

## Packet Tracer: Configuración de ACL estándar para IPv4 con nombre

**CHRISTIAN EMMANUEL VITAL TORRES**

### Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Puerta de enlace predeterminada
R1	F0/0	192.168.10.1	255.255.255.0	N/D
	F0/1	192.168.20.1	255.255.255.0	
	E0/0/0	192.168.100.1	255.255.255.0	
	E0/1/0	192.168.200.1	255.255.255.0	
Servidor de archivos	NIC	192.168.200.100	255.255.255.0	192.168.200.1
Servidor web	NIC	192.168.100.100	255.255.255.0	192.168.100.1
PC0	NIC	192.168.20.3	255.255.255.0	192.168.20.1
PC1	NIC	192.168.20.4	255.255.255.0	192.168.20.1
PC2	NIC	192.168.10.3	255.255.255.0	192.168.10.1

## Objetivos

**Parte 1: Configurar y aplicar una ACL estándar con nombre**

**Parte 2: Verificar la implementación de la ACL**

## Aspectos básicos/situación

El administrador de red ejecutivo le ha solicitado que cree una ACL con nombre estándar para impedir el acceso a un servidor de archivos. El servidor de archivos contiene la base de datos para las aplicaciones web. Sólo la estación de trabajo de Web Manager PC1 y el servidor Web necesitan tener acceso al servidor de archivos. Debe denegarse el resto del tráfico al servidor de archivos.

## Instrucciones

### Parte 1: Configurar y aplicar una ACL estándar con nombre

#### Paso 1: Verificar la conectividad antes de configurar y aplicar la ACL

Las tres estaciones de trabajo deberían poder hacer ping tanto al **servidor web** como al **servidor de archivos**.

#### Paso 2: Configurar una ACL estándar con nombre

- Configure la siguiente ACL con nombre en el R1.

```
R1(config)# ip access-list standard File_Server_Restrictions
```

```
R1(config-std-nacl)# permit host 192.168.20.4
R1 (config-std-nacl) # permit host 192.168.100.100
R1(config-std-nacl)# deny any
```

**Nota:** A efectos de puntuación, el nombre de la ACL distingue entre mayúsculas y minúsculas y las instrucciones deben estar en el mismo orden que se muestra.

- b. Utilice el comando **show access-lists** para verificar el contenido de la lista de acceso antes de aplicarla a una interfaz. Asegúrese de que no ha escrito mal ninguna dirección IP y de que las instrucciones están en el orden correcto.

```
R1# show access-lists
Standard IP access list File_Server_Restrictions
10 permit host 192.168.20.4
20 permit host 192.168.100.100
30 deny any
```

### Paso 3: Aplicar la ACL con nombre

- a. Aplique la salida de ACL en la interfaz Fast Ethernet 0/1.

**Nota:** En una red operativa real, aplicar una lista de acceso a una interfaz activa no es una buena práctica y debe evitarse si es posible.

```
R1(config-if)# ip access-group File_Server_Restrictions out
```

- b. Guarde la configuración.

## Parte 2: Verificar la implementación de la ACL

### Paso 1: Verificar la configuración de la ACL y su aplicación a la interfaz

Utilice el comando **show access-lists** para verificar la configuración de la ACL. Utilice el comando **show run** o **show ip interface fastethernet 0/1** para verificar que la ACL se haya aplicado de forma correcta a la interfaz.

### Paso 2: Verificar que la ACL funcione correctamente

Las tres estaciones de trabajo deberían poder hacer ping al **servidor web**, pero solo la **PC1** y el **servidor web** deberían poder hacer ping al **servidor de archivos**. Repita el comando **show access-lists** para ver el número de paquetes que coinciden con cada sentencia.

## RESPUESTAS

**En el ROUTER 1 poner los siguientes comandos:**

**enable**

**configure terminal**

**ip access-list standard File\_Server\_Restrictions**

**permit host 192.168.20.4**

**permit host 192.168.100.100**

**deny any**

**interface f0/1**

**ip access-group File\_Server\_Restrictions out**