

# ACL EN ROUTER

En los routers podemos entrar en un modo de configuración especial desde donde podremos escribir una o más sentencias, pertenecientes a un grupo. Una ACL específica que comunicaciones pueden pasar a través del router y que comunicaciones quedarán bloqueadas y no pasarán.

## ACL standard

```
Comando para entrar en el modo ACL: ip access-list standard nº
```

Solo podemos escribir dos tipos de sentencias en este modo ACL:

1. deny sentencia
2. permit sentencia.

Una vez generadas las sentencias ACL se tienen que asociar a una determinada interfaz.

```
ip access-group 1 in
```

Para borrar una sentencia ACL utilizaremos el comando:

```
no ip accesslist 1  
no ip access-group
```

Ejemplo entero de creación de reglas ACL en el router.

```
//Accedemos al modo ACL y creamos el grupo 1  
ip access-list standard 1  
// Denegamos una dirección red  
deny 11.0.0.0 0.255.255.255  
//Salimos  
exit  
//Vamos a la interfaz correspondiente  
interface f0/0  
//Asociamos las reglas ACL a la interfaz correspondiente  
ip access-group 1 in
```

Es importante tener en cuenta que una ACL puede estar compuesta de varias sentencias **permit/deny**. El orden de inserción de estas sentencias es importante porque se comparan con el paquete de datos una detrás de la otra, desde la primera hasta la última. Por eso si se indican sentencias **deny**, se debería añadir al final **permit any**, per tal de evitar que se deniegue todo el

tráfico no indicado explícitamente en la ACL.

# ACL extended

Las reglas ACL standard solo permiten filtrar por tránsito IP, no permiten filtrar por los puertos o los protocolos de capas superiores, además no permiten filtrar todo el tránsito de ip, solo en entrante (in).

Si queremos filtrar el tránsito basado en parámetros como pueden ser la red origen/destino, el equipo de origen/destino, el protocolo o la aplicación utilizados.

Las ACL standard suelen tener un número asignado entre 0 y 99. Las ACL extendidas suelen tener un número entre 100 y 199.

## Ejemplos prácticos

Denegar el tránsito de la red 11.0.0.0 hacia la red 192.168.2.0, permitiendo el resto de tránsito.

```
ip access-list extended 100
deny tcp 11.0.0.0 .0.255.255.255 192.168.2.0 0.0.0.255 eq 80
permit tcp any any
exit
interface f0/0
ip access-group 100 in
exit
exit
show ip access-list
```

Permitir el tránsito ICMP desde 11.0.0.2 hacia 172.17.0.2, el resto de tránsito de denegará.

```
ip access-list extended 100
permit icmp host 11.0.0.2 host 172.17.0.2 echo
permit icmp host 11.0.0.2 host 172.17.0.2 echo-reply
exit
interface f0/0
ip access-group 100 in
```

Denegar todo el tránsito telnet desde 11.0.0.2 hacia 192.168.1.0, el resto se ha de permitir.

```
ip access-list extended 100
deny tcp host 11.0.0.2 192.168.1.0 0.0.0.255 eq 23
permit tcp any any
exit
interface f0/0
ip access-group 100 in
```

Revision #1

Created 29 November 2023 00:44:52 by adminROM

Updated 29 November 2023 00:45:06 by adminROM