Government Women Engg College,Ajmer
I Mid Term Examination – 8 March 2018

Subject:Computer Networks (Code :6IT1A)
Branch :B.TECH 6 SEM IT
Faculty Name :Ms Bhawana Maurya

Attempt any 4 Questions.

Q1.Discuss Routing Algorithm and Explain Dijkstra's Algorithm to find shortest path from source to destination.

Ans.Routing is the process of selecting a path for traffic in a network, or between or across multiple networks.

Routing algorithms can be divided into two groups:

i. Nonadaptive algorithms:For this type of algorithms, the routing decision is not based on the measurement or estimations of current traffic and topology, However the choice of the route is done in advance, and known as static routing.

ii. Adaptive algorithms: For these algorithms the routing decision can be changed if there are any changes in topology or traffic etc. , This is called as dynamic routing.

The examples of static algorithms are:

i. Shortest path routing:

ii. Flooding:

iii. Flow Based Routing

The example of Dynamic Routing Algorithms are:

i. Distance vector Routing Algorithm

ii. Link State Routing

Dijkstra's algorithm is an algorithm for finding the shortest paths between nodes in a graph,

Algorithm :

Let the node at which we are starting be called the initial node. Let the distance of node Y be the distance from the initial node to Y. Dijkstra's algorithm will assign some initial distance values and will try to improve them step by step.

1. Mark all nodes unvisited. Create a set of all the unvisited nodes called the unvisited set.
2. Assign to every node a tentative distance value: set it to zero for our initial node and to infinity for all other nodes. Set the initial node as current.
3. For the current node, consider all of its unvisited neighbors and calculate their tentative distances through the current node. Compare the newly calculated tentative distance to the current assigned value and assign the smaller one. For example, if the current node A is marked with a distance of 6, and the edge connecting it with a neighbor B has length 2, then the distance to B through A will be 6 + 2 = 8. If B was previously marked with a distance greater than 8 then change it to 8. Otherwise, keep the current value.
4. When we are done considering all of the neighbors of the current node, mark the current node as visited and remove it from the unvisited set. A visited node will never be checked again.
5. Move to the next unvisited node with the smallest tentative distances and repeat the above steps which check neighbors and mark visited.

6. If the destination node has been marked visited (when planning a route between two specific nodes) or if the smallest tentative distance among the nodes in the unvisited set is infinity (when planning a complete traversal; occurs when there is no connection between the initial node and remaining unvisited nodes), then stop. The algorithm has finished.

7. Otherwise, select the unvisited node that is marked with the smallest tentative distance, set it as the new "current node", and go back to step 3.

Q2.Define Congestion and Explain Leaky Bucket Algorithm for achieve good Quality of Service.

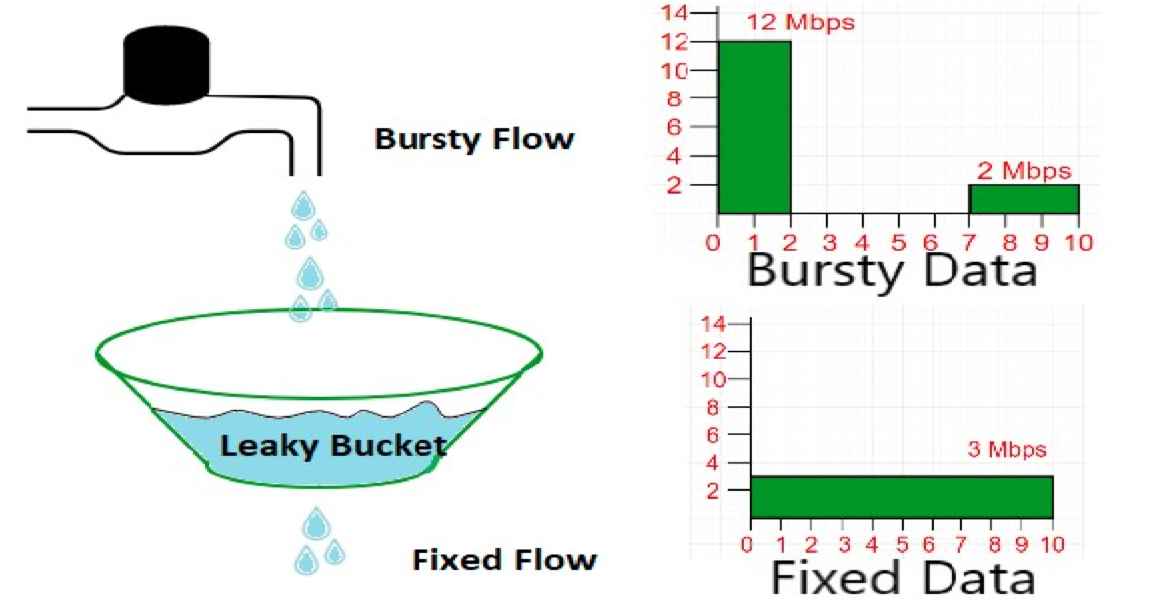
Ans:Congestion, in the context of networks, refers to a network state where a node or link carries so much data that it may deteriorate network service quality, resulting in queuing delay, frame or data packet loss and the blocking of new connections. In a congested network, response time slows with reduced network throughput. Congestion occurs when bandwidth is insufficient and network data traffic exceeds capacity.

Traffic Shaping : This is a mechanism to control the amount and the rate of the traffic sent to the network.

Two techniques can shape traffic:

1. Leaky Bucket

2.Token Bucket.



Suppose we have a bucket in which we are pouring water in a random order but we have to get water in a fixed rate , for this we will make a hole at the bottom of the bucket. It will ensure that water coming out is in a some fixed rate . And also if bucket will full we will stop pouring in it.

The input rate can vary, but the output rate remains constant. Similarly, in networking, a technique called leaky bucket can smooth out bursty traffic. Bursty chunks are stored in the bucket and sent out at an average rate.

In the figure given below, we assume that the network has committed a bandwidth of 3 Mbps for a host. The use of the leaky bucket shapes the input traffic to make it conform to this commitment. In Figure the host sends a burst of data at a rate of 12 Mbps for 2 s, for a total of 24 Mbits of data. The host is silent for 5 s and then sends data at a rate of 2 Mbps for 3 s, for a total of 6 Mbits of data. In all, the host has sent 30 Mbits of data in 10 s. The leaky bucket smooths the traffic by sending out data at a rate of 3 Mbps during the same 10 s. Without the leaky bucket, the beginning burst may have hurt the network by consuming more bandwidth than is set aside for this host. We can also see that the leaky bucket may prevent congestion.

A simple leaky bucket algorithm can be implemented using FIFO queue. A FIFO queue holds the packets. If the traffic consists of fixed-size packets (e.g., cells in ATM networks), 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.

The following is an algorithm for variable-length packets:

1.Initialize a counter to n at the tick of the clock.

2. If n is greater than the size of the packet, send the packet and decrement the counter by the packet size. Repeat this step until n is smaller than the packet size.

3. Reset the counter and go to step 1

Q3.Company is granted a site address of 201.70.64.0 with 6 subnet .Design the 6 subnet for given address.

Ans. Given address is class C network ,So the default mask is 255.255.255.0

For 6 subnet (2^n where n=3,we have maximum 8 subnet from which we choose 6 subnet)

So the subnet mask is 255.255.255.200

I.e 11111111.11111111.11111111.11100000

The six subnet are:

000,001,010,011,100,101

So the Address of 6 subnet are:

201.70.64.0

201.70.64.32

201.70.64.64

201.70.64.96

201.70.64.128

201.70.64.160

Q4.One of the address in a block is 167.199.170.82/27.Find the First and Last address of network

Ans. The value of n is 27 I.e 11111111.11111111.11111111.11100000 therefore the address is 255.255.255.224.To find the address 255.255.255.224

AND 167.199.170.82

…....................................

167.199.170.64

…....................................

1.To Find First Address:

Perform AND operation between (Address)167.199.170.64 and(Network Mask)255.255.255.224 I.e 167.199.170.64/27

We get the First Address : 167.199.170.64

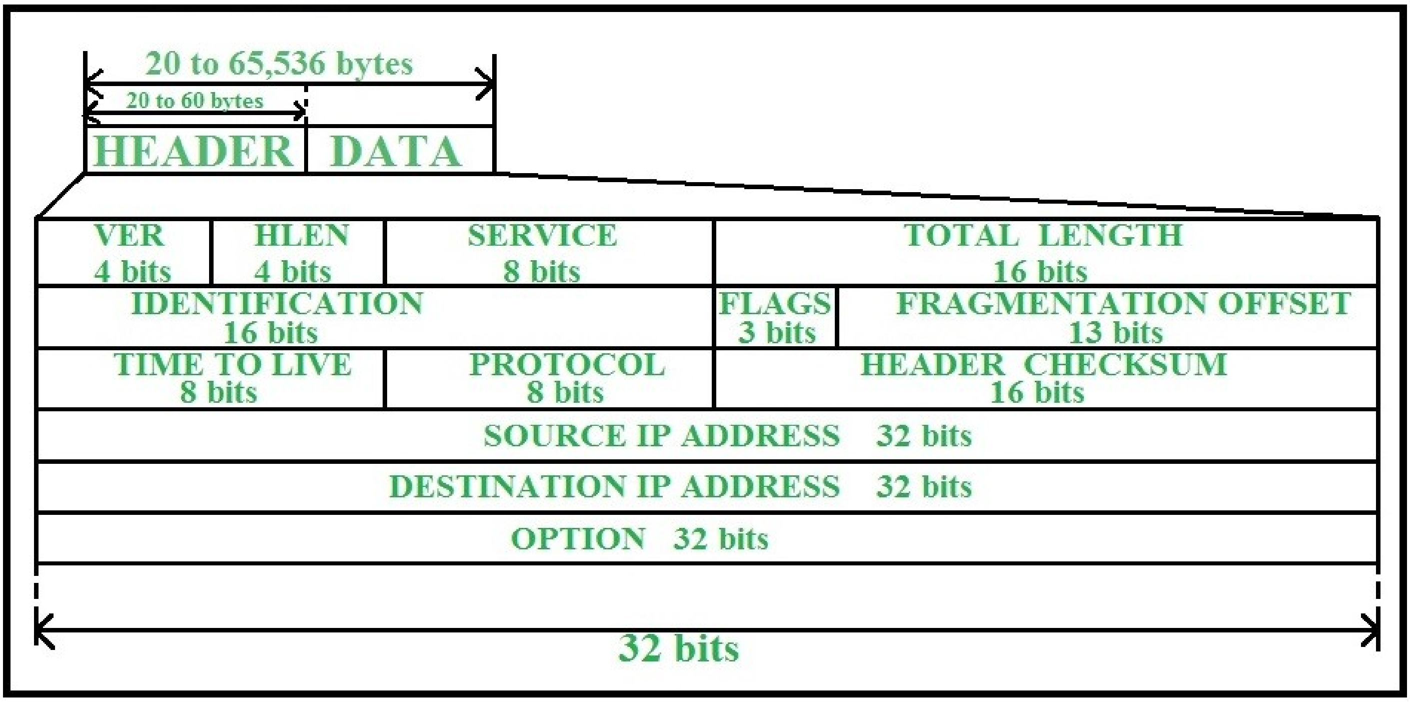
2.To Find Last Address:

Perform ones complement of network mask(255.255.255.224) and perform OR Operation with given address I.e 167.199.170.82.

We get the Last Address : 167.199.170.95

Q5.Draw and Explain the frame format of IPV4.

Ans: Frame Format of IPV4 is given below:



I) Version: This Field defines the version of IP. It is Static 4 bit value.

II) Header Length: This Field defines the length of the datagram header. It is 4 bit value.

III) Type of Service: It is 8 bit value. It is used tell the network how to treat the IP packet. These bits are generally used to indicate the Quality of Service (QoS) for the IP Packet.

IV) Packet Length: 16 bit value indicating the size of the IP Packet in terms of bytes. This gives a maximum packet size of 65536 bytes.

V) Identification: 16 bit field used for reassembling the packet at the destination.

VI) Flags: It is 3 bits value. It indicates if the IP packet can be further fragmented or not and if the packet is the last fragment or not of a larger transfer.

VII) Fragment offset: 13 bit value used in the reassembly process at the destination.

VIII) Time to Live: 8 bit value telling the network how long an IP packet can exist in a network before it is destroyed.

IX) Protocol: 8 bit value used to indicate the type of protocol being used (TCP, UDP etc.).

X) Header checksum: It is 16 bit value. It is used to indicate errors in the header only. Every node in the network has to check and re-insert a new checksum as the header changes at every node.

XI) Source address: 32 bit value representing the IP address of the sender of the IP packet.

XII) Destination address: 32 bit value representing the IP address of the packets final destination.

XIII) Options: Options are not required for every datagram. They are used for network testing and debugging.