

## Lab 10: Implementing ACL in Packet Tracer

### Theory

Access Control Lists (ACLs) are used to manage and control network traffic. They work by examining the IP addresses, protocols, and port numbers to determine whether to allow or block traffic. ACLs enhance network security by enforcing rules that either permit or deny traffic based on specific criteria. There are two main types of ACLs:

- **Standard ACLs:** These focus solely on the source IP address to control traffic.
- **Extended ACLs:** These offer more detailed control by evaluating both source and destination IP addresses, as well as protocols and port numbers.

### Network Diagram

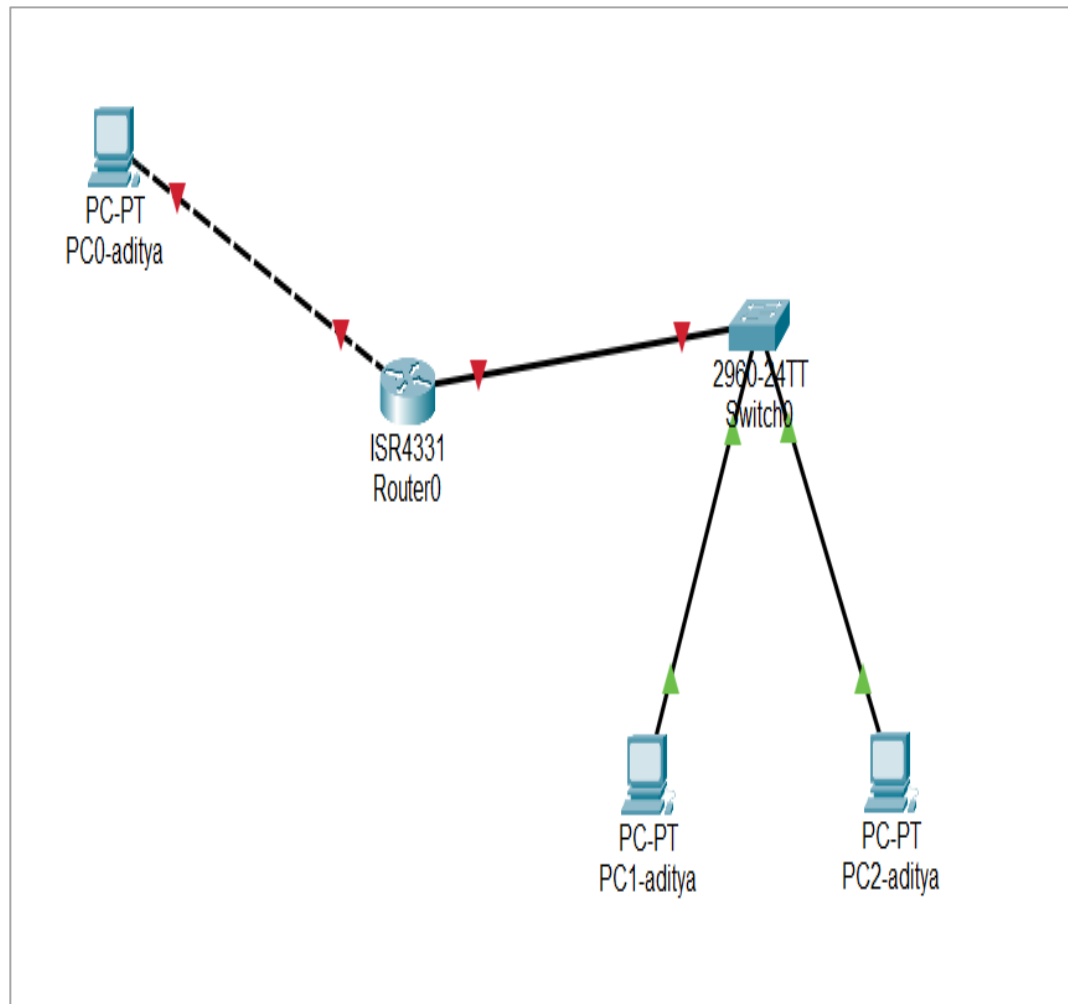


Fig: Network Diagram

## Implementation sequence

### 1. Open packet tracer and setup the devices

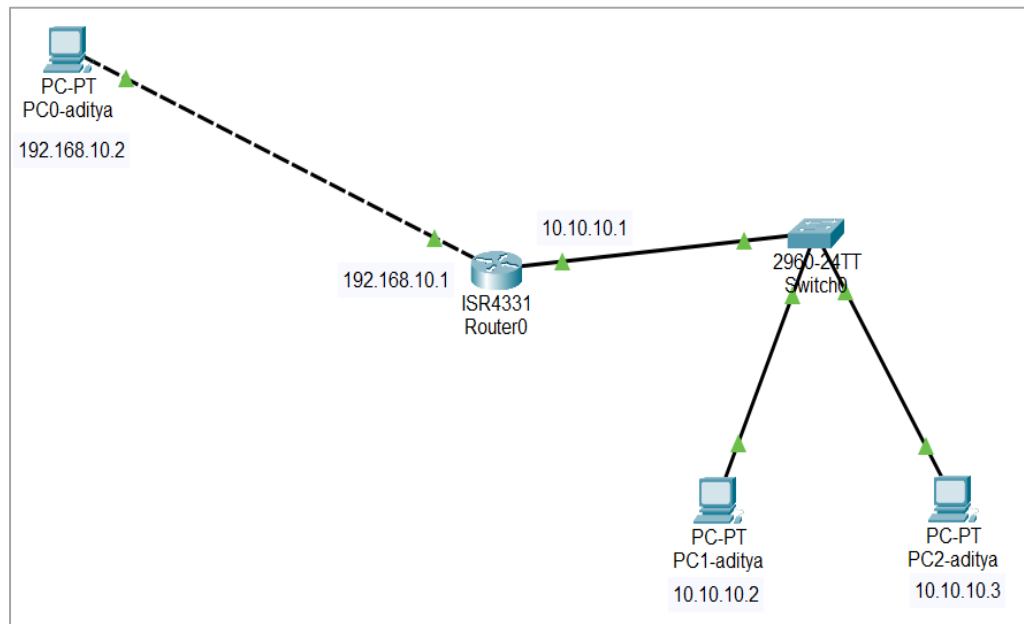


Fig: Network setup

### 2. Assign Ip address and subnet mask to each pc.

PC0: 192.168.10.2

PC1: 10.10.10.2

PC2: 10.10.10.3

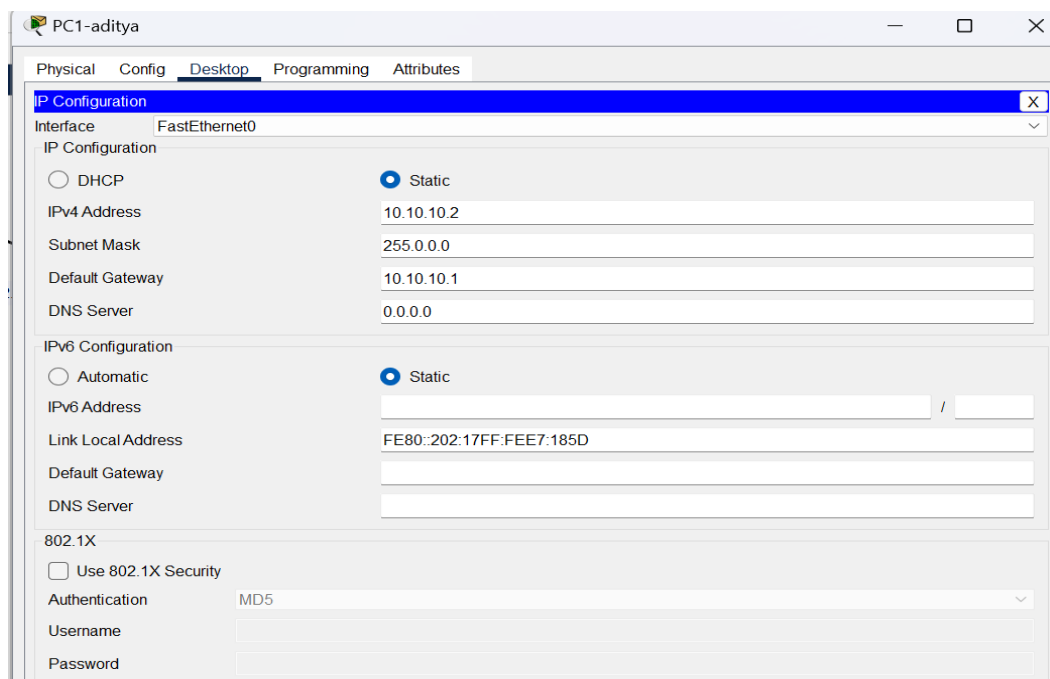


Fig: Ip configuration

### 3. Configure router and gigabit ethernet

Open routers CLI and run the commands to enable gigabit ethernet

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#ip address 10.10.10.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up
```

Fig: Router configuration

### 4. Configure deny and permit list

Open routers CLI and run the following commands to configure deny and permit list:

Router #conf t

Router(config) #access-list 1 deny host 10.10.10.2

Router(config) #access-list 1 permit host 10.10.10.3

Router(config) #int gig0/0/1

Router(config-if) #ip access-group 1 in

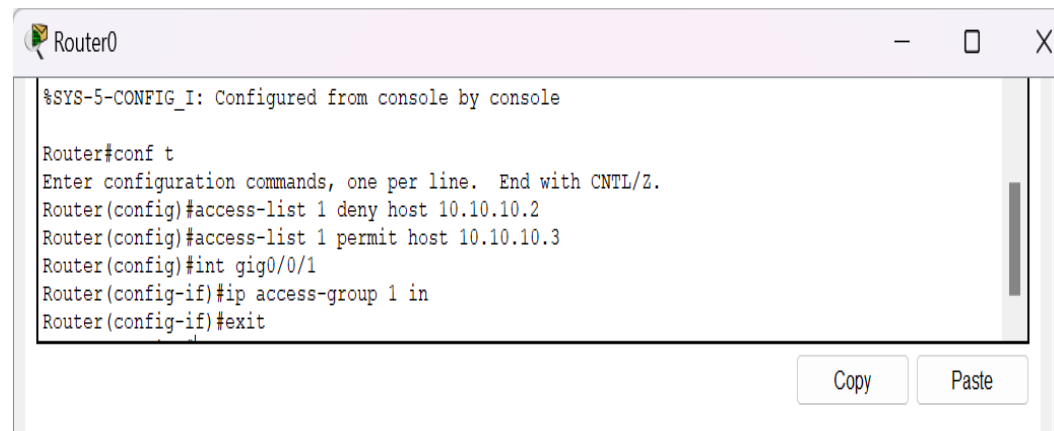
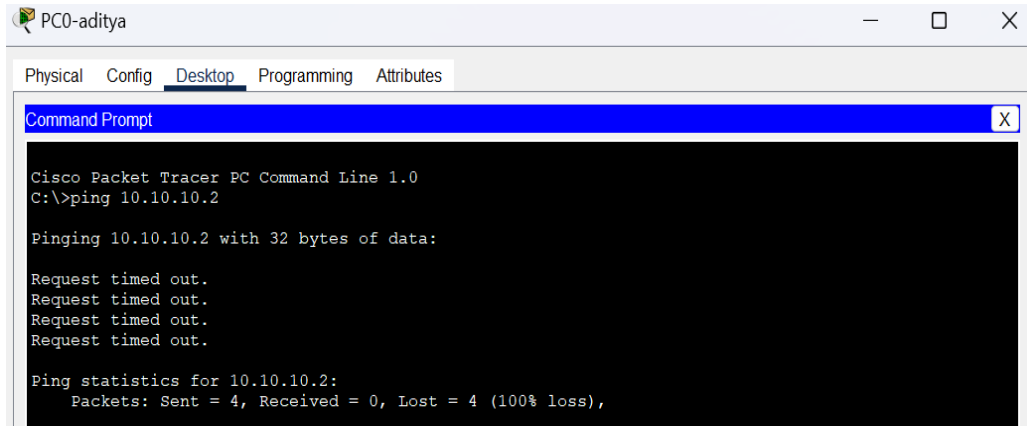


Fig: Configuration of deny and permit list

## 5. Verification and testing

Now to test if our ACL is working, we can use ping command to check the connectivity within the network and see if the ACL rules are being correctly enforced.



```
PC0-aditya
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.2

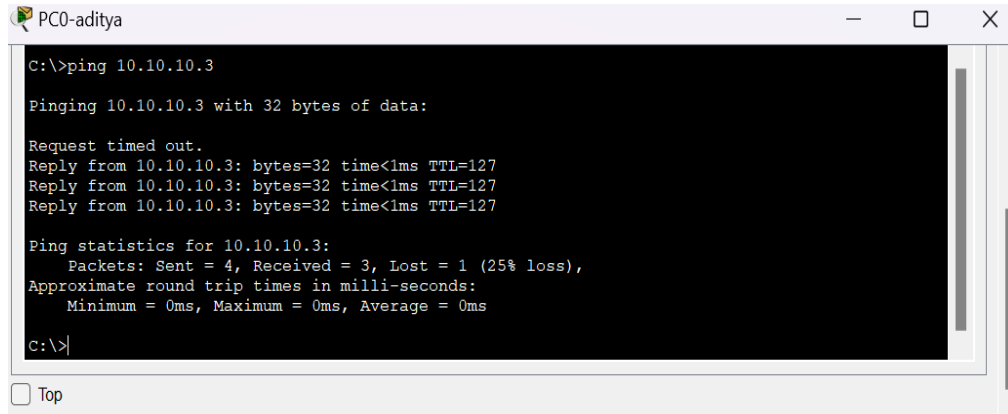
Pinging 10.10.10.2 with 32 bytes of data:

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

Ping statistics for 10.10.10.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Fig: Testing connectivity

Since we have put the Ip 10.10.10.2 in the deny list it cannot be accessed.



```
PC0-aditya
C:\>ping 10.10.10.3

Pinging 10.10.10.3 with 32 bytes of data:

Request timed out.
Reply from 10.10.10.3: bytes=32 time<1ms TTL=127
Reply from 10.10.10.3: bytes=32 time<1ms TTL=127
Reply from 10.10.10.3: bytes=32 time<1ms TTL=127

Ping statistics for 10.10.10.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Fig: Testing connectivity

But the Ip 10.10.10.3 can be accessed as it is in the permit list hence, we can say that the ACL rules are being properly enforced

## Conclusion

In this lab, we successfully implemented Access Control Lists (ACLs) using Cisco Packet Tracer. By applying both DENY and PERMIT rules, we were able to control the flow of traffic between subnets, demonstrating the utility of ACLs in securing networks by filtering and controlling traffic based on specific conditions.