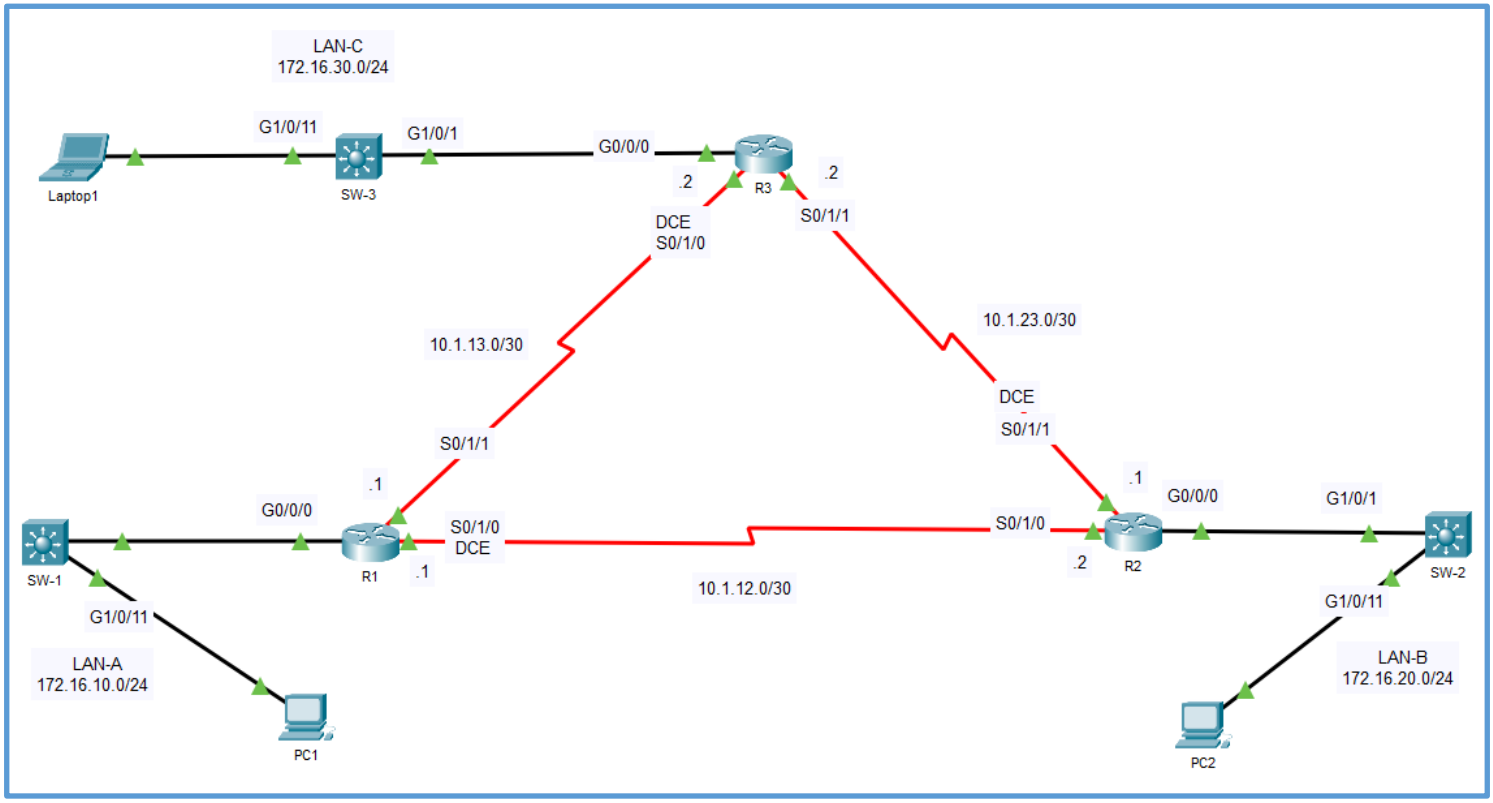
Lab Activity 1 – ACL Configuration:

There are three switches and three routers connected. Please develop the following topology on the physical pod/rack in the lab room.



Required Resources:

- Three Layer-3/Multilayer Switches (Cisco Catalyst 1000 Series with Cisco IOS Release 15.1+ image)
- Three Routers (Cisco 4221 with Cisco IOS Release 17.6+ image)
- Two PCs and one laptop (Windows with Terminal Emulation Program)
- Cables:
    - Console cables to configure the Cisco IOS devices via the console port.
    - Ethernet and serial cables as shown in the topology.

Addressing Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0/0	172.16.10.1	255.255.255.0	N/A

	S0/1/0	10.1.12.1	255.255.255.252	
	S0/1/1	10.1.13.1	255.255.255.252	
R2	G0/0/0	172.16.20.1	255.255.255.0	N/A
	S0/1/0	10.1.12.2	255.255.255.252	
	S0/1/1	10.1.23.1	255.255.255.252	
R3	G0/0/0	172.16.30.1	255.255.255.0	N/A
	S0/1/0	10.1.13.2	255.255.255.252	
	S0/1/1	10.1.23.2	255.255.255.252	
SW-1	VLAN 77	172.16.10.2	255.255.255.0	172.16.10.1
SW-2	VLAN 77	172.16.20.2	255.255.255.0	172.16.20.1
SW-3	VLAN 77	172.16.30.2	255.255.255.0	172.16.30.1
PC1	NIC	172.16.10.10	255.255.255.0	172.16.10.1
PC2	NIC	172.16.20.20	255.255.255.0	172.16.20.1
Laptop1	NIC	172.16.30.30	255.255.255.0	172.16.30.1

Lab Description:

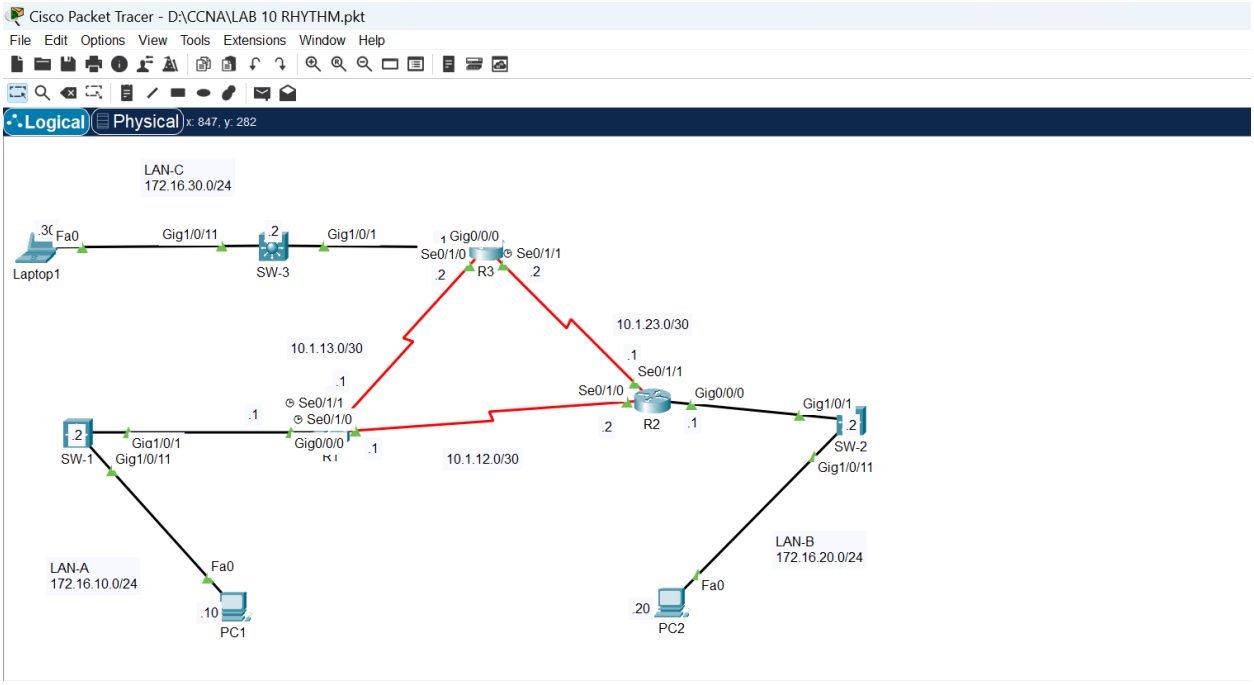
a. In this lab, please build a LAN and WAN based simple switched network.
b. You are also required to do the basic configuration on switches, routers, PCs, and laptops:
    - Switches: Hostnames, SVI, default gateway, DNS lookup (disable), banner, console and vty line passwords, privilege exec mode encrypted password, enable encryption service, and so on.
    - Routers: Hostnames, DNS lookup (disable), banner, console and vty line passwords, enable encryption service, privilege exec mode encrypted password, interface configurations, and so on.
    - PCs and laptop: IP address, Subnet Mask and Default Gateway.

Part –1:

SOLUTION

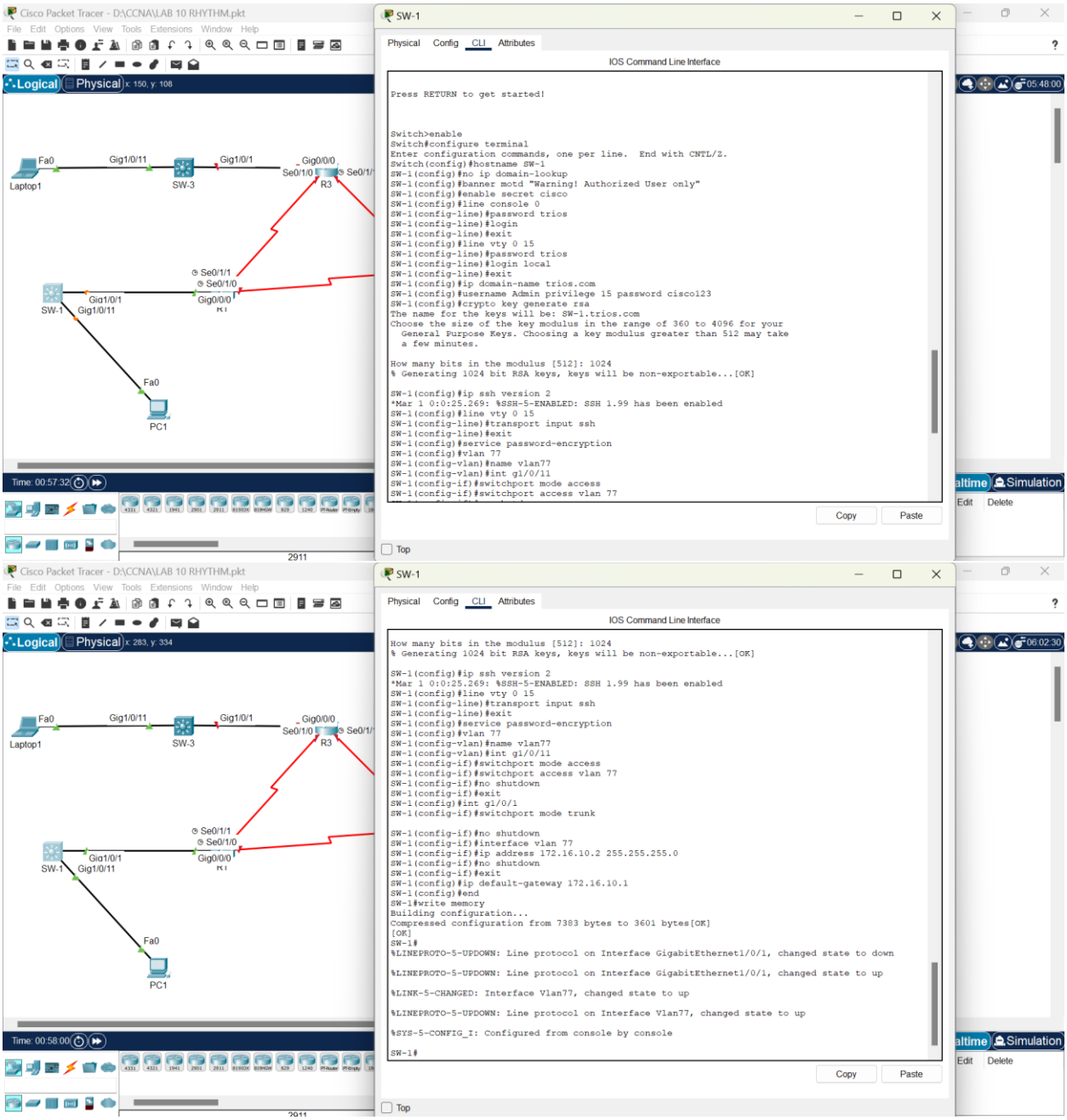
Step 1: Set up the network topology.

- Simulate the topology by using all the devices mentioned above and then cable them all together:
    - Turn on the devices.
    - Connect the switches with the default gateways.
    - Connect the routers using serial connections with other routers.
    - Connect the PCs and Server with their respective switches.
    - Make sure all the lights between switches and other devices are green.

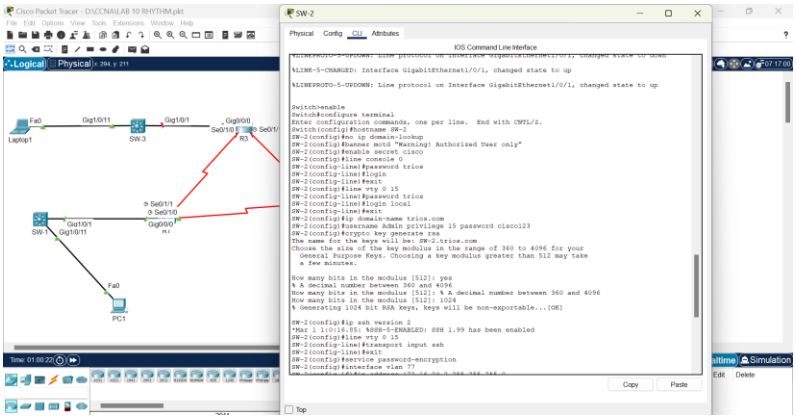


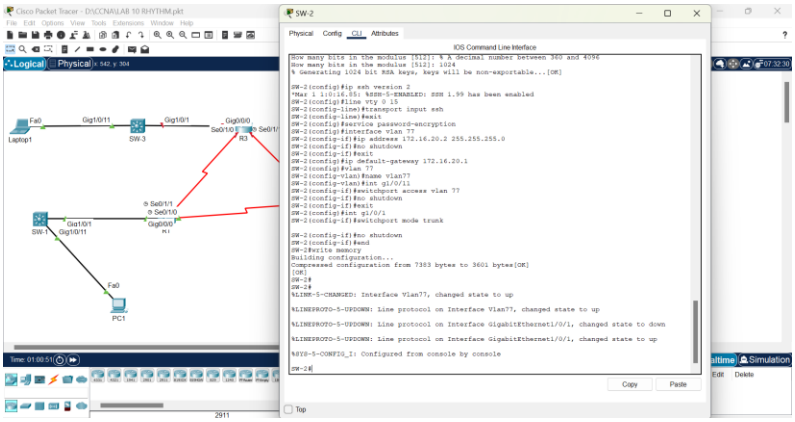
Step 2: Configure and verify basic switch settings on all switches.

S1

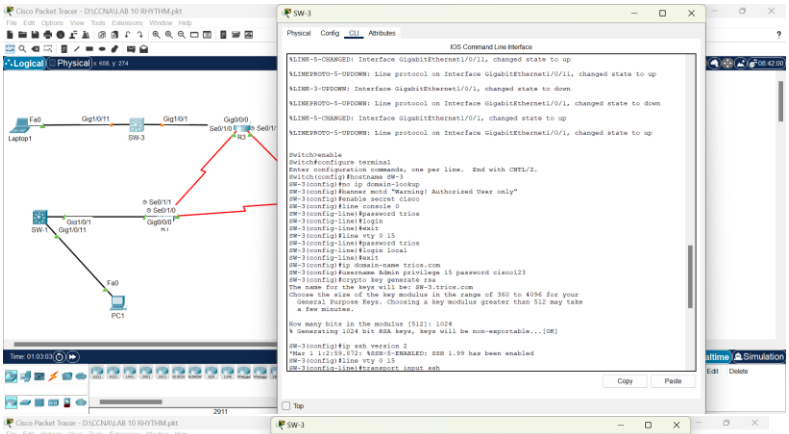


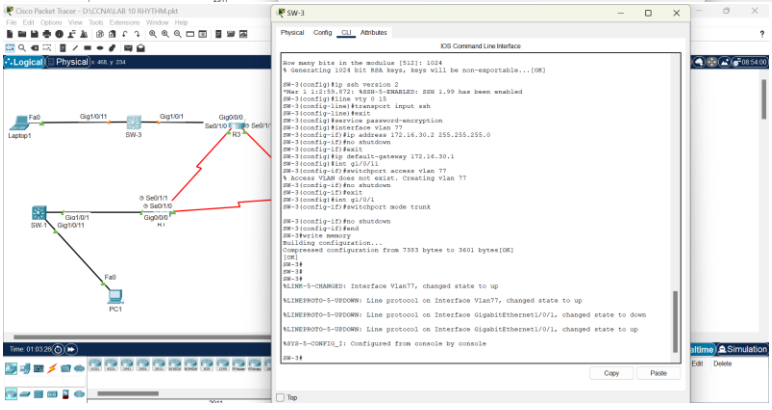
SW-2





S3

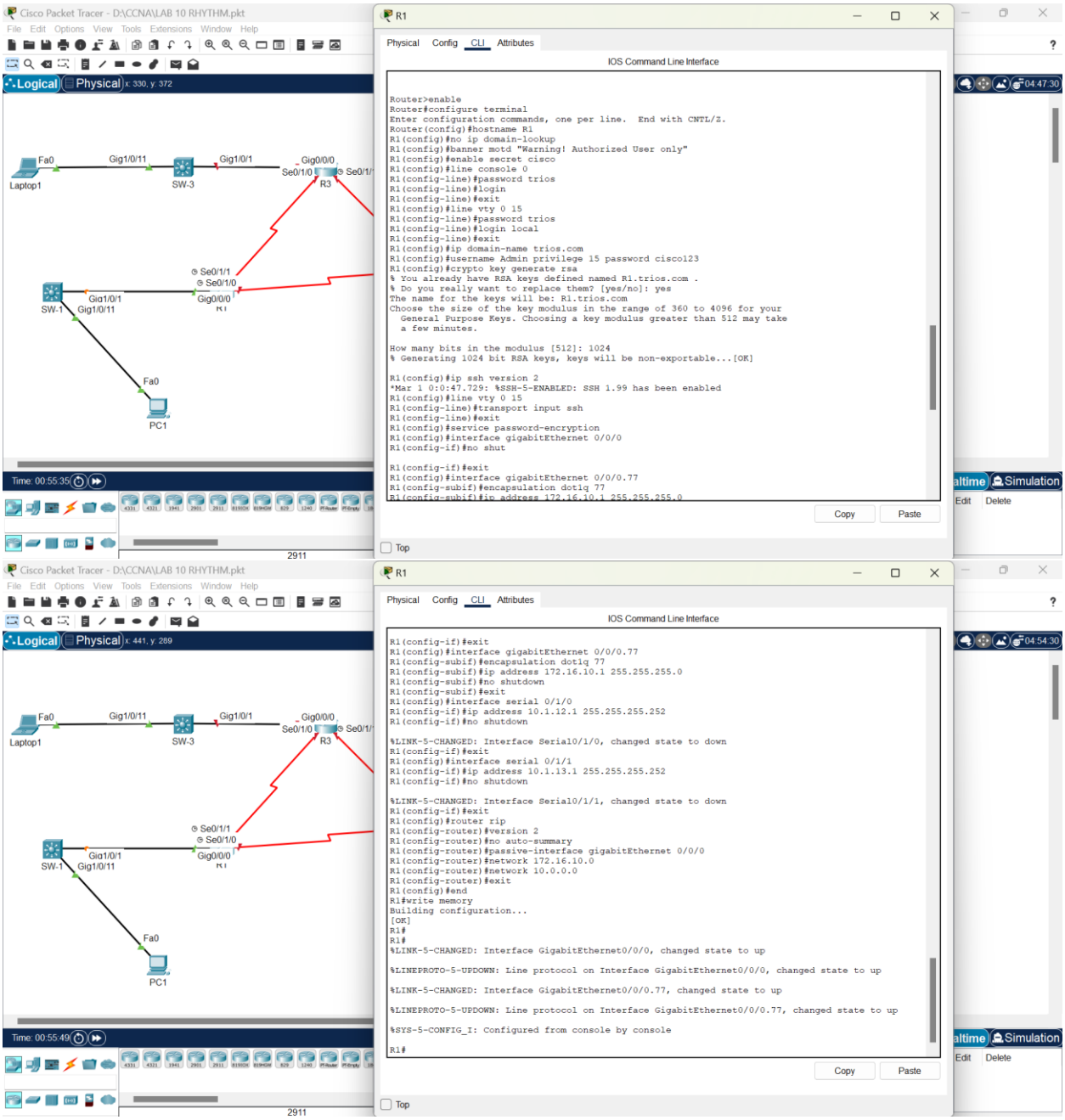




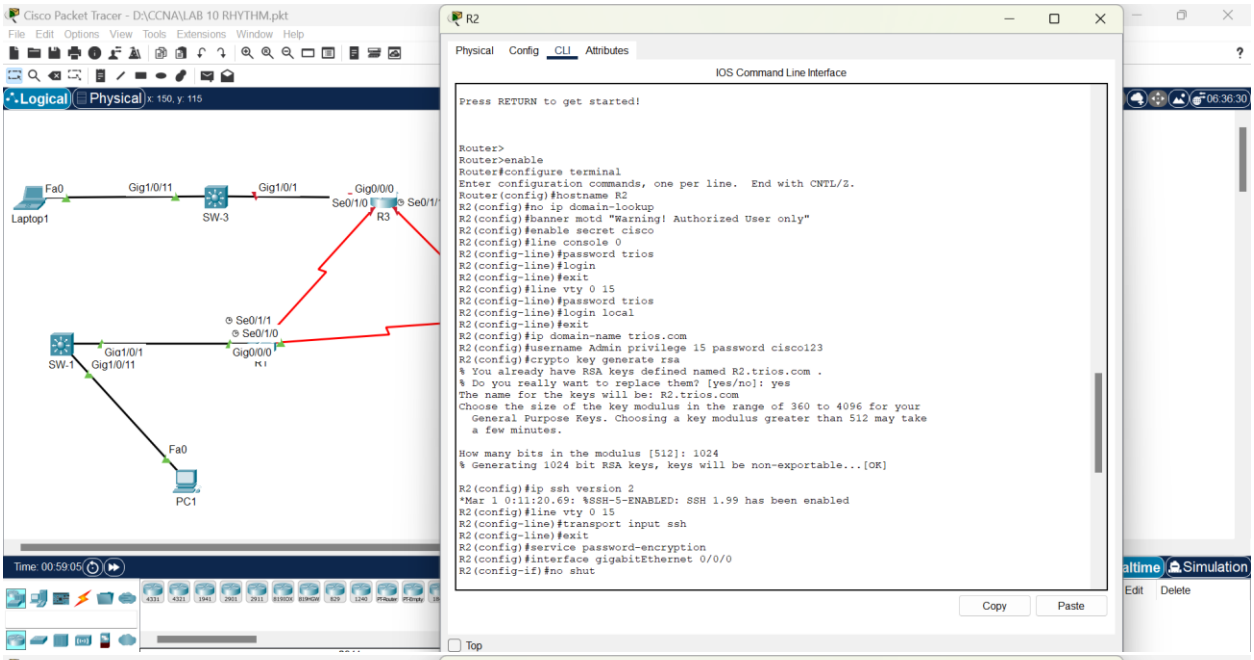
- Console into the switch and enter the global configuration mode:
    - Assign the switch with a host name according to the addressing table.
    - Disable unwanted DNS lookup.
    - Configure a login MOTD banner to warn about illegal access.
    - Assign the encrypted password cisco to privilege exec mode (#).
    - Protect the physical and virtual lines from having console access using the password cisco and configure ***logging synchronous*** for the console line.
    - Encrypt all current and future passwords by enabling the required service.
    - Configure and activate SVI according to the addressing table.
    - Configure default gateway according to the addressing table.
    - Save the configuration.

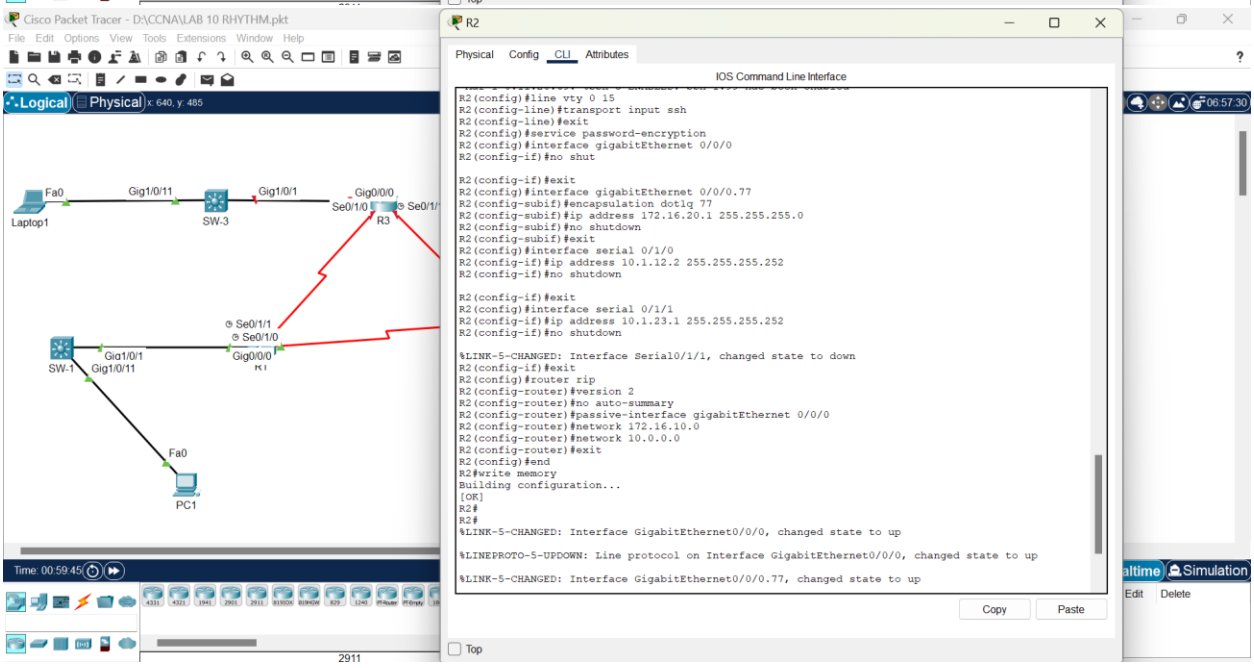
Step 3: Configure and verify connectivity in basic router settings on all routers.

R1

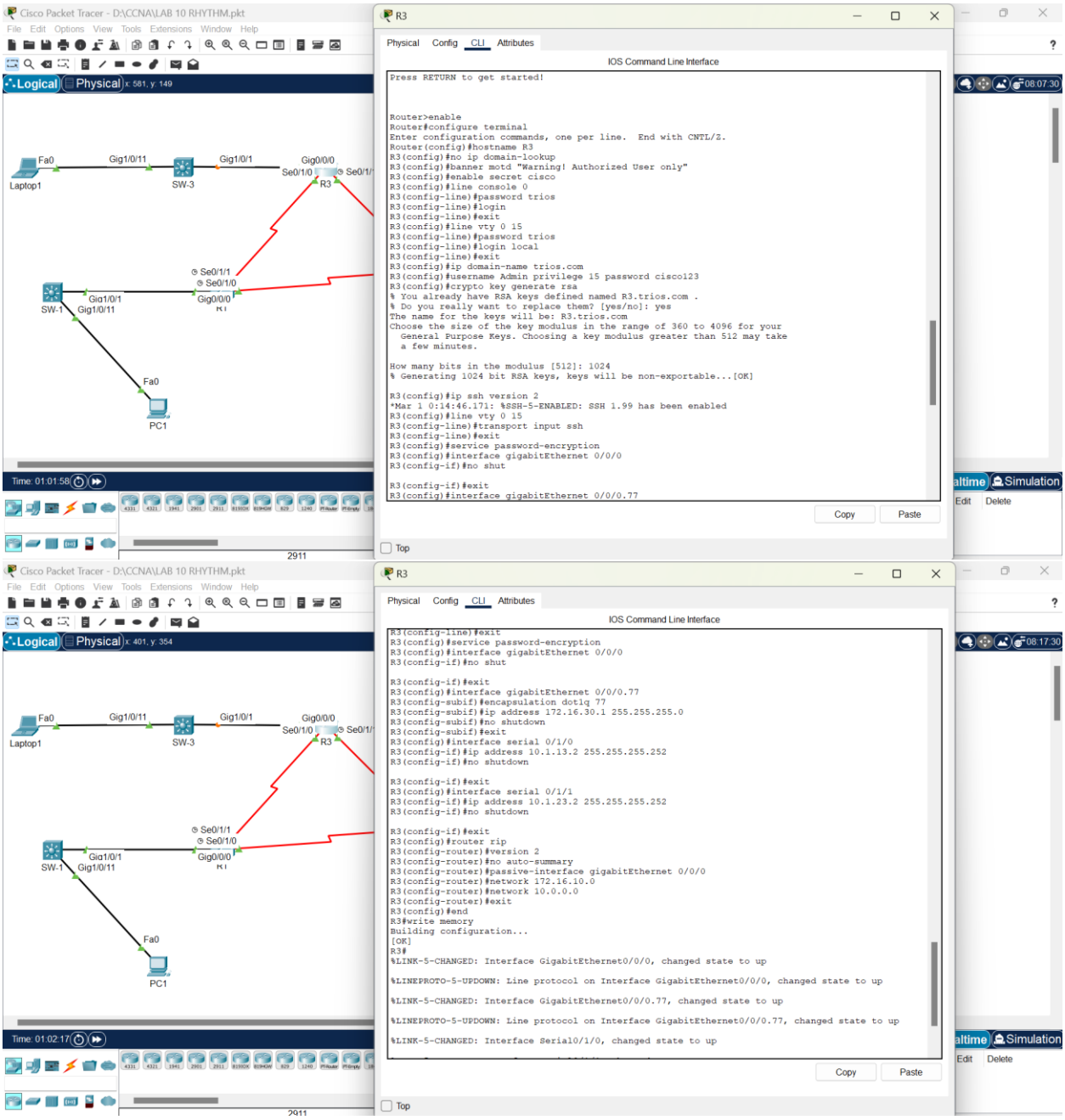


R2


Cisco Packet Tracer - D:\CCNA\LAB 10 RHYTHM.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 150, y: 115
Fa0
Gig1/0/11
Gig1/0/1
Gig0/0/0
Se0/1/0
Se0/1/1
Laptop1
SW-3
R3
SW-1
PC1
Time: 00:59:05
R2
Physical Config CLI Attributes
IOS Command Line Interface
Press RETURN to get started!
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#no ip domain-lookup
R2(config)#banner motd "Warning! Authorized User only"
R2(config)#enable secret cisco
R2(config)#line console 0
R2(config-line)#password trios
R2(config-line)#login
R2(config-line)#exit
R2(config)#line vty 0 15
R2(config-line)#password trios
R2(config-line)#login local
R2(config-line)#exit
R2(config)#ip domain-name trios.com
R2(config)#username Admin privilege 15 password cisco123
R2(config)#crypto key generate rsa
% You already have RSA keys defined named R2.trios.com .
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: R2.trios.com
Choose the size of the key modulus in the range of 360 to 4096 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]
R2(config)#ip ssh version 2
*Mar 1 0:11:20.69: %SSH-5-ENABLED: SSH 1.99 has been enabled
R2(config)#line vty 0 15
R2(config-line)#transport input ssh
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#interface gigabitEthernet 0/0/0
R2(config-if)#no shut
Copy
Paste
Top
06:36:30
Simulation
Edit
Delete


Cisco Packet Tracer - D:\CCNA\LAB 10 RHYTHM.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 640, y: 485
Fa0
Gig1/0/11
Gig1/0/1
Gig0/0/0
Se0/1/0
Se0/1/1
Laptop1
SW-3
R3
SW-1
PC1
Time: 00:59:45
R2
Physical Config CLI Attributes
IOS Command Line Interface
R2(config)#line vty 0 15
R2(config-line)#transport input ssh
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#interface gigabitEthernet 0/0/0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#interface gigabitEthernet 0/0/0.77
R2(config-subif)#encapsulation dot1q 77
R2(config-subif)#ip address 172.16.20.1 255.255.255.0
R2(config-subif)#no shutdown
R2(config-subif)#exit
R2(config)#interface serial 0/1/0
R2(config-if)#ip address 10.1.12.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface serial 0/1/1
R2(config-if)#ip address 10.1.23.1 255.255.255.252
R2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
R2(config-if)#exit
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#passive-interface gigabitEthernet 0/0/0
R2(config-router)#network 172.16.10.0
R2(config-router)#network 10.0.0.0
R2(config-router)#exit
R2(config)#end
R2#write memory
Building configuration...
[OK]
R2#
R2#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0.77, changed state to up
Copy
Paste
Top
06:57:30
Simulation
Edit
Delete
2911

R3

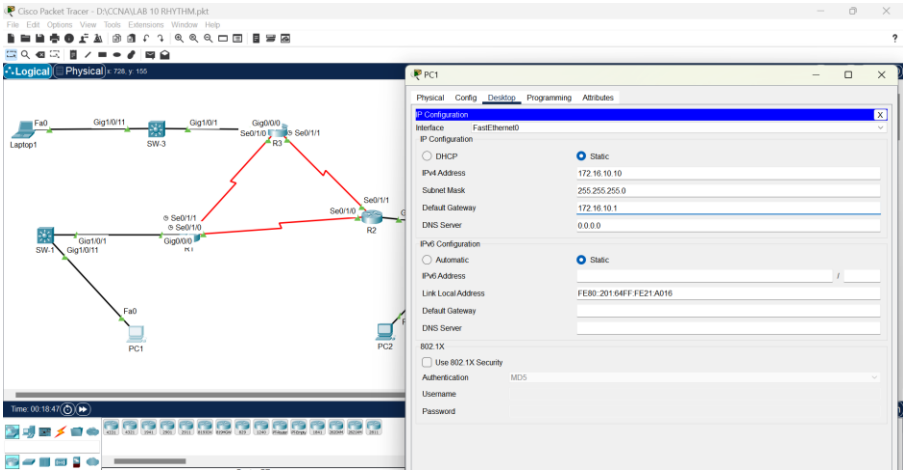


- Console into the switch and enter the global configuration mode:
  - Assign the router with a host name according to the addressing table.
  - Disable unwanted DNS lookup.
  - Configure a login MOTD banner to warn about illegal access.
  - Assign the encrypted password cisco to privilege exec mode (#).
  - Protect the physical and virtual lines from having console access using the password cisco and configure logging synchronous for the console line.
  - Encrypt all current and future passwords by enabling the required service.

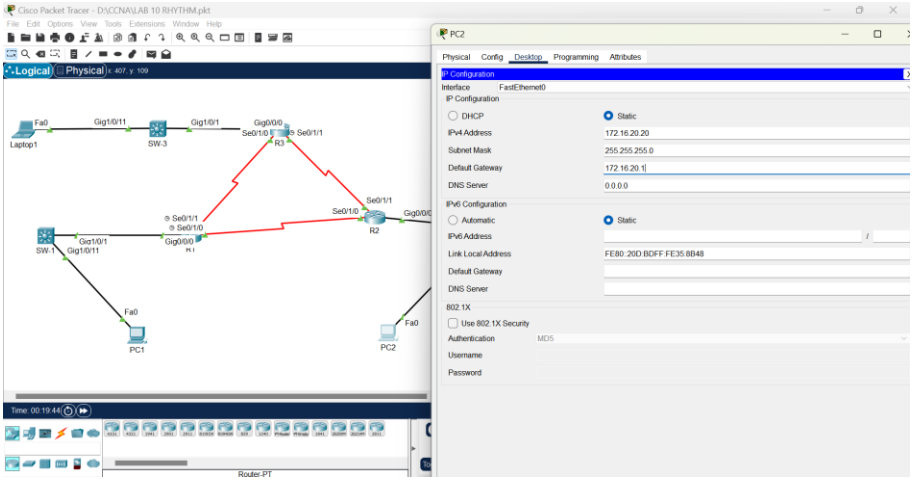
    - Configure and activate all active interfaces according to the addressing table on each router.
- Enable RIP routing protocol on all routers and apply the following configurations:
    - Use RIP version 2.
    - Make sure that auto-summarization of routes is disabled.
    - Advertise all directly connected networks.
    - The LAN interfaces must be configured as passive, so that the routing updates will not be forwarded towards LANs.
- Save the configuration.

Step 4: Configure the PCs and laptop.

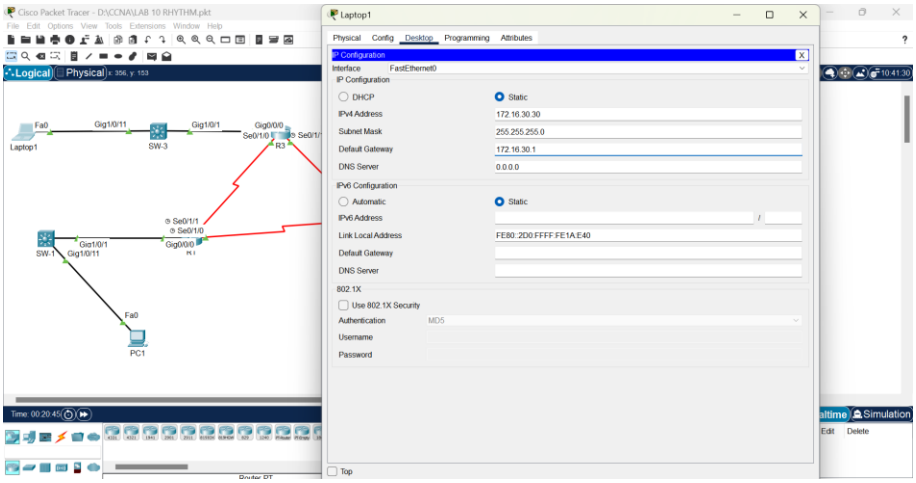
PC1



PC2



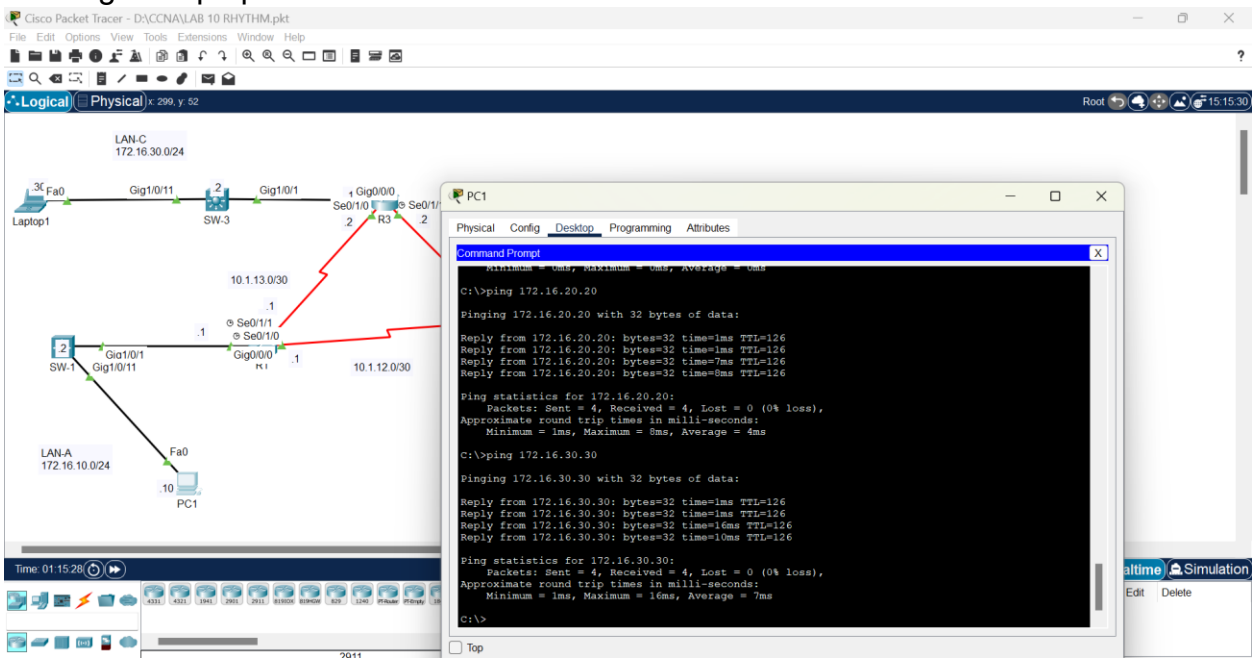
LAPTOP1



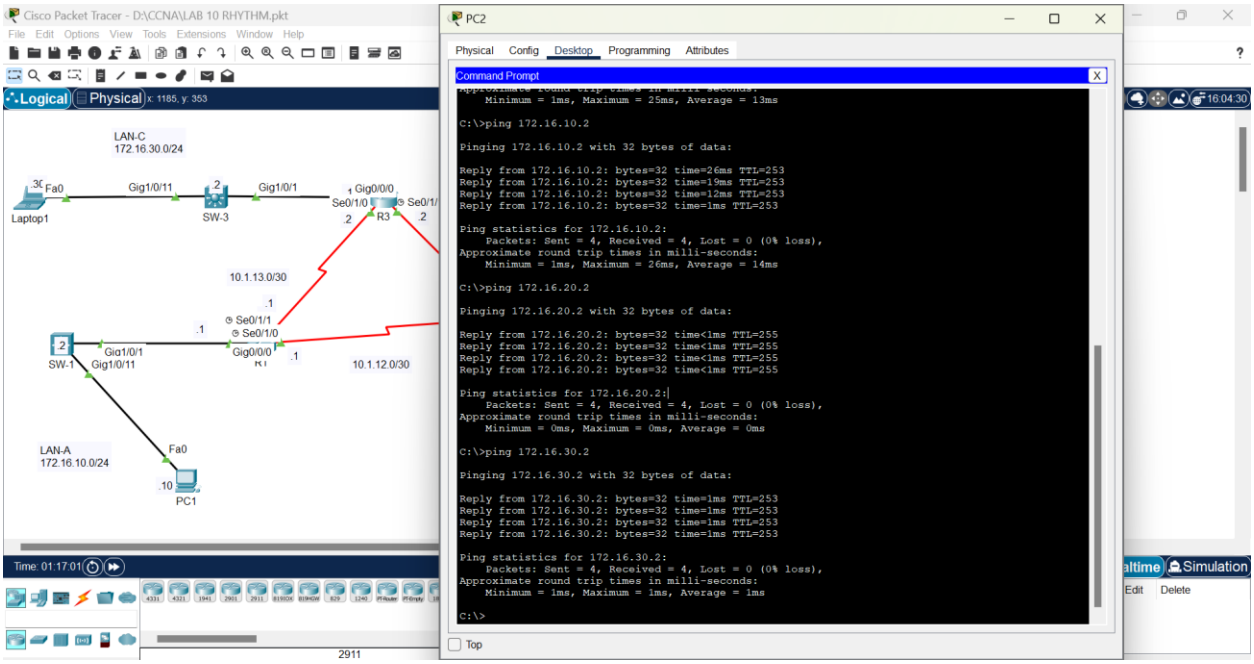
- Assign the appropriate IP address, subnet mask and default gateway to each PC and laptop as per the addressing table.

Step 5: Verify connectivity.

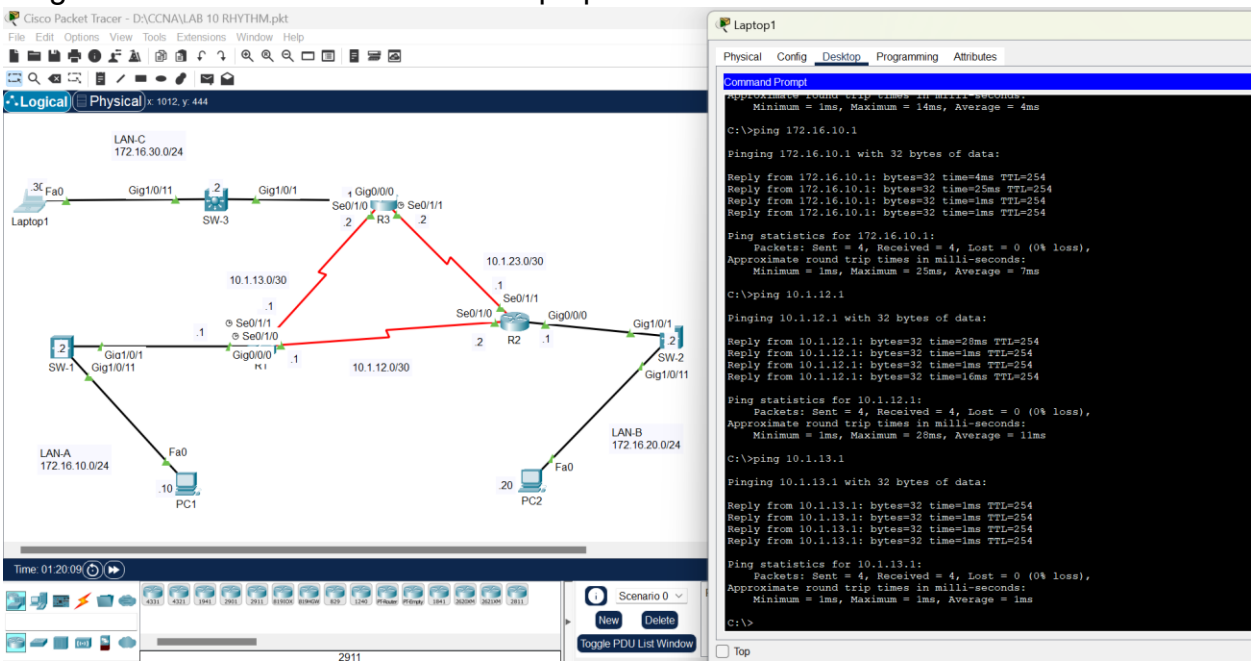
- Ping to PC2 from PC1.
- Ping to Laptop1 from PC1.



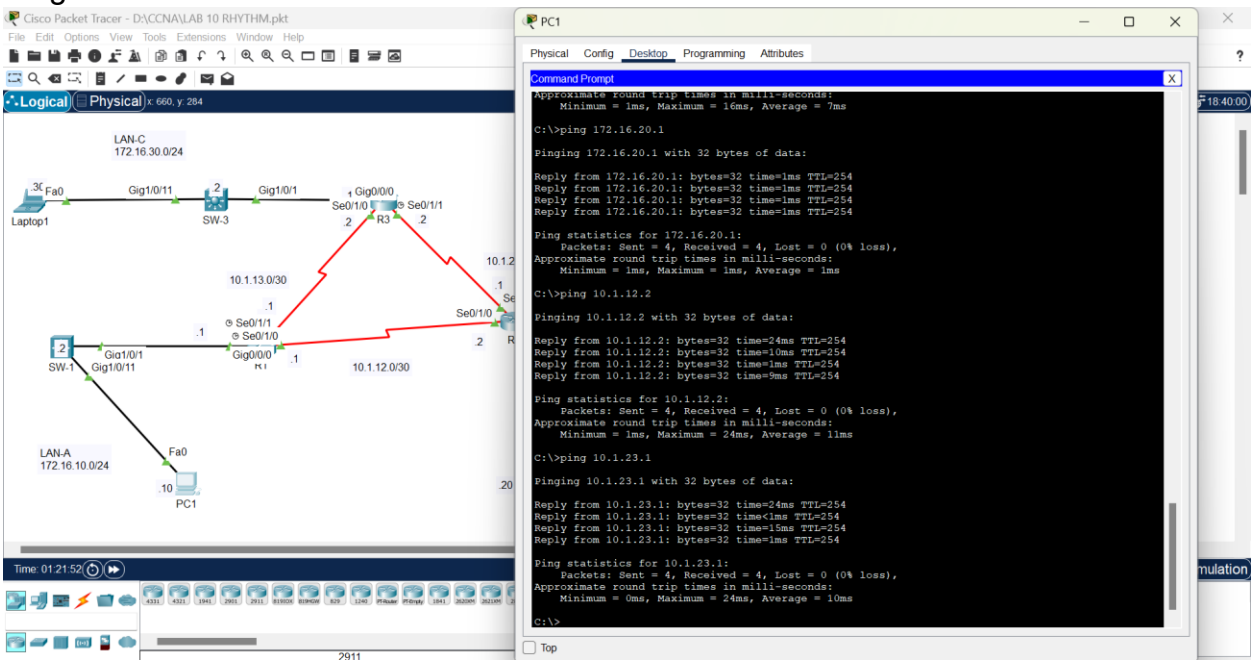
- Ping to SVI of S1 from PC2.
- Ping to SVI of S2 from PC2.
- Ping to SVI of S3 from PC2.



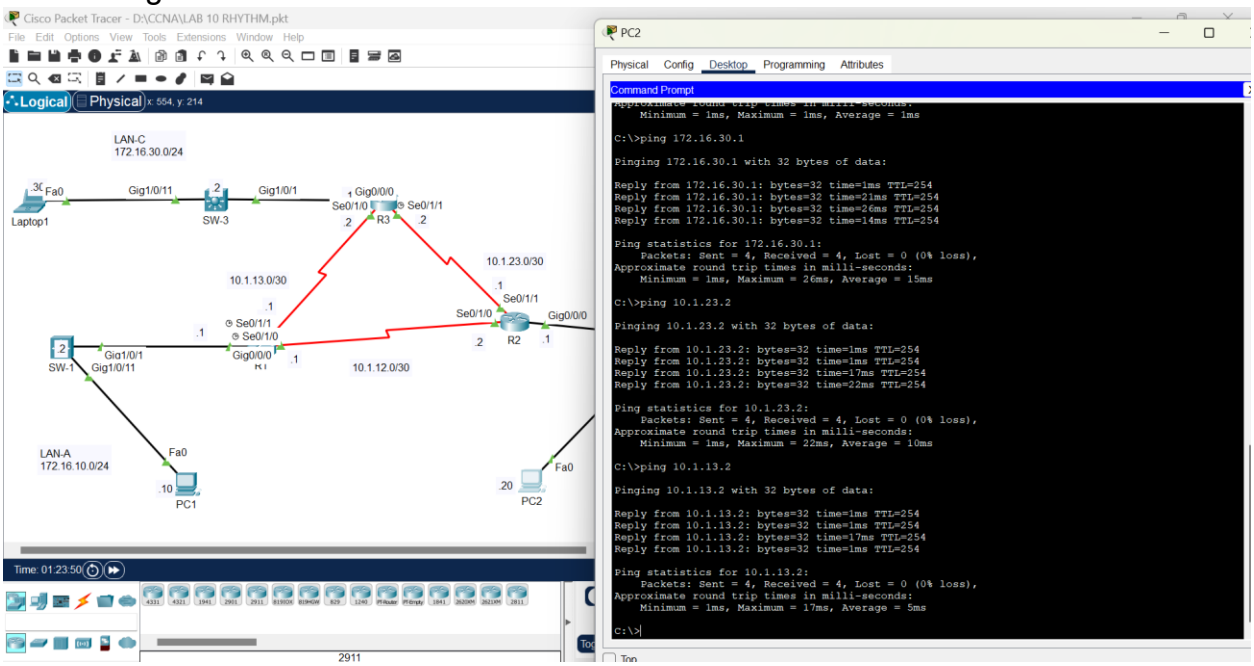
- Ping to G0/0/0 interface of R1 from Laptop1.
- Ping to S0/1/0 interface of R1 from Laptop1.
- Ping to S0/1/1 interface of R1 from Laptop1.



- Ping to G0/0/0 interface of R2 from PC1.
- Ping to S0/1/0 interface of R2 from PC1.
- Ping to s0/1/1 interface of R2 from PC1.



- Ping to G0/0/0 interface of R3 from PC2.
- Ping to S0/1/1 interface of R3 from PC2.
- Ping to S0/1/0 interface of R3 from PC2.



NOTE: All the above-mentioned pings must be successful, otherwise troubleshoot and fix the connectivity issues before moving to the next step. It is important to have full connectivity before applying any ACL.

Part 2:

Implement Access Control List:

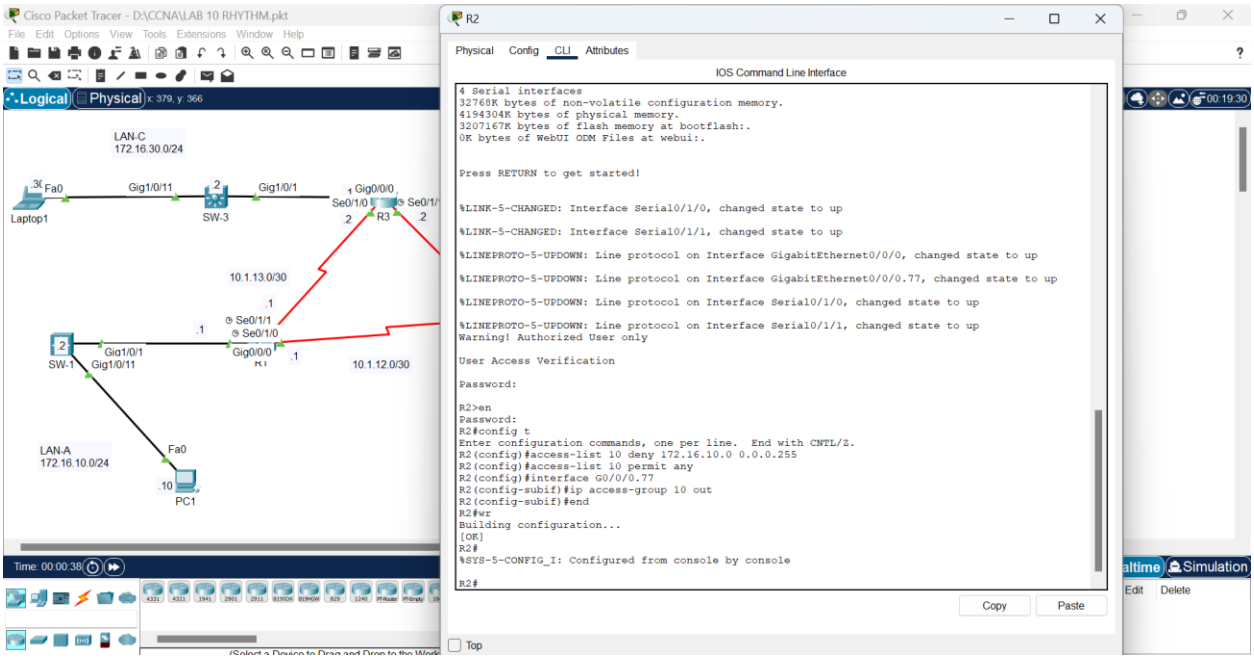
Step 1: Plan and implement the following policies on Router R2 and R3:

- The hosts from LAN-A are not allowed to access PC2 in LAN-B.
- The hosts from LAN-C are not allowed to access PC1 in LAN-A.
- All other traffic is permitted across the entire network as shown in the topology.

Note: The **Standard** ACL is placed as close as possible to the destination of the traffic that is required to be filtered, however the **Extended** ACL is placed as close as possible to the source of the traffic that is required to be filtered.

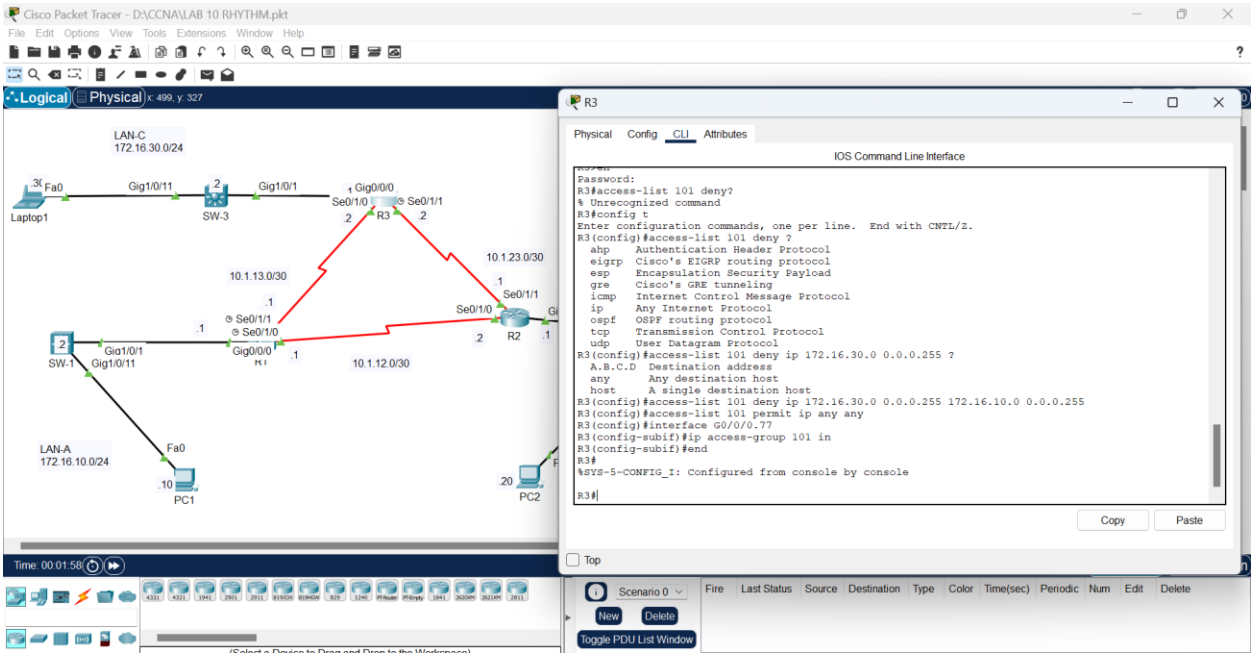
Step 2: Configure and apply the numbered **Standard** ACL on R2.

- Create an ACL using any number from the range of 1 to 99 to filter out the access to PC2 in LAN-B from LAN-A network.
- Permit all other traffic on R2.
- Apply the ACL on router R2 at the appropriate interface and in the appropriate direction.



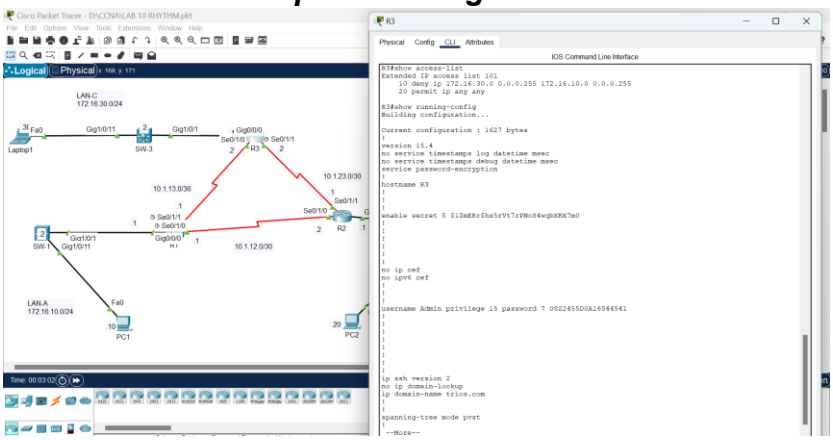
Step 3: Configure and apply **Extended** ACL on R3.

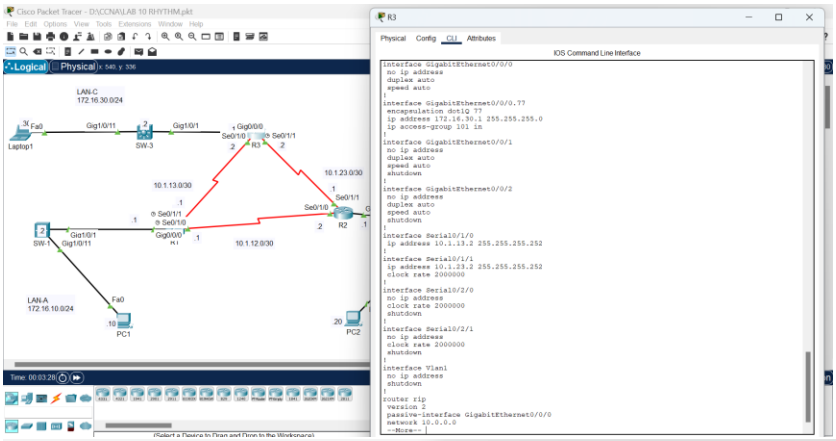
- Create an ACL using any number from the range of 100 to 199 to filter out the access to PC1 in LAN-A from LAN-C network.
- Permit all other traffic on R3.
- Apply the ACL on Router R3 at the appropriate interface and in the appropriate direction.

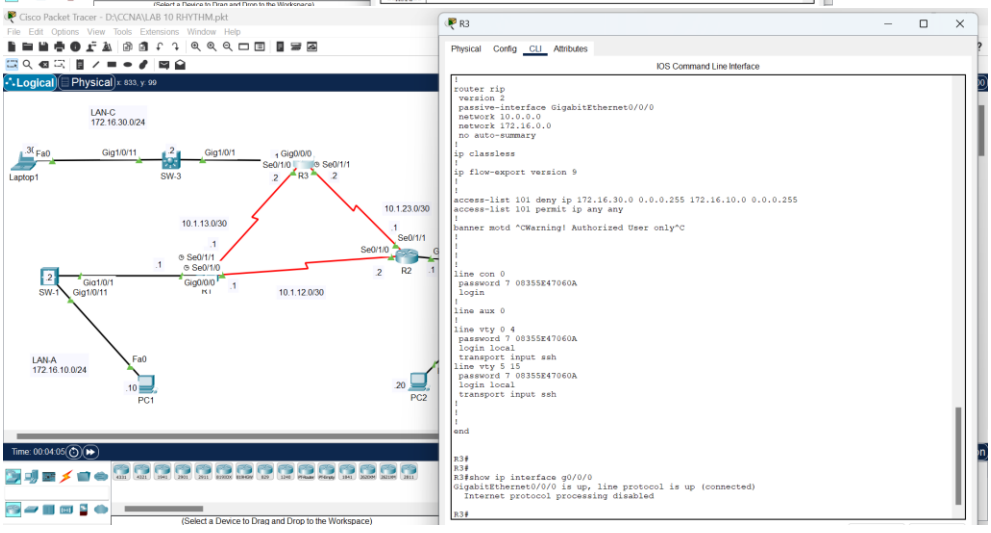


Step 4: Verify ACL configuration as per planning.

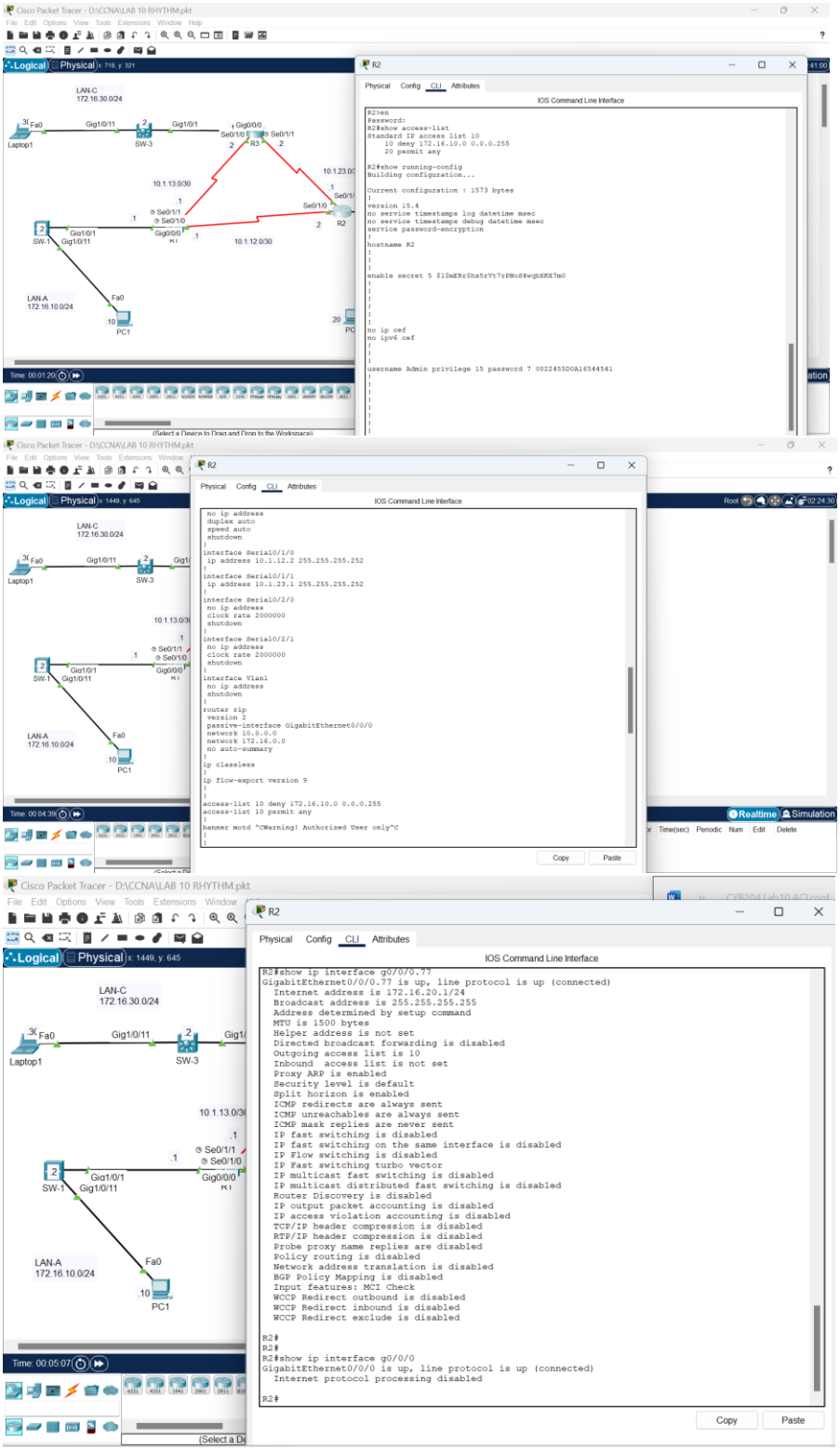
- Use the following commands to verify ACL configuration and placement on R3. For example:
  - ***show access-list***
  - ***show running-config***
  - ***show ip interface g0/0/0***



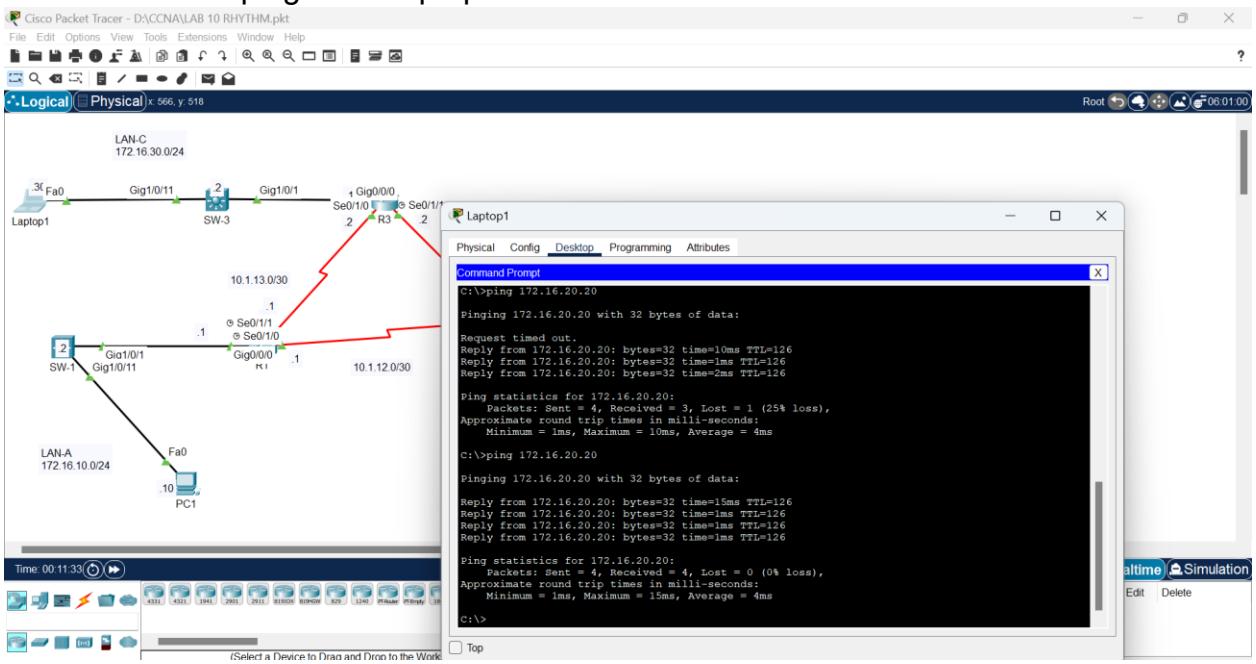




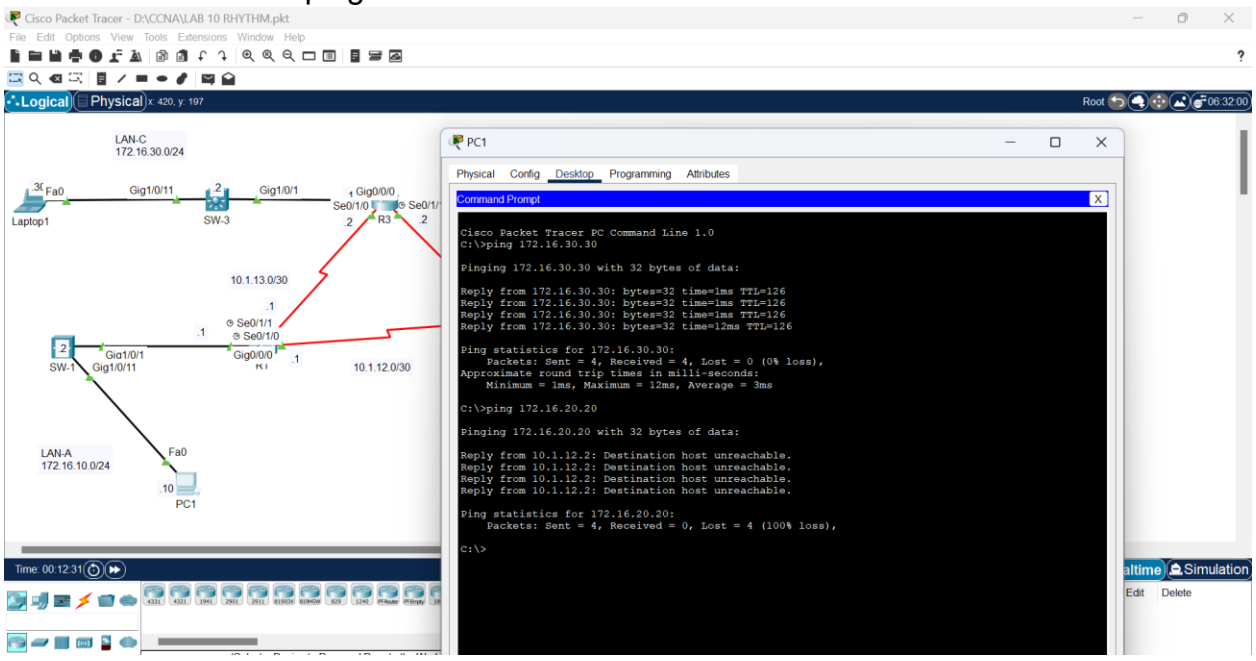
Use similar commands to verify ACL configuration and placement on R2 as well



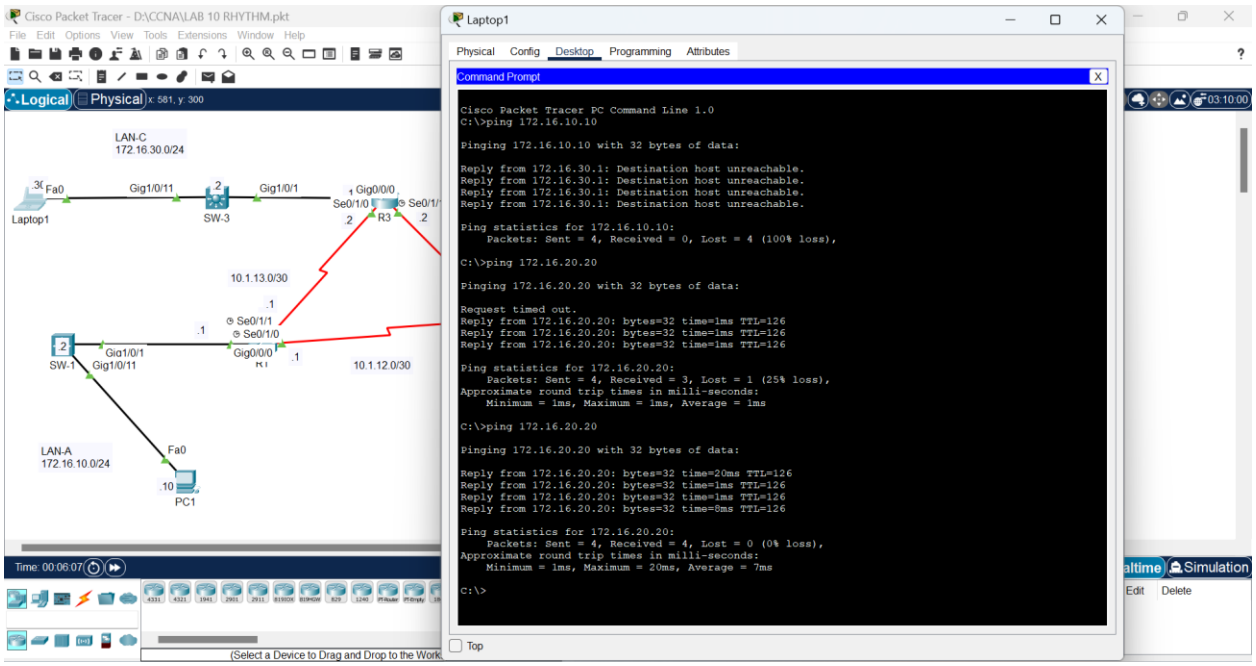
- A successful ping from Laptop1 to PC2 in LAN-B network.



- A successful ping from PC1 to Laptop1 in LAN-C network.
- An un-successful ping from PC1 to PC2 in LAN-B network.



- An un-successful ping from Laptop1 to PC1 in LAN-A network.
- A successful ping from PC-2 to Laptop1 in LAN-C network.



Question:

(a) If PC-2 tries to ping to PC-1, will it be successful or not? Provide the appropriate reason to support your answer.

Answer: it will be successful because there is no ACL configuration on R2 to black the traffic between LAN B and LAN A.

(b) If PC-1 tries to ping to Laptop1, will it be successful, or not? Provide the appropriate reason to support your answer.

ANSWER: PC-1 will be unsuccessful in pinging Laptop1. This is because an extended ACL has been configured on Router R3 to deny traffic from LAN-C.