CS457: Computer Networking
Date: 5/5/2008
Name: _____

Instructions:
1. Be sure that you have 10 questions
2. Write your Student ID (email) at the top of every page
3. Be sure to complete the honor statement after you complete the exam
4. This is a closed book exam
5. The seats on both sides of you should be empty
6. State all assumptions and be sure your answers are legible
7. Show all work; the graders will give partial credit
8. Answer each question clearly and to the point; do not define or describe concepts unless asked to do so; assume that the graders are familiar with the concepts

Question	Points	Score
1	10	
2	10	
3	10	
4	10	
5	10	
6	10	
7	10	
8	10	
9	10	
10	10	
total	**100**	

1. Answer the following True/False questions by circling either **T** or **F.**

    1. If a non-persistent, non-pipelined connection takes 100 RTTs to retrieve a web page, a persistent, non-pipelined connection would take 25 RTTs for the same page.   T   F

    2. Iterative DNS queries require shorter socket connections with DNS servers than recursive DNS queries.   T   F

    3. A machine can open more than one TCP socket on the same port.   T   F

    4. TCP is fair because of additive increase/multiplicative decrease, not because of slow start.   T   F

    5. NAT can support more than 65535 simultaneous processes.   T   F

    6. BGP emphasizes policy and scalability over routing efficiency, sometimes producing less-than-optimal routes.   T   F

    7. Some error detection schemes are guaranteed to detect errors for any number of flipped bits in the packet.   T   F

    8. An entity's "certificate" is its public key encrypted by a certificate authority's private key.   T   F

    9. In CSMA/CD, a node always waits a random time before transmitting any packet.   T   F

    10. A man-in-the-middle attack is more powerful with public key authentication than with symmetric key authentication.   T   F

2. **Reliable Transport**

For this problem, assume the pipeline size is 6, delay between packets is greater than 500ms, and timeout > 6*RTT. In other words, assume that six packets can be sent and acknowledged more quickly than a timer will timeout. Node A sends 6 messages to node B and the 3rd message is lost. How many messages do node A and B each send in total:

a. using Go-Back-N?

> A sends 6 + 4 = 10 messages
> B sends 2 + 4 = 6 acknowledgments
> 16 total

b. using Selective Repeat?

> A sends 6 + 1 = 7 messages
> B sends 5 + 1 = 6 acknowledgments
> 13 total

c. using TCP?

> A sends 6 + 4 = 10 messages
> B sends 5 + 4 = 9 acknowledgments
> 19 total
> (due to ambiguity in the phrasing of the original question, any answer is accepted here)

Node A sends 6 messages to node B and the 3rd , 4th, 5th, and 6th messages are all lost. How many messages do node A and B each send in total:

a. using Go-Back-N?

> A sends 6 + 4 = 10 messages
> B sends 2 + 4 = 6 acknowledgments
> 16 total

b. using Selective Repeat?

> A sends 6 + 4 = 10 messages
> B sends 2 + 4 = 6 acknowledgments

16 total

c. using TCP?

A sends 6 + 4 = 10 messages
B sends 2 + 4 = 6 acknowledgments
16 total

3. **Hubs, switches, and routers**

a. When MUST you use a switch instead of a hub?

When the links to be connected have different bit rates.

b. When MUST you use a router instead of a switch?

When the links between the switches contain a cycle.

c. Name the three basic types of switching fabrics used inside of a router.

1. Memory-based
2. Bus-based
3. Crossbar/ Banyan/interconnect networks

d. Which of these are susceptible to head-of-the-line blocking?

Only crossbar networks are susceptible to head of the line blocking, because the other two cannot simultaneously transfer packets from input to output ports anyway.

e. Which of these are susceptible to output port queuing?

All of these are susceptible to output port queuing.

4. **IP Addresses**

Assume an ISP is given the address space 201.198.240.0/20.

a. How many IP addresses does it have to assign?

    2^12

b. If this ISP wants to assign an equal number of addresses to 16 clients, how many addresses can it assign them?

    (2^12)/16 = 256

c. How many entries does this ISP need to have in its router, for each client?

    It needs one entry for each client, because it can give each client a contiguous address space and place only one CIDRized address into its routing tables.   Thus, 16 entries in total.

d. How many entries do this ISP and its 16 clients need to have in the router of this ISP's parent ISP?

    All of these clients and the ISP itself are pointed to by a single entry in the parent ISP's routers. In particular, the entry is: 201.198.240.0/20

e. How would the answers to (c) and (d) above change if one of this ISPs clients changed to another ISP, but kept the same address space allocation?

    For (c), the ISP would still have one entry per client, but would not only have 15 entries instead of 16. The last entry would be moved to the router of the client's new ISP.

    For (d), this ISP and its 15 clients could still be pointed to by a single entry in the parent ISP's router: 201.198.240.0/20. However, the client that moved would require a new entry in its new ISP's router, as well as the routers of the parent of its new ISP. Thus, if the new ISP has the same parent as the old ISP, the parent now has 2 entries for these 16 networks.

5. **Routing**

a. Use Dijkstra's algorithm to find the shortest path D(i) and the previous node on that path p(i) from node **u** to all other nodes **i** in the network shown below.

| Step	N'	D(v),p(v)	D(w),p(w)	D(x),p(x)	D(y),p(y)	D(z),p(z)
0	u	4,u	5,u	1,u	∞	∞
1	ux	3,x	5,u		10,x	∞
2	uxv		5,u		10,x	∞
3	uxvw				6,w	10,w
4	uxyvw					10,w
5	uxyvwz					
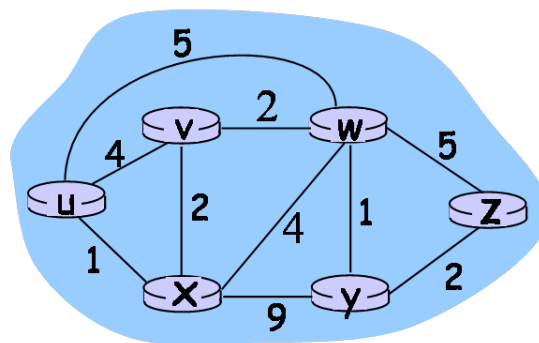
Routing table:

V: X
W: W
X: X
Y: W
Z: W

b. Convert this shortest path estimates calculated above into a routing table for **u**.

See above.

6. **Wireless Media Access Control**

In the following diagram, nodes A, B, C, and D have circular radio range. Recall that a "collision" occurs when a receiver can hear a data packet from two different transmitters at the same time.
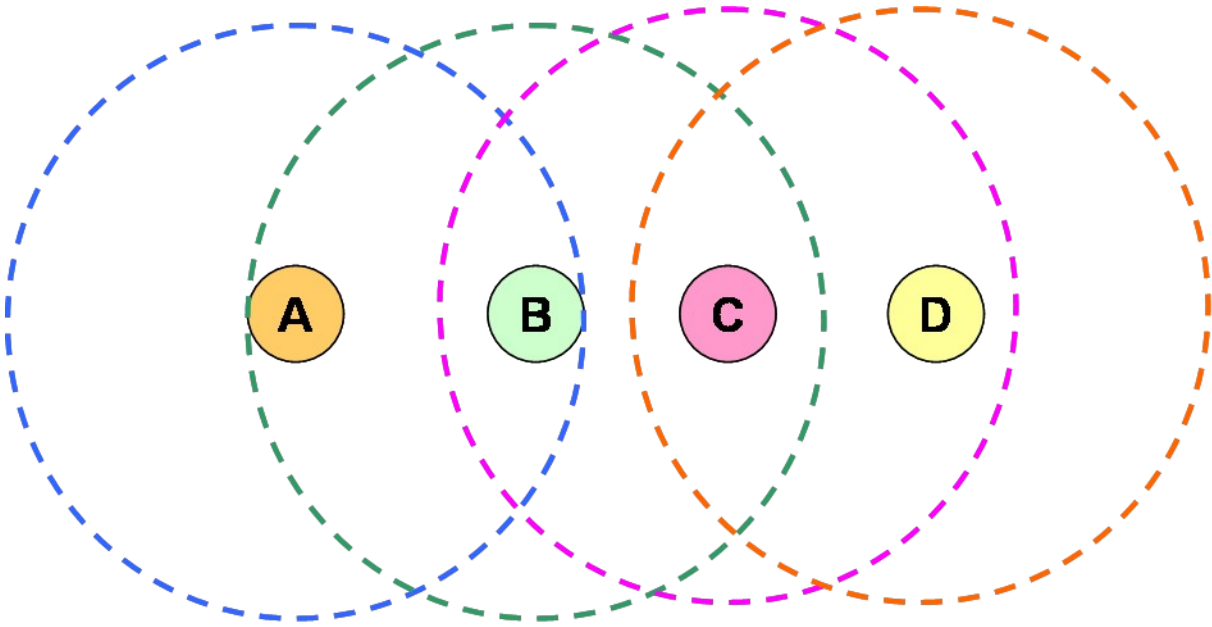
a. Which pairs of nodes can transmit without causing a collision?

     A-> B and D->C
     B-> A and C->D

b. Using CSMA/CA, which pairs of nodes can not transmit simultaneously, but would not cause a collision anyway if they did? What is the name of this problem?

     B-> A and C->D
     "Exposed Terminal problem"

c. Using CSMA/CA, which pairs of nodes can transmit simultaneously but would cause a collision? What is the name of this problem?

     A-> B and C->D
     B-> A and D->C
     "Hidden Terminal Problem"

d. Using RTS/CTS, which pairs of nodes can not transmit simultaneously, but would not cause a

collision anyway if they did? What is the name of this problem?

A-> B and D->C
"Blocked Terminal Problem"

e. Using RTS/CTS, which pairs of nodes can transmit simultaneously but would cause a collision? What is the name of this problem?

A-> B and C->D
B-> A and D->C
A CTS collision (can also be caused by asymmetric links)

7. **ARP**

In the following diagram, assume that all nodes have been configured with the correct IP addresses, subnet, and default gateway router. However, all of their ARP tables are currently empty.

a. Show all messages (including both IP and ARP messages) that must be sent/received in order to transfer a message from node A to node B.
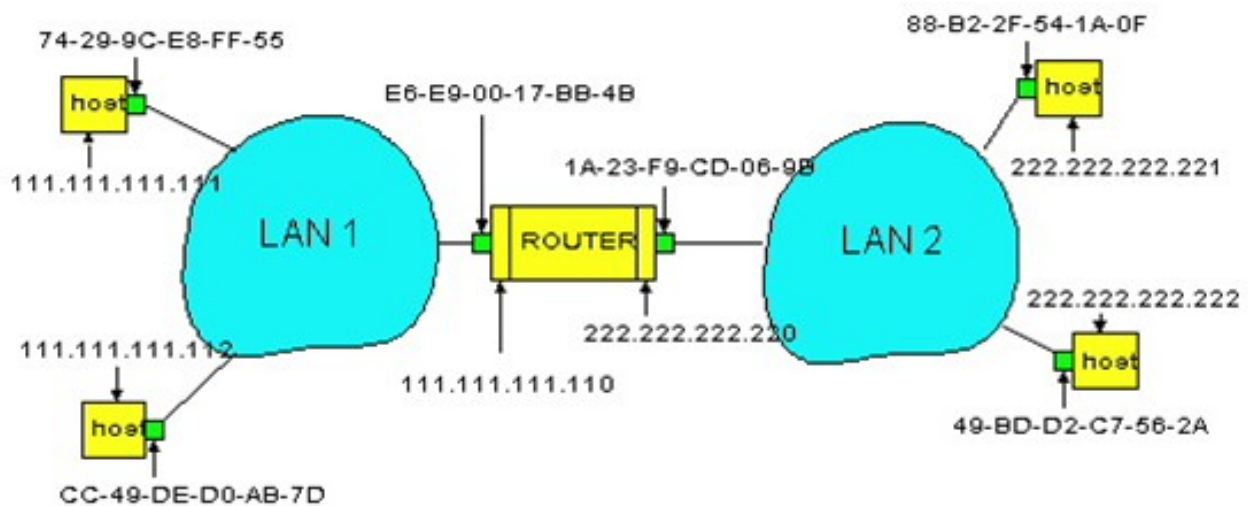
1. A sends ARP request for gateway physical address
2. Gateway responds with ARP reply
3. A sends message to gateway
4. Gateway sends ARP request for B's physical address
5. B responds with ARP reply
6. Gateway forwards message to B

b. How does each node decide whether to use the default gateway's physical address or that of the destination?

Nodes will send all messages to their gateway routers, unless the destination is on the same subnet. In that case, nodes will send the message directly to the destination.

8. **Public Key Cryptography**

For public key cryptography, we would like to choose values e, d, and n such that:

$$m = (m^e \bmod n)^d \bmod n$$

If we choose two values p and q to be prime such that pq = n, we can use the following number theory result

$$x^y \bmod n = x^{y \bmod (p-1)(q-1)} \bmod n$$

to help in step 2 of the derivation below:

$$(m^e \bmod n)^d \bmod n = m^{ed} \bmod n$$
$$= m^{ed \bmod (p-1)(q-1)} \bmod n$$
$$= m^1 \bmod n$$
$$= m$$

What constraints do we need to introduce in steps 3 and 4 to make those steps correct?

a. (e*d) mod (p-1) (q-1) = 1

b. m < n

9. PGP

PGP is a popular email security program. To encrypt a message, PGP uses three steps: 1) generate a message digest using the user's private key 2) encrypt the original message and the digest using a symmetric key 3) encrypt the symmetric key using the recipient's public key. These steps are illustrated below:
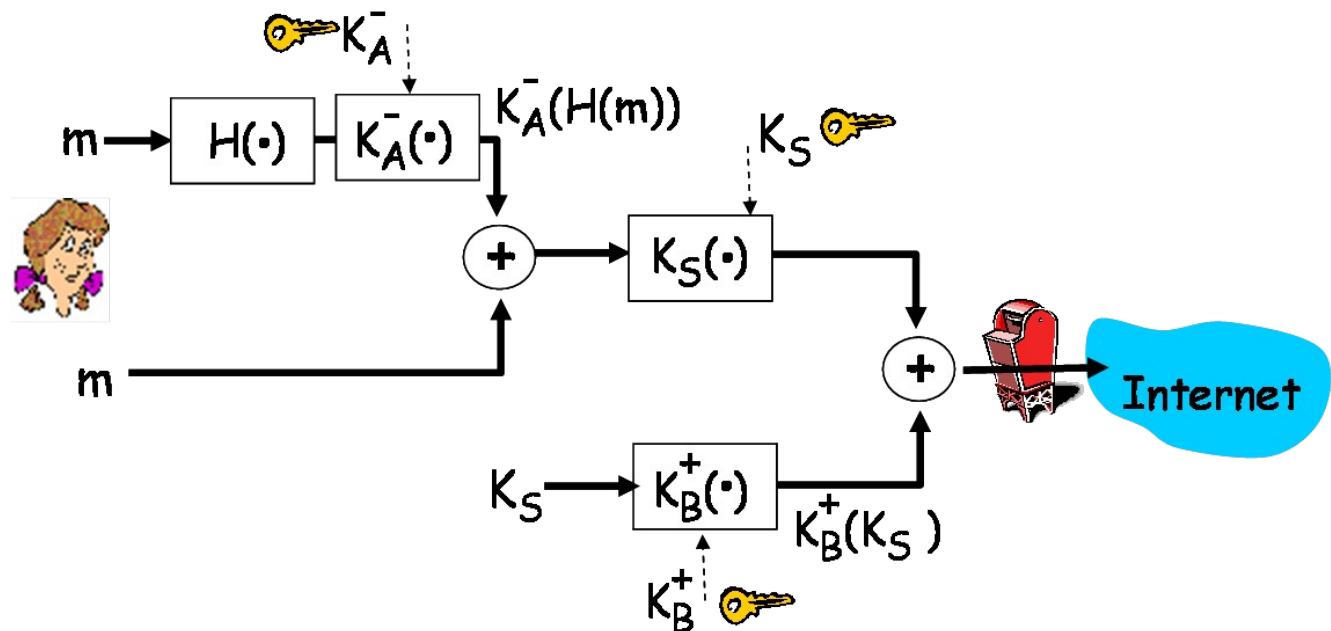
Explain the purpose of each of these three steps, using five words or less for each one:

a. "Message integrity" and "authentication"

b. Greater "efficiency" over public key

c. "Privacy" or "confidentiality"

10. **CDMA**

Assume that a CDMA receiver receives two simultaneous messages from different CSMA transmitters. The following values are read from the radio: 0 -2 0 2 0 0 2 2

a. What bit value is the first transmitter sending if it is using the code: 1 1 1 -1 1 -1 -1 -1

    -1

b. What bit value is the second transmitter sending if it is using the code: 1 -1 1 1 1 –1 1 1

    1

Honor Code

_____

_____

_____

                    Signature _____