Listas de Control de acceso
ACL

Laboratorio de Redes de Computadores

Grado de Ingeniería Informática

Listas de Control de acceso

- **Lista de Control de Acceso** o **ACL** (del inglés, *Access Control List*)
- Es una forma de determinar los permisos de acceso.
- Concepto de seguridad informática usado para filtrado de tráfico.
- Las ACLs permiten controlar el flujo del tráfico

Tipos de ACL

- **ACL estándar**, donde solo tenemos que especificar una dirección de origen.
- **ACL extendida**, en cuya sintaxis aparece el protocolo y una dirección de origen y de destino.
- ACL con nombre, permite dar nombres en vez de números a las ACL estándar o extendidas.

ACL estándar

- **(config)#access-list n {permit | deny} source {source-mask}**
- Ejemplos:
- (config)#access-list 1 deny 10.5.3.0 0.0.0.255
- (config)#access-list 1 permit host 10.5.3.37
- (config)#access-list 1 permit any

ACL extendida

- **(config)#access-list n {permit | deny}** ***protocol*** **source {source-mask} destination {destination-mask} [eq destination-port**]
- Ejemplos
- (config)#access-list 105 permit 10.5.4.0 0.0.0.255 host 10.5.64.30 eq 80
- (config)#access-list 105 permit host 10.5.3.37 10.5.64.0 0.0.63.255
- (config)#access-list 105 deny 10.5.3.0 0.0.0.255 any

Aplicar la lista a un interface:

- Ejemplo:
- (config)#interface serial 0/0
- (config-if)#ip access-group 100 out

Sintaxis

- Protocolo: ip | tcp | udp | icmp
- comparación: gt | lt | eq
- gt = greater than, lt = lesser than, eq = equal
- Origen de una sola ip: host
- Origen de cualquier ip: any
- Máscara wildcard: el inverso de la máscara.

¿Dónde se aplican las ACL?

- Las listas de acceso estándar se deben colocar cerca del destino.
- Las listas de acceso extendidas se deben colocar cerca de la fuente.

¿Dónde se aplican las ACL?

Ejemplo: Si se desea bloquear el tráfico del origen al destino, mejor aplicar una ACL entrante a E0 en el router A en vez de una lista saliente a E1 en el router C

¿Dónde se aplican las ACL?

- **In**: el tráfico que llega a la interfaz y luego pasa por el router.

- **Out**: el tráfico que ya ha pasado por el router y está saliendo de la interfaz.

Normas

- Se puede tener una lista de acceso por protocolo, por dirección y por interfaz.
- No se puede tener dos listas de acceso a la dirección entrante de una interfaz.
- Se puede tener una lista de acceso de entrada y una de salida aplicada a una interfaz.

Otros comandos ACL

- Mostrar las listas de acceso:

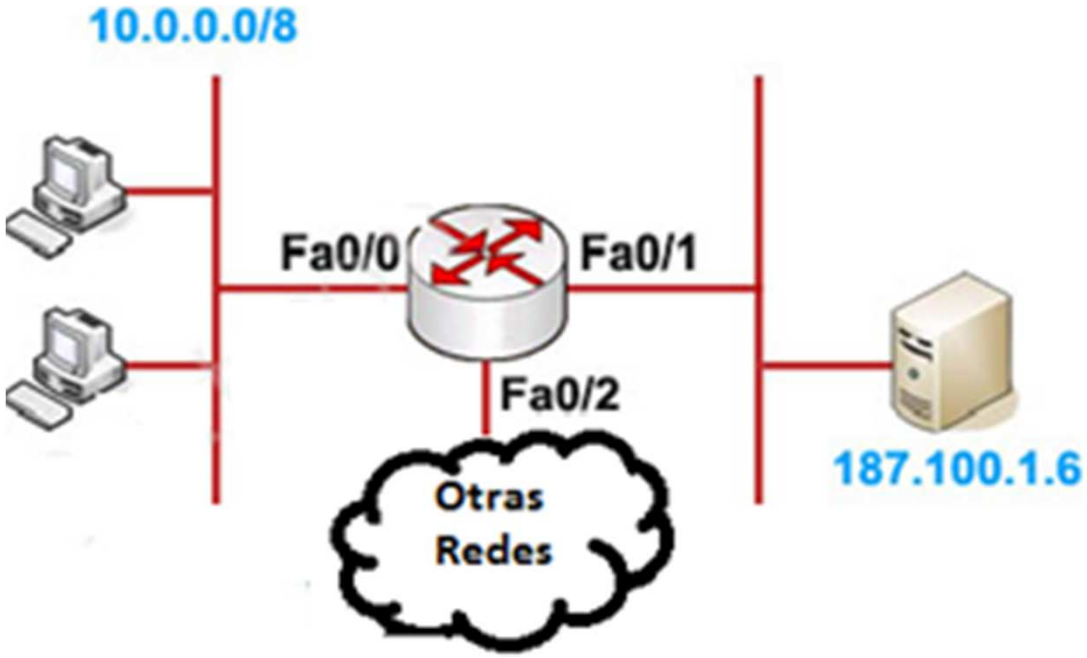
  Router#show access-list

- Borrar una ACL:

  Router(config)#no access-list n

- La modificación de una ACL requiere especial atención. Si intenta eliminar una línea concreta de una ACL numerada, se eliminará toda la ACL

Ejemplo ACL estándar



Definir una lista de acceso estándar que permita solo a la red 10.0.0.0/8 acceder al servidor localizado en la interface Fa0/1.

Ejemplo ACL estándar

- **Primer paso: Definir a quien se le permite el tráfico:**
- Router(config)#access-list 1 permit 10.0.0.0 0.255.255.255
- (Siempre hay implícito una prohibición (deny) al resto de tráfico al final de la ACL por eso no necesitamos añadir “deny” al resto de tráfico.

Ejemplo ACL estándar

- **Segundo paso: Aplicar la ACL a la interface:**
- Router(config)#interface Fa0/1
- Router(config-if)#ip access-group 1 out

Ejemplo ACL extendida

- Router(config)# access-list 101 deny icmp any any
- Router(config)# access-list 101 permit ip any any

- Router(config)#interface Fa0/0
- Router(config-if)#ip access-group 1 out

Ejemplo1 ACL nombrada

- Ejemplo de una ACL nombrada “INTRANET” denegando tráfico DNS:
- Router(config)#ip access-list extended INTRANET
  Router(config-ext-nacl)#deny tcp any any eq 25
  Router(config-ext-nacl)#permit ip any any
  Router(config-ext-nacl)#exit
  Router(config)#interface ethernet 1
  Router(config-if)#ip access-group INTRANET out

Ejemplo2 ACL nombrada

- router(config)# ip access-list extended test
- router(config-ext-nacl)# permit ip host 2.2.2.2 host 3.3.3.3
- router(config-ext-nacl)# permit tcp host 1.1.1.1 host 5.5.5.5 eq www
- router(config-ext-nacl)# permit icmp any any
- router(config-ext-nacl)# permit udp host 6.6.6.6 10.10.10.0 0.0.0.255 eq domain

Ejemplo2 ACL nombrada

- Router(config-ext-nacl)#exit
- Router(config)#interface ethernet 1
- Router(config-if)#ip access-group test out