CN Module 3 Important topics

What is network layer.? What are the functions of network layer.?

- This layer performs network routing, flow control and error control functions. Network routing simply means the way packets are routed from source to destination and flow control. prevents the possibility of congestion between packets which are present in the subnet.
- The main task of this layer is to decide the path from multiple paths. That is the key design issue is determining how packets are routed from source to destination. They are highly dynamic

---

What are the different design issues of network layer.?

Store-and-Forward Packet Switching

- A sending device (host) sends a packet to the nearest router.
- The packet is temporarily stored at the router to verify its integrity using a checksum.
- Once the checksum is verified, the packet is forwarded to the next router in the path.
- This process is repeated until the packet reaches the destination host, where it is delivered.
- This method is known as store-and-forward packet switching

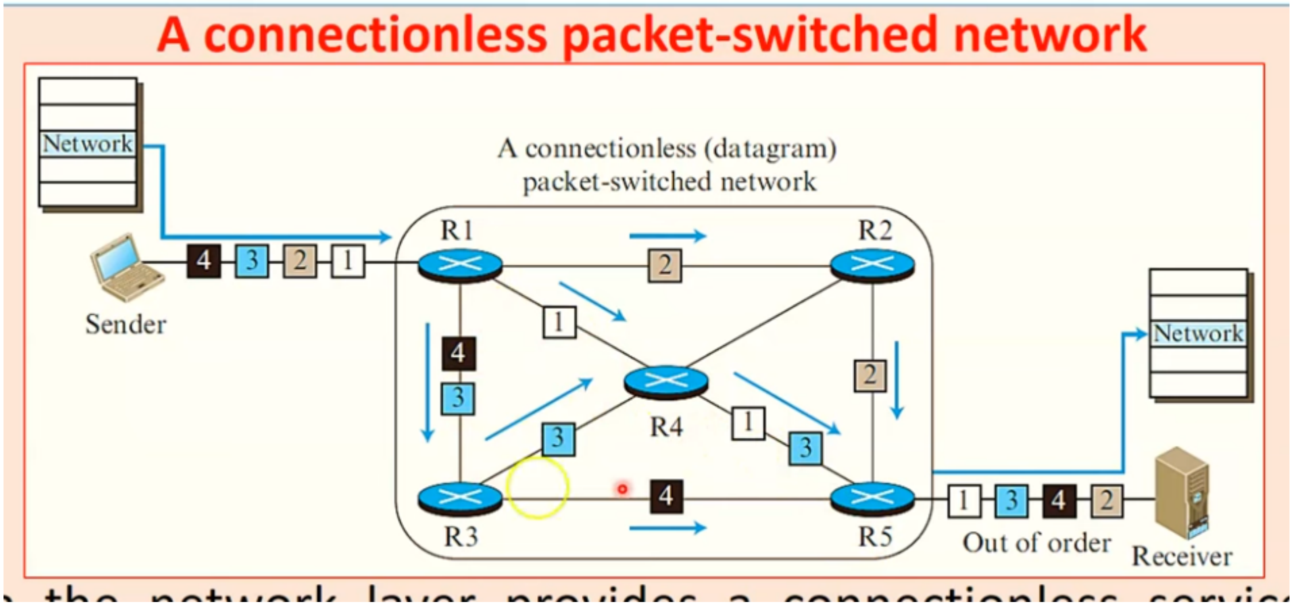
Connected devices in packet switched network still need to decide how to route the packets to final destination

There are two approaches to route

Datagram approach: Connectionless service

- Treats each packet independently
  - Each packet has no relationship to other packets

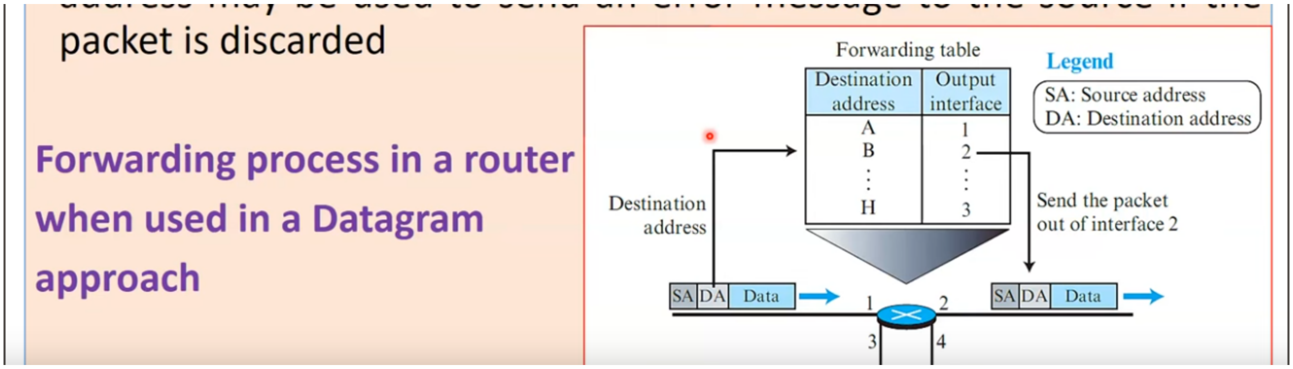
- Packets in a message may or may not travel in the same path to destination



A connectionless packet-switched network

A connectionless (datagram) packet-switched network

the network layer provides a connectionless servic

- Here the packets 1,2,3,4 and sent
- Each packet are going through different path(Different routers)
  - 4,3 going from R1,R3
  - 2 going from R1,R2
  - 1 Going from R1,R4
- Each packet is routed based on 2 values, source and destination
- 

  address may be used to send an error message to the source if the packet is discarded

  Forwarding process in a router when used in a Datagram approach

  Forwarding table

Destination address	Output interface
A	1
B	2
⋮	⋮
H	3

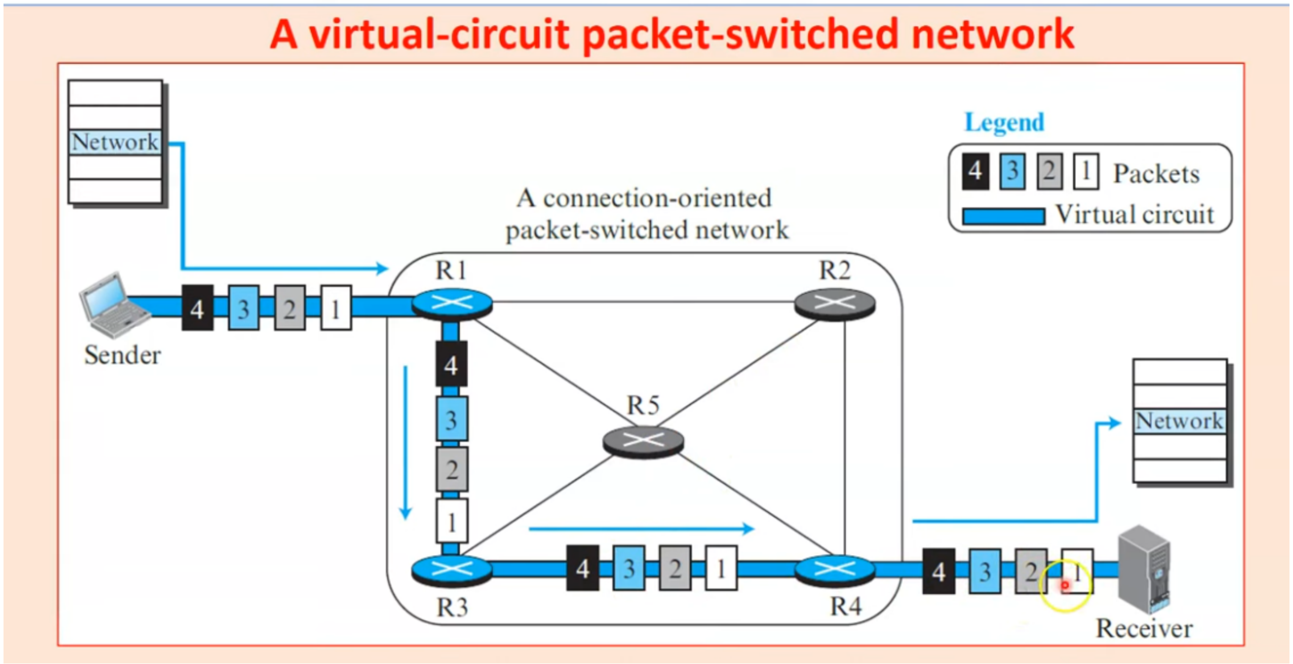
  Legend
  SA: Source address
  DA: Destination address

- This is how the routing of packets take place, We use a forwarding table
  - A forwarding table consists of destination address and output interface
  - This table gets updated based on the best routing possible
- Example: If a packet of desination A reached the router, it will be sent to interface 1

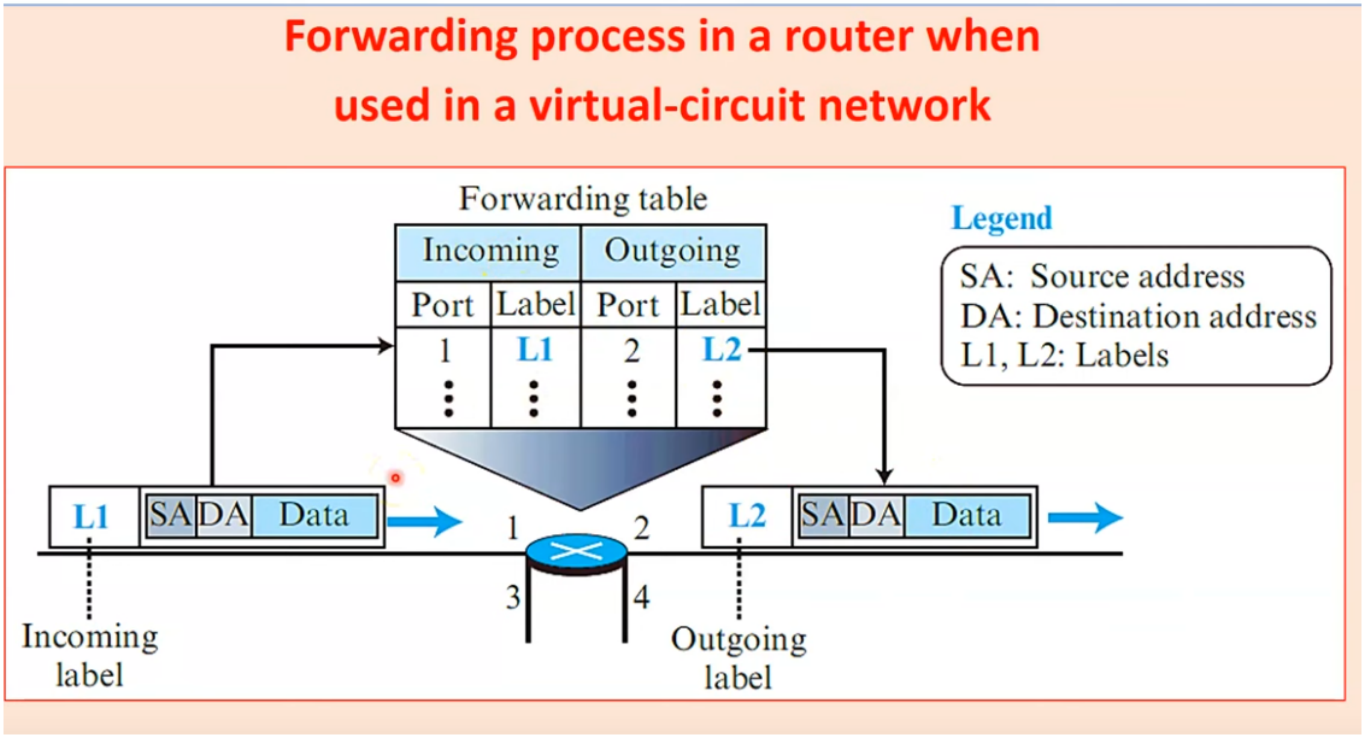
Virtual Circuit Approach: Connection oriented service

- In a connection oriented service, There is a relationship between all packets belonging to a message
- For all the datagram to go to the same path, a virtual connection will be setup
- The packet contains the following things
  - Source address

- Desintation address
- Flow label
- Virtual Circuit identifier
- Defines the virtual path



A virtual-circuit packet-switched network



Forwarding process in a router when used in a virtual-circuit network

Forwarding table

Incoming		Outgoing	
Port	Label	Port	Label
1	L1	2	L2
⋮	⋮	⋮	⋮

Legend

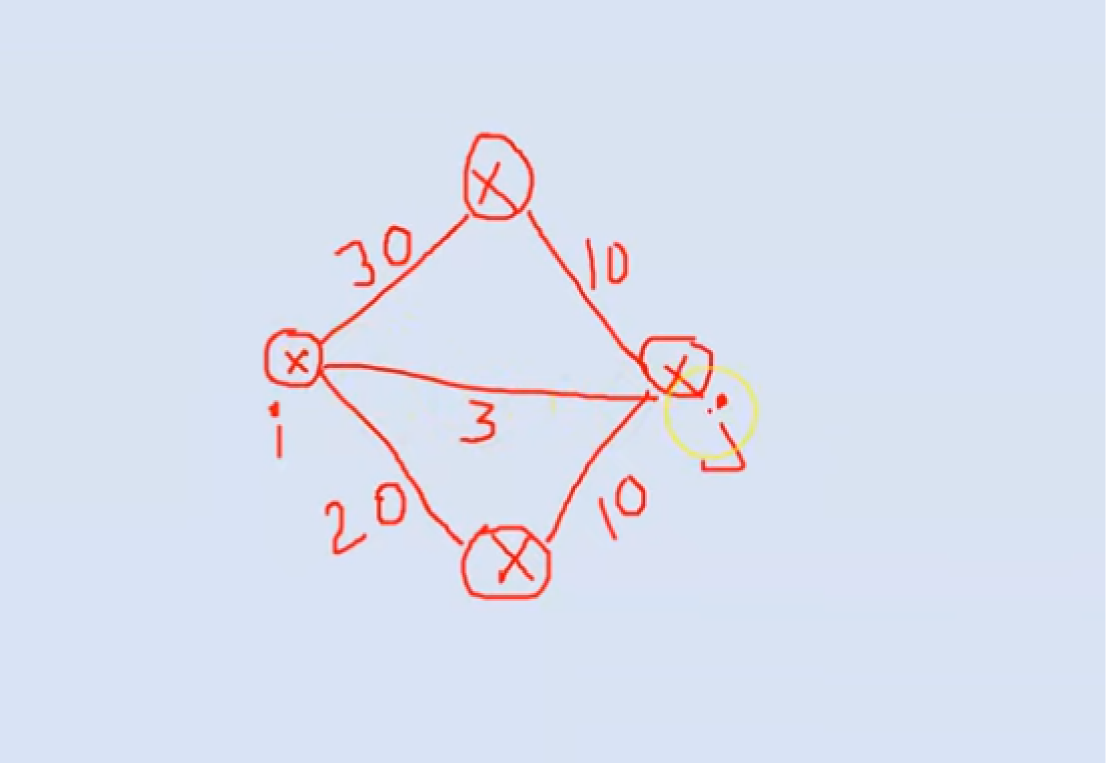
SA: Source address
DA: Destination address
L1, L2: Labels

- Here the forwarding table has incoming and outgoing
  - Inside that we have port and label

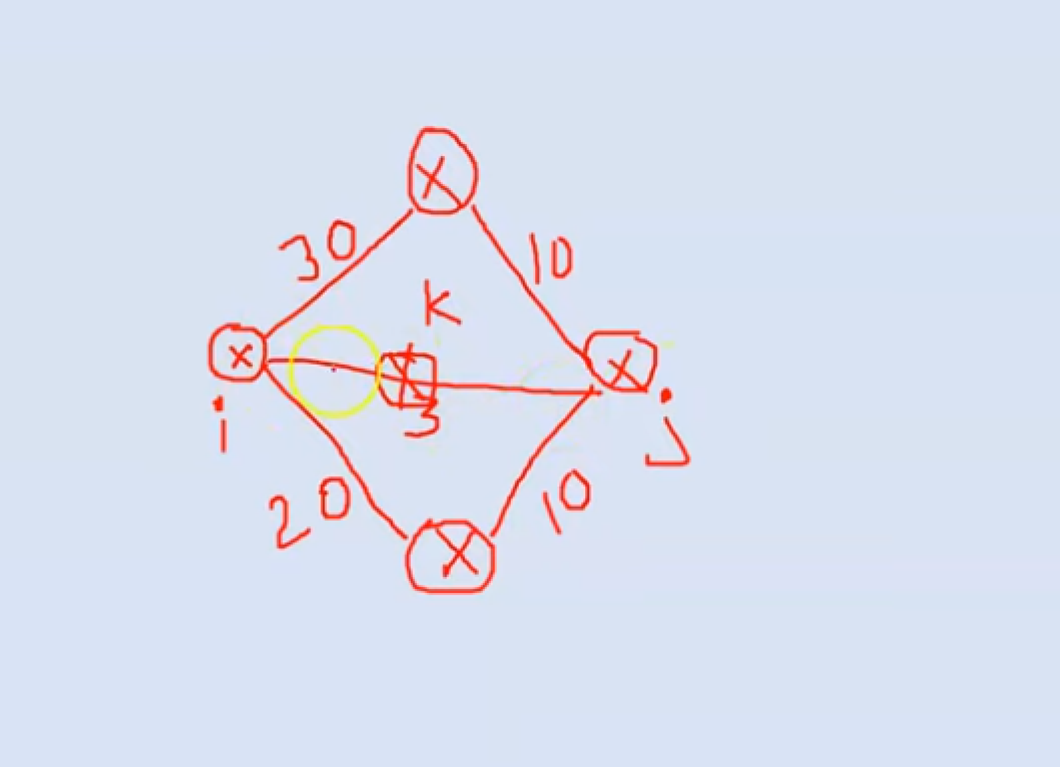
Explain the Optimality principle.

- The purpose of a routing algorithm at router is to decide which output line a packet should go
- The criteria for an optimal path are
    - least cost path
    - least distance path
    - least time path
    - least hops path
- If a particular path is optimal between 2 nodes, if there is a 3rd node between them, in between them also the distance will be optimal

Example



- Here 30,10,20,10,3 the costs, between each router
- 3 is having the least cost, so its the most optimal
- Suppose we insert another node

- 

- i -> k and k -> j will also be minimal

Discuss the shortest path routing. Also explain the Dijkstra's algorithm in detail.

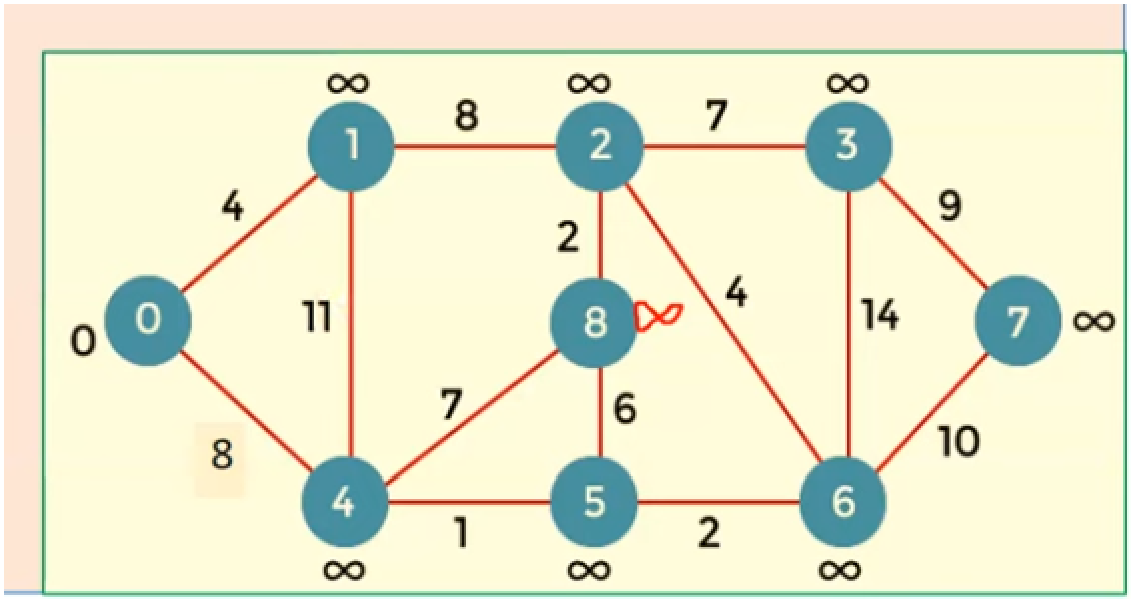
Shortest path routing

- Its a static routing algorithm
- to choose a route between any 2 notes, it simply chooses the one with shorter distance
- Shortest path can be defined as
    - Path where Anyone or more metrics are minimized
    - Metric can be
        - Distance
        - Bandwidth
        - Average traffic
        - Communication cost
        - Mean queue length

Djikstras Algorithm

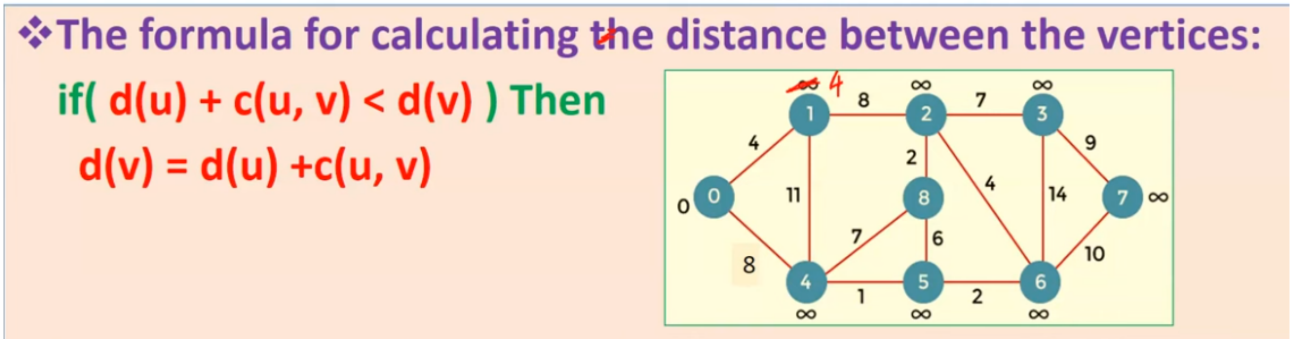
- Single source shortest path algorithm

- It means only one source is given
    - Shortest path from that source to all the nodes



- digarh University, Punjab EDULINE 28
- Start with a source vertex, Let it be 0
- We have 2 paths from 0
    - 0 -> 1
    - 0 -> 4
- Lets consisder 0->1

- Let 0 be x and 1 be y
- We have Distance of x d(x) = 0
- We have Distance of y d(y) = infinity
- We have the cost between x and y, c(x,y) = 4
- So to calculate the distance between 0 and 1
- d(x,y) = d(x) + c(x,y) <d(y)
- 0+4 < infinity
- Since 4 is less than infinity, we can update the value of d(y)
- d(y) = 4



❖The formula for calculating the distance between the vertices:

if(d(u) + c(u, v) < d(v)) Then

d(v) = d(u) +c(u, v)

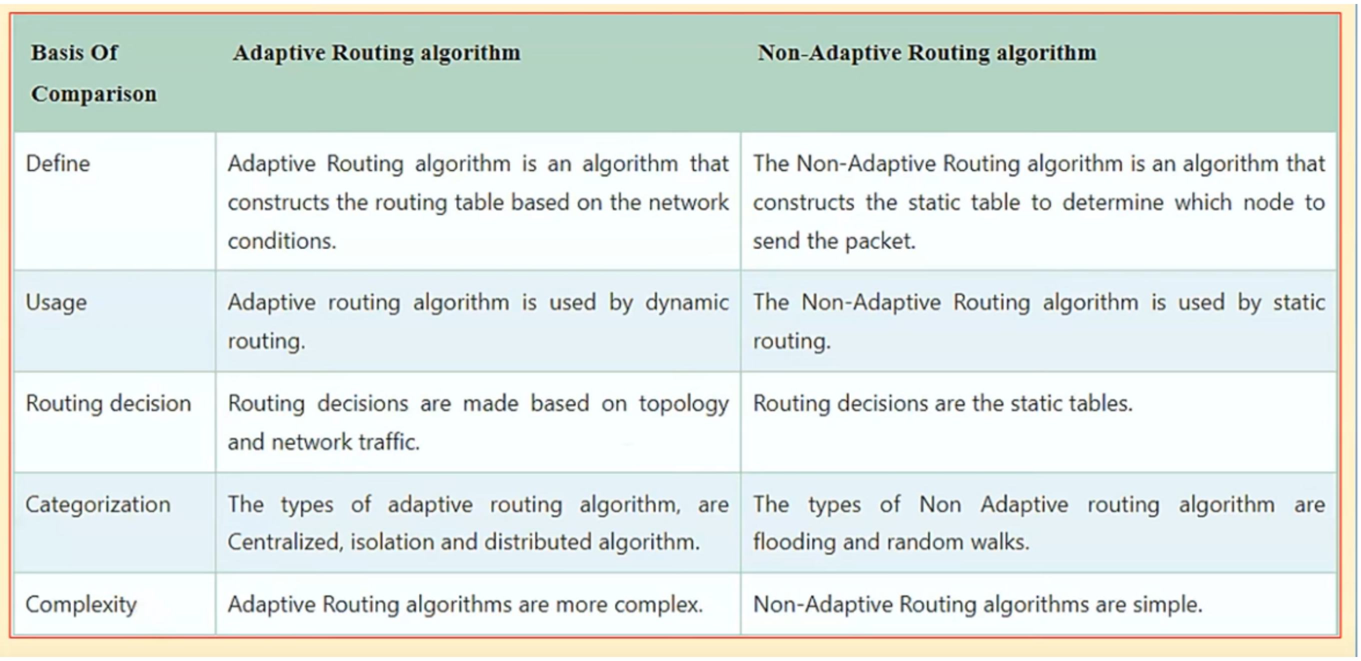
Differentiate between static and dynamic routing.

Dynamic routing

- Makes decision based on topology and network traffic
- Parameters used
  - Hop count, distance, estimated transit time

Static routing

- Doesnt make decision based on topology and network traffic



Basis Of Comparison	Adaptive Routing algorithm	Non-Adaptive Routing algorithm
Define	Adaptive Routing algorithm is an algorithm that constructs the routing table based on the network conditions.	The Non-Adaptive Routing algorithm is an algorithm that constructs the static table to determine which node to send the packet.
Usage	Adaptive routing algorithm is used by dynamic routing.	The Non-Adaptive Routing algorithm is used by static routing.
Routing decision	Routing decisions are made based on topology and network traffic.	Routing decisions are the static tables.
Categorization	The types of adaptive routing algorithm, are Centralized, isolation and distributed algorithm.	The types of Non Adaptive routing algorithm are flooding and random walks.
Complexity	Adaptive Routing algorithms are more complex.	Non-Adaptive Routing algorithms are simple.

Describe the distance vector routing algorithm in detail.

- Distance vector routing is a dynamic algorithm
- Each router maintains a distance table known as vector
- Information about the table is sent to the neighbours every 30 seconds

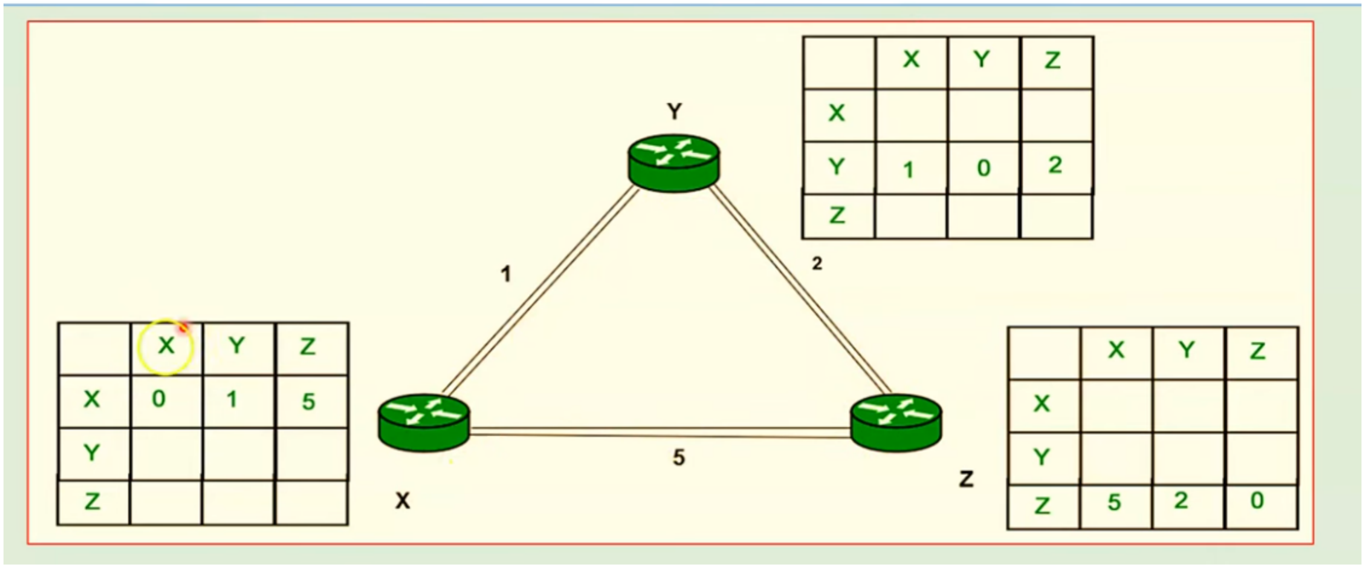
Algorithm

1. A router transmits its distance vector to each of its neighbors in a routing packet.
2. Each router receives and saves the most recently received distance vector from each of its neighbors.

3. A router recalculates its distance vector when
    1. It receives a distance vector from a neighbor containing different information than before.
    2. It discovers that a link to a neighbor has gone down

Example

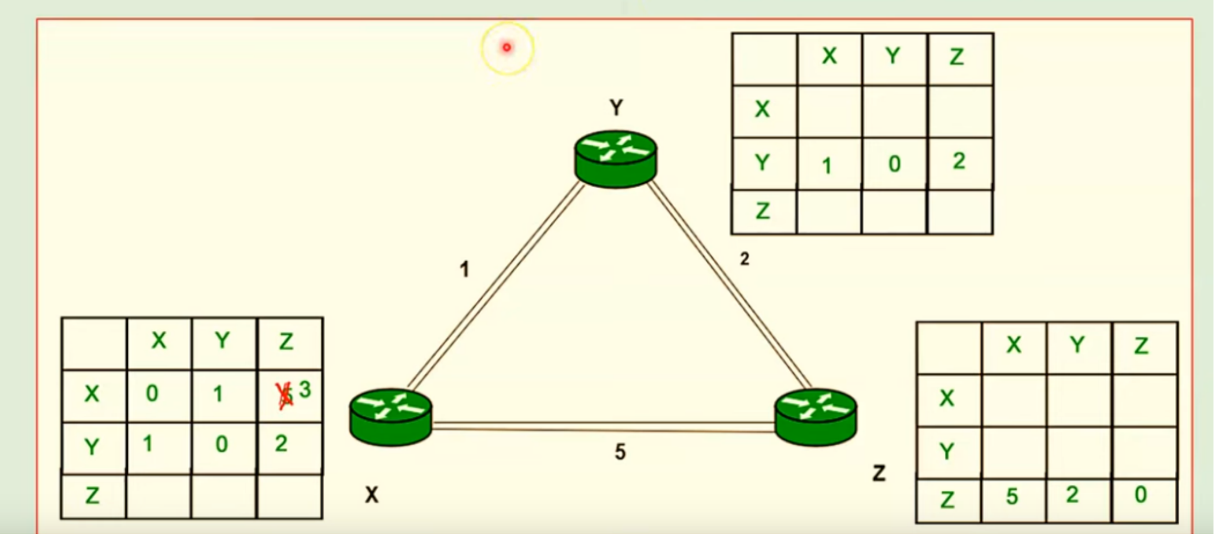
We have 3 routers



	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X	0	1	5
Y			
Z			

	X	Y	Z
X			
Y			
Z	5	2	0

- Each has their distance table
- information from Y, is sent to X
    - 

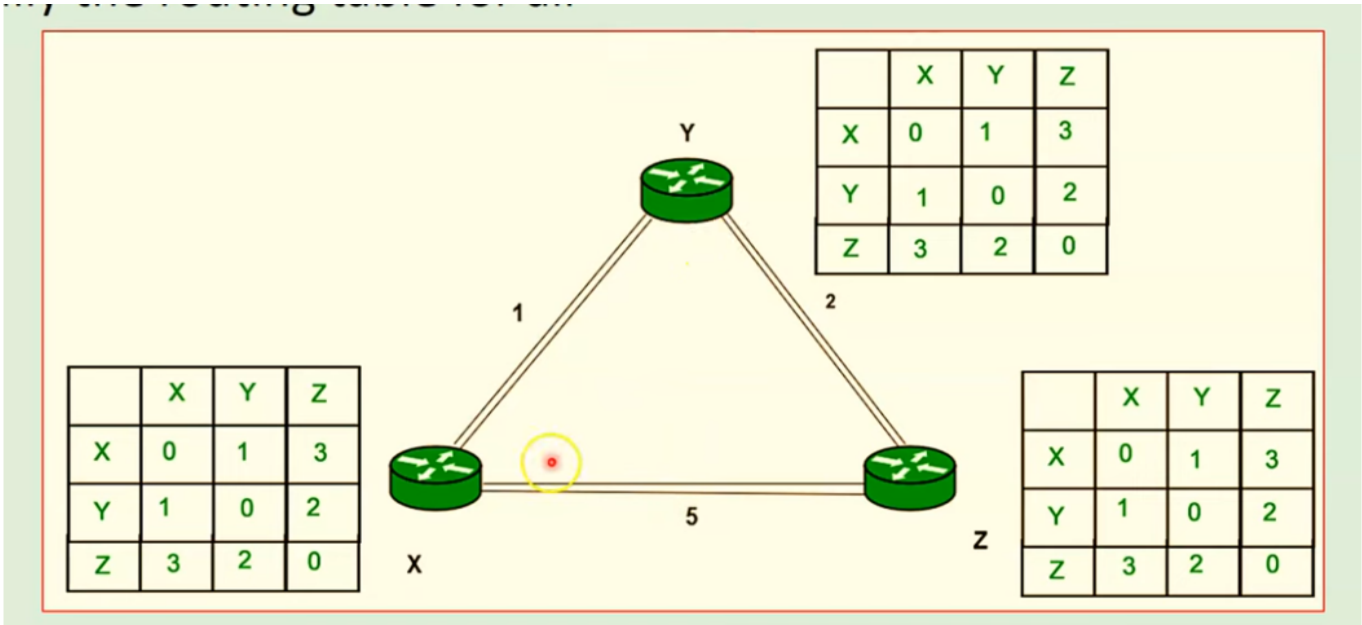
	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X	0	1	~~5~~ 3
Y	1	0	2
Z			

	X	Y	Z
X			
Y			
Z	5	2	0

- Based on this new information, it finds theres a shorter distance X->Y->Z which is 3

At the end we get

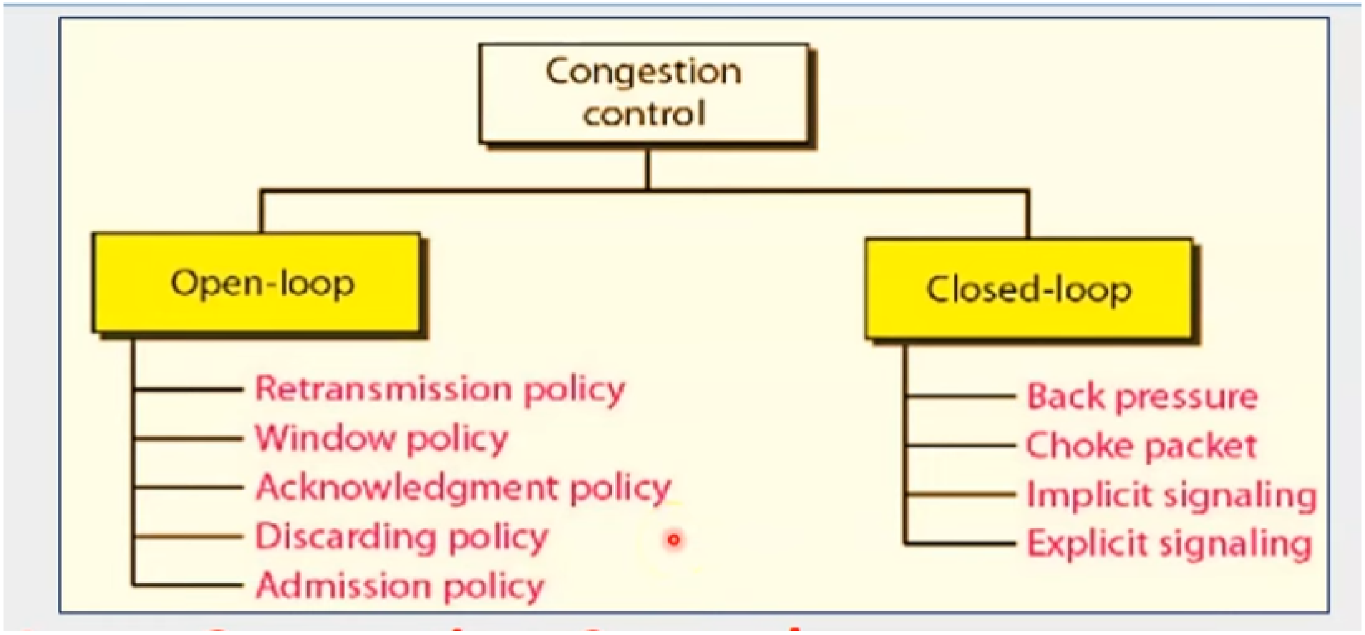


	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

What is open loop and closed loop congestion control.



Congestion control

Open-loop
- Retransmission policy
- Window policy
- Acknowledgment policy
- Discarding policy
- Admission policy

Closed-loop
- Back pressure
- Choke packet
- Implicit signaling
- Explicit signaling

- When there are too many packets in a subnet, performance degrades, This is called congestion
- There are 2 types of mechanisms
  - open-loop congestion control (prevention)
  - closed-loop congestion control (removal)

Open Loop Congestion control

- Policies are applied to prevent congestion before it happens

Retransmission policy

- Retransmission is sometimes unavoidable. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted
- Retransmission in general may increase congestion in the network. However, a good retransmission policy can prevent congestion
- Example retransmission policy used by TCP is designed to prevent or alleviate congestion

Window policy

- The type of window may affect congestion
- Select Repeat window is better than Go back N window
- In the Go-Back-N window, when the timer for a packet times out, several packets may be resent
- The Selective Repeat window, on the other hand, tries to send the specific packets that have been lost or corrupted

Acknowledgement policy

- Acknowledgments are part of the load in a network
- The receiver can choose to accept only N acknowledgements at a time
- Fewer acknowledgements means less load

Discarding policy

- Routers can discard packets to prevent congestion
- Example: In audio transmission, less sensiive packets can be discarded to prevent congestion

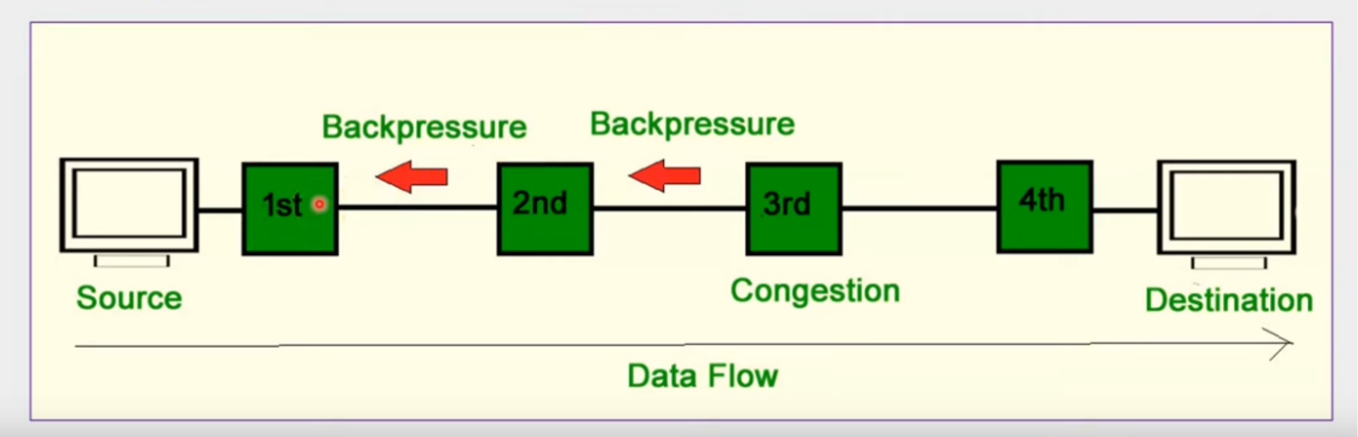
Admission policy

- Admission policy can prevent congestion in Virtual circuit networks
- Switches in a flow check resource requirements of flow before admitting to network
- Router can deny establishing a virtual connection if theres congestion in the network

Closed loop congestion control

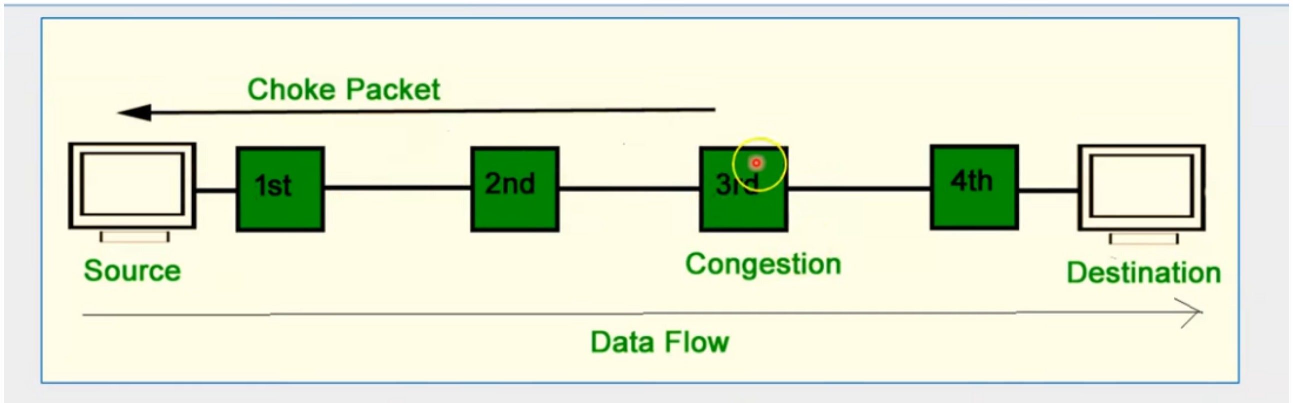
- Uses to allievate congestion after it happens
- There are several mechanisms to do this

Backpressure



- If node 3 has congestion, it informs node 2
    - node 2 slows down, and it causes congestion, it informs node 1
        - node 1, slows down, causes congestion and informs the source
- The source is informed and decides to slow down the transfer to fix the congestion

Choke Packet

- packet sent by a node to the source to inform it about a congestion
- 

- Here node 3 sends message to source about the congestion

Implicit signalling

- No communication between the congested node and the source
- The source senses the congestion by other symptoms
    - Example. when the source sends severals packets, and if there is acknowledgement
        - it assumes the network is congested
    - The delay in acknowledgment is interpreted as congestion

Explicit Signalling

- Node that experiences congestion, explicitly sends the signal to source or destination
- Unlike choke packet where a seperate packet is sent, here the signal is included in the packets that carry the data
- There are 2 types of signalling
    - Forward signalling
        - Bit can be set in the packet moving in the direction of congestion
            - It uses policies like slowing down acknowledgments to fix the congestion
    - Backward signalling
        - Bit can be set in the packet moving against the direction of congestion
            - It can warn the source about the congestion

What is meant by term QOS? What are the different flow characteristics.?

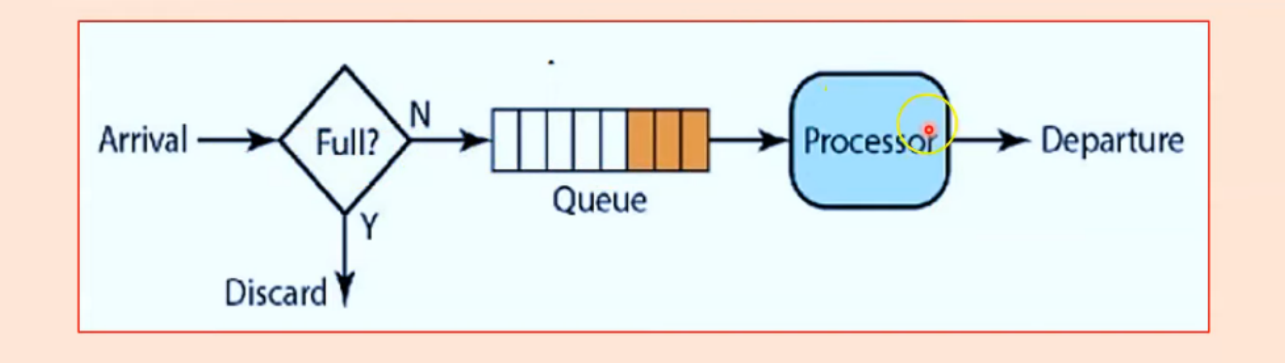
- Stream of packets from source to destination is called a flow
- The needs of each flow can be characterized by following parameters
    - Reliability
        - Lack of reliability means losing a packet or acknowledgment
    - Delay
        - Source to destination delay
    - Jitter
        - Variation of delay for packets belonging to same flow
    - Bandwidth
        - Different applications require different bandwidths
- These determine the Quality of Service the flow requires

Discuss the common techniques used in computer networks to improve the QoS.

Techniques for acheiving good Qos

1. Scheduling

FIFO Queueing

- Packets wait in a buffer until the node is ready to process them
- 

Priority Queuing

- Packets assigned to priority class
- Each priority class has a queue
- Highest priority processed first
- Lowest priority processed last
- Advantage
  - High priority like multimedia can be processed fast
- Disadvantage
  - If theres continous flow in high priority queue, then low priority wont be processed
  - This causes a condition called starvation

Weighted Fair queuing

- Packets are assigned to class and queues
- Queues are weighed based on priority of queues
- Number of packets selected from each queue depends on their weight

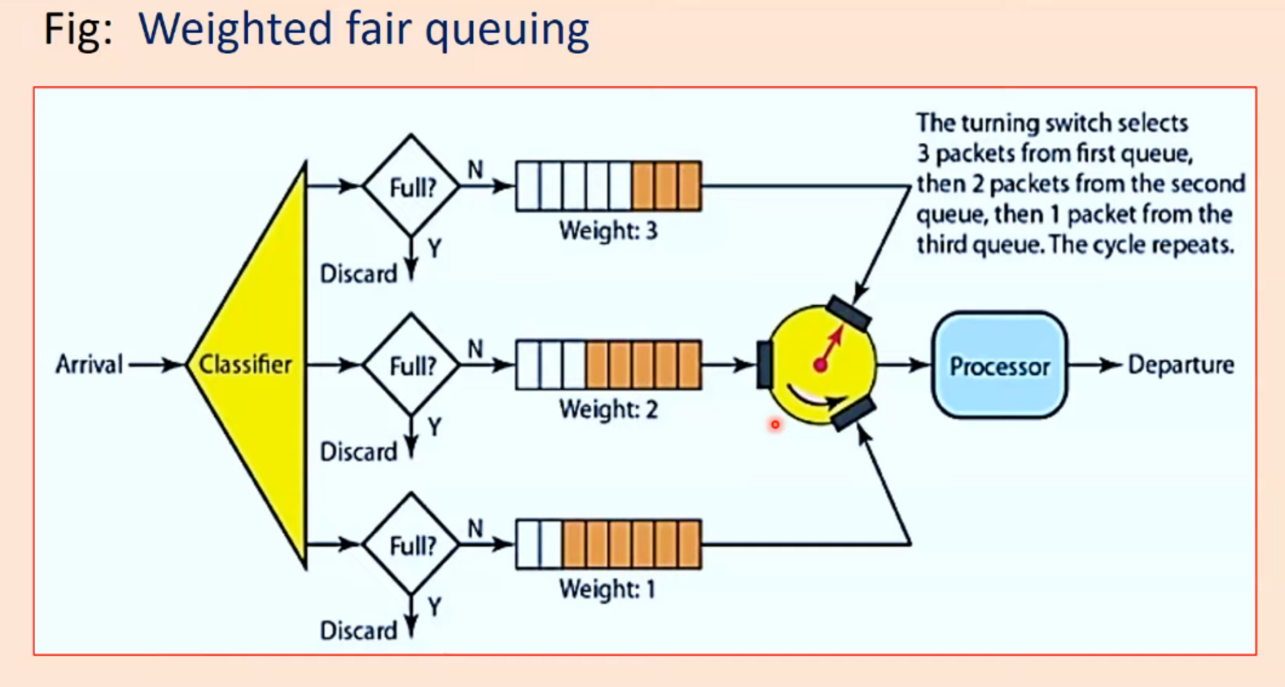
- 

Fig: Weighted fair queuing

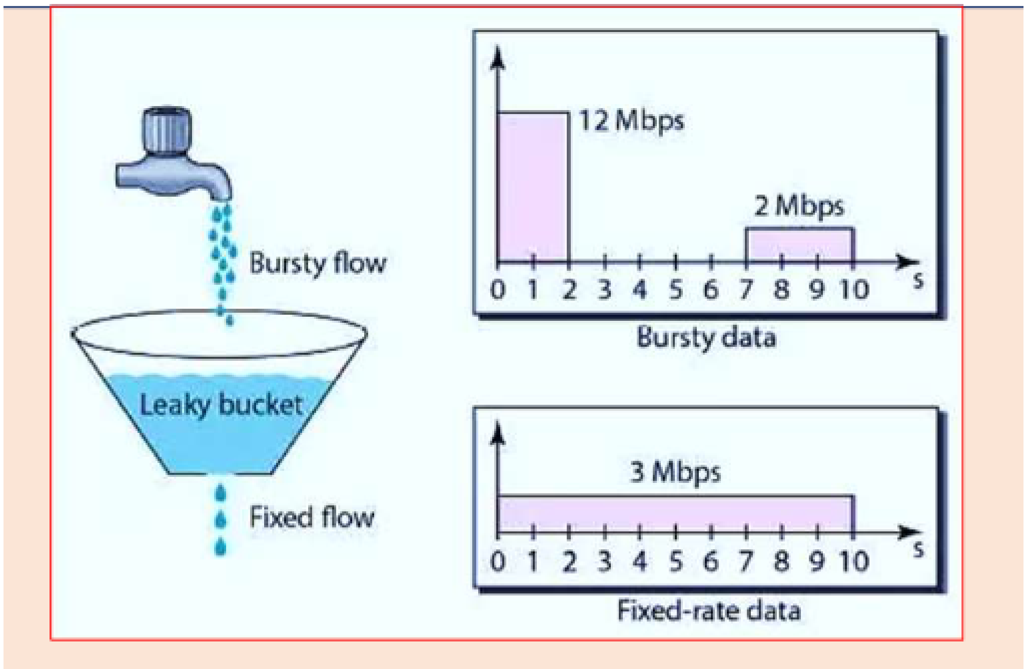
The turning switch selects 3 packets from first queue, then 2 packets from the second queue, then 1 packet from the third queue. The cycle repeats.

2. Traffic shaping

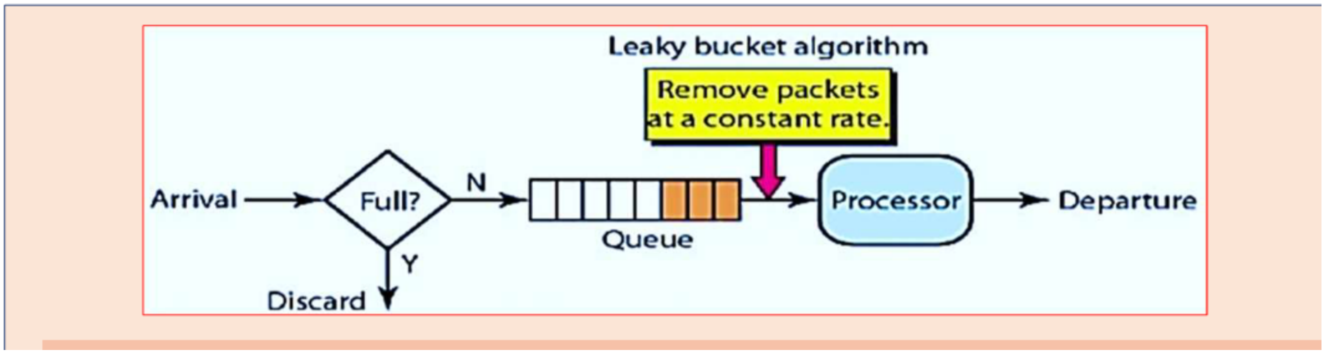
- Mechanism to control the amount and the rate of the traffic sent to the network
- The 2 techniques to shape traffic are

Leaky Bucket

- If a bucket has a small hole at the bottom, the water leaks from the bucket at a constant rate as long as there is water in the bucket.
- The rate at which the water leaks does not depend on the rate at which the water is input to the bucket unless the bucket is empty
- The input rate can vary, but the output rate remains constant

- 

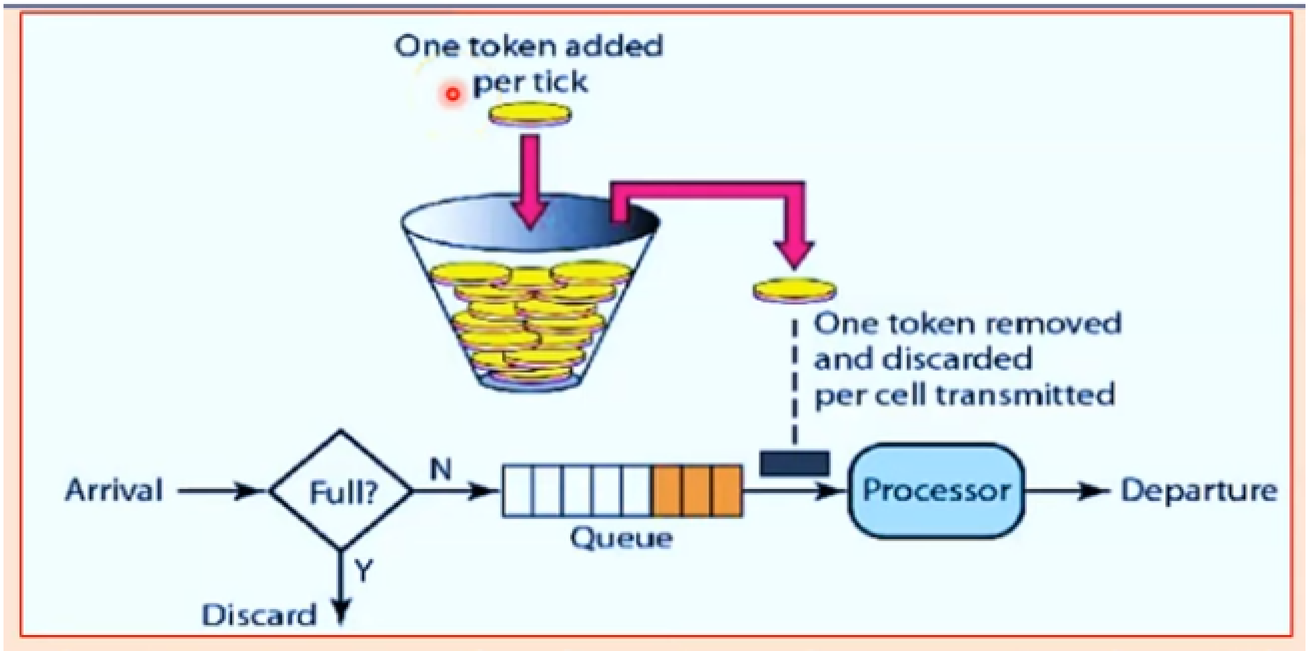
- Here, for 2 seconds, data is sent at 12 Mbps
  - Total Mb sent is 12 x 2 = 24 Mb
- After waiting for 5 seconds
  - 2 Mbps for 3 seconds
    - 2 x 3 = 6 Mb
- Total we have 30 Mb
- This same thing we can distribute at 3Mbps across 10 seconds
  - So each second 3 Mb is sent
    - for 10 seconds its 10x3 = 30 Mb



- A FIFO queue holds the packets. If the traffic consists of fixed-size packets, the process removes a fixed number of packets from the queue at each tick of the clock.
- If the traffic consists of variable-length packets, the fixed output rate must be based on the number of bytes or bits.

> A leaky bucket algorithm shapes bursty traffic into fixed-rate traffic by averaging the data rate. It may drop the packets if the bucket is full.

Token Bucket



- A token is added to the bucket per every tick
- Each time a unit of data is sent a token will be removed

Resource reservation

- Resources such as
  - Buffer
  - Bandwidth
  - CPU time
- If these resources are reserved beforehand the quality of service can be improved

Admission control

- Refers to mechanism used by router to accept or reject a flow based on predefined parameters called flow specification