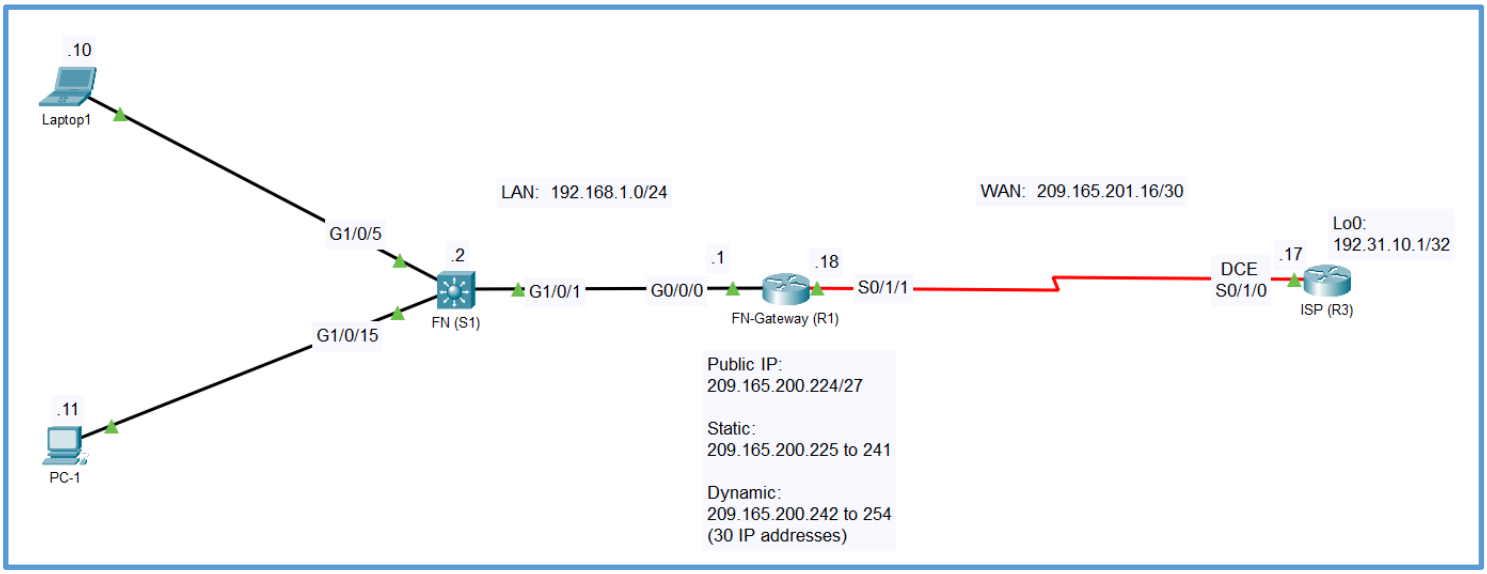
PART –1

Lab Activity – Static and Dynamic NAT Configuration:

- There is one LAN and WAN in the topology below. Please develop the following topology on the physical pod/rack in the lab room.



Required Resources:

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

Addressing Table:

Device	Interface	IP Address	Subnet Mask / CIDR	Default Gateway
FN-S1	VLAN 55	192.168.1.2	255.255.255.0	192.168.1.1
FN-Gateway	G0/0/0	192.168.1.1	255.255.255.0	N/A
	S0/1/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/1/0	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.10.1	255.255.255.255	N/A
Laptop1	N.I.C.	192.168.1.10	255.255.255.0	192.168.1.1
PC-1	N.I.C.	192.168.1.11	255.255.255.0	192.168.1.1

Lab Description:

- In this lab, please build a LAN and WAN based simple network.
    - LAN with one switch and two hosts
    - Site-to-site WAN with two routers

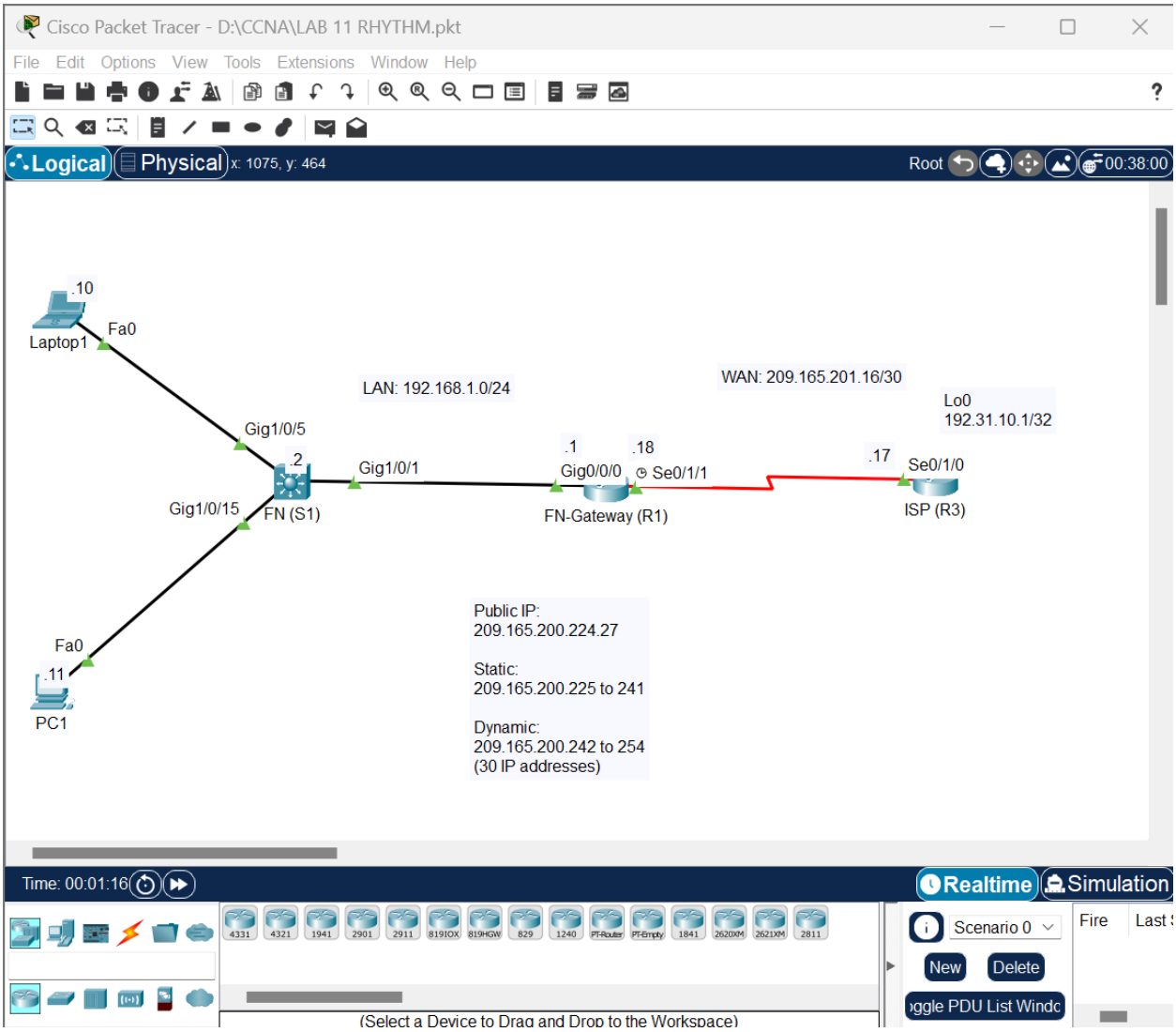
For this lab consideration, the ISP has allotted 30 public IP addresses to the company from the address space of 209.165.200.224/27. The first 17 addresses are for static NAT from 209.165.200.225 to 241, and the remaining 13 addresses are for dynamic NAT from 209.165.200.242 to 254.

- You are also required to do the basic configuration on the following devices:
    - Switch:
        - Hostnames
        - SVI
        - Default gateway
        - Login banner
        - DNS lookup (disable)
    - Routers:
        - Hostnames
        - IP addressing
        - Login banner
        - DNS lookup (disable)
    - PC and Laptop:
        - IP address, subnet mask, default gateway

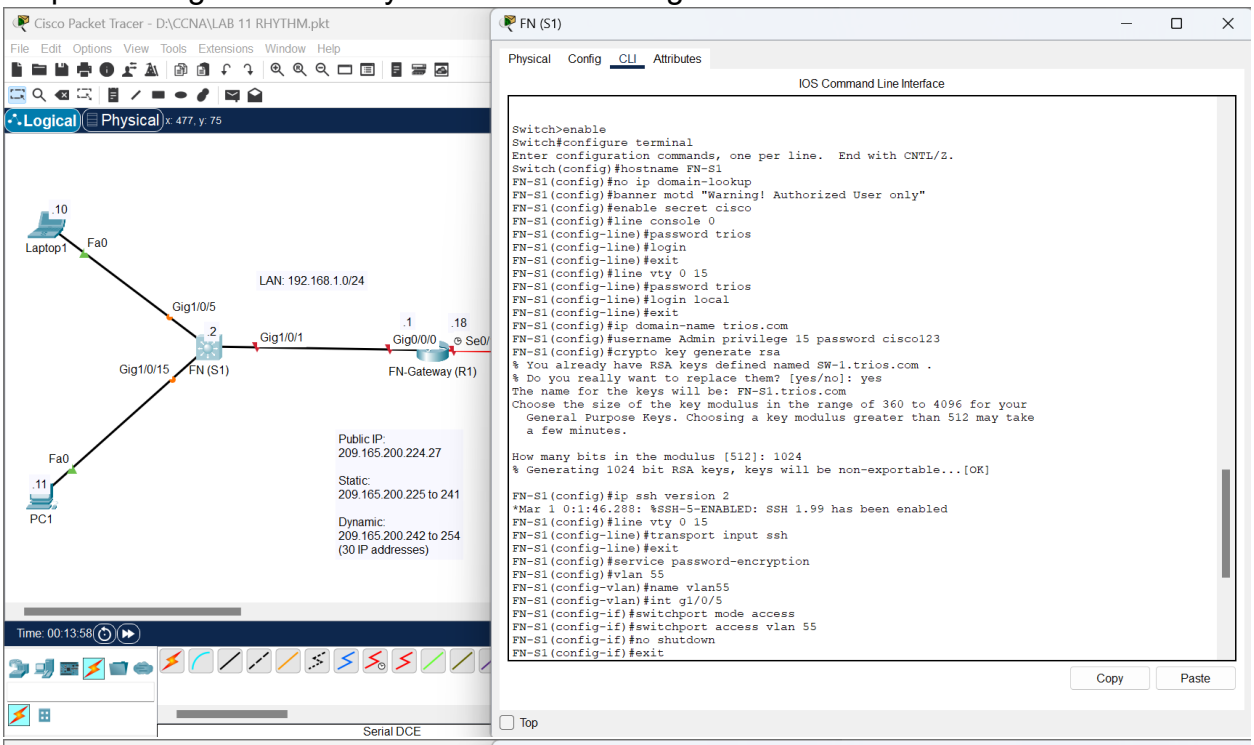
Solution

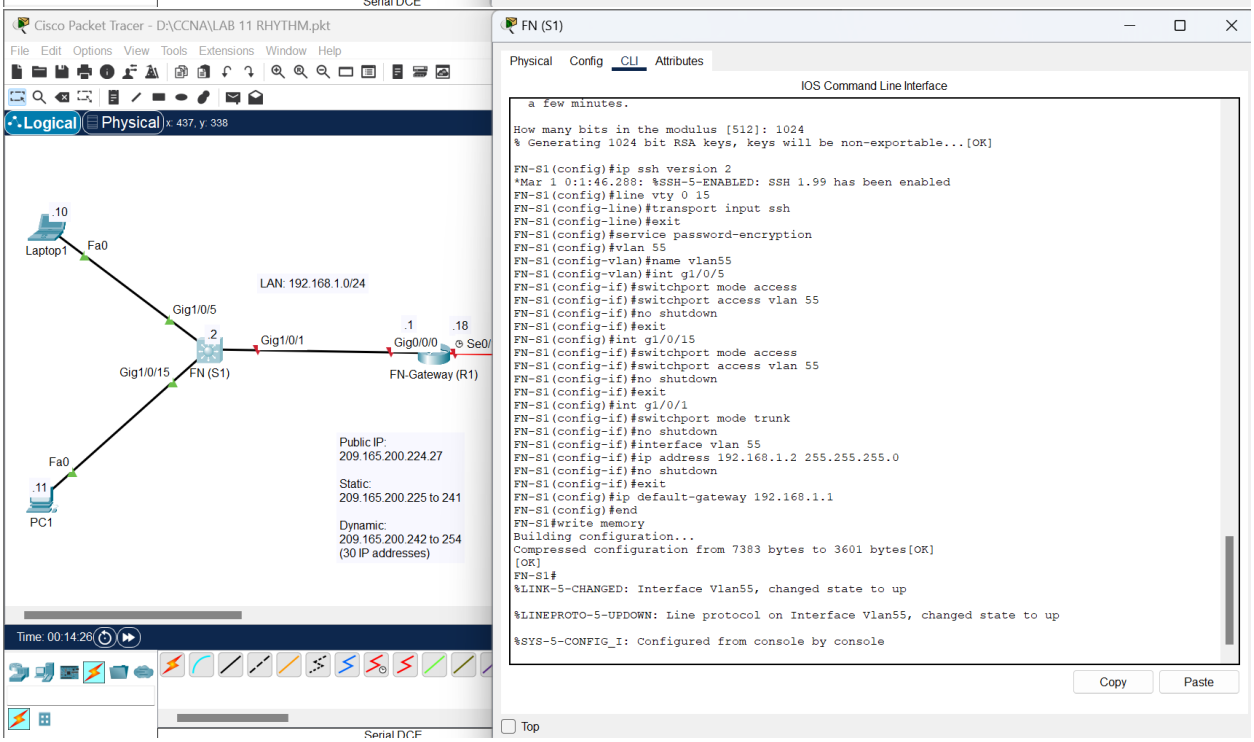
Step 1: Set up the network topology.

- Develop the topology by using all the physical devices mentioned above and cable them all together:
  - Turn on the devices.
  - Connect the switch with the default gateway.
  - Connect the PCs and laptop with their respective switches.
  - Make sure all the link/port lights between switches, PCs, and laptops are active/enabled.



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



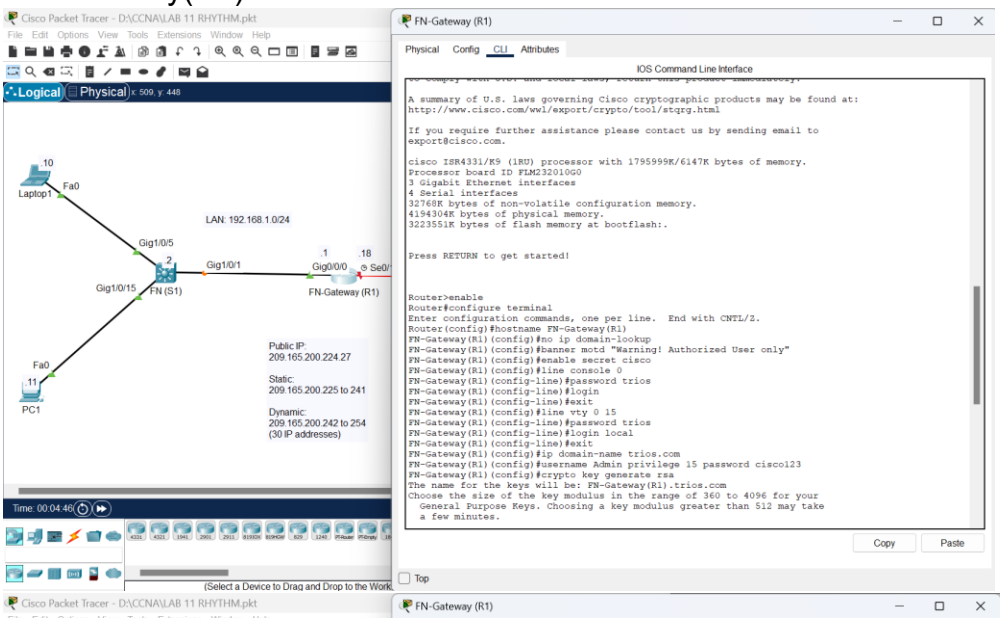


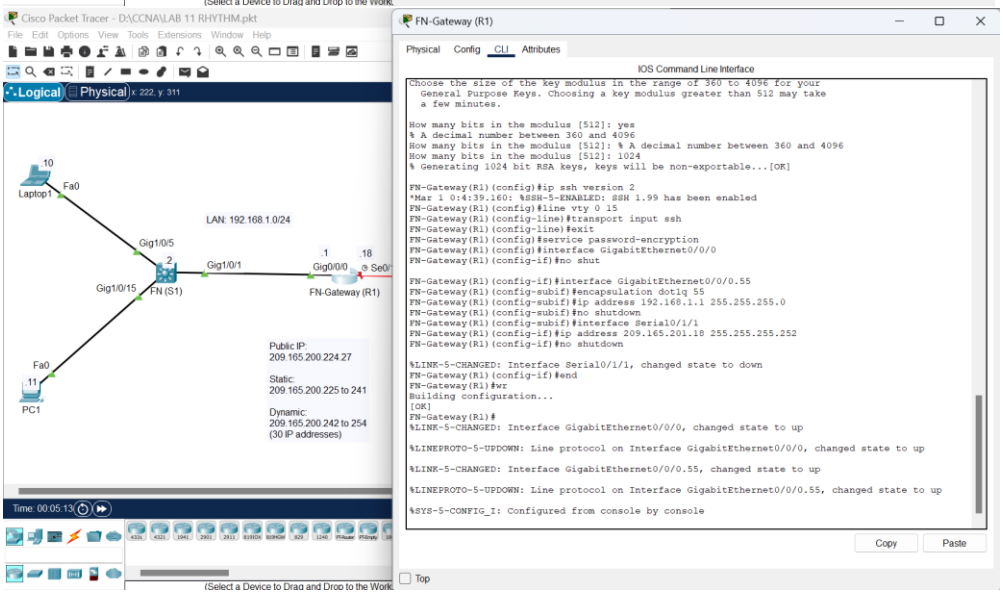
- Console into the switch and enter the global configuration mode:
  - Assign the switch with a host name according to the Addressing Table.
  - Disable unwanted DNS lookup.
  - Configure a login MOTD banner to warn about illegal access.
  - Assign the encrypted password cisco to privilege exec mode (#).

- Protect the physical and virtual lines from having console access.
- Configure username to access SSH client access as Admin and password as cisco.
- 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.

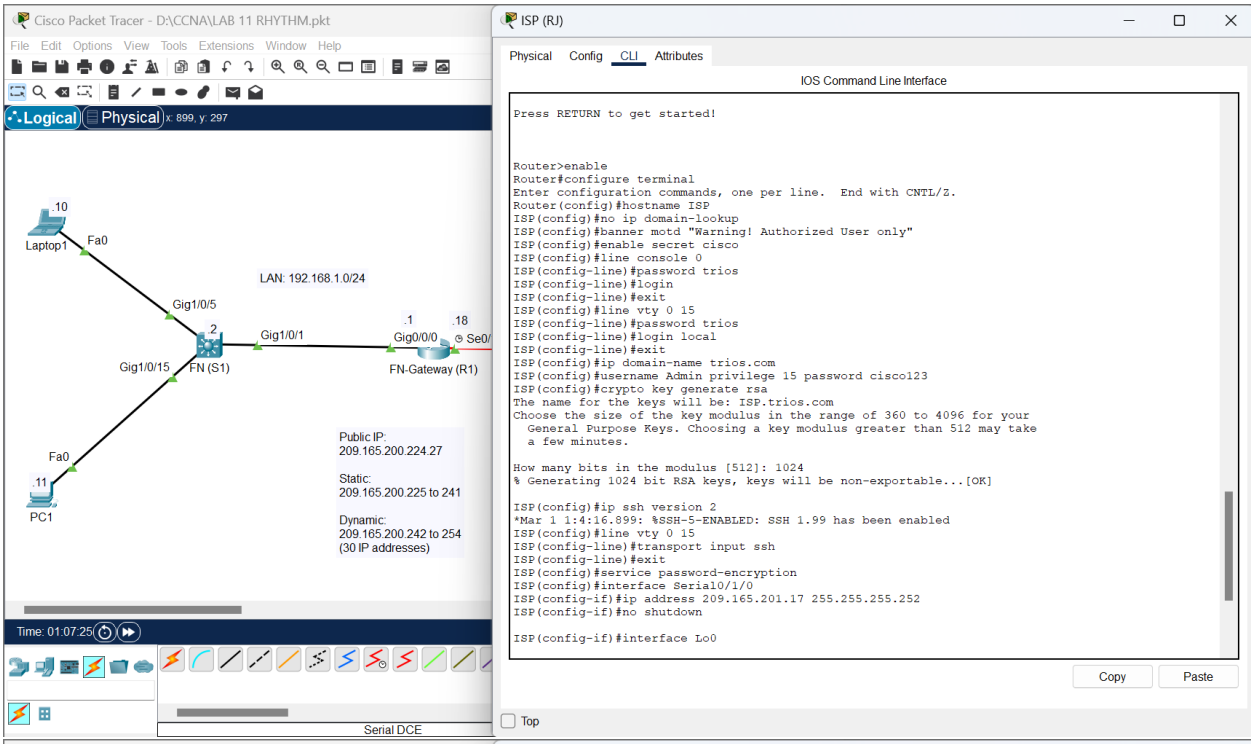
Step 3: Configure and verify basic router settings on all routers.

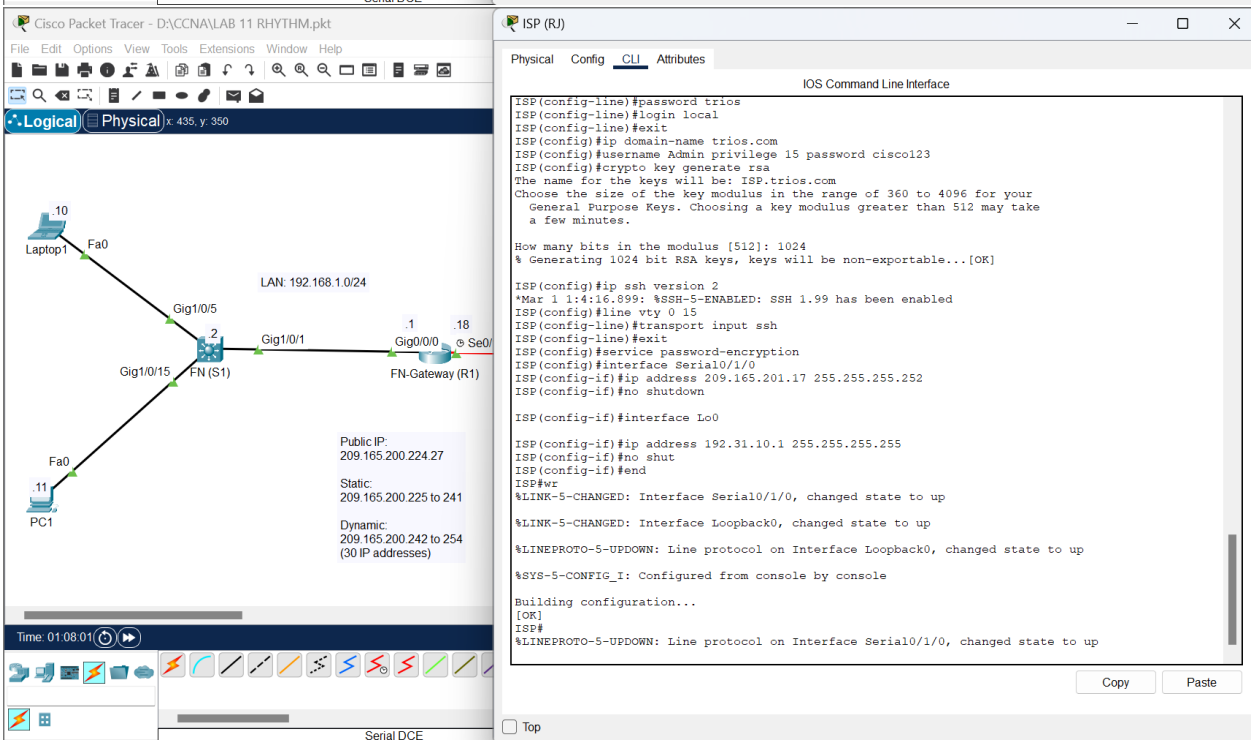
FN-Gateway(R1)





ISP



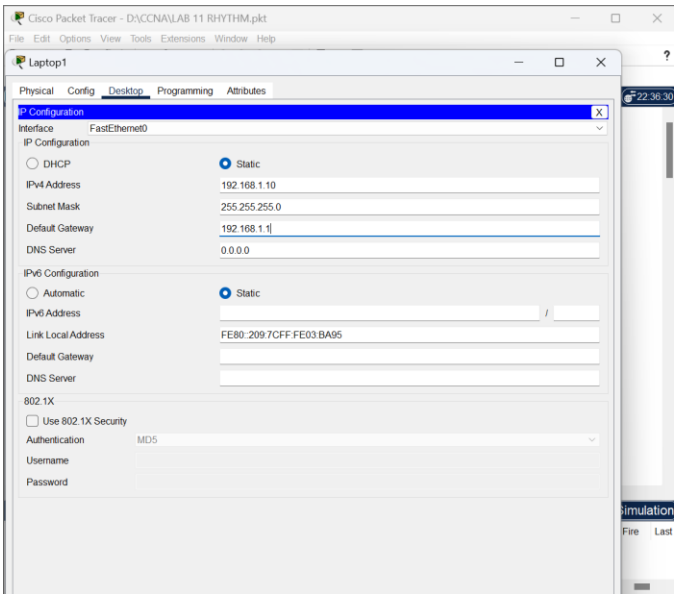


- Console into the router and enter the global configuration mode:
  - Assign the routers with host names according to the addressing table.
  - Disable unwanted DNS lookup.
  - Configure a login MOTD banner to warn about illegal access.

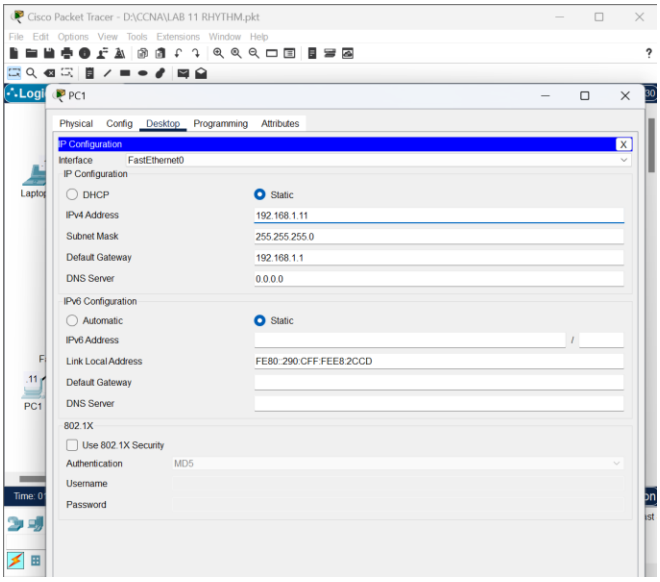
- Assign the encrypted password cisco to privilege exec mode (#).
- Protect the physical and virtual lines from having console access.
- Configure username to access SSH client access as Admin and password as cisco.
- Encrypt all current and future passwords by enabling the required service.
- Configure and activate all the interfaces according to the addressing table.
- Provide appropriate descriptions on all the active interfaces.
- Save the configuration.

Step 4: Configure the PC and laptop hosts as per the addressing table.

Laptop 1

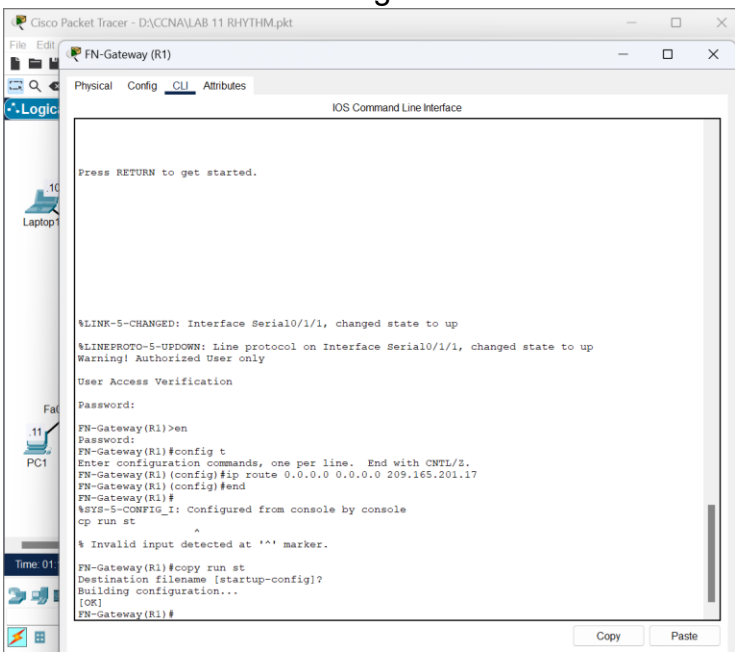


PC 1

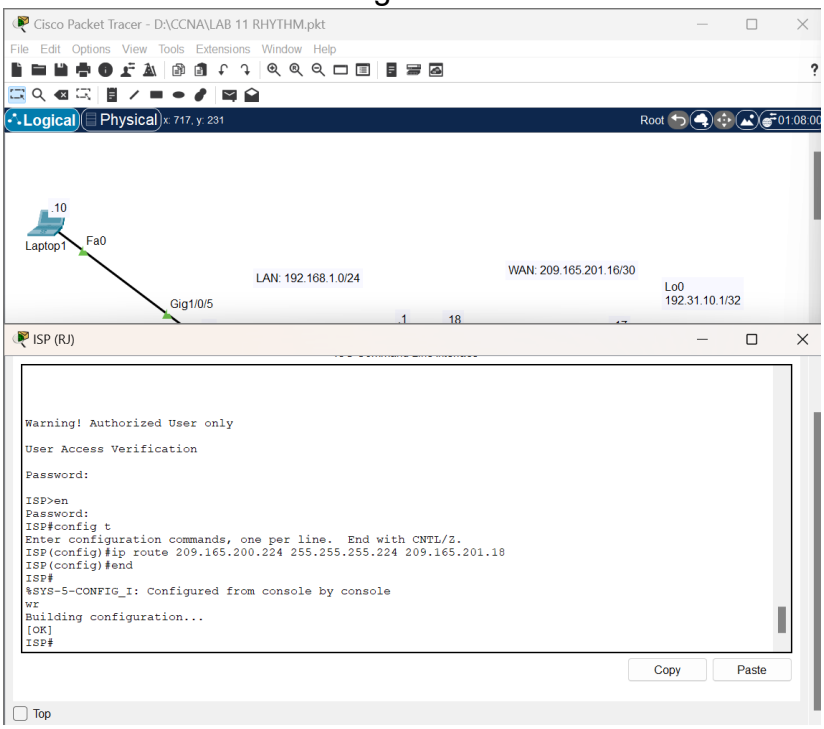


Step 5: Configure static routing on both routers as below:

- FN-Gateway router:
  - Configure the default route from the FN-Gateway router to the ISP router.
  - Save the configuration.

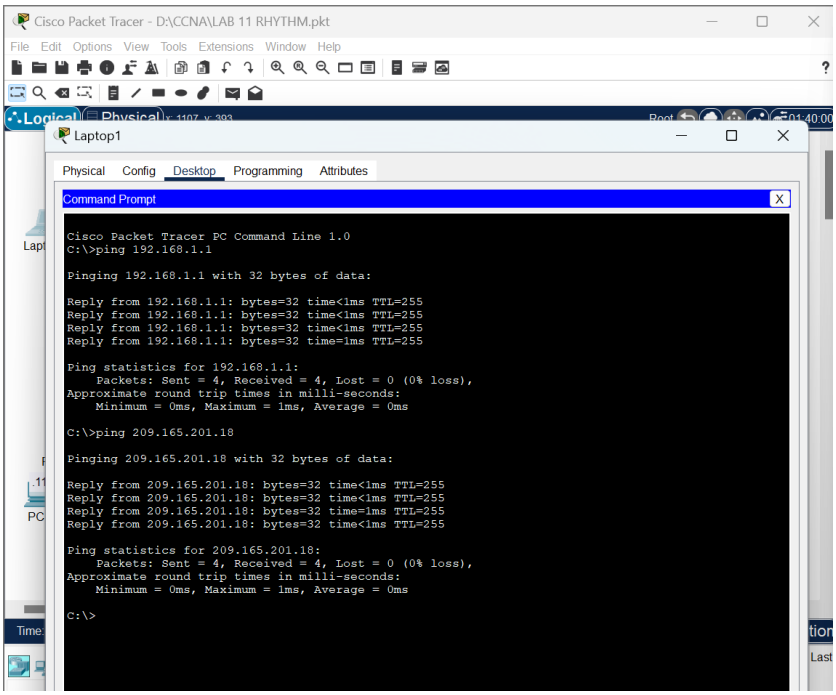


- ISP router:
  - Configure the static route from the ISP router to the allotted Public Address Range 209.165.200.224/27 of FN-Gateway router.
  - Save the configuration.

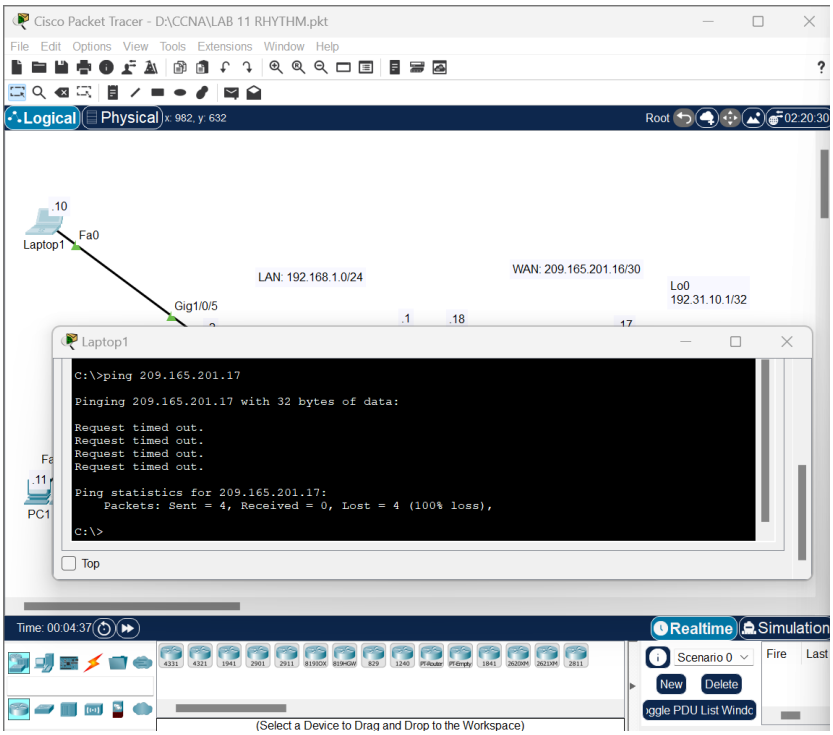


Step 6: Verification:

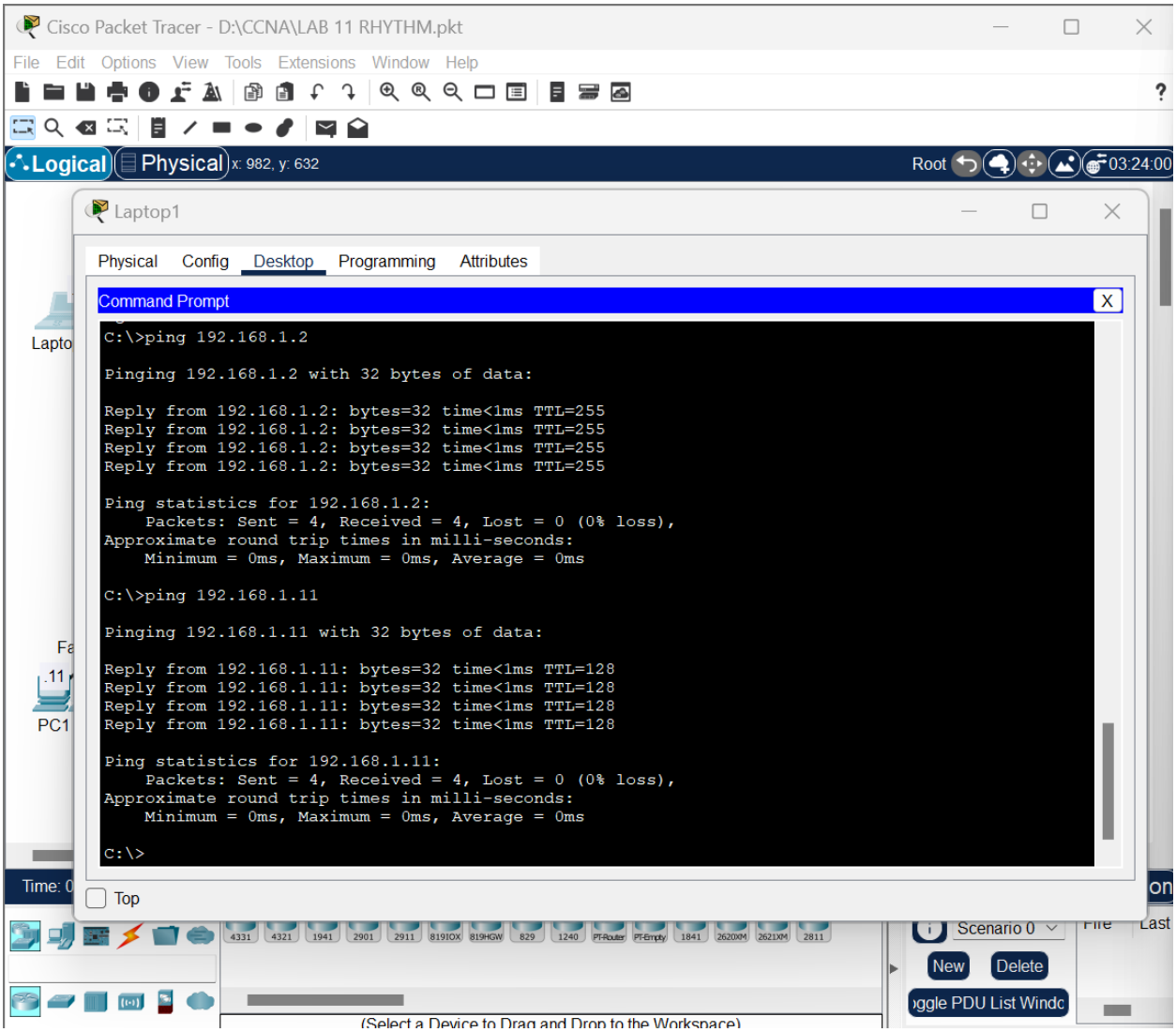
- Using the command line at Laptop1, ping the IP addresses of:
  - G0/0/0 and S0/1/1 interfaces of FN-Gateway router (R1).



  - S0/1/0 interface of the ISP router (R3).

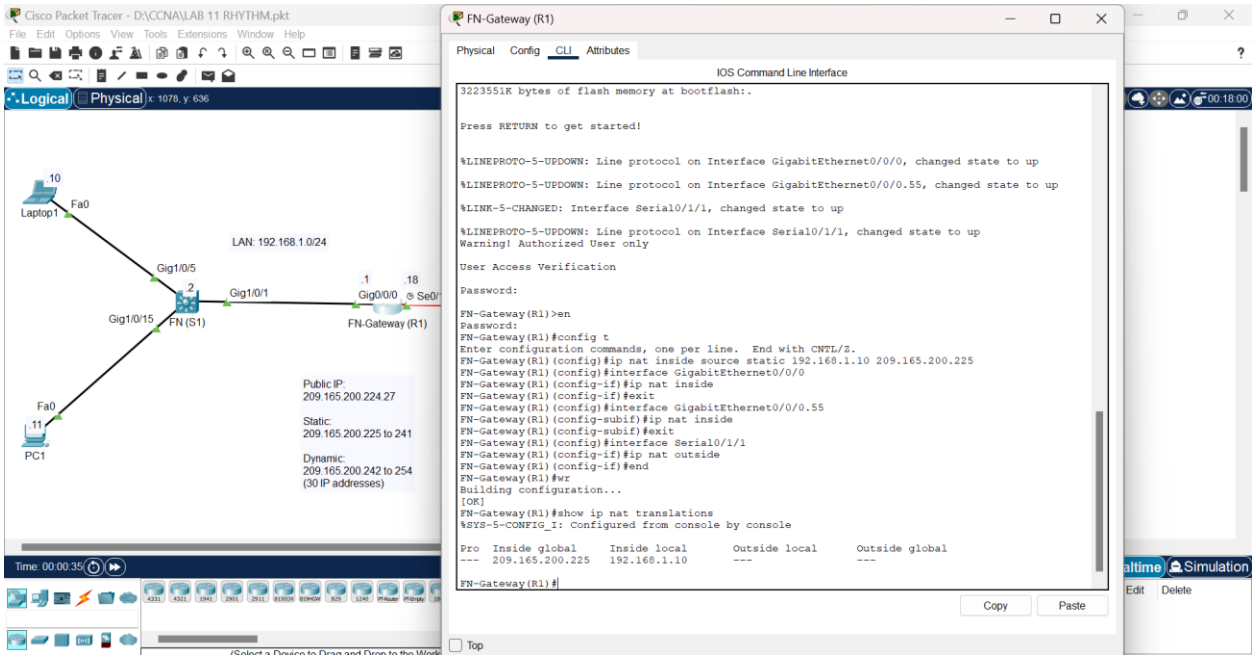


- Virtual Interface VLAN 55 of switch FN (S1).
- PC-A.

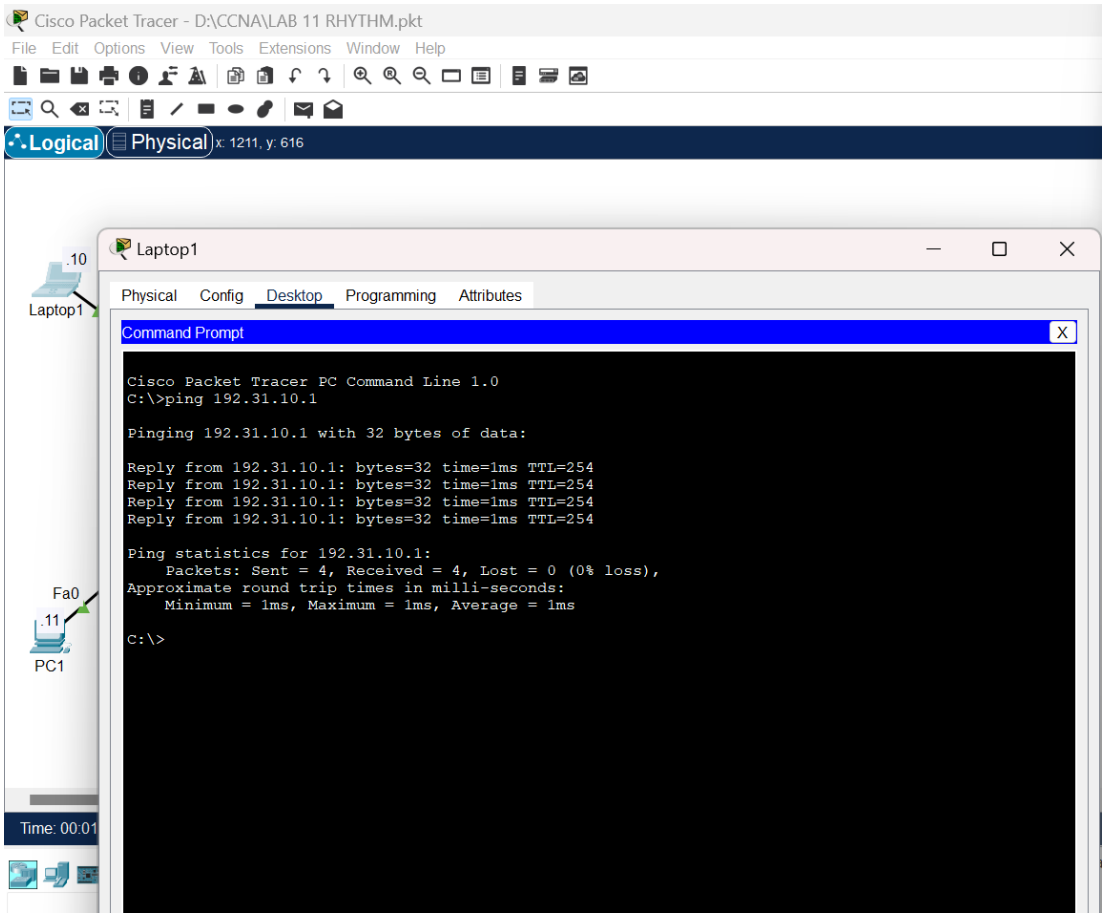


Step 7: Configure static NAT on the FN-Gateway router.

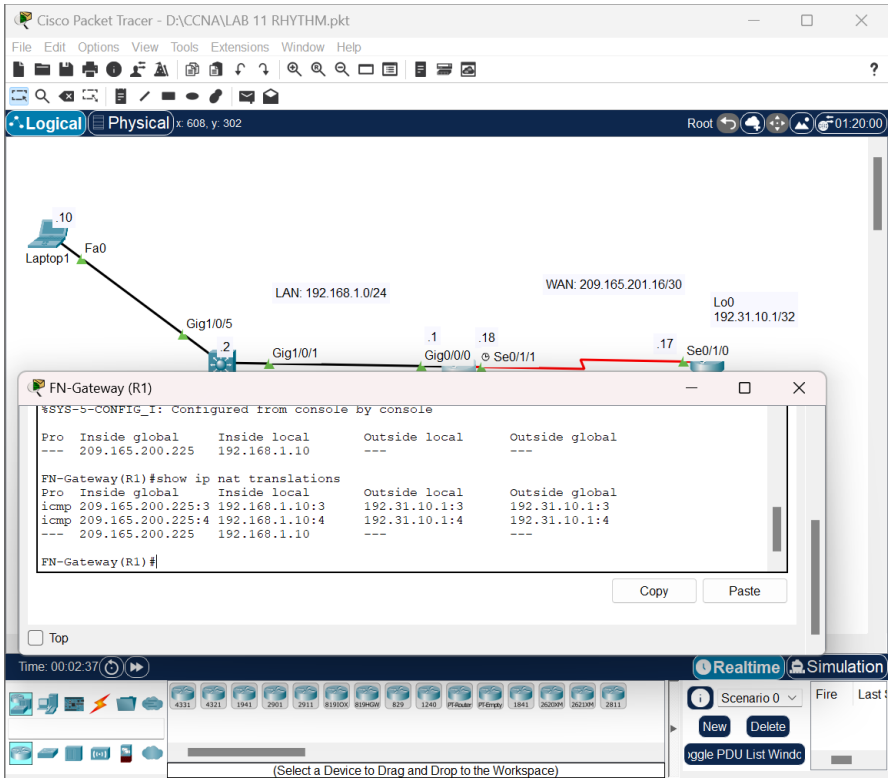
- Configure the FN-Gateway router to translate between the private inside Laptop1 address and the public address of 209.165.200.225.
- Configure the FN-Gateway router interfaces for inside and outside translation appropriately. (Hint: The interface facing/going towards the internet is usually configured as “ip nat outside”.).
- Show “ip nat translations” on Gateway router (inside global and inside local addresses should be visible).



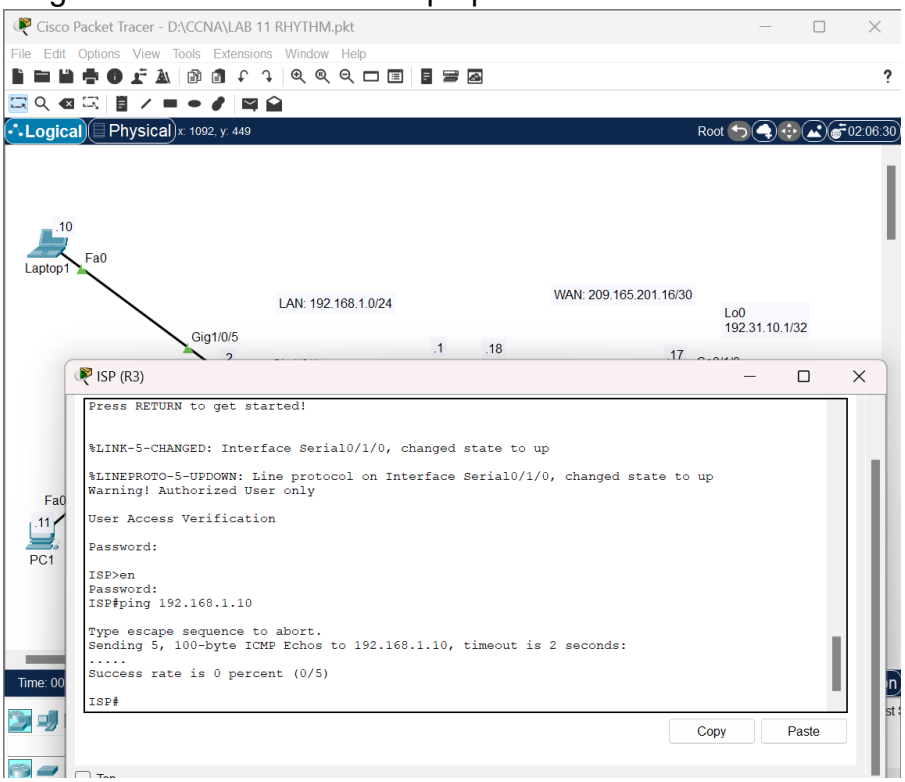
- Ping the Lo0 interface of the ISP router from Laptop1.



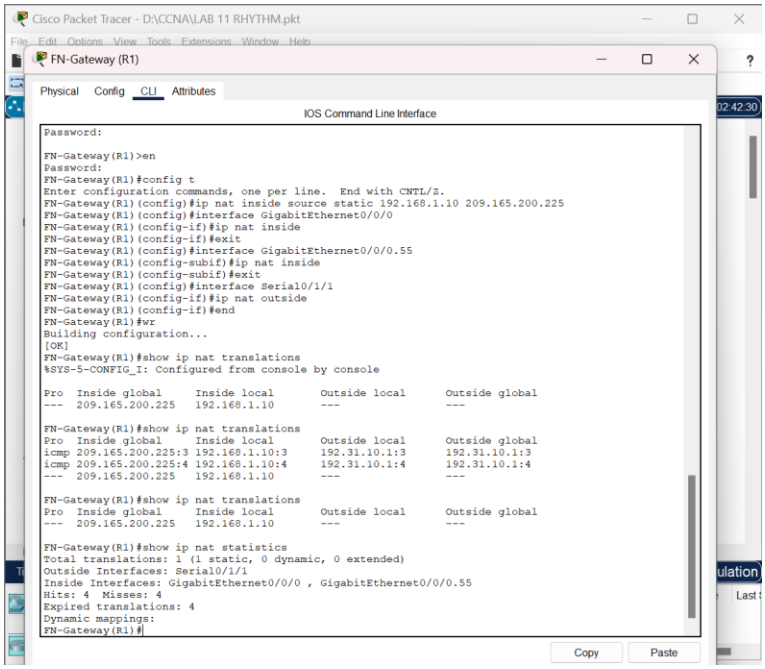
- “Show ip nat translations” on Gateway router (inside global, inside local, outside local, outside global).



- Ping from the ISP router to Laptop1.

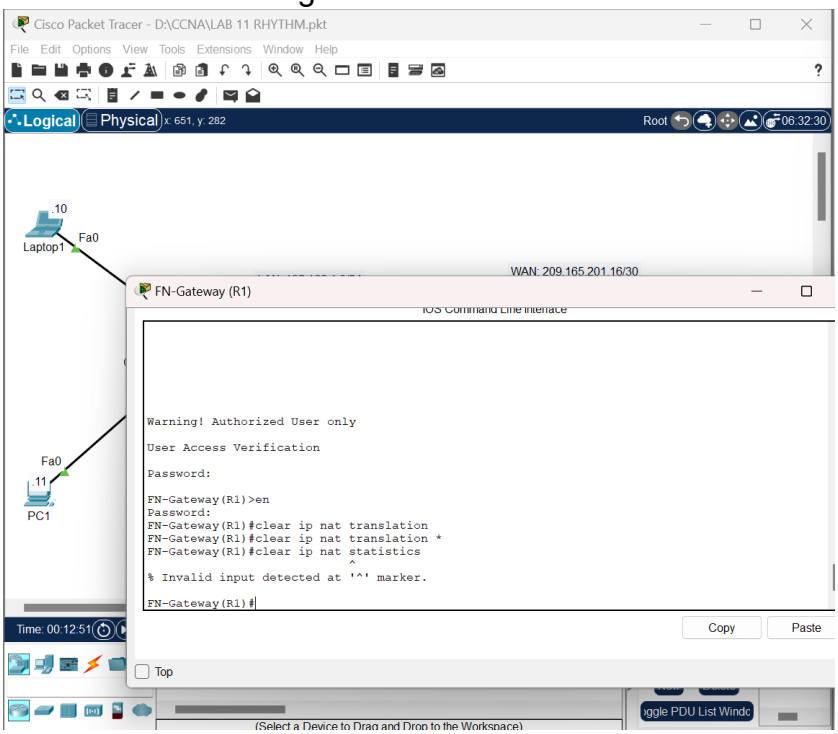


- “Show ip nat translations” (on Gateway router)
- “Show ip nat statistics”

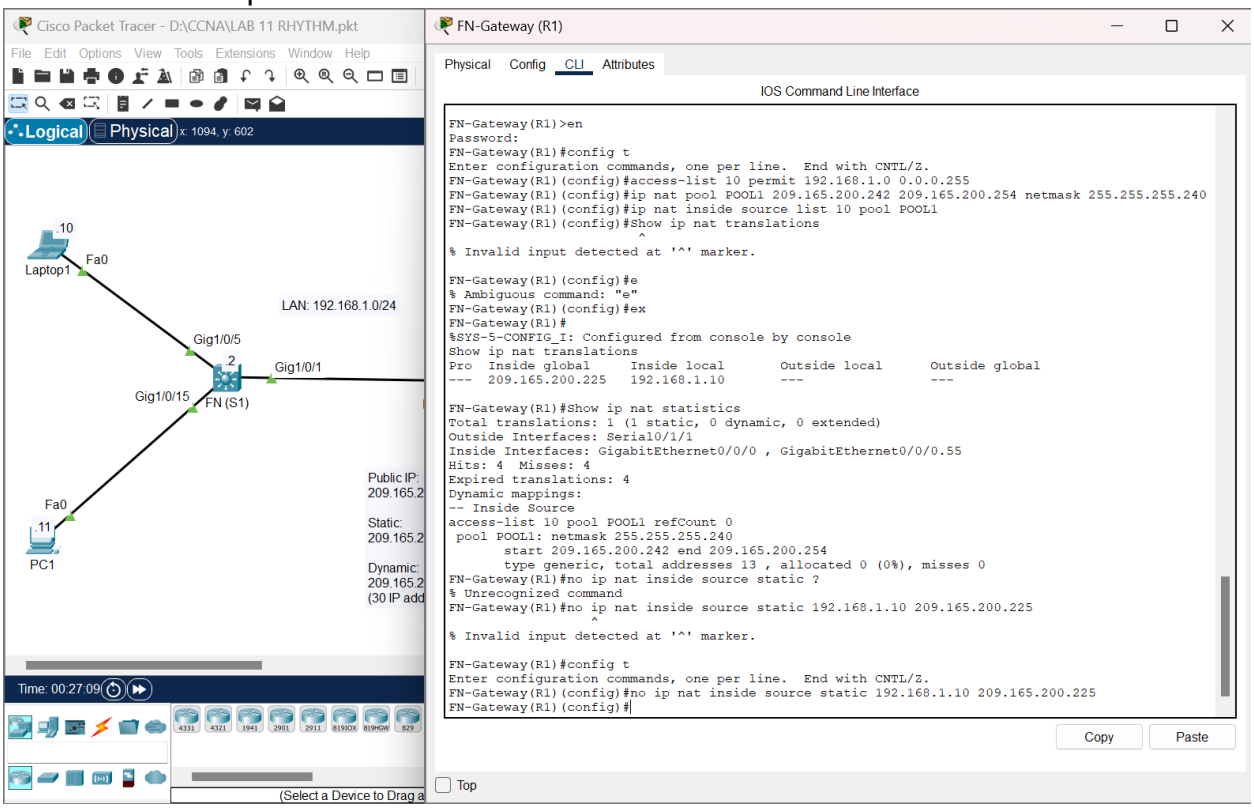


Step 8: Configure dynamic NAT on FN-Gateway router:

- Clear previous NAT translations and statistics.
    - clear ip nat translation *
    - clear ip nat statistics – it depends on routers so clear ip nat translations * is enough

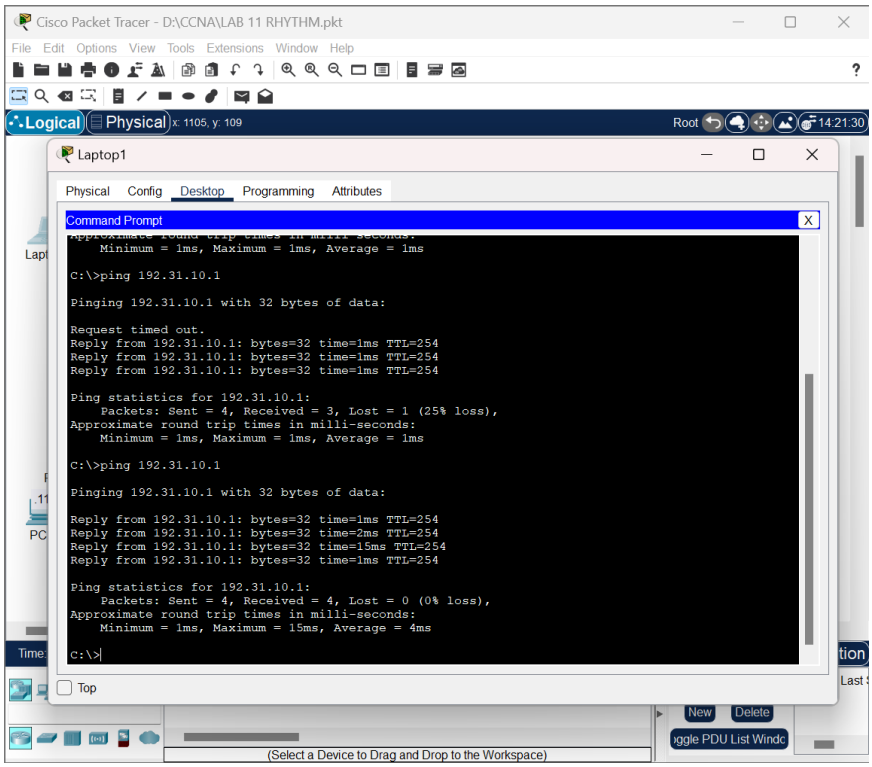


- Define a standard ACL that matches the LAN private IP address range.
- ACL 10 is allowing 192.168.1.0/24 network to be translated.
- Define the pool of usable public IP addresses.
- As per the give routing
- ip nat pool POOL1 209.165.200.242 209.165.200.254 netmask 255.255.255.240
  Define the NAT from the inside source list to the outside pool:
    - ip nat inside source list 10 pool POOL1
- Show ip nat translations on FN-Gateway router.
- Show ip nat statistics on FN-Gateway router.
- Remove the static NAT entry.
    - no ip nat inside source static 192.168.1.10 209.165.200.225

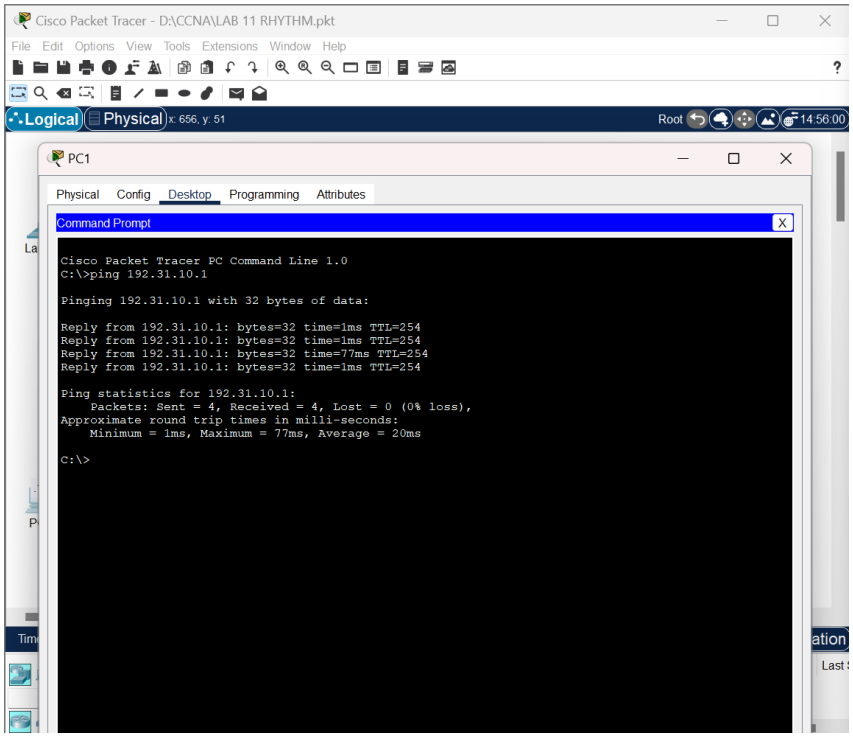


Step 9: Verify the connectivity.

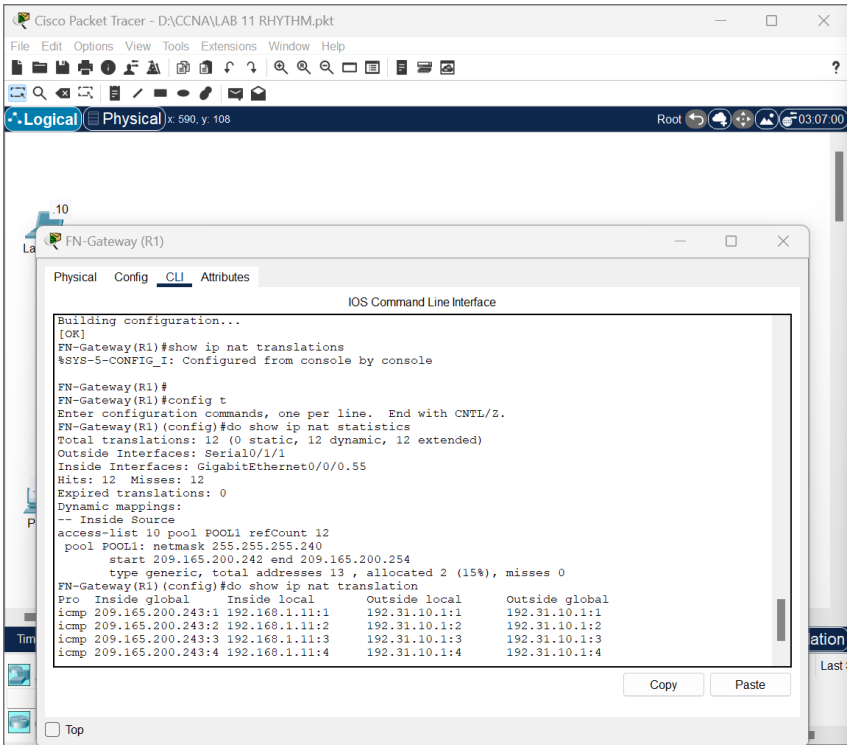
- Using the command line at Laptop1, ping the Lo0 interface of the ISP router.



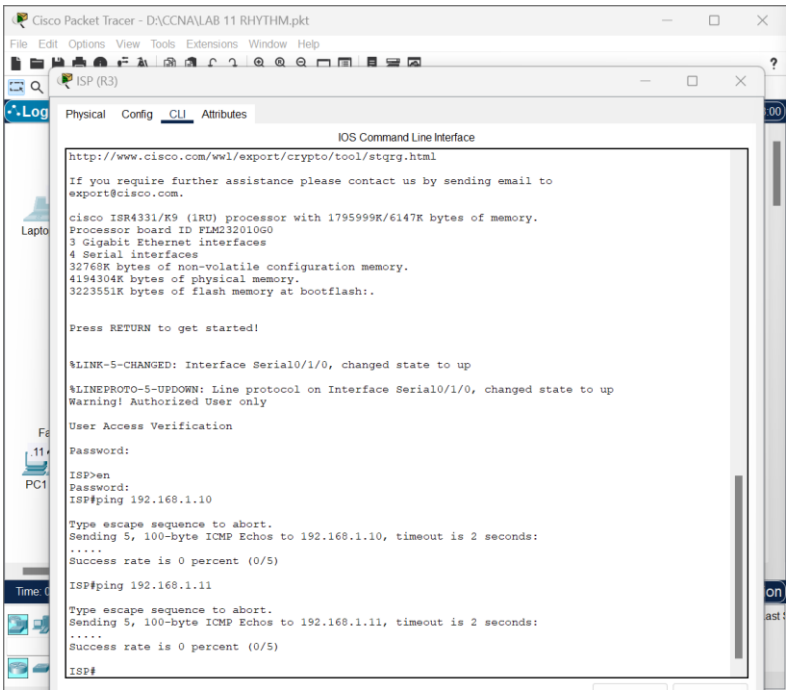
- Using the command line at PC1, ping the Lo0 interface of the ISP router.



- Check and verify the output of the following commands.
  - show ip nat statistics
  - show ip nat translations



- Ping Laptop1 and PC-A from the ISP router

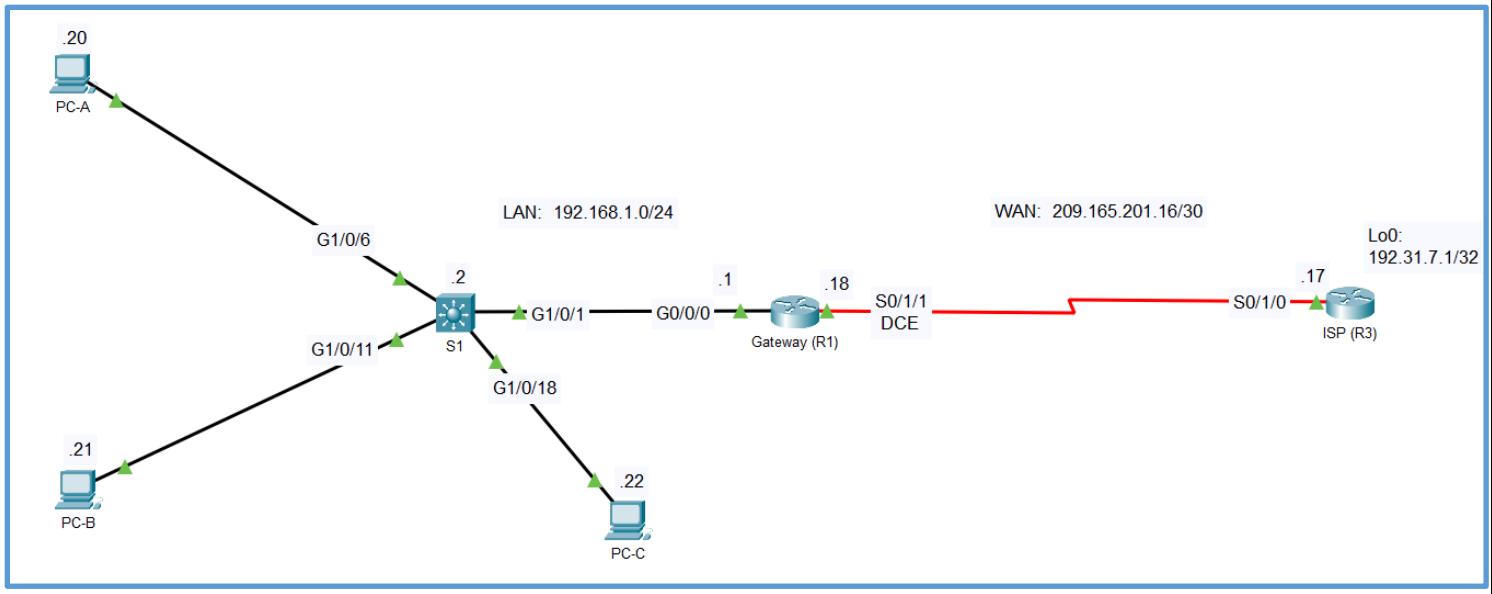


NOTE: All the above-mentioned pings must work, otherwise troubleshoot the network.

Lab 11 – Part 2:

Configuring Port Address Translation (PAT)

Topology:



Addressing Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
Gateway (R1)	G0/0/0	192.168.1.1	255.255.255.0	N/A
	S0/1/1	209.165.201.18	255.255.255.252	N/A
ISP (R3)	S0/1/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.22	255.255.255.0	192.168.1.1

Background / Scenario

Your company is allotted the public IP address range of 209.165.200.224/29 by the ISP. This provides the company with six public IP addresses. Dynamic NAT pool overload uses a pool of IP addresses in a many-to-many relationship. The router uses the first IP address in the pool and assigns connections using the IP address plus a unique port number. After the maximum number of translations for a single IP

address have been reached on the router (platform and hardware specific), it uses the next IP address in the pool. NAT pool overload is a form port address translation (PAT) that overloads a group of public IPv4 addresses.

In Part 2, the ISP has allocated a single IP address, 209.165.201.18, to your company for use on the internet connection from the company Gateway router to the ISP. You will use the PAT to convert multiple internal addresses into one usable public address. You will test, view, and verify that the translations are taking place, and you will interpret the NAT/PAT statistics to monitor the process.

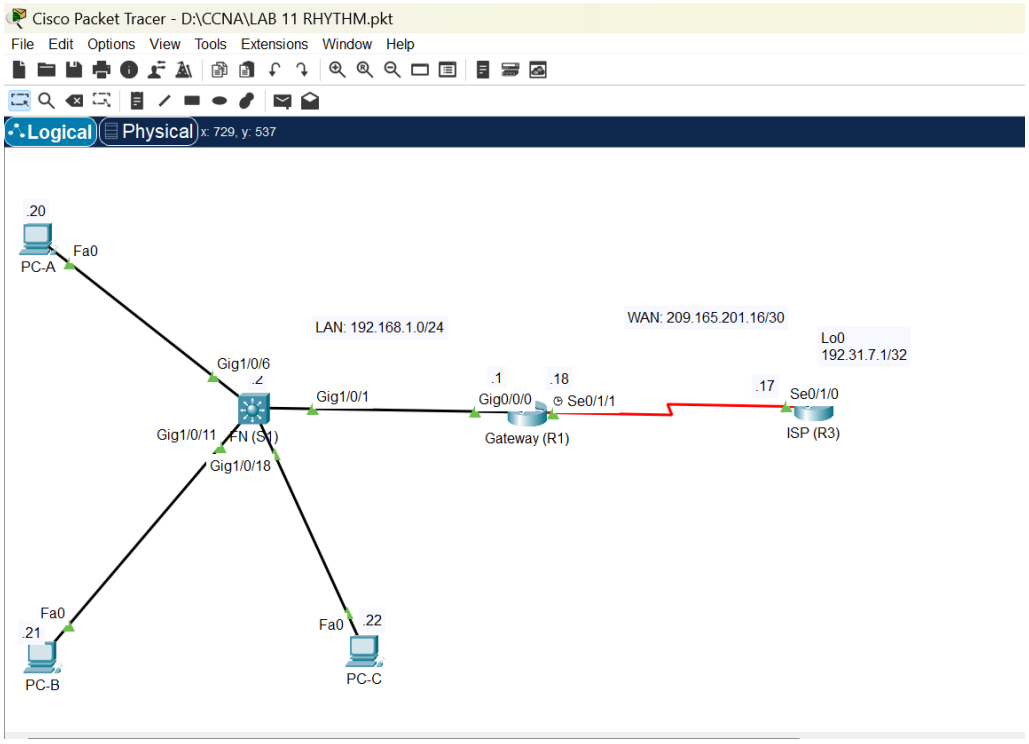
Required Resources:

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

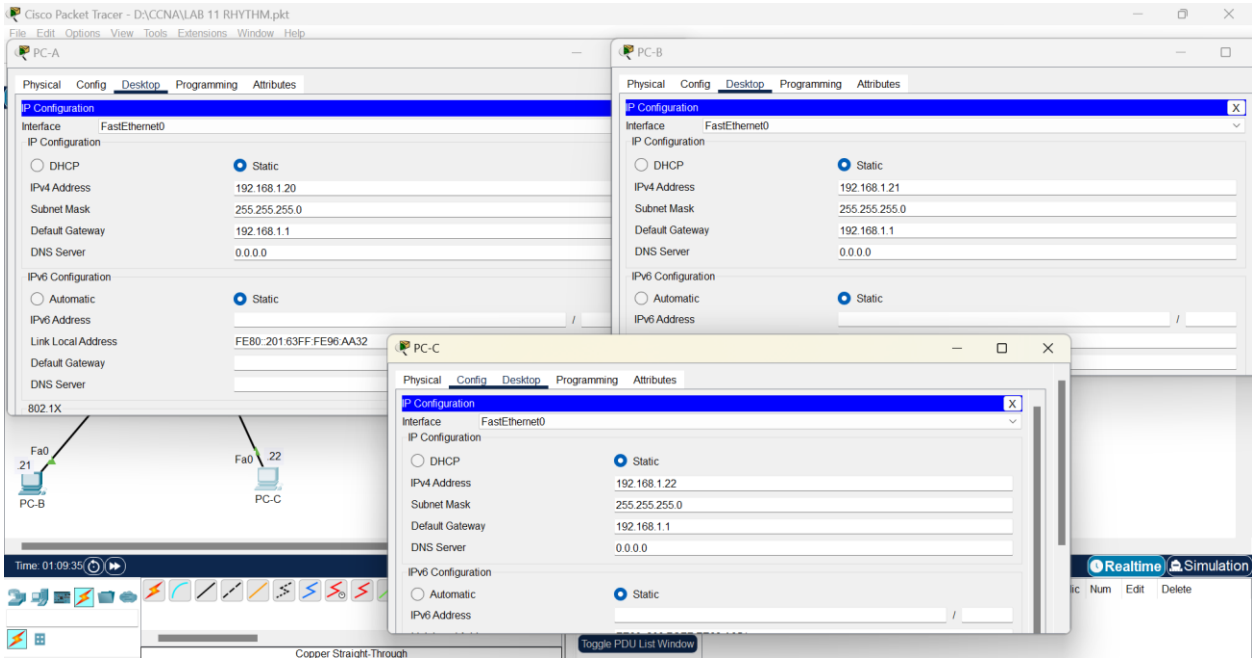
Step 1: Build the Network and Verify Connectivity

In Step 1, you will set up the network topology and configure basic settings such as the interface IP addresses, static routing, device access, and passwords.

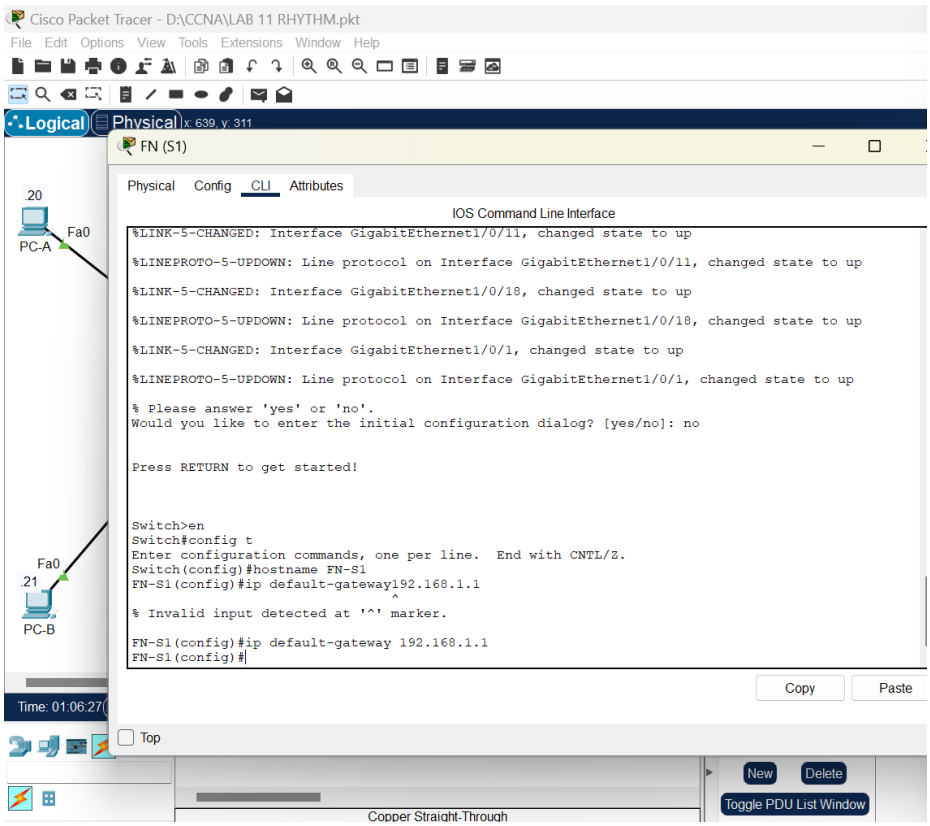
1. Cable the network as shown in the topology.



2. Configure PC hosts.



3. Initialize and reload the routers and switches.



4. Configure basic settings for each router.

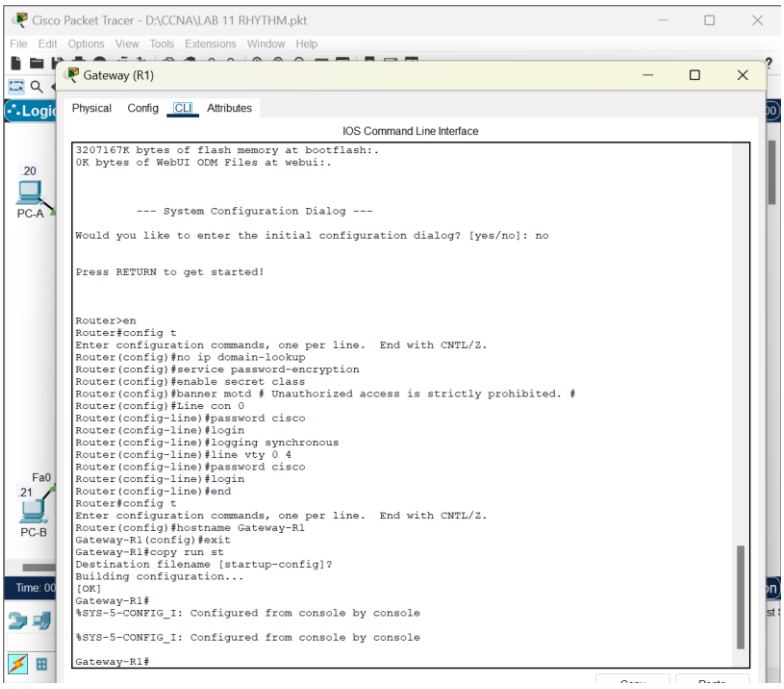
a) Console into the router and enter global configuration mode.

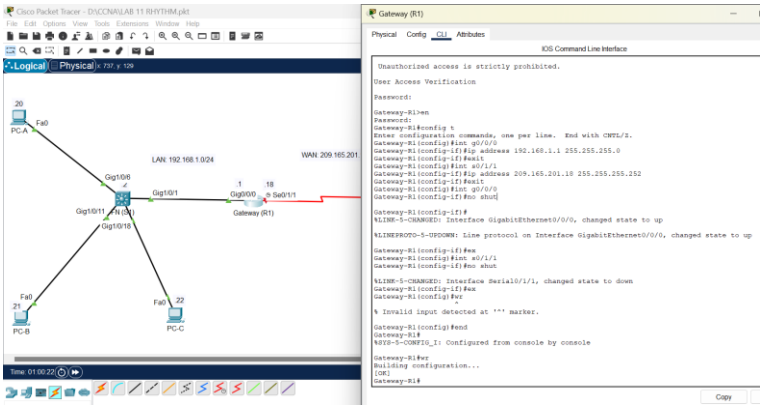
b) Copy the following basic configuration and paste it to the running-configuration on the routers.

no ip domain-lookup
service password-encryption
enable secret class
banner motd # Unauthorized access is strictly prohibited. #
Line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login

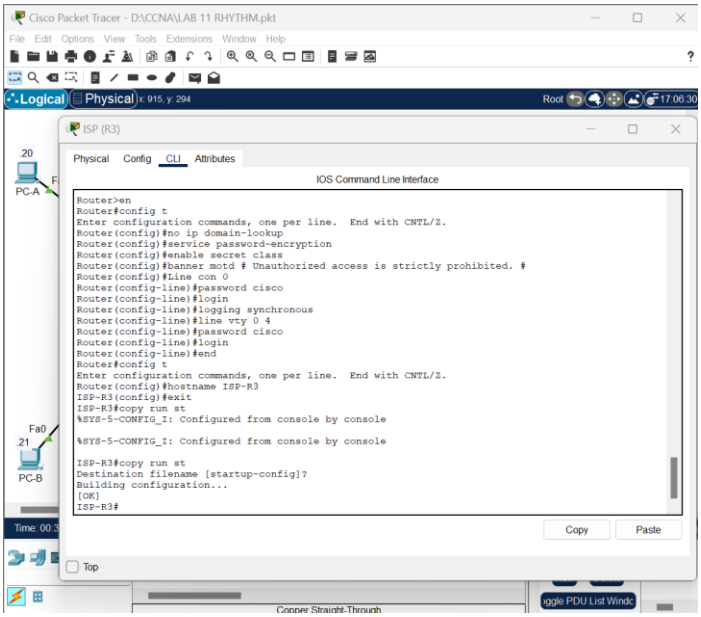
- Configure the host's name as shown in the topology.
- Copy the running configuration to the startup configuration.

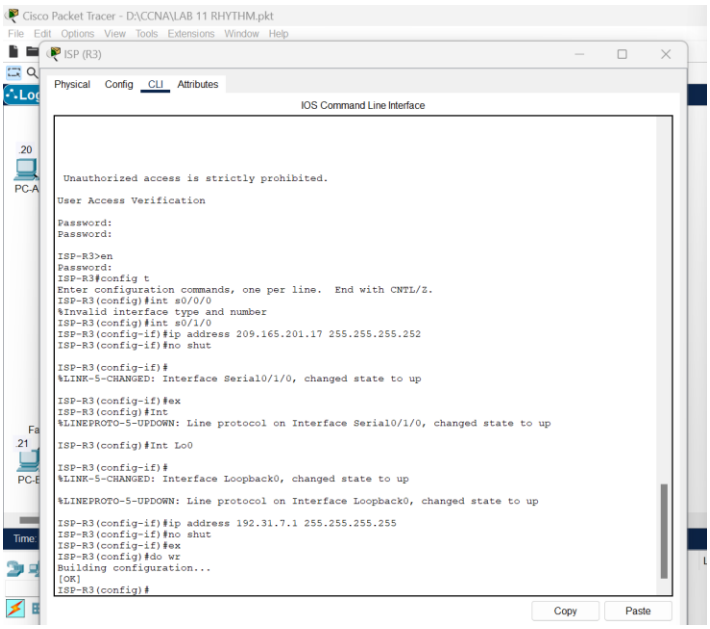
Gateway-R1




Cisco Packet Tracer - D:\CCNA\LAB 11 RHYTHM.pkt
Gateway (R1)
Physical
Config
CLI
Attributes
IOS Command Line Interface
Unauthorized access is strictly prohibited.
User Access Verification
Password:
Gateway-R1>en
Password:
Gateway-R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
Gateway-R1(config)#int g0/0/0
Gateway-R1(config-if)#ip address 192.168.1.1 255.255.255.0
Gateway-R1(config-if)#exit
Gateway-R1(config)#int s0/1/1
Gateway-R1(config-if)#ip address 209.165.201.18 255.255.255.252
Gateway-R1(config-if)#exit
Gateway-R1(config)#int g0/0/0
Gateway-R1(config-if)#no shut
Gateway-R1(config-if)#
%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
Gateway-R1(config-if)#ex
Gateway-R1(config)#int s0/1/1
Gateway-R1(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
Gateway-R1(config-if)#ex
Gateway-R1(config)#vr
% Invalid input detected at '^' marker.
Gateway-R1(config)#end
Gateway-R1#
%SYS-5-CONFIG_I: Configured from console by console
Gateway-R1#wr
Building configuration...
[OK]
Gateway-R1#
Copy
LAN: 192.168.1.0/24
WAN: 209.165.201
PC-A
PC-B
PC-C
Gateway (R1)

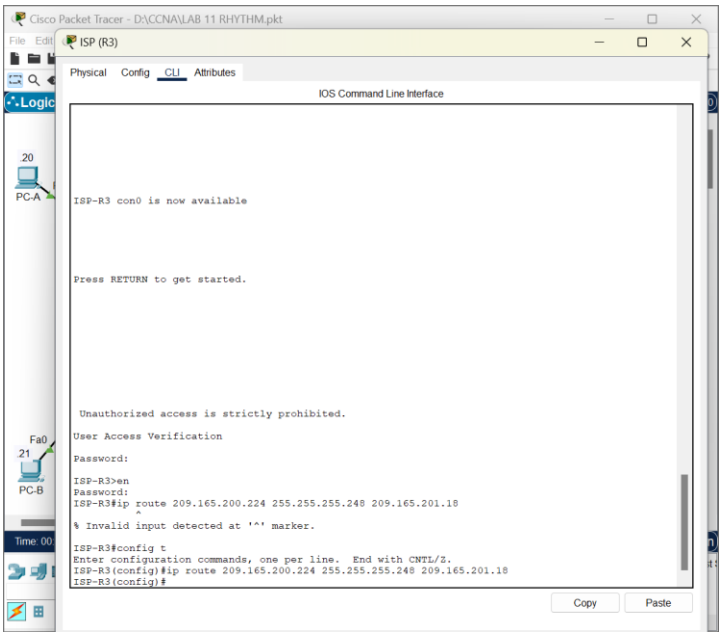
ISP-R3


Cisco Packet Tracer - D:\CCNA\LAB 11 RHYTHM.pkt
ISP (R3)
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#service password-encryption
Router(config)#enable secret class
Router(config)#banner motd # Unauthorized access is strictly prohibited. #
Router(config)#Line con 0
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#logging synchronous
Router(config-line)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#end
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ISP-R3
ISP-R3(config)#exit
ISP-R3#copy run st
%SYS-5-CONFIG_I: Configured from console by console
%SYS-5-CONFIG_I: Configured from console by console
ISP-R3#copy run st
Destination filename [startup-config]?
Building configuration...
[OK]
ISP-R3#
Copy
Paste
Top
PC-A
PC-B
Copper Straight-Through

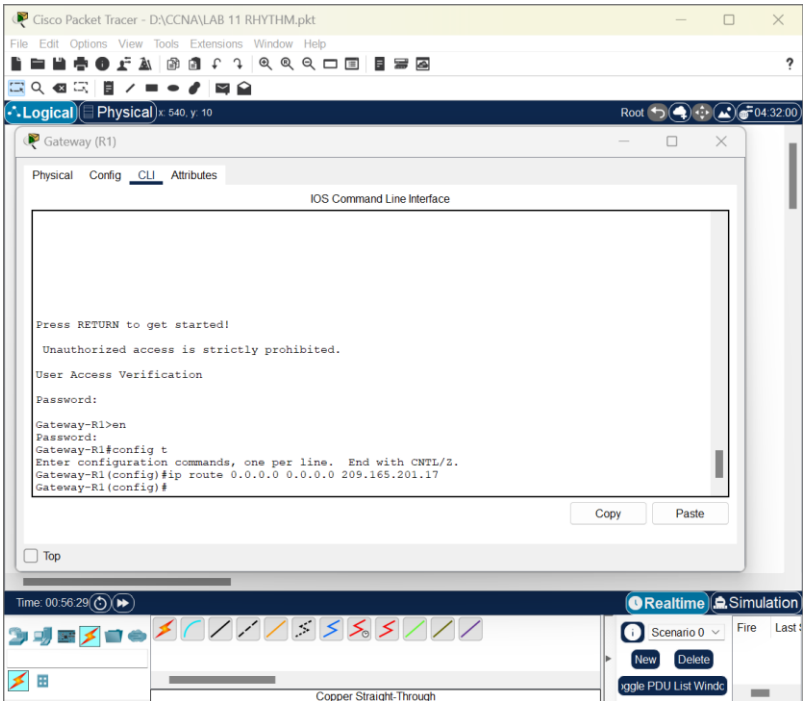

Cisco Packet Tracer - D:\CCNA\LAB 11 RHYTHM.pkt
ISP (R3)
Physical
Config
CLI
Attributes
IOS Command Line Interface
Unauthorized access is strictly prohibited.
User Access Verification
Password:
Password:
ISP-R3>en
Password:
ISP-R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
ISP-R3(config)#int s0/0/0
%Invalid interface type and number
ISP-R3(config)#int s0/1/0
ISP-R3(config-if)#ip address 209.165.201.17 255.255.255.252
ISP-R3(config-if)#no shut
ISP-R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
ISP-R3(config-if)#ex
ISP-R3(config)#Int
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
ISP-R3(config)#Int Lo0
ISP-R3(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
ISP-R3(config-if)#ip address 192.31.7.1 255.255.255.255
ISP-R3(config-if)#no shut
ISP-R3(config-if)#ex
ISP-R3(config)#do wr
Building configuration...
[OK]
ISP-R3(config)#
Copy
Paste
PC-A

5. Configure static routing.

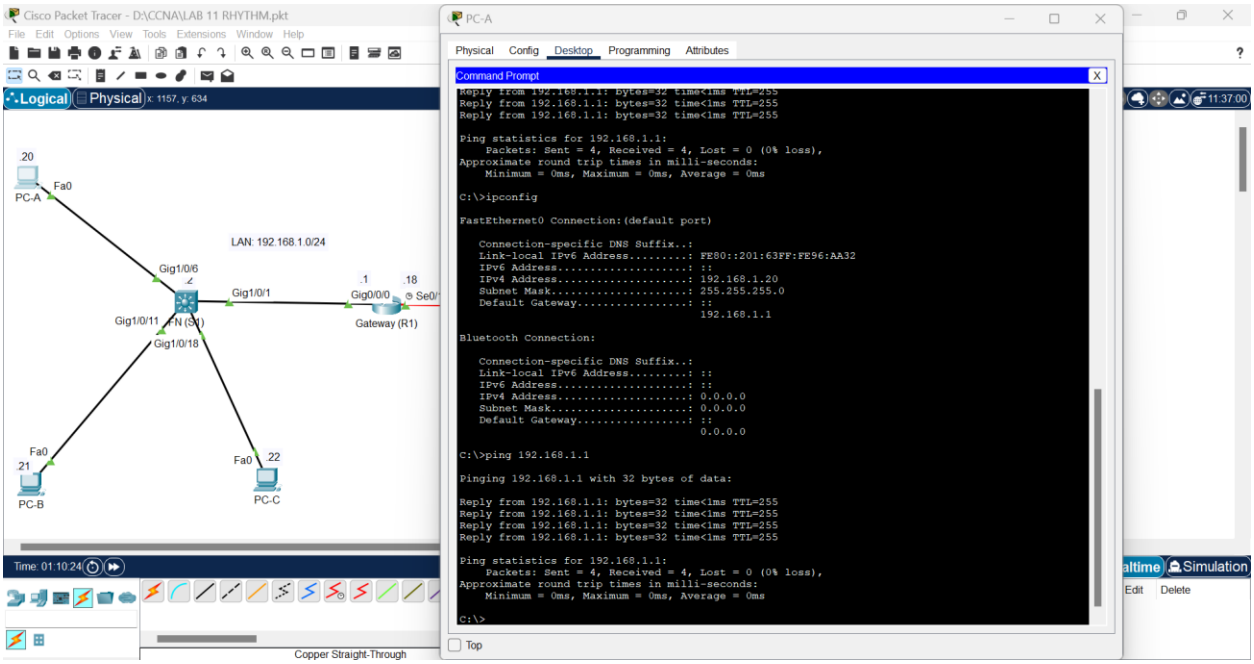
- Create a static route from the ISP router to the Gateway router.
- ISP(config)# **ip route 209.165.200.224 255.255.255.248 209.165.201.18**



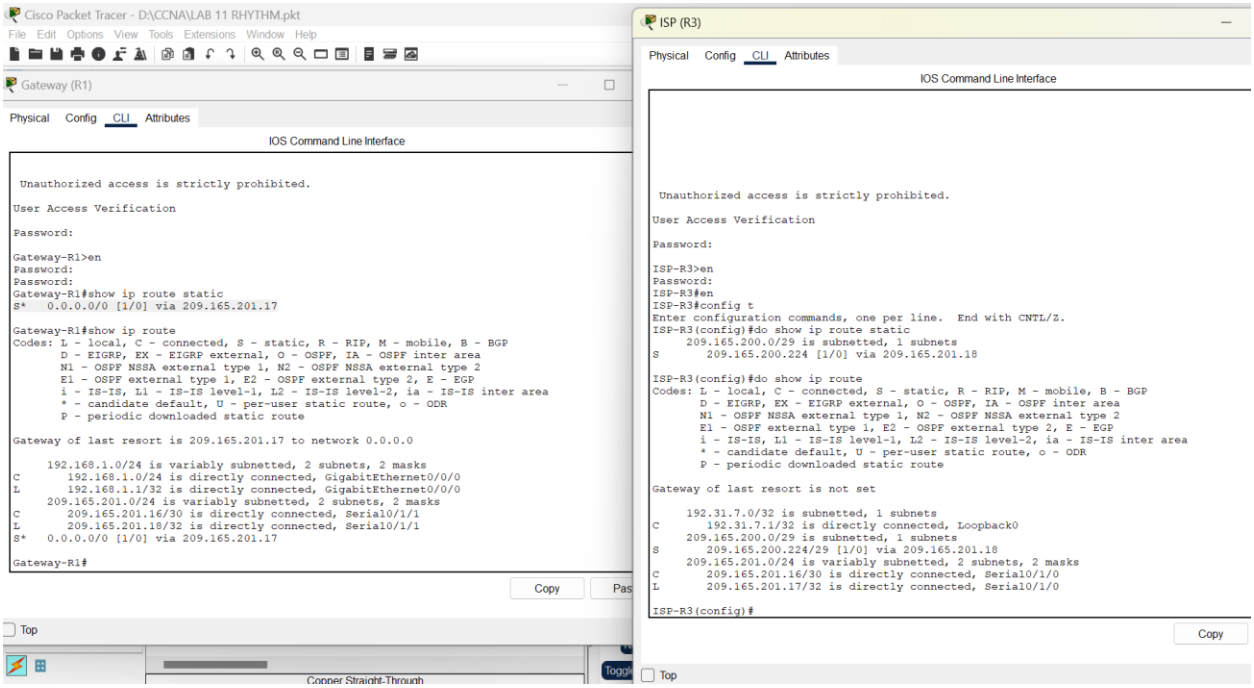
- Create a default route from the Gateway router to the ISP router.
- Gateway(config)# **ip route 0.0.0.0 0.0.0.0 209.165.201.17**



- Verify network connectivity.
- From the PC hosts, ping the G0/0/0 interface on the Gateway router. Troubleshoot if the pings are unsuccessful.



- Verify the static routes are configured correctly on both routers.



Step 2: Configure and Verify NAT Pool Overload

In Step 2, you will configure the Gateway router to translate the IP addresses from the 192.168.1.0/24 network to one of the six usable addresses in the 209.165.200.224/29 range.

6. **Define an access control list that matches the LAN private IP addresses.**

   ACL 1 is used to allow the 192.168.1.0/24 network to be translated.

   Gateway(config)# **access-list 1 permit 192.168.1.0 0.0.0.255**

7. **Define the pool of usable public IP addresses.**

   Gateway(config)# **ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248**

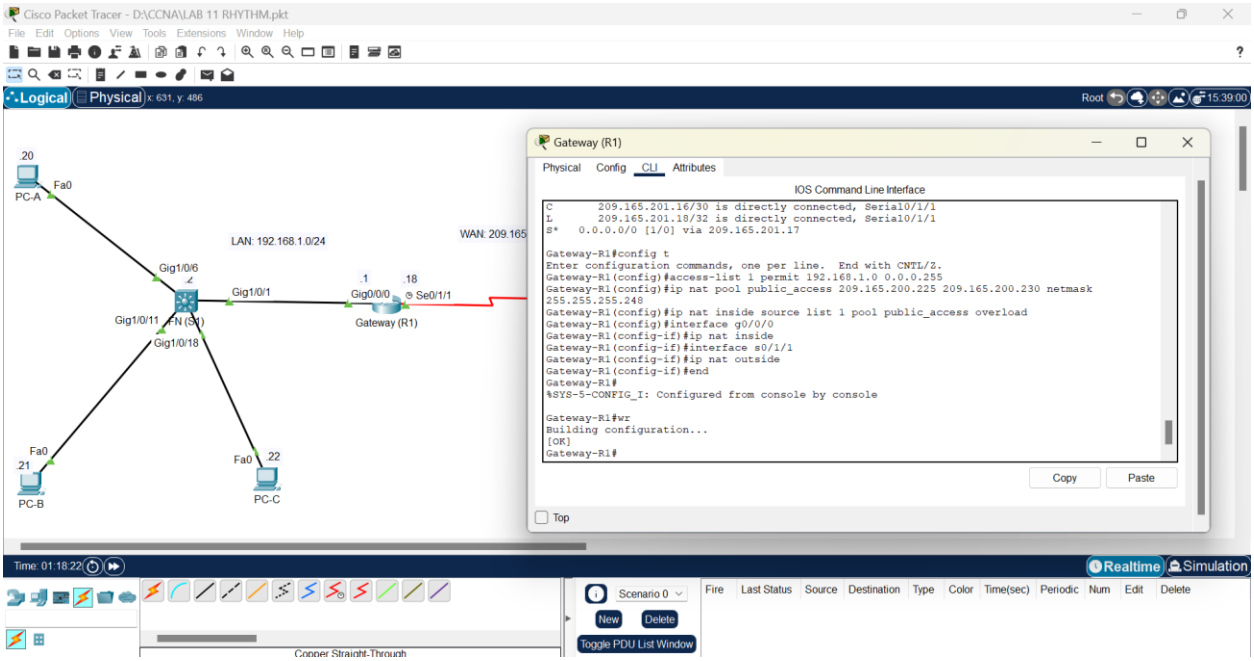
8. **Define the NAT from the inside source list to the outside pool.**

   Gateway(config)# **ip nat inside source list 1 pool public_access overload**

9. **Specify the interfaces.**

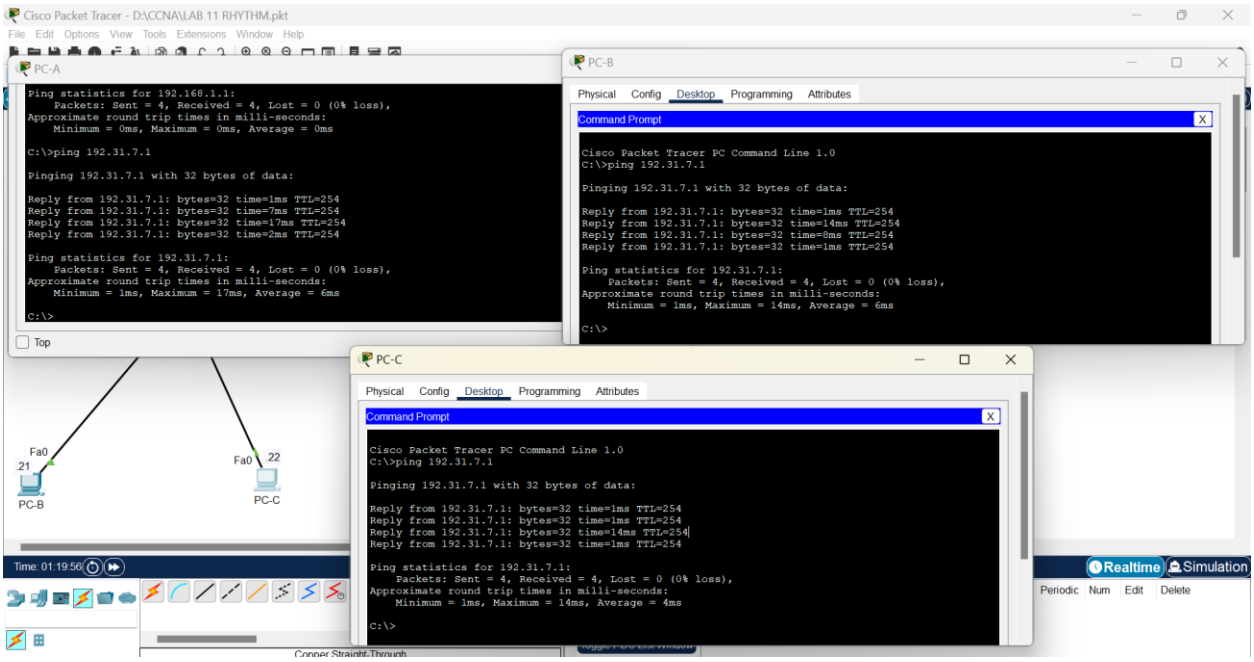
Issue the **ip nat inside** and **ip nat outside** commands to the interfaces.

Gateway(config)# **interface g0/0/0**
Gateway(config-if)# **ip nat inside**
Gateway(config-if)# **interface s0/1/1**
Gateway(config-if)# **ip nat outside**



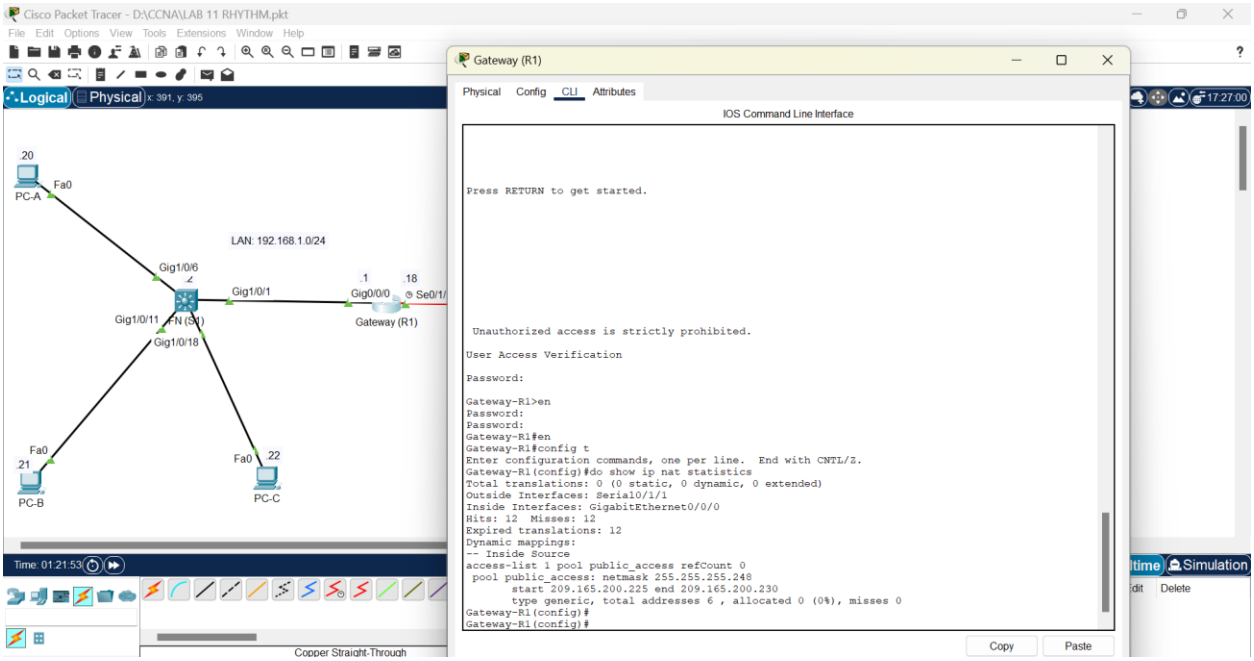
10. Verify the NAT pool overload configuration.

From each PC host, ping the 192.31.7.1 address on the ISP router.



Display NAT statistics on the Gateway router.

show ip nat statistics



Note: Depending on how much time has elapsed since you performed the pings from each PC, you may not see all three translations. ICMP translations have a short timeout value.

How many inside local IP addresses are listed in the sample output above?

Answer: Output doesn't explicitly mention. However, we knew that we try to ping from each PC once so 3 inside local IP addresses are listed.

How many inside global IP addresses are listed?

Answer: Total Six ranging start from 209.165.200.225 and end to 209.165.200.230.

How many port numbers are paired with the inside global addresses?

Answer: 3 ports

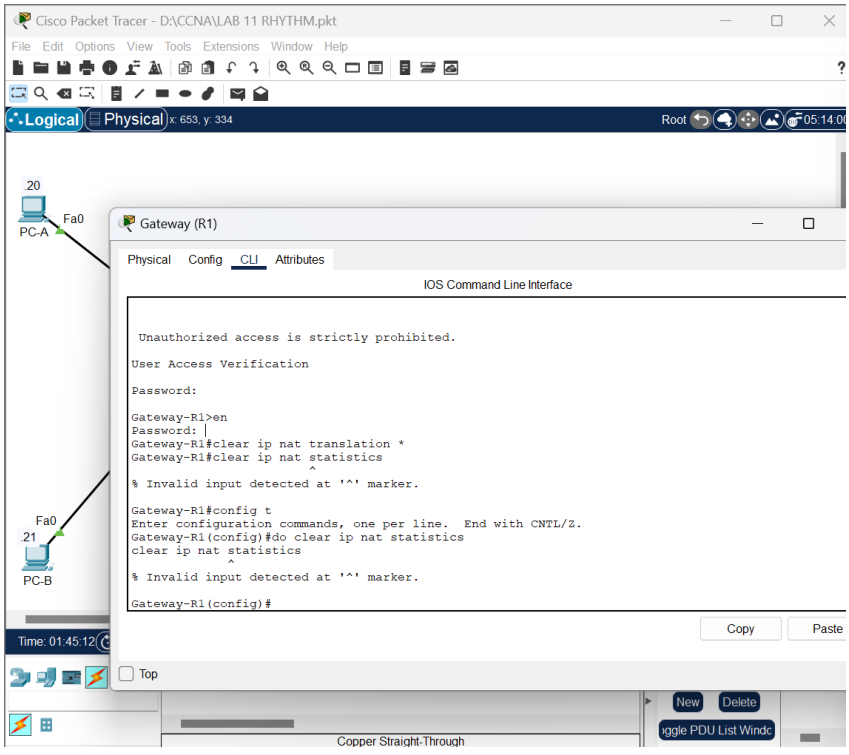
What would be the result of pinging the inside local address of PC-A from the ISP router? Why?

Answer: Pinging the inside local address of PC-A from the ISP router would not be successful because NAT translates private IP addresses to public IP addresses only for outgoing traffic from the internal network to the external network. The ISP router does not have knowledge of the internal network's private IP addresses

Step 3: Configure and Verify PAT

In Step 3, you will configure PAT by using an interface instead of a pool of addresses to define the outside address. Not all the commands in Step 2 will be reused in Step 3.

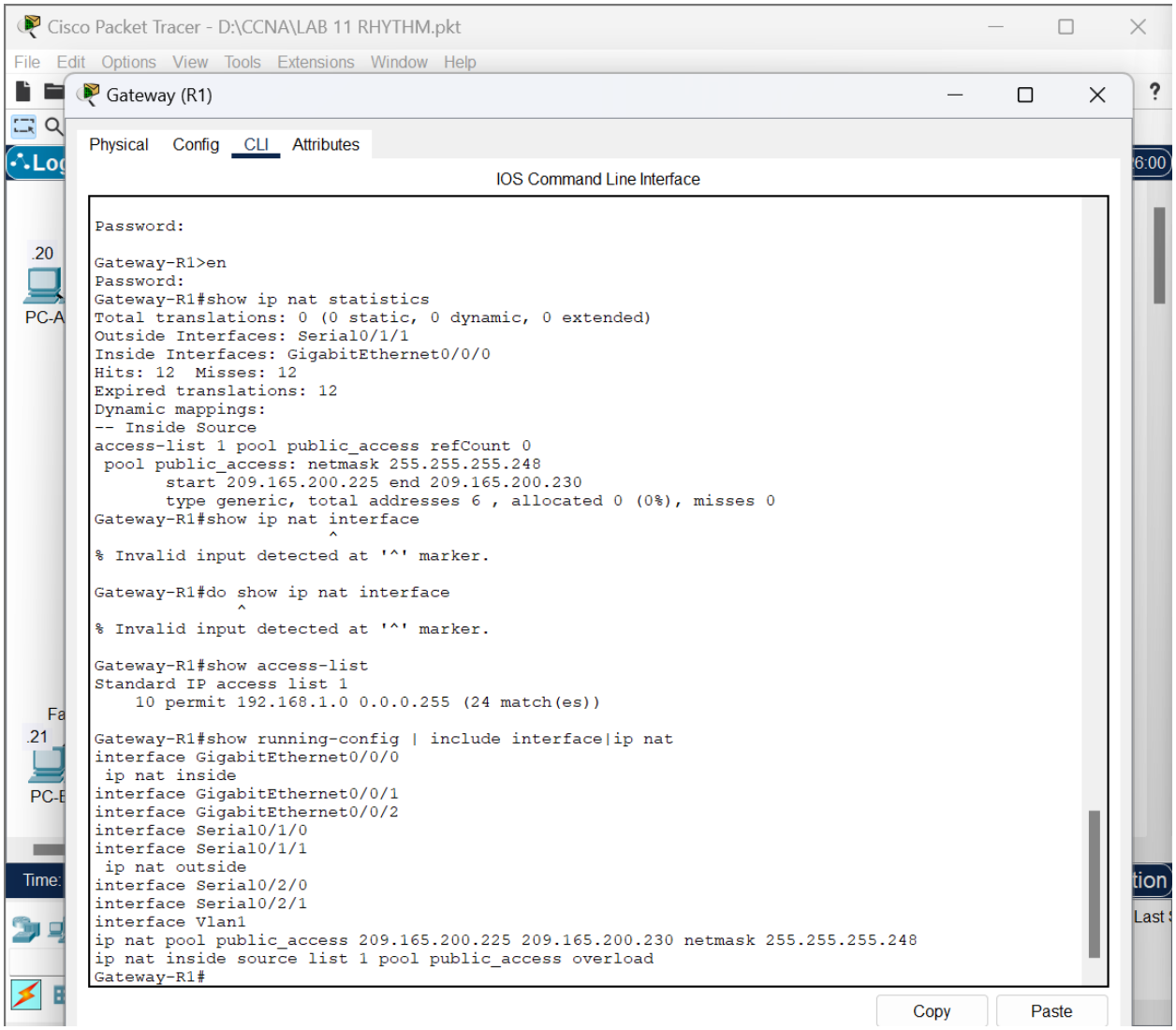
11. Clear NATs and statistics on the Gateway router.



12. Verify the configuration for NAT.

- Verify that statistics have been cleared.
- Verify that the outside and inside interfaces are configured for NATs.

  This command is not working on this router.
- Verify the ACL is still configured for NATs.
- What command did you use to confirm the results from steps a to c?



13. Remove the pool of useable public IP addresses.

Gateway(config)# **no ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248**

14. Remove the NAT translation from inside source list to outside pool.

Gateway(config)# **no ip nat inside source list 1 pool public_access overload**

15. Associate the source list with the outside interface.

Gateway(config)# **ip nat inside source list 1 interface serial 0/1/1 overload**

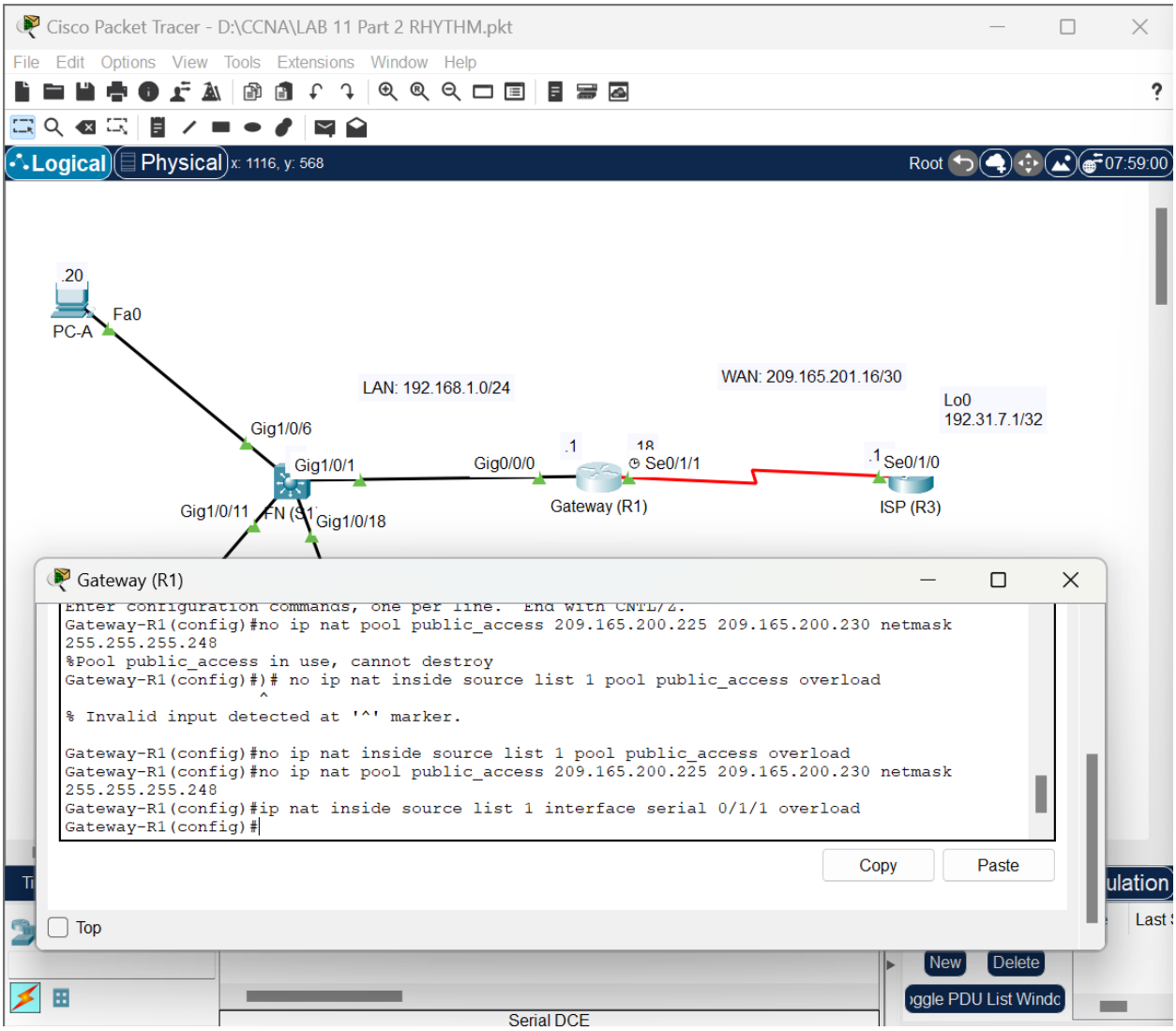
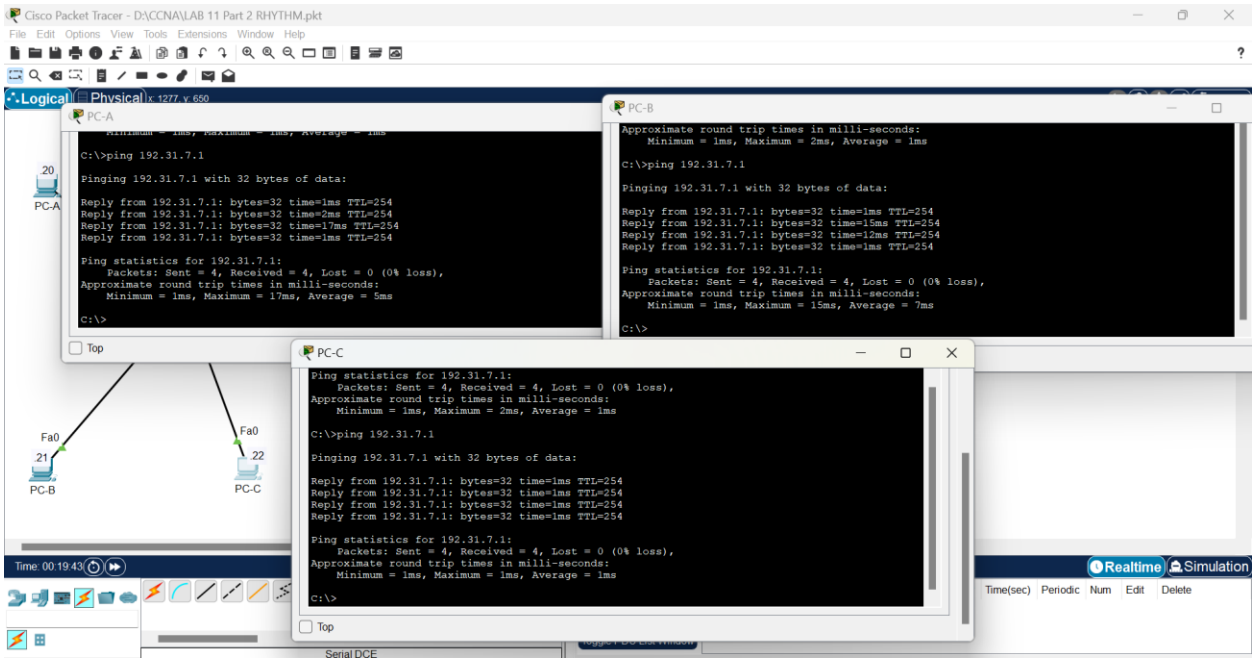


Figure 1

16. Test the PAT configuration.

- From each PC, ping the 192.31.7.1 address on the ISP router.

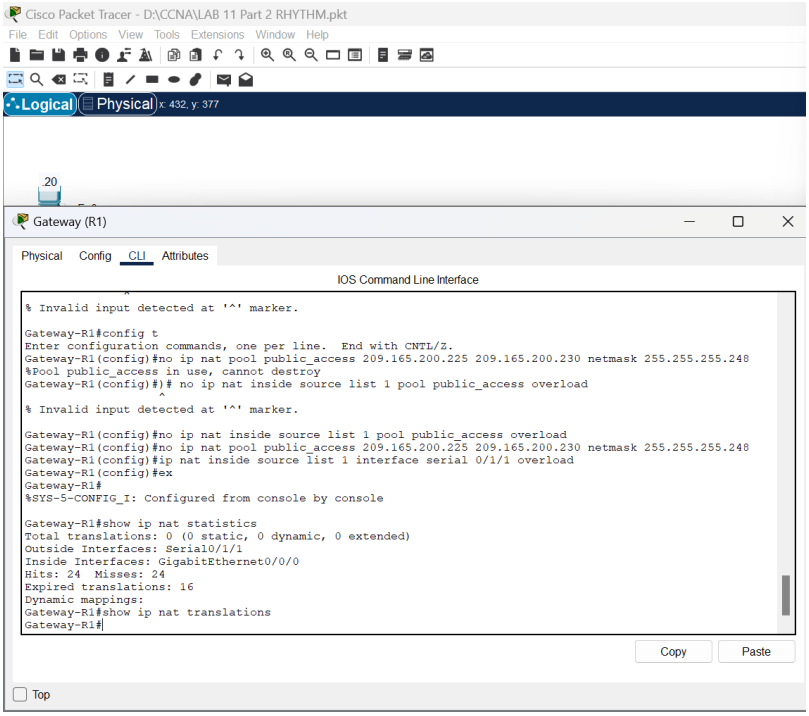


- Display NAT statistics on the Gateway router.

  Gateway# **show ip nat statistics**

- Display NAT translations on Gateway.

  Gateway# **show ip nat translations**



Reflection

What advantages does PAT provide?

Answer: 1. Better Security

2. Saving Public IP Addresses

3. Easier to Manage