UNIT-V

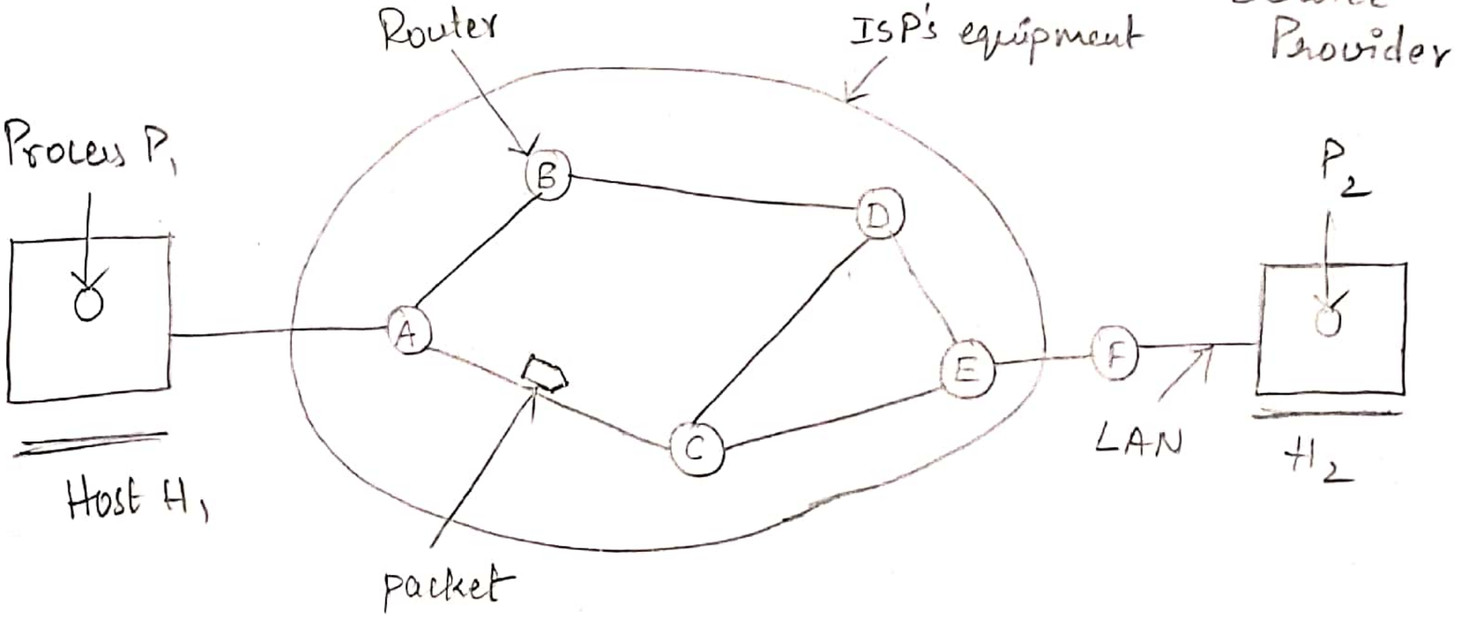
The Network Layer

Network Layer design Issues:

① Store and Forward Packet Switching
② Services provided to the Transport Layer
③ Implementation of Connectionless Service
④ Implementation of Connection-Oriented Service
⑤ Comparison of Virtual-Circuits & Datagram Networks.

① Store and Forward Packet Switching:

ISP: Internet Service Provider



- The major components of Network are ISP's equipment (routers connected by transmission lines) shown inside the oval and customer's equipment outside the oval.
- Host H_1 is directly connected to one of the ISP's routers.

- H_2 is on a LAN, which might be an office Ethernet with a router F, owned and operated by the customer.
- Host H_1 transmits the packet to the nearest router.
- The packet is stored there until it has fully arrived.
- The link performs error control by verifying the checksum.
- Then it is forwarded to the next router along the path until it reaches the destination host.
- This mechanism is called store-and-Forward packet Switching.

② Services provided to the Transport Layer:

- The Network Layer provides services to the Transport Layer at the Network Layer/Transport layer interface.
- The services need to be carefully designed with the following goals:

ⓐ The services should be independent of the router technology.

ⓑ The transport layer should be shielded from the number, type & topology of the routers present.

ⓒ The Network addresses made available to the transport layer should use a uniform numbering plan.

Connection oriented service / connectionless service :

- If the Network layer provides connectionless service, error correction & detection & flow control are done by the hosts themselves.

- Packets are transmitted from source to destination using the primitives SEND PACKET and RECEIVE PACKET where each packet must carry the full destination address, because each packet sent is carried independently. Does not provide Quality of Service (QoS)

- If the Network layer provides connection-oriented service, in case of voice calls & video calls connectionless service lags behind where as connection-oriented service have a good success of telephone Networks.

- With the entry of the following, connectionless service became stronger enough & provided good QoS

ⓐ ARPANET (Advanced Research Project Agency of Networks)

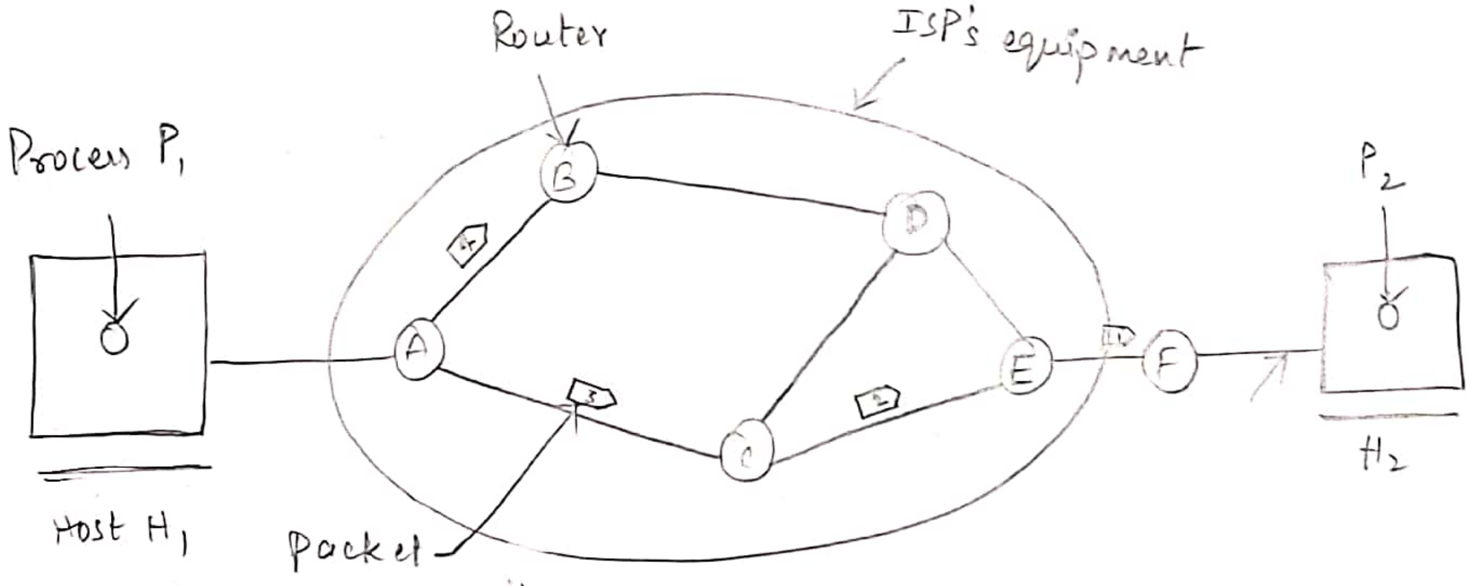
ⓑ ATM (Asynchronous Transfer Mode)

ⓒ INTERNET

ⓓ IP (Internet Protocol)

③ Implementation of Connectionless Service :

- If connectionless service is offered, packets are injected into the n/w individually and routed independently of each other.
- No advance setup is needed ie., predefined path is not required.
- In connectionless service, packets are called datagrams and the network is called a datagram n/w.



A's table (initially)

A	—
B	B
C	C
D	B
E	C
F	C

Dest Line

A's table (later)

A	—
B	B
C	C
D	B
E	B
F	B

C's table

A	A
B	A
C	–
D	E
E	E
F	E

E's table

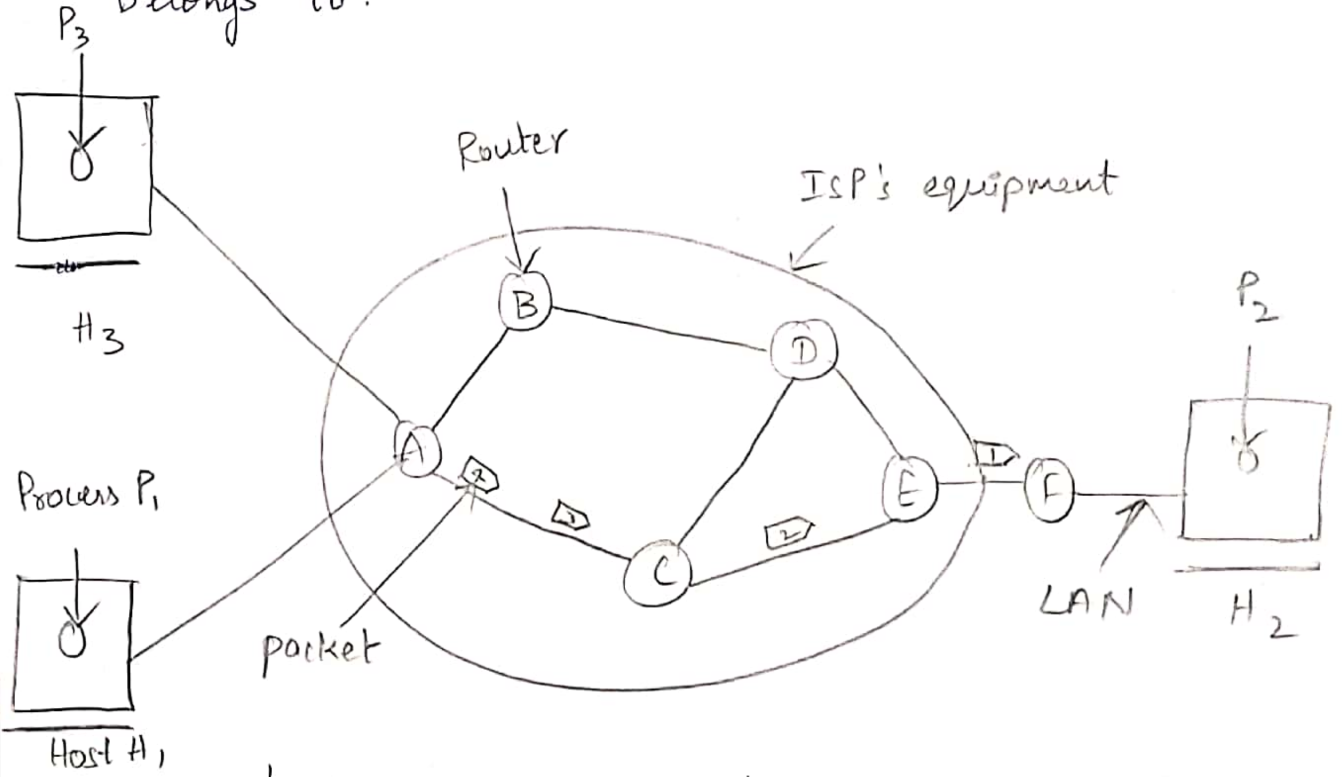
A	C
B	D
C	C
D	D
E	–
F	F

- In the above diagram, suppose that the Process P_1 on Host H_1 has a long message for Process P_2 on Host H_2.
- Assume that the message is four times longer than the maximum packet size, so the n/w Layer has to break it into four packets 1,2,3 & 4.
- Each packet is sent to router A, A has only two outgoing lines - B & C, so every incoming packet must be sent to one of these routers.
- At A, when packets arrived on the incoming link, their checksums are verified, then each packet is forwarded to the next outgoing link.
- Packets 1,2,3 follow the same route A CEF.
- But packet 4, due to traffic it is routed in a different path ABDEF
- The algorithm that manages the tables and makes the routing decisions is called the routing algorithm.

④ Implementation of Connection-Oriented Service:

- If connection-Oriented service is used, a path from the source router to the destination router must be established before any data packets can be sent

- This connection is called a VC (Virtual Circuit) and the network is called a Virtual-Circuit network.
- When a connection is established, a route from source to destination is chosen.
- That route is used for all traffic flowing over the connection.
- When the connection is released, the Virtual-Circuit is also terminated.
- In connection-oriented service, each packet carries an identifier telling which virtual circuit it belongs to.



A's table

In		Out	
H1	1	C	1
H3	1	C	2

C's table

A	1	E	1
A	2	E	2

E's table

C	1	F	1
C	2	F	2

- In the above diagram, host H_1 has established connection 1 with host H_2.
- The first line of A's table says that if a packet bearing connection identifier '1' comes in from H_1, it is to be sent to router C and given connection identifier 1.
- Similarly, the first entry at C routes the packet to F, also with connection identifier 1.
- Consider that H_3 also wants to establish a connection to H_2.
- It chooses connection identifier '1' and establishes VC.
- Here 'A' can easily distinguish connection 1 packets from H_1 and connection 1 packets from H_3, but C cannot do this.
- For this reason, A assigns a different connection identifier to the outgoing traffic for the second connection.
- This process is called label switching.

(5) Comparison of Virtual-Circuit & Datagram Networks.

Issue	Datagram N/w	Virtual-Circuit N/w
(1) Circuit setup	Not needed	Required
(2) Addressing	Each packet contains the full source and destination address.	Each packet contains a short VC number.
~~(3) State information~~		
(3) Routing	Each packet is routed independently.	Route is chosen when VC is set up; all packets follow it.
(4) Quality of Service (QoS)	Difficult	Easy if enough resources can be allocated in advance for each VC.
(5) Congestion Control	Difficult	Easy if enough resources can be allocated in advance for each VC.

Routing Algorithms :

- The main function of N/w Layer is routing packets from source machine to the destination machine.
- The routing Alg is responsible for deciding which output line an incoming packet should be transmitted on.
- Properties in a routing alg :

Correctness	Stability
Simplicity	Fairness
Robustness	Optimality

① Correctness The routing should be done properly and correctly so that the packets may reach their proper destination.

② Simplicity : The routing should be done in a simple manner without any complexity.

③ Robustness : Once a major network becomes operative, it may be expected to run continuously for years without any failures.

- Routing algs should be robust enough to handle hardware & software failures, should be able to cope with changes in the topology and traffic

(4) Stability :- The routing algs should be stable under all possible circumstances.

(5) Fairness :- Every node connected to the n/w should get a fair chance of transmitting their packets. This is generally done on a FCFS basis.

(6) Optimality : The routing algs should be optimal in terms of throughput & packet delays.

- Routing algs are grouped into two major classes. Non-adaptive routing algorithms & adaptive routing algs.

(1) Non-adaptive routing alg : ~~[illegible]~~ this alg, Do not base their routing decisions on any measurements or estimates of current topology and traffic. The choice of the route is computed in advance & downloaded to the routers when the n/w is booted. This procedure is called Static routing.

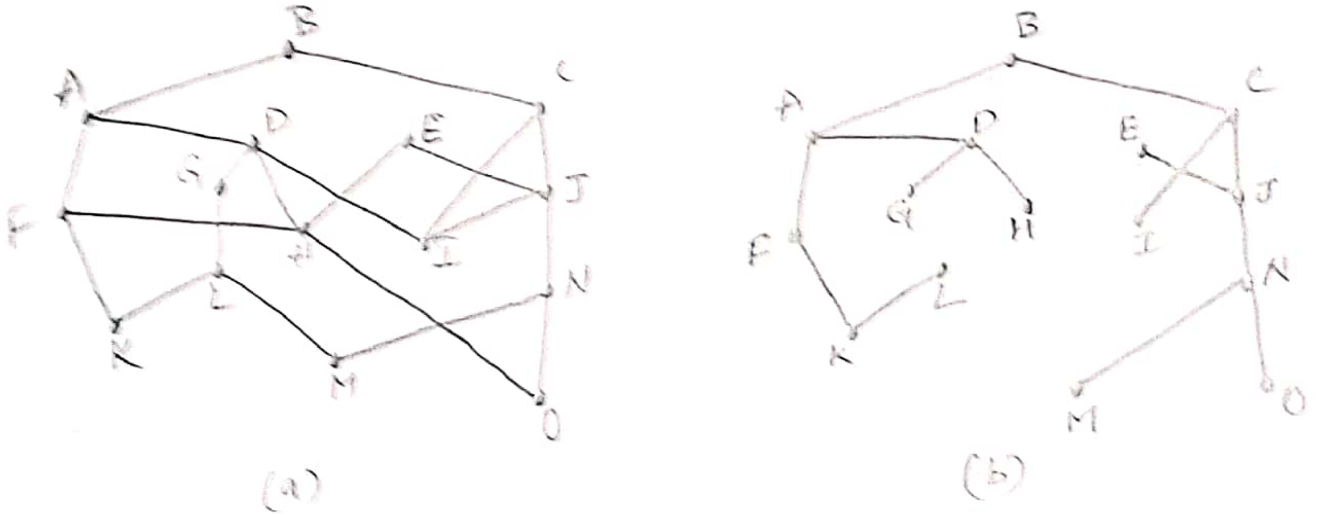
(2) Adaptive routing Alg : This alg changes their routing decisions according to the changes in topology & traffic. This procedure is called dynamic routing.

Routing Algorithms

- The optimality principle
- Shortest Path routing
- Flooding
- Distance Vector Routing
- Link State Routing
- Hierarchical Routing
- Broadcast Routing
- Multicast Routing

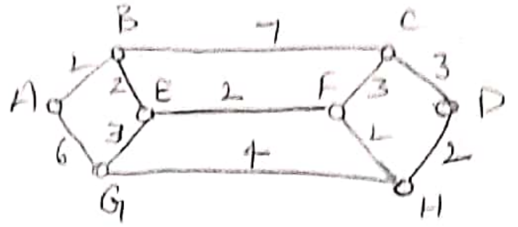
(i) The optimality principle :

- It states that if router J 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
- Consider the route from I to J as r_1.
  route from J to K as r_2
- If a route better than r_2 existed from J to K, it could be concatenated with r_1 to improve the route from I to K.
- In optimality principle, set of optimal routes from all sources to a given destination form a tree rooted at the destination.
- Such a tree is called as a sink tree
- A sink tree is not necessarily unique.
- A sink tree does not contain any loops.

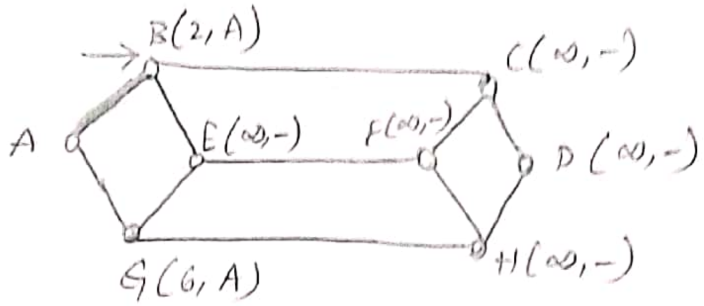


② Shortest Path Routing Algorithm :

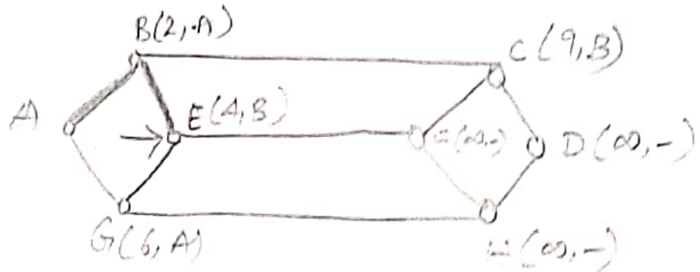
- In this alg, a graph of the N/w is developed, with each node of the graph representing a router and each edge of the graph representing a communication line or link.
- To choose a route b/w a given pair of routers, the alg just finds the shortest path b/w them on the graph.
- The cost of the link may be a function of distance, bandwidth, average traffic, Communication cost, delay etc.



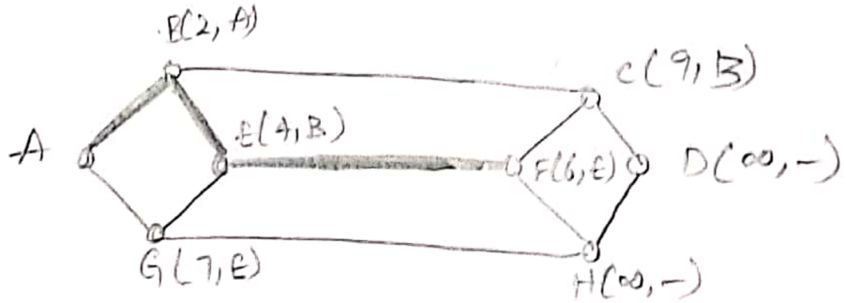
step1 :



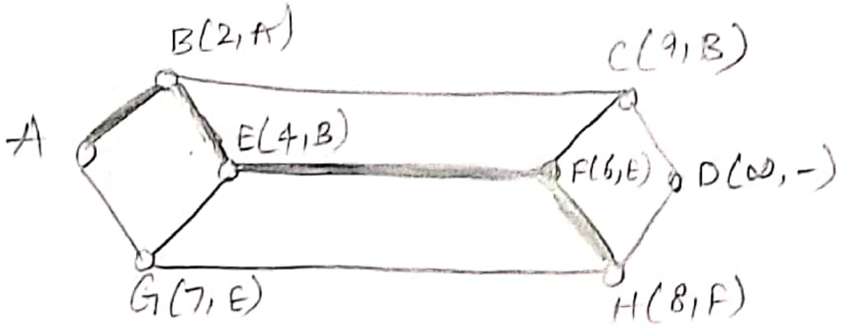
step 2 :



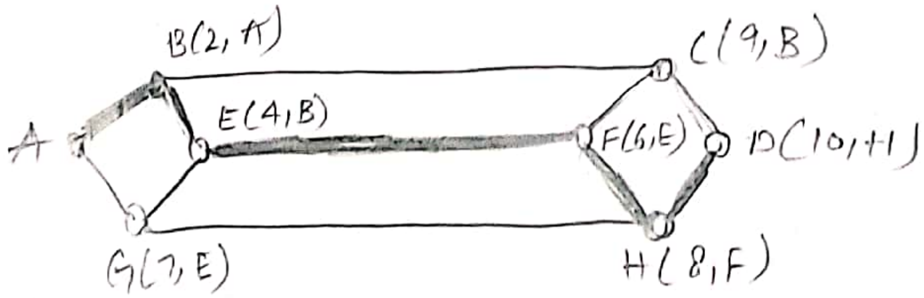
Step 3 :



Step 4 :

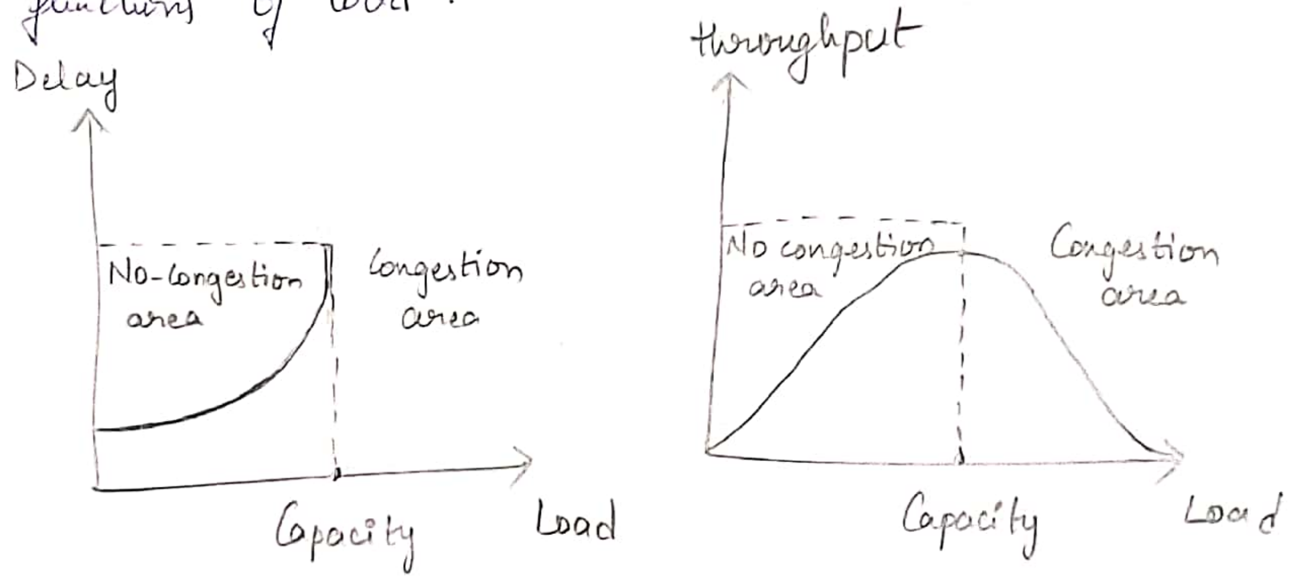


Step 5 :



Congestion Control :

- Too many packets present in a network causes packet delay and loss that degrades performance. This situation is called Congestion.
- Congestion at the network layer is related to two issues, throughput and delay.
- N/w performance with packet delay & throughput as functions of load :



- When the load is less than the N/w capacity, the delay is minimum.
- When the load reaches N/w capacity, the delay increases.
- Delay becomes infinite when the load is greater than the capacity.
- When load is below the capacity of the N/w, the throughput increases ~~pro~~ proportionally with the load.

- When the load exceeds the network capacity, the queues become full and the routers will discard some packets. So, the throughput decreases.
- Discarding packets does not reduce the number of packets in the n/w because the sources retransmit the packets using time-out mechanisms, when the packets do not reach the destinations.
- Congestion Control is of two types:-

Congestion Control

- open loop congestion control
  - policies
    - Retransmission policy
    - Window policy
    - Discarding policy
    - Acknowledgement policy
    - Admission policy
- closed loop congestion control
  - policies
    - Back pressure
    - Choke packets
    - Implicit signaling
    - Explicit signaling
      - Forward signaling
      - Backward signaling

<u>open loop</u> <u>congestion</u> <u>Control</u>: In open-loop congestion control,
① <u>Ratransmission</u> <u>policy</u>:- policies are applied to prevent congestion before it happens. In these mechanisms, congestion control is handled by either the source or destination.

- The policies that can prevent congestion are:-

① Retransmission policy : It is the policy in which retransmission of the packets are taken care. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted.

- This transmission may increase the congestion in the network. To prevent congestion, retransmission timers must be designed to prevent congestion & also able to optimize efficiency.

② Window policy :- The type of window at the sender side may also affect the congestion.

- Several packets in Go-back-n window are resent, although some packets are received succesfully at the receiver.
- This duplication increase the congestion in the network
- Therefore, selective repeat window should be adopted as it sends only the specific packet that is lost.

③ Discarding policy :- A good discarding policy adopted by the routers is the routers may prevent congestion and at the same time partially discards the corrupted or less sensitive packets and also able to maintain the quality of a message.

- In case of audio file transmission, routers can discard less sensitive packets to prevent congestion and also maintain the quality of audio file.

(4) Acknowledgement policy: Since acknowledgements are also part of the load in the network, the ACK policy imposed by the receiver may also affect congestion.

- Several approaches can be used to prevent congestion related to acknowledgement.
- ~~Th~~ One of the approach is:- The receiver should send acknowledgement for N packets rather than sending acknowledgement for a single packet.

(5) Admission policy: Admission policy can also prevent congestion in virtual-circuit networks.

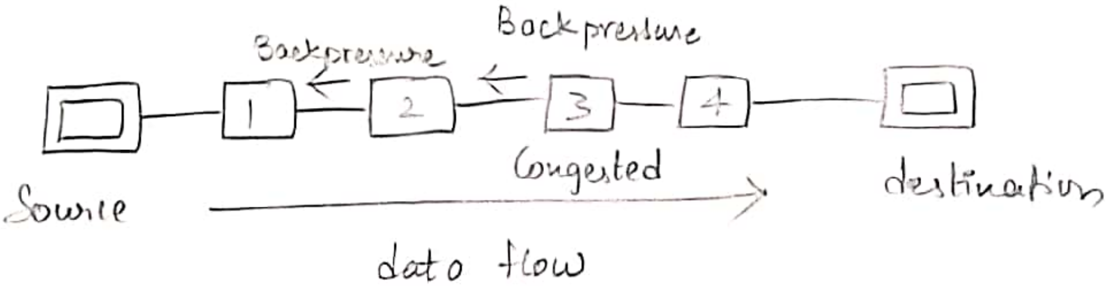
- Switches in a flow should first check the resource requirement of a network flow before transmitting it further.
- If there is a chance of congestion or there is congestion in the network, router should deny establishing a virtual network connection to prevent further congestion.

All these policies are adopted to prevent congestion before it happens in the network.

closed loop Congestion control : In closed loop congestion control, policies are used to treat or reduce congestion after it happens.

(1) Backpressure : It is a technique in which a congested node stops receiving packet from (previous) upstream node.

- This may cause the upstream node or nodes to become congested and rejects receiving data from above nodes.
- Backpressure is a node-to-node congestion control technique that propagate in the opposite direction of data flow
- The backpressure technique can be applied only to virtual-circuit where each node has information of its above upstream node.

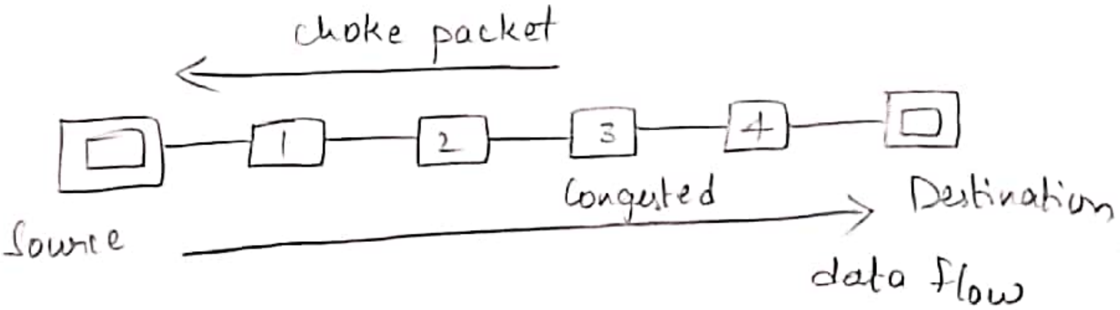


- In the above diagram, the 3rd node is congested and stops receiving packets as a result 2nd node also becomes congested due to slowing down of the output data flow.

- Similarly 1st node may get congested and informs the source to slow down.

② Choke packet technique : This technique is applicable to both virtual circuits as well as datagram subnets.

- A choke packet is a packet sent by a node to the source to inform it of congestion.
- Each router monitor its resources and the utilization at each of its output lines.
- Whenever the resource utilization exceeds the threshold value which is set by the administrator, the router directly sends a choke packet to the source giving it a feedback to reduce the traffic.
- But the intermediate nodes through which the packets has traveled are not warned about congestion.



③ Implicit Signaling : In implicit signaling, there is no communication b/w the congested nodes & the source.

- The source guesses that there is congestion in a network.
- For example, when sender sends several packets and there is no acknowledgement for a while, the source assumes that there is congestion.

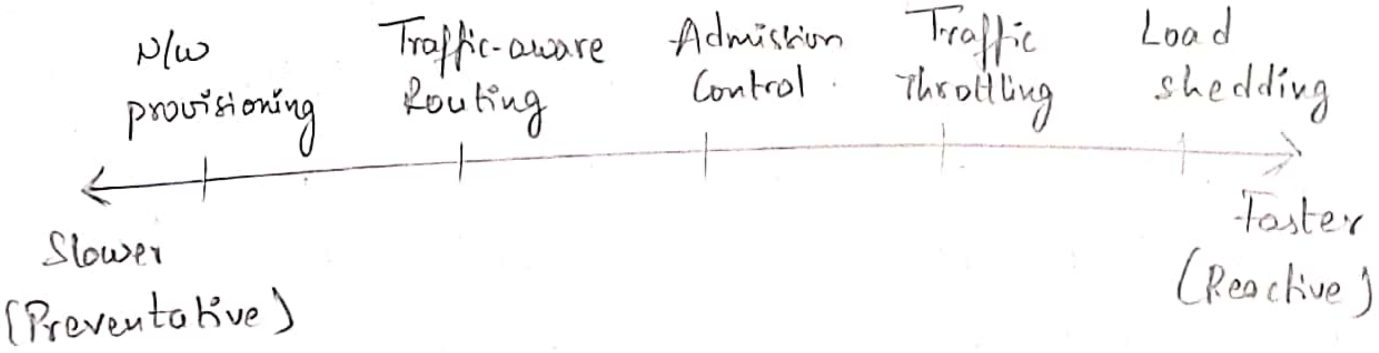
(4) <u>Explicity Signaling</u>. In explicit signaling, if a node experiences congestion it can explicitly send a packet to the source or destination to inform about congestion.

- The difference between choke packet and explicit Signaling is that the signal is included in the packets that carry data rather than creating different packet as in case of choke packet.
- <u>Forward Signaling</u>: In this, signal is sent in the direction of congestion ie to the destination.
- the destination is warned about congestion. the receiver in this case adopt policies to prevent further congestion.
- <u>Backward Signaling</u>. In this, signal is sent in the opposite direction of the congestion. The source is warned about congestion & it needs to slow down

Congestion Control algorithms.

Approaches to Congestion Control

- The presence of congestion means that the load is greater than the resources can handle.
- Two solutions can be used: either increase the resources or decrease the load.
- These solutions can be used either to prevent congestion or react to it once it has occurred.
- Different approaches are:-



① N/w provisioning:-

- In this approach, resources are added dynamically when there is congestion.

ways to add resources:-

ⓐ turning on spare routers or enabling lines that are normally used only as backups.

(b) purchasing bandwidth on the open market.

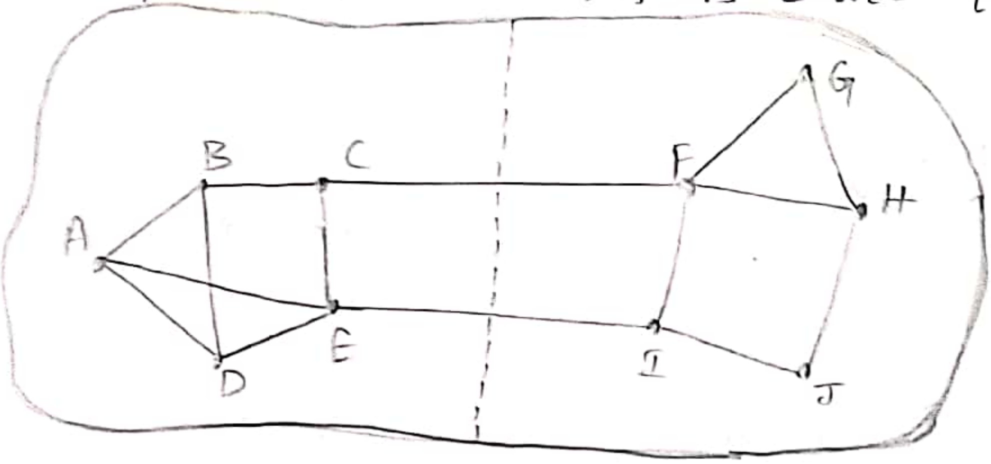
(c) links & routers that are regularly heavily utilized are upgraded.

- This is called provisioning & happens on a time scale of months, driven by long-term traffic trends

(2) Traffic-Aware Routing : This is done in the foll ways:-

- Routes can be changed by shifting the traffic from heavily used paths to lightly used paths.
- Splitting the traffic across multiple path can also be done.

Ex:- Some local radio stations have helicopters flying around their cites to report on road congestion to make it possible for their mobile listeners to route their packets (cars). This is called traffic-aware routing.



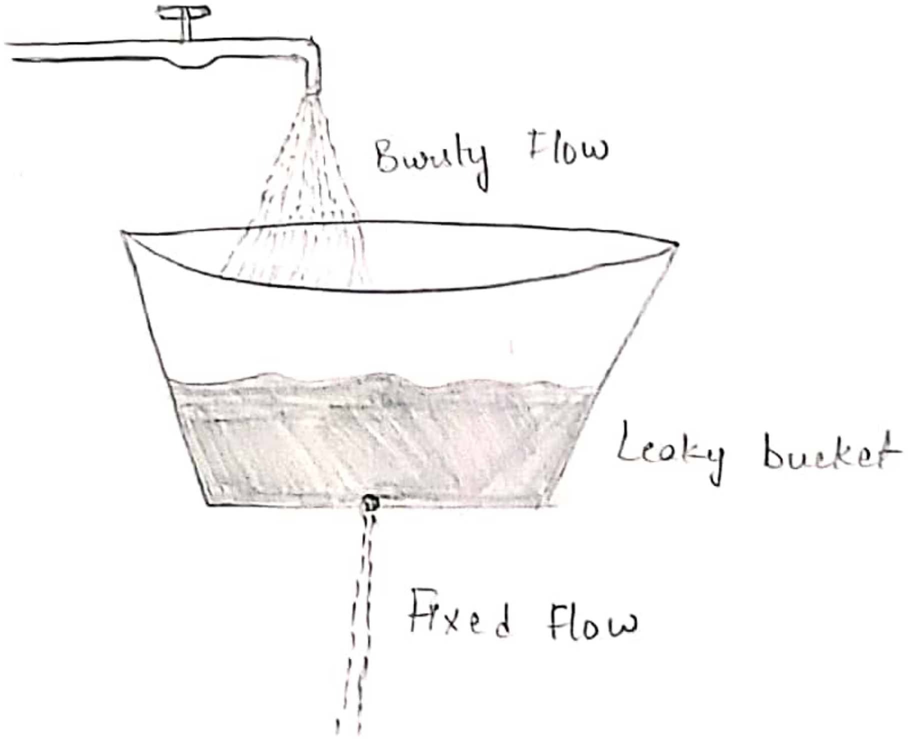
- Consider a network which is divided into two parts, East and West, connected by two links CF & EI.

- Suppose most of the traffic between East and West is using the link CF, the that link is congested.
- Then that traffic should be shifted to other link EI or the traffic should be splitted b/w CF & EI
- So that the congestion can be controlled.

③ Admission Control :- This technique is widely used in virtual-circuit networks.

- It states that : do not set up a new virtual circuit unless the n/w can carry the added traffic without becoming congested
- Admission control can be done by using leaky bucket or token bucket.

Leaky bucket :



- Leaky Bucket Algorithm :

- Imagine a bucket with a small hole in the bottom. No matter at what rate water enters the bucket, the outflow is at constant rate.

- When the bucket is full with water additional water entering spills over the sides and is lost.

- Similarly, each network interface contains a leaky bucket & the foll steps are involved in leaky bucket algorithm:

(1) When host wants to send packet, packet is thrown into the bucket.

(2) The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.

(3) Bursty traffic is converted to a uniform traffic by the leaky bucket.

(4) In practise the bucket is a finite queue that outputs at a finite rate.

(4) Traffic Throttling: This approach can be used in both datagram networks and virtual-circuit networks.

- This approach is done in the foll two steps:

Step 1:- Routers must determine when congestion is approaching before it has arrived.

- For the router to determine congestion, it should monitor the following things :

  (a) utilization of output links

  (b) Buffering of queued packets inside routers

  (c) Number of packets that are lost due to insufficient buffering.

- The queuing delay inside routers can also determine the congestion.

- If there is congestion, the queuing delay increases.

- The queuing delay can be calculated by the foll formula

$$d_{new} = \alpha d_{old} + (1-\alpha)s$$

α = constant

s = queue length.

This is called an EWMA (Exponentially Weighted Moving Average)

Step 2 : Routers must deliver timely feedback to the sender that are causing the congestion.

Different schemes use different feedback mechanisms, They are :- choke packets [in closed loop Congestion Control)

Explicit Congestion Notification [Explicit Signaling]

Hop-by-Hop Backpressure [Back pressure in closed loop]

⑤ Load shedding :-

- Load shedding means that when routers are being overloaded by packets that they cant handle they just throw them away.

- Packet drop is done in two ways:-

ⓐ wine : In this method it is assumed that old packet is better than new packet. ~~At~~ So, the new packet is discarded.

ⓑ milk :- In this method, it is assumed that new packet is better than old packet. So, the old packet is discarded.

Random Early Detection. In this method, Congestion is detected earlier and the packets the discarded.

- Packets should be discarded before all the buffer space is exhausted.

- To determine when to start discarding, routers maintain a running average of their queue lengths.

- When the avg queue length on some link exceeds, a threshold, the link is said to be congested & small fraction of packets are dropped at random.