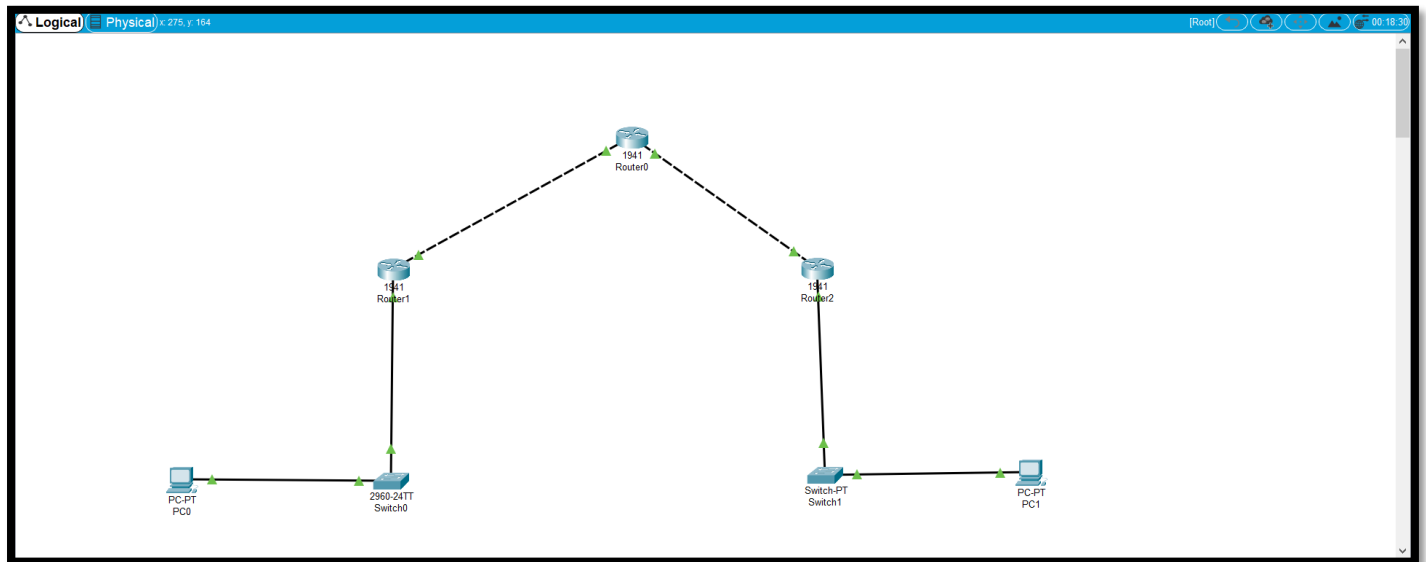


Practical no: 6**Aim: IP Security (IPsec) Configuration****Requirements:**

- Cisco Packet tracer

Steps:**1. Implementing the topology using Cisco packet tracer.****2. Ip addresses for following and component used in above topology:**

Components	IP	G0/0	G0/1	Default Gateway
PC0	192.168.1.2			192.168.1.1
PC1	192.168.2.2			192.168.2.1
1941 Router0		30.0.0.2	20.0.0.2	
1941 Router1		20.0.0.1	192.168.1.1	
1941 Router2		30.0.0.1	192.168.2.1	
2960 24TT Switch				

3. ISAKMP Policy Parameters

Parameters	Parameters Option & 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	Group5	Group5
ISE SA Lifetime	86400 seconds or less	86400	86400
ISAKMP Key	User Defined	ismile	ismile

4. IP Sec Policy Parameters

Parameters	R1	R1
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 Executed	R1->R2	R2->R1
Crypto map Name	IPSEC-MAP	IPSEC-MAP
SA Establishment	Ipssec-isakmp	Ipssec-isakmp

5. Router 1

```

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 0.0.0.0 0.0.0.0 20.0.0.2
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#

```

6. Router 2

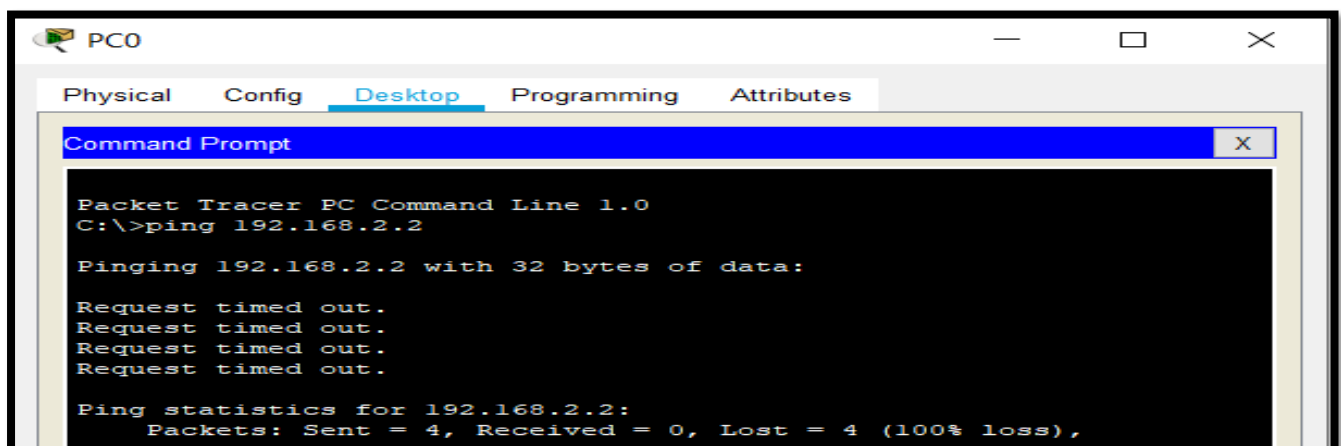
```

Router#
Router#
Router#
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#ip route 0.0.0.0 0.0.0.0 30.0.0.2
Router(config)#
Router(config)#
Router(config)#

```

7. Now ping from PC0 and PC1 to eachother.

It will get lost: ping from PC0->PC1



8. Assign Hostname to Routers:

Use this Command Before Assigning Hostname:

- Exit
- Enable

Router 1

```
Router(config)#
Router(config)#Hostname R1
```

Router 2

```
Router(config)#
Router(config)#Hostname R2
```

Router0

```
Router(config)#
Router(config)#Hostname R0
```

9. Router : R1 & R2

Checking whether security version is enabled or not

It will be disabled by default

To enable it use this Command in both router:

- Exit
- Show version
- Configure terminal
- License boot module c1900 technology-package securityk9
- Yes
- Copy run startup-config (Press Enter)
- Reload (Press Enter)
- Enable
- Show version

Technology Package License Information for Module:'c1900'

Technology	Technology-package Current	Technology-package Type	Technology-package Next reboot
ipbase	ipbasek9	Permanent	ipbasek9
security	None	None	None
data	None	None	None

Configuration register is 0x2102

```

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#license boot module c1900 technology-package
securityk9
PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE
LICENSE OR
LICENSE KEY PROVIDED FOR ANY CISCO PRODUCT FEATURE OR
USING SUCH
PRODUCT FEATURE CONSTITUTES YOUR FULL ACCEPTANCE OF THE
FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO BE

```

```

%SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with
ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bblc58
Self decompressing the image :
#####

```

Technology Package License Information for Module:'c1900'

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

Configuration register is 0x2102

**10. Now that security version is enabled
Configure access control list. (A C L)**

Router 1:

- Exit
- Enable
- Configure terminal
- access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
- crypto isakmp policy 10
- encryption aes 256
- authentication pre-share
- group5
- exit
- crypto isakmp key Rushi address 30.0.0.1
- crypto ipsec transform-set R1->R2 esp-aes 256 esp-sha-hmac

```
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)#
```

```
R1(config-if)#crypto isakmp key Rushi address 30.0.0.1
```

```
R1(config-if)#crypto ipsec transform-set R1->R2 esp-aes 256 esp-
sha-hmac
```

Router 2:

- **Exit**
- **Enable**
- **Configure terminal**
- **access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255**
- **crypto isakmp policy 10**
- **encryption aes 256**
- **authentication pre-share**
- **group5**
- **exit**
- **crypto isakmp key Rushi1 address 20.0.0.1**
- **crypto ipsec transform-set R2->R1 esp-aes 256 esp-sha-hmac**

```
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)#
```

```
R2(config)#
R2(config)#crypto isakmp key Rushi1 address 20.0.0.1
```

```
R2(config)#crypto ipsec transform-set R2->R1 esp-aes 256 esp-sha-
hmac
R2(config)#
```

11. Now we have to create the ipsec map 10 on both the routers**Router 1:**

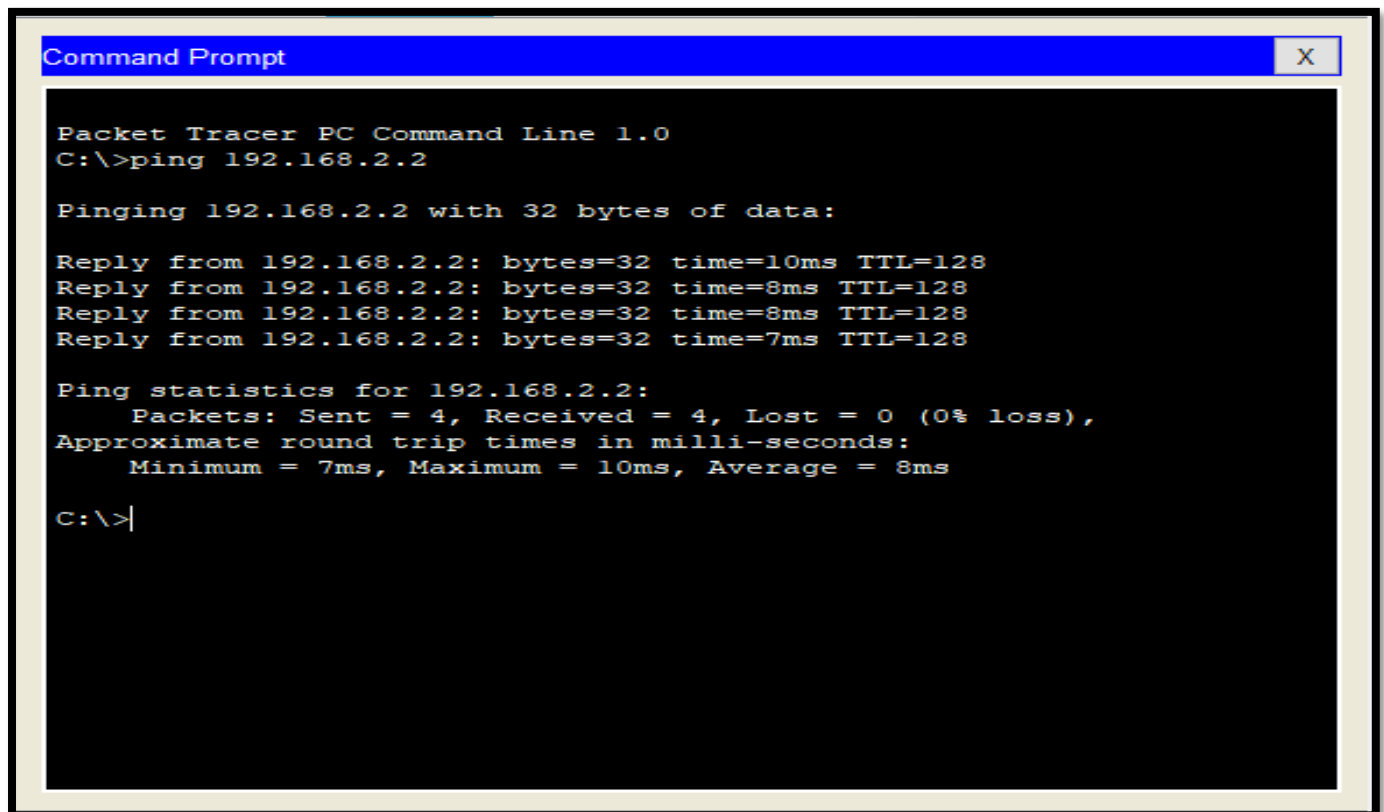
- exit
- enable
- configure terminal
- crypto map IPSEC-MAP 10 ipsec-isakmp
- set peer 30.0.0.1
- set pfs group5
- set security-association lifetime seconds 86400
- set transform-set R1->R2
- match address 100
- exit
- interface g0/0
- crypto map IPSEC-MAP

```
R1(config)#
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
ERROR: transform set with tag R1->R2 does not exist.
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-ISA_KMP_ON_OFF: ISAKMP is ON
R1(config-if)#
```

Router 2:

- exit
- enable
- configure terminal
- crypto map IPSEC-MAP 10 ipsec-isakmp
- set peer 20.0.0.1
- set pfs group5
- set security-association lifetime seconds 86400
- set transform-set R1->R2
- match address 100
- exit
- interface g0/0
- crypto map IPSEC-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
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R2(config-if)#
```


12. Ping From PC1 and PC0 to each other:**PC0->PC1**

```
Command Prompt X

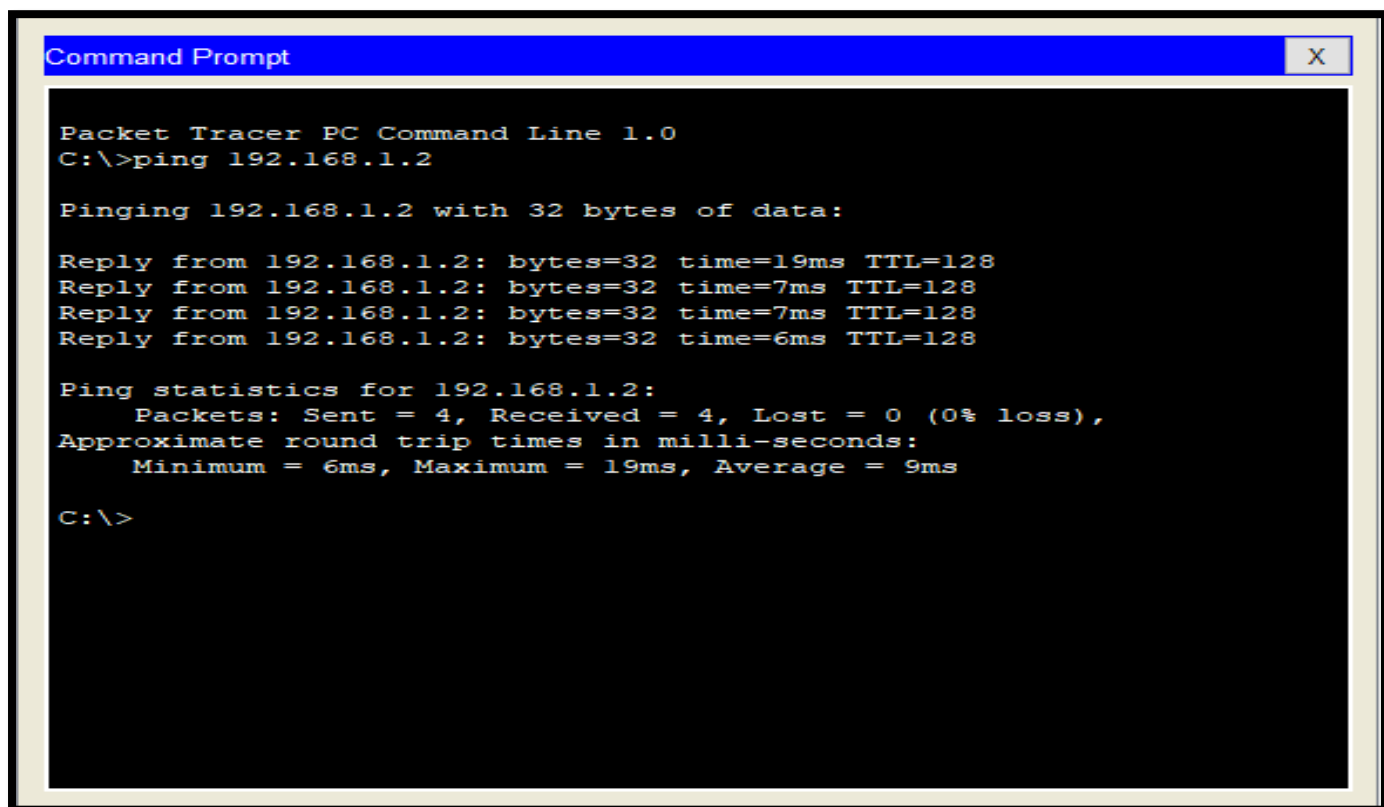
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=10ms TTL=128
Reply from 192.168.2.2: bytes=32 time=8ms TTL=128
Reply from 192.168.2.2: bytes=32 time=8ms TTL=128
Reply from 192.168.2.2: bytes=32 time=7ms TTL=128

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 10ms, Average = 8ms

C:\>|
```

PC1->PC0

```
Command Prompt X

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 192.168.1.2: bytes=32 time=19ms TTL=128
Reply from 192.168.1.2: bytes=32 time=7ms TTL=128
Reply from 192.168.1.2: bytes=32 time=7ms TTL=128
Reply from 192.168.1.2: bytes=32 time=6ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 19ms, Average = 9ms

C:\>
```