PUT YOUR NAME HERE

PUT TODAY’S DATE HERE

# COMP 204 Homework 2

Answer the following questions based on your reading of the text book, the module key points, and the instructor’s presentation this week.

1. **[4 points]** Domain Name Service (DNS) performs the translation of web names to IP addresses.

Bring up a command window and enter the commands in yellow:

C:\>nslookup

Default Server: some.server.name.here

Address: W.X.Y.Z

> set debug

> set recurse

> www.amazon.com

* Insert a screen shot of the results.
* Explain in general the steps of how your computer finds the correct address for [www.amazon.com](http://www.amazon.com).
* What is the name server your machine consults?
* What is one authoritative name server for www.amazon.com?
* How long can that name be cached?
1. **[3 points]** What is a “port” in TCP and UDP?
2. **[5 points]** Describe the purpose of “windowing” in TCP/IP connections and its relationship to throughput, reliability, and retransmission.
3. **[5 points]** Explain the differences between TCP and UDP in terms of characteristics and the ISO Layers used. Where would you use TCP and where would you use UDP?
4. **[3 points]** It is said that TCP offers “reliable” transport and UDP does not. In this context, what does “reliable” mean? Can you build “reliable” services on top of UDP?
5. **[4 points]** Explain how the TCP synchronizing handshake works. Why does UDP not have a similar handshake?
6. **[6 points]** Using your Virtual Machine setup from Lab 1, capture the packets (using Router 0) in the conversation between PC0 and cs.franklin.edu as you visit <http://cs.franklin.edu/~whittakt/http/> (using PC0). Examine the capture in Wireshark. Filter on the HTTP protocol only. Insert a screen shot of Wireshark showing these packets. What does the HTTP protocol look like? Draw a diagram showing the back-and-forth messages. What ports are being used for communication? What transport layer protocol is being used? Hint: see <http://wiki.wireshark.org/DisplayFilters> for details on how to filter in Wireshark.