**Moulik Tammana**

**Q11. Implement ACLs to restrict traffic based on source and destination ports. Test rules by simulating legitimate and unauthorized traffic.**

**An Access Control List (ACL) is a set of rules used to filter network traffic based on criteria like IP addresses, protocols, and port numbers. ACLs are primarily used on routers and firewalls to enhance security and manage network access.**



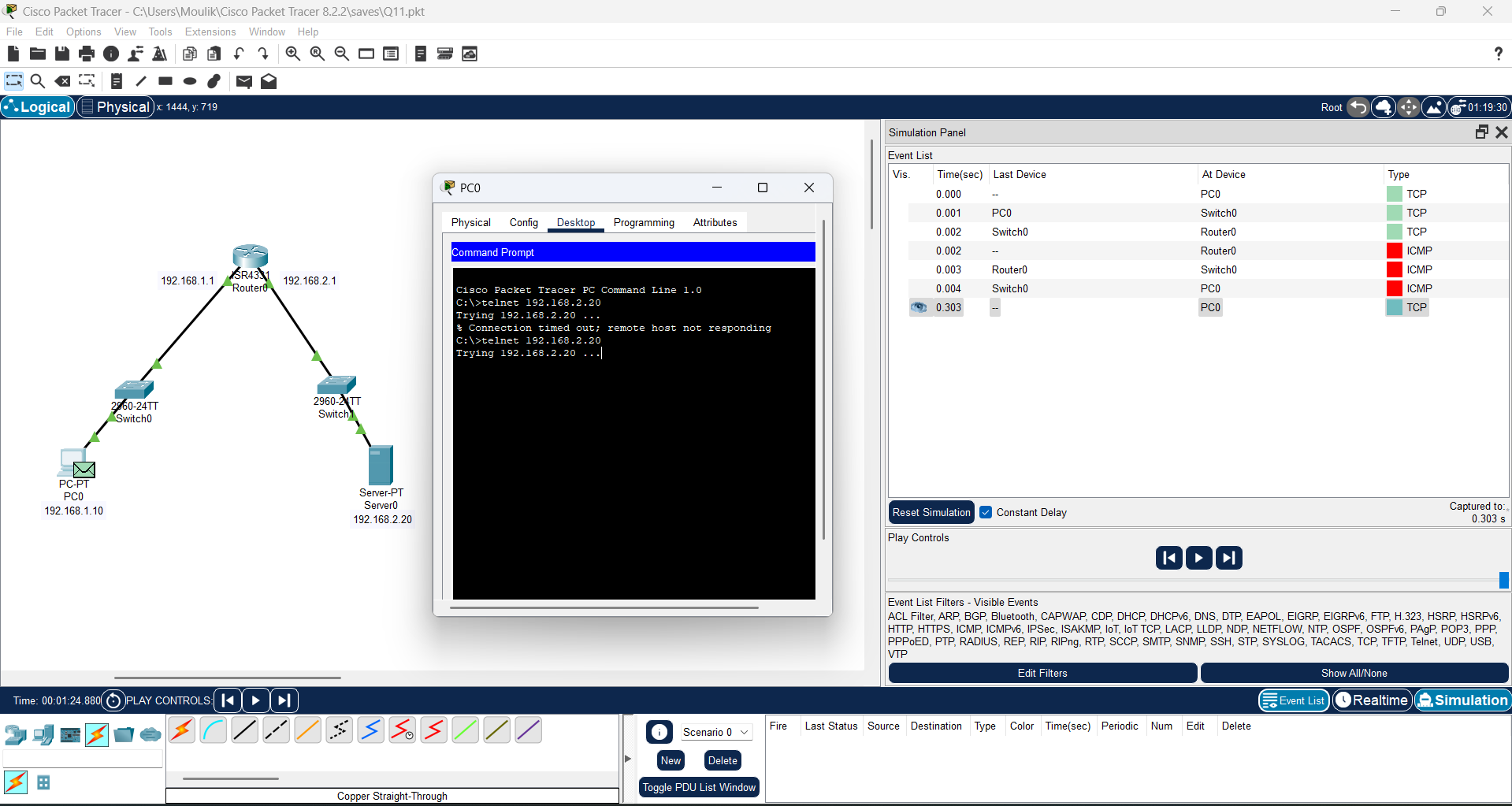
**Here the command denies tcp packets from 192.168.1.10 to 192.168.2.20 and eq 23 refers to port 23 which uses telnet protocol.**

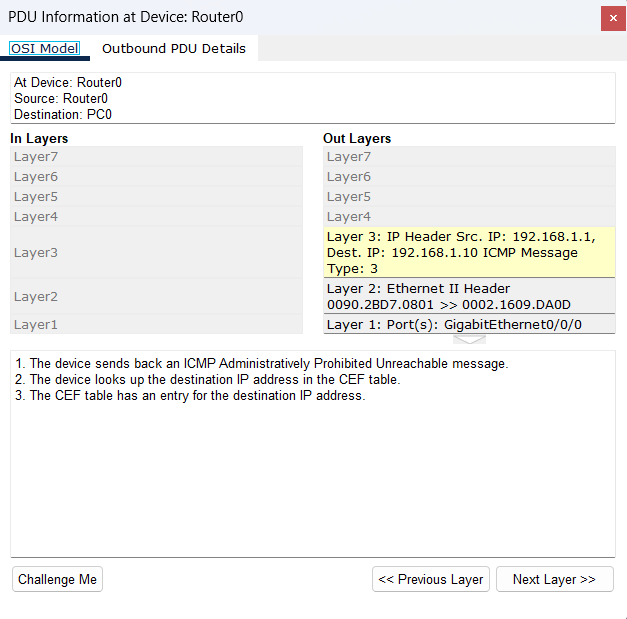
**The 0.0.0.0 after 192.168.1.10 is a Wildcard Mask. A wildcard mask is used in Access Control Lists (ACLs) to specify a range of IP addresses. It works opposite to a subnet mask:**

* **0 in a position means the corresponding bit in the IP must match exactly.**
* **1 in a position means the corresponding bit in the IP can be anything.**

**The next command is used to permit any other packets from any device to any device .i.e allow all other traffic.**

**When we try telnet from the PC to the server, it is blocked and we also receive a block message.**





**But when we try to ping, we were able to do it successfully.**

