Lab Number: 11 **Date: 2025/08/17**

Title: Implementing ACL in Packet Tracer

Theory:

a. **ACLs**: 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 allows 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.

b.**Network Diagram**

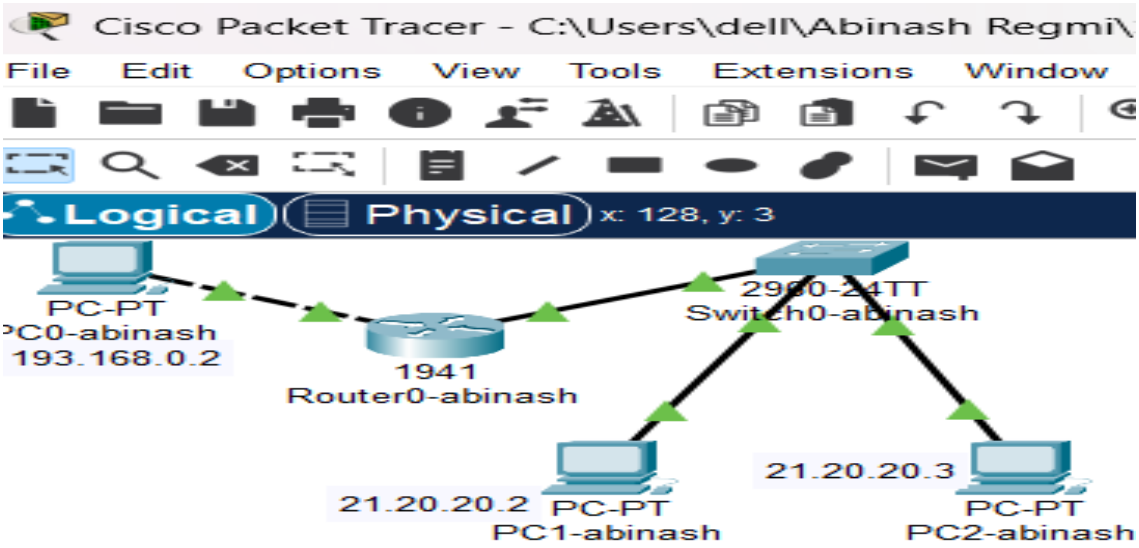


Fig: Network diagram including switch, router and pc's

Implementation Sequence

Here is the implementation sequence for Basic router configuration and static routing in Packet Tracer.

a) Configuring PCs and Routers

i.Configure PCs

Step 1: Open Packet Tracer and set up the devices.

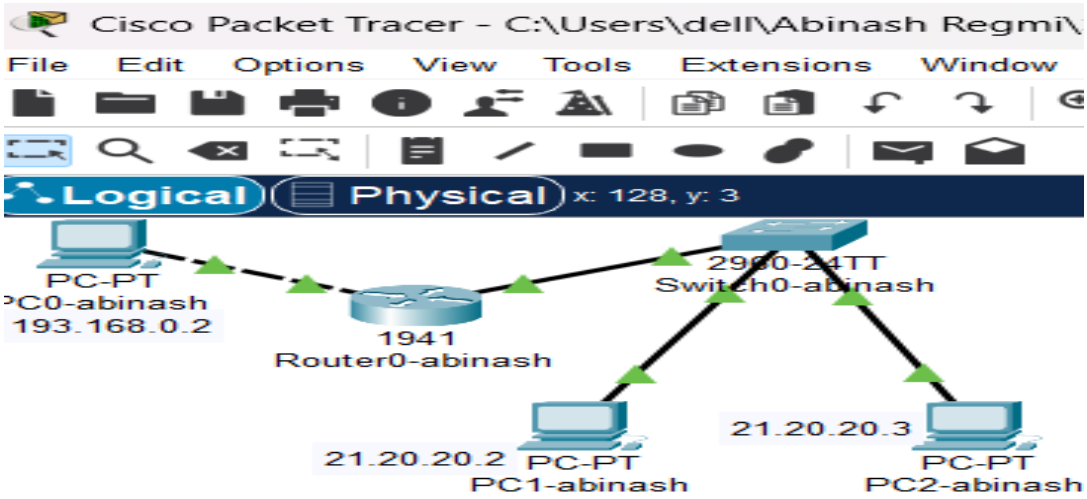
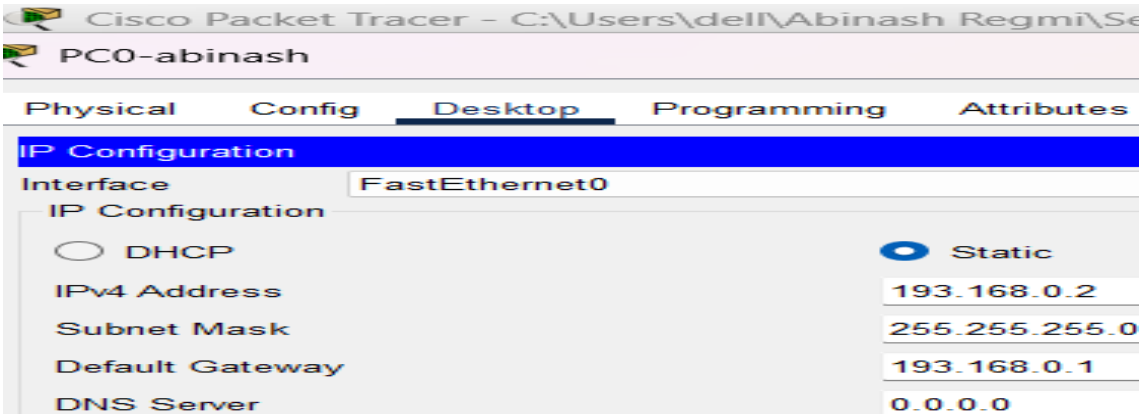
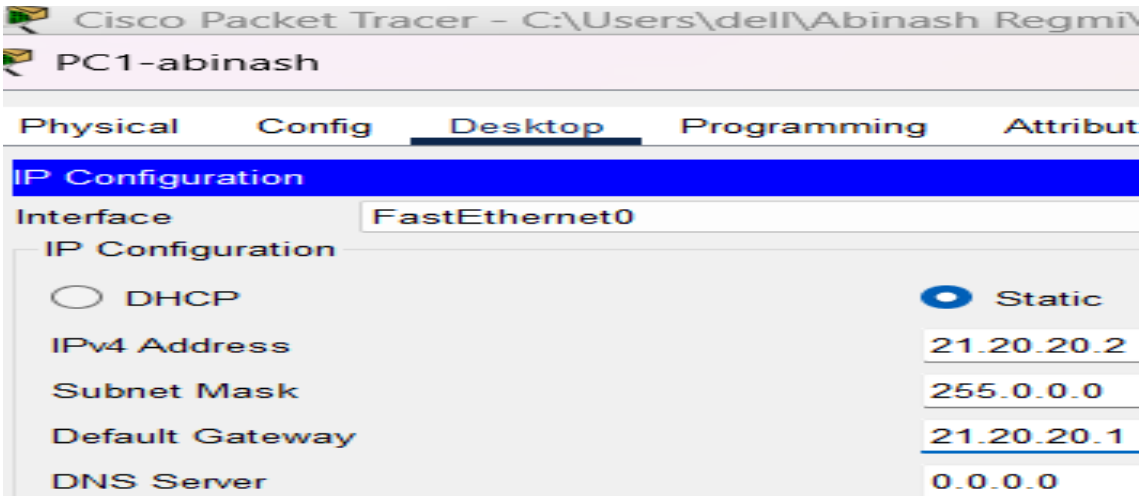


Fig: Simple Network Setup

Step 2: Assign IP addresses and subnet masks to each PC

- PC0-abinash: IP:193.168.0.2
- PC1-abinash: IP:21.20.20.2
- PC2-abinash: IP:21.20.20.3





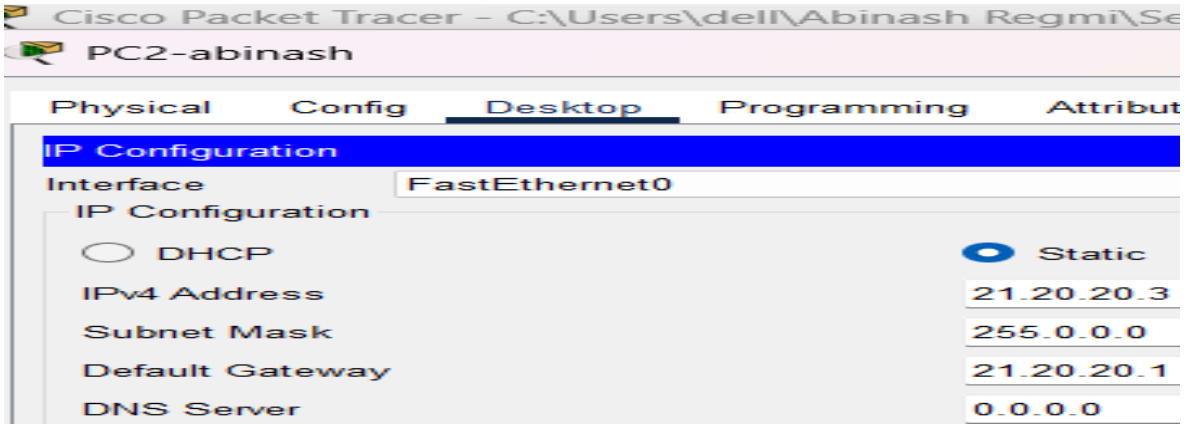


Fig: IP configuration on PCs

ii. **Configure Router**

Step 1: Configure the router with the correct IP addresses on its interfaces to connect the PC's networks.

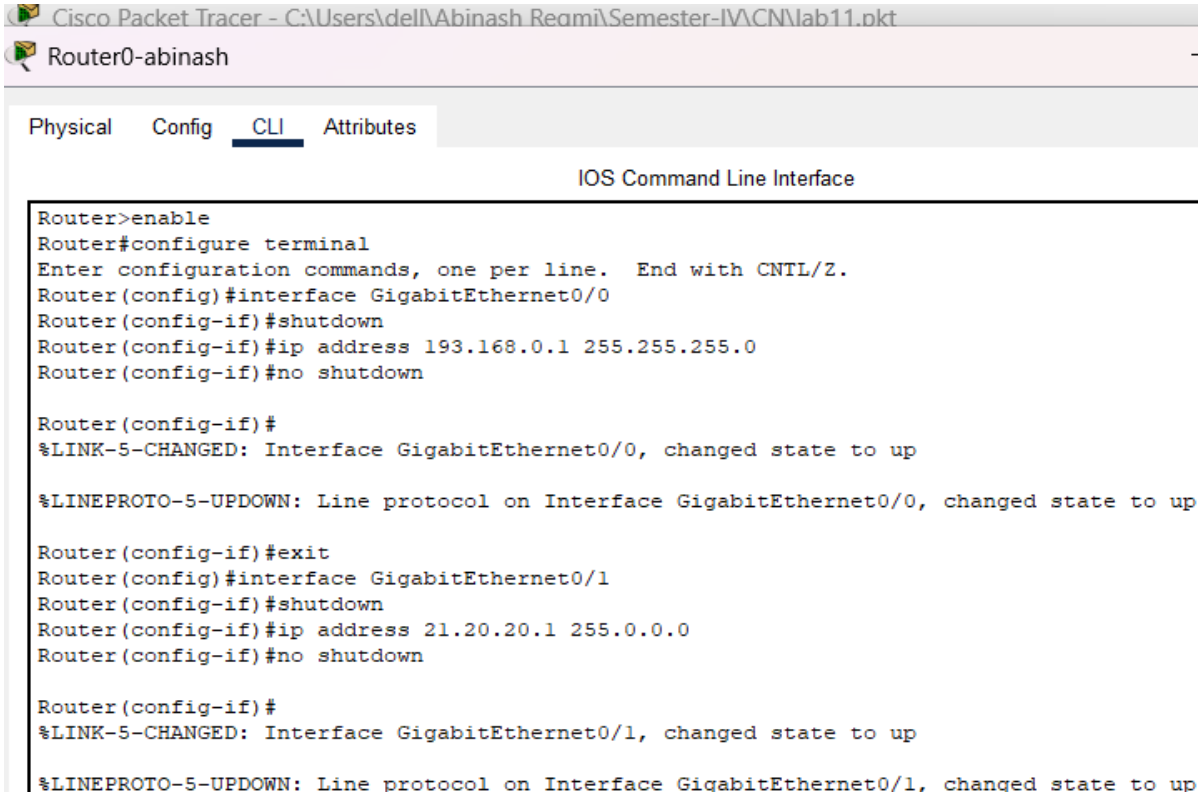


Fig: Router configuration

The figure shows the configuration of a router's interfaces to connect different PC networks. The router is assigned IP addresses to its interfaces: 193.168.0.1 for GigabitEthernet0/0 and 21.20.20.1 for GigabitEthernet0/1. After assigning Ips, the interfaces are enabled using the no shutdown command, bringing them into an operational state for network communication.

b) Configuring Access List

I. Configure the DENY and PERMIT lists

Step 1: Enter Global Configuration Mode and Apply the ACL

- Access the router's global configuration mode to configure and apply the Access Control List (ACL) to the interface connected to the PC. This will block the network access for the PC.

```
Router(config-if)#exit
Router(config)#access-list 1 deny host 21.20.20.2
Router(config)#access-list 1 permit host 21.20.20.3
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip access-group 1 in
Router(config-if)#exit
```

Fig: Configuring DENY and PERMIT list

c) **Implementation**

To verify network functionality, we should test connectivity between devices by using ping commands from each PC.

- Apply the ACLs to the relevant router interfaces.
- Use the ping command to check if the PCs can communicate with each other.
- Ensure that the ACL rules (DENY and PERMIT) are correctly enforced by observing the ping results.

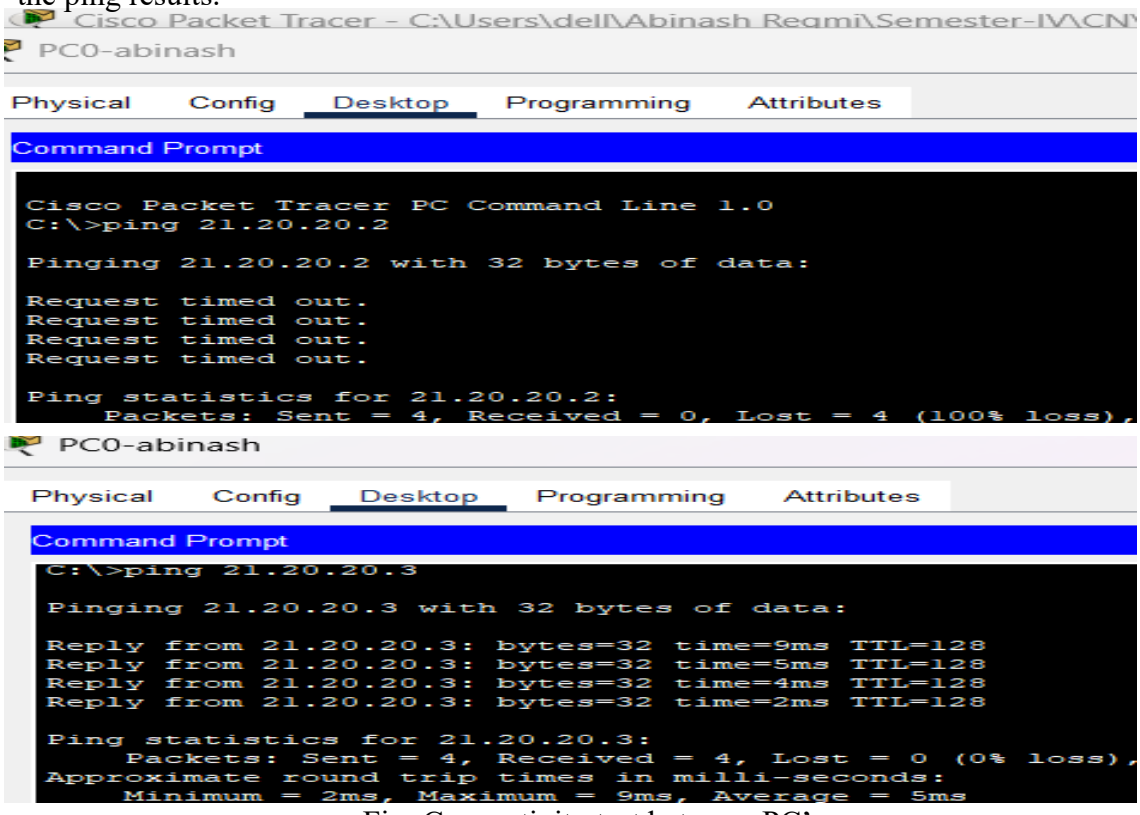


Fig: Connectivity test between PC's

Above figure shows connectivity tests between two PCs using ping commands. The first ping to IP address 21.20.20.2 fails, indicating that access is denied (possibly due to an ACL rule). The second ping to 21.20.20.3 succeeds, showing a successful communication between the devices, indicating that the connection is permitted by the ACL. The results demonstrate that the ACLs are correctly applied to control traffic.

Conclusion

In this lab, we implemented ACLs in Cisco Packet Tracer to control network traffic between PCs. By applying DENY and PERMIT rules, we successfully managed traffic flow and restricted access as required. The connectivity tests confirmed that the ACLs were effective, blocking traffic from the specified PC while allowing communication between others. This exercise demonstrated the importance of ACLs in enhancing network security and managing access control.

-Abinash Regmi