

**Ejercicio 11. Listas de control de acceso (ACLs)**

#### En la realización de estos ejercicios debes considerar como independiente cada una de las ACLs. Para probar las ACLs en PT se te recomienda desactivar las ACLs previas a cada inciso.

#### Utiliza la información de la siguiente gráfica y diseña cada una de las listas de control de acceso solicitadas.



1. Diseña una lista de control de acceso estándar para **impedir** que las computadoras de la subred de **Alumnos** tengan acceso a la subred de **Directivos**.

**access-list número\_lista {permit|deny} IP\_Origen wildcard**

**access-list 10 (lista entre 1 y 99 acceso estándar)**

**access-list 10 deny 132.254.89.0/25 wildcard**

255.255.255.1000 0000

**255.255.255.255**

**- 255.255.255.128**

**------------------------------**

**0 . 0. 0. 127**

**access-list 10 deny 132.254.89.0 0.0.0.127 (negamos el tráfico de todas la redes, por eso tenemos que permitir el tráfico de las otras redes)**

**0 . 0. 0. 127**

**access-list 10 deny 132.254.89.0 0.0.0.127**

**access-list 10 permit any**



**Una vez diseñada la ACL se asigna a una interfaz**

**interface int\_número**

**ip access-group número list {in | out}**

int g0/0

ip access-group 10 {in | out}



**access-list 10 deny 132.254.89.0 0.0.0.127**

**access-list 10 permit any**

**int g0/0**

**ip access-group 10 out**

¿En qué router instalarás esta lista de control de acceso? \_\_RouterA\_\_\_\_\_\_\_\_\_\_\_

router(config)#\_\_\_\_ **access-list 10 deny 132.254.89.0 0.0.0.127**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)#\_\_\_\_ **access-list 10 permit any**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)# interface \_g0/0\_\_\_\_\_\_\_\_

router(config-if)#\_\_\_ **ip access-group 10 out** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Diseña una lista de control de acceso estándar para **impedir** que las computadoras de la subred de **Profesores** tengan acceso a la subred de **Directivos**.

¿En qué router instalarás esta lista de control de acceso? \_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)# interface \_\_\_\_\_\_\_\_\_

router(config-if)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

access-list 20 deny 132.254.89.232/29

**access-list 20 deny 132.254.89.232 0.0.0.7**

**access-list 20 permit any (si quito este comando nadie va a poder entrar a la subred de Directivos ya que una un deny any implícito)**

**int g0/0**

**ip access-group 20 out**

255.255.255.11111000

255.255.255.255

255.255.255.248

---------------------------

0.0.0.7

Tengo que apagar mi lista de acceso anterior, ya que solamente puedo tener una lista de acceso in y otra out.

**no ip access-group 10 out (tengo que desactivar mi lista de acceso anterior de la interface, no la quito solo la desactivo) 10 o 20 es como darle un nombre a la lista de acceso. Las interfaces ya no tendrían asociadas listas de control de acceso.**

Si tengo dos listas de acceso in, va a tomar la última lista instalada. Cuantas listas soporta una interface de entrada y una lista soporta una interface de salida. Solamente podemos tener una lista de entrada y una de salida.

1. Diseña una lista de control de acceso estándar para **impedir** que las computadoras de la subredes de **Profesores y Alumnos** tengan acceso a la subred de **Directivos**.

¿En qué router instalarás esta lista de control de acceso? \_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)# interface \_\_\_\_\_\_\_\_\_

router(config-if)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

access-list 20 deny 132.254.89.232/29

**access-list 20 deny 132.254.89.232 0.0.0.7**

**access-list 20 deny 132.254.89.0 0.0.0.127**

**access-list 20 permit any**

**int g0/0**

**ip access-group 20 out**

255.255.255.11111000

255.255.255.255

255.255.255.248

---------------------------

0.0.0.7

Pregunta si invertimos que haría

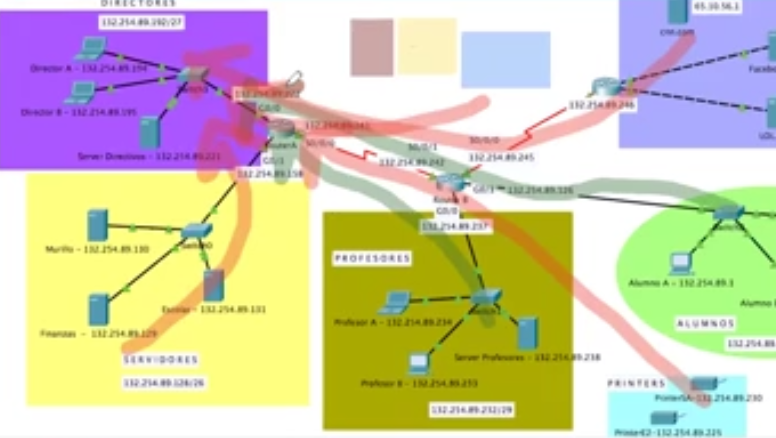
**access-list 20 permit 132.254.89.232 0.0.0.7**

**access-list 20 permit 132.254.89.0 0.0.0.127**

**access-list 20 deny any (niega el acceso a todas la demás subredes, incluyendo nuevas)**

**int g0/0**

**ip access-group 20 out**



Tengo que apagar mi lista de acceso anterior, ya que solamente puedo tener una lista de acceso in y otra out. Si tengo dos listas de acceso in, va a tomar la última lista instalada. Cuantas listas soporta una interface de entrada y una lista soporta una interface de salida. Solamente podemos tener una lista de entrada y una de salida.

1. Diseña una lista de control de acceso estándar para que el **visitante 01** no pueda acceder a la sección de **servidores**

¿En qué router instalarás esta lista de control de acceso? \_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)# interface \_\_\_\_\_\_\_\_\_

router(config-if)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**access-list 30 deny 132.254.89.120 0.0.0.0 (match exacto con la dirección ip)**

**hAY UN DENY ANY POR DEFAULT, POR ESO TENGO QUE PONER PERMIT ANY.**

**access-list 30 permit any**

**int g0/1**

**ip access-group 30 out**

**access-list 30 deny 132.254.89.120 0.0.0.0**

**access-list 30 permit any**

**int g0/1**

**ip access-group 30 out**

**access-list 30 deny host 132.254.89.120 (es lo mismo que lo anterior, niega al host el acceso y los comandos son equivalentes)**

**access-list 30 permit any**

**int g0/1**

**ip access-group 30 out**

!

access-list 10 deny 132.254.89.0 0.0.0.127

access-list 10 permit any

access-list 20 deny 132.254.89.232 0.0.0.7

access-list 20 permit any

access-list 30 deny host 132.254.89.120

access-list 30 permit any

En el router hay 3 listas de acceso, la última sería la que tendría efecto alguno.