Name (Print) _____

Email Address _____

ECE3076 Final Exam
April 30, 2007 2:50-5:30 p.m.

RULES.

i This quiz is **not** open book. Three original sheets of hand-written notes may be used. Calculators are ok.

ii Answer all questions and show all work to receive full credit. Use back of sheets only if necessary.

iii Please do not ask the proctors any questions during the exam about exam questions. Part of the test is understanding the question, as written, without supplemental information. If you feel additional data is needed to solve the problem, make (and state) an assumption and then work the problem.

iv. This is a time-limited test. If you find you are taking more than 10 minutes on a particular problem, move on and come back to that problem after finishing the others.

v. The Georgia Tech Honor Code applies (see last page).

Question 1 – TCP with no Congestion (6 points). A 10 Mbps network connection has a 20 ms round trip time (RTT). A server begins sending maximum-size (MSS=1500 byte) packets (after the initial SYN-ACK). The client ACK's every packet, and has a Receiver-Window which holds 10 maximum-size packets (segments).

What is the transmission time for a single packet (1500 bytes) ____*1500*8/1e7 = 12000e-7 = 1.2e-3* = **1.2 ms**_____

Show how many packets are sent in each RTT period below:

Time Period Start (ms)	No. Segments sent
0	1 (SYN-ACK)
20	1
40	2
60	4
80	8
100	10
120	10

What is the average transmission rate during the first 80 ms (0-79 ms)? *(1+2+4) * 1500 * 8 / 80 ms* = **1.05 Mbps**

Question 2 - Bandwidth-Delay Product(6 points)

a. What does TCP guarantee that UDP does not (for a byte-stream sent in multiple packets)?

All bytes will be delivered to the receiving application, in correct order.

b. If the round-trip time (RTT) for a dedicated 100 Mbit/s connection to California is 50 ms, what will the maximum throughput be if the window is 65 kbytes? _____65,000 * 8 / 0.05s = **10.4 Mbps**_____ (bits/s)

c. What is minimum TCP widow size that will allow this channel to be fully utilized? ___0.05s * 100 Mbps /8 = **625 kB**

Question 3 – IP Datagrams (8 points)

a. When is the ID number used? _____**When the packet is segmented**_____

b. What field in the IP header changes when a datagram is forwarded by a simple router? _____**TTL**_____

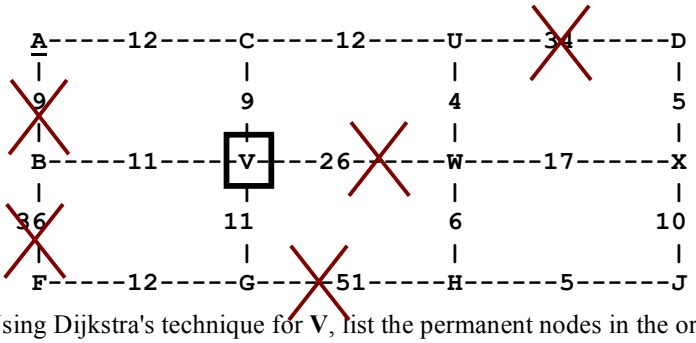
c. What other field always changes when a IP datagram if forwarded by a NAT router? _____**Local IP address**_____

d. What other field may or may not change, depending on the NAT implementation? _**local TCP or UDP port number**__

Question 4 – Routing, Link State, OSPF (14 points)

Every router (A, B, ..., J) has advertised the costs (delays) to its neighbors to all the other nodes
Based on all the advertisement messages, the network topology and link costs can be mapped. The letters below represent the nodes (routers) on the network. The numbers represent costs (delay-times) on the links between them. For simplicity, we assume the costs are the same in each direction of a link.

These nodes are all routers (no networks) and for simplicity routes have the same cost in both directions.



[Show numbers next to nodes]

A. Using Dijkstra's technique for **V**, list the permanent nodes in the order they are added, and the cost (distance) to them:

Node	V	C	B or	G	A OR	U	F	W	H	J	X	D
Cost	0	9	11	11	21	21	23	25	31	36	42	47

B. Fill in the Routing Table for Node B (* indicate physical port (link) by the node to which it connects).

Node **V** Table	
Destination	Port*
A	**C**
F	**G**
D	**C**
J	**C**

Question 5 – Packet Delay Calculation (8 points)

Two nodes(A and B) are connected by 100 km optical fiber (v=2e8 m/s). At time zero the next packet in A's buffer starts to transmit. The packet has 1250 bytes. The link transmission rate is 10 Mbits/s for A and B.

a. At what time is the last bit in the packet transmitted by A (in microseconds)? _1250 *8 / 10 M = **1000__ us**

b. At what time does the last bit arrive at B? ___1000 + 100,000 m / 2e8 m/s = **1500 __ us**

It takes 10 us for node B to decide where to send the packet, and copy it to the correct output buffer (ignore this time).

c. If the output buffer of B has five 1250-byte packets when our packet arrives, what is the queuing delay? 5*1000 = **5000 us**

d. What is the total delay for link A-B? ____1500 + 5000 = **6500 us** *(6510 us if you do not ignore processing delay)*

Names: a = transmission delay, b = a + propagation delay , 10us = processing delay, c = b + caching delay.

Question 6 – Streaming Media (14 points)

Which transport layer is most used for streaming media? _____**UDP**_____

What service does SIP and H.323 provide? _____**Set up interactive multimedia or VOIP connections**_____

On what 3 parameters does QoS guarantee certain performance? ___**delay**___, __**bitrate (bandwidth)**___, __**jitter**___

What technique can make up for occasional dropped packets on the data path? ____ **FEC** (forward error correction)_____

What technique can make up for several sequential packets being lost? _____ **interleaving** _____

Name (print) _____

Question 7 – Security (8 points)

What are the two basic services provided by a digital signature on a message?

a._____ **Authenticates the author**_____, b. ___ **No bit has been altered** _____

What attack is effective against to two hosts using RSA encryption if they swap public keys in the clear.

c._____ **Man-in-the-middle attack** _____

What is the purpose of using a "nonce" in an authentication routine (stops which attack)?

d. ____ **Stops replay attacks** _____

Question 8 – Encryption (16 points)

a. What is the main problem with symmetric (secret) key encryption? _____ **Secure Key Distribution** _____

b. How many possible keys are there if the key length is 64 bits? _____2^64 = **2e19** = *20,000,000,000,000,000,000*

For asymmetric (public/private) key encryption:

c. What is the longest bit string that can be encrypted in one block with a 512-bit public key? __**511 bits**_____

What are the steps to encrypt a 10,000 byte message with a 512-bit public key?

d. _____**Generate a random session key** _____ e. _**Encrypt the session key with the receiver's Public Key**__

f.___ **Encrypt the message using the session key and a symmetric-key technique**_____

g. When using HTTPS, how do you know the public key supplied by a merchant is not a fake? _**CA certificate** ____

h. How is a "hash" like MD5 or SHA used to provide a digital signature of a message?
____**Hash of message is encrypted with the signer's private key**_____

Question 9 – Host Configuration (16 points)

What four items of information are needed by a host before it can operate normally on the network:

1. __**Assigned IP adress**___ 2. __**Network mask**___ 3. ___**Gateway router IP address**____ 4. ___**DNS server IP** _____

If these are not configured manually, what protocol can be used to get them over the network? ____ **DHCP**_____

Before sending an IP datagram over Ethernet, what protocol is used to find the right Ethernet address? ___**ARP**__

What Ethernet address is used for a host not on the local network? ___ **Gateway router Ethernet address** ___

If a host knows its own IP address, what does it need to calculate its Network IP and Broadcast IP? _**Network mask**__

Question 10 – IP Addresses (4 points)

How does (a) CIDR and (b) NAT lead to much more efficient use of the available IP address space?

a. **CIDR allows the assigned network IP-address range to be tailored to fit the need**.

b. **NAT allows use of a single external address for private networks.**

Honor Code - I affirm that I have obeyed the rules of the Georgia Tech Honor Code*.

Signature _____

*Basically, I did not cheat, and I reported any observed cheating. A grade will not be recorded if there is no signature.