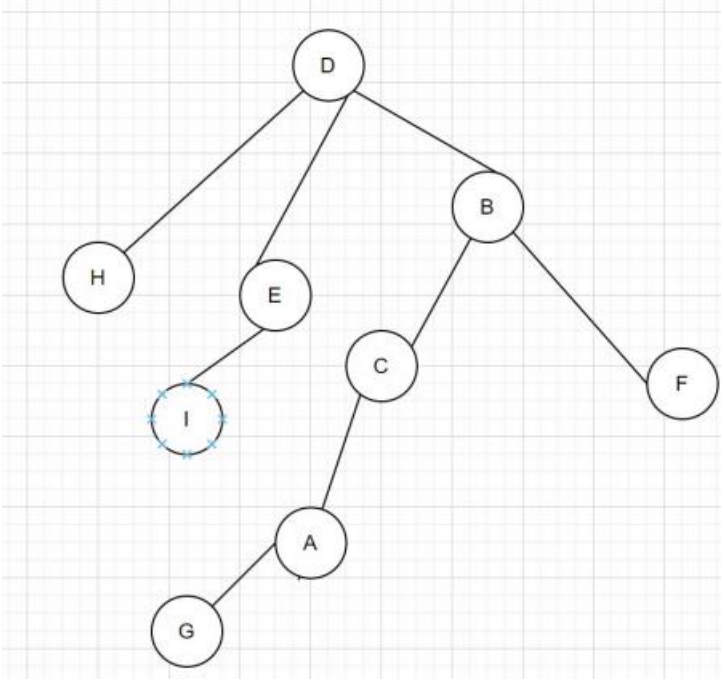
COMP 6461 Theory Assignment 3

Mrinal Rai – 40193024

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.

In pure aloha it allows users to send data whenever they want. Sender waits to see if a collision is occurred or not. If a collision is occurred then they will wait for a particular amount of time. In this system multiple users will be sharing a common communication channel. In slotted aloha is an improvement of pure Aloha as the chance of collision in pure Aloha is very high. In this the channel is divided into several discrete intervals which are known as slots. If a sender is not able to place the frame onto the beginning of the slot, then the sender has to wait until the next time slot. In realistic scenario in pure aloha lot of collisions can occur as anyone can send at anytime and chances of collisions are high. Whereas slotted aloha has keeps minimal time window of 2T which is estimated RTT of the message therefore the chances of collisions reduces and hence performance is imporoved.

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.

Double encryption method is more secure than single encryption method as it is sometimes easy to figure out pattern of cipher in single encryption scheme through statistical methods and analysing pattern of encryption. With double encryption method it is not easy to decipher as there are two layers of encryption and attacker must decode both the patterns which may seem to be difficult.

4. Consider the bit string 00101101010100001111101001101 and the key 10011. Use the key to encrypt and then decrypt the string using bit level ciphering.

Splitting the string into the size of keys: 00101 10101 01000 01111 11010 01101

Chunk	Key	Encryption
00101	10011	10110
10101	10011	00110
01000	10011	11011
01111	10011	11100
11010	10011	01001
01101	10011	11110

Encrypted string: 10110 00110 11011 11100 01001 11110

Chunk	Key	Decryption
10110	10011	00101
00110	10011	10101
11011	10011	01000
11100	10011	01111
01001	10011	11010
11110	10011	01101

Decrypted string: 00101 10101 01000 01111 11010 01101

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?

In a day there 86400 seconds so in 30 days there are 2592000 seconds. With 64-bit key there are 264 combinations possible. Therefore, per second we need to try 264 / 2592000 keys per second which is roughly 7 * 1012 keys per second.

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.

Cable access network uses FDM to divide the downstream (CMTS to modem) and upstream (modem to CMTS) network segments into multiple frequency channels. Frames transmitted on the downstream channel by the CMTS are received by all cable modems receiving that channel; since there is just a single CMTS transmitting into the downstream channel, however, there is no multiple access problem. The upstream direction, however, is more interesting and technically challenging, since multiple cable modems share the same upstream channel (frequency) to the CMTS, and thus collisions can potentially

occur. each upstream channel is divided into intervals of time (TDM-like), each containing a sequence of mini-slots during which cable modems can transmit to the CMTS. The CMTS explicitly grants permission to individual cable modems to transmit during specific mini-slots. The CMTS accomplishes this by sending a control message known as a MAP message on a downstream channel to specify which cable modem (with data to send) can transmit during which mini-slot for the interval of time specified in the control message. Since mini-slots are explicitly allocated to cable modems, the CMTS can ensure there are no colliding transmissions during a mini-slot. These mini-slot request frames are transmitted in a random-access manner and so may collide with each other. A cable modem can neither sense whether the upstream channel is busy nor detect collisions. Instead, the cable modem infers that its mini-slot-request frame experienced a collision if it does not receive a response to the requested allocation in the next downstream control message. When a collision is inferred, a cable modem uses binary exponential backoff to defer the retransmission of its mini-slot-request frame to a future time slot. When there is little traffic on the upstream channel, a cable modem may actually transmit data frames during slots nominally assigned for mini-slot-request frames (and thus avoid having to wait for a mini-slot assignment).

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.

The connection is very quick between any two nodes. The topology is very reliable as the failure of any line does not affect another link. The control among nodes is distributed. Each node does not require routing capability.

b. Explain why it is unlikely that such topology be used for network construction. You should clearly indicate the major disadvantages of such topology.

It is a very costly topology as if there are n nodes in the network, each node requires (n – 1) lines/links resulting in a total requirement of n((n−1)/2) links. If a new node is joined to the network, the cost raises multiple times depending on the total existing nodes and that number of lines are required.

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.

Assume each 10 hosts in rack 1 send to the 10 hosts of rack 5 similarly assume hosts in rack 2, 3 and 4 send to 6, 7 and 8 respectively, so there is 40 simultaneous flows through links A-B and B-C each of these 4 flows will receive 10G/40 = 250 Mbps, which is much less than the 1Gbps within the same rack. The problem become more acute for flows between hosts that need to travel higher up the hierarchy supporting high-bandwidth for host-to-host communication is important Now use fully connected topology Now, there are 4 distinct paths between A and C, providing an aggregate capacity of 40 Gbps, such design not only alleviates the host-to-host capacity limitations but also allows communication between hosts in any two racks, not connected to the same switch, to be logically equivalent, irrespective of their location in the data center

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?

Total number of bits to send is 15 bits.

Positions covered by different parity bits:

Parity 1: (1,3,5,7,9,11,13,15)

Parity 2: (2,3,6,7,10,11,14,15)

Parity 4: (4,5,6,7,12,13,14,15)

Parity 8: (8,9,10,11,12,13,14,15)

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?

Total number of bits to send is 24 bits.

Positions covered by different parity bits:

Parity 1: (1,3,5,7,9,11,13,15,17,19,21,23)

Parity 2: (2,3,6,7,10,11,14,15,18,19,22,23)

Parity 4: (4,5,6,7,12,13,14,15,20,21,22,23)

Parity 8: (8,9,10,11,12,13,14,15,24)

Parity 16: (16,17,18,19,20,21,22,23,24)

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.

Token ring network has certain disadvantages where the device having the token might fail and render the whole network useless as there is no token in the system. The size of ring matters as it might take time to reach to recipient in circular manner. The recipient node can also go down and the token might keep circulating whereas in ethernet bus topology there is no such issues and the collision problem in bus topology can be solved using switches because switch ports lead to different collision domains, and each device is connected to a separate port, there is no more collision anywhere.