Lab - Building a Switched Network

Topology
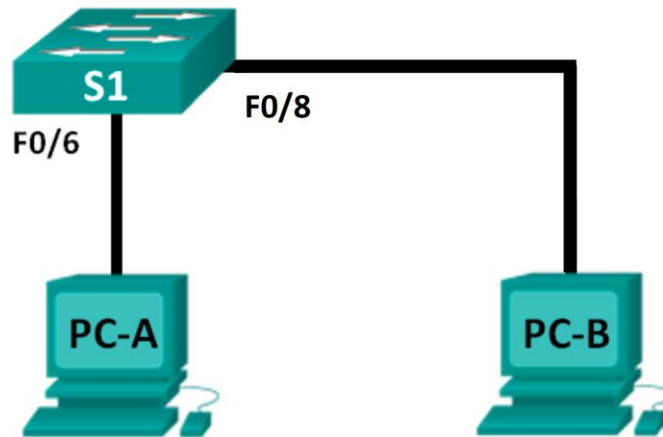
Addressing Table

Device	Interface	IP Address	Subnet Mask
PC-A	NIC	192.168.1.10	255.255.255.0
PC-B	NIC	192.168.1.11	255.255.255.0

Objectives

Part 1: Initialize and Reload a Switch

Part 2: Set Up the Network Topology (Ethernet only)

Part 3: Configure PC Hosts

Part 4: Use Wireshark to View Network Traffic

Background / Scenario

- 3 major components of networks:
    - Hosts
    - Switches
    - Routers

- In this lab, you will build a simple network with two hosts and two switches. You will initialize and reload the switches.

- You will apply IP addressing for this lab to the PCs to enable communication between these two devices.

- Use the **ping** utility to verify connectivity

- use Wirehshark to view the traffic.

Please note, you will need to disable the Firewall to allow "ping" traffic to go through. Follow the instructions in Appendix A to disable the Firewall in lab PCs.

Refer to "Lab-Network_Guide.pdf" for switch router instructions.

Required Resources

- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Initialize and Reload a Switch

To make sure that the switches have been erased and have no startup configurations.

### Step 1: Connect a Cisco switch and computer using a rollover console cable.

a. Connect the rollover console cable to the RJ-45 console port of the switch.

b. Connect the other cable end to the serial COM port on the computer.

Note: rollover console cable (blue flat cable) has already been connected to your desktop computer.

c. Turn on the Cisco switch and computer.

d. If confused, have a look at section 4 (c) of Document X. Steps are listed with graphical examples.

e. In example below, connect console port behind the PC (port no. 23) from RACK C to Console port of the switch.
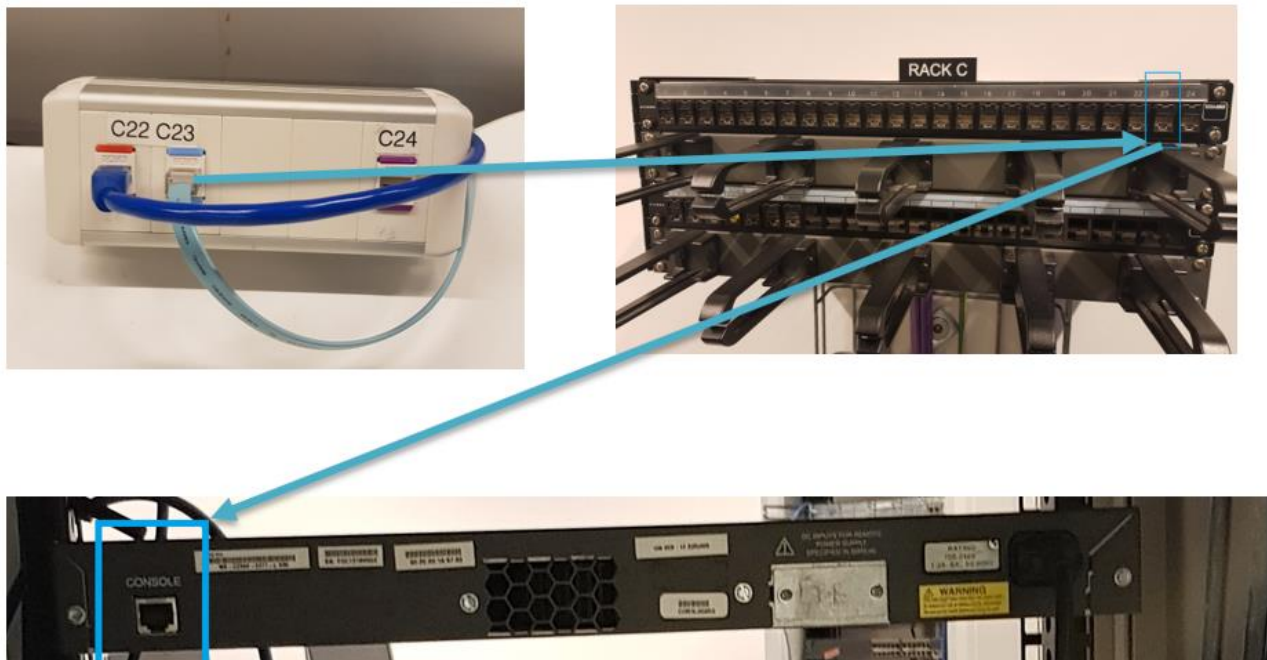
Step 2: Configure Putty to establish a console session with the switch.

Putty is a terminal emulation program. This program allows you to access the terminal output of the switch. It also allows you to configure the switch. Also given in Section 4.c of Week1-Lab-Guid.pdf with screenshots.

a. Start Putty by clicking the **Windows Start** button located in the task bar or you can open it from the desktop as well.
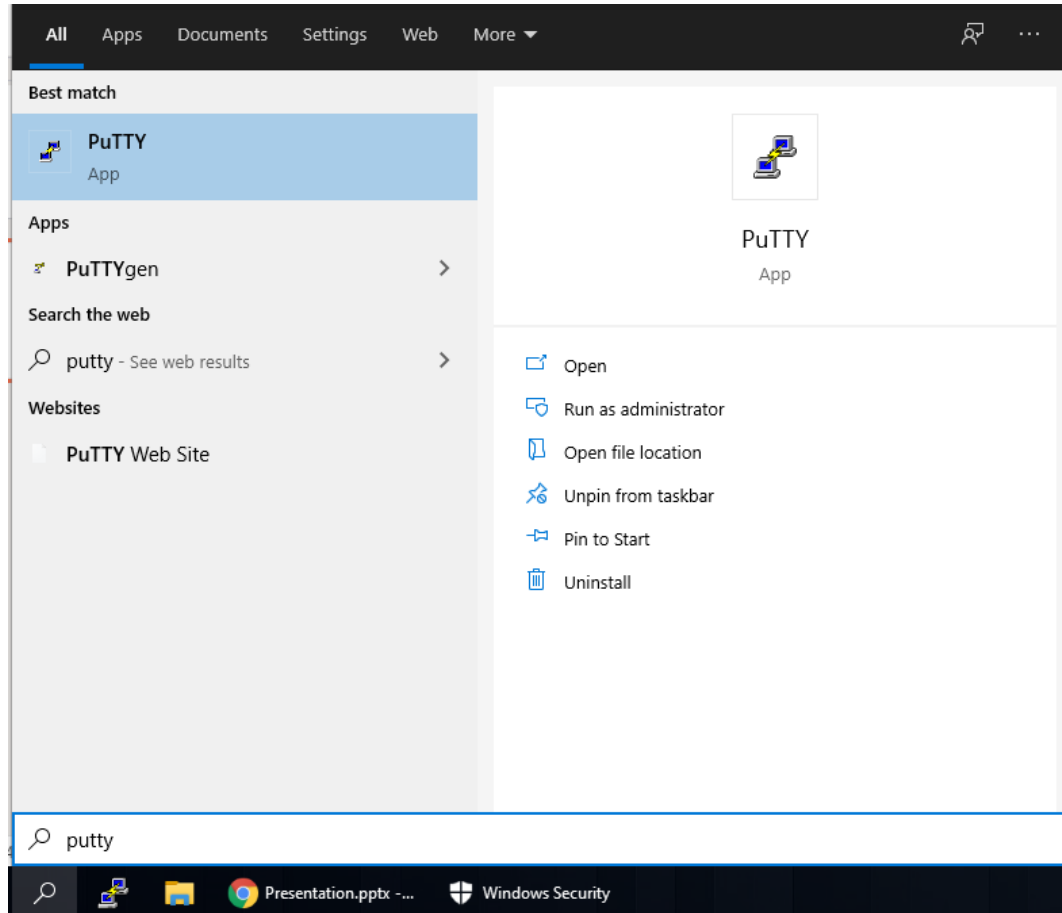
b. In the Putty Configuration dialog box, click the **Serial** radio button and click **Open**
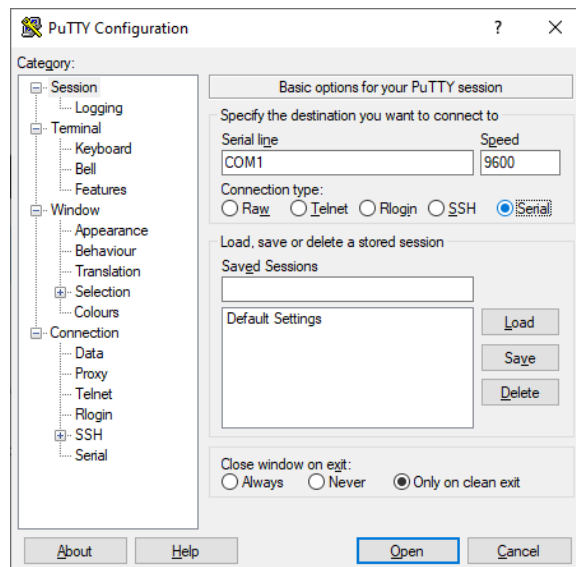
    c.   When you lick Open, you should see Command Cline Interface (CLI) and if the device is just powered on, you will see a initial configuration dialog box as shown below. Type **no** , and press **enter**.
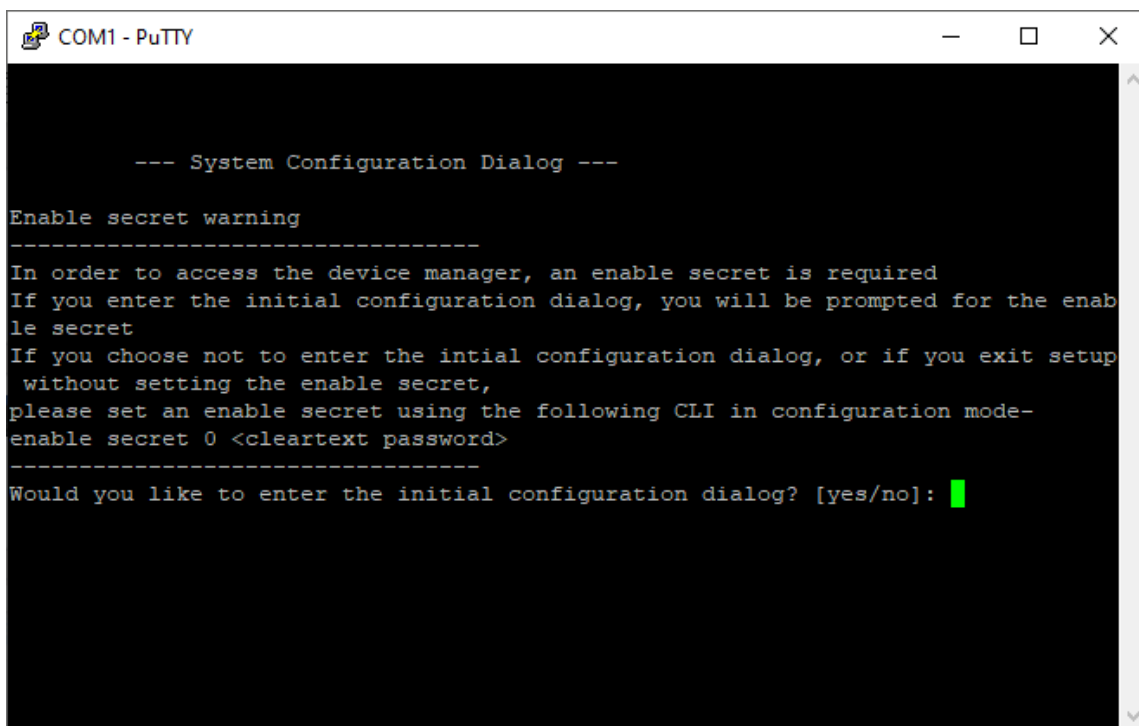
If everything was set up fine, you should see Switch> in CLI. If not, repeat the steps check the cabling or press some keys from the keyboard. You can also refer to Section 4.c of Week1-Lab-Guid.pdf or ask for help from Tutor.

    Press "enter" to access user mode "Switch>"

Type "enable" to access privileged EXEC mode "Switch#".

```
Switch> enable
Switch#
```

Step 3:   Determine if there have been any virtual local-area networks (VLANs) created.

Use the **show flash** command to determine if any VLANs have been created on the switch.

```
Switch# show flash

Directory of flash:/

    2  -rwx        1919   Mar 1 1993 00:06:33 +00:00  private-config.text
    3  -rwx        1632   Mar 1 1993 00:06:33 +00:00  config.text
    4  -rwx       13336   Mar 1 1993 00:06:33 +00:00  multiple-fs
    5  -rwx    11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2.SE.bin
    6  -rwx         616   Mar 1 1993 00:07:13 +00:00  vlan.dat

32514048 bytes total (20886528 bytes free)
Switch#
```

Step 4:   Delete the VLAN file.

a. If the **vlan.dat** file was found in flash, then delete this file.

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

You will be prompted to verify the file name. At this point, you can change the file name or just press Enter if you have entered the name correctly.

b. When you are prompted to delete this file, press Enter to confirm the deletion. (Pressing any other key will abort the deletion.)

```
Delete vlan.dat? [confirm]
Switch#
```

Step 5:   Erase the startup configuration file.

Use the **erase startup-config** command to erase the startup configuration file from NVRAM. When you are prompted to remove the configuration file, press Enter to confirm the erase. (Pressing any other key will abort the operation.)

```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
```

Step 6:   Reload the switch.

Reload the switch to remove any old configuration information from memory. When you are prompted to reload the switch, press Enter to proceed with the reload. (Pressing any other key will abort the reload.)

```
Switch# reload
Proceed with reload? [confirm]
```

Note: You may receive a prompt to save the running configuration prior to reloading the switch. Type **no** and press Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

Step 7: Bypass the initial configuration dialog.

After the switch reloads, you should see a prompt to enter the initial configuration dialog. Type **no** at the prompt and press Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>
```

Part 2: Set Up the Network Topology (Ethernet only)

You will cable the devices together according to the network topology.

Step 1: Power on the devices.

Power on all devices in the topology. The switches do not have a power switch; they will power on as soon as you plug in the power cord.

Step 2: Connect the two switches.

Connect one end of an Ethernet cable to F0/1 on S1 and the other end of the cable to F0/1 on S2. You should see the lights for F0/1 on both switches turn amber and then green. This indicates that the switches have been connected correctly.

Step 3: Connect the PCs to their respective switches.

a. Connect one end of the second Ethernet cable to the NIC port on PC-A. Connect the other end of the cable to F0/6 on S1. After connecting the PC to the switch, you should see the light for F0/6 turn amber and then green, indicating that PC-A has been connected correctly.

b. Connect one end of the last Ethernet cable to the NIC port on PC-B. Connect the other end of the cable to F0/18 on S2. After connecting the PC to the switch, you should see the light for F0/18 turn amber and then green, indicating that the PC-B has been connected correctly.

Step 4: Visually inspect network connections.

After cabling the network devices, take a moment to carefully verify the connections to minimize the time required to troubleshoot network connectivity issues later.
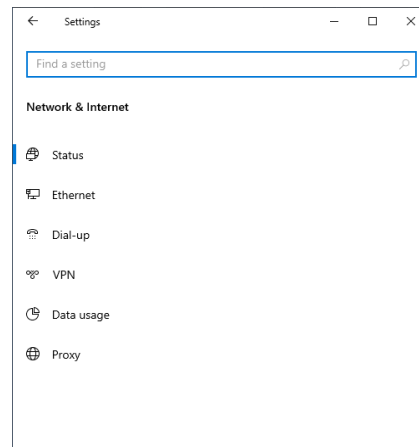
Part 3: Configure PC Hosts

Step 1: Configure static IP address information on the PCs.

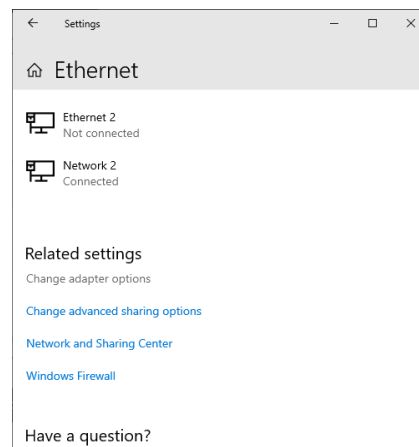a. Click the **Network** icon and then select **Network & Internet settings**.
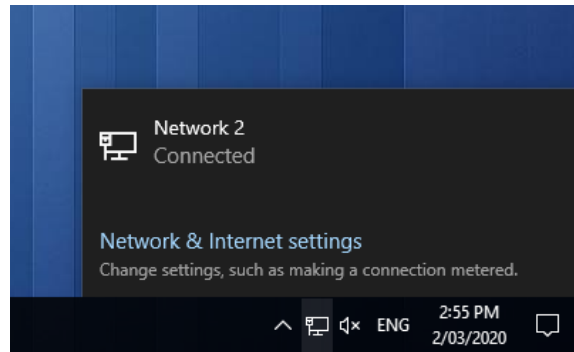
b. Click the **Ethernet** on the left-hand side.
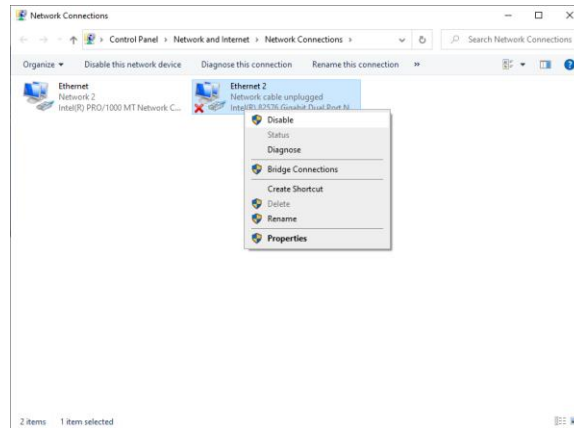

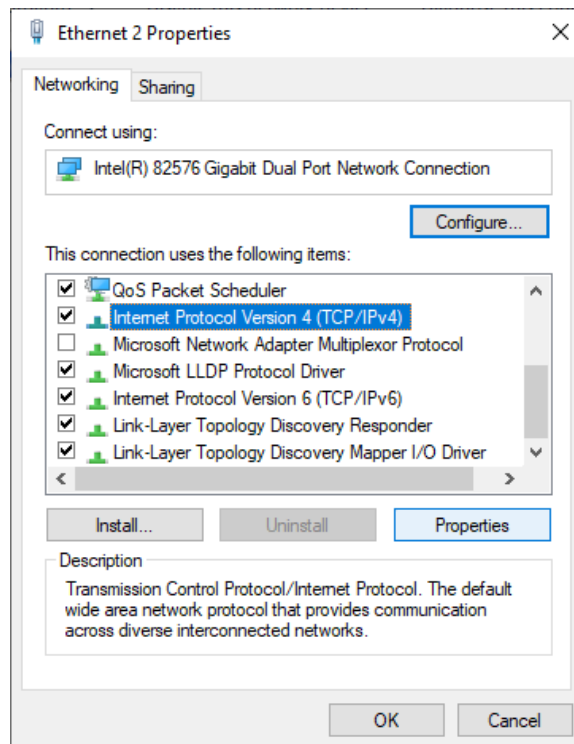c. Click the **Change adapter options** under the Related settings.

d. The Network Connections window displays the available interfaces on the PC. Right-click the **Ethernet 2** (the name can be others, e.g., Local Area Connection) interface and select **Properties**.
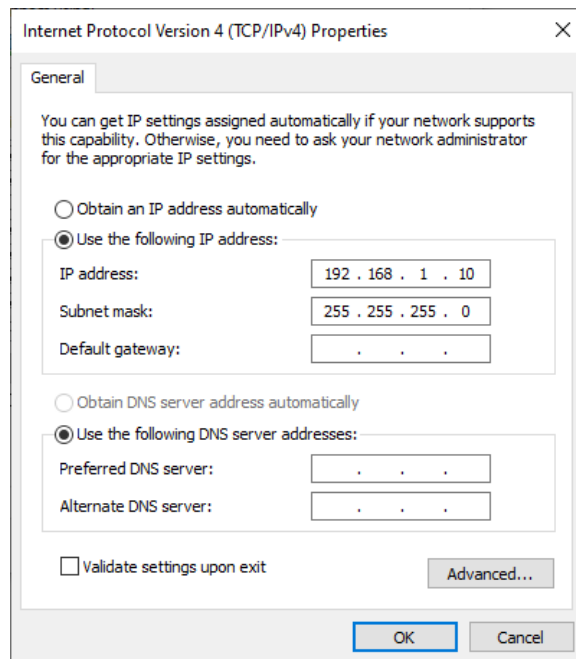
e. Select the **Internet Protocol Version 4 (TCP/IPv4)** option and then click **Properties**.

Note: You can also double-click **Internet Protocol Version 4 (TCP/IPv4)** to display the Properties window.

f. Click the **Use the following IP address** radio button to manually enter an IP address, subnet mask, and default gateway.

> **Note**: In the above example, the IP address and subnet mask have been entered for PC-A. The default gateway has not been entered, because there is no router attached to the network. Refer to the Addressing Table on page 1 for PC-B's IP address information.

g. After all the IP information has been entered, click **OK**. Click **OK** on the Local Area Connection Properties window to assign the IP address to the LAN adapter.

h. Repeat the previous steps to enter the IP address information for PC-B.

Step 2: Verify PC settings and connectivity.

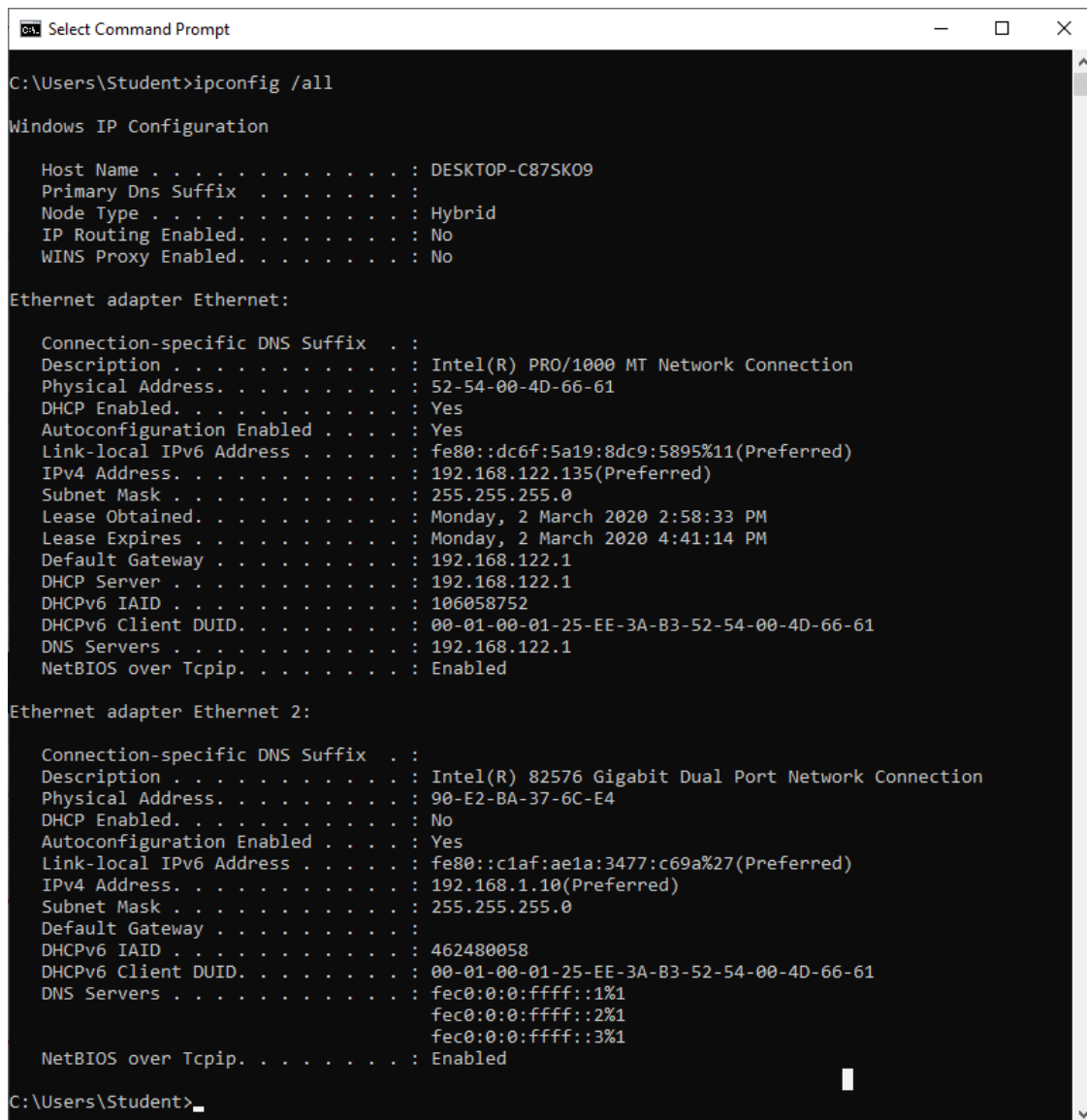Use the command prompt (**cmd.exe**) window to verify the PC settings and connectivity.

a. From PC-A, click the **Windows Start** icon, type **cmd** in the **Search programs and files** box, and then press Enter.
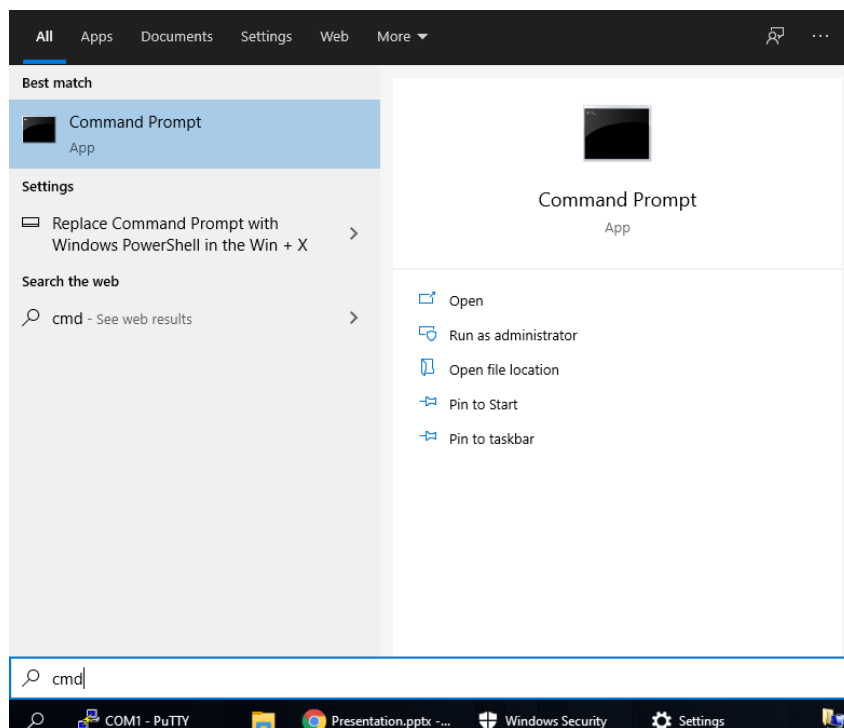
b. The cmd.exe window is where you can enter commands directly to the PC and view the results of those commands. Verify your PC settings by using the **ipconfig /all** command. This command displays the PC hostname and the IPv4 address information.

```
Select Command Prompt                                                      —   □   ×

C:\Users\Student>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-C87SKO9
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 52-54-00-4D-66-61
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::dc6f:5a19:8dc9:5895%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.122.135(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, 2 March 2020 2:58:33 PM
   Lease Expires . . . . . . . . . . : Monday, 2 March 2020 4:41:14 PM
   Default Gateway . . . . . . . . . : 192.168.122.1
   DHCP Server . . . . . . . . . . . : 192.168.122.1
   DHCPv6 IAID . . . . . . . . . . . : 106058752
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-EE-3A-B3-52-54-00-4D-66-61
   DNS Servers . . . . . . . . . . . : 192.168.122.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82576 Gigabit Dual Port Network Connection
   Physical Address. . . . . . . . . : 90-E2-BA-37-6C-E4
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::c1af:ae1a:3477:c69a%27(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.10(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 462480058
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-EE-3A-B3-52-54-00-4D-66-61
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Student>
```
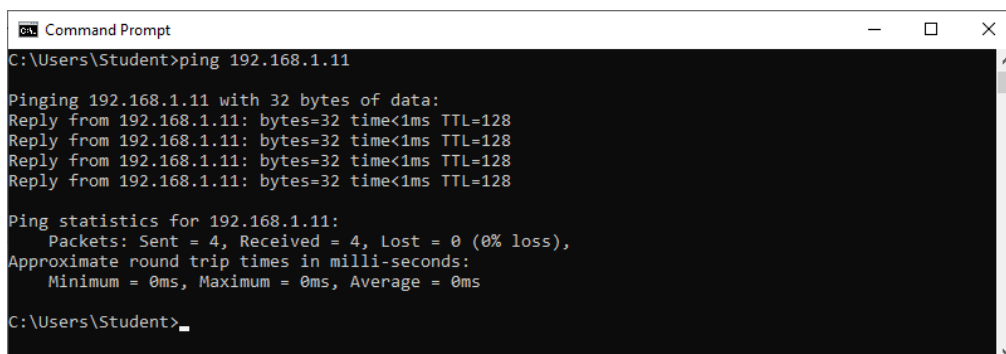
c. Type **ping 192.168.1.11** and press Enter.

```
Command Prompt                                                      —   □   ×

C:\Users\Student>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Student>
```

Were the ping results successful? _____

If not, troubleshoot as necessary, e.g., physical connection, IP configuration and firewall.

Note: If you did not get a reply from PC-B, try to ping PC-B again. If you still do not get a reply from PC-B, try to ping PC-A from PC-B. If you are unable to get a reply from the remote PC, then have your instructor help you troubleshoot the problem.

Part 4: Using Wireshark to Examine Network Traffic

Step 1: Retrieve your PC's interface addresses.

PC-A: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

PC-B: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

Step 2: Start Wireshark and begin capturing data.

a. Capture ping request data on PC-A, while PC-A ping PC-B

Source IP: _____._____._____._____ Source MAC: ____:____:____:____:____:____
Dest   IP: _____._____._____._____ Dest   MAC: ____:____:____:____:____:____

Does the Source MAC address match your PC-A's interface? _____

Which interface is the Destination MAC address? _____

b. Capture ping request data received on PC-B, while PC-A ping PC-B

Source IP: _____._____._____._____ Source MAC: ____:____:____:____:____:____
Dest   IP: _____._____._____._____ Dest   MAC: ____:____:____:____:____:____

Does the destination MAC address match your PC-B's interface? _____

Which interface is the source MAC address? _____
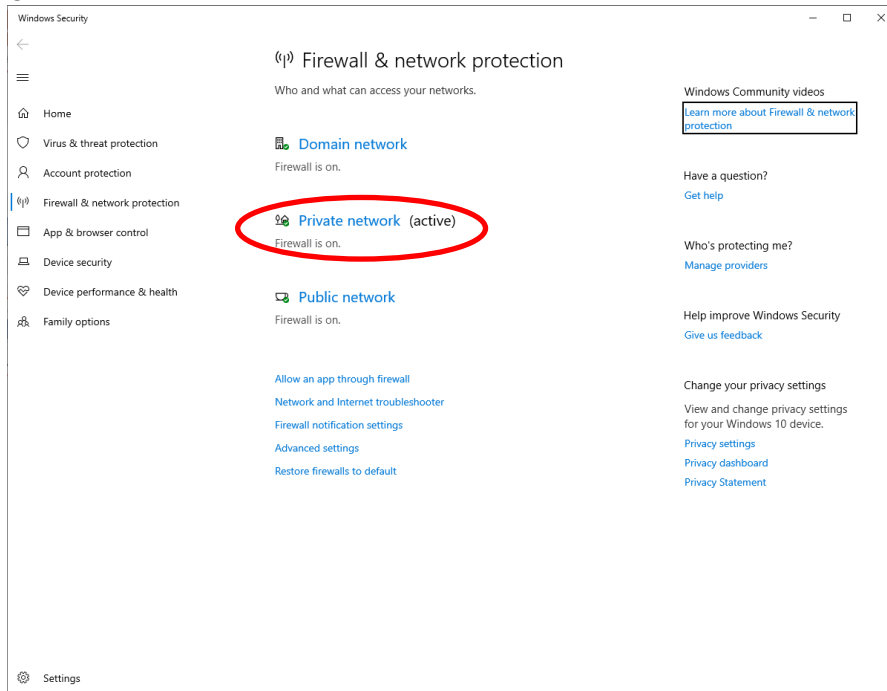
Appendix A. Turn Off Firewall

These steps are necessary to allow ICMP (ping packets) go through the networks.

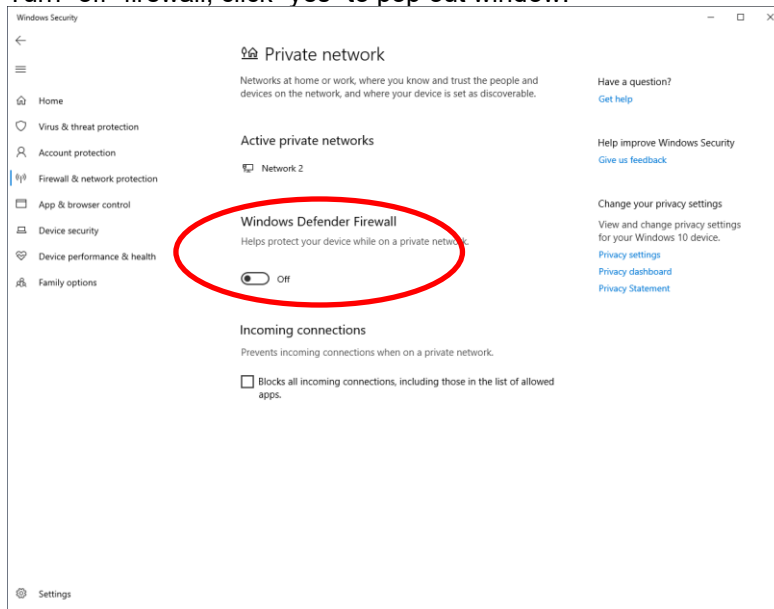1. Press the win key to search for "firewall", and Click on "Firewall & network protection"
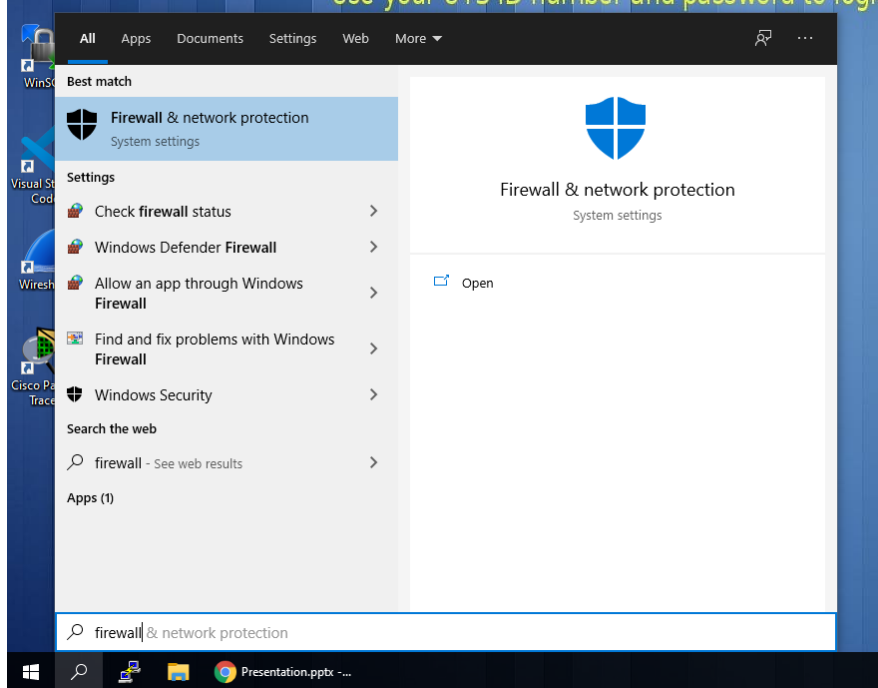
2. Click on "Private network" to view firewall status

3. Turn "off" firewall, click "yes" to pop out window.

4. Make sure all firewalls are "off"