Packet Tracer - 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.

# Addressing Table

|  |  |  |
| --- | --- | --- |
| Device | Interface | IP Address / Prefix |
| R1 | G0/0 | 192.168.10.1/24 |
| R1 | G0/1 | 192.168.11.1/24 |
| R1 | S0/0/0 | 10.1.1.1/30 |
| R2 | S0/0/0 | 10.10.1.2/30 |
| R2 | S0/0/1 | 10.10.1.5/30 |
| R3 | G0/0 | 192.168.30.1/24 |
| R3 | G0/1 | 192.168.31.1/24 |
| R3 | S0/0/1 | 10.10.1.6/24 |
| PC1 | NIC | 192.168.10.10/24 |
| PC2 | NIC | 192.168.10.11/24 |
| PC3 | NIC | 192.168.11.10/24 |
| PC4 | NIC | 192.168.30.12/24 |
| DNS Server | NIC | 192.168.31.12/24 |

# 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?

Type your answers here.

### 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.)

Type your answers here.

## Remove the ACL and Repeat the Test

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

* + - 1. Navigate to R1 CLI. 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:

Open configuration window

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 blocks any packets that originate 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 that may be applied to, and the list of all ACLs that are configured, use the following command:

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

interface GigabitEthernet0/0

interface GigabitEthernet0/1

interface Serial0/0/0

 ip access-group 11 out

interface Serial0/0/1

interface Vlan1

access-list 11 deny 192.168.10.0 0.0.0.255

access-list 11 permit any

The second pipe symbol ‘|” creates an OR condition that matches ‘interface’ OR ‘access’. It is important that no spaces are included in the OR condition. Use one or both of these commands to find information about the ACL.

#### Question:

To which interface and in what direction is the ACL applied?

Type your answers here.

### 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 when used without arguments deletes all ACLs configured on the router. The **no access-list** [*number of the ACL*] command removes only a specific ACL. Removing an ACL from a router does not remove the ACL from the interface. The command that applies the ACL to the interface must be removed separately.

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

R1(config)# **interface s0/0/0**

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**.

Close configuration window

End of document