Problem 1: Short Questions (20 pts)

Part A: State whether each of the following are true or false. Provide a brief and to-the-point explanation in not more than 1-2 sentences. No credit without proper justification. [6 × 2 = 12 pts]

(a) The IP layer guarantees that packets reach a destination with bounded delay. False. IP does not guarantee delivery

(b) It is possible to have packet loss in a circuit switching network. True

(c) AT&T has a peering agreement with each of Sprint and UUnet, but Sprint and UUnet do not have a peering agreement with each other. IBM is a customer of Sprint, and Microsoft is a customer of UUnet. It is possible for a packet sent from IBM to Microsoft to traverse Sprint, AT&T, and UUnet in that order. False

(d) The Random Early Drop (RED) scheme is effective in protecting against malicious participants that transmit at extremely high data rates. False

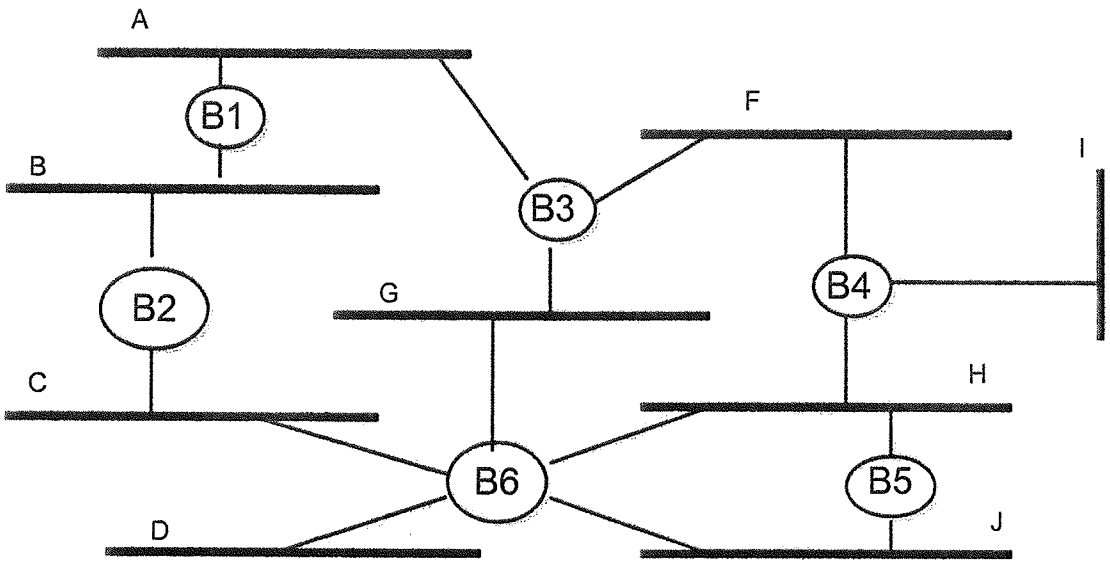
(e) In a Weighted Fair Queuing system, if packet A arrives earlier than packet B, then, packet A always finishes service first. False

(f) In a Weighted Fair Queuing system, if packet A has a smaller virtual finish time than packet B, then it must always finish service before packet B. True

Part B: Some researchers have proposed that the last-hop, or the wireless link between the end-host and its access-point should have explicit mechanisms to enhance reliability. Note that wireless links usually experience much higher loss rates than other wired Internet links. Provide an argument in 2-3 sentences why this could be viewed as consistent with the end-to-end argument. [8 pts] Performance enhancement

Write in Exam Book Only

Problem 2: Bridging (21 pts)



Answer the questions for the network above. Assume that the spanning tree algorithm is used. Assume that B1 has a lower id than B2, which has a lower id than B3, and so on. Use the following notation for a configuration message in the algorithm: a message from node *X* where it claims the root node is *Y* and *X*'s distance from *Y* is *d* hops is given as (*Y*, *d*, *X*).

[2 + 2 + 4 + 9 + 4 pts]

(a) The entire system, including all bridges, is reset at time 0. Who does B6 assume is the root, and what is the cost to the root right when the system is reset (and the spanning tree algorithm begins to run)? (B6, 0, B6)

(b) B5 assumes the root is B4, and the cost to the root is 1. It receives a message from B6, indicating that B6 thinks the root is B3, and the cost is 2. What in B5's opinion is the root, and cost to root at the end of this? (B3, 3)

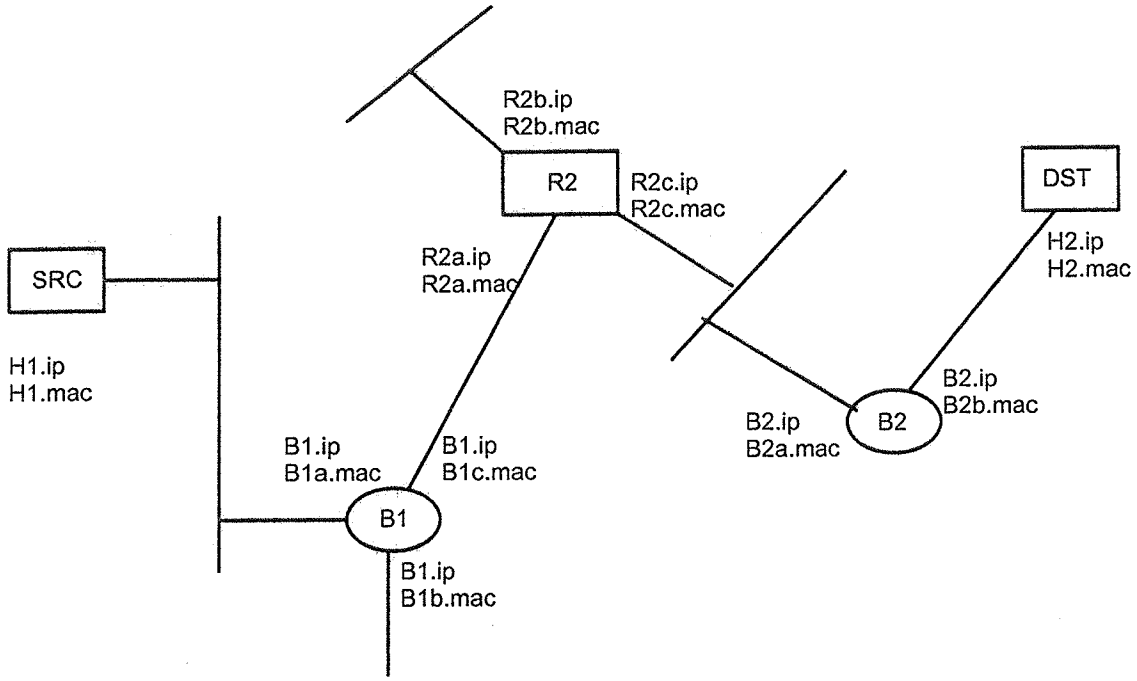
(c) After the system stabilizes, what is the designated bridge of Lan J? B6

Write in Exam Book Only

(d) After the system stabilizes, which links are disabled from the spanning tree? Express your answer as a set of <bridge,LAN> tuples. <B6, G> <B6, H> <B5, J>

(e) After the system stabilizes, if bridge B5 fails, what will happen? Explain your answer. Nothing. B5 has no designated bridge

Problem 3: Interconnects (20 pts)



Above is a picture of a network with 2 bridges (B1 and B2) and 1 router (R2). Each interface is labeled with both an IP address and an MAC address. Imagine that a host (SRC/H1) is sending a packet to another host (DST/H2). Please answer the following questions about this figure:

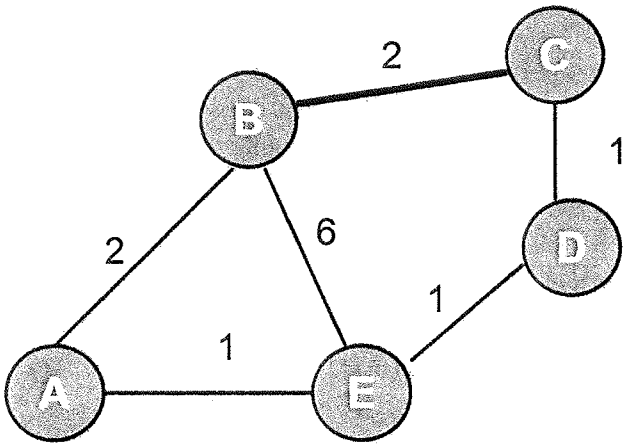
Note that each bridge has 1 IP address, but multiple MAC addresses corresponding to each of its links. Note also that each router has a distinct IP address and MAC address for every link (interface).

[4 × 5 pts]

Write in Exam Book Only

a. Just before the packet reaches bridge B1, what is its layer 2 destination? R2a.mac
b. When H1 sends out an ARP query, what is the reply to that query? R2a.mac
c. Just before the packet reaches bridge B2, what is its layer 2 source? R2c.mac
d. Just after the packet leaves router R2, what is its layer 3 source? H2.ip
e. Does the entry B2a.mac appear in B1's forwarding table? Why/why not? Explain in 1 sentence – no credit without explanation.
No, MAC address is not shared after a router

Problem 4: Multicast (12 pts)



Consider the topology shown above, with each link annotated by its cost. Consider a multicast group G with host E as the source, and all nodes as receivers.

(a) If the Reverse Path Broadcasting strategy is used, indicate all links which are traversed by data belonging to the multicast session.

(b) If the Reverse Path Broadcasting strategy is used, indicate all links which may see multiple copies of the same data packet.

Write in Exam Book Only

Problem 5: TCP (12 pts)

Assume that you are running TCP over a 2 Gbps link with a latency of 100 ms to transfer a 20 MB file. Assume the size of the TCP receive buffer (or TCP receiver window) and that of the TCP send buffer (or TCP send window) are infinite. Further, assume that the CongestionThreshold (ssthresh in 595 class notation) is initialized to infinity. Assume TCP sends 1 KB packets. Finally assume that there is no congestion, and no packets are lost. How many RTTs does the entire transfer take considering that the sender has just established the TCP session for transferring the file? What is the efficiency of the transfer given as a percentage of the raw bandwidth of the link used by the transfer? Please provide clear explanation for your answer, show the steps and justify. 15 RTT,
efficiency=160/(3*1024)

Problem 6: Network Security: (15 pts)

Two youngsters – August and Barbara (yes they got bored with their old names Alice and Bob) – wish to communicate with each other over the internet. Each uses RSA, the common asymmetric cryptography protocol. Thus, each has his/her own private key and knows the public key of the other. Let us denote these as:
Pr(*A*): Private key of August; Pr(*B*): Private key of Barbara
Pu(*A*): Public key of August; Pu(*B*): Public key of Barbara

Answer each of the questions below. *Note that parts (a),(b) and (c) are independent of each other. Further, for parts (a) and (b), please use the following notation in presenting your answers:*
$E_K(M)$: Message *M* is encrypted using key *K*
$D_K(M)$: Message *M* is decrypted using key *K*

[5 × 3 pts]
(a) August wants to send a message to Barbara so that no one else can read it. Let us denote the message as M_1.
  (i) How would he send the message? E_Pu(B)(M_1)
  (ii) Let us denote the message August sent as M_3.
  How would Barbara decipher the message? D_Pr(B)(M_3)
(b) In this situation, August does not care if anyone can read his message. But he does care that no one in the middle can change

Write in Exam Book Only

the message (in an undetectable manner). Let us denote the message as M_2.

(i) How would August send the message? E_Pr(A)(M_2)

(ii) What would Barbara do to verify that the message indeed came from August? E_Pr(A)(M_2)

(c) When August is on the web shopping for some article (may or may not be for Barbara), he goes to a site which claims it is Amazon. The site produces a public key which it says is Amazon's public key. How does August know, or to be more precise how does August's web browser know, that it is indeed the trusted book seller Amazon that is furnishing this public key? *[No need to use notation for this part]* Using the key provided by certification authority

Write in Exam Book Only