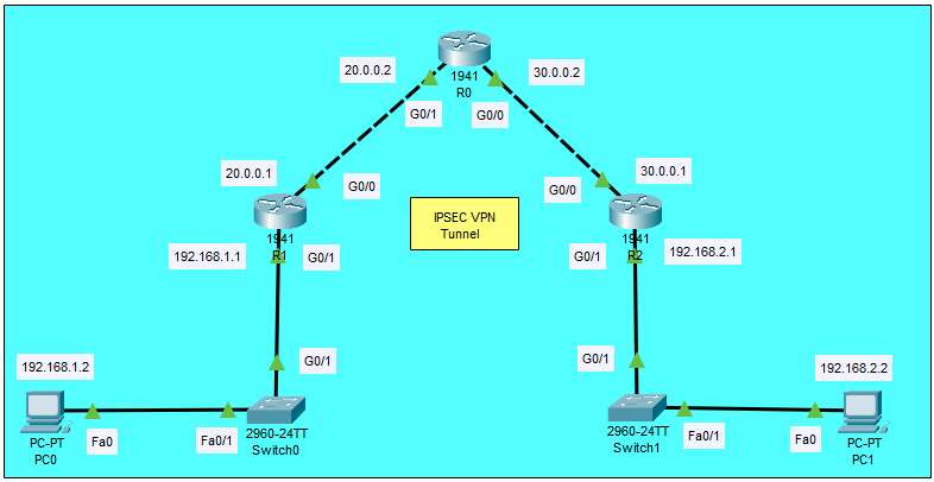
PRACTICAL-6 : IP Security (IPsec) Configurat

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 –



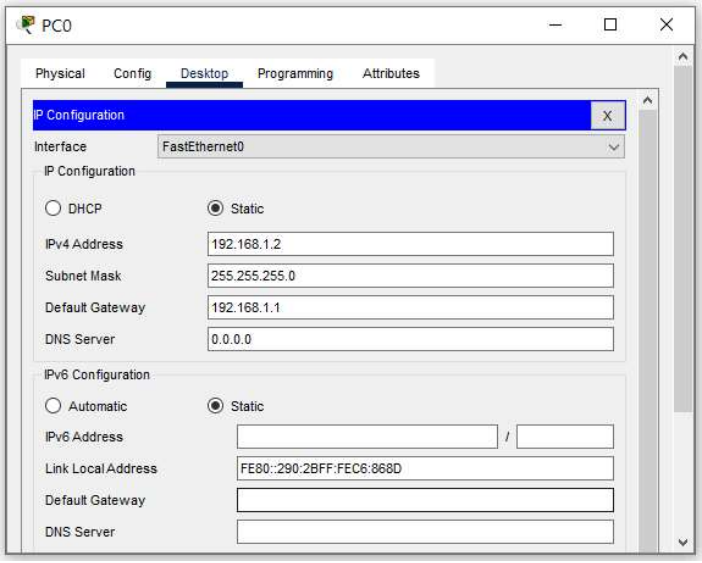
- **IP Configuration table for the above topology :-**

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

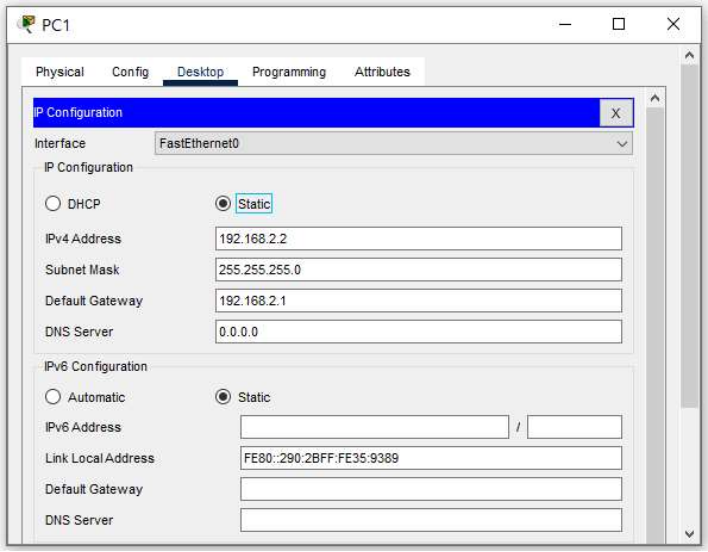
Now, we will configure all the devices step-by-step :-

PC0
PC1
Router0
Router1outer2

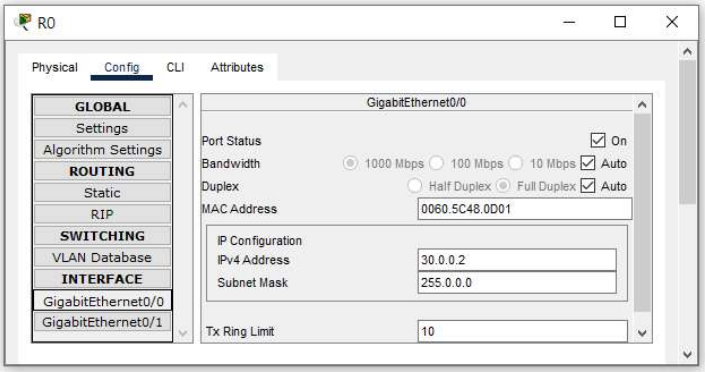
- **Configuring PC0 :**



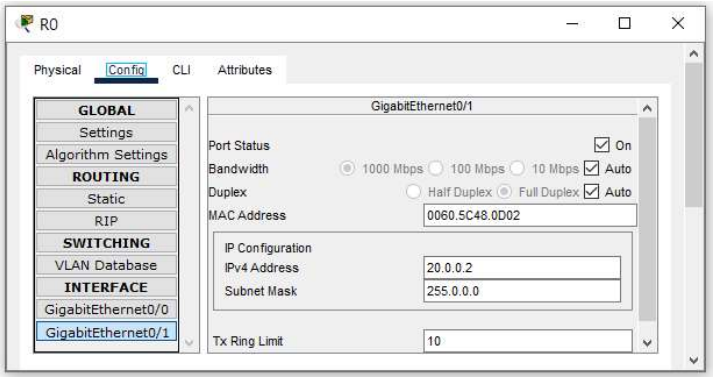
- **Configuring PC1 :**



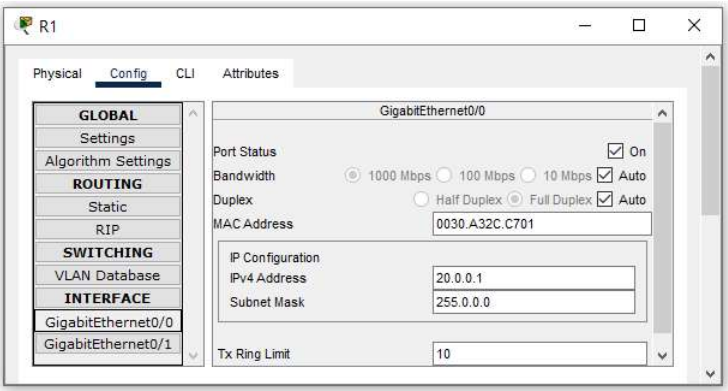
- **Configuring R0(GigabitEthernet0/0) :**



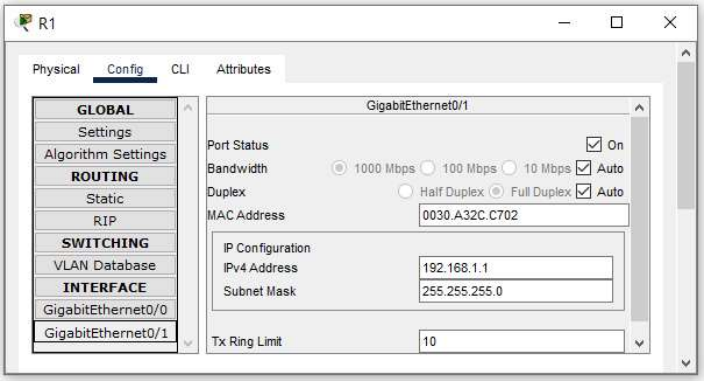
- **Configuring R0(GigabitEhternet0/1) :**



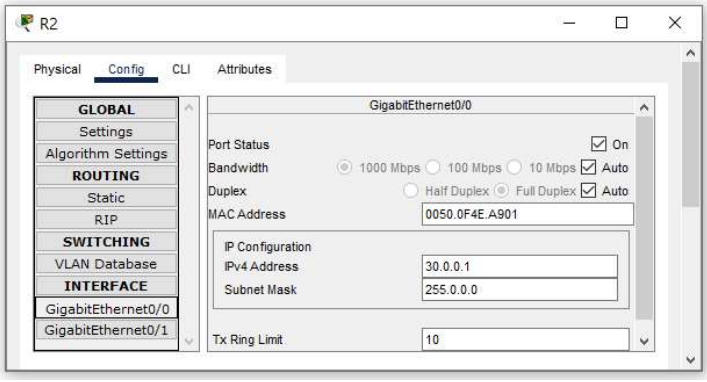
- **Configuring R1(GigabitEhternet0/0) :**



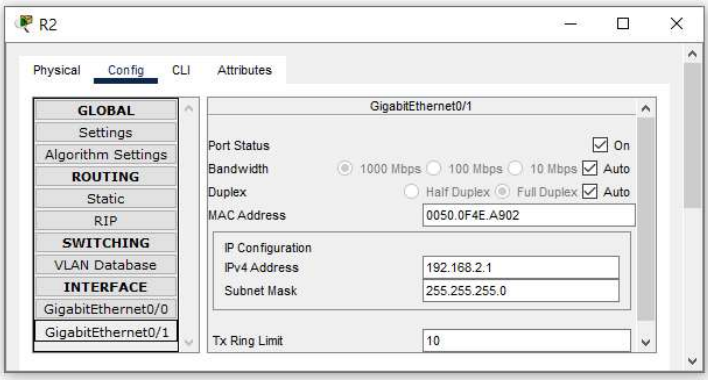
- **Configuring R1(GigabitEhternet0/1) :**



- **Configuring R2(GigabitEhternet0/0) :**



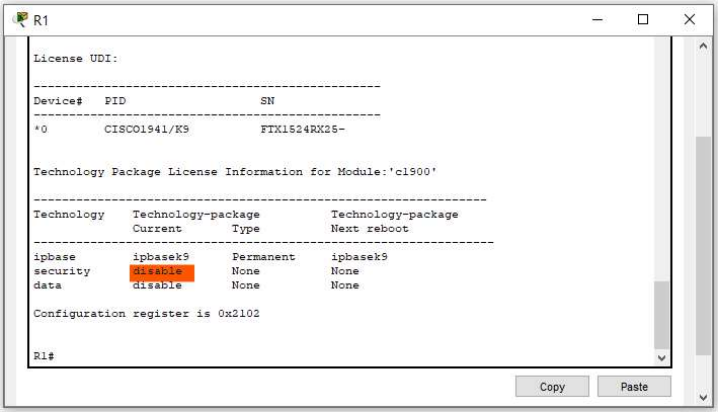
- **Configuring R2(GigabitEhternet0/1) :**



- **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

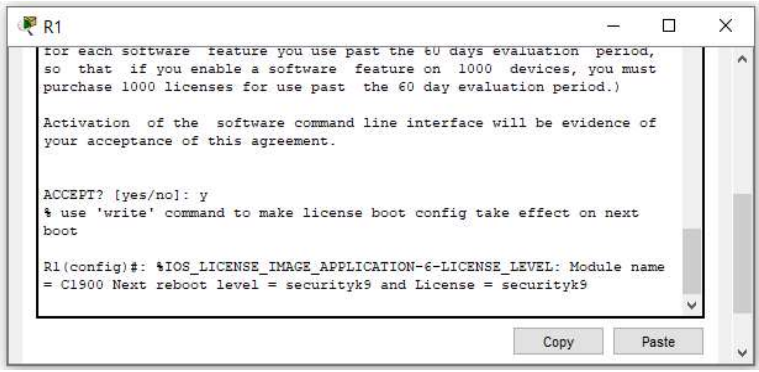


```
License UDI:

-------------------------------------------------
Device#   PID                    SN
-------------------------------------------------
*0        CISCO1941/K9           FTX1524RX25-


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


R1#
```

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

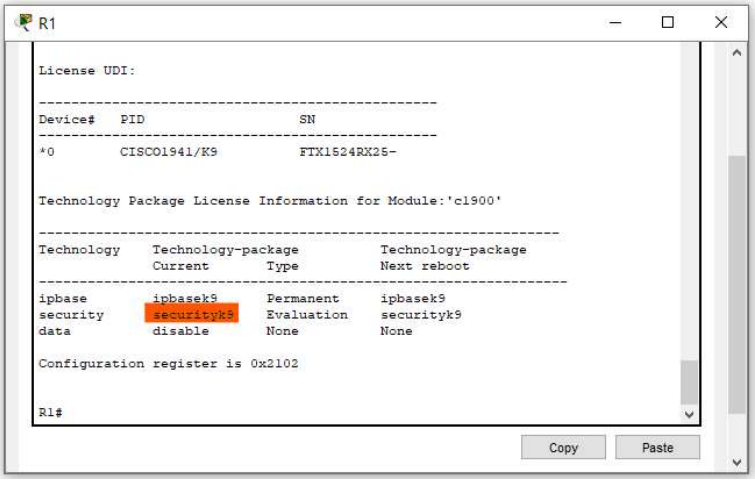
R1#
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#license boot module c1900 technology-package securityk9

Type : y



```
for each software  feature you use past the 60 days evaluation  period,
so  that  if you enable a software  feature on  1000  devices, you must
purchase 1000 licenses for use past  the 60 day evaluation period.)

Activation  of the  software command line interface will be evidence of
your acceptance of this agreement.


ACCEPT? [yes/no]: y
% use 'write' command to make license boot config take effect on next
boot

R1(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name
= C1900 Next reboot level = securityk9 and License = securityk9
```

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



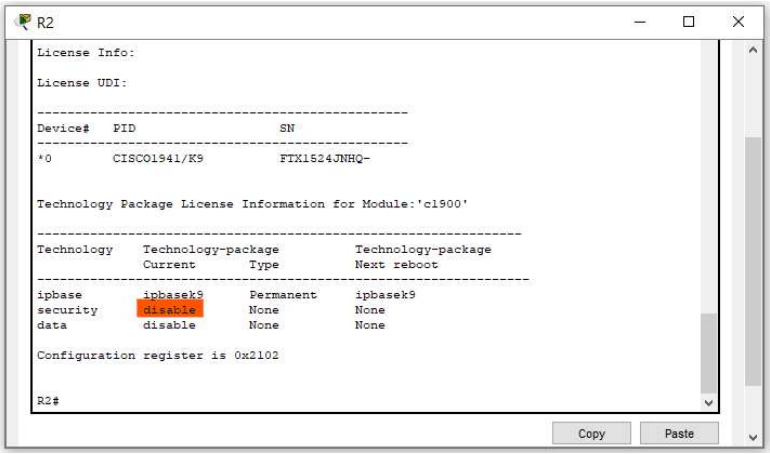
```
License UDI:

-------------------------------------------------
Device#   PID                    SN
-------------------------------------------------
*0        CISCO1941/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. <u>Enter the following command in the CLI mode of Router2</u> :-

R1>enable
R1#show version



```
License Info:

License UDI:

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

```
R2
software.  (The foregoing  notwithstanding, you must purchase a license
for each software  feature you use past the 60 days evaluation  period,
so  that  if you enable a software  feature on  1000  devices, you must
purchase 1000 licenses for use past  the 60 day evaluation period.)

Activation  of the  software command line interface will be evidence of
your acceptance of this agreement.


ACCEPT? [yes/no]: y
% use 'write' command to make license boot config take effect on next
boot

R2(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name
= C1900 Next reboot level = securityk9 and License = securityk9
|
Copy   Paste
```

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

```
R2
License UDI:

-------------------------------------------------
Device#   PID                    SN
-------------------------------------------------
*0        CISCO1941/K9           FTX1524JNHQ-


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


R2#
R2#
Copy   Paste
```

(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
```

---

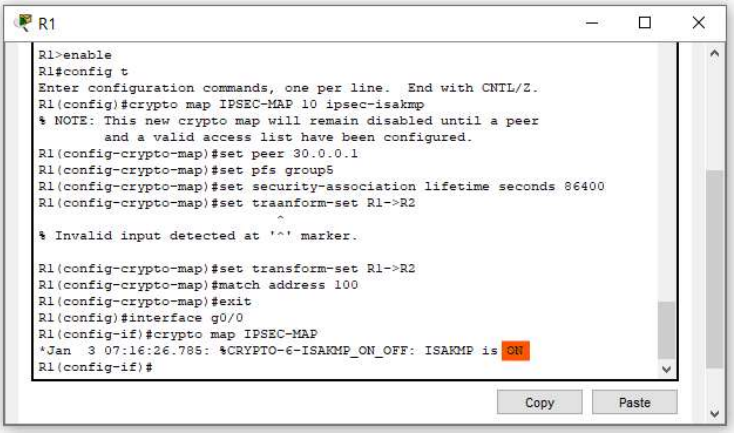
2. Enter the following command in the CLI mode of Router2 :-

```
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 :-

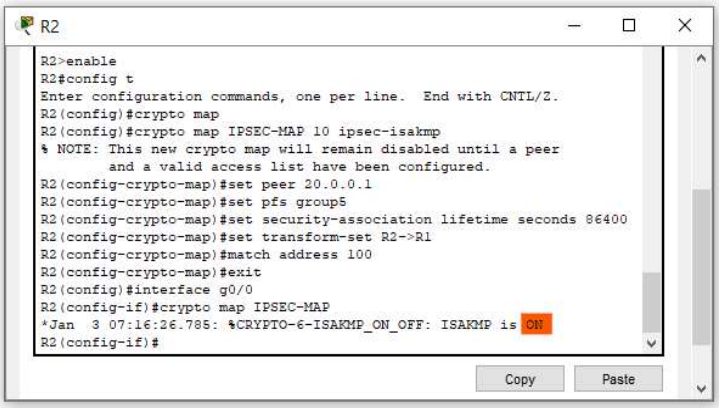
```
R1>enable
R1#configure terminal
R1(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
R1(config-crypto-map)#set peer 30.0.0.1
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#set security-association lifetime seconds 86400
R1(config-crypto-map)#set transform-set R1->R2
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#exit
R1(config)#interface g0/0
R1(config-if)#crypto map IPSEC-MAP
```



---

4. <u>Enter the following command in the CLI mode of Router2</u> :-

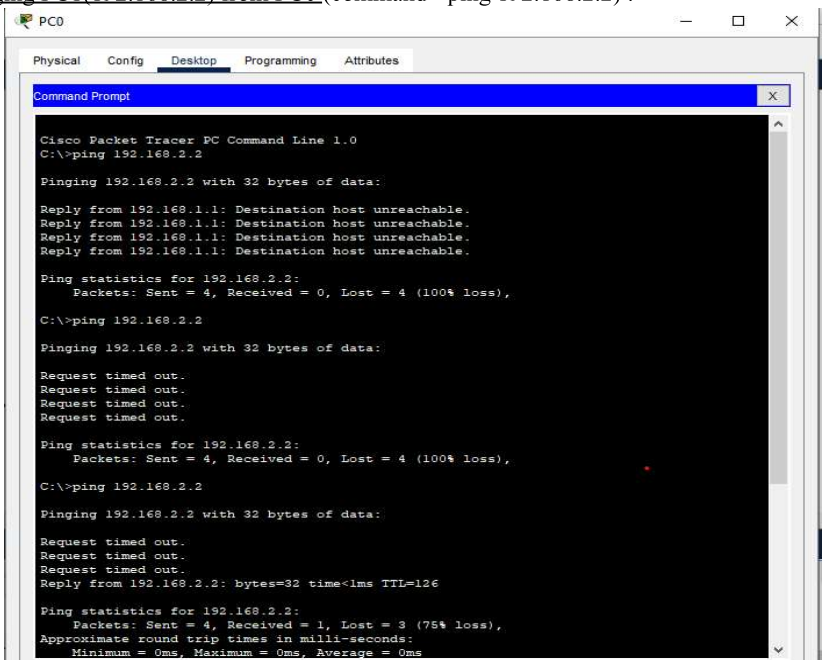
R2>enable
R2#configure terminal
R2(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
R2(config-crypto-map)#set peer 20.0.0.1
R2(config-crypto-map)#set pfs group5
R2(config-crypto-map)#set security-association lifetime seconds 86400
R2(config-crypto-map)#set transform-set R2->R1
R2(config-crypto-map)#match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



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

<u>Output</u> :-

1. <u>Pinging PC1(192.168.2.2) from PC0</u> (command - ping 192.168.2.2) :-



2. <u>Pinging PC0(192.168.1.2) from PC1</u> (command - ping 192.168.1.2) :-