Experiment 04: Access Control List (ACL) Configuration Using Cisco Packet Tracer (Standard and Extended)

1. Introduction

Access Control Lists (ACLs) are a fundamental security feature used in computer networks to control traffic flow and restrict unauthorized access. In Cisco networking devices, ACLs are used to permit or deny packets based on specific criteria such as source IP address, destination IP address, protocol type, and port number.

Cisco routers support two main types of ACLs:

- **Standard ACL**
- **Extended ACL**

This lab demonstrates how to configure both Standard and Extended ACLs using Cisco Packet Tracer.

2. Learning Outcomes

After completing this lab, students will be able to:

- Understand the purpose of Access Control Lists
- Differentiate between Standard and Extended ACLs
- Configure Standard ACLs on a Cisco router
- Configure Extended ACLs on a Cisco router
- Apply ACLs to router interfaces correctly
- Verify and troubleshoot ACL behavior using network testing tools

3. Software and Hardware Requirements

Software Requirements

- Cisco Packet Tracer

Hardware Requirements

- Cisco Router (e.g., 2911)
- Cisco Switch
- End Devices (PCs, Servers)

- Cables (Straight Through)

4. Basic Concepts

Standard ACL

- Filters traffic based **only on source IP address**
- ACL numbers: **1–99**
- Usually applied **close to the destination**

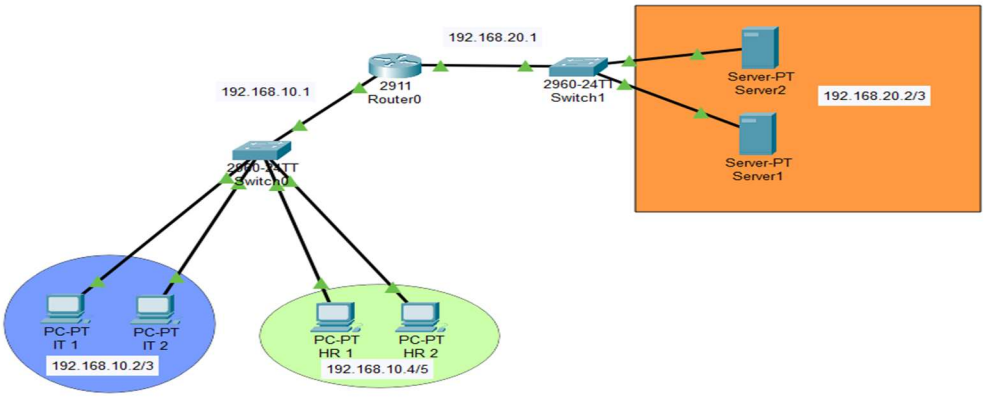
Extended ACL

- Filters traffic based on:
    - Source IP
    - Destination IP
    - Protocol (TCP, UDP, ICMP)
    - Port numbers
- ACL numbers: **100–199**
- Usually applied **close to the source**

5. Network Topology Description

The topology consists of:

- Two LANs
- A router connecting the networks
- ACLs applied on router interfaces to control communication



6. Procedure: Standard ACL Configuration

Step 1: Create the Network Topology

- Place a router, switch, and two PCs and servers in Packet Tracer
- Connect devices using appropriate cables

Step 2: Configure IP Addresses

- Assign IP addresses to PCs
- Configure router interfaces with IP addresses
- Set default gateways on PCs

Step 3: Configure Standard ACL

Enter router CLI and type:

enable

configure terminal

access-list 10 permit host 192.168.10.2

access-list 10 permit host 192.168.10.3

access-list 10 deny any

Step 4: Apply ACL to Interface

interface g0/0

ip access-group 10 in

exit

Step 5: Verify

- Use ping command
- Observe allowed and denied traffic

7. Procedure: Extended ACL Configuration

- **Step 1: Enter Global Configuration Mode**

  access-list 120 permit ip 192.168.10.2 255.255.255.0 192.168.20.2 255.255.255.0
  access-list 120 permit ip 192.168.10.3 255.255.255.0 192.168.20.2 255.255.255.0
  access-list 120 deny ip any any
  do wr

Apply ACL Near Source

int gig0/0

ip access-group 120 in

exit

Step 4: Verification

- Test using ping and web traffic
- Use Simulation Mode in Packet Tracer

10. Conclusion

In this lab, we have successfully configured Standard and Extended Access Control Lists using Cisco Packet Tracer. ACLs play a vital role in network security by controlling traffic flow and protecting network resources. Mastery of ACL configuration is essential for network administrators and cybersecurity professionals.