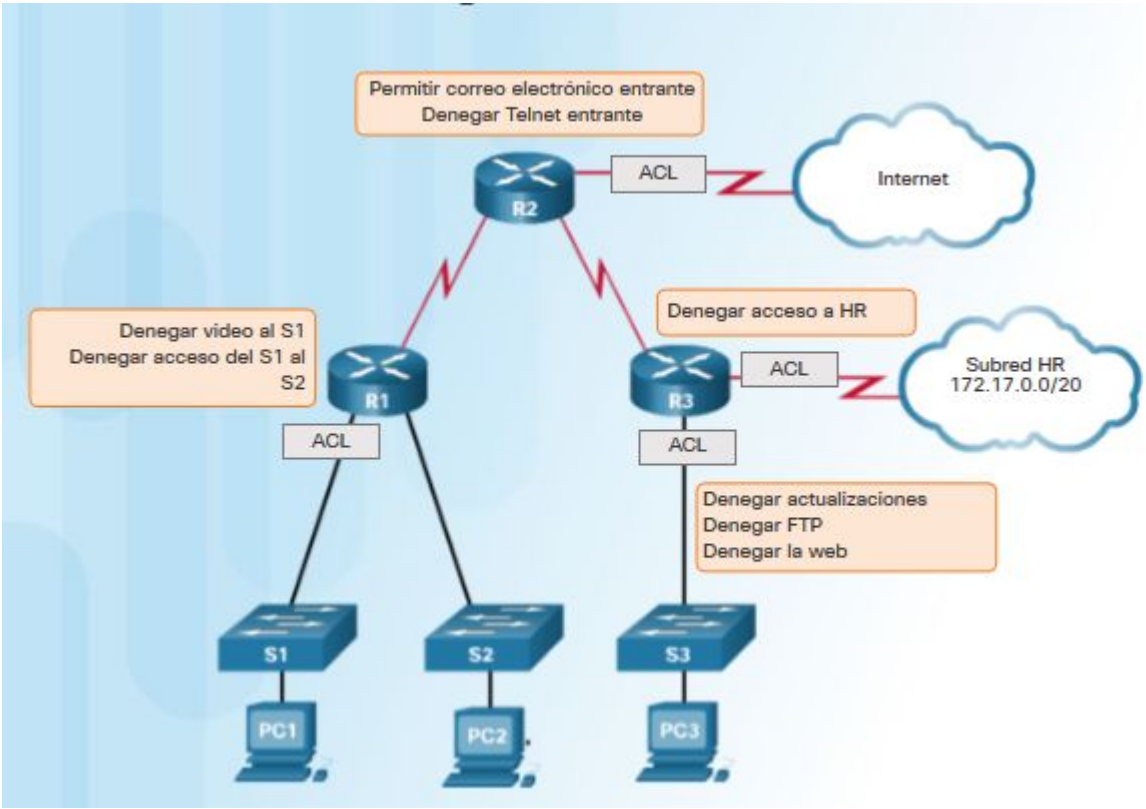
Listas de control de Acceso

Clase “07”

En este capítulo, se explica cómo configurar y solucionar problemas en las ACL estándar IPv4 en un router Cisco como parte de una solución de seguridad. Se incluyen consejos, consideraciones, recomendaciones y pautas generales sobre cómo utilizar las ACL. Además, en este capítulo se ofrece la oportunidad de desarrollar su dominio de las ACL con una serie de lecciones, actividades y ejercicios de práctica de laboratorio.

¿Qué es una ACL?



Una ACL es una serie de comandos del IOS que controlan si un router reenvía o descarta paquetes según la información que se encuentra en el encabezado del paquete.

Filtrado de paquetes

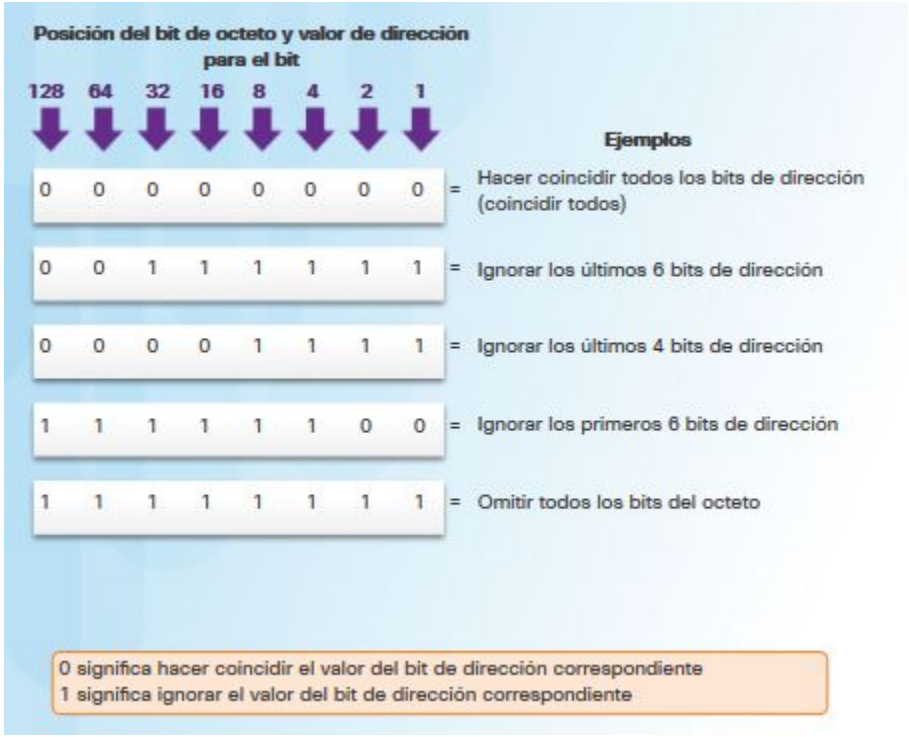
La última instrucción de una ACL es siempre una denegación implícita. Esta sentencia se inserta automáticamente al final de cada ACL, aunque no esté presente físicamente. La denegación implícita bloquea todo el tráfico.

Funcionamiento de una ACL

La última instrucción de una ACL es siempre una denegación implícita. Esta sentencia se inserta automáticamente al final de cada ACL, aunque no esté presente físicamente. La denegación implícita bloquea todo el tráfico.

Introducción a las máscaras Wildcard

Máscara wildcard



	Dirección decimal	Dirección binaria
Dirección IP para procesar	192.168.10.0	11000000.10101000.00001010.00000000
Máscara wildcard	0.0.255.255	00000000.00000000.11111111.11111111
Dirección IP resultante	192.168.0.0	11000000.10101000.00000000.00000000

Ejemplos de máscara wildcard

Ejemplo 1

	Decimal	Binario
Dirección IP	192.168.1.1	11000000.10101000.00000001.00000001
Máscara wildcard	0.0.0.0	00000000.00000000.00000000.00000000
Resultado	192.168.1.1	11000000.10101000.00000001.00000001

Ejemplo 2

	Decimal	Binario
Dirección IP	192.168.1.1	11000000.10101000.00000001.00000001
Máscara wildcard	255.255.255.255	11111111.11111111.11111111.11111111
Resultado	0.0.0.0	00000000.00000000.00000000.00000000

Ejemplo 3

	Decimal	Binario
Dirección IP	192.168.1.1	11000000.10101000.00000001.00000001
Máscara wildcard	0.0.0.255	00000000.00000000.00000000.11111111
Resultado	192.168.1.0	11000000.10101000.00000001.00000000

Cálculo de la máscara wildcard

Ejemplo 1	255.255.255.255 - 255.255.255.000 255
Ejemplo 2	255.255.255.255 - 255.255.255.240 15
Ejemplo 3	255.255.255.255 - 255.255.254.000 1.255

Palabras clave de las máscaras wildcard

Ejemplo 1

- 192.168.10.10 0.0.0.0 coincide con todos los bits de la dirección.
- Abrevie esta máscara de comodin con la dirección IP precedida por la palabra clave `host` (`host 192.168.10.10`)

Ejemplo 2

- 0.0.0.0 255.255.255.255 omite todos los bits de la dirección.
- Abrevie la expresión con la palabra clave `any`

Pautas generales para la creación de ACL

Con dos interfaces y dos protocolos en ejecución, este router podría tener un total de ocho ACL distintas aplicadas.

Reglas para aplicar las ACL

Solo se puede tener una ACL por protocolo, por interfaz y por sentido:

- Una ACL por protocolo (p. ej., IPv4 o IPv6)
- Una ACL por sentido (es decir, de entrada o de salida)
- Una ACL por interfaz (p. ej., GigabitEthernet0/0)

las ACL no deben configurarse en ambos sentidos. La cantidad de ACL y el sentido aplicado a la interfaz dependen de los requisitos que se implementen.

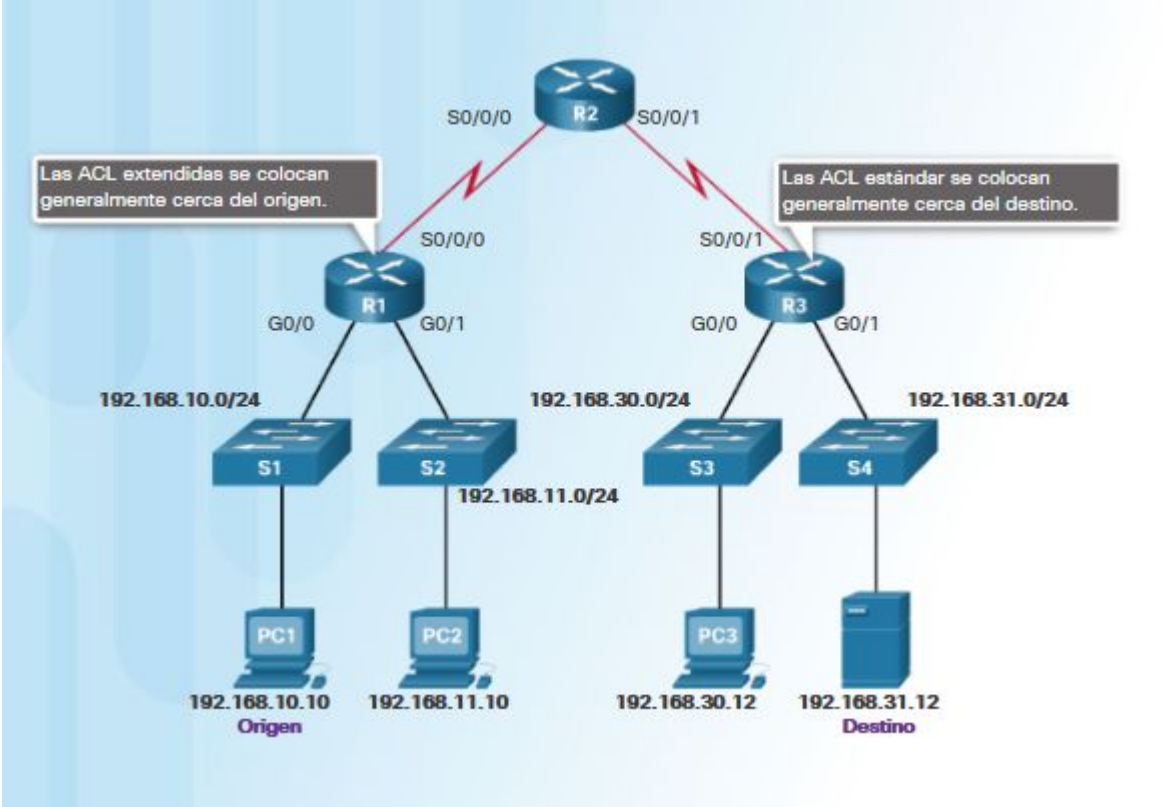
Optimizaciones de las ACL

Pautas	Ventaja
Fundamente sus ACL según las políticas de seguridad de la organización.	Esto asegurará la implementación de las pautas de seguridad de la organización.
Prepare una descripción de lo que desea que realicen las ACL.	Esto lo ayudará a evitar posibles problemas de acceso generados de manera inadvertida.
Utilice un editor de texto para crear, editar y guardar las ACL.	Esto lo ayudará a crear una biblioteca de ACL reutilizables.
Pruebe sus ACL en una red de desarrollo antes de implementarlas en una red de producción.	Esto lo ayudará a evitar errores costosos.

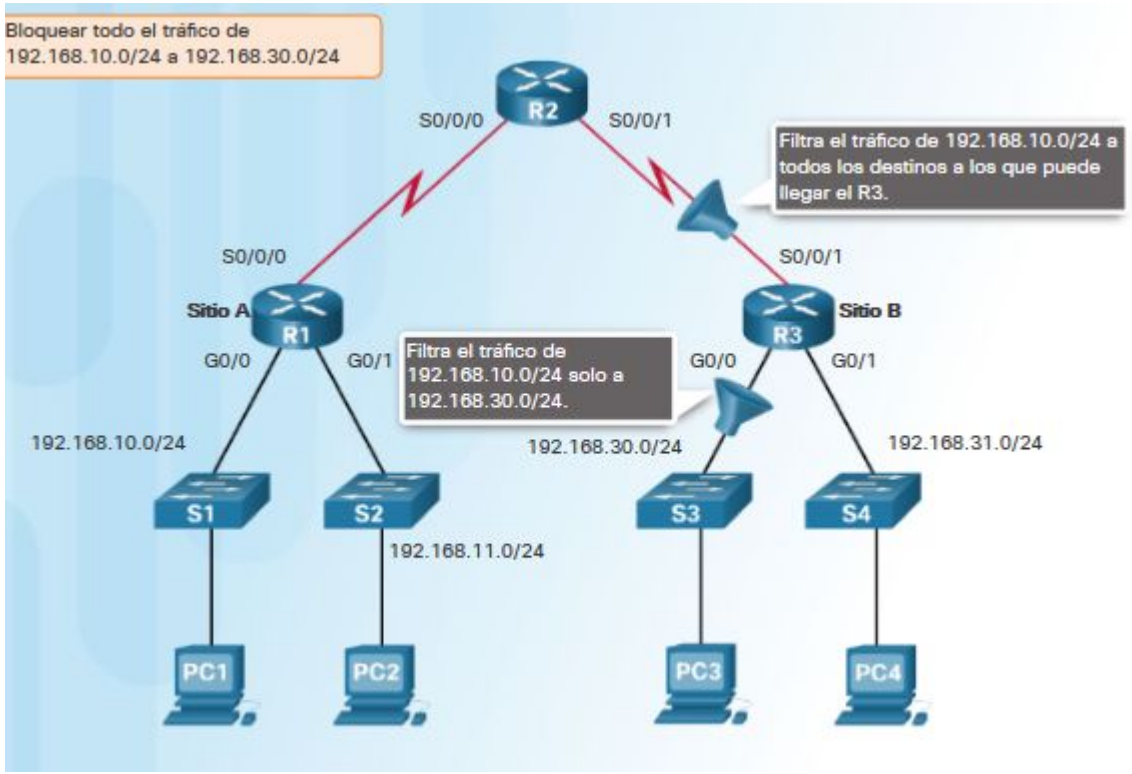
Dónde ubicar las ACL

ACL extendidas: coloque las ACL extendidas lo más cerca posible del origen del tráfico que se filtrará.

ACL estándar: debido a que en las ACL estándar no se especifican las direcciones de destino, colóquelas tan cerca del destino como sea posible



Ubicación de la ACL estándar



Sintaxis de ACL estándar numerada IPv4

Parámetro	Descripción
número-acl	Número de una ACL. Es un número decimal del 1 al 99 o del 1300 al 1999 (para las ACL estándar).
deny	Deniega el acceso si las condiciones concuerdan.
permit	Permite el acceso si las condiciones concuerdan.
remark	Agregue un comentario sobre las entradas en la lista de acceso IP para facilitar la comprensión y el análisis de la lista.
source	Número de la red o del host desde el que se envía el paquete. Existen dos formas de especificar el *origen*: • Utilice una cantidad de 32 bits en formato decimal punteado de cuatro partes. • Use la palabra clave **any** como abreviatura para *origen* y *wildcard-origen* de 0.0.0.0 255.255.255.255.
wildcard-origen	(Optativo) Máscara wildcard de 32 bits para aplicar al origen. Coloca unos en las posiciones de bits que desea omitir.
log	(Opcional) Genera un mensaje de registro informativo en la consola acerca del paquete que coincide con la entrada. (El nivel de mensajes registrados en la consola se controla mediante el comando **logging console**). El mensaje incluye el número de ACL, si el paquete fue permitido o

Aplicación de ACL estándar IPv4 a las interfaces

Paso 1: utilice el comando de configuración global `access-list` para crear una entrada en una ACL de IPv4 estándar.

```
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
```

La sentencia del ejemplo coincide con cualquier dirección que comience con 192.168.10.x. Utilice la opción `remark` (comentario) para agregar una descripción a la ACL.

Paso 2: utilice el comando de configuración `interface` para seleccionar una interfaz a la cual aplicarle la ACL.

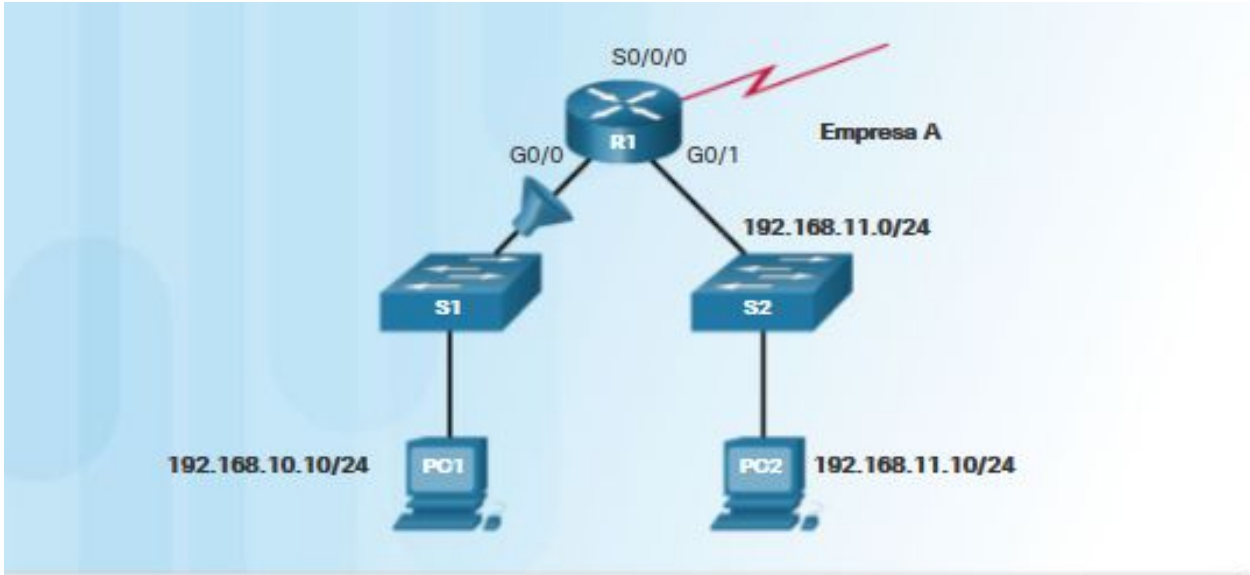
```
R1(config)# interface serial 0/0/0
```

Paso 3: utilice el comando de configuración de interfaz `ip access-group` para activar la ACL actual en una interfaz.

```
R1(config-if)# ip access-group 1 out
```

Este ejemplo activa la ACL estándar IPv4 1 en la interfaz como filtro de salida.

Sintaxis de ACL con nombre estándar IPv4




```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# deny host 192.168.11.10
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group NO_ACCESS out
```

Verificar las ACL

```
R1# show ip interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.1/30
<se omitió el resultado>
  Outgoing access list is 1
  Inbound access list is not set
<se omitió el resultado>

R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
<se omitió el resultado>
  Outgoing access list is NO_ACCESS
  Inbound access list is not set
<se omitió el resultado>
```

Estadísticas de ACL

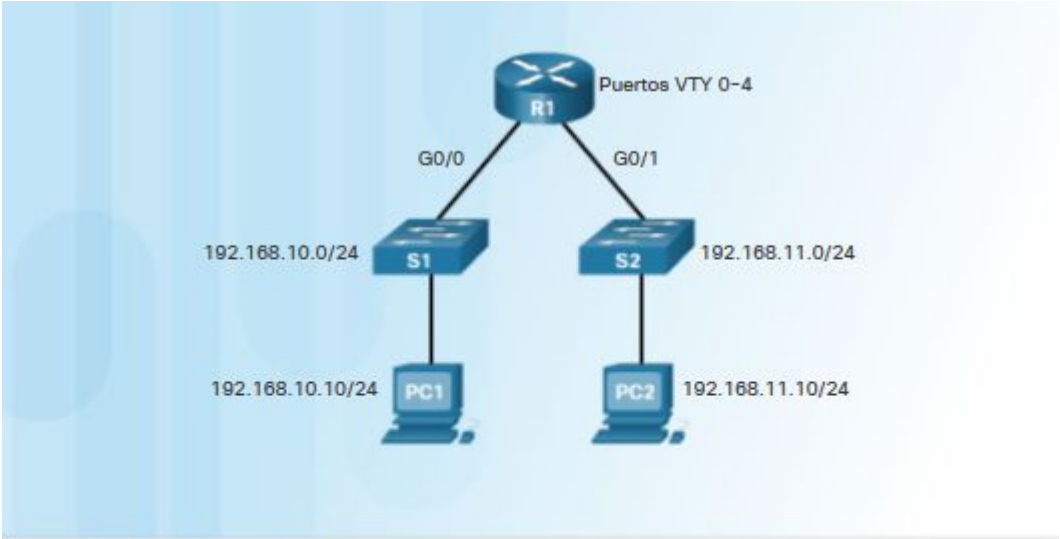
```
R1# show access-lists
Standard IP access list 1
    10 deny 192.168.10.10 (4 match(es))
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
    15 deny 192.168.11.11
    10 deny 192.168.11.10 (4 match(es))
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Resultado después de hacer ping a la PC3 desde la PC1

```
R1# show access-lists
Standard IP access list 1
   10 deny 192.168.10.10 (8 match(es))
   20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
   15 deny 192.168.11.11
   10 deny 192.168.11.10 (4 match(es))
   20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

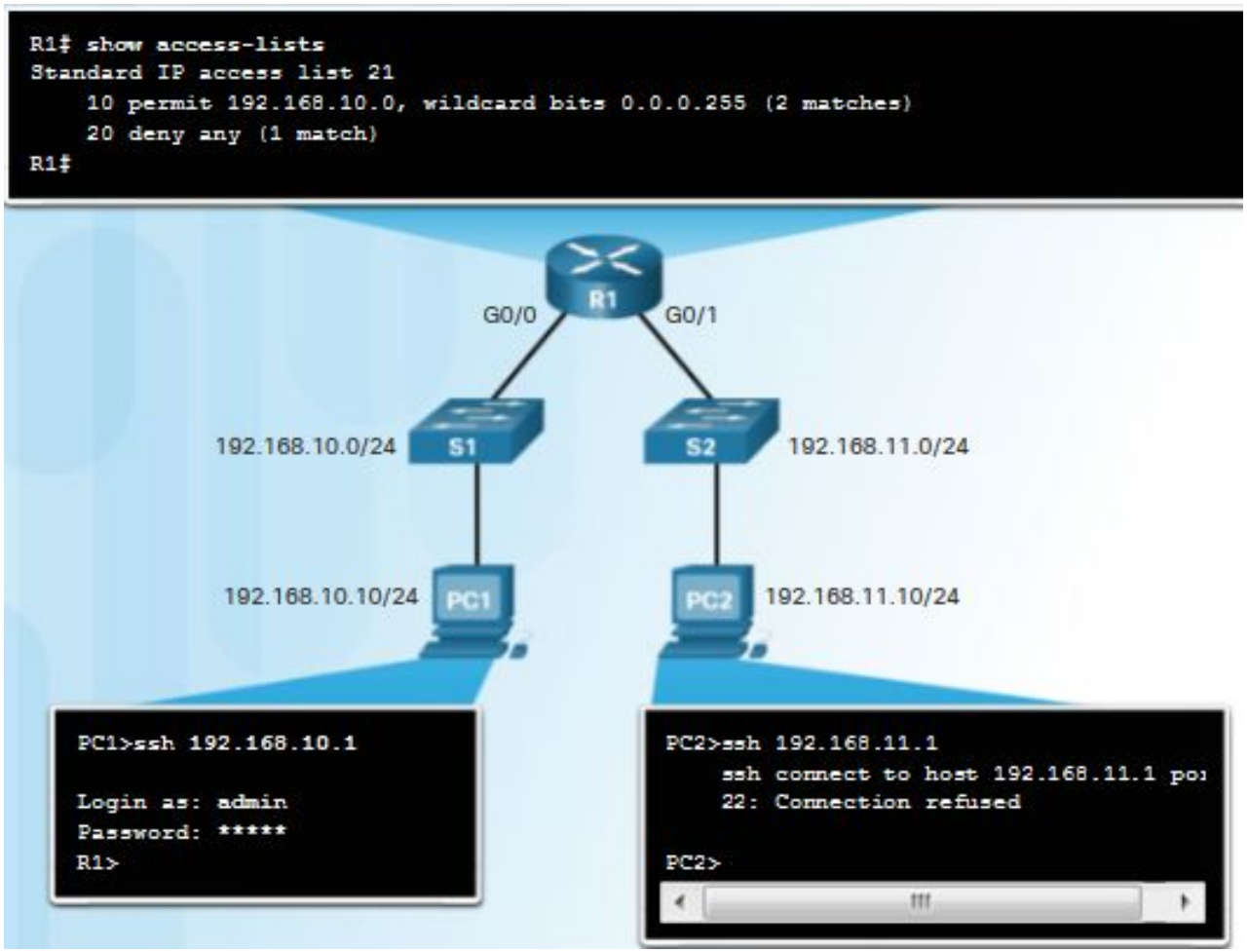
Aumentaron las coincidencias.

El comando access-class



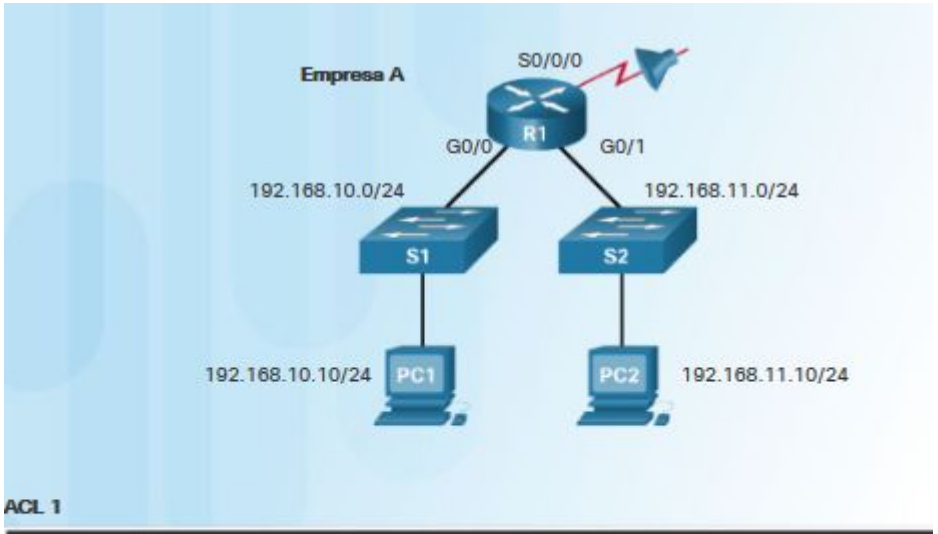

```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# access-class 21 in
R1(config-line)# exit
R1(config)# access-list 21 permit 192.168.10.0 0.0.0.255
R1(config)# access-list 21 deny any
```

Verificación de la seguridad del puerto VTY



Deny any implícita

Una ACL de entrada única con solo una entrada de denegación tiene el efecto de denegar todo el tráfico.



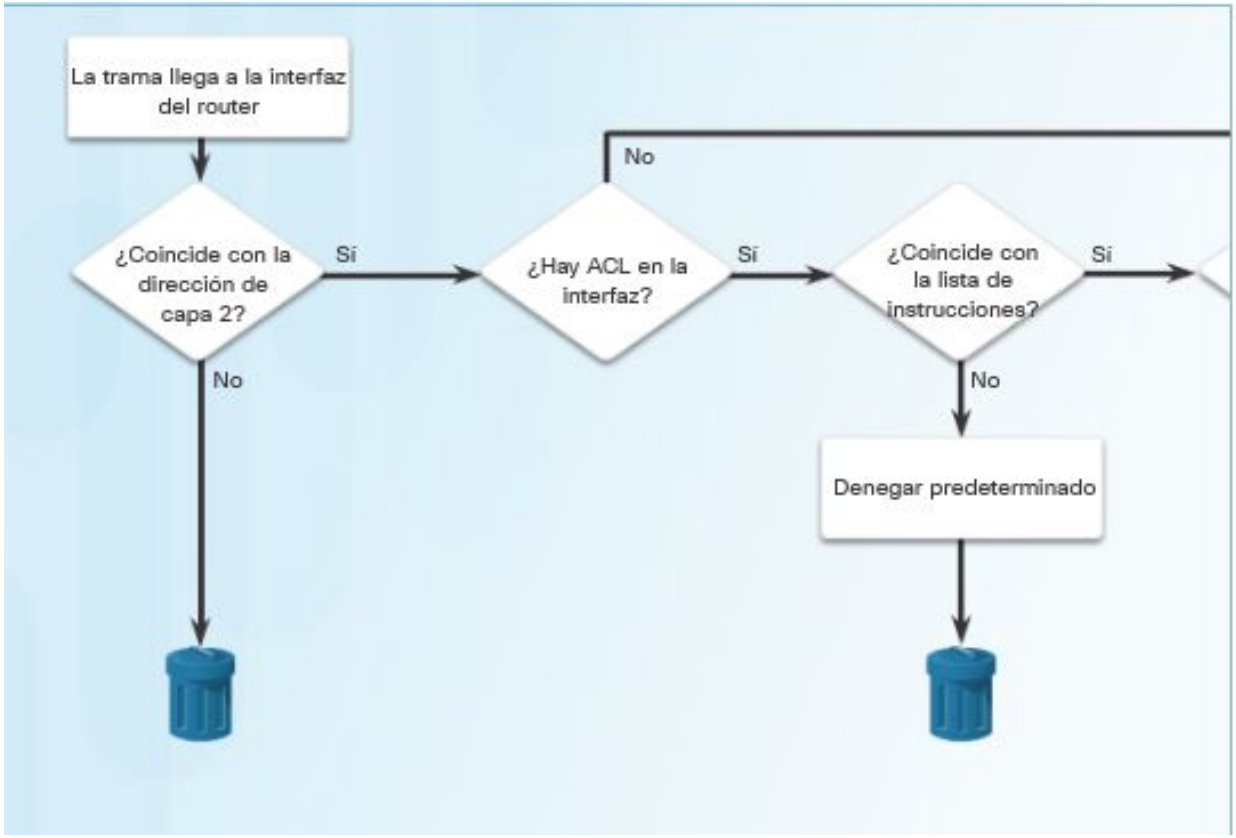
El orden de las ACE en una ACL

```
R1(config)# access-list 3 deny 192.168.10.0 0.0.0.255
R1(config)# access-list 3 permit host 192.168.10.10
%Access rule can't be configured at higher sequence num as it is part of the existing
rule at sequence num 10
R1(config)#
```

```
R1(config)# access-list 4 permit host 192.168.10.10
R1(config)# access-list 4 deny 192.168.10.0 0.0.0.255
R1(config)#
```

```
R1(config)# access-list 5 deny 192.168.10.0 0.0.0.255
R1(config)# access-list 5 permit host 192.168.11.10
R1(config)#
```

Procesos de enrutamiento y ACL



¿Preguntas?

¿Laboratorio?