LAB6 ACLs Configuration

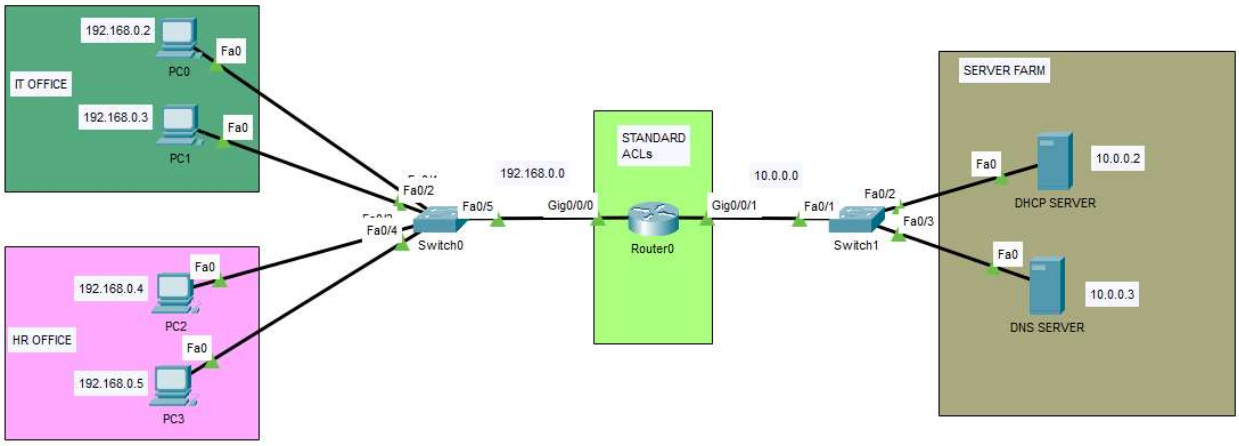
Standard ACL Configuration

Steps in Configuring Standard ACL

1. Draw necessary topology and label it accordingly
2. Configure IP addresses to the routers and hosts
3. Try to ping the servers from IT and HR departments
4. Configure standard ACLs to only permit the two IT PCs while denying the rest
5. Bind the ACL created on either router interfaces.
6. Try again to ping the servers from IT and HR departments

Set up the following topology

Assign IP addresses to all devices on your topology. For the router interfaces use the first IP address of that particular network.



Test Connectivity

Ensure you are able to ping the server farms from IT and HR departments.

Configure standard ACLs

Configure standard ACLs to only permit the two IT PCs access the server farms and deny the rest. On the router configure the following.

```
Router(config)#access-list 33 permit host 192.168.0.2
Router(config)#access-list 33 permit host 192.168.0.3
Router(config)#access-list 33 deny any
```

Binding the ACLs configuration to a specific interface or port.

```
Router(config)#interface gigabitEthernet 0/0/0
Router(config-if)#ip access-group 33 in
Router(config-if)#exit
```

After doing the above configurations, you can test connectivity again, this time IT should be able to access the server farm and HR should not.

Things to note:

As shown below, using number 1-99, represents Standard access control lists while 100-199, represents Extended access control lists. During configurations keep this in mind.

```
Router(config)#access-list ?
  <1-99>     IP standard access list
  <100-199>  IP extended access list
```

Below are options of what you can permit when setting ACLs policies, you can either permit specific IP address, any or host.

```
Router(config)#access-list 33 permit ?
  A.B.C.D  Address to match
  any      Any source host
  host     A single host address
```

To see your ACLs configuration use the following line.

```
Router#show access-lists
Standard IP access list 33
    10 permit host 192.168.0.2
    20 permit host 192.168.0.3
    30 deny any
```

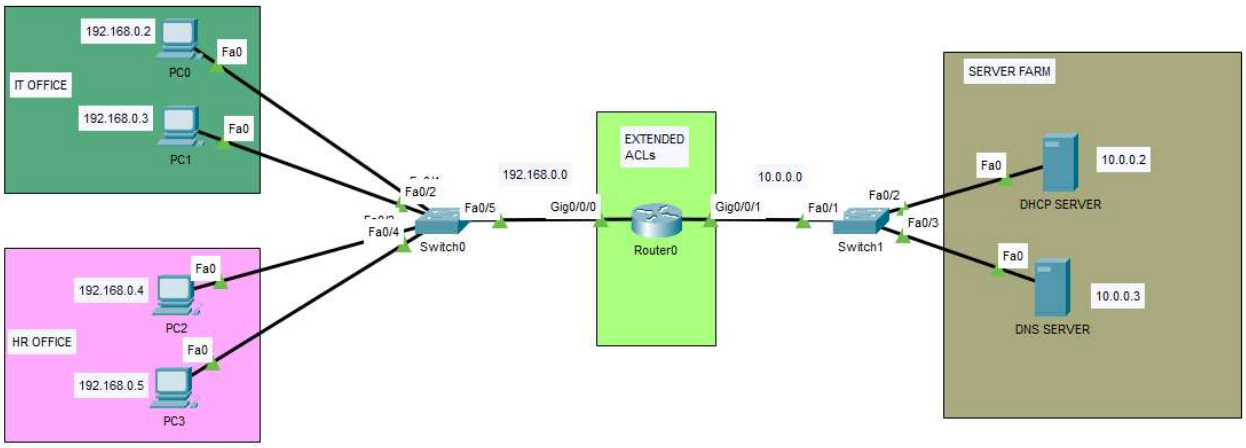
Extended ACL configuration

Steps in Configuring Extended ACL

1. Draw necessary topology and label it accordingly
2. Configure IP addresses to the routers and hosts
3. Try to ping the servers from IT and HR departments
4. Configure an extended ACL to only permit the two IT PCs to access DHCP server while denying the rest
5. Bind the ACL created on either router interfaces
6. Try again to ping the servers from IT and HR departments

Set up the following topology

Assign IP addresses to all devices on your topology. For the router interfaces use the first IP address of that particular network.



Test Connectivity

Ensure you are able to ping the server farms from IT and HR departments.

Configure Extended ACLs

Configure extended ACLs to only permit the two IT PCs access the DHCP server and deny the rest. On the router configure the following. When configuring E-ACLs you must declare the source IP and subnet mask, the destination IP and subnet mask as shown below.

```
Router(config)#access-list 120 permit ip 192.168.0.2 255.255.255.0 10.0.0.2 255.0.0.0
Router(config)#access-list 120 permit host 192.168.0.3 255.255.255.0 10.0.0.2 255.0.0.0
Router(config)#access-list 120 deny ip any any
```

Binding the ACLs configuration to a specific interface or port.

```
Router(config)#interface gigabitEthernet 0/0/0
Router(config-if)#ip access-group 120 in
Router(config-if)#exit
```

After doing the above configurations, you can test connectivity again, this time IT should be able to access the DHCP server and HR should not.