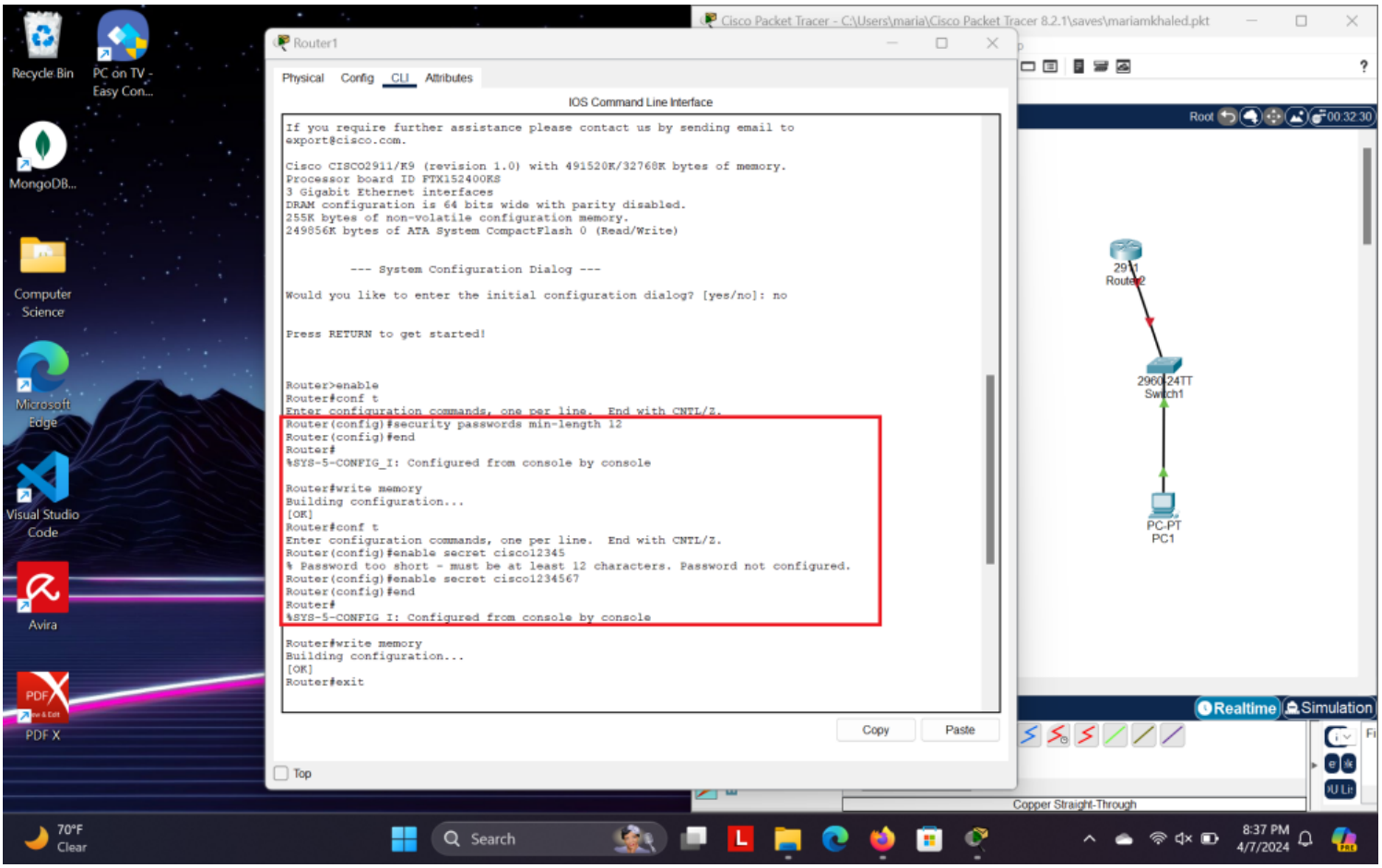
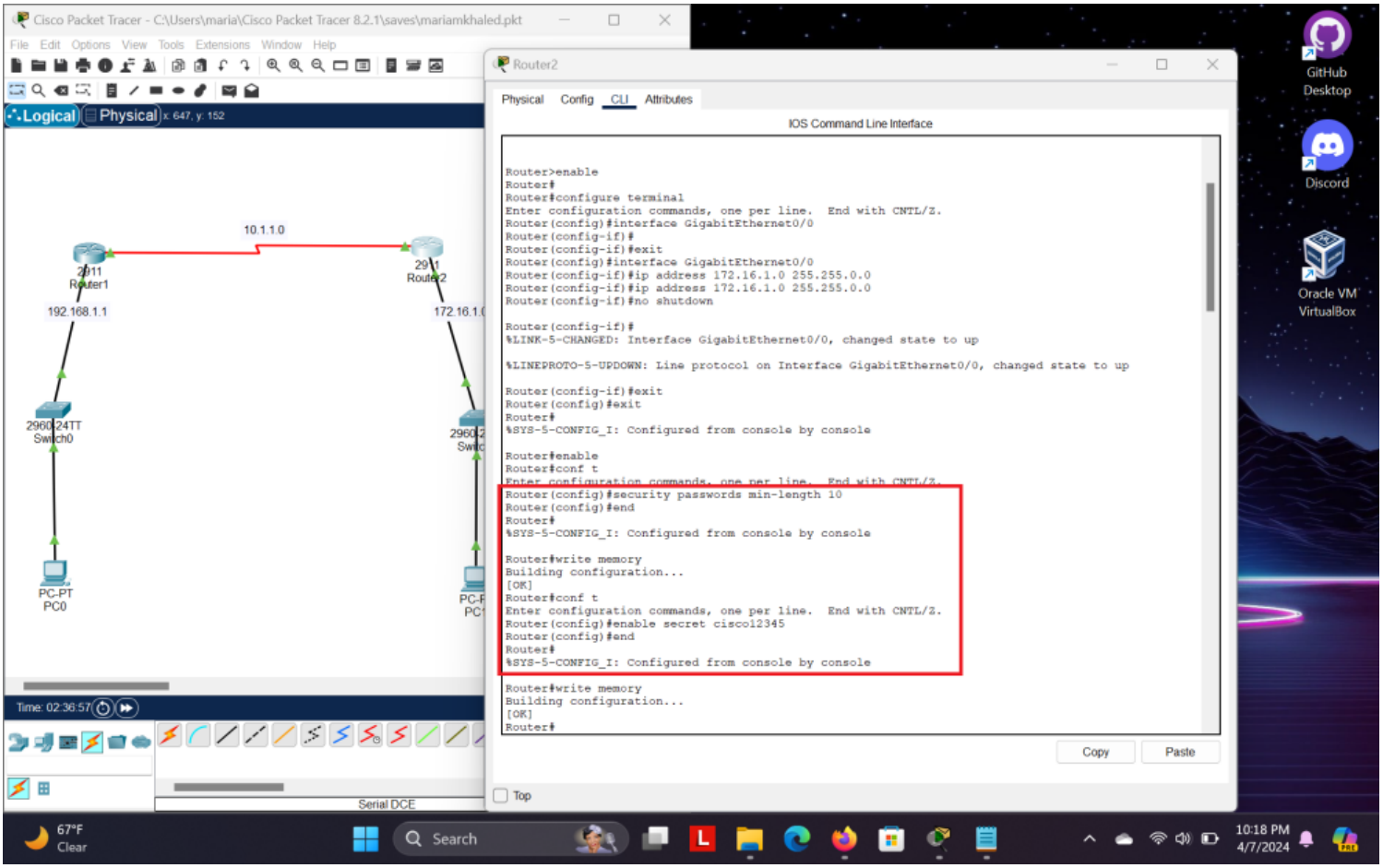
Exercise 1

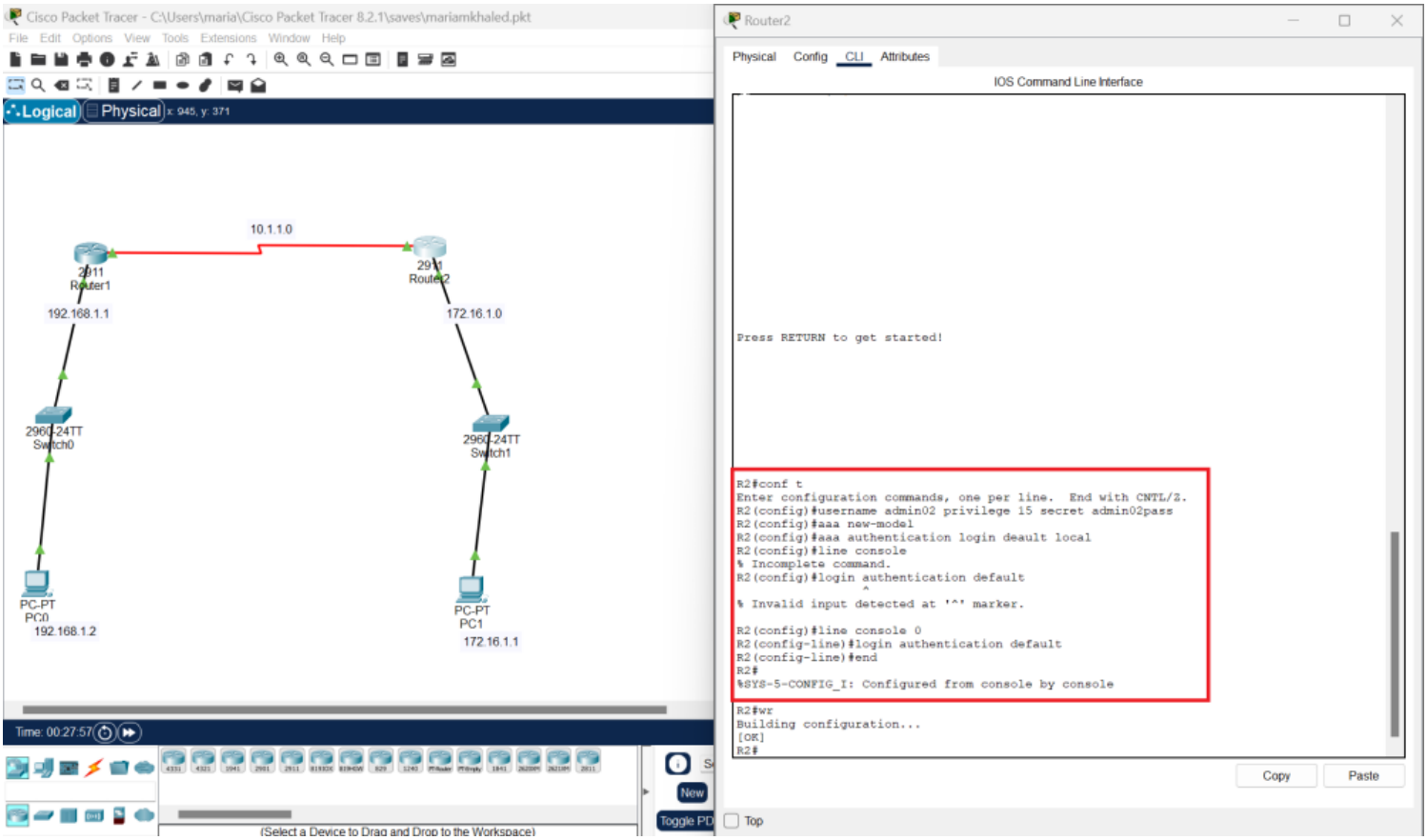
Mariam Khaled 7004693 T-08



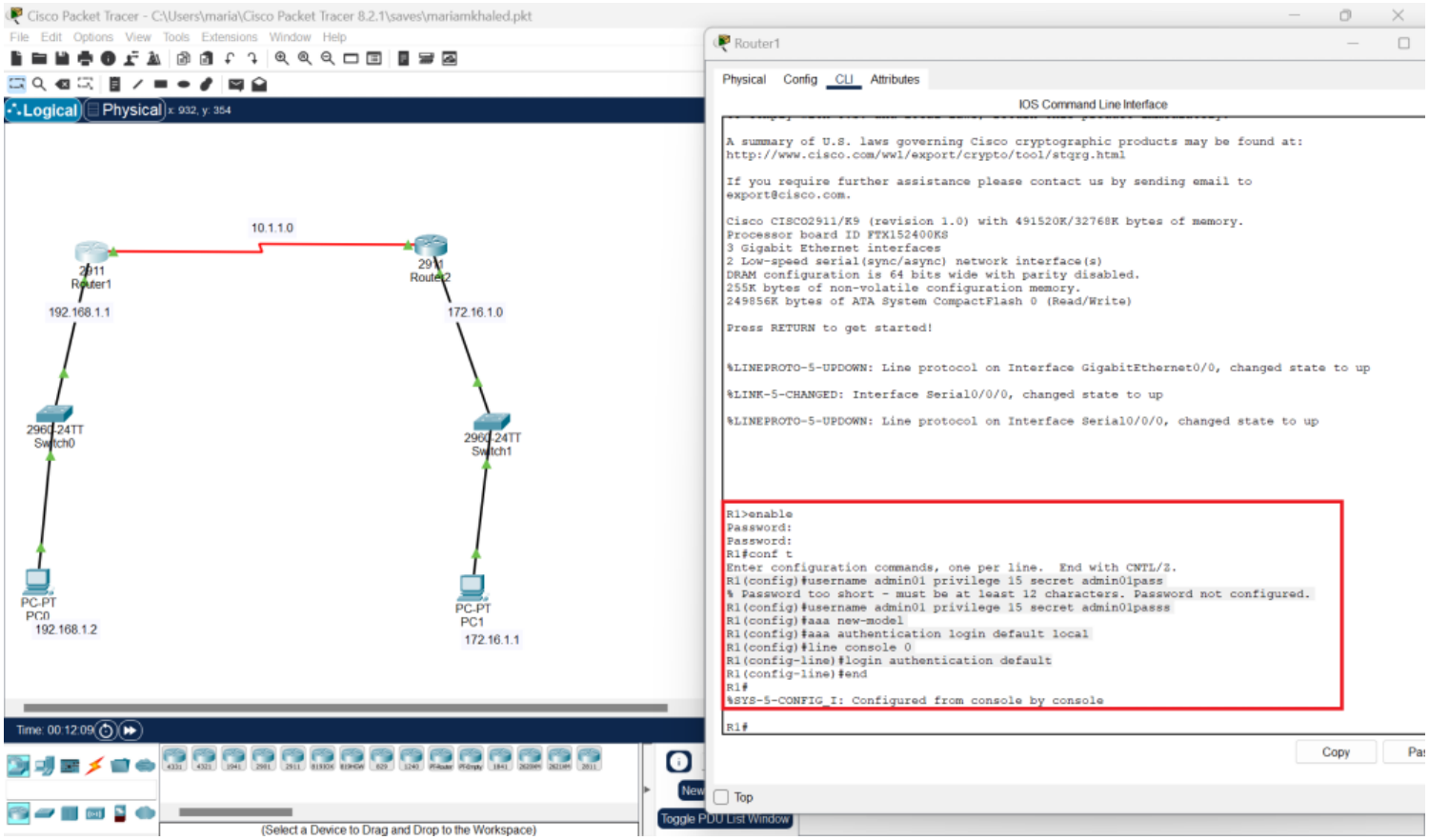
I configured Router R1 to enforce a minimum password length of 10 characters for all passwords. Additionally, I assigned the privileged EXEC password 'cisco12345' and encrypted it to ensure secure access to privileged mode.



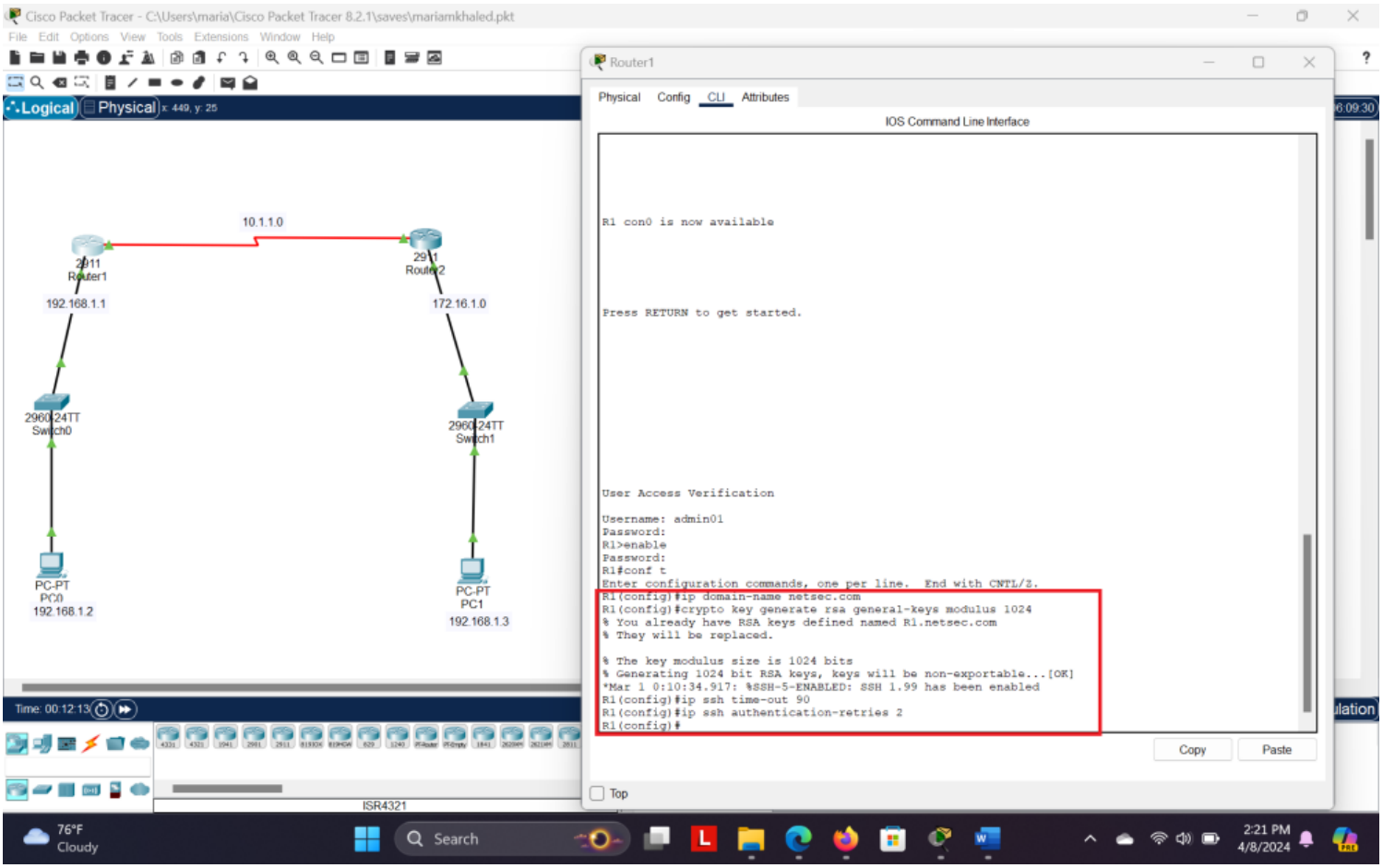
I configured Router R2 to enforce a minimum password length of 10 characters for all passwords. Additionally, I assigned the privileged EXEC password 'cisco12345' and encrypted it to ensure secure access to privileged mode.



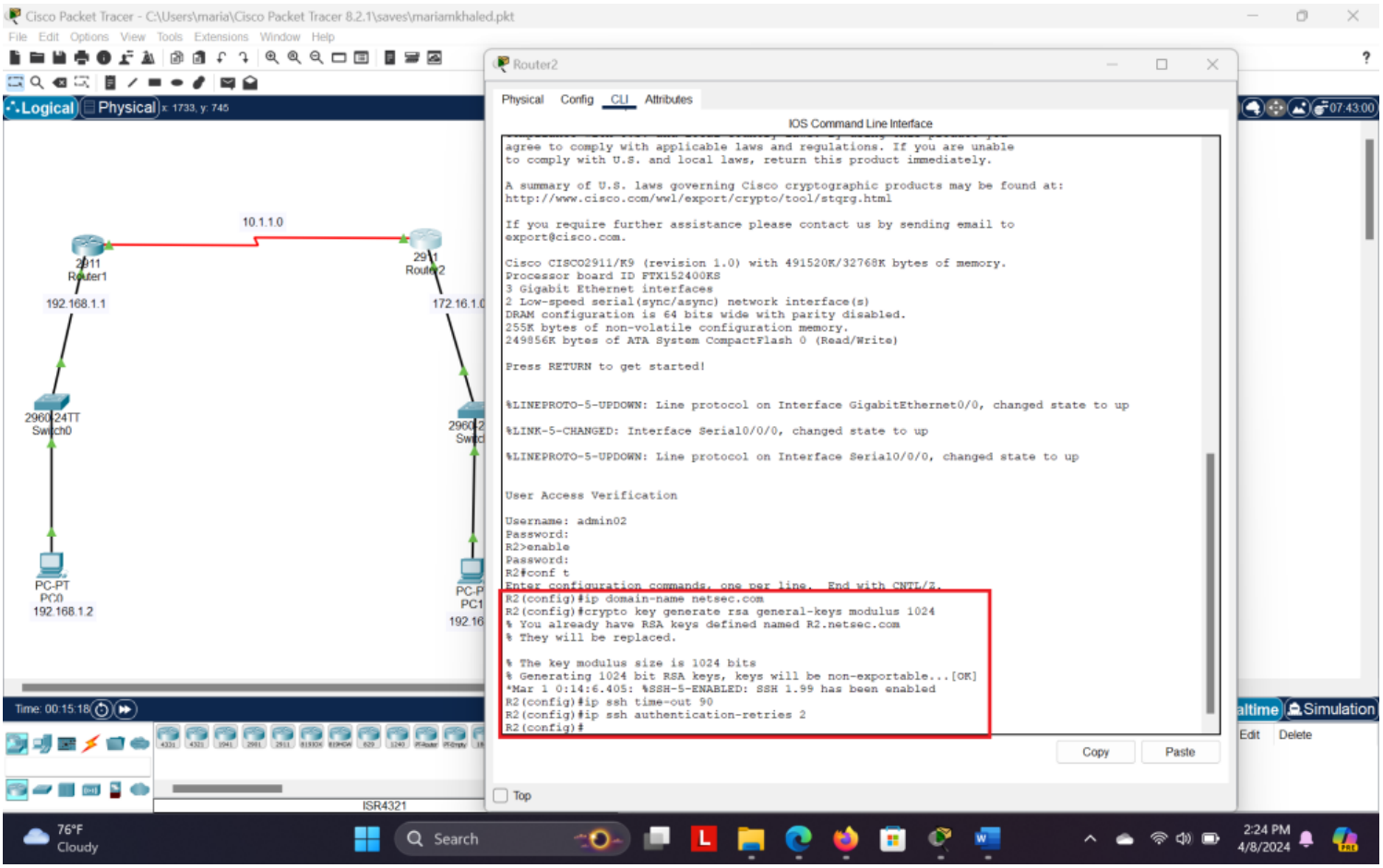
I added a user to the local database on Router R1 for administrator access. Specifically, I created a user named 'admin01' with privilege level 15 and set the password to 'admin01pass' to provide administrator access.
The commands used:
1) ‘username admin01 privilege 15 secret admin01passs’: Creates a user account named "admin01" with privilege level 15 and sets the password to "admin01passs".
2) 'aaa new-model': Enables the AAA (Authentication, Authorization, and Accounting) framework.
3) ‘aaa authentication login default local’: Sets the default authentication method for login attempts to use the local database (configured on the router).
4) 'line console 0': Enters configuration mode for the console line (the physical console port).
5 ‘login authentication default’: Configures the console line to use the default authentication method specified earlier.



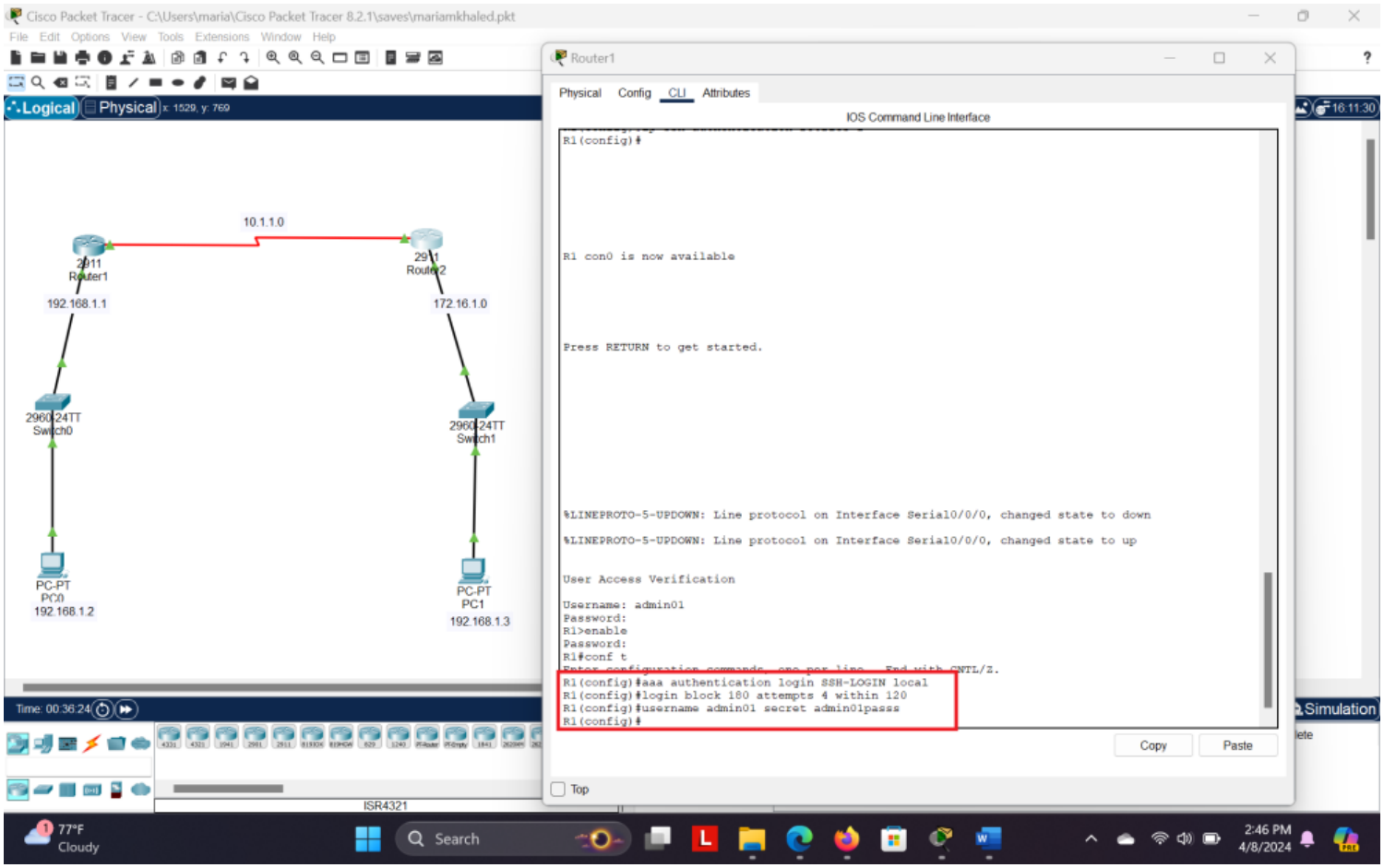
I added a user to the local database on Router R2 for administrator access. Specifically, I created a user named 'admin02' with privilege level 15 and set the password to 'admin02pass' to provide administrator access.
// Same commands used in the previous image. 😳



I configured SSH for secure remote access on Router R1 by enabling IP addresses for PCs and setting the domain name to 'netsec.com'. Additionally, I generated RSA keys with a size of 1024 bits for encryption. To enhance security, I set the SSH timeout to 90 seconds and authentication retries to 2.



I configured SSH for secure remote access on Router R2 by enabling IP addresses for PCs and setting the domain name to 'netsec.com'. Additionally, I generated RSA keys with a size of 1024 bits for encryption. To enhance security, I set the SSH timeout to 90 seconds and authentication retries to 2.



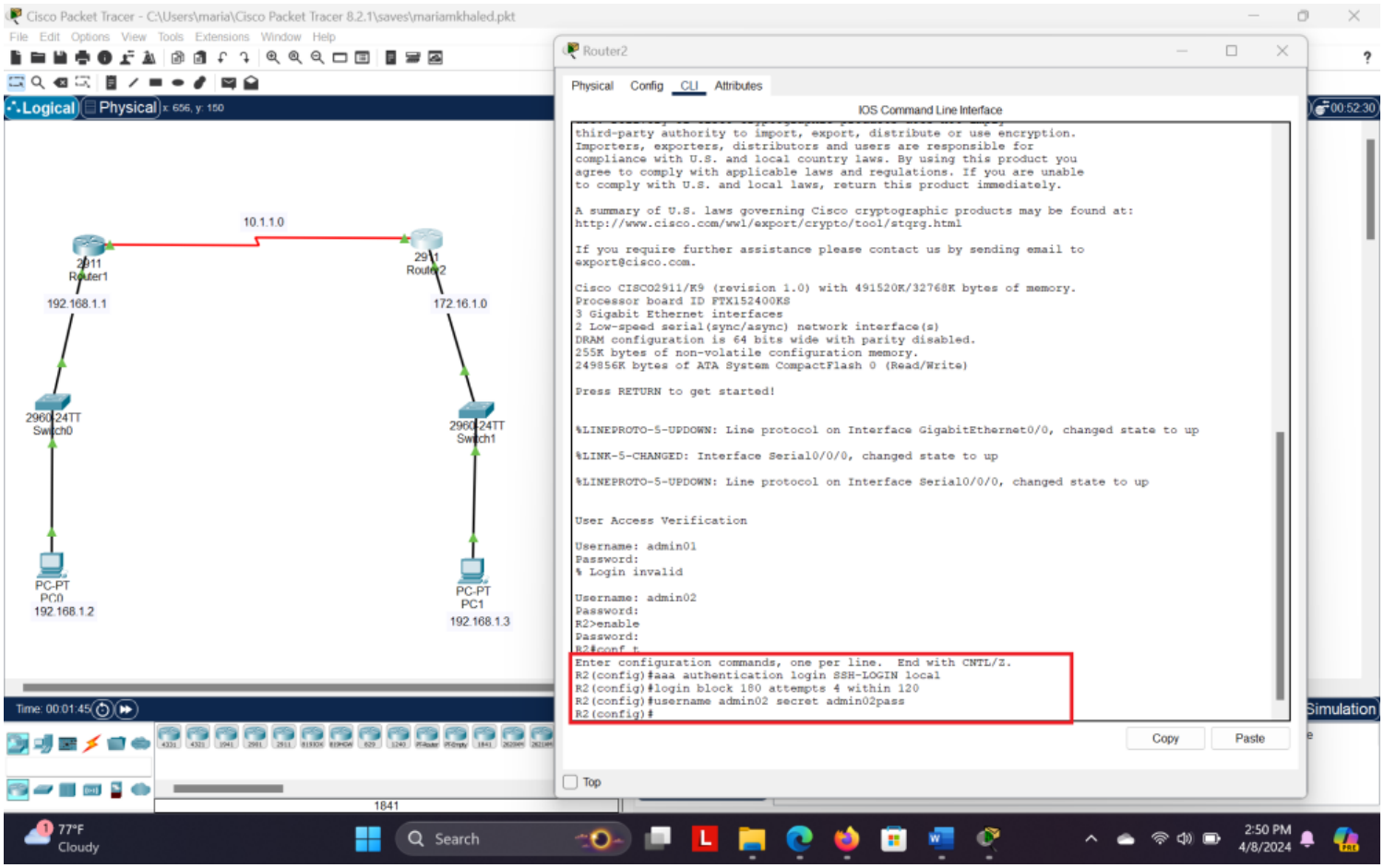
I've successfully configured AAA authentication settings on R1 with the following specifications:

-> AAA authentication has been enabled.

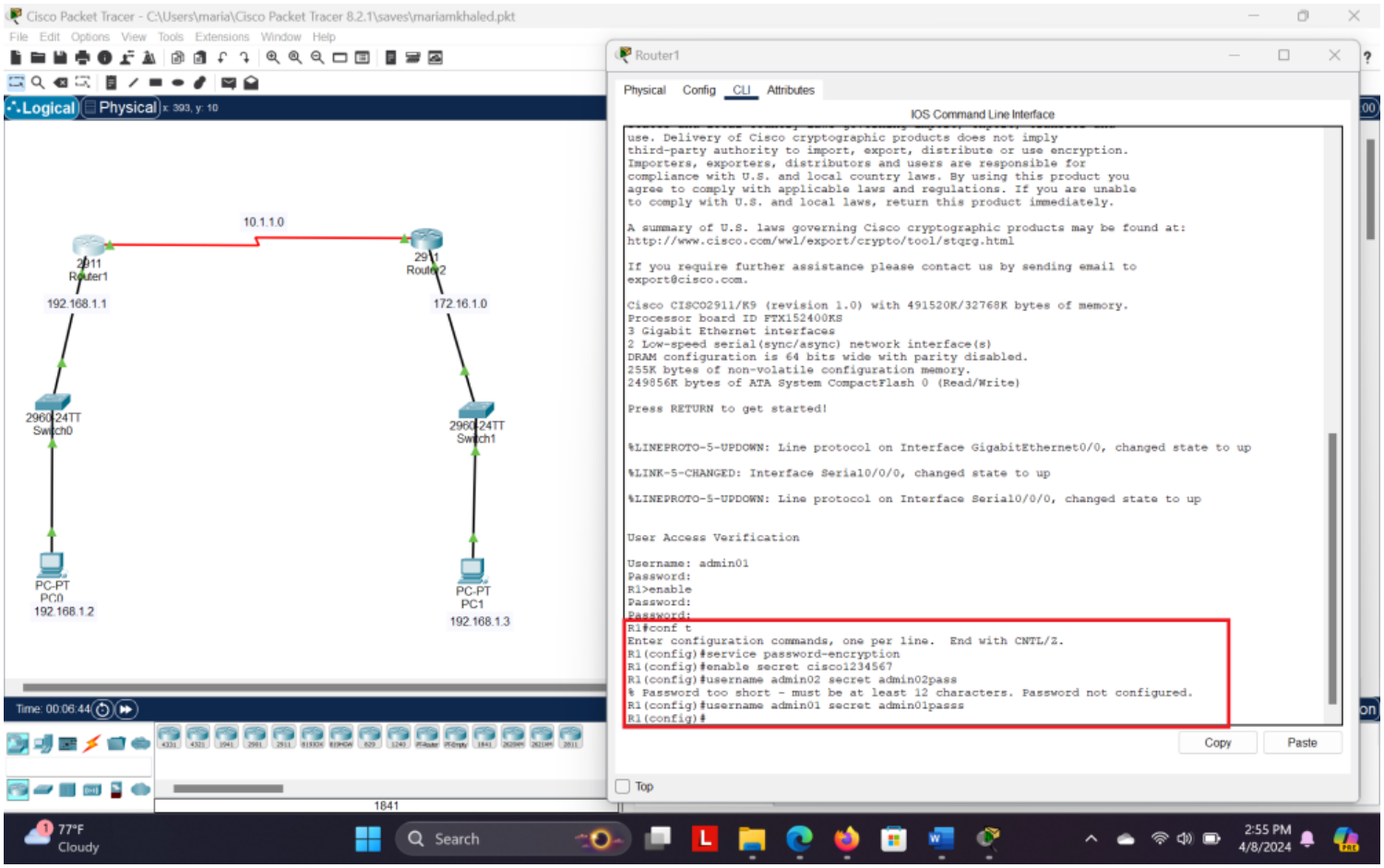
->The local database has been set as the default authentication method.

->Case-sensitive local username authentication has been implemented for enhanced security. (which was done in the previous step)

->Additionally, enhanced login settings have been applied to prevent access for three minutes after four failed login attempts within a two-minute period. This measure adds an extra layer of security to our system.



Configured AAA authentication on R2 with local database as default method, implementing case-sensitive usernames for security. Enhanced login settings block access for 3 minutes after 4 failed attempts in 2 minutes.



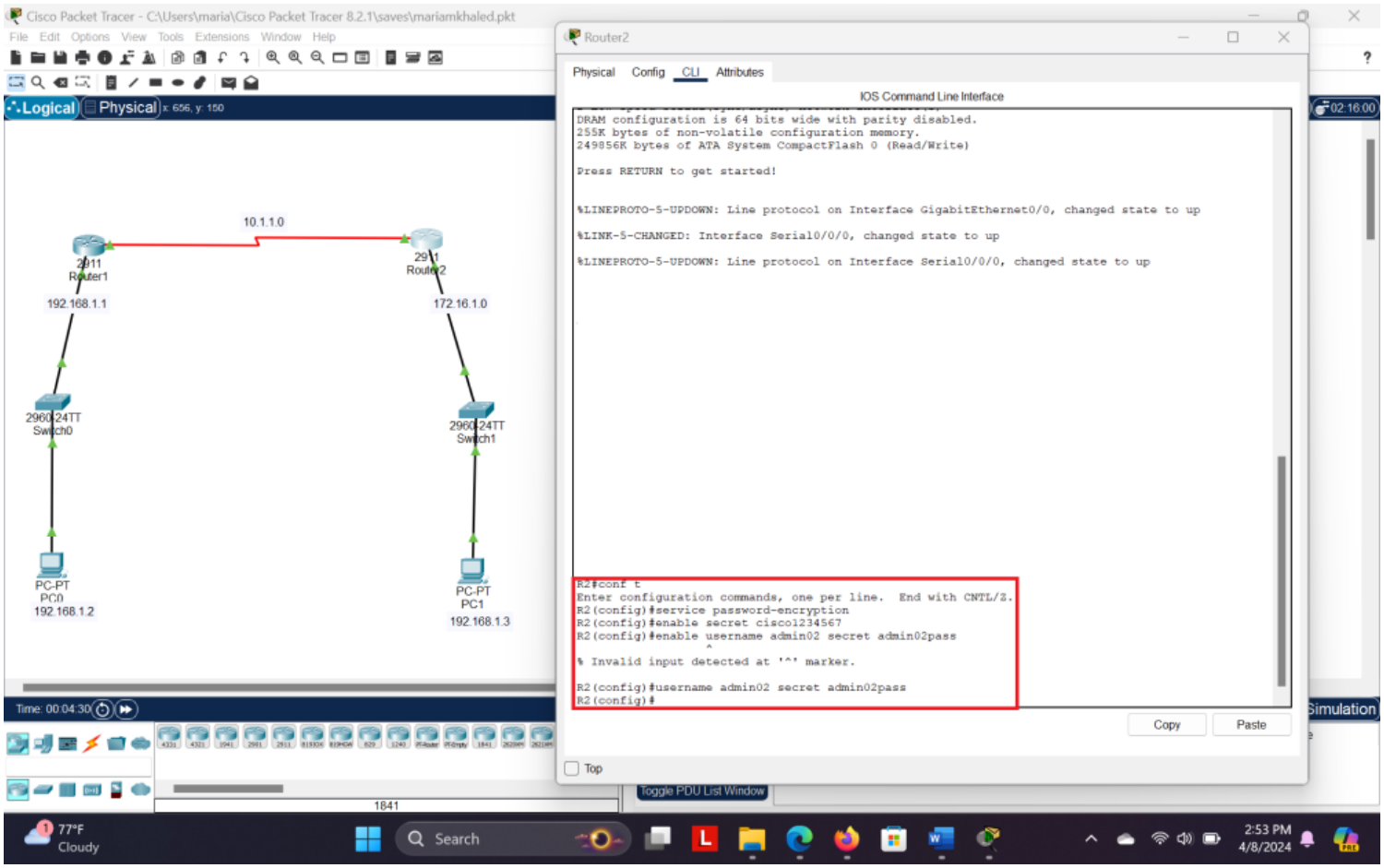
I've encrypted all passwords on R1 to safeguard information:

->Utilized 'service password-encryption' in configuration mode.

ⓘ used in Cisco IOS to encrypt plaintext passwords stored in the device's configuration file. It converts passwords into a hashed form using a weak encryption algorithm (Type 7 encryption)

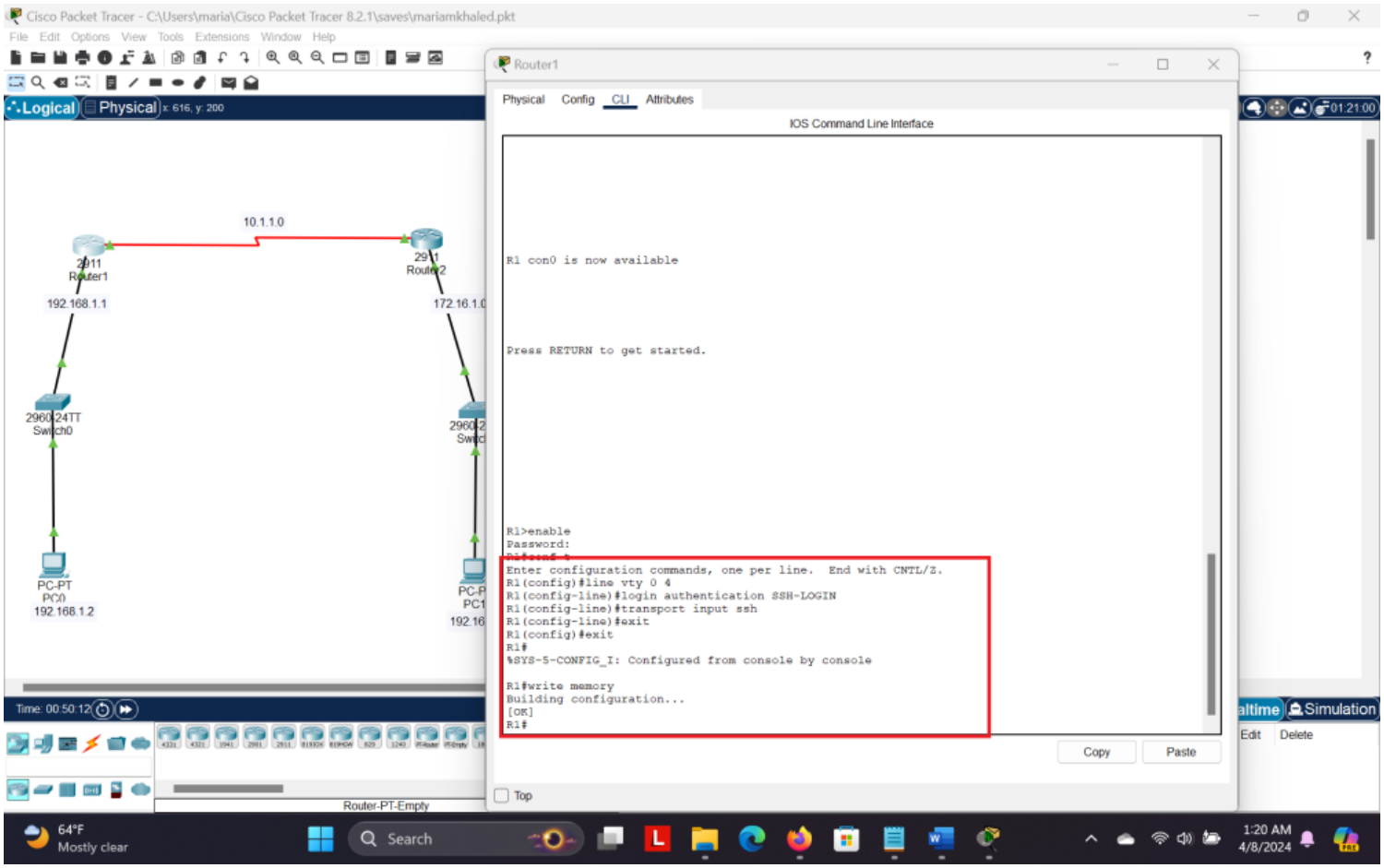
->Set a password for enable mode.

->Employed 'secret' for user authentication with MD5 encryption, enhancing security measures.



I've encrypted all passwords on R2 to safeguard information:

->Utilized 'service password-encryption' in configuration mode.
->Set a password for enable mode.
->Employed 'secret' for user authentication with MD5 encryption, enhancing security measures.



1) 'line vty 0 4': Specifies the VTY lines to configure (0 to 4).

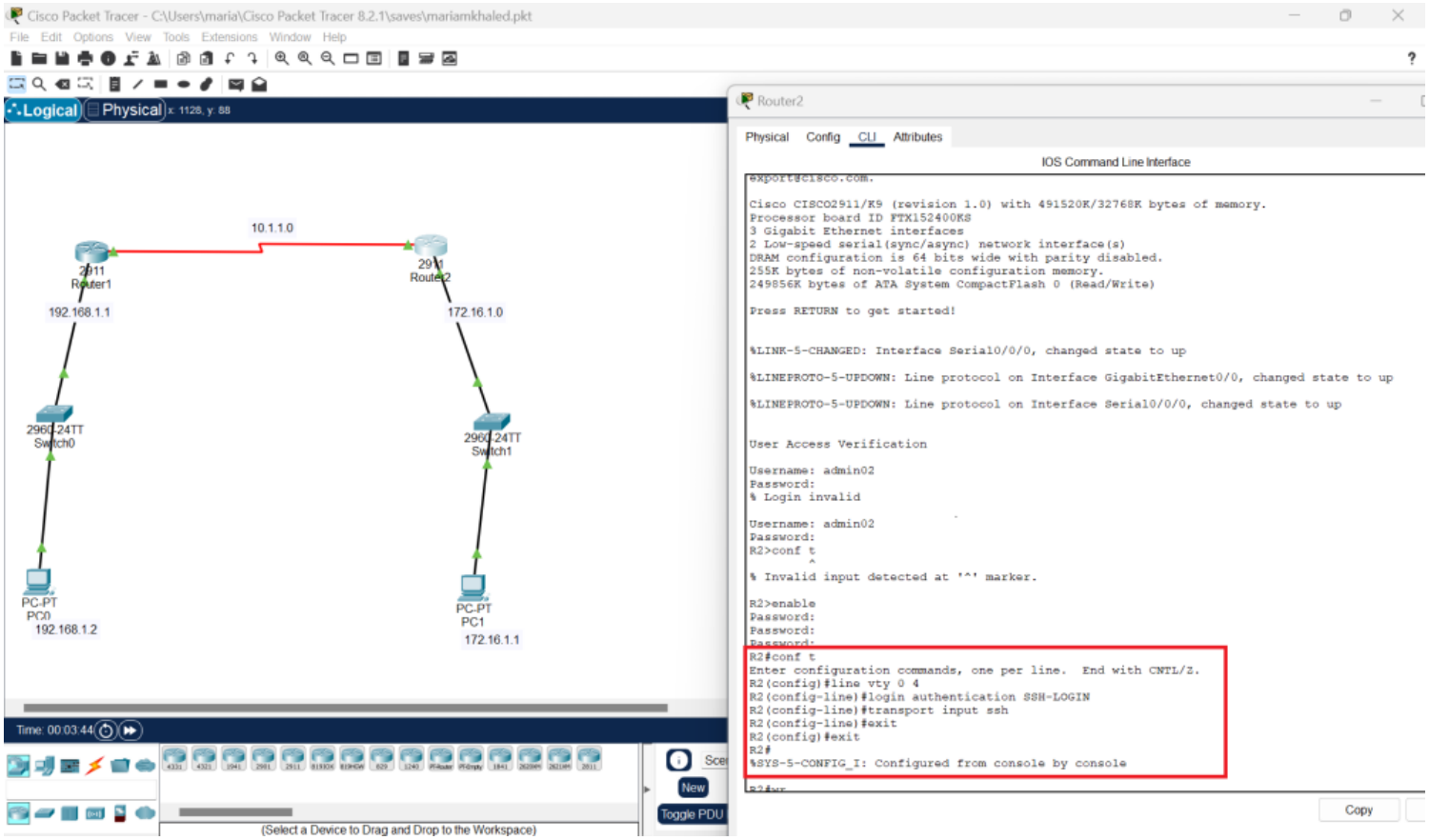
ⓘ specifying these lines, I'm indicating which lines I want to configure.

2) 'login authentication SSH_LOGIN': Sets the authentication method for login attempts to "SSH_LOGIN".

ⓘ specifies the authentication method that will be used for login attempts on the VTY lines

3) 'transport input ssh': Restricts input traffic to SSH only for secure access.

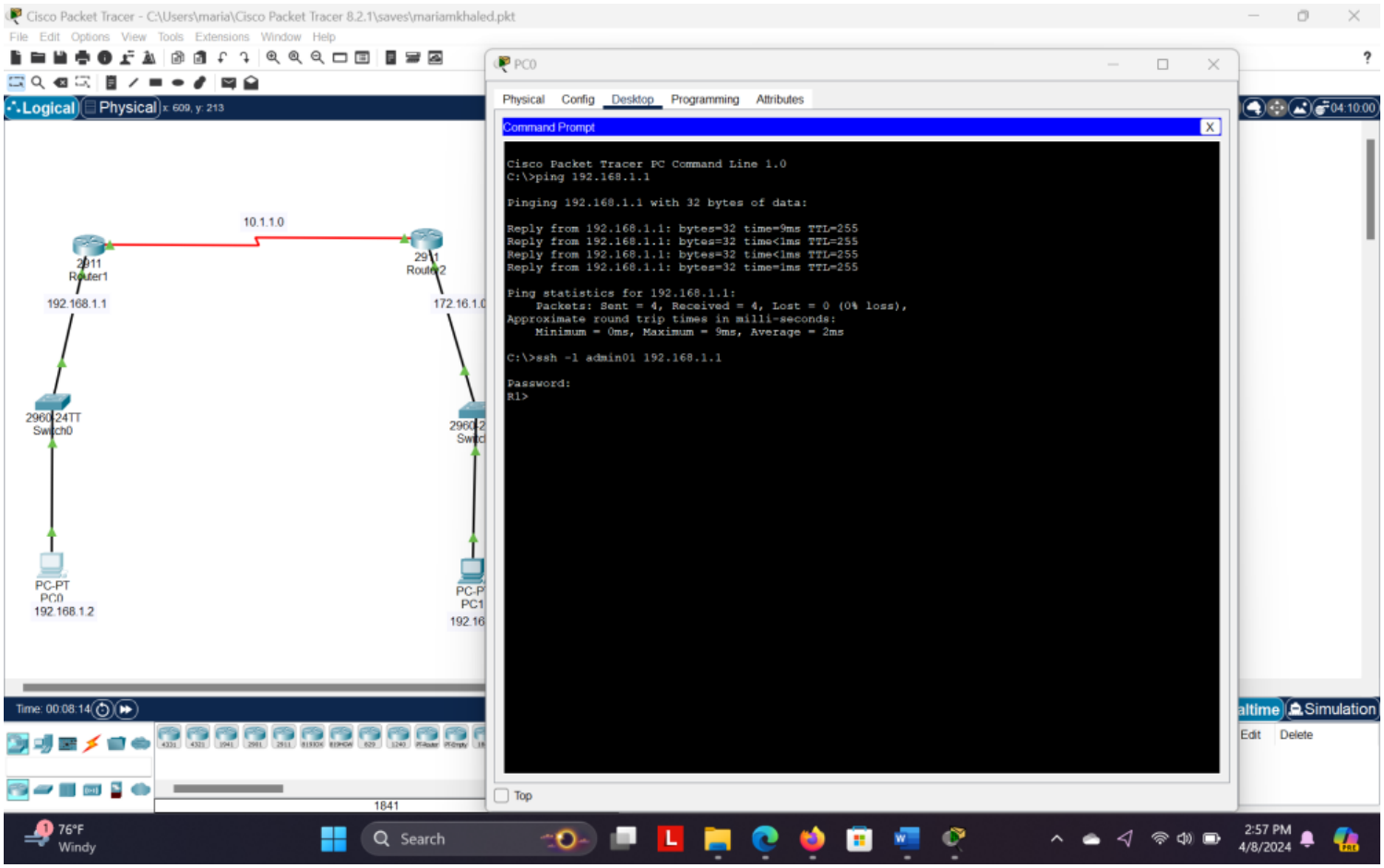
ⓘ command restricts the types of traffic that are allowed to enter the VTY lines. By allowing only SSH traffic, I'm ensuring that access to the device is encrypted and secure.



1) ‘line vty 0 4’: Specifies the VTY lines to configure (0 to 4).

2) ‘login authentication SSH_LOGIN’: Sets the authentication method for login attempts to "SSH_LOGIN".

3) ‘transport input ssh’: Restricts input traffic to SSH only for secure access.

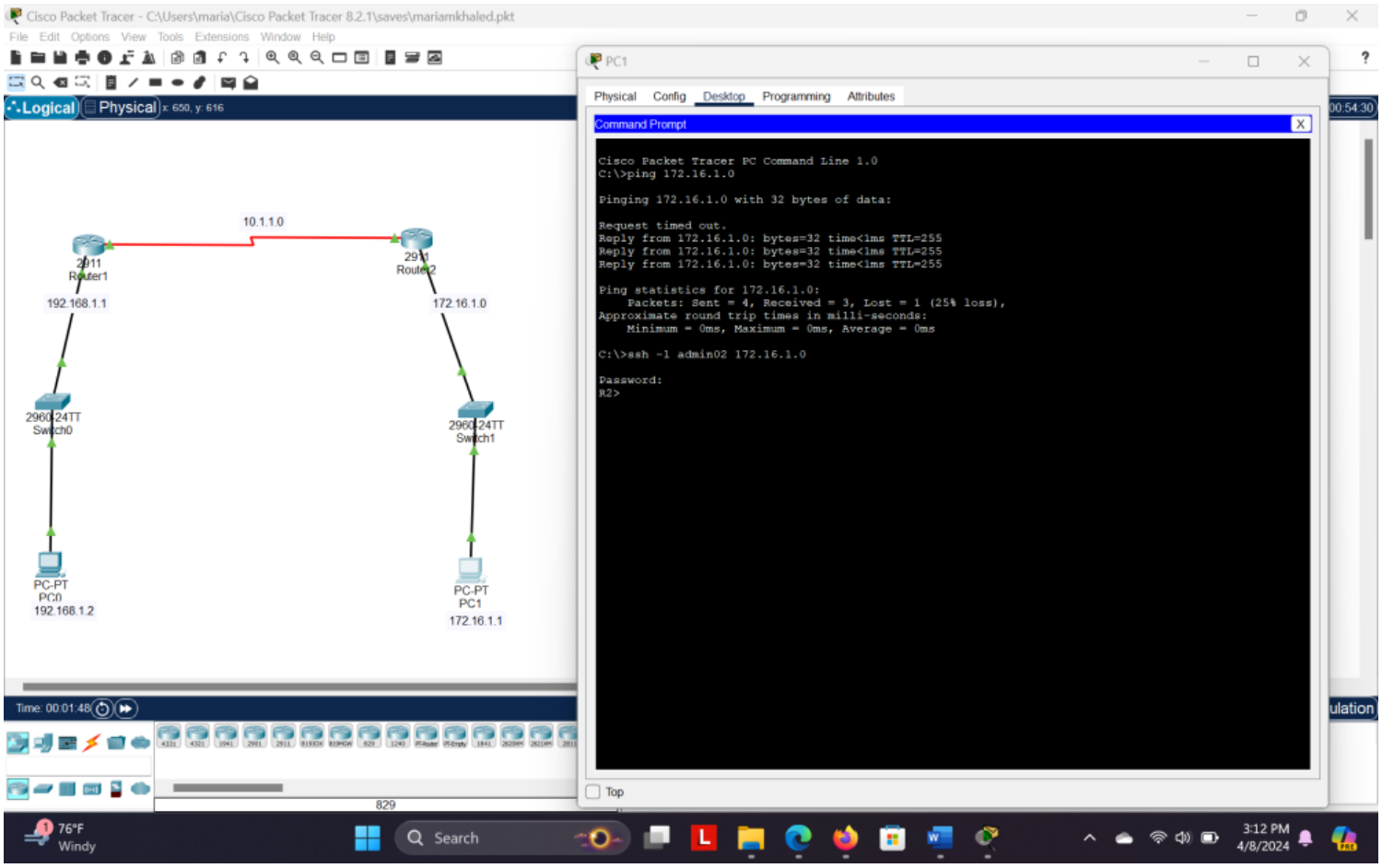


To test SSH access from PC0 to Router1:

1) Firstly, I initiated a ping command from PC0 to Router1. This step ensures that there is basic connectivity between the devices and that Router1 is reachable from PC0 over the network.

2) Following the successful ping, I entered the command 'ssh -l ' on PC0. This command initiates an SSH connection. The 'L' option specifies that we want to establish a connection to a remote host.

3) Then, I entered the IP address of Router1 after '-l', indicating that I want to connect to Router1 via SSH. This step prompts PC0 to initiate an SSH session to the specified IP address.

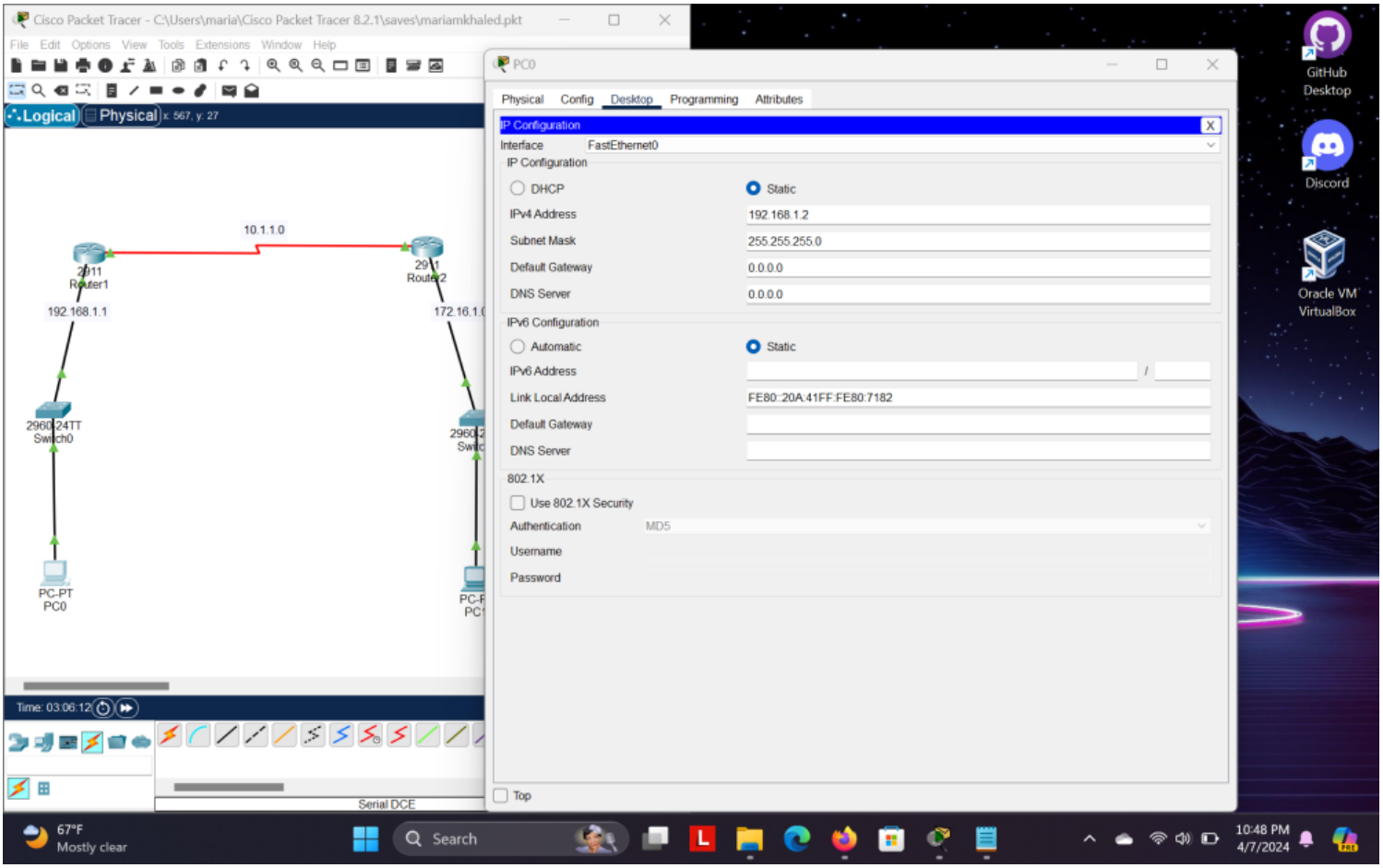


Of course I did the same thing regarding PC1:

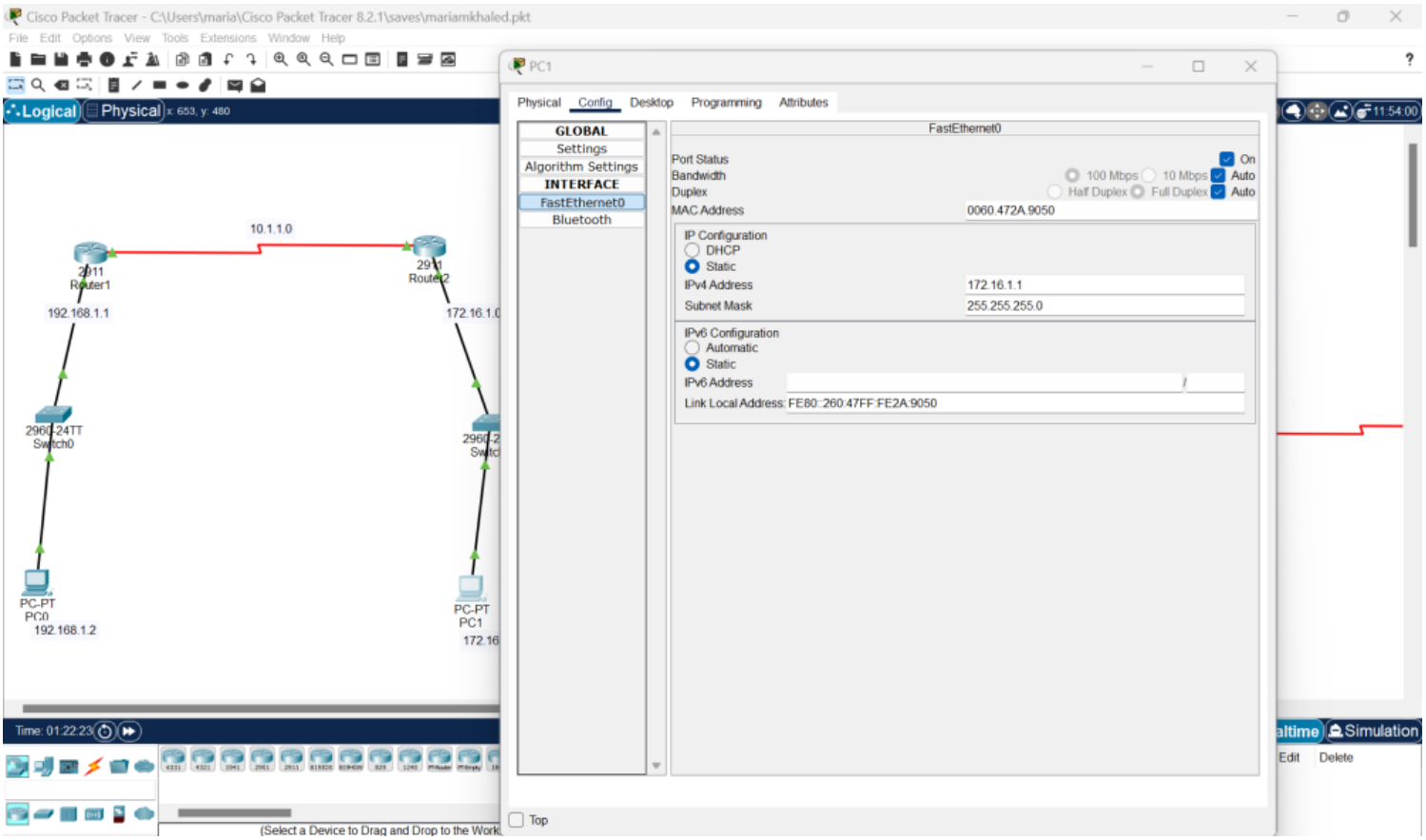
1) I initiated a ping command from PC1 to Router2.

2) Following the successful ping, I entered the command 'ssh -l ' on PC0.

3) Then, I entered the IP address of Router1 after '-l', indicating that I want to connect to Router1 via SSH. .

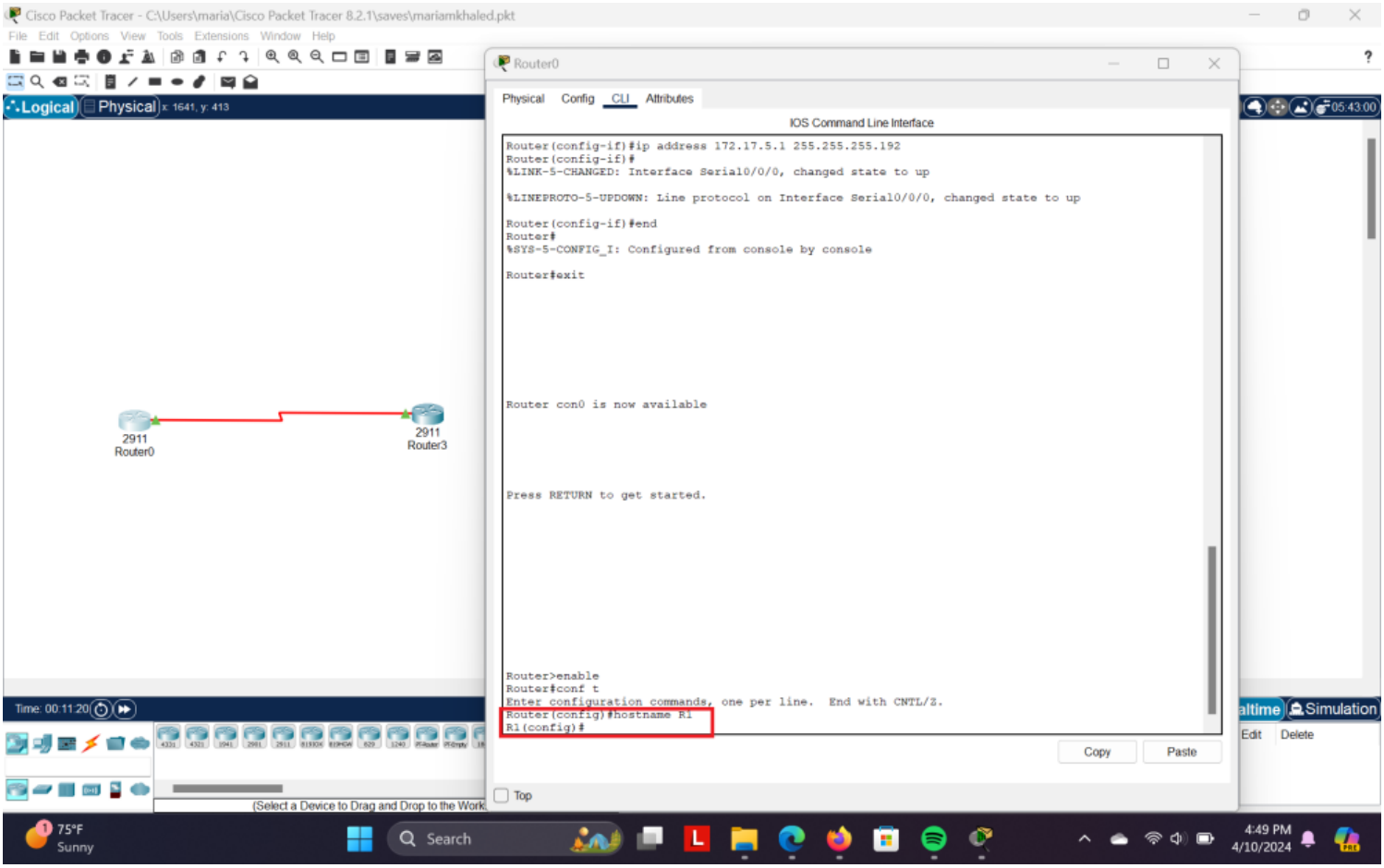


ⓘ This is the Ip for PC0 which is connected to Router 1

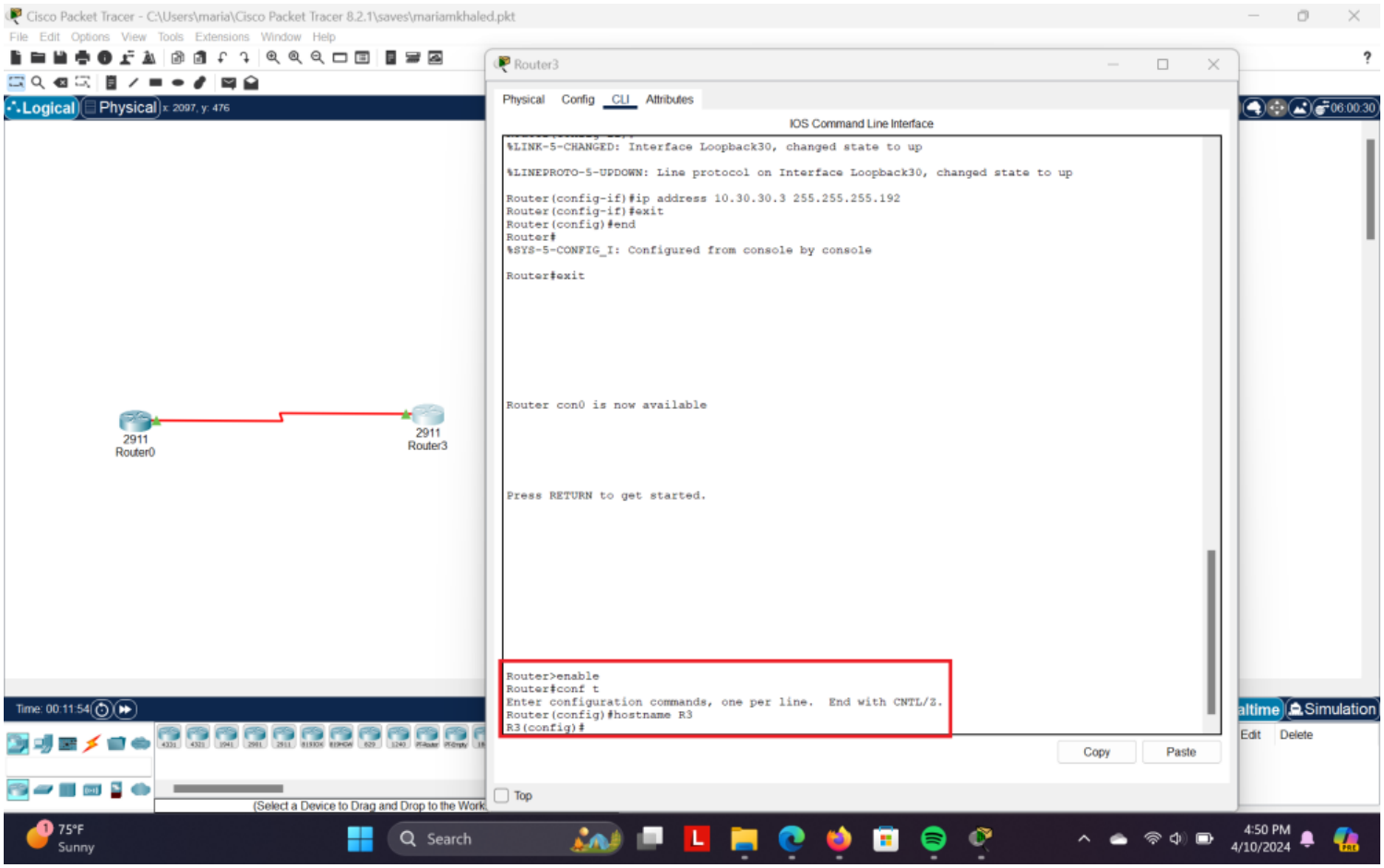


ⓘ This is the Ip for PC1 which is connected to Router 2

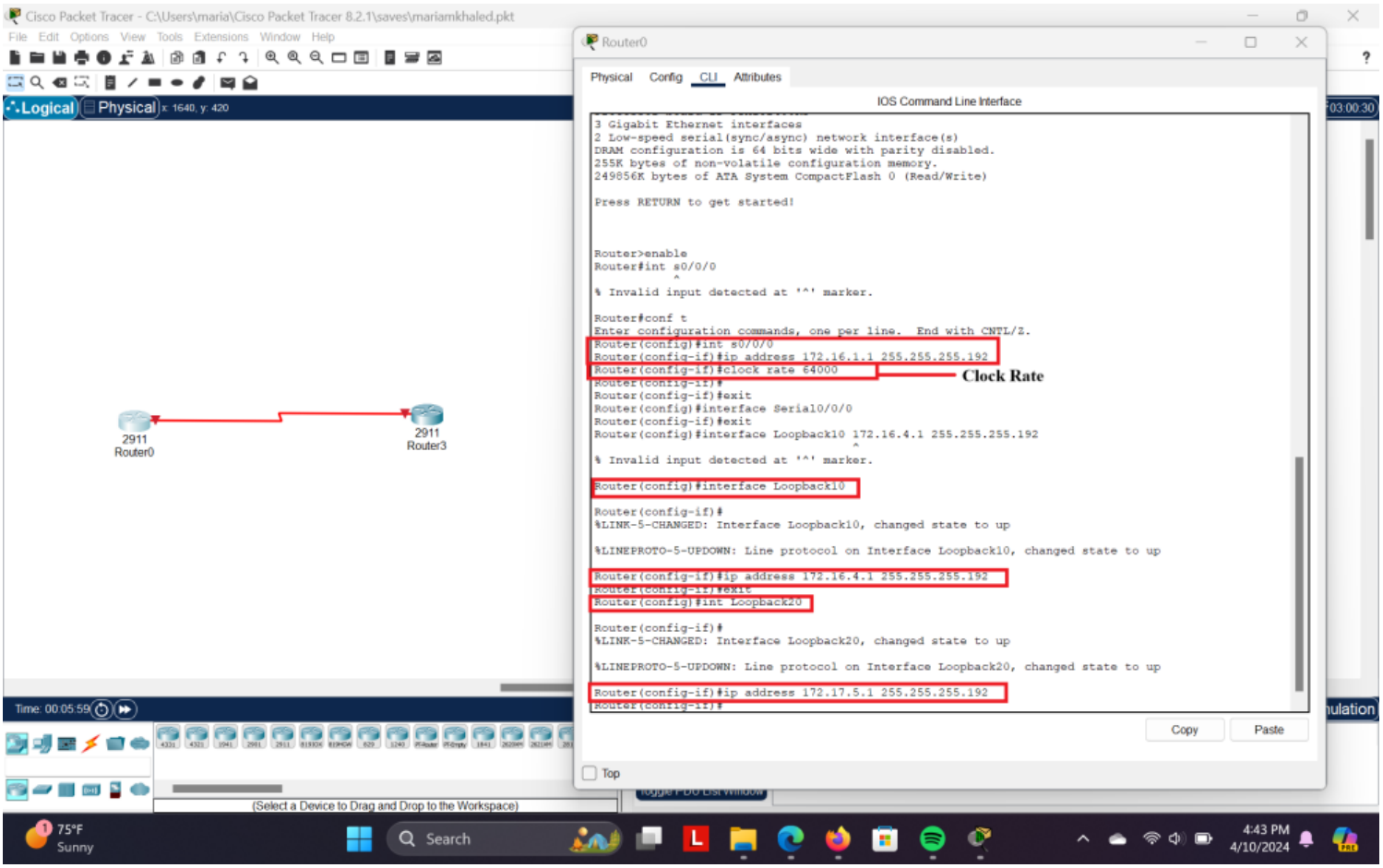
Exercise 2



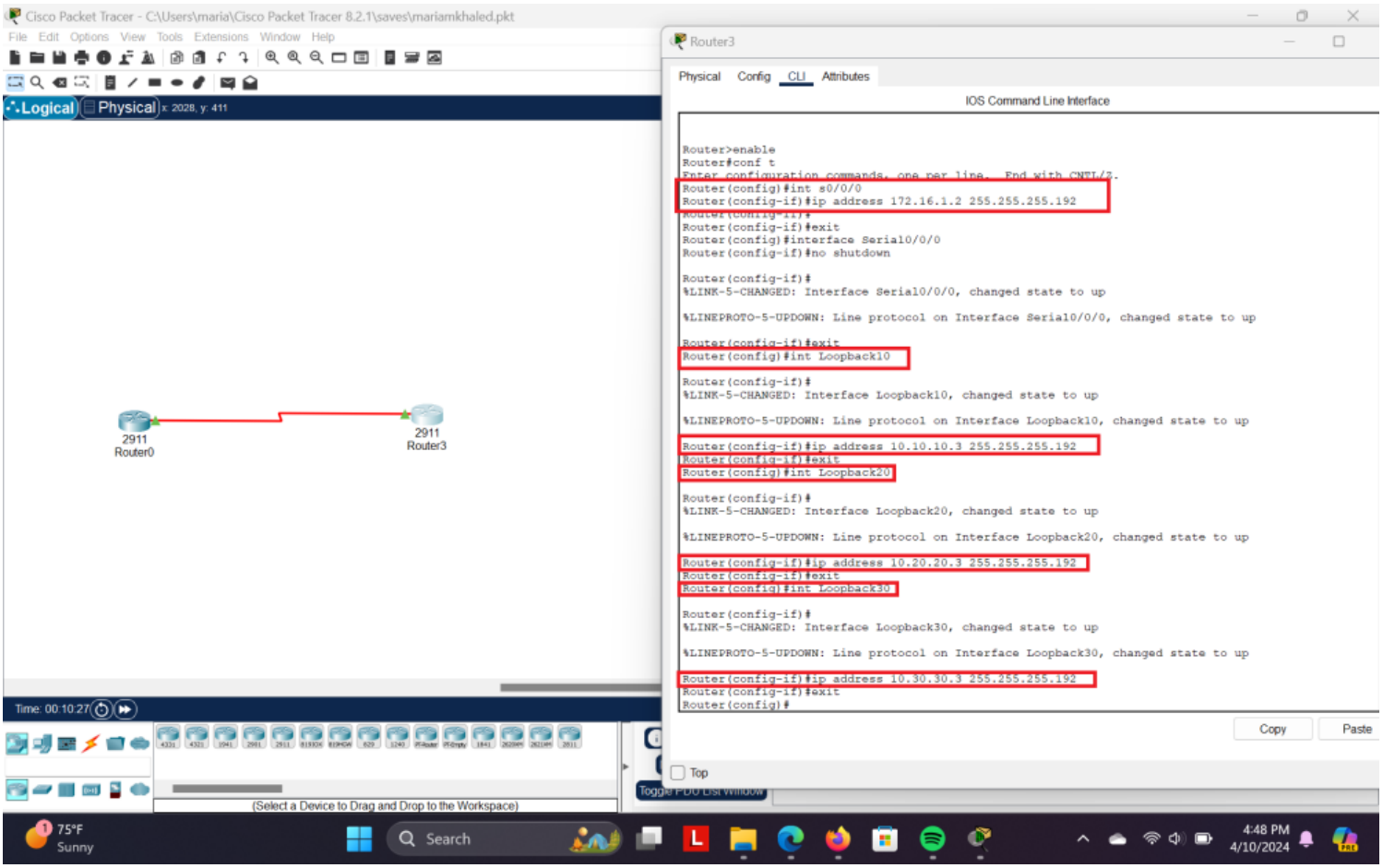
I accessed configuration mode and changed the router's name to R1 by entering the command 'hostname R1'.



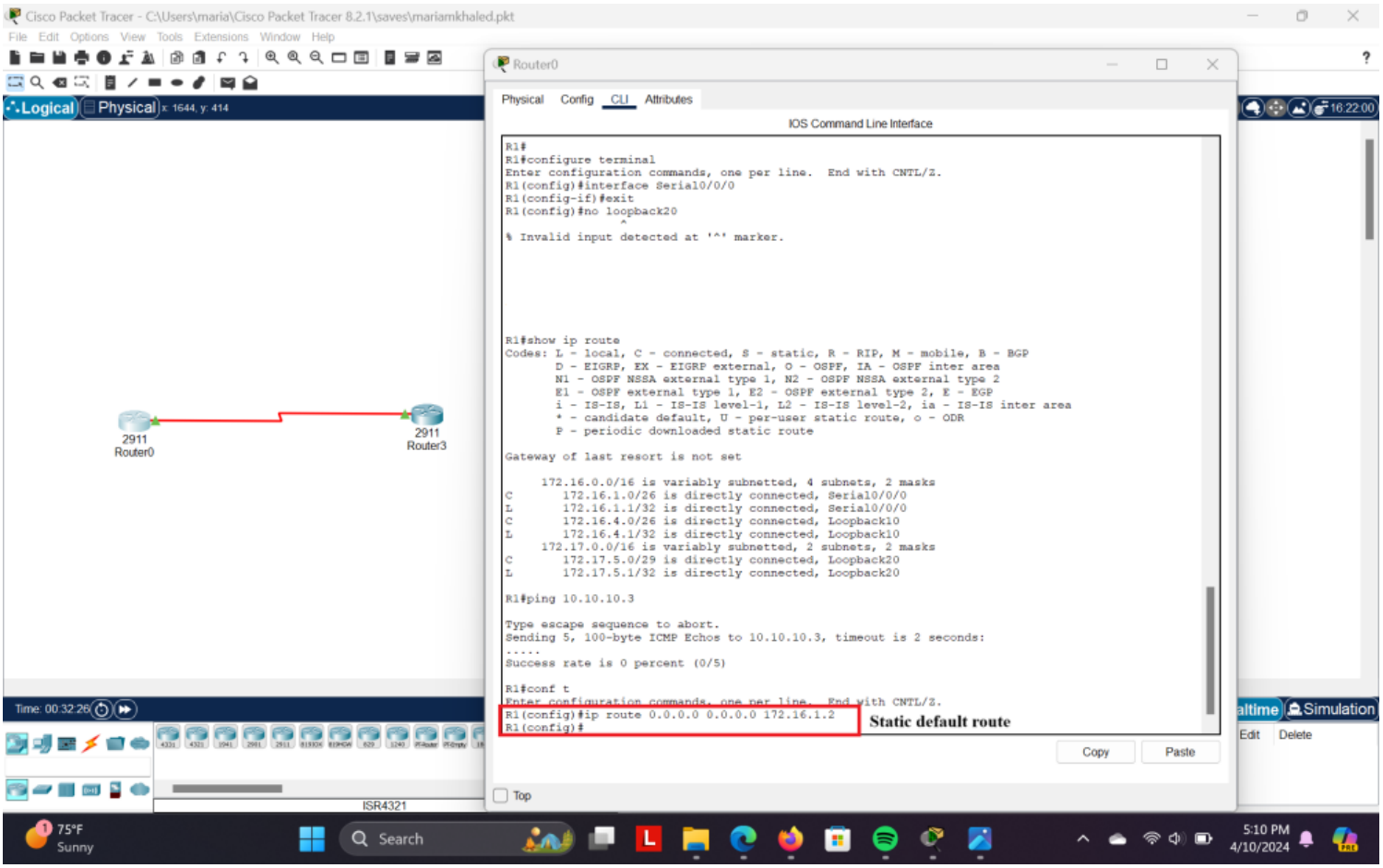
I accessed configuration mode and changed the router's name to R3 by entering the command 'hostname R3'.



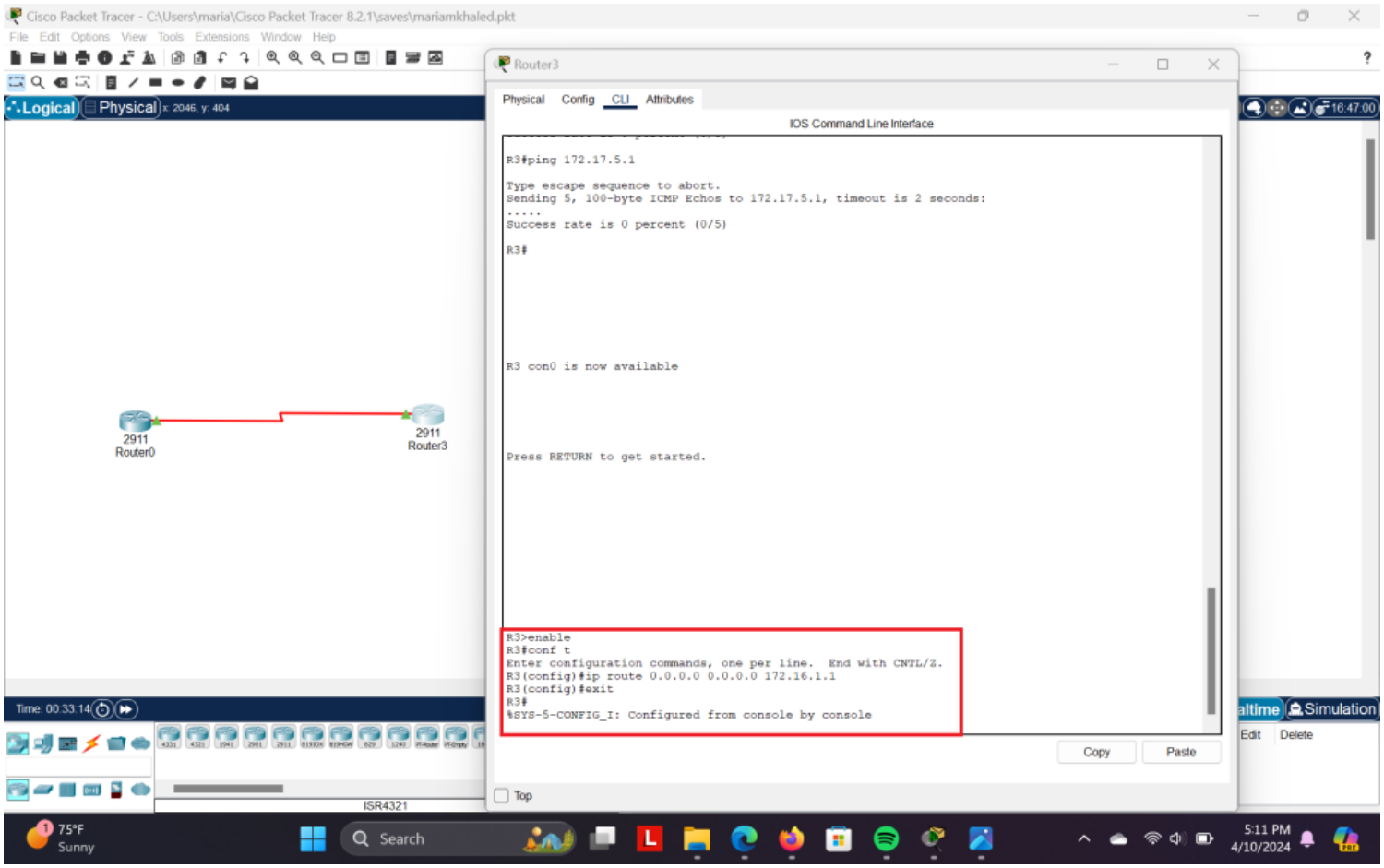
I configured the IP address for R1 and also set up IP addresses for two loopback interfaces.
IP address 172.16.1.1
Loopback10 172.16.4.1
Loopback20 172.17.5.1
ⓘ I set the clock rate of R1 to 64000 by entering serial interface and using the command 'clock rate 64000'.
ⓘ To set the IP address, I initially entered the configuration mode, proceeded to access the serial interface, and subsequently configured the IP address along with the subnet.
ⓘ I configured and activated two loopback interfaces, typically used for testing purposes, and assigned IP addresses along with subnet masks to both of them.



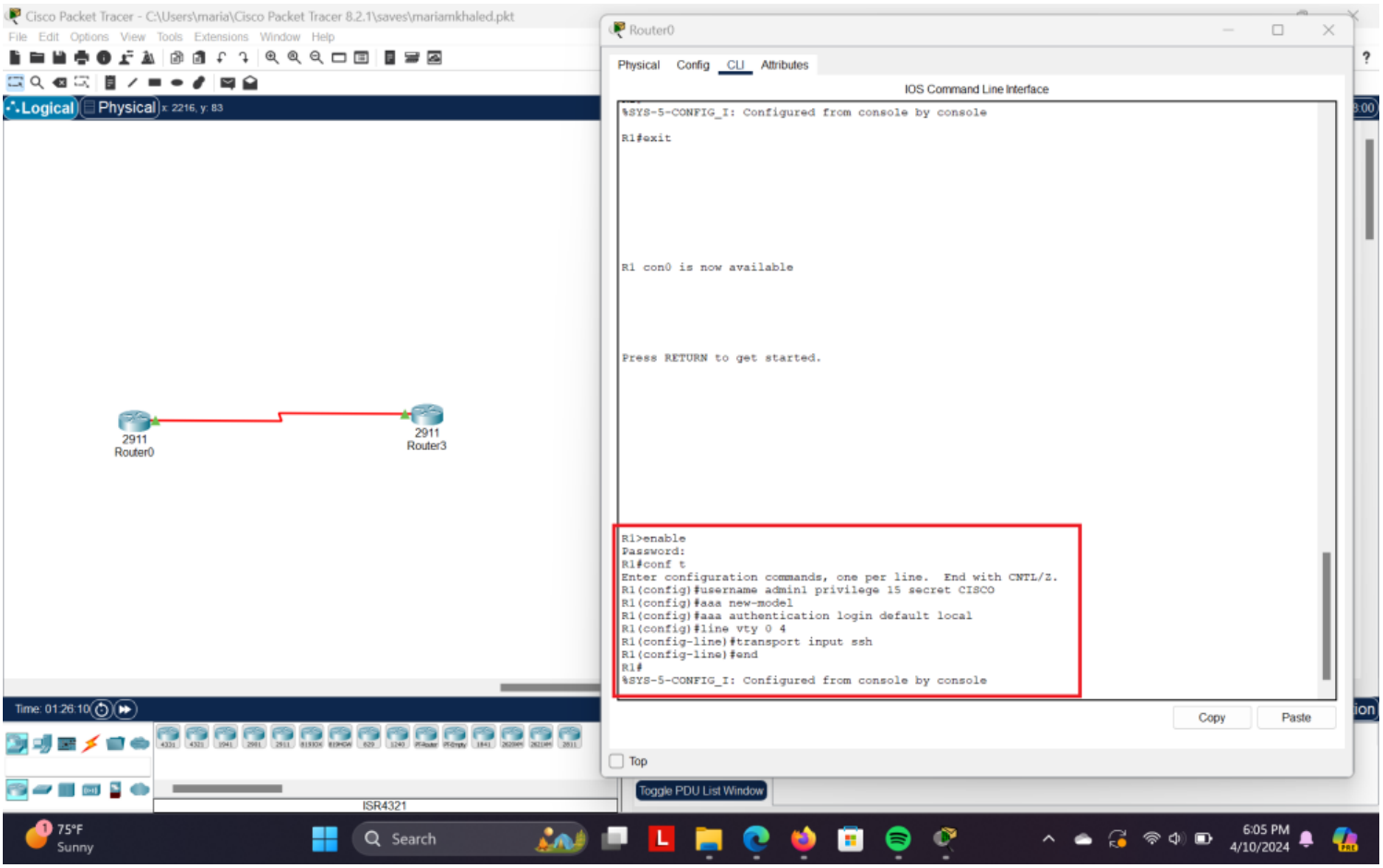
I configured the IP address for R3 and also set up IP addresses for three loopback interfaces.
Ip address 172.16.1.2
Loopback10 10.10.10.3
Loopback20 10.20.20.3
Loopback30 10.30.30.3
ⓘ To set the IP address, I first entered configuration mode, then accessed the serial interface, and finally configured the IP address along with the subnet.
ⓘ I configured and activated three loopback interfaces, typically used for testing purposes, and assigned IP addresses along with subnet masks to both of them.



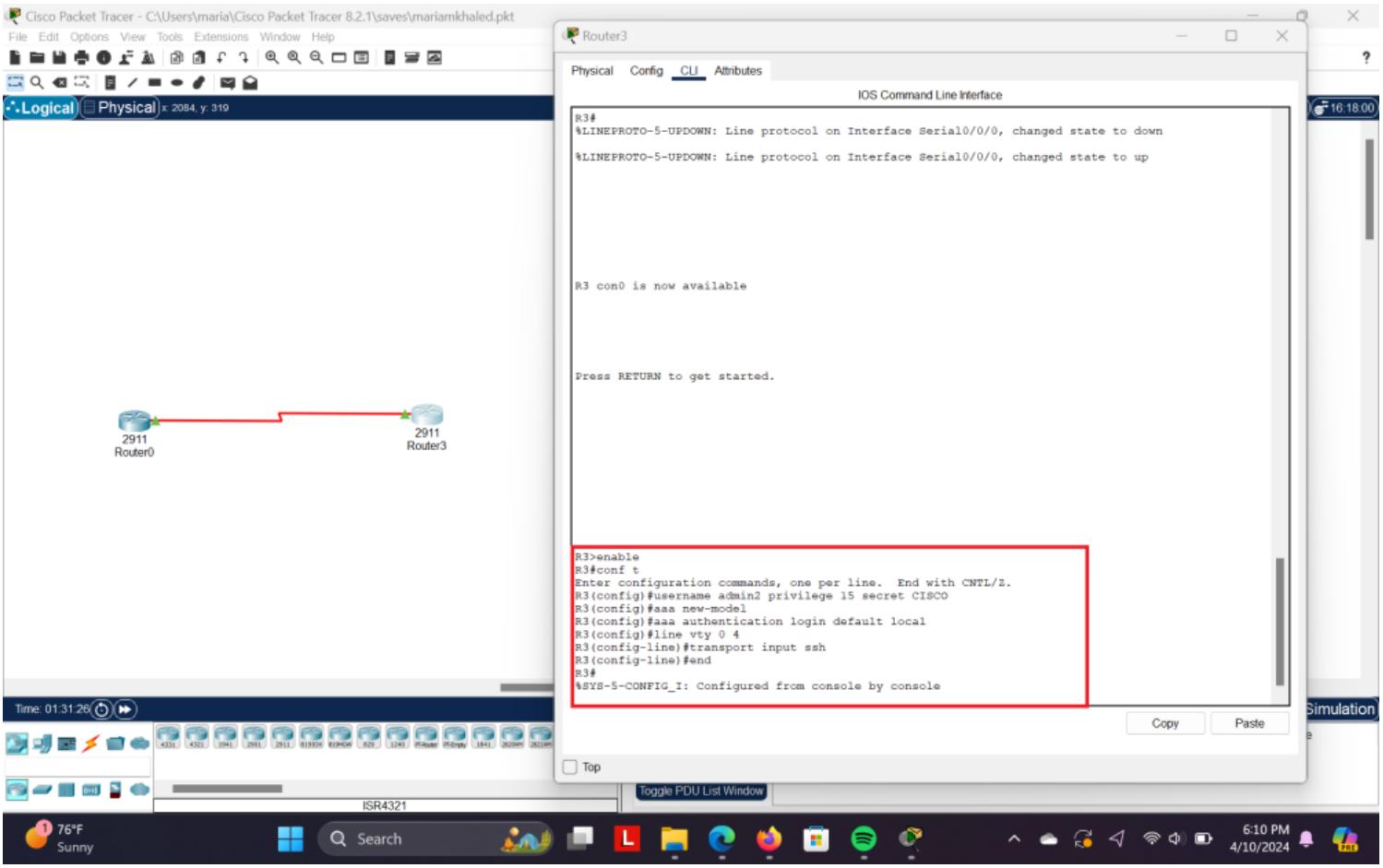
👉The command ip route 0.0.0.0 0.0.0.0 172.16.1.2 tells router R1: ' send packet from any address to 172.16.1.2 (R3).' It's like a default instruction for where to forward traffic when there's no specific route.



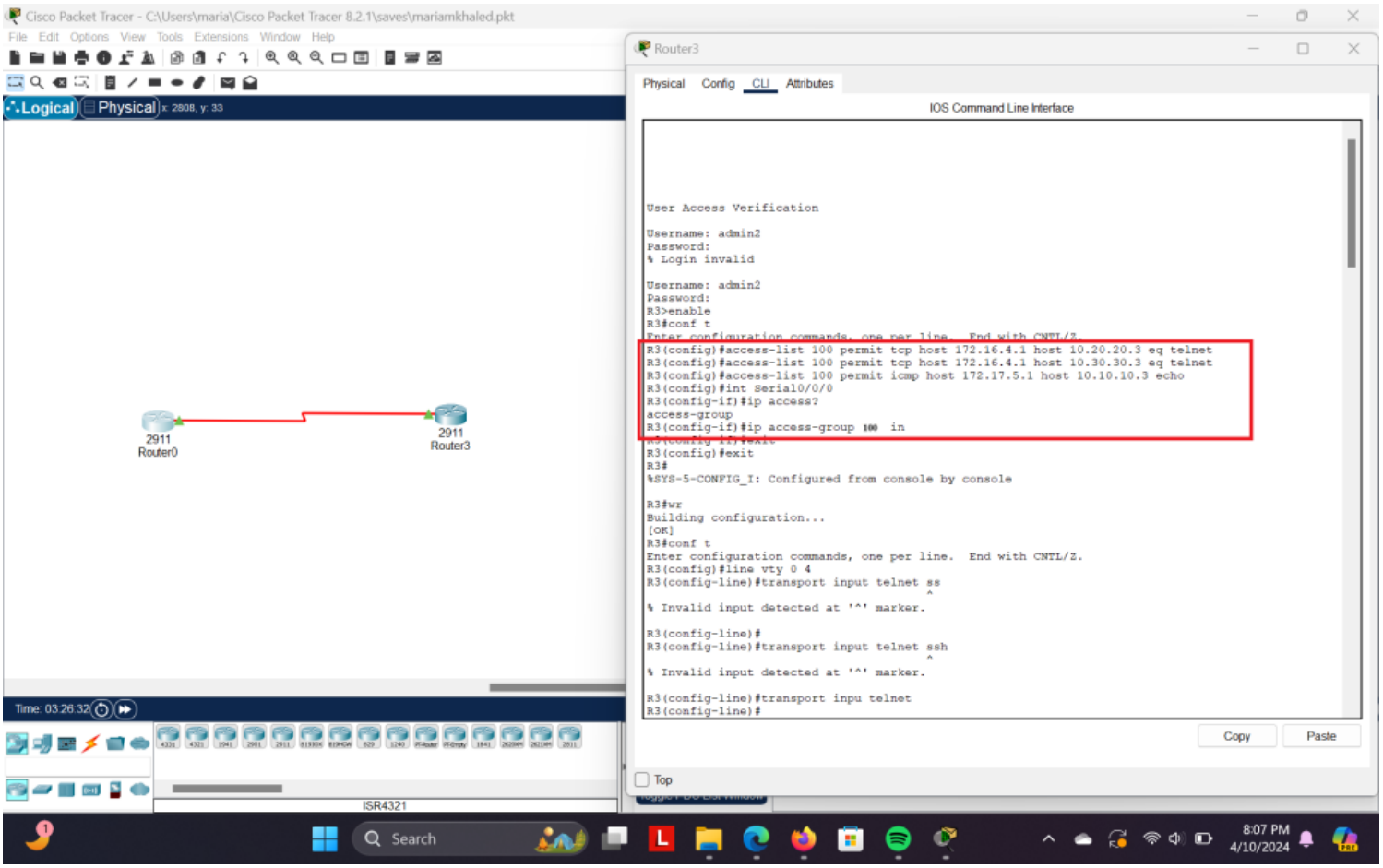
👉The command ip route 0.0.0.0 0.0.0.0 172.16.1.1 tells router R3: 'send packets from any address to 172.16.1.1 (R1).' It acts as a default instruction for forwarding traffic when no specific route is found.



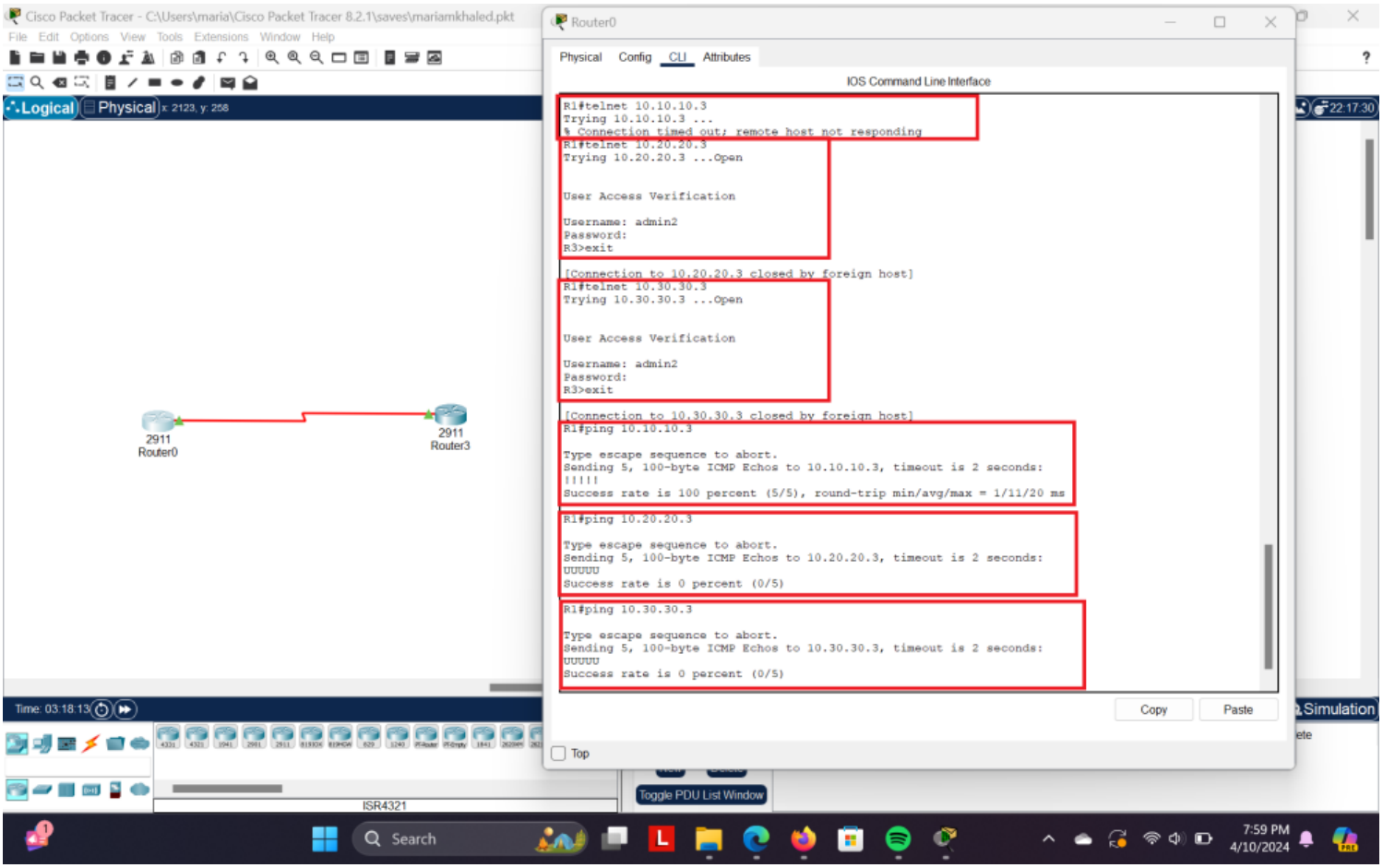
I configured both R1 routers to allow SSH connections with the password 'CISCO' set for SSH access.



I configured both R3 routers to permit SSH connections, utilizing the password 'CISCO' for SSH access.



For the first two commands, I permitted telnet connections from Router 1's Loopback10 to Router 3's Loopback20 and Loopback30.
For the third command, I allowed ping requests from Router 1's Loopback20 to Router 3's Loopback10.
👉Finally, I applied this ACL inbound on R3's Serial port.



I tested the Telnet ACL configuration by attempting Telnet connections from R1's Loopback10 to R3's Loopback10, Loopback20, and Loopback30 interfaces. Furthermore, I verified the ping ACL configuration by sending ping requests from R1's Loopback20 to R3's Loopback10, Loopback20, and Loopback30 interfaces.