Packet Tracer - Configure ACL IPv4 estándar numeradas

Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Puerta de enlace predeterminado
R1	G0/0	192.168.10.1	255.255.255.0	N/D
	G0/1	192.168.11.1	255.255.255.0	
	S0/0/0	10.1.1.1	255.255.255.252	
	S0/0/1	10.3.3.1	255.255.255.252	
R2	G0/0	192.168.20.1	255.255.255.0	N/D
	S0/0/0	10.1.1.2	255.255.255.252	
	S0/0/1	10.2.2.1	255.255.255.252	
R3	G0/0	192.168.30.1	255.255.255.0	N/D
	S0/0/0	10.3.3.2	255.255.255.252	
	S0/0/1	10.2.2.2	255.255.255.252	
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
Servidor Web	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Objetivos

Parte 1: planificar una implementación de ACL

Parte 2: configurar, aplicar y verificar una ACL estándar

Aspectos básicos/situación

Las listas de control de acceso (ACL) estándar son scripts de configuración del router que controlan si un router permite o deniega paquetes según la dirección de origen. Esta actividad se concentra en definir criterios de filtrado, configurar ACL estándar, aplicar ACL a interfaces de router y verificar y evaluar la implementación de la ACL. Los routers ya están configurados, incluidas las direcciones IP y el enrutamiento del Protocolo de Enrutamiento de la Puerta de Enlace Interior Mejorado (EIGRP).

Instrucciones

Parte 1: Planifique una implementación de ACL

Paso 1: Investigue la configuración actual de red.

Antes de aplicar cualquier ACL a una red, es importante confirmar que tenga conectividad completa. Elija una computadora y haga ping a otros dispositivos en la red para verificar que la red tenga plena conectividad. Debería poder hacer ping correctamente a todos los dispositivos.

Paso 2: Evalúe dos políticas de red y planificar las implementaciones de ACL.

a. Las siguientes políticas de red se implementan en **R2**

- La red 192.168.11.0/24 no tiene permiso para acceder al **servidor web** en la red 192.168.20.0/24.
- Se permite el resto de los tipos de acceso.

Para restringir el acceso de la red 192.168.11.0/24 al **servidor web** en 192.168.20.254 sin interferir con otro tráfico, se debe crear una ACL en el **R2**. La lista de acceso se debe colocar en la interfaz de salida hacia el **servidor web**. Se debe crear una segunda regla en el **R2** para permitir el resto del tráfico.

b. Las siguientes políticas de red se implementan en **R3**:

- La red 192.168.10.0/24 no tiene permiso para comunicarse con la red 192.168.30.0/24.
- Se permite el resto de los tipos de acceso.

Para restringir el acceso de la red 192.168.10.0/24 a la red 192.168.30/24 sin interferir con otro tráfico, se debe crear una lista de acceso en el **R3**. La ACL se debe colocar en la interfaz de salida hacia la **PC3**. Se debe crear una segunda regla en el **R3** para permitir el resto del tráfico.

Parte 2: Configure, aplique y verifique una ACL estándar

Paso 1: Configure y aplique una ACL estándar numerada en el R2.

a. Cree una ACL con el número **1** en **R2** con una instrucción que deniegue el acceso a la red 192.168.20.0/24 desde la red 192.168.11.0/24.

```
R2(config)# access-list 1 deny 192.168.11.0 0.0.0.255
```

b. De manera predeterminada, las listas de acceso deniegan todo el tráfico que no coincide con ninguna regla. Para permitir el resto del tráfico, configure la siguiente instrucción:

```
R2(config)# access-list 1 permit any
```

c. Antes de aplicar una lista de acceso a una interfaz para filtrar el tráfico, se recomienda revisar el contenido de la lista de acceso para verificar que filtrará el tráfico como se esperaba.

```
R2# show access-lists
Standard IP access list 1
        10 deny 192.168.11.0 0.0.0.255
        20 permit any
```

d. Para que la ACL realmente filtre el tráfico, se debe aplicar a alguna operación del router. Aplique la ACL colocándola para el tráfico saliente en la interfaz GigabitEthernet 0/0. Nota: En una red operativa real, no es una buena práctica aplicar una lista de acceso no probada a una interfaz activa.

```
R2(config)# interface GigabitEthernet0/0
R2(config-if)# ip access-group 1 out
```

Paso 2: Configure y aplique una ACL estándar numerada en el R3.

a. Cree una ACL con el número **1** en **R3** con una instrucción que deniegue el acceso a la red 192.168.30.0/24 desde la red de la **PC1** (192.168.10.0/24).

```
R3(config)# access-list 1 deny 192.168.10.0 0.0.0.255
```

b. De manera predeterminada, las ACL deniegan todo el tráfico que no coincide con ninguna regla. Para permitir el resto del tráfico, cree una segunda regla para la ACL 1.

```
R3(config)# access-list 1 permit any
```

c. Compruebe que la lista de acceso está configurada correctamente.

```
R3# show access-lists
Standard IP access list 1
        10 deny 192.168.10.0 0.0.0.255
        20 permit any
```

d. Aplique la ACL colocándola para el tráfico saliente en la interfaz GigabitEthernet 0/0.

```
R3(config)# interface GigabitEthernet0/0
R3(config-if)# ip access-group 1 out
```

Paso 3: Verifique la configuración y la funcionalidad de la ACL.

a. Introduzca el comando **show run** o **show ip interface gigabitethernet 0/0** para verificar la colocación de las ACL.

b. Una vez colocadas las dos ACL, el tráfico de la red se restringe según las políticas detalladas en la Parte 1. Utilice las siguientes pruebas para verificar las implementaciones de ACL:

- Un ping de 192.168.10.10 a 192.168.11.10 se realiza correctamente.
- Un ping de 192.168.10.10 a 192.168.20.254 se realiza correctamente.
- Un ping de 192.168.11.10 a 192.168.20.254 falla.
- Un ping de 192.168.10.10 a 192.168.30.10 falla.
- Un ping de 192.168.11.10 a 192.168.30.10 se realiza correctamente.
- Un ping de 192.168.30.10 a 192.168.20.254 se realiza correctamente.

c. Ejecute de nuevo el comando **show access-lists** en los routers **R2** y **R3**. Debería ver un resultado que indica el número de paquetes que han coincidido con cada línea de la lista de acceso. Nota: El número de coincidencias mostradas para sus routers puede ser diferente, debido al número de pings que se envían y reciben.

```
R2# show access-lists
Standard IP access list 1
        10 deny 192.168.11.0 0.0.0.255 (4 match(es))
        20 permit any (8 match(es))

R3# show access-lists
Standard IP access list 1
        10 deny 192.168.10.0 0.0.0.255 (4 match(es))
        20 permit any (8 match(es))
```