Listas de acceso

* **Estándar** bloquea con base a la dirección fuente. (**1 al 99** para identificar lista estándar)
* **Extendida:** filtra con base a dirección fuente, destino, tipo de protocolo e inclusive el puerto que se puede utilizar **(100 a 199)**

**Wildcard (MÁSCARA COMODÍN)** es un complemento de la máscara de Subneteo.

**Any** significa cualquier dirección : **0. 0. 0. 0 255.255.255.255**

Dirección inicial Todos los posibles cambios (permite cualquier dirección)

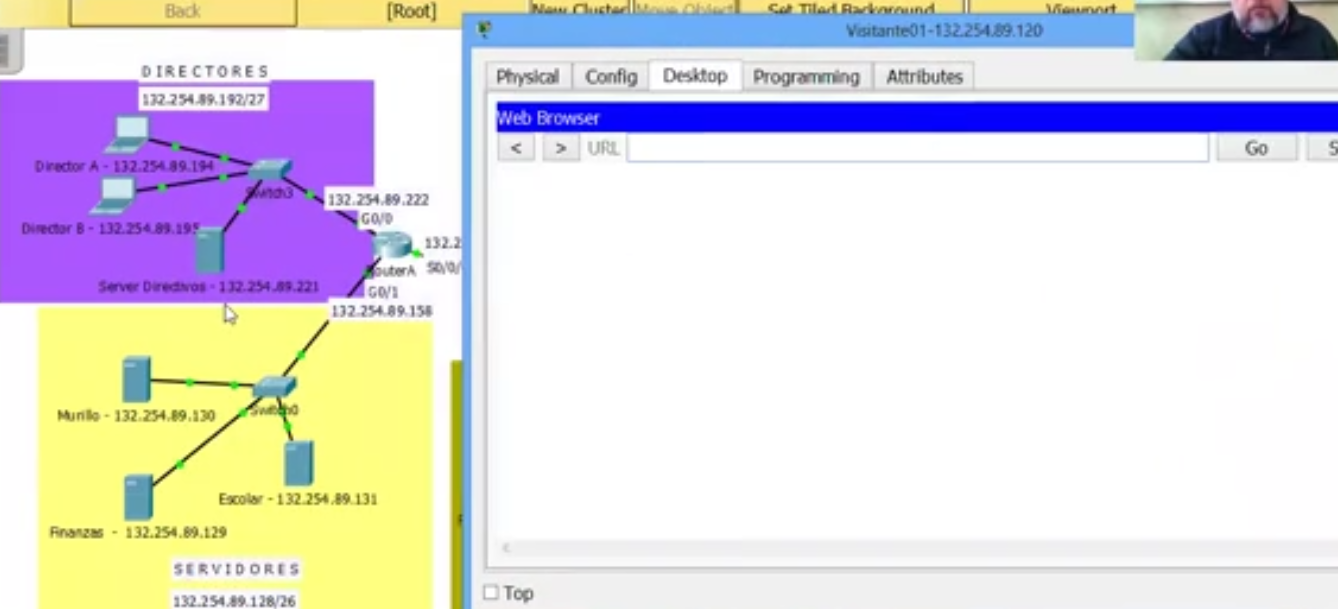
**Host :** match exacto

A B C D 0.0.0.0

La lista no tiene acceso hasta que no haya sido asignada a una interface.

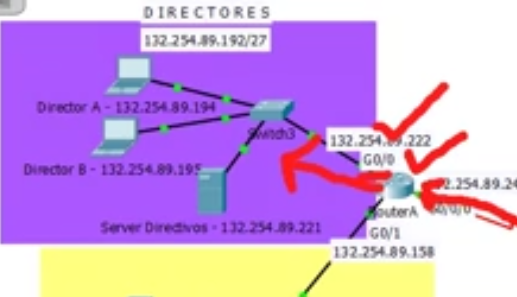
Cada lista a una lista de acceso de entrada y una lista de acceso de salida.

Acceder a través del protocolo web al servidor de directivos.



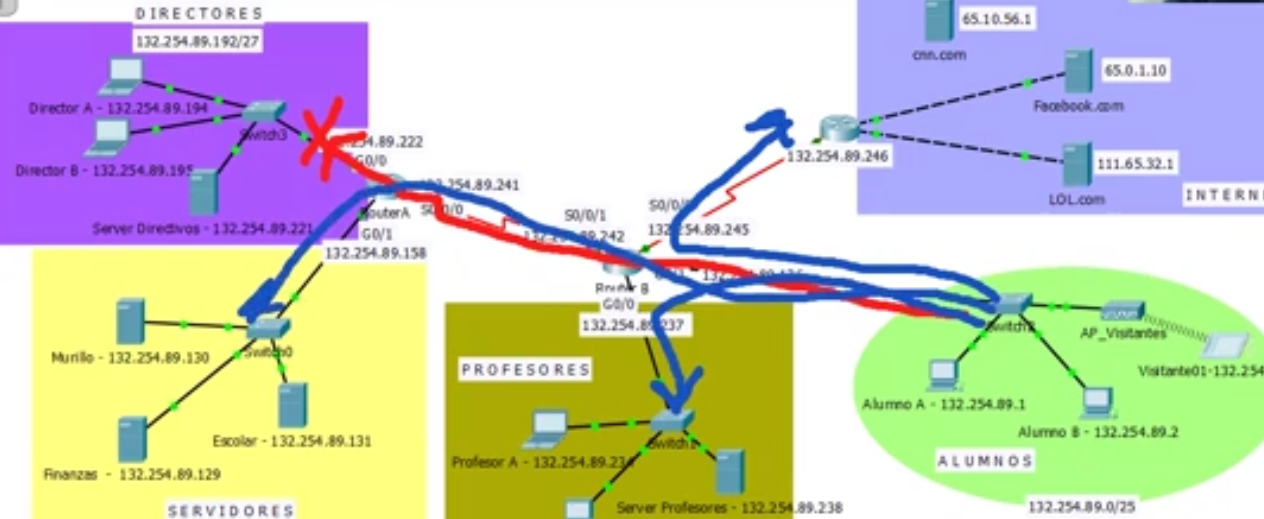
Mejores prácticas para el diseño de ACLs

1. Identificar el tráfico fuente o el origen (subred estudiantes)
2. Identificar en el diagrama gráficamente cual es la dirección hacia el destino. Trazar el flujo del tráfico no permitido.
3. Identificar el tráfico que está permitido.
4. Identificar el router en dónde se instalará la ACL. La lista de control de acceso se instala lo más lejano a la fuente o lo más cercano al destino. EN este caso es el router A.
5. Identificar la interfaz apropiada a bloquear. En este caso la interfaz g0/0 que es la interfaz del router A.
6. Una vez diseñada la ACL se asigna a una interfaz
7. Realizar pruebas de conectividad antes y después es una buena práctica.





Tráfico permitido en azul, tráfico no permitido está en rojo.



Todo el resto del tráfico en el router A está permitido:



Listas de control de acceso estándar bloquean todo el tipo tráfico (red donde esta el ping y la capa 4 tcp /ip donde está web).

Capa 4 es superior a la capa 3, ya no es necesario hacer ping si accedo por web.

**Desactivar una lista de acceso:**

**No ip Access-group 10 out**

Este comando no quita el deny any

no access **access-list 30 deny any**

**La ejecución de comandos va de arriba hacia abajo y el default any ya está implícito.**

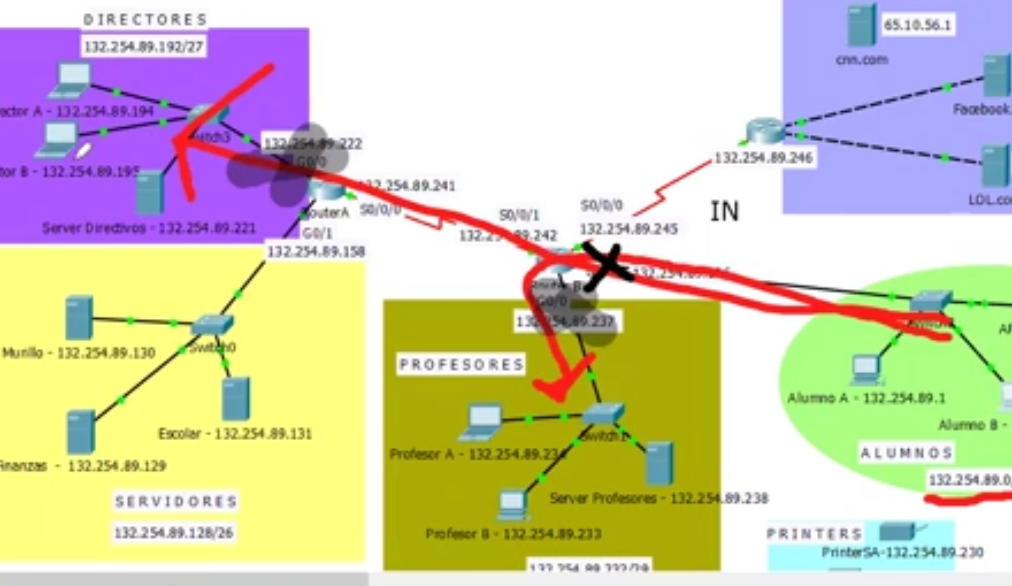
Listas de control de acceso extendidas

Las listas de control de acceso estándar se colocan lo más lejos al origen y las extendidas lo más cerca al origen.

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**.

Hay 2 alternativas

1. Pongo la lista de control de acceso en el router B, para bloquear la entrada al router del tráfico que vaya a directores y profesores. **(lista de control de acceso extendida lo más cerca al origen)**
2. Otra alternativa es colocar la lista de control de acceso de salida en el router b interface gigabit para que no llegue a la subred de profesores y en el router a de salida a la subred de directores en el interface g0/0. **(lista de control de acceso estándar lo más lejos del origen)**



Lista de acceso estandar



Router A y B

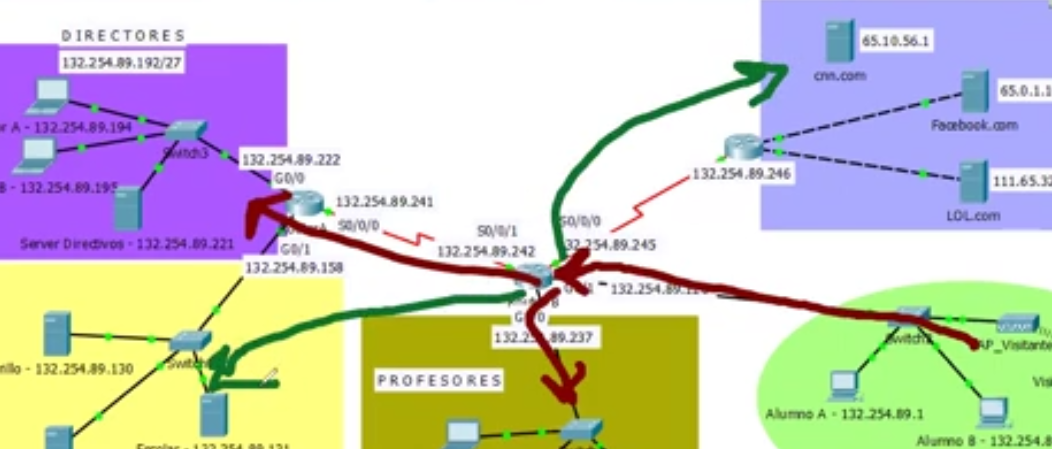
access-list 10 deny 132.254.89.0 0.0.0.127

access-list 10 permit any

int g0/0

ip access-group 10 out

Lista de acceso extendida



Ping ip

Respuesta Destination host unreachable, quiere decir que el router (no necesariamente el más cercano) no tiene ruta para poder llegar a ese destino.