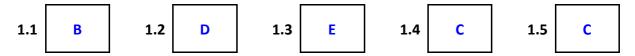
## Please DO NOT upload questions and answers onto the Internet.



2.

(a) 
$$3.6*10^7 / 2.4*10^8 = 0.15$$

(b) 
$$x / 10Mbps = 24$$
;  $x = 2.4 * 10^8$ 

3.

(a) **00111010** 

(b) 300 Kbps

(c) 
$$\frac{1.8*10^6}{60*3} = 10,000$$

(Draw timeline diagram. Consider the worst case that A sends a frame to B. Just before this frame reaches B, B starts transmission. It takes A around RTT to receive the first bit from B and thus detect collision.)

4.

Interface	IP Range	No. of IP
3	1100 0000 - 1100 1111 1110 0000 - 1111 1111	32+16=48
4	1010 0000 - 1011 1111	32
1	1000 0000 - 1001 1111	32
2	1101 0000 - 1101 1111	16
0	0000 0000 - 0111 1111	128

5.

# of pkt = 
$$\left[\frac{400 * 10^3}{1000 - 80}\right] = 435$$

Total # of bits sent = 435\*80 + 400,000 = 434,800

Length of first 434 packets: 1,000

Length of last packet: 800

End-to-end delay =  $\frac{1000}{10^3} + 40 + \frac{434,800}{10^3} + 40 = 515.8$  ms

6.

- 1. Alice encrypts m with her private key to create digital signature  $K_A^-$  (m).
- 2. Alice concatenates message with digital signature  $m \oplus K_A^-(m)$ , and encrypt the extended message with Bob's public key:  $K_B^+(m \oplus K_A^-(m))$ .
- 3. Alice sends  $K_B^+(m \oplus K_A^-(m))$  to Bob.
- 4. Bob decrypts the received message using his private key:  $K_B^-(K_B^+(m \oplus K_A^-(m))) = m \oplus K_A^-(m)$ .
- 5. Bob then uses Alice's public key to derive message from digital signature:  $K_A^+(K_A^-(m)) = m'$
- 6. If m = m', message integrity is preserved.
- 7. Because message is encrypted during transmission, message confidentiality is preserved.

(Another approach is for Alice to send  $K_B^+(m) \oplus K_A^-(K_B^+(m))$ )

7.

- (a) **1,000**
- (b) **53,000**
- (c) Y buffers out-of-order packets. The packet B is an out-of-order packet. However, it is not retransmitted even if a later packet D is already retransmitted. That implies 53,000 is buffered and already acknowledged.