**Lab 10: Implementing ACL in Packet Tracer**

**Theory**

An **Access Control List (ACL)** is a set of rules applied to router interfaces to manage the flow of traffic across a network. ACLs can be configured to permit or deny traffic based on various criteria, such as source and destination IP addresses, the protocol being used (e.g., TCP, UDP, ICMP), or specific port numbers.

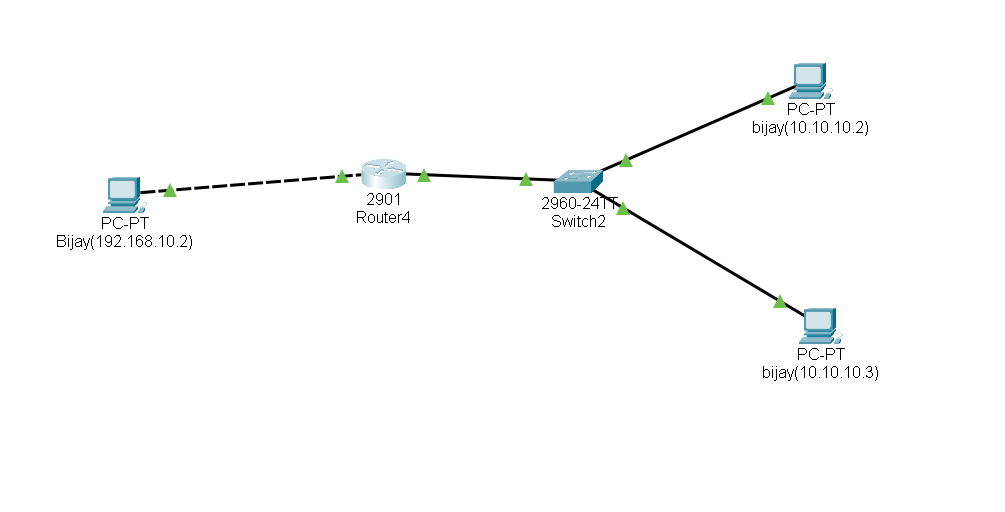
There are two main types of ACLs:

1. **Standard ACL**: Filters traffic solely based on the source IP address.
2. **Extended ACL**: Offers more control by filtering traffic based on multiple criteria, including source and destination IP addresses, protocols, and port numbers.

ACLs serve three key purposes:

* Boosting network security by restricting access to sensitive resources.
* Regulating traffic flow by allowing or blocking packets according to defined rules.
* Enhancing network performance by preventing unnecessary traffic from entering the network.

**Network Diagram**

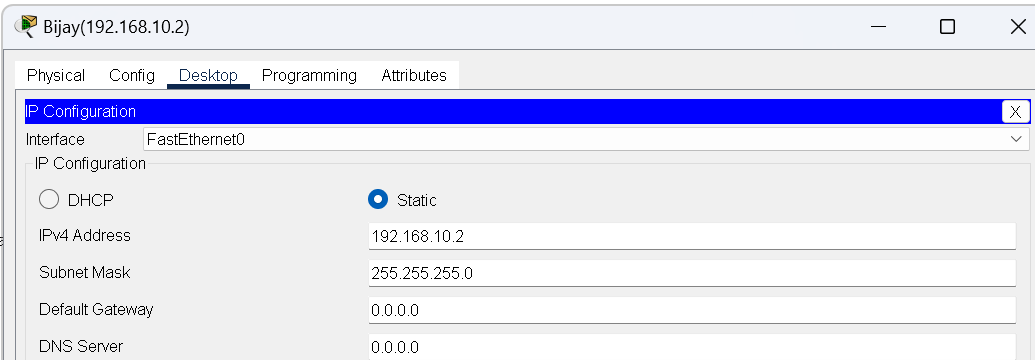


*Fig:Network Diagram*

**Configure network for PCs and Routers**

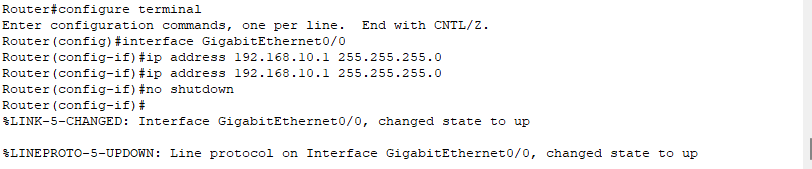
**Configure PCs**

1. Assign IP addresses to the PCs according to the network plan like PC(Bijay(192.168.10.2)), PC(Bijay1(10.10.10.2)) and PC(Bijay2(10.10.10.3)).

 *Fig:IP configuration on PC’s*

**Configure Routers**

1. Access the router's command-line interface.

2. Assign IP addresses to router interfaces that connect to the PCs.

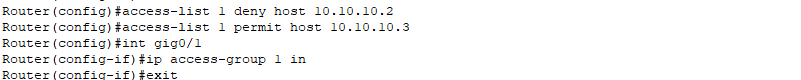
*Fig:Router configuration*

**Configuring Access List**

**Configure DENY and PERMIT list**

1.Access global configuration mode

2.Apply the ACL to an interface (e.g., blocking PC1's access to the network):

*Fig: Configuring DENY and PERMIT list*

**Code For Configuring DENY and PERMIT list**

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

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

Router(config)# interface gig0/0

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

Router(config-if)# exit

**Implementation and Testing**

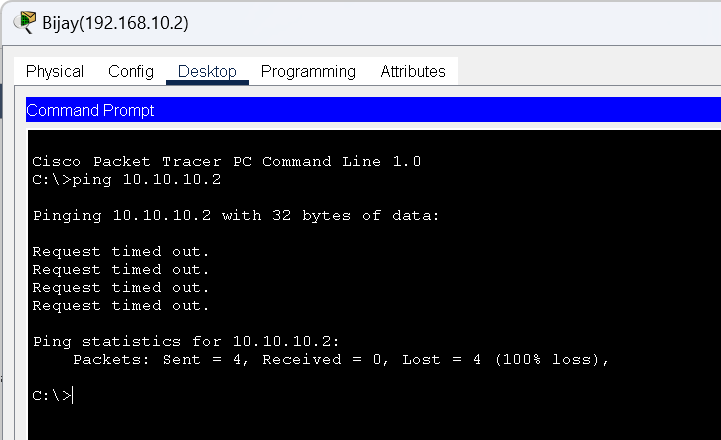
To test whether the network is working, you can ping other devices on the network from each PC.

**Steps:**

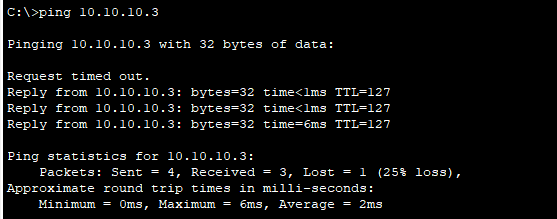
1. Ping PC(Bijay1(10.10.10.2)) from PC(Bijay(192.168.10.2)) to verify that the connection is denied.

2. Ping PC(Bijay2(10.10.10.3)) from PC(Bijay(192.168.10.2)) to verify that the connection is permitted.

3. If the ping is successful, you should see replies from the other device.



*Fig: Connectivity test from PC(Bijay(192.168.10.2)) to PC(Bijay1(10.10.10.2))*

 *Fig: Connectivity test from PC (Bijay(192.168.10.2)) to PC(Bijay2(10.10.10.3))*

**Conclusion**  
In conclusion, we successfully implemented Access Control Lists (ACLs) using Cisco Packet Tracer to manage and control network traffic. Both standard and extended ACLs were configured to permit or deny traffic based on specific IP addresses, protocols, and ports. This exercise highlighted the critical role of ACLs in strengthening network security by regulating access and blocking unauthorized traffic. Through testing, we verified the functionality and confirmed the effectiveness of the ACL configurations