

TIPS CREACION DE ACL

1 ¿Qué es la lista de control de acceso?

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.

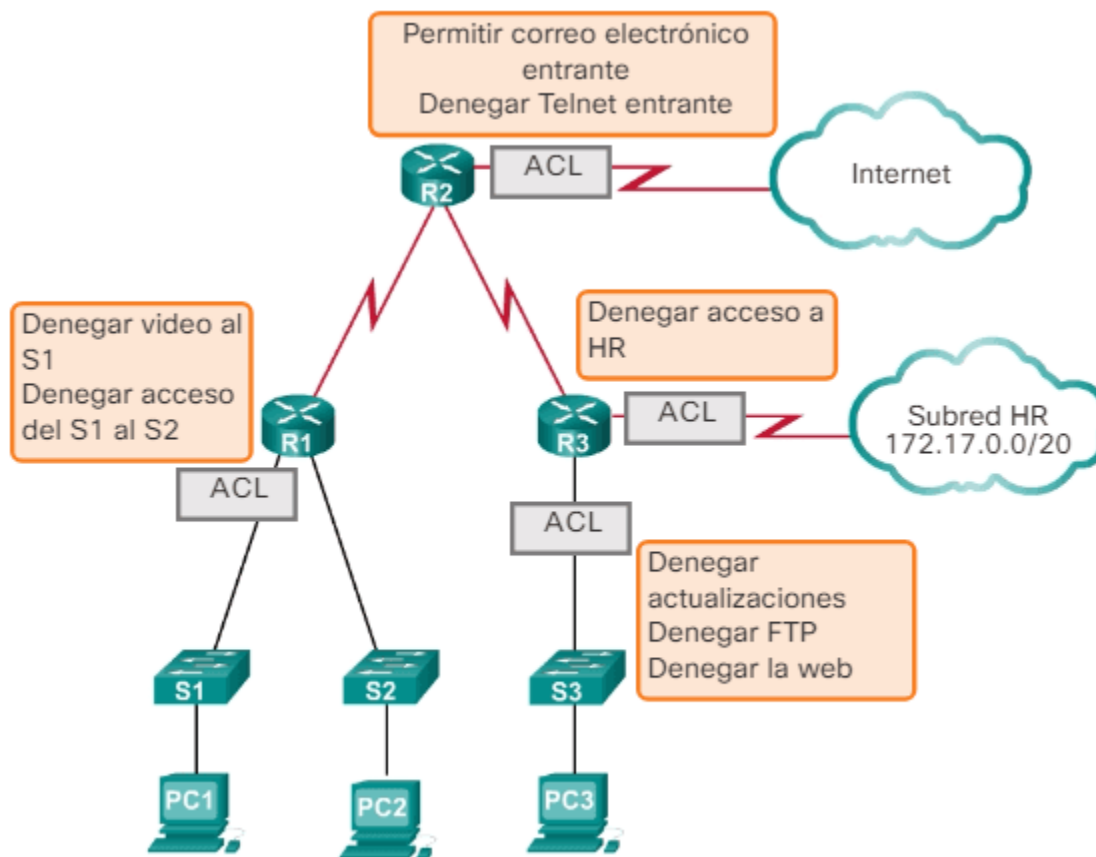


Imagen 1: Qué es una ACL

1.1 Tareas de las ACL

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.
- **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.

TIPS CREACION DE ACL

Los routers no tienen 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.

2 Filtrado de paquetes

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”. 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. Este proceso se denomina **filtrado de paquetes**.

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 determinados. El filtrado de paquetes puede producirse en la capa 3 o capa 4.

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**.

Filtrado de tráfico en un router mediante ACL



Con dos interfaces y dos protocolos en ejecución, este router podría tener un total de ocho ACL distintas aplicadas.

Reglas para aplicar las ACL

Solo se puede tener una ACL por protocolo, por interfaz y por sentido:

- Una ACL por protocolo (p. ej., IPv4 o IPv6)
- Una ACL por sentido (es decir, de entrada o de salida)
- Una ACL por interfaz (p. ej., GigabitEthernet0/0)

TIPS CREACION DE ACL

3 Funcionamiento de las ACL

Las Listas de Control de Acceso 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, como se muestra en la Imagen 2.

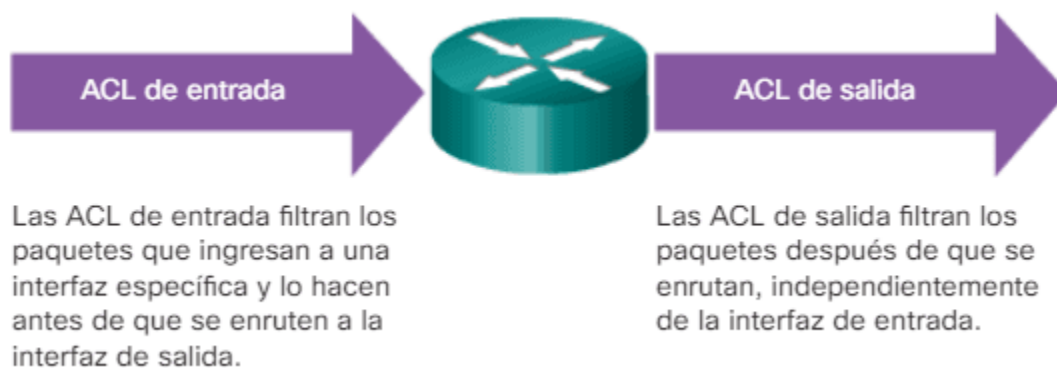


Imagen 2: ACL de Entrada y de Salida

- **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 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.

4. Máscaras wildcard en ACL

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 qué bits de la dirección debe examinar para obtener una coincidencia.

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 IPv4 correspondientes. Sin embargo, en una máscara wildcard, estos bits se utilizan para fines diferentes y siguen diferentes reglas.

Mientras que las máscaras de subred utilizan unos y ceros binarios para identificar la red, la subred y la porción de host de una dirección IPv4; las máscaras wildcard utilizan unos y ceros binarios para filtrar direcciones IPv4 individuales o grupos de direcciones IPv4 para permitir o denegar el acceso a los recursos.

TIPS CREACION DE ACL

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 primeras, utilizan las siguientes reglas para establecer la coincidencia entre los unos y ceros binarios:

- **Bit 0 de máscara wildcard:** se 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.



Imagen 3: Máscara wildcard

En la Imagen 3 se muestra cómo las diferentes máscaras wildcard filtran las direcciones IPv4. 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.

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.

4.1. Uso de una máscara wildcard

En la Imagen 4, 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.

TIPS CREACION DE ACL

	Dirección decimal	Dirección binaria
Dirección IP para procesar	192.168.10.0	11000000.10101000.00001010.00000000
Máscara wildcard	0.0.255.255	00000000.00000000.11111111.11111111
Dirección IP resultante	192.168.0.0	11000000.10101000.00000000.00000000

Imagen 4: Ejemplo de máscara wildcard

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.

4.2. Ejemplos de máscara wildcard

4.2.1. Máscaras wildcard para establecer coincidencias con subredes IPv4

Se necesita práctica para calcular la máscara wildcard. En la Imagen 5, se proporcionan tres ejemplos de máscara wildcard.

Ejemplo 1

	Decimal	Binario
Dirección IP	192.168.1.1	11000000.10101000.00000001.00000001
Máscara wildcard	0.0.0.0	00000000.00000000.00000000.00000000
Resultado	192.168.1.1	11000000.10101000.00000001.00000001

Ejemplo 2

	Decimal	Binario
Dirección IP	192.168.1.1	11000000.10101000.00000001.00000001
Máscara wildcard	255.255.255.255	11111111.11111111.11111111.11111111
Resultado	0.0.0.0	00000000.00000000.00000000.00000000

Ejemplo 3

	Decimal	Binario
Dirección IP	192.168.1.1	11000000.10101000.00000001.00000001
Máscara wildcard	0.0.0.255	00000000.00000000.00000000.11111111
Resultado	192.168.1.0	11000000.10101000.00000001.00000000

Imagen 5: 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.

TIPS CREACION DE ACL

- Para 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.

4.2.2. Máscaras wildcard para establecer coincidencias con rangos

Los dos ejemplos en la Imagen 6 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.

Ejemplo 1

	Decimal	Binario
Dirección IP	192.168.16.0	11000000.10101000.00010000.00000000
Máscara wildcard	0.0.15.255	00000000.00000000.00001111.11111111
Rango de resultados	De 192.168.16.0 a 192.168.31.255	De 11000000.10101000.00010000.00000000 a 11000000.10101000.00011111.11111111

Ejemplo 2

	Decimal	Binario
Dirección IP	192.168.1.0	11000000.10101000.00000001.00000000
Máscara wildcard	0.0.254.255	00000000.00000000.11111110.11111111
Resultado	192.168.1.0 Todas las subredes con número impar en la red principal 192.168.0.0	11000000.10101000.00000001.00000000

Imagen 6: Más Ejemplos de Máscaras wildcard

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.

4.3. Cálculo de la máscara wildcard

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

4.3.1. 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.

TIPS CREACION DE ACL

Ejemplo 1

255 . 255 . 255 . 255
- 255 . 255 . 255 . 000
255

Imagen 7: Cálculo de máscara wildcard ejemplo 1

4.3.2. 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 IPv4 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.

Ejemplo 2

255 . 255 . 255 . 255
- 255 . 255 . 255 . 240
15

Imagen 8: Cálculo de máscara wildcard ejemplo 2

4.3.3. 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 255.255.254.0. El resultado es 0.0.1.255.

Ejemplo 3

255 . 255 . 255 . 255
- 255 . 255 . 254 . 000
1 . 255

Imagen 9: Cálculo de máscara wildcard ejemplo 3

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 0.0.1.255
```

Considere un ejemplo en el cual se deben hacer coincidir las redes en el rango de 192.168.16.0/24 a 192.168.31.0/24. Estas redes resumirán en 192.168.16.0/20. En este caso, 0.0.15.255 es la máscara wildcard correcta para configurar una declaración eficaz de ACL, como se muestra a continuación:

TIPS CREACION DE ACL

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

4.4. Palabras clave de las máscaras wildcard: Ejemplos

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 para filtrar solo una dirección de host.
- 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 IPv4

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**.

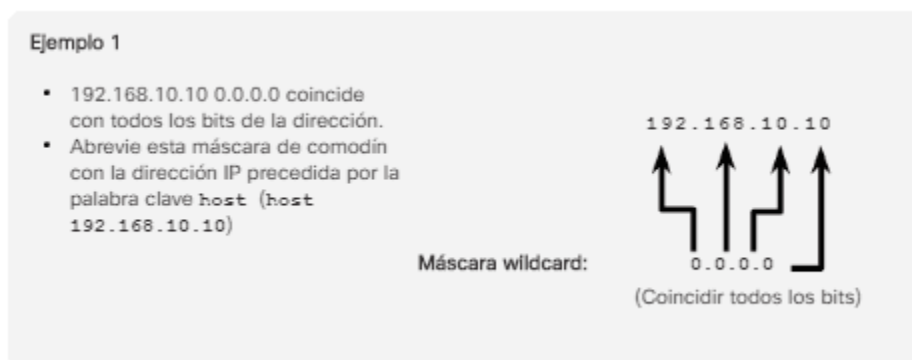


Imagen 10: Ejemplo 1 Abreviaturas de la máscara de bits wildcard

A continuación, 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.

```
R1(config)# access-list 1 permit 0.0.0.0 255.255.255.255
```

```
!OR<br>
```

```
R1(config)# access-list 1 permit any
```

Ejemplo 2: proceso de máscara wildcard con coincidencia con cualquier dirección IPv4

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.


TIPS CREACION DE ACL

Ejemplo 2

- 0.0.0.0 255.255.255.255 omite todos los bits de la dirección.
- Abrevie la expresión con la palabra clave **any**

Máscara wildcard: 255.255.255.255

0 . 0 . 0 . 0



(Omite todos los bits)

Imagen 11: Ejemplo 2 Abreviaturas de la máscara de bits wildcard

A continuación se muestra cómo utilizar la palabra clave **host** para sustituir la máscara wildcard para identificar un único host.

```
R1(config)# access-list 1 permit 192.168.10.10 0.0.0.0
```

```
!OR<br>
```

```
R1(config)# access-list 1 permit host 192.168.10.10
```

5. 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, 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 configurado en las interfaces del router de frontera.

TIPS CREACION DE ACL

5.1. Reglas para aplicar las ACL

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. (p. ej., IPv4 o IPv6)
- **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. (es decir, de entrada o de salida)
- **Una ACL por interfaz:** las ACL controlan el tráfico para una interfaz, por ejemplo, GigabitEthernet 0/0.

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, 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 configurado en las interfaces del router de frontera.

TIPS CREACION DE ACL

5.2. Optimizaciones de las ACL

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 siguiente tabla, se presentan pautas que constituyen la base de una lista de prácticas recomendadas para ACL.

Tabla de Optimizaciones de las ACL.	
Pautas	Ventajas
Fundamente sus ACL según las políticas de seguridad de la organización.	Esto asegurará la implementación de las pautas de seguridad de la organización.
Prepare una descripción de lo que desea que realicen las ACL.	Esto lo ayudará a evitar posibles problemas de acceso generados de manera inadvertida.
Utilice un editor de texto para crear, editar y guardar las ACL.	Esto lo ayudará a crear una biblioteca de ACL reutilizables.
Pruebe sus ACL en una red de desarrollo antes de implementarlas en una red de producción.	Esto lo ayudará a evitar errores costosos.

6. 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.

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.

TIPS CREACION DE ACL

6.1. Dónde ubicar las ACL

Cada ACL se debe colocar donde tenga más impacto en la eficiencia. Como se muestra en la Imagen 12, las reglas básicas son las siguientes:

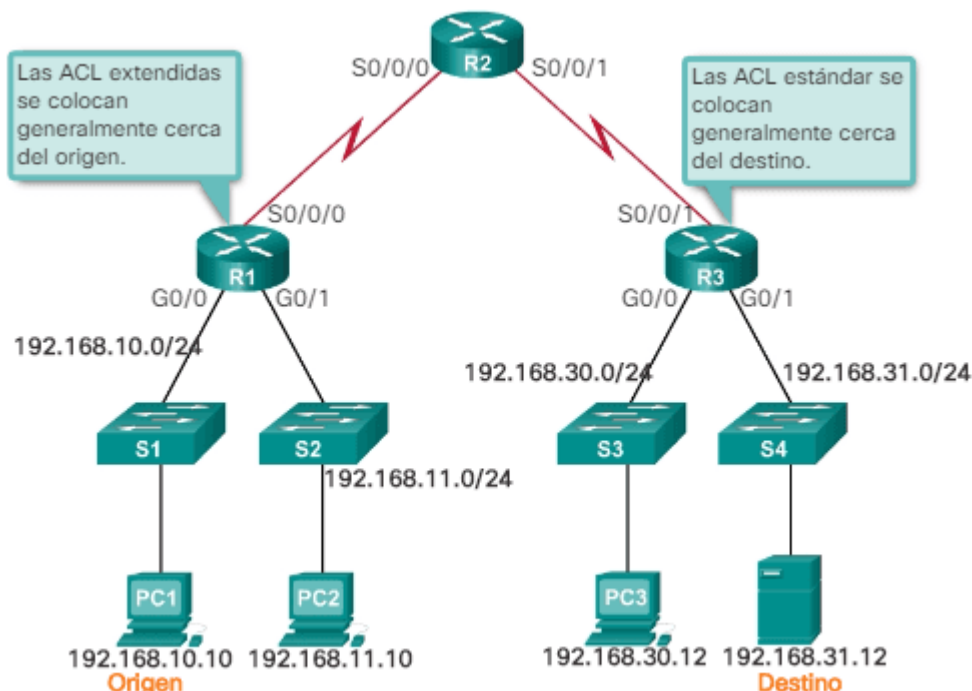


Image 12: Dónde ubicar las Listas de Control de Acceso

- **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 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.

6.2. Ubicación de la ACL estándar

La topología en la Imagen 13 se utiliza para demostrar cómo puede posicionarse una ACL estándar. 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.

TIPS CREACION DE ACL

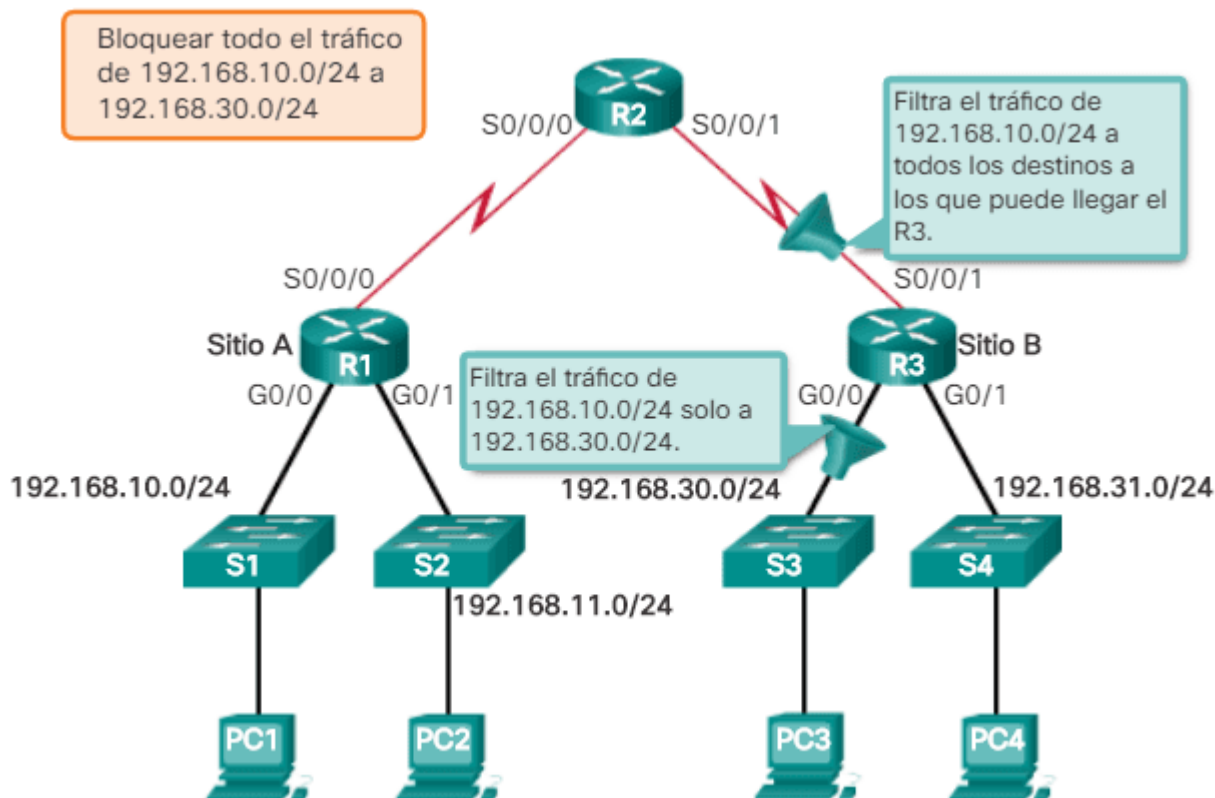


Imagen 13: Ubicación de la ACL estándar

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 192.168.10.0/24 aún pueden llegar a 192.168.31.0/24.