Materiales para el instructor Capítulo 7: Listas de control de acceso

CCNA Routing and Switching

Routing and Switching Essentials v6.0

Cisco | Networking Academy®
Mind Wide Open™

Materiales del instructor: Guía de planificación del capítulo 7

Esta presentación en PowerPoint se divide en dos partes:

1. Guía de planificación para el instructor
   - Información para ayudarlo a familiarizarse con el capítulo
   - Ayuda a la enseñanza
2. Presentación de la clase del instructor
   - Diapositivas opcionales que puede utilizar en el aula
   - Comienza en la diapositiva n.º 13

Nota: Elimine la Guía de planificación de esta presentación antes de compartirla con otras personas.

Guía de planificación de Routing and Switching Essentials 6.0
Capítulo 7: Listas de control de acceso

Cisco | Networking Academy®
Mind Wide Open™

Capítulo 7: Actividades

¿Qué actividades se relacionan con este capítulo?

N.° de página	Tipo de actividad	Nombre de la actividad	¿Opcional?
7.0.1.2	Actividad de clase	Permítame que lo ayude	Opcional
7.1.1.4	Packet Tracer	Demostración de ACL	Recomendado
7.1.2.6	Actividad	Determinar la máscara de comodín correcta	-
7.1.2.7	Actividad	Determinar el permiso o la denegación	-
7.1.3.3	Actividad	Funcionamiento de las ACL	-
7.2.1.5	Actividad	Configurar listas ACL de IPv4 estándares	-
7.2.1.6	Packet Tracer	Configuración de ACL de IPv4 estándar con números	Recomendado
7.2.1.7	Packet Tracer	Configuración de ACL de IPv4 estándar con nombre	Recomendado
7.2.2.7	Práctica de laboratorio	Configurar y modificar listas ACL de IPv4 estándares	Opcional

La contraseña utilizada en las actividades de Packet Tracer en este capítulo es: **PT_ccna5**

Capítulo 7: Actividades

¿Qué actividades se relacionan con este capítulo?

N.° de página	Tipo de actividad	Nombre de la actividad	¿Opcional?
7.2.3.1	Verificador de sintaxis	Proteger líneas VTY con una ACL de IPv4 estándar	-
7.2.3.3	Packet Tracer	Configuración de una ACL de IPv4 en líneas VTY	Recomendado
7.2.3.4	Práctica de laboratorio	Configuración y verificación de restricciones de VTY	Opcional
7.3.2.4	Packet Tracer	Solución de problemas de ACL de IPv4 estándar	Recomendado
7.3.2.5	Práctica de laboratorio	Solución de problemas de configuración y ubicación de las ACL de IPv4 estándar	Opcional
7.4.1.1	Actividad de clase	Denegación de FTP	Opcional
7.4.1.2	Packet Tracer	Desafío de integración de habilidades	Recomendado

La contraseña utilizada en las actividades de Packet Tracer en este capítulo es: **PT_ccna5**

Capítulo 7: Evaluación

- Los estudiantes deben completar la "Evaluación" del capítulo 7 después de completar el capítulo 7.
- Los cuestionarios, las prácticas de laboratorio, los Packet Tracers y otras actividades se pueden utilizar para evaluar informalmente el progreso de los estudiantes.

Capítulo 7: Prácticas recomendadas

Antes de enseñar el capítulo 7, el instructor debe:

- Completar el capítulo 7: "Evaluación".
- Los objetivos de este capítulo son:
  - Explicar de qué manera las listas ACL filtran el tráfico.
  - Explicar la forma en que las ACL utilizan máscaras de comodín.
  - Explicar cómo se crea una ACL.
  - Explicar cómo se ubica una ACL.
  - Configurar listas ACL de IPv4 estándares para filtrar el tráfico y así cumplir con los requisitos de red.
  - Utilizar números de secuencia para editar listas ACL de IPv4 estándares ya existentes.
  - Configurar una ACL estándar para proteger el acceso a VTY.
  - Explicar la forma en que procesa los paquetes un router cuando se aplica una ACL.
  - Solucionar errores comunes en listas ACL de IPv4 estándares con los comandos de la CLI.

Capítulo 7: Prácticas recomendadas (cont.)

Sección 7.1

- El instructor debe asegurarse de que este capítulo sea lo más práctico posible.
- Enfatice el hecho de que las ACL son listas secuenciales de instrucciones permit o deny, por lo que el orden es importante.
- Los routers no aplican las ACL a sí mismos. El tráfico generado por el router no tiene ninguna ACL aplicada, por lo que probar las ACL desde un router no generará los resultados esperados.

Capítulo 7: Prácticas recomendadas (cont.)

Sección 7.2

- Muestre la forma en que los estudiantes pueden utilizar un editor de texto para crear y luego pegar sus ACL en su programa de terminal. Esto facilita mucho la edición de ACL por parte de los estudiantes.

Capítulo 7: Prácticas recomendadas (cont.)

Sección 7.3

- ¡Práctica, práctica y más práctica!
- Haga que los estudiantes ideen situaciones en las que se deban permitir y/ o bloquear paquetes.

Capítulo 7: Ayuda adicional

- Para obtener ayuda adicional sobre las estrategias de enseñanza, incluidos los planes de lección, las analogías para los conceptos difíciles y los temas de debate, visite la Comunidad CCNA en https://www.netacad.com/group/communities/community-home.
- Prácticas recomendadas de todo el mundo para enseñar CCNA Routing and Switching. https://www.netacad.com/group/communities/ccna-blog
- Si tiene planes o recursos de lección que desee compartir, súbalos a la Comunidad CCNA, a fin de ayudar a otros instructores.
- Los estudiantes pueden inscribirse en **Packet Tracer Know How 1: Packet Tracer 101** (autoinscripción)

Cisco | Networking Academy®

Mind Wide Open™

Capítulo 7: Listas de control de acceso

Routing and Switching Essentials v6.0

Cisco | Networking Academy®
Mind Wide Open™

Capítulo 7: Secciones y objetivos

7.1 Funcionamiento de una ACL

- Explicar de qué manera las listas ACL filtran el tráfico.
- Explicar la forma en que las ACL utilizan máscaras de comodín.
- Explicar cómo se crea una ACL.
- Explicar cómo se ubica una ACL.

7.2 ACL de IPv4 estándar

- Configurar listas ACL de IPv4 estándares para filtrar el tráfico y así cumplir con los requisitos de red.
- Utilizar números de secuencia para editar listas ACL de IPv4 estándares ya existentes.
- Configurar una ACL estándar para proteger el acceso a VTY.

7.3 Solución de problemas en listas ACL

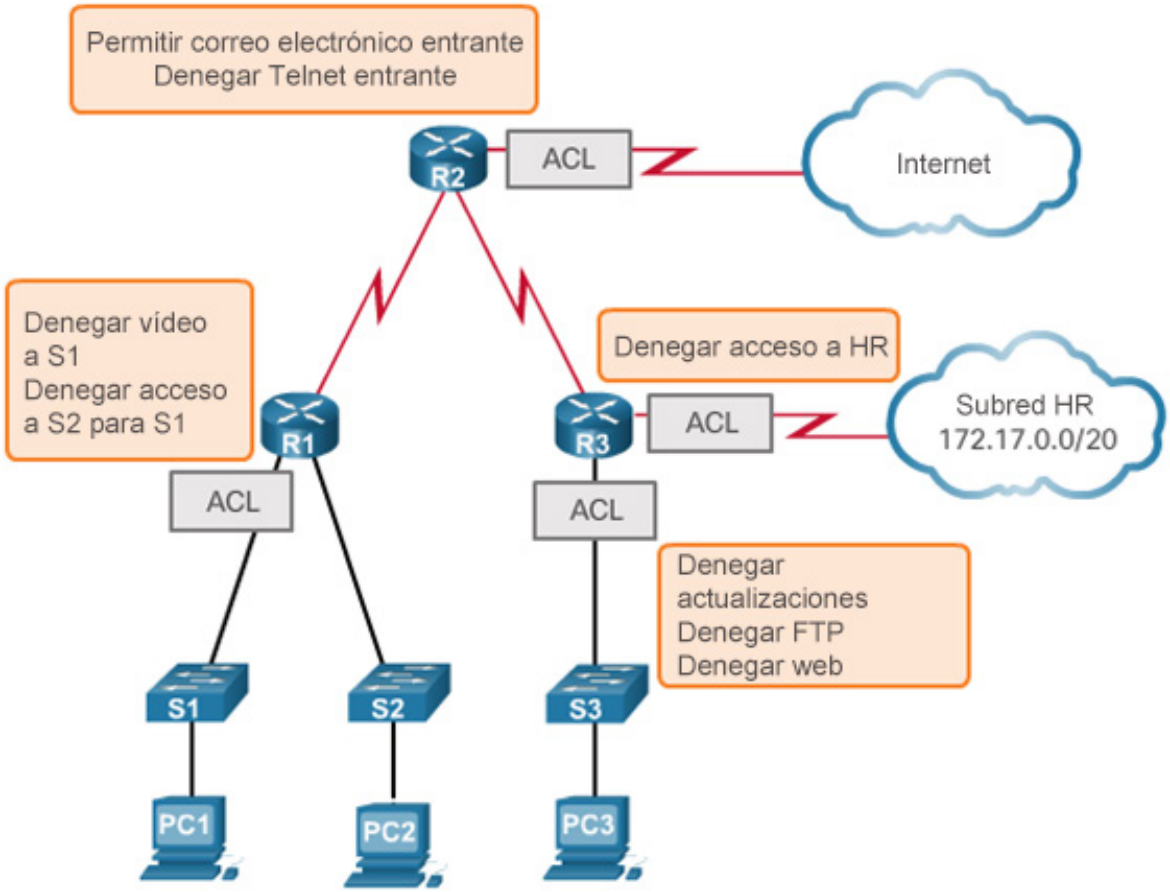
- Explicar la forma en que procesa los paquetes un router cuando se aplica una ACL.
- Solucionar errores comunes en listas ACL de IPv4 estándares con los comandos de la CLI.

7.1 Funcionamiento de una ACL

Cisco | Networking Academy®
Mind Wide Open™

¿Qué es una ACL?

- Los routers no tienen listas ACL configuradas de manera predeterminada, por lo que no filtran el tráfico de manera predeterminada.



Filtrado de paquetes

- El filtrado de paquetes, a veces denominado "filtrado de paquetes estático", controla el acceso a una red mediante el análisis de los paquetes entrantes y salientes y la transferencia o el descarte de estos según determinados criterios, como la dirección IP de origen, la dirección IP de destino y el protocolo incluido en el paquete.
- Cuando reenvía o deniega los paquetes según las reglas de filtrado, un router funciona como filtro de paquetes.
- Una ACL es una lista secuencial de instrucciones permit (permitir) o deny (denegar), conocidas como "entradas de control de acceso" (ACE).

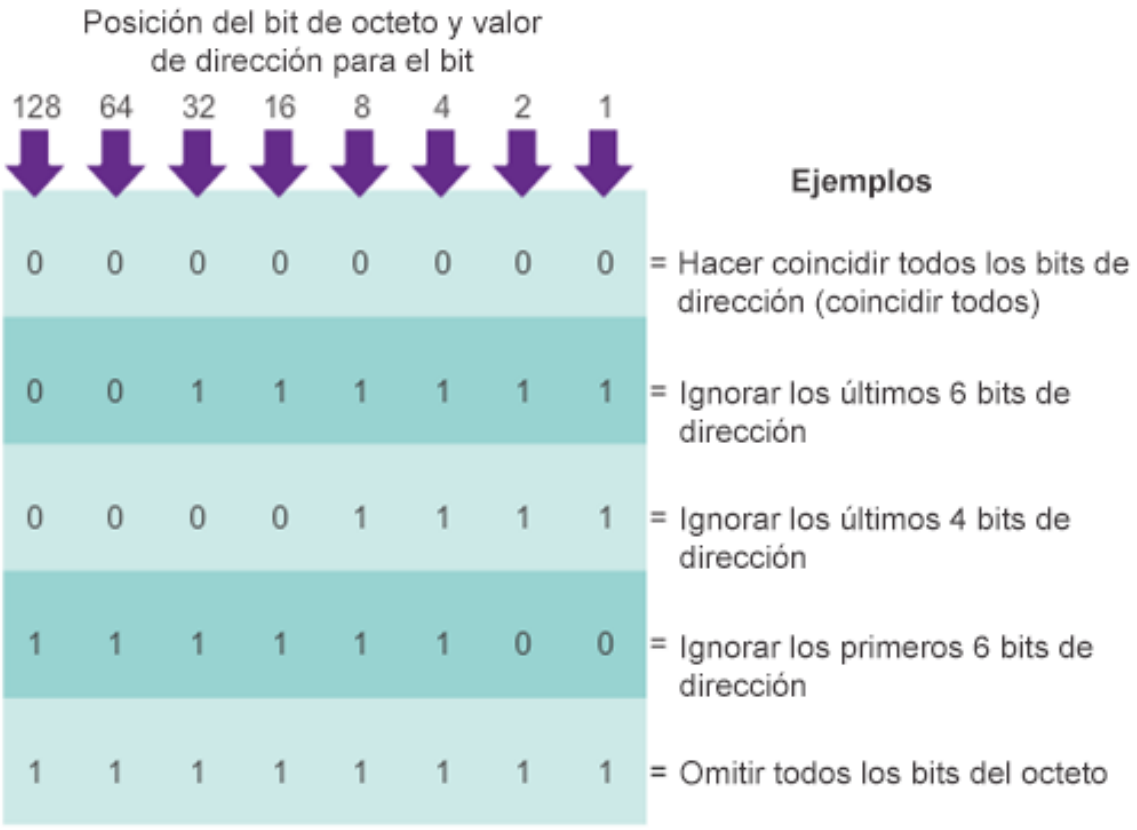
Funcionamiento de una ACL

Las ACL de entrada filtran los paquetes que ingresan a una interfaz específica y lo hacen antes de que se enruten a la interfaz de salida.

Las ACL de salida filtran los paquetes después de que se enrutan, independientemente de la interfaz de entrada.

Introducción a las máscaras de comodín en listas ACL

Máscaras de comodín



0 significa hacer coincidir el valor del bit de dirección correspondiente
1 significa ignorar el valor del bit de dirección correspondiente

Introducción a las máscaras de comodín en listas ACL (continuación)

Ejemplo

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

Máscaras de comodín en listas ACL

Ejemplos de máscaras de comodín

Máscaras de comodín para establecer coincidencias con hosts y subredes IPv4

Ejemplo 1

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

Ejemplos de máscaras de comodín (continuación)

Máscaras de comodín para establecer coincidencias con rangos

Ejemplo 1

	Decimal	Binario
Dirección IP	192.168.16.0	11000000.10101000.00010000.00000000
Máscara de comodín	0.0.15.255	00000000.00000000.00001111.11111111
Rango de resultados	192.168.16.0 a 192.168.31.255	11000000.10101000.00010000.00000000 a 11000000.10101000.00011111.11111111

Ejemplo 2

	Decimal	Binario
Dirección IP	192.168.1.0	11000000.10101000.00000001.00000000
Máscara de comodín	0.0.254.255	00000000.00000000.11111110.11111111
Resultado	192.168.1.0	11000000.10101000.00000001.00000000
	Todas las subredes con número impar en la red principal 192.168.0.0	

Cálculo de la máscara de comodín

- El cálculo de máscaras de comodín puede ser difícil. Un método abreviado es restar la máscara de subred a 255.255.255.255.

Ejemplo 1

```
  255.255.255.255
- 255.255.255.000
-----------------
  000.000.000.255
```

Ejemplo 2

```
  255.255.255.255
- 255.255.255.240
-----------------
  000.000.000.015
```

Ejemplo 3

```
  255.255.255.255
- 255.255.252.000
-----------------
  000.000.003.255
```

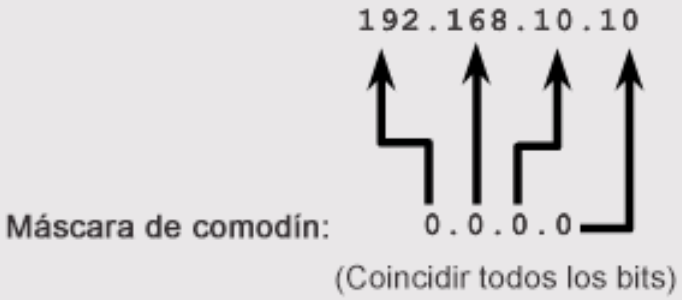
Máscaras de comodín en listas ACL

Palabras clave de una máscara de comodín

Abreviaturas de la máscara de bits de comodín

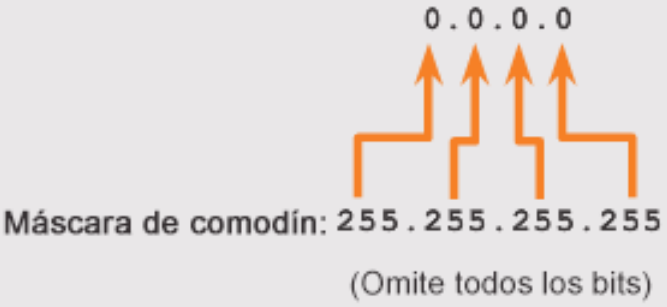
Ejemplo 1

- 192.168.10.10 0.0.0.0 coincide con todos los bits de la dirección.
- Abrevie esta máscara de comodín utilizando 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`



Ejemplos de palabras clave de una máscara de comodín

Ejemplo 1:

```
R1(config)# access-list 1 permit 0.0.0.0 255.255.255.255
!OR
R1(config)# access-list 1 permit any
```

Ejemplo 2:

```
R1(config)# access-list 1 permit 192.168.10.10 0.0.0.0
!OR
R1(config)# access-list 1 permit host 192.168.10.10
```

Este es el formato de las palabras clave opcionales any y host en una sentencia ACL.

Pautas generales para la creación de listas ACL

Filtrado de tráfico en un router mediante ACL

Una lista por interfaz, por dirección y por protocolo

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)

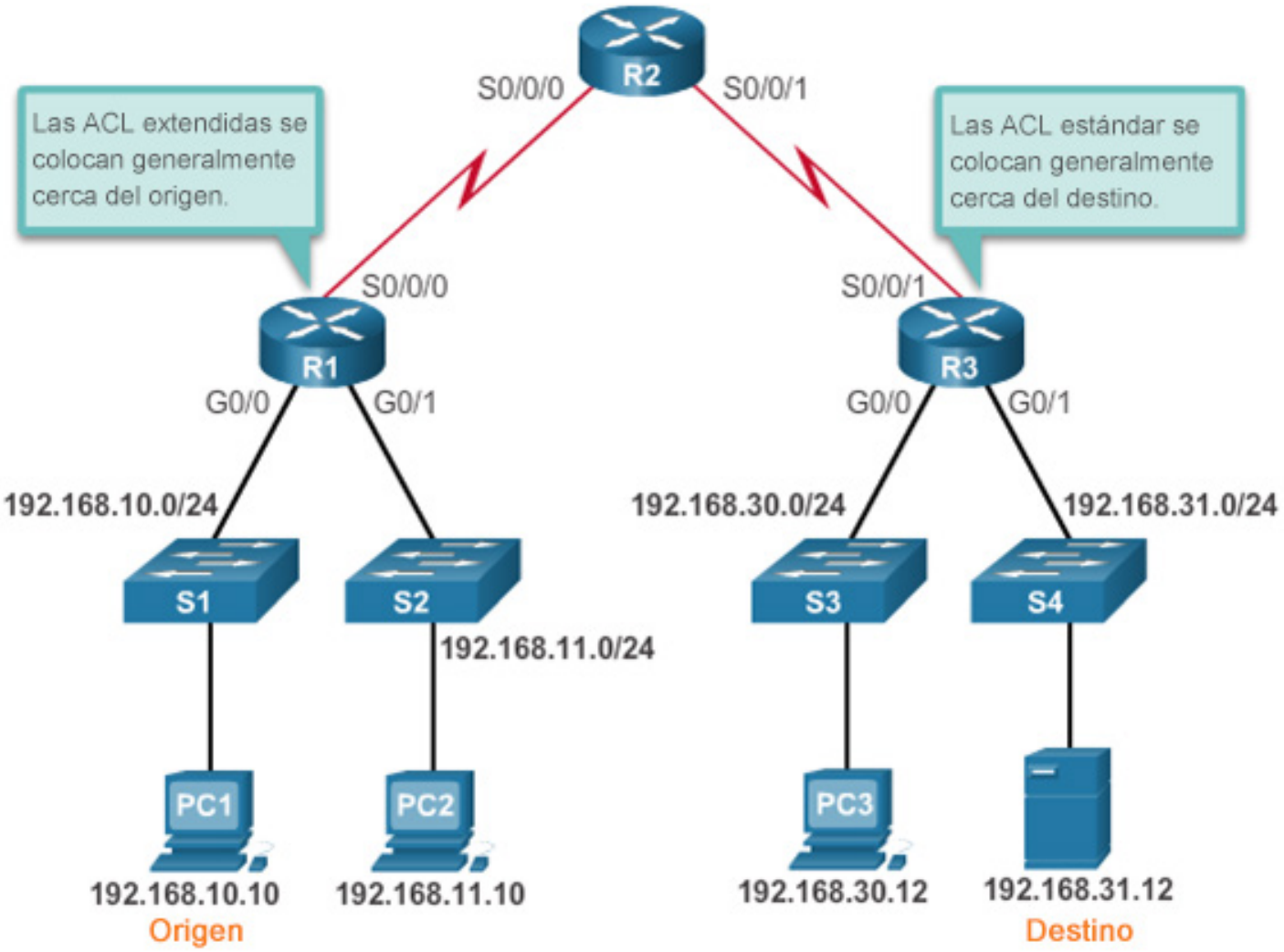
Pautas para la creación de listas ACL

Prácticas recomendadas para una 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.

Pautas para la ubicación de listas ACL

¿Dónde ubicar las listas ACL?

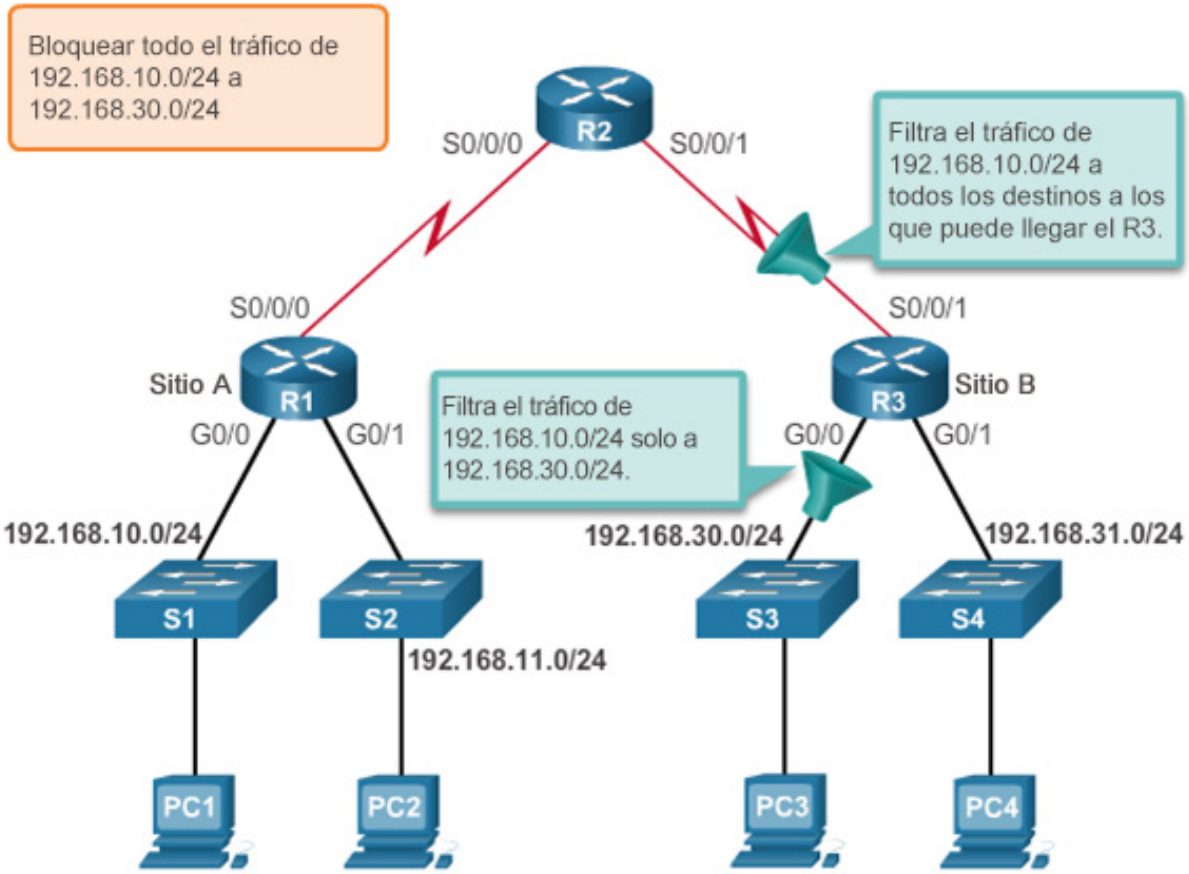


¿Dónde ubicar las listas ACL? (continuación)

- Cada ACL se debe colocar donde tenga más impacto en la eficiencia. Las reglas básicas son las siguientes:
  - Listas ACL extendidas: coloque las listas ACL extendidas lo más cerca posible del origen del tráfico que se filtrará.
  - Listas ACL estándares: debido a que en las listas ACL estándares no se especifican las direcciones de destino, colóquelas tan cerca del destino como sea posible.
  - La ubicación de la ACL y, por lo tanto, el tipo de ACL que se utiliza, también pueden depender del alcance del control del administrador de red, del ancho de banda de las redes que intervienen y de la facilidad de configuración.

Ubicación de listas ACL estándares

- El administrador desea impedir que el tráfico que se origina en la red 192.168.10.0/24 llegue a la red 192.168.30.0/24.



7.2 ACL de IPv4 estándar

Cisco | Networking Academy®
Mind Wide Open™

Sintaxis de una ACL de IPv4 estándar numerada

- Router(config)# **access-list** *número-de-lista-de-acceso* { **deny** | **permit** | **remark** } *origen* [*comodín-de-origen*] [**log**]

```
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)# exit
R1# show access-lists
Standard IP access list 10
    10 permit 192.168.10.0, wildcard bits 0.0.0.255
R1# conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
R1(config)# no access-list 10
R1(config)# exit
R1# show access-lists
R1#
```

```
R1(config)# access-list 10 remark Permit hosts from the
192.168.10.0 LAN
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)# exit
R1# show running-config | include access-list 10
access-list 10 remark Permit hosts from the 192.168.10.0 LAN
access-list 10 permit 192.168.10.0 0.0.0.255
R1#
```

Aplicar listas ACL de IPv4 estándares a las interfaces

Procedimiento para la configuración de ACL estándar

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 su 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
```

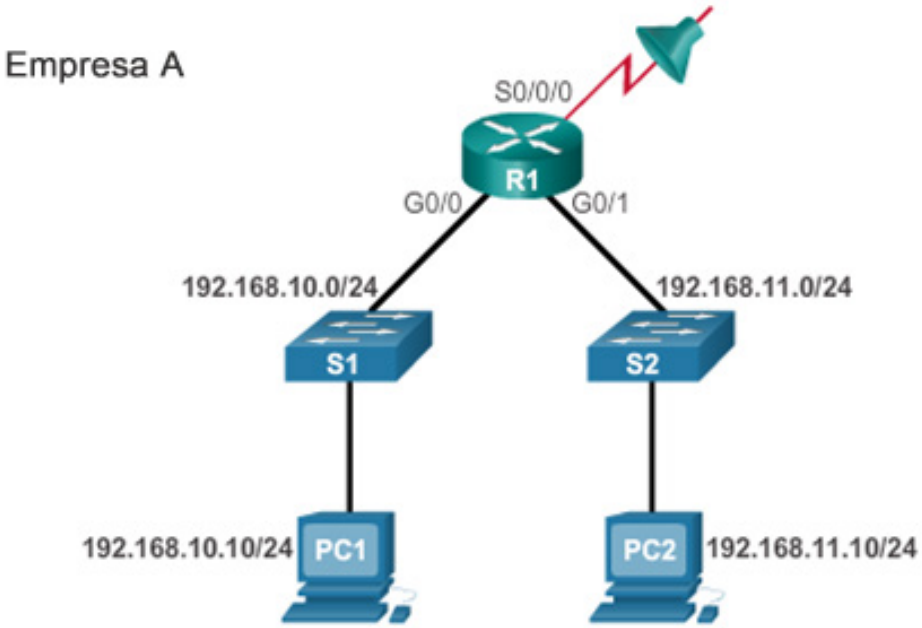
Paso 3: utilice el comando de configuración de interfaz `ip access-group` para activar la ACL actual en una interfaz.

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

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

Aplicar listas ACL de IPv4 estándares a las interfaces (continuación)

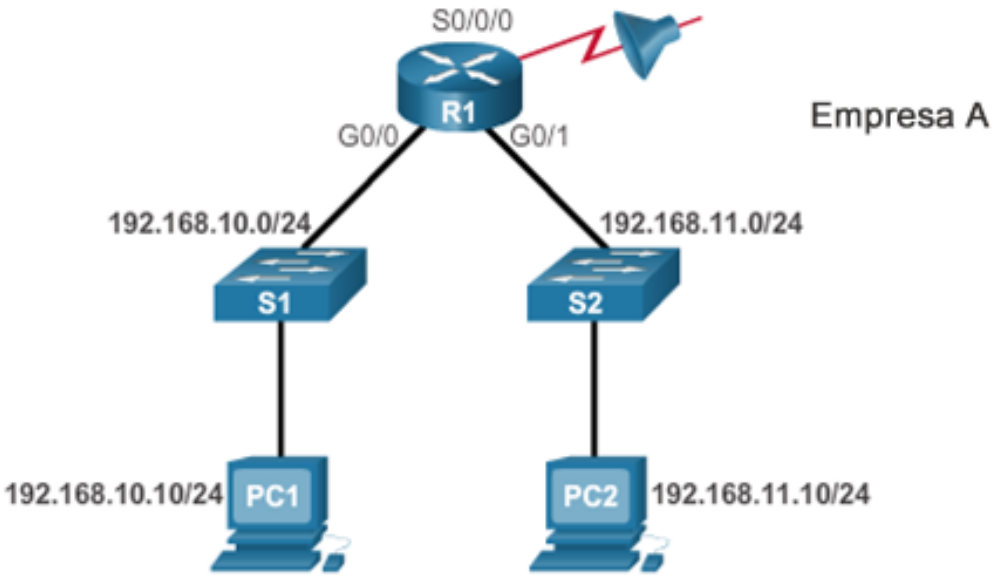
Admisión de una subred específica




```
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 1 out
```

Ejemplos de listas ACL de IPv4 estándares numeradas

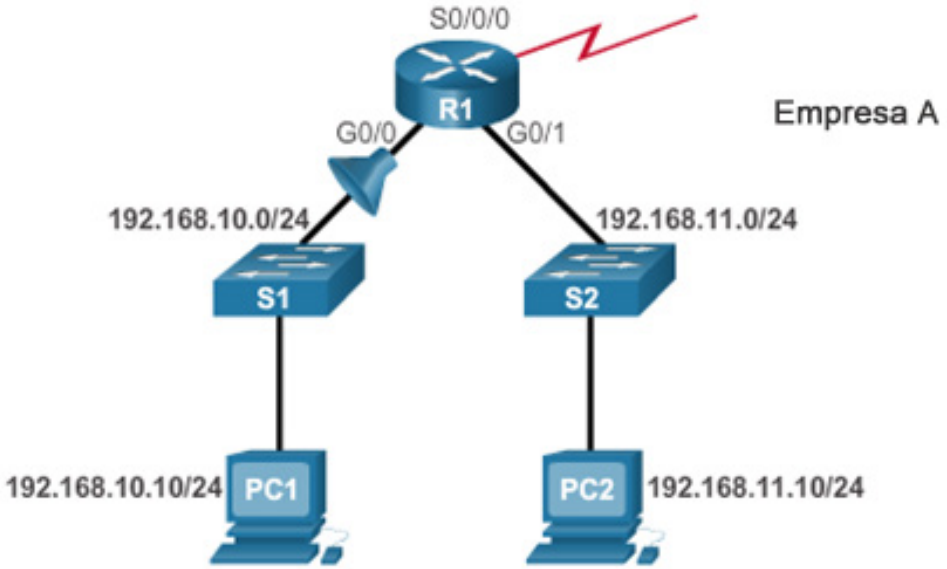
Denegación de un host específico y admisión de una subred específica




```
R1(config)# no access-list 1
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 1 out
```

Ejemplos de listas ACL de IPv4 estándares numeradas (continuación)

Denegación de un host específico




```
R1(config)# no access-list 1
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 permit any
R1(config)# interface g0/0
R1(config-if)# ip access-group 1 in
```

Sintaxis de una ACL de IPv4 estándar con nombre

Ejemplo de ACL denominada

```
Router(config)# ip access-list [standard | extended] name
```

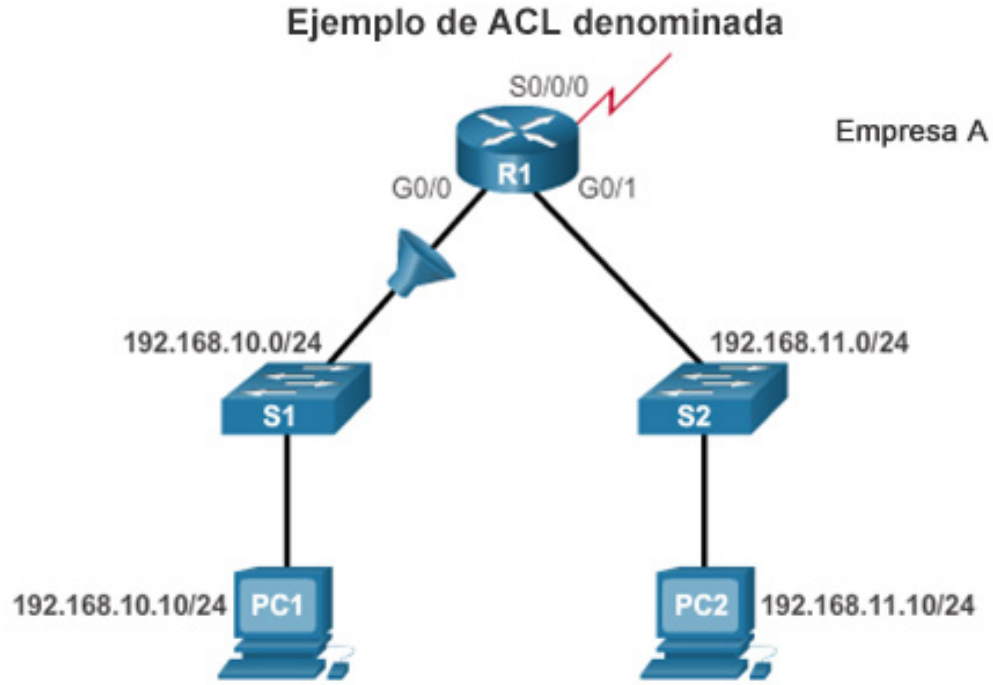
La cadena de nombres alfanuméricos debe ser única y no puede comenzar con un número.

```
Router(config-std-nacl)# [permit | deny | remark] {source
[source-wildcard]} [log]
```

```
Router(config-if)# ip access-group name [in | out]
```

Activa la ACL IP denominada en una interfaz.

Sintaxis de una ACL de IPv4 estándar con nombre (continuación)




```
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
```

Modificar listas ACL de IPv4

Método 1: Utilizar un editor de texto

Edición de ACL numeradas mediante un editor de texto

Configuración

```
R1(config)# access-list 1 deny host 192.168.10.99
R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Paso 1

```
R1# show running-config | include access-list 1
access-list 1 deny host 192.168.10.99
access-list 1 permit 192.168.0.0 0.0.255.255
```

Paso 2

```
<Text editor>
access-list 1 deny host 192.168.10.10
access-list 1 permit 192.168.0.0 0.0.255.255
```

Paso 3

```
R1# config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# no access-list 1
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Paso 4

```
R1# show running-config | include access-list 1
access-list 1 deny host 192.168.10.10
access-list 1 permit 192.168.0.0 0.0.255.255
```

Modificar listas ACL de IPv4

Método 2: Utilizar números de secuencia

Edición de ACL numeradas mediante números de secuencia

Configuración

```
R1(config)# access-list 1 deny host 192.168.10.99
R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Paso 1

```
R1# show access-lists 1
Standard IP access list 1
    10 deny   192.168.10.99
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
R1#
```

Paso 2

```
R1# conf t
R1(config)# ip access-list standard 1
R1(config-std-nacl)# no 10
R1(config-std-nacl)# 10 deny host 192.168.10.10
R1(config-std-nacl)# end
R1#
```

Paso 3

```
R1# show access-lists
Standard IP access list 1
    10 deny   192.168.10.10
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
R1#
```

Modificar listas ACL de IPv4

Editar listas ACL estándares con nombre

Cómo agregar una línea a la ACL denominada

```
R1# show access-lists
Standard IP access list NO_ACCESS
    10 deny   192.168.11.10
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1# conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# 15 deny host 192.168.11.11
R1(config-std-nacl)# end
R1# show access-lists
Standard IP access list NO_ACCESS
    10 deny   192.168.11.10
    15 deny   192.168.11.11
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Nota: el comando **no** *número-de-secuencia* de ACL con nombre se usa para eliminar instrucciones individuales.

Modificar listas ACL de IPv4

Verificar listas 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
<output omitted>
  Outgoing access list is 1
  Inbound  access list is not set
<output omitted>

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

```
R1# show access-lists
Standard IP access list 1
    10 deny   192.168.10.10
    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
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Modificar listas ACL de IPv4

Estadísticas de una 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

Aumentaron las coincidencias.

```
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#
```

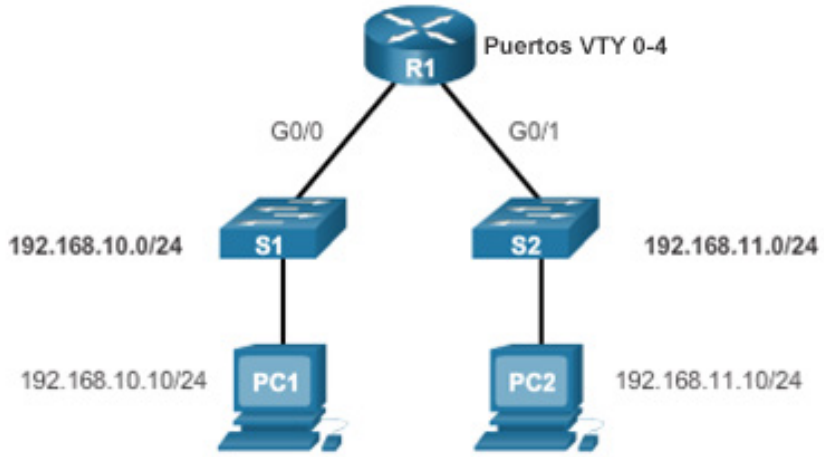
```
R1# show access-lists
Standard IP access list 1
    10 deny   192.168.10.10 (8 match(es))
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
    15 deny   192.168.11.11
    10 deny   192.168.11.10 (4 match(es))
    20 permit 192.168.11.0, wildcard bits 0.0.0.255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

Se borraron las coincidencias.

Asegurar puertos VTY con una ACL de IPv4 estándar

El comando access-class

- El comando **access-class** configurado en el modo de configuración de línea restringe las conexiones entrantes y salientes entre una VTY determinada (en un dispositivo de Cisco) y las direcciones incluidas en una lista de acceso.

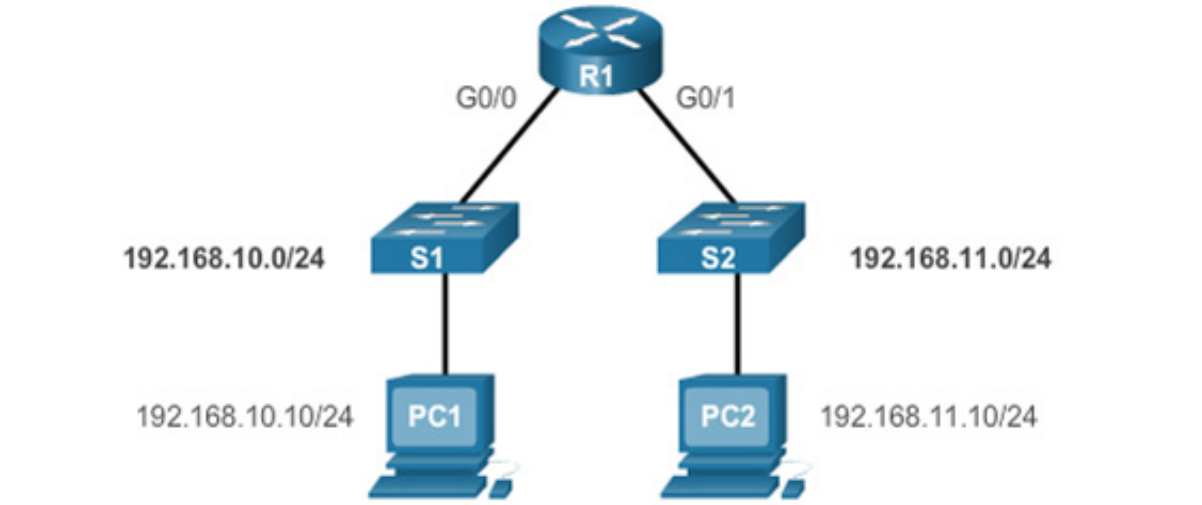



```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# access-class 21 in
R1(config-line)# exit
R1(config)# access-list 21 permit 192.168.10.0 0.0.0.255
R1(config)# access-list 21 deny any
```

Asegurar puertos VTY con una ACL de IPv4 estándar

Verificar que el puerto VTY esté asegurado

```
R1# show access-lists
Standard IP access list 21
    10 permit 192.168.10.0, wildcard bits 0.0.0.255 (2 matches)
    20 deny   any (1 match)
R1#
```




```
PC1>ssh 192.168.10.1

Login as: admin
Password: *****
R1>
```

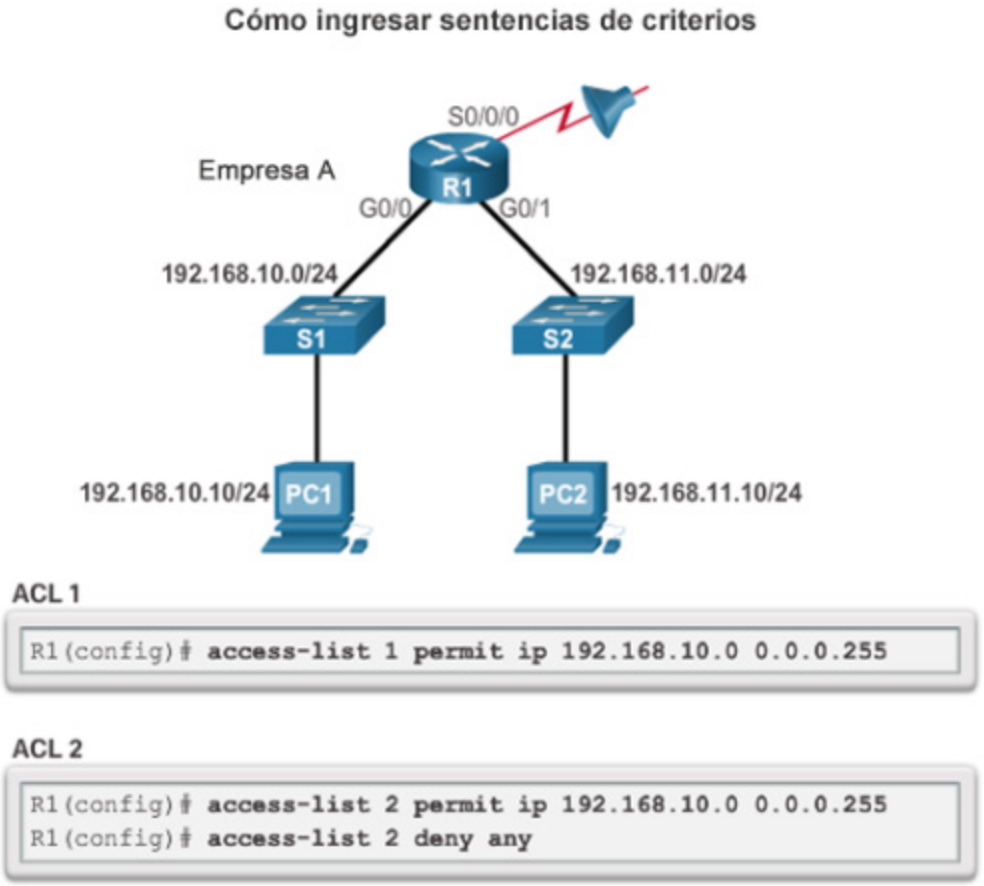
```
PC2>ssh 192.168.11.1
ssh connect to host 192.168.11.1 port
22: Connection refused

PC2>
```

7.3 Solución de problemas en listas ACL

Cisco | Networking Academy®
Mind Wide Open™

Denegar todo implícito

- Se debe configurar al menos una ACE permit en una ACL. En caso contrario, se bloquea todo el tráfico.
- Para la red en la ilustración, si se aplica la ACL 1 o la ACL 2 a la interfaz S0/0/0 del R1 en el sentido de salida, se obtiene el mismo resultado.



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)#
```

ACL 3: la instrucción de host entra en conflicto con la instrucción de rango anterior.

```
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)#
```

ACL 4: la instrucción de host siempre puede configurarse antes que las instrucciones de rango.

El orden de las ACE en una ACL (continuación)

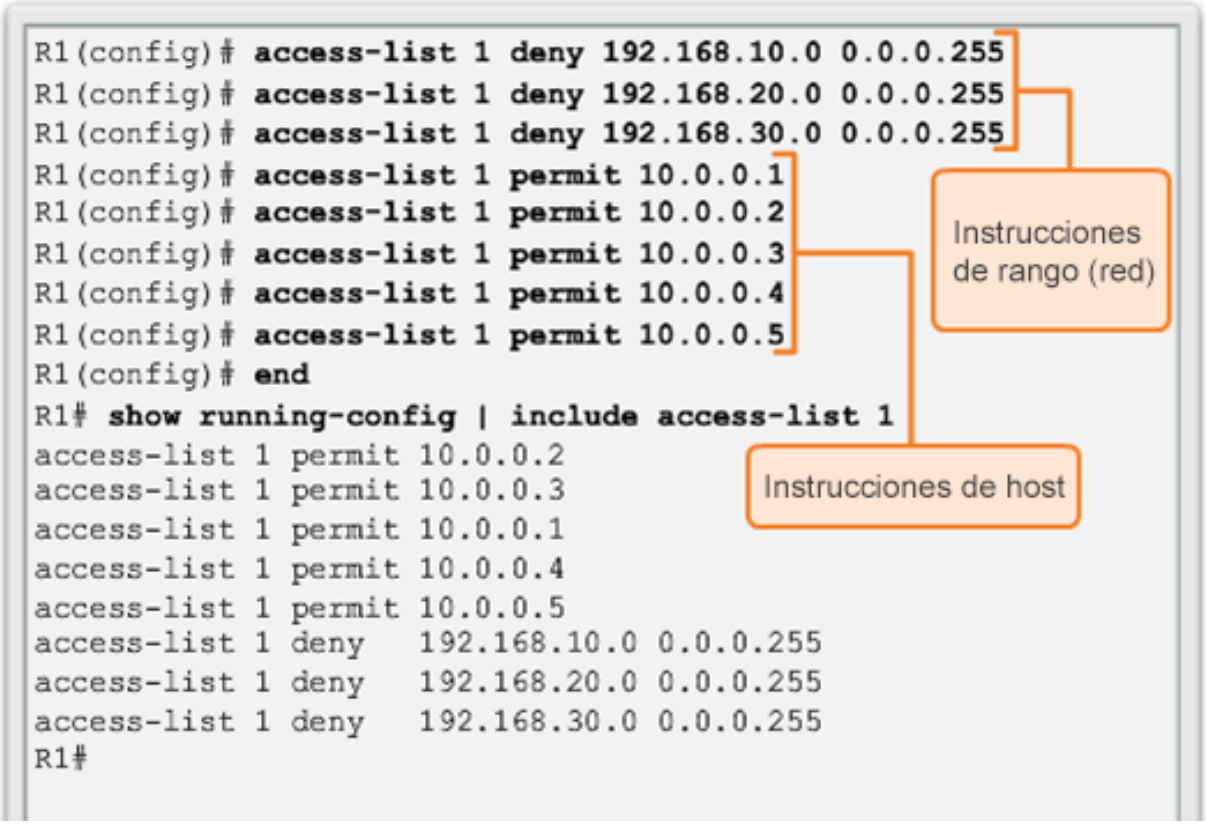
```
R1(config)# access-list 5 deny 192.168.10.0 0.0.0.255
R1(config)# access-list 5 permit host 192.168.11.10
R1(config)#
```

ACL 5: si no existen conflictos, la instrucción de host se puede configurar después que la instrucción de rango.

Cisco IOS reordena las listas ACL estándares

Observe que las instrucciones se enumeran en un orden distinto al orden en que se introdujeron.

Consideraciones de secuenciación durante la configuración



Cisco IOS reordena las listas ACL estándares (continuación)

El orden en que se enumeran las ACE estándar es la secuencia utilizada por el IOS para procesar la lista.

```
R1# show access-lists 1
Standard IP access list 1
 50 permit 10.0.0.2
 60 permit 10.0.0.3
 40 permit 10.0.0.1
 70 permit 10.0.0.4
 80 permit 10.0.0.5
 10 deny   192.168.10.0, wildcard bits 0.0.0.255
 20 deny   192.168.20.0, wildcard bits 0.0.0.255
 30 deny   192.168.30.0, wildcard bits 0.0.0.255
R1# copy running-config startup-config
R1# reload
R1# show access-lists 1
Standard IP access list 1
 10 permit 10.0.0.2
 20 permit 10.0.0.3
 30 permit 10.0.0.1
 40 permit 10.0.0.4
 50 permit 10.0.0.5
 60 deny   192.168.10.0, wildcard bits 0.0.0.255
 70 deny   192.168.20.0, wildcard bits 0.0.0.255
 80 deny   192.168.30.0, wildcard bits 0.0.0.255
R1#
```

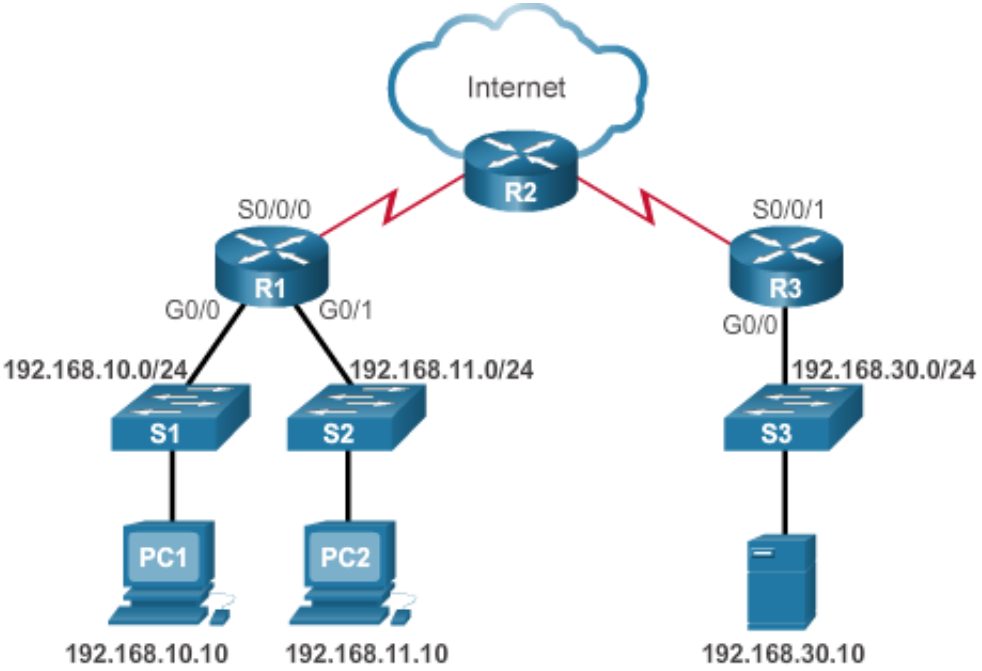
Las instrucciones de host se enumeran primero en un orden que permita que IOS los procese de manera eficaz.

Las instrucciones de rango se enumeran después de las instrucciones de host, en el orden en que se introdujeron.

Procesos de routing y listas ACL

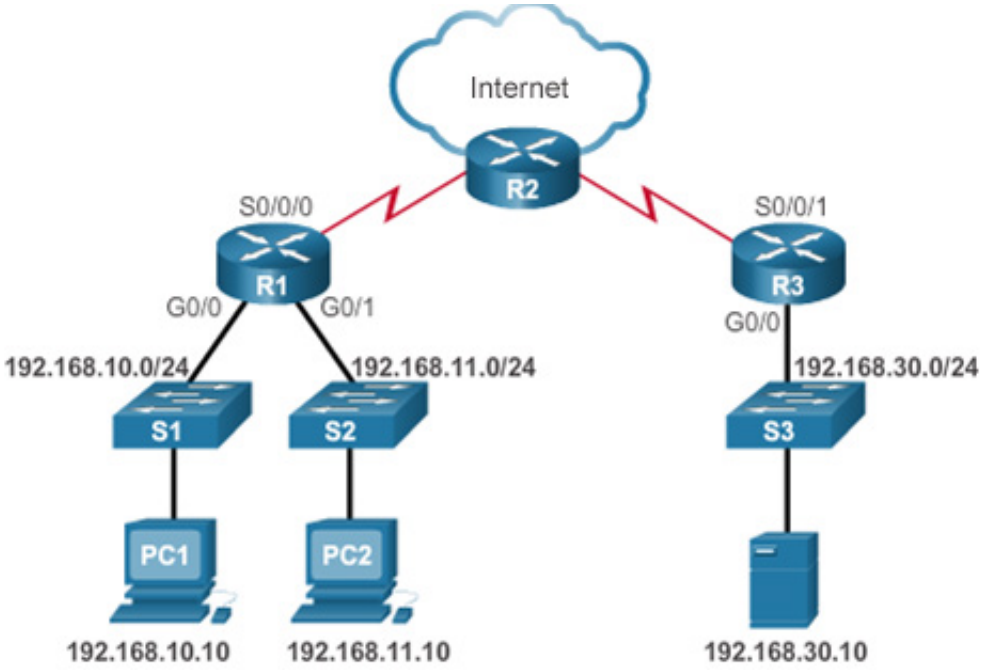
- Cuando una trama ingresa a una interfaz, el router revisa si la dirección de capa 2 de destino coincide con la dirección de capa 2 de la interfaz, o si dicha trama es una trama de difusión.
- Si se acepta la dirección de la trama, se desmonta la información de la trama y el router revisa si hay una ACL en la interfaz de entrada.
- Si existe una ACL, el paquete se prueba en relación con las instrucciones de la lista.
- Si el paquete coincide con una instrucción, se permite o se deniega.
- Si se acepta el paquete, se compara con las entradas en la tabla de routing para determinar la interfaz de destino.
- Si existe una entrada para el destino en la tabla de routing, el paquete se conmuta a la interfaz de salida. De lo contrario, se descarta.
- A continuación, el router revisa si la interfaz de salida tiene una ACL. Si existe una ACL, el paquete se prueba en relación con las instrucciones de la lista. Si el paquete coincide con una instrucción, se permite o se deniega.
- Si no hay una ACL o si se permite el paquete, este se encapsula en el nuevo protocolo de capa 2 y se reenvía por la interfaz al siguiente dispositivo.

Solucionar problemas en listas ACL de IPv4 estándares: Ejemplo 1




```
R3# show access-list
Standard IP access list 10
    10 deny   192.168.11.10
R3#
```

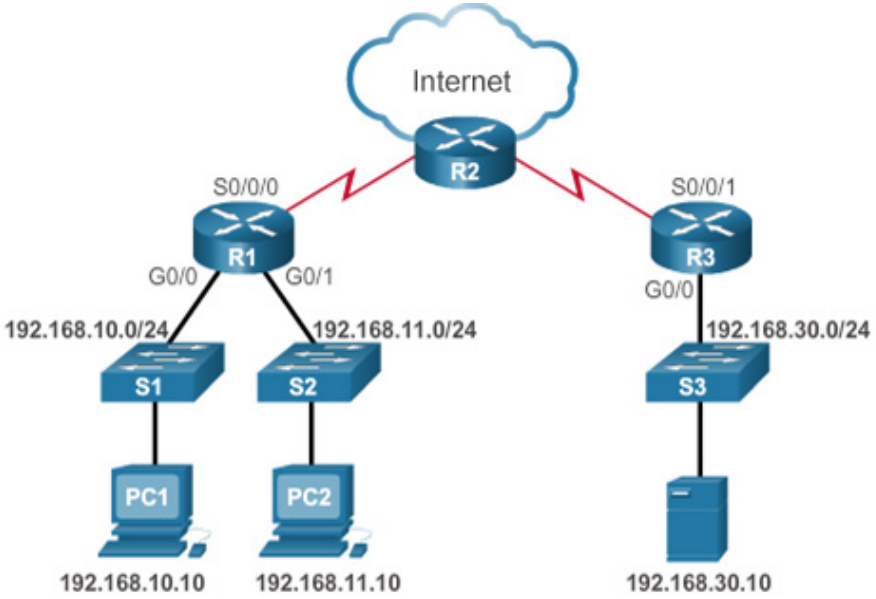
Solucionar problemas en listas ACL de IPv4 estándares: Ejemplo 1 (continuación)




```
R3(config)# access-list 10 permit any
R3(config)# end
R3# show access-list
Standard IP access list 10
    10 deny   192.168.11.10
    20 permit any (4 match(es))
R3#
```

Solucionar problemas en listas ACL de IPv4 estándares: Ejemplo 2

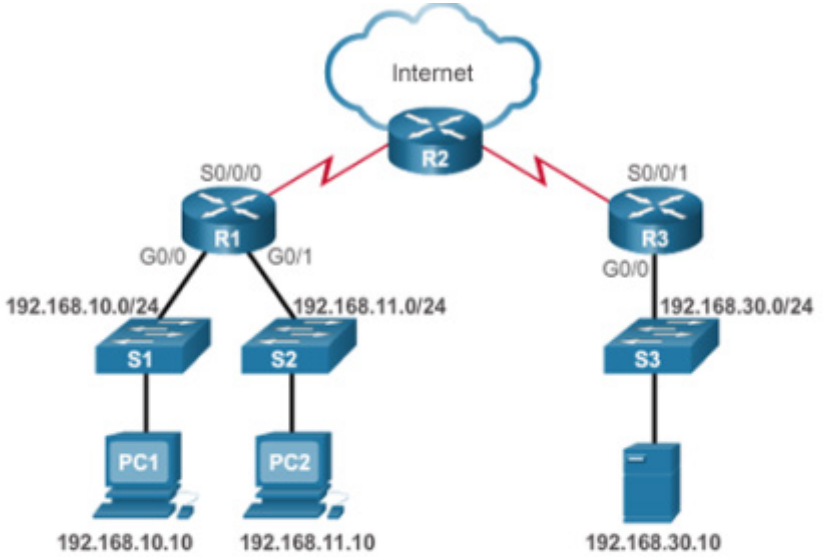
Política de seguridad: la red 192.168.11.0/24 no debería poder acceder a la red 192.168.10.0/24.




```
R1# show access-list
Standard IP access list 20
    10 deny   192.168.11.0, wildcard bits 0.0.0.255 (8 match(es))
    20 permit any
```

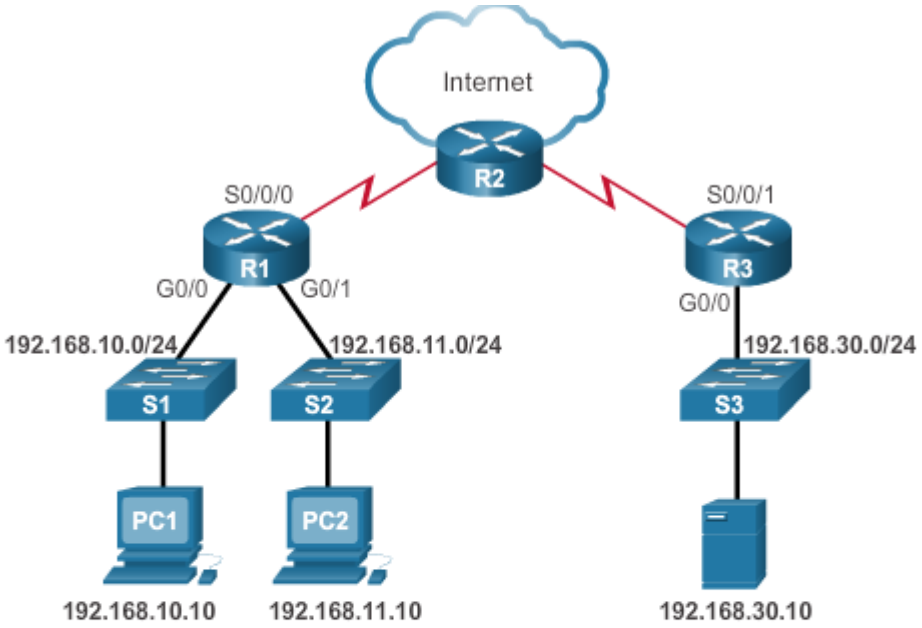
Solucionar problemas en listas ACL de IPv4 estándares: Ejemplo 2 (continuación)

Se aplicó la ACL 20 a la interfaz equivocada en la dirección equivocada. Se deniega todo el tráfico entrante de 192.168.11.0/24 a través de la interfaz G0/1.



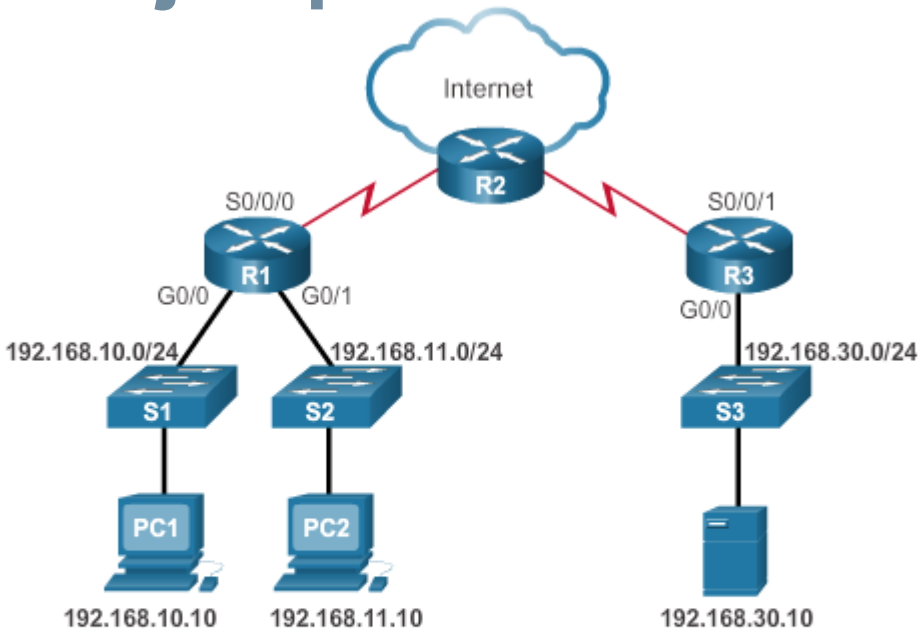

```
speed auto
interface GigabitEthernet0/1
ip address 192.168.11.1 255.255.255.0
ip access-group 20 in
duplex auto
speed auto
<Output omitted>
```

Solucionar problemas en listas ACL de IPv4 estándares: Ejemplo 2 (continuación)




```
R1# config t
R1(config)# interface g0/1
R1(config-if)# no ip access-group 20 in
R1(config-if)# interface g0/0
R1(config-if)# ip access-group 20 out
```

Solucionar problemas en listas ACL de IPv4 estándares: Ejemplo 3



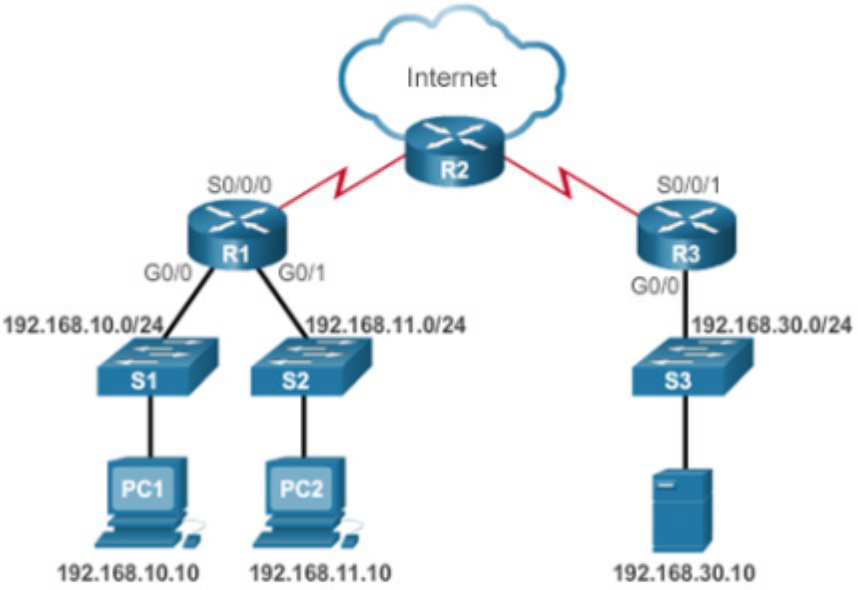
Problema

Política de seguridad: Solo a PC1 se le permite el acceso remoto SSH a R1.

```
R1# show run | section line vty
line vty 0 4
 access-class PC1-SSH in
 login
 transport input ssh
```

```
R1# show access-list
Standard IP access list PC1-SSH
    10 permit 192.168.10.1
    20 deny   any (5 match(es))
R1#
```

Solucionar problemas en listas ACL de IPv4 estándares: Ejemplo 3 (continuación)




```
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip access-list standard PC1-SSH
R1(config-std-nacl)# no 10
R1(config-std-nacl)# 10 permit host 192.168.10.10
R1(config-std-nacl)# end
R1# clear access-list counters
```

```
R1# show access-list
Standard IP access list PC1-SSH
    10 permit 192.168.10.10 (2 match(es))
    20 deny   any
R1#
```

¡Solución!

Política de seguridad: Solo a PC1 se le permite el acceso remoto SSH a R1.

7.4 Resumen

Cisco | Networking Academy®
Mind Wide Open™

Resumen

- Explicar de qué manera las listas ACL filtran el tráfico.
- Explicar la forma en que las ACL utilizan máscaras de comodín.
- Explicar cómo se crea una ACL.
- Explicar cómo se ubica una ACL.
- Configurar listas ACL de IPv4 estándares para filtrar el tráfico y así cumplir con los requisitos de red.
- Utilizar números de secuencia para editar listas ACL de IPv4 estándares ya existentes.
- Configurar una ACL estándar para proteger el acceso a VTY.
- Explicar la forma en que procesa los paquetes un router cuando se aplica una ACL.
- Solucionar errores comunes en listas ACL de IPv4 estándares con los comandos de la CLI.

Sección 7.1
Términos y comandos

- Lista de control de acceso (ACL)
- Filtrado de paquetes
- Entradas de control de acceso (ACE)
- Listas ACL estándares
- Listas ACL extendidas
- Listas ACL entrantes
- Listas ACL salientes
- Máscaras de comodín
- Bit 0 de la máscara de comodín
- Bit 1 de la máscara de comodín
- **access-list *número-de-lista-de-acceso* permit *dirección_ip máscara de comodín***
- host
- cualquiera

Sección 7.2
Términos y comandos

- **access-list *número-de-lista-de-acceso* { deny | permit | remark }*origen* [*comodín-de-origen*][log]**
- **show access-lists**
- **no access-list *número-de-lista-de-accesso***
- **ip access-group {*número-de-lista-de-acceso* | *nombre-de-lista-de-acceso*} { in | out }**
- **ip access-list standard** *nombre*
- **clear access-list counters**
- **access-class *número-de-lista-de-acceso* { in |out }**