

**Ejercicio 8. 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.



Este esquema tenemos varias subredes, la subred de alumnos con 128-2 direcciones disponibles.

La subred de profesores con 8-2 direcciones disponibles.

Tres servidores simulando Intenet (cnn solo ping) Facebook y LOL si se pueden acceder por TCP

**Pruebas de conectividad con servidores son exitosos. Hay conectividad desde directores hacia el Internet**

Pc (Director A) directores hacia servidor 65.0.1.10 Facebook.com (WEB)

Pc (Director A) directores hacia servidor 111.65.32.1 LOL Server (WEB)

Pc (Director A)directores hacia 65.10.56.1 CNN por ping

**Para checar tráfico de subred de Alumnos a Directores**

Tablet01 (Visitante 01) acceder a través del protocolo Web a los directivos (**Server Directivos) 132.254.89.221**.

**Para checar tráfico de Alumnos a Servidores**

Tablet01 (Visitante 01) acceder a través del protocolo Web al servidor **Murillo 132.254.89.130** y **Escolar 132.254.89.131 (Punto Azul)**

**Para checar tráfico de Alumnos a Profesores**

Tablet01 (Visitante 01)acceder a través del protocolo Web al servidor **Profesores 132.254.89.232**

La conectividad existe.

El tráfico llega al router y se analiza. **Las listas de control de acceso estándar bloquean todo el tráfico web y ping.** (capa 3 ping y capa 4 aplicaciones protocolo http)

Mejores prácticas para el diseño de ACLs

1. Identificar la fuente/origen (tráfico fuente) **SUBRED ALUMNOS**
2. Identificar el tráfico no permitido. trayecto de la fuente al destino Trazar el flujo de tráfico
3. Identificar el tráfico permitido.
4. Identificar el router donde se instalará la lista de control de acceso.
5. Identificar la interfaz donde se va a asociar la lista de control de acceso.
6. Determinar la interface donde se va a insertar la lista de acceso. Si pongo lista de acceso en la interfaz s0/0/0 las subredes de servidores y directores no recibirán tráfico de los alumnos y eso no se pide. La interface g0/0/0 es la que hay que seleccionar ya que es la que se conecta con la subred morada.

**REGLA, LA LISTA DE ACESO ESTÁNDAR SE DEBEN INSTALAR LO MAS CERCA DEL DESTINO.**

Red de estudiantes hacia Internet, servidores,

**EJERCICIO 1**

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**

**¡deny any IMPLICITO (negamos el tráfico el tráfico anterior y de TODAS LAS redes a la subred de directivos, por eso tenemos que permitir el tráfico de las otras redes)**

**DISEÑO DE LA ACL**

**access-list 10 deny 132.254.89.0 0.0.0.127**

**access-list 10 permit any QUE PERMITA EL RESTO DEL TRÁFICO**



**ASOCIAR ACL A LA INTERFAZ**

**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** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Primero **pruebo el acceso de Tablet visitantes 01 a un servidor de directores** (funciona)

Después **copio y pego la configuración de la lista de acceso en el router A** en config t.

Intentar acceso de **alumnos (tablet visitantes 01)**

* Al servidor de directivos 132.254.89.221 por **web (no)**
* Al servidor de directivos 132.254.89.221 por **ping (no)**
* Al servidor Murillo (Servidores) (Murillo 132.254.89.130)
* Al servidor de profesores (Profesores) (132.254.89.238)
* Al Intenet Facebook 65.0.1.10

**El tráfico llega al router y se analiza. Las listas de control de acceso estándar bloquean todo el tráfico web y ping.**

* **Capa 3 del modelo OSI (red) donde está incluido el ping**
* **Capa 4 del modelo OSI (transporte) donde están los protocolos de transporte tcp /udp donde está incluido el protocolo http (80) con la que funciona la aplicación web**

Hay que probar lista de acceso y luego la desinstalo o la hago independiente. Desasocio la lista de control de acceso, la desactivo. No elimino la lista de acceso, solamente la desasocio o la desactivo. **Checo conectividad y checo sh run y la interface yo no tiene asociada una lista de acceso.**

**no ip acces-group 10 out**



La interface g0/0 es la que da servicio a los directores

La interface g0/1 es la que da servicio a los servidores.

En la interface g0/0 es donde vamos a instalar la lista de control de acceso.

**Hay dos direcciones de tráfico en las interfaces**, el tráfico de entrada hacia el router **(in)** y el tráfico de **salida** hacia los dispositivos. **G0/0 y dirección de salida**

**EJERCICIO 2**

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

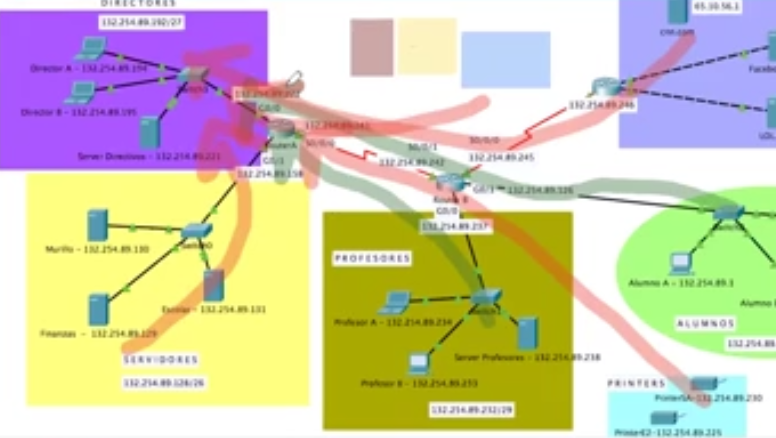
**access-list 20 permit 132.254.89.232 0.0.0.7**

**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.

**No ip access-group 20 out no quito la lista de control de acceso, solo la desactvo de la interface. Hay listas que no se están ocupando.**

**EJERCICIO 3**

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. Y ESTO BLOQUEARÍA TODO EL TRÁFICO.**

**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 GROUP ES UN GRUPO DE INSTRUCCIONES)**

**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) SOLAMENTE EN NOMENCLATURA DE CISCO**

**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.

SI QUISIERAMOS BLOQUEAR TAMBIÉN EL ACCESO A DIRECTORES PUEDO APLICAR LA LISTA DE ACCESO A DIRECTORES G0/0

PROBAR DE MANERA INDEPENDIENTE CADA LISTA.

LA EJECUCIÓN DE LOS COMANDOS VA DE ARRIBA HACIA ABAJO.

CUMPLE PRIMERA REGLA, SEGUNDA REGLA Y SINO TENGO UN DENY ANY CONFIGURADO, ESTÁ IMPLÍCITO AL FINAL.

**AL FINAL HAY QUE PERMITIR TODO EL TRÁFICO O NEGAR TODO EL TRÁFICO DE FORMA EXPLICITA.**

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

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.

Diagrama

Descripción generada automáticamente

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

Diagrama

Descripción generada automáticamente

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 **impedir** que las computadoras de la subred de **Profesores** tengan **acceso al server de la subred de Directivos**.

**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**

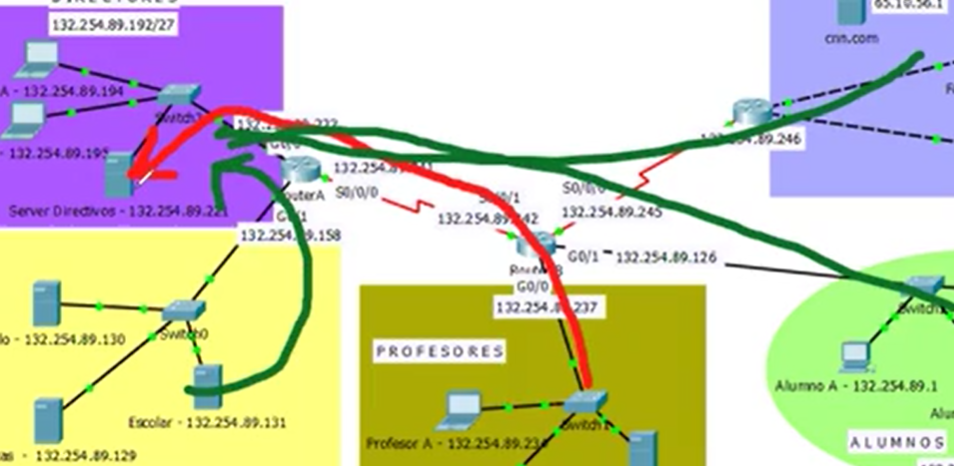
**access-list 120 deny ip 132.254.89.232 0.0.0.7 host 132.254.89.221 SOLO EQUIPOS CISCO**

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

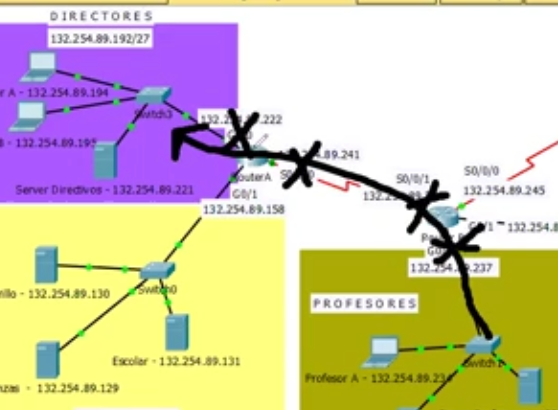
**int g0/0**

**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**

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.

Diagrama

Descripción generada automáticamente

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

Diagrama

Descripción generada automáticamente

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**.

**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**

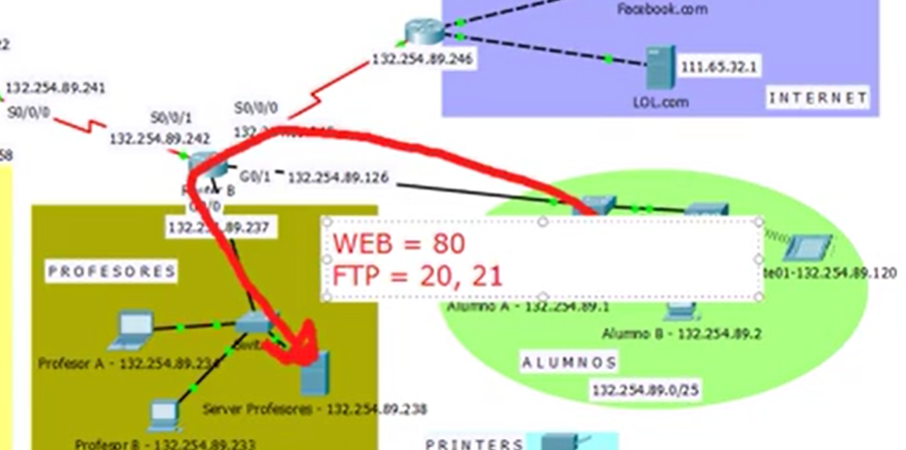
**PUEDO PONER LOS PUERTOS 20, 21 y 80, o en desorden se checa de arriba abajo.**

**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**

**EJERCICIO 7**

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?

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**