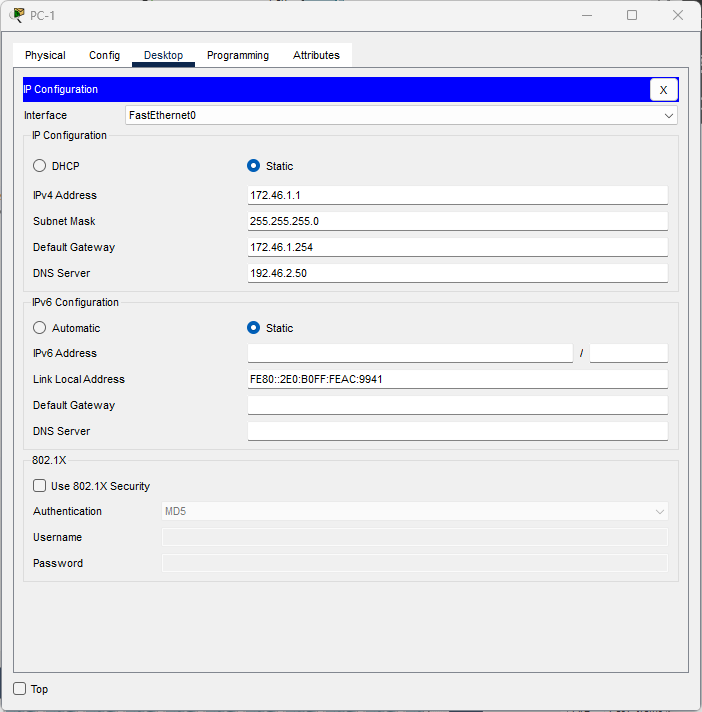
**NST31042 – Practical for Scaling and Connecting**

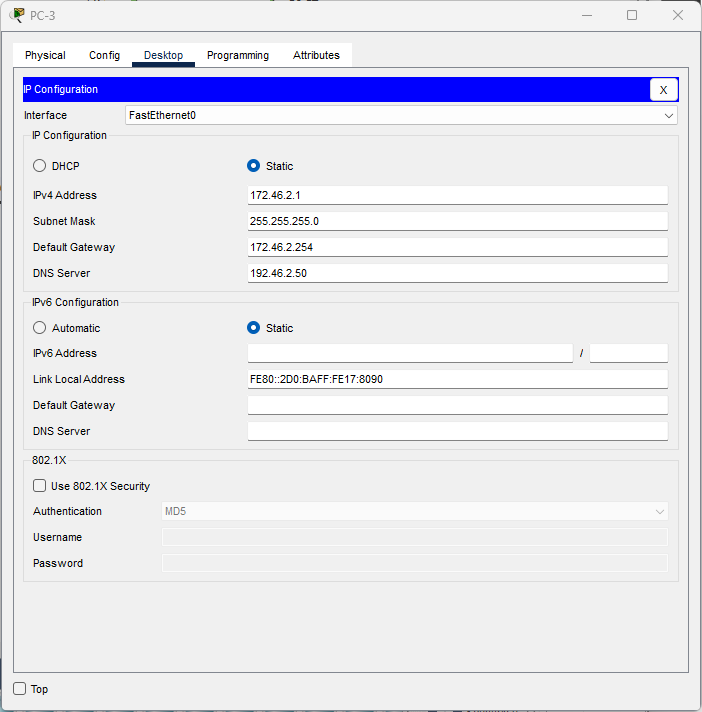
Registration number: SEU/IS/19/ICT/046

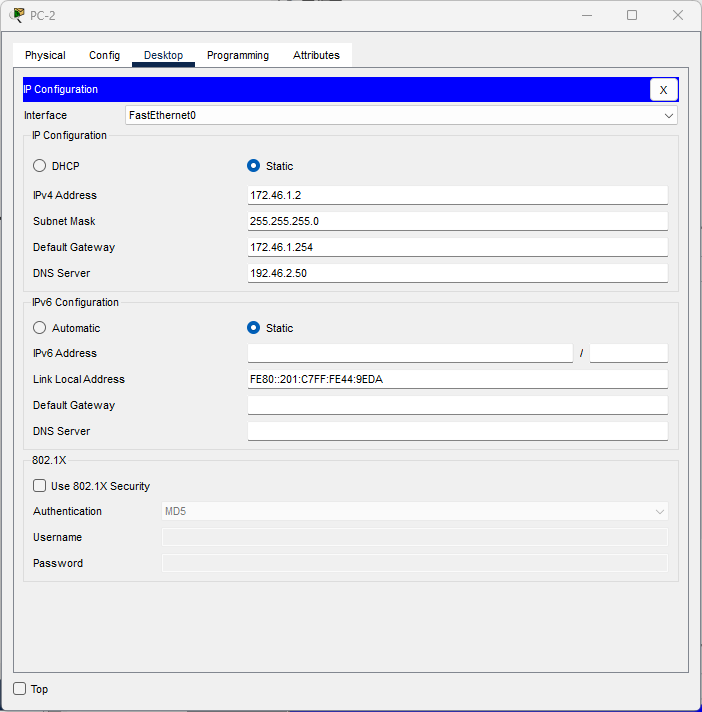
Academic Year: 2019/2020

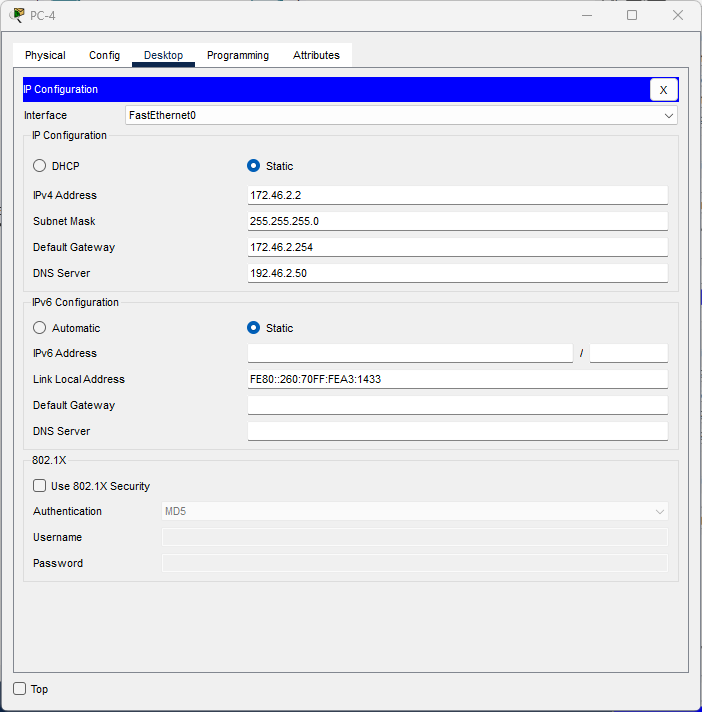
CA 4

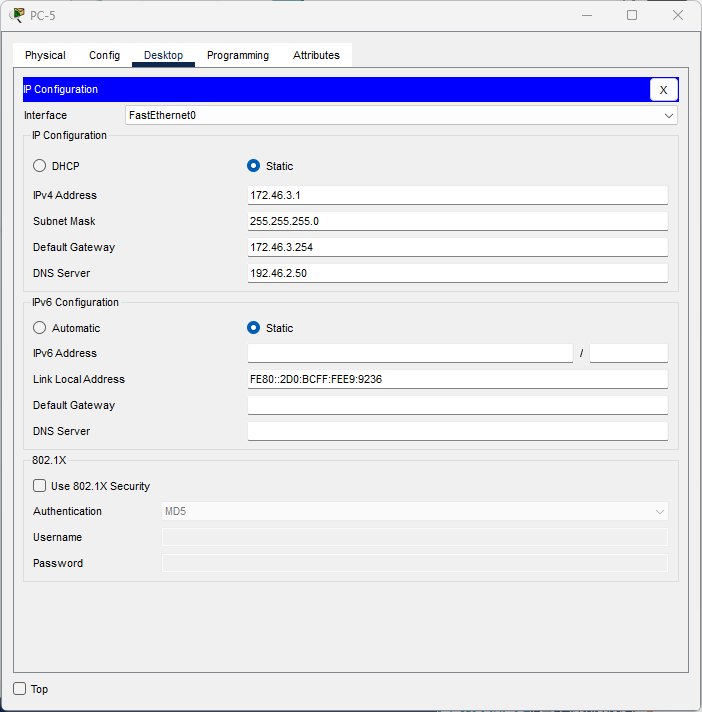
1. Configure Ip address to Each interface

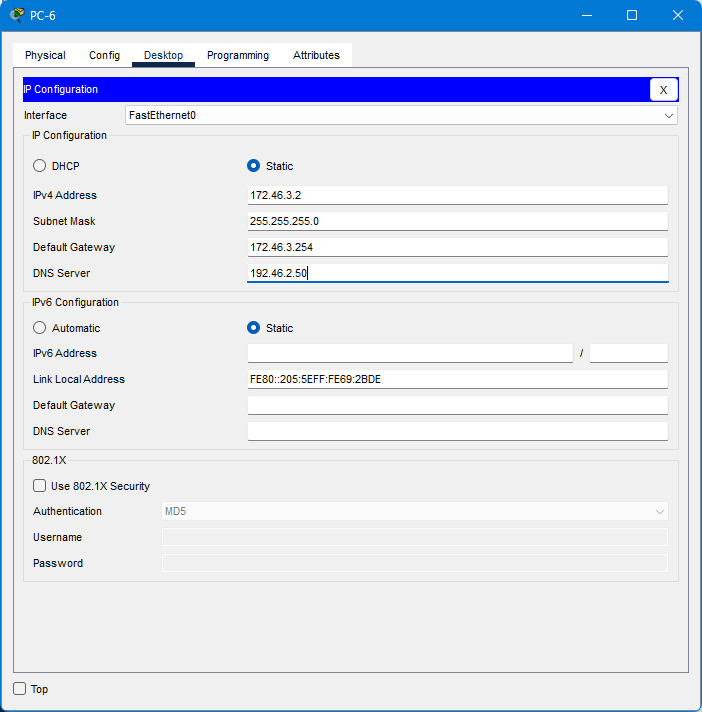


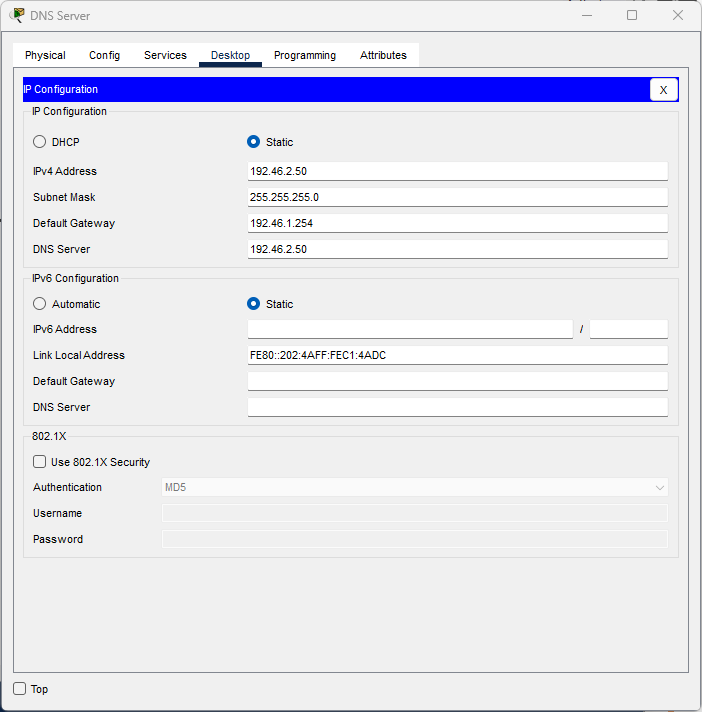


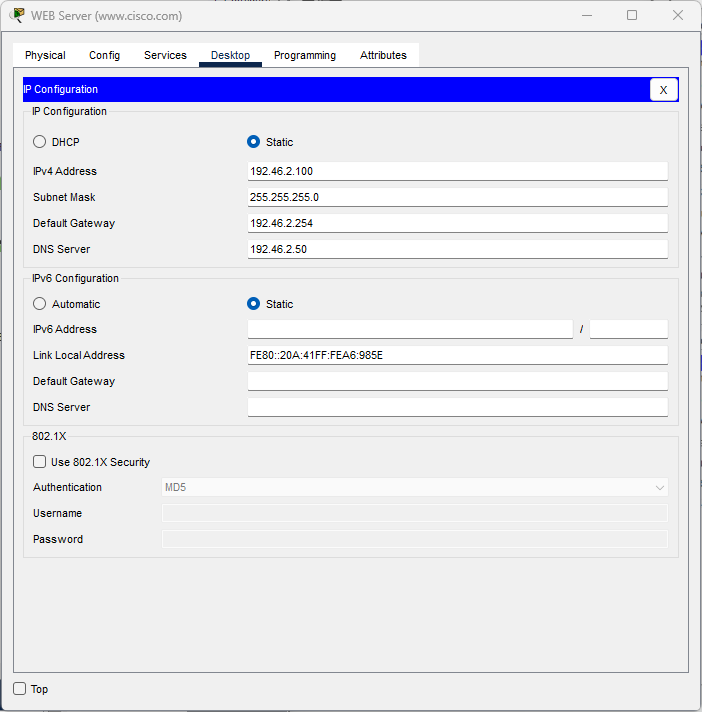


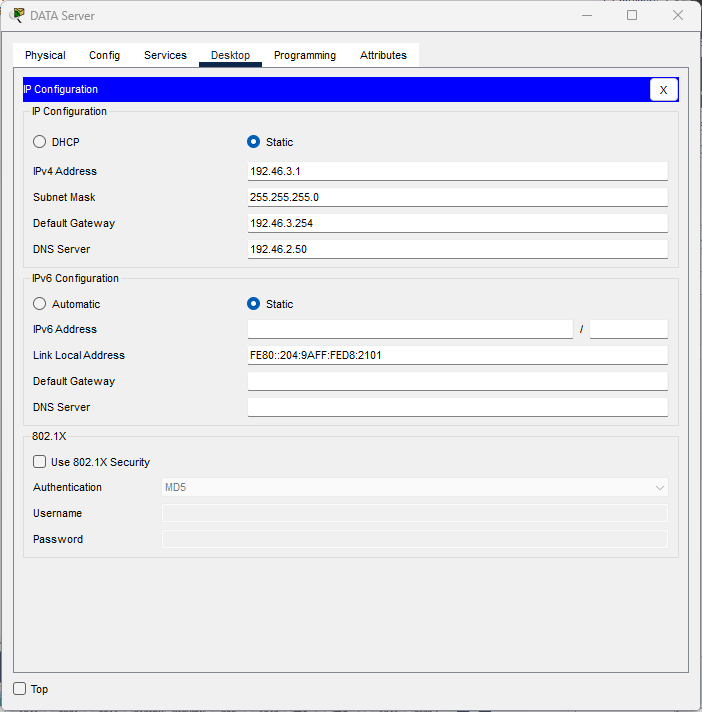


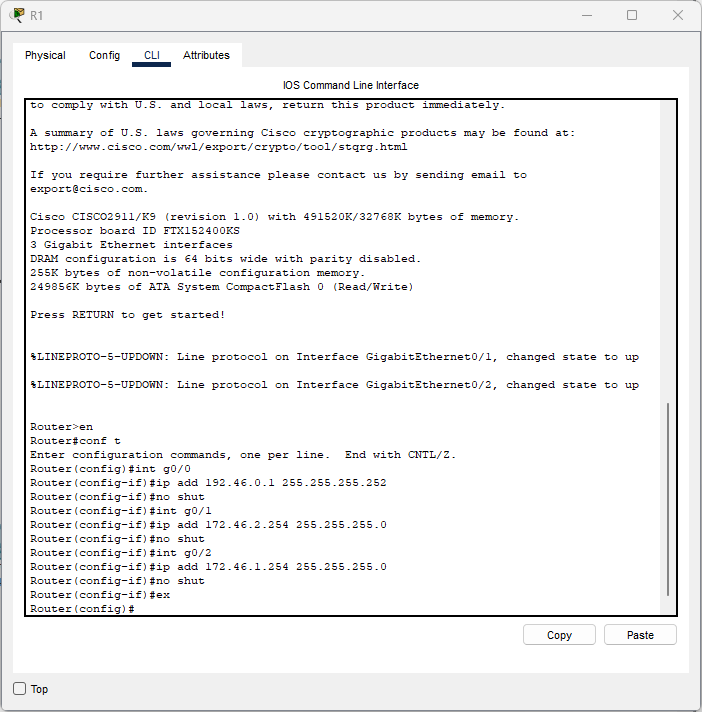


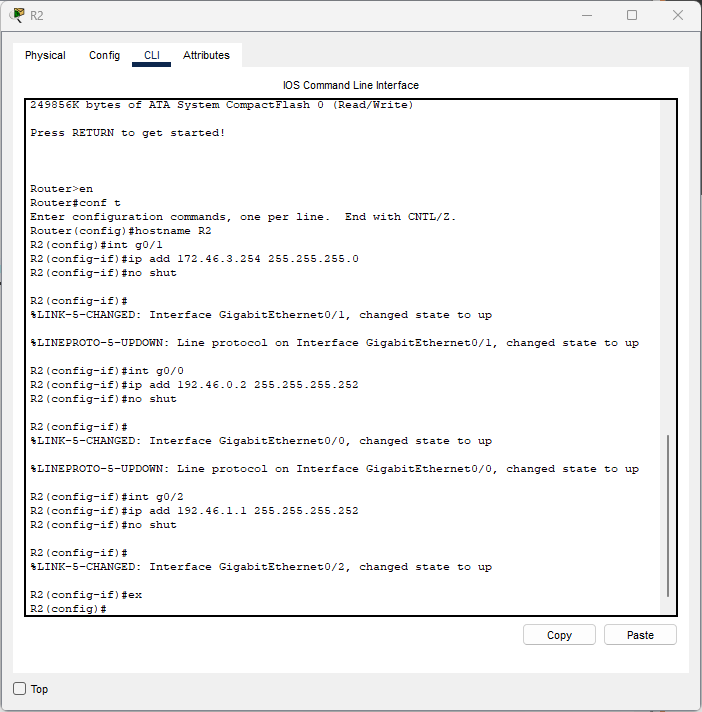


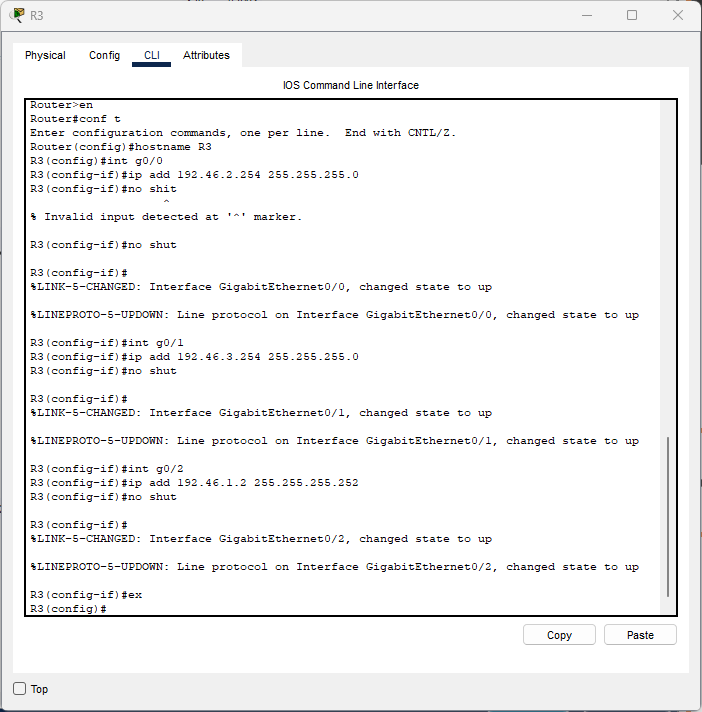




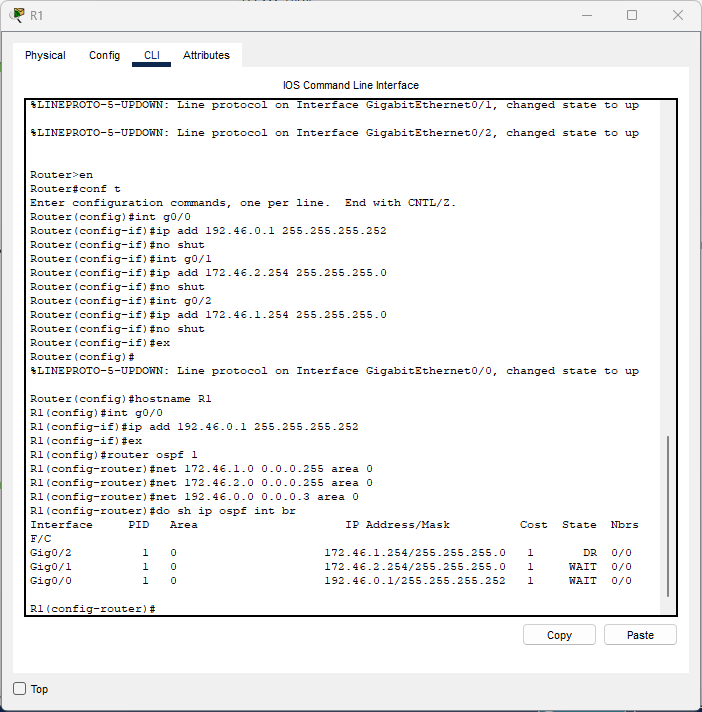


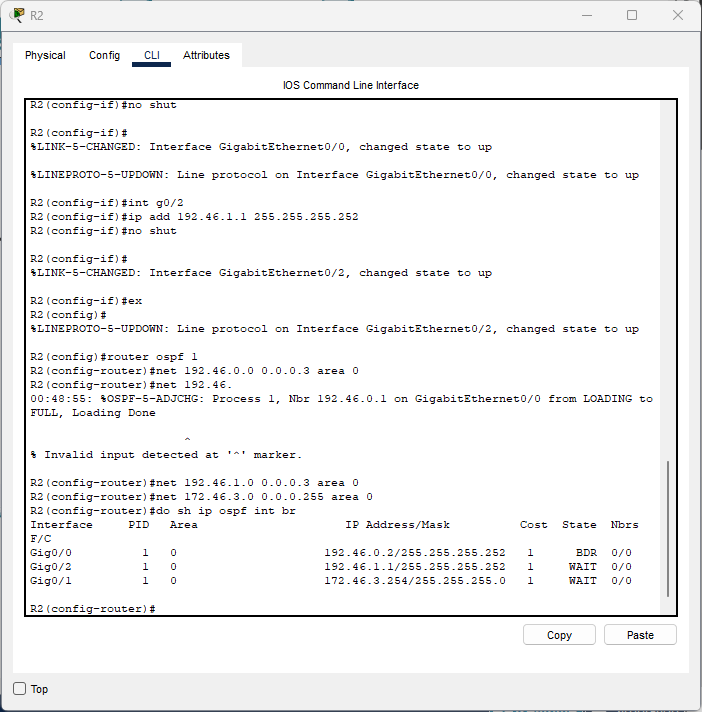


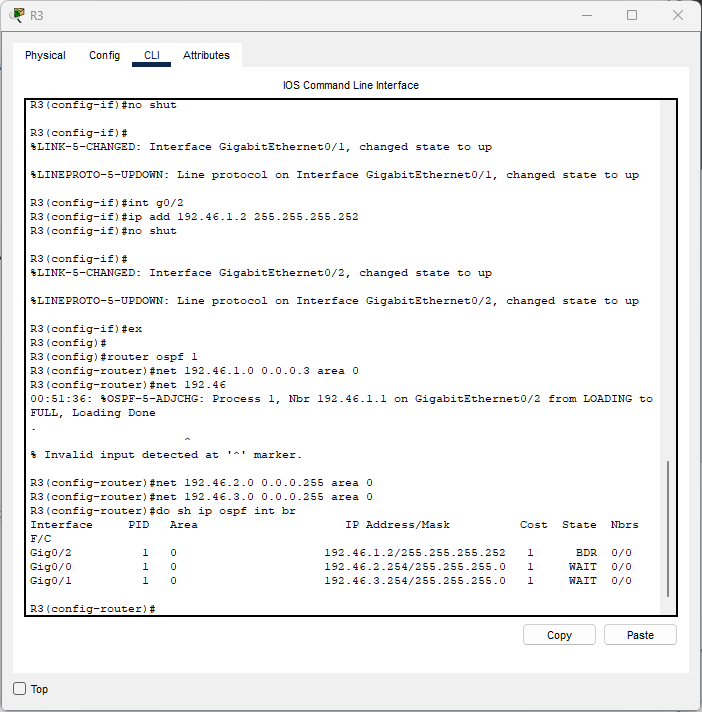


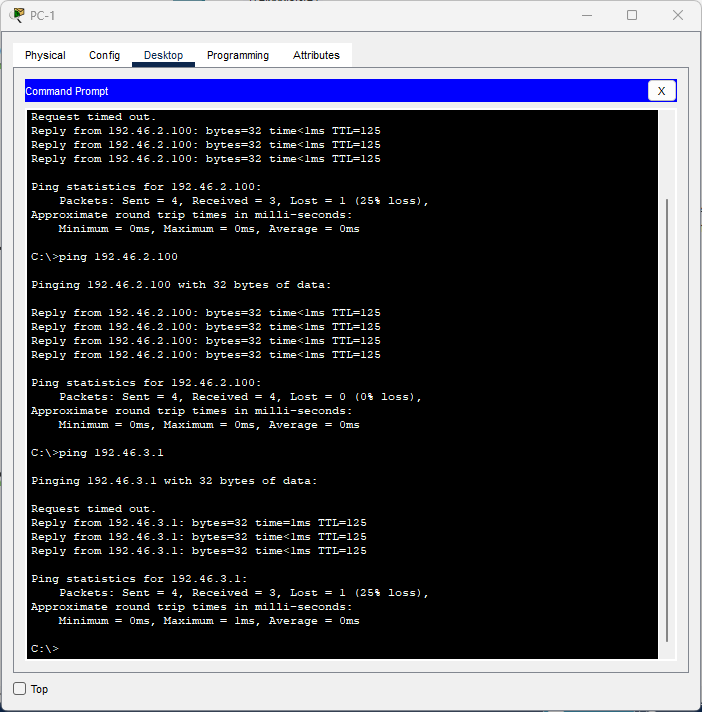


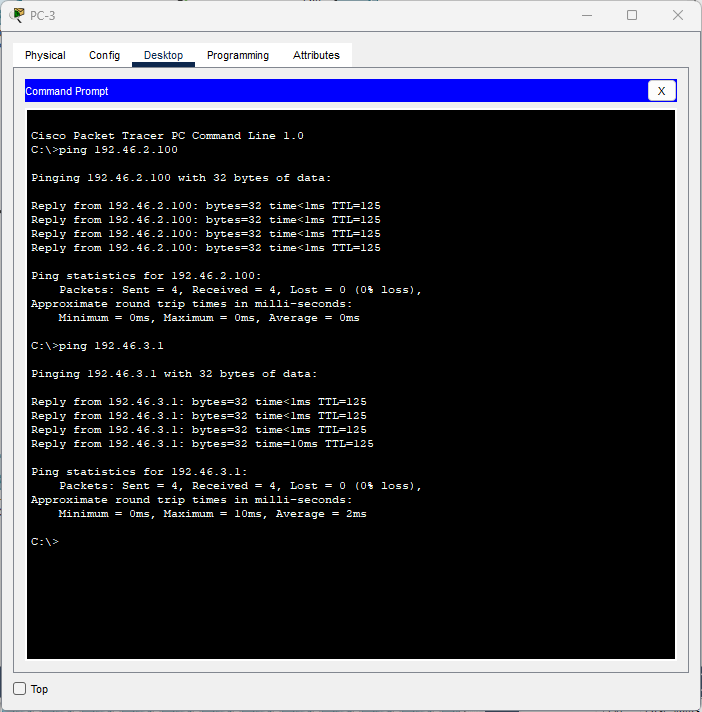
1. Configure OSPF on R1, R2 and R3 to allow full connectivity between the PCs and servers.

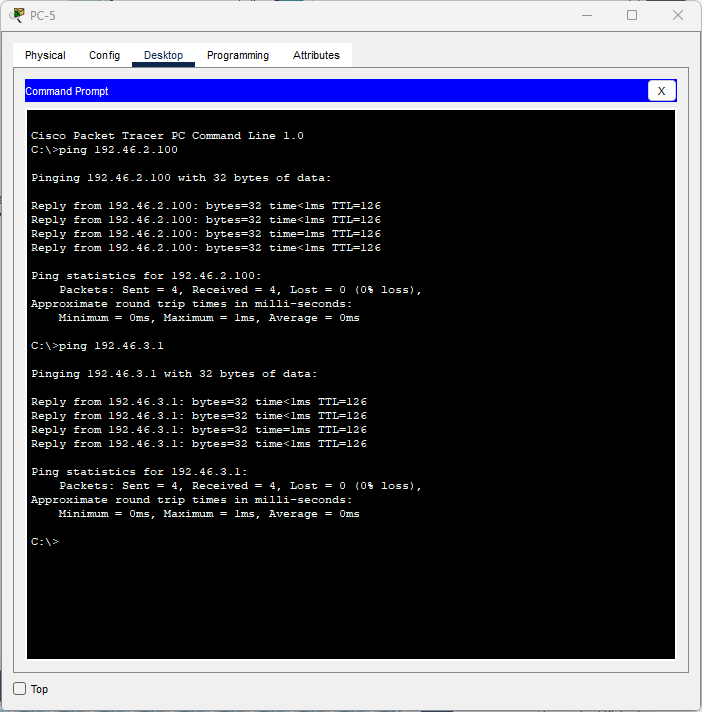


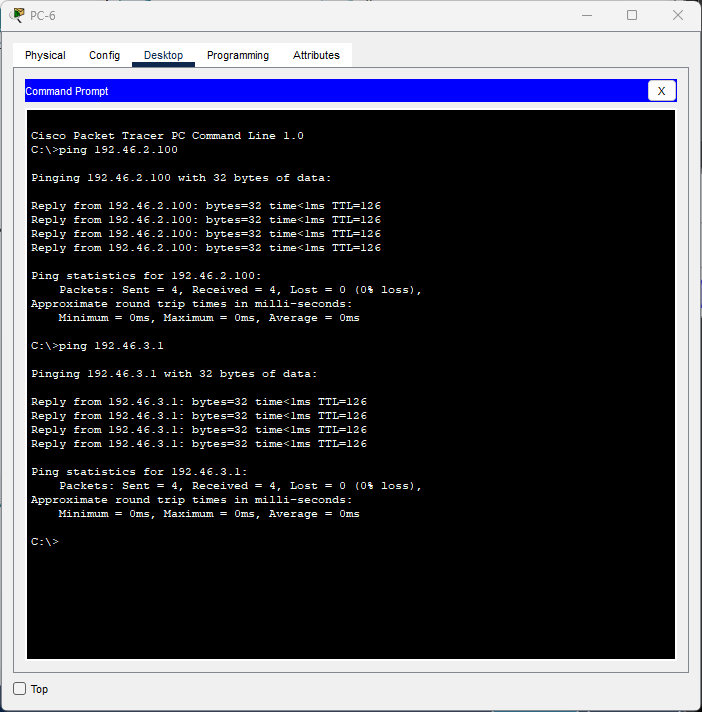








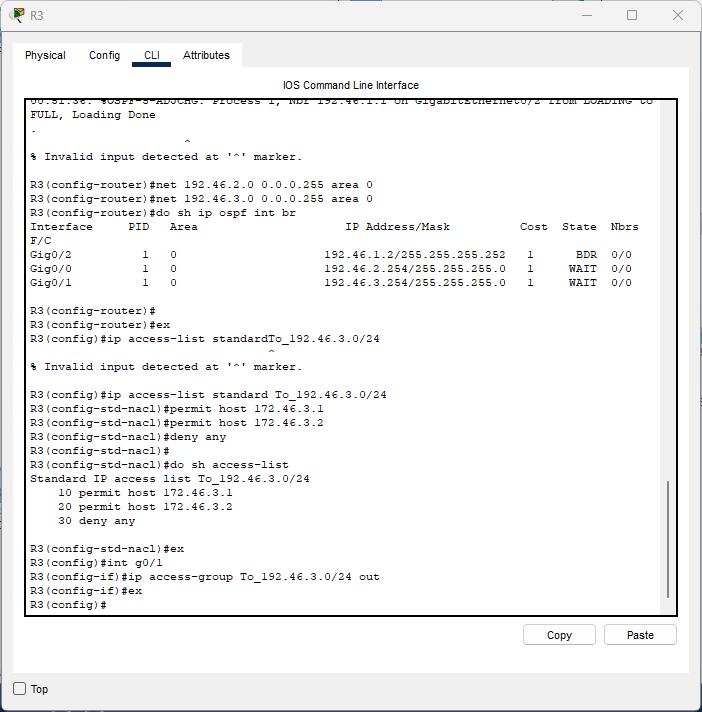




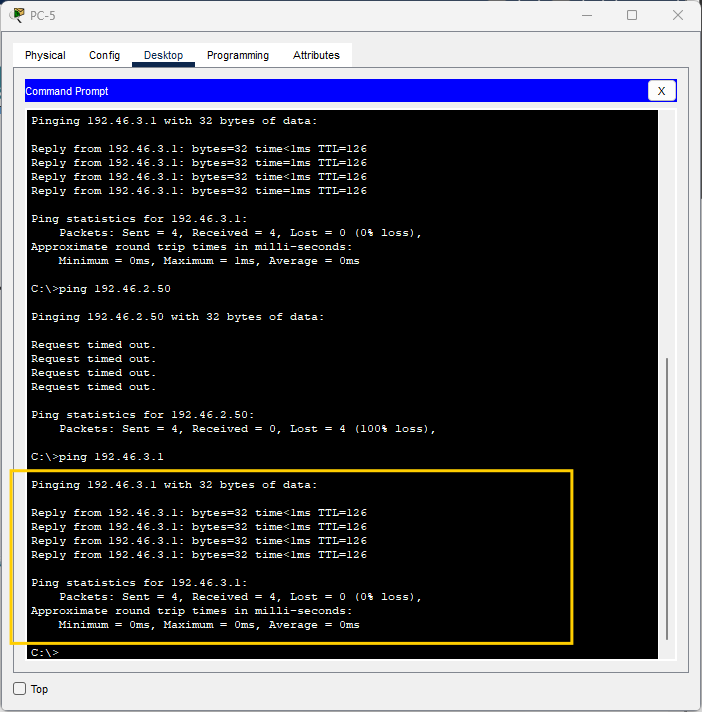
3. Configure standard numbered ACLS on R1 and standard named ACLs on R3

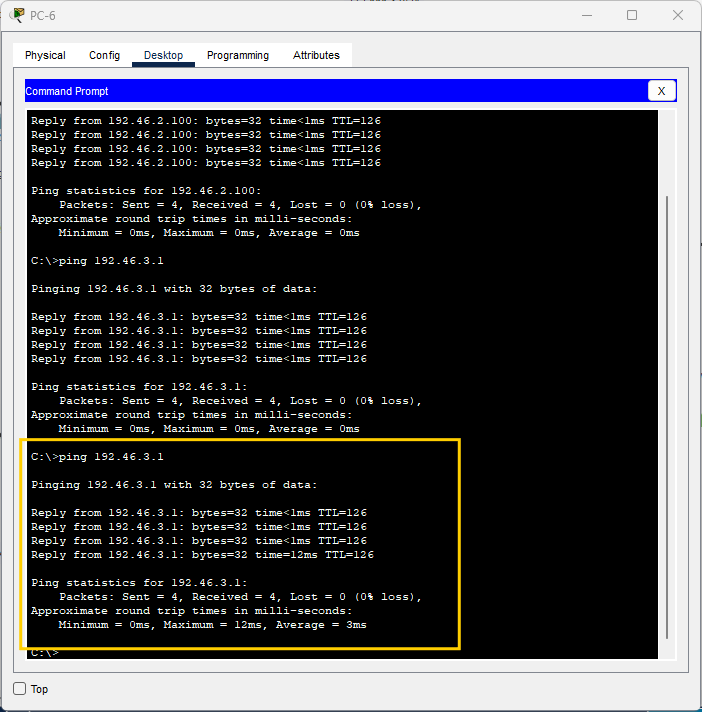
to fulfil the following network policies:

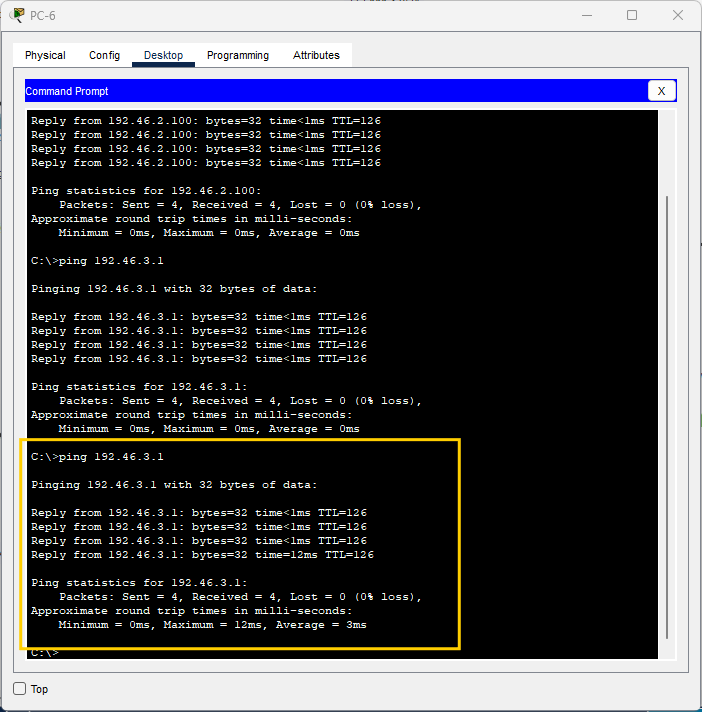
-Only PC5 and PC6 can access 192.168.3.0/24

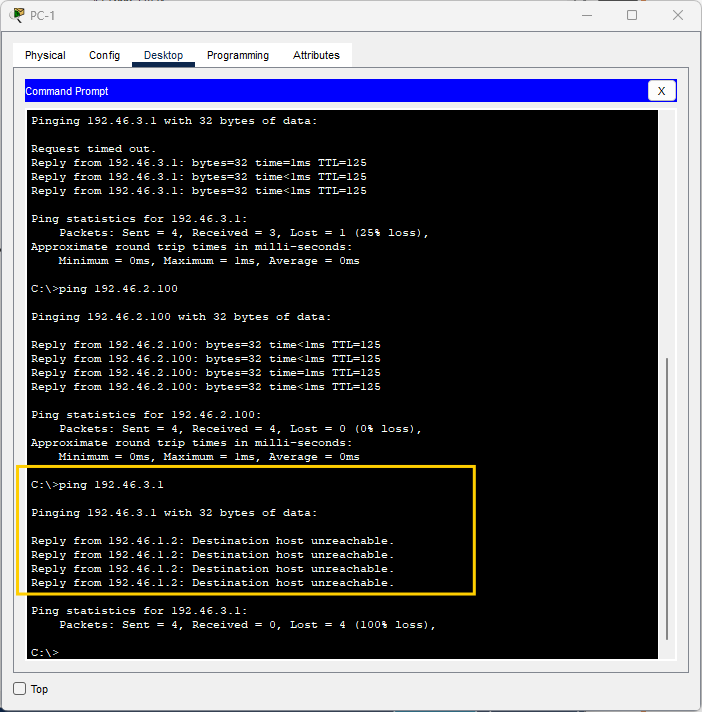


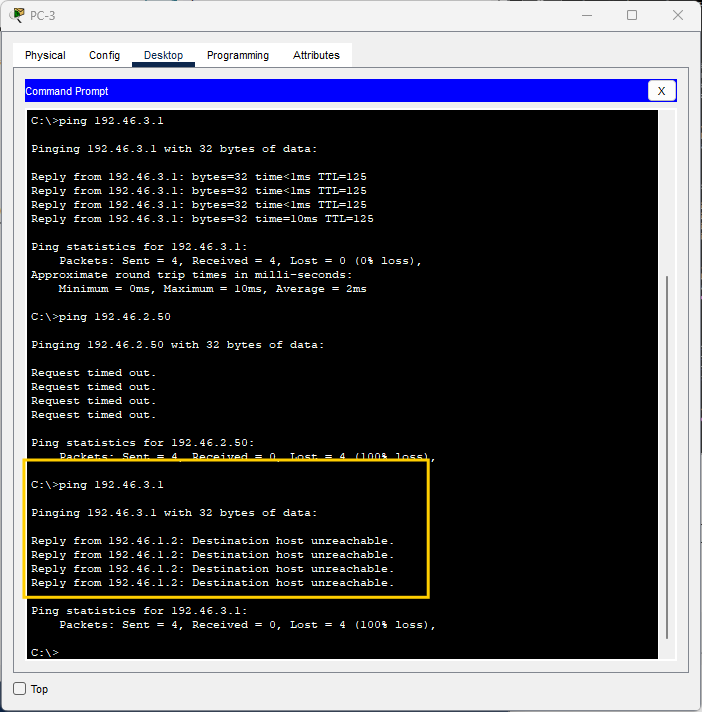
Only 5 and 6 can access others are can’t access



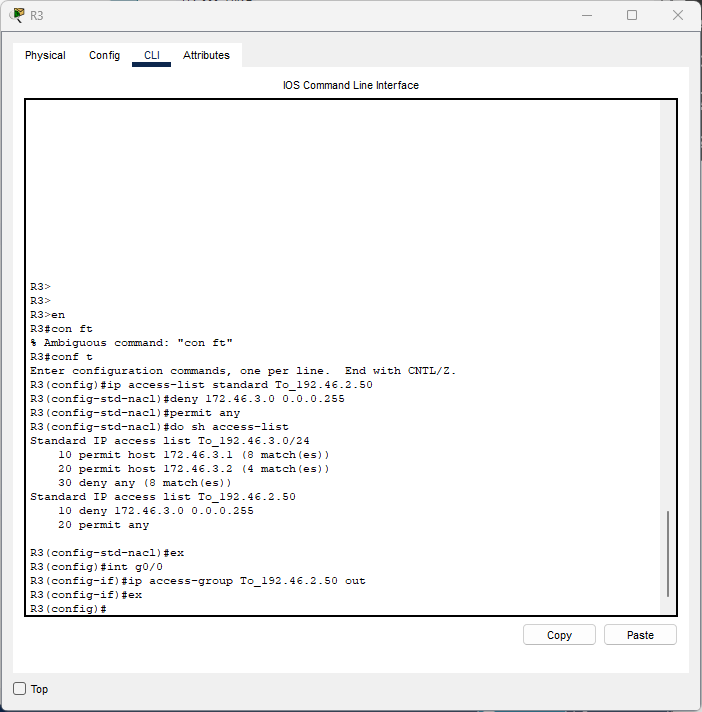


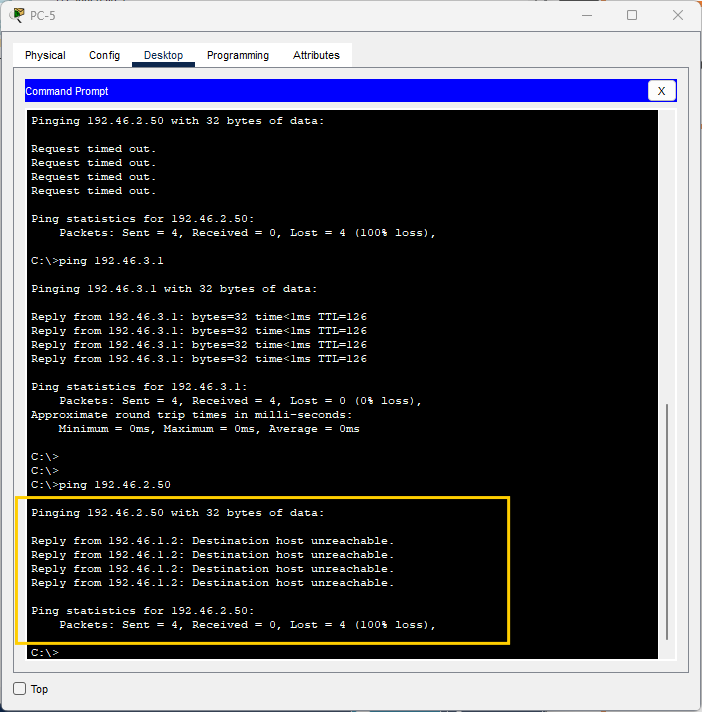


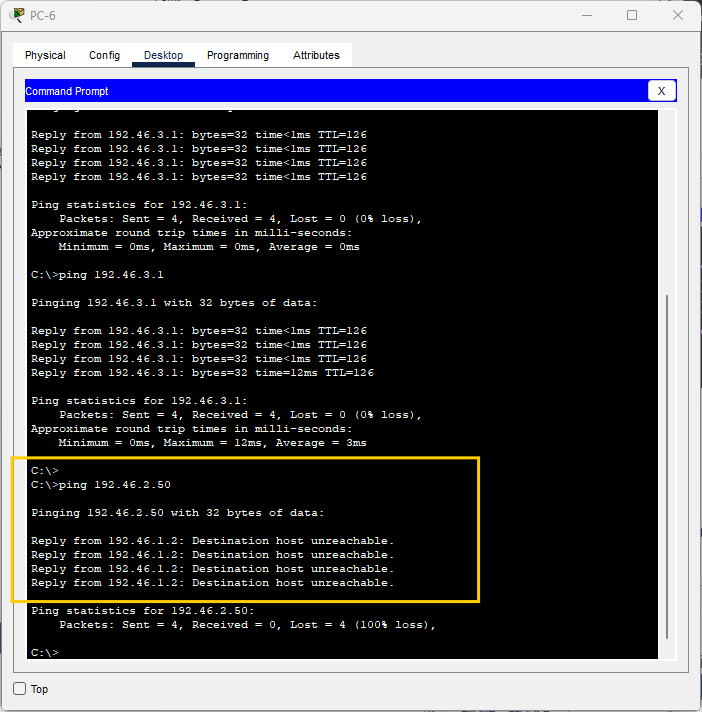




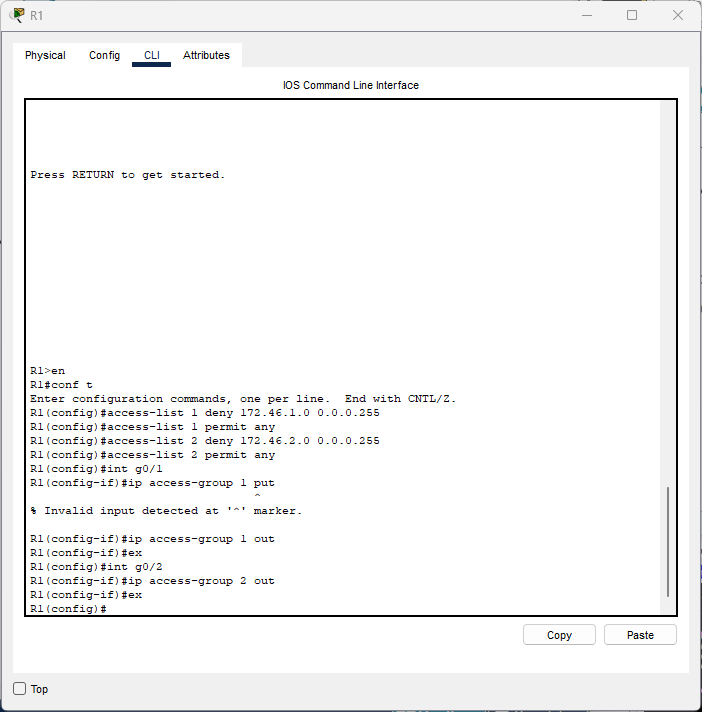
-Hosts in 172.16.3.0/24 can't access 192.168.2.50

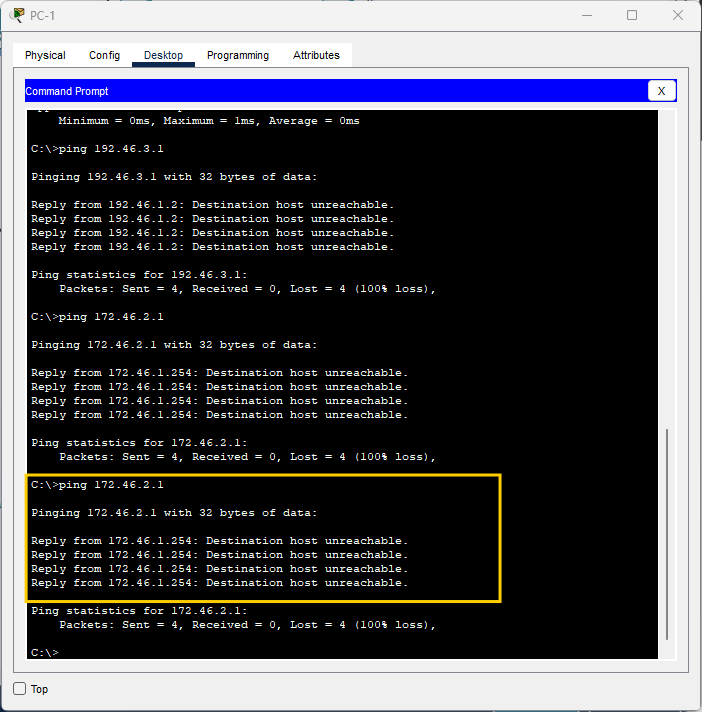


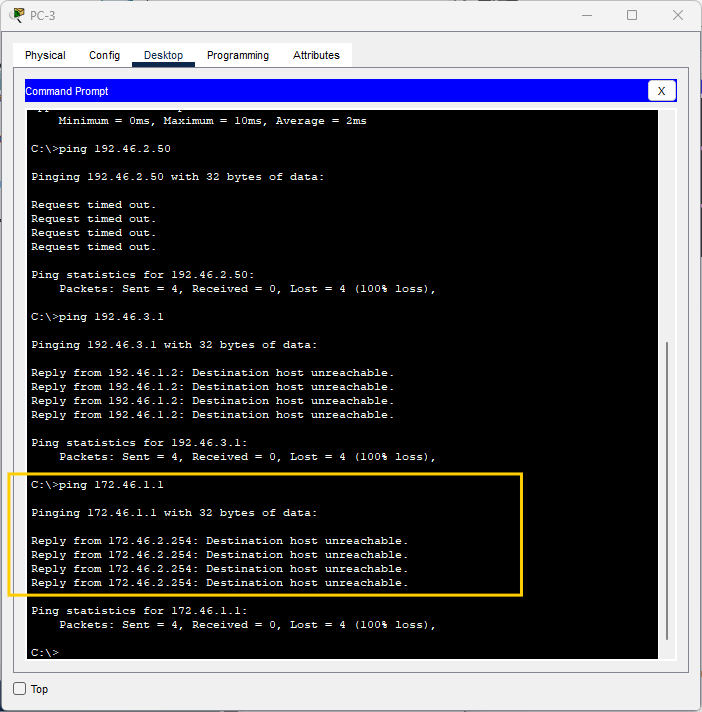




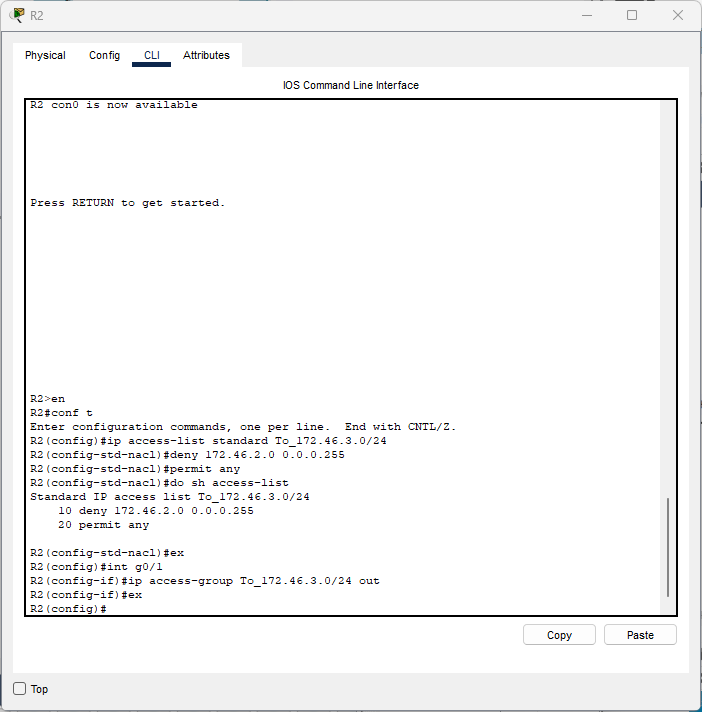
-172.16.1.0/24 can't access 172.16.2.0

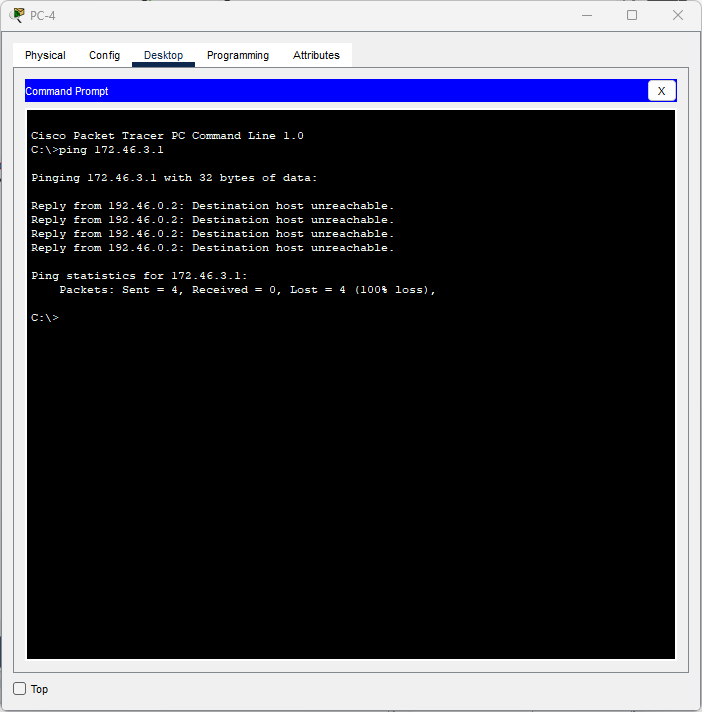






-172.16.2.0/24 can't access 172.16.3.0

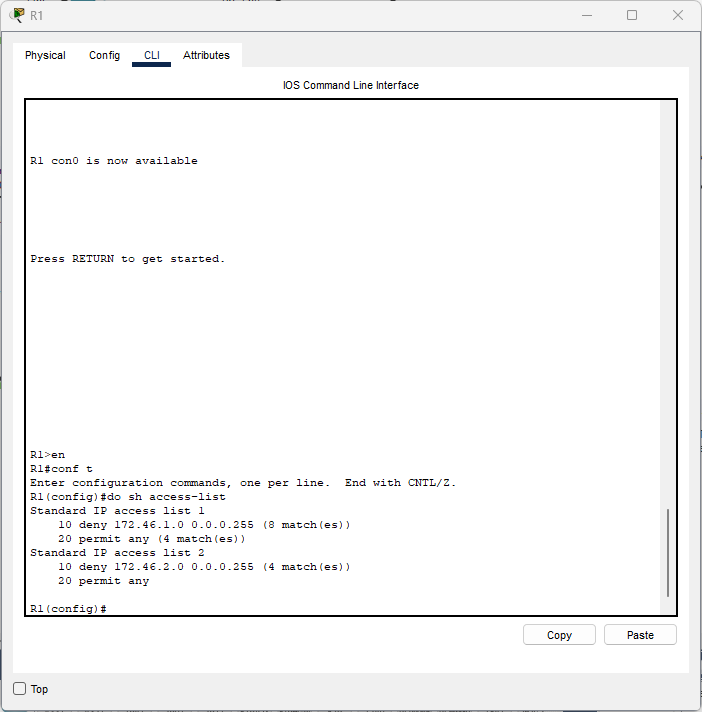


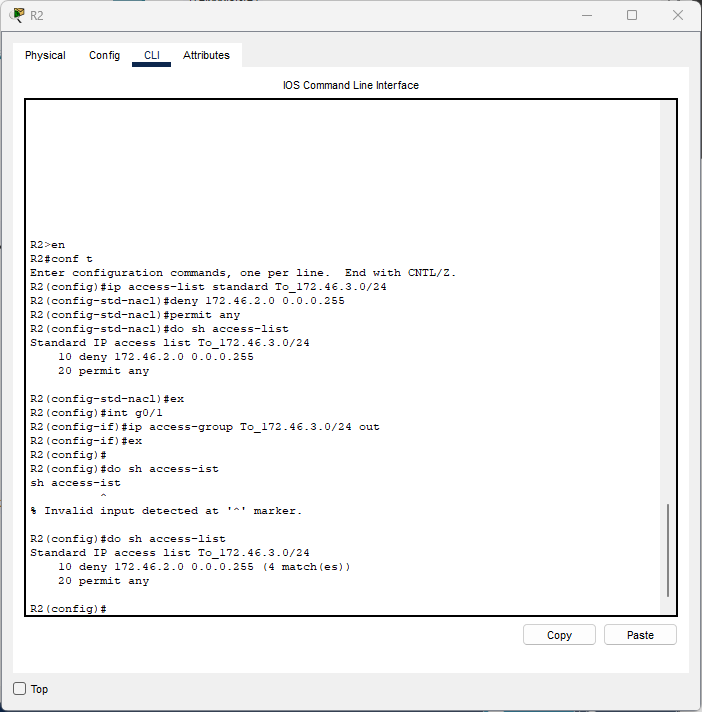


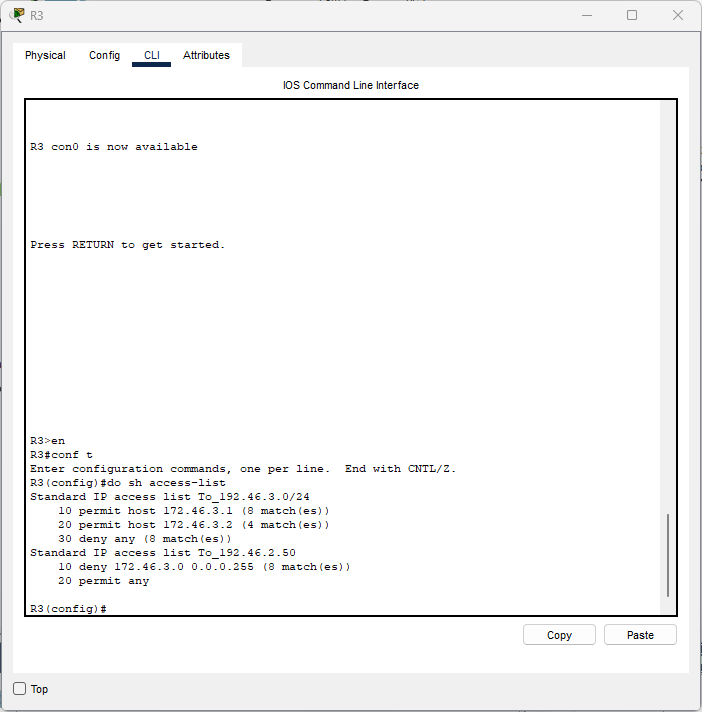
4.Verify Each Entries

Here gave under the each and every network policies.

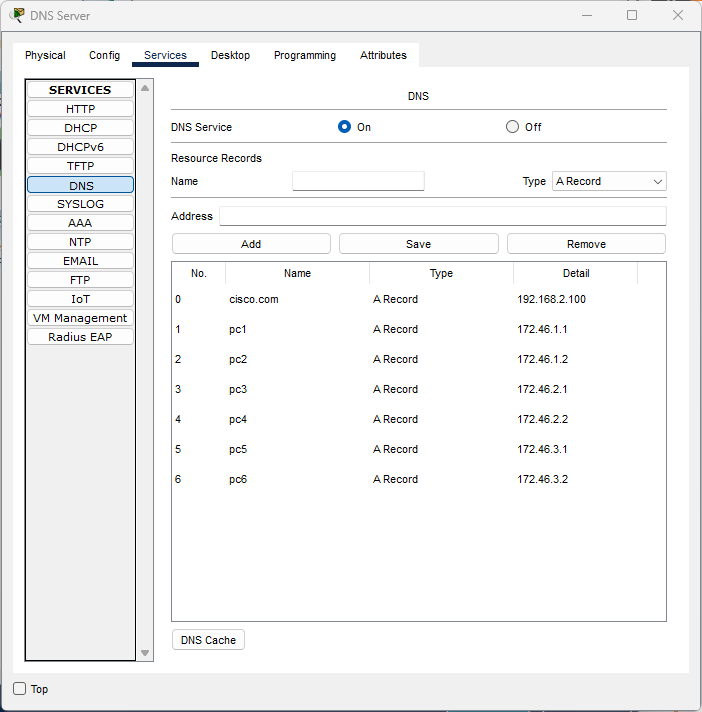
5.Print the Access lists





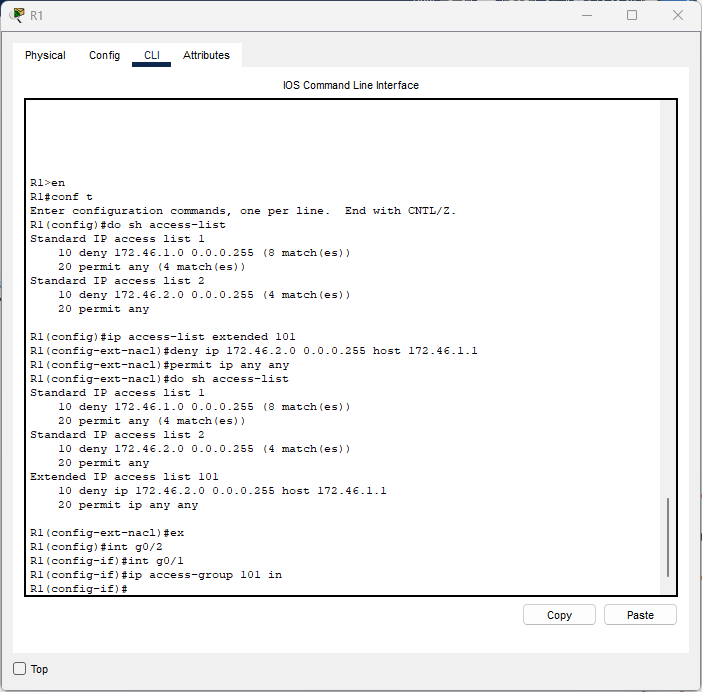


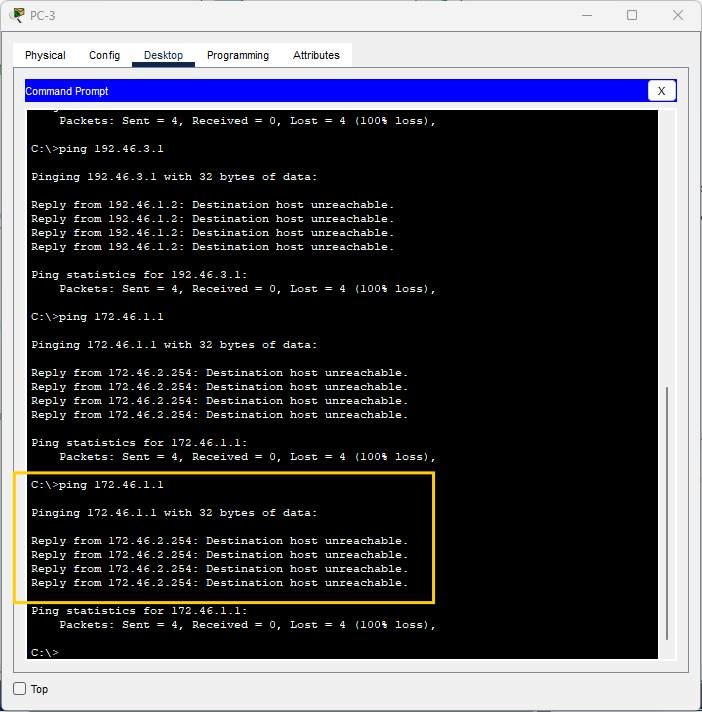
6.Create DNS services in DNS Server. (pc1-pc6 )

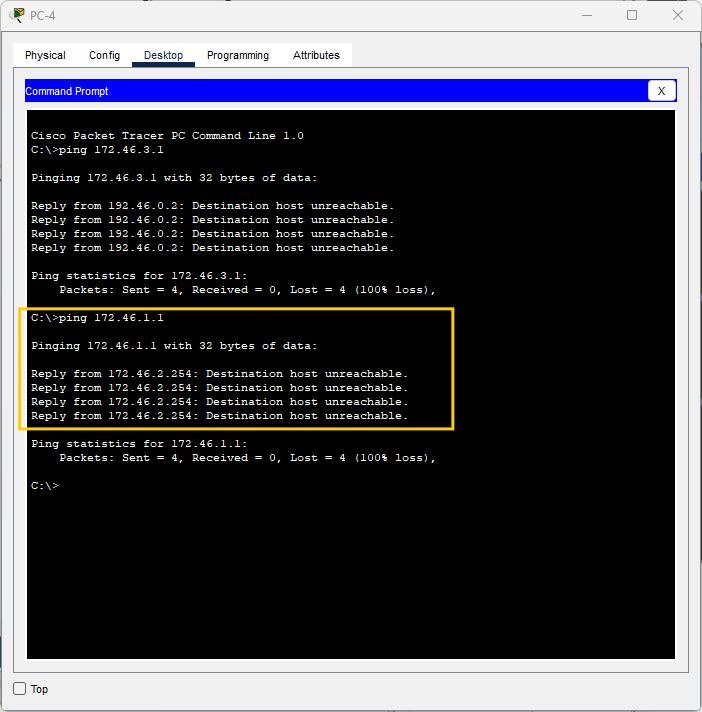


7.Configure extended ACLS to fulfil the following network policies:

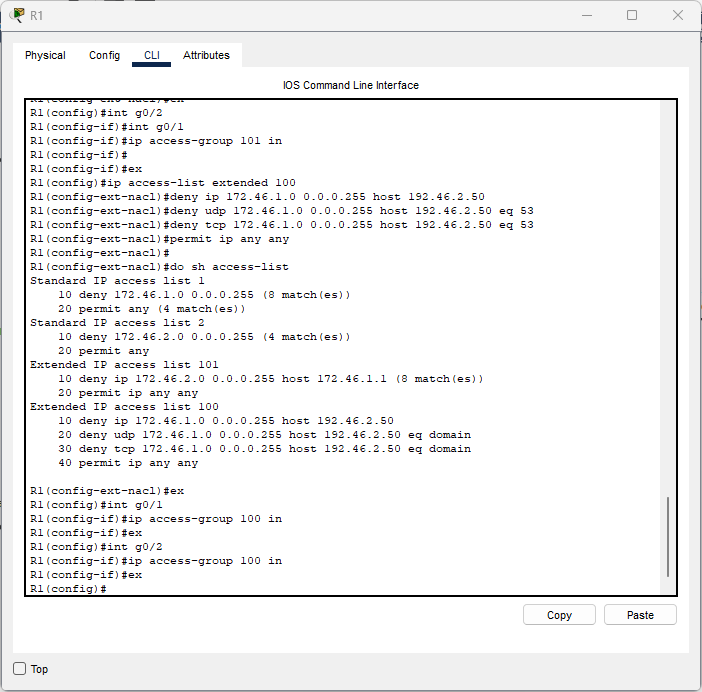
-Hosts in 172.16.2.0/24 can't communicate with PC1.

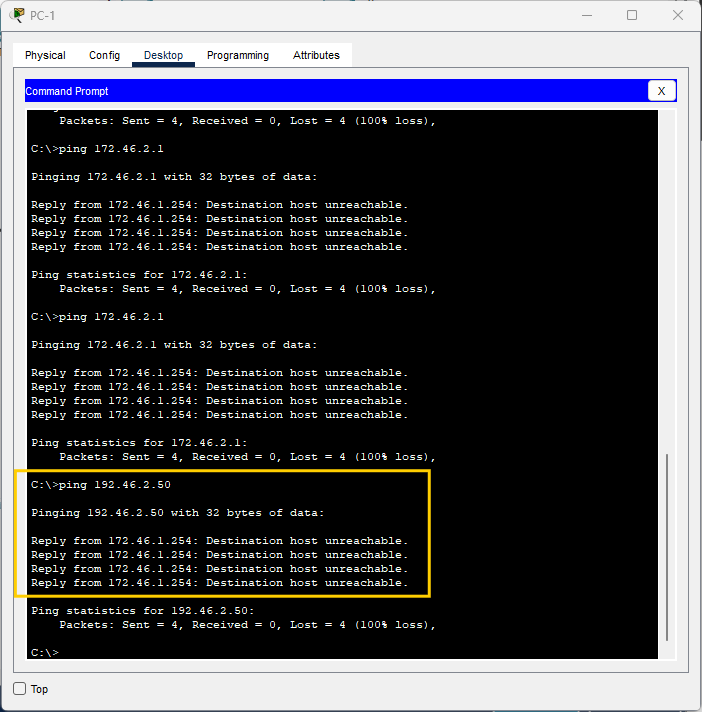


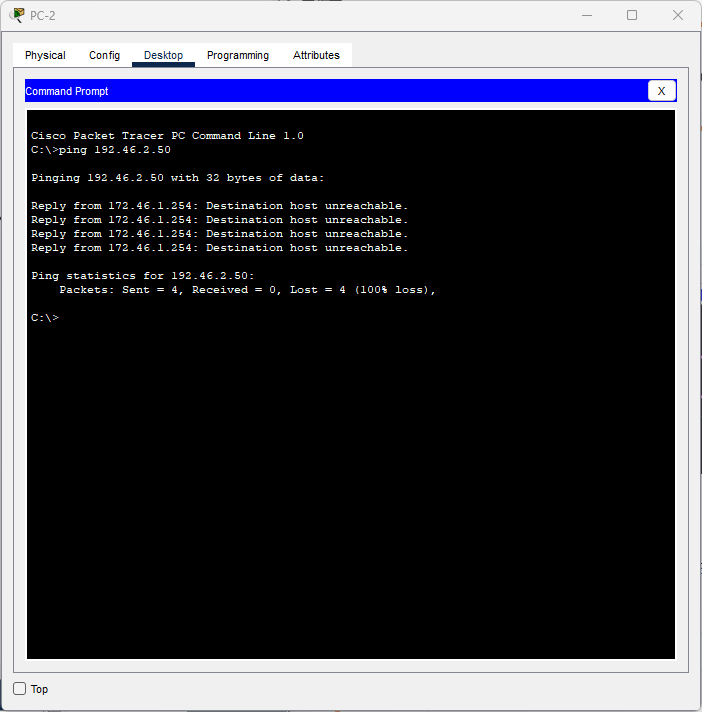




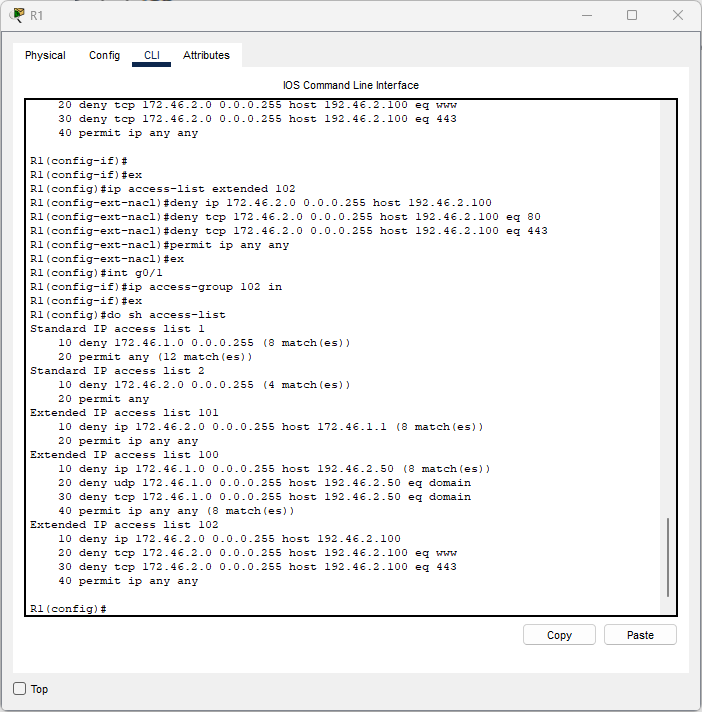
-Hosts in 172.16.1.0/24 can't access the DNS service on SRV1.

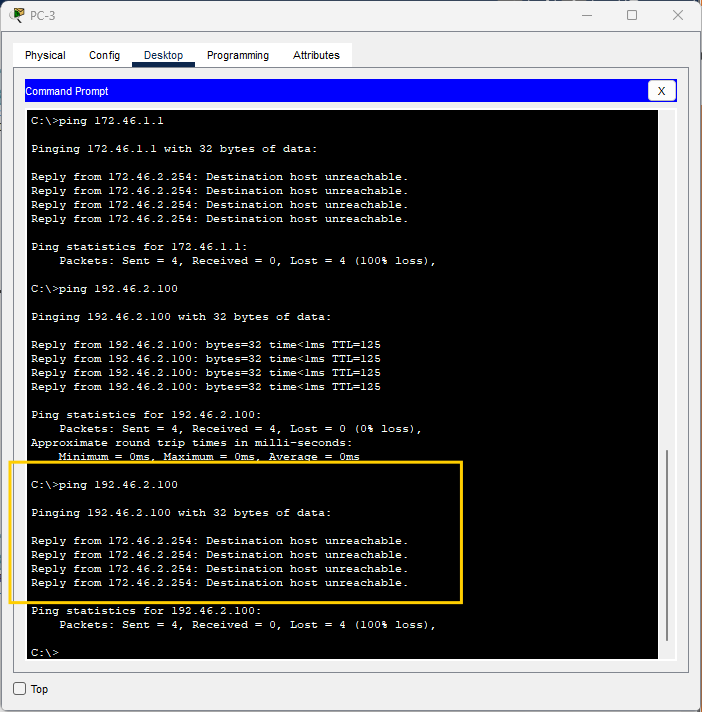


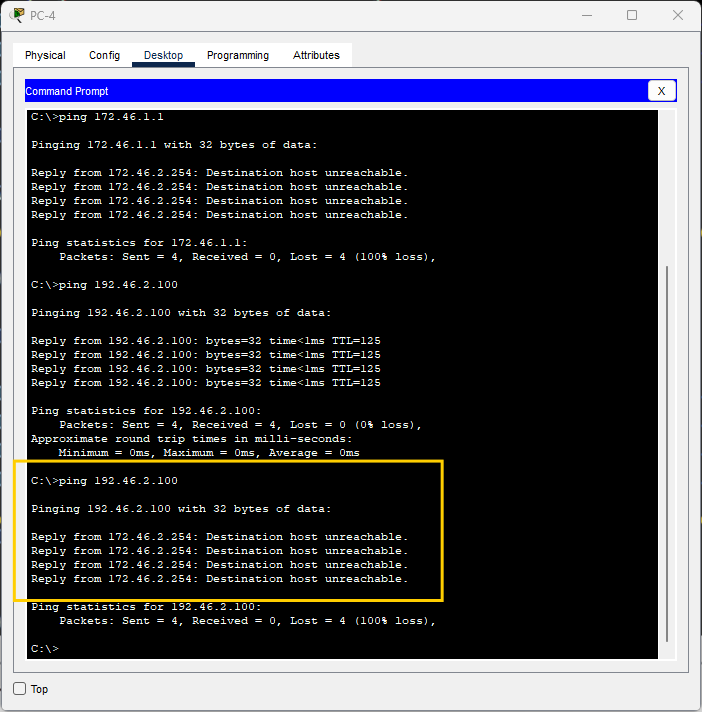


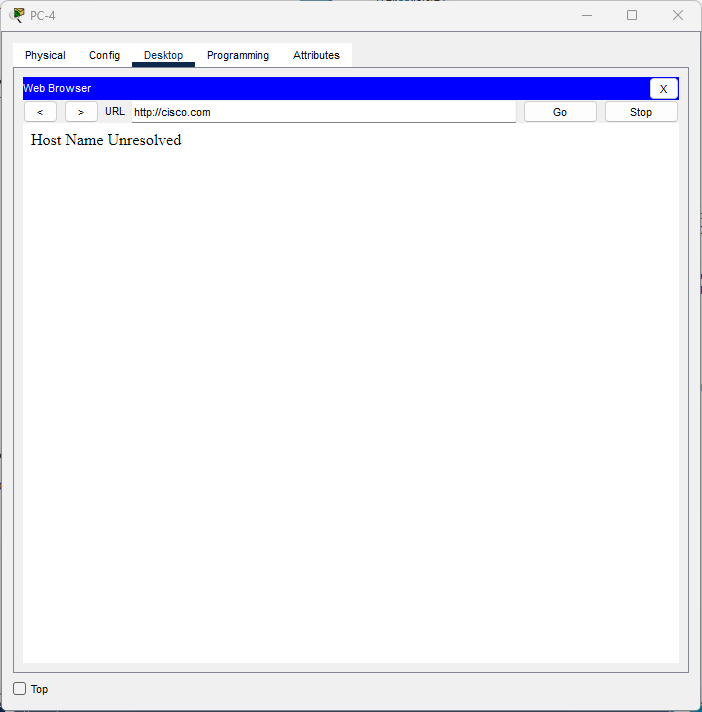


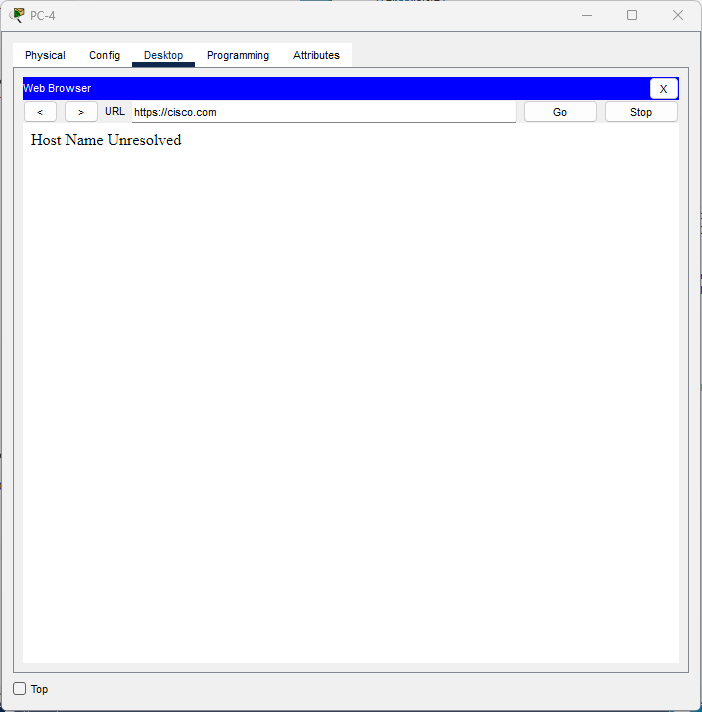
-Hosts in 172.16.2.0/24 can't access the HTTP or HTTPS services on SRV2.











8.Verify Each Entries

above gave under the each and every network policies.

9.Print the Access lists

