CSE 123: Computer Networks

Homework 4 Solutions

Out: 12/03 Due: 12/10

1. **Routers and QoS**

Packet #	Size	Flow
1	100	1
2	110	1
3	50	1
4	160	2
5	80	2
6	240	2
7	90	3
8	180	3

Suppose a router has three input flows and one output. It receives the packets listed in the table above all at about the same time, in the order listed, during a period in which the output port is busy but all queues are otherwise empty.

Give the order in which the packets are transmitted for

a. Fair queuing.

First we calculate the finishing times F_i. In this case, we have $A_i = 0$ hence, F_i just becomes F_{i-1} and P_i

Packet #	Size	Flow	F_i
1	100	1	100
2	110	1	210
3	50	1	260
4	160	2	160
5	80	2	240

6	240	2	480
7	90	3	90
8	180	3	270

Thus, Packets in the order: 7, 1, 4, 2, 5, 3, 8, 6

b. Weighted fair queuing with flow 2 having twice as much share as flow 1, and flow 3 having 1.5 times as much share as flow 1.
Note: Resolve ties in the order of flow 1, flow 2, and flow 3.
In this case, we are weighting the flows. To simplify our calculations we give F_1 a weight of 2 F_3 a weight of 4 F_3 a weight of 3 so that we have the shares mentioned above. Accordingly the F_i changes as below.

Packet #	Size	Flow	**Weighted F_i**
1	100	1	50
2	110	1	105
3	50	1	130
4	160	2	40
5	80	2	60
6	240	2	120
7	90	3	30
8	180	3	90

Thus, Packets in the order: 7, 4, 1, 5, 8, 2, 6, 3

2. **Congestion Avoidance: RED**
Consider a RED gateway with MaxP = 0.02, and with an average queue length halfway between the two thresholds.
   a. Find the drop probability P_{count} for count = 10 and count = 50.

$$TempP = MaxP * \frac{AvgLen - MinThreshold}{MaxThreshold - MinThreshold}$$

AvgLen is halfway between MinThreshold and MaxThreshold, which implies that the fraction here is ½ and so TempP =

MaxP/2 = 0.01. We now have P_{count} = TempP/(1 − count × TempP) = 1/(100−count).
For count=10 this is 1/90; for count=50 it is 1/50.

b. Calculate the probability that none of the first 10 packets are dropped.

This is the probability that the first packet is not dropped times the probability that the second packet is not dropped times the probability…
$\frac{98}{99} * \frac{97}{98} * \frac{96}{97} * ... * \frac{89}{90} = \frac{89}{99} = 89.899\%$

3. Congestion Control and Congestion Avoidance

a. What is the main benefit that RED provides when compared to drop-tail?

The main benefit of RED is that it tries to be 'proactive' and avoid congestion while drop-tail is a congestion control mechanism and more 'reactive'.

b. What is the difference between congestion avoidance and congestion control?

In congestion avoidance we try to remain to the left of the 'knee' that is try and be proactive. On the other hand, in congestion control we try to the left of the cliff, that is try and be reactive.

c. Assume we have a simple network with 5 hosts and a router. The router connects each of the 5 hosts in a star topology. The RTT between each pair of hosts is 10 ms. Each host uses a simple UDP query and response protocol (i.e., each packet sent to a destination results in a single packet being sent back to the sender) to communicate between hosts. Additionally, if a sender does not receive a response within 20 ms, it retransmits the request. Multiple requests can be outstanding at one time, but each request will be retransmitted until a response is received.

Assume that the router queue is empty at the beginning. All hosts start sending requests to each other at a very high (fixed) rate. Very shortly thereafter, we notice a congestion collapse. Briefly explain (however, please be precise about your assumptions) how each of the following techniques, if implemented, would affect/prevent the congestion collapse?

i. Double the timeout value from 20 ms to 40 ms.

This might help avoid the collapse. If the buffers in the router are deep, then there is a possibility that the packet is still in the router queue when we decide to retransmit the packet. Hence, there is a chance that increasing the timeout may prevent congestion collapse as this can possible give the packet a chance to make it out of the router queue.

ii. Double the size of the queue in the router.
This might also help avoid collapse. If the router buffers are currently shallow then increasing the size of the queue can possibly help as it can reduce the number of retransmissions.

iii. If a query is not answered within a timeout interval, multiplicatively reduce the maximum rate at which the client sends query packets.
This will most definitely help. This is in essence, the multiplicative decrease that TCP uses.

iv. Use a flow control window at each receiver to prevent buffer overruns.
Not really, since flow control will not help as it doesn’t directly help reduce the traffic sent to the router. *Note, flow control is not the same as congestion control.*

4. **Network Address Translation**
Network Address Translation, NAT, is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network.

a. Why do we need NAT? Why is it a service that is present on many routers today?
The number of IPv4 addresses is much less than the number of devices. As a result, using NAT has become necessary. Another cause for NAT to become popular is that it allows, private networks where the organization cannot afford enough IP addresses for each of its hosts.

b. NAT is considered to be a temporary solution. What technology when deployed will do away with the need of NAT?
It is hoped that IPv6 when deployed will do away with the need of NAT.

Recall, a NAT capable router essentially translates private address within a network to public addresses that can be used publicly. In this question, we try and understand the working behind a simple NAT capable router. A simple NAT capable router will have mappings between the private addresses within the network (here, the private addresses all fall within the 10/8 network) to the public address(es) that it uses. Let us assume that the router has a single public address `138.76.29.7` which it uses for all communication with hosts that are not part of the private network. The router multiplexes its public IP address(es) as needed and keeps track of the multiplexing in a NAT translation table.

Assume that the router multiplexes the public address using ports starting from `8000` and then incrementing by one. For example, if a host in the private network with address `10.0.0.5:5000` sends a message to `132.239.8.45:80` then the entry in the NAT table would be filled in as below. The next time the router will use `8001` as the port to establish a new connection and so on.

NAT Translation Table	
WAN Side Address	**LAN Side Address**
138.76.29.7:8000	10.0.0.5:5000
138.76.29.7:8001	10.0.0.6:5000
138.76.29.7:8002	10.0.0.10:6000
138.76.29.7:8003	10.0.1.101:6001
138.76.29.7:8004	10.0.0.7:7000

`Note: iv, v, vii, viii will not create any new entries.`

c. What would be the entries in the NAT Translation Table at the end of the following events
   i. 10.0.0.6:5000 sends a message to 74.125.239.33:80
   ii. 10.0.0.10:6000 sends a message to 204.79.197.200:80
   iii. 10.0.1.101:6001 sends a message to 206.190.36.45:80
   iv. 10.0.0.10:6000 sends another message to 204.79.197.200:80
   v. 10.0.1.101:6001 sends a message to 74.125.239.33:80
   vi. 10.0.0.7:7000 sends a message to 63.245.215.20:80
   vii. 204.79.197.200:80 sends a message to 10.0.0.10:6000
   viii. 206.190.36.45:80 sends a message to 74.125.239.33:80

   Note: The NAT Table should like the one above with the entries generated from the events in (c.) filled in

d. For simplicity, let us assume that message format is `MSG<Sender, Receiver>.` In that case, if a host in the private network with address `10.0.0.5:5000` sends a message to `132.239.8.45:80` then the message recevied at the router and leaving at the router would look as follows

Message Received from Host: *`MSG<10.0.0.5:5000, 132.239.8.45:80>`*
Message Sent from Router: *`MSG<138.76.29.7:8000,132.239.8.45:80>`*
Note: We will need to use the entries from the table we filled in (c.) to do this.

List out the message received from the host at the router and the message sent from the router (like shown above) for the following messages:

1. `10.0.0.6:5000` sends a message to `74.125.239.33:80`
   `Incoming: MSG<10.0.0.6:5000,` `74.125.239.33:80>`
   `Outgoing: MSG<138.76.29.7:8001``,74.125.239.33:80>`

2. `10.0.0.10:6000` sends a message to `204.79.197.200:80`
   `Incoming: MSG<10.0.0.10:6000,` `204.79.197.200:80>`
   `Outgoing: MSG<138.76.29.7:8002``,204.79.197.200:80>`

e. If the router gets a message `MSG<74.125.239.33:80,`*`138.76.29.7:8001>`*`,` what would the message look like leaving the router?
`Outgoing: MSG<74.125.239.33:80,`*`10.0.0.6:5000`*`>`

f. Finally, if the router gets a message `MSG<10.0.0.10:6000, 10.0.1.101:6001>`, what what would the message look like leaving the router?
`No change since the message is within the private network.`
`MSG<10.0.0.10:6000, 10.0.1.101:6001>`