

**Ejercicio 11. Listas de control de acceso extendidas**

#### 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 los **Alumnos** tengan acceso a la subred de **Directivos** y a la subred de **Profesores**.

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

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

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

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

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

**Router A y B**

**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**



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

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

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

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

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

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

**Router B**

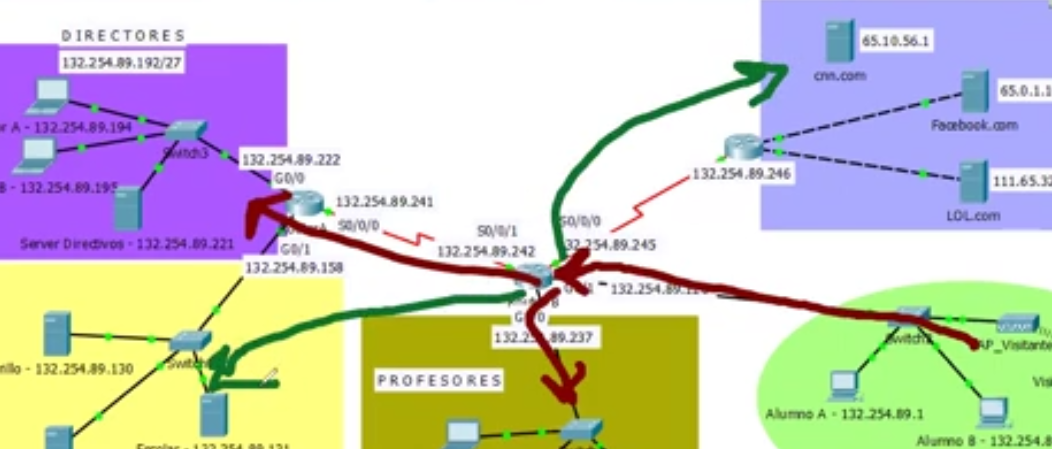
**access-list 110 deny ip 132.254.89.0 0.0.0.127 132.254.89.192 0.0.0.31**

**access-list 110 deny ip 132.254.89.0 0.0.0.127 132.254.89.232 0.0.0.7**

**access-list 110 permit ip any any**

**int g0/1**

**ip access-group 110 in**



1. Diseña una lista de control de **acceso extendida** para **impedir** que las computadoras de la subred de **Profesores** tengan **acceso al server de la subred de Directivos**.

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

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

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

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

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

**Router B**

**!access-list 120 deny ip 132.254.89.232 0.0.0.7 132.254.89.221 0.0.0.0**

**access-list 120 deny ip 132.254.89.232 0.0.0.7 host 132.254.89.221**

**access-list 120 permit ip any any**

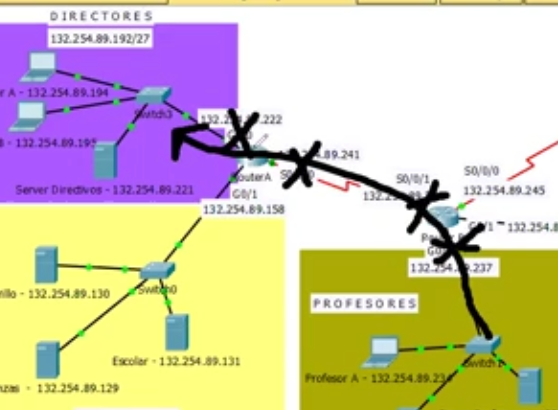
**int g0/0**

**ip access-group 120 in**

La lista de control de acceso puede ir en varios lugares, pero la mejor práctica es colocarla

Entre más me aleje de la fuente el tráfico fluye de manera innecesaria hasta llegar al destino.

Como una sugerencia de mejores prácticas una lista de acceso extendida debe de ubicarse lo más cercana a la fuente.



Aquí se ubicaría la lista de acceso



1. Diseña una lista de control de **acceso extendida** para que el **visitante 01** no pueda acceder a las servicios externos de **Internet**

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

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

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

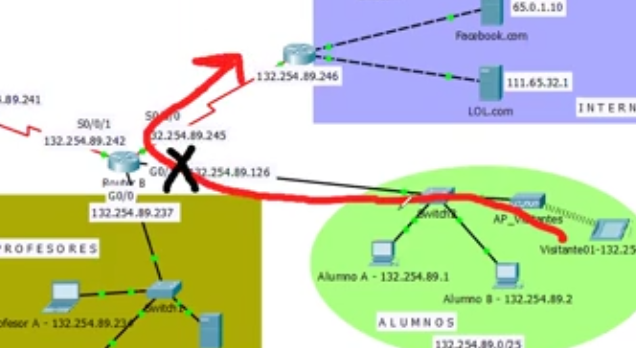
router(config)# interface \_\_\_\_\_\_\_\_\_

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

Todo el tráfico que no conozco se va a llamar ANY.



Bloquear el tráfico en este punto no es la mejor idea, ya que podría bloquear el tráfico hacia las subredes que sí tiene acceso como la de profesores y otras.



Bloquear el tráfico en la s0/0/0 sería la mejor opción y se bloquearía con el tráfico de salida.



No queremos que salga a Internet puedo bloquear todo el protocolo ip o puedo bloquear el protocolo tcp. Nosotros decidimos. Podemos bloquear el protocolo tcp. Todo el protocolo tcp estaría bloqueado, pero el ping va a poder salir.

El destino es any, ya que quiero que le niege el acceso a cualquier dispositivo en el exterior. No le pongo el puerto ya que quiero incluir todos los puertos de tCP incluyendo UDP.

**Router B**

**access-list 130 deny tcp host 132.254.89.1 any (NEGANDO PROTOCOLO TCP A UN HOST A CUALQUEIR DESTINO)**

**access-list 130 permit ip any any (PERMITO EL RESTO DEL TRÁFICO)**

**! Voy a permitir el ping**

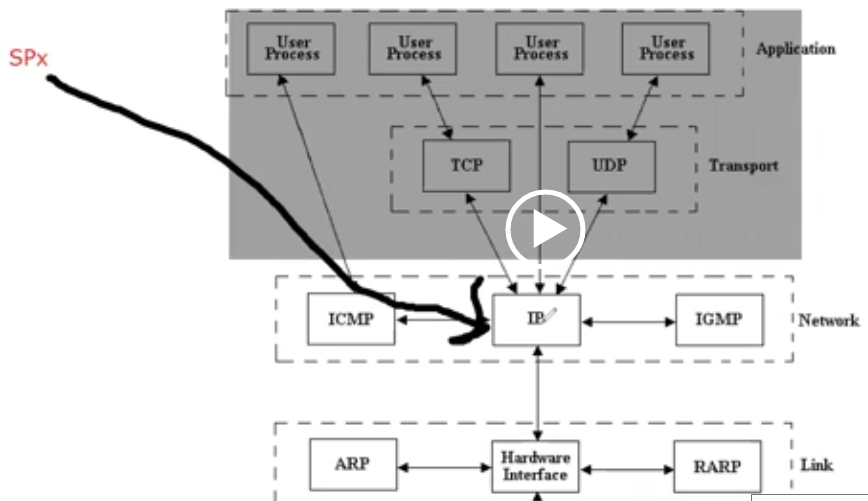
**int s0/0/0**

**ip access-group 130 out**

**Se bloquea procolo capa 4, pero está permitido el protocolo capa 3. Por eso permitiría el ping. Puede transportar todos los protocolos que no sean de la capa 4.**

**Todos los protocolos de la capa 4, 5, 6 y 7 hacen uso del protocolo ip.**

**Muchos protocolos no ligados a TCP pueden fluir, como protocolos de la capa de sesión que se ligan con la capa de red, etc.. TCP y UDP bloqueados.**

****

1. Diseña una lista de control de acceso extendida para que la sección de **Alumnos** no pueda acceder al **servidor de profesores** vía el protocolo **WEB** ni por **FTP**.

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

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

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

router(config)#

interface \_\_\_\_\_\_\_\_\_

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

**Router B**

**!PROTOCOLO FTP**

**access-list 140 deny tcp 132.254.89.0 0.0.0.127 host 132.254.89.238 eq 20**

**access-list 140 deny tcp 132.254.89.0 0.0.0.127 host 132.254.89.238 eq 21**

**!PROTOCOLO WEB**

**access-list 140 deny tcp 132.254.89.0 0.0.0.127 host 132.254.89.238 eq 80**

**access-list 140 permit ip any any**

**! Voy a permitir el ping**

**int G0/0**

**ip access-group 140 out**

1. Diseña una lista de control de acceso extendida para que ninguna dirección IP interna de nuestra red pueda acceder al servidor de **LOL** vía el protocolo **WEB**. ¿En qué router instalarás esta lista de control de acceso?

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

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

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

router(config)#

interface \_\_\_\_\_\_\_\_\_

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

Se instalaría en el router B, DE SALIDA. Entrada ANY y salida ANY



**Router B**

**access-list 150 deny tcp any host 111.65.32.1 eq 80**

**access-list 150 permit ip any any**

**int s0/0/0**

**ip access-group 150 out**