Capítulo 7: Listas de control de acceso

Routing and Switching Essentials v6.0

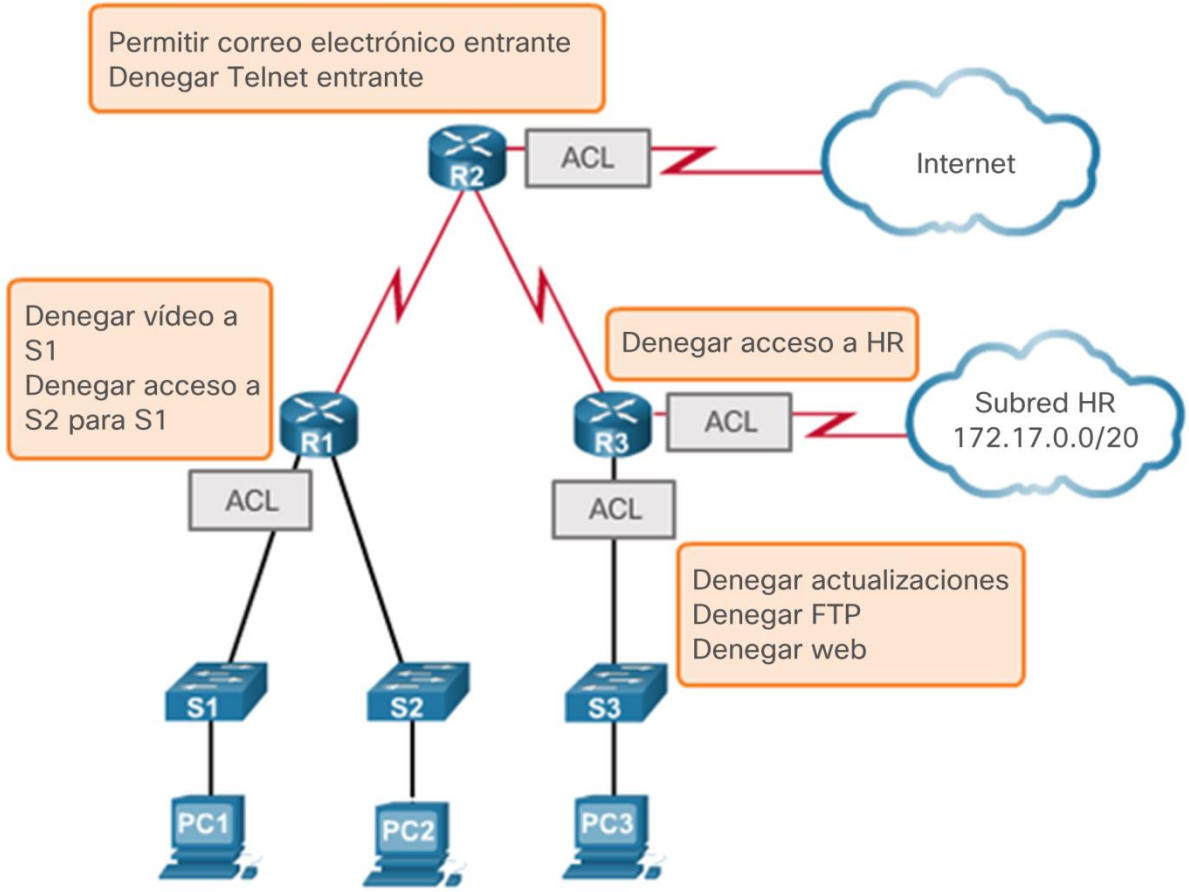
Cisco | Networking Academy®
Mind Wide Open™

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.

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

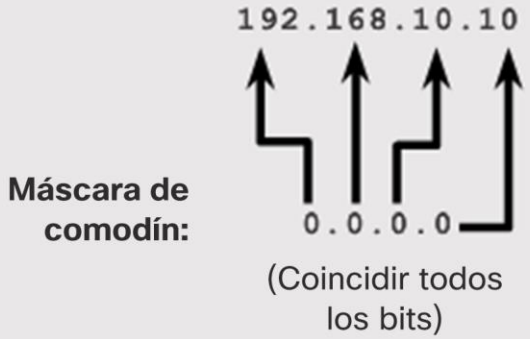
	255.255.255.255
-	255.255.252.000
	000.000.003.255

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**.

Máscaras de comodín en listas ACL

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
```

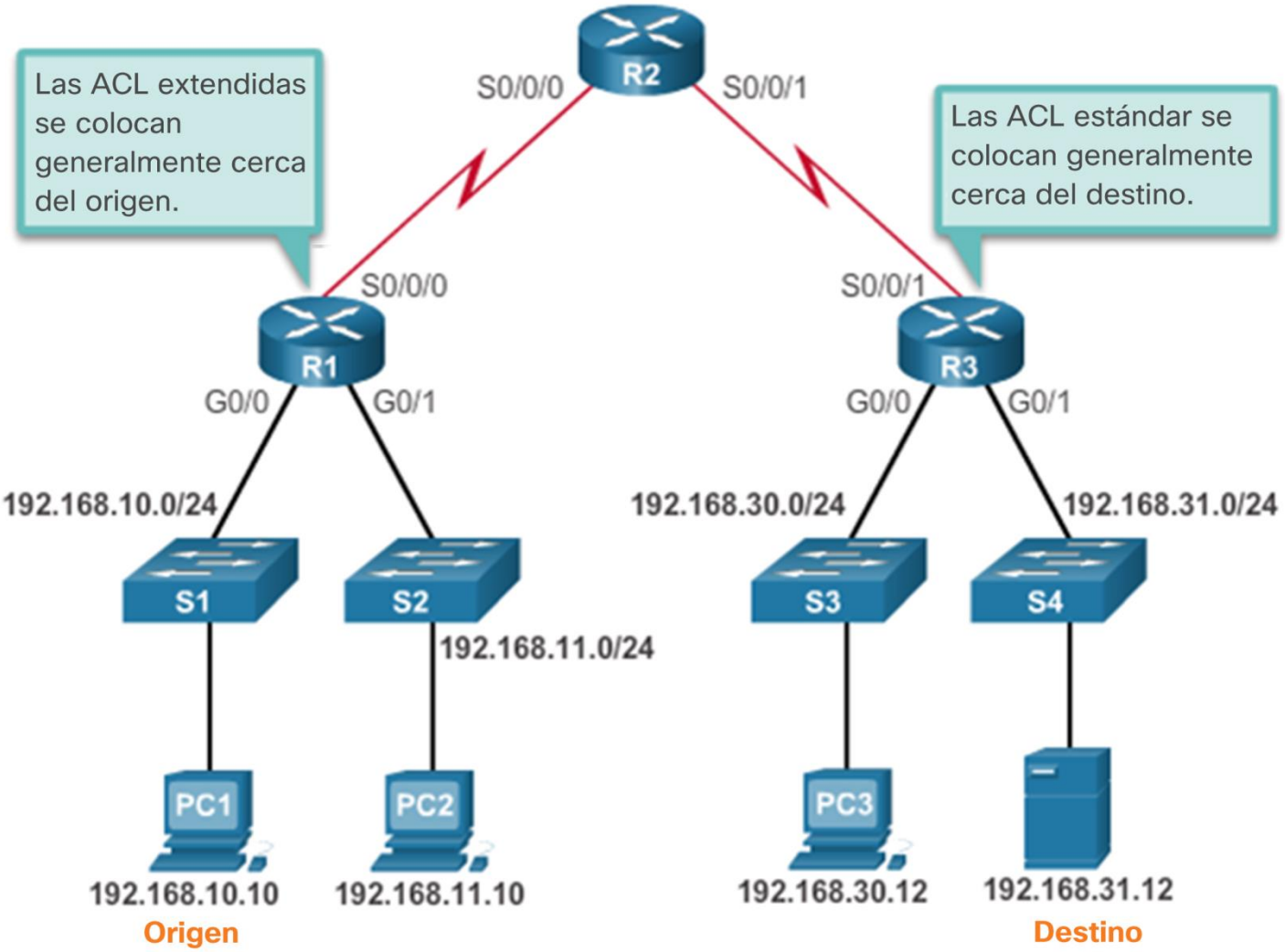
Ejemplo 2:

```
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 para la ubicación de listas ACL

¿Dónde ubicar las listas ACL?

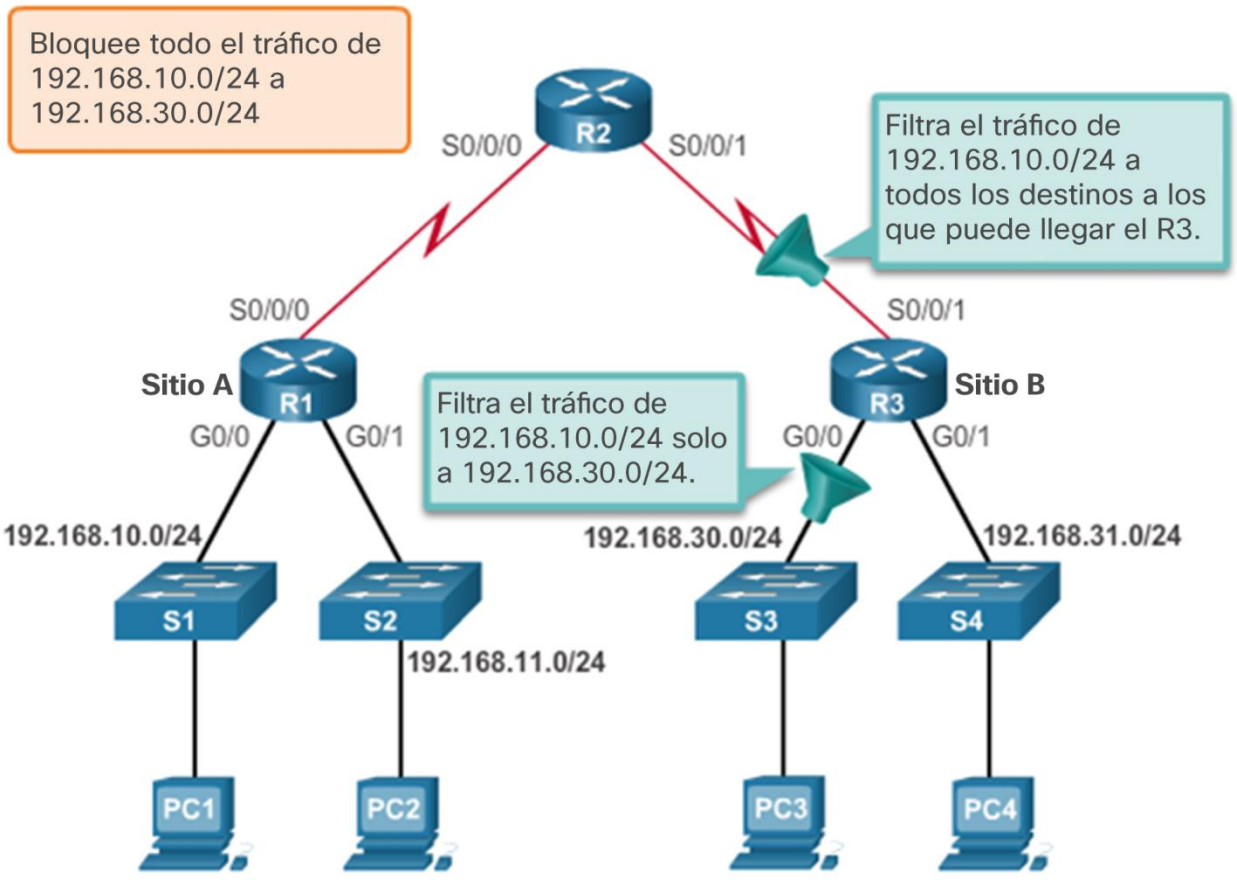


¿Dónde ubicar las listas ACL? (continuación)

- 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 estándar:** Debido a que en las listas ACL estándares no se especifican las direcciones de destino, colóquelas **tan cerca del destino como sea posible**.

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™

Configurar listas ACL de IPv4 estándares

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#
```

Un **access list remark** es un comentario opcional que se coloca antes o después de una lista de acceso, que describe la ACL. Cada comentario tiene un límite de 100 caracteres.

```
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 instrucción 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
```

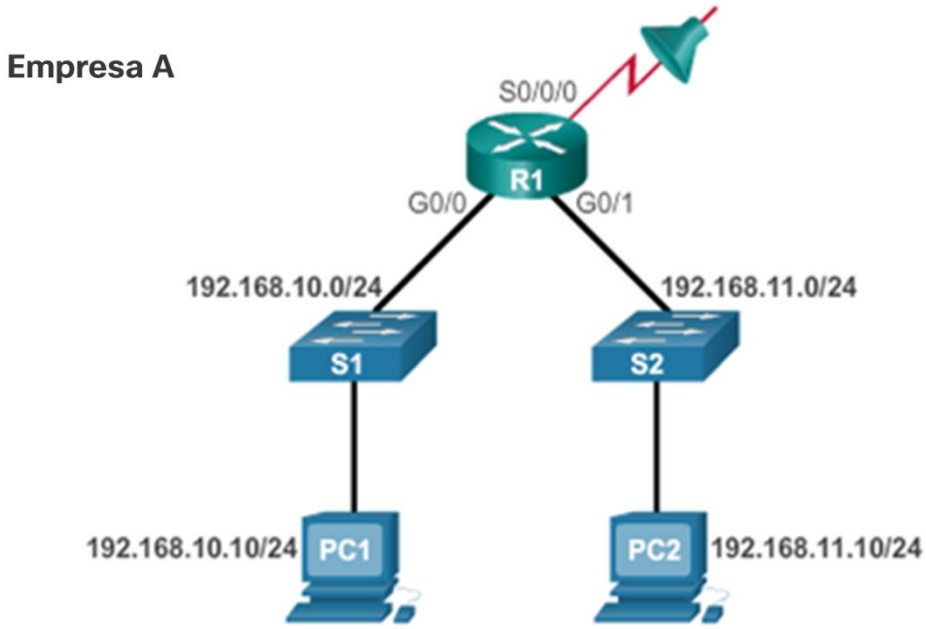
Paso 3: Utilice el comando de configuración de interfaz **ip access-group** para activar la ACL actual en una interfaz.

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

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

Aplicar listas ACL de IPv4 estándares a las interfaces

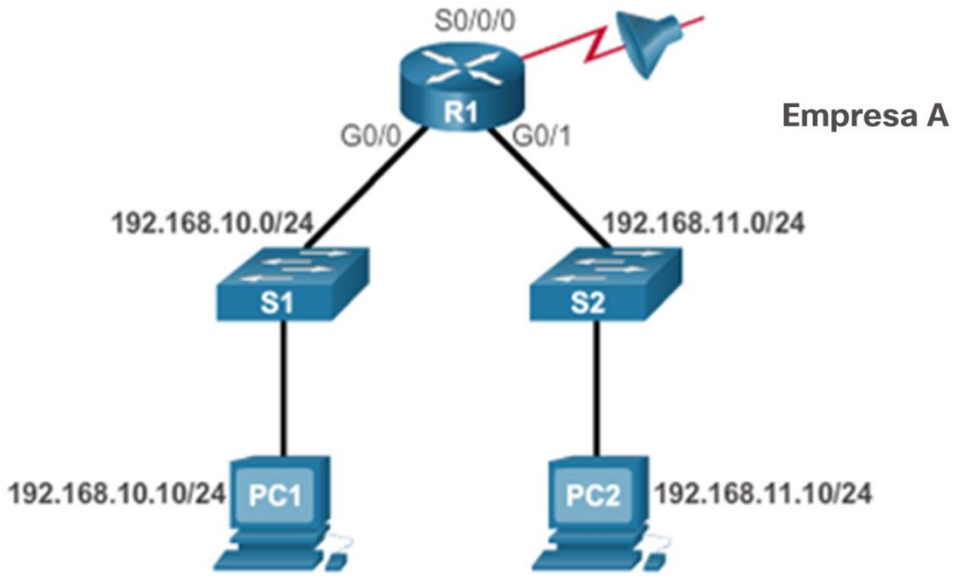
Admisión de una subred específica




```
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

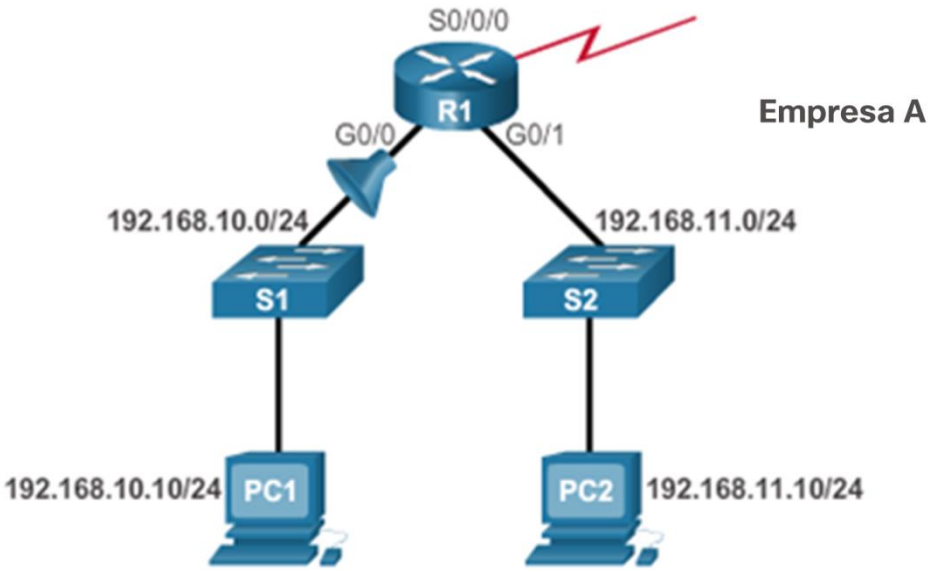
Denegación de un host específico y admisión de una subred específica




```
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

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
```

Configurar listas ACL de IPv4 estándares

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]
```

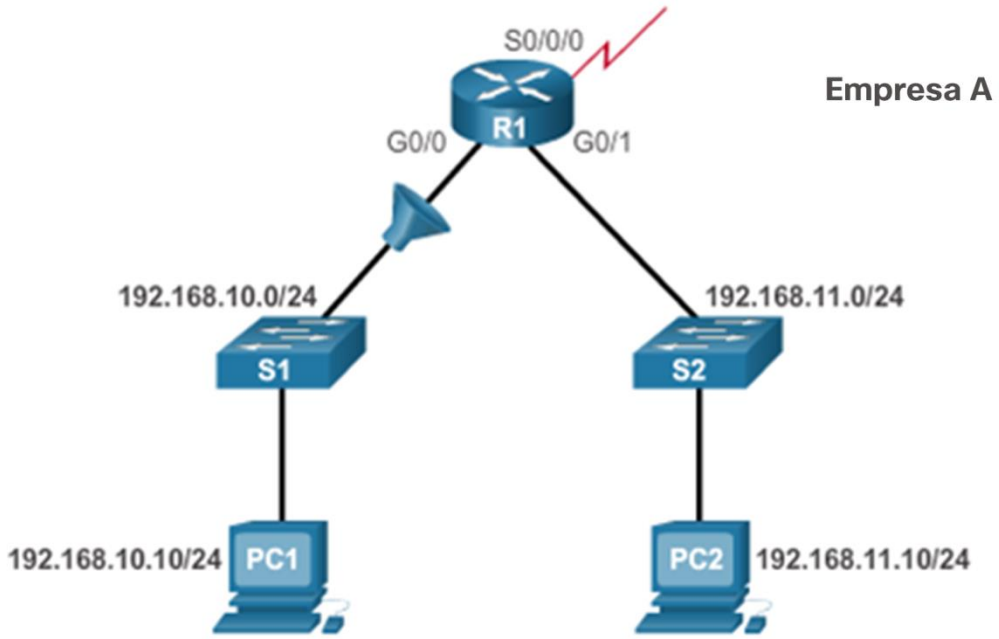
```
Router(config-if)# ip access-group name [in | out]
```

Activa la ACL IP denominada en una interfaz.

Configurar listas ACL de IPv4 estándares

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

Ejemplo de ACL denominada




```
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
```

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 *sequence-number* named-ACL 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>
```

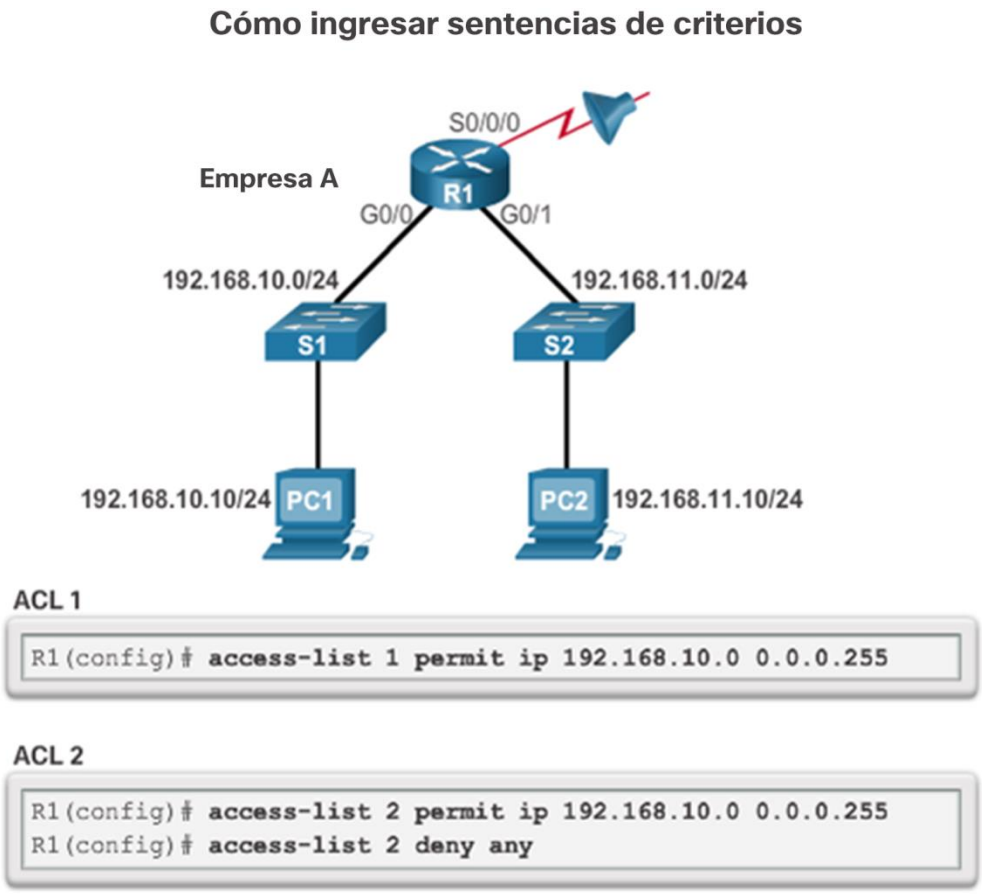
```
R1# show access-lists
Standard IP access list 1
    10 deny   192.168.10.10
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
    15 deny   192.168.11.11
    10 deny   192.168.11.10
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

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 entradas de control de acceso (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 entradas de control de acceso (ACE) en una ACL

```
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.