Homework #3-7

5,14,- a) Host A will check sequence number of both SYN packets. If 2nd packet is retransmitted of the original packet then its sequence number will be the same as the first.

b) Begin
If (sport is unwilling to accept new connection)
Then send RST // Reset
Else if (there is no entry like (caddress, cport, sport) in the table). // New connection
Put this entry into the table;
Set cISN to the ISN of the received packet of the client
set sISN to own ISN
Send ACK to the client (caddress, cport)
Record the connection
Else if (there is already entry like (caddress, cport, sport) in the table)
If (ISN in the packet is the same as cISN of the entry)
Do nothing // Duplicate SYN has arrived
Else
Send RST to the client (caddress, cport)
End.

5,19,- a) Step 1: Host C initiates a TCP connection with host A. It gets host A's ISN, after 3 way handshake. ISN is based on a clocks value at the time of a connection

Step 2: Host C masquerades as B and sends SYN packet to A. In response to this SYN packet, A sends his SYN+ACK message to B which contains ISN_2. The underlying assumption over here is that the B will not give reply to SYN+ACK packet A is tricked into presenting to it

Step 3: Host C has ISN_1 with it from the previous connection with the host A, It makes a guess of ISN_2 by adding some value to ISN_1. It can just add the time elapsed since it got the ISN_1 from the host A which can be a good guess as A generates ISN on the basis of clocks value. Now, host C again masquerades as host B and sends a packet with ACK of ISN_2 to host A along with some arbitrary data