VANIER COLLEGE – Computerized Systems Technology – Winter 2021

Networking Fundamentals (247-409-VA)

Leonardo Fusser (1946995)

LABORATORY EXPERIMENT 3

Understanding Network Elements and Addresses

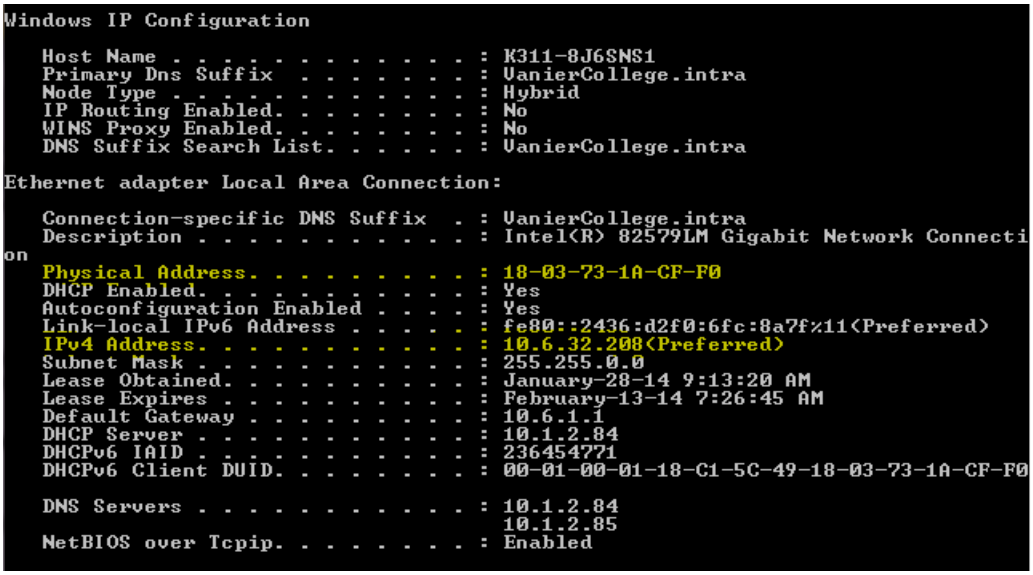
NOTE:
To be completed in one lab session of 3 hrs.
To be submitted using the semi formal lab report, **at the end** of your respective lab session. This exercise is to be done individually except where specified in the procedure. **Each** student must submit a lab report with original **observations and conclusions**.

Part A: Determine MAC and IP addresses

Every computer on an Ethernet local network has a Media Access Control (MAC) address that is burned into the Network Interface Card (NIC). Computer MAC addresses are usually displayed as 6 sets of two hexadecimal numbers separated by dashes or colons. Example: 15-EF-A3-45-9B-57.

Every computer connected to the Internet has a logical unique identifier, called an IP address. IP addresses are displayed as four numbers, known as octets, separated by periods. Example: 192.168.1.4.

1. Enable **ALL** your network adapter.
2. At Windows command prompt window, enter the **ipconfig /all** command. This command displays a list of information about your computer's MAC and IP configuration. Take a screen shot. (Example as shown below:



3. Use the table below to fill in the description of the *ALL* your Ethernet adapter, and the corresponding Physical (MAC) address, and IPv4 address, if any.

Description	Physical Address	IPv4 Address
Adapter "D-265"	D4-BE-D9-A2-CE-BD	None
Adapter "Vanier Ethernet"	00-E0-4C-68-69-12	192.168.50.231
Adapter "Wi-Fi"	00-14-D1-ED-7D-FC	None
Adapter "D-245 NO"	00-E0-4C-68-68-E5	169.254.29.204

a. Why might a computer have more than one MAC address?

- The computer might have more than one physical network adapter installed, therefore multiple MAC addresses will show up. Each network adapter has a MAC address installed. For example, you will see two MAC addresses on a computer with a wireless ethernet adapter and wired ethernet adapter.

b. Do you find IP address on all your adapters? If no, why?

- Some adapters do not have an IP address because they are not connected to any network. For example, the Wi-Fi adapter does not have an IP address because it is not connected to any wireless network. The same applies to the wired ethernet adapters because they are not connected to a wired network.

c. Try to disconnect the cable(s) to your network adapter(s) and use **ipconfig /all** command again. What changes do you observe? Does the MAC address still display? Will the MAC address ever change? (please note that on normal circumstances you are not allowed to do this in this lab)

- The adapters still show up and the MAC address still show up. Even though the cables have been disconnected, the MAC addresses still show up because they are permanently stored onto the network adapters. Therefore, the MAC address never changes and will never be lost. The only difference is that there are no longer any IP addresses because the adapters are not connected to any network anymore.

d. What are the other names for the MAC address?

- Some other names for MAC addresses are commonly referred to as physical addresses.

Part B: IP Addresses and Network Communication (team of 2)

4. Enable **ONLY** your network adapter connecting to D-265 Disable all the others including the wireless. Like lab 1 settings, you will use a different method to connect your PC with your partner, to create a peer-to-peer network, follow the steps below.

5. Verify the physical connectivity by checking if the network appears in your "Network and Sharing Center".

6. Configure IP settings for the 2 PCs

    a. Configure the logical IP addresses for the two PCs so that they are able to communicate using TCP/IP. On PC1, right click the connected D-265 Connection icon. Choose **Properties** from the pull-down menu.

    b. Highlight **Internet Protocol Version 4 (TCP/IPv4)**, click the **Properties** button.

    c. Select the **Use the following IP address** radio button and enter an IP address of 192.168.1.1 and a subnet mask of 255.255.255.0.

    d. With this IP address and subnet mask, what is the network ID that you are on?

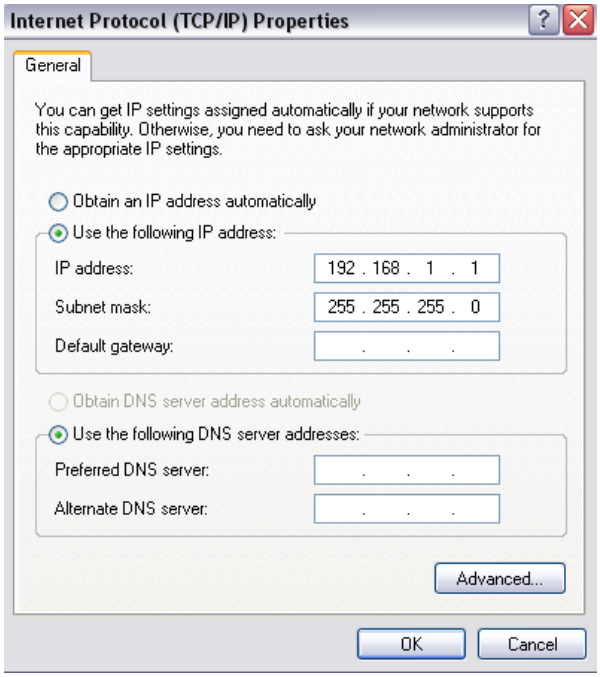
    ➢ Network ID: 192.168.1.0

    e. Click **OK** and exit the setting windows.

    f. Repeat step 6a – 6e for PC2 using an IP address of 192.168.1.2 and a subnet mask of 255.255.255.0 and answer 6d for this computer as well.

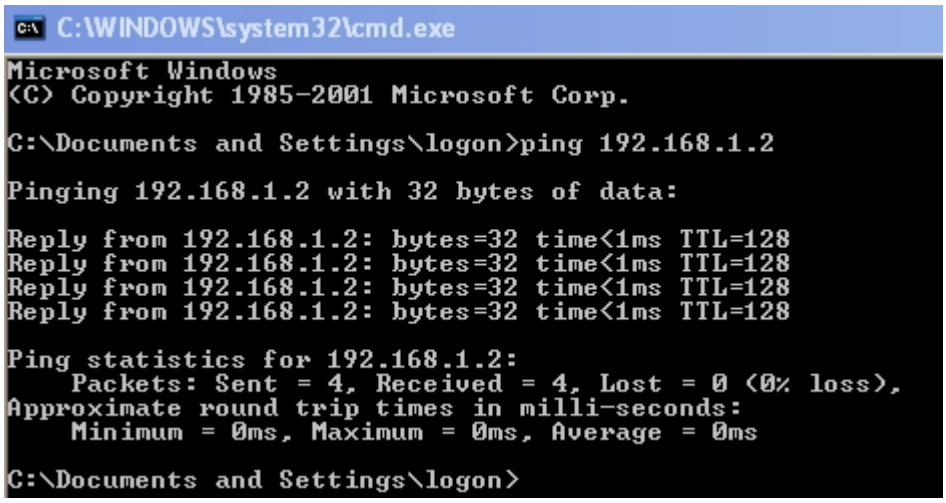
    PC2 answer 6d:

    ➢ Network ID: 192.168.1.0 (same as PC1).



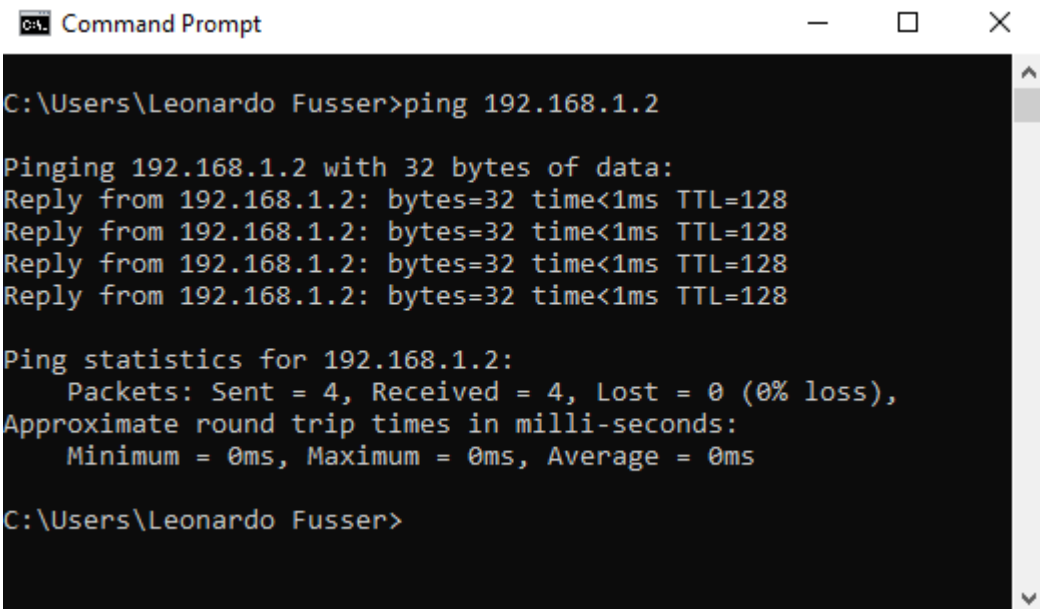
7. Verify IP connectivity between the 2 PCs. (** *To test TCP/IP connectivity between the PCs, Windows Firewall must be disabled temporarily on both PCs*)

    a. The **ping** command is a simple way to accomplish this task. The **ping** command is included with the Windows operating system. At command prompt of PC1, enter **ping 192.168.1.2**. A successful ping will verify the IP connectivity. The result should look like the following:



b. Repeat this procedure for PC2 by pinging 192.168.1.1

c. Show the screen shot of your ping results in the lab report.



Result of ping command sent to PC2 (192.168.1.2) shown above. Result shows that the network settings on PC1 are configured correctly and that a successful communication can be made between PC1 and PC2.

8. Change IP address for PC2

   a. Change the logical IP address for PC2 from 192.168.1.2 to **192.168.2.2** and leave the subnet mask set to 255.255.255.0. On what network is PC2 now?

      - Network ID: 192.168.2.0 (different network than PC1!).

   b. As the IP of PC1 remains unchanged, on what network is PC1?

      - Network ID: 192.168.1.0 (PC1 is on a completely different network than PC2).

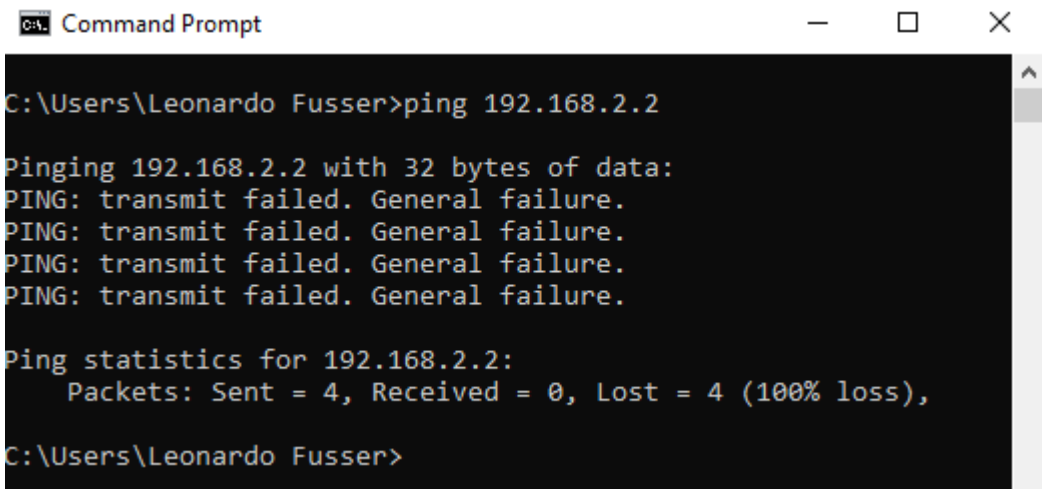
   c. The two PCs are still on the same physical Ethernet network. Are they on the same logical IP network?

      - As mentioned above, since PC2 is on network 192.168.2.0 and PC1 is on network 192.168.1.0, the two computers are on two different networks even though they are physically connected together using a copper cross-over cable.

   d. What are the consequences?

      - One major consequence of having this configuration is that there are major security flaws. Instead of the networks being segregated physically, they are mingled together on one physical network.

9. On PC1, enter **ping 192.168.2.2**. Was it successful? (screenshot) Why or why not?



Result of ping command sent to PC2 (192.168.2.2) after PC2 changes it's IP address (PC1 doesn't change) shown above. The result shows that there is no more successful communication between the two computers. This further shows that the two computers are not connected on the same network.

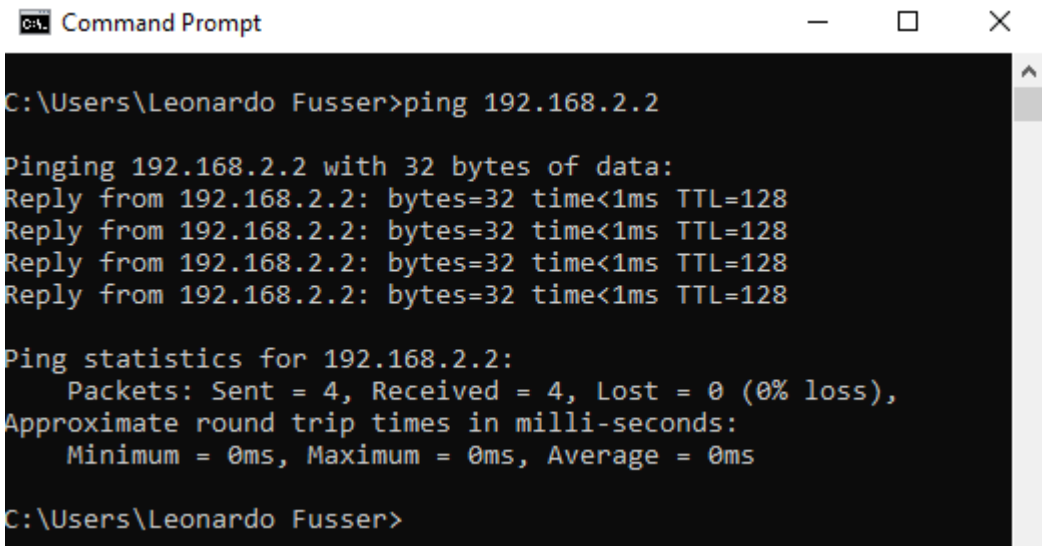
10. Change the logical IP address for PC1 from 192.168.1.1 to **192.168.2.99** and leave the subnet mask set to 255.255.255.0. On what network is PC1 now?

    - Network ID: 192.168.2.0 (same network as PC2).

11. The two PCs are still on the same physical Ethernet network. Are they on the same logical IP network now?

    - With the change in PC1's IP address (192.168.2.99), they are now both connected on the same network since PC1 is now on the 192.168.2.0 network and PC2 is also on the 192.168.2.0 network. They are still connected physically together using a copper cross-over cable.

12. On PC2, enter **ping 192.168.2.99**. Was it successful? (screenshot) Why or why not?



Result of ping command sent to PC2 (192.168.2.2) after PC1 changes IP address (192.168.2.99) shown above. Since the two computers are connected to the same network, they can now successfully communicate with each other once again. As mentioned before, the two computers are connected to the 192.168.2.0 network. They remain physically connected together using a copper cross-over cable.

13. Take the time to understand the concept well and do some research. Include your findings in discussion (try to teach me something I did not know). Show all your sources.

- Since we are configuring networks and viewing what happens when networks are not configured as desired, there is a greater problem that we can't necessarily see besides just having mismatched IP addresses. According to a survey response from attendees of the DEFCON 18 conference, it was revealed that 73% came across a misconfigured network more than three quarters of the time. According to 76% of the sample, it was the easiest IT resource to exploit (to hackers). Misconfigured networks are more common than one would expect and consequences could lead to a complete network shutdown.

Source used:

https://www.helpnetsecurity.com/2010/08/31/misconfigured-networks-main-cause-of-breaches/