Cloud and Network Security-C1-2026

Student Name: **Felix Webbo**

Student No: **CS-CNS11-26044**

SUNDAY, JANUARY 27, 2026

Week 2: Assignment 1

Class Exercise: **Build a Switch and Router Network**

1 ABSTRACT

This laboratory exercise was conducted to design, configure, and verify a small routed network using Cisco IOS devices. The lab involved configuring a router, a switch, and two end devices with both IPv4 and IPv6 addressing. Emphasis was placed on correct device configuration, secure access control, and end-to-end connectivity verification. The exercise also examined potential security risks associated with improper switch and router configurations. The lab provided practical experience in applying secure networking principles and reinforced the importance of accurate and secure device configuration in modern network environments.

Table of Contents

2 INTRODUCTION

This laboratory exercise was conducted as part of the Cisco Networking Academy curriculum to reinforce fundamental networking concepts using Cisco IOS devices. The primary focus was on building and managing a basic routed network topology consisting of a router, a switch, and two personal computers. The lab aimed to strengthen understanding of IPv4 and IPv6 addressing, device configuration, and routing behavior. Additionally, the exercise highlighted the security implications of proper and improper switch and router configuration within enterprise networks.

3 OBJECTIVES

The objectives of this laboratory exercise were to:

- Design and implement a basic routed network topology.
- Configure IPv4 and IPv6 addressing on network devices.
- Apply basic security controls to Cisco IOS devices.
- Verify end-to-end network connectivity.
- Analyze routing and interface information using IOS commands.
- Identify security concerns arising from device misconfiguration.

4 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

5 NETWORK TOPOLOGY AND ADDRESSING

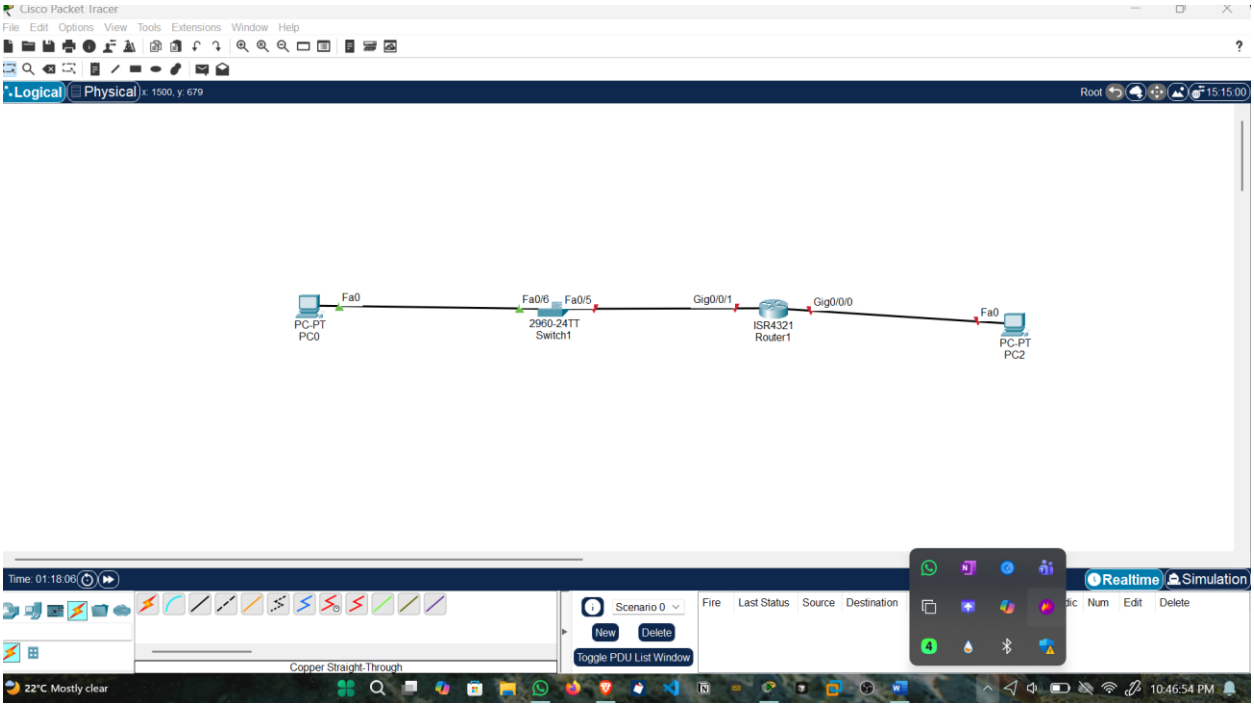
The implemented network topology consisted of one Cisco 4221 router (R1), one Cisco Catalyst 2960 switch (S1), and two personal computers (PC-A and PC-B). PC-A was connected to the switch, while PC-B was connected directly to the router. Two IPv4 subnets and corresponding IPv6 prefixes were assigned to enable communication between different network segments. The router interfaces functioned as default gateways, while the switch VLAN interface was configured for management purposes.

6 METHODOLOGY

6.1 Part 1: Set Up Topology and Initialize Devices

6.1.1 Step 1: Cable the network as shown in the topology.

1. Attach the devices shown in the topology diagram, and cable, as necessary.
2. Power on all the devices in the topology.



6.1.2 Step 2: Initialize and reload the router and switch

If configuration files were previously saved on the router and switch, initialize and reload these devices back to their default configurations.

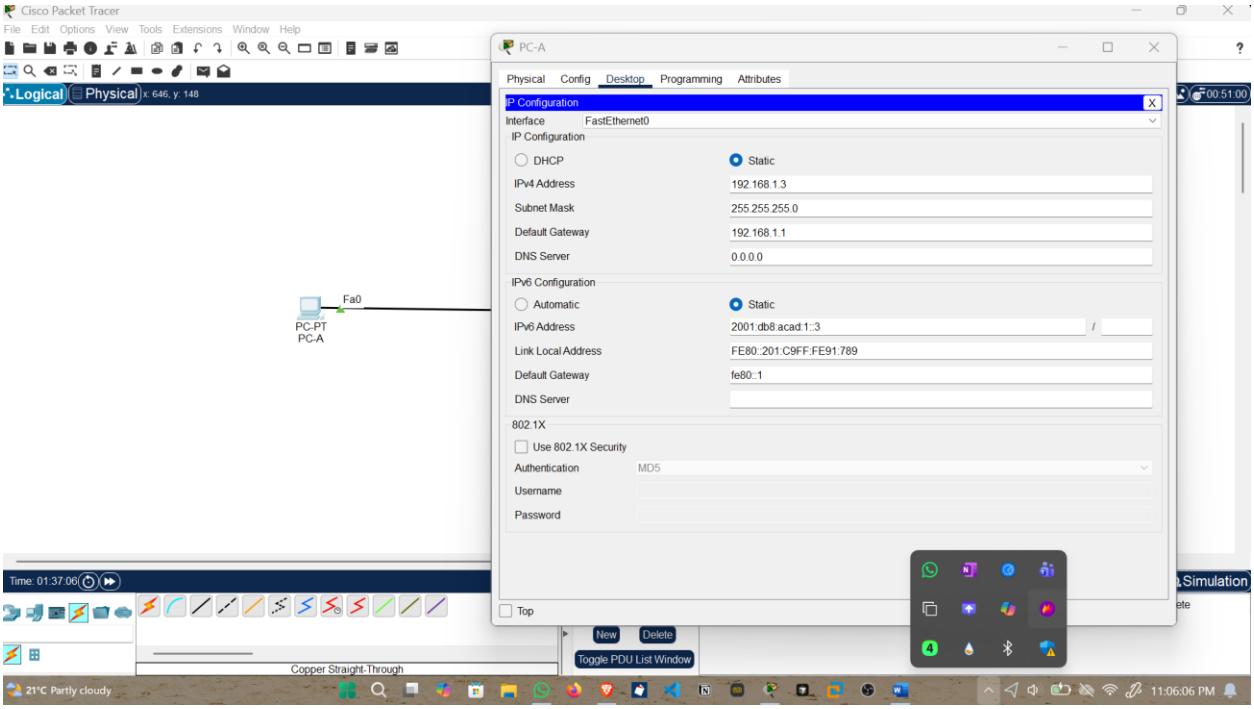
All network devices were cabled and powered on according to the topology diagram. Any existing configurations were erased to eliminate configuration conflicts and reduce security risks. The switch SDM template was verified and configured to support both IPv4 and IPv6 operations.

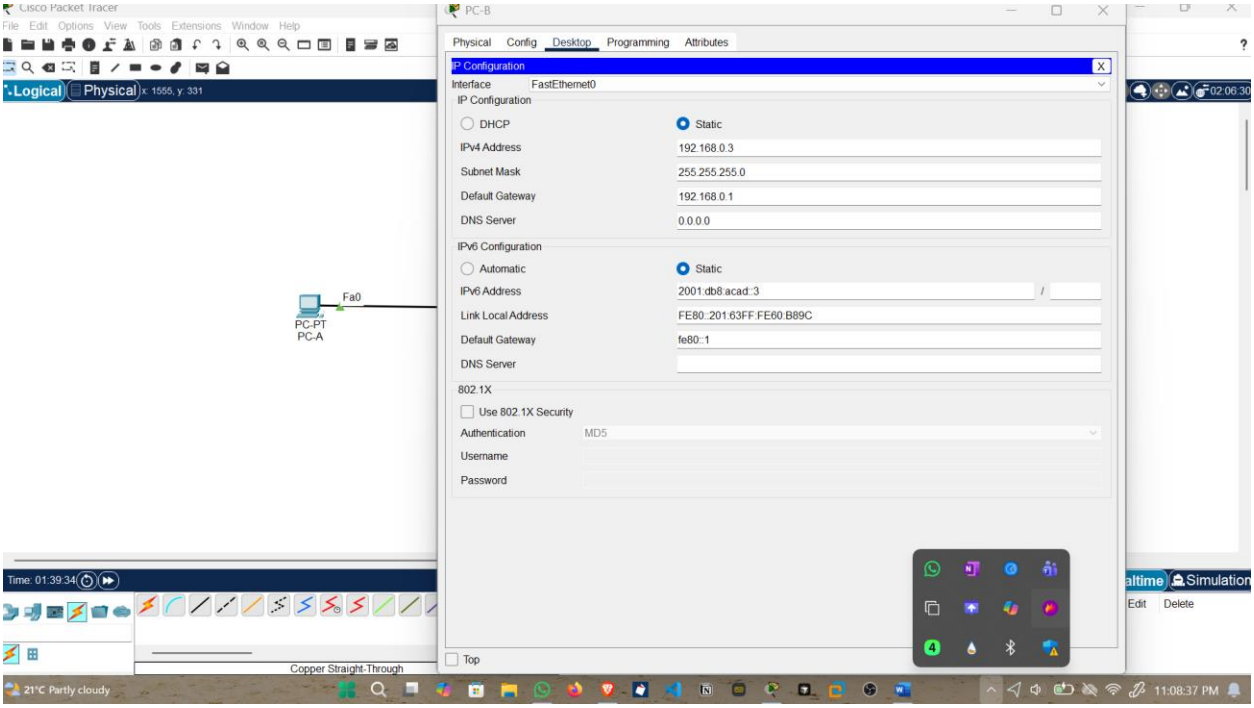
6.2 Part 2: Configure Devices and Verify Connectivity

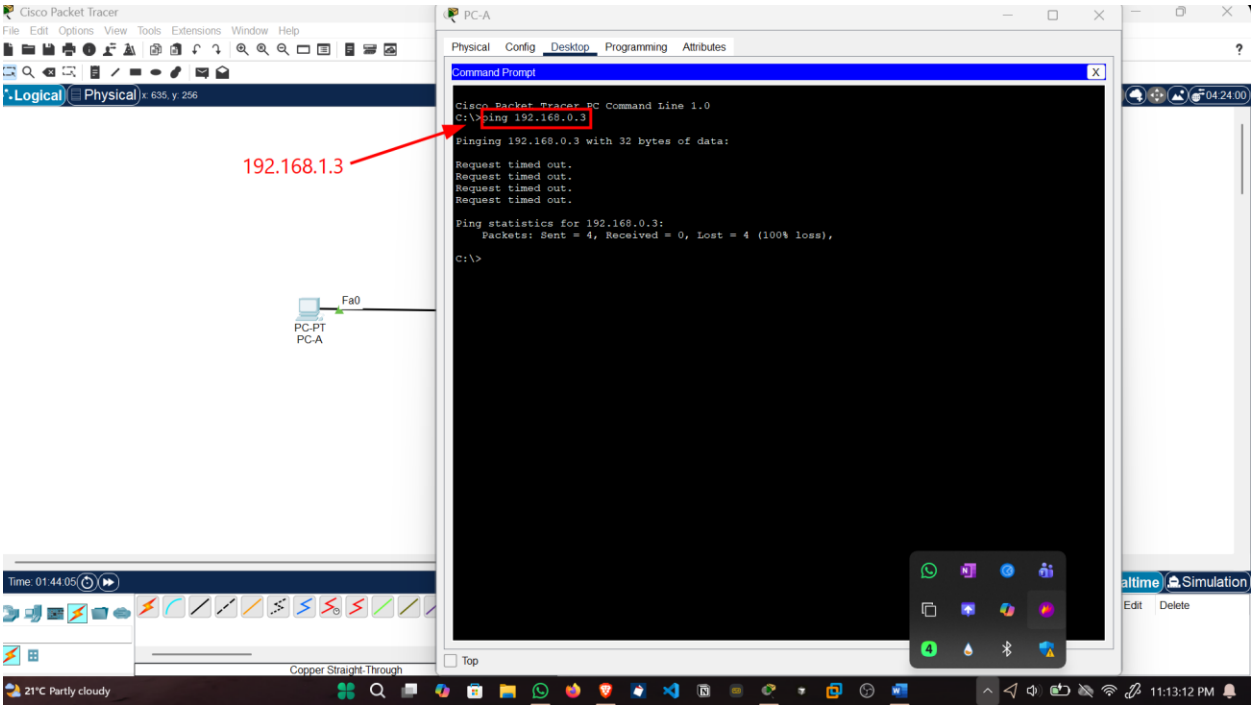
6.2.1 Step 1: Assign static IP information to the PC interfaces.

1. Configure the IP address, subnet mask, and default gateway settings on PC-A.
2. Configure the IP address, subnet mask, and default gateway settings on PC-B.
3. Ping PC-B from a command prompt window on PC-A.

PC-A	NIC	192.168.1.3 /24	192.168.1.1
		2001:db8:acad:1::3/64	fe80::1
PC-B	NIC	192.168.0.3 /24	192.168.0.1
		2001:db8:acad::3/64	fe80::1


Cisco Packet Tracer
PC-A
Physical Config Desktop Programming Attributes
IP Configuration
Interface FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address 192.168.1.3
Subnet Mask 255.255.255.0
Default Gateway 192.168.1.1
DNS Server 0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address 2001:db8:acad:1::3
Link Local Address FE80::201:C9FF:FE91:789
Default Gateway fe80::1
DNS Server
802.1X
Use 802.1X Security
Authentication MD5
Username
Password
Top
Fa0
PC-PT
PC-A
Time: 01:37:06
Copper Straight-Through
New
Delete
Toggle PDU List Window
21°C Partly cloudy
11:06:06 PM


Cisco Packet Tracer
PC-B
Physical Config Desktop Programming Attributes
IP Configuration
Interface FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address 192.168.0.3
Subnet Mask 255.255.255.0
Default Gateway 192.168.0.1
DNS Server 0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address 2001:db8:acad::3
Link Local Address FE80::201:63FF:FE60:B89C
Default Gateway fe80::1
DNS Server
802.1X
Use 802.1X Security
Authentication MD5
Username
Password
Top
Fa0
PC-PT
PC-A
Time: 01:39:34
Copper Straight-Through
Edit
Delete
21°C Partly cloudy
11:08:37 PM



Static IPv4 and IPv6 addresses, subnet masks, and default gateways were configured on both PCs. Initial connectivity tests were unsuccessful due to the absence of router interface configuration, demonstrating the necessity of proper Layer 3 setup.

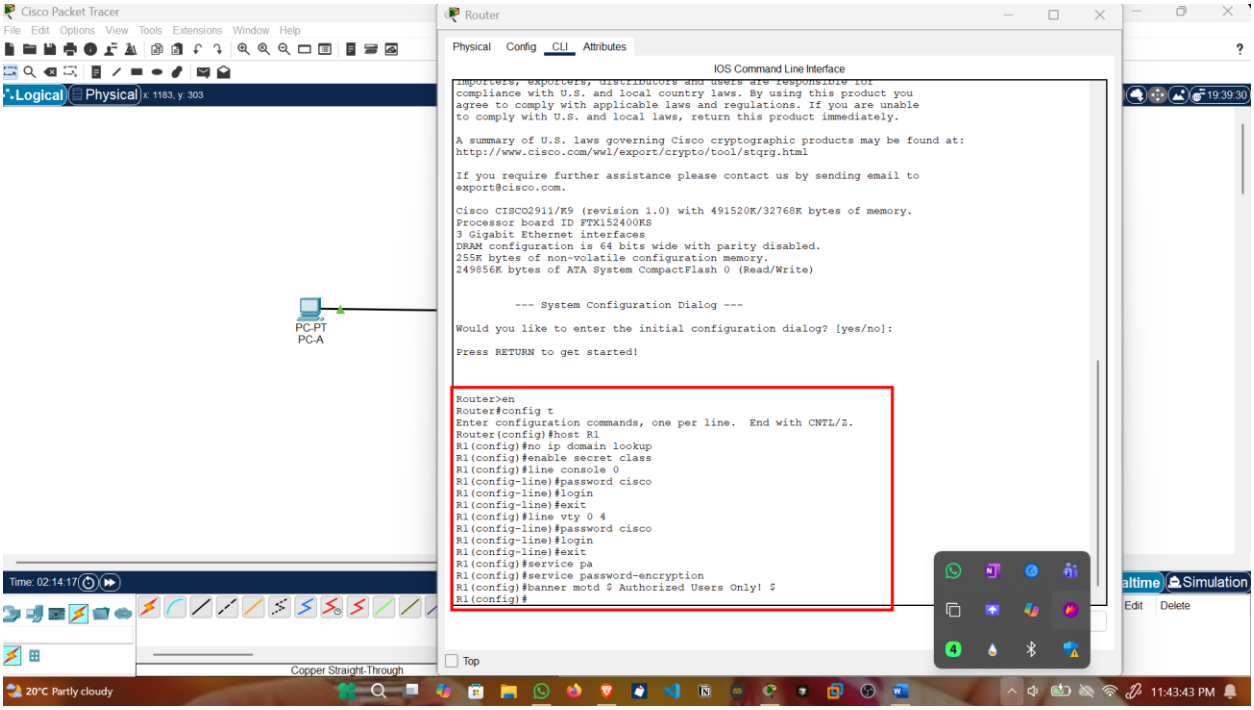
The router interfaces (default gateways) have not been configured yet so Layer 3 traffic is not being routed between subnets.

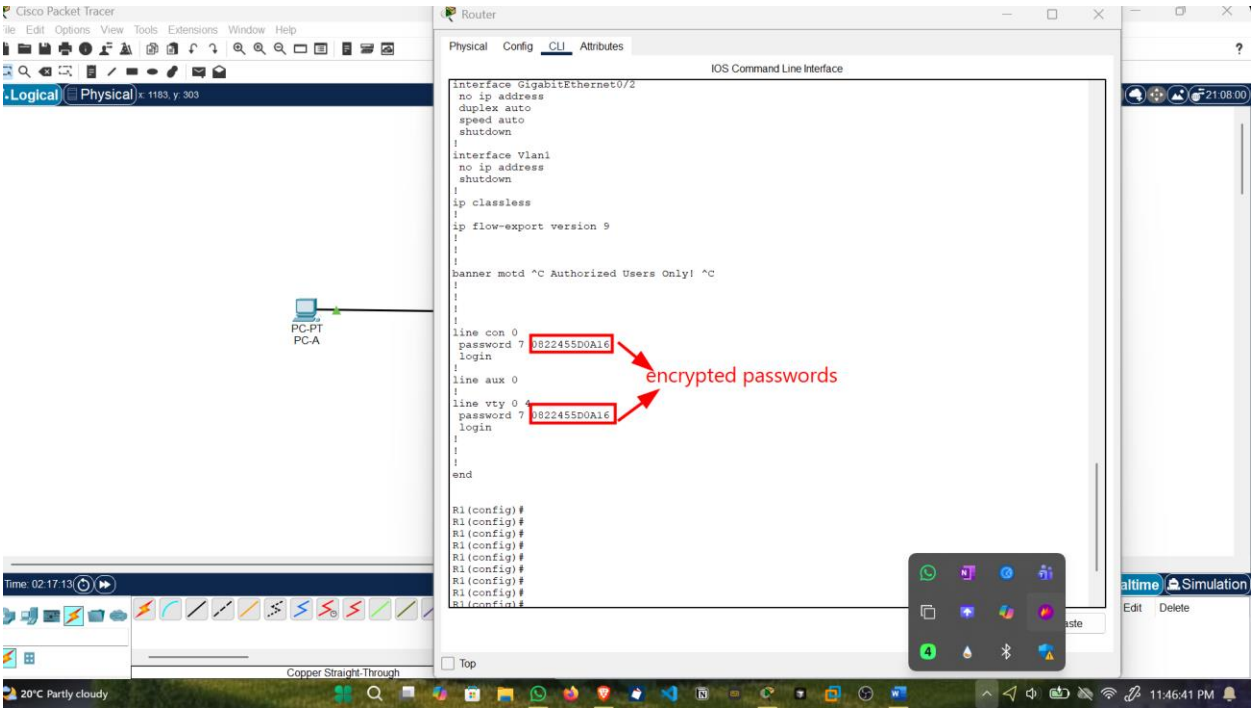
6.2.2 Step 2: Configure the router.

The router was configured with a hostname, DNS lookup was disabled, and secure access controls were implemented using encrypted privileged EXEC passwords, console passwords, and VTY passwords. A warning banner was configured to deter unauthorized access. Router interfaces were assigned IPv4 and IPv6 addresses and activated. Interface descriptions were added for administrative clarity, and IPv6 unicast routing was enabled. The configuration was saved, and the system clock was set.

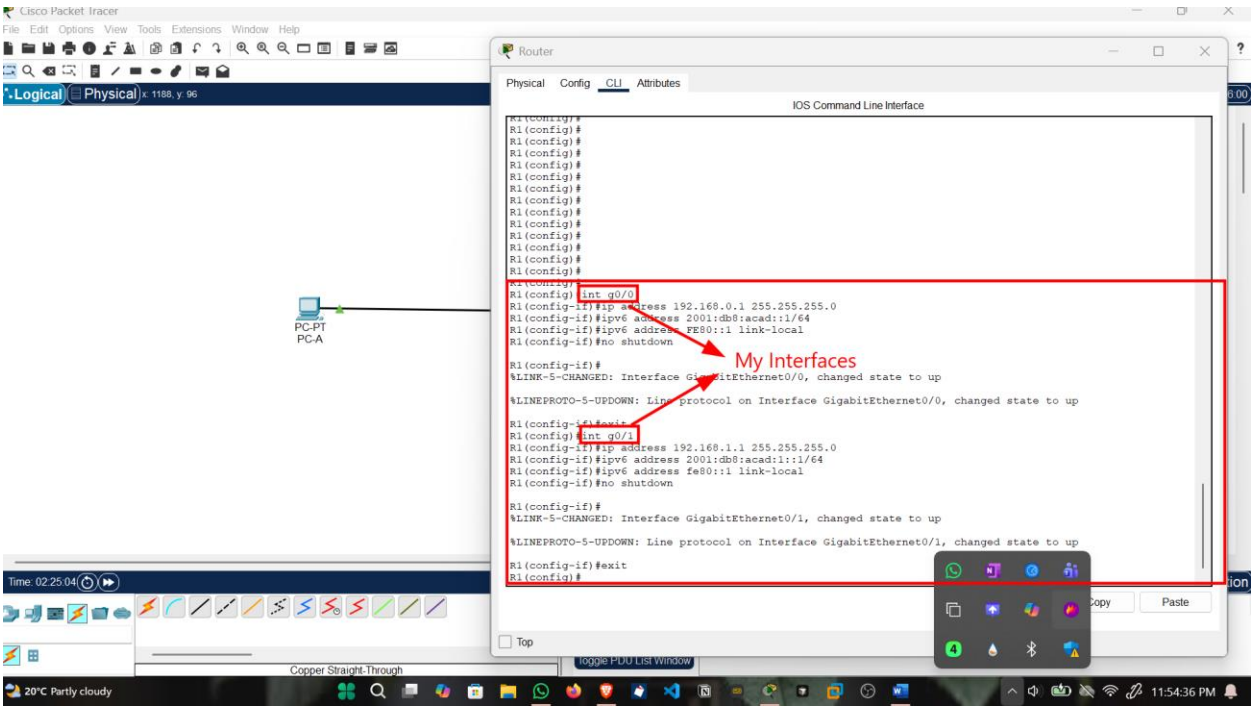
1. Console into the router and enable privileged EXEC mode.
2. Enter configuration mode.
3. Assign a device name to the router.

4. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
5. Assign class as the privileged EXEC encrypted password.
6. Assign cisco as the console password and enable login.
7. Assign cisco as the VTY password and enable login.
8. Encrypt the plaintext passwords.

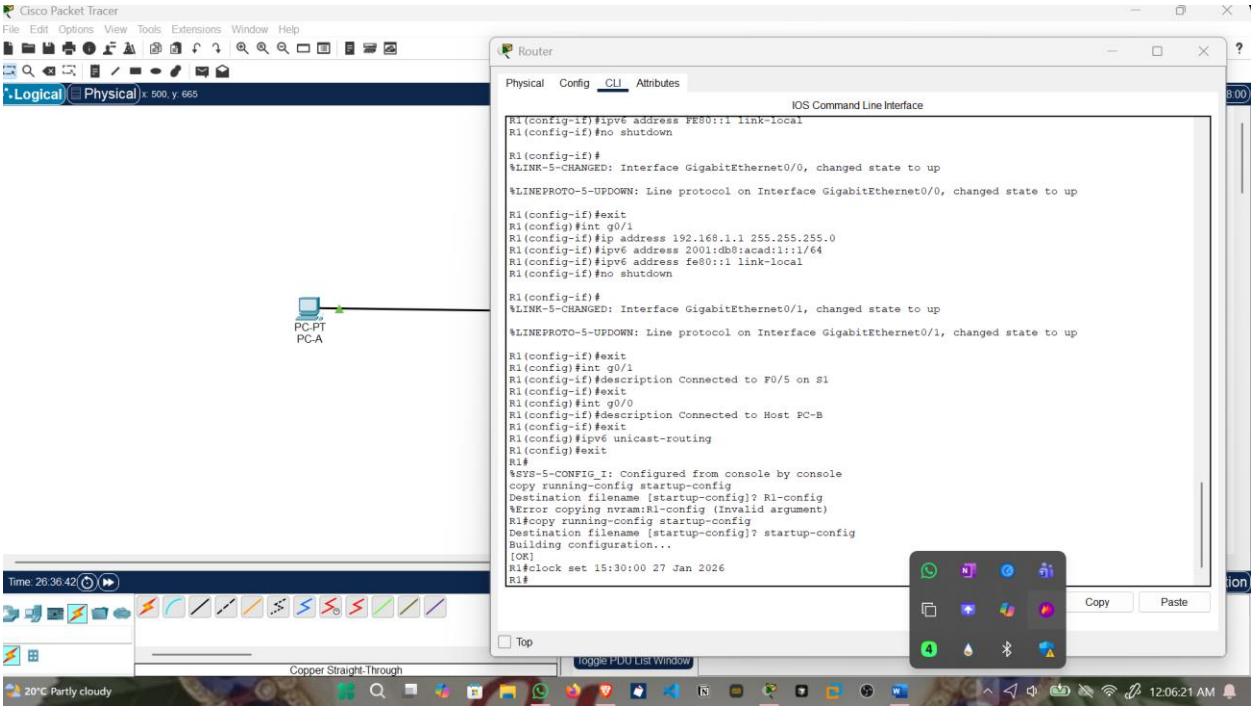




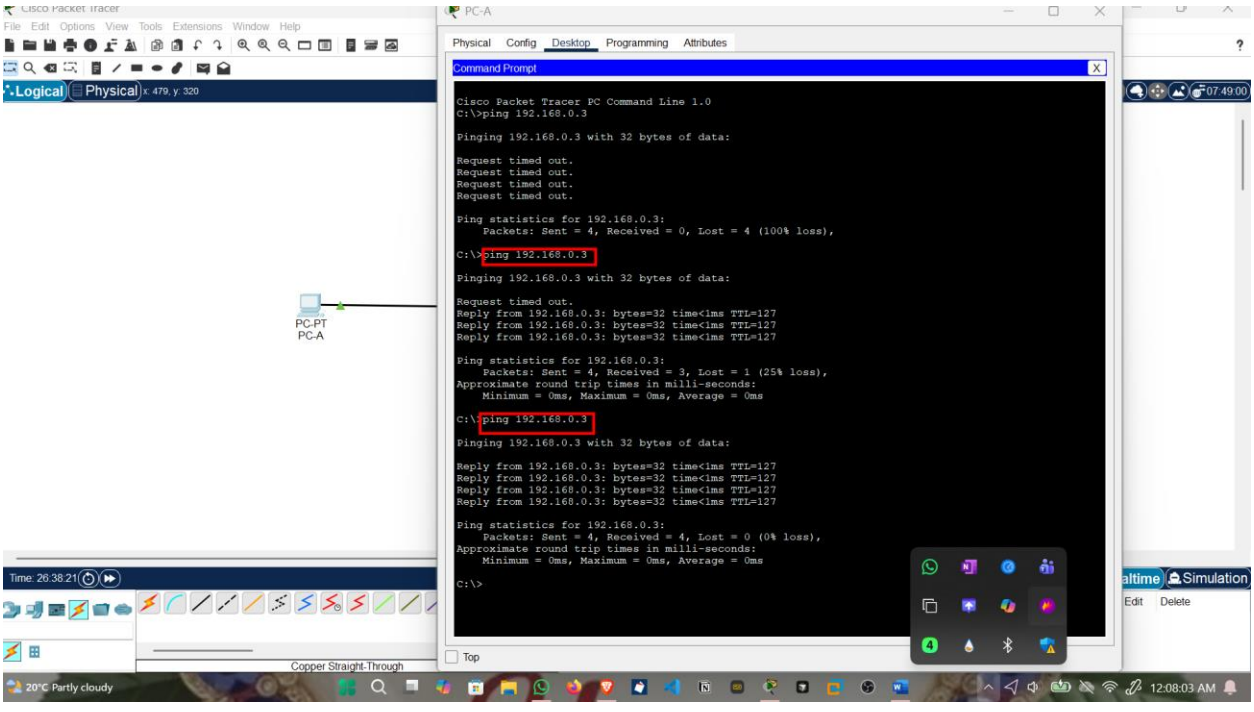
9. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.
10. Configure an interface description for each interface indicating which device is connected to it.



11. To enable IPv6 routing, enter the command ipv6 unicast-routing.
12. Save the running configuration to the startup configuration file.
13. Set the clock on the router.



14. Ping PC-B from a command prompt window on PC-A.

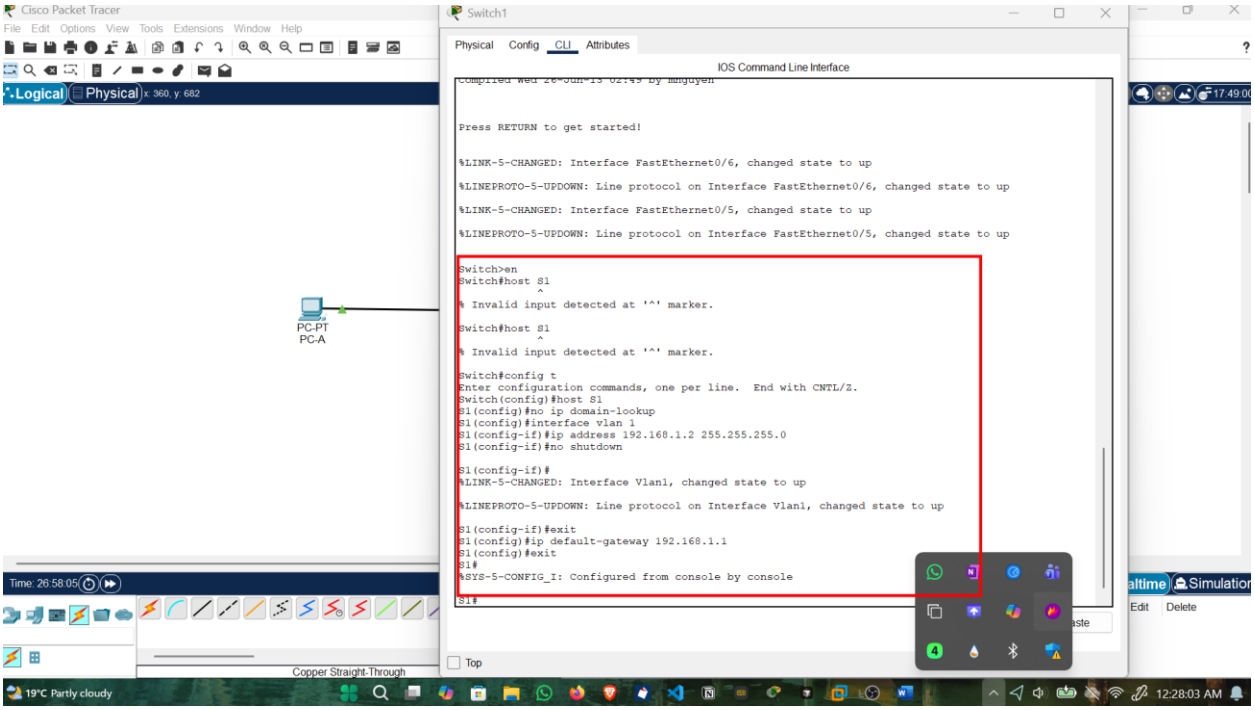


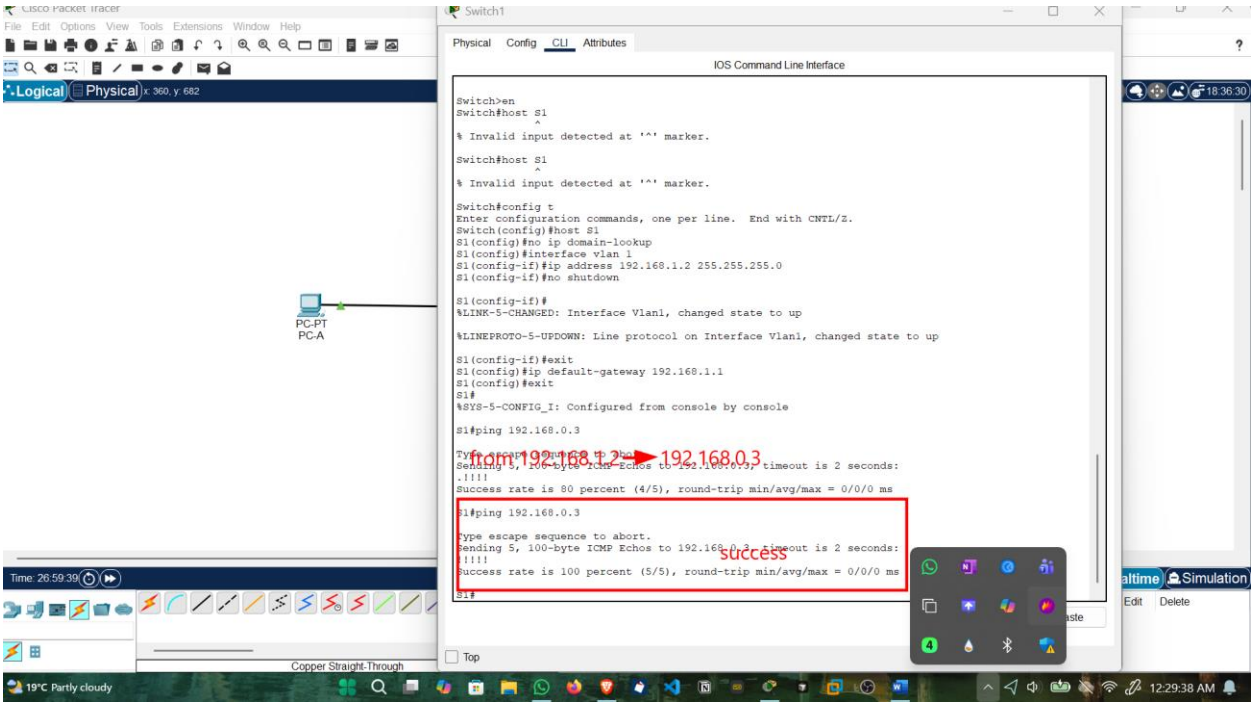
Yes. The router is routing the ping traffic across the two subnets. The default settings for the 2960 switch automatically turned up the interfaces that are connected to devices.

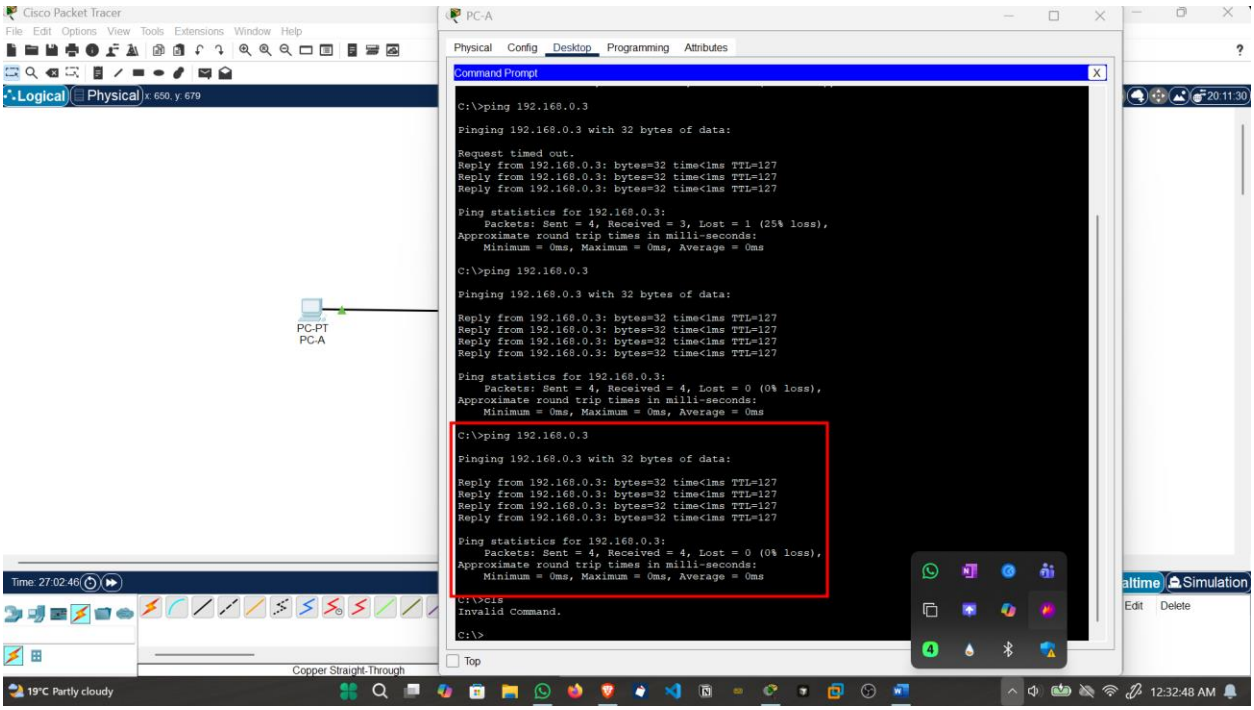
6.2.3 Step 3: Configure the switch.

The switch was configured with a hostname and DNS lookup disabled. The VLAN 1 management interface was assigned an IP address and enabled. A default gateway was configured to allow remote management, and the running configuration was saved.

1. Console into the switch and enable privileged EXEC mode.
2. Enter configuration mode.
3. Assign a device name to the switch.
4. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
5. Configure and activate the VLAN interface on the switch S1.
6. Configure the default gateway for the switch S1.
7. Save the running configuration to the startup configuration file.





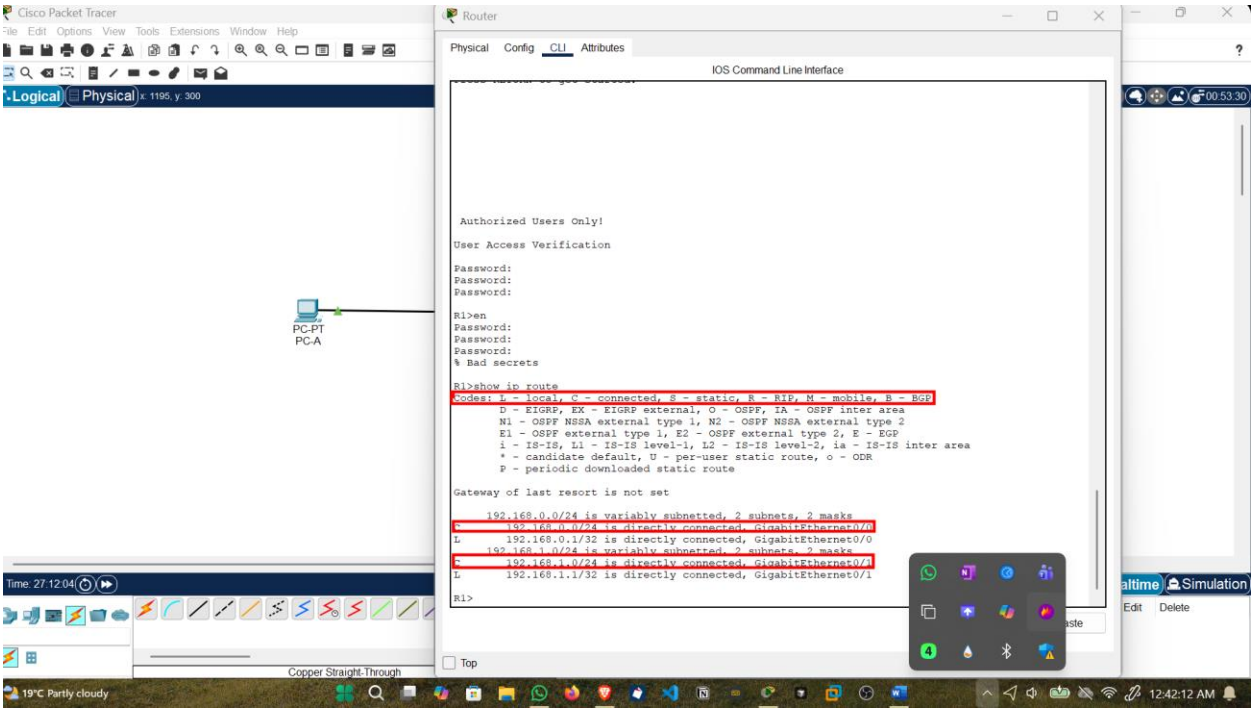


Connectivity was verified using ICMP echo requests between PC-A and PC-B and between the switch and PC-B. All tests were successful, confirming correct addressing, routing, and interface activation. Diagnostic commands were used to validate interface and routing status.

6.3 Part 3: Display Device Information

6.3.1 Step 1: Display the routing table on the router.

Use the show ip route command on the router R1 to answer the following questions.

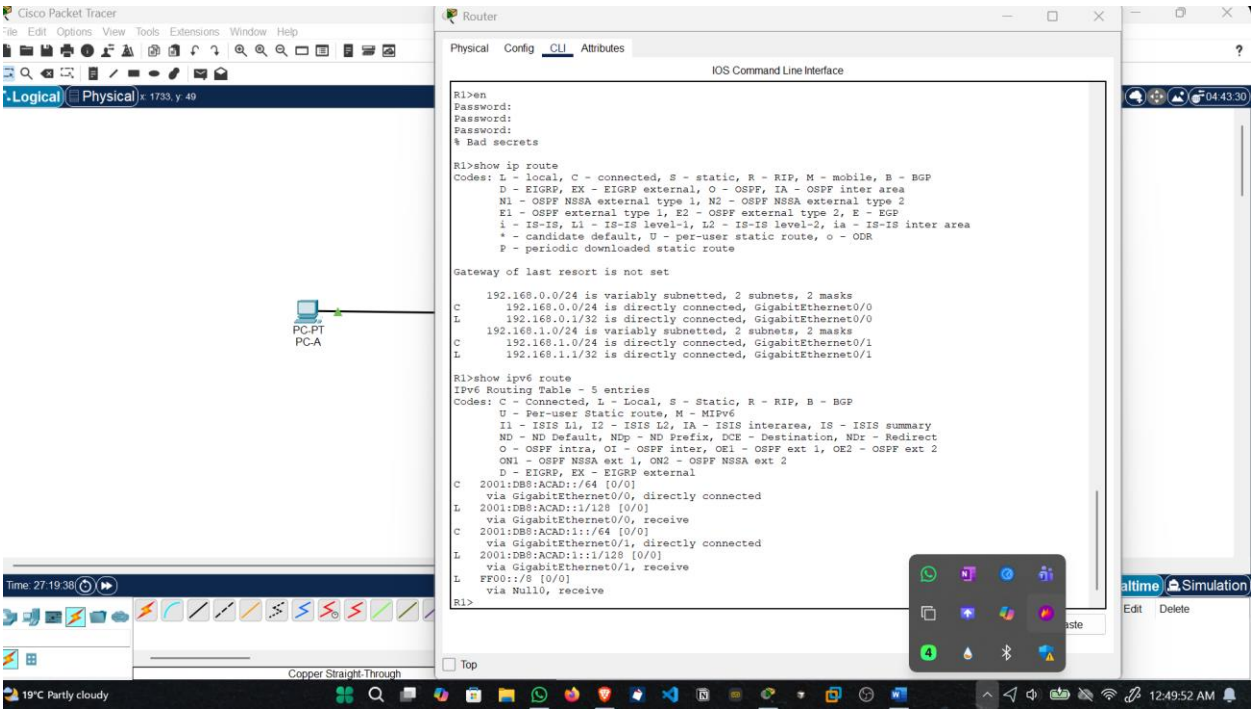


The C designates a directly connected subnet. An L designates a local interface.

Two route entries are coded with a C code in the routing table

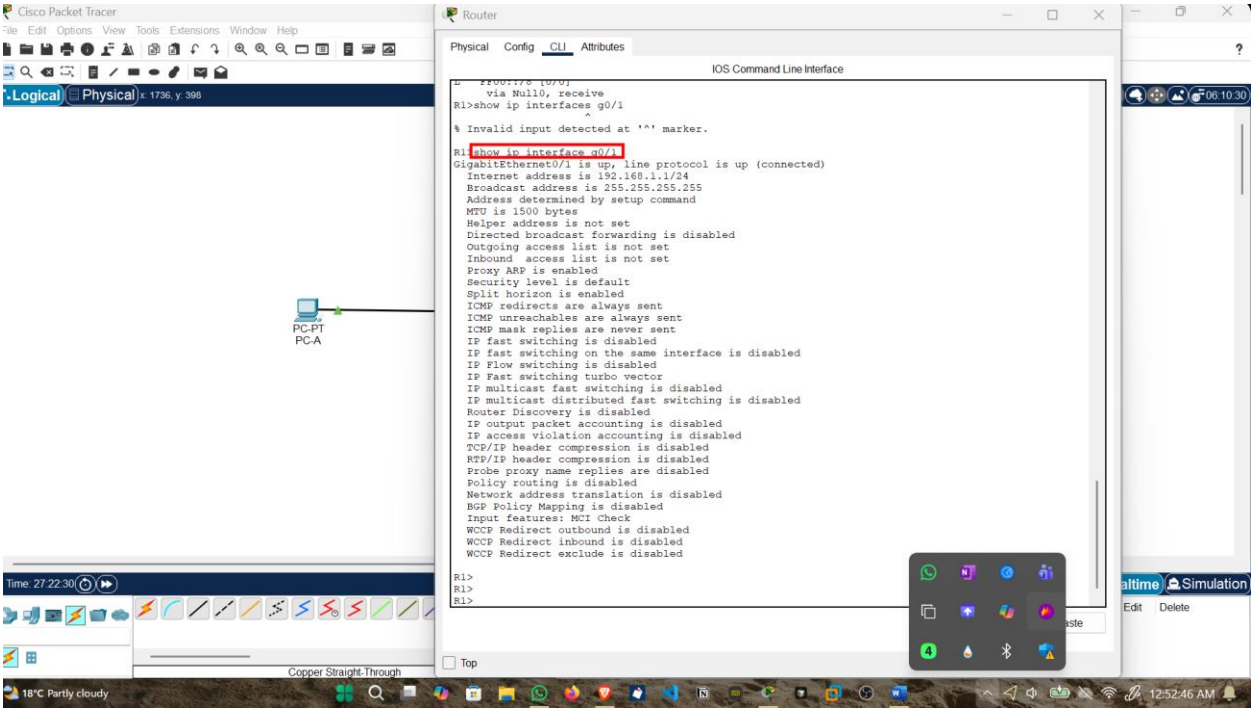
Interface types are associated to the C coded routes: g0/0, g0/1

Use the show ipv6 route command on router R1 to display the IPv6 routes.



6.3.2 Step 2: Display interface information on the router R1.

1. Use the show ip interface g0/0/1 to answer the following questions.

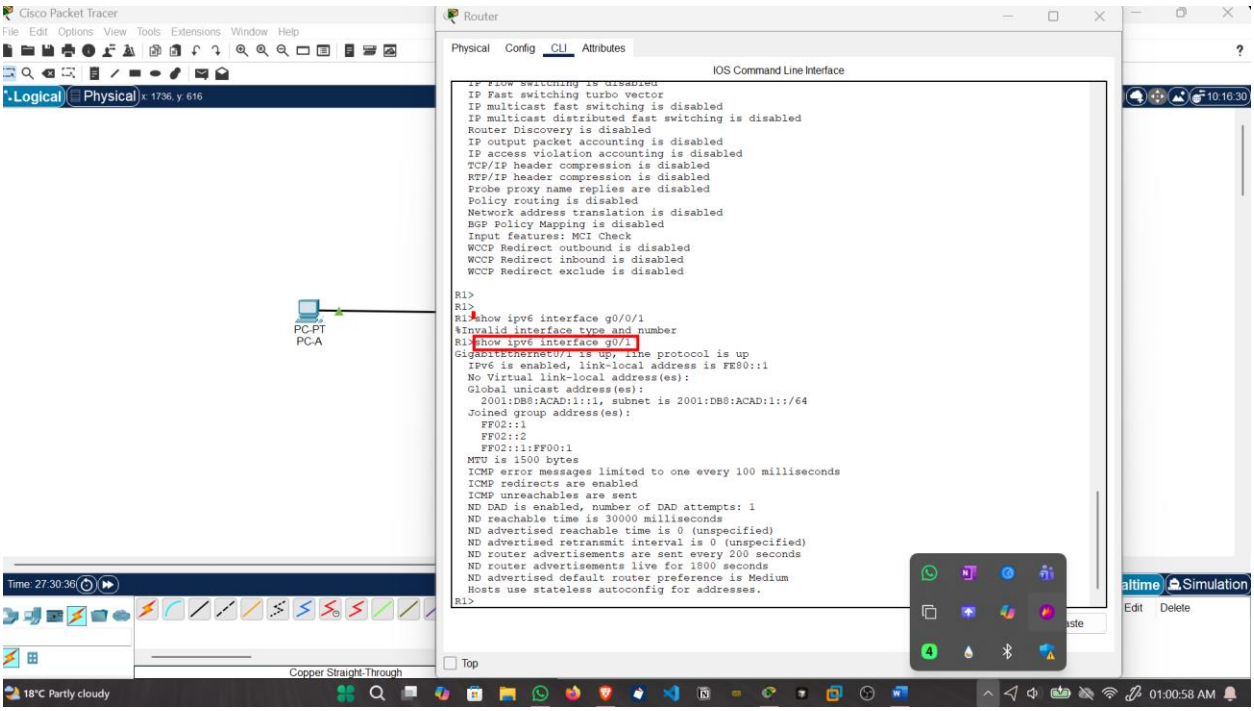


The operational status of the G0/0/1 interface is up,

Internet address is 192.168.1.1/24.

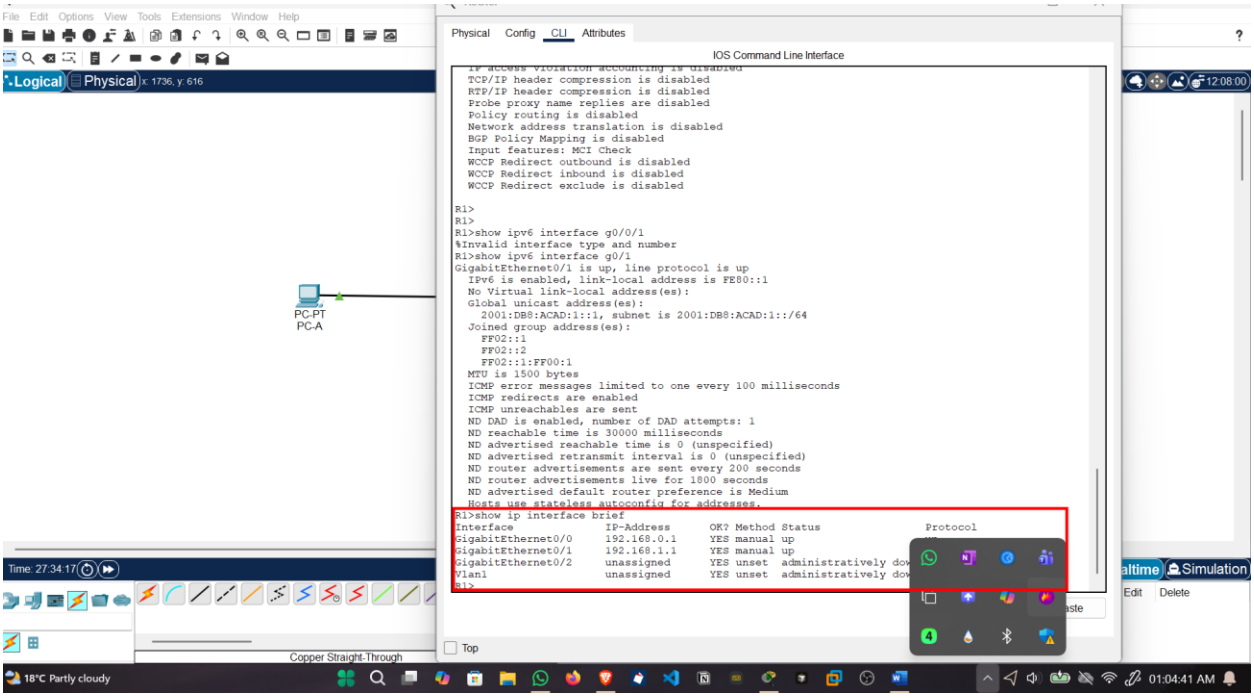
the Media Access Control (MAC) address of the G0/1 interface is

2. For the IPv6 information, enter the show ipv6 interface interface command.

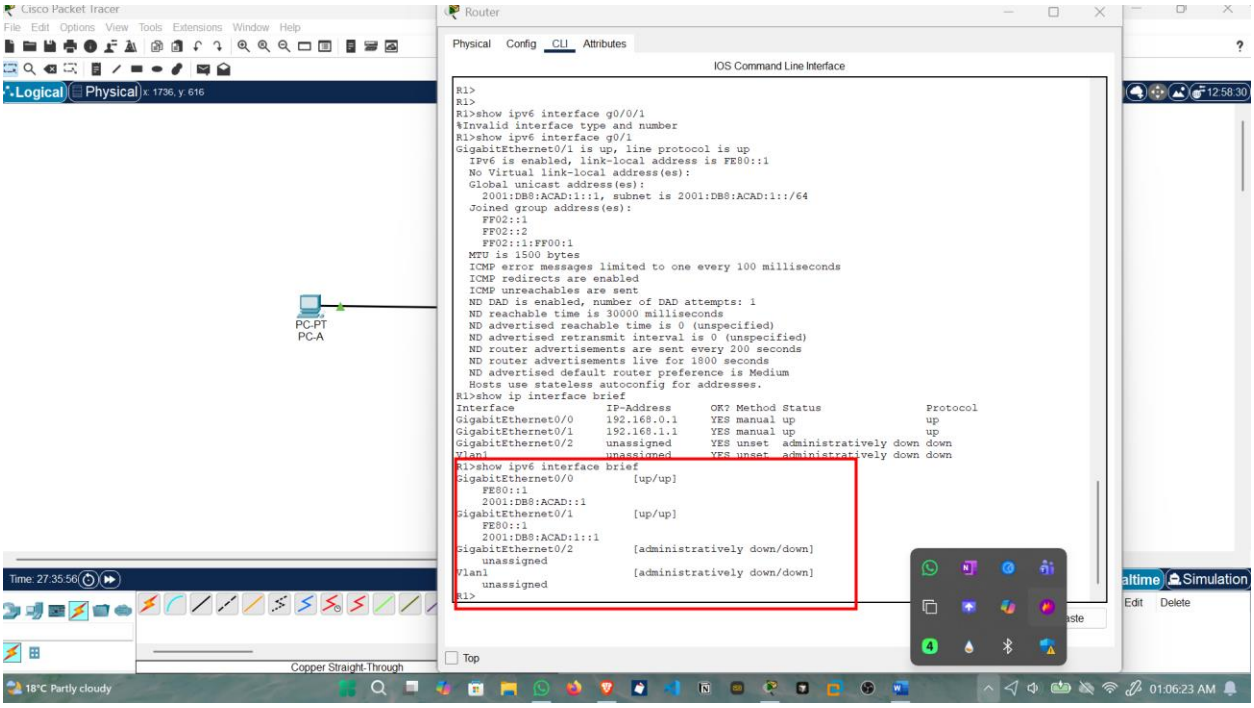


6.3.3 Step 3: Display a summary list of the interfaces on the router and switch.

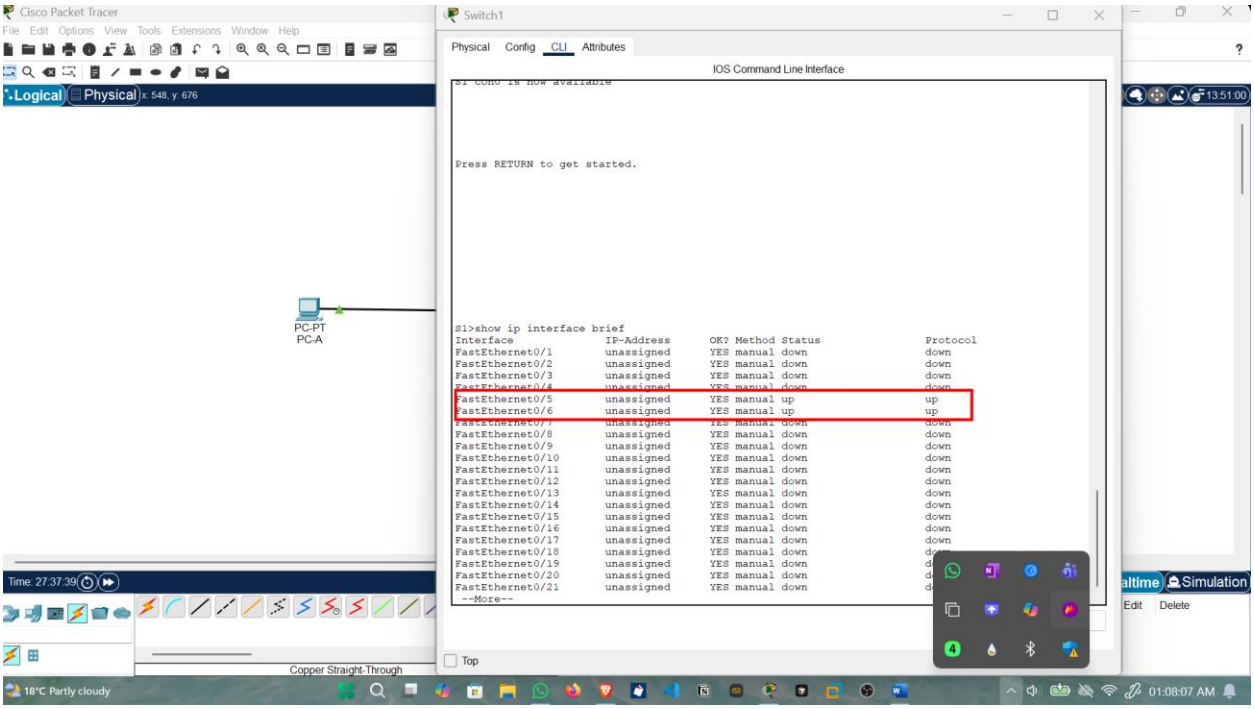
1. Enter the show ip interface brief command on the router R1.



2. To see the IPv6 interface information, enter the show ipv6 interface brief command on R1.



3. Enter the show ip interface brief command on the switch S1.



7 Reflection Questions

If the G0/1 interface showed that it was administratively down, I will run no shutdown command to turn the interface up

When g0/1 is incorrectly configured on the router with an IP address of 192.168.1.2, PC-A would not be able to ping PC-B. This is because PC-B is on a different network than PC-A which requires the default-gateway router to route these packets. PC-A is configured to use the IP address of 192.168.1.1 for the default-gateway router, but this address is not assigned to any device on the LAN. Any packets that need to be sent to the default-gateway for routing will never reach their destination.

8 SECURITY CONCERNS RELATED TO SWITCH AND ROUTER CONFIGURATION

Improper configuration of routers and switches introduced several security risks. Weak or unencrypted passwords could allow unauthorized access to network devices. Misconfigured IP addressing or default gateways could result in traffic misrouting, denial of service, or interception. Failure to secure unused switch ports could permit unauthorized device connections. In addition, improperly configured IPv6 settings could expose networks to unintended routing or attack vectors.

Proper network configuration was essential for ensuring reliable connectivity, operational efficiency, and security. Accurate addressing, interface documentation, and controlled administrative access reduced configuration errors and improved troubleshooting. Secure configurations strengthened the network's resilience against unauthorized access and service disruptions.

9 CONCLUSION

This laboratory exercise successfully demonstrated the implementation of a secure and functional routed network using Cisco IOS devices. Correct configuration of router and switch interfaces enabled reliable IPv4 and IPv6 connectivity. The lab emphasized that proper configuration was critical not only for network functionality but also for security. Misconfigurations could lead to unauthorized access, network outages, or exposure of sensitive resources. The exercise reinforced the importance of secure configuration practices in maintaining stable and protected network infrastructures.

References

1. Cisco Networking Academy.
2. Cyber Shujaa LLM