

Group 4

Namrata Bhorade - 2018130004

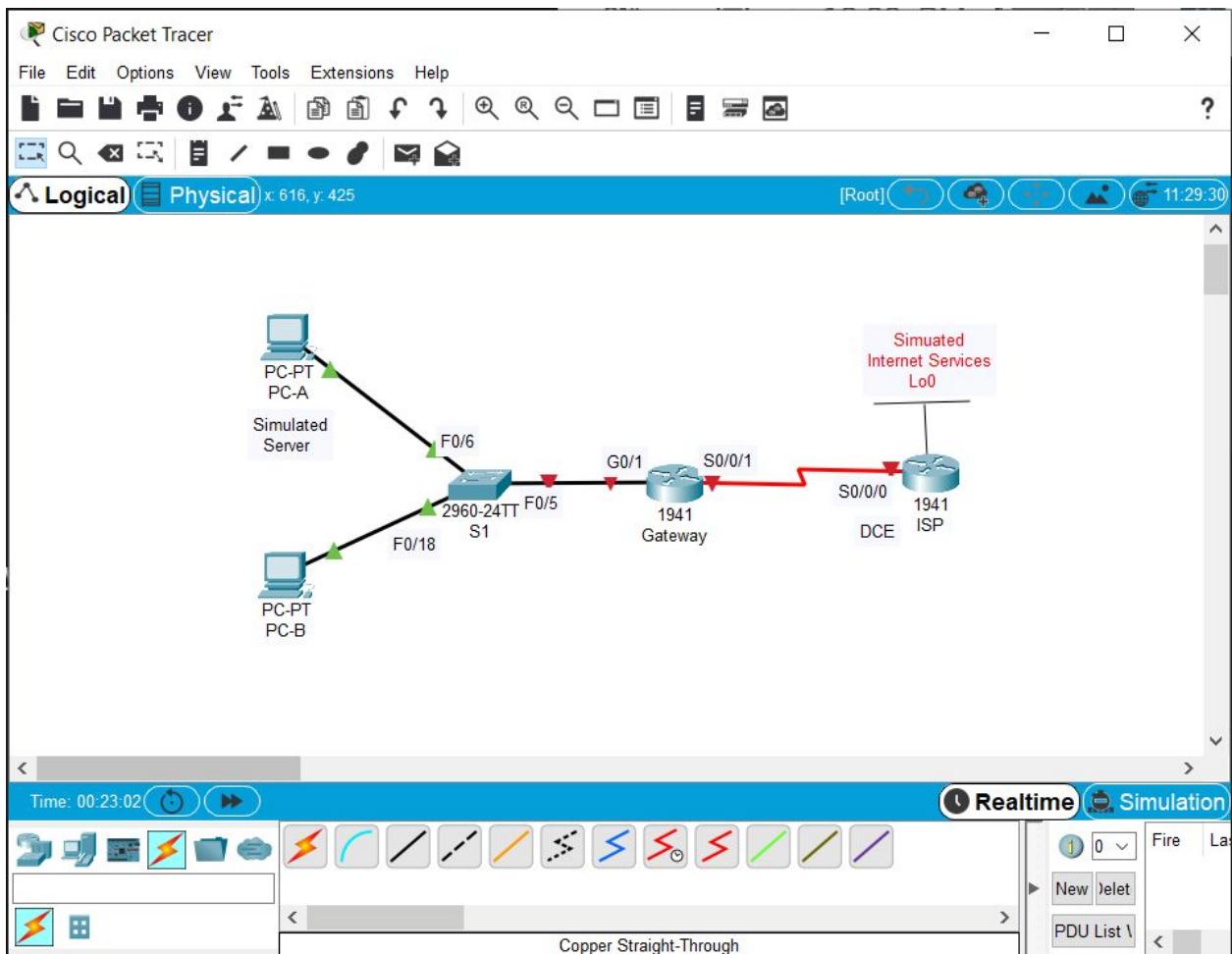
Nikita Chitre - 2018130006

Ojasa Chitre - 2018130007

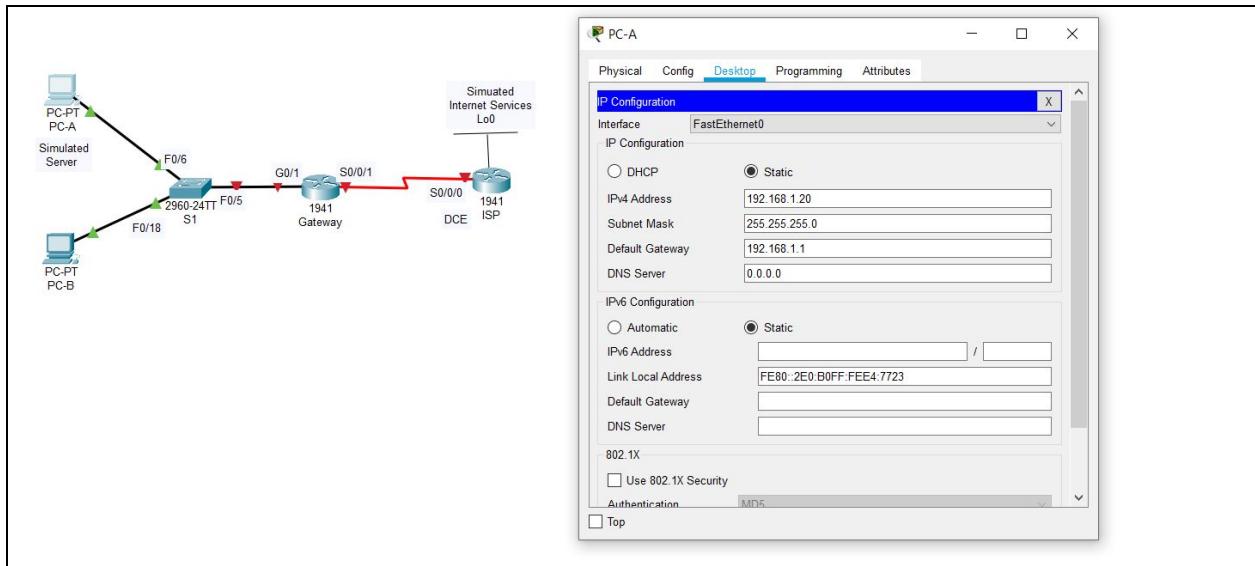
DCCN LAB ISE

Task 1

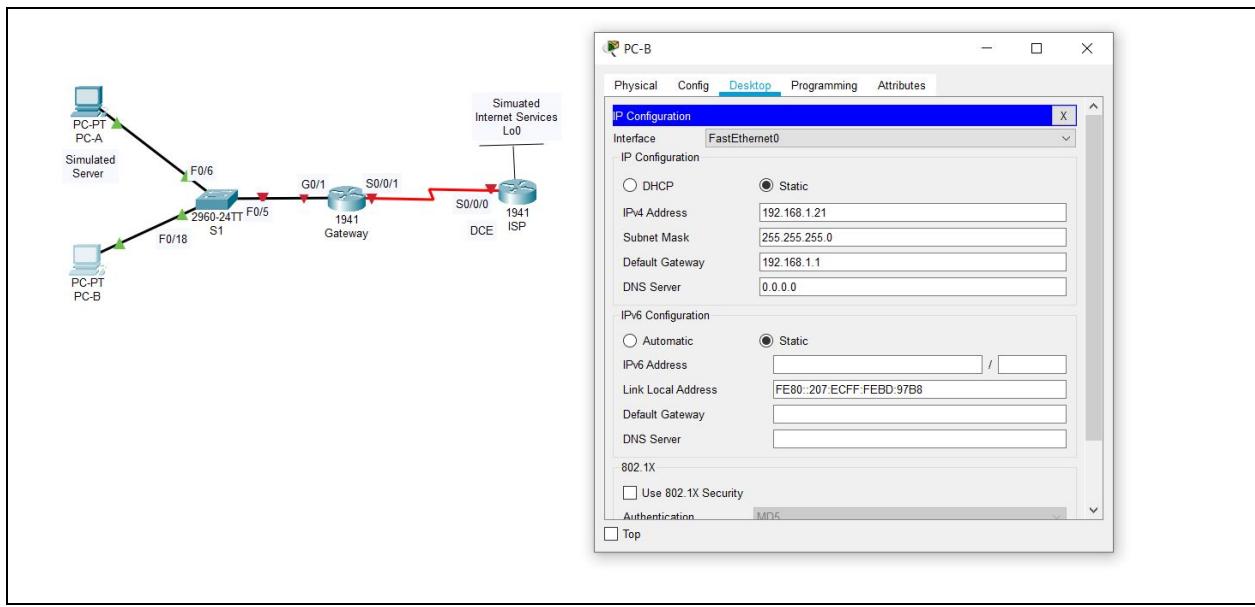
Step 1 : Topology setup with appropriate devices and wiring.



Step 2: Configure PC hosts.

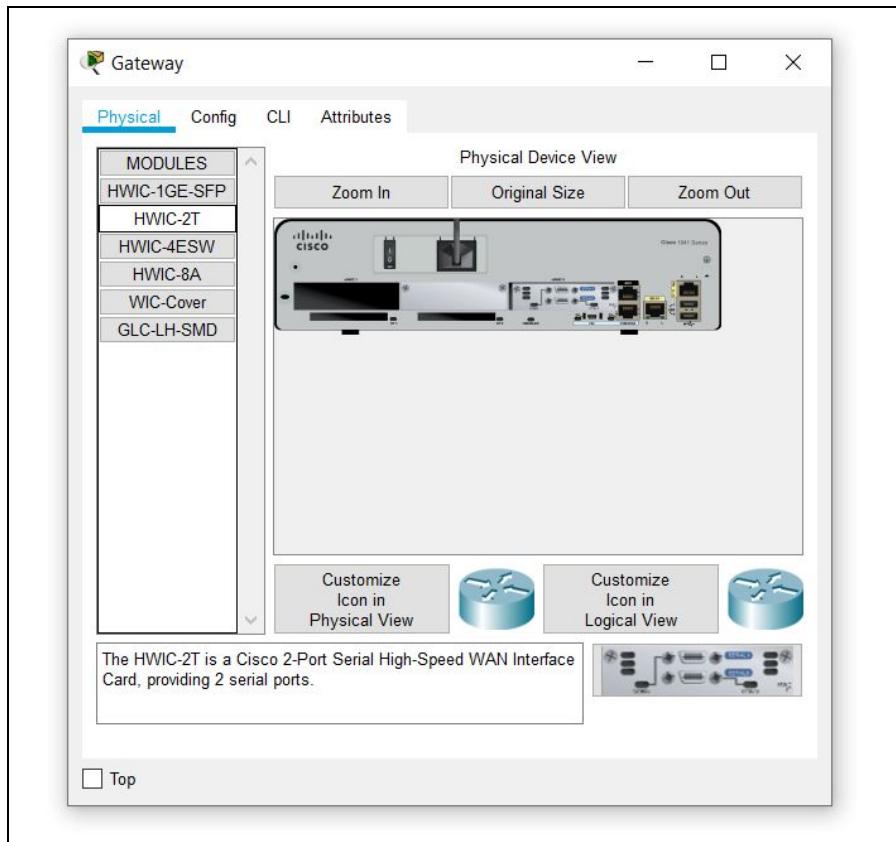
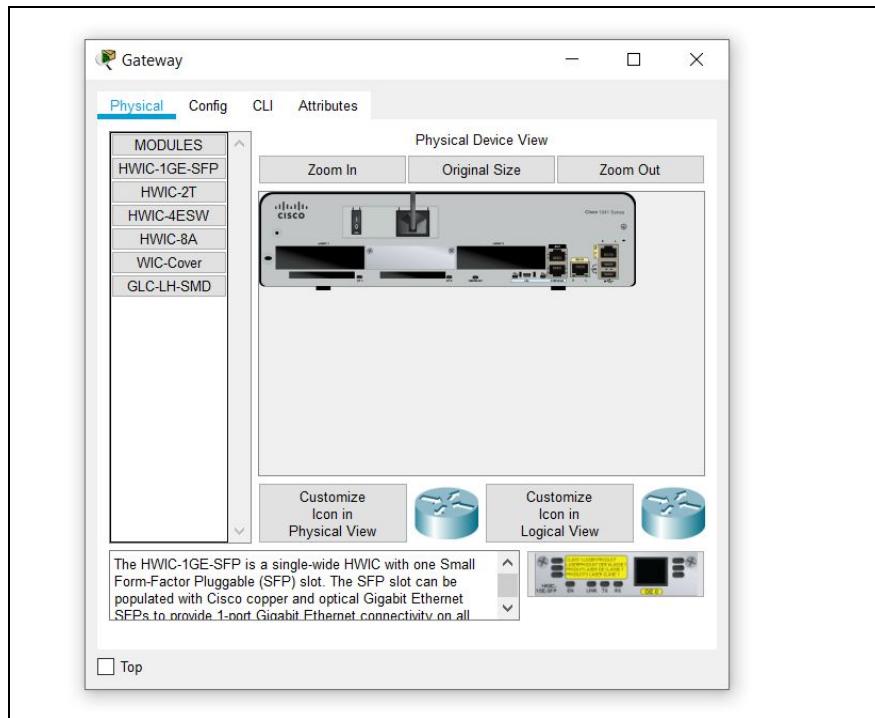


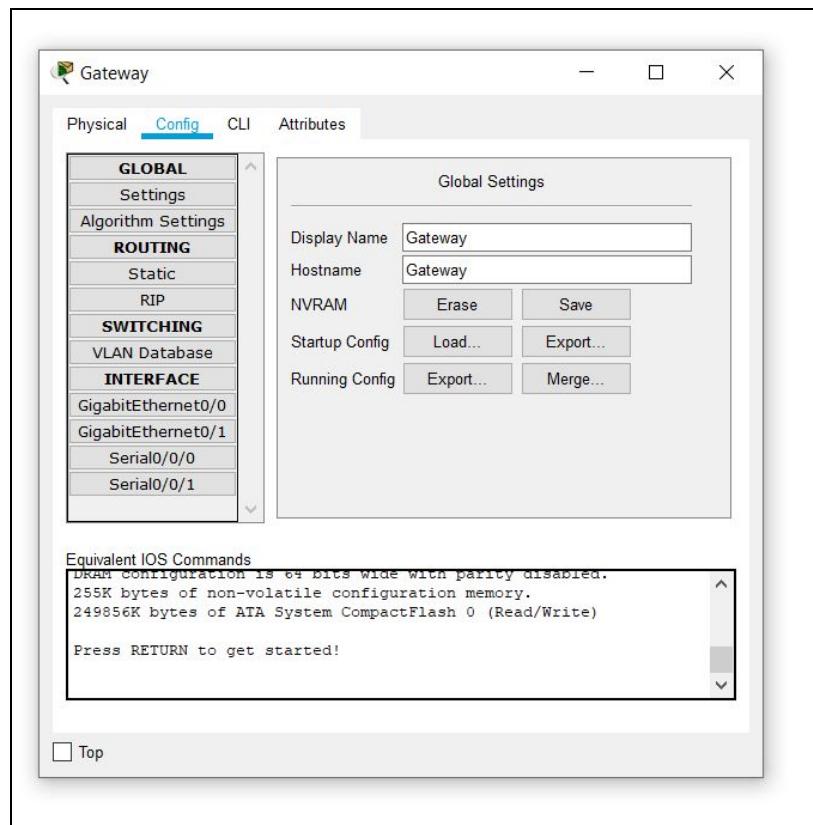
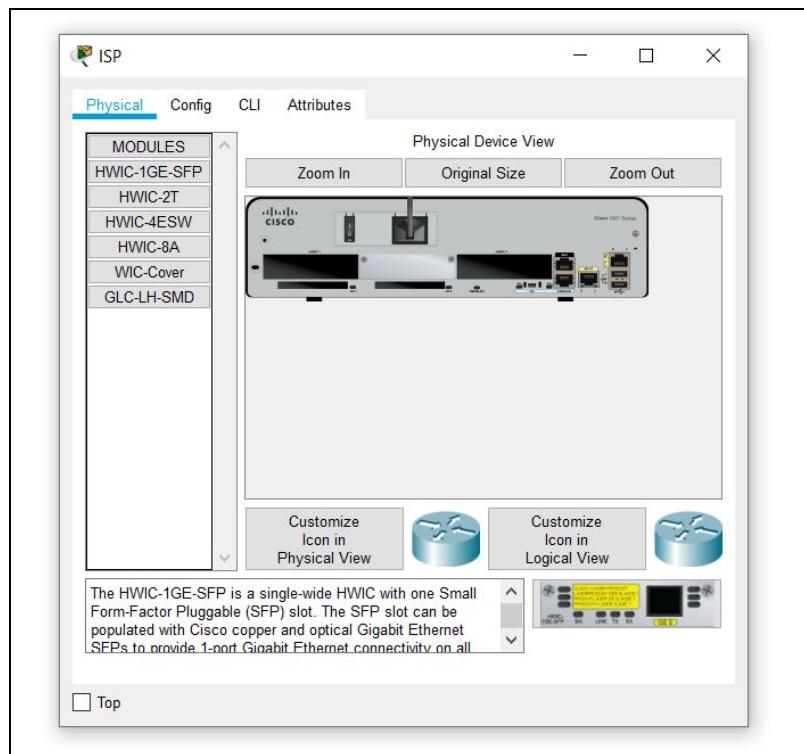
Configuring the PC-A by adding the ip address, subnet mask and default gateway as shown above.

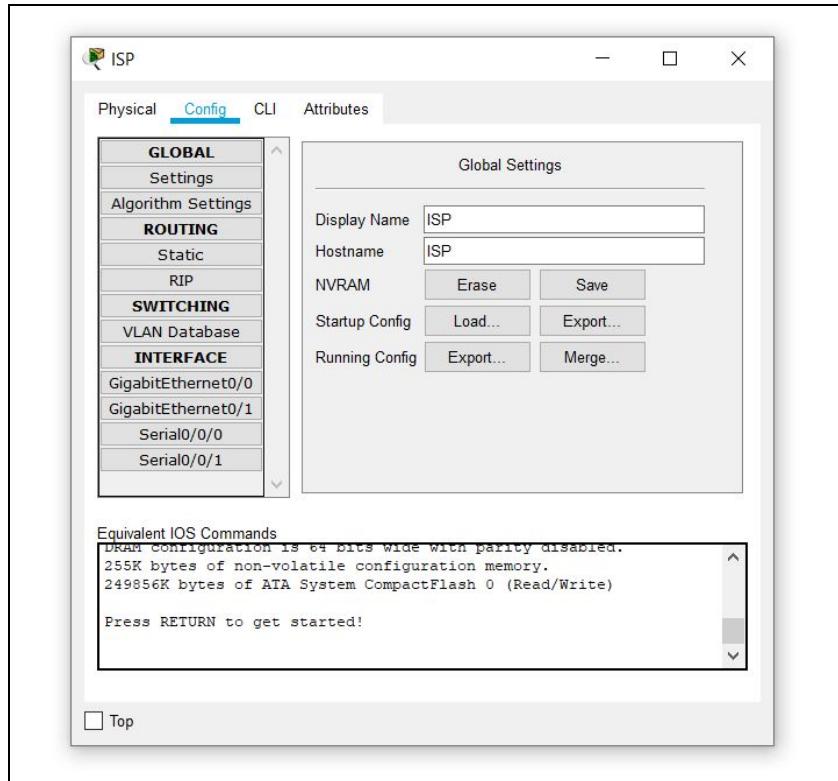
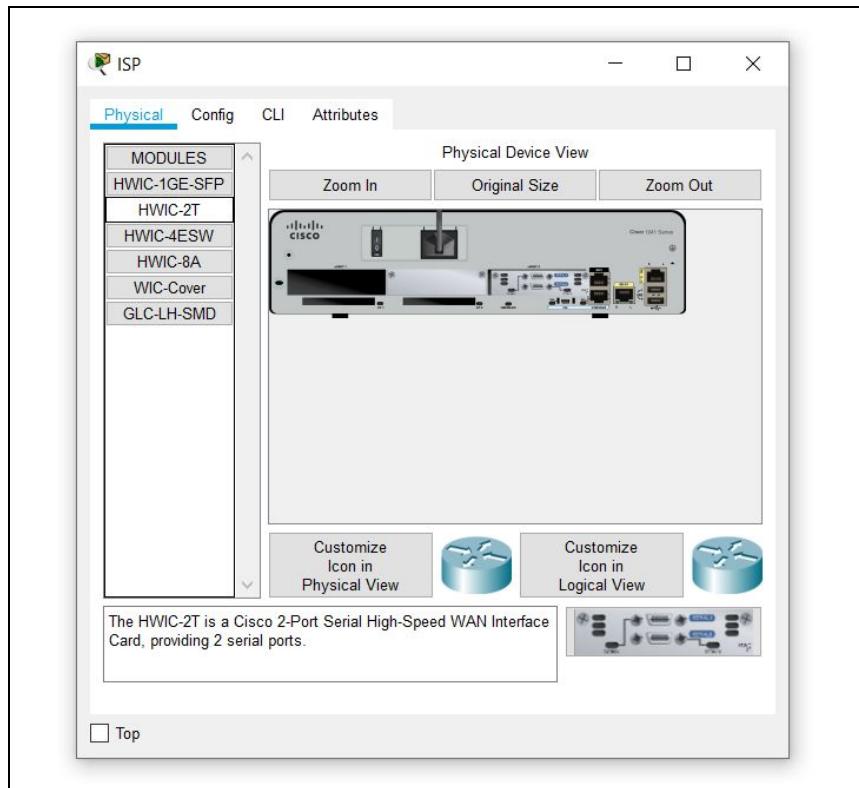


Configuring the PC-B by adding the ip address, subnet mask and default gateway as shown above.

Step 3: Initialize and reload the routers and switches as necessary.

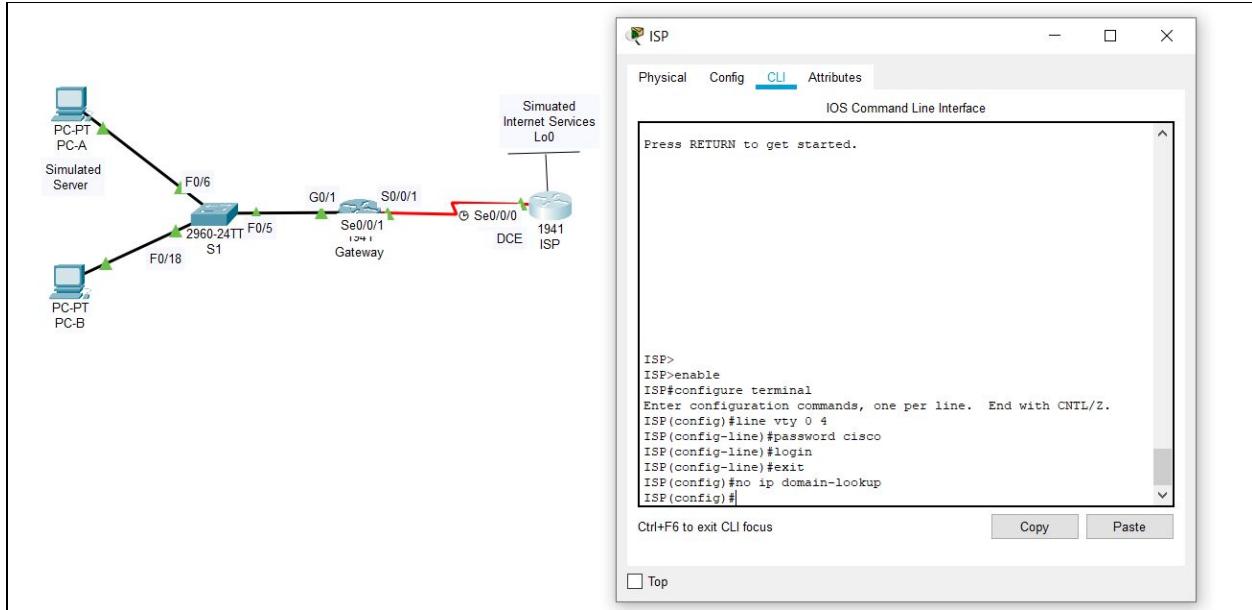




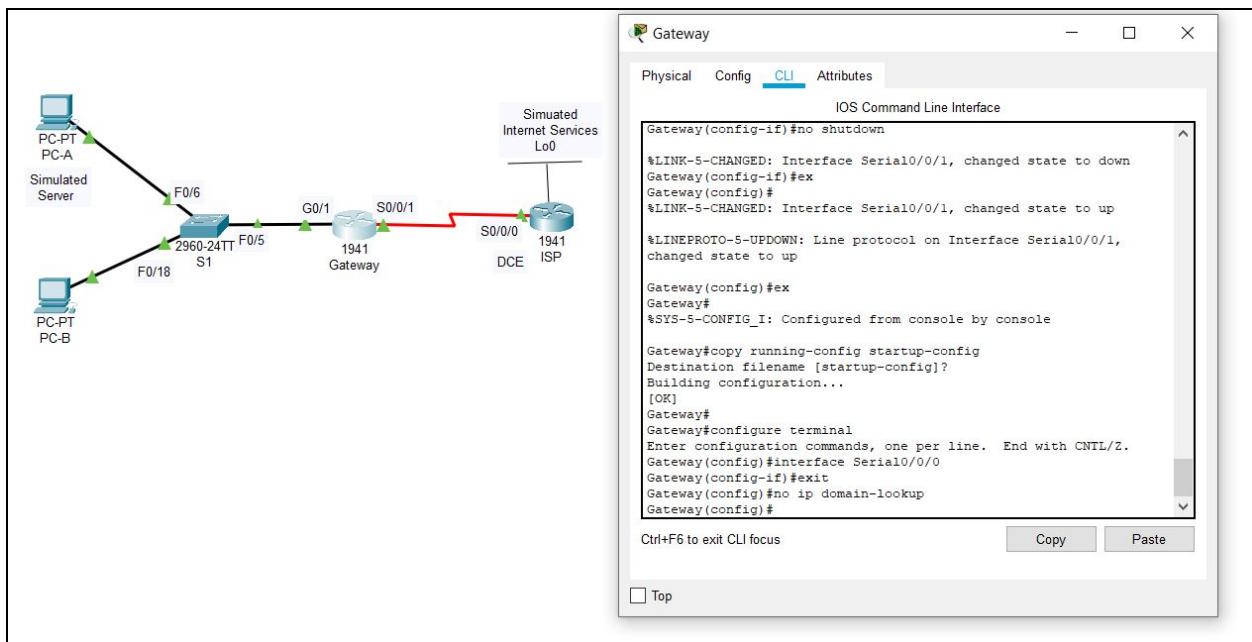


Step 4: Configure basic settings for each router.

a. Disable DNS lookup.



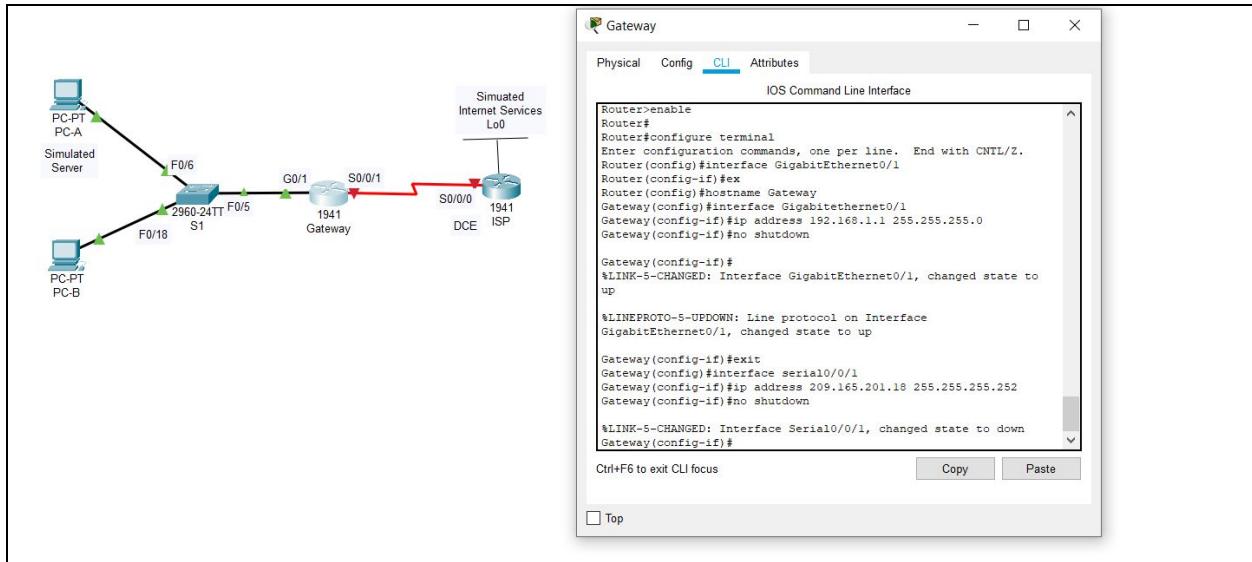
Disable DNS lookup for ISP as shown above.



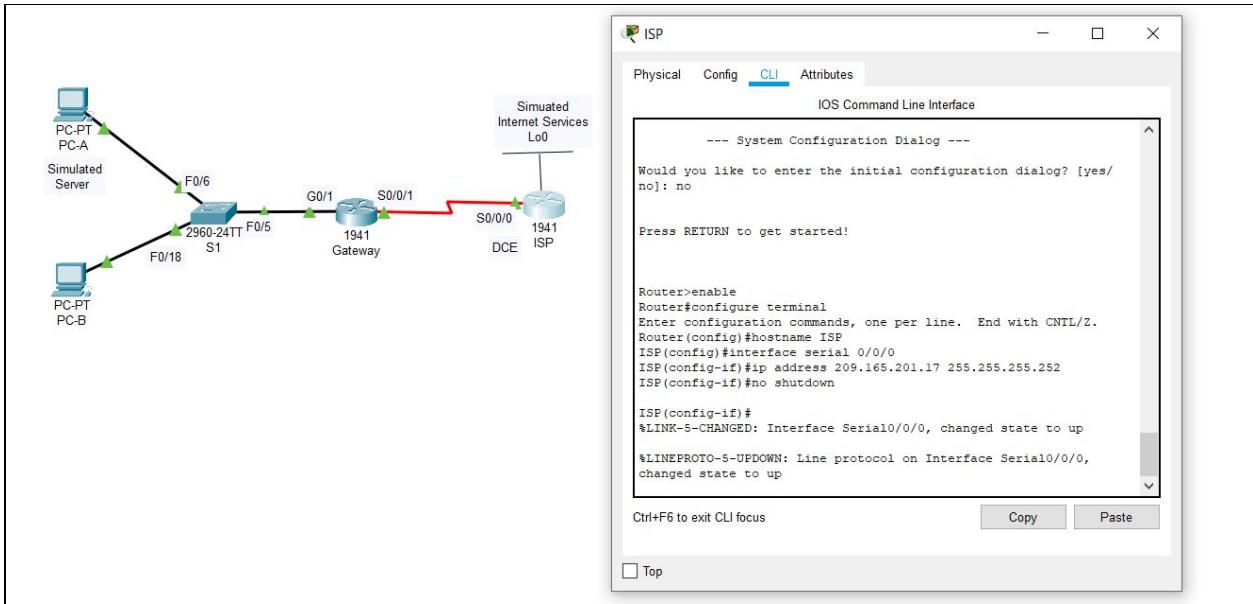
Disable DNS lookup for Gateway as shown above.

b. Configure IP addresses for the routers as listed

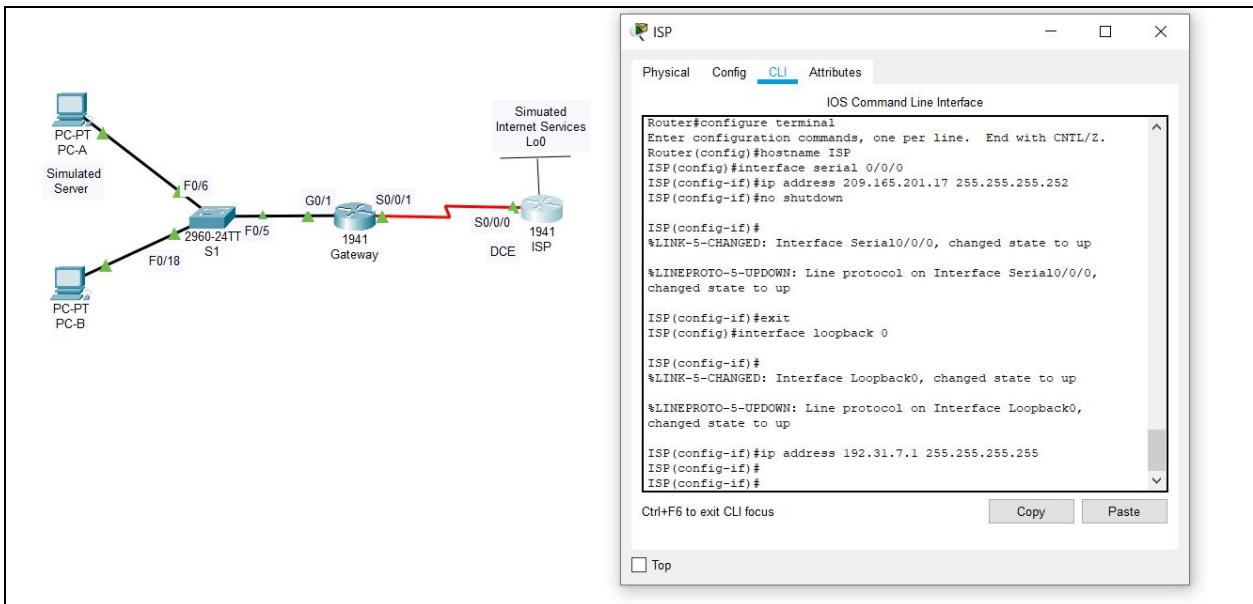
Configuring GigabitEthernet0/1 interface in gateway router by adding ip address and subnet mask as shown above.



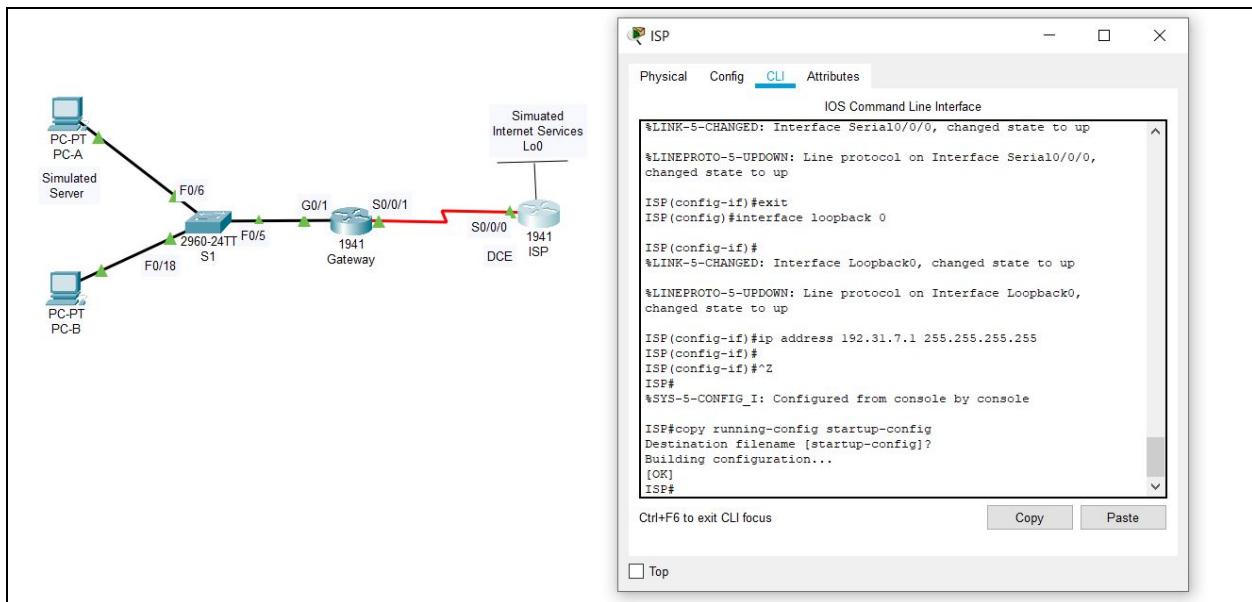
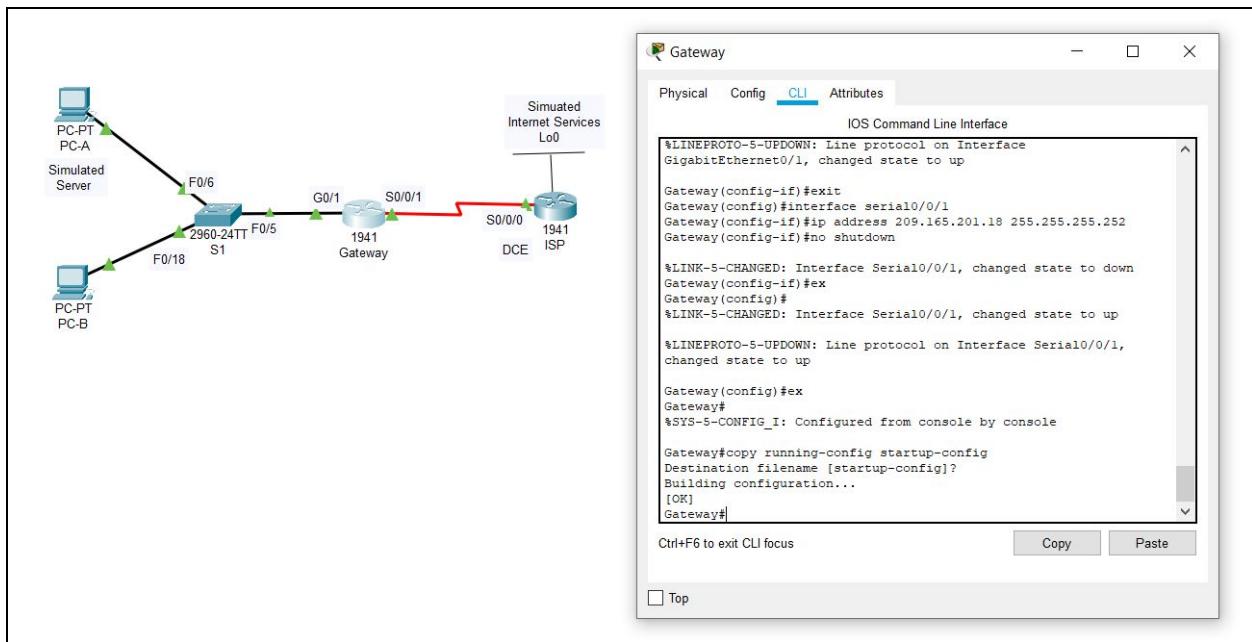
Configuring Serial0/0/1 interface in gateway router by adding ip address and subnet mask as shown above.



Configuring Serial0/0/0 interface in ISP router by giving ip address and subnet mask as shown above.

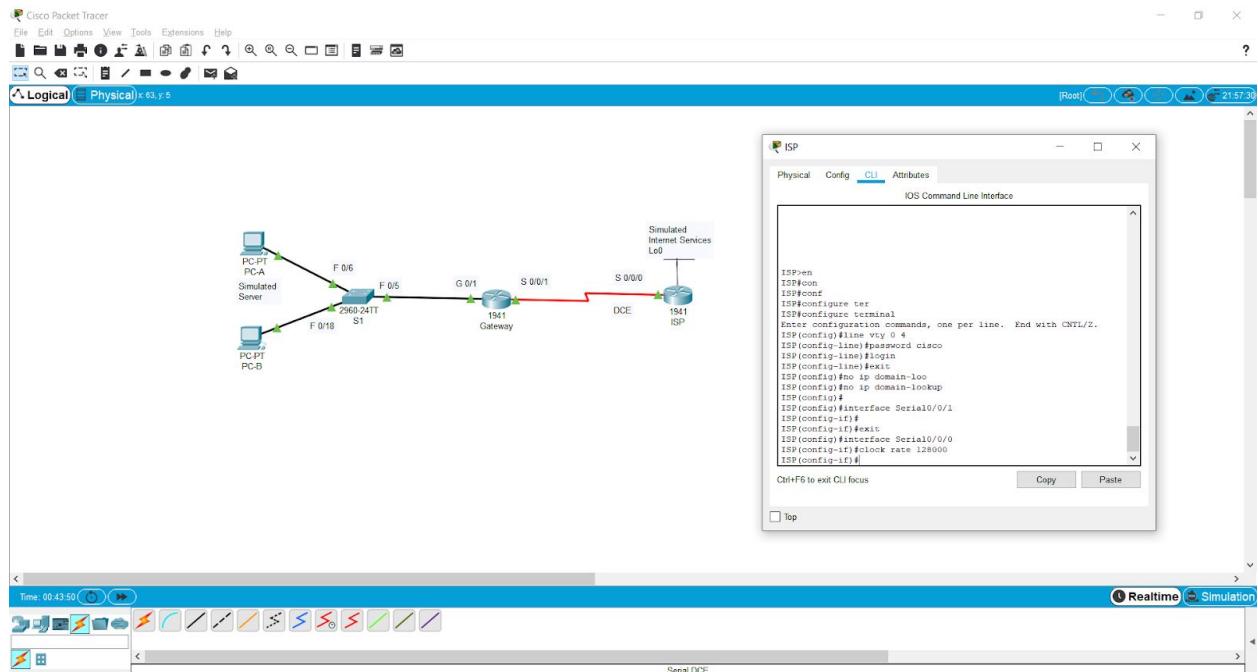


Configuring Loopback0 interface in ISP router by giving ip address and subnet mask as shown above.



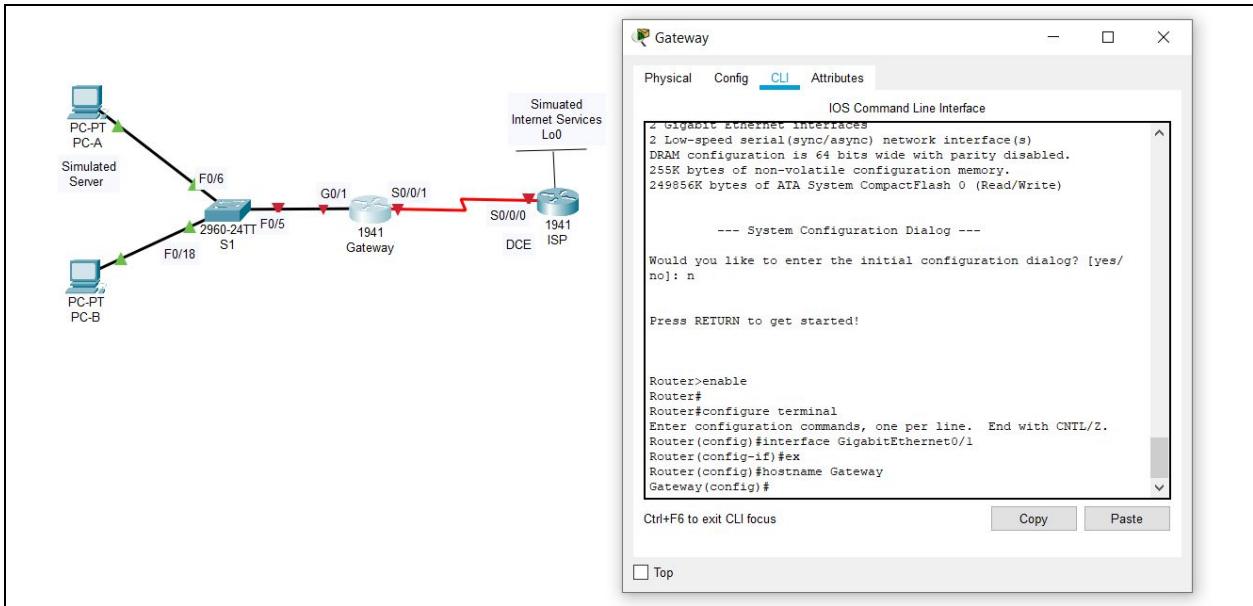
Copying running configuration into startup-configuration as shown above.

c. Set clock rate to 128000 for DCE serial0/0/0 interface

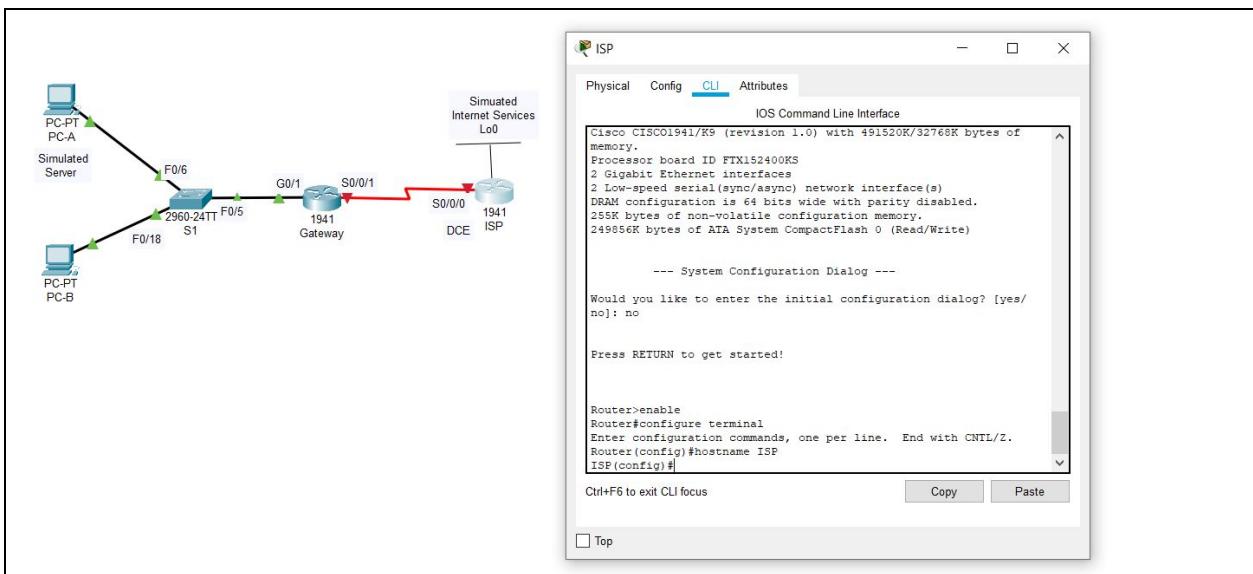


Set clock rate to 128000 for DCE serial0/0/0 interface of ISP router as shown above

d. Configure device name as shown in the topology.

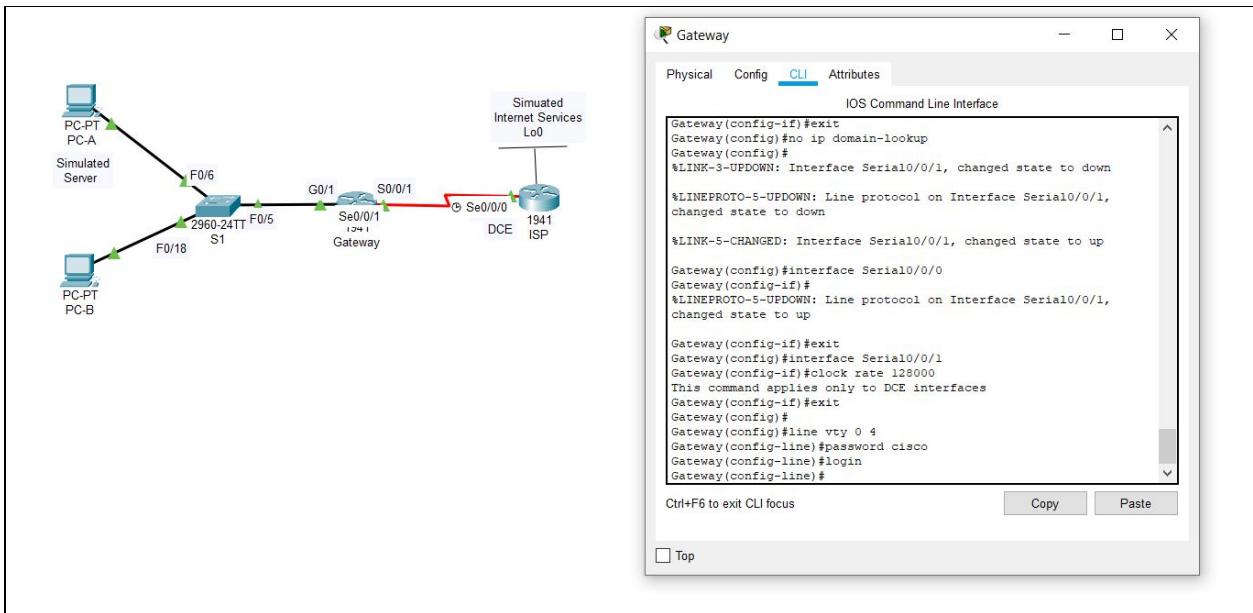


Configuring the hostname of the Router as Gateway.

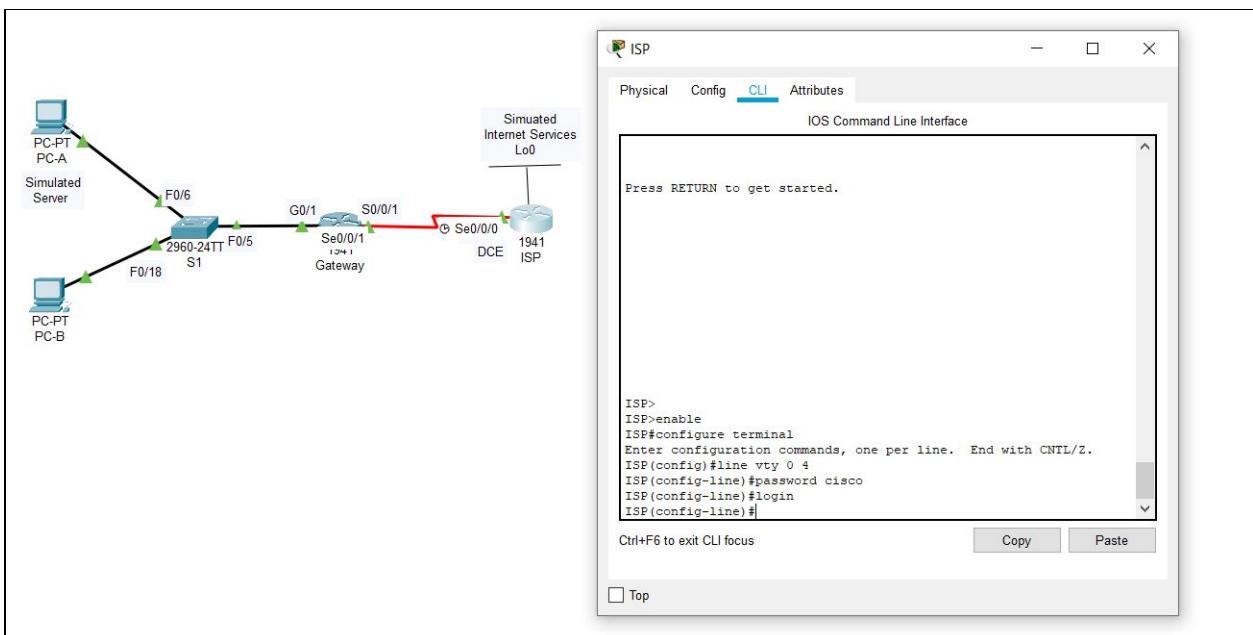


Configuring the hostname of the Router as ISP as shown above.

e. Assign cisco as console and vty passwords

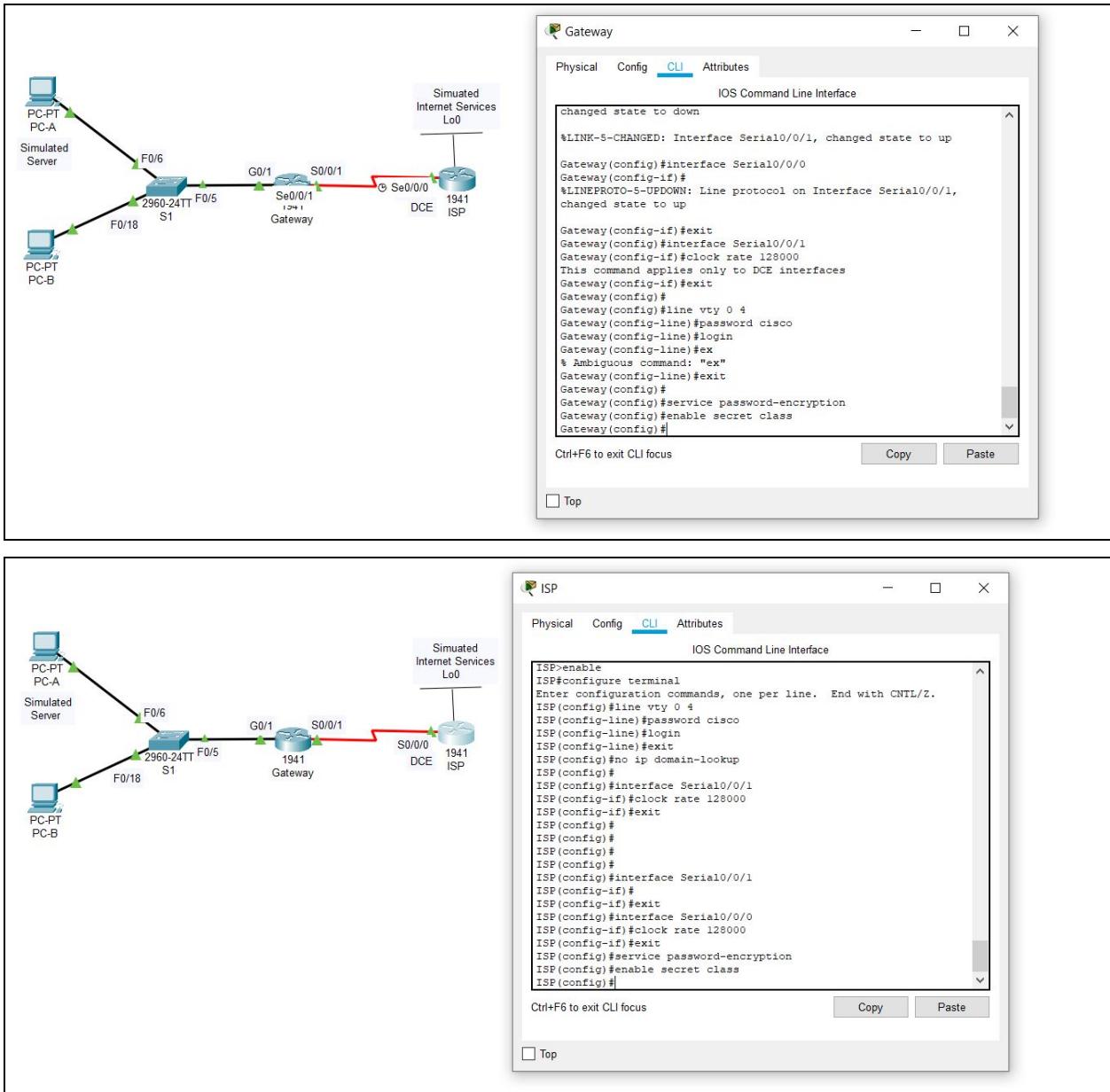


Assign cisco as console and vty passwords as shown above.



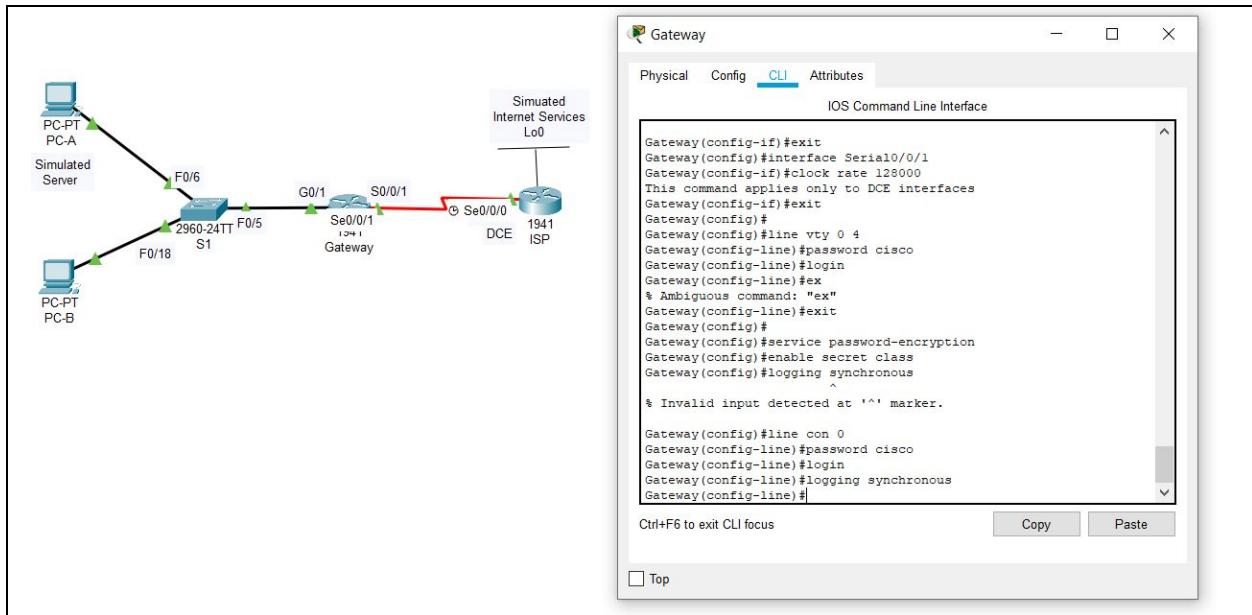
Assign cisco as console and vty passwords as shown above.

f. Assign class as encrypted privileged EXEC mode password.

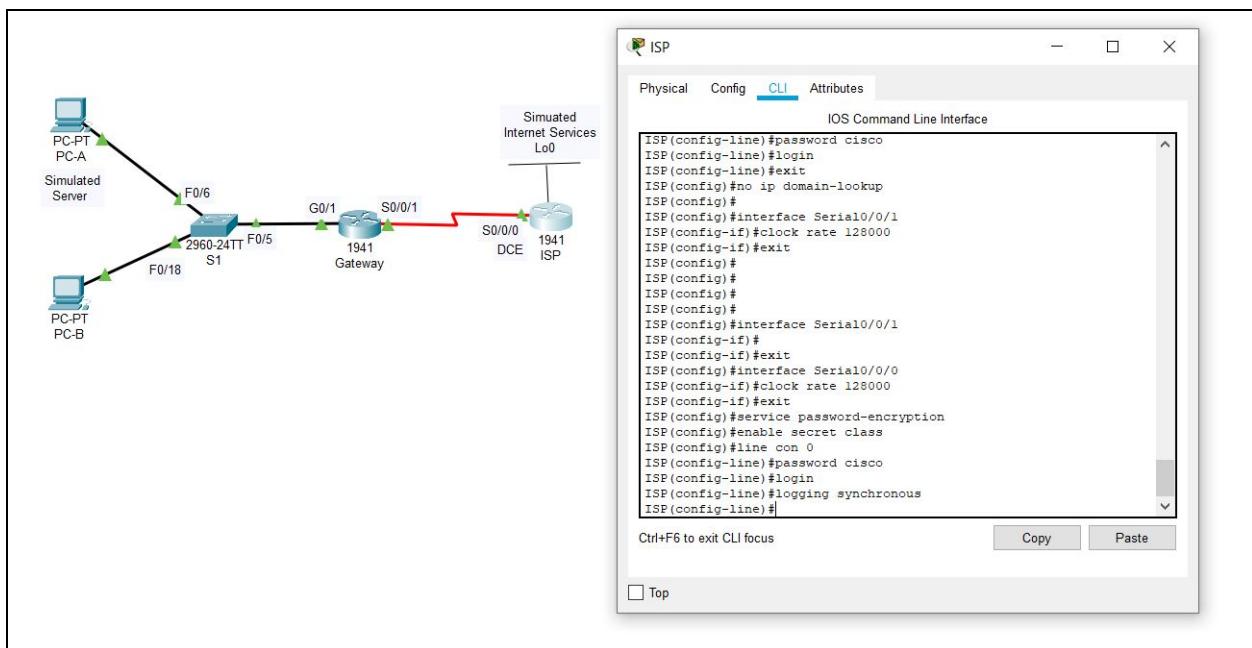


Assign class as encrypted privileged EXEC mode password as shown above.

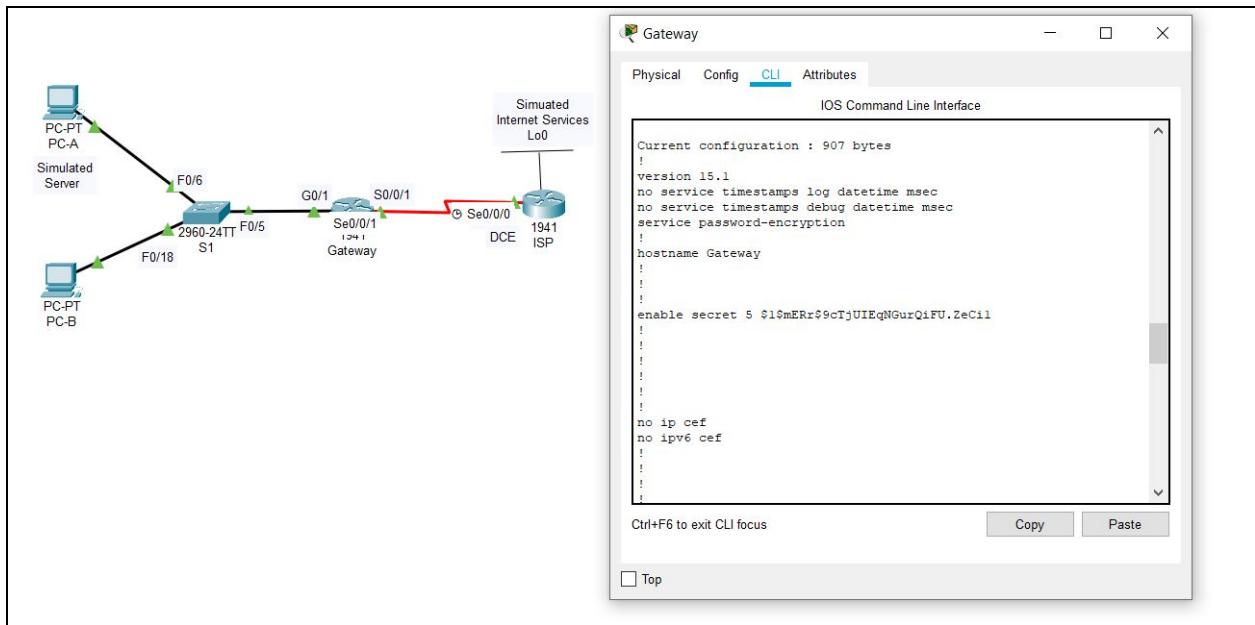
g. Configure logging synchronous to prevent console messages from interrupting the command entry



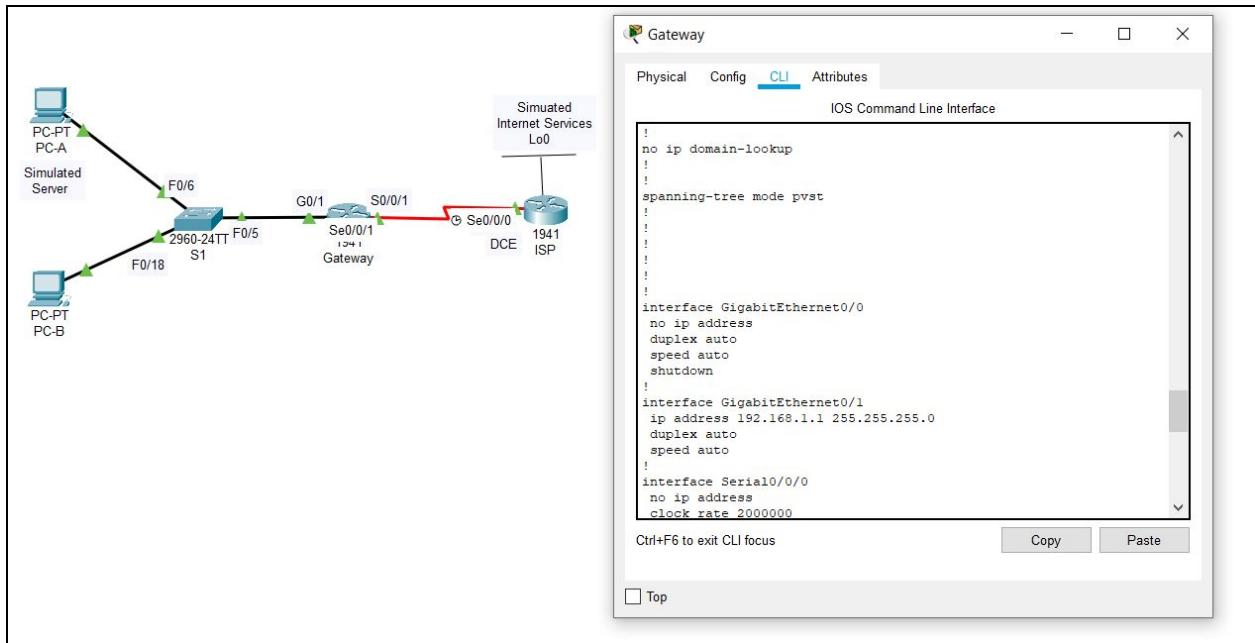
Configure logging synchronous to prevent console messages from interrupting the command entry as shown above



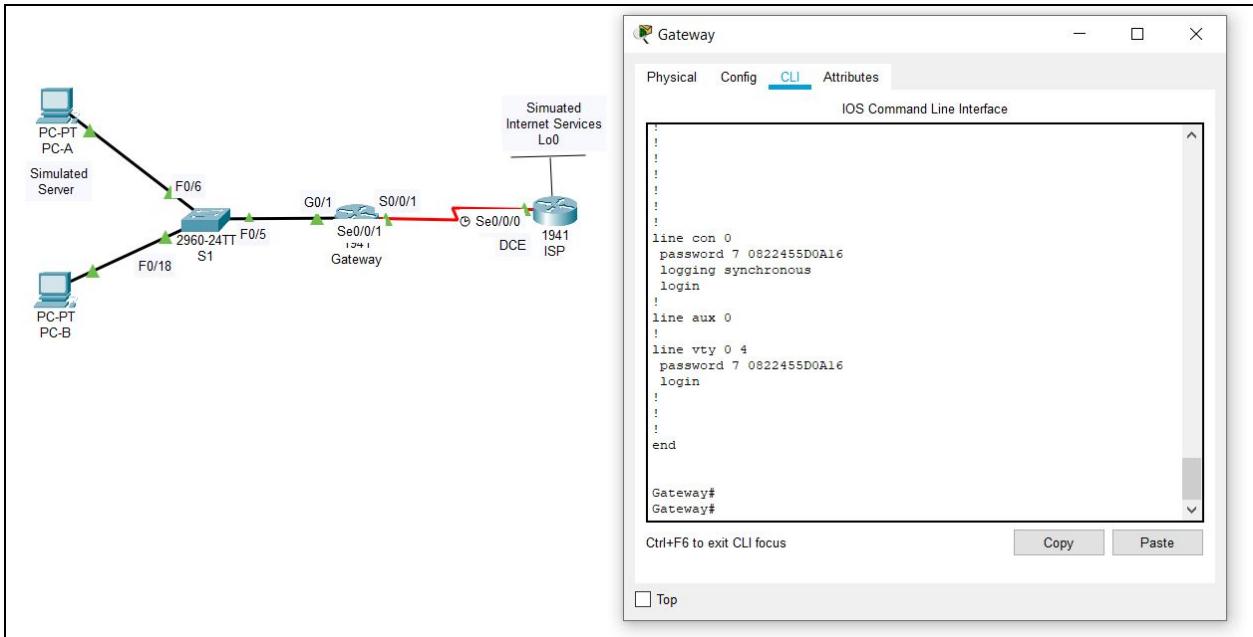
Configure logging synchronous to prevent console messages from interrupting the command entry as shown above



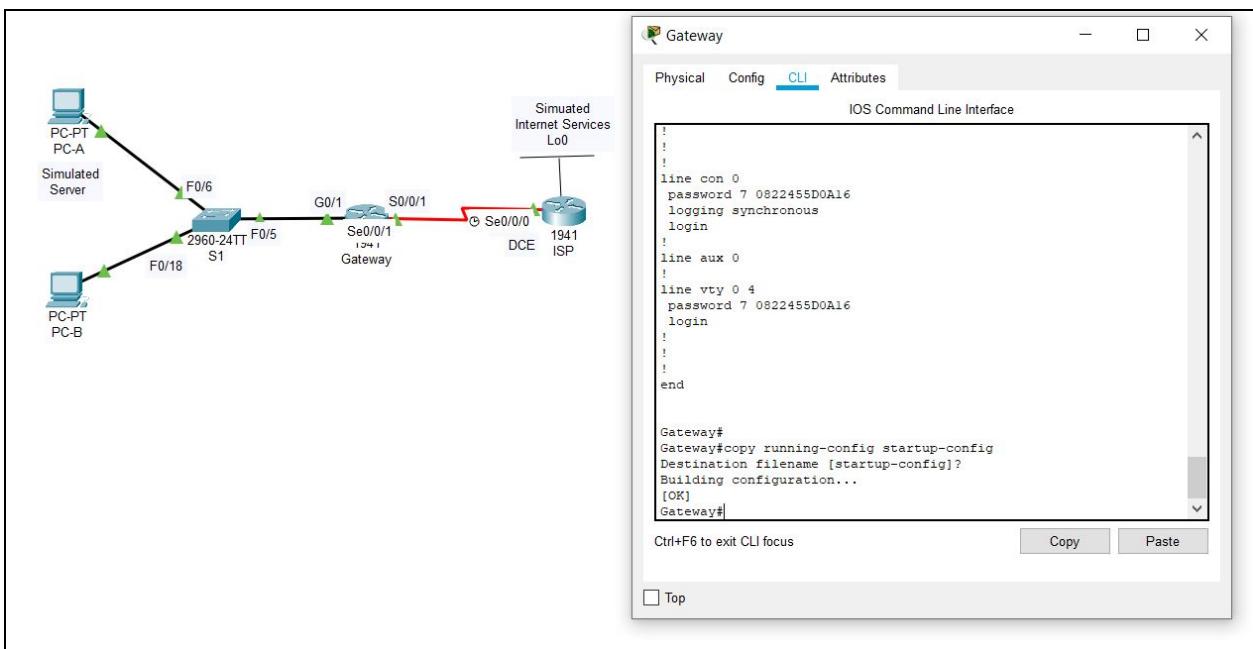
Show running configurations.



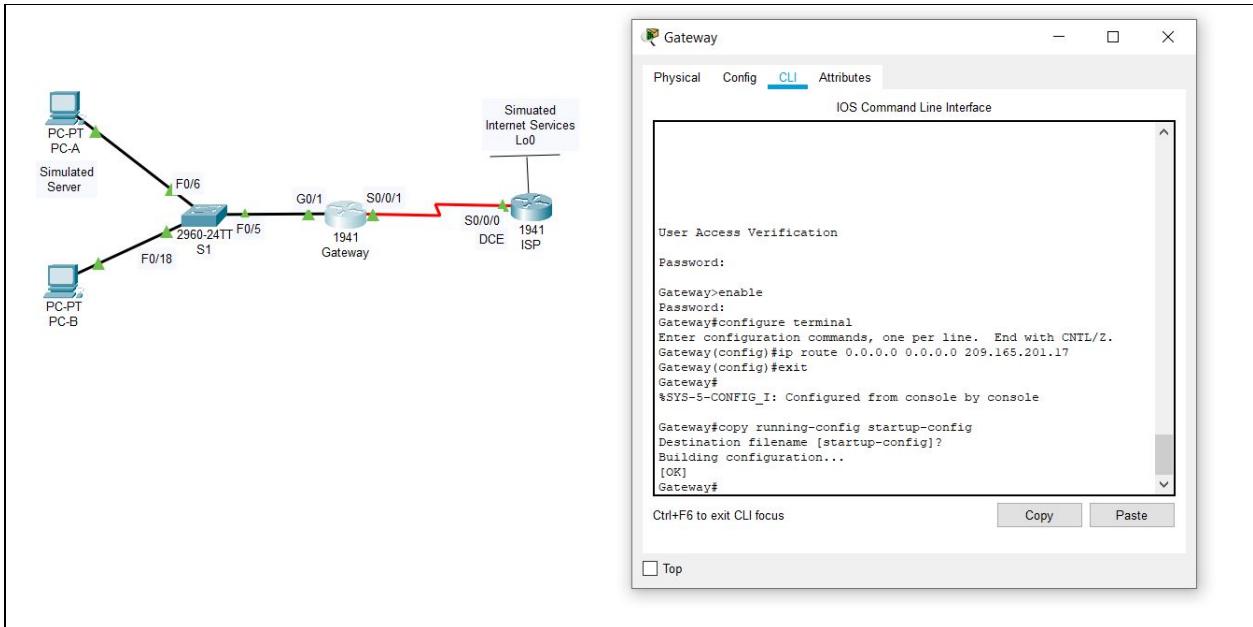
Show running configurations.



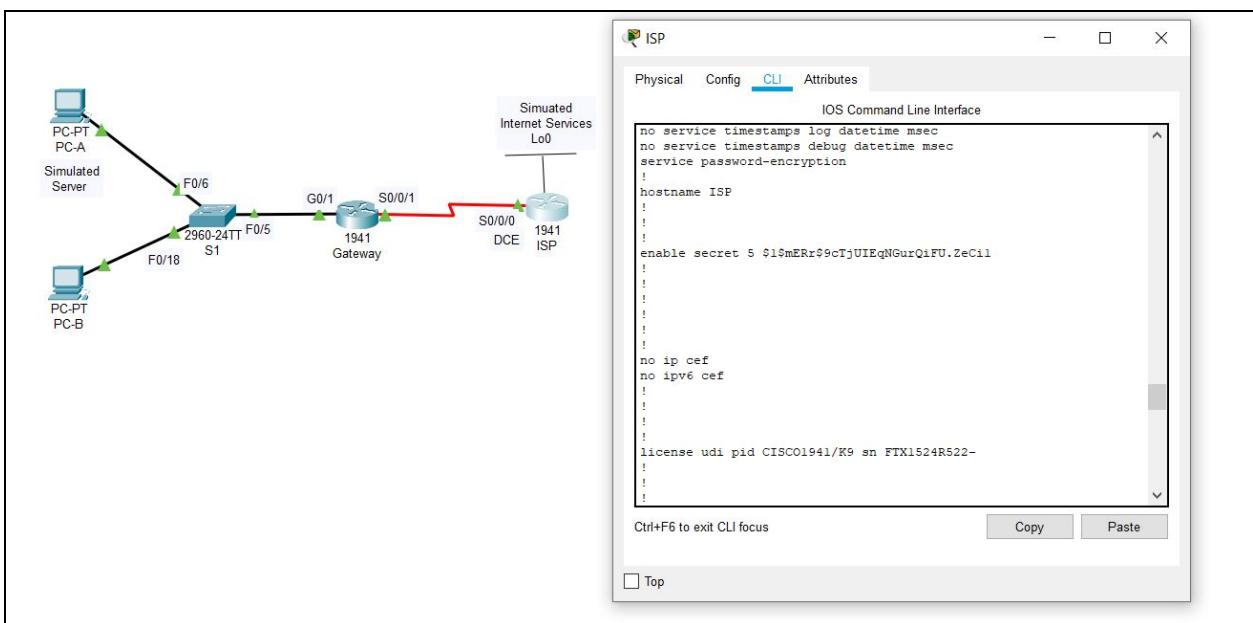
Show running configuration.



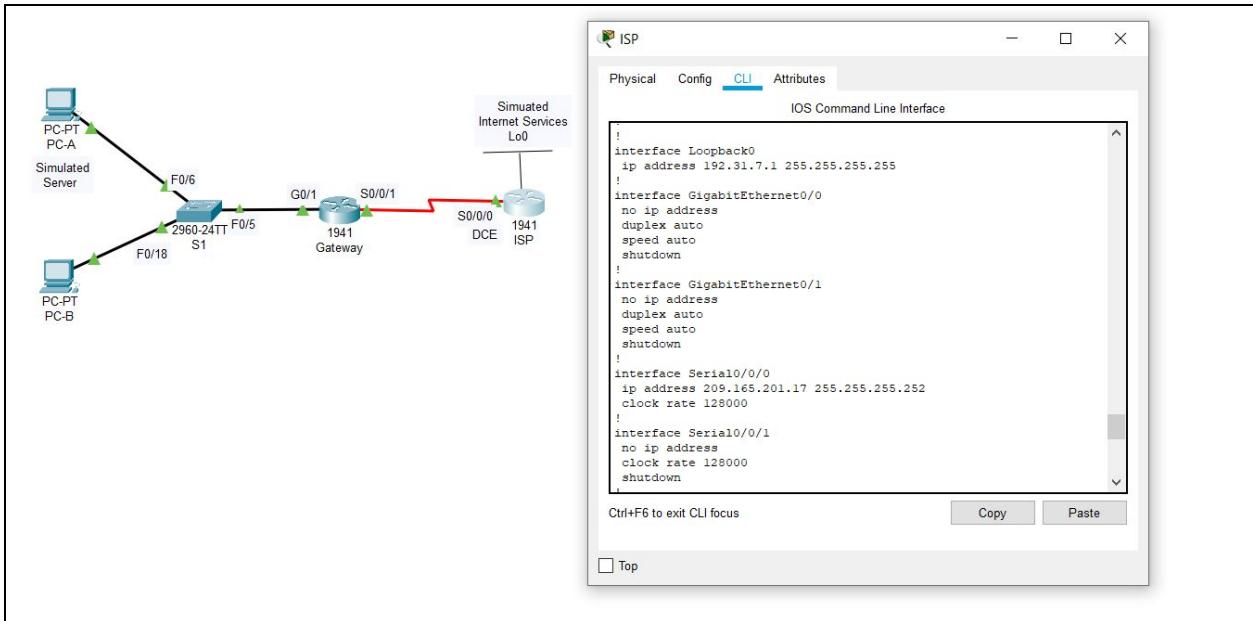
Show running configuration.



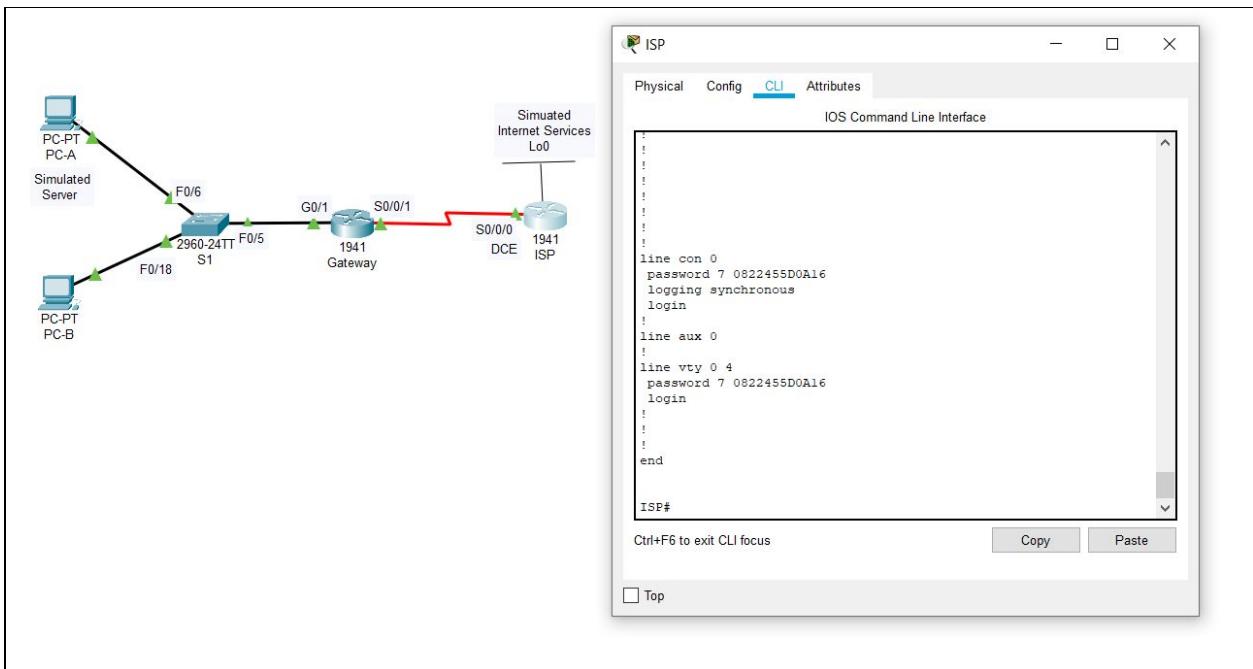
Copying running configuration to startup config



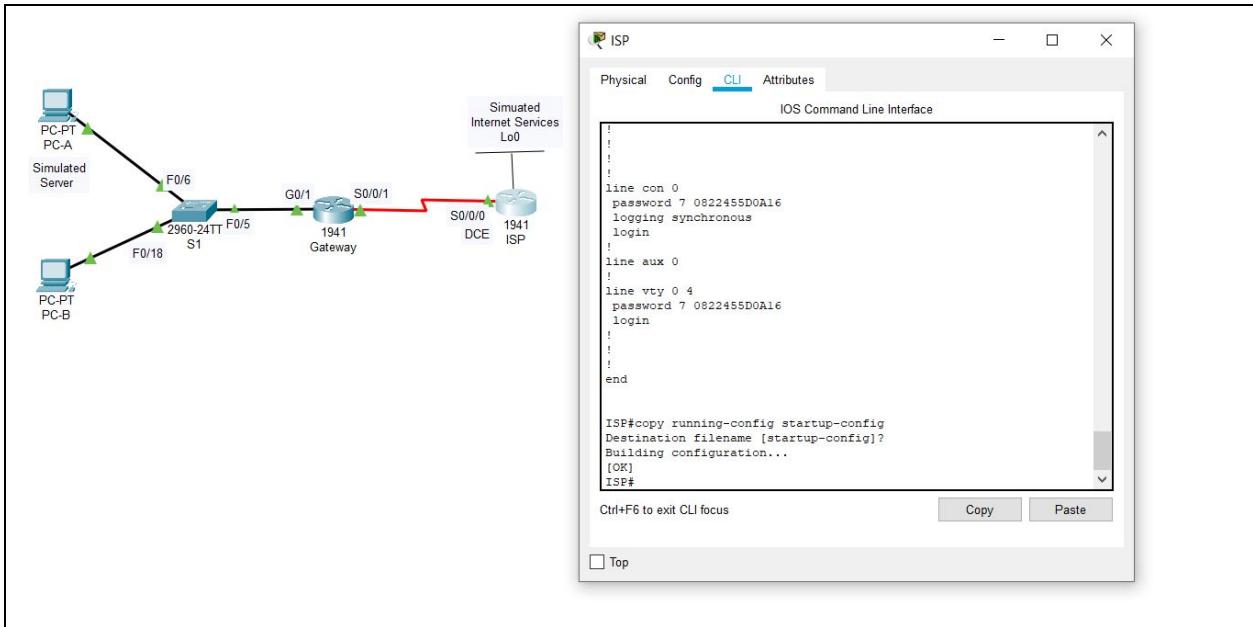
Show running configurations.



Show running configurations.



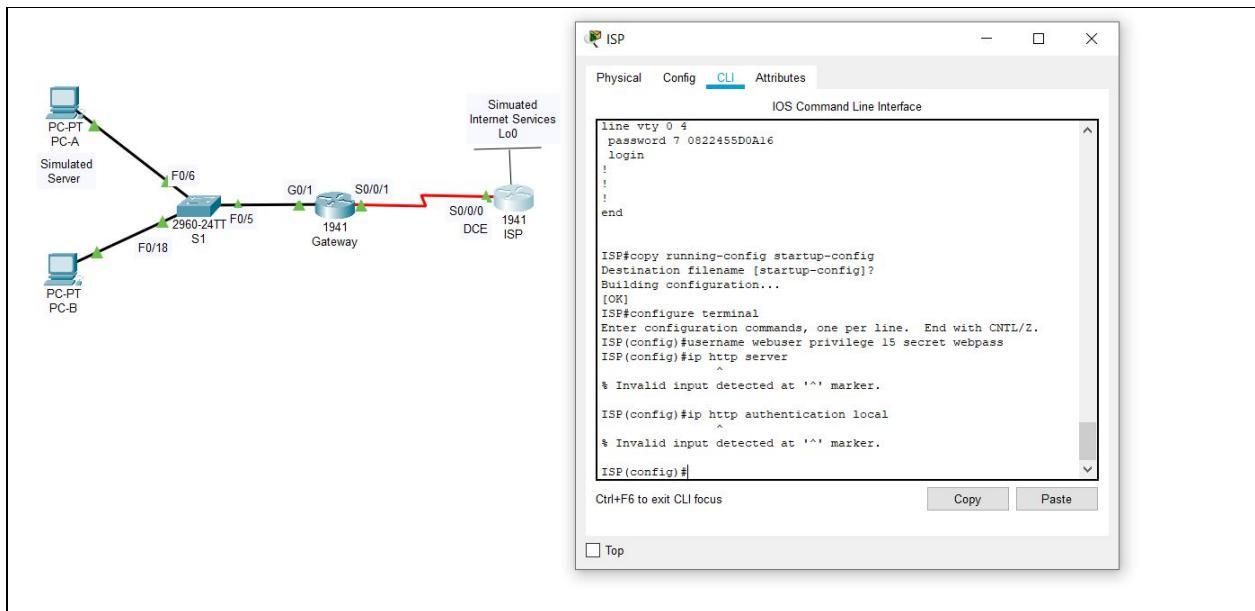
Show running configurations.



Copy running configuration to startup configuration.

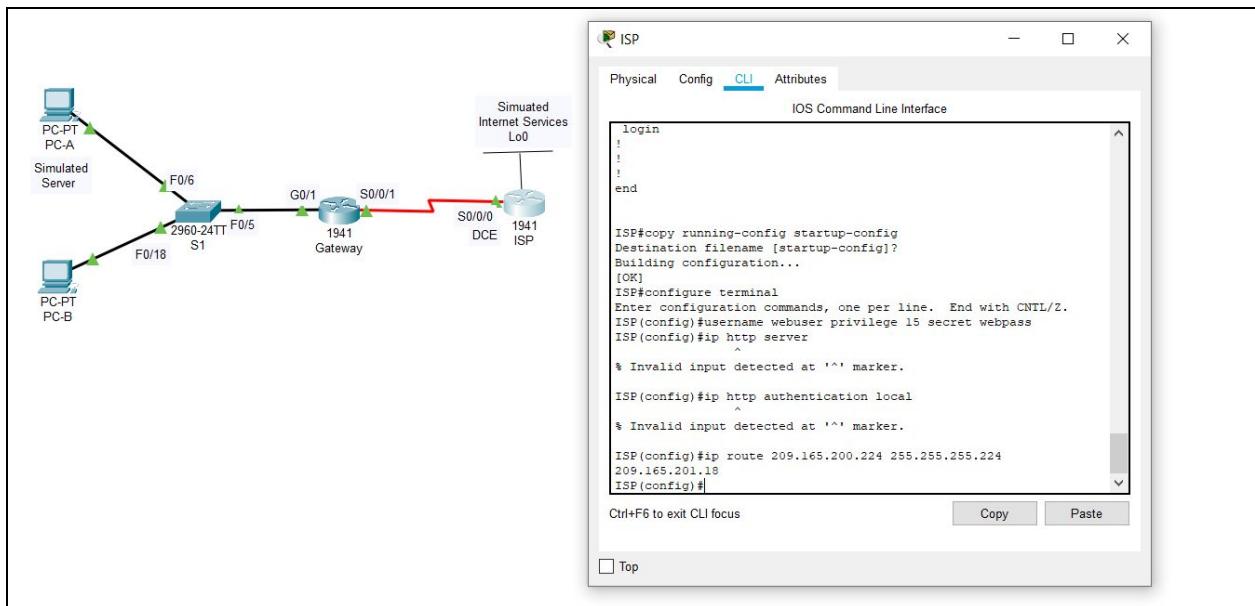
Step 5: Create a simulated web server on ISP.

- Create a local user named webuser with an encrypted password of webpass
- Enable the HTTP server service on ISP.
- Configure the HTTP service to use the local user database

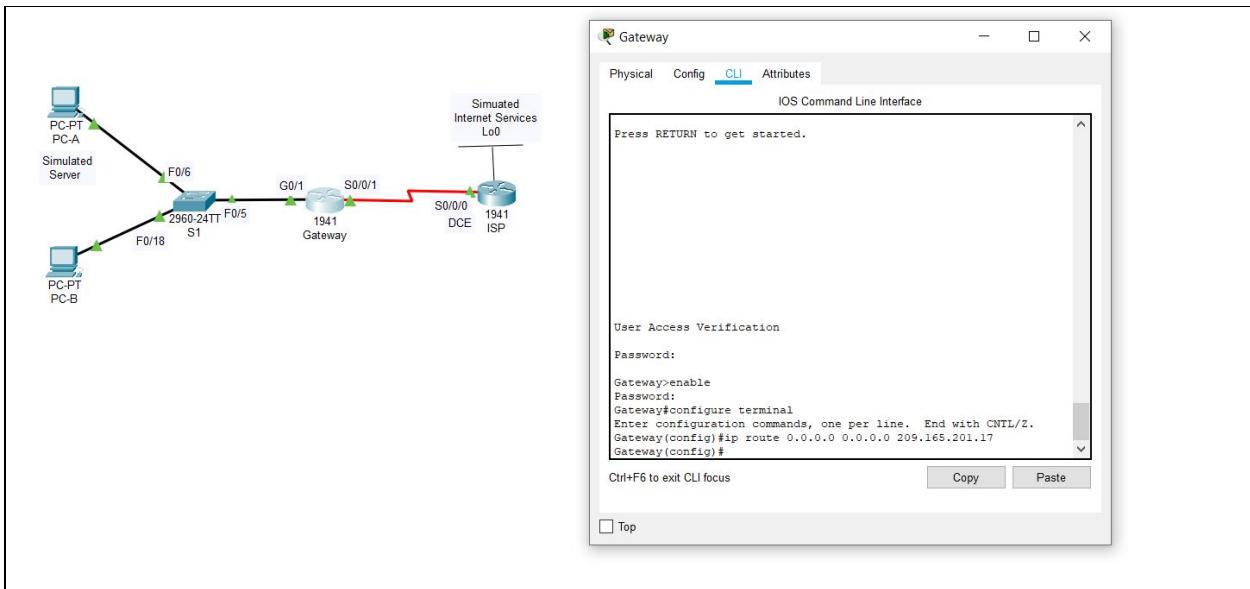


Step 6: Configure static routing

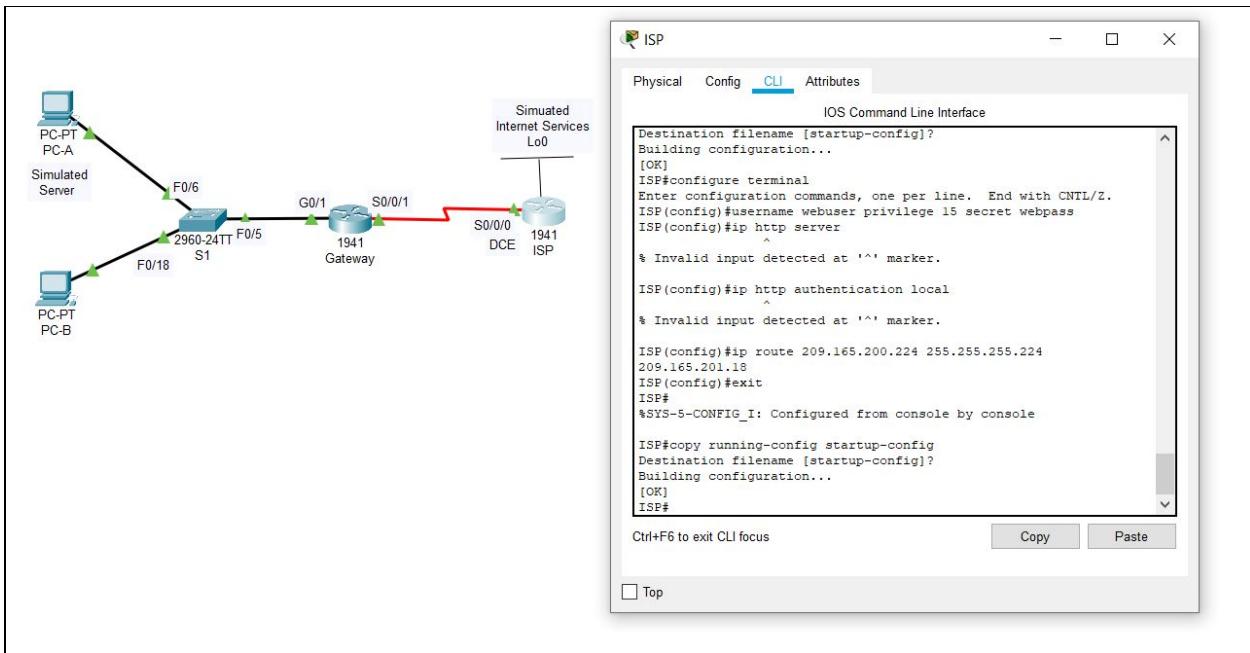
- a. Create a static route from the ISP router to the Gateway router using the assigned public network address range 209.165.200.224/27.



b. Create a default route from the Gateway router to the ISP router.



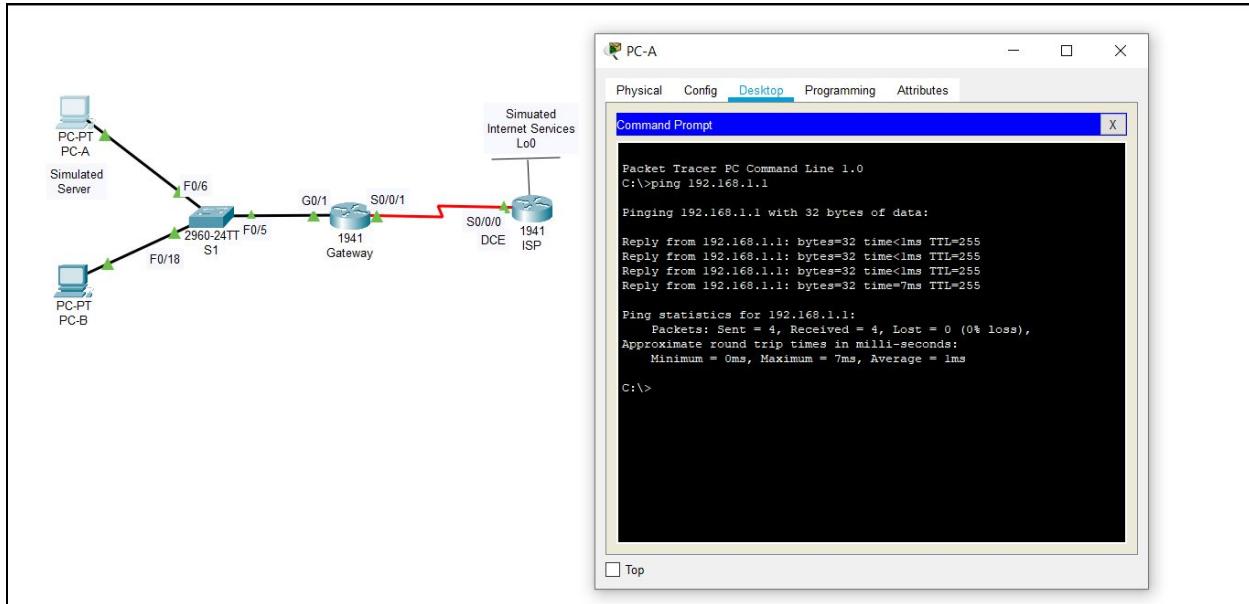
Step 7: Save the running configuration to the startup configuration.



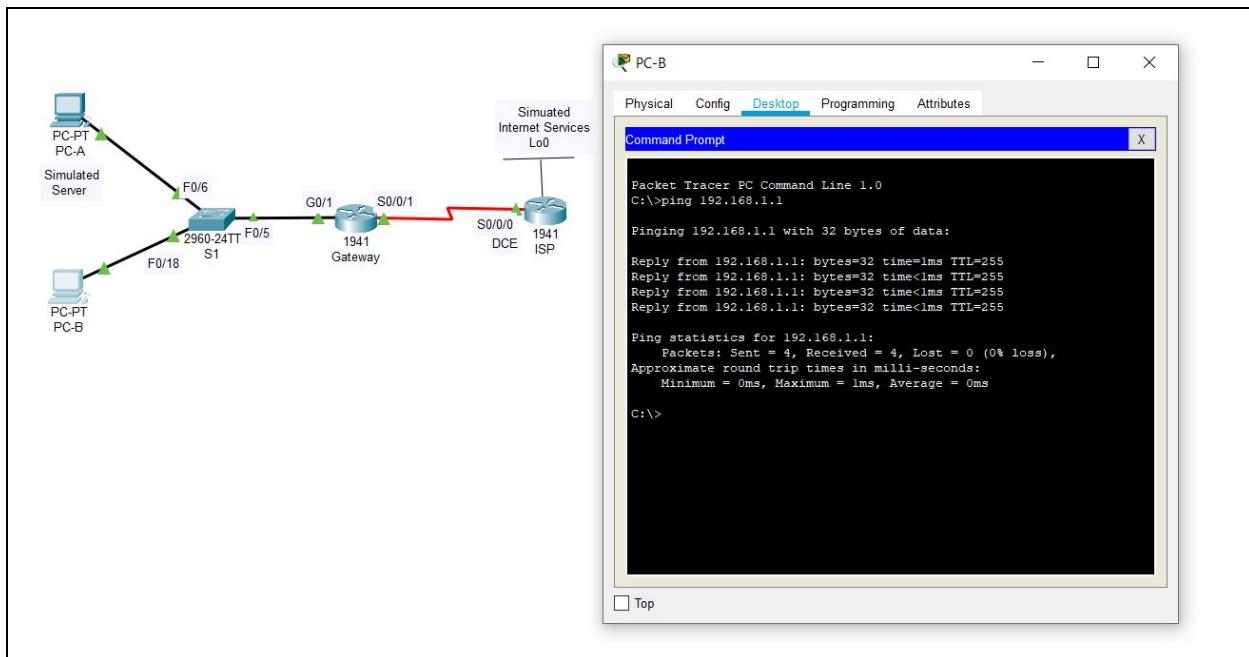
Step 8: Verify network connectivity.

- From the PC hosts, ping the G0/1 interface on the Gateway router. Troubleshoot if the pings are unsuccessful.

From PC-A pinging Gateway G0/1 interface as shown above.

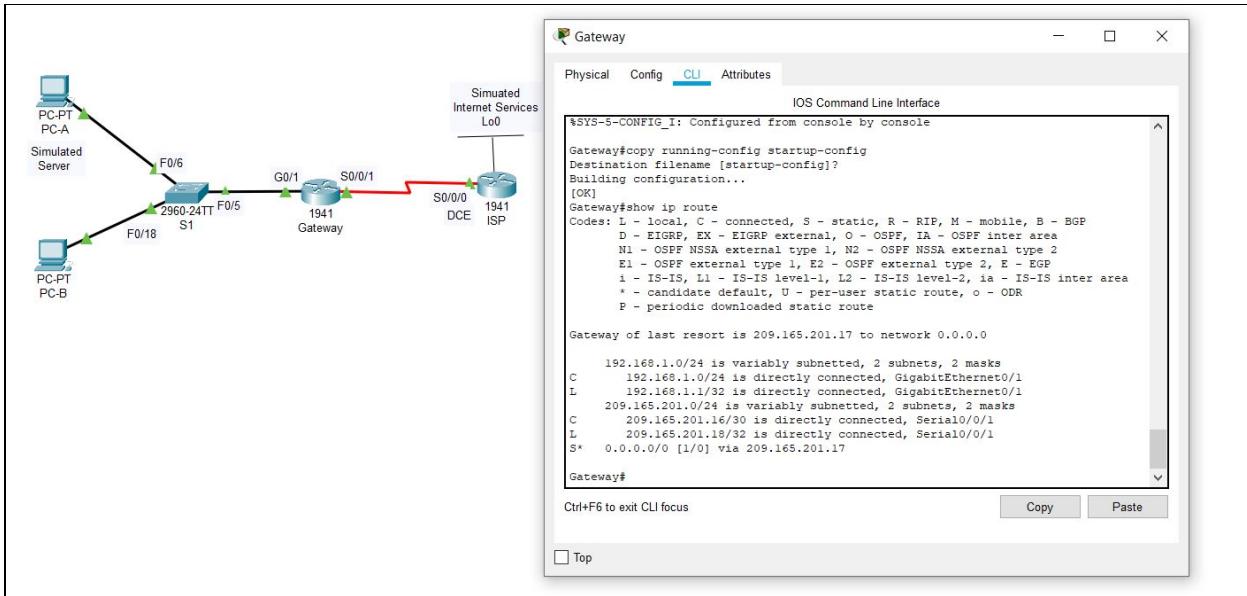


From PC-B pinging Gateway G0/1 interface as shown above.

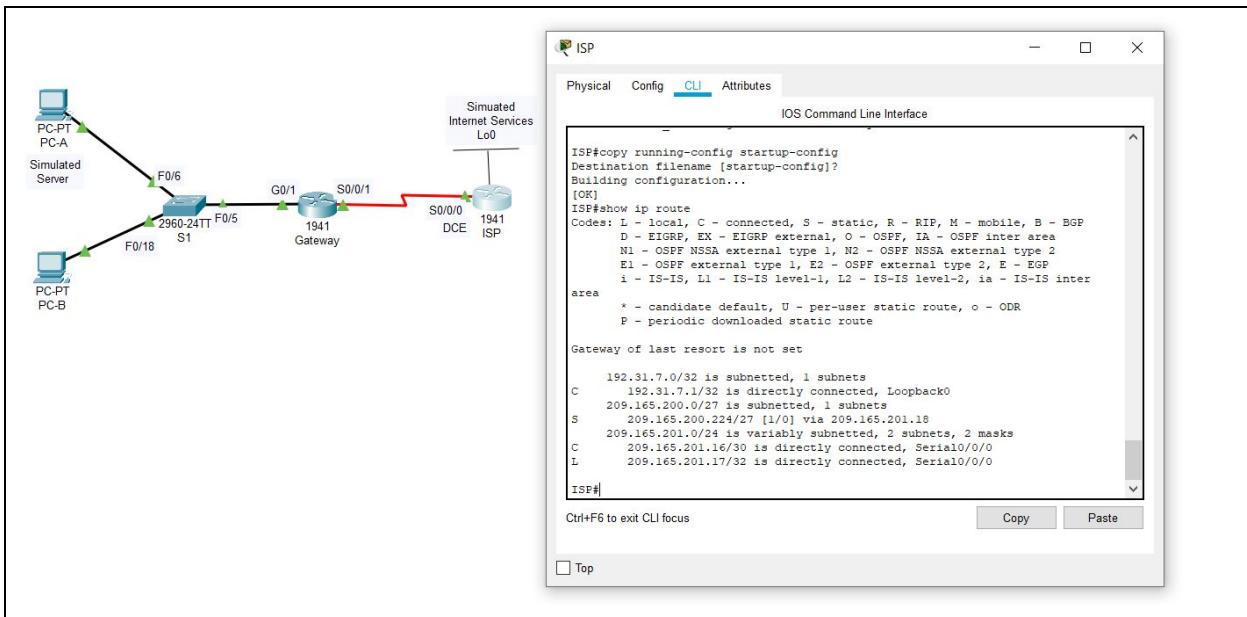


b. Display the routing tables on both routers to verify that the static routes are in the routing table and configured correctly on both routers.

Showing routing table of Gateway.



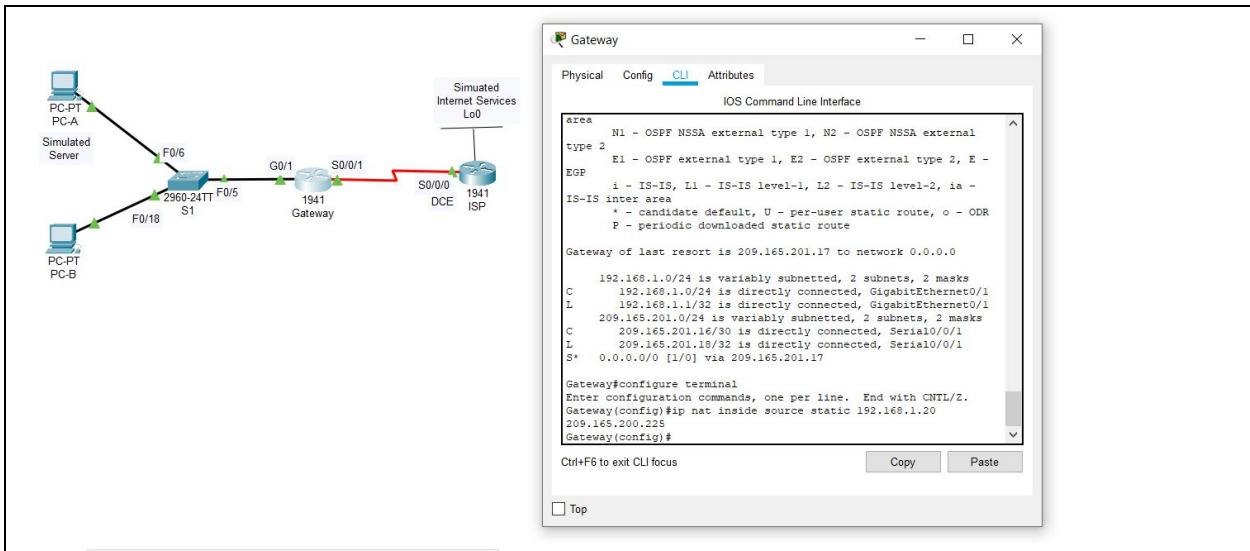
Showing routing table of ISP router.



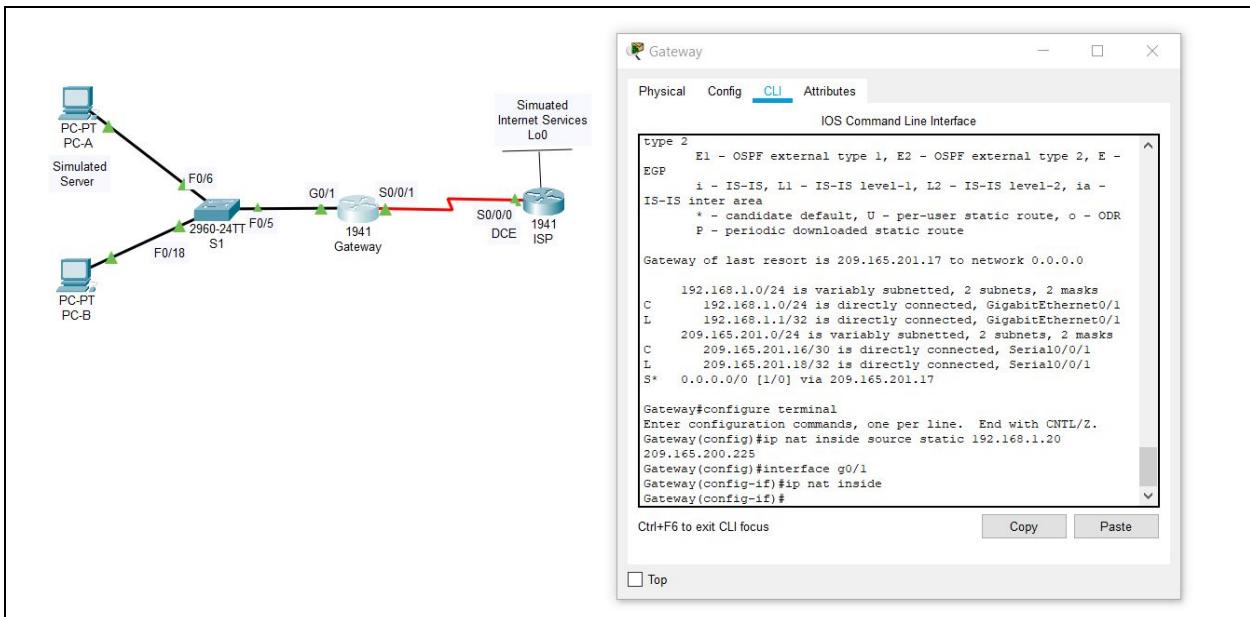
Task 2:

Step 1: Configure a static mapping.

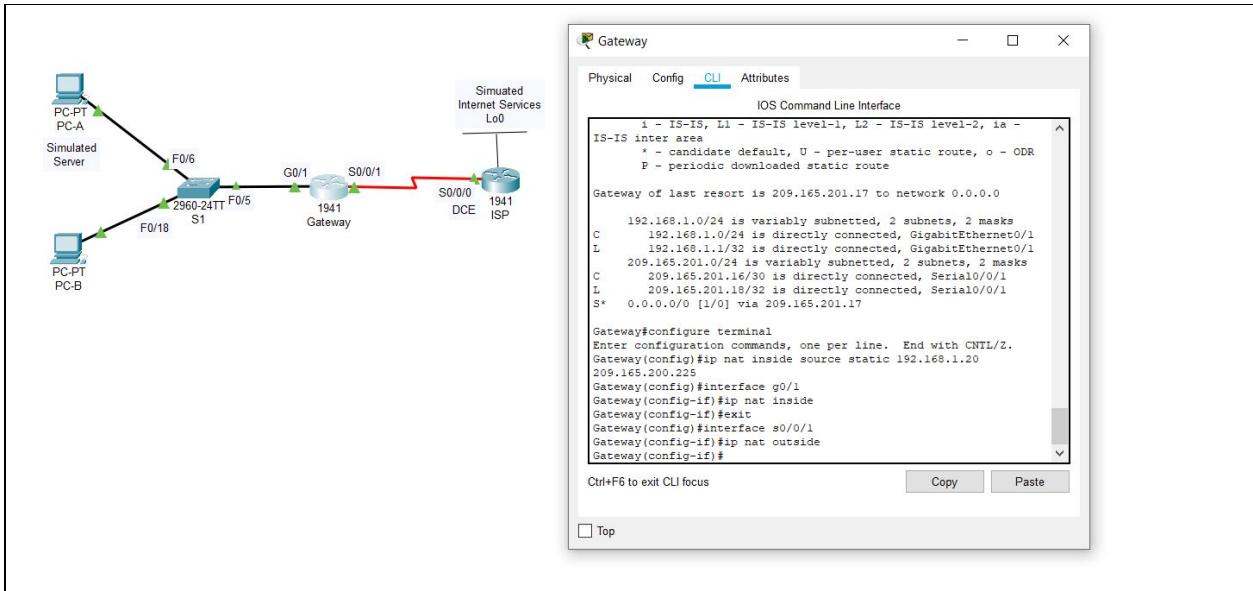
Configuring static mapping in gateway router to translate between private inside server address 192.168.1.20 and the public address 209.165.200.225.



Step 2: Specify the interfaces.



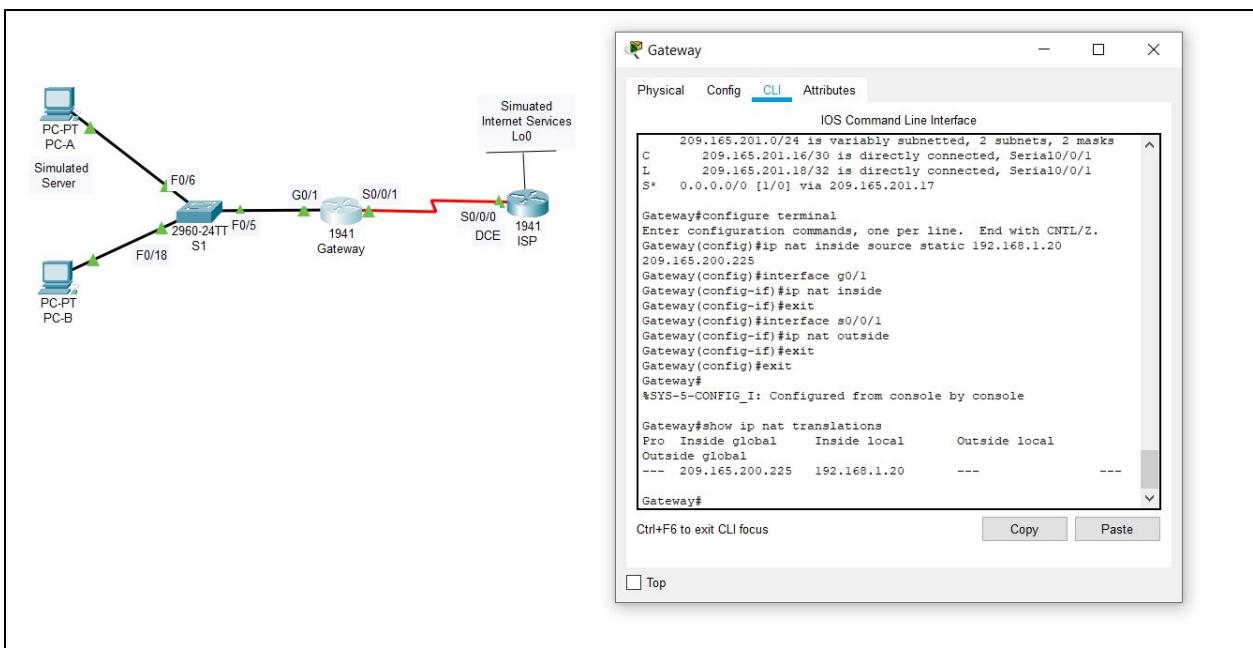
Issue the ip nat inside command to the interface g0/1



Issue the ip nat outside command to the interface S0/0/1

Step 3: Test the configuration

- Display the static NAT table by issuing the show ip nat translations command.



Showing the nat translations in Gateway.

What is the translation of the Inside local host address?

Answer :

192.168.1.20 = 209.165.200.225

The Inside global address is assigned by?

Answer :

Static - ISP

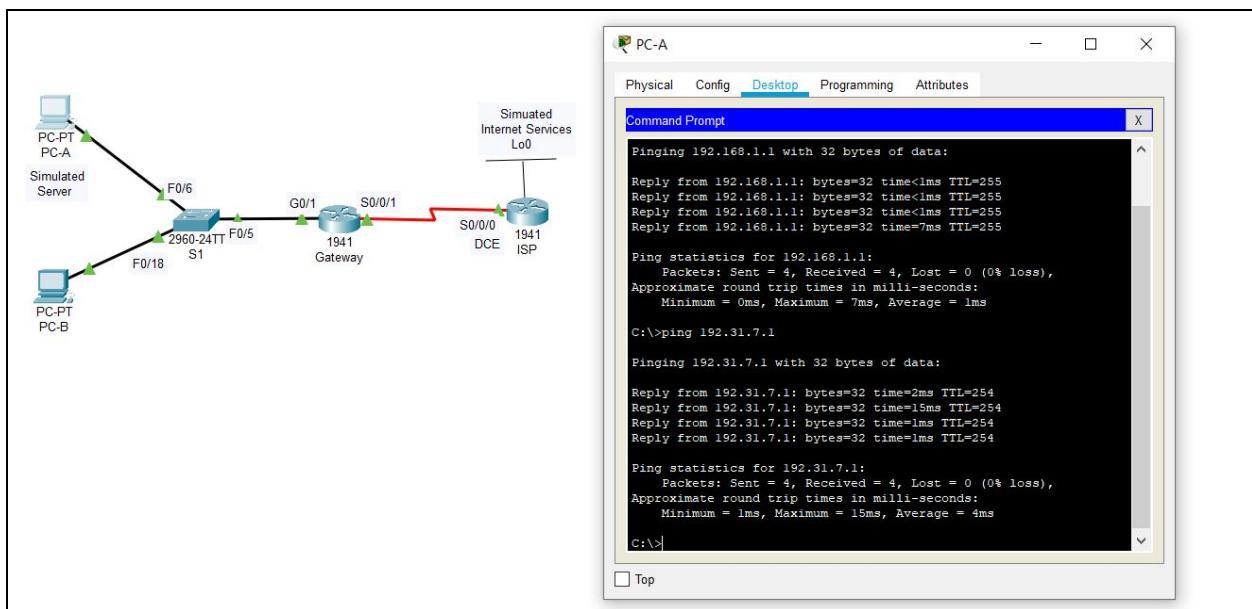
Dynamic - NAT Pool

The Inside local address is assigned by?

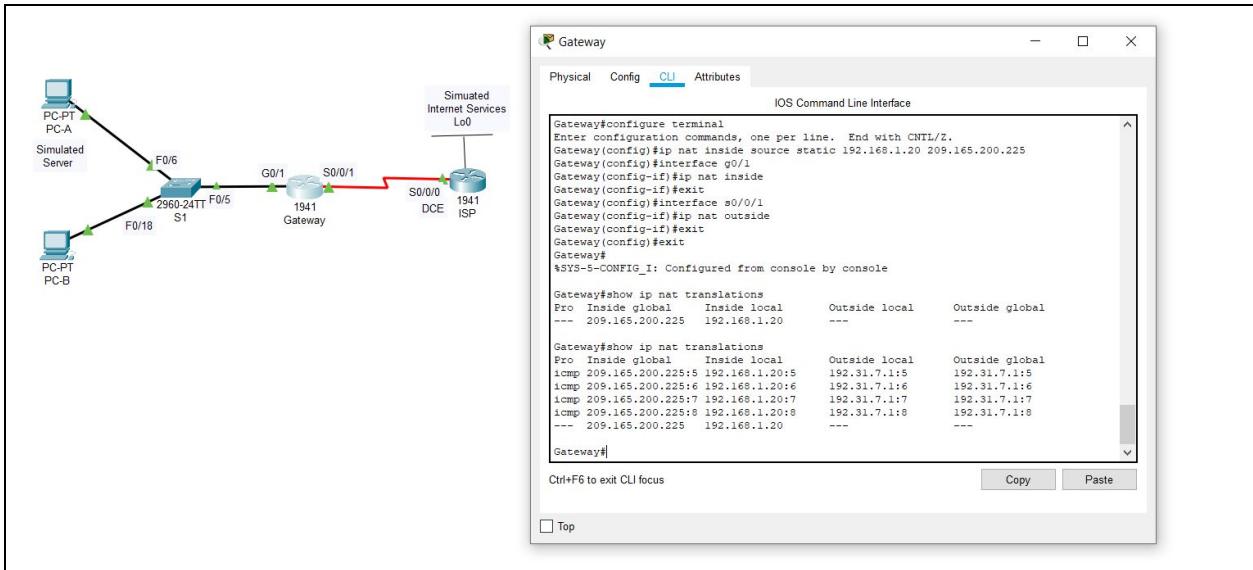
Answer :

System Administrator

b. From PC-A, ping the Lo0 interface (192.31.7.1) on ISP. If the ping was unsuccessful, troubleshoot and correct the issues. On the Gateway router, display the NAT table.



From PC-A, pinging the Lo0 interface (192.31.7.1) on ISP as shown above



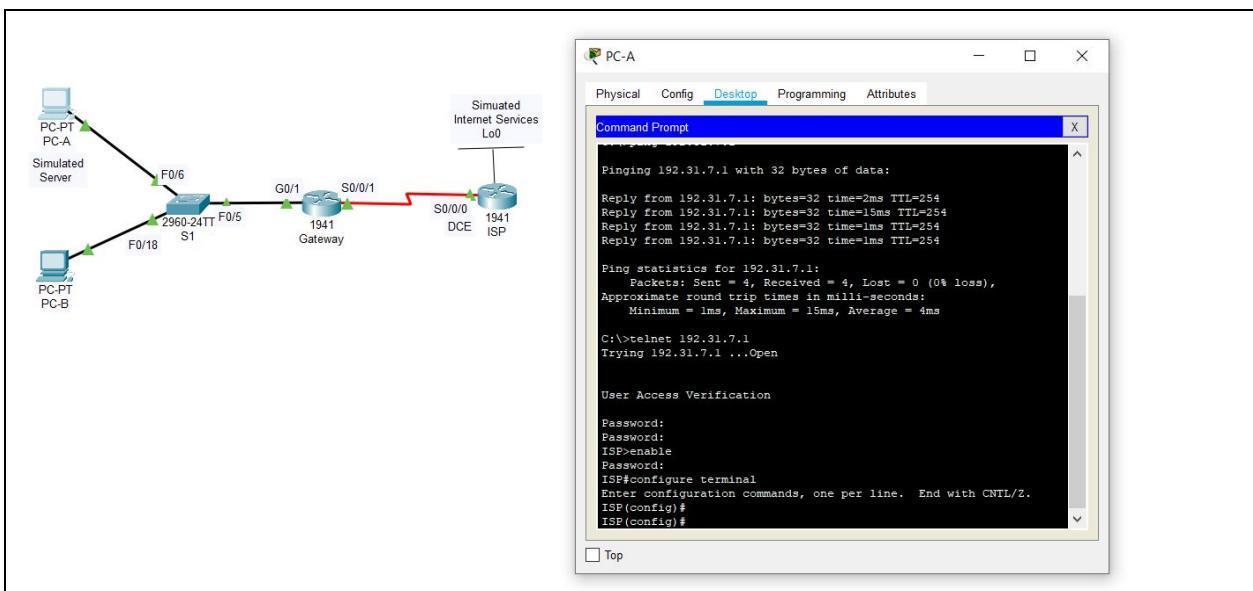
Showing nat translations in Gateway router after pinging as shown above.

What port number was used in this ICMP exchange?

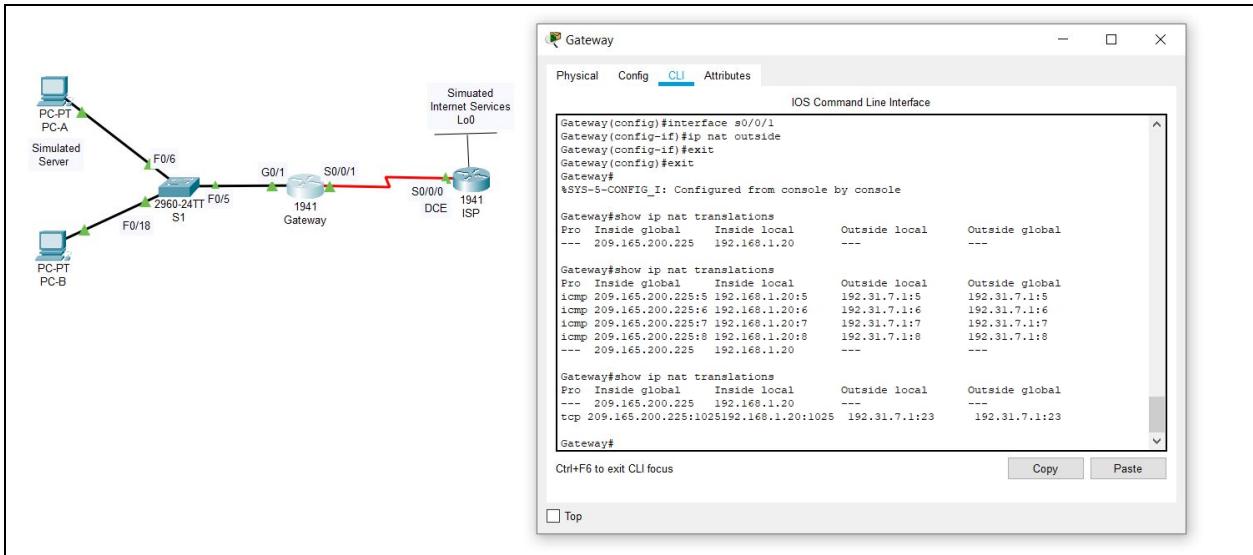
Answer :

5,6,7,8

c. From PC-A, telnet to the ISP Lo0 interface and display the NAT table.



From PC-A, telnet to the ISP Lo0 interface as shown above.



Displaying the nat table in Gateway after telnet

What was the protocol used in this translation?

Answer :

TCP

What are the port numbers used?

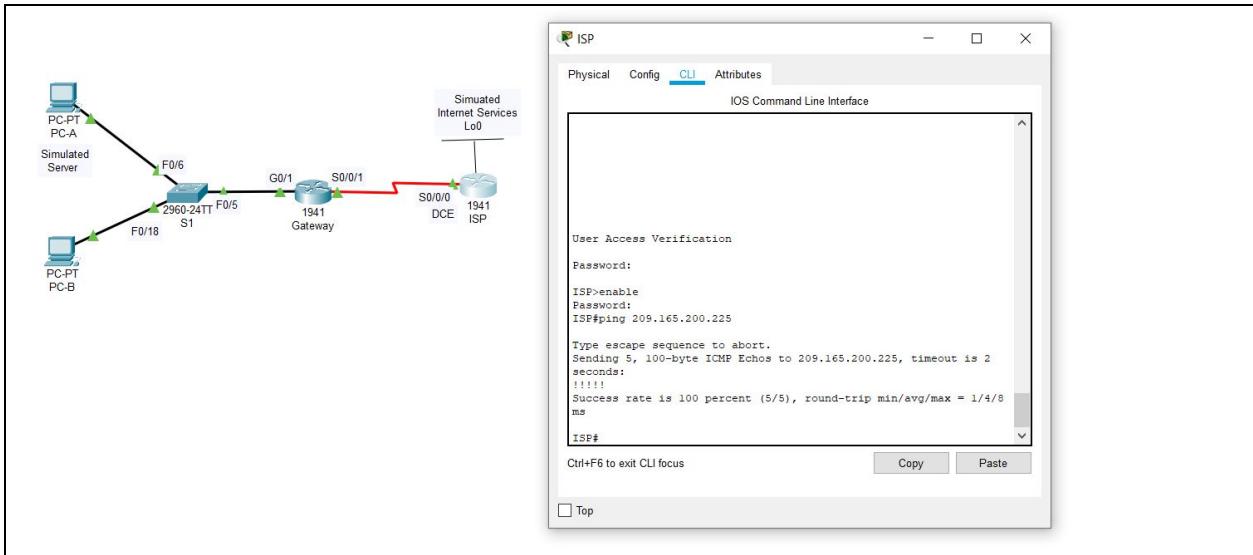
Inside global / local:

1025

Outside global / local:

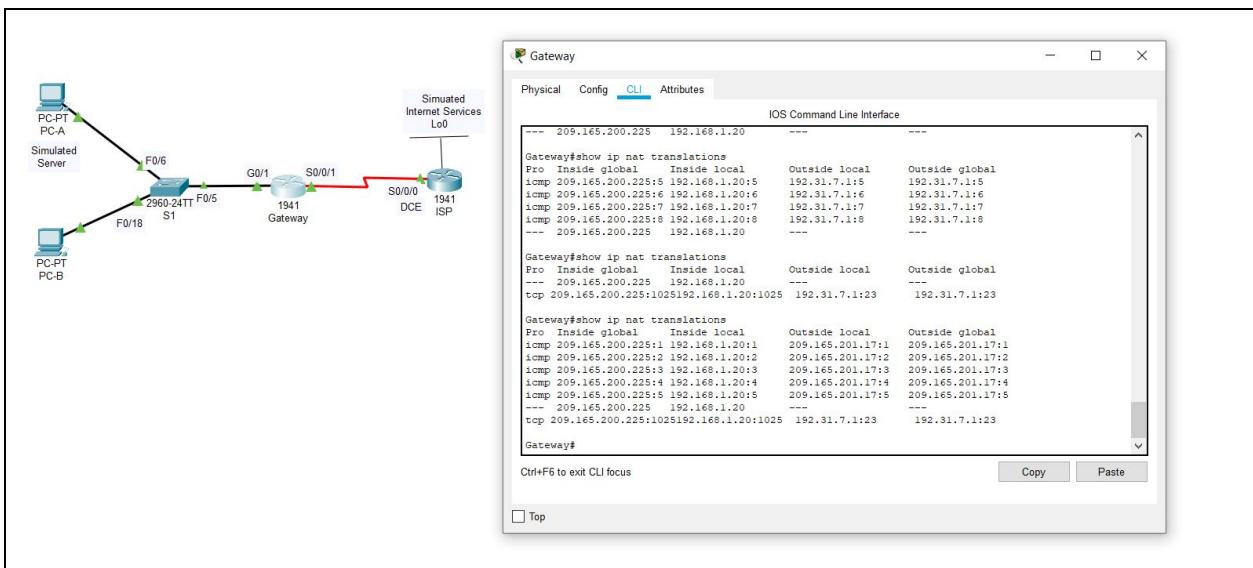
23 (Telnet port)

d. Because static NAT was configured for PC-A, verify that pinging from ISP to PC-A at the static NAT public address (209.165.200.225) is successful.



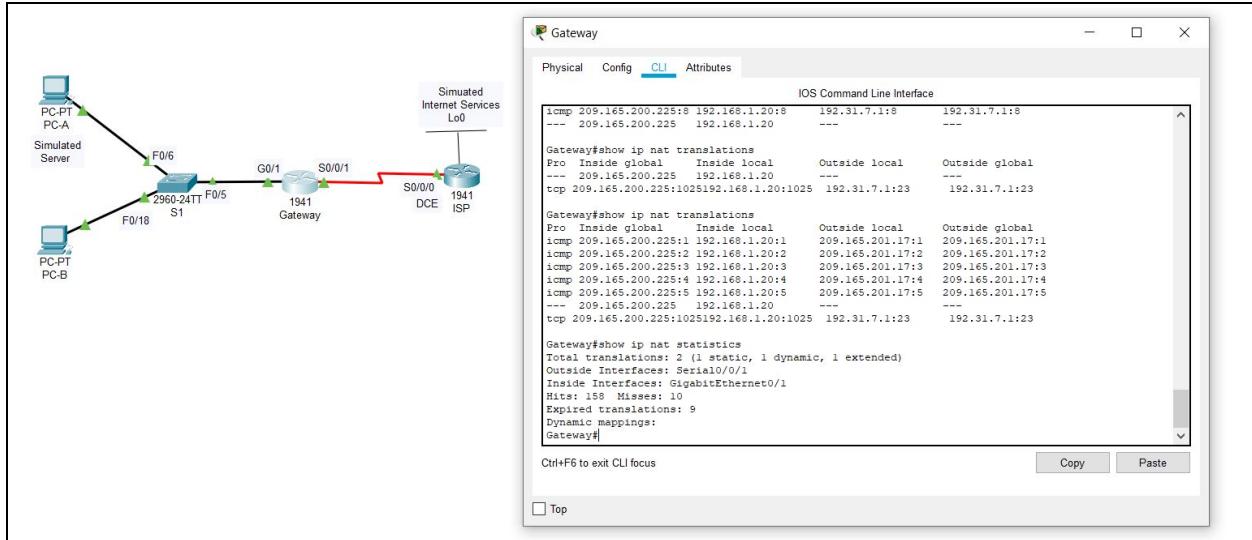
Pinging from ISP to PC-A at the static NAT public address (209.165.200.225)
As shown above.

e. On the Gateway router, display the NAT table to verify the translation.



On the Gateway router, display the NAT table to verify the translation as shown above.

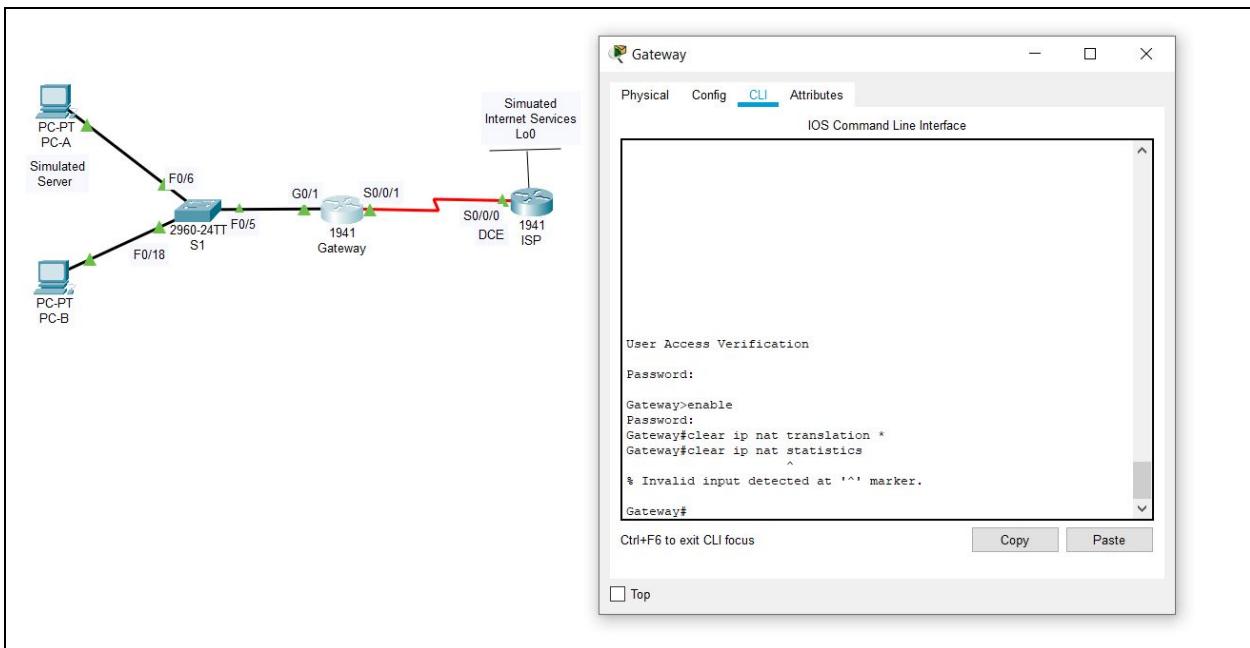
f. Verify NAT statistics by using the show ip nat statistics command on the Gateway router.



Verify NAT statistics by using the show ip nat statistics command on the Gateway router.

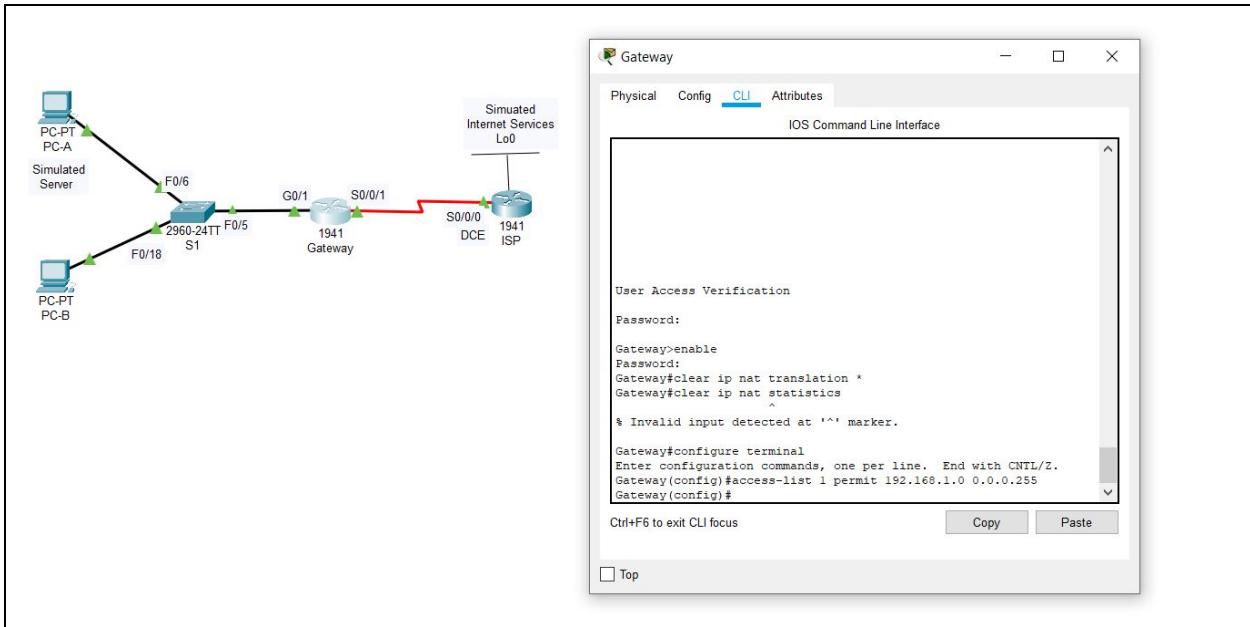
Task 3

Step 1: Clear NATs.



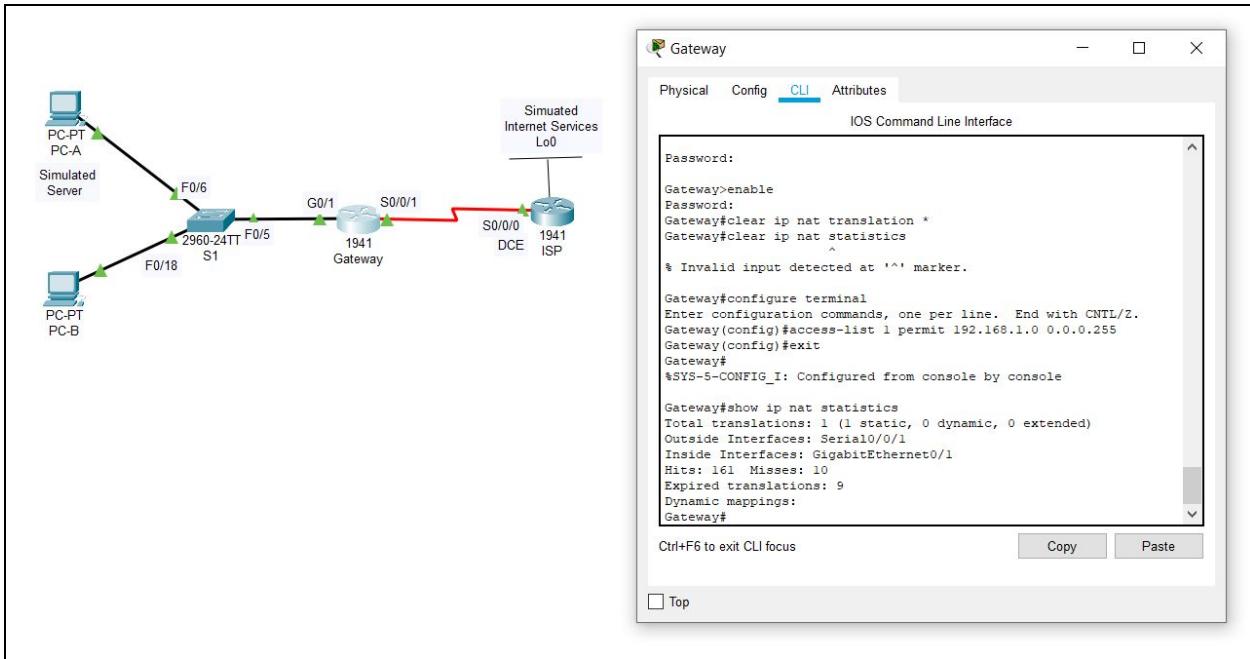
Before proceeding to add dynamic NATs, clear the NATs and statistics from Part 2 as shown above

Step 2: Define an access control list (ACL) that matches the LAN private IP address range



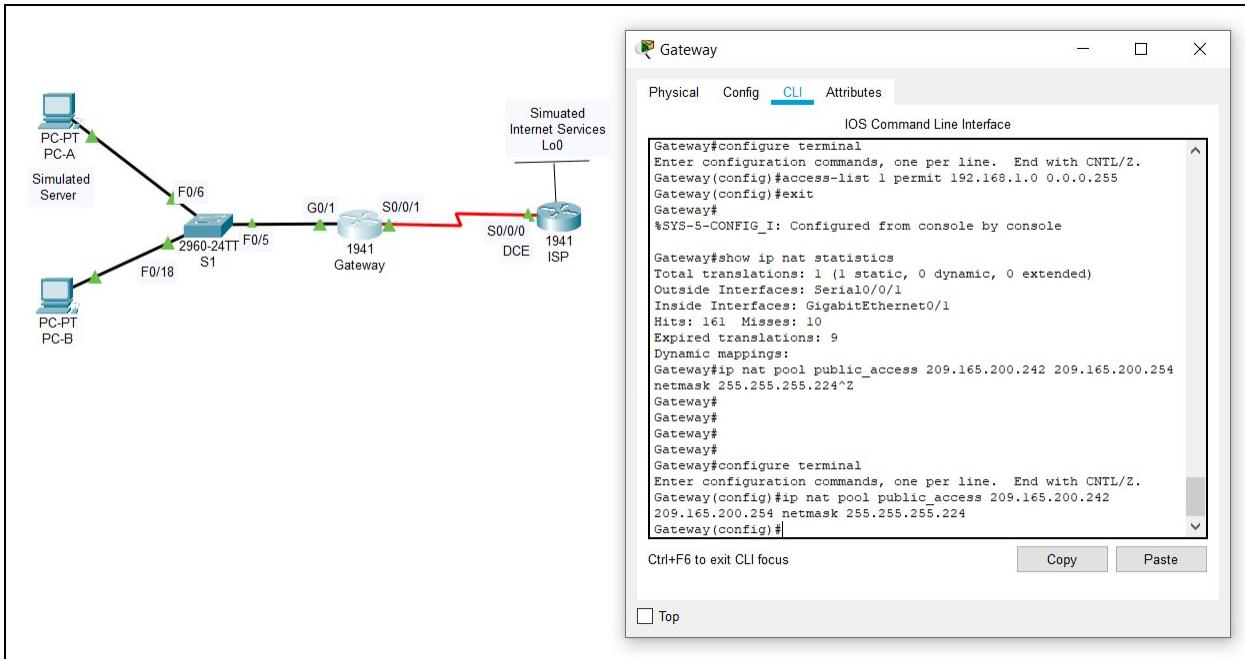
Access List 1 is used to allow 192.168.1.0/24 network to be translated as shown above.

Step 3: Verify that the NAT interface configurations are still valid.

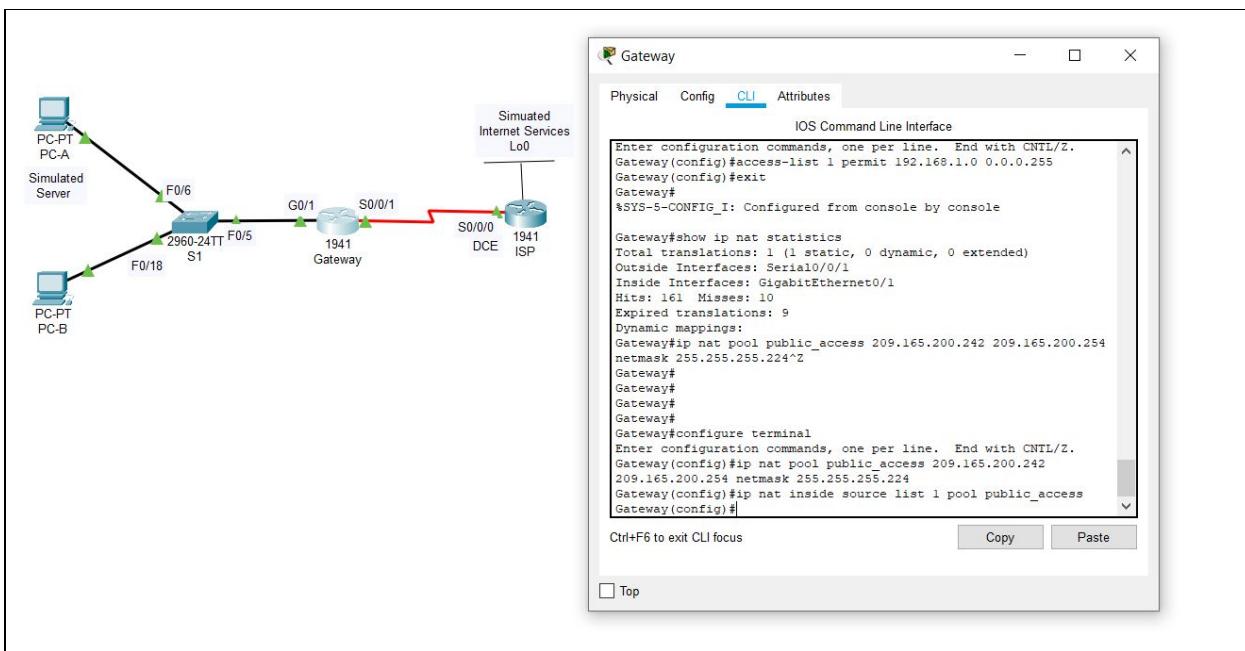


Showing the network

Step 4: Define the pool of usable public IP addresses.

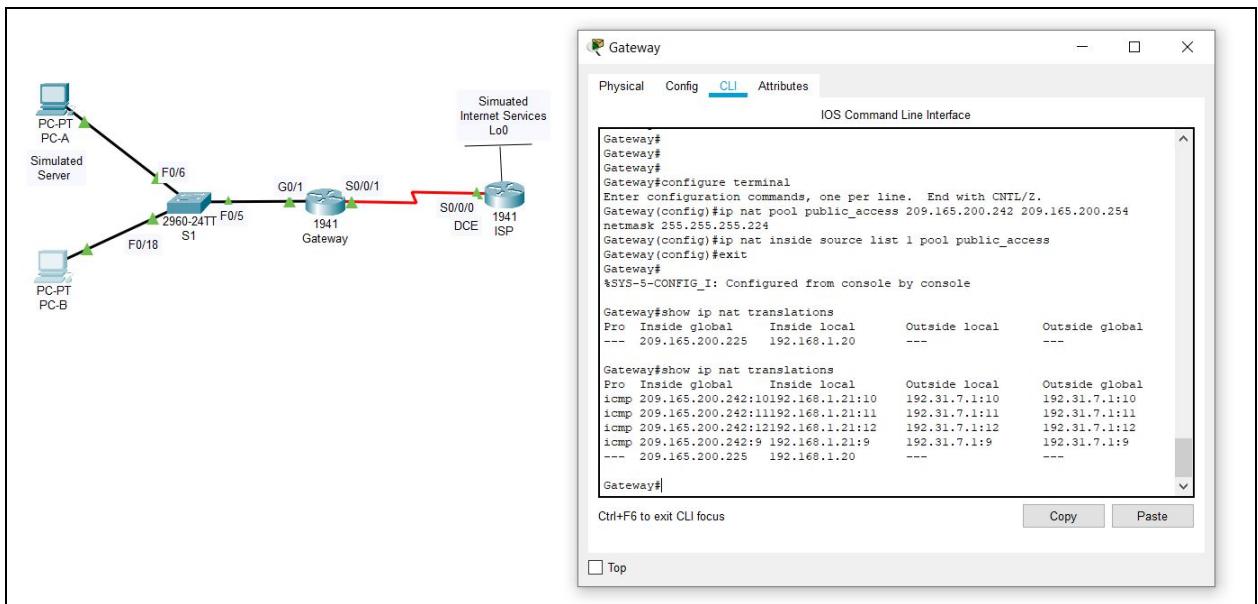
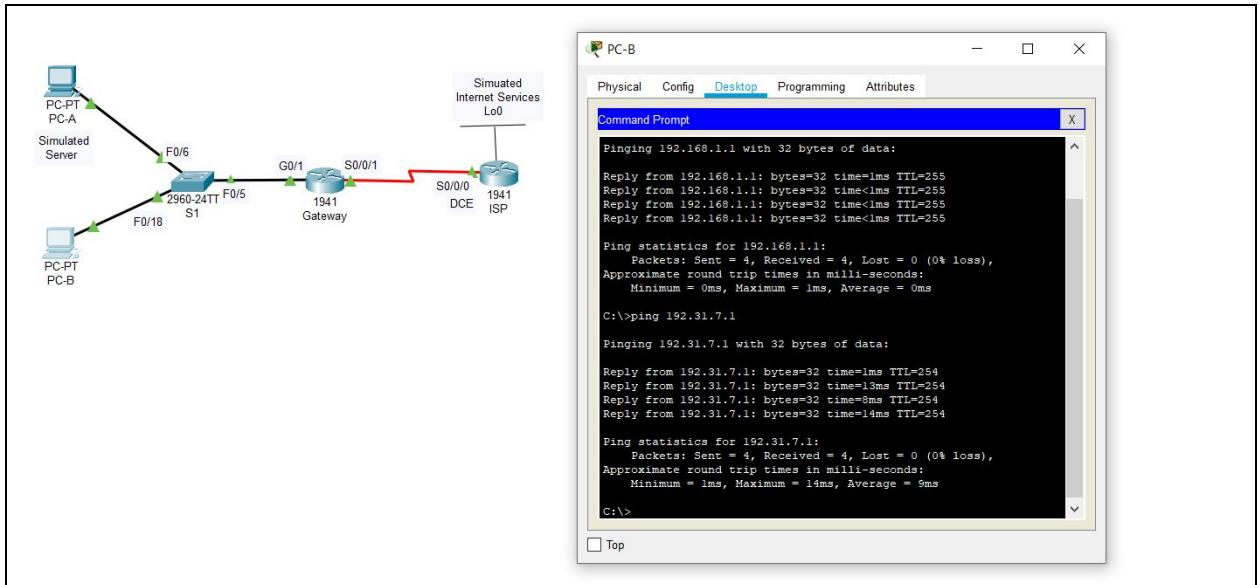


Step 5: Define the NAT from the inside source list to the outside pool.



Step 6: Test the configuration.

- From PC-B, ping the Lo0 interface (192.31.7.1) on ISP. If the ping was unsuccessful, troubleshoot and correct the issues. On the Gateway router, display the NAT table.



What is the translation of the Inside local host address for PC-B?

192.168.1.21

Ans: 209.165.200.242

A dynamic NAT entry was added to the table with ICMP as the protocol when PC-B sent an ICMP message to 192.31.7.1 on ISP.

What port number was used in this ICMP exchange?

Ans: 10, 11, 12, 9

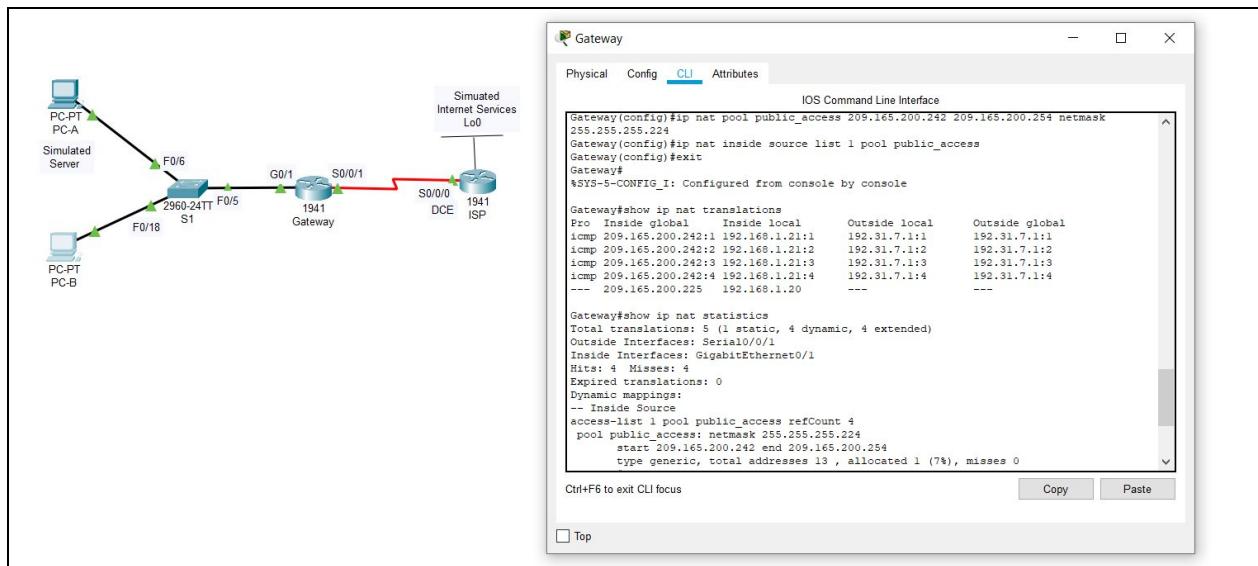
2. From PC-B, open a browser and enter the IP address of the ISP-simulated web server (Lo0 interface). When prompted, log in as webuser with a password of webpass.

We couldn't implement as HTTP server was not supported

3. Display the NAT table.

We couldn't implement as HTTP server was not supported

4. Verify NAT statistics by using the show ip nat statistics command on the Gateway router.

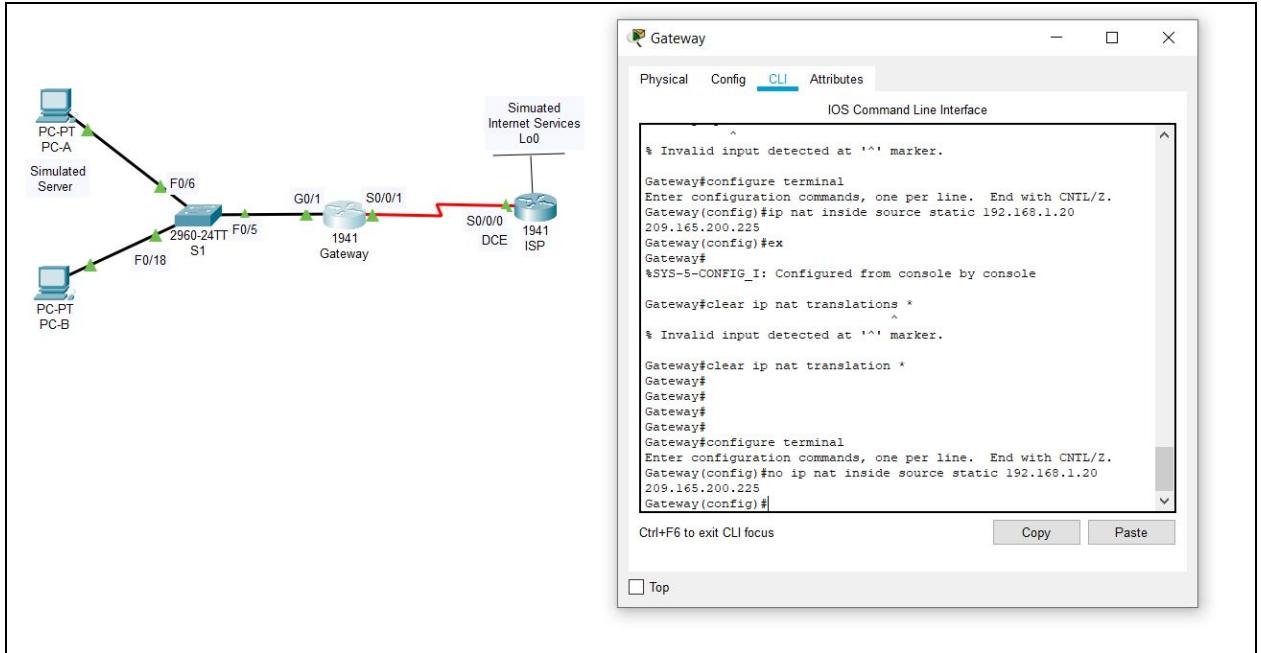


Total Translations = 5 (1 static and 4 dynamic)

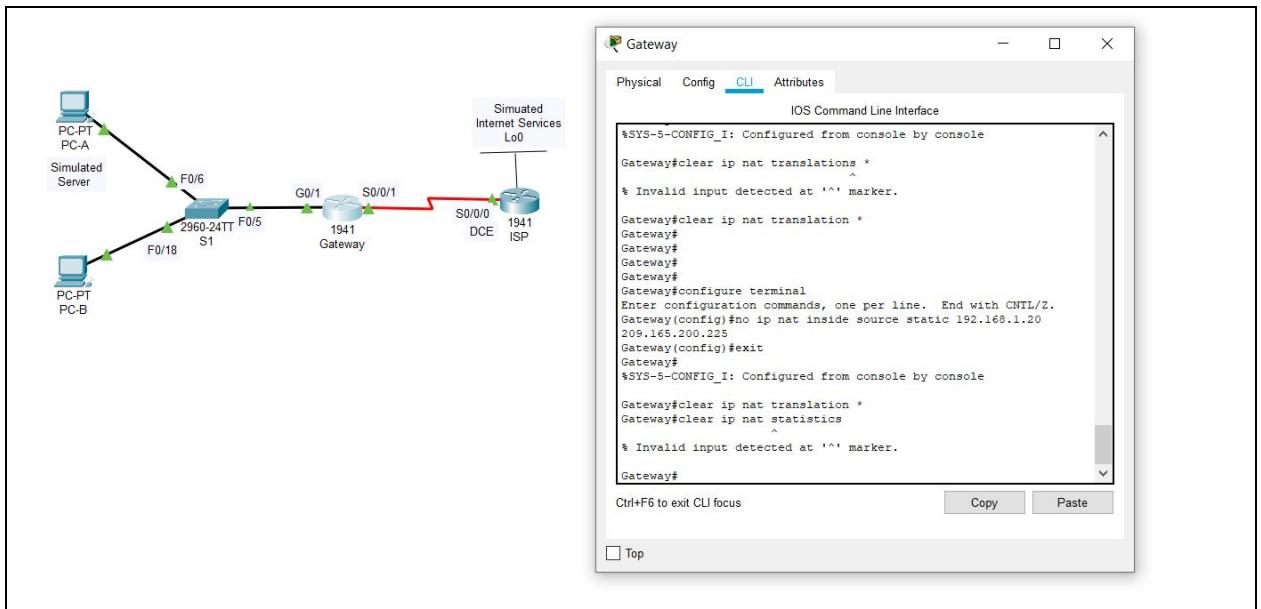
Step 7: Remove the static NAT entry.

In Step 7, the static NAT entry is removed and you can observe the NAT entry.

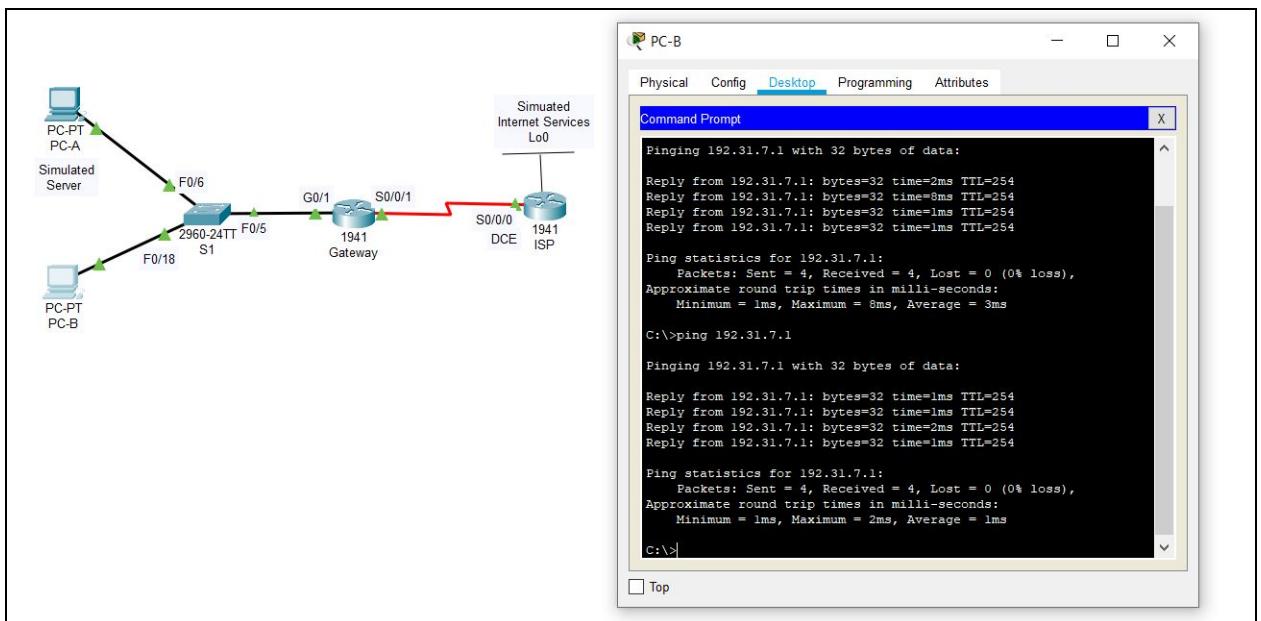
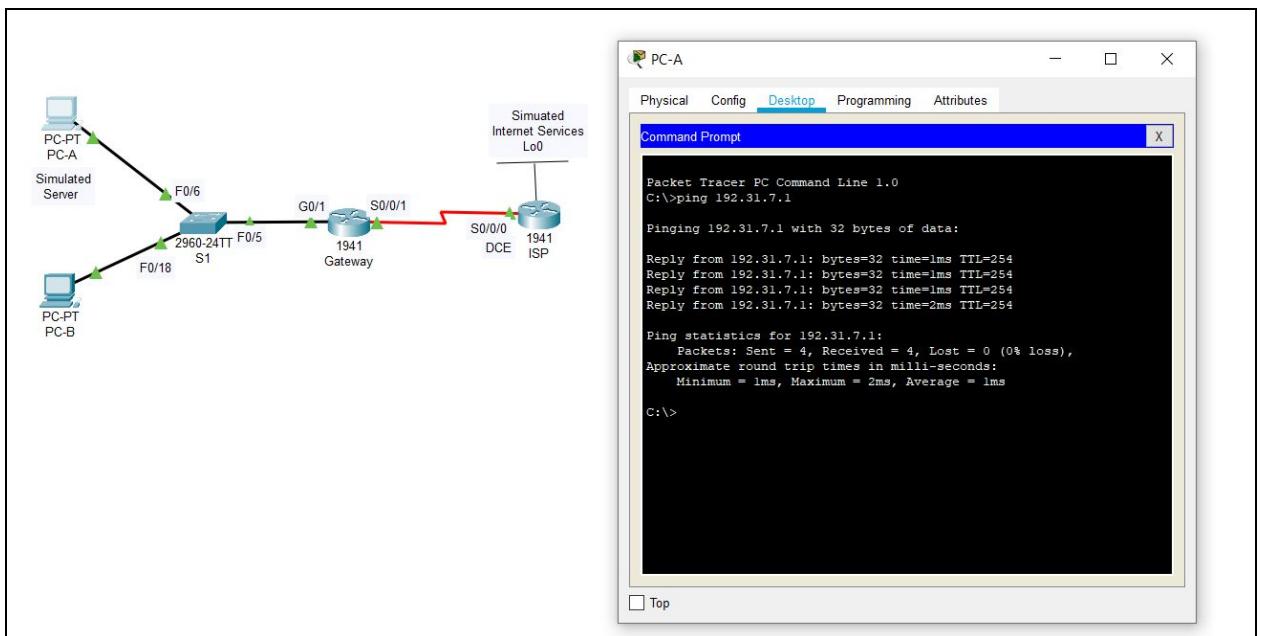
1. Remove the static NAT from Part 2. Enter yes when prompted to delete child entries.



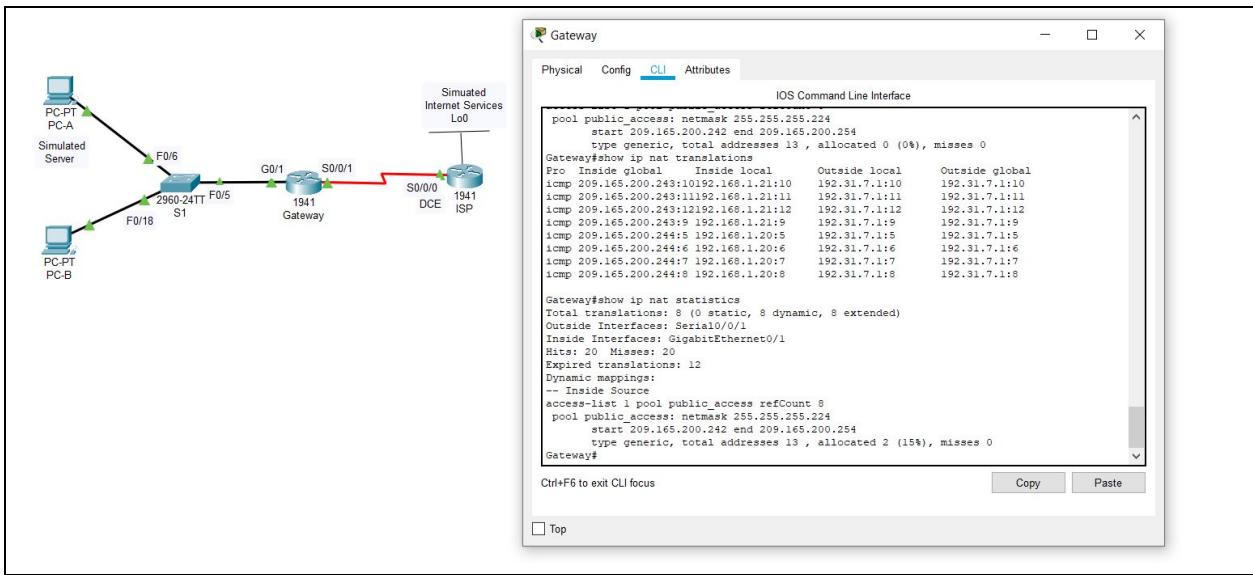
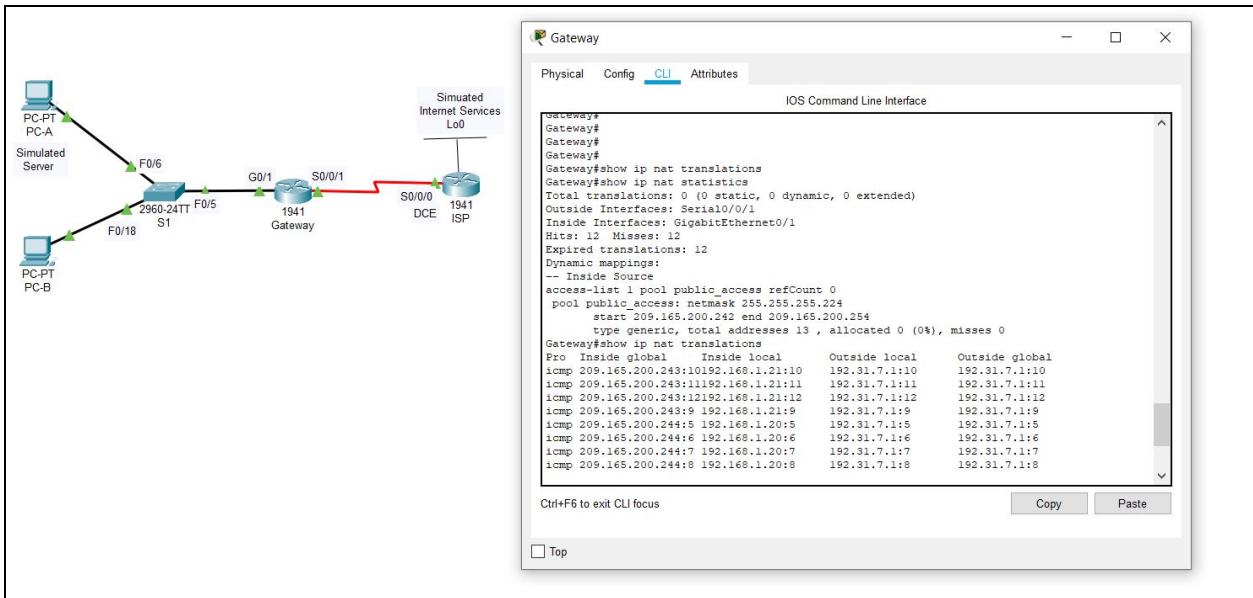
2. Clear the NATs and statistics.



3. Ping the ISP (192.31.7.1) from both hosts.



4. Display the NAT table and statistics.



Total Translations: 8 (all dynamic)

Conclusion:

1. In this ISE, we learned about Static and dynamic NAT configurations.
 2. We learned how to configure the routing table.