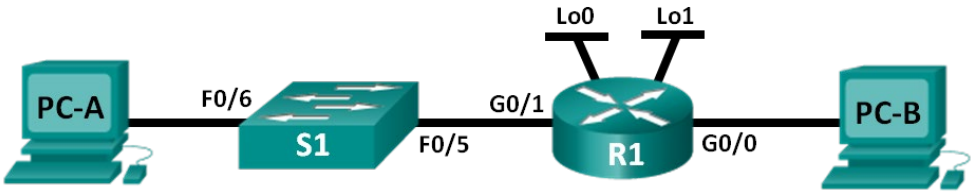
Activity 8.1 – Configuring Subnetted IPv4 Addressing

PACKET TRACER

Not assessed

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	10.16.0.1	255.240.0.0	N/A
	G0/1	10.32.0.1	255.240.0.0	N/A
	Lo0	10.48.0.1	255.240.0.0	N/A
	Lo1	10.64.0.1	255.240.0.0	N/A
S1	VLAN 1	10.47.255.254	255.240.0.0	10.32.0.1
PC-A	NIC	10.32.0.2	255.240.0.0	10.32.0.1
PC-B	NIC	10.16.0.2	255.240.0.0	10.16.0.1

Objectives

Part 1: Configure the Devices

Part 2: Test and Troubleshoot the Network

Background / Scenario

You will configure the host PCs, switch and router interfaces, including loopback interfaces. The loopback interfaces are created to simulate additional LANs attached to router R1. You will also set up ssh to allow remote connections to the router instead of using telnet. You will not configure ssh for remote access to the switch in this exercise and will continue to use telnet for remote access to the switch.

After the network devices and host PCs have been configured, you will use the **ping** command to test for network connectivity.

Required Resources

Packet Tracer 8.2.2

Part 1: Configure the Devices

In Part 1, set up the network topology and configure settings on the PCs, Switch and Router, such as the router Gigabit Ethernet interface IP addresses, and the PC's IP addresses, subnet masks, and default gateways. Use only a **1941 Router** and **2960 Switch**. Refer to the Addressing Table for device names and address information.

Step 1: Fully configure the switch as per the standard configuration steps discussed in previous labs.

1) Correct device names as per the topology
2) DNS lookup turned off
3) IP address as listed in Addressing Table
4) Configure the default gateway for the Switch
5) Clear text passwords encrypted.
6) **cisco** as the console and vty passwords with login and logging synchronous enabled
7) **class** as the privileged EXEC password
8) Banner that warns anyone accessing the device that unauthorized access is prohibited. With the following text:

Unauthorised access is prohibited and will be strictly prosecuted.

Step 2: Configure the router.

Configure the routers as per the standard configuration in previous labs:

1) Assign a device name to the router.
2) Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
3) Assign **class** as the privileged EXEC encrypted password.
4) Assign **cisco** as the console password and enable login and logging synchronous.
5) Assign **cisco** as the VTY password and enable login and logging synchronous. Verify the number of vty lines on the router.
6) Encrypt the clear text passwords.
7) Create a banner that warns anyone accessing the device:

Unauthorised access is prohibited and you will be strictly prosecuted.

8) Assign *IPv4* addresses to all interfaces on Router as per the addressing table and enable them.
9) Setting up ssh:

Using Telnet to connect to a network device is a security risk because all information is transmitted in a clear text format. SSH encrypts the session data and provides device authentication, which is why SSH is recommended for remote connections. You will now configure the router to accept SSH connections over the VTY lines:

The device name and domain are used as part of the cryptographic key when it is generated. Therefore, these names must be entered prior to issuing the crypto key command. The hostname has already been entered in Step 2.1 (above). We need to supply a domain name:

Step A: Configure the domain for the device.

```
R1(config)# ip domain-name networklab.com
```

Step B: Configure the encryption key method. Please note this command has two parts, first the 'crypto key generate rsa' command, then you will be prompted for the number of bits to use. We will use 1024 bits.

```
R1(config)# crypto key generate rsa

      The name for the keys will be: R1.networklab.com
      Choose the size of the key modulus in the range of 360 to
      2048 for your General Purpose Keys. Choosing a key modulus
      greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024

      % Generating 1024 bit RSA keys, keys will be non-
      exportable...[OK]
      (elapsed time was 1 seconds)
      *Jan 28 21:09:29.867: %SSH-5-ENABLED: SSH 1.99 has been enabled

R1(config)#
```

Step C: Configure a local database username. We will use **admin** as username, with **adminpass** as password.

```
R1(config)# username admin privilege 15 secret adminpass
```

Note: A privilege level of 15 gives the user administrator rights.

Step D: Enable SSH on the VTY lines.

a. Enable only SSH on the inbound VTY lines using the **transport input** command.

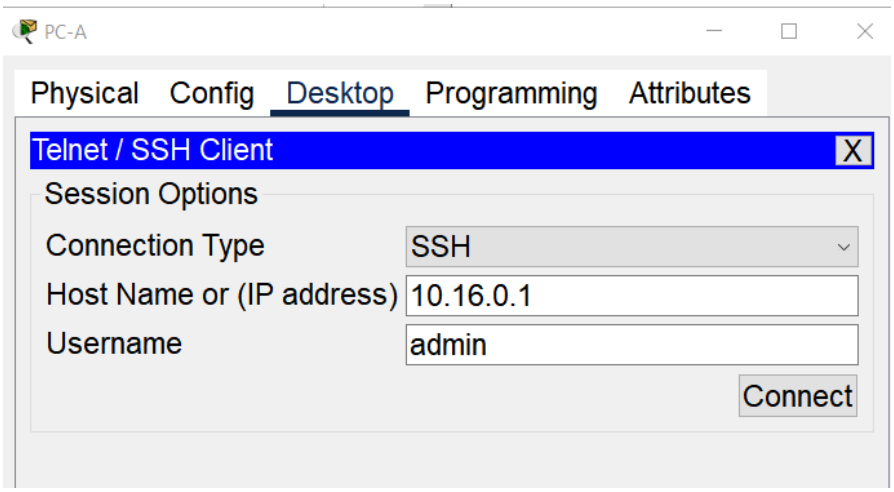
```
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
```

b. Change the login method to use the local database for user verification.

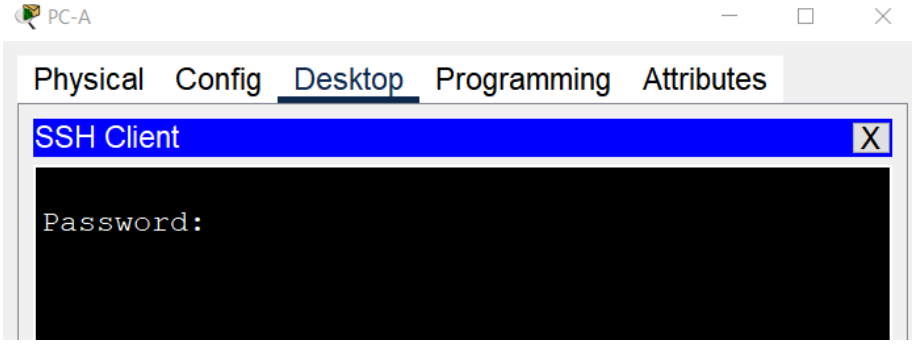
```
R1(config-line)# login local
R1(config-line)# end
R1#
```

Testing the SSH connection:

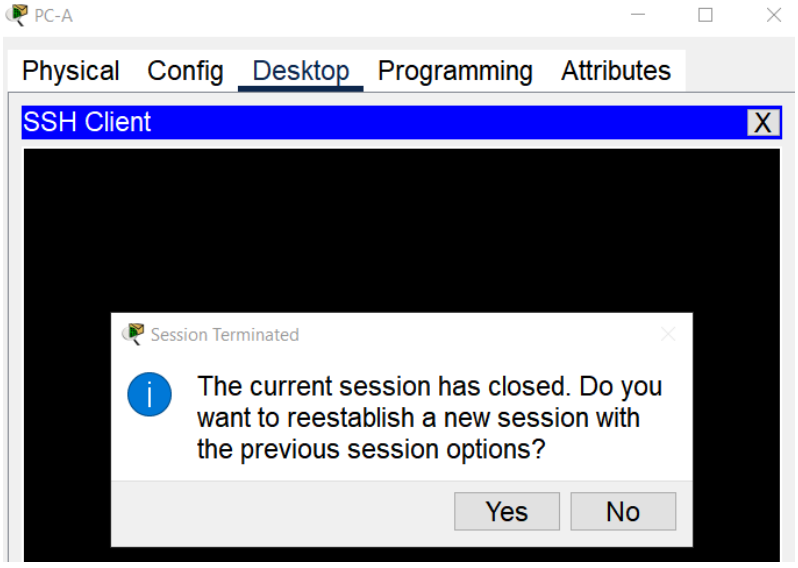
Establish an SSH session to R1. Use the username **admin** and password **adminpass**. You should be able to establish an SSH session with R1. Use Telnet/ssh to make the connection to R1 G0/0 (10.16.0.1):



If the configuration is correct you will see a password prompt:



Note: If you try to use the telnet option to connect to R1 you will get an error as telnet is not enable based on the above configuration:



Step 3: Configure the PC interfaces.

a. Configure the IP address, subnet mask, and default gateway settings on PC-A.

b. Configure the IP address, subnet mask, and default gateway settings on PC-B.

Part 2: Test and Troubleshoot the Network:

Use appropriate commands to verify the configuration