Configuración de ACLs con Packet Tracer

¿QUÉ ES UNA ACL?

Una **lista de control de acceso** o ACL (del inglés, access control list) es un concepto de **seguridad informática** usado para fomentar la **separación de privilegios**. Es una forma de determinar los **permisos de acceso** apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

Las ACL permiten controlar el flujo del tráfico en equipos de **redes**, tales como **enrutadores** y **conmutadores**. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición. Sin embargo, también tienen usos adicionales, como, por ejemplo, distinguir "tráfico interesante" (tráfico suficientemente importante como para activar o mantener una conexión) en **RDSI**.

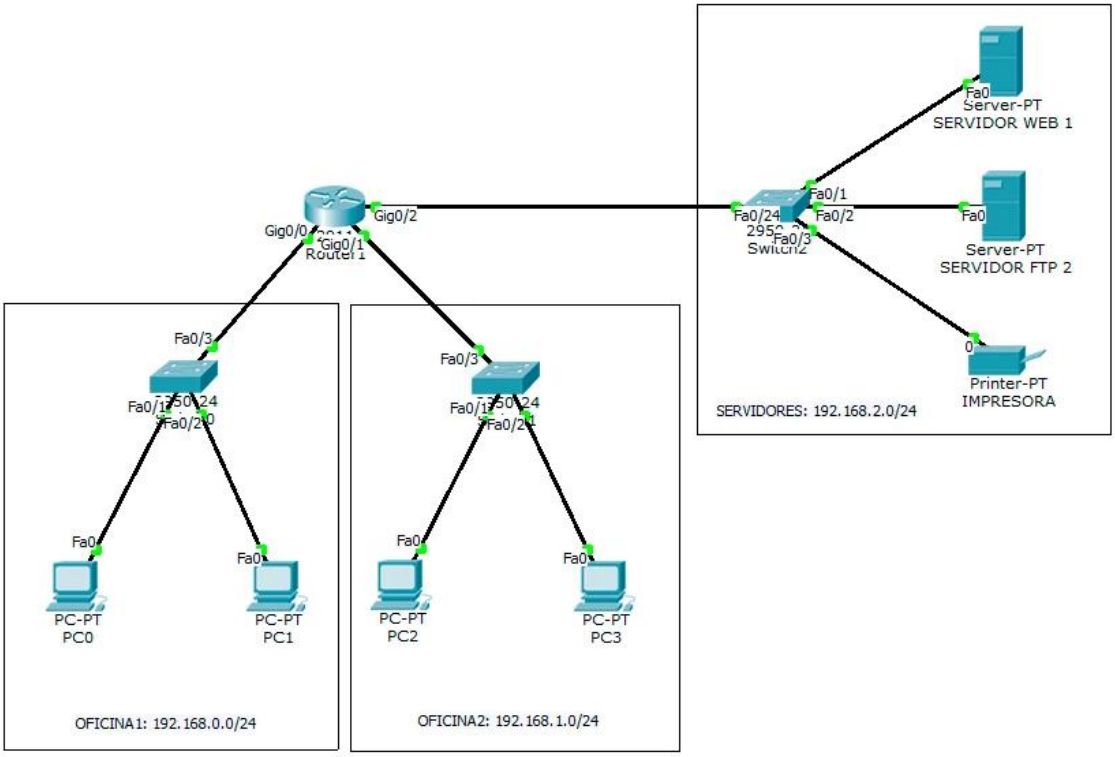
El motivo por el que suele gestionarse en una clase o sistema separado y no en cada una de las partes que pretenden asociarse a permisos es por seguir las reglas SOLID, en este caso la S (Principio de responsabilidad única), lo cual te permite incluso escalar mejor. Se asemejaría a un sistema de control de accesos físico típico de un edificio, donde esa parte está centralizada en un lugar. Este lugar solo necesita saber dos cosas: Quien eres (por ejemplo un ID de una tarjeta, tu id de usuario) y que quieres hacer. El te responde si tienes permiso de hacerlo o no. Con este enfoque este mismo sistema no solo puede ser utilizado para acceder a lugares si no para cualquier cosa que necesite separarse de personas que pueden y no pueden hacer cosas, por ejemplo: acceder a una página o sección, publicar un comentario, hacer una amistad, enviar un correo, ... En **redes informáticas**, ACL se refiere a una lista de reglas que detallan puertos de servicio o nombres de **dominios** (de redes) que están disponibles en un terminal u otro dispositivo de **capa de red**, cada uno de ellos con una lista de terminales y/o redes que tienen permiso para usar el servicio. Tanto **servidores** individuales como **enrutadores** pueden tener ACL de redes. Las listas de control de acceso pueden configurarse generalmente para controlar tráfico entrante y saliente y en este contexto son similares a un **cortafuegos**.

Existen dos tipos de listas de control de acceso: listas fijas y listas variables.

2.- ESQUEMA DE RED

El esquema de la red que queremos emular, es el que se ve en la imagen siguiente. Tenemos **2 oficinas** o aulas con N equipos conectados en cada una de ellas (en este caso hay 2 equipos en cada oficina). **En cada oficina hay un switch**, y cada switch se conecta a un **router central**. Por último, tenemos una **zona llamada servidores** donde hay 3 servidores diferentes (servidor web, servidor ftp y una impresora):

El esquema de red es el siguiente:



Esquema de red

El **direccionamiento de red** de cada uno de los equipos es el siguiente (entiendo que es tan sencillo configurar las direcciones IPs que no es necesario explicarlo):

ZONA	EQUIPO	IP	MÁSCARA DE RED	PUERTA DE ENLACE
Oficina1	PC0	192.168.0.2	255.255.255.0	192.168.0.1
Oficina1	PC1	192.168.0.3	255.255.255.0	192.168.0.1
Oficina1	Switch0	-----	-----	-----
Oficina2	PC2	192.168.1.2	255.255.255.0	192.168.1.1
Oficina2	PC3	192.168.1.3	255.255.255.0	192.168.1.1
Oficina2	Switch1	-----	-----	-----
Servidores	Servidor Web	192.168.2.2	255.255.255.0	192.168.2.1
Servidores	FTP	192.168.2.3	255.255.255.0	192.168.2.1
Servidores	Impresora	192.168.2.4	255.255.255.0	192.168.2.1
		192.168.0.1	255.255.255.0	
-----	Router0	192.168.1.1	255.255.255.0	-----
		192.168.2.1	255.255.255.0	

Direccionamiento de red

3.- ACLs

Aunque existen millones de opciones en función de los equipos y servicios que queremos gestionar dentro de una red, en este ejemplo lo que queremos hacer es aprender a usar las ACLs y como es su funcionamiento. Para ello, se van a crear una serie de reglas de acceso que permitirán el acceso entre una zona origen y una zona destino según la siguiente tabla:

ZONA ORIGEN	EQUIPO ORIGEN	ZONA DESTINO	EQUIPO DESTINO	SERVICIO O PROTOCOLO
Oficina1	PC0 y PC1	Servidores	Server Web 1	80 TCP
Oficina1	PC0 y PC1	Servidores	FTP 2	20 y 21 TCP
Oficina2	PC2	Servidores	FTP 2	20 y 21 TCP
Oficina2	PC2	Servidores	Impresora	631 TCP
Oficina2	PC3	Servidores	FTP 2	20 y 21 TCP

Todo **el tráfico que no coincida** con las reglas creadas, **será denegado**.

4.- SWITCHES

En este ejemplo, **los switches no necesitan ninguna configuración especial**, como por ejemplo la creación de VLANs (aunque se podría hacer). Nuestro objetivo es explicar y comprender el funcionamiento y configuración de las ACLs y por tanto, no complicar el ejemplo. Los switches solamente se usarán para **conectar los diferentes elementos** y no le aplicaremos **ninguna configuración especial**.

5.- ROUTER

En Cisco Packet Tracer, las listas de acceso se dividen en dos tipos: **standard** y **extended**. Las **listas de acceso standard**, son muy sencillas y solo permiten filtrar tráfico desde una ip concreta a un destino

concreto. Las **listas de acceso extendidas**, permiten un control mas potente de las reglas como tipo de protocolos, rango de puertos, etc etc ... En este tutorial **usaremos las listas extendidas**. Las ACLs standard van desde el número 1 al 99 y las listas de acceso extendidas del 100 al 199.

Tipos de ACLs:

```
<1-99> IP standard access list
<100-199> IP extended access list
```

Con los siguientes comandos crearemos la **ACL-101** en la cual especificaremos que queremos permitir al acceso al FTP, y Servidor WEB desde cualquier equipo de la Oficina1. Debemos especificar en que interfaz queremos aplicar la lista de control de acceso, en este ejemplo la interfaz que conecta con el swicth0. **Todo lo demás será denegado**:

ACL-101:

```
Router>en
Router#conf t
Router(config)# access-list 101 permit tcp any host 192.168.2.3 eq 20
Router(config)# access-list 101 permit tcp any host 192.168.2.3 eq 21
Router(config)# access-list 101 permit tcp any host 192.168.2.2 eq 80
Router(config)# access-list 101 deny ip any any
Router(config)# int GigabitEthernet0/0
Router(config-if)# ip access-group 101 in
```

Con los siguientes comandos crearemos la **ACL-102** en la cual especificaremos que queremos permitir al acceso al FTP desde el PC2 y PC3 y acceso a la impresora únicamente desde el PC2. **Todo lo demás será denegado** y la interfaz donde aplicar la regla es GigabitEthernet0/1:

ACL-102:

```
Router>en
Router#conf t
Router(config)# access-list 102 permit tcp 192.168.1.2 0.0.0.255 host 192.168.2.3 range 20 21
Router(config)# access-list 102 permit tcp 192.168.1.2 0.0.0.255 host 192.168.2.4 eq 631
Router(config)# access-list 102 permit tcp 192.168.1.3 0.0.0.255 host 192.168.2.3 range 20 21
Router(config)# access-list 102 deny ip any any
Router(config)# int GigabitEthernet0/1
Router(config-if)# ip access-group 102 in
```

Una vez que tenemos creadas las ACLs, podremos ver con el siguiente comando (**show access-list**) el resumen de cada una de ellas:

Lista de ACLs:

```
Router#show access-lists
Extended IP access list 101
 permit tcp any host 192.168.2.3 eq 20
 permit tcp any host 192.168.2.3 eq ftp
 permit tcp any host 192.168.2.2 eq www
 deny ip any any
Extended IP access list 102
 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.3 range 20 ftp
 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.4 eq 631
 deny ip any any
```

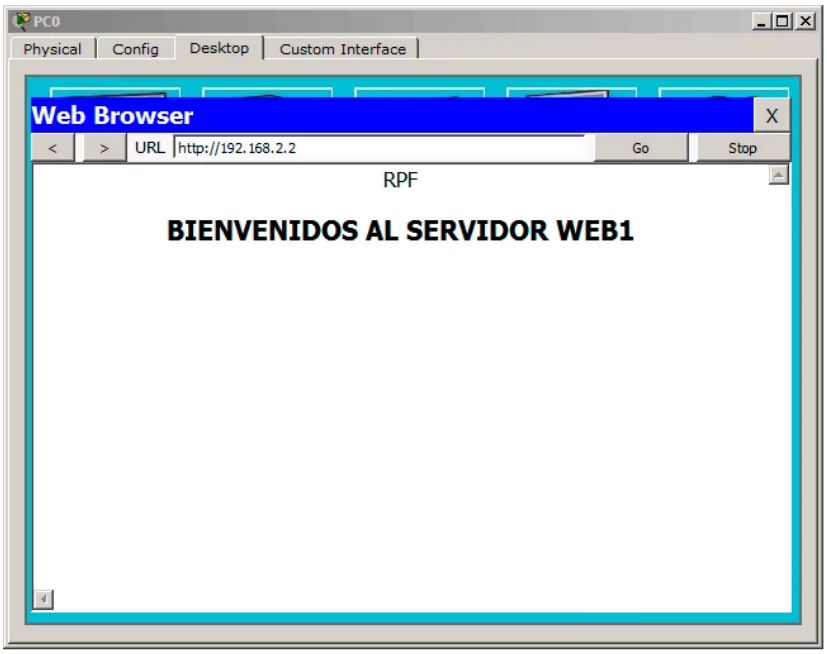
Si lo que queremos es borrar las listas de acceso, usaremos el siguiente comando para cada una de ellas: **no access-list <número>**:

Borrar ACLs:

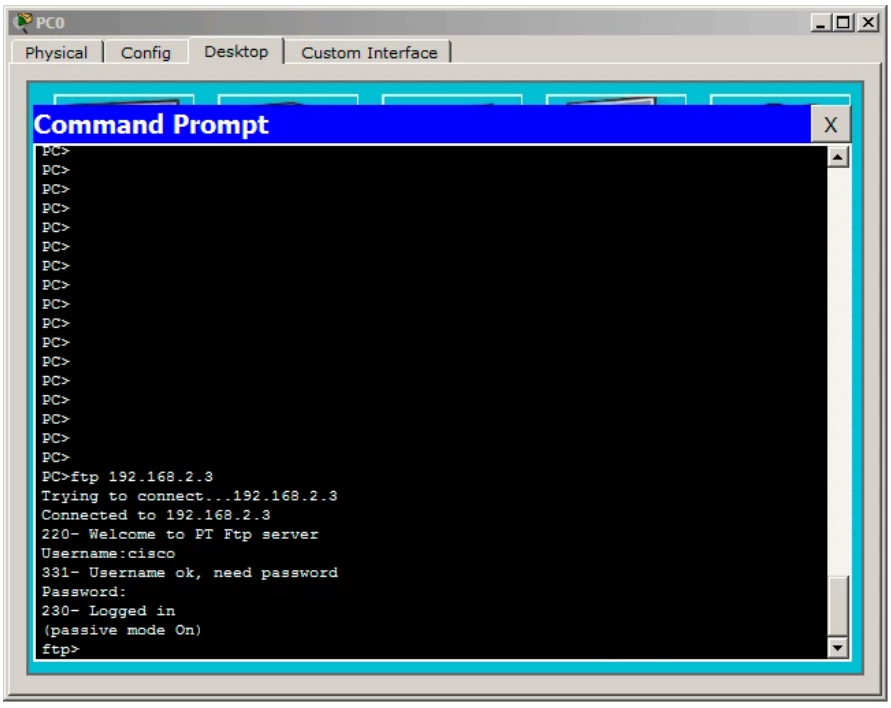
```
Router>
Router>en
Router#conf t
Router(config)#no access-list 101
Router(config)#no access-list 102
```

6.- PROBAR LAS ACLS

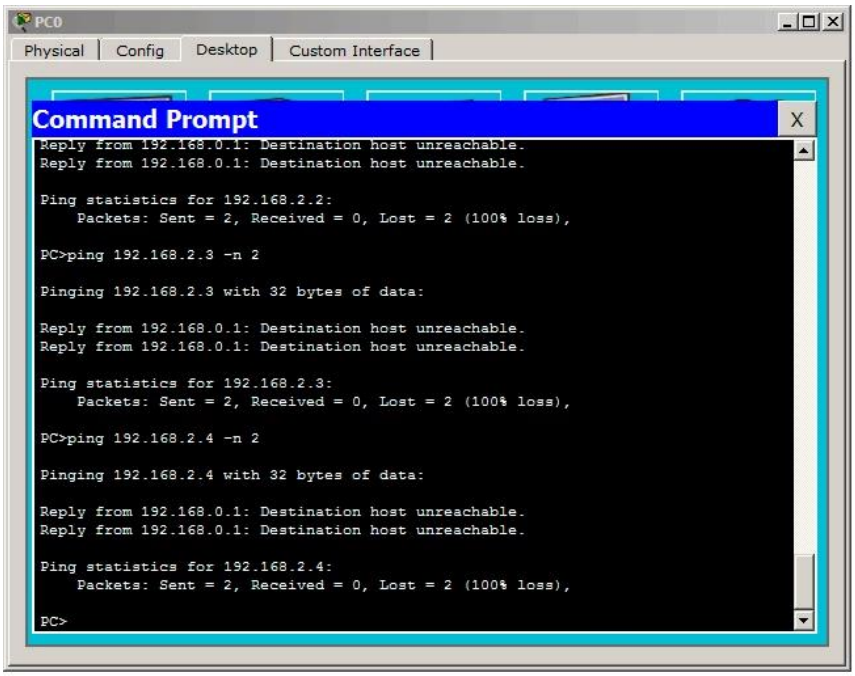
Ahora es el momento de probar las ACLs creadas y comprobar si están creadas correctamente y funcional tal y como queremos. En este ejemplo **no se van a detallar el 100% de las pruebas** (ya que son bastantes y se hacen todas de la misma forma), por tanto, se realizarán solamente las pruebas básicas.



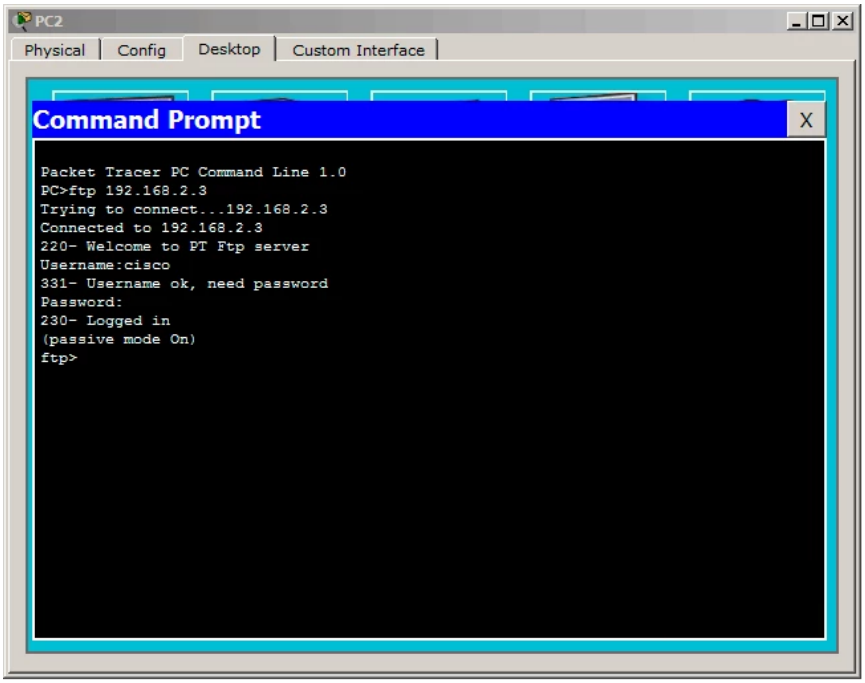
Acceso desde PC0 al servidor web



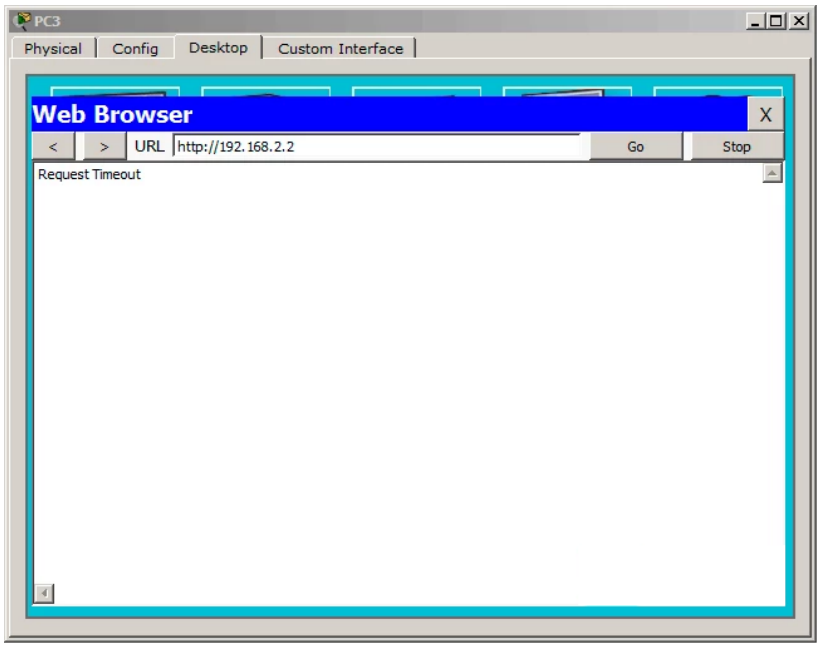
Acceso desde PC0 al FTP



Acceso desde PC0 denegado a todo lo demás



Acceso desde PC2 al FTP



Acceso desde PC3 al servidor web denegado