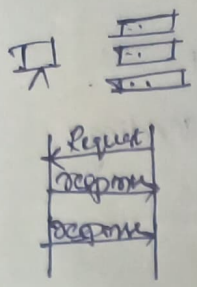
TCP - Transmission Control protocol



(1) TCP is connection-oriented protocol.

(2) TCP is reliable as it guarantees the delivery of data to destination router

(3) TCP provides extensive error checking mechanism - Provides flow control

(4) An acknowledgement segment is present

(5) TCP is comparatively slower than UDP.

(6) Retransmission of lost packets is possible in TCP.

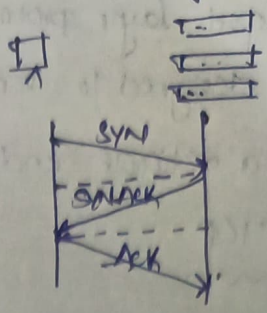
(7) TCP has (20-60) bytes variable length header.

(8) TCP is used by HTTP, HTTPS, FTP, SMTP...

(9) It does not support Broadcasting.

(10) TCP Connection is Byte-stream

UDP - User Datagram Protocol.



(1) UDP is connectionless-oriented protocol.

(2) The delivery of data to destination router cannot be guaranteed in UDP.

(3) UDP provides basic error checking mechanism using checksum.

(4) No acknowledgement segment is present.

(5) UDP is faster, simpler and more efficient than TCP.

(6) Retransmission of lost packets is not possible in UDP.

(7) UDP has 8 bytes of fixed length header.

(8) UDP is used by DNS, DHCP, TFTP, SNMP, RIP...

(9) UDP supports Broadcasting.

(10) UDP connection is message-stream.

Transmission Control protocol:

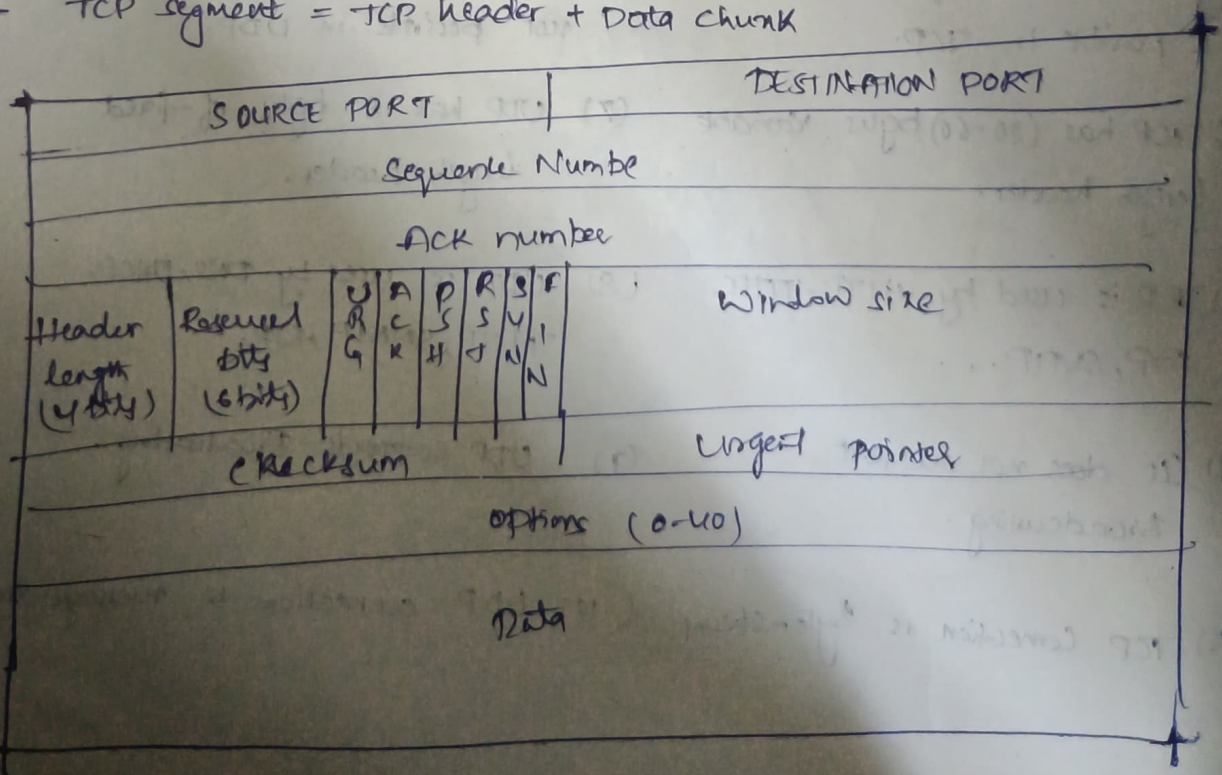
- It is a transport layer protocol.
- It has been designed to send data packets over internet.
- It establishes a reliable end to end connection before sending.

Charectesistics of TCP

- It guarantees the delivery of data packets to its correct destination.
- After receiving the data packet, receiver sends an acknowledgement to the sender.
- ~~TCP employs re~~
- It tells the sender whether data packet has reached its destination safely or not.
- TCP employs retransmission to compensate for packet loss.

Need of TCP

- It divides the data into chunks where each chunk is a collection of bytes.
- creates TCP segments by adding a TCP header to the data chunks.
- TCP segments are encapsulated in IP datagram.
- TCP segment = TCP header + Data chunk



User Datagram protocol.

- It is a transport layer protocol.
- It has been designed to send data packets over the internet.
- It takes the datagram from n/w layer, attaches its header and send it to the user.
- UDP is short for user Datagram protocol.

Characteristics of UDP

- UDP is connectionless protocol.
- It is a stateless protocol.
- It is a unreliable protocol.
- The delivery of data to destination cannot be guaranteed.
- Does not provide congestion control mechanism.
- It is a fast protocol.

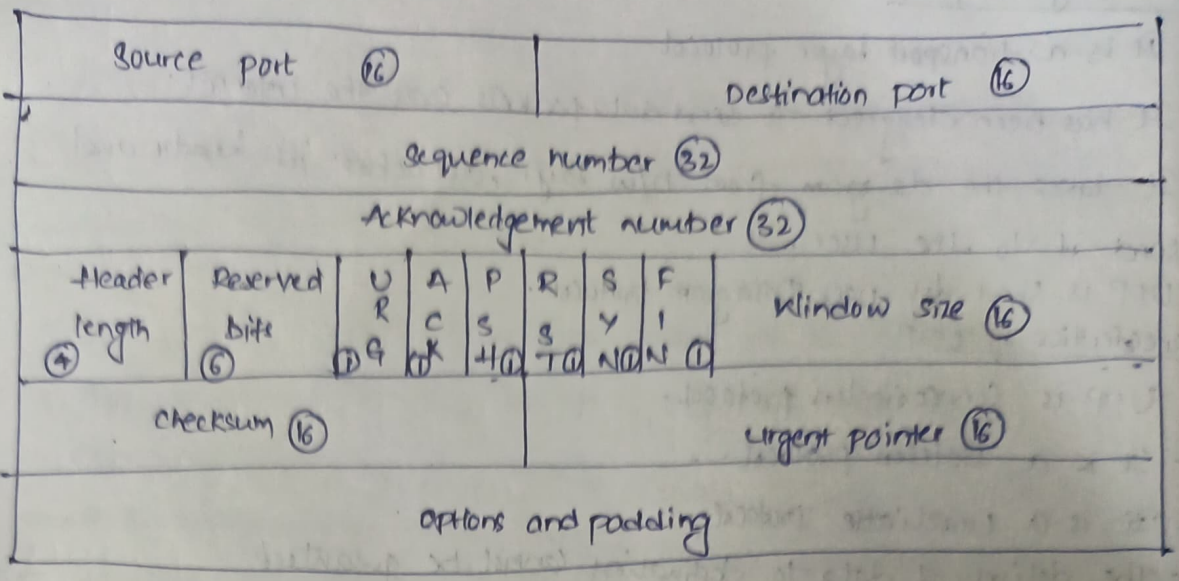
Need of UDP

- Used for time-critical data transmissions.
- It produces a minimal number of overheads.

As we know that UDP is an unreliable protocol, but we still require it in some cases. The UDP is deployed where the packets require a large amount of bandwidth along with actual data. For example, in video streaming, acknowledging thousands of packets is troublesome and wastes a lot of bandwidth. In the case of video streaming, the loss of some packets couldn't create a problem, as it can also be ignored.

Source port (2 bytes) 2x8 = 16	Destination port (2 bytes) 2x8 = 16 bits
Length (2 bytes) 2x8 = 16 bits	checksum (2 bytes) 2x8 = 16 bits

TCP Header.



Source port

- It is a 16 bit field.
- Identifies the port of the sending application.

Destination port

- It is a 16 bit field.
- Identifies the port of the receiving application.

Sequence Number

- It is a 32 bit field.
- TCP assigns a unique sequence number to each byte of data contained in TCP segment.

Acknowledgement Number.

- It is a 32 bit field.
- It contains sequence number of data byte that receiver expects to receive next from the sender side.
- Sequence number of last received data byte is incremented by 1.

Header length

- It is a 4-bit field.
- It contains the length of TCP header

Header length = Header length field value × 4 bytes

Reserved Bits

- 6 bits are reserved
- these bits are not used.

URG - Urgent pointer

- URG bit is used to treat certain data on urgent basis.
- When URG bit is set to 1, the urgent data has to be prioritized.
- if it is set to 0, it is less prioritized.

ACK - Acknowledgement

- ACK bit indicates whether acknowledgement number field is valid or not.
- if ACK bit is set to 1, Acknowledgement number contained in TCP header is valid.
- if ACK bit is 0, simply it is said to be "Not-Valid".

PSH - Request for push

- PSH bit is used to push the entire buffer immediately to receiving application.
- if it is set to 1, message would be inserted in the queue.
- if it is 0, message would not be inserted. (pop-from Que)

RST - Reset the connection

- RST bit is used to reset the TCP connection.
- if it is set to 1, connection should be immediately reset.
- if it is 0, connection is normal and that data can be sent and received.

SYN - Synchronization

- It is used to synchronize the sequence numbers.
- if it is set to 1, message will be sent in sequence.
- if it is 0, message would be sent in random.

FN - Terminate the connection

- if it is set to 1, Sender wants to terminate the connection.
- if it is set to 0, To make the connection.

Window size

- It is 16 bit field.
- It contains the size of receiving window of the sender.
- Window size is used for flow control.

Checksum

- It is 16 bit field.
- It is used for error control.

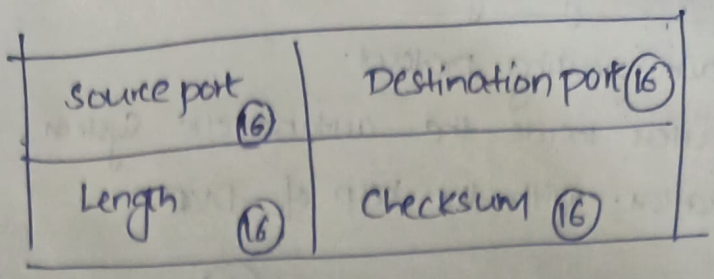
Urgent pointer

- It is 16 bit field
- It indicates how much data in the current segment is counting from first data byte.

Options

- The size is vary from 0 byte to 40 bytes
- It is used for following purposes;
  (1) Time stamp.
  (2) Window size extension
  (3) parameter negotiation
  (4) padding.

UDP Header



Source port

- 16 bit field
- Identifies the port of sending application.

Destination port

- 16 bit field.
- Identifies the port of receiving application.

Length

- 16 bit field.
- Combined length of UDP header and Encapsulated data

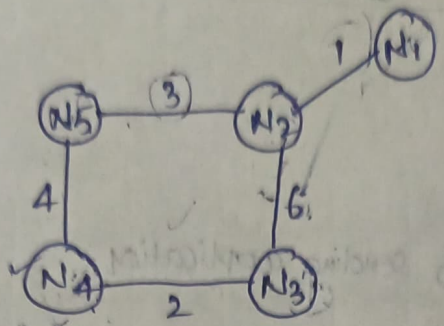
Length = Length of UDP Header + Length of Encapsulated data

Checksum

- 16 bit field used for error control.
- It is calculated on UDP header, encapsulated data and IP pseudo header.
- Checksum calculation is not mandatory in UDP.

Distance Vector Routing Algorithm.

- Intra Domain routing protocol.
- All the routers inside the autonomous system, How they will share information with the help of DVR.



Step-①:

(N1)

Destination	Distance	Next Hop
N1	0	N1
N2	1	N2
N3	∞	-
N4	∞	-
N5	∞	-

(N2)

Destination	Distance	Next Hop
N1	1	N1
N2	0	N2
N3	6	N3
N4	∞	-
N5	3	N5

(N3)

Dest	Dist	Next
N1	∞	-
N2	6	N2
N3	0	N3
N4	2	N4
N5	∞	-

(N4)

Dest	Dist	Next
N1	∞	-
N2	∞	-
N3	2	N3
N4	0	N4
N5	4	N5

(N5)

Dest	Dist	Next
N1	∞	-
N2	3	N2
N3	∞	-
N4	4	N4
N5	0	N5

Step-②:

- only Neighbours and its Distance vector would be shared.

(N1)

Dest	Dist	Next
N1	0	N1
N2	1	N2
N3	7	N3
N4	∞	-
N5	4	N5

N2
1
0
6
∞
3

(N2)

Dest	Dist	Next
N1	1	N1
N2	0	N2
N3	6	N3
N4	7	N4
N5	3	N5

N5	N3	N1
∞	∞	0
3	6	1
∞	0	7
4	2	∞
0	∞	4

$N_2 \xrightarrow{6} N_3 + N_3 \xrightarrow{2} N_4 = 8$

$N_2 \to N_5 + N_5 \to N_4 = 7$

4 3

Dest	Dist	Next
N_1	7	N_1
N_2	6	N_2
N_3	0	N_3
N_4	2	N_4
N_5	6	N_5

(N3)

N_4	N_2
∞	1
∞	0
2	6
0	∞
4	3

Desti	Dist	Next
N_1	∞	N_1
N_2	7	N_2
N_3	2	N_3
N_4	0	N_4
N_5	4	N_5

(N4)

N_5	N_3
∞	∞
3	6
∞	0
4	2
0	∞

$N_4 \to N_5 + N_5 \to N_1 \quad 4 + \infty = \infty$

$N_4 \to N_3 + N_3 \to N_1 \quad 2 + \infty = \infty$

Dest	Dist	Next
N_1	4	N_1
N_2	3	N_2
N_3	6	N_3
N_4	4	N_4
N_5	0	-

(N5)

N_4	N_2
∞	1
∞	0
2	6
0	∞
4	3

$N_5 \to N_4 + N_4 \to N_1$

$N_5 \to N_2 + N_2 \to N_1 = 3 + 1 = 4$

$N_5 \to N_4 + N_4 \to N_3 = 6$

$N_3 \to N_2 + N_2 \to N_3 = 9$

step (3):

Dest	Dist	Next
N_1	0	-
N_2	1	N_2
N_3	7	N_3
N_4	8	N_4
N_5	4	N_5

(N1)

N_2
0
6
7
3

$N_1 \to N_2 + N_2 \to N_3$

$1 + 6 = 7$

$N_1 \to N_2 + N_2 \to N_4$

$1 + 7 = 8$

$N_1 \to N_2 + N_2 \to N_5$

Dest	Dist	Next
N_1	8	N_1
N_2	7	N_2
N_3	2	N_3
N_4	0	N_4
N_5	4	N_5

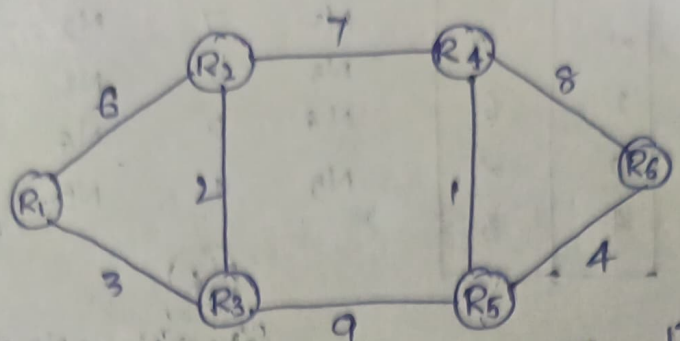
(N4)

N_5	N_3
4	7
3	6
6	0
4	2
0	6

$N_4 \to N_5 + N_5 \to N_1 = 8$ (4 + 4)

$N_4 \to N_3 + N_3 \to N_1 = 9$ (2 + 7)

Link State Routing



S-1

R1	
R2	6
R3	3

R2	
R4	7
R3	2
R1	6

R3	
R2	2
R5	9
R1	3

R4	
R5	1
R6	8
R2	7

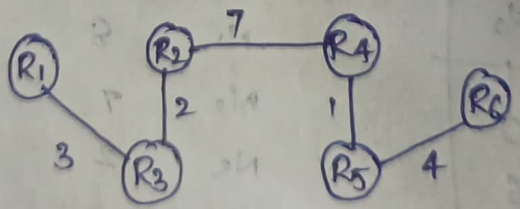
R5	
R3	9
R4	1
R6	4

R6	
R5	4
R4	8

S-2

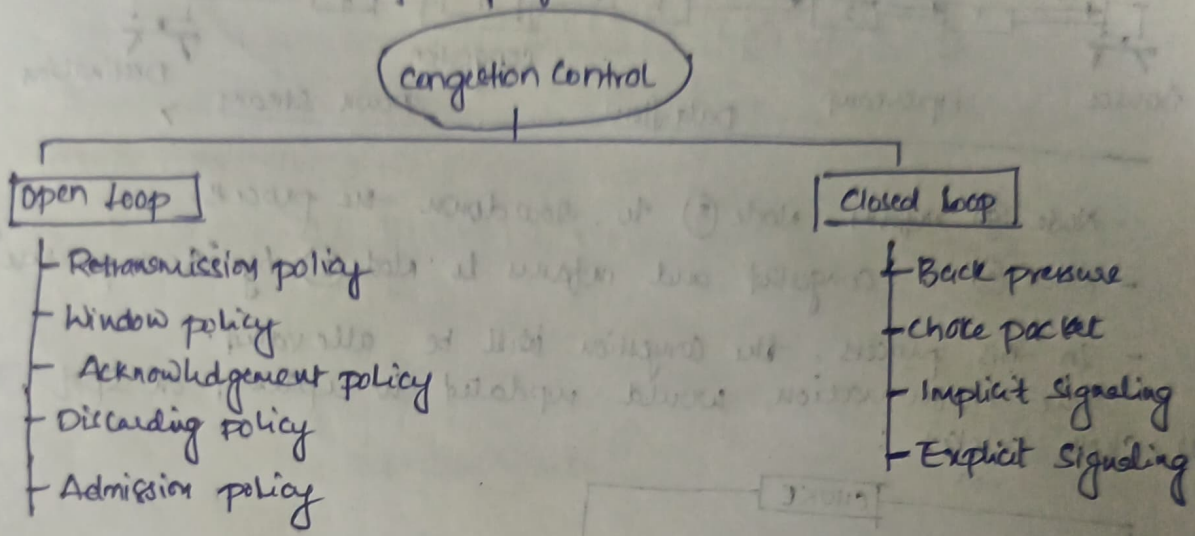
R1	R2	R3	R4	R5	R6
R1	6	(3)	∞	∞	∞
R1, R3	(5)	-	∞	12	∞
R1, R3, R2	-	-	(12)	12	∞
R1, R3, R2, R4	-	-	-	(12)	21
R1, R3, R2, R4, R5	-	-	-	-	(16)

$R_1 \rightarrow R_3 \rightarrow R_2 \rightarrow R_4 \rightarrow R_5 \rightarrow R_6$



Congestion Control

- Congestion in a network ~~layer~~ may occur, if the load on the network is greater than capacity of network.
- Congestion refers to mechanism and techniques which keeps the load below the capacity of that network.



Open loop: protocols to avoid congestion.

(1) Retransmission policy: The sender can retransmit the packet to the source, if packet has been lost or corrupted.

(2) Window policy: By implementing, -Go-Back N ARQ we can -Selective Repeat ARQ prevent congestion.

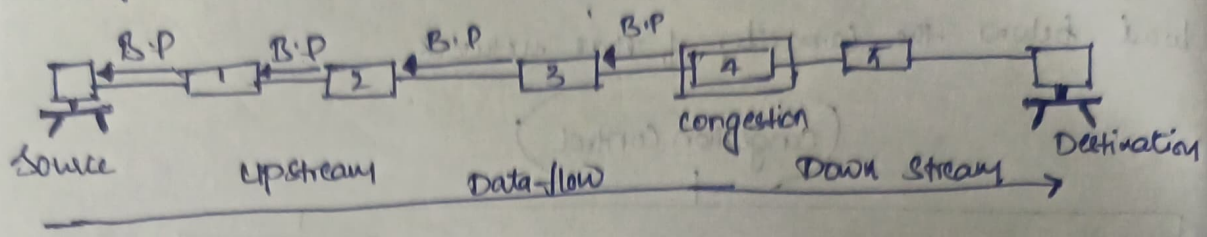
(3) Acknowledgement policy: Receiver sends an acknowledgement to the sender.
- After receiving the packet, it tells the sender whether packet has reached to the destination safely or not.

(4) Discarding policy: The packet will discard, if it has low priority and the packet which is NOT meant to destination.

(5) Admission policy: A router can deny establishing a virtual circuit connection if there is a congestion.
- if there are insufficient resources to handle transmission, they do not accept any more packets from sender.

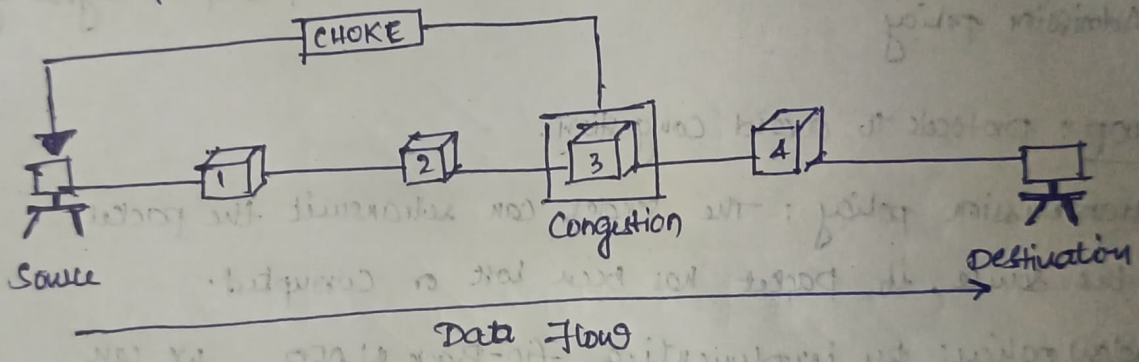
Closed loop: Try to remove Congestion.

(1) Back pressure: Back pressure method for alleviating Congestion.



- Node ④ inform Node ③ to slow down the process.
- Node ③ is congested and informs to Node ② by "Back pressure"
- In this process, the Congestion will be alleviated.
- The information would updated to upstream on spot.

(2) Choke packet:



- When Congestion occurs, the choke packet will directly sent to the source without interrupting the intermediary nodes.
- Here, the Congestion does not update information to upstream as we did in Back pressure.

(3) Implicit Signaling:

- There is no communication between Congested node and source.
- Source guesses there is a Congestion in network when it does not receive any acknowledgement from sender.

(4) Explicit Signaling:

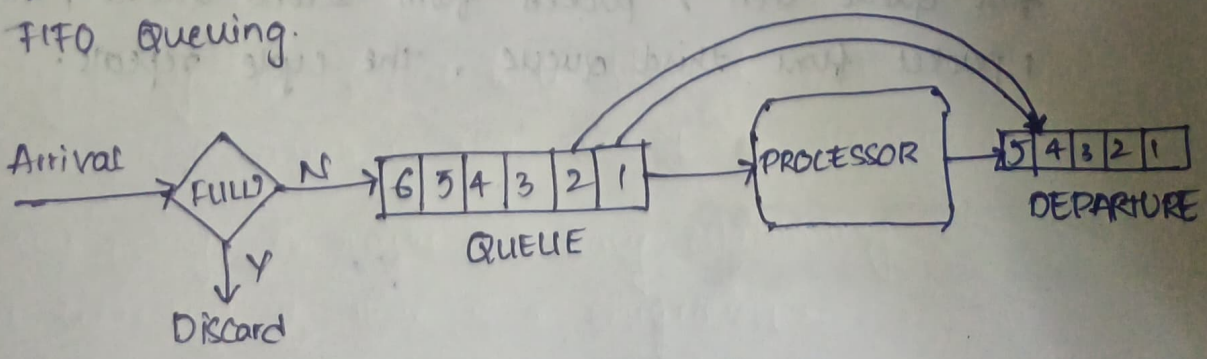
- The Congestion node explicitly send a signal to source or destination to inform about congestion.
- But it is different from choke packet.
- (Network alerts sender or destination to slow down the rate of transmission by sending signal that is included in packet that carry data. That's why it is different from choke packet.)

* Backward Signaling: Warning the source, to slowdown the packets.

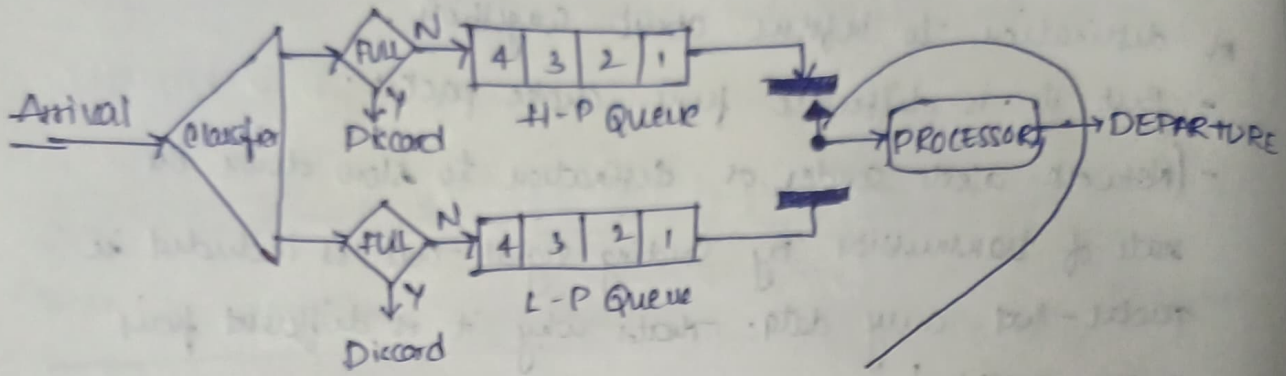
* Forward Signaling: Warning the Destination, to slowdown the acknowledgement

Quality of Service (QoS)

- Quality of service, let a network with less capacity meet application requirements just as well at a lower cost.
- characteristics of QoS.
  - Reliability (follow all policies)
  - Delay (got delayed from packet that should be departed)
  - Jitter (variation in delay)
  - Bandwidth (Equal amount of time)
- Techniques to improve QoS.
  - FIFO Queuing.

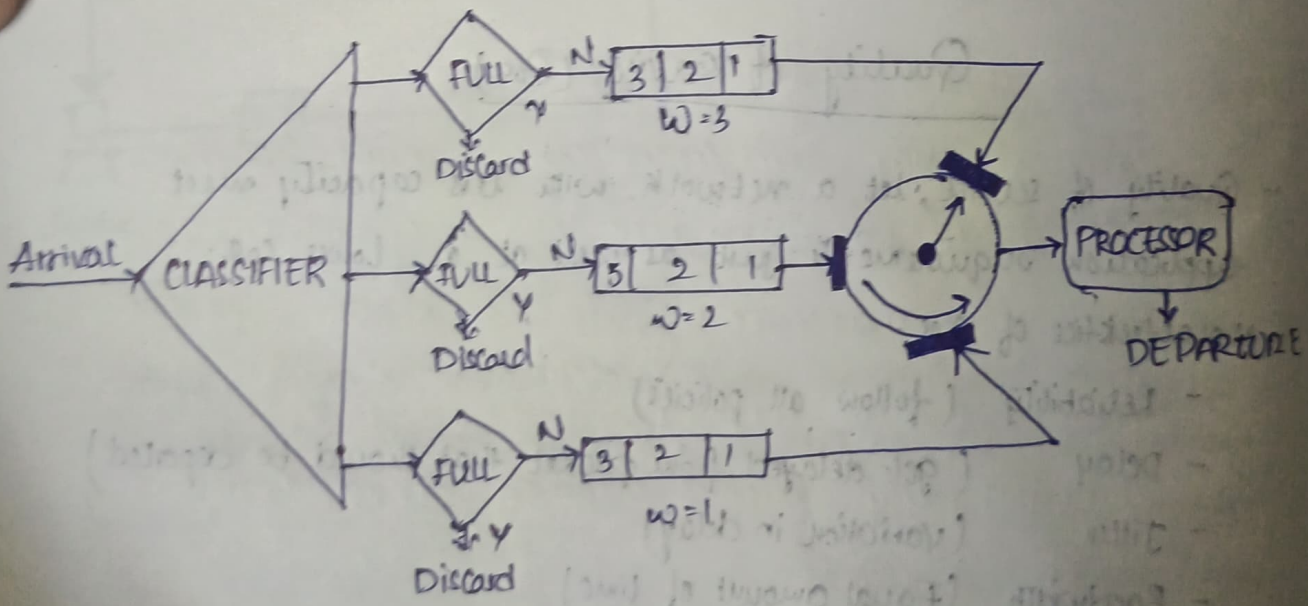


- Priority Queuing.



The switch turns to the other queue when the current one is empty.

- Weighted fair Queuing.

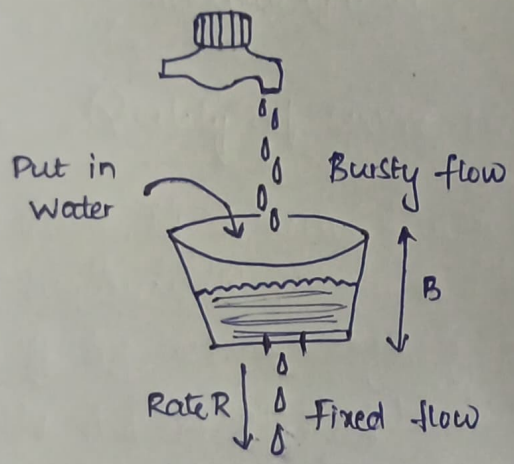


- The ~~switch~~ turning switch selects 3 packets from first queue then 2 packets from second queue, then 1 packet from third queue. the cycle repeats.

- Techniques to improve QoS
  - ① Traffic Shapping.
    - Leaky Bucket
    - Token Bucket

- Traffic Shapping: The technique for controlling the average rate and burstiness of a flow of data that enters the network.

* Leaky Bucket * 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.
  - Can't control the arrival of messages.



* Token Bucket *
  - Token bucket allows bursty traffic at a regulated maximum rate.