CSC358 - Problem Set 2

Arslan Qamar, 100 269 7897

Feb. 28 , 2018

Solutions

1. (a) There would be three paths to P through links 1, 2, and 3.

   (b) If they adopt the policy that outbound traffic is routed to the closest link to the destination provider then Path or cross link 1 will be for traffic from host A to host B. However, path 2 will be used for traffic from host B to host A.

2. (a) Routing would be inefficient for this organization's inbound traffic since it has a single address network in the world further tell us there is only a single address and thus all incoming traffic uses that single path even if shorter paths are available.

   (b) The organization can make sure that it directs the outbound traffic to exit through it's addresses that are geographically close to the traffic destination.

   (c) It has to divide the network into subnets based on geographical locations. This would cause inbound traffic to route to the closest subnet. In order to fix the problem for outside networks, they would be told the particular addresses of the subnets so they can send traffic to particular subnets within the organization.

   (d) Internal routing structure will look like this; Every internal router needs to know subnets and route internal traffic to required subnets and making sure its doesn't leave the organization.

3. The sequence number will not be wrapping around from $2^{32} - 1$ to 0 always because it is randomly generated or sometimes clock generated when a connection is made. The reason for being a randomly generated is to help avoid the collision/interface between different hosts and/or servers.

4. (a) Compare to lossless transmission, The sender has lost 1100 ms. The 1100 ms is compose of 300 ms and 800 ms. 300 ms required to detect three duplicate ACKs before the lost packet could be send and 800 ms required for the ACK of lost packet that was send again. $\therefore$ sender has lost 1100 ms

   (b) The sender has lost 400 ms in the case when the sender uses the continued arrival of each duplicate ACK. the sender started again at 1100 ms. However, the sender could have sent four time before, that gives us the 400 ms. So, 400 ms would be subtracted from 1100 ms will give us 700 ms.

5. The measurements taken by us as a Service Provider is to rule out duplicate ACK's in order to identify fast re transmit algorithm.

   We can detect that the host is using slow start because the number of ACK received by router should never be different or packet being sent out is greater than ACK received. After a timeout condition, congestion window will fall at least in half.

6. Since all the incoming traffic becomes outgoing traffic due to the same bandwidth, so R1 can never get congested.
   So, to find a traffic pattern that congests that router alone, we know for each router R; 2 links from children and 1 link from parent. Router R's parent link has throughput of twice that is for its child. Suppose if all 6 right-hosts carrying 6 MBps sends to two-left hosts there will be a congestion since it can only handle 2 MBps.

7. (a) From A to S, the source port can be 1025 (in range of 1024-65535), and destination port will be 23. (since port range from 1024-65525 are considered for connection of temporary nature).
   (b) From B to S, the source port can be 1030 (in range of 1024-65535) and destination port will be 23.
   (c) From S to A, the source port will be 23 and destination port can be 1025 (in range of 1024-65535).
   (d) From S to B, the source port will be 23 and destination port can be 1030 (in range of 1024-65535).
   (e) No, it is not possible that source port in the segments from A to S is the same as that from B to S. There is not as such relationship between source port within the different hosts which are A and B.
   (f) Even if they are same host the same source port number will not be assigned because OS only assigns port number that haven't been assigned already. Thus, avoid duplication's.

8. Sum of these 8-bit bytes:

	0	1	0	1	0	0	1	1
	0	1	1	0	0	1	1	0
+	0	1	1	1	0	1	0	0
	0	0	1	0	1	1	0	1

   The answer is 1 0 0 1 0 1 1 0 1, there is a 1 (carry bit not shown in calculation).
   It becomes as 0 0 1 0 1 1 1 0.
   The 1's compliment would be 1 1 0 1 0 0 0 1.
   UDP takes the 1s complement of the sum in order to simplify error detection at receiver end. Moreover, avoids different check sum value depending on the sender-receiver endian formats.
   The receiver detects the error by adding the total four 16 bit words which includes the 3 words and a single check sum header in UDP segment header. For the sake of this question adding all 4 words which are 8 bits should give us 1111 1111. Thus, if any sum contains a zero, An error has been occurred. We know from previous all one bit error can be detected but two bit errors can be undetected sometimes.

9. (a) Cwnd begins from 6 MSS,
   1 RTT need 6 MSS to be sent and cwnd increased to 7
   2 RTT need 7 MSS to be sent and cwnd increased to 8
   3 RTT need 8 MSS to be sent and cwnd increased to 9
   4 RTT need 9 MSS to be sent and cwnd increased to 10
   5 RTT need 10 MSS to be sent and cwnd increased to 11
   6 RTT needed 11 MSS to be sent and cwnd increased to 12
   So, it needed altogether 6 RTT to increase cwnd from 6 MSS to 12 MSS
   (b) MSS sent in 6 RTT are 6, 7, 8, 9, 10, 11 MSS respectively.
   Average Throughout = $\frac{totalMSSsent}{6RTT}$

   Average Throughout = $\frac{6+7+8+9+10+11}{6RTT}$
   $\therefore$Average Throughout would be $8.50\frac{MSS}{RTT}$

10. (a) The routing protocol would be eBGP.
    (b) The routing protocol would be iBGP.

(c) The routing protocol would be eBGP.

(d) The routing protocol would be iBGP.

11. The below table shows the Dijkstra's algorithm to compute the shortest path from x to all network nodes xvuwytz.

Step	N'	D(v),p(v)	D(u),p(u)	D(w),p(w)	D(y),p(y)	D(z),p(z)	D(t),p(t)
0	x	3,x	∞	6,x	6,x	8,x	∞
1	xv	3,x	6,v	6,x	6,x	8,x	7,v
2	xvu	3,x	6,v	6,x	6,x	8,x	7,v
3	xvuw	3,x	6,v	6,x	6,x	8,x	7,v
4	xvuwy	3,x	6,v	6,x	6,x	8,x	7,v
5	xvuwyt	3,x	6,v	6,x	6,x	8,x	7,v
6	xvuwytz	3,x	6,v	6,x	6,x	8,x	7,v

12. There would be 4 fragments generated for 2400 bytes. 20 bytes are reserved for IP header.

ID	Frag Flags	Fragmentation offset
422	1	0
422	1	85
422	1	170
422	0	255