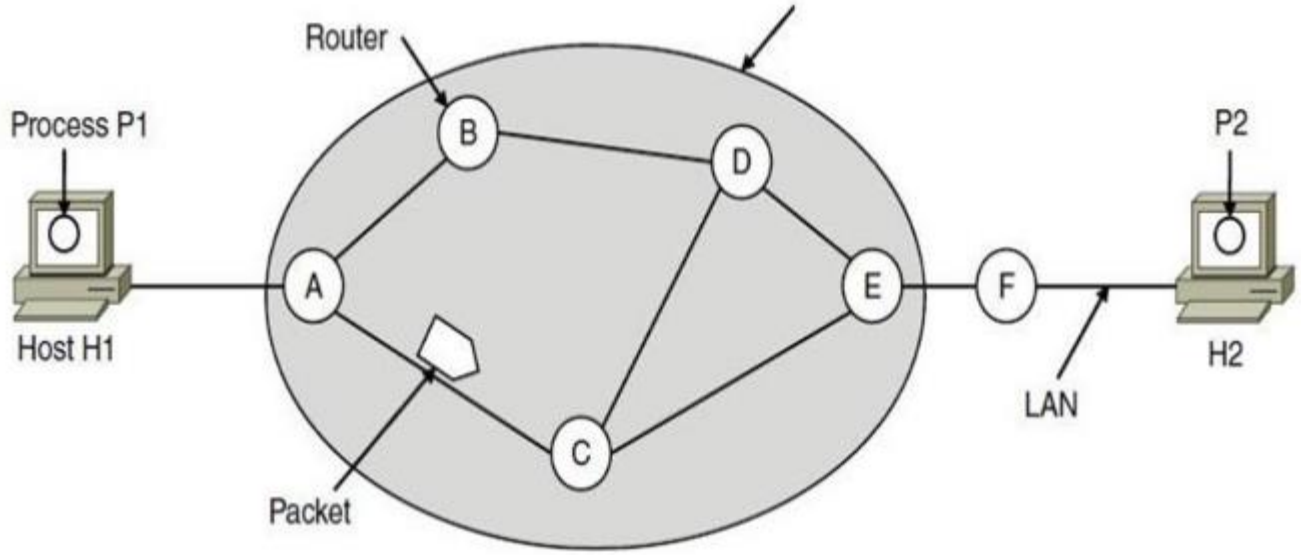
UNIT III
Network Layer

- Network Layer Design Issues
- Store-and-forward packet switching
- Services provided to transport layer
- Implementation of connectionless service
- Implementation of connection-oriented service
- Comparison of virtual-circuit and datagram networks

1.Store-and-forward packet switching

- 1.Store-and-forward packet switching A host with a packet to send transmits it to the nearest router, either on its own LAN or over a point-to-point link to the ISP.



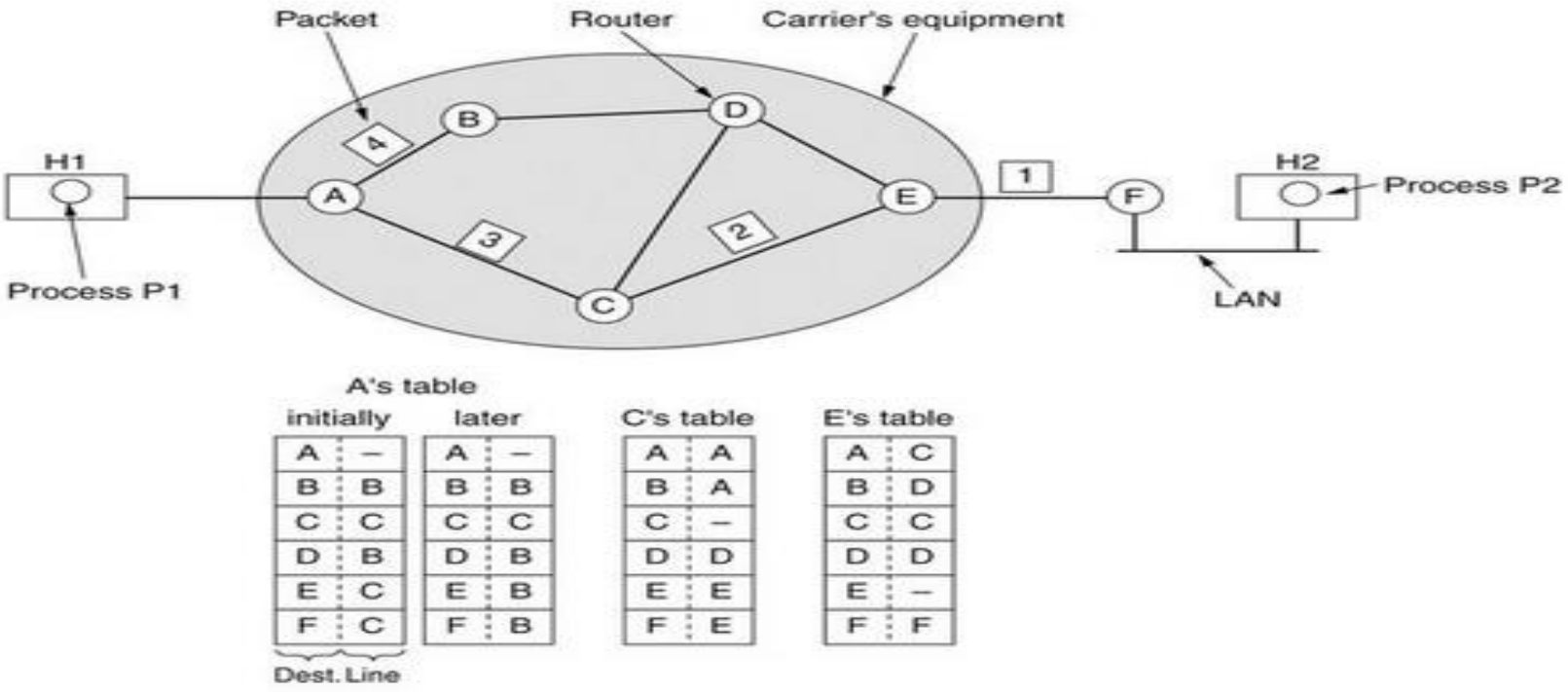
- The packet is stored there until it has fully arrived and the link has finished its processing by verifying the checksum.
- Then it is forwarded to the next router along the path until it reaches the destination host, where it is delivered. This mechanism is store-and-forward packet switching.

2.Services provided to 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 in mind:
- Services independent of router technology.
- Transport layer shielded from number, type, topology of routers.
- Network addresses available to transport layer use uniform numbering plan even across LANs and WANs

3.Implementation of connectionless service

- If connectionless service is offered, packets are injected into the network individually and routed independently of each other.
- No advance setup is needed. In this context, the packets are frequently called datagrams (in analogy with telegrams) and the network is called a datagram network

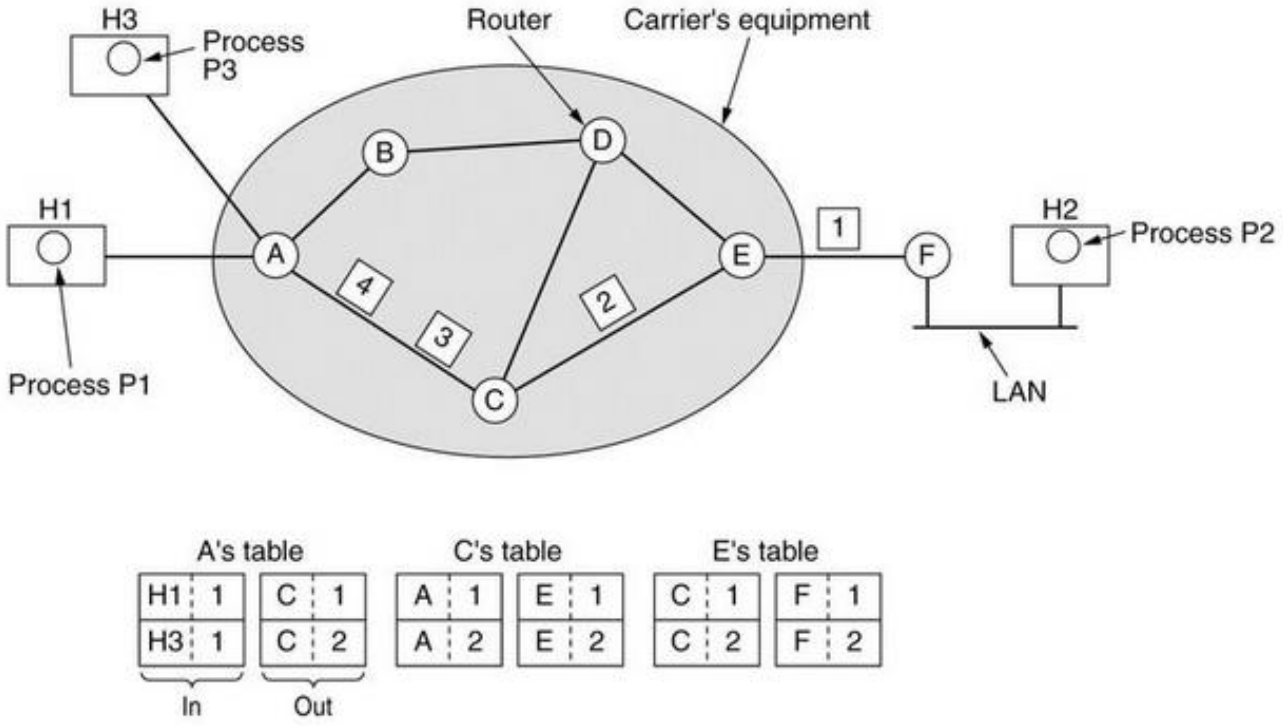


Routing within a diagram subnet.

Implementation of connectionless service

- Let us assume for this example that the message is four times longer than the maximum packet size, so the network layer has to break it into four packets, 1, 2, 3, and 4, and send each of them in turn to router A.
- Every router has an internal table telling it where to send packets for each of the possible destinations.
- Each table entry is a pair(destination and the outgoing line). Only directly connected lines can be used.

4.Implementation of connection-oriented service



Routing within a virtual-circuit subnet.

Implementation of connection-oriented service

- If connection-oriented service is used, a path from the source router all the way 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 the source machine to the destination machine is chosen as part of the connection setup and stored in tables inside the routers.

5.Comparison of virtual-circuit and datagram networks

Issue	Datagram subnet	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

- Routing Algorithms
- The main function of NL (Network Layer) is routing packets from the source machine to the destination machine.
- There are two processes inside router:

  a)One of them handles each packet as it arrives, looking up the outgoing line to use for it in the routing table. This process is forwarding.

  b)The other process is responsible for filling in and updating the routing tables. That is where the routing algorithm comes into play. This process is routing.

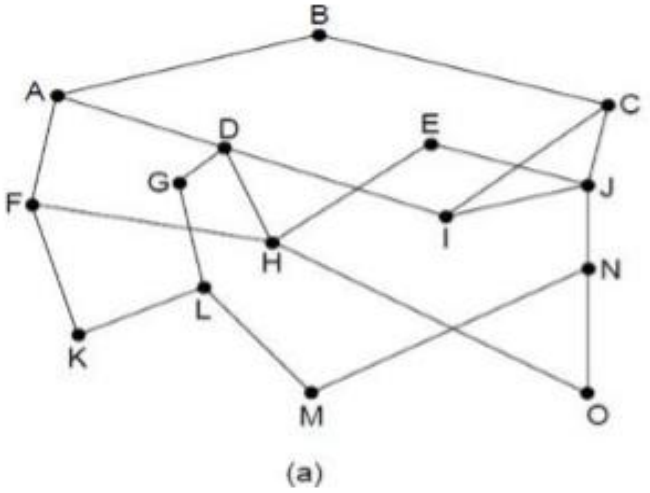
Routing algorithms can be grouped into two major classes: –

- Nonadaptive (Static Routing) – Adaptive(Dynamic Routing)
- Nonadaptive algorithm do not base their routing decisions on measurements or estimates of the current traffic and topology. Instead, the choice of the route to use to get from I to J is computed in advance, off line, and downloaded to the routers when the network is booted. This procedure is sometimes called static routing.
- Adaptive algorithm, in contrast, change their routing decisions to reflect changes in the topology, and usually the traffic as well.

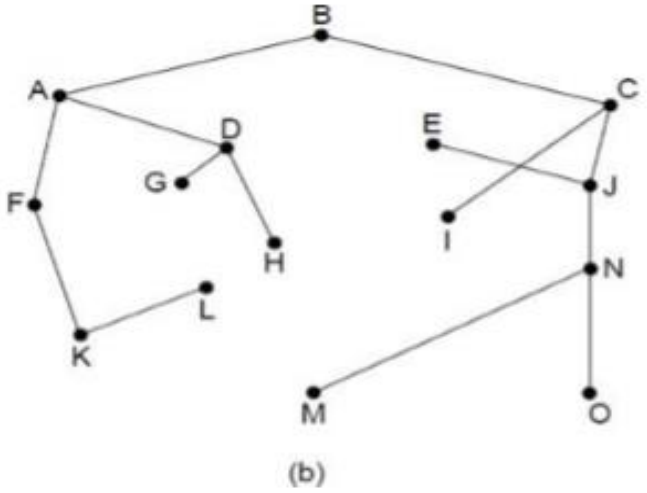
Different Routing Algorithms

- Optimality principle
- Shortest path algorithm
- Flooding
- Distance vector routing
- Link state routing
- Hierarchical Routing

- Optimality principle One can make a general statement about optimal routes without regard to network topology or traffic. This statement is known as the optimality principle.



a) A network.



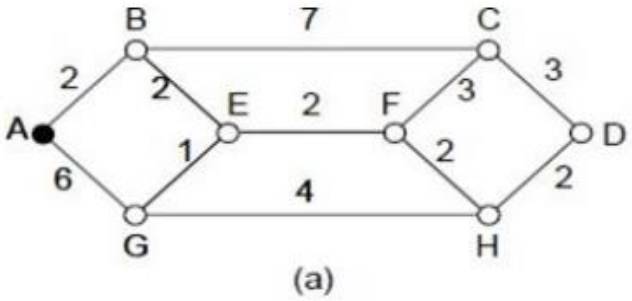
(b) A sink tree for router B.

- 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
- As a direct consequence of the optimality principle, we can see that the set of optimal routes from all sources to a given destination form a tree rooted at the destination. Such a tree is called a sink tree.

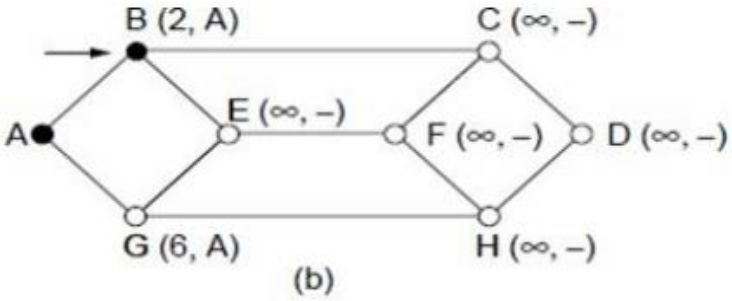
Shortest Path Routing (Dijkstra's)

- The idea is to build a graph of the subnet, with each node of the graph representing a router and each arc of the graph representing a communication line or link.
- To choose a route between a given pair of routers, the algorithm just finds the shortest path between them on the graph
- Start with the local node (router) as the root of the tree. Assign a cost of 0 to this node and make it the first permanent node.
- Examine each neighbor of the node that was the last permanent node.
- Assign a cumulative cost to each node and make it tentative
- Among the list of tentative nodes
- Find the node with the smallest cost and make it Permanent
- If a node can be reached from more than one route then select the route with the shortest cumulative cost.

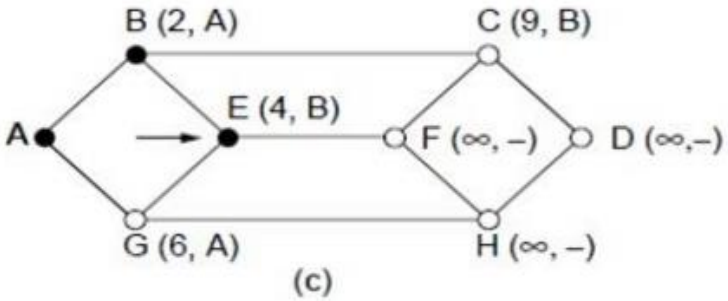
Shortest Path Routing (Dijkstra's)



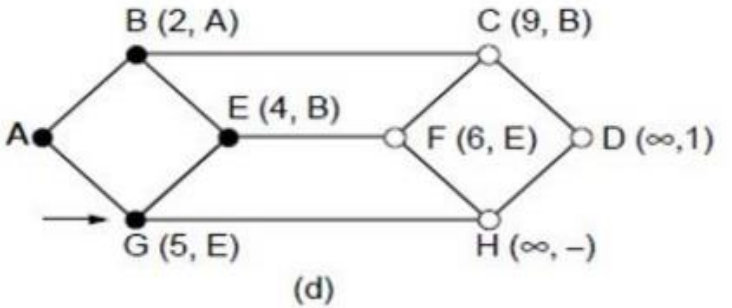
(a)



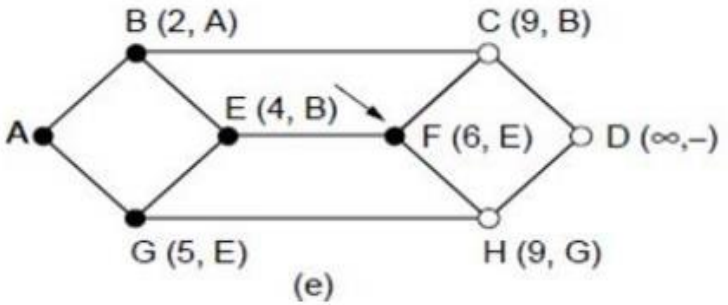
(b)



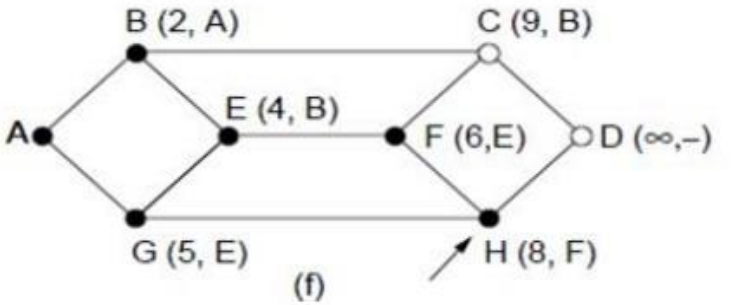
(c)



(d)

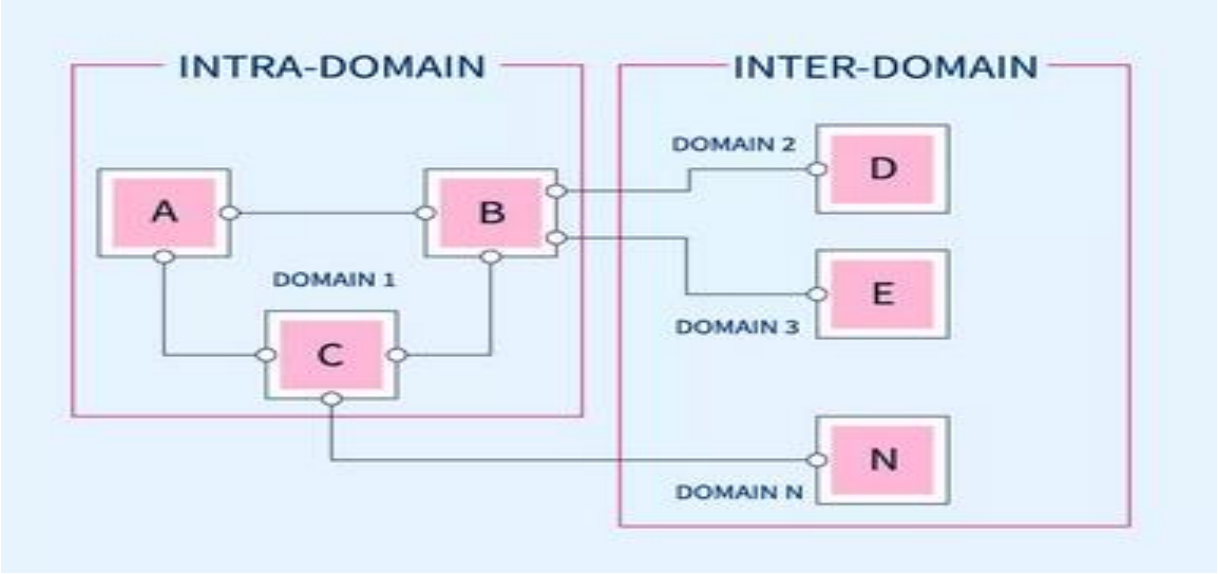


(e)

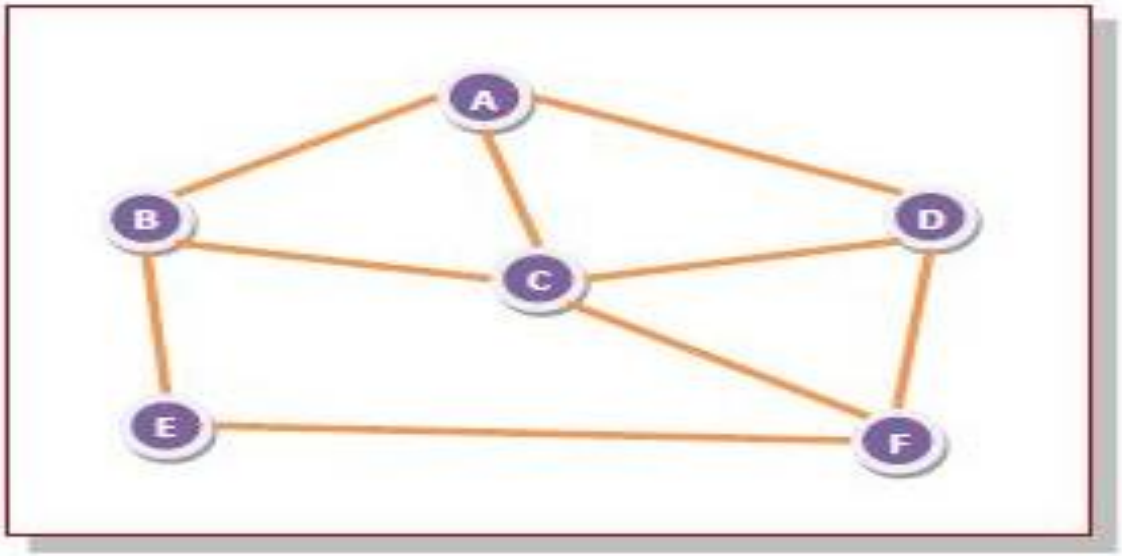


(f)

- Interdomain Routing is the protocol in which the routing algorithm works both within and between domains. Domains must be connected in some way, for hosts inside one domain to exchange data with hosts in other domains.
- Intradomain Routing is the routing protocol that operates only within a domain. In other words, intradomain routing protocols are used to route packets within a specific domain, such as within an institutional network for e-mail or web browsing



- Flooding
- Flooding is a Non-adaptive routing technique following this simple method: when a data packet arrives at a router, it is sent to all the outgoing links except the one it has arrived on.
- For example, let us consider the Network in the figure, having six routers that are connected through transmission lines.



- Using flooding technique –
- An incoming packet to A, will be sent to B, C and D.
- B will send the packet to C and E.
- C will send the packet to B, D and F.
- D will send the packet to C and F.
- E will send the packet to F.
- F will send the packet to C and E.

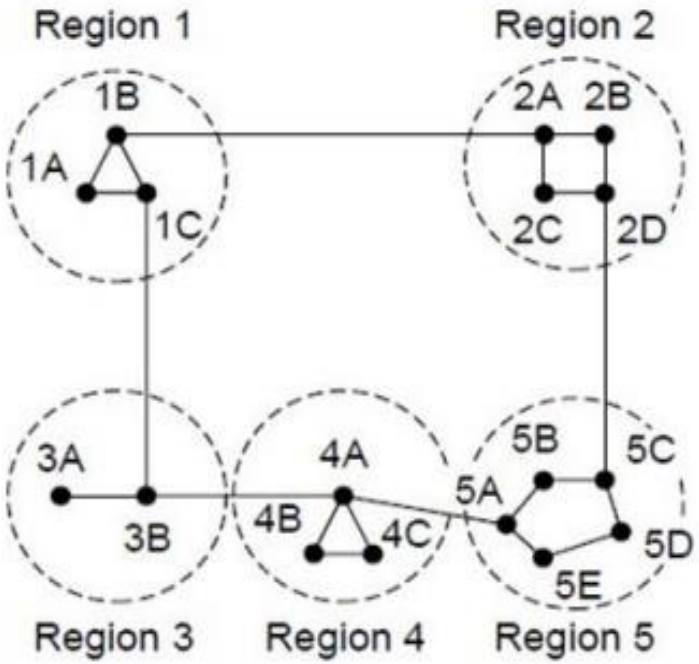
- **Types of Flooding**
- Flooding may be of three types −
- **Uncontrolled flooding** − Here, each router unconditionally transmits the incoming data packets to all its neighbours.
- **Controlled flooding** − They use some methods to control the transmission of packets to the neighbouring nodes. The two popular algorithms for controlled flooding are Sequence Number Controlled Flooding (SNCF) and Reverse Path Forwarding (RPF).
- **Selective flooding** − Here, the routers don't transmit the incoming packets only along those paths which are heading towards approximately in the right direction, instead of every available paths.

- **Advantages of Flooding**
- It is very simple to setup and implement, since a router may know only its neighbours.
- It is extremely robust. Even in case of malfunctioning of a large number routers, the packets find a way to reach the destination.

- **Limitations of Flooding**
- Flooding tends to create an infinite number of duplicate data packets, unless some measures are adopted to damp packet generation.

- Hierarchical Routing
- As networks grow in size, the router routing tables grow proportionally. Not only is router memory consumed by ever-increasing tables, but more CPU time is needed to scan them and more bandwidth is needed to send status reports about them.
- At a certain point, the network may grow to the point where it is no longer feasible for every router to have an entry for every other router, so the routing will have to be done hierarchically, as it is in the telephone network.

Hierarchical Routing



(a)

Full table for 1A

Dest.	Line	Hops
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

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

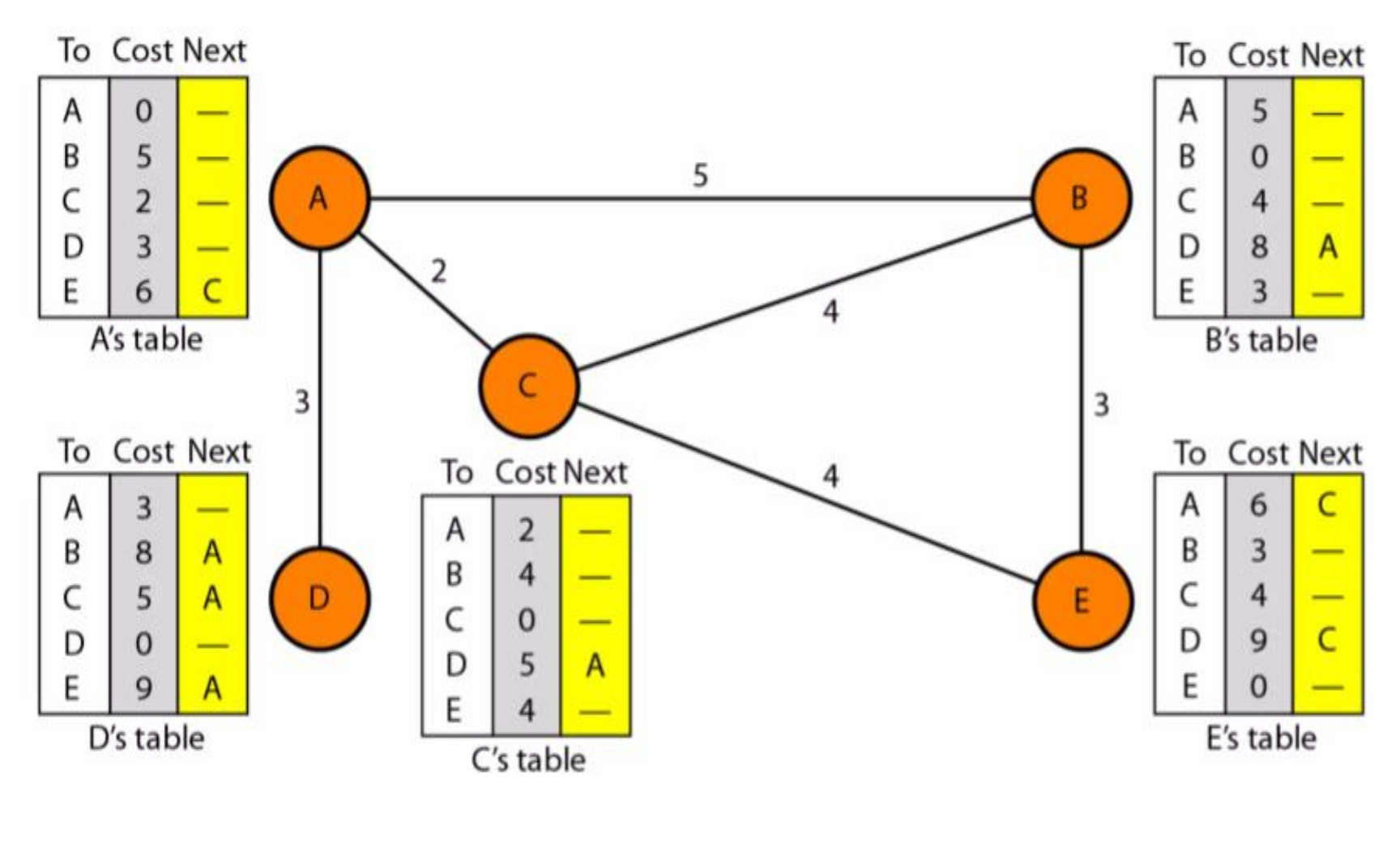
(c)

Activa

Distance Vector Routing (Bellman ford Algorithm)

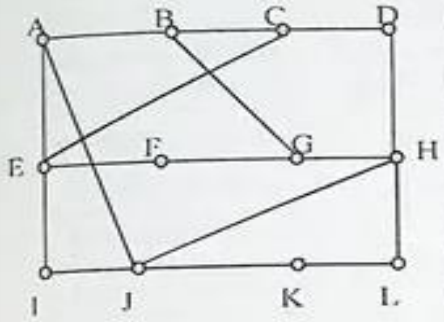
- In distance vector routing, the least-cost route between any two nodes is the route with minimum distance. In this protocol, as the name implies, each node maintains a vector (table) of minimum distances to every node.
- Mainly
- Initialization of tables in distance vector routing
- Sharing,
- Updating
- Each node can know only the distance between itself and its immediate neighbors, those directly connected to it. So for the moment, we assume that each node can send a message to the immediate neighbors and find the distance between itself and these neighbors.

Initialization of tables in distance vector routing



- Distance vector routing algorithms Distance vector routing algorithms 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 neighbors.
- 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 metric used might be number of hops, time delay in milliseconds, total number of packets queued along the path, or something similar.

Distance Vector Routing



New estimated delay from J

TO	A	I	H	K		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

Vector received from J's four neighbors

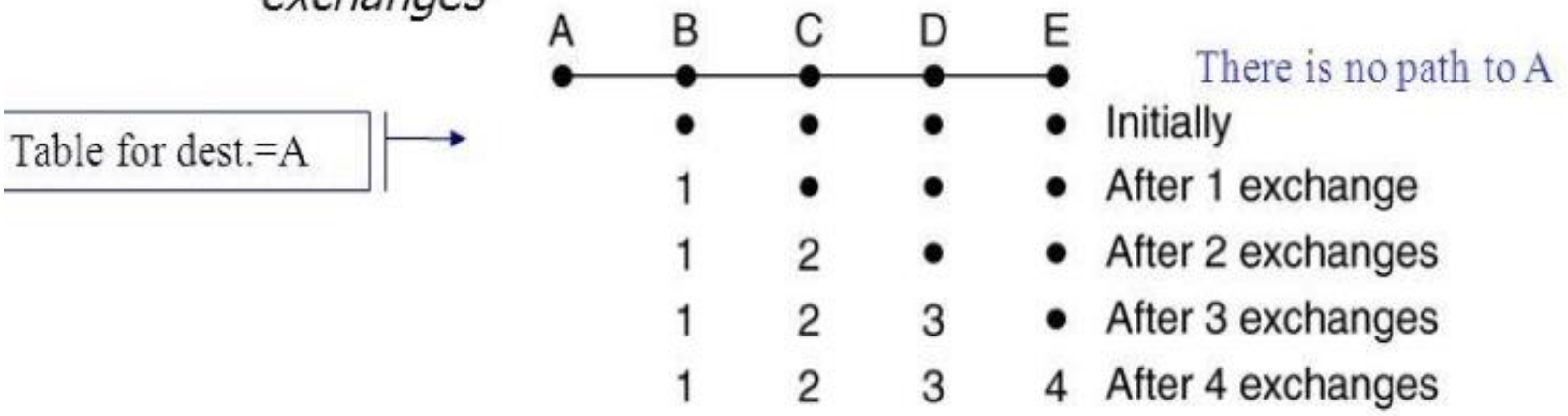
(a) Subnet (b) Input from routers A, I, H and K and new routing table for J.

Fig: Distance Vector Routing Table Format

- **Count to infinity problem:**
- One of the important issue in Distance Vector Routing is County of Infinity Problem.
- Counting to infinity is just another name for a routing loop.
- In distance vector routing, routing loops usually occur when an interface goes down.
- It can also occur when two routers send updates to each other at the same time.

Count –to-infinity Problem

- Problem:
  - Convergence is slow!
  - Good news travels quickly, bad news travels slowly (count-to-infinity) problem
- Example: Propagation of good news
  - Initially A is down and all other routers know this
  - When *A comes up, the other routers learn about it via the vector exchanges*



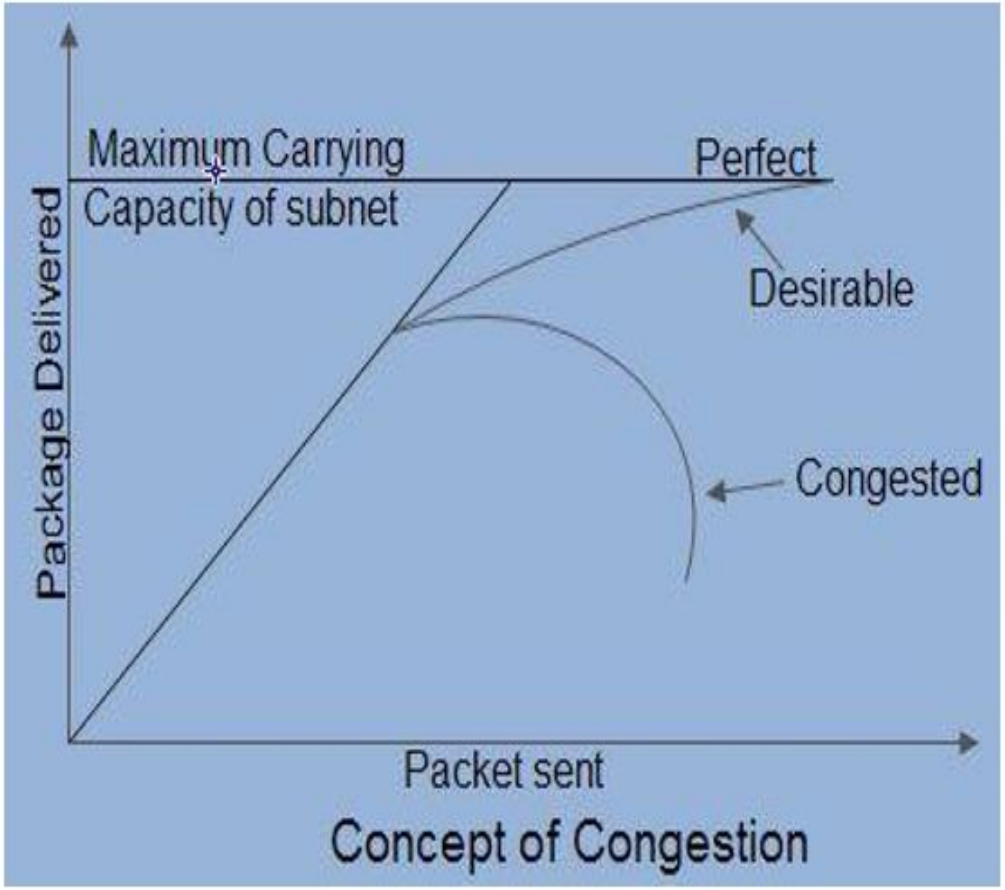
Count to Infinity Problem

B	C	D	E	
1	2	3	4	Initially
3	2	3	4	After 1 exchange
3	4	3	4	After 2 exchanges
5	4	5	4	After 3 exchanges
5	6	5	6	After 4 exchanges
7	6	7	6	After 5 exchanges
7	8	7	8	After 6 exchanges
	⋮			
∞	∞	∞	∞	

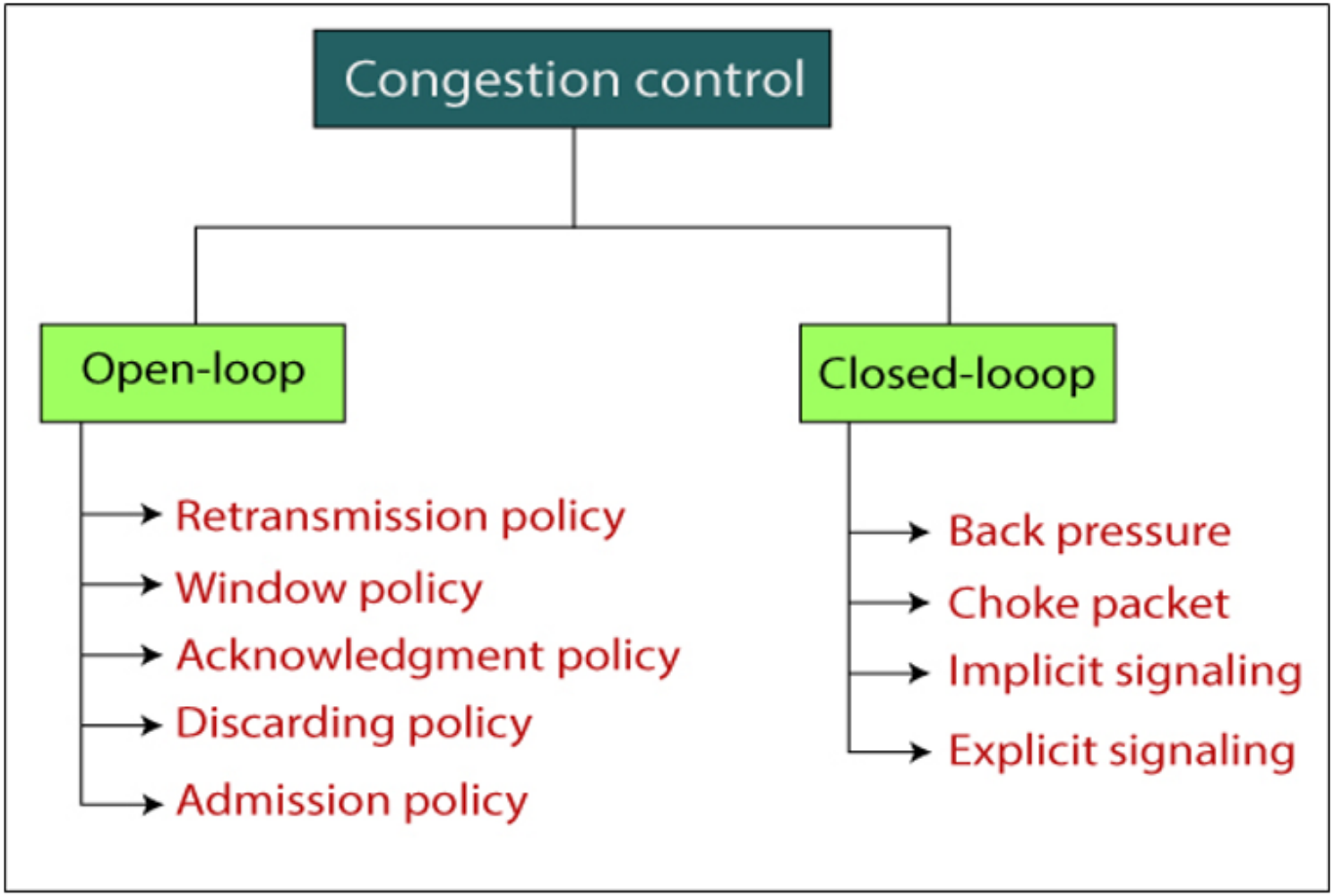
CONGESTION

- Congestion occurs when the number of packets being transmitted through the network approaches the packet handling capacity of the network
- Congestion control aims to keep number of packets below level at which performance falls off dramatically
- What is congestion?
- A state occurring in network layer when the message traffic is so heavy that it slows down network response time.
- Effects of Congestion
- As delay increases, performance decreases.
- If delay increases, retransmission occurs, making situation worse.

Network congestion occurs in case of traffic overloading.



CONGESTION


Congestion control
Open-loop
Closed-looop
Retransmission policy
Window policy
Acknowledgment policy
Discarding policy
Admission policy
Back pressure
Choke packet
Implicit signaling
Explicit signaling

- Open Loop Congestion Control Open loop congestion control policies are applied to prevent congestion before it happens. The congestion control is handled either by the source or the destination.
- Policies adopted by open loop congestion control –

1.Retransmission Policy : It is the policy in which retransmission of the packets are taken care of. 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 and also able to optimize efficiency.

2.Window Policy : The type of window at the sender's side may also affect the congestion. Several packets in the Go-back-n window are re-sent, although some packets may be received successfully at the receiver side.

- This duplication may increase the congestion in the network and make it worse. Therefore, Selective repeat window should be adopted as it sends the specific packet that may have been lost.

3. Discarding Policy : A good discarding policy adopted by the routers is that the routers may prevent congestion and at the same time partially discard the corrupted or less sensitive packages and also be 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 the audio file.

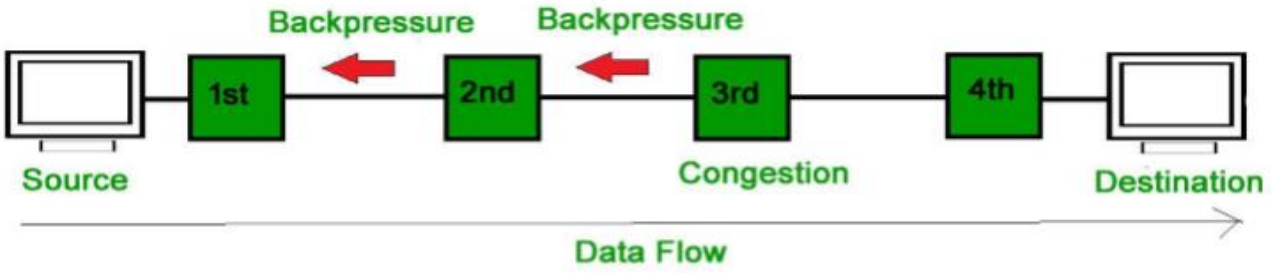
4. Acknowledgment Policy : Since acknowledgements are also the part of the load in the network, the acknowledgment policy imposed by the receiver may also affect congestion. Several approaches can be used to prevent congestion related to acknowledgment.

- The receiver should send acknowledgement for N packets rather than sending acknowledgement for a single packet. The receiver should send an acknowledgment only if it has to send a packet or a timer expires.

5.Admission Policy : In admission policy a mechanism should be used to prevent congestion. Switches in a flow should first check the resource requirement of a network flow before transmitting it further. If there is a chance of a congestion or there is a congestion in the network, router should deny establishing a virtual network connection to prevent further congestion.

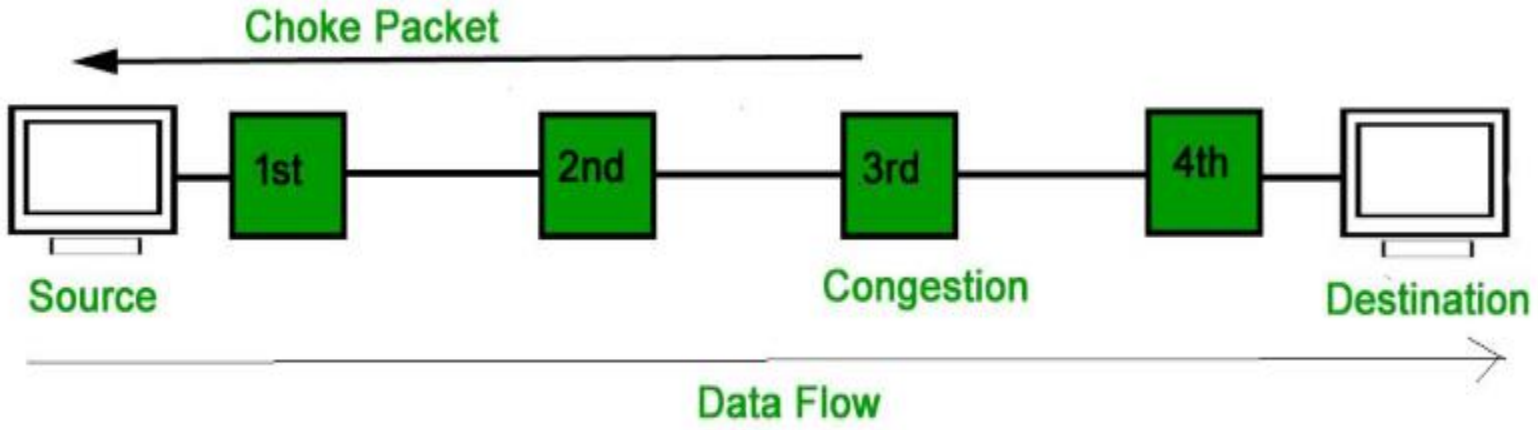
- Closed Loop Congestion Control Closed loop congestion control techniques are used to treat or alleviate congestion after it happens. Several techniques are used by different protocols; some of them are:

1. Backpressure : Backpressure is a technique in which a congested node stops receiving packets from upstream node. This may cause the upstream node or nodes to become congested and reject 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.



2. Choke Packet Technique：Choke packet technique is applicable to both virtual networks 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 monitors 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.



3. Implicit Signaling : In implicit signaling, there is no communication between the congested nodes and the source. The source guesses that there is congestion in a network. For example when sender sends several packets and there is no acknowledgment for a while, one assumption is that there is a congestion.

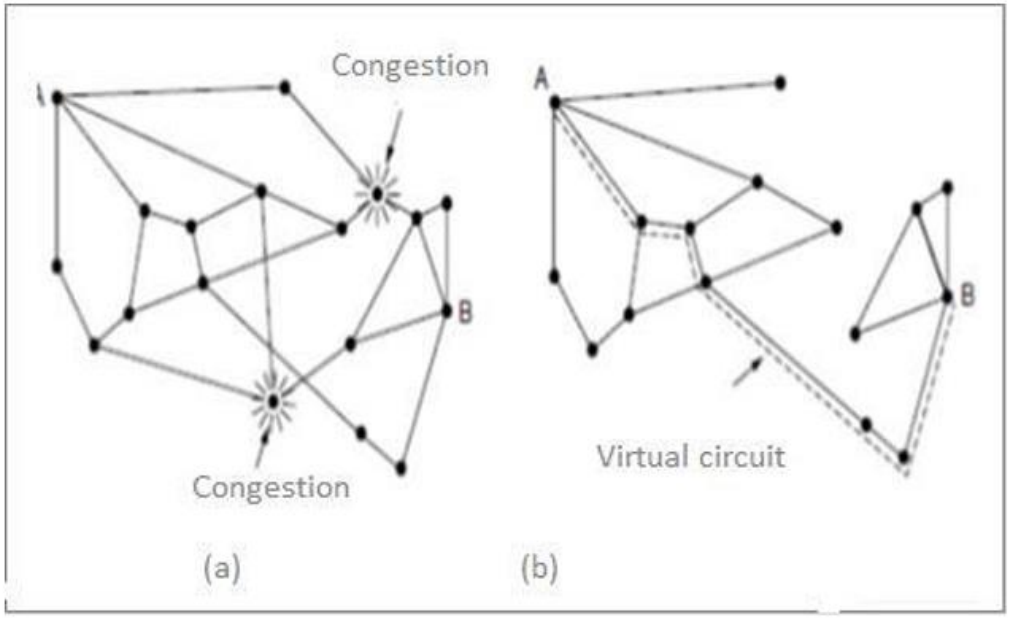
4. Explicit Signaling : In explicit signaling, if a node experiences congestion it can explicitly sends a packet to the source or destination to inform about congestion. The difference between choke packet and explicit signaling is that the signal is included in the packets that carry data rather than creating a different packet as in case of choke packet technique.

Explicit signaling can occur in either forward or backward direction.

Forward Signaling : In forward signaling, a signal is sent in the direction of the congestion. The destination is warned about congestion. The receiver in this case adopt policies to prevent further congestion.

Backward Signaling : In backward signaling, a signal is sent in the opposite direction of the congestion. The source is warned about congestion and it needs to slow down.

- Admission Control
- It is one of techniques that is widely used in virtualcircuit networks to keep congestion at bay. The idea is do not set up a new virtual circuit unless the network can carry the added traffic without becoming congested. Admission control can also be combined with traffic aware routing by considering routes around traffic hotspots as part of the setup procedure.
- Example Take two networks (a) A congestion network and (b) The portion of the network that is not congested. A virtual circuit A to B is also shown below −



- Explanation

  Step 1 − Suppose a host attached to router A wants to set up a connection to a host attached to router B. Normally this connection passes through one of the congested routers.

  Step 2 − To avoid this situation, we can redraw the network as shown in figure (b), removing the congested routers and all of their lines.

  Step 3 − The dashed line indicates a possible route for the virtual circuit that avoids the congested routers