UNIT 3 CONGESTION CONTROL ALGORITHMS

3.0 INTRODUCTION

In the Internet nodes acting as transmitting nodes are inserting packets into the Internet and nodes acting as receiving nodes consume the packets from the Internet. Internet has a capacity to handle the traffic load (packets). When the rate of insertion of packets into the Internet is higher than the rate of consumption of the packets from the Internet at last Internet is unable to handle the traffic and the performance of the resources of the Internet is degraded. This situation is termed as congestion.

Hence, the goal of congestion control algorithms is to refrain the transmitter from inserting packets in the network more than the handling capacity of the Internet.

In this unit section 3.3 discusses about the reasons for congestion in the network. Section 3.4 differentiates congestion control from flow control. Congestion prevention mechanisms are covered in section 3.5. In section 3.6 general principles of congestion control are elaborated. Further in section 3.7 congestion control technique namely: Open loop control is discussed. Section 3.8 is about the congestion control in packet-switched networks. Section 3.9 summarizes the unit. Problems and their solutions covering the entire unit are discussed in the section 3.10. Section 3.11 enlists further readings.

3.1 OBJECTIVES

After completing this unit, one should be able to:

- Identify the reasons of the congestion in the Internet;
- Differentiate congestion control and the flow control;
- Devise the preventive measures of the congestion;
- understand the congestion control techniques;

- understand the close loop and open loop congestion control techniques, and
- understand congestion control in packet-switched networks.

3.2 REASONS FOR CONGESTION IN THE NETWORK

In the Internet there can be several reasons to occur the congestion. When many transmitters insert data packets on to input lines at a time and are to be sent on the same output line, assuming that the capacity of the output line is much less than that of the packets received then a long queue will be build up for that output line. In this situation if the buffer memory if not big enough to hold all these packets, then extra packets will be dropped. To stop dropping of the packets, if the memory available is made infinitely large even then the congestion may be reduced but the overall quality of the service of the traffic will be worse; because by the time packets reach to the output line to get dispatched, there TTL (time to live) value gets expired and their duplicate packets been already inserted into the network. If all the packets carried to the final destination, these duplicate packets will increase the traffic load only in the Internet and will be discarded, due to time out. So, it will be good for the Internet to drop these packets as soon as their TTL value gets expired.

Another reason of the congestion in the Internet is the slugging performance of the processors of the intermediate devices. If any of the intermediate router's CPU is performing slower than expected speed, their jobs (i.e. Queuing buffers, routing packets, updating tables, reporting any exceptions etc.), will be slowed down. The arrival rate of the packets at input line is greater than the processing and removal of the packet from output line. This again creates a situation of congestion.

Another point of issue is the Low Bandwidth. Due to low bandwidth capacity of the lines amount of the traffic increases in the network causing congestion.

Resolution of any one of the issues discussed above will not handle the congestion; instead it will just shift the bottleneck to some other point. The root cause of the real problem is the mismatch of the capacity (computing or the carrying) of various components of the system. Once congestion happens in the network the routers respond to overloading by simply dropping the packets.

The bursty nature of traffic is one of the major causes of congestion. This could be controlled by restricting the insertion of the traffic at a uniform rate.

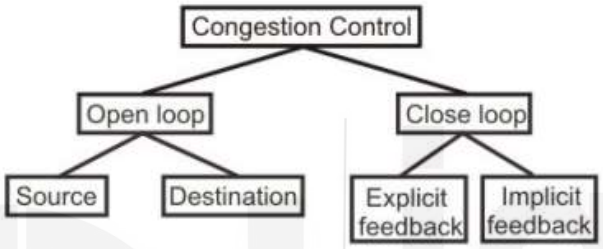
3.3 CONGESTION CONTROL VS. FLOW CONTROL

Congestion control and flow control are two different things, which are mixed up at times. As discussed earlier congestion control is the entity of the network whereas flow control is about regulating the transmission of data between devices on the connection/link between them, and not what is happening in devices between them. Flow control is about point-to-point traffic control between sender and receiver for a specific transmission to avoid packet drop at receiver. If the incoming traffic rate is

higher than the processing rate at receiver, the receiver is flooded and packet will be dropped. To overcome this situation the receiver should send some kind of feedback to sender to inform the sender about the drop of packets and to slow down the sending speed. This is called flow control between sender and receiver and is handled at transport layer responsible for end-to-end data delivery. Congestion is a situation when the traffic in the network is higher than the handling capacity of the network.

3.4 CONGESTION PREVENTION MECHANISM

Congestion control is to restrict the traffic load below the handling capacity of the network. As shown in Figure below, the congestion control techniques can be broadly classified into two categories:



• Open loop: Methods to prevent or avoid congestion are classified as open loop techniques. Open loop methods ensure that congestion state never exists in the network. Open loop policies are applied in the network to prevent congestion before it happens. The congestion control policies are applied either at the source or the destination.

• Close loop: these methods acts to treat or alleviate the congestion once it happens. Once the system enters to congestion state, closed loop techniques used to detect it, and then take action to bring the system out of it.

Open Loop solutions are static in nature. These policies are not adaptive in nature and do not change according to the present state of the system. These methods take decisions about when to accept packets, when to drop them etc. These methods make decision without taking into consideration the present state of the system. The open loop congestion control methods are further classified on the basis of whether these are applied on source or on destination.

Close loop congestion control techniques are based on the concept of feedback. These techniques are dynamic in nature and actions are taken during transmission. Some system parameters are continuously measured in the network and whenever a congestion state is observed, feedback system is used to take action to reduce the congestion. Open loop techniques work as per the following 3 steps:

Step 1: Continuous monitoring of the network to detect the congestion state, the actual location of the congestion and devices involved.

Step 2: Sending the feed back about congestion state to the devices where actions can be taken

Step 3: Take the necessary actions to remove the located congestion.

Some of congestion control algorithms based on these techniques are discussed in following sections.

3.5 GENERAL PRINCIPLES OF CONGESTION CONTROL

Congestion in the network can be measured in terms of various Metrics like: the average queue length, timed-out packets, delay, packets dropped due to unavailability of buffer space, etc.

As discussed previously, congestion occurs in the network when senders insert packets more than the handling capacity of the network. The responsible entities for the congestion in the network are: the sender: sending packets without considering the status of the network, the intermediate resources: speed of the router, bandwidth of the bottleneck link, control messages generated by intermediate device etc. The congestion in the network can be controlled by either dropping the excess packets or to restrict the sender by inserting packets into the network at a lower speed. In general TCP provides mechanism to control the congestion. Internet protocol header also provides ECN field to notify the sender about the congestion in the network. The congestion happens in the network and happened due to sender, hence the network entities are required to notify the sender about the congestion and accordingly the sender takes necessary steps to control it.

3.6 OPEN LOOP CONTROL

As discussed in previous section, open loop methods are preventive measure for congestion control.

Some of the open loop method based policies of congestion control are discussed here:–

Retransmission Policy :

A packet transmitted with reliable data delivery protocol, if it's TTL value expired before it reaches to destination, gets dropped. The sender has to retransmit such packets until get delivered successfully. More the congestion in the network leads to more packet drops which leads to retransmission of these packets leading to more traffic in the network. This retransmission leads to congestion in the system.

To prevent congestion due to this issue, value of timers used by retransmission policy must be set such that state of congestion in the network is prevented and also able to optimize the efficiency of the network.

Window Policy:

In Go-Back-N window if a packet is lost/received out of order, several packets are resent, although some packets may be received successfully at the receiver side. This

may increase the congestion in the network. Therefore, selective repeat window should be preferred instead of Go-Back-N. In selective repeat window packets dropped are that may have been lost.

Discarding Policy :

Routers has to adapt a good discarding policy such that congestion in the network is prevented at the same time a router must attempt to discard corrupted or packets of unreliable services (i.e. UDP) by maintaining the quality of the messages with reduced number of retransmission of dropped packets.

Packets transmitted with UDP services may be discarded before the packets transmitted with reliable services i.e. TCP. The video streaming over the internet may tolerate some loss of packets while text messages may not tolerate loss of any packet.

Acknowledgment Policy :

Acknowledgment is sent by receiver to notify the sender about receipt of the packet or not. Even though the size of acknowledgement packets is small in comparison to the data packets but still they also offer traffic load in network. In order to reduce the number of acknowledgement packets sent, the receiver should wait for the next incoming packet and if it is in sequence with the previous packet instead of sending the acknowledgement of individual packet a cumulative acknowledgement is sent for both the packets. That is sending a cumulative acknowledgement of packets received in sequence can save the bandwidth of the network.

Admission Policy :

Admission policy is applied in a network to prevent the congestion. Before allowing the traffic to enter into the network, switches first check whether the resources required are available or not. The traffic is only admitted if the available resources are more than the requirement of the traffic. The requested virtual circuit is established if there is no chance of congestion after reserving the resources for this.

The policies discussed above can be used to prevent congestion before it happens in the network.

3.6.1 Admission Control

In this section, how the congestion is handled in a virtual circuit network is discussed. Admission control is a closed-loop technique, in which action is taken once network enters into a congestion state. Admission control policy is the first and very simple rule to prevent the congestion in network. It says that admit the traffic on the condition that it will not be responsible for congestion in the network. If there is congestion in the network, the first attempt to recover the network from congestion state could be to stop new packets to be inserted into the network. The thumb rule to prevent the traffic is “admit traffic only when the network can handle it without congestion”. Admission control policy is feasible and can be applied successfully in the circuit-switched datagram networks. This is not easy to identify the source of congestion hence could not be applied in packet-switched networks.

Some of the admission control systems are as follows:

Admission Control Methods:

The goal of admission control methods is to estimate the expected bandwidth requirement for the incoming traffic and determine whether this traffic can be allocated the needed bandwidth, such that congestion state does not occur. Admission control methods are widely used for real time application sensitive towards delay and jitter. Many admission control methods are available. Some admission control methods are based on mathematical calculations and statistical indicators, and others are based on measuring traffic state.

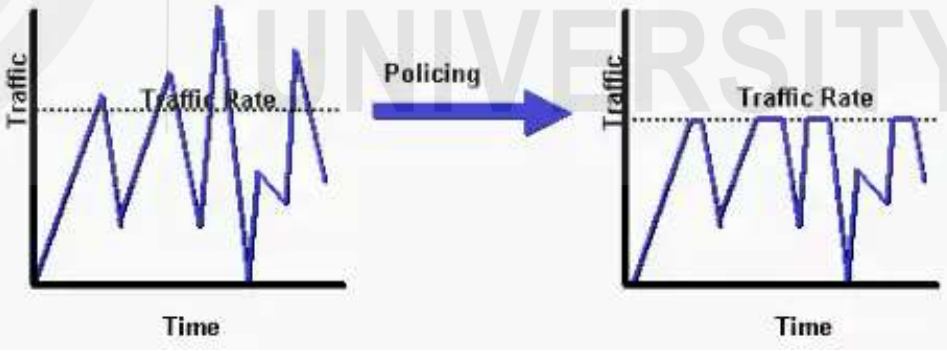
Admission control methods are generally classified into two categories: parameter based and measurement based admission control. Parameter based methods are based on the characteristics of the active traffic and do not consider new incoming traffic, hence are not optimal. Measurement based methods consider the real time network conditions by serving new incoming traffic, hence a higher network utilization may be achieved.

Each admission control method follows the principle that, allocate the available bandwidth to the incoming traffic flows only in case of not exceeding the capacity of the line. For a node to implement admission control policy, it should have access to QoS parameters i.e. delay, packet drop rate etc. By doing so the traffic can achieve the QoS as desired, but should be independent of the type of traffic underwent.

Similarly, in case of virtual circuit subnets, no more new virtual circuits are accepted once congestion state in the network is identified.

3.6.2 Traffic Policing and its Implementation

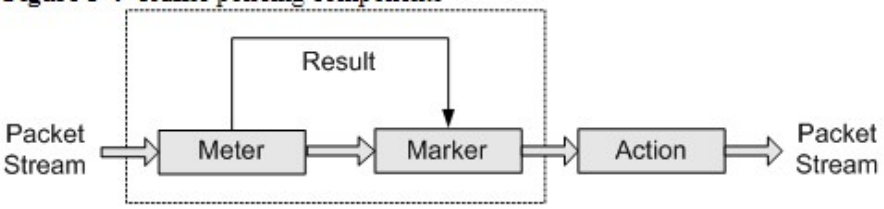
Traffic policing is to monitor the traffic flow in the network. If the traffic flow rate is greater than the specified rate, traffic policing methods simply discards the overflow packets. Traffic policing can be used to control both inbound and outbound traffic. Traffic policing methods maintain a constant flow (pre-defined) of traffic.



Traffic policing does not hold packets received above the allowed flow rate, hence does not require buffer. It is easy to implement traffic policing in comparison to traffic shaping as it does not require maintaining packet buffers. Traffic policing does not cause delay, and queuing, rather it simply discards the packets.

Components of an implementation of traffic policing system are as follows:

Figure 5-4 Traffic policing components

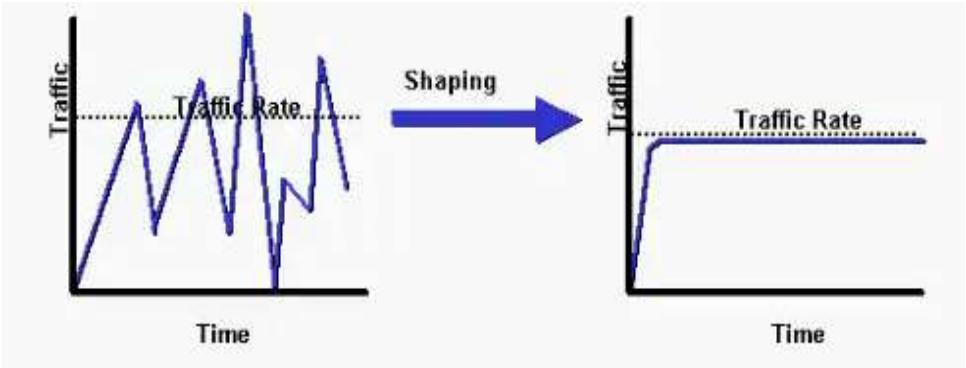


- Meter: this component measures the traffic and provides the measurement result to the next component (marker) for further action.
- Marker: marker assigns colors to packets out of green, yellow, or red based on the measurement result provided by the meter. Marker provides this coloring information to the next component namely: Action.
- Action: this component performs actions based on packet coloring results received from the marker. This component performs following actions in accordance to the pre-defined rules:
  - Pass: a packet will be forwarded further if it meets network requirements.
  - Re-mark + pass: local priority of the packets not meets the network requirements are changed and forwarded.
  - Discard: packets not meeting network requirements are dropped.

If the rate of traffic is below the threshold value, packets are marked with green and yellow color and forwarded, whereas if the rate of traffic exceeds the threshold value, packets are either marked with yellow, lowers the priority and forwarded or marked with red color and dropped according to the traffic policing configuration.

3.6.3 Traffic Shaping and its Implementation

In contrast to traffic policing, traffic shaping tries to adjust the rate of outgoing traffic instead of dropping the packets to ensure an even transmission rate. Traffic shaping makes use of a buffer to hold bursty traffic for a while to control the traffic. Packets are delayed if the system is unable to forward all of them at a time and will be forwarded as the link is found free. It is a congestion control technique which delays some packets to remove the congestion state. Traffic shaping is not practically applicable to traffic of real time applications. Traffic shaping can be used to control the outbound traffic onl



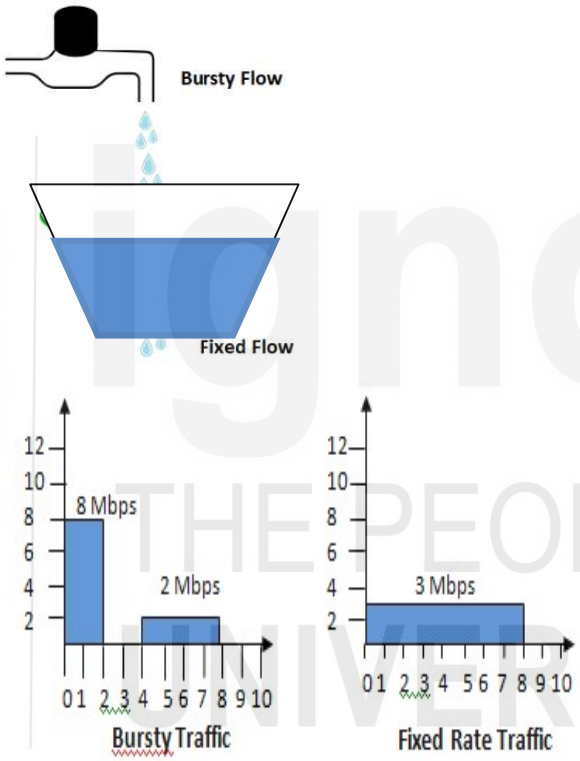
Further, Traffic shapers can be classified into two categories based on their capabilities; simple traffic shaper and advanced or more sophisticated traffic shapers. Simple traffic shapers shape all traffic uniformly. Whereas advanced traffic shaper

can classify the traffic and can be used as a technique to provide Quality of Service (QoS) to a traffic category by delaying other category of traffic to bring them into compliance with a desired traffic profile.

Two of the widely known traffic-shaping algorithms are leaky bucket and token bucket, discussed in next section in detail.

3.6.3.1 Leaky Bucket Shaper

Leaky bucket shaper as its name says, is based on the way a leaky bucket functions. It sends out the traffic at a fix rate even if the incoming traffic is bursty in nature. Bursty traffic could not be sent out at a time,, will be stored in the buffer (called the leaky bucket) and will be sent out once the outgoing line is free.



In the figure above, it is considered that the capacity of the network to carry the traffic is of 3 Mbps. The leaky bucket traffic shaper will not send traffic above 3 mbps in the network. Here, the host inserts a burst of data at a rate of 8 Mbps for 2 sec, and sends 16Mbits of data. Further, it does not send any data for next2 sec and then sends data at a rate of 2 Mbps for 4 sec, by sending 8Mbits of data. The host inserts a total data of 24Mbits in a duration of a 8 sec. After applying the leaky bucket traffic shaping policy the traffic is sent out at a rate of 3 Mbps for the duration of 8 sec. Here, traffic shaping policy smooth the traffic in the network. There are not data in the duration 2 to 3 sec, and a burst of data during the interval 0 to 2 forcing the network to congestion state. Leaky bucket policy can transmit this whole data in a smooth manner without any congestion in the network.

3.6.3.2 Token Bucket Shaper

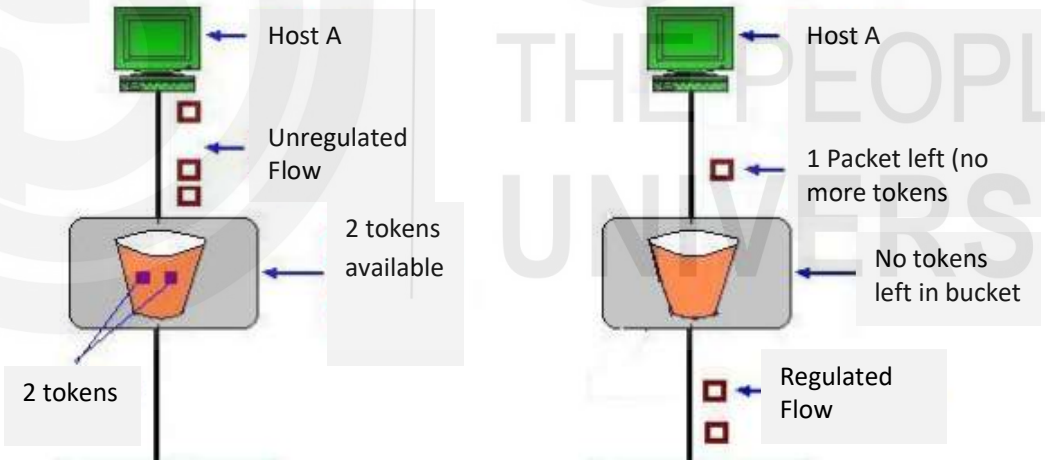
The leaky bucket traffic shaping policy discussed in previous section, does not consider the input traffic pattern. It shapes the traffic with a fixed defined rate.

Token bucket traffic shaping policy considers the input traffic bursts and allows sending the traffic on a higher rate also to prevent the drop of packets.

Token bucket policy uses the leaky bucket which holds tokens generated at regular intervals (one policy to add tokens is to generate a token per clock tick). Token bucket policy works as follows:

- Token are generated at regular intervals and placed into the bucket.
- The bucket has a maximum capacity of holding the tokens.
- A packet can be sent to the output line only if a token is available in the bucket.
- Once a packet is sent on output line, is removed from the bucket.
- As many tokens are removed from the buckets as number of packets are sent from the bucket.
- If there is no token available in the bucket, the packet cannot be sent.

Token bucket policy shapes the bursty traffic by allowing bursty traffic on output line but to a limit of available number of tokens. Figure below shown the working of the token bucket traffic shaping mechanism. In the figure host A sent 3 packets and there are only 2 tokens available in the bucket, hence only 2 of these packets are transmitted on the output line and 1 is hold back and will be sent once a token is placed in the bucket.



3.6.4 Difference between Leaky Bucket Traffic Shaper and token Bucket Traffic Shaper

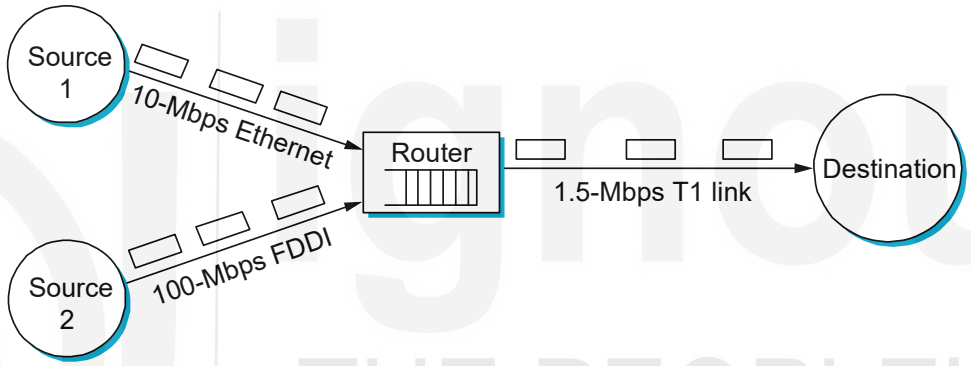
Difference between Leaky and Token buckets –

Leaky Bucket	Token Bucket
Host places the packet to be sent in the bucket.	Tokens are generated in fix intervals and placed into the bucket.
The traffic is sent onto the output link at a constant rate	Output traffic rate is regulated by the number of tokens available in the bucket.

Leaky bucket shapes the bursty traffic into uniform traffic.	The output traffic may be bursty (to a limit of tokens available in the bucket).
The bucket can hold a finite number of packets in a queue and outputs at finite rate	A packet can be sent only when a token is available in bucket.

3.7 CONGESTION CONTROL IN PACKET-SWITCHED NETWORKS

Congestion control is one of the very important parts to be considered while designing any packet-switching networks due to rapidly growing network and bandwidth intensive network applications. Various methods are proposed for congestion control.



In the figure above, source 1 and 2 inserts traffic at a rate of 10 and 100 Mbps respectively. The router can transmit the traffic on output link limited to 1.5 Mbps. The packets will start dropping at router once the buffer is full and the state is known as the congestion state. Congestion control mechanism in packet switched network can be applied on either transport layer or network layer. Flow is a sequence of packets flowing between a source/destination pair and following the same route through the network.TCP provides connection oriented reliable service at transport layer while Internet protocol (IP) provides connectionless packet delivery service.Routers does not maintain any state of the flow for connectionless service whereas state of the flow is maintained at routers for the connection oriented service. **The Internet Protocol** (**IP**) provides the basis for packet delivery and **the Transmission Control Protocol** (**TCP**) provides a best-effort delivery mechanism. **Best-effort** delivery **service** is the basic packet delivery **services** without guarantee of delivering it. The best efforts are made to deliver packets to the destination, but there is no mechanism to recover lost packets. At transport layer a TCP window is used to control the transmission rate according to feedback received from the sub network. As the congestion is a network layer issue and happens in the network, the routers play crucial role in handling the congestion state. Each router is installed with certain buffers to hold the incoming packets could not be sent at the moment due to congestion. Many policies are applied to these incoming packets to handle them in the buffer queuing. Some of the possible choices in queuing algorithms are: FIFO *also called* Drop-Tail, Fair Queuing (FQ), Weighted Fair Queuing (WFQ), Random Early Detection (RED) etc. Routers also send a special type of packet namely: choke packet

for the purpose of congestion handling. Routers monitor the utilization of their output line and send choke packets back to hosts using output lines whose utilization has exceeded some warning level. Another solution frequently used to control the congestion state is Explicit Congestion Notification (ECN) used by routers at network layer to notify the sender about the congestion state.An ECN-aware router sets a field in the header of the IP instead of dropping a packet to signal about the congestion. The receiver of the packet notifies about the congestion to the sender, which reduces its transmission rate.

3.8 SUMMARY

In this section we have discussed about the congestion control state in the network. A network is congested when traffic in the network is more than its capacity to handle it. The congestion occurs when the number of packets into the network is more than its handling capacity. The bursty nature of traffic is the root cause of congestion. When part of the network no longer can cope with a sudden increase of traffic, congestion builds upon. Other factors, such as lack of bandwidth, ill-configuration and slow routers can also bring up congestion.

Flow control is an issue of data link layer whereas congestion control is an issue of network layer. Flow control is meant to prevent a fast sender from crushing a slow receiver. Flow control can be helpful at reducing congestion, but it can't really solve the congestion problem. Many congestion control techniques are applied in the network to avoid the congestion state in the network. Open loop and closed loop congestion control techniques are the broad categories of the congestion control algorithms. Traffic policing and traffic shaping are the main techniques of open loop congestion control. Traffic policing is, sending the traffic at a fix rate irrespective of the incoming traffic pattern. In contrast to traffic policing, traffic shaping tries to adjust the rate of outgoing traffic instead of dropping the packets to ensure an even transmission rate.

3.9 SOLUTION/ANSWERS

Q1. What is congestion?

Ans : In the Internet nodes acting as transmitting nodes are inserting packets into the Internet and nodes acting as receiving nodes consume the packets from the Internet. Internet has a capacity to handle the traffic load (packets). When the rate of insertion of packets into the Internet is higher than the rate of consumption of the packets from the Internet at last Internet is unable to handle the traffic and the performance of the resources of the Internet is degraded. This situation is termed as congestion.

Q2. Why congestion occurs?

Ans: In a packet switched network, every intermediate device maintains buffers/ queues to hold packets while processing them to forward further. Under the situations of receipt of the bursty traffic these buffers gets full and packets are dropped. As a result as per the quality of service of the dropped packets, they may require to be

retransmitted, further increasing the traffic in the network. At last the system enters to congestion state.

Q3. What are the two basic mechanisms of congestion control?

Ans :Congestion in the network can be addressed in two ways: preventive method and recovery method. In preventive method, actions are taken such that congestion doesn't occur and recovery method allows the system to enter in congestion state and then it tries to remove it.

Q4. How congestion control is performed by leaky bucket algorithm?

Ans : In leaky bucket algorithm, packets are inserted into the bucket. In case of bucket overflow, packets are dropped. The packets are exited from the bucket at a constant rate allowing bursty incoming traffic into the network at a constant rate.

Q4. In what way token bucket algorithm is superior to leaky bucket algorithm?

Ans : The leaky bucket algorithm is very conservative in nature in the sense that it is not adaptive to the incoming traffic. Token bucket algorithm is made sensitive towards incoming traffic. The output rate is not dependent on the predefined upper limit rather, it depends on the availability of the tokens in the bucket. In the starting if the tokens are available in enough quantity the rate can be more and once there are no tokens available after that the output is limited by the rate of token generation.

Q5. Differentiate traffic policing and traffic shaping.

Ans. **Difference between Traffic Policing and Traffic Shaping:**

S.NO.	Traffic Policing	Traffic Shaping
1.	Traffic policing is a mechanism which monitors the traffic in any network.	Traffic Shaping is a congestion control mechanism that brings delays in packets.
2.	The packets with rates that are greater than the traffic policing rate are discarded.	It buffers the packets with rates that are greater than the traffic shaping rate.
3.	Traffic policing doesn't cause delay.	Traffic shaping causes delay of packets.
4.	The token values are calculated in bytes per second.	The token values are calculated in bits per second.
5.	In traffic policing queuing of traffic is not performed.	Queuing of traffic is not performed in traffic shaping.
6.	Traffic policing supports traffic	Traffic shaping doesn't supports

S.NO.	Traffic Policing	Traffic Shaping
	remarking.	traffic remarking.
7.	Traffic policing can be used to control outbound or inbound traffic.	Traffic policing can used to control outbound traffic only.

3.10 FURTHER READINGS

Computer Network, S. Tanenbaum, 4th edition, Prentice Hall of India,New Delhi 2002.
Data Network, DrnitriBerteskas and Robert Galleger, Second edition,Prentice Hall of India, 1997, New Delhi.
Data and Computer Communication, William Stalling, Pearson Education,2nd Edition, Delhi.