Listas de Control de Acceso - ACL

Juan M. Hurtado A., MSc

Tomado de:
https://enredandoconredes.com/2015/01/08/acls-listas-de-control-de-acceso/

http://recursostic.educacion.es/observatorio/web/es/component/content/article/1065-listas-de-control-de-acceso-acl?start=3

ACLs, Listas de Control de Acceso

¿Qué son?

Una Lista de Control de Acceso es un conjunto de sentencias que permiten o deniegan un tráfico determinado. Algo similar a lo que viene hacer un cortafuegos (Firewall).

¿Para qué se utilizan?

Se utilizan como una manera “sencilla” de filtrar el tráfico que pasa por un dispositivo de red de capa 3.
Son útiles para aplicar ciertas políticas de seguridad.

¿Qué tipos hay?

“Standard”: emplearemos como parámetro de filtrado las direcciones IP de origen.
“Extended”: utilizaremos la IPs de origen, destino y puertos.
“Named”: lo mismo que las dos anteriores pero nos permiten asignarlas un nombre en lugar de un número

ACLs, Listas de Control de Acceso

Objetivos de crear ACLs

- Limitar el tráfico de red y mejorar el rendimiento de la red. Al restringir el tráfico de vídeo, por ejemplo, las ACL pueden reducir ampliamente la carga de la red y en consecuencia mejorar el rendimiento de la misma.
- Controlar el flujo del tráfico. Las ACL pueden restringir el envío de las actualizaciones de enrutamiento. Si no se necesitan actualizaciones debido a las condiciones de la red, se preserva el ancho de banda.
- Proporcionar un nivel básico de seguridad para el acceso a la red. Por ejemplo, las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro acceda a la misma área. Por ejemplo, el host-1 se le permite el acceso a la red de Producción, y al host-2 se le niega el acceso a esa red.
- Establecer qué tipo de tráfico se envía o se bloquea en las interfaces del router. Por ejemplo, permitir que se envíe el tráfico relativo al correo electrónico, y se bloquea el tráfico de ftp.
- Otorgar o denegar permiso a los usuarios para acceder a ciertos tipos de archivos. Por ejemplo FTP o HTTP.

ACLs, Listas de Control de Acceso

¿Cómo funcionan?

Una Lista de Control de Acceso se compone de una serie de **sentencias** que **permiten o deniegan** un tráfico determinado.

El equipo irá comparando cada paquete con cada una de las sentencias de la ACL, de la primera a la última.

En el momento que un paquete coincida con la sentencia, ésta se ejecuta y no se sigue comparando.

Cada ACL tiene un **"deny any"** implícito al final de las sentencias, esto es, si un paquete no coincide con ninguna de las sentencias se descarta.

ACLs, Listas de Control de Acceso

Proceso de funcionamiento completo

1. Cuando entra una trama a través de una interfaz, el router verifica si la dirección de capa 2 (MAC) concuerda o si es una trama de broadcast.
2. Si se acepta la dirección de la trama, la información de la trama se elimina y el router busca una ACL en la interfaz entrante.
3. Si existe una ACL se comprueba si el paquete cumple las condiciones de la lista.
4. Si el paquete cumple las condiciones, se ejecuta la acción de aceptar o rechazar el paquete.
5. Si se acepta el paquete en la interfaz, se compara con las entradas de la tabla de enrutamiento para determinar la interfaz destino y conmutarlo a aquella interfaz. Luego el router verifica si la interfaz destino tiene una ACL.
6. Si existe una ACL, se compara el paquete con las sentencias de la lista y si el paquete concuerda con una sentencia, se acepta o rechaza el paquete según se indique.
7. Si no hay ACL o se acepta el paquete, el paquete se encapsula en el nuevo protocolo de capa 2 y se envía por la interfaz hacia el dispositivo siguiente.

Fuente: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1065-listas-de-control-de-acceso-acl?start=3

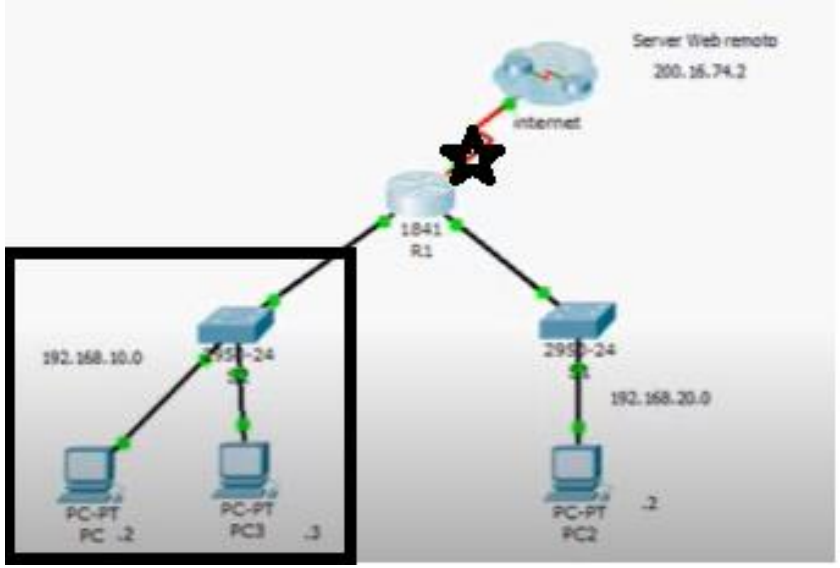
ACLs, Listas de Control de Acceso

¿Cómo se utilizan?

Una vez que la ACL está creada, se debe aplicar a una intefaz, y también en un sentido determinado. Es decir, en sentido entrante (Inbound) o saliente (Outbound) a esa interfaz.

A este respecto debemos tener en cuenta dos aspectos importantes. Cuando una ACL se aplica en sentido entrante, los paquetes que serán evaluados primero por dicha ACL, y en caso de ser permitidos será entonces cuando el equipo los enrute por alguna interfaz de salida. Obviamente, todos los paquetes que se denieguen no serán sometidos a la tabla de enrutamiento.

Sin embargo, cuando una ACL se aplica a en sentido “Saliente”, ésta se aplicará una vez los paquetes hayan sido enrutados. O lo que es lo mismo, primero se enrutan y luego se ve si se permiten o deniegan.



ACL estándar, se asigna a la interfaz del Router mas cerca del destino negado

ACLs, Listas de Control de Acceso

ACL Estandar Router(config)# access-list numACL permit|deny origen [wild-mask]

Las Listas de Control de Acceso Estándar son aquellas que efectúan el filtrado, permitiendo o denegando inspeccionando la IP de origen.
Cada ACL de este tipo lo podremos numerar de un rango que podrá ir de 1-99 o 1300-1999.

```
Switch01(config)#access-list ?

  <1-99> IP standard access list
  <100-199> IP extended access list
  <1000-1099> IPX SAP access list
  <1100-1199> Extended 48-bit MAC address access list
  <1200-1299> IPX summary address access list
  <1300-1999> IP standard access list (expanded range)
  <200-299> Protocol type-code access list
  <2000-2699> IP extended access list (expanded range)
  <300-399> DECnet access list
  <600-699> Appletalk access list
  <700-799> 48-bit MAC address access list
  <800-899> IPX standard access list
  <900-999> IPX extended access list
   dynamic-extended Extend the dynamic ACL absolute timer
   rate-limit Simple rate-limit specific access list
```

https://enredandoconredes.com/2015/01/08/acls-listas-de-control-de-acceso/

ACLs, Listas de Control de Acceso

ACL Estandar

Definido el número, a continuación deberemos especificar si permitimos o denegamos el tráfico en cuestión.

```
Switch01(config)#access-list 5 ?

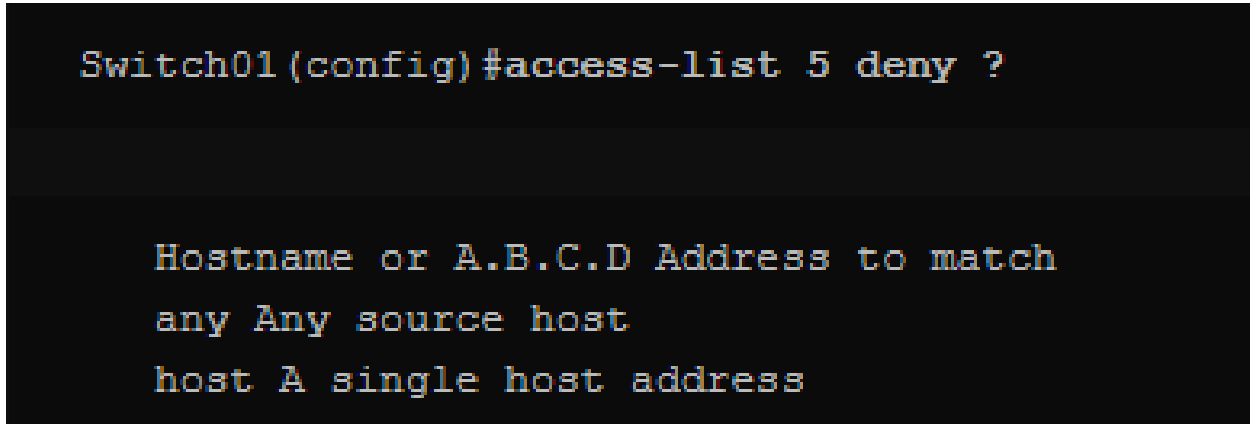
  deny   Specify packets to reject
  permit Specify packets to forward
  remark Access list entry comment
```

https://enredandoconredes.com/2015/01/08/acls-listas-de-control-de-acceso/

ACLs, Listas de Control de Acceso

ACL Estandar

El siguiente paso será proporcionar los valores:



La primera de las opciones hace referencia a la IP o rango de éstas.
La segunda y la tercera permiten, en lugar de especificar en formato numeral “cualquier IP” o “una IP concreta”, introducir los términos “any” y “host” respectivamente.

https://enredandoconredes.com/2015/01/08/acls-listas-de-control-de-acceso/

ACLs, Listas de Control de Acceso

ACL Estandar

Máscaras Wildcard

Las Máscaras Wildcard son utilizadas por las ACLs para indicar un equipo, un conjunto de éstos o una red completa.
Se asemeja a lo que vendría ser una máscara de subred aunque con bien significado es distinto.

Cuando en una Máscara Wildcard figura un “0” se entiende que el valor que consta en la IP debe coincidir. Sin embargo cuando aparece un “255” puede tomar cualquier valor.

```
Switch01(config)#access-list 10 deny 192.168.1.0 0.0.0.255
```

Esto añadirá una sentencia en la que se denegarán todos los paquetes con IP de origen “192.168.1” ya que la máscara tiene un “0”. El cuarto octeto puede tener cualquier valor “255”, entre 1 y 254.

Para indicar rango de subredes deberemos de realizar cálculos. Una manera sencilla para indicar redes es restar “255” a la máscara de subred de una dirección IP contenida en ese rango.

https://enredandoconredes.com/2015/01/08/acls-listas-de-control-de-acceso/

ACLs, Listas de Control de Acceso

ACL Estandar

Aplicar a una Interfaz del Router Router (config-if)# ip access-group numACL in|out

En la configuración anterior configuramos la access list "Standard", número 5, en la que denegaríamos la red 192.168.1.0/24, y luego permitiríamos el resto de tráfico.
Luego, aplicaríamos dicha ACL a la interfaz Ethernet 0 en sentido saliente.

```
Switch01#config t
Switch01(config)#access-list 10 deny 192.168.1.0 0.0.0.255
Switch01(config)#access-list 5 permit any
Switch01(config)#interface Ethernet 0
Switch01(config-if)#ip access-group 10 out
```

In: tráfico a filtrar que ENTRA por la interfaz del router
out : tráfico a filtrar que SALE por la interfaz del router.

ACLs, Listas de Control de Acceso

ACL Estandar (Comnados Importantes)

Creación de ACL:
Router(config)# access-list numACL permit|deny origen [wild-mask]

Router0(config)# access-list 10 deny 192.168.1.2 0.0.0.0

Asignación de una ACL a una Interface del Router:
Router (config-if)# ip access-group numACL in|out

Router0(config)# interface FastEthernet 0/0

Router0(config-if)# ip access-group 10 out

Eliminación de una ACL:
Router0(config)# no access-list 10

Mostrar una ACL:
Router0# show access-list

Creación de ACLs

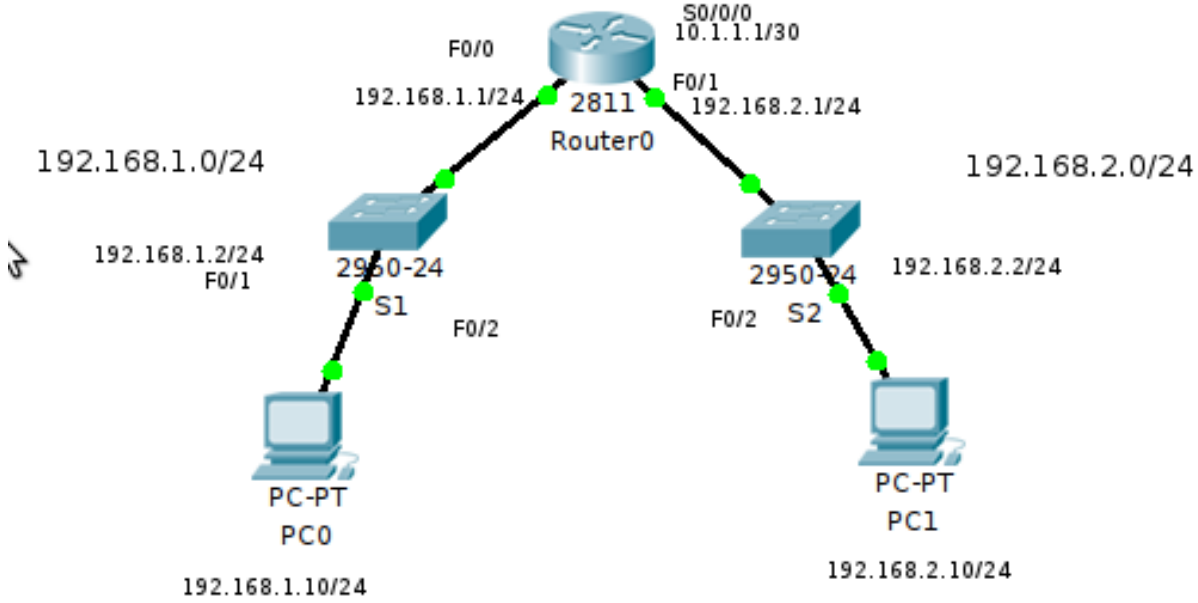
Caso Ejemplo #1

Vamos a definir una ACL estándar que permita el trafico de salida de la red 192.168.1.0/24.

La primera cuestión que se plantea es ¿dónde instalar la ACL? ¿en qué router? ¿en qué interfaz de ese router?.

En este caso no habría problema porque solo tenemos un router, el Router0. Pero la regla siempre es instalar la ACL lo más cerca posible del destino.

```
Router0#configure terminal
Router0(config)#access-list 1 permit  192.168.1.0    0.0.0.255
Router0(config)#interface S0/0/0
Router0(config-if)#ip access-group 1 out
```



Ahora borramos la ACL anterior y vamos a definir una ACL estándar que deniegue un host concreto.

```
Router0(config)#no access-list 1
Router0(config)#access-list 1 deny 192.168.1.10 0.0.0.0
Router0(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router0(config)#interface S0/0/0
Router0(config-if)#ip access-group 1 out
```

http://recursostic.educacion.es/observatorio/web/es/component/content/article/1065-listas-de-control-de-acceso-acl?start=3