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

For each of the following, state whether true or false **and justify briefly. No credit 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.

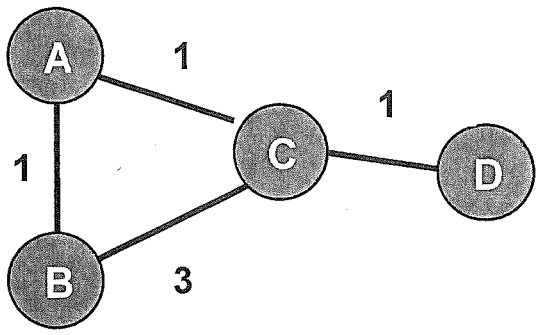
(b) A packet switched network consists of a 1 Mbps link, and 10 total users. Then, each user can at most transmit 100 Kbps at any time.

(c) Jonathan claimed that he designed a new transport protocol (running on top of the IP layer), which could guarantee that any packet sent to that layer would be delivered in a reliable fashion to the receiver, and within 100 milliseconds. It is impossible for Jonathan to have designed such a protocol.

(d) Jacob (a Purdue student) owns a laptop, that he uses at various locations including his off-campus house, Purdue University, and a café. The MAC address associated with the laptop is different at each location.

(e) ISP A has a peering relationship with each of ISP B, and ISP C. However, ISPs B and C do not have a peering relationship with each other. 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: 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 A to D?

(b) At some point after the system has converged, link C-D fails. C detects the failure, and updates its cost to D to INFINITY. Immediately following this, A sends a routing table update to C. What is the next hop and cost from C to D when this update is processed by C ?

(c) This part continues on Part (b). Immediately following the events in Part (b), B sends a routing table update to C. What is the next hop and cost from C to D when this update is processed by C?

(d) Repeat Part (b) if we are told that the split horizon rule is NOT used.

(e) Does use of the split horizon rule guarantee that count to infinity problems will not occur with distance vector protocols? Say Yes/No, and justify in 2-3 lines.

Problem 3: Congestion Control (6 x 4 = 24 points)

Consider the following table which describes the evolution of TCP's congestion window size as a function of time. The table only shows the first 7 rounds, though TCP continues to operate for more rounds, and the questions in Part B pertain to the later rounds. Each round here corresponds to 1 RTT. The protocol used here is TCP Reno and includes slowstart, congestion avoidance, and fast retransmit and recovery.

Start of Round #	Congestion Window (in MSS)
1	1
2	2
3	4
4	8
5	16
6	1
7	2

Part A: Answer the following questions:

a) What are the possible values of Congestion Threshold at the start of Round 1?

b) Clearly, a packet loss occurred during Round 5. Does the packet loss during this round correspond to a timeout or a duplicate acknowledgement? Justify in 1-2 lines.

c) What is the value of Congestion Threshold at the start of Round 6 (after the loss and necessary adjustments)?

Part B: Building on the previous part, assume that TCP continues as per normal operations, and the next packet loss occurs during Round 15.

d) Is TCP ever in the congestion avoidance phase before Round 15? If so, in which rounds? If not, why?

e) What is the Congestion Window at the start of Round 15 (before the loss)?

f) Assume that a loss occurs due to a triple duplicate ACK during Round 15? What are the values of Congestion Threshold and cwnd after the loss is detected, and the necessary adjustments are made?

Problem 4: Ethernet (4 + 4 + 8 = 16 points)

Let A and B be two hosts attempting to transmit on an Ethernet. Let T microseconds be the exponential backoff base unit. Suppose A and B simultaneously attempt to send a frame, resulting in a collision. After this first collision, A and B both back-off for exactly the same amount of time, and their first re-transmission attempt also unfortunately results in collision. A and B are now trying to transmit again after this second collision.

(a) Enumerate the possible backoff times chosen by A after the second collision. Express your answer in multiples of T.

(b) Enumerate the possible backoff times chosen by B after the second collision. Express your answer in multiples of T.

(c)We are told that A and B choose backoff times such that:

(i) A wins after the second collision, i.e. A transmits successfully before B

(ii) There is an idle time of T after the second collision.

Enumerate the possible combinations of backoff times chosen by A and B after the second collision so these conditions are satisfied. Express your answer in multiples of T.

For each possible combination, express your answer as a tuple <X,Y>, where X is the backoff time chosen by A, and Y is the backoff time chosen by B. E.g., <7T, 20T> indicates A chooses 7T and B chooses 20T.

Write in Exam Book Only

Problem 5: Security (5 x 4 = 20 points)

In SSL, there are three entities: client (C), server (S), and Certificate Authority (CA). Please answer the questions below, using the following notations:

Pu(C): Public key of client C
Pr(C): Private key of client C
Pu(S): Public key of server S
Pr(S): Private key of server S
Pu(CA): Public key of Certificate Authority CA
Pr(CA): Private key of Certificate Authority CA

a) When a client contacts the server, it first sends a certificate to the client. Which of the 6 keys listed above is used to sign the information contained in the certificate?

b) Which of the 6 keys listed above does the client learn for the first time when it receives a certificate?

c) Why is data sent from the server to the client encrypted using a symmetric key rather than a public/private key system?

d) To help generate the symmetric key, the client sends the server a secret encrypted with one of the 6 keys listed above. Please indicate which key.

e) How does the client typically learn the public key of the certificate authority (Pu(CA))?

Write in Exam Book Only