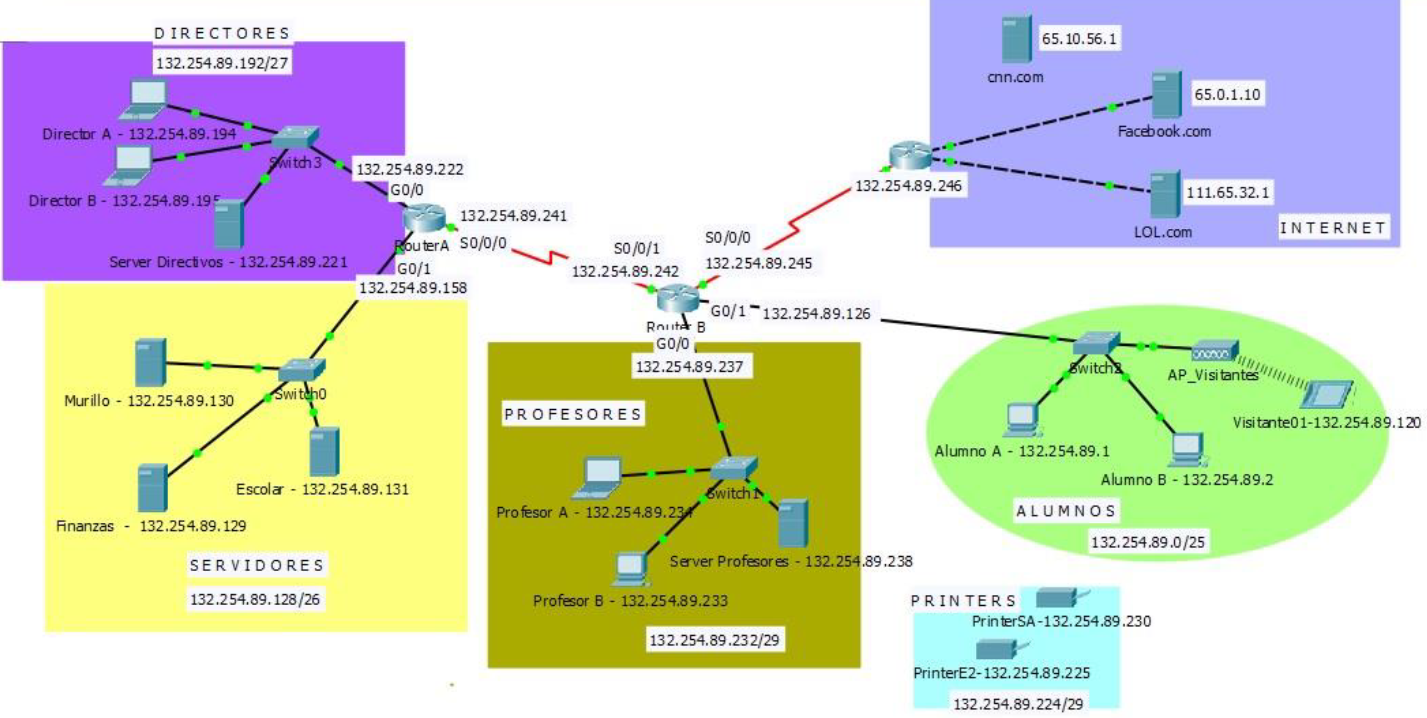


**Ejercicio 12. Listas de control de acceso extendidas**

#### 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)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Primero hago acceso web de Alumnos a los servidores de Directivos (221) y Profesores (238). Si utilizo el protocolo capa 4, garantizo que también el protocolo 3 esta funcionando.**

**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**

****

Tenemos dos opciones ponemos la lista de control de acceso en el routeb de entrada o la otra opción es colocarlo en cada interface de las subredes que no queremos llegar. Es importante buscar que la lista de acceso sea lo más eficiente.



Primero instalo en router b y pruebo el acceso a los dos servidores y luego instalo en router a. Pruebo hacia l subred de servidores y también al exterior Facebook.



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**

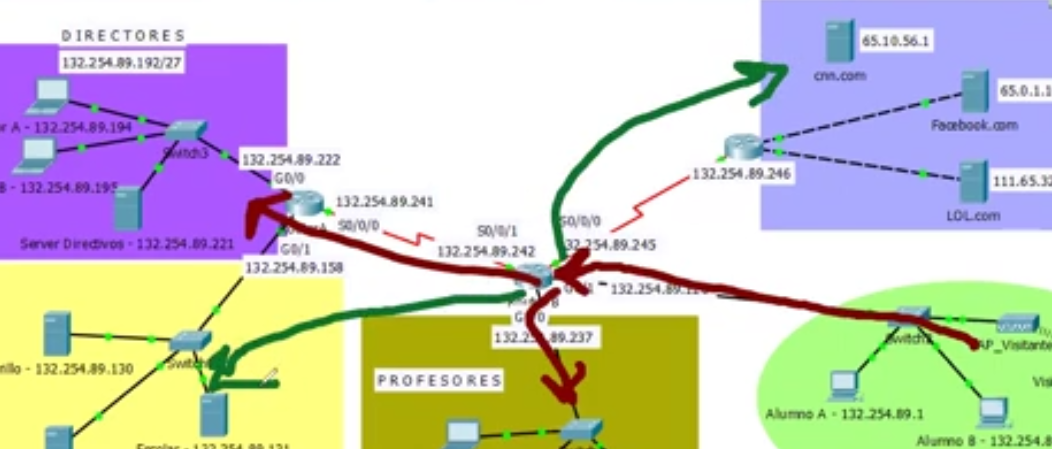
**access-list 110 deny ip 132.254.89.0 0.0.0.127 132.254.89.192 0.0.0.31**

**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 (fuente destino)**

**int g0/1**

**ip access-group 110 in**



Quitar listas de acceso anteriores y pruebo el tráfico si fluye.

Voy a colocar la lista extendida en el router b para que el tráfico no pueda fluir en los sentidos no permitidos. EN el protocolo si le pongo tcp bloqueo solamente tráfico de la capa 4, si bloqueo IP bloqueo tráfico de la capa 3, 4, 5, 6 y 7. Y no queremos que tenga acceso a nada. Operando número de puerto se ocupa si utilizamos protocolo tcp, si utilizamos ip no se ocupa.

Primero negamos el tráfico de estudiantes a profesores y luego a directivos. Luego debo permitir todo el tipo de tráfico.

Se asigna al router b de entrada para que se filtre el tráfico a la entrada.

Primero antes de colocar la lista de control de acceso, checamos acceso web hacia directores y profesores.

Colocamos lista y probamos el acceso a los servidores de directores y profesores (Web y ping), y también a los que sí tengo acceso de servidores y acceso al exterior. Ping destination host unreachable el router no tiene ruta a destino. Quitar lista de acceso y probar.

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 EQUIPOS NO CISCO**

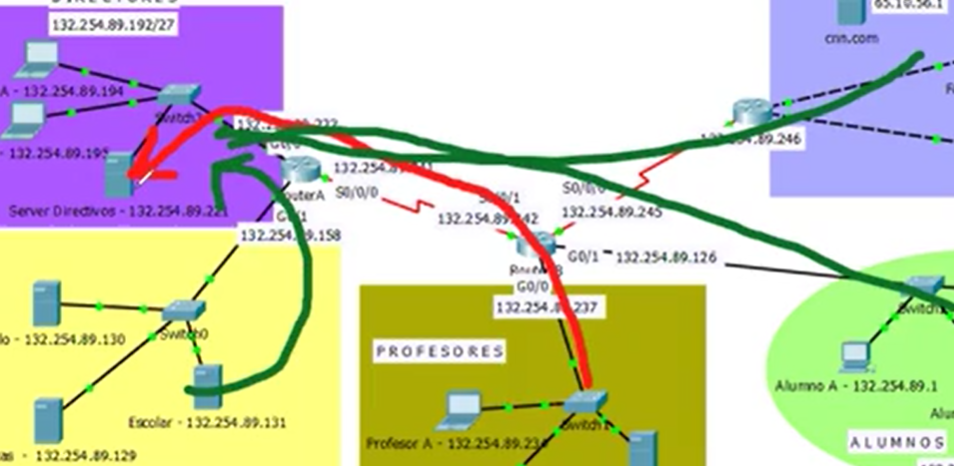
**access-list 120 deny ip 132.254.89.232 0.0.0.7 host 132.254.89.221 SOLO EQUIPOS CISCO**

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

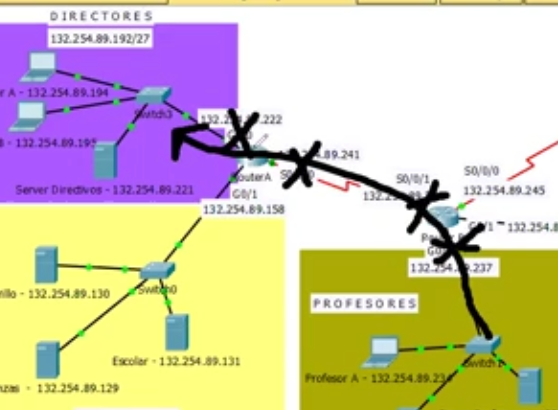
**int g0/0**

**ip access-group 120 in**

**Se quiere negar tráfico ip y tcp de profesores al server de directivos.**



**Las listas de acceso extendidas pueden ir en cualquier lugar, pero la intensión de las listas de control de acceso extendidas es evitar que el tráfico fluya dentro de la red ya que va a inundar los canales de comunicaciones.** La lista de control de acceso puede ir en varios lugares, pero entre más me aleje de la fuente el tráfico está fluyendo de forma 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



Primero hago acceso web de una compu de profesores al servidor de directivos (132.254.89.221) y funciona.

Luego coloco lista de acceso en router b.

Vuelvo a probar el acceso web de profesores al servidor de directivos (.221) y no funciona.

Probamos acceso web de profesores a Servidores (murillo .130) debe funcionar.

Probar acceso web a los servicios hacia el exterior Facebook (6.0.1.10)

Con ping hago acceso a impresoras (.130)

Comunicarme por ping al servidor de Directivos (89.221)

Los estudiantes pueden entrar al servidor de Directivos (89.221)

Quitar la lista de acceso para completar los siguientes incisos.

Probar acceso a Directivos.

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)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

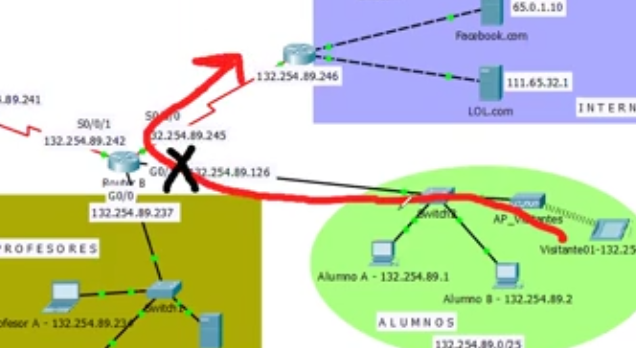
Visitante 01 puede acceder a todas las redes menos al exterior.

Todo el tráfico que no conozco y que está en el exterior lo vamos a identificar como ANY.

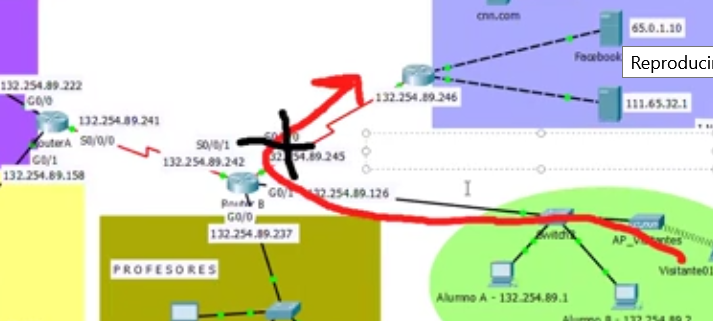


Donde colocamos la lista de acceso?

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, servidores y directores.



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. Incluyo todo el tráfico de TCP

**Primero verifico el acceso del visitante01 a los servicios internos (servidor de directores (.221) funciona, servidor de profesores (.238). Finalmente al exterior 65.0.1.10 no permite salir.**

**Bloqueamos protocolo TCP, pero no bloqueamos IP, hay que probar ping hacia FACEBOOK (65.0.1.10). Si lo debe permitir.**

**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 protocolo 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.**

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 PUERTO EN PARTICULAR 80**

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

**! Voy a permitir el ping**

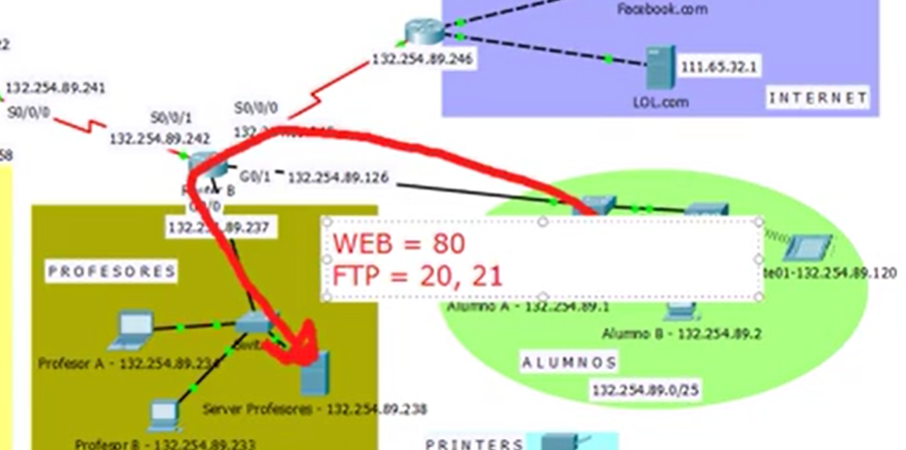
**PUEDO PONER LOS PUERTOS 20, 21 y 80, o en desorden se checa de arriba abajo.**

**int G0/1**

**ip access-group 140 in**

**Los estudiantes no pueden entrar al servidor de profesores solamente por dos protocolos WEB que utiliza el puerto 80 y el protocolo FTP que utiliza los puertos 20 y 21. Un puerto es de control y otro es para el intercambio de los datos. Hay que bloquear ambos puertos 20 y 21. La lista de acceso la puedo establecer en el router B g0/1 y en la g0/0. La voy a asignar lo más cerca al origen**

**Hacer ping a servidor de profesores (.238) funciona**



**Hacer ping a servidor de profesores (.238) funciona y ftp.**

**Para probar ftp: LA CUENTA Y PASSWORD ES CISCO. Con dir puedes ver directorio**

**ftp 132.254.89.238**

**Configurar lista de acceso en router**

**Probar ftp no acceso y ping si acceso (.238)**

**Pruebo desde web (.238) no acceso**

**Pruebo acceso al exterior y a las otras redes.**

**Quitas la lista de acceso**

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)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

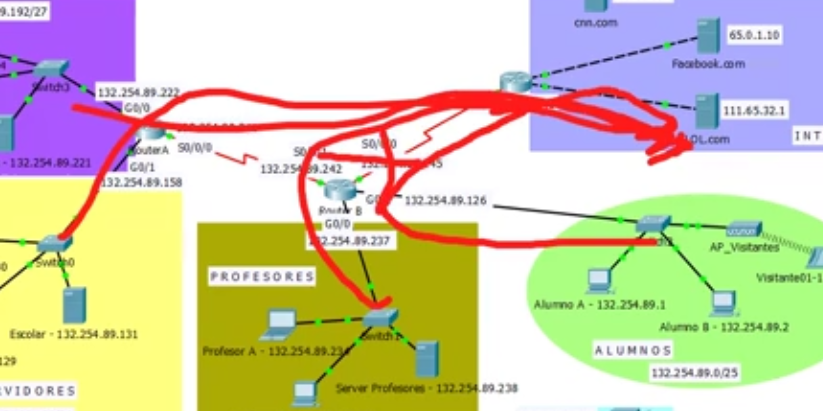
router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)#

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

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

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



**Nadie va a poder entrar a LOL VÍA el protocolo WEB**

**Primero probar todos los accesos a LOL funcionan desde cualquier subred.**

**Asignar lista al router b intefaz de salida**

**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**