CE-5
August 2013 QE

Problem 1: True or False (20 points).
Please justify your answer with a 1-2 sentence explanation. No points without proper explanation.

(a) If any one fragment of an IP datagram is lost, then the entire IP packet is dropped.

True

(b) All packets in a TCP connection must follow exactly the same sequence of routers from the source to the destination.

False

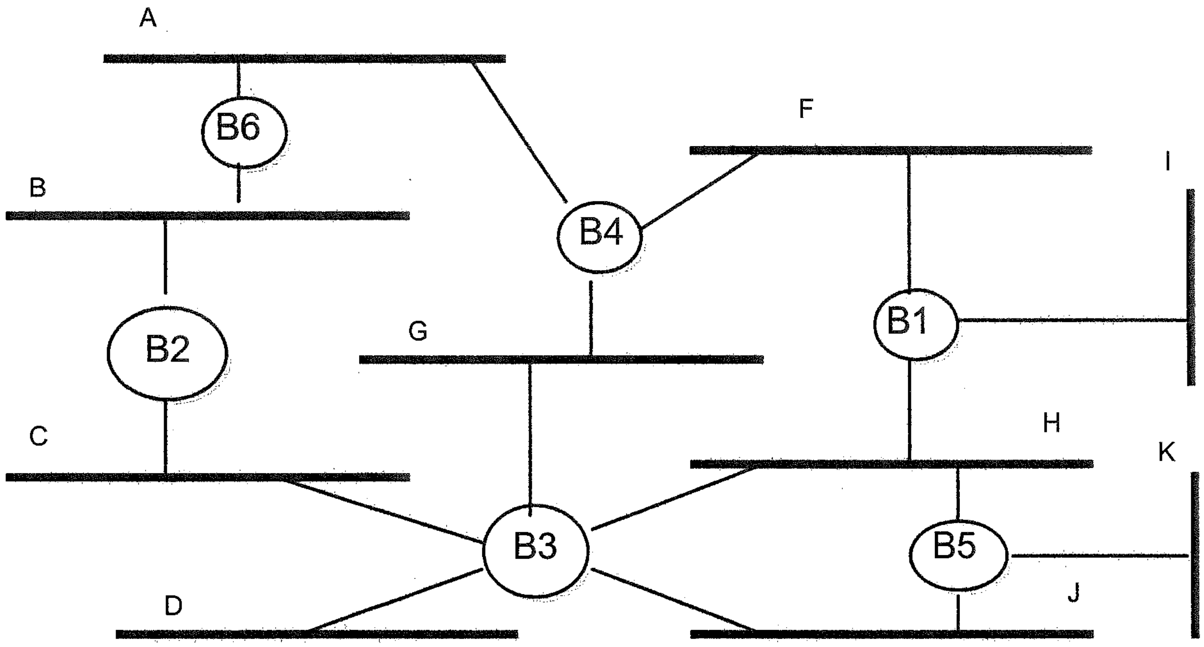
(c) Given a MAC address of a host, the Address Resolution Protocol discovers its IP Address.

False

(d) A sliding window protocol with cumulative acknowledgements is used. A receiver has already received and acknowledged packets 1-3. No other packets have been received. If packet 5 is now received, an ACK is sent for packet 5.

False

Problem 2: Bridging (20 pts)



Consider 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.

We are told that bridge B2 fails at some point, and the spanning tree algorithm is re-run. Please answer the questions about the resulting spanning tree produced **when the protocol has converged after the failure.** No explanation is needed for any part of this problem.

(a) What is the designated bridge of LAN G? (3 points) B3
(b) What is the designated bridge of LAN B? (3 points) B6
(c) What is the designated bridge of LAN J? (3 points) B3
(d) List all links in the topology which are disabled? Express your answer as a set of <bridge,LAN> tuples. Do not include links attached to bridge B2 (8 points) <B4, G> <B5, J>
(e) List all LANs that sees a different path to the root after the failure than before the failure occurred. You may say "None exists" if all LANs have the same path to the root before and after the failure. (3 points) LAN B

Problem 3: TCP (20 pts)

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 3 RTTs? (hint: after 1 RTT, it is 2KB) . Assume no packet losses occur in the first 3 RTTs. 8KB

(b) We are told that a packet loss occurs after 5 RTTs (i.e., during the 6th RTT). Further, the packet loss was detected by duplicate acknowledgements and not a time out. After the packet loss and all necessary adjustments have been made

(i) What is the value of the Congestion Window? 16KB

(ii) What is the value of the Congestion Threshold? 16KB

(c) We are told that at the end of 20 RTTs, the Congestion Window is 128 KB, and the Congestion Threshold is 64 KB. If no packet losses occur between the 20th RTT and the 30th RTT.

(i) What is the value of the Congestion Threshold at the end of 30 RTTs? 64KB

(ii) What is the value of Congestion Window at the end of 30 RTTs? 138KB

.

Problem 4: Addressing (20 points)

The table below is a routing table using Classless Interdomain Routing (CIDR). Address bytes for the subnet number as well as the subnet mask are in hexadecimal notation. Thus, the subnet number 128.46.101.0 is represented as 80.2E.65.0 and the subnet mask 255.255.255.0 is represented as FF.FF.FF.0.

Subnet Number	Subnet Mask	Next Hop
D5.3F.0.0	FF.FF.00.00	A
D5.3F.E4.0	FF.FF.FF.00	B
D5.30.0.0	FF.F0.00.00	C
D5.3F.E0.0	FF.FF.F0.00	D
Default	—	E

State to what next hop a packet for the following destination IP addresses will be delivered. No explanation is needed for any part of this problem. [5 x 4 = 20 points]

(a) D5.3E.F4.BC C
(b) D3.5E.F4.34 E
(c) D5.5B.4F.2E E
(d) D5.3F.EE.85 D
(e) D5.3F.D4.92 A

Problem 5: Security (20 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) Jill wishes to transmit M to Jack in a manner that no one other than Jack can access the data.

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

E(M, Jack-Pub)

(ii) When large messages must be encrypted, symmetric key cryptography is usually preferred to public key cryptography. Explain why in 1 or 2 lines.

Symmetric key is faster in terms of encryption and decryption than public key

(b) Jill does not mind other people viewing the data she sends Jack. However, she is concerned that Dr. Evil might intercept her message, and send fake data to Jack pretending that he is Jill.

(i)What should Jill transmit to Jack, to enable Jack to verify that it was indeed Jill who sent the message. *Use the notation above. Do not worry about computational efficiency concerns.*

E(M, Jill-Pvt)

(ii)If computational efficiency is a concern, what should Jill transmit to Jack to enable him to verify it was Jill who sent the message? Use public key cryptography along with other mechanisms as appropriate.

M || E(H(M), Jill-Pvt)