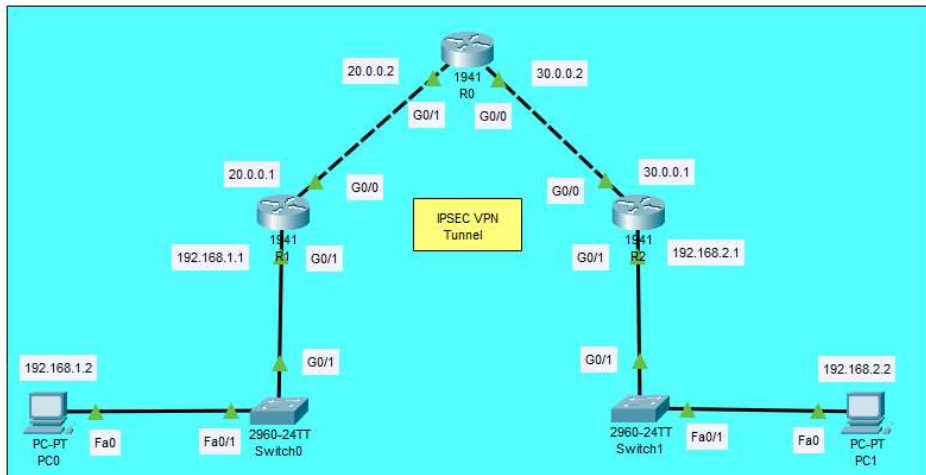


PRACTICAL-6 : IP Security (IPsec) Configurat

AIM :- To Configure IPsec on network devices to provide secure communication and protect against unauthorized access and attacks.

Topology : We will use the following topology –



• IP Configuration table for the above topology :-

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC0	FastEthernet0	192.168.1.2	255.255.255.0	192.168.1.1
PC1	FastEthernet0	192.168.2.2	255.255.255.0	192.168.2.1
R0(Router 0) (1941-Router)	GigabitEthernet0/0 GigabitEthernet0/1	30.0.0.2 20.0.0.2	255.0.0.0 255.0.0.0	NIL NIL
R1(Router 1) (1941-Router)	GigabitEthernet0/0 GigabitEthernet0/1	20.0.0.1 192.168.1.1	255.0.0.0 255.255.255.0	NIL NIL
R2(Router 2) (1941-Router)	GigabitEthernet0/0 GigabitEthernet0/1	30.0.0.1 192.168.2.1	255.0.0.0 255.255.255.0	NIL NIL
Switch0(2960-24TT)	FastEthernet0/1(to PC0) GigabitEthernet0/1(to R1)	NIL	NIL	NIL
Switch1(2960-24TT)	FastEthernet0/1(to PC1) GigabitEthernet0/1(to R2)	NIL	NIL	NIL

Now, we will configure all the devices step-by-step :-

PC0

PC1

Router0

Router1router2

- **Configuring PC0 :**

The screenshot shows the 'PC0' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section is expanded, showing the 'Interface' as 'FastEthernet0'. Under 'IP Configuration', the 'Static' radio button is selected. The fields are filled with: IPv4 Address: 192.168.1.2, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.1.1, and DNS Server: 0.0.0.0. The 'IPv6 Configuration' section is also visible, with 'Static' selected and a Link Local Address of FE80::290:2BFF:FE35:9389.

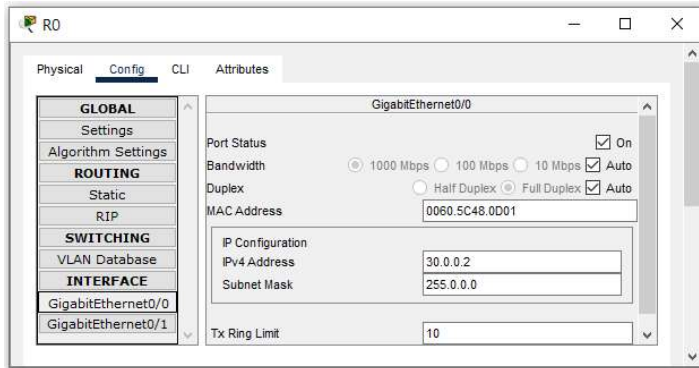
Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0
IPv6 Configuration	
<input type="radio"/> Automatic	<input checked="" type="radio"/> Static
IPv6 Address	
Link Local Address	FE80::290:2BFF:FE35:9389
Default Gateway	
DNS Server	

- **Configuring PC1 :**

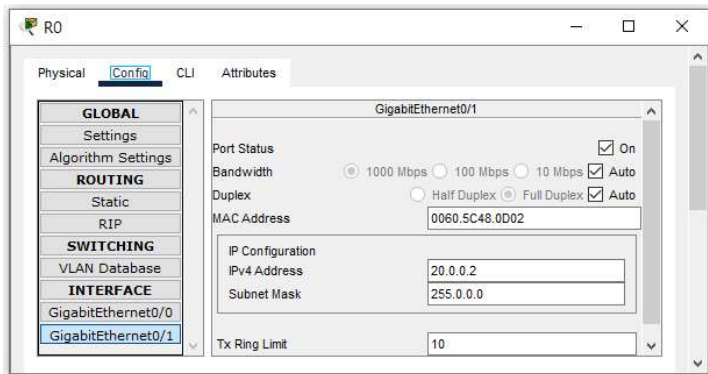
The screenshot shows the 'PC1' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section is expanded, showing the 'Interface' as 'FastEthernet0'. Under 'IP Configuration', the 'Static' radio button is selected. The fields are filled with: IPv4 Address: 192.168.2.2, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.2.1, and DNS Server: 0.0.0.0. The 'IPv6 Configuration' section is also visible, with 'Static' selected and a Link Local Address of FE80::290:2BFF:FE35:9389.

Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.2.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server	0.0.0.0
IPv6 Configuration	
<input type="radio"/> Automatic	<input checked="" type="radio"/> Static
IPv6 Address	
Link Local Address	FE80::290:2BFF:FE35:9389
Default Gateway	
DNS Server	

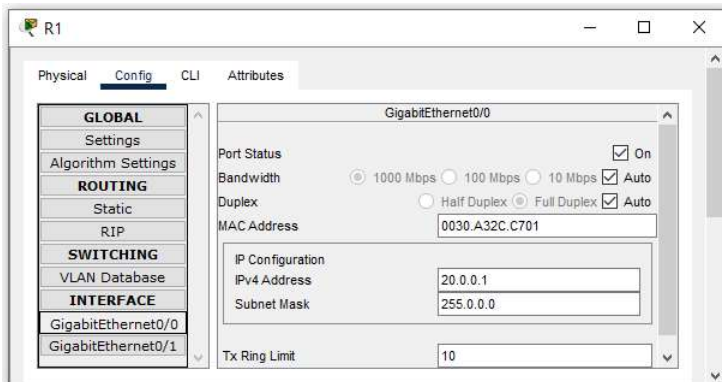
- **Configuring R0(GigabitEthernet0/0) :**



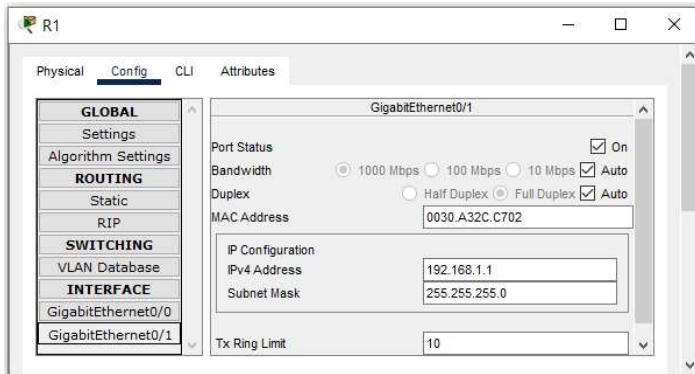
- **Configuring R0(GigabitEthernet0/1) :**



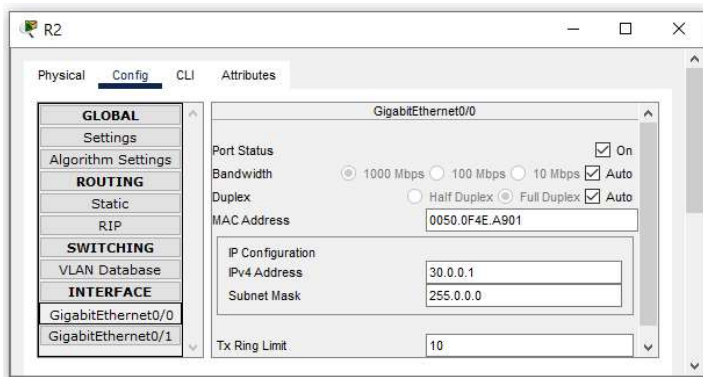
- **Configuring R1(GigabitEthernet0/0) :**



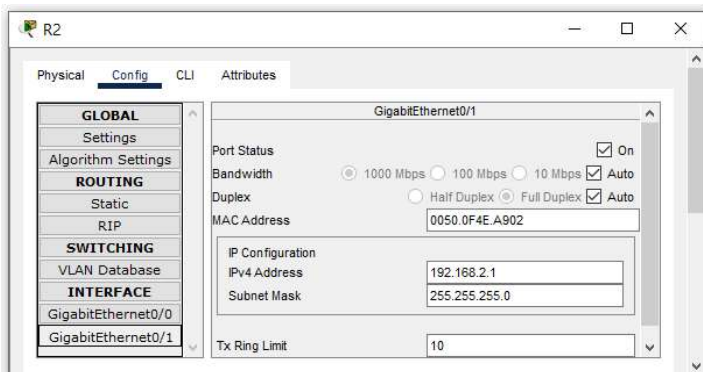
- **Configuring R1(GigabitEthernet0/1) :**



- **Configuring R2(GigabitEthernet0/0) :**



- **Configuring R2(GigabitEthernet0/1) :**

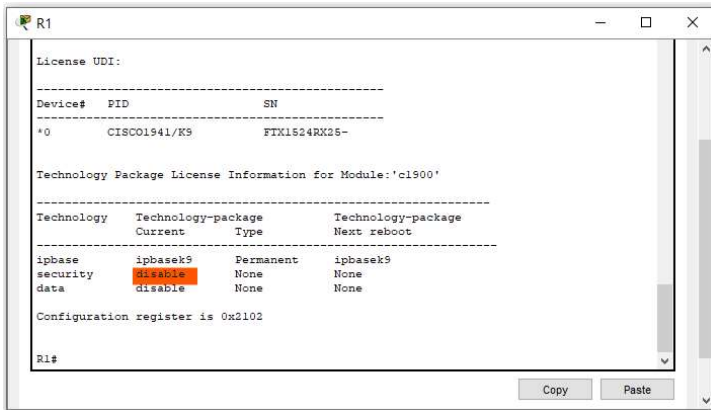


- **Checking and Enabling the Security features on Router1(R1) and Router2(R2) :**

1. Enter the following command in the CLI mode of Router1 :-

R1>enable

R1#show version



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

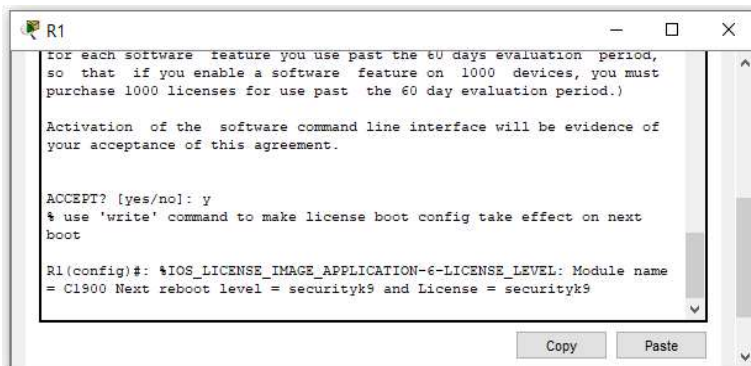
R1#

R1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#license boot module c1900 technology-package securityk9

Type : y



R1(config)#exit

R1#

R1#copy run startup-config

R1#reload

R1>show version

```
R1
License UDI:
-----
Device# PID SN
-----
*0 CISC01941/K9 FTX1524RX25-

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#
```

(The security package is enabled) .

2. Enter the following command in the CLI mode of Router2 :-

R1>enable
R1#show version

```
R2
License Info:
License UDI:
-----
Device# PID SN
-----
*0 CISC01941/K9 FTX1524JNHQ-

Technology Package License Information for Module:'c1900'
-----
Technology Technology-package Technology-package
Current Type Next reboot
-----
ipbase ipbasek9 Permanent ipbasek9
security disable None None
data disable None None

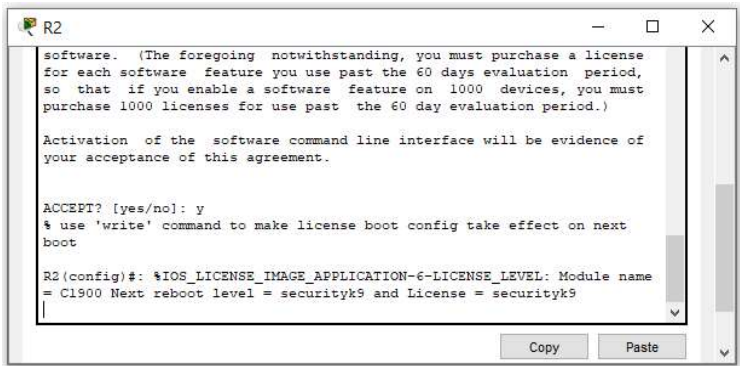
Configuration register is 0x2102

R2#
```

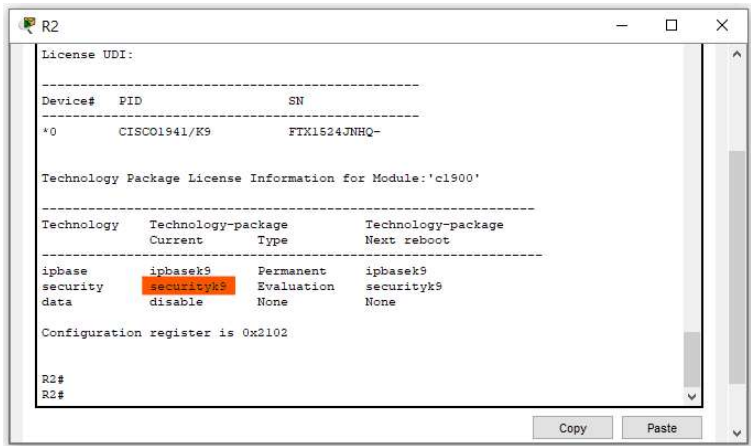
(We can see that the security feature is not enabled, hence we need to enable the security package)

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

Type : y



R1(config)#exit
R1#
R1#copy run startup-config
R1#reload
R1>show version



(The security package is enabled) .

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

1. Enter the following command in the CLI mode of Router1 :-

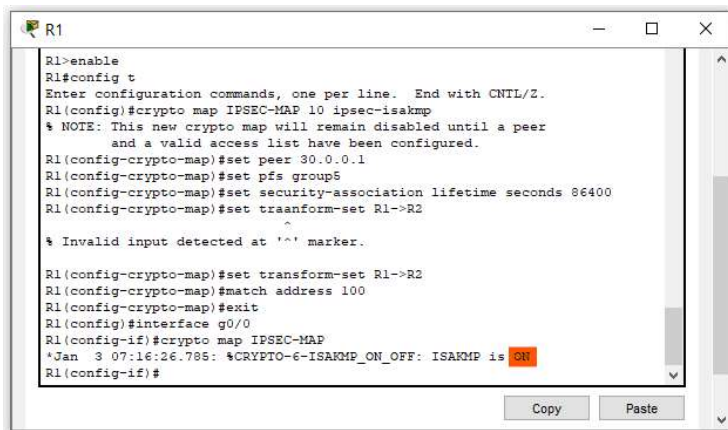
```
R1>enable
R1#configure terminal
R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp) #group 5
R1(config-isakmp)#exit
R1(config)#crypto isakmp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

2. Enter the following command in the CLI mode of Router2 :-

```
R2>enable
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
R1(config-isakmp)#exit
R1(config)#crypto isakmp key ismile address 20.0.0.1
R1(config)#crypto ipsec transform-set R2->R1 esp-aes 256 esp-sha-hmac
R1(config)#
```

3. Enter the following command in the CLI mode of Router1 :-

```
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
```

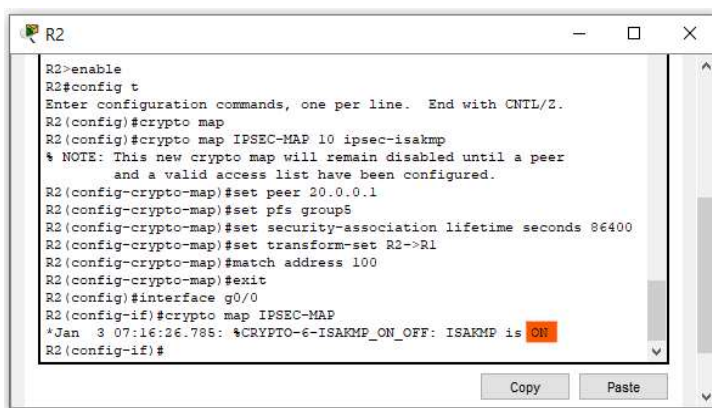



A screenshot of a terminal window titled 'R1' showing the configuration of an IPsec crypto map. The commands entered are: `R1>enable`, `R1#config t`, `R1(config)#crypto map IPSEC-MAP 10 ipsec-isakmp`, `R1(config-crypto-map)#set peer 30.0.0.1`, `R1(config-crypto-map)#set pfs group5`, `R1(config-crypto-map)#set security-association lifetime seconds 86400`, `R1(config-crypto-map)#set transform-set R1->R2`, `R1(config-crypto-map)#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`, and `R1(config-if)#`. A status message at the bottom indicates 'CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON'.

```
R1>enable
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#crypto map IPSEC-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)#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)#set transform-set R1->R2
% Invalid input detected at '^' marker.
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
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
```

4. Enter the following command in the CLI mode of Router2 :-

```
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
```



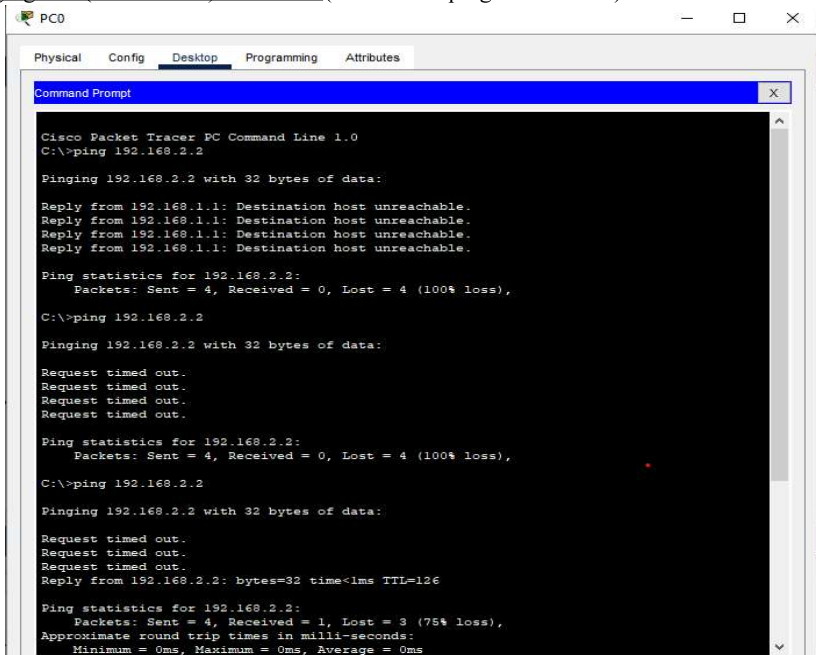
A screenshot of a terminal window titled 'R2' showing the configuration of an IPsec crypto map. The commands entered are: `R2>enable`, `R2#config t`, `R2(config)#crypto map`, `R2(config)#crypto map IPSEC-MAP 10 ipsec-isakmp`, `R2(config-crypto-map)#set peer 20.0.0.1`, `R2(config-crypto-map)#set pfs group5`, `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`, and `R2(config-if)#`. A status message at the bottom indicates 'CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON'.

```
R2>enable
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#crypto map
R2(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
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
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R2(config-if)#
```

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

Output :-

1. Pinging PC1(192.168.2.2) from PC0(command - ping 192.168.2.2) :-



```
PC0
Physical  Config  Desktop  Programming  Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

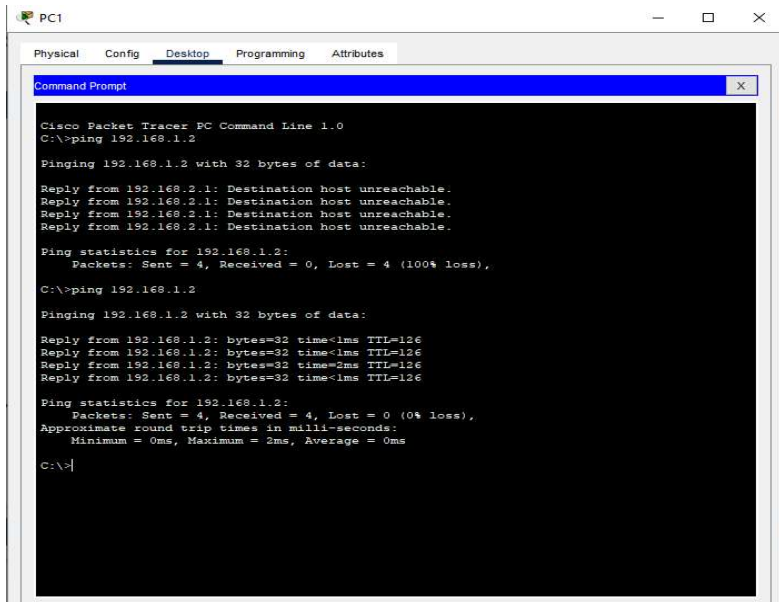
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. Pinging PC0(192.168.1.2) from PC1(command - ping 192.168.1.2) :-



```
PC1
Physical  Config  Desktop  Programming  Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=2ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms
C:\>|
```