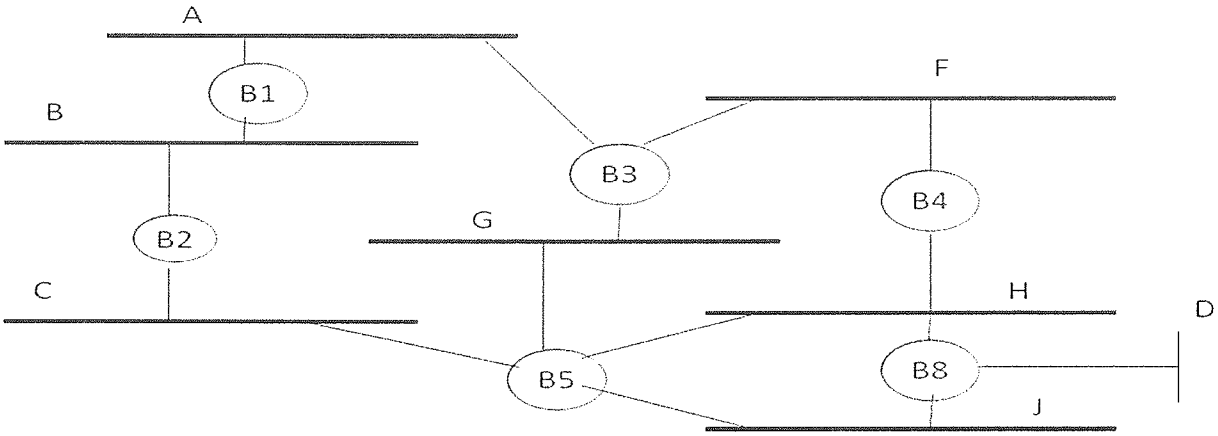
Problem 1: Bridging (22 points)

No explanation is needed for any part in this problem. Just provide the answer.

Consider the network given below. A,B,C,D,F,G,H and J are LANs. B1, B2, B3, B4, B5 and B8 are LAN bridges. We are using the spanning tree algorithm to compute routes to the different LANs.



(a) Indicate the designated bridge for each LAN below [5x2=10 pts]

(i) LAN C B2
(ii) LAN F B3
(iii) LAN G B3
(iv) LAN H B4
(v) LAN J B5

(b) Enumerate all links that are deactivated by the spanning tree algorithm. Each deactivated link must be indicated as a <bridge,LAN> pair, which implies that the bridge attached to that LAN has its port attached to that LAN deactivated. [12 points]

<B5, G>
<B5, H>
<B8, J>

Write in Exam Book Only

Problem 2: Network Performance (24 points)

Assume that a link with bandwidth *B bytes per second* is set up between the sender and the receiver. The distance between the sender and receiver is approximately *L meters*. Data travels over the link at the speed of light – *S m/s*. The sender is sending data of *M bytes*, split into packets, each of size *P* bytes to the receiver. After each packet is sent, the sender waits for an acknowledgement before sending the next packet. The size of the acknowledgement can be neglected.

Pay attention to units. Express all your answer in seconds. No explanation is needed for any part in this problem. Just provide the answer. [6 X 4 =24 points]

(i) What is the one-way propagation delay of the link? Express your answers in terms of **B, L, S, M, P**. Likely you will only need to use a subset of these parameters. Denote the answer to this part as **T1**. **[4 points]** L/S

(ii) What is the transmission time of a packet by the sender, for any given transmission attempt? That is, how long does it take from when a sender starts transmitting a packet to when it finishes transmitting? Express your answers in terms of **B, L, S, M, P**. Again, it is likely that you will only need to use a subset of these parameters. Denote the answer to this part as **T2**. P/B

(iii) How long does it take from when the sender begins transmitting a packet to when the packet is completely received at the receiver? Note that we are only talking about a single packet here. Express your answer in terms of **T1** and **T2**. T1 + T2

(iv) How long does it take from when the sender begins transmitting a packet to when an acknowledgement for that packet is received at the sender? Note that we are only talking about a single packet here. Express your answer in terms of **T1** and **T2**. Denote the answer to this part as **T4**. 2*T1 + T2

(v) If a sender does not receive an acknowledgement for a transmitted packet, it must retransmit the packet. Is it advisable to choose a timeout value of T4/2? Justify in 1-2 lines. No, Ack will never be received before timeout

(vi) How long does it take from when the sender begins transmission, to when the complete data is received at the receiver, and an acknowledgement for all packets including the last packet is received at the sender? Assume that each packet is successfully transmitted in

its first attempt. Express your answers in terms of T4, B, L, S, M, P, using only parameters that are relevant. (M/P)*T4

Problem 3: Addressing (16 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
C4.5E.40.0	FF.FF.F0.00	A
C4.5E.4F.0	FF.FF.FF.00	B
C4.50.0.0	FF.F0.00.00	C
C4.5E.0.0	FF.FF.00.00	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. [4 x 4 = 16 points]

(a) C4.5E.4.1 D
(b) C4.5E.4E.23 A
(c) C4.5B.4F.2E C
(d) C4.5E.FF.85 D

Write in Exam Book Only

Problem 4: TCP Reliability (16 points)

Consider a TCP connection where a sender is transmitting a large file which is several gigabytes long to the receiver. At a particular time snapshot, the TCP layer at the receiver end has received bytes 0-2999 of the file, and the appropriate acknowledgments have reached the sender.

Answer the questions below to indicate the action that must be taken when a packet with a given byte range arrives. The first row has been completed to illustrate this. No explanation is needed for any part of this problem.

The following assumptions may be made:

- A cumulative acknowledgment scheme is used.
- The TCP receiver socket buffer is extremely large, and any data that arrives always fits in the buffer.
- The questions build on top of each other, e.g., when answering part (c), you must assume packets in parts (a) and (b) have arrived.

Assume that a packet arrives containing bytes in the file with the byte range indicated below	What data (if any) may now be forwarded to the application for the first time as a result of the arrival of this packet? If none, say "None". Express your answer as a byte range in the original file.	Which byte of data is acknowledged in the ACK? Assume that each ACK contains the largest byte of data that the receiver must acknowledge. Write "None" if no acknowledgment is sent.
(a)First, packet with Bytes 3000-3999	(i)3000-3999	(i)3999
(b) Next, packet with Bytes 5000-5999	(i) None	(ii) 3999
(c) Next, packet with Bytes 2000-2999	(i) None	(ii) 3999
(d)Next, packet with Bytes 6000-6999	(i) None	(ii) 3999
(e)Next, Packets with Bytes 4000-4999	(i) 4000-6999	(ii) 6999

Write in Exam Book Only

Problem 5: Network Security (22 points)

A. For an encryption algorithm (such as RSA), is it important to keep the algorithm secret, the key secret, or both? (2 points) Key secret, algorithm public

B. Adam and Eve are in the mood to communicate, albeit electronically. Even in those early days, RSA cryptography and MD5 hashing schemes have been developed. Adam has a private key denoted as $K_{Pr,Adam}$ and a public key denoted as $K_{Pu,Adam}$. Similarly, Eve has a private key $K_{Pr,Eve}$ and a public key $K_{Pu,Eve}$.

The following notation is used in this problem:
E(m, k) denotes message m is encrypted with key k.
S(m, k) denotes message m is signed with key k.
D(m, k), denotes that a message m is decrypted with key k.
MD5(m), denotes the result when the MD5 hash is applied on message m.

For each of the parts, fill in the blanks with the appropriate answer to correctly complete the statements made in that part. [4 + 4 + 8 + 4]

(i) Adam wants to send a message M so that Eve can read it and no one else can. Then, he must send the message M_{sent} = E(M, _____) K_Pu,Eve

(ii) Adam wants to sign a message M so that Eve can verify that Adam has sent it. Then, Adam generates a signature of message M as M_{sign} = S (M, _____) K_Pr,Adam

(iii) Instead of signing on the entire message M (as in part (ii) above), Adam wants to be more efficient and combine MD5 hashing with public key cryptography. He should then generate a signature M_{sign} = S (_____ , _____) MD5(M), K_Pr,Adam

(iv) Eve receives message M from Adam which has been signed as in part (iii). The key that Eve needs to verify the signature is _____. K_Pu,Adam

Write in Exam Book Only