Practical 4

Aim : Implement access control list in a network of an organization containing different departments.

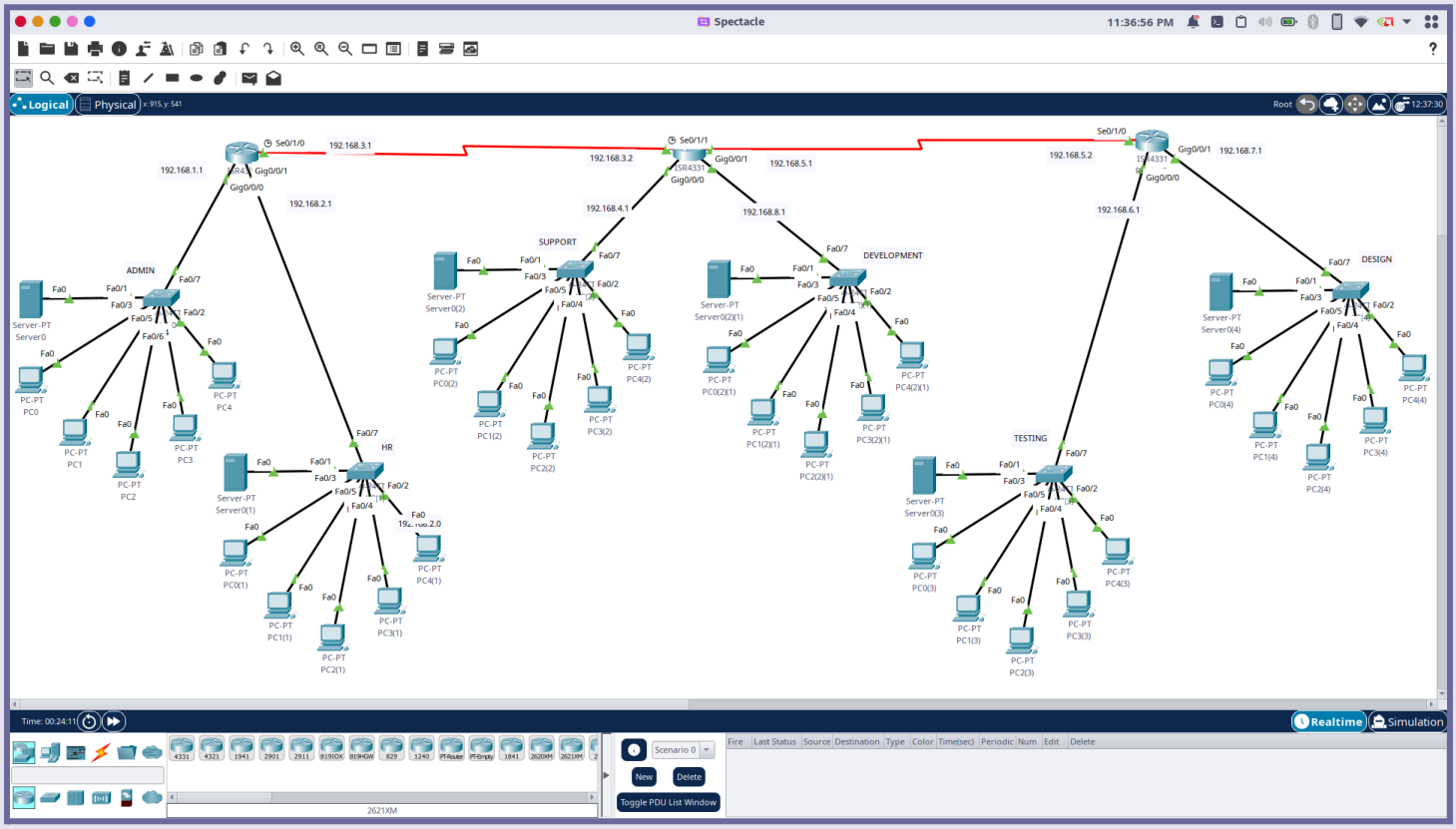
Scenario : There is an organization named CORPUS having 6 different departments Admin, HR, Support, Development, Testing and Design. IPv4 addressing scheme is used for assigning the IP address to the device. Each department has multiple employees, which have specific rights to communicate within the network. The details of the rights are as mentioned below :

The Admin Department can access all the devices in the organization. The Testing Department can only communicate with the Admin, HR and Development department. Only the head of the development department can communicate with the support department. Two members of the support department out of five members can contact the design department.

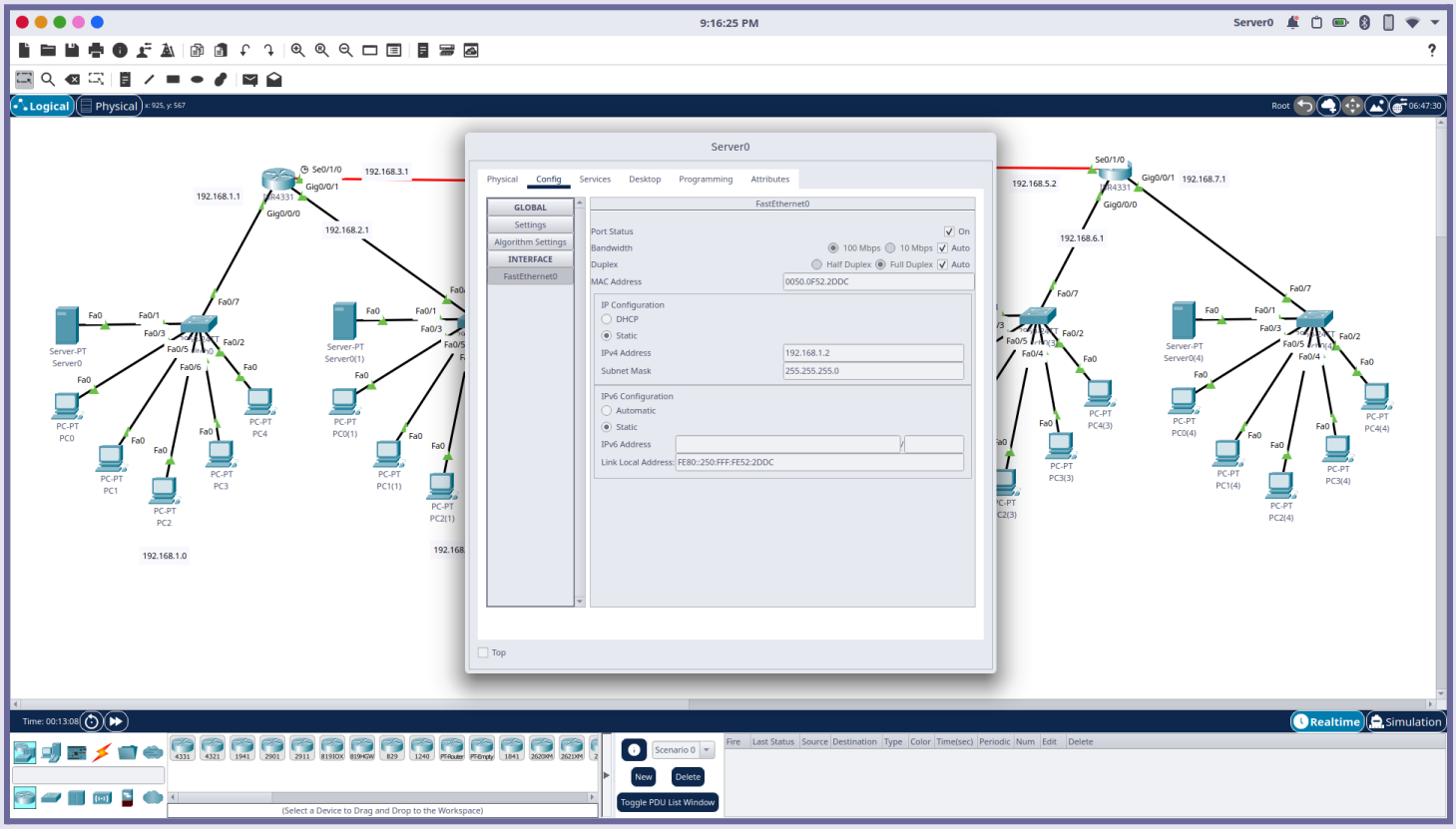
Implement the network in Cisco packet tracer, as per the requirement. As the number of the end devices are not mentioned in the requirement, you can take as per your requirement.

Procedure :

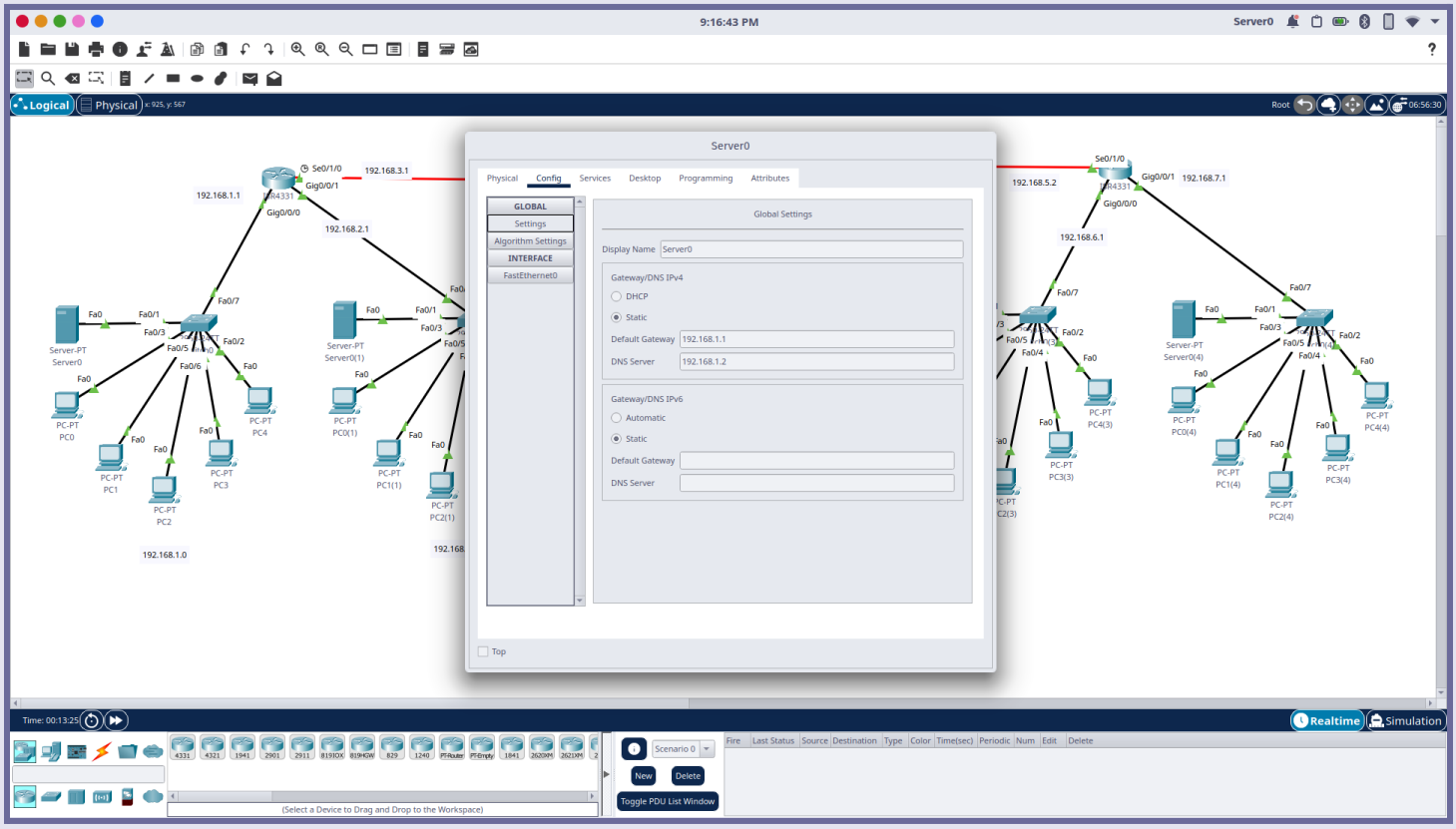
1. Design the network as given in the scenario with networks 192.168.1.0, 192.168.2.0, … 192.168.8.0 as shown in the figure


Spectacle
11:36:56 PM
Logical
Physical
Root
ADMIN
HR
SUPPORT
DEVELOPMENT
TESTING
DESIGN
192.168.1.1
192.168.2.1
192.168.3.1
192.168.3.2
192.168.4.1
192.168.5.1
192.168.5.2
192.168.6.1
192.168.7.1
192.168.8.1
Realtime
Simulation

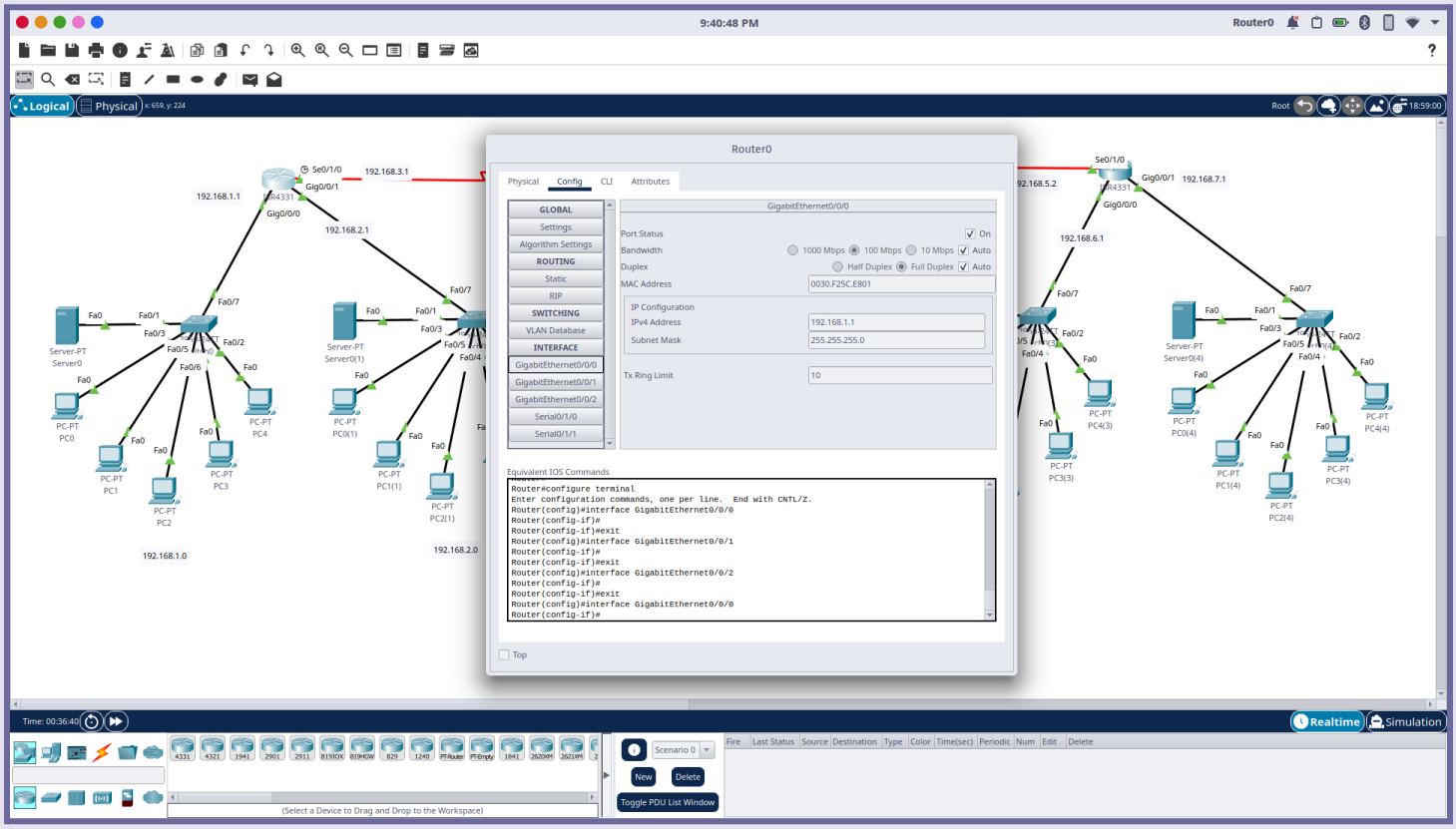
2. Assign an IP address 192.168.1.2 to the Server0 of the Admin department of the network 192.168.1.0



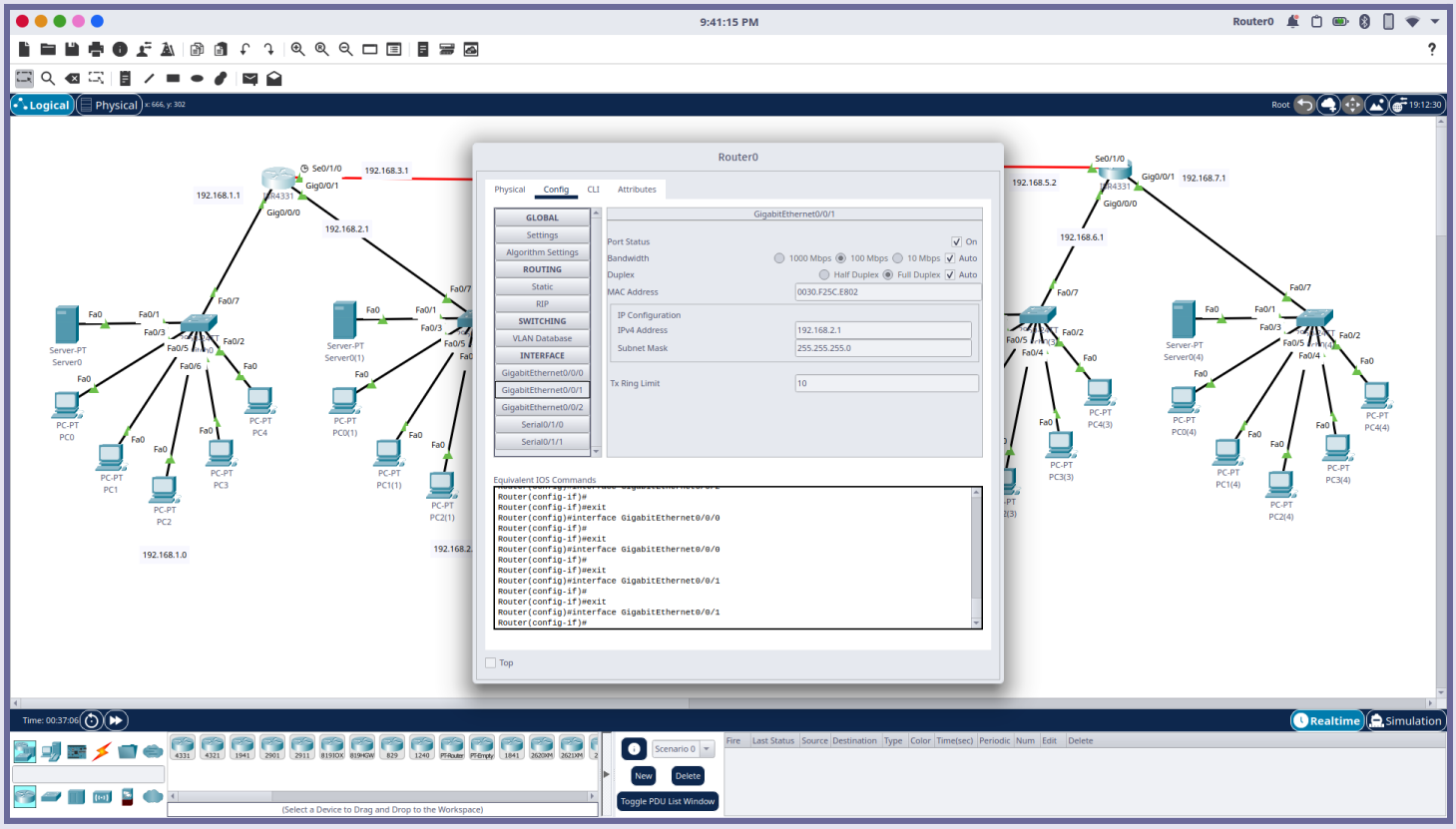
3. Assign gateway IP of the router connected to it and its own IP as DNS server

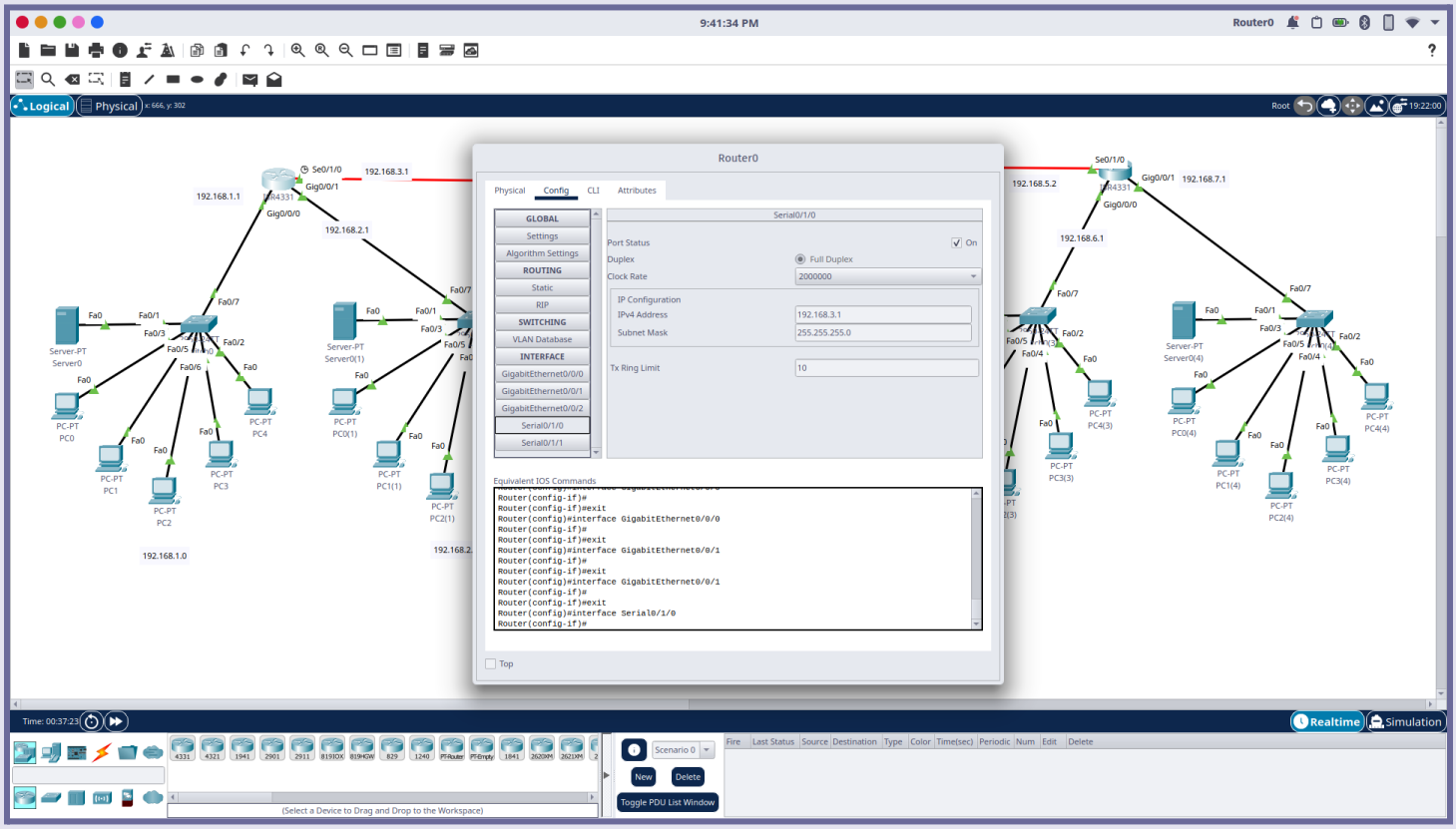


4. Assign IP to Router0’s gigabit ethernet port connected to the router, which was given as gateway in Server0

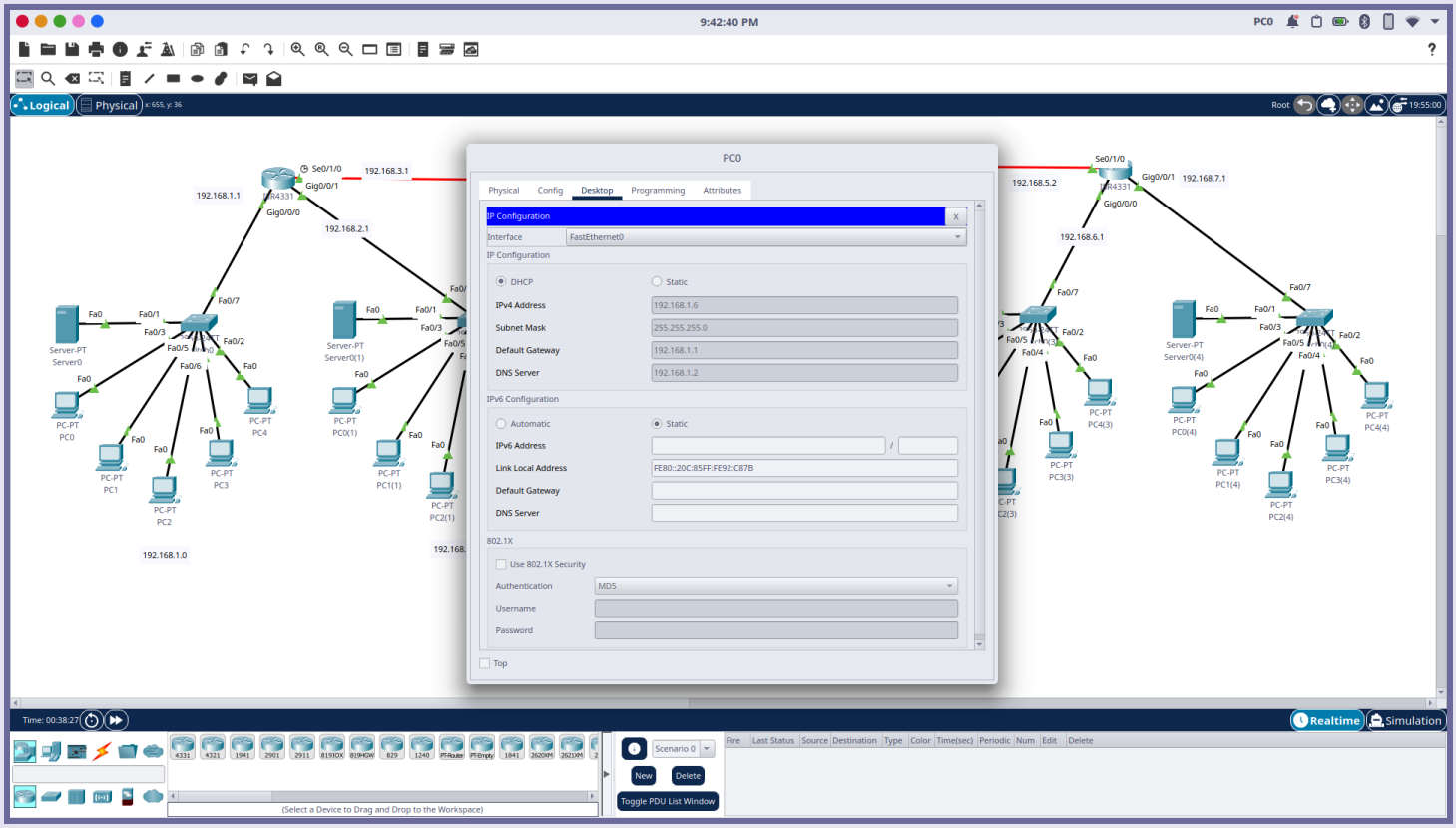


5. Assign IP to other ports of Router0 accordingly.

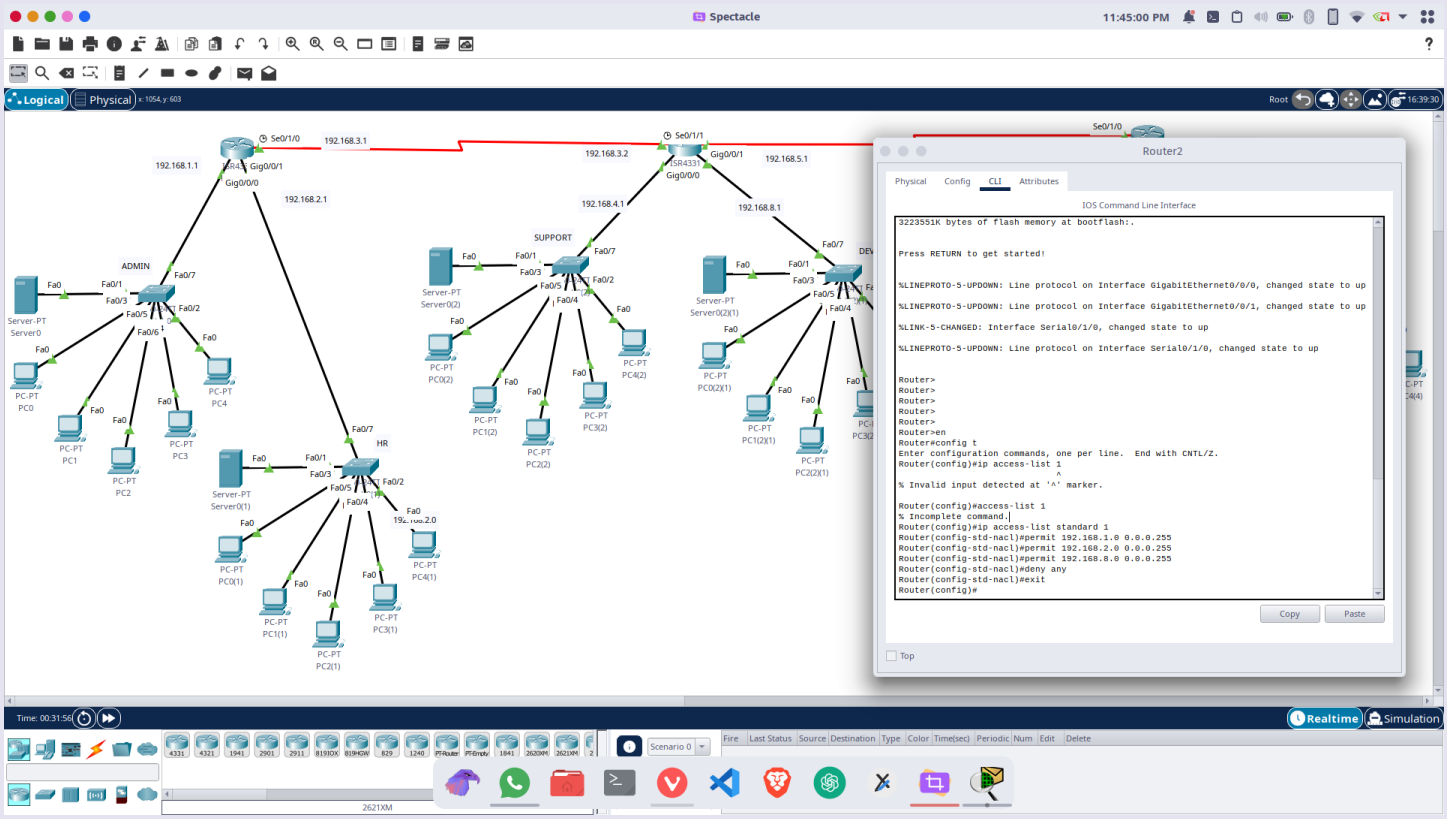




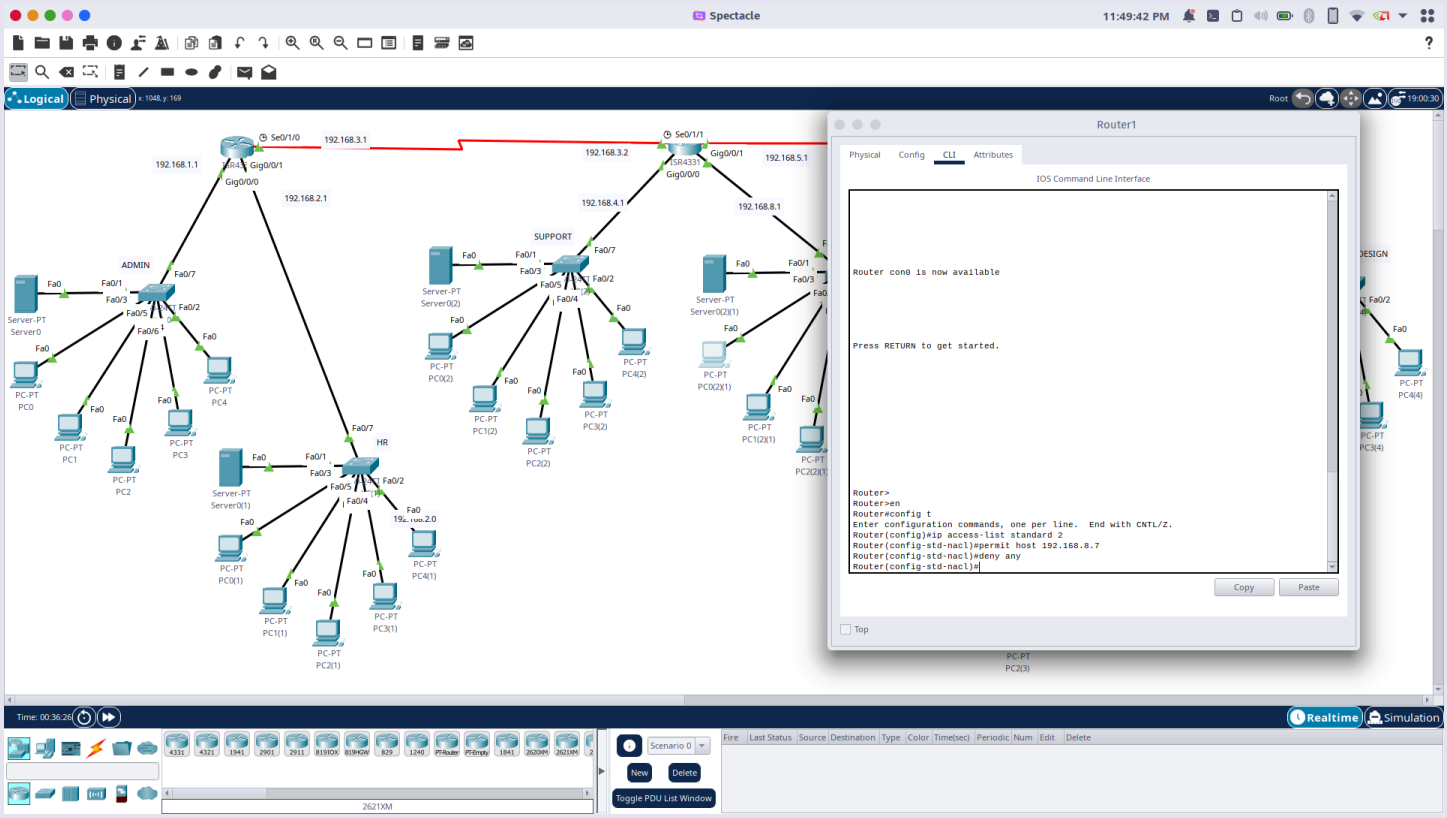
6. Configure all end devices connected to Server0 to use DHCP for IP addresses.



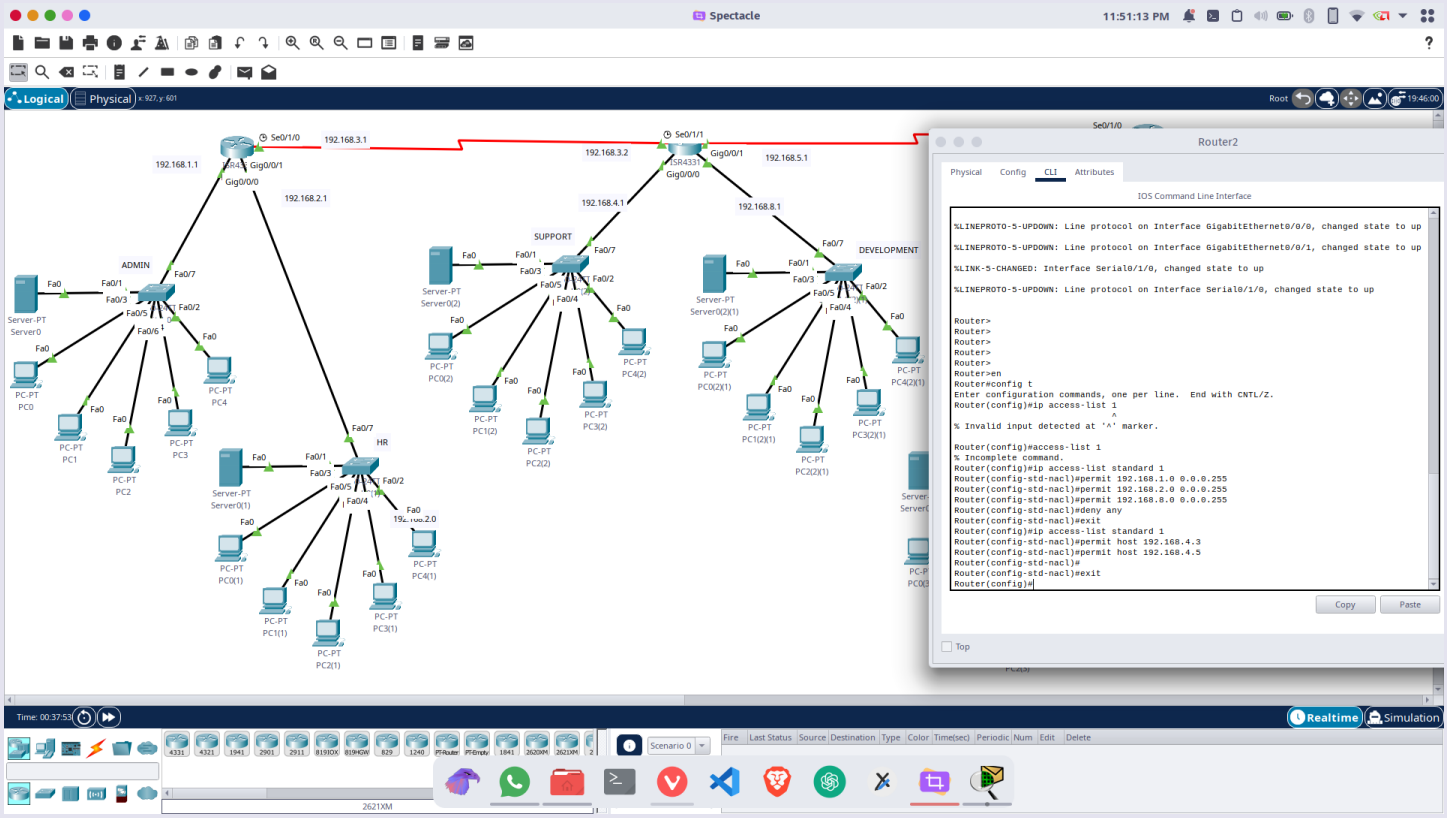
7. Similarly, follow the same steps for all other networks with IP and network range given in the figure 1 of first step. Then set up the Router2 access list for Testing department to allow communication only with Admin, HR and Development department.



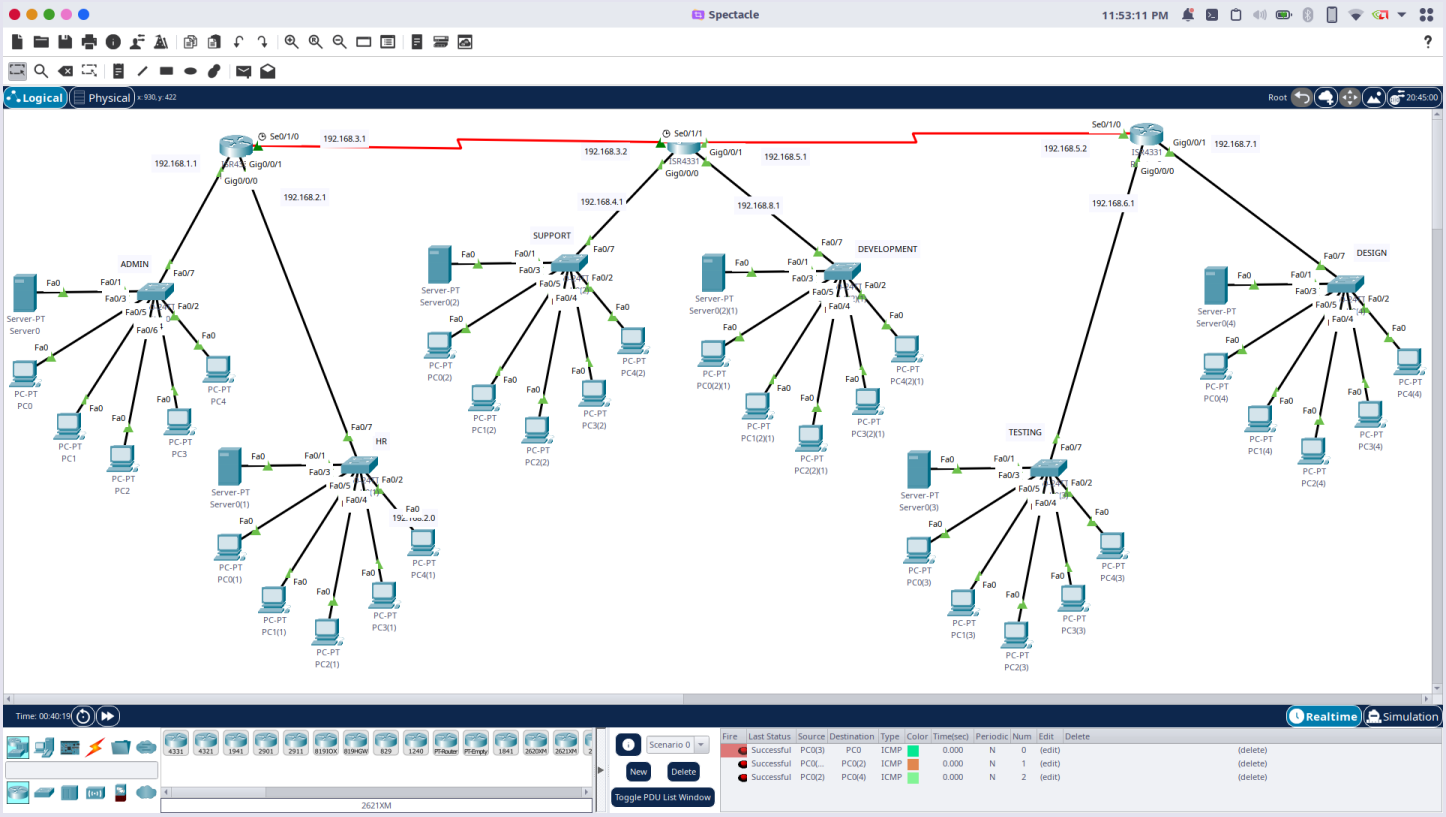
8. Now, configure access list for Router1 to allow communication between support department and head of development department.



9. Configure Router2 again to allow communication between 2 end devices of the support department with the design department.



10. Check the communications between departments specified via access list, others are denied, only successful communication will be that specified in access lists



Conclusion : It is concluded that access lists can be set to permit or deny the inter communication among departments and/or end devices.