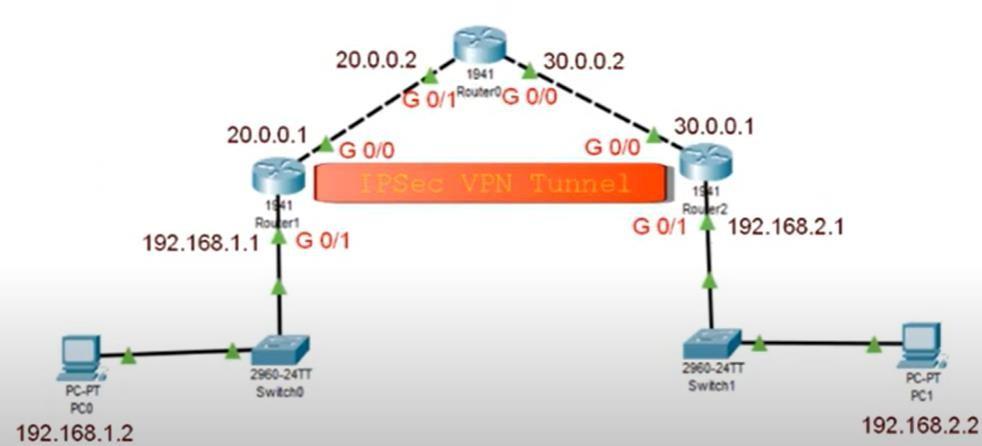
**Practical – 6**

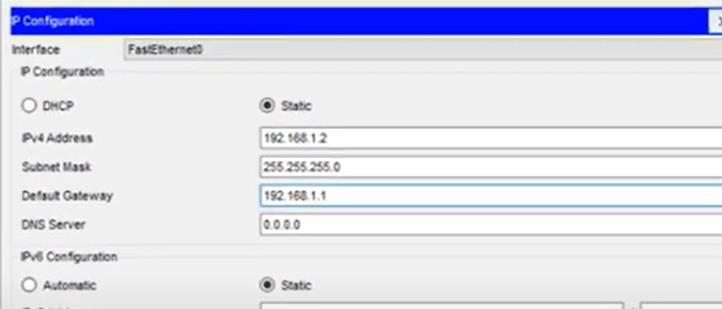
**Aim:** Configure IPsec on network devices to provide secure communication and protect against unauthorized access and attacks.

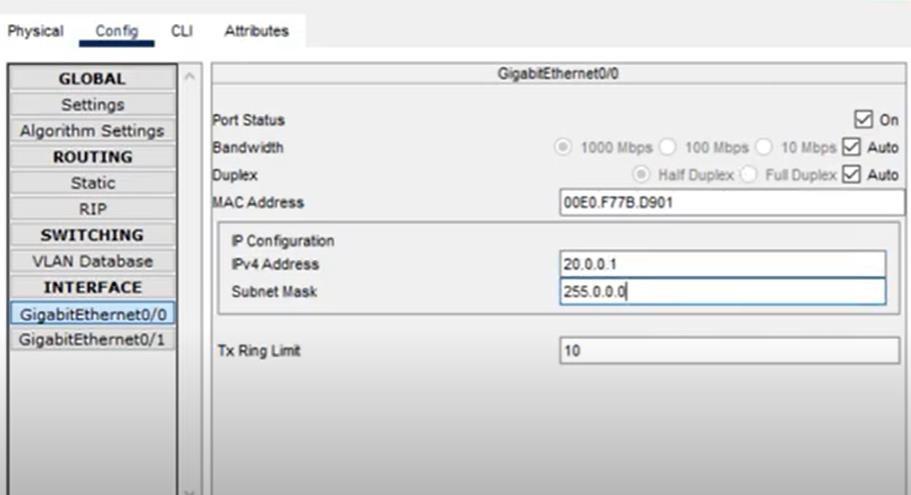
**Part 1: Implementing the Topology using Cisco Packet Tracer, configure the IP and set the IP route**

Step1 : Implement the topology as given in the below diagram



Step2 : Configure the IP address of the PC and gateway



Step 3 : Configure all the router as

**Part 2: Configure the Hostname on all Routers and enable the security package on R1 and R2, Ping on PC from the other(All packets are lost)**

Step 1: Click on router 1 click on CLI and execute the following command

Router>**enable** Router#**configure terminal**

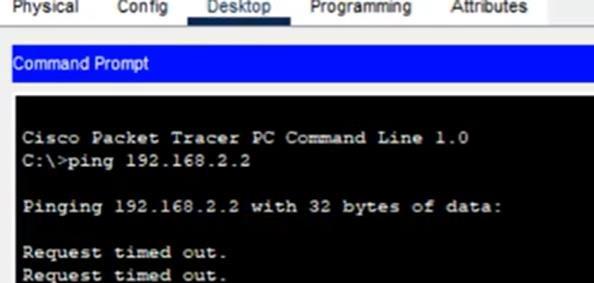
Router(config)#**ip route 0.0.0.0 0.0.0.0 20.0.0.2**

Step 2 : Click on router 2 and click on CLI and execute the following command

Router>**enable** Router#**configure terminal**

Router(config)#**ip route 0.0.0.0 0.0.0.0 30.0.0.2**

Step3: Now ping one PC from another from the command line( Ping should fail)



**Part 3: Apply the Access Control List(ACL) at Router 1 and 2, Set the ISALMP policy and ISAKMP key, Set IPSec transform set**

Step 1: Go to the CLI of router 1 and type the following command and enable security package

Router>**enable** Router#**configure terminal** Router(config)#**hostname R1**

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

R1(config)#**exit**

R1#**copy run startup-config**

R1#**reload** R1>**enable** R1#**show version**

Step2: Repeat the above step for Router 2 with hostname R2

Step 3: Enable the policy. To do so go to CLI and type the following command

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

Step4: Repeat the above step for Router 2

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

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-hamc

**Part 4 : Create the crypto map and apply to the required interface. Verify the output by pinging one PC from other**

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 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

Repeat the same for router 2.

R2(Config-crypto-map)#set peer 20.0.0.1 R1(Config-crypto-map)#set transform-set R2->R1

**Now ping the system again we will get the output**

