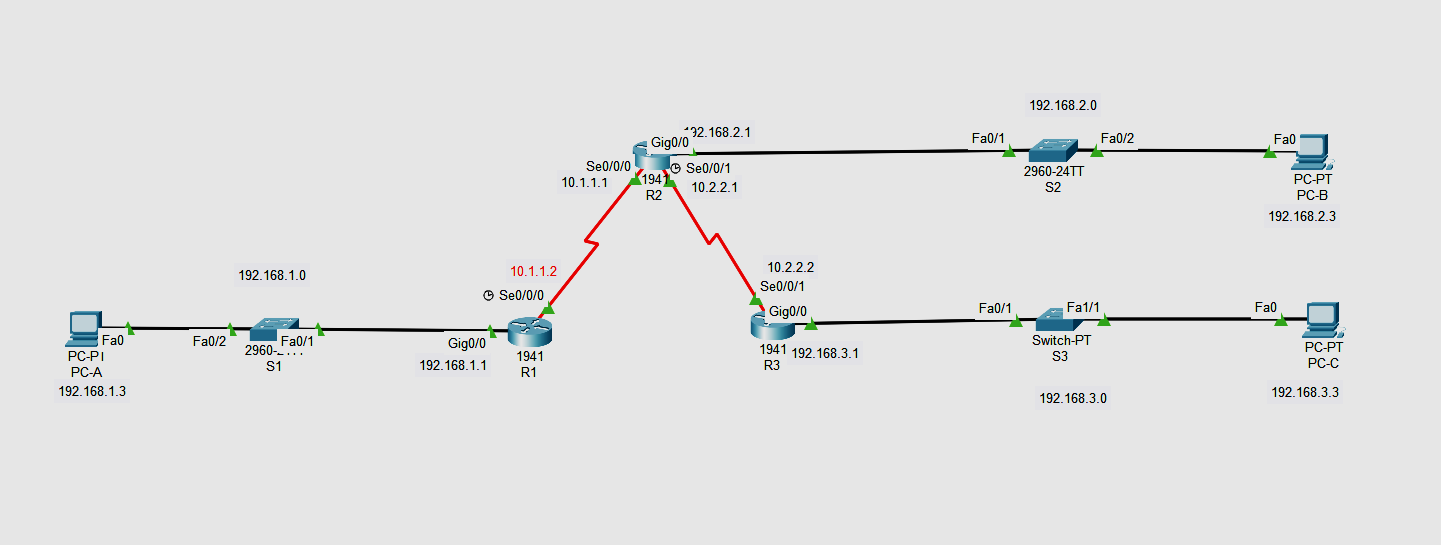
Implement IPsec Site-to-Site VPNs

**Implement IPsec Site-to-Site VPNs**

**Topology**

**Addressing Table**

| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** | **Switch Port** |
| --- | --- | --- | --- | --- | --- |
| R1 | G0/0 | 192.168.1.1 | 255.255.255.0 | N/A | S1 F0/1 |
| S0/0/0 (DCE) | 10.1.1.2 | 255.255.255.252 | N/A | N/A |
| R2 | G0/0 | 192.168.2.1 | 255.255.255.0 | N/A | S2 F0/2 |
| S0/0/0 | 10.1.1.1 | 255.255.255.252 | N/A | N/A |
| S0/0/1 (DCE) | 10.2.2.1 | 255.255.255.252 | N/A | N/A |
| R3 | G0/0 | 192.168.3.1 | 255.255.255.0 | N/A | S3 F0/5 |
| S0/0/1 | 10.2.2.2 | 255.255.255.252 | N/A | N/A |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 | S1 F0/2 |
| PC-B | NIC | 192.168.2.3 | 255.255.255.0 | 192.168.2.1 | S2 F0/1 |
| PC-C | NIC | 192.168.3.3 | 255.255.255.0 | 192.168.3.1 | S3 F0/18 |

**Part 1 : Configure the Routers and pc according to Addressing Table**

R1>enable

R1#config terminal

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

R1(config)#int G0/0

R1(config-if)#ip address 192.168.1.1 255.255.0.0

R1(config)#int S0/0/0

R1(config-if)#ip address 10.1.1.2 255.255.255.252

R1(config-if)#no shut

R1(config-if)#exit

R2>enable

R2#config terminal

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

R2(config)#int G0/0

R2(config-if)#ip address 192.168.2.1 255.255.0.0

R2(config)#int S0/0/0

R2(config-if)#ip address 10.1.1.1 255.255.255.252

R2(config)#int S0/0/1

R2(config-if)#ip address 10.2.2.1 255.255.255.252

R2(config-if)#no shut

R2(config-if)#exit

R3>enable

R3#config terminal

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

R3(config)#int G0/0

R3(config-if)#ip address 192.168.3.1 255.255.0.0

R3(config)#int S0/0/0

R3(config-if)#ip address 10.2.2.2 255.255.255.252

R3(config-if)#no shut

R3(config-if)#exit

**NOW RIP ALL THE ROUTER**

R1

Router(config)#router rip

Router(config-router)# network 10.0.0.0

Router(config-router)# network 192.168.0.0

R2

Router(config)#router rip

Router(config-router)# network 10.0.0.0

Router(config-router)# network 192.168.0.0

R3

Router(config)#router rip

Router(config-router)# network 10.0.0.0

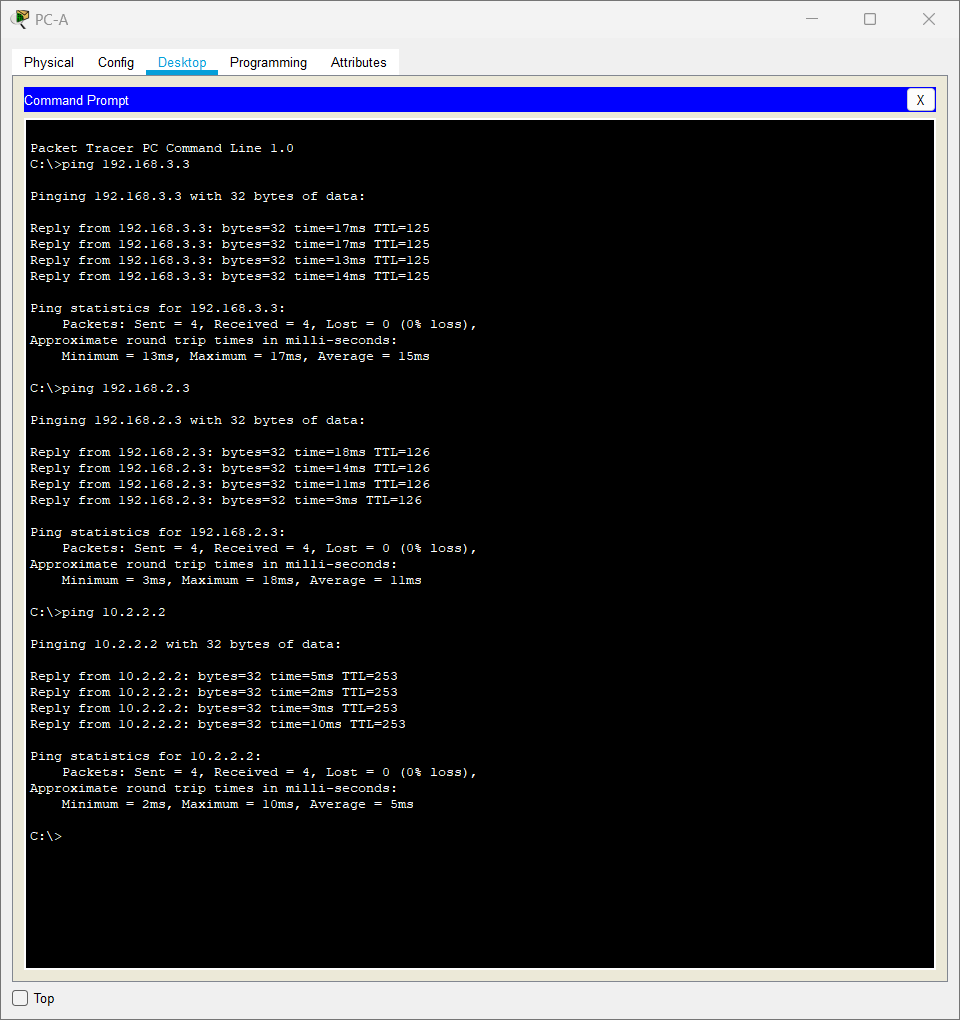
Router(config-router)# network 192.168.0.0

**Part 2 Configure IPsec Parameters on R1**

### Step 1: Test connectivity.

### Ping from PC-A to PC-C.

Ping from pcs



### **Step 2: Enable the Security Technology package.**

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

### **Step 3: Identify interesting traffic on R1.**

R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

### **Step 4 :Configure the IKE Phase 1 ISAKMP policy on R1.**

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 vpnpa55 address 10.2.2.2**

### **Step 5:Configure the IKE Phase 2 IPsec policy on R1.**

Create the transform-set VPN-SET to use **esp-aes** and **esp-sha-hmac**.

**R1(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac**

Create the crypto map VPN-MAP that binds all of the Phase 2 parameters together. Use sequence number 10 and identify it as an ipsec-isakmp map.

R1(config)# **crypto map VPN-MAP 10 ipsec-isakmp**

R1(config-crypto-map)# **description VPN connection to R3**

R1(config-crypto-map)# **set peer 10.2.2.2**

R1(config-crypto-map)# **set transform-set VPN-SET**

R1(config-crypto-map)# **match address 110** R1(config-crypto-map)# **exit**

### **Step 6: Configure the crypto map on the outgoing interface.**

Bind the **VPN-MAP** crypto map to the outgoing Serial 0/0/0 interface.

R1(config)# **interface s0/0/0**

R1(config-if)# **crypto map VPN-MAP**

