Assignment 2

Name:Hongzhi Fu

1.1)

	Distance to B						Set P
n	A	B	C	D	E	F	
1	∞	0	∞	∞	∞	∞	{B}
2	6	--	3	∞	∞	8	{B, C}
3	6	--	--	7	5	8	{B, C, E}
4	6	--	--	7	--	7	{B, C, E, A}
5	--	--	--	7	--	7	{B, C, E, A, D}
6	--	--	--	--	--	7	{B, C, E, A, D, F}

2) Based on the table above, the shortest path from node B to node F is 7.

2.

Organization	Starting Address	Ending Address	Number of Addresses Allocated	Mask
A	159.27.0.0	159.27.7.255	2048	255.255.248.0/21
B	159.27.8.0	159.27.15.255	2048	255.255.248.0/21
C	159.27.16.0	159.27.19.255	1024	255.255.252.0/22
D	159.27.32.0	159.27.47.255	4096	255.255.240.0/20

3.

Application	**Bandwidth**	**Delay**	**Jitter**	**Loss**
Download Music	Medium	Low	Low	Medium
Instant Messaging	Low	High	Low	Medium
Online Card Game	Low	High	High	Medium
Skype(Voice) Call	Low	High	High	Low

4.

Segmentation is the process that chops data stream into several consecutive smaller segments, which is then encapsulated into IP packets. For different size of segments the transport layer choose will have a significant impact on efficiency and reliability of transmission.

For larger segments, the benefits lie in two aspects. One is to save resources on both source and destination hosts to segment larger segments into small pieces, and then

reassembly them together. On the other hand, we do not take too much the ordering of the different segments into consideration, because of relatively smaller number of segments to be reordered to guarantee reliability.

In terms of packet loss that needs retransmission, it is the smaller segments that has a distinctive advantage. Compared with the larger segment, which needs to retransmit the entire large segment, segment with the smaller size cost less to maintain stability and reliability of transmission. Besides, small-sized segments can reduce the pressure of network layer, because network layer do not need to further segment those packets.

5.

If R_A is removed from Alice, when Alice received a response from Bob, Alice cannot convince herself that the message is sent from Bob. Because only Bob owns private key to decrypt the message that Alice encrypts, there is no other people(intruders) that know what Alice transmits. Therefore, Bob can send back R_A to authenticate his identity to Alice, so Alice has confidence to use the shared key to communicate with Bob. Suppose we have a situation where there is an intruder who replays what Alice does to Bob without R_A, instead of sending the shared key back to original Alice, Bob may be misdirected by the intruder to send shared key to him. Thus, this protocol cannot guarantee the security of both sides.