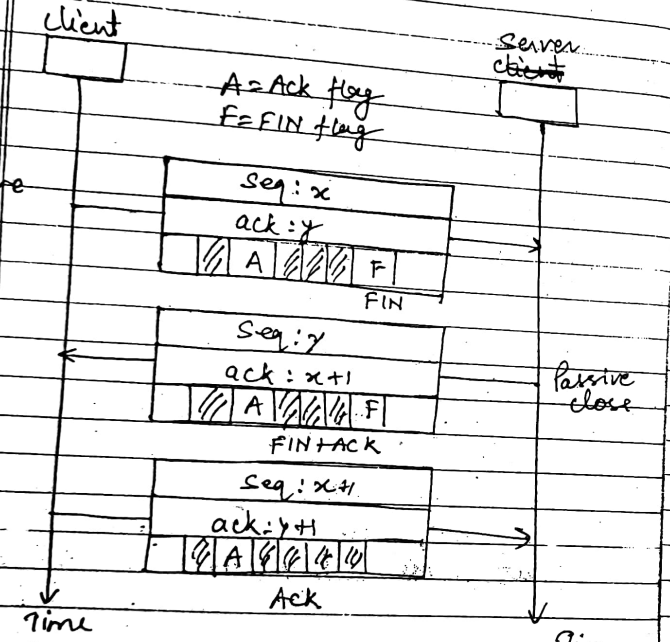
TCP uses a buffer to store the stream of data come from the sending app^n program. If the app^n program one one side wants to send a key-stroke to the app^n program at the other side & receives an immediate response.

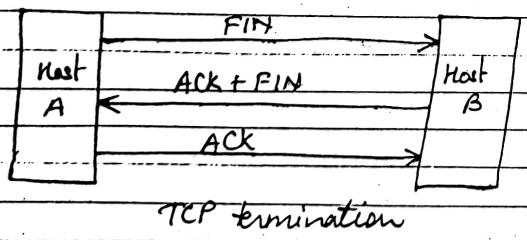
Urgent data :-

The sending TCP creates a segment & inserts the urgent data. The urgent data at the begning of the segment. The rest of the segment can contain normal data from the buffer.

When the receiving receives the segment with the URG bit set, it Extracts the urgent data from segment using the value of the urgent pointer. & delivers them out of order to the receiving app^n program

(iii) Connection Termination :→





TCP termination

Connection Management acc. to client's point of view :→

1) Issue a Connect Request
2) Send a SYN segment
3) Receive SYN + ACK from the server
4) Goes into the established state (By 3 way Handshake).
5) Now send & Receive of data.
6) When sending data is finished an application execute a close primitive.
7) Send FIN segment & then wait for ack.
8) When Receive ack from server.
9) Then transition is made state FIN.
10) Wait to close the connection in one direction.
11) At last, both sides are closed.

Connection Management from Server's point of view :→

1) first LISTEN & waits.
2) When a SYN comes, it is acknowledged by server.
3) Server enters into SYN RCVD state.
4) Goes to the established state.

5) Data flow can be transferred.
6) When the client does a closed, a FIN is sent to the client.
7) Receive the acknowledgement from the client.
8) Server Release the connection & deletes the connection records.

TCP Congestion Control :→

We have already discussed the reason of congestion in the network.

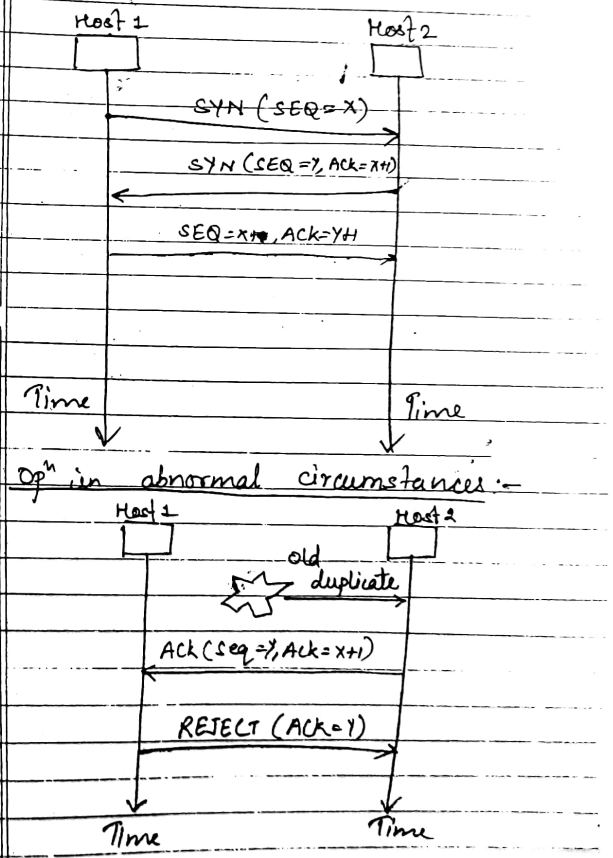
→ The n/w layer also tries to prevent the congestion but TCP takes max. responsibility in the congestion control.

Principle of congestion control :→

Ref→

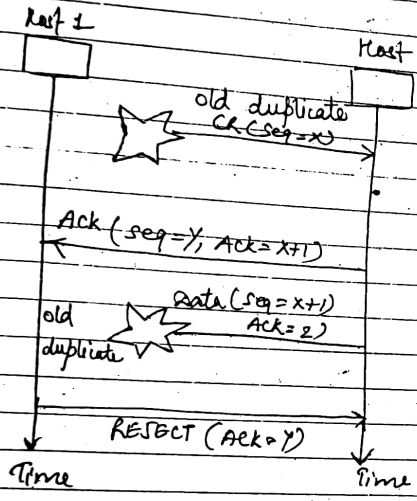
3-way Handshaking :→

(a) Normal op^n →



(b) Op^n in abnormal circumstances :-

(c) Duplicate connection Request & duplicate ack :→

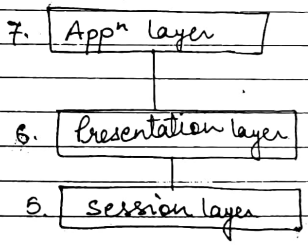


Presentation layer :→ (10 Marks)

Some of the responsibilities of presentation layer are —

(i) translation
(ii) Encryption
(iii) Compression

position of presentation layer :→



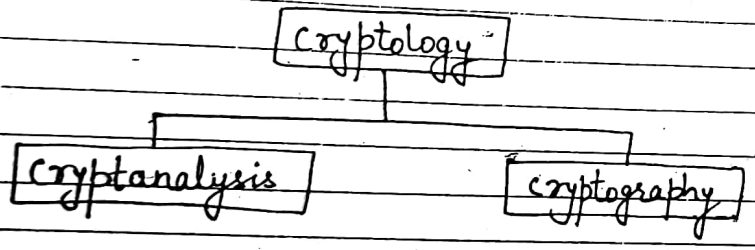
(i) Translation :→

→ The commu system usually exchange the info. in the form of characters, numbers

→ This is essential because different systems use the different encoding technique.

→ The presentation layer at the sending end converts the info into a common format & the presentation layer at the receiving end will convert this common format into one which is compatible to the receiver.

Cryptography :→

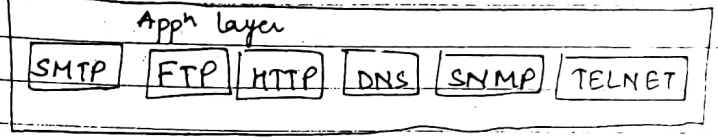


~~Cryptography :→~~ Cryptology :→ it is the study of secure communication which encompasses both cryptoanalysis & cryptography.

26/4/11

UNIT-5

Application layer :→



(i) The appn layer is responsible for providing services to the users.

(ii) it provide the user interface & support for services such as Email, Remote file access & transfer.

Basic services are :—

(i) Network virtual terminal :— it allow a user to log on to the Remote host.

(ii) File transfer, ~~to it~~ access & Management This services provide a user to access file in a remote host.

(iii) Mail services :— This appn provides the basis for email forwarding & storage.

(iv) Directory services →

This application provides distributed database source & access for global info. about various objects & services.

Applications of the appⁿ layer :→

(i) Email
(ii) www
(iii) Multimedia
(iv) Remote file transfer & Access.

SMTP:-

FTP:- File transfer Protocol (authentication)

TFTP:→ (without authentication)

Difference b/w FTP & TFTP

S.No	Parameter	FTP	TFTP
1.	Deffinition	File transfer protocol	Trival file transfer protocol.
2.	operation	transferring files	Transferring files
3.	Authentication	Yes	No
4.	Control & data	separated	not-separated
5.	Protocol	TCP	UDP.
6.	Data Transfer	Reliable	unreliable.

Post office Protocol (POP) :→

Receiver side पर Perform होता है जिसमें file को read, login or download करने के लिए.

POP-3

→ it stands for post office protocol version-3

↳ POP-3 s/w is installed on the receiving computer whereas POP-3 server is installed on the Mail server.

↳ When the user wants to download E-mail from mailbox on the Email server, this is called downloading.

Modes of POP-3 :→

(i) Delete mode :→
delete from Mailbox.

(ii) Keep mode :-
This mail remains in the mail box server.

POP-3 Server :-
it is the simplest implementation of POP-3

↳ When recheck above email, client connects to the POP-3 server by using port number- 110.

↳ POP3 server requires an account name & password.

Commands for POP :→

1) USER :- enter your user ID.
2)
3) PASS :- enter your password.
4) QUIT :- quit the POP3 server.
5) LIST :- list the message & their size
6) RETR :- Retrieve a message & pass it a message number.
7) DELE :- Delete a message & pass it a message number.
8) TOP :- Show the top x lines of a message & pass it a message number & no. of lines.

Telnet :→ (Remote login Protocol)

↳ Telnet is a remote login protocol
↳ Telnet is an appn used on the internet to connect to a remote computer enabling access to that computer & its resources.

↳ it uses TCP/IP protocols & communication takes place through ~~stat~~ satelite, PSTN.

↳ Telnet is old terminal emulation program to login to the remote system.

Email:→

It is the most popular services, SMTP is the standard ~~mechnas~~ mechnism for the email in the internet.

HTTP:→

is used, fetching the webpages from the www.

↳ it is the combination of FTP & SMTP & uses the service of TCP.

IMAP:→ (Internet mail access protocol)

↳ like POP3.

↳ it is similar to POP3 but with some extra features:—

(i) it is possible for users to create, rename or delete mailboxes on the mail server.

(ii) it is possible for the user to search for the contain of email before download.

(iii) it is possible to partialy downloading

URL:→

↳ (uniform Resource Locator)

↳ it is divided into four parts:—

Method : // HOST : PORT / PATH

http : www.w3.org / hypertext/www/project.html

Path

Diff^n b/w web & internet:—

web:— web is the collection of standard protocols & instruction to gain access to the information on the internet.

internet:—

network of the networks is called the internet.

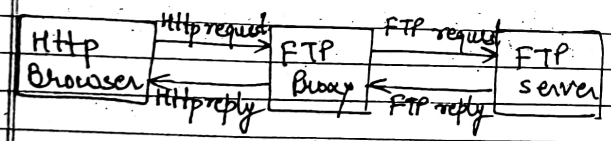
WWW:—

it is an architectural frame work for accessing documents which are spread out over the machines over internet.

↳ Thousands of people today gain access to the internet.

↳ Http is a FTP which is specifically designed to facilitate to the WWW.

Proxy Server:→



↳ Proxy server is basically a gateway which speaks HTTP to the browser but FTP or some other protocols to the servers.

↳ Proxy server can be a program running on the same working machine as a browser.

↳ A proxy server can be put inside firewall.

↳ All the servers can not speak HTTP, some of them use the FTP or other protocols.

↳ A large information is available on FTP so it should be made available to the web users. To do so one solution can be to have a browser which can be use HTTP as well as FTP & other protocols.

↳ And other solution to this problem is proxy server.

MIME:→

↳ multipurpose internet mail Extension.

↳ Some problems are encounter in sending & receiving the following type of messages.→

(i) Messages in the language such as - French or Germans.

(ii) Messages which don't contain text, e.g. audio & video.

(iii) Messages in the language which don't have alphabets e.g. chinese & japaniese.

(iv) Messages in non-lattin alphabets such as Russian.

The solution to these problem was MIME.

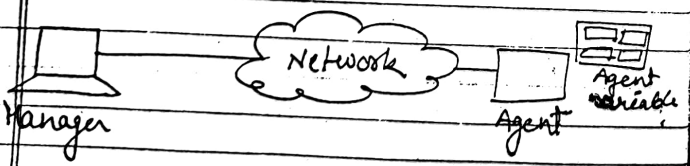
→ SNMP :→

Simple N/w Management Protocol

↳ SNMP provides a systematic way for monitoring & Managing a computer Network.

↳ This protocol were widely implement in the commercial product.

↳ it use the concept of Managers & Agents.



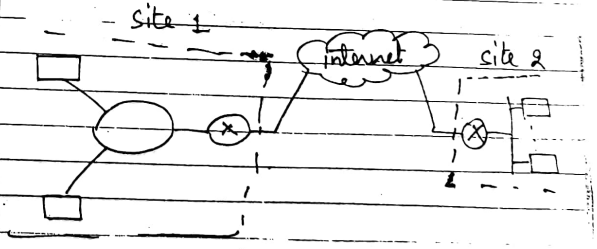
↳ A management section or manager is a station or host that runs on the SNMP client.

↳ A managed section or Agent is a router that run as SNMP server program.

↳ Management section called Manager.
↳ Managed section called Agent.

↳ Management is acheived through a simple internet connection between interaction b/w Manager & agent.

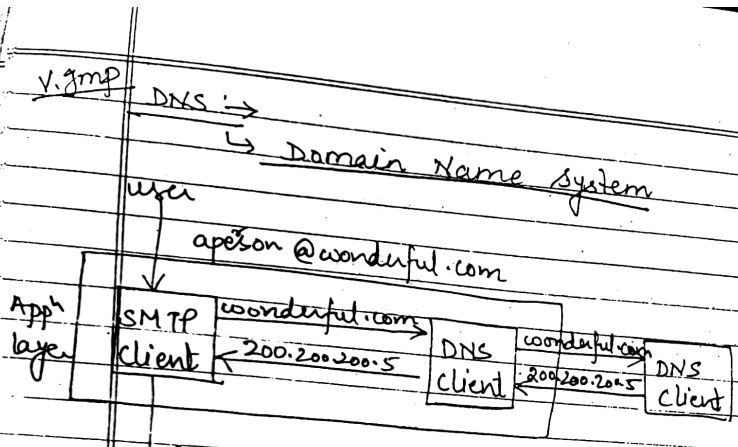
VPN :—



XML :—

V. Imp DNS :→

↳ Domain Name System



* To map a name onto an IP address.
* An appn program.

27/4/11 Mod Imp Cryptography

UNIT-4

RSA Algorithm :→

① ∵ $a = qn + r$ i.e. $7)\overset{1}{11}\overset{7}{4}$ then $a=11$, $q=1$, $n=7$, $r=4$

② → $11 \bmod 7 = 4$

∴ i.e. $a \pmod n$

e.g.

③ → $-11 \bmod 7 = ?$

$a = qn + r$

$-11 = -2 \times 7 + 3 = -11$

∴ $-11 \bmod 7 = 3$

④ → congruent modulo

$73 \equiv 4 \bmod 23$

↓

$73 \bmod 23 = 4 \bmod 23$

GCD (1970, 1066) = ?

$1970 = 1 \times 1066 + 904$	gcd (1066, 904)
$1066 = 1 \times 904 + 162$	gcd (904, 162)
$904 = 5 \times 162 + 94$	gcd (162, 94)
$162 = 1 \times 94 + 68$	gcd (94, 68)
$94 = 1 \times 68 + 26$	gcd (68, 26)
$68 = 2 \times 26 + 16$	gcd (26, 16)
$26 = 1 \times 16 + 10$	gcd (16, 10)
$16 = 1 \times 10 + 6$	gcd (10, 6)

$10 = 1 \times 6 + 4$ gcd(10, 6)

$6 = 1 \times 4 + 2$ gcd(6, 4)

$4 = 2 \times 2 + 0$ gcd(2, 0)

$\therefore$ **GCD (1970, 1066) = 2**

To calculate $C = 88^7 \bmod 187$

$\therefore 88^7 \bmod 187 = [88^4 \bmod 187 * 88^2 \bmod 187 * 88^1 \bmod 187]$

I) $88^1 \bmod 187 = 88$

II) $88^2 \bmod 187 = 7744 \bmod 187 = 77$

III) $88^4 \bmod 187 = 59,969,536 \bmod 187 = 132$

IV) $88^7 \bmod 187 = [88 \times 77 \times 132) \bmod 187$

$= 894,432 \bmod 187$

$= 11$

$\phi(n)$:-

Euler's Totient Function $\phi(n)$:-

if p & q are two prime nos with $p \neq q$, then we can show that

$n = pq$

$\phi(n) = \phi(p) \times \phi(q)$

$\phi(n) = (p-1) \times (q-1)$

e.g. $p = 3, q = 7$ prime nos.

$\phi(21) = \phi(3) \times \phi(7)$

$= (3-1) \times (7-1)$

$= 2 \times 6$ gcd = 1

$= 12$

$= \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$

$\phi(n)$:- Total no of relative prime.

$d \equiv e^{-1} \bmod (\phi(n))$

$d e = 1 \times \bmod (\phi(n))$

$d \times e \bmod (160) = 1$

RSA algorithm :-

Key generation ↓

select p, q , p ≠ q both prime, p≠q

Calculate $n = p \times q$

Calculate $\phi(n) = (p-1) \times (q-1)$

select integer e → $\gcd(\phi(n), e) = 1$;
$1 < e < \phi(n)$

Calculate d → $d \equiv e^{-1} (\bmod \phi(n))$

public key → $PU = \{e, n\}$

private key , $PR = \{d, n\}$

Encryption ↓

plaintext $M < n$

ciphertext $C = M^e \bmod n$

Decryption ↓

Ciphertext C

plaintext $M = C^d \bmod n$

e.g. we have two prime nos. p=17, q=11, M=8

sol :-

$p = 17, q = 11$

$n = 17 \times 11$

$= 187$

$\phi(n) = 16 \times 10$

$= 160$

$e \rightarrow \gcd(160, e) = 1$

let e = 7

$d \rightarrow d \equiv e^{-1} \bmod (\phi(n))$

$\equiv 7^{-1} \bmod 160$

$de = 1 \bmod 160$

$\Rightarrow de \times \bmod 160 = 1$

$d \times 7 = 1$ $d \times 7 \bmod 160 = 1$

$\therefore 23 \times 7 \bmod 160 = 1$

$d = \frac{1}{7}$ $\therefore d = 23$

$PU = \{7, 187\}$

$PR = \{23, 187\}$

encryption $88 < 187$

$\therefore C = 88^7 \bmod 187$

$= 11$

Decryption ciphertext C

plaintext $M = 11^{23} \bmod 187$

16 4 2 1

$M = 11^{23} \bmod 187$

encryption: $88^7 \bmod 187 = 11$ ⟷ ciphertext ⟷ decryption: $11^{23} \bmod 187 = 88$

$11^{23} \bmod 187$

$= [11^1 \bmod 187 \times 11^2 \bmod 187 * 11^4 \bmod 187 * 11^8 \bmod 187 \times 11^8 \bmod 187]$

$\rightarrow 11 \bmod 187 = 11$

$11^2 \bmod 187 = 121$

$11^4 \bmod 187 = 14,641 \bmod 187 = 55$

$11^8 \bmod 187 = 214,358,881 \bmod 187 = 33$

$\rightarrow 11^{23} \bmod 187 = (11 \times 121 \times 55 \times 33 \times 33) \bmod 187$

$= 79,720,245 \bmod 187$

$= -88$

use RSA.

Q. If $n = 119$, publickey $e = 5$, private key $d = 77$ the demonstrate how to send the character numeric F

Soln →

∴ F is 6th character

$M = 6$

encryption: $C = 6^5 \bmod 119$

$= 6 \times 6 \times 6 \times 6 \times 6 \bmod 119$

$= 7776 \bmod 119$

$C = 41$

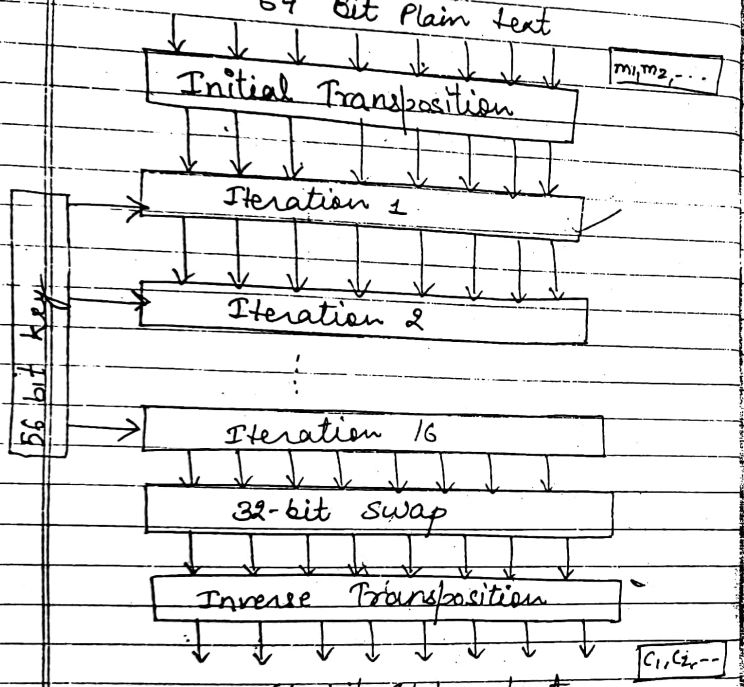
decryption: $M = C^d \bmod n$

$= (7776)^{77} \bmod 119$

$= (41)^{77} \bmod 119$

$= 6$

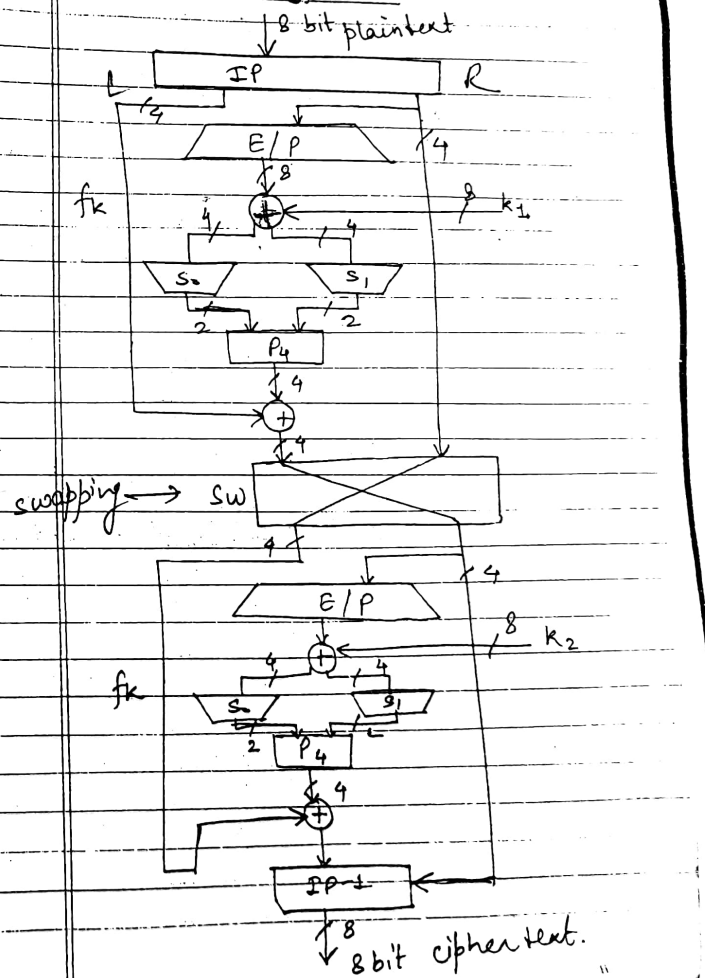
DES (Data Encryption Standard) :→



DES is developed in 1972, 56 bit key is used for encryption. figure shows the details of operation so as to encrypt the message.

Iteration 1 :-

S-DES Encryption :-



E/P : Expention / Permutation

S_0, S_1 : S_0-box, S_1-box.

IP : Initial permutation

IP^{-1} : Inverse permutation.

e.g. → suppose 8 bit PT = 10010201

→ 1st step

Initial permutation

Defaultly

IP							
2	6	3	1	4	8	5	7

0	1	0	1	1	1	0	0

2nd step: Divide or split 8 bit ~~header~~ plaintext into Left & Right Halves.

0 1 0 1 (L) 1 1 0 0 (R)

3rd step: (E/P)

E/P							
4	1	2	3	2	3	4	1

for Right Halves

0	1	1	0	1	0	0	1

4th step:- suppose k_1 = 10010010 (any code)

after this, we will find this

E/P ⊕ k_1 (Ex-OR)

0 1 1 0 1 0 0 1

⊕ 1 0 0 1 0 0 1 0

1 1 1 1 1 0 1 1

5th step:- split it into S_0 & S_1.

1111 (S_0) 1011 (S_1)

S_0 = 1 1 1 1

R_0

R_0 = $(11)_{10}$ = 3 (inside two bits)

R_0 = $(11)_{10}$ = 3 (outside 2 bits)

S_0 =

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

R_0 & C_0

⇒ $S_0(3,3) = 2 = (10)_2$.

from so matrix, we find third row & 3rd column = $(2)_2$ = 10 (Binary)

S_1 = 1 of 1

C_1 = 01 = 1

R_1 = 11 = 3

$S_1(3,1)$

S_1 =

	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

$S_1(3,1)$ = 1 ⇒ $(01)_2$

S Box = $S_0 S_1$
= 1001

Working of P_4 :-

P_4			
2	4	3	1

P_4 is 0101

Step VII :- Now X-OR with left Halves

Left 4-bit

P_4 ⇒ 0101
⊕ 0101
0000

Step (VIII) :- Switch fun

0000 (P4) ↔ 1100 (R)

1	1	0	0	0	0	0	0
1	2	3	4	5	6	7	8

Step (IX) :- Inverse permutation

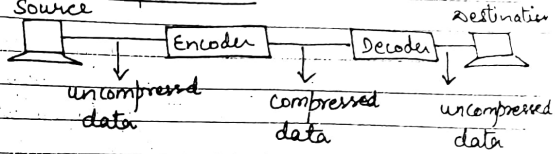
IP^{-1}							
4	1	3	5	7	2	8	6
0	1	0	0	0	1	0	0

(C) →

LZW → Lempal zip weiser.

28/4/11

Data Compression :→



Types :→
1) lossless Data compression
2) Lossy " "

→ Data Compression is essential for efficient storage & transmission of data.

→ A compression system consist of an encoder & a decoder.
→ Encoder performs compression & Decoder is used for decompression & reconstruction.

Types :-

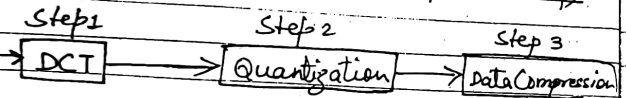
1) Lossless Data Compression :-

↳ There is no loss of data hence called the lossless compression & it is used for the text compression
→ Redundant info. contained in the data is removed e.g. → LZW compression used for digital data.

(2) Lossy Compression:-

→ There is a loss of information
→ some app^n's use this compression technique without a significant loss of the imp. info.
e.g.: used for video & audio app's.

* JPEG (Joint Photographic Expert Group):→



→ video is simply a sequence of images so video compression is also called image compression.

steps:-

(i) DCT:- (Descrete Cosine Transform)
* image is in the form of blocks of 8x8

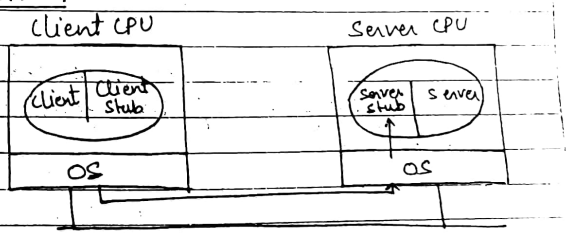
(ii) Quantization:- it reduces the no. of bits required to be used for encoding.
→ it is the process of approximation. Hence we loss some information & it is not possible to recover this info. at all: i.e by JPEG is called lossy compression.

* MPEG:- (Motion Picture Expert Group)

↳ MPEG is another of standard
↳ when compression takes into account fast forward, fast reverse or normal reverse playback modes can be made available in addition to normal playback.

Imp session layer → (Remote Procedure Calls)

RPC:-



→ RPC Method allows the commu b/w client & its Remote server.
→ The client communicate with the server for geting any procedure of the server but the direct message transfer is not possible here.

→ RPC Mechanism is based on the concept of using the procedure for communication.

Steps:-

→ The client request the server for the procedure & make a remote call for activating the server.

→ The procedure at the server corresponding to the client procedure is activated & it is called as the stub procedure.

→ RPC Mechnism uses the stub-procedure concept.

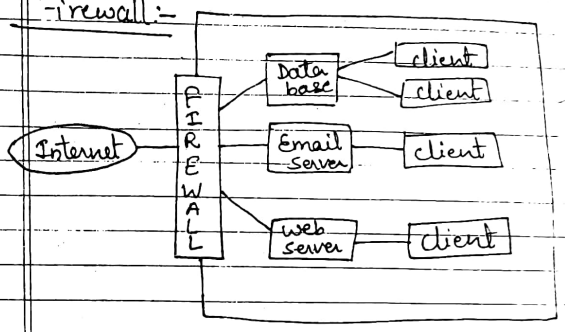
→ The client machine contains the user program & the local stub procedure

similarly,

→ Server Machine contain the Remote procedure + stub procedure.

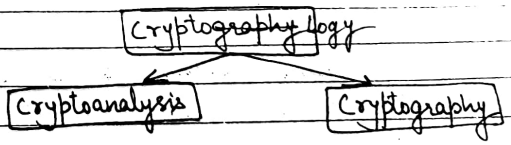
→ The client process calls the client stub procedure which is in turn transfer a Message to the remote procedure & after that to the remote server machine. on the server side, Receive primitive initiates the stub procedure to receive the message.

:-firewall:-



Types of firewall:->

(i) Packet Filtering.
(ii) Application level gateway.
(iii) Circuit level gateway.



* Hacker, Crackers.
* Brute Force Attack

↳ Dealing with the design of algo. for encryption & decryption to ensure the secrecy & authenticity of message.

↳ Other security measures :—
* Encryption System.
* Firewall.
* Intrusion detection System.
* Digital signature & Digital certificate.

Type of attack :→
(1) Passive attack :—
(a) Release of message content.
(b) Traffic Analysis.

(2) Active attack :—
(a) Masquarade.
(b) Replay
(c) Modification of message.
(d) Denial of services (entire w/o of corrupt).

Cryptographic system can be categorized into three independent dimension :—

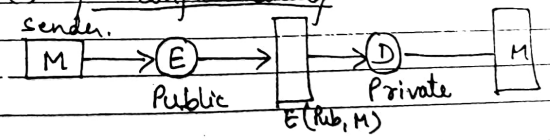
1). Type of operation used for transforming from plain text to cipher text.
(a) substitution techniques.
* Caesar cipher
* Monoalphabetic cipher
* Polyalphabetic cipher
* Hill cipher
* Play fair cipher

(b) Transposition Techniques.

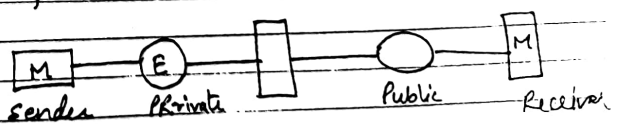
2). The no. of key used (a) Public key.
(b) Private key.

3). The way in which plaintext is processed —
(a) stream cipher.
(b) Block cipher.

① Symmetric key cryptography (same key)
② Asymmetric " "
(a) for Confidentiality :→
sender.



(b) for Authentication :—



Subnet mask = 255.255.240.0

↓ class B

2^7 +

= 288

2^4 = 16

240 = $2^7 + 2^6 + 2^5 + 2^4$ (4 bits)

1 1 1 1 0 0 0 0

$2^{12} - 2$

10.112

0000 0

255

1 1 1 1 (16)

2^7 ... + 2^0

6 subnet

n = 3

$2^3 = 8$

$2^2 = 4$

8

256/8 = 32

0 – 31 — 000

0 – 63 — 001

1 – 32

32

0 – 31

32

0 – 255

Physical address — MAC
IP address — Logical
Subnet mask —
default gateway
DNS server
Alternate DNS S.

32 bit

8 bit	8 bit		

Subnet mask 11111111
Class A = 255.0.0.0 address
Net ID Host
256 256

Class B 255.255.0.0
16 bit Net ID 16 Host = 65536

Class C 255.255.255.0
24 Net ID 8 Host

256

192.2.6. 000 00000 0

255.255.255.255

= 2^{32}

2 ↓ 2 ↓ 2

$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$

Host 3 bit
32
5 bit Host

n = 3 Total number of Subnet $= 2^n = 2^3 = 8$

000
001
010
011
100
101
110
111

0 – 255
= 256 / 32 = 8

Sub

192.1.6. 000 00000 Network address
000 00001 First Host
00010
00011 (0–31)
82
000 11111 Last Host
192.1.6 001 00000

Physical address — MAC
IP address — Logical
Subnet mask —
default gateway
DNS server
Alternate DNS S.

32 bit

8 bit	8 bit		

Subnet mask

11111111

Class A = 255.0.0.0 — address

Net ID — Host

256

Class B 255.255.0.0

16 bit Net ID — 16 Host — 65536

Class C 255.255.255.0

24 Net ID — 8 Host

256

255

192.2.6. 00000000

255.255.255.255

256

32

$= 2^{32}$

$2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0$

32

Host — 8 octet — 5 bit Host

n = 3

Total number of Subnet = $2^n = 2^3 = 8$

000
001
010
011
100
101
110
111

0 – 255

$\frac{256}{8} = 32$

Sub

192.1.6. 000 00000 — N/w address

000 00001 — First Host

00010

00011

0 – 31

32

000 11111 Last Host

192.1.6 001 . 00000

Theorems are —

1). Nyquist Theorem is
↳ for Noiseless channel.

2). Shannon's Theorem:→
↳ for Noisy channel.

1). Nyquist Theorem:→

Two important characteristics of a transmission channel are—

(i) Signal to Noise ratio (SNR)
(ii) Bandwidth

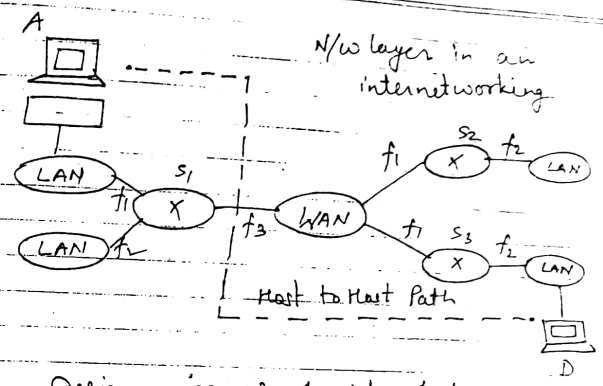
Nyquist theorem states that "If the Bandwidth of channel is 'B' which carry a signal having 'L' no. of levels then the max. data rate 'R' on this channel —

$$R = 2B \log_2 L$$

As max. datarate for reliable transmission is defined as channel capicity 'C'. The above expression gets modified as —

$$C = 2B \log_2 L$$

NETWORK LAYER



Design issues of Network layer:→

(i) Services provided to the transport layer.
(ii) internal organisation of the network layer.
(a) To use the connection oriented services.
(b) To use the connectionless services.

(a) To use the connection oriented service :-

it is called virtual ckt connection it is similar to the physical connection.

- establish the connection
- uses the connection
- release the connection

(b) To use connection less service:

- it is also called datagram ckt.
- Packets move independently

Difference b/w virtual ckt & Datagram ckt

S.No.	Parameter	Virtual ckt Subnet	Datagram Subnet
1.	ckt setup	Required	Not Required
2.	Addressing	each packets contains a virtual ckt number	each packet contains source as well as Destination Address
3.	Repair	Harder to Repair	easy to Repair
4.	State info.	A table is needed to hold the state info.	Subnet does not hold state info.
5.	Routing	Each packets of the message follows the same route. This is also called static Routing.	each packet is route independently This is called Dynamic Routing.
6.	conjection Control	easy to control	Difficult
7.	effect of Router failure	All virtual ckts which passed through failed Router are terminated	No other effect except for the packet at the time of crash.

Router :→

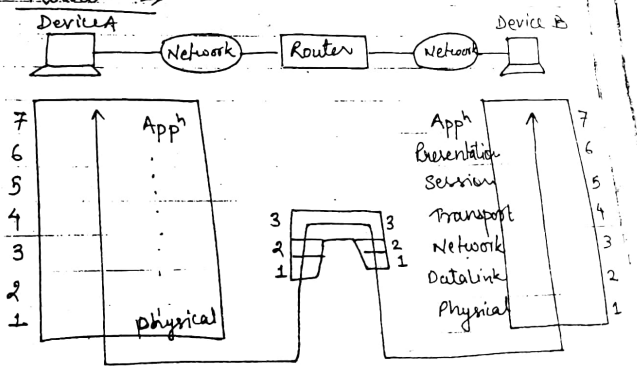


fig: A router in OSI Model.

- Router are the devices that connects two or more networks which is shown in figure.

- They consist of a combination of hardware & software.
- The hardware can be a network server, a separate computer, or a special device.
- The softwares in the Router are operating systems, Router protocols, Management softwares can also be used.
- The Routers use logical & physical addressing to connect two or more logically separate networks.
- Route discovery is the process of finding the possible routes through the internetwork & then building routing tables to store that informations.
- The two methods of Route discovery are —
  - (i) Distance Vector Routing. (Dynamic Alg.)
  - (ii) Link State Routing.
- Router works at the network layer of the OSI Model.

Routing Algorithms :→ (Imp) (static → Dijkstra, Dynamic)

- it is used to provide the best path from source to destination.
- it is responsible for deciding the output-line on which a packet is to be send.
- Such a decision is dependent on the robustness on the virtual ckt. it is a datagram ckt.

Properties of Routing Algorithms :→

- Correctness & Simplicity :→
- Stability :-
- Robustness :-
  - it should be able to coperate with the changes in the topology & traffic without requiring all jobs in all host (PC) to be abort it and the network to be rebooted every time some router crashes
- fairness & optimality :→
  - ↳ fair if No one approach.
  - ↳ enough traffic between A & A', to saturate the Horizontal link.