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.

Instructions

Part 1: Verify Local Connectivity and Test Access Control List

Step 1: Ping devices on the local network to verify connectivity.

a. From the command prompt of **PC1**, ping **PC2**.

b. From the command prompt of **PC1**, ping **PC3**.

Why were the pings successful?

Step 2: Ping devices on remote networks to test ACL functionality.

a. From the command prompt of **PC1**, ping **PC4**.

b. From the command prompt of **PC1**, ping the **DNS Server**.

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

Part 2: Remove ACL and Repeat Test

Step 1: Use show commands to investigate the ACL configuration.

a. 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# 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.

b. 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.

Using one or both of these commands, to which interface and direction is the ACL applied?

Step 2: 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.

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

```
R1(config)# int se0/0/0
R1(config-if)#no ip access-group 11 out
```

b. In global configuration mode, remove the ACL by entering the following command:

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

c. Verify that **PC1** can now ping the **DNS Server** and **PC4**.