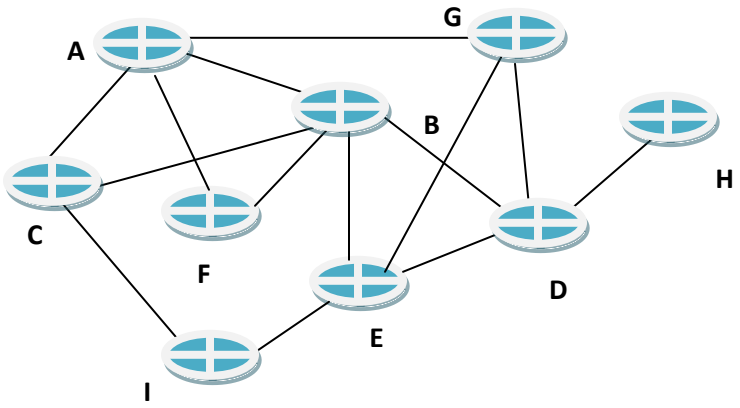
COMP 445 - Fall 2015
Theory Assignment 3

1) What is the main difference between *Pure Aloha* and *Slotted Aloha*? Are there any circumstances where Pure Aloha would perform better than Slotted Aloha? If so, give such circumstances/conditions. If no, explain why Pure Aloha could never perform better that Slotted Aloha.

2) Given a network with 9 routers as shown in the figure below. Assume the utilization of *center-based* spanning tree construction, where router D is assigned as the *center* (or *root*) router. Assume routers join the tree in the following order: C, A, H, B, F, G, E, and I. Show the final constructed spanning tree for that given network.



3) Consider two substitution ciphers. One adds a value of i to the ASCII code of the plaintext character. The other adds a value of j to the plaintext character. All additions are modulo 256. Now consider a double-encryption method that adds i to each plaintext character and then adds j to the resulting ciphertext character to get another ciphertext character. Again, all calculations are modulo 256 How much more secure is this double encryption when compared with either single-encryption method? Explain your answer.

4) Consider the bit string 00101101010100001111111010011101 and the key 10110. Use the key to encrypt and then decrypt the string using bit level ciphering.

5) Suppose you were trying to crack an encryption method that used a 64-bit key. Assuming a brute force attack, how many keys per second must you try to crack the code in 30 days?

6) Three broad classes to multiple access techniques exist, which are: channel partitioning, random access and taking turns. In general, it is assumed that any network would use one of these techniques or the other. However, *cable Internet access networks* utilize all three techniques. Describe how this is done by such networks, and explain how the utilization of any of these techniques does not conflict with the utilization of the other two.

7) In general, fully-connected topology is exhaustive and very unlikely to be used for the construction of a network.
    a. Are there any clear and significant advantages of such topology? Explain clearly.
    b. Explain why it is unlikely that such topology be used for network construction. You should clearly indicate the major disadvantages of such topology.
    c. While this topology seems to make little sense for the construction of networks, in the general terms, it is actually used as part of *Data Centers* to connect Tier-1 and Tier-2 switches. Explain clearly the major advantages of such utilization in data centers. You should provide some example that shows, through some numerical values, the obvious advantages of such utilization.

8) Assume the utilization of Hamming Codes for single-bit error correction.
    a. What is the total number of bits that need to be transmitted if the original data string has 11 bits? Which positions will be covered by the different parity bits?
    b. What is the total number of bits that need to be transmitted if the original data string has 19 bits? Which positions will be covered by the different parity bits?

9) Token Ring LANs have the clear advantage of avoiding collisions, which is surely not the case for networks, i.e. Ethernet, that use buses as the main segment to connect the different devices. In spite of that, Ethernet LANs are capable today of providing a superior performance in comparison to Token Ring LANs. Explain how the Ethernet was able to achieve that regardless of the collision issues. In particular, your answer should consider: 1) the disadvantages of Token Rings, and 2) Switched Ethernet.