Lab 3 – Network Diagnostic Tools

Write down the name of the equipment used in this lab:

Computer Name	
Start Time	

In this lab, we will learn more Network Diagnostic Tools such as ping, tracert, nslookup, arp, and we will also observe the network traffic at the same time to help you visualize packet content and network dialogue.

A. Network Diagnostic Tool: IPCONFIG

Login to a computer by clicking the CSIS student icon by using the following password: **STF@ll2016**
Run the Oracle VM Virtualbox program, double-click on Windows Server 2012 VM and login to the server (username: `administrator`, password: `Id0ntf0rget`).Go to View and click *Switch to Fullscreen* or simply press [RightCtrl] + F to switch to fullscreen. You can go back to the windowed mode any time by pressing [RightCtrl] + F.

Before you start the lab, make sure you have internet connectivity.

Open a command prompt window and enter the following commands at the prompt:

```
ipconfig /release
ipconfig /renew
```

The first command releases your current IP address and the second command requests a new IP address and configuration from a DHCP server on your network.

(Q.1). Record the following information:

Virtual server's IPv4 address	
Default gateway address	
Subnet mask	
DHCP server address	
DNS server address(es)	
MAC address (Physical address)	

B. Network Diagnostic Tool: PING

Ping (packet internet gopher) is a command-line diagnostic utility used to test network communications. It uses the ICMP protocol to ask another computer or network device (host) to reply to you. The general form of the PING utility is "`ping` address" where "address" can be an IP address such as 98.137.236.150 or a domain name such as www.langara.ca.
Open a command prompt and type **`ping /?`** to find out how to use the **`ping`** command.

The address 127.0.0.1 is called the "loopback address". It is a special address that refers back to the computer you are using. You can use PING with the loopback address to test your TCP/IP set up.

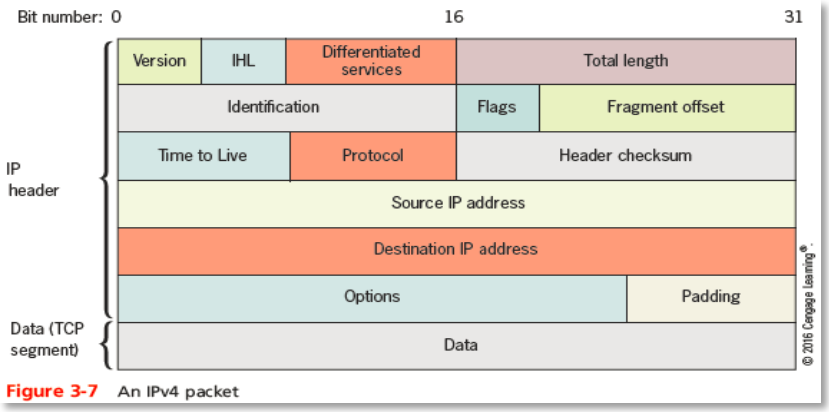

Figure 3-7 An IPv4 packet

1 Byte = 8 bits
2 Bytes = 16 bits
1 bit => two possible values (0 or 1)

(Q.2). 32 bits = _____ bytes

(Q.3). Ping the loopback address as follows: **`ping 127.0.0.1`**

TTL => Time to Live (measured differently. It depends which application is using it)
When used with ping, it refers to the # of hops.
What is the TTL ?

(Q.4). execute: ping google.com

a. What is the TTL? (hint: the most obvious answer could be the real answer)
b. Type: tracert google.com (take a screenshot of the result)
How many hops? (hint: count the number of rows or just look at left most column)
c. execute: ping google.com -i NumberOfHops
Let NumberOfHops = your answer in Q.4b
Take a screenshot of the results
d. execute: ping google.com -i NumberOfHops
Let NumberOfHops = your answer in Q.4b less 1
example: 8 hops – 1 => ping google.com -i 7
Take a screenshot of the results

(Q.5). **`ping www.yahoo.ca`** (take a screenshot of the reply)

C. Network Diagnostic Tool: TRACERT

The Trace Route utility, TRACERT, shows you all the routers you go through to reach another computer on the network. The general format of the TRACERT utility is the same as PING. Try the following exercises from a Command prompt, while connected to the Internet.

a. Use TRACERT to show the path to the following two sites on the Internet.

`tracert www.microsoft.com`

(Q.6). What are the first 3 addresses?

b. Use TRACERT to trace the route from your computer to www.novell.com and ftp.novell.com

(Q.7). Copy and paste the traceroute result of www.novell.com

(Q.8). Copy and paste the traceroute result of ftp.novell.com

*(Q.9). www.novell.com's IPv4 address :*_____
*ftp.novell.com's IPv4 address :*_____

hint: you can verify by using ping. Example: ping ftp.novell.com
if you are getting "*", it could mean that the request is being blocked or unreachable

(Q.10). How many hops did it take to get out of Langara's network? What is the first public IP address reached? Who does it belong to?

This might help verify.
Online tool: https://www.ultratools.com/tools/ipWhoisLookupResult

D. Network Diagnostic Tool: NSLOOKUP

The Name Service Lookup utility uses DNS to display all the IP addresses for a domain name and can also display the domain name associated with a specific IP address. Remember that you can use /? after the command name for help/instruction.

1. From a command prompt, use NSLOOKUP to show the IP address(es) associated with a domain name. Try the following commands:
   `nslookup www.google.com`

(Q.11). How many addresses are associated with the name www.google.com? Please list all

To verify

- *you can use online tool*
- *you can use a browser. Type: http://ipv4_address*
- *not all ipv6 works with browser. http://[ipv6_address]*

(Q.12). What other names is associated with www.yahoo.ca?

Hint

- *try using nslookup*

E. ARP table

The Address Resolution Protocol or ARP is necessary to translate (resolve) a logical IP address into a physical or MAC address. Using Window's ARP utility, you can see which IP addresses have recently been resolved and what the corresponding MAC addresses are. The ARP table resides in your computer, so it doesn't go through the network when you use this command.

Open the command prompt as administrator.
Hint: Use right click and select "Run as Administrator"

a. To clear the cache: netsh interface ip delete arpcache
b. Type: ping the_default_gateway_ip
c. Type: **`arp -a`**

(Q.13). What is the MAC address (physical address) of the default gateway?

F. End of the lab

✪ You need to get the lab instructor to check your work or you won't get any marks for the lab report.

After your work is inspected and marked, shutdown the server gracefully. Select "Other (planned)" and continue. Logoff the Windows 7 computer after you have saved all your files on an external USB/cloud storage. **All changes made to the computer will be erased.**

Deliverables

- Submit a report named **Lab3.docx** The report should contain:
  - Answer to the questions for each section
- Submit to D2L by the due date (posted in D2L Dropbox).