Unit - 2

1) TCP:

* TCP is also known as transmission control protocol
* TCP connection is byte stream.
* TCP does not supports multicast and broadcasting
* TCP provides error control and flow control
* TCP does not supports half duplex
* TCP supports full duplex
* TCP is highly reliable.
* TCP packet is called Segment

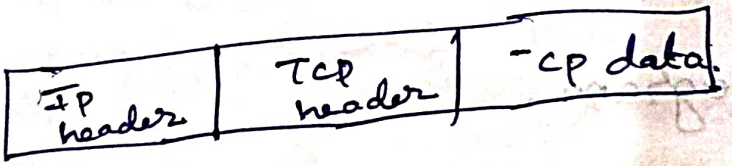
* TCP header contains Six flag bits they are URG, ACK, PSH, RST, SYN, FIN

* A stream of 8-bit bytes are used for the connection between two applications.

* TCP and UDP uses a same network layer

* TCP maintains a Checksum on header and data.

TCP Segment format:



TCP connection Establishment:

CLOSED - No active

LISTEN - Server is waiting for incoming call

SYN RCVD - A connection Request has received

SYN SENT - A connection Request has sent

2) UDP:

* UDP is Connectionless
* UDP connection is Message Stream
* UDP supports broadcasting
* It does not provide flow control and error control
* UDP does not supports full duplex transmission
* UDP is Unreliable
* UDP packet is called user datagram.
* UDP is also known as User Datagram protocol.
* TCP is used to built a UDP.

3) Congestion control:

Congestion:

* When too many packets rushing to a node or a part of network, the network performance may degrades and this situation is called congestion.

* The primary goal of congestion control is to ensure the network operates efficiently

Congestion control:

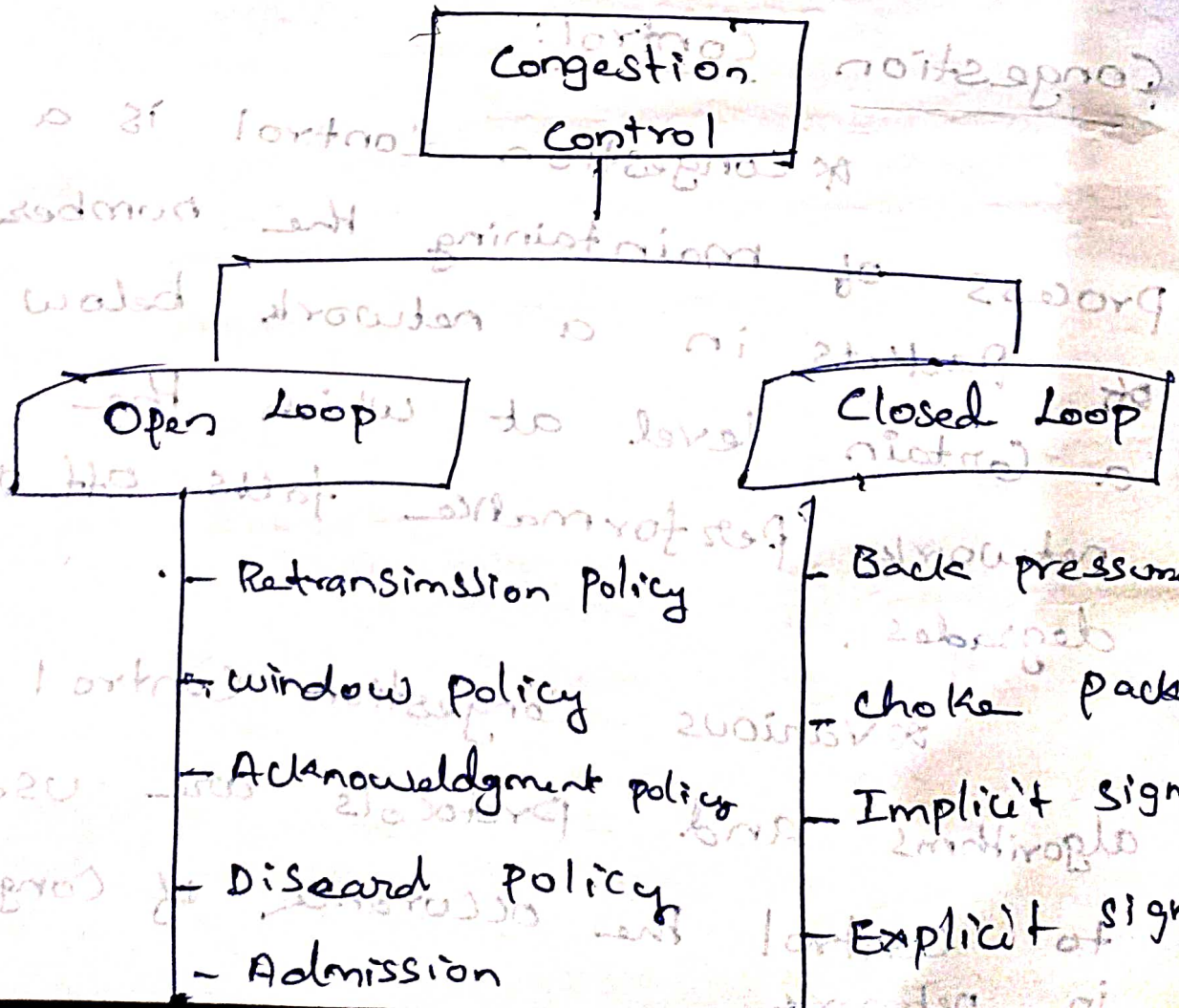
* congestion control is a process of maintaining the number of packets in a network below a certain level at which the network performance falls off or degrades.

* various Congestion Control algorithms and protocols are used to control the occurance of congest

* Congestion occurs due high User traffic in network.

* Congestion control refers to techniques and mechanisms that can either prevent congestion before it happens, or after it has happened.

* Congestion control can also remove the congestion.



* In general open loop used for prevention congestion and closed Loop is used for removal

Open Loop congestion control :

* It is applied to prevent congestion before it happens.

* In this mechanism congestion can be handled either in source or destination.

i) Retransimission Policy:

* Retransmission policy is unavoidable.

* If a Sender feels that a Send packet is lost or corrupted. the packet needs to be retransmitted. This process is called retransimission policy.

* In general retransimission increase congestion in the network

Window Policy:

* The window policy at Sender may also affect congestion.
* windows policy selectively rejects the packet using windows method for congestion control.

Acknowledgement policy:

* Acknowledgement policy was imposed by receiver. It may also affects a congestion.
* If the receiver does not acknowledge on every packet. it may slow down the Sender.

Discarding policy:

* Congestion can be controlled by the routers and at the same time may not harm the integrity of the transmission.

5) Admission policy:

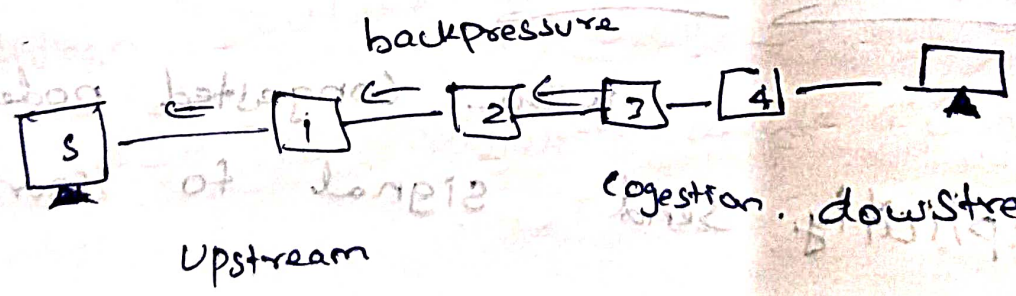
- mechanism, the congestion can be prevented.

Closed Loop Congestion control:

Closed loop congestion control is applied after the congestion happened.

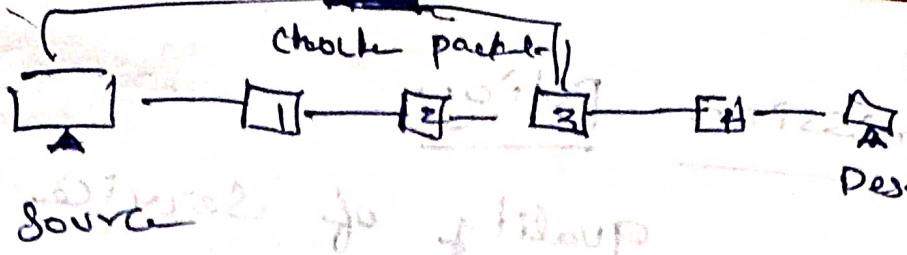
Backpressure

*It is a node to node congestion control



Choke packet:

*A choke packet is a packet sent by a node to source to inform it congestion happened.



Implicit signaling:

* In Implicit signalling there is no communication between nodes.
* the ~~Congested~~ Source node guesses that there is congestion and recovery from congestion
* It guesses, the Congestio Symptoms from Network

Explicit signalling:

* the Congested node explicitly send signal to source or destination
* It is of two types. Backward signalling and forward signalling.

Congestion Avoidance:

Congestion avoidance is a prevention mechanism while congestion control is a recovery mechanism.

DEC bit:

* DEC bit means destination experiency congestion bit
* DEC bit was developed by DNA (Digital Network Architecture).
* DEC bit split the responsibilty between routers and end hosts
* It is router based congestion control.
* According to the packet arrival queue length is calculated
* Queue length can be calculated by (last bust + idle) period + current busy period.

* Source Machine adjust the packet flow rate.

* Source Machine maintains a Congestion window.

RED.

* RED Stands for Random Early Detection.

* The main of RED is to provide Congestion Control at the router.

* RED is based of DEC Bit.

* RED is designed to work well with TCP.

* RED Notifies Sender by dropping packets.

* packets are dropped, when the average queue length increases.