ECE4436A–NETWORKING: PRINCIPLES, PROTOCOLS, AND ARCHITECTURES

Laboratory 1: Network Tracing

Objectives:
 This lab exercise will familiarize you with the network utilities such as *ping* and *traceroute*. Ping is often used for network testing, measurement, and management. Traceroute will help you gain a better understanding of the organization of the Internet.

Equipment: Windows workstation and Internet access.

Schedule:
TAs will be available at TEB 244 during your assigned lab hours to answer your questions. You are required to demonstrate and discuss your work based on the lab checkpoints times to your TA and make sure that the TA add check mark in his/her follow-up sheet. Lab reports are due Friday October 2, 2015 at 11:59 pm.

Background:
Ping is a basic Internet application that lets you verify that a particular network host is online and available. It got its name from the SONAR signals used to locate underwater objects. Ping can test basic connectivity between two hosts on a network. Ping makes use of the layer three **I**nternet **C**ontrol **M**essage **P**rotocol (ICMP) to send ICMP_ECHO requests and receive ICMP_RESPONSE replies. Since the TCP/IP protocol suite incorporates ICMP, any workstation with TCP/IP installed can reply to ping. It also provides a measurement for round trip time (RTT), making performance measurements somewhat easier to record. The command in its simplest form is **ping <hostname>**.

Traceroute is a tool to help debug network route problems. It allows users to determine the route taken by a packet from the local host to a remote host, as well as latency and reachability from the source to each hop on the route. It uses ICMP and the **t**ime-**t**o-**l**ive (TTL) field in the IP header. The TTL field is used to prevent routing loops that can sometimes occur on networks. If the TTL is 0 or 1, the router is supposed to return the ICMP datagram to the originating host with ICMP_TIMXCEED message. The router appends its IP address as the source address for the error message. As each router on a route receives the traceroute ICMP packet, it decrements the TTL by one; effectively making TTL a hop count parameter. Using this methodology, the traceroute program sends out a packet to the first router in the sequence with a TTL of 1. The router decrements the TTL and returns an error message, but reveals its IP address. Traceroute records this, sends out another ICMP echo request, but this time with a TTL of two. This will get to the second router in the sequence and the process repeats until each router is identified and the destination host is reached. Read section 1.4.3 on "Delay and Routes in the Internet" from the Ross-Kurose textbook.

Procedure:
   a. Use **ping** and **tracert** on your workstations to familiarize yourself with these commands. Also search for these terms in the Internet Encyclopedia. List a few of the flags that are used with these two commands. (7)

1- Ping your workstation's loopback interface using the command: (3)
      `ping localhost`   or   `ping 127.0.0.1`
It is a good way to test your machine's basic network configuration.
Was the ping successful? If the ping is successful, then TCP/IP is properly installed and functioning on this workstation.

2- Ping your default gateway and your DNS server. Use the *ipconfig* command on your Windows workstation to identify your DNS server and your default gateway. (3)

b. Use ping to measure Round Trip Time (RTT) for 10 messages of size 64, 256, and 4096 bytes. Graph (10 each plot) the message size versus RTT for:
1- two hosts on a LAN (two workstations in the lab or in your house)
2- two nodes on a WAN (for instance, your workstation and a host in East Asia)
Analyze your results. Discuss the effects of distance (3), message size (3), and their relationship with bandwidth and latency.

c. Use the *tracert* utility on your lab workstation to find the route to a host:
1- in another city in Ontario (3)
2- on the east or west coast of Canada (3)
3- outside Canada (3)
Analyze your results. (e.g. How many hops did it take to reach the destination host? (3) How many ISPs did you traverse? Why do you see "* * *" (3) on some of the output lines?)

d. Use the trace route utilities at the site www.traceroute.org to find the routes between two hosts on different continents. Trace the route again between these two hosts after at least an hour. Provide reasons why the two routes could differ. (4)

e. Briefly discuss why **ping** would not necessarily provide an accurate estimate of the round trip time for packets exchanged by two hosts on the Internet? (4)

f. Another useful tool/utility that is helpful in network performance monitoring is **netstat**. What information does it provide? List at least three other such utilities and briefly describe their use. (14)

g. Briefly describe the Multi Router Traffic Grapher (MRTG) tool and its use in network traffic analysis. How is this tool being used by ITS at UWO? (7)

h. What is an "Internet traffic report"? What types of data are gathered by Internet sites that provide these reports? (7)

Note: You may use a UNIX workstation in one of the UNIX labs rather than a PC for this exercise.

Lab Report:
Write a report that describes the experiments you carried out (including the sites you visited) and your analysis of the output from the various experiments. Include your comments regarding the various utilities. Attach samples of some of the output results. Answer the following in your lab report: What did learn from this lab? Where/when did you have difficulties? (10)

APPENDIX A: References

Internet Encyclopedia

http://www.whatis.com/

http://www2.rad.com/networks/1997/nettut/mainmenu.html

Traceroute

http://www.traceroute.org/

http://www.networkingfiles.com/PingFinger/Neotraceexpress.htm

Internet Topology and Internet Traffic Statistics

http://www.caida.org/

http://www.cybergeography.org/statistics.html

http://www.internettrafficreport.com/main.htm

Multi Router Traffic Grapher (MRTG)

http://people.ee.ethz.ch/~oetiker/webtools/mrtg/index-2.html

http://www.uwo.ca/its/network/backbone/mrtg/

http://mrtg.largnet.on.ca/index.html

Other useful references

http://manuel.brad.ac.uk/BEGIN/nettrain/index.htm

http://www.techtutorials.com/Networking/General/

http://www.isoc.org/

http://www.ietf.org/

http://www.w3c.org/

APPENDIX B: A few useful network commands in Windows/Unix

	Windows	Unix
1	ping	ping
2	finger	finger
3	ipconfig	ifconfig
4	tracert	traceroute
5	telnet	telnet
6	arp	arp