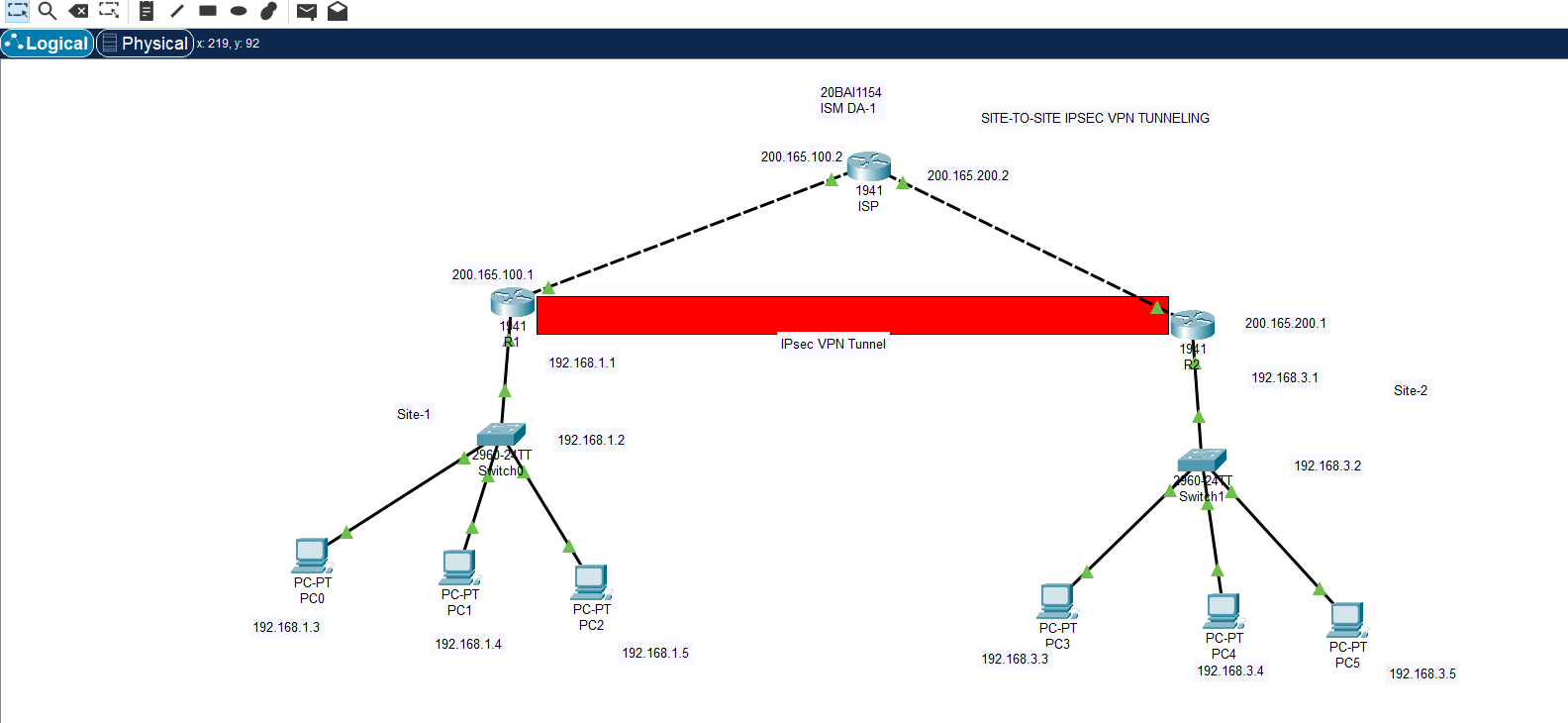
**Name: Shangirne Kharbanda**

**Reg, No, : 20BAI1154**

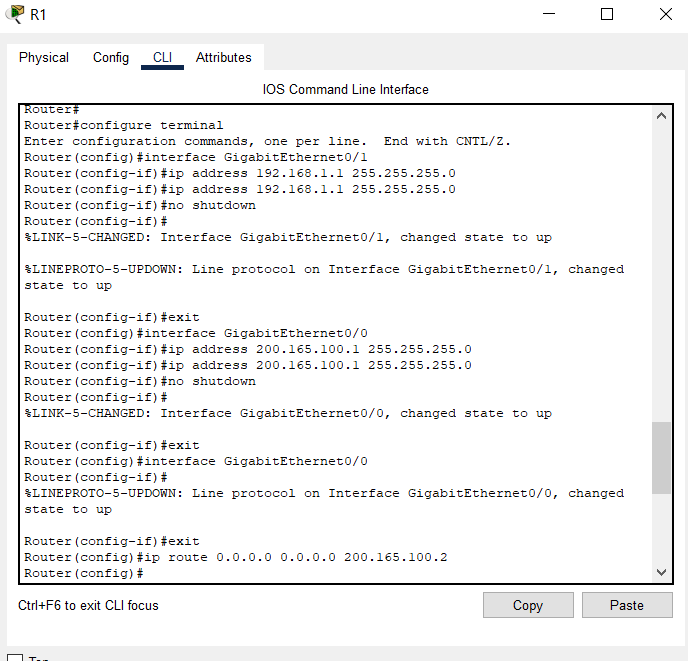
**LAB – 5**

**VPN**

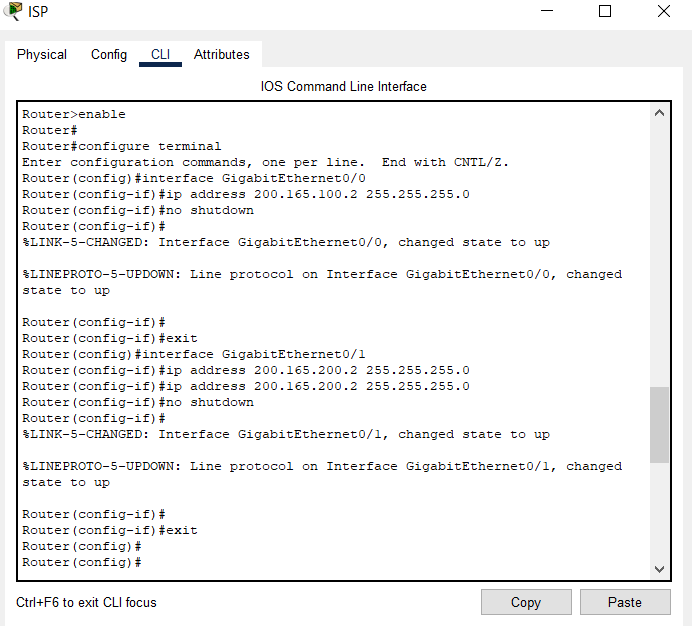
The topology created will be as follows:



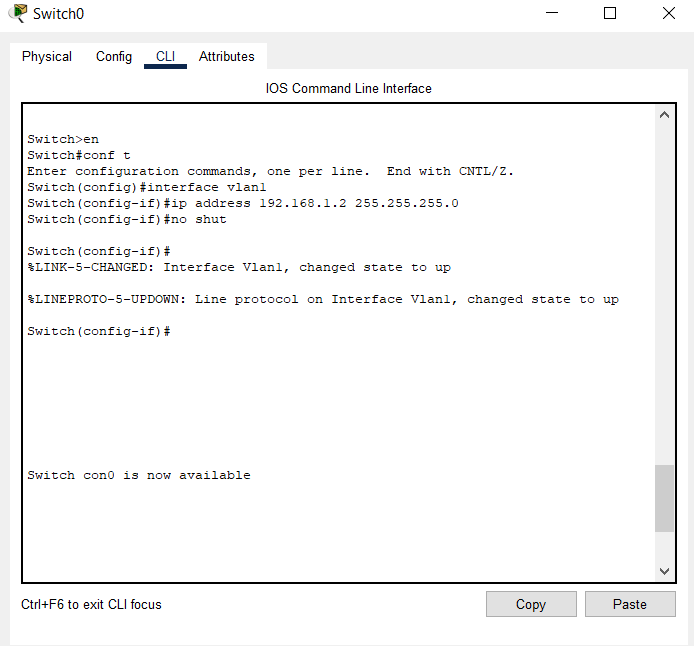
The router R1 for Site-1 will be configured as follows and similarly R2 for Site-2.



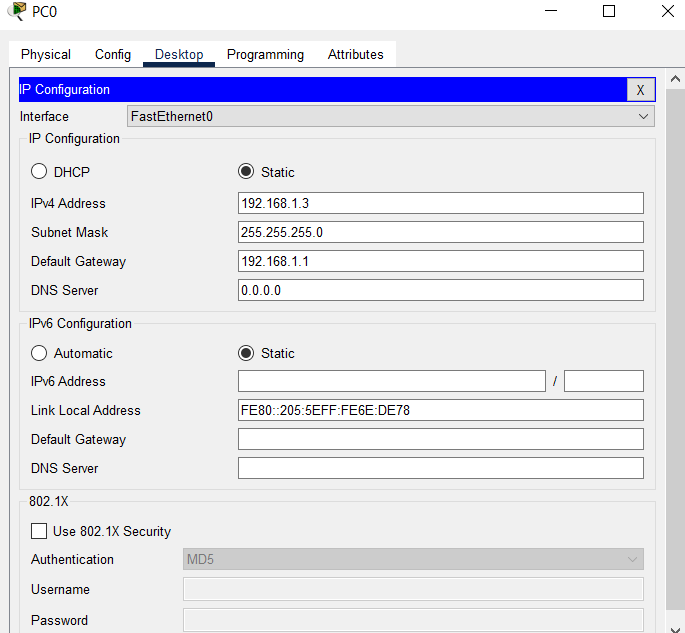
The router ISP will be configured as follows:



The switches will be configured as follows:



PCs will be configured and assigned IP addresses as follows:



Now we will begin configuring IPsec VPN tunnel from site-1 to site-2.

**We will follow 5 phases in completing this task, which include:**

**IPsec VPN:**

**1.ACL**

**2.ISAKMP policy(PHASE 1)**

**3.IPsec transform-set(PHASE 2)**

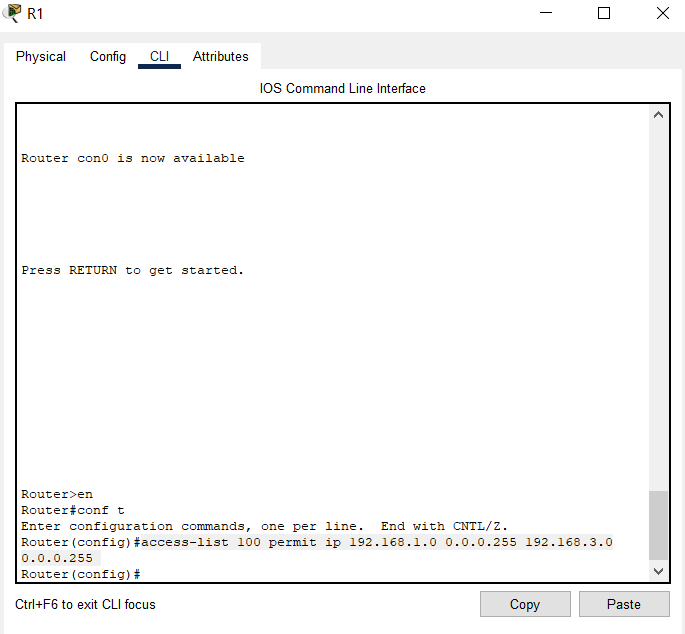
**4. Crypto map**

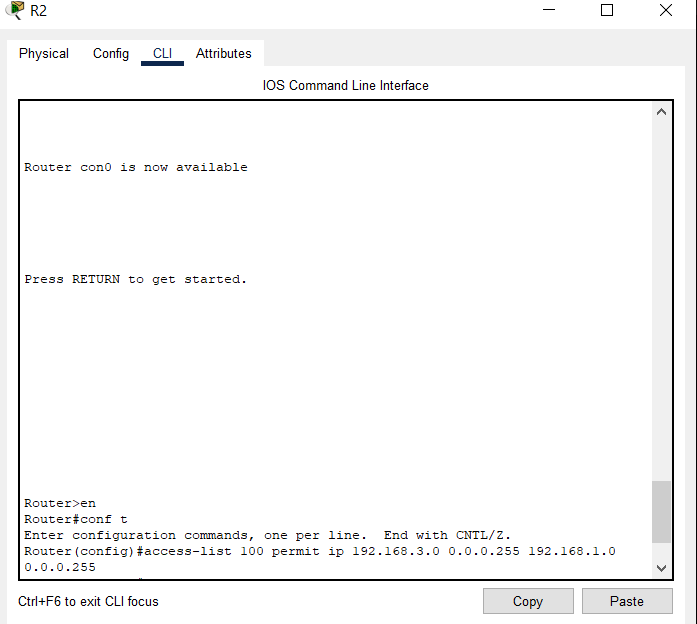
**5. Applying the crypto map on the relevant interfaces**

**1. ACL**

Access Control lists will be first applied on routers R1 and R2 to control the flow of communication.

First we will begin by configuring ACL on our Router R1.

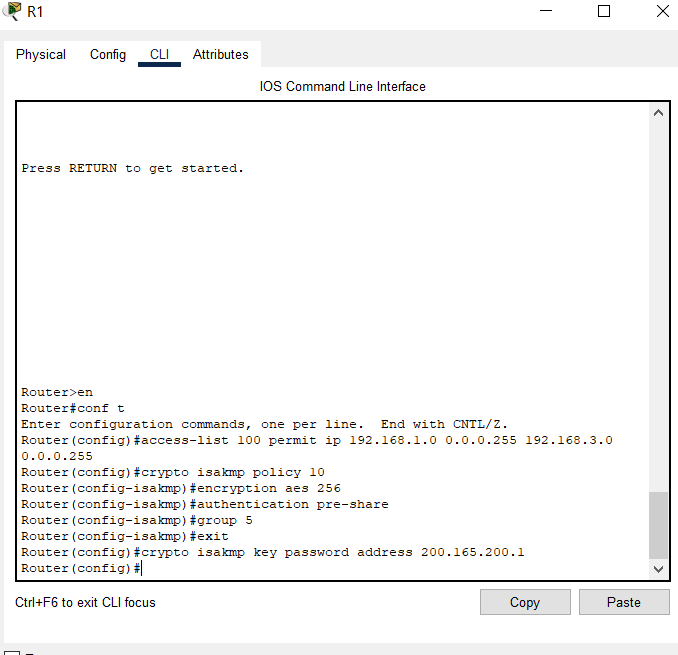


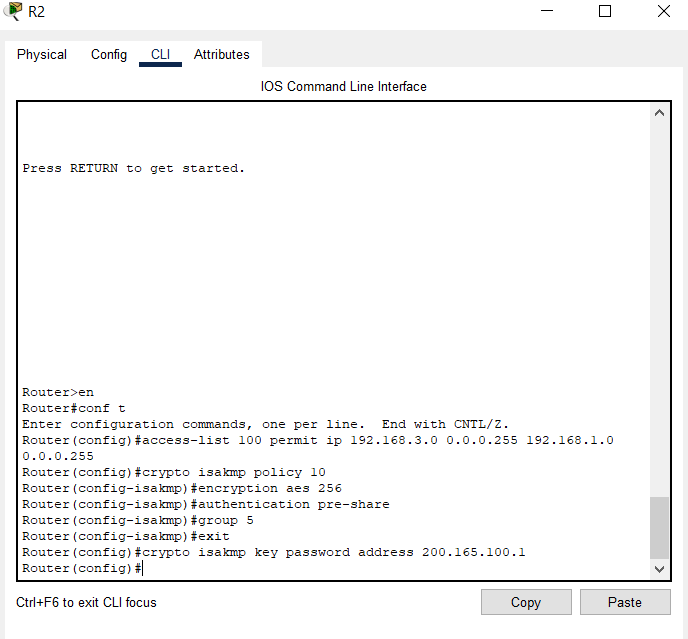


**2.ISAKMP policy (PHASE 1)**

This phase 1 ISAKMP policy sets up the key authentication and effectively the tunnel.

It will be applied on the routers on both sites R1 and R2 as follows:

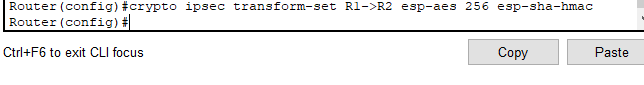




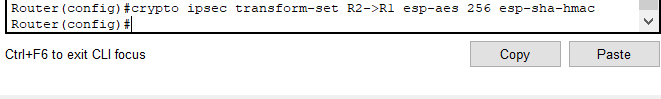
**3. IPsec transform set (PHASE 2)**

This Phase 2 IPsec transform set sets up the tunnel for transferring the data and the encryption and protocols used.

For R1:



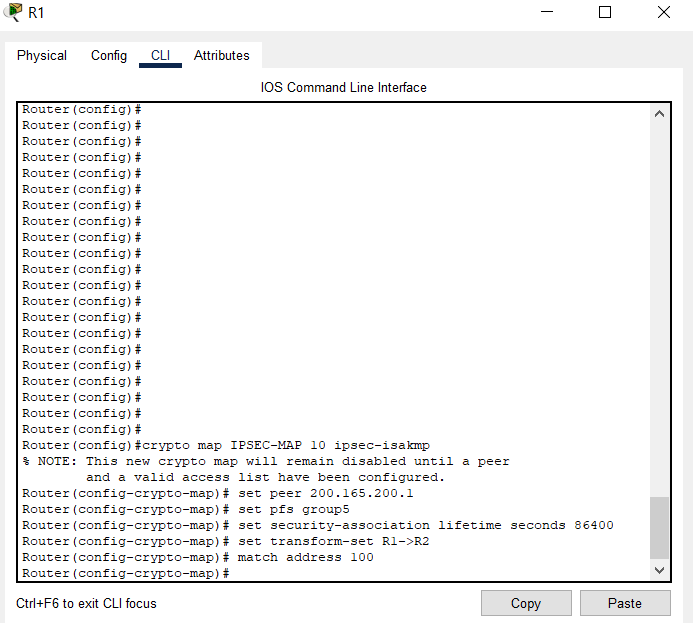
For R2:

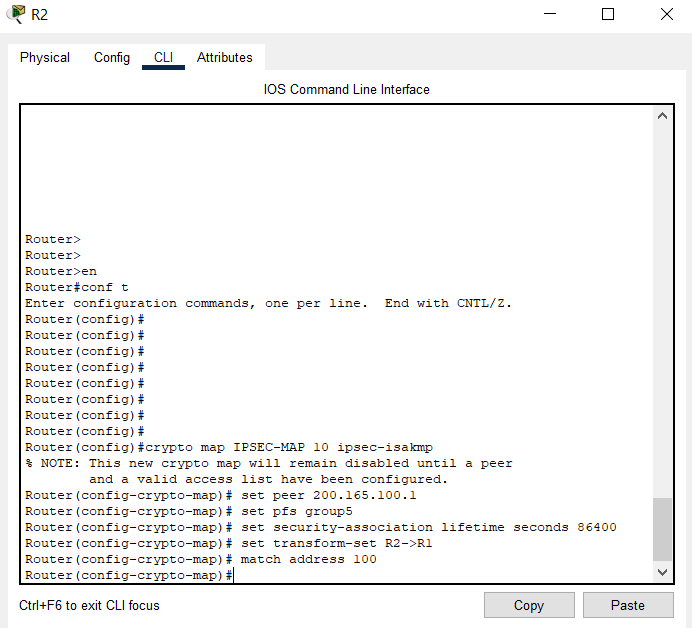


**4. Crypto map**

A crypto map ties everything together to have Perfect forward secrecy, transform sets applied, acls applied and peer address applied to the interface.

It is applied on R1 and R2 on both sites as follows:

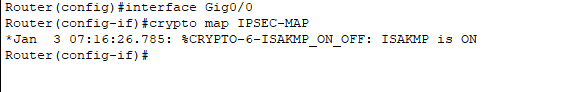




**5. Applying the crypto map on the relevant interfaces.**

We apply the crypto map we constructed on the relevant interfaces. This will be done as follows on R1 and R2:

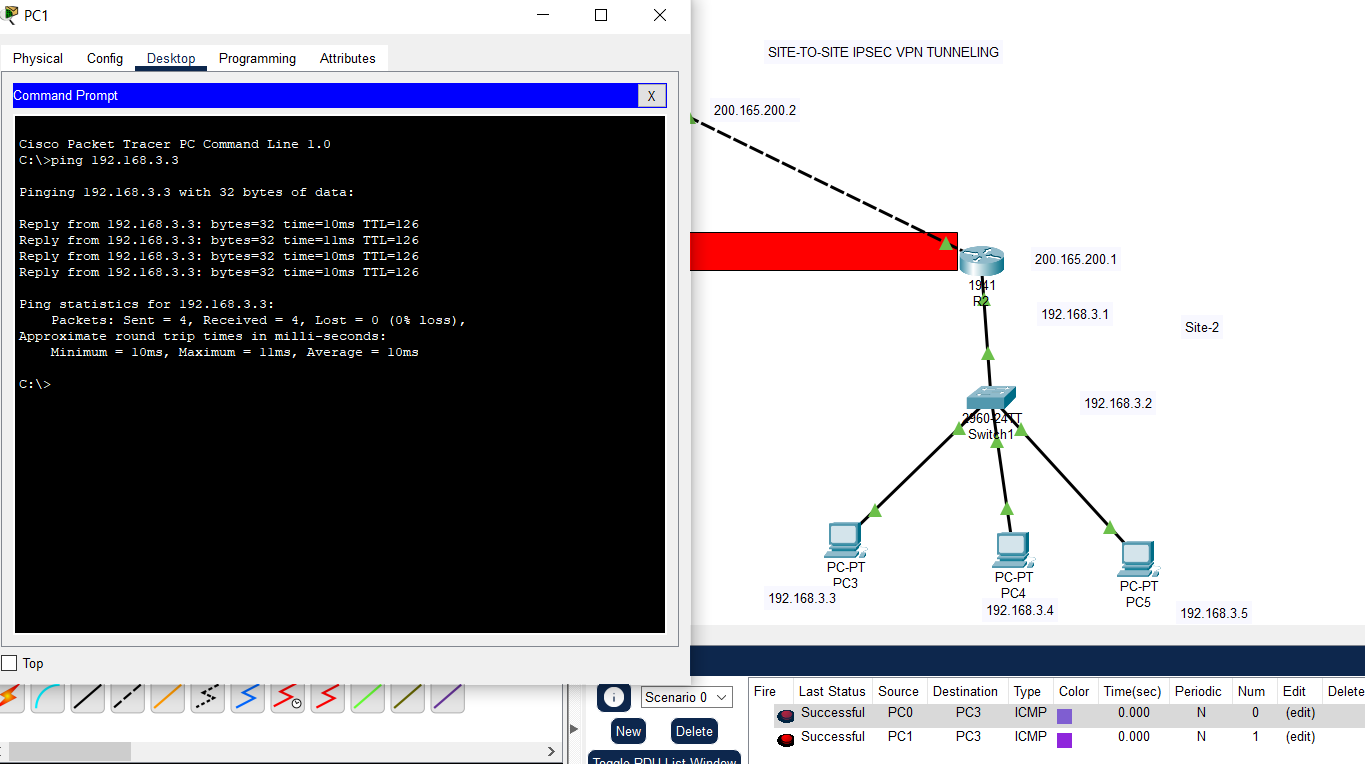
For both the routers R1 and R2, we are going to apply the crypto map IPSEC-MAP on interface Gig0/0.



Now that our 5 phases are complete, we have implemented Site-to-site IPsec VPN tunnelling.

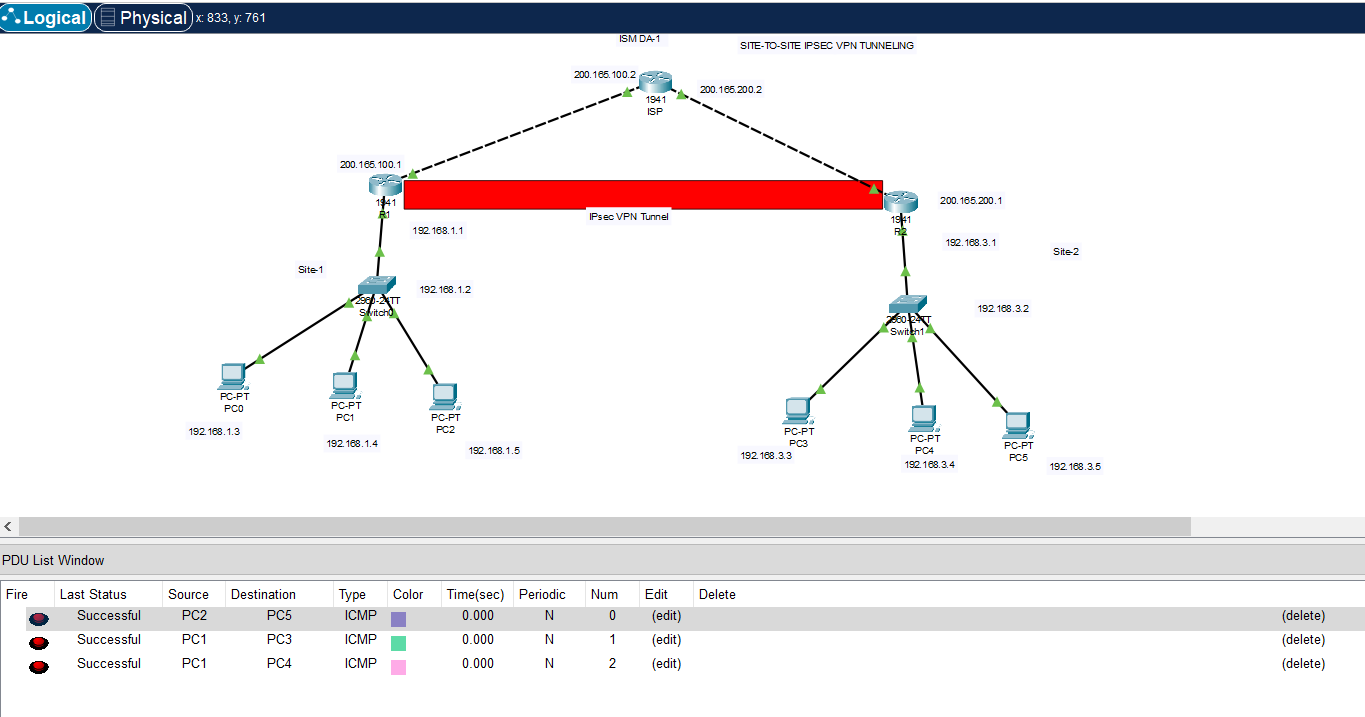
Lets see if it works.

We will try pinging across the network from PC-1(192.168.1.4) to PC-3 (192.168.3.3) and it should work.



The message sent goes throw the IPsec tunnelling across the network through the tunnel and not through the ISP router.

The ISP router has no idea that 192.168.1.0/24 and 192.168.3.0/24 networks even exist.



We can see that the messages are going through.

Therefore we have successfully implemented VPN in this Lab exercise.