CSE 4412 [Data Communication and Networking]

Lab # 7

1. Objectives:

- Describe the concept of Access Control List (ACL)
- Implement standard numbered ACL
- Define and describe the concept of DHCP
- Configure DHCP on a router and also using a server
- Fetch IP addresses on host devices using DHCP
- Understand and implement DHCP on specific VLANs

2. Theory:

Access Control Lists (ACL):

Defining ***who*** *can/can't access* ***what*** is basically the gist of ACL. In our day-to-day life, we are applying the concept of ACL in many areas. A simple example could be like you need to show your ID card to enter an office. There's a list of employees and your ID is checked against that list to grant access. Similar access controls are in effect in virtually everywhere, especially in places where security is critical. In digital world, this access control is more needed so that only allowed ones can access a certain digital resource. For example, only admins would be allowed access in the backend of a web server or only database admins would be allowed to access database server etc.

In networked devices, ACLs play a crucial role to allow only authorized person/devices to a certain resource. For example, you can define that only a certain host device would be able to access your webserver. You can also define ACLs so that hosts belonging to a particular network can't communicate with hosts of certain other network. There are more scenarios that can be defined depending on the needs of an administrator.

In this lab, we'll learn about Cisco IP ACL i.e., filtering network traffic based on IP address. There are several ACL types that can be configured on a Cisco device. But for the purpose of this lab, we'll only focus on *Numbered Standard IPv4 ACL*. There are two steps to implement an ACL. First, **define the rule**. Second, **apply the rule to an interface**.

The command format for defining a numbered standard IP ACL is:

```
Router(config)# access-list access-list-number
                {permit|deny}
               {source_address source_wildcard|any}
```

You can either permit or deny a packet based on the source IP of the packet in numbered standard IP ACL. As like the OSPF configuration, you need to specify a wildcard mask to permit/deny a range of

source IP addresses based on the given pattern. One important thing you should keep in mind that whenever you apply an ACL to an interface, **all the traffic that doesn't match any ACL rule will be discarded by default**. So, for example, you have defined an ACL to deny a certain source IP. Whenever you apply that rule to an interface, all other packets other than the denied source will also be discarded because there's no matching rule for those packets. So, you must allow other traffic explicitly by defining another ACL. The **`any`** keyword is handy in this case. To permit (or deny) any packet other than the previously specified rules, you can just add the keyword **`any`** in place of the source_address and source_wildcard like the following:

```
Router(config)# access-list 1 permit any
```

Another thing is you can only use numbers in the range *1 to 99* for specifying the *`access-list-number`*. Other numbers are used for **extended numbered ACL**. After defining the ACL rule, now we need to apply it to an interface. Remember that the ACL has no effect until you apply it. The command format for applying an ACL to an interface is like below:

```
Router(config-if)# ip access-group access-list-number
                   {in|out}
```

The ACL is applied either for inbound traffic or outbound traffic of an interface and you need to specify the corresponding keyword i.e., **`in`** or **`out`** for that. One best practice before applying an ACL to an interface is to *verify* the rule by using the following command:

```
Router# show access-lists
```

[For the commands, the **`bold`** ones are *constant keywords* which should be exactly same. `Non-bold` ones are the configurable options.]

DHCP:

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automate the process of configuring devices on IP networks, thus allowing them to use network services such as DNS, NTP, and any communication protocol based on UDP or TCP. A DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks.

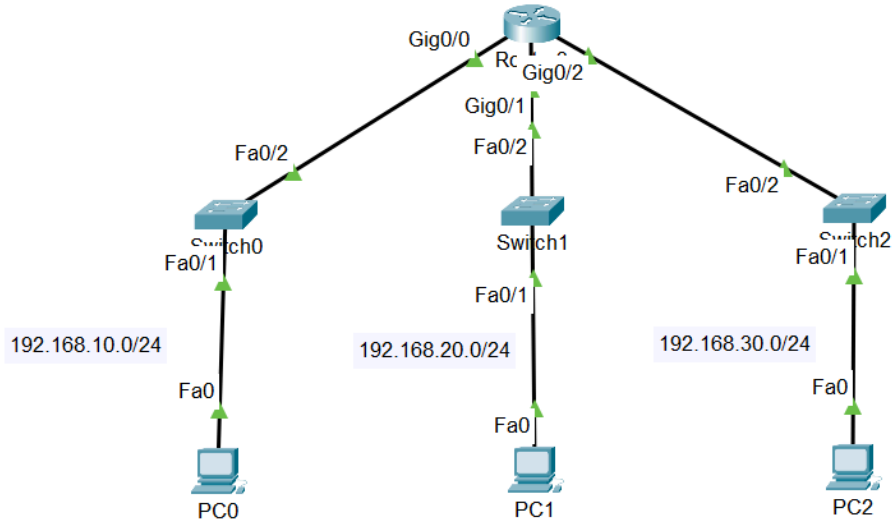
The DHCP server maintains a database of available IP addresses and configuration information. When it receives a request from a client, the DHCP server determines the network to which the DHCP client is connected, and allocates an IP address or prefix appropriate for the client, and sends configuration information appropriate for that client.

The DHCP server and DHCP client must be connected to the same network link. In larger networks, each network link contains one or more DHCP relay agents. These DHCP relay agents receive messages

from DHCP clients and forward them to DHCP servers. DHCP servers send responses back to the relay agent, and the relay agent then sends these responses to the DHCP client on the local network link.

DHCP servers typically grant IP addresses to clients for a limited interval called a lease. DHCP clients are responsible for renewing their IP address before that interval has expired, and must stop using the address once the interval has expired, if they have not been able to renew it.

3. Configure ACL:



I. Configure Router Interfaces

```
Router(config)# int g0/0
Router(config-if)# ip address 192.168.10.1 255.255.255.0
Router(config-if)# no shutdown
Router(config)# int g0/1
Router(config-if)# ip address 192.168.20.1 255.255.255.0
Router(config-if)# no shutdown
Router(config)# int g0/2
Router(config-if)# ip address 192.168.20.1 255.255.255.0
Router(config-if)# no shutdown

Router(config-if)# exit
Router# copy running-config startup-config
```

II. Configure PC0

```
IP: 192.168.10.5
Mask: 255.255.255.0
Gateway: 192.168.10.1
```

III. Configure PC1

```
IP: 192.168.20.5
Mask: 255.255.255.0
Gateway: 192.168.20.1
```

IV. Configure PC2

```
IP: 192.168.30.5
Mask: 255.255.255.0
Gateway: 192.168.30.1
```

V. Define ACL

```
Router(config)# access-list 1 deny 192.168.10.0 0.0.0.255
Router(config)# access-list 1 permit any
```

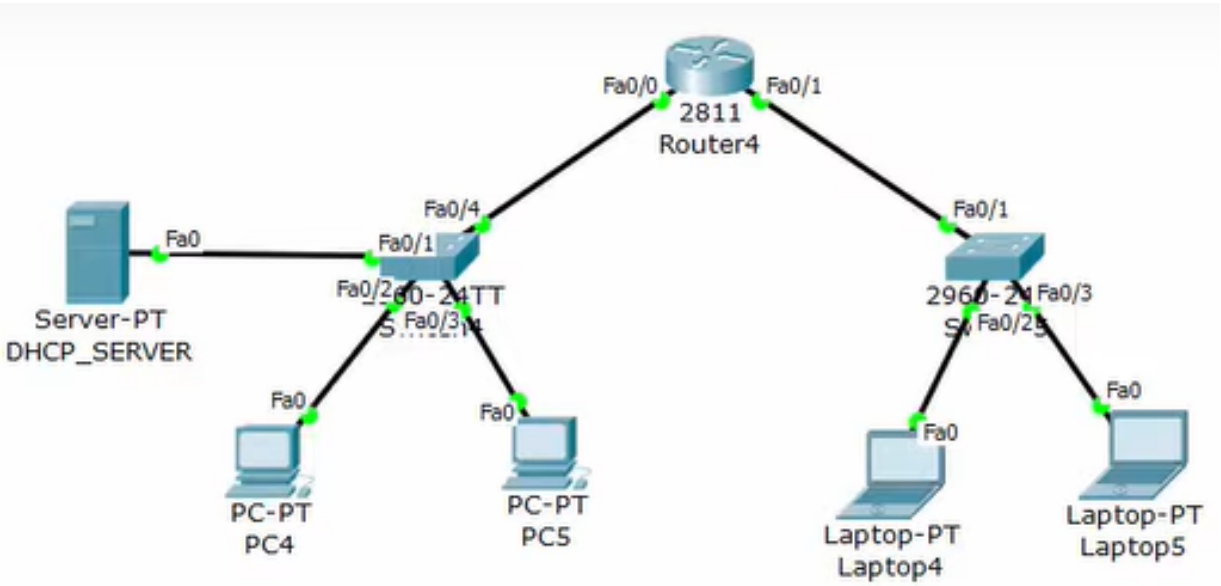
VI. Verify ACL

```
Router# show access-lists
```

VII. Apply ACL

```
Router(config)# interface gigabitEthernet 0/2
Router(config-if)# ip access-group 1 out
```

4. Configure DHCP (using server):



I. Configure DHCP Server

Go to Desktop and then IP config

```
IP Address: 192.168.1.2
Default: 192.168.1.1
```

II. Make DHCP Pools

Go to Services and then DHCP

```
Pool Name: dotONEnetwork
Default: 192.168.1.1
Start IP: 192.168.1.3
Max Number: 20

Pool Name: dotTWOnetwork
Default: 192.168.2.1
Start IP: 192.168.2.2
Max Number: 20

Do not forget to turn on the DHCP server
```

III. **Configure R1 Interfaces**

```
R1(config)#int fa0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# ip helper-address 192.168.1.2
R1(config-if)#no shutdown
R1(config-if)#exit

R1(config)#int fa0/1
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# ip helper-address 192.168.1.2
R1(config-if)#no shutdown
R1(config-if)#exit
```

IV. Configure all the PCs

```
Just click DHCP and the server will do the rest
```

V. Verify

```
Ping PC1 from PC0
```

5. Configure DHCP (inside router):

```
R1(config)# ip dhcp pool dotONEnetwork
R1(dhcp-config)# default-router 192.168.1.1
R1(dhcp-config)# network 192.168.1.0 255.255.255.0
R1(dhcp-config)# exit

R1(config)# ip dhcp pool dotTWOnetwork
R1(dhcp-config)# default-router 192.168.2.1
R1(dhcp-config)# network 192.168.2.0 255.255.255.0
R1(dhcp-config)# exit
```

Use "show ip dhcp binding" inside the router to see the status of the configured DHCP

6. Tasks: (Make sure you are prepared for a viva)

I. IUT is given an IP address of 192.167.X+5.0 where X= last 2 digits of your Student ID. IUT Medical Center only wants to allow traffic from IUT Administrative Building and block traffic from Academic Building -1 and Academic Building -2. Make appropriate connections with subnet masks to form the topology. (You can consider the academic buildings sharing a single switch) Then apply ACL to fulfill the criteria.

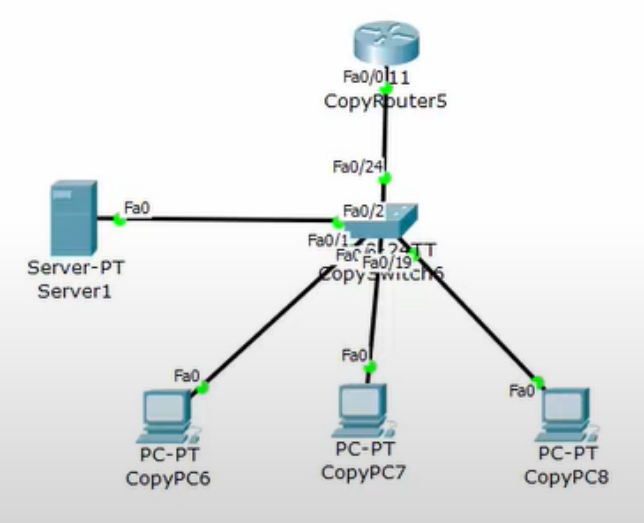
For task II and III

Here, consider **3 VLANs for the 3 PCs.**

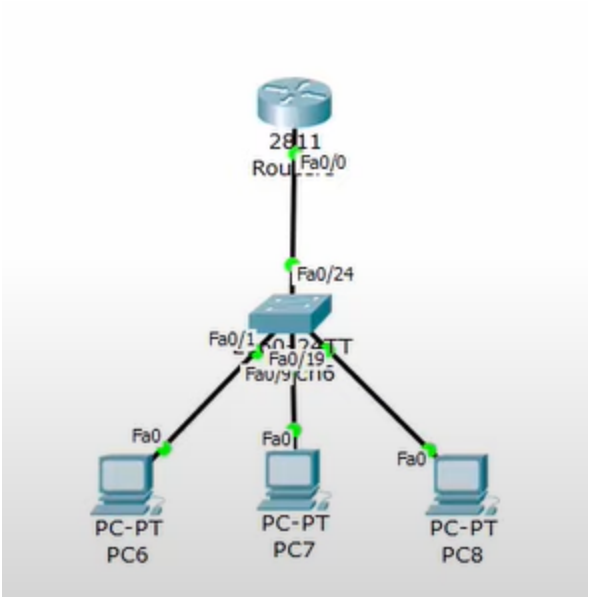
Use the network 192.167.X+5.0 /24

Here, X= last 2 digits of your student ID

II. You will implement **DHCP using a server** following the address configurations in a given network topology in this task.



III. You will implement **DHCP using a router** following the address configurations in a given network topology in this task.


2811
Fa0/0
Fa0/24
Fa0
Fa0
Fa0
PC-PT
PC6
PC-PT
PC7
PC-PT
PC8