NAME: MODALLA PRANITH REDDY

ROLL NO: 2420030158

**Lab-10**

Configure the Standard and Extended Access Control List using Cisco Packet Tracer.

## Aim:

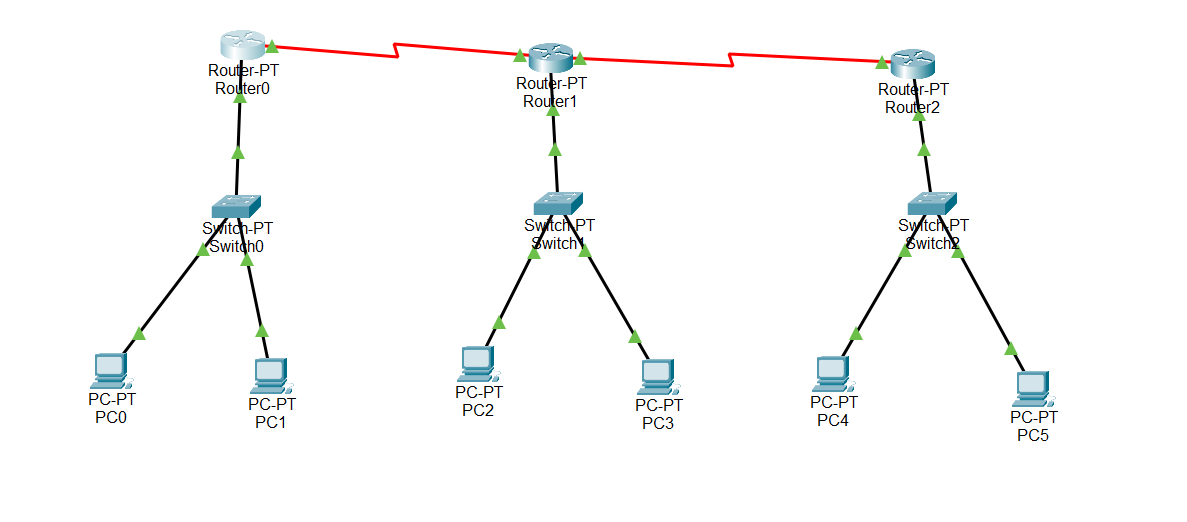
To configure and apply Standard Access Control List (ACL) and Extended Access Control List (ACL) on Router0 to control network traffic based on source IP address, destination IP address, and transport layer protocol/port.

## Apparatus / Software Required:

• Cisco Packet Tracer  
• Routers, Switches, PCs  
• Console cable for CLI configuration

## Topology:

As per the given figure, 3 routers with 6 PCs connected through switches.



## IP Addressing Table:

|  |  |  |  |
| --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask |
| PC0 | NIC | 192.168.1.1 | 255.255.255.0 |
| PC1 | NIC | 192.168.1.2 | 255.255.255.0 |
| PC2 | NIC | 192.168.2.1 | 255.255.255.0 |
| PC3 | NIC | 192.168.2.2 | 255.255.255.0 |
| PC4 | NIC | 192.168.3.1 | 255.255.255.0 |
| PC5 | NIC | 192.168.3.2 | 255.255.255.0 |
| Router0 | G0/0 | 192.168.1.254 | 255.255.255.0 |
| Router0 | G0/1 | 10.0.0.1 | 255.255.255.0 |
| Router1 | G0/0 | 10.0.0.2 | 255.255.255.0 |
| Router1 | G0/1 | 20.0.0.1 | 255.255.255.0 |
| Router2 | G0/0 | 20.0.0.2 | 255.255.255.0 |
| Router2 | G0/1 | 192.168.3.254 | 255.255.255.0 |

## Procedure:

Step 1: Configure IP addresses on PCs and Routers.  
Assign IP addresses as per the addressing table. Ensure connectivity using ping.

Step 2: Configure Standard ACL on Router0.  
Block PC1 (192.168.1.2) from accessing any network. Allow all other hosts.

Router0> enable  
Router0# configure terminal.  
Router0(config)# access-list 1 deny 192.168.1.2 0.0.0.0  
Router0(config)# access-list 1 permit any  
Router0(config)# interface gigabitEthernet0/0  
Router0(config-if)# ip access-group 1 out  
Router0(config-if)# exit

Step 3: Configure Extended ACL on Router0.  
Deny Telnet (TCP port 23) from any source to any destination. Permit all other traffic.

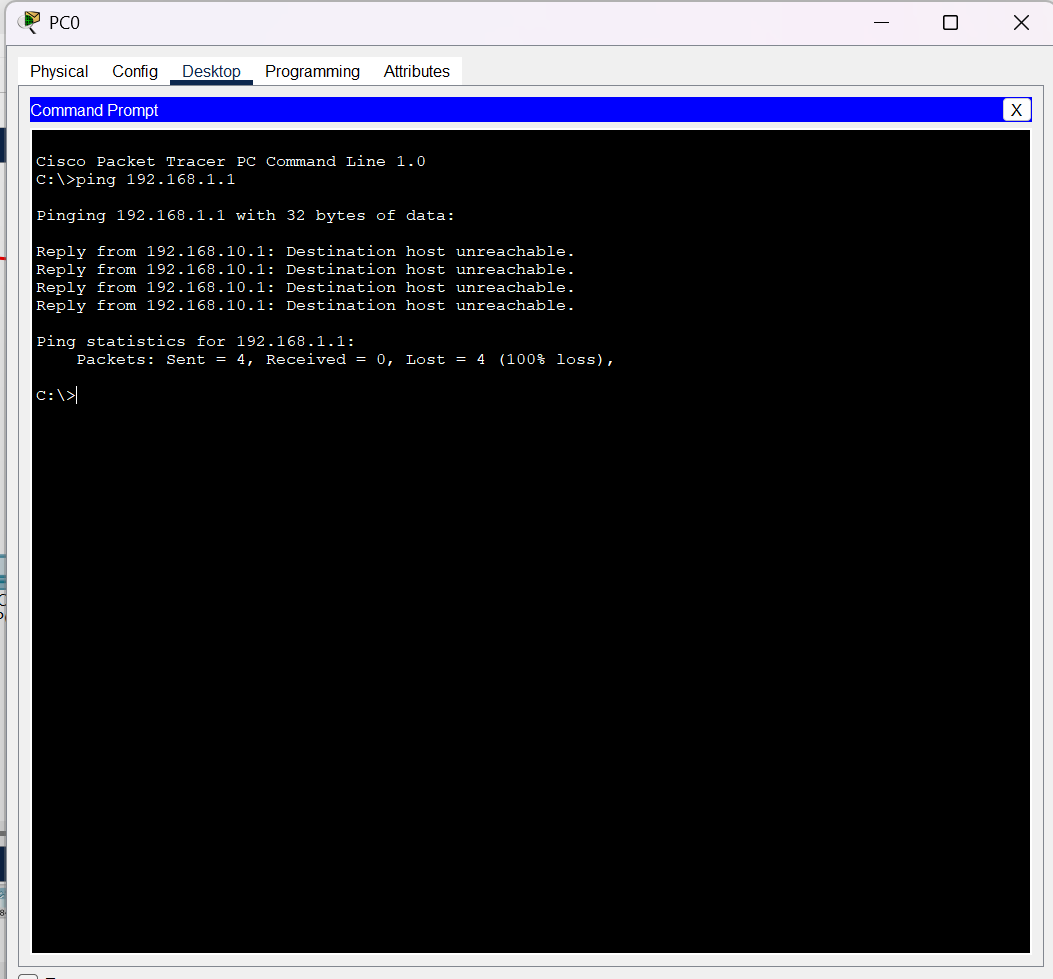
Router0# configure terminal.  
Router0(config)# access-list 101 deny tcp any any eq 23  
Router0(config)# access-list 101 permit ip any any  
Router0(config)# interface gigabitEthernet0/1  
Router0(config-if)# ip access-group 101 in  
Router0(config-if)# exit

Step 4: Verification  
Use the following commands:

Router0# show access-lists  
Router0# show ip interface gigabitEthernet0/0  
Router0# show ip interface gigabitEthernet0/1

## Output (Expected):

• PC1 cannot access outside networks.  
• Other PCs can access all networks.  
• Telnet traffic is blocked for all PCs.  
• ACL configuration is displayed correctly with show access-lists.



## Result:

The Standard ACL and Extended ACL were successfully configured on Router0. Standard ACL controls traffic based on source IP. Extended ACL-controlled traffic based on protocol and port number. Connectivity was verified using ping and telnet commands.

## Conclusion:

ACLs are useful in controlling and securing network traffic. Standard ACLs provide filtering based only on source IP, whereas Extended ACLs provide more granular control, including source, destination, protocol, and port numbers.