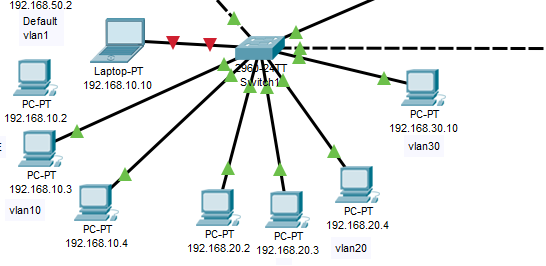
**DISCUSSIONS**

**After configuration, we have got the following achievements:**

1. We can create numbers of networks on the switches by using VLAN technology.
2. Here every PCs in Switch 1 are bind with port number and their MAC address. For this reason, no unauthorized PC, laptop can be a part of the network. If any unauthorized PC or laptop try to connect with the switch, then the port will be turn off and hence no further communication can take place for this unauthorized PC, laptop.

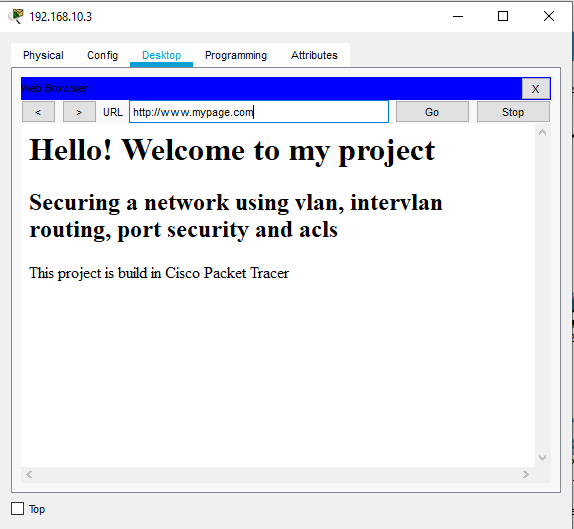
From the Figure 7.1, we can see that an unauthorized user is trying to get access of the network. Later he/she takes the cable of PC0 and connect with the laptop to get the access.



**Figure 7.1 Port- security**

But as the switchport port security has been enabled here, so the unauthorized can’t communicate with others though the laptop is connected with the network cable. When he/she tries to communicate with other, the port of the switch will be shutdown (see Figure 7.1, the port is coloured red that means shutdown) as the MAC address of the unknown laptop has not been included or bind on the switch.

1. No one can change the VLAN by themselves.
2. We can access the DNS server from any of the network. **Figure 7.2**



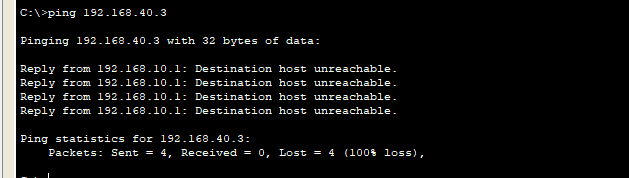
**Figure 7.2: Accessing DNS server**

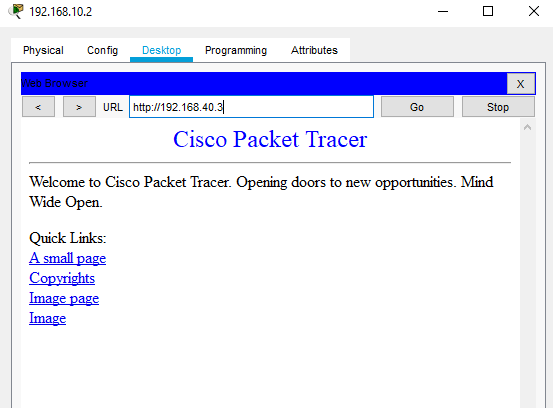
1. By using ACLs (Access Control Lists) we can restrict someone to the use of the network asset. For example, in our configuration, following ACLs are configured:

* Users on the network 192.168.10.0 should not able to ping the http server but they should be able to access the website. **Figure 7.3 and 7.4**
* Users on the network 192.168.20.0 cannot access the http server but can use other services. **Figure 7.5 and 7.6**
* Mr. X and Mr. Y cannot ping each other but the other members in the network can communicate with each other. **Figure 7.7**

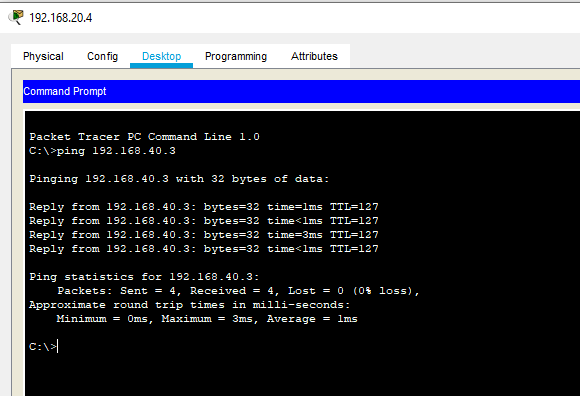
All others can communicate with each other, even these two PCs can ping or do any other communication except HTTP service. In this way we can restrict anyone to access any service of the network.

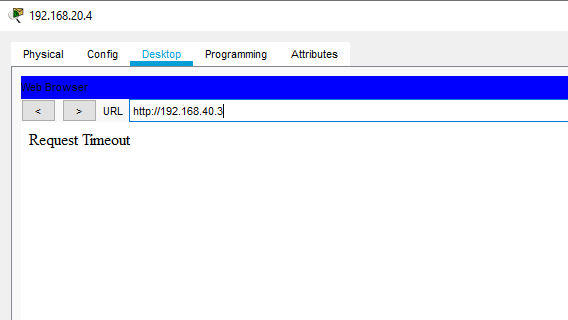
**Screenshots of the restrictions caused by ACLs:**





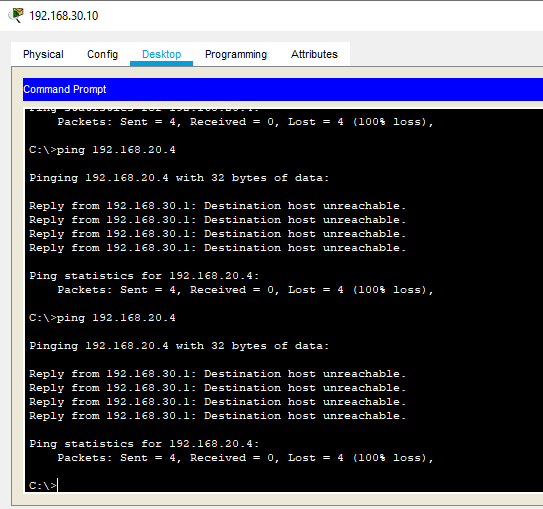
**Figure 7.3 and Figure 7.4**





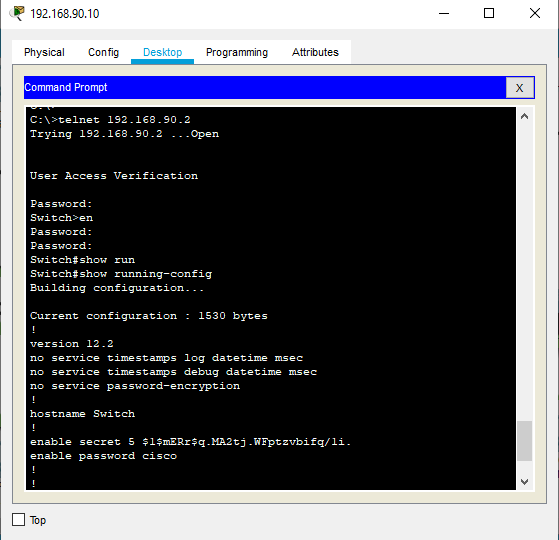
**Figure 7.5 and 7.6**

1. We can use the router as a firewall by using the ACL commands.
2. By using router’s sub interfaces feature, we can reuse the router’s limited fast Ethernet ports for multiple networks with the help of VLAN technology. In our case, we have used 1 physical port for 3 networks. If we don’t use sub interface feature, then we were needed 3 fast Ethernet ports for 3 different networks.



**Figure 7.7**

1. For Switch 0 we have created the Management PC for telnet, SSH purposes. By using this PC we can communicate with switch remotely. **Figure 7.8**



**Figure 7.8**