Computer Networks - HW5

Ans:- Network Layer - I

a)

Subnet Id	Subnet Mask
130.31.160.0	/19
134.40.0.0	/20
129.66.128.0	/18
134.40.144.0	/20
133.41.0.0	/17

There are 5 different subnets in this inter-network.

b) Host H1 (134.40.12.125) can be placed in network A.
Host H2 (134.40.145.100) can be placed in network D.

Proof: For H1: 10000110.00101000.00001100.01111101
A subnet: 10000110.00101000.00000000.00000000
these 20 bits (subnet bits match)

For H2: 10000110.00101000.10010001.01100100
D subnet: 10000110.00101000.10010000.00000000
these 20 bits (subnet bits match)

c)

Destination Address	Next Hop Address
134.40.0.0 /20	134.40.14.33 /20
134.40.144.0/20	134.40.145.2 /20
129.66.128.0/18	129.66.161.3 /18
130.31.160.0 /19	134.40.14.33 /20
133.41.0.0/17	134.40.145.2 /20

Ans2- Network Layer - II

Link	Src. MAC	Dst. MAC	Src. IP	Dst IP	Src. Port	Dst. Port	Type
1	P1E0	R1E0	10.0.1.11	50.1.2.4	2000	80	TCP SYN
2	R1E1	R2E0	30.1.2.3	50.1.2.4	3333	80	TCP SYN
3	R2E1	P2E0	30.1.2.3	50.1.2.4	3333	80	TCP SYN
4	P2E0	R2E1	50.1.2.4	30.1.2.3	80	3333	TCP SYN ACK
5	R2E0	R1E1	50.1.2.4	30.1.2.3	80	3333	TCP SYN ACK
6	R1E0	P1E0	50.1.2.4	10.0.1.11	80	2000	TCP SYN ACK

Ans3- Transport Layer - I

a)

Estimated RTT = $(1-\alpha)$ Estimated RTT + (α) Sample RTT

Given : Starting value of Estimated RTT = 0

$\alpha = 0.2$

Calculation :

1st Estimated RTT = $(1-\alpha)$ Estimated RTT + (α) Sample RTT

$= [(1-0.2) \times 0] + [0.2 \times 55]$

$= 11.0$ ms

2nd Estimated RTT = $(1-\alpha)$ Estimated RTT + (α) Sample RTT

$= [(1-0.2) \times 11] + [0.2 \times 60]$

$= 8.8 + 12$

$= 20.8$ ms

3rd Estimated RTT = $(1-\alpha)$ Estimated RTT + (α) Sample RTT

$= [(1-0.2) \times 20.8] + (0.2 \times 50)$

$= [0.8 \times 20.8] + 10$

$= 16.64 + 10$

$= 26.64$ ms

4^{th} Estimated RTT = $(1-\alpha)$ Estimated RTT + (α) Sample RTT

$= [(1-0.2) \times 26.64] + (0.2 \times 45)$

$= (0.8 \times 26.64) + (9)$

$= 21.312 + 9$

$= 30.312$ ms

Therefore, latest RTT = 30.312 ms

b) To uniquely identify a UDP Socket, [destination IP address and destination port number] are needed.

To uniquely identify a TCP Socket, [Source IP address, Source port number, destination IP address and destination port number] are needed.

c) i) Sequence number of the 2^{nd} segment = 120
Sequence number of the 3^{rd} segment = 130

ii) ACK number for the first delivered packet that Host B sends to host A is 120. Since the second packet is undelivered, for the third packet, again an ACK of 120 is sent from Host B to Host A. Therefore, in total, there will be 2 acknowlegements of 120 sent from Host B to Host A.

iii) If TCP reliability algorithm is using selective acknowlegements (ie. TCP SACK), then Host B will send acknowlegements for packets successfully received ie. ACK 120 for packet 1 and ACK 180 for packet 3

d)

	Advantage of Connection Oriented Service	Advantage of Connectionless Service
i)	Sequencing of data packets is guaranteed.	It is simple and has less overhead and does not require circuit setup time

	Disadvantage of Connection Oriented Service	Disadvantage of Connectionless Service
i)	Less speed of connection due to the time taken for establishing and relinquishing the connection.	It is not a reliable connection and is prone to network Congestions

Ans 4-

i) Phase 1: Slow Start Phase
Phase 2: Congestion Avoidance Phase

ii) Region to the right of line 2 is the slow start is the Slow Start phase. Throughput in this region makes a sharp decline because this stage is reached after timeout happens in the congestion avoidance phase and hence, the MSS (Maximum Segment Size) is set to 1.

iii) Slow Start Threshold is used to detect the placement of Line 1.

The congestion window size at which timeout happens triggers the placement of Line 2.

b)

i) Segment loss is detected by a triple duplicate Ack since the congestion window size is reduced by half.

ii) Segment loss after 7th transmission round is detected by a timeout since congestion window size is reduced to 1.

iii) Value of threshold at the 18th transmission round is approximately 18 segments.

iv) At the first transmission round (when the network is just established), ssthreshold is set to half the value at which the 1st timeout occurs

c) If we ignore that there any retransmissions ie. packet loss, we assume that there is no timeout. Hence, packets are transmitted in multiples of 2. This forms a Geometric Progression with terms:

1, 2, 4, 8, 16, ____, n terms

Sum, $200 \leq \frac{a(r^n - 1)}{r - 1}$

$\Rightarrow 200 \leq \frac{1(2^n - 1)}{1} \Rightarrow 201 \leq 2^n \Rightarrow n = 8$

Hence, 200th packet is sent in the 8th round.

Ans5- SECURITY

a) Given : $p = 17$, $q = 19$, $e = 5$
Plain text message, $m = 10$

To find : ciphertext c

Solution : $c = m^e \pmod n$
where $n = p \times q$, $e = 5$ and $m = 10$

$n = p \times q = 17 \times 19 = 323$

Therefore, $c = 10^5 \% 323$
$c = 193$

b) We have, $c = m^e \% n$
Now, if $e = 1$ is chosen, then $c = m$ if $m < n$
Therefore, cipher will be the same as original message. This defeats the purpose of creating a cipher in the first place.

c) Advantage of public key design over symmetric key design is that there is increased security. Public key design provides a method for digital signatures.

Disadvantage of public key design is that the speed of encryption is slow.