Homework 2 solutions

---

1. Imagine a flow specification that has a maximum packet size of 100 bytes, a token bucket rate of 10 million bytes/sec, a token bucket size of 1 million bytes, and a maximum transmission rate of 50 million bytes/sec. how long can a burst at maximum speed last?

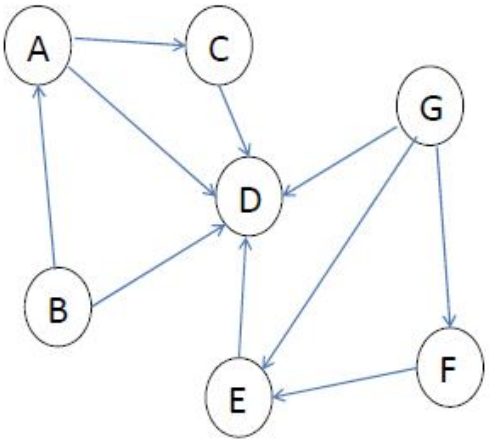
The correct answer can be obtained by using the formula

S = C/(M -p). Substituting, we get S = 1/(50-10) = 0.025sec.

---

2. The following shows a destination oriented DAG in which the destination is D.

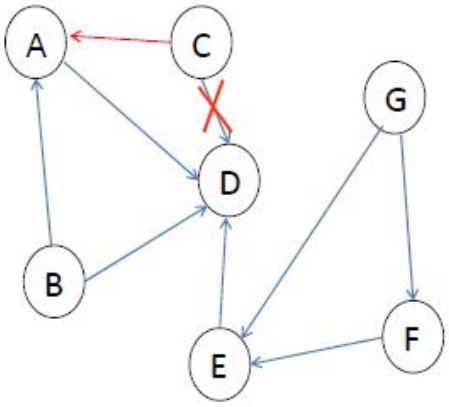
Show step by step how TORA works if the following successive events happen?



1) The link GD fails

All nodes still have an outbound link, so none of the nodes generate an UPD message.

2) The link CD fails



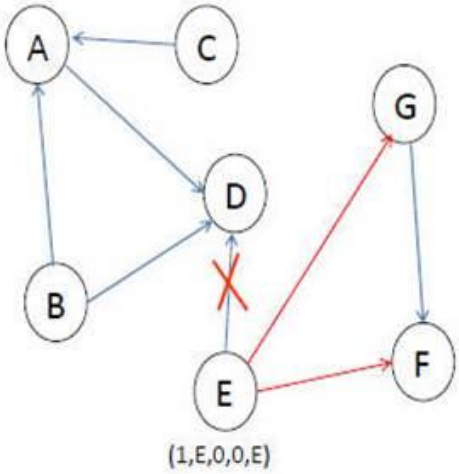
Only C doesn't have an outgoing link, so it reverses its incoming link. Now C has a route to D.

3) The link ED fails

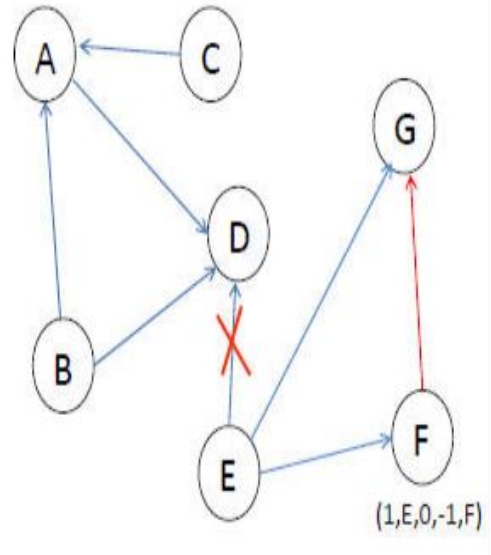
a. A, B, C are OK. E detects the link failure. Since it doesn't have any outbound link, so E does the followings:

- E generates a new reference level which is 1

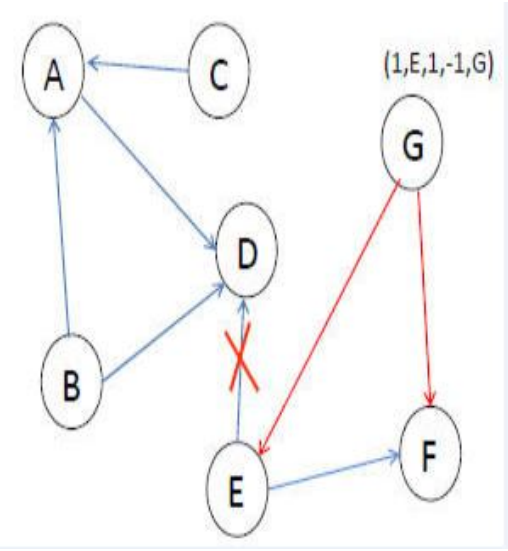
- sets the oid to E and transmits an UPD message.
- It also reverses the direction of all its inbound links.



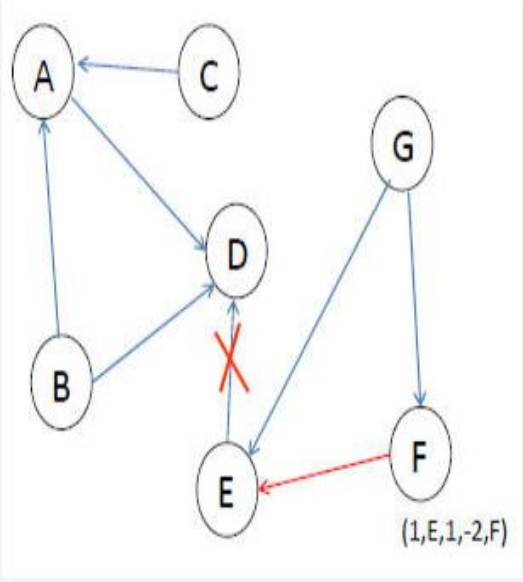
b. Now, F doesn't have any outbound link. It resorts to partial link reversal and reverses the direction of its links to G and transmits an UPD.
It also sets its own offset to –1 to ensure that it is at a lower level compared to E.



c. Now G doesn't have any outbound link. Since all its links have been reversed, it resorts to a full reversal, flip the r_i bit and sends reflection to E and F.



d. F doesn't have any outbound link, it reverses the link to E and propagates the reflection to E



e. Now E realizes that there is a partition. It sets its height to NULL and sends an CLR to G and F.

---

3. Consider an RTP session consisting of 4 users, all of which are sending and receiving RTP packets into the same multicast address. Each user sends video at 100kbps.

a) RTCP will limit its traffic to what rate?

b) A particular receiver will be allocated how much RTCP bandwidth?

c) A particular sender will be allocated how much RTCP bandwidth?

a) The session bandwidth is 4* 100 kbps = 400 kbps. Five percent of the session bandwidth is 20 kbps.

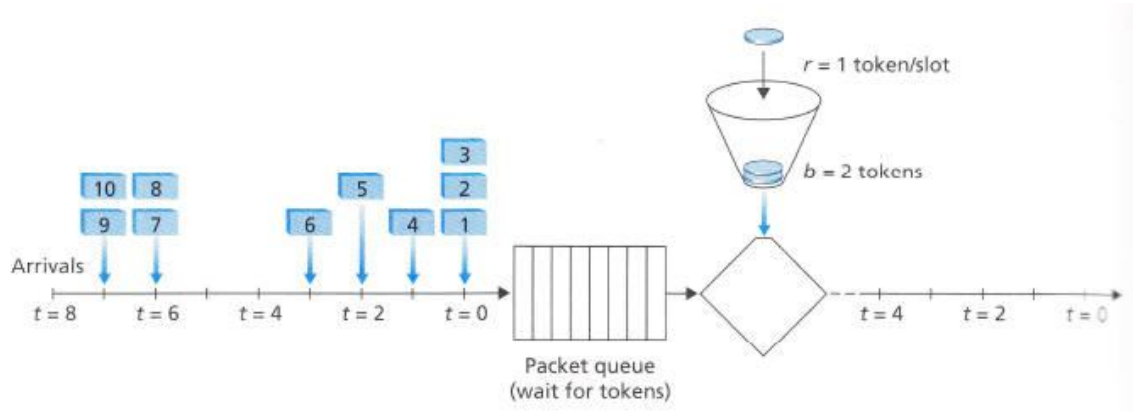
b) RTCP protocol offers 75% of the BW to the receiver i.e. 75% of 20Kbps = 15Kbps shared by remaining users 3 receivers i.e. 15/3 = 5Kbps

c) RTCP gives 75 % of its control traffic bandwidth to the receiver and 25% to sender.

In this case: sender gets 25 % of 20Kbps = 5kbps

---

4. Consider the figure below, which shows a leaky bucket being bed by a stream of packets. The token buffer can hold at most two tokens, and is initially full at at t=0. New tokens arrive at a rate of one token per slot. The output link speed is such that if two packets obtain tokens at the beginning of a time slot, they can both to to the output link in the same slot. The timing details of the system are as follows:



1) Packets (if any) arrive at the beginning of the slot. Thus in the figure, packets 1,2 and 3 arrive in slot 0. if there are already packets in the queue, then the arriving packets join the end of the queue. Packets proceed towards the front of the queue in a FIFO manner.

2) After the arrivals have been added to the queue, of there are any queued packets, one or two of those packets (depending on the number of available tokens) will each remove a token from the token buffer and go to the output link during that slot. Thus, packets 1 and 2 each remove a token from the buffer (since there are initially two tokens) and to to the output link during slot 0.

3) A new token is added to the token buffer if it is not full, since the token generation rate is r=1token/slot.

4) Time then advances to the next time slot, and these steps repeat.

Answer the following questions:

a) For each time slot, identify the packets that are in the queue and the number of tokens in the bucket, immediately after the arrivals have been processed (step 1 above) but before any of the packets have passed through the queue and removed a token. Thus, for the t=0 time slot in the example above, packets 1,2 and 3 are in the queue, and there are two tokens in the buffer.

Time Slot	Packets in the queue	Number of tokens in bucket
0	1, 2, 3	2
1	3, 4	1
2	4,5	1
3	5,6	1
4	6	1
5	-	1
6	7, 8	2
7	9, 10	1
8	10	1

b) For each time slot indicate which packets appear on the output after the token(s) have been removed from the queue. Thus, for the t=0 time slot in the example above, packets 1 and 2 appear on the output link from the leaky buffer during slot 0.

Time Slot	Packets in output buffer
0	1, 2
1	3

2	4
3	5
4	6
5	-
6	7, 8
7	9
8	10

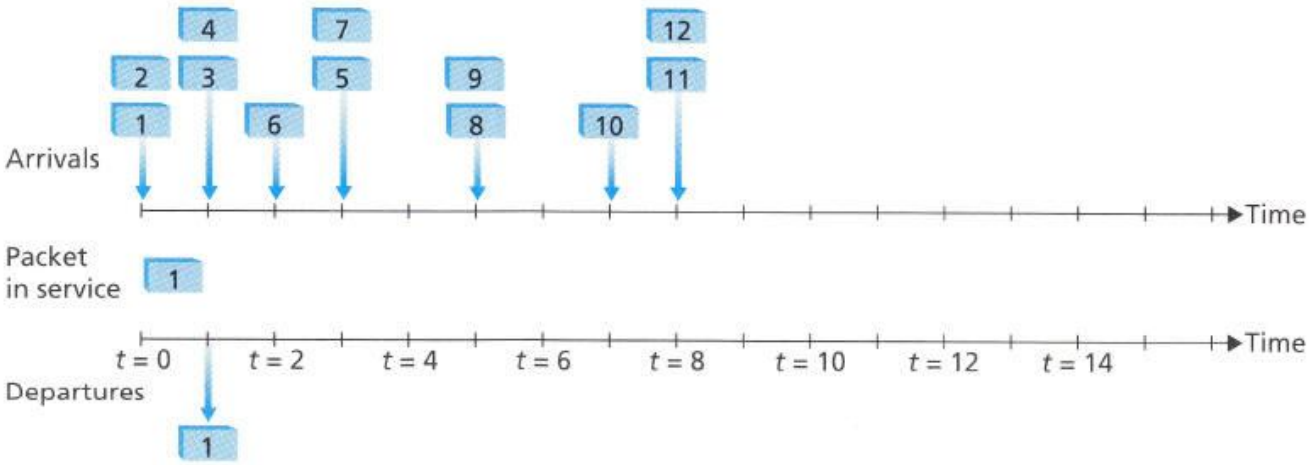
---

5. Repeat the above problem but assume that r=2. Assume again that the bucket is initially full

Time Slot	Packets in the queue	Number of tokens in bucket
0	1, 2, 3	2
1	3, 4	2
2	5	2
3	6	2
4	-	2
5	-	2
6	7, 8	2
7	9, 10	2
8	-	2

Time Slot	Packets in output buffer
0	1, 2
1	3, 4
2	5
3	6
4	-
5	-
6	7, 8
7	9, 10
8	-

6.Consider the following figure, answer the following questions:



a. Assuming FIFO service, indicate the time at which packets 2 through 12 each leave the queue. for each packet, what's the delay between its arrival and the beginning of the slots in which it is transmitted? What is the average of this delay over all 12 packets?

Packet	Time leaving the queue	Delay
1	0	0
2	1	1
3	2	1
4	3	2
5	5	2
6	4	2
7	6	3
8	7	2
9	8	3
10	9	2
11	10	2
12	11	3
Average Delay		1.91

b. Now assume a priority service, and assume that odd-numbered packets are high priority, and even-numbered packets are low priority. Indicate the time at which packets 2 through 12 each leave the queue. for each packet, what's the delay between its arrival and the beginning of the slots in which it is transmitted? What is the average of this delay over all 12 packets?

Packet	Time leaving the queue	Delay
1	0	0
2	2	2
3	1	0
4	6	5
5	4	1
6	7	5
7	3	0
8	9	4
9	5	0
10	10	3
11	8	0
12	11	3

Average Delay	1.91

c. Now assume round robin service. Assume that packets 1,2,3,6,11, and 12 are from class 1, and packets 4,5,7,8,9, and 10 are from class 2.Indicate the time at which packets 2 through 12 each leave the queue. for each packet, what's the delay between its arrival and the beginning of the slots in which it is transmitted? What is the average of this delay over all 12 packets?

Packet	Time leaving the queue	Delay
1	0	0
2	2	2
3	4	3
4	1	0
5	3	0
6	6	4
7	5	2
8	7	2
9	9	4
10	11	4
11	8	0
12	10	2
Average Delay		1.91

d. Now assume weighted fair queueing (WFQ) service. Assume that odd-numbered packets are from class 1, and even-numbered packets are from class 2. Class 1 has a WFQ weight of 2, while class 2 has a WFQ weight of 1. Indicate the time at which packets 2 through 12 each leave the queue. for each packet, what's the delay between its arrival and the beginning of the slots in which it is transmitted? What is the average of this delay over all 12 packets? (Note that it may not be possible to achieve an idealized WFQ schedule).

Packet	Time leaving the queue	Delay	Note
1	0	0	WFQ
2	2	2	WFQ
3	1	0	WFQ
4	5	4	WFQ
5	3	0	WFQ
6	7	5	Idealized WFQ scheduling
7	4	1	WFQ
8	9	4	WFQ
9	6	1	Idealized WFQ scheduling
10	10	3	WFQ
11	8	0	WFQ
12	11	3	WFQ
Average Delay		1.91	

e. What do you notice about the average delay in all four cases (FIFO, priority, RR, and WFQ)?

It can be noticed that the average delay for all four cases is the same (1.91 seconds).

---

7. break the following columnar transposition cipher. The plaintext is taken from a popular computer textbook, so "computer" is a probable word The plaintext consists entirely of letters (no spaces). The ciphertext is broken up blocks of five characters for readability

aauan cvlre rurnn dltme aeepb ytust iceat npmey iicgo gorch srsoc nntii imiha oofpa gsivt tpsit lbolr otoex

The plaintext is: a digital computer is a machine that can solve problems for people by carrying out instructions given to it.

---

8. Using the RSA public key cryptosystem, with a=1, b=2, etc.

a) if p=7 and q=11, list five legal values for d

For these parameters, z = 60, so we must choose d to be relatively prime to 60. Possible values are: 7, 11, 13, 17, and 19.

b) If p=5, q=11, d=27, and e=3, show how to encrypt and decrypt "abcde".

With these parameters, e = 3. To encrypt P we use the function C = P3 mod 55. For P = 1 to 10, C = 1, 8, 27, 9, and 15 respectively.

---

9. The Diffie--Hellman key exchange is being used to establish a secret key between Alice and Bob. Alice sends Bob p=719, g=3 and her public key 191. Bob responds with his public key 543. Alice's private key is 16. Bob's private key is 15. How Alice and Bob computes the shared secret key?

Alice: $Y_b^{Xa} \bmod p = 543^{16} \bmod 719 = 40$

Bob: $Y_a^{Xb} \bmod p = 191^{15} \bmod 719 = 40$
