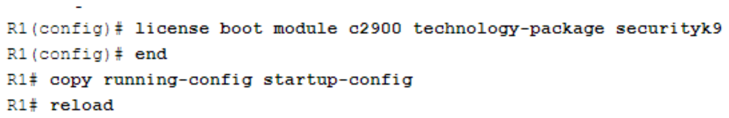
ASSIGNMENT 2: CONFIGURING VPNS (OPTIONAL) WRITEUP

Introduction

IPsec, short for Internet Protocol Security, is a set of protocols and standards used to secure and authenticate Internet Protocol (IP) communications. It provides a framework for ensuring confidentiality, integrity, and authentication of IP packets transmitted over a network. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (peers), such as Cisco routers. In this assignment, we learn how to enable security features and configure two routers to support a site-to-site IPsec VPN for traffic flowing from their respective LANs to understand how to secure networks from layer 1-3 in the OSI model.

Part 1: Enable Security Features

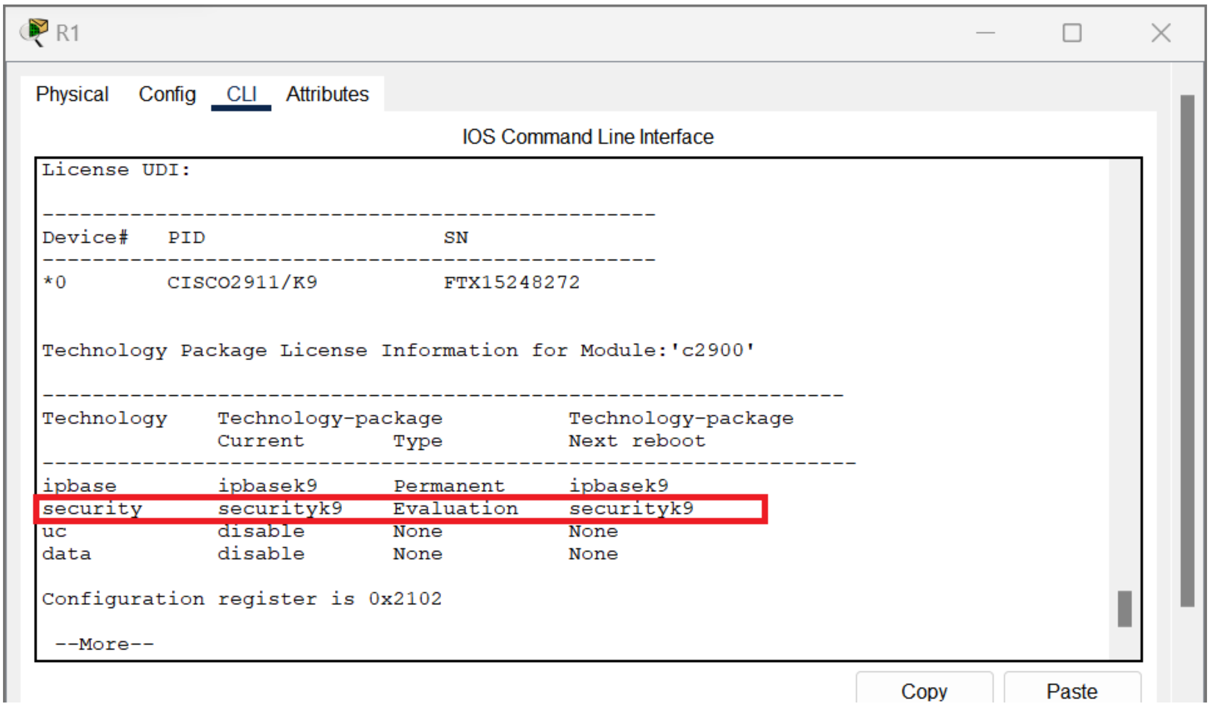
In this section details the process of enabling the security features by activating the securityk9 module by keying the following commands:



```
R1(config)# license boot module c2900 technology-package securityk9
R1(config)# end
R1# copy running-config startup-config
R1# reload
```

Figure 1: Commands for activating securityk9 module.

and verifying using the show version command under the CLI on R1 and R3 as shown below.



```
License UDI:

-------------------------------------------------
Device#   PID                     SN
-------------------------------------------------
*0        CISCO2911/K9            FTX15248272


Technology Package License Information for Module:'c2900'

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

Configuration register is 0x2102

 --More--
```

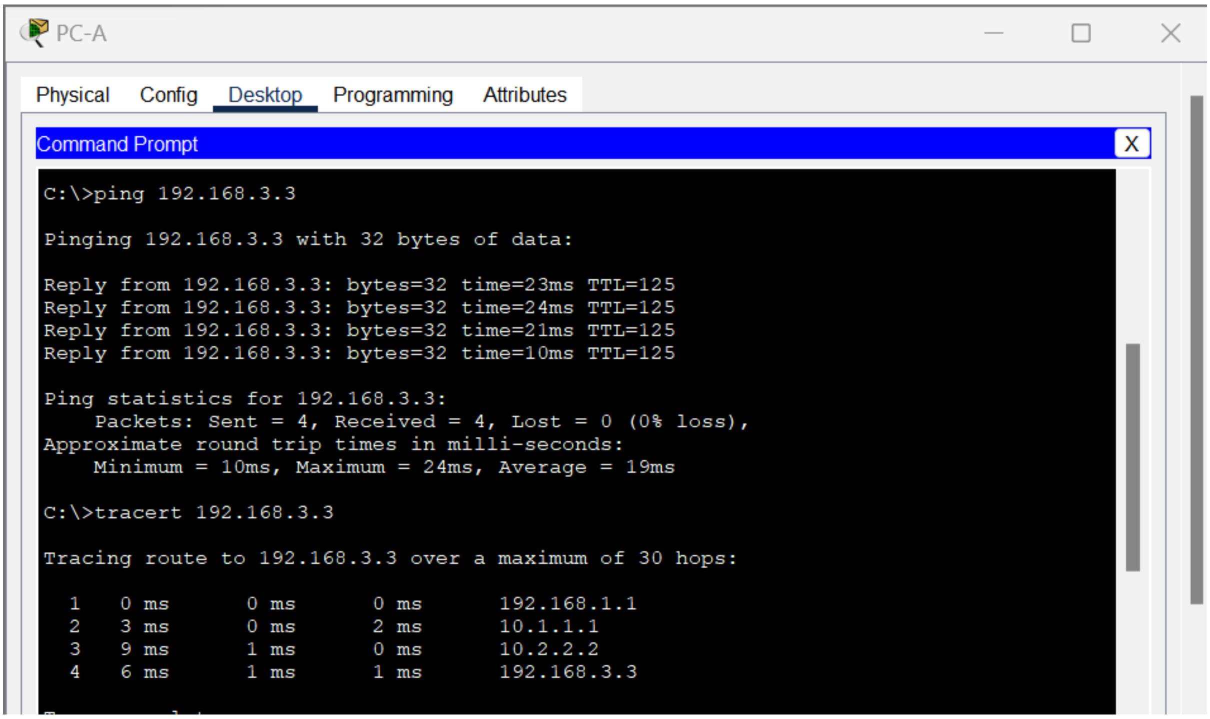
Figure 2:Verifying using show command.

Part 2: Configure IPsec Parameters on R1

This section details a step-by-step process of configuring IPsec Parameter on Router 1.

Step 1: Test connectivity.

The first step is testing the connectivity by pinging from PC-A to PC-C.

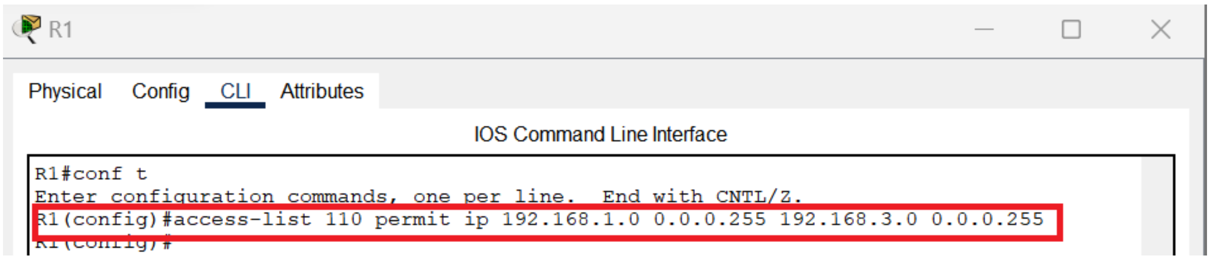


```
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=23ms TTL=125
Reply from 192.168.3.3: bytes=32 time=24ms TTL=125
Reply from 192.168.3.3: bytes=32 time=21ms TTL=125
Reply from 192.168.3.3: bytes=32 time=10ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 24ms, Average = 19ms

C:\>tracert 192.168.3.3

Tracing route to 192.168.3.3 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.1.1
  2   3 ms      0 ms      2 ms      10.1.1.1
  3   9 ms      1 ms      0 ms      10.2.2.2
  4   6 ms      1 ms      1 ms      192.168.3.3
```

Figure 3: Testing connectivity

Step 2: Identify interesting traffic on R1.

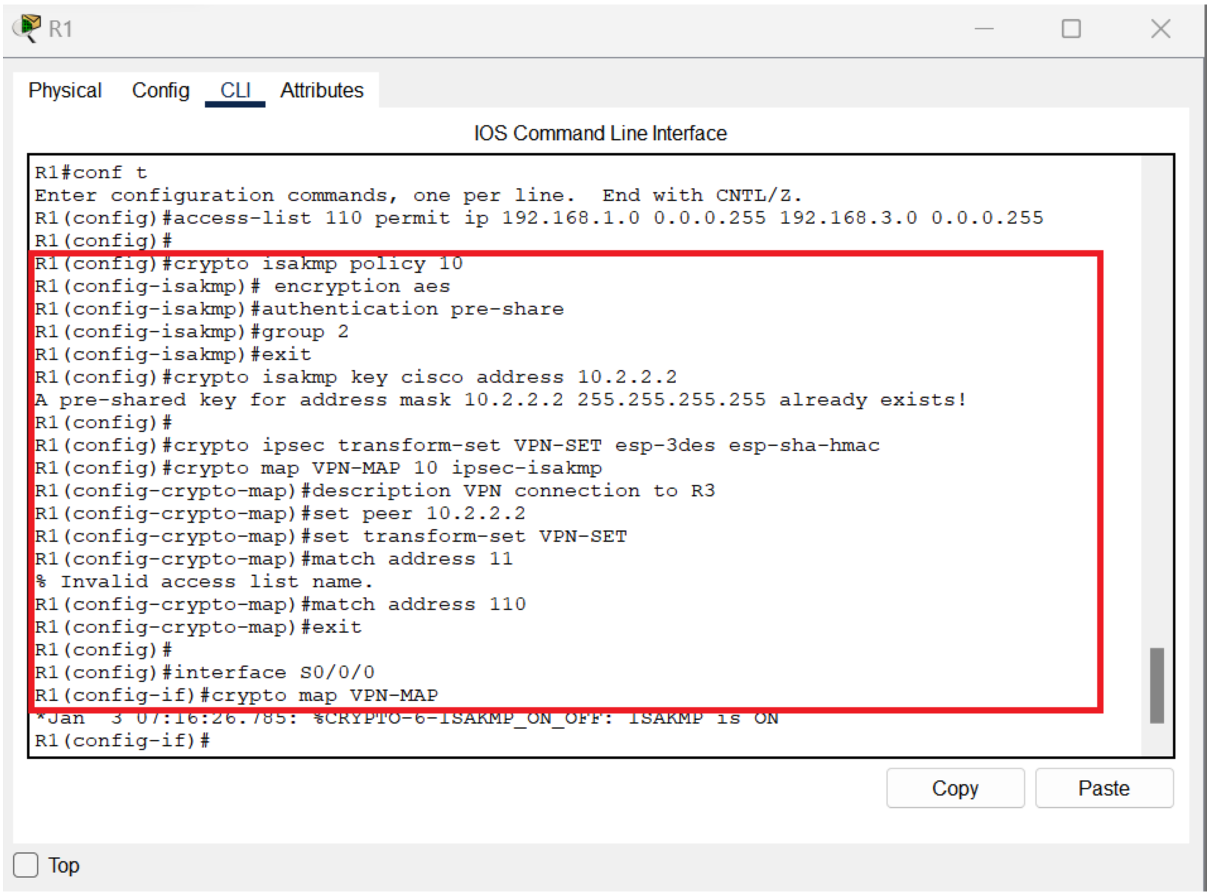
The next step is identifying interesting traffic on R1 by configuring Access list 110 to identify the traffic from the LAN on R1 to the LAN on R3 as interesting. This interesting traffic will trigger the IPsec VPN to be implemented whenever there is traffic between R1 to R3 LANs. All other traffic sourced from the LANs will not be encrypted.



```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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 and the ISAKMP Phase 2 properties on R1.

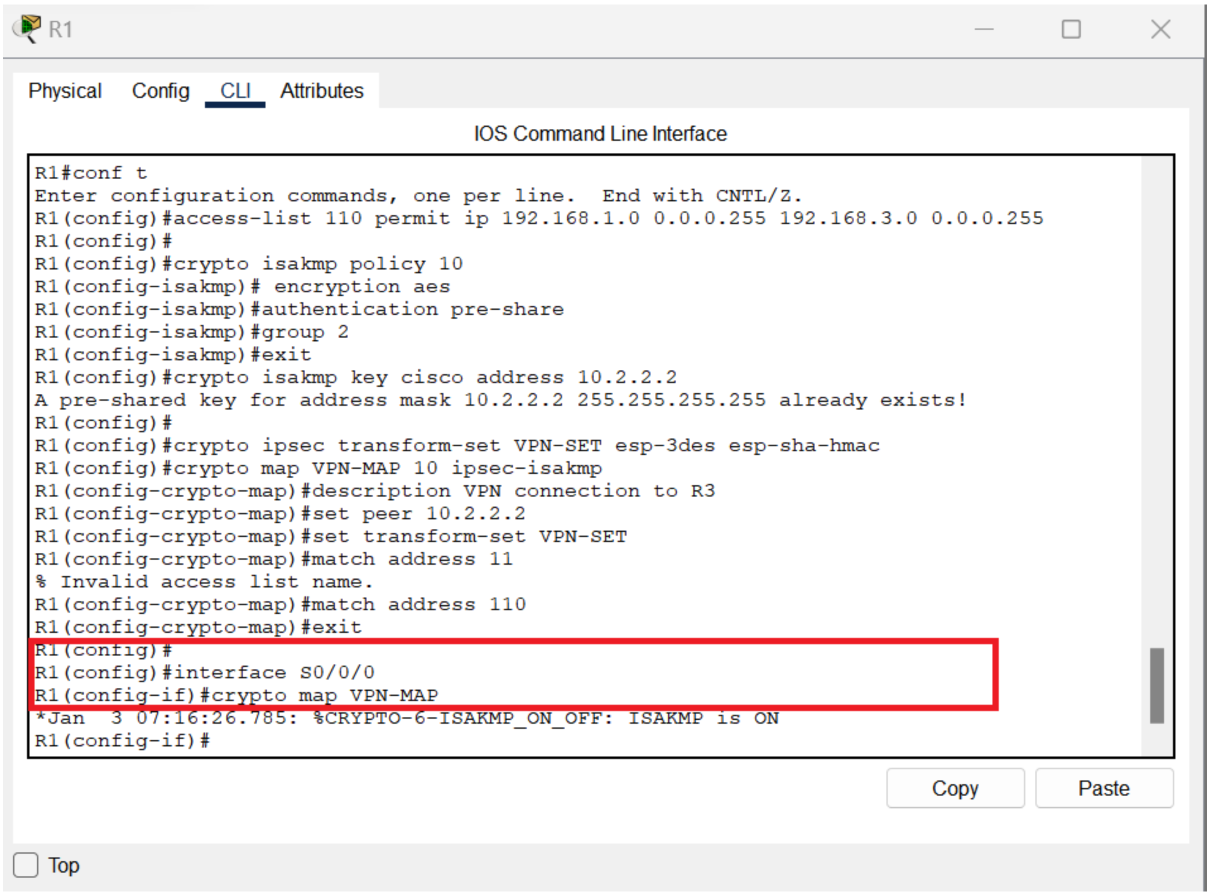
In this step, configuring the crypto ISAKMP policy 10 properties on R1 along with the shared crypto key cisco and Create the transform-set VPN-SET to use esp-3des and esp-sha-hmac, then create the crypto map VPN-MAP that binds all of the Phase 2 parameters together. Use sequence number 10 and identify it as an ipsec-isakmp map.



```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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)#
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
A pre-shared key for address mask 10.2.2.2 255.255.255.255 already exists!
R1(config)#
R1(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R1(config)#crypto map VPN-MAP 10 ipsec-isakmp
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 11
% Invalid access list name.
R1(config-crypto-map)#match address 110
R1(config-crypto-map)#exit
R1(config)#
R1(config)#interface S0/0/0
R1(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
```

Step 4: Configure the crypto map on the outgoing interface.

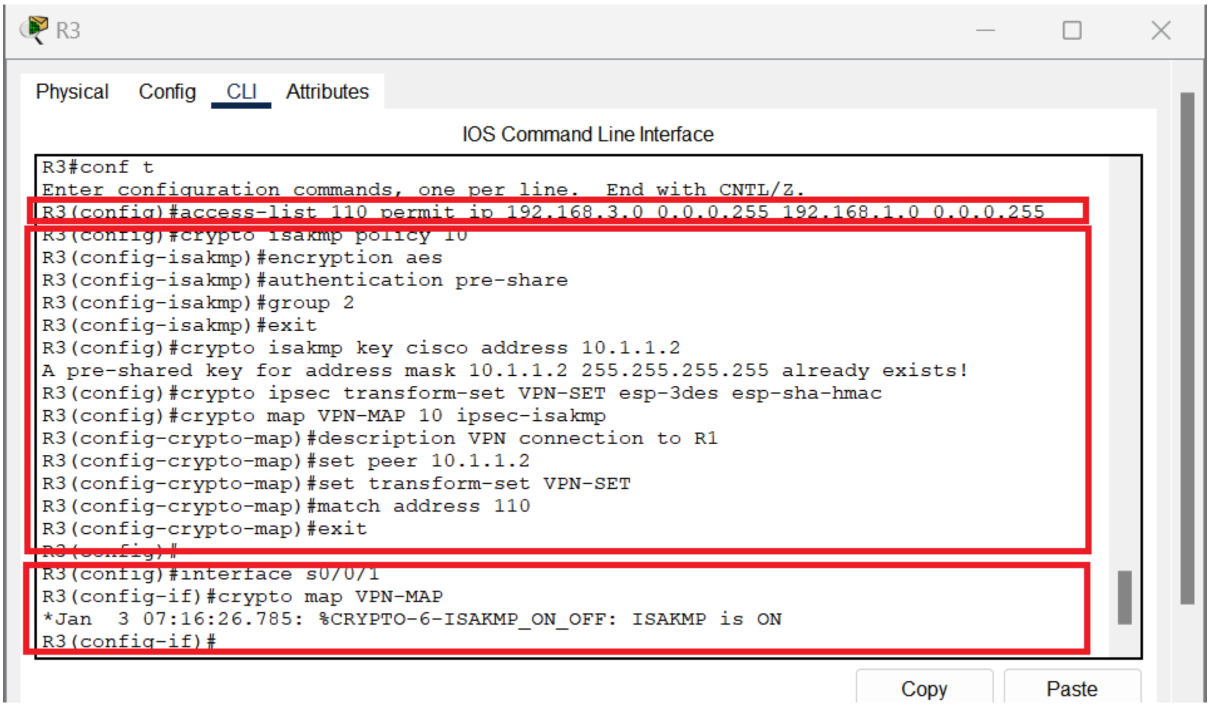
Finally, bind the VPN-MAP crypto map to the outgoing Serial 0/0/0 interface by running the following command.



```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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)#
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
A pre-shared key for address mask 10.2.2.2 255.255.255.255 already exists!
R1(config)#
R1(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R1(config)#crypto map VPN-MAP 10 ipsec-isakmp
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 11
% Invalid access list name.
R1(config-crypto-map)#match address 110
R1(config-crypto-map)#exit
R1(config)#
R1(config)#interface S0/0/0
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

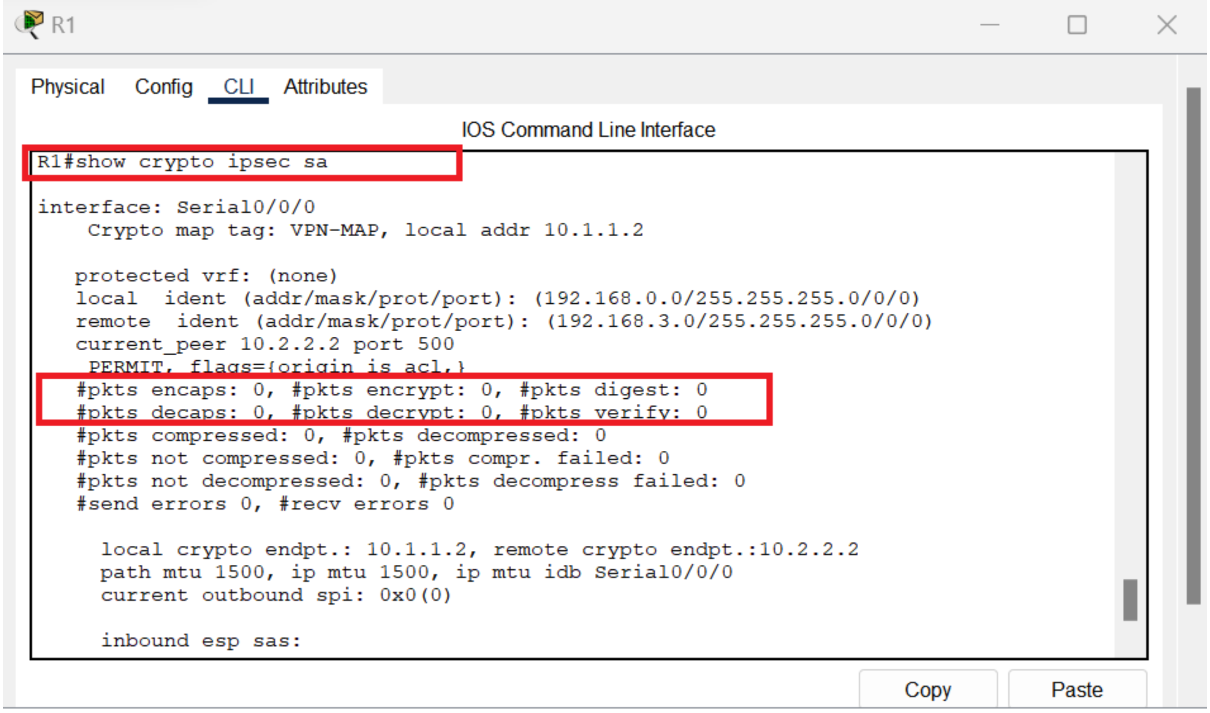
In the section, configuring IPsec Parameters on Router 3(R3), like router 1, follow the same steps as part 2.



```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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
A pre-shared key for address mask 10.1.1.2 255.255.255.255 already exists!
R3(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R3(config)#crypto map VPN-MAP 10 ipsec-isakmp
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)#
R3(config)#interface s0/0/1
R3(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#
```

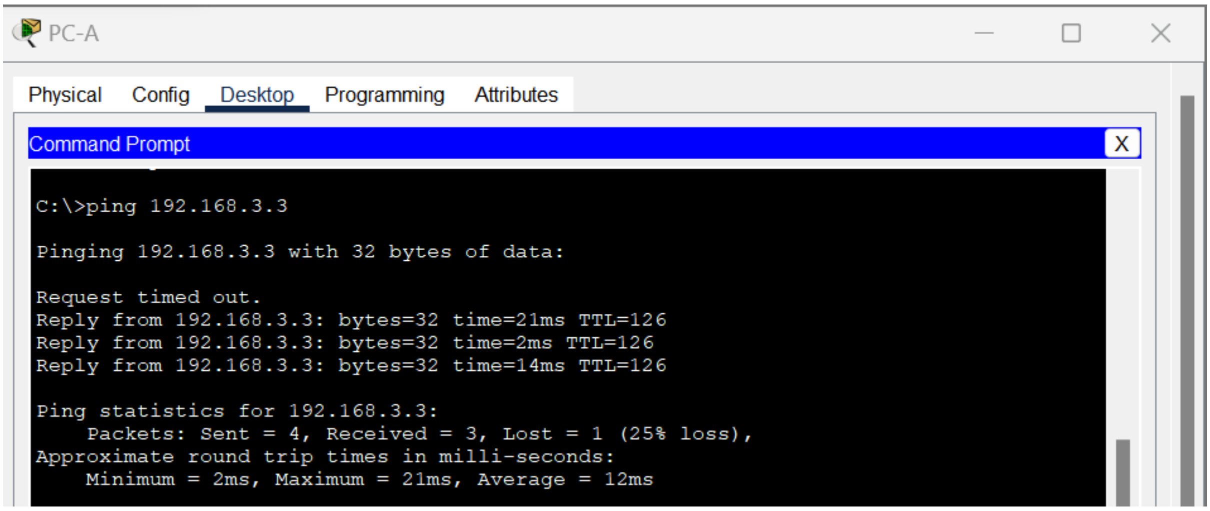
Part 4: Verify the IPsec VPN

In this section, verification of the IPsec VPN was done by verifying the tunnel prior to interesting traffic by using the show ipsec sa command as shown below.

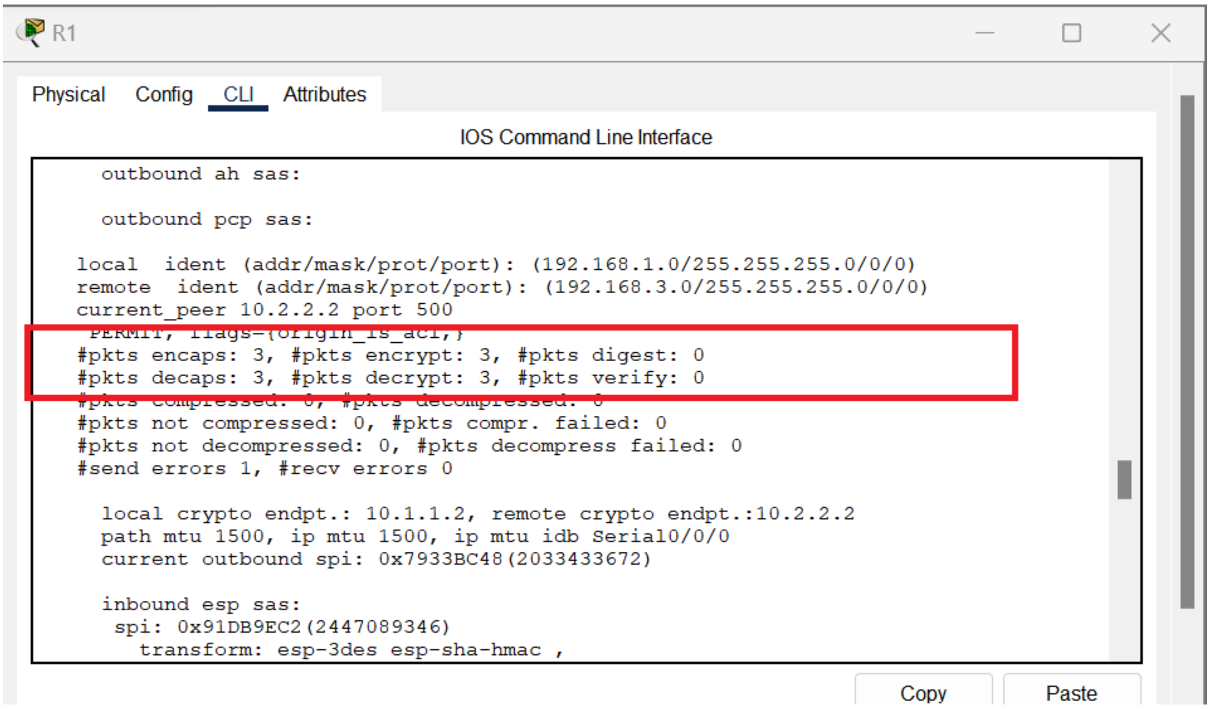


```
R1#show crypto ipsec sa

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

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)
   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 Serial0/0/0
     current outbound spi: 0x0(0)

     inbound esp sas:
```

Then create traffic by pinging PC-C from PC-A then use the show ipsec sa command again and the number of packets is more than 0 indicating that the IPsec VPN tunnel is working.



```
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.3: bytes=32 time=21ms TTL=126
Reply from 192.168.3.3: bytes=32 time=2ms TTL=126
Reply from 192.168.3.3: bytes=32 time=14ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 21ms, Average = 12ms
```



```
    outbound ah sas:

    outbound pcp sas:

  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: 3, #pkts encrypt: 3, #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 1, #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 Serial0/0/0
    current outbound spi: 0x7933BC48(2033433672)

    inbound esp sas:
     spi: 0x91DB9EC2(2447089346)
       transform: esp-3des esp-sha-hmac ,
```

Conclusion

In conclusion, by successfully completing this task, I have been provided with hands on experience in implementing a secure connection between two LANs by enabling IPsec VPN on the routers, which has allowed me to create a secure tunnel that safeguards the communication between the two networks by implementing encryption algorithms, such as AES which ensures that data remains confidential during transmission. In addition, I have understood the importance of this setup in which can be valuable to organizations that have multiple branch offices or remote locations that need to securely exchange sensitive information over public networks.