LISTAS DE CONTROL DE ACCESO

1. Introducción

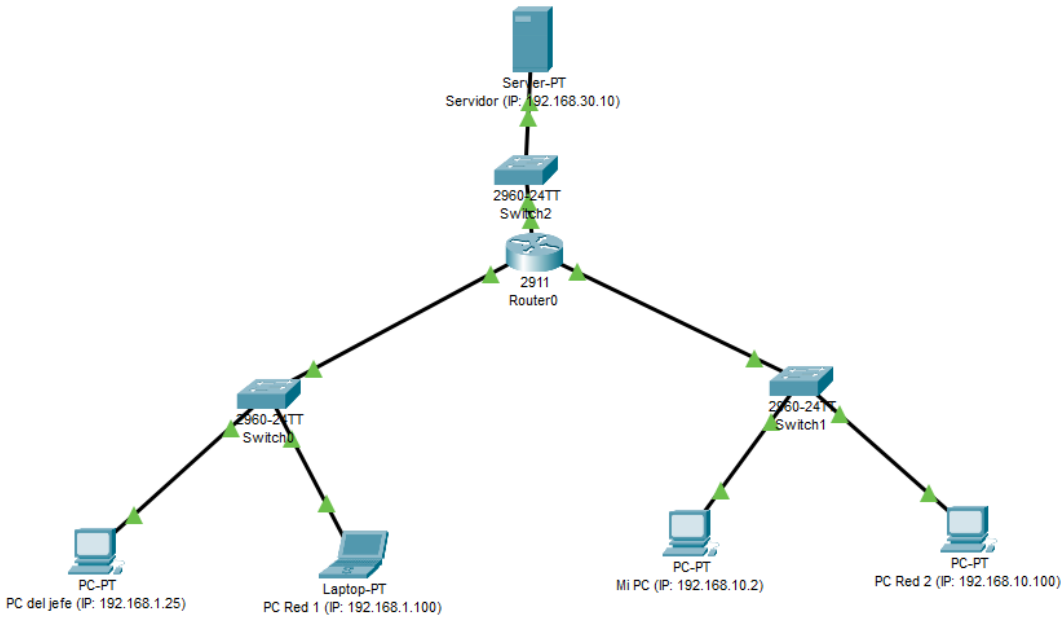
En esta actividad me he puesto en el papel de técnico de sistemas en una empresa de publicidad, encargado de administrar y proteger la red de la empresa. Mi jefe me pidió que configurara el acceso a una de nuestras redes internas, concretamente a la red 192.168.30.0/24, de forma que solo su ordenador y el mío pudieran conectarse a ella, bloqueando a cualquier otro dispositivo.

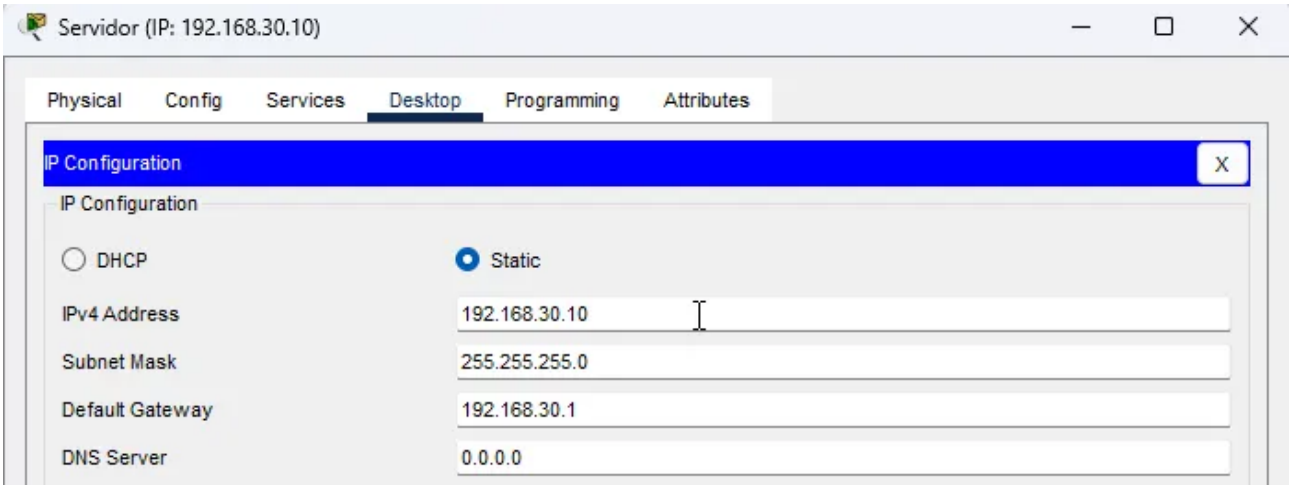
Para cumplir con este encargo, he diseñado una pequeña red utilizando diferentes dispositivos (router, switches, PCs y servidor), asignando las direcciones IP correspondientes a cada uno, y aplicando una lista de control de acceso (ACL) que me permitiera filtrar el tráfico según lo solicitado. Además, también he detallado el procedimiento para conectarme al router a través del puerto de consola, ya que es el primer paso necesario para poder configurar el equipo desde cero.

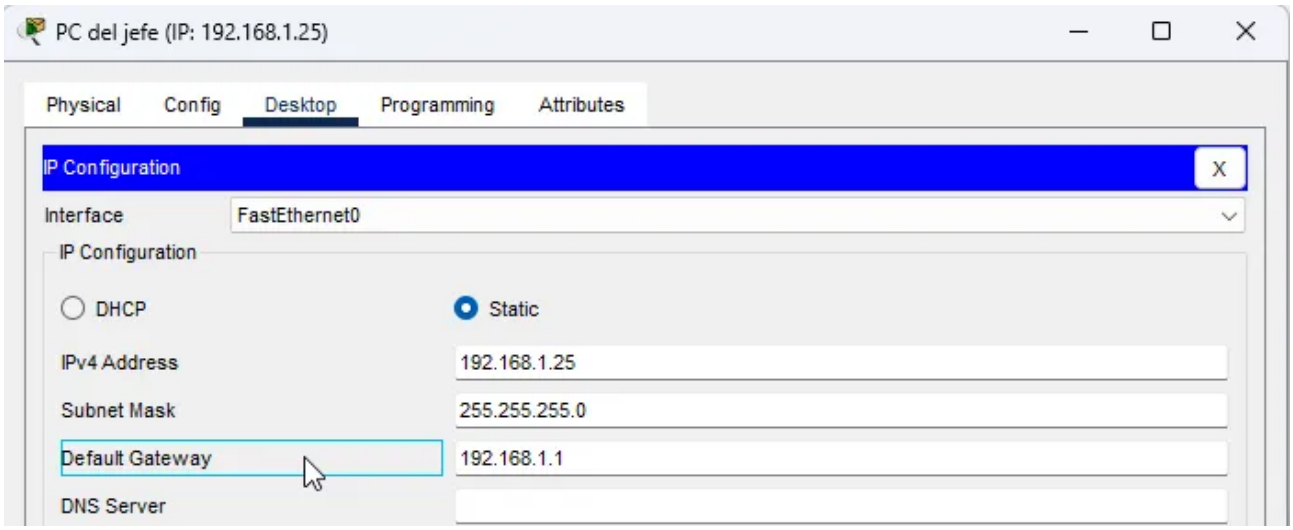
Durante el desarrollo de la actividad, no solo he realizado la configuración, sino que también he explicado por qué he elegido una ACL extendida en lugar de una estándar, he mostrado los modos de operación del router por los que he ido pasando durante la configuración, y he hecho pruebas para asegurarme de que todo funcionara correctamente.

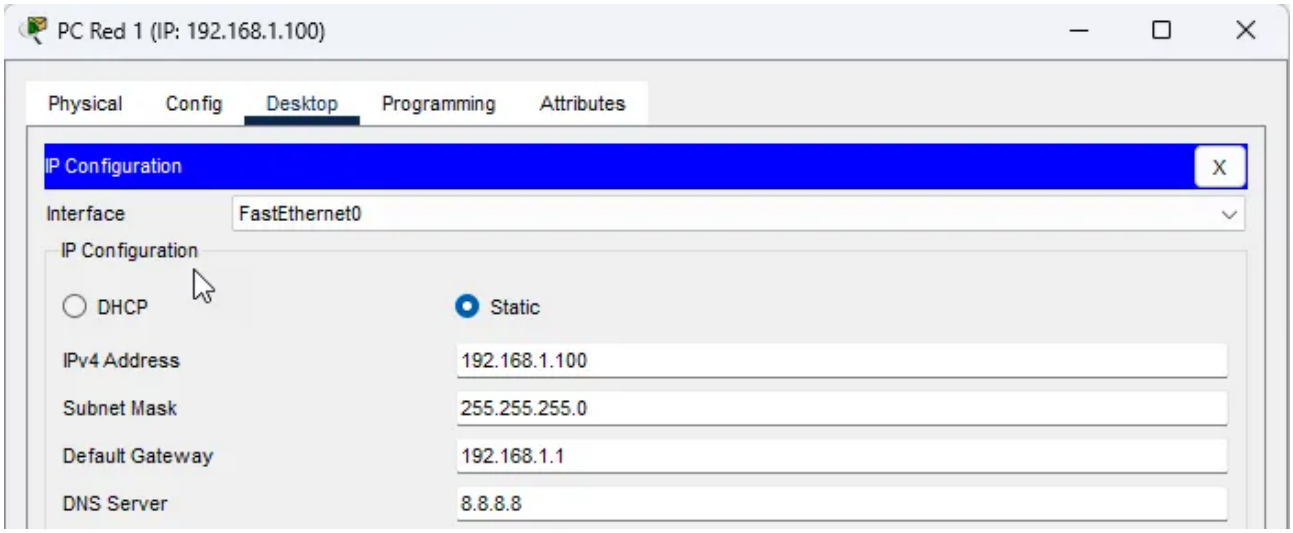
El objetivo de este trabajo ha sido no solo configurar la red correctamente, sino también entender mejor cómo controlar los accesos a través de ACLs y cómo trabajar de manera organizada a la hora de administrar dispositivos de red.

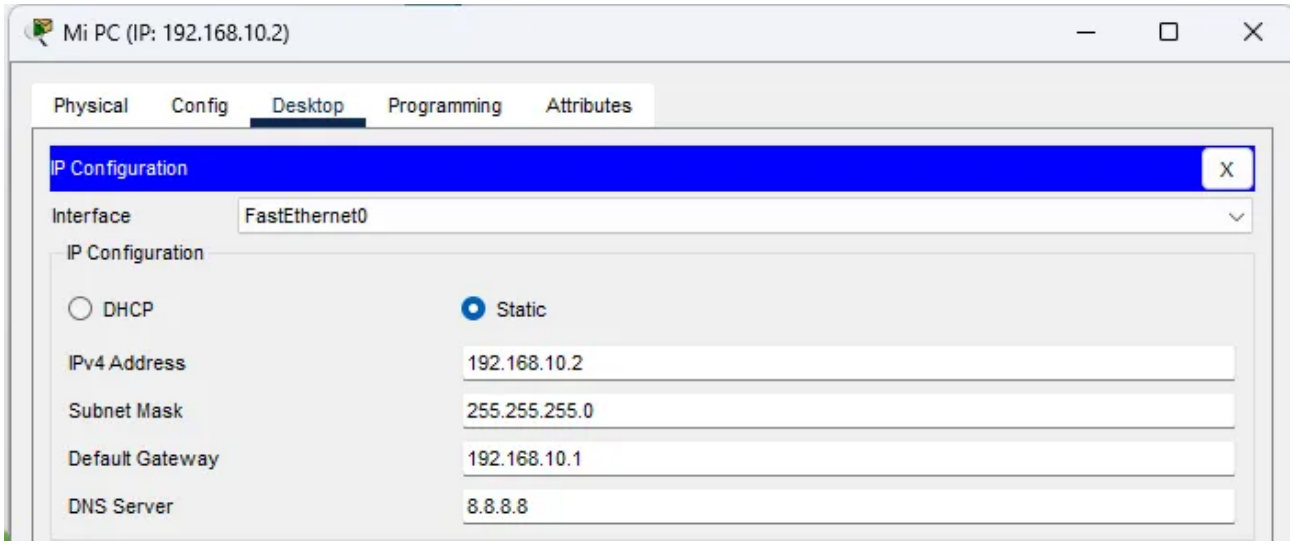
2. Topología de Red

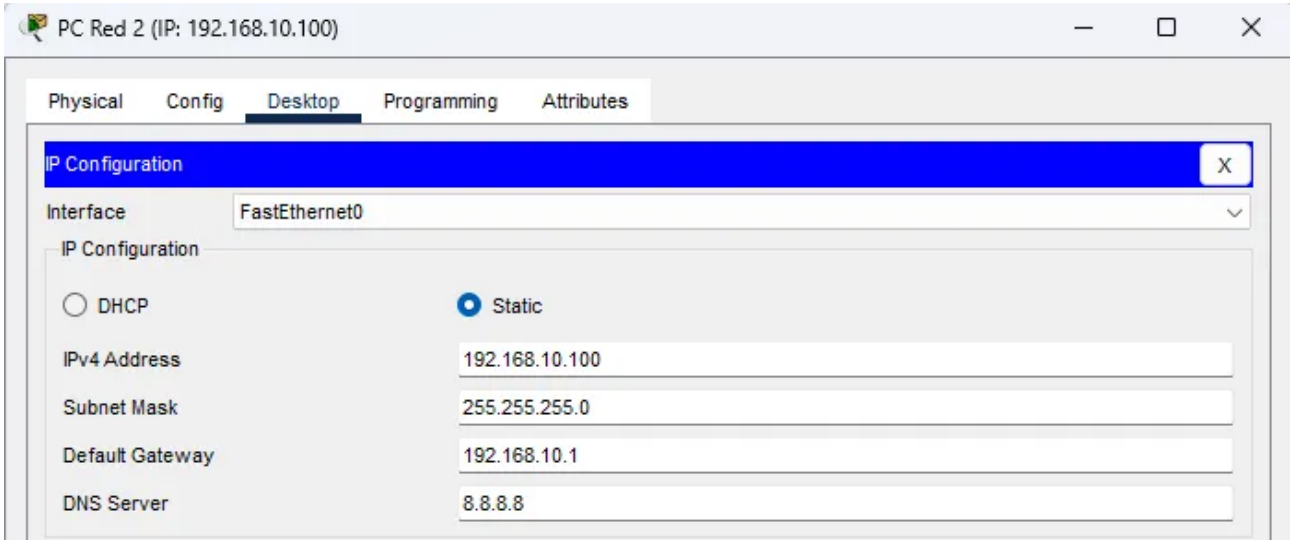



Servidor (IP: 192.168.30.10)
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
192.168.30.10
Subnet Mask
255.255.255.0
Default Gateway
192.168.30.1
DNS Server
0.0.0.0


PC del jefe (IP: 192.168.1.25)
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.25
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server


PC Red 1 (IP: 192.168.1.100)
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.100
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
8.8.8.8





2.2. Cuadro de Diseño de la Red

Dispositivo	Dirección IP	Máscara de Subred	Gateway	Red	Observación
Router - G0/0	192.168.1.1	255.255.255.0	-	192.168.1.0/24	Interfaz hacia Switch1
Router - G0/1	192.168.10.1	255.255.255.0	-	192.168.10.0/24	Interfaz hacia Switch2
Router - G0/2	192.168.30.1	255.255.255.0	-	192.168.30.0/24	Interfaz hacia el servidor
PC del jefe	192.168.1.25	255.255.255.0	192.168.1.1	192.168.1.0/24	Acceso permitido
PC red 1	192.168.1.100	255.255.255.0	192.168.1.1	192.168.1.0/24	Acceso denegado
Mi PC	192.168.10.2	255.255.255.0	192.168.10.1	192.168.10.0/24	Acceso permitido
PC red 2	192.168.10.100	255.255.255.0	192.168.10.1	192.168.10.0/24	Acceso denegado
Servidor	192.168.30.100	255.255.255.0	192.168.30.1	192.168.30.0/24	Destino protegido

3. Conexión al router mediante consola

Para poder configurar el router desde cero, lo primero que hice fue conectarme a él a través de la consola. A continuación, explico paso a paso cómo realicé esta conexión, especificando qué cable usé, qué puertos están implicados y para qué sirve cada uno.

3.1. Selección del cable adecuado

Lo primero que hice fue elegir el cable correcto para poder conectarme al router. Utilicé un **cable de consola**, también conocido como **cable rollover**. Este cable suele tener un conector RJ-45 en un extremo (que va al router) y un conector RS-232 o incluso USB en el otro, dependiendo del tipo de PC o adaptador que estemos usando. En Cisco Packet Tracer, es fácil de identificar porque aparece como un cable azul claro.

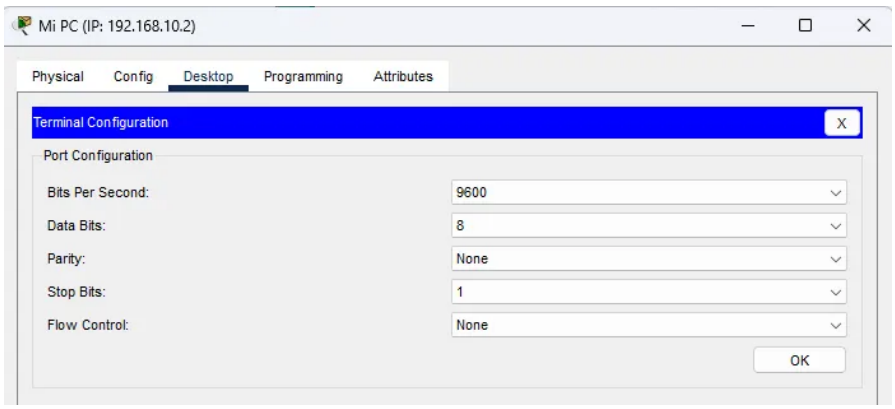
3.2. Conexión de los puertos

Después, conecté un extremo del cable al **puerto Console** del router, que es un puerto que viene pensado específicamente para configuraciones iniciales o para casos de recuperación. El otro extremo lo conecté al **puerto RS-232** de mi PC, que en Packet Tracer aparece también como "Con" o "Console". De esta manera creé una conexión directa entre mi ordenador y el router, sin necesidad de que el router estuviera configurado previamente en red.

3.3. Acceso a la consola desde el PC

Una vez conectado el cable, abrí el **PC que usé para la configuración** y seguí estos pasos:

1. Fui a la pestaña **"Desktop"**.
2. Hice clic en **"Terminal"**.
3. Se abrió una ventana para configurar la conexión por puerto serie. Dejé la configuración predeterminada (9600 baudios, 8 bits de datos, sin paridad, 1 bit de parada, sin control de flujo).
4. Pulsé en **"OK"** y accedí directamente al **modo usuario del router** (Router>), desde donde ya pude empezar con la configuración.



¿Por qué esta conexión es importante?

Conectarse al router por consola es esencial cuando el equipo todavía no tiene ninguna configuración de red, o si se ha perdido la conectividad y necesitamos recuperarlo. Es el método más seguro para acceder directamente al dispositivo y poder configurarlo desde cero, sin depender de que el router esté funcionando en la red.
En definitiva, es la forma básica y fiable de tener acceso total al router cuando más lo necesitamos.

4. Justificación del tipo de ACL que debo crear:

Para cumplir con el objetivo que me plantea mi jefe —que solo su ordenador y el mío puedan acceder al servidor en la red 192.168.30.0/24—, **he decidido utilizar una ACL extendida**.

¿Por qué una ACL extendida y no una estándar?

Porque **las ACL estándar solo filtran tráfico basándose en la dirección IP de origen**, es decir, no permiten distinguir a qué destino se está intentando acceder ni qué tipo de tráfico se está utilizando. En este caso, eso no sería suficiente, ya que quiero permitir a ciertos equipos (los nuestros) acceder **únicamente** a la red del servidor (192.168.30.0/24), **pero no a otras redes**, ni quiero que otros equipos accedan a esta red. Si usara una ACL estándar, al aplicarla en una interfaz, podría limitar la entrada o salida por IP, pero **no tendría control sobre el destino**, y eso podría bloquear tráfico útil o permitir tráfico no deseado.

En cambio, con una **ACL extendida**, puedo especificar:

- **Qué equipos (IP origen)** tienen permitido o denegado el acceso.
- **A qué red o dispositivo (IP destino)** se dirigen.
- **Qué protocolo o puerto** están utilizando (por ejemplo, TCP, ICMP, HTTP, etc.).

Esto me da el control que necesito para **permitir únicamente el acceso desde mi PC (192.168.10.2) y el del jefe (192.168.1.25) hacia el servidor (192.168.30.10)**, y al mismo tiempo denegar ese acceso a cualquier otro equipo.

En resumen:

- **Tipo de ACL elegida**: **ACL extendida**.
- **Razón**: Me permite filtrar tráfico no solo por IP origen, sino también por IP destino y protocolos, lo cual es imprescindible para cumplir con el requisito de seguridad de este escenario.
- **Beneficio adicional**: Mayor control y precisión en la política de acceso, evitando que se bloquee o permita más tráfico del necesario.

5. Comandos de configuración y explicación paso a paso:

Una vez que ya tengo configuradas las interfaces del router y cada equipo en su red correspondiente, ahora paso a aplicar una **ACL extendida** que cumpla con el requisito de mi jefe:

que **solo su PC (192.168.1.25) y el mío (192.168.10.2)** puedan acceder al servidor en la red 192.168.30.0/24, en este caso al servidor con IP 192.168.30.10.

Paso 1: Crear la ACL extendida

Primero, accedo al router y entro al modo de configuración global:

Router> enable

Router# configure terminal

Ahora creo la ACL extendida, por ejemplo con el número **100** (por convención, las ACLs extendidas van del 100 al 199):

Router(config)# access-list 100 permit ip host 192.168.1.25 host 192.168.30.10

Router(config)# access-list 100 permit ip host 192.168.10.2 host 192.168.30.10

Router(config)# access-list 100 deny ip any 192.168.30.0 0.0.0.255

Router(config)# access-list 100 permit ip any any

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 100 permit ip host 192.168.1.25 host 192.168.30.10
Router(config)#access-list 100 permit ip host 192.168.10.2 host 192.168.30.10
Router(config)#access-list 100 deny ip any 192.168.30.0 0.0.0.255
Router(config)#access-list 100 permit ip any any
Router(config)#
```

¿Qué hace cada línea?

1. access-list 100 permit ip host 192.168.1.25 host 192.168.30.10:
   Permite que el **PC del jefe** acceda al servidor.
   Uso host para que coincida exactamente con esa dirección IP.
2. access-list 100 permit ip host 192.168.10.2 host 192.168.30.10:
   Permite que **mi PC** acceda al mismo servidor.
3. access-list 100 deny ip any 192.168.30.0 0.0.0.255:
   Deniega el acceso al resto de dispositivos que intenten comunicarse con la red del servidor.
   Esta línea se encarga de cumplir la política de seguridad que se me ha solicitado.
4. access-list 100 permit ip any any:
   Esta línea es muy importante. Si no la pongo, la ACL terminaría con un "deny all" implícito que **bloquearía el resto del tráfico**, incluso entre otras redes.
   Con esta línea, me aseguro de que todo lo que **no va al servidor** pueda seguir funcionando con normalidad.

Paso 2: Aplicar la ACL en la interfaz correcta

La ACL la aplico en la interfaz de **entrada** del tráfico que llega desde las otras redes al router. En este caso, las redes origen son la 192.168.1.0/24 y la 192.168.10.0/24, así que debo aplicar la ACL en las interfaces de entrada **GigabitEthernet0/0 y GigabitEthernet0/1**:

Router(config)# interface GigabitEthernet0/0

Router(config-if)# ip access-group 100 in

Router(config-if)# exit

Router(config)# interface GigabitEthernet0/1

Router(config-if)# ip access-group 100 in

Router(config-if)# exit

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip access-group 100 in
Router(config-if)#exit
Router(config)#
```

¿Cómo contribuyen estos comandos?

Con esta configuración, **garantizo que solo los dos ordenadores autorizados pueden acceder al servidor**, cumpliendo con la solicitud de mi jefe. El resto del tráfico sigue funcionando normalmente, lo cual es muy importante en un entorno empresarial, donde no podemos arriesgar interrumpir servicios innecesariamente.

Además, al usar una ACL extendida y especificar tanto IP de origen como de destino, logro **precisión y seguridad** en el control de accesos, sin afectar al resto de la red.

6. Modos de trabajo del router

Durante la configuración del router para aplicar la ACL y establecer la conectividad entre las distintas redes, pasé por **varios modos de trabajo del router**, cada uno con su propósito específico. Aquí detallo cada uno de ellos, cómo accedí y qué configuraciones realicé en cada momento:

6.1. Modo usuario (User EXEC mode)

Cuando accedí al router por consola (a través del Terminal del PC conectado al puerto Console), lo primero que vi fue un mensaje como este:

Router>

Esto indica que estoy en el **modo usuario**. En este modo se pueden ejecutar comandos muy básicos de visualización, como ping o show, pero **no se puede hacer ninguna configuración**. Es un modo pensado para usuarios sin privilegios administrativos.

6.2. Modo privilegiado (Privileged EXEC mode)

Desde el modo usuario, escribí el comando:

```
enable
```

Y el prompt cambió de:

```
Router>
```

a:

```
Router#
```

Esto significa que entré al **modo privilegiado**, donde ya puedo acceder a configuraciones más avanzadas y ejecutar comandos como show running-config, copy running-config startup-config, etc.

Este modo es el punto de partida para realizar cambios reales en el sistema, pero **aún no me permite configurar interfaces, ACLs o IPs**.

6.3. Modo de configuración global (Global Configuration mode)

Desde el modo privilegiado, escribí:

```
configure terminal
```

Y el prompt cambió a:

```
Router(config)#
```

Aquí ya estoy en el **modo de configuración global**, que es el entorno donde puedo empezar a modificar la configuración del router: interfaces, rutas, ACLs, nombres, etc.

En este modo es donde realicé la mayor parte del trabajo. Por ejemplo:

- Configuré las IPs en las interfaces del router (interface GigabitEthernet0/0, etc.).
- Creé y edité la ACL extendida (access-list 100 ...).
- Asigné la ACL a interfaces con ip access-group.

6.4. Modo de configuración de interfaz (Interface Configuration mode)

Dentro del modo global, cuando necesitaba configurar una interfaz específica, como por ejemplo para asignar IP o aplicar una ACL, entré al modo de configuración de interfaz con:

```
interface GigabitEthernet0/0
```

Y el prompt cambió a:

```
Router(config-if)#
```

En este modo configuré lo siguiente:

- La dirección IP de la interfaz.
- Activé la interfaz con no shutdown.

- Apliqué la ACL con el comando ip access-group 100 in.

Repetí esto para las demás interfaces que conectan con las otras redes (GigabitEthernet0/1, GigabitEthernet0/2).

¿Por qué es importante conocer los modos?

Identificar correctamente los modos de trabajo del router me permite tener **control y seguridad** sobre los cambios que estoy haciendo. Cada modo tiene un propósito específico y comandos permitidos. Cambiar entre ellos conscientemente es esencial para trabajar de forma profesional con dispositivos Cisco.

7. Pruebas realizadas para verificar el correcto funcionamiento de la configuración

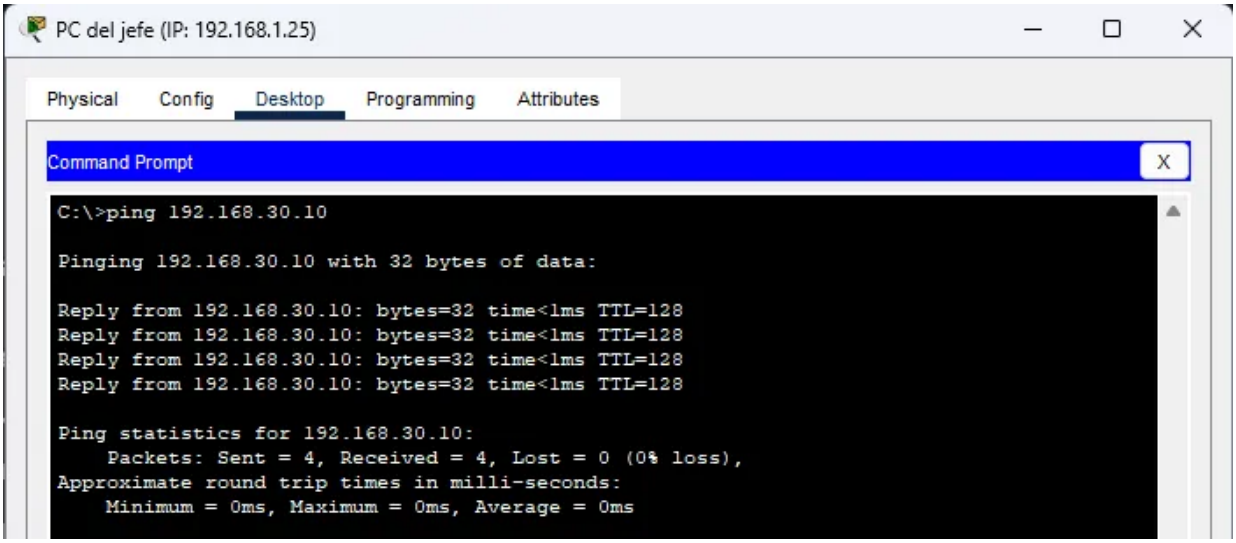
Una vez configurada toda la red y aplicada la ACL, realicé una serie de pruebas para asegurarme de que **todo funciona tal y como se pide en el enunciado**. Mi objetivo principal era comprobar que **solo el PC de mi jefe y el mío podían acceder a la red 192.168.30.0/24**, donde se encuentra el servidor, y que el resto de dispositivos quedaran bloqueados. Además, también quería verificar que **la comunicación entre el resto de las redes seguía funcionando sin problema**.

A continuación, detallo todas las pruebas que llevé a cabo, el motivo de cada una y los resultados esperados.

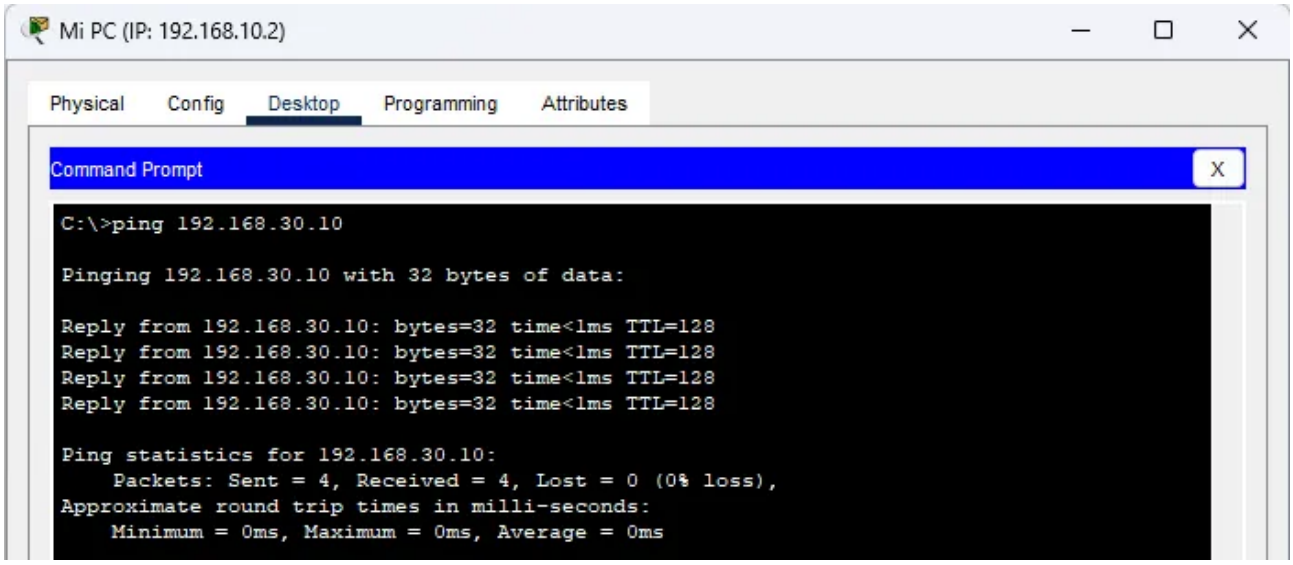
1. Acceso desde PCs autorizados (después de aplicar la ACL)

Después de aplicar la ACL, repetí los pings **desde los dos PCs que sí deberían tener acceso**:

- Desde el PC de mi jefe al servidor.



- Desde mi propio PC al servidor.

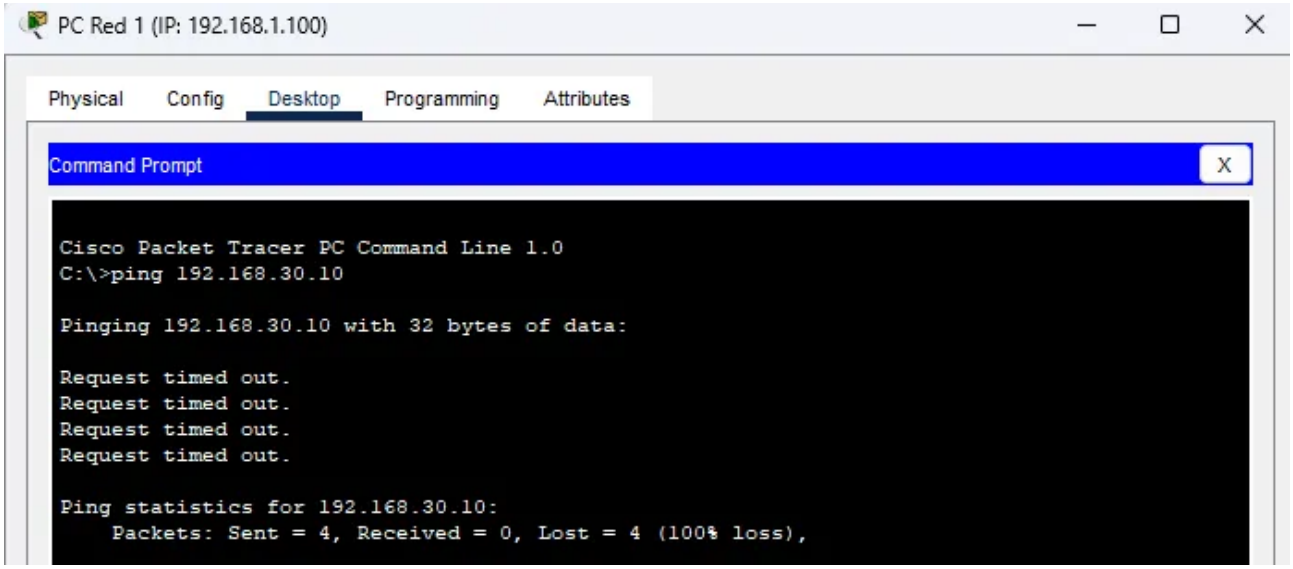


En ambos casos el ping funcionó, lo que demuestra que **la ACL está permitiendo correctamente el acceso a esos dos equipos concretos**.

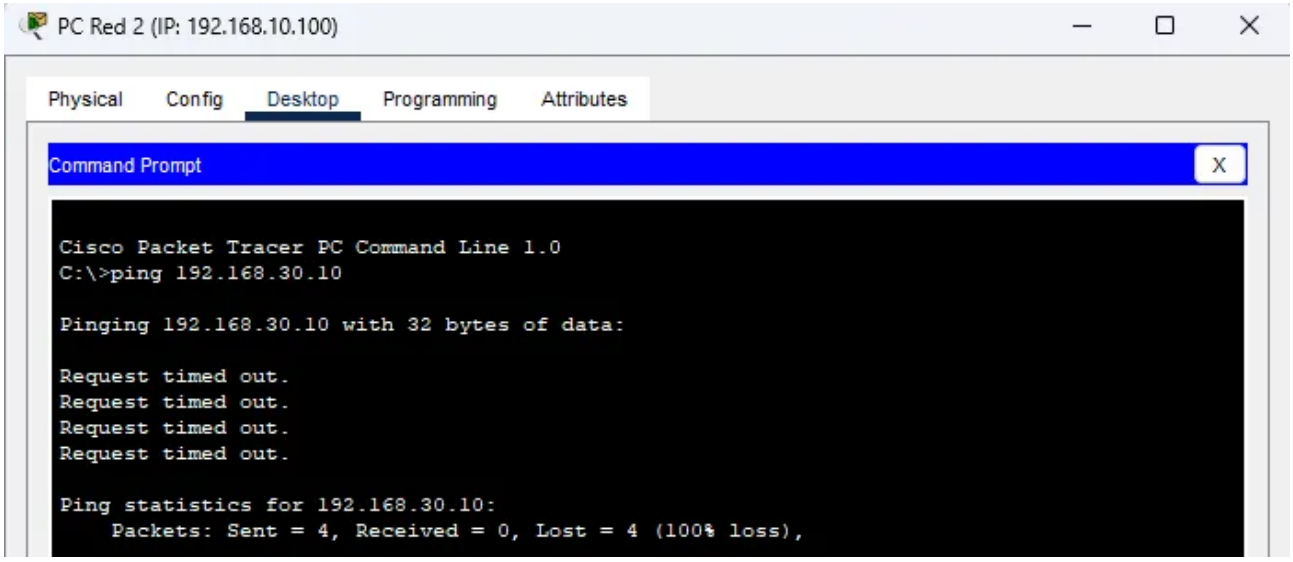
2. Bloqueo de acceso desde PCs no autorizados

Para asegurarme de que la ACL estaba funcionando correctamente, hice ping al servidor desde:

1. Otro PC de la red del jefe (192.168.1.100).



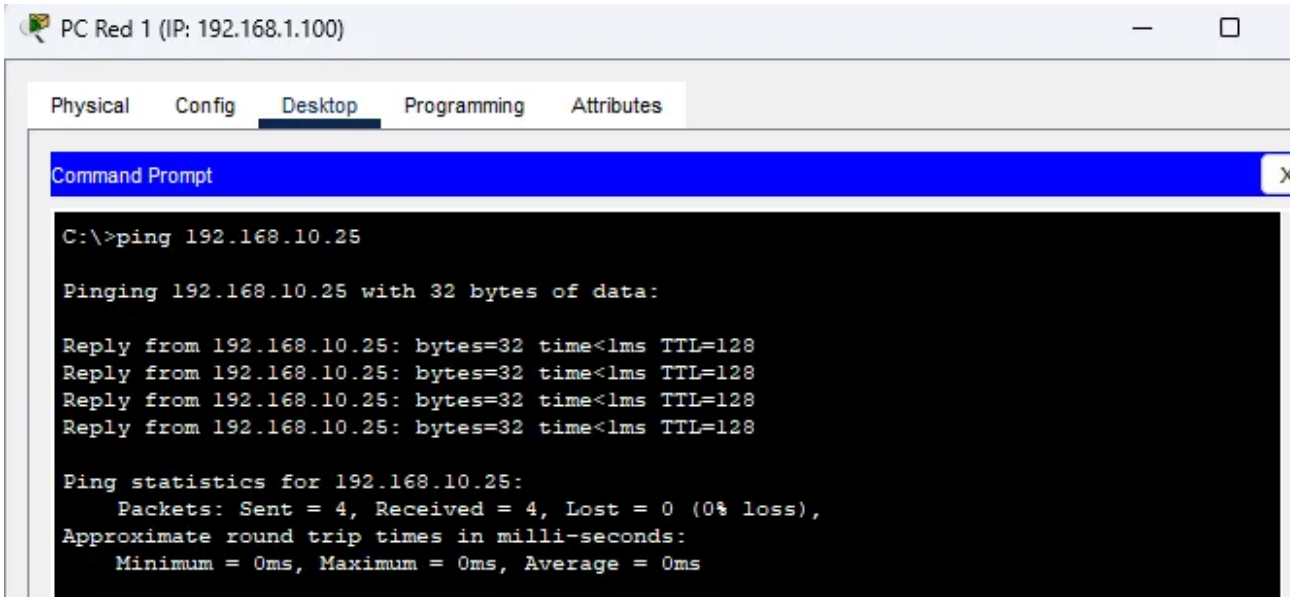
2. Otro PC de mi red (192.168.10.100).



En ambos casos, el ping falló, lo que es justo el comportamiento esperado: **la ACL está bloqueando el acceso a la red 192.168.30.0 desde cualquier IP que no sea la del jefe o la mía**.

3. Comunicación entre otras redes

También quise comprobar que la ACL **no estaba interfiriendo con el resto de la comunicación interna entre redes**, así que hice una prueba desde un PC de la red 1 (192.168.1.100) a otro PC de la red 10 (192.168.10.25).



El ping funcionó perfectamente. Esto me confirmó que la línea permit ip any any que añadí al final de la ACL está funcionando correctamente, permitiendo el tráfico que no afecta a la red del servidor.

---

4. Comprobación técnica desde el router

Por último, ejecuté el comando:

show access-lists

```
Router#show access-lists
Extended IP access list 100
    10 permit ip host 192.168.1.25 host 192.168.30.10
    20 permit ip host 192.168.10.2 host 192.168.30.10
    30 deny ip any 192.168.30.0 0.0.0.255
    40 permit ip any any
```

Esto me permitió ver que **la ACL estaba activa y que las líneas estaban recibiendo coincidencias (matches)**, lo que demuestra que el tráfico se está filtrando tal como he configurado.

📋 Resumen de resultados

Prueba	Resultado esperado
Ping desde el PC del jefe al servidor	✅ Éxito
Ping desde mi PC al servidor	✅ Éxito
Ping desde otros PCs al servidor	❌ Fallo (bloqueado por ACL)
Ping entre PCs de diferentes redes (no servidor)	✅ Éxito
Comprobación con show access-lists	✅ ACL activa y funcionando

Conclusión

Con estas pruebas pude demostrar que la configuración cumple perfectamente con los requisitos planteados: **solo los PCs autorizados pueden acceder a la red 192.168.30.0, mientras que el resto quedan correctamente bloqueados**, y al mismo tiempo, la red en su conjunto sigue funcionando sin interrupciones.

Bibliografía y Fuentes de Información

1. Ministerio de Asuntos Económicos y Transformación Digital (España)
    - Guía de Direccionamiento IP y Subnetting
      URL: https://avancedigital.gob.es
2. RedIRIS - Red Española para la I+D
    - Recursos y documentación sobre redes de computadoras, direccionamiento IP y subnetting.
      URL: https://www.rediris.es
3. CIFP César Manrique - Material de Redes y Comunicaciones
    - Curso de Administración de Redes y material sobre subnetting.
      URL: http://www3.gobiernodecanarias.org/medusa
4. Universidad Politécnica de Madrid (UPM) - Facultad de Informática
    - Apuntes de "Redes de Computadores".
      URL: https://www.fi.upm.es
5. Guía de Subnetting - Cisco Networking Academy España
    - Material de formación en redes y direccionamiento IP.
      URL: https://www.netacad.com
6. Normativa y documentación de RIPE NCC
    - Organismo encargado de la asignación de direcciones IP en Europa.
      URL: https://www.ripe.net