ECE 361 Lab #2: TCP/IP Utilities

Overview

In this lab you will learn to use several of the TCP/IP utilities, which enable you to discover information about IP hosts and domains and to measure Internet performance.

Pre-lab

PING is an application used to determine whether a host is online and available. *PING* uses the Internet Control Message Protocol (ICMP). It sends ICMP Echo messages to a specified host requesting a reply. *PING* can be used to measure round-trip delay between two hosts. The simplest way to use *PING* is as follows:

```
ping <hostname>
```

Tip: When using ping consider adding the ***–c*** option which allows you to set the number of echo requests.

TRACEROUTE is a tool that allows users to determine the route that a packet takes from the local host to a remote host, as well as latency and reachability from the source to each hop. *TRACEROUTE* uses both ICMP and UDP. It can also use TCP to perform the operations. *TRACEROUTE* can be used by entering the command: **`traceroute <hostname>`**

NETSTAT queries a host about its TCP/IP network status including network drivers and interface cards, routing table information and active TCP connections. **Read section 2.5.3 to learn more about the above utilities.**

NSLOOKUP is a tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping. **HOST** and **DIG** are alternative approaches to **NSLOOKUP**.

IP is another tool that allows you to show/manipulate routing, devices and policy routing. The *IP* tool has an extensive set of commands and options available.
For more information regarding the above mentioned tools, refer to their manual pages in Linux by typing:

```
man <tool name>
i.e. man nslookup
```

Exercises

These utilities can be invoked using the command line interface. Begin by opening up a **Terminal** session and trying each of the above commands and examine the output. Answer the following questions:

1. Briefly describe how ping uses ICMP to find out about IP hosts and the information that it collects.
2. Briefly describe how traceroute uses UDP and ICMP together to determine a route to a specified host.
3. Use ping to find values for minimum, average and maximum round trip time to www.utoronto.ca. Compare this to the min/avg/max round trip time to www.163.com (free e-mail service in China). What causes the difference in round trip time to the two servers?
4. The distance from Toronto to China is approximately 10,000 km. If light travels at 3x10^8 m/s what is the approximate minimum round trip time from your machine to www.163.com? Compare this to the average round trip time found in question 1. Explain your findings.
5. Estimate the round trip ping time to www.bbc.co.uk (British News site)?
6. Find the actual round trip ping time to www.bbc.co.uk and compare it to your estimate. Explain your findings.
7. Find the option in ping which lets you change the packet size. Now ping a machine with 10 byte packets and repeat for 10,000 byte packets and compare the round trip times.
8. What is the default packet size for ping?
9. Issue the following command to find the server hosting the Harvard website: `nslookup www.harvard.com`
   - The first part of the response informs you which DNS server handled your request
   - The second part informs you of the IP address corresponding to the domain you queried
   - What is the IP address of the DNS server you queried and what is the IP address of the server hosting **www.harvard.com**?
10. Use the traceroute command to find the # of hops to the DNS server and web server you found in question #2. What is the reason for the difference in number of hops? Is the DNS server likely a Local Name Server or a Root Name Server?

11. Use the command: **`netstat --tcp`** to find the number of active TCP connections on your machine.
12. Open a browser and connect to www.cnn.com. Now issue the same command as in question **11** and find the TCP entry corresponding to your new http session. Explain your findings.
13. Use the command: **`netstat --statistics`** to answer the following questions:
    a) How many ICMP echo requests did your machine receive?
    b) How many ICMP echo replies did your machine send?
    c) How many UDP packets to unknown ports did your machine receive?
14. Use the command: **`ip addr`** to find the Ethernet address and IP address of your machine. What are the addresses?
15. Perform an **`nslookup`** on the IP address of your machine to determine the hostname of your machine. What is the hostname?
16. Use the command: **`ip route show`** to inspect the local routing table. There should be two entries. Explain what each of the entries means.

Demonstration

Once you have completed the exercise questions, **signal to the Lab TA that you are ready to perform the demo**. Each student in the group may be asked questions about the TCP/IP utilities or asked to perform a specific operation using the tools in order to demonstrate understanding of the lab.

Submission Instructions

You must submit the answers to the questions in the Exercises section in a text file. The file must be named **exercises_lab2.txt**. This file must also contain the names and student numbers of the group members (at the beginning of the file) prefixed by #. Please do not prefix other lines by # as this would confuse the automated scripts.

```
#first1 last1, studentnum1
#first2 last2, studentnum2
```

Note: Only one student in the group needs to submit. You can submit the file using the following command:

```
submitece361s <lab_number> <filename>
```

Example: `submitece361s 2 exercises_lab2.txt`

You can verify if you have submitted successfully by using the following command: `submitece361s -l 2`

For more information regarding the command, please refer to it’s man page: `submitece361s`

The submitted files will be used to verify your answers and check for plagiarism.

Marking

This lab is worth a total of **3 marks** with the following break down:

- Exercises: **2** marks (marked as group)
- Demonstration: **1** mark (marked individually)

All marks will be assigned by the end of the lab session.