Practical 8: Access Control Lists (ACLs)

Practical Title: Use Standard and Extended ACLs to permit/deny traffic.

Aim: To configure and implement both Standard and Extended Access Control Lists (ACLs) to control network traffic on a Cisco router.

Objective:

- To understand the purpose of ACLs in network security.
- To configure a Standard ACL to filter traffic based on source IP address.
- To configure an Extended ACL to filter traffic based on source/destination IP, protocol, and port number.
- To apply ACLs to router interfaces and test their functionality.

Theory: An **Access Control List (ACL)** is a numbered or named list of rules that a router uses to control which packets can pass through its interfaces. **Standard ACLs** filter traffic based only on the source IP address. They are generally placed close to the destination. **Extended ACLs** provide more granular control, allowing filtering based on source/destination IP, protocol (e.g., TCP, UDP), and port number. They should be placed as close to the source as possible.

Steps:

1. **Create the Network Topology:**
    - Use a topology with two routers connecting two separate LANs (similar to Practical 2). A third PC can be added to the second LAN to demonstrate the ACL filtering.
2. **Configure a Standard ACL:**
    - **Aim:** Block PC0 (192.168.1.10) from reaching the server on the other network.
    - **On Router1 (the router connected to the destination):**

■ Enter the command: access-list 1 deny 192.168.1.10 0.0.0.0

■ Enter the command: access-list 1 permit any

■ Apply the ACL to the interface: interface fastethernet 0/0 > ip access-group 1 in

3. **Verify the Standard ACL:**
    - Ping the server from PC0 (it should fail).
    - Ping the server from PC1 (it should succeed). This demonstrates that the ACL is working correctly.
4. **Configure an Extended ACL (alternative to Standard ACL):**
    - **Aim:** Block Telnet traffic (TCP port 23) from PC0 to the server.
    - **On Router0 (the router closest to the source):**

■ Enter the command: access-list 101 deny tcp 192.168.1.10 0.0.0.0 192.168.2.10 0.0.0.0 eq 23

■ Enter the command: access-list 101 permit ip any any

■ Apply the ACL to the interface: interface fastethernet 0/0 > ip access-group 101 out

5. **Verify the Extended ACL:**
    - From PC0, try to Telnet to the server's IP address (it should fail).
    - From PC1, try to Telnet to the server's IP address (it should succeed).

Conclusion: This practical successfully demonstrated the use of both Standard and Extended ACLs. We configured ACLs to filter traffic based on source IP, protocol, and port number, showing how ACLs are a powerful tool for controlling network access and enhancing security.

Viva / Oral Questions:

1. What is the difference between a Standard and an Extended ACL?
2. Where should a Standard ACL be placed, and where should an Extended ACL be placed? Why?
3. What is the "implicit deny" rule in ACLs?
4. How do you apply an ACL to a router interface?
5. Why are ACLs considered a fundamental component of network security?

CLI COMMANDS:

Router 0

Router0> enable

Router0# configure terminal

Router0(config)# access-list 101 deny tcp 192.168.1.10 0.0.0.0 192.168.2.10 0.0.0.0 eq 23

Router0(config)# access-list 101 permit ip any any

Router0(config)# interface fastethernet 0/0

Router0(config-if)# ip access-group 101 out

Router0(config-if)# exit

Router0# end

Router0# write

Router 1

Router1> enable

Router1# configure terminal

Router1(config)# access-list 1 deny 192.168.1.10 0.0.0.0

Router1(config)# access-list 1 permit any

Router1(config)# interface fastethernet 0/0

Router1(config-if)# ip access-group 1 in

Router1(config-if)# exit

Router1# end

Router1# write

Verify Connectivity:

Cisco Packet Tracer PC Command Line 1.0

C:\>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.10.10: bytes=32 time=13ms TTL=128

Reply from 192.168.10.10: bytes=32 time=5ms TTL=128

Reply from 192.168.10.10: bytes=32 time<1ms TTL=128

Reply from 192.168.10.10: bytes=32 time=5ms TTL=128

Ping statistics for 192.168.10.10:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 13ms, Average = 5ms