CS 349: Networks Lab

(January-May 2020)

Assignment – 1

Instructions:

- Make sure that you read, understand, and follow these instructions carefully. Your cooperation will help to speed up the grading process. Thank you.
- Following are generic instructions. Make sure that you also check carefully and follow any specific instructions associated with particular questions.
- 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.
- Solve the questions individually. Submit a soft copy of the report, preferably PDF, on all these experiments. The file name should be same as your roll number. Example, *130101001.pdf or 130101001.docx.* Once done, submit the report in Moodle on or before the submission deadline.
- All the experiments need to be performed on a Unix/Linux-based computer (i.e. the operating system must be from the Unix or GNU/Linux family). Examples of recommended operating systems: Fedora, Ubuntu, Linux Mint, openSUSE.
- Submission deadline: **11:55 PM on Monday, 20th January 2020 (Hard Deadline)**.
- 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 is 1.5.
  - 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.

Note: The report should not contain more than **6 pages** (+1 page allowed in exceptional case). No need to describe how these tools work.

Ethical Guidelines (lab policy):

- Deadlines: Deadlines should be strictly followed. Assignments submitted after their respective deadlines will not be considered for evaluation.
- 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).
- If you have problems meeting a deadline, it is much better to talk to the instructor about it than to cheat.

Questions:

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?
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 32 bytes, what will be the total packet size?

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. Check if there exist cases, which show

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 impact RTT. 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

Q3. Select an IP address (e.g., 202.141.80.14) of your choice connected in the intranet (mention the address in your report). Capture the outcome of 1,000 pings in two 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 analyse 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?
b) What was the minimum, maximum, mean, and median latency of the pings that succeeded? Ignore pings that failed in the calculation.
c) Plot graphs to visualise 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 behaviour 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. With regard to *ifconfig* and *route* commands, answer the following questions:

a) Run *ifconfig* command and describe its output (identify and explain as much of what is printed on the screen as you can).
b) What options can be provided with the *ifconfig* command? Mention and explain at least four options.
c) Explain the output of *route* command.
d) Mention and explain at least four options of the *route* command. Execute the *route* command with these four options and show the output.

Q5. Answer the following questions related to netstat command.

a) What is the command *netstat* used for?
b) What parameters for *netstat* should you use to show **all** the established TCP connections? Include a screenshot of this list for your computer and explain all the fields of the table in the output.
c) What does "*netstat –r*" show? Explain all the fields of the output.
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.
e) What option of *netstat* can be used to show the statistics of all UDP connections? Run the command for this purpose on your computer and show the output.
f) Show and explain the function of loopback interface.

Q6. What is a **traceroute** tool used for? 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) List out the hop counts for each host in each time slot. Determine the common hops between two routes if they exist.
b) Check and explain the reason if route to same host changes at different times of the day.
c) Inspect the cases when traceroute does not find complete paths to some hosts and provide reasoning.

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

Q7. Answer the following questions with regard to network addresses.

a) How do you show the full ARP table for your machine? Explain each column of the ARP table.
b) 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 four new hosts to the ARP table and include a printout.
c) What are the parameters that determine how long the entries in the cache of the ARP module of the kernel remain valid and when they get deleted from the cache? Describe a trial-and-error method to discover the timeout value for the ARP cache entries.
d) 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 the *nmap* command to discover which hosts are online. Use a command such as: *nmap –n –sP <Subnet Range> (e.g., 172.16.112.0/26)*
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 find the number of hosts online. Do it for at least 6 times with sufficient time gap. Plot a graph against time to see if there are any hourly trends for when computers are switched ON or OFF in your LAN.