Lab01: Overview of Networking Tools
OSL, Thu Jan 14, 2016

Objective:

1. Get acquainted with some commonly used networking commands and TCP/IP diagnostic tools.
2. Understand the concept of layering/encapsulation by looking at Link, IP and TCP headers.
3. Understand the concept of multiplexing using Ethernet "frame type" field, IP "protocol field", transport "port number" field.
4. Understand how some commonly used metrics like throughput, delay are calculated.

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. For each exercise I have also provided an approximate time it would take to complete. This is already a bit exaggerated, so do ensure you finish before this.
4. In some of the exercises, I will specify a goal. You job is to design an experiment that meets the goal, conduct it and answer the questions asked.

Lab instructions:

Exercise 1: Play Time **[0 Marks, 45 Min]**

Useful Reference: Man pages and http://danielmiessler.com/study/tcpdump/

Play around with tcpdump, wireshark, ping, arp, route, ifconfig, host
Look at /etc/hostname; /etc/hosts; /etc/network/interfaces; /etc/resolv.conf; /etc/protocols; /etc/services and understand what the files are for.

Lots of new stuff. Many things you will definetly not understand since theory will be covered much later but we have to start somewhere. Don't worry about it, practice makes it perfect (over time). We will reuse many of these tools again and again over many labs.

At the end of this exercise, you should have some basic understanding of how a host manages network information as well as gain some experience on using networking tools.
You should be able to collect a trace via tcpdump and view the trace in wireshark (using the -r option).

Exercise 2: Simple Stuff **[10 Marks, 15 Min]**

1. Whats your machine's host name and IP address? How did you get this information?
2. What is the next hop router's IP address and MAC address? How did you get this information?
3. What is the local DNS server's host name and IP address? How did you get this information?
4. What do the numbers in the file /etc/protocols represent?
5. What is the port number associated with applications: ssh, ftp, nfs, smtp (email)? How did you get this information?

Exercise 3: Encapsulation and Demultiplexing **[12 Marks, 40 Min]**

Goal: To understand layering and demultiplexing, Hari Puttar wants to capture packets. He also wants to understand how web flows operate at the same time. So, help him design an experiment that captures only those packets that are exchanged between his machine and IITB web server when he clicks the url http://www.iitb.ac.in/.

Guidance: Use wget to download the url. You could also use firefox/chrome, but this is cleaner and simpler. Your trace should not capture any background traffic. Before answering the questions, explore different packets by clicking on the individual packets. Also note the sequence of packet exchange.

Report:

1. Explain your design by specifying the exact commands (with options) you will run and in which order. Avoid description unless absolutely necessary.
2. Select the first TCP packet listed.
   a) Which next-hop node is it destined to? Specify the next-hop node's MAC and IP address. How did you determine this information?
   b) Who is the packet's final destination? Specify the final destinations' MAC and IP address? How did you determine this information?
   c) What are the fields used at the link(Ethernet), IP and TCP headers to demux the packet at the destination? Specify the values of these fields in decimal format and the corresponding process (protocol) the packet is passed to.
3. Apart from the above reporting, name your trace file as "exercise3.pcap" and add the file to your roll-number directory.

Exercise 4: More DeMultiplexing **[12 Marks, 40 Min]**

Goal: With the success of the previous experiment, Hari Puttar now wants to capture and examine different types of traffic, basically arp, ICMP (protocol used by ping) and ssh. He wants to capture all of the above in just one single trace. Help him design an experiment to do the same.

Guidance: In wireshark, click on the protocol field to order the packets according to the protocol.

Report:

1. Explain your design by specifying the exact commands (with options) you will run and in which order. Avoid description unless absolutely necessary.
2. Arp protocol: Click on any one of the ARP packets.
   a) Trace the flow of this packet up the protocol stack i.e specify what all processes/protocols handle this packet.
   b) What is the value of the field used in Ethernet header to pass packets to the ARP module? Express it in decimal format.
3. ICMP protocol: Click on any one of the ICMP packets.
   a) Trace the flow of this packet up the protocol stack i.e specify what all processes handle this packet.
   b) Expand the "Ethernet" header. Which higher level process (protocol) is this packet passed to and what is the value in decimals?
   c) Expand the IP header. What is the value of the field used in this header to pass packets to the ICMP module? Express it in decimal format.
4. SSH protocol: Click on any one of the SSH packets.
   a) Click on the IP header field. Specify the source and destination IP addresses.
   b) Expand the TCP header. Specify the source and destination port numbers.
   c) Which machine (IP address) is the SSH server? Hint: SSH server's listen on designated ports as specified in /etc/services.
5. Name your trace file as "exercise4.pcap" and add the file to your roll-number directory.

Exercise 5: Metrics **[6 Marks, 30 Min]**

Goal: Hari Puttar has heard of the terms throughput and delay and want to measure them via an actual experiment. To measure throughput, he wishes to download an mp4 file and see how fast the download happens on his network interface. And to measure delay, specifically round-trip delay, he wishes to send a packet to a neighbor and see how long it takes for an acknowledgment to come back for the packet. Design an experiment for him to achieve this.

Guidance: Use wget and ping for these experiments. You can find some mp4 files at http://bodhitree1.cse.iitb.ac.in/media/static/video/goals-1.mp4 or http://bodhitree1.cse.iitb.ac.in/media/static/video/Motivation-new.mp4

Capture all required data for measuring throughput and delay in one trace file. Also look in detail at packets labelled as HTTP.

Report:

1. wget displays something like the following after the download.
   100%[==>] 3,33,92,010 11.2MB/s in 2.8s
   X Y Z

   Looking at the captured trace, can you explain how the X, Y and Z were determined/calculated by wget.
2. What is the throughput of the download expressed in Mbps? Are you connected to a 10Mbps Ethernet or 100Mbps Ethernet LAN?
3. Ping displays something like this "64 bytes from 10.129.1.153: icmp_seq=1 ttl=64 time=0.739 ms" Can you look at the trace and determine how the "time" value was calculated by ping?
4. DO NOT include your trace file in the directory since the file size can be large.

Wrap up **[10 min]**

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

1. lab01.txt
2. exercise3.pcap
3. exercise4.pcap

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

Submit the file <rollnumber1>_<rollnumber2>_lab01.tgz via BodhiTree1 (under assignments) for grading.