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) Every router in a distance vector protocol maintains the full topology of the network.

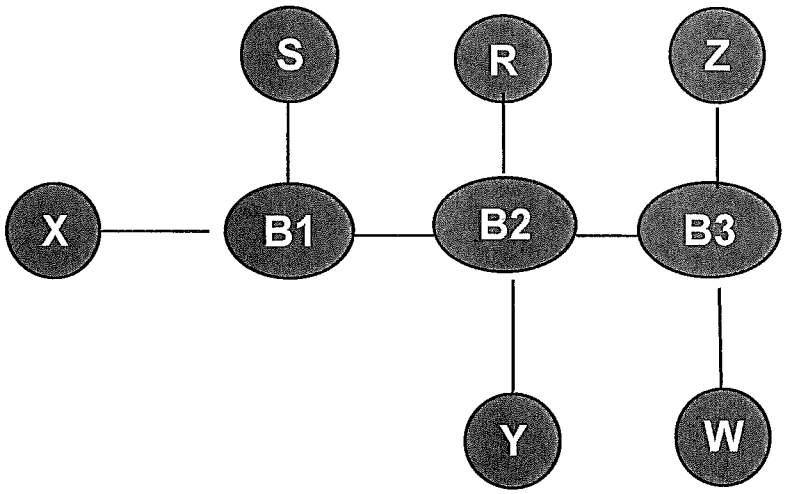
(b) Link state protocols have better convergence properties on failures than distance vector protocols.

(c) A packet traverses a switch S on the path from the original source host to the final destination host. When the packet enters S, it has a source MAC address A, and a destination MAC address B. Then, when the packet exits S, the source MAC address is modified, and no longer A.

(d) 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.

(e) ISPs B and C are customers of ISP A. Further, B1 and C1 are customers of ISPs B and C respectively. Then, it is possible that traffic from B1 to C1 is routed through ISP A.

Problem 2: Bridging (20 points)



Consider hosts R,S, X, Y,Z, W and learning bridges B1, B2, B3 as in the figure. Assume all forwarding tables are empty initially. Please answer the following questions. You may answer "None" for any part if you think that is the appropriate answer for that part.

Suppose Y sends to R	(a)Which bridges learn/refresh where Y is? (2 points)
	(b)List all hosts which are neither the source nor destination, whose network interface sees the packet. (3 points)
Next, R sends to Y.	(c)Which bridges learn/refresh where R is? (2 points)
	(d)List all hosts which are neither the source nor destination, whose network interface sees the packet. (3 points)
Next, X sends to R	(e)Which bridges learn/refresh where X is? (2 points)
	(f)List all hosts which are neither the source nor destination, whose network interface sees the packet. (3 points)
Next, Z sends to X	(g)Which bridges learn/refresh where Z is? (2 points)
	(h)List all hosts which are neither the source nor destination, whose network interface sees the packet. (3 points)

Problem 3: TCP (20 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. What is the value of cwnd after 4 RTTs? (hint: after 1 RTT, it is 2KB) . Assume no packet losses occur in the first 4 RTTs. (4 points)

(b) We are told that a packet loss occurs after 7 RTTs (i.e., during the 8^{th} RTT). Further, the packet loss was detected by a timeout. After the packet loss and all necessary adjustments have been made

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

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

(c) We are told that at the end of 15 RTTs, the Congestion Window is 32 KB, and the Congestion Threshold is 64 KB. If no packet losses occur between the 15^{th} RTT and the 20^{th} RTT.

(i) What is the value of the Congestion Threshold at the end of 20 RTTs? (4 points)

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

Problem 4: DNS (21 points)

Below is a list of domains, and the name servers of those domains.

Domain	Name Server
Root	a.root-servers.net
.edu	A.GTLD-SERVERS.NET
.com	H.COM-SERVERS.NET
.facebook.com	a.ns.facebook.com
.mit.edu	abcd.mit.edu
.rice.edu	netscaler2.rice.edu
.amazon.com	ns.amazon.com
.berkeley.edu	ns.berkeley.edu

PART A. **(6 points)**
The local name server of Purdue University sees a lookup for the host www.facebook.com. Please list all the DNS servers that are contacted by the local name server in the process of resolving this query.
You may assume that

- The local name server begins with an empty cache
- All name servers employ an iterative name resolution process (however the local name server itself resolves host names on behalf of the client).

PART B. **(5 x 3 = 15 points)**
This part continues from Part A. Immediately after the lookup for www.facebook.com in Part A, the local name server of Purdue University sees a series of host names that are being looked up, as indicated in the table below. Each lookup could result in a series of queries to the appropriate DNS servers.

You may assume that:

- The local name server starts off with the cache including all information cached during Part A, and no other information.
- All name servers employ an iterative name resolution process (however the local name server itself resolves host names on behalf of the client).
- The queries below occur in a short interval of time, and cached entries from prior lookup do not timeout.

For each of the hostnames that is looked up, please indicate what is the first DNS server that is contacted by the local name server (*only the first DNS server is needed for this part*)

1. www.rice.edu
2. www.amazon.com
3. www.berkeley.edu
4. ftp.berkeley.edu
5. www.facebook.com

Write in Exam Book Only

Problem 5: Security (19 points)

Jill wishes to electronically transmit an important message M to Jack using public key cryptography. Answer each of the questions below. *Please use the following notation in presenting your answers:*

Jack-Pub, Jack-Pvt:	Public and private keys of Jack
Jill-Pub, Jill-Pvt:	Public and private keys of Jill
E(M,K):	Message M is encrypted (or signed) using key K
H(M):	One way hash or secure digest of message M

(a) Jack wishes to transmit M to Jill in a manner that no one other than Jill can access the data.

(i) What should Jack transmit to Jill assuming we are restricted to public key cryptosystems? *Use the notation above.* (5 points)

(ii)Is the above solution acceptable from a computational efficiency stand-point? State Yes/No. If Yes, explain why in a sentence or two. If No, propose a solution to improve the computational efficiency. (5 points)

(b) Jack does not mind other people viewing the data he sends to Jill. However, he is concerned that a malicious third-party might intercept his message, and send fake data to Jill pretending that he is Jack. What should Jack transmit to Jill to enable her to verify it was Jack who sent the message? Use public key cryptography along with other mechanisms as appropriate. Please ensure the scheme is acceptable from a computational efficiency stand-point. (5 points)

(c) Jack proposes using the following algorithm for the hash function H(M). Specifically, the message M is taken, and the remainder when divided by a large prime number is computed. Is this an acceptable algorithm for H(M)? State Yes/No, and justify your answer briefly in 1-2 lines. (4 points)