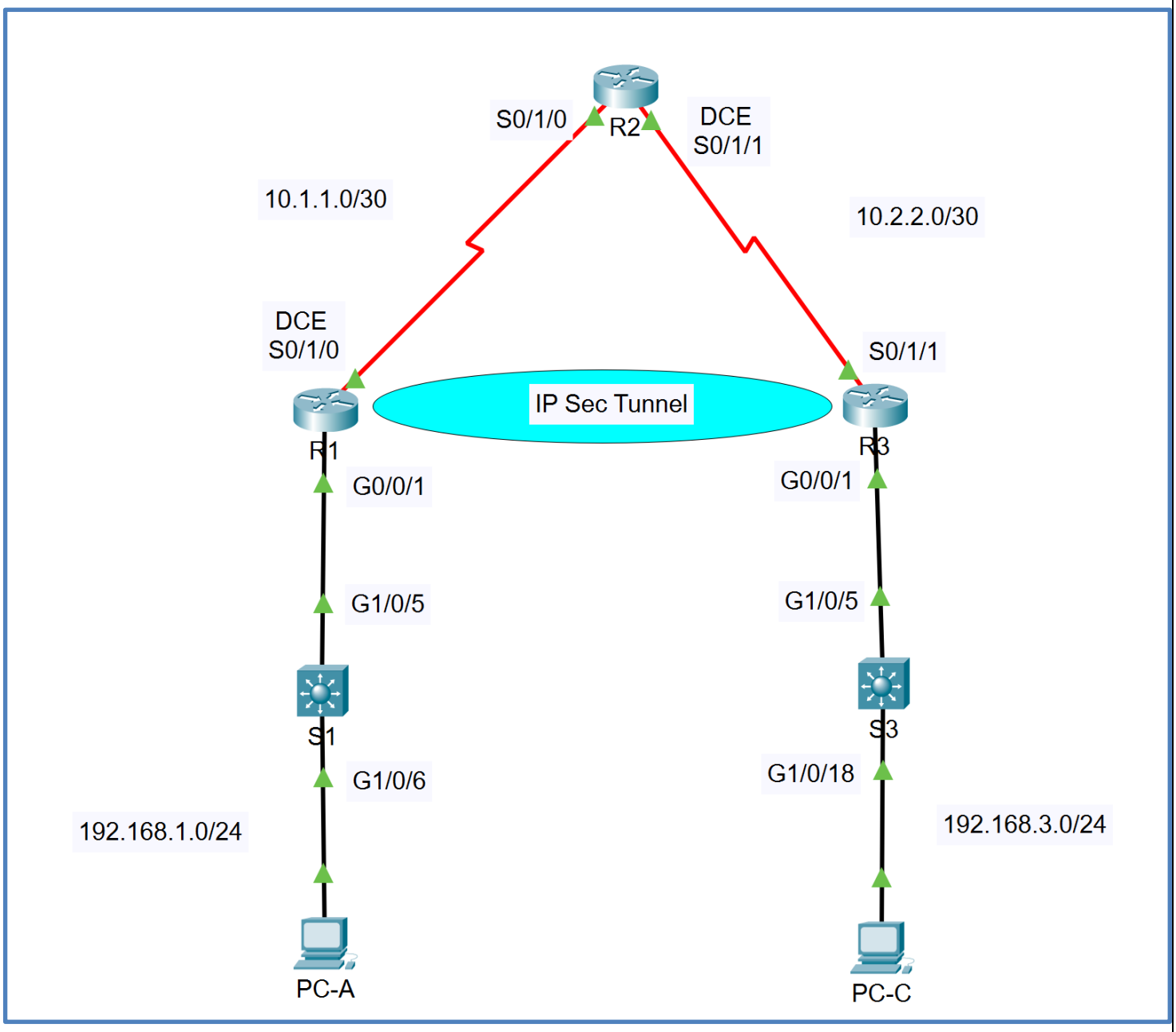
Lab Activity: VPN Configuration (Phase 1):

There are two LANs and two site-to-site WANs in following the topology. Please develop the following topology on the physical pod/rack in the lab room.



IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0/1	192.168.1.1	255.255.255.0	N/A	S1 G1/0/5
	S0/1/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/1/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/1/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/0/1	192.168.3.1	255.255.255.0	N/A	S3 G1/0/5
	S0/1/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 G1/0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 G1/0/18

Objectives

Part 1: Configure Basic Device Settings

- Configure hostnames, interface IP addresses, and access passwords.
- Configure the OSPF dynamic routing protocol.

Part 2: Configure a Site-to-Site VPN Using Cisco IOS

- Configure IPsec VPN settings on R1 and R3.
- Verify site-to-site IPsec VPN configuration.
- Test IPsec VPN operation.

Part 3 (Lab 15 – Phase 2): Configure a Site-to-Site VPN Using CCP

- Configure IPsec VPN settings on R1.
- Create a mirror configuration for R3.
- Apply the mirror configuration to R3.
- Verify the configuration.
- Test the VPN configuration using CCP.

Background/Scenario

VPNs can provide a secure method of transmitting data over a public network such as the Internet. VPN connections can help reduce the costs associated with leased lines. Site-to-site VPNs typically provide a secure (IPsec or other) tunnel between a branch office and a central office. Another common implementation that uses VPN technology is remote access to a corporate office from a telecommuter location, such as a small office or home office.

In this lab, you will build and configure a multi-router network, use Cisco IOS and CCP to configure a site-to-site IPsec VPN, and test it. The IPsec VPN tunnel is from router R1 to router R3 via R2. R2 acts as a pass-through and has no knowledge of the VPN. IPsec

provides secure transmission of sensitive information over unprotected networks such as the internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (peers) such as Cisco routers.

Note: Make sure that the routers and the switches have been erased and have no startup configurations.

Required Resources:

- Two 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 (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.

To run CCP, it may be necessary to temporarily disable antivirus programs and O/S firewalls. Make sure that all pop-up blockers are turned off in the browser.

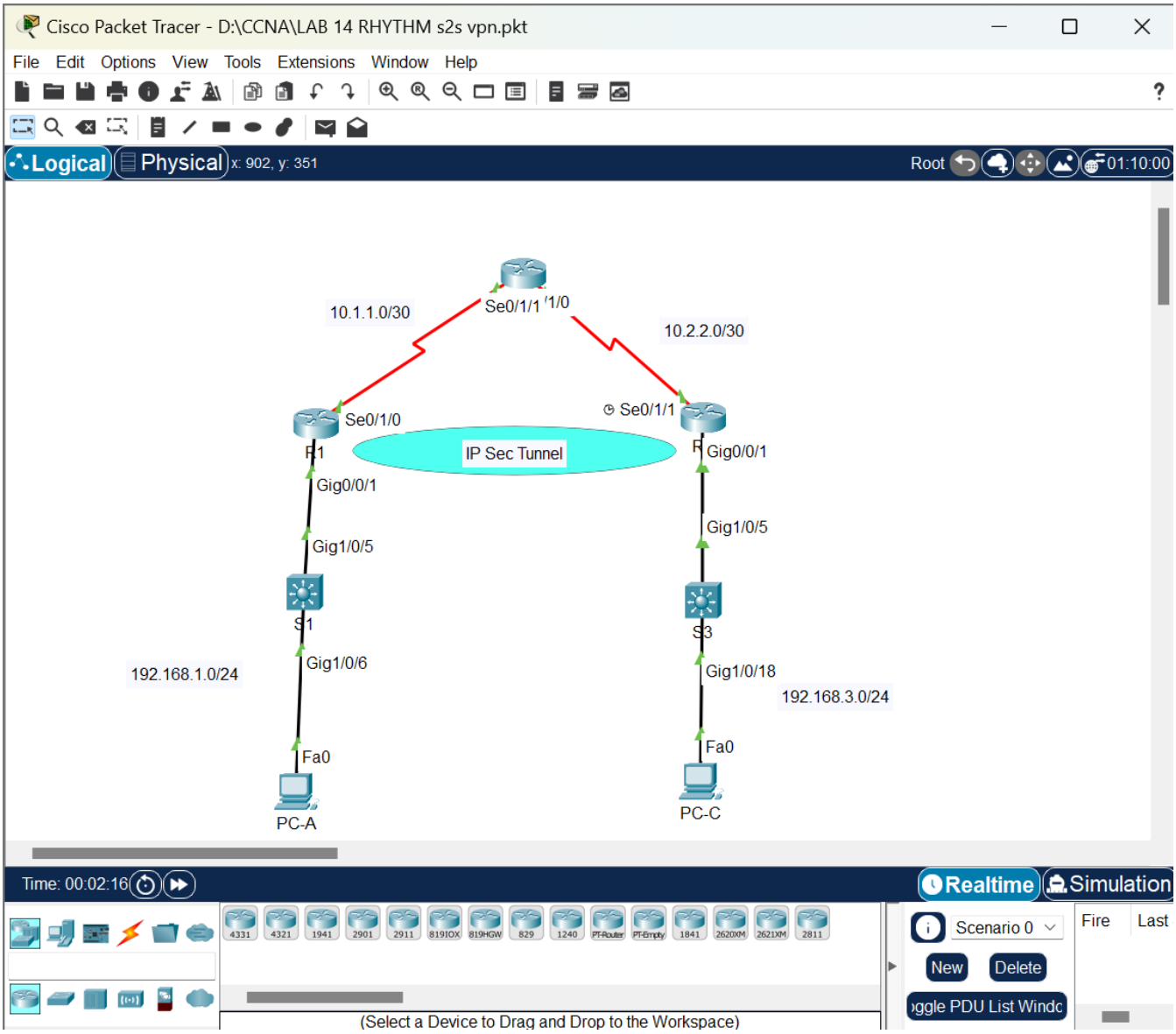
Part 1: Configure Basic Device Settings

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

Note: All tasks should be performed on R1, R2, and R3. The procedure for R1 is shown here as an example.

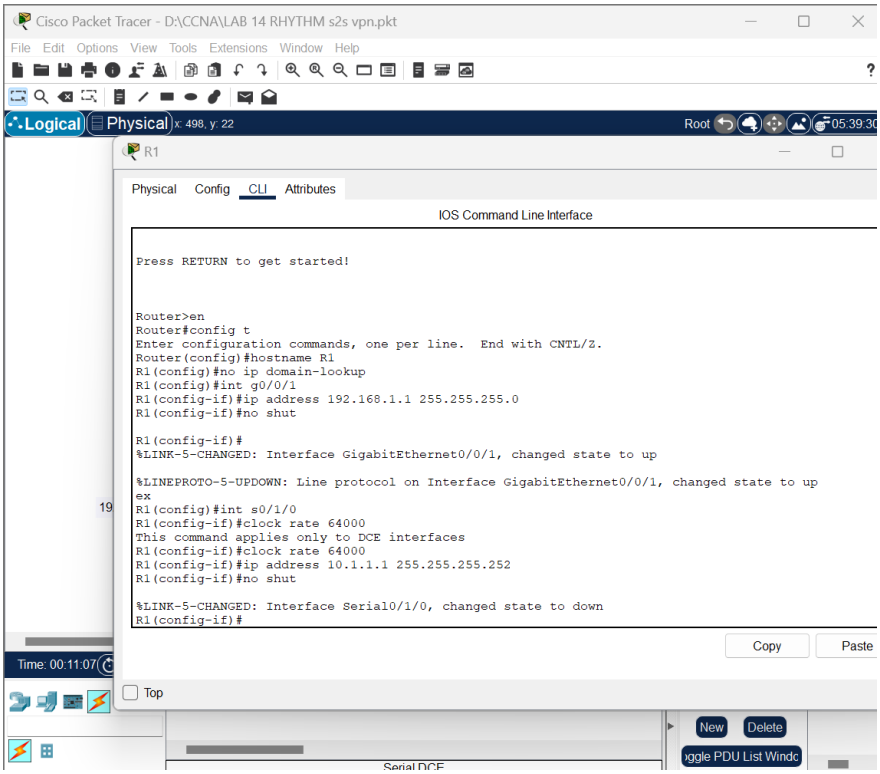
Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram and cable as necessary.

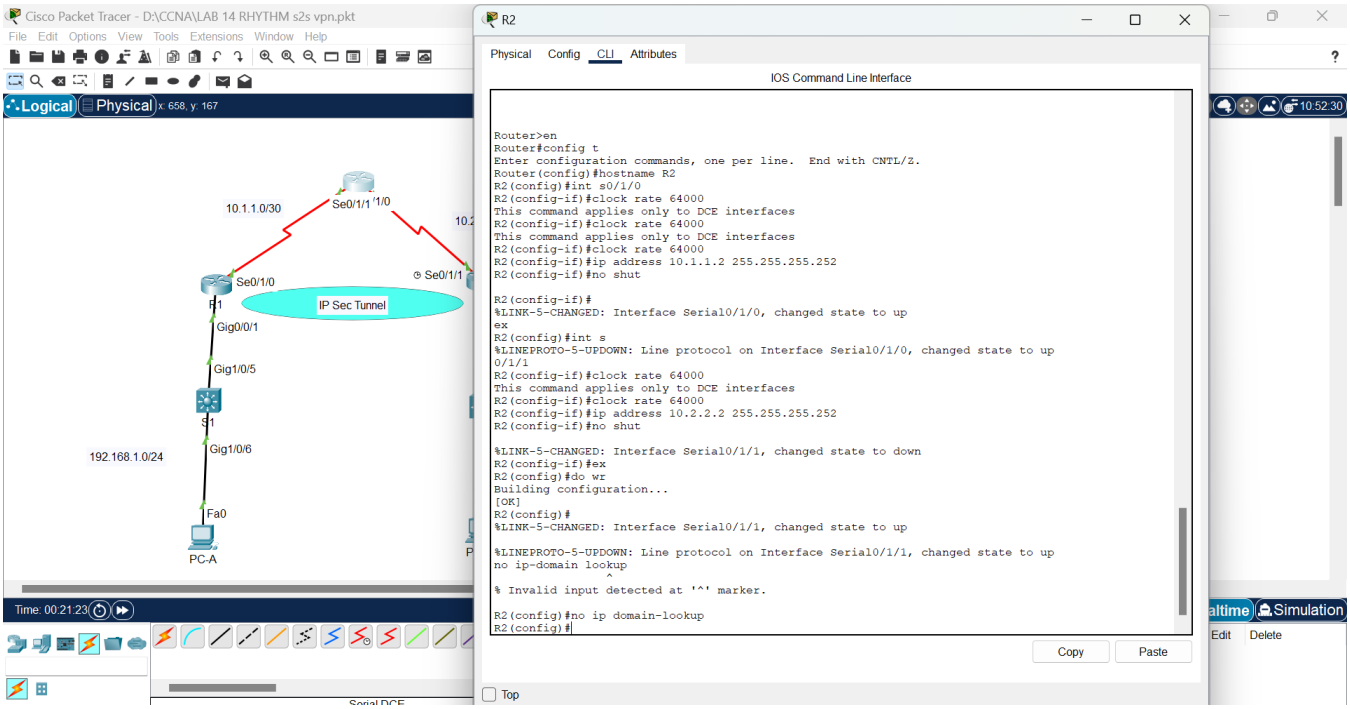


Step 2: Configure basic settings for each router.

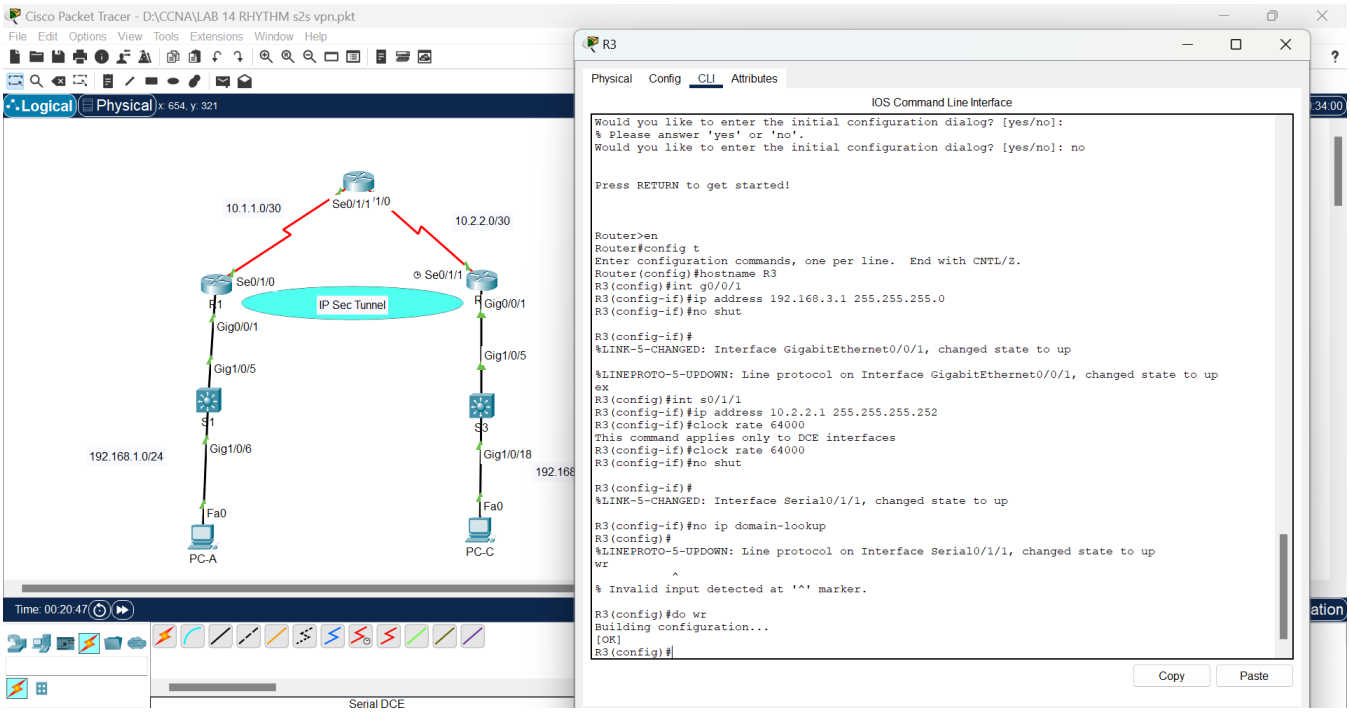
R1



R2



R3



a. Configure hostnames as shown in the topology.

b. Configure the interface IP addresses as shown in the IP Addressing Table.

c. Configure a clock rate of **64000** for the serial router interfaces with a DCE serial cable attached.

```
R1(config)# interface S0/1/0
R1(config-if)# clock rate 64000
```

Step 3: Disable DNS lookup.

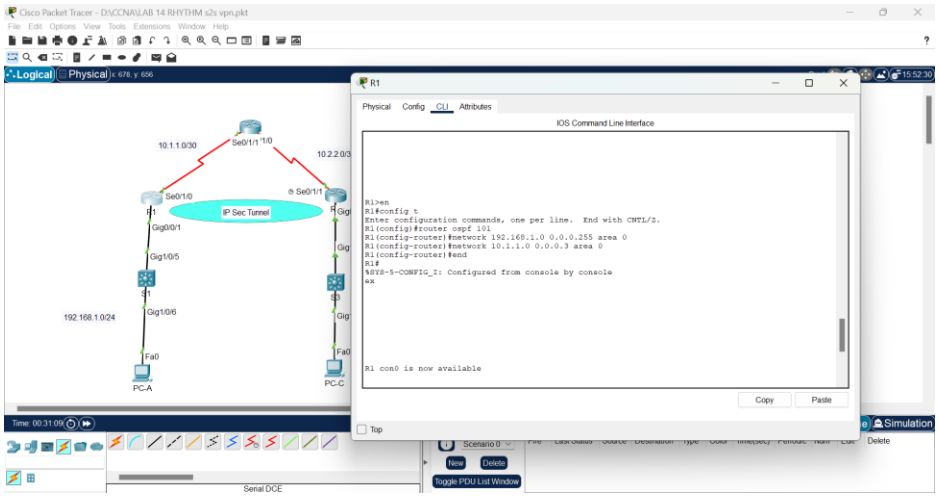
To prevent the router from attempting to translate incorrectly entered commands, disable DNS lookup.

```
R1(config)# no ip domain-lookup
```

Step 4: Configure the OSPF routing protocol on R1, R2, and R3.

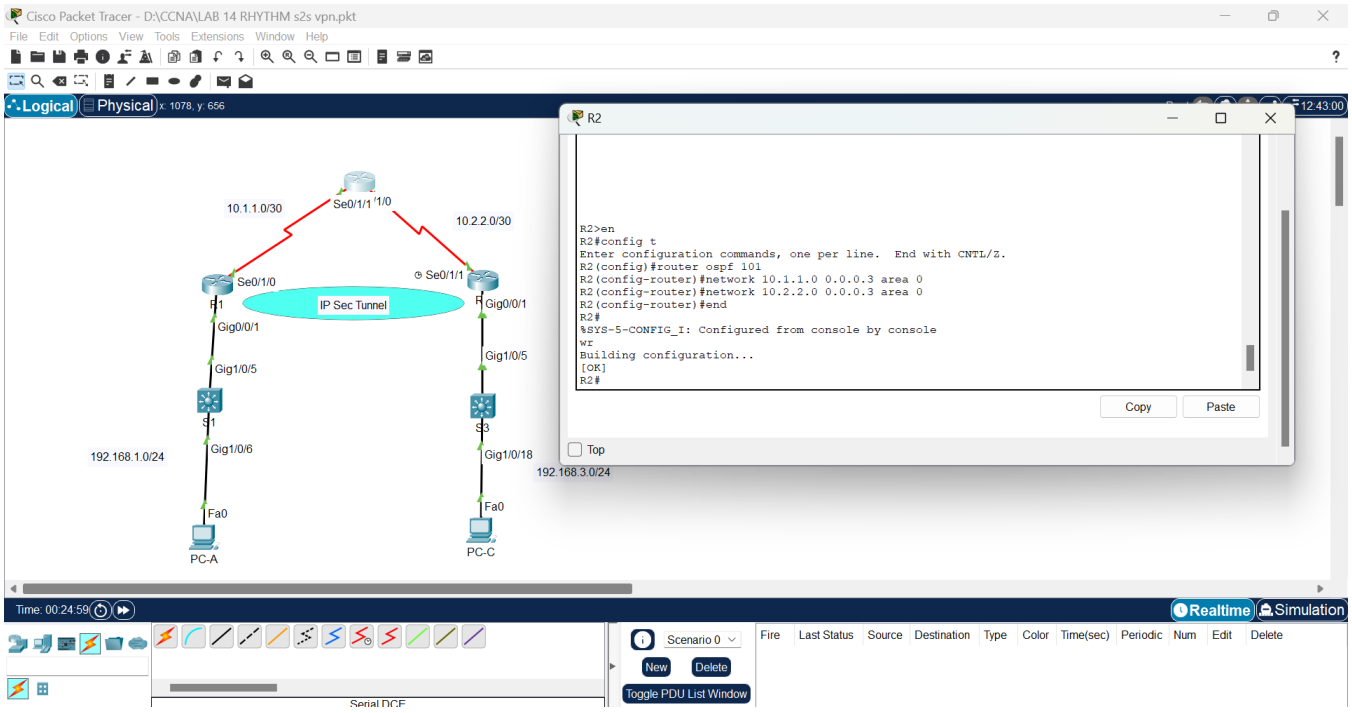
a. On R1, use the following commands:

```
R1(config)# router ospf 101
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
```



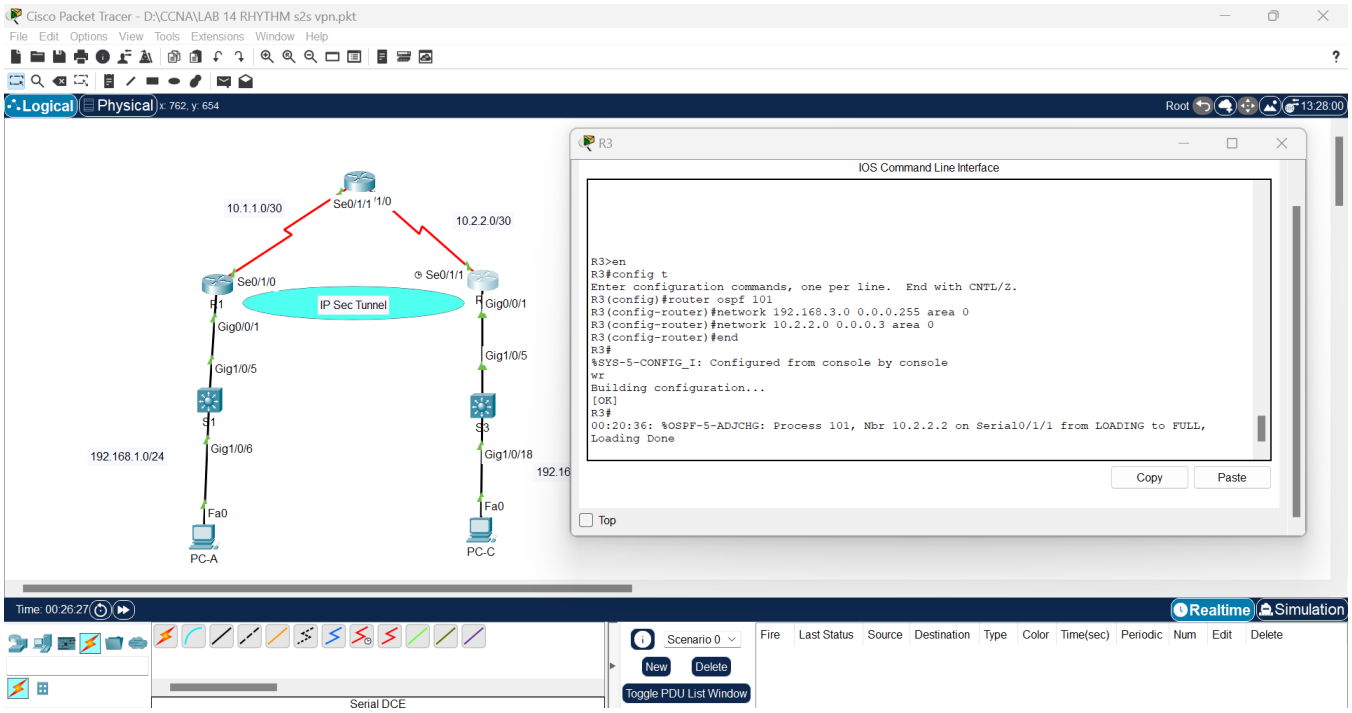
b. On R2, use the following commands:

```
R2(config)# router ospf 101
R2(config-router)# network 10.1.1.0 0.0.0.3 area 0
R2(config-router)# network 10.2.2.0 0.0.0.3 area 0
```



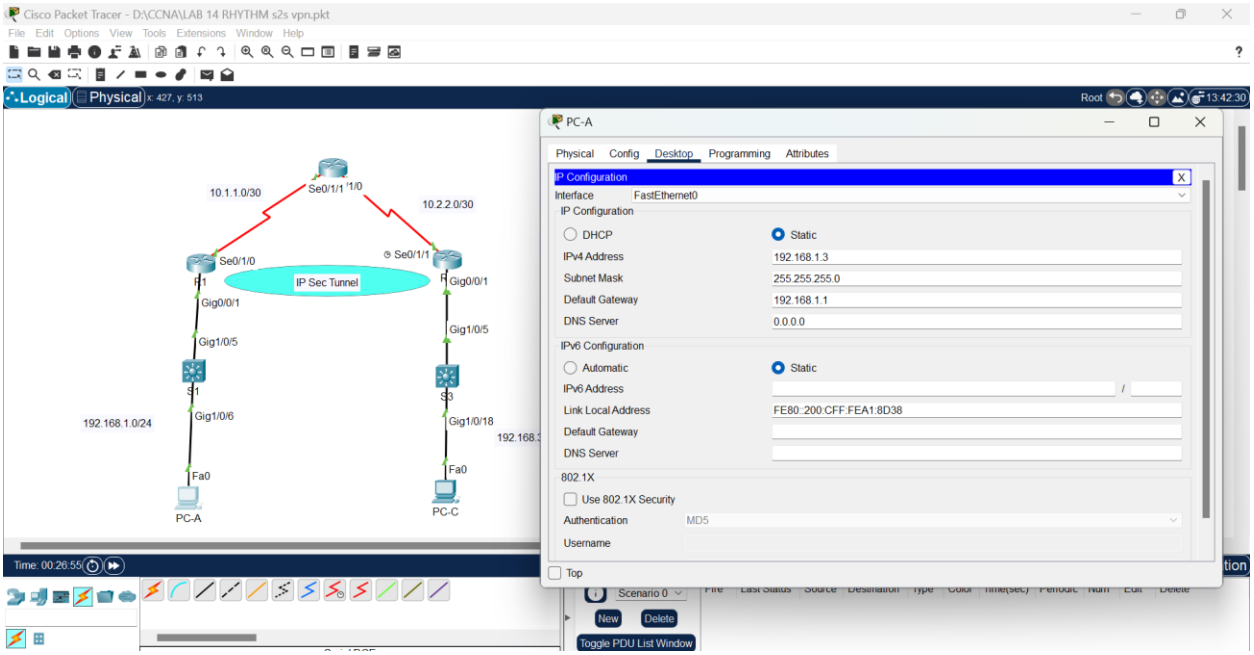
c. On R3, use the following commands:

```
R3(config)# router ospf 101
R3(config-router)# network 192.168.3.0 0.0.0.255 area 0
R3(config-router)# network 10.2.2.0 0.0.0.3 area 0
```

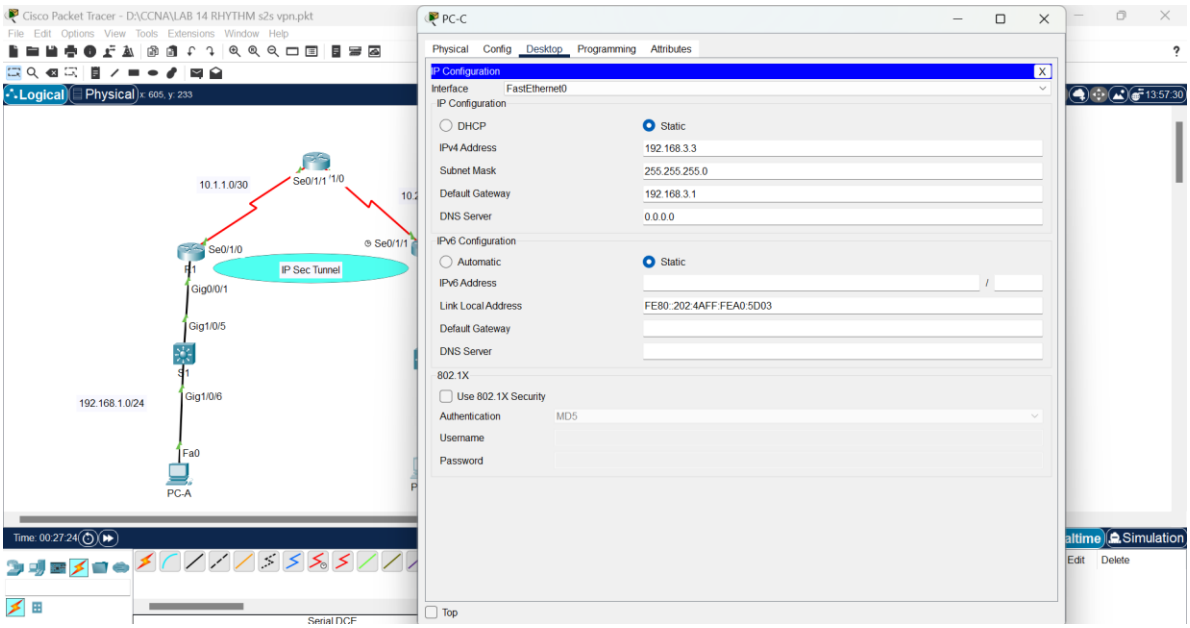


Step 5: Configure PC host IP settings.

a. Configure a static IP address, subnet mask, and default gateway for PC-A as shown in the IP Addressing Table.

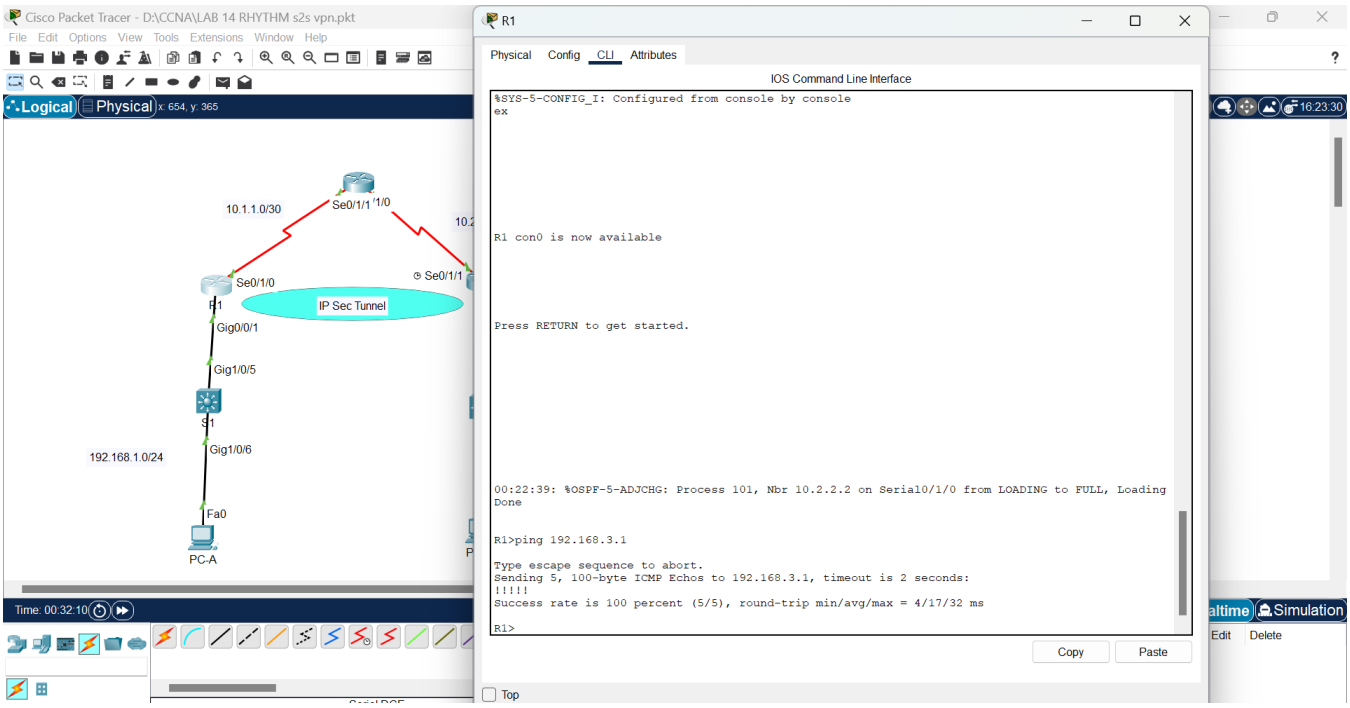


b. Configure a static IP address, subnet mask, and default gateway for PC-C as shown in the IP Addressing Table.



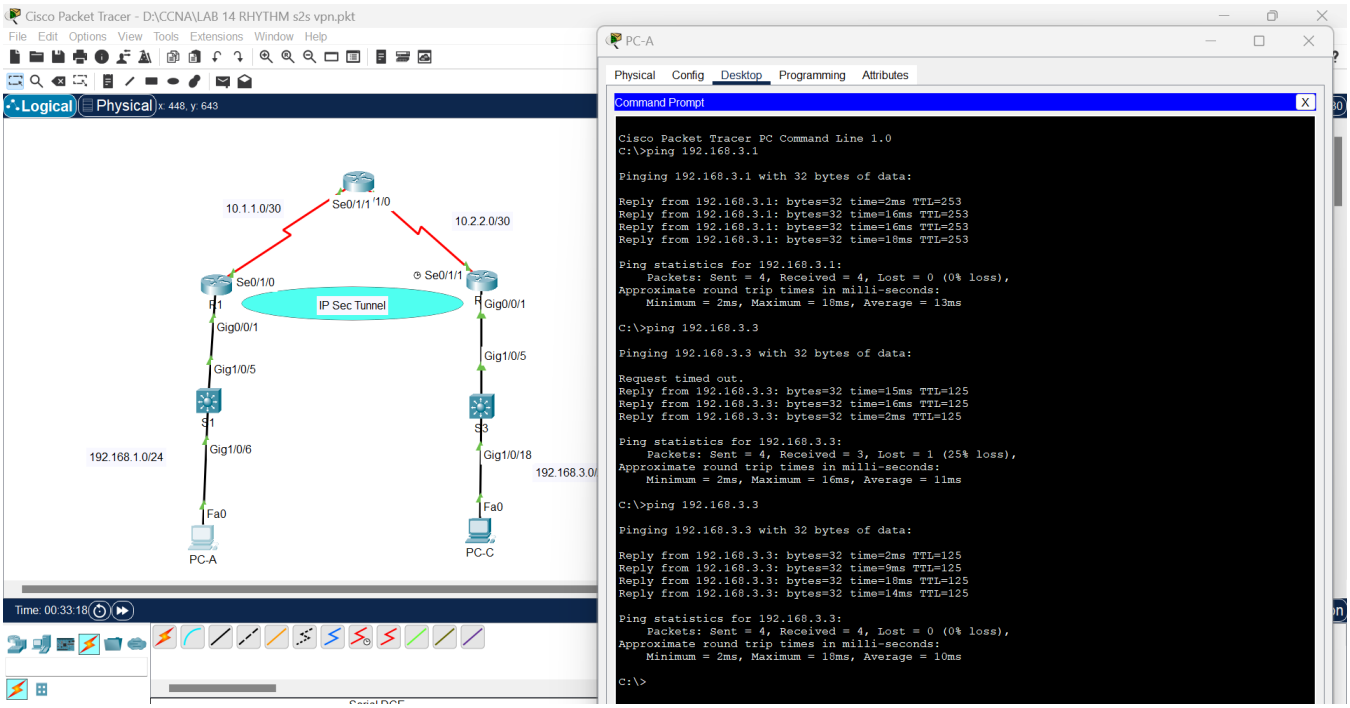
Step 6: Verify basic network connectivity.

a. Ping from R1 to the R3 G0/0/1 interface at IP address **192.168.3.1**.



If the pings are unsuccessful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A on the R1 LAN to PC-C on the R3 LAN.



If the pings are unsuccessful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-A to PC-C, you have demonstrated that the OSPF routing protocol is configured and functioning correctly. If you cannot ping, but the device interfaces are up and IP addresses are correct, use the **show run** and **show ip route** commands to help identify routing protocol-related problems.

Step 7: Configure a minimum password length.

Note: Passwords in this lab are set to a minimum of 10 characters but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

Use the **security passwords** command to set a minimum password length of **10** characters.

```
R1(config)# security passwords min-length 10
```

Step 8: Configure the basic console and vty lines.

a. Configure **ciscoconpass** as the console password and enable login for R1. For additional security, the **exec-timeout** command causes the line to log out after **5** minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry.

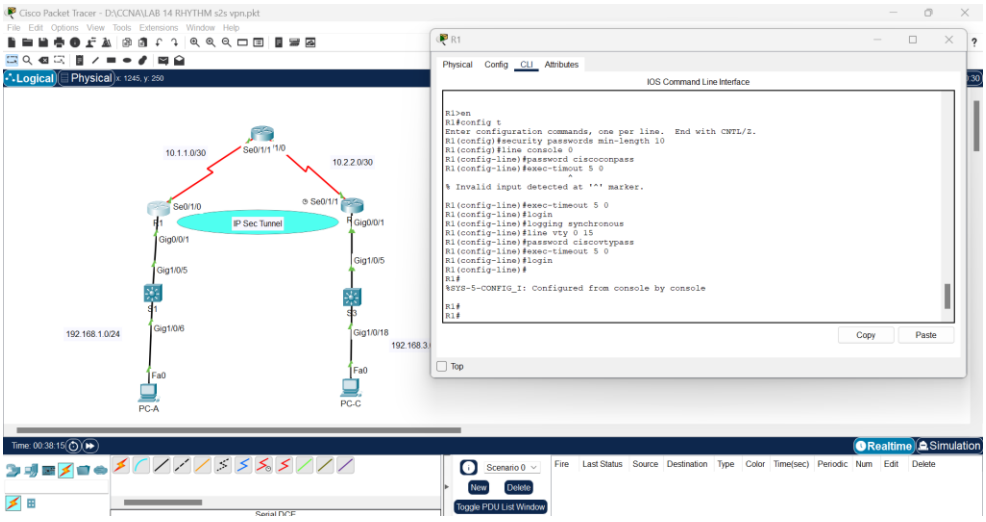
```
R1(config)# line console 0
R1(config-line)# password ciscoconpass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous
```

b. Configure **ciscovtypass** as the vty line password and enable login on R1. For additional security, the **exec-timeout** command causes the line to log out after **5** minutes of inactivity.

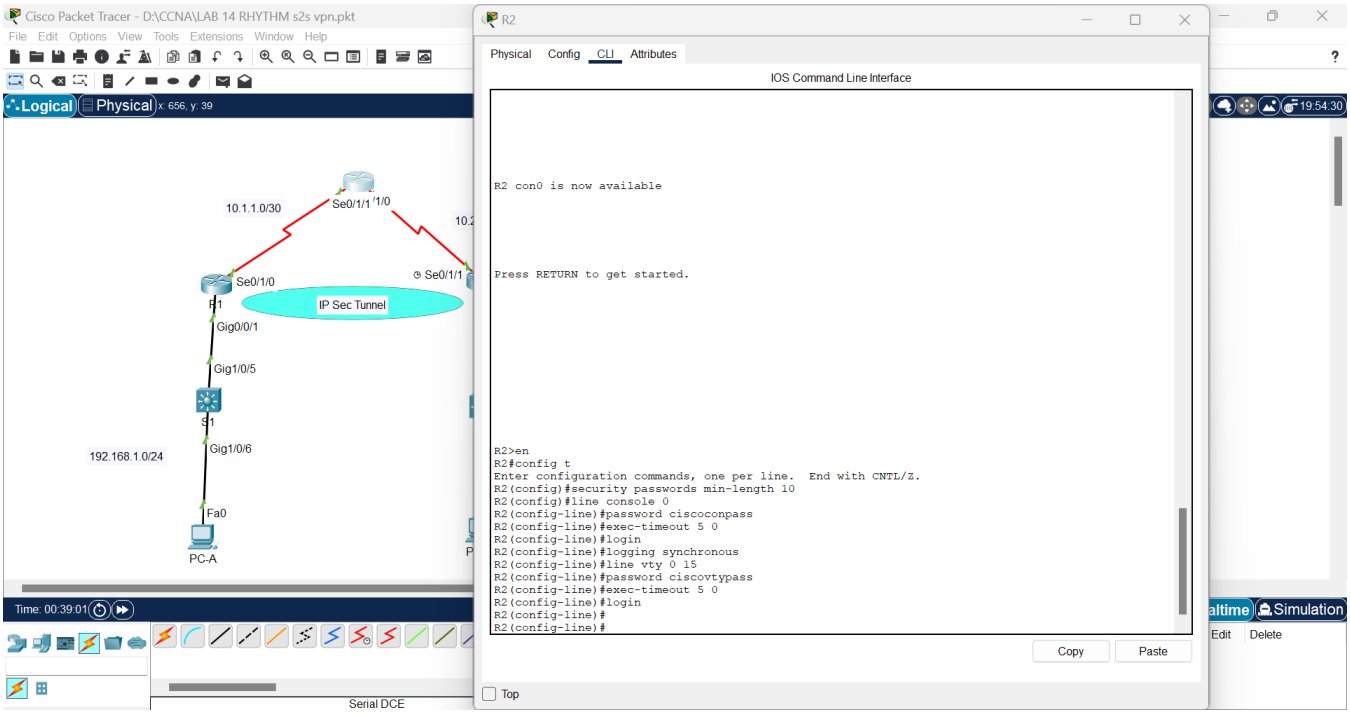
```
R1(config)# line vty 0 15
R1(config-line)# password ciscovtypass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
```

c. Repeat these configurations on both R2 and R3.

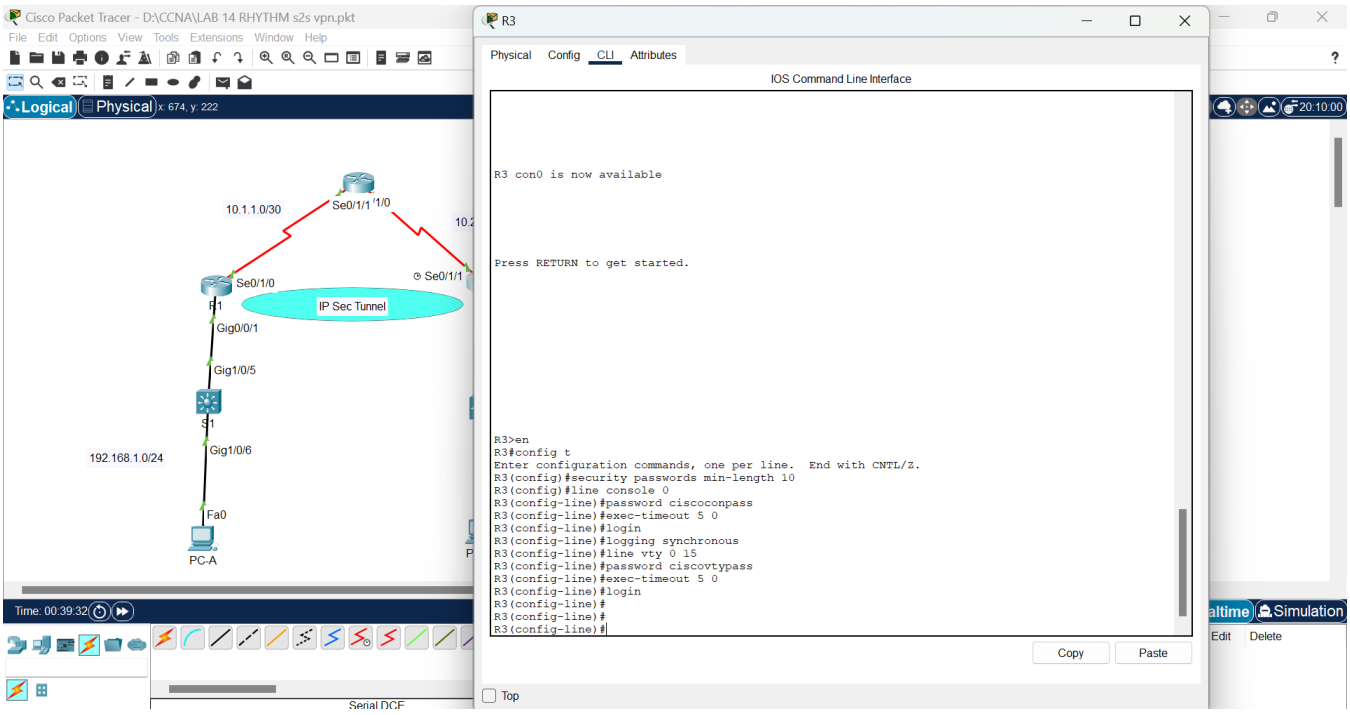
R1



R2


Cisco Packet Tracer - D:\CCNA\LAB 14 RHYTHM s2s vpn.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 656, y: 39
10.1.1.0/30
Se0/1/1
Se0/1/0
R1
IP Sec Tunnel
Gig0/0/1
Gig1/0/5
S1
Gig1/0/6
192.168.1.0/24
Fa0
PC-A
Time: 00:39:01
Serial DCE
R2
Physical Config CLI Attributes
IOS Command Line Interface
R2 con0 is now available
Press RETURN to get started.
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#security passwords min-length 10
R2(config)#line console 0
R2(config-line)#password ciscoconpass
R2(config-line)#exec-timeout 5 0
R2(config-line)#login
R2(config-line)#logging synchronous
R2(config-line)#line vty 0 15
R2(config-line)#password ciscovtypass
R2(config-line)#exec-timeout 5 0
R2(config-line)#login
R2(config-line)#
R2(config-line)#
Copy
Paste
Top
19:54:30
Simulation
Edit
Delete

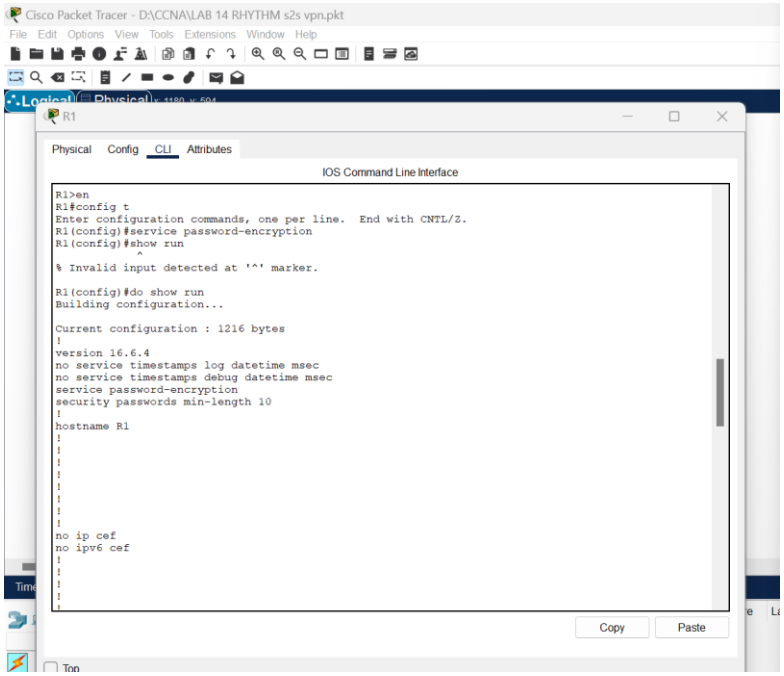
R3


Cisco Packet Tracer - D:\CCNA\LAB 14 RHYTHM s2s vpn.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 674, y: 222
10.1.1.0/30
Se0/1/1
Se0/1/0
R1
IP Sec Tunnel
Gig0/0/1
Gig1/0/5
S1
Gig1/0/6
192.168.1.0/24
Fa0
PC-A
Time: 00:39:32
Serial DCE
R3
Physical Config CLI Attributes
IOS Command Line Interface
R3 con0 is now available
Press RETURN to get started.
R3>en
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#security passwords min-length 10
R3(config)#line console 0
R3(config-line)#password ciscoconpass
R3(config-line)#exec-timeout 5 0
R3(config-line)#login
R3(config-line)#logging synchronous
R3(config-line)#line vty 0 15
R3(config-line)#password ciscovtypass
R3(config-line)#exec-timeout 5 0
R3(config-line)#login
R3(config-line)#
R3(config-line)#
R3(config-line)#
Copy
Paste
Top
20:10:00
Simulation
Edit
Delete

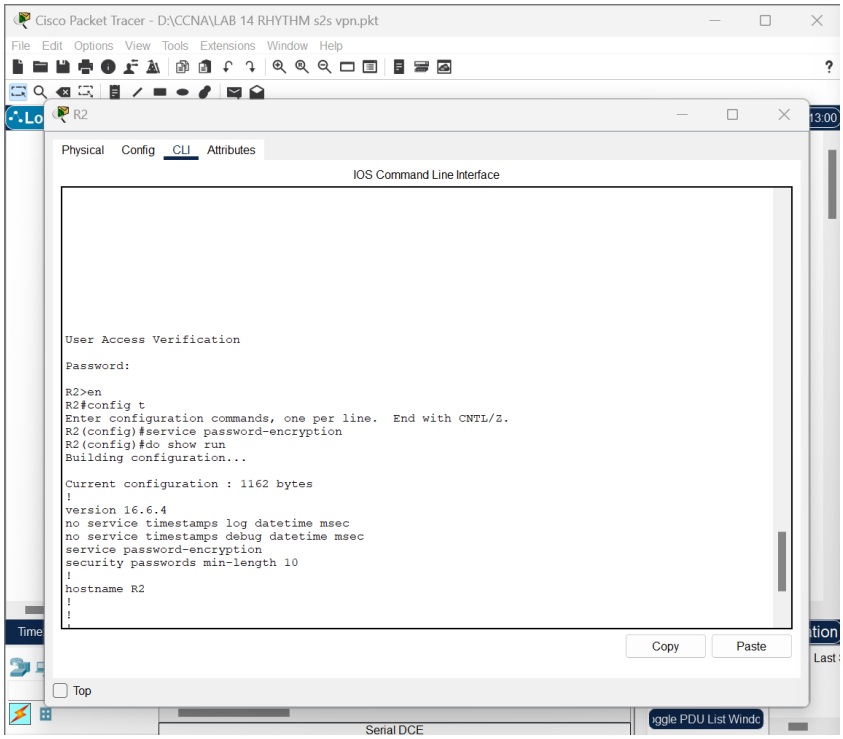
Step 9: Encrypt clear text passwords.

a. Use the **service password-encryption** command to encrypt the console, aux, and vty passwords.

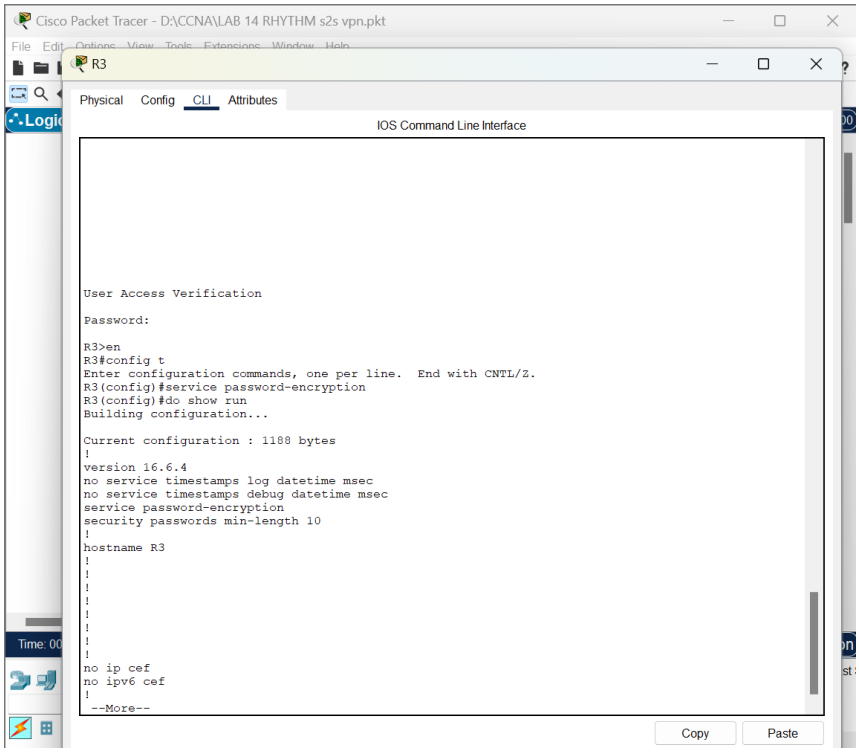
```
R1(config)# service password-encryption
```



R2

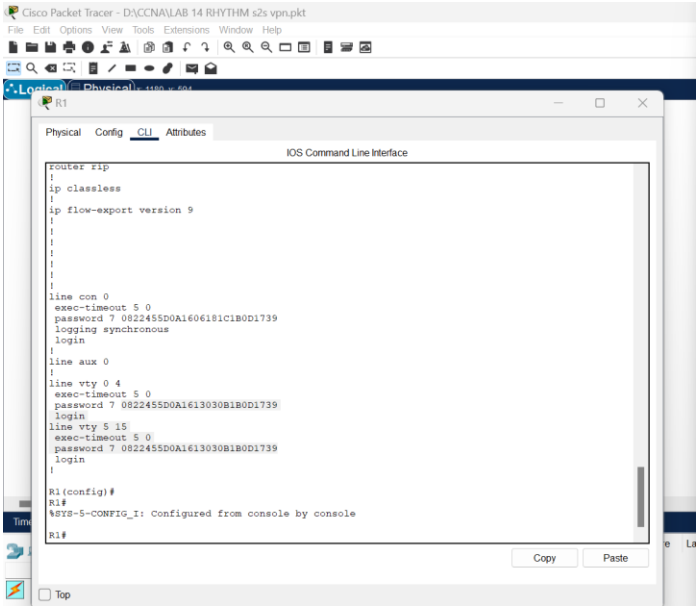


R3



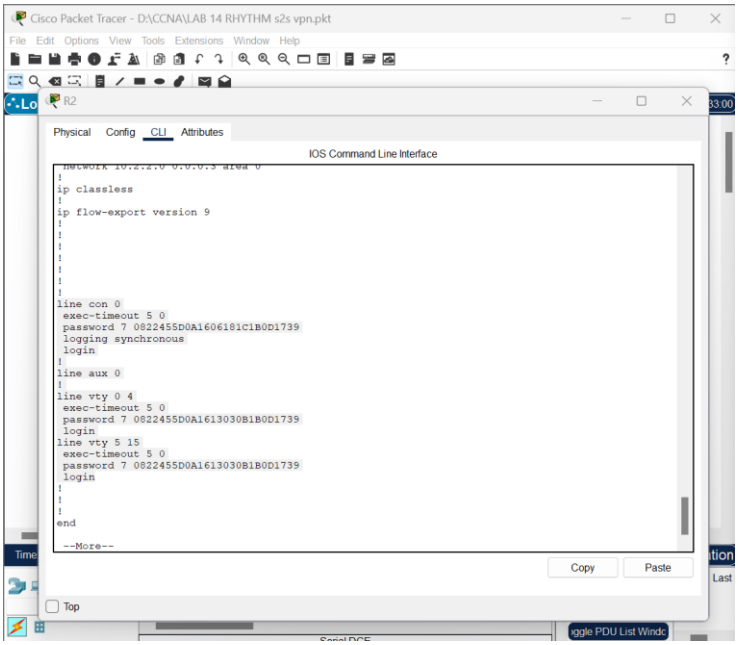
b. Issue the **show run** command. Can you read the console, aux, and vty passwords? Explain. No, I am not able to read console, aur and vty password due to cisco encryption

using **service password-encryption** enable encryption for all plain-text passwords in the configuration file

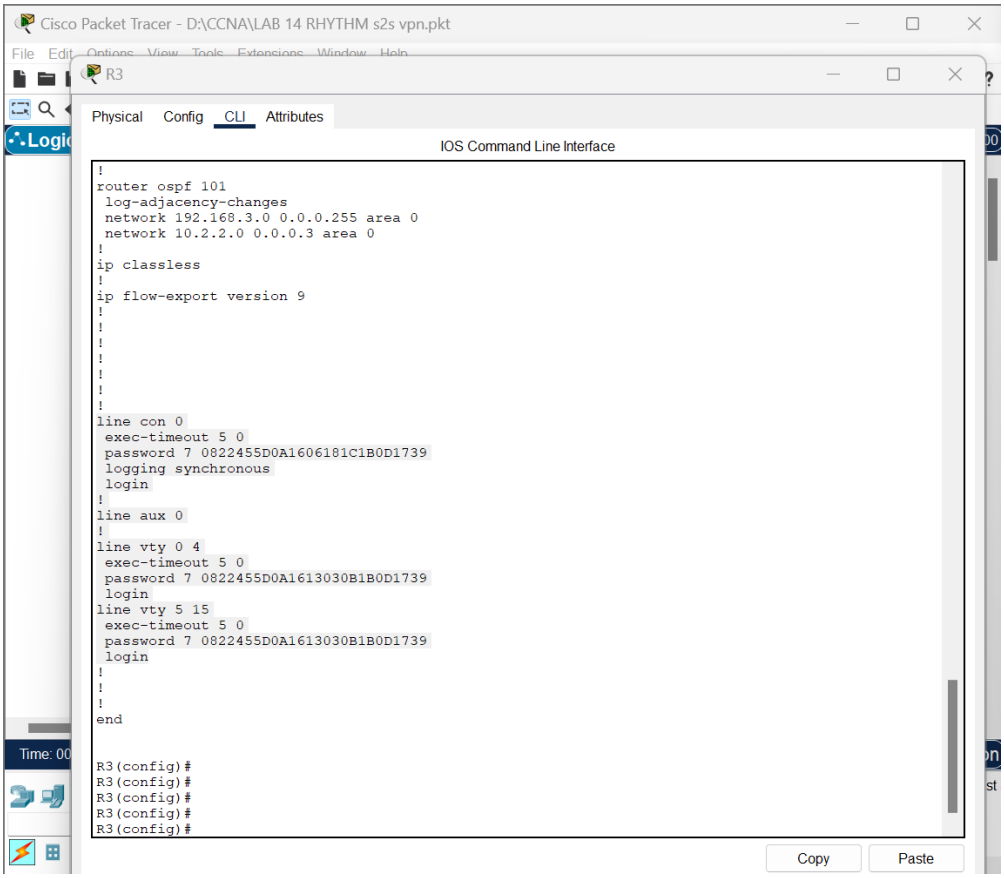


c. Repeat this configuration on both R2 and R3.

R2


Cisco Packet Tracer - D:\CCNA\LAB 14 RHYTHM s2s vpn.pkt
File Edit Options View Tools Extensions Window Help
R2
Physical Config CLI Attributes
IOS Command Line Interface
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
exec-timeout 5 0
password 7 0822455D0A1606181C1B0D1739
logging synchronous
login
!
line aux 0
!
line vty 0 4
exec-timeout 5 0
password 7 0822455D0A1613030B1B0D1739
login
line vty 5 15
exec-timeout 5 0
password 7 0822455D0A1613030B1B0D1739
login
!
!
!
end
--More--
Copy
Paste
Top

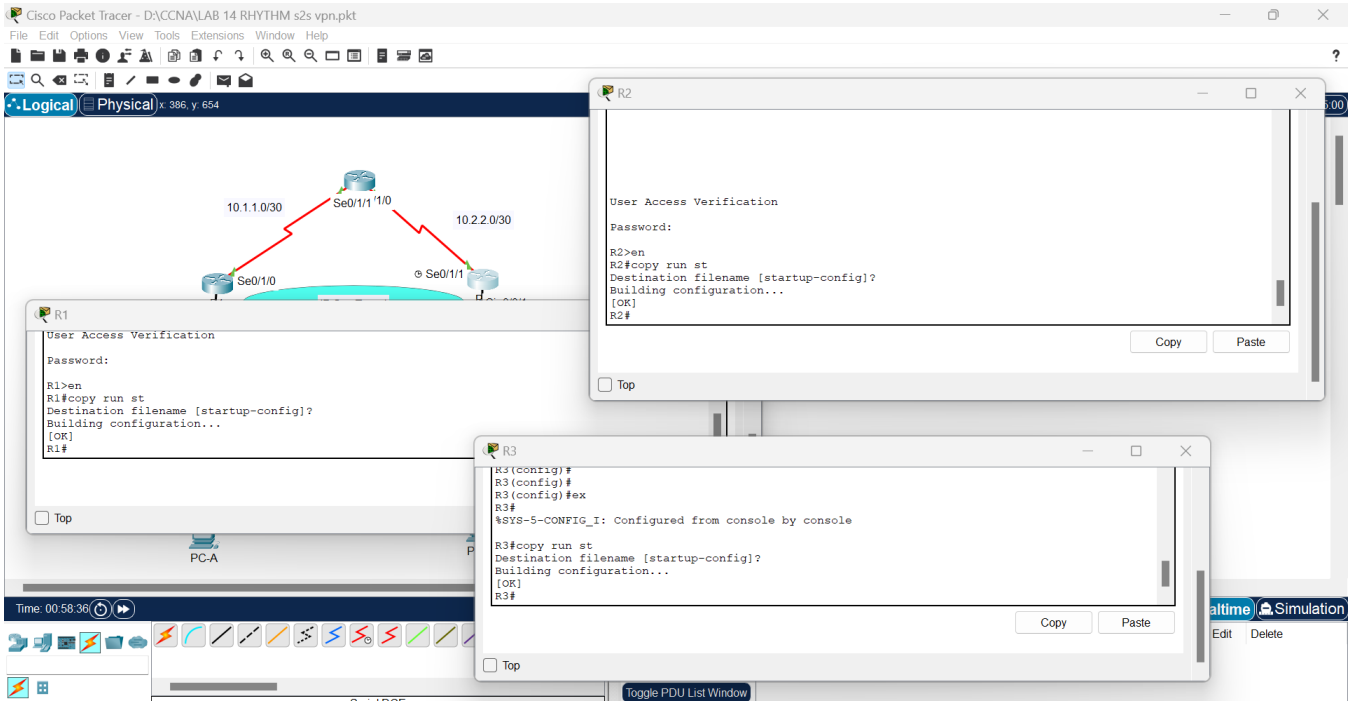
R3


Cisco Packet Tracer - D:\CCNA\LAB 14 RHYTHM s2s vpn.pkt
File Edit Options View Tools Extensions Window Help
R3
Physical Config CLI Attributes
IOS Command Line Interface
!
router ospf 101
log-adjacency-changes
network 192.168.3.0 0.0.0.255 area 0
network 10.2.2.0 0.0.0.3 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
exec-timeout 5 0
password 7 0822455D0A1606181C1B0D1739
logging synchronous
login
!
line aux 0
!
line vty 0 4
exec-timeout 5 0
password 7 0822455D0A1613030B1B0D1739
login
line vty 5 15
exec-timeout 5 0
password 7 0822455D0A1613030B1B0D1739
login
!
!
!
end
R3(config)#
R3(config)#
R3(config)#
R3(config)#
R3(config)#
Copy
Paste

Step 10: Save the basic running configuration for all three routers.

Save the running configuration to the startup configuration from the privileged EXEC mode prompt on R1, R2, and R3.

```
R1# copy running-config startup-config
```



Step 11: Save the configuration on R1 and R3 for later restoration.

Save the R1 and R3 running configurations as text files so the configurations can be used later (in Part 3 of this lab) to restore the routers to configure the VPN with CCP.

Part 2: Configure a Site-to-Site VPN with Cisco IOS

In Part 2 of this lab, you will configure an IPsec VPN tunnel between R1 and R3 that passes through R2. You will configure R1 and R3 using the Cisco IOS CLI. You will then review and test the resulting configuration.

Task 1: Configure IPsec VPN settings on

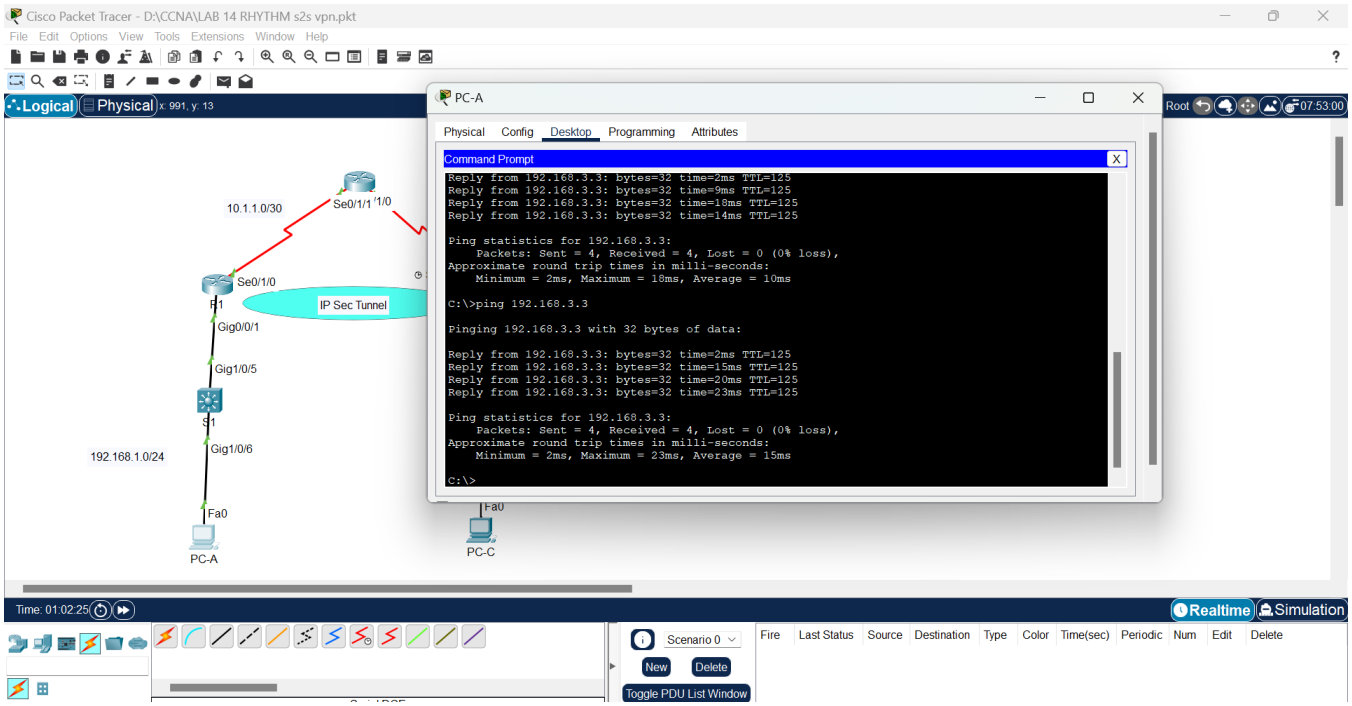
Task 2: R1 and R3.

Step 1: Verify connectivity from the R1 LAN to the R3 LAN.

In this task, you will verify that with no tunnel in place, the PC-A on the R1 LAN can ping the PC-C on R3 LAN.

From PC-A, ping the PC-C IP address of **192.168.3.3**.

```
PC-A:\> ping 192.168.3.3
```



If the pings are unsuccessful, troubleshoot the basic device configurations before continuing.

Step 2: Enable Internet Key Exchange (IKE) policies on R1 and R3.

IPsec is an open framework that allows the exchange of security protocols as new technologies, such as encryption algorithms, are developed.

There are two central configuration elements to the implementation of an IPsec VPN:

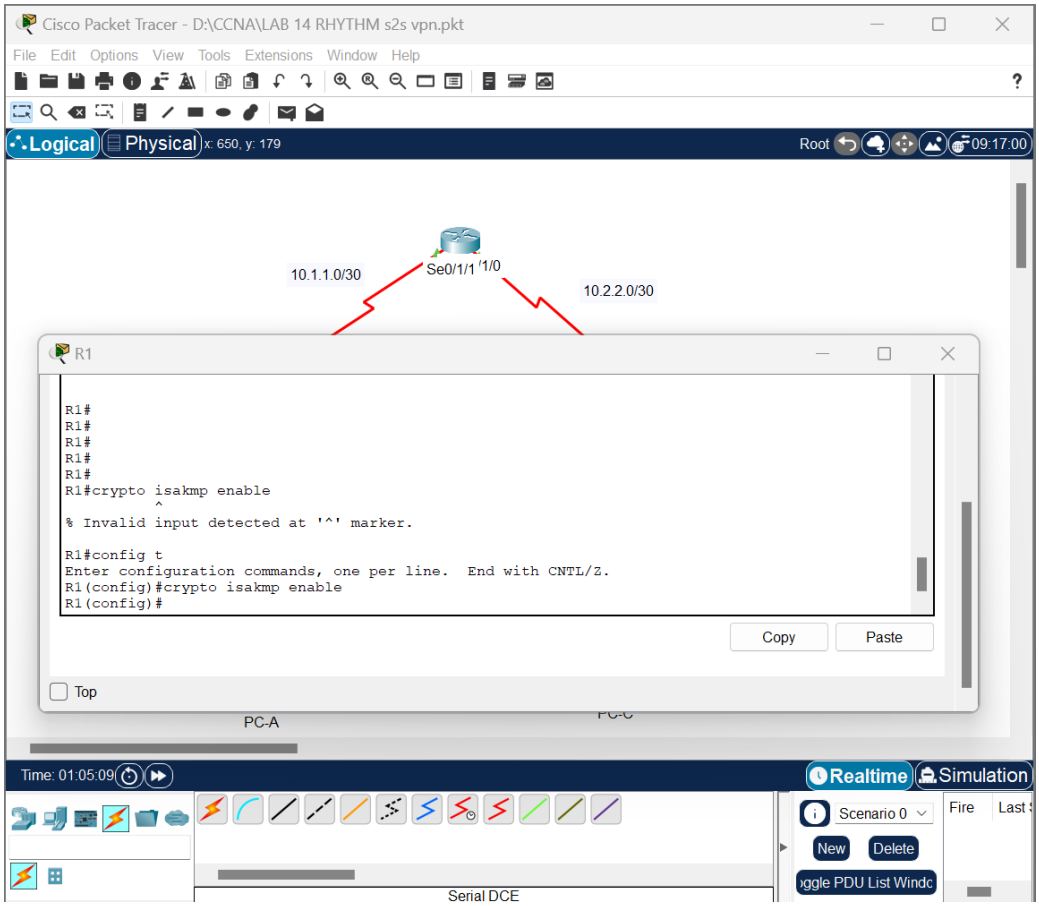
- Implement Internet Key Exchange (IKE) parameters.
- Implement IPsec parameters.

a. Verify that IKE is supported and enabled.

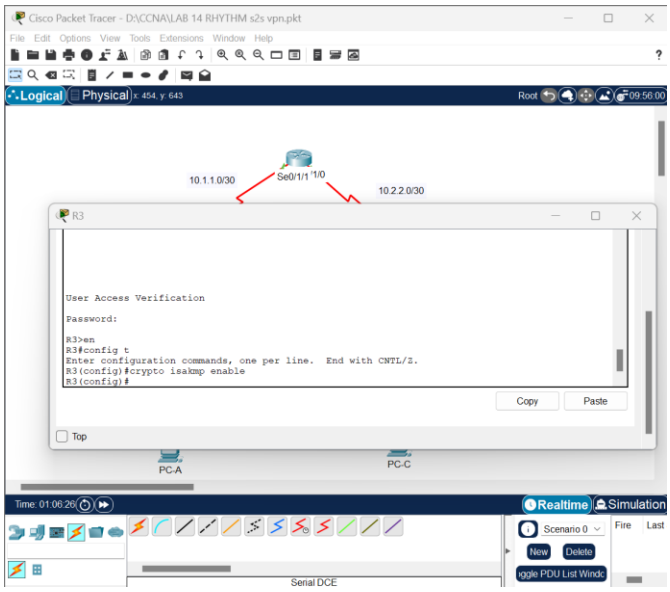
IKE Phase 1 defines the key exchange method used to pass and validate IKE policies between peers. In IKE Phase 2, the peers exchange and match IPsec policies for the authentication and encryption of data traffic.

IKE must be enabled for IPsec to function. IKE is enabled, by default, on IOS images with cryptographic feature sets. If it is disabled, you can enable it with the **crypto isakmp enable** command. Use this command to verify that the router IOS supports IKE and that it is enabled.

R1(config)# ***crypto isakmp enable***



R3(config)# ***crypto isakmp enable***



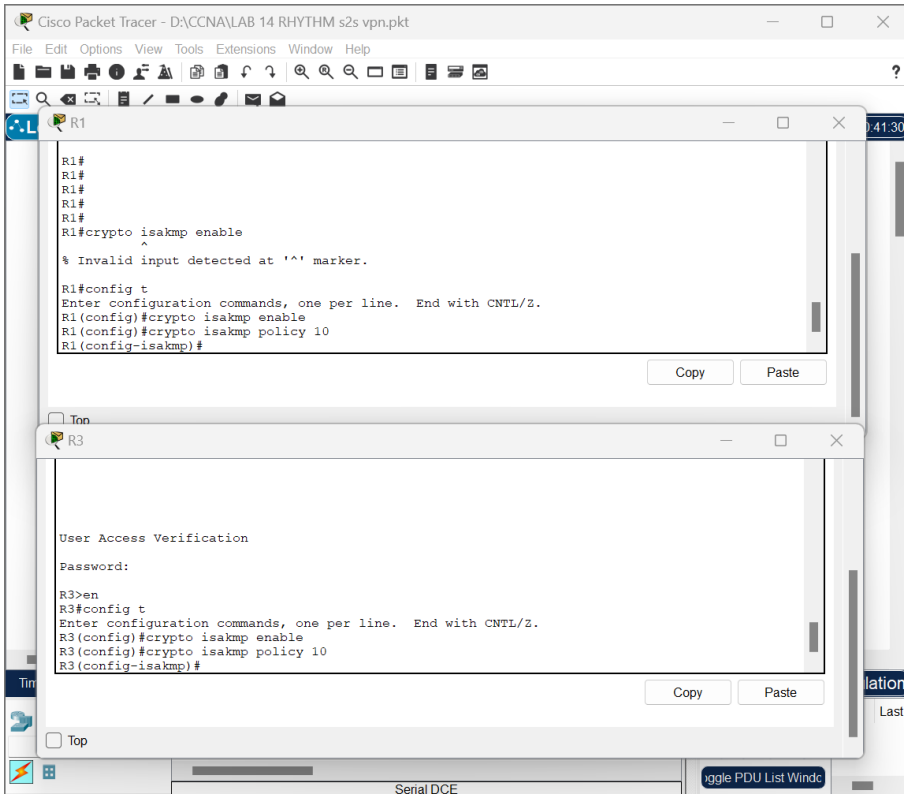
Note: If you cannot execute this command on the router, you must upgrade the IOS image that includes the Cisco cryptographic services.

b. Establish an Internet Security Association and Key Management Protocol (ISAKMP) policy and view the available options.

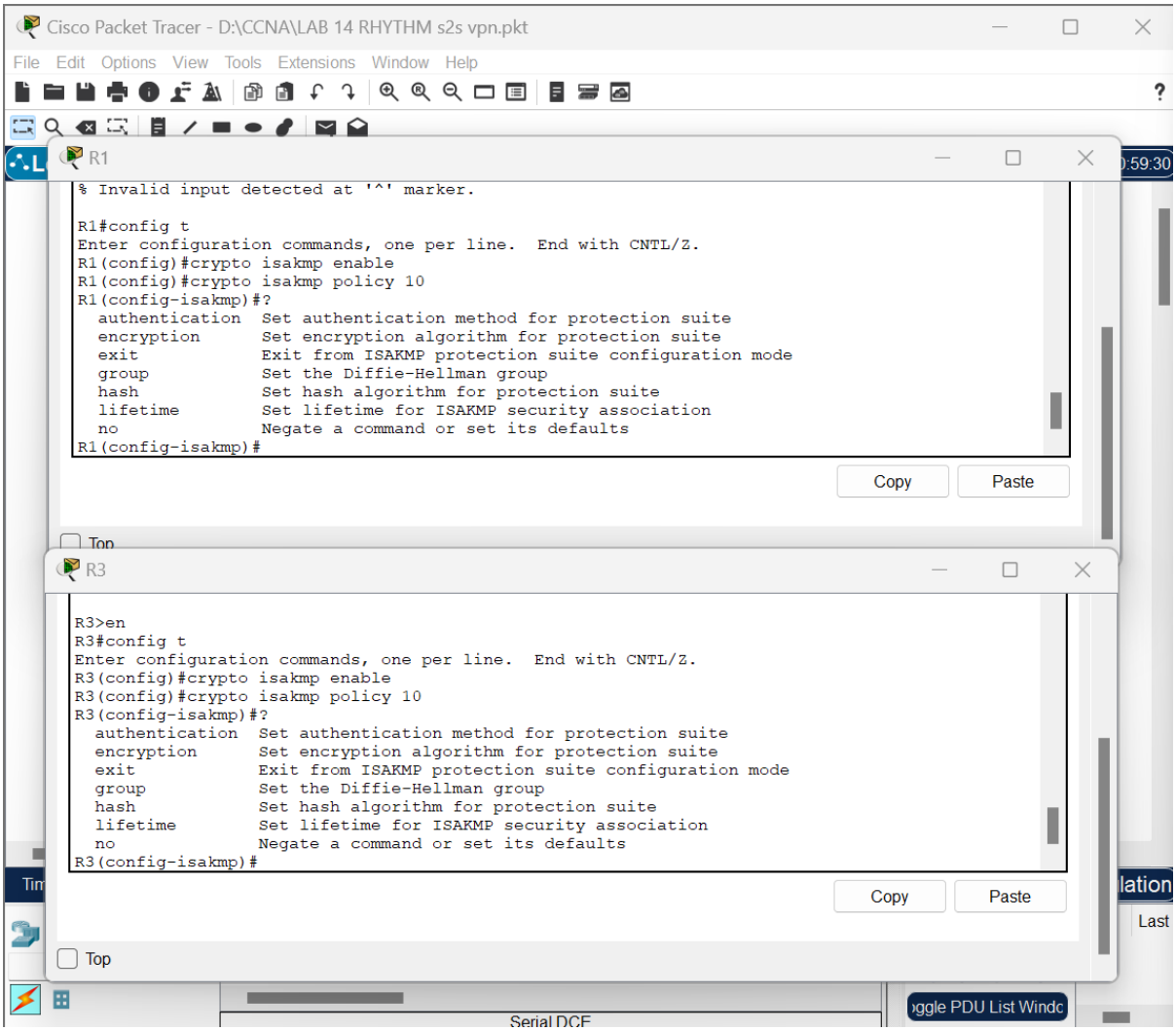
To allow IKE Phase 1 negotiation, you must create an ISAKMP policy and configure a peer association involving that ISAKMP policy. An ISAKMP policy defines the authentication and encryption algorithms and hash function used to send control traffic between the two VPN endpoints. When an ISAKMP security association has been accepted by the IKE peers, IKE Phase 1 has been completed. IKE Phase 2 parameters will be configured later.

Issue the **crypto isakmp policy number** global configuration mode command on R1 for policy 10.

```
R1(config)# crypto isakmp policy 10
```



c. View the various IKE parameters available using Cisco IOS help by typing a question mark (**?**).




```
R1(config-isakmp)# ?

ISAKMP commands:
  authentication  Set authentication method for protection suite
  default         Set a command to its defaults
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite
configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
```

Step 3: Configure ISAKMP policy parameters on R1 and R3.

Your choice of an encryption algorithm determines how confidential the control channel between the endpoints is. The hash algorithm controls data integrity, ensuring the data received from a peer has not been tampered with in transit. The authentication type ensures that the packet was, indeed, sent and signed by the remote peer. The Diffie-Hellman group is used to create a secret key shared by the peers that has not been sent across the network.

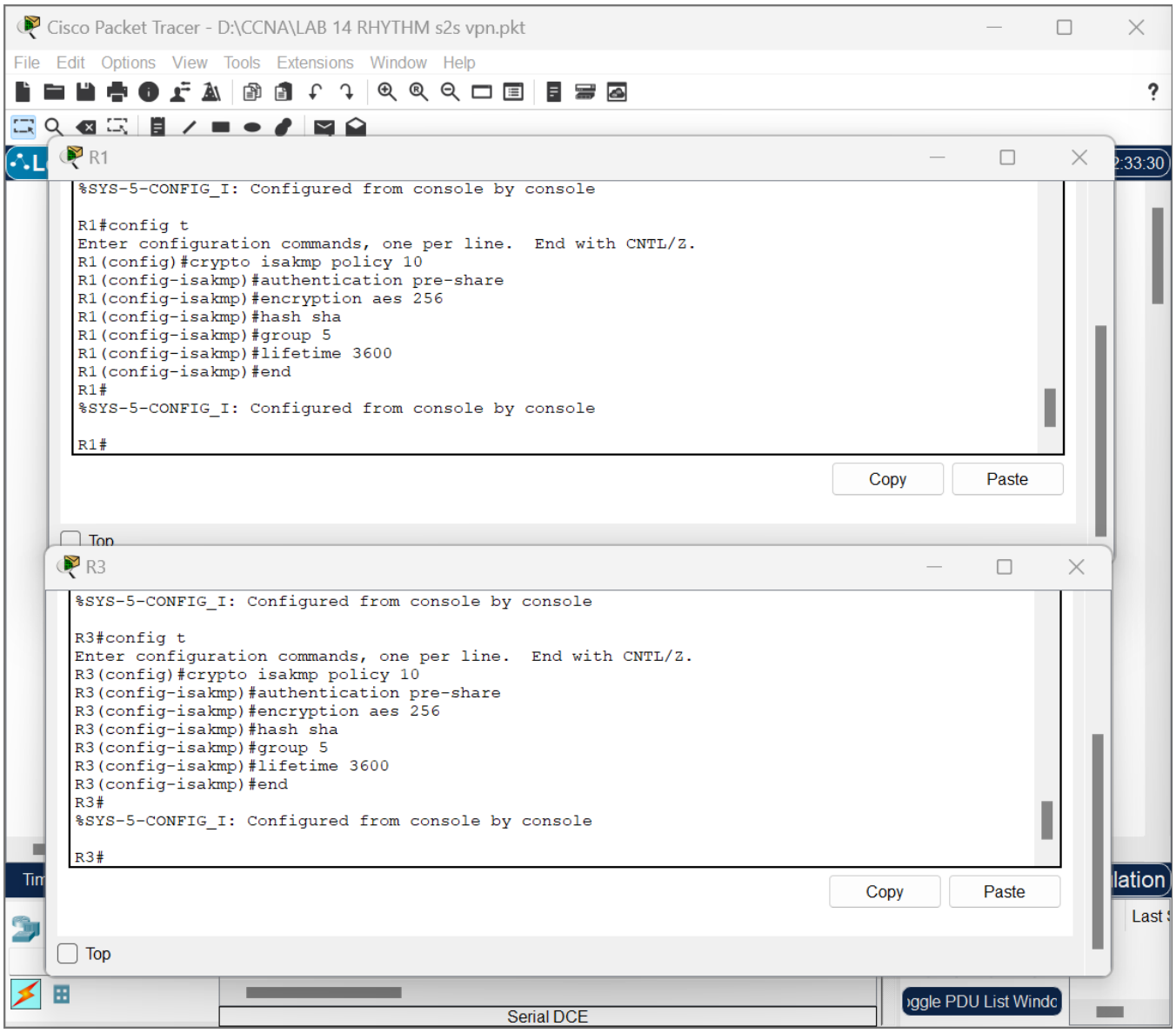
a. Configure an ISAKMP policy with a priority of **10**. Use **pre-shared key** as the authentication type,.**aes 256** for the encryption algorithm, **sha** as the hash algorithm, and Diffie-Hellman group **5** key exchange. Give the policy a lifetime of **3600** seconds (one hour).

Note: Older versions of Cisco IOS do not support AES 256 encryption and SHA as a hash algorithm. Substitute whatever encryption and hashing algorithm your router supports. Ensure the same changes are made on the other VPN endpoint to be in sync.

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# hash sha
R1(config-isakmp)# group 5
R1(config-isakmp)# lifetime 3600
R1(config-isakmp)# end
```

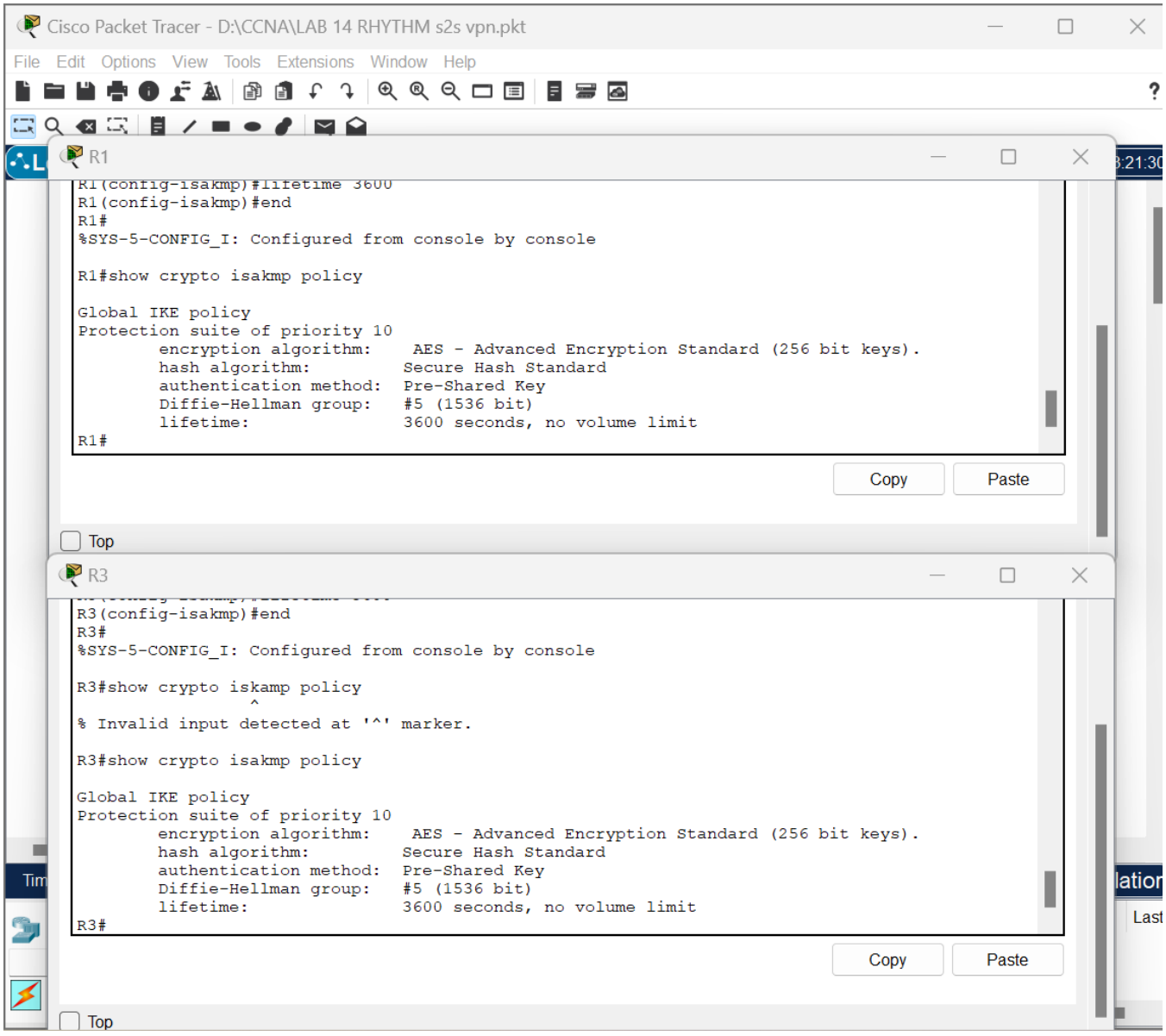
b. Configure the same policy on R3.

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# encryption aes 256
R3(config-isakmp)# hash sha
R3(config-isakmp)# group 5
R3(config-isakmp)# lifetime 3600
R3(config-isakmp)# end
```



c. Verify the IKE policy with the **show crypto isakmp policy** command.

```
R1# show crypto isakmp policy
Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption
Standard (256 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               3600 seconds, no volume limit
```


Cisco Packet Tracer - D:\CCNA\LAB 14 RHYTHM s2s vpn.pkt
File Edit Options View Tools Extensions Window Help
R1
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#show crypto isakmp policy
Global IKE policy
Protection suite of priority 10
encryption algorithm: AES - Advanced Encryption Standard (256 bit keys).
hash algorithm: Secure Hash Standard
authentication method: Pre-Shared Key
Diffie-Hellman group: #5 (1536 bit)
lifetime: 3600 seconds, no volume limit
R1#
Copy
Paste
Top
R3
R3(config-isakmp)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#show crypto iskamp policy
^
% Invalid input detected at '^' marker.
R3#show crypto isakmp policy
Global IKE policy
Protection suite of priority 10
encryption algorithm: AES - Advanced Encryption Standard (256 bit keys).
hash algorithm: Secure Hash Standard
authentication method: Pre-Shared Key
Diffie-Hellman group: #5 (1536 bit)
lifetime: 3600 seconds, no volume limit
R3#
Copy
Paste
Top

Step 4: Configure pre-shared keys.

Because pre-shared keys are used as the authentication method in the IKE policy, a key must be configured on each router that points to the other VPN endpoint. These keys must match for authentication to be successful. The global configuration mode **crypto isakmp key key-string address address** command is used to enter a pre-shared key. Use the IP address of the remote peer, the remote interface that the peer would use to route traffic to the local router.

Question:

Which IP addresses should you use to configure the IKE peers given the topology diagram and IP addressing table?

Answer:

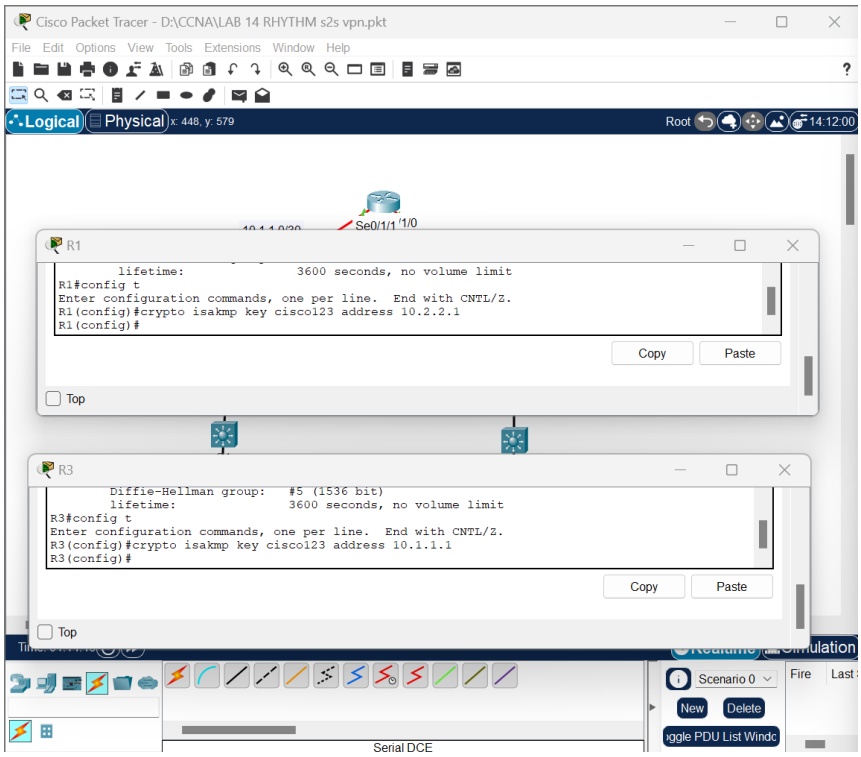
The IP addresses should be R1 S0/1/0 IP address 10.1.1.1 and R3 S0/1/1 IP address 10.2.2.1. These are the addresses that are used to send normal traffic between R1 and R3.

a. Each IP address that is used to configure the IKE peers is also referred to as the IP address of the remote VPN endpoint. Configure the pre-shared key of **cisco123** on router R1. Production networks should use a complex key. This command points to the remote peer R3 S0/1/1 IP address.

```
R1(config)# crypto isakmp key cisco123 address 10.2.2.1
```

b. Configure the pre-shared key of **cisco123** on router R3. The command for R3 points to the R1 S0/1/0 IP address.

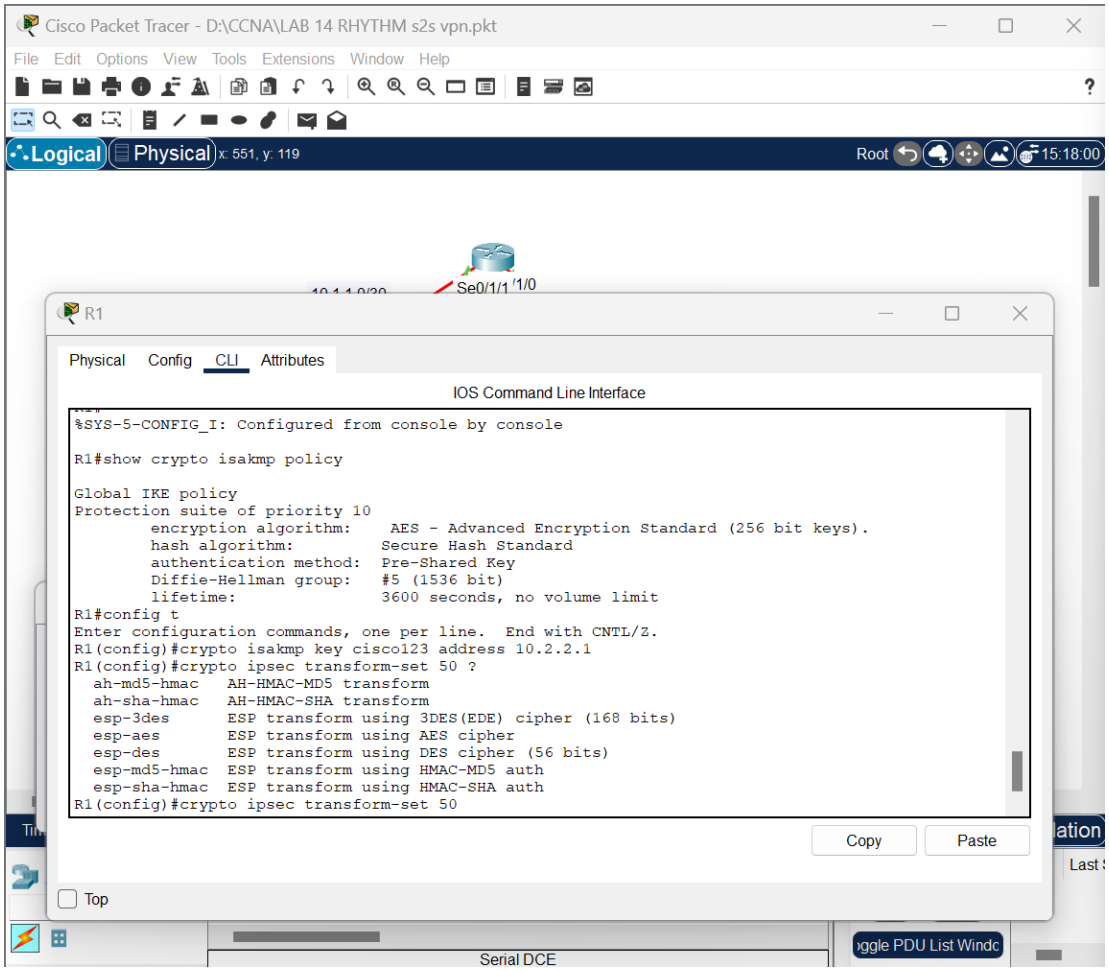
```
R3(config)# crypto isakmp key cisco123 address 10.1.1.1
```



Step 5: Configure the IPsec transform set and lifetimes.

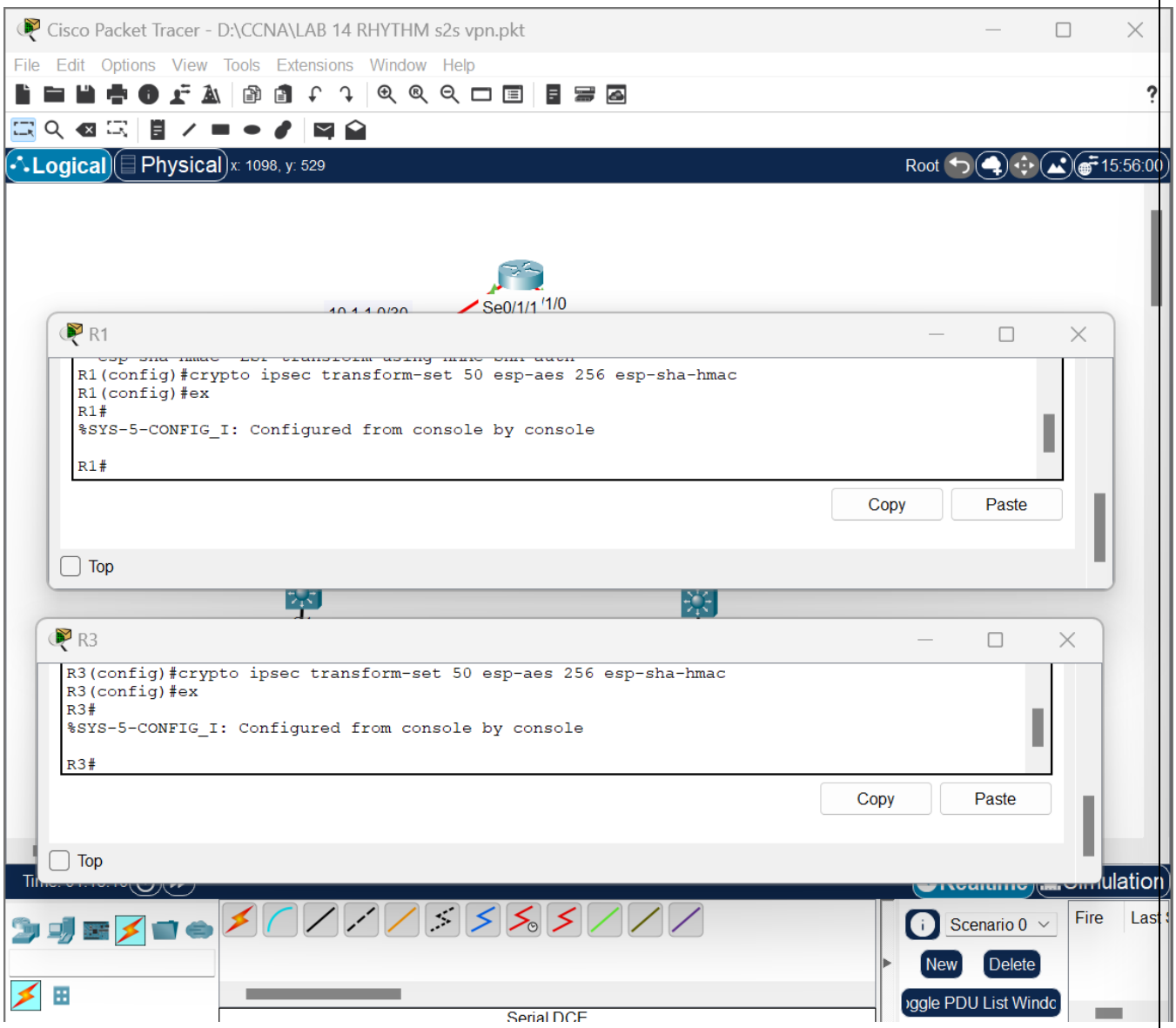
a. The IPsec transform set is another crypto configuration parameter that routers negotiate to form a security association. To create an IPsec transform set, use the **crypto ipsec transform-set tag** command. Use **?** to see which parameters are available.

```
R1(config)# crypto ipsec transform-set 50 ?
  ah-md5-hmac   AH-HMAC-MD5 transform
  ah-sha-hmac   AH-HMAC-SHA transform
  comp-lzs      IP Compression using the LZS compression
algorithm
  esp-3des      ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes       ESP transform using AES cipher
  esp-des       ESP transform using DES cipher (56 bits)
  esp-md5-hmac  ESP transform using HMAC-MD5 auth
  esp-null      ESP transform w/o cipher
  esp-seal      ESP transform using SEAL cipher (160 bits)
  esp-sha-hmac  ESP transform using HMAC-SHA auth
```



b. On R1 and R3, create a transform set with tag **50** and use an Encapsulating Security Protocol (ESP) transform with an AES 256 cipher with ESP and the SHA hash function. The transform sets must match.

```
R1(config)# crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
R1(cfg-crypto-trans)# exit

R3(config)# crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
R3(cfg-crypto-trans)# exit
```



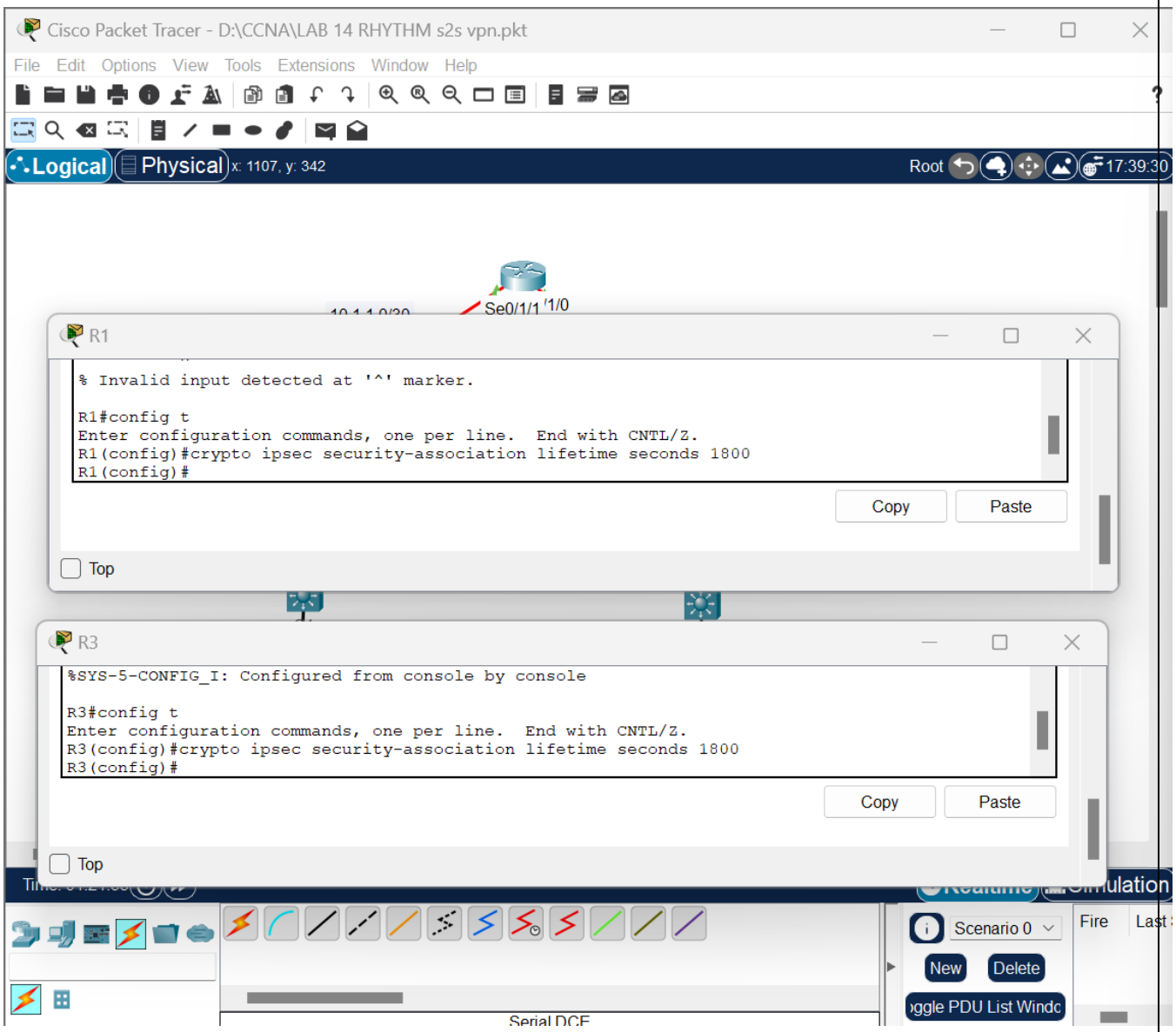
What is the function of the IPsec transform set?

IPsec transform set have a important role in establishing secure communication channels between IPsec peers by defining the security parameters used for authentication, encryption, and key exchange.

c. You can also change the IPsec security association lifetimes from the default of 3600 seconds. On R1 and R3, set the IPsec security association lifetime to 30 minutes, or **1800** seconds.

```
R1(config)# crypto ipsec security-association lifetime seconds
1800
```

```
R3(config)# crypto ipsec security-association lifetime seconds
1800
```



Step 6: Define interesting traffic.

To make use of the IPsec encryption with the VPN, it is necessary to define extended access lists to tell the router which traffic to encrypt. A packet that is permitted by an access list used for defining IPsec traffic is encrypted if the IPsec session is configured correctly. A packet that is denied by one of these access lists is not dropped but sent unencrypted. Also, like any other access list, there is an implicit deny at the end, which, in this case, means that the default action is not to encrypt traffic. If there is no IPsec security association correctly configured, no traffic is encrypted and traffic is forwarded as unencrypted.

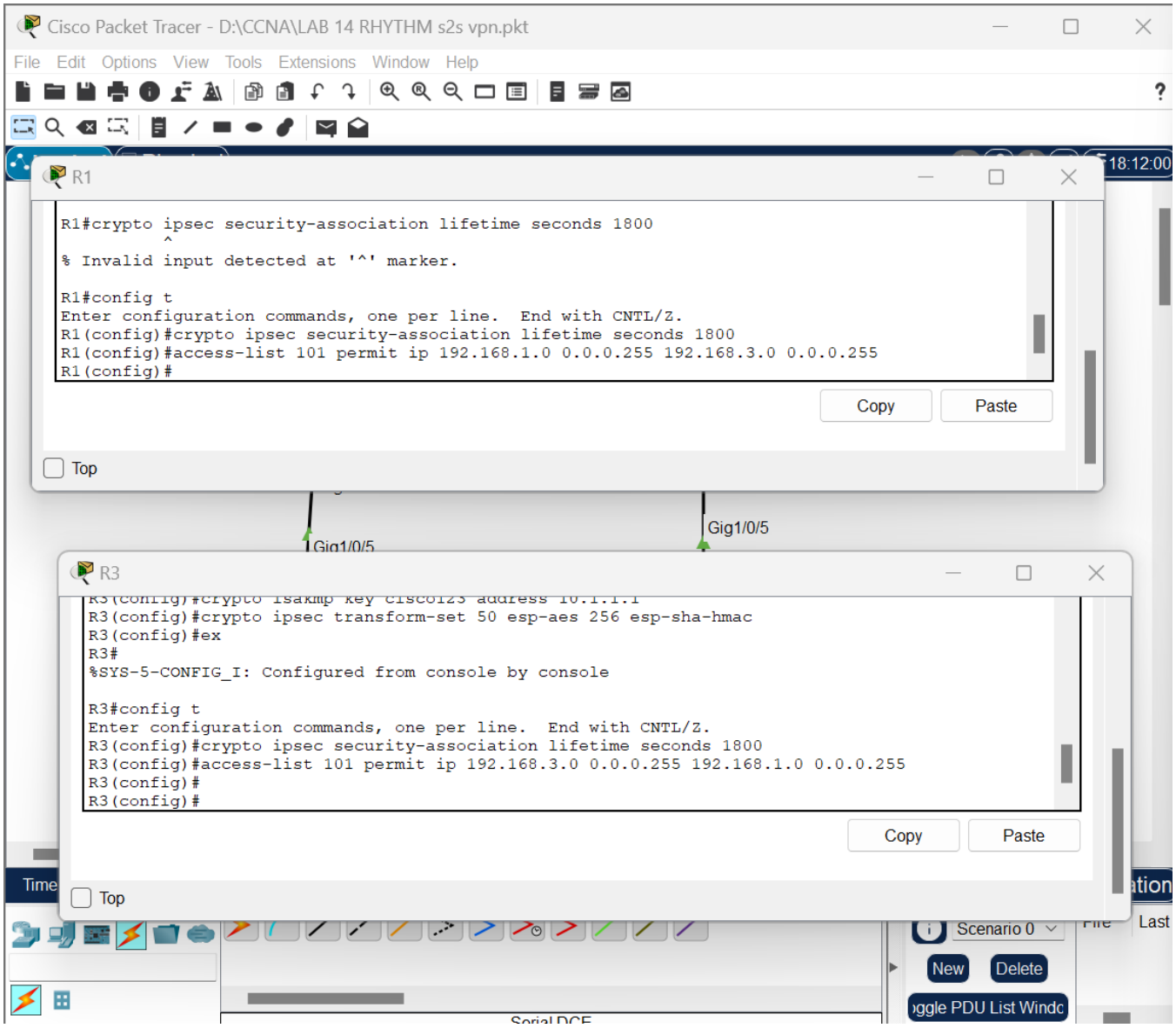
In this scenario, the traffic you want to encrypt is traffic going from R1's Ethernet LAN to R3's Ethernet LAN, or vice versa. These access lists are used outbound on the VPN endpoint interfaces and must mirror each other.

a. Configure the IPsec VPN interesting traffic ACL on R1.

```
R1(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255
192.168.3.0 0.0.0.255
```

b. Configure the IPsec VPN interesting traffic ACL on R3.

```
R3(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255
```



Does IPsec evaluate whether the access lists are mirrored as a requirement to negotiate its security association?

Yes, for a site-to-site VPN configuration to function properly, it is a best practice to ensure that the access lists defining interesting traffic are mirrored on both ends of the VPN tunnel.

Step 7: Create and apply a crypto map.

A crypto map associates traffic that matches an access list to a peer, various IKE, and IPsec settings. After the crypto map is created, it can be applied to one or more interfaces. The interfaces it is applied to should be the ones facing the IPsec peer.

To create a crypto map, use **crypto map name sequence-num type** command in global configuration mode to enter crypto map configuration mode for that sequence number. Multiple crypto map statements can belong to the same crypto map and are evaluated in

ascending numerical order. Enter crypto map configuration mode on R1. Use a type of ipsec-isakmp, which means IKE is used to establish IPsec security associations.

a. Create the crypto map on R1, name it **CMAP**, and use **10** as the sequence number. A message displays after the command is issued.

```
R1(config)# crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
```

b. Use the **match address access-list** command to specify which access list defines which traffic to encrypt.

```
R1(config-crypto-map)# match address 101
```

c. To view the list of possible **set** commands you can do in a crypto map, use the help function.

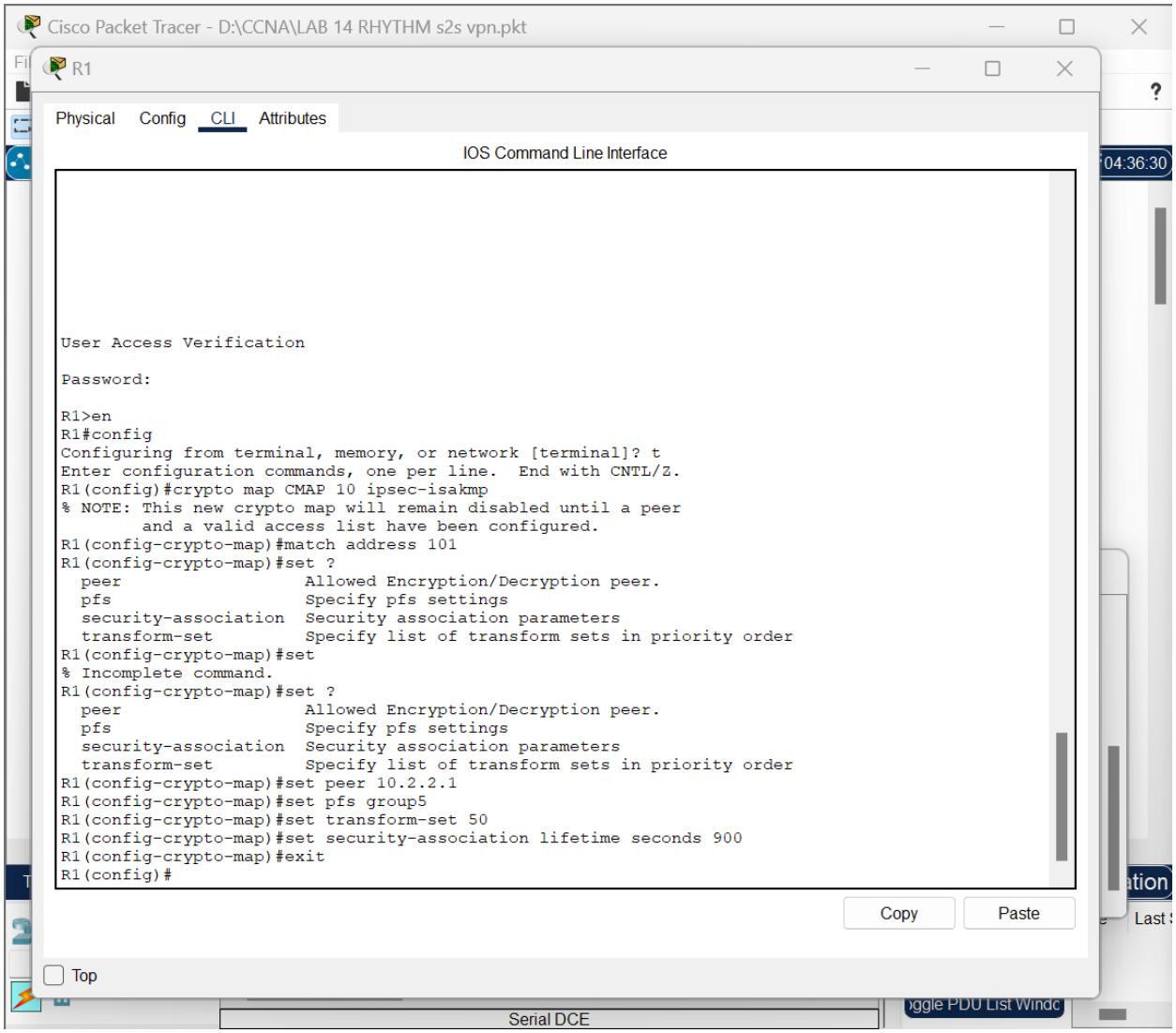
```
R1(config-crypto-map)# set ?
  identity              Identity restriction.
  ip                    Interface Internet Protocol config
commands
  isakmp-profile        Specify isakmp Profile
  nat                   Set NAT translation
  peer                  Allowed Encryption/Decryption peer.
  pfs                   Specify pfs settings
  reverse-route         Reverse Route Injection.
  security-association  Security association parameters
  transform-set         Specify list of transform sets in
priority order
```

d. Setting a peer IP or hostname is required. Set it to R3's remote VPN endpoint interface using the following command.

```
R1(config-crypto-map)# set peer 10.2.2.1
```

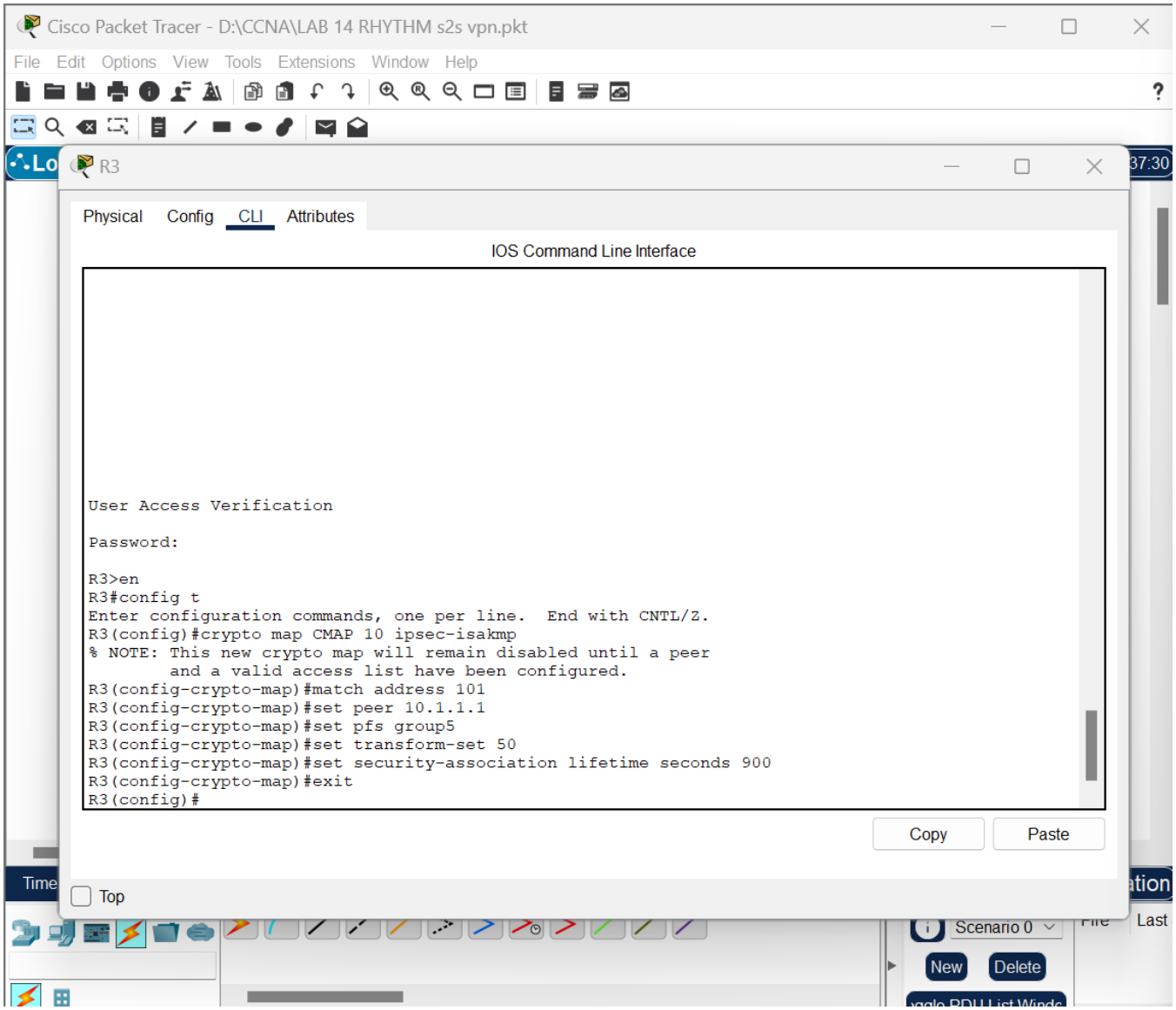
e. Hard code the transform set to be used with this peer, using the **set transform-set tag** command. Set the perfect forwarding secrecy type using the **set pfs type** command, and also modify the default IPsec security association lifetime with the **set security-association lifetime seconds seconds** command.

```
R1(config-crypto-map)# set pfs group5
R1(config-crypto-map)# set transform-set 50
R1(config-crypto-map)# set security-association lifetime seconds
900
R1(config-crypto-map)# exit
```



f. Create a mirrored matching crypto map on R3.

```
R3(config)# crypto map CMAP 10 ipsec-isakmp
R3(config-crypto-map)# match address 101
R3(config-crypto-map)# set peer 10.1.1.1
R3(config-crypto-map)# set pfs group5
R3(config-crypto-map)# set transform-set 50
R3(config-crypto-map)# set security-association lifetime seconds
900
R3(config-crypto-map)# exit
```

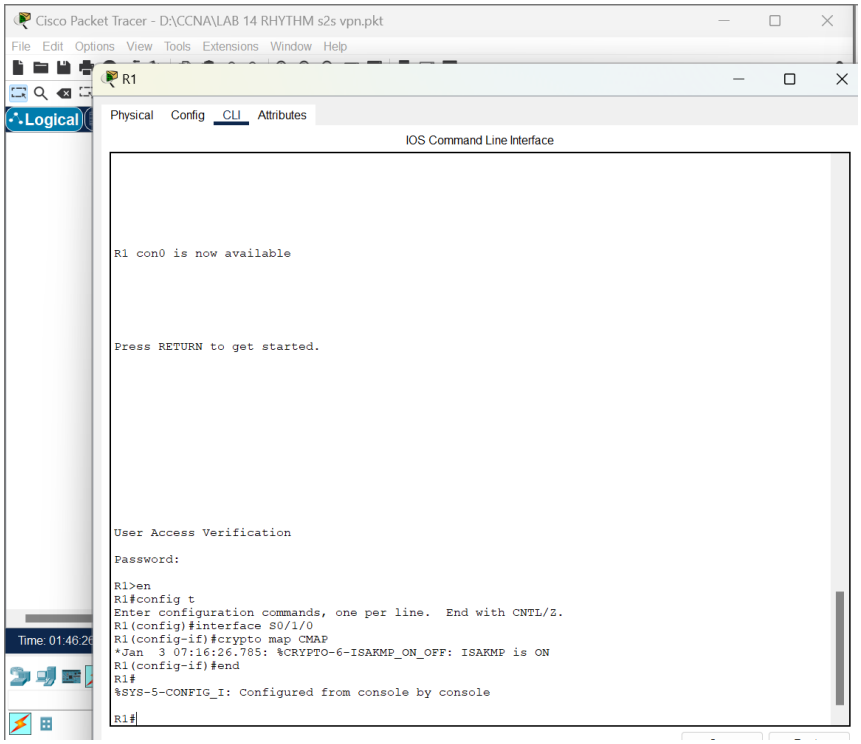


g. The last step is to apply the crypto map to the interfaces.

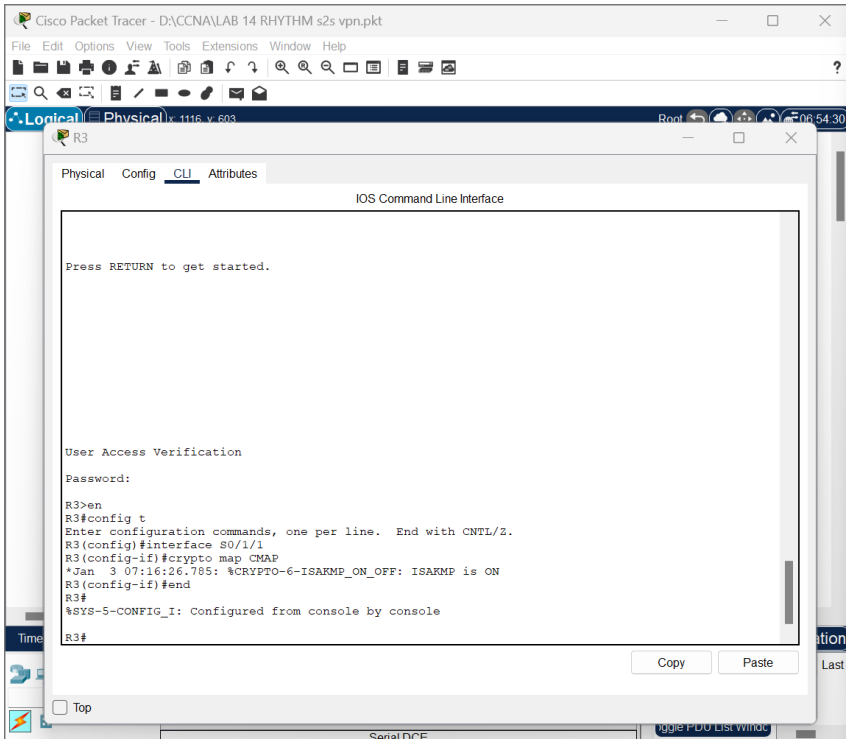
Note: The security associations (SAs) are not established until the crypto map has been activated by interesting traffic. The router generates a notification that the crypto is now on.

Apply the crypto maps to the appropriate interfaces on R1 and R3.

```
R1(config)# interface S0/1/0
R1(config-if)# crypto map CMAP
*Jan 28 04:09:09.150: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config)# end
```




```
R3
R3(config)# interface S0/1/1
R3(config-if)# crypto map CMAP
*Jan 28 04:10:54.138: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config)# end
```

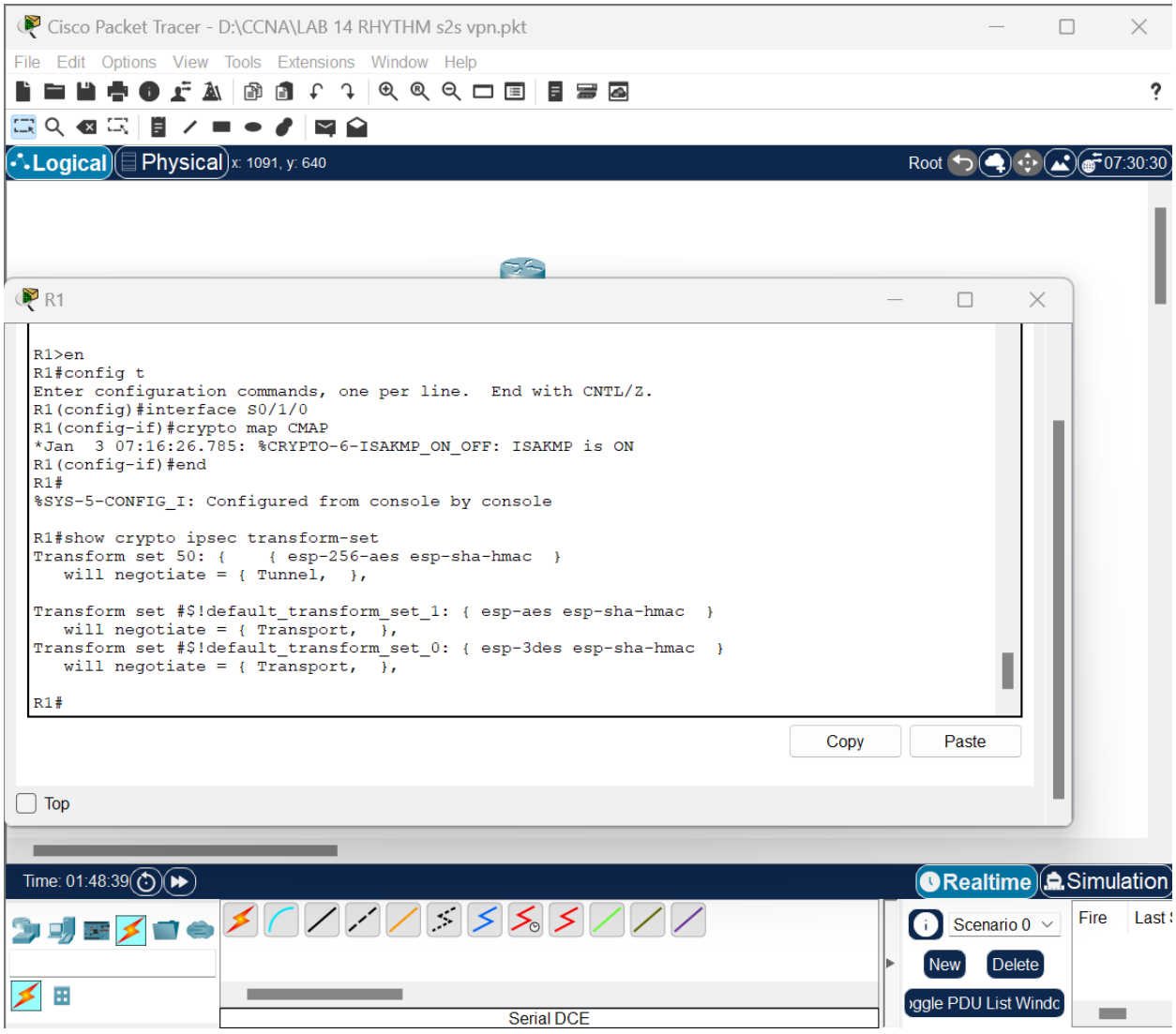


Task 3: Verify the site-to-site IPsec VPN configuration.

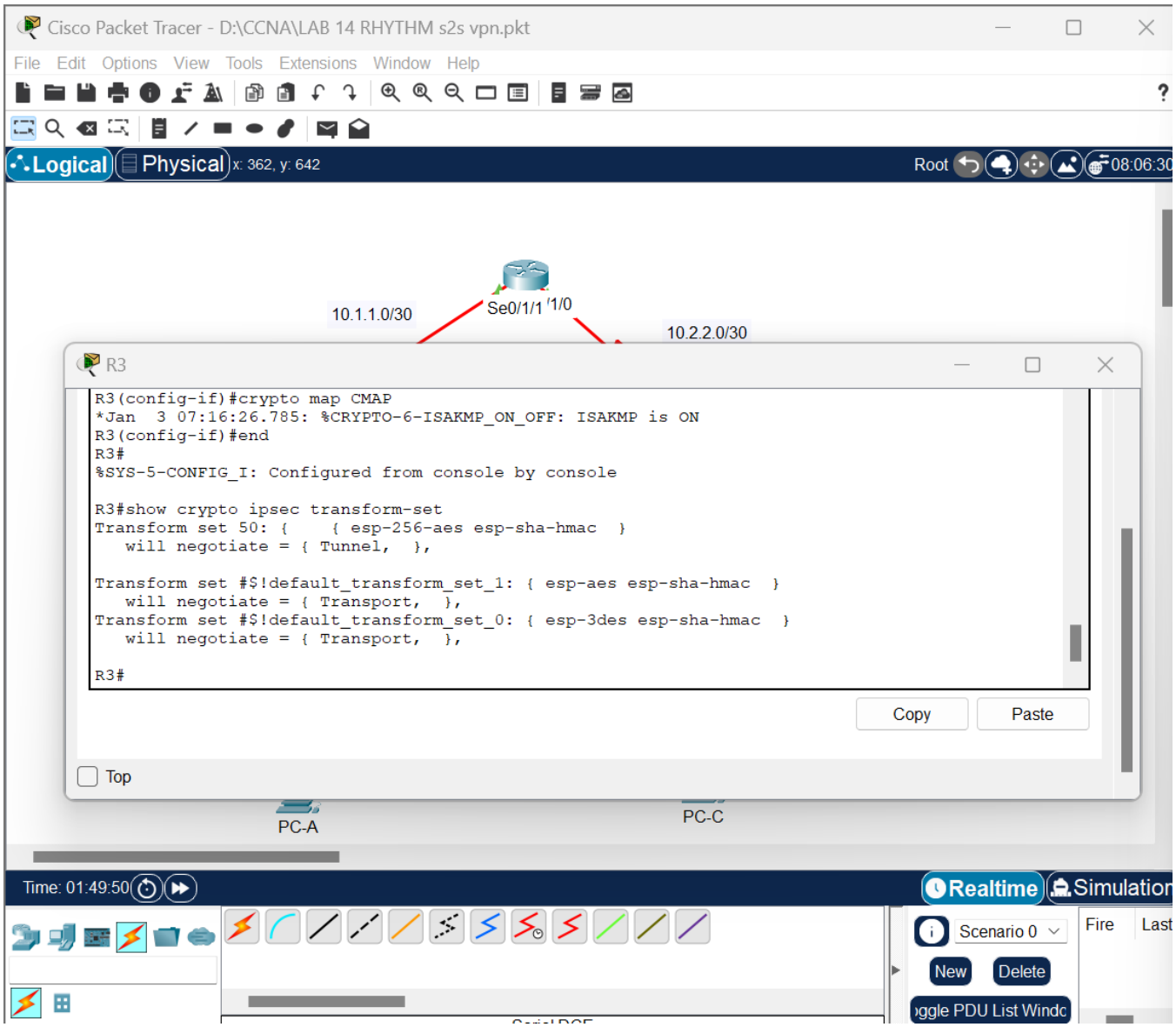
Step 1: Verify the IPsec configuration on R1 and R3.

a. Previously, you used the **show crypto isakmp policy** command to display the configured ISAKMP policies on the router. Similarly, the **show crypto ipsec transform-set** command displays the configured IPsec policies in the form of the transform sets.

```
R1# show crypto ipsec transform-set
Transform set 50: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

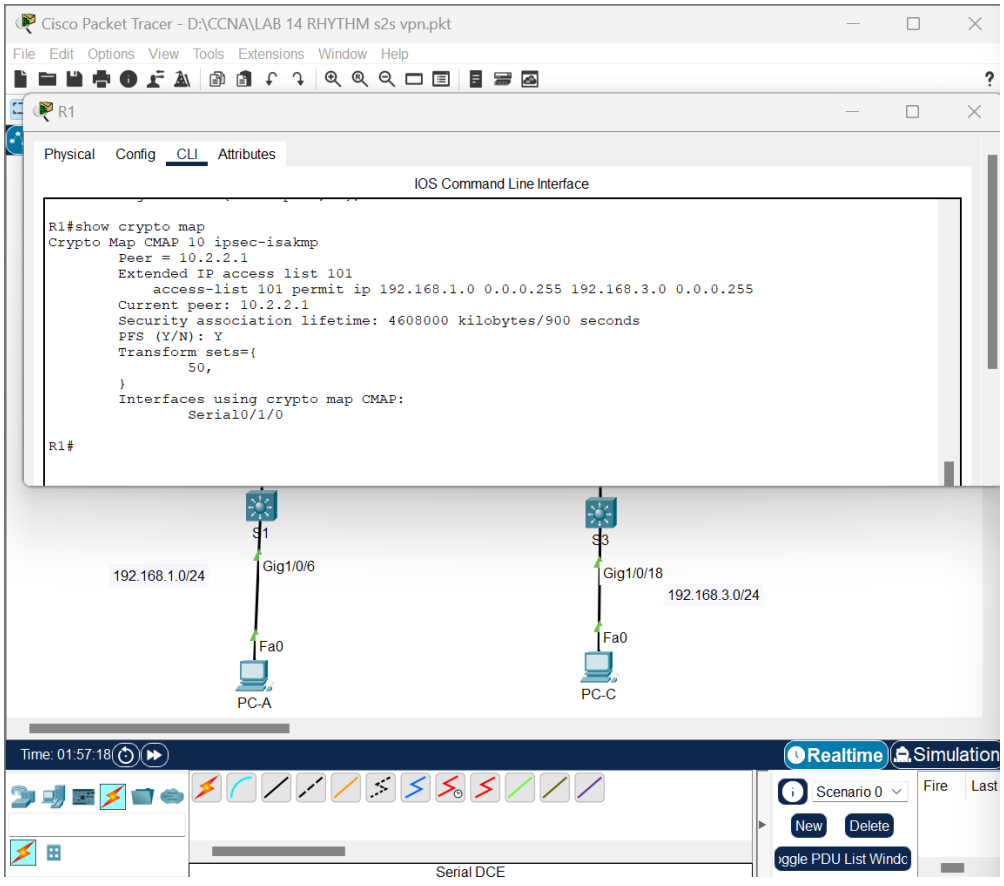


```
R3# show crypto ipsec transform-set
Transform set 50: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

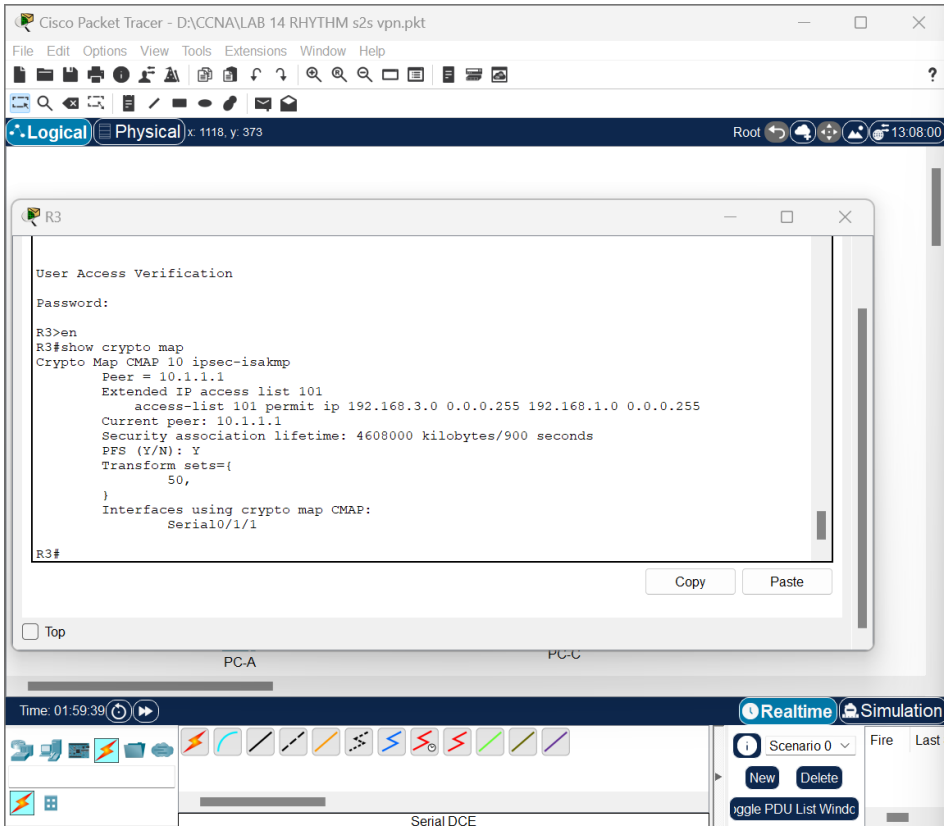


b. Use the **show crypto map** command to display the crypto maps that will be applied to the router.

```
R1# show crypto map
Crypto Map "CMAP" 10 ipsec-isakmp
        Peer = 10.2.2.1
        Extended IP access list 101
            access-list 101 permit ip 192.168.1.0 0.0.0.255
192.168.3.0 0.0.0.255
        Current peer: 10.2.2.1
        Security association lifetime: 4608000 kilobytes/900
seconds
        Responder-Only (Y/N): N
        PFS (Y/N): Y
        DH group:  group5
        Transform sets={
                50:  { esp-256-aes esp-sha-hmac  } ,
        }
        Interfaces using crypto map CMAP:
                Serial0/1/0
```



```
R3# show crypto map
Crypto Map "CMAP" 10 ipsec-isakmp
        Peer = 10.1.1.1
        Extended IP access list 101
            access-list 101 permit ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255
        Current peer: 10.1.1.1
        Security association lifetime: 4608000 kilobytes/900
seconds
        Responder-Only (Y/N): N
        PFS (Y/N): Y
        DH group:  group5
        Transform sets={
                50:  { esp-256-aes esp-sha-hmac  } ,
        }
        Interfaces using crypto map CMAP:
                Serial0/1/1
```



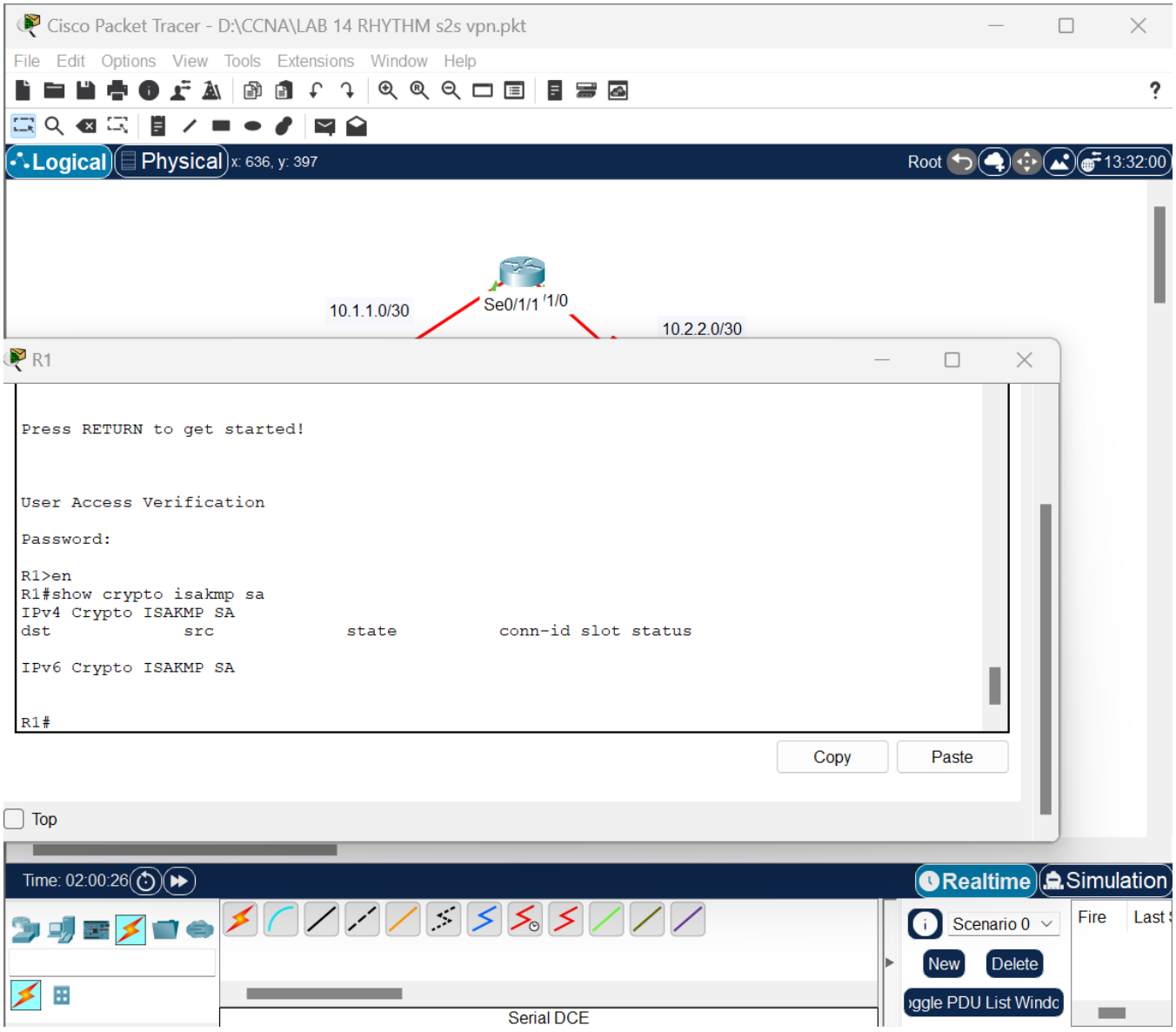
Note: The output of these **show** commands does not change if interesting traffic goes across the connection. You will test various types of traffic in the next task.

Task 4: Verify the IPsec VPN operation.

Step 1: Display isakmp security associations.

The **show crypto isakmp sa** command reveals that no IKE SAs exist yet. When interesting traffic is sent, this command output changes.

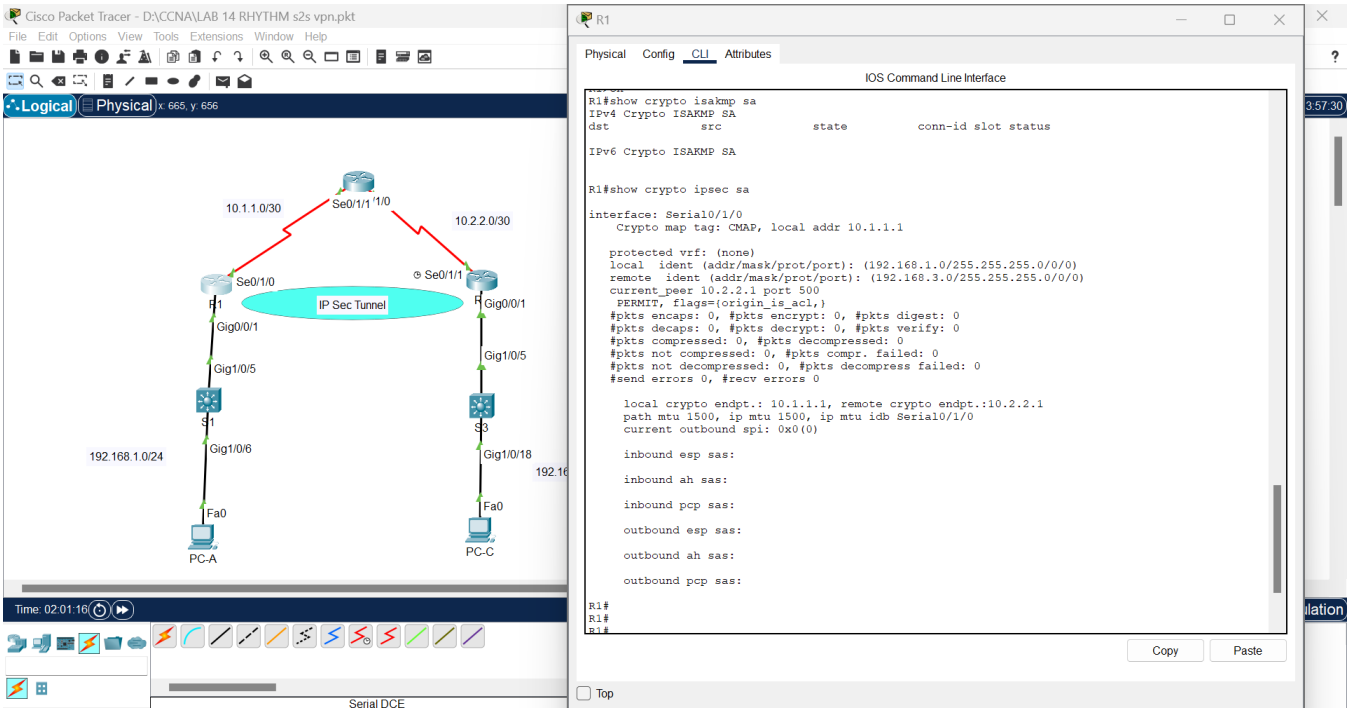
```
R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status

IPv6 Crypto ISAKMP SA
```



Step 2: Display IPsec security associations.

The **show crypto ipsec sa** command shows the unused SA between R1 and R3.

Note: The number of packets sent across and the lack of any security associations are listed toward the bottom of the output. The output for R1 is shown here.




```
R1# show crypto ipsec sa
interface: Serial0/1/0
    Crypto map tag: CMAP, local addr 10.1.1.1
   protected vrf: (none)
   local  ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.1.1.1, remote crypto endpt.:
10.2.2.1
```

```
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x0(0)
PFS (Y/N): N, DH group: none

inbound esp sas:

inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:
```

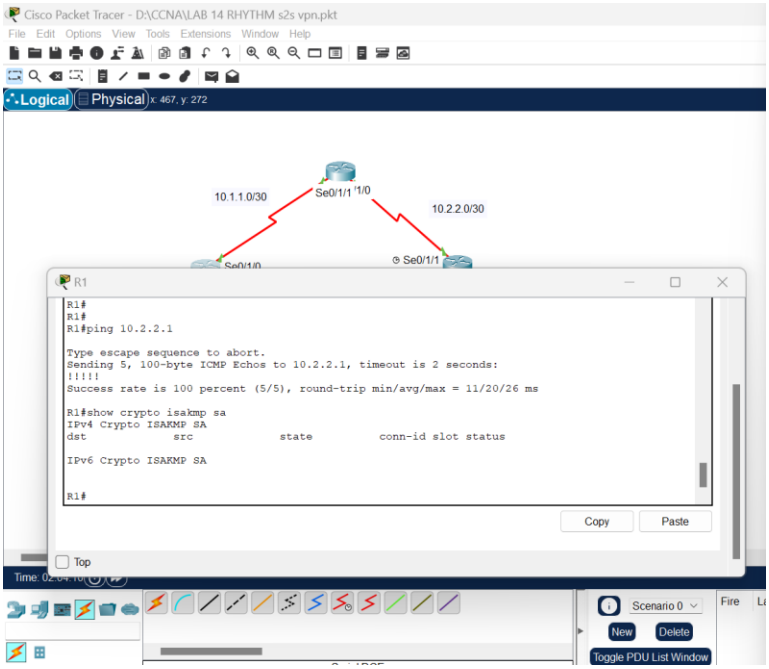
Why have no SAs been negotiated?

Ans Misconfiguration, Problems with authentication mechanisms or key exchange protocols, Routing Issue

Step 3: Generate some uninteresting test traffic and observe the results.

a. Ping from R1 to the R3 S0/1/1 interface IP address **10.2.2.1**. These pings should be successful.

b. Issue the **show crypto isakmp sa** command.

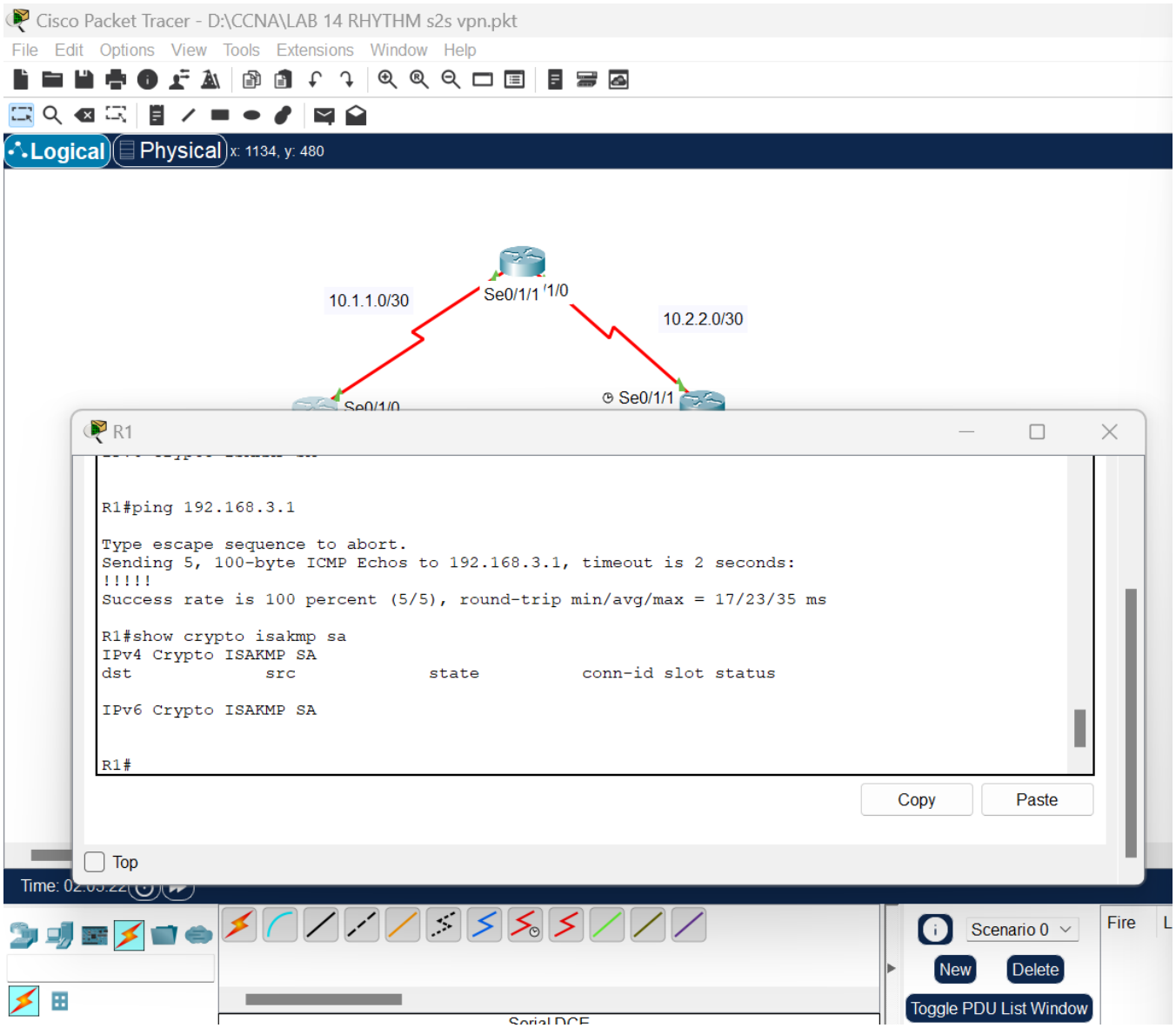


c. Ping from R1 to the R3 G0/0/1 interface IP address **192.168.3.1**. These pings should be successful.

d. Issue the **show crypto isakmp sa** command again. Was an SA created for these pings? Explain.

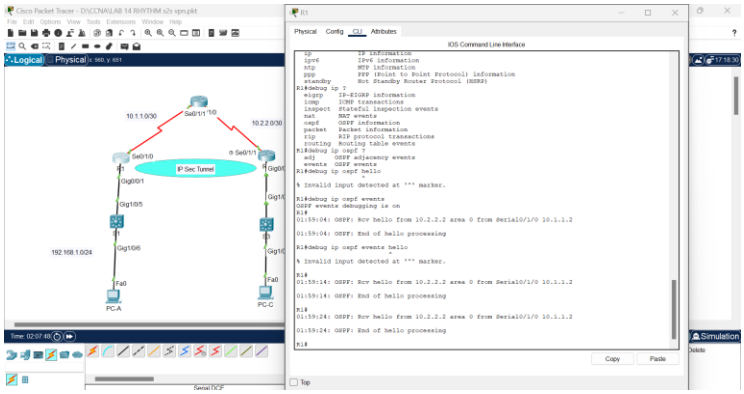
Answer:

SA was not created. The source address of both pings was the R1 S0/1/0 address of 10.1.1.1. In the first case, the destination address was 10.2.2.1. In the second case, the destination address was 192.168.3.1. This is not “interesting” traffic. The ACL 101 that is associated with the crypto map for R1 defines interesting traffic as IP packets from the 192.168.1.0/24 network to the 192.168.3.0/24 network.

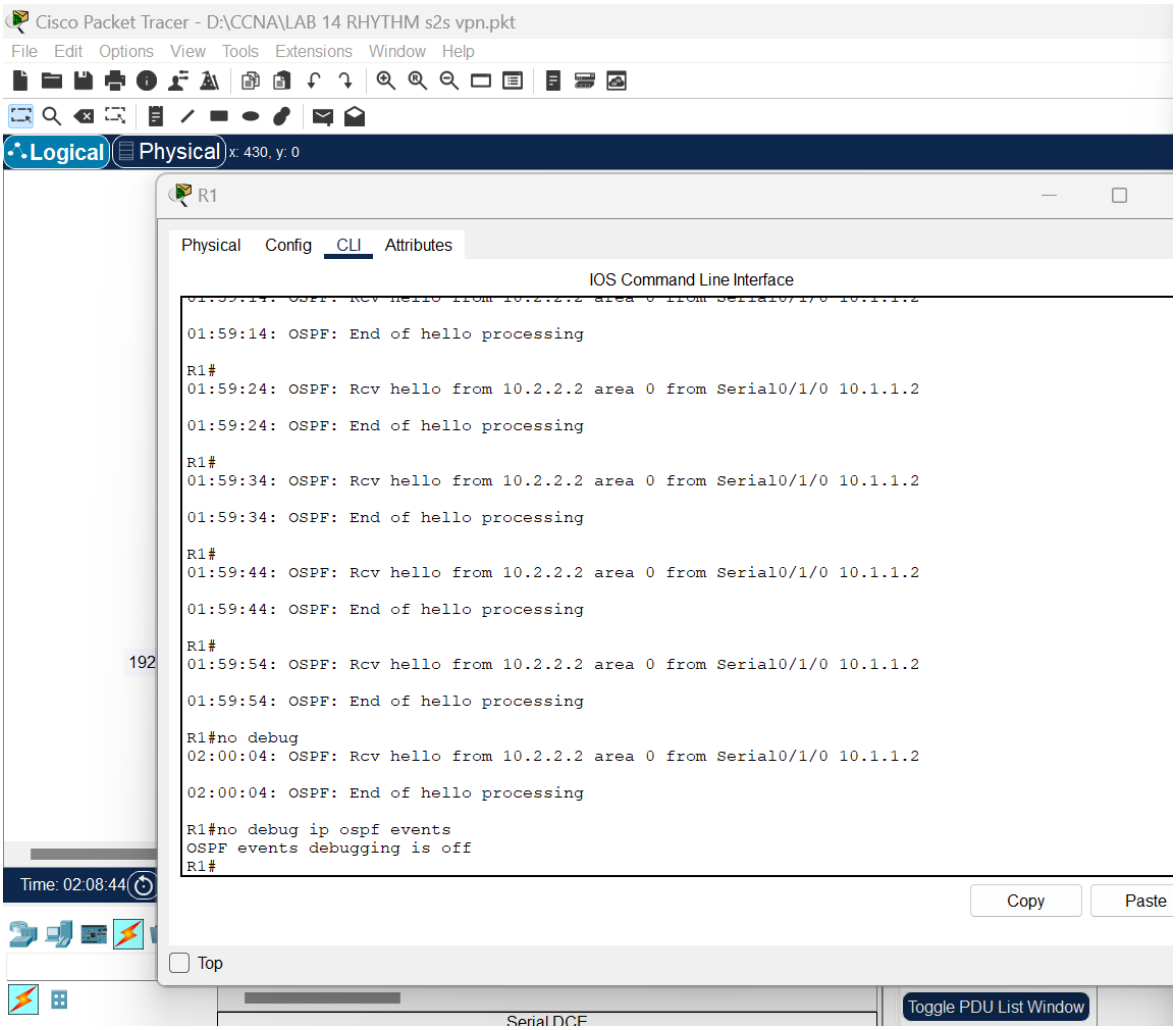


e. Issue the **debug ip ospf hello** command. You should see OSPF hello packets passing between R1 and R3.

```
R1# debug ip ospf hello
OSPF hello events debugging is on
```



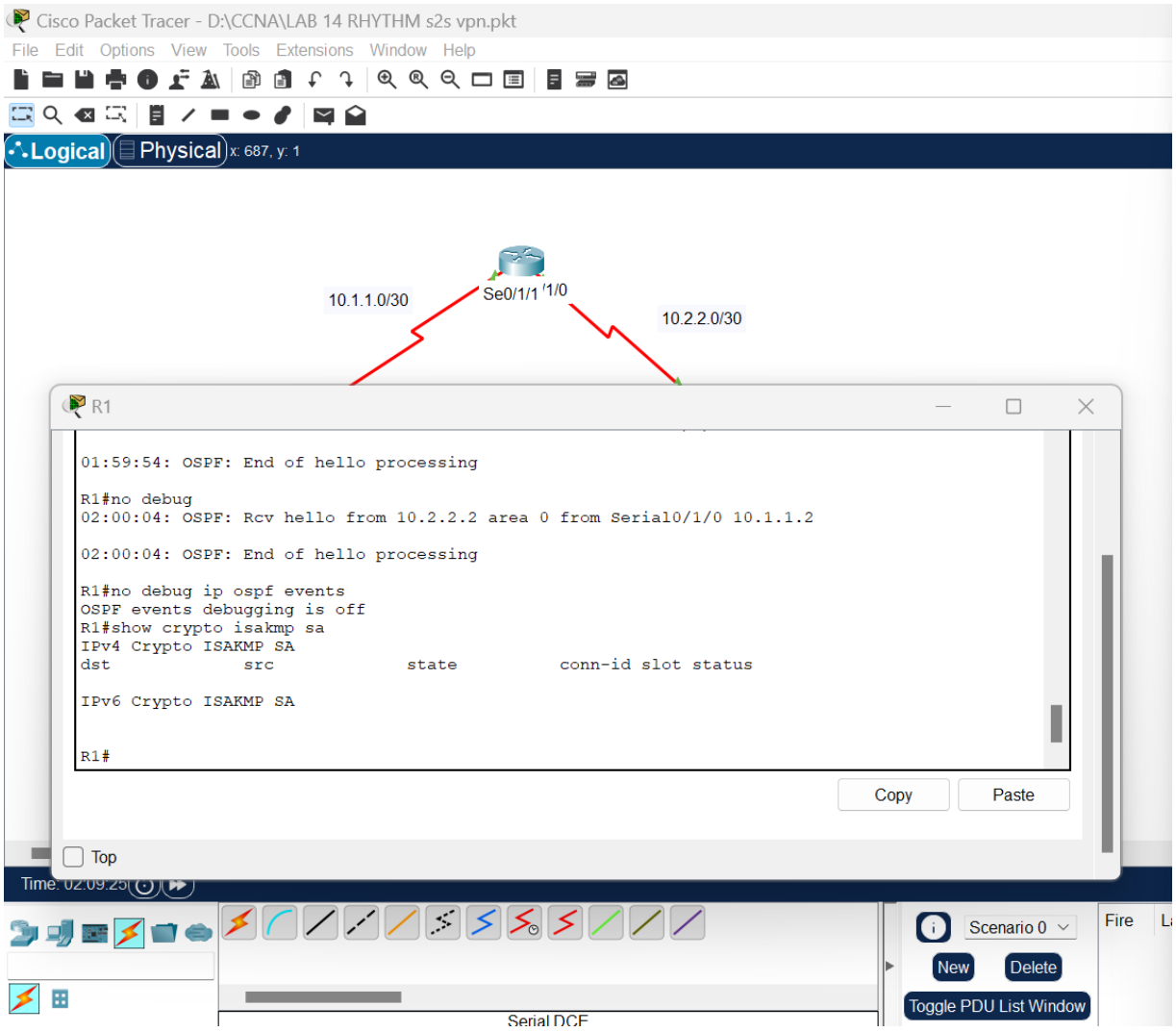
f. Turn off debugging with the **no debug ip ospf hello** or **undebug all** command.



g. Re-issue the **show crypto isakmp sa** command. Was an SA created between R1 and R3? Explain.

Answer:

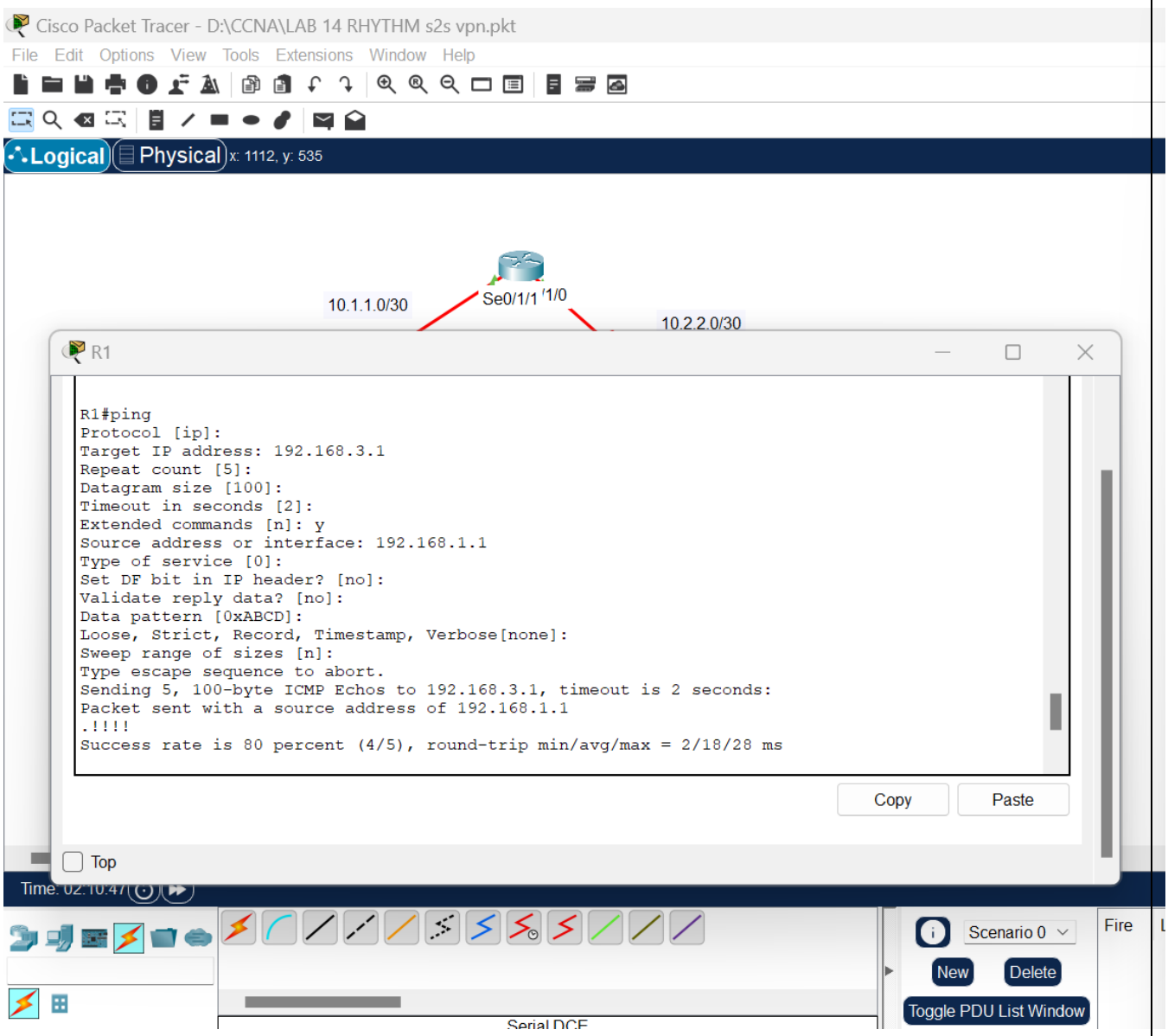
No. This is router-to-router routing protocol traffic. The source and destination of these packets is not interesting, does not initiate the SA, and is not encrypted.



Step 4: Generate some interesting test traffic and observe the results.

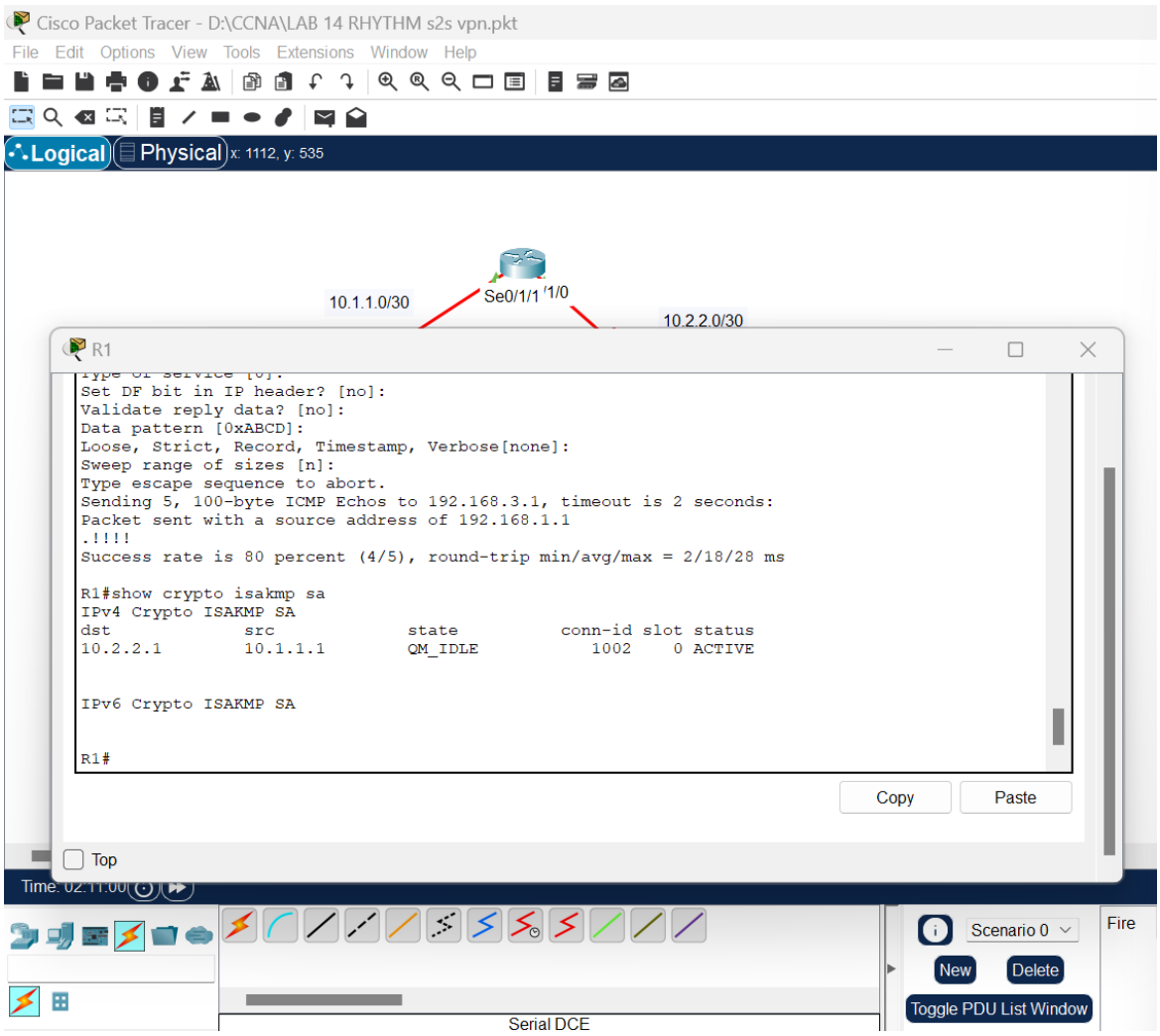
a. Use an extended ping from R1 to the R3 G0/0/1 interface IP address **192.168.3.1**. Extended ping allows you to control the source address of the packets. Respond as shown in the following example. Press **Enter** to accept the defaults, except where a specific response is indicated.

```
R1# ping
Protocol [ip]:
Target IP address: 192.168.3.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2
seconds:

Packet sent with a source address of 192.168.1.1
..!!!
Success rate is 100 percent (3/5), round-trip min/avg/max =
92/92/92 ms
```



b. Re-issue the **show crypto isakmp sa** command.

```
R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.2.2.1        10.1.1.1        QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA
```



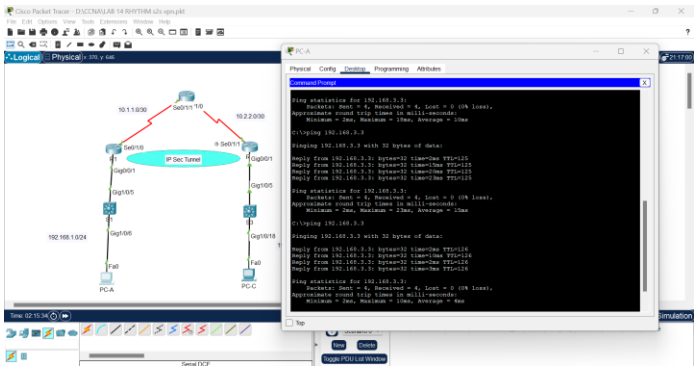
Why was an SA created between R1 and R3 this time?

Answer: Resolve the issue and observe some interesting traffic and observe the result

What are the endpoints of the IPsec VPN tunnel?

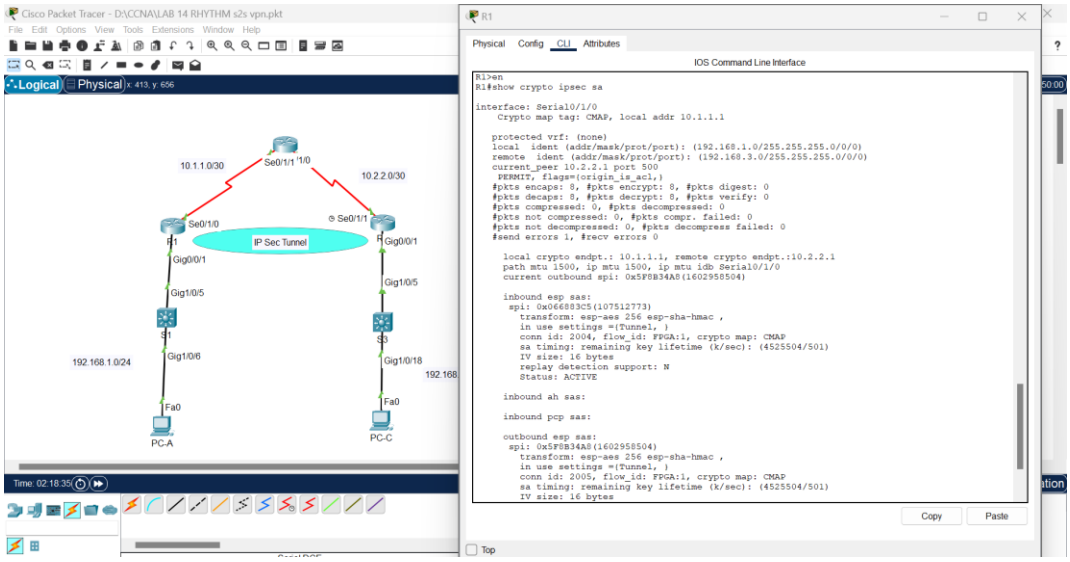
Answer: R1 and R3

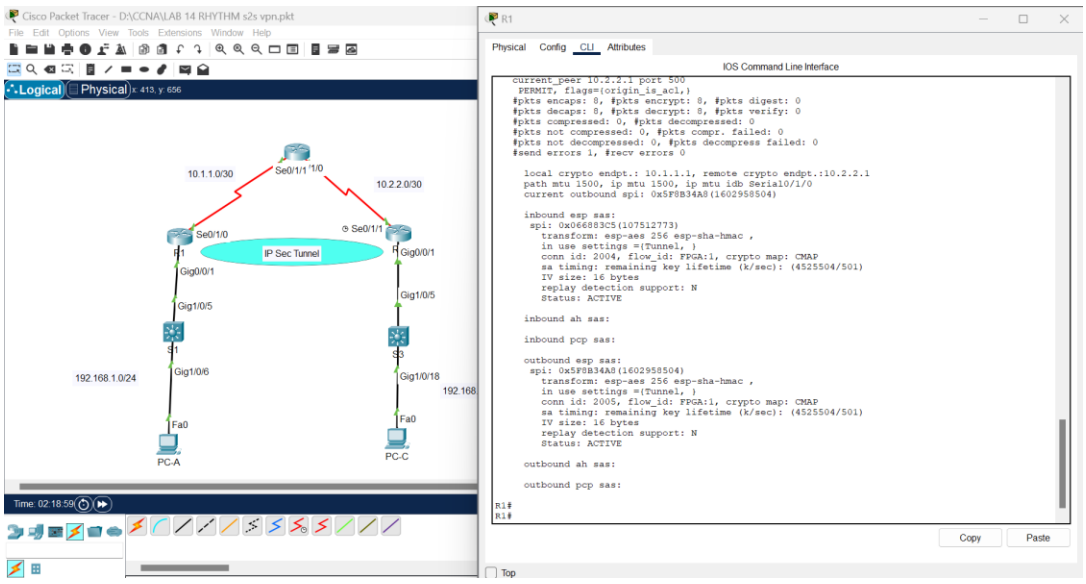
c. Ping from PC-A to PC-C. If the pings were successful, issue the **show crypto ipsec sa** command. How many packets have been transformed between R1 and R3?



```
R1# show crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: CMAP, local addr 10.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7
    #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 7
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 2, #recv errors 0

     local crypto endpt.: 10.1.1.1, remote crypto endpt.:
10.2.2.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0xC1DD058(203280472)

     inbound esp sas:
      spi: 0xDF57120F(3747025423)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2005, flow_id: FPGA:5, crypto map: CMAP
        sa timing: remaining key lifetime (k/sec): (4485195/877)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
```

```
    spi: 0xC1DD058(203280472)
      transform: esp-256-aes esp-sha-hmac ,
      in use settings ={Tunnel, }
      conn id: 2006, flow_id: FPGA:6, crypto map: CMAP
      sa timing: remaining key lifetime (k/sec): (4485195/877)
      IV size: 16 bytes
      replay detection support: Y
      Status: ACTIVE

  outbound ah sas:

  outbound pcp sas:
```





d. The previous example used pings to generate interesting traffic. What other types of traffic would result in an SA forming and tunnel establishment?

Answer: UDP Traffic : UDP based application -like DNS and voIP, TCP Traffics: this used for particular HTTP website, SSH or RDP, Application specific which allow hosts to use specific database.