**Lab 3 Write-Up**

**Network Diagnostic Tools**

Submitted by:

Joao Berardo

Paarth

Date: May, 24 2017

**LAB STEPS AND PROCEDURES**

**Lab Activities**

1- Log on to your host computer and then run the virtual Windows server.

We opened Virtual Box and started the virtual Windows server with no problems.

2- Verify that TCP/IP is working.

a. How did you verify that the network and TCP/IP work?

We checked the network icon at windows tray.

We also checked via command prompt, typing ipconfig to check the Windows server IP address.

b. ipconfig /release and /renew

We did this step and after the ipconfig /renew command, our Windows server received the same IP address as before.

c. ipconfig /all

After we typed this command, we got the necessary information to answer the following questions:

i. Your (Host) IPv4 address, default gateway address and subnet mask.

IP address:

192.168.14.246

Default gateway:

192.168.14.1

Subnet mask:

255.255.255.0

ii. The DHCP server address

DHCP server (same as gateway):

192.168.14.1

iii. The DNS server addresses (there are probably two)

DNS Servers:

10.65.0.100

10.65.0.101

10.65.0.102

iv. Your MAC address (Physical address).

MAC address:

08-00-27-64-3D-FA

3 - Ping utility

a. Ping 127.0.0.1

We successfully used the ping command to test if our TCP/IP is working.

b. Ping gateway

Our default gateway responded normally to our ping.

c. Ping [www.yahoo.ca](http://www.yahoo.ca/)

Host IP address: 98.137.236.150.

The ping was successful.

d. Ping 192.168.14.255

No address responded.

This is the broadcast address of our network.

4 – Trace Route Utility (TRACERT)

a. Tracert [www.microsoft.com](http://www.microsoft.com/) and [www.ubc.ca](http://www.ubc.ca/)

Microsoft:

192.168.14.1

10.5.253.254

UBC:

192.168.14.1

10.5.253.254

b. Tacert www.novell.com and ftp.novell.com

What is the IP address of each site?

[www.novell.com](http://www.novell.com/)

130.57.66.5

[ftp.novell.com](ftp://ftp.novell.com/)

130.57.1.173

b.i. What is the first IP address listed in the trace and what does that represent?

The first IP address listed in tracert is 192.168.14.1.

This is the gateway IP address.

b.ii. What is the second IP address listed in the trace and what does that represent?

The second IP address listed in tracert is 10.5.253.254.

This IP address is a class A address, and it is used for internal network, not internet. I assume that this is a router from Langara College, probably the router that connects the College with the internet.

b.iii. Are the first two addresses in both traces the same or different?

The first two addresses are the same in both trace routes.

b.iv. What are the final IP addresses listed in the trace and what do these represent?

The final IP addresses are:

[www.novell.com](http://www.novell.com/)

130.57.66.5

[ftp.novell.com](ftp://ftp.novell.com/)

130.57.1.173

The IP addresses represent the IP address for each host.

The IP address 130.57.66.5 represents the host www from the novell.com domain and the IP address 130.57.1.173 represents the host ftp from the novell.com domain.

b.v.Are there any similarities in the final addresses of the www.novell.com and

ftp.novell.com traces?

Yes, there are. Both IP addresses start with 130.57.x.x. We can assume that the domain novell.com has the range 130.57.x.x allocated for them.

b.vi. What might this suggest about the relative “location” of the www.novell.com

and ftp.novell.com hosts - i.e. are they probably on the same or on different

networks? Are the hosts probably running on the same computer or on different

computers?

After doing a “whois” search, we confirm the IP address range:

NetRange: 130.57.0.0 - 130.57.255.255

CIDR: 130.57.0.0/16

Organization: Novell, Inc. (NOVELL-1)

This means that both IP addresses are in the same network. However, that not necessarily means that they are in the same location or same computer. We only know that both IP addresses belong to the same company. They can be in different computers, even in different cities.

5 – Manage IP Configuration

a. Open Network & Sharing

We executed this step without any difficulties.

b. Connection Status Window. Note the Activity counts. Are they non-zero? Wait for a few seconds. Have they increased?

Initially it had 40,763 / 63,346 bytes received/sent. It wasn’t changing, so we pinged the gateway to generate some traffic and after that both counts increased.

c. Details

All the addresses in the details matched with the previous results.

d. Diagnose

Does the system report that all is well?

We had a problem with a DNS server not responding, but after a few seconds everything was back to normal.

Did the Activity Count change?

The activity count increased again. Both, received and sent.

e. Properties

i. Double-click the “Internet Protocol Version 4 (TCP/IPv4)” entry to examine the

properties. What are the current settings? What specific protocol is necessary to

support these settings?

The setting are set to automatic. For this setting to work, we need to use the DHCP (Dynamic Host Control Protocol) protocol. The DHCP server (same as gateway in this case) allocates IP addresses to hosts that request an IP address.

ii. Set up a static IP configuration by selecting “Use the following IP address:”, “Use the following DNS server addresses:” and filling in the addresses using the information that you recorded earlier.

We configured our computer to use static IP.

Configuration was:

IP address: 192.168.14.246

Default gateway: 192.168.14.1

Subnet mask: 255.255.255.0

DNS Servers: 10.65.0.100, 10.65.0.101, 10.65.0.102

iii. Test the new configuration by trying to surf to www.yahoo.ca. If you are able to reach www.yahoo.ca, make a list of devices, services and protocols that must be

functioning properly.

We tested the configuration navigating to [www.yahoo.ca](http://www.yahoo.ca/). Everything worked as planned and we had access to internet.

6 – Faulty DNS Server

a. Specify our own IP address for the Preferred DNS

We removed every entry on DNS Server settings and set the primary DNS server to 192.168.14.246 (our IP address).

b. Using ipconfig /flushdns

The command executed without any problems.

c. Ping www.yahoo.ca by name. Explain the result.

We had an error trying to ping [www.yahoo.ca](http://www.yahoo.ca/). We changed our DNS server to our own IP address, and since we are not running any DNS server on our machine, any request to a DNS service will fail. Our computer is not able to translate the name [www.yahoo.ca](http://www.yahoo.ca/) to an IP address.

d. Ping the IP address you recorded for www.yahoo.ca. Explain the result.

We pinged [www.yahooo.ca](http://www.yahooo.ca/) IP address (98.137.236.150) successfully because we don’t need any DNS server to ping a IP address. We only need a connection with the internet, no need for name resolution when pinging directly an IP.

e. Restore the original DNS server addresses

We changed back the DNS servers to the previous IPs. Then we tested the and everything was working accordingly.

7 – Name Server Lookup Utility (nslookup)

a. Use NSLOOKUP to show the IP address(es) associated with a domain name.

Try the following commands:

nslookup [www.google.com](http://www.google.com/)

nslookup www.yahoo.ca

How many addresses are associated with the name www.google.com?

One address.

What other name is associated with www.yahoo.ca?

The other name is rc.yahoo.com.

Examine all the yahoo.ca addresses you looked up. What might you guess about the

location of these servers?

We guess that yahoo.ca is located in Canada. We did confirm that using a whois query on yahoo.ca address.

b. Use NSLOOKUP to show the name associated with a specific IP address.

Try the following commands:

nslookup 127.0.0.1

nslookup 198.103.98.139

nslookup 8.8.8.8

What’s the name associated with the loopback address?

Localhost.

What names are associated with the addresses 198.103.98.139 and 8.8.8.8?

198.103.98.139

www.rcmp-grc.ca

8.8.8.8

google-public-dns-a.google.com

8 – Address Resolution Protocol (ARP)

a. Ping the default gateway

Pinged successful.

b. Use ‘arp -a’ command to show recently resolved IP addresses and corresponding MAC addresses

What’s the MAC address of the default gateway?

Gateway MAC address: 00-1E-E5-6C-A0-92