AIEP
DE LA UNIVERSIDAD ANDRES BELLO

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

Diseñador instruccional: Francisca Capponi

Editora instruccional: Trinidad Marshall

VALIDACIÓN

Experto disciplinar: Rodrigo Orellana Núñez

Jefa de Diseño Instruccional: Alejandra San Juan

EQUIPO DE DESARROLLO

Welearn

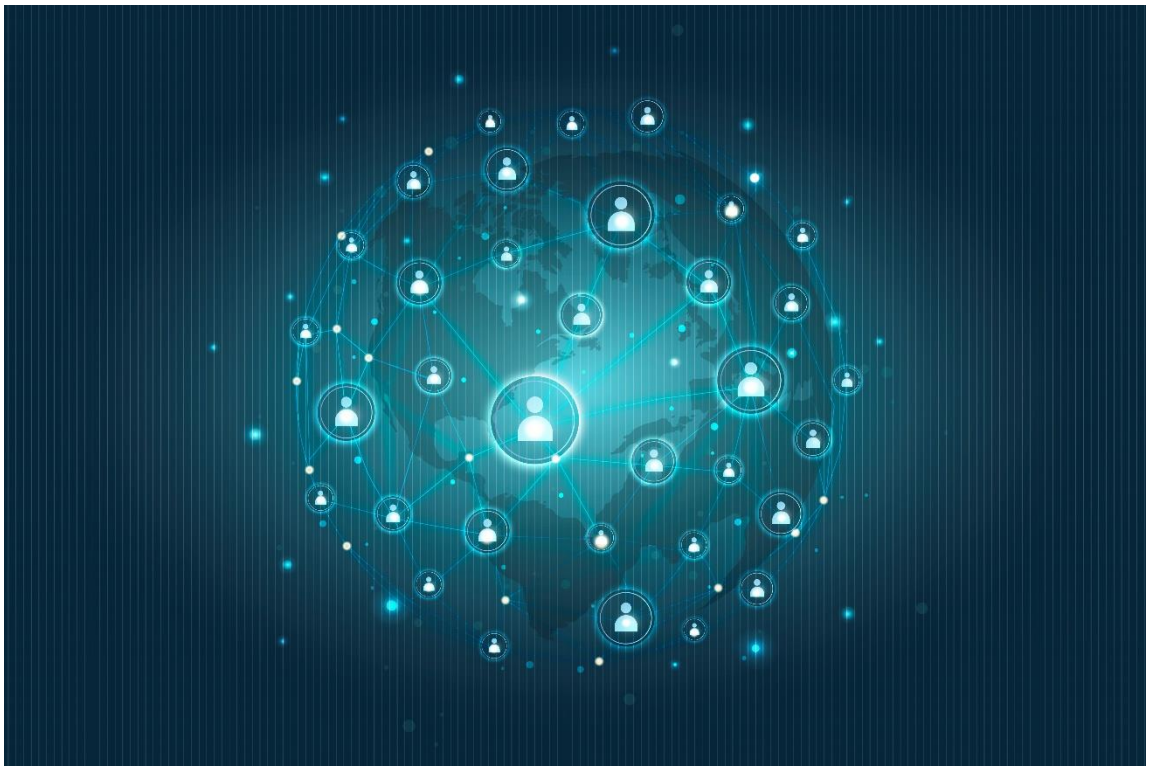
AÑO

2022

Tabla de contenidos

Aprendizaje esperado

Aplicar listas de control de acceso de tipo **IPv4** e **IPv6** para implementaciones medias de seguridad, según requerimientos técnicos.



Fuente: rawpixel.com en Freepik (s.f)

Introducción

Esta semana revisaremos una implementación y solución de problemas de las **Listas de Acceso** y de la configuración de **ACL IPv4** e **Ipv6**. Junto con ello, explicaremos cómo solucionar problemas de las listas de acceso IPv4 e IPv6 en un *router* Cisco como parte de una solución de seguridad.

Considerando la seguridad de las redes y el cómo y dónde se aplican las Listas de Acceso estándares nombradas y numeradas, al final de esta semana podrán responder a la pregunta: ¿Cómo dar soluciones a problemas comunes de ACL?

1. Lógica de ACL de entrada y salida

1.1 Lógica de ACL de entrada

En la figura 1, se muestra la lógica para una **ACL de entrada**. Si hay una coincidencia entre la información de un encabezado de paquete y una instrucción de ACL, el resto de las instrucciones de la lista se omiten y se permite o se deniega el paquete según lo especificado por la instrucción de la coincidencia. Si no existe una coincidencia entre un encabezado de paquete y una instrucción de ACL, el paquete se prueba en relación con la siguiente instrucción de la lista. Este proceso de búsqueda de coincidencias continúa hasta que se llega al final de la lista.

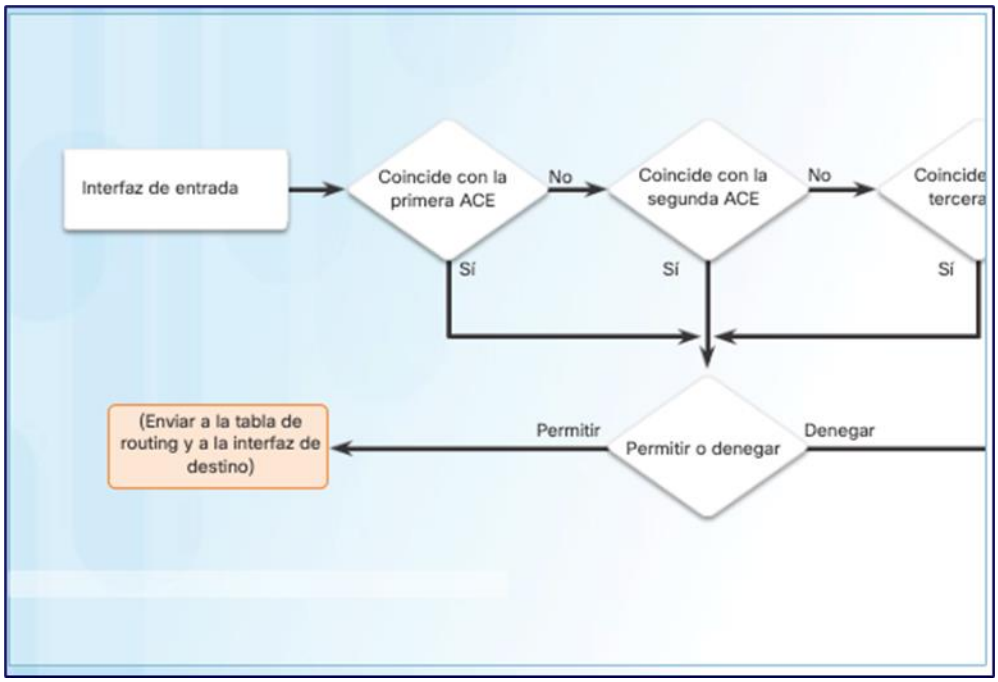


Figura 1: Proceso de ACL de entrada.

Fuente: Cisco Networking Academy (2022)

Al final de cada ACL hay una instrucción ***deny any*** implícita que no se muestra en el resultado. Esta instrucción se aplica a todos los paquetes cuyas condiciones no se probaron como verdaderas. Esta condición de prueba final coincide con el resto de los paquetes y da como resultado una acción de denegación. En lugar de avanzar en el sentido de entrada o de salida de una interfaz, el *router* descarta todos los paquetes restantes. A esta instrucción final se la suele conocer como instrucción "***deny any*** implícita" o "denegación de todo el tráfico". Debido a esta instrucción, una ACL debería incluir, por lo menos, una instrucción ***permit***. De lo contrario, la ACL bloquea todo el tráfico.

1.2 Lógica de ACL de salida

En la figura 2, se muestra la lógica para una **ACL de salida**. Antes de que se reenvíe un paquete a una interfaz de salida, el *router* revisa la tabla de *routing* para ver si el paquete es enrutable. Si no lo es, se descarta y no se prueba en relación con las **ACE**. A continuación, el *router* revisa si la interfaz de salida está agrupada con una ACL. Si la interfaz de salida no está agrupada con una ACL, el paquete se puede enviar al búfer de salida. Algunos ejemplos de la operación de la ACL de salida son:

- **No se aplica ACL a la interfaz**: Si la interfaz saliente no se agrupa con una ACL saliente, el paquete se envía directamente a la interfaz saliente.

- **Se aplica ACL a la interfaz**: Si la interfaz saliente se agrupa con una ACL saliente, el paquete no se envía a la interfaz saliente hasta que se lo pruebe combinando **ACE** asociadas con dicha interfaz. Según las pruebas de ACL, el paquete se permite o se deniega.

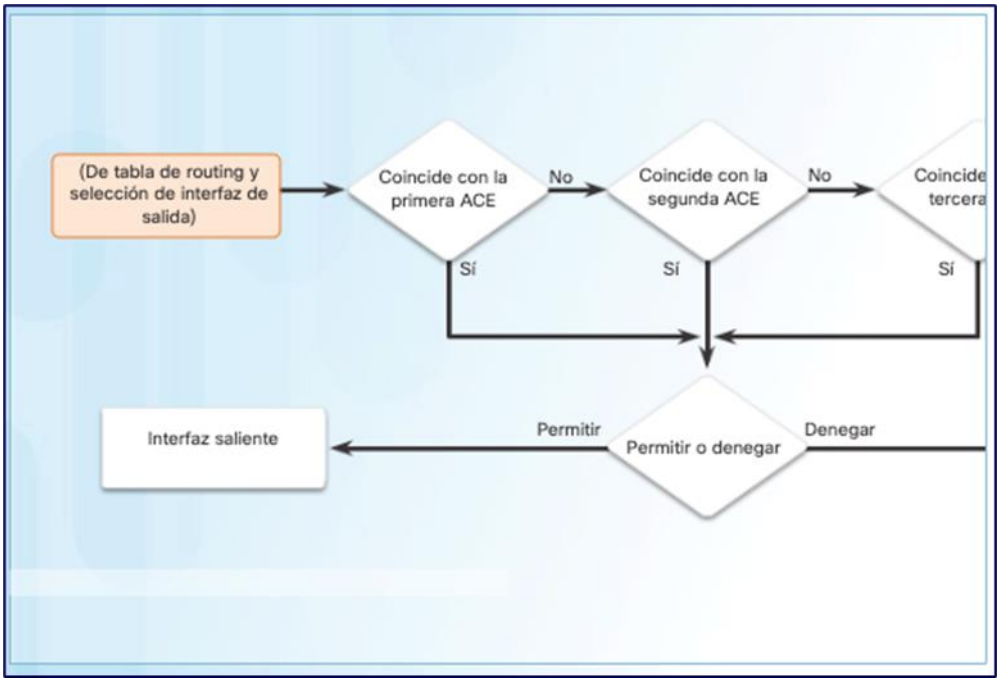


Figura 2: Proceso de ACL de salida.

Fuente: Cisco Networking Academy (2022)

Para las listas de salida, "***permit***" (permitir) significa enviar el paquete al búfer de salida y "***deny***" (denegar) significa descartar el paquete.

2. Operaciones lógicas de ACL

En la figura 3, se muestra la lógica de los procesos de ***routing*** y **ACL**. Cuando un paquete llega a una interfaz del *router*, el proceso del *router* es el mismo, ya sea si se utilizan ACL o no.

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.

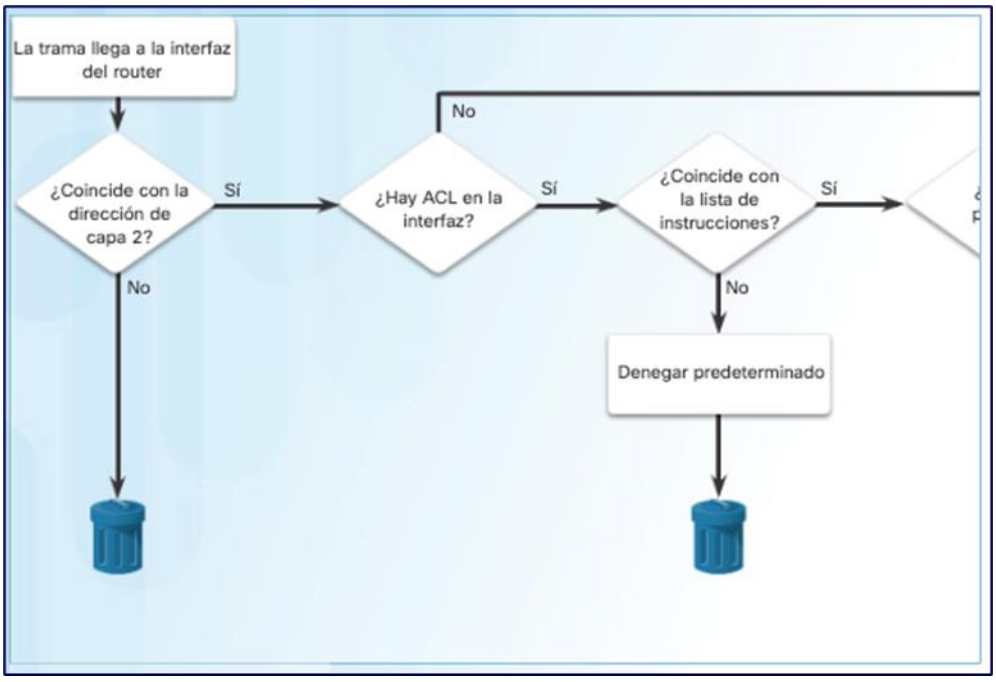


Figura 3: Procesos de ACL y *routing* en un *router*.

Fuente: Cisco Networking Academy (2022)

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. En caso de que lo tenga, 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.

3. Proceso de decisión de ACL estándar

Las **ACL estándar** solamente examinan la dirección **IPv4** de origen, el destino del paquete y los puertos involucrados no se tienen en cuenta. El proceso de decisión de una ACL estándar se detalla en la figura 4. El *software* **IOS** de Cisco prueba las direcciones en relación con cada una de las condiciones de la ACL. La primera coincidencia determina si el *software* acepta o rechaza la dirección.

Dado que el *software* deja de probar las condiciones después de la primera coincidencia, el orden de las condiciones es fundamental. Si no coincide ninguna condición, la dirección se rechaza.

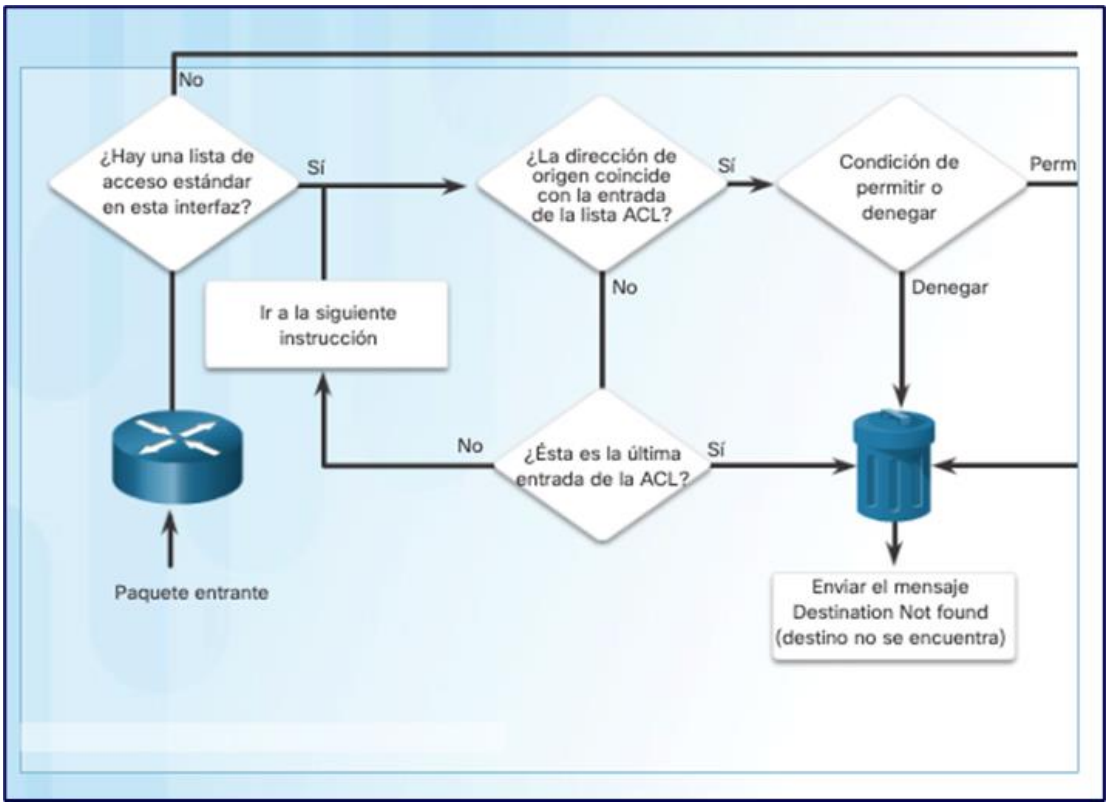


Figura 4: ¿Cómo funciona una ACL estándar?

Fuente: Cisco Networking Academy (2022)

4. Proceso de decisión de ACL extendida

En la figura 5, se muestra la ruta de decisión lógica que utiliza una **ACL extendida** creada para filtrar direcciones de origen y destino, y números de protocolo y de puerto. En este ejemplo, la ACL primero filtra sobre la dirección de origen y, a continuación, sobre el puerto y el protocolo de origen. Luego, filtra por la dirección de destino y después por el puerto y el protocolo de destino, y toma la decisión final de permiso o denegación.

Recuerde que las entradas en las ACL se procesan una tras otra, de modo que una decisión negativa (***no***) no es necesariamente una decisión de denegación (***deny***). A medida que avance a través de la ruta de decisión lógica, tenga en cuenta que un ***no*** significa que se debe pasar a la siguiente entrada hasta que encuentre una coincidencia para una condición.

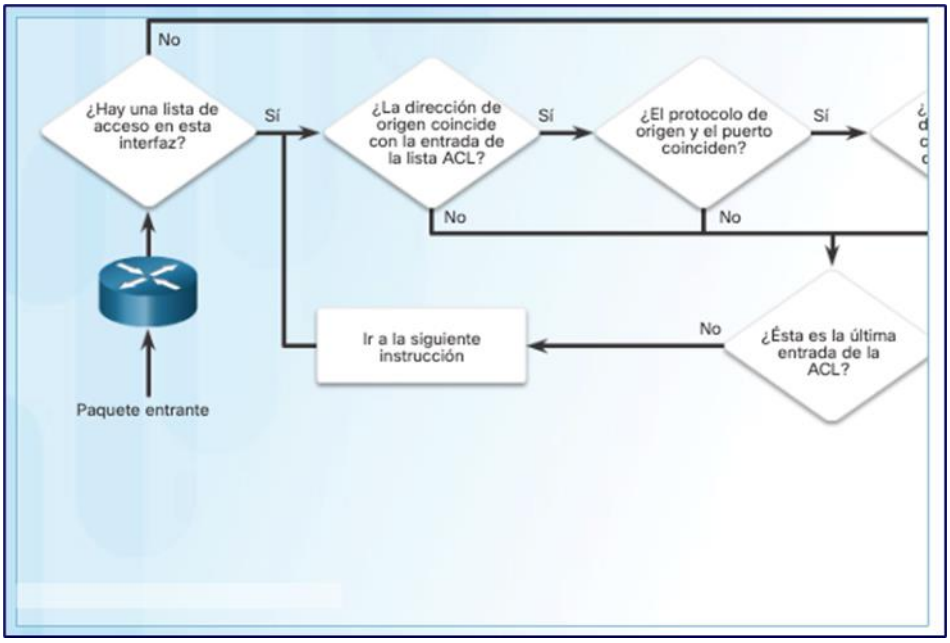


Figura 5: Prueba de paquetes con ACL extendidas.

Fuente: Cisco Networking Academy (2022)

5. Solución de problemas de ACL IPv4 e IPv6

5.1 Solución de problemas de ACL IPv4. Ejemplo 1

Los comandos ***show*** descritos anteriormente sirven para detectar la mayoría de los errores comunes de ACL. Los errores más comunes incluyen introducir las **ACE** (***access control entry*** – entradas de control de acceso) en el orden incorrecto y no aplicar los criterios adecuados a las reglas del ACL.

En la figura 6, el host 192.168.10.10 no tiene conectividad de Telnet con 192.168.30.12. Al observar el resultado del comando ***show access-lists***, se muestran las coincidencias para la primera instrucción ***deny***. Esto indica que la instrucción coincidió con el tráfico.

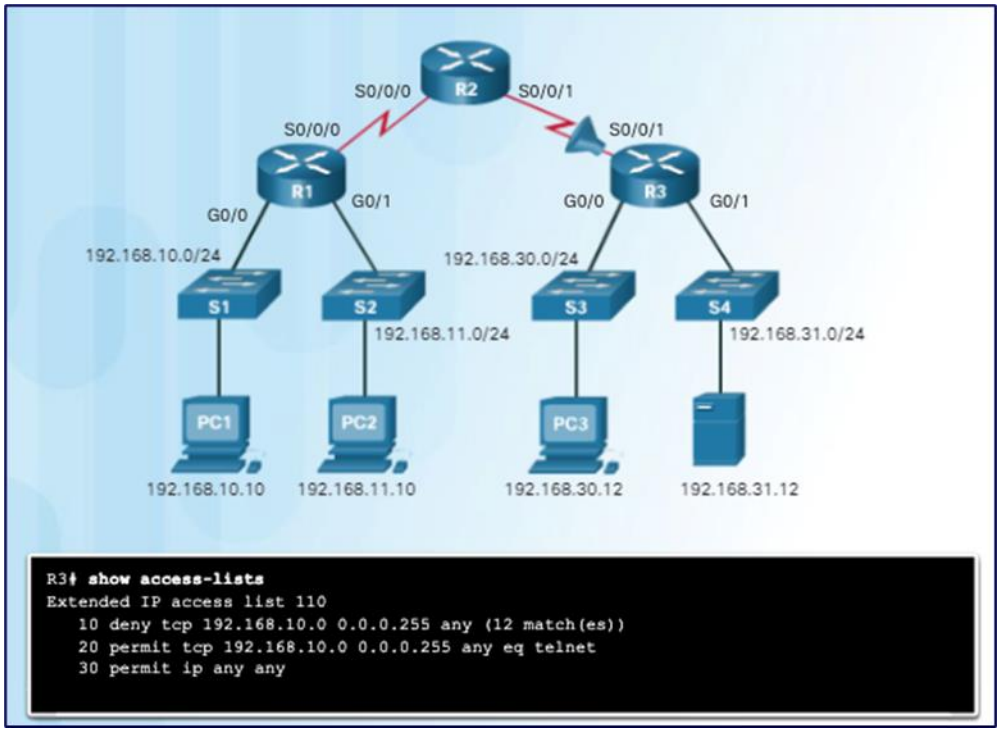


Figura 6: Ejemplo 1 IPv4.

Fuente: Cisco Networking Academy (2022)

Solución: Mire el orden de las ACE. El *host* 192.168.10.10 no tiene conectividad con 192.168.30.12, debido al orden de la regla 10 en la lista de acceso. Dado que el *router* procesa las ACL en orden descendente, la instrucción 10 deniega el *host* 192.168.10.10, por lo que la instrucción 20 nunca puede tener una coincidencia. Las instrucciones 10 y 20 deben invertirse. La última línea permite el resto del tráfico que no es **TCP** y que se clasifica como **IP** (ICMP, UDP, etcétera).

5.2 Solución de problemas de ACL IPv4. Ejemplo 2

En la figura 7, la red 192.168.10.0/24 no puede utilizar **TFTP** para conectarse a la red 192.168.30.0/24.

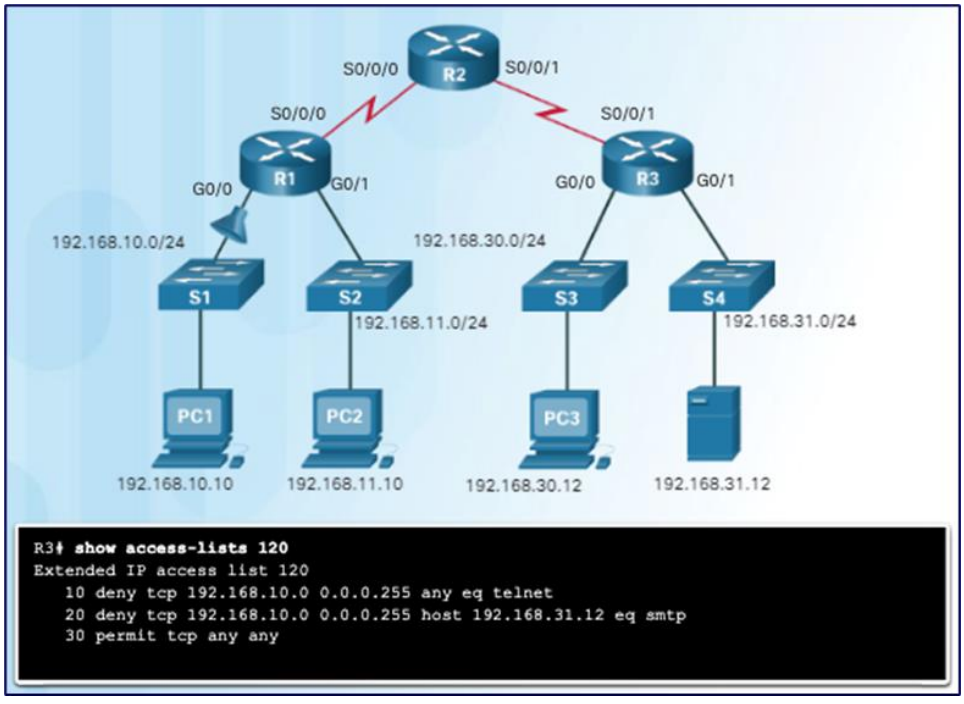


Figura 7: Ejemplo 2 IPv4.

Fuente: Cisco Networking Academy (2022)

Solución: La red 192.168.10.0/24 no puede utilizar TFTP para conectarse a la red 192.168.30.0/24, porque TFTP utiliza el protocolo de transporte **UDP**. La instrucción 30 en la lista de acceso 120 permite todo el resto del tráfico **TCP**. Sin embargo, debido a que TFTP utiliza UDP en lugar de TCP, se deniega implícitamente. Recuerde que la instrucción ***deny any*** implícita no aparece en el resultado del comando ***show access-lists*** y, por lo tanto, las coincidencias no se muestran. La instrucción 30 debería ser ***ip any any***.

Esta ACL funciona si se aplica a G0/0 del R1, a S0/0/1 del R3 o a S0/0/0 del R2 en sentido de entrada. Sin embargo, según la regla que indica colocar las ACL extendidas más cerca del origen, la mejor opción es colocarla en sentido de entrada en G0/0 del R1, porque permite que el tráfico no deseado se filtre sin cruzar la infraestructura de la red.

5.3 Solución de problemas de ACL IPv4. Ejemplo 3

En la figura 8, la red 192.168.11.0/24 puede utilizar **Telnet** para conectarse a 192.168.30.0/24, pero según la política de la empresa, esta conexión no debería permitirse. Los resultados del comando ***show access-lists 130*** indican que se encontró una coincidencia para la instrucción ***permit***.

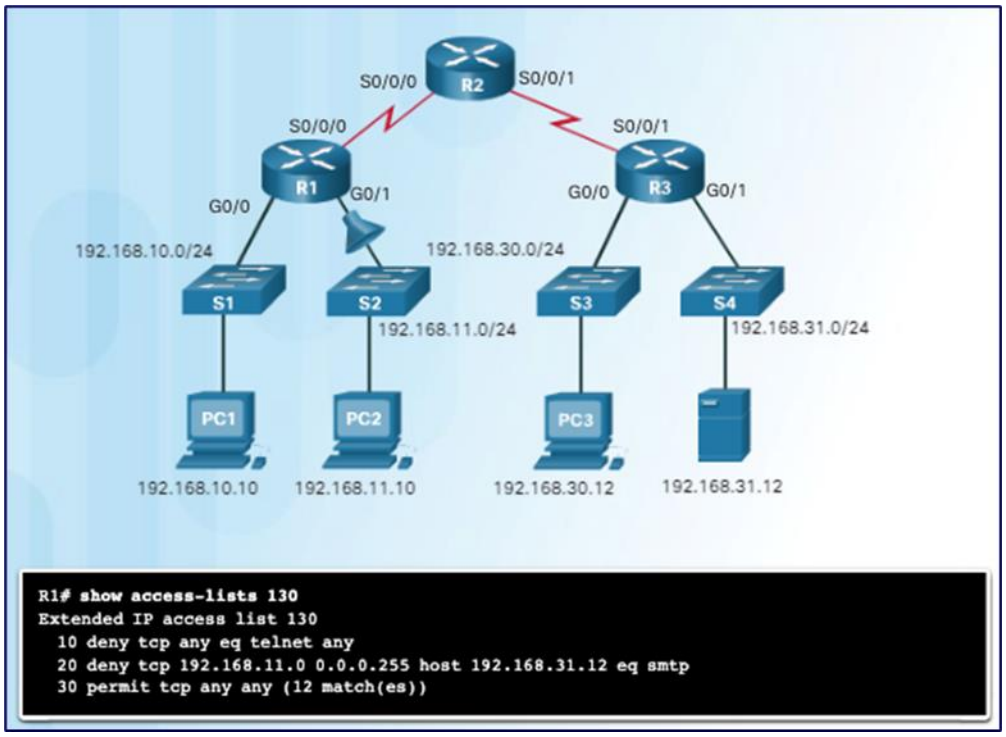


Figura 8: Ejemplo 3 IPv4.

Fuente: Cisco Networking Academy (2022)

Solución: La red 192.168.11.0/24 puede usar Telnet para conectarse a la red 192.168.30.0/24 porque el número de puerto de Telnet de la instrucción 10 de la lista de acceso 130 figura en la posición incorrecta en la instrucción de **ACL**. Actualmente, la instrucción 10 deniega cualquier paquete de origen con un número de puerto que equivalga a Telnet. Para denegar el tráfico de Telnet entrante en G0/1, debe denegar el número de puerto de destino equivalente a Telnet, por ejemplo **10 deny tcp 192.168.11.0 0.0.0.255 192.168.30.0 0.0.0.255 eq telnet**.

5.4 Solución de problemas de ACL IPv4. Ejemplo 4

En la figura 9, el *host* 192.168.30.12 puede conectarse a 192.168.31.12 mediante Telnet, pero la política de la empresa establece que esa conexión no debe permitirse. Los resultados del comando ***show access-lists 140*** indican que se encontró una coincidencia para la instrucción ***permit***.

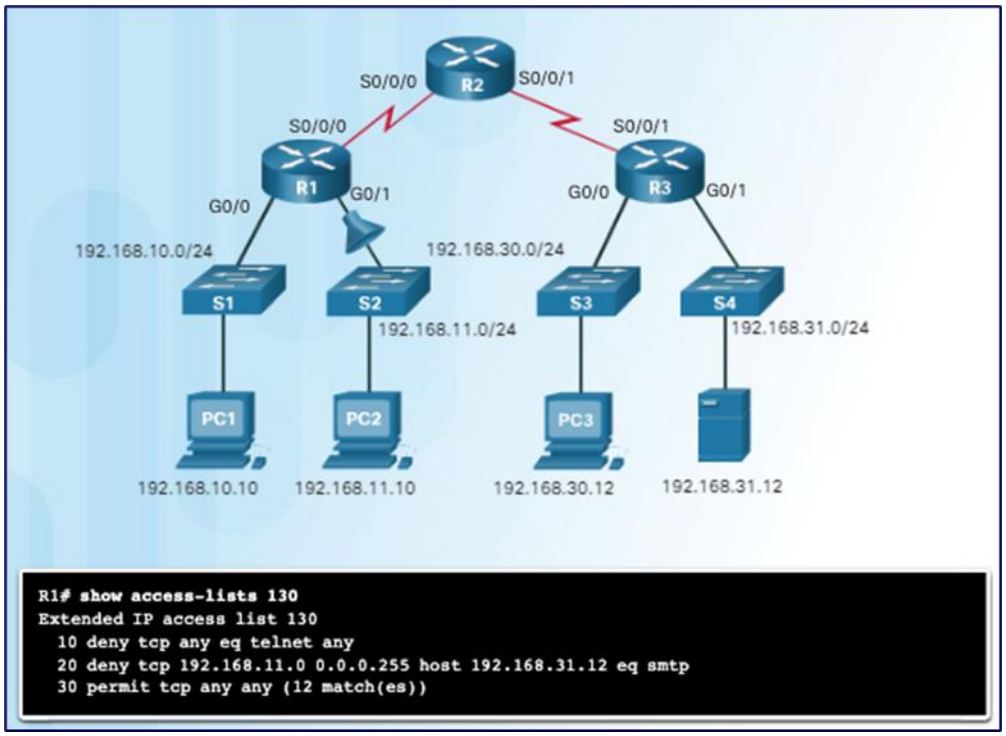


Figura 9: Ejemplo 4 IPv4.

Fuente: Cisco Networking Academy (2022)

Solución: El *host* 192.168.30.12 puede utilizar Telnet para conectarse a 192.168.31.12 porque no hay reglas que denieguen el *host* 192.168.30.12 o su red como origen. La instrucción 10 de la lista de acceso 140 deniega la interfaz del *router* por la que el tráfico ingresa a este. La dirección *host* IPv4 en la instrucción 10 debería ser 192.168.30.12.

5.5 Solución de problemas de ACL IPv4. Ejemplo 5

En la figura 10, el *host* 192.168.30.12 puede utilizar Telnet para conectarse a 192.168.31.12, pero según la política de seguridad esta conexión no debe permitirse. El resultado del comando ***show access-lists 150*** indica que no se encontraron coincidencias para la instrucción ***deny*** según se esperaba.

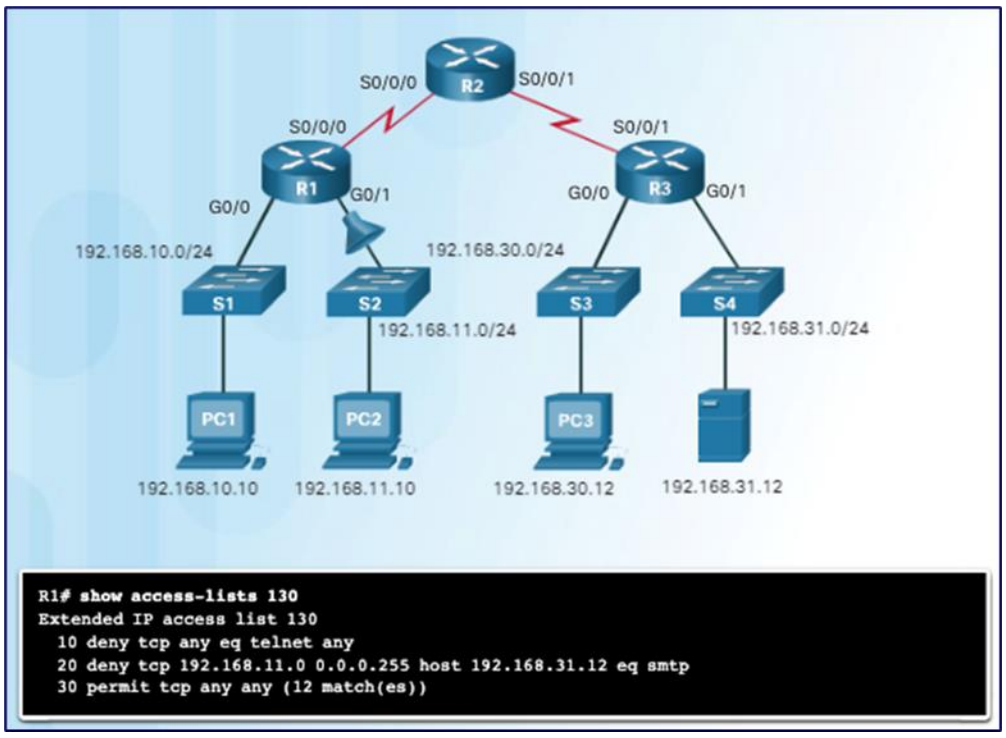


Figura 10: Ejemplo 5 IPv4.

Fuente: Cisco Networking Academy (2022)

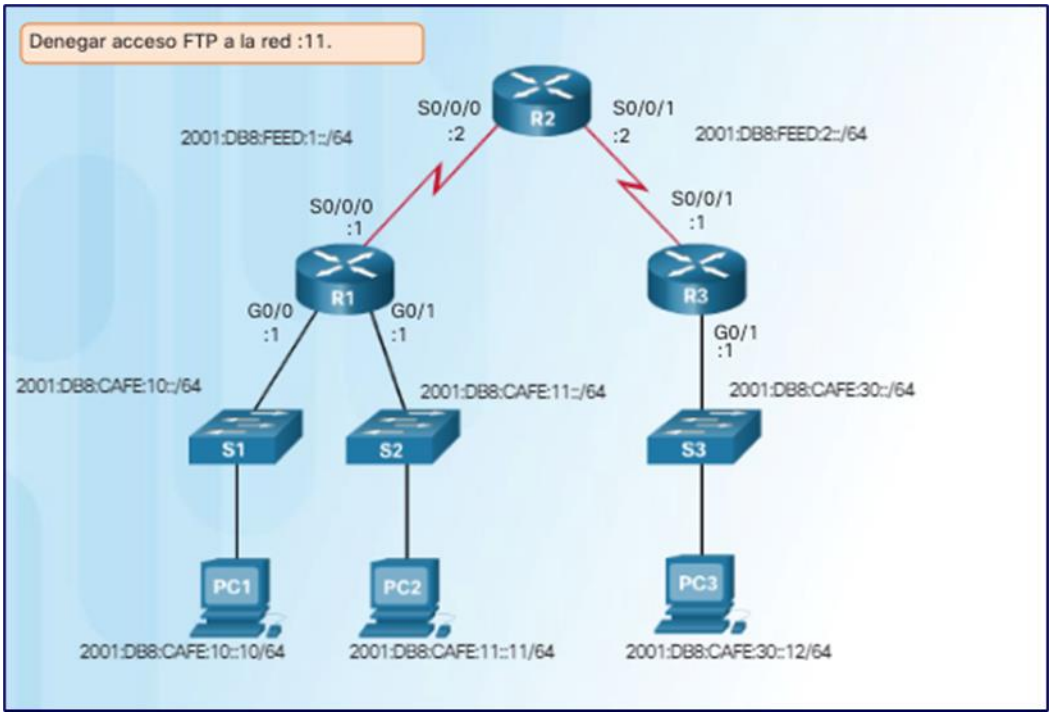
Solución: El *host* 192.168.30.12 puede utilizar Telnet para conectarse a 192.168.31.12, debido al sentido en el que se aplica la lista de acceso 150 a la interfaz G0/1. La instrucción 10 deniega la conexión de todas las direcciones de origen al *host*

192.168.31.12 mediante Telnet. Sin embargo, para un filtrado correcto, este filtro se debe aplicar en sentido de salida en G0/1.

5.6 Solución de problemas de ACL IPv6. Ejemplo 1

Como sucede con ACL IPv4, los comandos ***show ipv6 access-list*** y ***show running-config*** sirven para ver los errores típicos de ACL IPv6.

En la figura 11, R1 está configurado con un ACL IPv6 para denegar el acceso **FTP** de la red :10 a la red :11. Sin embargo, después de configurar la ACL, el PC1 todavía puede conectarse al servidor FTP que se ejecuta en 2. Al consultar la salida del comando ***show ipv6 access-list*** en la figura 12, se muestran las coincidencias para la instrucción de



permitir, pero no para las instrucciones de denegar.

Figura 11: Topología - Ejemplo 1 IPv6.

Fuente: Cisco Networking Academy (2022)

Solución: Las ACE de la ACL no muestran problemas de orden ni de criterio en las reglas. El paso siguiente consiste en considerar cómo se aplica la ACL en la interfaz con el comando ***ipv6 traffic-filter***. ¿La ACL se aplicó utilizando el nombre correcto y la interfaz y dirección correctas? Para comprobar si hay errores de configuración en la interfaz, consulte la configuración en ejecución, como se muestra en la figura 12.

```
R1# show ipv6 access-list
IPv6 access list NO-FTP-TO-11
    deny tcp any 2001:DB8:CAFE:11::/64 eq ftp sequence 10
    deny tcp any 2001:DB8:CAFE:11::/64 eq ftp-data sequence 20
    permit ipv6 any any (11 matches) sequence 30
R1# show running-config | begin interface G
interface GigabitEthernet0/0
 no ip address
 ipv6 traffic-filter NO-FTP-TO-11 out
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:1:10::1/64
 ipv6 eigrp 1
<resultado omitido>
R1#
```

Figura 12: Verificación de configuración - Ejemplo 1 IPv6.

Fuente: Cisco Networking Academy (2022)

La ACL se aplicó con el nombre correcto, pero con una dirección incorrecta. La dirección entrante o saliente se determina desde la perspectiva del *router*, lo que significa que, en este momento, la ACL se aplica al tráfico antes de que se la reenvíe por la interfaz G0/0 e ingrese en la red :10. Para corregir este problema, elimine el comando ***ipv6 traffic-filter NO-FTP-TO-11 out*** y reemplácelo con el comando ***ipv6 traffic-filter NO-FTP-TO-11 in***, como se muestra en la figura 13. Desde ahora, se denegarán los intentos de PC1 de acceder al servidor FTP, como se verificó con el comando ***show ipv6 access-list***.

```
R1(config)# interface g0/0
R1(config-if)# no ipv6 traffic-filter NO-FTP-TO-11 out
R1(config-if)# ipv6 traffic-filter NO-FTP-TO-11 in
R1(config-if)# end
R1#
!PC1 attempts to access the FTP server again.
R1# show ipv6 access-list
IPv6 access list NO-FTP-TO-11
    deny tcp any 2001:DB8:CAFE:11::/64 eq ftp (37 matches) sequence 10
    deny tcp any 2001:DB8:CAFE:11::/64 eq ftp-data sequence 20
    permit ipv6 any any (11 matches) sequence 30
```

Figura 13: Corregir y verificar ACL - Ejemplo 1 IPv6.

Fuente: Cisco Networking Academy (2022)

5.7 Solución de problemas de ACL IPv6. Ejemplo 2

En la figura 14, R3 está configurado con una ACL IPv6 llamada ***RESTRICTED-ACCESS*** que debe aplicar la siguiente política a la LAN de R3:

- Permitir acceso a la red :10
- Denegar acceso a la red :11
- Permitir acceso SSH a el PC en 2001:DB8:CAFE:11::11

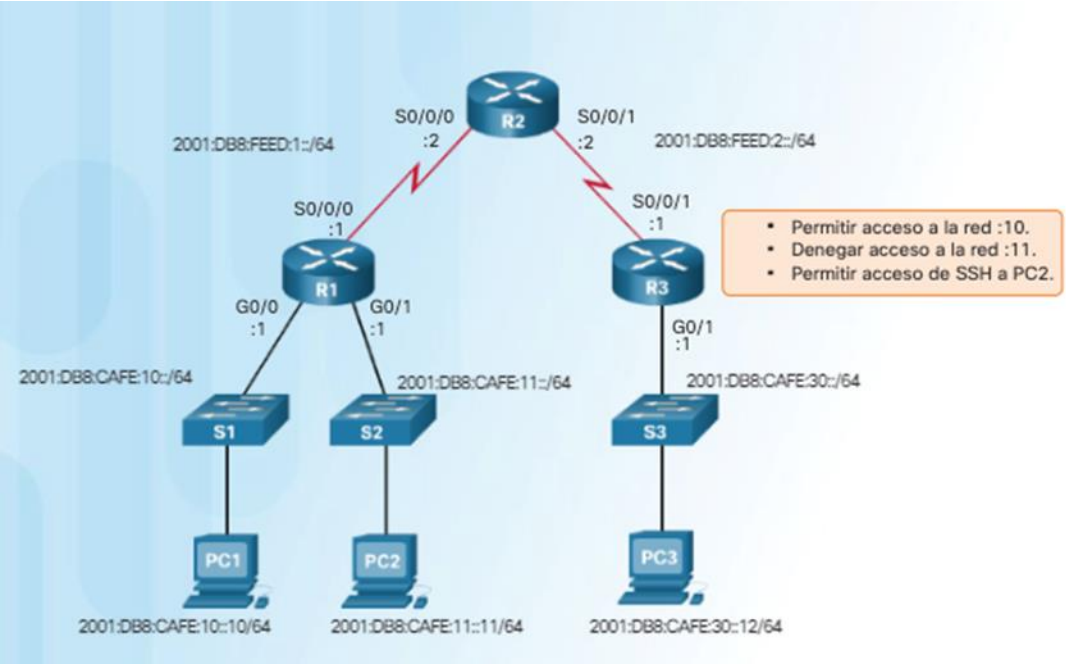


Figura 14: Topología - Ejemplo 2 IPv6.

Fuente: Cisco Networking Academy (2022)

Sin embargo, después de configurar la ACL, el PC3 no puede llegar a la red 10 o la red 11, y no puede utilizar **SSH** en el *host* en 2001:DB8:CAFE:11::11.

Solución: En esta situación, el problema no se debe a cómo se aplicó la ACL. En la interfaz, la ACL no está mal escrita, y la dirección y la ubicación son correctas, como se muestra en la figura 15. Al analizar en detalle la ACL IPv6, se puede notar que el problema está en el orden y los criterios de las reglas de ACE. La primera declaración de permiso debería permitir el acceso a la red :10. Sin embargo, el administrador configuró una instrucción de *host* y no especificó un prefijo. En este caso, se otorga acceso únicamente a 2001:DB8:CAFE:10:: y se permite el *host*.

Figura 15: Verificación de configuración ACL - Ejemplo 2 IPv6.

Fuente: Cisco Networking Academy (2022)

Para corregir este problema, elimine el argumento de *host* y cambie el prefijo /64 a. Puede hacer esto sin eliminar la ACL reemplazando la ACE con el número de secuencia 10, como se muestra en la figura 16.

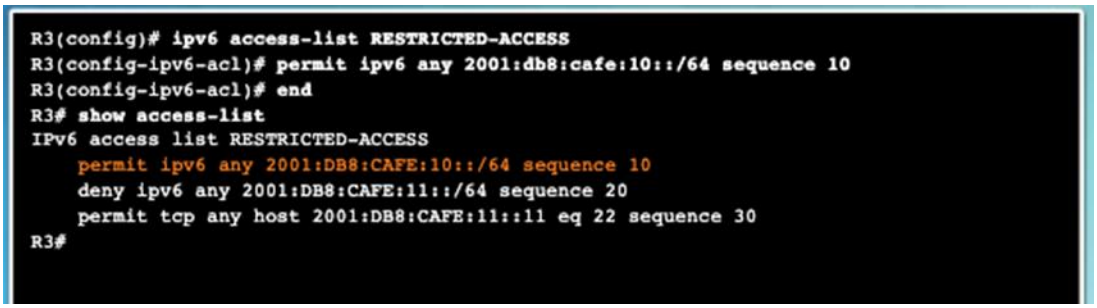


Figura 16: Reemplazar instrucción de host - Ejemplo 2 IPv6.

Fuente: Cisco Networking Academy (2022)

El segundo error en la ACL es el orden de las dos siguientes afirmaciones. La política especifica que los *hosts* en la LAN del R3 deben poder utilizar SSH en el *host* 2001:DB8:CAFE:11::11. Sin embargo, la declaración ***deny*** para la red :11 se encuentra antes de la declaración ***permit***, por lo tanto, todos los intentos para acceder a la red :11 se deniega antes de que la instrucción que permite el acceso de SSH pueda evaluarse. Una vez que se establece una coincidencia, no se analizan otras instrucciones. Para corregir este problema, se deberá eliminar las instrucciones e ingresarlas en el orden correcto, como se muestra en la figura 17.

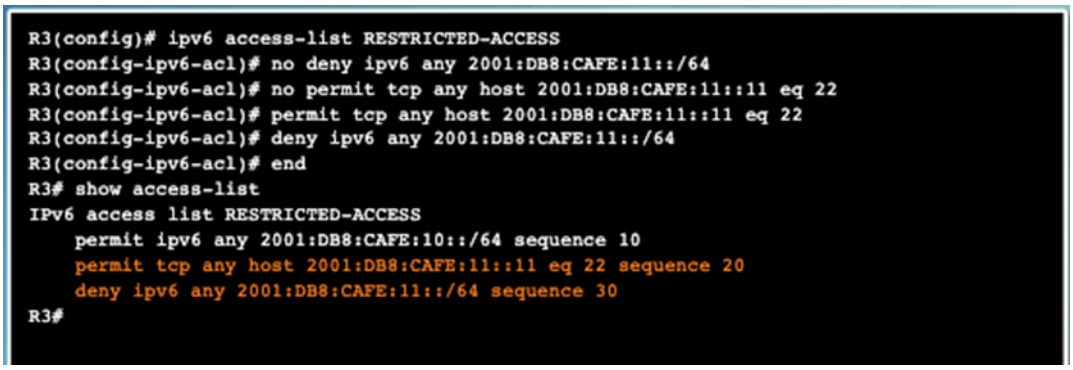


Figura 17: Reordenar las declaraciones - Ejemplo 2 IPv6.

Fuente: Cisco Networking Academy (2022)

5.8 Solución de problemas de ACL IPv6. Ejemplo 3

En la figura 18, R1 está configurado con una ACL IPv6 llamada ***DENY-ACCESS*** que debe aplicar la siguiente política para la LAN de R3:

- Permitir acceso a la red :11 desde la red :30
- Denegar acceso a la red :10

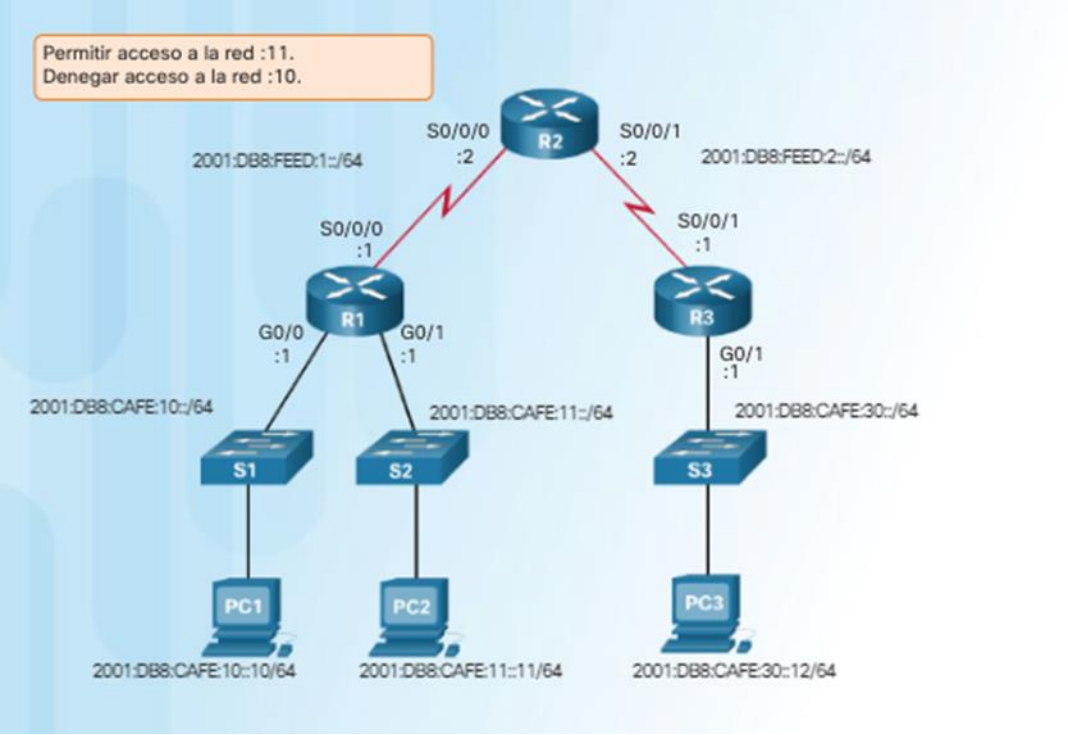


Figura 18: Topología - Ejemplo 3 IPv6.

Fuente: Cisco Networking Academy (2022)

La figura 19 muestra la configuración y la aplicación de la ACL IPv6. La ACL ***DENY-ACCESS*** debe permitir el acceso a la red :11 desde la red :30 y denegar el acceso a la red :10. Sin embargo, después de aplicar la ACL a la interfaz: la red 10 aún es accesible desde la red :30.

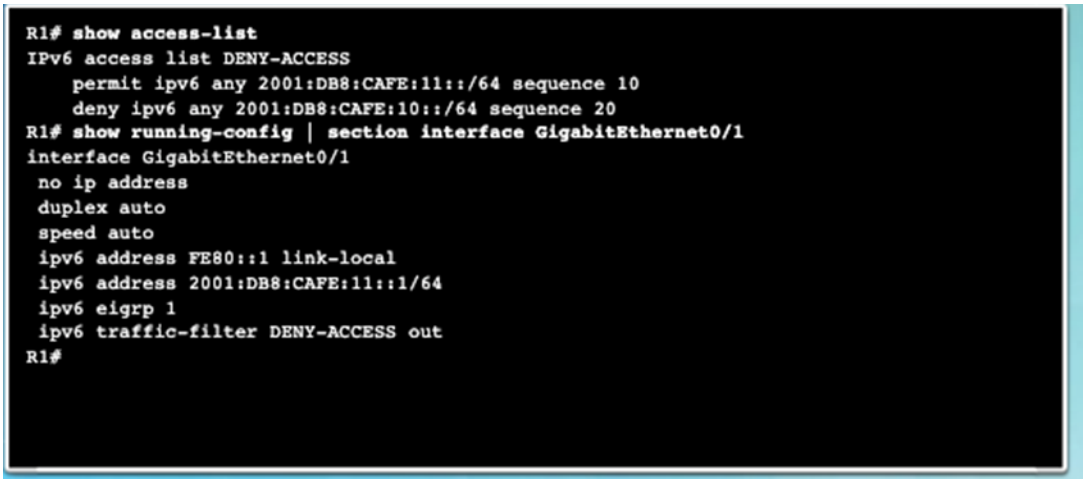


Figura 19: Verificación de configuración y aplicación - Ejemplo 3 IPv6.

Cisco Networking Academy (2022)

Solución: En esta situación, el problema no tiene que ver con la manera en la que se escribieron las instrucciones de las ACL, sino con la ubicación de la ACL. Dado que las ACL de IPv6 deben configurarse con un origen y un destino, debe aplicarse lo más cerca posible del origen del tráfico. La ACL ***DENY-ACCESS*** se aplicó en el sentido saliente en la interfaz G0/1 de R1 que es la que está más cerca del destino. Como resultado, el tráfico a la red :10 no se ve no se ve afectado porque alcanza la red :10 a través de la otra interfaz de la red LAN, G0/0. Puede aplicar la ACL entrante en la interfaz S0/0/0 del R1, sin embargo, al tener control sobre el R3, la mejor ubicación sería configurar y aplicar la ACL lo más cerca posible del origen del tráfico. La figura 20 muestra la eliminación de la ACL en R1 y la configuración y la aplicación correctas de la ACL en R3.

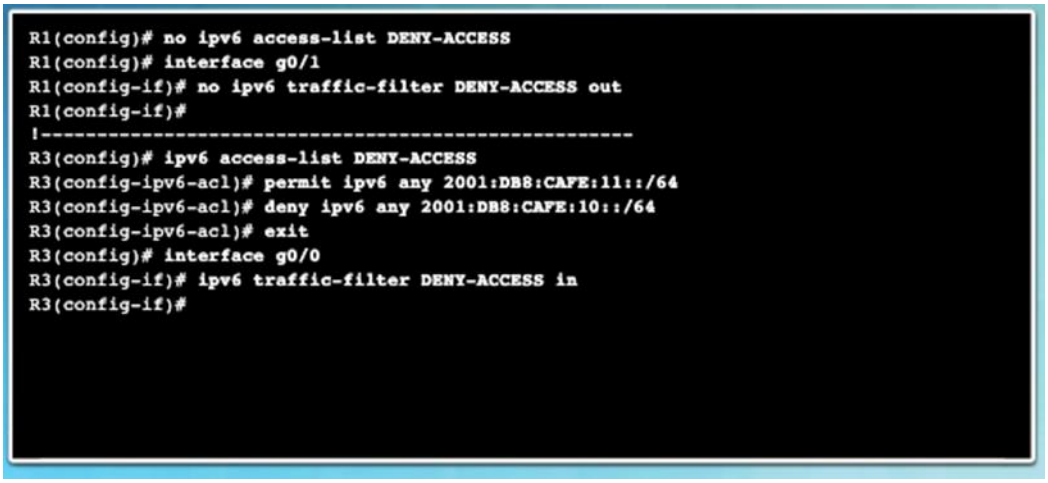


Figura 20: Eliminar ACL en R1 y configurar ACL en R2 - Ejemplo 3 IPv6.

Fuente: Cisco Networking Academy (2022)

Cierre

Cómo dar soluciones a problemas de ACL en IPv4 e IPv6:

Una ACL es una lista secuencial de instrucciones ***permit*** o ***deny***	La última instrucción de una ACL siempre es una denegación implícita de cualquier instrucción que bloquee todo el tráfico	Una vez configurada la ACL, se la vincula a una interfaz con el comando **ip access-group** en modo de configuración de interfaz
Para que la denegación implícita de cualquier instrucción al final de la ACL no bloquee todo el tráfico, se puede agregar la instrucción ***permit ip any any***	Un dispositivo puede tener solo una ACL por protocolo, por dirección y por interfaz.	La regla básica para la colocación de una ACL extendida es colocarla lo más cerca posible del origen
Para eliminar una ACL de una interfaz, primero introduzca el comando **no ip access-group** en la interfaz	El comando **show ip interface** se utiliza para verificar la ACL en la interfaz y el sentido en el que se aplicó.	Los comandos **show running-config** y **show access-lists** sirven para verificar la configuración de ACL

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