Computer Networks Lab (CS 212)

Lab Assignment – 1

Introduction to Networking Tools

1. **Background**:

In this experiment, you will learn about some network communication utilities in Linux. When you work in a distributed environment, you need to communicate with remote users and you also need to access remote Unix machines. There are several Unix utilities that help users compute in a networked, distributed environment.

You will learn to use the utilities **ping, route, traceroute, arp, ifconfig, host,**
and nmcli. Read more about 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.

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

Useful References: Read Unix man pages.

2. **Warm-up Questions**

1. What is your machine's hostname 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 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?
6. How many of these questions can you answer for the phone? (android / iOS)

3. **Questions:**

1. **Goal:** The Unix utility Ping can be used to find the RTT to various Internet hosts.
   Read the man page for ping, and use it to find the RTT to various websites that
   may be of interest to you. You may also try the following websites: www.iitb.ac.in, www.cse.iitb.ac.in, gymkhana.iitb.ac.in.

   Report
   (a) Explain the results that you obtain; For example, the success and failure of the Ping,
   (b) What are the reasons for the values of RTTs that you see.

2. Read the man page for the Unix utility Traceroute and use it for the websites
   that you pinged in the previous experiment.

   Report:
   (a) Explain what you see. Whenever successful, draw a network map from your
   machine to the destination, which includes the hop addresses obtained from
   Traceroute.
   (b) How can you change the maximum hop number?
   (c) What do the three timestamps signify in the result of Traceroute?
   (d) What is the use of TTL (Time To Live) field in ICMP packets?

3. **Goal:** Look at the following files and understand what they are for **/etc/hostname**
   /etc/hosts /etc/network/interfaces /etc/resolv.conf
   /etc/protocols /etc/services

   Report:

   (a) What's your machine's hostname and IP address? How did you get this information?
   (b) What is the next hop router's IP address and MAC address? How did you get
   this information?
   (c) What is the local DNS server's IP address? How did you get this information?
   (d) What do the numbers in the file /etc/protocols represent?

(e) What is the port number associated with applications: **ssh, ftp, nfs, smtp** (email)? How did you get this information?

4. **Goal:** Familiarize with the Wireshark interface. Open Wireshark on your Linux machine and start a browser, in the browser go to the http://www.iitb.ac.in/. After your browser has displayed the http://www.iitb.ac.in/ page, stop Wireshark packet capture by selecting stop in the Wireshark capture window. This will cause the Wireshark capture window to disappear and the main Wireshark window to display all packets captured since you began packet capture.

Guidance:

Color Coding: You will see packets highlighted in green, blue, and black. Wireshark uses colors to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems - for example, they could have been delivered out-of-order. You now have live packet data that contains all protocol messages exchanged between your computer and other network entities! However, as you will notice the **http** messages are not clearly shown because there are many other packets included in the packet capture. Even though the only action you took was to open your browser, there are many other programs in your computer that communicate via the network in the background. To filter the connections to the ones we want to focus on, we have to use the filtering functionality of Wireshark by typing **http** in the filtering field. Notice that we now view only the packets that are of protocol **http**. However, we also still do not have the exact communication we want to focus on because using http as a filter is not descriptive enough to allow us to find our connection to http://www.iitb.ac.in/. We need to be more precise if we want to capture the correct set of packets. To further filter packets in Wireshark, we need to use a more precise filter. By setting the **http.host==www.iitb.ac.in**, we are restricting the view to packets that have as an http host the www.iitb.ac.in website.

Now, we can try another protocol. Let's use the Domain Name System (DNS) protocol as an example here. Let's try now to find out what are those packets following one of the conversations (also called network flows), select one of the packets and press the right mouse button. Click on Follow UDP Stream.

Report:

(a) Carefully read the lab instructions and finish all the tasks above.
(b) If a packet is highlighted by black, what does it mean for the packet?
(c) What is the filter command for listing all outgoing http traffic?
(d) Why does DNS use Follow UDP Stream while http use Follow TCP Stream?

4. **Submission Details:**

Make a directory and submit the screenshots of the results obtained in the Question No.1 & 2(please name the screenshot with corresponding question number like 1.a or 3.3.b or 2.2.a). Also, Submit also the additional report files.

Now tar your screenshots and report (result folder) as follows:

tar -zcvf < rollnumber > _lab01.tgz <Result Folder/Directory >

Submit the file < rollnumber > _lab01.tgz for grading

After completing all the tasks please show it to us. Once the result is correct then only we allow you to upload to the moodle.