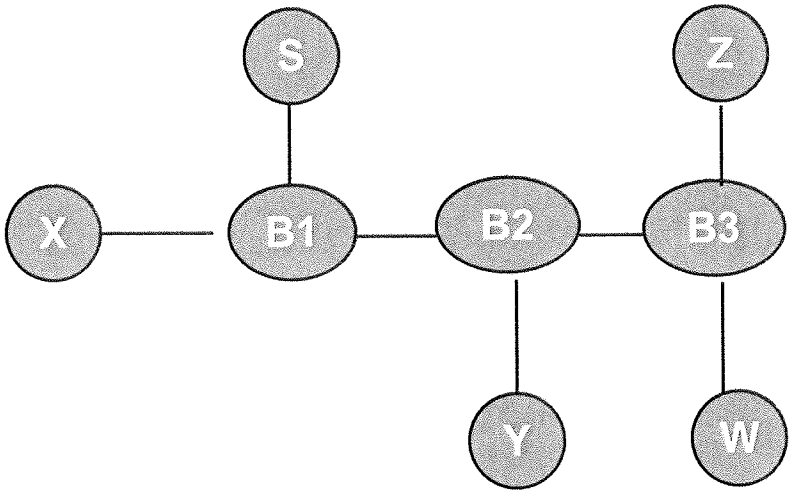
Problem 1: Bridging (18 points)



Consider hosts X,S,Y,Z,W and learning bridges B1, B2, B3 as in the figure. Assume all forwarding tables are empty initially. Please complete the table. Just give the answer, no explanation is needed.

[6 x 3 = 18 points]

Suppose Y sends to W	(a)Which bridges learn/refresh where Y is?
	(b)List all hosts which are neither the source nor destination, whose network interface sees the packet.
Next, Z sends to Y.	(c)Which bridges learn/refresh where Z is?
	(d) List all hosts which are neither the source nor destination, whose network interface sees the packet.
Next, X sends to Z	(e) Which bridges learn/refresh where X is?
	(f) List all hosts which are neither the source nor destination, whose network interface sees the packet.

Write in Exam Book Only

Problem 2: BGP (20 points)

Consider 4 ISPs, AT&T, Sprint, UUNet, and Comcast.

- The following pairs of ISPs are known to share a peering relationship
  - AT&T and Sprint
  - Comcast and Sprint
  - UUNet and Comcast
- In addition, UUNet and Comcast are customers of AT&T.

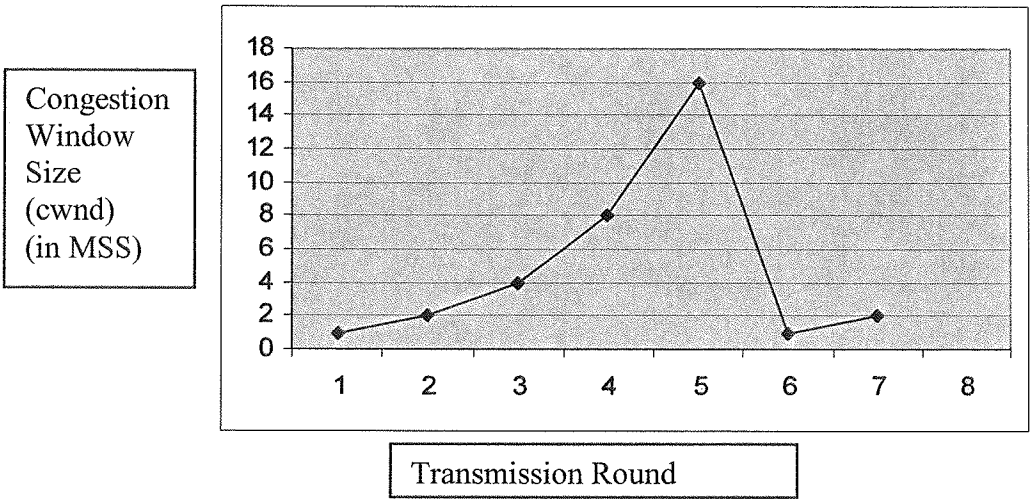
For each of the following paths, say "Yes/No" to indicate whether they are possible or not. If you said "No", briefly explain why. Use the concept of valley free routing for the parts where applicable.

[4 x 5 =20points]

(a) Client - UUNet – Comcast – AT&T – Client
(b) Client - Sprint - AT&T – UUNet – Client
(c) Client - Comcast – Sprint – AT&T – UUNet – Client
(d) Client - AT&T – Comcast – UUNet – Client

Write in Exam Book Only

Problem 3: TCP (24 points)



Consider the following plot of TCP congestion window size as a function of time. The protocol used here is TCP Reno, and includes slowstart, congestion avoidance, and fast retransmit and recovery. The initial period is graphed. Assume that a packet loss occurs at the end of the 5th transmission round as shown. The next packet loss occurs at the end of the 15th transmission round. Note that the congestion window is not graphed from times 8 to 15, but there is sufficient information for you to answer the questions below. No explanation is needed for any part unless explicitly requested.

Answer the following questions pertaining to the graph: [3 + 3 + 3 + 3 + 12]

a) John says CongestionThreshold at time 1 was 8*MSS. Do you think John is right? Briefly justify.

b) Does the packet loss at the end of time 5 correspond to a timeout or a duplicate acknowledgement?

c) What is the value of Congestion Threshold at the end of time 5?

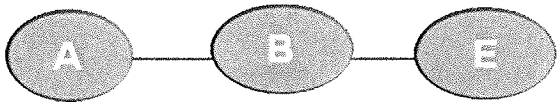
d) In which transmission round would the congestion avoidance phase begin (note this could be in a later transmission round than shown in the graph)?

e) Assume that a loss occurs due to a triple duplicate ACK at the end of transmission round 15.

(i) What were the values of CongestionThreshold and cwnd just before the loss?

(ii) What are the values of CongestionThreshold and cwnd just after the loss?

Problem 4: Routing (26 points)



Consider the network shown in the figure above, in which A,B,E are routers. Assume the routers run a distance vector protocol. Assume that the split horizon rule is not used. All links have cost 1. Suppose the link B-E fails.

[5 + 5 + 8 + 4 + 4]

(a) What is the next hop and cost from B to E (for destination E) before the failure? (No explanation is needed)

(b) What is the next hop and cost from A to E (for destination E) before the failure? (No explanation is needed)

(c) Give a sequence of routing table updates that leads to a routing loop between A and B.

(d) Estimate the probability of a loop forming if B broadcasts an updated report within 5 seconds of discovering the B-E link failure, and A broadcasts every 30 seconds uniformly. Clearly explain and justify your answers – you will not get credit if you simply wrote down the final answer.

(e) Is it possible to see Count to Infinity Problems with Link State Protocols? Explain why.

Write in Exam Book Only

Problem 5: Security:SSL (12 points)

In SSL, there are three entities, a client, a server and a certification authority. Each entity is associated with a public and private key. Answer the following questions:

(a) When a client receives a certificate from a server
  (i) What key should the client use to verify the certificate?
  (ii) How does the client obtain this key?

(b) After receiving the certificate, the client generates a shared key, and sends it to the server. What key is used to encrypt this information?

(c) When the server transmits encrypted data to the client, symmetric key cryptography is used, rather than asymmetric. Why?

Write in Exam Book Only