Sistemas de Computación 2

<< Redes >>

Listas de Control de Acceso

Listas de Control de Acceso

Los administradores de redes utilizan firewalls para proteger las redes del uso no autorizado de sus recursos, servicios o trafico de mensajes/paquetes. Los firewalls son soluciones de hardware o de software que aplican las políticas de seguridad de la red, filtran los paquetes no autorizados o potencialmente peligrosos e impiden que ingresen a la red.

En un router se puede configurar un firewall simple que proporcione capacidades básicas de filtrado de tráfico mediante Listas de Control de Acceso. Los administradores utilizan las ACL para detener el tráfico o para permitir solamente tráfico específico en sus redes.

Una Lista de Control de Acceso o ACL (Access Control List) es una serie de comandos del OS que controlan si un router reenvía o descarta paquetes según la información que se encuentra en el encabezado del paquete.

Las ACLs permiten controlar el flujo del tráfico en equipos de redes, tales como routers y switches. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.

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.

Tareas de las ACL

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.

Aplicación de ACL

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.

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.

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.

Evaluación de las ACL

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

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

También puede extraer información de capa superior del encabezado de capa 4, como:

- Puerto de origen TCP/UDP
- Puerto de destino TCP/UDP

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. Las ACL de entrada 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.

Tipos de ACL

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.

Las listas de control de acceso pueden configurarse generalmente para controlar tráfico entrante y saliente y en este contexto son similares a unos firewalls.

Existen dos tipos de ACL:

- 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.
- **ACL extendida**, en cuya sintaxis pueden aparece el protocolo, dirección de origen, de destino, puertos UDP o TCP de origen y destino.

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

ACL numeradas, Asignar un numero según el protocolo

- 1 a 99 y del 1300 a 1999: ACL de IP estándar
- 100 a 199 y del 2000 a 2699: ACL de IP extendida

ACL con nombre:

- Incluye caracteres alfanuméricos
- Se sugiere sean en mayúsculas
- No puede haber espacios ni puntuación

Máscara 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.

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.

- Bit 0 de wildcard: establece 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.

A las máscaras wildcard a menudo se las denomina “máscaras inversas”.

- Tanto en la dirección de origen, como en la dirección de destino, se especifican las direcciones como dos grupos de números: un número IP, y una máscara wildcard.
- Si se traduce a binario, los “1” en la máscara wildcard significan que en la dirección IP correspondiente puede ir cualquier valor.
- Para permitir o denegar una red o subred, la máscara wildcard es igual a la máscara de subred, cambiando los “0” por “1” y los “1” por “0” (en binario).
- Sin embargo, las máscaras wildcard también permiten más; por ejemplo, se pueden permitir el rango de IP 1-31, en varias subredes a la vez.

Máscara Wildcard

Posición del bit en el octeto y valor de dirección para el bit

128	64	32	16	8	4	2	1	Ejemplo
0	0	0	0	0	0	0	0	= hacer coincidir todos los bits de la dirección
0	0	1	1	1	1	1	1	= ignorar los últimos 6 bits de la dirección
0	0	0	0	1	1	1	1	= omitir los últimos 4 bits de la dirección
1	1	1	1	1	1	0	0	= ignorar los primeros 6 bits de la dirección
1	1	1	1	1	1	1	1	= omitir todos los bits de la dirección

	Dirección Decimal	Dirección Binaria
Dirección IP a procesar	192.168.10.1	11000000.10101000.00001010.00000001
máscara Wildcard	0.0.255.255	00000000.00000000.11111111.11111111
Dirección IP resultante	192.168.0.0	11000000.10101000.00000000.00000000

Máscara Wildcard

	Dirección Decimal	Dirección Binaria
Dirección IP a procesar	192.168.16.1	11000000.10101000.00010000.00000001
máscara Wildcard	0.0.15.255	00000000.00000000.00001111.11111111
Rango IP resultante	De 192.168.16.0 a 192.168.31.255	11000000.10101000.00010000.00000000 11000000.10101000.00011111.11111111

	Dirección Decimal	Dirección Binaria
Dirección IP a procesar	192.168.1.1	11000000.10101000.00000001.00000001
máscara Wildcard	0.0.254.255	00000000.00000000.11111110.11111111
Rango IP resultante	192.168.1.0 ...	11000000.10101000.00000001.00000000 Todas las subredes con nro impar en red 192.168.0.0

Máscara Wildcard

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

Supongamos que deseamos permitir el acceso a todos los usuarios en la red 192.168.3.0. 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.

	255.255.255.255
-	255.255.255.000
	000.000.000.255

Cálculo de máscara wildcard: ejemplo 2

Supongamos que deseamos 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, a 255.255.255.255 se le resta la máscara de subred 255.255.255.240. El resultado genera la máscara wildcard 0.0.0.15.

	255.255.255.255
-	255.255.255.240
	000.000.000.015

Cálculo de máscara wildcard: ejemplo 3

Supongamos que solo queremos establecer la coincidencia con las redes 192.168.10.0 y 192.168.11.0. Una vez más, a 255.255.255.255 se le resta la máscara de subred regular que, en este caso, es 255.255.252.0. El resultado es 0.0.3.255.

	255.255.255.255
-	255.255.252.000
	000.000.003.255

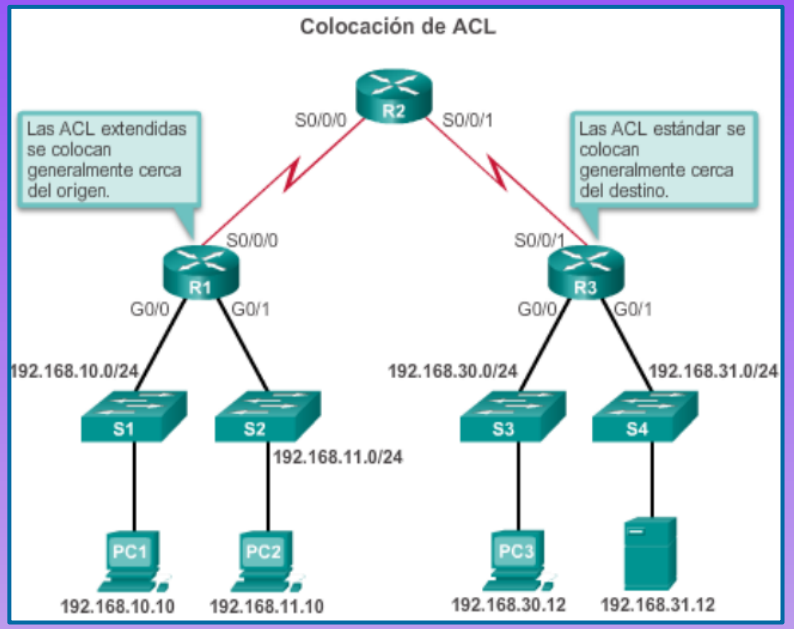
Máscara Wildcard

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



Políticas ACL

Las políticas a seguir al crear una ACL pueden ser de dos tipos:

1) Se bloquea todo excepto los indicados.
2) Se permite todo excepto los indicados

Siempre van primero los indicados o específicos y por último lo general ya que las lista son jerárquicas y la primera que encuentra con la condición se ejecuta y no verifica ninguna más.

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. El router 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 contrario, se bloquea todo el tráfico.

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.

Procesamiento ACL

Lógica de ACL de entrada

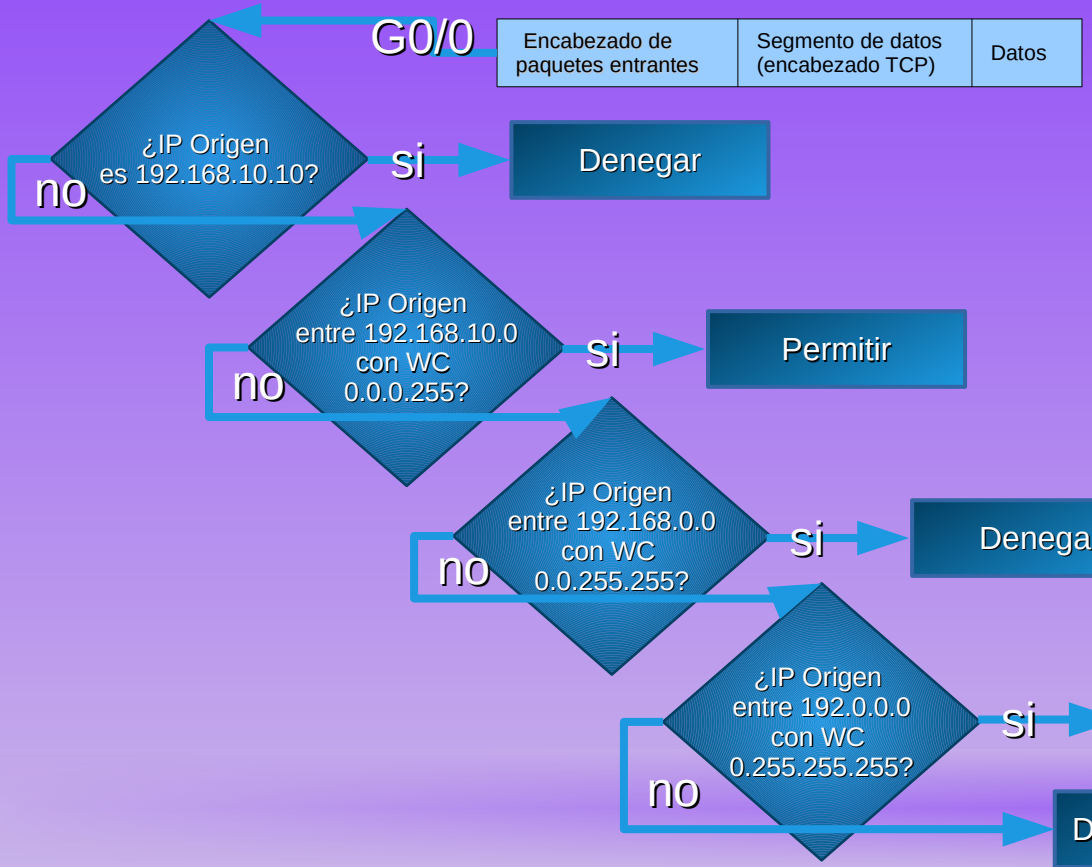
En la figura, se muestra la lógica para una ACL de entrada. Si hay una coincidencia entre la información en un encabezado de paquete y una instrucción de ACL, el resto de las instrucciones de la lista se omiten y se permite o se deniega el paquete según lo especificado por la instrucción de la coincidencia. 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 ACL Estándar

Para bloqueo de redes o habilitación de las mismas

```
access-list [1-99] [permit/deny] [dirección de red] [máscara wildcard]
```



Ejemplo: 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
```

Procesamiento ACL

Lógica de 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

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.

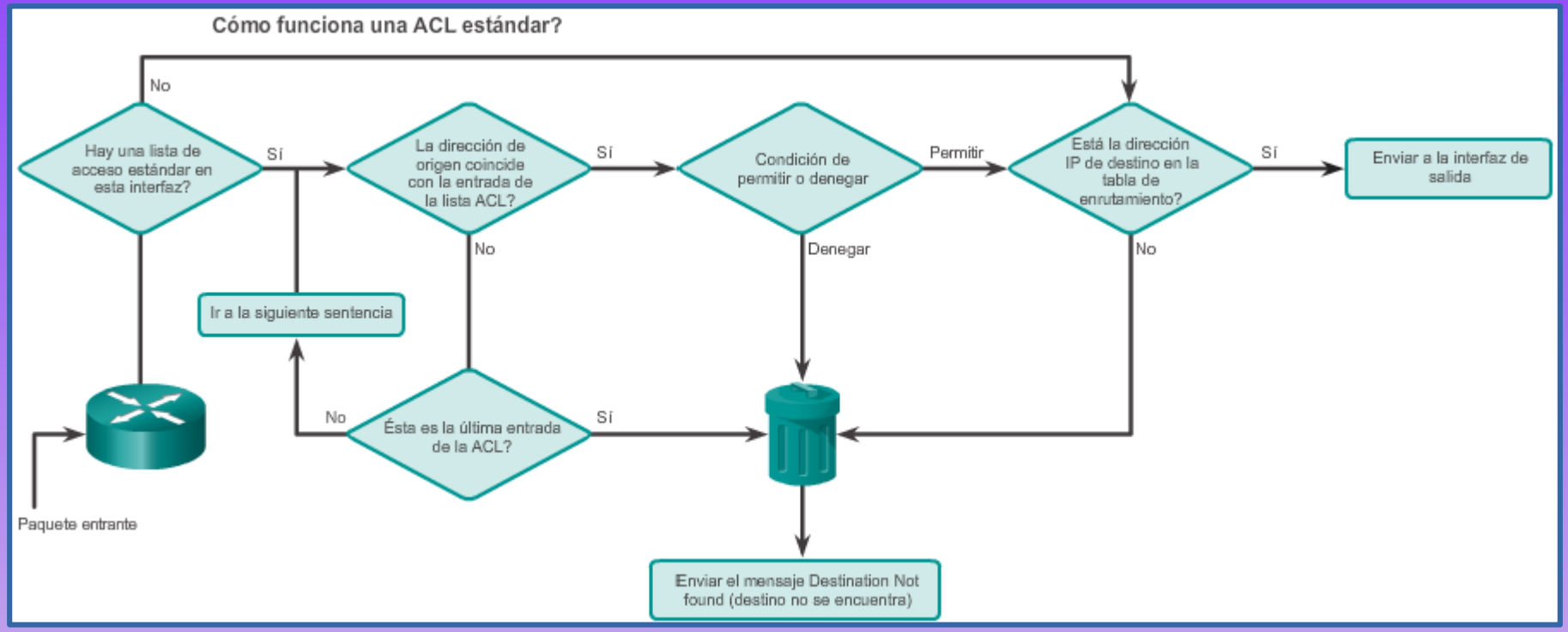
Si se acepta la dirección de la trama, se desmonta la información de la trama y el router revisa si hay una ACL en la interfaz de entrada. Si existe una ACL, el paquete se prueba en relación con las instrucciones de la lista.

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.

ACL y routing



ACL Estándar

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

Parámetro	Descripción
access-list-number	Es un número decimal del 1 al 99 o del 1300 al 1999 (para las ACL estándar).
deny	Deniega el acceso si las condiciones concuerdan.
permit	Permite el acceso si las condiciones concuerdan.
remark	Agrega un comentario sobre las entradas en la lista de acceso IP para facilitar la comprensión y el análisis de la lista.
source	Número de la red o del host desde el que se envía el paquete. Existen dos formas de especificar el origen. Expresar con dirección de 32 bits en formato decimal punteado de cuatro octetos. Utilice la palabra clave any como abreviatura de origen y wildcard-origen de 0.0.0.0 255.255.255.255.
source-wildcard	(Optativo) Máscara wildcard de 32 bits para aplicar al origen. Coloca unos en las posiciones de bits que desea omitir.
log	(Optativo) Genera un mensaje de registro informativo en la consola acerca del paquete que coincide con la ACL

ACL Extendida

```
Router(config)# access-list access-list-number {permit | deny | remark} protocol source [source-wildcard] destination {destination-wildcard} [operator operand] [port port-number] [established]
```

Parámetro	Descripción
access-list-number	Es un número decimal del 100 al 199 o del 2000 al 2699 (para las ACL estándar).
deny	Deniega el acceso si las condiciones concuerdan.
permit	Permite el acceso si las condiciones concuerdan.
remark	Agrega un comentario para facilitar la comprensión y el análisis de la lista.
protocol	Nombre o numero de un protocolo de internet (icmp, ip, tpc, udp)
source	Número de la red o del host desde el que se envía el paquete.
source-wildcard	(Optativo) Máscara wildcard de 32 bits para aplicar al origen.
destination	Numero de la red o del host al cual se envían los paquetes.
destination-wildcard	Máscara wildcard de 32 bits para aplicar al destino.
operator	(Optativo) Compara los puertos de origen y destino. lt (menor que) gt (mayor que) eq (igual a) neq (distinto que)
port	(Optativo) El numero decimal o el nombre del puerto (21 FTP, 23 Telnet, 25 SMTP, 69 TFTP, 53 DNS, 80 HTTP)
established	(Optativo) Solo para el protocolo TCP. indica que sólo pasarán paquetes TCP con los flags ACK o RST activados, es decir, que no permite pasar ningún comienzo de conexión con el flag SYN=1 ACK=0, de inicio de sesión TCP. Esto fuerza a que el establecimiento de la conexión se realice en el sentido contrario donde está la ACL.

ACL con nombre

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.

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.
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.
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`).

Comandos ACL

La forma **no** de este comando se utiliza para eliminar la ACL:

```
Router(config)#no access-list access-list-number

Router(config)#no ip access-list {extended|standard} access-list-name
```

Una vez creada la ACL habrá que asociarla a una interfaz entrante o saliente.

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

Antes de eliminar una ACL es recomendable desasociarla de la interfaz con **no**:

```
Router(config-if)#no ip access-group {access-list-number | access-list-name} {in | out}
```

Para poder verificar las ACL creadas en el router:

```
Router#show access-list
```

Para ver la configuración completa del router y verificar las ACL en cada interfaz:

```
Router#show running-config
```

ACL

- *Configurar ACL de IP de uso general*
- *Configuracion ACL Standard*
- *Configuracion ACL Extended*
- *Bloquear servicios con ACL Extendida*
- *Configurando ACL con nombre en una red Packet Tracer*

Bibliografía & Licencia

- CCNA 2 (2017). Switching, Routing and Wireless Essentials. Cisco Press.
- Textos tomados, corregidos y modificados de diferentes páginas de Internet, tutoriales y documentos.

- Autor:

Matías E. García

Prof. & Tec. en Informática Aplicada

www.profmatiasgarcia.com.ar

info@profmatiasgarcia.com.ar