ACLs: Listas de Control de Acceso

Creación de las ACL

Las ACL se crean en el modo de configuración global. Existen varias clases diferentes de ACLs: estándar, extendidas, IPX, AppleTalk, entre otras. Cuando configure las ACL en el router, cada ACL debe identificarse de forma única, asignándole un número. Este número identifica el tipo de lista de acceso creado y debe ubicarse dentro de un rango específico de números que es válido para ese tipo de lista.

Protocolo	Intervalo
IP	1-99, 1300-1999
IP extendido	100-199, 2000-2699
AppleTalk	600-699
IPX	800-899
IPX extendido	900-999
Protocolo de publicación de servicio IPX	1000-1099

Después de ingresar al modo de comando apropiado y que se decide el número de tipo de lista, el usuario ingresa sentencias de lista de acceso utilizando el comando access-list, seguida de los parámetros necesarios. Estando en el modo de comandos adecuado y definido el tipo de número de lista, el usuario tipea las condiciones usando el comando access-list seguido de los parámetros apropiados. Este es el primero de un proceso de dos pasos. El segundo paso consiste en asignar la lista a la interfaz apropiada.

Paso 1	Definir la ACL con el siguiente comando: `Router(config)#access-list access-list-number {permit | deny} {test-conditions}` Una sentencia global identifica la ACL. Específicamente, el intervalo 1-99 se reserva para IP estándar. Este número se refiere al tipo de ACL. En la versión 11.2 o posterior de Cisco IOS, las ACL también pueden usar un nombre ACL, como educación_grupo, en lugar de un número El término permit o deny (permitir o denegar) de la sentencia ACL global indica cuántos paquetes que cumplan con las condiciones de prueba maneja el software Cisco IOS. Permit generalmente significa que el paquete puede usar una o más interfaces que se especifican posteriormente. El (Los) último(s) término(s) especifican las condiciones de prueba que utiliza la sentencia ACL.
	A continuación, es necesario aplicar las ACL en una interfaz mediante el comando access-group, como se muestra en el ejemplo.

En TCP/IP, las ACL se asignan a una o más interfaces y pueden filtrar el tráfico entrante o saliente, usando el comando ip access-group en el modo de configuración de interfaz. Al asignar una ACL a una interfaz, se debe especificar la ubicación entrante o saliente. Es posible establecer la dirección del

filtro para verificar los paquetes que viajan hacia dentro o fuera de una interfaz. Para determinar si la ACL controla el tráfico entrante o saliente, el administrador de red necesita mirar las interfaces como si se observara desde dentro del router. Este es un concepto muy importante. Una lista de acceso entrante filtra el tráfico que entra por una interfaz y la lista de acceso saliente filtra el tráfico que sale por una interfaz.

```
Router(config)#access-list 2 deny 172.16.1.1
Router(config)#access-list 2 permit 172.16.1.0 0.0.0.255
Router(config)#access-list 2 deny 172.16.0.0 0.0.255.255
Router(config)#access-list 2 permit 172.0.0.0
Router(config)#interface e0
Router(config-if)#ip access-group 2 in
```

Una ACL que contiene sentencias ACL numeradas no puede ser alterada. Se debe borrar utilizando el comando no access-listlist-number y entonces proceder a recrearla.

```
Router(config)#no access-list 2
```

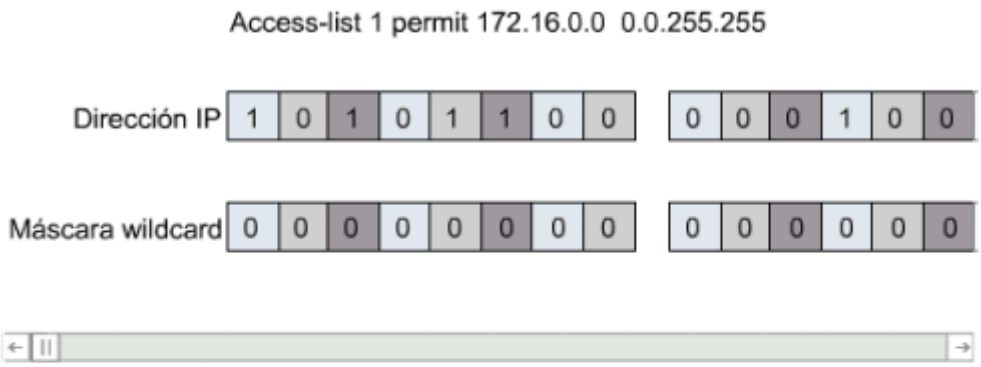
Es necesario utilizar estas reglas básicas a la hora de crear y aplicar las listas de acceso.

- Una lista de acceso por protocolo y por dirección.
- Se deben aplicar las listas de acceso estándar que se encuentran lo más cerca posible del destino.
- Se deben aplicar las listas de acceso extendidas que se encuentran lo más cerca posible del origen.
- Utilice la referencia de la interfaz entrante y saliente como si estuviera mirando el puerto desde adentro del router.
- Las sentencias se procesan de forma secuencial desde el principio de la lista hasta el final hasta que se encuentre una concordancia, si no se encuentra ninguna, se rechaza el paquete.
- Hay un deny any (denegar cualquiera)implícito al final de todas las listas de acceso. Esto no aparece en la lista de configuración.
- Las entradas de la lista de acceso deben realizar un filtro desde lo particular a lo general. Primero se deben denegar hosts específico y por último los grupos o filtros generales.
- Primero se examina la condición de concordancia. El permiso o rechazo se examina SÓLO si la concordancia es cierta.
- Nunca trabaje con una lista de acceso que se utiliza de forma activa.
- Utilice el editor de texto para crear comentarios que describan la lógica, luego complete las sentencias que realizan esa lógica.
- Siempre, las líneas nuevas se agregan al final de la lista de acceso. El comando no access-listx elimina toda la lista. No es posible agregar y quitar líneas de manera selectiva en las ACL numeradas.

- Una lista de acceso IP envía un mensaje ICMP llamado de host fuera de alcance al emisor del paquete rechazado y descarta el paquete en la papelera de bits.
- Se debe tener cuidado cuando se descarta una lista de acceso. Si la lista de acceso se aplica a una interfaz de producción y se la elimina, según sea la versión de IOS, puede haber una deny any (denegar cualquiera) por defecto aplicada a la interfaz, y se detiene todo el tráfico.
- Los filtros salientes no afectan al tráfico que se origina en el router local.

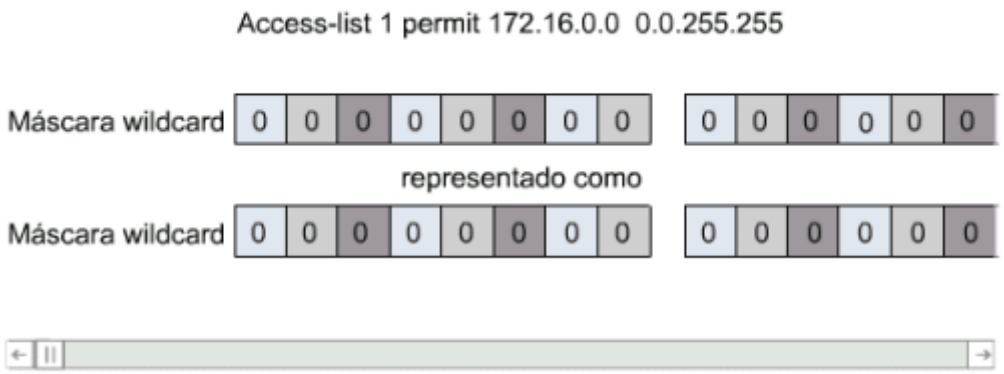
Función de la máscara wildcard

Una máscara wildcard es una cantidad de 32-bits que se divide en cuatro octetos. Una máscara wildcard se compara con una dirección IP. Los números uno y cero en la máscara se usan para identificar cómo tratar los bits de la dirección IP correspondientes. El término máscara wildcard es la denominación aplicada al proceso de comparación de bits de máscara y proviene de una analogía con el “wildcard” (comodín) que equivale a cualquier otro naipe en un juego de póquer. Las máscaras wildcard no guardan relación funcional con las máscaras de subred. Se utilizan con distintos propósitos y siguen distintas reglas. Las máscaras de subred y las máscaras de wildcard representan dos cosas distintas al compararse con una dirección IP. Las máscaras de subred usan unos y ceros binarios para identificar las porciones de red, de subred y de host de una dirección IP. Las máscaras de wildcard usan unos y ceros binarios para filtrar direcciones IP individuales o en grupos, permitiendo o rechazando el acceso a recursos según el valor de las mismas. La única similitud entre la máscara wildcard y la de subred es que ambas tienen 32 bits de longitud y se componen de unos y ceros.

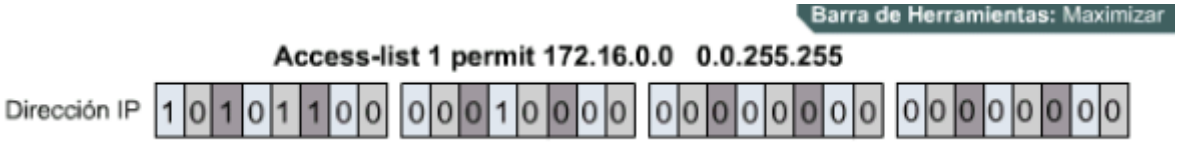


Esta máscara wildcard permitirá una comparación con cualquier valor IP desde 172.16.0.0 a 172.16.255.255. Es importante recordar que la comparación sólo dice que esta sentencia se debe aplicar al paquete. La ACL puede permitir o denegar el acceso al router.

Para evitar la confusión, se substituirán las X por 1 en los gráficos de máscaras wildcard. La máscara en la Figura se escribe como 0.0.255.255. Un cero significa que se deje pasar el valor para verificarlo. Las X (1) significan impedir que se compare el valor.



Se utilizan X para reducir la confusión al aplicar la máscara wildcard. Esta es la convención que se utilizará para mostrar las máscaras wildcard en el resto de los gráficos.



Durante el proceso de máscara wildcard, la dirección IP en la sentencia de la lista de acceso tiene la máscara wildcard aplicada a ella. Esto crea el valor de concordancia, que se utiliza para comparar y verificar si esta sentencia ACL debe procesar un paquete o enviarlo a la próxima sentencia para que se lo verifique. La segunda parte del proceso de ACL consiste en que toda dirección IP que una sentencia ACL en particular verifica, tiene la máscara wildcard de esa sentencia aplicada a ella. El resultado de la dirección IP y de la máscara debe ser igual al valor de concordancia de la ACL ACL.

Hay dos palabras clave especiales que se utilizan en las ACL, las opciones any y host. Para explicarlo de forma sencilla, la opción any reemplaza la dirección IP con 0.0.0.0 y la máscara wildcard por 255.255.255.255. Esta opción concuerda con cualquier dirección con la que se la compare. La máscara 0.0.0.0 reemplaza la opción host. Esta máscara necesita todos los bits de la dirección ACL y la concordancia de dirección del paquete. Esta opción sólo concuerda con una dirección.

```
Router(config)#access-list 1 permit 0.0.0.0 255.255.255.255
```

Se puede escribir como:

```
Router(config)#access-list 1 permit any
```

```
Router(config)#access-list 1 permit 172.30.16.29 0.0.0.0
```

Se puede escribir como:

```
Router(config)#access-list 1 permit host 172.30.16.29
```

Este es el formato de **any** y **host** palabras claves opcionales de la declaración ACL