IP Security (IPSec) Configuration

Aim: To Configure IPSec on network devices to provide secure communication and protect against unauthorized access and attacks.

Theory:

Some theoretical aspects of IPSec and the concept of an IPSec VPN tunnel:

1. IPSec Overview:
   - IPSec (Internet Protocol Security) is a comprehensive suite of protocols and standards used for securing communication over IP networks, such as the Internet.
   - It ensures the confidentiality, integrity, and authenticity of data transmitted between devices or networks.

2. Security Goals of IPSec:
   - Confidentiality: IPSec achieves data privacy through encryption.
   - Integrity: It guarantees that data remains unaltered during transit.
   - Authentication: IPSec verifies the identity of communicating parties to prevent unauthorized access and impersonation.

3. Components of IPSec:
   - IPSec comprises multiple protocols and elements, including Authentication Header (AH), Encapsulating Security Payload (ESP), Security Associations (SAs), and key management protocols.

4. IPSec VPN Tunnel:
   - An IPSec VPN tunnel is a secure, encrypted connection established between two endpoints or networks over the Internet or untrusted networks.
   - It is created using the IPSec suite to provide a secure and private channel for data transmission.

5. Establishing a VPN Tunnel:
   - The process begins with the negotiation and establishment of Security Associations (SAs) between the endpoints.
   - These SAs define parameters like encryption methods, authentication, and shared keys.

6. Modes of Operation:
   - VPN tunnels can operate in either Transport Mode (securing data payload) or Tunnel Mode (securing entire IP packets, including headers).
   - Transport Mode is often used for host-to-host communication, while Tunnel Mode is suitable for network-to-network connections.

7. Data Encryption and Authentication:
   - Data transmitted through the VPN tunnel is encrypted using algorithms specified in the SAs, ensuring data privacy.
   - Authentication and data integrity checks prevent tampering or unauthorized access.

8. Routing and Secure Communication:
   - Once established, the VPN tunnel allows secure data routing between the endpoints or networks.

- Applications and services on either side can communicate securely, even over untrusted networks like the Internet.

9. Use Cases:
- IPSec VPN tunnels are used for various purposes, including remote access VPNs, site-to-site VPNs, secure data transfer, and protecting real-time communication like VoIP and video conferencing.

10. Key Management:
- Secure key management is critical for the long-term security of IPSec VPN tunnels.
- Keys can be generated manually or through automated key exchange protocols like Internet Key Exchange (IKE).

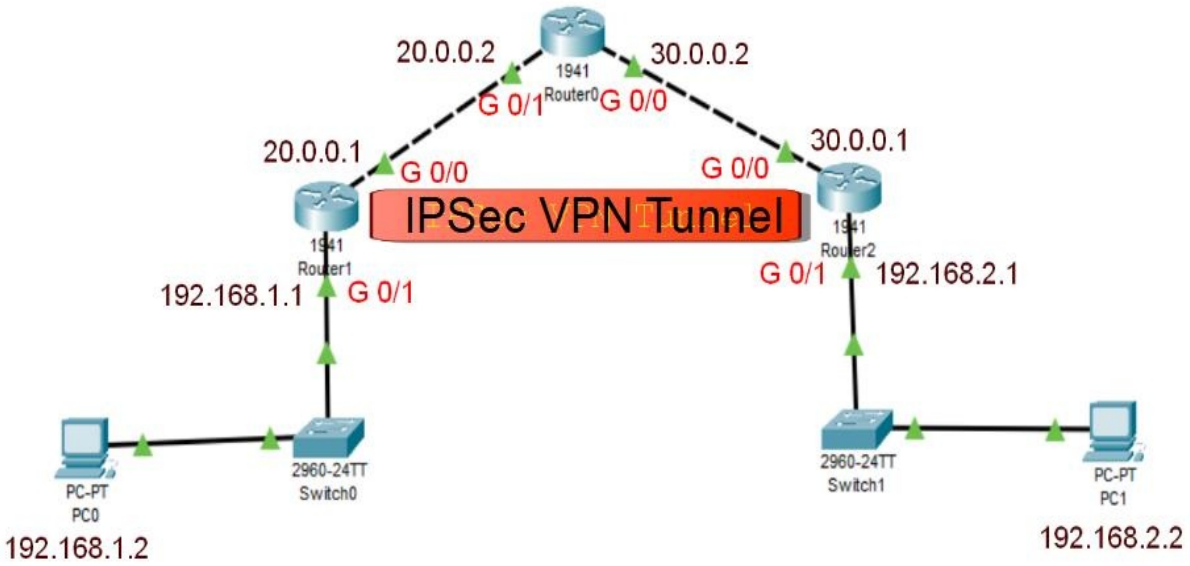
11. Security Policies:
- Organizations define security policies that determine when and how IPSec should be applied to protect specific types of traffic or communication.

12. Interoperability:
- IPSec is widely adopted, ensuring interoperability between different vendors' equipment and making it a versatile choice for securing networks and data.

Understanding the principles of IPSec and IPSec VPN tunnels is essential for designing, deploying, and managing secure communication in various network environments, ensuring data remains confidential, unaltered, and protected from unauthorized access.

Topology:

We use the following topology for the present case



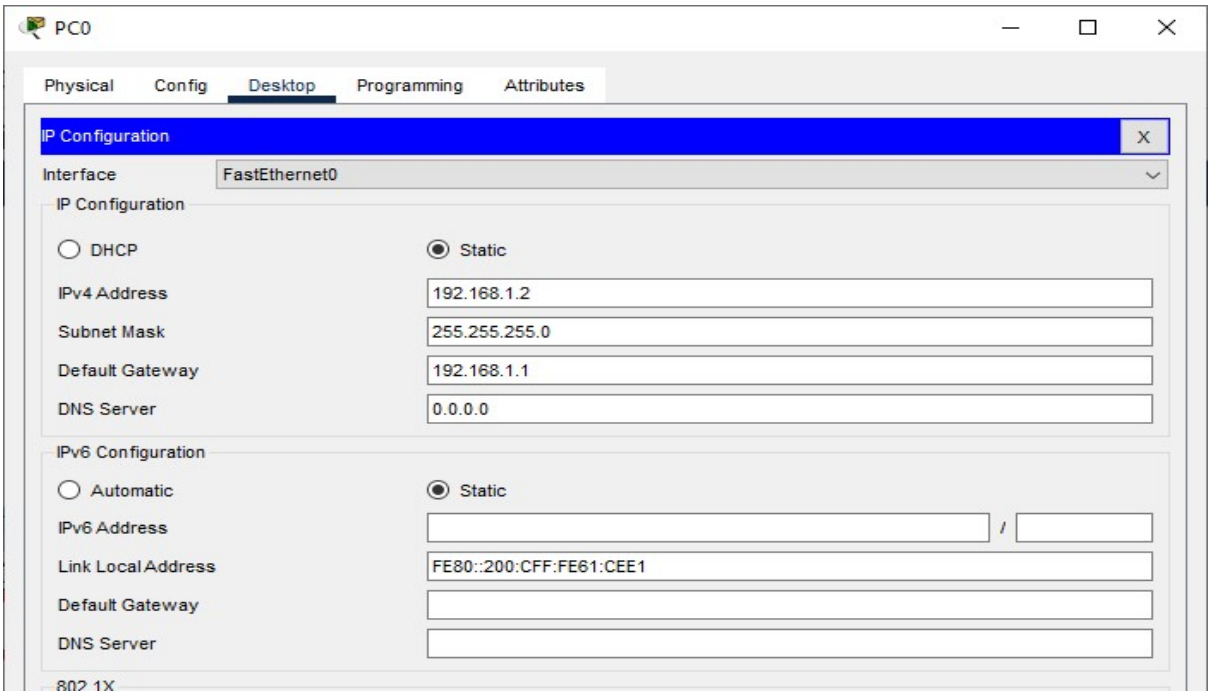
ISAKMP Policy Parameters

Parameters	Parameter Options and Defaults	R1	R2
Key Distribution Method	Manual or ISAKMP	ISAKMP	ISAKMP
Encryption Algorithm	DES. 3DES or AES	AES-256	AES-256
Hash Algorithm	MD5 or SHA-1	SHA-1	SHA-1
Authentication Method	Pre-shared Key or RSA	Pre-shared	Pre-shared
Key Exchange	DH Group 1, 2 or 5	Group 5	Group 5
ISE SA Lifetime	86400 seconds or less	86400	86400
ISAKMP Key	User defined	ismile	ismile

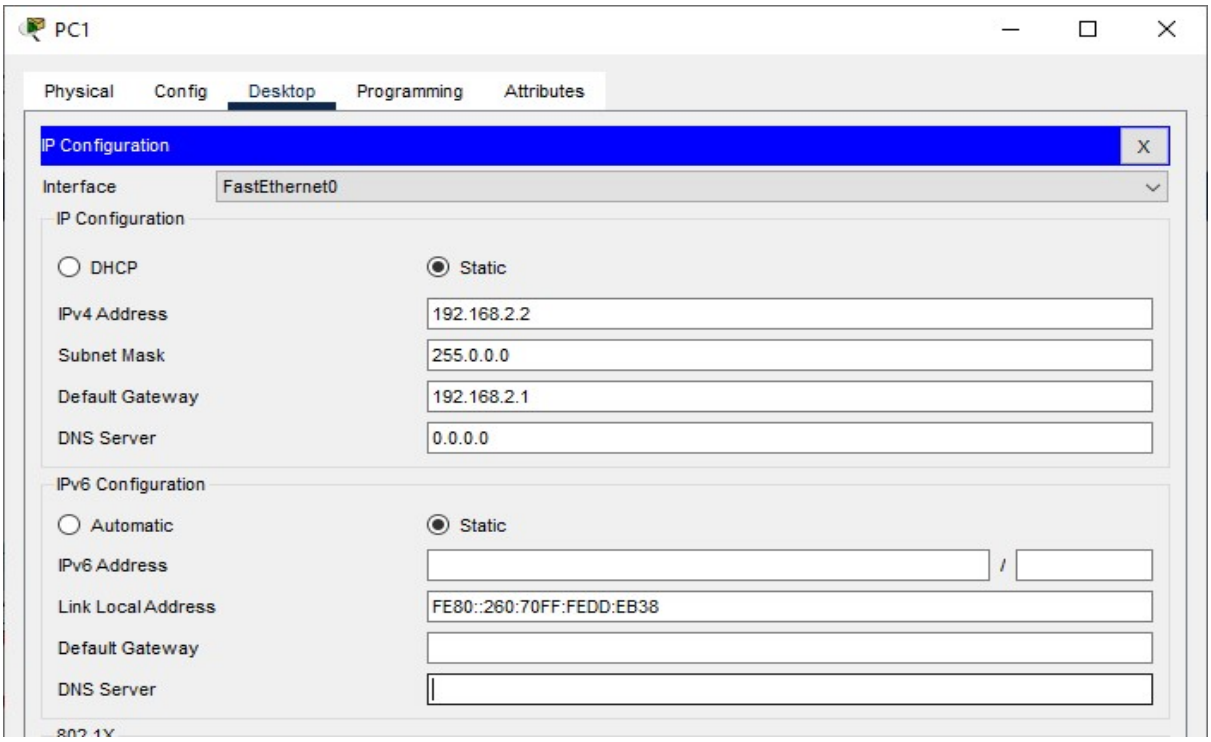
IPSec Policy Parameters

Parameters	R1	R2
Transform Set Name	VPN-SET	VPN-SET
ESP Transform Encryption	esp-aes	esp-aes
ESP Transform Authentication	esp-sha-hmac	esp-sha-hmac
Peer IP Address	30.0.0.1	20.0.0.1
Traffic to be Encrypted	R1->R2	R2->R1
Crypto Map Name	IPSEC-MAP	IPSEC-MAP
SA Establishment	ipsec-isakmp	ipsec-isakmp

Configuring PC0:

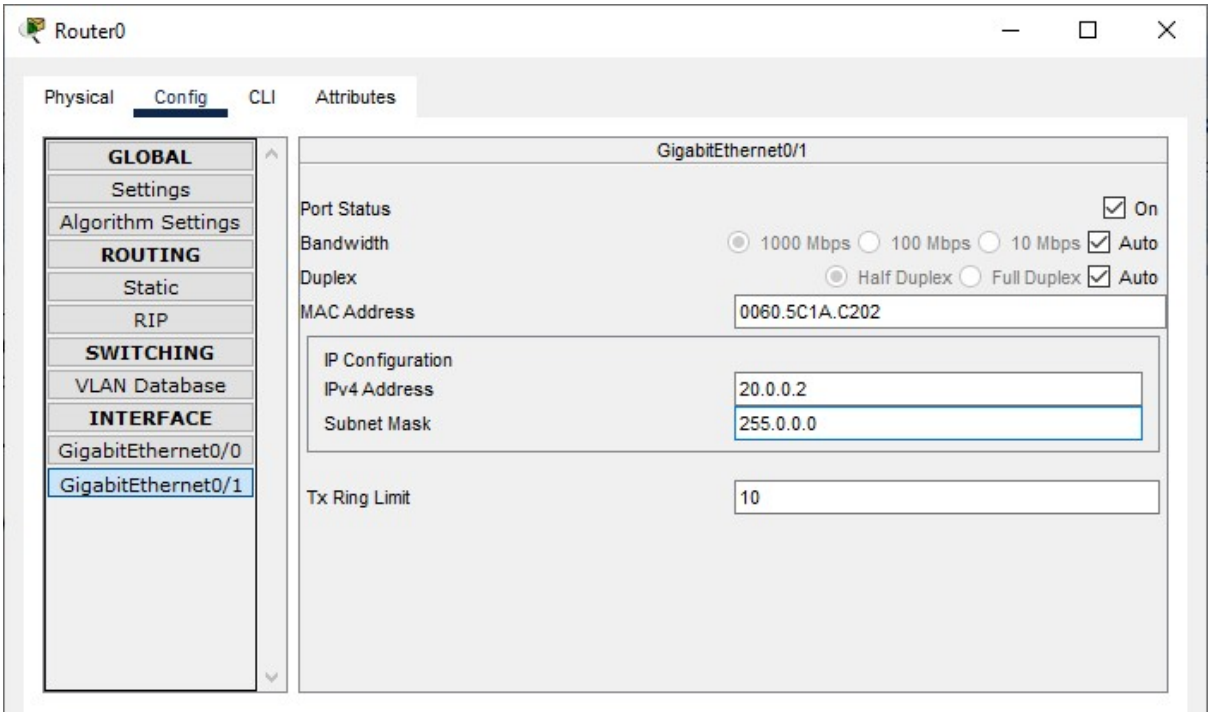


Configuring PC1:

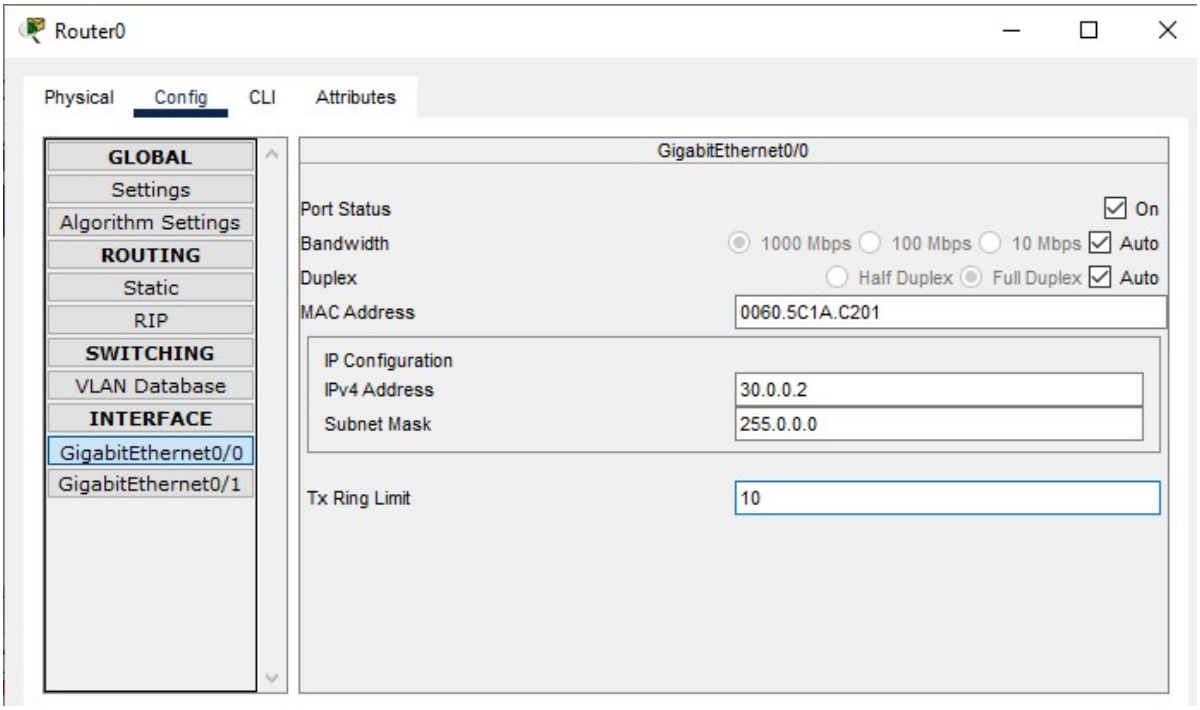


Configuring Router0:

Interface GigabitEthernet0/1:

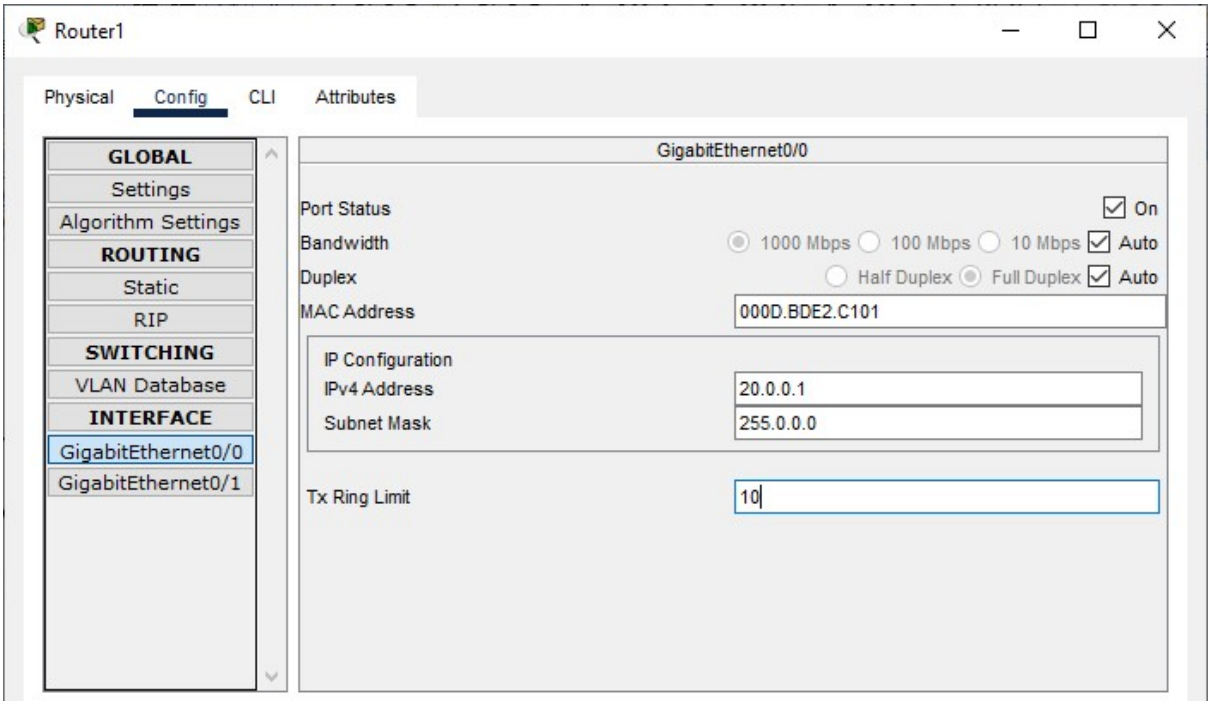


Interface GigabitEthernet0/0:

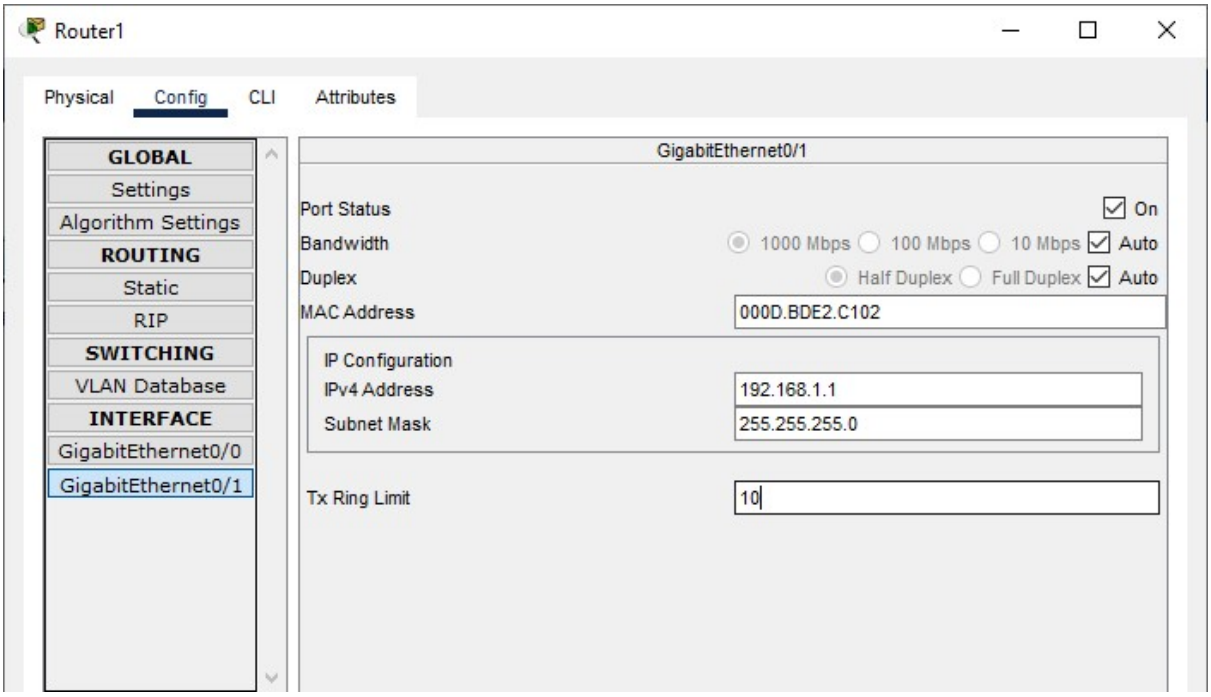


Configuring Router1:

Interface GigabitEthernet0/0:

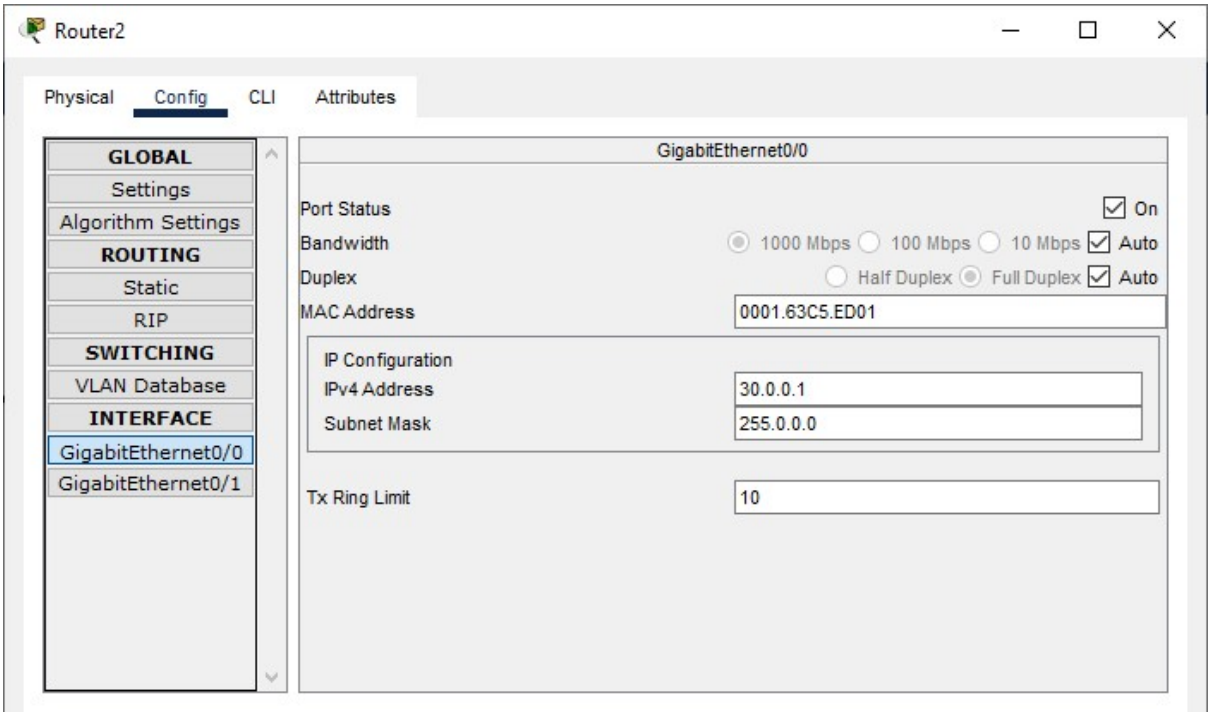


Interface GigabitEthernet0/1:

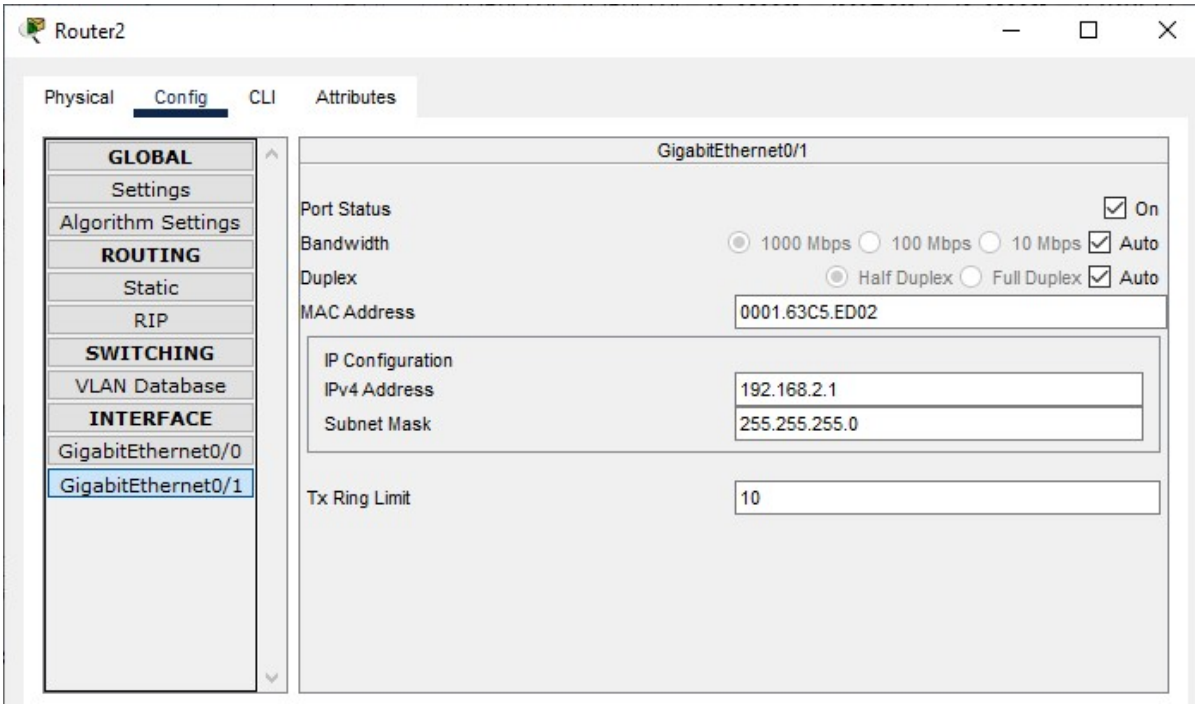


Configuring Router2:

Interface GigabitEthernet0/0:



Interface GigabitEthernet0/1:



Checking and Enabling the Security features in Router R1 and R2:

Enter the following command in the CLI mode of Router1

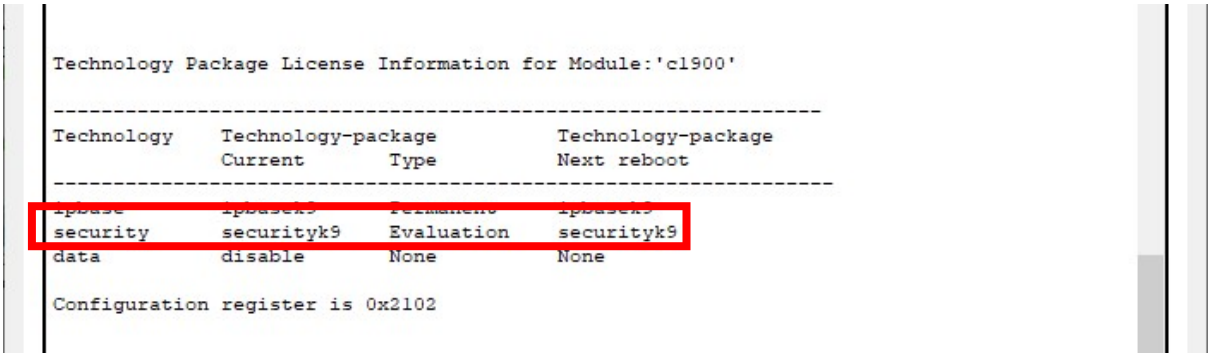
Router(config)#ip route 0.0.0.0 0.0.0.0 20.0.0.2
Router(config)#hostname R1
R1(config)#exit
R1#show version

```
Device#   PID                   SN
------------------------------------------------
*0        CISCO1941/K9          FTX1524N826-


Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
security      None          None          None
data          None          None          None

Configuration register is 0x2102
```

(We see that the security feature is not enabled, hence we need to enable the security package

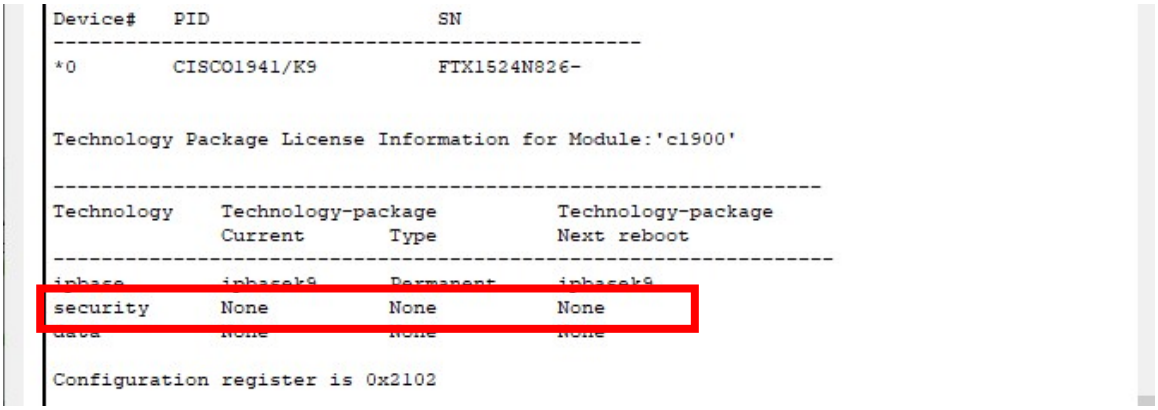
R1#
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)#license boot module c1900 technology-package securityk9
R1(config)#exit
R1#
R1#copy run startup-config

R1#reload
R1>enable
R1#show version



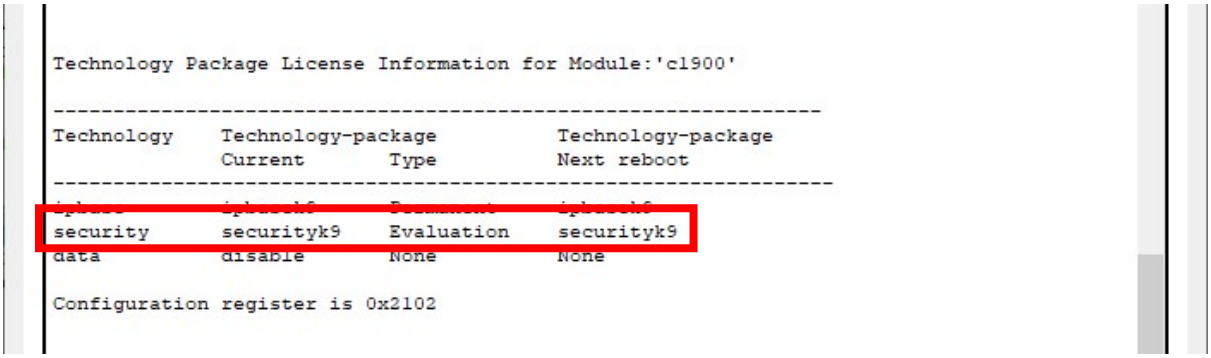
(The security package is enabled)

Enter the following command in the CLI mode of Router2
Router(config)#ip route 0.0.0.0 0.0.0.0 30.0.0.2
Router(config)#hostname R2
R2(config)#exit
R2#show version



(We see that the security feature is not enabled, hence we need to enable the security package

R2#
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#
R2(config)#license boot module c1900 technology-package securityk9
R2(config)#exit
R2#
R2#copy run startup-config
R2#reload
R2>enable
R2#show version



(The security package is enabled)

Enter the following command in the CLI mode of Router0

Router>enable
Router#configure terminal
Router(config)#hostname R0
R0(config)#

Defining the Hostname for all Routers and Configuring the Routers R1 and R2 for IPSec VPN tunnel

R1#configure terminal
R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#crypto isakmp key ismile address 30.0.0.1
R1(config)#crypto ipsec transform-set R1->R2 esp-aes 256 esp-sha-hmac
R1(config)#

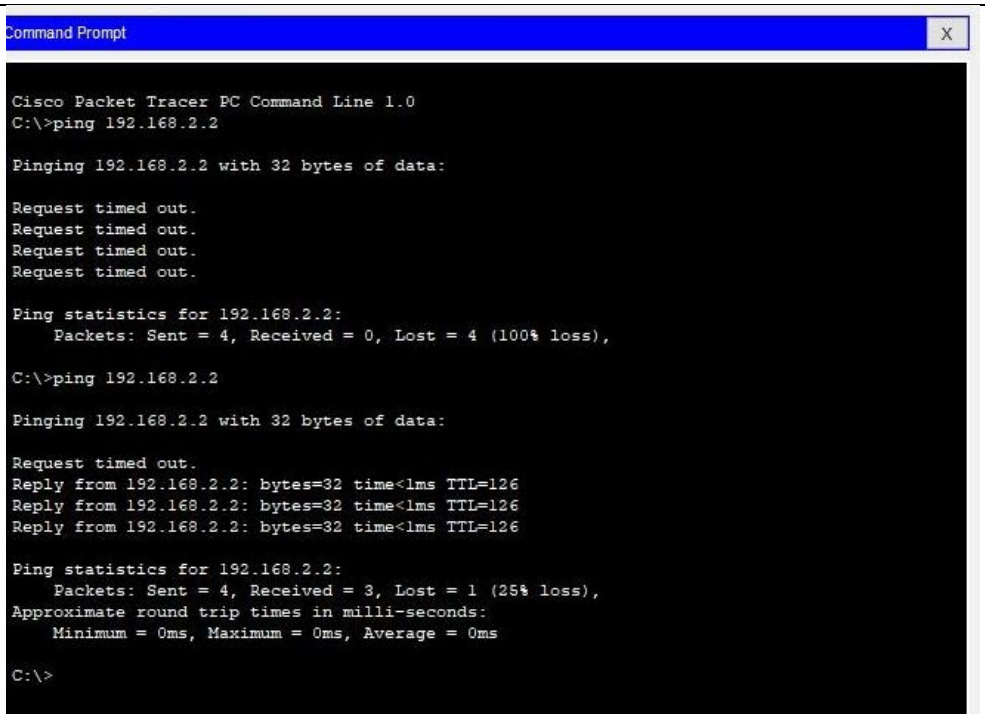
R2#
R2#configure terminal
R2(config)#access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#encryption aes 256
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 5
R2(config-isakmp)#exit
R2(config)#crypto isakmp key ismile address 20.0.0.1
R2(config)#crypto ipsec transform-set R2->R1 esp-aes 256 esp-sha-hmac
R2(config)#

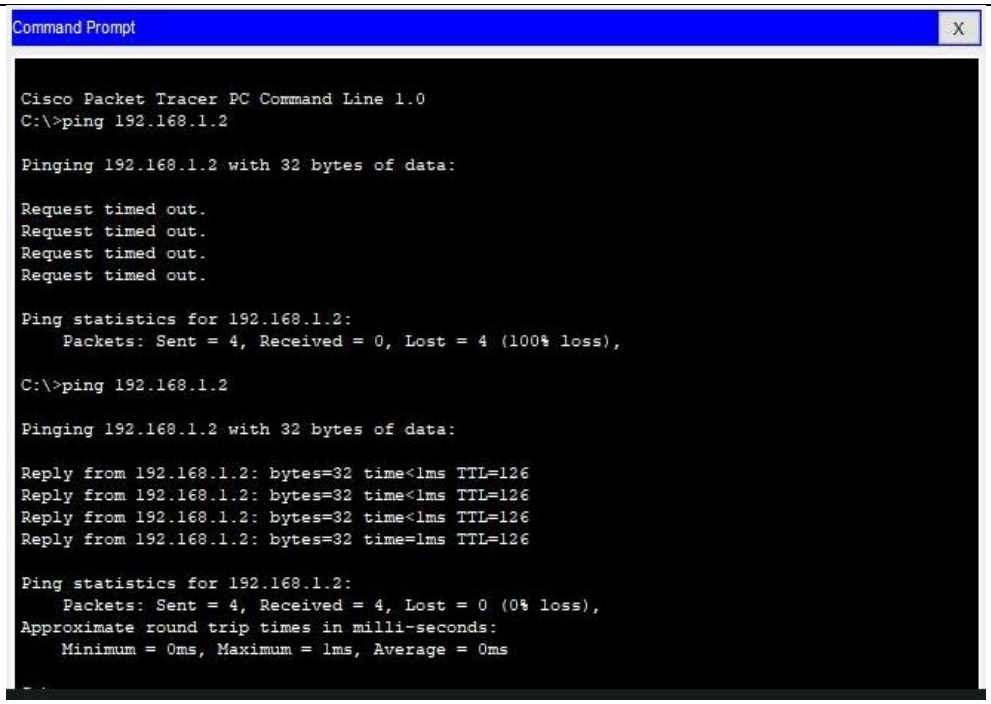
R1>enable
R1#configure terminal
R1(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
R1(config-crypto-map)#set peer 30.0.0.1
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#set security-association lifetime seconds 86400
R1(config-crypto-map)#set transform-set R1->R2

```
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#exit
R1(config)#interface g0/0
R1(config-if)#crypto map IPSEC-MAP

R2>enable
R2#configure terminal
R2(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
R2(config-crypto-map)#set peer 20.0.0.1
R2(config-crypto-map)#set pfs group5
R2(config-crypto-map)#set security-association lifetime seconds 86400
R2(config-crypto-map)#set transform-set R2->R1
R2(config-crypto-map)#match address 100
R2(config-crypto-map)#exit
R2(config)#interface g0/0
R2(config-if)#crypto map IPSEC-MAP
```

We verify the working of the IPSec VPN tunnel using the ping command as follows

Output:	Pinging PC2(192.168.2.2) from PC1 and then PC1(192.168.1.2) from PC2





For the video demonstration of the above practical click on the link below or scan the QR-code

https://youtu.be/QHR6cbvB6X0