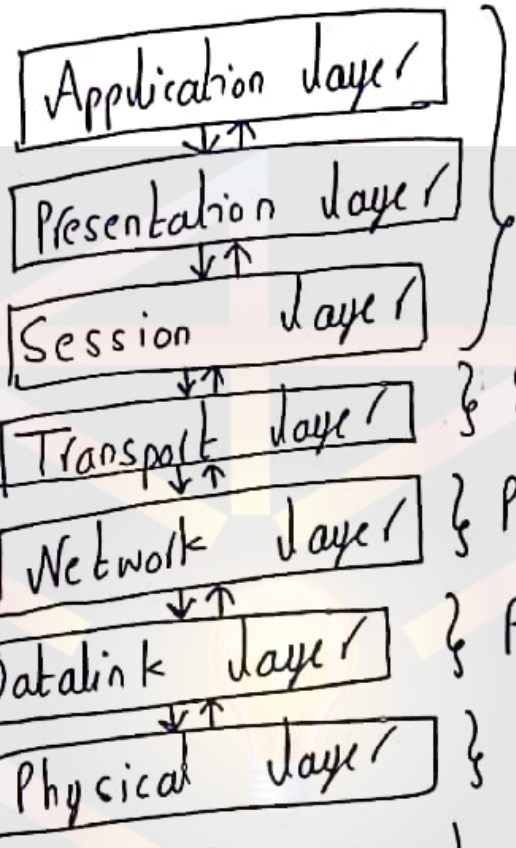
1) Explain in detailed about ISO - OSI & TCP/IP reference model indetailed.

Ans OSI



→ OSI (Open System interconnection)

→ Created by ISO

→ It was created as a frame work & reference model to explain how different technologies work together & interact.

→ It is not a standard that networking protocols follow each layer

has specific functions it is responsible for all layers work together in the correct order to move data around a network.

→ Physical layer :-

TCP - 7 layers
UDP - virtual (5 layers)

→ Deals with all aspects of physically moving data from one computer to the next.

→ Converts data from upper layers into 1's & 0's for transmmission over media.

→ Defines how data is encoded on to the media to transmit the data.

→ Defines on this layer cable standards wireless standards & fiber optics standards

→ It is copper wiring, fiber optics cable, anything that can be used to transmit data is defined on the physical layer of OSI model

ex: of devices

HUB: Use to transmit data

→ Functions of Physical layer:

→ bit synchronization: moving info in one particular order

→ bit rate control: bit per sec

→ Physical topologies: all types of topology

→ Transmission mode: Simple duplex, half duplex & Full duplex.

→ Data link layer: (Wired connection)

→ It is responsible for moving frames from node to node or computer to computer

→ It can move frames from one adjacent computer to another

→ It cannot move frames across routers (wireless).

[Frames cannot be sent segments are used]

→ requires MAC address or physical address

→ Protocols defined include:
ethernet protocol & point to point protocol.

→ Device example switch, bridge

→ Two subdayers of Data link layer

i) LLC (logical link control)

ii) MAC (Media access control)

→ logical link control:

→ Data link layer addressing, flow control, address notification & error control.

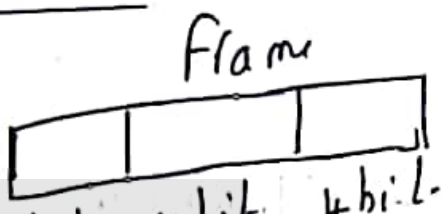
→ Media access control:

→ Determines which computer has access to the network media at any given time

→ Determines where one frame ends & the next one starts called frame synchronizabion.

→ Funchions of DLL:

- → framming
- → Physical Addressing
- → error control
- → flow control
- → Acecs control



→ Network dayer: (wiredess)

Responsible for moving packets (data) from one end of the net-work to end the other, called end to end communication

- → requires logical addres (IP)
- → exi router
- → routing is the abiliby of various network devices & their redated software to move data packets from source to destination.

→ Segments in the network layer is referred as packet.

→ Functions of NL :-

→ routing
→ logical address.

→ Transport layer :-

→ Takes data from higher level of OSI model and breaks it into segments that can be sent to lower level layers for data transmission
→ Reassembles data segments into data that high level protocols & applications can be used
→ Also puts segments in correct order called sequencing so that they can reassemble in correct order at destination
→ Concerned with the reliability of the transport of sent data.

→ May use a connection oriented protocol such as TCP to ensure destination received segment

→ May use a connectionless protocol such as UDP to send segments without assurance of delivery.

→ Functions of transport layer :-

→ Segmentation & Reassembling

→ Session layer :-

→ Responsible for managing the dialogue b/n Network divisors

→ Establishes, manages & terminates connection

→ Provides duplex, half duplex or simplex duplex communications b/n devices

→ Provides procedures for establishing checkpoints, termination & restart or recovery.

→ Functions of Session layer:

→ Session establishment, maintanance & termination
→ Synchronization
→ Dialogue controller

→ Presentation layer:

→ concerned with how data is presented to network.
→ Handles 3 primary tasks

i) Translation
ii) Compression
iii) Encryption

} Functions & tasks

Translation → Changes data so that another type of computer can understand it (ASCII codes).

Compression → Makes data similar to send more data in same amount of time.

Encryption → Encodes data to protect from interception or droping.

→ Application layer :-

→ Contains all services or protocols needed by application software or operating systems to communicate on the network

ex:- → Firefox web browser uses http

→ Email program may use pop 3 (post office protocol) to read emails & SMTP to send emails

→ Functions of Application layers:

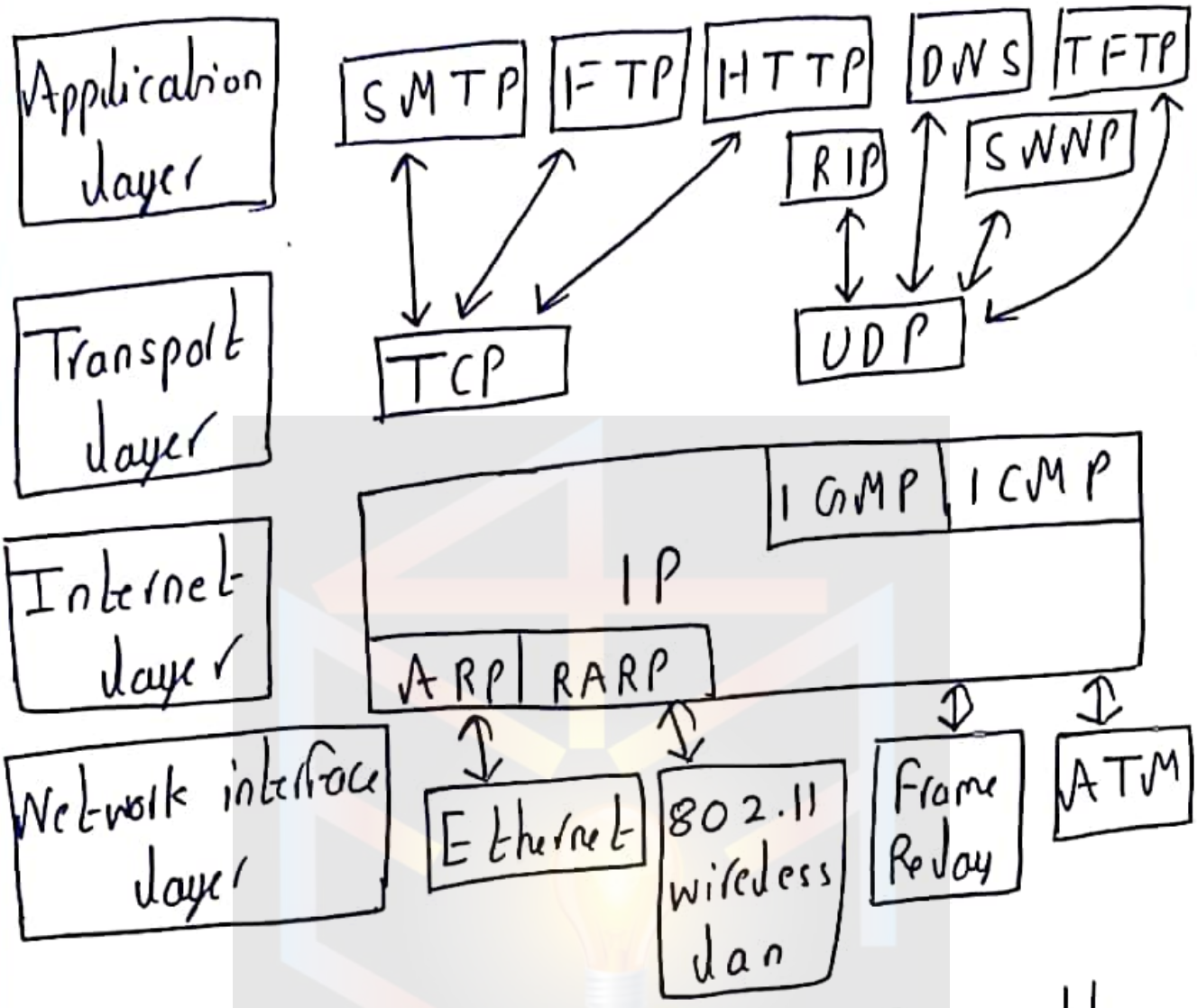
→ Network virtual Terminal

→ FTAM (File transfer Access & Management).

→ Mail Services

→ Directory services.

→ TCP/IP Model :-



→ Application layer : protocol define the rules when implementing specific network applications to provide accurate & effecient data delivery.

→ Tipical protocols.

FTP - File transfer protocol

Telnet - remote terminal protocol.

SMTP - Simple mail transfer protocol

HTTP - Hypertext transfer protocol (Web browsing)

→ W compases same functions as these OSI model layers presentation layer, application, & session layer.

→ Transport layer: TCP & UDP

TCP: (connection)

→ Physical connection

→ TCP provides a function to allow virtually exist also called virtual circuit.

UDP (connection less layer)

→ Dividing the chunks of data

→ reassamble segments into the original chunk

→ provides functions reordering & data resend

→ offering a reliable bit stream delivery service.

→ Functions are same as transport layer

→ Synchronize source & destination computer to setup the session b/n the respective computer.

→ Internet (or) Network layer:

Host to network layer: It is the lowest layer of TCP/IP reference model

→ It combines the datalink & physical layer are combined

→ Data transfer b/n network nodes in a single WAN & b/n nodes on same LAN.

2) Explain congestion control algorithms in detailed.

Ans Congestion: To many packets present in the network causes packet delay & loss that degrades performance. This is congestion.

→ CNP assignment 1 (PDF)

→ Services / Responsibilities of Network layer

→ Responsible for moving packets (data) from one end of the network to the other, called end to end communication (source to destination).
(it requires logical address (IP))
ex: routers are used.

→ routing is the ability of various network devices & their related software to move data packets from source to destination.

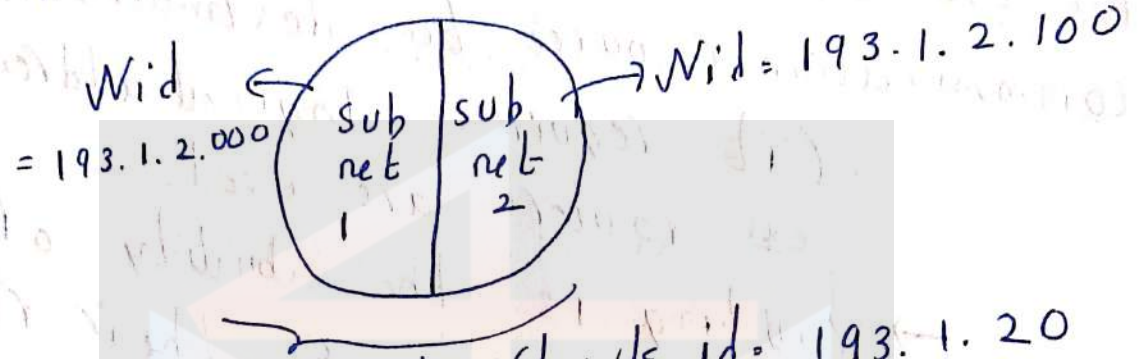
→ Fragmentation, dividing data into frames. (based on reciever acceptance).

→ Congenshion control using some standard algo's, we also try to solve it.

we will discuss abt routing & congenshion in this chapter further.

→ Subnetting :-

When a bigger network is divided into smaller networks in order to maintain security then that is known as subnetting



→ datagram Subnet/ circuit

→ Connection less
→ each packet is routed independently
→ each packet header contains the full destination address
→ No reservation

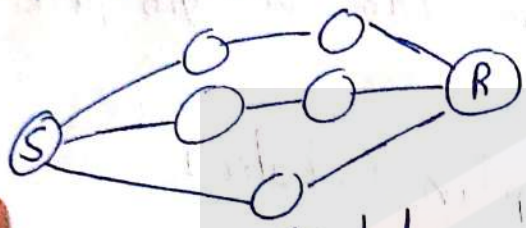
Virtual Circuit Subnet

→ connection oriented
→ All packets follow the same route
→ only first packet header contains Full destination & rest have short virtual circuit numbers.
→ reservation exist for bandwidth, CPU, Buffers etc..

→ can be received in no order (out of order).

→ cost ↓

→ delay ↑



→ not realiable

→ always in order.

→ cost ↑

→ delay ↓

→ ~~not~~ Realiable

→ **Routing algorithm:**

→ Main function of network layer is routing packets from source machine to destination machine.

→ Their are two processes ~~inside~~ each packet as it arrives looking of the outgoing line to use for it in the routing table.

i) One of them handles

(This process is called forwarding)

ii) The other process is responsible for filling in & updating the routing table.

This is where routing algorithms come into play.

→ Routing algorithm can be grouped into 2 major classes

i) Non-Adaptive (static)
ii) Adaptive (Dynamic).

i) Non-Adaptive algorithms: They don't base their routing decision on measurement or estimate of the current traffic & topology.

→ No dynamic all are static pre written steps/paths are followed.

→ It is computed in advance offline & downloaded to the router when the network booted.

→ also called as static.

ii) Adaptive algorithm: This algorithm will change their routing decisions to reflect changes in the topology & usually the traffic as well.

→ info will be collected from either adjacent or from all routers.

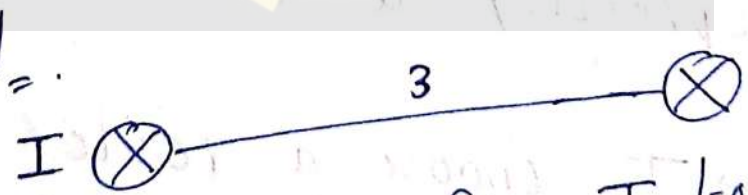
→ As it changes as per requirement it is also called, dynamic

Few routing algorithms:

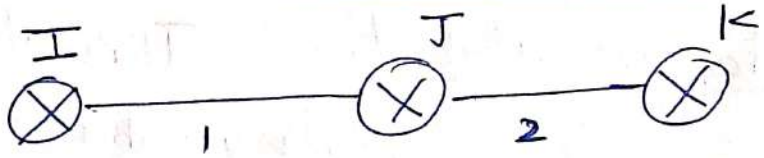
i) Optimality principle: (just a principle)

→ One can make a general statement about optimal route, without regard to network topology or traffic.

→ It just a principle which can be applied.



if the path from I to K is optimal then.



if any router exist between I & K i.e J

So the path from I to J and J to K will also be optimal (stable)

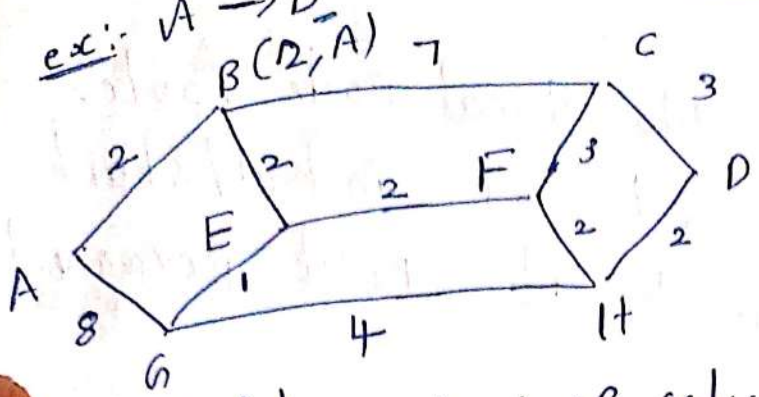
II) Shortest path (Dijkstra's)

→ here we find the shortest cost path b/n sender to receiver

→ The idea is to build a graph of subnet with each node of the graph representing a router & each arc of graph representing a communication line or link.

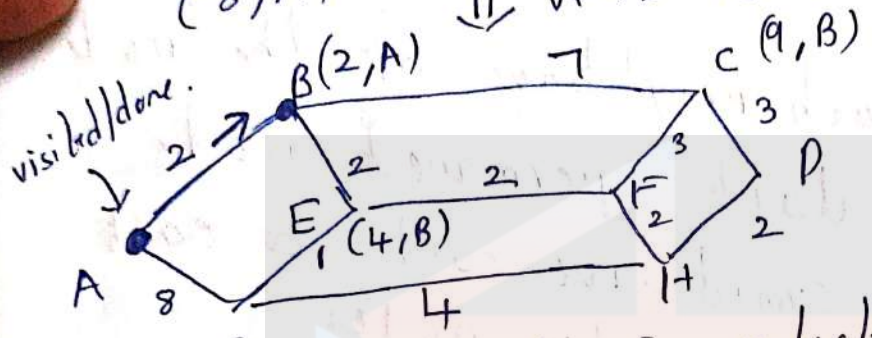
→ To choose a router b/n a given pair of routers the algorithm just finds shortest path b/n them in the graph.

ex:- A → D



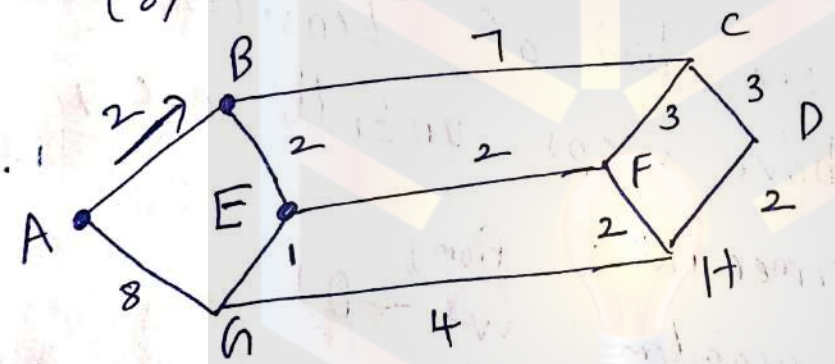
(8, A)

// A → B selected ⇒ 2 cost.

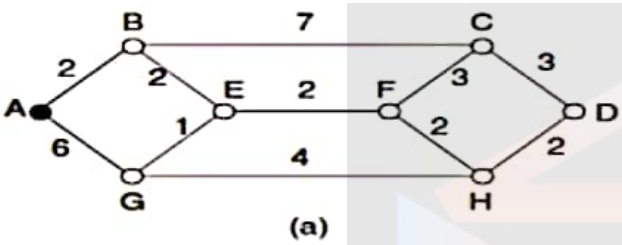


(8, A)

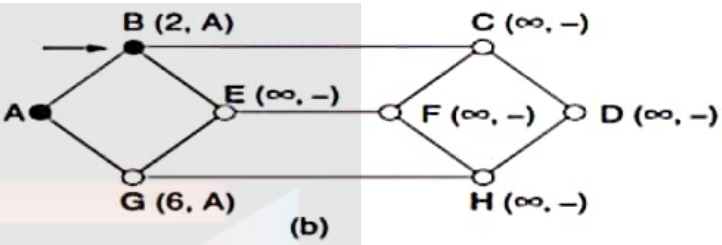
// B → E selected - 4 cost total



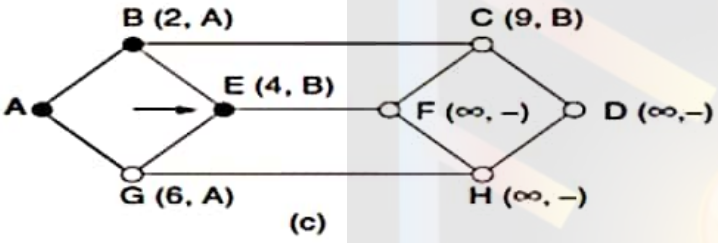
Pasbe diagram.



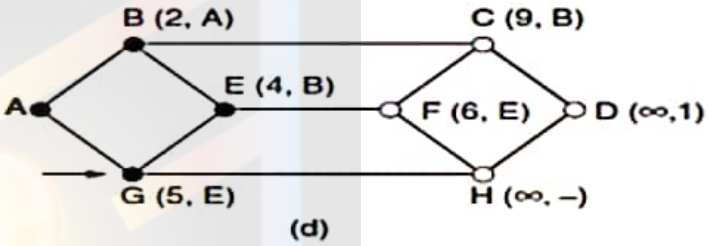
(a)



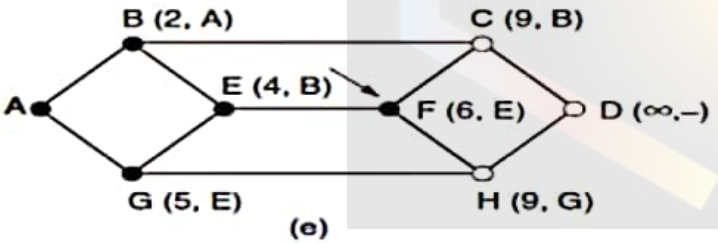
(b)



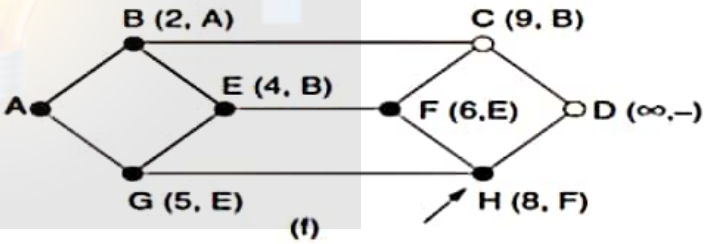
(c)



(d)



(e)



(f)

Steps

→ start with the local node router
→ Assign the cost of inital/start node to 0 & make it first permanent /visited nodes
→ Examin each neighbour of the node that was the last permanent node
→ Assign a cumidative cost to each node & it tentitive/adj nodes
→ Among the list of tensitive nodes
→ repeat above steps untill every node becomes permenant.

For same previous problem

Iteration	Permanent	Tentitive	A	B	C	D	E	F	G	H
Inital	{A}	{B, G}		2	∞	∞	∞	∞	8	∞
1	{A, B}	{G, C, E}				4	∞	8	∞	
2	{A, B, E}	{G, C, F}					9	∞	4	6	5	∞
3	{A, B, E, G}	{C, F}						9	∞	4	6	5	∞
4	{A, B, E, G, F}	{C, D, H}							9	∞	4	6	5	8

5 {A, B, E, G, F, H} {C, D} 2 9 10 4 6 5 8

6 {A, B, E, G, F, H, C} {D} 2 9 10 4 6 5 8

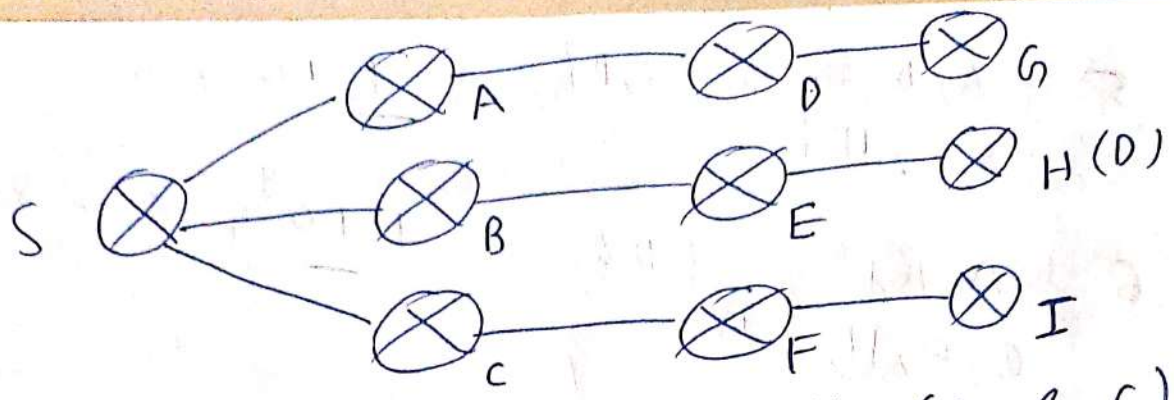
11 {A, B, E, G, F, H, C, D} { } 2 9 10 4 6 5 8

hence from the above table we can send data from a to any node we have found the cost (static method).

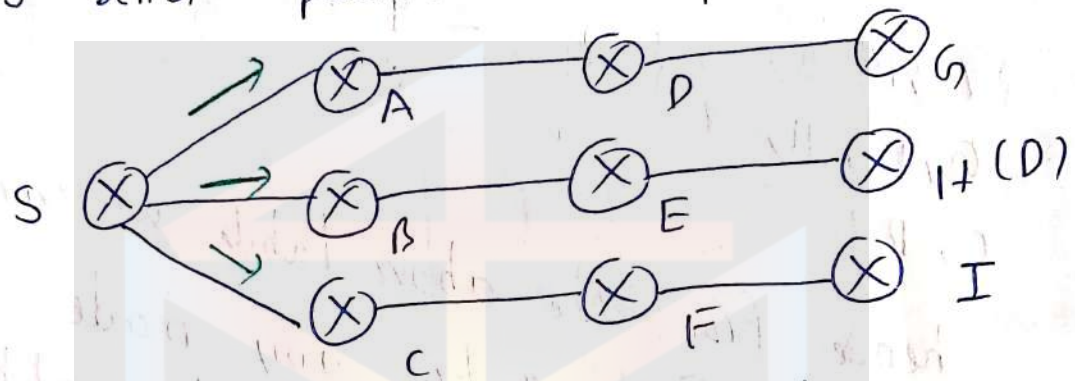
III) Flooding: (static).

→ As the name flooding the algorithm sends the packet in all the possible paths except itself.

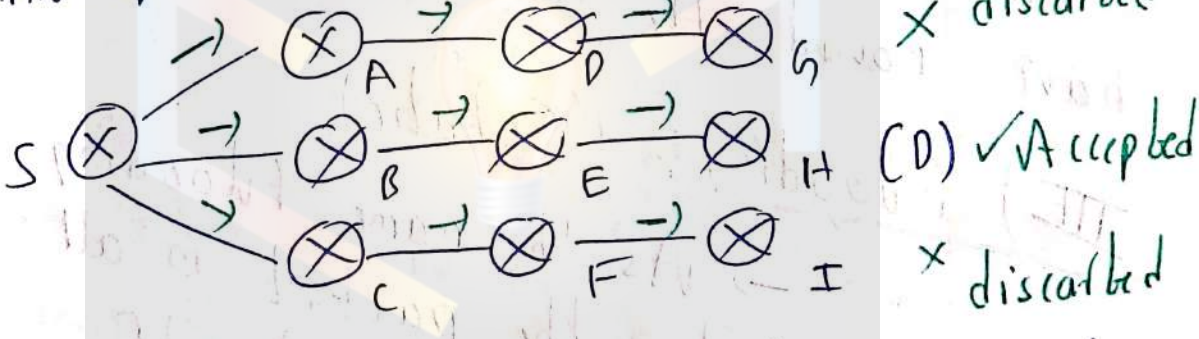
→ This process continues at each & every node. Once the packet reaches end (dead end) it is discarded & if it is received by the receiver it will be accepted.



S sends packet to all paths (A, B, C)



similarly forward till deadends



→ flooding obviously generated vast no. of duplicate packets in fact an infinite of useless packets

→ hence flooding not practically used. but it garentees delivery of packet if path exist.

IV) Distance vector routing :-

→ In distance vector routing the least cost route b/n any two nodes is the route with minimum distance.

→ In this protocol as the name says each node maintains a vector (table) of min distance to every node.

3 stages / steps. [also called Bellman Ford routing algorithm].

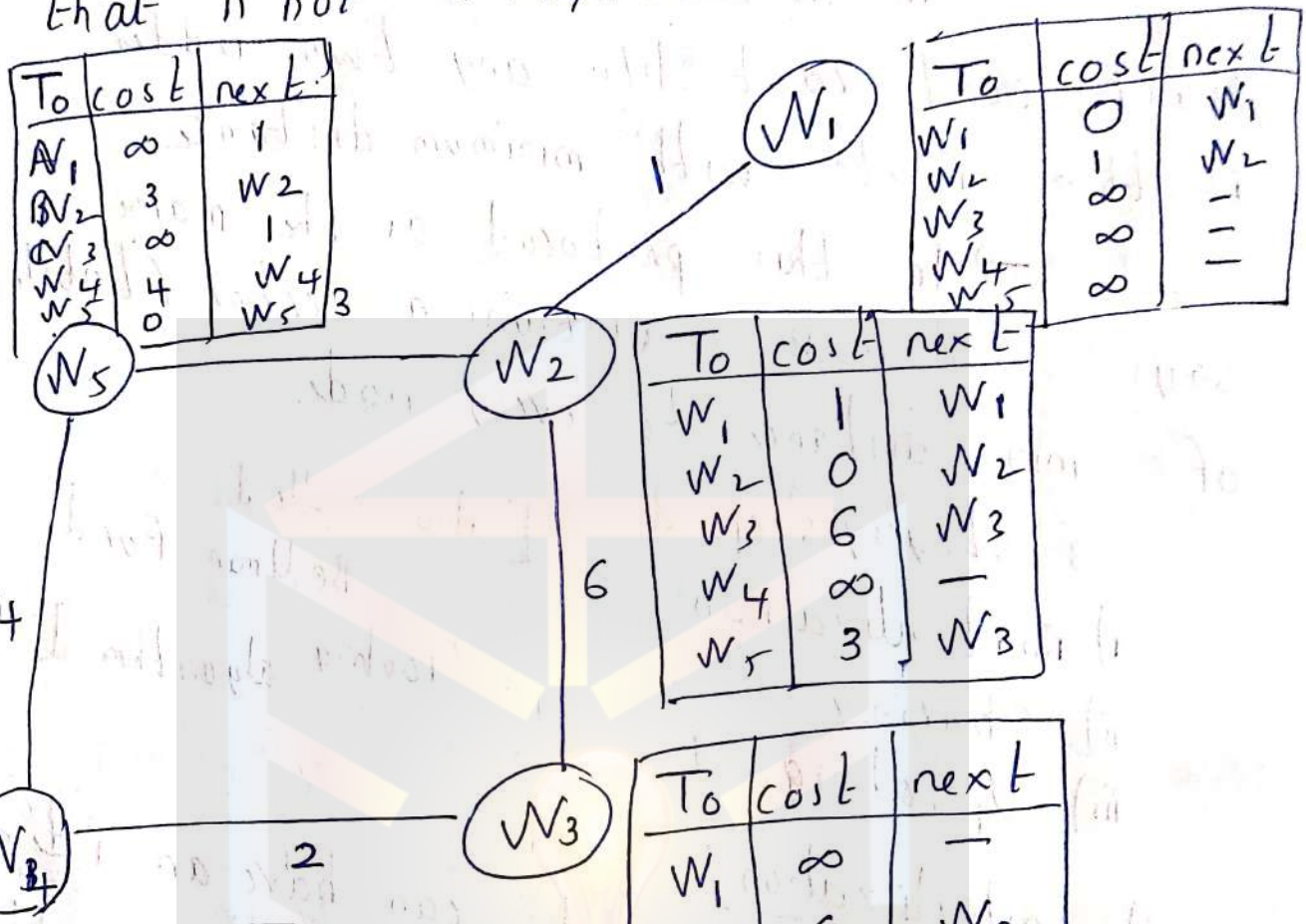
i) initialization
ii) sharing
iii) updating

i) Initialization :-

→ each node can have an idea abt the distance b/n itself & the neighbours those are directly connected.

→ each node will send a message to the immediate neighbour to find the distance b/n itself & their neighbours.

→ The distance for any entry that is not a neighbour is ∞ (unreachable)



To	cost	next
W1	∞	1
W2	3	W2
W3	∞	1
W4	4	W4
W5	0	W5

To	cost	next
W1	0	W1
W2	1	W2
W3	∞	—
W4	∞	—
W5	∞	—

To	cost	next
W1	1	W1
W2	0	W2
W3	6	W3
W4	∞	—
W5	3	W3

To	cost	next
W1	∞	—
W2	6	W2
W3	0	W3
W4	2	W4
W5	∞	—

To	cost	next
W1	∞	—
W2	∞	—
W3	2	W3
W4	0	W4
W5	4	W5

Now initialization is done

ii) Sharing:

→ The whole idea of distance vector routing is the sharing of the info b/n neighbour (info is nothing but distance vector).

For previous example.

→ N_1 share with N_2
→ N_2 " " N_1, N_3, N_5
→ N_3 " " N_2, N_4
→ N_4 " " N_3, N_5
→ N_5 " " N_2, N_4

Note: shared only with neighbour as mentioned above & only distance vector is share not whole table.

iii) Updating:

→ Once a node receive the distance vector now it will try to update the table of this node.

eg: assume N_1 received N_2 distance vector.

received W_2

1
0
6
∞
3

W_1's distance vector table

To	cost	next
W_1	0	W_1
W_2	1	W_2
W_3	∞	–
W_4	∞	–
W_5	∞	–

new table

To	cost	next
W_1	0	W_1
W_2	1	W_2
W_3	7	~~W_2~~, W_3
W_4	∞	–
W_5	4	~~W_2~~, W_5

$W_1 \to W_2$ & $W_2 \to W_2$
1 + 0 = 1

$W_1 \to W_2$ & $W_2 \to W_3$
1 + 6 = 7

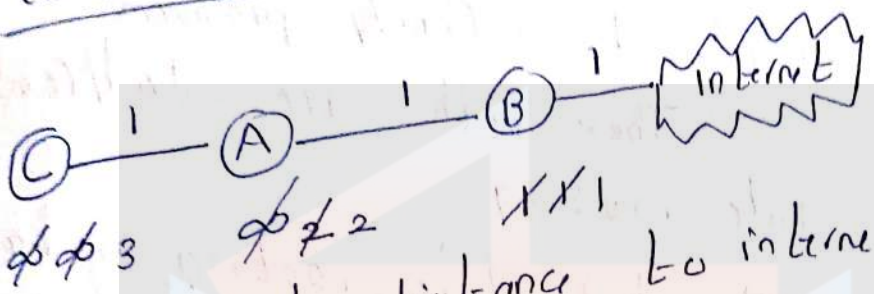
$W_1 \to W_2$ & $W_2 \to W_4$
1 + ∞ = ∞

$W_1 \to W_2$ & $W_2 \to W_5$
1 + 3 = 4

similarly all tables are updated & again sharing is done & updated & this process keep on continuing.

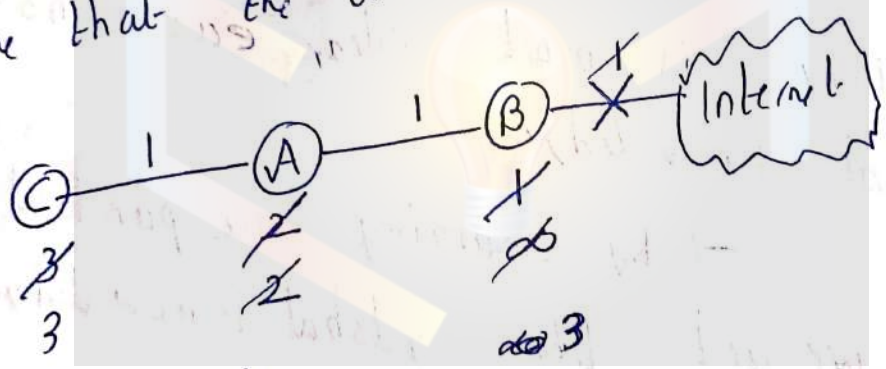
Hence after 2 or 3 iterations we get the final tables with distance b/n any dest is available

→ Count to Infinity problem:



every node distance to internet.

Now the above diagram is a normal scenario assume that the link b/n B & internet broken



4 4 5

5

hence an disadvantage/problem in Distance vector routing.

VI. Link state routing:

→ As we have seen previously the problems caused by the distance vector routing by sharing only distance vector & only to it neighbour which caused multiple pases & count to infinity problem.

→ These both are solved/resolved using link state routing.

→ link state routing is based on the assumption that although the global knowledge (about all other nodes) about the topology is not clear, each node have partial knowledge.

→ By combining the partial knowledge we get the global knowledge of the node.

→ here also we maintain a linkstate table. (Packet)

Steps :

i) Creation of the states of the links by each node called link state packet (LSP).

ii) Discover its neighbors & learn their network addresses

iii) Set the distance or cost metric to each of its neighbour in LSP.

iv) ~~Construct a packet telling~~ Passing of LSP to every other router called hope (using flooding)

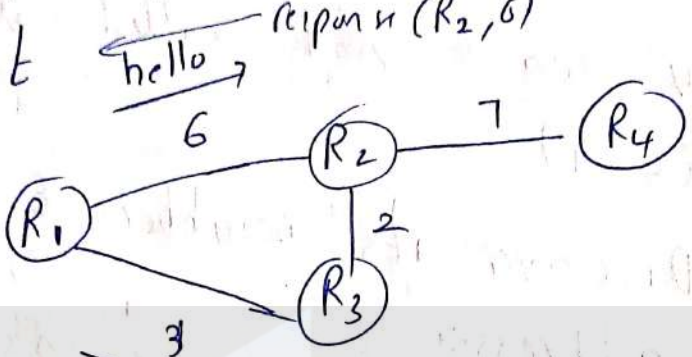
v) formulate/cacudate shortest path to each other.

vi) Update LSP's using the global info/ shorter path.

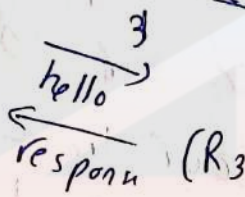
I) Discover its neighbours

→ To find distance b/n neighbours the node sends hello packet to each path (Hello packet) & neighour reipond

back through which it can determine who is the neighbour & what is the distance / cost

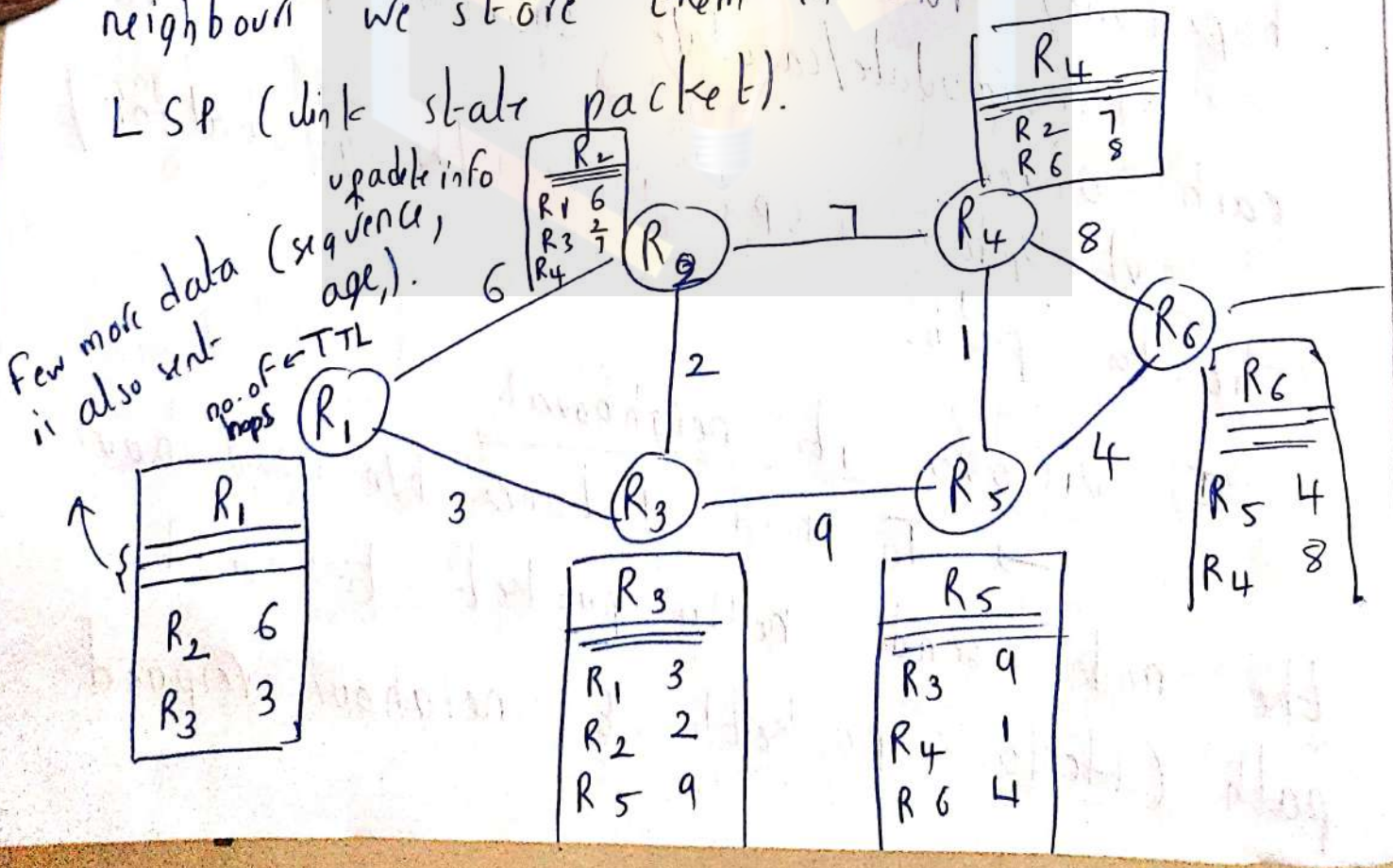


at R1



ii) setting up / updating / creating LSP:

→ As we got the responses from neighbours we store them in a table called LSP (link state packet).



iii) Passing of LSP to every other router called hope (using flooding)

→ using the concept of flooding every node sends / transmits to all the possible nodes.

→ Node to neighbour → neighbour will all reached.

hence here

R_1's table will be available at- R_2, R_3, R_4, R_5, R_6.

similarly all have all other tables

iv) calculating the shortest path

→ by combing all the partial knowledge the who graph is recreated.

→ using shortest path.

Source (R_1)	R_2	R_3	R_4	R_5	R_6	
	6	3	∞	∞	∞	
R_1, R_3	5	3	∞	12	∞	
R_1, R_3, R_2	5	3	12	12	∞	runtimes for each node.
R_1, R_3, R_2, R_4	5	3	12	12	21	
R_1, R_3, R_2, R_5	5	3	12	12	16	

v) Update the LSP:

For R_1

		Via
R_1	0	R_1
R_2	5	R_3
R_3	3	R_1
R_4	12	R_3, R_2
R_5	12	R_3
R_6	16	R_3, R_5

Hence in the same way for all nodes we do the same to know the cost b/n any 2 nodes.

VI) Hierarchical routing:

→ Hierarchical routing is introduced to resolve the problems faced in Distance vector or link state routing.

few are 1) more memory needed to store routing tables.

2) more cpu time is needed to scan each routing table.

3) more bandwidth required to send scanning report.

→ In hierarchical routing, routers are classified in group known as region.

→ each router has only the information about the routers in its own region & has no information about routers in other regions

→ routers just save one record in their table for every other region.

→ even after dividing into regions if the network is too big then we go to make clusters

→ each cluster contain no. of regions & each region contain no. of routers.

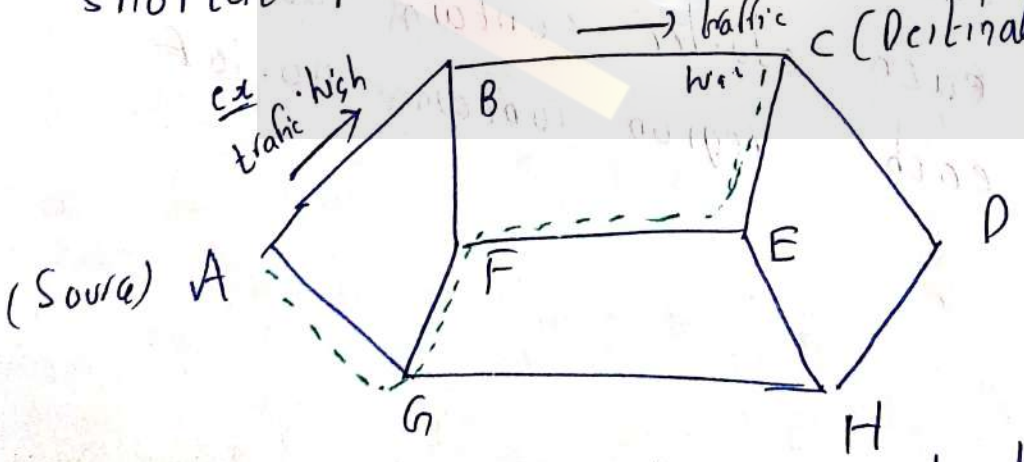
VII) Flow Based routing (static)

→ This is a static algorithm which uses topology & load condition (traffic) for deciding a route.

→ As in shortest path algo we select shortest path b/n node to send data.

→ but if every node refer/ uses the shortest path eventhough it is shorter could take long time (due to traffic)

→ Hence in fload bas routing if their is traffic we select the next shortest path to send data.



Note: when cost/distance not give us no. of hops as cost

hence we will select next shut path like A-G-F-E C or A-G-H-E-C

~~VIII~~ P

→ To use this technique of flow based routing the following info should be known

i) subnet topology (paths)
ii) Traffic matrix (traffic status current)
iii) the capacity matrix. (max bandwidth/capacity per link/path).

VIII) Broadcast Routing :-

Sending a packet to all the nodes on the network simultaneously is called broadcasting.

ex: → weather reports
→ radio program etc...

methods:

i) Distinct Point to Point routing: This is a simply send a distinct packet to each destination → hence it is waste of bandwidth but it also require complete list of all destinations

ii) Flooding :- Flooding algorithm send a packet on every outgoing line except the line on which it arrived.

→ drawback more bandwith consumed & duplicate packets

iii) Multi Destination Routing :- here each packet contains either a list of destinations or a bit map indicating the desired destination.

→ when a packet received from broad casting, it decides the number of output lines that are needed by examining each destination.

→ based on that router generates a new copy of packet to each output line.

iv) Use of Spanning tree :- here we use sink tree for the router willing to broadcast a packet (use of spanning tree).

→ A spanning tree is a subset of the subset that includes all the routers but contains no loops. iv) Reverse Path Forwarding next page

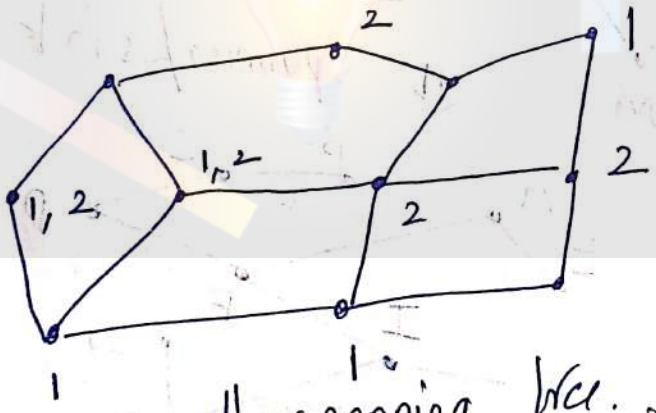
IX) Multicast routing :-

→ Sending a message to a group (large) is called multicasting

→ Multicasting requires group management need to create & destroy groups, & to allow processes to join & leave groups.

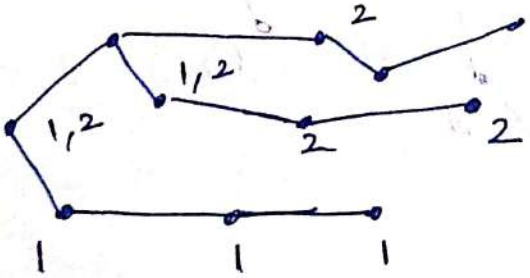
→ To do multicast routing each router computes a spanning tree covering all other routers.

ex:

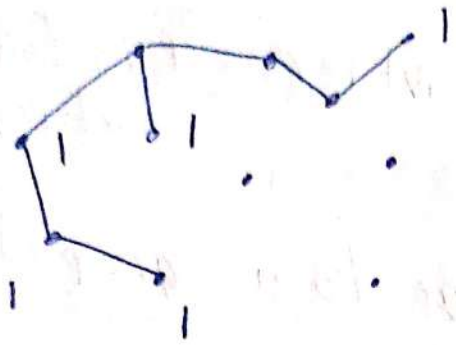


Group 1 → 1
Group 2 → 2

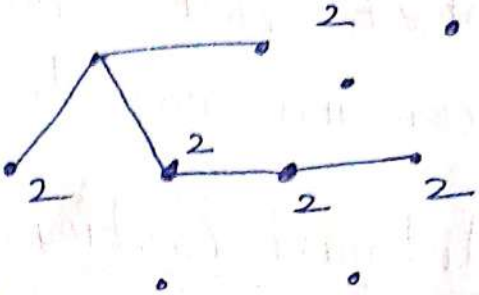
⇓ spanning tree.



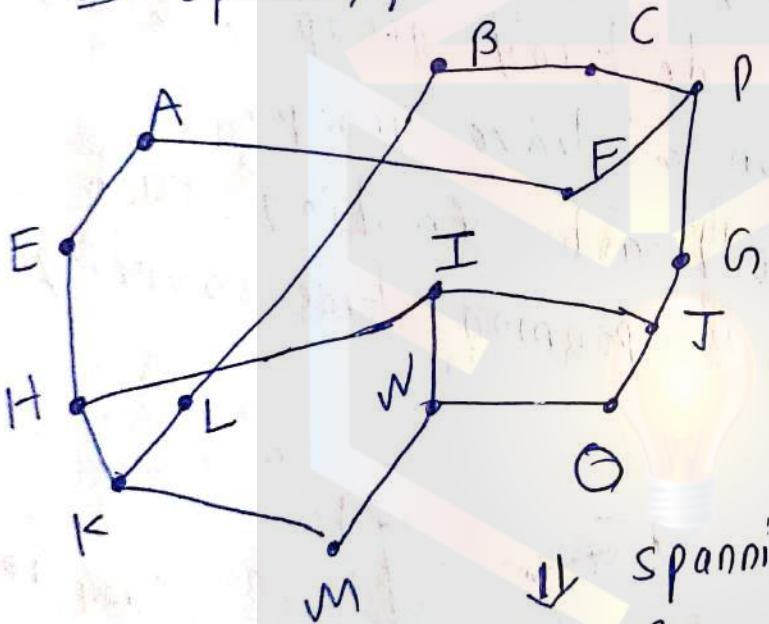
For group 1



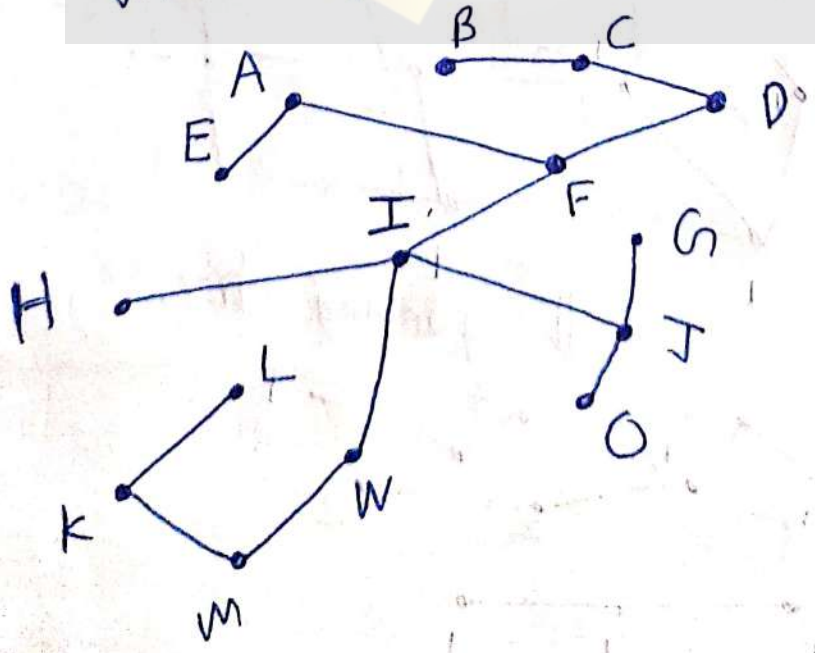
For group 2



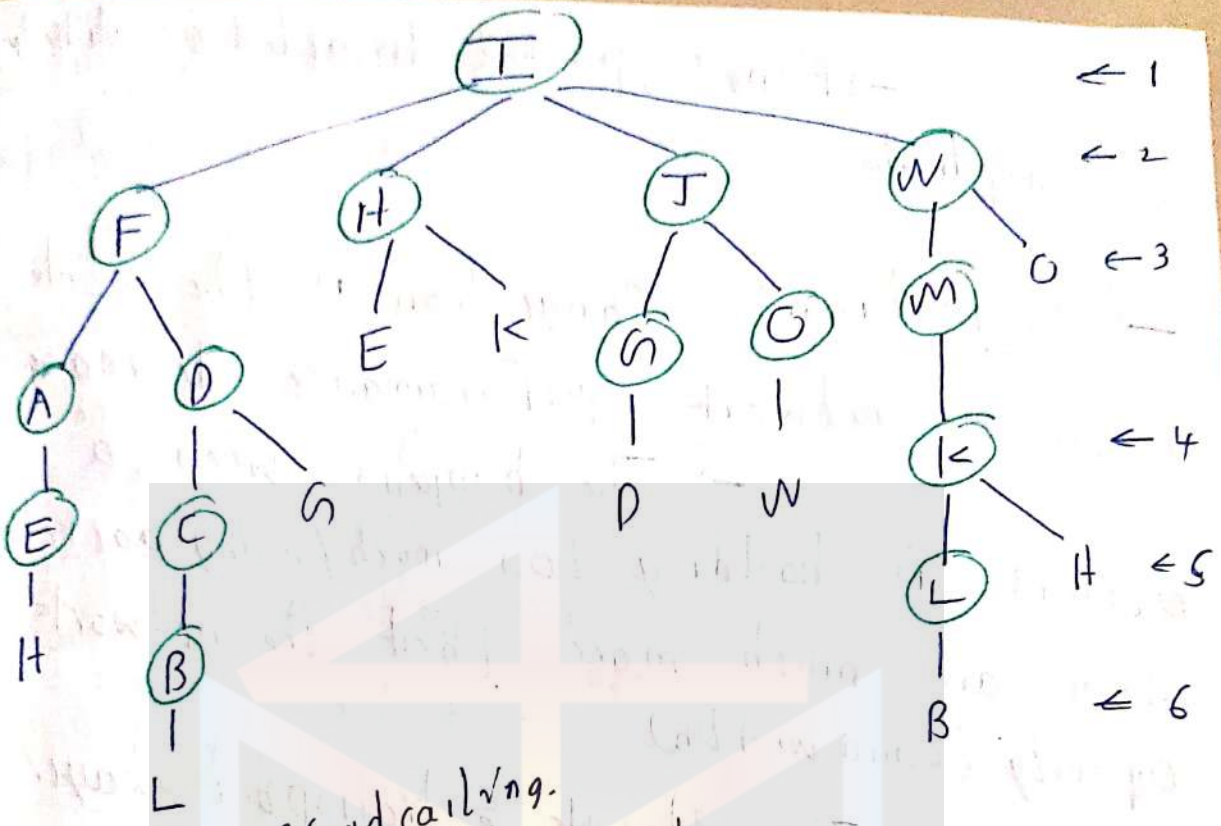
ex: spanning / sink tree.



⇓ spanning / sink tree.



⟹ Reverse path Forwarding



Broadcasting.

6 - 1 = 5 ⇒ hops

24 ⇒ packets

in reverse dvd forwarding

5 - 1 = 4 hops

15 packets.

v) Reverse Path Forwarding :-

→ Router checks whether broadcast packet arrived on interface that is used to send packet to source of broadcast

- if so it's likely that it's following best route

- if not, packet discarded as likely duplicate.

→ **Congestion:-** Congestion is the state in which network performance decreases

→ The happens when a network is holding too much/many packets which are much more that the network capacity (bandwidth)

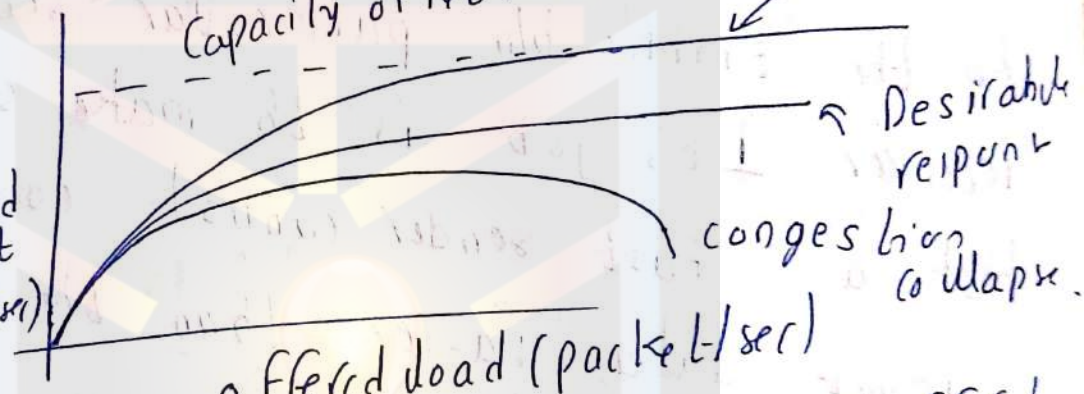
→ The network & transport layer share the responsibility for handing congesion

→ **Congestion control:**

→ refers to the mechanism & techniques that can either prevent congestion before it happen (or) remove congestion after it happen.

→ As we know conjussion occurs within the network layer that directly experiences it & must ultimately determine what to do with the excess packets.

→ The most effective way to control conjusion is to reduce the load that the transport layer is placing on the network.



→ When too much traffic is offered conjusion comes into play & performance degrades.

→ hence we should find a solution to this.

→ Diff b/n Conjusion Control & Flow control

→ Conjusion control has to do with making sure that the network is able to carry offered traffic it is a global issue involving the behavior of all host & routers

→ Flow control in contrast related to the traffic b/n particular sender & receiver. It's job is to make sure that a fast sender cannot continously transmit data faster than the receiver is able to absorb it

→ A simple solution for both could be making to host sending data slowdown thus a host can ~~or~~ send slower either receiver cannot handle the speed/load or the network cannot handle it.

→ Congestion prevension policies

Open loop
(Prevent congestion before it happens)

- Retransmission policy
- window policy
- Ack policy
- discarding policy
- Admission policy.

Closed loop
(Remove congestion after it happened)

- back pres
- Chocke packet
- implicit signaling
- explict signaling.

→ open loop :- Prevent congestion before it happens

i) Retransmission :- It is the policy in which retramission of the packets are taken care. If the sender feels that a sent packet is lost or corrupted the packet need to retransmitted.

ii) Window Policy :- The type of window at the sender side may also affect the congestion

→ It's better to use selective repeat window should be adopted as it sends the specific packet that may have been lost.

iii) Discarding Policy :- A good discarding policy adopted by the routers is that the router may prevent congestion & at the same time discard the currupted packet.

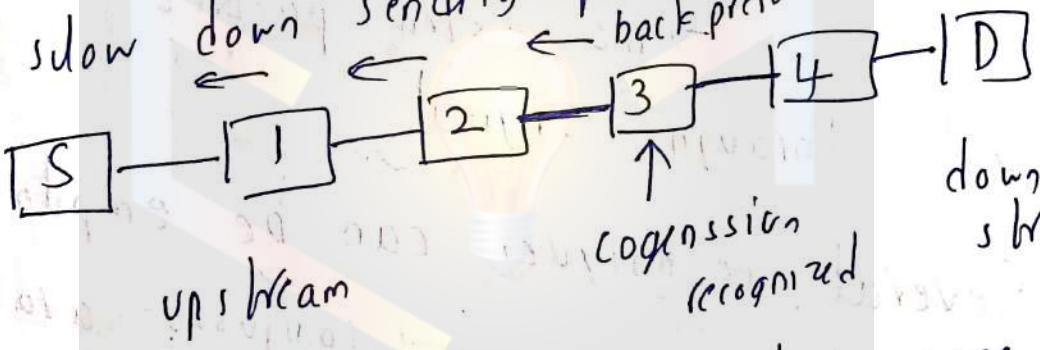
iv) Acknowledgement Policy :- Since receving acknowledgement also increases the changes of congesion. Hence receiver should send Acknowledgment for N packets other than 1 packet

v) Admission Policy :- any change in flow if it may cause congestion we should not do it.

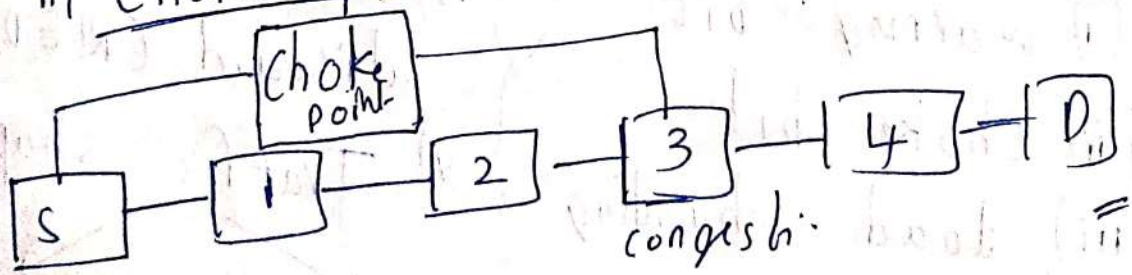
→ closed loop (try to remove congestion) after it happens

i) back pressure :-

When congestion occured at one node in a network it sends the info about congestion to the opposite side of congestion informing (in command words stop/slow down sending packets)



ii) Choice packet :- (A direct message to source).



→ Data flow

iii) implicit signaling :

→ Source guesses there is a congestion in network when it does not receive any ACK.

→ then source transmission slows down

iv) explicit signaling :

→ Sending direct signal to ~~son~~ source or destination.

→ forward or backward

→ no extra packet direct is sent through signal.

→ Several techniques can be employed these include.

(congestion detection)
- i) warning bit
- ii) Choke bit
- iii) load shadding

→ congestion avoidance.
- iv) Random early discard (RED)
- v) Traffic shapping
  - leaky bucket
  - token bucket.

I) warning bit :- (adjust transmit speed)

→ A special bit in the packet header is set by the router to warn the source when congesion is detected.

→ The bit is copied & piggy backed on the ACK & sent to the sender.

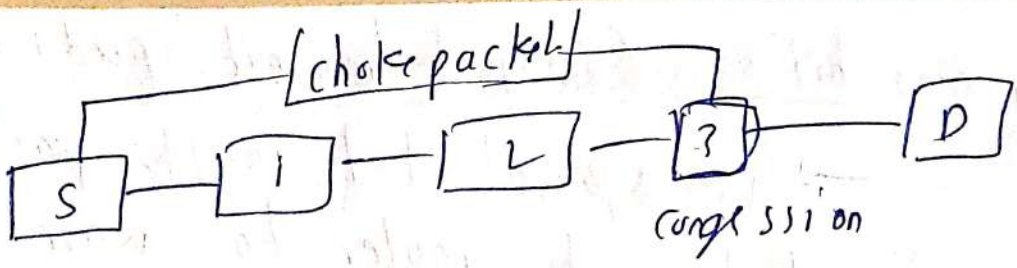
→ The sender monitors the number of ACK packets it receive with the warning bit set & adjust its transmission rate accordingly.

II) Choke packet:

→ A more direct way of telling the source to slow down

→ A coke packet is a control packet generated at a congested node & transmitted to restrict traffic flow.

→ The source, on receiving the choke packed must reduce its transmission rate by a certain percentage.



→ hop by hop choke packet:

→ over long distances or at high speeds choke packets are not very effective

→ A more efficient method is to send the choke packet node by node

III) load shedding:

→ when buffer becomes full routers simply discard packets (as no place to store)

→ Which packet is choosen to be the victim depends on the application & on the error strategy used in the data link layer.

eg:

→ For a file transfer we cannot discard older packet since this will cause a gap in received data.

→ For real time voice or video chat app, it is probably better to throw away old data & keep new packets

→ get the application to mark packets with discard priority.

IV) Random early Discard (RED)

→ This is a proactive approach in which the router discards one or more packets before the buffer becomes completely full.

→ Each time a packet arrives the RED algorithm computes the average queue length. it is average.

→ IF average is lower than ~~some~~ threshold (min & not exist).

→ If average is greater than some upper threshold conjusion is assumed to be serious & packet is discarded.

→ If average b/n 2 thresolds this might indicate the 1st stage of conjustion. The probability of conjusion is calculated.

V) Traffic shapping:

→ Another method of congestion control is to shape the traffic before it enters the network.

→ Traffic shapping controls the rate at which packets are sent (not just howmany). Used in ATM & many integrated service networks.

→ At connection setup time, the sender & carrier negosiate a traffic pattern (shape).

→ Two traffic shapping algorithm's are

i) leaky bucket

ii) token bucket.

i) leaky bucket :-

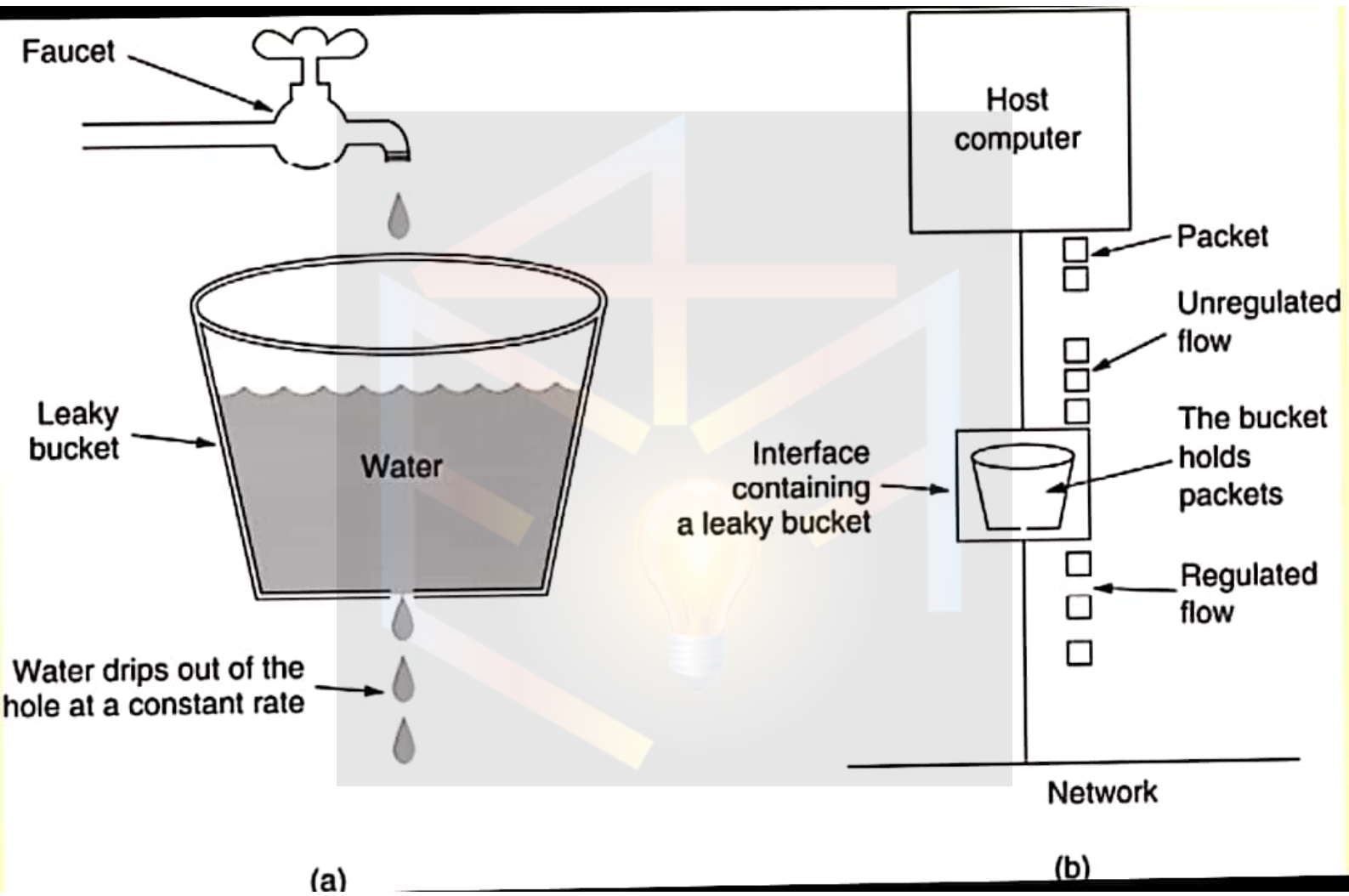
→ The leaky bucket algorithm used to control rate in a network.

→ It is implemented as a single server queue with constant service time

→ If the bucket (buffer) overflow, then packets are discarded

ing

a) leaky bucket with water | b) leaky bucket with packet



→ If average is greater than some upper the

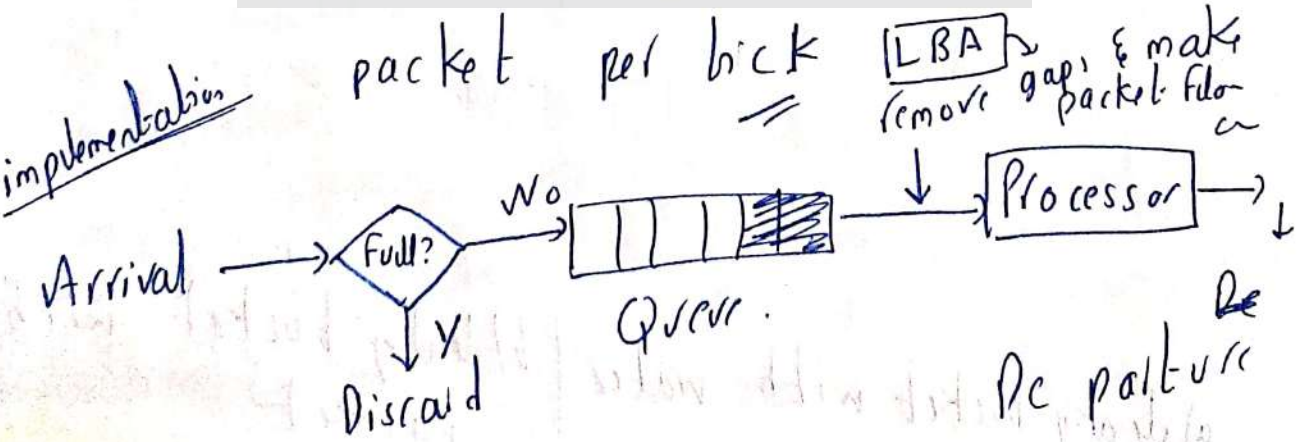
→ The leaky bucket enforce, a constant output rate (avg rate). regardless of random input rate (burst). → Hence uniform flow

only disadvantage → if bucket is full/overflow then packets are discarded.

it is assu → for one tick of time, one packet is sent

ex: if packet size is 1024 then 1 - 1024 or 2 - 512 or 4 - 256 or 8 - 128 & one packet per tick

implementation



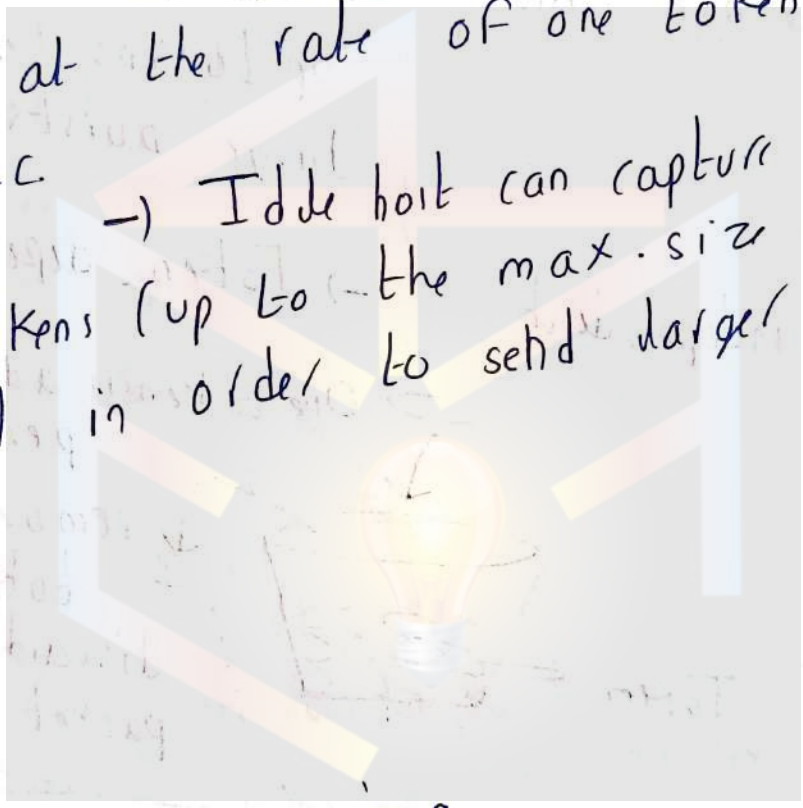
ii) Token bucket :

→ In contrast to leaky bucket the token Bucket algorithm, allows the output rate to vary, depending on the size of burst.

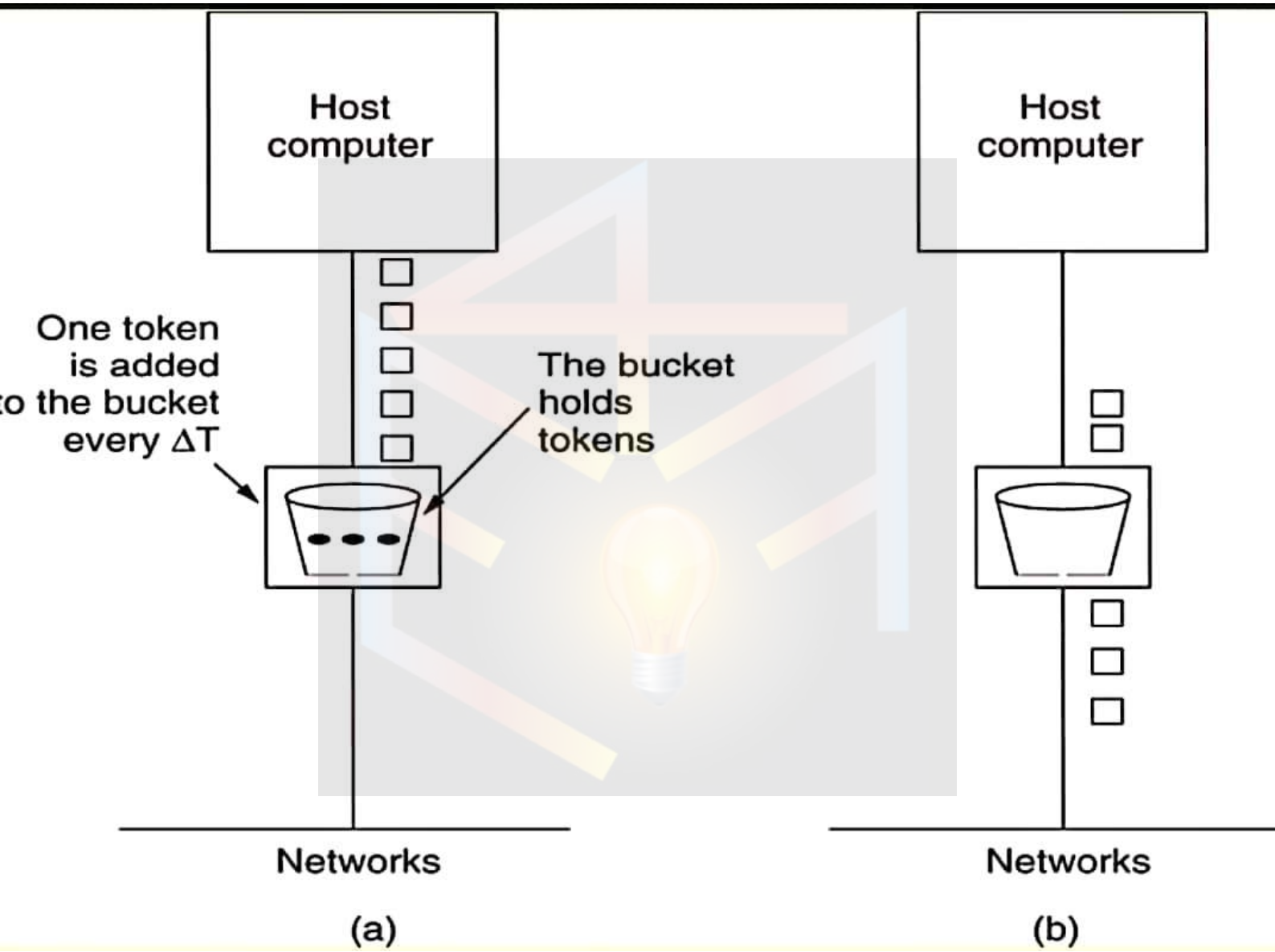
→ here the bucket holds tokens.

→ Tokens are generated by a clock at the rate of one token every Δt sec.

→ Idle host can capture & save up tokens (up to the max. size of the bucket) in order to send larger bursts later

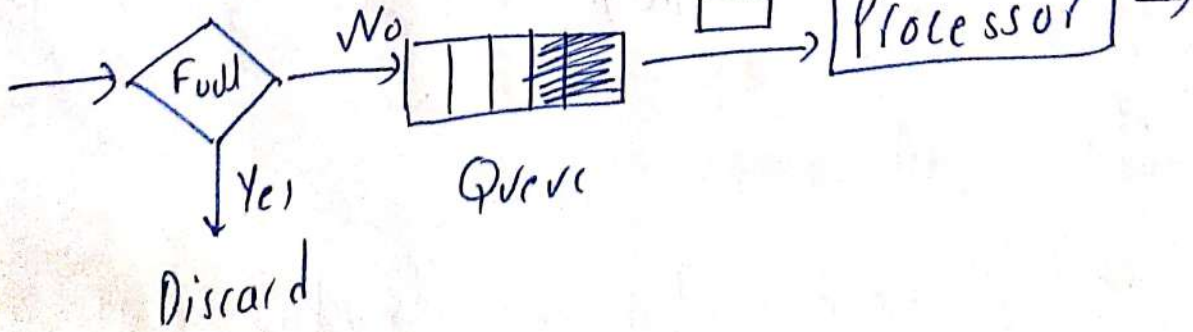


img.



Leaky Bucket	v/s	Token Bucket
→ LB discards packets		→ TB doesnot discard packets it discards tokens
→ LB sends packets at average rate		→ TB allows for large bursts to be sent.
→ LB does not allow saving		→ TB allows saving up tokens to send large bursts.
→ Token independent		→ Token depended.

Token Bucket flow

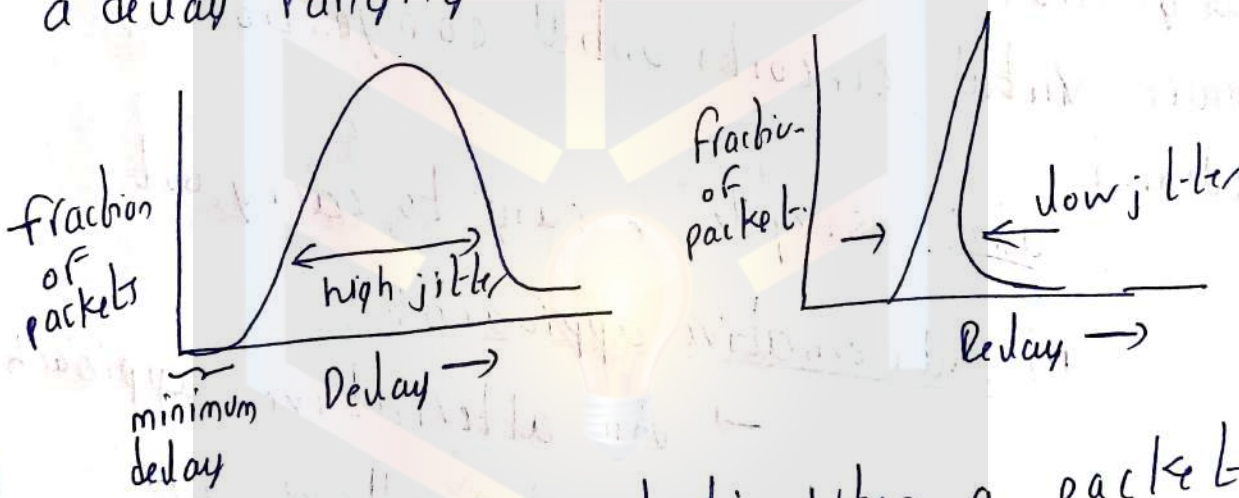


→ Jitter Control :-

→ Jitter may be defined as the variation in delay for the packets belonging to the same flow.

i.e the variation in the packet arrival time is called jitter.

→ prabically we can say that- 99.1. packets should be delivered with a delay ranging from 24.5 msec to 2.5 msec



→ Jitter control : When a packet arrives at a router, the router will check to see whether the packet is behind or a head & by what time.

If packet is ahead (early) of schedule it will be kept hold else if it's already late then will be sent ASAP.

→ Congestion Control in Virtual Circuit Subnets

i) Admission Control:

→ This technique is used to keep the congestion which has already begun.

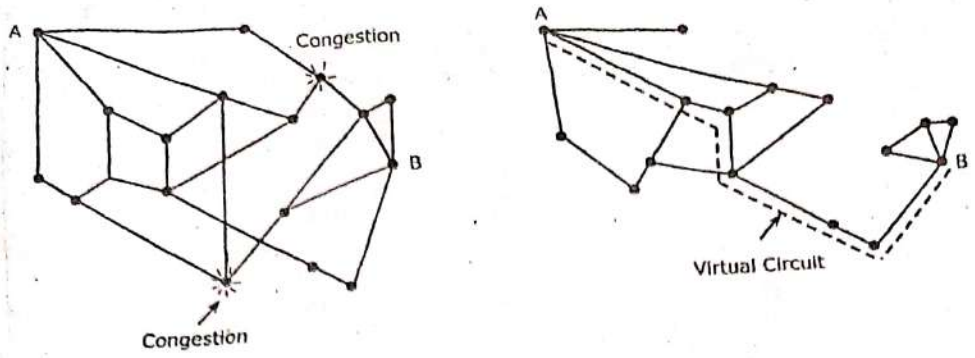
→ It state that once congestion is detected donot setup any more vitual circuits until congestion is cleared

adv: simple & easy to carry out.

ii) Alternative approach:

→ An alternative approach to admission control is to allow the vitual circuit to set up even when congestion has taken place.

→ But carefully route all the vitual circuits around the problem area.



(a) A Congested Subnet (b) A Redrawn Subnet that Eliminates the Congestion

→ Congestion Control in Datagram Subnets:

In datagram subnet for each output line & other resources the router maintains an estimate of it's utilization

new_Est = (P * old_Est) + (1 − P) I

P - constant

I - 1 or 0

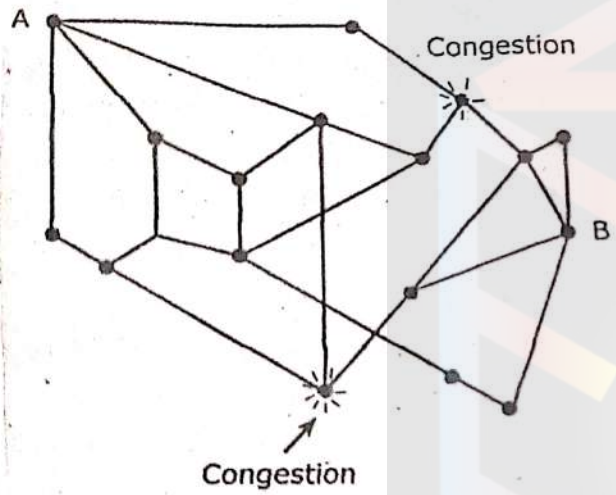
2 methods

i) warning bit

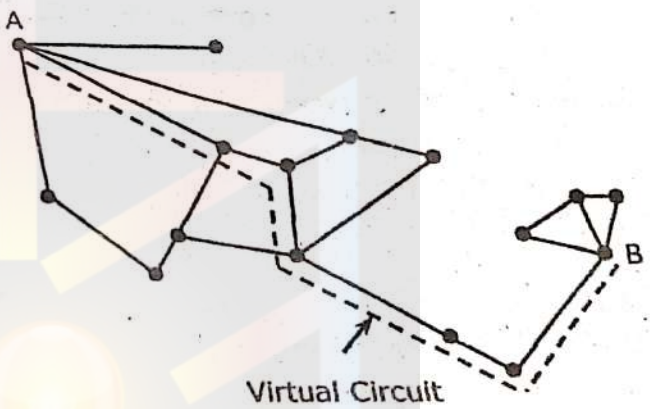
ii) choke packet

a) hop by hop choke

} Previous written same PDF.



(a) A Congested Subnet



(b) A Redrawn Subnet that Eliminates the Congestion

→ Quality of Service (QOS)

↳ we try to create an appropriate environment for traffic

Few characteristics

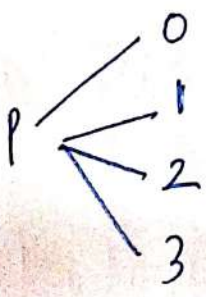
- reliability
- delay
- Jitter
- Bandwidth.

i) reliability :- lack of reliability means losing a packet or ack. (ideally high).
if it happens the packet is retransmitted which decreases reliability
ex:- email, file transfer

ii) delay :- Source to destination delay.
ex: audio conference

S → D
0 to 8
8 sec delay.

iii) Jitter :- variation in Delay



	Delay
received at	
4	= 4 - 0 = 4
6	= 1 - 6 = 5
8	= 2 - 8 = 6
10	= 3 - 10 = 7

} jitter

iv) Bandwidth :- Different Application require different bandwidth

email need less bandwidth

video conferencing need high bandwidth

(if asked for diag)

→ Technique for achieving Good QOS

i) Traffic shapping
ii) leaky bucket algorithm
iii) Token bucket algorithm

} already written in sam PDF.