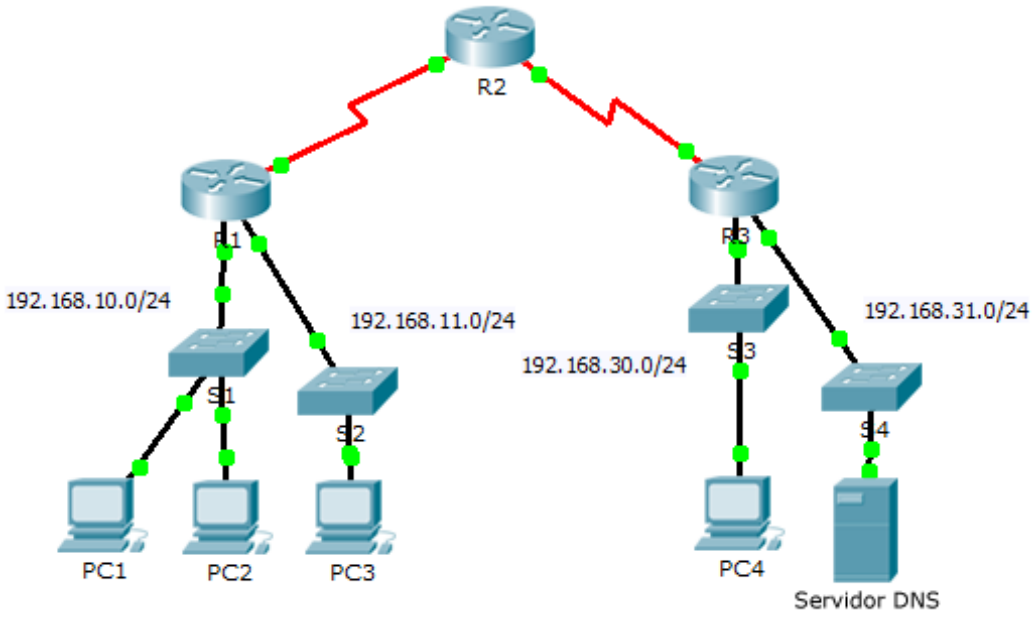
# Packet Tracer: Demostración de listas de control de acceso

## Topología




## Objetivos

**Parte 1: Verificar la conectividad local y probar la lista de control de acceso**

**Parte 2: Eliminar la lista de control de acceso y repetir la prueba**

## Aspectos básicos

En esta actividad, observará cómo se puede utilizar una lista de control de acceso (ACL) para evitar que un ping llegue a hosts en redes remotas. Después de eliminar la ACL de la configuración, los pings se realizarán correctamente.

# Parte 1. Verificar la conectividad local y probar la lista de control de acceso

### Paso 1. Hacer ping a los dispositivos de la red local para verificar la conectividad

a. Desde el símbolo del sistema de la **PC1**, haga ping a la **PC2**.

b. Desde el símbolo del sistema de la **PC1**, haga ping a la **PC3**.

¿Por qué se realizaron de forma correcta los pings?

_____

### Paso 2. Hacer ping a los dispositivos en las redes remotas para probar la funcionalidad de la ACL

a. Desde el símbolo del sistema de la **PC1**, haga ping a la **PC4**.

b. Desde el símbolo del sistema de la **PC1**, haga ping al **servidor DNS**.

¿Por qué fallaron los pings? (Sugerencia: utilice el modo de simulación o vea las configuraciones del router para investigar).

_____

# Parte 2. Eliminar la ACL y repetir la prueba

## Paso 1. Utilizar el comando show para investigar la configuración de la ACL

a. Utilice los comandos **show run** y **show access-lists** para ver las ACL configuradas actualmente. Para obtener una vista rápida de las ACL vigentes, utilice **show access-lists**. Introduzca el comando **show access-lists** seguido de un espacio y un signo de interrogación (?) para ver las opciones disponibles:

```
R1#show access-lists ?
  <1-199>  ACL number
  WORD     ACL name
  <cr>
```

Si conoce el número o el nombre de la ACL, puede filtrar aún más el resultado del comando **show**. Sin embargo, el **R1** tiene solo una ACL, por lo que basta con el comando **show access-lists**.

```
R1#show access-lists
Standard IP access list 11
    10 deny 192.168.10.0 0.0.0.255
    20 permit any
```

La primera línea de la ACL impide cualquier paquete que se origine en la red **192.168.10.0/24**, lo que incluye los ecos del protocolo de mensajería de control de Internet (ICMP) (solicitudes de ping). La segunda línea de la ACL permite que todo el resto del tráfico **ip** de **cualquier** origen atraviese el router.

b. Para que una ACL tenga efecto en el funcionamiento del router, debe aplicarse a una interfaz en una dirección específica. En esta situación, la ACL se utiliza para filtrar el tráfico que sale de una interfaz. Por lo tanto, todo el tráfico que sale de la interfaz especificada de R1 se examinará contra la ACL 11.

Aunque pueda ver la información de IP con el comando **show ip interface**, en algunos casos puede ser más eficaz utilizar solo el comando **show run**.

Usando uno o los dos comandos, ¿a qué interfaz y dirección se aplica la ACL?

_____

## Paso 2. Eliminar la lista de acceso 11 de la configuración

Es posible eliminar las ACL de la configuración por medio de la emisión del comando **no access list** *[número de ACL]*. El comando **no access-list** elimina todas las ACL configuradas en el router. El comando **no access-list** [*número de ACL*] solo elimina una ACL específica.

a. En la interfaz Serial0/0/0, elimine la lista de acceso 11 aplicada antes a la interfaz como filtro de **salida**:

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

b. En el modo de configuración global, elimine la ACL por medio del siguiente comando:

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

c. Verifique que la **PC1** ahora pueda hacer ping al **servidor DNS** y a **PC4**.

## Tabla de calificación sugerida

| Ubicación de la consulta | Puntos posibles | Puntos obtenidos |
|---|---|---|
| Parte 1, paso 1 b. | 50 | |
| Parte 1, paso 2 b. | 40 | |
| Parte 2, paso 2 b. | 10 | |
| **Puntuación total** | **100** | |