Tutorial 2 Solutions

Question 1.

(a) The total number of packets is 1 MByte/100 Bytes = 10,000. For each of the 10,000 packets, the receiver will generate exactly one ACK. Go-back-N uses cumulative Acks, so it will incur no more than 10,000 bytes since the ACK losses are recovered by the next cumulative-ACK.

On the other hand, for SR, since each ACK is not a cumulative ACK, on an average one extra transmission will happen for each lost ACK. Thus, number of extra packets that need to be sent will be $0.1 \times 10,000 = 1,000$, which will generate an extra 1,000 acknowledgements in the reverse direction. However, again out of these 1,000 Acks, 10% will be lost. So, another extra 100 packets need to be sent, and another 10 to counter the lost Acks within these 100 Acks. So, the total number of extra packets that need to be sent is 1,000+100+10+1=1111 packets.

(b) In the forward direction, things are bit more complicated. For selective repeat, exactly 1% of lost packets need to be resent. That means an extra 100 packets. But, again these packets may be lost, so that would require another 1 packet transmission. Thus, the total number of extra transmissions required for the selective repeat is 101.

For GBN, this is a problematic scenario. For every lost packet, it needs to transmit up to N packets. Given a loss rate of 1%, the total number of extra packets is $N \times 100 = 1,000$. However, every time the entire window is transmitted, 1% of the packets might get lost within the window. Thus, again another $N \times 1\% \times 1000 = 100$ packets might be lost. And so on. The total number of transmitted packets would be 1110.

Question 2.

In the slow-start mode, the congestion window doubles in size each transmission round. During the fourth round when the congestion window equals to 8 MSS, all 8 transmitted packets are lost. Hence, the sender determines the losses via a timeout, sets the threshold to 4 MSS, and reduces the congestion window to 1 MSS. Staring from the fifth round, the sender retransmits the lost data and then transmits the remaining portion of the file. The congestion window doubles until it becomes equal to the threshold (i.e., 4 MSS) during the seventh transmission round. Then, the TCP connection switches to the congestion-avoidance mode and increases the congestion window by 1 MSS per transmission round. Host A finishes the delivery of the 32-MSS file during the tenth round:

Round	*Congestion window (MSS)*	*Transmitted data (MSS)*	*Delivered data (MSS)*	*Cumulative delivered data (MSS)*
1	*1*	*1*	*1*	*1*
2	*2*	*2*	*2*	*3*
3	*4*	*4*	*4*	*7*
4	*8*	*8*	*0*	*7*
5	*1*	*1*	*1*	*8*
6	*2*	*2*	*2*	*10*
7	*4*	*4*	*4*	*14*
8	*5*	*5*	*5*	*19*
9	*6*	*6*	*6*	*25*
10	*7*	*7*	*7*	*32*

Question 3.

(a) 128.8.128.252 – Port 3
(b) 128.8.128.5 – Port 4
(c) 128.8.25.223 – Port 2
(d) 155.128.45.21 – Port 5

Question 4.

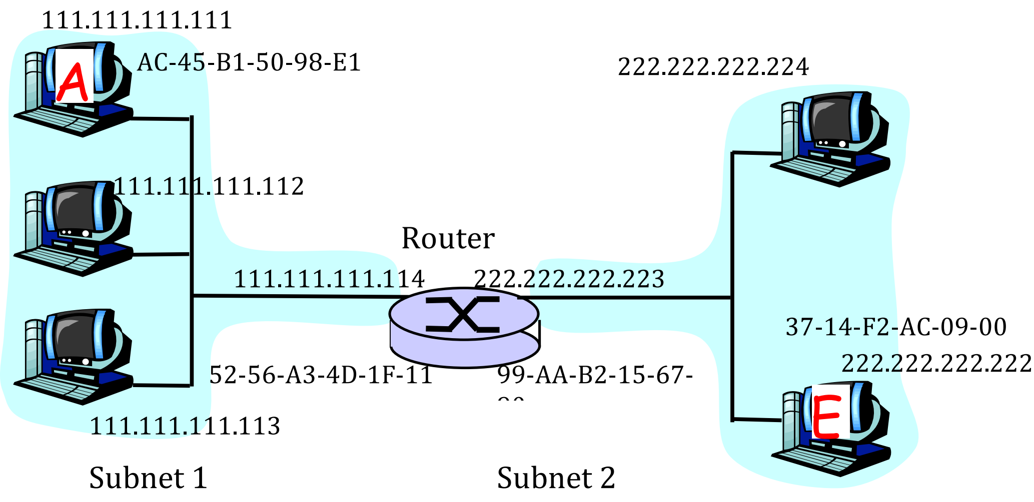
N'	D(s), p(s)	D(t), p(t)	D(u), p(u)	D(v), p(v)	D(w), p(w)	D(y), p(y)	D(z), p(z)
x	Inf	Inf	Inf	3,x	1,x	6,x	Inf
xw	Inf	Inf	4,w	2,w		6,x	Inf
xwv	Inf	11,v	3,v			3,v	Inf
xwvu	7,u	5,u				3,v	Inf
xwvuy	7,u	5,u					17,y
xwvuyt	6,t						7,t
xwvuyts							7,t
xwvuytsz							

The forwarding table is as follows:

Destination	Link
w	xw
v	xw
u	xw
y	xw
t	xw
s	xw
z	xw

Question 5.

(a) If the network part of the address is 24 bits (/24), then all interfaces in the left network must be of the form 111.111.111.xxx, while the interfaces in the right part must be of the form 222.222.222.xxx. The IP addresses are shown in the figure on the next page.



(b) LAN addresses are 48 bits long and are very different from the 32 bit IP addresses from part a). The LAN addresses are shown in the above figure.

(c)

(i) In the IP datagrams from A to the router the addresses are as follows: source: 111.111.111.111, destination: 222.222.222.222. In the IP datagrams from the router to E the source and destination addresses are same.

(ii) Hopcount (TTL), upper layer protocol, options (see book/notes for others).

(iii) Using the address resolution protocol (ARP).

(d)

(i) The IP addresses of A and E would have to have the <u>same</u> network prefix since they are now part of the same subnet.

(ii) They would stay the same in A and E.

(iii) When an attached host sent a frame through the switch (e.g., arriving on interface x) the switch would observe the LAN (physical) address of the sender, and then know that a host with that physical address was reachable via the interface (x) on which the original frame was received.

Question 6.

(a)

The one-way propagation delay is,

$$\frac{900m}{2\cdot 10^{8} m/\sec} + 4\cdot\frac{20 bits}{10\times 10^{6} bps}$$

$$= (4.5\times 10^{-6} + 8\times 10^{-6})\sec$$

$$= 12.5\mu\sec$$

(b)

- At time $t = 0$, both A and B transmit.
- At time $t = 12.5\mu\sec$, A detects a collision.
- At time $t = 25\mu\sec$ last bit of B's aborted transmission arrives at A.
- Since A draws K=0 in the backoff algorithm it can instantly start the retransmission at time $t = 25\mu\sec$.
- At time $t = 37.5\mu\sec$ first bit of A's retransmission arrives at B. Note that, this time is smaller than the 512 bit time that B has to wait for backoff. Hence, B does not begin its transmission since it detects A's transmission. (In CSMA, the node senses the channel before transmit)
- At time $t = 37.5\mu\sec + \dfrac{1000 bits}{10 \times 10^6 bps} = 137.5\mu\sec$ A's packet is completely delivered at B.

If you had assumed that the nodes A and B detect the collision at time, t=0, then your solution should be 12.5 μ sec less than the above answer.

Question 7.

(a) A is sending data to B.

(i) Yes, because C does not hear A.

(ii) No, because C has heard the CTS sent by B.

(b) B is sending data to A.

(i) No, because C has heard the data transmission from B.

(ii) Yes, because C has not heard the CTS from A, even if it heard the RTS from B.

Question 8.

We first need to determine the private key.
Since n = 55, p and q are 5 and 11 respectively.
Hence, z = (p-1)(q-1) = 40.
e is 27, we need to find d such that (ed-1) is exactly divisible by 40. Hence, d = 3.
(NOTE: You could choose other values of d provided they satisfy the above property)
So the private key pair is (d,n) = (3, 55).

We can down convert the ciphertext to plaintext using the formula, $P = C^3 \text{ mod } 55$.
Using this we get: (8)(1)(16)(16)(25)(27)(8)(15)(12)(9)(4)(1)(25)(19)
This translates to: HAPPY HOLIDAYS
(NOTE: 27 indicates a white space between HAPPY and HOLIDAYS)

Question 9.

The message associated with a message digest value need not be encrypted. Encrypting the message provides for confidentiality, while the message digest provides for integrity – two different goals.