TIPOS DE ACLs.

Al crear listas de control de acceso, el administrador de red tiene varias opciones. La complejidad de las pautas de diseño determina el tipo de ACL necesaria.

Hay tres clases de ACL:

ACL estándar

La ACL estándar es la más simple de las tres clases. Al crear una ACL IP estándar, las ACL filtran según la dirección IP de origen de un paquete. Las ACL estándar permiten o deniegan el acceso de acuerdo con la totalidad del protocolo, como IP. De esta manera, si un dispositivo host es denegado por una ACL estándar, se deniegan todos los servicios provenientes de ese host. Este tipo de ACL sirve para permitir el acceso de todos los servicios de un usuario específico, o LAN, a través de un router y, a la vez, denegar el acceso de otras direcciones IP. Las ACL estándar están identificadas por el número que se les ha asignado. Para las listas de acceso que permiten o deniegan el tráfico IP, el número de identificación puede variar entre 1 y 99 y entre 1300 y 1999.

ACL extendidas

Las ACL extendidas filtran no sólo según la dirección IP de origen, sino también según la dirección IP de destino, el protocolo y los números de puertos. Las ACL extendidas se utilizan más que las ACL estándar porque son más específicas y ofrecen un mayor control. El rango de números de las ACL extendidas va de 100 a 199 y de 2000 a 2699.

ACL nombradas

Las ACL nombradas (NACL, Named ACL) son ACL estándar o extendidas a las que se hace referencia mediante un nombre descriptivo en lugar de un número. Cuando se configuran ACL nombradas, el IOS del router utiliza un modo de subcomando de NACL.

Tipos de Listas de acceso IOS

Tipo de ACL	Ejemplo de comando/sentencia ACL	Objetivo de sentencia
Estándar	`Router(config)#access-list 1 permit host 172.16.2.88`	• Permite una dirección IP específica
Extendida	`Router(config)#access-list 100 deny tcp 172.16.2.0 0.0.0.255 any eq telnet`	• Deniega el acceso desde la subred 172.16.2.0/24 a cualquier otro host, si están intentando utilizar telnet
Nombrado	`Router(config)#ip access-list standard permit-ip` `Router(config-ext-nacl)#permit host 192.168.5.47`	• Crea una lista de acceso estándar que se denomina permit-ip • Permite el acceso desde la dirección IP 192.168.5.47 • El primer comando configura al router en el modo de subcomando NACL

Las listas de control de acceso consisten de una o más sentencias. Cada sentencia puede permitir o denegar el tráfico según parámetros específicos. El tráfico se compara con cada sentencia de la ACL en forma secuencial hasta encontrar una coincidencia o hasta que no haya más sentencias.

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. Esta función impide la entrada accidental de tráfico no deseado.

Después de crear una lista de control de acceso, aplíquela a una interfaz para que entre en vigencia. La ACL se aplica al tráfico entrante o saliente a través de la interfaz. Si un paquete coincide con una sentencia de permiso, se le permite entrar o salir del router. Si coincide con una sentencia de denegación, no puede seguir avanzando. Una ACL que no tiene al menos una sentencia de permiso bloquea todo el tráfico. Esto se debe a que al final de todas las ACL hay una denegación implícita. Por lo tanto, una ACL rechazará todo el tráfico que no está específicamente permitido.

El administrador aplica una ACL entrante o saliente a una interfaz de router. La dirección se considera entrante o saliente desde la perspectiva del router. El tráfico que ingresa a un interfaz será entrante y el tráfico que sale de ella será saliente.

Cuando un paquete llega a una interfaz, el router controla los siguientes parámetros:

¿Hay una ACL asociada con la interfaz?
¿La ACL es entrante o saliente?
¿El tráfico coincide con los criterios para permitir o para denegar?

Una ACL aplicada en dirección saliente a una interfaz no tiene efectos sobre el tráfico entrante en esa misma interfaz.

Cada interfaz de un router puede tener una ACL por dirección para cada protocolo de red. Respecto del protocolo IP, una interfaz puede tener una ACL entrante y una ACL saliente al mismo tiempo.

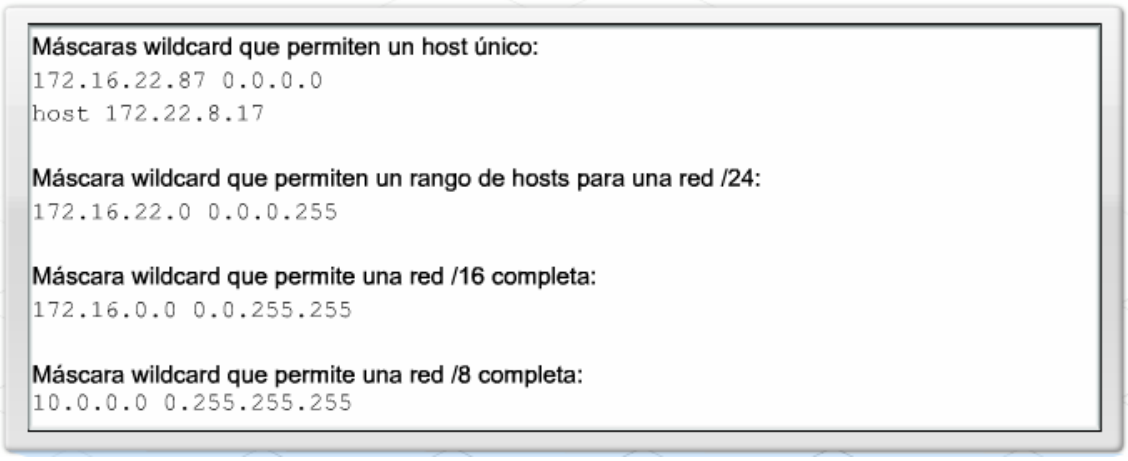
Las ACL aplicadas a una interfaz agregan latencia al tráfico. Incluso una ACL larga puede afectar el rendimiento del router.

MÁSCARA DE WILDCAD.

Las ACL simples especifican solamente una dirección permitida o denegada. Para bloquear varias direcciones o rangos de direcciones se deben utilizar varias sentencias o una máscara wildcard. El uso de una dirección de red IP con una máscara wildcard proporciona una flexibilidad mucho mayor. Una máscara wildcard puede bloquear un intervalo de direcciones o una red entera con una sentencia.

Las máscaras wildcard utilizan ceros para indicar la parte de una dirección IP que debe coincidir exactamente y unos para indicar la parte de una dirección IP que no debe coincidir con un número específico.

La máscara wildcard 0.0.0.0 requiere una coincidencia exacta con los 32 bits de la dirección IP. Esta máscara equivale al uso del parámetro host.



La máscara wildcard que se utiliza con las ACL funciona como la que se utiliza en el protocolo de enrutamiento OSPF. Sin embargo, el propósito de cada máscara es diferente. Con las sentencias ACL, la máscara wildcard especifica un host o un intervalo de direcciones que se deben permitir o denegar.

Al crear una sentencia ACL, la dirección IP y la máscara wildcard se convierten en los campos de comparación. Todos los paquetes que entran o salen de una interfaz se comparan con cada una de las sentencias de la ACL para determinar si hay coincidencia. La máscara wildcard determina cuántos bits de la dirección IP entrante coinciden con la dirección de comparación.

A modo de ejemplo, la siguiente sentencia permite todos los hosts de la red 192.168.1.0 y bloquea todos los demás:

access-list 1 permit 192.168.1.0 0.0.0.255

La máscara wildcard especifica que sólo los primeros tres octetos deben coincidir. Por lo tanto, si los primeros 24 bits del paquete entrante coinciden con los primeros 24 bits del campo de comparación, se permite el paquete. Cualquier paquete con una dirección IP de origen comprendida dentro del intervalo de 192.168.1.1 a 192.168.1.255 coincide con la combinación de dirección y máscara de comparación del ejemplo. Todos los demás paquetes son denegados por la sentencia ACL deny any implícita.

Objetivo de la sentencia ACL	Máscara wildcard
Deniegue todos los hosts de la red 192.168.55.0/24	
Permita todos los hosts de la subred 172.20.4.0/24	
Permita sólo el host 10.10.10.1	
Deniegue sólo el host 192.168.93.240	
Deniegue todos los hosts de la red 172.30.0.0/16	
Deniegue todos los hosts de la red 172.25.0.0/16	
Permita todos los hosts de la red 10.0.0.0/8	
Deniegue todos los hosts de la subred 10.0.0.0/16	

Al crear una ACL, hay dos parámetros especiales que se pueden utilizar en lugar de una máscara wildcard: host y any.

Parámetro host

Para filtrar un único host específico, use la máscara wildcard 0.0.0.0 después de la dirección IP o el parámetro host antes de la dirección IP.

R1(config)#access-list 9 deny 192.168.15.99 0.0.0.0

Es igual a:

R1(config)#access-list 9 deny host 192.168.15.99

Parámetro any

Para filtrar todos los hosts, use parámetros formados por unos configurando la máscara wildcard 255.255.255.255. Cuando se usa la máscara wildcard 255.255.255.255, se considera que todos los bits coinciden, por lo tanto la dirección IP normalmente se representa como 0.0.0.0. Otra forma de filtrar todos los hosts es usar el parámetro any.

R1(config)#access-list 9 permit 0.0.0.0 255.255.255.255

Es igual a:

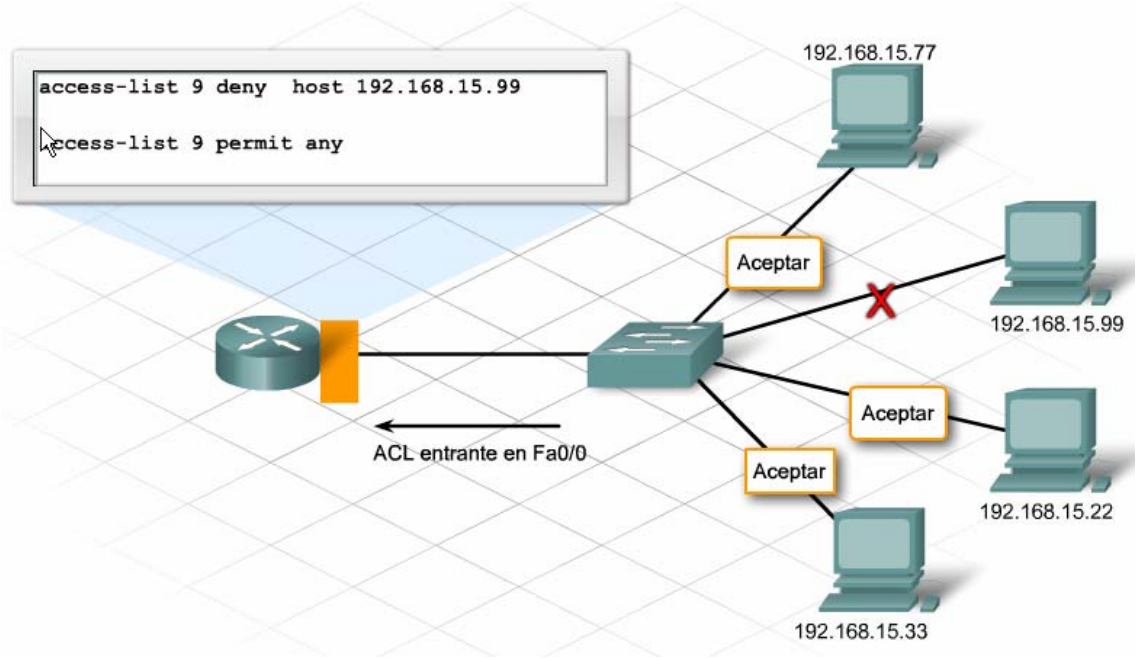
R1(config)#access-list 9 permit any

Considere el ejemplo siguiente, donde se deniega un host específico y se permiten todos los demás:

R1(config)#access-list 9 deny host 192.168.15.99

R1(config)#access-list 9 permit any

El comando permit any permite todo el tráfico que no está específicamente denegado en la ACL. Cuando se utiliza esta configuración, ningún paquete llega al parámetro deny any implícito al final de la ACL.



En una red empresarial con un esquema de direccionamiento IP jerárquico, con frecuencia es necesario filtrar el tráfico de la subred.

Si se usan 3 bits para dividir en subredes la red 192.168.77.0, la máscara de subred es 255.255.255.224. Si se resta la máscara de subred de la máscara compuesta por todos 255, el resultado es la máscara wildcard 0.0.0.31. Para permitir los hosts de la subred 192.168.77.32, la sentencia ACL es:

access-list 44 permit 192.168.77.32 0.0.0.31

Los primeros 27 bits de cada paquete coinciden con los primeros 27 bits de la dirección de comparación. El intervalo general de direcciones permitidas por esta sentencia va de 192.168.77.33 a 192.168.77.63, que es el intervalo de todas las direcciones de la subred 192.168.77.32.

Dirección de subred: 192.168.77.32 255.255.255.224

Valor del bit	128	64	32	16	8	4	2	1	Valor decimal
Todos 1	1	1	1	1	1	1	1	1	255
Máscara de subred	1	1	1	0	0	0	0	0	224
Máscara wildcard	0	0	0	1	1	1	1	1	31

Bits que coinciden

Bits que no coinciden

Dirección de comparación/base: 192.168.77.32 0.0.0.31

La creación de máscaras wildcard precisas para sentencias ACL proporciona el control necesario para ajustar detalladamente el flujo de tráfico. El filtrado del tráfico de subredes diferentes es el concepto más difícil para los principiantes.

La red 192.168.77.0, con la máscara de subred 255.255.255.192 o /26, crea las siguientes cuatro subredes:

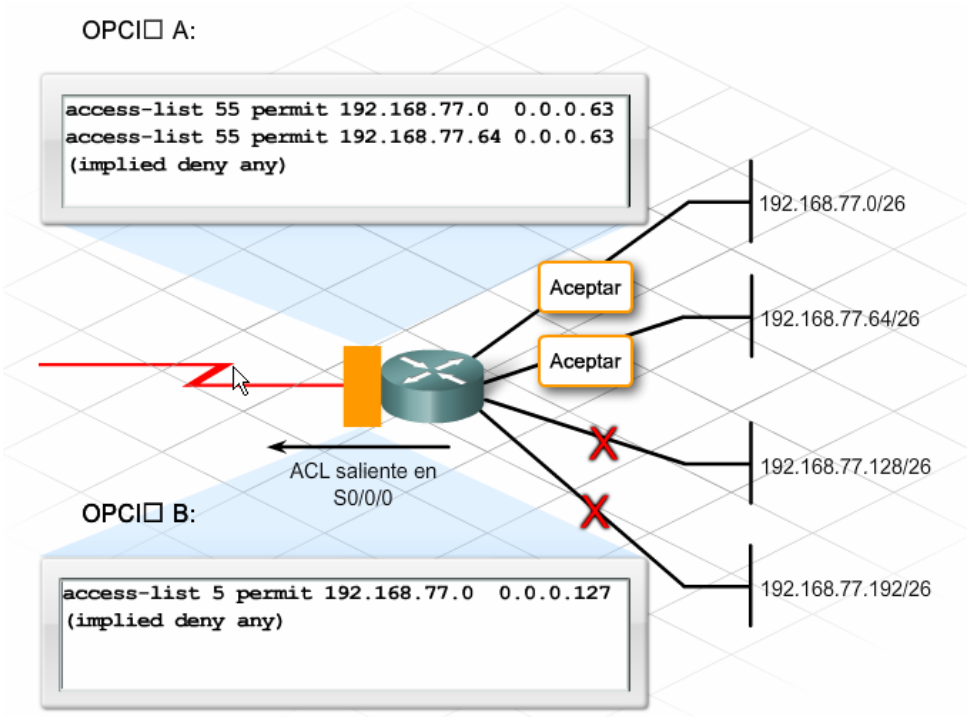
- 192.168.77.0/26
- 192.168.77.64/26
- 192.168.77.128/26
- 192.168.77.192/26

Para crear una ACL para filtrar cualquiera de estas cuatro subredes, reste la máscara de subred 255.255.255.192 de la máscara compuesta por todos 255, que da como resultado la máscara wildcard 0.0.0.63. Para permitir el tráfico proveniente de las dos primeras subredes, use dos sentencias ACL:

access-list 55 permit 192.168.77.0 0.0.0.63
access-list 55 permit 192.168.77.64 0.0.0.63

Las dos primeras redes también se resumen en 192.168.77.0/25. La resta de la máscara de subred resumida de 255.255.255.128 de la máscara con todos 255 da como resultado una máscara wildcard de 0.0.0.127. Al usar esta máscara se agrupan estas dos subredes en una sentencia ACL en lugar de hacerlo en dos sentencias.

access-list 5 permit 192.168.77.0 0.0.0.127



Setencias ACL	Dirección de paquete IP	Permitir	Denegar
access-list 66 permit 192.168.122.128 0.0.0.63	192.168.122.195		
access-list 66 permit 192.168.223.64 0.0.0.31	192.168.223.27		
access-list 66 permit 192.168.223.32 0.0.0.31	192.168.223.60		
access-list 66 permit 192.168.155.0 0.0.0.255	192.168.155.245		
access-list 66 permit 10.93.76.8 0.0.0.3	10.93.76.10		
access-list 66 permit 192.168.155.0 0.0.0.255	192.168.156.245		
access-list 66 permit 172.16.0.0 0.0.255.255	172.17.0.5		

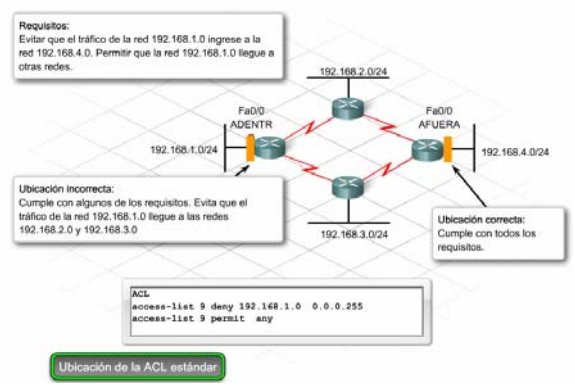
COLOCACION DE LAS ACL.

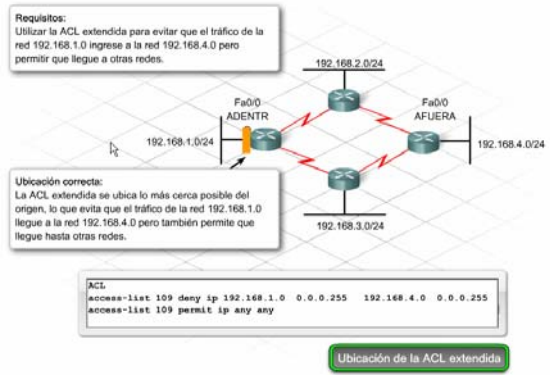
La decisión de utilizar una ACL estándar o una ACL extendida depende de los requisitos de filtrado de la situación. La elección del tipo de ACL puede afectar la flexibilidad de la ACL, así como el rendimiento del router y el ancho de banda del enlace de red.

Las ACL estándar son simples de crear e implementar. Sin embargo, las ACL estándar sólo filtran según la dirección de origen y filtrarán todo el tráfico independientemente del tipo o destino del tráfico. Con rutas hacia varias redes, es posible que una ACL estándar colocada demasiado cerca del origen bloquee involuntariamente el tráfico que se debe permitir. Por lo tanto, es importante colocar las ACL estándar tan cerca del destino como sea posible.

Cuando los requisitos de filtrado sean más complejos, use una ACL extendida. Las ACL extendidas proporcionan un control mayor que las ACL estándar. Filtran en las direcciones origen y destino También filtran observando el protocolo de capa de red, el protocolo de capa de transporte y los números de puertos si fuera necesario. Este detalle de filtrado incrementado permite que los administradores de red creen ACL que satisfagan las necesidades específicas de un plan de seguridad.

Coloque una ACL extendida cerca de la dirección origen. Al observar la dirección origen y destino, la ACL bloquea los paquetes destinados para una red de destino específica antes de que abandonen el router de origen. Los paquetes se filtran antes de cruzar la red, lo que ayuda a conservar el ancho de banda.

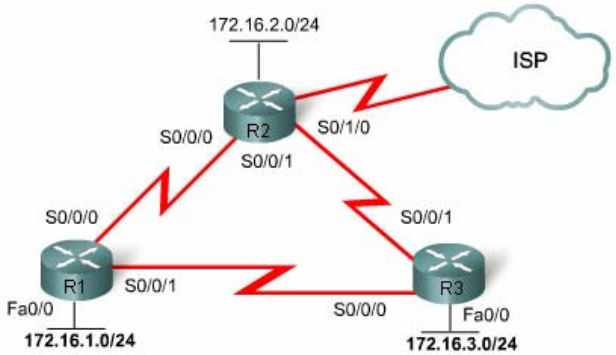




Actividad

Determine el router, la interfaz y la dirección de ubicación correcta de una ACL.

Arrastre el nombre del router, la ubicación de la interfaz y la dirección adecuada para cada lista de control de acceso.



s0/0/1	R2	ADENTRO
R3	S0/1/0	R1
s0/0/0	AFUERA	Fa0/0

Requisito 1:

Usted tiene una ACL extendida que evita que el tráfico de la red 172.16.1.0 llegue a la red 172.16.3.0 pero que permite que llegue a la red 172.16.2.0 y al ISP. Necesita minimizar el tráfico en los enlaces de WAN y sólo puede ubicar la ACL en una interfaz.

```
access-list 101 deny ip 172.16.1.0 0.0.0.255 172.16.3.0 0.0.0255
access-list 101 permit ip any any
```

Router	Interfaz	Dirección

Requisito 2:

Usted tiene una ACL que permite que todo el tráfico de cualquier red 172.16.0.0 llegue a la red ISP pero que bloquea todo otro tráfico.

```
access-list 1 permit 172.16.0.0 0.0.255.255
```

Router	Interfaz	Dirección

Una vez capturados los requisitos, planificada la lista de control de acceso y determinada la ubicación, configure la ACL.

Cada ACL requiere un identificador exclusivo. Este identificador puede ser un número o un nombre descriptivo.

En las listas de control de acceso numeradas, el número identifica el tipo de ACL creada:

Las ACL IP estándar tienen números que van de 1 a 99 y de 1300 a 1999.
Las ACL IP extendidas tienen números que van de 100 a 199 y de 2000 a 2699.

También se puede crear ACL de AppleTalk e IPX.

El límite de cualquier interfaz de router es una ACL por protocolo para cada dirección. Si un router está ejecutando IP exclusivamente, cada interfaz admite un máximo de dos ACL: una entrante y una saliente. Dado que cada ACL compara cada paquete que pasa a través de una interfaz, las ACL aumentan la latencia.

CREACION DE ACLs.

La configuración de una lista de control de acceso exige la realización de dos pasos: creación y aplicación.

Creación de ACL

Entre al modo de configuración global. Con el comando access-list, introduzca las sentencias de la lista de control de acceso. Introduzca todas las sentencias con el mismo número de ACL hasta que la lista de control de acceso esté completa.

La sintaxis de la sentencia de la **ACL ESTÁNDAR** es:

access-list [número de lista de acceso] [deny|permit] [dirección de origen] [source-wildcard][log]

Dado que cada paquete se compara con cada una de las sentencias de ACL hasta encontrar una coincidencia, el orden en el que se colocan las sentencias dentro de la ACL puede afectar la latencia introducida. Por lo tanto, ordene las sentencias de manera que las condiciones más comunes aparezcan en la ACL antes que las menos comunes. Por ejemplo: las sentencias que encuentran una coincidencia para la mayor cantidad de tráfico deben ser colocadas al principio de la ACL.

No obstante, debe tener en cuenta que una vez que se encuentra una coincidencia, el paquete ya no se compara con ninguna de las otras sentencias dentro de la ACL. Esto significa que si una línea permite un paquete, pero una línea que se encuentra más abajo en la ACL lo deniega, el paquete será permitido. Por ello, planifique la ACL de modo que los requisitos más específicos aparezcan antes que los más generales. En otras palabras: rechace un host específico de una red antes de permitir el resto de toda la red.

Documente la función de cada sección o sentencia de la ACL mediante el comando remark:

access-list [número de lista] remark [texto]

Para eliminar una ACL, use el comando:

no access-list [número de lista]

No es posible eliminar una única línea de una ACL estándar o extendida. En cambio, se elimina la totalidad de la ACL y debe ser íntegramente reemplazada.

Una ACL no filtra tráfico hasta tanto haya sido aplicada, o asignada, a una interfaz.
Aplicación de ACL

Asigne una ACL a una o más interfaces y especifique el tráfico entrante o saliente. Aplique una ACL estándar tan cerca del destino como sea posible.

R2(config-if)#ip access-group número de lista de acceso [in | out]

Los siguientes comandos colocan access-list 5 en la interfaz R2 Fa0/0 que filtra tráfico entrante:

R2(config)#interface fastethernet 0/0
R2(config-if)#ip access-group 5 in

La dirección predeterminada de una ACL aplicada a una interfaz es out. Aunque out es el comando predeterminado, es muy importante especificar la dirección para evitar confusiones y garantizar que el tráfico se filtre en la dirección correcta.

Para eliminar una ACL de una interfaz y que la ACL quede intacta, use el comando
no ip access-group interface.

Hay varios comandos de ACL que evalúan la sintaxis correcta, el orden de las sentencias y su colocación en las interfaces.

show ip interface

Muestra información de la interfaz IP e indica las ACL asignadas.

show access-list [número de lista de acceso]

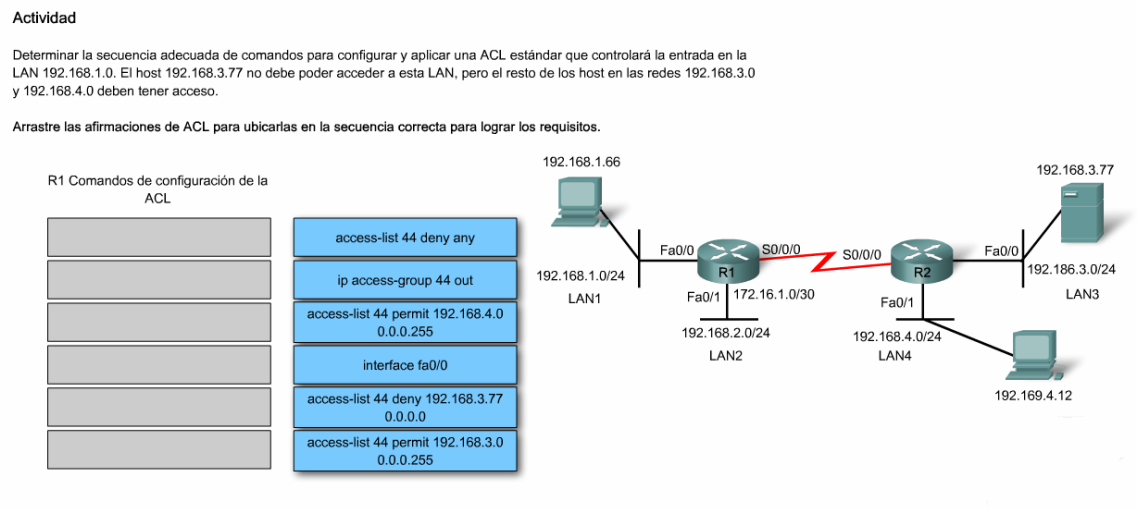
Muestra los contenidos de todas las ACL del router. También muestra la cantidad de coincidencias para cada sentencia de permiso o denegación desde la aplicación de la ACL. Para ver una lista específica, agregue el nombre o número de la ACL como opción a este comando.

show running-config

Muestra todas las ACL configuradas en un router, incluso si no están aplicadas a una interfaz.

Si se utilizan ACL numeradas, las sentencias introducidas después de la creación inicial de la ACL se agregan al final. Este orden no pueden alcanzar los resultados deseados. Para resolver este problema, elimine la ACL y vuelva a crearla.

Con frecuencia se recomienda crear ACL en un editor de texto. Esto permite que la ACL sea fácilmente editada y copiada en la configuración del router. No obstante, al copiar y pegar la ACL tenga en cuenta que es importante eliminar primero la ACL aplicada actualmente; de lo contrario, todas las sentencias se copiarán al final.



ACL EXTENDIDA.

Las ACL extendidas proporcionan un mayor control que las ACL estándar. La ACL extendida permite o deniega el acceso según la dirección IP de origen, la dirección IP de destino, el tipo de protocolo y los números de puertos. Dado que las ACL extendidas pueden ser muy específicas, tienden a aumentar su tamaño rápidamente. Cuantas más sentencias contenga una ACL, más difícil será administrarla.

Las ACL extendidas usan un número de access-list que va de 100 a 199 y de 2000 a 2699. Las mismas reglas que se aplican a las ACL estándar se aplican también a las ACL extendidas:

- Configure varias sentencias en una ACL.
- Asigne el mismo número de ACL a cada sentencia.
- Use las palabras clave host o any para representar direcciones IP.

Una diferencia clave en la sintaxis de las ACL extendidas es el requisito de especificar un protocolo después de la condición de permitir o denegar. Este protocolo puede ser IP, e indicar todo el tráfico IP, o puede indicar el filtrado en un protocolo IP específico, como TCP, UDP, ICMP y OSPF.

```
R2(config)#access-list 105 permit tcp 192.168.5.0 0.0.0.255 host 172.16.5.254 eq http
```

Número ACL

Identifica una ACL con un número único. Una ACL estándar utiliza números dentro de los intervalos de 1 a 99 y de 1300 a 1999. Las ACL extendidas utilizan números entre 100 y 199, y entre 2000 y 2699.

```
R2(config)#access-list 105 permit tcp 192.168.5.0 0.0.0.255 host 172.16.5.254 eq http
```

Condición

Identifica si un paquete debe ser permitido o denegado.

```
R2(config)#access-list 105 permit tcp 192.168.5.0 0.0.0.255 host 172.16.5.254 eq http
```

Protocolo

Identifica protocolos de capa 3 / 4. Las opciones comunes incluyen:

- eigrp protocolo de enrutamiento EIGRP de Cisco
- esp Carga de seguridad de encapsulación
- gre GRE tunneling de Cisco
- icmp Protocolo de mensajes de control de Internet
- igmp Protocolo de mensajes gateway de Internet

```
R2(config)#access-list 105 permit tcp 192.168.5.0 0.0.0.255 host 172.16.5.254 eq http
```

Dirección IP de origen

Identifica la dirección IP del origen del paquete. Este valor puede ser:

- Una dirección de host individual
- Un rango de direcciones de host
- El parámetro del host
- Cualquier parámetro

```
R2(config)#access-list 105 permit tcp 192.168.5.0 0.0.0.255 host 172.16.5.254 eq http
```

Dirección IP de destino

Identifica la dirección IP del destino del paquete. Este valor puede ser:

- Una dirección de host individual
- Un rango de direcciones de host
- El parámetro del host
- Cualquier parámetro

```
R2(config)#access-list 105 permit tcp 192.168.5.0 0.0.0.255 host 172.16.5.254 eq http
```

Condición de coincidencia

Determina si ciertos campos deben coincidir con la aplicación, si deben ser superiores, si deben ser inferiores, etc.

```
R2(config)#access-list 105 permit tcp 192.168.5.0 0.0.0.255 host 172.16.5.254 eq http
```

Aplicación TCP

Identifica la aplicación por número de puerto o por acrónimo.

Por lo general, hay muchas maneras diferentes de cumplir un conjunto de requisitos.

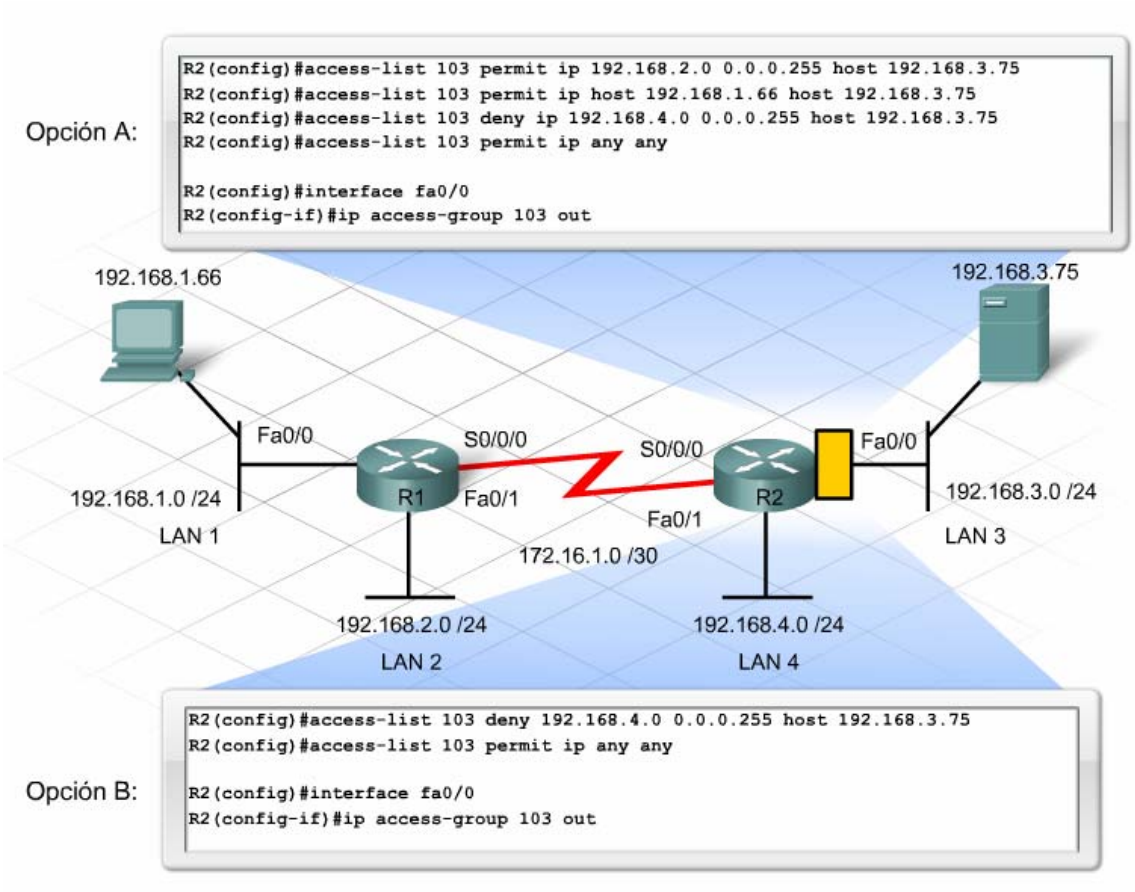
Por ejemplo: una empresa tiene un servidor con la dirección: 192.168.3.75. Tiene los siguientes requisitos:

Permitir el acceso a los hosts de la LAN 192.168.2.0
Permitir el acceso al host 192.168.1.66
Denegar el acceso a los hosts de la LAN 192.168.4.0
Permitir el acceso a todas las personas de la empresa

Hay al menos dos soluciones posibles que cumplen con estos requisitos. Al planificar la ACL, intente minimizar las sentencias siempre que sea posible.

Algunas formas de minimizar sentencias y reducir la carga de procesamiento del router incluyen:

Haga coincidir el tráfico de gran volumen y deniegue el tráfico bloqueado anteriormente en la ACL. Este enfoque garantiza que los paquetes no se comparen con sentencias posteriores.
Consolide varias sentencias de permitir y denegar en una única sentencia mediante intervalos.
Considere la posibilidad de denegar un grupo particular en lugar de permitir un grupo opuesto y más grande.



Las ACL extendidas filtran en las direcciones IP origen y destino. A menudo es conveniente filtrar paquetes en detalles aún más específicos. El protocolo de red de Capa 3 OSI, los protocolos de transporte de Capa 4 y los puertos de la aplicación proporcionan esta capacidad.

Algunos de los protocolos disponibles para el filtrado incluyen IP, TCP, UDP e ICMP.

Las ACL extendidas también filtran en números de puertos destino. Estos números de puerto describen la aplicación o el servicio exigido por el paquete. Cada aplicación tiene asignado un número de puerto registrado.

El router debe investigar la trama Ethernet para extraer todas las direcciones IP y la información necesaria acerca de los números de puerto, para su comparación con las ACL.

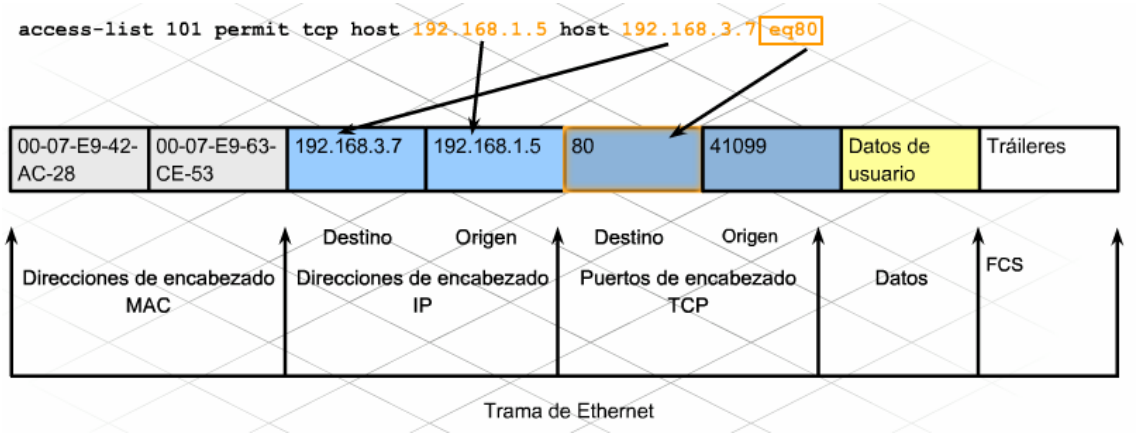
Además de introducir los números de puerto, se debe especificar una condición antes de comparar una sentencia. Las abreviaturas más utilizadas son:

eq: equivale a
gt: mayor que
lt: menor que

Considere el siguiente ejemplo:

R1(config)#access-list 122 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.89 eq 80

Esta sentencia ACL permite el tráfico de 192.168.1.0 que está solicitando acceso HTTP a través del puerto 80. Si un usuario intenta hacer telnet o FTP dentro del host 192.168.2.89, el usuario será denegado debido a la sentencia implícita deny adoptada al final de cada lista de acceso.



El filtrado basado en una aplicación particular exige el conocimiento del número de puerto para esa aplicación. Las aplicaciones están asociadas con un número de puerto y un nombre. Una ACL puede hacer referencia al puerto 80 o HTTP.

Si no se conoce el número de puerto ni el nombre de una aplicación, intente seguir estos pasos para encontrar esa información:

1. Investigue uno de los sitios de registro de las direcciones IP en la Web, como http://www.iana.org/

2. Consulte la documentación del software.

3. Consulte el sitio Web del proveedor de la aplicación.

4. Use un programa detector de paquetes y capture datos de la aplicación.

5. Use la opción ? del comando access-list. La lista incluye nombres y números de puertos conocidos para el protocolo TCP.

Algunas aplicaciones usan más de un número de puerto. Por ejemplo: los datos del FTP se transmiten a través del puerto 20, pero el control de la sesión que hace posible el FTP utiliza el puerto 21. Para rechazar todo el tráfico del FTP, deniegue ambos puertos.

Para incluir varios números de puerto, las ACL del IOS de Cisco filtran un rango de puertos. Use los operadores gt, lt o range en la sentencia ACL para lograr esto. Por ejemplo: dos sentencias ACL de FTP pueden filtrar dentro de una con el comando:

R1(config)#access-list 181 deny tcp any 192.168.77.0 0.0.0.255 range 20 21

A menudo las ACL se crean para proteger una red interna de fuentes externas. Sin embargo, mientras se protege la red interna, se debe permitir que los usuarios internos obtengan acceso a todos los recursos. Cuando los usuarios internos acceden a los recursos externos, dichos recursos solicitados deben pasar a través de la ACL. Por ejemplo: si un usuario interno deseara establecer una conexión con un servidor Web externo, la ACL debe permitir los paquetes html solicitados. Debido al uso de la denegación implícita por parte de las ACL, los recursos deben estar específicamente permitidos por la ACL. Las sentencias individuales de permiso de todos los recursos solicitados pueden traducirse en una ACL larga y dejar resquicios en la seguridad.

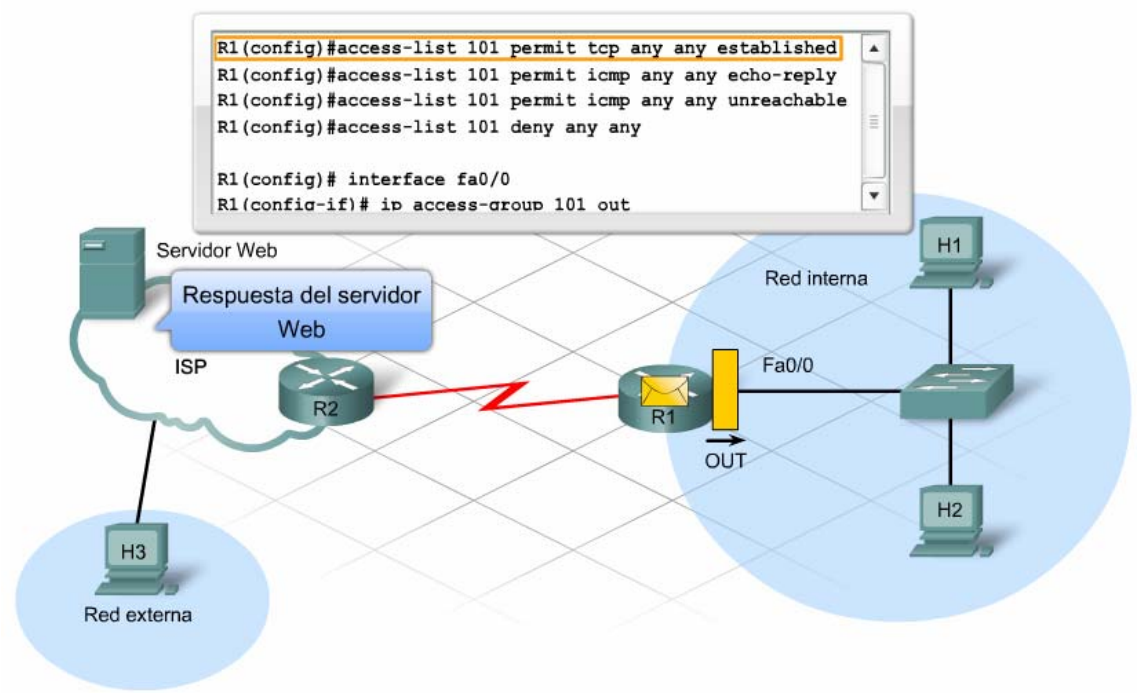
Para resolver este problema se puede crear una sentencia única que permita que los usuarios internos establezcan una sesión TCP con recursos externos. Una vez que se logre el protocolo de enlace de tres vías de TCP y se establezca la conexión, se permitirán todos los paquetes enviados entre los dos dispositivos. Para lograr esto, use la palabra clave: establecido.

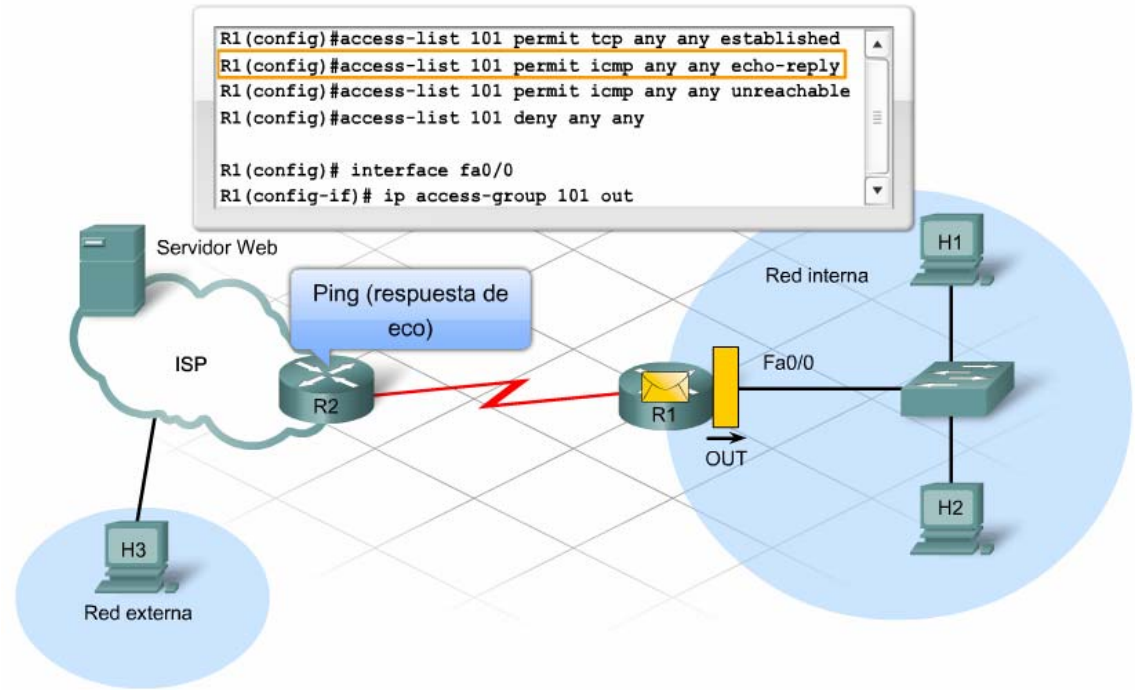
access-list 101 permit tcp any any established

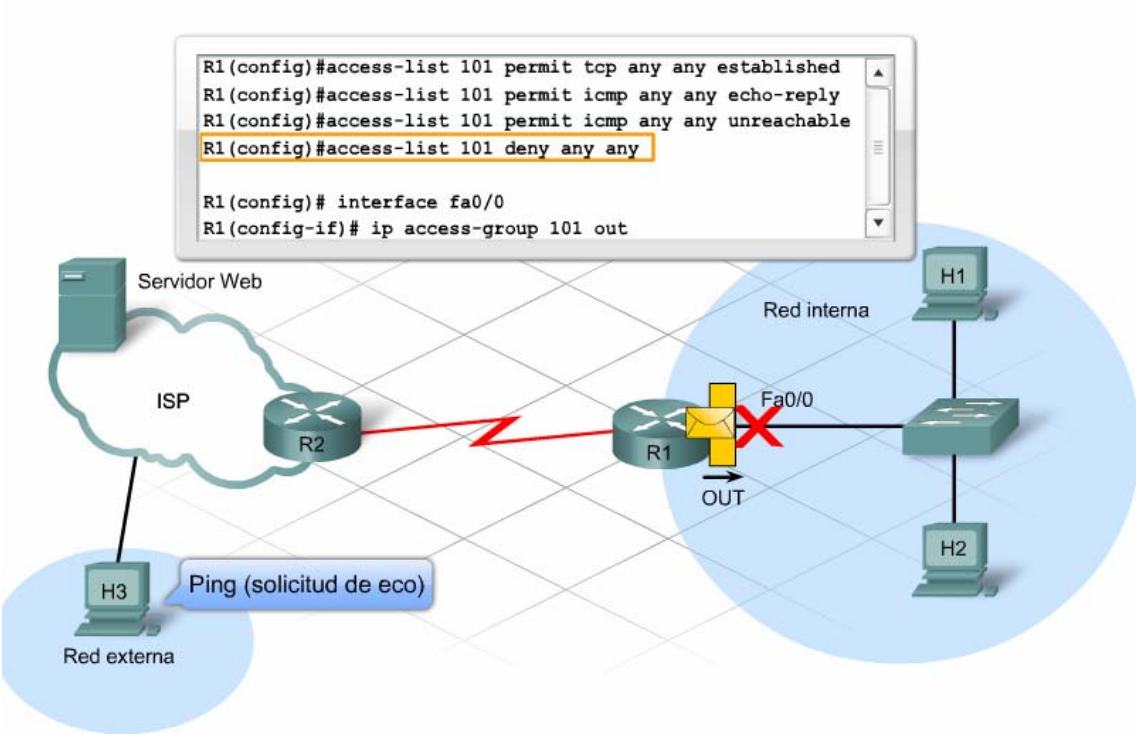
Mediante esta sentencia se permitirán todos los paquetes tcp externos bajo la condición de que sean respuestas a solicitudes internas. Permitir las respuestas entrantes a las comunicaciones establecidas es una forma de Inspección de paquetes con estado (SPI, Stateful Packet Inspection).

Además del tráfico establecido, puede ser necesario que un usuario interno haga ping a dispositivos externos. Sin embargo, no conviene permitir a los usuarios externos hacer ping o rastrear un dispositivo en la red interna. En este caso se puede escribir una sentencia con las palabras clave echo-reply y unreachable para permitir respuestas de

ping y mensajes inalcanzables. Sin embargo, un ping que se origina en fuentes externas será denegado a menos que esté específicamente permitido en otra sentencia.







ACLs NOMBRADAS.

Las versiones 11.2 y superiores del software IOS de Cisco pueden crear ACL nombradas (NACL). En una NACL, un nombre descriptivo reemplaza los intervalos numéricos necesarios para las ACL estándar y extendidas. Las ACL nombradas ofrecen todas las funciones y las ventajas de las ACL estándar y extendidas; sólo difieren en la sintaxis necesaria para crearlas.

El nombre dado a una ACL es único. El uso de mayúsculas en el nombre facilita el reconocimiento en el resultado del comando del router y la resolución de problemas.

Una ACL nombrada se crea con el comando:

ip access-list {standard | extended} name

Después de emitir este comando, el router cambia al modo del subcomando de configuración de NACL. Después del comando inicial de asignación de nombres, introduzca todas las sentencias de permitir y denegar, una por vez. Las NACL usan una sintaxis de comandos de ACL estándar o extendida que comienza con la sentencia de permitir o denegar.

Aplique una ACL nombrada a una interfaz de la misma manera en la que aplica una ACL estándar o extendida.

Los comandos que ayudan a evaluar las ACL nombradas para su correcta sintaxis, el orden de las sentencias y su colocación en interfaces son iguales a los comandos de las ACL estándar.

```
R1(config)#ip access-list extended SALES-ONLY
R1(config-ext-nacl)#permit ip 192.168.1.66 0.0.0.0 any
R1(config-ext-nacl)#permit ip 192.168.1.77 0.0.0.0 any

R1(config)#interface fa0/0
R1(config-if)#ip access-group SALES-ONLY in
```

La edición de las ACL con versiones anteriores del IOS hacen que sea necesario:

Copiar la ACL a un editor de texto.
Eliminar la ACL del router.
Volver a crear y aplicar la versión editada.

Desafortunadamente, este proceso permite que todo el tráfico fluya a través de la interfaz durante el ciclo de edición, y de esa manera se deja la red abierta a potenciales violaciones de seguridad.

Con las versiones actuales del IOS, edite las ACL nombradas y numeradas mediante el comando ip access-list. Las ACL se muestran con las líneas numeradas como 10, 20, 30 y así sucesivamente. Para ver los números de línea, utilice el comando:

show access-lists

Para editar una línea existente:

Elimine la línea mediante el comando no line number
Vuelva a agregar la misma línea mediante su número de línea.
Para insertar una nueva línea entre las líneas 20 y 30 actuales:
Emita la sentencia new ACL, que debe comenzar con un número entre las dos líneas existentes, como 25

Emita el comando show access-lists para mostrar las líneas ordenadas y numeradas nuevamente de 10 en 10.

```
R1(config)#ip access-list extended SERVER-ACCESS
R1(config-ext-nacl)# no 20
R1(config-ext-nacl)# 20 permit ip host 192.168.1.77 any
R1(config-ext-nacl)# end
R1#show access-lists
Extended IP access list SERVER-ACCESS
    10 permit ip host 192.168.1.66 host 192.168.3.75
    20 permit ip host 192.168.1.77 any
    30 deny ip 192.168.1.0 0.0.0.255 host 192.168.3.75
```


R1(config)#ip access-list extended SERVER-ACCESS
R1(config-ext-nacl)# 25 deny ip host 192.168.1.88 any
R1(config-ext-nacl)# end
R1#show access-lists
Extended IP access list SERVER-ACCESS
10 permit ip host 192.168.1.66 host 192.168.3.75
20 permit ip host 192.168.1.77 any
30 deny ip host 192.168.1.88 any
40 deny ip 192.168.1.0 0.0.0.255 host 192.168.3.75