Lab Number 10
Router Access List Configuration

Aim: To configure Access Control Lists (ACLs) on a router.

Theory

Access Control Lists (ACLs) are essential tools in network management and security. They allow network administrators to control traffic flow in and out of the network by creating filtering rules. ACLs can be applied to routers and other network devices to manage traffic based on a variety of parameters such as IP addresses, protocols, and port numbers.

ACLs come in two main types:

1. **Standard ACLs**: These are the simplest form of ACLs and filter traffic based only on the source IP address. They are typically numbered from 1 to 99 and can only allow or deny traffic based on the source.

Example:

access-list 10 permit 192.168.1.0 0.0.0.255

2. **Extended ACLs**: Extended ACLs are more versatile as they can filter traffic based on both source and destination IP addresses, as well as protocols and port numbers. Extended ACLs are typically numbered from 100 to 199.

   Example:

   access-list 110 permit tcp 192.168.1.0 0.0.0.255 host 10.0.0.2 eq 80

Key Concepts:

- **Access-List Number**: This identifies the type of ACL. For example, numbers 1-99 represent standard ACLs, while 100-199 represent extended ACLs.
- **Permit/Deny**: Specifies whether to allow or block traffic that meets the conditions specified in the ACL rule.
- **Wildcard Mask**: Used to specify a range of IP addresses. It operates like a subnet mask but with inverted bits.
- **Interface Direction**: ACLs can be applied to an interface in the "inbound" or "outbound" direction. "Inbound" means the ACL filters traffic as it enters the interface, while "outbound" filters it as traffic leaves the interface.

Advantages of ACLs:

- Enhance network security by restricting unauthorized access.
- Manage traffic by controlling what data flows through the network.
- Improve network performance by reducing unwanted traffic.

Limitations:

- ACLs require careful configuration and can block necessary traffic if not properly set up.
- Standard ACLs provide limited control as they only filter based on source IP addresses.

Codes

Configuring a Standard ACL:

Enter configuration mode

Router(config)# access-list 100 permit icmp any host 192.168.2.3

Router(config)# access-list 100 deny icmp any host 192.168.2.4

Router(config)# access-list 100 permit ip any any

Router(config)# interface GigabitEthernet0/0

Router(config-if)# ip access-group 100 in

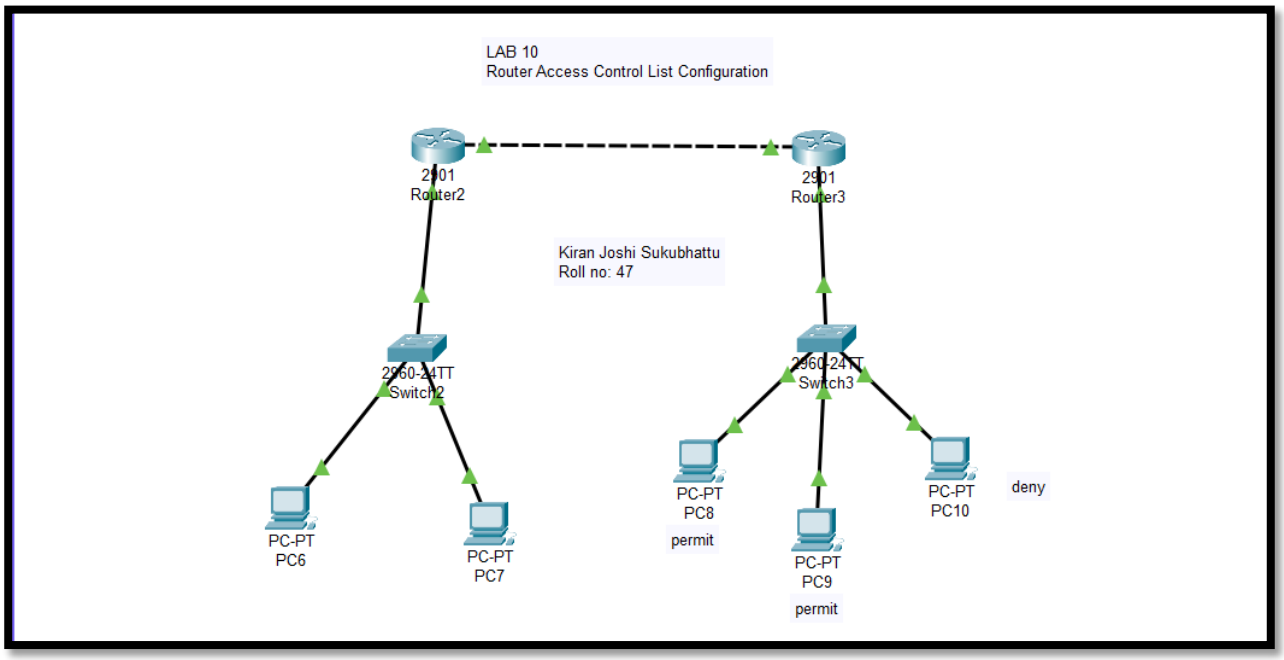
Router(config-if)# exit

Router(config)# end

Router# write memory

Explanation:

- **access-list 100 permit icmp any host 192.168.2.3**: This allows ICMP (ping) traffic from any source to the host **192.168.2.3**.
- **access-list 100 deny icmp any host 192.168.2.4**: This blocks ICMP traffic to **192.168.2.4**.
- **access-list 100 permit ip any any**: This allows all other traffic to pass through.
- **ip access-group 100 in**: This applies the ACL to inbound traffic on the specified interface.



Before Deny:

```
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.3: bytes=32 time<1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=12ms TTL=126
Reply from 192.168.2.3: bytes=32 time=13ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 8ms

C:\>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.4: bytes=32 time<1ms TTL=126
Reply from 192.168.2.4: bytes=32 time=1ms TTL=126
Reply from 192.168.2.4: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

After Deny:

```
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time<1ms TTL=126
Reply from 192.168.2.3: bytes=32 time<1ms TTL=126
Reply from 192.168.2.3: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

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

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

```
!
!
interface GigabitEthernet0/0
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip access-group 1 out
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
```

6. Conclusion

In this lab, we successfully configured both standard and extended ACLs on a router. The standard ACL was used to filter traffic based on the source IP address, while the extended ACL allowed more granular control by filtering traffic based on both IP addresses and protocols (such as blocking HTTP traffic). This experiment highlights the importance of ACLs in network security, as they provide a mechanism to control and limit access to resources based on predefined rules. The configurations worked as expected, and we were able to block unwanted traffic while allowing necessary communications. Proper ACL implementation can significantly enhance a network's security posture, especially when used in conjunction with other security mechanisms such as firewalls and intrusion detection/prevention systems.

7. Discussion

This practical demonstrates the importance of Access Control Lists (ACLs) in network security, emphasizing the careful placement of ACLs, proper rule order, and awareness of the implicit "deny all" rule. Misconfigurations can block valid traffic, so best practices like adding comments, regularly reviewing ACLs, and testing in controlled environments are crucial to prevent disruptions and ensure smooth network operation.