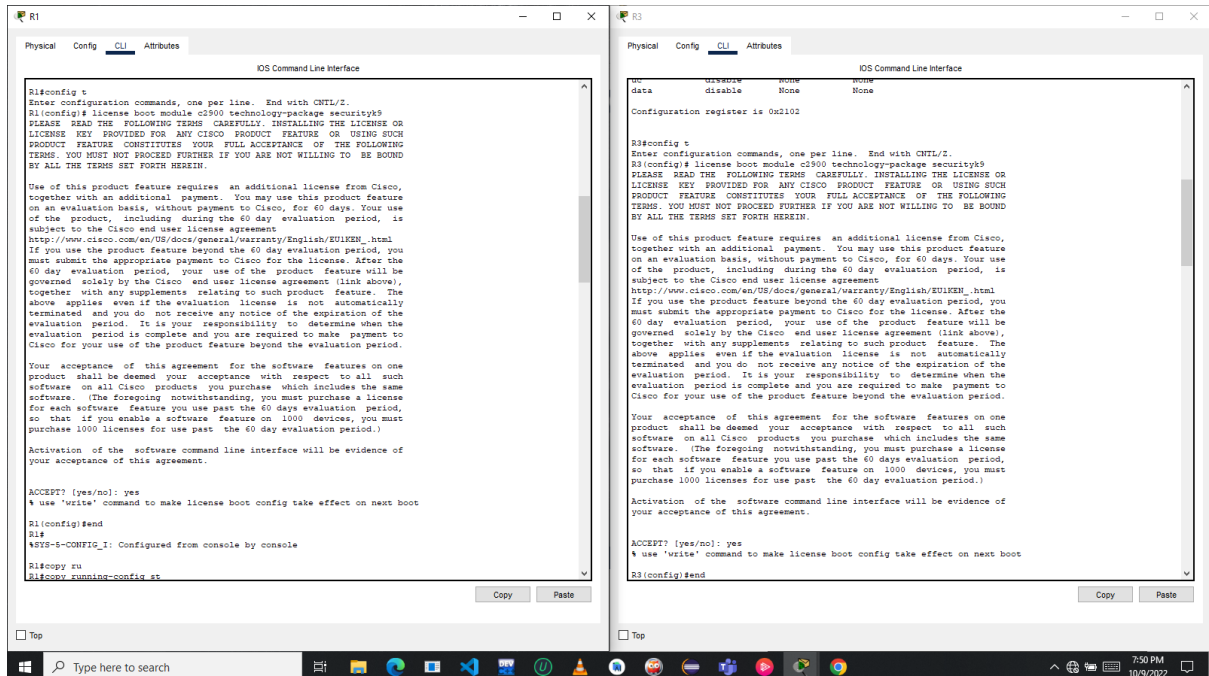


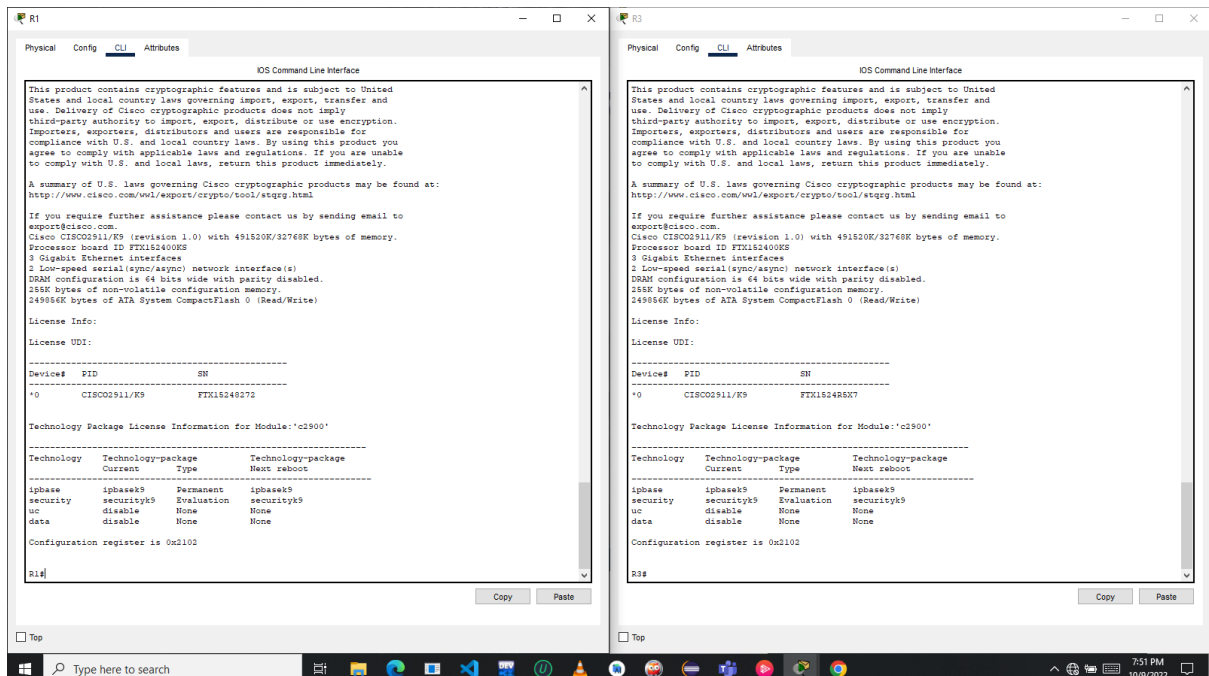
Packet Tracer – Configuring VPNs

Part 1: Enable Security Features

Step 1: Activate securityk9 module.



Issue the show version command

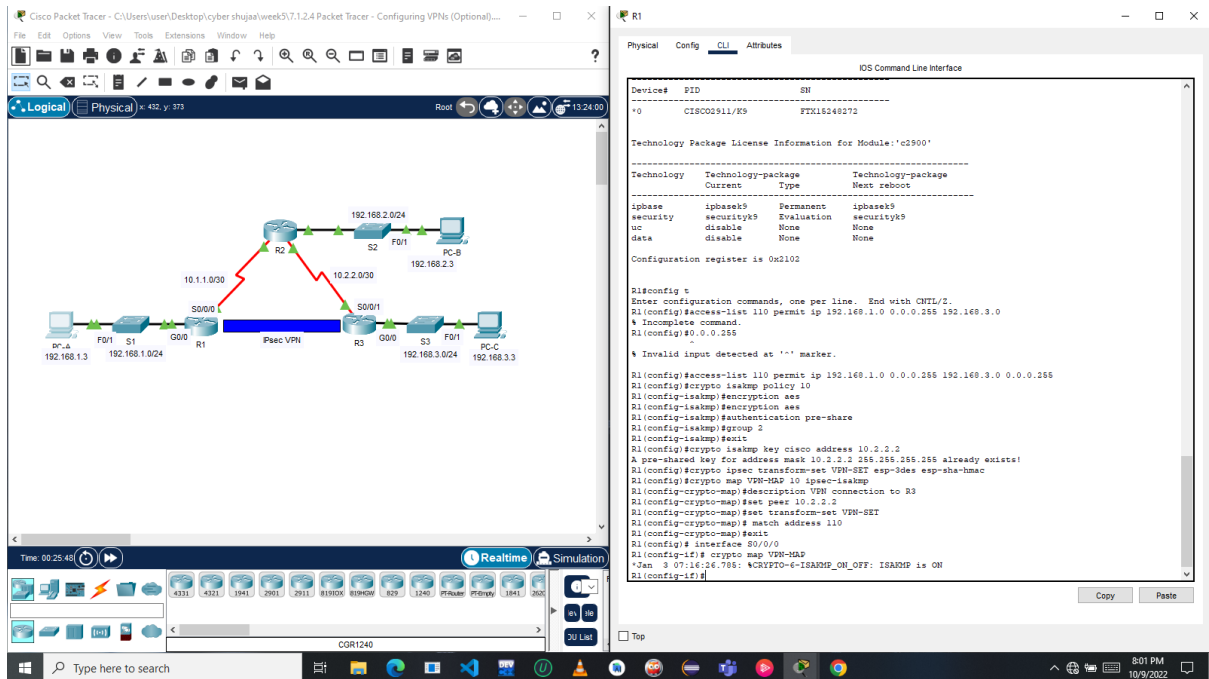


Part 2: Configure IPsec Parameters on R1

Configure the ISAKMP Phase 1 properties on R1.

Configure the ISAKMP Phase 2 properties on R1

Configure the crypto map on the outgoing interface.

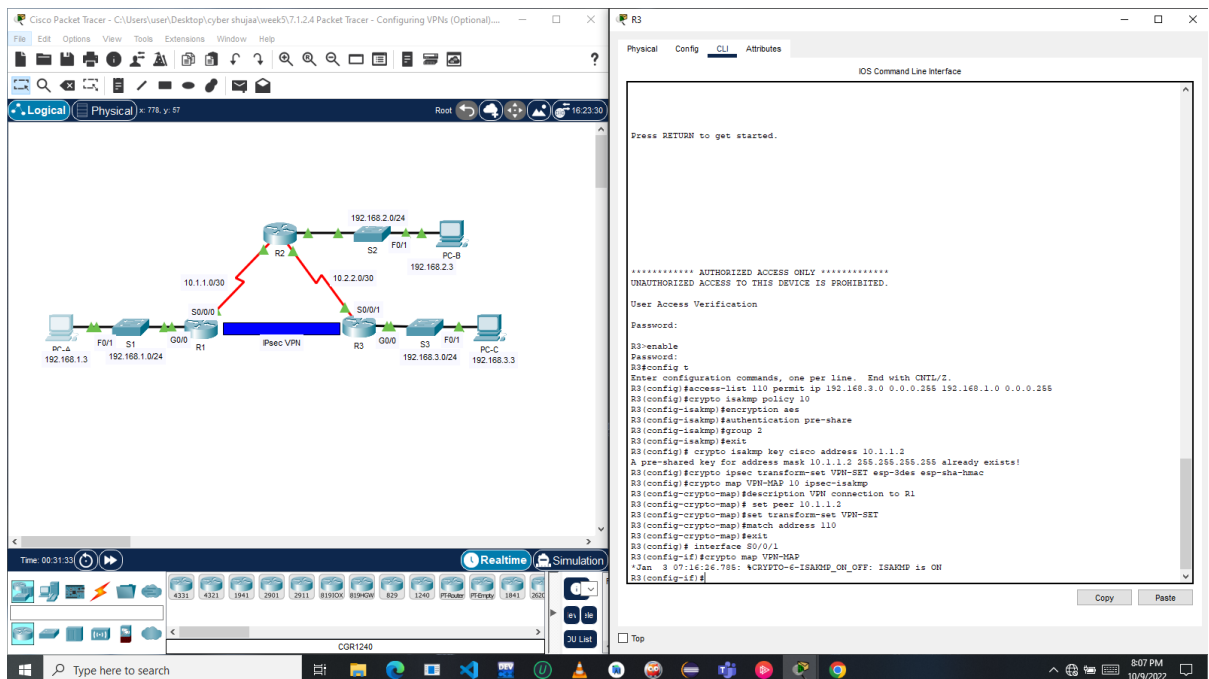


The image shows a Cisco Packet Tracer network diagram and the configuration window for router R1. The network diagram illustrates a VPN setup with three routers: R1, R2, and R3. R1 is connected to R2 via a serial link (S0/0/0 to S0/0/1) with IP addresses 10.1.1.0/30 and 10.2.2.0/30. R2 is connected to R3 via a serial link (S2 to S3) with IP addresses 192.168.2.0/24 and 192.168.3.0/24. R1 is also connected to a PC-A (192.168.1.3) via a fast Ethernet link (F0/1 to F0/0/0). R3 is connected to a PC-C (192.168.3.3) via a fast Ethernet link (F0/1 to F0/0/0). The VPN is configured on R1 and R3. The configuration window for R1 shows the following commands:

```
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#exit
R1(config)#crypto isakmp key cisco address 10.2.2.2
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 10.2.2.2
R1(config-crypto-map)#set transform-set VPN-SET
R1(config-crypto-map)#match address 110
R1(config-crypto-map)#exit
R1(config)#interface S0/0/0
R1(config-if)# crypto map VPN-MAP
R1(config-if)#
R1(config-if)#
```

Part 3: Configure IPsec Parameters on R3

Configure the ISAKMP Phase 1 properties on R3.



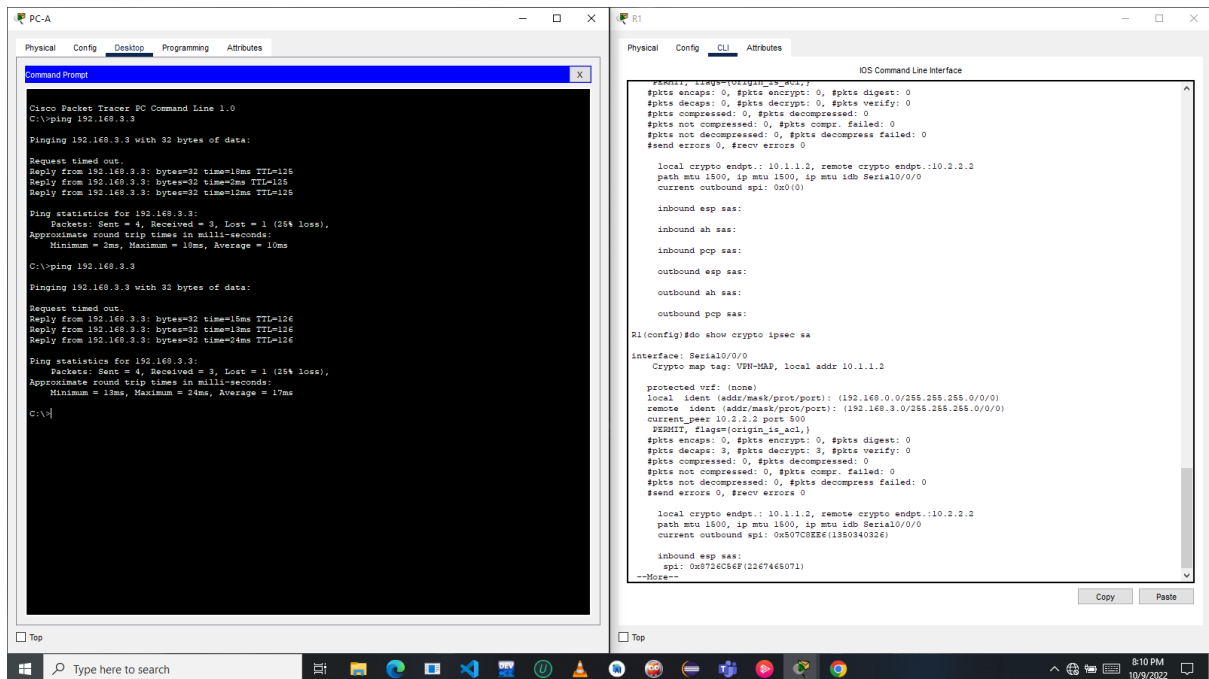
The image shows a Cisco Packet Tracer network diagram and the configuration window for router R3. The network diagram is identical to the one in Part 2. The configuration window for R3 shows the following commands:

```
R3#enable
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
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 10.1.1.2
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 10.1.1.2
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
R3(config-if)#
R3(config-if)#
```

Part 4: Verify the IPsec VPN

Step 1: Verify the tunnel prior to interesting traffic.

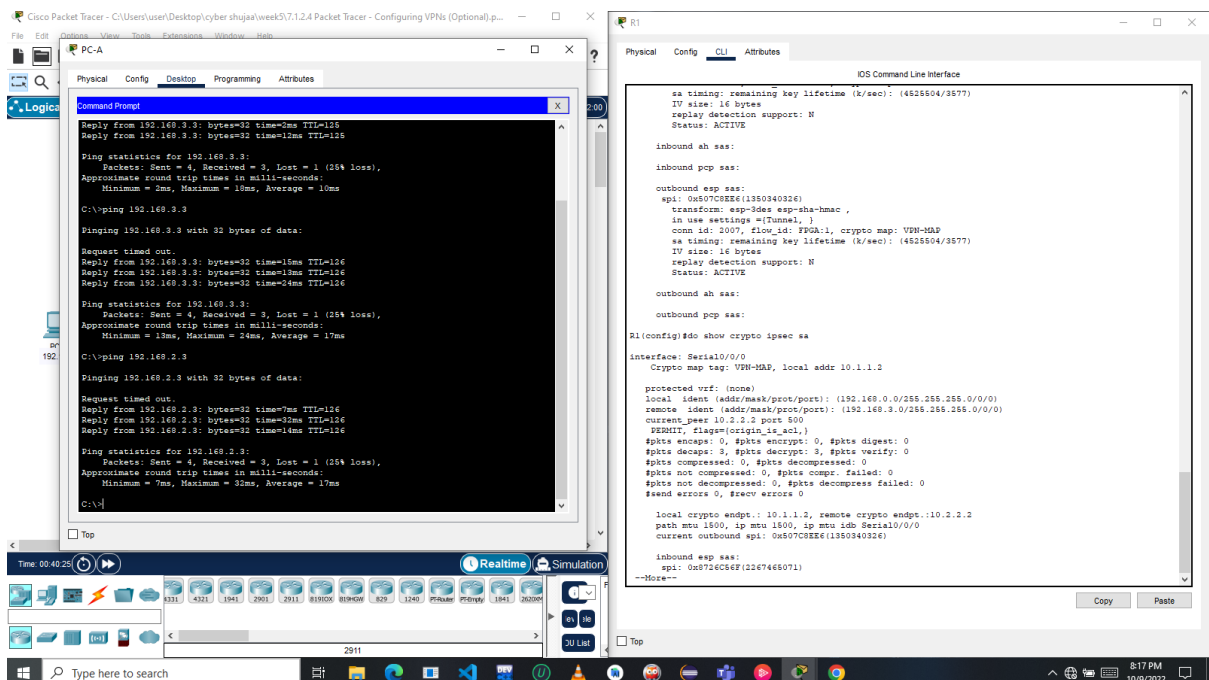
Ping PC-C from PC-A



Step 4: Create uninteresting traffic.

Ping PC-B from PC-A.

Verify the tunnel



Cisco Packet Tracer - C:\Users\user\Desktop\cyber shujaa\week5\7.1.2.4 Packet Tracer - Configuring VPNs (Optional).pkt

File Edit Options View Tools Extensions Window Help

Logical Physical 1385 yr 550

Time: 00:40:57

Scenario 0

Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete

Successful	PC-A	PC-C	ICMP	0.000	N	0	(edit)	(delete)
Successful	PC-A	PC-B	ICMP	0.000	N	1	(edit)	(delete)
Successful	PC-C	PC-B	ICMP	0.000	N	2	(edit)	(delete)
Successful	PC-A	R2	ICMP	0.000	N	3	(edit)	(delete)

2911

Type here to search

8:17 PM 10/9/2022