Assignment #2 for Computer Networks (CNT 4004) <<<

Due September 26, 2017 at the start of class

This assignment covers material from chapter 2 of the textbook and from roughly the second two weeks of class lecture. Each problem is worth 25 points.

Problem #1

Answer the following short questions about protocols in general and application layer protocols specifically. Recall that the five elements of a protocol (from Holzmann 1999) are 1) service to be provided, 2) assumptions on environment, 3) vocabulary of messages to implement, 4) encoding of each message, and 5) procedure rules to guarantee consistency.

a) What are elements (1) and (2) for FTP?

b) Which of the five elements from Holzmann is arguably the most complicated to design and why?

c) Application layer protocols define four things. What are these four things?

d) How does Amazon use cookie technology? Describe by example.

e) What is the purpose of a conditional GET and how does it work?

f) DNS has three classes of servers – name and briefly describe them. DNS has four types of records – name and briefly describe them. Note that this is the kind of incredibly dry stuff you need to know (as in memorize) to pass the CompTIA Network+ certification exam.

Problem #2

Read the short section on the “Clayton tunnel accident” in the week #3 readings (on the readings page on the class website). Then, answer for following two questions.

a) Whose fault is the accident? Or was no one at fault? Carefully justify your answer. “Fault” assumes that something could have been done to prevent the accident (otherwise it would have been deemed an act of god).

b) How could the protocol have been feasibly designed to prevent the accident? That is, propose a fix to the protocol.

Problem #3

How are Email and DTNs similar in concept (or “big idea”)? DTN is Delay (or Disruption) Tolerant Network. DTNs are, oddly enough, not covered in the textbook so you will have to dig a little. This is a very simple idea, you do not need to go into the weeds for the answer.

Problem #4

Every student who has taken a Networks course has to, at some point or another, decode a packet from raw hex. This is laborious to do, but very educational. So, here below is a packet sniffed from an Ethernet network. Your job is to decode it and answer the below questions. You can find packet header formats on Wikipedia.

```
00 00 0c 07 ac 00 48 4d 7e b5 fb ea 08 00 45 00
03 64 57 df 40 00 80 06 00 00 83 f7 03 de d8 3a
db 44 f6 c5 00 50 25 0f e0 cd 61 90 ac a9 50 18
01 02 3e ab 00 00 47 45 54 20 2f 20 48 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 0d 0a 55 73 65 72
```
What is the Ethernet destination and source address (in hex)?

b) Identify the vendor of the equipment of the sender?

c) What is the protocol type (in the Ethernet header)?

d) What version of IP is this?

e) What are the IP destination and source addresses (give in proper dotted decimal notation)?

f) Identify if the transport protocol is TCP or UDP.

What are the transport protocol destination and source port numbers (in decimal)?

h) What is the application protocol (be sure to give the version number)?

i) What is the function being performed at the application layer (that is, what is the purpose of this packet)?

j) What are the checksum values for all protocols that have a checksum in this packet? Note that a CRC is not a checksum.

k) Explain the IP checksum. Here is a hint, the trace was taken in the sending host and not “on the wire”.

Note:
The TA and I are here to help you! Make use of help if you need it.