Assignment#3

Final Grade: 7% (100 points)

In this lab, you will get a chance to experiment with very useful and widely-used network diagnostic tools and commands.

Part A (20 points): Use the ping utility to measure the round-trip times to several hosts on the Internet. Note: Some firewalls may block ping requests.
The hosts are:

- www.google.com
- www.163.com (free e-mail service in China) or www.health.gov.au

Question 1: For each host: indicate what percentage of packets sent resulted in a successful response. For the packets from which you received a response, write down the minimum, average, and maximum round trip times in milliseconds.

Question 2: Explain the differences in minimum round-trip time to each of these hosts. Why did this happen? Explain your answer.

Question 3: What is the default packet size for ping? See your ping response.

Question 4: Find the option in ping which lets you change the packet size. Type ping and press enter to find the option required. Now, use this option to ping a machine with 10-byte packets and repeat for 10,000-byte packets, and compare the round-trip times. What did you observe? Why did this happen? You can ping any website/server.

Question 5. The distance from Fort Worth 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 ? Do calculations and compare this to the average round trip time found in question 1. Explain your findings.

Part B (10 points): For the following two hosts, indicate what percentage of the packets resulted in a successful response. Send minimum of 4 packets.

www.wits.ac.za (University of the Witwatersrand, Johannesburg)
www.intel.com

- For first host _____%
- For Second host _____%

Question 6: For some of the hosts, you may not have received any responses for the packets you sent. What are some reasons as to why you might have not gotten a response? (**Be sure to check the hosts in a web browser before listing the reasons.).** Write at least four reasons. Attach the screenshot.

Question 6.1: Ping 10.10.10.10 and then ping www.tcu.edu. What did you observe. Explain your findings.

Part C (20 points): Run a traceroute from your terminal/command prompt, through your routers, to the Internet and IP address 8.8.8.8. Redirect the output of the traceroute into a text file. You will find the file in the root of the current directory.

Redirection: use this command to capture the output of the traceroute command:

tracert 8.8.8.8 > traceroute.txt

Question 7. Use a text editor to add your name, email, and the date to the beginning of the captured file. The result should look similar to this screenshot. Submit this file along with your assignment file.

```
Tracing route to 8.8.8.8 over a maximum of 30 hops

  1     5 ms     1 ms     1 ms  10.65.56.1
  2     *        *        *     Request timed out.
  3     1 ms     1 ms     1 ms  2.ne.business.static.dsci-net.com [204.13.77.2]
  4     7 ms     6 ms     6 ms  161.ne.business.static.dsci-net.com [209.104.251.161]
  5     7 ms     6 ms     6 ms  be1.asbr1.bstpmallca.telepacific.net [66.81.211.18]
  6     6 ms     6 ms     6 ms  be1.asbr1.bstpmallca.telepacific.net [66.81.211.18]
  7     4 ms     5 ms     4 ms  bost-b1-link.ip.twelve99.net [213.248.66.186]
  8    13 ms    13 ms    13 ms  nyk-bb2-link.ip.twelve99.net [62.115.122.234]
  9    12 ms    12 ms    12 ms  nyk-b2-link.ip.twelve99.net [62.115.137.99]
 10    12 ms    12 ms    12 ms  72.14.218.254
 11    15 ms    14 ms    14 ms  108.170.248.65
 12    14 ms    13 ms    13 ms  172.253.70.13
 13    13 ms    13 ms    13 ms  dns.google [8.8.8.8]

Trace complete.
```

Question 8: Show the output of the traceroute command below (include screenshot). Describe what is strange about the observed output, and why traceroute gives you such an output. Explain your answer. Do a web search to find the answer.

tracert 18.31.0.200

Part D (10 points)**:** The Address Resolution Protocol is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address. This mapping is a critical function in the Internet protocol suite.

Run the arp –a command from your command prompt/terminal.

Question 9: What is the arp table for your local machine? Include a screenshot.

Question 10: What is the main function of ARP?

Part E (40 Points): Use the TCP/IP tools to answer the following questions.

Example: To obtain the IP address for your computer, at the command prompt/terminal, type ipconfig /all and press Enter. (Note: Unix/Linux user should use ifconfig). Do a web search to find commands suitable for your OS.

Question 11: Fill in the blanks. (10 Points)

- Physical address (MAC address):_____, the address embedded in your network card.
- IP address: _____, IP address is changeable, unlike the MAC address.
- Subnet Mask address: _____, subnet mask number tells your computer whether it is located on a subnetwork, a part of a larger network
- Default Gateway: _____ , computer or router that connect to the rest of the world, outside your subnet or LAN
- IP address of the DHCP server: _____ , server that issues IP addresses to any device.

Question 12 (30 Points): Answer the questions and attach a screenshot showing the use of the commands below. Do a web search to find the answers if required.

a) **Netstat**:
   a. How can **netstat** be used to display active network connections on a system?
   b. What does the **-n** option do in **netstat**?
   c. How can you filter **netstat** results to show only listening ports?

b) **Nmap**:
   a. What is the purpose of the **nmap** tool?
   b. How do you perform a basic port scan using **nmap**?
   c. Can you demonstrate how to use **nmap** to detect the operating system of a remote host?

c) **Dig and Nslookup**:
   a. What are **dig** and **nslookup** used for in DNS troubleshooting?
   b. How do you query DNS records for a specific domain using **dig** or **nslookup**?
   c. Can you perform a reverse DNS lookup using these tools?

d) **Netcat**:
   a. What is the **netcat** tool, and how can it be used for network troubleshooting?
   b. Demonstrate how to use **netcat** to check if a port is open on a remote host.

e) TCP/IP utilities, often referred to as network utilities, are a set of command-line tools that are indispensable for network administrators and security professionals. What are some ways in which TCP/IP utilities help in network security? Answer in 100-150 words.

Submission Instructions:

- Submit a filled pdf of this document including all the screenshots.
- Submit electronically through D2L.
- Email or hardcopy submissions will not be accepted.