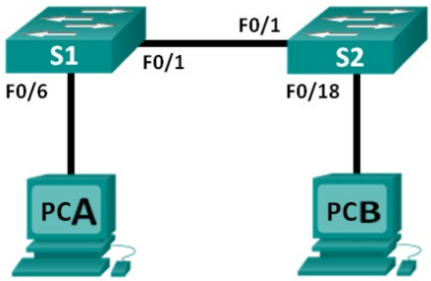
Lab 2 Activity 2.1 Packet Tracer - Building a Simple Network Not Assessed

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
PCA	NIC	192.168.1.10	255.255.255.0
PCB	NIC	192.168.1.11	255.255.255.0

Objectives

Part 1: Investigate binary values for IP Address and Subnet Mask (Not assessed)

Part 2: Set Up the Network Topology (Assessed)

Part 3: Configure PC Hosts (Assessed)

Part 4: Configure Basic Switch Settings (Assessed)

Part 5: Verify configuration (Not assessed)

Part 6: Submit Packet Tracer file

Background / Scenario

Networks are constructed of three major components: hosts, switches, and routers. In this lab, you will build a simple network with two hosts and two switches. You will investigate the relationship between the IP address and subnet Mask. You will also configure basic settings including hostname, local passwords, and login banner. Use **show** commands to display the running configuration, IOS version, and interface status.

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.

Required Resources

- Packet Tracer 8.2.2
- 2 Packet Tracer Cisco 2960 Switches
- 2 Packet Tracer PCs
- Ethernet cables as shown in the topology

Part 1: Investigate relationship between IP Address and Subnet Mask (

In Part 1, you will investigate the relationship between the IP Address and subnet masks for PCA and PCB.

Note that this activity is not assessed but you should upload the completed Packet Tracer file using the workshop upload page to ensure that you are familiar with the uploading of packet tracer files for the upcoming Packet Tracer assessments. The Packet Tracer file for the non-assessed workshop is self-marking and will give feedback in the form of marks / completion. The activity is completed correctly when the full mark is obtained.

Step 1: Compute the binary values for PCA and PCB IP addresses and Subnet Masks

IP Addresses:

Device	IP Address	Binary version of IP address
PCA	192.168.1.10	_____ . _____ . _____. _____
PCB	192.168.1.11	_____ . _____ . _____. _____

Subnet Masks:

Device	Subnet Mask	Binary version of Subnet Mask address
PCA	255.255.255.0	_____ . _____ . _____. _____
PCB	255.255.255.0	_____ . _____ . _____. _____

Step 2: Perform Logical AND on PCA IP address with PCA Subnet Mask

The subnet mask is used to isolate the network part of the IP address. This is very useful when working with subnets (a topic formally introduced in Chapter 7 of the course). To isolate the network part of the IP address, perform a LOGICAL AND on the IP address and the subnet mask for PCA and PCB.

PCA: Binary IP address: _____ . _____ . _____. _____

Binary subnet mask: _____ . _____ . _____. _____

AND

Binary Result: _____ . _____ . _____. _____

What is the decimal value of the Binary result from the above LOGICAL AND computation?

Decimal result: _____ . _____ . _____. _____

Why is part of the result the same as the original IP address, and why is the other part of the result set to 0?

_____

_____

Repeat the LOGICAL AND computation for PCB:

PCB:

Binary IP address: _____ . _____ . _____. _____

Binary subnet mask: _____ . _____ . _____. _____

AND

Binary Result: _____ . _____ . _____. _____

What is the decimal value of the Binary result from the above LOGICAL AND computation?

Decimal result: _____ . _____ . _____. _____

Are PCA and PCB on the same network?

_____

How can you tell?

_____

_____

Part 2: Set Up the Network Topology

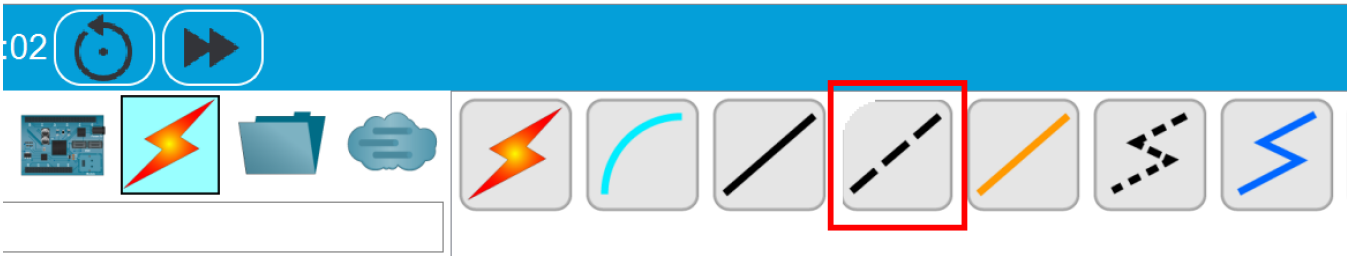
In this part you will complete the Packet Tracer activity. This Packet Tracer activity is not assessed. You must use the supplied Packet Tracer file for Lab 2 to complete the workshop as otherwise you will not be able to use the built in feed-back and scoring system that will also be used for the assessments. Using the supplied Packet Tracer file, you will cable the devices together according to the network topology.

Step 1: Create the devices.

Create all devices in the topology using Packet Tracer. Use the 2960 Switch and PC as end-devices. Update the Packet Tracer display names for the devices based on the topology.

Step 2: Connect the two switches.

Connect one end of a Cross-over Ethernet cable to F0/1 on S1 and the other end of the cable to F0/1 on S2. The cross-over cable is made of dashed lines in Packet Tracer and is used to connect two similar devices like switches together. It is identified in Packet Tracer in the image below:



You can connect a cable from one device to the next by using the cable menu (shown above), then:

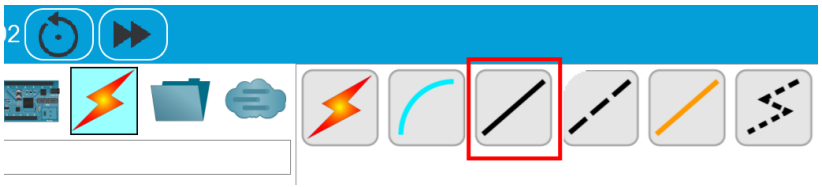
- left click on the cable type (Crossover cable in the example above)
- left click on device 1
- choosing the port to connect to from the pop-up menu
- move the mouse (and the cable) to the second device
- left-click on the second device
- finally choose the port that you want to connect to on the second device.

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 an Ethernet cable to the NIC port on PCA. In Packet Tracer this will be port FastEthernet 0. The type of cable that is required is the Copper Straight-Through cable.

The Copper Straight-Through cable is made of a single solid line in Packet Tracer and is used to connect an end device to an intermediate device like a switch. It is identified in Packet Tracer in the image below:



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 PCA has been connected correctly.

b. Connect one end of an Ethernet cable to the NIC port on PCB. In Packet Tracer this will be port FastEthernet 0. 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 PCB has been connected correctly.

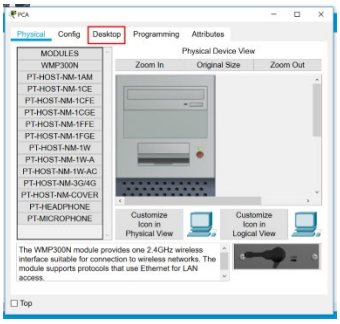
Step 4: Visually inspect network connections.

After cabling the network devices, take a moment to carefully verify the connections to minimize the time required to troubleshoot network connectivity issues later.

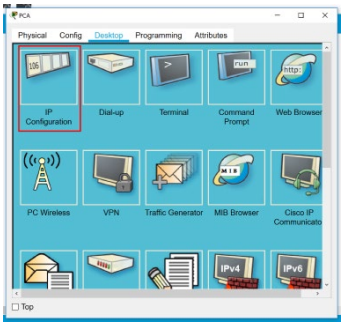
Part 3: Configure PC Hosts

Step 1: Configure PC settings.

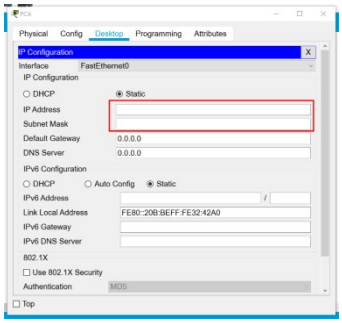
Left click on PCA and select the Desktop tab:



Then select IP Configuration:



Enter the IP address and subnet mask as specified in the Topology:

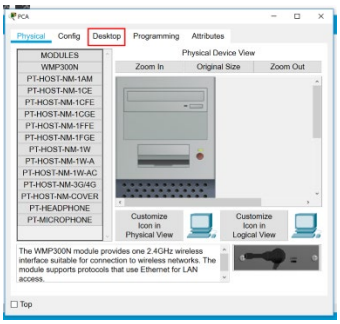


Repeat the previous steps to enter the IP address information for PCB.

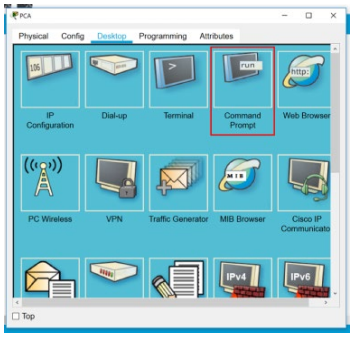
Step 2: Verify PC settings and connectivity.

Before continuing, check that there is connectivity between PCA and PCB.

Left click on PCA and select the Desktop tab:

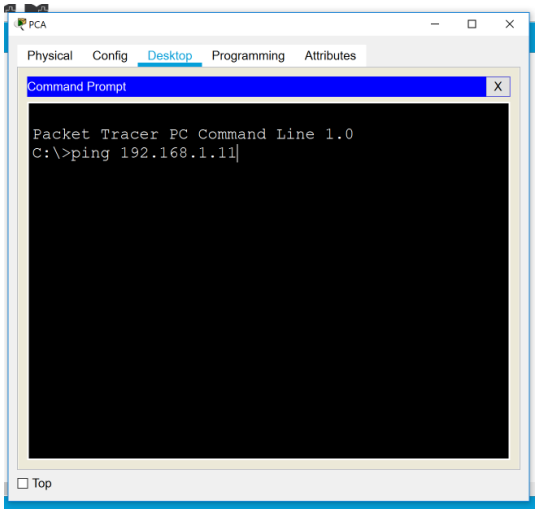


Then select Command prompt:

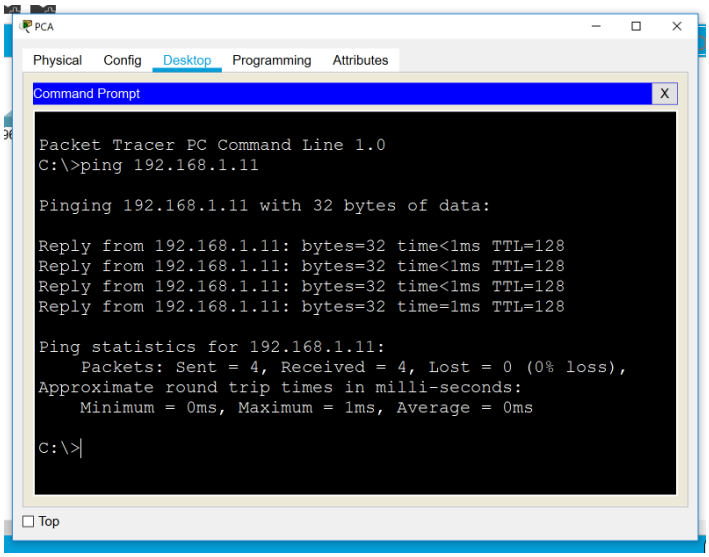


Now use the ping command to check the connectivity between PCA and PCB. The IP address for PCB is 192.168.1.11

In the command prompt window, type **ping 192.168.1.11** and press Enter:



You should see a result something like this (note that the first ping may be unsuccessful if the network is still resolving the connectivity between devices):



The information in the above ping result shows that there were 4 ping connectivity requests sent to PCB (192.168.1.11) and all 4 of them resulted in a response from PCB (0% loss).

In your Packet Tracer network, were the ping results successful? _____

If not, troubleshoot as necessary.

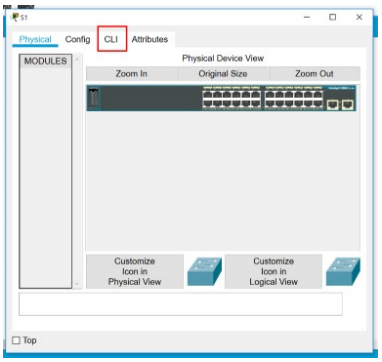
Note: If you did not get a reply from PCB, try to ping PCB again – sometimes it takes a little while for the network connectivity to resolve. If you still do not get a reply from PCB, try to ping PCA from PCB. If you are unable to get a reply from the remote PC, then ask your workshop instructor during your lab or ask for assistance during the common time.

Part 4: Configure and Verify Basic Switch Settings

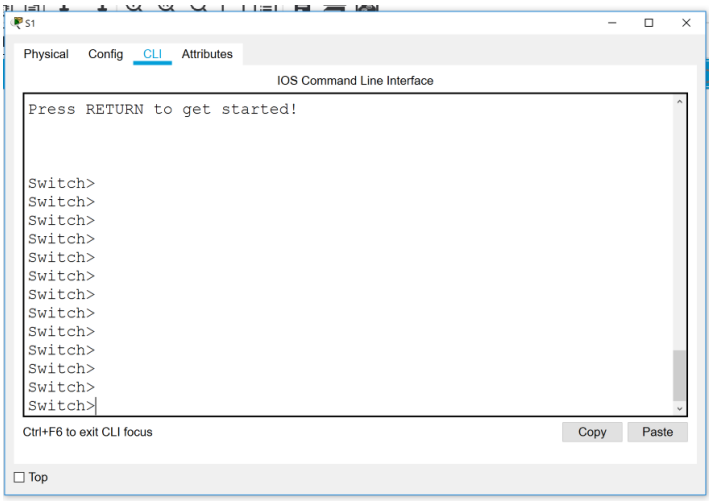
Step 1: Configure switch S1

For now, we will not use a console cable to configure the switch – instead we will configure the switch straight from the CLI window in Packet Tracer. In future assessments there may be a requirement to use the console cable.

Left click on Switch S1 and select the CLI (Command Line interface) tab:



A new window will open into which you can type commands to the device directly. Note: You may have to hit enter once or twice to wake up the device.



Step 2: Enter privileged EXEC mode.

You can access all switch commands in privileged EXEC mode. The privileged EXEC command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes are gained. Enter privileged EXEC mode by entering the **enable** command.

```
Switch> enable
Switch#
```

The prompt changed from **Switch>** to **Switch#** which indicates privileged EXEC mode.

Step 3: Enter configuration mode.

Use the **configuration terminal** command to enter configuration mode.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

Note: The prompt changed to reflect global configuration mode. You can use '**exit**' to go back one level, or '**end**' to go back to privileged exit mode directly. In this case **exit** would take you back to the privileged exec mode from Step 2 with prompt: `Switch#`

Step 4: Give the switch a name.

Use the **hostname** command to change the switch name to **S1**.

```
Switch(config)# hostname S1
S1(config)#
```

Step 5: Prevent unwanted DNS lookups.

To prevent the switch from attempting to translate incorrectly entered commands as though they were hostnames, disable the Domain Name System (DNS) lookup.

```
S1(config)# no ip domain-lookup
S1(config)#
```

Step 6: Enter local passwords.

To prevent unauthorized access to the switch, passwords must be configured and a login is required on the console line (con 0).

Set the enable secret password:

```
S1(config)# enable secret class
```

Configure the console line:

```
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)#
```

To prevent the switch from interrupting you when typing commands, turn on synchronous logging messages from within the console line configuration.

```
S1(config)# line con 0
S1(config-line)# logging synchronous
S1(config-line)# exit
S1(config)#
```

Step 7: Enter a login MOTD banner.

A login banner, known as the message of the day (MOTD) banner, should be configured to warn anyone accessing the switch that unauthorized access will not be tolerated.

The **banner motd** command requires the use of delimiters to identify the content of the banner message. The delimiting character can be any character as long as it does not occur in the message. For this reason, symbols, such as the **single quote '**, are often used.

Important: Please enter the following banner exactly as written. Using the correct and approved language is critical to ensure that legal requirements are met. If you change any character in the **Unauthorised access is strictly prohibited and prosecuted to the full extent of the law.** (including the final full-stop at the end) the banner will be marked as incorrect as it does not exactly meet the requirement:

```
S1(config)# banner motd 'Unauthorised access is strictly prohibited and
prosecuted to the full extent of the law.'
S1(config)# exit
S1#
```

Step 8: Configure Switch S2.

Repeat Steps 1 to 7 for Switch S2 – make sure that the name for Switch 2 is correctly configured as S2.

Part 5: Verify Basic Switch Settings

The **show running-config** command displays the entire running configuration, one page at a time. Use the spacebar to advance paging when you see the "- - More –" prompt. The commands configured in Steps 1 – 8 are highlighted below for S1. Also confirm for S2.

```
S1# show running-config
Building configuration...

Current configuration : 1409 bytes
!
! Last configuration change at 03:49:17 UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
<output omitted>
!
banner motd ^C
Unauthorized access is strictly prohibited and prosecuted to the full extent of the
law. ^C
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 login
line vty 5 15
 login
!
end
S1#
```

Part 6: Submit your Packet Tracer file

When you have completed the configuration activities in your Packet Tracer file, please save it as a .pka file (do not save as .pkz), and submit it using the Lab 2 submission point. By submitting it you will be able to become familiar with the submission process used for later Packet Tracer Assessments. We may also use your submissions to give feedback on if your name / student number has been correctly assigned to the file.