COMP3331/9331 XXXX
Computer Networks and Applications
Final Examination (SAMPLE SOLUTIONS)

Question 1 (**X marks**)

(a) The one-way propagation delay between A and B is 100/1 = 100 seconds. The RTT will be 2 x one-way propagation delay = 200 seconds.

(b) delay x bandwidth product = 100 seconds x 1000bps = 1 x 10^5 bread crumbs.

(c) Time for the messenger to reach hole B = one-way propagation delay = 100 seconds.

The time for the 10,000 ants to arrive at Hole A = transmission time + one-way propagation delay = 10,000/1000 + 100 = 110 seconds.

Total delay = 100 + 110 = 210 seconds. (or 210.001 seconds).

Question 2 (**X marks**)

(i) SendBase is set to 7500.

(ii) First segment carries 500 bytes, second segment carries 1000 bytes, third one carries 1500 bytes and the last segment carries 500 bytes. Thus, the total data in the four segments is 3500 bytes.

(iii) The window size is set to the minimum of congestion window and receive window. Hence, the window size will now be set to 6000 bytes. Since current SendBase is 7500, this implies that the last byte that the sender can send with certainty is 13499.

(iv) Since the sender receives three duplicate ACKs, the CongWin is reduced to half the current value (current value = 10000 bytes), which is 5000 bytes.

(v) Since the sender received three duplicate ACKs for 7500, it will now retransmit the segment with sequence number 7500.

Question 3 (**X marks**)

Refer to Figure below. In Figure (a), the ratio of the linear decrease on loss between connection 1 and connection 2 is the same - as ratio of the linear increases: unity. In this case, the throughputs never move off of the AB line segment. In Figure (b), the ratio of the linear decrease on loss between connection 1 and connection 2 is 2:1. That is, whenever there is a loss, connection 1 decreases its window by twice the amount of connection 2. We see that eventually, after enough losses, and subsequent increases, that connection 1's throughput will go to 0, and the full link bandwidth will be allocated to connection 2.

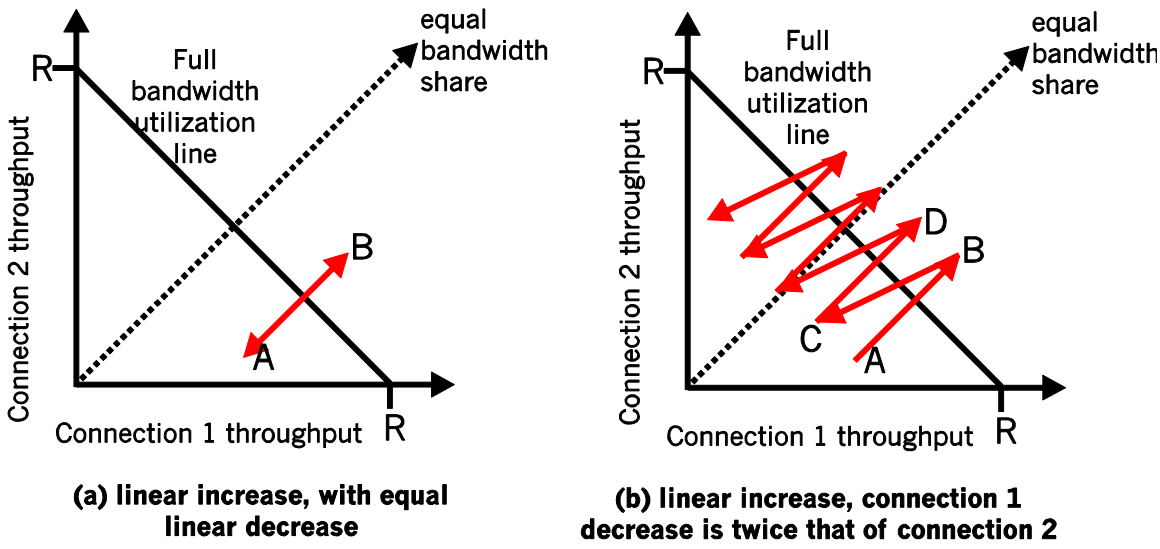

Figure: Lack of TCP convergence with linear increase, linear decrease

Question 4 (X marks)

a) Let W denote the max window size measured in segments. Then, W*MSS/RTT = 10Mbps, as packets will be dropped if the maximum sending rate exceeds link capacity. Thus, we have W*1500*8/0.15=10*10^6, then W is about 125 segments.

b) As congestion window size varies from W/2 to W, then the average window size is 0.75W=94 (ceiling of 93.75) segments. Average throughput is 94*1500*8/0.15 =7.52Mbps.

c) 125/2 *0.15 = 9.375 seconds, as the number of RTTs (that this TCP connections needs in order to increase its window size from W/2 to W) is given by W/2. Recall the window size increases by one in each RTT.

Question 5 (X marks)

(a)

Step	N'	D(B),p(B)	D(C),p(C)	D(D),p(D)	D(E),p(E)	D(F),p(F)
0	A	20,A	2,A	2,A	2,A	INF
1	AC					
2	ACD	5,D				5,D
3	ACDE	3,E				
4	ACDEB					
5	ACDEBF					

(b)

If we take the distance table to be the set of distance vectors, then the table at A is:

	Destinations					
NEIGHBORS	A	B	C	D	E	F
A	0	3	2	2	2	5
B	3	0	5	3	1	6
C	2	5	0	4	4	7
D	2	3	4	0	4	3
E	2	1	4	4	0	7

(c)

(i) Failure of link A-B has no effect on the routing tables since the link is not part of the shortest path topology, hence no action will be taken.

(ii) When link A-C fails, A realizes that the link has failed and tries to find a new neighbor to route through to C. A's routing table shows that the shortest available path to C is through neighbor D and has cost 6 (cost 2 to reach D and cost 4 from D to C). Without realizing that D's next hop to C is A, A makes D the next hop neighbor for its route to C, and advertises a new cost of 6 to C in its routing advertisement. D then updates its cost to 8 since the cost to get from D to A is 2 and the advertised cost from A to C is 6. Thus, A and D "count to infinity" by updating costs by two each time. Once the cost through A becomes greater than (or equal to 20), D chooses the link D-C as the shortest path and advertises 20 to A. A updates its cost to 22, and the count stops.

(iii) When link A-E fails, A realizes that the link has failed and tries to find a new neighbor to route through to E. A's routing table shows that the shortest available path to E is through neighbor B and has cost 4 (cost 3 to reach B and cost 1 from B to E). But now the path to B is through E and hence A will no select this option as A-E is down. A's routing table shows that the second shortest available path to E is through neighbor D and has cost 6 (cost 2 to reach D and cost 4 from D to E). Without realizing that D's next hop to E is A, A makes D the next hop neighbor for its route to C, and advertises a new cost of 6 to C in its routing advertisement. D then chooses the real shortest path of D-B-E. Though count to infinity occurs briefly due to the presence of an alternative path it is averted. Also if D advertises its path to C through B this situation will never have occurred. So this case may or may not cause count to infinity.

A solution to the count-to-infinity problem is poisoned reverse.

Question 6 (X marks)

(a) This is because Sheldon's NAT device is not recomputing the TCP and IP checksums after it changes the IP address and port numbers in each packet that passes through it. As a result, when routers in the Internet compute the checksum for these packets, they detect an error and hence, drop the packets

(b) Remember that FTP commands contain the port number and IP address of the end hosts (e.g. PORT). For FTP to work effectively through a NAT, the NAT must be configured to replace the IP addresses and port numbers used in accordance with the NAT translation table. Sheldon has not configured his NAT accordingly and hence he cannot use FTP. However, no such configuration is required for Web and hence he can successfully browse the Web.

Question 7 (X marks)

(a) 128.96.171.92 – Interface 0
(b) 128.96.167.151 – Interface 2
(c) 128.96.163.151 – Interface 4
(d) 128.96.169.192 – Interface 1
(e) 128.96.165.121 – Interface 3

Question 8 (X marks)

Action	**Switch Table State**	**Link(s) packet is forwarded to**	**Explanation**
B sends a frame to E	Switch learns interface corresponding to MAC address of B	A, C, D, E, and F	Since switch table is empty, so switch does not know the interface corresponding to MAC address of E
E replies with a frame to B	Switch learns interface corresponding to MAC address of E	B	Since switch already knows interface corresponding to MAC address of B
A sends a frame to B	Switch learns the interface corresponding to MAC address of A	B	Since switch already knows the interface corresponding to MAC address of B
B replies with a frame to A	Switch table state remains the same as before	A	Since switch already knows the interface corresponding to MAC address of A

Question 9 (X marks)

The energy magnitude of the signals from the sender may overwhelm other signals from other nodes, since the wireless signals decay very quickly in distance. It is thus hard to physically detect collision at the sender.

With those difficulties, 802.11 implements CSMA/CA (Collision Avoidance, with RTS/CTS) instead.

Question 10 (X marks)

(a) C's packet would indeed arrive successfully at D, since D cannot hear A's transmission. Hence, there is no interference from the perspective of the receiver (i.e. D).
However, A's packet would not arrive successfully at B, since there will be a collision at B due to interference from C's transmission.

(b) C will not transmit while A is transmitting. This is because C would have overhead the CTS frame sent by B (in response to the RTS request from A). The CTS frame will contain the duration of time for which the on-going transmission between A and B will go on. Thus, C will know when A is transmitting.

(c) Same reason as above. The CTS contains the time and hence, C will know when A's transmission will end.

Question 11 (X marks)

a) No, without a public-private key pair or a pre-shared secret, Bob cannot verify that Alice created the message.

b) Yes, Alice simply encrypts the message with Bob's public key and sends the encrypted message to Bob.

Question 12 (X marks)

Rule	*Source*	*Destination*	*Application*	*Action*
R1	Any-outside	98.2.3.4	HTTP	Allow
R2	Any-outside	98.4.5.6	SMTP	Allow
R3	25.5.6.7	98.3.4.5	HTTP	Allow
R4	Any-outside	98.3.4.5	HTTP	Disallow
R5	Any-outside	98.4.5.6	BitTorrent	Disallow
R6	98.4.5.6	Any-outside	BitTorrent	Disallow
R7	Any-outside	Any-inside	BitTorrent	Allow
R8	Any-inside	Any-outside	BitTorrent	Allow
R9	Any-internal	Any-outside	HTTP	Allow
R10	98.4.5.6	Any-outside	SMTP	Allow
R11	Any-inside	Any-outside	SMTP	Disallow

END OF EXAM