Módulo II Capítulo 7 – ACLs

Nota aclaratoria:
Que tipo de ACLs hay?
Standard (Unicamente capa 3)
    numerada
    nombrada

Extendida (Capa 3 y 4)
    numerada
    nombrada

¿Cuál es la diferencia entre Access-list y Access Group en una ACE?
- ip access-group 100 in (es para asignarlo a una interfaz en concreto)
- access-list 100 permit ip any any (es para asignarlo a a todo el router)

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 **ACLs o Listas de Control de Acceso**, son un **conjunto** de **reglas** que los **router** y **switches aplican** al **encabezado** de los **paquetes**. Si el **encabezado** del paquete **coincide** con la **regla**, esta se **aplica** sino, se pasará a la **siguiente** de forma **secuencial** hasta llegar a una **compatible** con su **encabezado**. La regla que se aplique finalmente **podrá permitir** o **denegar** el paso del **paquete**.
Es decir, una **ACL filtra el trafico que nos interesa** dejar pasar en base a la IP(de origen o destino), protocolo de transporte, puerto, … de la cabecera del paquete.

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 para asegurar que las actualizaciones provienen de un origen conocido.

- **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 tienen ACL configuradas 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.

Filtrado de paquetes.

Ejemplo de acl(es una acl extendida nombrada):

Extended IP access list HTTP_ONLY

10 permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www

20 permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62

Todas las líneas forman la ACL.

La primera línea indica que es una ACL extendida nombrada con el nombre ***HTTP_ONLY***

La segunda y tercera línea son las ACE(Entrada de control de acceso) por las cuales esta formada la ACL.

Las reglas(ACE) se comprueban secuencialmente.

Cada ACE comienza con un número secuencia(10, 20). Es el orden de comprobación. Las que tienen un número menor se evalúan antes.

Se pueden especificar nuevas reglas e intercalarlas con las anteriores poniéndole un número de secuencia intermedio, por ejemplo 15.

Condensación de los contenidos de CISCO → CADA PALABRA CUENTA

Una ACL es una lista secuencial de instrucciones **permit** (permitir) o **deny** (denegar), conocidas como "**entradas de control de acceso" (ACE)**. 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 ACE. El filtrado de paquetes puede producirse en la capa 3 o capa 4, como se muestra en la ilustración. Las **ACL estándar filtran sólo en la Capa 3**. Las **ACL extendidas filtran en las capas 3 y 4**.El **criterio de filtrado establecido en cada ACE de una ACL de IPv4 estándar es la dirección IPv4 de origen**. Un router configurado con una ACL de IPv4 estándar recupera la dirección IPv4 de origen del encabezado del paquete. El router comienza en la parte superior de la ACL y compara la dirección con cada ACE de manera secuencial. **Cuando encuentra una coincidencia, el router realiza la instrucción, que puede ser permitir o denegar** el paquete. Una vez que se halla una coincidencia, **las ACE restantes** de la ACL, si las hubiera, **no se analizan**. Si la dirección IPv4 de origen no coincide con ninguna ACE en la ACL, se descarta el paquete. La última instrucción 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 ACL **no operan sobre paquetes que se originan en el router mismo**

ACL de entrada:

- Los paquetes entrantes se procesan antes de enturarse a la interfaz de salida.
- Esto ahorran la sobrecarga si el paquete se descarta.
- Si las ACL 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.

wildcard en ACL

La máscara de wildcard es inversa a la máscara de red:

- Máscara de red: 255.255.255.0

  Máscara wildcard equivalente : 0 .0 .0 .255
- Al contrario de la máscara de red, en la máscara wildcard: los bit 0 deben coincidir y los 1 no tienen por que.
- A diferencia de la máscara de red, en la máscara wildcard: los 1 y los ceros se pueden intercalar.

  Regla:

  IP de la regla: 192.168.10.0

  Máscara de wildcard: 255.255.128.255

  Si aplicamos la máscara a la IP anterior nos da la IP con la que debe coincidir la IP de los paquetes después de aplicarles la wildcard: 0.0.10.0

  IP de Origen del paquete:172.16.138.40 a validar

  Si aplicamos la máscara de wildcard a esta IP nos da 0.0.10.0 por lo tanto esta IP cumple la reglas.

  Visto en binario(Donde la wildcard es 1 el resultado sera un 0 y donde la wildcard es 0 el resultado será el valor del bit que tiene na IP):

IP en decimal	192.168.10.0	172.16.138.40
IP en binario	11000000.10101000.00001010.00000000	10101100.00010000.10001010.00000000
Máscara de wildcard en binario	11111111.11111111.10000000.11111111	11111111.11111111.10000000.11111111
Resultado de aplicar la máscara	00000000.00000000.0**0001010**.00000000	00000000.00000000.0**0001010**.00000000

El resultado es coincidente. La IP del paquete cumple la regla.

- Si las máscara de red y la máscara de wildcard son complementarias, podemos calcular la máscara de wildcard a partir de la máscara de red. Hay que restar a la IP de Broadcast(255.255.255.255) la máscara de red. Ej:

Máscara de Broadcast	255.255.255.255
Máscara de red	255.255.255.240
Máscara de wildcard(Resta)	0 .0 .0 . 15

- **host**

  Si la máscara wildcard en una ACE son ceros(0.0.0.0) quiere decir que la IP debe coincidir por completo para cumplir la regla.

  Ejemplo de regla:

  access-list 1 permit 192.168.10.10 0.0.0.0 (ACL de host estándar)

  En este caso podemos substituir esta regla utilizando la palabra “host” por esta otra:

  access-list 1 permit host 192.168.10.10 (ACL de host estándar resumida)

- **any**

  Si la máscara wildcard en una ACE son 1(255.255.255.255) quiere decir que cualquier IP cumplira la regla.

  Ejemplo de regla:

  access-list 1 permit 0.0.0.0 255.255.255.255 (ACL resumida)

  En este caso podemos substituir esta regla utilizando la palabra “any” por esta otra:

  access-list 1 permit any (ACL estándar resumida)

Pautas generales para la creación de ACL

- Utilice las ACL en los **routers de firewall** ubicados entre su red interna y una red externa, como Internet.

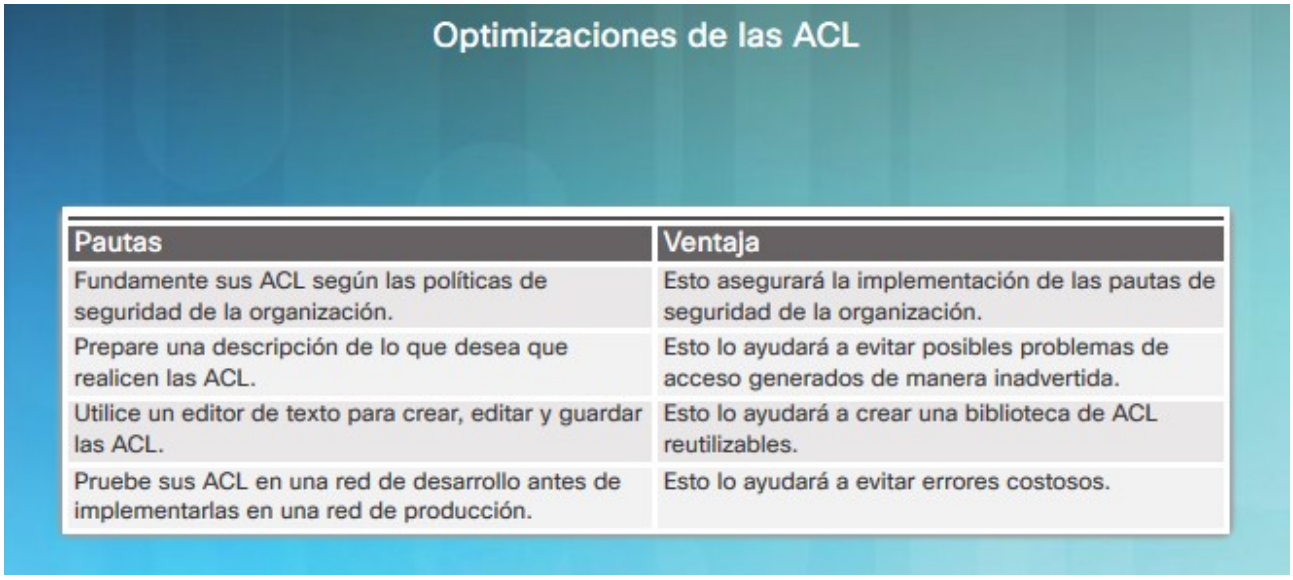
- Utilice las ACL en **un router ubicado entre dos partes de la red** para controlar el tráfico que entra a una parte específica de su red interna o que sale de esta.
- Configure las ACL en los **routers de frontera**, es decir, los routers ubicados en los límites de las redes. Esto proporciona una separación 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(IPV4 o IPv6) configurado en las interfaces del router de frontera.

Reglas para **aplicar** las ACL

Se puede configurar una ACL por protocolo(IPv4 o IPv6), por sentido(in o out) y por interfaz(g0/0, s0/0/0,…).

Si un router tiene dos interfaces(g0/0 y g0/1) configuradas para IPv4 e IPv6. Si necesitáramos ACL para ambos protocolos, en ambas interfaces y en ambos sentidos, esto requeriría **ocho** ACL diferentes.

Antes de configurar una ACL, se requiere una planificación básica.



Dónde ubicar las ACL

Esto depende del tipo de ACL

Hay dos tipos de ACLs:

ACLs **estándar**:

Solo limitan el tráfico basándose en la **IP de origen** del paquete.

Se deben poner lo mas cerca posible del destino. (Justo en el router antes del destino)

ACLs **extendidas** **(ES LA QUE DEBEMOS UTILIZAR)**:

Limitan el trafico según la **IP, puerto, protocolo de origen y destino**

Se deben poner lo más cerca posible del origen. (Justo en el router de origen del paquete)

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.

Sintaxis de ACL estándar numerada IPv4

El comando de configuración global **access-list** define una ACL estándar con un **número entre 1 y 99** y los números que van de **1300 a 1999**

Router(config)# **access-list** *número_acl* **{ deny | permit | remark }** *ip_origen* **[** *wildcard-origen* **][log]**

Ejemplo:

R1(config)# **access-list 10 remark Permitir acceso al host 192.168.10.10**

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

ó

R1(config)# **access-list 10 permit 192.168.10.10 0.0.0.0 log**

otro ejemplo:

R1(config)# access-list 10 permit 192.168.11.0 0.0.0.255 log

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.

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.

Si se añade al final la palabra **log** se genera un mensaje por consola la primera vez que el paquete coincida y después cada 5 minutos. Podemos habilitar los mensajes de log en consola con el comando **logging console** o deshabilitarlos con **no logging console.** También se puede establecer un nivel de depuración(0-emergencia, 1-alerta, 2-crítico, 3-error,…)

Aplicación de ACL estándar IPv4 a las interfaces

Router(config-if)# **ip access-group {** *número-acl* | *nombre-acl* **} { in | 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.

interfaz Serial 0/0/0

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

Sintaxis de ACL con nombre estándar IPv4

ip access-list [standard|extended] *name*

[permit|deny|remark] {ip_fuente [mascara_wildcard]} [log]

ip access-group *name* **[in|out]**

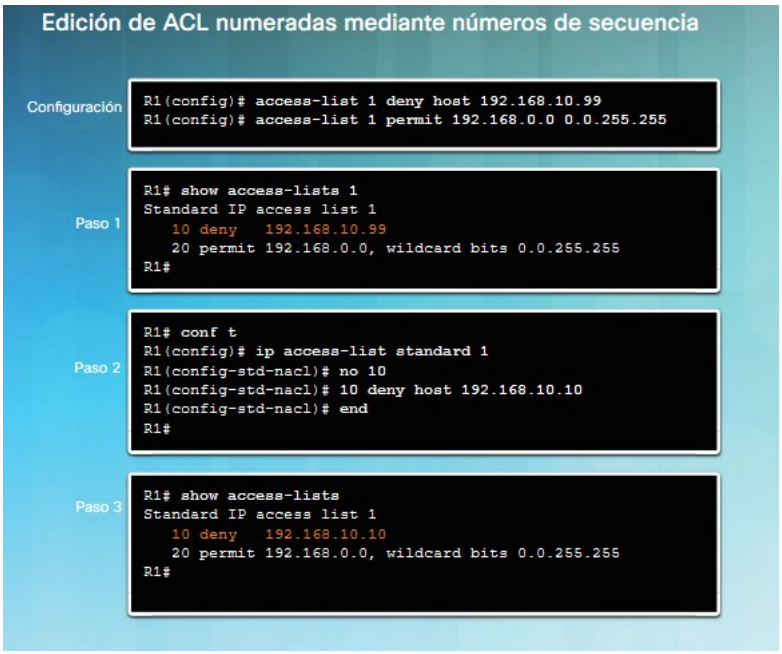
Modificación de ACL de IPv4

Método 1: usar un editor de texto

Cuando eliminamos una ACL eliminamos toda sus ACEs. También podemos eliminar ACEs individuales.

Guarde siempre las ACLs en un archivo de texto plano y cuando tenga que modificar sus reglas elimínelas del router, edítelas en el archivo y vuelve pegarlas en la línea de comando.

Método 2: usar números de secuencia



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. 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.

ip access-lists standard 1

no 10

Esto elimina la ACE:

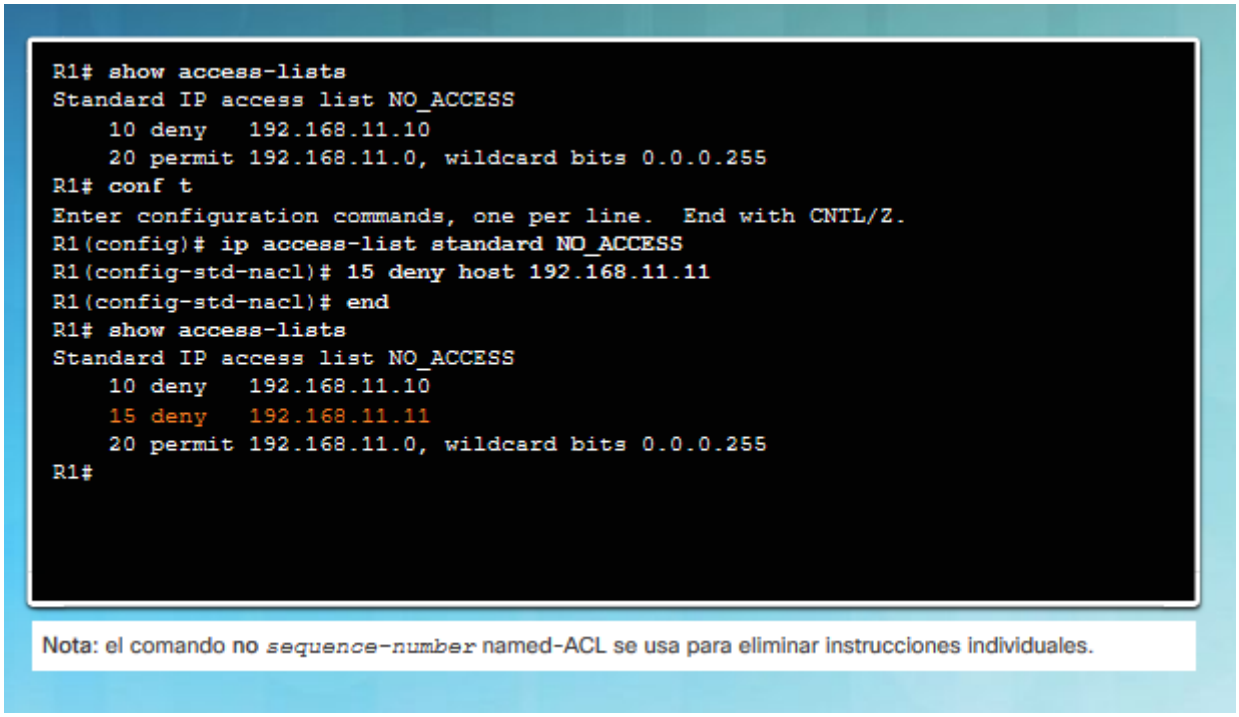
10 deny host 192.168.10.10

También se pueden insertar ACEs en el medio de otras ya configuradas dándole un número de secuencia intermedio.

15 deny host 192.168.10.11

Edición de ACL estándar con nombre

Igual que las numeradas. Solo que aquí el nombre es su nombre no el número.



En esta caso por orden.

> Debemos poner las de denegar los host de la subred 192.168.11.0 ANTES que la de permitir la subred
>
> Lo lee por orden
>
> 1. deniega 192.168.11.10
> 2. deniega 192.168.11.11
> 3. Permite toda la subred 192.168.11.11
>
> Cuando establezcamos las reglas Cisco IOS reordena las ACLS para que las de host vayan siempre antes que las de subred.

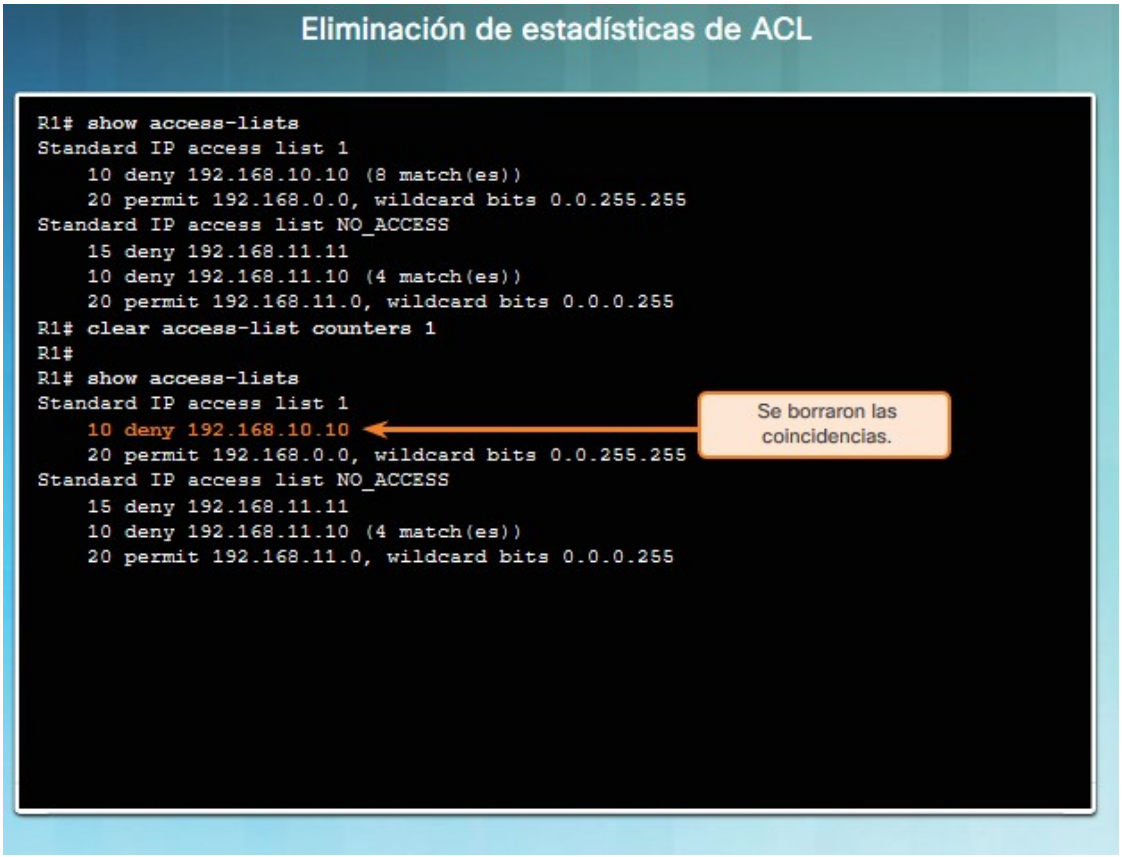
Verificar las ACL

> **show ip interface** se utiliza para verificar la ACL en la interfaz.
>
> **show access-list**

Estadísticas de ACL

show access-lists muestra las estadísticas para cada instrucción que tiene coincidencias.

Para ver las estadísticas de la instrucción **deny any implícita**, la instrucción se puede configurar manualmente y aparecerá en el resultado.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**.



En la imagen la ACE 10 de la ACL 1 tiene 8 coincidencias(mach). Posteriormente ponemos los contadores a cero de toda la ACL 1: **clear access-list counters 1**

access-class

Puede controlar qué direcciones IP pueden acceder remotamente al router mediante la configuración de una ACL(numeradas o nombradas) y una instrucción **access-class** en las líneas VTY.

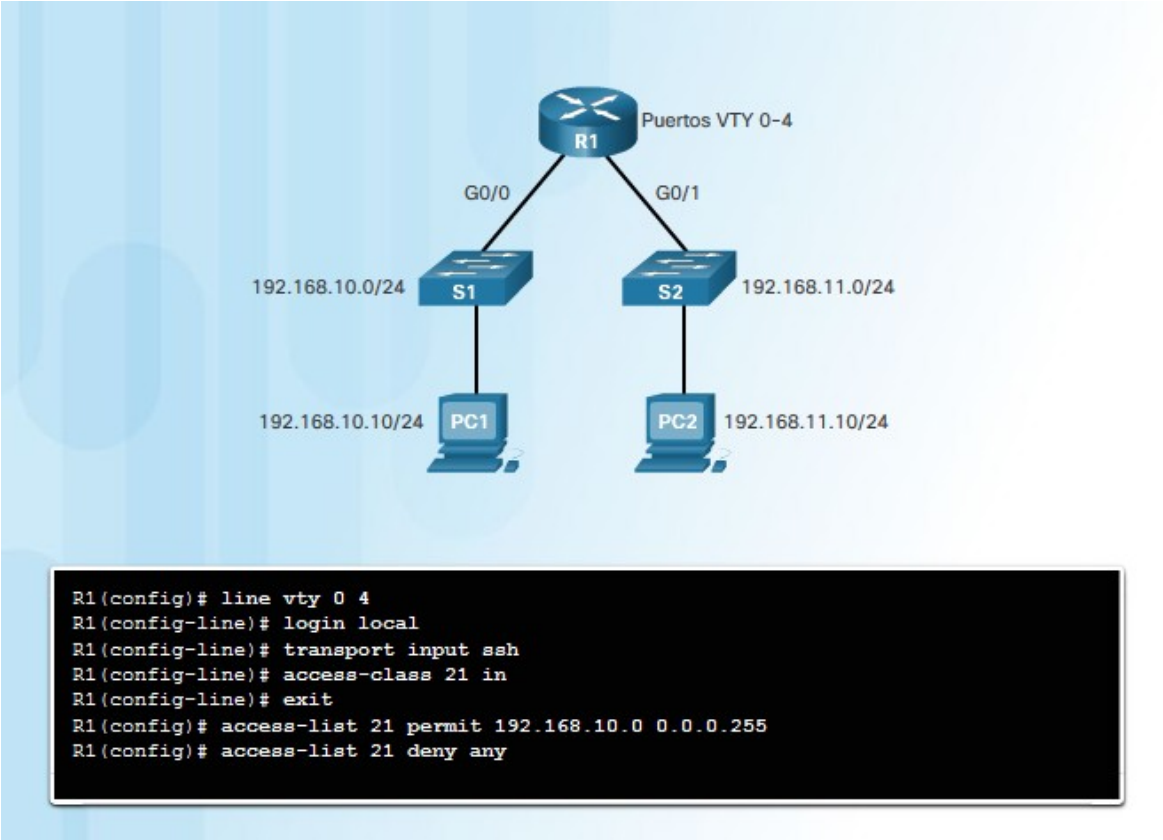
Se deben **establecer restricciones idénticas en todos los VTY**, porque un usuario puede intentar conectarse a cualquiera de ellos.

Router (config)# **access-class access-list-number { in [vrf-also] | out }**

vrf-also esta palabra clave excede de este curso. Pero son enrutamientos virtuales(Virtual Routing Forwarding) es decir instancias de distintas tablas de enrutamiento. Esto permite segmentar la red y crear redes virtuales para clientes(VPN). Sí ponemos vrf-also estamos permitiendo la administración desde cualquier instancia de enrutamiento virtual.

En la siguiente imagen solo los equipos de la red 192.168.10.0/24 pueden administrar el router 1 de forma remota a través de ssh.

Nota: Las listas de acceso 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. De manera predeterminada, las ACL de salida no evita las conexiones de acceso remoto que se inician desde el router.



Primero permitimos los host de la red 192.168.10.0 255.255.255.0 para administrar mediante vty 0 4

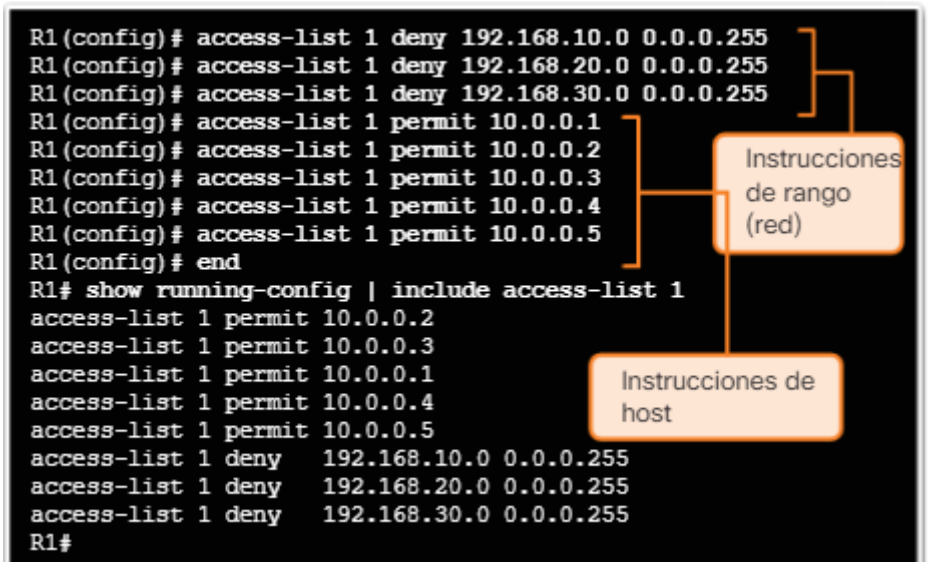
Denegamos los ANY

Importante el orden

Deny any implícita

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.

El IOS reordena las ACL estándar



Independientemente de como listemos o metamos las ACEs **estándar**, Cisco tiene un **algoritmo para mejorar el rendimiento de las ACL de sus dispositivos.** Así, **este algoritmo alterará el orden de aplicación de las ACLs**. (1º **todos los hosts y después las redes, los host también los reordena para mayor eficiencia en la busqueda**).
En caso de que **sean ACLs estándar con nombre**, estas no se ordenan según este **algoritmo.**
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(las de rango, las subredes) se enumeran en el orden en que se introdujeron.
Nota: la función de hash se aplica solamente a las instrucciones de host en listas de acceso de IPv4 estándar. Los detalles de la función de hash exceden el ámbito de este curso.
Nota: En Packet Tracer el hash no funciona o no actúa.

Procesos de enrutamiento y ACL

Los routers de Cisco aplican las ACLs de la siguiente forma :
- 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 **direccion** 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 distintas ACE de la lista.**
- Si el **paquete coincide con una instrucción (ACE)**, 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.**