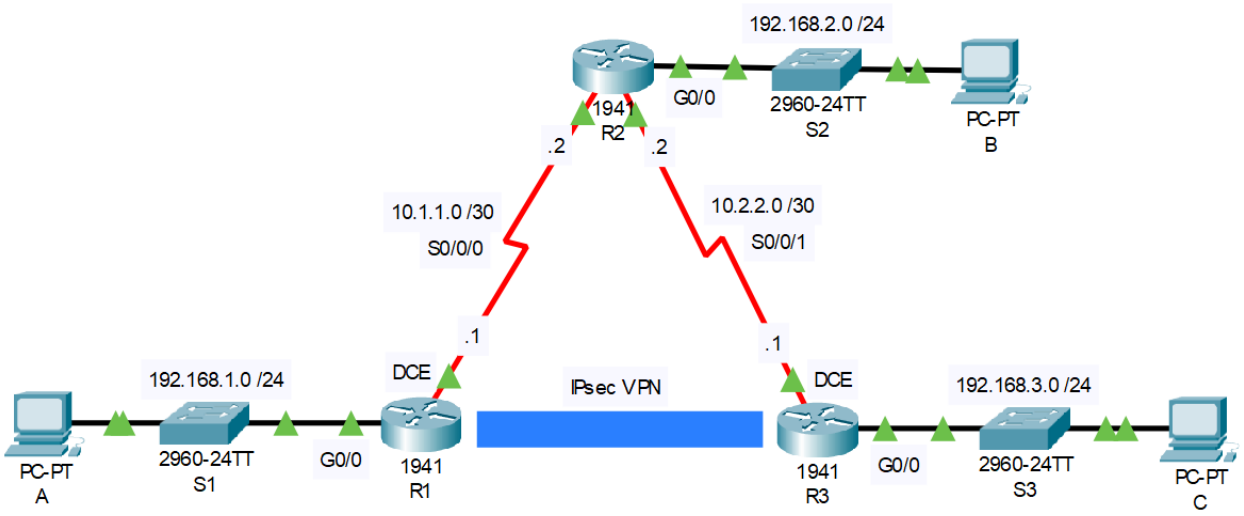
Goal. Use the provided PKT file and configure an IPsec tunnel between routers R1 and R3.

Hostnames, IP addresses and routing are already configured.



R1

1. Check if the "Security Technology package" license is activated, check router model version:

```
R1#show version
```

2. Activate the "securityk9" module:

```
R1(config)#license boot module c1900 technology-package securityk9
R1(config)#end
R1#copy running-config startup-config
R1#reload
```

3. After reboot, accept the license by typing in "yes".

4. Repeat the process on router R3.

5. Create an Access List that will select the packets for the tunnel:

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

6. ISAKMP, phase 1 configuration. In this phase, the two routers negotiate the terms of further communication, or otherwise known as "SA".

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2

R1(config)#crypto isakmp key cisco address 10.2.2.1
```

7. ISAKMP, phase 2 configuration. In this phase, the routers are communicating according to the terms agreed in phase 1, and they're now negotiating on the parameters of the actual communication (regular network traffic flowing through the tunnel).

```
R1(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)# description VPN connection to R3
R1(config-crypto-map)# set peer 10.2.2.1
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# exit
```

8. Connecting the crypto-map with the interface connecting to the other end of the IPsec tunnel:

```
R1(config)# interface S0/0/0
R1(config-if)# crypto map VPN-MAP
```

R3

```
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255


R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)# exit
R3(config)# crypto isakmp key cisco address 10.1.1.1


R3(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
R3(config-crypto-map)# description VPN connection to R1
R3(config-crypto-map)# set peer 10.1.1.1
R3(config-crypto-map)# set transform-set VPN-SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)# exit


R3(config)# interface S0/0/1
R3(config-if)# crypto map VPN-MAP
```