# Listas de control de acceso

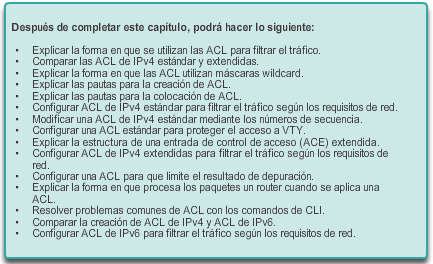
La seguridad de red es un tema muy amplio, y gran parte de este tema se encuentra más allá del ámbito de este curso. Sin embargo, una de las habilidades más importantes que necesita un administrador de red es el dominio de las listas de control de acceso (ACL).

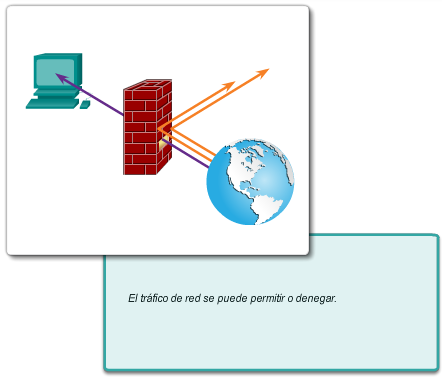
Los diseñadores de red utilizan firewalls para proteger las redes del uso no autorizado. Los firewalls son soluciones de hardware o de software que aplican las políticas de seguridad de la red. Imagine una cerradura en la puerta de una habitación dentro de un edificio. La cerradura permite que solo los usuarios autorizados que poseen una llave o una tarjeta de acceso puedan entrar. De igual forma, un firewall filtra los paquetes no autorizados o potencialmente peligrosos e impide que ingresen a la red. En un router Cisco, puede configurar un firewall simple que proporcione capacidades básicas de filtrado de tráfico mediante ACL. Los administradores utilizan las ACL para detener el tráfico o para permitir solamente tráfico específico en sus redes.

Una ACL es una lista secuencial de instrucciones permit (permitir) o deny (denegar) que se aplican a los protocolos de capa superior o a las direcciones. Las ACL son una herramienta potente para controlar el tráfico hacia y desde la red. Se pueden configurar ACL para todos los protocolos de red enrutada.

El motivo más importante para configurar ACL es aportar seguridad a una red. En este capítulo, se explica cómo utilizar las ACL estándar y 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.

En este capítulo, se ofrece la oportunidad de desarrollar su dominio de las ACL con una serie de lecciones, actividades y ejercicios de práctica de laboratorio.





## Funcionamiento de ACL de IP

### Propósito de los ACLs

Una ACL es una serie de comandos del IOS que controlan si un router reenvía o descarta paquetes según la información que se encuentra en el encabezado del paquete. Las ACL son una de las características del software IOS de Cisco más utilizadas.

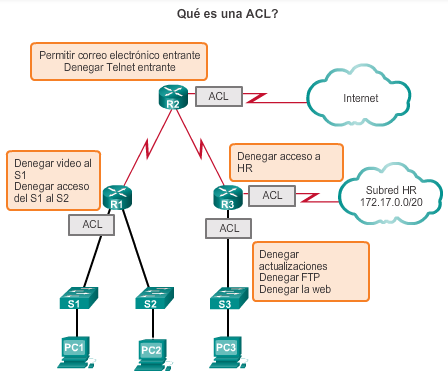
Cuando se las configura, las ACL realizan las siguientes tareas:

* Limitan el tráfico de la red para aumentar su rendimiento. Por ejemplo, si la política corporativa no permite el tráfico de video en la red, se pueden configurar y aplicar ACL que bloqueen el tráfico de video. Esto reduciría considerablemente la carga de la red y aumentaría su rendimiento.
* Proporcionan control del flujo de tráfico. Las ACL pueden restringir la entrega de actualizaciones de routing. Si no se requieren actualizaciones debido a las condiciones de la red, se preserva ancho de banda.
* Proporcionan un nivel básico de seguridad para el acceso a la red. Las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro host acceda a la misma área. Por ejemplo, se puede restringir el acceso a la red de Recursos Humanos a los usuarios autorizados.
* Filtran el tráfico según el tipo de tráfico. Por ejemplo, una ACL puede permitir el tráfico de correo electrónico, pero bloquear todo el tráfico de Telnet.
* Filtran a los hosts para permitirles o denegarles el acceso a los servicios de red. Las ACL pueden permitirles o denegarles a los usuarios el acceso a determinados tipos de archivos, como FTP o HTTP.

Los routers no tienes ACL configuradas de manera predeterminada, por lo que no filtran el tráfico de manera predeterminada. El tráfico que ingresa al router se enruta solamente en función de la información de la tabla de routing. Sin embargo, cuando se aplica una ACL a una interfaz, el router realiza la tarea adicional de evaluar todos los paquetes de red a medida que pasan a través de la interfaz para determinar si el paquete se puede reenviar.

Además de permitir o denegar tráfico, las ACL se pueden utilizar para seleccionar tipos de tráfico para analizar, reenviar o procesar de otras formas. Por ejemplo, se pueden utilizar ACL para clasificar el tráfico a fin de permitir el procesamiento por prioridad. Esta capacidad es similar a tener un pase vip para un concierto o un evento deportivo. El pase vip brinda a ciertos invitados privilegios que no se ofrecen a los asistentes que poseen entradas de admisión general, como prioridad de entrada o el ingreso a un área restringida.

En la ilustración, se muestra una topología de ejemplo a la que se le aplicaron ACL.



Las ACL permiten a los administradores controlar el tráfico hacia y desde la red. Este control puede ser tan simple como permitir o denegar el tráfico según las direcciones de red o tan complejo como controlar el tráfico de la red según el puerto TCP solicitado. Es más fácil comprender cómo filtra el tráfico una ACL si se examina el diálogo que se produce durante una conversación TCP, por ejemplo, cuando se solicita una página web.

**Comunicación TCP**

Cuando un cliente solicita datos a un servidor web, IP administra la comunicación entre la computadora (origen) y el servidor (destino). TCP administra la comunicación entre el navegador web (aplicación) y el software del servidor de red.

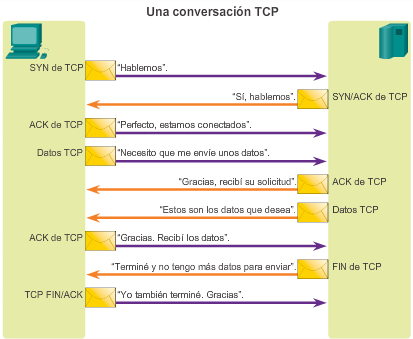
Cuando envía un correo electrónico, observa una página web o descarga un archivo, TCP se encarga de descomponer los datos en segmentos para IP antes de que se envíen. TCP también administra el montaje de los datos de los segmentos cuando estos llegan. El proceso de TCP es similar a una conversación en la que dos nodos en una red acuerdan transmitirse datos entre sí.

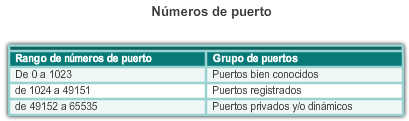
TCP proporciona un servicio de flujo de bytes confiable y orientado a la conexión. Que sea orientado a la conexión significa que las dos aplicaciones deben establecer una conexión TCP antes de intercambiar datos. TCP es un protocolo full-duplex, lo que significa que cada conexión TCP admite un par de flujos de bytes, y cada flujo fluye en una sentido. TCP incluye un mecanismo de control del flujo para cada flujo de bytes que permite que el receptor limite la cantidad de datos que puede transmitir el emisor. TCP también implementa un mecanismo de control de la congestión.

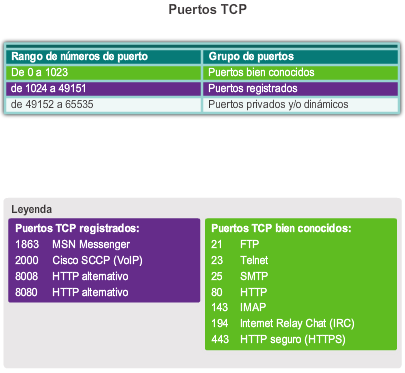
En la animación que se muestra en la figura 1, se ilustra cómo se lleva a cabo una conversación TCP/IP. Los segmentos TCP se marcan con indicadores que denotan su objetivo: la sesión comienza (se sincroniza) con un indicador SYN, el indicador ACK es un acuse de recibo de un segmento esperado, y un indicador FIN finaliza la sesión. Un indicador SYN/ACK confirma que la transferencia está sincronizada. Los segmentos de datos TCP incluyen el protocolo del nivel más alto necesario para dirigir los datos de aplicación a la aplicación correcta.

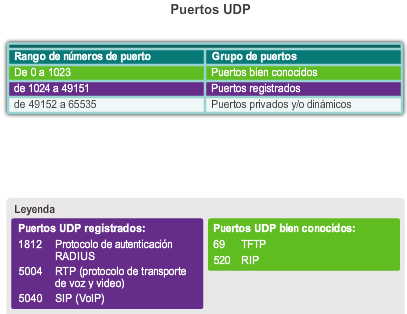
Los segmentos de datos TCP también identifican el puerto que coincide con el servicio solicitado. Por ejemplo, para HTTP es el puerto 80, para SMTP es el puerto 25 y para FTP son los puertos 20 y 21. En la figura 2, se muestran los rangos de puertos UDP y TCP.

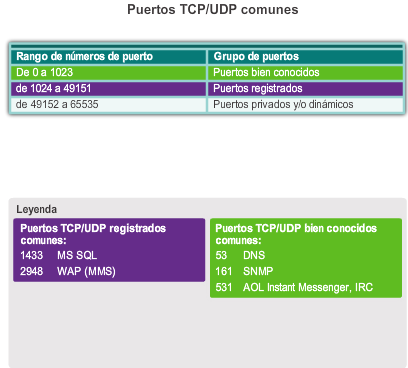
En las figuras 3 a 5, se exploran los puertos TCP/UDP.











Entonces, ¿cómo es que una ACL utiliza la información transferida durante una conversación TCP/IP para filtrar tráfico?

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. Cuando llega un paquete a un router que filtra paquetes, el router extrae cierta información del encabezado. Con esta información, el router decide si el paquete puede pasar o si se debe descartar, según las reglas de los filtros configurados. Como se muestra en la ilustración, el filtrado de paquetes puede operar en diversas capas del modelo OSI o en la capa de Internet de TCP/IP.

Un router que filtra paquetes utiliza reglas para determinar si permite o deniega el tráfico. Un router también puede realizar el filtrado de paquetes en la capa 4, la capa de transporte. El router puede filtrar paquetes según el puerto de origen y de destino del segmento TCP o UDP. Estas reglas se definen mediante el uso de ACL.

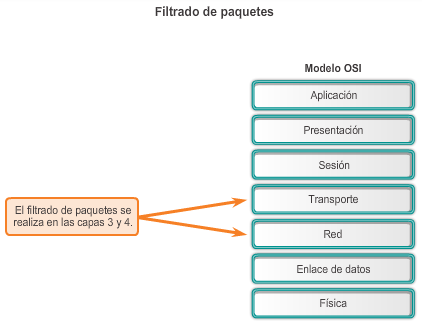
Una ACL es una lista secuencial de instrucciones permit (permitir) o deny (denegar), conocidas como “entradas de control de acceso” (ACE). Las ACE también se denominan comúnmente “instrucciones de ACL”. Las ACE se pueden crear para filtrar tráfico según ciertos criterios, como la dirección de origen, la dirección de destino, el protocolo y los números de puerto. Cuando el tráfico de la red atraviesa una interfaz configurada con una ACL, el router compara la información dentro del paquete con cada ACE, en orden secuencial, para determinar si el paquete coincide con una de las instrucciones. Si se encuentra una coincidencia, el paquete se procesa según corresponda. De esta manera, se pueden configurar ACL para controlar el acceso a una red o a una subred.

Para evaluar el tráfico de la red, la ACL extrae la siguiente información del encabezado de capa 3 del paquete:

* Dirección IP de origen
* Dirección IP de destino
* Tipo de mensaje ICMP

La ACL también puede extraer información de capa superior del encabezado de capa 4, incluido lo siguiente:

* Puerto de origen TCP/UDP
* Puerto de destino TCP/UDP



**Ejemplo del filtrado de paquetes**

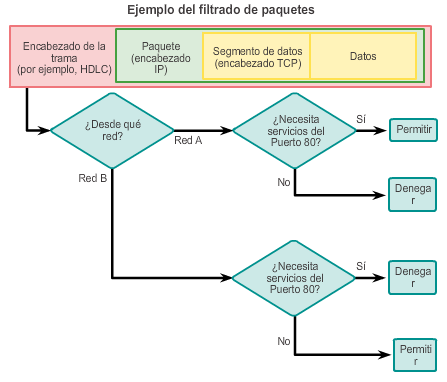
Para entender el concepto de cómo utiliza el router el filtrado de paquetes, imagine que se coloca un guarda en una puerta cerrada con llave. Las instrucciones del guarda son que solo permita el acceso por esa puerta a aquellas personas cuyos nombres aparecen en una lista. El guarda filtra las personas según el criterio de que los nombres aparezcan en la lista autorizada. Las ACL funcionan de manera similar: toman decisiones sobre la base de criterios establecidos.

Por ejemplo, una ACL se puede configurar para “permitir el acceso web a los usuarios de la red A, pero denegar el resto de los servicios a los usuarios de esa red. Denegar el acceso HTTP a los usuarios de la red B, pero permitir que los usuarios de esa red tengan todos los otros tipos de acceso”, de manera lógica. Consulte la ilustración para examinar la ruta de decisión que utiliza el filtro de paquetes para llevar a cabo esta tarea.

Para esta situación, el filtro de paquetes examina cada paquete de la siguiente manera:

* Si el paquete es un SYN de TCP de la red A que utiliza el puerto 80, tiene permiso para pasar. El resto de los tipos de acceso se deniega a esos usuarios.
* Si el paquete es un SYN de TCP de la red B que utiliza el puerto 80, se bloquea. Sin embargo, se permite el resto de los tipos de acceso.

Este es solo un ejemplo sencillo. Se pueden configurar varias reglas para permitir o denegar otros servicios a usuarios específicos.



Las ACL definen el conjunto de reglas que proporcionan un control adicional para los paquetes que ingresan por las interfaces de entrada, para los que retransmiten a través del router y para los que salen por las interfaces de salida del router. Las ACL no operan sobre paquetes que se originan en el router mismo.

Las ACL se configuran para aplicarse al tráfico entrante o al tráfico saliente

* **ACL de entrada:** los paquetes entrantes se procesan antes de enrutarse a la interfaz de salida. Son eficaces, porque ahorran la sobrecarga de enrutar búsquedas si el paquete se descarta. Si las pruebas permiten el paquete, este se procesa para el routing. Las ACL de entrada son ideales para filtrar los paquetes cuando la red conectada a una interfaz de entrada es el único origen de los paquetes que se deben examinar.
* **ACL de salida:** los paquetes entrantes se enrutan a la interfaz de salida y después se procesan mediante la ACL de salida. Las ACL de salida son ideales cuando se aplica el mismo filtro a los paquetes que provienen de varias interfaces de entrada antes de salir por la misma interfaz de salida.

La última sentencia de una ACL es siempre una denegación implícita. Esta sentencia se inserta automáticamente al final de cada ACL, aunque no esté presente físicamente. La denegación implícita bloquea todo el tráfico. Debido a esta denegación implícita, una ACL que no tiene, por lo menos, una instrucción permit bloqueará todo el tráfico.



### Comparación entre ACL de IPv4 estándar y extendidas

Los dos tipos de ACL de IPv4 de Cisco son estándar y extendida.

**Nota:** las ACL de IPv6 de Cisco son similares a las ACL de IPv4 extendidas y se abordarán en una sección posterior.

**ACL estándar**

Las ACL estándar se pueden utilizar para permitir o denegar el tráfico de direcciones IPv4 de origen únicamente. El destino del paquete y los puertos involucrados no se evalúan. En el ejemplo de la figura 1, se permite todo el tráfico de la red 192.168.30.0/24. Debido al “deny any” (denegar todo) implícito al final, todo el resto del tráfico se bloquea con esta ACL. Las ACL estándar se crean en el modo de configuración global.

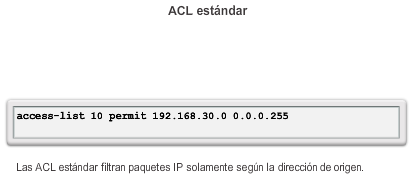
**ACL extendidas**

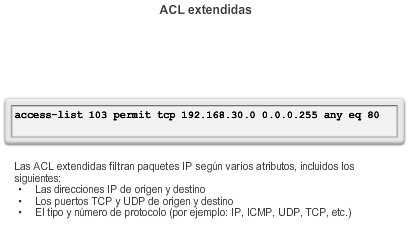
Las ACL extendidas filtran paquetes IPv4 según varios atributos:

* Tipo de protocolo
* Dirección IPv4 de origen
* Dirección IPv4 de destino
* Puertos TCP o UDP de origen
* Puertos TCP o UDP de destino
* Información optativa de tipo de protocolo para un control más preciso

En la figura 2, la ACL 103 permite el tráfico que se origina desde cualquier dirección en la red 192.168.30.0/24 hasta cualquier red IPv4 si el puerto de host de destino es 80 (HTTP). Las ACL extendidas se crean en el modo de configuración global.

Los comandos para las ACL se abordan en los siguientes temas.



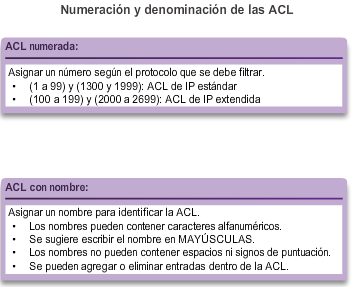


Las ACL estándar y extendidas se pueden crear con un número o un nombre para identificar la ACL y su lista de instrucciones.

El uso de ACL numeradas es un método eficaz para determinar el tipo de ACL en redes más pequeñas con tráfico definido de forma más homogénea. Sin embargo, un número no proporciona información sobre el propósito de la ACL. Por este motivo, a partir de la versión 11.2 del IOS de Cisco, se puede utilizar un nombre para identificar una ACL de Cisco.

En la ilustración, se resumen las reglas que se deben seguir para designar las ACL.

En relación con las ACL numeradas, se omiten los números del 200 al 1299 debido a que esos números los utilizan otros protocolos, muchos de los cuales son antiguos u obsoletos. Este curso se centra solamente en las ACL de IP. Algunos ejemplos de números de protocolos ACL antiguos van del 600 al 699, utilizados por AppleTalk y del 800 al 899, utilizados por IPX.



### Máscaras wildcard en ACL

**Máscara wildcard**

Las ACE de IPv4 incluyen el uso de máscaras wildcard. Una máscara wildcard es una cadena de 32 dígitos binarios que el router utiliza para determinar los bits de la dirección que debe examinar para encontrar una coincidencia.

**Nota:** a diferencia de las ACL de IPv4, las ACL de IPv6 no utilizan máscaras wildcard. En cambio, se utiliza la longitud de prefijo para indicar cuánto de una dirección IPv6 de origen o destino debe coincidir. Las ACL de IPv6 se analizan más adelante en este capítulo.

Como ocurre con las máscaras de subred, los números 1 y 0 en la máscara wildcard identifican lo que hay que hacer con los bits de dirección IP correspondientes. Sin embargo, en una máscara wildcard, estos bits se utilizan para fines diferentes y siguen diferentes reglas.

Las máscaras de subred utilizan unos y ceros binarios para identificar la red, la subred y la porción de host de una dirección IP. Las máscaras wildcard utilizan unos y ceros binarios para filtrar direcciones IP individuales o grupos de direcciones IP para permitir o denegar el acceso a los recursos.

Las máscaras wildcard y las máscaras de subred se diferencian en la forma en que establecen la coincidencia entre los unos y ceros binarios. Las máscaras wildcard utilizan las siguientes reglas para establecer la coincidencia entre los unos y ceros binarios:

* Bit 0 de máscara wildcard: se establecer la coincidencia con el valor del bit correspondiente en la dirección.
* Bit 1 de máscara wildcard: se omite el valor del bit correspondiente en la dirección.

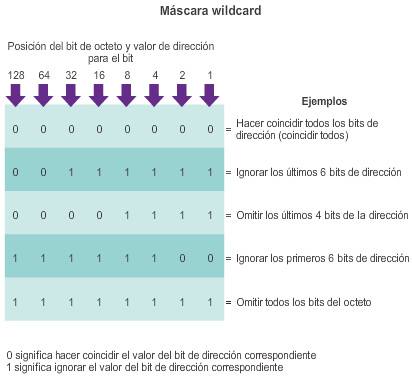
En la figura 1, se muestra cómo las diferentes máscaras wildcard filtran las direcciones IP. Recuerde que, en el ejemplo, el valor binario 0 indica un bit que debe coincidir y el valor binario 1 indica un bit que se puede ignorar.

**Nota:** a las máscaras wildcard a menudo se las denomina “máscaras inversas”. La razón es que, a diferencia de una máscara de subred en la que el 1 binario equivale a una coincidencia y el 0 binario no es una coincidencia, en las máscaras wildcard es al revés.

**Uso de una máscara wildcard**

En la tabla de la figura 2, se muestran los resultados de la aplicación de una máscara wildcard 0.0.255.255 a una dirección IPv4 de 32 bits. Recuerde que un 0 binario indica un valor con coincidencia.

Las máscaras wildcard también se utilizan para configurar algunos protocolos de routing IPv4, como OSPF, a fin de habilitar el protocolo en interfaces específicas.





**Máscaras wildcard para establecer coincidencias con subredes IPv4**

Se necesita práctica para calcular la máscara wildcard. En la figura 1, se proporcionan tres ejemplos de máscara wildcard.

En el primer ejemplo, la máscara wildcard estipula que cada bit en la IPv4 192.168.1.1 debe coincidir con exactitud.

En el segundo ejemplo, la máscara wildcard estipula que no habrá coincidencias.

En el tercer ejemplo, la máscara wildcard estipula que cualquier host dentro de la red 192.168.1.0/24 tendrá una coincidencia.

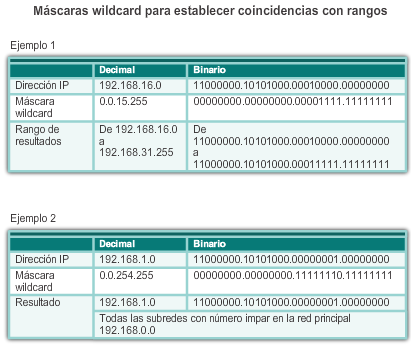
Estos ejemplos son bastante simples y directos. Sin embargo, el cálculo de máscaras wildcard puede ser más complejo.

**Máscaras wildcard para establecer coincidencias con rangos**

Los dos ejemplos en la figura 2 son más complejos. En el ejemplo 1, los primeros dos octetos y los primeros cuatro bits del tercer octeto deben coincidir con exactitud. Los cuatro últimos bits del tercer octeto y el último octeto pueden ser cualquier número válido. Esto genera una máscara que verifica el rango de redes 192.168.16.0 a 192.168.31.0.

En el ejemplo 2, se muestra una máscara wildcard que coincide con los primeros dos octetos y el bit con menor importancia del tercer octeto. El último octeto y los primeros siete bits en el tercer octeto pueden ser cualquier número válido. Esto genera una máscara que permite o deniega todos los hosts de subredes impares de la red principal 192.168.0.0.





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

**Cálculo de máscara wildcard: ejemplo 1**

En el primer ejemplo en la ilustración, suponga que desea permitir el acceso a todos los usuarios en la red 192.168.3.0. Dado que la máscara de subred es 255.255.255.0, podría tomar 255.255.255.255 y restarle la máscara de subred 255.255.255.0. El resultado genera la máscara wildcard 0.0.0.255.

**Cálculo de máscara wildcard: ejemplo 2**

En el segundo ejemplo en la ilustración, suponga que desea permitir el acceso a la red a los 14 usuarios en la subred 192.168.3.32/28. La máscara de subred para la subred IP es 255.255.255.240; por lo tanto, tome 255.255.255.255 y réstele la máscara de subred 255.255.255.240. Esta vez, el resultado genera la máscara wildcard 0.0.0.15.

**Cálculo de máscara wildcard: ejemplo 3**

En el tercer ejemplo en la ilustración, suponga que solo quiere establecer la coincidencia con las redes 192.168.10.0 y 192.168.11.0. Una vez más, tome 255.255.255.255 y reste la máscara de subred regular que, en este caso, es 255.255.252.0. El resultado es 0.0.3.255.

Puede lograr el mismo resultado con instrucciones como las dos que se muestran a continuación:

R1(config)# **access-list 10 permit 192.168.10.0**

R1(config)# **access-list 10 permit 192.168.11.0**

Resulta mucho más eficaz configurar la máscara wildcard de la siguiente manera:

R1(config)# **access-list 10 permit 192.168.10.0 0.0.3.255**

Tenga en cuenta la configuración que se indica a continuación para establecer coincidencias con las redes en el rango entre 192.168.16.0 y 192.168.31.0:

R1(config)# **access-list 10 permit 192.168.16.0**

R1(config)# **access-list 10 permit 192.168.17.0**

R1(config)# **access-list 10 permit 192.168.18.0**

R1(config)# **access-list 10 permit 192.168.19.0**

R1(config)# **access-list 10 permit 192.168.20.0**

R1(config)# **access-list 10 permit 192.168.21.0**

R1(config)# **access-list 10 permit 192.168.22.0**

R1(config)# **access-list 10 permit 192.168.23.0**

R1(config)# **access-list 10 permit 192.168.24.0**

R1(config)# **access-list 10 permit 192.168.25.0**

R1(config)# **access-list 10 permit 192.168.26.0**

R1(config)# **access-list 10 permit 192.168.27.0**

R1(config)# **access-list 10 permit 192.168.28.0**

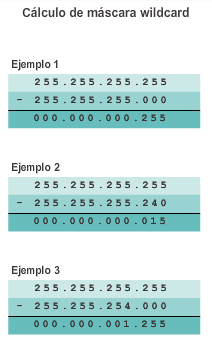
R1(config)# **access-list 10 permit 192.168.29.0**

R1(config)# **access-list 10 permit 192.168.30.0**

R1(config)# **access-list 10 permit 192.168.31.0**

Las 16 instrucciones de configuración indicadas anteriormente se pueden reducir a una sola instrucción con la máscara wildcard correcta, como se muestra a continuación:

R1(config)# **access-list 10 permit 192.168.16.0 0.0.15.255**



**Palabras clave de la máscara de bits wildcard**

Trabajar con representaciones decimales de los bits binarios de máscaras wildcard puede ser tedioso. Para simplificar esta tarea, las palabras clave**host**y**any**ayudan a identificar los usos más comunes de las máscaras wildcard. Estas palabras clave eliminan la necesidad de introducir máscaras wildcard para identificar un host específico o toda una red. También facilitan la lectura de una ACL, ya que proporcionan pistas visuales en cuanto al origen o el destino de los criterios.

La palabra clave**host**reemplaza la máscara 0.0.0.0. Esta máscara indica que todos los bits de direcciones IPv4 deben coincidir o que solo un host coincide.

La opción **any** sustituye la dirección IP y la máscara 255.255.255.255. Esta máscara establece que se omita la dirección IPv4 completa o que se acepte cualquier dirección.

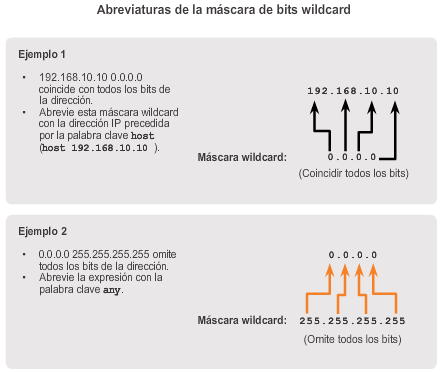
**Ejemplo 1: proceso de máscara wildcard con una única dirección IP**

En el ejemplo 1 en la ilustración, en vez de introducir **192.168.10.10 0.0.0.0**, puede utilizar **host 192.168.10.10**.

**Ejemplo 2: proceso de máscara wildcard con coincidencia con cualquier dirección IP**

En el ejemplo 2 en la ilustración, en vez de introducir **0.0.0.0 255.255.255.255**, puede utilizar la palabra clave**any**(cualquier) sola.

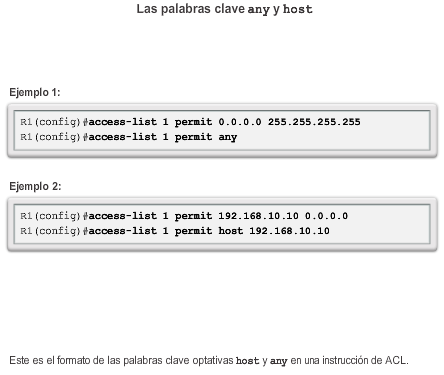
**Nota:** Las palabras clave **host** y**any** solo se pueden utilizar al configurar una ACL de IPv6.



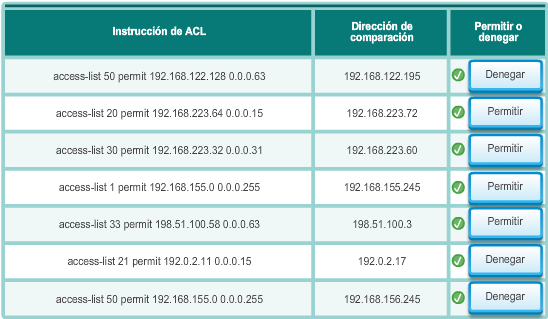
**Las palabras** **clave any** **y host**

En el ejemplo 1 en la ilustración, se muestra cómo utilizar la palabra clave**any**para sustituir la dirección IPv4 0.0.0.0 por una máscara wildcard 255.255.255.255.

En el ejemplo 2, se muestra cómo utilizar la palabra clave**host**para sustituir la máscara wildcard para identificar un único host.







### Pautas para la creación de ACL

La composición de ACL puede ser una tarea compleja. Para cada interfaz, puede haber varias políticas necesarias para administrar el tipo de tráfico que tiene permitido ingresar a la interfaz o salir de ella. El router en la ilustración tiene dos interfaces configuradas para IPv4 e IPv6. Si necesitáramos ACL para ambos protocolos, en ambas interfaces y en ambos sentidos, esto requeriría ocho ACL diferentes. Cada interfaz tendría cuatro ACL: dos ACL para IPv4 y dos ACL para IPv6. Para cada protocolo, una ACL es para el tráfico entrante y otra para el tráfico saliente.

**Nota:** las ACL no deben configurarse en ambos sentidos. La cantidad de ACL y el sentido aplicado a la interfaz dependen de los requisitos que se implementen.

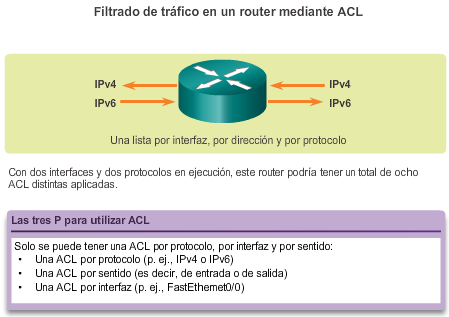
Las siguientes son algunas pautas para el uso de ACL:

* Utilice las ACL en los routers de firewall ubicados entre su red interna y una red externa.
* Utilice las ACL en un router ubicado entre dos partes de la red para controlar el tráfico que entra a una parte específica de su red interna o que sale de esta.
* Configure las ACL en los routers de frontera, es decir, los routers ubicados en los límites de las redes. Esto proporciona una separación muy básica de la red externa o entre un área menos controlada y un área más importante de su propia red.
* Configure las ACL para cada protocolo de red configurado en las interfaces del router de frontera.

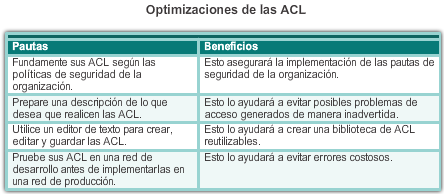
**Las tres P**

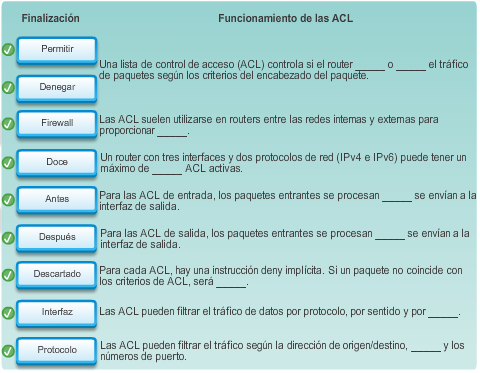
Para recordar una regla general de aplicación de ACL en un router, puede pensar en “las tres P”. Se puede configurar una ACL por protocolo, por sentido y por interfaz:

* **Una ACL por protocolo:** para controlar el flujo de tráfico en una interfaz, se debe definir una ACL para cada protocolo habilitado en la interfaz.
* **Una ACL por sentido:** las ACL controlan el tráfico en una interfaz de a un sentido por vez. Se deben crear dos ACL diferentes para controlar el tráfico entrante y saliente.
* **Una ACL por interfaz:** las ACL controlan el tráfico para una interfaz, por ejemplo, GigabitEthernet 0/0.



El uso de las ACL requiere prestar atención a los detalles y un extremo cuidado. Los errores pueden ser costosos en términos de tiempo de inactividad, esfuerzos de resolución de problemas y servicio de red deficiente. Antes de configurar una ACL, se requiere una planificación básica. En la ilustración, se presentan pautas que constituyen la base de una lista de prácticas recomendadas para ACL.





### Pautas para la colocación de ACL

La correcta colocación de las ACL puede contribuir a que la red funcione de forma más eficaz. Se puede colocar una ACL para reducir el tráfico innecesario. Por ejemplo, el tráfico que se denegará en un destino remoto no se debe reenviar mediante recursos de red por la ruta hacia ese destino.

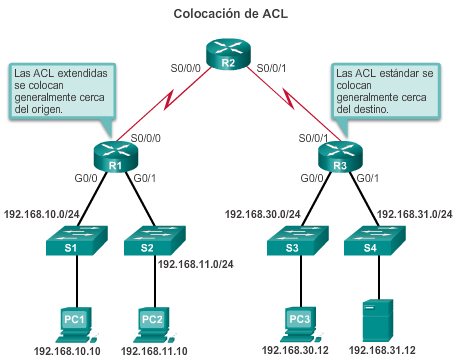
Cada ACL se debe colocar donde tenga más impacto en la eficiencia. Como se muestra en la ilustración, las reglas básicas son las siguientes:

* **ACL extendidas:** coloque las ACL extendidas lo más cerca posible del origen del tráfico que se filtrará. De esta manera, el tráfico no deseado se deniega cerca de la red de origen, sin que cruce la infraestructura de red.
* **ACL estándar:** debido a que en las ACL estándar no se especifican las direcciones de destino, colóquelas tan cerca del destino como sea posible. Si coloca una ACL estándar en el origen del tráfico, evitará de forma eficaz que ese tráfico llegue a cualquier otra red a través de la interfaz a la que se aplica la ACL.

La colocación de la ACL y, por lo tanto, el tipo de ACL que se utiliza también puede depender de lo siguiente:

* **Alcance del control del administrador de la red:** la colocación de la ACL puede depender de si el administrador de red controla tanto la red de origen como la de destino o no.
* **Ancho de banda de las redes involucradas:** el filtrado del tráfico no deseado en el origen impide la transmisión de ese tráfico antes de que consuma ancho de banda en la ruta hacia un destino. Esto es de especial importancia en redes con un ancho de banda bajo.
* **Facilidad de configuración:** si un administrador de red desea denegar el tráfico proveniente de varias redes, una opción es utilizar una única ACL estándar en el router más cercano al destino. La desventaja es que el tráfico de dichas redes utilizará ancho de banda de manera innecesaria. Se puede utilizar una ACL extendida en cada router donde se origina tráfico. Esto ahorra ancho de banda, ya que el tráfico se filtra en el origen, pero requiere la creación de ACL extendidas en varios routers.

**Nota:** para la certificación CCNA, la regla general es que las ACL extendidas se coloquen lo más cerca posible del origen y que las ACL estándar se coloquen lo más cerca posible del destino.



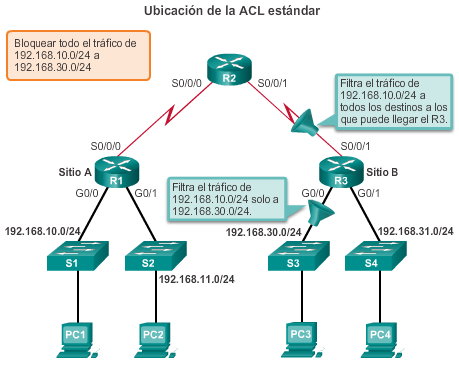
Las ACL estándar solo pueden filtrar tráfico según la dirección de origen. La regla básica para la colocación de una ACL estándar es colocar la ACL lo más cerca posible de la red de destino. Esto permite que el tráfico llegue a todas las demás redes, excepto la red que filtra los paquetes.

En la ilustración, 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.

Si la ACL estándar se coloca en la interfaz de salida del R1, eso evitaría que el tráfico de la red 192.168.10.0/24 alcance cualquier red a través de la interfaz Serial 0/0/0 del R1.

De acuerdo con las pautas básicas de colocación de ACL estándar cerca del destino, en la ilustración se muestran dos interfaces posibles del R3 a las que aplicar la ACL estándar:

* **Interfaz S0/0/1 del R3:** la aplicación de una ACL estándar para impedir que el tráfico de 192.168.10.0/24 ingrese a la interfaz S0/0/1 evita que dicho tráfico llegue a 192.168.30.0/24 y al resto de las redes a las que puede llegar el R3. Esto incluye la red 192.168.31.0/24. Dado que el objetivo de la ACL es filtrar el tráfico destinado solo a 192.168.30.0/24, no se debe aplicar una ACL estándar a esta interfaz.
* **Interfaz G0/0 del R3:** al aplicar una ACL estándar al tráfico que sale por la interfaz G0/0, se filtran los paquetes que van de 192.168.10.0/24 a 192.168.30.0/24. Esto no afecta a las otras redes a las que puede llegar el R3. Los paquetes de 192.16810.0/24 aún pueden llegar a 192.168.31.0/24.



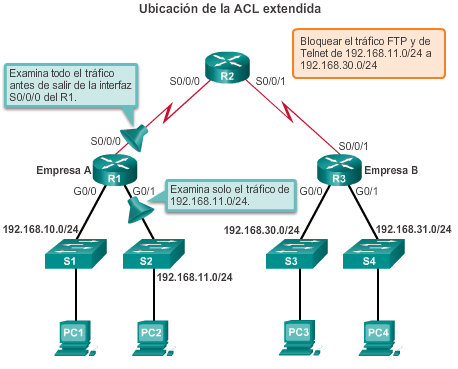
Al igual que las ACL estándar, las ACL extendidas pueden filtrar el tráfico según la dirección de origen. Sin embargo, las ACL extendidas también pueden filtrar el tráfico según la dirección de destino, el protocolo y el número de puerto. Esto permite que los administradores de red tengan más flexibilidad en cuanto al tipo de tráfico que se puede filtrar y dónde colocar la ACL. La regla básica para la colocación de una ACL extendida es colocarla lo más cerca posible del origen. Esto evita que el tráfico no deseado se envíe a través de varias redes y luego sea denegado cuando llegue a destino.

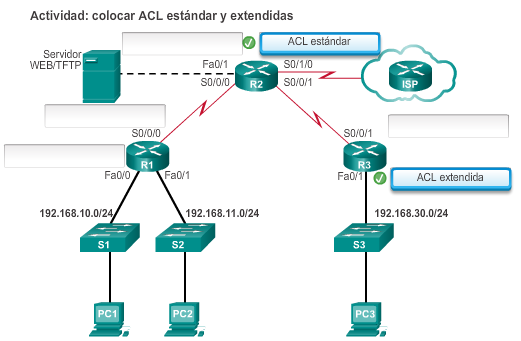
Los administradores de red solo pueden colocar ACL en los dispositivos que controlan. Por lo tanto, la colocación se debe determinar en el contexto de hasta dónde se extiende el control del administrador de red. En la ilustración, se muestra que el administrador de la empresa A, que incluye las redes 192.168.10.0/24 y 192.168.11.0/24 (denominadas .10 y .11 en este ejemplo), desea controlar el tráfico a la empresa B. Lo que el administrador desea específicamente es denegar el tráfico de Telnet y FTP de la red .11 a la red 192.168.30.0/24 de la empresa B (.30 en este ejemplo). Al mismo tiempo, se debe permitir que el resto del tráfico de la red .11 salga de la empresa A sin restricciones.

Existen varias formas de lograr estos objetivos. Una ACL extendida en el R3 que bloquee Telnet y FTP de la red .11 cumpliría el objetivo, pero el administrador no controla el R3. Además, esta solución también permite que el tráfico no deseado cruce toda la red y luego sea bloqueado en el destino. Esto afecta la eficacia general de la red.

Una mejor solución es colocar una ACL extendida en el R1 que especifique tanto las direcciones de origen como las de destino (redes .11 y .30, respectivamente) y que aplique la regla “no se permite que el tráfico de Telnet y FTP de la red .11 vaya a la red .30”. En la ilustración, se muestran dos interfaces posibles en el R1 para aplicar la ACL extendida:

* **Interfaz S0/0/0 del R1 (de salida):**una de las posibilidades es aplicar una ACL extendida de salida en la interfaz S0/0/0. Debido a que la ACL extendida puede examinar tanto la dirección de origen como la de destino, solo se deniegan los paquetes FTP y Telnet de 192.168.11.0/24, y el R1 reenvía el resto del tráfico de 192.168.11.0/24 y de otras redes. La desventaja de colocar la ACL extendida en esta interfaz es que la ACL debe procesar todo el tráfico que sale de S0/0/0, incluidos los paquetes de 192.168.10.0/24.
* **Interfaz G0/1 del R1 (de entrada):** la aplicación de una ACL extendida al tráfico que ingresa a la interfaz G0/1 implica que solamente los paquetes de la red 192.168.11.0/24 están sujetos al procesamiento de la ACL en el R1. Debido a que el filtro se debe limitar solo a aquellos paquetes que salen de la red 192.168.11.0/24, la aplicación de una ACL extendida a G0/1 es la mejor solución.





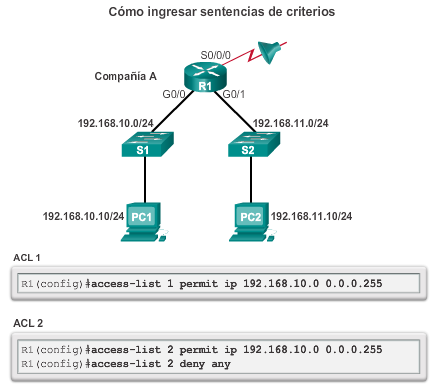
## ACL de IPv4 estándar

### Configuración de ACL de IPv4 estándar

Cuando el tráfico ingresa al router, se compara con todas las ACE en el orden en que las entradas se encuentran en la ACL. El router continúa procesando las ACE hasta que encuentra una coincidencia. Procesa el paquete según la primera coincidencia y no se examinan más ACE.

Si no se encuentran coincidencias cuando el router llega al final de la lista, se deniega el tráfico. Esto se debe a que, de manera predeterminada, hay una denegación implícita al final de todas las ACL para el tráfico sin coincidencias con una entrada configurada. Una ACL de entrada única con solo una entrada de denegación tiene el efecto de denegar todo el tráfico. Se debe configurar al menos una ACE permit en una ACL. En caso contario, 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. A la red 192.168.10.0 se le permite acceder a las redes a las que puede llegar mediante S0/0/0, mientras que a 192.168.11.0 no se le permite acceder a esas redes.



**Lógica de las ACL estándar**

En la ilustración, se revisa la dirección de origen de los paquetes que ingresan al router a través de la interfaz G0/0 según las siguientes entradas:

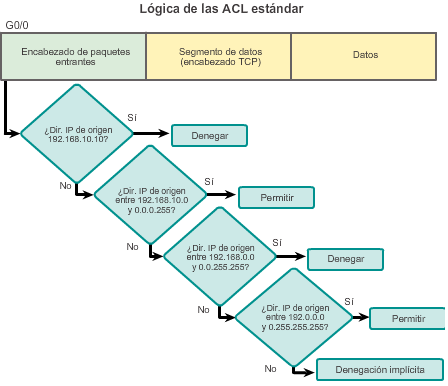
**access-list 2 deny 192.168.10.10**

**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**

Si se permiten los paquetes, se enrutan a través del router hacia una interfaz de salida. Si se deniegan los paquetes, se descartan en la interfaz de entrada.



**Configurar las ACL estándar.**

Para utilizar ACL estándar numeradas en un router Cisco, primero debe crear la ACL estándar y, a continuación, activarla en una interfaz.

El comando de configuración global**access-list** define una ACL estándar con un número entre 1 y 99. La versión 12.0.1 del software IOS de Cisco amplió ese intervalo y permite que se utilicen los números que van de 1300 a 1999 para las ACL estándar. Esto permite que se genere un máximo de 798 ACL estándar posibles. A estos números adicionales se los denomina “ACL de IP extendidas”.

La sintaxis completa del comando de ACL estándar es la siguiente:

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

En la figura 1, se explica detalladamente la sintaxis para una ACL estándar.

Las ACE pueden permitir o denegar un solo host o un rango de direcciones host. Para crear una instrucción de host en la ACL numerada 10 que permita un host específico con la dirección IP 192.168.10.0, debe introducir lo siguiente:

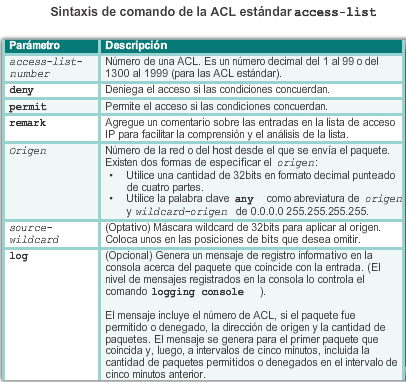
R1(config)# **access-list 10 permit host 192.168.10.10**

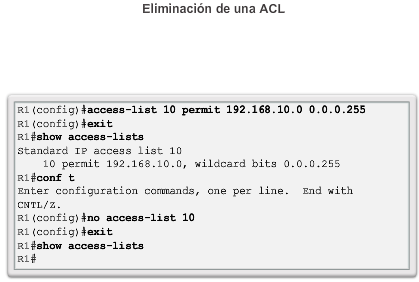
Como se muestra en la figura 2, para crear una instrucción que permita un rango de direcciones IPv4 en una ACL numerada 10 que permite todas las direcciones IPv4 en la red 192.168.10.0/24, debe introducir lo siguiente:

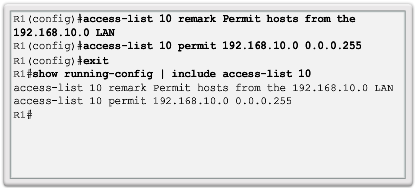
R1(config)# **access-list 10 permit 192.168.10.0 0.0.0.255**

Para eliminar la ACL, se utiliza el comando de configuración global **no access-list**. La ejecución del comando **show access-list** confirma que se eliminó la lista de acceso 10.

Por lo general, cuando un administrador crea una ACL, conoce y entiende el objetivo de cada instrucción. Sin embargo, para asegurar que el administrador y otras personas recuerden el propósito de las instrucciones, se deben incluir comentarios (remarks). La palabra clave **remark** se utiliza en los documentos y hace que sea mucho más fácil comprender las listas de acceso. El texto de cada comentario tiene un límite de 100 caracteres. La ACL que se muestra en la figura 3, que es bastante simple, se utiliza a modo de ejemplo. Cuando se revisa la ACL en la configuración mediante el comando **show running-config**, también se muestra el comentario.







El IOS de Cisco aplica una lógica interna al aceptar y procesar las ACE estándar. Como se mencionó anteriormente, las ACE se procesan en forma secuencial, por lo que el orden en que se introducen es importante.

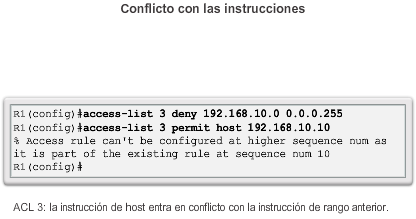
Por ejemplo, en la figura 1, la ACL 3 contiene dos ACE. La primera ACE utiliza una máscara wildcard para denegar un rango de direcciones que incluye todos los hosts en la red 192.168.10.0/24. La segunda ACE es una instrucción de host que examina un host específico: 192.168.10.10. Este es un host dentro del rango de hosts que se configuró en la instrucción anterior. Es decir, 192.168.10.10 es un host en la red 192.168.10.0/24. La lógica interna del IOS para las listas de acceso estándar rechaza la segunda instrucción y envía un mensaje de error, porque es un subconjunto de la instrucción anterior. Observe que, en la ilustración, el router asigna automáticamente el número de secuencia 10 como número de secuencia asignado a la primera instrucción introducida en este ejemplo. El resultado del router incluye el mensaje “part of the existing rule at sequence num 10” en referencia a la regla (“parte de la regla existente en el número de secuencia 10”) y no acepta la instrucción.

**Nota:** actualmente, las ACL extendidas no producen errores similares.

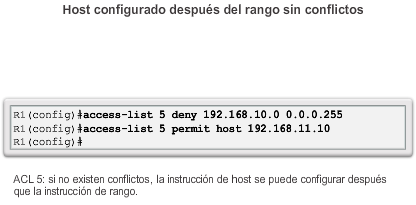
La configuración en la figura 2 de la ACL 4 tiene las mismas dos instrucciones, pero en orden inverso. Esta es una secuencia válida de instrucciones, porque la primera instrucción se refiere a un host específico, no a un rango de hosts.

En la figura 3, la ACL 5 muestra que se puede configurar una instrucción de host después de una instrucción que denota un rango de hosts. El host no debe estar dentro del rango que abarca una instrucción anterior. La dirección host 192.168.11.10 no forma parte de la red 192.168.10.0/24, por lo que se trata de una instrucción válida.

**Nota:** es posible que el orden en que se introducen las ACE estándar no sea el orden en que se almacenen, se muestren o se procesen en el router. Esto se analizará en una sección posterior.







**Procedimientos de configuración de ACL estándar**

Después de que se configura una ACL estándar, se vincula a una interfaz mediante el comando **ip access-group** del modo de configuración de interfaz:

Router(config-if)# **ip access-group**{ *access-list-number*|*nombre-lista-acceso* } { **pre**| **out**}

Para eliminar una ACL de una interfaz, primero introduzca el comando **no ip access-group** en la interfaz y, a continuación, introduzca el comando global**no access-list** para eliminar la ACL completa.

En la figura 1, se enumeran los pasos y la sintaxis para configurar y aplicar una ACL estándar numerada en un router.

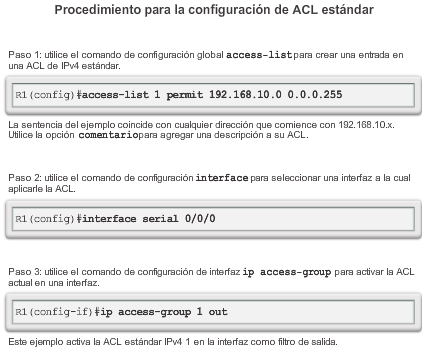
En la figura 2, se muestra un ejemplo de una ACL para permitir una sola red.

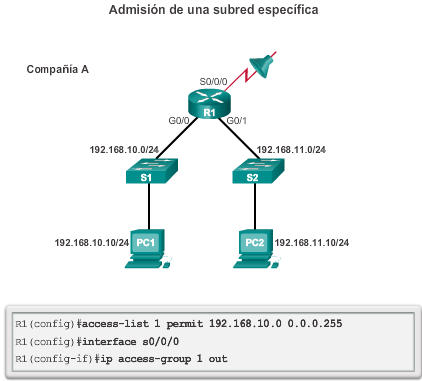
Esta ACL solo permite que se reenvíe mediante la interfaz S0/0/0 el tráfico de la red de origen 192.168.10.0. El tráfico proveniente de redes distintas de la red 192.168.10.0 se bloquea.

En la primera línea, se identifica la ACL como lista de acceso 1. Esta lista permite el tráfico que coincide con los parámetros seleccionados. En este caso, la dirección IPv4 y la máscara wildcard que identifican a la red de origen son 192.168.10.0 0.0.0.255. Recuerde que existe una denegación implícita de todas las instrucciones que equivale a agregar la línea**access-list 1 deny 0.0.0.0 255.255.255.255**.

El comando de configuración de interfaz**ip access-group 1 out** vincula la ACL 1 a la interfaz Serial 0/0/0 como filtro de salida.

Por lo tanto, la ACL 1 solo permite que los hosts de la red 192.168.10.0/24 salgan por el router R1. Esta lista deniega cualquier otra red, incluida la red 192.168.11.0.





En la figura 1, se muestra un ejemplo de una ACL que permite una subred específica, a excepción de un host específico en esa subred.

Esta ACL reemplaza el ejemplo anterior, pero también bloquea el tráfico de una dirección específica. El primer comando elimina la versión anterior de la ACL 1. La siguiente instrucción de ACL deniega el host de la PC1 ubicado en 192.168.10.10. Todos los demás hosts en la red 192.168.10.0/24 se permiten. En este caso, la instrucción deny implícita también coincide con todas las demás redes.

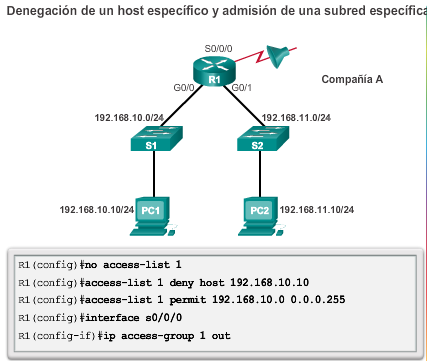
La ACL se vuelva a aplicar a la interfaz S0/0/0 en sentido de salida.

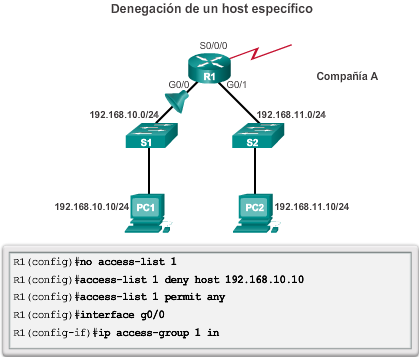
En la figura 2, se muestra un ejemplo de una ACL que deniega un host específico. Esta ACL reemplaza el ejemplo anterior. En este ejemplo, se sigue bloqueando el tráfico del host PC1, pero se permite el resto del tráfico.

Los primeros dos comandos son los mismos que en el ejemplo anterior. El primer comando elimina la versión anterior de la ACL 1, y la siguiente instrucción de ACL deniega el host PC1 que está ubicado en 192.168.10.10.

La tercera línea es nueva y permite el resto de los hosts. Esto significa que se permiten todos los hosts de la red 192.168.10.0/24, excepto PC1, que se denegó en la instrucción anterior.

Esta ACL se aplica a la interfaz G0/0 en sentido de entrada. Debido a que el filtro afecta únicamente a la LAN 192.168.10.0/24 en G0/0, es más eficaz aplicar la ACL a la interfaz de entrada. Se puede aplicar la ACL a s0/0/0 en sentido de salida, pero entonces el R1 tendría que examinar los paquetes de todas las redes, incluida 192.168.11.0/24.





La asignación de nombres a las ACL hace más fácil comprender su función. Por ejemplo, una ACL configurada para denegar el tráfico FTP se podría llamar NO\_FTP. Cuando se identifica la ACL con un nombre en lugar de un número, el modo de configuración y la sintaxis de los comandos son sutilmente diferentes.

En la figura 1, se muestran los pasos necesarios para crear una ACL estándar con nombre.

**Paso 1.**En el modo de configuración global, utilice el comando **ip access-list** para crear una ACL con nombre. Los nombres de las ACL son alfanuméricos, distinguen mayúsculas de minúsculas y deben ser únicos. El comando **ip access-list standard***nombre* se utiliza para crear una ACL estándar con nombre, mientras que el comando **ip access-list extended***nombre* se utiliza para una lista de acceso extendida. Después de introducir el comando, el router se encuentra en el modo de configuración de ACL estándar con nombre, según lo que indica la petición de entrada.

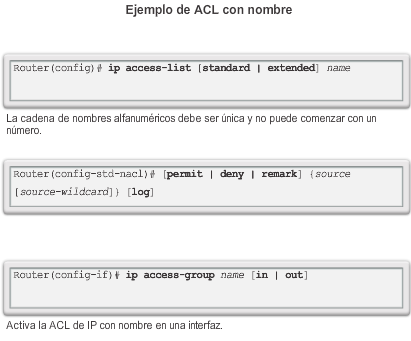
**Nota:** las ACL numeradas utilizan el comando de configuración global **access-list**, mientras que las ACL de IPv4 con nombre utilizan el comando **ip access-list**.

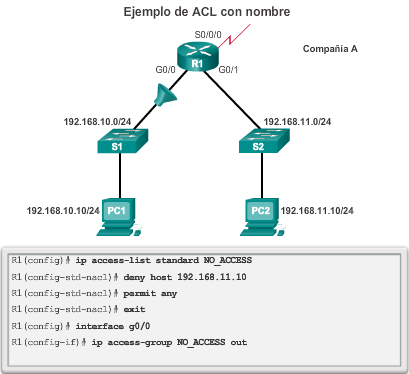
**Paso 2.**En el modo de configuración de ACL con nombre, utilice las instrucciones**permit** o **deny** a fin de especificar una o más condiciones para determinar si un paquete se reenvía o se descarta.

**Paso 3.**Aplique la ACL a una interfaz con el comando**ip access-group**. Especifique si la ACL se debe aplicar a los paquetes cuando ingresan por la interfaz (**in**) o cuando salen de la interfaz (**out**).

En la figura 2, se muestran los comandos que se utilizan para configurar una ACL estándar con nombre en el router R1, en la que la interfaz G0/0 deniega el acceso del host 192.168.11.10 a la red 192.168.10.0. La ACL se llama NO\_ACCESS.

No es necesario que los nombres de las ACL comiencen con mayúscula, pero esto los hace destacarse cuando se observa el resultado de show running-config. También hace que sea menos probable que cree accidentalmente dos ACL diferentes con el mismo nombre pero con distinto uso de mayúsculas.





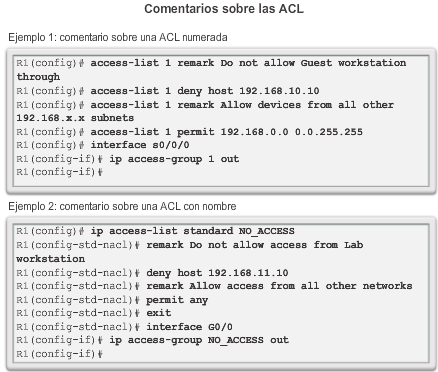
Puede utilizar la palabra clave **remark** para incluir comentarios (remarks) sobre entradas en cualquier ACL de IP estándar o extendida. Estos comentarios facilitan la comprensión y la revisión de las ACL. Cada línea de comentarios tiene un límite de 100 caracteres.

El comentario puede ir antes o después de una instrucción **permit** o **deny**. Debe ser coherente en cuanto a la ubicación del comentario, de manera que quede claro qué comentario describe cuál de las instrucciones **permit** o **deny**. Por ejemplo, sería confuso colocar algunos comentarios antes de las instrucciones **permit** o **deny** correspondientes y otros después de estas.

Para incluir un comentario para las ACL de IPv4 estándar o extendidas numeradas, utilice el comando de configuración global **access-list***lista-acceso\_número* **remark***comentario*. Para eliminar el comentario, utilice la versión **no** de este comando.

En el primer ejemplo, se muestra que la ACL numerada deniega la salida de la estación de trabajo de invitado 192.168.10.10 por S0/0/0, pero permite el resto de los dispositivos de 192.168.0.0/16.

Para crear una entrada en una ACL estándar o extendida con nombre, utilice el comando de configuración de lista de acceso **remark**. Para eliminar el comentario, utilice la versión **no** de este comando. En el ejemplo 2, se muestra una ACL estándar con nombre. En este ejemplo, las instrucciones remark indican que se deniega la estación de trabajo de laboratorio con la dirección host 192.168.11.10, pero que los dispositivos de las demás redes están permitidos.



### Modificación de ACL de IPv4

**Edición de ACL numeradas**

Cuando se configura una ACL estándar, las instrucciones se agregan a la configuración en ejecución. Sin embargo, no hay una característica de edición incorporada que permita realizar cambios en una ACL.

Existen dos maneras de editar una ACL estándar numerada.

**Método 1: uso de un editor de texto**

Después de familiarizarse con el proceso de creación y edición de ACL, puede ser más fácil generar la ACL mediante un editor de texto como el Bloc de notas de Microsoft. Esto permite crear o editar la ACL y luego pegarla en el router. Para una ACL existente, puede utilizar el comando**show running-config** para mostrar la ACL, copiarla y pegarla en el editor de texto, realizar los cambios necesarios y pegarla nuevamente en el router.

**Configuración.** Suponga, por ejemplo, que la dirección host IPv4 de la ilustración se introdujo incorrectamente. En lugar del host 192.168.10.99, debería ser el host 192.168.10.10. Los pasos para editar y corregir la ACL 1 son los siguientes:

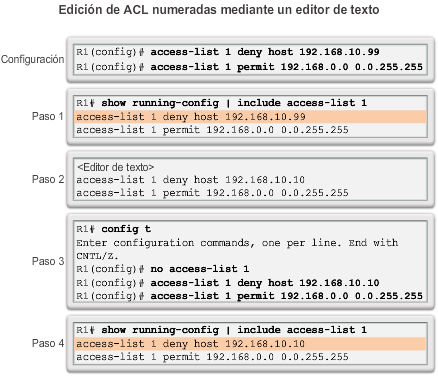
**Paso 1.**Muestre la ACL mediante el comando **show running-config**. En el ejemplo de la ilustración, se utiliza la palabra clave **include** para mostrar solamente las ACE.

**Paso 2.**Seleccione la ACL, cópiela y, luego, péguela en el Bloc de notas de Microsoft. Edite la lista según sea necesario. Una vez que la ACL se muestre correctamente en el Bloc de notas de Microsoft, selecciónela y cópiela.

**Paso 3.**En el modo de configuración global, elimine la lista de acceso con el comando **no access-list 1**. De lo contrario, las nuevas instrucciones se agregarán a la ACL existente. A continuación, pegue la nueva ACL en la configuración del router.

**Paso 4.**Verifique los cambios mediante el comando **show running-config**.

Es necesario recordar que, al utilizar el comando **no access-list**, las distintas versiones del software IOS actúan de forma diferente. Si la ACL que se eliminó sigue estando aplicada a una interfaz, algunas versiones del IOS actúan como si no hubiera ninguna ACL que proteja la red, mientras que otras deniegan todo el tráfico. Por esta razón, es aconsejable eliminar la referencia a la lista de acceso de la interfaz antes de modificar la lista. Además, tenga en cuenta que si hay un error en la nueva lista, debe deshabilitarla y solucionar el problema. En ese caso, la red no tiene ninguna ACL durante el proceso de corrección.



**Método 2: uso del número de secuencia**

Como se muestra en la ilustración, en la configuración inicial de la ACL 1 se incluyó una instrucción de host para el host 192.168.10.99, pero eso fue un error. Se debería haber configurado el host 192.168.10.10. Para editar la ACL con los números de secuencia, siga estos pasos:

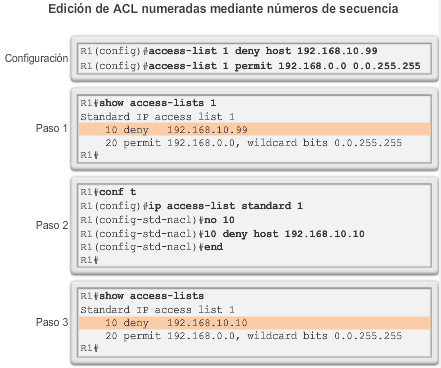
**Paso 1.**Muestre la ACL actual mediante el comando **show access-lists 1**. El resultado de este comando se analizará en mayor detalle más adelante en esta sección. El número de secuencia se muestra al principio de cada instrucción. El número de secuencia se asignó automáticamente cuando se introdujo la instrucción de la lista de acceso. Observe que la instrucción que está mal configurada tiene el número de secuencia 10.

**Paso 2.**Introduzca el comando **ip access-lists standard** que se utiliza para configurar las ACL con nombre. El número de la ACL, 1, se utiliza como nombre. Primero, la instrucción mal configurada se debe eliminar con el comando **no 10**, donde “10” se refiere al número de secuencia. Luego, se agrega una nueva instrucción de número de secuencia 10 mediante el comando **10 deny host 192.168.10.10**.

**Nota:** las instrucciones no se pueden sobrescribir con el mismo número de secuencia que el de una instrucción existente. Primero se debe eliminar la instrucción actual y, luego, se puede agregar la nueva.

**Paso 3.**Verifique los cambios mediante el comando **show access-lists**.

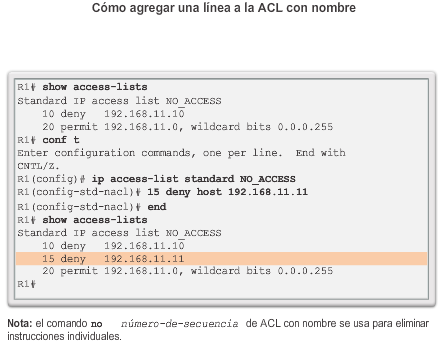
Como se mencionó anteriormente, el IOS de Cisco implementa una lógica interna en las listas de acceso estándar. Es posible que el orden en que se introducen las ACE estándar no sea el orden en que se almacenen, se muestren o se procesen en el router. El comando **show access-lists** muestra las ACE con sus números de secuencia.



En un ejemplo anterior, se utilizaron los números de secuencia para editar una ACL estándar numerada. Mediante una referencia a los números de secuencia de la instrucción, se pueden insertar o eliminar fácilmente instrucciones individuales. Este método también se puede utilizar para editar las ACL estándar con nombre.

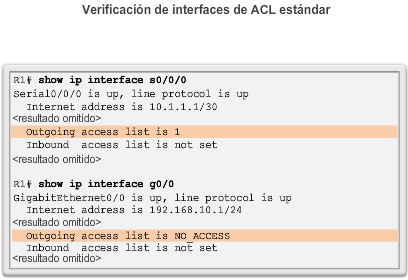
En la ilustración, se muestra un ejemplo de inserción de una línea en una ACL con nombre.

* En el primer resultado del comando**show**, se puede ver que la ACL con el nombre NO\_ACCESS tiene dos líneas numeradas que indican las reglas de acceso para una estación de trabajo con la dirección IPv4 192.168.11.10.
* El comando **ip access-list standard** se utiliza para configurar las ACL con nombre. Se pueden insertar o eliminar instrucciones desde el modo de configuración de listas de acceso con nombre. El comando **no***número-secuencia* se utiliza para eliminar instrucciones individuales.
* Para agregar una instrucción para denegar otra estación de trabajo, se debe insertar una línea numerada. En el ejemplo, se agrega la estación de trabajo con la dirección IPv4 192.168.11.11 mediante el nuevo número de secuencia 15.
* Mediante el último resultado del comando **show**, se verifica que la nueva estación de trabajo ahora tiene el acceso denegado.



Como se muestra en la figura 1, el comando **show ip interface** se utiliza para verificar la ACL en la interfaz El resultado de este comando incluye el número o el nombre de la lista de acceso y el sentido en el que se aplicó la ACL. El resultado muestra que la lista de acceso 1 se aplica a la interfaz de salida S0/0/0 del router R1 y que la lista de acceso NO\_ACCESS se aplica a la interfaz g0/0, también en sentido de salida.

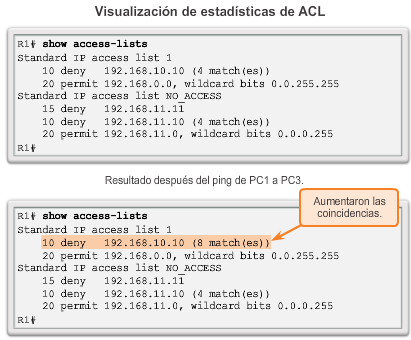
En el ejemplo de la figura 2, se muestra el resultado de emitir el comando **show access-lists** en el router R1. Para ver una lista de acceso individual, utilice el comando **show access-lists** seguido del número o el nombre de la lista de acceso. Es posible que las instrucciones de NO\_ACCESS se vean extrañas. Observe que el número de secuencia 15 se muestra antes que el número de secuencia 10. Esto se debe al proceso interno del router y se analizará más adelante en esta sección.

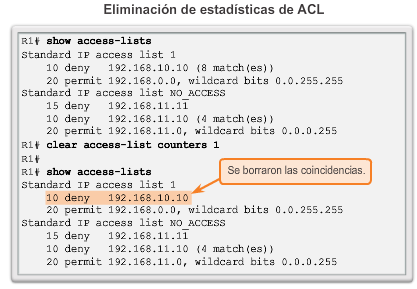


Una vez que la ACL se aplicó a una interfaz y se realizaron algunas pruebas, el comando **show access-lists** muestra las estadísticas para cada instrucción que tiene coincidencias. En el resultado que se muestra en la figura 1, observe que se encontraron coincidencias para algunas de las instrucciones. Cuando se genera tráfico que debe coincidir con una instrucción de ACL, las coincidencias que se muestran en el resultado del comando **show access-lists** deberían aumentar. Por ejemplo, en este caso, si se hace ping de la PC1 a la PC3 o la PC4, en el resultado se mostrará un aumento en las coincidencias para la instrucción deny de ACL 1.

Tanto las instrucciones permit como las deny realizan un seguimiento de las estadísticas de coincidencias; sin embargo, recuerde que cada ACL tiene una instrucción deny any implícita como última instrucción. Esta instrucción no aparece en el comando **show access-lists**, por lo que no se muestran estadísticas para esa instrucción. Para ver las estadísticas de la instrucción deny any implícita, la instrucción se puede configurar manualmente y aparecerá en el resultado. Se debe tener sumo cuidado cuando se configura manualmente la instrucción deny any, ya que coincidirá con todo el tráfico. Si esta instrucción no se configura como la última instrucción en la ACL, podría ocasionar resultados inesperados.

Durante la prueba de una ACL, se pueden borrar los contadores mediante el comando **clear access-list counters**. Este comando se puede utilizar solo o con el número o el nombre de una ACL específica. Como se muestra en la figura 2, este comando borra los contadores de estadísticas para una ACL.





El IOS de Cisco implementa una lógica interna en las ACL estándar. Como se mencionó anteriormente, una parte de esta lógica evita que las instrucciones de host se configuren después de una instrucción de rango si el host es parte de ese rango, como se muestra en la figura 1.

Otra parte de la lógica interna del IOS es responsable de la secuenciación interna de las ACE estándar. En la figura 2, se muestra la configuración de una lista de acceso estándar. Las instrucciones de rango que deniegan tres redes se configuran primero, y después se configuran cinco instrucciones de host. Las instrucciones de host son todas instrucciones válidas, porque sus direcciones IP host no forman parte de las instrucciones de rango introducidas previamente.

El comando **show running-config** se utiliza para verificar la configuración de la ACL. Observe que las instrucciones se enumeran en un orden distinto al orden en que se introdujeron. Utilizaremos el comando **show access-lists** para comprender la lógica.

Como se muestra en la figura 3, el comando **show access-lists** muestra las ACE junto con sus números de secuencia. Sería de esperar que el orden de las instrucciones en el resultado reflejara el orden en que se introdujeron. Sin embargo, el resultado de **show access-lists** muestra que este no es el caso.

El orden en que se enumeran las ACE estándar es la secuencia utilizada por el IOS para procesar la lista. Observe que las instrucciones se agrupan en dos secciones: las instrucciones de host seguidas por las instrucciones de rango. El número de secuencia indica el orden en que se introdujo la instrucción, no el orden en que se procesará.

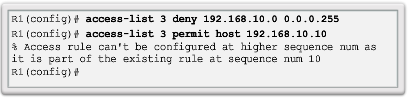
Las instrucciones de host se enumeran primero, pero no necesariamente en el orden en que se introdujeron. El IOS ordena las instrucciones de host mediante una función de hash especial. El orden resultante optimiza la búsqueda de una entrada de ACL de host.

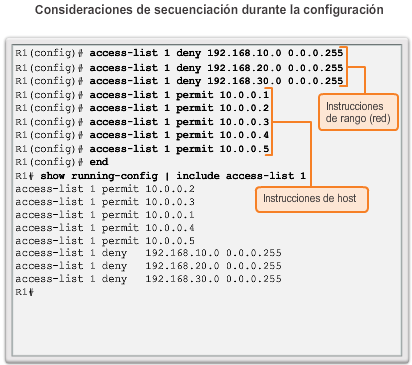
Las instrucciones de rango se muestran después de las instrucciones de host. Estas instrucciones se enumeran en el orden en que se introdujeron.

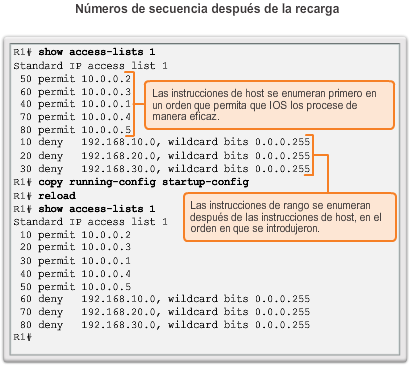
Recuerde que las ACL estándar y numeradas se pueden editar con números de secuencia. El número de secuencia que se muestra en el resultado del comando**show access-lists** es el número utilizado para eliminar las instrucciones individuales de la lista. Cuando se introduce una nueva instrucción de ACL, el número de secuencia solo afecta a la ubicación de una instrucción de rango en la lista. Las instrucciones de host siempre se ordenan con la función de hash.

Siguiendo con el ejemplo, una vez que se guarda la configuración en ejecución, el router se vuelve a cargar (se reinicia). Como se muestra en la figura 3, el comando **show access-lists** muestra la ACL en el mismo orden, sin embargo, las instrucciones se volvieron a numerar. Los números de secuencia ahora están en orden numérico.

**Nota:** la función de hash se aplica solamente a las instrucciones de host en listas de acceso de IPv4 estándar. El algoritmo no se utiliza para las ACL de IPv4 extendidas ni las ACL de IPv6. Esto se debe a que las ACL extendidas e IPv6 filtran más de una sola dirección de origen. Los detalles de la función de hash exceden el ámbito de este curso.







### Protección de puertos VTY con una ACL de IPv4 estándar

**Uso de una ACL para controlar el acceso a VTY**

Cisco recomienda utilizar SSH para las conexiones administrativas a los routers y switches. Si la imagen del software IOS de Cisco en su router no admite SSH, puede mejorar la seguridad de las líneas administrativas mediante la restricción del acceso a VTY. La restricción del acceso a VTY es una técnica que permite definir las direcciones IP a las que se les permite acceder por Telnet al proceso de EXEC del router. Puede controlar qué estación de trabajo administrativa o qué red administra el router mediante la configuración de una ACL y una instrucción **access-class** en las líneas VTY. También puede utilizar esta técnica con SSH para mejorar aún más la seguridad de acceso administrativo.

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

Las listas de control de acceso estándar y extendidas se aplican a los paquetes que se transportan a través de un router, no están diseñadas para bloquear los paquetes que se originan en el router. Una ACL extendida para Telnet de salida no evita las sesiones de Telnet iniciadas por el router de manera predeterminada.

Por lo general, se considera que el filtrado del tráfico de Telnet o SSH es una función de una ACL de IP extendida, porque filtra un protocolo de nivel superior. Sin embargo, debido a que se utiliza el comando **access-class** para filtrar sesiones de Telnet/SSH entrantes o salientes por dirección de origen, se puede utilizar una ACL estándar.

La sintaxis del comando **access-class**es la siguiente:

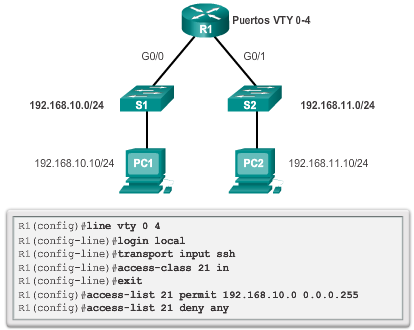
Router(config)# **access-class** *número-lista-acceso* { **pre**[ **vrf-also** ] | **out** }

El parámetro **in** limita las conexiones de entrada entre las direcciones en la lista de acceso y el dispositivo de Cisco, mientras que el parámetro **out** limita las conexiones de salida entre un dispositivo de Cisco en particular y las direcciones en la lista de acceso.

En la figura 1, se muestra un ejemplo en el que se permite que un rango de direcciones acceda a las líneas VTY de 0 a 4. La ACL de la ilustración se configuró para permitir que la red 192.168.10.0 acceda a las líneas VTY de 0 a 4, pero para denegar las demás redes.

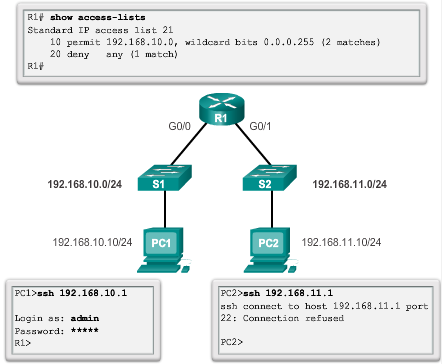
Para configurar listas de acceso en los VTY, se debe tener en cuenta lo siguiente:

* Solamente se pueden aplicar listas de acceso numeradas a los VTY.
* Se deben establecer restricciones idénticas en todos los VTY, porque un usuario puede intentar conectarse a cualquiera de ellos.



Después de configurar la ACL para restringir el acceso a las líneas VTY, es importante verificar que funcione correctamente. En la ilustración, se muestran dos dispositivos que intentan conectarse al R1 mediante SSH. Se configuró la lista de acceso 21 en las líneas VTY en el R1. La PC1 logra conectarse, mientras que la PC2 no puede establecer una conexión SSH. Este es el comportamiento que se espera, ya que la lista de acceso configurada permite el acceso a VTY desde la red 192.168.10.0/24 y deniega al resto de los dispositivos.

El resultado del R1 muestra lo que se produce al emitir el comando **show access-lists** después de que la PC1 y la PC2 intentan conectarse mediante SSH. La coincidencia en la línea permit del resultado es producto de una conexión SSH correcta de la PC1. La coincidencia en la instrucción deny se debe al intento fallido de la PC2, un dispositivo en la red 192.168.11.0/24, de establecer una conexión SSH.



## ACL de IPv4 extendidas

### Estructura de una ACL de IPv4 extendida

**Prueba de paquetes con ACL extendidas**

Para un control más preciso del filtrado del tráfico, se pueden crear ACL de IPv4 extendidas. Las ACL extendidas se numeran del 100 al 199 y del 2000 a 2699, lo que da un total de 799 ACL extendidas numeradas posibles. Las ACL extendidas también pueden tener nombre.

Las ACL extendidas se utilizan con más frecuencia que las ACL estándar, porque proporcionan un mayor grado de control. Como se muestra en la ilustración, al igual que las ACL estándar, las ACL extendidas revisan las direcciones de origen de los paquetes, pero también revisan la dirección de destino, los protocolos y los números de puerto (o de servicios). Esto proporciona una gama de criterios más amplia sobre la cual basar la ACL. Por ejemplo, una ACL extendida puede permitir el tráfico de correo electrónico de una red a un destino específico y, simultáneamente, denegar la transferencia de archivos y la navegación Web.



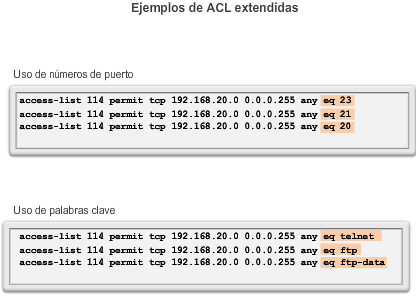
**Prueba de puertos y servicios**

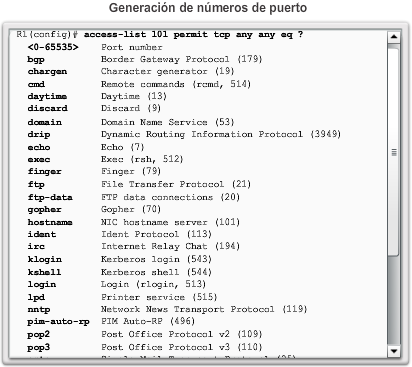
La capacidad de filtrar por protocolos y números de puerto permite que los administradores de red creen ACL extendidas muy específicas. Se puede especificar una aplicación mediante la configuración del número o el nombre de un puerto bien conocido.

En la figura 1, se muestran algunos ejemplos de la forma en que un administrador especifica un número de puerto TCP o UDP colocándolo al final de la instrucción de la ACL extendida. Se pueden utilizar operaciones lógicas, por ejemplo, igual que (eq), distinto de (neq), mayor que (gt) y menor que (lt).

En la figura 2, se muestra cómo visualizar una lista de números de puerto y de palabras clave que pueden utilizarse al generar una ACL mediante el siguiente comando:

R1(config)# **access-list 101 permit tcp any any eq?**





### Configuración de ACL de IPv4 extendidas

Los pasos del procedimiento para configurar ACL extendidas son los mismos que para las ACL estándar. Primero se configura la ACL extendida y, a continuación, se activa en una interfaz. Sin embargo, la sintaxis de los comandos y los parámetros son más complejos, a fin de admitir las funciones adicionales proporcionadas por las ACL extendidas.

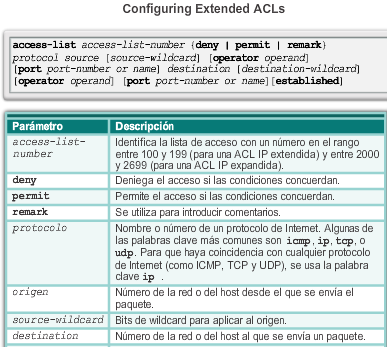
**Nota:** la lógica interna aplicada al ordenamiento de las instrucciones de las ACL estándar no se aplica a las ACL extendidas. El orden en que se introducen las instrucciones durante la configuración es el orden en que se muestran y se procesan.

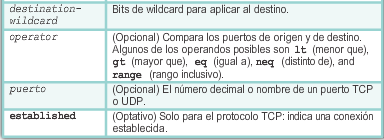
En la figura 1, se muestra la sintaxis frecuente de los comandos para las ACL de IPv4 extendidas. Observe que hay muchas palabras clave y parámetros para las ACL extendidas. No es necesario utilizar todas las palabras clave y todos los parámetros al configurar una ACL extendida. Recuerde que puede utilizar el símbolo**?** para obtener ayuda al introducir comandos complejos.

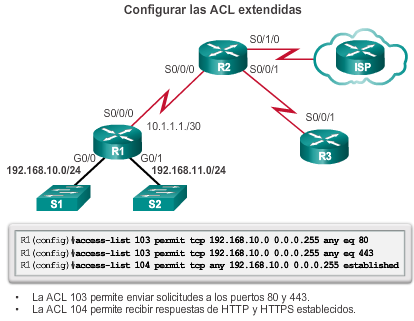
En la figura 2, se muestra un ejemplo de una ACL extendida. En este ejemplo, el administrador de red configuró las ACL para restringir el acceso de red a fin de permitir la navegación de sitios web solo desde la LAN conectada a la interfaz G0/0 a cualquier red externa. La ACL 103 permite que el tráfico proveniente de cualquier dirección en la red 192.168.10.0 vaya a cualquier destino, sujeto a la limitación de que el tráfico utilice solo los puertos 80 (HTTP) y 443 (HTTPS).

La naturaleza de HTTP requiere que el tráfico fluya nuevamente hacia la red desde los sitios web a los que se accede mediante clientes internos. El administrador de red desea restringir ese tráfico de retorno a los intercambios HTTP de los sitios web solicitados y denegar el resto del tráfico. La ACL 104 logra esto mediante el bloqueo de todo el tráfico entrante, excepto las conexiones establecidas previamente. La instrucción permit en la ACL 104 permite el tráfico entrante con el parámetro **established**.

El parámetro **established** permite que solo las respuestas al tráfico procedente de la red 192.168.10.0/24 vuelvan a esa red. Si el segmento TCP que regresa tiene los bits ACK o de restablecimiento (RST) establecidos, que indican que el paquete pertenece a una conexión existente, se produce una coincidencia. Sin el parámetro **established** en la instrucción de ACL, los clientes pueden enviar tráfico a un servidor web, pero no recibir el tráfico que vuelve de dicho servidor.





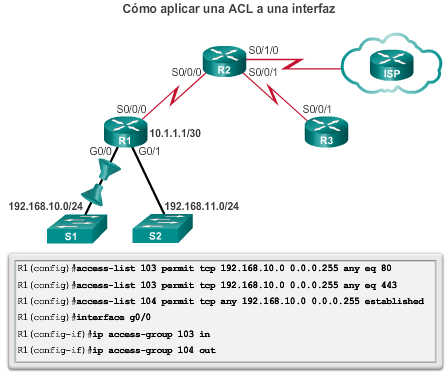


En el ejemplo anterior, el administrador de red configuró una ACL para permitir que los usuarios de la red 192.168.10.0/24 exploren sitios web seguros e inseguros. Aunque se configuró, la ACL no filtrará el tráfico hasta que se aplique a una interfaz. Para aplicar una ACL a una interfaz, primero debe considerar si el tráfico que se filtrará es entrante o saliente. Cuando un usuario de la LAN interna accede a un sitio web en Internet, hay tráfico que sale hacia Internet. Cuando un usuario interno recibe un correo electrónico de Internet, el tráfico ingresa al router local. Sin embargo, cuando se aplica una ACL a una interfaz, los términos “entrada” y “salida” tienen otros significados. Desde el punto de vista de una ACL, la entrada y salida son respecto de la interfaz del router.

En la topología de la ilustración, el R1 tiene tres interfaces: una interfaz serial, S0/0/0, y dos interfaces Gigabit Ethernet, G0/0 y G0/1. Recuerde que una ACL extendida comúnmente se debería aplicar cerca del origen. En esta topología, la interfaz más cercana al origen del tráfico de destino es la interfaz G0/0.

La solicitud de tráfico web de los usuarios en la LAN 192.168.10.0/24 entra a la interfaz G0/0. El tráfico de retorno de las conexiones establecidas a los usuarios en la LAN sale de la interfaz G0/0. En el ejemplo, se aplica la ACL a la interfaz G0/0 en ambos sentidos. La ACL de entrada, 103, revisa el tipo de tráfico. La ACL de salida, 104, revisa si hay tráfico de retorno de las conexiones establecidas. Esto restringe el acceso a Internet desde 192.168.10.0 para permitir solamente la navegación de sitios web.

**Nota:** las listas de acceso se podrían haber aplicado a la interfaz S0/0/0, pero en ese caso el proceso de ACL del router tendría que examinar todos los paquetes que ingresan al router y no solo el tráfico que va hacia 192.168.11.0 y que vuelve de esa red. Esto provocaría que el router realice un procesamiento innecesario.



En el ejemplo que se muestra en la figura 1, se deniega el tráfico FTP de la subred 192.168.11.0 que va a la subred 192.168.10.0, pero se permite el resto del tráfico. Observe el uso de las máscaras wildcard y de la instrucción deny any explícita. Recuerde que FTP utiliza los puertos TCP 20 y 21, por lo tanto, la ACL requiere ambas palabras claves de nombre de puerto **ftp** y **ftp-data** o **eq 20** y **eq 21** para denegar el tráfico FTP.

Si se utilizan números de puerto en vez de nombres de puerto, los comandos se deben escribir de la siguiente forma:

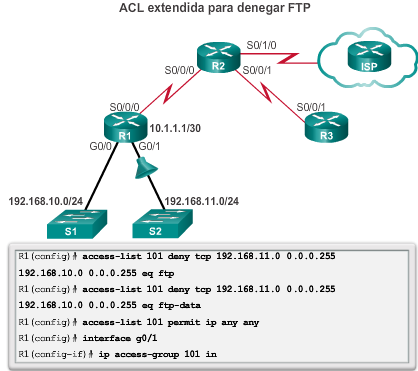
**access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20**

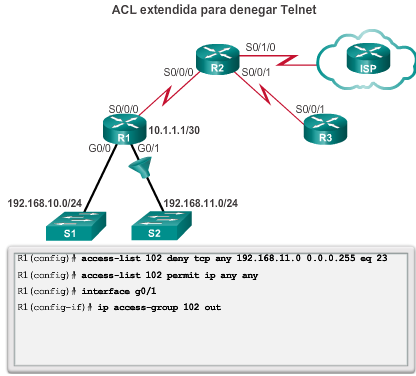
**access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21**

Para evitar que la instrucción deny any implícita al final de la ACL bloquee todo el tráfico, se agrega la instrucción **permit ip any any**. Si no hay por lo menos una instrucción **permit** en una ACL, todo el tráfico en la interfaz donde se aplicó esa ACL se descarta. La ACL se debe aplicar en sentido de entrada en la interfaz G0/1 para filtrar el tráfico de la LAN 192.168.11.0/24 cuando ingresa a la interfaz del router.

En el ejemplo que se muestra en la figura 2, se deniega el tráfico de Telnet de cualquier origen a la LAN 192.168.11.0/24, pero se permite el resto del tráfico IP. Debido a que el tráfico destinado a la LAN 192.168.11.0/24 sale de la interfaz G0/1, la ACL se aplica a G0/1 con la palabra clave**out**. Observe el uso de las palabras clave**any** en la instrucción permit. Esta instrucción permit se agrega para asegurar que no se bloquee ningún otro tipo de tráfico.

**Nota:** en ambos ejemplos en las figuras 1 y 2, se utiliza la instrucción **permit ip any any** al final de la ACL. Para obtener mayor seguridad, se puede utilizar el comando **permit 192.168.11.0 0.0.0.255 any**.





Las ACL extendidas con nombre se crean esencialmente de la misma forma que las ACL estándar con nombre. Para crear una ACL extendida con nombre, realice los siguientes pasos:

**Paso 1.**En el modo de configuración global, utilice el comando**ip access-list extended***nombre* para definir un nombre para la ACL extendida.

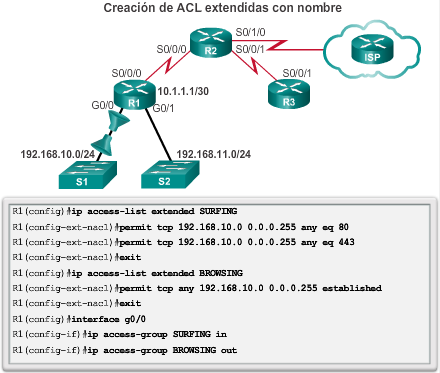
**Paso 2.**En el modo de configuración de ACL con nombre, especifique las condiciones para **permit** o **deny**.

**Paso 3.**Vuelva al modo EXEC privilegiado y verifique la ACL con el comando **show access-lists***nombre*.

**Paso 4.**Guarde las entradas en el archivo de configuración mediante el comando **copy running-config startup-config**.

Para eliminar una ACL extendida con nombre, utilice el comando de configuración global **no ip access-list extended***nombre*.

En la ilustración, se muestran las versiones con nombre de las ACL creadas en los ejemplos anteriores. La ACL con nombre SURFING permite que los usuarios en la LAN 192.168.10.0/24 accedan a sitios web. La ACL con nombre BROWSING permite el tráfico de retorno de las conexiones establecidas. Cuando se utilizan las ACL con nombre, las reglas se aplican en sentido de entrada y de salida en la interfaz G0/0.



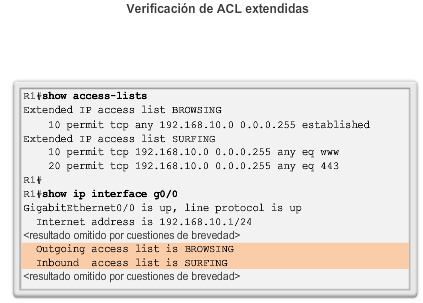
Después de configurar una ACL y aplicarla a una interfaz, utilice los comandos **show** del IOS de Cisco para verificar la configuración. En la ilustración de arriba se muestra el comando del IOS de Cisco que se utiliza para mostrar el contenido de todas las ACL. En el ejemplo de abajo, se muestra el resultado de emitir el comando **show ip interface g0/0** en el router R1.

Las ACL extendidas no implementan la misma lógica interna ni la misma función de hash. El resultado y los números de secuencia que se muestran en el resultado del comando **show access-lists** están en el orden en que se introdujeron las instrucciones. Las entradas de host no se enumeran automáticamente antes de las entradas de rango.

El comando **show ip interface** se utiliza para verificar la ACL en la interfaz y el sentido en el que se aplicó. El resultado de este comando incluye el número o el nombre de la lista de acceso y el sentido en el que se aplicó la ACL. Los nombres de las ACL BROWSING y SURFING en mayúscula se destacan en el resultado que se ve en la pantalla.

Después de verificar la configuración de una ACL, el siguiente paso es confirmar que la ACL funcione según lo esperado, es decir, que bloquee y permita el tráfico según se espera.

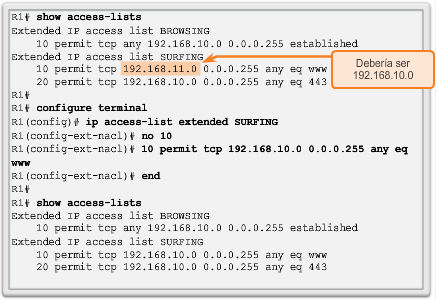
Las pautas analizadas anteriormente en esta sección sugieren que las ACL se configuren en una red de prueba y después se implementen en la red de producción.



Se puede editar una ACL extendida mediante el mismo proceso que una ACL estándar, el cual se analizó en una sección anterior. Las ACL extendidas se pueden modificar mediante los métodos siguientes:

* **Método 1: editor de texto.** Con este método, la ACL se copia y pega en el editor de texto, donde se realizan los cambios. La lista de acceso actual se elimina mediante el comando **no access-list**. Luego, la ACL modificada se pega nuevamente en la configuración.
* **Método 2: números de secuencia.**Los números de secuencia se pueden utilizar para eliminar o para insertar una instrucción de ACL. El comando**ip access-list extended***nombre* se utiliza para ingresar al modo de configuración de ACL con nombre. Si la ACL es numerada en vez de tener un nombre, se utiliza el número de la ACL en el parámetro*nombre*. Las ACE se pueden insertar o eliminar.

En la ilustración, se muestra que el administrador debe editar la ACL con nombre SURFING para corregir una errata en la instrucción de la red de origen. Para ver los números de secuencia actuales, se utiliza el comando **show access-lists**. La instrucción que se edita se identifica como instrucción 10. La instrucción original se elimina con el comando **no***número\_secuencia*. La instrucción corregida se agrega y se reemplaza la instrucción original.



## Resolución de problemas de ACL

### Procesamiento de paquetes con ACL

**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 en 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.

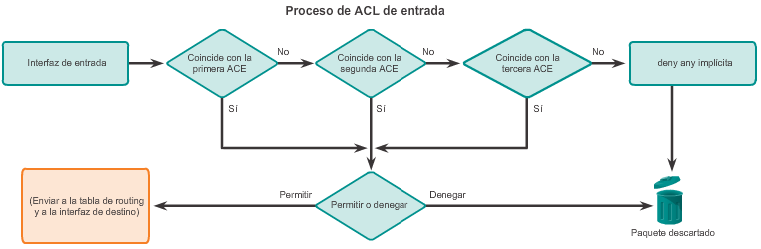
Al final de cada ACL, hay una instrucción deny any implícita. Esta instrucción no se muestra en el resultado. Esta instrucción implícita final se aplica a todos los paquetes cuyas condiciones no se probaron como verdaderas. Esta condición de prueba final coincide con el resto de los paquetes y da como 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.

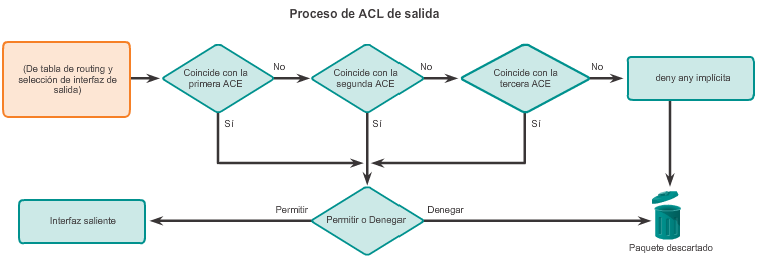
**Lógica de ACL de salida**

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 en una ACL. Si la interfaz de salida no está agrupada en una ACL, el paquete se puede enviar al búfer de salida. A continuación, se indican algunos ejemplos de la operación de la ACL de salida:

* **Ninguna ACL aplicada a la interfaz:**si la interfaz de salida no está agrupada en una ACL de salida, el paquete se envía directamente a la interfaz de salida.
* **ACL aplicada a la interfaz:** si la interfaz de salida está agrupada en una ACL de salida, el paquete no se envía por la interfaz de salida hasta que se lo prueba mediante la combinación de ACE relacionadas con esa interfaz. Según las pruebas de ACL, el paquete se permite o se deniega.

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





**ACL y routing, y procesos de ACL en un router**

En la ilustración, 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.

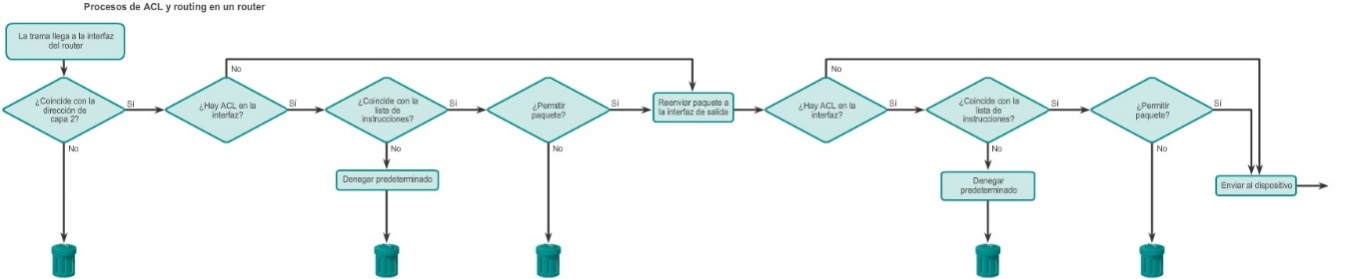
Si se acepta la dirección de la trama, se desmonta la información de la trama y el router revisa si hay una ACL en la interfaz de entrada. Si existe una ACL, el paquete se prueba en relación con las instrucciones de la lista.

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.

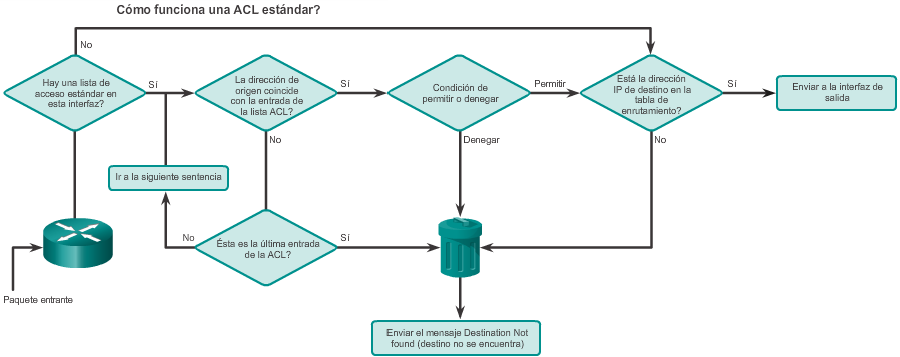
Si el paquete coincide con una instrucción, se permite o se deniega.

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.



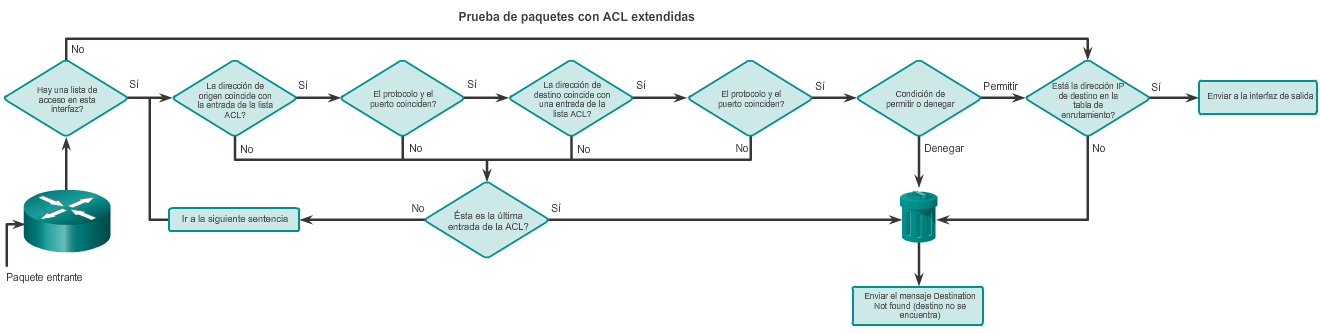
Las ACL estándar solo examinan la dirección IPv4 de origen. El destino del paquete y los puertos involucrados no se tienen en cuenta.

El proceso de decisión de una ACL estándar se detalla en la ilustración. 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.



En la ilustración, 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 sobre la dirección de destino y después sobre 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 avanza 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 se encuentre una coincidencia para una condición.



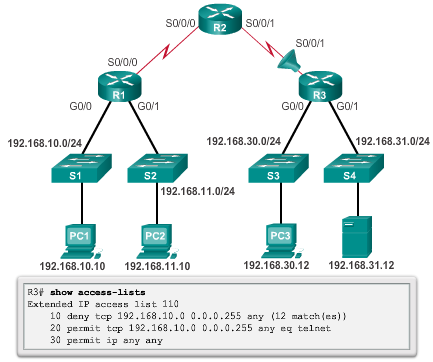
### Errores comunes de ACL

Mediante los comandos **show** descritos anteriormente, se revela la mayoría de los errores más comunes de ACL. Los errores más comunes incluyen introducir las ACE en el orden incorrecto y no aplicar los criterios adecuados a las reglas de ACL.

**Ejemplo de error 1**

En la ilustración, el host 192.168.10.10 no tiene conectividad 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.

**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).



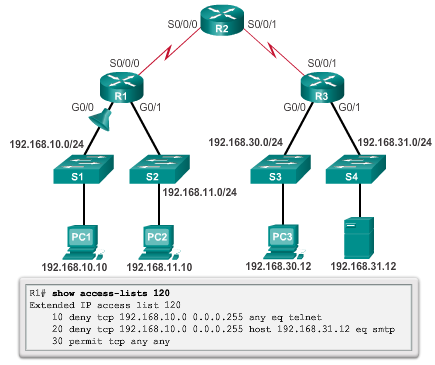
**Ejemplo de error 2**

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

**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**.

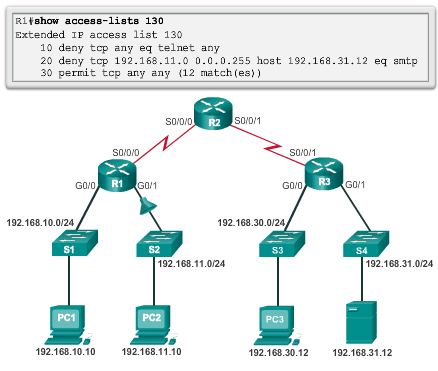
Esta ACL funciona si se aplica a G0/0 del R1, a S0/0/1 del R3 o a S0/0/0 del R2 en sentido de entrada. Sin embargo, según la regla que indica colocar las ACL extendidas más cerca del origen, la mejor opción es colocarla en sentido de entrada en G0/0 del R1, porque permite que el tráfico no deseado se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



**Ejemplo de error 3**

En la ilustración, 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.

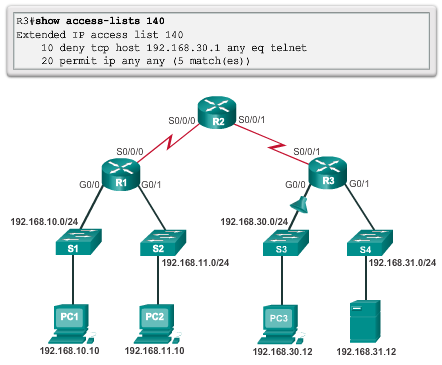
**Solución:** la red 192.168.11.0/24 puede utilizar Telnet para conectarse a la red 192.168.30.0/24, porque el número de puerto Telnet en la instrucción 10 de la lista de acceso 130 aparece en una posición incorrecta en la instrucción de ACL. Actualmente, la instrucción 10 deniega cualquier paquete de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



**Ejemplo de error 4**

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

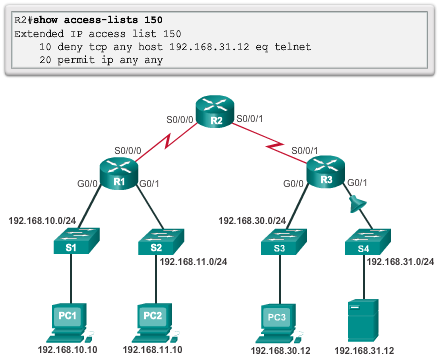
**Solución:** el host 192.168.30.12 puede utilizar Telnet para conectarse a 192.168.31.12 porque no hay reglas que denieguen el host 192.168.30.12 o su red como origen. La instrucción 10 de la lista de acceso 140 deniega la interfaz del router por la que el tráfico ingresa a este. La dirección host IPv4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



**Ejemplo de error 5**

En la ilustración, 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.

**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 que cualquier dirección de origen se conecte 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.



## ACL de IPv6

### Creación de ACL de IPv6

Las ACL de IPv6 son similares a las ACL de IPv4 en cuanto a la configuración y el 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: las 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. En resumen, las características de las ACL de IPv6 son las siguientes:

* Son ACL con nombre únicamente.
* Equivalen a la funcionalidad de una ACL de IPv4 extendida.

Una ACL de IPv4 y una ACL de IPv6 no pueden tener el mismo nombre.



Aunque las ACL de IPv4 y de IPv6 son similares, hay tres diferencias fundamentales entre ellas.

* **Aplicación de una ACL de IPv6**

La primera diferencia es 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.

* **Ausencia de máscaras wildcard**

A diferencia de las ACL de IPv4, las ACL de IPv6 no utilizan máscaras wildcard. En cambio, se utiliza la longitud de prefijo para indicar cuánto de una dirección IPv6 debe coincidir.

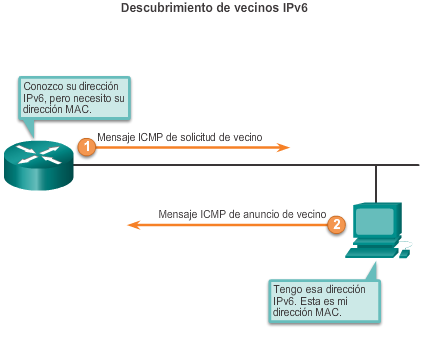
* **Instrucciones predeterminadas adicionales**

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 de IPv4 estándar o extendidas, hay una instrucción **deny any** o **deny 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 en IPv6 también se incluyen otras dos instrucciones implícitas de manera predeterminada:

* **permit icmp any any nd-na**
* **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).

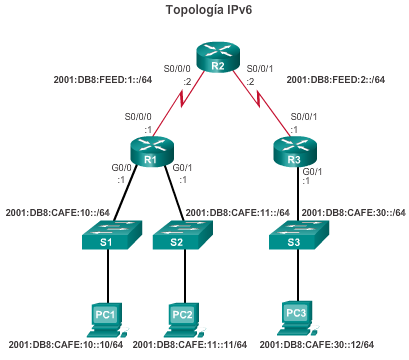
Los mensajes ND se encapsulan en paquetes IPv6 y requieren los servicios de la capa de red IPv6, mientras que ARP para IPv4 no utiliza la capa 3. Dado que IPv6 utiliza el servicio de la capa 3 para el descubrimiento de vecinos, las ACL de IPv6 deben permitir implícitamente que los paquetes ND se envíen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

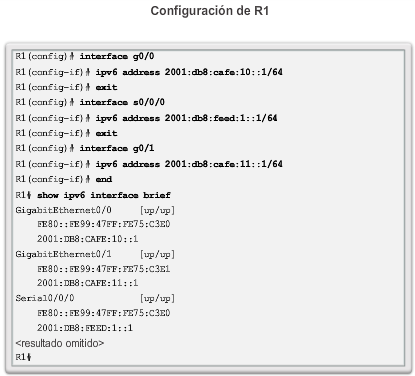


En la figura 1, se muestra la topología que se utilizará para configurar las ACL de IPv6. Esta es similar a la topología de IPv4 anterior, excepto por el esquema de direccionamiento IPv6. Hay tres subredes de 2001:DB8:CAFE::/64: 2001:DB8:CAFE:10::/64, 2001:DB8:CAFE:11::/64 y 2001:DB8:CAFE:30::/64. Hay dos redes seriales que conectan los tres routers: 2001:DB8:FEED:1::/64 y 2001:DB8:FEED:2::/64.

En las figuras 2, 3 y 4, 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.

**Nota:** el comando **no shutdown** y el comando **clock rate** no se muestran.









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

En la figura 1, 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.

Hay tres pasos básicos para configurar una ACL de IPv6:

**Paso 1.**En el modo de configuración global, utilice el comando **ipv6 access-list***nombre* para crear una ACL de 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.

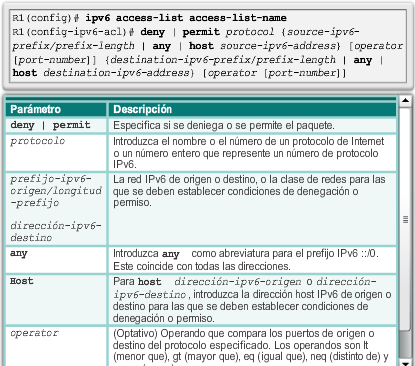
**Paso 2.**En el modo de configuración de ACL con nombre, utilice las instrucciones**permit** o **deny** para especificar una o más condiciones para determinar si un paquete se debe reenviar o descartar.

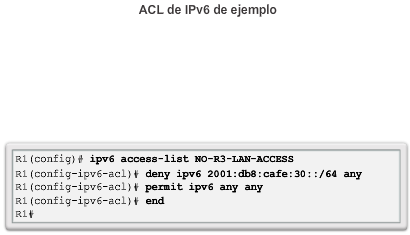
**Paso 3.**Regrese al modo EXEC privilegiado con el comando **end**.

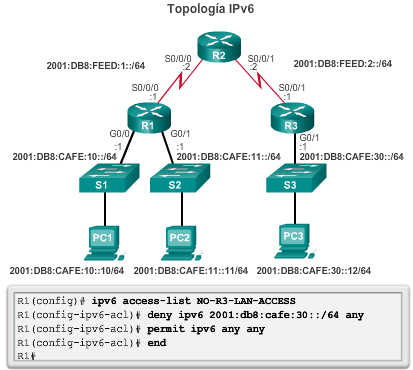
En la figura 2, se muestran los pasos para crear una ACL de IPv6 con un ejemplo simple basado en la topología anterior. La primera instrucción da el nombre NO-R3-LAN-ACCESS a la lista de acceso de IPv6. Al igual sucede que con las ACL de IPv4 con nombre, no es necesario el uso de mayúsculas en los nombres de las ACL de IPv6, pero esto hace que se destaquen cuando se observa el resultado de la configuración en ejecución.

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 3, se muestra la ACL en contexto con la topología.







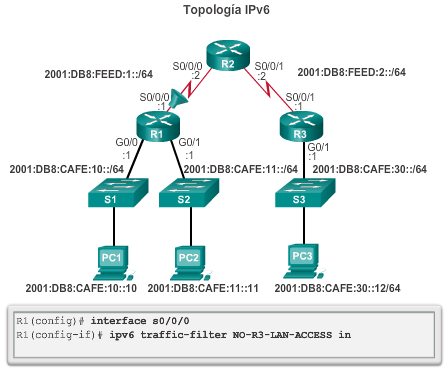
Después de que se configura una ACL de IPv6, se la vincula a una interfaz mediante el comando **ipv6 traffic-filter**:

Router(config-if)# **ipv6 traffic-filter** *nombre-lista-acceso*{ **pre**| **out** }

En la ilustración, 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.

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 **ip access-class** para aplicar una lista de acceso a los puertos VTY.



**Denegar FTP**

La topología para los ejemplos se muestra en la figura 1.

En el primer ejemplo que se muestra en la figura 2, el router R1 está configurado con una lista de acceso de 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). Debido a que el filtro se aplica en sentido de entrada a la interfaz G0/0 en el R1, solo se denegará el tráfico de la red 2001:DB8:CAFE:10::/64.

**Acceso restringido**

En el segundo ejemplo que se muestra en la figura 3, se configura una ACL de IPv6 para proporcionarle a la LAN en el R3 acceso limitado a las LAN en el R1. Se agregan comentarios en la configuración para documentar la ACL. Se marcaron las siguientes características:

1. Las primeras dos instrucciones permit proporcionan acceso desde cualquier dispositivo al servidor web en 2001:DB8:CAFE:10::10.

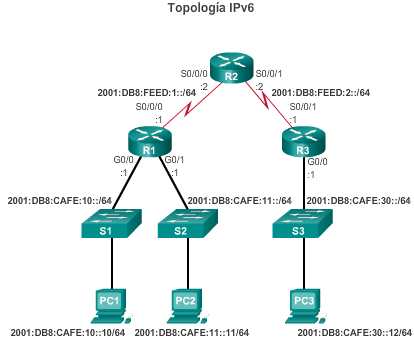
2. El resto de los dispositivos tienen denegado el acceso a la red 2001:DB8:CAFE:10::/64.

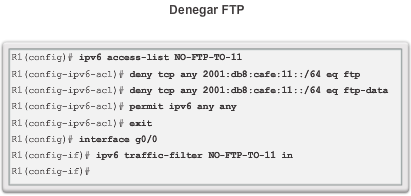
3. A la PC3 en 2001:DB8:CAFE:30::12 se le permite el acceso por Telnet a la PC2, que tiene la dirección IPv6 2001:DB8:CAFE:11::11.

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.





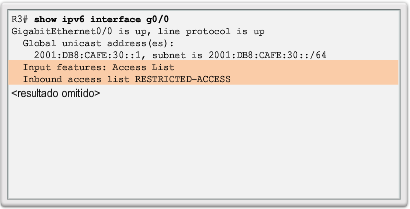


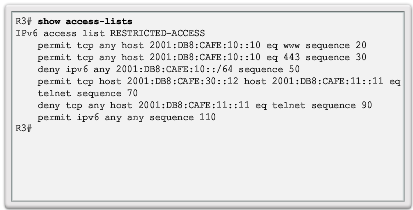
Los comandos que se utilizan para verificar una lista de acceso de IPv6 son similares a los que se utilizan para las ACL de IPv4. Con estos comandos, se puede verificar la lista de acceso de IPv6 RESTRICTED-ACCESS que se configuró anteriormente. En la figura 1, se muestra el resultado del comando **show ipv6 interface**. El resultado confirma que la ACL RESTRICTED-ACCESS está configurada en sentido de entrada en la interfaz G0/0.

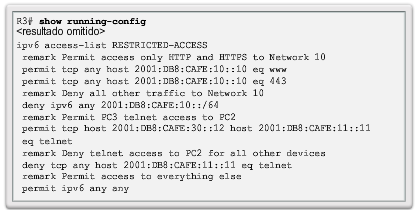
Como se muestra en la figura 2, el comando **show access-lists** muestra todas las listas de acceso en el router, incluidas las ACL de IPv4 y de IPv6. Observe que, en las ACL de IPv6, los números de secuencia se colocan al final de la instrucción y no al principio, como ocurre en las listas de acceso 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**.

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 3, 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.







## Resumen

Los routers no filtran tráfico de manera predeterminada. El tráfico que ingresa al router se enruta solamente en función de la información de la tabla de routing.

El filtrado de paquetes controla el acceso a una red mediante el análisis de los paquetes entrantes y salientes y la transferencia o el descarte de estos según criterios como la dirección IP de origen, la dirección IP de destino y el protocolo incluido en el paquete. Un router que filtra paquetes utiliza reglas para determinar si permite o deniega el tráfico. Un router también puede realizar el filtrado de paquetes en la capa 4, la capa de transporte.

Una ACL es una lista secuencial de instrucciones permit o deny. La última instrucción de una ACL siempre es una instrucción deny implícita que bloquea todo el tráfico. Para evitar que la instrucción deny any implícita al final de la ACL bloquee todo el tráfico, es posible agregar la instrucción**permit ip any any**.

Cuando el tráfico de la red atraviesa una interfaz configurada con una ACL, el router compara la información dentro del paquete con cada entrada, en orden secuencial, para determinar si el paquete coincide con una de las instrucciones. Si se encuentra una coincidencia, el paquete se procesa según corresponda.

Las ACL se configuran para aplicarse al tráfico entrante o al tráfico saliente.

Las ACL estándar se pueden utilizar para permitir o denegar el tráfico de direcciones IPv4 de origen únicamente. El destino del paquete y los puertos involucrados no se evalúan. La regla básica para la colocación de una ACL estándar es colocarla cerca del destino.

Las ACL extendidas filtran paquetes según varios atributos: el tipo de protocolo, la dirección IPv4 de origen o de destino y los puertos de origen o de destino. La regla básica para la colocación de una ACL extendida es colocarla lo más cerca posible del origen.

El comando de configuración global**access-list** define una ACL estándar con un número en el intervalo de 1 a 99 o una ACL extendida con un número en el intervalo de 100 a 199 y de 2000 a 2699. Tanto las ACL estándar como las extendidas pueden tener un nombre. El comando **ip access-list standard***nombre* se utiliza para crear una ACL estándar con nombre, mientras que el comando **ip access-list extended***nombre* se utiliza para una lista de acceso extendida. Las ACE de IPv4 incluyen el uso de máscaras wildcard.

Después de que se configura una ACL, se vincula a una interfaz mediante el comando **ip access-group** del modo de configuración de interfaz. Recuerde la regla de las tres P: una ACL por protocolo, por sentido y por interfaz.

Para eliminar una ACL de una interfaz, primero introduzca el comando **no ip access-group** en la interfaz y, a continuación, introduzca el comando global**no access-list** para eliminar la ACL completa.

Los comandos **show running-config** y**show access-lists** se utilizan para verificar la configuración de la ACL. El comando **show ip interface** se utiliza para verificar la ACL en la interfaz y el sentido en el que se aplicó.

El comando **access-class** configurado en el modo de configuración de línea restringe las conexiones de entrada y salida entre una VTY determinada y direcciones en una lista de acceso.

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 global, utilice el comando **ipv6 access-list** *nombre* para crear una ACL de IPv6. A diferencia de las ACL de IPv4, las ACL de IPv6 no utilizan máscaras wildcard. En cambio, se utiliza la longitud de prefijo para indicar cuánto de una dirección IPv6 de origen o destino debe coincidir.

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

