Assignment 1
Network Programming

(Networking Tools)

Q1. The Internet Ping command bounces a small packet(s) to test network communications. Then tells how long these packet(s) took to make the round trip. The Internet Ping program works much like a sonar echo-location, sending a small packet of information containing an ICMP ECHO_REQUEST to a specified computer, which then sends an ECHO_REPLY packet in return. Explore more about the PING command and answer the following questions (Unix version only):

a) What is the option required to specify the number of echo requests to send with ping?

b) What is the option required to set time interval (in seconds), rather than the default one second interval, between two successive ping ECHO_REQUESTs?

c) What is the command to send ECHO_REQUEST packets to the destination one after another without waiting for a reply? What is the limit for sending such ECHO_REQUEST packets by normal users (not super user)?

d) What is the command to set the ECHO_REQUEST packet size (in bytes)? If the PacketSize is set to 64 bytes, what will be the total packet size?

Q2. Select five hosts of your choice in the Internet (mention the list in your report) and experiment with pinging each host 20 times (i.e., one invocation with 20 ECHO_REQUESTs) at three different hours of the day. Check if there exist cases, which shows packet loss greater than 0% and provide reasoning. Find out average RTT for each host and explain whether measured RTTs are strongly or weakly correlated with the geographical distance of the hosts? Pick one of the above used hosts and repeat the experiment with different packet sizes ranging from 64-bytes to 2048-bytes. Plot the average RTT and explain how change in packet size and time of the day impacts RTT.

You can use these online tools http://www.spfld.com/ping.html or http://ping.online-domain-tools.com/ for this experiment.

Q3. Select an IP address of your choice. Capture the outcome of 1,000 ping ECHO_REQUESTs in to separate files by executing the following ping commands.
- ping -n <IP Address>
- ping -p ff00 <IP Address>

Come up with a method to read and analyze the observations captured in the files and answer the following questions. You are free look for a tool, programming/scripting language that is best suitable for the task and learn just enough of it to get analysis done.

(a) What was the packet loss rate for each command?
(b) What was the minimum, maximum, mean, and median latency/Round Trip Time (RTT) of the pings that succeeded? Ignore pings that failed in the calculation.
(c) Plot graphs to visualize the normal distribution of the ping latencies. The goal here is to find a method to present the data in a way that is clear and easy to understand.
(d) Describe the significant network behavior you observed between the two experiments. The two scenarios were set up to be very similar except for two aspects. Describe your answer precisely, as best as you can.

Q4. Capture the output of *ifconfig* with necessary options, and identify and explain as much of what is printed as you can. Explain the output of route command and its options.

Q5. What is *netstat* and what is it used for? What parameters for *netstat* should you use to show all the TCP connections established? Include a printout of this list for your machine and explain all the fields. What does "*netstat*

–r" show and explain all the fields of output? What option of *netstat* can be used to display network interface status? By using *netstat*, figure out the number of interfaces on your machine. Show and explain the function of loopback interface.

Q6. Perform traceroute experiment (with same hosts used in Q2) at three different hours of the day to determine the routes used. Use any one of following online tools for this experiment:
http://network-tools.com, http://ping.eu and http://www.cogentco.com/en/network/looking-glass
1. List out the hop counts for each host in each time slot. Determine the common hops between two routes if they exist.
2. Check and explain the reason if route to same host changes at different times of the day.
3. Inspect the cases when traceroute does not find complete paths to some hosts and provide reasoning.
4. Is it possible to find the route to certain hosts which fail to respond with ping experiment? Give reasoning.

Q7. How do you show the full ARP table for your machine? Explain each column of the ARP table. Check and explain what happens if you try and use the "*arp*" command to add or delete an entry to the ARP table? Find out how to add, delete or change entries in the ARP table? Use this mechanism to add at least two new hosts to the ARP table and include a printout. How long do entries stay cached in the ARP table? Describe a trial-and-error method to discover the timeout value. What will happen if two IP addresses map to the same Ethernet address? Be specific on how all hosts on the subnet operate.

Q8. Local network analysis: Query your LAN using nmap to discover which hosts are online. Use a command such as: *nmap –n –sP <Subnet Range>*

You can choose a different LAN subnet address as well (make sure you report the same in your report explicitly). Now run the command repeatedly at different times of the day, and finds the number of hosts online. Do it for at least 5 times with sufficient time gap. Plot a graph against time to see if there are any hourly trends to when computers are switched ON or OFF in your LAN.