COMPUTER NETWORKS

ASSIGNMENT NO-04

COURSE: T.E. **Year: 2020-2021** **Semester: V**

DEPT: Computer Engineering

FACULTY: Umesh Mantale **DUE DATE: 12/10/2020**

==========

Roll No. 50 **Name:** Amey Thakur

Class: TE-Comps B **Date of Submission:** 28/09/2020

Questions:

Solve the following

1. Discuss the Protocols -
    a. ARP
    b. RARP
    c. ICMP
    d. IGMP

2. Discuss the Congestion control algorithms -
    a. Open-loop congestion control
    b. Closed-loop congestion control
    c. QoS parameters
    d. Token & Leaky bucket algorithms

Q.1 Discuss the protocols.

a. ARP

- Address Resolution Protocol (ARP) is a procedural for mapping a dynamic internet protocol address. (IP address) to a permanent physical machine address in a Local Area Network (LAN).
- The job of ARP is essentially to translate 32-bit addresses to 48 bit-addresses and vice versa. This is necessary because IP version 4 (IPv4).

b. RARP

- Reverse Address Resolution Protocol (RARP) is based on computer Networking which is employed by a client computer to request its IP address from a gateway servers Address Resolution Protocol table or cache.
- The network administrator creates a table in gateway router which is used to map the MAC address to corresponding IP address.

c. ICMP

- Internet Control Message Protocol
- ICMP is an error reporting and message control protocol that network devices used to report problems in packet delivery

D. IGMP.

- Internet Group Management Protocol
- IGMP is communication protocol used by hosts and adjacent routers for multicasting communication with IP networks and uses the resources efficiently to transmit the message / data packets.

Q.2. Discuss Congestion Control Algorithms.

A. Open Loop Congestion Control

- Open Loop Congestion Control policies are applied to prevent congestion before it happens. The congestion control is handled either by the source or by destination
- Policies.

① Retransmission Policy

- It is the policy in which retransmission of the packets are taken care. If the sender feels that a sent packet is lost or corrupted. The packet needs to be retransmitted The transmission may increase the congestion in the network

② Window policy

- The type of policy at the sender side may also affect the congestion. Several packets in the Go-back-N window are resent, although some packets may be received successfully at the receiver side

③ Discarding policy

- A good discarding policy adopted by the routers is that the routers may prevent congestion and at the same time partially discards the corrupted or less sensitive package and also able to maintain the quality of a message.

④ Acknowledgement Policy

- Since it is also the part of the load in-network, this policy imposed by the receiver may also affect congestion several approaches can be used to prevent congestion related to acknowledgement.

⑤ Admission Policy

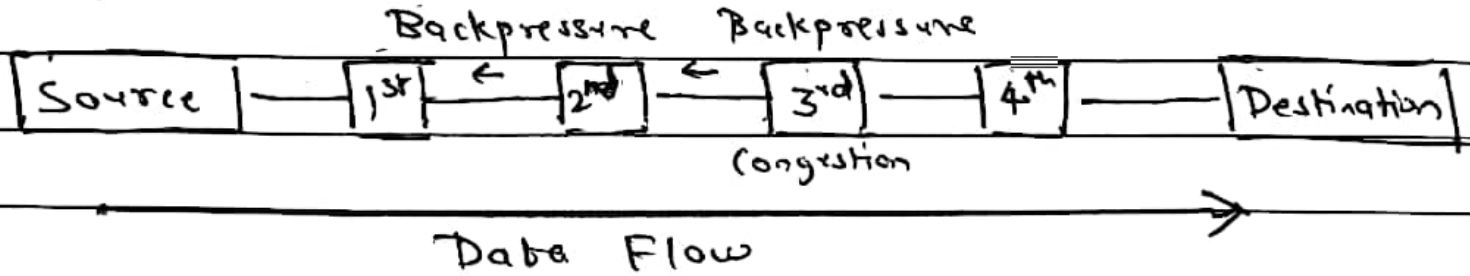
- In admission policy, a mechanism should be used to prevent congestion. Switches in a flow should first check the resource requirement of a network flow before transmitting it further. If there is a chance of congestion or there is congestion in network, the router should deny establishing a virtual network connection

B. Closed Loop Congestion Control.

- Closed loop congestion control technique is used to treat or alleviate congestion after it happens.

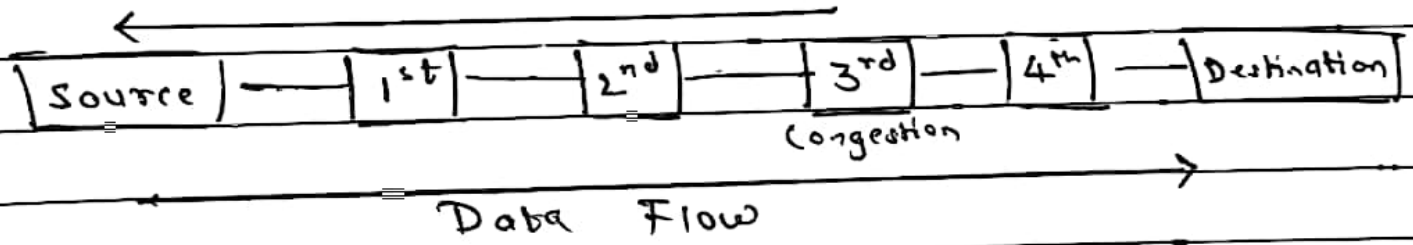
① Backpressure :

- Backpressure is a technique in which a congested node stop receiving packet from upstream node. This may cause the upstream node or nodes to become congested and rejects receiving data from above nodes. Backpressure is a node to node congestion control technique that propogate in the opposite direction of data flow. The backpressure technique can only be applied to virtual circuit where each node has information of its above upstream node.



(2) Choke Packet Technique

- It is applicable to both virtual networks as well as datagram subnets. A choke packet is a packet sent by a node to the source to uniform it of congestion. Each router monitor its resources and the utilization at each of its output lines. Whenever the resource utilization exceeds the threshold value which is set by the administrator, the router directly sends a choke packet to the source giving it a feedback to reduce the traffic. The intermediate nodes through which the packets has travelled are not warned about congestion.
- Choke Packet



(3) Implicit Signaling

- In implicit signalling, there is no communication between the congested nodes and the source. The source guesses that there is congestion in a network.
- For example, when sender sends several packets and there is no acknowledgement for a while, one assumption is that there is a congestion

④ Explicit Signaling

- In explicit signaling, if a node experiences congestion it can explicitly sends a packet to the source or destination to inform about congestion. The difference between choke packet and explicit signaling is that the signal is included in the packets that carry data rather than creating different packet as in case of choke packet technique
- Explicit signaling can occur in either forward or backward direction.

A. Forward Signaling

→ In forward signaling, signal is sent in the direction of the congestion.
→ The destination is warned about congestion
→ The receiver in this case adopt policies to prevent further congestion

B. Backward Signaling

→ In backward signaling signal is sent in the opposite direction of the congestion.
→ The source is warned about congestion and it needs to slow down.

C QoS Parameters

- Quality of service is an networking issue that has been discussed more than defined.
We can informally defined quality of service as something a flow seeks to attain where flow is the stream of packets from source to destination.

- Flows characteristics (QoS parameters)
  1. Reliability
  2. Delay
  3. Jitter
  4. Bandwidth

① Reliability

- If a packet gets lost or acknowledgement is not recieved (at sender). The retransmission of data will be needed. This decreases the reliability. The importance of reliability can differ accordingly to the application

② Delay

- Delay of a message from source to destination is a very important characteristic. However, delay can be tolerated differently by different application

③ Jitter

- The jitter is the variation in the packet delay. If the difference between delay is large, then it is called as high jitter. On the contrary, if the difference between delay is small then it is low jitter.

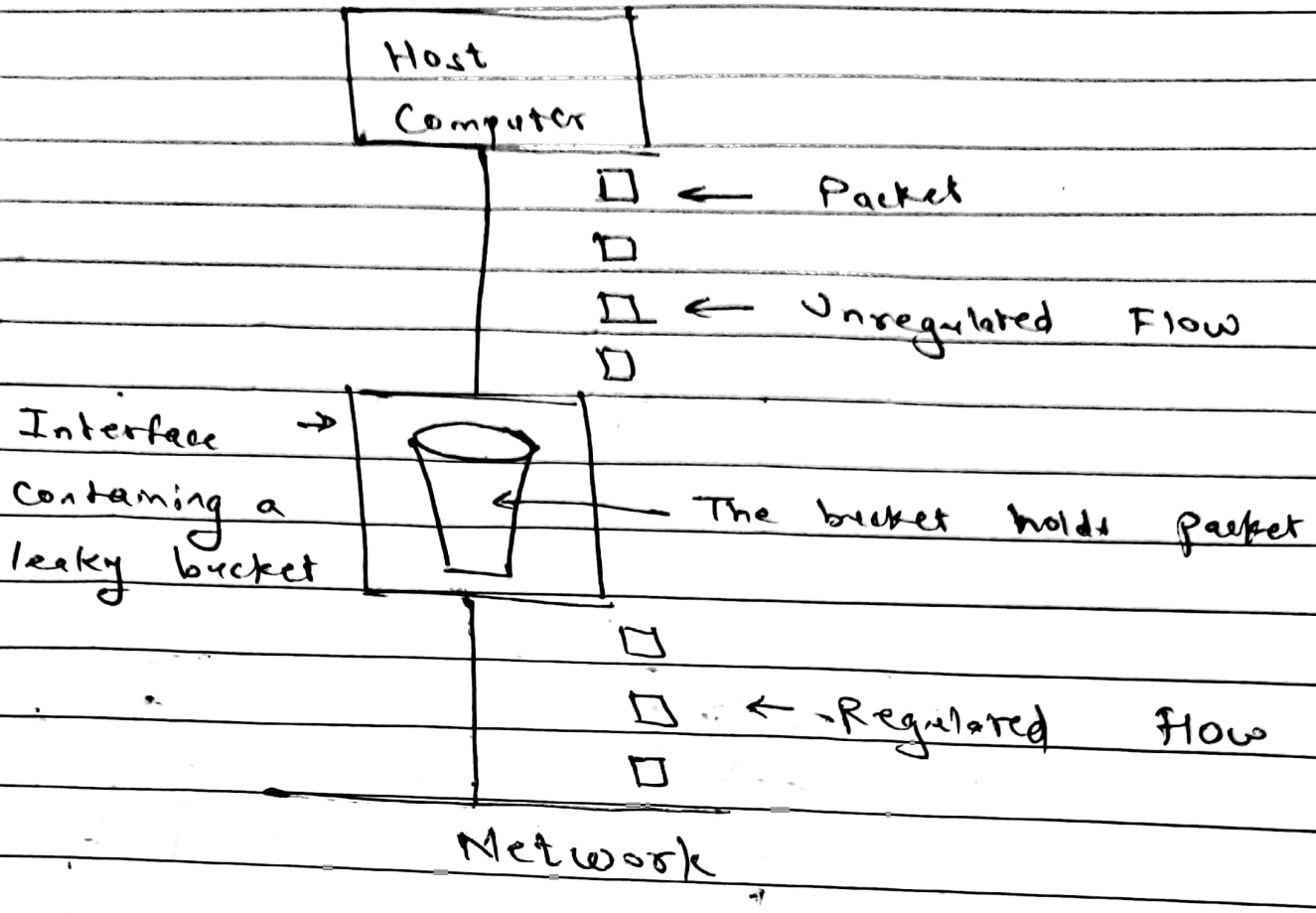
④ Bandwidth:

- Bandwidth is measured by bits per second. Different application needs different bandwidth.

D Token and Leaky Bucket Algorithm

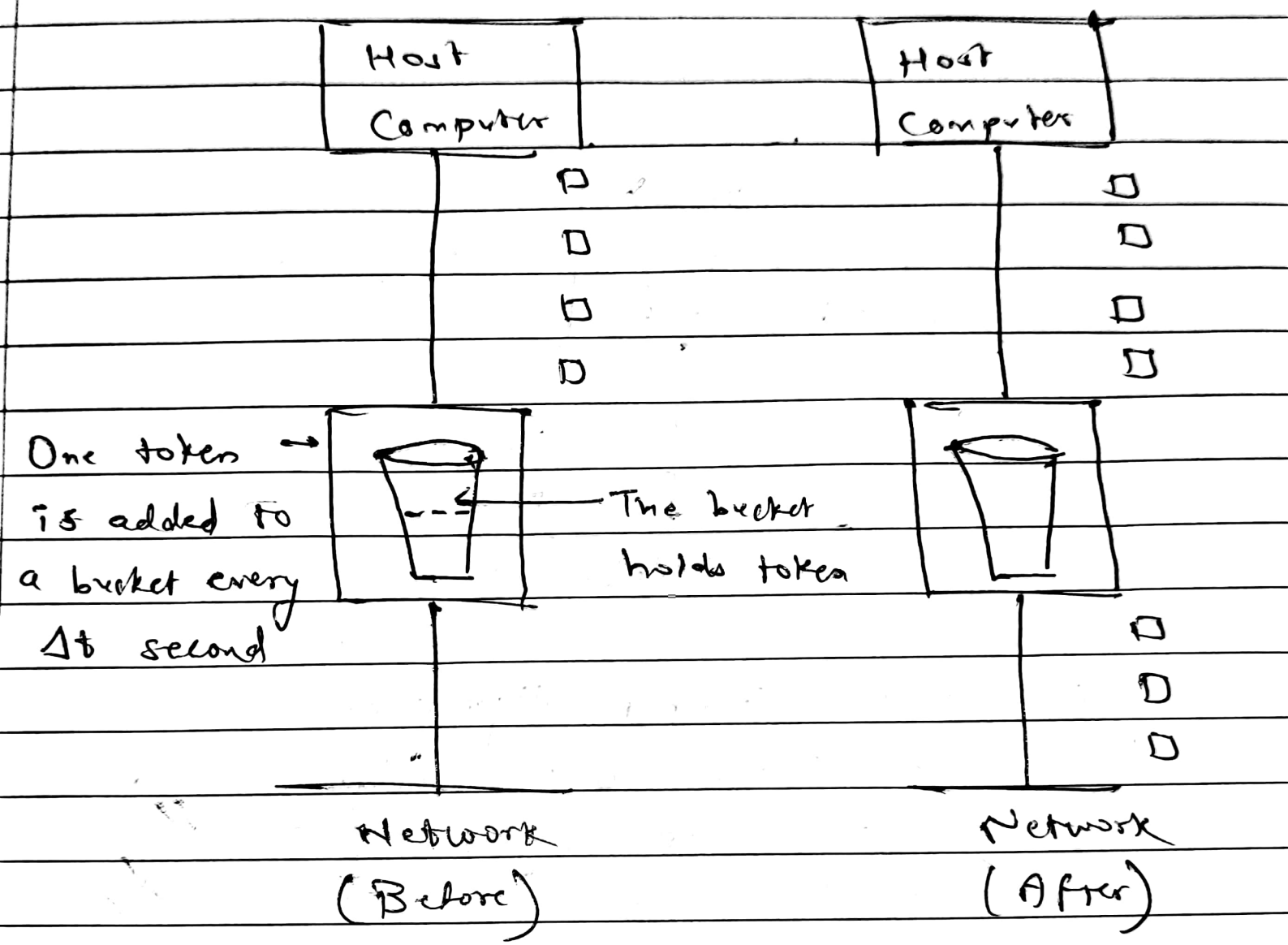
① Leaky Bucket Algorithm

- The leaky bucket algorithm is used to control the rate of a network. It is implemented as a single server queue with constant service time. If the bucket overflows then the packets are discarded.
- It enforces a constant output rate regardless of the business of the input and does nothing when input is idle.
- The host injects one packet per clock tick onto the network. This results in a uniform flow of packets smoothing out bursts and reducing congestion.
- When packets are of the same size. One packet per tick is okay. For variable length packets though, it is better to allow a fixed number of byte per tick.



(2) Token Bucket Algorithm

- The token bucket algorithm allows the output rate to vary, depending on the size of the burst.
- The bucket holds the tokens. To transmit a packet, the host must capture and destroy one token.
- Tokens are generated by a clock at the rate of one token every Δt second
- Idle hosts can capture and save up tokens in order to send larger bursts later.


Host Computer
Host Computer
One token is added to a bucket every Δt second
The bucket holds tokens
Network (Before)
Network (After)