

# SEGURIDAD EN NETWORKING



## Unidad 2

Vulnerabilidades, procedimientos, acciones de  
mitigación y Controles de ISO 27001



## **ESCUELA DE INGENIERÍA Y CONSTRUCCIÓN**

**Director:** Marcelo Lucero Yáñez

### **ELABORACIÓN**

**Experto disciplinar:** Luis Ignacio Jaque

**Diseñadora instruccional:** Francisca Capponi

**Editora instruccional:** Francisca Aránguiz Jiménez

### **VALIDACIÓN**

**Experto disciplinar:** Rodrigo Orellana Núñez

**Jefa de Diseño Instruccional:** Alejandra San Juan

### **EQUIPO DE DESARROLLO**

Welearn

**AÑO**

2022



## Tabla de contenidos

Aprendizaje esperado .....	4
Introducción.....	5
1. Tipos de ACL IPv6 .....	6
2. Comparación entre ACL de IPv4 y de IPv6 .....	7
3. Configuración de topología de IPv6 .....	9
4. Configuración de ACL de IPv6.....	12
5. Aplicación de una ACL de IPv6 a una interfaz .....	15
6. Ejemplos de ACL de IPv6.....	17
6.1. Denegar FTP.....	17
6.2. Acceso restringido.....	18
7. Verificación de ACL de IPv6.....	20
Cierre .....	22
Referencias bibliográficas .....	23



# Aprendizaje esperado

Aplicar listas de control de acceso de tipo **IPv6** para implementaciones básicas de seguridad, según requerimientos de la empresa y estándares.



**Fuente:** Freepik

# Introducción

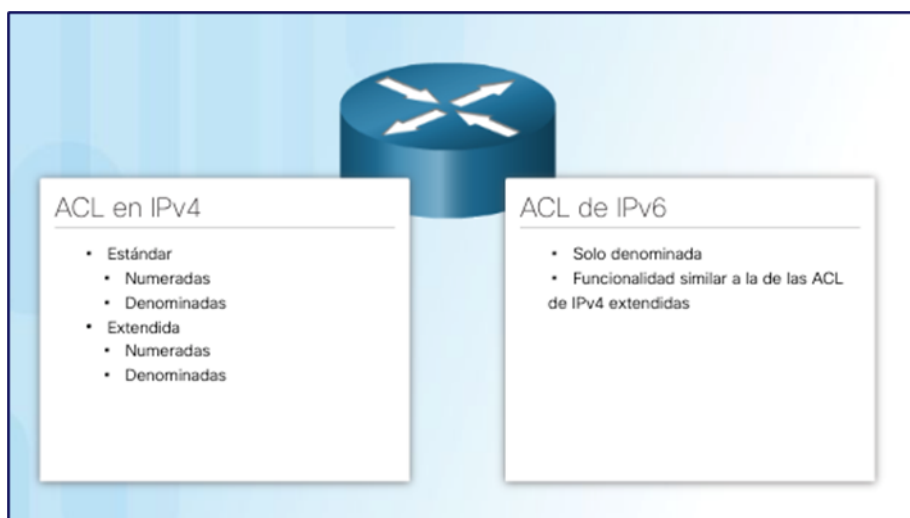
Esta semana realizaremos una revisión de las Listas de Acceso y de la configuración de **ACL IPv6** estándar. Junto con ello se explica cómo configurar y solucionar problemas en las **ACL IPv6** extendidas en un *router* Cisco como parte de una solución de seguridad. Se incluyen consejos, consideraciones, recomendaciones y pautas generales sobre cómo utilizar las **ACL**.

Considerando la seguridad de las redes, el cómo y dónde se aplican las **ACL IPv6** estándares nombradas y numeradas, al final de esta semana podrán responder la siguiente pregunta: ¿cómo y dónde aplicar estas listas de acceso?

# 1. Tipos de ACL IPv6

Las **ACL IPv6** son similares a las **ACL IPv4** tanto en su configuración como en su funcionamiento. Si ya está familiarizado con las listas de acceso de **IPv4**, las **ACL** de **IPv6** serán fáciles de comprender y configurar.

Existen dos tipos de ACL en **IPv4**: el estándar y las extendidas. Ambos tipos de ACL pueden ser numeradas o con nombre. En cuanto a **IPv6**, hay solamente un tipo de ACL, que equivale a la ACL de **IPv4** extendida con nombre. No existen **ACL** numeradas en **IPv6**. Una ACL de **IPv4** y una **ACL** de **IPv6** no pueden tener el mismo nombre.



**Figura 1:** ACL de IPv6.

Fuente: Cisco Networking Academy (2022)

## 2. Comparación entre ACL de IPv4 y de IPv6

Aunque las **ACL IPv4** e **IPv6** son muy similares, hay tres diferencias fundamentales entre ellas:

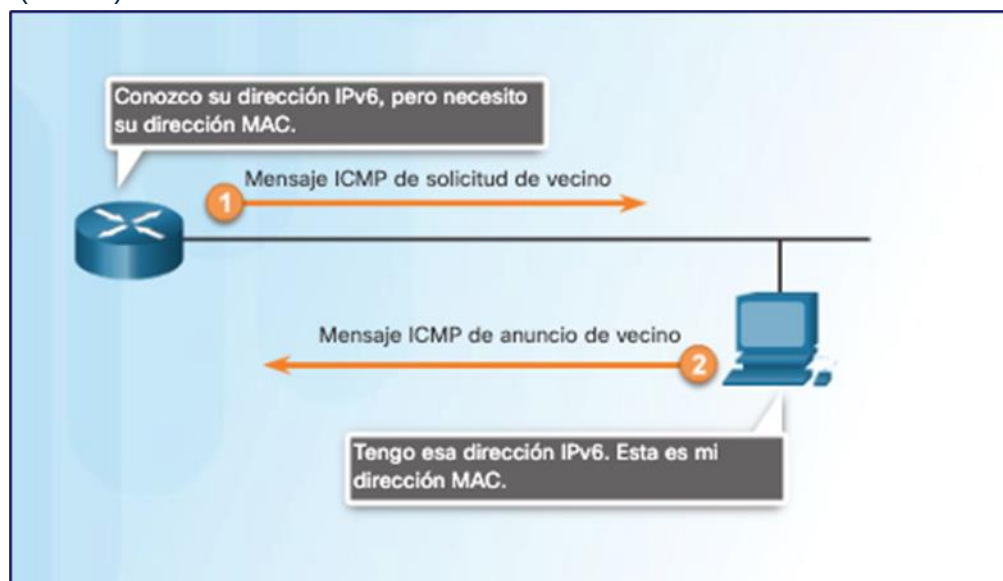
1. El comando que se utiliza para aplicar una **ACL** de **IPv6** a una interfaz. **IPv4** utiliza el comando ***ip access-group*** para aplicar una **ACL** de **IPv4** a una interfaz **IPv4**. **IPv6** utiliza el comando ***ipv6 traffic-filter*** para realizar la misma función para las interfaces **IPv6**.
2. A diferencia de las **ACL** de **IPv4**, las **ACL** de **IPv6** no utilizan máscaras **wildcard**. En cambio, se utiliza la longitud del prefijo para indicar cuánto de una dirección **IPv6** de origen o destino debe coincidir.
3. La última diferencia principal tiene que ver con la inclusión de dos instrucciones ***permit*** implícitas al final de cada lista de acceso de **IPv6**. Al final de todas las **ACL IPv4** estándar o extendidas, hay una instrucción ***deny any*** o ***deny ip any any*** implícita. En **IPv6** se incluye una instrucción ***deny ipv6 any any*** similar al final de cada **ACL** de **IPv6**. La diferencia es que **IPv6** también incluye dos otras instrucciones implícitas de forma predeterminada: ***permit icmp any any nd-na*** y ***permit icmp any any nd-ns***.

Estas dos instrucciones permiten que el *router* participe en el equivalente de **ARP** para **IPv4** en **IPv6**. Recuerde que **ARP** se utiliza en **IPv4** para resolver las direcciones de capa 3 a direcciones **MAC** de capa 2. Como se muestra en la ilustración, en **IPv6** se



utilizan mensajes **ICMP** de descubrimiento de vecinos (**ND**) para lograr el mismo propósito. **ND** utiliza mensajes de solicitud de vecino (**NS**) y de anuncio de vecino (**NA**).

Los mensajes **ND** se encapsulan en paquetes **IPv6** y requieren los servicios de la capa de red **IPv6**, mientras que **ARP** para **IPv4** no utiliza la capa 3. Dado que **IPv6** utiliza el servicio de la capa 3 para el descubrimiento de vecinos, las **ACL** de **IPv6** deben permitir implícitamente que los paquetes **ND** se envíen y reciban por una interfaz. Específicamente, se permiten tanto los mensajes de descubrimiento de vecinos-anuncio de vecinos (**nd-na**) como los de descubrimiento de vecinos-solicitud de vecinos (**nd-ns**).



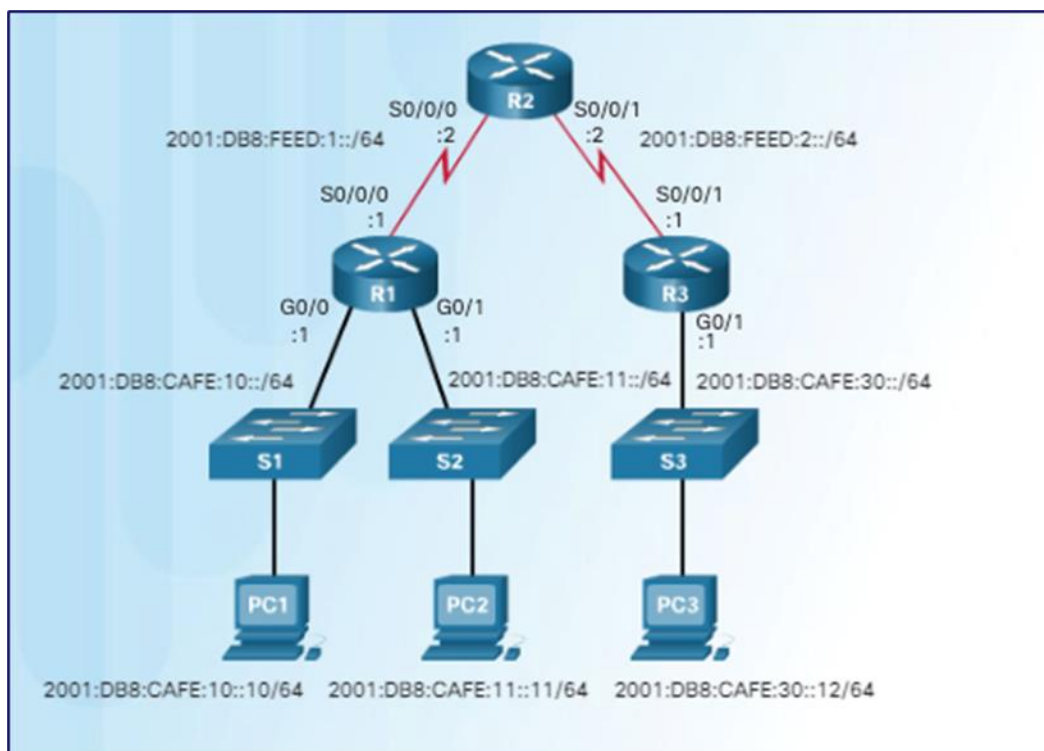
**Figura 2:** Descubrimiento de vecinos IPv6.

**Fuente:** Cisco Networking Academy (2022)

### 3. Configuración de topología de IPv6

En la figura 3 se muestra la topología que se utilizará para configurar las **ACL** de **IPv6**. Esta es similar a la topología de **IPv4** anterior, excepto por el esquema de direccionamiento **IPv6**. Existen tres subredes 2001:DB8: CAFE: :/64:

- 2001:DB8: CAFE:10: :/64
- 2001:DB8: CAFE:11: :/64
- 2001:DB8: CAFE:30: :/64



**Figura 3:** Topología IPv6.

**Fuente:** Cisco Networking Academy (2022)

Dos redes seriales conectan los tres *routers*:

- 2001:DB8: FEED:1: :/64
- 2001:DB8: FEED:2: :/64

En las figuras 4, 5 y 6 se muestra la configuración de la dirección **IPv6** para cada uno de los *routers*. El comando ***show ipv6 interface brief*** se utiliza para verificar la dirección y el estado de la interfaz.

```
R1(config)# interface g0/0
R1(config-if)# ipv6 address 2001:db8:cafe:10::1/64
R1(config-if)# exit
R1(config)# interface s0/0/0
R1(config-if)# ipv6 address 2001:db8:feed:1::1/64
R1(config-if)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:11::1/64
R1(config-if)# end
R1# show ipv6 interface brief
GigabitEthernet0/0      [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:CAFE:10::1
GigabitEthernet0/1      [up/up]
    FE80::FE99:47FF:FE75:C3E1
    2001:DB8:CAFE:11::1
Serial0/0/0             [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:FEED:1::1
<se omitió el resultado>
R1#
```

**Figura 4:** Configuración de R1.

**Fuente:** Cisco Networking Academy (2022)

```

R2(config)# interface s0/0/0
R2(config-if)# ipv6 address 2001:db8:feed:1::2/64
R2(config-if)# exit
R2(config)# interface s0/0/1
R2(config-if)# ipv6 address 2001:db8:feed:2::2/64
R2(config-if)# end
R2# show ipv6 interface brief
Serial0/0/0          [up/up]
    FE80::FE99:47FF:FE71:78A0
    2001:DB8:FEED:1::2
Serial0/0/1          [up/up]
    FE80::FE99:47FF:FE71:78A0
    2001:DB8:FEED:2::2
<se omitió el resultado>
R2#

```

**Figura 4:** Configuración de R2.

**Fuente:** Cisco Networking Academy (2022)

```

R3(config)# interface s0/0/1
R3(config-if)# ipv6 address 2001:db8:feed:2::1/64
R3(config-if)# exit
R3(config)# interface g0/0
R3(config-if)# ipv6 address 2001:db8:cafe:30::1/64
R3(config-if)# end
R3# show ipv6 interface brief
GigabitEthernet0/0   [up/up]
    FE80::FE99:47FF:FE71:7A20
    2001:DB8:CAFE:30::1
Serial0/0/1          [up/up]
    FE80::FE99:47FF:FE71:7A20
    2001:DB8:FEED:2::1
R3#

```

**Figura 5:** Configuración de R3.

**Fuente:** Cisco Networking Academy (2022)

## 4. Configuración de ACL de IPv6

En **IPv6** solo hay **ACL** con nombre. La configuración es similar a la de una **ACL** de **IPv4** extendida con nombre.

En la figura 6 se muestra la sintaxis de los comandos para las **ACL** de **IPv6**. La sintaxis es similar a la que se utiliza en **ACL** de **IPv4** extendidas. Una diferencia importante es el uso de la longitud de prefijo **IPv6** en lugar de una máscara *wildcard IPv4*.

<pre>R1(config)# ipv6 access-list access-list-name R1(config-ipv6-acl)# deny   permit protocol {source-ipv6-prefix/prefix-length   any   host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length   any   host destination-ipv6-address} [operator [port-number]]</pre>	
Parámetro	Descripción
<b>deny   permit</b>	Especifica si se deniega o se permite el paquete.
<i>Protocolo</i>	Introduzca el nombre o el número de un protocolo de Internet o un número entero que represente un número de protocolo IPv6.
<i>source-ipv6-prefix/prefix-length</i>	La red IPv6 de origen o destino, o la clase de redes para las que se deben establecer condiciones de denegación o permiso.
<i>destination-ipv6-address</i>	
<b>cualquiera</b>	Introduzca <b>any</b> como abreviatura para el prefijo IPv6 <b>::/0</b> . Este coincide con todas las direcciones.
<b>host</b>	Para el <b>host</b> <i>source-ipv6-address</i> o <i>destination-ipv6-address</i> , ingrese la dirección de host IPv6 de origen o destino al cual se asignarán las condiciones de permitir o denegar.
<i>operator</i>	(Optativo) Operando que compara los puertos de origen o destino del protocolo especificado. Los operandos son lt (menor que), gt (mayor que), eq (igual que), neq (distinto de) y range (rango).
<i>número-puerto</i>	(Optativo) Número decimal o nombre de un puerto TCP o UDP para filtrar TCP y UDP respectivamente.

**Figura 6:** Sintaxis de comandos ACL IPv6.

**Fuente:** Cisco Networking Academy (2022)

Hay tres pasos básicos para configurar una **ACL** de **IPv6**:

- En el modo de configuración global, se usa el comando **ipv6 access-list** se para crear una **ACL IPv6**. Al igual que las **ACL** de **IPv4** con nombre, los nombres en **IPv6** son alfanuméricos, distinguen mayúsculas de minúsculas y deben ser únicos. A diferencia de **IPv4**, no hay necesidad de una opción estándar o extendida.
- En el modo de configuración de **ACL** con nombre, utilice las instrucciones **permit** o **deny** para especificar una o más condiciones para determinar si un paquete se debe reenviar o descartar.
- Regrese al modo **EXEC** con privilegios con el comando **end**.

En la figura 7, se muestran los pasos para crear una **ACL** de **IPv6** con un ejemplo simple basado en la topología anterior. La primera instrucción da el nombre **NO-R3-LAN-ACCESS** a la lista de acceso de **IPv6**. Al igual que sucede con las **ACL** de **IPv4** con nombre, no es necesario el uso de mayúsculas en los nombres de las **ACL** de **IPv6**, pero esto hace que se destaquen cuando se observa el resultado de la configuración en ejecución.

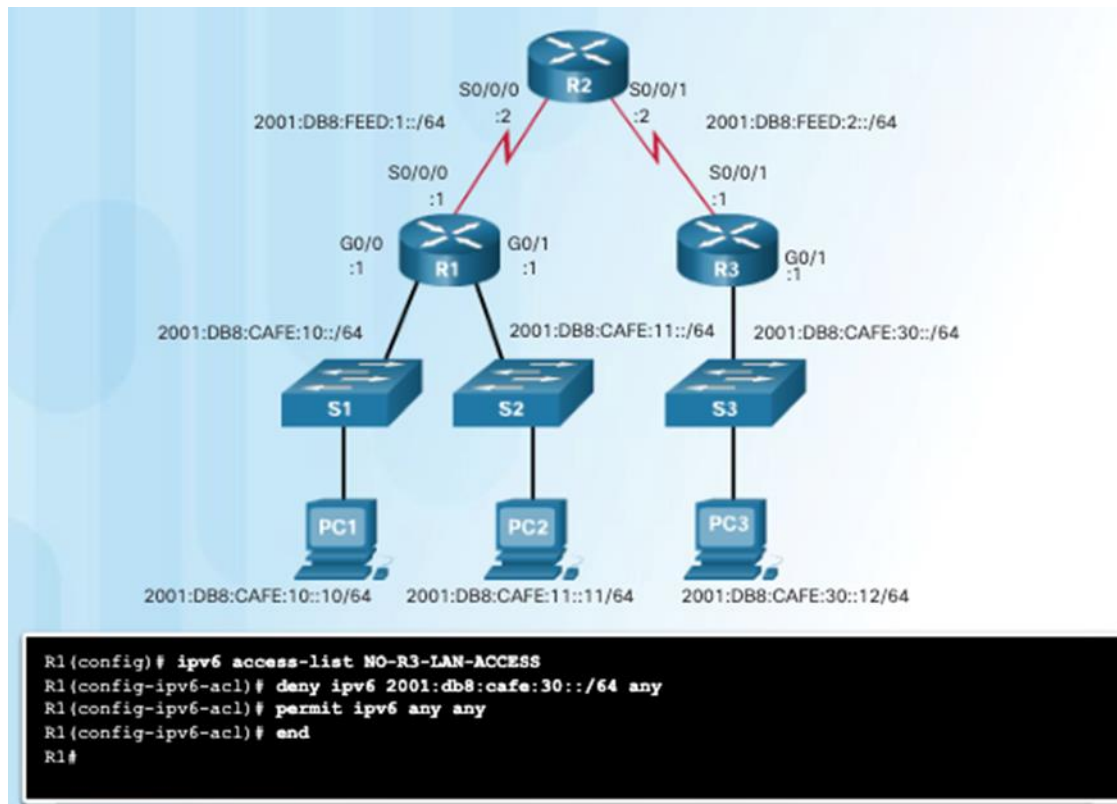
```
R1(config)# ipv6 access-list NO-R3-LAN-ACCESS
R1(config-ipv6-acl)# deny ipv6 2001:db8:cafe:30::/64 any
R1(config-ipv6-acl)# permit ipv6 any any
R1(config-ipv6-acl)# end
R1#
```

**Figura 7:** ACL de IPv6 de ejemplo.

Fuente: Cisco Networking Academy (2022)

La segunda instrucción deniega todos los paquetes 2001:DB8:CAFE:30::/64 destinados a cualquier red **IPv6**. La tercera instrucción permite el resto de los paquetes **IPv6**.

En la figura 8 se muestra la **ACL** en contexto con la topología.



**Figura 8:** Topología IPv6 de ejemplo.

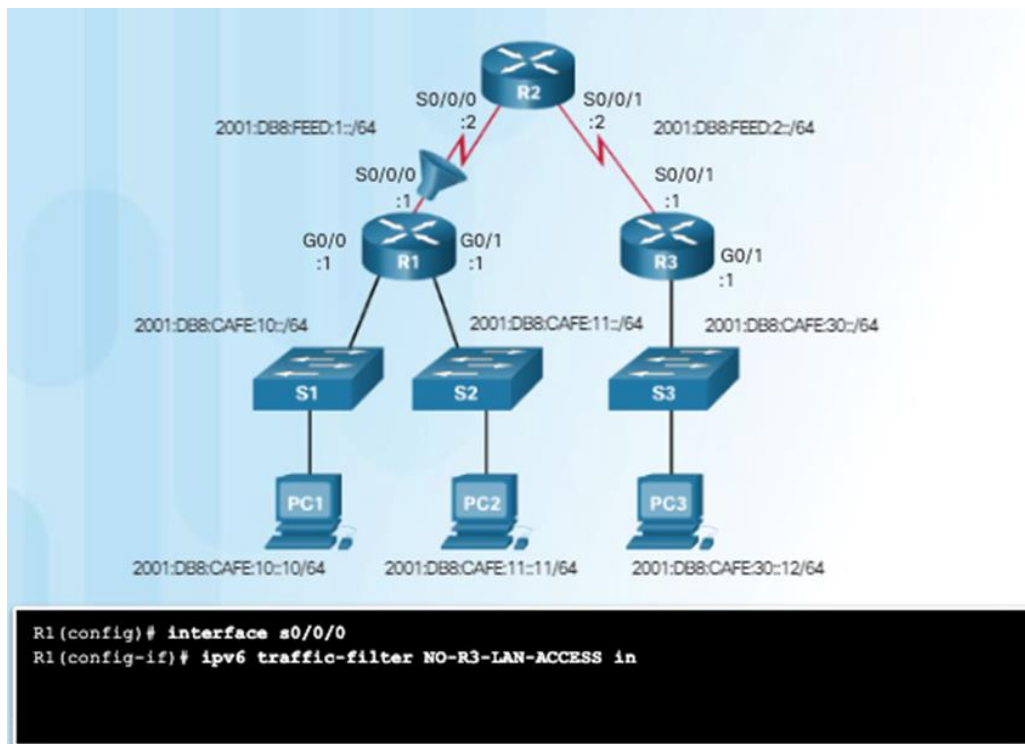
Fuente: Cisco Networking Academy (2022)

## 5. Aplicación de una ACL de IPv6 a una interfaz

Después de que se configura una **ACL** de **IPv6**, se la vincula a una interfaz mediante el comando **ipv6 traffic-filter**:

```
Router(config-if) # ipv6 traffic-filter access-list-name {in | out}
```

En la figura 9, se muestra la **ACL** NO-R3-LAN-ACCESS configurada anteriormente y los comandos utilizados para aplicar la **ACL** de **IPv6** de entrada a la interfaz S0/0/0. Si se aplica la **ACL** a la interfaz S0/0/0 de entrada, se denegarán los paquetes de 2001:DB8:CAFE:30::/64 en ambas LAN en el R1.



**Figura 9:** Topología IPv6 de ejemplo 2.

**Fuente:** Cisco Networking Academy (2022)



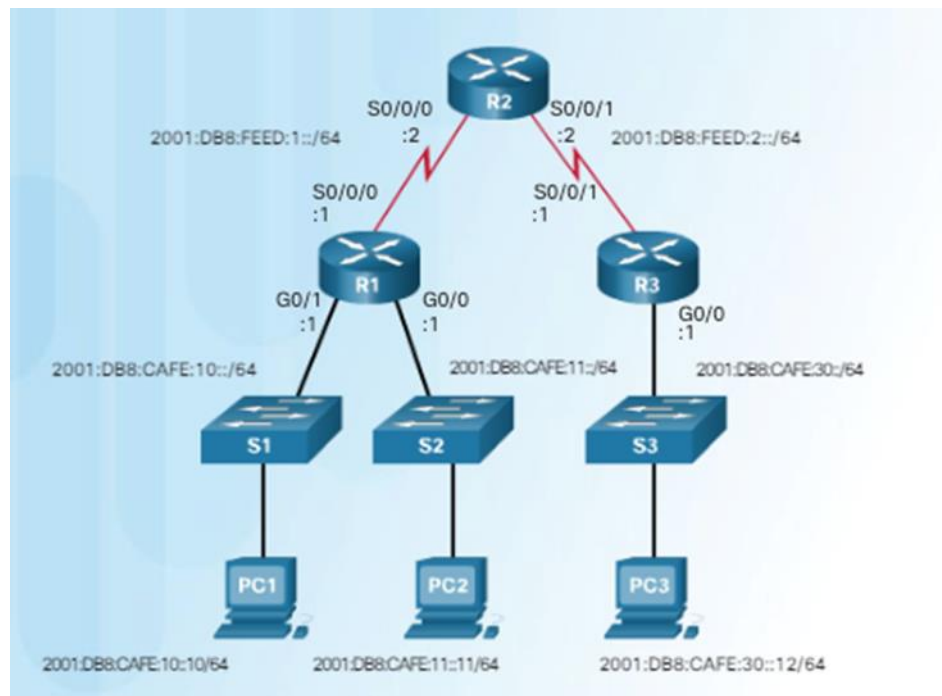
Para eliminar una **ACL** de una interfaz, primero introduzca el comando ***no ipv6 traffic-filter*** en la interfaz y, luego, introduzca el comando global ***no ipv6 access-list*** para eliminar la lista de acceso.

**Nota:** Tanto en **IPv4** como en **IPv6** se utiliza el comando **access-class** para aplicar una lista de acceso a los puertos VTY.

## 6. Ejemplos de ACL de IPv6

### 6.1. Denegar FTP

La topología para los ejemplos se muestra en la figura 10.



**Figura 10:** Topología IPv6 de ejemplo 3.

**Fuente:** Cisco Networking Academy (2022)

En el primer ejemplo (figura 11), el *router* R1 está configurado con una lista de acceso **IPv6** para denegar el tráfico FTP a 2001:DB8: CAFE:11: ::/64. Se deben bloquear los puertos para los datos FTP (puerto 20) y el control FTP (puerto 21). Como se aplica un

filtro entrante en la interfaz G0/0 de R1, solo se denegará el tráfico de la red 2001:DB8:CAFE:10::/64.

```
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)#
```

**Figura 11:** Denegar FTP.

Fuente: Cisco Networking Academy (2022)

## 6.2. Acceso restringido

En el segundo ejemplo (figura 12), se configura una **ACL IPv6** para proporcionar a la red LAN en R3 acceso limitado a las redes LAN en R1. Se agregan comentarios en la configuración para documentar la **ACL**. Se marcaron las siguientes características en la **ACL**:

1. Las primeras dos instrucciones **permit** proporcionan acceso desde cualquier dispositivo al servidor *web* en 2001:DB8:CAFE:10::10.
2. El resto de los dispositivos tienen denegado el acceso a la red 2001:DB8:CAFE:10::/64.
3. A la PC3 en 2001:DB8:CAFE:30::12 se le permite el acceso por Telnet a la PC2, que tiene la dirección IPv6 2001:DB8:CAFE:11::11.

4. El resto de los dispositivos tiene denegado el acceso por Telnet a la PC2.
5. El resto del tráfico **IPv6** se permite al resto de los destinos.
6. La lista de acceso de **IPv6** se aplica a la interfaz G0/0 en sentido de entrada, por lo que solo la red 2001:DB8: CAFE:30::/64 se ve afectada.

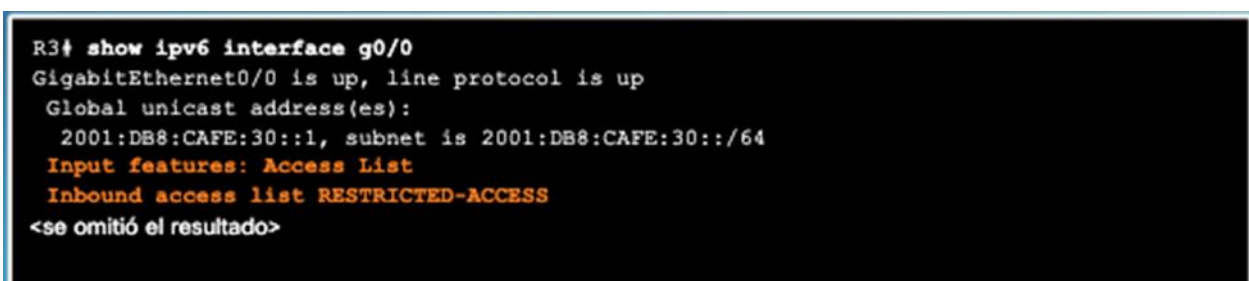
```
R3(config)# ipv6 access-list RESTRICTED-ACCESS
R3(config-ipv6-acl)# remark Permit access only HTTP and HTTPS to Network 10
R3(config-ipv6-acl)# permit tcp any host 2001:db8:cafe:10::10 eq 80
R3(config-ipv6-acl)# permit tcp any host 2001:db8:cafe:10::10 eq 443
R3(config-ipv6-acl)# remark Deny all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

**Figura 12:** Restricción de acceso.

**Fuente:** Cisco Networking Academy (2022)

## 7. Verificación de ACL de IPv6

Los comandos que se utilizan para verificar una lista de acceso de **IPv6** son similares a los que se utilizan para las ACL de **IPv4**. Con estos comandos, se puede verificar la lista de acceso de **IPv6** RESTRICTED-ACCESS que se configuró anteriormente. En la figura 13, se muestra el resultado del comando **show ipv6 interface**. El resultado confirma que la ACL RESTRICTED-ACCESS está configurada en sentido de entrada en la interfaz G0/0.



```
R3# show ipv6 interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Global unicast address(es):
  2001:DB8:CAFE:30::1, subnet is 2001:DB8:CAFE:30::/64
Input features: Access List
Inbound access list RESTRICTED-ACCESS
<se omitió el resultado>
```

**Figura 13:** Restricción de acceso.

Fuente: Cisco Networking Academy (2022)

Como se muestra en la figura 14, el comando **show access-lists** muestra todas las listas de acceso en el *router*, incluidas las **ACL** de **IPv4** y de **IPv6**. Observe que, en las **ACL** de **IPv6**, los números de secuencia se colocan al final de la instrucción y no al principio, como ocurre en las listas de acceso de **IPv4**. Aunque las instrucciones aparecen en el orden en que se introdujeron, no siempre se presentan en incrementos de 10. Esto se debe a que las instrucciones **remark** que se introdujeron utilizan un número de secuencia, pero no se muestran en el resultado del comando **show access-lists**.

```

R3# show access-lists
IPv6 access list RESTRICTED-ACCESS
  permit tcp any host 2001:DB8:CAFE:10::10 eq www sequence 20
  permit tcp any host 2001:DB8:CAFE:10::10 eq 443 sequence 30
  deny ipv6 any 2001:DB8:CAFE:10::/64 sequence 50
  permit tcp host 2001:DB8:CAFE:30::12 host 2001:DB8:CAFE:11::11 eq
  telnet sequence 70
  deny tcp any host 2001:DB8:CAFE:11::11 eq telnet sequence 90
  permit ipv6 any any sequence 110
R3#

```

**Figura 14:** Restricción de acceso.

Fuente: Cisco Networking Academy (2022)

Al igual que las **ACL** extendidas para **IPv4**, las listas de acceso de **IPv6** se muestran y se procesan en el orden en que se introducen las instrucciones. Recuerde que las **ACL** de **IPv4** estándar utilizan una lógica interna que cambia el orden y la secuencia de procesamiento.

Como se muestra en la figura 15, el resultado del comando **show running-config** incluye todas las **ACE** y las instrucciones **remark**. Las instrucciones **remark** pueden colocarse antes o después de las instrucciones **permit** o **deny**, pero se debe mantener una ubicación coherente.

```

R3# show running-config
<resultado omitido>
ipv6 access-list RESTRICTED-ACCESS
  remark Permit access only HTTP and HTTPS to Network 10
  permit tcp any host 2001:DB8:CAFE:10::10 eq www
  permit tcp any host 2001:DB8:CAFE:10::10 eq 443
  remark Deny all other traffic to Network 10
  deny ipv6 any 2001:DB8:CAFE:10::/64
  remark Permit PC3 telnet access to PC2
  permit tcp host 2001:DB8:CAFE:30::12 host 2001:DB8:CAFE:11::11
  eq telnet
  remark Deny telnet access to PC2 for all other devices
  deny tcp any host 2001:DB8:CAFE:11::11 eq telnet
  remark Permit access to everything else
  permit ipv6 any any

```

**Figura 15:** Restricción de acceso.

Fuente: Cisco Networking Academy (2022)

# Cierre

Recomendaciones sobre cómo aplicar **ACLs IPv4** e **IPv6**:

ACL estándar lo más  
cerca posible del  
destino

ACL estándar No  
especifican direcciones  
destino

ACL extendidas lo más  
cerca posible del origen  
del tráfico denegado

Utiliza el comando de  
configuración **interface**  
para seleccionar una  
interfaz a la cual  
aplicarle la ACL

El comando **show ip  
interface** se utiliza para  
verificar la ACL en la  
interfaz.

El comando **show  
access-lists** muestra las  
estadísticas para cada  
instrucción que tiene  
coincidencias

Se pueden borrar los  
contadores mediante el  
comando **clear access-  
list counters**

# Referencias bibliográficas

- Cisco Networking Academy (2022). *Conexión de redes. Capítulo 4 – Listas de Control de acceso*. <https://bit.ly/3vzi7lQ>
- Cisco Networking Academy (2022). *Principios básicos de routing y switching. Capítulo 7 – Listas de Control de acceso*. <https://bit.ly/3vzi7lQ>