INSTITUTE OF ENGINEERING

ADVANCED COLLEGE OF ENGINEERING AND MANAGEMENT
Kupondole, Lalitpur
(AFFILIATED TO TRIBHUVAN UNIVERSITY)

Lab no:5
Subject: Computer Network

Submitted By:

Name: Sameep Dhakal
Roll no: ACE074BCT063
Date: 09/07/2021

Submitted To:

Department of Computer
and
Electronics Engineering

Lab 5

Title: Access Control List (ACL)

Objective:

To Learn about filtering of the network traffic

Introduction:

Access-list (ACL) is a set of rules defined for controlling the network traffic and reducing network attack. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network.

There are two main different types of ACL:

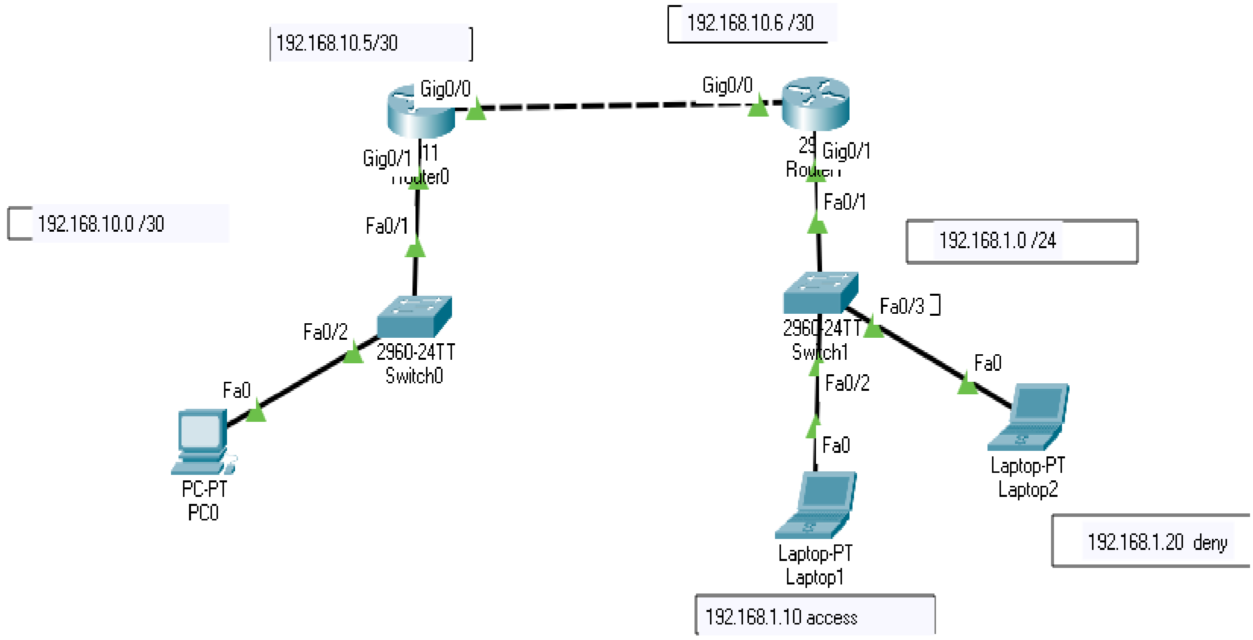
1. Standard Access-list:

   These are the Access-list which are made using the source IP address only. These ACLs permit or deny the entire protocol suite. They don't distinguish between the IP traffic such as TCP, UDP, Https etc.

2. Extended Access-list:

   These are the ACL which uses both source and destination IP address. In this type of ACL, we can also mention which IP traffic should be allowed or denied. These use range 100-199 and 2000-2699.

Design:



Procedure:

1. First the required tools are selected.
2. The required ports of the routers were turned on.
3. Then th Ip and subnet mask of the laptops, pc and routers were set
    a. For each laptop and pc this was done by going to the desktop and Ip configurations
    b. For routers this was done by going to the configuration and selecting the required port
4. Required connections were made between the routers and laptops
5. Then the Acl is used in router for giving permission to the network traffics

Code

```
Router0>enable
Router0# config terminal
Router0(config)#enable secret cisco
Router0(config)#line console 0
Router0(config-line)#password cisco
Router0(config-line) # login
Router0(config-line) # exit
Router0(config)#interface gig 0/0
Router0(config-if) # ip address 192.168.10.5 255.255.255.252
Router0(config-if) # no shutdown
Router0(config-if)#exit
Router0(config)#interface gig 0/1
Router0(config-if)#ip address 192.168.10.1 255.255.255.0
Router0(config-if)#no shutdown
Router0(config-if)#exit
Router0(config)#ip route 192.168.1.0 255.255.255.0 192.168.10.6
```

Access Control List

Specify the allow and deny address of the router port 0/1

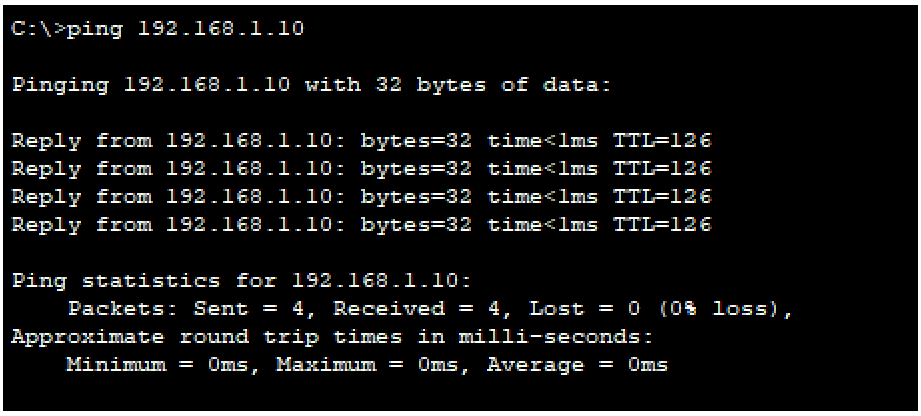
```
Router0(config)#interface gig 0/1
Router0(config-if)#access-list 1 deny 192.168.1.20
Router0(config)#access-list 1 permit any
Router0(config)#interface gig 0/1
Router0(config-if)#ip access-group 1 in
Router0(config-if)#exit
```

```
Router1>enable
Router1# config terminal
Router1(config)#enable secret cisco
Router1(config)#line console 0
Router1(config-line)#password cisco
Router1(config-line) # login
Router1(config-line) # exit
Router1(config)#interface gig 0/0
Router1(config-if) # ip address 192.168.10.6 255.255.255.252
Router1(config-if) # no shutdown
Router1(config-if)#exit
Router1(config)#interface gig 0/1
Router1(config-if)#ip address 192.168.1.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#ip route 192.168.10.0 255.255.255.252 192.168.10.5
```

Outputs:

Ping PC0 to Laptop1

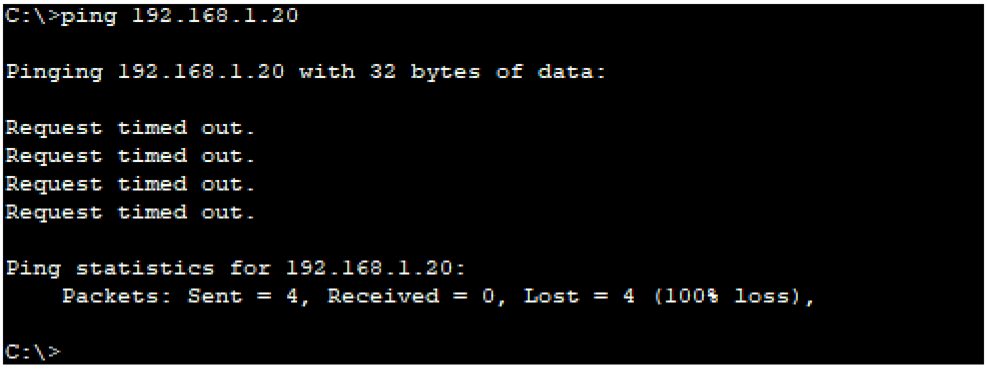
Access Route



```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<1ms TTL=126
Reply from 192.168.1.10: bytes=32 time<1ms TTL=126
Reply from 192.168.1.10: bytes=32 time<1ms TTL=126
Reply from 192.168.1.10: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ping PC0 to laptop2

Deny Route



```
C:\>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Result and Conclusion

In this lab we able to filter traffic from the network and which can be used for blocking the access of unwanted routes.