CN - UNIT - I
NETWORK LAYER

By: SANDEEP UPADHYAY

Design Issues of Network Layer:

① Every layer needs a mechanism for identifying senders & receivers. If multiple receivers are there then some 'destination address' is needed & if multiple senders are there then some form of 'source address' mechanism is also needed.

② Another set of design decisions concern the rules for data transfer. Some channels allow only unidirectional flow of data and some need bidirectional. Sometimes, priority of data packet also come into the picture.

③ Error Control is also an issue b'coz communication circuits are not perfect. Many error detecting & error correcting codes are known but depending upon the agreement of sender & receiver, any one type of mechanism get used. In addition, the receiver must have some mechanism in order to reply about those data packets which have been received error free.

④ Not all channels preserve the order of messages sent on them. To deal with the issue of sequencing of packets, some provision of protocol should be there in order to reassemble the data packets sequentially.

⑤ There should be some mechanism to bring synchronization between the sender's sending speed & receiver's receiving speed. Means deployment of flow control mechanism is needed.

⑥ Another problem that must be solved at several levels is the inability of all processes to accept arbitrarily long messages.

⑦ When it's inconvenient or expensive to set up a separate connection for each pair of communicating processes, the underlying layer may decide to use the same connection for multiple, UNRELATED conversations. As long as this phenomena of MULTIPLEXING & DEMULTIPLEXING is used transparently.

(8) When there are multiple paths between source and destination, a route must be chosen. Sometimes this decision must be split over two or more layers. This phenomena of passing the data packet node by node is called routing.

Network Criteria

Network should meet certain Criteria like -

Performance: Performance Criteria has many factors but two are most important & that are-

Transit time - Amount of time required to travel the path from sending node device to receiving node device.

Response time - The time between the finish of Input & just start of Generation of output.

other factor of performance are no. of nodes in N/W, type of N/W medium, mode of transmission etc. etc.

Reliability - How long the network can work efficiently without causing / suffering from some major / minor kind of flaw/error.
* These days it's somewhat defined in the way that how long it will take to recover from failure, in many books. But Sandeep Sir says that this '*' definition, then is not Reliability instead it's recovery or recovery time :)

Security: Synonyms to 'Safety', the security of N/W means protecting the N/W or making the N/W safe from any unauthorized access or flaw.

Distributed System:- A system with one master as Controller & all other slaves as controlled bodies Plus the master Generates commands to all other slaves automatically driven by some software. This kind of structure is called Distributed System. Basically, a distributed system is a computer N/W with software sitting at it's head.

Protocol :- You've read this in previous class but to just make you remind - It's a set of rule deployed over the N/W to make the transmission efficiently.

Need of Computer N/W -

1. Sharing the resources such as printer, database etc.
2. To become in communication with geographically distributed computers.
3. To reduce the expensiveness.
4. For educational purposes.
5. To make the life better through N/W for eg. you must have heard about e-billing, e-banking, e-ticketing etc.

Advantages of Computer N/W

(a) Increased Speed :- N/W provides means of -
→ Sharing resources, hence no need to create the resources, instead just use the shared resources.
→ If the computer N/W wouldn't have been there, we would have to copy our documented mails in the floppy & tried for some courier service.

(b) Reduced cost :- ofcourse, by the use of N/Ws the cost of usability is reduced. for eg. it cost nothing to send a mail or video to others.

(c) Improved security :- When you are using some kind of N/W, ofcourse your data is secured by that N/W's security protocal through provision of login - Passwords or any other constrained accesses.

(d) Centralized access : Any kind of resource get shared by some system which is open to access by all other. This is called centralized accessibility.

(e) Flexible access :- You can sit anywhere, anytime on any networked system to stay tunned with the services of computer N/W.

Disadvantages of Computer N/W :- All points are xplained in class

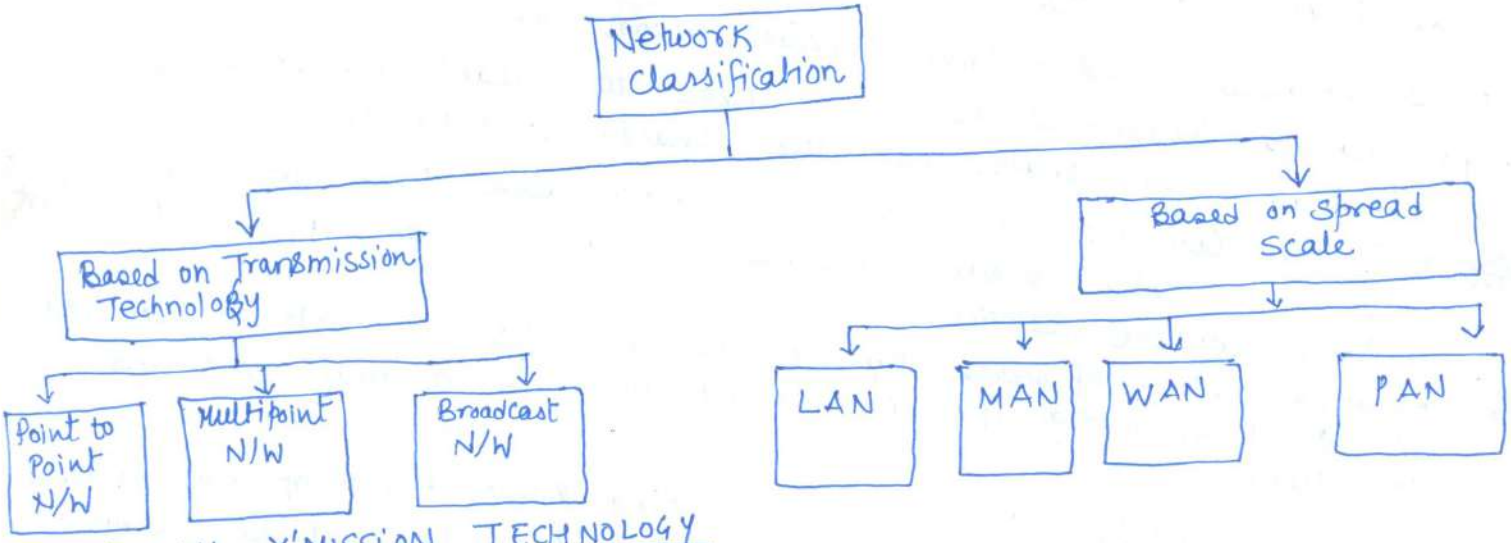
1. High cost of installation
2. failure of server
3. cable faults
4. Requires time for administration.

Components of Computer N/W :-

1. few nodes, infact two or more than two nodes means Computers.
2. Medium of N/W such as Cable / Wi fi etc.
3. A Network ~~fata~~ Interface card (NIC) on each Computer
4. Switches means routers
5. An OS supporting the Network.

Network Classification :-

Let's re-ignite the defn of Computer Network. A computer network is a web like structure or two or more devices connected through links. for visualization purposes you can imagine the link between two nodes as a line.



BASED ON X'MISSION TECHNOLOGY

(i) Point to Point Network :-

→ It has dedicated channel between two nodes.
→ Entire capacity of link is for transmission between two nodes.
→ The channel can be hard wired or softwired.
→ eg when you are controlling some TV channel with the help of remote control. It's P2P Comm^n.

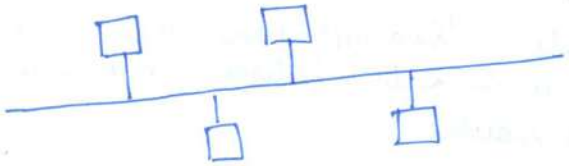
(ii) MULtipoint Networks :-

→ It has a channel but shared among more than two nodes
→ Two types of multipoint N/W –
- If many devices share the channel simultaneously, then it called 'spatially shared connection'.
- If many devices share the channel one by one means at different times then it's called 'Time shared connection'

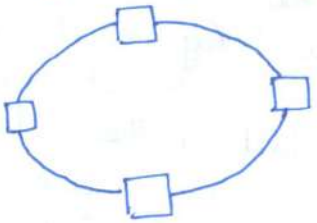
(iii) Broadcast N/W :-
- When in a N/W, a node becomes sender for all other nodes then that kind of N/W is called Broadcast N/W.
- When a msg. get broadcasted to specific set of nodes then this phenomena is called 'MULTICASTING'.

BASED ON SPREAD SCALE

(i) Local Area Network (LAN) :-
- LAN provides network connectivity physically confined to some office, factory or building etc.
- LAN are easy to design, test & maintain.
- Data rate in LAN ranges from 4 to 16 Mbps.
- LAN follows mainly two network topologies i.e. Bus & ring.



(Bus Topology)



(Ring Topology)

LAN Components :
(a) Workstation : Workstation refers to individual single computer.
(b) File server : File server is a computer that allows the sharing of data.
(c) Gateway : Assists transfer of data from one LAN to other LAN.
(d) Network Interfacing unit : Provides workstations, the interface with Computer N/W.
(e) LAN Cables or Commⁿ Channel : A medium / channel for transmission.

Advantages of LAN

1. High reliability to failure
2. It's possible to add new workstation easily.
3. The transmission of data rate is very high.
4. Sharing of peripheral devices like printer/scanner is possible.

Applications of LAN

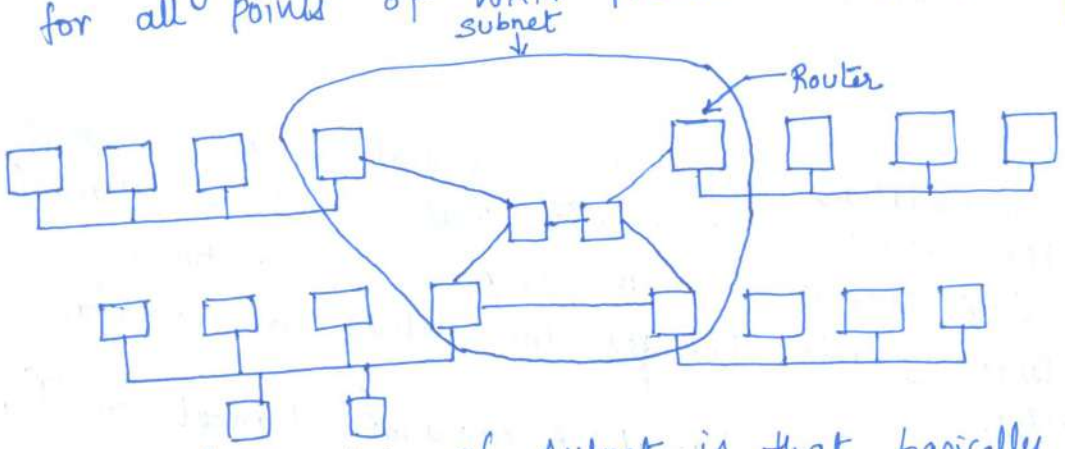
1. file transfer & file access
2. Remote access to database / Network
3. Fast document distribution
4. Personal Computing
5. Distributed Computing
6. Electronic messaging

(ii) Metropolitan Area Network (MAN) :-

- A MAN is basically bigger network than LAN as it's confined (~~to~~) to entire city, rather then just a building.
- It can be understood in a way such that many LANs are connected
- Cable TV network is the example of it.
- IEEE 802.6 standard says or given it a name Distributed Queue Dual Bus (DQDB).

(iii) Wide Area Network (WAN) :-

- WAN is confined to more big geographical area confined to country, continent and even world over. It contains collection of client computers running application programs. We will call these client computers as hosts. The hosts are connected by a subnet.
- The hosts are owned by customers & subnet is owned by telephone company or ISP (Internet service Provider)
- The job of subnet is to carry messages from host by host just as the telephone system carries words from speaker to listener.
- In most WAN, subnet consists - transmission line & switching elements. Transmission lines move bits between machines. Switching element means a router.
- for all points of WAN please see the following diagram -



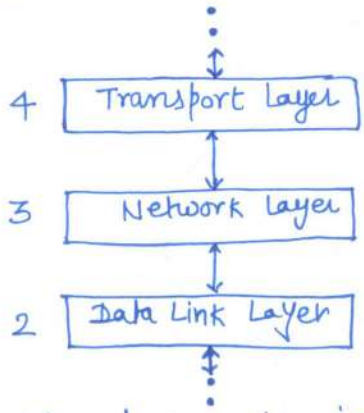
- The soul meaning of subnet is that basically it's a collection of routers & transmission lines.

COMPARISON B/W LAN - WAN - MAN

S.No.	Parameter	LAN	WAN	MAN
1	Ownership of N/W	Private	Private or Public	Private or Public
2.	Area Covered	Small	Very large (State/countries)	Moderate (city)
3.	Design & Maintenance	Easy	Not Easy	Not Easy
4.	Communication Medium	Coaxial cable	Satellite Links	Coaxial cables or optical fibre or wireless
5.	Principle	Broadcasting	Switching	Both
6.	Mode of Communication	Each node can transmit & receive	Each station can't transmit	Each station can transmit or receive
7.	Data rate	High	Low	Moderate
8.	Propagation Delay	Short	Long	Moderate

Re-Introduction to Network Layer:

- Network Layer is designed for delivery through several links from source to destination.
- Network Layer resides between data link layer & transport layer



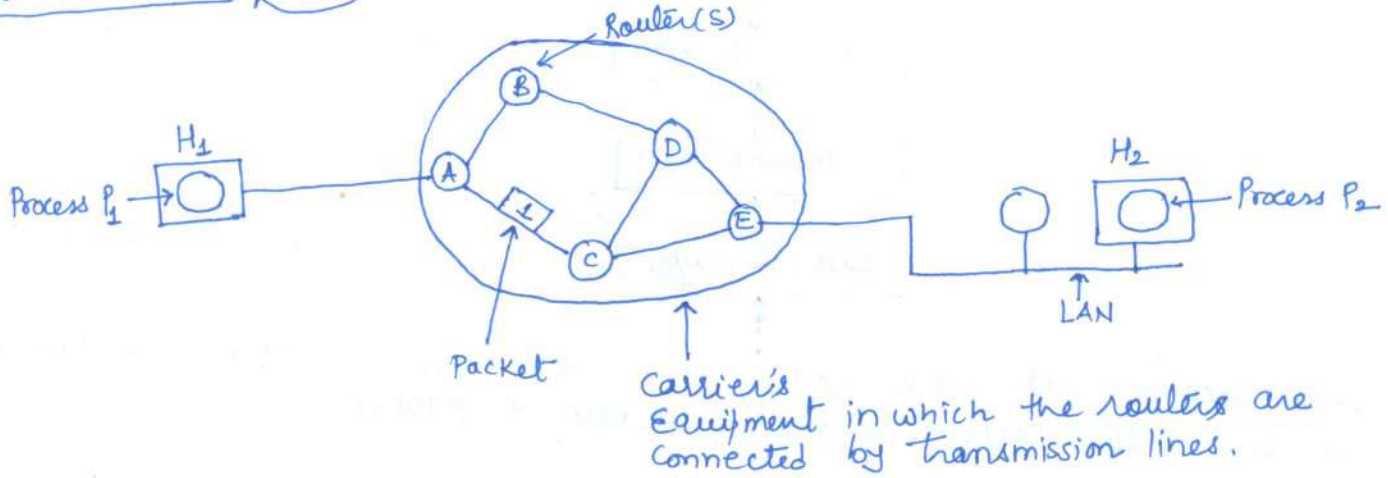
- Data received at N/W Layer is in the form of packets. A packet consists of two parts – A packet Header & packet body.

Network Layer Duties

1. Internetworking: It provides the logical connection between different types of networks.
2. Addressing: Each entity that needs to use the network must have it's identification on the basis of some address. Till now Computer network was following the addressing mechanism as IPV4 & IP V6.
3. Routing: In a network there are multiple number of switches from source to destination. ~~Or~~ Every packet moves switch by switch from source to destination. Routing algo can be Centralized or decentralized. In centralized routing the switching of packet depends or controlled by one centralized router, whereas in decentralized this doesn't happen.
4. Packetizing:- The N/W layer encapsulates the packets received from upper layer protocol & makes new packets. This is done by adding the headers to the ~~packet~~ received packet & this phenomena is called packetizing.
5. Fragmenting: The datagram at this step may not be ready to be passed to Data Link (DL) layer. The datagram prepared at the network layer may be larger than that limit. So the datagram needs to be fragmented to smaller units before being passed to DL layer

There are many other issues which are not of that much importance-
(a) address resolution (b) multicasting (c) Routing protocols.

Store & packet forward switching :-



* Explaination of store & forward Packet Switching has been given in the lecture.

Connection oriented & Connection less Service

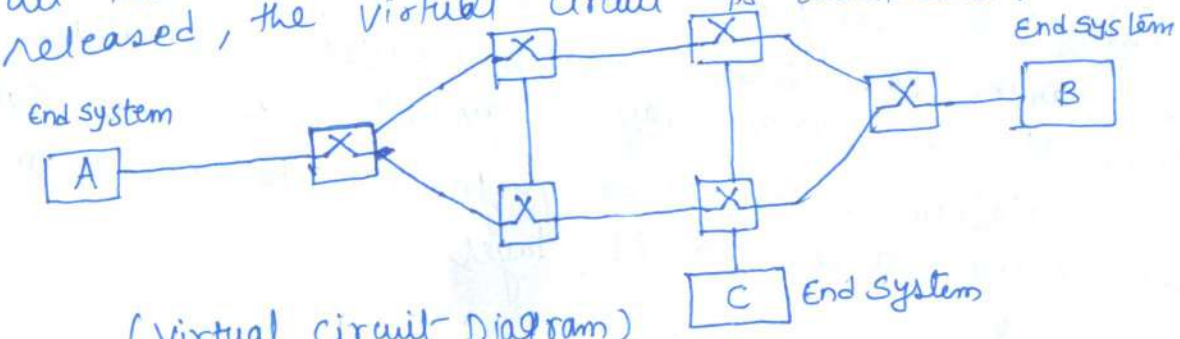
The network services can be Connectionless or Connection oriented.

1) Connection oriented Service:-
In Conection Oriented services (COS), there is a connection before the first data packet transfer. Connection setup needs some handshake mechanism. eg virtual circuit.

2) Connectionless service:-
In connectionless Service (CS), there is no need of connection setup. Every independent packet called as datagram moves towards source by it's own route.

Virtual Circuit

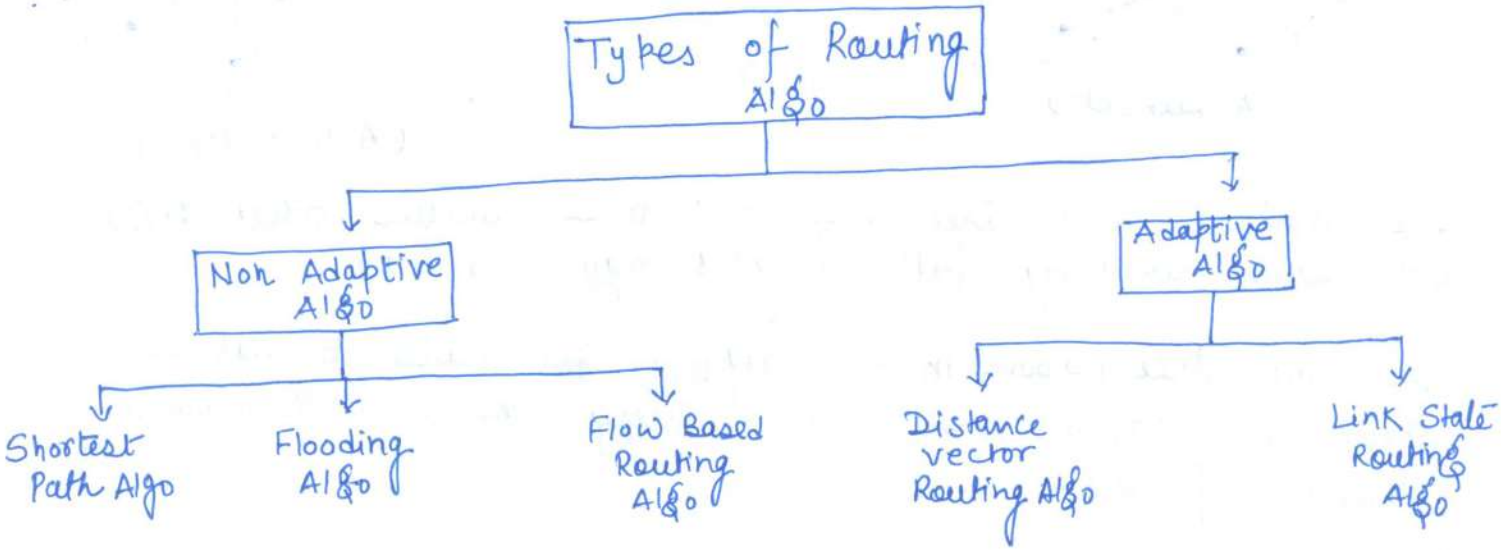
→ It follows the principle of only single route from source to destination, means when a connection is established, it is used for all the traffic flowing over the connection. When the connection is released, the virtual circuit is terminated.



(Virtual Circuit Diagram)

Routing Algorithm:-

Routing algorithm is a part of network layer. It's responsible for deciding the output line over which a packet is to be sent.



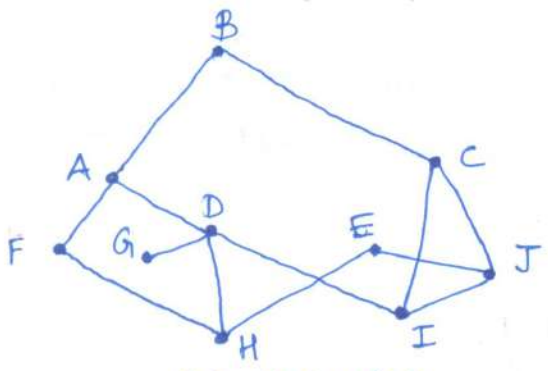
The optimality Principle

Before we enter into specific algos, it may be helpful to note that one can make a general statement about optimal routes without regard to network topologies or traffic. This phenomena is called Optimality Principle.

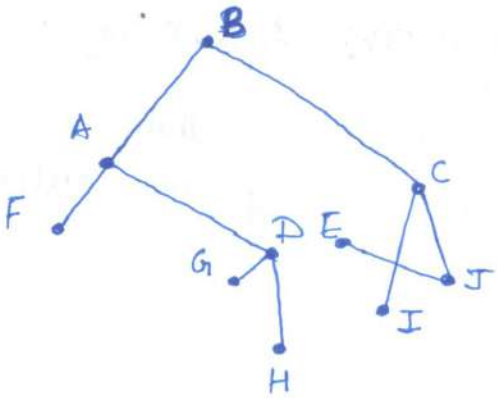
"It states that if J router is on the optimal path from router I to router K, then the optimal path from J to K also falls along the same route"

To check this, call the part from router I to router J as r_1 & rest as r_2. If a route better than r_2 existed from J to K, it could be concatenated with r_1 to improve route from I to K.

As a consequence, the set of optimal routes from all sources to a given distination form a tree rooted at the destination, such a tree is called sink tree.



(A subset)



(A sink tree)

→ Note that a sink tree need not to be unique. other trees with same weightage path lengths may also exists.

→ The sink tree (above, in the diagram) for router B has been shown. The paths from B to every router with minimum number of hops.

STATIC ALGORITHMS

3 types of static algorithms –

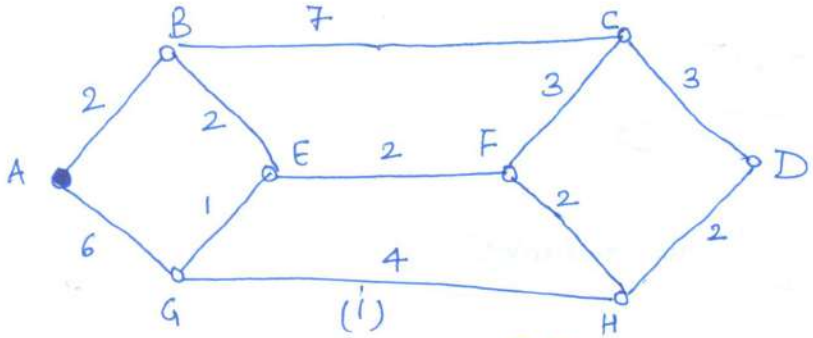
(i) Shortest path routing :- Here each node represents a router.

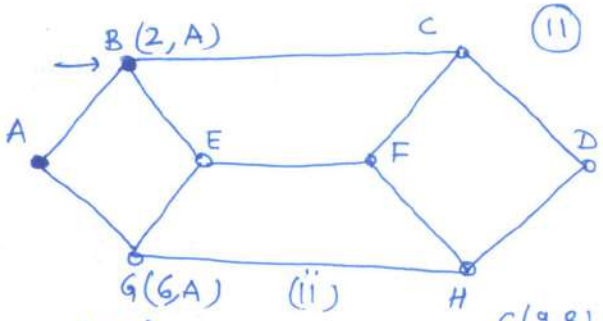
Steps :-

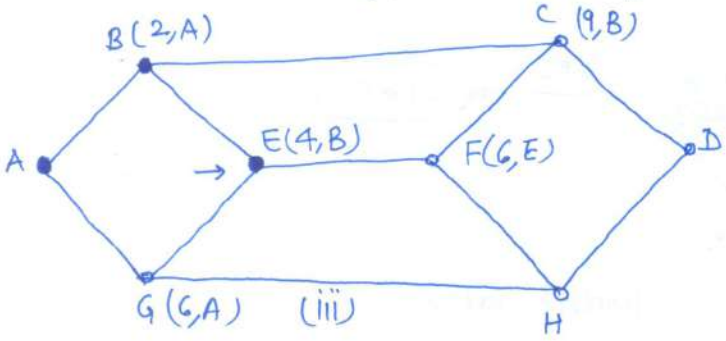
(a) Measurement of path :
(i) One way of measuring the path length is the no. of hops.
(ii) Another way is geographical distance in kms.

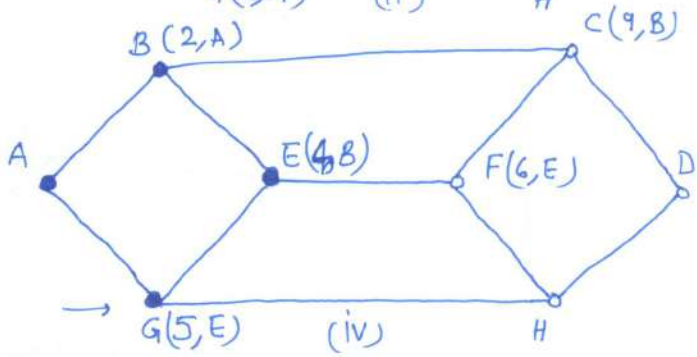
(b) Making distance on Arcs :
The arcs can be labelled as a function of distance or cost of communication.

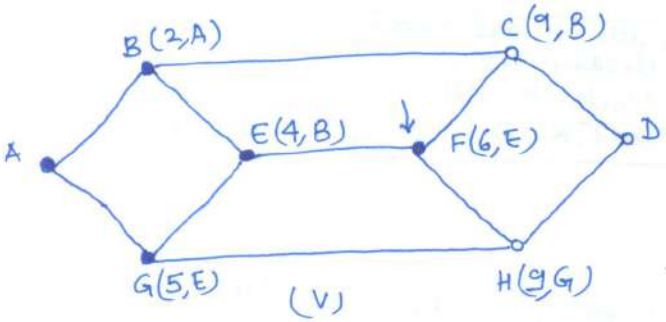
There are many algorithms for computing the shortest path between two nodes -

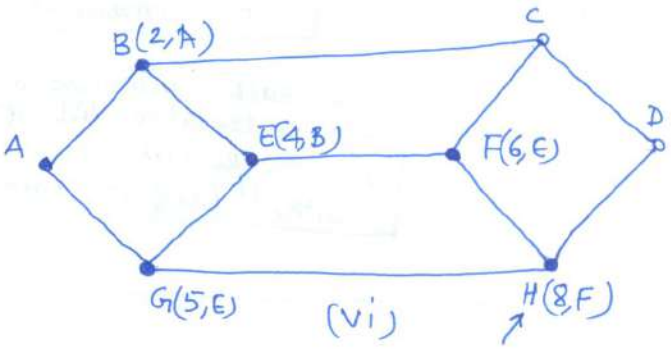












The above diagram has been explained in class.

Dijkstra's Algorithm :-

Step 1 :- Start from the desired node say P. Write P in the set P.

Step 2 :- for this node P, add each of its neighbour n to T set.

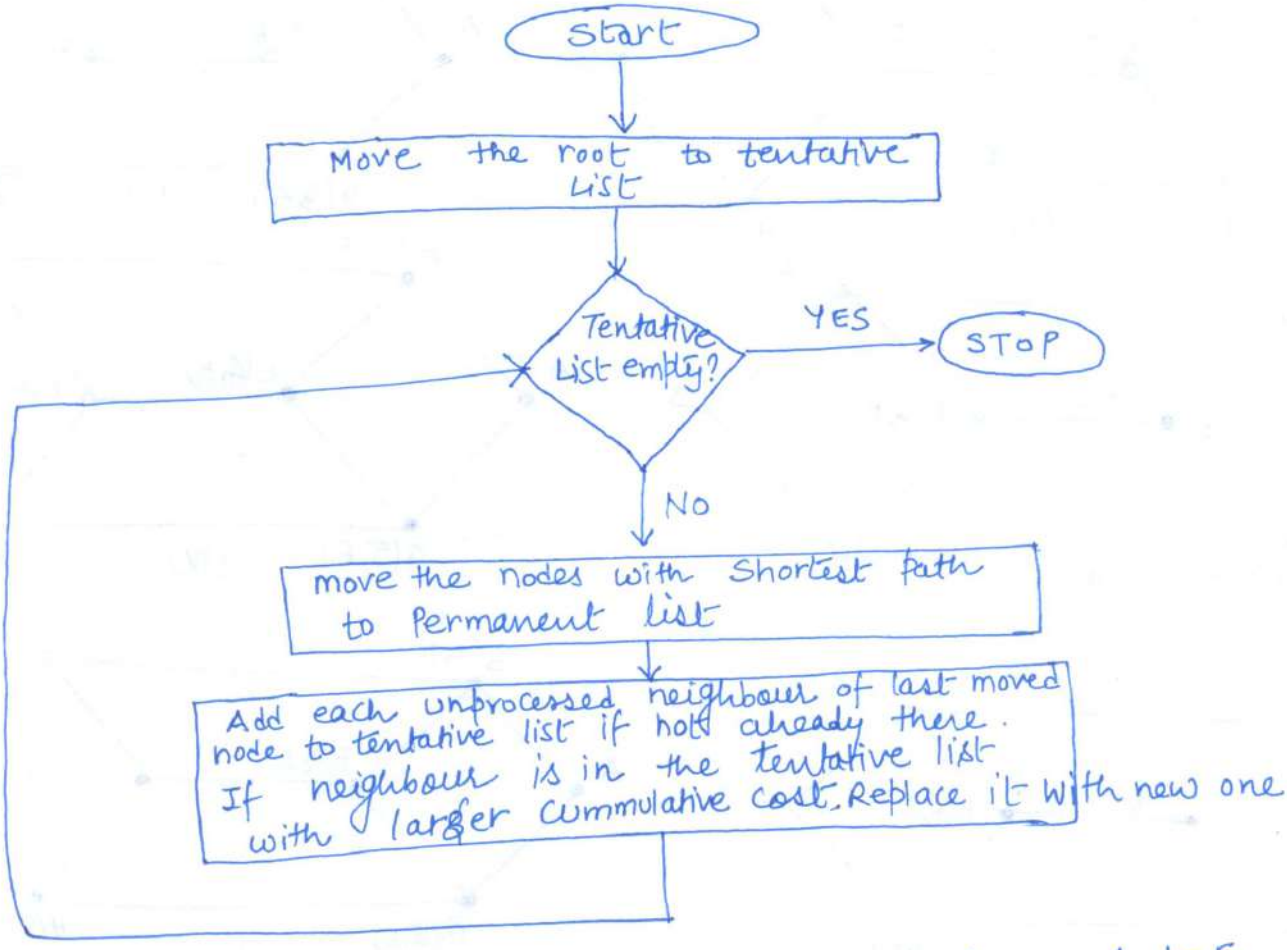
step-2 should get followed under following conditions -

(a) if the neighbouring node (say n) is not there in T then add it. ~~cannot~~

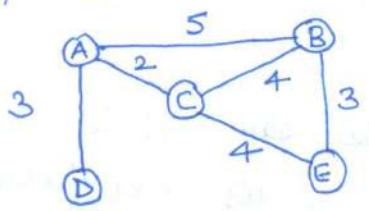
(b) if the node (say n) is already present in T & path to n through P has a lower cost, then remove the earlier instance of n and add the new instance annotated with the new cost.

P.T.O..

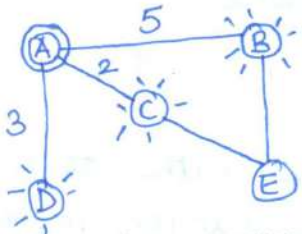
Flow chart for Dijkstra's Algo-



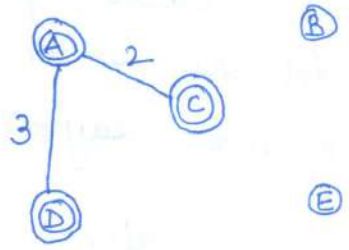
eg Initial N/W Topology given- We need to Go from A to E.



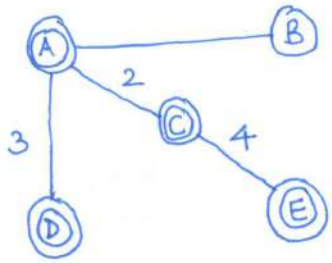
← start frm root A & move it to Permanent list



Starting frm A, ~~are~~ neighbour of A are B, C, D But Minimum is for C so Move C to Permanent list.



Now, neighbour of A & C are D, B, E; of which Min is D. Move ~~D~~ to Permanent list



Node	cost	Next Router
A	0	-
B	5	-
C	2	-
D	3	-
E	6	C

Flooding :-

This algorithms floods (flood means बाढ़) the entire N/W with Packets to be transmitted.

The main features of it are-

→ Every incoming packet is sent out on every outgoing Line except the one on which it has arrived.

→ one disadvantage of it is that, it generates a large no. of duplicate packets.

→ The duplicate packets need to be dumped by various techniques-

(a) Using a hop counter - Hop counter get decremented at each hop with the packets being discarded when the counter reaches zero. Initially the hop counter should be initialized to the length of the path from source to destination. If the sender doesn't know how long the path is, it can initialize the counter to the worst case, namely to the full diameter of subnet i.e. full width of subnet.

(b) To keep a track of those packets which are been flooded.

(c) selective flooding :- In this algorithm, the routers don't send every incoming packet out on every line, only on those lines that are going approximately in right direction.

Applications of Flooding :-

→ Flooding is used in military applications.

→ In distributed database applications, flooding get used.

Flow Based Routing :-

It's static algorithm which uses topology & load condition for deciding a route.

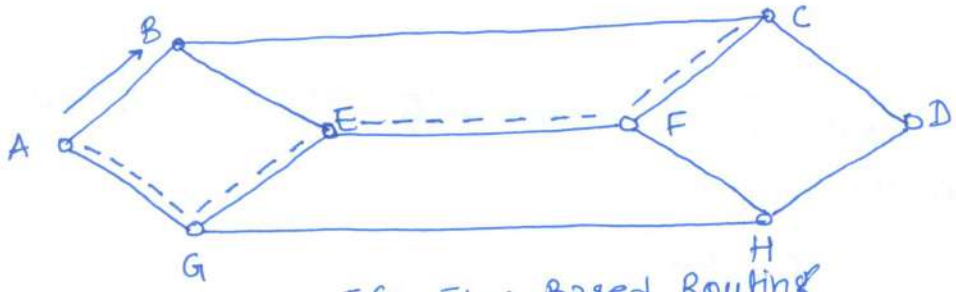


Fig: Flow Based Routing

→ In the above figure, there is always a huge traffic from A to B. Then the traffic from A to C should not be routed through B.

→ Instead Route it through AGEFC even through it is a longer path than ABC. This is called as Flow Based Routing.

→ The analyzation of data flow get done mathematically.

→ From the mean delays on all the lines it is possible to calculate the mean packet delay for the whole subnet.

→ To use the techniques of flow based routing, the following information should be known in advance -

(a) Subnet topology
(b) Traffic Matrix / traffic analysis

DYNAMIC ROUTING ALGORITHMS

Modern Computer N/Ws generally use dynamic routing algorithms rather than the static ones described above because static algorithms don't take the current network load into account.

Two dynamic routing algorithms are widely implemented -

(i) DISTANC VECTOR ROUTING ALGORITHM -

This algo operate by having each router maintain a table (i.e. a vector) giving the best known distance to each destination and which line to use to get there. These tables are updated by exchanging information with the neighbours.

The distance vector Routing algo also called as Bellman ford routing algorithm or ford fulkerson algorithm.

In distance vector Routing, each router maintains a routing table indexed by and containing one entry for each router in the subnet. This entry contains two parts: the preferred outgoing line to use for that destination and an estimate of the time or distance to that destination.

The router is assumed to know the 'distance' to each of its neighbours. If the metric is hops, the distance is just one hop. If the metric is queue length, the router simply examines each queue. If the metric is delay, the router can measure it directly with special ECHO packets that the receiver just timestamps & sends back as fast as it can.

This algo is interactive, asynchronous & distributed.

Asynchronous ~~Interactive~~, because it doesn't require all nodes to operate in lock step with each other.

Interactive because process continues on untill no more information is exchanged between neighbours.

Distributed because each node receives some information from one or more of its directly attached neighbour performs a calculation & then distributes the results of its calculation back to its neighbours.

In Distance Vector Routing (DVR), each router maintains a routing table. It contains one entry for each router in the subnet.

This entry has three parts -

1. The destination node
2. Cost i.e. the no. of hops a pkt must make to get there.
3. Next Router in the path to its way to destination.

Distance vector :

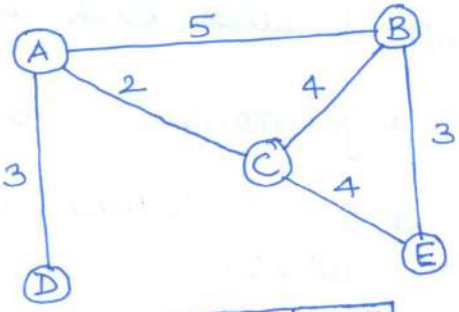
→ In distance vector routing, we assume that each router knows the identity of every other router in N/W but the shortest path is not known.

→ Distance vector (DV) is defined as the list of <destination, cost> tuples, one tuple per destination. Each router maintains a distance vector.

→ The cost should be minimum till destination has achieved.

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	3	-
B	∞	
C	∞	
D	0	-
E	∞	

D's Table

To	COST	NEXT
A	2	-
B	4	-
C	0	-
D	∞	-
E	4	-

C's Table

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

E's Table

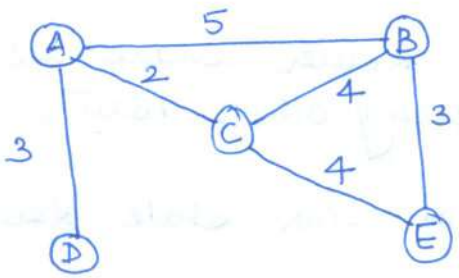
Updating the Routing tables –

Step 1 :- Distance from sending to destination node gets compared from all permutations like A to E via E is 2+4=6 & A to E via B is 5+3=8

Step 2 : Name of that node is set added to routing table's next column which is providing the optimized that is shortest path.

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	3	–
B	8	A
C	5	A
D	0	–
E	9	A

D's Table

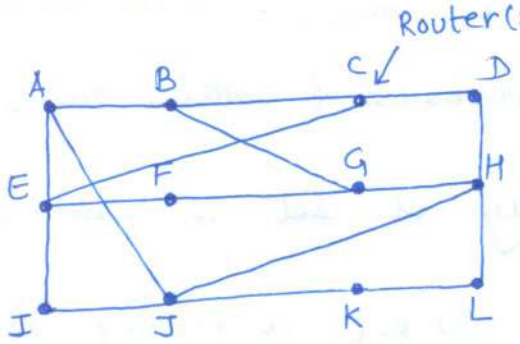
To	Cost	Next
A	2	–
B	4	–
C	0	–
D	5	A
E	4	–

C's Table

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

E's Table

Another Good eg. of Distance vector Algo take from A.S. Tanenbaum (P-358)



To	A	I	H	K	NEW ESTIMATED DELAY FROM I	LINE
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	–
K	24	22	22	0	6	K
L	29	33	9	9	15	K
	JA delay is 8	JI delay is 10	JH delay is 12	JK delay is 6	New routing table for J	

In the above figure J computes its new route to router G. It knows that it can get to A in 8 msec. & A claims to be able to get to G in 18 msec., so J knows it can count on a delay of 26 msec. to G if it forwards packets bound for G to A. Similarly, it computes the delay to G via I, H & K as 41 (31+10), 18 (6+12) and 37 (31+6) msec, respectively. The best of these values is 18, so it makes an entry in its routing table that the delay to G is 18 msec & that the route to use is via H.

LINK State Routing

In link state Routing, each Router share its knowledge to its neighbourhood with every other router in the internetwork

following are the features of Link State Routing-

(1) Knowledge about the neighbourhood: A router sends information about its neighbourhood ONLY.

(2) To all Routers: Each router send this information to every other router on the internetwork, not just to its neighbours. it does so by a process called flooding.

(3) Information sharing when there is a change: Each router sends out information about the neighbours when there is a change.

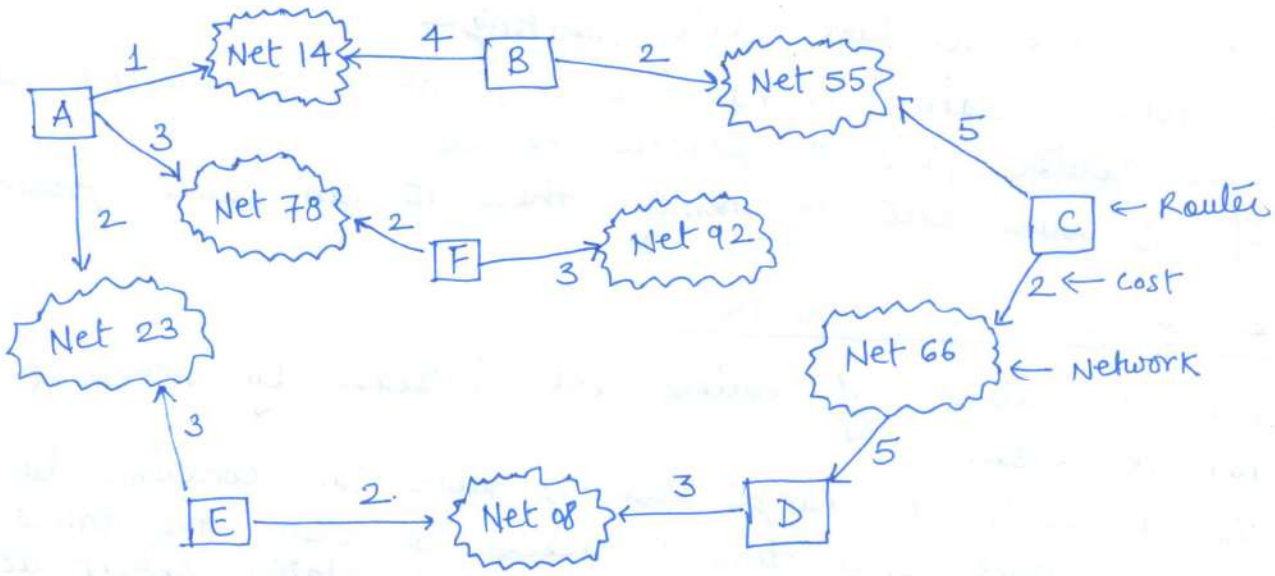
Five kind of operations for Router are there-

1. Each Router should discover its neighbours & obtain their network address.
2. Then it should measures the delay or cost to each of these neighbours.
3. It should construct a link state packet containing four fields: ID of advertisor, ID of destination network, cost & ID of neighbour router.

Advertisor	Network	Cost	Neighbour
—	—	—	—
—	—	—	—

Link State Packet

4. Send this packet to all other Routers.
5. Compute the shortest path to every other Router.



→ Every Router Receives every Link State Packet (LSP) & puts the information into a Link State database.

Advertisor	Network	Cost	Neighbour
A	14	1	B
A	78	3	F
A	23	2	E
B	14	4	A
B	55	2	C
C	55	5	B
C	66	2	D
D	66	5	C
D	08	3	E
E	23	3	A
E	08	2	D
F	78	2	A
F	92	3	—

1.13 COMPARISON OF LINK STATE ROUTING AND DISTANCE VECTOR ROUTING

S.No.	Distance Vector Routing	Link State Routing
1.	Each router maintains routing table indexed by and containing one entry for each router in the subnet.	It is the advanced version of distance vector routing.
2.	Sends message only to its directly connected neighbours.	Sends messages to every node in network.
3.	Sends larger updates to neighbours only.	Even smaller updates are sent to whole network.
4.	Uses Bellman Ford algorithm to calculate shortest path.	Uses Dijkstra's algorithm.
5.	Decentralized routing algorithm.	Centralized Global Routing algorithm.
6.	Simple to implement and support.	Expensive to Impliment.
7.	Bandwidth is less.	Wide Bandwidth is available.
8.	It converges slowly than link state.	It converges faster.

BY SANDEEP UPADHYAY

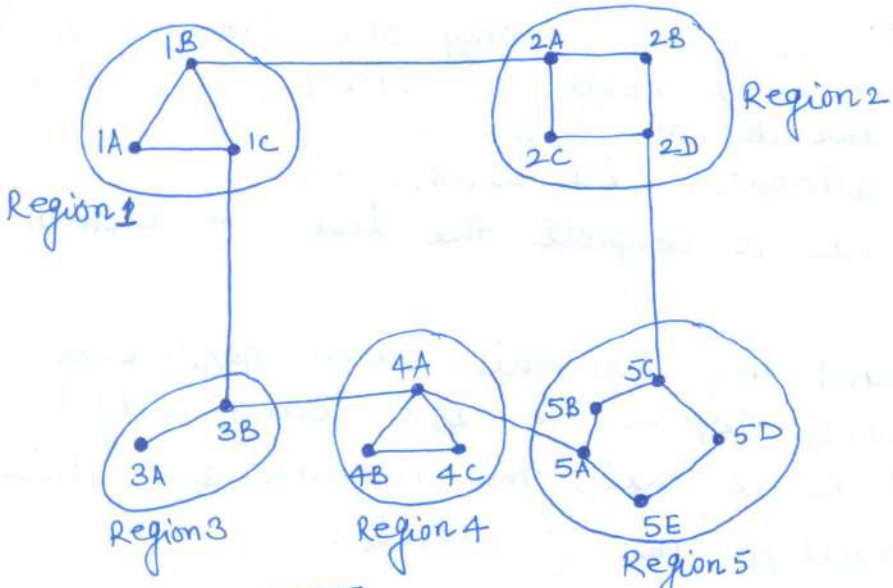
Some problems in Link state Routing –

- If router claims to have a line, which it doesn't have then router fails to forward packets.
- If it runs out of memory then it can cause problems.

HIERARCHICAL ROUTING

- Routing tables of routers get increase by increment in network size.
- As a result, a large routing table can consume large memory, more CPU time is needed to scan the tables & more bandwidth is required to send status report about the tables.
- Consequences of excessively large routing tables make it impossible for every router to have an entry for every other router.
- To tackle the above given situations hierarchial routing used similar to telephone networks.
- The hierarchy is structured as follows –

Level 1: Group of routers is called Region
Level 2: Group of Region is called cluster
Level 3: Group of clusters is called Zone
Level 4: Group of zones is called Groups



Dest.	LINE	HOP
1A	—	—
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

FULL Table for 1A

Summarised form of this Table through Hierachial Routing

Dest.	Line	Hop
1A	—	—
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

Hierachial Table for 1A

The reduced table size has a price tag attached to it. It comes at the expense of increased path length which is practically acceptable. It's a disadvantage of it.

If the subnet is of N routers, the optimum number of hierarchy levels is $\log_e N$ & it requires a total $e\log_e N$ entries per router table.

Broadcast Routing

In this, the host sends packets to more than one other hosts simultaneously. This phenomena is called Broadcasting. Various broadcasting methods are-

(a) Simple Broadcasting
(b) Flooding
(c) multidestination Routing
(d) Spanning tree
(e) Reverse path forwarding

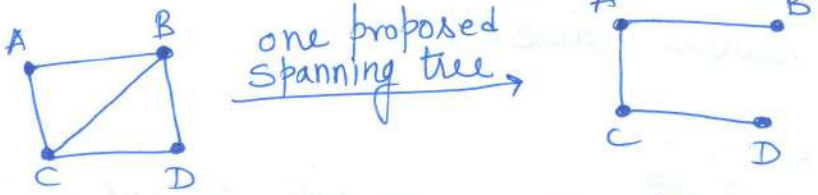
(a) Simple Broadcasting:- In this there is only one sending host & rest other are receiving hosts. The packet(s) get broadcasted simultaneously. The drawbacks of it are -
→ it may waste the allocated bandwidth.
→ The sending node has to complete the list of destination nodes.

(b) Flooding:- Flood means ~~ATG~~. In this every host send multiple no. of packet copies on it's every outgoing line. Consequence of it is that, the network get flooded by unnecessarily multiple no. of packets.

(c) Multidestination Routing:- In it when a packet arrives at any particular router, the router first checks all the destinations. Then it decides the set of output (O/P) lines on which it will send through.
The router then generates a new copy of the received packet for each output line to be used.

(d) Spanning tree:- Before reading it aapko maaloom hona chahiye ki what is spanning tree?- It's a tree made from any Graph in such a way that all nodes get traversed & no cycle should get built.

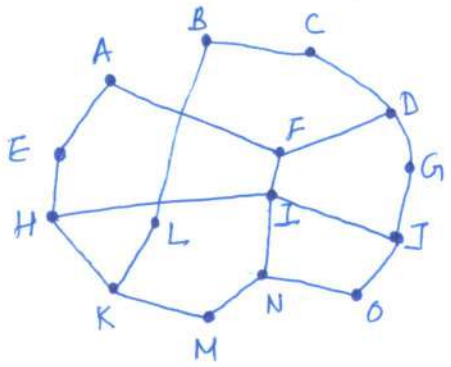
for eg.



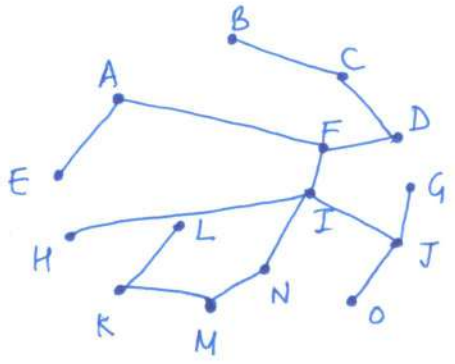
If the router knows which of its line belong to spanning tree, it can copy an incoming broadcasted packet onto all the spanning tree lines except the one it arrived upon. This method makes excellent use of Bandwidth, Generate optimum no. of packets to propagate. Drawback of it is that every router must have knowledge of some spanning tree.

(e) Reverse Path Forwarding:-

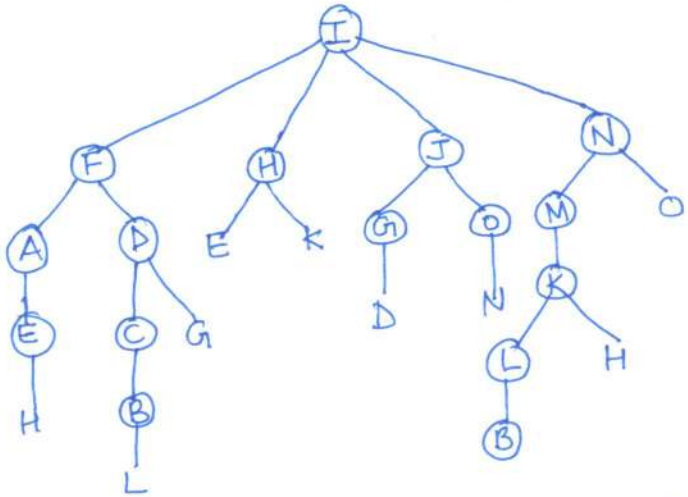
→ When a broadcast packet arrives at a router, the router checks to see if the packet arrived on the line that is normally used for sending packets to the source of the broadcast. If so, there is an excellent chance that the broadcast packet itself followed the best route from the router & is therefore the first copy to arrive at the router. This being the case, the router forwards copies of it onto all lines except the one it arrived on. If however, the broadcast packet arrived on a line other than the preferred one for reaching the source, the packet is discarded as a likely duplicate.



(A Subnet)



(A sink tree)



Tree Built By Reverse Path Fwding

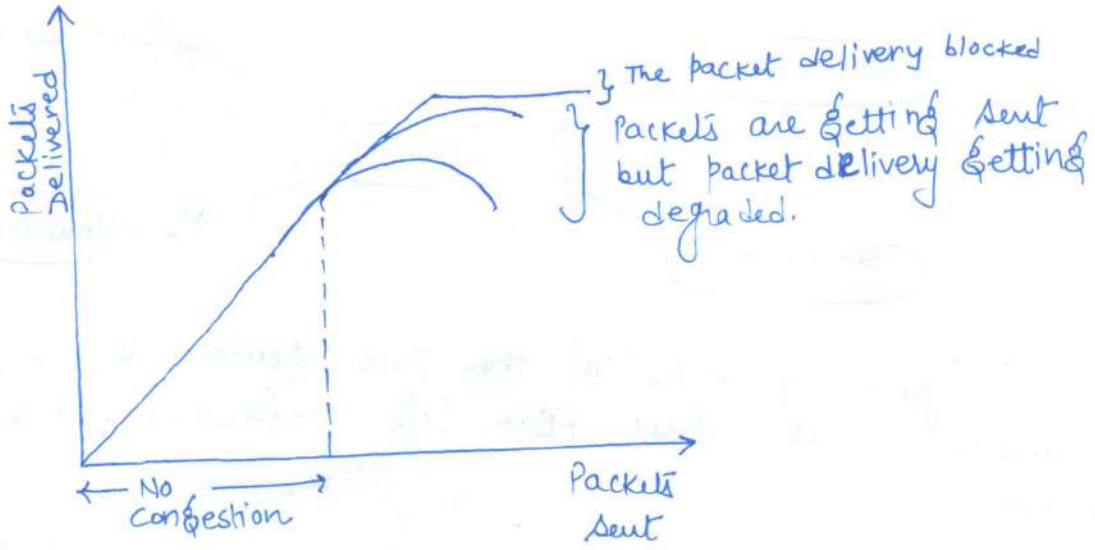
The advantage of Reverse path forwarding is that it is both reasonably efficient & easy to implement. It doesn't require routers to know about spanning trees. It doesn't require any special mechanism to stop the process, as flooding does.

Congestion Control:-

→ When too many packets are present in the subnet, the performance degrades. This situation of flow is called congestion.

→ Congestion occurs in the network when the load on the network i.e. the number of packets sent to the network is/are greater than the capacity of network.

→ The figure given below shows the congestion-

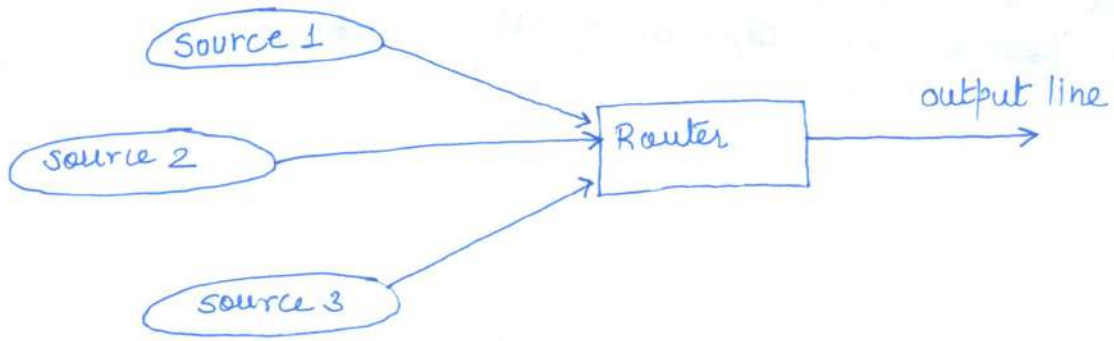


At high traffic when too many packets get sent, the delivery get blocked.

→ Some congestion control mechanism is must needed to control the congestion.

Causes of Congestion:-

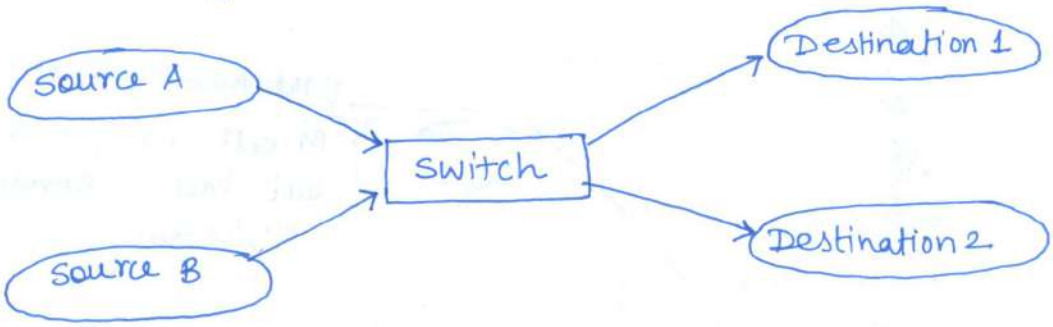
1) if a stream of packets starts coming on three or four input lines, which all need the same output line. Then a queue will build up. If the memory capacity is not sufficient to hold them, some of them will lost.



2) If a processor is slow, then the packets will wait, again making a situation of queue & packets may lost.

3) Low Bandwidth lines can also cause congestion.

4) Congestion is also caused by slow links. So High speed links are necessary. Sometimes even high speed links makes the situation ~~=~~ aggravate (और भी खराब) because higher speed links may make the Network (N/W) more unbalanced. For ~~the~~ this, see fig below -



in the figure if both of the two sources begin to send to destination at their peak rate, congestion will occur at the switch.

What is the difference between Congestion Ctrl & Flow Ctrl

Congestion Control	Flow Control
① Congestion control is concerned with making ~~the~~ sure that the N/W is able to carry the offered traffic.	① Flow control ensures the synchronization between the speed of sender & receiver
② Congestion control never provides feedback from receiver to sender.	② Flow control ensures feedback from receiver to sender.
③ Congestion control depends on behaviour of all hosts, routers & other factors which reduces the capacity of N/W	③ Flow control depends on behaviour of sender(s) & Receiver(s).

General principles of Congestion Control :-

The solution to congestion control problem can be divided into two groups :

(i) open loop solutions - These kind of solutions attempt to solve the problem by concept of good design. The open loop congestion control is focused on prevention of congestion. It decides, when to accept the new packet, when to discard them, which packets are to be discarded and makes the scheduling decisions at various steps.

(ii) closed loop solutions - These are based on concept of feedback loop. The closed loop solution is focused on removing congestion. It uses feedback mechanism based on three steps -

(a) Detect the congestion & locate it
(b) Transfer the information to the places where actions can be taken.
(c) Adjust the system operations to remove congestion.

Comparison of open Loop & Closed Loop

open Loop	Closed Loop
1. open Loop uses no feedback mechanism.	1. closed loop uses feedback received from the Network.
2. open loop principle is fast.	2. closed loop principle is too slow in today's high speed large N/W

Congestion Prevention Policies :-

Policies are designed to minimize congestion in the first place, rather than letting it happen & reacting after the fact.
Policies are achieved at various layers -

Policies at Data Layer :-

(i) Retransmission Policy :- It's concerned with how fast a sender times out and what it do/transmits upon time out.

(ii) out of order Policy :- If receiver regularly discard all out of order packets, these packets will have to be transmitted again later which creates an extra load & results in congestion.

(iii) Acknowledgement policy :- If each packet is acknowledged immediately, the acknowledgement packets generates extra packets/overhead packets if we concern about traffic. If acknowledgement are saved upto delayed propagation. A tight flow control scheme reduces the data rate & thus helps fight congestion.

Policies at Network Layer :-

(i) Virtual ckt. versus datagram :- At N/W layer, the choice b/w using virtual ckts and using datagrams affects congestion.

(ii) Packet queuing & service policy :- Packet queuing & service policy relates to whether routers have one queue per input line and/or output line or not. It also relates to the order in which packets are processed.

(iii) Packet discard Policy :- Discard policy is the rule telling which packet is dropped when there is no space. A good policy can prevent from congestion & bad can make it worse.

(iv) Routing algorithm :- A good policy can help from congestion by spreading the traffic over all the lines.

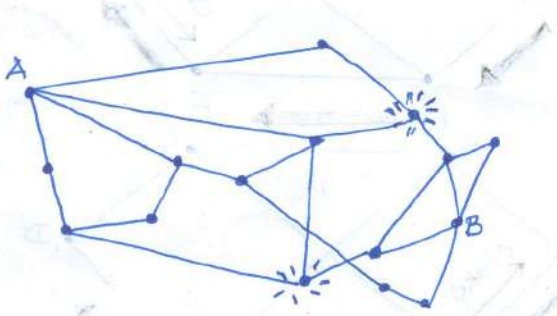
(v) Packet Lifeline management:- It tells how long a packet may ~~live~~ before being discarded. this time should be of appropriate value so that Congestion can be avoided.

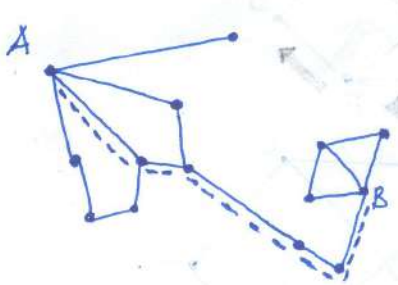
Policies of Transport Layer:-
The policies are similar to Data Link Layer, in addition determining the time out interval is harder because the transit time accross the N/W is less predictable than the transit time over a wire between two routers. If the timeout interval is too short, extra packets will get sent ~~unnecessirily~~ unnecessarily. If the timeout interval is too long, the chances of late response are more. so it's better to make the timeout interval of moderate in nature.

Congestion Control in Virtual Circuit Subnets

To dynamically control the congestion in virtual circuit, the admission control Principle get used-

Admission Control Principle:- As per this, once the congestion has been signaled, no more virtual circuits get setup until the problem get partially or totally diminish. It's easy to carryout this Control.





Suppose that a host attached to router A wants to setup a connection to a host attached to router B. Normally, this connection would pass through one of the congested routers (represented by ⁘ in above given diagram). To avoid the congestion, we omit those routers and lines passing through those routers. The dashed line shows a possible ~~true~~ route for the virtual circuit that avoids the congested routers.

Another strategy is to negotiate the agreement while setting up the virtual circuit. This agreement specifies the volume & shape of traffic, quality of service required & other parameters. To keep its part of agreement the subnet will typically reserve resources along the path when the circuit is set up. These resources can include table & buffer space in the routers & bandwidth on the lines. In this way, congestion is unlikely to occur on the new virtual circuits because all the necessary resources are guaranteed to be available. A disadvantage of doing it all the time is that it tends to waste resources.

Congestion Control in Datagram Subnets :-

A specialised packet that is used for flow control along a network. A router detects congestion by measuring the percentage of buffers in use, line utilization & average queue lengths. When it detects congestion, it sends choke packets across the network to all the data sources with the congestion. The sources respond by reducing the amount of data they are sending.

Hope by Hope choke Packets :-

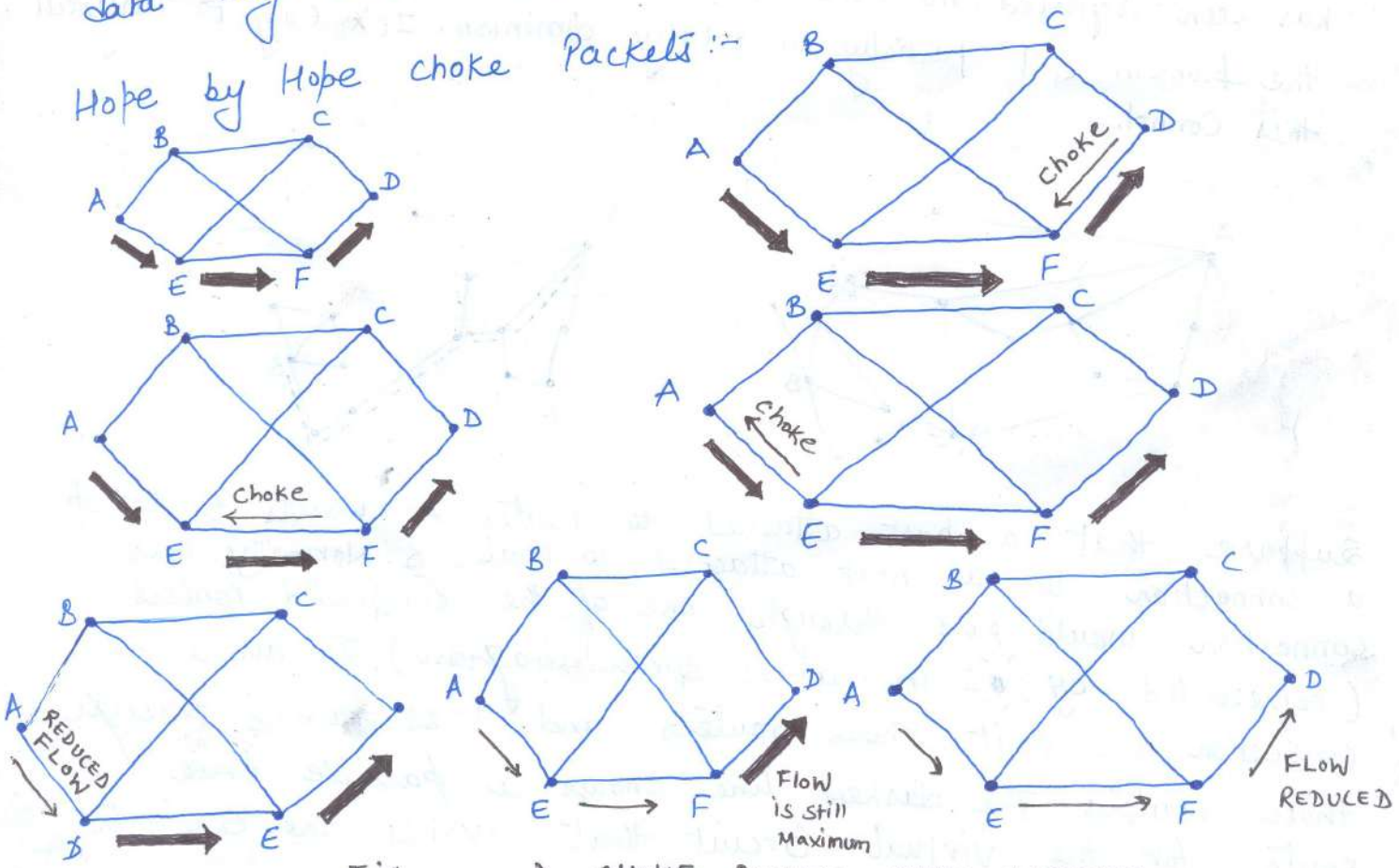


FIG- A CHOKE PACKET THAT AFFECTS ONLY THE SOURCE

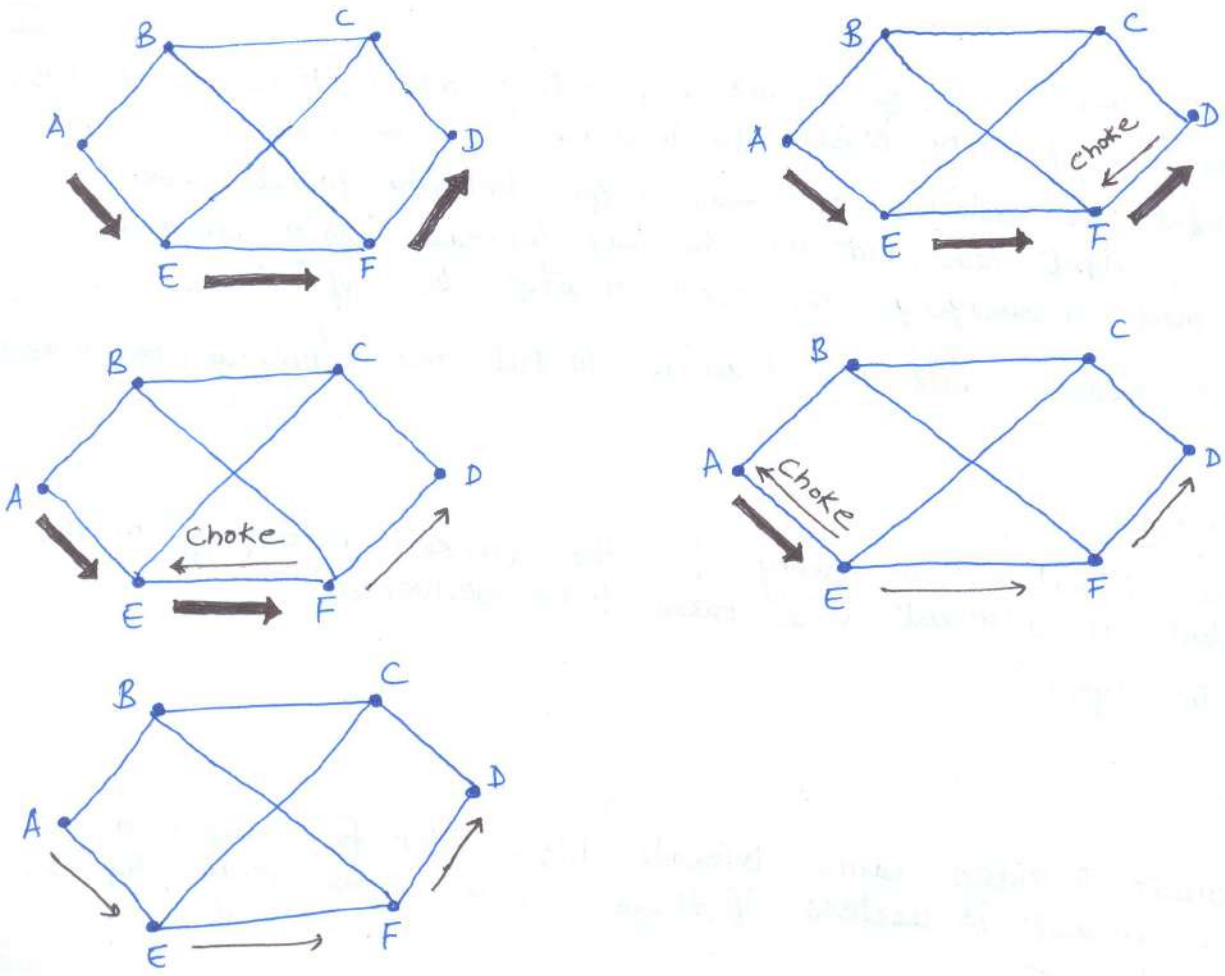


FIG: A CHOKE PACKET THAT AFFECTS EACH HOP IT PASSES THROUGH

LOAD SHEDDING

It's a technique used in heavy congestion situations, called as load shedding. In load shedding when the routers are heavily loaded by packets that they can't handle, they should simply throw the packets away.

→ A router which is flooded with packets due to congestion can drop any packet at random. Which packet to discard may depend on the application running.

→ An old packet is worth more than a new one because dropping packets 5 and keeping packet 6 will cause a gap at the receiver, which results in retransmission of packets from 5 to 6. This policy is called wine.

→ In contrast, for multimedia, a new packet is more important than old one. This policy is called MILK.

→ To implement an intelligent discard policy, applications must mark their packets in priority order to indicate the importance.

→ Senders might be allowed to send high priority packets under conditions of light load, but as the load increased they would be discarded thus encouraging the users to stop sending them.

→ One or more header bits are required to put the priority. ~~for making the~~

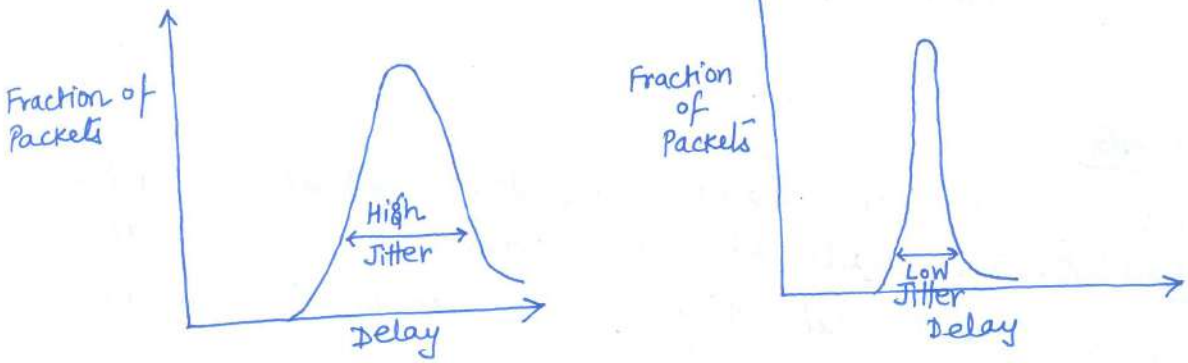
JITTER CONTROL

Jitter is the variation in delay for the packets belonging to the same flow but at different time taken to be delivered.

Jitter is of two types –

1. High Jitter
2. Low Jitter

Real time audio & video cannot tolerate high jitter. for example, a real time video broadcast is useless if there is a 2 ms delay for the first & second packets.



Jitter Control :-

→ When a packet arrives at a router, the router checks to see how much the packet is varying from it's schedule.

→ This information is stored in each packet & updated at each hop.

→ If the packet is ahead of it's schedule, it will be held by the router for a slightly longer time & if the packets are behind the schedule, then the router will try to send it out as quickly as possible. By this the packets get their synchronized & normalized speed.

→ In some applications, such as video on demand, jitter can be eliminated by buffering at the receiver & then fetching data for display from the buffer instead of from the network.

Difference between End to End delay & Jitter :-

End to End delay is the time required for the signal to travel from transmitter to receiver. This delay is time consumed in buffering, queuing, switching & routing. This delay remains same for all types of packets.

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

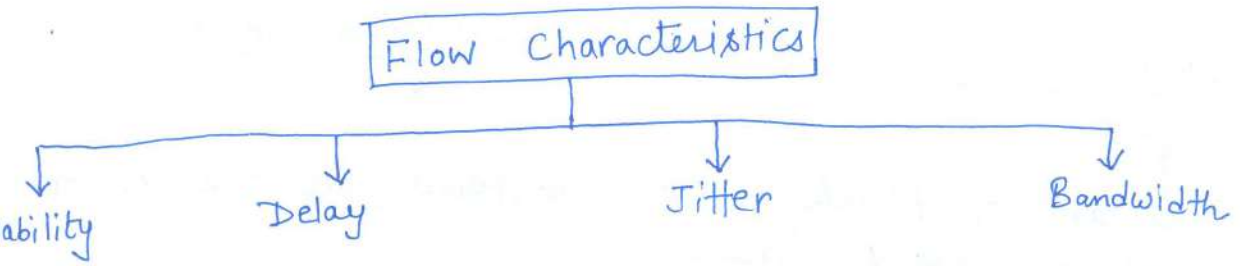
Quality of Service (QoS)

'Quality' means providing/delivering the solutions as per functional & non-functional requirements by following certain standards. Advancements in networks brought the needs of 'quality' word in Network.

Some basic requirements as per the quality are needed always -

→ A stream of Packets with consistant flow is needed.

→ If a connection oriented network, all the packets belonging to a flow, follow the same route & a different route in connectionless network. There are certain characteristics of flow -



Reliability:- It ensures that for how long the bits can get delivered Correctly or successfully. Lack of Reliability brings the consequences of retransmission.

eg email is more reliable mode of communication than telephone communication.

Delay:- Depending upon the type of application, a delay can be tolerable (no matter - untolerable or partially tolerable or fully tolerable but still, everything depends upon type of application). Delay should be uniform atleast.

eg email is less delay sensitive, whereas video conferencing is strictly delay sensitive.

Jitter:-

Jitter is the variation in delay for packets belonging to the same flow. Real time applications such as audio or video cannot tolerate high jitter.

eg There should not be a delay more than 2ms in real time video broadcast.

The transport layer at the destination waits untill all packets arrive before delivery to the application layer.

Bandwidth:-

It's but obvious that different applications need different bandwidth. constant bit rate is an attempt to provide a uniform bandwidth.

Techniques for achieving Good Quality of Service

i) Buffering:-

→ The stream of packets can be buffered on the receiving side before being processed.

→ Buffering doesn't affect reliability or bandwidth. It just increases delay & lowers the jitter. See diagram in book.

(ii) Traffic shaping:- if the packets are sent enormously & irregularly sent then this may cause congestion. Traffic shaping is a technique which smoothens the traffic rate on server side i.e. sender's side rather than client's side or receiver's side.

→ In a connexn oriented network, when a connection is set up, an agreement gets done on a certain traffic pattern or structure. This agreement process is called service Level Agreement (SLA). Traffic shapping reduces the congestion & provides good Quality of Service.

→ After defining the agreement, also called descriptor; traffic flow still goes into regular monitoring. This is called Traffic Policing. If a packet stream voilates the descriptor, it must ~~obey~~ give some penalty like -

- dropping the packets which voilated rules
- Turn them into of low priority

Two traffic shapping Algorithms are -

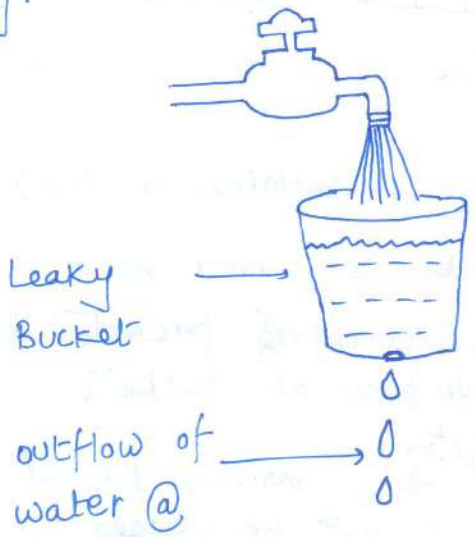
(a) Leaky Bucket (b) Token Bucket

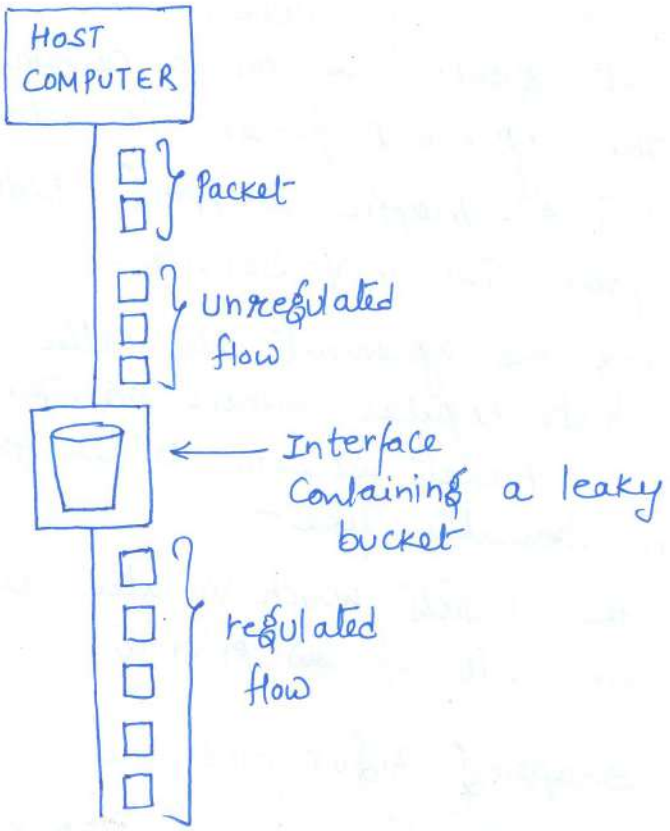
Leaky Bucket

→ Leaky bucket algo provides a solution to control congestion.

→ Leaky bucket has a small hole at it's bottom. As a consequence, the entry of water can be at enormous rate but the outflow of water is maintained at constant rate due to small hole.

→ Once the bucket is full, the additional water gets thrown away.

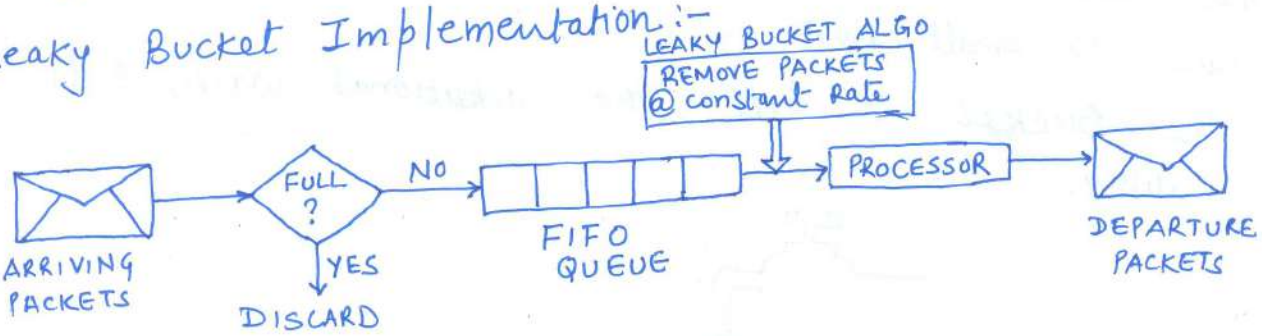




→ Every host in network is having a buffer with finite queue length.

→ A variant of leaky bucket is token bucket. The bucket is filled with tokens at a certain rate. A packet must grab & destroy a token to leave the bucket. Packets never gets lost, they just have to wait for an available token.

Leaky Bucket Implementation :-



<The diagram is Explained in class>

The implementation is under two conditions -

(a) Fixed size packets :- If the arriving packets are of fixed size, then fixed sized - Fixed number of packets will get removed from queue & hence propagated.

(b) Variable size packets :- If the arriving packets are of different size, the fixed o/p rate will not be based on number of departing packets.

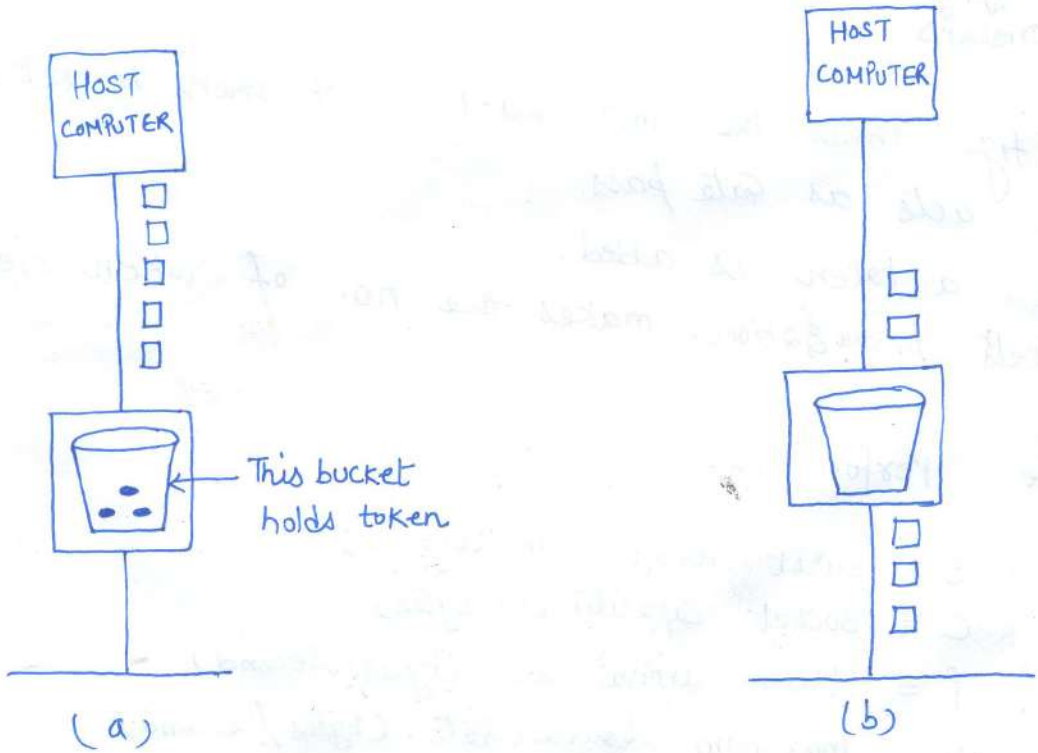
The algorithm in case of variable packet length will be as follows -

1. Initialize the counter to n at certain mark of clock.
2. In n > packet size then send the packet & decrement the counter by the packet size.
3. Repeat step 2 until n becomes smaller than the packet size.
4. Reset the counter & go back to step-1.

Token Bucket Algo

→ It's similar to leaky bucket algo but with some limitations.

→ Token bucket algo is useful for large burst of traffic.



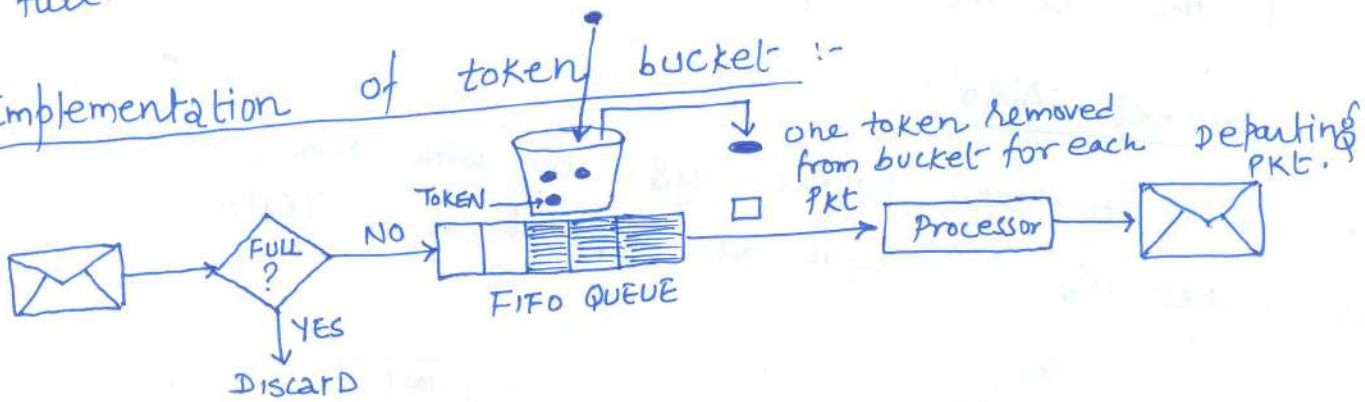
In fig (a) - The bucket holding three tokens with five packets waiting to be transmitted for a packet to be transmitted, it must capture & destroy one token.

In fig (b), three of the five packets have gone through but the remaining two are still waiting for more tokens to be generated because at every st, a token get generated depending upon the needs.

Difference between Leaky bucket & token bucket :-

The ~~leaky~~ token buckets allow or bound the remaining packets to wait for some time until they acquire some token whereas the leaky bucket discards the packets if the bucket is full.

Implementation of token bucket :-



→ The above fig. shows the implementation of token bucket.
→ The token acts as gate pass.
→ Each time a token is added.
→ Each packet's propagation makes the no. of token decremented.

Token Bucket Performance :-

S = Burst length (in seconds)
C = Bucket capacity (in bytes)
ρ = token arrival rate (bytes/second)
m = maximum source rate (bytes/second)

(i) maximum bytes sent from the token bucket during a burst is = $C + \rho S$ bytes
(ii) maximum bytes the source can send during a burst is = $m \cdot S$
(iii) By eqn (i) & (ii) –

$$S = \frac{C}{m - \rho}$$

Note:- Please go through Resource Reservation, Admission Control, Proportional Routing & Packet Scheduling from P-1.59 to 1.61 on your own. They are taught in class but not included in NOTES. So STUDY IT.