Assignment –1

CS 342: Networks Lab (September – November2020)

Instructions:

a) Make sure that you read, understand, and follow these instructions carefully. Your cooperation will help to speed up the grading process.
b) Following are generic instructions. Make sure that you also check carefully and follow any specific instructions associated with particular questions.
c) In this assignment, you will explore the various network diagnostic tools. An end user makes use of these tools to discover how a machine is connected to the network and how the network looks like beyond the first hop.
d) Solve the questions individually. Prepare a single report (PDF only) for all these experiments. The file name should be same as your roll number. Example:*180101001.pdf.* Once done, submit the report in Moodle on or before the submission deadline.
e) All the experiments need to be performed on a Unix/Linux-based computer (preferably Ubuntu 16 or newer).
f) Submission deadline: 11.59 pm, 20 September 2020 (Hard Deadline).
g) These are some additional formatting related information:
   - Make sure that you include your name and roll number on the first page of the report.
   - The font size of the report body should be a value from 10 to 12 points, and maximum line spacing is1.5.
   - Your grade is not proportional to the number of pages you submit.
   - Clear and concise writing is preferred.
   - Make sure that the report can be opened using any standard PDF viewer.
   - PDFs consisting of photographs of handwritten assignments will not be considered for grading.
   - Screenshots should be avoided unless there is a good reason to use them(or specifically mentioned in the question).
   - Please structure your report such that your answers are clearly indicated for each question of the assignment. The evaluator should not need to search for your answers.
   - The report should not contain more than **6 pages**(+1 page allowed in exceptional case).

Ethical Guidelines (lab policy):

h) **Deadlines**: Deadlines should be strictly followed. Assignments submitted after their respective deadlines will not be considered for evaluation.
i) **Cheating**: You are expected to do the complete assignments by yourself. Cases of unfair means and copying others' solutions will not be tolerated, even if you make cosmetic changes to them. If we suspect that this or any other form of cheating has happened, we are compelled to award NEGATIVE marks (equal to the maximum marks for the assignment).
j) **If you have problems meeting a deadline, it is much better to talk to the instructor about it than to cheat.**

Questions (Full Marks:40)

Q1. The Internet **Ping** command bounces a small packet(s) to test network communications, and then shows how long this 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 or GNU/Linux version only):

a) What is the option required to specify the number of echo requests to send with *ping* command*?* **(0.5)**

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?**(0.5)**

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 superuser)? **(0.5 + 0.5)**

d) What is the command to set the ECHO_REQUEST payload/data size (in bytes)? If the payload size is set to 32 bytes, what will be the total packet size? **(0.5 + 0.5)**

Total marks: 3

Q2. Select six hosts of your choice in the Internet (mention the list in your report) and experiment with pinging each host 25 times at three different hours of the day. You can use the following online tools for this experiment:

i) http://www.spfld.com/ping.html

ii) https://www.subnetonline.com/pages/network-tools/online-ping-ipv4.php

a) List out the average RTT for each host in tabular form, and explain whether RTT has a correlation with the geographical distance of the destinations from source. **(0.5+0.5)**

b) Check if in any case, packet loss is greater than 0% and provide reason for the same. **(1)**

c) Pick one of the above used hosts, and repeat the experiment with different packet sizes ranging from 64 bytes to 2048 bytes. Plot average RTT vs packet size. **(1)**

d) Explain how change in packet size, and time of the day impact RTT. **(1)**

Total marks: 4

Q3. Select an IP address of your choice (mention the address in your report) and capture the outcome of 1,000 pings in two separate files by executing the following *ping* commands.

- ping -n <IPAddress>
- ping -p ff00 <IPAddress>

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

a) What was the packet loss rate for each command? **(1)**
b) What was the minimum, maximum, mean, and median latency of the pings that succeeded? Ignore pings that failed in the calculation. **(2)**
c) Give plot to show the normal distribution of the ping latency. **(1)**
d) The two experiments are almost similar except in few aspects. Describe the significant network behavior difference (if any) you observed between the two experiments. **(1)**

Total marks: 5

Q4. With regard to ***ifconfig*** and ***route*** commands, answer the following questions:

a) Run *ifconfig* command and briefly describe its output (important attributes). **(2)**
b) What options can be provided with the *ifconfig* command? Mention and explain at least four options. **(1)**
c) Explain the output of *route command.* **(1)**
d) Mention and explain at least four options of the *route* command. Execute the *route* command with these four options and show the output. **(1)**

Total marks: 5

Q5. Answer the following questions related to ***netstat*** command.

a) What is the command *netstat* used for? **(1)**
b) What parameters for *netstat* should you use to show the established TCP connections? Include a screenshot of the command and output **(1)**
c) What does "*netstat –r*" show? Explain all the fields of the output. **(1)**
d) What option of *netstat* can be used to display the status of all network interfaces? By using *netstat*, figure out the number of interfaces on your computer. **(1)**
e) What option of *netstat* can be used to show the statistics of all UDP connections? Run the command on your computer and show the output. **(1)**
f) Show and explain the function of loop-back interface. **(1)**

Total marks: 6

Q6. Perform a **traceroute** experiment (with same hosts used in **Q2**) at three different hours of the day, and then answer the questions below. Use any one of the following online tools for this experiment:

- http://ping.eu;
- http://www.cogentco.com/en/network/looking-glass;
- https://www.ultratools.com/tools/traceRoute;
- http://network-tools.com;

a) What is the use of traceroute tool? **(1)**

b) List out the hop counts for each host in each time slot. Determine the common hops between two routes if they exist. **(1)**

c) Check and explain the reason, if route to same host changes at different times of the day. **(1)**

d) Inspect the cases when traceroute does not find complete paths to some hosts, and explain the reasons. **(2)**

e) Is it possible to find the route to certain hosts which fail to respond with ping experiment? Give reasoning. **(2)**

Total marks: 7

Q7. Answer the following questions regarding **ARP**.

a) How do you see the full ARP table on your machine? Explain each column of the ARP table. **(2)**

b) What command is used to add or delete an entry into the ARP table. Use this mechanism to add at least two new hosts to the ARP table and include a screenshot. **(1)**

c) Can there be an entry for any IP from different subnet in the ARP table of your PC? Explain your answer. **(2)**

d) Check and report what happens when you forcefully replace (using delete, add command of arp) the Ethernet address of an existing entry with the Ethernet address of another existing entry of the ARP table in your PC, and send ping to those IPs. Explain the behavior. **(1+2)**

Total marks: 8

Q8. Install network tool **nmap** in your PC and perform the following experiments:

a) What is the command to check which PCs of your sub-net are up? **(0.5)**

b) How to detect firewall settings of your own PC using nmap? **(0.5)**

c) Run the command of question (a) at least 6 different times of a day, and find the number of hosts online. Plot the number of on PCs vs time, to see if there is an hourly trend for when computers are switched ON or OFF in your LAN. **(1)**

Total marks: 2