Listas de control de acceso

RAUL BAREÑO GUTIERREZ

Cisco | Networking Academy®
Mind Wide Open™

Objetivos

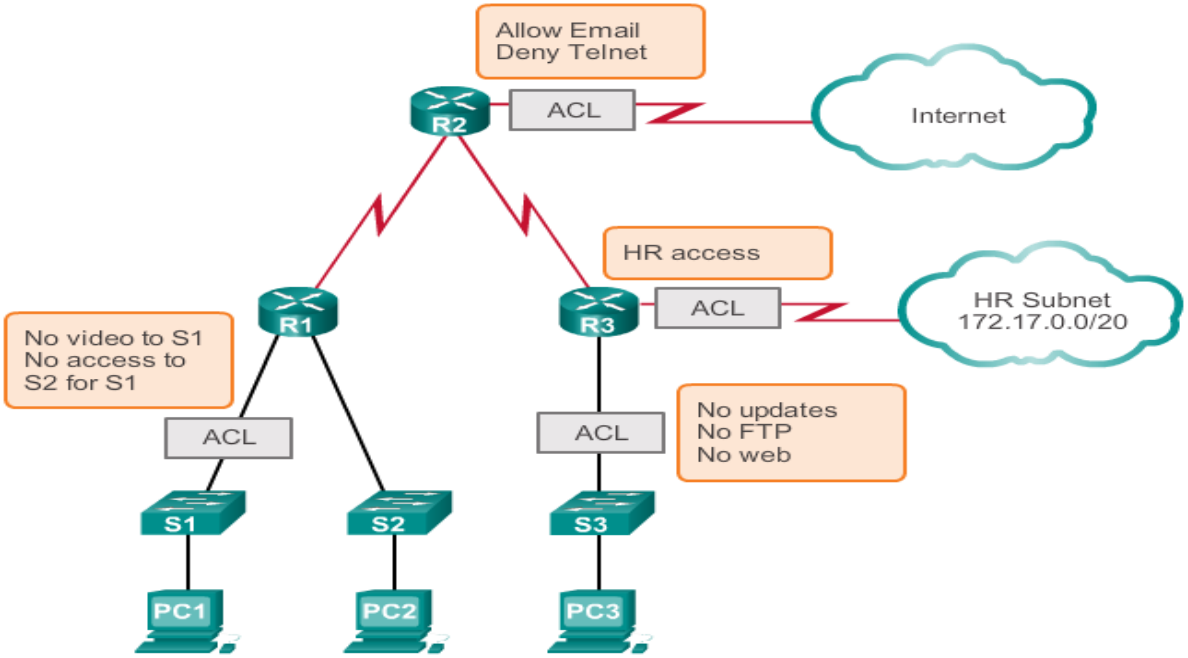
- Explicar cómo se usan las ACL para filtrar el tráfico.
- Comparar las ACL en IPv4 estándar y extendida.
- Explicar cómo las ACL usan máscaras wildcard.
- Explicar las directrices para la creación de ACL.
- Explicar las directrices para la ubicación de las ACL.
- Configurar ACL estándar en IPv4 para filtrar el tráfico.
- Modificar una IPv4 ACL estándar nombrada utilizando los números de secuencia.
- Configurar una ACL estándar para asegurar el acceso vty.

Objetivos

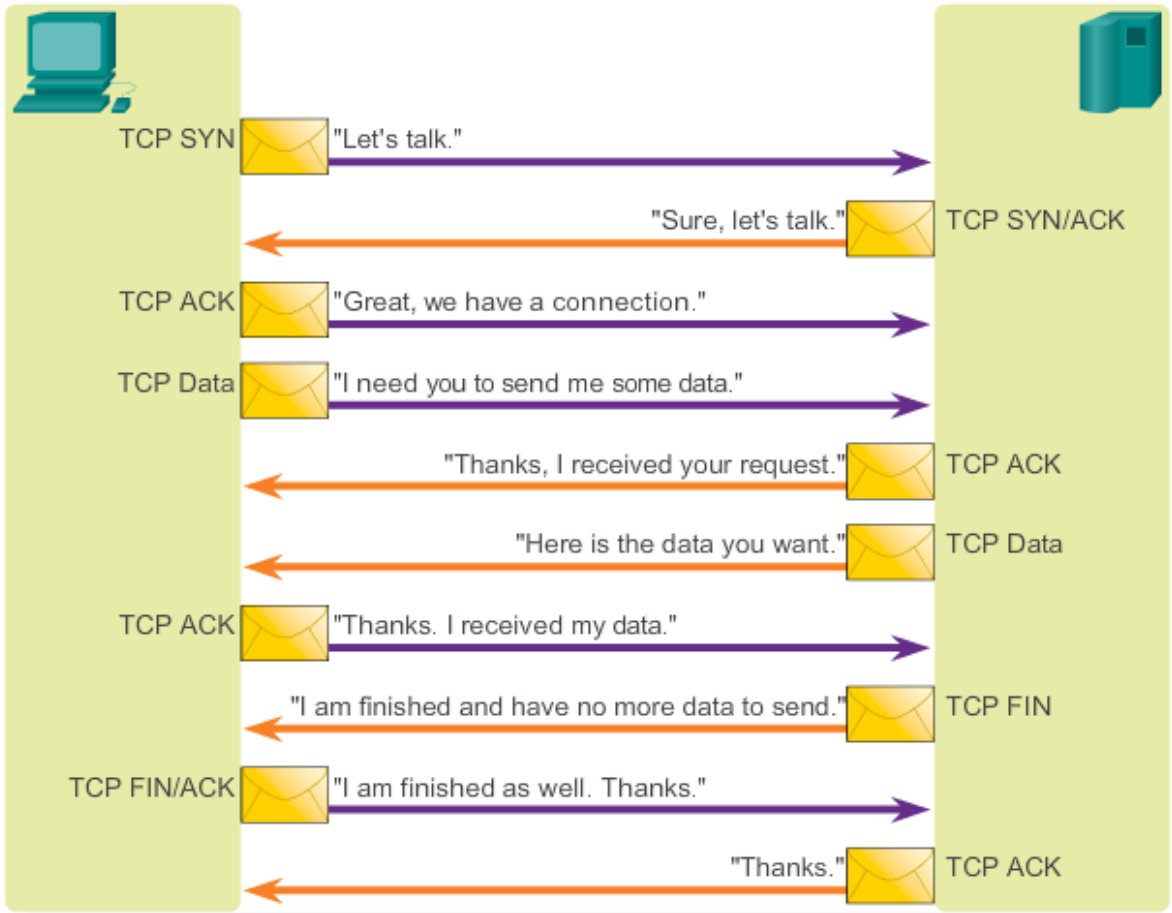
- Configurar una ACL extendida IPv4 para filtrar el tráfico de acuerdo a las necesidades de red.
- Explique cómo un router procesa paquetes cuando se aplica una ACL.
- Comparar la creación ACL IPv4 e IPv6.
- Configurar ACL IPv6 para filtrar el tráfico de acuerdo a las necesidades de red.

¿Qué es una ACL?

Una ACL es una lista secuencial que permite o niega las declaraciones, conocidas según las sentencias de la lista de control de acceso (ACE).



Una conversación TCP



Filtrado de paquetes

- Filtrado de paquetes estático, controla el acceso a una red mediante el análisis de los paquetes entrantes y salientes pasando o dejándolos caer sobre la base de los criterios dados, tales como la IP de origen, o destino y el protocolo realizado dentro del paquete.

- Un router actúa como un filtro de paquetes para enviar o denegar paquetes de acuerdo con las reglas de filtrado.

ACL Operación

An inbound ACL filters packets coming into a specific interface and before they are routed to the outbound interface.

An outbound ACL filters packets after being routed, regardless of the inbound interface.

La última declaración de una ACL es siempre una negación implícita. Se inserta automáticamente al final de cada ACL a pesar de que no está presente físicamente. Por ello una ACL debe contener una declaración de permiso o bloqueará todo el tráfico.

Tipos de ACL Cisco en IPv4

ACL estándar

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

Standard ACLs filter IP packets based on the source address only.

ACL extendidas

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

Extended ACLs filter IP packets based on several attributes, including the following:

- Source and destination IP addresses
- Source and destination TCP and UDP ports
- Protocol type/ Protocol number (example: IP, ICP, UDP, TCP, etc.)

Numeradas y nombradas de las ACL

Numbered ACL:

You assign a number based on which protocol you want filtered:

- (1 to 99) and (1300 and 1999): Standard IP ACL
- (100 to 199) and (2000 to 2699): Extended IP ACL

Named ACL:

You assign a name by providing the name of the ACL:

- Names can contain alphanumeric characters.
- It is suggested that the name be written in CAPITAL LETTERS.
- Names cannot contain spaces or punctuation.
- You can add or delete entries within the ACL.

Introducción de mascaras wildcard en las ACL

Las máscaras wildcard y máscaras de subred se diferencian en la forma en que coinciden con 1s y 0s binarios.

Las máscaras wildcard usan las siguientes reglas para que coincida con 1s y 0s binarios:

Máscara wildcard bits – validan el valor del bit 0.

Bit de máscara wildcard - Ignoran el valor del bit 1.

Máscaras wildcard se refieren a menudo como una máscara inversa.

Ejemplos máscara wildcard: rangos de coincidencia

Example 1

	Decimal	Binary
IP Address	192.168.16.0	11000000.10101000.00010000.00000000
Wildcard Mask	0.0.15.255	00000000.00000000.00001111.11111111
Result Range	192.168.16.0 to 192.168.31.255	11000000.10101000.00010000.00000000 to 11000000.10101000.00011111.11111111

Example 2

	Decimal	Binary
IP Address	192.168.1.0	11000000.10101000.00000001.00000000
Wildcard Mask	0.0.254.255	00000000.00000000.11111110.11111111
Result	192.168.1.0	11000000.10101000.00000001.00000000
	All odd numbered subnets in the 192.168.0.0 major network	

Cálculando la máscara wildcard

Uno de los métodos de acceso directo es restar la máscara de subred de 255.255.255.255.

Example 1

	255.255.255.255
–	255.255.255.000
	000.000.000.255

Example 2

	255.255.255.255
–	255.255.255.240
	000.000.000.015

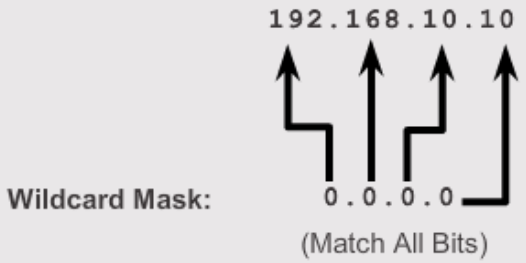
Example 3

	255.255.255.255
–	255.255.252.000
	000.000.003.255

Palabras clave de la Mascara wildcard

Example 1

- 192.168.10.10 0.0.0.0 matches all of the address bits
- Abbreviate this wildcard mask using the IP address preceded by the keyword **`host`** (**`host 192.168.10.10`**)



Example 2

- 0.0.0.0 255.255.255.255 ignores all address bits
- Abbreviate expression with the keyword **`any`**

Ejemplos de Palabras clave de la Mascara wildcard

Example 1:

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

Example 2:

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

Directrices generales para la Creación de las ACL

- Utilice una ACL en los routers firewall situados entre la red interna y una red externa, como Internet.
- Utilice una ACL en un router situado entre dos partes de su red para controlar el tráfico que entra o sale de una parte específica de su red interna.
- Configure las ACL en los routers de frontera, es decir routers situados en los bordes de sus redes.
- Configure las ACL para cada protocolo de red configurado en las interfaces del router de frontera.

Directrices generales para la Creación de las ACL

Las Tres P

- **Una ACL por protocolo** - una ACL se debe definir para cada protocolo habilitado en la interfaz.
- **Una ACL por sentido** - ACL controlan el tráfico en una sola dirección a la vez en una interfaz. Dos ACL independientes deben crearse para controlar el tráfico entrante y saliente.
- **Una ACL por interfaz** - ACL controlan el tráfico de una interfaz, por ejemplo, GigabitEthernet 0/0.

Mejores Prácticas de las ACL

Guideline	Benefit
Base your ACLs on the security policy of the organization.	This will ensure you implement organizational security guidelines.
Prepare a description of what you want your ACLs to do.	This will help you avoid inadvertently creating potential access problems.
Use a text editor to create, edit and save ACLs.	This will help you create a library of reusable ACLs.
Test your ACLs on a development network before implementing them on a production network.	This will help you avoid costly errors.

Dónde colocar las ACL

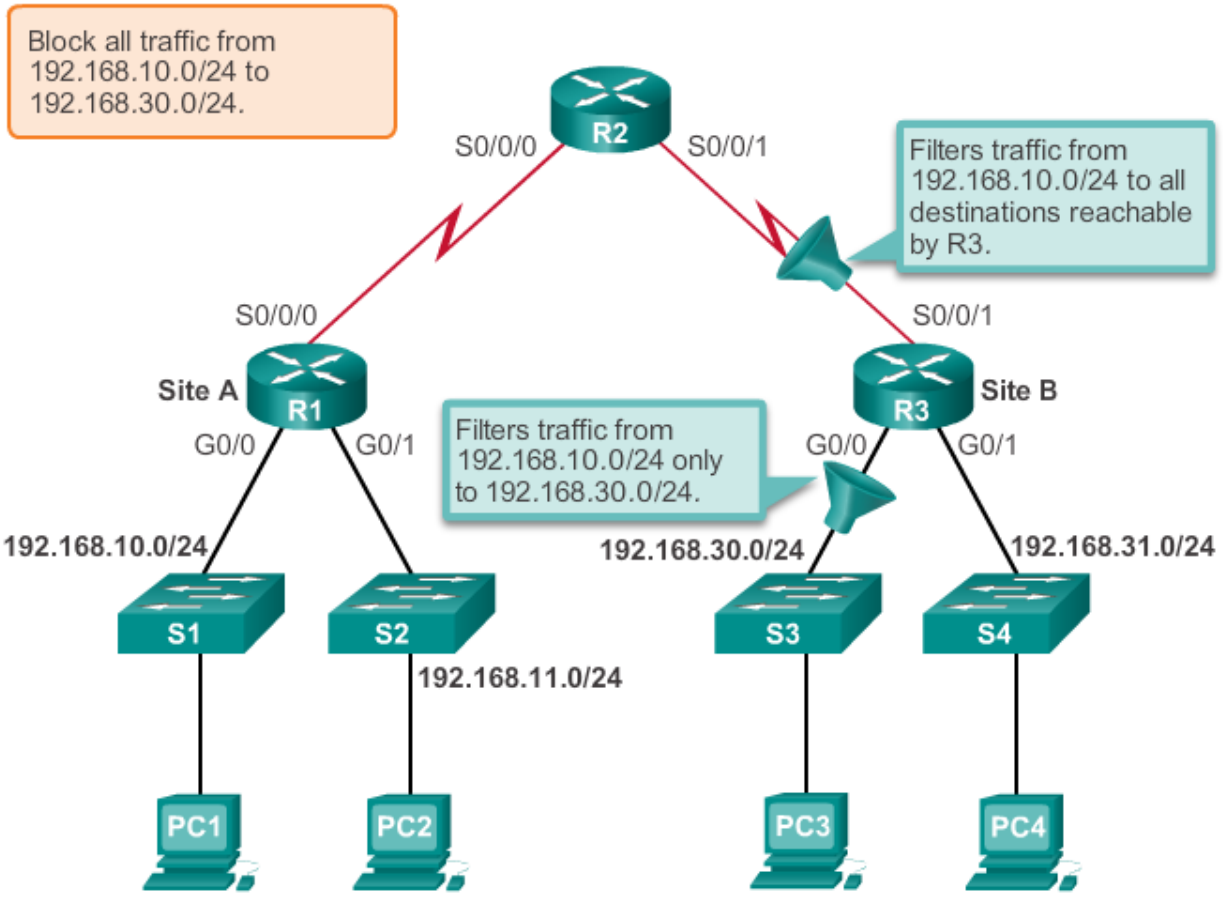
Las reglas básicas son:

ACL extendidas: colóquela lo más cerca posible del origen del tráfico a filtrar.

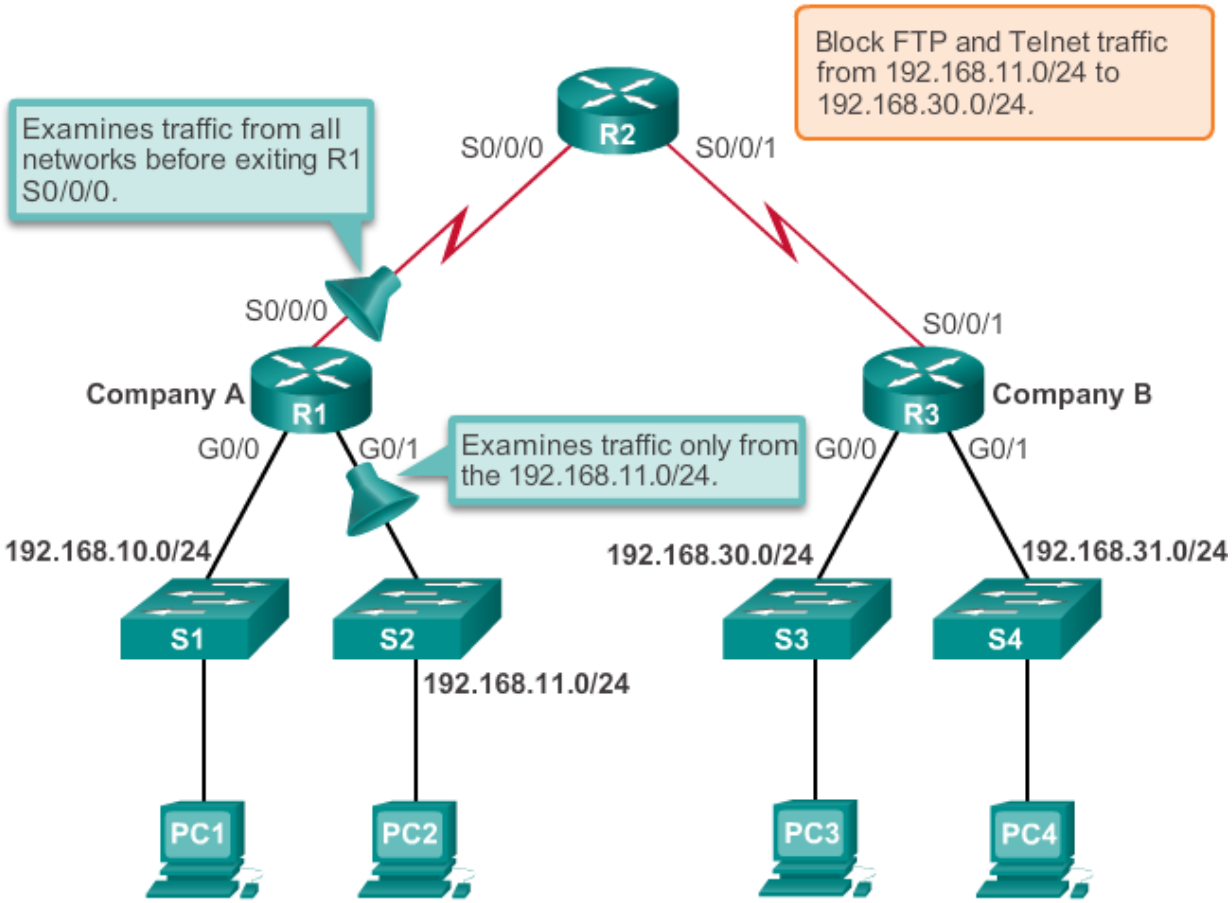
ACL estándar: colóquela lo más cerca posible del destino.

La colocación de la ACL y por lo tanto el tipo de ACL utilizado también pueden depender de: el grado de control del administrador de red, ancho de banda de las redes involucradas, y la facilidad de configuración.

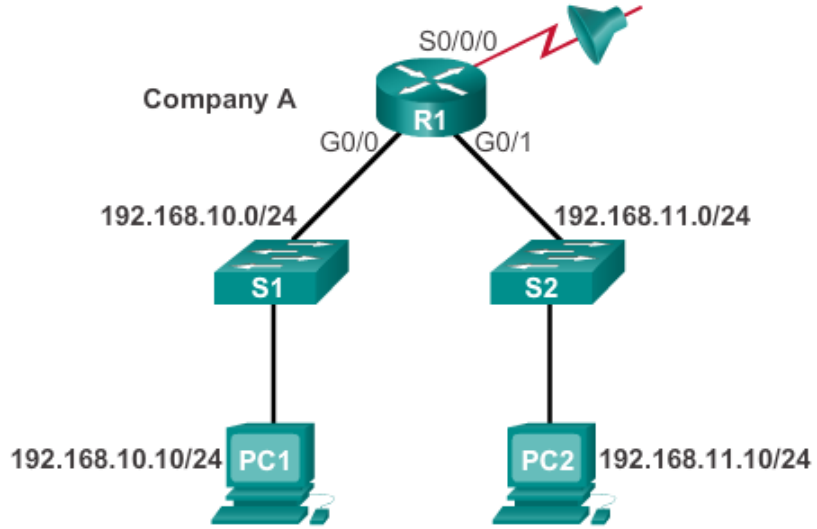
Colocación ACL estándar



Colocación de la ACL extendida



Introducir instrucciones o Criterios



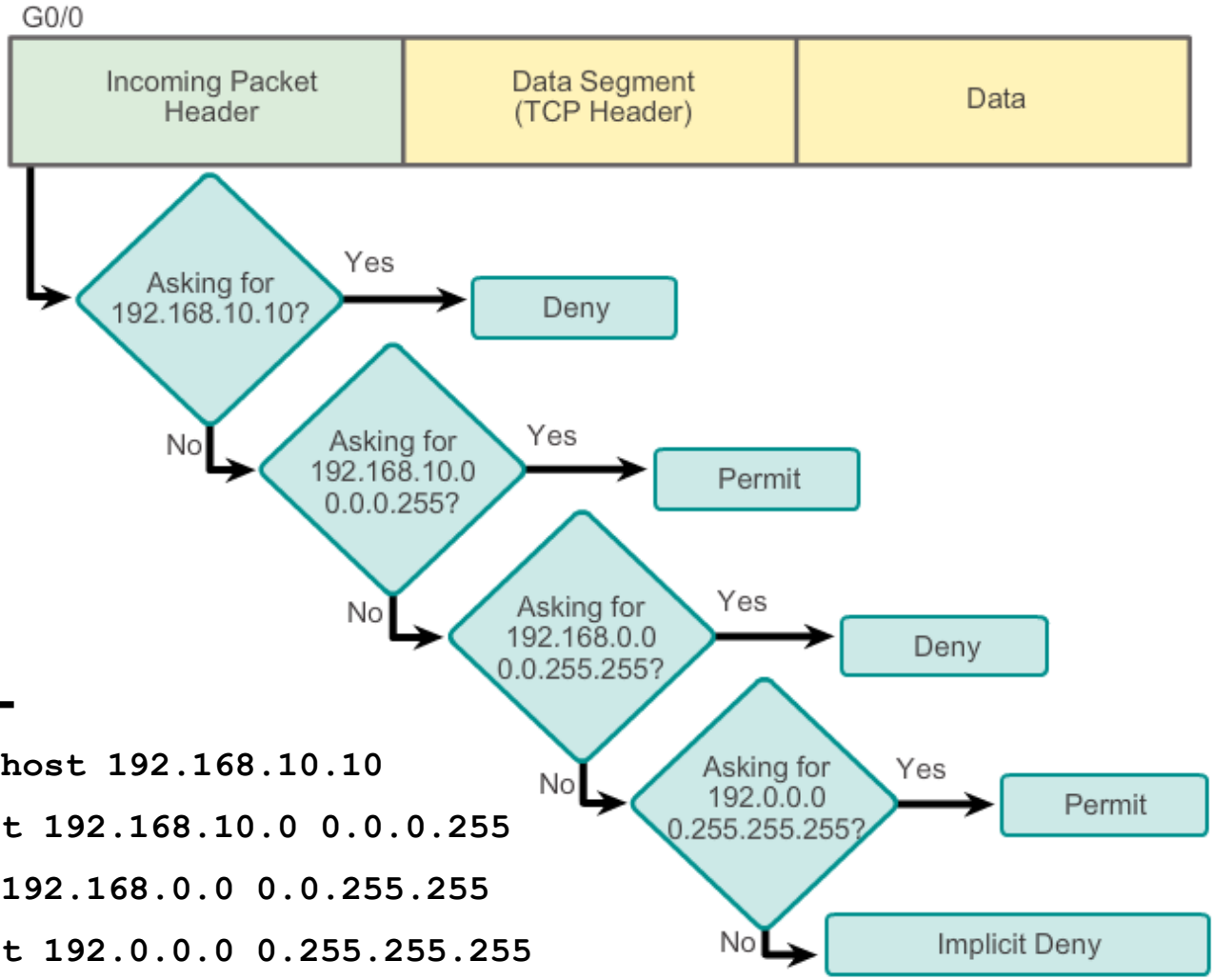
ACL 1

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

ACL 2

```
R1(config)#access-list 2 permit ip 192.168.10.0 0.0.0.255
R1(config)#access-list 2 deny any
```

Configurar una ACL estándar



Ejemplo de ACL

- `access-list 2 deny host 192.168.10.10`
- `access-list 2 permit 192.168.10.0 0.0.0.255`
- `access-list 2 deny 192.168.0.0 0.0.255.255`
- `access-list 2 permit 192.0.0.0 0.255.255.255`

Configurar una ACL estándar

Router(config)# **access-list** *access-list-number* **deny permit remark** *source* [*source-wildcard*] [**log**]

Para eliminar la ACL, desde modo de configuración global se utiliza ningún no access-list.

La palabra clave remark se utiliza para la documentación y hace que las ACL más fácil de entender.

lógica interna

- Cisco IOS aplica una lógica interna al aceptar y procesar las declaraciones de la ACL.
- Las declaraciones de la ACL se procesan de forma secuencial. el orden en que se introducen declaraciones es importante.

```
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: Host statement conflicts with previous range statement.

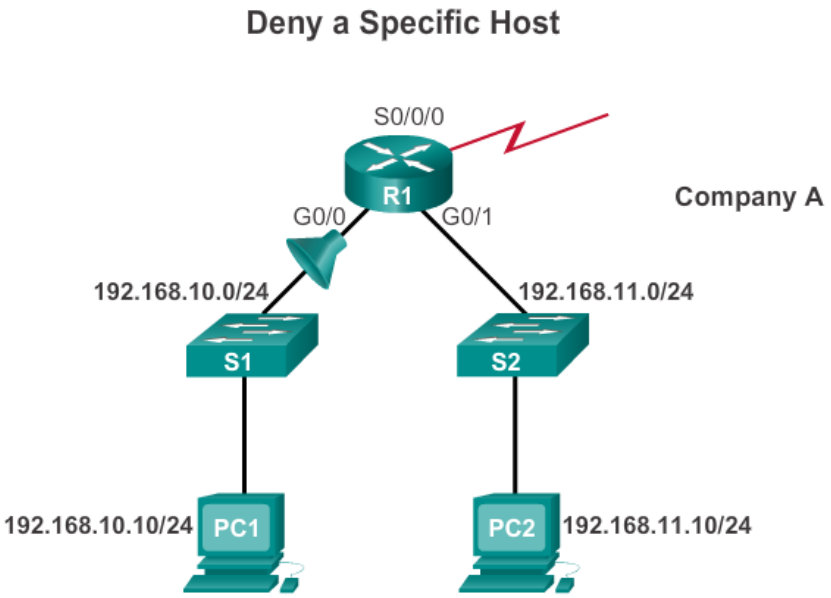
Aplicando las ACL estándar en las interfaces

Después de configurar una ACL, se debe vincular a una interfaz con ip access-group:

- `Router(config-if)#` **`ip access-group`** { *`access-list-number`* | *`access-list-name`* } { **`in`** | **`out`** }

Para eliminar una ACL de una interfaz, primero introduzca el comando no IP access-group en la interfaz, y luego desde modo global no access-list para eliminar toda la ACL.

Aplicando las ACL estándar en las interfaces




```
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
```

Creación de las ACL estándar nombrada

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

Alphanumeric name string must be unique and cannot begin with a number.

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

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

Activates the named IP ACL on an inteface.

comentando las ACL

Example 1: Commenting a numbered ACL

```
R1(config)#access-list 1 remark Do not allow Guest workstation
through
R1(config)#access-list 1 deny host 192.168.10.10
R1(config)#access-list 1 remark Allow devices from all other
192.168.x.x subnets
R1(config)#access-list 1 permit 192.168.0.0 0.0.255.255
R1(config)#interface s0/0/0
R1(config-if)#ip access-group 1 out
R1(config-if)#
```

Example 2: Commenting a named ACL

```
R1(config)#ip access-list standard NO_ACCESS
R1(config-std-nacl)#remark Do not allow access from Lab
workstation
R1(config-std-nacl)#deny host 192.168.11.10
R1(config-std-nacl)#remark Allow access from all other networks
R1(config-std-nacl)#permit any
R1(config-std-nacl)#interface G0/0
R1(config-if)#ip access-group NO_ACCESS out
R1(config-if)#
```

Edición estándar de las ACL numeradas

Editing Numbered ACLs Using a Text Editor

Configuration

```
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
```

Step 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
```

Step 2

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

Step 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
```

Step 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
```

Edición estándar de las ACL nombradas

Editing Numbered ACLs Using Sequence Numbers

Configuration

```
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
```

Step 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#
```

Step 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#
```

Step 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#
```

Editando las ACL nombradas estándar

Adding a Line to a Named ACL

```
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#
```

Note: The **no sequence-number** named-ACL command is used to delete individual statements.

Verificando 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
<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#
```

Estadísticas de las 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#
```

Output after pinging PC3 from PC1.

Matches have been incremented.

```
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#
```

Números de secuencia estándar ACL

- Las declaraciones deben negar los host y se configuran primero seguidos por las redes. Los hosts son válidados primero debido a que sus direcciones IP no son parte de los estados de rango previamente introducidos.
- Los host locales aparecen en primer lugar por el comando show, pero no necesariamente en el orden en que se introdujeron. El IOS pone la sentencia de host en un orden mediante una función especial de hash. El orden resultante optimiza la búsqueda de una entrada de ACL

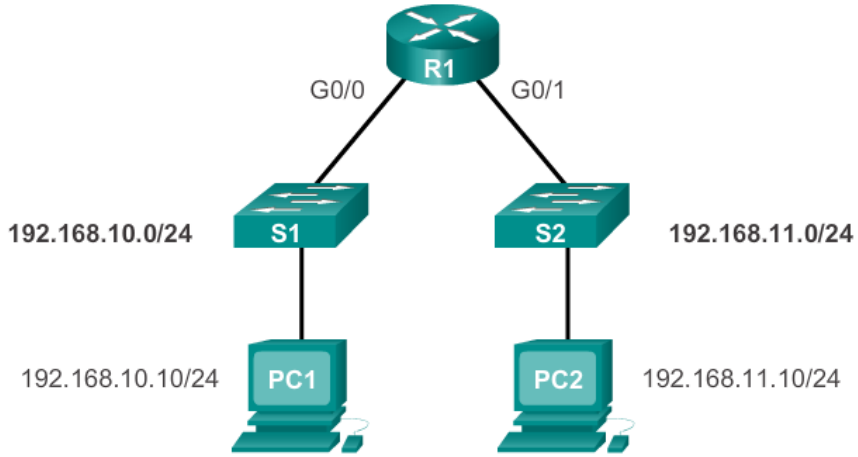
Configurar una ACL estándar para Asegurar un puerto VTY

Filtrado del tráfico de Telnet o SSH se considera normalmente una función ACL IP extendida porque filtra un protocolo de nivel superior. Sin embargo, debido a que el comando **access-class** se utiliza para filtrar las sesiones de Telnet / SSH por la dirección de origen, una ACL estándar se puede utilizar.

- `Router(config-line)# **access-class** *access-list-number* { **in** [ **vrf-also** ] | **out** }`
- Sobre las terminales virtuales (config)#line vty 0 4
- (config-line)#access-class <# lista>
- Ejemplo: (config-line)#access-class 10 in

Verificación de una ACL estándar utilizado para asegurar un Puerto VTY

```
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>
```

ACL extendidas

Extended ACLs can filter on:

- Source address
- Destination address
- Protocol
- Port numbers

ACL extendidas

Using Port Numbers

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 23
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20
```

Using Keywords

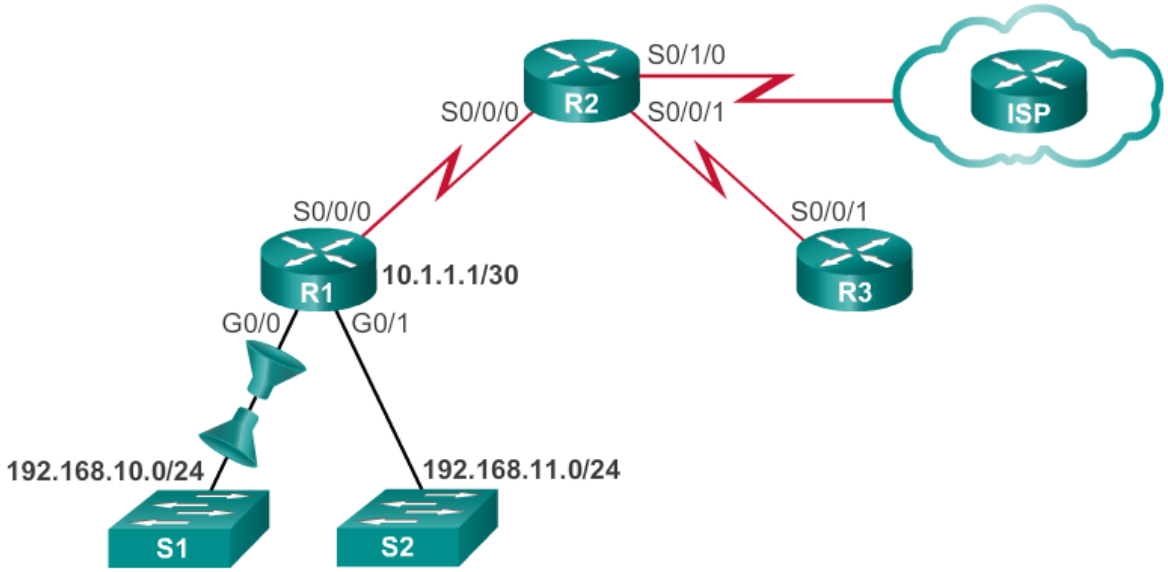
```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data
```

Configuración de las ACL extendidas

Los pasos o procedimientos para la configuración de ACL extendidas son las mismas que para las ACL estándar.

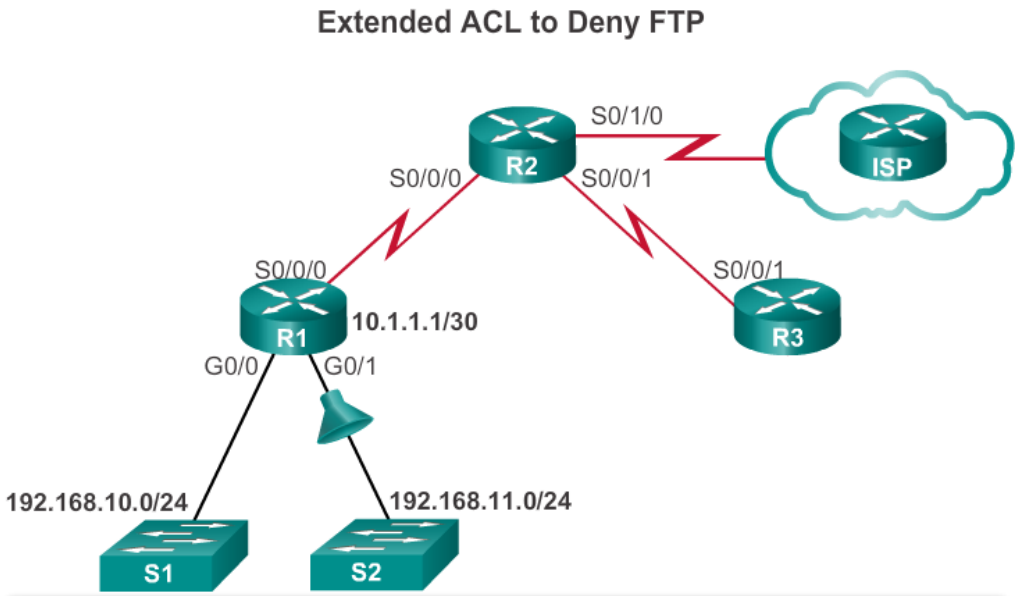
La extendida se configura primero, y posteriormente se activa en una interfaz. Sin embargo, la sintaxis de comandos y los parámetros son más complejos para admitir las características adicionales proporcionadas por ACL extendidas.

La aplicación de las ACL extendidas en las Interfaces



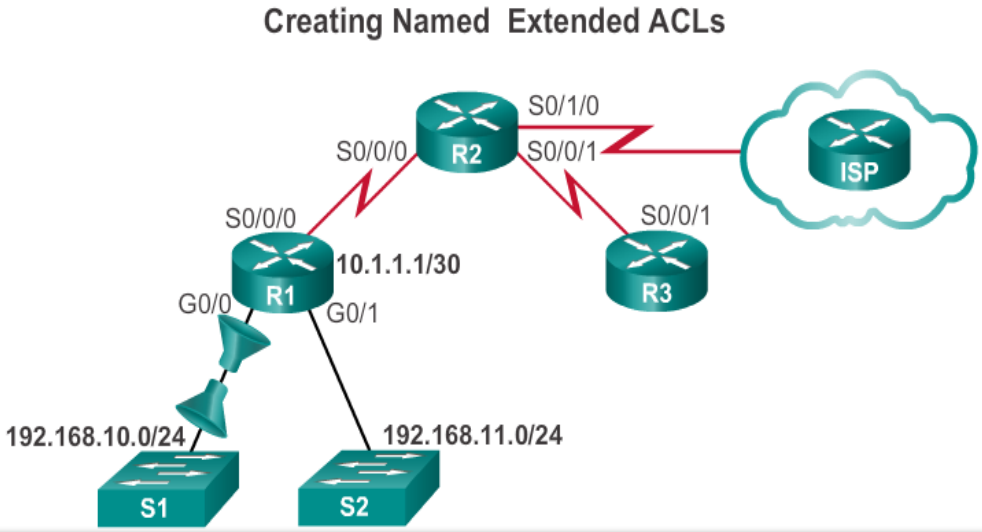

```
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)#access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established
R1(config)#interface g0/0
R1(config-if)#ip access-group 103 in
R1(config-if)#ip access-group 104 out
```

Filtrado de tráfico con ACL extendidas




```
R1(config)#access-list 101 deny tcp 192.168.11.0 0.0.0.255 192.168.10.0
0.0.0.255 eq ftp
R1(config)#access-list 101 deny tcp 192.168.11.0 0.0.0.255 192.168.10.0
0.0.0.255 eq ftp-data
R1(config)#access-list 101 permit ip any any
R1(config)#interface g0/1
R1(config-if)#ip access-group 101 in
```

Creación de las ACL extendidas nombradas




```
R1(config)#ip access-list extended SURFING
R1(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config-ext-nacl)#exit
R1(config)#ip access-list extended BROWSING
R1(config-ext-nacl)#permit tcp any 192.168.10.0 0.0.0.255 established
R1(config-ext-nacl)#exit
R1(config)#interface g0/0
R1(config-if)#ip access-group SURFING in
R1(config-if)#ip access-group BROWSING out
```

Verificación de las ACL extendidas

```
R1#show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
R1#show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
<output omitted for brevity>
  Outgoing access list is BROWSING
  Inbound  access list is SURFING
<output omitted for brevity>
```

Editar las ACL extendidas

Se puede lograr usando el mismo proceso que la edición de un estándar. Una ACL extendida puede ser modificado usando:

Método 1 - Editor de texto

Método 2 - Los números de secuencia

Lógica de la ACL entrando

- Los paquetes son testeados en la ACL entrante, si es que existe, **antes de ser enrutados**.
- Si un paquete entrante coincide con una sentencia ACL con permiso, se envía para ser enrutado.
- Si un paquete entrante coincide con una sentencia ACL con negar, se eliminan y no se enrutan.
- Si un paquete entrante no cumple ninguna de las declaraciones de ACL, entonces es "implícitamente denegado" y eliminan y no son enrutados

Lógica de la ACL saliendo

- **Los paquetes se comprueban primero para una ruta antes de ser enviado a una interfaz de salida.** Si no hay ninguna ruta, los paquetes son descartados.
- Si una interfaz de salida no tiene una ACL, a continuación, los paquetes se envían directamente a esa interfaz.
- Si hay una ACL en la interfaz de salida, se prueba antes de ser enviado a esa interfaz.
- Si un paquete de salida coincide con una sentencia ACL con un permiso, se envía a la interfaz.
- Si un paquete de salida coincide con una sentencia ACL con negar, se eliminan.
- Si un paquete de salida no se ajusta a ninguna de las declaraciones de ACL, entonces los elimina

Proceso de decisión de la ACL estándar

- **Sólo examinan la dirección IPv4 de origen**. El destino y los puertos implicados no son considerados.

- Se testea las direcciones contra las condiciones en la ACL una por una.

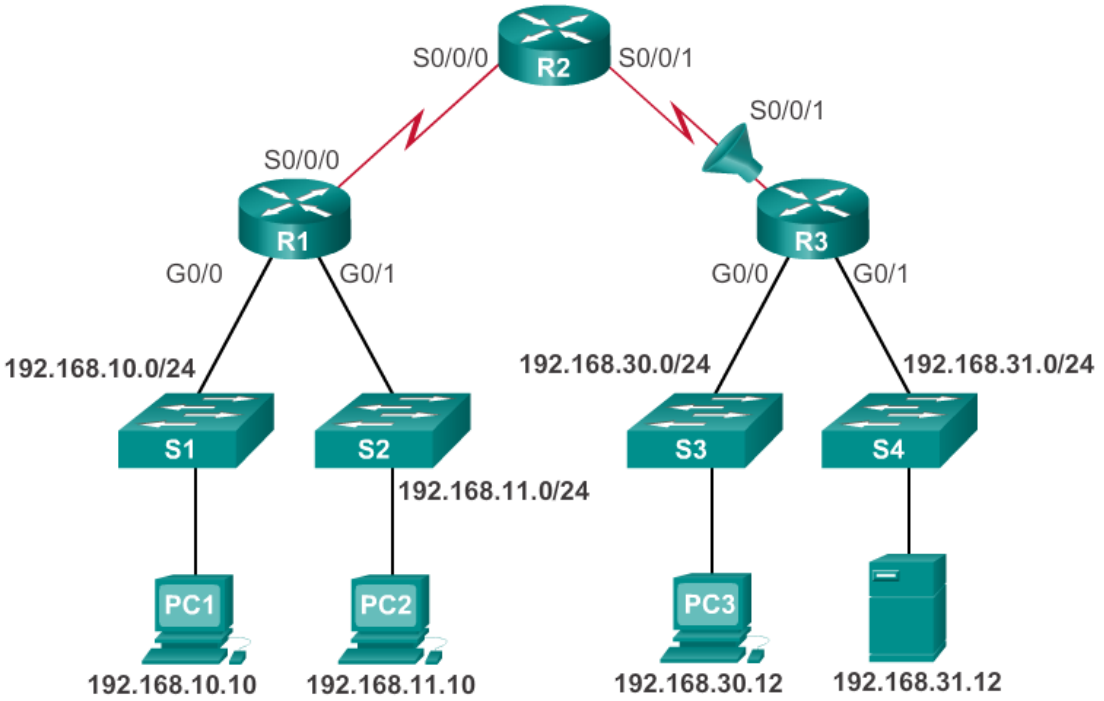
- Si no hay condiciones de coincidencia la dirección y los paquetes son rechazados.

Proceso de decisión de la ACL extendida

- La ACL filtra primero en la dirección de origen,
- luego el puerto y el protocolo de origen.
- A continuación, se filtra en la dirección de destino,
- después el puerto y el protocolo del destino,
- y hace una revisión final de permiso o de rechazo.

Solución de problemas o errores comunes de ACL - Ejemplo 1

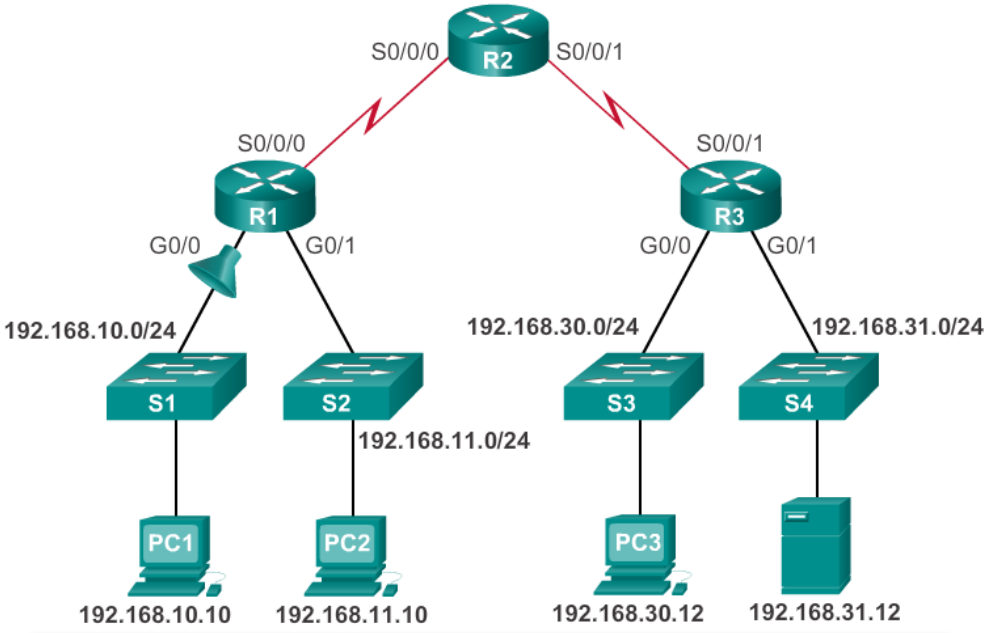
Host 192.168.10.10 no tiene conectividad con 192.168.30.12.




```
R3#show access-lists
Extended IP access list 110
    10 deny tcp 192.168.10.0 0.0.0.255 any (12 match(es))
    20 permit tcp 192.168.10.0 0.0.0.255 any eq telnet
    30 permit ip any any
```

Solución de problemas o errores comunes de ACL - Ejemplo 2

La red 192.168.10.0 / 24 no puede utilizar TFTP para conectarse a la red 192.168.30.0 / 24.

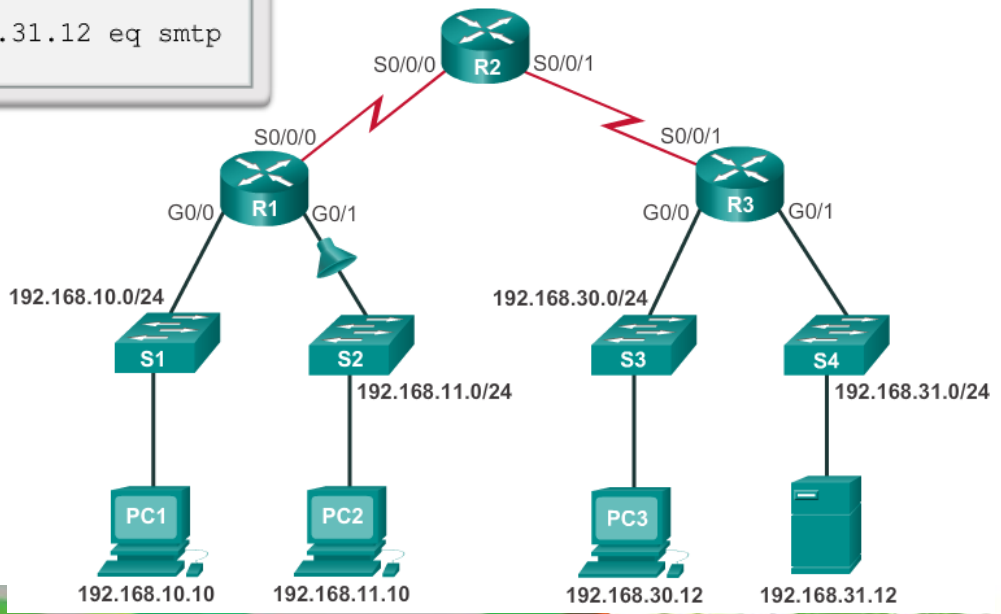



```
R1#show access-lists 120
Extended IP access list 120
    10 deny tcp 192.168.10.0 0.0.0.255 any eq telnet
    20 deny tcp 192.168.10.0 0.0.0.255 host 192.168.31.12 eq smtp
    30 permit tcp any any
```

Solución de problemas o errores comunes de ACL - Ejemplo 3

La red 192.168.11.0 / 24 puede usar Telnet para conectarse a 192.168.30.0 / 24, pero de acuerdo con la política de la empresa, esta conexión no debe ser permitido.

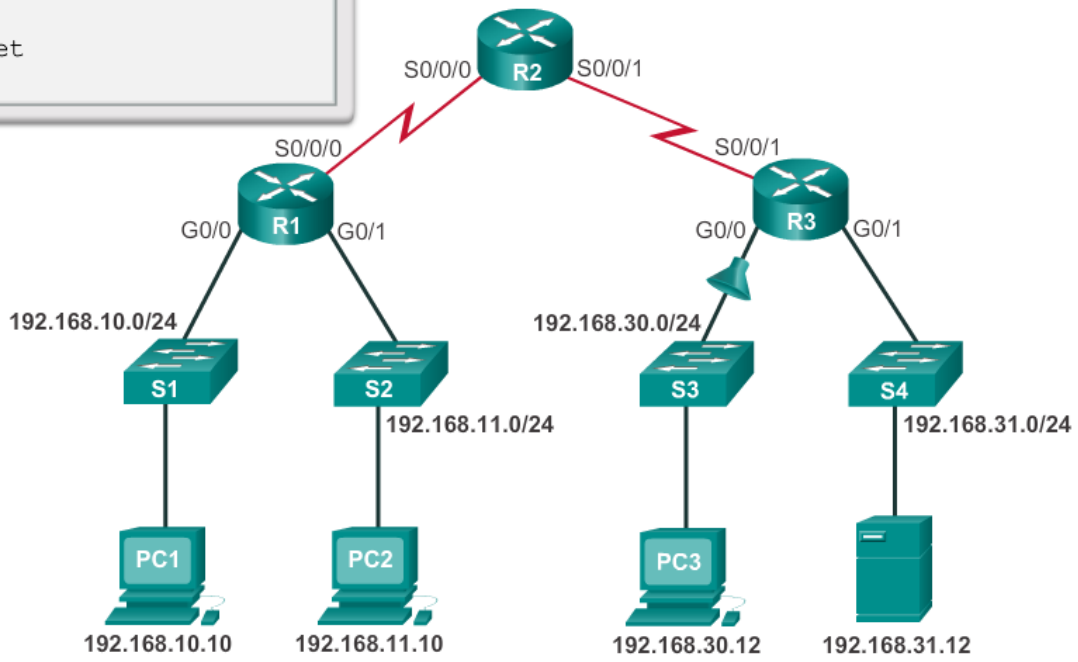
```
R1#show access-lists 130
Extended IP access list 130
    10 deny tcp any eq telnet any
    20 deny tcp 192.168.11.0 0.0.0.255 host 192.168.31.12 eq smtp
    30 permit tcp any any (12 match(es))
```



Solución de problemas o errores comunes de ACL - Ejemplo 4

El host 192.168.30.12 Hace Telnet para conectarse a 192.168.31.12, Pero la Política de la Compañía Afirma Que esta conexión No Se debe permitir.

```
R3#show access-lists 140
Extended IP access list 140
    10 deny tcp host 192.168.30.1 any eq telnet
    20 permit ip any any (5 match(es))
```



Tipos ACL en IPv6

IPv4 ACLs

- Standard
  - Numbered
  - Named
- Extended
  - Numbered
  - Named

IPv6 ACLs

- Named only
- Similar in functionality to IPv4 Extended ACL

Comparando ACL entre IPv4 e IPv6

Las ACL IPv4 e IPv6 son muy similares, existen tres diferencias.

- **La aplicación de una ACL en IPv6**

IPv6 utiliza el comando **`ipv6 traffic-filter`** para llevar a cabo la misma función para las interfaces de IPv6.

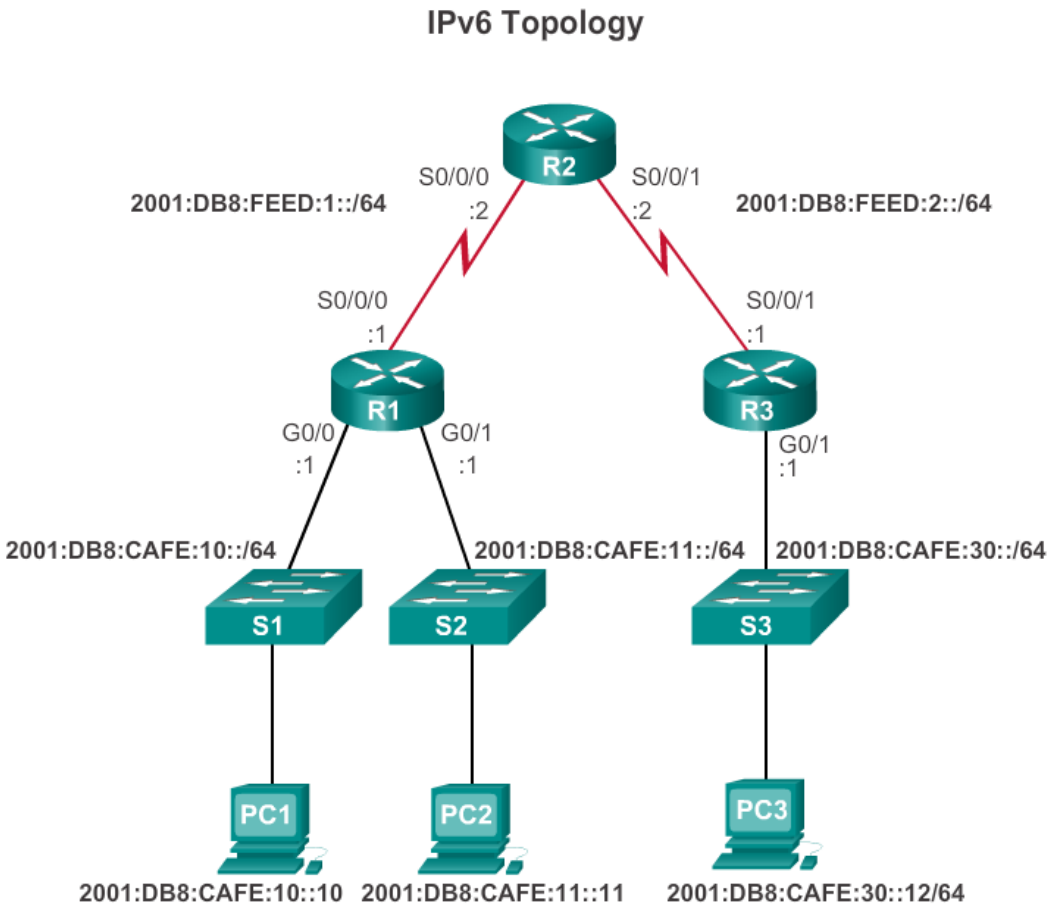
- **No hay máscaras wildcard**

El prefijo de longitud se utiliza para indicar la cantidad de la IPv6 de origen o de destino que debe concordar o debe ser evaluada.

- **Declaraciones adicionales por defecto.**

```
permit icmp any any nd-na
permit icmp any any nd-ns
```

Configuración de la Topologia IPv6



Configuración de la ACL en IPv6

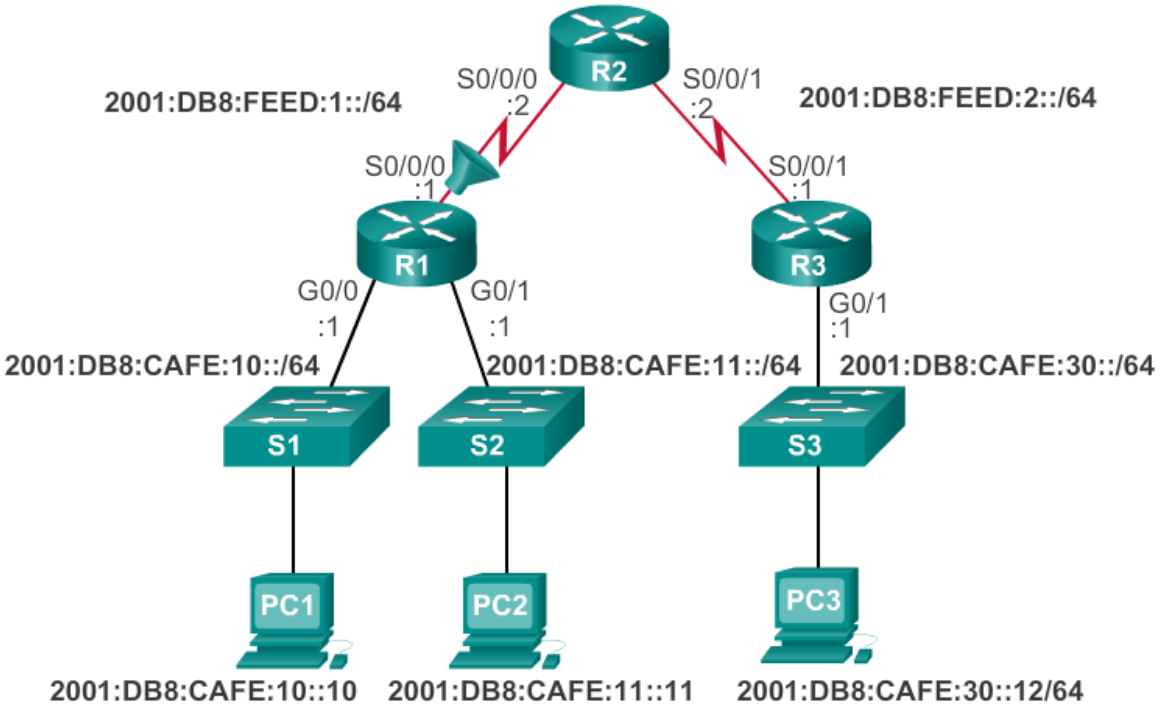
Hay tres pasos básicos para configurar una ACL IPv6:

Desde el modo global, utilice el comando **`ipv6 access-list`** *`name`* para crear una ACL IPv6.

Desde el modo de la ACL nombrada, utilice **`permit`** or **`deny en`** las declaraciones para especificar una o más condiciones para determinar si un paquete se reenvía o se elimina.

Vuelva al modo EXEC privilegiado con el comando end

La aplicación de una ACL IPv6 a una interfaz




```
R1(config)#interface s0/0/0
R1(config-if)#ipv6 traffic-filter NO-R3-LAN-ACCESS in
```

Ejemplos de ACL en IPv6

Denegar FTP

```
R1(config)#ipv6 access-list NO-FTP-TO-11
R1(config-ipv6-acl)#deny tcp any 2001:db8:cafe:11::/64 eq ftp
R1(config-ipv6-acl)#deny tcp any 2001:db8:cafe:11::/64 eq ftp-data
R1(config-ipv6-acl)#permit ipv6 any any
R1(config-ipv6-acl)#exit
R1(config)#interface g0/0
R1(config-if)#ipv6 traffic-filter NO-FTP-TO-11 in
R1(config-if)#
```

Restringir el acceso

```
R3(config)#ipv6 access-list RETRICTED-ACCESS
R3(config-ipv6-acl)#remark Permit access only HTTP and HTTPS to Network 1
R3(config-ipv6-acl)#permit tcp any host 2001:db8:cafe:10::10 eq 80
R3(config-ipv6-acl)#permit tcp any host 2001:db8:cafe:10::10 eq 443   1
R3(config-ipv6-acl)#remark Deny all other traffic to Network 10
R3(config-ipv6-acl)#deny ipv6 any 2001:db8:cafe:10::/64   2
R3(config-ipv6-acl)#remark Permit PC3 telnet access to PC2
R3(config-ipv6-acl)#permit tcp host 2001:DB8:CAFE:30::12 host 2001:DB8:CA
R3(config-ipv6-acl)#remark Deny telnet access to PC2 for all other device
R3(config-ipv6-acl)#deny tcp any host 2001:db8:cafe:11::11 eq 23   4
R3(config-ipv6-acl)#remark Permit access to everything else
R3(config-ipv6-acl)#permit ipv6 any any   5
R3(config-ipv6-acl)#exit
R3(config)#interface g0/0
R3(config-if)#ipv6 traffic-filter RESTRICTED-ACCESS in   6
R3(config-if)#
```

Resumen

- El filtrado de paquetes, controla el acceso a una red mediante el análisis de los paquetes entrantes y salientes y permite o niega sobre la base de criterios como la IP de origen, o de destino y el protocolo realizado dentro del paquete.

- Un router hace filtrado de paquetes utilizando las reglas si se permite o niega el tráfico. también puede realizar el filtrado de paquetes en la Capa 4, o la capa de transporte.

- Una ACL es una lista secuencial de permiso o negación de sentencias.

Resumen

- La última declaración de una ACL es siempre una negación implícita que bloquea todo el tráfico.
- Para evitar esta condición al final de la ACL se debe colocar una **`permit ip any any`**.
- Cuando el tráfico de red pasa a través de una interfaz configurada con una ACL, el router compara la información dentro del paquete en cada entrada, en orden secuencial. Si se encuentra una coincidencia, el paquete es procesado en consecuencia.
- Las ACL están configuradas para aplicar al tráfico entrante o para aplicar al tráfico saliente.

Resumen

- **Las ACL estándar** se pueden utilizar para permitir o denegar el tráfico sólo a partir de **una dirección IPv4 de origen.** El destino del paquete y los puertos implicados no son evaluados. **Colocarla lo mas cerca del destino**.

- **Las ACL Extendidas** filtran paquetes basado en: el tipo de protocolo, origen o destino de las IPv4, o los puertos de destino de origen. **Colocarla lo más cerca posible del origen**.

Resumen

- El comando **`access-list`** desde configuración global define una ACL estándar con un número de 1 a 99 o una extendida con números en el rango de 100 a 199 y 2000 a 2699. Ambas también pueden ser nombradas.

- **`ip access-list standard o extended`** *`name`*, para listas nombradas en ACL en IPv4 incluyen el uso de máscaras wildcard.

- Después de configurar una ACL, se vincula a una interfaz con **ip access-group** en el modo de configuración de interfaz.

Resumen

- Recuerda **las tres Ps, una ACL por protocolo, por dirección, por interfaz.**

- Para eliminar una ACL de una interfaz, **no ip access-group**, y luego el comando **no access-list** para eliminar toda la ACL desde el modo global

- **show running-config y show access-lists** para verificar la configuración de la ACL.
- **show ip interface** se utiliza para verificar la ACL en la interfaz y la dirección en la que se aplicó.

Resumen

- **`access-class`** en el modo de configuración de línea restringe las conexiones entrantes y salientes entre un VTY particular y las direcciones en una lista de acceso.

- Las ACL nombradas en IPv4 en IPv6 son alfanuméricos, mayúsculas y minúsculas y debe ser única. A diferencia de IPv4, no hay necesidad de una opción estándar o extendida.
- Desde el modo global, **`ipv6 access-list`** ***`name`*** crea una ACL IPv6. El prefijo de longitud se utiliza para indicar la cantidad de una IPv6 de origen o destino que debe coincidir.

- Después que una ACL en IPv6 está configurada, se vincula a una interfaz con **`ipv6 traffic-filter`**.

Cisco | Networking Academy®
Mind Wide Open™

MUCHAS GRACIAS

CONSTRUIMOS FUTURO