Problem 1: True or False (5 x 4 = 20 points).

Please justify your answer with a 1-2 sentence explanation. No points without proper explanation.

(a) An IP packet from the source to the destination splits into multiple fragments. If any fragment is lost, then only the missing fragment is retransmitted by the IP layer.

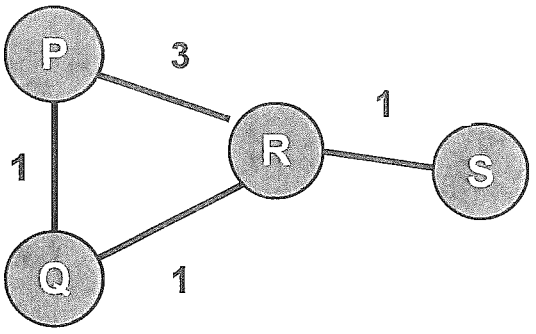
(b) A sliding window protocol with cumulative acknowledgements is used. A receiver has already received and acknowledged packets 1-6. No other packets have been received. If packet 8 is now received, an ACK is sent for packet 8.

(c) Answer the following with respect to the BGP protocol. ISPs A and B share a peering relationship. Further, ISPs B and C share a peering relationship. Then, traffic may be routed from a customer of A to a customer of C by traversing the ISPs in the sequence A-B-C.

(d) A bridge B receives a packet with source MAC address S, and destination MAC address D. Then, bridge B learns/refreshes its table entry for both S and D.

(e) Consider a network where B1, B2,.... B8 denote bridges. We are told that B1 has a lower id than B2, which has a lower id than B3, and so on. At one point, B4 assumes the root is B3, and the cost to the root is 1. It receives a message from directly connected neighbor B6, indicating that B6 thinks the root is B2, and the cost is 4. Then, after processing this message B6 still considers the root to be B3, with cost to the root of 1.

Problem 2: Distance Vector Routing [5 x 4 = 20 points]



Consider the network above. Assume the routers are running a full-fledged distance vector protocol which includes the split horizon rule.

(a) After the system has converged, what is the next hop and cost from P to S?

(b) At some point after the system has converged, link R-S fails. R detects the failure, and updates its cost to S to INFINITY.

(i) Immediately following this, P sends a routing table update to R. What is the next hop and cost from R to S when this update is processed by R?

(ii) Would your answer to b (i) change if split horizon were not used? If so, indicate the new answer. If not, say "Does not change".

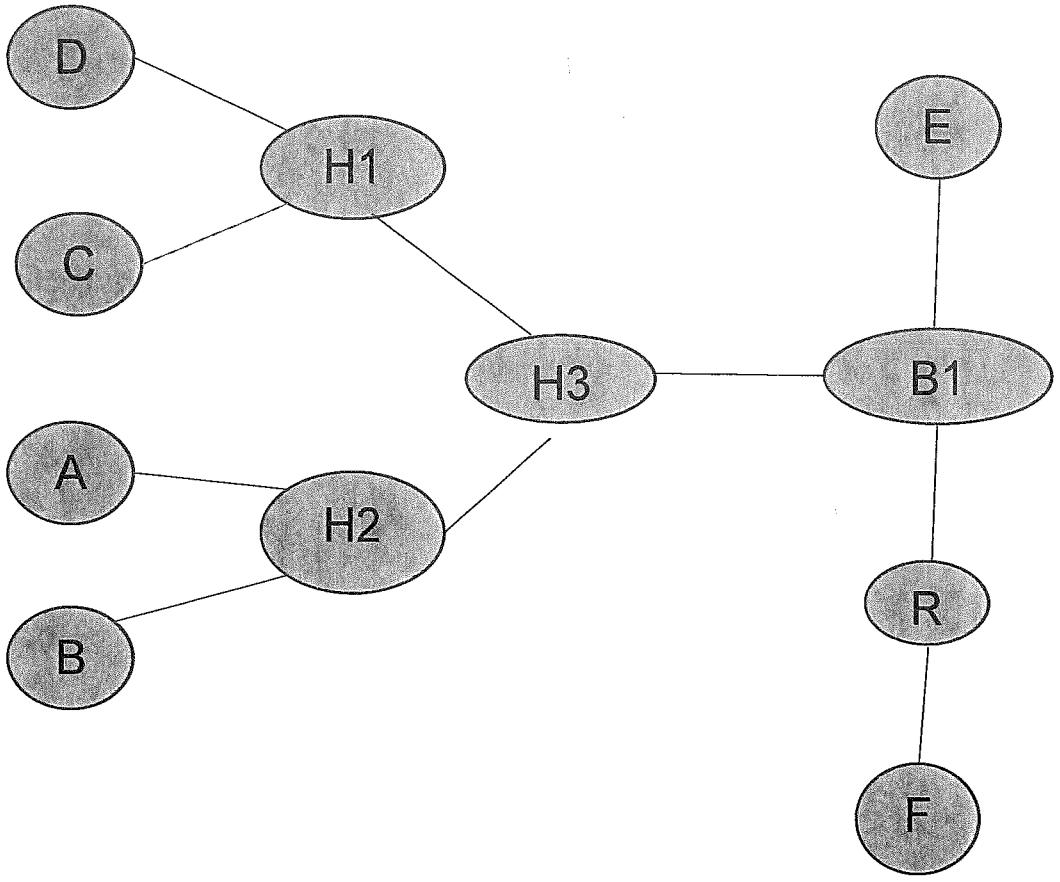
(c) This part is independent of Part (b). At some point after the system has converged, link R-S fails. R detects the failure, and updates its cost to S to INFINITY.

(i) Immediately following this, Q sends a routing table update to R. What is the next hop and cost from R to S when this update is processed by R?

(ii) Would your answer to c (i) change if split horizon were not used? If so, indicate the new answer. If not, say "Does not change".

Write in Exam Book Only

Problem 3: Interconnects [5 x 4 = 20 points]



In the network above, H1,H2, and H3 are hubs, B1 is a bridge, R is a router, all other nodes are end hosts. All bridges have converged after the spanning tree algorithm. Please answer the following questions *[all parts are independent of each other and do not build on each other]*

(a) C is transmitting a large file to D. At the same time, A is transmitting a large file to B. Will the performance of the file transfers be affected by each other? State Yes/No and justify briefly.
(b) Host F is transmitting a broadcast packet. Please list all other hosts that will see the broadcast packet. You may write "None" if you think that is the answer.
(c) Host C is moved to be attached directly to bridge B1. Do either the IP or MAC address of host C (or both) need to be changed? If so, which addresses must be changed and why? If not, why not? Justify clearly in 1-2 lines
(d) Host A sends a packet to Host F. Please list all devices on the path that change the destination MAC address of the packet. If none exist, say none.
(e) Host A sends a packet to Host F. Please list all devices on the path that change the destination IP address of the packet. If none exist, say none.

Problem 4: TCP (24 points)

You are running TCP Reno (which includes fast retransmit and fast recovery) over a 4 Gbps link with one-way propagation delay of 50 ms to transfer an extremely large file (several gigabytes). TCP sends 1 KB packets (1MSS = 1KB). Answer the questions below. In doing so, you may assume (i) 1MB=1024KB; and (ii) the receiver advertised window is extremely high, and is larger than the Congestion Window for the entire problem and at all times. No explanation is needed for any part of the problem.

(a) The CongestionWindow (cwnd) is initialized to 1 KB and the sender enters the slow start phase.

(i) What is the value of cwnd after 6 RTTs? (hint: after 1 RTT, it is 2KB) . Assume no packet losses occur in the first 6 RTTs. (4 points)

(ii) We are told that the first packet loss occurs after 6 RTTs (i.e., during the 7^{th} RTT). Further, the packet loss was detected by duplicate acknowledgements. After the packet loss and all necessary adjustments have been made

(a) What is the value of the Congestion Window? (4 points)

(b) What is the value of the Congestion Threshold? (4 points)

(b) We are told that at the end of 20 RTTs, the Congestion Threshold is 64 KB and we are in the congestion avoidance phase. A packet loss occurs at the end of 25 RTTs. After the packet loss and all necessary adjustments have been made, the Congestion Window is 38 KB.

(i) What is the value of the Congestion Window at the end of 25 RTTs just before the packet loss? (4 points)

(ii) What is the value of the Congestion Window at the end of 20 RTTs? (4 points)

(iii) What is the value of Congestion Threshold at the end of 25 RTTs, after the packet loss and all adjustments have been made? (4 points)

Problem 5: Network Security: (16 pts)

In SSL, there are three entities: a client (C), a server (S), and a certificate authority (A).

Let **Pr(X)** and **Pu(X)** respectively denote the private key and public key of the corresponding entity – e.g., Pr (C) and Pu(C) denote the private and public keys of the client.

Let **r** denote a shared secret between the client and the server generated during the session.

Let $E_K(M)$ denote that message M is encrypted using key K
Let $D_K(M)$ denote that message M is decrypted using key K

Answer each of the questions below *using the notation above in presenting your answers:*

(a) In the first step, a client obtains a certificate from the server.
(i) What key is used to sign the certificate? (3 pts)
(ii)What key does the client learn after receiving and verifying the certificate? (3 pts)

(b) In the next step, a client generates the shared **secret r,** and sends this to the server. Using the notation above, indicate the actual message transmitted to the server. (5 pts)

(c) In the final step, the server sends the data message to the client in encrypted form. Denoting the unencrypted data as M, indicate how this information would be sent from the server to client using the notation above (5 pts).

Write in Exam Book Only