Course: Cloud and Network Security-C1-2026
Cyber Shujaa Program

Week 5: Securing Network Layers 4, 5, 6 &7

Assignment 2: Configuring Site-to-Site VPNs

Student Name: Salim Katana Karuku

Student ID: CS-CNS11-26048

Contents

Introduction

This lab involves the configuration of Site-to-Site IPsec VPN between routers R1 and R3. Utilizing the provided addressing table and topology, the goal is to define interesting traffic, configure crypto maps, and establish a secure IPsec tunnel. This ensures that communicatrion between PC-A and PC-C is encrypted providing a secure path over the non-secure serial links connecting the 10.1.1.0 and 10.2.2.0

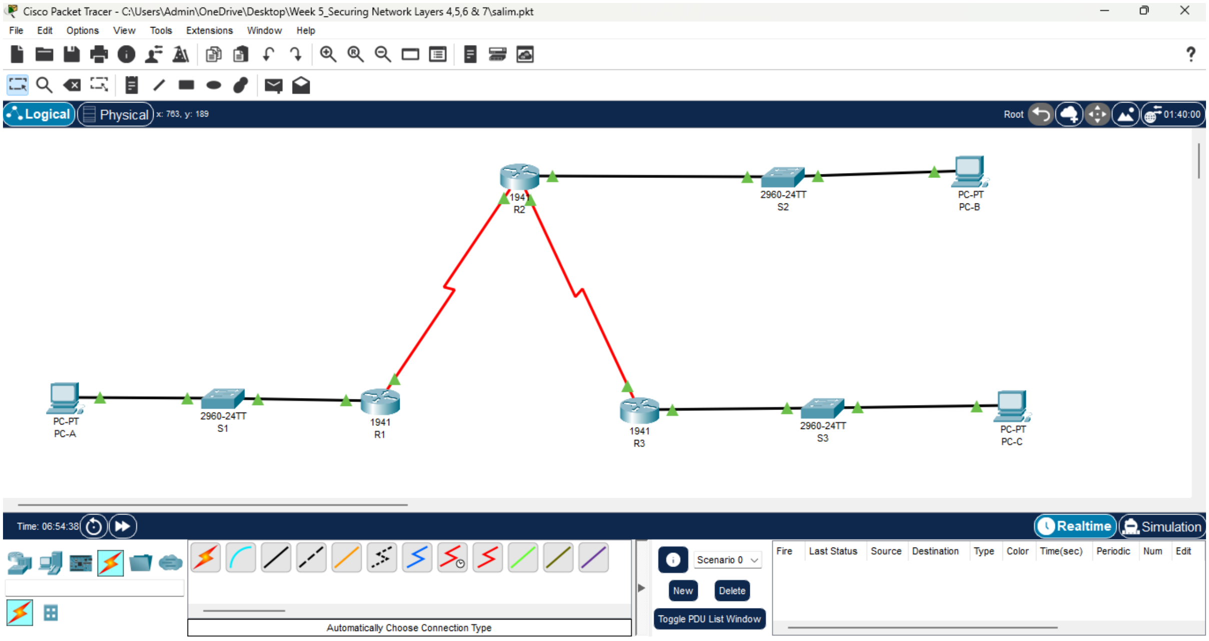
Objectives

The objectives of the assignment were:

1. To configure Site-to-Site IPsec VPN
2. To define interesting tarffic
3. To implement IKE Phase 1 (ISAKMP)
4. To implement IKE phase 2 (IPsec)
5. To apply Crypto Maps

Packet Tracer – Configuring VPNs (Optional)

Topology

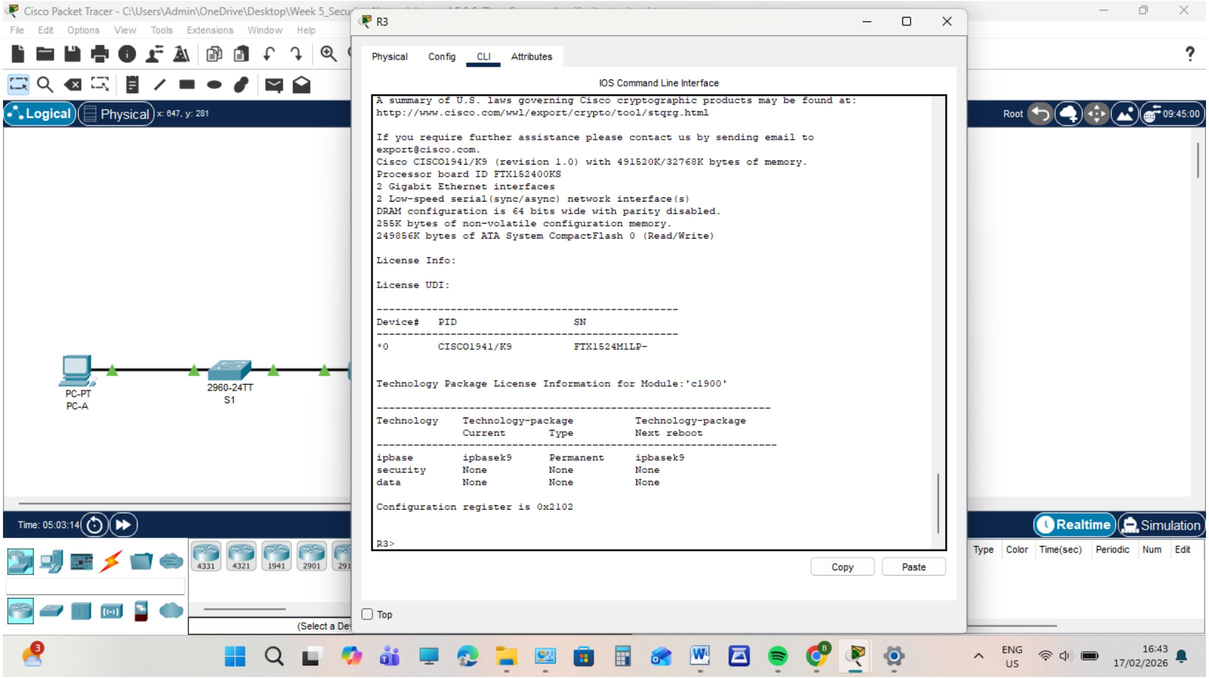


Part 1: Enable Security Features

Step 1: Activate securityk9 module

a) Verification

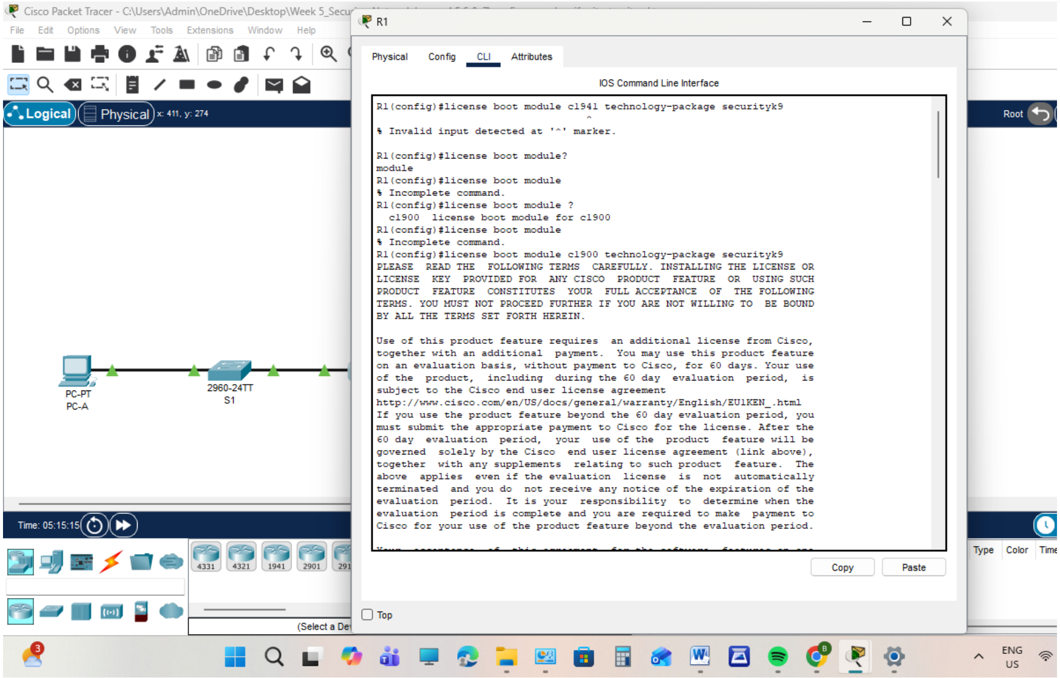
I initially accessed the CLI of R1 and used the show version command to check the current license status. I observed that the securityk9 package was not yet active



```
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
*0        CISCO1941/K9          FTX1524M1LP-


Technology Package License Information for Module:'c1900'

----------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent      ipbasek9
security      None          None           None
data          None          None           None

Configuration register is 0x2102


R3>
```

b) Activation

I entered Global Configuration mode and issued the command license boot module c1900 technology-package securityk9 the officially accepted the End User License Agreement (EULA) by typing yes when prompted

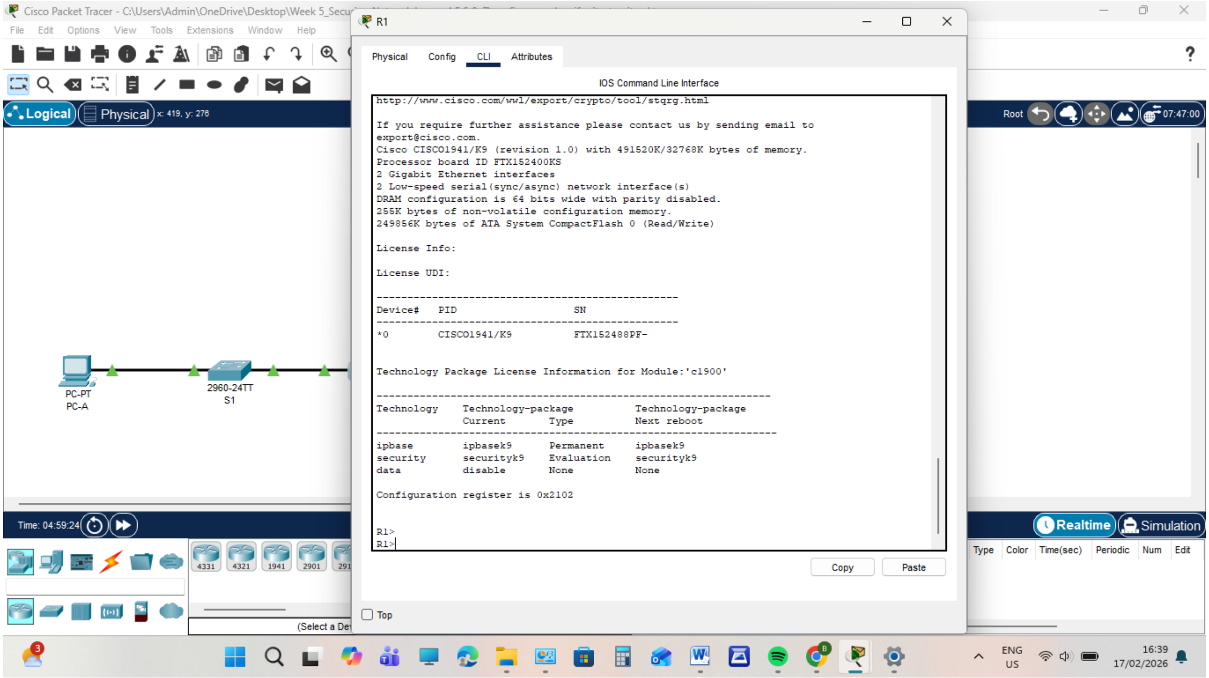


Cisco Packet Tracer - C:\Users\Admin\OneDrive\Desktop\Week 5_Secu
R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Copy
Paste
Top
PC-PT
PC-A
2960-24TT
S1
Time: 05:15:15

```
R1(config)#license boot module c1941 technology-package securityk9
                                  ^
% Invalid input detected at '^' marker.

R1(config)#license boot module?
module
R1(config)#license boot module
% Incomplete command.
R1(config)#license boot module ?
  c1900  license boot module for c1900
R1(config)#license boot module
% Incomplete command.
R1(config)#license boot module c1900 technology-package securityk9
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO  BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires  an additional license from Cisco,
together with an additional  payment.  You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the  product,  including  during the 60 day  evaluation  period,  is
subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
If you use the product feature beyond the 60 day evaluation period, you
must submit the appropriate payment to Cisco for the license. After the
60 day  evaluation  period,  your  use of the  product  feature will be
governed  solely by the Cisco  end user license agreement (link above),
together  with any supplements  relating to such product  feature.  The
above  applies  even if the evaluation  license  is  not  automatically
terminated  and you do  not receive any notice of the expiration of the
evaluation  period.  It is your  responsibility  to  determine when the
evaluation  period is complete and you are required to make  payment to
Cisco for your use of the product feature beyond the evaluation period.
```

c) *Saving and initialization*

To finalize the process I moved back to privileged EXEC mode saved the configuration using copy running-config startup-config and execute a reload. This restart was necessary for the router to initialize the security technology package



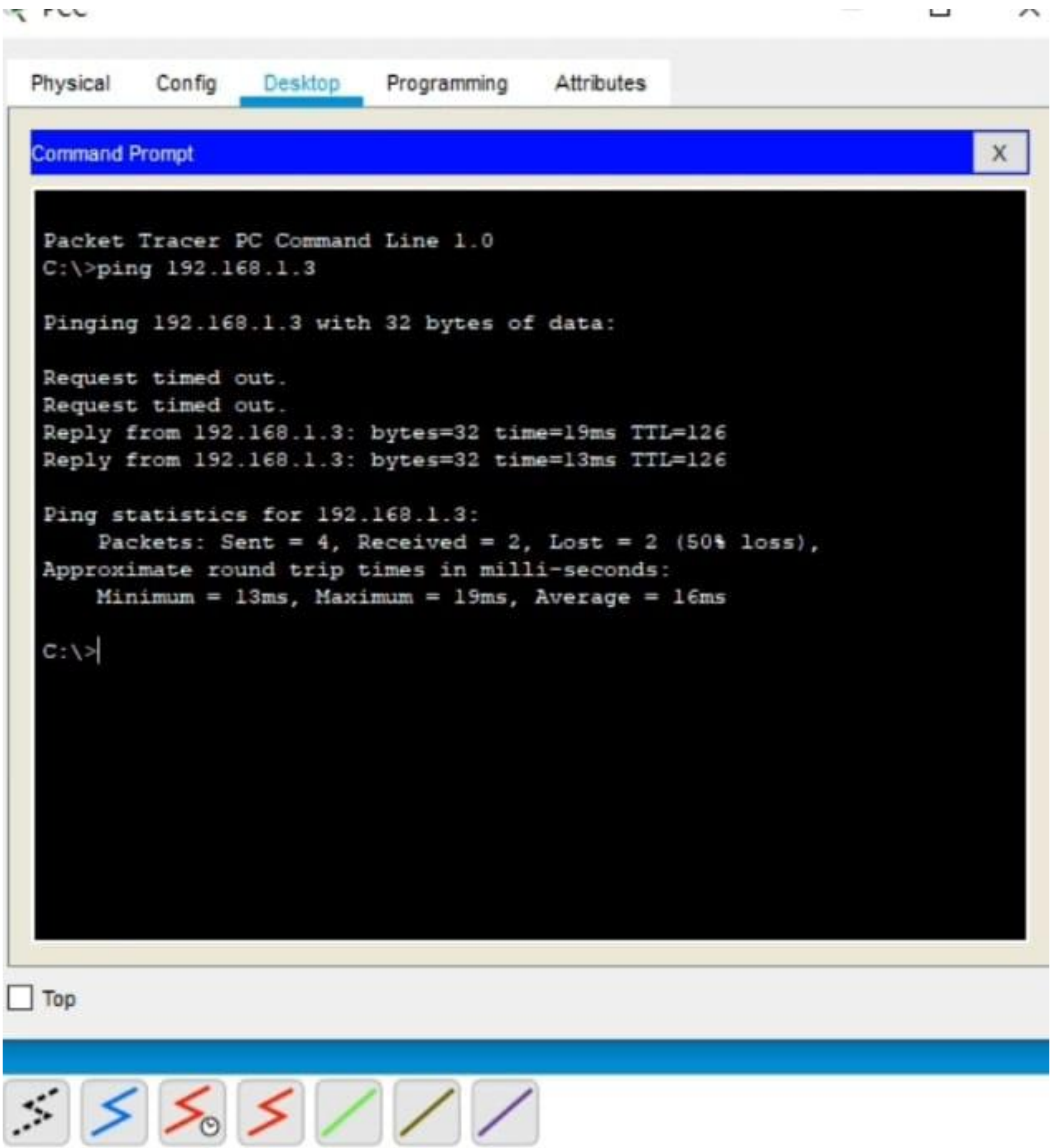
```
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
*0        CISCO1941/K9          FTX152488PF-


Technology Package License Information for Module:'c1900'

----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
data          disable       None          None

Configuration register is 0x2102


R1>
R1>
```

Part 2: Configure IPsec Parameters on R1

Step 1: Test connectivity

Ping from PC-A to PC-C

I ping and I got the following results

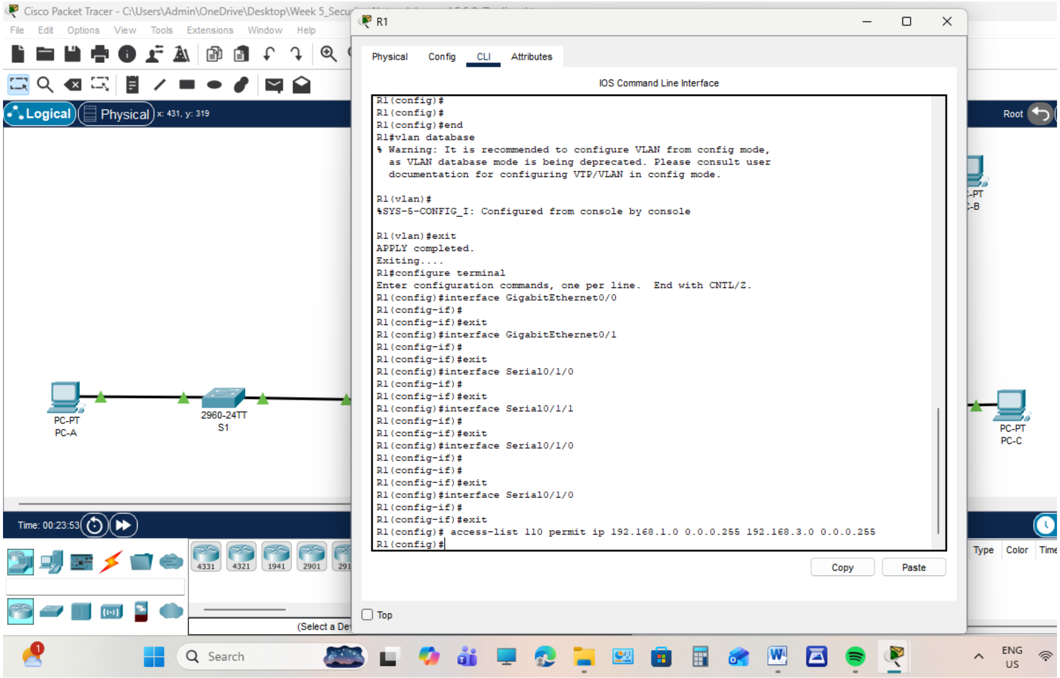


```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.1.3: bytes=32 time=19ms TTL=126
Reply from 192.168.1.3: bytes=32 time=13ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 19ms, Average = 16ms

C:\>
```

Step 2: identify interesting traffic on R1

This is the definition of “Interesting Traffic”

The router uses this list to distinguish between regular internet traffic and traffic that needs to be encrypted. I defined a rule that permits any IP traffic travelling from the local LAN (192.168.1.0) to the remote LAN (192.168.3.0) to trigger the VPN tunnel



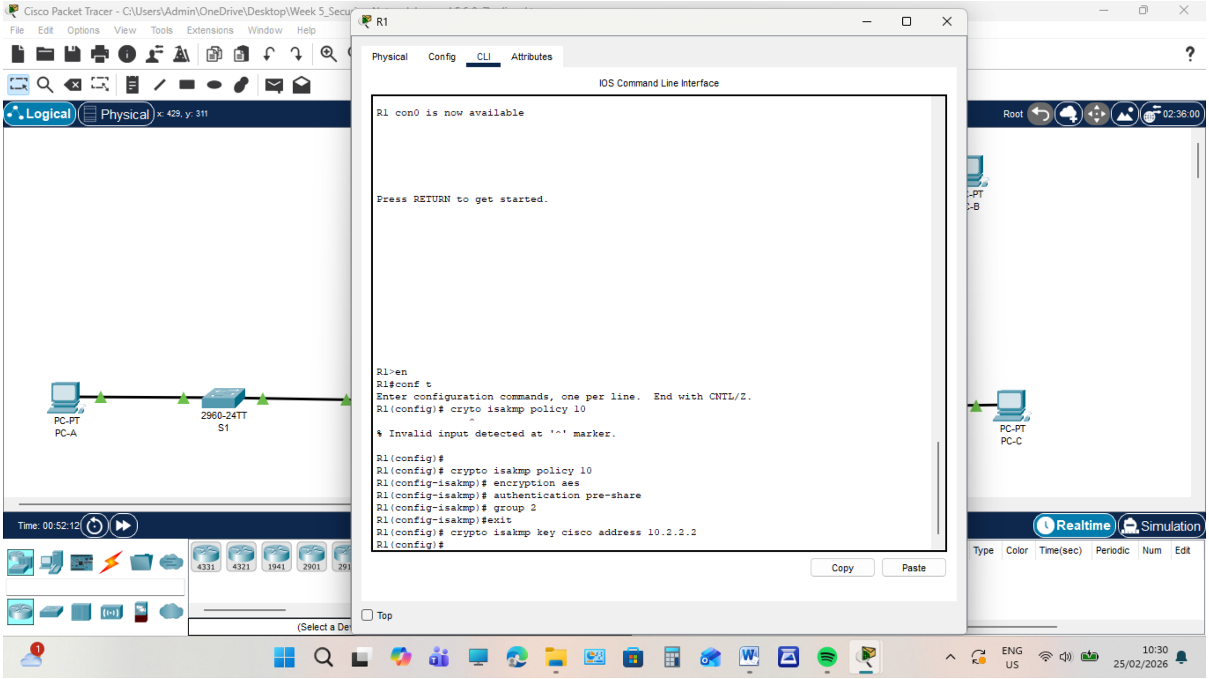
```
R1(config)#
R1(config)#
R1(config)#end
R1#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

R1(vlan)#
%SYS-5-CONFIG_I: Configured from console by console

R1(vlan)#exit
APPLY completed.
Exiting....
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface GigabitEthernet0/0
R1(config-if)#
R1(config-if)#exit
R1(config)#interface GigabitEthernet0/1
R1(config-if)#
R1(config-if)#exit
R1(config)#interface Serial0/1/0
R1(config-if)#
R1(config-if)#exit
R1(config)#interface Serial0/1/1
R1(config-if)#
R1(config-if)#exit
R1(config)#interface Serial0/1/0
R1(config-if)#
R1(config-if)#
R1(config-if)#exit
R1(config)#interface Serial0/1/0
R1(config-if)#
R1(config-if)#exit
R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#
```

Step 3: Configure the ISAKMP Phase 1 properties on R1

This screenshot shows the configuration of IKE Phase 1. This phase establishes a secure management connection between R1 and R3

Policy 10- it defines the encryption (AES) and Diffie-Hellman group (Group 2) used for the handshake

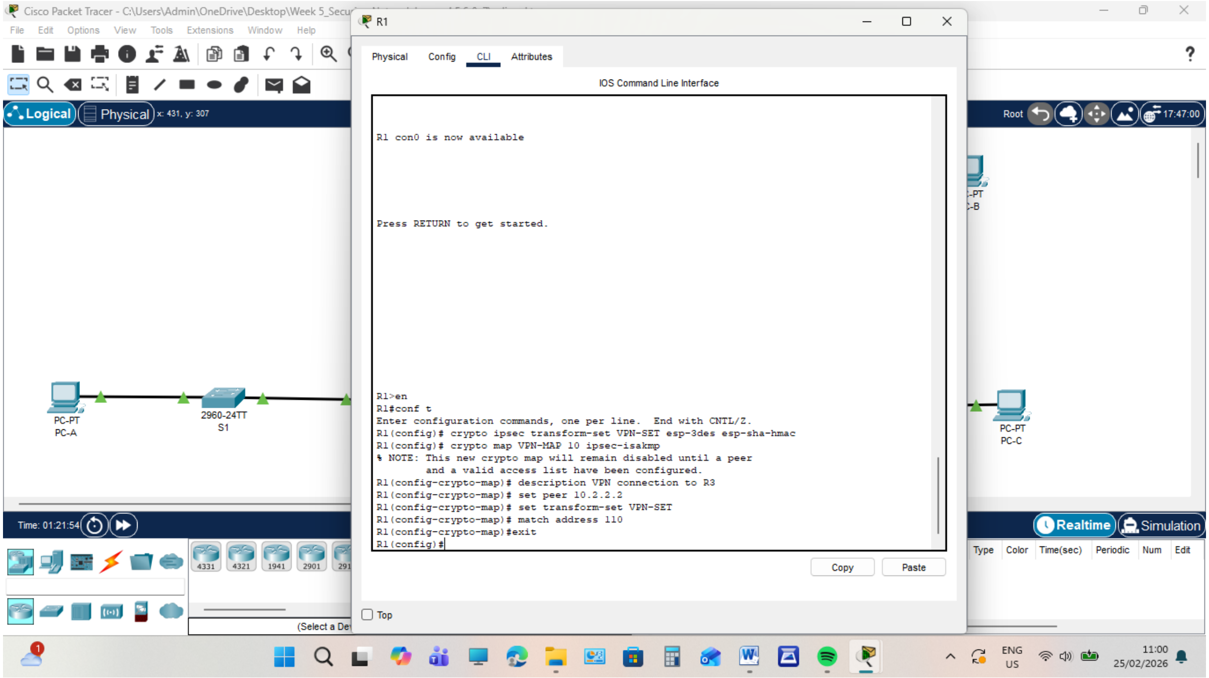
Pre-shared key-the cryptoisakmp key cisco command sets a shared password (“cisco”) that both routers use to authenticate each other before building the tunnel



```
R1 con0 is now available




Press RETURN to get started.










R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# cryto isakmp policy 10
               ^
% Invalid input detected at '^' marker.

R1(config)#
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)#exit
R1(config)# crypto isakmp key cisco address 10.2.2.2
R1(config)#
```

Step 4: Configure the ISAKMP Phase 2 properties on R1

This is the final step that binds the phase 1 and phase 2 configurations together. Applying the crypto map to the outgoing serial interface activates the VPN logic for all traffic exiting the router toward the internet



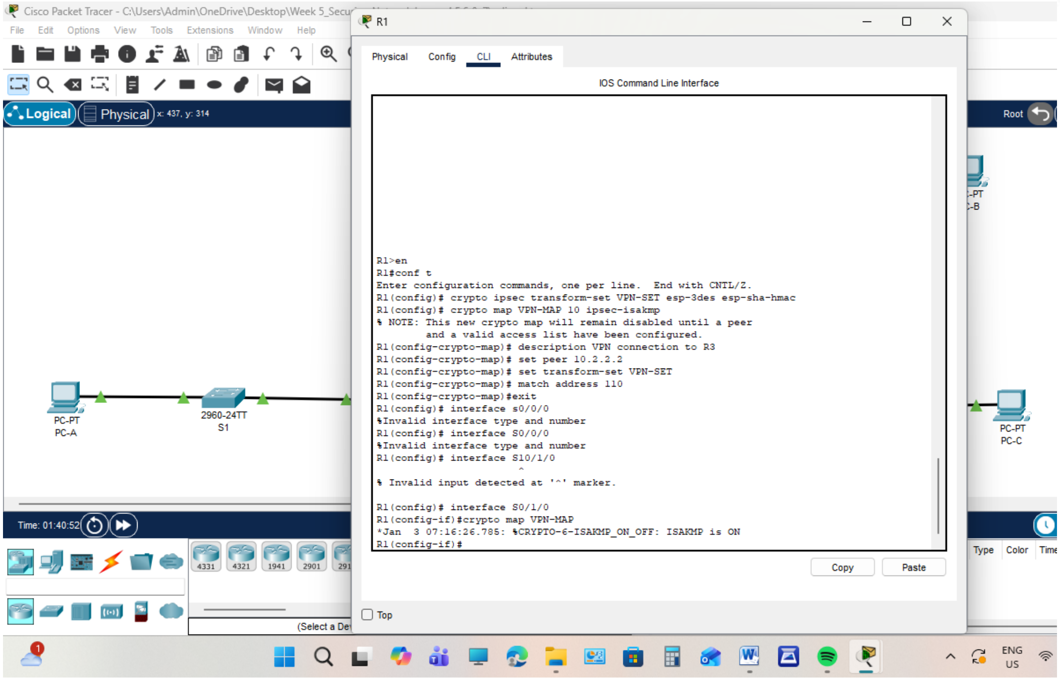
```
R1 con0 is now available



Press RETURN to get started.



R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)# description VPN connection to R3
R1(config-crypto-map)# set peer 10.2.2.2
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)#exit
R1(config)#
```

Step 5: Configure the crypto map on the outgoing interface

I encountered an 'Invalid input' error when trying to bind the VPN to the interface. This served as a key troubleshooting moment. I used the show ip interface brief command to verify the exact hardware naming. I discovered that while the lab manual suggested S0/0/0, my specific Packet Tracer topology required **Serial0/1/0**. Correcting this allowed the crypto map to attach successfully.

Here, I am building the **Crypto Map**, which serves as the 'logic center' for the VPN. It ties together three distinct parts:

1. **Where to go:** The Peer IP (10.2.2.2).
2. **How to encrypt:** The Transform Set (ESP-3DES-SHA).
3. **What to protect:** The ACL 110. The final log message *Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON confirms that the VPN engine is now active on the interface.

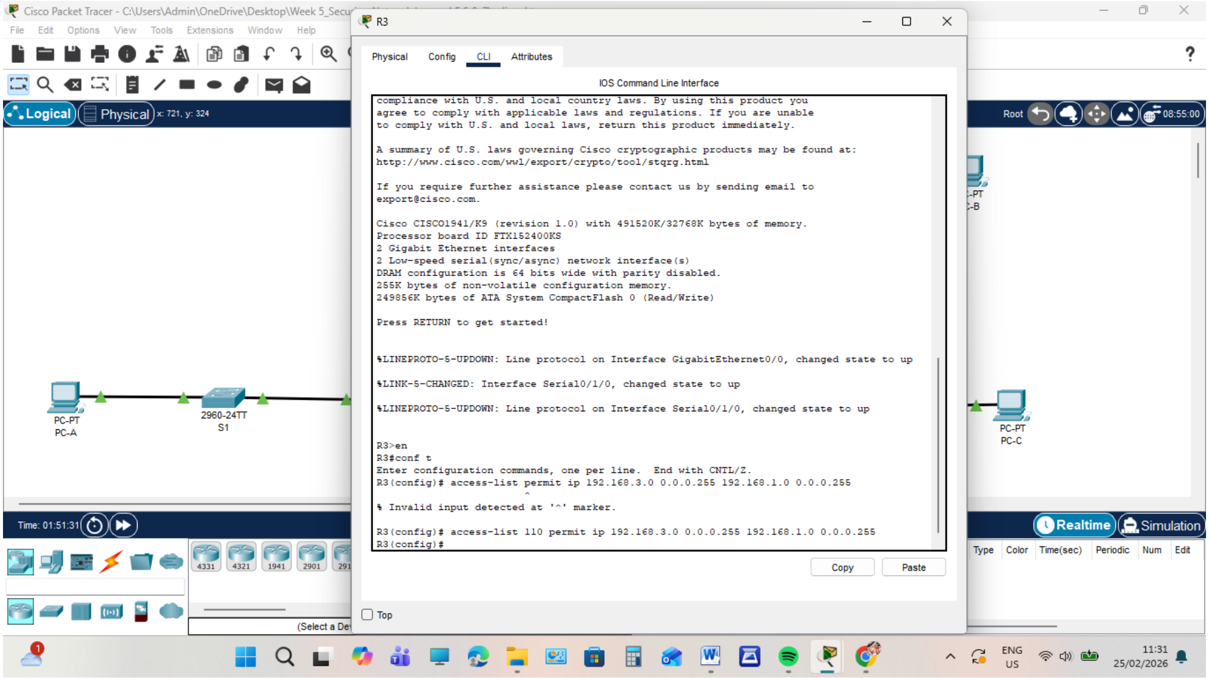


```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)# description VPN connection to R3
R1(config-crypto-map)# set peer 10.2.2.2
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)#exit
R1(config)# interface s0/0/0
%Invalid interface type and number
R1(config)# interface S0/0/0
%Invalid interface type and number
R1(config)# interface S10/1/0
                          ^
% Invalid input detected at '^' marker.

R1(config)# interface S0/1/0
R1(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
```

Part 3: Configure IPsec Parameters on R3

Step 1: Configure router R3 to support a site-to-site VPN with R1

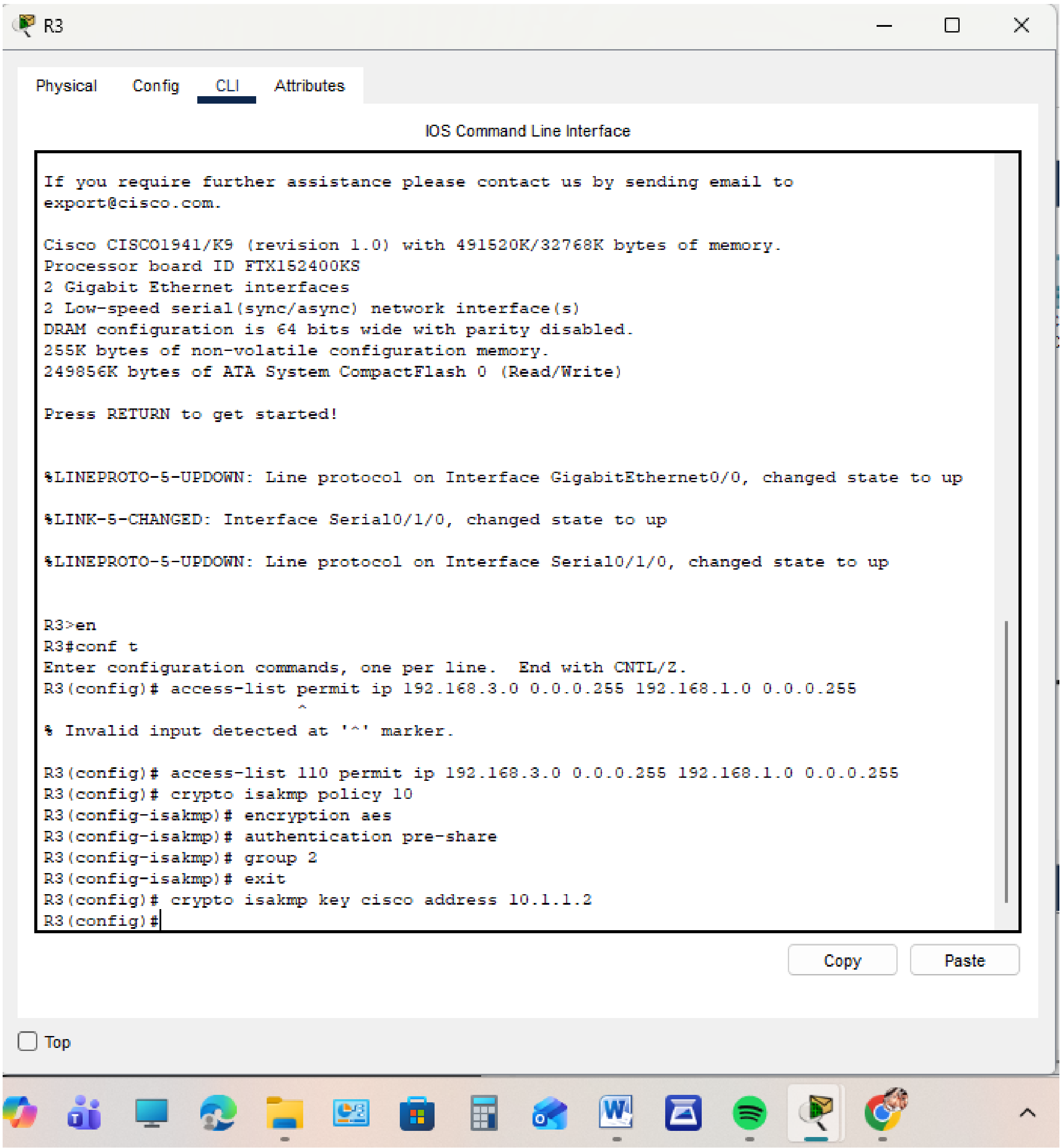
To establish a Site-to-Site VPN, the configuration on the remote peer (R3) must be a 'mirror image' of the local peer (R1). In this screenshot, I configured **ACL 110** on R3. Notice that the source and destination networks are swapped compared to R1: it now identifies traffic coming from R3's LAN (**192.168.3.0**) going to R1's LAN (**192.168.1.0**) as the interesting traffic to be encrypted.



```
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!


%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up


R3>en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# access-list permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
                        ^
% Invalid input detected at '^' marker.

R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#
```

Step 2: Configure the ISAKMP Phase 1 properties on R3

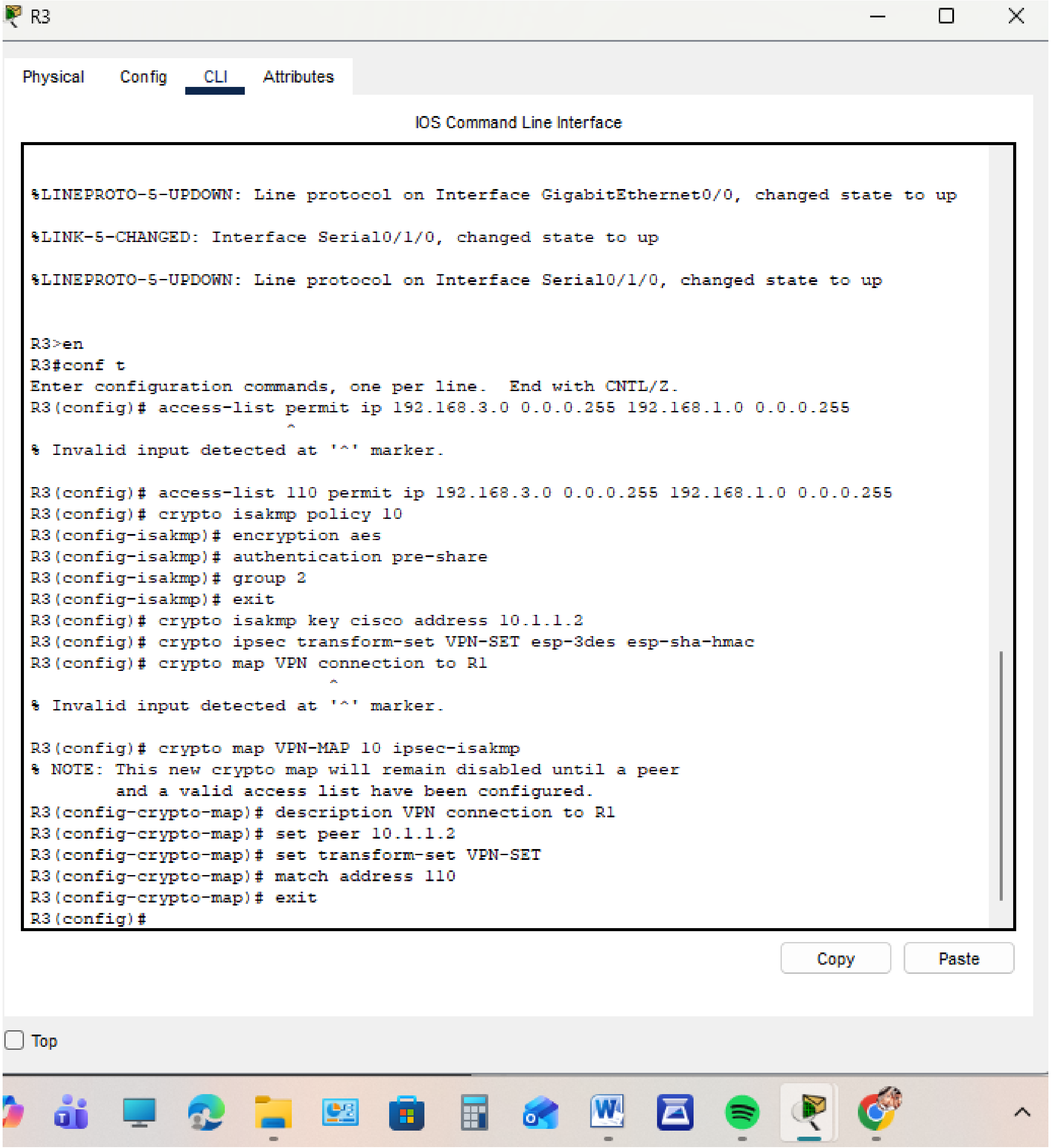
Shows the IKE Phase 1 handshake configuration on R3. Note that the crypto isakmp key cisco address 10.1.1.2 command uses R1's public Serial interface IP as the peer address. This ensures both routers have a matching "secret" to authenticate each other.



```
If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!


%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up


R3>en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# access-list permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
                        ^
% Invalid input detected at '^' marker.

R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)# exit
R3(config)# crypto isakmp key cisco address 10.1.1.2
R3(config)#
```

Step 3: Configure the ISAKMP Phase 2 properties on R1

"In this final configuration phase for R3, I created the Crypto Map named VPN-MAP. This map binds the security policy together by specifying the remote peer (**R1**) and the traffic to be encrypted (ACL 110). The router issued a notification that the map would remain 'disabled' until a valid peer and ACL were bound, which I successfully completed in these steps

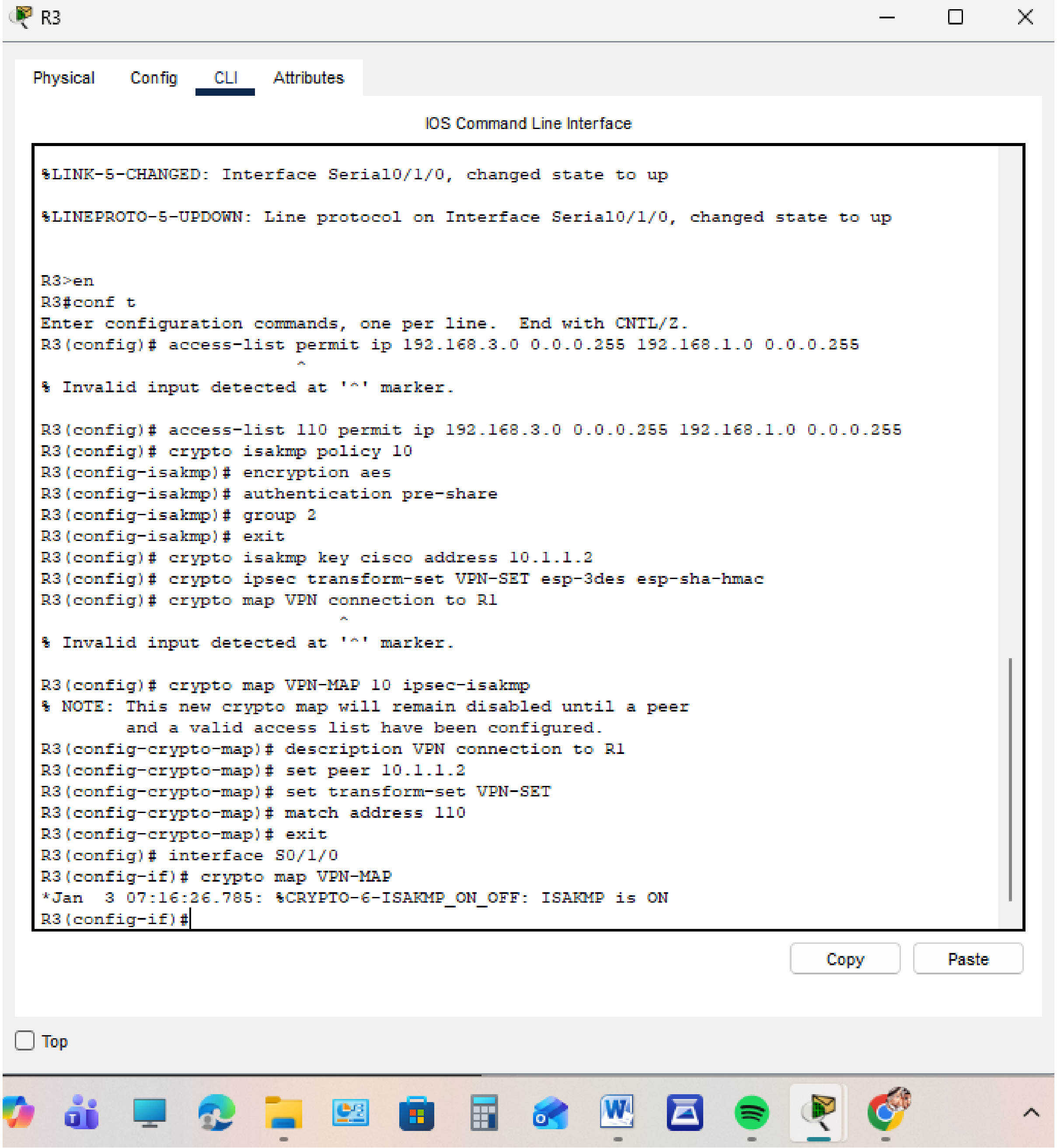


```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up


R3>en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# access-list permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
                         ^
% Invalid input detected at '^' marker.

R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)# exit
R3(config)# crypto isakmp key cisco address 10.1.1.2
R3(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R3(config)# crypto map VPN connection to R1
                             ^
% Invalid input detected at '^' marker.

R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)# description VPN connection to R1
R3(config-crypto-map)# set peer 10.1.1.2
R3(config-crypto-map)# set transform-set VPN-SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)# exit
R3(config)#
```

Step 4: configure the crypto map on the outgoing interface

□ *Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON.

This message is the "heartbeat" of the configuration. It proves that the router has verified all the settings and has officially activated the VPN engine on the outgoing port.

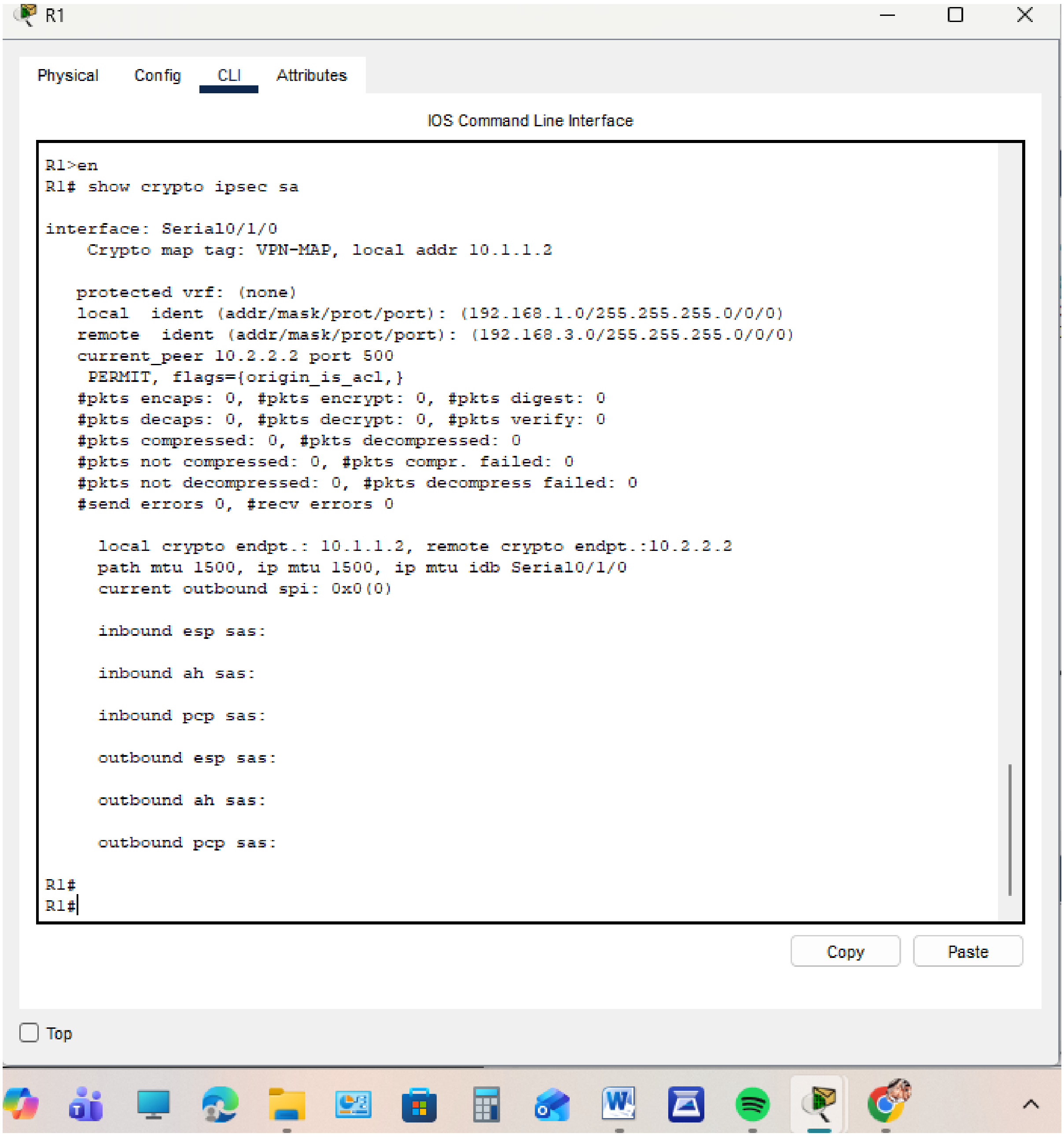


```
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up


R3>en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# access-list permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
                        ^
% Invalid input detected at '^' marker.

R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)# exit
R3(config)# crypto isakmp key cisco address 10.1.1.2
R3(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R3(config)# crypto map VPN connection to R1
                            ^
% Invalid input detected at '^' marker.

R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)# description VPN connection to R1
R3(config-crypto-map)# set peer 10.1.1.2
R3(config-crypto-map)# set transform-set VPN-SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)# exit
R3(config)# interface S0/1/0
R3(config-if)# crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#
```

Part 4: Verify the IPsec VPN

Step 1: Verify the tunnel prior to interesting traffic

Definitive proof that the data was not sent as plain text. The increasing counters show that the router is actively "wrapping" (encapsulating) my pings in an encrypted IPsec header before sending them across the public network.

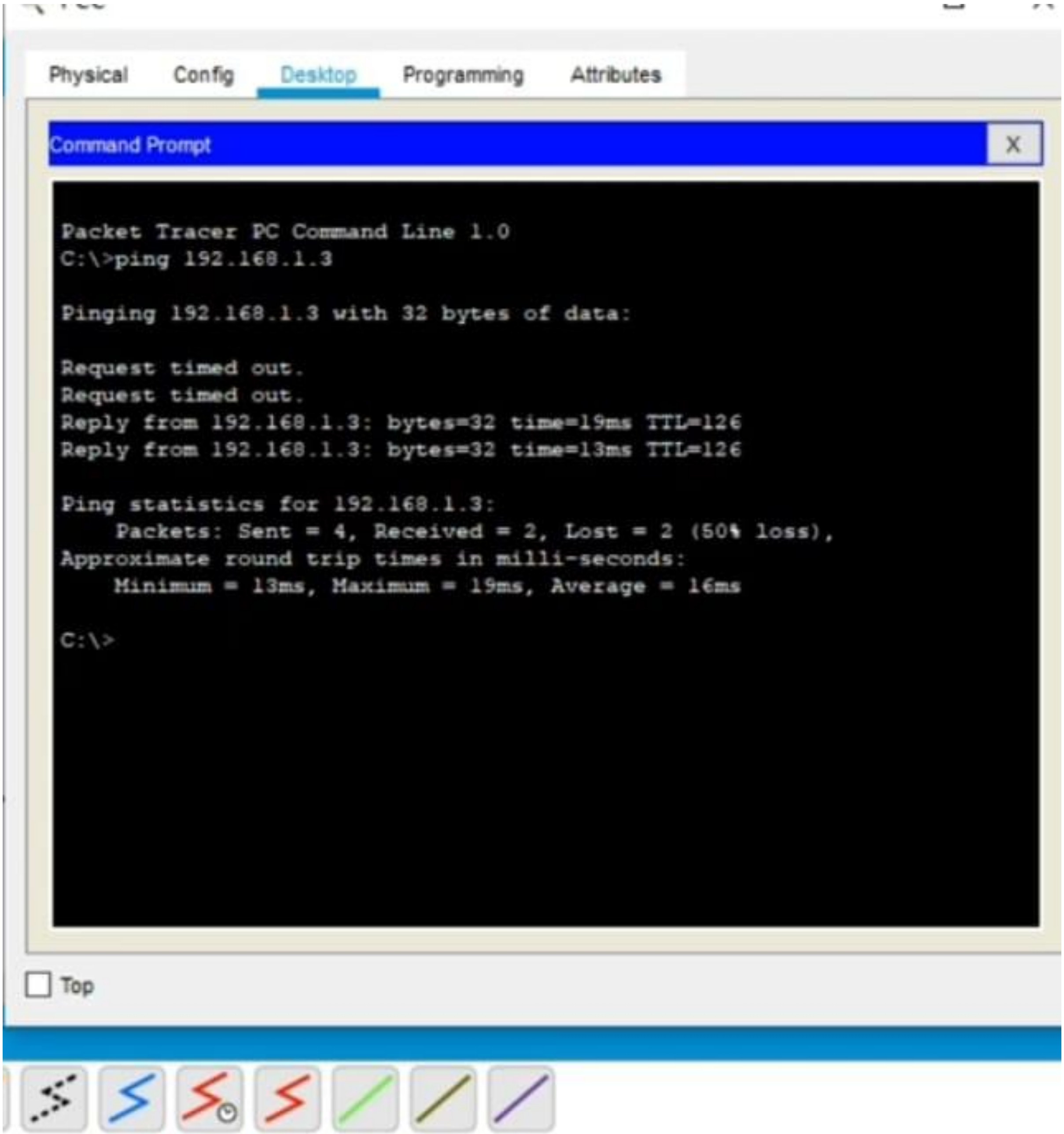


```
R1>en
R1# show crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   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 10.2.2.2 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.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:

R1#
R1#
```

Step 2: Create Interesting traffic

Ping PC-C from PC-A

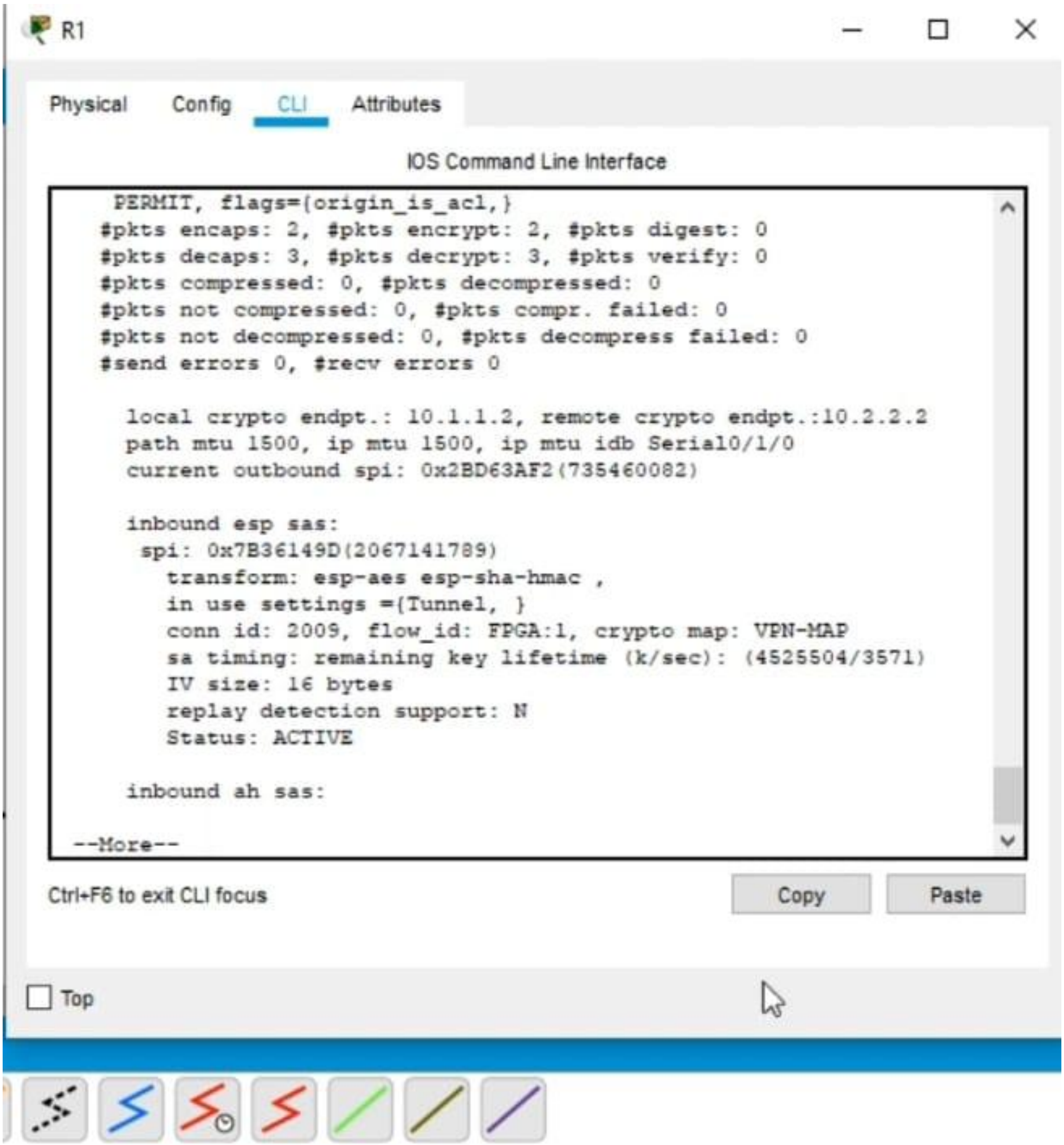
The subsequent "Reply" messages confirm that the tunnel became active. This proves that the local and remote crypto endpoints (R1 at **10.1.1.2** and R3 at **10.2.2.2**) successfully authenticated using the pre-shared key "cisco"



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.1.3: bytes=32 time=19ms TTL=126
Reply from 192.168.1.3: bytes=32 time=13ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 19ms, Average = 16ms

C:\>
```

Step 3: Verify the tunnel after interesting traffic

By generating 'interesting traffic' via a ping, I forced the routers to move from an idle state to an active encrypted state. The increase in the encapsulation counters in the show crypto ipsec sa output provides definitive evidence that the site-to-site VPN is correctly securing the data as it traverses the public network

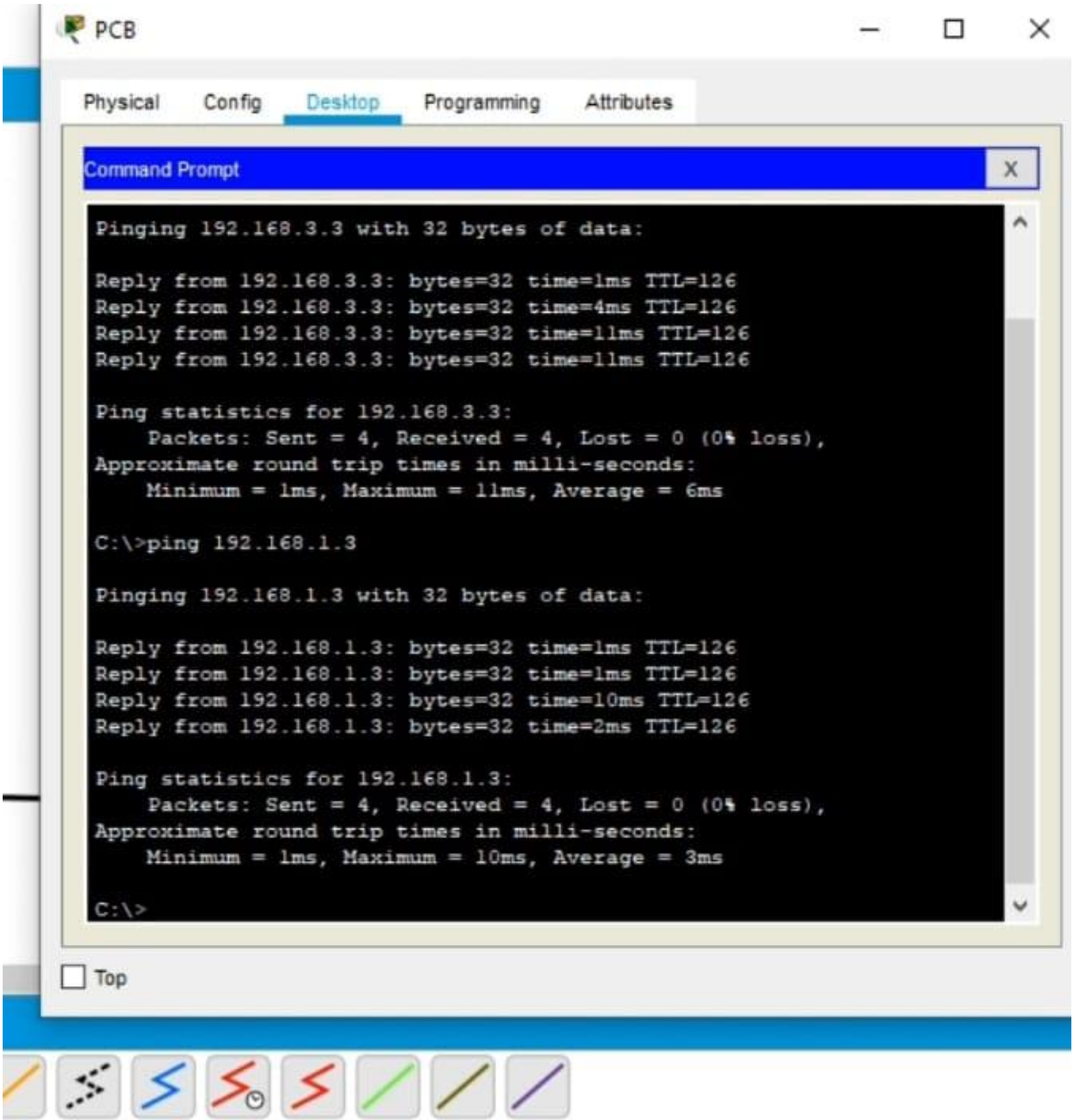


```
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 0
    #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

      local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
      path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
      current outbound spi: 0x2BD63AF2(735460082)

      inbound esp sas:
       spi: 0x7B36149D(2067141789)
         transform: esp-aes esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 2009, flow_id: FPGA:1, crypto map: VPN-MAP
         sa timing: remaining key lifetime (k/sec): (4525504/3571)
         IV size: 16 bytes
         replay detection support: N
         Status: ACTIVE

      inbound ah sas:

--More--
```

Step 4: Create uninteresting traffic

Ping PC-B from PC-A

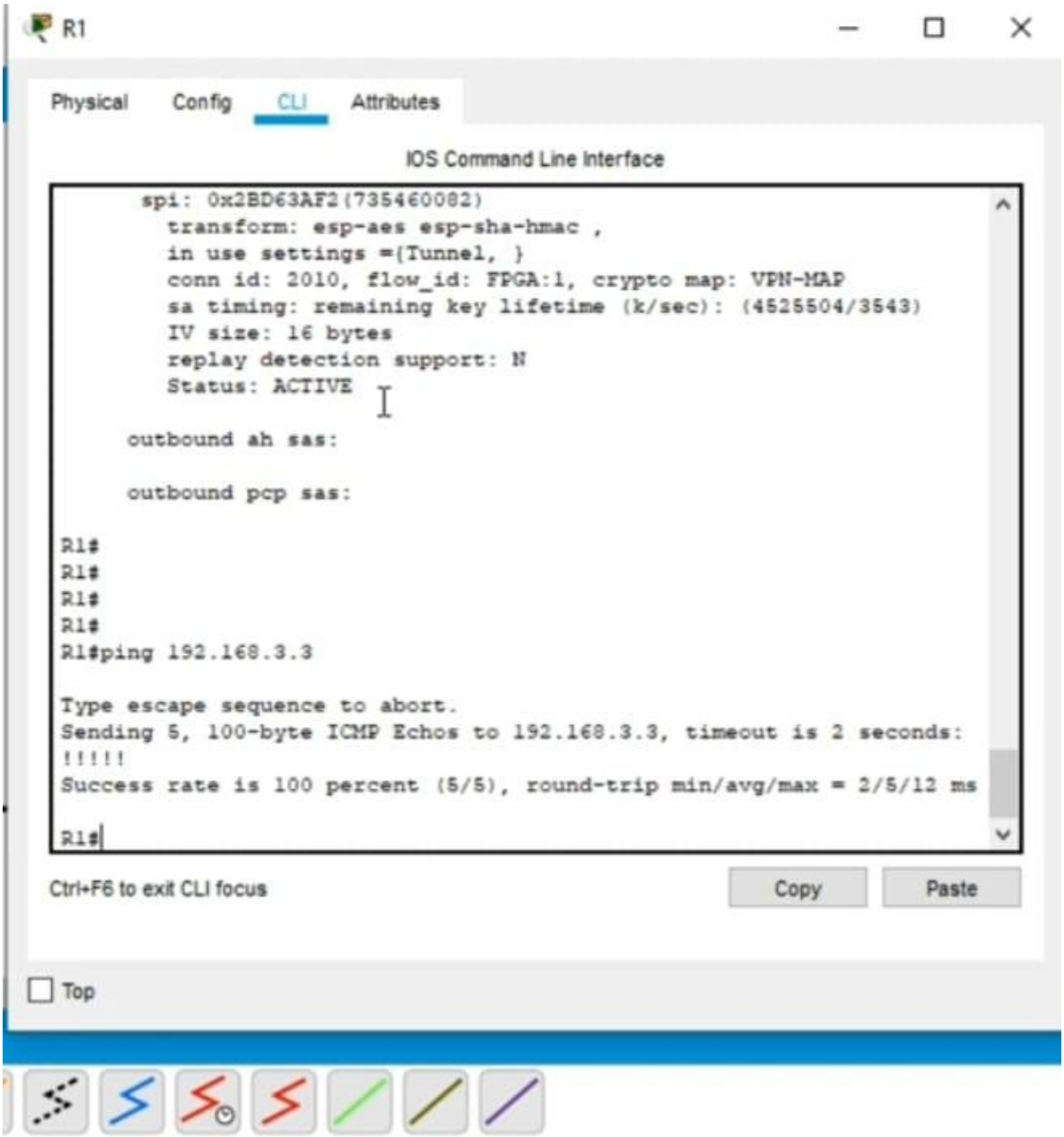
By testing both 'interesting' (Remote) and 'uninteresting' (Local) traffic, I have verified the precision of the Security Association. The VPN tunnel only activates for traffic destined for the remote branch office, ensuring that local network performance remains high while remote communications remain secure.



```
Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=4ms TTL=126
Reply from 192.168.3.3: bytes=32 time=11ms TTL=126
Reply from 192.168.3.3: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 6ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=10ms TTL=126
Reply from 192.168.1.3: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 10ms, Average = 3ms

C:\>
```

Step 5: Verify the tunnel

"By testing both types of traffic, I have verified that the VPN configuration is highly targeted. The tunnel provides security for remote branch communications while allowing local network traffic to function with maximum efficiency and zero encryption overhead. This completes the verification phase of the Site-to-Site IPsec VPN.



```
         spi: 0x2BD63AF2(735460082)
           transform: esp-aes esp-sha-hmac ,
           in use settings ={Tunnel, }
           conn id: 2010, flow_id: FPGA:1, crypto map: VPN-MAP
           sa timing: remaining key lifetime (k/sec): (4525504/3543)
           IV size: 16 bytes
           replay detection support: N
           Status: ACTIVE

        outbound ah sas:

        outbound pcp sas:

R1#
R1#
R1#
R1#
R1#ping 192.168.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/5/12 ms

R1#
```

Conclusion

In conclusion the objective of this assignment was to implement and verify a secure Site-to-Site IPsec VPN between two branch offices using Cisco routers. Through the successful configuration of IKE Phase 1 (ISAKMP) and IPsec Phase 2, I established an encrypted tunnel that ensures data confidentiality and integrity while traversing an untrusted public ISP network. **Verification through IOS commands confirmed that 'interesting traffic' was successfully encapsulated and encrypted, while local 'uninteresting traffic' remained unaffected.**"