Network Programming (ECE-C433)

Programming Assignment #2 (HW2)

Due February 16, 2012, 11:00am

Mandatory Requirements:

- For every problem you work on, you are required to save it in folder HW2 in your home folder on SPIRIT. For example, Problem 1a from HW2 must be saved in folder HW2 as p1a.c. The code must run on SPIRIT (129.25.36.57). The name of the executable must be of the form pXY where X is the problem number and Y is the subpart. This will help me in scripting things if I need to.
- All code should be on the server by the given deadline. Server will be offline after the deadline.
- All your work should be original.

Notes:

- Your login name is your full first & last name together, and your password is ecec433. Please change your password after you log in.
- When compiling, use the -lpcap compilation flag: gcc -lpcap file_name.c
- To run, remember to use sudo for root priviledges: sudo ./a.out

---

Problem 1. Sniffing Basics (2+3+10+10). This exercise is intended to get your packet capture instincts warmed up. Write a program to:
a Find the devices available on your system for sniffing.
b. Show the network address and mask on which the system resides.
c. Sniff packets on an interface for a user-specified amount of time. The user-specified duration should be accepted as a command line argument. For every packet captured, a counter should be incremented and shown as output on the screen.
d. Obtain separate graphs that show the number of packets captured every minute, second and milli-second, respectively. In other words, I expect three plots, the y-axis of all should show the number of packets. The x-axis of the first plot should be minutes, the second plot should be seconds and the third one should have milliseconds as the units of the third. Sniff for 5-10 minutes (Hint: Look at the graphs on the Lec1 slides to get an idea).
e. For each of the above graphs, plot the CDF (cumulative distribution function) of captured packet sizes.

Problem 2. Link Layer (5+10+10). Write a packet capture engine to do the following:
a. Sniff packets on an interface for a user-specified time. For every packet captured, printout on the screen the following information in the following order:

- Destination address in Hex.
- Source address in Hex.
- Type of payload in ASCII.

b. Capture packets for 60 seconds using this code and report a distribution of the type of payload carried by the Ethernet Frame. Do not make your own Ethernet frame structure, use the one located in /usr/include/net/ethernet.h file.
c. Start a packet capture, initiate either an ssh/sftp/HTTP session and give a trace of the packets which are related to the machine you are sniffing from. Set the promisc flag in pcap open live() to 0 and 1 and report the difference (Tip: To initiate an HTTP session, type in lynx on the CLI of the sniffing server to use the classic text based browser. Lynx is a very old and one of the first HTTP text browsers from the days when the Internet was completely text based. See the menu on the bottom of the lynx screen to use it.).

Deliverables:

- Hardcopoy of good commented code.
- Output (no screenshots necessary).
- Explanations where required (Short and to the point).
- Plots where required.
- Be green, keep number of pages down to a minimum.

Credit Basis:

- Code runs on SPIRIT.
- Good commenting.
- Efficient coding techniques (such as modularization etc.).
- Initiative to show something useful and interesting.
- DO NOT just copy and paste the sample code provided.