Experiment#03

Lab# 3.1: - Packet Tracer - Navigating the two different networks.

Topology

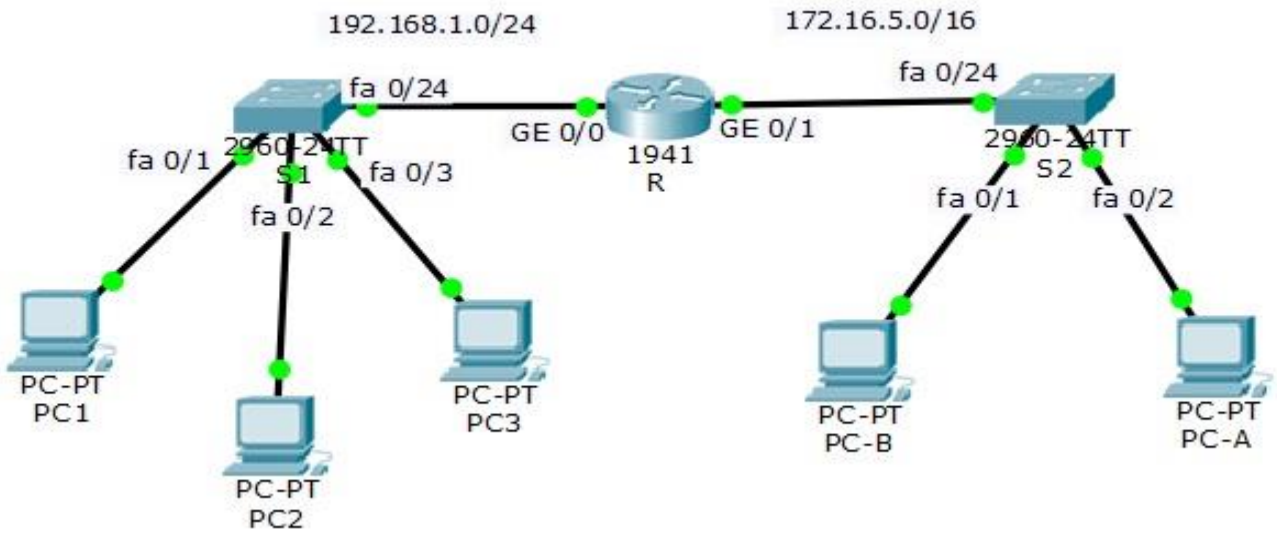


Figure 3.1

Objectives

Part 1: Connections using copper straight through wires.

Part 2: Accessing the CLI of each network device to do basic configuration.

Part 3: Assign IP address to each device and router's interfaces.

Part 4: Configure telnet on each network device.

Part 5: Set default gateways.

Part 6: Verify Network Connectivity by using PING.

Part 7: Establish telnet session to each network device via command prompt of different PCs.

Part 8: Home activity.

Part 1: Basic Connections, Accessing the CLI and Exploring Help

In Part 1 of this activity, you connect the all the devices together using copper straight through connection as mentioned in figure 3.1.

Connect PC1 to S1 using a console cable.

a. Click the **Connections** icon (the one that looks like a lightning bolt) in the lower left corner of the Packet Tracer window.

b. Select the black copper straight through cable by clicking it. The mouse pointer will change to what appears to be a connector with a cable dangling off of it.

c. Click on **PC1**; a window displays an option for a fast Ethernet connection.

d. Drag the other end of the copper straight through connection to the S1 switch and click the switch to bring up the connection list.

e. Select the Fast Ethernet 0/1 port to complete the connection.

f. Click on **PC2**; a window displays an option for a fast Ethernet connection.

g. Drag the other end of the copper straight through connection to the S1 switch and click the switch to bring up the connection list.

h. Select the Fast Ethernet 0/2 port to complete the connection.

i. Click on **PC3**; a window displays an option for a fast Ethernet connection.

j. Drag the other end of the copper straight through connection to the S1 switch and click the switch to bring up the connection list.

k. Select the Fast Ethernet 0/3 port to complete the connection.

l. Click on **PC-A**; a window displays an option for a fast Ethernet connection.

m. Drag the other end of the copper straight through connection to the S2 switch and click the switch to bring up the connection list.

n. Select the Fast Ethernet 0/1 port to complete the connection.

o. Click on **PC-B**; a window displays an option for a fast Ethernet connection.

p. Drag the other end of the copper straight through connection to the S2 switch and click the switch to bring up the connection list.

q. Select the Fast Ethernet 0/2 port to complete the connection.

r. Click on **R router**; a window displays some option for Gigabit Ethernet or fast Ethernet ports. Select the Fast Ethernet 0/0 or Gigabit Ethernet 0/0.

s. Drag the other end of the copper straight through connection to the S1 switch and click the switch to bring up the connection list.

t. Select the Fast Ethernet 0/24 port to complete the connection.

u. Again Click on **R router**; a window displays some option for Gigabit Ethernet or fast Ethernet ports. Select the Fast Ethernet 0/1 or Gigabit Ethernet 0/1.

v. Drag the other end of the copper straight through connection to the S2 switch and click the switch to bring up the connection list.

w. Select the Fast Ethernet 0/24 port to complete the connection.

Part 2: Accessing the CLI of each network device to do basic configuration.

- Click on S**1switch** and then select the CLI tab to access the CISCO IOS.
- Do some basic configurations like setting the clock, assign name to each network device, set banner, console password, privilege mode password or enable secret and encrypt them.

Step 1: Assign a name to a switch.

To configure parameters on a switch, you may be required to move between various configuration modes. Notice how the prompt changes as you navigate through the switch.

Switch# **clock set 15:00:00 31 Jan 2035**
Switch# **configure terminal**
Switch(config)# **hostname S1**
S1(config)# **exit**
S1#

Step 2: Secure access to the console line.

To secure access to the console line, access config-line mode and set the console password to **letmein**.

S1# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# **line console 0**
S1(config-line)# **password letmein**
S1(config-line)# **login**
S1(config-line)# **exit**
S1(config)# **exit**
%SYS-5-CONFIG_I: Configured from console by console
S1#

Step 3: Verify that console access is secured.

Exit privileged mode to verify that the console port password is in effect.

S1# **exit**
Switch con0 is now available
Press RETURN to get started.

User Access Verification
Password:
S1>

Note: If the switch did not prompt you for a password, then you did not configure the **login** parameter in Step 2.

Step 4: Secure privileged mode access.

Set the **enable** password to **c1$c0**. This password protects access to privileged mode.

Note: The **0** in **c1$c0** is a zero, not a capital O. This password will not grade as correct until after you encrypt it in Step 8.

S1> **enable**
S1# **configure terminal**
S1(config)# **enable password c1$c0**
S1(config)# **exit**
%SYS-5-CONFIG_I: Configured from console by console
S1#

Step 5: Verify that privileged mode access is secure.

a. Enter the **exit** command again to log out of the switch.

b. Press **<Enter>** and you will now be asked for a password:

User Access Verification
Password:

c. The first password is the console password you configured for **line con 0**. Enter this password to return to user EXEC mode.

d. Enter the command to access privileged mode.

e. Enter the second password you configured to protect privileged EXEC mode.

f. Verify your configurations by examining the contents of the running-configuration file:

S1# **show running-config**

Notice how the console and enable passwords are both in plain text. This could pose a security risk if someone is looking over your shoulder.

Step 6: Configure an encrypted password to secure access to privileged mode.

The **enable password** should be replaced with the newer encrypted secret password using the **enable secret** command. Set the enable secret password to **itsasecret**.

S1# **config t**
S1(config)# **enable secret itsasecret**
S1(config)# **exit**
S1#

Note: The **enable secret** password overrides the **enable** password. If both are configured on the switch, you must enter the **enable secret** password to enter privileged EXEC mode.

Step 7: Verify that the enable secret password is added to the configuration file.

a. Enter the **show running-config** command again to verify the new **enable secret** password is configured.

Note: You can abbreviate **show running-config** as
S1# **show run**

Step 8: Encrypt the enable and console passwords.

As you noticed in Step 7, the **enable secret** password was encrypted, but the **enable** and **console** passwords were still in plain text. We will now encrypt these plain text passwords using the **service password-encryption** command.

S1# **config t**
S1(config)# **service password-encryption**
S1(config)# **exit**

Configure a MOTD Banner

Step 9: Configure a message of the day (MOTD) banner.

The Cisco IOS command set includes a feature that allows you to configure messages that anyone logging onto the switch sees. These messages are called message of the day, or MOTD banners. Enclose the banner text in quotations or use a delimiter different from any character appearing in the MOTD string.

S1# **config t**
S1(config)# **banner motd "This is a secure system. Authorized Access Only!"**
S1(config)# **exit**
%SYS-5-CONFIG_I: Configured from console by console
S1#

Step 10: Save Configuration Files to NVRAM

- **Verify that the configuration is accurate using the show run command.**
- **Save the configuration file.**

You have completed the basic configuration of the switch. Now back up the running configuration file to NVRAM to ensure that the changes made are not lost if the system is rebooted or loses power.

S1# **copy running-config startup-config**
Destination filename [startup-config]?**[Enter]**
Building configuration...
[OK]

Configure Router (R) and Switch2 (S2):

You have completed the configuration on S1. You will now configure S2. If you cannot remember the commands, refer to Step 1 to 10 for assistance.

Configure S2 with the following parameters:

a. Name device: **S2**

b. Protect access to the console using the **letmein** password.

c. Configure an enable password of **c1$c0** and an enable secret password of **itsasecret**.

d. Configure a message to those logging into the switch with the following message:

Authorized access only. Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law.

e. Encrypt all plain text passwords.

f. Ensure that the configuration is correct.

g. Save the configuration file to avoid loss if the switch is powered down.

Part 3 and 4: - Implement Basic Addressing and Connectivity

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R	Gi 0/0	192.168.1.1	255.255.255.0	---
R	Gi 0/1	172.16.5.1	255.255.0.0	---
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
S2	VLAN 1	172.16.5.2	255.255.0.0	172.16.5.1
PC-A	NIC	172.16.5.3	255.255.0.0	172.16.5.1
PC-**B**	NIC	172.16.5.4	255.255.0.0	172.16.5.1
PC1	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC2	NIC	192.168.1.4	255.255.255.0	192.168.1.1
PC2	NIC	192.168.1.4	255.255.255.0	192.168.1.1

table 3.1

Configure the PCs

Configure PC1, PC2 and PC3 with IP addresses, subnet mask and default gateway.

Step 1: Configure both PCs with IP addresses.

a. Click **PC-A**, and then click the **Desktop** tab.

b. Click **IP Configuration**. In the **Addressing Table** above, you can see that the IP address for PC1 is 172.16.5.3, the subnet mask is 255.255.0.0 and the default gateway is 172.16.5.1. Enter these information for PC-A in the **IP Configuration** window.

c. Repeat steps 1a and 1b for PC-B, PC1, PC2 and PC3.

Configure the Switch Management Interface

Configure S1 and S2 with an IP address.

Step 2: Configure S1 with an IP address. Also configure Virtual Terminal Line (VTY):

a. Use the following commands to configure S1 with an IP address.

S1 #**configure terminal**
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# **interface vlan 1**
S1(config-if)# **ip address 192.168.1.2 255.255.255.0**
S1(config-if)# **no shutdown**
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
S1(config-if)#
S1(config-if)# **exit**
S1#

b. Configure the virtual terminal (VTY) line for the switch to allow Telnet access. If you do not configure a VTY password, you will not be able to Telnet to the switch.

```
S1(config)# line vty 0 4
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# end
S1#
```

Step 2: Configure S2 with an IP addresses.

Use the information in the addressing table to configure S2 with an IP address.

Step 3: Configure Router's (R) Interfaces with IP addresses.

R> enable
R # configure terminal
R (config) # interface gigabitEthernet 0/0
R(config-if)# **ip address 192.168.1.2 255.255.255.0**
R(config-if)# **no shutdown**
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
R(config-if)#
R(config-if)# **exit**
R (config) # interface gigabitEthernet 0/1
R(config-if)# **ip address 172.16.5.1 255.255.0.0**
R(config-if)# **no shutdown**
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
R(config-if)#
R(config-if)# **end**
R# copy run start
R#exit

Step 4: Verify the IP address configuration on R, S1 and S2.

Use the **show ip interface brief** command to display the IP address and status of the all the switch ports and interfaces. Alternatively, you can also use the **show running-config** command.

Part 5: - Configure default gateway on both Switches (S1 and S2):

On switch, following command is used to configure default gateway

```
S1 >en
S1 # configure terminal
S1 (config)# ip default-gateway 192.168.1.1
S1 (config)#exit
S1 # copy run start
```

Likewise on S2:

```
S2 >en
S2 # configure terminal
S2 (config)# ip default-gateway 172.16.5.1
S2 (config)#exit
S2 # copy run start
```

Part 6: Verify Network Connectivity by using PING .

Network connectivity can be verified using the **ping** command. It is very important that connectivity exists throughout the network. Corrective action must be taken if there is a failure. Ping S1's and S2's IP address from PC1, PC2, PC3,PC-A and PC-B.

a. Click **PC-A**, and then click the **Desktop** tab.

b. Click **Command Prompt**.

c. Ping the IP address for PC-B.

d. Ping the IP address for S1.

e. Ping the IP address for S2.

f. Ping the IP address of default gateway.

g. Ping the IP address for PC1.

h. Ping the IP address for PC2.

i. Ping the IP address for PC3.

Note: You can also use the same **ping** command on the switch CLI and on PCs.

All pings should be successful. If your first ping result is 80%, retry; it should now be 100%. You will learn why a ping may fail the first time later in your studies. If you are unable to ping any of the devices, recheck your configuration for errors.

Part 7: Test and verify remote management of S1.

You will now use Telnet to remotely access the switch S1 using the SVI management address. In this lab, PC-A and S1 reside side by side. In a production network, the switch could be in a wiring closet on the top floor while your management PC is located on the ground floor. Telnet is not a secure protocol. However, you will use it in this lab to test remote access. All information sent by Telnet, including passwords and commands, is sent across the session in plain text. In subsequent labs, you will use Secure Shell (SSH) to remotely access network devices.

Note: Windows 7 does not natively support Telnet. The administrator must enable this protocol. To install the Telnet client, open a command prompt window and type **pkgmgr /iu:"TelnetClient"**.

C:\Users\NetAcad> **pkgmgr /iu:"TelnetClient"**

j. With the command prompt window still open on PC-A, issue a Telnet command to connect to S1 via the SVI management address. The password is **cisco**.

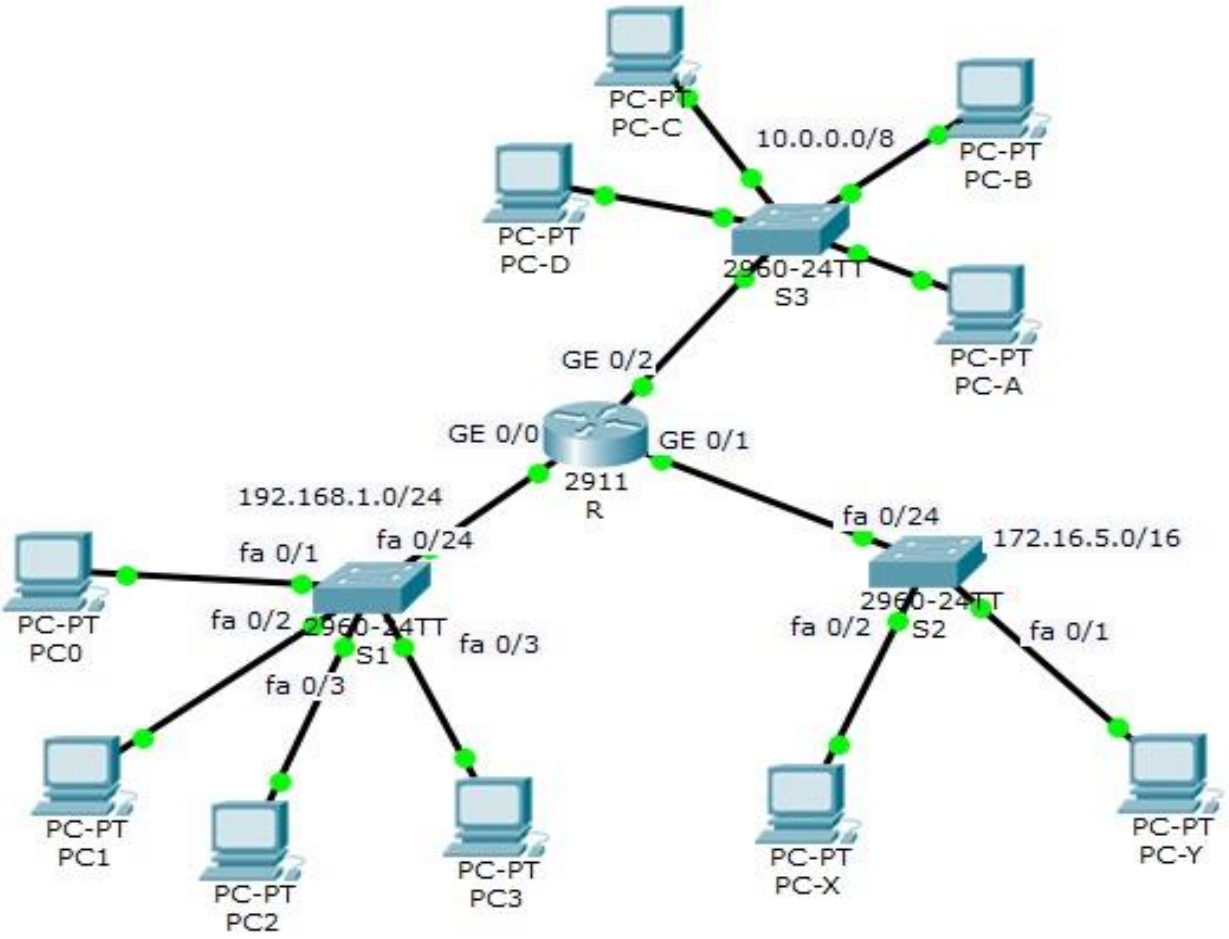
C:\Users\NetAcad> **telnet 192.168.1.2**

Your output should be similar to the following screen:

k. After entering the **cisco** password, you will be at the user EXEC mode prompt. Type **enable** at the prompt. Enter the **class** password to enter privileged EXEC mode and issue a **show run** command.

Part 8: Home Activity:

Complete the addressing table of the given topology. Configure a following topology in the light of experiment#3 by using c2911(router). Attach the screen shots of the **topology**, **addressing table** and **startup configuration of each intermediary device** at end of this experiment.



Lab's Evaluation Sheet

Students Registration No:	
Date Performed:	
Group No:	
Date of Submission:	

Sr. No.	Categories	Total Marks/Grade	Marks /Grade Obtained
1	Student's Behavior	2.5	
2	Lab Performance	2.5	
3	On Time Submission	5	
4	Home Activity	10	
	Net Result	20	

Examined By: (Instructor's Name & Initial's)

Date