Lab01:TCP/IP overview

NSL, Mon, 30th July 2012

Objective:

1. Get acquainted with some commonly used networking commands
2. Preview some TCP/IP diagnostic tools.
3. Understand the concept of layering/encapsulation by looking at link, IP and TCP headers.

General instructions

1. This lab is to be done in groups of two students
2. Create a directory called <rollnumber1>_<rollnumber2>_lab01. Open a file "lab01.txt" inside the directory using a text editor. As you proceed with the lab instructions below, for each exercise, note down the answers to the exercise along with any interesting observations in the file. ***Take care to ensure that the content in the file is neatly organized***. You will be submitting this file for grading at the end of the lab.
3. Apart from the above file, you may have to submit some code, along with input/output files. The details for this are specified in the respective exercises.
4. At the end of the report, Against your name: include in % your and your partner's contribution to the lab. Eg. ABC: ABC 100%, XYZ 80%; XYZ: ABC 100% XYZ:100%

Lab instructions:

Exercise 1: Popular Network Commands

Read the man pages for the following commands:

arp ifconfig route

host ping tcpdump wireshark

Study the different options associated with each command. Throughout the CS378 lab, you will use these commands extensively. You can also execute the first row commands, without arguments and see what they output.

Report: Explain what the above commands do in 2-3 sentences (per command).

Exercise 2: Network Configuration Files

Explore the following network configuration files and **answer the following questions in the report.** You can also browse the web to get information about these files.

1. /etc/hosts
   - What is the purpose of this file? Explain the meaning of the first two lines in the file.
2. /etc/network/interfaces
   - What is the IP address and gateway associated with your computer? How was this IP address obtained?
3. /etc/resolv.conf
   - What is the purpose of this file? What is the IP address of the local DNS nameserver
4. /etc/protocols
   - What does this file list? What are the numbers associated with tcp, udp and ospf?
5. /etc/services
   - What are the port numbers used by ssh, telnet, ftp, http, nfs, smtp, pop3, imap? The last 3 protocols are used for email.

Exercise 3: Encapsulation/DeMultiplexing

Tcpdump and wireshark are two very useful network diagnostic tools. In this exercise, we will use these tools to understand encapsulation and demultiplexing. We will use tcpdump to capture packets containing different headers (Link, IP, TCP) on your ethernet interface and then use wireshark to analyze the captured packets.

Your job is to capture only those packets that are exchanged between your computer and the CSE webserver, when you download my webpage http://www.cse.iitb.ac.in/ In one terminal, run the tcpdump command with appropriate filters (use -n option to avoid name lookup). Store the packets in a trace file titled 'exercise3.out'. There is typically lot of background traffic on the computers, the trace file should NOT capture these packets. In another terminal run "wget http://www.cse.iitb.ac.in/". Wget is a command line utility that downloads webpages much like firefox. You could also use firefox, but this is cleaner and simpler.

You can now use wireshark to evaluate the packet trace captured by tcpdump. Run "wireshark -r exercise3.out". Explore the different packets captured by clicking on the individual packets. Also note the sequence of packet exchange.

For your report, you will need to submit the Link, IP and TCP headers of one packet. For this,
* Select the first TCP packet listed. Then go to the edit menu and choose mark packet.
* Go the file menu and choose print. Select "plain text", output to file (give file name as headers.txt). Select marked packets only, all expanded. Click on print, the output should get dumped to the headers.txt file.

Answer the following in the lab report.

1. Refer to the figures of Link, IP and TCP headers as shown in class (lab-overview.pdf). Fill in the values of all the header fields in hexadecimal format for each header i.e one for Link, one for IP and one for TCP.
2. What are the fields used at the link(Ethernet), IP and TCP headers to demux the packet? Specify the values of these fields in decimal format and the corresponding process(protocol) the packet is passed to. Verify these values with what you observed in the /etc/protocols and /etc/services files.

Apart from the above reporting, also add the "exercise3.out", "headers.txt" file to the directory.

<The End>

The directory named <rollnumber1>_<rollnumber2>_lab01 that you will submit should contain the following files:

1. lab01.txt
2. exercise3.out
3. headers.txt

Now tar it as follows:
tar -zcvf <rollnumber1>_<rollnumber2>_lab01.tgz <rollnumber1>_<rollnumber2>_lab01/

Submit the file <rollnumber1>_<rollnumber2>_lab01.tgz via moodle for grading.