1. **Information Security**
2. **Chapter 4: Network Infrastructure**
4. **Lab 18 - Access Control List Demonstration**

# Objectives

Part 1: Verify Local Connectivity and Test Access Control List.

Part 2: Remove Access Control List and Repeat Test.

# Background

In this activity, you will observe how an access control list (ACL) can be used to prevent a ping from reaching hosts on remote networks. After removing the ACL from the configuration, the pings will be successful.

# Instructions

## Verify Local Connectivity and Test Access Control List

### Ping devices on the local network to verify connectivity.

* + - 1. From the command prompt of **PC1**, ping **PC2**.
      2. From the command prompt of **PC1**, ping **PC3**.

#### Question:

Why were the pings successful?

Ans: Yes

### Ping devices on remote networks to test ACL functionality.

* + - 1. From the command prompt of **PC1**, ping **PC4**.
      2. From the command prompt of **PC1**, ping the **DNS Server**.

#### Question:

Why did the pings fail? (Hint: Use simulation mode or view the router configurations to investigate.)

Ans: The pings fail because R1 is configured with an ACL that denies any ping packets from exiting the Serial 0/0/0 interface. R1 block the traffic from S1.

## Remove ACL and Repeat Test

### Use show commands to investigate the ACL configuration.

* + - 1. Navigate to R1 CLI. Use the **enable** command. Use the **show run** and **show access-lists** commands to view the currently configured ACLs. To quickly view the current ACLs, use **show access-lists**. Enter the **show access-lists** command, followed by a space and a question mark (?) to view the available options:

R1> enable

R1#

R1# **show access-lists ?**

<1-199> ACL number

WORD ACL name

<cr>

If you know the ACL number or name, you can filter the **show** output further. However, **R1** only has one ACL; therefore, the **show access-lists** command will suffice.

R1# **show access-lists**

Standard IP access list 11

10 deny 192.168.10.0 0.0.0.255

20 permit any

The first line of the ACL prevents any packets originating in the **192.168.10.0/24** network, which includes Internet Control Message Protocol (ICMP) echoes (ping requests). The second line of the ACL allows all other **ip** traffic from **any** source to transverse the router.

* + - 1. For an ACL to impact router operation, it must be applied to an interface in a specific direction. In this scenario, the ACL is used to filter traffic exiting an interface. Therefore, all traffic leaving the specified interface of R1 will be inspected against ACL 11.

Although you can view IP information with the **show ip interface** command, it may be more efficient in some situations to simply use the **show run** command. To obtain a complete list of interfaces that the ACL may be applied to, and the list of all ACL that are configured, use the following command:

R1# **show run | include interface|access**

#### Question:

To which interface and direction is the ACL applied?

Ans: interface serial0/0/0 block 11 out going packets.

### Remove access list 11 from the configuration.

You can remove ACLs from the configuration by issuing the **no access list** [*number of the ACL*] command. The **no access-list** command deletes all ACLs configured on the router. The **no access-list** [*number of the ACL*] command removes only a specific ACL.

* + - 1. Under the Serial0/0/0 interface, remove access-list 11, previously applied to the interface as an **outgoing** filter:

R1#config

R1(config)# **int se0/0/0**

R1(config-if)#**no ip access-group 11 out**

* + - 1. In global configuration mode, remove the ACL by entering the following command:

R1(config)# **no access-list 11**

* + - 1. Verify that **PC1** can now ping the **DNS Server** and **PC4**.

Ans: It worked now.