Network Layer(CO1)

Topic Objective

- The student will be able to understand the networking issues
- Functions of network layer and
- Services provided by the network layer

Network Layer(CO1)

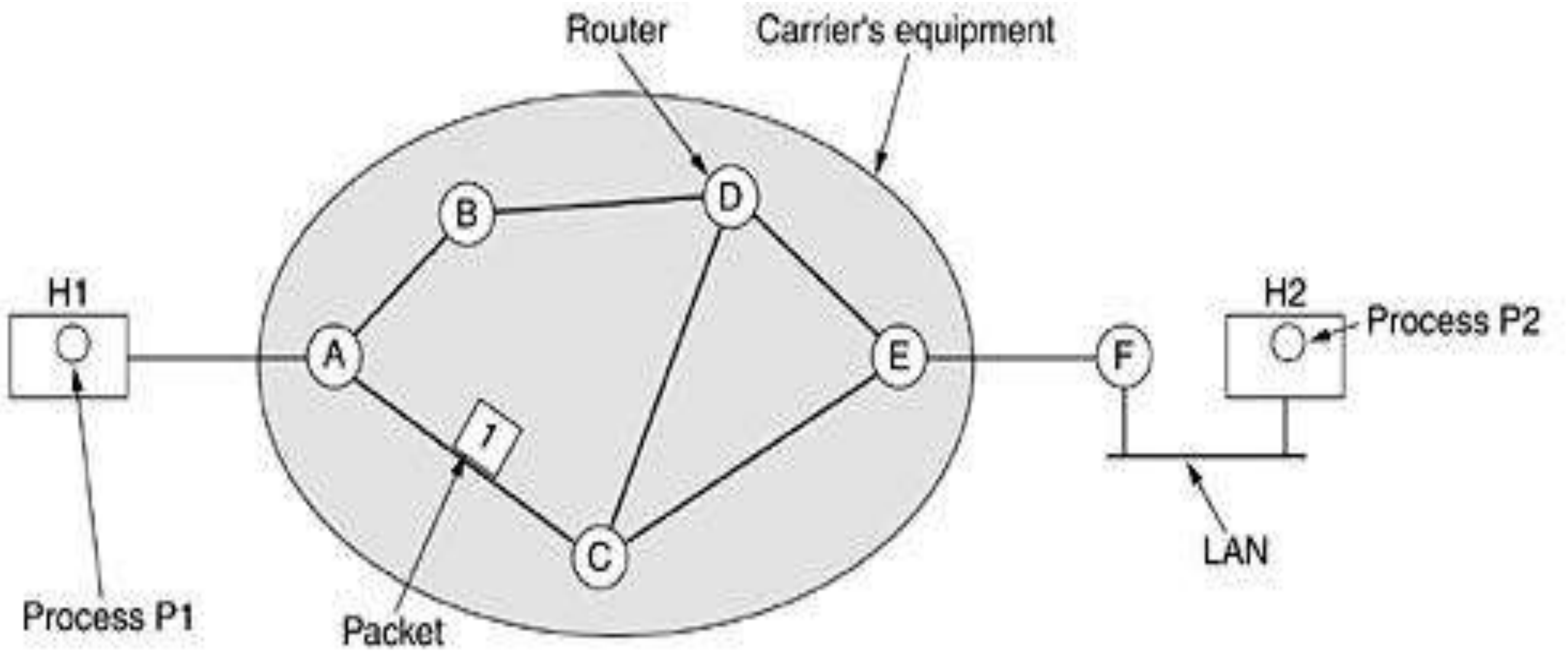
- This is the third layer in OSI model in computer networking.
- Network layer provides support for end to end communication (helps to forward the packets from source to destination) by using routers and switches.
- Network layer manages the Quality of Services (QoS).
- The service provided by the network layer to the transport layer is called as **network service.**

Network Layer(CO2)

- Store – and – forward Packet Switching
- Services provided to the Transport Layer
- Implementation of connectionless Service
- Implementation of Connection-Oriented Service
- Comparison of Virtual-Circuit and Datagram Networks

Network Layer

Store-and-Forward Packet Switching



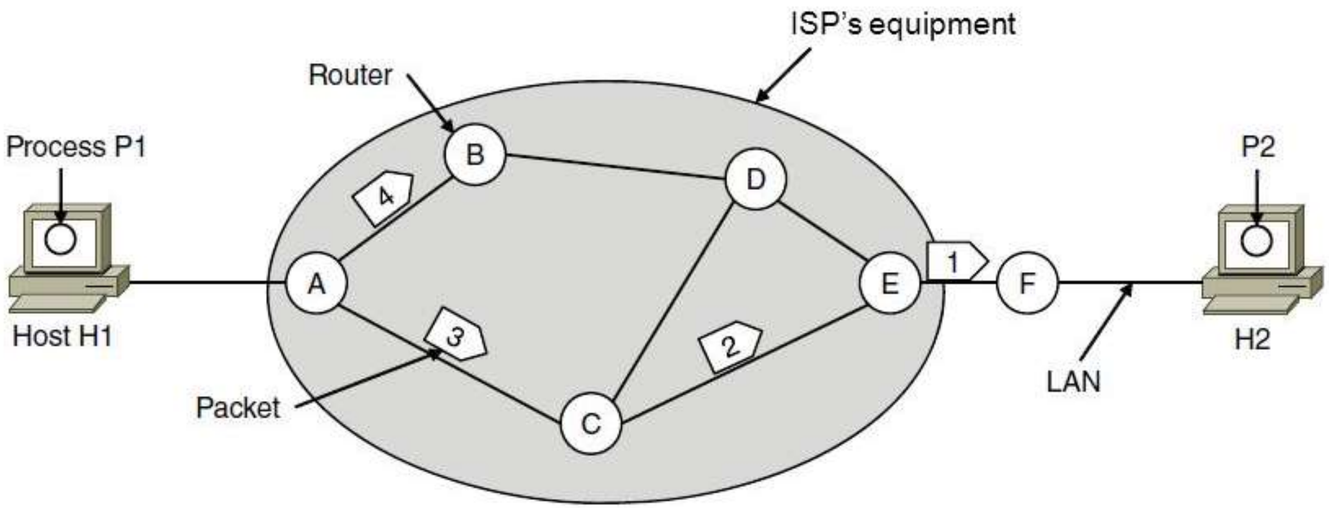
Network Layer

Services provided to the Transport Layer

- The services should be independent of the router technology
- The transport layer should be shielded from the number, type, and topology of the routers present
- The network addresses made available to the transport layer should use a uniform numbering plan, even across LANs and WANs.

Network Layer

Implementation of connectionless Service



A's table (initially)

Dest.	Line
A	
B	B
C	C
D	B
E	C
F	C

A's table (later)

A	
B	B
C	C
D	B
E	D
F	D

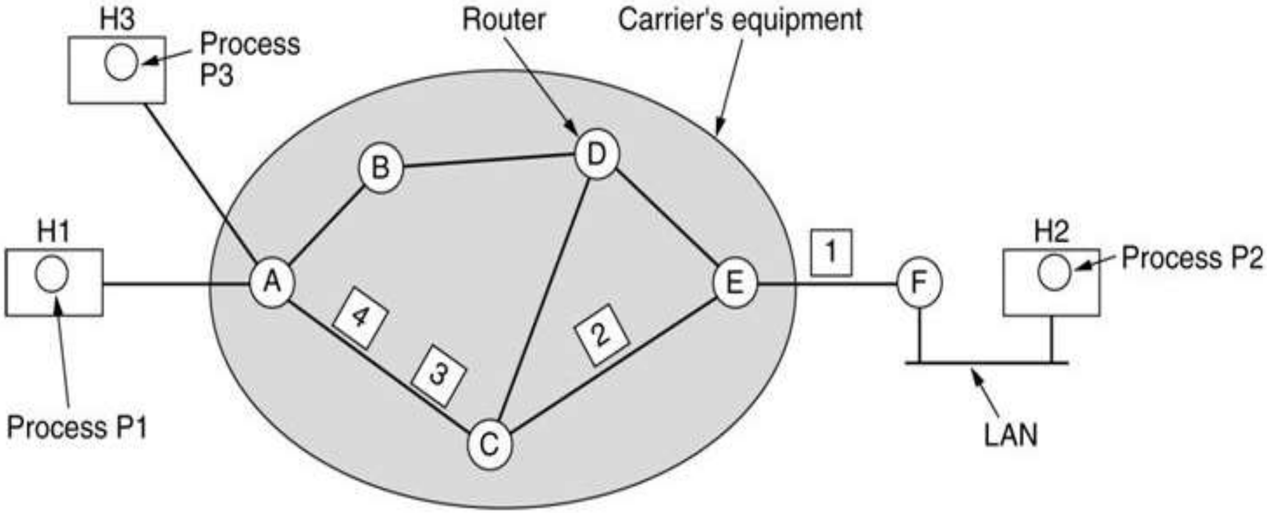
C's Table

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

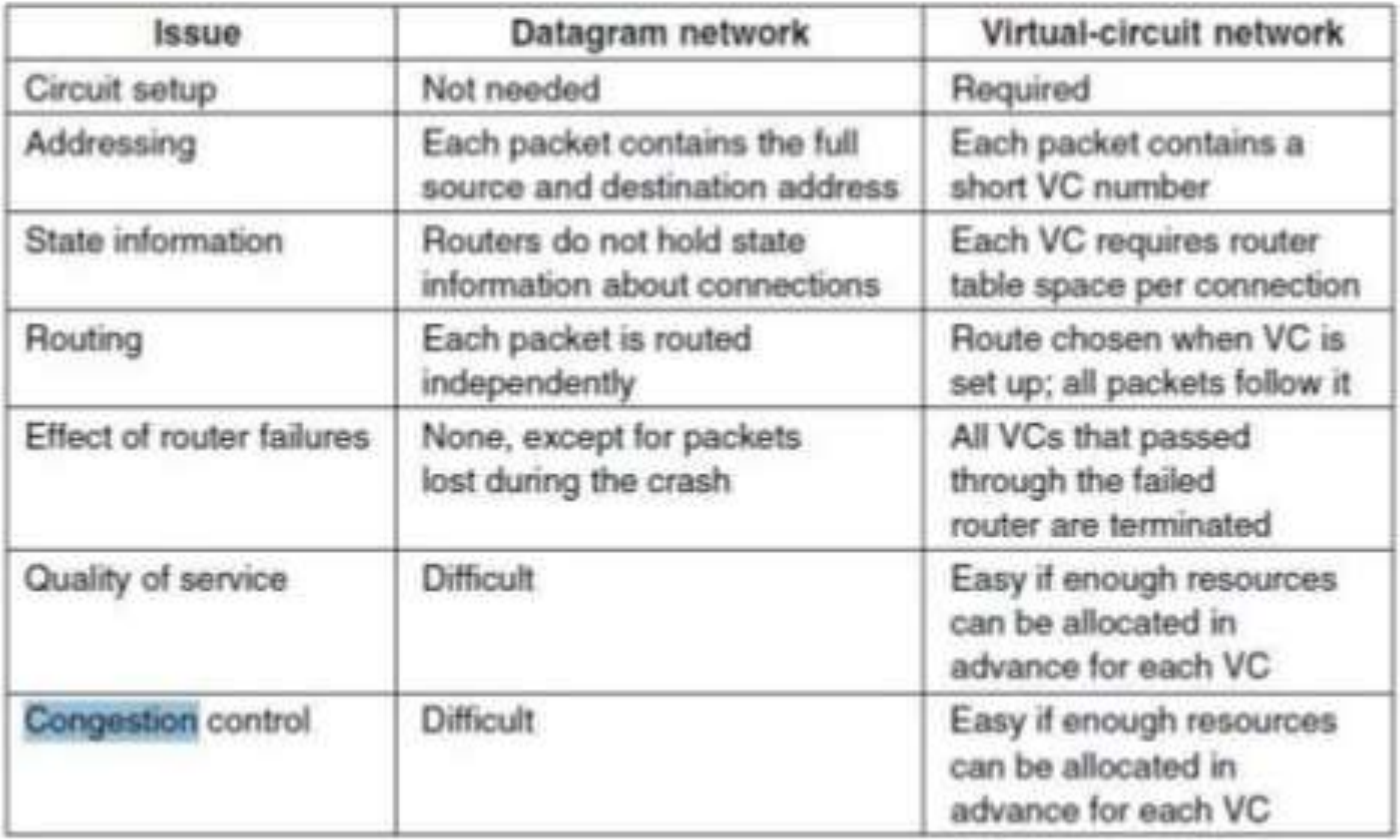
Implementation of Connection-Oriented Service



A's table		C's table		E's table	
H1 1	C 1	A 1	E 1	C 1	F 1
H3 1	C 2	A 2	E 2	C 2	F 2
In	Out				

Network Layer

Comparison of Virtual-Circuit and Datagram Networks



Issue	Datagram network	Virtual-circuit network
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

Network Layer design issue(CO5)

- Reliability
- Scalability
- Addressing
- Error Control
- Flow Control
- Resource Allocation
- Statistical Multiplexing
- Routing
- Security

Functions of Network Layer(CO1)

Routing –

- transferring packets received from the Data Link Layer of the source network to the Data Link Layer of the correct destination
- Involves decision making at each intermediate node on where to send the packet next so that it eventually reaches its destination.
- The node which makes this choice is called a router.
- For routing we require some mode of addressing which is recognized by the Network Layer.

Functions of Network Layer

Inter-networking –

- The network layer is the same across all physical networks (such as Token-Ring and Ethernet).
- the packets that arrive at the Data Link Layer of the node which connects these two physically different networks, would be stripped of their headers and passed to the Network Layer.

Functions of Network Layer

Congestion Control –

- If the incoming rate of the packets arriving at any router is more than the outgoing rate.
- If suddenly, packets begin arriving on many input lines and all need the same output line, then a queue will build up.
- If there is insufficient memory to hold all of them, packets will be lost.
- Another reason for congestion are slow processors.
- Similarly, low-bandwidth lines can also cause congestion.

Routing Algorithms(CO3)

Topic Objective

- To understand the basics of routing
- Various adaptive and non adaptive routing algorithms
- Implementation of the algorithms

Recap of previous topic

- Network layer provides unreliable transmission of data
- Provides services to transport layer
- Error and flow control

Routing Algorithms(CO3)

Routing is the process of forwarding of a packet in a network so that it reaches its intended destination.

- Correctness:
- Simplicity:
- Robustness:
- Stability:
- Fairness:
- Optimality:

Routing Algorithms

Types

- Optimality Principle
- Shortest Path Routing
- Flooding
- Distance Vector Routing
- Link State Routing
- Hierarchical Routing
- Broadcast Routing
- Multicast Routing

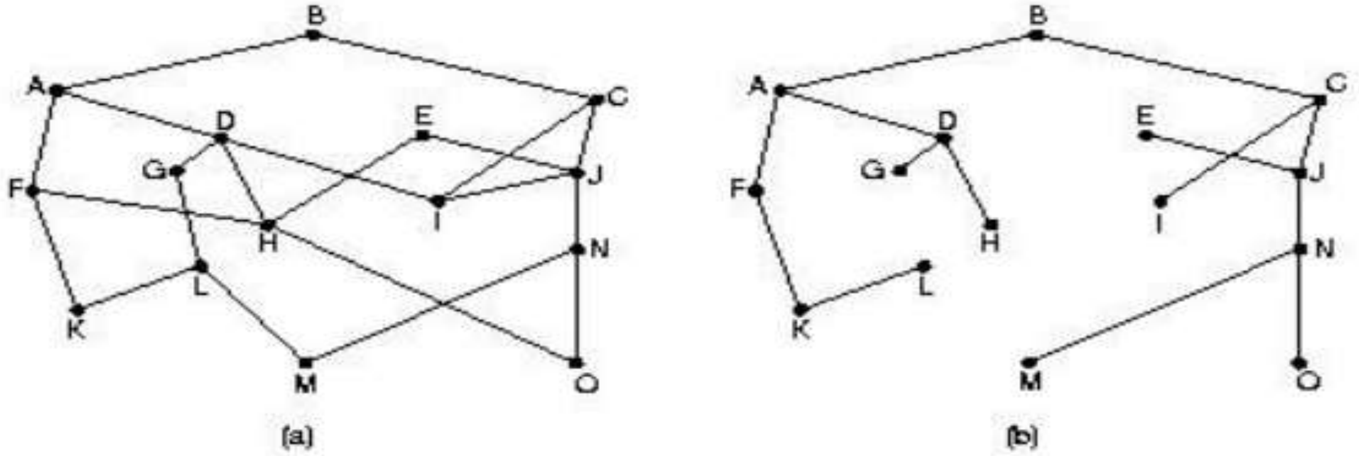
Types of Routing Algorithms(CO5)

- Non-adaptive (Static)
  - Do not use measurements of current conditions
  - Static routes are downloaded at boot time
- Adaptive Algorithms
  - Change routes dynamically
  - Gather information at runtime
    - locally
    - from adjacent routers
    - from all other routers
  - Change routes
    - Every delta T seconds
    - When load changes
    - When topology changes

Types of Routing Algorithms-Non adaptive(CO4)

The Optimality Principle

- If router j is on the optimal path from i to k, then the optimal path from j to k also falls along the same route.
- The set of optimal routes to a particular node forms a sink tree.
- Sink trees are not necessarily unique
- Goal of all routing algorithms – Discover sink trees for all destinations



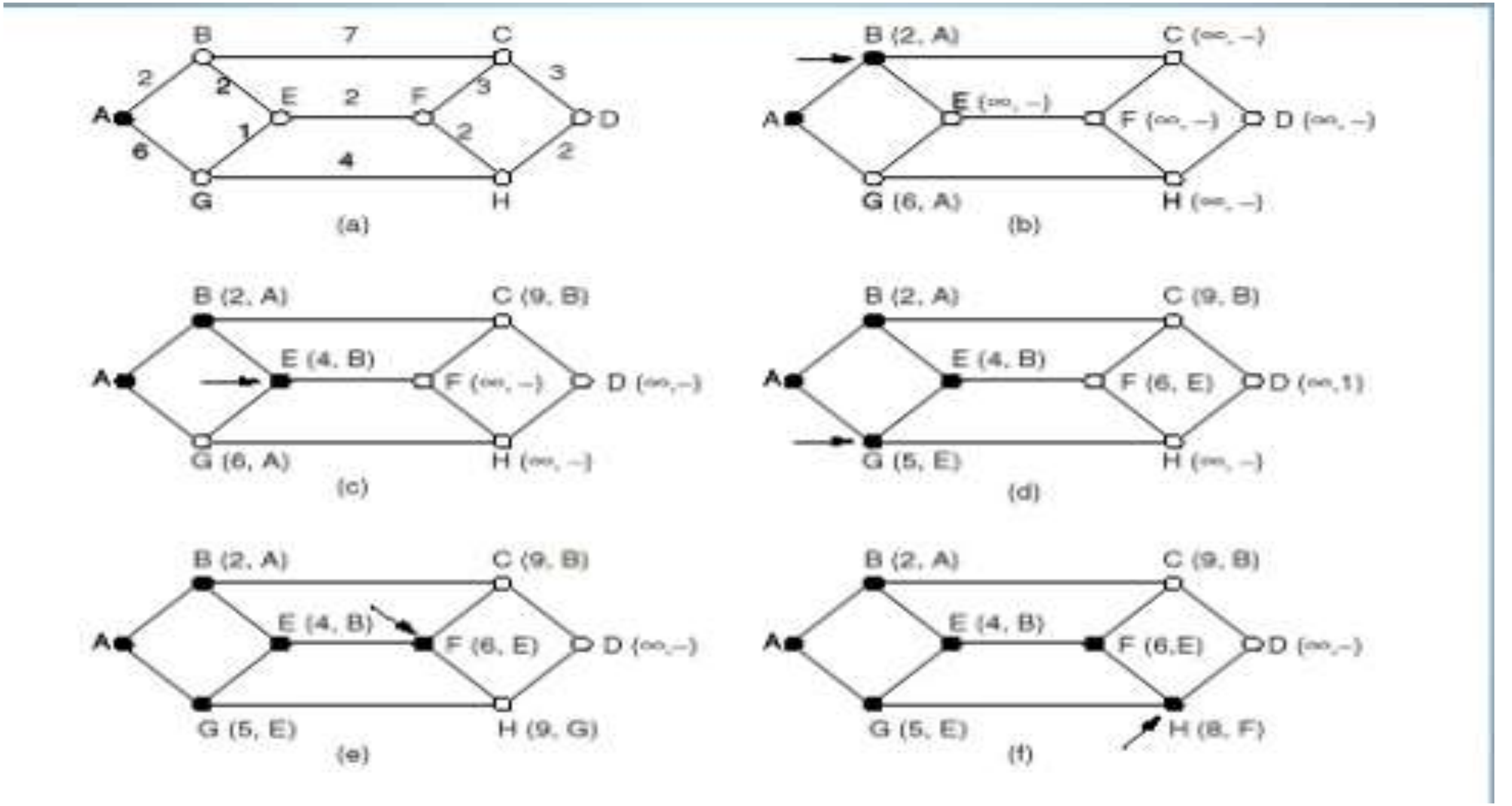
Types of Routing Algorithms-Non Adaptive(CO4)

Shortest Path Routing

- Given a network topology and a set of weights describing the cost to send data across each link in the network
- Find the shortest path from a specified source to all other destinations in the network.
- Shortest path algorithm first developed by E. W. Dijkstra Shortest Path Routing (a non-adaptive routing algorithm)

Types of Routing Algorithms-Non Adaptive(CO5)

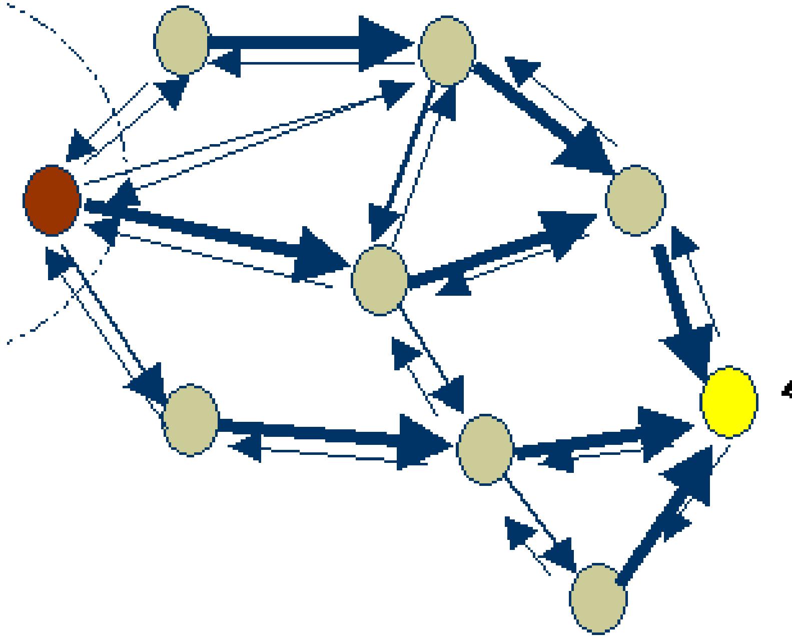
Example for shortest path routing



Types of Routing Algorithms-Non Adaptive(CO4)

Flooding

- No network information is required
- Packet send by node to every neighbor
- Incoming packets retransmitted on every link without incoming link
- Eventually a numbers of copies will arrives at destination
- Each packet is uniquely numbered so duplicate can be discarded
- Nodes can remember packets already forwarded to keep network load in bounds
- All nodes are visited – All possible routes are tried



Types of Routing Algorithms-Non Adaptive

Selective Flooding – Flood only in the direction of the destination

- To prevent packets from looping forever, each router decrements a hop count contained in the packet header.
- Whenever the hop count decrements to zero, the router discards the packet.
- To reduce looping even further:

  1. Add a sequence number to each packet's header.
  2. Each router maintains a private sequence number. When it sends a new packet, it copies the sequence number into the packet, and increments its private sequence number.
  3. For each source router S, a router:

     a) Keeps track of the highest sequence number seen from S.

     b) Whenever it receives a packet from S containing a sequence number lower than the one stored in its table, it discards the packet.

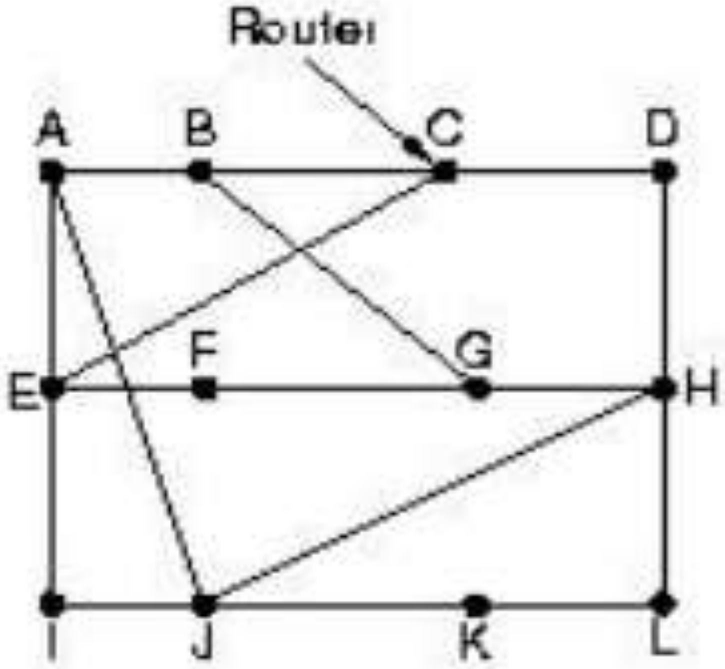
     c) Otherwise, it updates the entry for S and forwards the packet on Non-Adaptive Algorithm

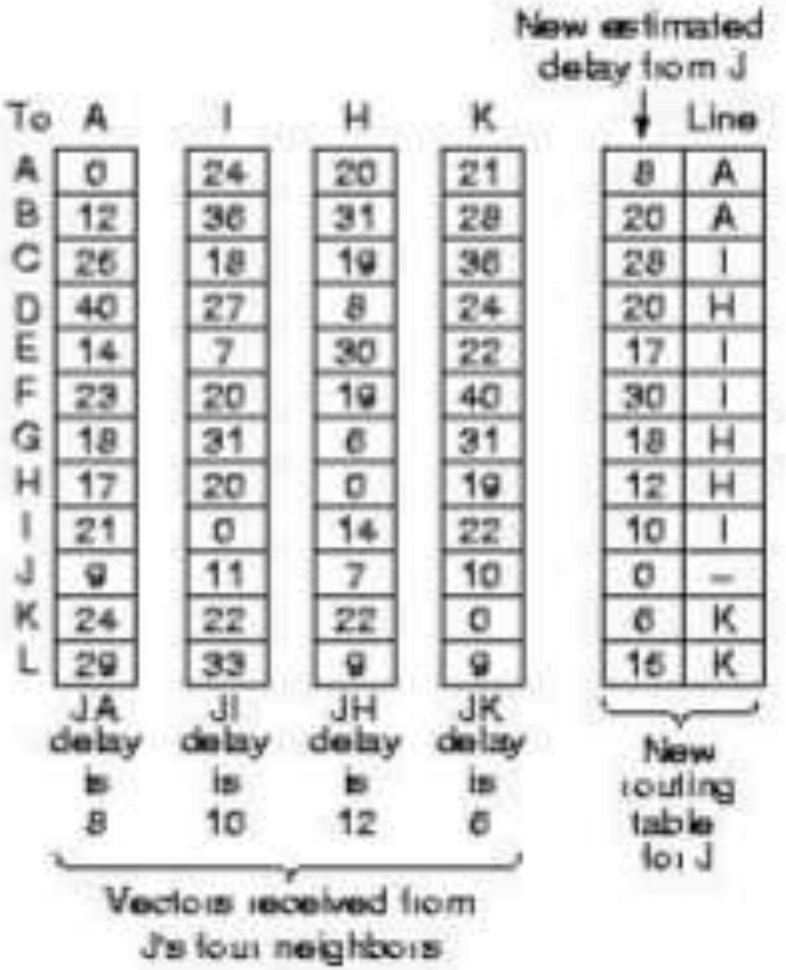
Types of Routing Algorithms- Adaptive(CO1,CO5)

Distance Vector Routing

1. Each router maintains a table (vector) giving the best known distance to a destination and the line to use for sending there. Tables are updated by exchanging information with neighbors.
2. Each router knows the distance (cost) of reaching its neighbors (e.g. send echo requests).
3. Routers periodically exchange routing tables with each of their neighbors.
4. Upon receipt of an update, for each destination in its table, a router:
   – Compares the metric in its local table with the metric in the neighbor's table plus the cost of reaching that neighbor. – if the path via the neighbor has a lower cost, the router updates its local table to forward packets to the neighbor.

Types of Routing Algorithms- Adaptive



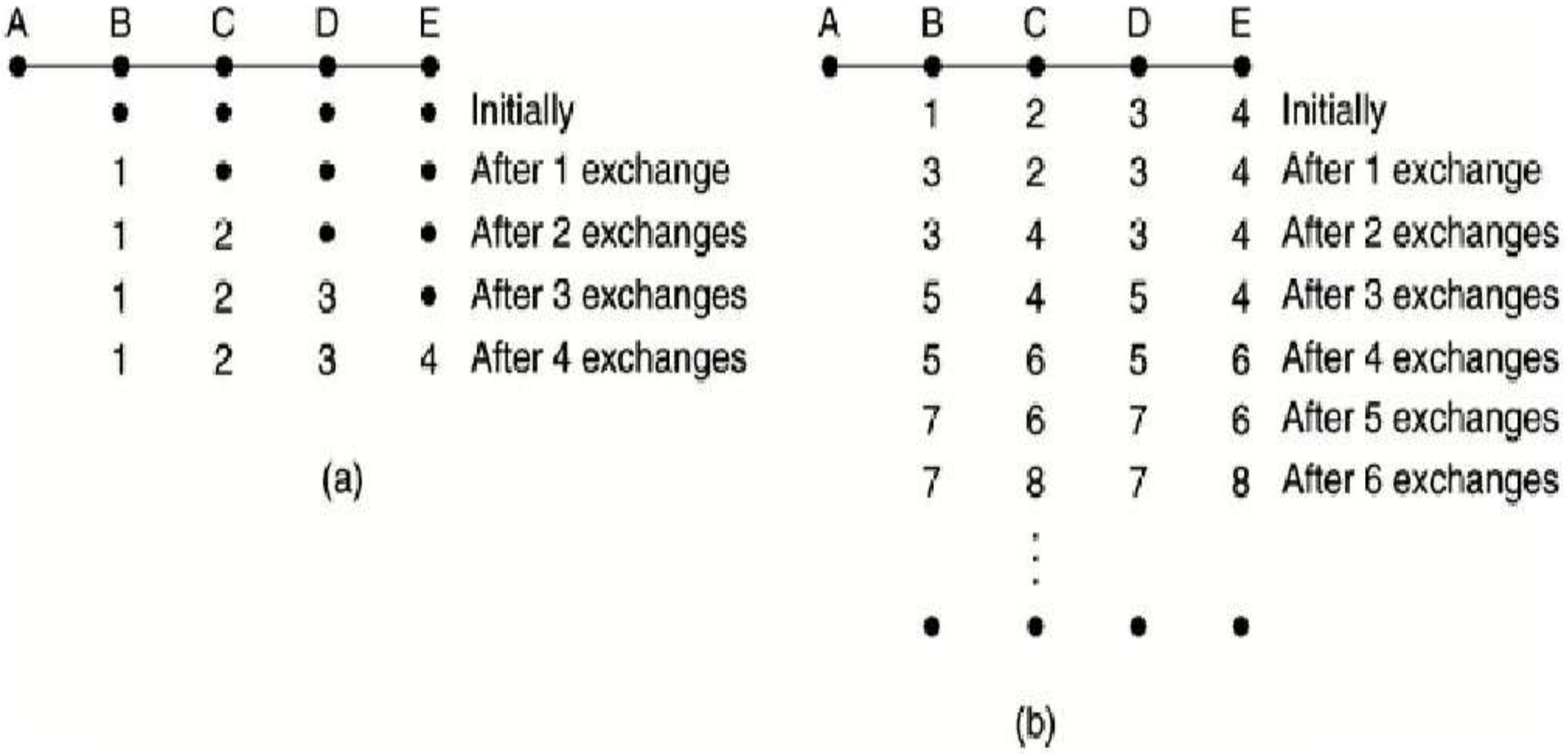


To	A	I	H	K	New estimated delay from J	Line
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	–
K	24	22	22	0	6	K
L	29	33	9	9	15	K
	JA delay is 8	JI delay is 10	JH delay is 12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

Vectors received from J's four neighbors

Types of Routing Algorithms- Adaptive

The count –to – infinity Problem



A	B	C	D	E	
	•	•	•	•	Initially
	1	•	•	•	After 1 exchange
	1	2	•	•	After 2 exchanges
	1	2	3	•	After 3 exchanges
	1	2	3	4	After 4 exchanges

(a)

A	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
		⋮			
	•	•	•	•	

(b)

Types of Routing Algorithms- Adaptive

Distance Vector Routing

- This algorithm was used in the original ARPANET.
- Unfortunately, it suffers from the problem: good news travels quickly, bad news travels slowly (count-to-infinity problem).
- The fundamental problem with the old Arpanet algorithm is that it continues to use `old' information that is invalid, even after newer information becomes available.

Types of Routing Algorithms- Adaptive

Link State Routing

- The `old' Arpanet routing algorithm was replaced in 1979.
- Problems with old algorithm included:

1. High-priority routing update packets were large, adversely affecting traffic.

2. Network was too slow in adapting to congestion, too fast to react to minor changes.

3. Average queue length was used to estimate delay. – This works only if all lines have the same capacity and propagation delay.d – Doesn't take into account that packets have varying sizes.

Types of Routing Algorithms- Adaptive

Link State Routing

1.) Discover your neighbors and learn their addresses.

2.) Measure the cost (delay) to each neighbor.

3.) Construct a packet containing all this information

4.) Send this packet to all other routers.

5.) Compute the shortest path to every other router.

Types of Routing Algorithms- Adaptive

Link State Routing

1. Discovering Your Neighbors

- Send “Hello” packet on each point-to-point line. Destination node replies with its address.

2. Measure the cost (delay) to each neighbor.

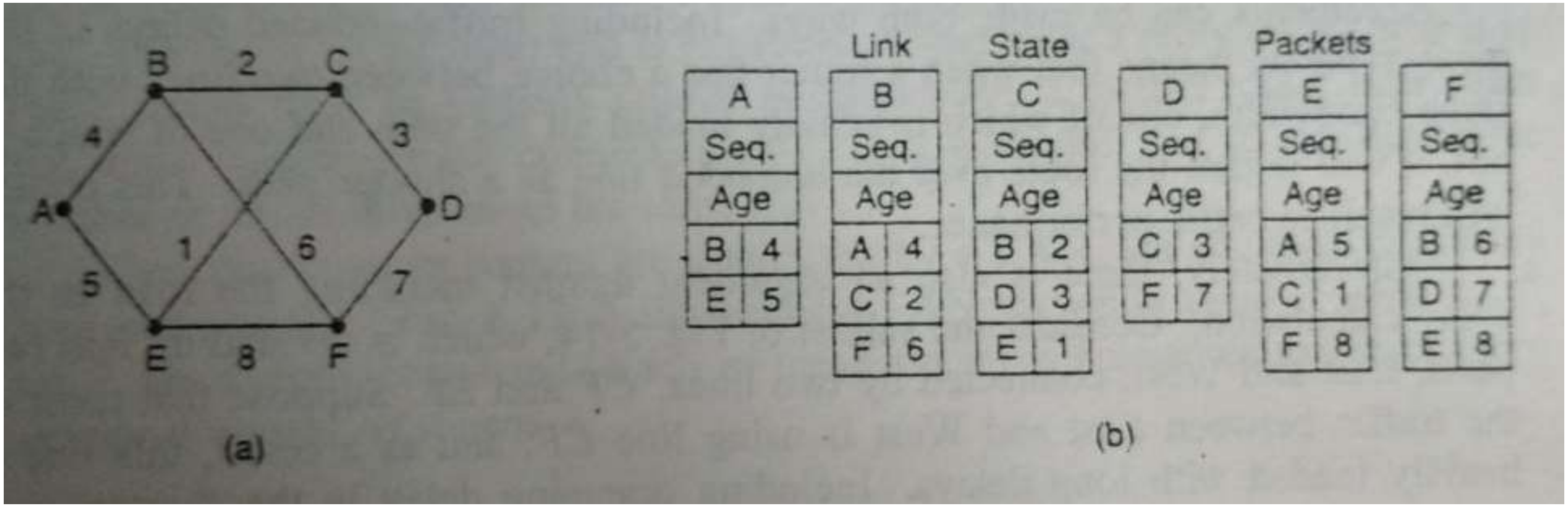
- Send an “ECHO” packet over the line.
- Destination is required to respond to “ECHO” packet immediately.
- Measure the time required for this operation

Types of Routing Algorithms- Adaptive

Link State Routing

3. Building Link State Packets

- Build a packet containing all the data



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

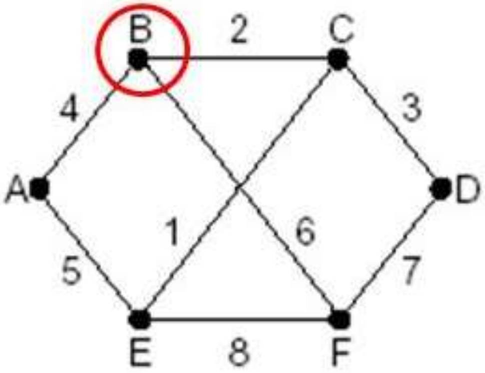
(b)

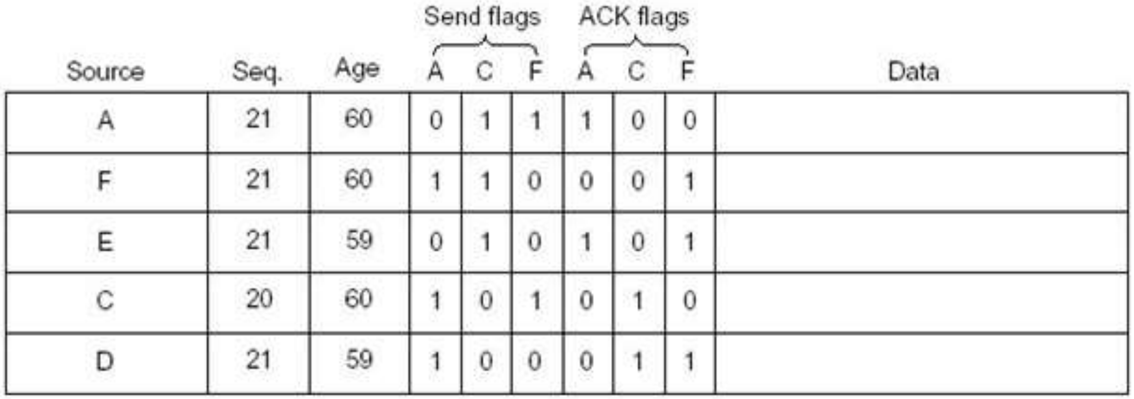
Types of Routing Algorithms- Adaptive

Link State Routing

4.Distributing the Link State Packets

- Use selective flooding
- Sequence numbers prevent duplicate packets from being propagated
- Lower sequence numbers are rejected as obsolete





			Send flags			ACK flags			
Source	Seq.	Age	A	C	F	A	C	F	Data
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	

Types of Routing Algorithms- Adaptive

Link State Routing

5. Computing the New Routes

- Dijkstra’s Shortest Path algorithm is used to determine the shortest path to each destination.

Types of Routing Algorithms- Adaptive

Hierarchical Routing

- One of the fundamental issues regarding routing is scaling.

a) As a network becomes larger, the amount of information that must be propagated increases, and the routing calculation becomes increasingly expensive.

b) Obviously, there are limits to how big a network can be.

Hierarchical routing is an approach that hides information from far-away nodes, reducing the amount of information a given router needs to perform routing:

- Divide the network into regions, with a router only knowing the details of how to route to other routers in its region.

a) In particular, a router does not know about the internal topology of other regions.

b) Gateway is a router that knows about other regions.

Types of Routing Algorithms- Adaptive

Hierarchical Routing

A node in each region is designated as an entry point, and the entry point knows how to reach the entry points in all the other regions.

When traffic flows from A to B, it actually follows the path

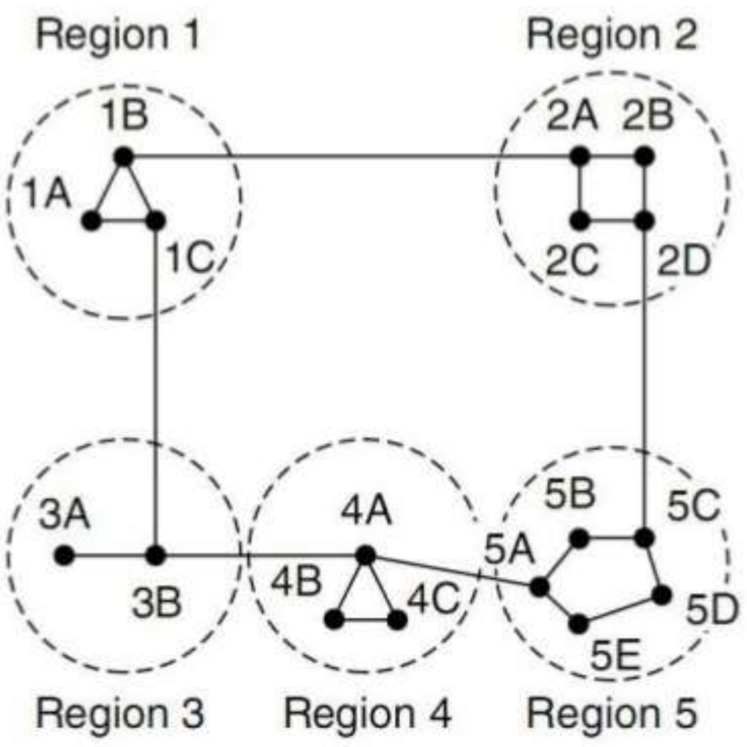
A - AENTRY - BENTRY - B,

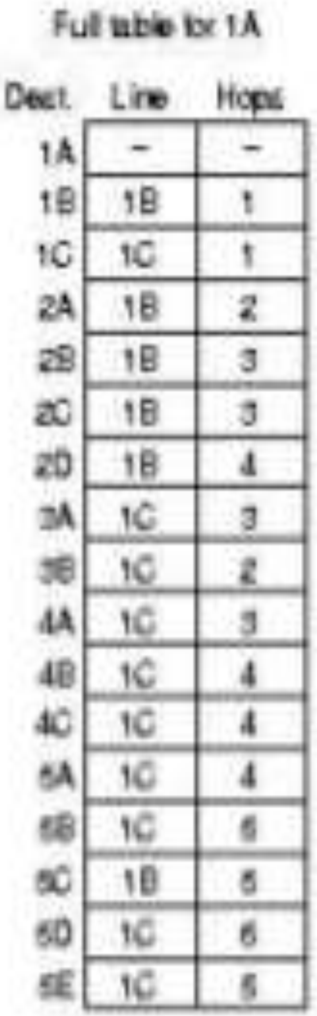
where AENTRY and BENTRY are the entry points to the respective regions.

- Advantage: Scaling. Each router needs less information (table space) to perform routing.
- Disadvantage: Sub optimal routes. The average path length increases because there may be a shorter path that bypasses the entry points, but we don't use it.

Types of Routing Algorithms- Adaptive

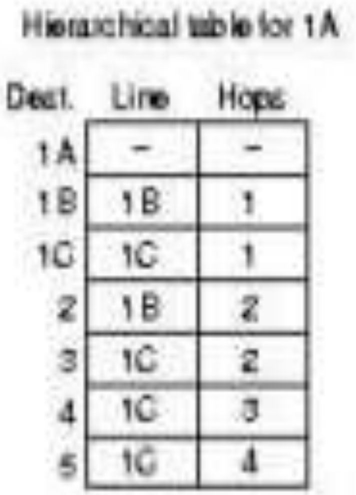
Hierarchical Routing





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



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

Types of Routing Algorithms- Adaptive

Broadcast Routing

- Sending a packet to all destinations simultaneously is known as broadcasting.
- There are several ways to implement broadcasting:
- For Broadcast Networks:

1. The implementation is trivial: designate a special address as the `all hosts address'.

- For non broadcast Networks:

1. Send a unicast packet to each destination. However, this approach makes poor use of resources.

2. Flood packets to all nodes. Flooding generates many packets and consumes too much bandwidth.

Types of Routing Algorithms- Adaptive

Broadcast Routing

- For non broadcast Networks:

  3. Use multi-destination routing:

     a) Each packet contains a list (or bitmap) of all destinations, and when a router forwards a packet across two or more lines, it splits the packet and divides the destination addresses accordingly.

     b) This approach is similar to sending uni-cast packets, except that we don't send individual copies of each messages.

     c) However, the copy operations slow down the ability of a router to process many packets.

Types of Routing Algorithms- Adaptive

Broadcast Routing

- For non broadcast Networks:

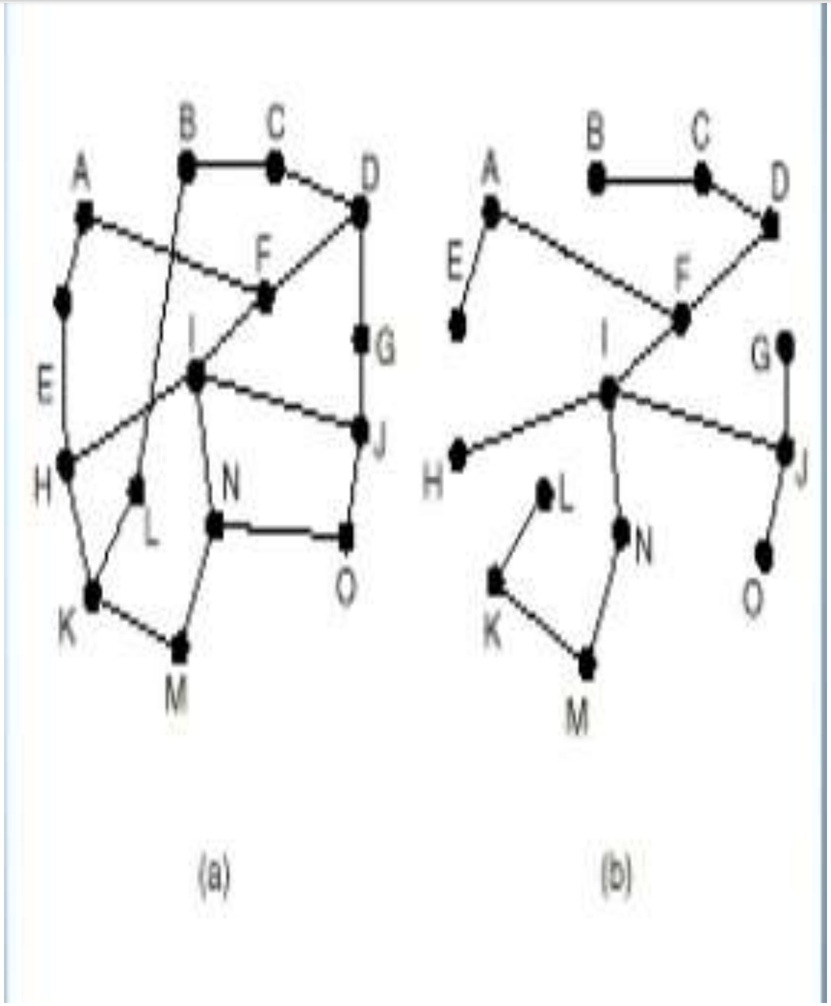
4. Use a spanning tree.

If the network can be reduced to a tree

a) (There's only one path between any two pairs of routers), copy a packet to each line of spanning tree except the one on which it arrived.

b) Works only if each router understands the same spanning tree.

c) Uses the minimum number of packets necessary



Types of Routing Algorithms- Adaptive

Broadcast Routing

- For non broadcast Networks:

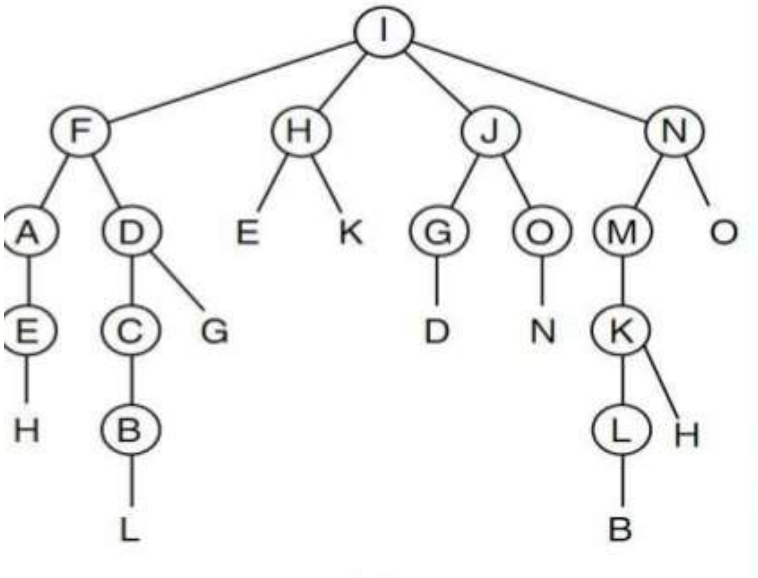
5. Reverse Path Forwarding (RPF):

a) Use a sink tree (assume sink/source trees are the same).

b) If a packet, originating from X, arrives on a line of the sink tree leading to X, the packet is traveling along the shortest path, so it "must" be the first copy we've seen.

c) Copy the packet to all outgoing lines of the sink tree. If the packet arrives on another line, assume that the packet is a copy - it didn't arrive on the shortest path - and discard it.

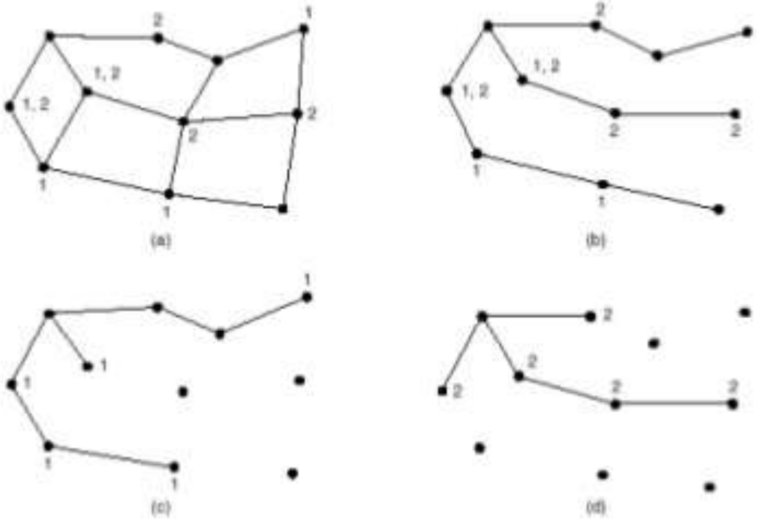
RPF is easy to implement and makes efficient use of bandwidth.



Types of Routing Algorithms- Adaptive

Multicast Routing

- A method to broadcast packets to well- defined groups
- Hosts can join multicast groups. – They inform their routers – Routers send group information throughout the subnet
- Each router computes a spanning tree for each group.
- The spanning tree includes all the routers needed to broadcast data to the group



Congestion control Algorithms(CO4)

Topic Objective

- To understand the basics of Congestion
- Various Congestion control algorithms
- Usage of the algorithms

Recap of previous topic

- Concept of Routing
- Usage of various routing algorithms

Congestion Control Algorithms(CO4)

- As Internet can be considered as a Queue of packets, where transmitting nodes are constantly adding packets and some of them (receiving nodes) are removing packets from the queue.
- So, consider a situation where too many packets are present in this queue (or internet or a part of internet), such that constantly transmitting nodes are pouring packets at a higher rate than receiving nodes are removing them.
- This degrades the performance, and such a situation is termed as Congestion. Main reason of congestion is more number of packets into the network than it can handle.

Congestion Control Algorithms

- When the number of packets dumped into the network is within the carrying capacity, they all are delivered, expect a few that have too be rejected due to transmission errors .
- As traffic increases too far, the routers are no longer able to cope, and they begin to lose packets. This tends to make matter worse.
- At very high traffic, performance collapse completely, and almost no packet is delivered

Causes of Congestion

- Congestion can occur due to several reasons.
- if all of a sudden a stream of packets arrive on several input lines and need to be out on the same output line, then a long queue will be build up for that output. If there is insufficient memory to hold these packets, then packets will be lost (dropped) .
- If router have an infinite amount of memory even then instead of congestion being reduced, it gets worse; because by the time packets gets at the head of the queue, to be dispatched out to the output line, they have already timed-out.
- All the packets will be forwarded to next router up to the destination, all the way only increasing the load to the network more and more.
- Finally when it arrives at the destination, the packet will be discarded, due to time out, so instead of been dropped at any intermediate router (in case memory is restricted) such a packet goes all the way up to the destination, increasing the network load throughout and then finally gets dropped there.
- Slow processors also cause Congestion. If the router CPU is slow at performing the task .

Effects of Congestion

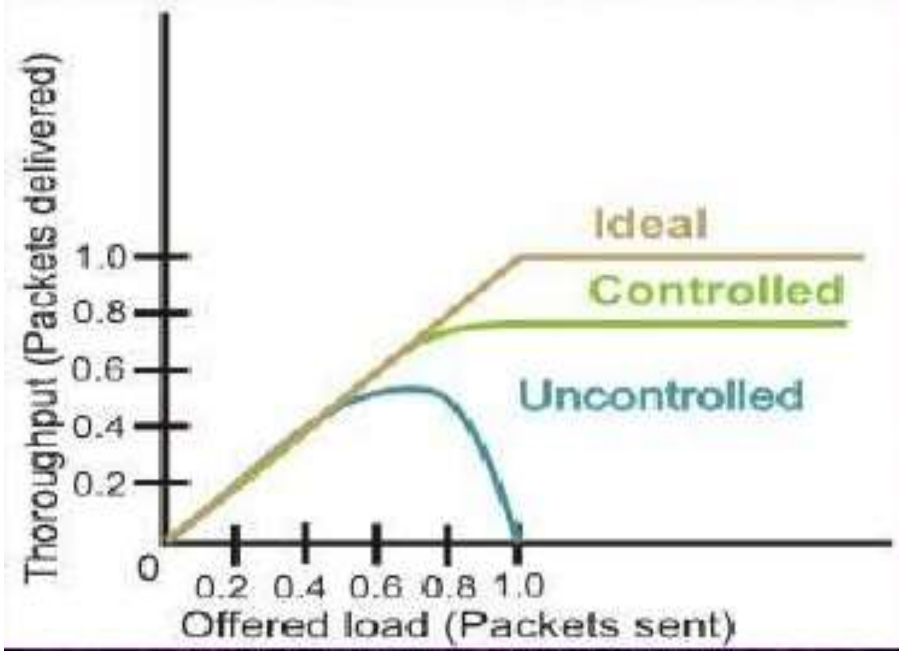
Congestion affects two vital parameters of the network performance .

1. Through put
2. Delay

- Initially throughput increases linearly with offered load, because utilization of the network increases.
- However, as the offered load increases beyond certain limit, say 60% of the capacity of the network, the throughput drops.
- If the offered load increases further, a point is reached when not a single packet is delivered to any destination, which is commonly known as deadlock situation

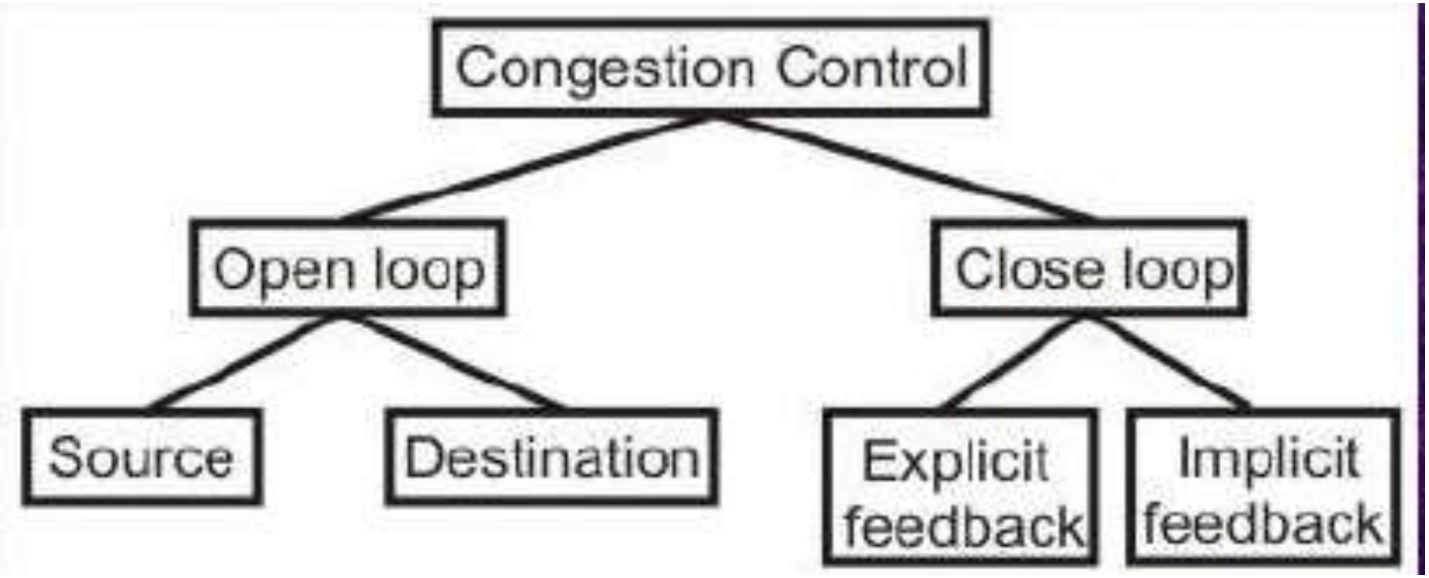
Effects of Congestion

- The ideal one corresponds to the situation when all the packets introduced are delivered to their destination up to the maximum capacity of the network.
- The second one corresponds to the situation when there is no congestion control.
- The third one is the case when some congestion control technique is used. This prevents the throughput collapse, but provides lesser throughput than the ideal condition due to overhead of the congestion control technique



Congestion Control Techniques

- Open loop: Protocols to prevent or avoid congestion, ensuring that the system never enters a Congested State.
- Close loop: Protocols that allow system to enter congested state, detect it, and remove it.



Congestion Control Techniques(CO5)

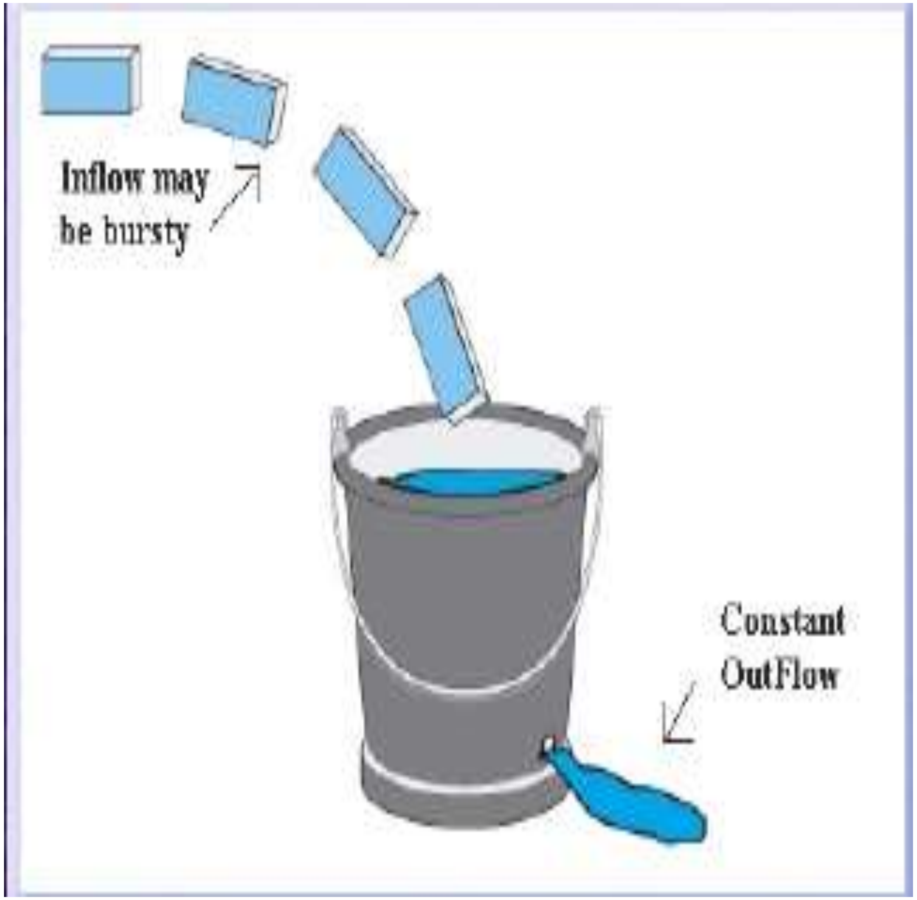
Open Loop Approach

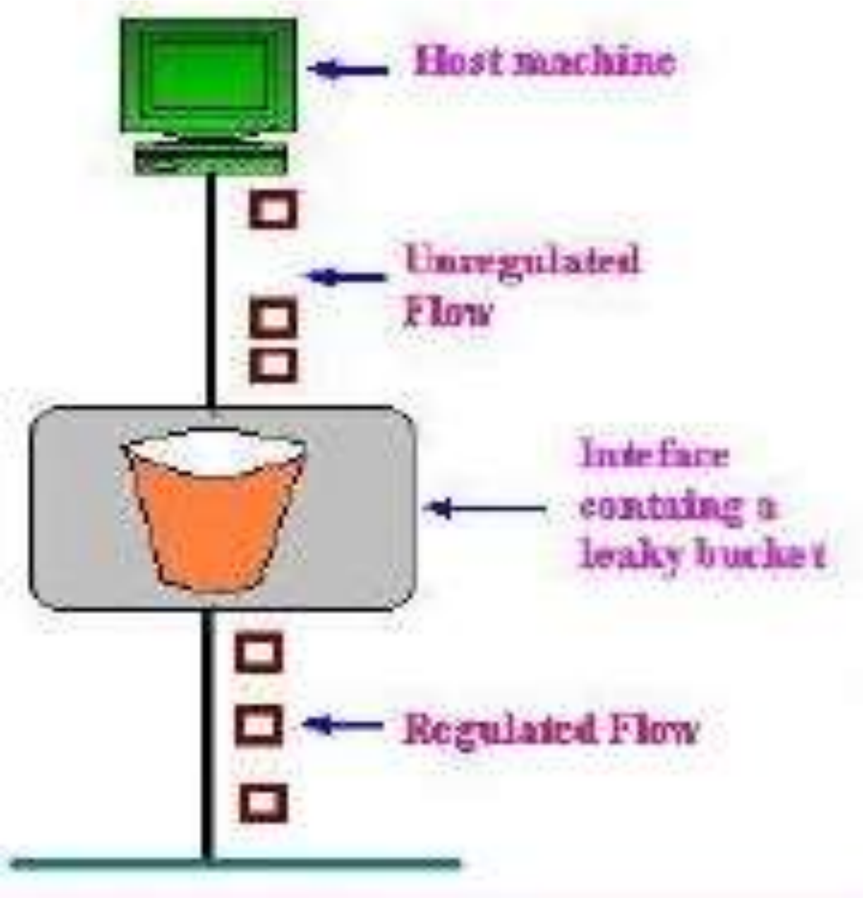
1.Leaky Bucket Algorithm

Consider a Bucket with a small hole at the bottom, whatever may be the rate of water pouring into the bucket, the rate at which water comes out from that small hole is constant. Once the bucket is full, any additional water entering it spills over the sides and is lost . The same idea of leaky bucket is applied to packets. When the host has to send a packet, the packet is thrown into the bucket. The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate

Congestion Control Techniques

Leaky Bucket Algorithm





Congestion Control Techniques

Open Loop Approach

2.Token Bucket Algorithm

For many applications it is better to allow the output to speed up somewhat when a larger burst arrives than to loose the data. In this algorithm leaky bucket holds token, generated at regular intervals.

In regular intervals tokens are thrown into the bucket.

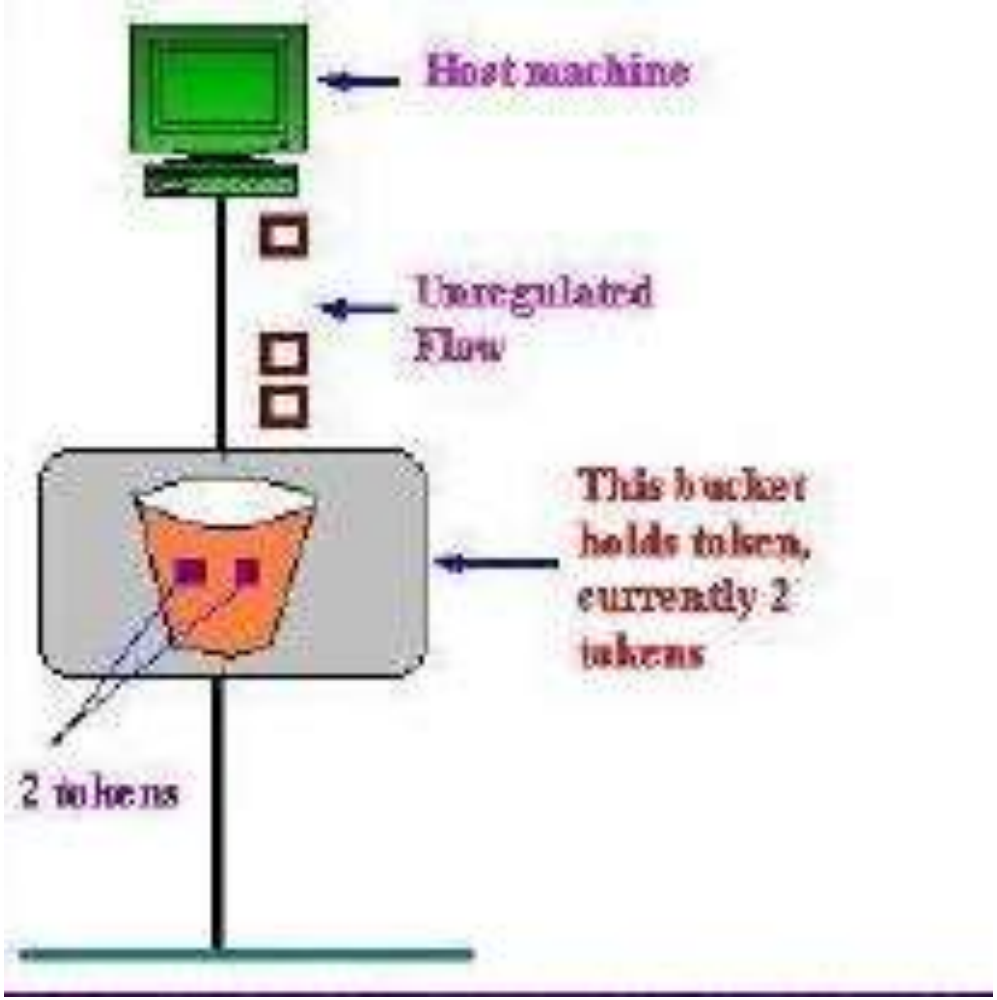
The bucket has a maximum capacity.

If there is a ready packet, a token is removed from the bucket, and the packet is send.

If there is no token in the bucket, the packet cannot be send.

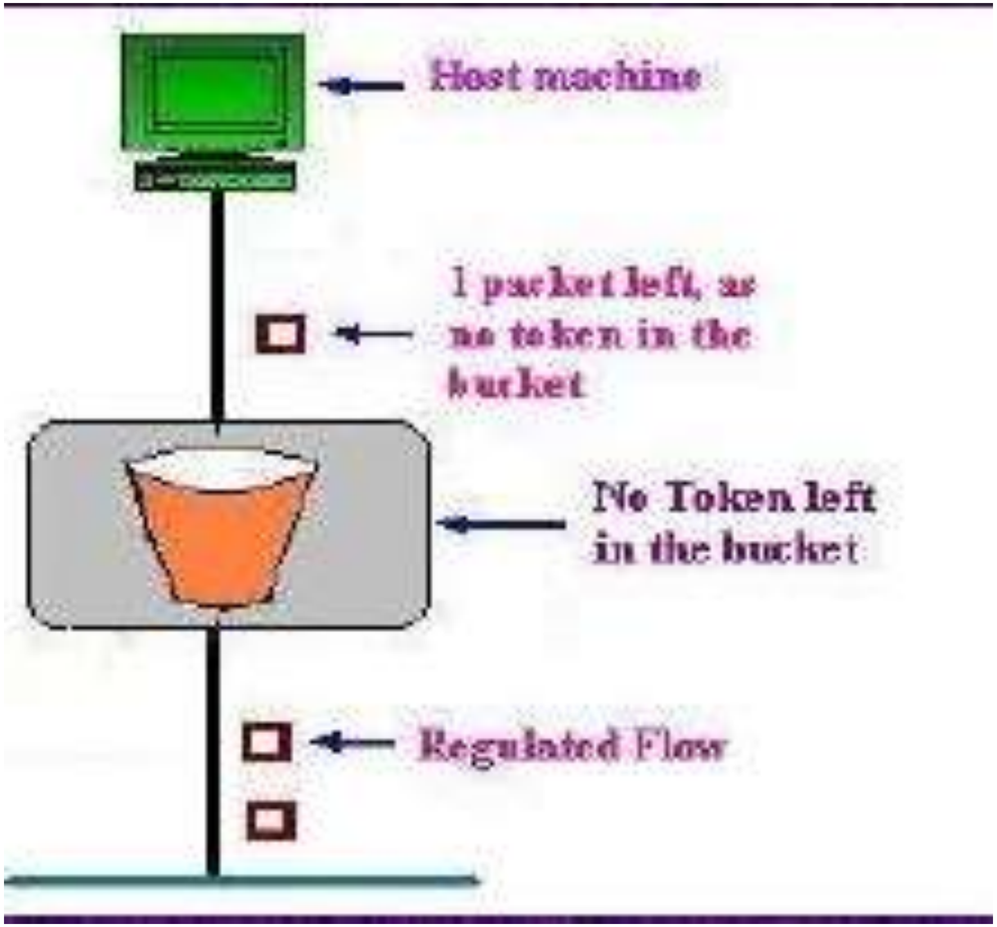
Congestion Control Techniques

Token Bucket Algorithm – a bucket has two tokens and three packets to be delivered



Congestion Control Techniques

Token Bucket Algorithm – after two tokens consumed for two packets and left with one packet to be delivered


Host machine
1 packet left, as no token in the bucket
No Token left in the bucket
Regulated Flow

Congestion Control Techniques

Congestion control in virtual Circuit

- Admission control is one such closed-loop technique, where action is taken once congestion is detected in the network.
- Simpler one “Do not set-up new connections, once the congestion is signalled. This type of approach is often used in normal telephone networks. When the exchange is overloaded, then no new calls are established. “
- Another approach “To allow new virtual connections, but route these carefully so that none of the congested router (or none of the problem area) is a part of this route”

Congestion Control Techniques

Choke Packet Technique

- Each router monitors its resources and the utilization at each of its output line.
- There is a threshold set by the administrator, and whenever any of the resource utilization crosses this threshold and action is taken to curtail down this.
- For Example, when source A receives a choke packet with destination B at first, it will curtail down the traffic to destination B by 50%, and if again after a fixed duration of time interval it receives the choke packet again for the same destination, it will further curtail down the traffic by 25% more and so on

Congestion Control Techniques

Choke Packet Technique

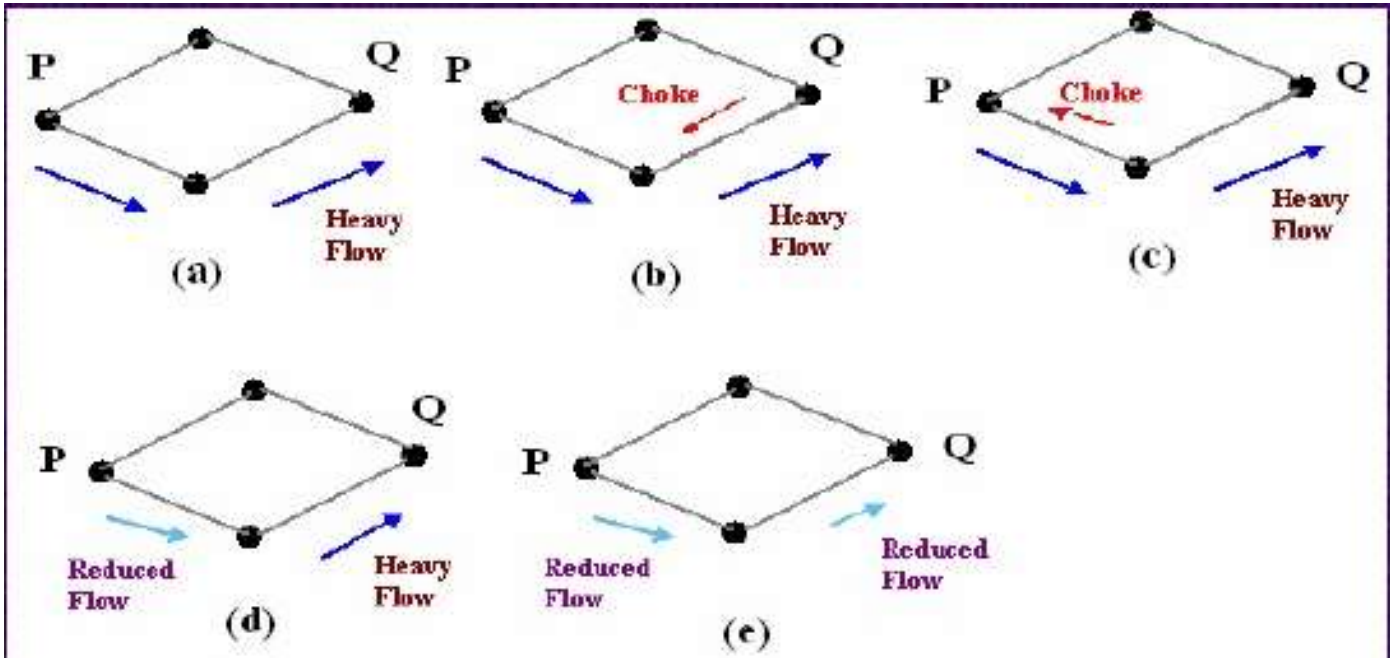
(a) Heavy traffic between nodes P and Q,

(b) Node Q sends the Choke packet to P,

(c) Choke packet reaches P,

(d) P reduces the flow and send a reduced flow out,

(e) Reduced flow reaches node



Congestion Control Techniques

Hop-by-Hop Choke Packets

- This technique is an advancement over Choked packet method.
- At high speed over long distances, sending a packet all the way back to the source doesn't help much, because by the time choke packet reach the source, already a lot of packets destined to the same original destination would be out from the source.
- Hop-by-Hop Choke packets are used.
- the choke packet affects each and every intermediate router through which it passes by.
- Here, as soon as choke packet reaches a router back to its path to the source, it curtails down the traffic between those intermediate routers. intermediate nodes must dedicate few more buffers for the incoming traffic as the outflow through that node will be curtailed down immediately as choke packet arrives it, but the input traffic flow will only be curtailed down when choke packet reaches the node which is before it in the original path.

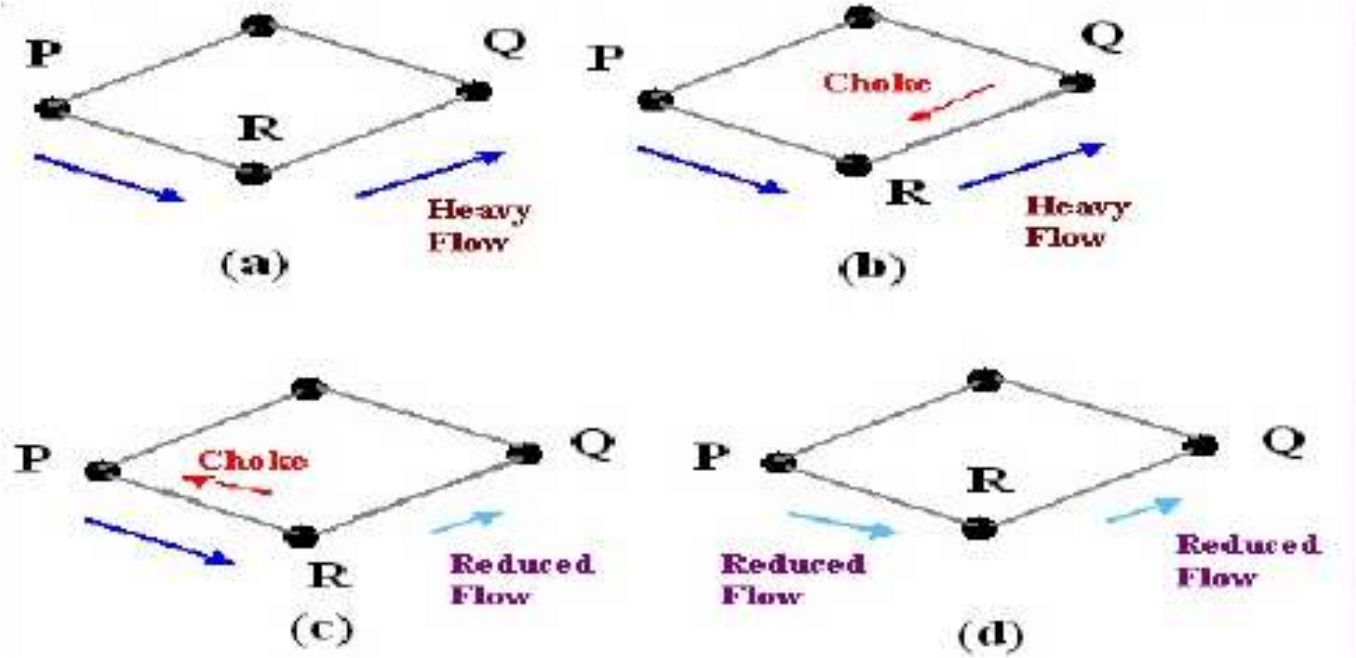
Congestion Control Techniques

Hop-By-Hop

a) Heavy traffic between nodes P and Q,

(b) Node Q sends the Choke packet to P,
(c) Choke packet reaches R, and the flow between R and Q is curtail down,

(d)Choke packer reaches P, and P reduces the flow out



Congestion Control Techniques

Load Shedding

- one of the simplest and more effective techniques.
- whenever a router finds that there is congestion in the network, it simply starts dropping out the packets.
- There are different methods by which a host can find out which packets to drop.
- choose the packets randomly which has to be dropped.
- For many applications, some packets are more important than others. So, sender can mark the packets in priority classes to indicate how important they are. If such a priority policy is implemented than intermediate nodes can drop packets from the lower priority classes and use the available bandwidth for the more important packets.

Internet as a connectionless protocol(CO3)

- The connectionless network services are also known as datagrams.
- The internet at the network layer works as packet-switched network.
- Internet routes the packets by using universal address defined in the network layer.
- In connectionless service, the network layer protocol operates each packet independently.
- The internet is built from several heterogeneous networks. So, it is not possible to create a connection between the source and destination, before knowing the nature of the network.

Internet as a connectionless protocol(CO3)

Addressing Scheme

- IP addresses are of 4 bytes and consist of :
  i) The network address- network on which the host resides
  ii) The host address - identifies the particular host on the given network
- A fixed size for each of these would lead to wastage or under-usage that is either there will be too many network addresses and few hosts in each
- or there will be very few network addresses and lots of hosts

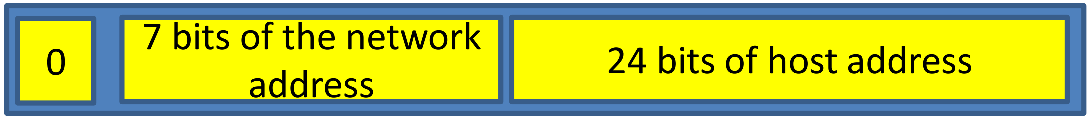
Internet as a connectionless protocol

Addressing

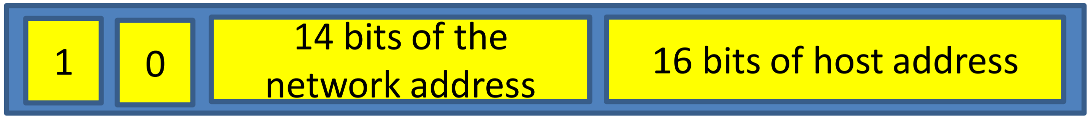
- **Large Networks :** 8-bit network address and 24-bit host address.
- **Medium Networks :** 16-bit network address and 16-bit host address.
- **Small networks :** 24-bit network address and 8-bit host address.

Internet as a connectionless protocol

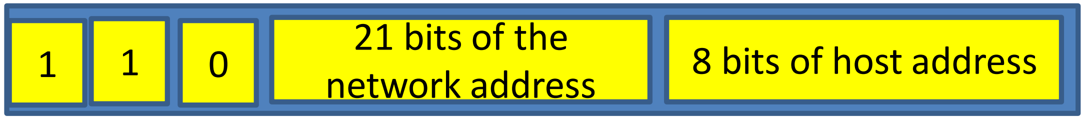
Class A – For large networks



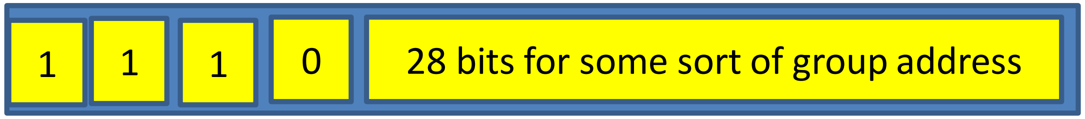
Class B - For medium networks



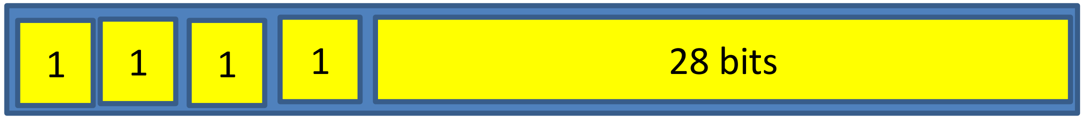
Class C - For small networks



Class D - For multi-cast messages (multi-cast to a "group" of networks)



Class E - Currently unused, reserved for potential uses in the future



IPv4(CO3)

- The **Internet Protocol version 4 (IPv4)** is a connectionless protocol which is used for delivery mechanism (used by TCP/ IP protocols).
- The IPv4 is an unreliable protocol, but to make it reliable IPv4 is paired with a reliable protocol such as TCP.
- The IPv4 uses the datagram approach which means, that each datagram is handled independently and each datagram can follow the different route to the destination. Due to this, the datagrams sent from the same source to the same destination can reach at any order while some may get lost.

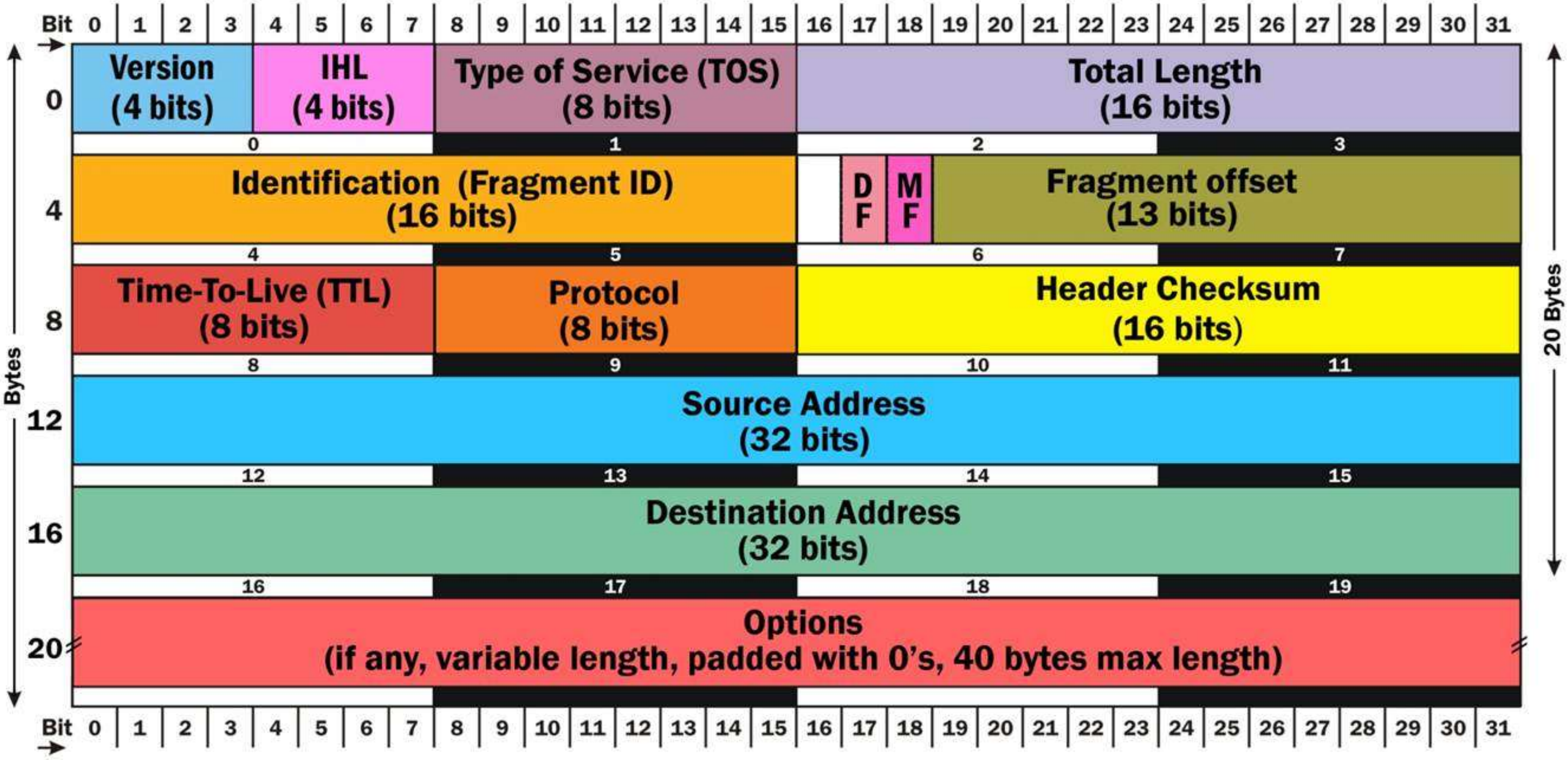
IPv4

- Datagrams
  - Packets in the IPv4 layer are called as datagrams.
  - A datagram is a variable- length packet consists of header and data.
  - The size of header is 20 to 60 bytes, which is essential for routing and delivery.
- Fragmentation
  - The data travels through the different networks. Each router first decapsulates the IPv4 datagram from the received frame, then process it and again encapsulates in the another frame.
  - The format and the size depends on the protocol used by the physical network through which it is going to travel.
- Maximum Transfer Unit
  - When a datagram is encapsulated in a frame, the total size of the datagram should be less than maximum size, which is defined or restricted by the hardware and software used in the network.

IPv4

- **IPv4** - **Packet Structure**. Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into **packets**.
- IP **packet** encapsulates data unit received from above layer and add to its own **header** information.
- The encapsulated data is referred to as IP Payload.

IPv4



Bit 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Bytes
0
4
8
12
16
20
Version (4 bits)
IHL (4 bits)
Type of Service (TOS) (8 bits)
Total Length (16 bits)
0 1 2 3
Identification (Fragment ID) (16 bits)
D F
M F
Fragment offset (13 bits)
4 5 6 7
Time-To-Live (TTL) (8 bits)
Protocol (8 bits)
Header Checksum (16 bits)
8 9 10 11
Source Address (32 bits)
12 13 14 15
Destination Address (32 bits)
16 17 18 19
Options (if any, variable length, padded with 0's, 40 bytes max length)
20 Bytes

IPv4

- The *Header Length* field (4 bits) indicates how long the header is, in 32 bit “words”.
- The *Type of Service* field (8 bits implement a fairly simple QoS (Quality of Service).
- The *Total Length* field (16 bits) contains the total length of the packet, including the packet header, in bytes.
- The *Identification (Fragment ID)* field (16 bits) identifies which fragment of a once larger packet this one is, to help in reassembling the fragmented packet later.
- The next three bits are flags related to fragmentation. The first is reserved and must be zero.

IPv4

- The next bit is the **DF** (Don’t Fragment) flag. If DF is set, the packet cannot be fragmented (so if such a packet reaches a part of the network that can’t handle one that big, that packet is dropped).
- The third bit is the **MF** (More Fragments) flag. If MF is set, there are more fragments to come. Unfragmented packets of course have the MF flag set to zero.

IPv4

- The *Fragment Offset* field (13 bits) is used in reassembly of fragmented packets. It is measured in 8 byte blocks. The first fragment of a set has an offset of 0.
- If you had a 2500 byte packet, and it was fragmented into chunks of 1000 bytes or less, you would have three fragments as follows:

Fragment ID	MF Flag	Total Length	Data Size	Offset
1	1	1020	1000	0
2	1	1020	1000	125
3	0	520	500	250

IPv4

The *Time To Live (TTL)* field (8 bits) is to prevent packets from being shuttled around indefinitely on a network.

The *Header Checksum* field (16 bits).

The *Source Address* field (32 bits) contains the IPv4 address of the sender

The *Destination Address* field (32 bits) contains the IPv4 address of the recipient

Options (0 to 40 bytes)

IPv4

IPv4 is well designed, but has some shortfalls, which are listed below:

- The real-time audio and video transmission should properly work on the Internet. This type of transmission needs minimum delay strategies and reservation of the resources, which are not provided in IPv4.
- Encryption and authentication facility is not provided in the IPv4.
- Address depletion problem.