Logo

Description automatically generatedLogo

Description automatically generated

**Polytechnic University of the Philippines**

**College of Engineering**

**Computer Engineering Department**

**CMPE 30174**

**Computer Networks and Security**

**MP -1 Perform Chapter 1 Activities**

**Tedie N. Villacuatro**

Submitted by

**BSCpE 3-3**

Course/Year/Section

**April 12, 2022**

Date Submitted

**Engr. Jake Binuya**

Submitted to

**Villacuatro, Tedie N. BSCOE 3-3**

**Packet Tracer - Configure SSH**

# Addressing Table

| **Device** | **Interface** | **IP Address** | **Subnet Mask** |
| --- | --- | --- | --- |
| S1 | VLAN 1 | 10.10.10.2 | 255.255.255.0 |
| PC1 | NIC | 10.10.10.10 | 255.255.255.0 |

# Objectives

**Part 1: Secure Passwords**

**Part 2: Encrypt Communications**

**Part 3: Verify SSH Implementation**

# Background

SSH should replace Telnet for management connections. Telnet uses insecure plain text communications. SSH provides security for remote connections by providing strong encryption of all transmitted data between devices. In this activity, you will secure a remote switch with password encryption and SSH.

# Instructions

## Part 1: Secure Passwords

a.     Using the command prompt on **PC1**, Telnet to **S1**. The user EXEC and privileged EXEC password is **cisco**.

b.     Save the current configuration so that any mistakes you might make can be reversed by toggling the power for **S1**.

c.     Show the current configuration and note that the passwords are in plain text. Enter the command that encrypts plain text passwords:

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

d.     Verify that the passwords are encrypted.

## Part 2: Encrypt Communications

### Step 1: Set the IP domain name and generate secure keys.

It is generally not safe to use Telnet, because data is transferred in plain text. Therefore, use SSH whenever it is available.

a.     Configure the domain name to be **netacad.pka**.

b.     Secure keys are needed to encrypt the data. Generate the RSA keys using a 1024 key length.

### Step 2: Create an SSH user and reconfigure the VTY lines for SSH-only access.

a.     Create an **administrator** user with **cisco** as the secret password.

b.     Configure the VTY lines to check the local username database for login credentials and to only allow SSH for remote access. Remove the existing vty line password.

### Step 3: Verify SSH Implementation

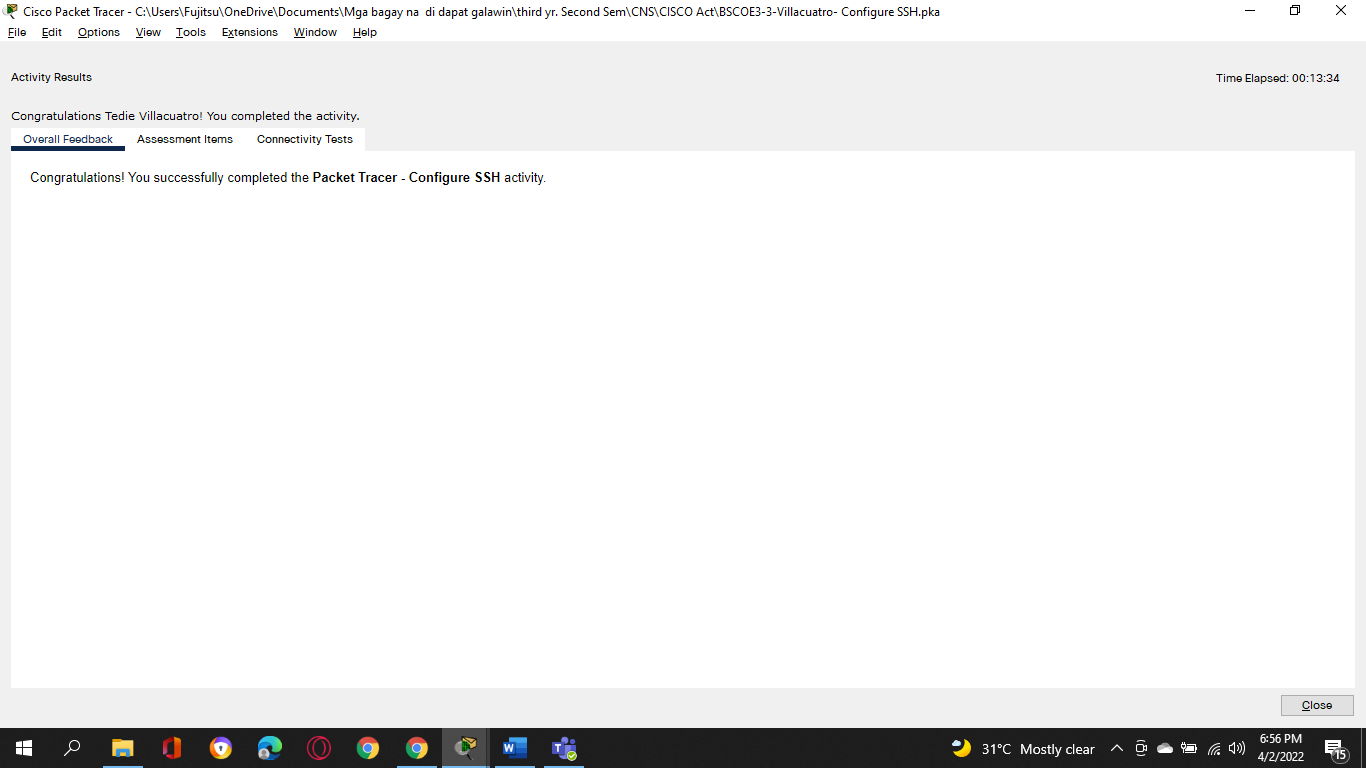
a.     Exit the Telnet session and attempt to log back in using Telnet. The attempt should fail.

b.     Attempt to log in using SSH. Type **ssh** and press **Enter** without any parameters to reveal the command usage instructions. **Hint**: The **-l** option is the letter “L”, not the number 1.

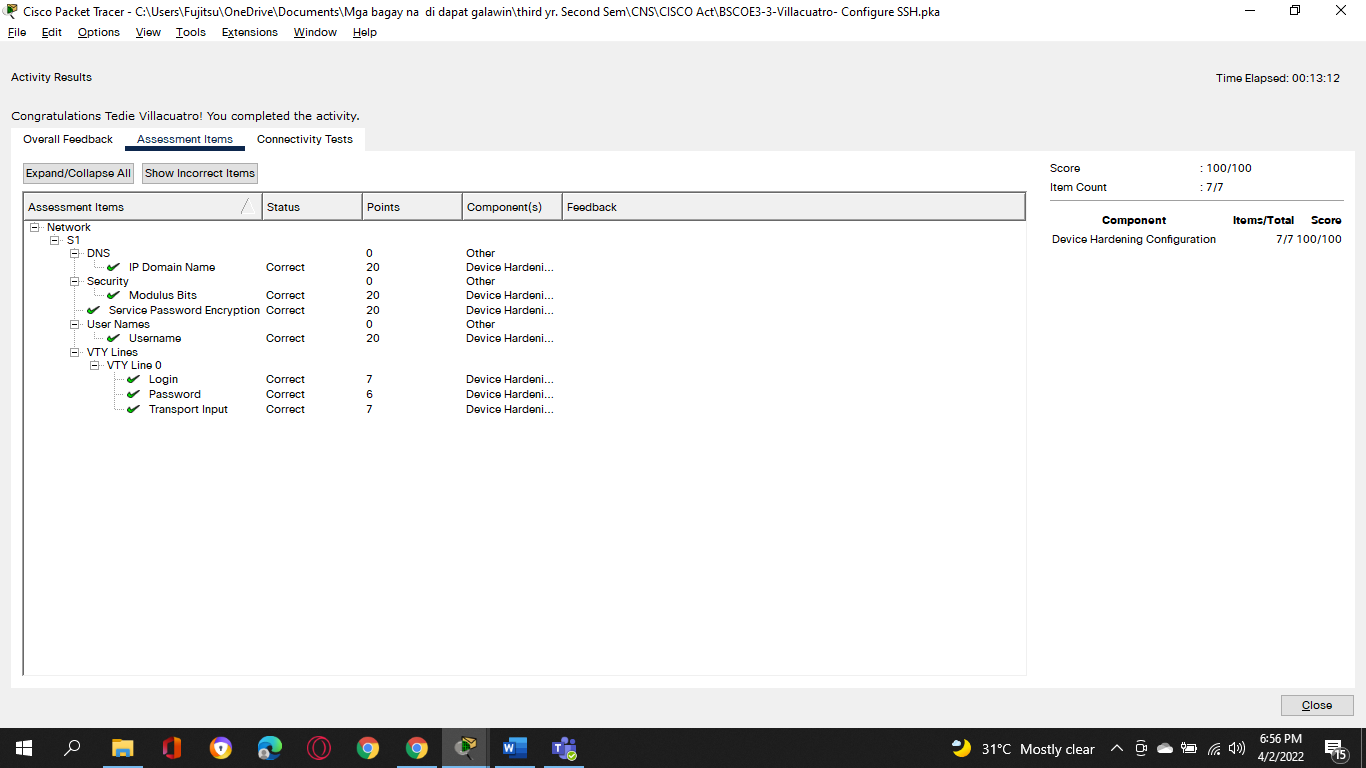
c.     Upon successful login, enter privileged EXEC mode and save the configuration. If you were unable to successfully access **S1**, toggle the power and begin again at Part 1.

*End of document*

Activity completion:



Assessment Items:



**Villacuatro, Tedie N.**

**BSCOE 3-3**

**Packet Tracer - Verify Directly Connected Networks**

**Addressing Table**

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address / Prefix** | **Default Gateway** |
| R1 | G0/0/0 | 172.16.20.1/25 | N/A |
| *R1* | G0/0/1 | 172.16.20.129/25 | N/A |
| *R1* | S0/1/0 | 209.165.200.225/30 | N/A |
| PC1 | NIC | 172.16.20.10/25 | 172.16.20.1 |
| PC2 | NIC | 172.16.20.138/25 | 172.16.20.129 |
| R2 | G0/0/0 | 2001:db8:c0de:12::1/64 | N/A |
| *R2* | G0/0/1 | 2001:db8:c0de:13::1/64 | N/A |
| *R2* | S0/1/1 | 2001:db8:c0de:11::1/64 | N/A |
| *R2* | *S0/1/1* | fe80::2 | N/A |
| PC3 | NIC | 2001:db8:c0de:12::a/64 | fe80::2 |
| PC4 | NIC | 2001:db8:c0de:13::a/64 | fe80::2 |

**Objectives**

·         Verify IPv4 Directly Connected Networks

·         Verify IPv6 Directly Connected Networks

·         Troubleshoot connectivity issues.

**Background**

Routers R1 and R2 each have two LANs. Your task is to verify the addressing on each device and verify connectivity between the LANs.

**Note**: The user EXEC password is **cisco**. The privileged EXEC password is **class**.

**Instructions**

**Part 1: Verify IPv4 Directly Connected Networks**

**Step 1: Verify IPv4 addresses and port status on R1.**

a.     Check the status of the configured interfaces by filtering the output.

*Open configuration window*

R1# **show ip interface brief | exclude unassigned**

b.     Based on the output, correct any port status problems that you see.

c.     Refer to the **Addressing Table** and verify the IP addresses configured on R1. Make any corrections to addressing if necessary.

d.     Display the routing table by filtering to start the output at the word **Gateway**.

**Note:** Terms that are used to filter output can be shortened to match text as long as the match is unique. For example, Gateway, Gate, and Ga will have the same effect. G will not. Filtering is case-sensitive

R1# **show ip route | begin Gate**

Question:

What is the Gateway of last resort address?

* **Gateway of last resort is 209.165.200.226 to network 0.0.0.0**

e.     Display interface information and filter for **Description** or **connected**.

**Note**: When using **include** or **exclude** multiple searches can be performed by separating the search strings with a pipe symbol ( **|** )

R1# **show interface | include Desc|conn**

Question:

What is the Circuit ID displayed from your output?

* **CIRCUIT ID BCB123450001**

f.      Display specific interface information for G0/0/0 by filtering for **duplex**.

Question:

What is the duplex setting, speed, and media type?

* **Full duplex, 100Mb/s, Media type is RJ45**

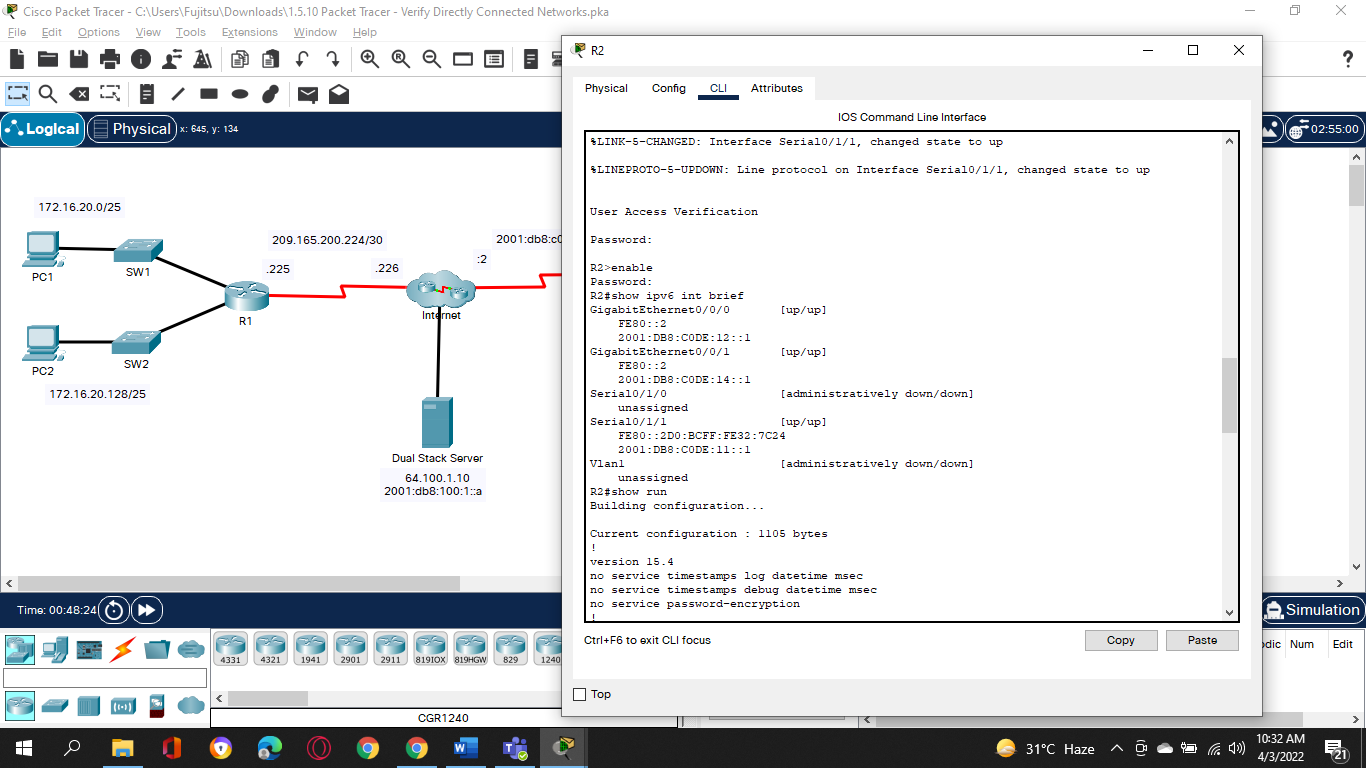
*Close configuration window*

**Step 2: Verify connectivity.**

**PC1** and **PC2** should be able to ping each other and the **Dual Stack Server**. If not, verify the status of the interfaces and the IP address assignments.

**Part 2: Verify IPv6 Directly Connected Networks**

**Step 1: Verify IPv6 addresses and port status on R2.**

a.     Check the status of the configured interfaces.

*Open configuration window*

R2# **show ipv6 int brief**

Question:

What is the status of the configured interfaces?

**Most of the interfaces have an up/up status except for serial 0/1/0 and the Vlan1, both have a status “administratively down /down”.**

**It is noted that IPv6 address of interface Gigabit Ethernet 0/0/1 is different compare to the table.**

b.     Refer to the **Addressing Table** and make any corrections to addressing as necessary.

**Note**: When changing an IPv6 address it is necessary to remove the incorrect address since an interface is capable of supporting multiple IPv6 networks.

R2(config)# **int g0/0/1**

R2(config-if)# **no ipv6 address 2001:db8:c0de:14::1/64**

Question:

Configure the correct address on the interface.

c.     Display the IPv6 routing table.

**Note**: Filtering commands do not presently work with the IPv6 commands.

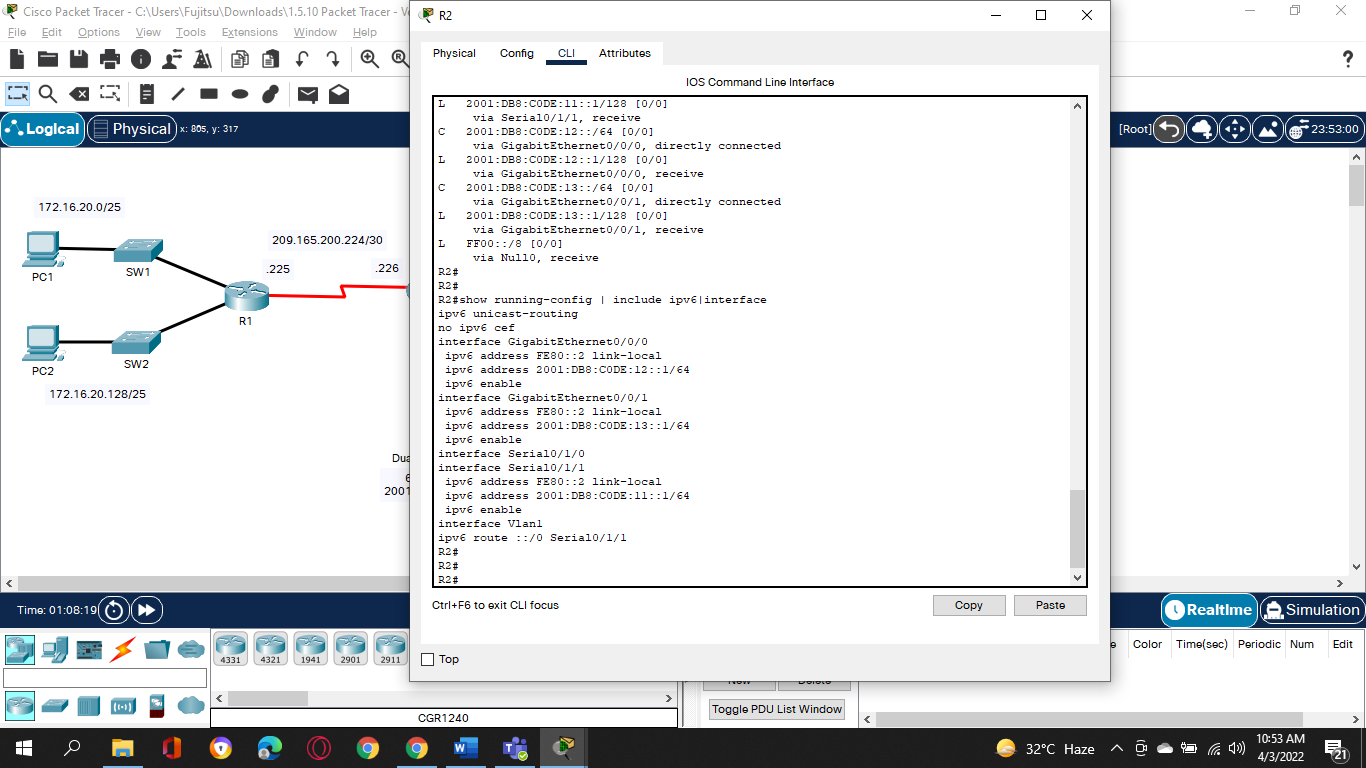
d.     Display all IPv6 addressing configured on interfaces by filtering the output of the **running-config**.

Filter the output on **R2** for **ipv6** or **interface**.

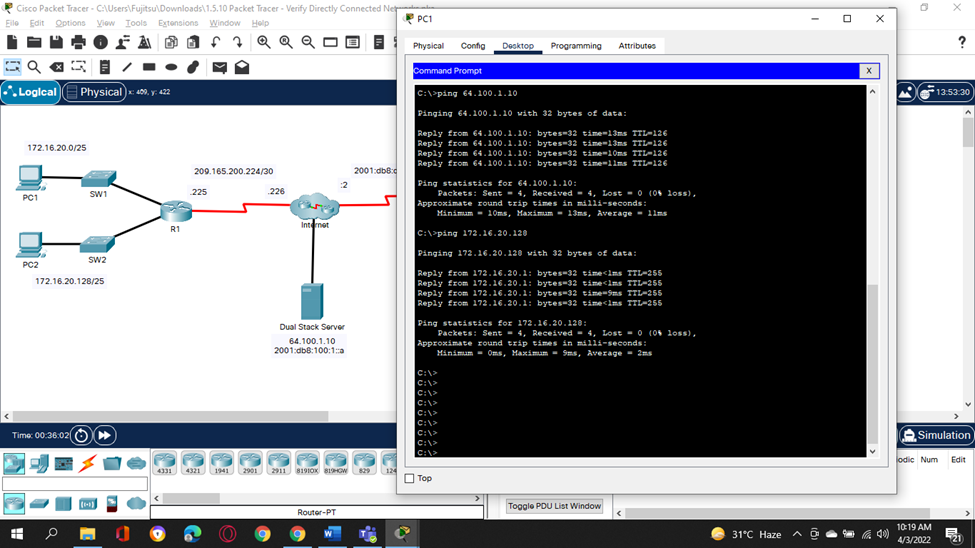
R2# **sh run | include ipv6|interface**

Question:

How many addresses are configured on each Gigabit interface?

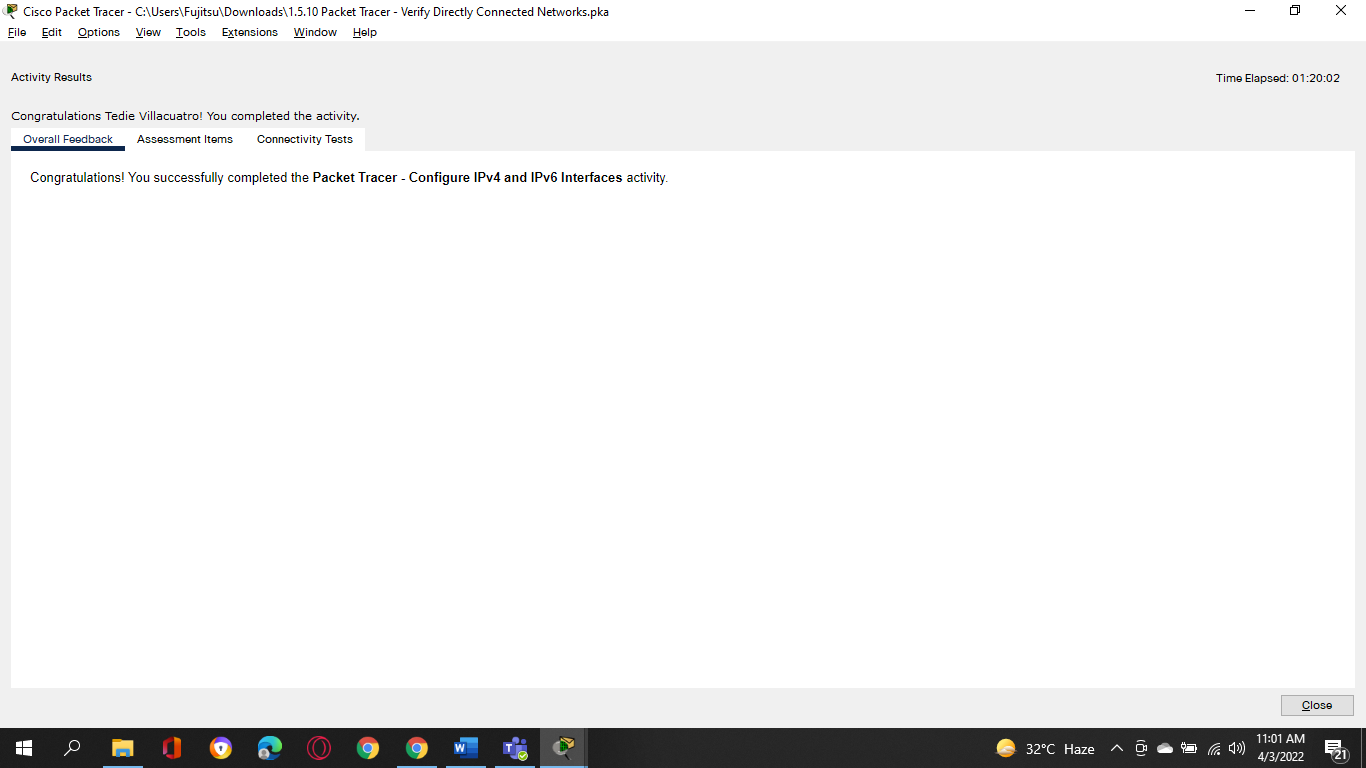
*Close configuration window*

**Both Gigabit Ethernet 0/0/0 and Gigabit Ethernet 0/0/1 have 2 addresses.**

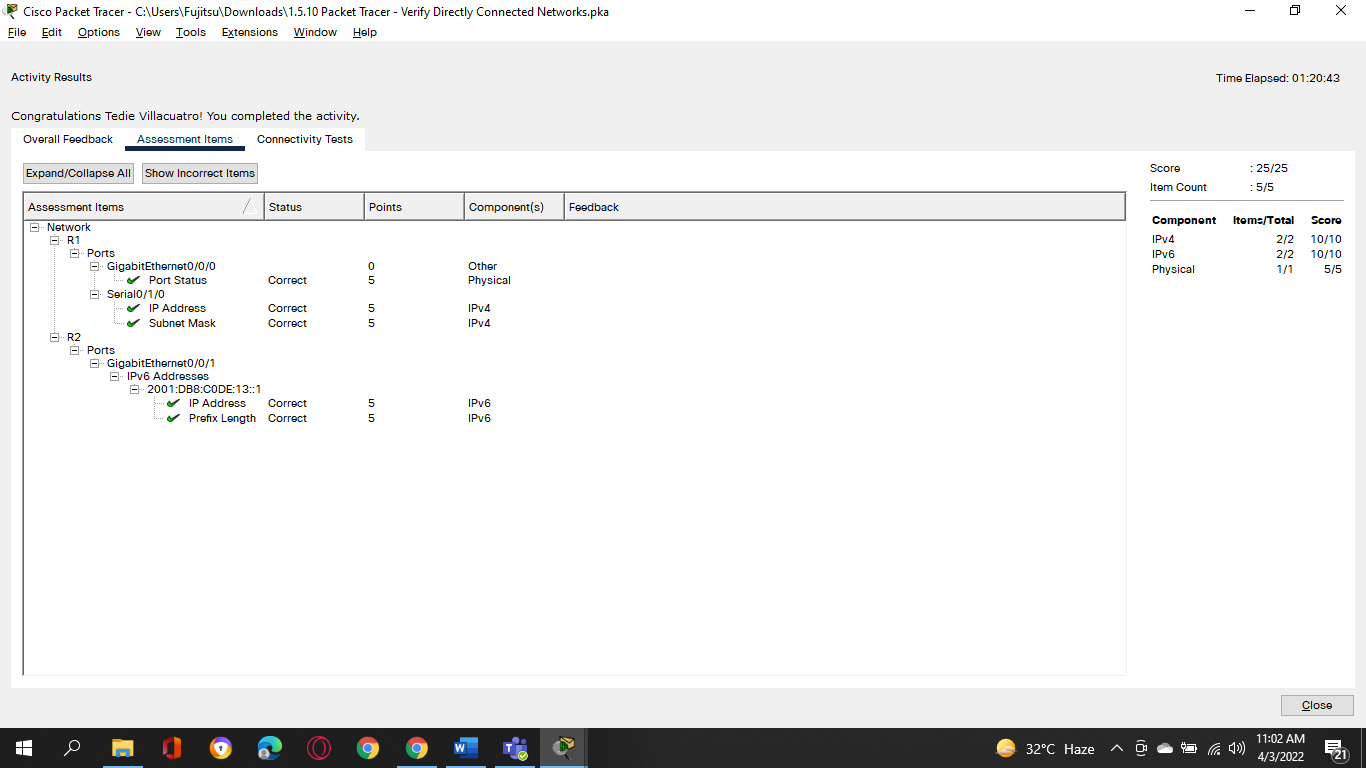
**Step 2: Verify connectivity.**

**PC3** and **PC4** should be able to ping each other and the **Dual Stack Server**. If not, verify the interface status and IPv6 address assignments.

**Activity completion:**



**Assessment Items:**



**Villacuatro, Tedie N. Computer Network System**

**BSCoE 3-3**

**Packet Tracer - Configure Router Interfaces**

**Addressing Table**

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address/Prefix** | **Default Gateway** |
| R1 | G0/0 | 172.16.20.1 /25 | N/A |
| *R1* | G0/1 | 172.16.20.129 /25 | N/A |
| *R1* | S0/0/0 | 209.165.200.225 /30 | N/A |
| PC1 | NIC | 172.16.20.10 /25 | 172.16.20.1 |
| PC2 | NIC | 172.16.20.138 /25 | 172.16.20.129 |
| R2 | G0/0 | 2001:db8:c0de:12::1/64 | N/A |
| *R2* | G0/1 | 2001:db8:c0de:13::1/64 | N/A |
| *R2* | S0/0/1 | 2001:db8:c0de:11::1/64 | N/A |
| *R2* | *S0/0/1* | fe80::2 | N/A |
| PC3 | NIC | 2001:db8:c0de:12::a/64 | fe80::2 |
| PC4 | NIC | 2001:db8:c0de:13::a/64 | fe80::2 |

**Objectives**

**Part 1: Configure IPv4 Addressing and Verify Connectivity**

**Part 2: Configure IPv6 Addressing and Verify Connectivity**

**Background**

Routers R1 and R2 each have two LANs. Your task is to configure the appropriate addressing on each device and verify connectivity between the LANs.

**Note**: The user EXEC password is **cisco**. The privileged EXEC password is **class**.

**Instructions**

**Part 1: Configure IPv4 Addressing and Verify Connectivity**

**Step 1: Assign IPv4 addresses to R1 and LAN devices.**

Referring to the **Addressing Table**, configure IP addressing for **R1** LAN interfaces, **PC1** and **PC2**. The serial interface has already configured.

**Step 2: Verify connectivity.**

**PC1** and **PC2** should be able to ping each other and the **Dual Stack Server**.

**Part 2: Configure IPv6 Addressing and Verify Connectivity**

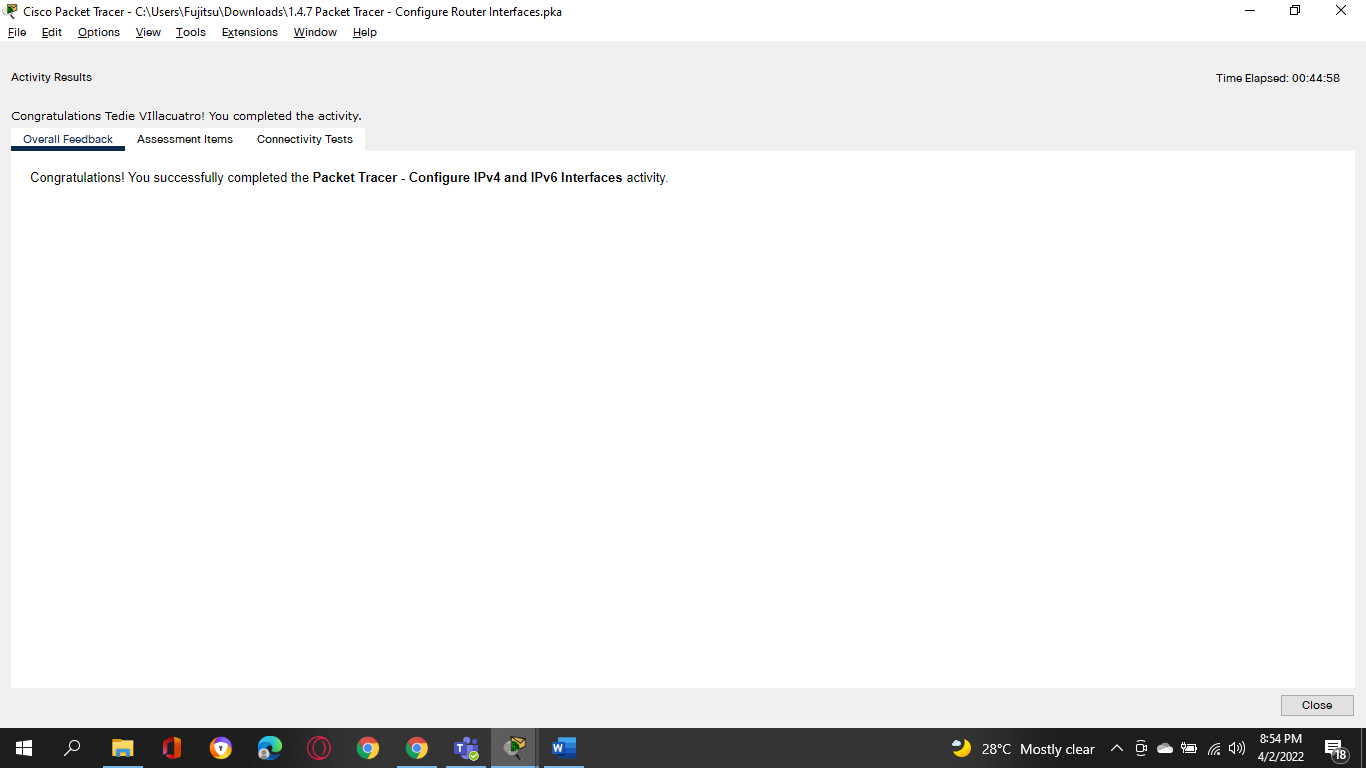
**Step 1: Assign IPv6 addresses to R2 and LAN devices.**

Referring to the **Addressing Table**, configure IP addressing for **R2 LAN interfaces**, **PC3** and **PC4**. The serial interface is already configured.

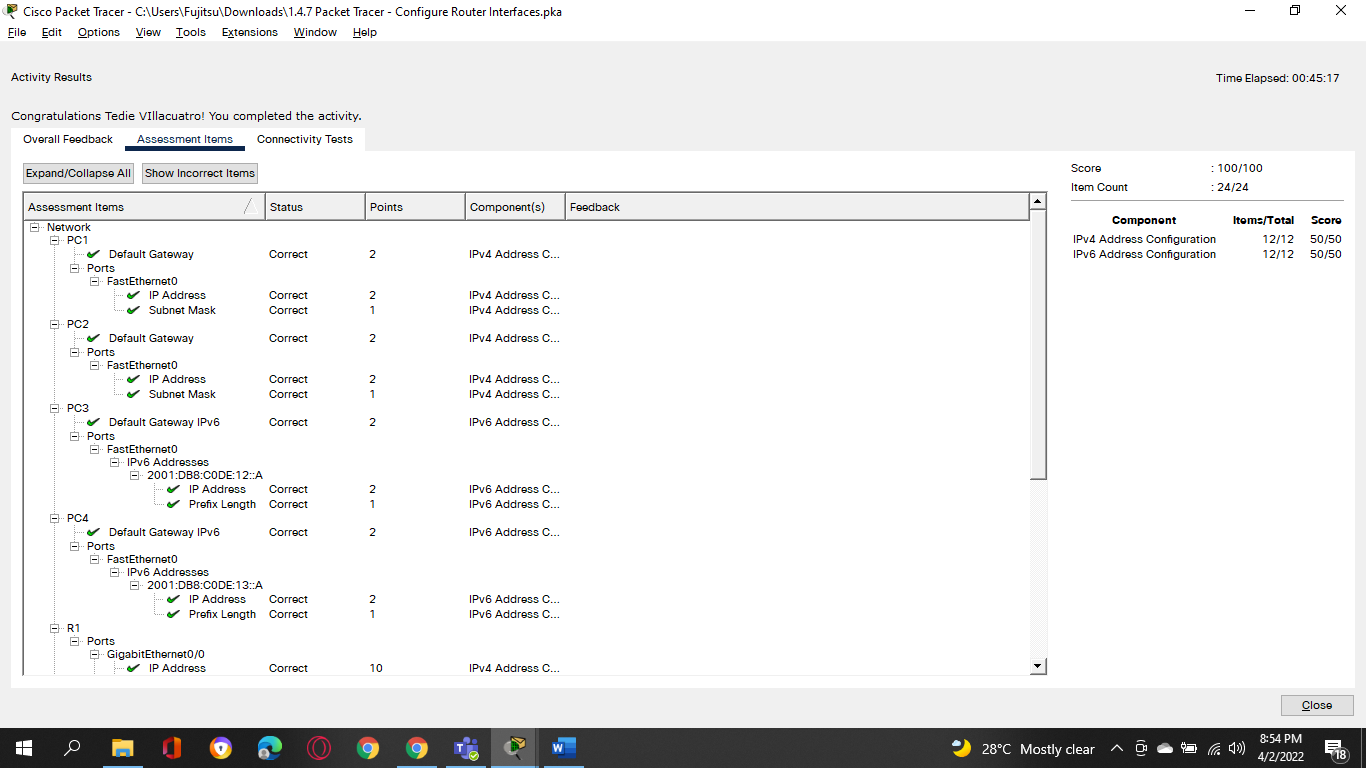
**Step 2: Verify connectivity.**

**PC3** and **PC4** should be able to ping each other and the **Dual Stack Server**.

**Activity Completion:**



**Assessment Items:**



**Tedie N. Villacuatro**

**BSCoE 3-3**

**Packet Tracer - Implement a Small Network**

**Addressing Table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **Address** | **Subnet Mask** | **Default Gateway** |
| RTA | G0/0 | 10.10.10.1 | 255.255.255.0 | N/A |
| *RTA* | G0/1 | 10.10.20.1 | 255.255.255.0 | N/A |
| SW1 | VLAN1 | 10.10.10.2 | 255.255.255.0 | *blank* |
| SW2 | VLAN1 | 10.10.20.2 | 255.255.255.0 | *blank* |
| PC-1 | NIC | *blank* | 255.255.255.0 | *blank* |
| PC-2 | NIC | *blank* | 255.255.255.0 | *blank* |

**Objectives**

**Part 1: Create the Network Topology**

**Part 2: Configure Devices and Verify Connectivity**

**Instructions**

**Part 1: Create the Network Topology**

**Step 1: Obtain the required devices.**

a.     Click the **Network Devices** icon in the bottom tool bar.

b.     Click the router icon in the submenu.

c.     Locate the **1941** router icon. Click and drag the icon for the 1941 router into the topology area.

d.     Click the switch entry in the submenu.

e.     Locate the **2960** switch icon. Click and drag the icon for the 2960 switch into the topology area.

f.      Repeat the step above so that there are **two** 2960 switches in the topology area.

g.     Click the **End Devices** icon.

h.     Locate the PC icon. Drag **two** PCs to the topology area.

i.      Arrange the devices into a layout that you can work with by clicking and dragging.

**Step 2: Name the devices.**

The devices have default names that you will need to change. You will name the devices as shown in the Addressing Table. You are changing the display names of the devices. This is the text label that appears below each device. Your display names must match the information in the Addressing Table **exactly**. If a display name does not match, you will not be scored for your device configuration.

a.     Click the device display name that is below the device icon. A text field should appear with a flashing insertion point. If the configuration window for the device appears, close it and try again, clicking a little further away from the device icon.

b.     Replace the current display name with the appropriate display name from the Addressing Table.

c.     Repeat until all devices are named.

**Step 3: Connect the devices.**

a.     Click the orange lightning bolt connections icon in the bottom toolbar.

b.     Locate the Copper Straight-Through cable icon. It looks like a solid black diagonal line.

c.     To connect the device, click the Copper Straight-Through cable icon and then click the first device that you want to connect. Select the correct port and then click the second device. Select the correct port and the devices will be connected.

d.     Connect the devices as specified in the table below.

|  |  |  |  |
| --- | --- | --- | --- |
| **From Device** | **Port** | **To Device** | **Port** |
| RTA | G0/0 | SW1 | G0/1 |
| *RTA* | G0/1 | SW2 | G0/1 |
| SW1 | F0/1 | PC-1 | Fastethernet0 |
| SW2 | F0/1 | PC-2 | Fastethernet0 |

**Part 2: Configure Devices**

Record the PC addressing and gateway addresses in the addressing table. You can use any available address in the network for PC-1 and PC-2.

**Step 1: Configure the router.**

*Open configuration window*

a.     Configure basic settings.

1)    Hostname as shown in the Addressing Table.

2)    Configure **Ciscoenpa55** as the encrypted password.

3)    Configure **Ciscolinepa55** as the password on the lines.

4)    All lines should accept connections.

5)    Configure an appropriate message of the day banner.

b.     Configure interface settings.

1)    Addressing.

2)    Descriptions on the interfaces.

3)    Save your configuration.

**Step 2: Configure switch SW1 and SW2.**

a.     Configure the default management interface so that it will accept connections over the network from local and remote hosts. Use the values in the addressing table.

b.     Configure an encrypted password using the value in step 1a above.

c.     Configure all lines to accept connections using the password from step 1a above.

d.     Configure the switches so that they can send data to hosts on remote networks.

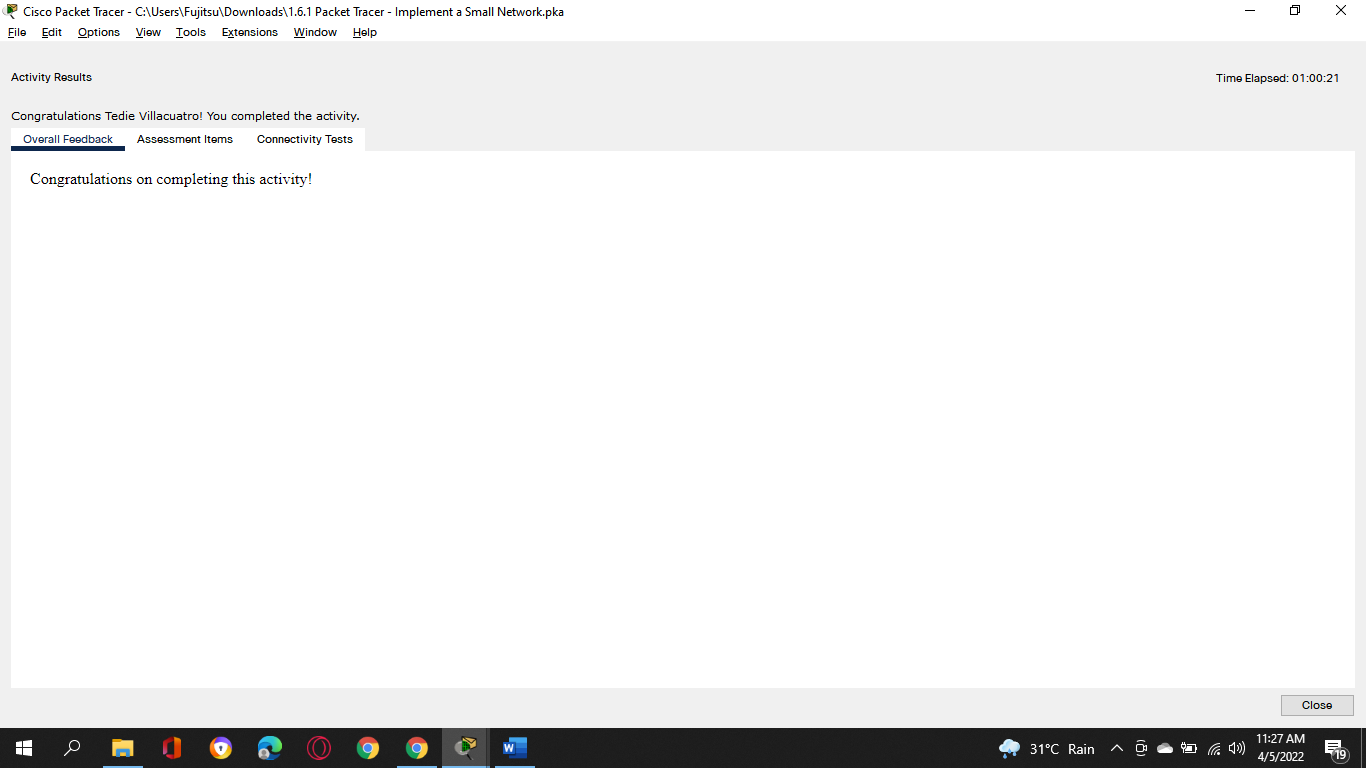
e.     Save your configuration.

*Close configuration window*

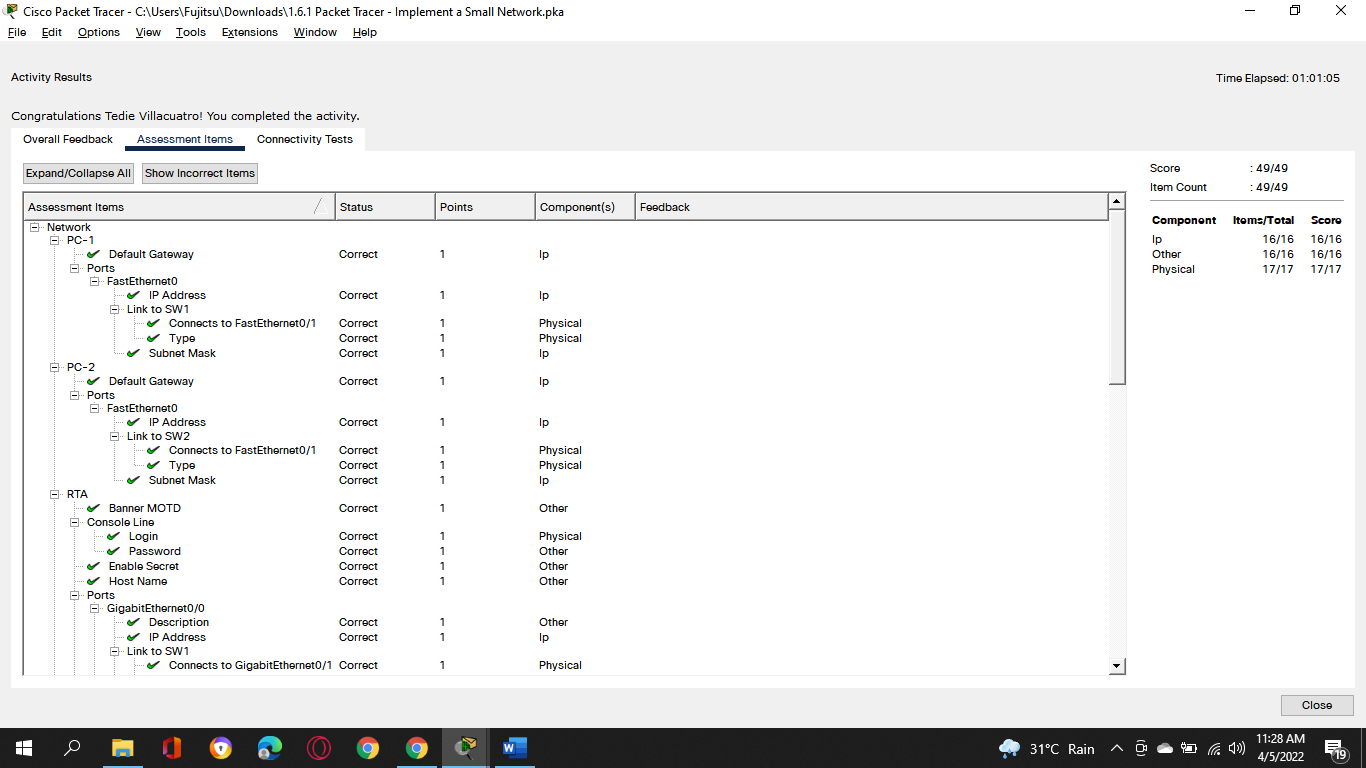
**Step 3: Configure the hosts.**

Configure addressing on the hosts. If your configurations are complete, you should be able to ping all devices in the topology.

**Activity Completion:**

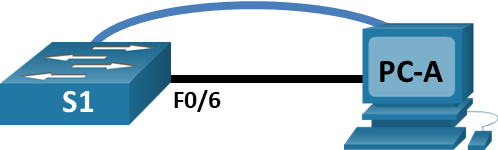


**Assessment Items:**



**Lab – Configure Basic Router**

**Topology**



**Addressing Table**

| **Device** | **Interface** | **IP Address / Prefix** |
| --- | --- | --- |
| S1 | VLAN 99 | 192.168.1.2/24 |
| *S1* | *VLAN 99* | 2001:db8:acad:1::2 /64 |
| *S1* | *VLAN 99* | fe80::2 |
| PC-A | NIC | 192.168.1.10 /24 |
| *PC-A* | *NIC* | 2001:db8:acad:1::10 /64 |

**Objectives**

**Part 1: Cable the Network and Verify the Default Switch Configuration**

**Part 2: Configure Basic Network Device Settings**

Configure basic switch settings.

Configure the PC IP address.

**Part 3: Verify and Test Network Connectivity**

Display device configuration.

Test end-to-end connectivity with ping.

Test remote management capabilities with Telnet.

**Part 4: Manage the MAC Address Table**

Record the MAC address of the host.

Determine the MAC addresses that the switch has learned.

List the **show mac address-table** command options.

Set up a static MAC address.

**Background / Scenario**

Cisco switches can be configured with a special IP address known as the switch virtual interface (SVI). The SVI, or management address, can be used for remote access to the switch to display or configure settings. If the VLAN 1 SVI is assigned an IP address, by default all ports in VLAN 1 have access to the SVI IP address.

In this lab, you will build a simple topology using Ethernet LAN cabling and access a Cisco switch using the console and remote access methods. You will examine default switch configurations before configuring basic switch settings. These basic switch settings include device name, interface description, local passwords, message of the day (MOTD) banner, IP addressing, and static MAC address. You will also demonstrate the use of a management IP address for remote switch management. The topology consists of one switch and one host using only Ethernet and console ports.

**Note**: The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.2(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

**Note**: Make sure that the switches have been erased and have no startup configurations. If you are unsure, contact your instructor. Refer to Appendix A for the procedures to initialize and reload a switch.

The **default bias** template used by the Switch Database Manager (SDM) does not provide IPv6 address capabilities. Verify that SDM is using either the **dual-ipv4-and-ipv6** template or the **lanbase-routing** template. The new template will be used after reboot even if the configuration is not saved.

*Open configuration window*

S1# **show sdm prefer**

Use the following commands to assign the **dual-ipv4-and-ipv6** template as the default SDM template.

S1# **configure terminal**

S1(config)# **sdm prefer dual-ipv4-and-ipv6 default**

S1(config)# **end**

S1# **reload**

*Close configuration window*

**Required Resources**

1 Switch (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)

1 PC (Windows with terminal emulation program, such as Tera Term)

1 Console cable to configure the Cisco IOS device via the console port

1 Ethernet cable as shown in the topology

**Cable the Network and Verify the Default Switch Configuration**

In Part 1, you will set up the network topology and verify default switch settings.

**Cable the network as shown in the topology.**

Connect the console cable as shown in the topology. Do not connect the PC-A Ethernet cable at this time.

**Note**: If you are using Netlab, shut down F0/6 on S1. This has the same effect as not connecting PC-A to S1.

Connect to the switch from PC-A using Tera Term or other terminal emulation program.

Question:

Why must you use a console connection to initially configure the switch? Why is it not possible to connect to the switch via Telnet or SSH?

**There are currently no IP addressing settings defined. When a Cisco 2960 switch is first put into operation, it has no networking setup.**

***Type your answers here.***

**Verify the default switch configuration.**

In this step, you will examine the default switch settings, such as current switch configuration, IOS information, interface properties, VLAN information, and flash memory.

You can access all the switch IOS commands in privileged EXEC mode. Access to privileged EXEC mode should be restricted by password protection to prevent unauthorized use because it provides direct access to global configuration mode and commands used to configure operating parameters. You will set passwords later in this lab.

The privileged EXEC mode command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes is gained. Use the **enable** command to enter privileged EXEC mode.

Assuming the switch had no configuration file stored in nonvolatile random-access memory (NVRAM), A console connection using Tera Term or other terminal emulation program will place you at the user EXEC mode prompt on the switch with a prompt of Switch>. Use the **enable** command to enter privileged EXEC mode.

*Open configuration window*

Notice that the prompt changed in the configuration to reflect privileged EXEC mode.

Verify that there is a clean default configuration file on the switch by issuing the **show running-config** privileged EXEC mode command. If a configuration file was previously saved, it must be removed. Depending on the switch model and IOS version, your configuration may look slightly different. However, there should be no configured passwords or IP address. If your switch does not have a default configuration, erase and reload the switch.

**Note**: Appendix A details the steps to initialize and reload a switch.

Examine the current running configuration file.

Questions:

How many FastEthernet interfaces does a 2960 switch have?

**There are 24 FastEthernet interfaces on a 2960 switch**

***your answers here.***

How many Gigabit Ethernet interfaces does a 2960 switch have?

**There are 2 GigabitEthernet interfaces on a 2960 switch**

***Type your answers here.***

What is the range of values shown for the vty lines?

**0-4 and 5-15 or 0-15**

***Type your answers here.***

Examine the startup configuration file in NVRAM.

Question:

Why does this message appear? **There are no configurations saved to NVRAM**

***Type your answers here.***

Examine the characteristics of the SVI for VLAN 1.

Questions:

Is there an IP address assigned to VLAN 1? **No**

***Type your answers here.***

What is the MAC address of this SVI? Answers will vary. **0002:1726:0671**

***Type***

***your answers here.***

Is this interface up?

**The no shutdown command is enabled by default on Cisco switches for VLAN 1, however VLAN 1 will not reach the up/up state until a port is allocated to it and this port is also up. If no ports in VLAN 1 are in the up state, the VLAN 1 interface will be up, but the line protocol will be down. By default, all ports are assigned to VLAN 1 at the start.**

.

Examine the IP properties of the SVI VLAN 1.

Question:

What output do you see?

**Vlan1 is up, line protocol is down**

**Internet protocol processing disabled**

***Type your answers here.***

Connect an Ethernet cable from PC-A to port 6 on the switch and examine the IP properties of the SVI VLAN 1. Allow time for the switch and PC to negotiate duplex and speed parameters.

**Note**: If you are using Netlab, enable interface F0/6 on S1.

Question:

What output do you see?

**Vlan1 is up, line protocol is up**

**Internet protocol processing disabled**

***answers here.***

Examine the Cisco IOS version information of the switch.

Questions:

What is the Cisco IOS version that the switch is running? **Version 15.0(2) SE4**

***Type your answers here.***

What is the system image filename? **c2960-lanbasek9-mz.150-2.SE4.bin**

***Type your answers here.***

What is the base MAC address of this switch? **00:17:59:A7:51:80**

***Type your answers here.***

Examine the default properties of the FastEthernet interface used by PC-A.

Switch# **show interface f0/6**

Question:

Is the interface up or down?  **It should be up unless there is a cabling problem**

***Type your answers here.***

What event would make an interface go up? **Connecting a host or other device**

***Type your answers here.***

What is the MAC address of the interface? **0030.a38a.8906**

***Type your answers here.***

What is the speed and duplex setting of the interface? **Full-duplex, 100Mb/s**

***Type your answers here.***

Examine the default VLAN settings of the switch.

Question:

What is the default name of VLAN 1? **default**

***Type your answers here.***

Which ports are in VLAN 1? **all ports; F0/1 – F0/24; G0/1, G0/2**

***Type your answers here.***

Is VLAN 1 active? **Yes**

***Type your answers here.***

What type of VLAN is the default VLAN? **Vlan type is enet**

***Type your answers here.***

Examine flash memory.

Issue one of the following commands to examine the contents of the flash directory.

Switch# **show flash:**

Switch# **dir flash:**

Files have a file extension, such as .bin, at the end of the filename. Directories do not have a file extension.

Question:

What is the filename of the Cisco IOS image? **2960-lanbasek9-mz.150-2.SE4.bin**

***Type your answers here.***

**Configure Basic Network Device Settings**

In Part 2, you will configure basic settings for the switch and PC.

**Configure basic switch settings.**

Copy the following basic configuration and paste it into S1 while in global configuration mode.

no ip domain-lookup

hostname S1

service password-encryption

enable secret class

banner motd #

Unauthorized access is strictly prohibited. #

Set the SVI IP address of the switch. This allows remote management of the switch.

Before you can manage S1 remotely from PC-A, you must assign the switch an IP address. The default configuration on the switch is to have the management of the switch controlled through VLAN 1. However, a best practice for basic switch configuration is to change the management VLAN to a VLAN other than VLAN 1.

For management purposes, use VLAN 99. The selection of VLAN 99 is arbitrary and in no way implies that you should always use VLAN 99.

First, create the new VLAN 99 on the switch. Then set the IP address of the switch to 192.168.1.2 with a subnet mask of 255.255.255.0 on the internal virtual interface VLAN 99. IPv6 address can also be configured on the SVI interface. Use the IPv6 addresses listed in the Addressing Table.

Notice that the VLAN 99 interface is in the down state even though you entered the **no shutdown** command. The interface is currently down because no switch ports are assigned to VLAN 99.

Assign all user ports to VLAN 99.

To establish connectivity between the host and the switch, the ports used by the host must be in the same VLAN as the switch. Notice in the above output that the VLAN 1 interface goes down because none of the ports are assigned to VLAN 1. After a few seconds, VLAN 99 comes up because at least one active port (F0/6 with PC-A attached) is now assigned to VLAN 99.

Issue the **show vlan brief** command to verify that all ports are in VLAN 99.

Configure the default gateway for S1. If no default gateway is set, the switch cannot be managed from a remote network that is more than one router away. Although this activity does not include an external IP gateway, assume that you will eventually connect the LAN to a router for external access. Assuming that the LAN interface on the router is 192.168.1.1, set the default gateway for the switch.

Console port access should also be restricted with a password. Use **cisco** as the console login password in this activity. The default configuration is to allow all console connections with no password needed. To prevent console messages from interrupting commands, use the **logging synchronous** option.

S1(config)# **line con 0**

S1(config-line)# **logging synchronous**

Configure the virtual terminal (vty) lines 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.

Question:

Why is the **login** command required?

**The switch will not request for a password until you use the login command.**

***Type your answers here.***

*Close configuration window*

**Configure an IP address on PC-A.**

Assign the IP address and subnet mask to the PC as shown in the Addressing Table. An abbreviated version of the procedure is described here. A default gateway is not required for this topology; however, you can enter **192.168.1.1** and **fe80::1** to simulate a router attached to S1.

1. Navigate to the **Control Panel**.
2. In the Category view, select **View network status and tasks**.
3. Click **Change adapter settings** on the left panel.
4. Right-click an **Ethernet** interface, and choose **Properties**.
5. Choose **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
6. Click the **Use the following IP address** radio button and enter the IP address and subnet mask and click **OK**.
7. Select **Internet Protocol Version 6 (TCP/IPv6)** and click **Properties**.
8. Click the **Use the following IPv6 address** radio button and enter the IPv6 address and prefix and click **OK** to continue
9. Click **OK** to exit the Properties window.

**Verify and Test Network Connectivity**

In Part 3, you will verify and document the switch configuration, test end-to-end connectivity between PC-A and S1, and test the switch’s remote management capability.

**Display the switch configuration.**

Use the console connection on PC-A to display and verify the switch configuration. The **show run** command displays the entire running configuration, one page at a time. Use the spacebar to advance paging.

A sample configuration is shown here. The settings you configured are highlighted in yellow. The other configuration settings are IOS defaults.

*Open configuration window*

S1# **show run**

Building configuration...

Current configuration : 2206 bytes

!

version 15.2

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname S1

!

boot-start-marker

boot-end-marker

!

enable secret 5 $1$mtvC$6NC.1VKr3p6bj7YGE.jNg0

!

no aaa new-model

system mtu routing 1500

!

!

no ip domain-lookup

!

<output omitted>

!

interface FastEthernet0/24

switchport access vlan 99

!

interface GigabitEthernet0/1

switchport access vlan 99

!

interface GigabitEthernet0/2

switchport access vlan 99

!

interface Vlan1

no ip address

no ip route-cache

!

interface Vlan99

ip address 192.168.1.2 255.255.255.0

ipv6 address FE80::2 link-local

ipv6 address 2001:DB8:ACAD:1::2/64

!

ip default-gateway 192.168.1.1

ip http server

ip http secure-server

!

banner motd ^C

Unauthorized access is strictly prohibited. ^C

!

line con 0

password 7 00071A150754

logging synchronous

login

line vty 0 4

password 7 121A0C041104

login

line vty 5 15

password 7 121A0C041104

login

!

end

Verify the management VLAN 99 settings.

S1# **show interface vlan 99**

Questions:

What is the bandwidth on this interface? **BW** **100000 Kbit**

***Type your answers here.***

What is the VLAN 99 state? **VLAN 99 is up**

***Type your answers here.***

What is the line protocol state? **Line protocol is up**

***Type your answers here.***

*Close configuration window*

**Test end-to-end connectivity with ping.**

From the command prompt on PC-A, ping the address of PC-A first.

C:\> **ping 192.168.1.10**

C:\> **ping 2001:db8:acad:1::10**

From the command prompt on PC-A, ping the SVI management address of S1.

C:\> **ping 192.168.1.2**

C:\> **ping 2001:db8:acad:1::2**

Because PC-A needs to resolve the MAC address of S1 through ARP, the first packet may time out. If ping results continue to be unsuccessful, troubleshoot the basic device configurations. Check both the physical cabling and logical addressing.

**Test and verify remote management of S1.**

You will now use Telnet to remotely access the switch. 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. In this step, you will use Telnet to remotely access switch S1 using its SVI management address. Telnet is not a secure protocol; however, you will use it to test remote access. With Telnet, all information, including passwords and commands, are sent across the session in plain text. In subsequent labs, you will use SSH to remotely access network devices.

Open Tera Term or other terminal emulation program with Telnet capability.

Select the Telnet server and provide the SVI management address to connect to S1. The password is **cisco**.

After entering the password **cisco**, you will be at the user EXEC mode prompt. Access privileged EXEC mode using the **enable** command and providing the secret password **class**.

Save the configuration.

Type **exit** to end the Telnet session.

**Manage the MAC Address Table**

In Part 4, you will determine the MAC addresses that the switch has learned, set up a static MAC address on one interface of the switch, and then remove the static MAC address from that interface.

**Record the MAC address of the host.**

Open a command prompt on PC-A and issue the **ipconfig /all** command to determine and record the Layer 2 (physical) addresses of the NIC.

***Type your answers here.***

**Determine the MAC addresses that the switch has learned.**

*Open configuration window*

Display the MAC addresses using the **show mac address-table** command.

S1# **show mac address-table**

Questions:

How many dynamic addresses are there?

***Type your answers here.***

How many MAC addresses are there in total? **1**

***Type your answers here.***

Does the dynamic MAC address match the MAC address of PC-A? **Yes**

***Type your answers here.***

**List the show mac address-table options.**

Display the MAC address table options.

S1# **show mac address-table ?**

Question:

How many options are available for the **show mac address-table** command? **3**

***Type your answers here.***

Issue the **show mac address-table dynamic** command to display only the MAC addresses that were learned dynamically.

S1# **show mac address-table dynamic**

Question:

How many dynamic addresses are there? **1**

***Type your answers here.***

View the MAC address entry for PC-A. The MAC address formatting for the command is xxxx.xxxx.xxxx.

S1# **show mac address-table address <PC-A MAC here>**

**Set up a static MAC address.**

Clear the MAC address table.

To remove the existing MAC addresses, use the **clear mac address-table dynamic** command in privileged EXEC mode.

S1# **clear mac address-table dynamic**

Verify that the MAC address table was cleared.

S1# **show mac address-table**

Question:

How many static MAC addresses are there? **None**

***Type your answers here.***

How many dynamic addresses are there? **None**

***Type your answers here.***

Examine the MAC table again.

More than likely, an application running on your PC has already sent a frame out the NIC to S1. Look at the MAC address table again in privileged EXEC mode to see if S1 has relearned the MAC address of PC-A.

S1# **show mac address-table**

Questions:

How many dynamic addresses are there? 1

***Type your answers here.***

Why did this change from the last display?

**Because we ping the IP address of the switch so it stored the PC-A MAC address.**

***Type your answers here.***

If S1 has not yet relearned the MAC address for PC-A, ping the VLAN 99 IP address of the switch from PC-A, and then repeat the **show mac address-table** command.

To specify which ports a host can connect to, one option is to create a static mapping of the host MAC address to a port.

Set up a static MAC address on F0/6 using the address that was recorded for PC-A in Part 4, Step 1. The MAC address 0050.56BE.6C89 is used as an example only. You must use the MAC address of PC-A, which is different than the one given here as an example.

S1(config)# **mac address-table static 0050.56BE.6C89 vlan 99 interface fastethernet 0/6**

Verify the MAC address table entries.

S1# **show mac address-table**

Questions:

How many total MAC addresses are there? 1

***Type your answers here.***

How many static addresses are there? 1

***Type your answers here.***

Remove the static MAC entry. Enter global configuration mode and remove the command by putting a **no** in front of the command string.

**Note**: The MAC address 0050.56BE.6C89 is used in the example only. Use the MAC address for PC-A.

S1(config)# **no mac address-table static 0050.56BE.6C89 vlan 99 interface fastethernet 0/6**

Verify that the static MAC address has been cleared.

S1# **show mac address-table**

Question:

How many total static MAC addresses are there? **None**

***Type your answers here.***

*Close configuration window*

**Reflection Questions**

Why should you configure the vty password for the switch?

**You will be unable to telnet to the switch if you do not configure a vty password.**

***Type your answers here.***

Why change the default VLAN 1 to a different VLAN number?

**For improved security**

***our answers here.***

How can you prevent passwords from being sent in plain text?

**Using the service password-encryption command.**

***Type your answers here.***

Why configure a static MAC address on a port interface?

**To specify which ports a host can connect to**

***Type your answers here.***

**Appendix A: Initialize and Reload a Switch**

* + - 1. Console into the switch and enter privileged EXEC mode.

*Open configuration window*

Switch> **enable**

Switch#

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)

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

Switch# **delete vlan.dat**

Delete filename [vlan.dat]?

You are prompted to verify the filename. If you have entered the name correctly, press Enter; otherwise, you can change the filename.

You are prompted to confirm deletion of this file. Press Enter to confirm.

Delete flash:/vlan.dat? [confirm]

Switch#

Use the **erase startup-config** command to erase the startup configuration file from NVRAM. You are prompted to remove the configuration file. Press Enter to confirm.

Switch# **erase startup-config**

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

Switch#

Reload the switch to remove any old configuration information from memory. You will then receive a prompt to confirm reloading of the switch. Press Enter to proceed.

Switch# **reload**

Proceed with reload? [confirm]

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

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

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

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

Switch>

**Lab – Configure Basic RouterSettings**

**Topology**



**Addressing Table**

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address / Prefix** | **Default Gateway** |
| R1 | G0/0/0 | 192.168.0.1 /24 | N/A |
| *R1* | *G0/0/0* | 2001:db8:acad::1 /64 | *N/A* |
| *R1* | *G0/0/0* | fe80::1 | *N/A* |
| *R1* | G0/0/1 | 192.168.1.1 /24 | *N/A* |
| *R1* | *G0/0/1* | 2001:db8:acad:1::1 /64 | *N/A* |
| *R1* | *G0/0/1* | fe80::1 | *N/A* |
| *R1* | Loopback0 | 10.0.0.1 /24 | *N/A* |
| *R1* | *Loopback0* | 2001:db8:acad:2::1 /64 | *N/A* |
| *R1* | *Loopback0* | fe80::1 | *N/A* |
| PC-A | NIC | 192.168.1.10 /24 | 192.168.1.1 |
| *PC-A* | *NIC* | 2001:db8:acad:1::10 /64 | fe80::1 |
| PC-B | NIC | 192.168.0.10 /24 | 192.168.0.1 |
| *PC-B* | *NIC* | 2001:db8:acad::10 /64 | fe80::1 |

**Objectives**

**Part 1: Set Up the Topology and Initialize Devices**

Cable equipment to match the network topology.

Initialize and restart the router and switch.

**Part 2: Configure Devices and Verify Connectivity**

Assign static IPv4 and IPv6 information to the PC interfaces.

Configure basic router settings.

Configure the router for SSH.

Verify network connectivity.

**Part 3: Display Router Information**

Retrieve hardware and software information from the router.

Interpret the output from the startup configuration.

Interpret the output from the routing table.

Verify the status of the interfaces.

**Background / Scenario**

This is a comprehensive lab to review previously covered IOS router commands. In Parts 1 and 2, you will cable the equipment and complete basic configurations and interface settings on the router.

In Part 3, you will use SSH to connect to the router remotely and utilize the IOS commands to retrieve information from the device to answer questions about the router.

For review purposes, this lab provides the commands necessary for specific router configurations.

**Note**: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.2(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

**Note**: Make sure that the router and switch have been erased and have no startup configurations. Consult with your instructor for the procedure to initialize and reload a router and switch.

**Required Resources**

1 Router (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)

1 Switch (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)

2 PCs (Windows with a 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

**Note**: The Gigabit Ethernet interfaces on Cisco 4221 routers are autosensing and an Ethernet straight-through cable may be used between the router and PC-B. If using another model Cisco router, it may be necessary to use an Ethernet crossover cable.

**Instructions**

* 1. **Set Up the Topology and Initialize Devices**
     1. **Cable the network as shown in the topology.**

Attach the devices as shown in the topology diagram, and cable as necessary.

Power on all the devices in the topology.

* + 1. **Initialize and reload the router and switch.**
  1. **Configure Devices and Verify Connectivity**
     1. **Configure the PC interfaces.**

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

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

* + 1. **Configure the router.**

*Open configuration window*

Console into the router and enable privileged EXEC mode.

Enter configuration mode.

Assign a device name to the router.

Set the router’s domain name as ccna-lab.com.

Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

Encrypt the plaintext passwords.

Configure the system to require a minimum 12-character password.

Configure the username **SSHadmin** with an encrypted password of **55Hadm!n2020**.

Generate a set of crypto keys with a 1024 bit modulus

Assign the privileged EXEC password to **$cisco!PRIV\***

Assign **$cisco!!CON\*** as the console password, configure sessions to disconnect after four minutes of inactivity, and enable login.

Assign **$cisco!!VTY\*** as the vty password, configure the vty lines to accept SSH connections only, configure sessions to disconnect after four minutes of inactivity, and enable login using the local database.

Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

Enable IPv6 Routing

Configure all three interfaces on the router with the IPv4 and IPv6 addressing information from the addressing table above. Configure all three interfaces with descriptions. Activate all three interfaces.

The router should not allow vty logins for two minutes if three failed login attempts occur within 60 seconds.

Set the clock on the router.

Save the running configuration to the startup configuration file.

Question:

What would be the result of reloading the router prior to completing the **copy running-config startup-config** command?

* **This command lets you save your running configuration to the router’s startup configuration (NVRAM) so it will survive a reload.**

1. ***Type your answers here.***

*Close configuration window*

* + 1. **Verify network connectivity.**

Using the command line at PC-A, ping the IPv4 and IPv6 addresses for PC-B.

**Note**: It may be necessary to disable the PCs firewall.

Question:

Were the pings successful?

* **Yes! Although on first ping there is one packet loss, subsequent pings were sucessfull**

1. ***Type your answers here.***

Remotely access R1 from PC-A using the Tera Term SSH client.

Using Tera Term on PC-A, open an SSH session to the R1 Loopback interface IPv4 address. Ensure that the **SSH** radio button is selected and then click **OK** to connect to the router. Log in as **SSHadmin** with the password **55Hadm!n2020**.

Question:

Was remote access successful? **Yes**

1. ***Type your answers here.***

Using Tera Term on PC-A, open an SSH session to the R1 Loopback interface IPv6 address. Ensure that the **SSH** radio button is selected and then click **OK** to connect to the router. Log in as **SSHadmin** with the password **55Hadm!n2020**. **Note**: The IPv6 address should be surrounded with square brackets, i.e. [*IPv6 address*]

Questions:

Was remote access successful? **Yes**

1. ***Type your answers here.***

Why is the Telnet protocol considered to be a security risk?

* **A Telnet session can be seen in clear text. It is not encrypted.**

1. ***Type your answers here.***
   1. **Display Router Information**

In Part 3, you will use **show** commands from an SSH session to retrieve information from the router.

* + 1. **Establish an SSH session to R1.**

Using Tera Term on PC-B, open an SSH session to the R1 Loopback interface IPv6 address and log in as **SSHadmin** with the password **55Hadm!n2020**.

* + 1. **Retrieve important hardware and software information.**

Use the **show version** command to answer questions about the router.

Questions:

What is the name of the IOS image that the router is running?

1. **X86\_64\_LINUX\_IOSD-UNIVERSALK9-M*Type your answers here.***

How much non-volatile random-access memory (NVRAM) does the router have?

* **32768K bytes of non-volatile configuration memory.**

1. ***Type your answers here.***

How much Flash memory does the router have?

* **3223551K bytes of flash memory at bootflash**

1. ***Type your answers here.***

The **show** commands often provide multiple screens of outputs. Filtering the output allows a user to display certain sections of the output. To enable the filtering command, enter a pipe (**|**) character after a **show** command, followed by a filtering parameter and a filtering expression. You can match the output to the filtering statement by using the **include** keyword to display all lines from the output that contain the filtering expression. Filter the **show version** command, using **show version | include register** to answer the following question.

What is the boot process for the router on the next reload? **Configuration Register is 0x2102**

1. ***Type your answers here.***
   * 1. **Display the startup configuration.**

Use the **show startup-config** command on the router to answer the following questions.

How are passwords presented in the output?

* **Passwords are encrypted due to the service password-encryption command.**
  + **The line console and line vty password of $cisco!!CON\* is encrypted as 08654F471A1A0A565328232A60.**
  + **The SSHadmin password of 55Hadm!n2020 is encrypted as $1$mERr$fuFUxOtVJZMfnQOcoB7vt/.**

1. ***Type your answers here.***

Use the **show startup-config | section vty** command.

What is the result of using this command?

* **Shows the entire section that starts with the filtering expression*Type your answers here.***
  + 1. **Display the routing table on the router.**

Use the **show ip route** command on the router to answer the following questions.

Questions:

What code is used in the routing table to indicate a directly connected network?

* **The C designates a directly connected subnet. An L designates a local interface. Both answers are correct.**

1. ***Type your answers here.***

How many route entries are coded with a C code in the routing table? **3**

1. ***Type your answers here.***
   * 1. **Display a summary list of the interfaces on the router.**

Use the **show ip interface brief** command on the router to answer the following question.

Question:

What command changed the status of the Gigabit Ethernet ports from administratively down to up?

* **No shutdown** command
* ***Type your answers here.***
  + 1. Use the **show ipv6 int brief** command to verify IPv6 settings on R1.

Question:

What is the meaning of the [up/up] part of the output?

* **The [up/up] status reflects the Layer 1 and Layer 2 status of the interface and does not rely on Layer 3 for status.**

***Ty***

* + 1. On PC-B, change its configuration so that it no longer has a static IPv6 address. You may have to reboot the machine. Then, issue the **ipconfig** command on PC-B to examine the IPv6 configuration.

Questions:

What is the IPv6 address assigned to PC-B?

* **2001:DB8:ACAD:0:260:47FF:FE7B:329**

1. ***Type your answers here.***

What is the default gateway assigned to PC-B? **Yes**

1. ***Type your answers here.***

Issue a ping from PC-B to the R1 default gateway link local address. Was it successful? **Yes**

1. ***Type your answers here.***

Issue a ping from PC-B to the R1 IPv6 unicast address 2001:db8:acad::1. Was it successful? **Yes**

1. ***Type your answers here.***

**Reflection Questions**

In researching a network connectivity issue, a technician suspects that an interface was not enabled. What **show** command could the technician use to troubleshoot this issue?

**The show commands show ip interface brief or show startup-config would provide the information**

***Type your answers here.***

In researching a network connectivity issue, a technician suspects that an interface was assigned an incorrect subnet mask. What **show** command could the technician use to troubleshoot this issue?

**show startup-config or show running-config**

**Router Interface Summary Table**

| **Router Model** | **Ethernet Interface #1** | **Ethernet Interface #2** | **Serial Interface #1** | **Serial Interface #2** |
| --- | --- | --- | --- | --- |
| 1800 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 4221 | Gigabit Ethernet 0/0/0 (G0/0/0) | Gigabit Ethernet 0/0/1 (G0/0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 4300 | Gigabit Ethernet 0/0/0 (G0/0/0) | Gigabit Ethernet 0/0/1 (G0/0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |

**Note**: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.