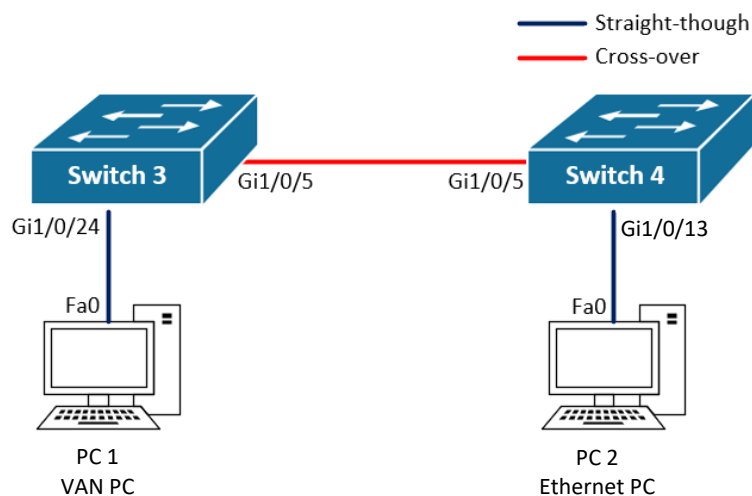# Lab SU-2a – Packet Tracer, ARP and the Switch CLI

Topology Diagram and Addressing Table

Device Name	IP address	Subnet Mask
PC1	192.168.1.10	255.255.255.0
PC2	192.168.1.11	255.255.255.0
Switch3	192.168.1.3	255.255.255.0
Switch4	192.168.1.4	255.255.255.0

Objectives

Use Packet Tracer to simulate a small network topology

Observe the Address Resolution Protocol process

Explore the switch CLI and execute basic configuration commands

Background / Scenario

Cisco **Packet Tracer** is a network simulation tool that you can use for learning purposes during the semester. This tool is freely available to you, and you can download it from Canvas or from the Cisco NetAcademy website.

In this lab you will learn how to use Packet Tracer to simulate a small network as per the specifications on the Topology Diagram and Addressing Table section. Once you have a built a working network topology, you will use **Internet Control Message Protocol** (ICMP) command tools to validate they can successfully communicate with each other.

The network you will be simulating today is implemented with IP routers and Ethernet switches, therefore, the layer 3 protocol in use is the **Internet Protocol**, while the Layer 2 and Layer 1 protocols are **Ethernet** protocols. For IP communication to happen between two devices across an Ethernet network, said devices need to know each other's IP address and Ethernet MAC address. This is because, as data is passed down the communication layers, it needs to be encapsulated with header information, including addressing and other control information, required to perform the communication functions. The **Address Resolution Protocol** allows devices to learn the destination MAC address to be used in the layer 2 header for a specific destination IP address. In this lab you will observe the ARP binding tables built by devices as they communicate with other devices in the network.

You will also perform basic switch configuration tasks to change the default settings of the switches in your topology. More specifically, you will learn how to change the hostname, management IP, interface status and passwords. You will observe how cisco switches store the current configuration settings in a file named **running-config**, while settings that need to be maintained after a reload are saved to a file named **startup-config**.

Finally, you will use the ATC facilities to build the Network Topology using real Cisco switches. If you are working on-campus, you will learn how to start, configure and connect two **virtual machines** to your network for testing purposes.

Note: in this lab you will be configuring device passwords and saving your configuration settings to the startup configuration file, however, this is the only lab where you will need to perform these tasks in order to learn how to do it. We ask that you do not configure passwords or save your configuration settings in future lab practices.

Required Resources

- Personal Computer
- Cisco Packet Tracer
- 2 x Cisco Catalyst 3650 Switches
- 2 x Virtual PCs

Part 1:   Use Packet Tracer to Simulate a Small Network Topology

In Part 1, you will learn how to use Cisco Packet Tracer to simulate a small network.

Step 1:   Download and Install Cisco Packet Tracer

Download the Packet tracer installation for your client operating system from the **Packet Tracer Canvas** page. In this page you will also view a **FAQ document** with installation instructions

https://swinburne.instructure.com/courses/35148/pages/packet-tracer?module_item_id=2003806

**Note:** you can also download Packet Tracer from the Cisco NetAcademy Website.

Launch Packet Tracer after installation. The latest versions of Packet Tracer require user authentication using your NetAcademy account. If you do not currently have a NetAcademy account, click on the **Guest Login** button. This will launch a web page inviting you to enrol in the "Introduction to Packet Tracer" for free and get a netacad.com account. Please ignore this page, you will be getting your NetAcademy account on your student email in Week 2 of semester, therefore, you do not need to request one. Go back to the Packet Tracer application and click on **Confirm Guest** when this button becomes available.

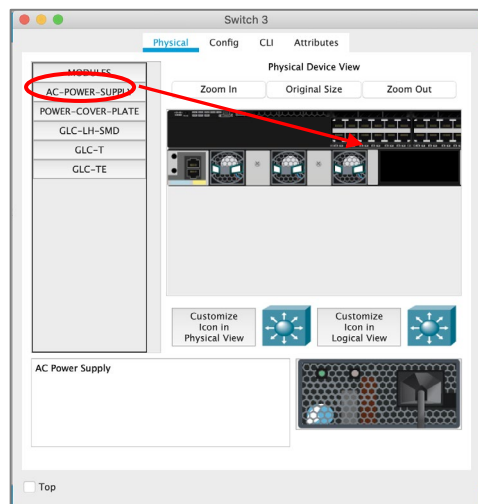### Step 2:   Add the Required Devices to the Workspace

On the bottom left panel, select the **Network Devices** icon on the first row, and the **Switches** icon on the second row.
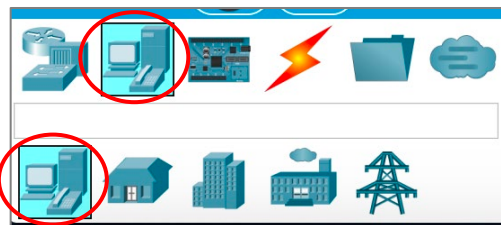

This will display a selection of switches. In this lab, you will be using Catalyst 3650s to match the model of Switch3 and Switch4 in the ATC rooms. Drag and drop **2 x 3650 24PS** switches onto the workspace.
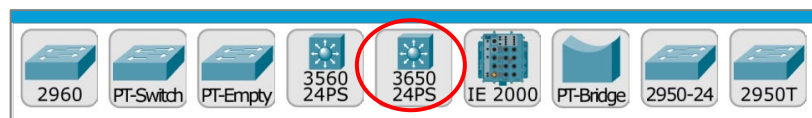

Insert at least one **AC-POWER-SUPLY** in the power supply slots of the 3650 switches. To do this, double click on the switch to open the configuration window, then drag and drop the power supply into the slot.

On the bottom left panel, select on the **End Devices** icon on the first row, and then again the **End Devices** icon on the second row.

This will display a selection of end devices to choose from. Drag and drop **2 x PCs** onto the workspace
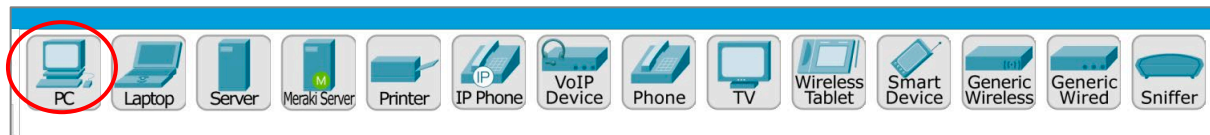
Arrange the devices in the workspace as per the **Topology Diagram.** You can also change the name labels of the devices to match the names specified in the diagram.
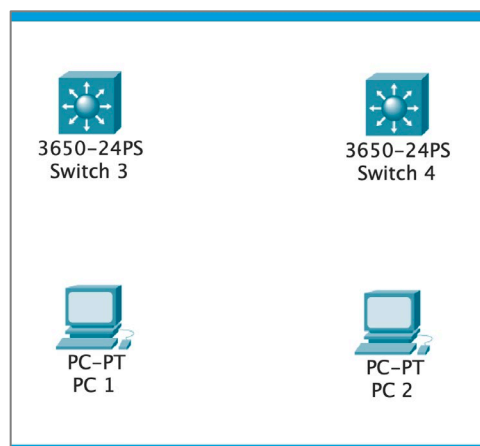

Step 3: Interconnect the Devices

The network interfaces in Catalyst 3650 switches are Gigabit Ethernet interfaces, more specifically they are 1000BASE-T interfaces built to send and receive data over **unshielded twisted pair** (UTP) copper cabling. Depending on how the copper pairs inside the UTP cable are arranged, the connection is either **cross-over** or **straight-through**.

For interconnecting devices in the same layer of operation we use cross-over cables. For interconnecting devices in different layers of operations use straight-through cables. I this scenario, you will need to use straight-trough cables to connect the PCs to the switches, an a cross-over cable to interconnect Switch3 and Switch4.

Note: computers and routers operate at layer 3, while switches operate at layer 2

On the bottom left panel, select on the **Connections** icon on the first row, and then again the **Connections** icon on the second row.
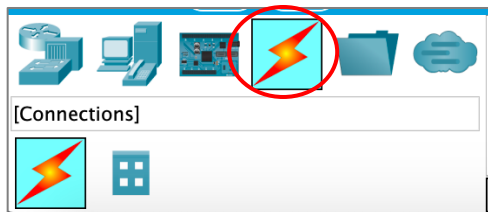
This will display a selection of cable types to choose from. Select a **copper cross-over** connection to interconnect Switch3 to Switch4.
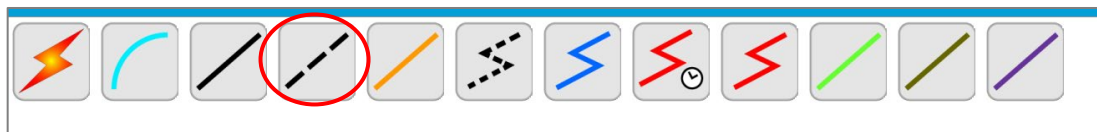
To interconnect Switch3 to Switch4, click on Switch3 select Gi1/0/5 from the drop-down interface list then click on Switch4 and select Gi1/0/5 from the drop-down interface list.

Follow a similar procedure to interconnect the PCs to the switches as per the Topology Diagram and using **copper straight-through** cabling.

Step 4: Configure IP address on the PCs

Double click on PC1, this will open the configuration window. Go to the **Desktop** tab, and double clink on the **IP configuration** icon. Set PC1 IP address and Subnet Mask as per the specifications in the **Addressing Table** above.
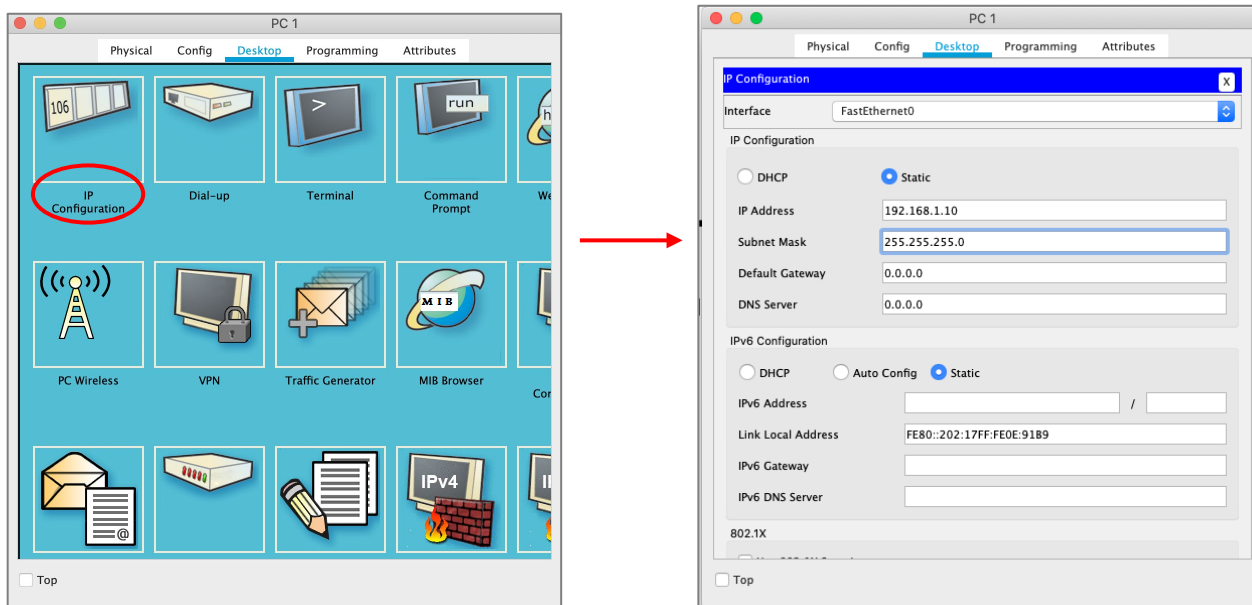
Follow a similar procedure con configure IP address and Subnet Mask settings on PC2.

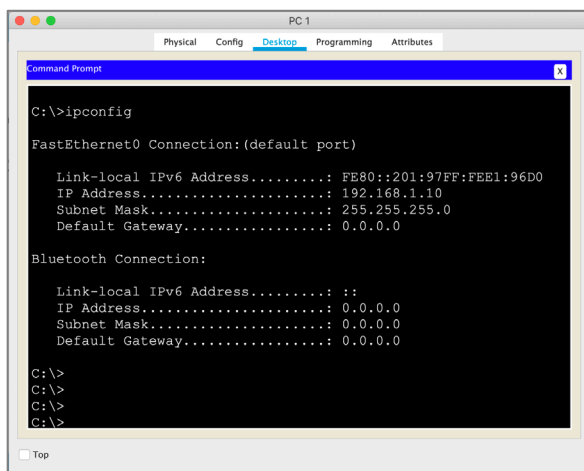## Step 5: Test your Network using ICMP

From PC1 and PC2 Desktop, click on the **Command Prompt** icon. This will give you access to the PCs command line interface. Use the **ipconfig** command to validate the IP configuration on both PC1 and PC2
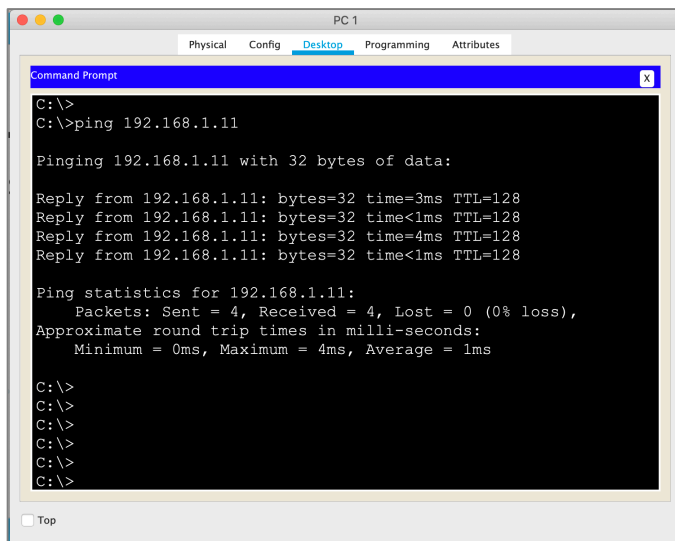
From PC1 command line interface, you can use ICMP command tools to send a **ping request** to PC2. A ping request is a small message prompting the receiver to reply with a **ping reply**. If you followed all the previous steps correctly and you have a working network topology, you will receive a ping reply from PC2.

Note: by default, the ping command sends <u>four</u> ping request messages to the destination IP address and you should expect to receive <u>four</u> ping replies.

Part 2: Observe the Address Resolution Protocol process

In Part 2, you will observe the ARP process that binds destination IP addresses to destination MAC addresses

Step 1: Display the ARP tables

Before IP packets can be transmitted over an Ethernet networks, the sender must first learn the Ethernet (MAC) Address to use as the destination in the Layer 2 headers. However, programs only refer to the IP address of the destination. The process through which IP addresses are mapped to MAC addresses is called ARP (Address Resolution Protocol).

In Part 1, Step 5 you used the ping command to send a message from PC1 to PC2. Before the ping actually takes place, a number of things have to happen:

- PC1 sends a broadcast Ethernet packet known as an **ARP request**.

- The contents of this packets essentially say: "Who has IP address 192.168.1.11?"

- This packet is received by all computers connected to the same Local Area Network

- The computer with the nominated IP address, i.e. PC2, will respond with an **ARP reply**

- PC1 now knows the destination MAC address.

Through this process PC1 updates its internal **ARP table** and then sends the ping encapsulated inside an Ethernet frame to the correct destination MAC address. If PC1 needs to send another message to PC2 in the future, the ARP request/reply for PC2 IP address is not needed as the result is stored in the ARP table for future use.

You can use the **arp -a** command on the command line interface of PC1 to display the ARP table information

```
C:\>arp -a
  Internet Address        Physical Address        Type
  192.168.1.11            0030.a38a.5916          dynamic
```

Based on the content of PC1 ARP table, what is the MAC address of PC2? _00d0.bad2.22cb_____

Based on the content of PC2 ARP table, what is the MAC address of PC1? _0002.4aa4.e5c6_____

You can use the **arp -d** command on the PCs command line interface to empty the content of the ARP table

```
C:\>arp -d
C:\>arp -a
No ARP Entries Found
```

Ping PC2 from PC1 again and validate the ARP tables have been populated again.

Part 3: The CLI and Basic Switch Configuration

In Part 3, you will explore the switch CLI (command line interface) and execute basic configuration tasks

Note: remember from Lab SU-1a that devices will ask you an initial question prompting you to start the configuration dialog, you must enter "no". Some devices will then prompt you to confirm.

Step 1: Explore the CLI Help

When entering commands at the CLI, the **<tab>** key and "**?"** help you auto-complete commands and display the CLI help. You can also use shorter forms of the configuration commands as long as the short form results to be un-ambiguous.

- Typing a **"?"** at any time on the command line will result in a list of all available commands available at the present time, along with a brief description of what those commands do.

- Typing a partial command followed by a **"?"** will result in a list of all available commands that start with the letters you have typed in, along with a brief description of what those commands do

- Typing a command, followed by a space and then a **"?"** will list what the command is expecting as the next parameter, along with a description of the parameter itself.

- Typing some letters, then hitting the **<tab>** key will auto-complete the command (or parameter). For example, typing **"sh"** and hitting the **<tab>** key will auto-complete to **"show".**

- Auto-completion only works if the partial command is un-ambiguous, for example typing **"s"** and hitting the **<tab>** key, will not auto-complete because multiple commands begin with **"s".**

- You can enter partial commands/parameters as long as they are un-ambiguous. For example, the command "**show running-config**" can be entered as "**sh run**" as there is no other command that starts with **"sh"** and no other parameter that starts with **"run"**

Test some of the above tips at the CLI of your switches in Packet Tracer. To access the switch CLI, double click on the switch to open the configuration window and go to the CLI tab. Alternatively, you can choose to run this step and the following steps using the real devices in the ATC Cisco labs via SmartRack.

Step 2: Explore the CLI Operation Modes

The CLI on Cisco devices can operate on different modes. You can tell which mode a device is in by looking at the prompt. The prompt always begins with the device name. The default name for a router is "Router" and for a switch is "Switch. There are three primary modes of operation:

User Mode – signified by a **">"** after the device name. This mode has minimal privileges, you will not be able to change configuration settings and you will only be able to view the status of a subset of parameters and some configuration settings.

Administrator Mode – signified by a **"#"** after the device name. Also called "enable mode" or "privileged execution mode". In this mode you will be able to examine the status of the full set of parameters and all configuration settings.

Configuration Mode – signified by a **"(config)#"** after the device name. In this mode you will be able to change the device configuration.

Other than these three primary modes, a number of sub-configuration modes exist. For example, if you are configuring a network interface the prompt will be followed by **"(config-if)#"**.

Different commands are used to enter and leave different configuration modes. Go to the CLI of your switches and try to move from one mode to another using the following instructions:

- You can transition from User Mode to Administrator Mode by entering the command **"enable"**

- Logout from User Mode by entering **"exit"**

- Transition from Administrator Mode to User Mode by entering **"exit"**

- Transition from Administrator Mode to Configuration Mode by entering **"configure terminal"**

- Transition from Configuration Mode to Administrator Mode by entering **"exit"**

- Transition from a Sub-configuration Mode to Configuration Mode by entering **"exit"**

- Transition from Configuration or Sub-configuration Modes to Administrator Mode by entering **"end"**

Step 3: Set the Device Name on Switch3 and Switch4

To set the switch name, you need to use the **hostname** command in Configuration mode. Enter the following commands at Switch3 CLI:

```
Switch>ena
Switch#conf t
Switch(config)#hostname Switch3
Switch3(config)#end
Switch3#
```

Note how after you set the switch name using the **hostname** command, the switch name was instantly changed and reflected in the prompt. The hostname command takes one parameter, the new name for the switch.

Use the **hostname** command on Switch4 to change the device name to Switch4

Step 4: Set the MOTD on the Switches

The message of the day (MOTD) is displayed to the user when connecting to the CLI <u>before</u> entering the User Mode. It is typically used as a security warning advising the user to disconnect if they are not authorised to access de device. To configure the MOTD we use the **banner motd** from the Configuration mode. Enter the following commands at Switch3 CLI:

```
Switch3#conf t
Switch3(config)#banner motd + *******************
** This is Week 2 **
** of Semester 2 **
** at Swinburne **
******************* +
Switch3(config)#end
Switch3#
```

The **'+'** can be replaced by any character that is <u>not present</u> in the actual message. This is because the **banner motd** command uses this character as a flag to determine the start and the end of the MOTD.

You can validate the configured MOTD in the current configuration using the **show run** command. You can also type **exit** as many times as needed to log out of the switch, press Enter to log back in and observe note that the entered MOTD is displayed before you see the prompt **"Switch3>"**.

Use the above commands to configure the MOTD on Switch4. You can try using a different start/end character.

Step 5: Saving the Configuration and Rebooting the Switch

Cisco network devices typically store two configuration files; the running configuration or **running-config**) and the startup configuration or **startup-config**.

- **running-config** – the current configuration of the switch/router. We use the **show running-config** command (from Administrator Mode) to display this file. This command will read the current configuration, generate it as a text file and print it to the CLI. Running configurations are stored on RAM. When you power on a switch/router for the first time, the running-config contains default settings. Changes to the running-config are not maintained after a reboot, unless they are saved to the startup-config.

- **startup-config** – this configuration is saved on the NVRAM of the switch/router. We use the **show startup-config** command (from Administrator Mode) to this file. When the device boots up, it checks to see if this file exists, if so, it loads the stored configuration in this file into the running configuration. If this file does not exist, there is no configuration so the device is loaded with a default running configuration, and the switch/router will prompt you if you wish to use the wizard display to configure the device. If you do not get prompted, then a startup-config exists and was loaded, the device has been previously configured and is not running default settings.

Note: when you start your lab practices you should <u>always</u> use the **show startup-config** to validate that the devices you are working on have not been previously configured and are running with default settings.

Use the **show running-config** and **show startup-config** command at the CLI of your switches and answer the following questions:

Is Switch3 startup configuration empty? Yes _____

Is Switch4 startup configuration empty? Yes _____

Is Switch3 running configuration to default settings? Yes _____

Is Switch4 running configuration to default settings? Yes _____

On Switch3, save the running configuration to the startup configuration and then reload the switch. To do this, you must be on Administrator Mode and use the copy running-config startup-config command:

```
Switch3#copy running-config startup-config
Switch3#reload
```

Now, reload Switch4 <u>without</u> saving the running configuration to the startup configuration. The switch will prompt you so save the configuration, enter "no" and then hit enter to confirm.

```
Switch4#reload
System configuration has been modified. Save? [yes/no]:no
Proceed with reload? [confirm]
```

The switches will take some time to reboot, while that is happening you will see several output messages on the CLI, these are related to the booting tasks the switch is running. Once the switches have finished booting use the **show running-config** and **show startup-config** again to answer the following questions:

Is Switch3 startup configuration empty? No _____

Is Switch4 startup configuration empty? No _____

Is Switch3 running configuration to default settings? No _____

Is Switch4 running configuration to default settings? Yes _____

Step 6: Configure Passwords on Switch3

In production networks, basic security configuration is advised to restrict access to network devices for configuration purposes. Cisco IOS provides for three passwords:

User Mode Password – must be entered before you can login to the device in User Mode via console

Administrator Mode Password – must be entered after typing "**enable**" before entering Administrator Mode

Line VTY Password – must to be entered when telneting to the device before you login in User Mode

By default, these passwords are not set.

To set the **User Mode Password** to **"ccna"** on Switch3, enter the following commands:

```
Switch3#conf t
Switch3(config)#line console 0
Switch3(config-line)#password ccna
Switch3(config-line)#login
Switch3(config-line)#end
Switch3#exit
```

Note: configuring the password is not enough, you must use the login command to indicate the password should be prompted before allowing user access via console.

If you attempt to connect to Swtich3 CLI now that you have configured a User Mode password, you will need to enter the password before the switch grants you access.

To delete the User Mode Password, you can use the following commands:

```
Switch3#conf t
Switch3(config)#line console 0
Switch3(config-line)#no password
Switch3(config-line)#no login
Switch3(config-line)#end
Switch3#exit
```

To set the **Administrator Mode Password** to **"cisco"** on Switch3, enter the following commands:

```
Switch3#conf t
Switch3(config)#enable secret cisco
```

If you type enable on Swtich3 CLI now that you have configured an Administrator Mode password, you will need to enter the password before the switch allows you to transition to the Administrator Mode.

You can use the **enable password** form of the command instead of the **enable secret** form, however, in that case the enable password will show in plain text when you display the configuration files. Always use the enable secret command. When using the keyword secret, the encrypted password will be display when you use the show run command.

To delete the Administrator Mode Password, you can use the following commands:

```
Switch3#conf t
Switch3(config)#no enable secret
```

Step 7: Configure Ethernet Interfaces on Switch4

Switch interfaces are enabled by default. Later in the semester you will learn that it is a security best practice to disable unused interfaces.

Disable Switch4 GigabitEthernet interface 1/0/1 by using the following commands:

```
Switch4#conf t
Switch4(config)# interface gigabitEthernet 1/0/1
Switch4(config-if)#shutdown
Switch4(config-if)#end
```

You can also disable a range of interfaces using the **range** keyword.

Disable Switch4 GigabitEthernet interfaces 1/0/2 through to GigabitEthernet interface 1/0/4 using the following commands:

```
Switch4#conf t
Switch4(config)# interface range gigabitEthernet 1/0/2 - 4
Switch4(config-if)#shutdown
Switch4(config-if)#end
```

Use the **show ip interface brief** command to validate the interface status on Switch4

What's the status of GigabitEthernet 1/0/1 - 4 interfaces? Administratively down

To re-enable Switch4 GigabitEthernet interface 1/0/1 use following commands:

```
Switch4#conf t
Switch4(config)# interface gigabitEthernet 1/0/1
Switch4(config-if)#no shutdown
Switch4(config-if)#end
```

Use the **range** keyword to re-enable GigabitEthernet interfaces 1/0/2 – 4. Then use the show ip interface brief command again.

What is the status of GigabitEthernet 1/0/1 - 4 interfaces? 1/0/1 and 1/0/2 is up, while 1/0/3 and 1/0/4 is down

Is this the status output you expected? Yes? No? Why? Yes, as switch 4 only connects to 2 devices,hence, assuming only 2 interface is up is correct.

Step 8: Configure the Switch Management Interface

In a production network, we want to be able to communicate with the switch remotely, so we don't have to physically connect to the switch whenever we need to manage it. In order for remote access to work, the switch (or other network device) must be allocated a **management IP address**. We will learn how to configure remote access in future labs, however, in this lab you will learn how to configure a management interface on the switches and allocate an IP address to it. The default management interface on Cisco devices is a virtual interface named **Vlan1.** You might have noticed this interface when using the **show ip interface brief** command.

Configure Swtich3 management **IP address** and **Subnet Mask** as per the Addressing Table above. To do this, use the following commands:

```
Switch3(config)interface vlan1
Switch3(config-if)#ip address 192.168.1.3 255.255.255.0
Switch3config-if)#no shutdown
Switch3config-if)#end
```

Configure Switch4 management IP address and Subnet Mask as per the Addressing Table above.

The term VLAN stands for Virtual Local Area Network. We can configure multiple VLANs in a switch to have multiple, isolated layer 2 virtual networks within the same physical switch. This is a concept that will be discussed in detail later in the semester. You will also learn that, if we don't have a routing (layer 3) device in our network, an IP address configured on a Vlan interface is only reachable from other devices in the same VLAN. By default, all switchports in a switch belong to VLAN 1. Therefore, by default, all devices connected to the switch will be connected to the same VLAN (i.e. VLAN 1). Now that you know this, answer the following questions:

Will PC1 be able to communicate with PC2? Yes_____

Will PC1 be able to communicate with Switch3 and Switch4? Yes_____

Will PC2 be able to communicate with Switch3 and Switch4? Yes_____

Will the switches be able to communicate with each other? Yes_____

Use the **ping** command on the switches and PCs to validate your answers. For example, if you want to send a ping request from Switch3 to Switch4, use de following command from Administrator or User Mode:

```
Switch3#ping 192.168.1.4
```

In cisco switches, a **"!"** signifies a received **ping reply**, and a **"."** signifies that the destination failed to reply. By default, a ping command in a switch sends out five ping requests, therefore a successful reply will look like this: "**!!!!!**"

Note: if you are running Part 3 of the lab using real devices (as previously suggested), PC1 and PC2 will not be available for testing. In this case, just use the ping command on the switches to validate whether or not the can communicate with each other.

Step 9: Cleaning Up

In the lab environment you must always clean the configuration settings on the devices before you release your booking. Also, remember this is the only lab practice where you should configure passwords on the devices for learning purposes.

To properly clean your switches, you must remove two files: the **startup configuration** file and the **vlan database** files. You did not configure VLANs in this lab, therefore you have not modified the default vlan configuration, however, we will erase the vlan data base for learning purposes.

Delete the startup configuration on Switch3 using the command below. You must hit Enter to confirm.

```
Switch3#write erase
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
```

Delete the vlan database on Switch3 using the command below. You must hit Enter to confirm.

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

Use the same commands to remove the **startup configuration** file and the **vlan database** files on Switch4.

Note: the vlan.dat file is created when you change the default VLAN settings. Note that you have not configured custom VLANs during this lab practice, therefore, if there weren't custom VLANs previously configured, your switches will print an error saying the vlan.dat file has not been found.

Part 4: Build the Network Using ATC equipment

In Part 4, you will use networking devices and test computers in the ATC labs to build a small network.

If you are physically in the ATC labs, complete Part 4 in full. If you are completing this practice outside the ATC labs, you are advised to complete steps 1 and 2 only, as you will not be able to use the Virtual PCs via remote access.

Step 1: Book and Power On the Required Network Devices

Use the skills learned in Lab SU-1a to perform the following tasks:

1. Go to **SmartRack** Web Interface and reserve a networking kit in your allocated room

2. Power on **Switch 3** and **Switch 4**

3. Leave all other devices powered off

4. Validate that both switches have default settings. If not, **clean up** the configuration as needed

5. Use the **show ip interface brief** command to validate device interconnections

Do the existing physical connections match the Topology Diagram on page 1?

_____

If not, what discrepancies did you find?

_____

In the ATC labs, there are two pre-cabled interconnections between Switch 3 and Switch 4. This differs from the Network Topology required for this practice, where there is only one interconnection between the switches. To match the physical topology to the Topology Diagram, we must disable the second switch interconnection.

Use the skills learned in Part 3, Step 7 to disable interface **Gi1/0/6** on **Switch 3** and **Switch4.**

Step 2: Configure the Switch Management Interface

Use the skills learned in Part 3, Step 8 to configure the management IP on **Switch 3** and **Switch 4** as per the Addressing Table.

Use the **ping** command to validate that the switches can communicate with each other.

Step 3: Start, Connect and Configure the Ethernet PC (PC 2)

A Virtual PC is a virtual computer managed by the primary operating system on a physical PC. Within the Virtual PC, you can run a unique copy of any operating system you'd like, and it will not interfere with the primary PC. The primary PCs in the ATC labs are restricted in what students can do configuration-wise, whereas in the Virtual PCs you have full access to all aspects of the computer configuration.

On the PCs in the ATC lab, you can run up to two Virtual PCs, configure them with specified IP settings and connect them to your networking devices for testing purposes. These virtual PCs are named based on how they connect to the networking equipment:

- The **Ethernet PC** uses a secondary network card installed in the computer. You will find there is an Ethernet cable connected to this secondary card. This cable extends from your desk to a patch panel in networking enclosure, and from there we can extend this connection to the switch or router we want to connect the Ethernet PC to.

- The **VAN PC** uses a Virtual Area Network connection. Physically, this connection shares the same network card as the physical PC. However, this card is partitioned to establish one connection to the Swinburne network, and another connection to the VAN infrastructure within the lab.

In this step we will start, configure and connect the **Ethernet PC (PC 2)** as per the Topology Diagram and Addressing Table.

1. Ask your instructor for assistance to extend the Ethernet connection from your desk to port **Gi1/0/13** on **Switch 4**.

2. Start the **Virtual Machine Launcher** application via the start menu on your PC.

3. From the **Virtual Machine Launcher**, within the **Cisco** menu, launch the **PC with Ethernet** virtual PC

4. In the Virtual PC, go to Control Panel → **Network Connections** (this might vary depending on the Windows OS version). A new dialog window will open.

5. Right-click the network card (most likely called Local Area Network or LAN) and select **Properties.** A new dialog window will open.

6. Select **Internet Protocol (TCP/IP)** and click on **Properties.** A new dialog window will open.

7. Select the **Use the following IP address** radio button and configure PC 2 **IP address** and **Subnet Mask** as per the Addressing Table on page 1.

8. Close all dialog windows (IP settings will not take effect until you do so)

9. Launch a DOS command line: Start Menu → Programs → Accessories → **Command Prompt**

10. At the prompt, type **ipconfig** to check the computer network configuration, make sure that the IP address and subnet mask matches the Addressing Table specifications.

Step 4: Start, Connect and Configure the VAN PC (PC 1)

In this step we will start, configure and connect the **VAN PC (PC 1)** as per the Topology Diagram and Addressing Table.

1. From the **Virtual Machine Launcher**, within the **Cisco** menu, launch the **PC with VAN** virtual PC

2. On the **Virtual Machine Launcher**, click the **Virtual Networks** tab. You should see a list of all the devices you have booked.

   Note: If this list is empty is because you have started the Virtual Machine Launcher <u>before</u> you booked the devices. In this case, you will have to exit and re-start the Virtual Machine Launcher.

3. From the list of devices, select **Switch 3**. This will establish a connection from your VAN PC to port **Gi1/0/24** on **Switch 3**.

4. Follow the steps learned on Part 4, Step 3 to **configure PC2 IP settings** on the VAN PC.

Step 5: Test your Network

You can now use **ping** and **arp** command prompt tools to test connectivity between your two virtual PCs and observe their ARP tables. You can also use **ping** to test connectivity from the PCs to the switches.

Note: you learned how to use **ping** and **arp** command prompt tools in Part 1, Step 5 and Part 2.

Can PC1 communicate with PC2? _____

Can PC1 communicate with Switch3 and Switch4? _____

Can PC2 communicate with Switch3 and Switch4? _____