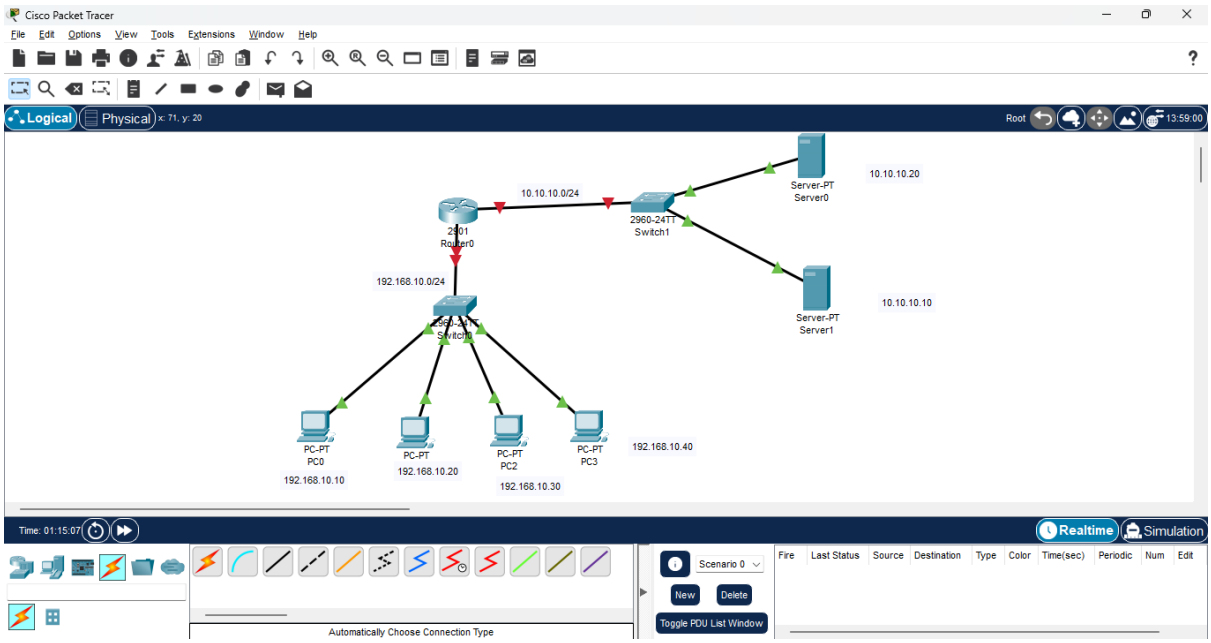
Q12) Create an extended ACL to block specific applications, such as HTTP or FTP traffic. Test the ACL rules by attempting to access blocked services.



CLI:

Router> enable

Router# configure terminal

Router(config)# interface FastEthernet 0/0

Router(config-if)# ip address 192.168.1.1 255.255.255.0

Router(config-if)# no shutdown

Router(config-if)# exit

Router(config)# access-list 100 deny tcp host 192.168.1.10 host 192.168.1.20 eq 80

Router(config)# access-list 100 deny tcp host 192.168.1.10 host 192.168.1.20 eq 20

Router(config)# access-list 100 deny tcp host 192.168.1.10 host 192.168.1.20 eq 21

Router(config)# access-list 100 permit ip any any

Router(config)# interface FastEthernet 0/0

Router(config-if)# ip access-group 100 in

Router(config-if)# exit

Router# show access-lists

Router# show running-config | include access-group

Output:

Router# show access-lists

Extended IP access list 100

10 deny tcp host 192.168.1.10 host 192.168.1.20 eq www

20 deny tcp host 192.168.1.10 host 192.168.1.20 eq ftp-data

30 deny tcp host 192.168.1.10 host 192.168.1.20 eq ftp

40 permit ip any any

This output confirms that ACL **100** is active and correctly blocking HTTP (port 80), FTP Data (port 20), and FTP Control (port 21) while allowing all other traffic.

Testing the ACL Rules:

PC1> ping 192.168.1.20

Reply from 192.168.1.20: bytes=32 time<1ms TTL=128

Blocked Traffic:

PC1> curl http://192.168.1.20

Request timed out