

2016 Network and Communication Examination Solution

1. a. AIMD is fair because it increases the congestion window linearly and reduce by half when packet loss occurs. In this way, applications with higher window will lose more in packet loss. This will result in the share of bandwidth being evenly distributed in the long run.

b. DNS is not necessary for the World Wide Web. It is invented to aid human users to easily remember the address of a server instead of a digit-based IP address. Had DNS never existed, we have to visit everything using IP addresses, which take more efforts to remember.

c. i) A packet filtering router is a router in the network layer with packet filtering software installed to block packets sent from certain server.

ii) A circuit level gateway is a firewall works between application and transport layer that monitors TCP handshaking between packets to determine whether a session is legitimate.

iii) An application level gateway is a security component that enhances a firewall and allows the firewall to look inside packets to determine its type.

d. i) Assume that the data will be sent in n separate different packets. If we choose to use TCP connection, then there will be $9 + 2n$ packets sent since there are 3 packets for the initiation (`SYN` -> `ACK` -> `ACK+1`) and 4 packets for termination of connection (`FIN` -> `ACK` -> `FIN` -> `ACK`). There will also be a request and `ACK` packet for the request, adding up to 9 packets in total. Since each packet will also trigger an `ACK` packet to be sent, there will be $2n$ packets for the data transmission, adding up to $9 + 2n$ packets sent in total.

ii) If UDP is used, then only $1 + n$ packets will be sent since there are no procedure for establishing and destroying a connection. The extra 1 packet is the request message.

e. UDP has a smaller header and does not require establishment of connection, thus is faster for real-time applications like game messaging service or Facetime. However, because it does not guarantee the receiving of packets, it is less reliable and errors might need to be handled in the application layer.

f. i) The maximum number of available TCP packets with non-repeating sequence number is 2^{32} . Hence the maximum value of L is $2^{32} = 4$ GByte. Notice that the sequence number of TCP packet is indicating how many bytes are in the packet, so it's not a packet-labeling number (i.e. we do not multiply the MSS)

ii) Adding the 64 extra bytes, the total number of bytes in a packet is 600. There will be a total number of $\frac{4 \text{ GByte}}{536 \text{ Byte}} = 8,012,998.68 \approx 8,012,999$ packets being sent out. Thus the time it takes to transmit the file is $\frac{8,012,999 \cdot 600 \cdot 8}{50 \times 10^6} \approx 769.25 \text{ seconds} = 12.82 \text{ minutes}$.
2. a. Distance-vector routing is a way in the network layer to find the best/shortest route to send packets from source to destination. It works as Bellman-Ford algorithm and first to find the direct costs of neighbors of each node, and then add the edges with the shortest cost to find the optimal way to send packets.

b. i) Distance vector routing is 1 relatively easy to implement and 2 have less redundancy.

ii) However, it 1 converges slower compared to Link State Routing, and 2 might suffer from count-to-infinity problem and 3 the routing table could be huge if the network grows.

c. $(R4, R3, 1) \Rightarrow (R4, R4, 1)$

$(R5, R3, 7) \Rightarrow (R5, R3, 6)$

d. 2 rounds. The first round would be sensing the direct neighbors of R2, and the second round is used to sense the neighbors of the direct neighbors of R2. (i.e. two layers/depth of 2) In the corrected version in c), the deepest path length is 2. (i.e. $(R5, R3, 6)$)

e. $\{(R1, R1, 2), (R2, R2, 0), (R3, R3, 4), (R4, R4, 1), (R5, R3, 6), (R6, R5, R3, 7), (R7, R6, R4, 13)\}$

f. i) R6 can either 1 send a forged routing table such that the packets will not take the optimal route hence slow down the network, or 2 it can send routing table claimed that it is shorter if packets go through R6, thus is able to monitor the network traffic from all parties. It can also 3 block R7 by never including R7 in its routing table.

ii) R2 can do experiments of sending packets using different routes and measure the RTT or TTL to see if the claimed routing table is indeed correct/valid.