**Name: Shangirne Kharbanda**

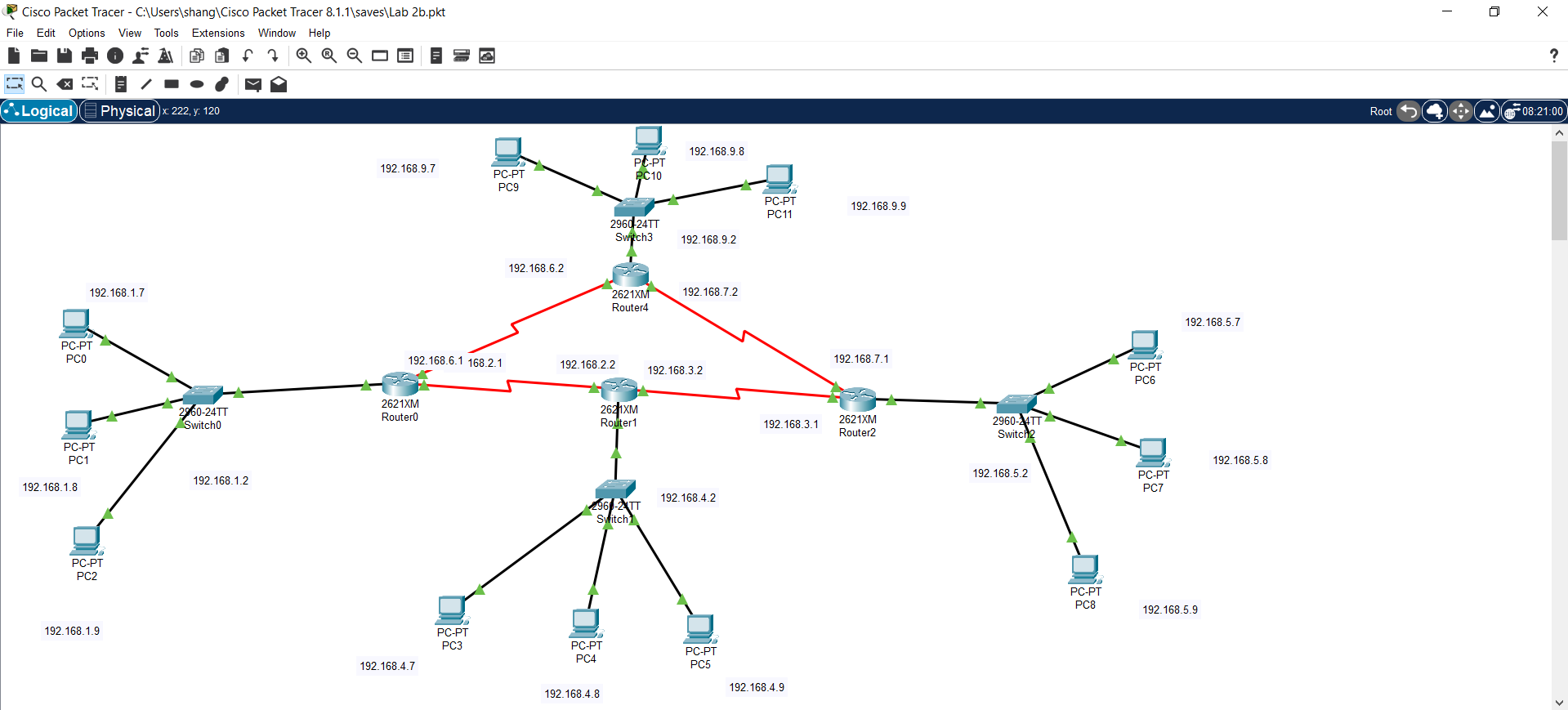
**Registration Number: 20BAI1154**

**ISAA LAB-2**

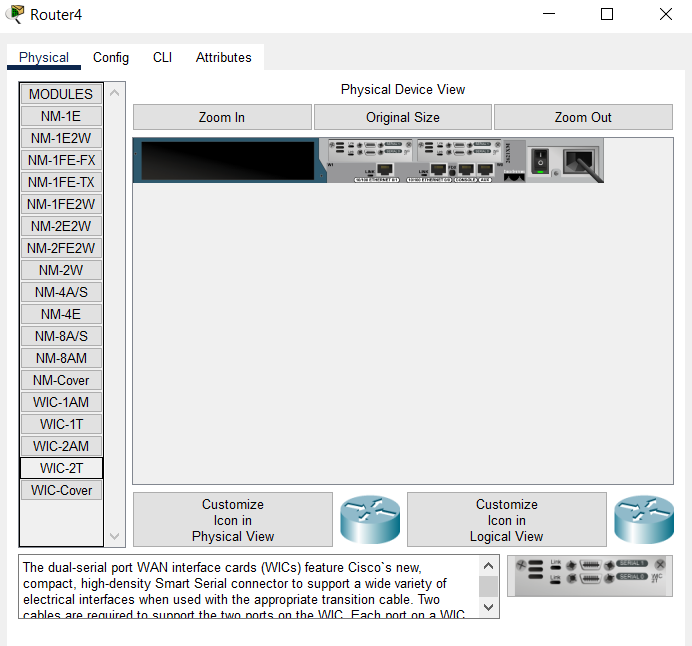
**STANDARD AND EXTENDED ACL**

**STANDARD ACL:**

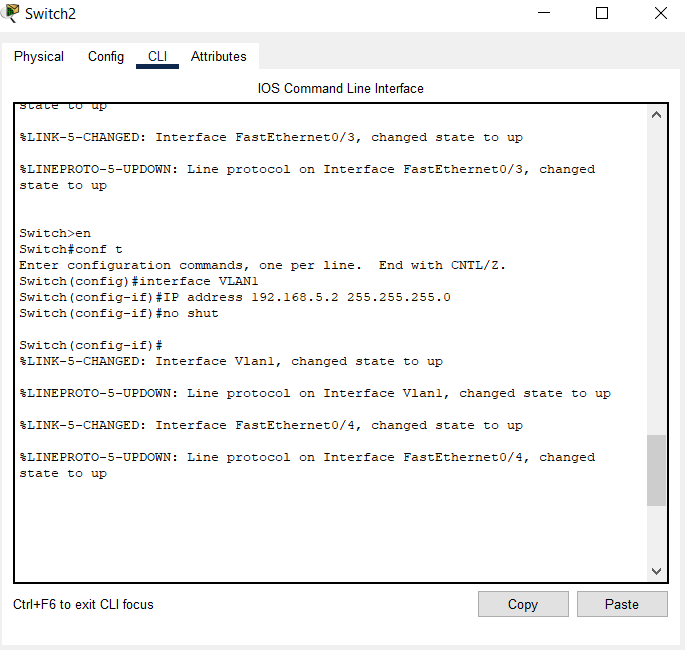
First, create a topology as shown in the following screenshot.



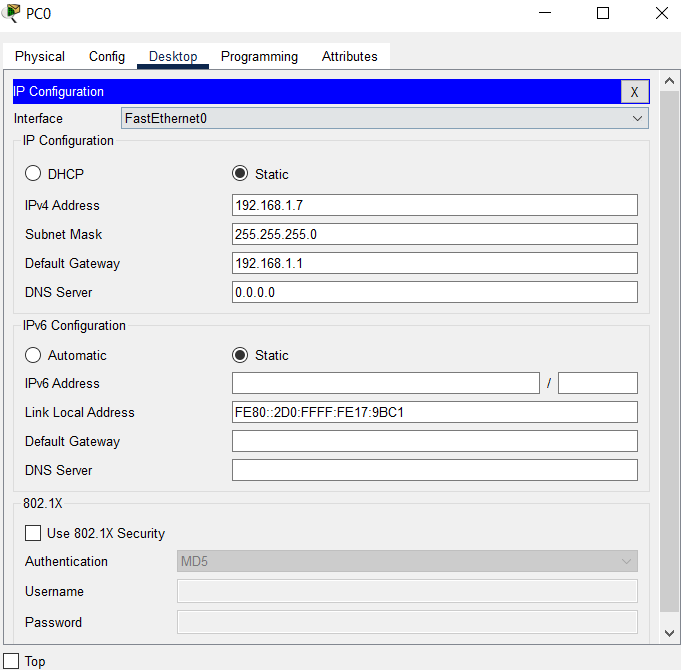
Connect all the switches, routers and PCs. When connecting routers, make sure it’s a serial connection. For that, turn off each router and change its physical configuration to WIC-1T or WIC-2T.



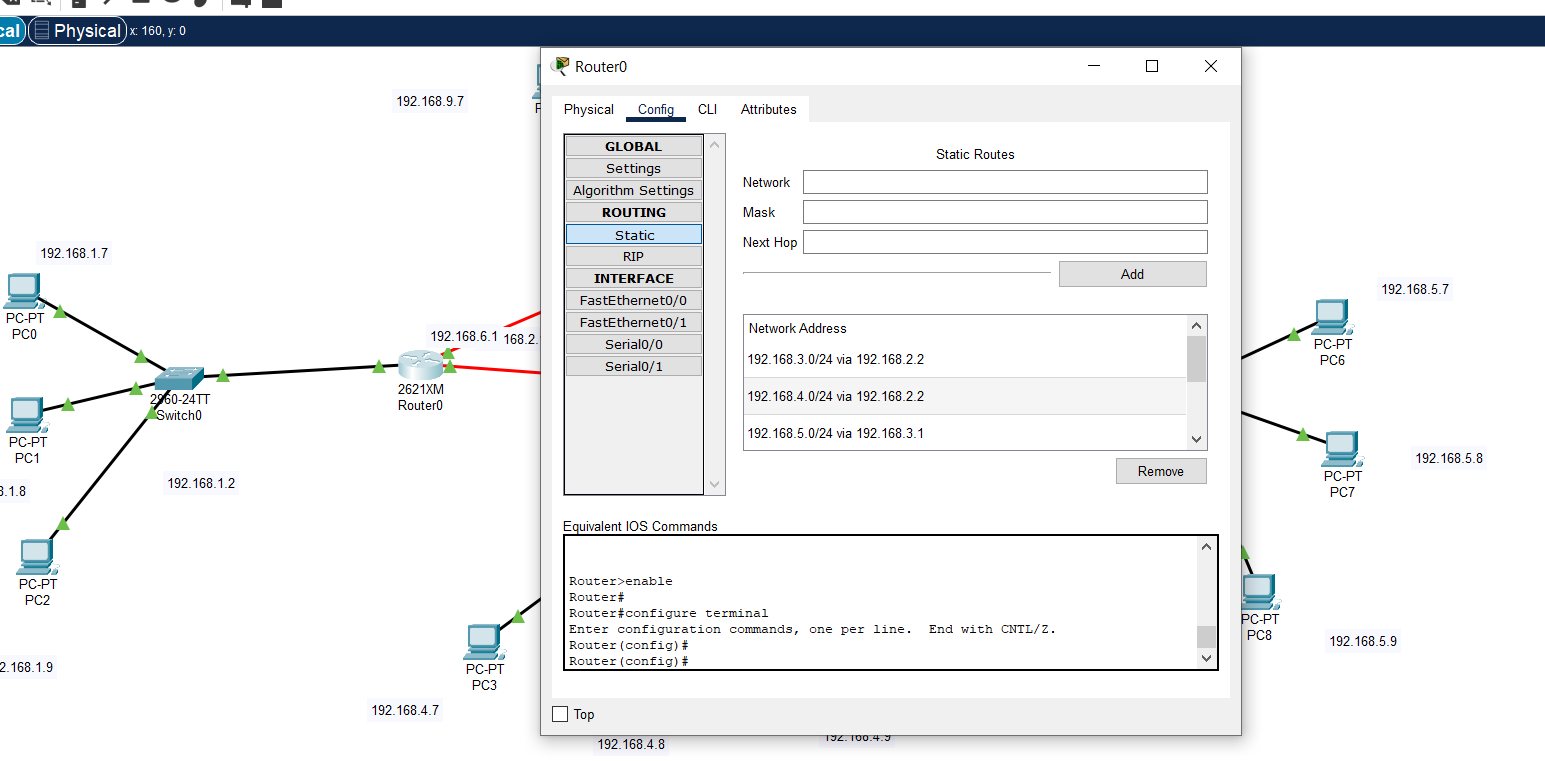
Configure the switches using CLI in the following manner:



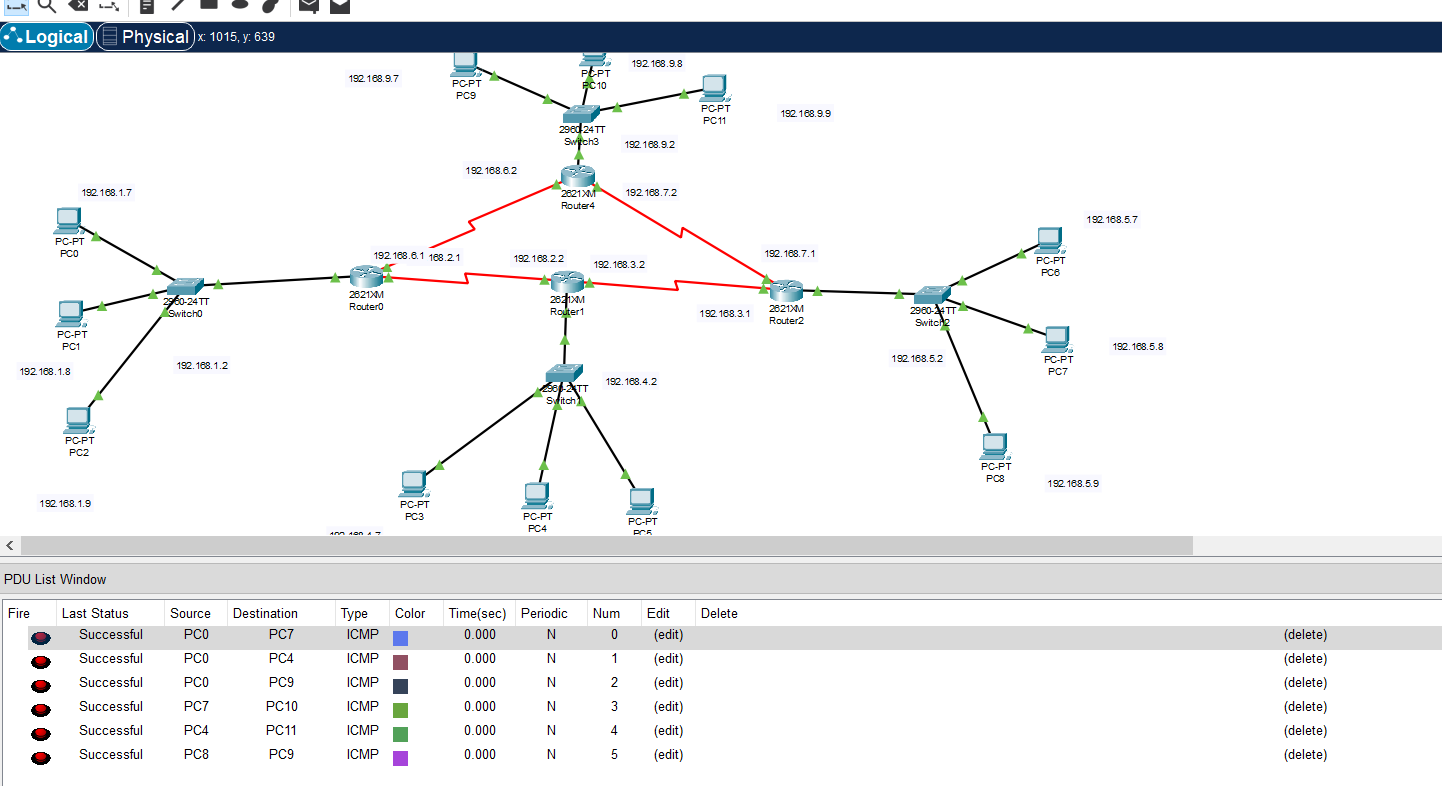
Assign IPs and default gateway to the PCs.



After that, to establish a connection between all the networks, create routing tables for all the routers using the IP route command in the CLI.

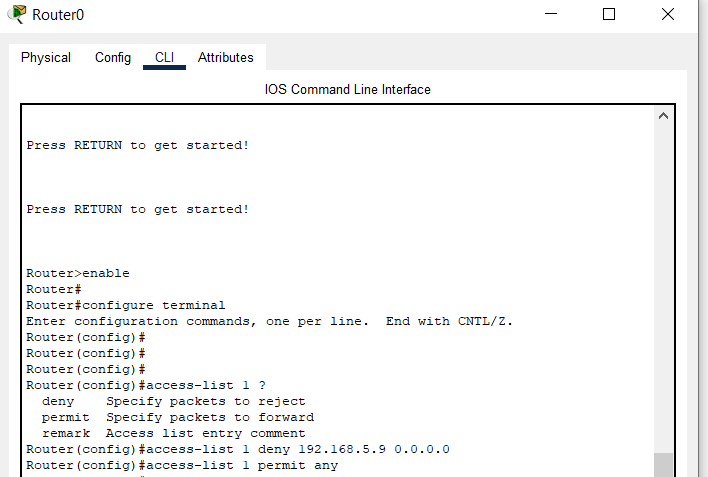


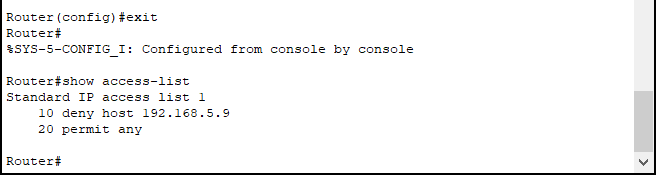
After that, a successful connection is established between all the networks as we can see in the screenshot below.



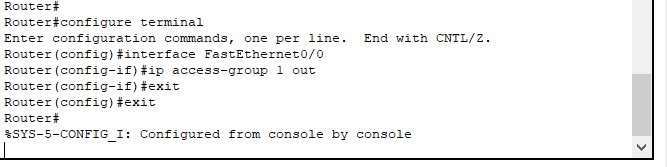
Now, we want to deny PC8 i.e 192.168.5.9 connection to 192.168.1.0/24 and permit everything else using a Standard ACL. So lets do that.

First we configure a ACL in Router0.

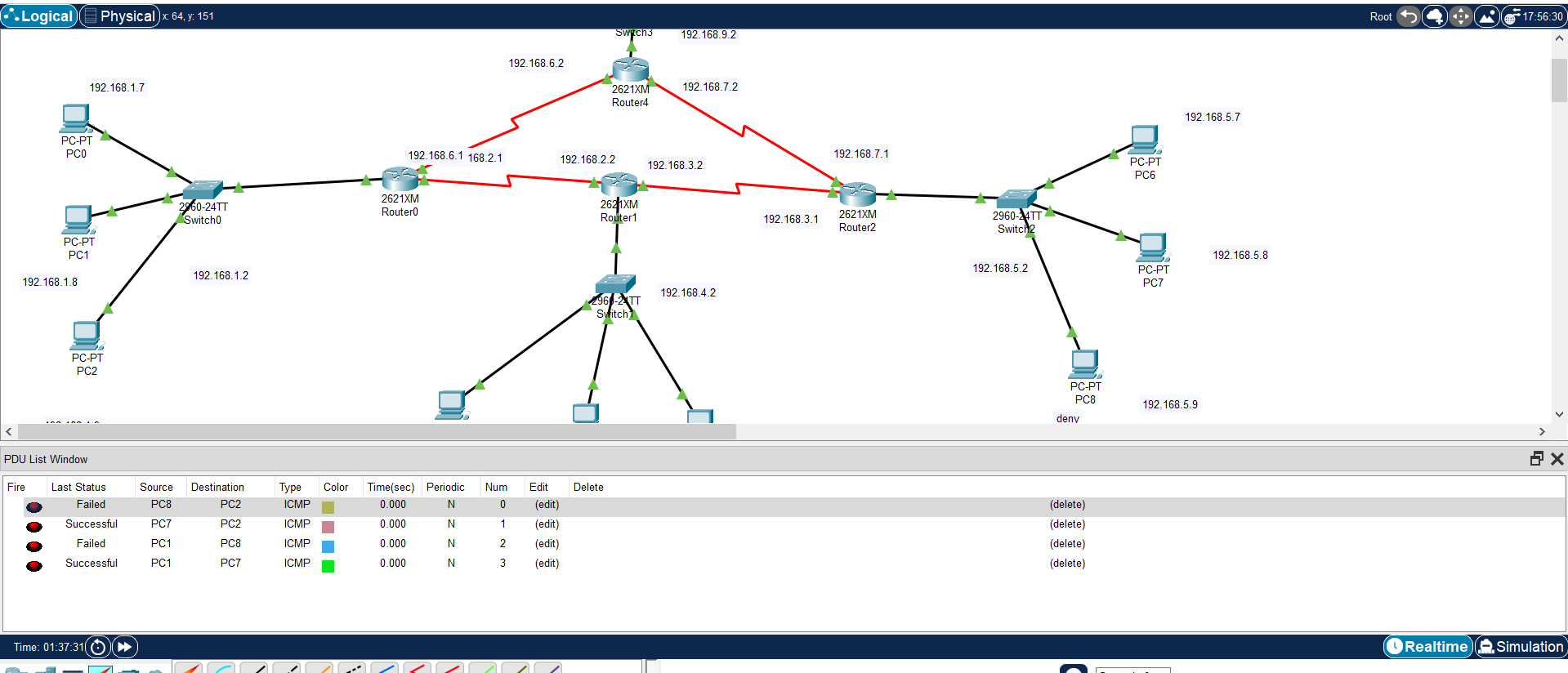


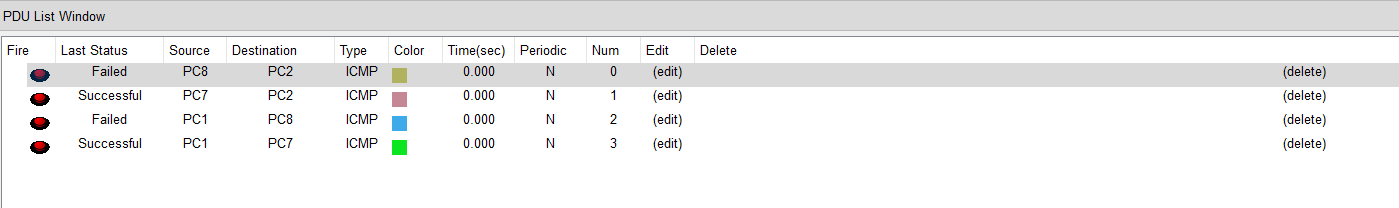


Now we apply the access-list to the interface Fa0/0 outbound.



Now we can note that PC8 that is 192.168.5.9 cannot connect to the network 192.168.1.0/24 and every other PC can.



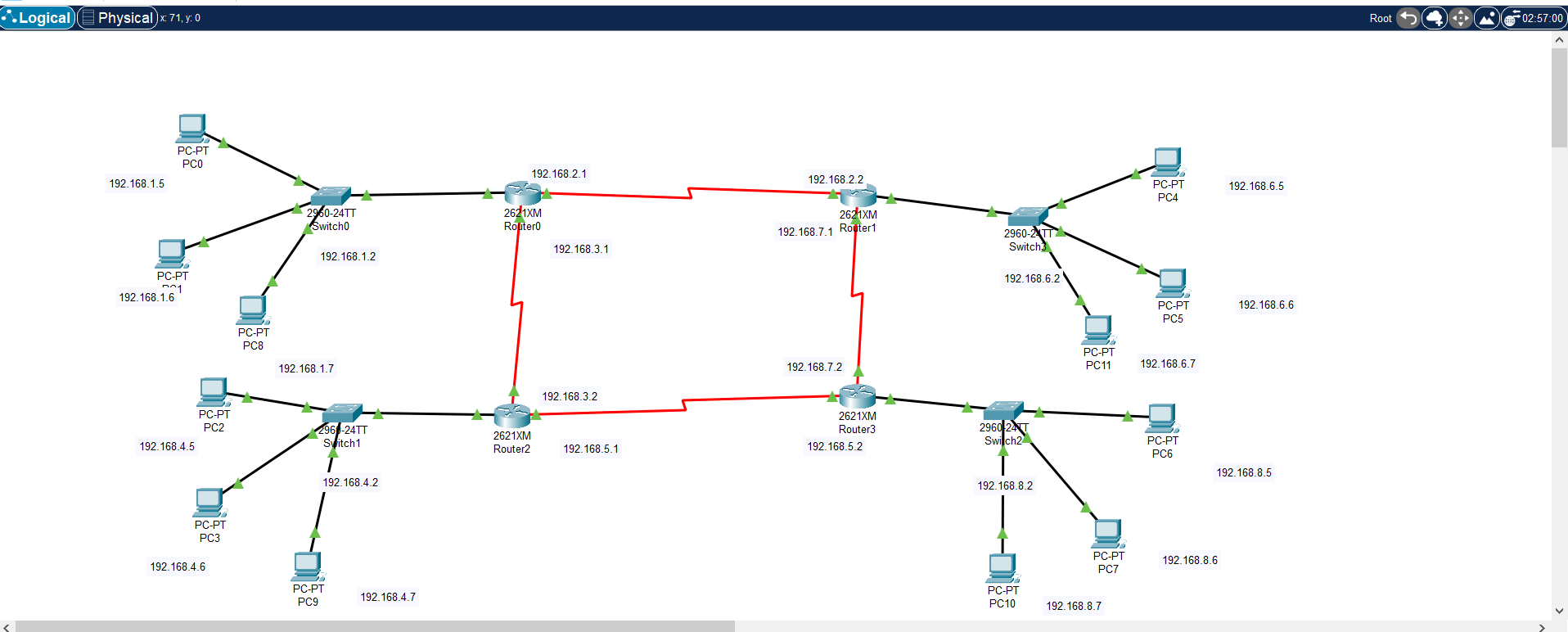


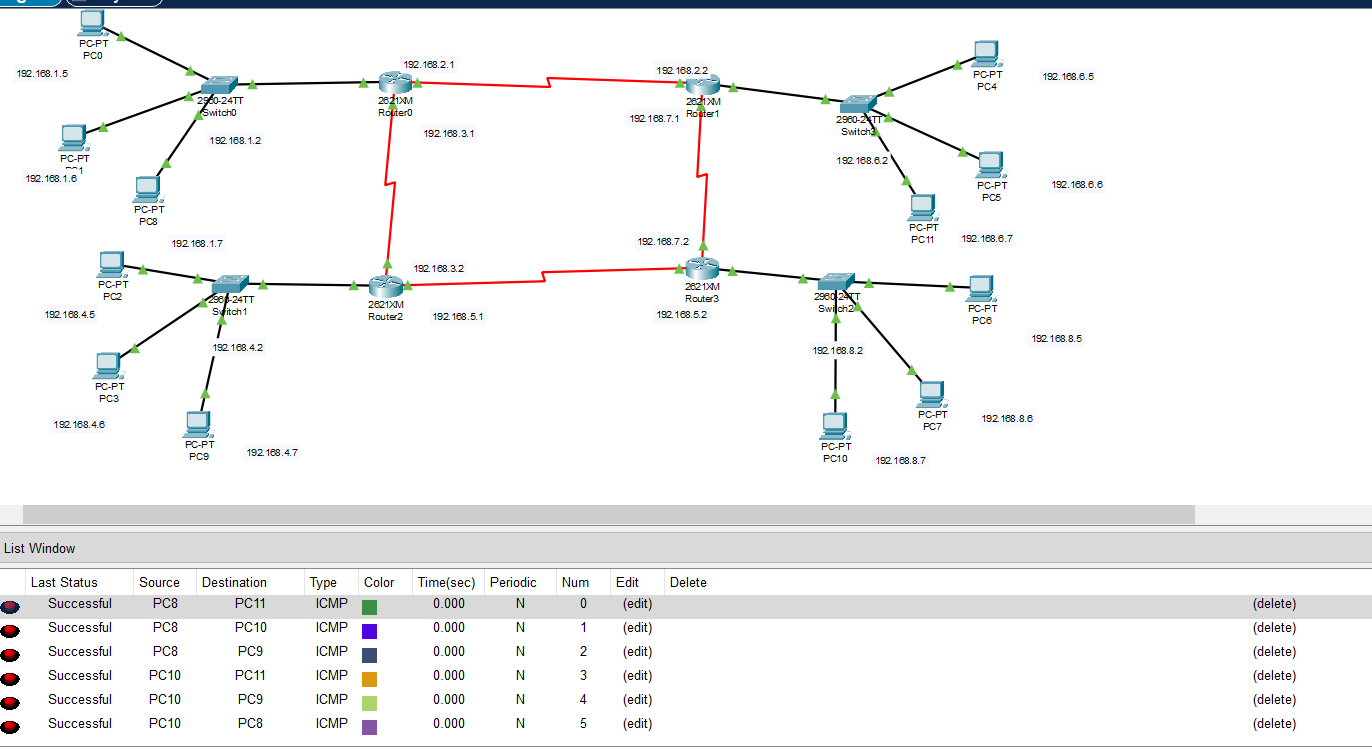
We have successfully used a Standard ACL to its intent.

**EXTENDED ACL:**

For Extended ACL, create the following topology and configure all the routers, switches and end devices like discussed before.

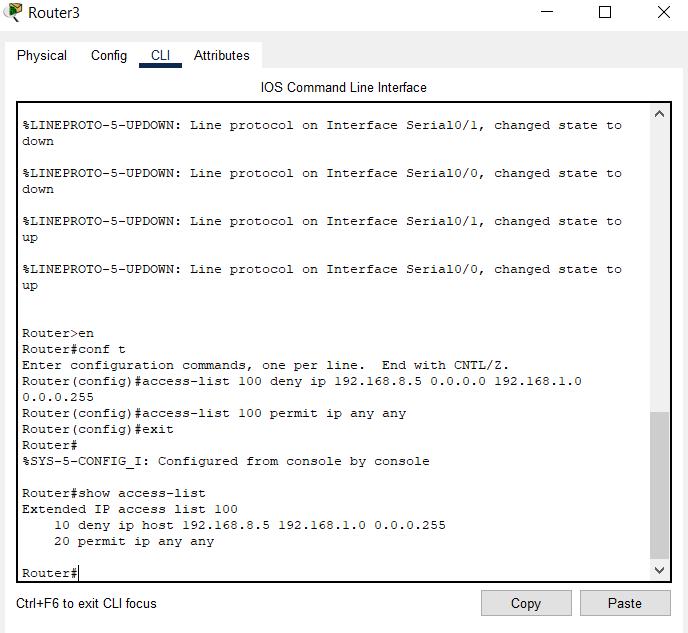
Also establish a connection between all the networks using IP route and creating routing tables for all routers like discussed before.



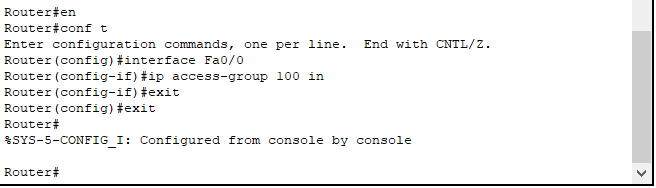


Now we will try to deny PC6 192.168.8.5 access to the network 192.168.1.0/24 using an Extended ACL.

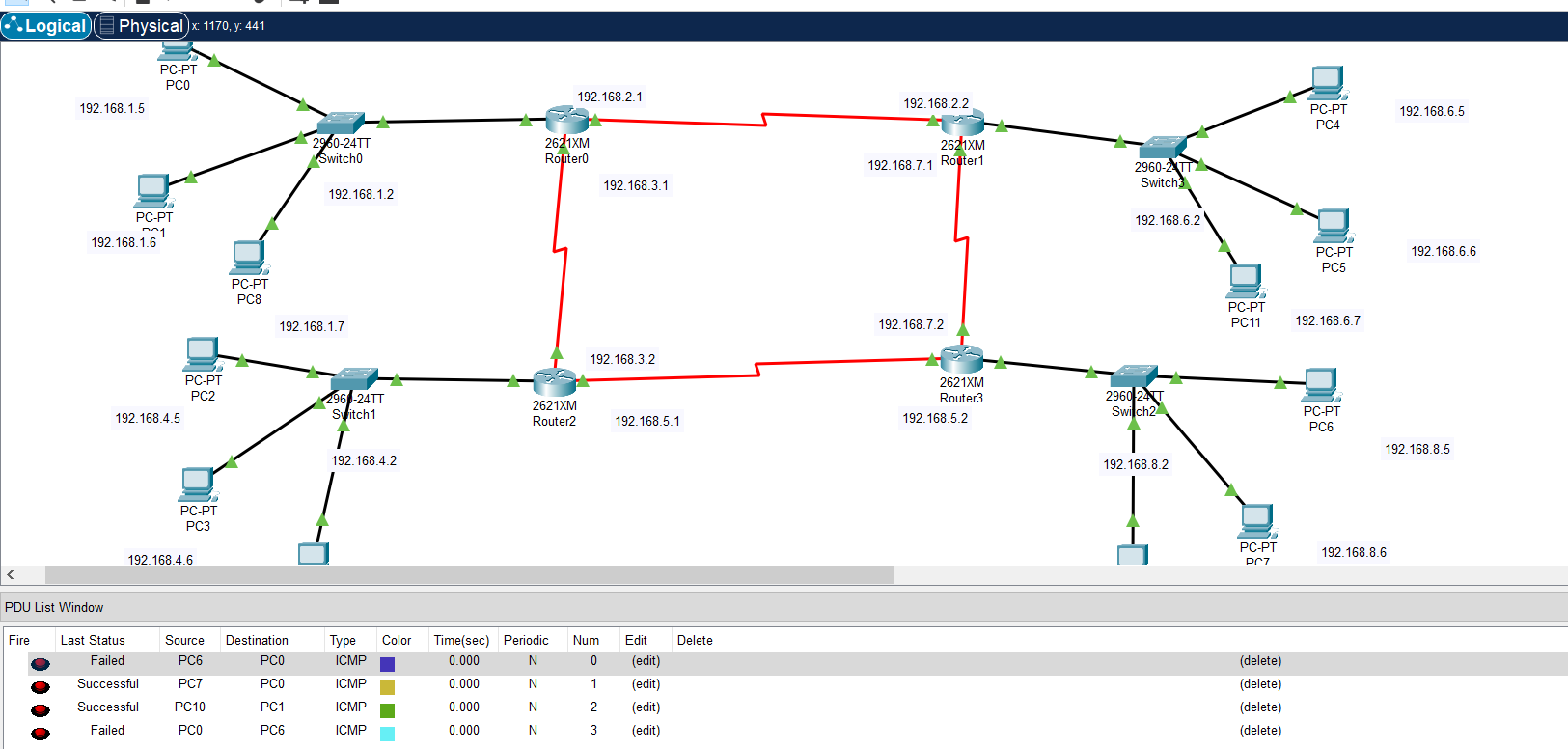
First, we configure the Extended ACL as follows in the CLI closest to the source that is, we will configure it for Router3.

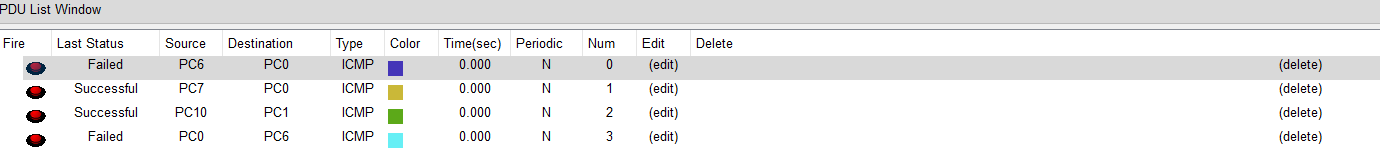


Now we will go to the interface Fa0/0 and apply the Extended ACL 100 to this interface for it to take effect.



Now we have successfully blocked PC6 that is 192.168.8.5 connection to 192.168.1.0/24 using an Extended ACL as demonstrated in the screenshot below.





Other PCs from 192.168.8.0/24 can connect to 192.168.1.0/24 except PC6 i.e. 192.168.8.5 but PC6 cannot connect to 192.168.1.0/24.

We have successfully used an Extended ACL to its intent.