Administración de redes

Prof. Andrea Mesa Múnera

Listas de Control de Acceso

AGENDA

1. Introducción y definición.
2. Configuración de las listas de control de acceso

Listas de Control de Acceso

Una lista de control de acceso o Access Control List (ACL) es una lista secuencial de órdenes que permiten o deniegan un paquete.

Se pueden definir también como una serie secuencial de comandos que sirven para filtrar información.

Las ACL son la especificación de una acción a realizar sobre paquetes que cumplan ciertas condiciones.

De [1]

UNIVERSIDAD EIA
Ser, Saber y Servir
Con Acreditación Institucional

Listas de Control de Acceso

Una ACL es un conjunto de reglas identificadas con un número o un nombre y cada regla especifica una acción y una condición. Las acciones a aplicar son permitir o denegar todos los paquetes que cumplan la condición asociada a la regla.

Una ACL se identifica con un número o un nombre y todas las reglas que tengan el mismo número/nombre hacen parte de la ACL, éstos identificadores suelen indicar también qué tanta expresividad tendrá la ACL, es decir, qué tan específicas pueden ser las reglas.

De [1]

UNIVERSIDAD EIA
Ser, Saber y Servir
Con Acreditación Institucional

Listas de Control de Acceso

El motivo más importante para configurar las ACL es brindar seguridad a la red permitiendo controlar el tráfico de entrada o de salida de la red.

La ACL es una configuración de router que controla sí un router permite o deniega paquetes según el criterio encontrado en el encabezado del paquete. Las ACL también se utilizan para seleccionar los tipos de tráfico por analizar, reenviar o procesar de otras maneras.

De [1]

Listas de Control de Acceso

Como cada paquete llega a través de una interfaz con una ACL asociada, la ACL se revisa línea a línea, y cuando una línea coincida con el paquete entrante se le aplica esa regla. La ACL hace cumplir una o más políticas de seguridad corporativas al aplicar una regla de permiso o denegación para determinar el destino del paquete. Es posible configurar las ACL para controlar el acceso a una red o subred.

De [1]

Listas de Control de Acceso

Para aplicar las ACL en un router tenga presente que se puede configurar una ACL por protocolo, por dirección y por interfaz.

- Una ACL por protocolo: para controlar el flujo de tráfico de una interfaz, se debe definir una ACL para cada protocolo habilitado en la interfaz.
- Una ACL por dirección: las ACL controlan el tráfico en una dirección a la vez de una interfaz. Deben crearse dos ACL por separado para controlar el tráfico entrante y saliente.
- Una ACL por interfaz: las ACL controlan el tráfico para una interfaz, por ejemplo, FastEthernet 0/0.

De [1]

Listas de Control de Acceso

Un ejemplo de cómo es conceptualmente una ACL es así:

Lista-de-acceso X ACCION1 CONDICION1

Lista-de-acceso X ACCION2 CONDICION2

Lista-de-acceso X ACCION3 CONDICION3

La X es el nombre o número que identifica la ACL, por lo tanto todas las reglas anteriores componen la ACL X, una sola ACL. Si cierto paquete cumple la condición1 se le aplica la Acción1, si un paquete cumple la condición 2 se le aplica la Acción2 y así sucesivamente.

De [1]

UNIVERSIDAD EIA
Ser, Saber y Servir
Con Acreditación Institucional

Listas de Control de Acceso

La lógica de funcionamiento de las ACLs es que **una vez que se cumpla una condición, se aplica su acción correspondiente y no se examinan más reglas de la ACL.**

Así se disminuye la cantidad de procesamiento del enrutador, pero también tiene una consecuencia, si una regla abarca un conjunto de direcciones y otra un subconjunto del primero, la regla de subconjunto debe estar antes de la regla del conjunto completo.

De [1]

Listas de Control de Acceso

Por ejemplo, si se especifica en una regla *denegar el acceso a un host de cierta subred* y en otra *permitir toda la subred,* la ACL diría *permita el acceso a todos los hosts de la subred X menos al host Y.*

Si la ACL se escribe con la regla de la subred antes que la regla del host, la ACL permitiría acceso incluso al host, porque la regla de host cumpliría también la regla de la subred y la regla del host nunca se examinaría por estar debajo de la regla general.

De [1]

UNIVERSIDAD EIA
Ser, Saber y Servir
Con Acreditación Institucional

Listas de Control de Acceso

Es necesario tener claro que cuando se configuran ACL la última sentencia es denegar todo el tráfico, la cual se denomina "implicit deny any statement" (denegar implícitamente una sentencia) o "deny all traffic" (denegar todo el tráfico). Sin embargo, es importante que antes exista al menos una sentencia de permiso, ya que si no se pone, la ACL bloqueará todo el tráfico y no podrá haber enrutamiento.

La sentencia es: **deny any**

De [1]

Listas de Control de Acceso

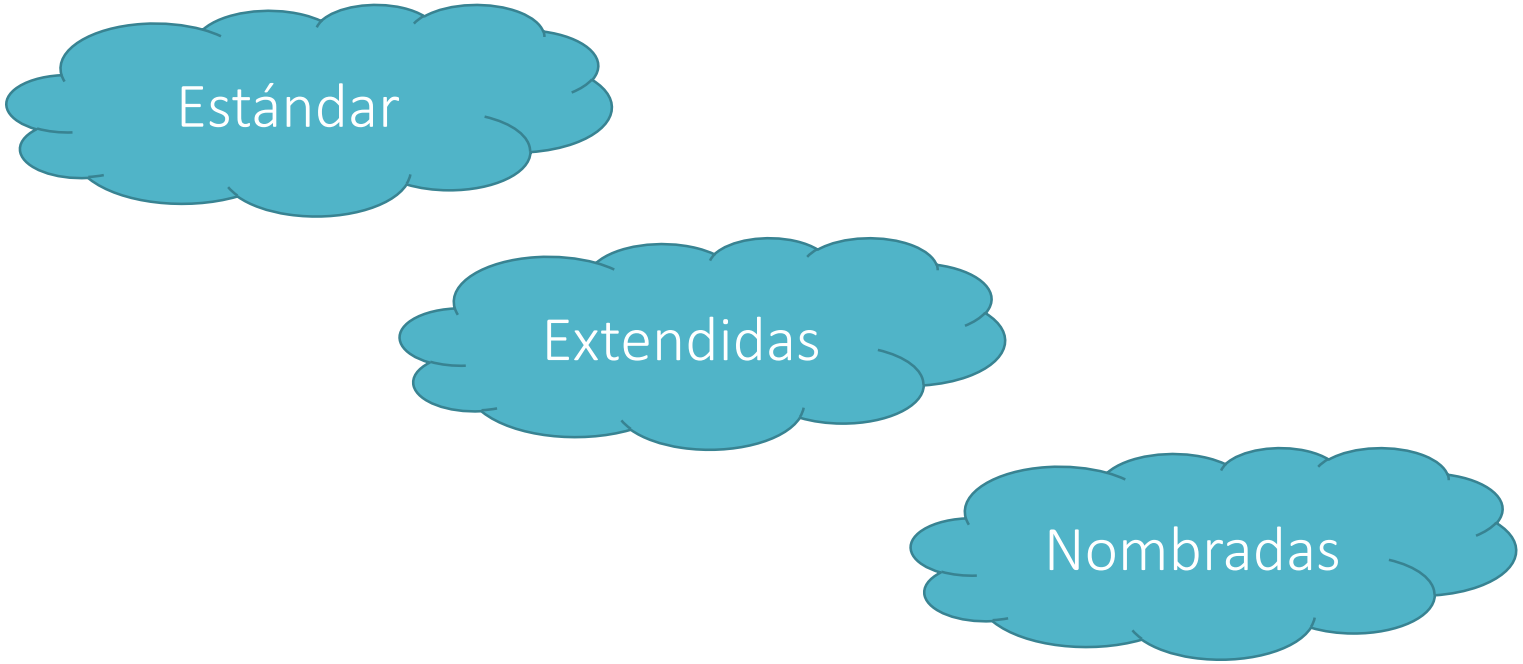
En otras palabras, las **reglas más específicas deben estar al principio de la ACL** para evitar que las reglas generales se apliquen siempre y nunca se examinen las específicas.

Finalmente todas las ACLs **terminan, implícitamente, con una regla *No permitir nada más***.

De [1]

Listas de Control de Acceso

Existen tres tipos de ACL:



De [1]

ACL Estándar

Sólo pueden filtrar tráfico a partir de las direcciones IP origen. No importa el destino del paquete ni los puertos involucrados.

El número asociado a este tipo de listas varía entre 1 y 99.

De [1]

ACL Estándar

Configuración de ACL Estándar

Los pasos generales para configurar ACLs son 3:

1. Crear la ACL en modo de configuración global
2. Aplicar la ACL en una interfaz indicando la dirección del tráfico al que se le va a aplicar
3. Verificar su funcionamiento

De [1]

ACL Estándar

1. Crear la ACL en modo de configuración global

   interface <interfaz>

   ip access-group <n> [in|out]

2. Aplicar la ACL en una interfaz indicando la dirección del tráfico al que se le va a aplicar

   access-list <n> permit <referencia1> <wildcard1>

   access-list <n> deny <referencia2> <wildcard2>

3. Verificar su funcionamiento

   show access-list

   show ip interface <interfaz>

De [1]

ACL Estándar

La condición tiene la siguiente estructura:

ValorDeReferencia **BitsAComparar**

Donde:

ValorDeReferencia: tiene el formato de dirección IP

BitsAComparar: es una máscara wildcard

Cada bit en cero en la wildcard hace comparar el bit correspondiente en la dirección.

De [1]

ACL Estándar

Ejemplo 1:

Access-list 10 permit 192.168.30.0 0.0.0.255

Permite todo el tráfico desde la red 192.168.30.0/24. Debido a la sentencia implícita "deny any" (denegar todo) al final, todo el otro tráfico se bloquea con esta ACL.

Las ACL estándar se crean en el modo de configuración global. Se recomienda que se configuren en la interfaz más cercana al destino.

De [1]

ACL Estándar

Ejemplo 2: Bloquear el primer host del rango de la red 192.168.1.0 /24 pero permitir el resto de la red

```
access-list 1 deny 192.168.1.1 0.0.0.0
access-list 1 permit 192.168.1.0 0.0.0.255
```

De [1]

ACL Estándar

Ejemplo 3: Aplicar una acción sólo a los hosts de dirección impar de la subred 192.168.1.0 /26

Access-list 20 permit/deny 192.168.1.1 0.0.0.62

La máscara wildcard de /26 es: 0.0.0.63, pero traduciendo el último octeto de la wildcard a binario 62 = 00111110, **el cero al final le indica al enrutador que compare el último bit de la dirección de referencia con el último bit de cada paquete interceptado,** por lo tanto, como sabemos que todo número impar en binario tiene que tener el último bit en 1, la condición se cumple para cada paquete que tenga los primeros 3 octetos y el último bit iguales a la dirección de referencia, es decir, toda dirección IP de la forma 192.168.1.[impar], con el último octeto en binario así 0 0 X X X X X 1, donde X es un bit cualquiera, porque un **1 en la WC significa no comparar** el bit con la dirección de referencia.

De [1]

ACL Extendida

Pueden filtrar tráfico con más parámetros que las listas de control de acceso estándar. Estos parámetros pueden ser:

- Direcciones IP origen
- Direcciones IP destino
- Tipo de protocolo (TCP, UDP)
- Número de puertos

El número asociado a este tipo de listas varía entre 100 y 199.

De [1]

ACL Extendida

Configuración de ACL Extendida

Los pasos generales para configurar ACLs son 3:

1. Crear la ACL en modo de configuración global
2. Aplicar la ACL en una interfaz indicando la dirección del tráfico al que se le va a aplicar
3. Verificar su funcionamiento

De [1]

ACL Extendida

1. Crear la ACL en modo de configuración global

   interface <interfaz>

   ip access-group <n> [in|out]

2. Aplicar la ACL en una interfaz indicando la dirección del tráfico al que se le va a aplicar

access-list <n> permit <protocolo> <referencia1> <wildcard1> <referencia2> <wildcard2>

access-list <n> deny <protocolo> <referencia1> <wildcard1> <referencia2> <wildcard2>

3. Verificar su funcionamiento

   show ip access-list

   show ip interface <interfaz>

De [1]

ACL Extendida

A diferencia de lo que sucede con la ACL estándar, las extendidas **permiten especificar hacia dónde se dirige el tráfico** y con ésta característica, se puede bloquear o permitir un tráfico **mucho más específico:** sólo tráfico que proviene del host pero se dirige a una red en particular o a otro host en particular o sólo el tráfico de una red que se dirige a otra red en particular. El truco se logra con el hecho de permitir **comparar las direcciones destino** de los paquetes contra la ACL, no sólo las direcciones origen.

De [1]

ACL Extendida

En las ACL extendidas se especifican dos pares de direcciones de referencia/wildcard, un par para la dirección origen de los paquetes y otro par para la dirección destino de los mismos.

Las ACL extendidas no sólo permiten especificar las direcciones origen y destino sino **discriminar por protocolos** e incluso por **parámetros particulares de cada protocolo.**

De [1]

ACL Extendida

El segundo par de dirección de referencia/máscara wildcard, compara la dirección destino de los paquetes con la dirección de la regla. Para las ACL extendidas, el paquete debe coincidir tanto en la dirección origen como en la destino.

La dirección de referencia *0.0.0.0* con máscara wildcard *255.255.255.255,* significa que ningún bit del paquete se compara con la dirección de referencia, es decir, no importa qué escriba en la dirección de referencia cualquier destino coincide. Esta máscara es lo mismo que *any,* debido a que la máscara es equivalente a cualquier dirección y puede usarse tanto para el origen como para el destino.

De [1]

ACL Extendida

Ejemplo 1: Permitir el tráfico del host 192.168.1.1, excepto lo que vaya de ese host a un host particular 172.16.1.1. Además que de la red completa 192.168.1.0 /26 se deniegue todo el tráfico excepto lo que vaya a un servidor en especial, digamos el 192.168.2.1.

Las reglas de la ACL estándar sirven de inicio, como de costumbre lo más específico lo vamos a poner de primero en la regla para evitar que las reglas más generales incluyan a las particulares.

```
access-list 100 deny ip 192.168.1.1 0.0.0.0 172.16.1.1 0.0.0.0
access-list 100 permit ip 192.168.1.1 0.0.0.0 0.0.0.0 255.255.255.255
access-list 100 permit ip 192.168.1.0 0.0.0.63 192.168.2.1 0.0.0.0
access-list 100 deny ip 192.168.1.0 0.0.0.63 0.0.0.0 255.255.255.255
access-list 100 permit ip any any
```

De [1]

ACL Extendida

IP indica que todos los protocolos que se encapsulan dentro de IP serán afectados por ésta lista de acceso. En este caso, la palabra ***ip*** **para los protocolos es similar a *any* en las direcciones,** casi todo se encapsula en ip por lo tanto especificar ip es como especificar cualquier protocolo (de capa 4 en adelante).

En vez de *ip* se puede poner un protocolo equivalente o de capa 4, por ejemplo se puede filtrar *icmp, tcp o udp,* cambiando la palabra *ip* por éstas últimas.

De [1]

ACL Extendida

Ejemplo 2:

Access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80

La ACL 103 permite el tráfico que se origina desde cualquier dirección en la red 192.168.30.0/24 hacia cualquier puerto 80 de host de destino (HTTP).

Las ACL extendidas se crean en el modo de configuración global.

Se recomienda que se configuren en la interfaz más cercana al origen.

Las ventajas de estas listas incluyen que no hacen utilizar el ancho de banda de las interfaces seriales y tienen mayor versatilidad para filtrar información.

De [1]

ACL Nombrada

La idea básica de éstas ACLs es permitir una administración mnemónica de las ACL, ya que en vez de números se usan nombres arbitrarios. Éstas listas pueden ser extendidas o nombradas con las mismas características que las ACLs numeradas y abren un modo especial de configuración (*nacl*) en el que se introducen las reglas una por una empezando por la acción (*permit/deny*).

De [1]

ACL Nombrada

Configuración de ACL Estándar

En su configuración las palabras clave son *ip access-list*, lo que hemos visto hasta este momento, todas las listas de acceso comienzan con la palabra reservada *access-list*, éstas comienzan con *ip access-list*, seguidas del tipo de lista *extended/standard* y el *nombre* (arbitrario). Luego se entra en el modo especial de configuración.

Éstas listas se aplican como se aplican todas las ACLs y se verifican con los mismos comandos. *show ip access-list* y *show ip interface*.

De [1]

ACL Nombrada

Ejemplo 1:

ip access-list extended *INB*

(config-ext-nacl)#permit 172.16.0.0 0.0.255.255 172.17.0.0 0.0.255.255

(config-ext-nacl)#deny any any

De [1]

EJERCICIO

Realizar el Ejercicio 1 – Clase 1: “Configuración básica de ACL” – Simulación 15

REFERENCIAS

[1] (CCNA, 2008)