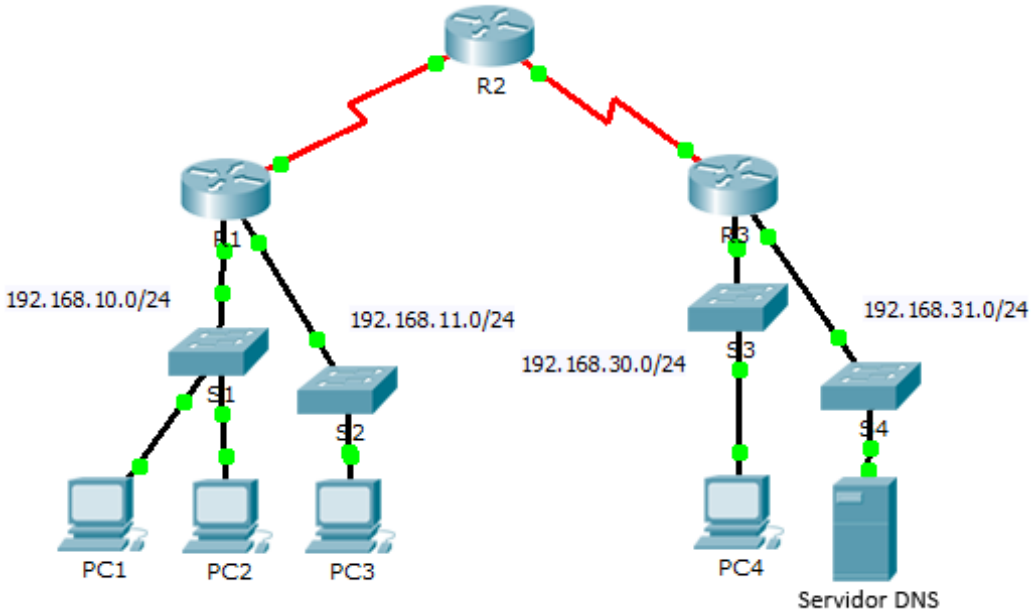
Packet Tracer: demostración de listas de control de acceso

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

Información básica

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
Extended IP access list 101
    deny icmp any any echo
    permit ip any any
```

La primera línea de la ACL impide los ecos del protocolo de mensajes de control de Internet (ICMP) (es decir, las solicitudes de ping) desde **cualquier (any)** origen hasta **cualquier (any)** destino. La segunda línea de la ACL permite el resto del tráfico **ip** desde **cualquier (any)** origen hasta **cualquier (any)** destino.

b. Para que una ACL afecte el funcionamiento del router, debe aplicarse en algún lugar. En esta situación, la ACL se utiliza para filtrar el tráfico en una interfaz. 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**. Al usar uno o ambos comandos, ¿a qué interfaz se aplica la ACL? _____

Paso 2: eliminar la lista de acceso 101 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 el modo de configuración global, elimine la ACL por medio del siguiente comando:

```
R1(config)# no access-list 101
```

b. Verifique que la **PC1** ahora pueda hacer ping al **servidor DNS**.

Tabla de calificación sugerida

Ubicación de la pregunta	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**	