Practical No.: 8: Implementation of IPSec Site -to -Site VPNs

Aim: Implement IP Sec Site -to -Site VPNs

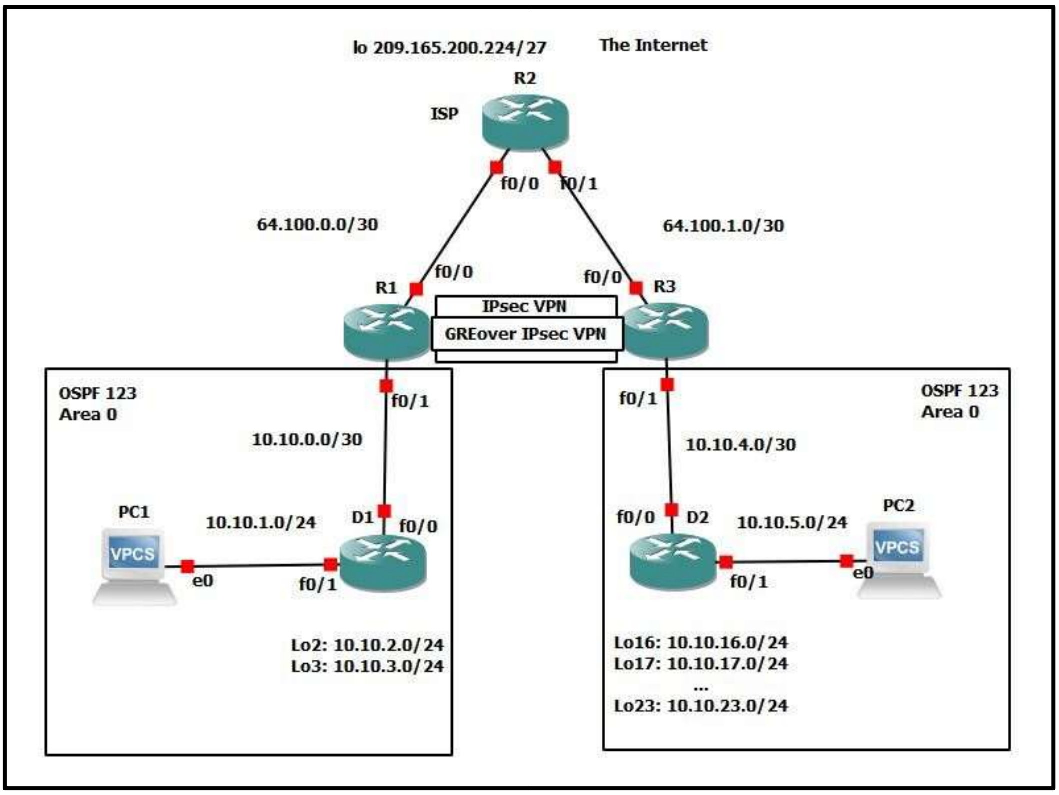
What is IP Sec VPN?

- IPsec is a set of protocols that work together to establish encrypted connections between devices. It contributes to the security of data sent over public networks. IPsec is a popular VPN protocol that works by encrypting IP packets and authenticating the source of the packets.

- Users can connect to an IPsec VPN by launching a VPN client application. This usually necessitates the user having the application installed on their device.

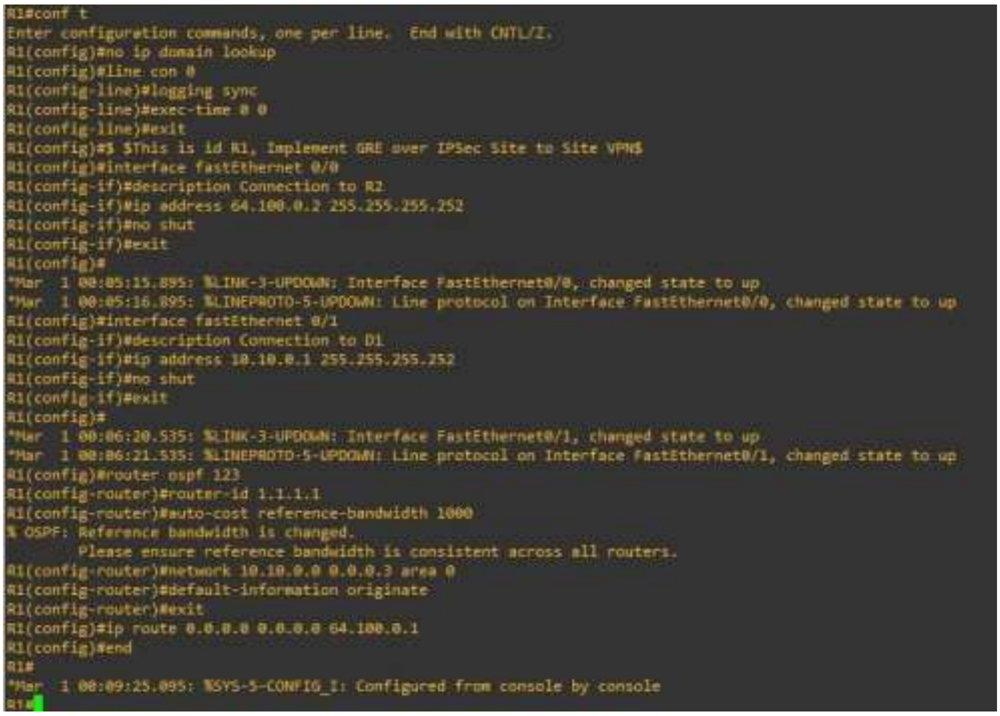
- VPN logins are usually password-based. While data sent over a VPN is encrypted, if user passwords are compromised, attackers can log into the VPN and steal this encrypted data. Using two-factor authentication (2FA) can strengthen IPsec VPN security, since stealing a password alone will no longer give an attacker access.

Step 1: Design the network topology.



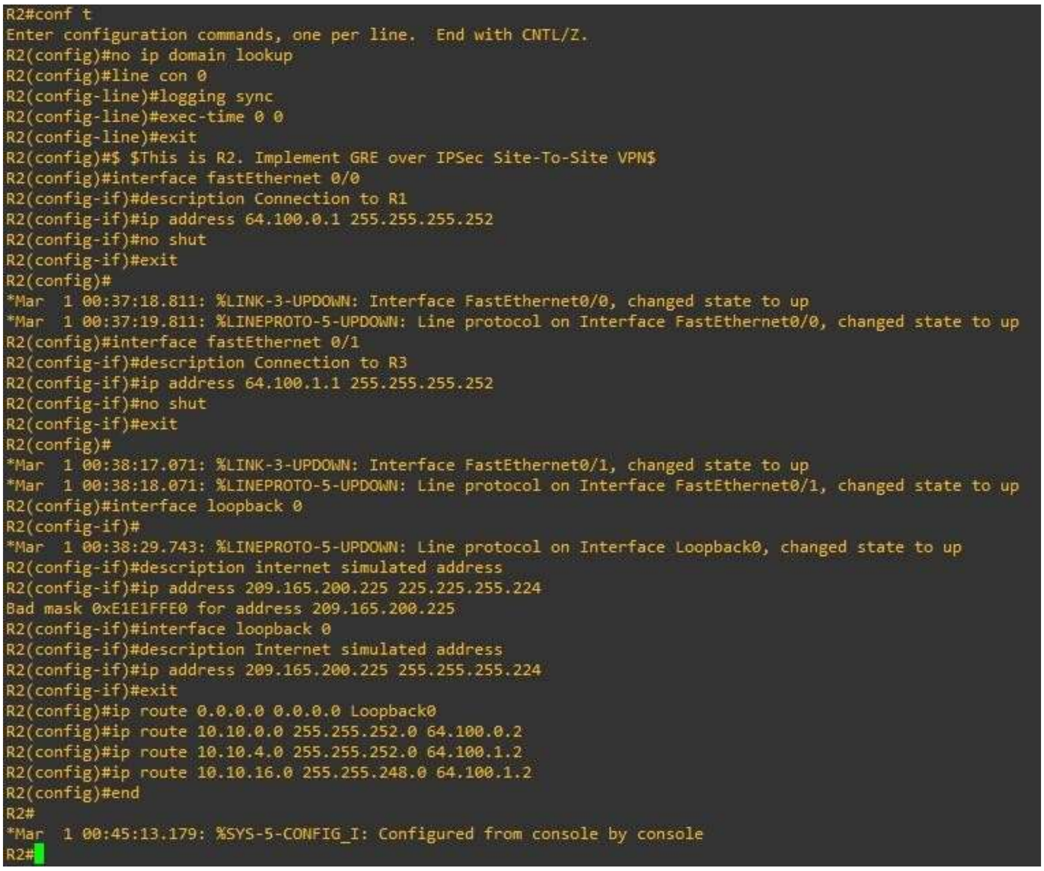
Step 2: Configure

Router 1 (R1):

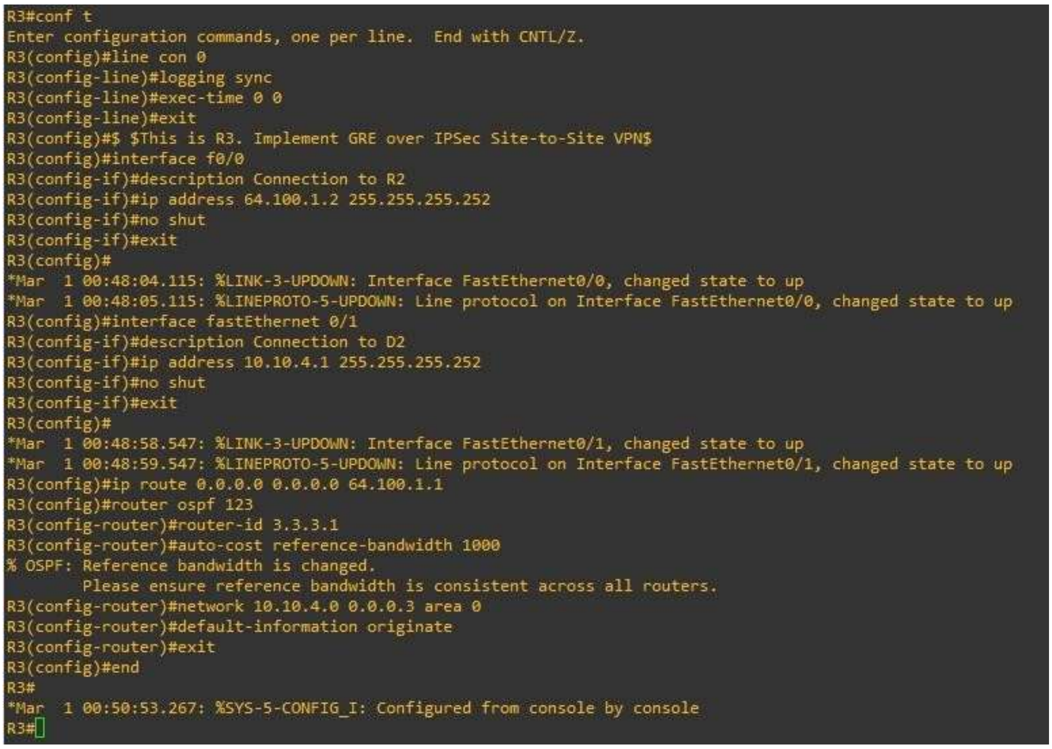


```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#no ip domain lookup
R1(config)#line con 0
R1(config-line)#logging sync
R1(config-line)#exec-time 0 0
R1(config-line)#exit
R1(config)#$ $This is id R1, Implement GRE over IPSec Site to Site VPN$
R1(config)#interface fastEthernet 0/0
R1(config-if)#description Connection to R2
R1(config-if)#ip address 64.100.0.2 255.255.255.252
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#
*Mar  1 00:05:15.895: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:05:16.895: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config)#interface fastEthernet 0/1
R1(config-if)#description Connection to D1
R1(config-if)#ip address 10.10.0.1 255.255.255.252
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#
*Mar  1 00:06:20.535: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:06:21.535: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R1(config)#router ospf 123
R1(config-router)#router-id 1.1.1.1
R1(config-router)#auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
R1(config-router)#network 10.10.0.0 0.0.0.3 area 0
R1(config-router)#default-information originate
R1(config-router)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 64.100.0.1
R1(config)#end
R1#
*Mar  1 00:09:25.095: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

Router 2 (R2):



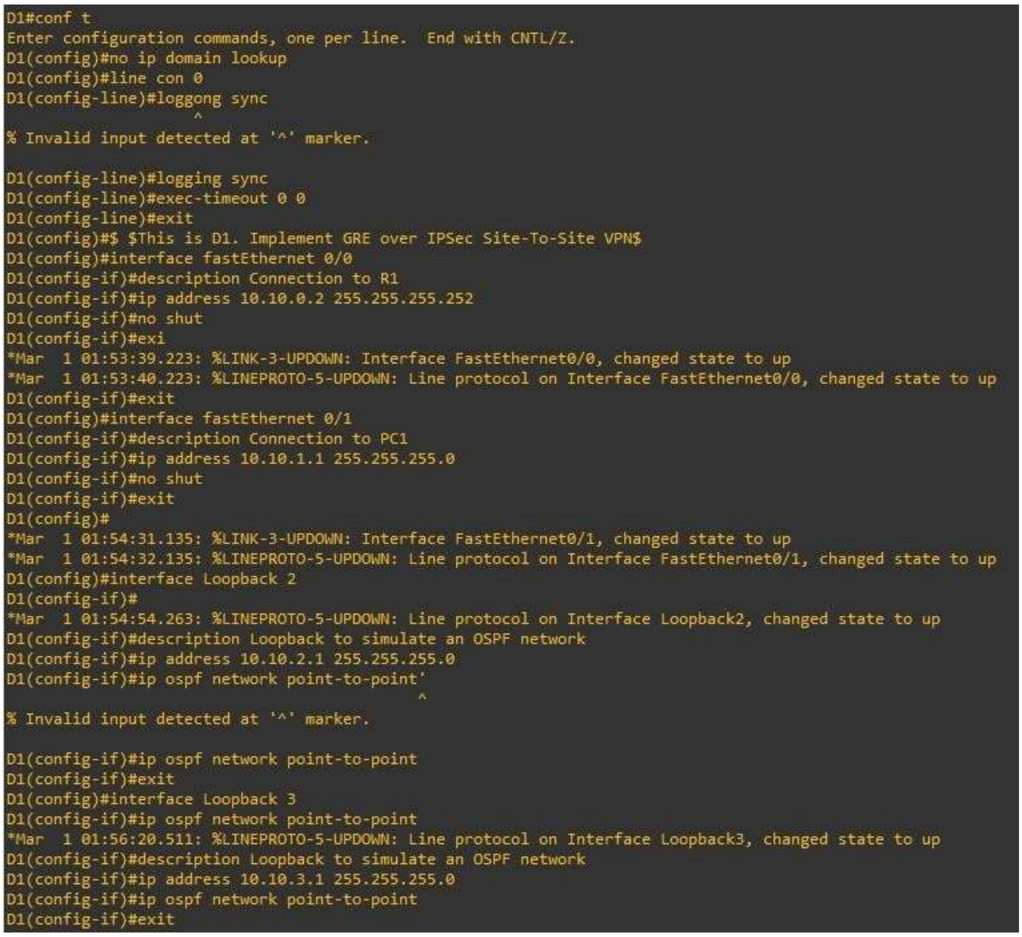
```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#no ip domain lookup
R2(config)#line con 0
R2(config-line)#logging sync
R2(config-line)#exec-time 0 0
R2(config-line)#exit
R2(config)#$ $This is R2. Implement GRE over IPSec Site-To-Site VPN$
R2(config)#interface fastEthernet 0/0
R2(config-if)#description Connection to R1
R2(config-if)#ip address 64.100.0.1 255.255.255.252
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#
*Mar  1 00:37:18.811: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:37:19.811: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R2(config)#interface fastEthernet 0/1
R2(config-if)#description Connection to R3
R2(config-if)#ip address 64.100.1.1 255.255.255.252
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#
*Mar  1 00:38:17.071: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:38:18.071: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R2(config)#interface loopback 0
R2(config-if)#
*Mar  1 00:38:29.743: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R2(config-if)#description internet simulated address
R2(config-if)#ip address 209.165.200.225 225.225.255.224
Bad mask 0xE1E1FFE0 for address 209.165.200.225
R2(config-if)#interface loopback 0
R2(config-if)#description Internet simulated address
R2(config-if)#ip address 209.165.200.225 255.255.255.224
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 Loopback0
R2(config)#ip route 10.10.0.0 255.255.252.0 64.100.0.2
R2(config)#ip route 10.10.4.0 255.255.252.0 64.100.1.2
R2(config)#ip route 10.10.16.0 255.255.248.0 64.100.1.2
R2(config)#end
R2#
*Mar  1 00:45:13.179: %SYS-5-CONFIG_I: Configured from console by console
R2#
```



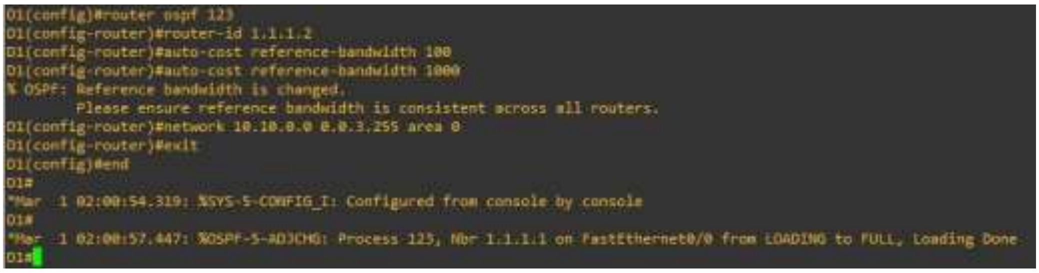
```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#line con 0
R3(config-line)#logging sync
R3(config-line)#exec-time 0 0
R3(config-line)#exit
R3(config)#$ $This is R3. Implement GRE over IPSec Site-to-Site VPN$
R3(config)#interface f0/0
R3(config-if)#description Connection to R2
R3(config-if)#ip address 64.100.1.2 255.255.255.252
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#
*Mar  1 00:48:04.115: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:48:05.115: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R3(config)#interface fastEthernet 0/1
R3(config-if)#description Connection to D2
R3(config-if)#ip address 10.10.4.1 255.255.255.252
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#
*Mar  1 00:48:58.547: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:48:59.547: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R3(config)#ip route 0.0.0.0 0.0.0.0 64.100.1.1
R3(config)#router ospf 123
R3(config-router)#router-id 3.3.3.1
R3(config-router)#auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
R3(config-router)#network 10.10.4.0 0.0.0.3 area 0
R3(config-router)#default-information originate
R3(config-router)#exit
R3(config)#end
R3#
*Mar  1 00:50:53.267: %SYS-5-CONFIG_I: Configured from console by console
R3#
```

Router 3 (R3):

Router 4 (D1):

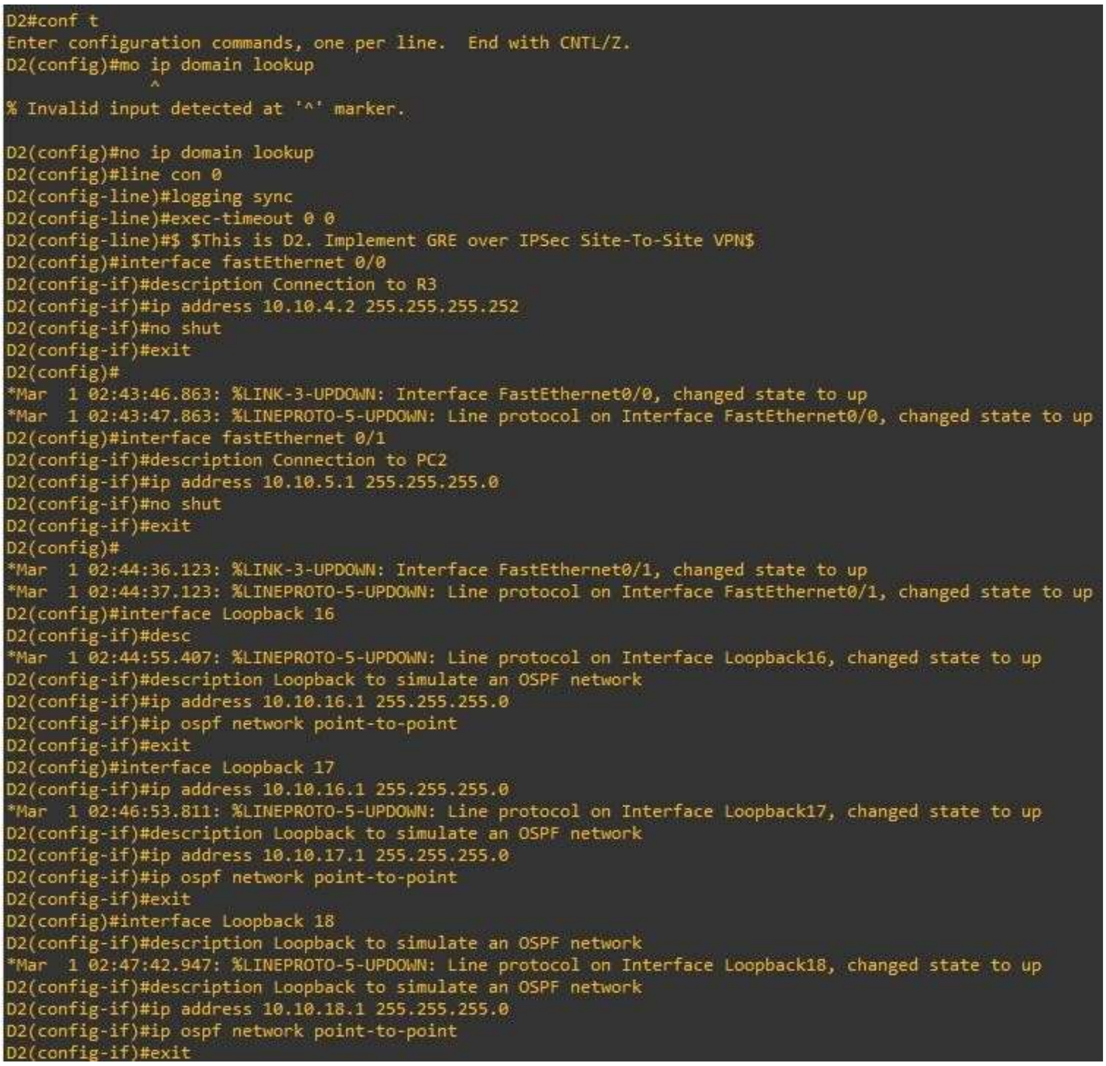


```
D1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)#no ip domain lookup
D1(config)#line con 0
D1(config-line)#loggong sync
                    ^
% Invalid input detected at '^' marker.

D1(config-line)#logging sync
D1(config-line)#exec-timeout 0 0
D1(config-line)#exit
D1(config)#$ $This is D1. Implement GRE over IPSec Site-To-Site VPN$
D1(config)#interface fastEthernet 0/0
D1(config-if)#description Connection to R1
D1(config-if)#ip address 10.10.0.2 255.255.255.252
D1(config-if)#no shut
D1(config-if)#exi
*Mar  1 01:53:39.223: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 01:53:40.223: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
D1(config-if)#exit
D1(config)#interface fastEthernet 0/1
D1(config-if)#description Connection to PC1
D1(config-if)#ip address 10.10.1.1 255.255.255.0
D1(config-if)#no shut
D1(config-if)#exit
D1(config)#
*Mar  1 01:54:31.135: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 01:54:32.135: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
D1(config)#interface Loopback 2
D1(config-if)#
*Mar  1 01:54:54.263: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback2, changed state to up
D1(config-if)#description Loopback to simulate an OSPF network
D1(config-if)#ip address 10.10.2.1 255.255.255.0
D1(config-if)#ip ospf network point-to-point'
                                            ^
% Invalid input detected at '^' marker.

D1(config-if)#ip ospf network point-to-point
D1(config-if)#exit
D1(config)#interface Loopback 3
D1(config-if)#ip ospf network point-to-point
*Mar  1 01:56:20.511: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback3, changed state to up
D1(config-if)#description Loopback to simulate an OSPF network
D1(config-if)#ip address 10.10.3.1 255.255.255.0
D1(config-if)#ip ospf network point-to-point
D1(config-if)#exit
```

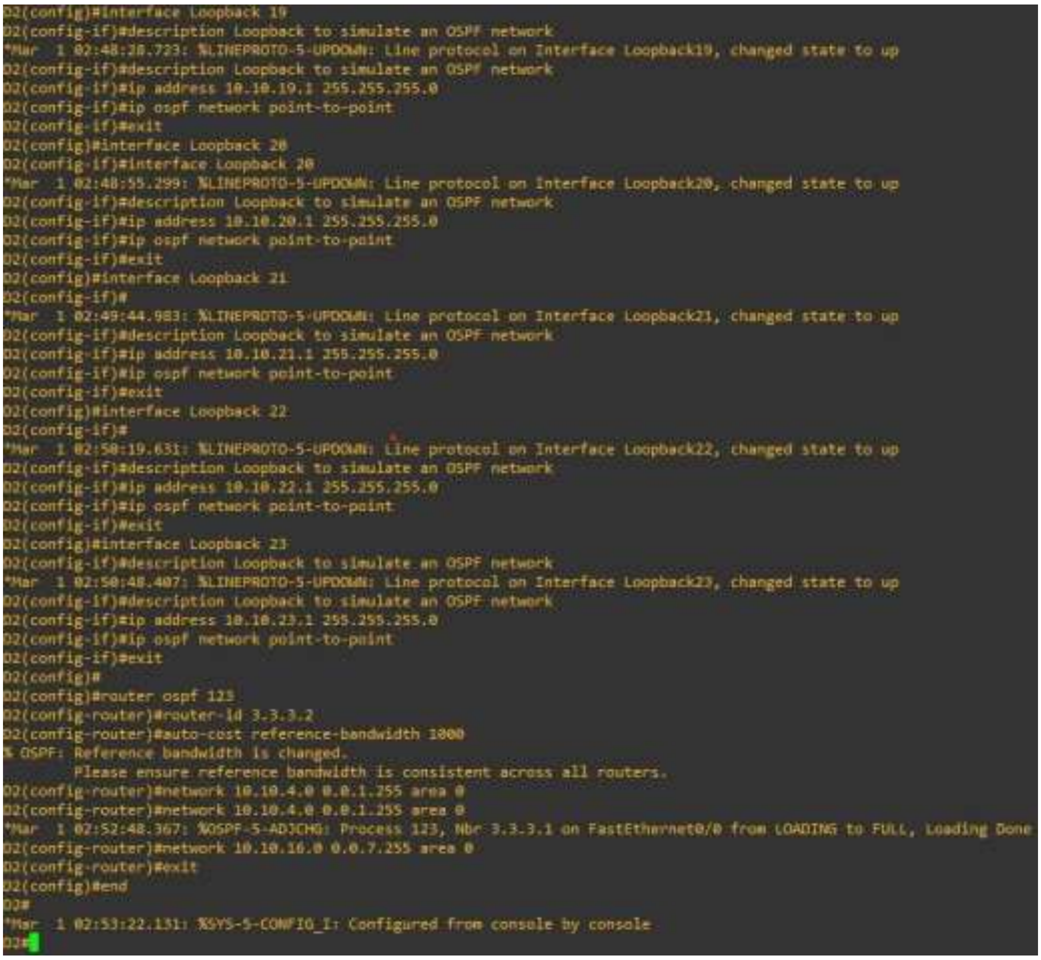


```
D1(config)#router ospf 123
D1(config-router)#router-id 1.1.1.2
D1(config-router)#auto-cost reference-bandwidth 100
D1(config-router)#auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
D1(config-router)#network 10.10.0.0 0.0.3.255 area 0
D1(config-router)#exit
D1(config)#end
D1#
*Mar  1 02:00:54.319: %SYS-5-CONFIG_I: Configured from console by console
D1#
*Mar  1 02:00:57.447: %OSPF-5-ADJCHG: Process 123, Nbr 1.1.1.1 on FastEthernet0/0 from LOADING to FULL, Loading Done
D1#
```

Router 5 (D2):

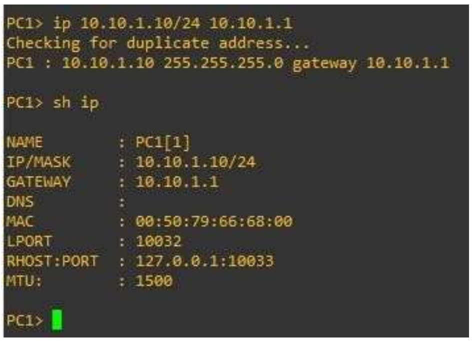


```
D2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
D2(config)#mo ip domain lookup
              ^
% Invalid input detected at '^' marker.

D2(config)#no ip domain lookup
D2(config)#line con 0
D2(config-line)#logging sync
D2(config-line)#exec-timeout 0 0
D2(config-line)#$ $This is D2. Implement GRE over IPSec Site-To-Site VPN$
D2(config)#interface fastEthernet 0/0
D2(config-if)#description Connection to R3
D2(config-if)#ip address 10.10.4.2 255.255.255.252
D2(config-if)#no shut
D2(config-if)#exit
D2(config)#
*Mar  1 02:43:46.863: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 02:43:47.863: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
D2(config)#interface fastEthernet 0/1
D2(config-if)#description Connection to PC2
D2(config-if)#ip address 10.10.5.1 255.255.255.0
D2(config-if)#no shut
D2(config-if)#exit
D2(config)#
*Mar  1 02:44:36.123: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 02:44:37.123: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
D2(config)#interface Loopback 16
D2(config-if)#desc
*Mar  1 02:44:55.407: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback16, changed state to up
D2(config-if)#description Loopback to simulate an OSPF network
D2(config-if)#ip address 10.10.16.1 255.255.255.0
D2(config-if)#ip ospf network point-to-point
D2(config-if)#exit
D2(config)#interface Loopback 17
D2(config-if)#ip address 10.10.16.1 255.255.255.0
*Mar  1 02:46:53.811: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback17, changed state to up
D2(config-if)#description Loopback to simulate an OSPF network
D2(config-if)#ip address 10.10.17.1 255.255.255.0
D2(config-if)#ip ospf network point-to-point
D2(config-if)#exit
D2(config)#interface Loopback 18
D2(config-if)#description Loopback to simulate an OSPF network
*Mar  1 02:47:42.947: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback18, changed state to up
D2(config-if)#description Loopback to simulate an OSPF network
D2(config-if)#ip address 10.10.18.1 255.255.255.0
D2(config-if)#ip ospf network point-to-point
D2(config-if)#exit
```



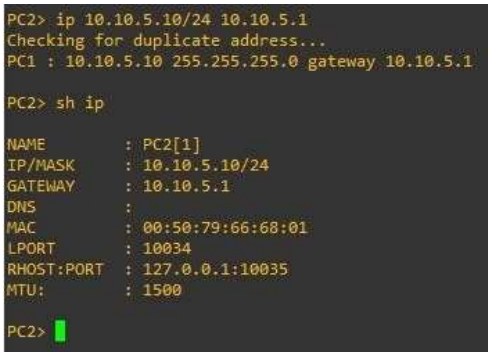
```
D2(config)#interface Loopback 19
D2(config-if)#description Loopback to simulate an OSPF network
*Mar  1 02:48:28.723: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback19, changed state to up
D2(config-if)#description Loopback to simulate an OSPF network
D2(config-if)#ip address 10.10.19.1 255.255.255.0
D2(config-if)#ip ospf network point-to-point
D2(config-if)#exit
D2(config)#interface Loopback 20
D2(config-if)#interface Loopback 20
*Mar  1 02:48:55.299: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback20, changed state to up
D2(config-if)#description Loopback to simulate an OSPF network
D2(config-if)#ip address 10.10.20.1 255.255.255.0
D2(config-if)#ip ospf network point-to-point
D2(config-if)#exit
D2(config)#interface Loopback 21
D2(config-if)#
*Mar  1 02:49:44.983: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback21, changed state to up
D2(config-if)#description Loopback to simulate an OSPF network
D2(config-if)#ip address 10.10.21.1 255.255.255.0
D2(config-if)#ip ospf network point-to-point
D2(config-if)#exit
D2(config)#interface Loopback 22
D2(config-if)#
*Mar  1 02:50:19.631: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback22, changed state to up
D2(config-if)#description Loopback to simulate an OSPF network
D2(config-if)#ip address 10.10.22.1 255.255.255.0
D2(config-if)#ip ospf network point-to-point
D2(config-if)#exit
D2(config)#interface Loopback 23
D2(config-if)#description Loopback to simulate an OSPF network
*Mar  1 02:50:48.407: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback23, changed state to up
D2(config-if)#description Loopback to simulate an OSPF network
D2(config-if)#ip address 10.10.23.1 255.255.255.0
D2(config-if)#ip ospf network point-to-point
D2(config-if)#exit
D2(config)#
D2(config)#router ospf 123
D2(config-router)#router-id 3.3.3.2
D2(config-router)#auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
D2(config-router)#network 10.10.4.0 0.0.1.255 area 0
D2(config-router)#network 10.10.4.0 0.0.1.255 area 0
*Mar  1 02:52:48.367: %OSPF-5-ADJCHG: Process 123, Nbr 3.3.3.1 on FastEthernet0/0 from LOADING to FULL, Loading Done
D2(config-router)#network 10.10.16.0 0.0.7.255 area 0
D2(config-router)#exit
D2(config)#end
D2#
*Mar  1 02:53:22.131: %SYS-5-CONFIG_I: Configured from console by console
D2#
```

PC 1:



```
PC1> ip 10.10.1.10/24 10.10.1.1
Checking for duplicate address...
PC1 : 10.10.1.10 255.255.255.0 gateway 10.10.1.1

PC1> sh ip

NAME        : PC1[1]
IP/MASK     : 10.10.1.10/24
GATEWAY     : 10.10.1.1
DNS         :
MAC         : 00:50:79:66:68:00
LPORT       : 10032
RHOST:PORT  : 127.0.0.1:10033
MTU:        : 1500

PC1>
```

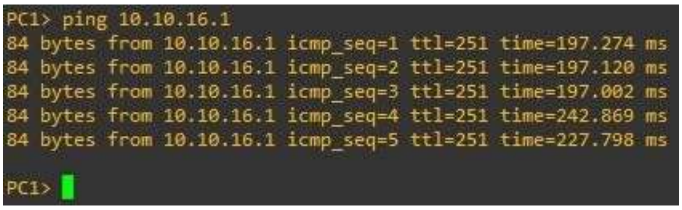
PC 2:



```
PC2> ip 10.10.5.10/24 10.10.5.1
Checking for duplicate address...
PC1 : 10.10.5.10 255.255.255.0 gateway 10.10.5.1

PC2> sh ip

NAME        : PC2[1]
IP/MASK     : 10.10.5.10/24
GATEWAY     : 10.10.5.1
DNS         :
MAC         : 00:50:79:66:68:01
LPORT       : 10034
RHOST:PORT  : 127.0.0.1:10035
MTU:        : 1500

PC2>
```

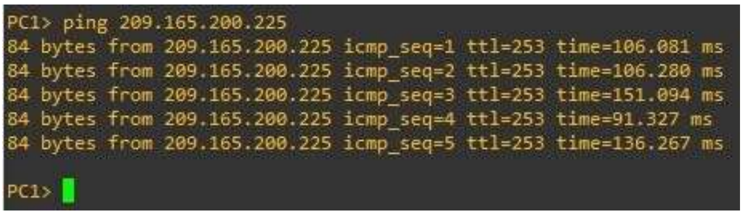
Step 3: On PC1, verify end-to-end connectivity.

From PC1, ping the first loopback on D3 (10.10.16.1).



```
PC1> ping 10.10.16.1
84 bytes from 10.10.16.1 icmp_seq=1 ttl=251 time=197.274 ms
84 bytes from 10.10.16.1 icmp_seq=2 ttl=251 time=197.120 ms
84 bytes from 10.10.16.1 icmp_seq=3 ttl=251 time=197.002 ms
84 bytes from 10.10.16.1 icmp_seq=4 ttl=251 time=242.869 ms
84 bytes from 10.10.16.1 icmp_seq=5 ttl=251 time=227.798 ms

PC1>
```

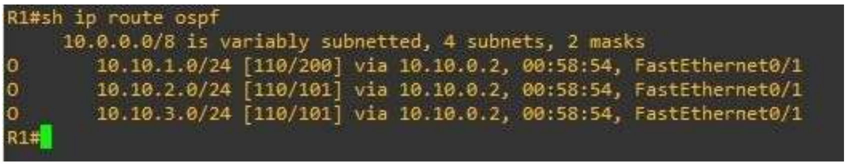
Finally, from PC1, ping the default gateway loopback on R2 (209.165.200.225).



```
PC1> ping 209.165.200.225
84 bytes from 209.165.200.225 icmp_seq=1 ttl=253 time=106.081 ms
84 bytes from 209.165.200.225 icmp_seq=2 ttl=253 time=106.280 ms
84 bytes from 209.165.200.225 icmp_seq=3 ttl=253 time=151.094 ms
84 bytes from 209.165.200.225 icmp_seq=4 ttl=253 time=91.327 ms
84 bytes from 209.165.200.225 icmp_seq=5 ttl=253 time=136.267 ms

PC1>
```

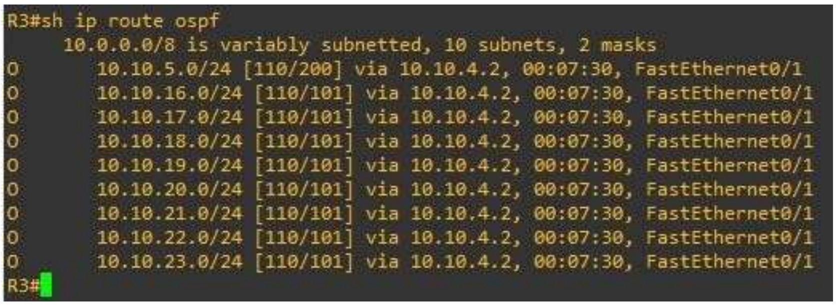
Step 4: Verify the routing table of R1 and R3.

Verify the OSPF routing table of R1.



```
R1#sh ip route ospf
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O       10.10.1.0/24 [110/200] via 10.10.0.2, 00:58:54, FastEthernet0/1
O       10.10.2.0/24 [110/101] via 10.10.0.2, 00:58:54, FastEthernet0/1
O       10.10.3.0/24 [110/101] via 10.10.0.2, 00:58:54, FastEthernet0/1
R1#
```

Verify the routing table of R3.



```
R3#sh ip route ospf
     10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
O       10.10.5.0/24 [110/200] via 10.10.4.2, 00:07:30, FastEthernet0/1
O       10.10.16.0/24 [110/101] via 10.10.4.2, 00:07:30, FastEthernet0/1
O       10.10.17.0/24 [110/101] via 10.10.4.2, 00:07:30, FastEthernet0/1
O       10.10.18.0/24 [110/101] via 10.10.4.2, 00:07:30, FastEthernet0/1
O       10.10.19.0/24 [110/101] via 10.10.4.2, 00:07:30, FastEthernet0/1
O       10.10.20.0/24 [110/101] via 10.10.4.2, 00:07:30, FastEthernet0/1
O       10.10.21.0/24 [110/101] via 10.10.4.2, 00:07:30, FastEthernet0/1
O       10.10.22.0/24 [110/101] via 10.10.4.2, 00:07:30, FastEthernet0/1
O       10.10.23.0/24 [110/101] via 10.10.4.2, 00:07:30, FastEthernet0/1
R3#
```

Step 5: Configure GRE over IPsec using a Crypto Map on R1.

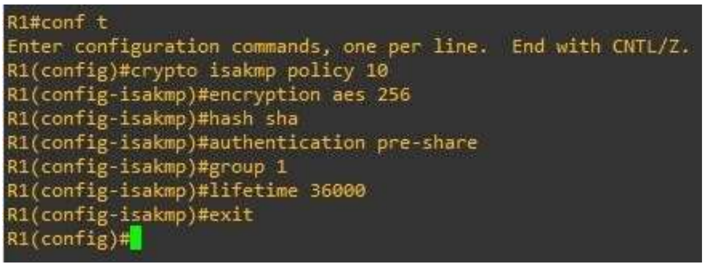
- **On R1, configure the ISAKMP policy and pre-shared key.**

Like site-to-site VPNs using crypto maps, GRE over IPsec also requires an ISAKMP policy configuration and pre-shared key configured.

In this lab, we will use the following parameters for the ISAKMP policy 10 on R1:

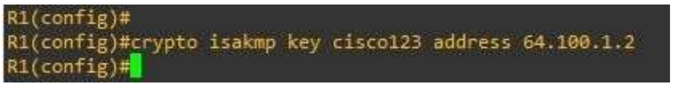
- Encryption: aes 256
- Hash: sha256
- Authentication method: pre-share key
- Diffie-Hellman group: 14 o Lifetime: 3600 seconds
  (60 minutes / 1 hour)

Configure ISAKMP policy 10 on R1:



```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#hash sha
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 1
R1(config-isakmp)#lifetime 36000
R1(config-isakmp)#exit
R1(config)#
```

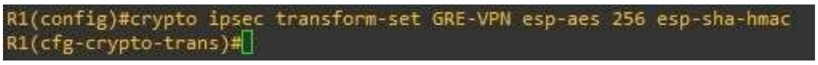
Configure the pre-shared key of cisco123 on R1. This command points to the remote peer R3 G0/0/0 IP address.



```
R1(config)#
R1(config)#crypto isakmp key cisco123 address 64.100.1.2
R1(config)#
```

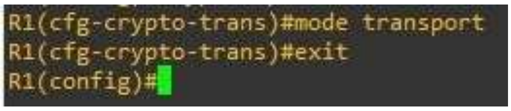
- **On R1, configure the transform set and VPN ACL.**

Create a transform set called GRE-VPN using AES 256 cipher with ESP and the SHA 256 hash function.



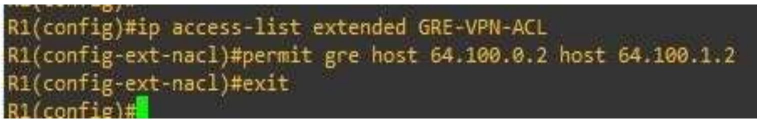
```
R1(config)#crypto ipsec transform-set GRE-VPN esp-aes 256 esp-sha-hmac
R1(cfg-crypto-trans)#
```

Unlike a site-to-site IPsec VPN, the transform must use transport mode. The mode command is used to identify the type of tunnel that will be established. The default is mode tunnel mode. However, GRE over IPsec should be configured using the mode transport command.



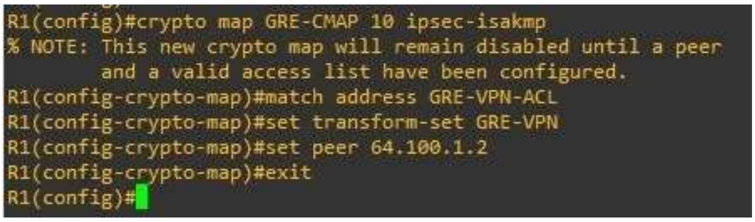
```
R1(cfg-crypto-trans)#mode transport
R1(cfg-crypto-trans)#exit
R1(config)#
```

Next, create a named extended ACL called GRE-VPN-ACL that makes the tunnel interface traffic interesting.



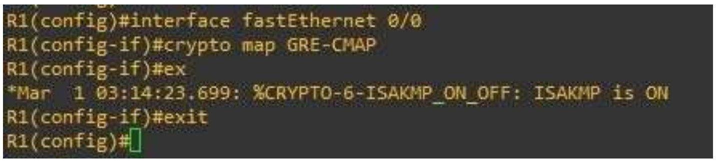
```
R1(config)#ip access-list extended GRE-VPN-ACL
R1(config-ext-nacl)#permit gre host 64.100.0.2 host 64.100.1.2
R1(config-ext-nacl)#exit
R1(config)#
```

- **On R1, configure the crypto map and apply it to the interface.**
  Create a crypto map called GRE-CMAP that associates the new GRE-VPN-ACL, transform set, and peer.



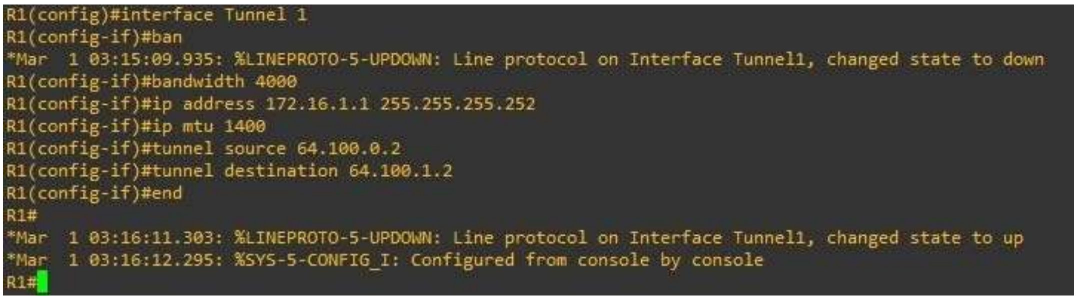
```
R1(config)#crypto map GRE-CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#match address GRE-VPN-ACL
R1(config-crypto-map)#set transform-set GRE-VPN
R1(config-crypto-map)#set peer 64.100.1.2
R1(config-crypto-map)#exit
R1(config)#
```

Finally, assign a crypto map called GRE-MAP on G0/0/0



```
R1(config)#interface fastEthernet 0/0
R1(config-if)#crypto map GRE-CMAP
R1(config-if)#ex
*Mar  1 03:14:23.699: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#exit
R1(config)#
```

- **On R1, configure the GRE tunnel interface.**
  Configure a GRE tunnel interface as shown. To enable GRE on the tunnel interface, the tunnel mode gre ipv4 command is required. However, this command is enabled by default and will therefore not be configured in our example.



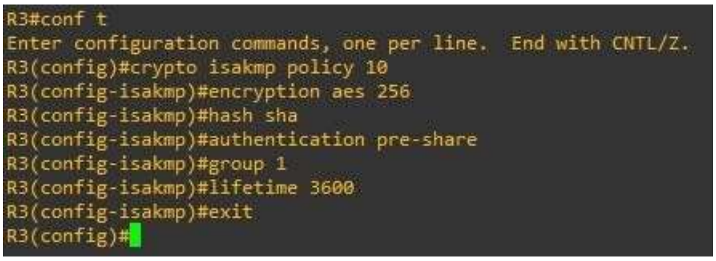
```
R1(config)#interface Tunnel 1
R1(config-if)#ban
*Mar  1 03:15:09.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
R1(config-if)#bandwidth 4000
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#ip mtu 1400
R1(config-if)#tunnel source 64.100.0.2
R1(config-if)#tunnel destination 64.100.1.2
R1(config-if)#end
R1#
*Mar  1 03:16:11.303: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
*Mar  1 03:16:12.295: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

Step 6: Configure GRE over IPsec using a Tunnel IPsec Profile on R3.

In this part, we will configure GRE over IPsec using tunnel IPsec profiles on R3.

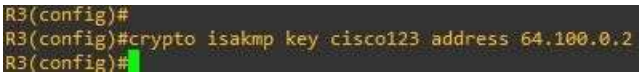
- **On R3, configure the ISAKMP policy, pre-shared key, and transform set.**
  In this step, we will configure the same parameters for the ISAKMP policy 10 that we configured on R1.

Configure ISAKMP policy 10 on R3:



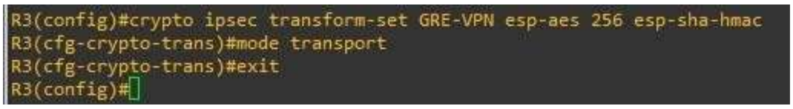
```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#hash sha
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 1
R3(config-isakmp)#lifetime 3600
R3(config-isakmp)#exit
R3(config)#
```

Configure the pre-shared key of cisco123 on R1. This command points to the remote peer R3 G0/0/0 IP address.



```
R3(config)#
R3(config)#crypto isakmp key cisco123 address 64.100.0.2
R3(config)#
```

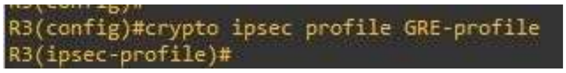
Create a new transform set called GRE-VPN using the same security parameters and transport mode that we configured on R1. Also configure the mode transport command.



```
R3(config)#crypto ipsec transform-set GRE-VPN esp-aes 256 esp-sha-hmac
R3(cfg-crypto-trans)#mode transport
R3(cfg-crypto-trans)#exit
R3(config)#
```

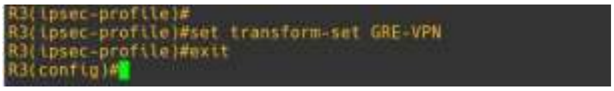
- **On R3, configure the IPsec profile.**

Instead of a crypto map, we will configure an IPsec profile called GRE-PROFILE using the crypto ipsec profile ipsec-profile-name global configuration command.



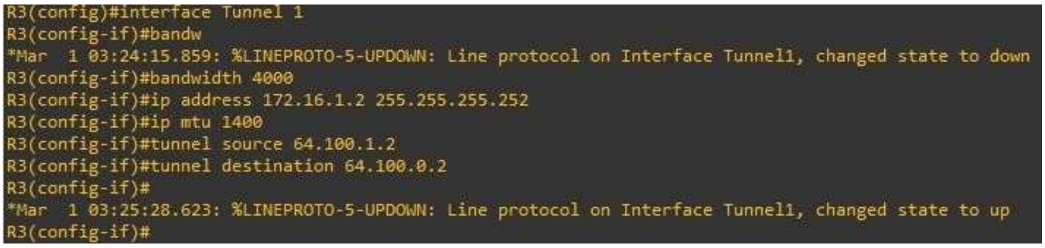
```
R3(config)#
R3(config)#crypto ipsec profile GRE-profile
R3(ipsec-profile)#
```

In IPsec profile configuration mode, specify the transform set to be negotiated using the set transform-set transform-set-name command. Multiple transform sets can be specified in order of priority. The fist transform-set-name specified is the highest priority.



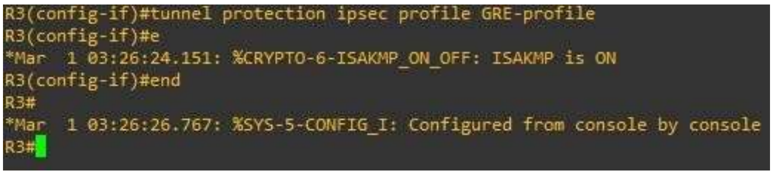
```
R3(ipsec-profile)#
R3(ipsec-profile)#set transform-set GRE-VPN
R3(ipsec-profile)#exit
R3(config)#
```

- **On R3, configure the tunnel interface.** On R3, configure a GRE tunnel interface.



```
R3(config)#interface Tunnel 1
R3(config-if)#bandw
*Mar  1 03:24:15.859: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
R3(config-if)#bandwidth 4000
R3(config-if)#ip address 172.16.1.2 255.255.255.252
R3(config-if)#ip mtu 1400
R3(config-if)#tunnel source 64.100.1.2
R3(config-if)#tunnel destination 64.100.0.2
R3(config-if)#
*Mar  1 03:25:28.623: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
R3(config-if)#
```

Apply the IPsec profile GRE-PROFILE to the Tunnel 1 interface using the tunnel protection ipsec profile profile-name command.



```
R3(config-if)#tunnel protection ipsec profile GRE-profile
R3(config-if)#e
*Mar  1 03:26:24.151: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#end
R3#
*Mar  1 03:26:26.767: %SYS-5-CONFIG_I: Configured from console by console
R3#
```

- **On R1 and R3, enable OSPF routing on the tunnel interface.**