Washington State University
CptS 455 Sample Final Exam
Final exam is 8AM Tuesday, Dec. 13, 2016

Your name: ____

This exam consists 13 numbered problems on 6 pages printed front and back on 3 sheets. Please check to make sure that you have the entire exam before beginning.

You may have one 8 1/2 x 11 sheet of notes (both sides, typewritten or handwritten). Otherwise, this is a **closed book, closed notes, closed neighbor** exam. Calculators are allowed.

1. (20 pts) In column A, number the protocol layers named in column B in order from 1, for the "lowest" to 5 for the highest.

A	B	C
	Application layer	web page serving
	Physical layer	operates between directly connected hosts
	Transport layer	primarily characterized by electrical or optical signalling techniques
	Network layer	reliable bytestream delivery to applications
	Link layer	deliver datagrams across multiple connected links

Draw a line connecting each protocol layer name in column B to the *one best* corresponding description or characteristic in column C.

2. (15) Describe in detail the TCP connection-establishment protocol (sometimes called the *three-way-handshake*). Make sure to describe the use of features of the TCP header, such as the SYN bit, the sequence number and acknowledgement number fields, etc.

3. (20) Suppose that the largest ACK that a TCP sender has received is *a,* that the most recently received receiver window size is *w* and the sender's current congestion window is *c*. If the highest sequence number it has sent so far is *h* then how many more bytes is it allowed to send? I'm looking for an arithmetic expression using variables *a*, *w*, *c*, and *h*.

4. (20) IP Network addressing

   If a host's IPv4 address and netmask are given as 134.121.127.22 and 255.255.248.0, respectively:

   a) (5 pts) How many bits make up the subnet part of the address?

   b) (5 pts) How many bits make up the host part of the address?

   c) (5 pts) Is a host with address 134.121.255.22 on the same subnet? Explain.

   d) (5 pts) What is the broadcast address for this subnet?

5. (15 pts) Consider a communication link with ***round-trip latency*** of 80 msec., and bandwidth 1 Mbit/s. Assume that the transmission time (but not the latency!) for ACKs/NAKs is 0. If a sender sends 1600 bit packets what is the *maximum* bandwidth that can be achieved (show your work and please be careful to properly distinguish bits and bytes)
   a. (5 pts) if the sender waits for an acknowledgement after each packet before sending the next?

   b. (5 pts) if the sender uses a protocol such as TCP that allows multiple packets to be unacknowledged?

   c. (5 pts) What is the required *window size* in order to achieve the maximum bandwidth in part b.

6. (15) Draw an illustration of how a TCP congestion window typically varies over time. Label a) regions where slow-start is occurring b) regions where additive increase is occurring c) points where time-outs occur d) threshold values. E) What on the diagram corresponds to the "multiplicative decrease" in the so-called "additive increase, multiplicative decrease" congestion window strategy.

7. (10 pts) Explain how the idea of a exponential moving average is used in computing TCP round-trip times, and RTT variation.

8. (20) Suppose a program executes the statement `res = select(...);`
   a. After select returns, what are the meanings of the various values that might be stored in res:

      0?

      a positive number?

      a negative number?

   b. After select returns how does the calling program determine which file descriptors are now ready to perform I/O?

9. (20) Consider RSA cryptography with p=5, q=11.
   a. What are n and z?

   b. Why is e=27 an appropriate choice for an encryption key given this p and q?

   c. Why is d=3 the correct choice for the corresponding decryption key?

   d. If the ciphertext, c=20, what was the original message, m?

10. (10) *Cryptographic hash* functions map arbitrary messages to fixed length strings. What characteristics are important for a hash function to be considered *cryptographic*?

11. (10) Given a cryptographic hash function H, describe how to use H for a message authentication code? I'm looking for a description of the sender and receiver behavior when using HMACs.

12. (15) Why is UDP preferred to TCP as the protocol for carrying voice signals when doing telephony over the Internet (so-called VOIP)?

13. (20) Suppose that G=1101 is used as a generator for a CRC calculation for the data 100111.
    a. How many bits are in the generated CRC? Explain.

    b. What is the generated CRC? Show your work.

Note that this sample exam is rather light on material from Chapters 6 and 8: for Chapter 6 be sure to study the material on the *hidden terminal problem* and make sure you know what CSMA/CA is and why it is typically used instead of CSMA/CD for wireless networks.

For Chapter 8: make sure you understand the role of *certificates* and *certificate authorities;* make sure you understand how message authentication and encryption work when using Public Key Cryptography – in particular make sure that you understand the roles of different parties' public and private keys in providing confidentiality and message integrity. Also understand what different kinds of firewalls are and how their rule sets work to exclude or admit traffic.