Access Control list

1. Introduction:

1.1. Standard Access Control List:

These are the ACLs in which filtering rules are defined using the source IP address only. These ACLs permit or deny the entire protocol suite of higher layers while filtering is applied on specific source IP address. Standard ACLs can't distinguish between the TCP, UDP and Https traffic of same source IP so all traffic of specific IP address will stay blocked. By using numbers 1-99 or 1300-1999 during configuration, router will understand it as a standard ACL and the specified address as source IP address.

1.2. Features:

- Standard Access-list is generally applied close to destination (but not always).
- In standard access-list, whole network or sub-network is denied.
- Standard access-list uses the range 1-99 and extended range 1300-1999.
- Standard access-list is implemented using source IP address only.
- If numbered with standard Access-list is used then remember rules can't be deleted. If one of the rule is deleted then the whole access-list will be deleted.
- If named with standard Access-list is used then you have the flexibility to delete a rule from access-list.

1.3. Types of Access Lists:

There are two ways in which inter-VLAN routing can be accomplished.

- Standard Access list
- Extended Access list

2. Tools required:

- CISCO Packet tracer

3. Objective of the Experiment:

Upon completion of this lab, you will be able to

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a switch to the default state.
- Perform basic configuration tasks on a switch
- Create Access List
- Able to do packet control
- Add, move, and change ports.
- Verify Access list configuration
- Enabling of access list on single host

- Enabling of access list on entire network
- Save the Access list configuration
- Removal of Access list

4. Walk through tasks:

4.1. Task1:

Construct a topology that have two switches attached with each other with copper cross through wire and four PC's attached with them, a pair with each switch, configure inter Virtual LAN in this configuration and show the results.

To configure this, we have to execute following steps:

1. Open CISCO packet tracer.
2. Add three generic routers in the workspace.
3. Add six generic PC's in the workspace.
4. Add 3 generic switches.
5. Connect each pair of generic computers with switch using copper straight through ire.
6. Also connect each router with a switch with copper straight through cable.
7. Connect each router together with serial cables.
8. The topology should be seen like this:

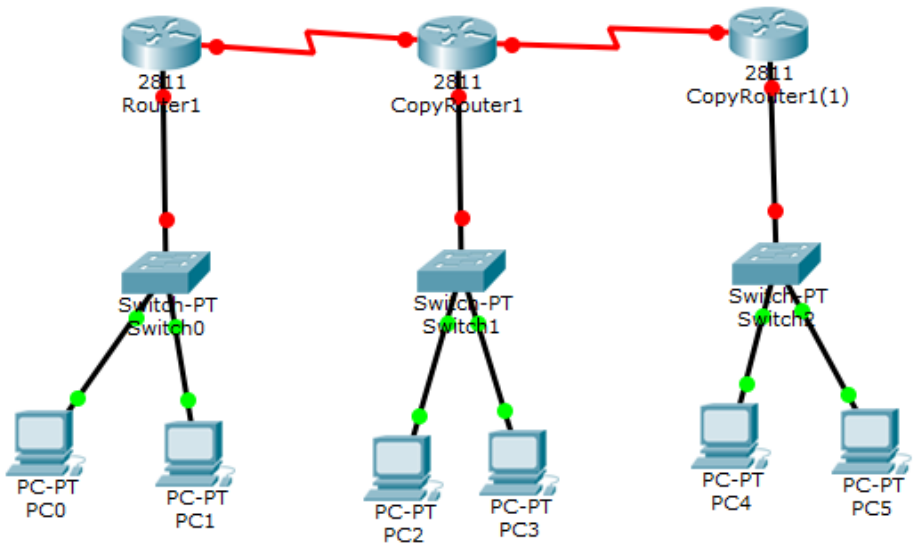

Figure 1: topology connection

9. Now add notes on the workspace in the front of every network entity with IP address and also mention the port numbers.
10. The workspace should be seen like this:

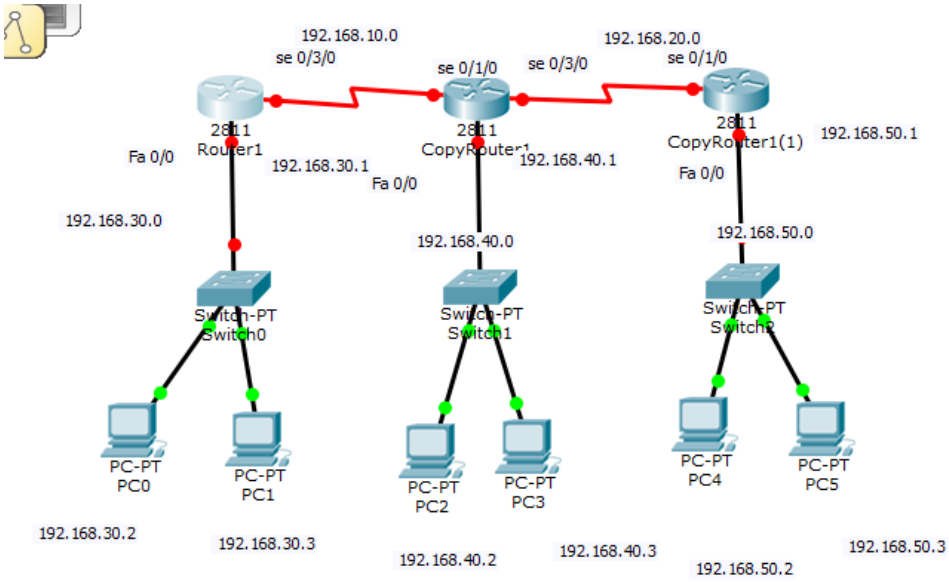

Figure 2: captions of the network entities.

11. Click on the router 1 and go in command line interface
12. Go in the privileged mode by using command **enable**.
13. Go in the configuration mode by using command **configure terminal**.
14. Now configure all the interfaces that you have already done in the previous labs.
15. Also configure serial ports and assign clock rate and proper bandwidth.
16. After configuring this you have to do IP routing whether, static routing or dynamic routing.
17. Your workspace should be seen like in the figure below, in which you can see all the interfaces turn on with green lights and the configuration is done. should be as:

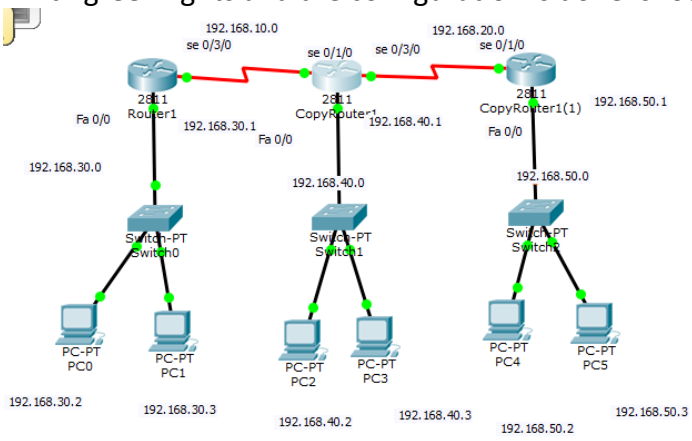

Figure 3: open ports.

18. Moreover, provide IP addresses to PC's and DO IP routing and check the connectivity by sending PDU. In this topology I have done dynamic routing by enabling RIP routing protocol.

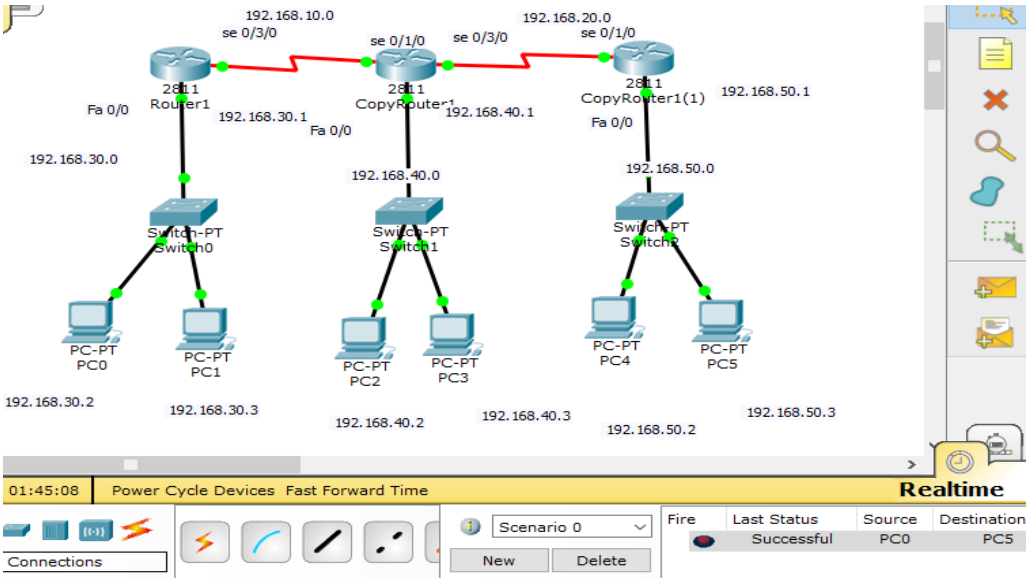

Figure 4: Successful PDU.

19. Now after bringing our topology in working condition, we have to apply ACL in topology, two types of ACL that can be implemented as discussed earlier, we will only apply Standard ACL in this task.
20. Standard ACL uses source address and are applied near the destination.
21. Now we want for example to control the computers of R1 that they can access or may not access the Router 3 computer therefore we have to apply the ACL on router 3.
22. Now go into the CLI of router 3 and after entering in configure terminal write command **access-list 1 deny host "which you want to block",** as 1 is the ACL number or group number, 1-99 is designated for standard ACL or 100-199 is for extended ACL. This is for blocking single host.
23. For this an additional command is also written which is after the above-mentioned command that is **access-list 1 permit any**, that will permit any other hosts in the network.
24. If you want to block entire network then write command, **access-list 1 deny "give network you want to block" "wildcard mask".**
25. Wildcard mask is the inverse of network mask. For example, a mask is 255.255.255.0 and wildcard mask is 0.0.0.255.
26. For viewing access list write command **show access-list**.
27. You can see access-list after this command but we didn't apply the access list anywhere, therefore, we have to apply on destination which can be applied in either as inbound or outbound, inbound is while packet is entering the router and outbound is while packet leaving the router.
28. Now go into the interface Fa 0/0 as we are applying on outbound, and write command after entering the interface which is **ip access-group 1 out** and press enter. Then check with PDU that is the router 3 blocking the PC of router 1 or not.

29. Check also by ping command.

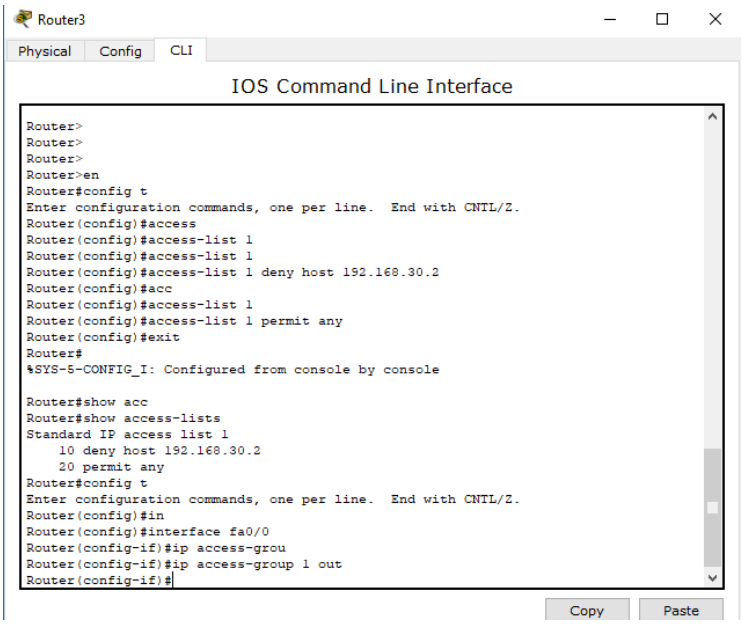

Figure 5: shows the CLI of the router.

5. Practice task:

5.1. Task 1:Block 192.168.1.0 from reaching to sarah's PC.

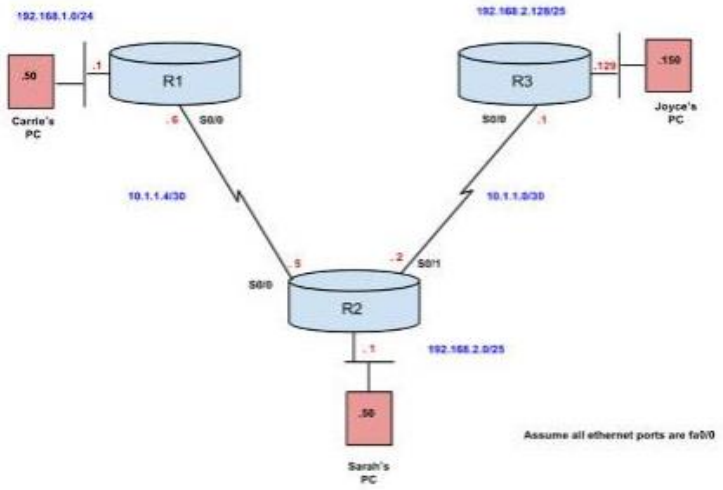

Figure 6: Practice Task 1.

5.2. . Task 2:

In the topology of walk-through task configure, ACL in such a pattern that only 192.168.40.3 can able to communicate with 192.168.50.3, no other host can communicate with either 192.168.40.3 and 192.168.50.3.