MCS-377 Final Exam

Serial #:

This exam is closed-book and mostly closed-notes. You may, however, use a single 8 1/2 by 11 sheet of paper with *hand-written* notes for reference. (Both sides of the sheet are OK.)

Please write your name only on this page. Do not turn the page until instructed, in order that everyone may have the same time. Then, be sure to look at all problems before deciding which one to do first. Some problems are easier than others, so plan your time accordingly. You have 120 minutes to work.

Write the answer to each problem on the page on which that problem appears. You may also attach additional paper, which should be labeled with your test number and the problem number.

You must sign the honor pledge below and abide by it.

Printed name: _____

On my honor, I pledge that I have not given, received, nor tolerated others' use of unauthorized aid in completing this work.

Signature for above honor pledge: _____

Problem	Page	Possible	Score
1	2	12	
2	3	12	
3	3	8	
4	4	9	
5	5	8	
6	5	9	
7	6	6	
8	6	8	
9	7	7	
10	8	8	
11	9	8	
12	9	5	
Total		100	

1. [**12 Points**]

   (a) What is the difference between a firewall that filters based on layer four and below and one that filters also based on layer seven content? Give an example of a desirable kind of filtering rule that might be made possible by layer seven analysis.

   (b) What is the difference between a firewall that filters based on layer seven content and an application gateway?

   (c) Explain why a NAT also acts as a form of firewall.

2. [**12 Points**]

   (a) Having either a KDC or a CA available greatly increases the flexibility and scalability of network security relative to a situation where neither a KDC nor a CA is available. Explain why.

   (b) What kind of cryptography is used by a KDC and what kind by a CA?

   (c) Both KDCs and CAs need to be carefully secured, because if either is breached, that can have large-scale security ramifications. Explain why a CA is easier to secure than a KDC.

   (d) Explain why interruptions in the service availability of a CA do not cause as much trouble for communications as interruptions in the availability of a KDC.

3. [**8 Points**] Suppose Alice has a long message, m, to send to Bob, and that she and Bob know each others public keys for an asymmetric key cipher. (Alice's public key is K_A^+ and Bob's is K_B^+.) Further suppose that Alice wants to ensure the message's confidentiality and integrity. Finally, suppose that for efficiency reasons, Alice does not want to use the asymmetric key cipher on anything so large as m; therefore she (and Bob) may also use additional kinds of cryptographic operations. Draw a diagram of the overall cryptographic process that Alice would use to transform the message for transmission.

4. [**9 Points**]

(a) Why can't collisions be reliably detected by the transmitting stations in wireless networks?

(b) How then do the transmitting stations determine whether their frames are being successfully received?

(c) Given that collisions can't be detected, how can a mobile station avoid transmitting an entire, long, frame in a situation that results in a collision? (There are several mechanisms that play a role in collision avoidance, one of which applies particularly to long frames. For full credit, mention that length-dependent mechanism and at least one other.)

5. [**8 Points**] Explain why 802.11 data frames contain three addresses when the wireless link is between an access point and a mobile station. Explain why 802.11 data frames contain four addresses when the wireless link is between two access points.

6. [**9 Points**]

   (a) In what context is BGP used for routing?

   (b) How does BGP differ from distance-vector routing protocols?

   (c) How does this difference allow BGP to avoid the count-to-infinity problem?

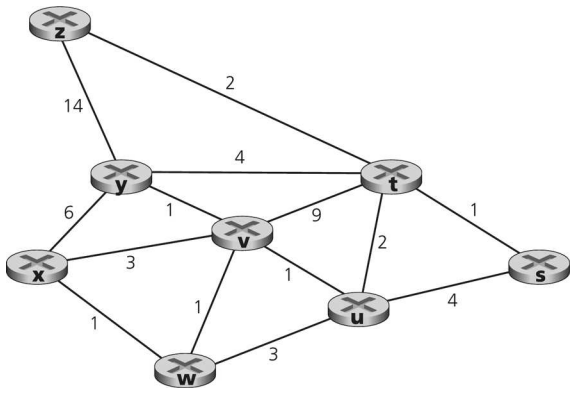
7. [**6 Points**] Translate between notations as indicated:

   (a) Express the subnet mask 255.255.128.0 in the /x form (i.e., as a number of prefix bits).

   (b) Express the subnet mask /19 in dotted decimal form (producing a result akin to 255.255.128.0, but for a different number of prefix bits).

8. [**8 Points**] An organization has been assigned the prefix 173.215.72.0/23. It wishes to subdivide this address range, establishing four subnets within the organization. The four subnets should be of equal size. What would suitable prefixes, expressed in a.b.c.d/x form, be for the four subnets? Approximately how many interfaces would each subnet accommodate?

9. [**7 Points**] The following network is similar to the one you used for problem 4.p22. Once again you are to use Dijkstra's shortest-path algorithm to compute the shortest path to all network nodes, showing your work in a table. However, this time, you are to compute the paths starting from s. If you need to break any tie, pick the node that comes earlier in the alphabet.



step	N'	$D(t)$, $p(t)$	$D(u)$, $p(u)$	$D(v)$, $p(v)$	$D(w)$, $p(w)$	$D(x)$, $p(x)$	$D(y)$, $p(y)$	$D(z)$, $p(z)$
0	s							
1								
2								
3								
4								
5								
6								
7								

10. [**8 Points**]

(a) What is the difference between the goals of flow control and congestion control in TCP?

(b) Both of these forms of control involve a "window" that specifies how much unacknowledged data the sender can have outstanding. For which one does the sender receive messages over the network telling it how many bytes in size the window should be?

(c) What is the difference between slow-start mode and congestion-avoidance mode in TCP?

11. [**8 Points**]

    (a) What two numbers are used to identify a UDP destination?

    (b) What four numbers are used to identify a TCP connection?

    (c) Why might a web browser keep several TCP connections open to the same server?

    (d) Why might a web browser keep several TCP connections open, each to a different server, even if it only uses one of them at a time?

12. [**5 Points**] List five commands or header fields used in the HTTP/1.1 protocol. For each one, specify whether it is a command, a header typically sent by clients, a header typically sent by servers, or a header used equally by clients and servers.