COMPUTER NETWORKS MODULE 3.1

MS. JINCY J FERNANDEZ

ASST. PROF, CSE

RSET

Network Layer- Introduction

- Provides services to the transport layer and receives services from the data link layer.
- Get packets from the source all the way to the destination.
- This may require making many hops at intermediate routers along the way.

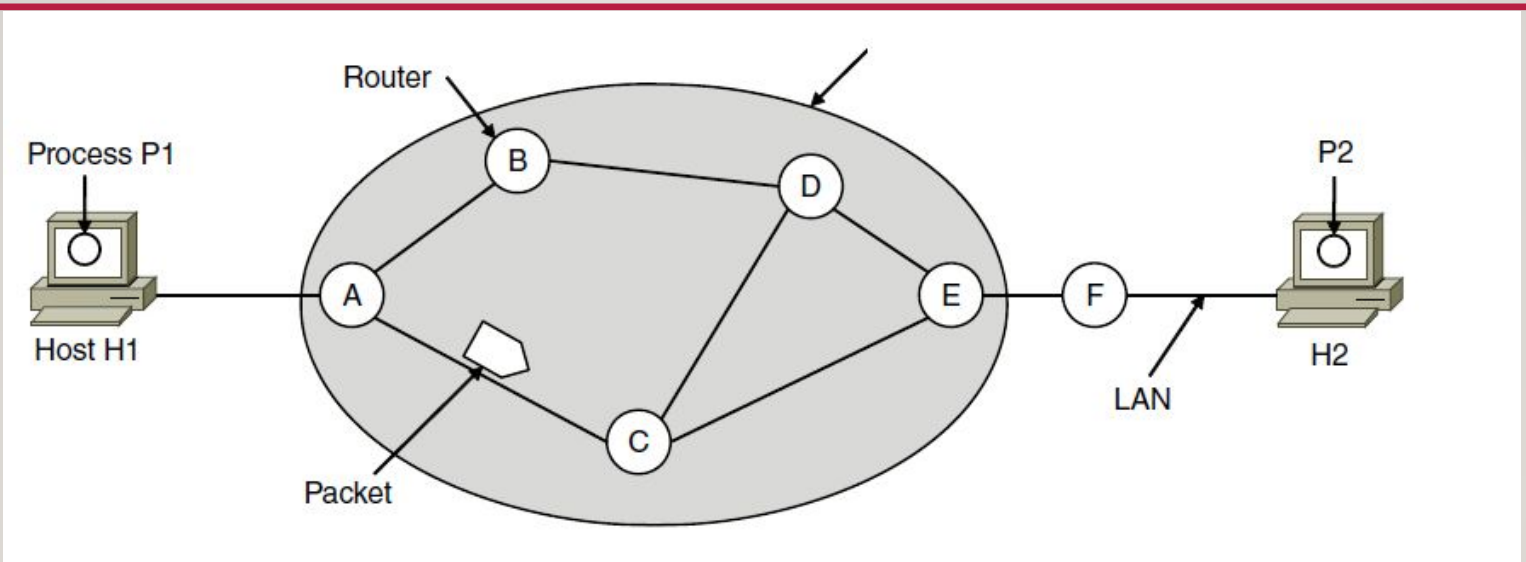
Network Layer- Introduction

- Duties of Network layer:
  - Awareness about topology of the network and choose appropriate paths through it.
  - Choose routes to avoid overloading some of the communication lines and routers while leaving others idle.
  - Deal with cases of source and destination on different networks.

Network Layer- Design Issues

- Store-and-forward packet switching
- Services provided to transport layer
- Implementation of connectionless service
- Implementation of connection-oriented service

Store-and-forward Packet Switching



- A host with a packet to send transmits it to the nearest router.
- The packet is stored in the router until it has fully arrived, checksum is verified.
- Then the packet is forwarded to the next router along the path until it reaches the destination host.

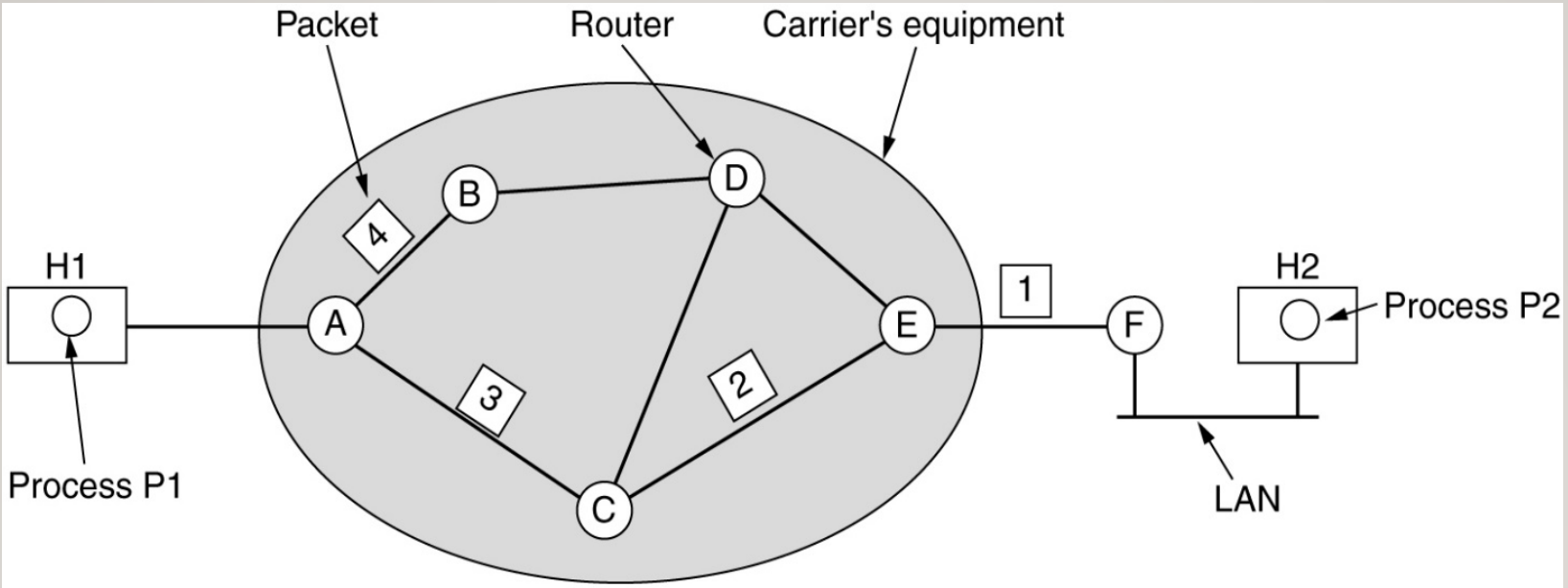
Services Provided To Transport Layer

- Services should be designed to achieve the following goals:
  - Services independent of router technology.
  - Transport layer should be shielded from number, type, topology of routers.
  - Network addresses available to transport layer should use a uniform numbering plan.

- Connectionless Service (Internet)
- Connection – oriented Service (ATM Networks)

Implementation Of Connectionless Service

- Packets are injected into the network individually and routed independently of each other.
- No advance setup is required.
- Packets are called datagrams and the network is called a datagram network.
- H1 sends a message to H2.
- Message broken down into 4 packets.
- Packets are routed based on the entry in the routing table.
- Routing Algorithm is the algorithm that manages the tables and makes the routing decisions.



A's table

initially		later	
A	–	A	–
B	B	B	B
C	C	C	C
D	B	D	B
E	C	E	B
F	C	F	B

Dest. Line

C's table

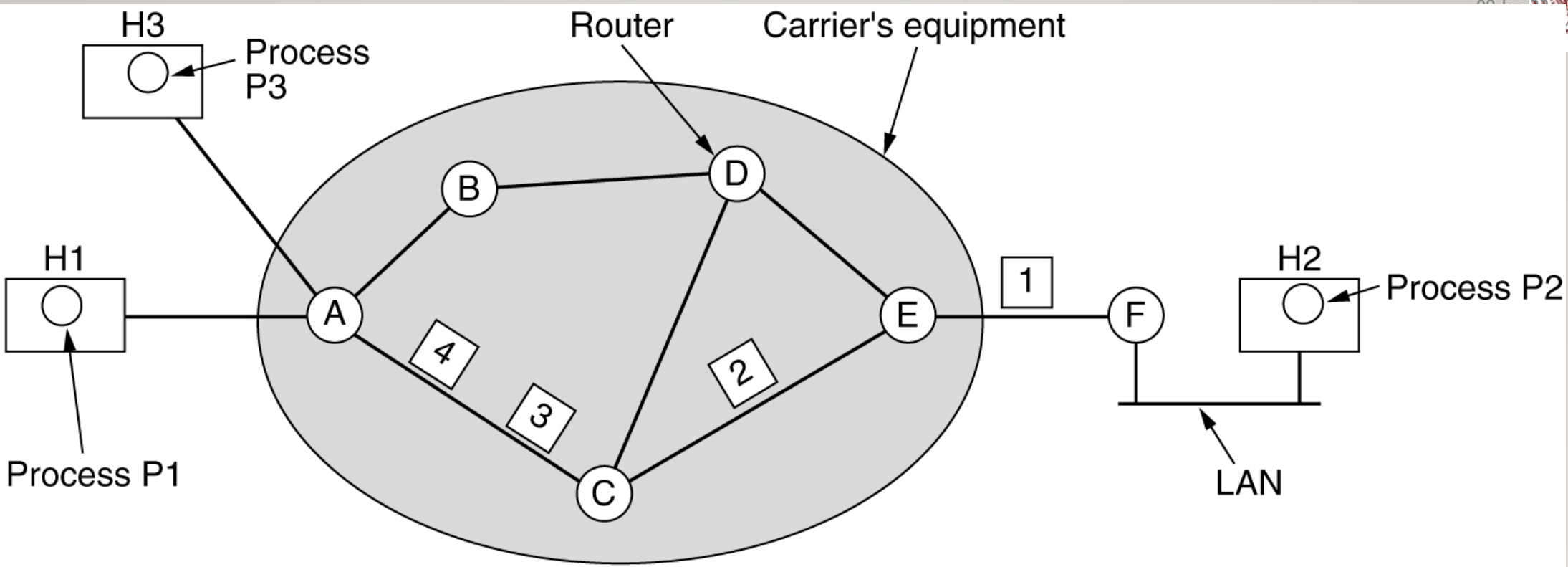
A	A
B	A
C	–
D	D
E	E
F	E

E's table

A	C
B	D
C	C
D	D
E	–
F	F

Implementation of Connection-oriented Service

- Before sending a message, a connection is established (virtual circuit).
- 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.
- This route is used for all traffic flowing over the connection.
- When the connection is released, the virtual circuit is also terminated.
- Each packet will carry an identifier telling which virtual circuit it belongs to.
- Subnet is called a virtual circuit subnet.
- Label switching: Routers replacing connection identifiers in outgoing packets.



If a packet with ID 1 comes in from H1, it is to be given to router C and given the ID 1

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

Comparison Of Datagram Network And Virtual Circuit

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

- Routing algorithms: part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on.
- Construction and maintenance of routing table is done by the routing algorithm.
- Forwarding - Decides to which output line an incoming packet should be transmitted.
- Routing- Decision is made based on the routing table.
  - If datagrams are used, the decision is made anew for every arriving data packet.
  - If virtual circuits are used, the decision is made when the new virtual circuit is set up – all the data packets follow the established route – called session routing.

Properties Desirable in a Routing Algorithm

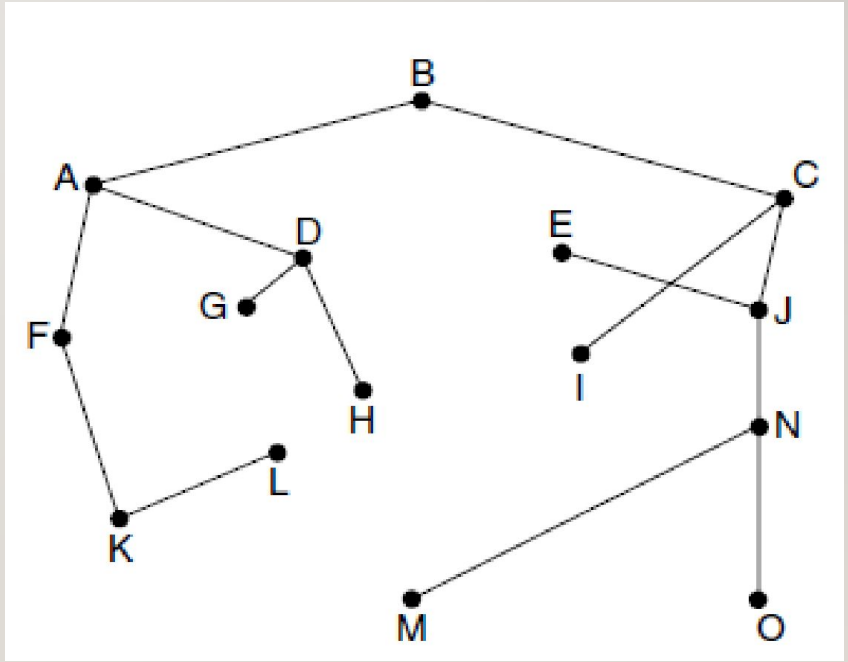
- Correctness
- Simplicity
- Robustness: able to cope with changes in the topology and traffic without requiring all jobs in all hosts to be aborted.
- Stability
- Fairness
- Efficiency: improve the overall network throughput.

Routing Algorithms

- Non-adaptive Routing Algorithms
  - Static: Current topology and traffic not considered for making routing decisions.
  - The choice of the route is computed in advance, offline, and downloaded to the routers when the network is booted.
- Adaptive Routing Algorithms
  - Dynamic: Routing decisions changes to reflect changes in the topology and in the traffic.
  - Differ in where they get their information, when they change the routes and what metric is used for optimization.

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.
- 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.
- Here distance metric is the number of hops.

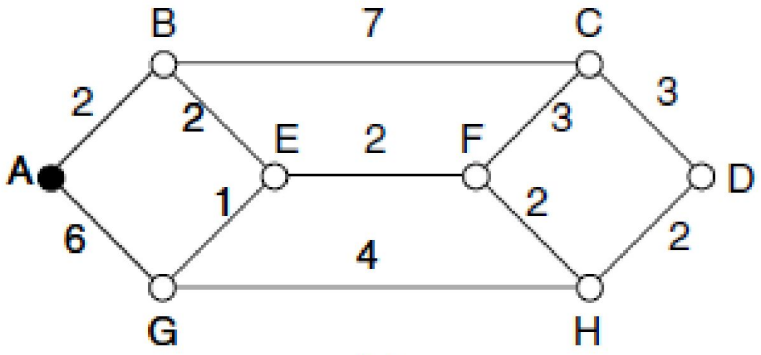


Shortest Path Algorithm

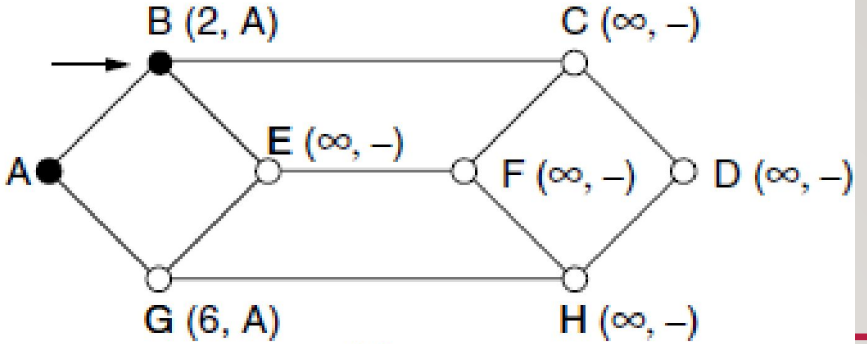
- Simple and easy to understand.
- Network represented as a graph.
- Nodes represent routers.
- Edge represents a communication link.
- Given a pair of routers, the algorithm finds the shortest path between the routers.
- The metric for the shortest path can number of hops, distance, mean delay, average bandwidth, communication cost etc.

Shortest Path Algorithm- Dijkstra's Algorithm

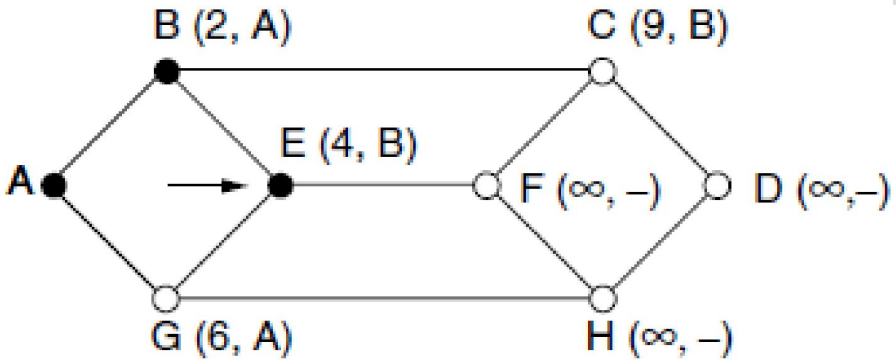
- Dijkstra's algorithm used – finds the shortest path between a source and all destinations in the network.
- Initially all the nodes are labelled with infinity and all the labels are tentative. Source node is set.
- As the algorithm proceeds, the nodes are labelled with its distance from the source along the best known path.
- When the label represents the shortest possible path from the source, it is made permanent.



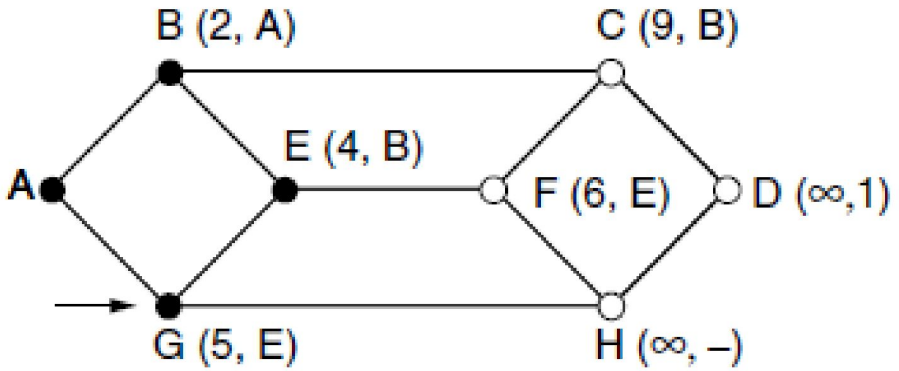
(a)



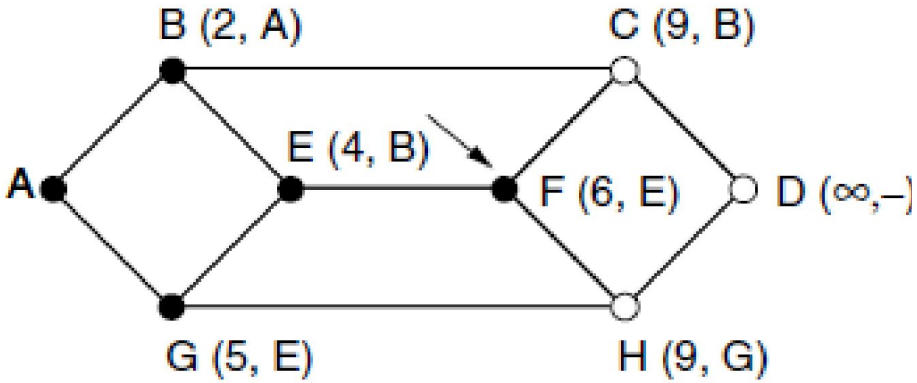
(b)



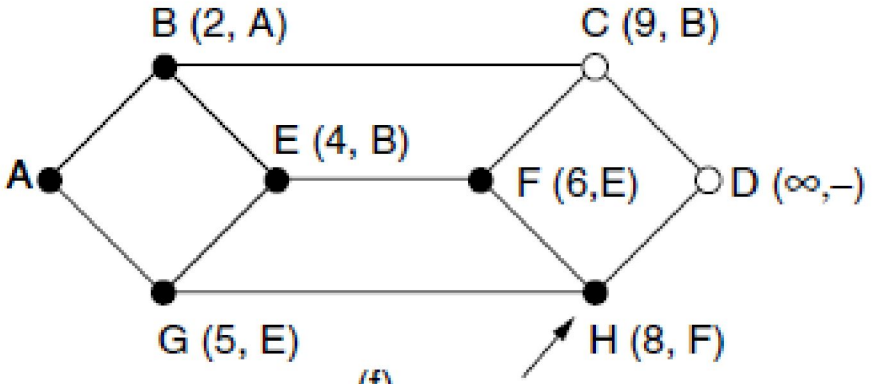
(c)



(d)



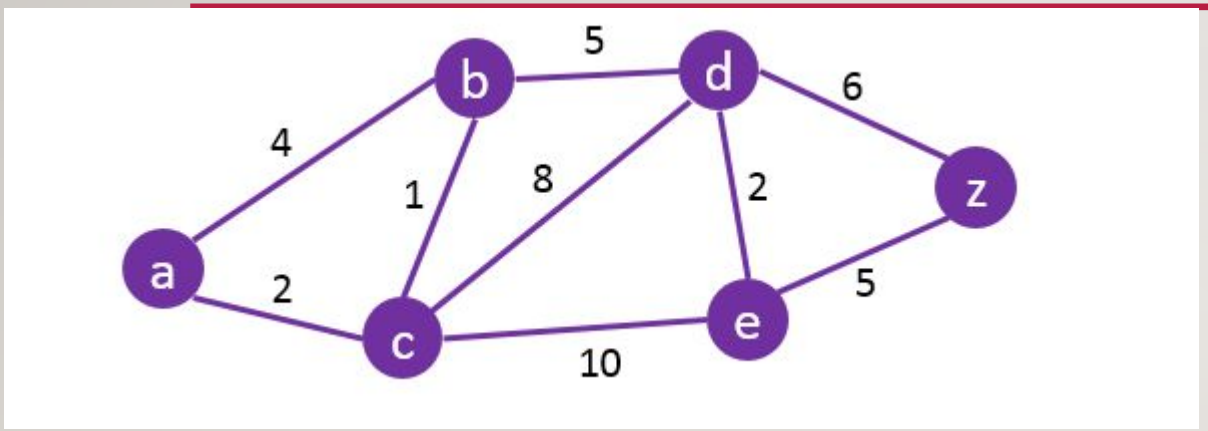
(e)

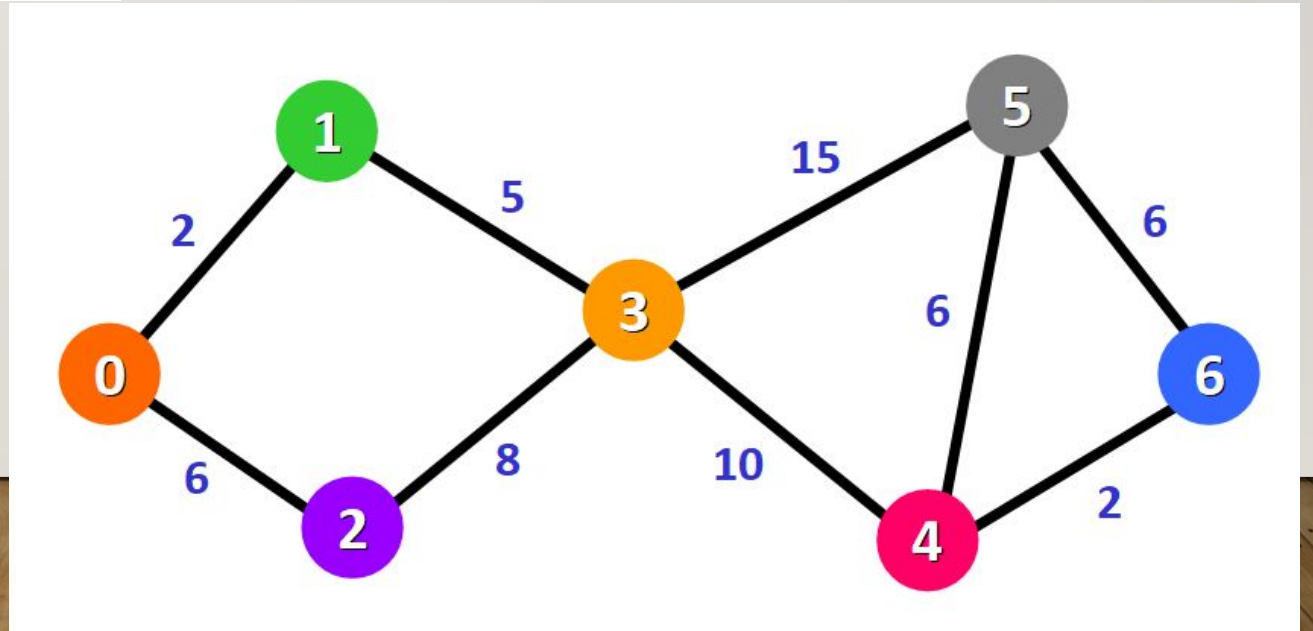


(f)

- Make node A permanent
- Relabel the nodes adjacent to A with the distance to A
- Examine all the tentatively labeled nodes and make the one with the smallest label permanent

Questions..





Algorithm

- An array of distances **dist[ ]** of size |V| (number of nodes), where **dist [s] = 0** and **dist[u] =** ∞ (infinity), where '**s**' represents the source vertex and '**u**' represents a node in the graph except s.
- An array, **Q**, containing all nodes in the graph. When the algorithm runs into completion, **Q** will become empty.
- An initially empty set, **S**, to add the visited node. When the algorithm runs into completion, **S** will contain all the nodes in the graph.

Algorithm

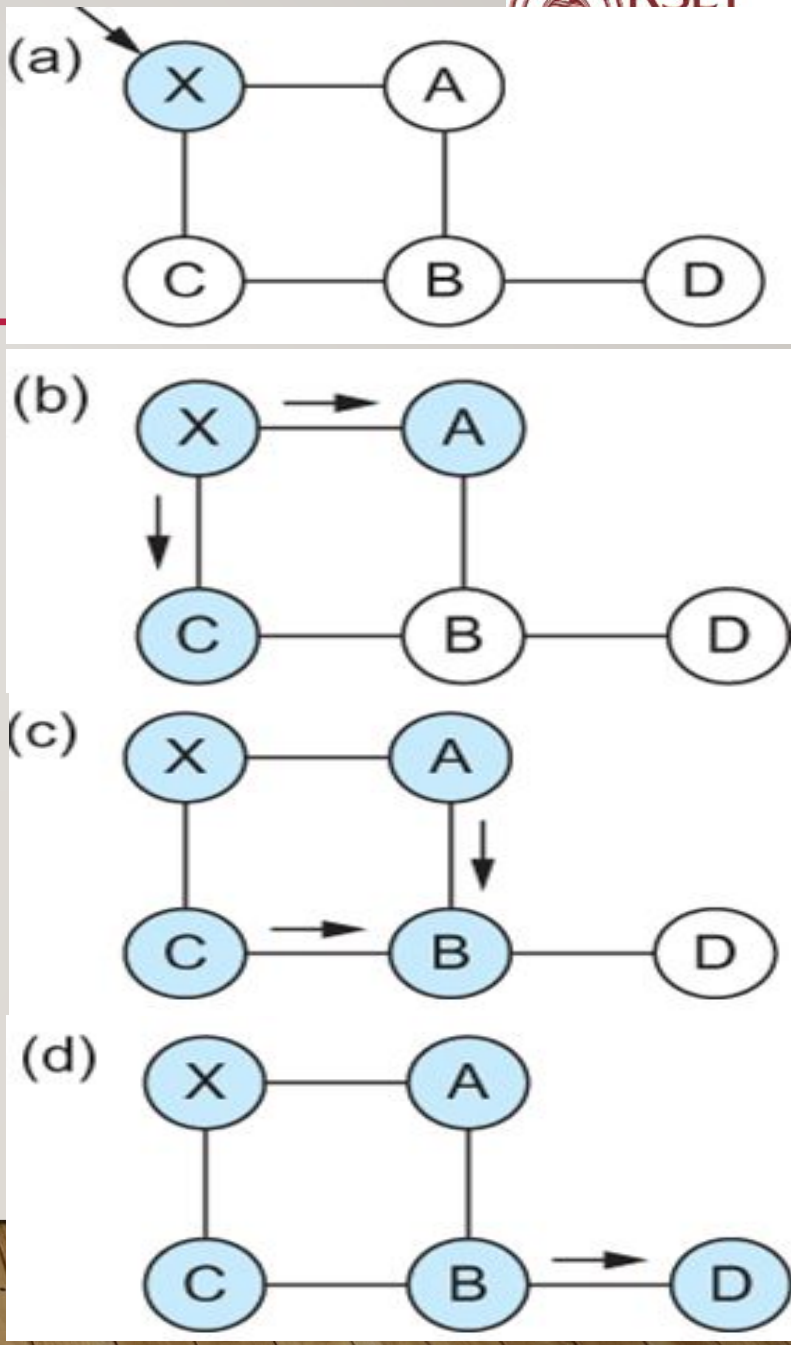
- Repeat while **Q** is not empty –
  - Remove from **Q**, the node, '**u**' having the smallest **dist[u]** and which is not in S. In the first run, **dist[s]** is removed.
  - Add '**u**' to S, marking u as visited.
  - For each node '**v**' which is adjacent to u, update dist[v] as –
    - If (**dist[u] + weight of edge u-v**) **< dist[v],** Then
      - Update **dist[v] = dist[u] + weight of edge u-v**
- The array **dist[ ]** contains the shortest path from s to every other node.

Disadvantages

- It does a blind search, so wastes a lot of time while processing.
- It can't handle negative edges.
- It leads to the acyclic graph and most often cannot obtain the right shortest path.
- Need to keep track of vertices that have been visited.

Flooding

- Non adaptive routing algorithm.
- Every incoming packet is sent out on every outgoing line except the one it arrived on.
- Disadvantage:
  - Duplicate Packets.
- Solution:
  - Source router put a sequence number in each packet it receives from its hosts.
  - Each router maintains a list per source router telling which sequence numbers originating at that source have already been seen.
  - If an incoming packet is on the list, it is not flooded.



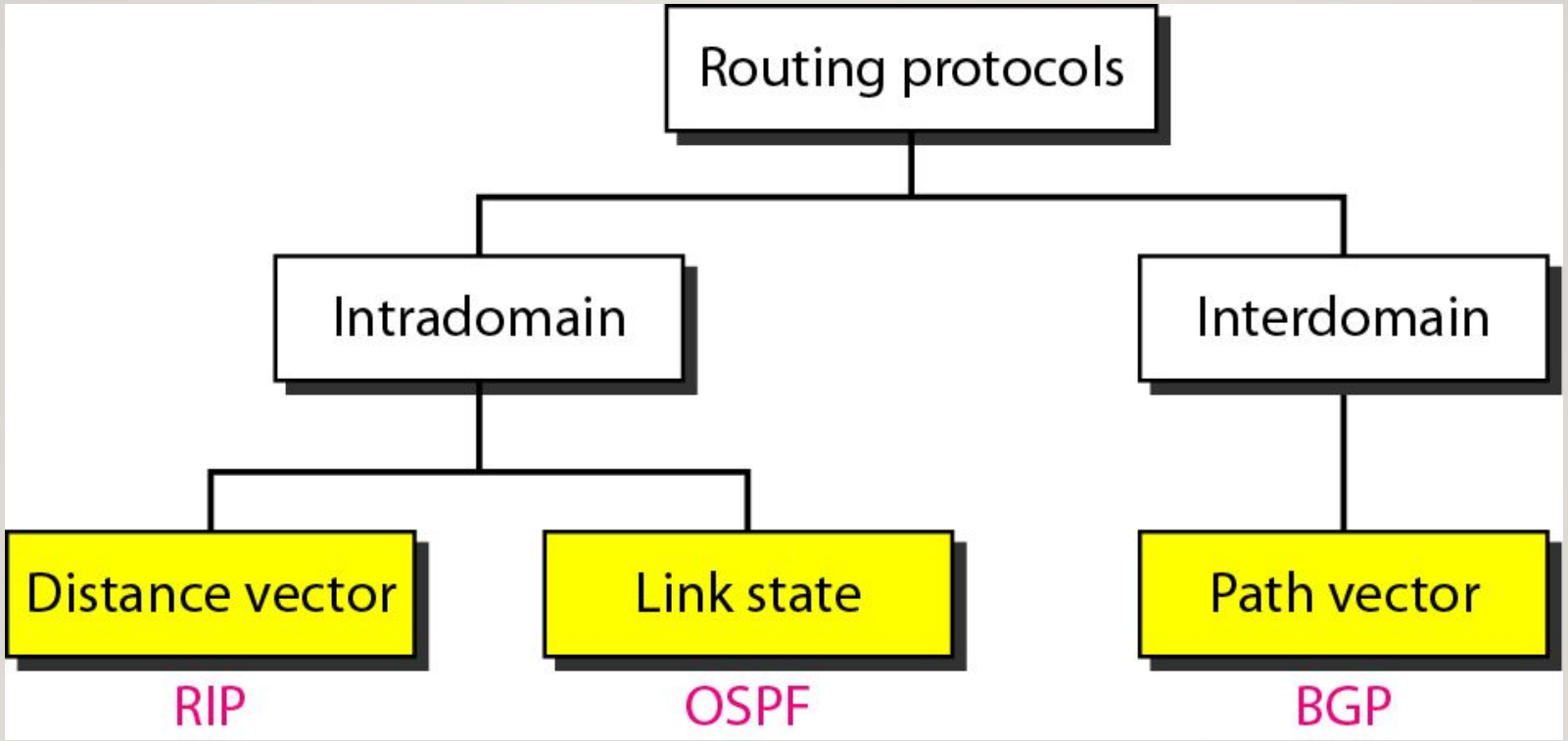
Flooding - Disadvantages

- Flooding tends to create an infinite number of duplicate data packets, unless some measures are adopted to damp packet generation.
- It is wasteful if a single destination needs the packet, since it delivers the data packet to all nodes irrespective of the destination.
- The network may be clogged with unwanted and duplicate data packets. This may hamper delivery of other data packets.

Inter and Intra Domain Routing

- Internet is divided into autonomous systems (AS).
- An AS is a group of networks and routers under the authority of a single administration.
- Routing inside an AS is called intra-domain routing.
- Routing between AS is called inter-domain routing.

Routing Protocols



Distance Vector Routing

- Dynamic (Adaptive) routing algorithm.
- Also known as Bellman – Ford routing algorithm or Ford-Fulkerson algorithm.
- It is used in Internet under the name Routing Information Protocol (RIP).
- Each router maintains a routing table indexed by, and containing one entry for each router in the network.

Distance Vector Routing

- Routing table for a router keeps three pieces of information:
  - destination router.
  - the distance/cost (The distance might be measured as the number of hops or using another metric).
  - the next hop (preferred outgoing line).

Distance Vector Routing- Working

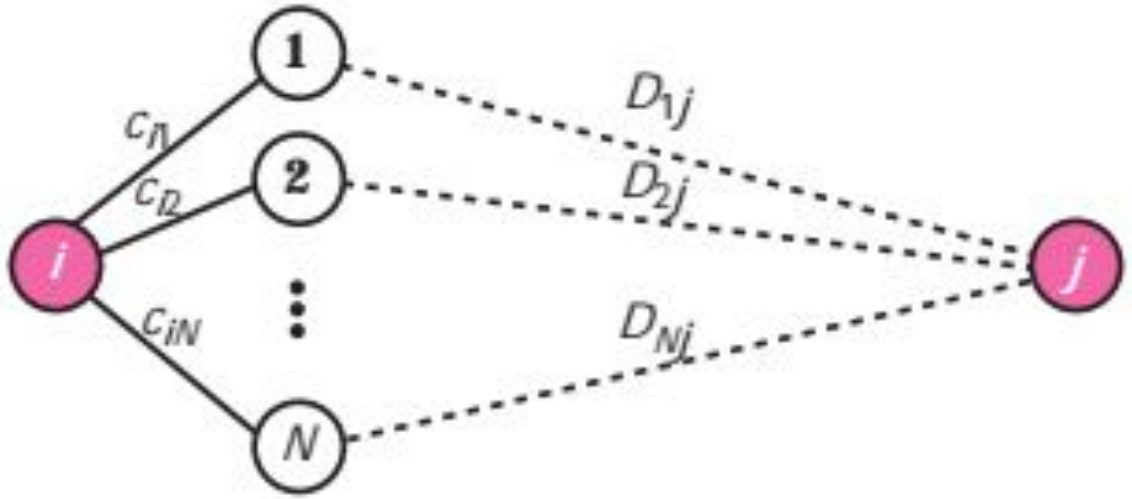
- Every router discovers the identity of the immediate neighbours and knows the distance to each of its neighbours.
- Each router constructs a list containing the distances to all other nodes and distributes this to all its immediate neighbours at regular intervals.
- A router receives this vector from all its neighbours and updates its table.
- After a router has updated its routing table, it should send the result to its neighbours so that they can also update their routing table.

Distance Vector Routing-Bellman Ford Algorithm

$$D_{ij} = \text{minimum } \{(c_{i1} + D_{1j}), (c_{i2} + D_{2j}), \ldots (c_{iN} + D_{Nj})\}$$

Legend

D_{ij} Shortest distance between i and j
c_{ij} Cost between i and j
N Number of nodes



Distance Vector Routing-Shortest Distance Table

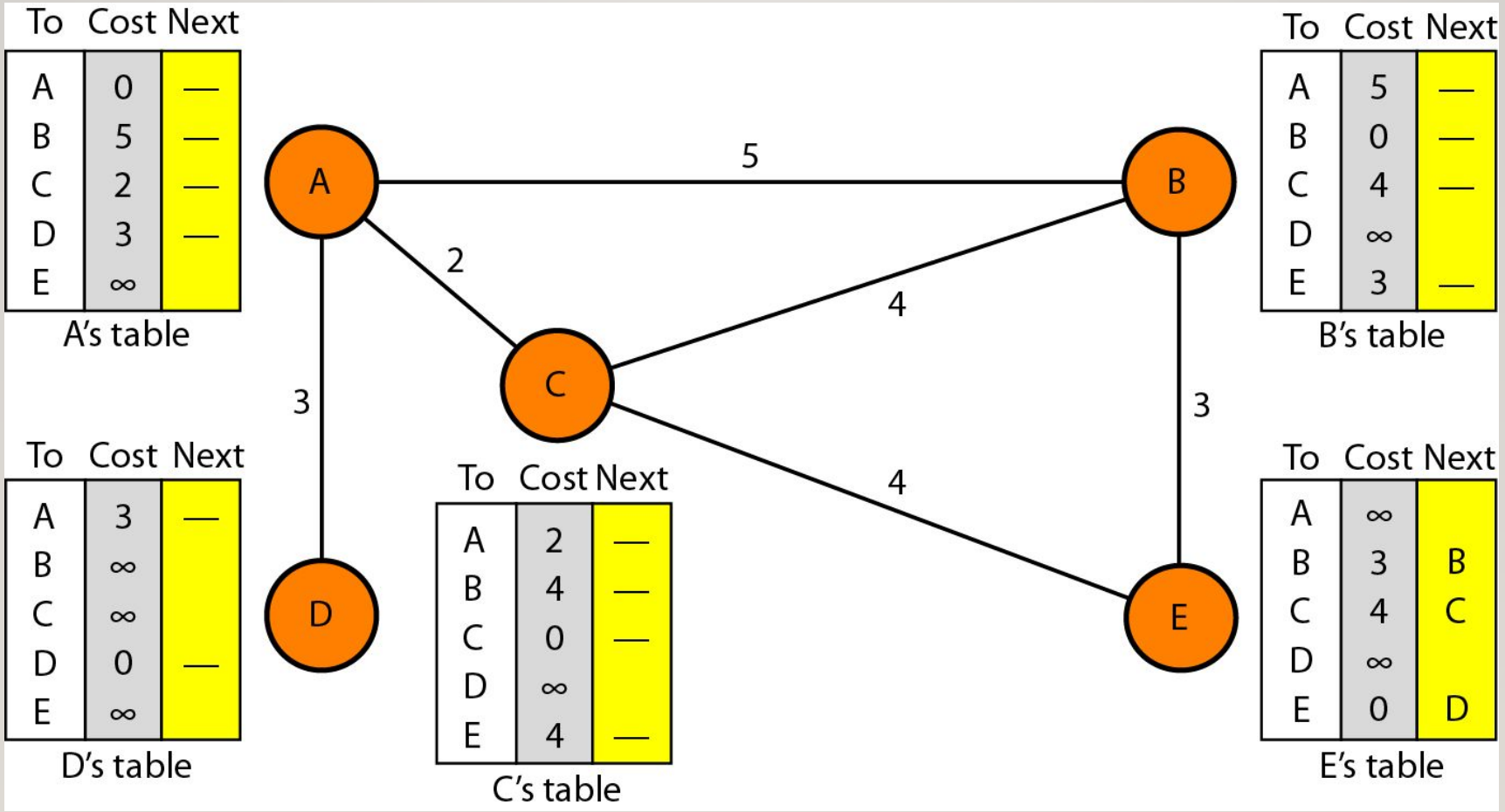
- Create a shortest distance table for each node:
  - Shortest distance and cost between a node and itself is initialized to 0.
  - Shortest distance between a node and any other node is set to infinity.
  - Cost between a node and any other node will be available if connected, else infinity.
- Run the algorithm.
- Cost- hop count

```
Bellman_Ford ( )
{
    // Initialization
    for (i = 1 to N; for j = 1 to N)
    {
        if(i == j)   D_ij = 0    c_ij = 0
        else         D_ij = ∞    c_ij = cost between i and j
    }
    // Updating
    repeat
    {
        for (i = 1 to N; for j = 1 to N)
        {
            D_ij ← minimum [(c_i1 + D_1j)  ...  (c_iN + D_Nj)]
        } // end for
    } until (there was no change in previous iteration)
} // end Bellman-Ford
```

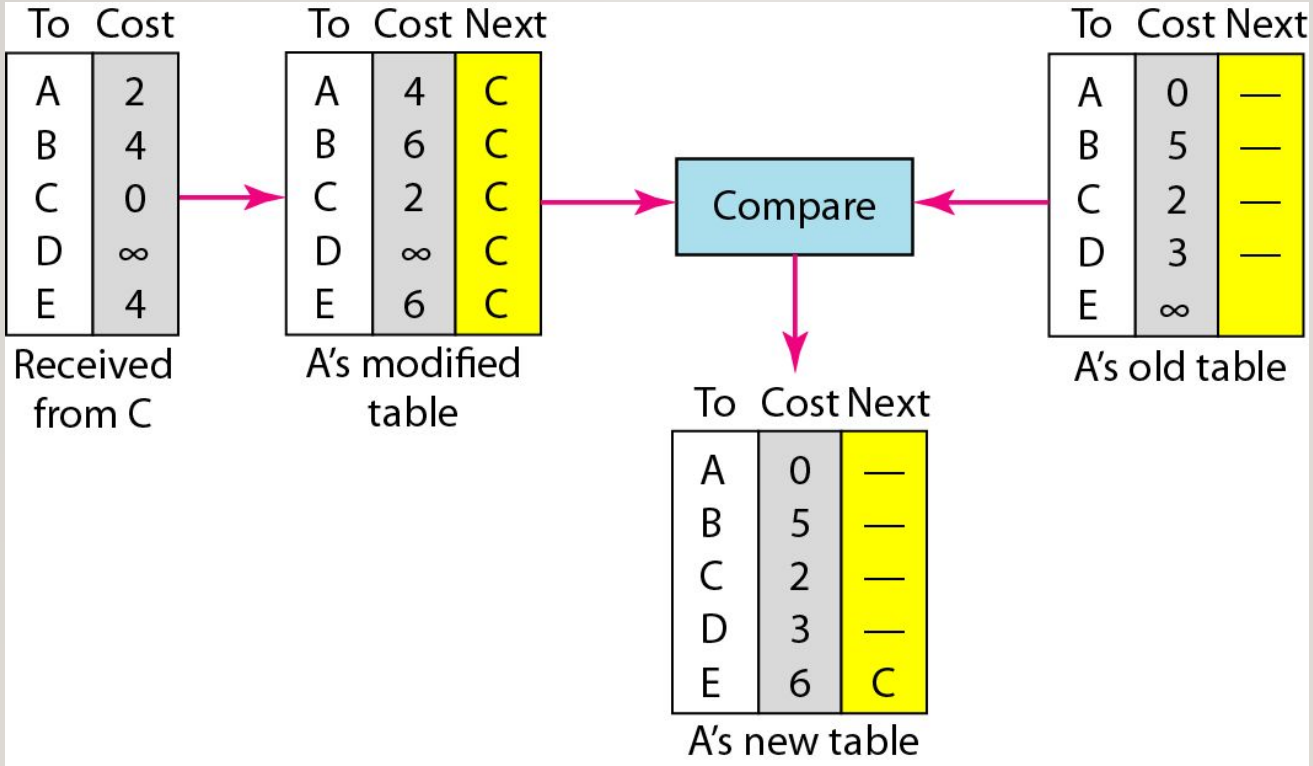
Distance Vector Routing- Steps

- Initialization
  - Each node knows distance between itself and immediate neighbour only. Others are marked as infinity.
- Sharing
  - Nodes share their routing table with immediate neighbours periodically when there is a change.
- Updating
  - Update the infinity values using information obtained.

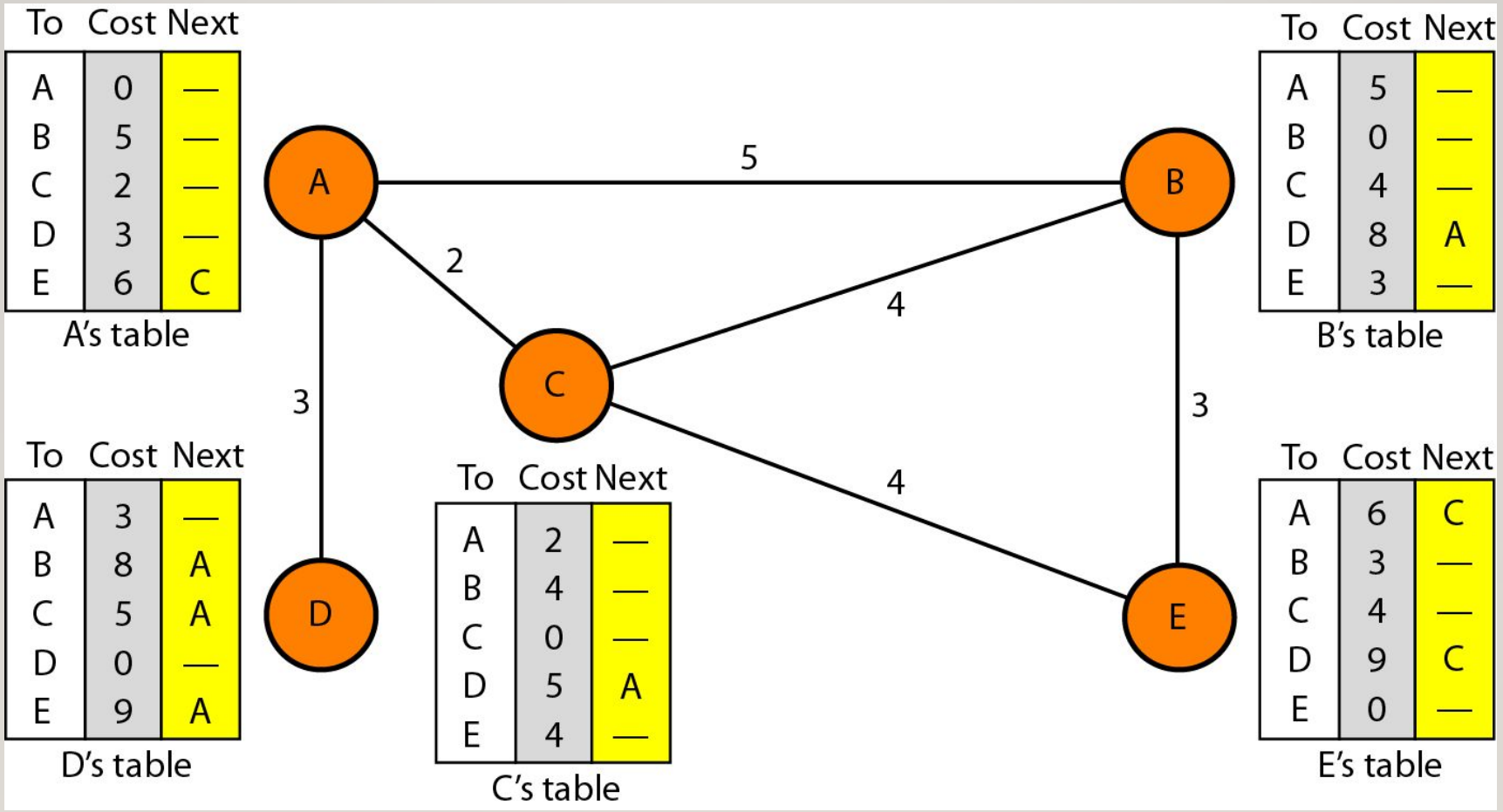
Example : ***Step1: Initialization of tables in distance vector routing***



Step 2: Updating in distance vector routing



Distance vector routing tables



Updating The Routing Table

- If the next hop entry is different:
  - If new value is smaller than cost in table, take new one.
  - If there is a tie, the old one is kept.
  - If entry not in table, then add to the table.

When To Share the Routing Table??

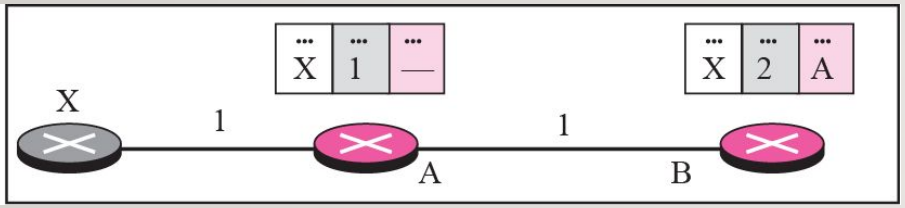
- Periodic Update
  - A node sends its routing table, normally every 30 s, in a periodic update. The period depends on the protocol that is using distance vector routing.
- Triggered Update
  - A node sends its routing table to its neighbors anytime there is a change in its routing table.

Limitations of DVR- Count To Infinity Problem.

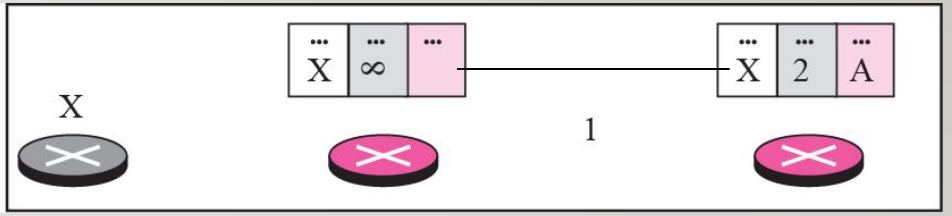
- The settling of routes to best paths across the network is called Convergence.
- It converges to the correct route, but it may do so slowly.

Count To Infinity Problem

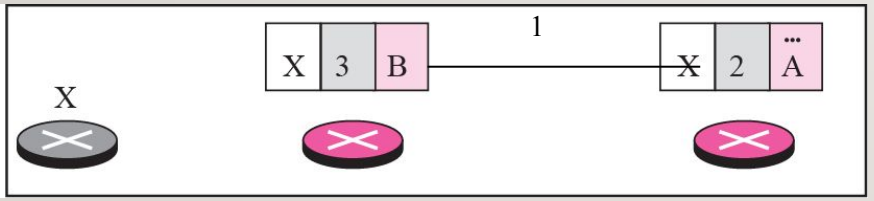
Before failure



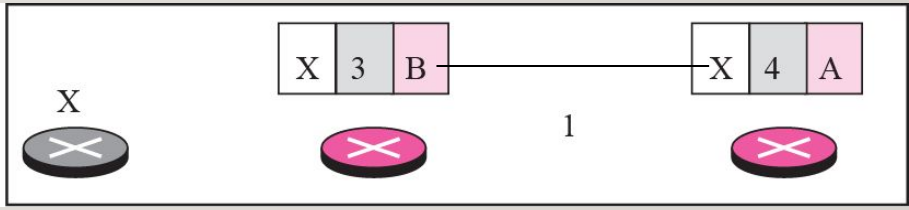
After failure



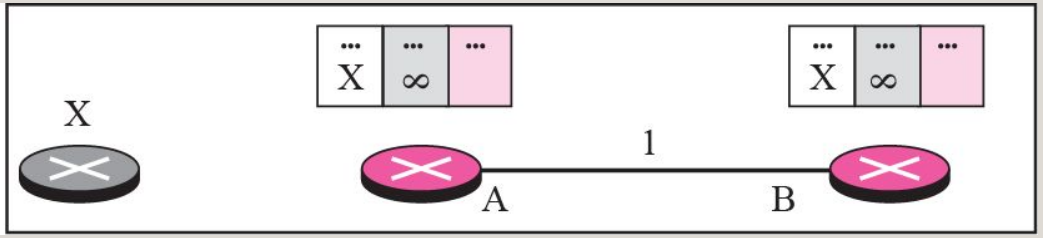
After A receives update from B



After B receives update from A



Finally



SOLUTION

- Defining infinity
  - Most implementations define 16 as infinity. So DVR cannot be used in large systems. Maximum 15 hops only allowed.
- Split Horizon
  - Instead of flooding the table through each interface, each node sends only part of its table through each interface. So even if some connections are mistaken to be true, confusions wont be created.

COMPARISON

Parameter	Bellman-Ford	Dijkstra
Overheads	More	Less
Scalability	Less	More
Quality of the best available route	Less	More
Negative edges	Yes	No
Delay	More	Less

RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

Link State Routing

- If each node in the domain has the information on entire topology of the domain- the list of nodes, links, how they are connected, type, cost and condition of links:
  - Then Dijkstra's algorithm can be used to build a routing table.
- But the topology is dynamic, it represents the latest situation of each node and link. If there are any changes in the network, topology must be updated.
- For this a partial knowledge of the topology is maintained at every node- Link state knowledge.

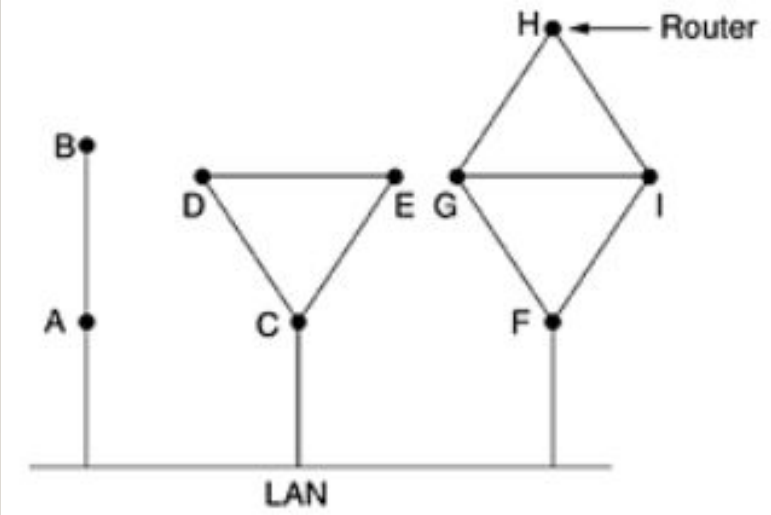
RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

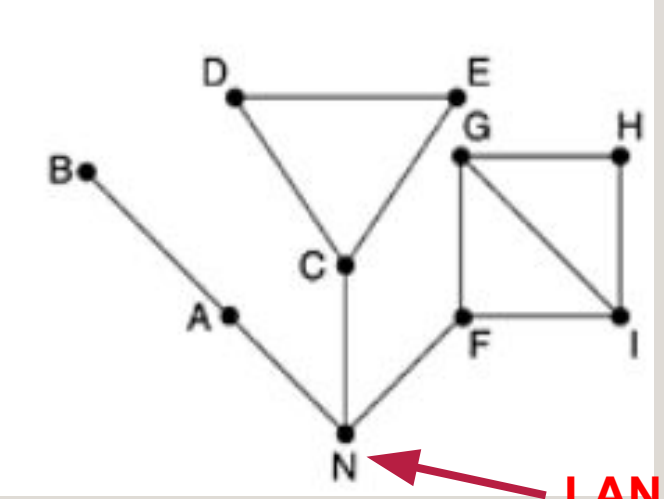
Steps In Link State Routing

- Each router must:
  1. Discover its neighbours and learn their network addresses.
  2. Measure the delay or cost to each of its neighbours.
  3. Construct a packet telling all information just learned.
  4. Send this packet to all other routers.
  5. Compute the shortest path to every other router.

~~Learning About Neighbours~~

- On booting, the router will send a HELLO packet on each of its links.
- The router on the other end will send back a reply which contains its network address.





LAN represented as a node

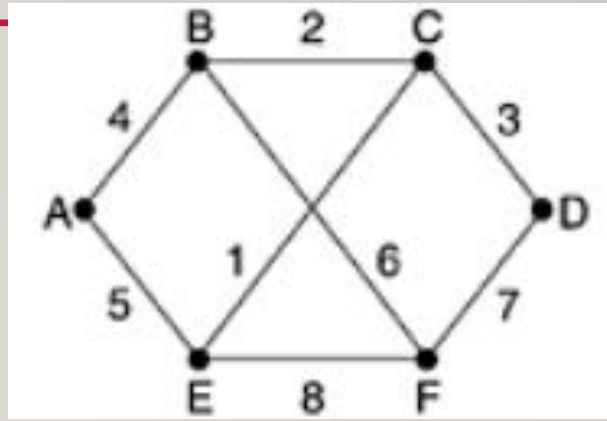
RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

~~Measuring The Link Cost~~

- LSR algorithm requires each link to have a distance or cost metric for finding shortest paths.
- The Cost to reach neighbours can be set automatically or configured by the network operator.
- The most common way to determine this cost is by sending ECHO packets and measuring the round trip time and dividing it by two.

Building Link State Packets

- Router builds a packet that contains:
  - Identity of the sender.
  - Sequence number.
  - Age- bound the maximum lifetime of a link state packet in the network.
  - List of neighbours and the cost to each.



Link State Packets

A		B		C		D		E		F	
Seq.		Seq.		Seq.		Seq.		Seq.		Seq.	
Age		Age		Age		Age		Age		Age	
B	4	A	4	B	2	C	3	A	5	B	6
E	5	C	2	D	3	F	7	C	1	D	7
		F	6	E	1			F	8	E	8

~~Building Link State Packets~~

- When to build the packet?
  - Build them periodically at regular intervals.
  - Build them when some significant event occurs, such as a line or neighbour going down or coming back up again.

Distributing The Link State Packets

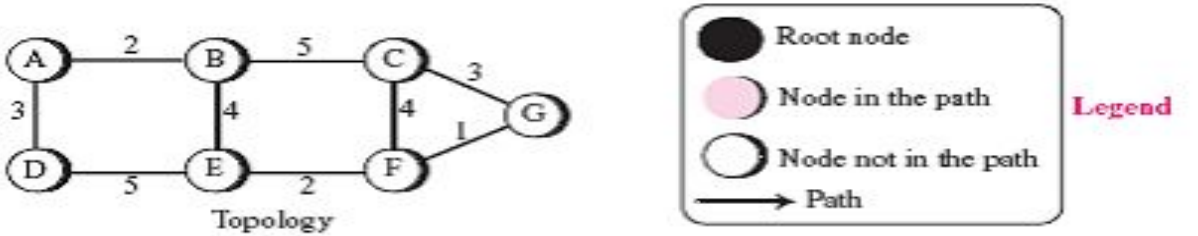
- Flooding is used to disseminate this information.
- A node will sent its LSP out on all its directly connected links.
- Each node that receives the LSP from some node will check if it already has a copy of the LSP.
    - If not it will store it and will sent it out on all its links.
    - If it already has a copy it will compare the SEQNO.
        - If the new LSP has a larger SEQNO; it is more recent – so this LSP is stored and is sent out on all its links.
        - If the new LSP has a smaller (or equal) SEQNO it is discarded.

~~Distributing The Link State Packets~~

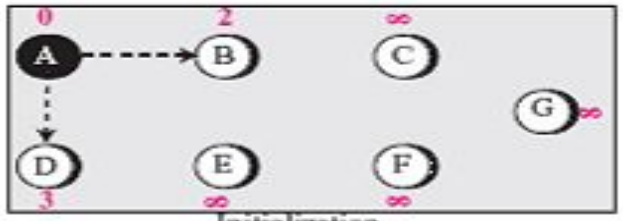
- Problems with comparing sequence number:
  - If a router crashes, it will lose track of its sequence number. If it starts again at 0, the next packet it sends will be rejected as a duplicate.
- Solution: Use the **age** field
  - When a router generates a LSP, it sets its lifetime (usually measured in seconds) in the *age* field
  - Decrement age once per second.
  - When age hits zero, the information from that router is discarded.
  - Helps to make sure that no packet live for an indefinite period of time.
  - LSPs from a failed router does not remain.

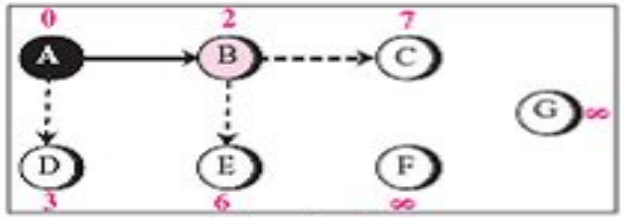
~~Computing The New Routes~~

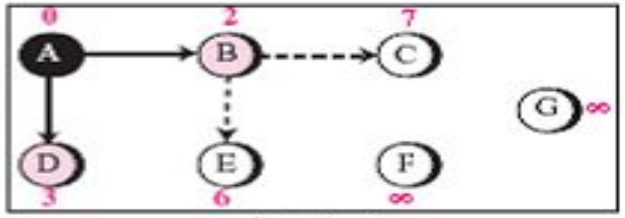
- When a router gets the full set of LSPs, it constructs the routing table.
  - Use Dijkstra algorithm is used to find the shortest path to all destinations.
  - Then construct the routing table.

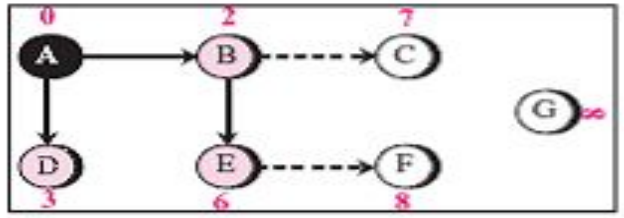


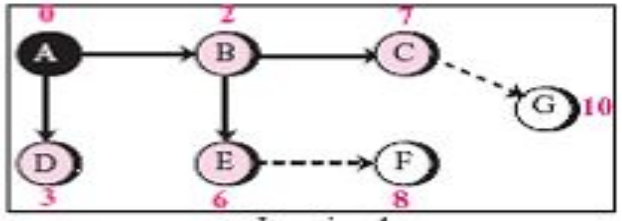
Topology

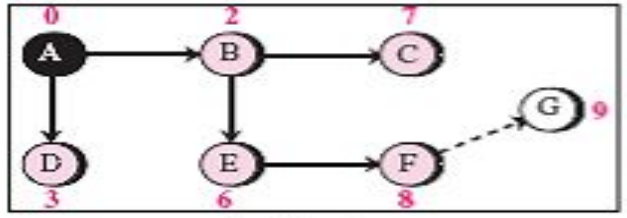

Initialization

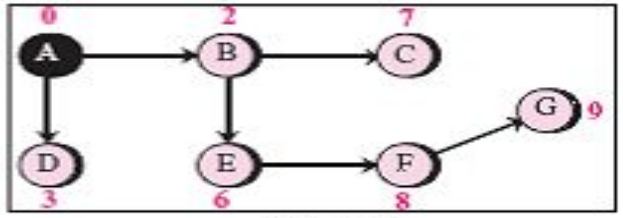

Iteration 1


Iteration 2


Iteration 3


Iteration 4


Iteration 5


Iteration 6

Routing table for node A

Destination	Cost	Next router
A	0	-
B	2	-
C	7	B
D	3	-
E	6	B
F	8	B
G	9	B

Limitations

- They require more memory and processor power than distance vector protocols. This makes it expensive to use for organizations with small budgets and legacy hardware.
- They require strict hierarchical network design, so that a network can be broken into smaller areas to reduce the size of the topology tables.
- They require an administrator who understands the protocols well.
- They flood the network with LSPs during the initial discovery process. This process can significantly decrease the capability of the network to transport data. It can noticeably degrade the network performance.

Link State routing algorithm	Distance Vector routing algorithm
The network topology and all the link costs are the input to this algorithm.	The input to the algorithm is all the associated costs with the current node to all its neighbors.
It computes the least-cost path from source to destination with a complete knowledge on the network.	It computes the least-cost path in an iterative and distributed manner.
The shortest path is calculated using dijkstras algorithm.	The shortest cost path is calculated using Bellman Ford algorithm.
Open Shortest Path First (OSPF) is an example of link state routing algorithm.	Routing Information Protocol (RIP) is an example of distance vector routing algorithm.

THANK YOU!!!

COMPUTER NETWORKS

MS. JINCY J. FERNANDEZ

ASST. PROF, CSE

RSET

RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

Multicast Routing

- Some applications require widely separated processes to work together in groups.
- It may be required for 1 process to send messages to all other members of the group.
- Broadcasting and unicasting may not be good in these cases.
- So go for multicasting: sending messages to well-defined groups that are numerically large in size, but small compared to the network as a whole.
- Routing algorithm for performing multicasting is called multicast routing.
- A single router in a network can be part of two or more different groups.
- Multicasting requires group management.

Multicast Routing

- There should be provision to create, destroy groups, join and leave groups.
- Main concern of the routing algorithm is to identify which routers are members of a group.
- Hosts can then inform their routers about changes in the network.
- Each group is identified by a multicast address and that routers know the groups to which they belong.
- To do multicast routing, each router computes a spanning tree covering all other routers.

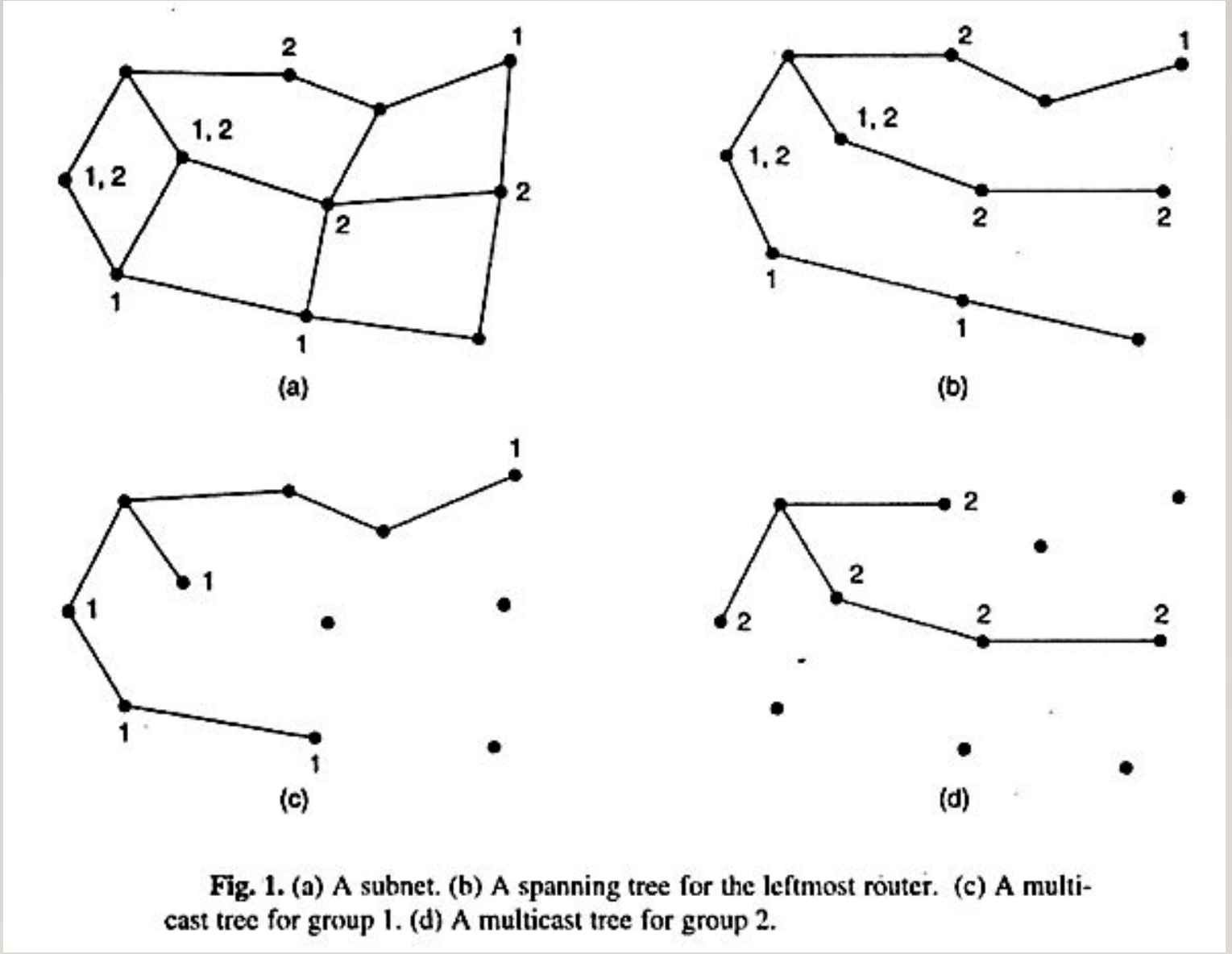


Fig. 1. (a) A subnet. (b) A spanning tree for the leftmost router. (c) A multicast tree for group 1. (d) A multicast tree for group 2.

Working

- When a process sends a multicast packet to a group, the first router examines its spanning tree and prunes it, removing all lines that do not lead to hosts that are members of the group.
- In previous example, Fig. 1(c) shows the pruned spanning tree for group 1. Similarly, Fig. 1(d) shows the pruned spanning tree for group 2.
- Multicast packets are forwarded only along the appropriate spanning tree.

How To Prune?- Multicast Distance Vector

- Extension of Unicast routing.
- Uses the source-based tree approach to multicasting.
- Each router that receives a multicast packet to be forwarded implicitly creates a source-based multicast tree in 3 steps:
  - Router uses an algorithm called **Reverse Path Forwarding (RPF)** to simulate creating part of the optimal source-based tree between source and itself.
  - Router uses an algorithm called **Reverse Path Broadcasting (RPB)** to create a broadcast spanning tree whose root is the router itself and whose leaves are all networks in the internet.
  - Router uses an algorithm called **Reverse Path Multicasting (RPM)** to create a multicast tree by cutting some branches of the tree that end in networks with no member in the group.

How To Prune?-Link State Routing

- The simplest one can be used if link state routing is used, and each router is aware of the complete subnet topology, including which hosts belong to which groups.
- Then the spanning tree can be pruned by starting at the end of each path and working toward the root removing all routers that do not belong to the group in question.

How To Prune?- Multicast Distance Vector

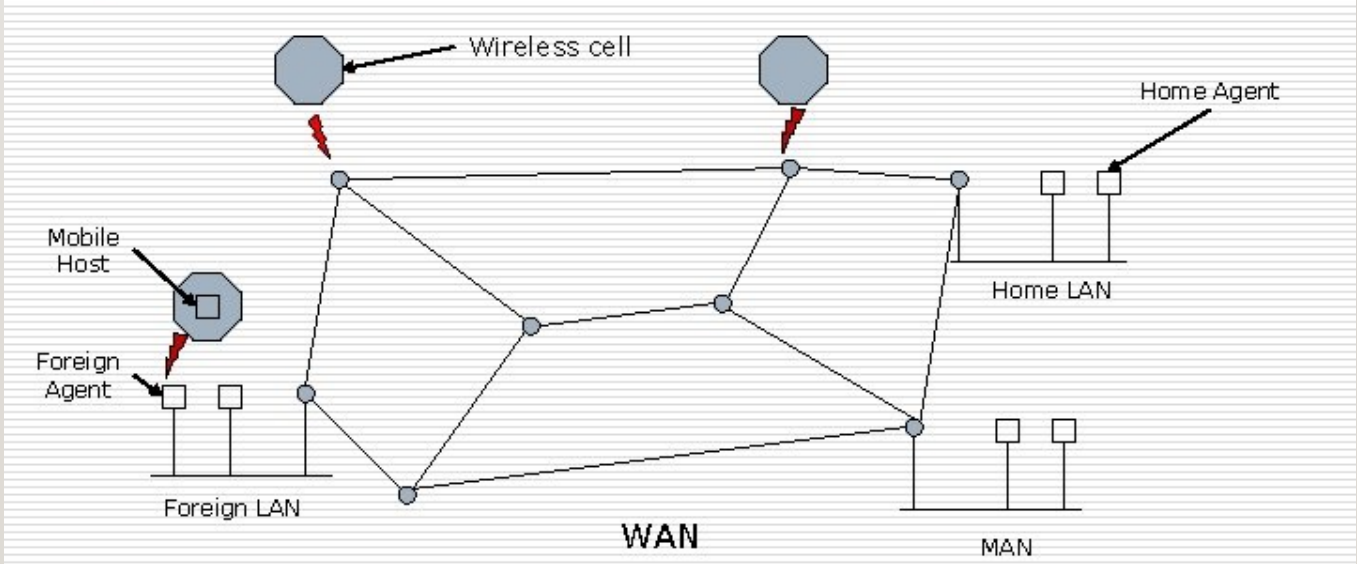
- With distance vector routing, a different pruning strategy can be followed. The basic algorithm is reverse path forwarding. However, whenever a router with no hosts interested in a particular group and no connections to other routers receives a multicast message for that group, it responds with a PRUNE message, telling the sender not to send it any more multicasts for that group. When a router with no group members among its own hosts has received such messages on all its lines, it, too, can respond with a PRUNE message. In this way, the subnet is recursively pruned.

Types of Multicast Routing Protocol

- 1) Multicast Distance Vector Routing Protocol (DVMRP)
- 2) Multicast Link State (MOSPF)
- 3) Protocol Independent Multicast (PIM)

Routing For Mobile Hosts

- People use portable computers and devices nowadays.
- Routing of packets to such devices is also necessary.
- Mobile Hosts: Hosts that move from one network to another.



Routing For Mobile Hosts

- Two addresses for a mobile host:
  - Home address: a permanent address that associates the hosts with its **home network** (home location).
  - Care of address: a temporary address; it changes when a host moves from one network to another. It is associated with the **foreign network** (the network to which the host moves).
- The role of routing is to make it possible to send packets to mobile hosts using their fixed home addresses and have the packets efficiently reach them wherever they may be.

RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY (AUTONOMOUS)

Mobile Host Routing

- World is divided geographically into areas.
- Home location will have a home agent (a router attached to the home network of the mobile host).
- Home agent acts on behalf of the mobile host when a remote host sends a packet to the mobile host.
- Each area has a foreign agent that keep track of mobile hosts visiting an area.
- Once the home agent knows where the mobile host is currently located, it can forward packets so that they are delivered to the mobile host.

Mobile Host Routing- Working- 3 phases

1. Agent Discovery
   - Mobile host must learn the address of the home agent before it leaves the network.
   - Mobile host must discover a foreign agent after it has moved to a foreign network.
   - Discovery involves two types of messages:
     - Agent Advertisement: router advertise its presence on the network if it acts as an agent.
     - Agent Solicitation: When a mobile host has moved to a new network and has not received agent advertisement, it can initiate agent solicitation.

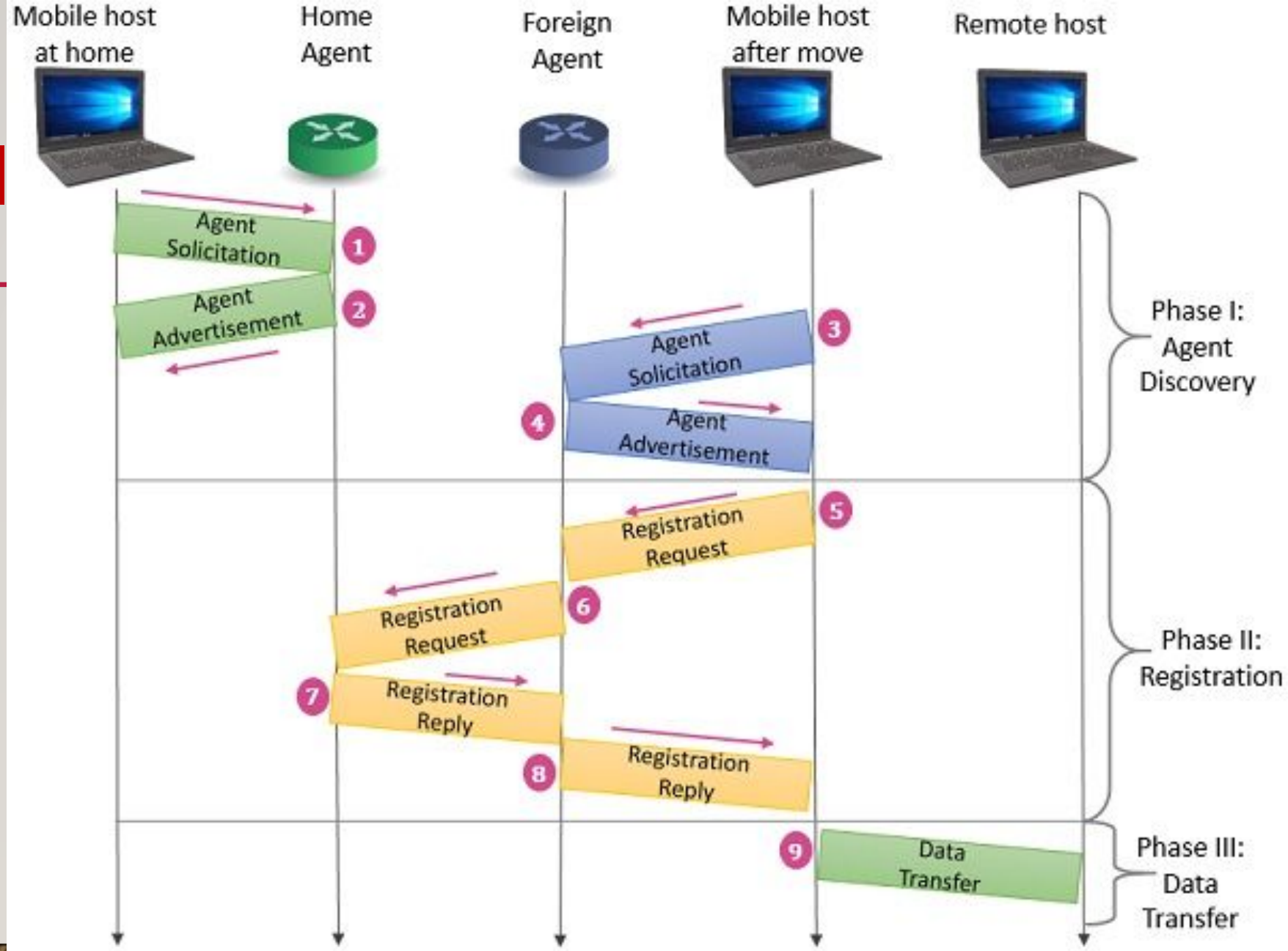
Mobile Host Routing- Working- 3 phases

2. Registration
   - After a mobile host has moved to a foreign network and discovered the foreign agent, it must register.
   - Aspects of Registration
     - Mobile hosts registers with the foreign agent and home agent.
     - Mobile host must renew the registration if it has expired.
     - Mobile host must cancel its registration when it returns home.
   - Mobile host uses a registration request and registration reply to register with the foreign agent and the home agent.

Mobile Host Routing- Working- 3 phases

2. Registration :
   - Request and Reply
     - Send registration request from the mobile host to the foreign agent to register its care of address and to announce home address and home agent address.
     - Foreign agent relays the message to the home agent.
     - Home agent knows the address of the foreign agent.
     - A registration reply is sent from the home agent to the foreign agent and then relayed to the mobile host.
     - The reply confirms or denies the registration request.

Mobil



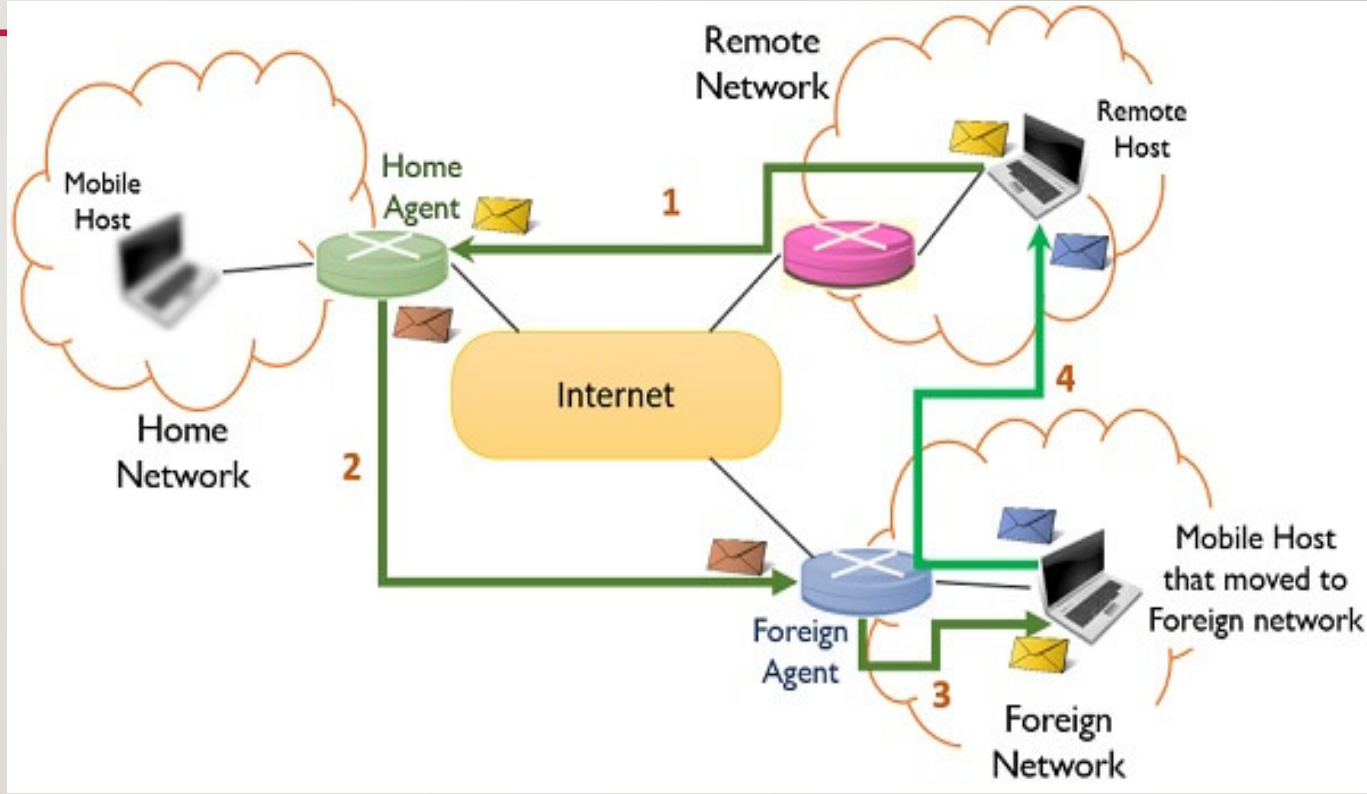
Communication Between Mobile Host and Remote Host

Mobile Host Routing- Working- 3 phases

3. Data Transfer
   - A mobile host can communicate with the remote host.

   a) Remote host sends to home agent.

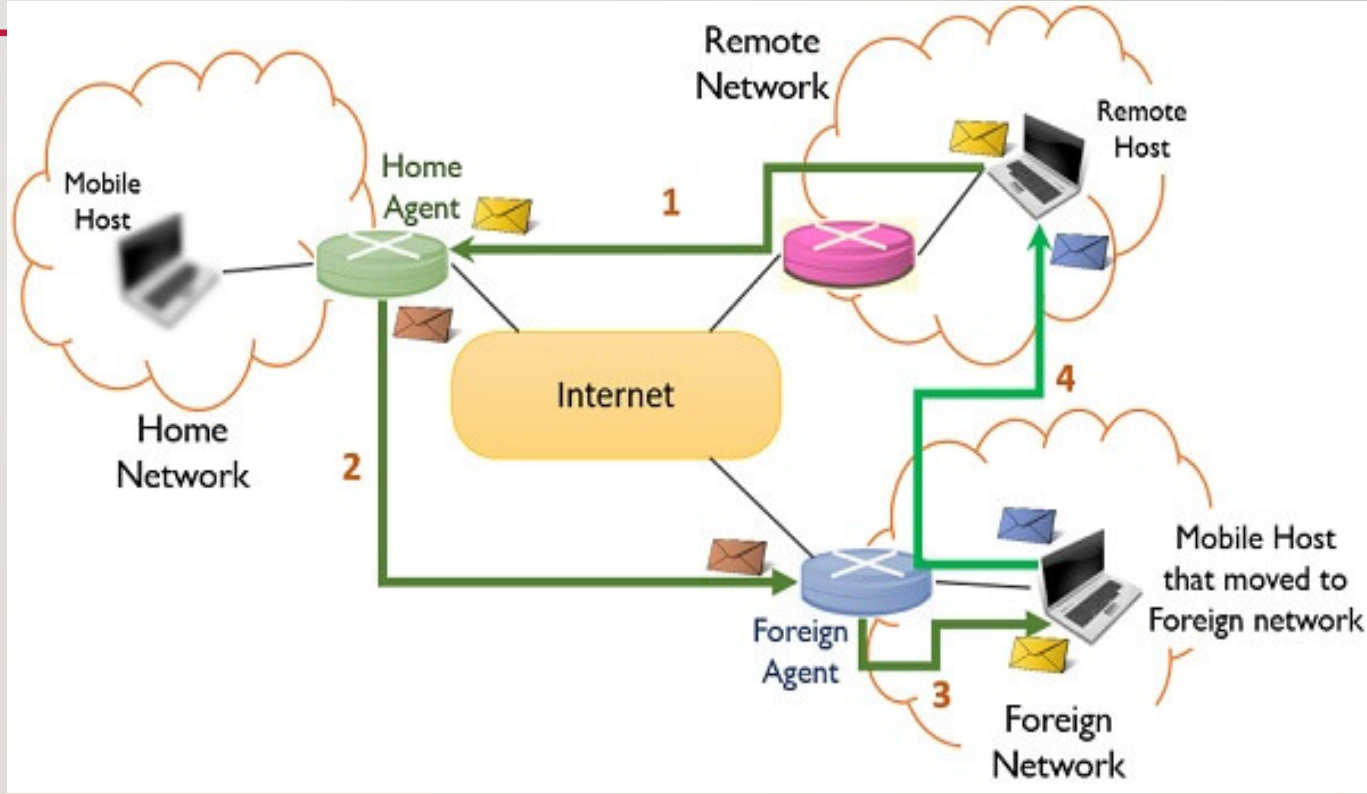
   b) Home agent then wraps or encapsulates the packet with a new header and sends this bundle to the foreign agent- This mechanism is called tunneling.



Mobile Host Routing- Working- 3 phases

3. Data Transfer

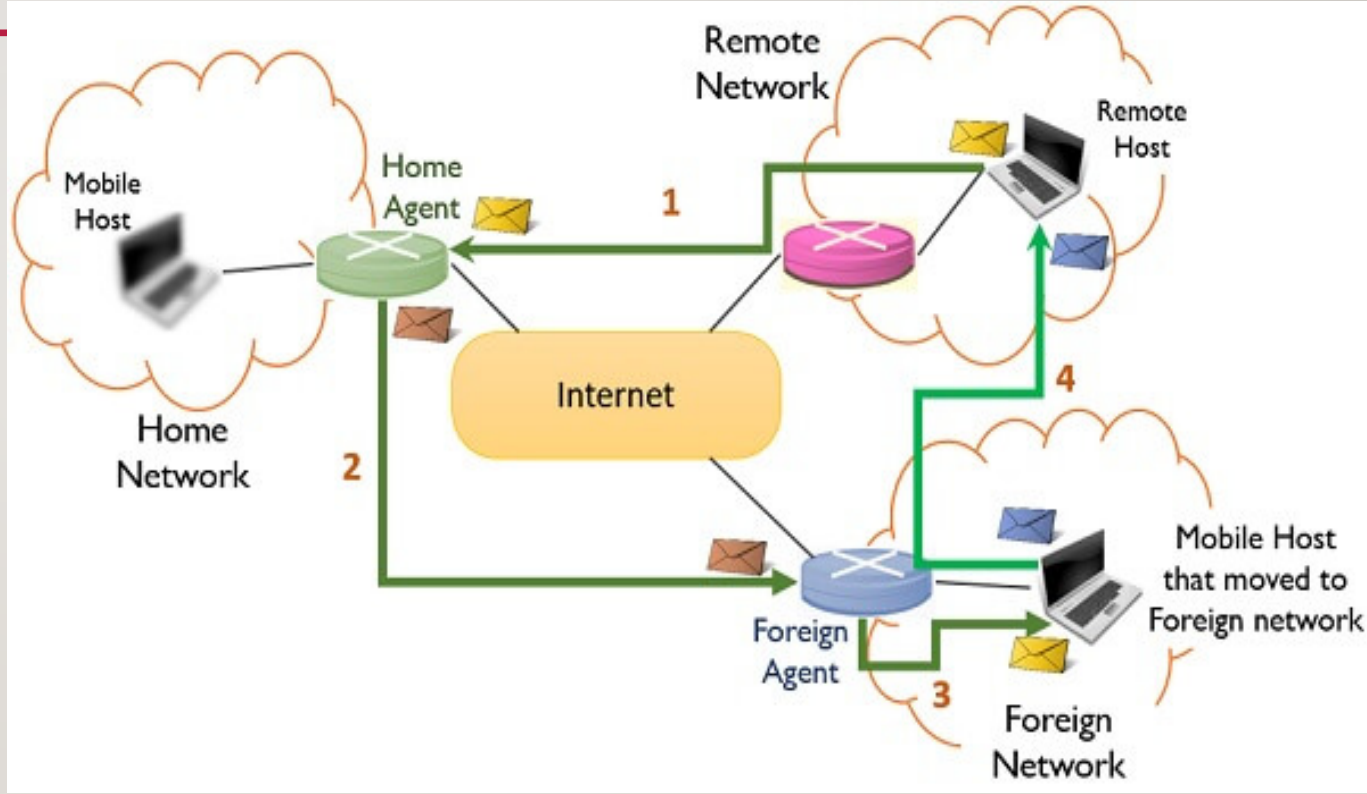
   c) When foreign agent receives the packet, it takes the original packet. Foreign agent consults a registry table to find the care of address of the mobile host. Send the packet to the care of address.



Mobile Host Routing- Working- 3 phases

3. Data Transfer

   d) Normal data transfer if mobile host wants to send to a remote host.



THANK YOU!!!

COMPUTER NETWORKS

MS. JINCY J FERNANDEZ

ASST. PROF, CSE

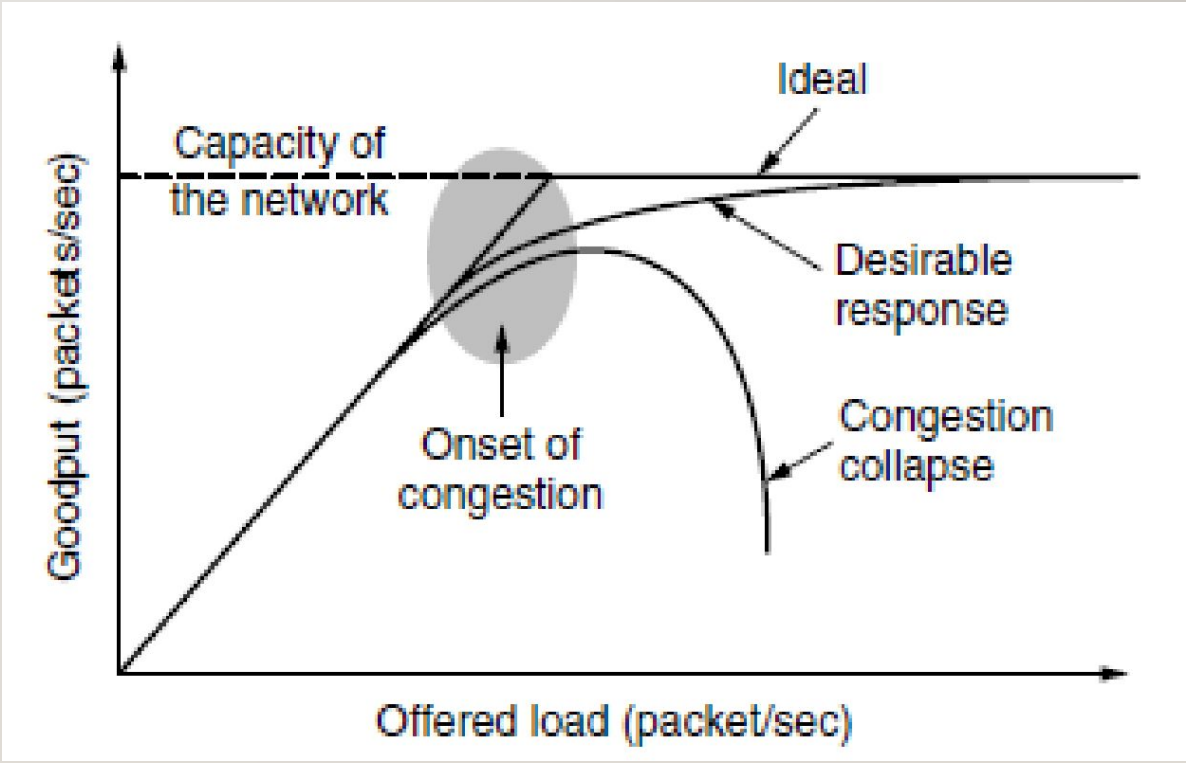
RSET

Congestion Control Algorithms

- Congestion: Too many packets in the network cause packet delay and loss that degrades the performance.
- The network and transport layers share the responsibility for handling congestion.
- The most effective way to control congestion is to reduce the load that the transport layer is placing on the network.

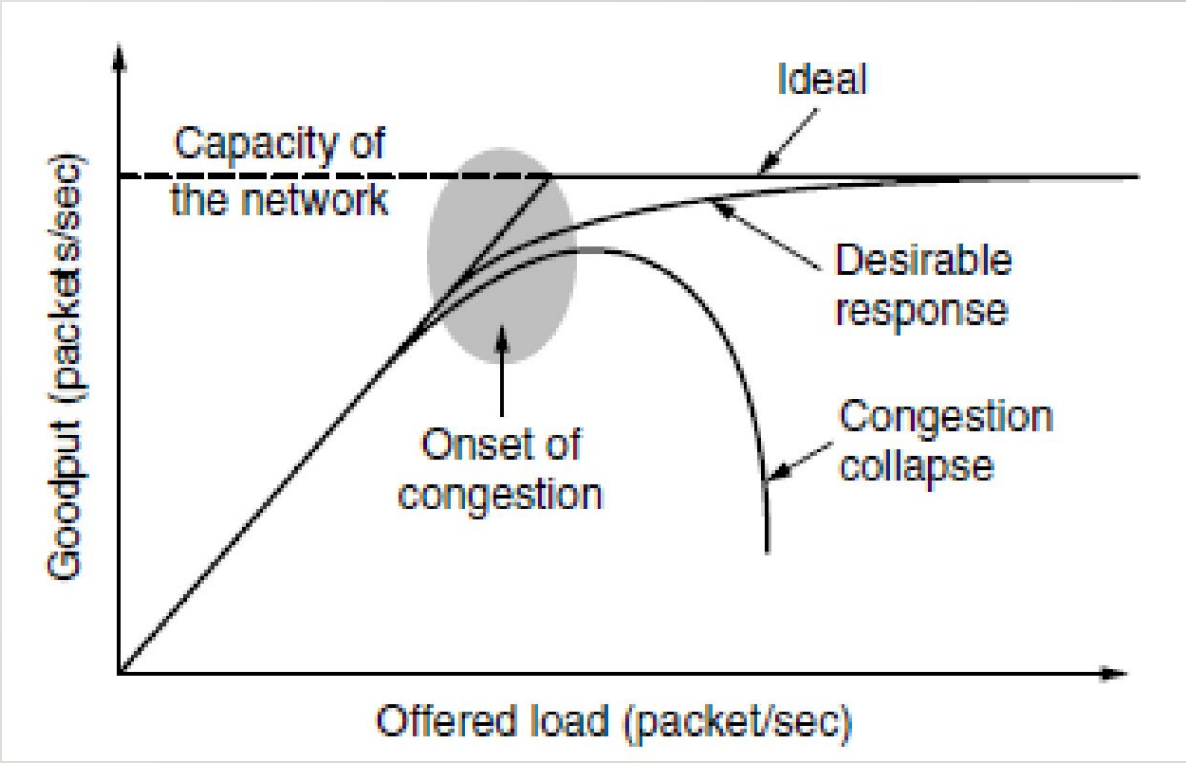
Congestion

- When the number of packets the hosts sent is within the carrying capacity, the number of packets delivered will be proportional to the number of packets sent.
- As the offered load approaches the carrying capacity, bursts of traffic fills up the buffers inside the routers & some packets are lost.
- The lost packets consume some of the capacity, so the number of delivered packets falls below the ideal curve.



Congestion

- Goodput:
  - The rate at which *useful* packets are delivered by the network.
  - Duplicate copies of the same packet delivered is not considered.
- Congestion Collapse:
  - Performance rapidly drops as the offered load increases beyond the capacity.



Congestion

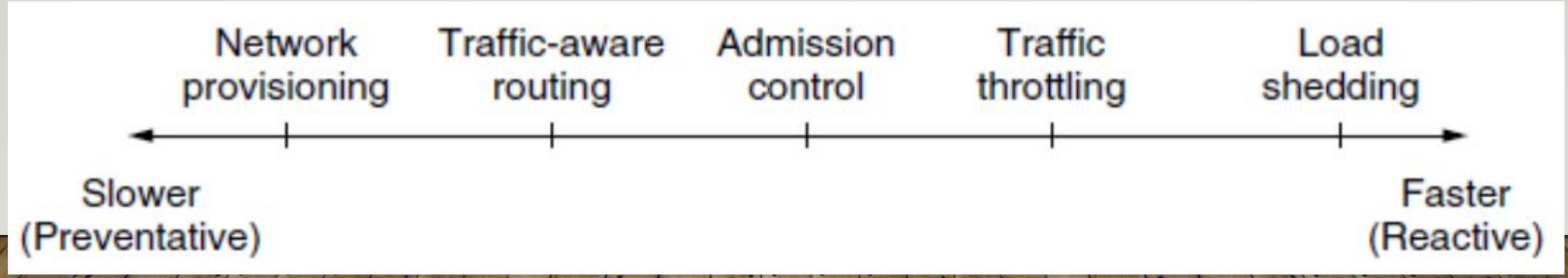
- Design networks that:
  - Avoid congestion where possible.
  - Do not suffer from congestion collapse if they do become congested.

Reasons for Congestion

- Streams of packets arriving from multiple input lines require a common output line a queue will build up.
- Insufficient memory or buffer space to accumulate packets.
- Slow processing speed of machines.
- Low bandwidth of channels.

How To Avoid Congestion?

- Presence of congestion means that the load is greater than the resources in the network can handle.
- Solutions:
  - Increase the resources.
  - Decrease the load.



Approaches To Congestion Control

- Provisioning
  - Upgrading links and routers that are regularly heavily utilized.
    - Turning on spare routers.
    - Enabling lines that are normally used only as backups.
    - Purchasing bandwidth on the open market.
- Traffic-aware Routing
  - Routes may be changed to shift traffic away from heavily used paths by changing shortest path weights.

Approaches To Congestion Control

- Admission Control
  - Decrease the load.
  - Used in virtual circuit networks.
  - Do not add a new virtual circuit unless the network can carry the added traffic without becoming congested.

Approaches To Congestion Control

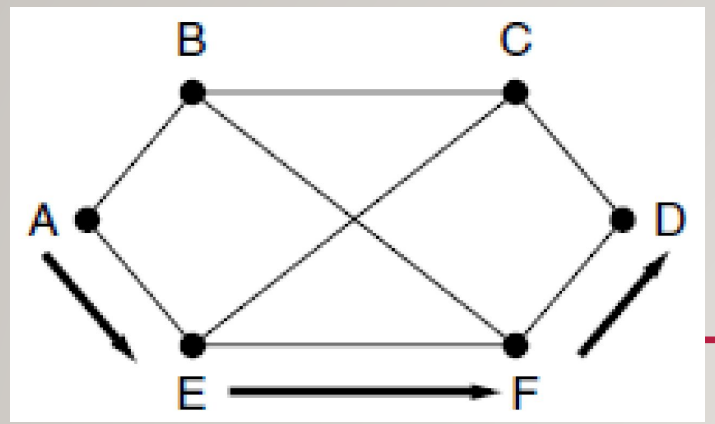
- Traffic throttling
  - Senders adjust their transmissions to send as much traffic as the network can readily deliver.
  - In this setting the network aim is to operate just before the onset of congestion.
  - Approach should consider:
    - Routers must determine when congestion is approaching. continuous monitoring of the resources.
    - Routers must deliver timely feedback to the senders that are causing the congestion.

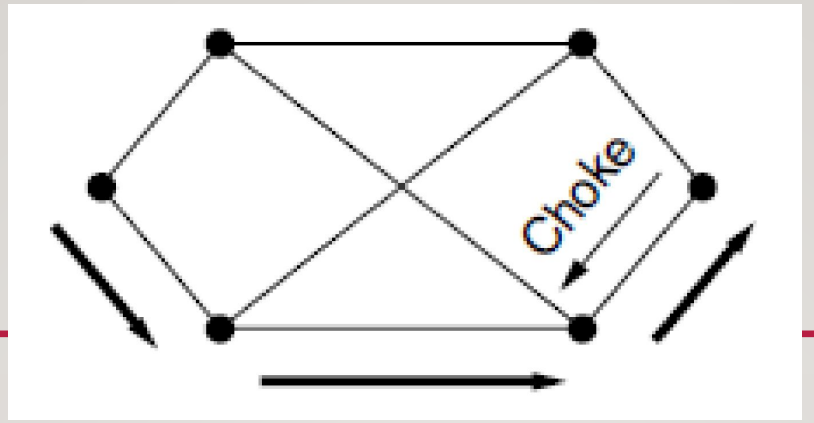
Approaches To Congestion Control

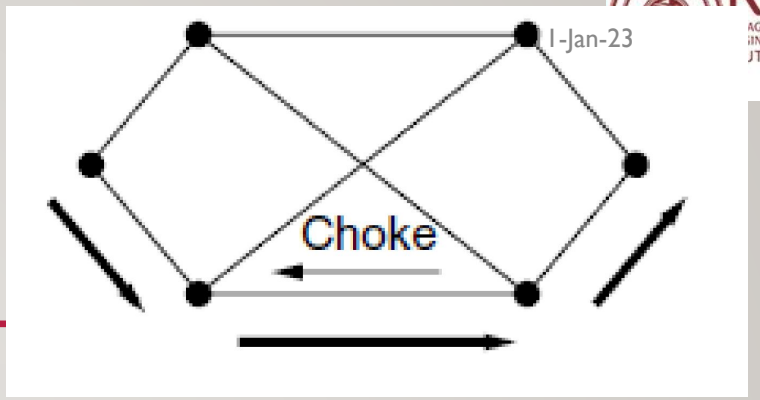
- Traffic throttling
  - Feedback Mechanisms
    - Router must identify the appropriate senders

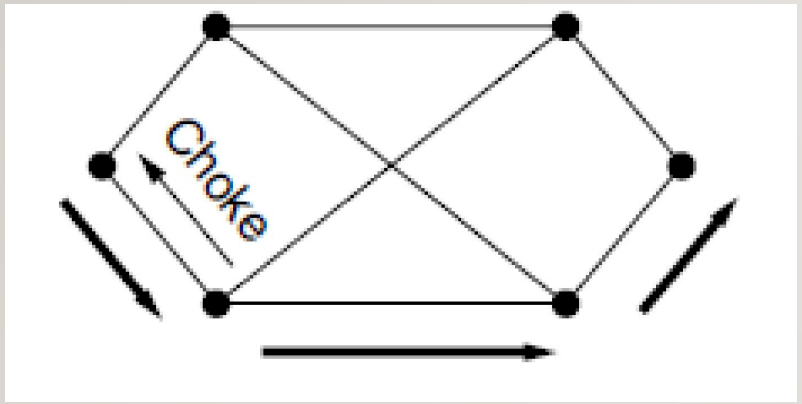
a) Choke Packets: direct way to notify a sender of congestion.

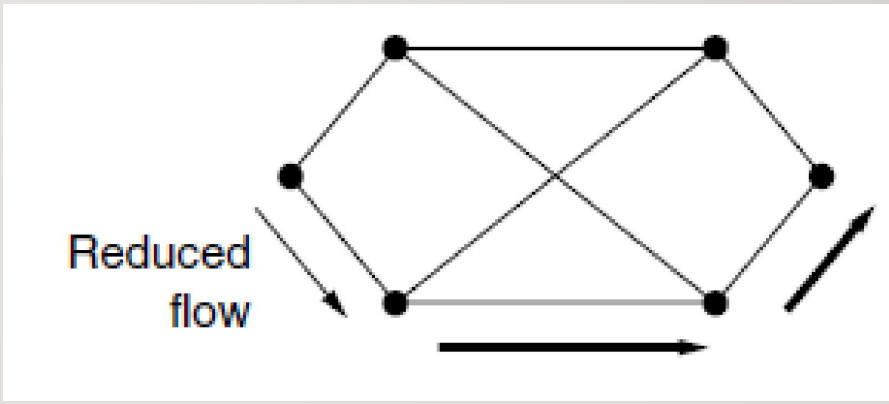
- A choke packet is a packet sent by a router to the source to inform it of congestion.
- Router selects a congested packet and sends a choke packet back to the source host.

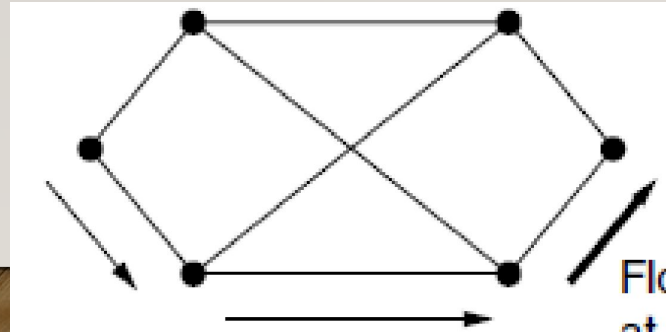




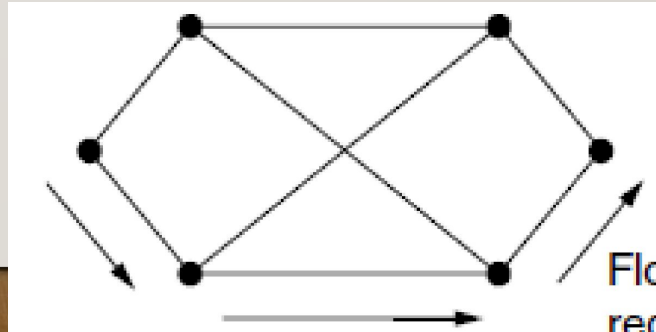








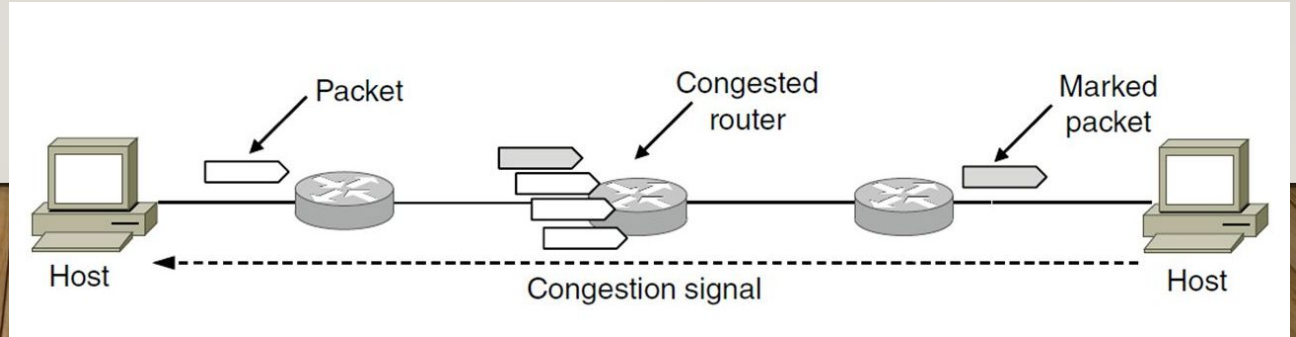
Flow is still
at maximum rate



Flow is
reduced

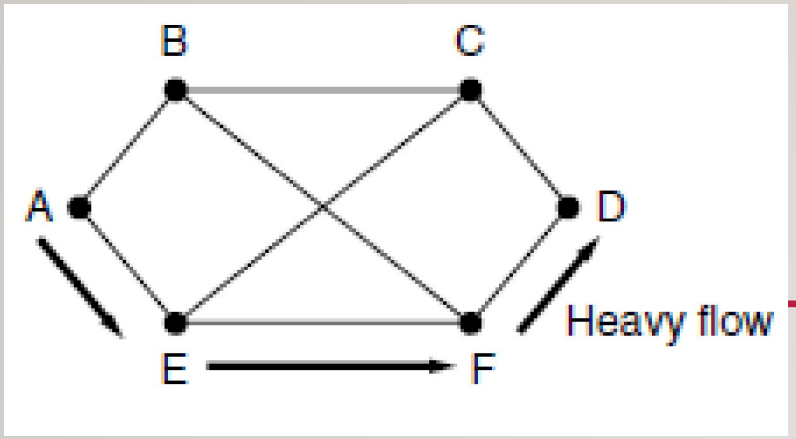
Approaches To Congestion Control

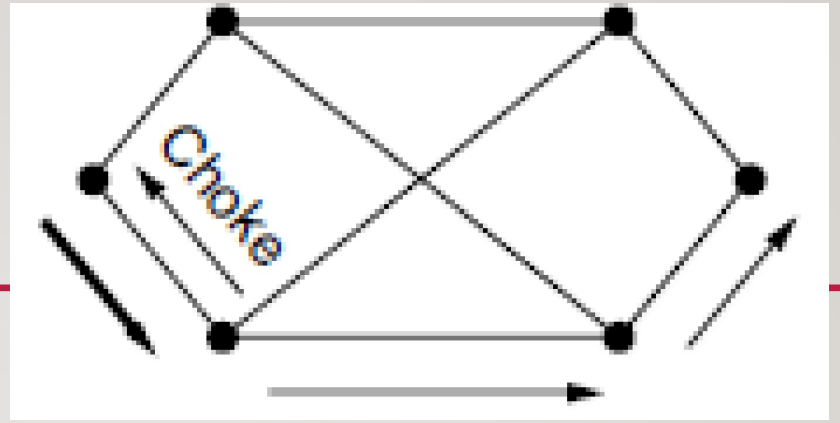
- Traffic throttling
  - Feedback Mechanisms
    - b) Explicit congestion Notification:
      - Instead of generating additional packets to warn of congestion, a router can tag any packet it forwards (by setting a bit in the header field) to signal that it is experiencing congestion.
      - When the network delivers the packet, the destination can note that there is congestion and inform the sender when it sends a reply packet.

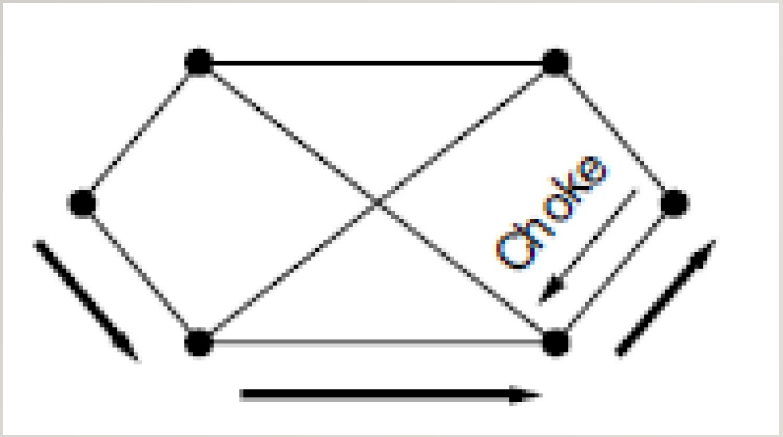


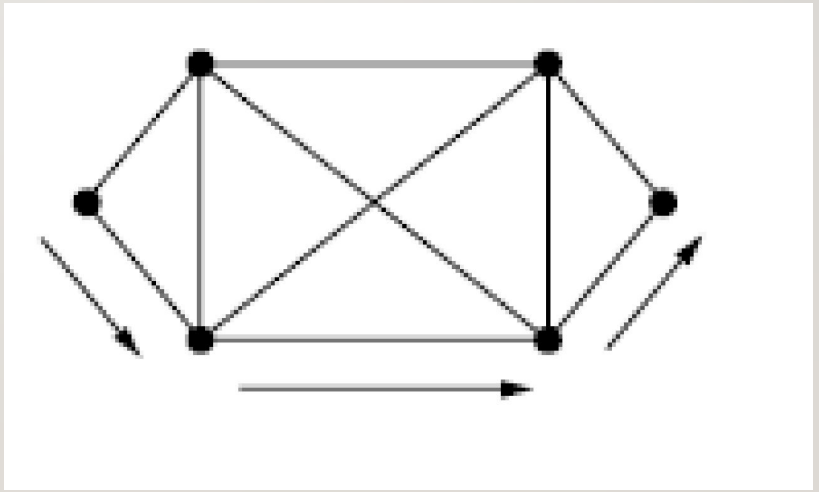
Approaches To Congestion Control

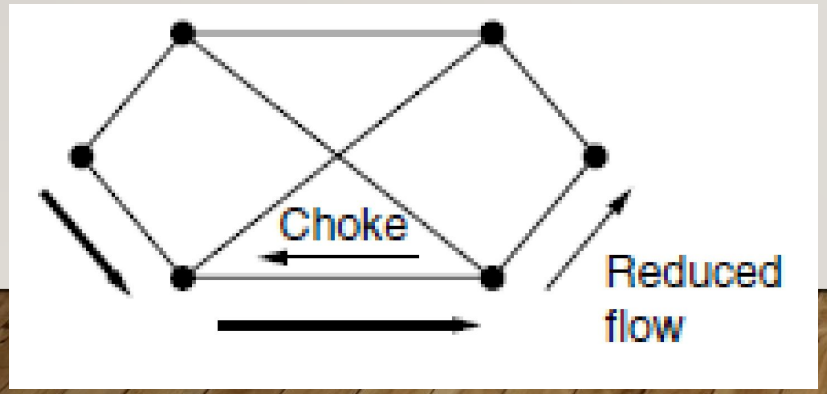
- Traffic throttling
  - Feedback Mechanisms
    - c) Hop by Hop backpressure:
      - Backpressure is a node-to-node congestion control technique that propagate in the opposite direction of data flow.
      - Choke packets take effect at every hop it passes through.
      - Provide quick relief at the point of congestion at the price of using up more buffers upstream.


B
C
A
D
E
F
Heavy flow


Choke


Choke




Choke
Reduced
flow

Approaches To Congestion Control

- Load Shedding
  - Discard packets that the network cannot deliver.
  - Question is which packets to drop?
  - A good policy for choosing which packets to discard can help to prevent congestion collapse.
    - To implement an intelligent discard policy, applications must mark their packets into priority classes.
    - When packets have to be discarded, routers first drops packets from the lowest priority class.

THANK YOU!!!

COMPUTER NETWORKS

MS. JINCY J FERNANDEZ

ASST. PROF, CSE

RSET

Quality of Service- Introduction

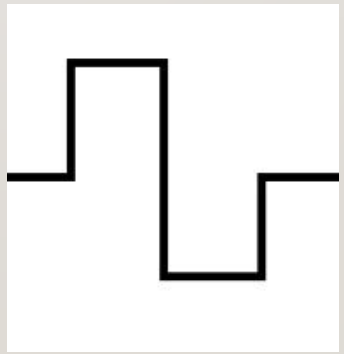
- Strong performance guarantees are required from networks.
- Need to ensure quality of service in networks.
- Issues to deal??
  - What applications need from the network?
  - How to regulate traffic that enters the network?
  - How to reserve resources at routers to guarantee performance?
  - Whether the network can safely accept more traffic?

QUALITY OF SERVICE

- Flow is a stream of packets from the source to the destination.
- Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic/flow.
- The Quality of Service (QoS) a flow requires is characterized by four parameters:

Bandwidth

Delay



Jitter

Reliability

Applications and their QOS Requirements

Application	Reliability	Delay	Jitter	Bandwidth
E-mail	High	Low	Low	Low
File transfer	High	Low	Low	Medium
Web access	High	Medium	Low	Medium
Remote login	High	Medium	Medium	Low
Audio on demand	Low	Low	High	Medium
Video on demand	Low	Low	High	High
Telephony	Low	High	High	Low
Videoconferencing	Low	High	High	High

Techniques For Achieving Good QOS

- Overprovisioning
- Traffic Shaping
  - Leaky Bucket
  - Token Bucket
- Resource Reservation
- Proportional Routing
- Packet Scheduling
- Integrated Services
  - RSVP
- Differentiated Services
  - Expedited Forwarding
  - Assured Forwarding

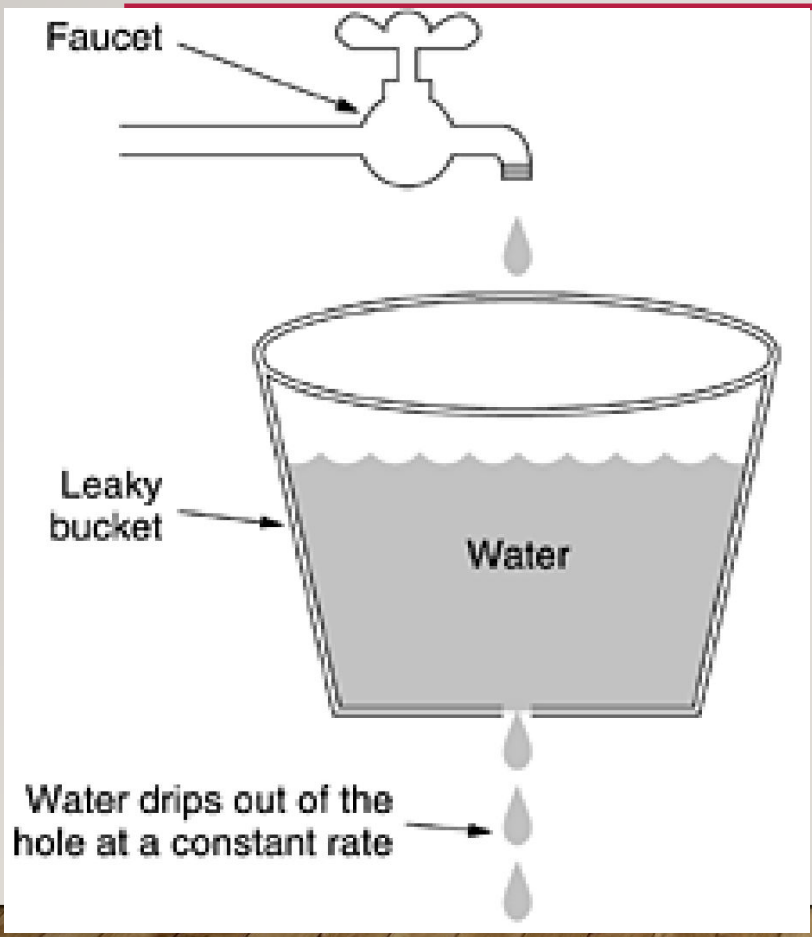
Overprovisioning

- Build a network with enough capacity for whatever traffic will be thrown at it.
- Provide so much router capacity, buffer space and bandwidth so that data can fly through easily.
- Expensive in nature.

Traffic Shaping

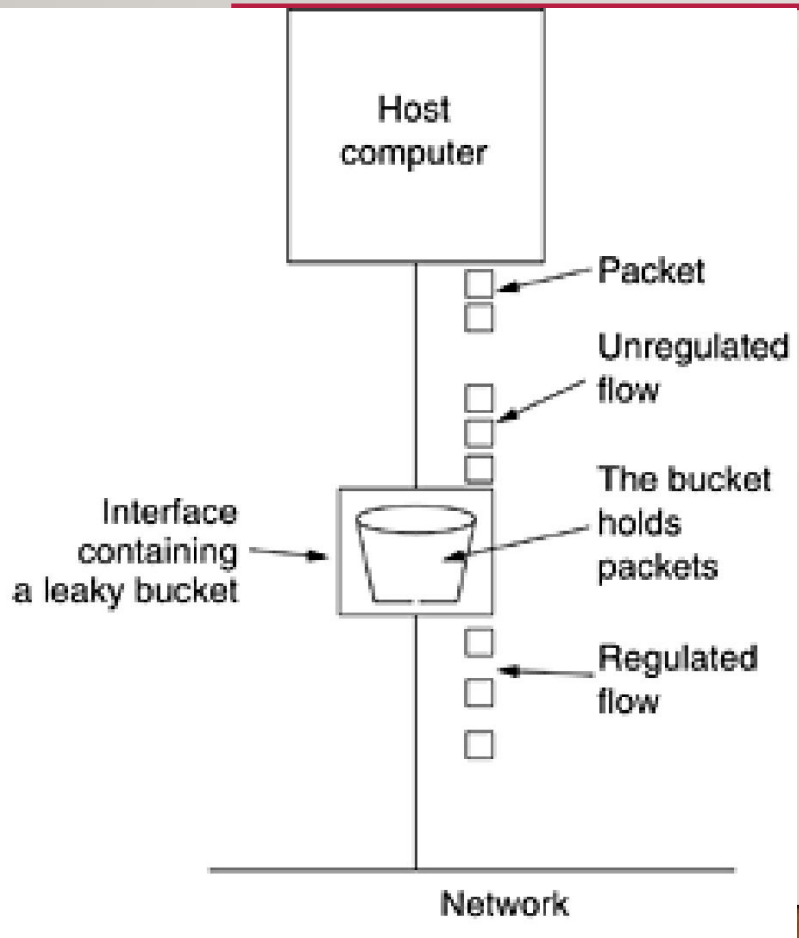
- Regulating the average rate of data transmission.
- When a connection is set up, the user and the subnet agree on a certain traffic pattern called Service Level Agreement.
- Carrier should monitor the traffic to ensure that the customer is following the agreement.
- Monitoring a traffic flow is called Traffic Policing.
- Shaping and Policing is important for real time data such as audio and video.

Traffic Shaping- Leaky Bucket Algorithm



- No matter the rate at which water enters the bucket, the outflow is at a constant rate, ρ, when there is water in the bucket.
- Once the bucket is full, any additional water entering it spills over the sides and is lost.
- Enforces a rigid output rate how much ever input is coming.

Traffic Shaping- Leaky Bucket Algorithm

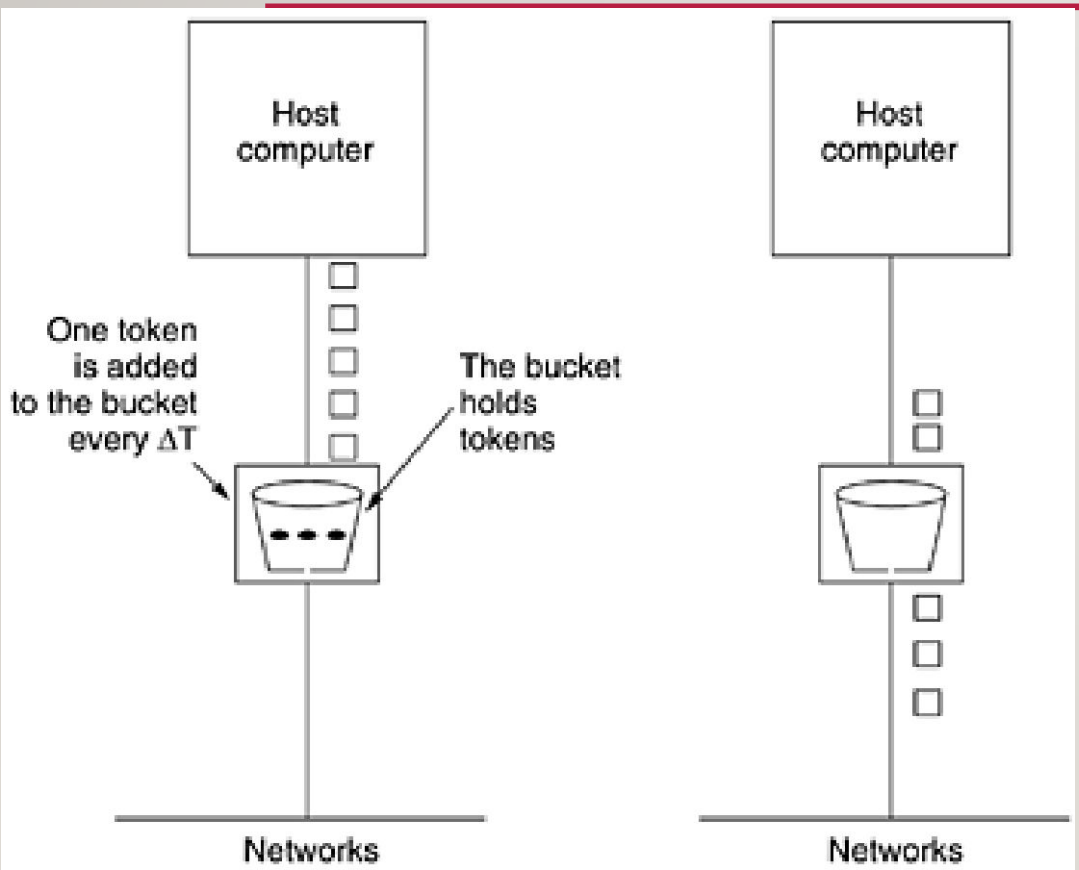


- Each host is connected to the network by an interface containing a leaky bucket (finite internal queue).
- To send a packet into the network, it must be possible to put more packets into the bucket.
- If a packet arrives when the bucket is full, the packet must either be queued until enough packets leaks out to hold it or be discarded.
- This technique was proposed by Turner (1986) and is called the leaky bucket algorithm.
- Not good for bursty traffic.

Traffic Shaping- Leaky Bucket Algorithm

- The host is allowed to put one packet per clock tick onto the network.
- An uneven flow of packets from the user processes inside the host is turned into an even flow of packets onto the network, smoothing out bursts and greatly reducing the chances of congestion.
- Works well when the packets are all the same size.
- When the packets are of variable-sized, it is often better to allow a fixed number of bytes per tick, rather than just one packet.
- Byte counting leaky bucket algorithm.

Traffic Shaping- Token Bucket Algorithm



- This allows output rate to vary depending on size of burst.
- The leaky bucket holds tokens.
- The tokens are generated by a clock at the rate of one token every ΔT sec.
- For a packet to be transmitted, it must capture and destroy one token.
- A minor variant is possible, in which each token represents the right to send not one packet, but k bytes.

Comparison

TOKEN BUCKET	LEAKY BUCKET
Token dependent.	Token independent.
If bucket is full token are discarded, but not the packet.	If bucket is full packet or data is discarded.
Packets can only transmitted when there are enough token	Packets are transmitted continuously.
It allows large bursts to be sent faster rate after that constant rate	It sends the packet at constant rate
It saves token to send large bursts.	It does not save token.

Resource Reservation

- Once a specific route for a flow is established, it becomes possible to reserve resources along that route to make sure the needed capacity is available.
- Resources that can be reserved are:
  - Bandwidth
  - Buffer space
  - CPU cycles

Proportional Routing

- Most routing algorithms finds the best path for each destination and send all traffic to that destination over the best path.
- A different approach to provide a higher quality of service is to split the traffic for each destination over multiple paths.
- Divide the traffic equally or in proportion to the capacity of the outgoing links.

Packet Scheduling

- If a router is handling multiple flows, there is a danger that one flow will take over too much of its capacity and starve all the other flows.
- A good scheduling technique treats the different flows in a fair and appropriate manner.
- FIFO queuing algorithm
  - Packets wait in a buffer (queue) until the node is ready to process them.

Packet Scheduling

- Priority queuing algorithm
  - Packets are assigned to priority classes.
  - The packets in the highest priority queue are processed first.
  - The packets in the highest priority queue are processed last.
  - If there is a continuous flow in a high priority queue, the packets in the low priority queues will never have a chance to be processed Starvation.

Packet Scheduling

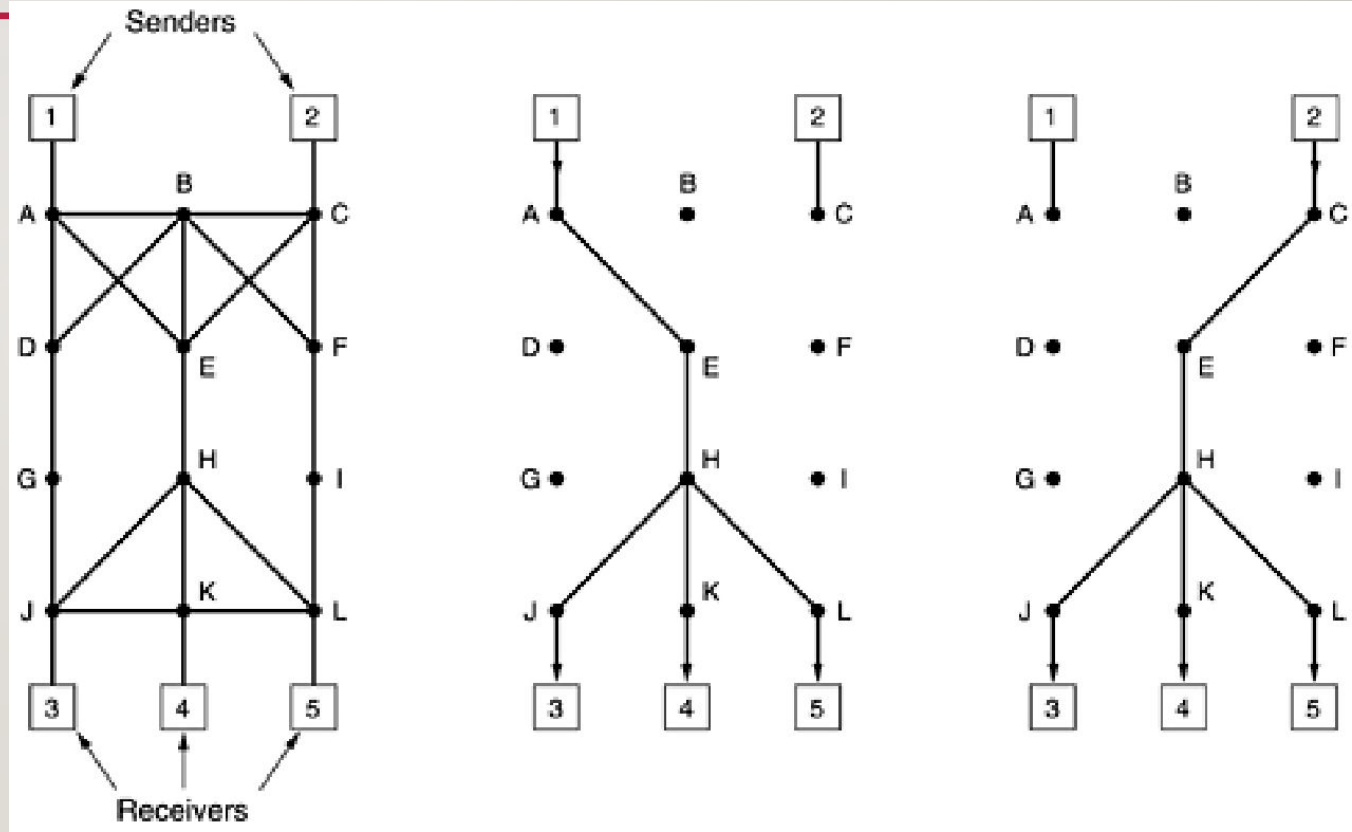
- Weighted Fair algorithm
  - Packets are assigned to different classes and admitted to different queues.
  - The queues are weighted based on the priority of the queues; higher priority means a higher weight.
  - Process the packets in each queue in a round robin fashion with the number of packets selected from each queue based on the corresponding weight.
  - Starvation is avoided.

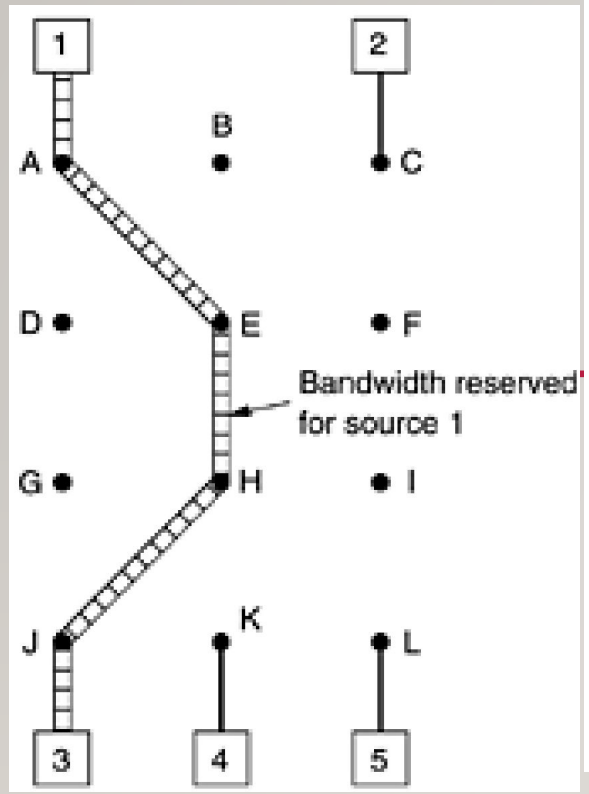
INTEGRATED SERVICES

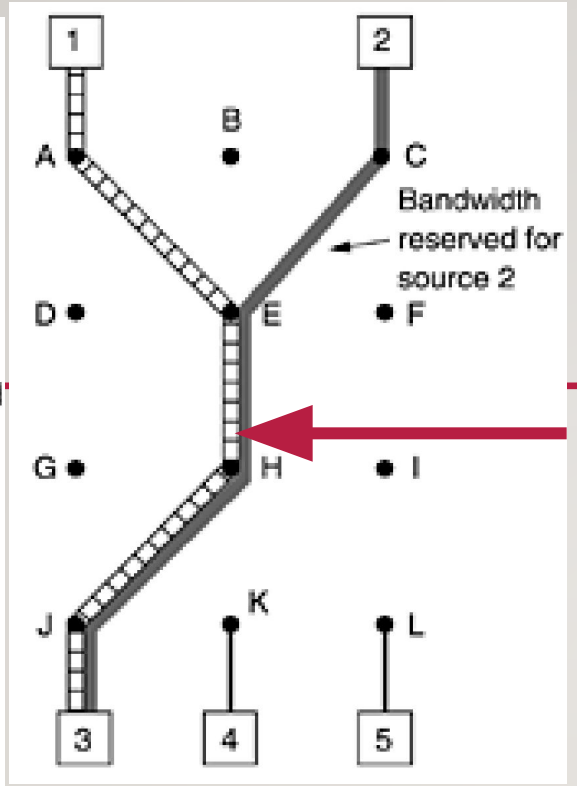
- Architecture for streaming multimedia.
- Flow Based Algorithms or Integrated Services.
- Advance setup required to establish each flow.
- For unicast and multicast applications.
- Resource reSerVation Protocol (RSVP) is the IETF architecture for the integrated services architecture.
  - Allows multiple senders to transmit to multiple groups of receivers.
  - Permits individual receivers to switch channels freely.
  - Optimizes bandwidth eliminating congestion.

RSVP

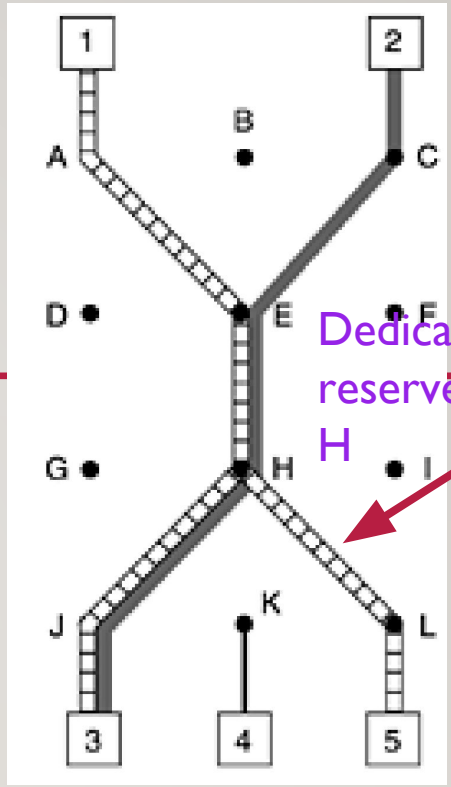
- Each group is assigned a group address.
- To send to a group, the sender put the group's address in its packets.
- The standard multicast routing algorithm builds a spanning tree covering all group members.







Two separate channels are needed from host 3 to router E, because two independent streams are being transmitted



Dedicated bandwidth reserved as far as router H

- Receivers can sent a reservation message to the sender
- The message is forwarded using the reverse path forwarding algorithm.
- At each hop, the router notes the reservation and reserves the necessary bandwidth.

DIFFERENTIATED SERVICES

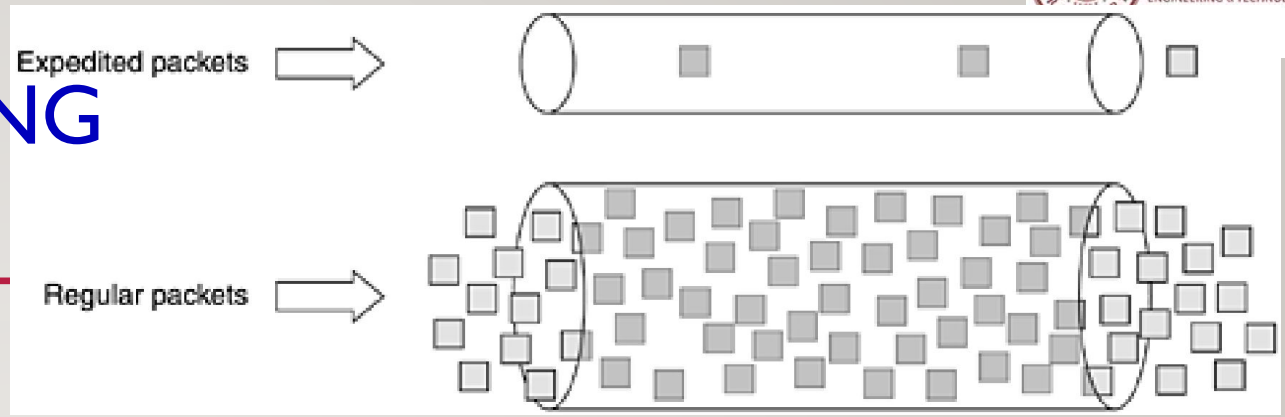
- Architecture for class based QoS and not flow based.
- Differentiated Services (DS) can be offered by a set of routers forming an administrative domain eg: ISP.
- The administration defines a set of service classes with corresponding forwarding rules.
- If a customer signs up for a DS, the customer packets may carry a Type of Service field in them.
- Better services may be provided to some classes compared to others.
- Traffic within the same class need to follow shaping. (leaky or token bucket).

ADVANTAGES

- No advance setup needed.
- No resource reservation required.
- No time consuming end to end negotiation for each flow.

- So easy to implement compared to integrated services.

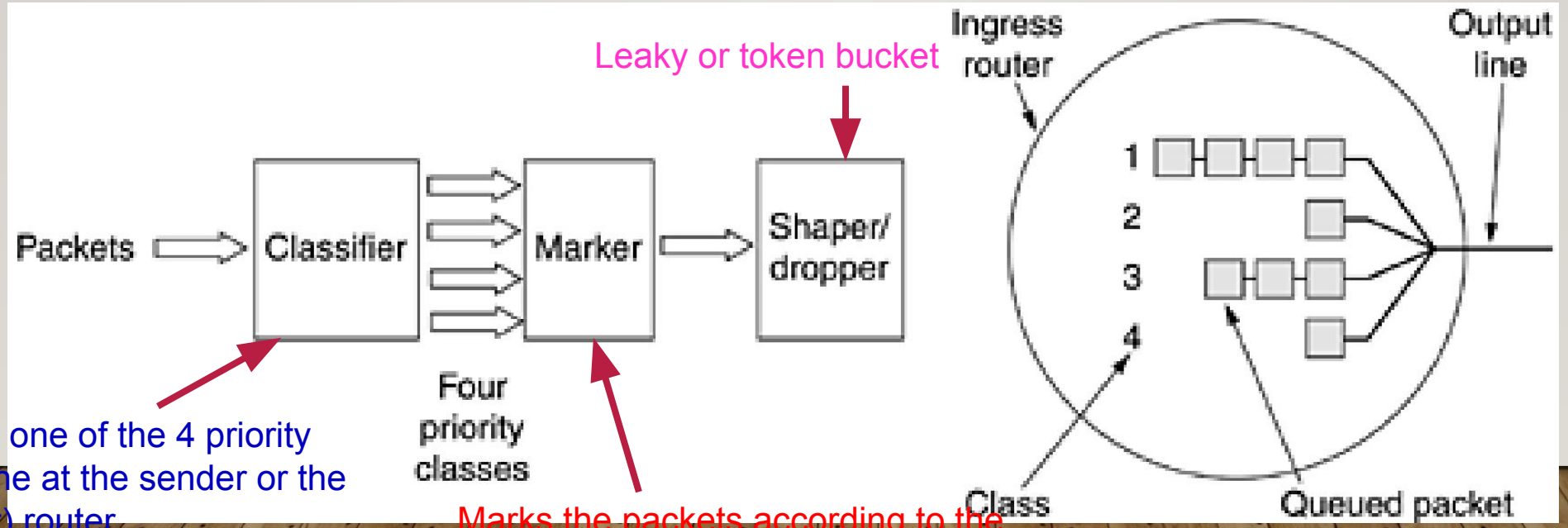
EXPEDITED FORWARDING



- Two classes of services are available:
  - Regular
  - Expedited
- Majority of the traffic (90%) is regular.
- Small fraction of the packets are expedited (10%).
- Expedited packets transit the subnet as though no other packets are present.
- 20% of the bandwidth may be dedicated for expedited traffic.
- Only 1 physical line is present (implemented as 2 queues).

ASSURED FORWARDING

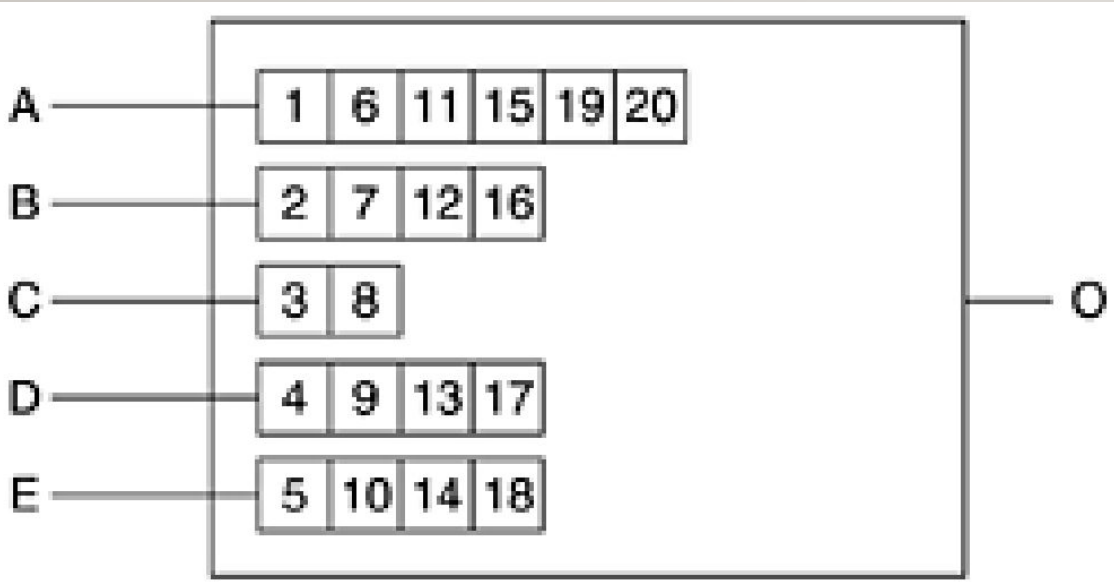
- Four priority classes – each with its own resources.
- Three discard policies (low, medium, high).
- Together 12 service classes.



Classifies to one of the 4 priority classes. Done at the sender or the ingress (first) router

Marks the packets according to the class. Use Type of Service field

THANK YOU!!!



Packet	Finishing time
C	8
B	16
D	17
E	18
A	20

- The algorithm gives more bandwidth to hosts that use large packets than to hosts that use small packets.
- Simulate Byte-by-byte round robin, instead of a packet-by-packet round robin.
- Packets are sorted in order of finishing and sent in that order.