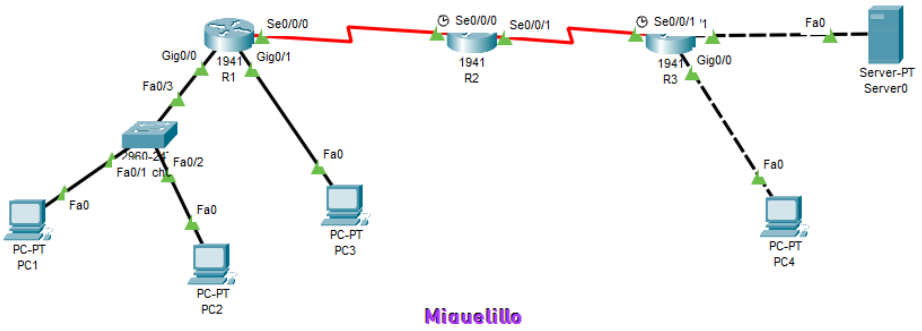
Índice:

Ejercicio ACL Cisco

a) 8.1.5-packet-tracer---acl-demonstration

Solución:

Escenario



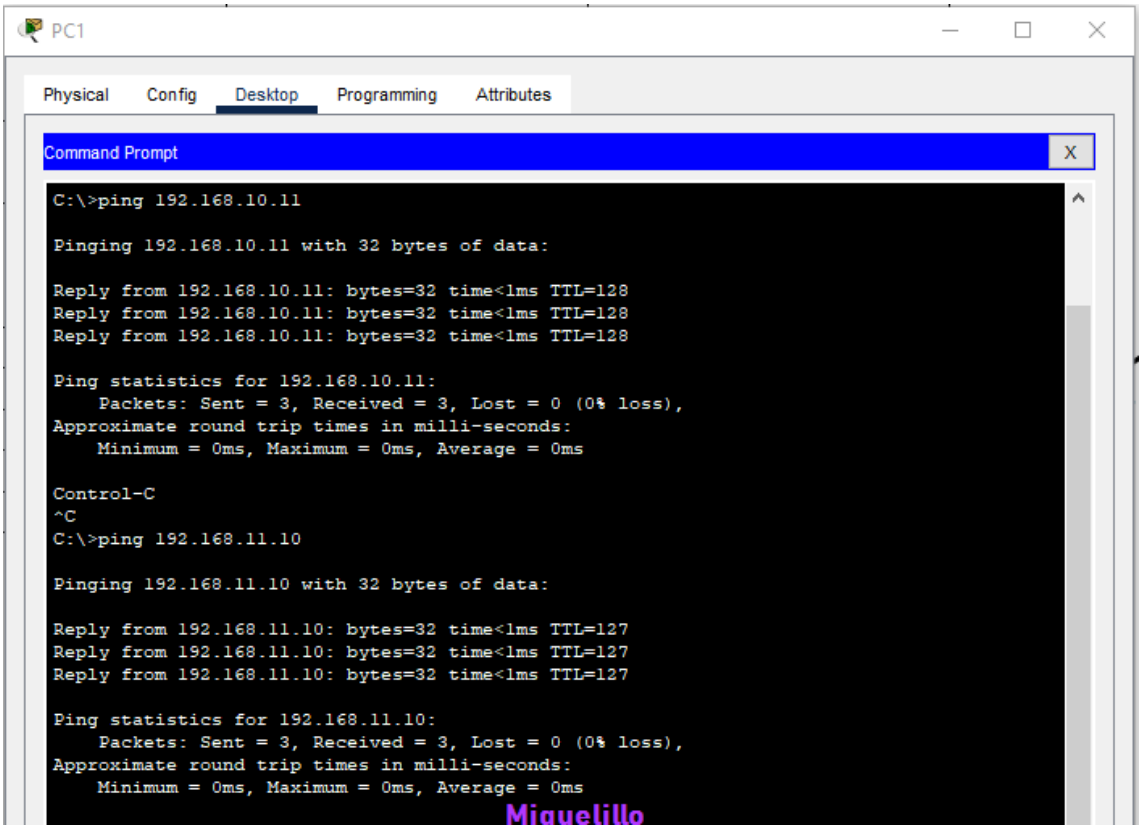
PARTE 1

Paso 1: Hacer ping a dispositivos en la red local para verificar la conectividad.

De PC1 a PC2 y de PC1 a PC3

¿Por qué fueron exitosos los pings?

Han tenido éxito ya que la ACL que hay solamente boquea a esa red cuando sale por el serial0/0/0



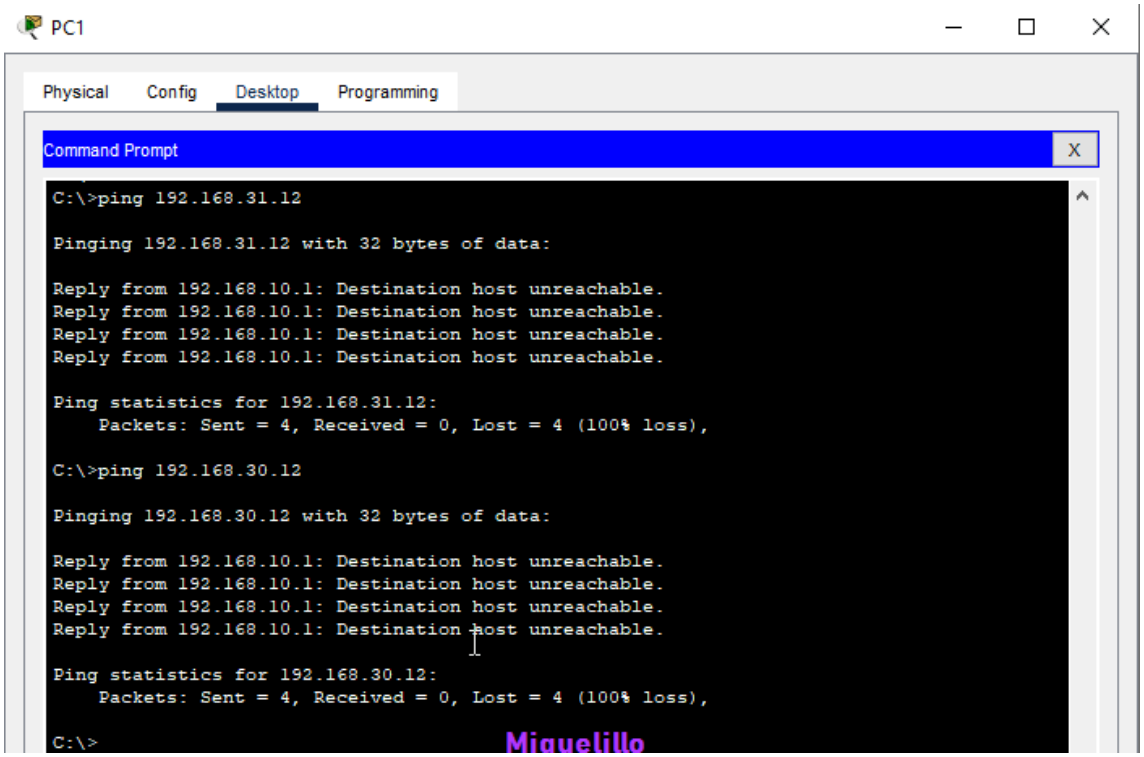
Paso 2: Hacer ping a dispositivos en redes remotas para probar la funcionalidad de la ACL.

a. Desde PC1, haz ping a PC4.

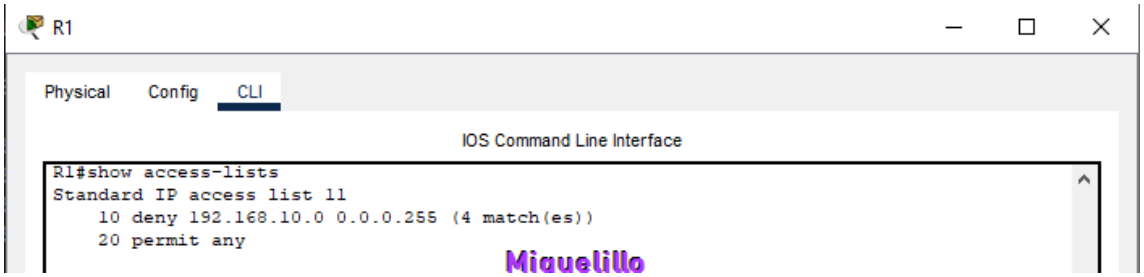
b. Desde PC1, haz ping al Servidor DNS.

¿Por qué fallaron los pings?

No hace ping ya que la ACL que no permite que el tráfico de la red 192.168.10.0/24 salga por el serial



ACL implicada

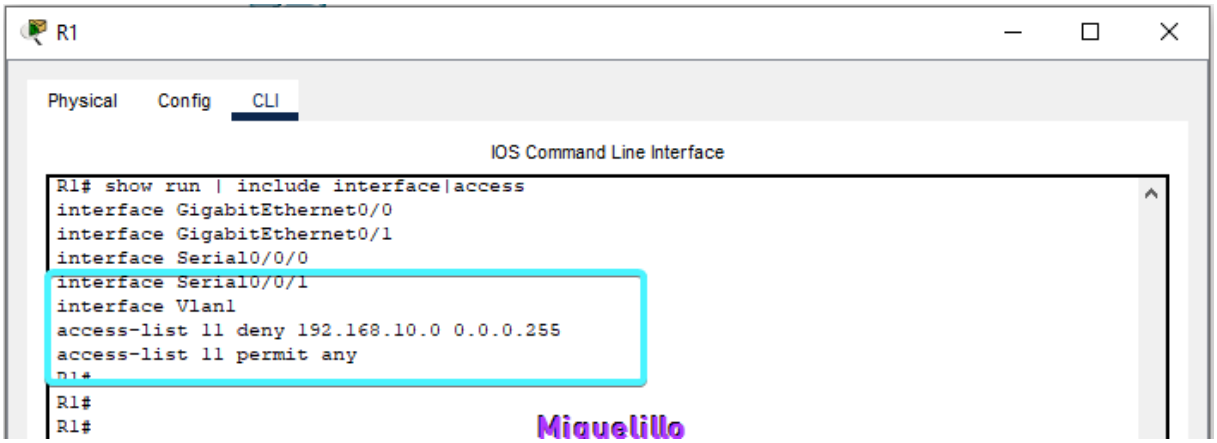


PARTE 2

Paso 1: Utilizar comandos show para investigar la configuración de la ACL.

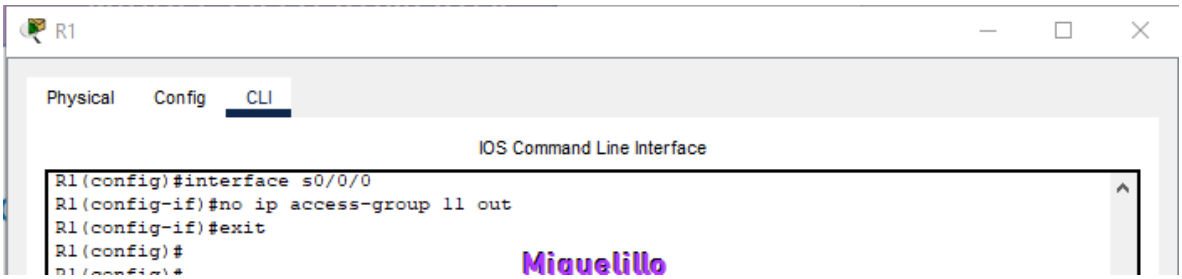
a) Utilizar comandos show para investigar la configuración de la ACL

b) para ver las interfaces que tiene una ACL asignada



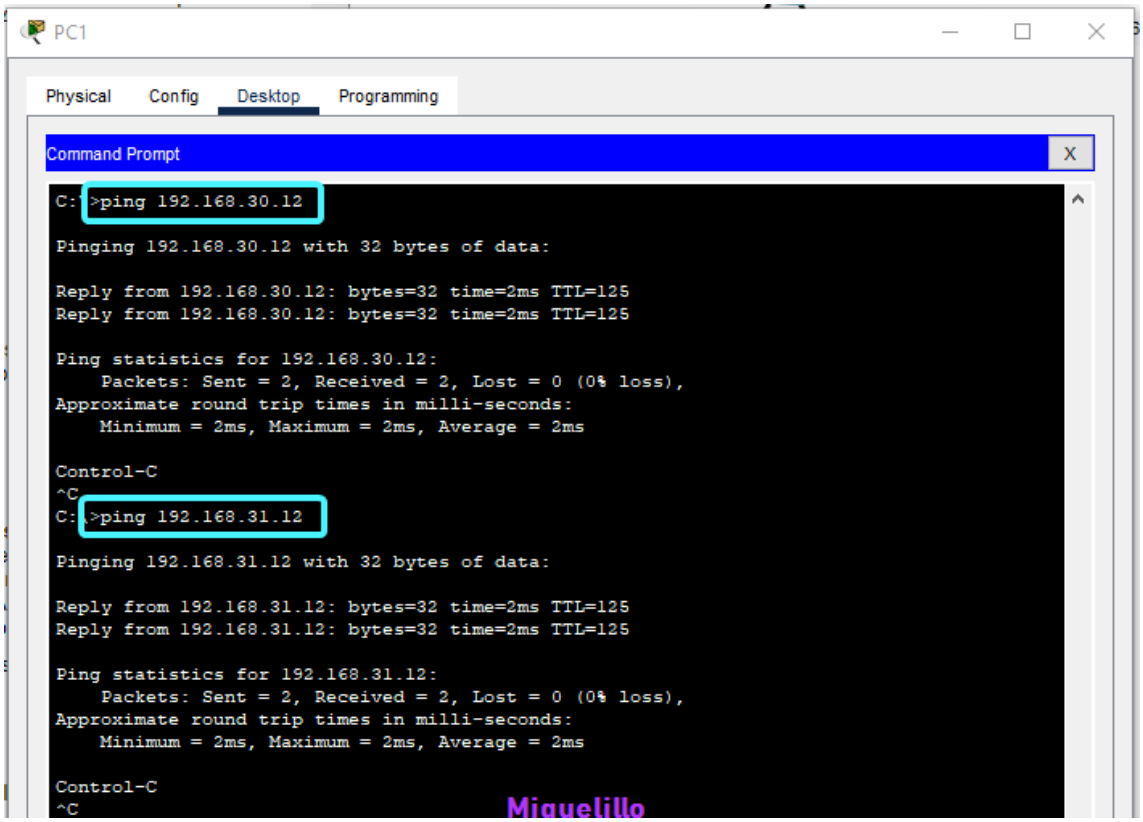
Paso 2

a) Quitamos la ACL



b) En modo de configuración global, elimina la ACL

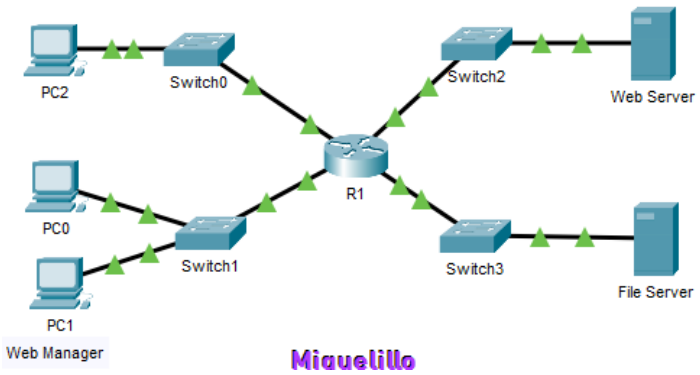
c) Una vez quitada probamos a hacer ping a la red externa



b) 8.5.5-packet-tracer---configure-named-standard-ipv4-acls

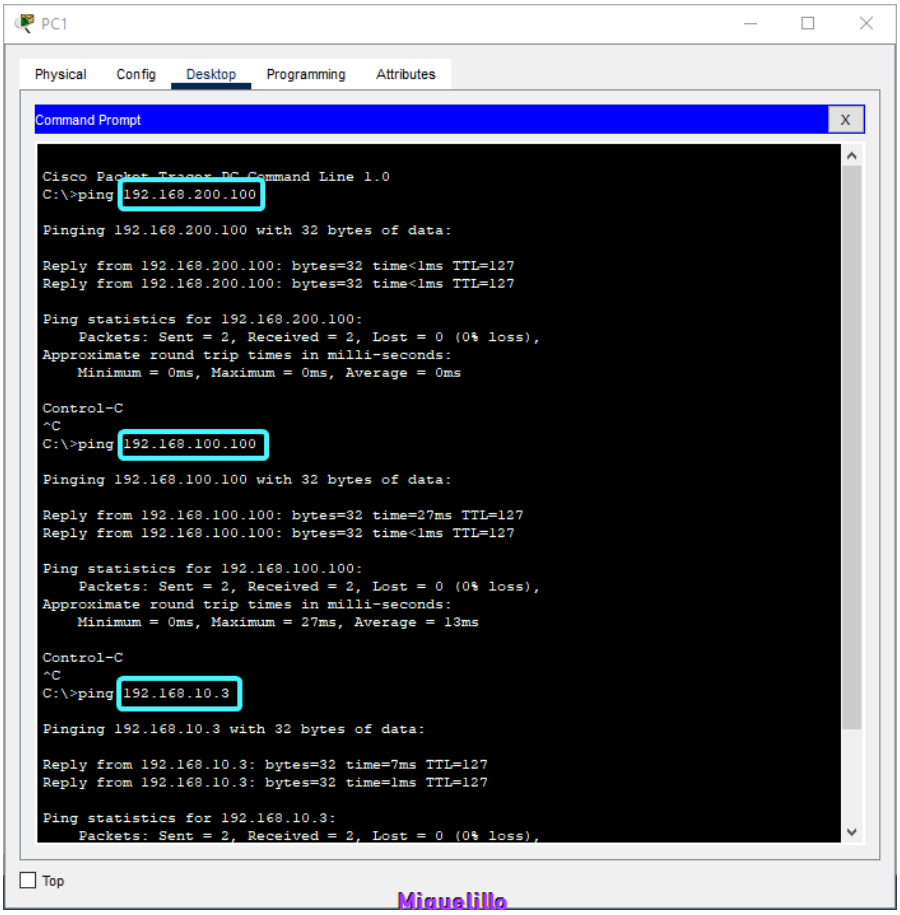
Solución:

Escenario



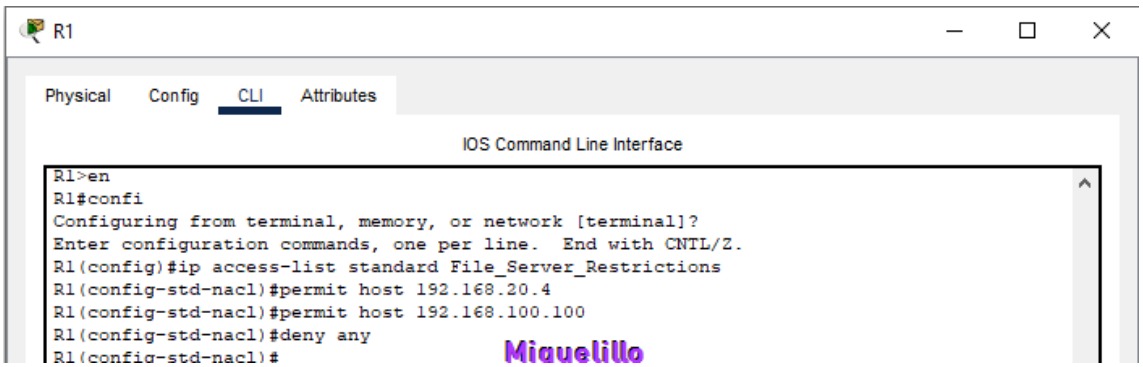
Parte 1

Paso 1Verificar la conectividad antes de configurar y aplicar la ACL. Las tres estaciones de trabajo deberían poder hacer ping tanto al Servidor Web como al Servidor de Archivos.



Paso 2 configura la ACL

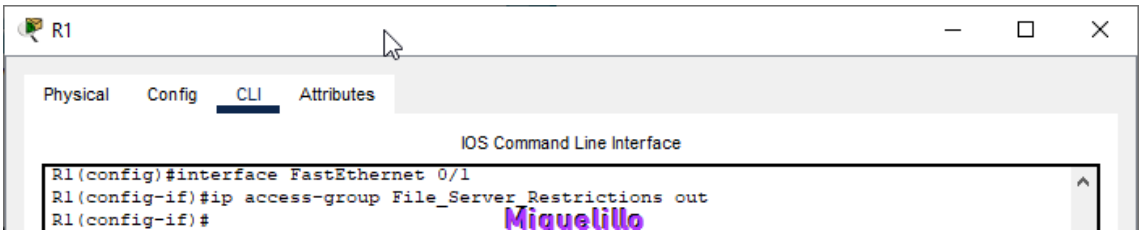
a.Configura la siguiente ACL nombrada en R1.



b. Usa el comando show access-lists para verificar el contenido de la lista de acceso antes de aplicarla a una interfaz.

Paso 3: Aplicar la ACL nombrada.

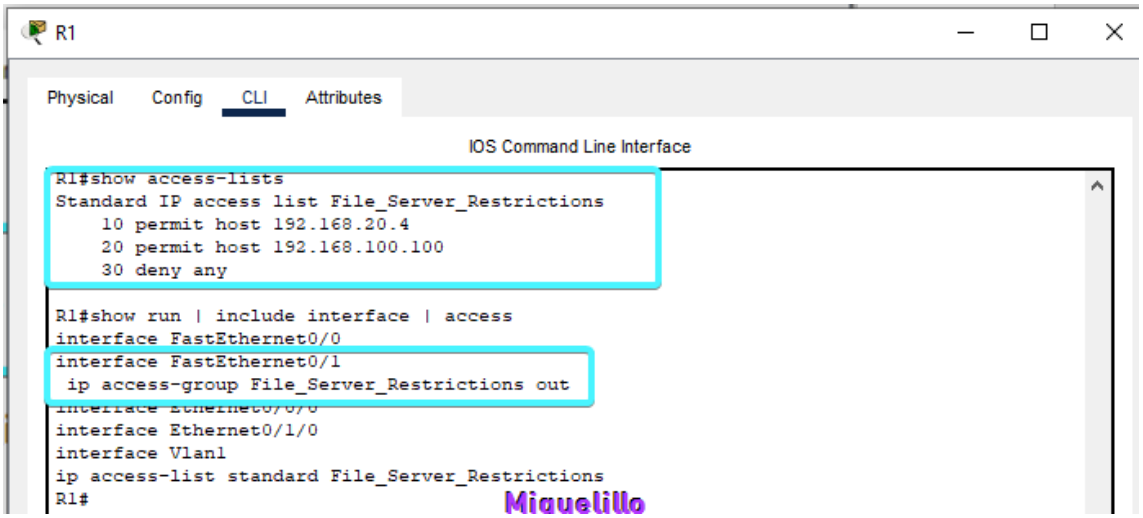
a. Aplica la ACL en la interfaz FastEthernet 0/1 en dirección de salida.



b. Guarda la configuración.

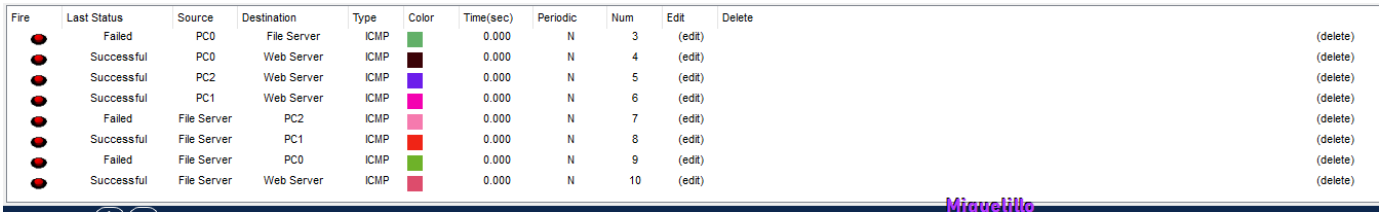
Parte 2

Paso 1: Verificar la configuración de la ACL y su aplicación a la interfaz.

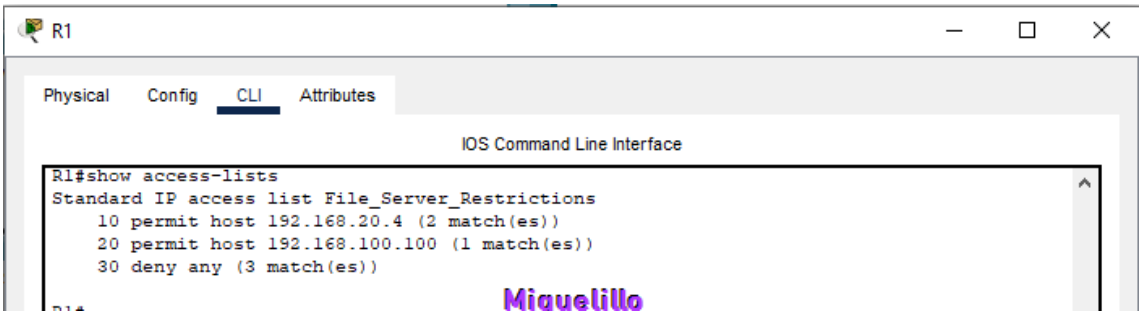


Paso 2: Verificar que la ACL funcione correctamente.

Las tres estaciones de trabajo deberían poder hacer ping al Servidor Web, pero solo PC1 y el Servidor Web deberían poder hacer ping al Servidor de Archivos



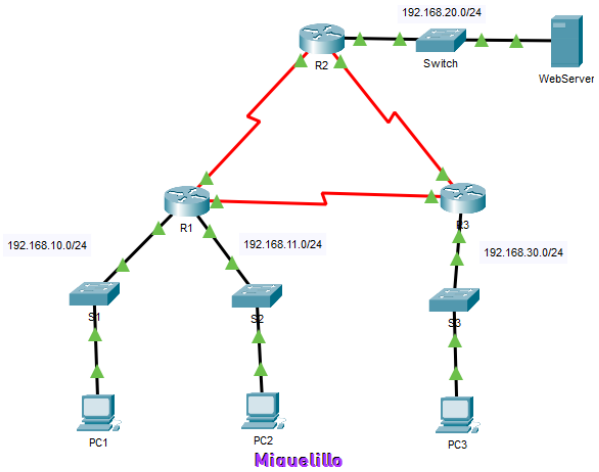
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC0	File Server	ICMP		0.000	N	3	(edit)	(delete)
	Successful	PC0	Web Server	ICMP		0.000	N	4	(edit)	(delete)
	Successful	PC2	Web Server	ICMP		0.000	N	5	(edit)	(delete)
	Successful	PC1	Web Server	ICMP		0.000	N	6	(edit)	(delete)
	Failed	File Server	PC2	ICMP		0.000	N	7	(edit)	(delete)
	Successful	File Server	PC1	ICMP		0.000	N	8	(edit)	(delete)
	Failed	File Server	PC0	ICMP		0.000	N	9	(edit)	(delete)
	Successful	File Server	Web Server	ICMP		0.000	N	10	(edit)	(delete)



c) 8.5.6-packet-tracer---configure-numbered-standard-ipv4-acls

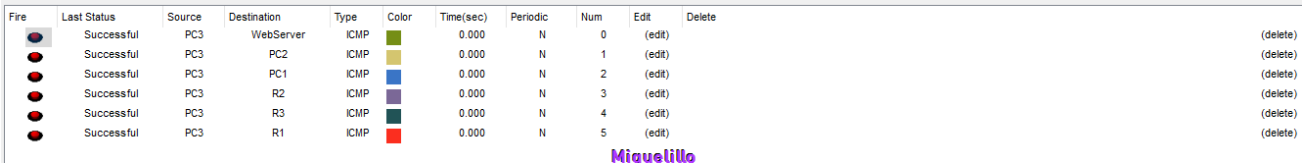
Solución:

Escenario:



Parte 1: Planear la Implementación de la ACL

Paso 1: Confirmar que tienes conectividad completa.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC3	WebServer	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC3	PC2	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC3	PC1	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC3	R2	ICMP		0.000	N	3	(edit)	(delete)
	Successful	PC3	R3	ICMP		0.000	N	4	(edit)	(delete)
	Successful	PC3	R1	ICMP		0.000	N	5	(edit)	(delete)

Miguelillo

Paso 2: Evaluar dos políticas de red y planificar implementaciones de ACL.

R2

La red 192.168.11.0/24 no tiene permitido el acceso al WebServer en la red 192.168.20.0/24.

Se permite todo otro acceso.

R3

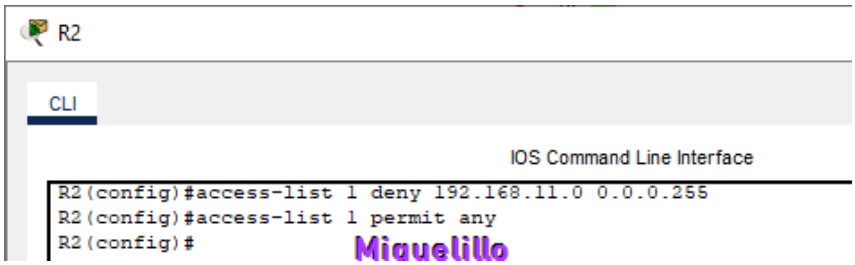
La red 192.168.10.0/24 no tiene permitido comunicarse con la red 192.168.30.0/24.

Se permite todo otro acceso.

Parte 2 Configurar, Aplicar y Verificar una ACL Estándar Numerada

Paso 1: Configurar y aplicar una ACL estándar numerada en R2.

a. Crea una ACL utilizando el número 1 en R2
b. Por defecto, una lista de acceso deniega todo el tráfico que no coincide con ninguna regla. Para permitir todo otro tráfico,

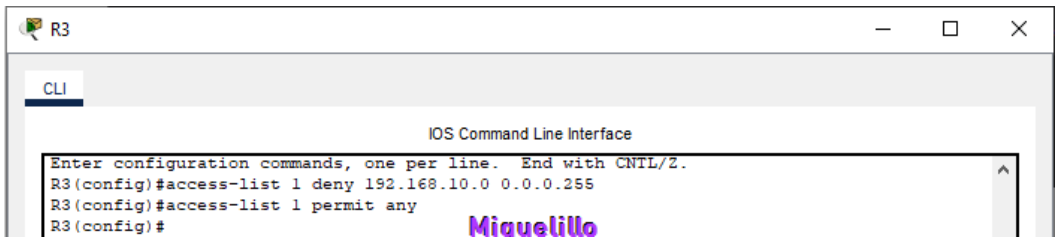


c. Antes de aplicar una lista de acceso a una interfaz para filtrar tráfico, es una buena práctica revisar el contenido de la lista de acceso.

d. Aplica la ACL colocándola para el tráfico de salida en la interfaz GigabitEthernet 0/0.

Paso 2: Configurar y aplicar una ACL estándar numerada en R3.

a. Crea una ACL utilizando el número 1 en R3 con una declaración que deniega el acceso desde la red 192.168.10.0/24 a la red 192.168.30.0/24.
b. Por defecto, una ACL deniega todo el tráfico que no coincide con ninguna regla. Para permitir todo otro tráfico, crea una segunda regla para la ACL.

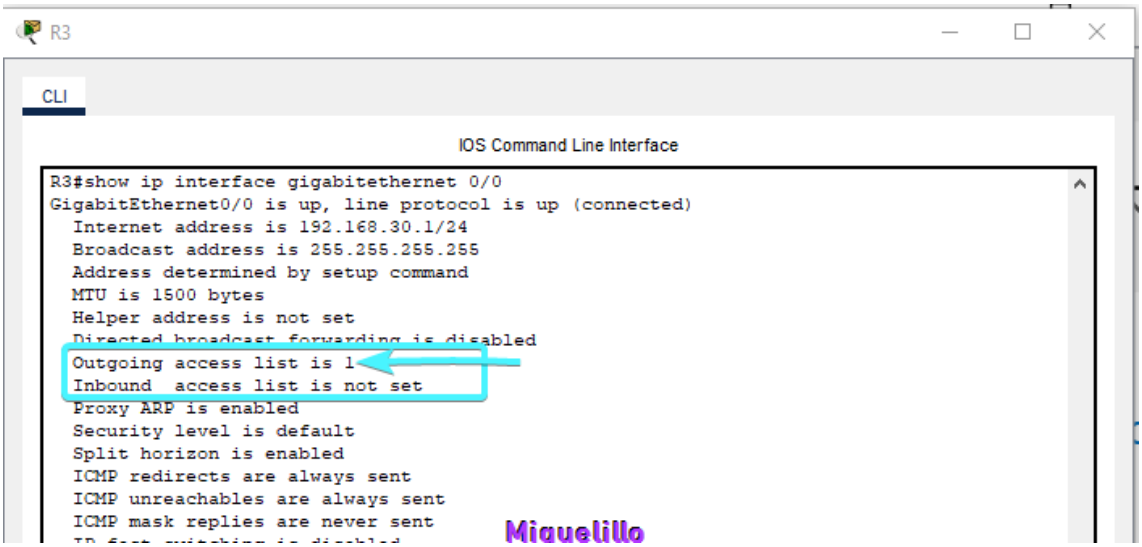


c. Verifica que la lista de acceso esté configurada correctamente.

d. Aplica la ACL colocándola para el tráfico de salida en la interfaz GigabitEthernet 0/0.

Paso 3: Verificar la configuración y funcionalidad de la ACL

a. Ingresa el comando show run o show ip interface gigabitethernet 0/0 para verificar las ubicaciones de la ACL.



b. Utiliza las siguientes pruebas para verificar las implementaciones de la ACL:

c. Escribe el comando show access-lists en los routers R2 y R3. Deberías ver una salida que indique el número de paquetes que coinciden con cada línea.

d) 8.5.12-packet-tracer---configure-extended-ipv4-acls---scenario-1

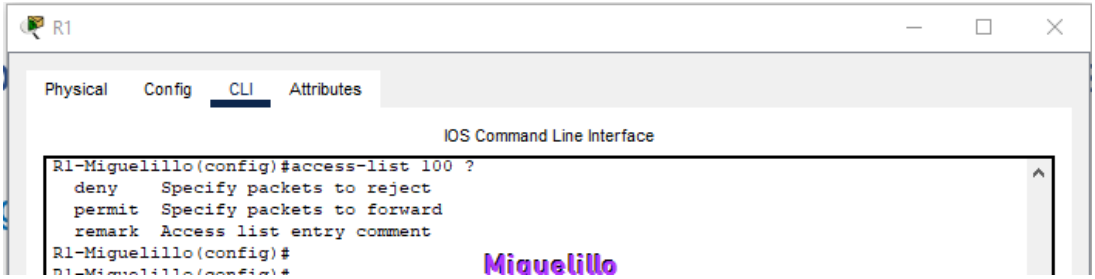
Solución:

Parte 1: Configurar, Aplicar y Verificar una ACL Extendida Numerada

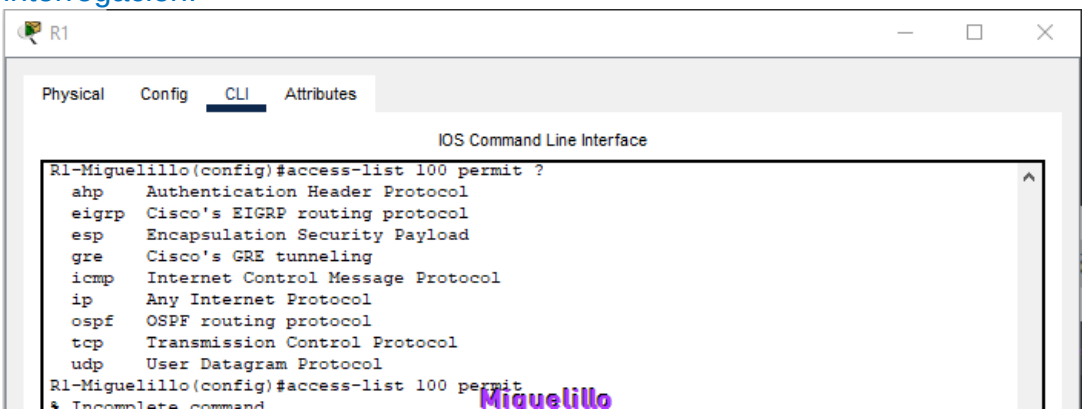
Paso 1: Configurar una ACL para permitir FTP e ICMP desde la LAN de PC1.

a. Desde el modo de configuración global en R1, introduce el siguiente comando para determinar el primer número válido para una lista de acceso extendida.

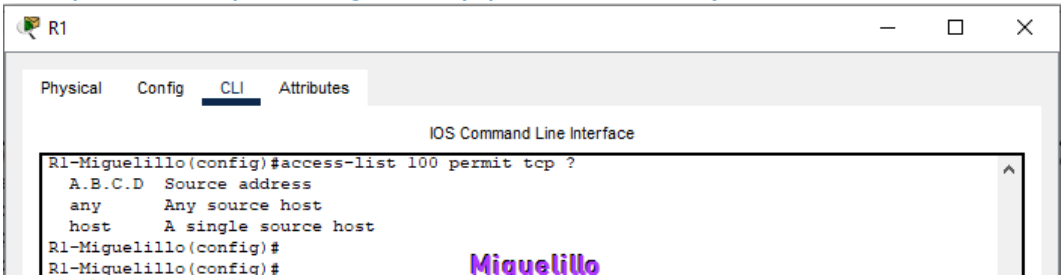
b. Sumamos 100 al comando, seguido de un signo de interrogación.



c. Para permitir tráfico FTP, ingresa permit, seguido de un signo de interrogación.



d. Como FTP es un protocolo de la capa de aplicación que utiliza TCP en la capa de transporte, ingresa tcp para refinar la ayuda de ACL.



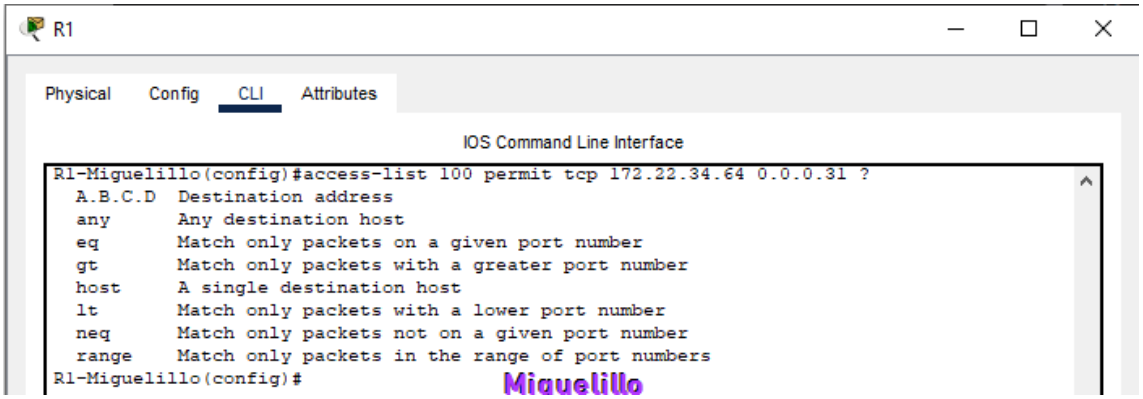
e. La dirección de origen puede representar un único dispositivo, como PC1, utilizando la palabra clave host y luego la dirección IP de PC1. En este caso, es cualquier host que tenga una dirección perteneciente a la red 172.22.34.64/27. Ingresa esta dirección de red, seguida de un signo de interrogación.

f. Calcula la máscara wildcard determinando la inversa binaria de la máscara de subred /27.

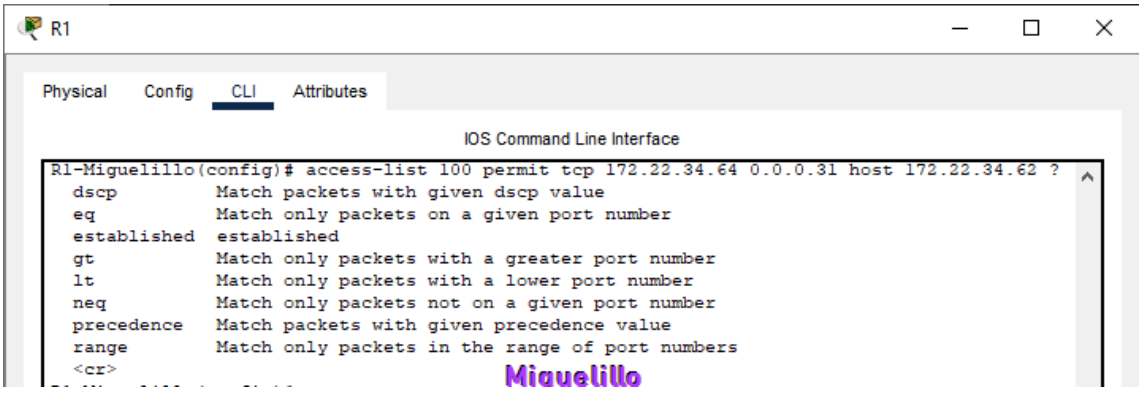
```
11111111.11111111.11111111.11100000 = 255.255.255.224

00000000.00000000.00000000.00011111 = 0.0.0.31
```

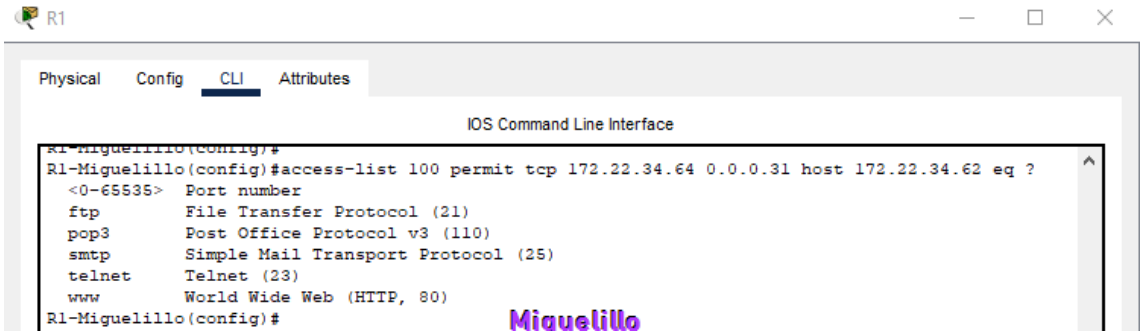
g. Ingresa la máscara wildcard, seguida de un signo de interrogación.

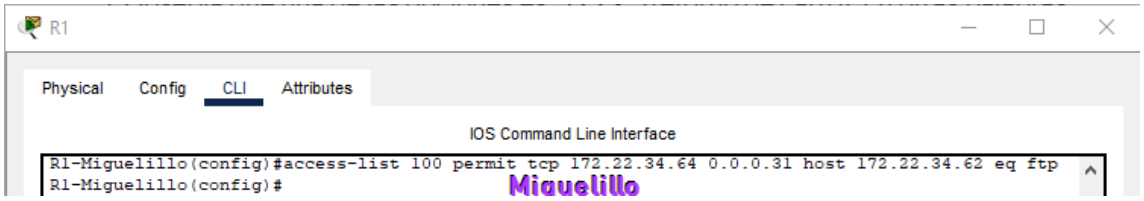


h. Configura la dirección de destino. Ingresa la palabra clave host seguida de la dirección IP del servidor seguida de una interrogación



i. Observa que una de las opciones es <cr> puedes presionar Enter y la declaración permitiría todo el tráfico TCP. Sin embargo, solo estamos permitiendo tráfico FTP; por lo tanto, ingresa la palabra clave eq, seguida de un signo de interrogación para mostrar las opciones disponibles. Luego, ingresa ftp y presiona Enter.





j. Crea una segunda declaración de lista de acceso para permitir tráfico ICMP desde PC1 hasta el servidor.

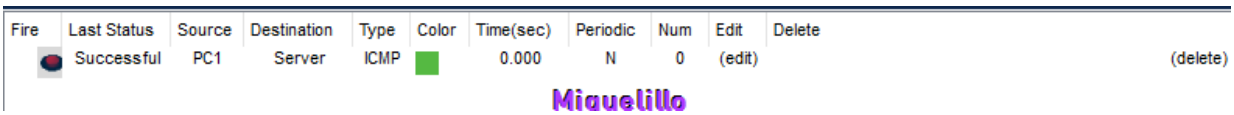
k. Todo otro tráfico se deniega por defecto. Con lo cual no tenemos que pone ninguna directiva

l. Ejecuta el comando show access-list y verifica que la lista de acceso 100 contiene las declaraciones correctas.

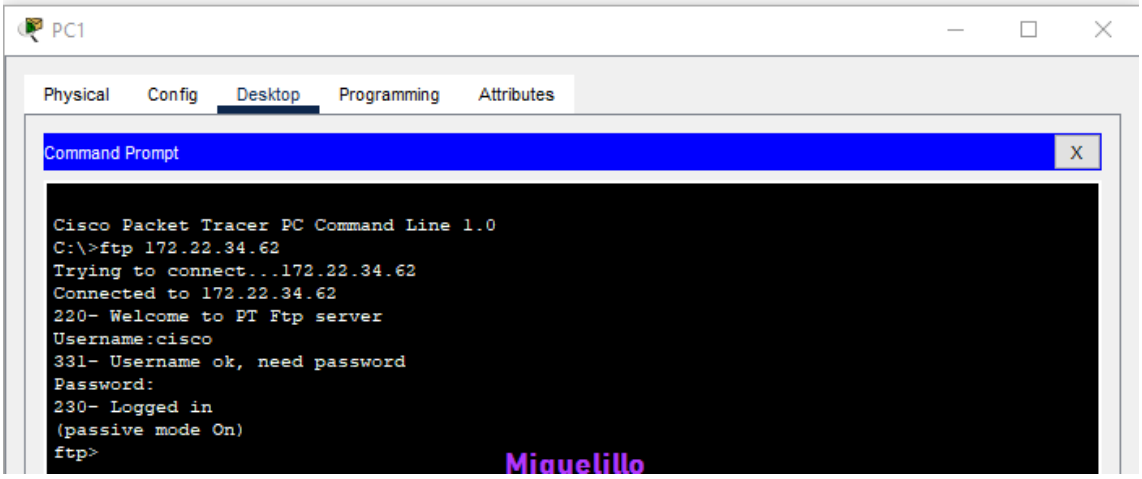
Paso 2: Aplicar la ACL en la interfaz correcta para filtrar el tráfico.

Paso 3: Verificar la implementación de la ACL.

a. Realiza un ping desde PC1 hasta el servidor.

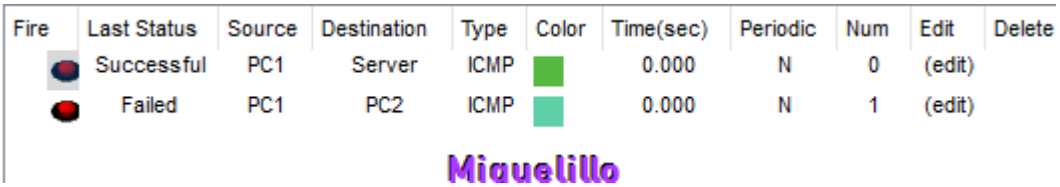


b. Realiza un FTP desde PC1 hasta el servidor



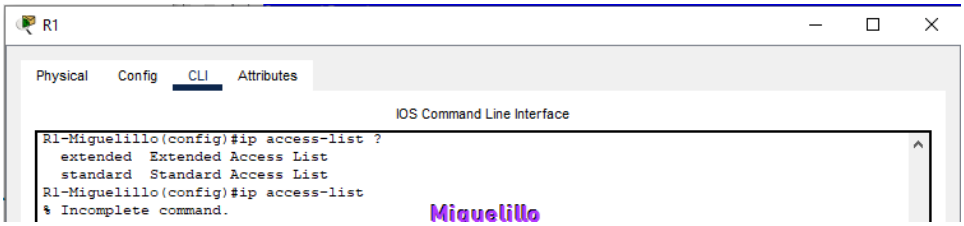
c. Sal del servicio FTP.

d. Realiza un ping desde PC1 hasta PC2. El host de destino debe ser inalcanzable por la ACL

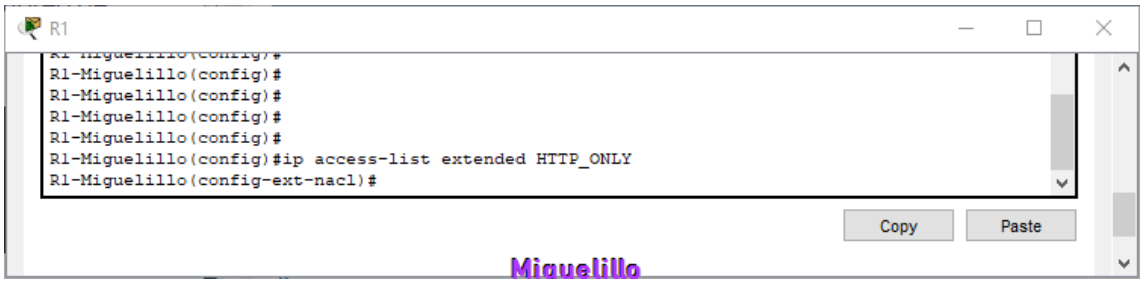


Parte 2: Configurar, Aplicar y Verificar una ACL Extendida Nombrada

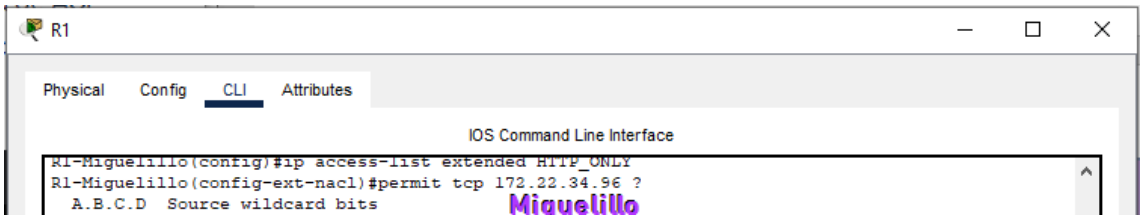
a. Las ACL con nombre comienzan con la palabra clave ip pon una interrogación al final



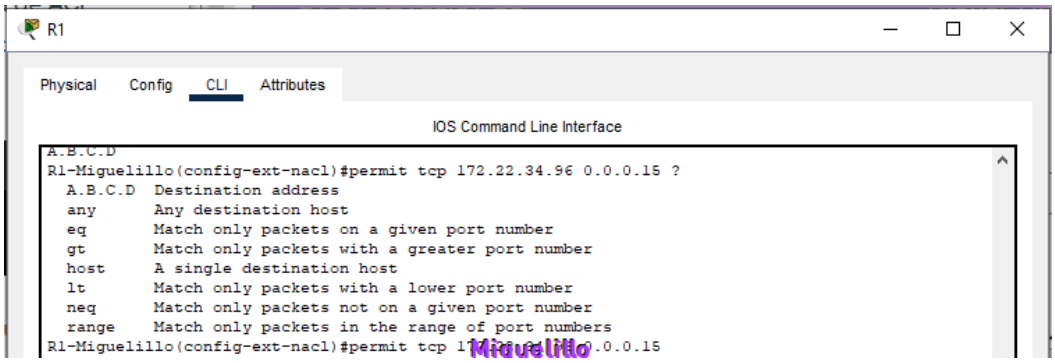
b. Puedes configurar ACL con nombre estándar y extendidas. Pon extendida HTTP_ONLY como nombre



c. El indicador cambia. Ahora estás en el modo de configuración extendida de ACL con nombre. Ingresa la dirección de red, seguida de un signo de interrogación.



d. Calculamos la wildcar

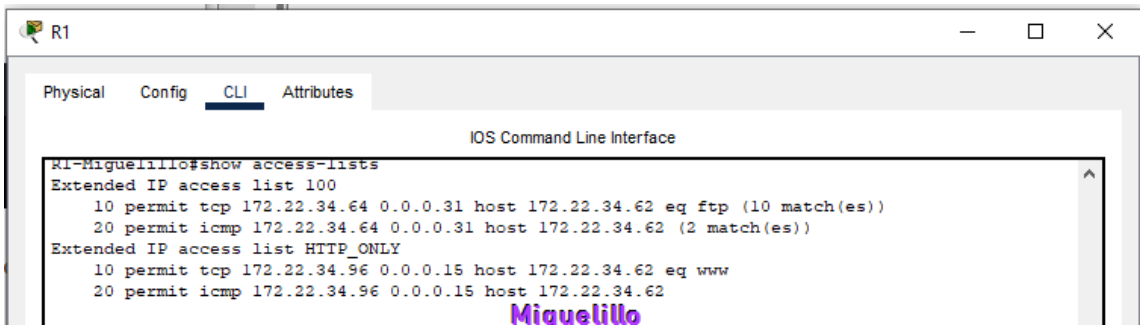


e. Finaliza la declaración especificando la dirección del servidor como hiciste en la Parte 1 y filtra el tráfico de www.

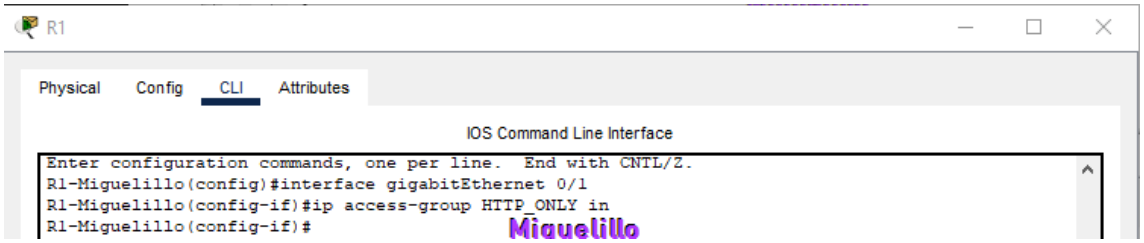
f. Crea una segunda declaración de lista de acceso para permitir tráfico ICMP desde PC2 hasta el servidor.

g. Todo otro tráfico se deniega por defecto. Sal del modo de configuración de ACL con nombre extendida.

h. Ejecuta el comando show access-list y verifica que la lista de acceso HTTP_ONLY contiene las declaraciones correctas.

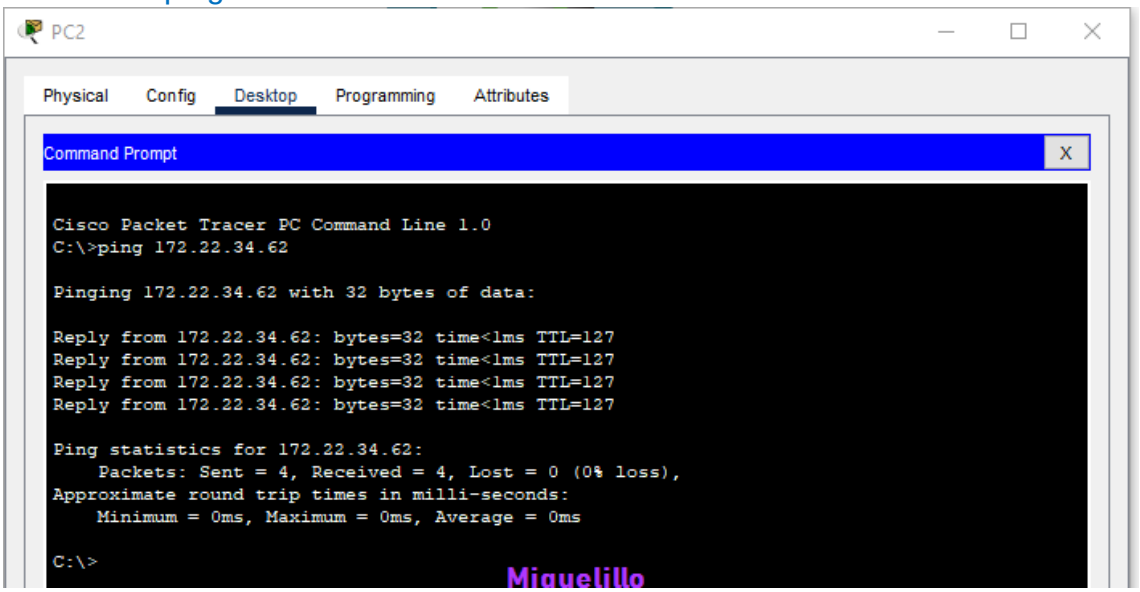


Paso 2: Aplicar la ACL en la interfaz correcta para filtrar el tráfico.

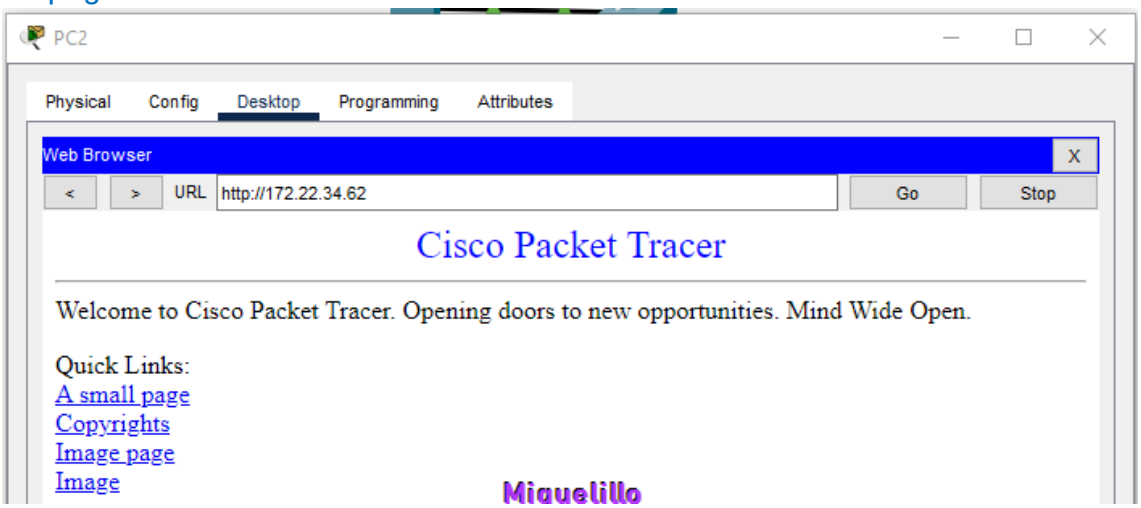


Paso 3: Verificar la Implementación de la ACL.

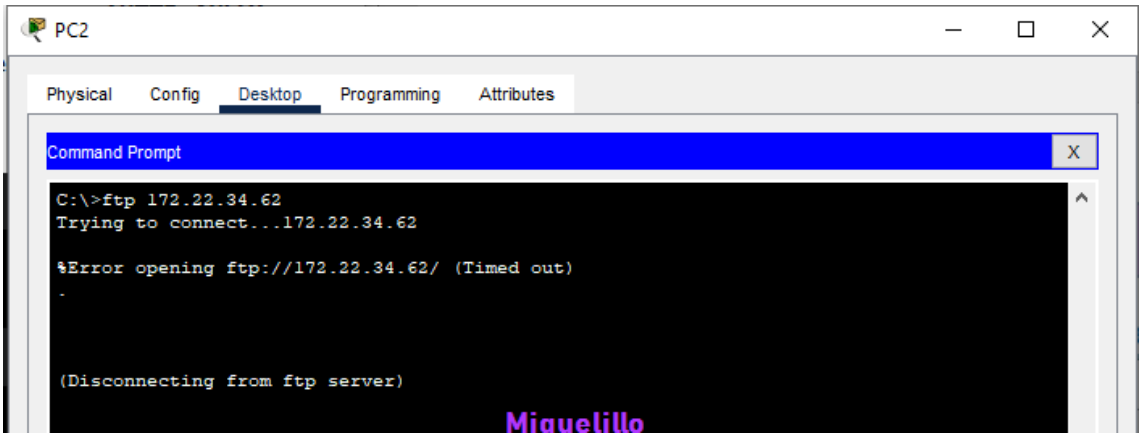
a. Realiza un ping desde PC2 hasta el servidor. Deberían resolver.



b. Desde PC2, abre un navegador web e ingresa la dirección IP del servidor. La página web del servidor debería mostrarse.



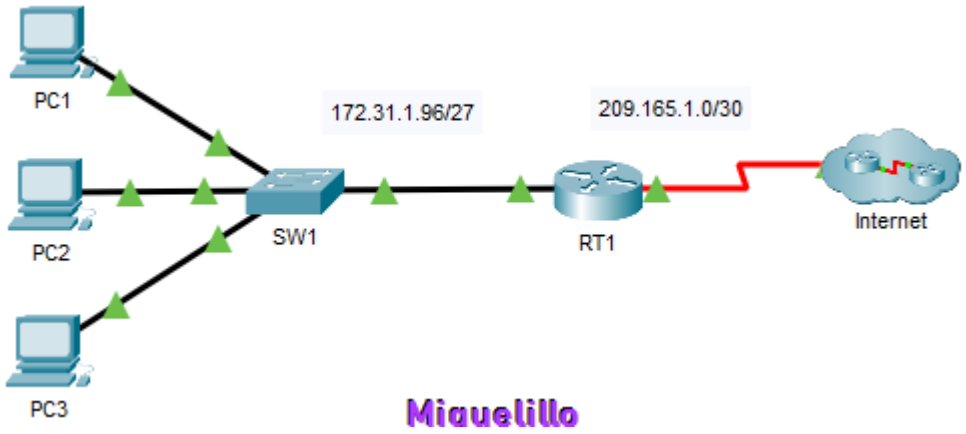
c. Intenta hacer FTP desde PC2 hasta el servidor. La conexión debería fallar.



e) 8.5.13-packet-tracer---configure-extended-ipv4-acls---scenario-2

Solución:

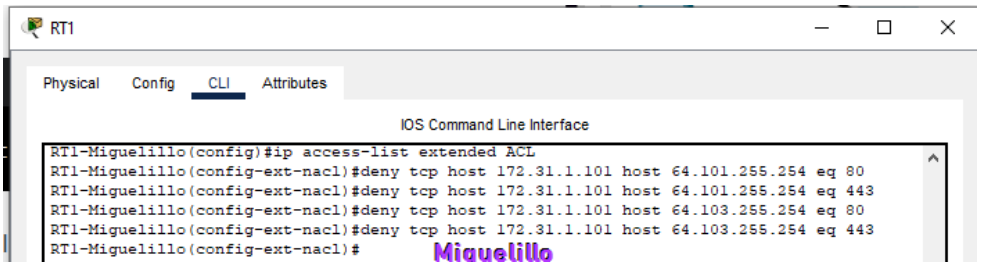
Escenario



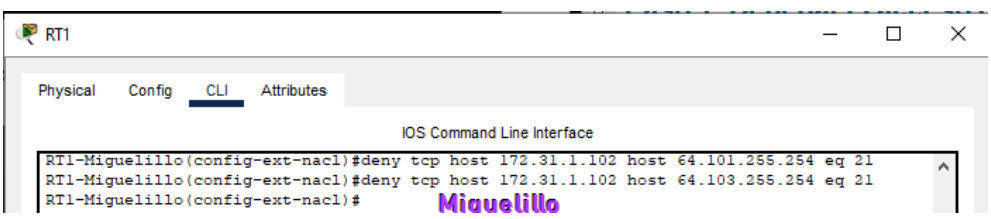
Parte 1: Configurar una ACL Extendida con Nombre

Paso 1: Denegar el acceso de PC1 a los servicios HTTP y HTTPS en Server1 y Server2.

a. Crea una lista de acceso extendida con nombre en el router RT1. Usa el nombre ACL para la lista de acceso con nombre.
b. Comienza la configuración de la ACL con una declaración que deniegue el acceso desde PC1 a Server1, solo para HTTP (puerto 80) Continúa con la declaración que deniega el acceso desde PC1 a Server1, solo para HTTPS (puerto 443).
c. Ingresa la declaración que deniega el acceso desde PC1 a Server2, solo para HTTP. Añade la declaración que deniega el acceso desde PC1 a Server2, solo para HTTPS.

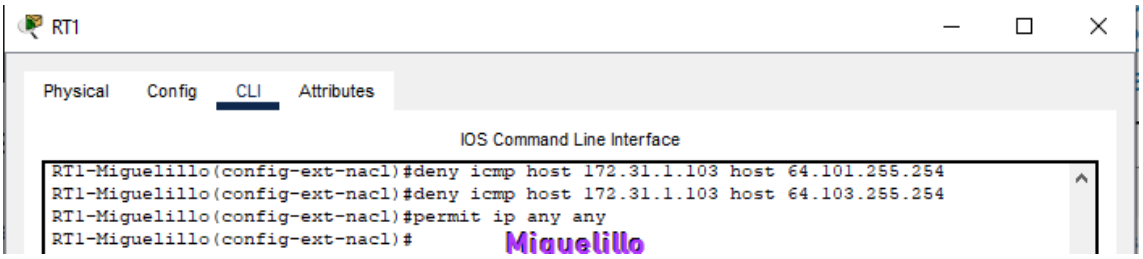


d. Deniega a PC2 el acceso a los servicios FTP en Server1 y Server2. Usa la dirección IP de PC2 de la tabla de direcciones. Añade la declaración que deniega a PC2 el acceso a FTP en Server2.



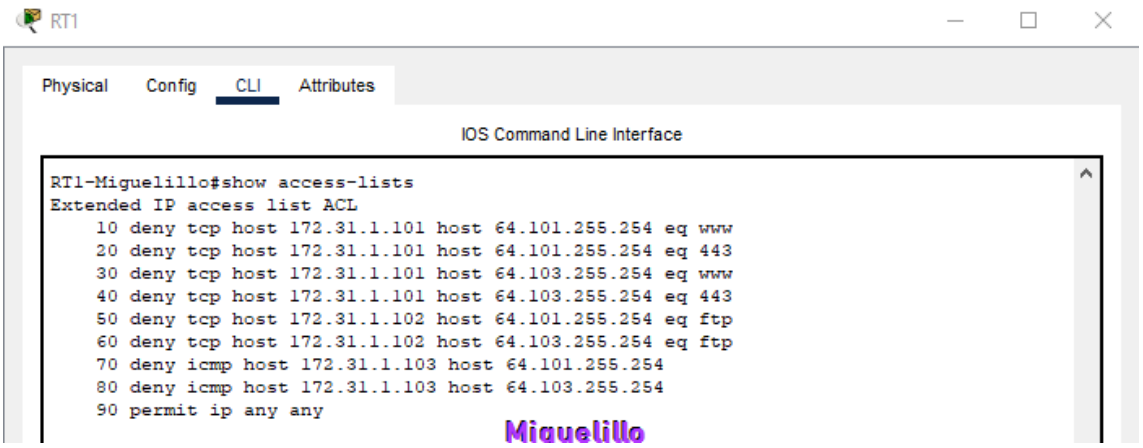
Paso 2: Denegar que PC3 haga ping a Server1 y Server2

a. Ingresa la declaración que deniega el acceso ICMP desde PC3 a Server1.
b. Añade la declaración que deniega el acceso ICMP desde PC3 a Server2.
c. Permite todo otro tráfico IP.



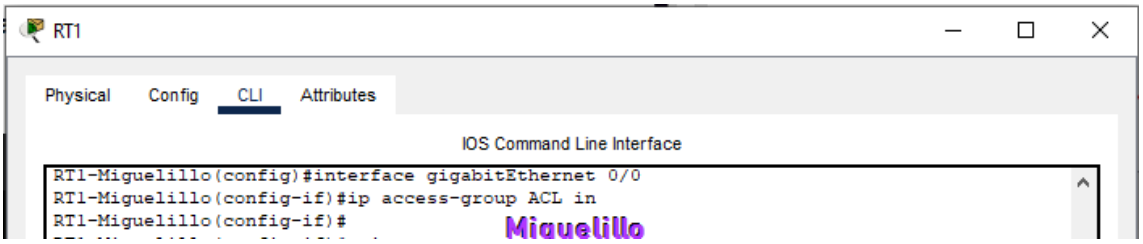
Paso 3: Verificar la configuración de la lista de acceso antes de aplicarla a una interfaz.

Utiliza los comandos show access-lists o show running-config.



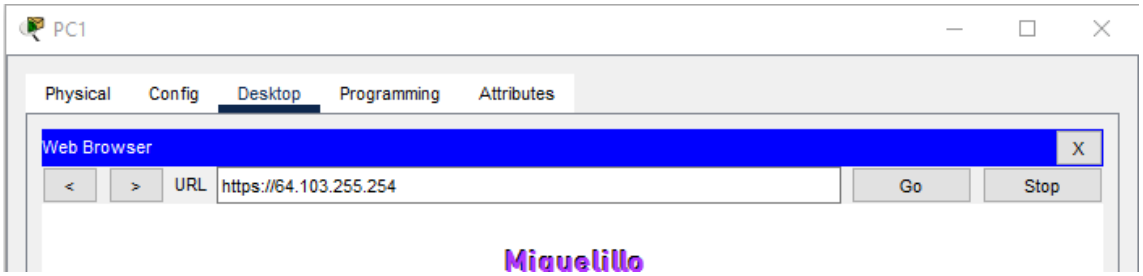
Parte 2: Aplicar y Verificar la ACL Extendida

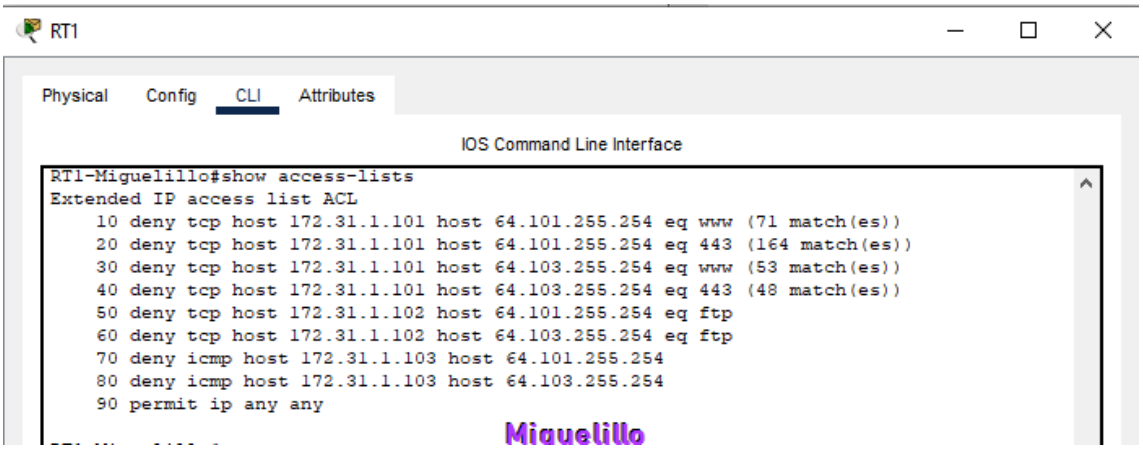
Paso 1: Aplicar la ACL a la interfaz y en la dirección correcta.



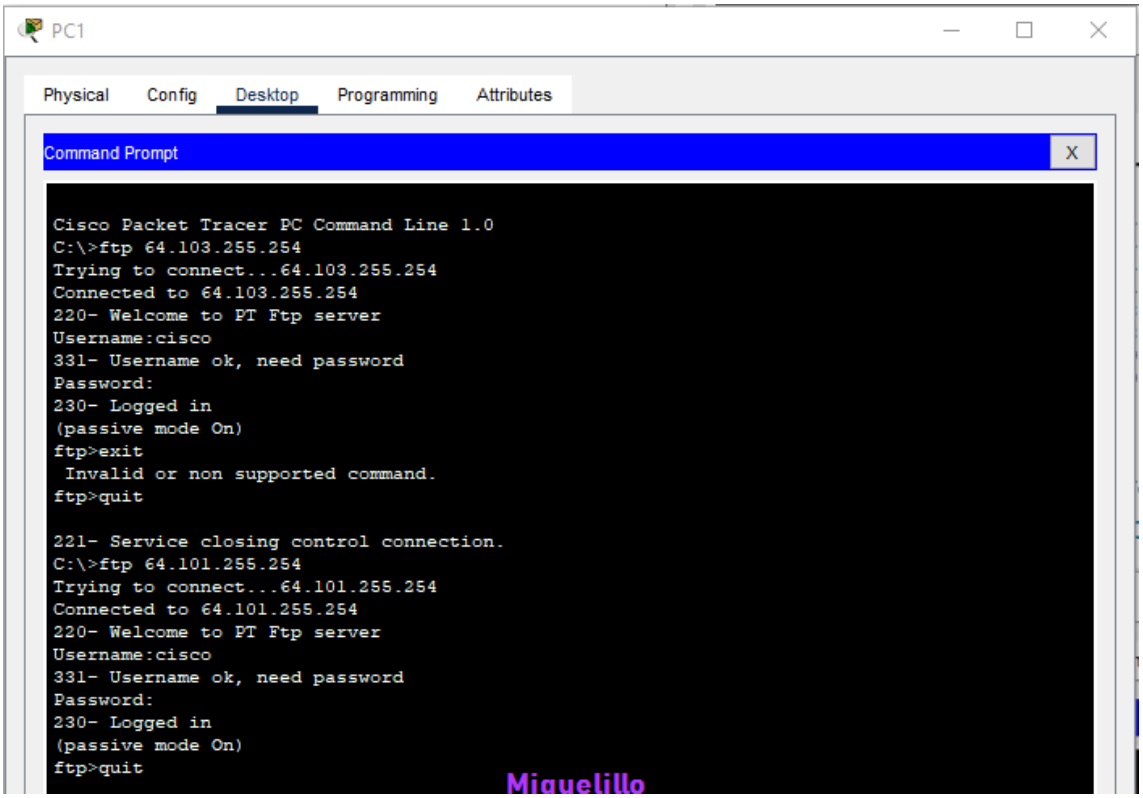
Paso 2: Probar el acceso para cada PC.

a. Accede a los sitios web de Server1 y Server2 desde el navegador de PC1, utilizando tanto HTTP como HTTPS. Usa show access-lists para ver qué declaración de la lista de acceso permitió o denegó el tráfico.

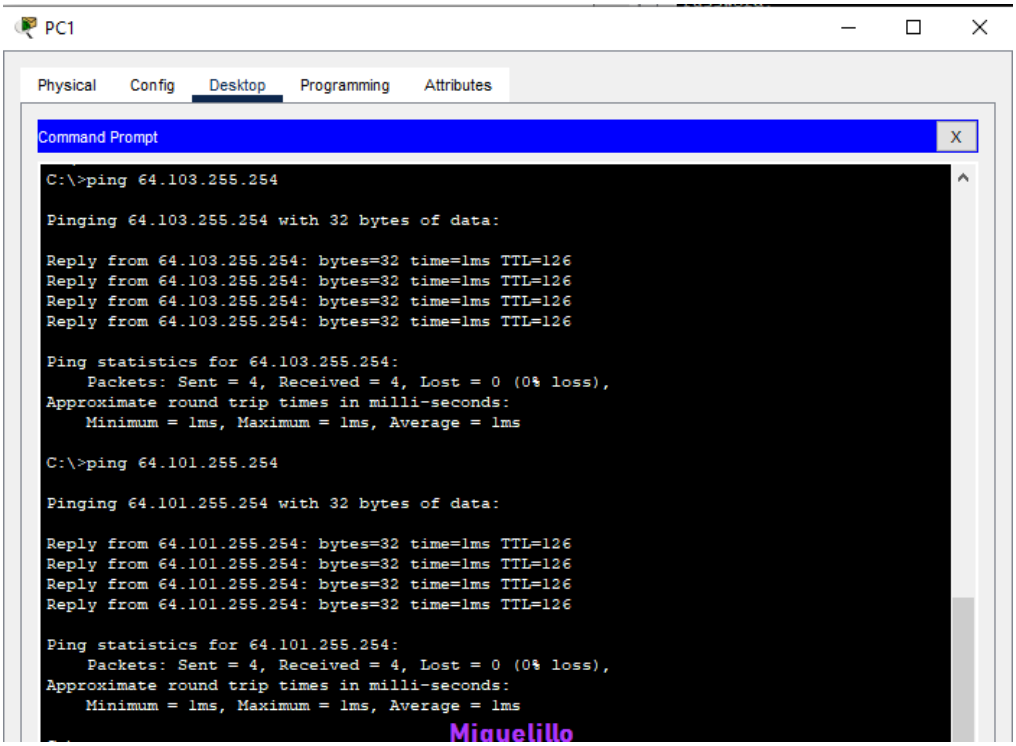




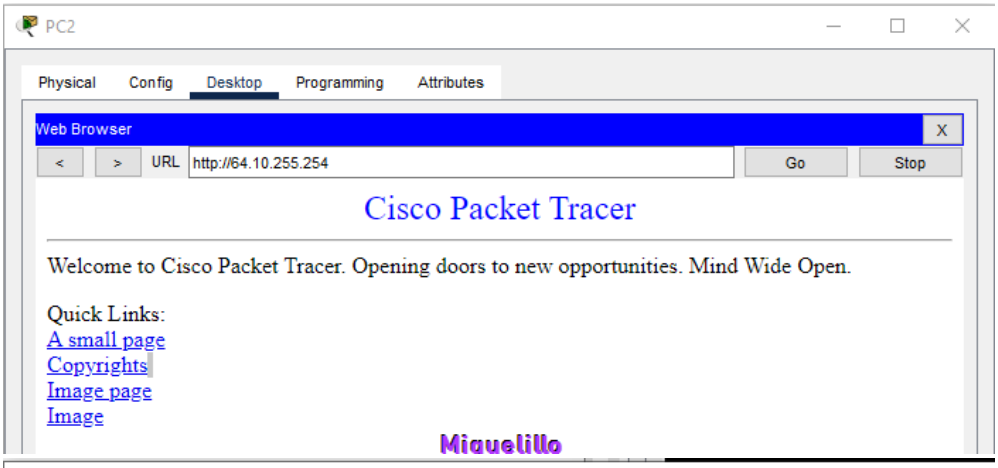
b. Accede a FTP en Server1 y Server2 desde PC1. El nombre de usuario y la contraseña son cisco.

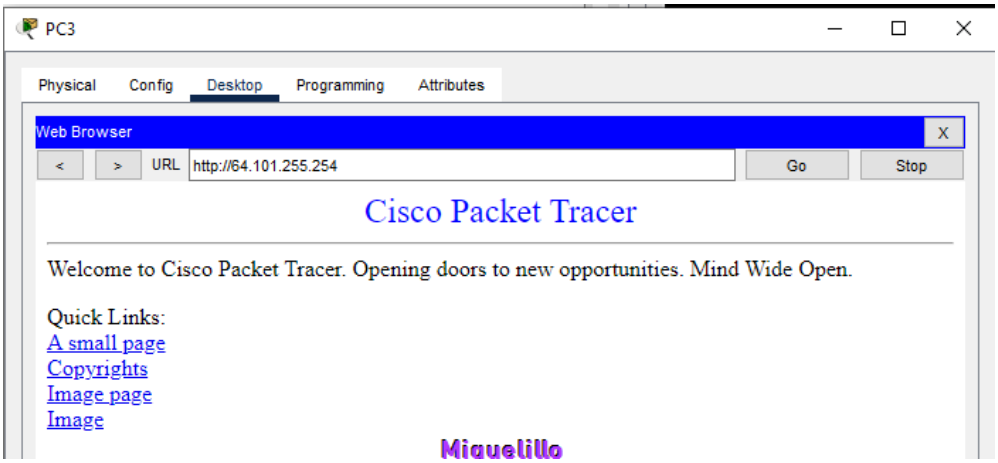


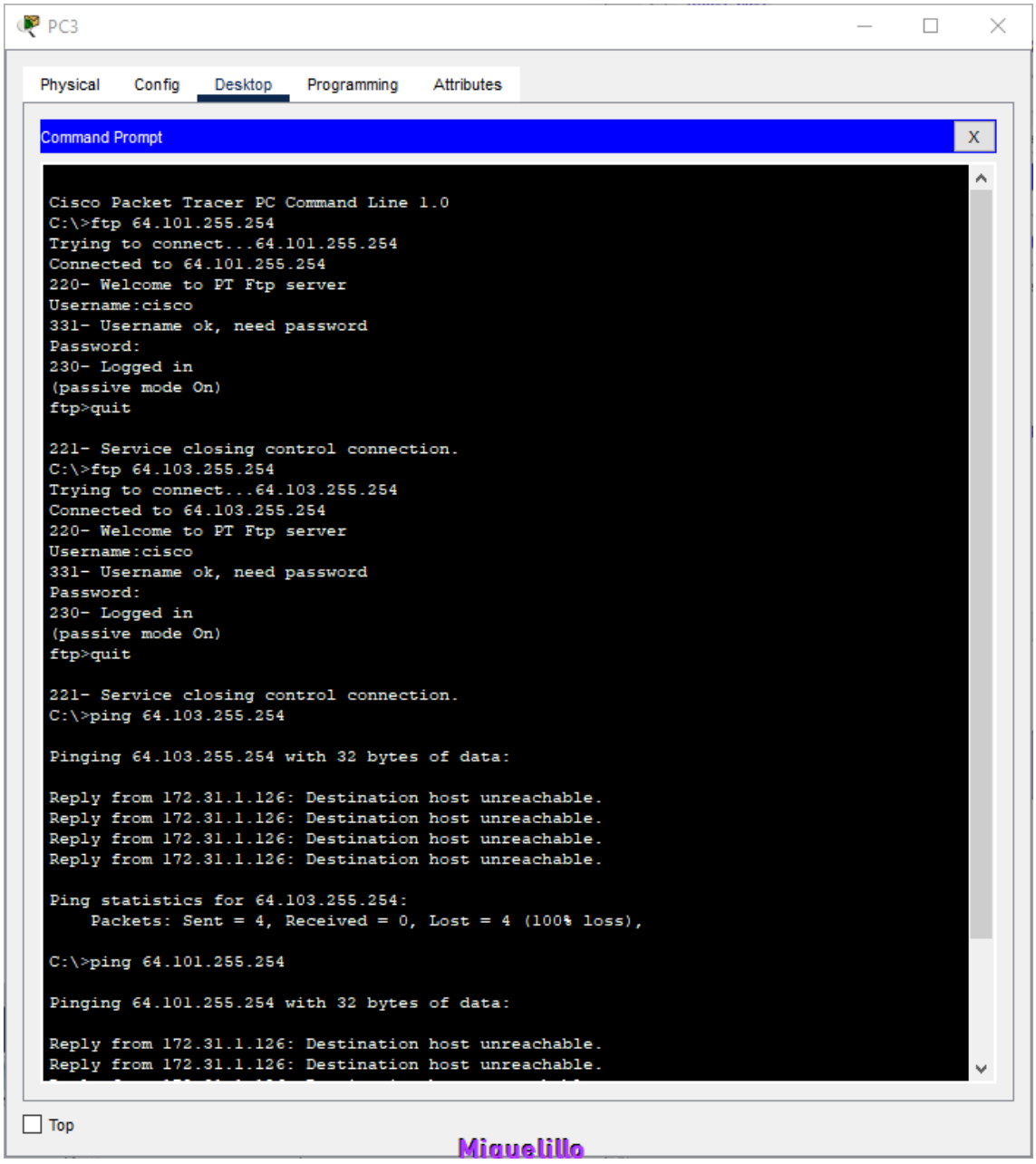
c. Realiza un ping a Server1 y Server2 desde PC1.

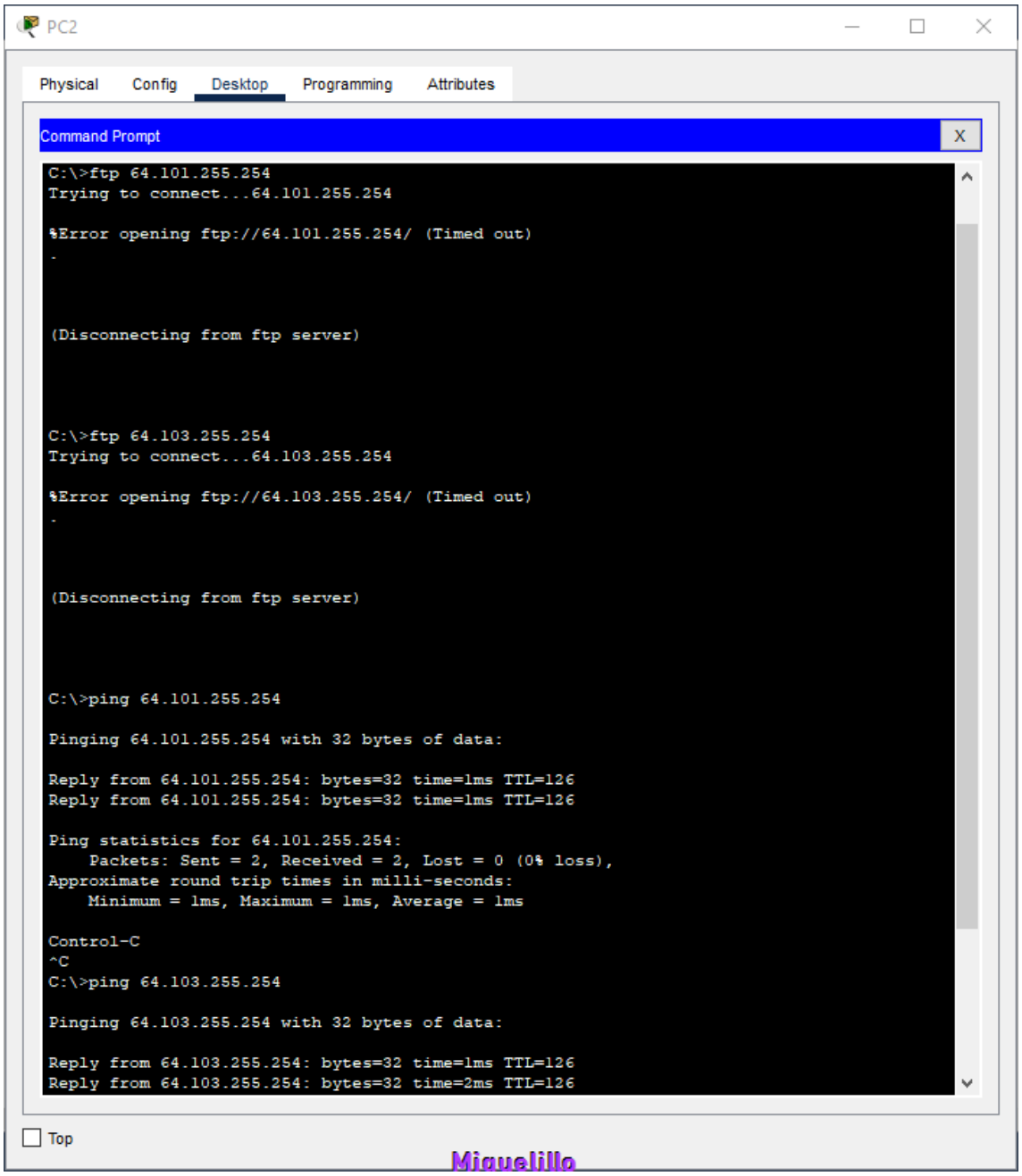


d. Repite los pasos a-c con PC2 y PC3 para verificar el funcionamiento adecuado de la lista de acceso.

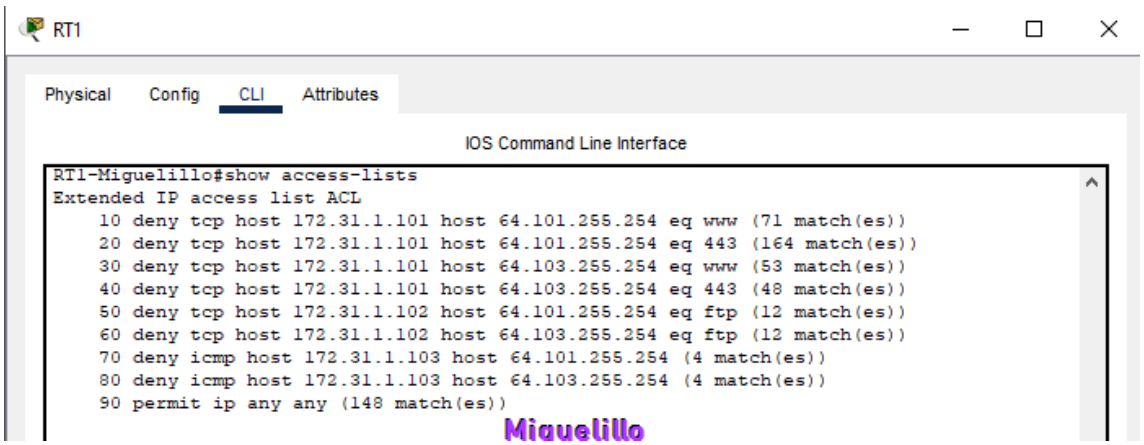





PC3
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 64.101.255.254
Trying to connect...64.101.255.254
Connected to 64.101.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit
221- Service closing control connection.
C:\>ftp 64.103.255.254
Trying to connect...64.103.255.254
Connected to 64.103.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit
221- Service closing control connection.
C:\>ping 64.103.255.254
Pinging 64.103.255.254 with 32 bytes of data:
Reply from 172.31.1.126: Destination host unreachable.
Reply from 172.31.1.126: Destination host unreachable.
Reply from 172.31.1.126: Destination host unreachable.
Reply from 172.31.1.126: Destination host unreachable.
Ping statistics for 64.103.255.254:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 64.101.255.254
Pinging 64.101.255.254 with 32 bytes of data:
Reply from 172.31.1.126: Destination host unreachable.
Reply from 172.31.1.126: Destination host unreachable.
Top
Miguelillo



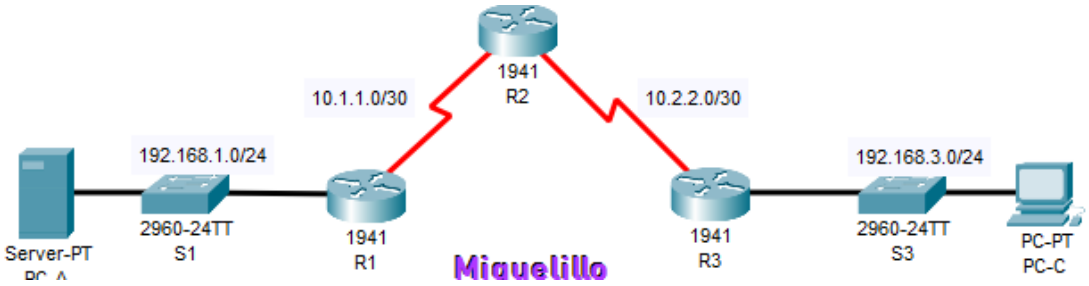
Comprobamos los matches



f) 8.6.5-packet-tracer---configure-ip-acls-to-mitigate-attacks

Solución:

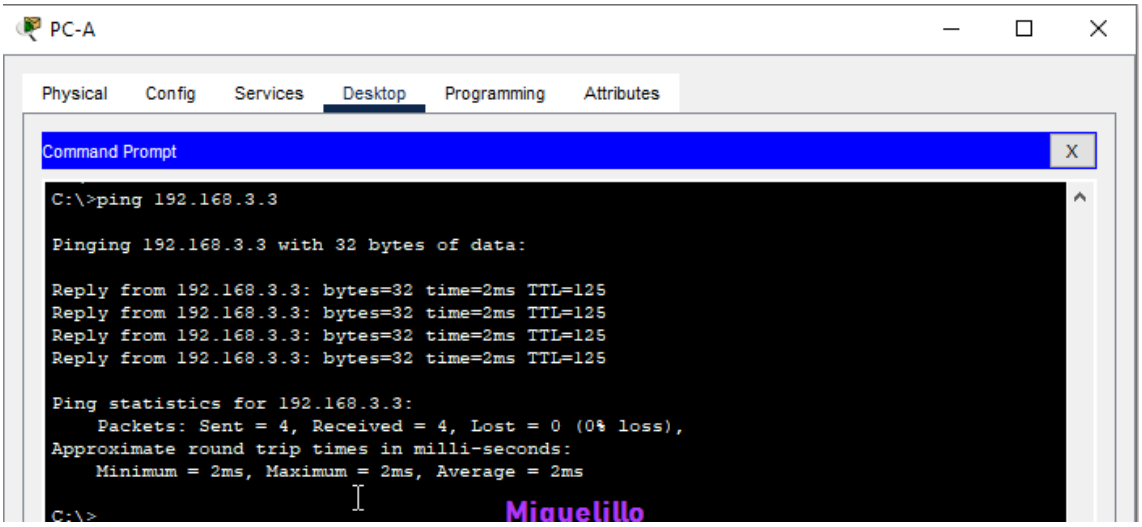
Escenario



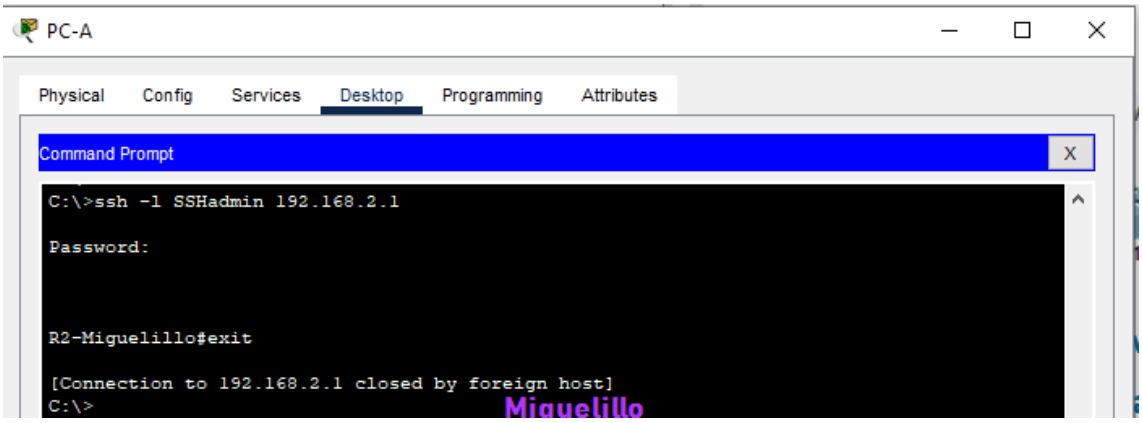
Parte 1: Verificar la Conectividad Básica de la Red

Paso 1: Desde PC-A, verifica la conectividad con PC-C y R2.

a. Desde la línea de comandos, realiza un ping a PC-C (192.168.3.3).

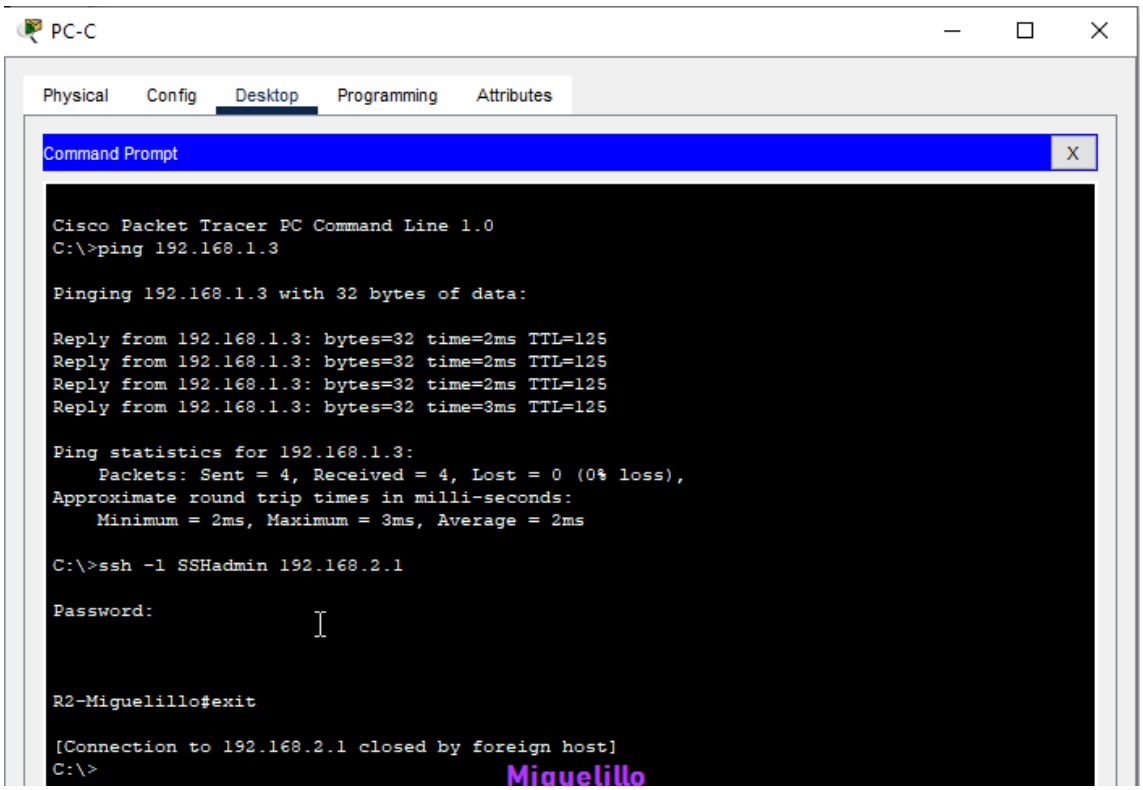


b. Desde la línea de comandos, establece una sesión SSH a la interfaz Lo0 de R2 (192.168.2.1) usando el nombre de usuario SSHadmin y la contraseña ciscosshpa55.



Paso 2: Desde PC-C, verifica la conectividad con PC-A y R2.

a. Desde la línea de comandos, realiza un ping a PC-A (192.168.1.3).
b. Desde la línea de comandos, establece una sesión SSH a la interfaz Lo0 de R2 (192.168.2.1) usando el nombre de usuario SSHadmin y la contraseña ciscosshpa55.

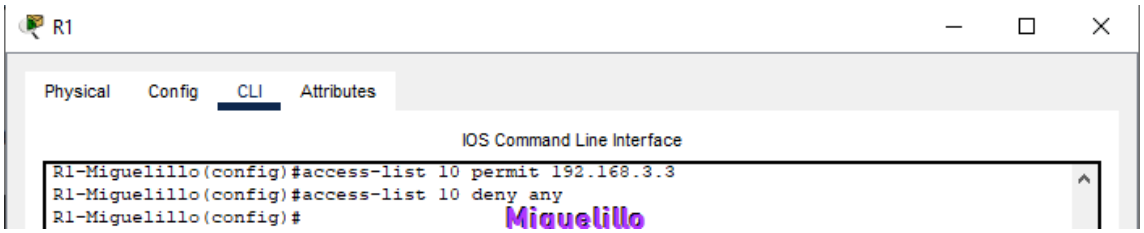


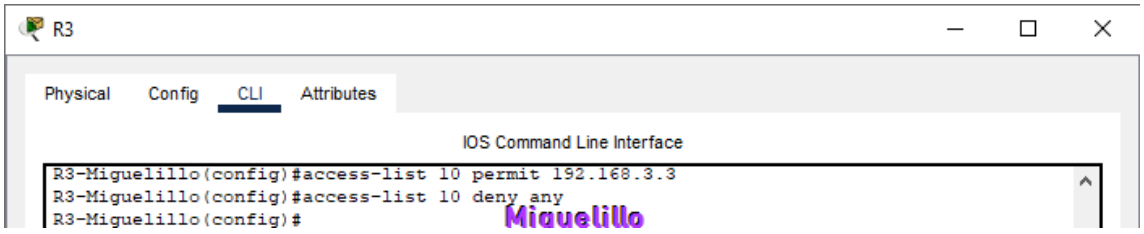
c. Abre un navegador web hacia el servidor PC-A (192.168.1.3) para mostrar la página web. Cierra el navegador cuando hayas terminado.

Parte 2: Acceso Seguro a los Routers

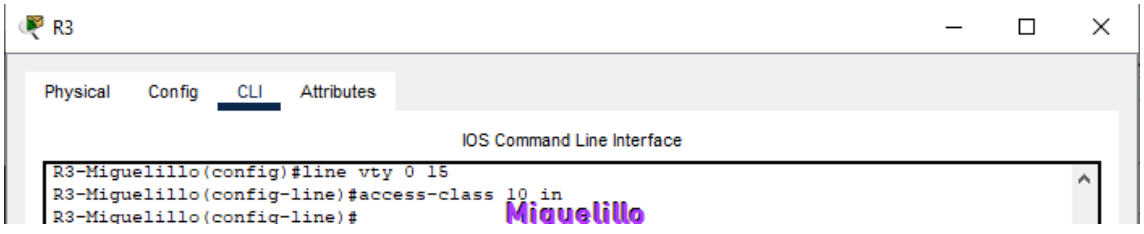
Paso 1: Configura la ACL 10 para bloquear todo el acceso remoto a los routers excepto desde PC-C.

a. Utiliza el comando access-list para crear una ACL numerada en R1, R2 y R3.



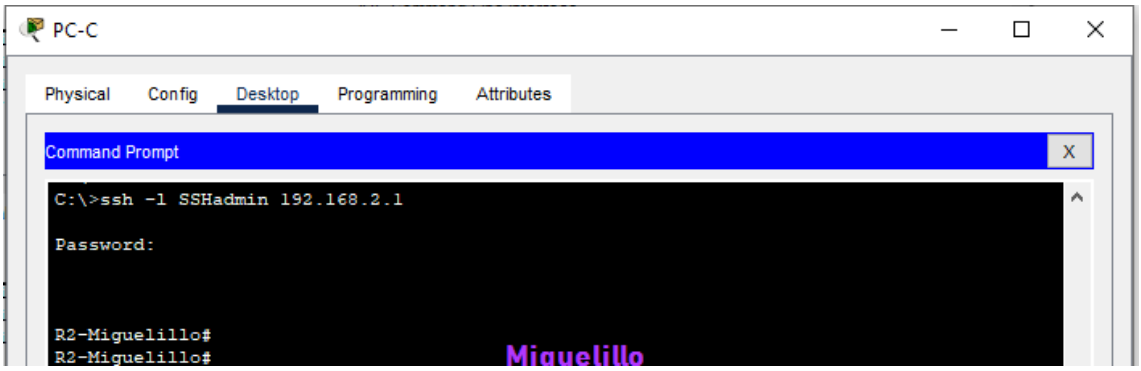


Paso 2: Aplica la ACL 10 al tráfico de entrada en las líneas VTY.



Paso 3: Verifica el acceso exclusivo desde la estación de administración PC-C.

a. Establece una sesión SSH a 192.168.2.1 desde PC-C (debería tener éxito).

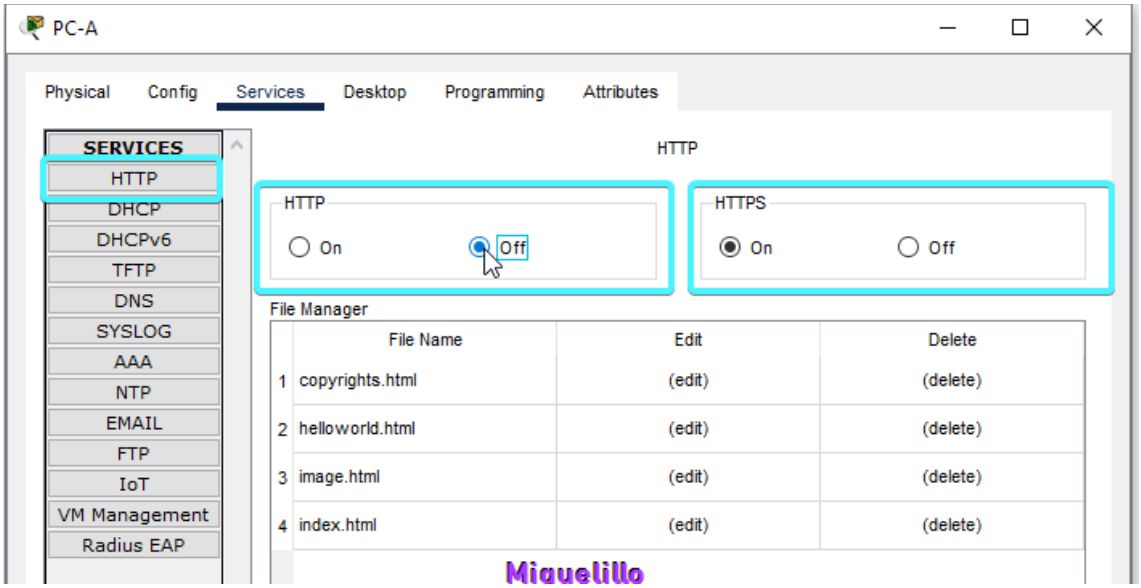


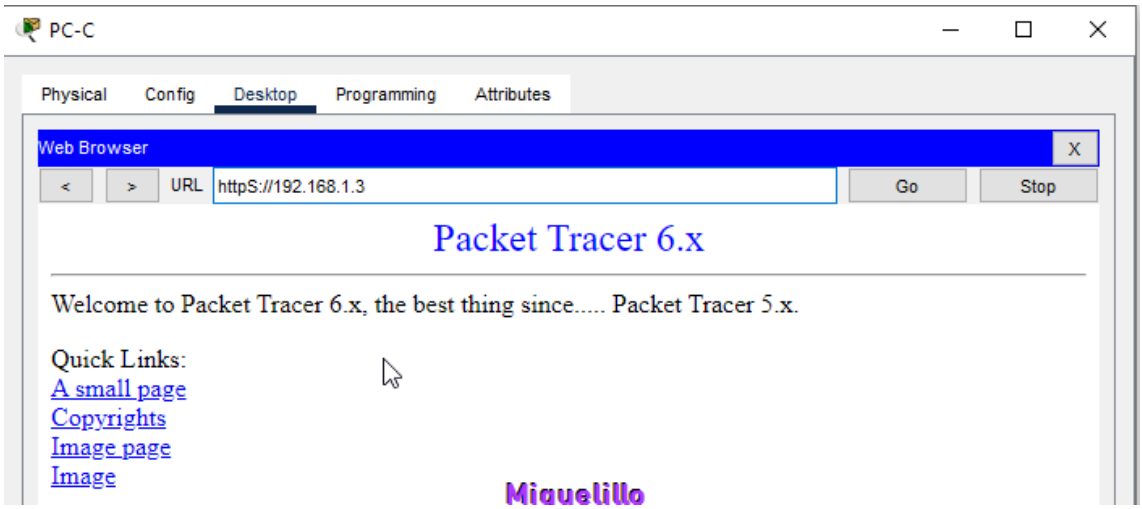
b. Establece una sesión SSH a 192.168.2.1 desde PC-A (debería fallar).

Parte 3: Crea una ACL Numerada 120 en R1

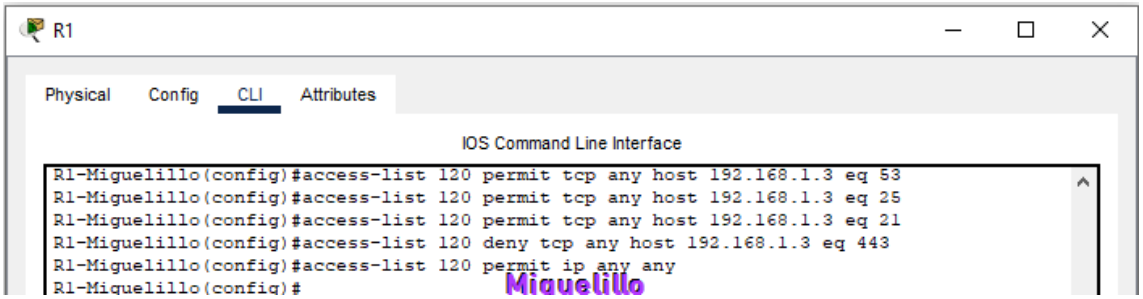
- Permitir que cualquier host externo acceda a los servicios DNS, SMTP y FTP en el servidor PC-A.
- Denegar el acceso de cualquier host externo a los servicios HTTPS en PC-A.
- Permitir a PC-C acceder a R1 a través de SSH.

Paso 1: Verifica que PC-C pueda acceder al PC-A a través de HTTPS utilizando el navegador web.

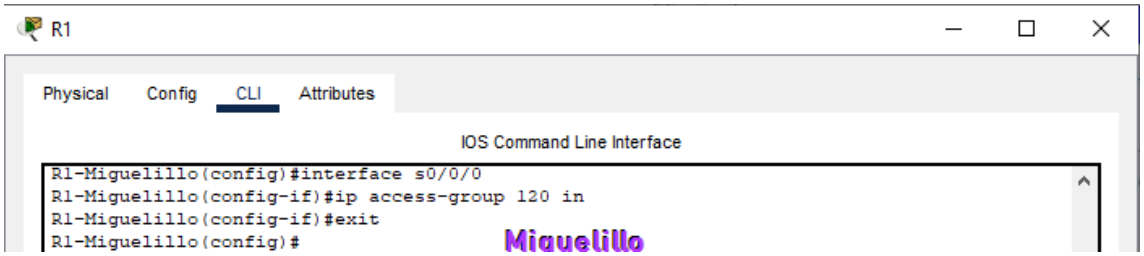




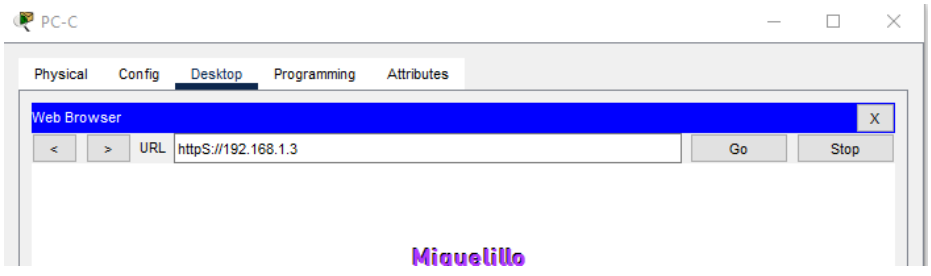
Paso 2: Configura la ACL 120 para permitir y denegar específicamente el tráfico.



Paso 3: Aplica la ACL a la interfaz S0/0/0.



Paso 4: Verifica que PC-C no pueda acceder a PC-A a través de HTTPS usando el navegador web.



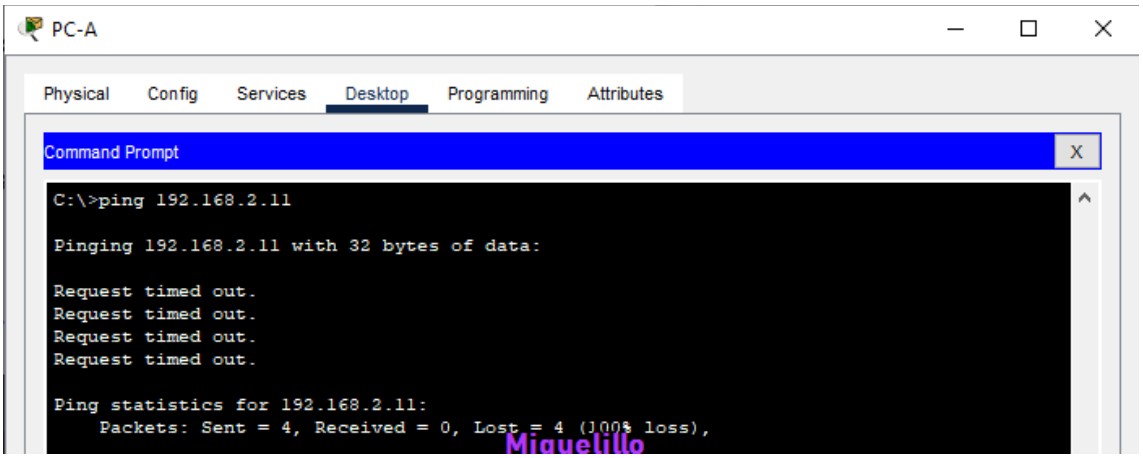

```
R1-Miguelillo#show access-lists
Standard IP access list 10
    10 permit host 192.168.3.3
    20 deny any
Extended IP access list 120
    10 permit tcp any host 192.168.1.3 eq domain
    20 permit tcp any host 192.168.1.3 eq smtp
    30 permit tcp any host 192.168.1.3 eq ftp
    40 deny tcp any host 192.168.1.3 eq 443 (141 match(es))
    50 permit ip any any
```

Miguelillo

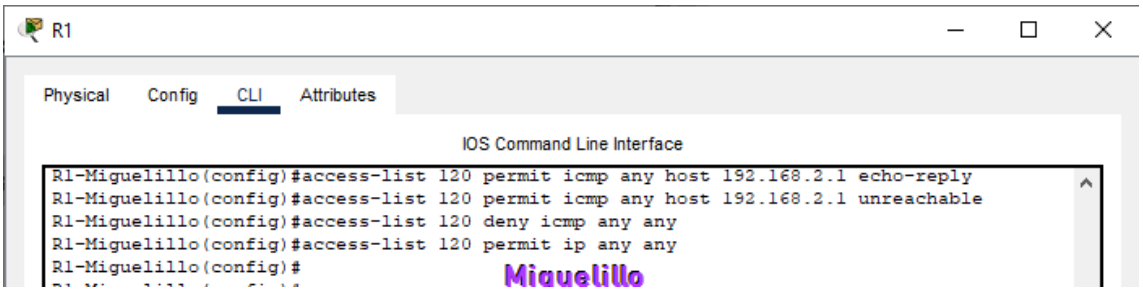
Parte 4: Modifica una ACL Existente en R1

Permite respuestas de eco ICMP y mensajes de inaccesibilidad de destino desde la red externa (en relación con R1). Deniega todos los demás paquetes ICMP entrantes.

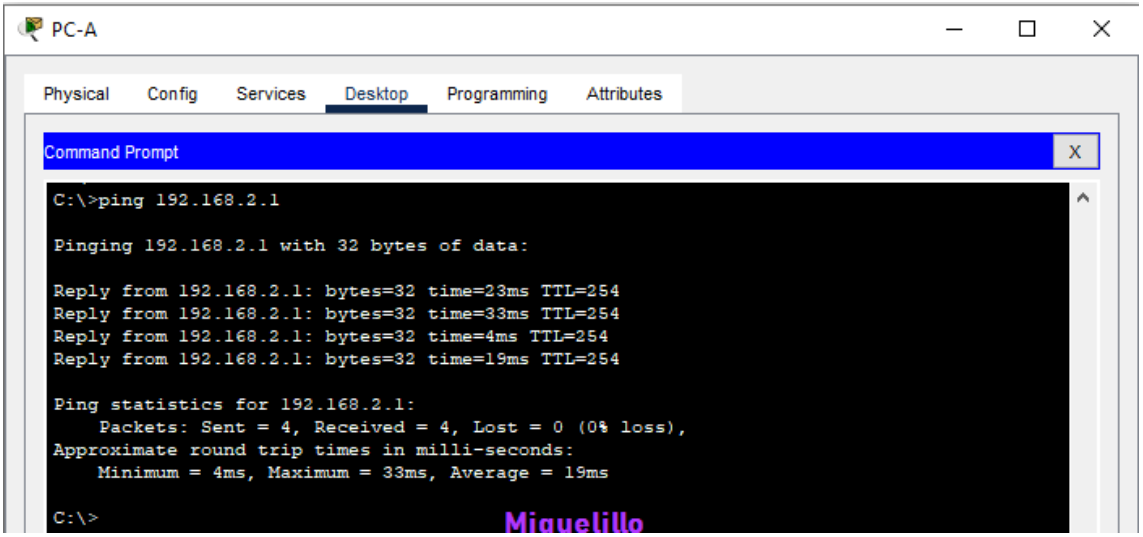
Paso 1: Verifica que PC-A no pueda hacer ping exitosamente a la interfaz loopback en R2.



Paso 2: Realiza los cambios necesarios en la ACL 120 para permitir y denegar el tráfico especificado.



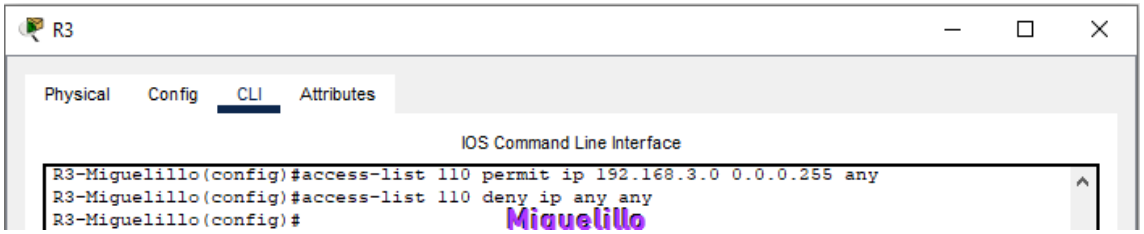
Paso 3: Verifica que PC-A pueda hacer ping exitosamente a la interfaz loopback en R2.



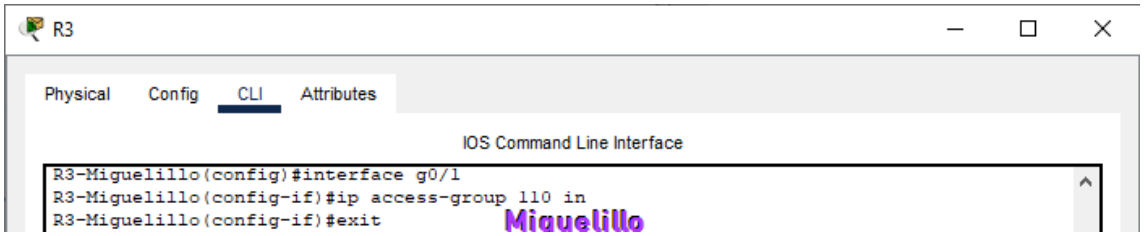
Parte 5: Crea una ACL Numerada 110 en R3

Deniega todos los paquetes de salida con dirección fuente fuera del rango de direcciones IP internas en R3.

Paso 1: Configura la ACL 110 para permitir solo tráfico desde la red interna.



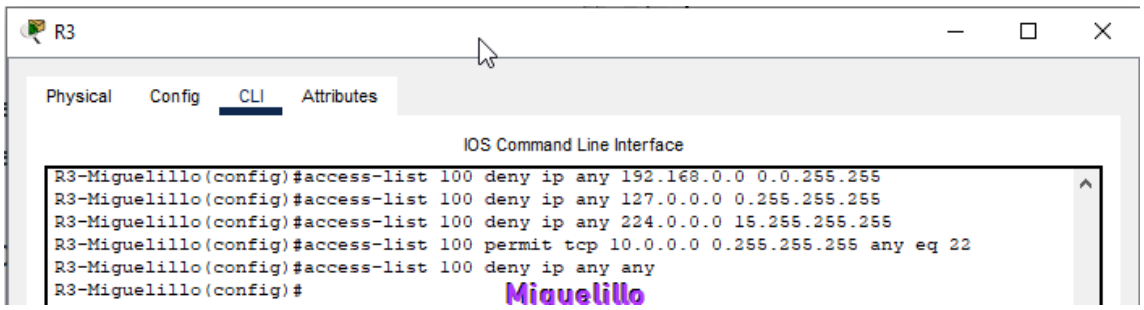
Paso 2: Aplica la ACL a la interfaz G0/1



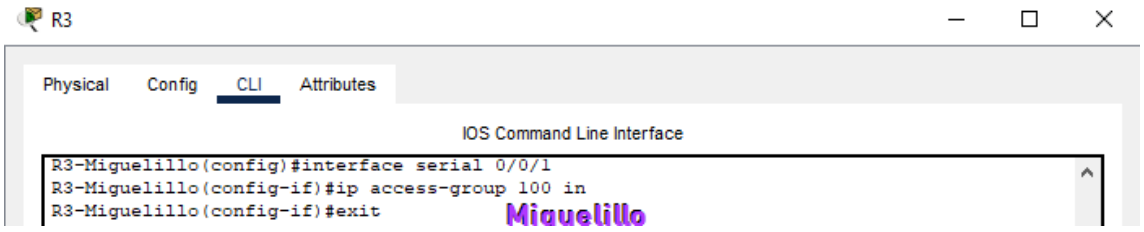
Parte 6: Crear una ACL numerada 100 en R3

En R3, bloquea todos los paquetes de cualquier dirección privada RFC 1918, 127.0.0.0/8 y cualquier dirección IP de multidifusión. Dado que PC-C se utiliza para administración remota, permite el tráfico SSH desde la red 10.0.0.0/8 para que pueda regresar al host PC-C.

Paso 1: Configurar la ACL 100 para bloquear todo el tráfico especificado desde la red externa.

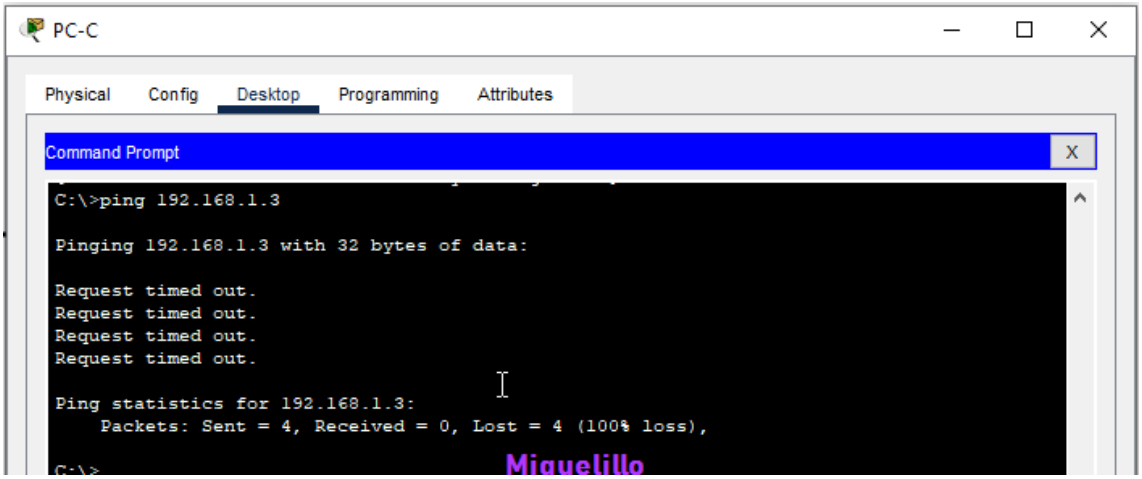


Paso 2: Aplicar la ACL en la interfaz Serial 0/0/1



Paso 3: Confirmar que el tráfico especificado que entra en la interfaz Serial 0/0/1 se maneja correctamente.

a. Desde la línea de comandos de PC-C, haz ping al servidor PC-A. (debería fallar)

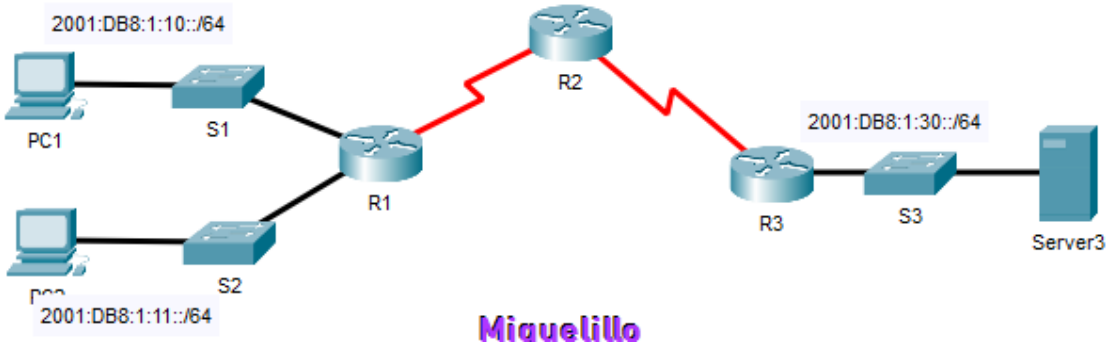


b. Intenta establecer una sesión SSH a 192.168.2.1 desde PC-C. (debería fallar)

g) 8.7.4-packet-tracer---configure-ipv6-acls

Solución:

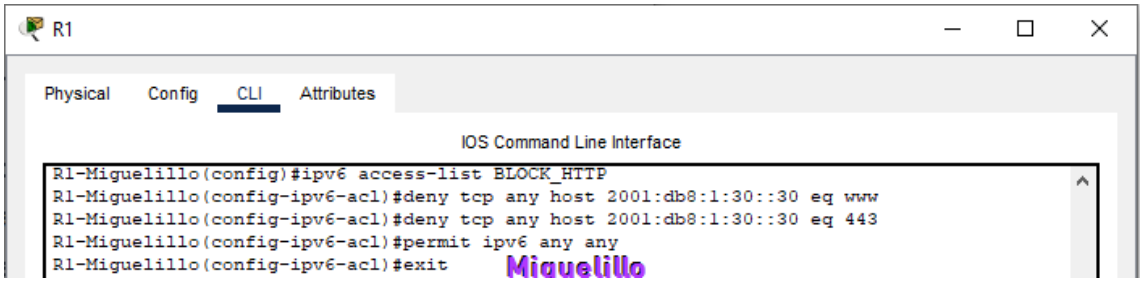
Escenario



Parte 1: Configurar, Aplicar y Verificar un ACL IPv6

Los registros indican que una computadora en la red 2001:db8:1:11::0/64 está actualizando repetidamente una página web. Esto está causando un ataque de Denegación de Servicio (DoS) contra Server3. Hasta que el cliente pueda ser identificado y limpiado, debes bloquear el acceso HTTP y HTTPS a esa red con una lista de acceso.

Paso 1: Configurar un ACL que bloqueará el acceso HTTP y HTTPS.



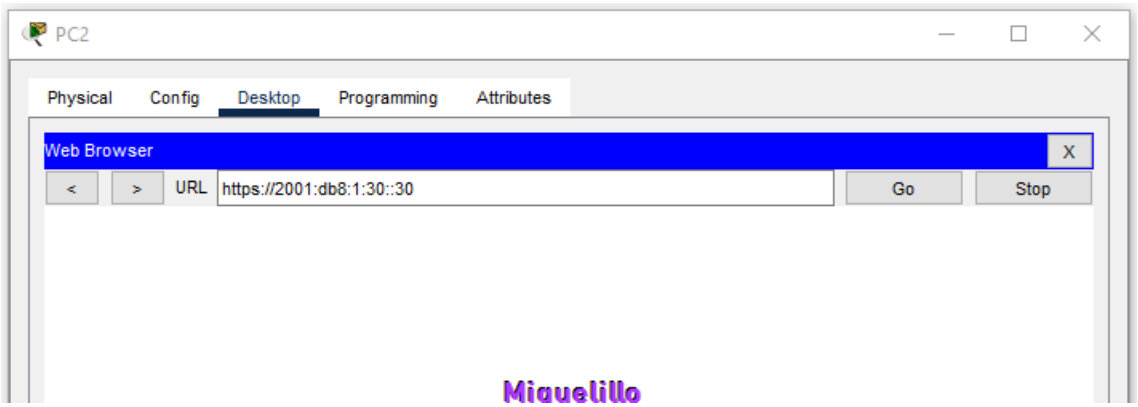
Paso 2: Aplicar el ACL en la interfaz correcta.

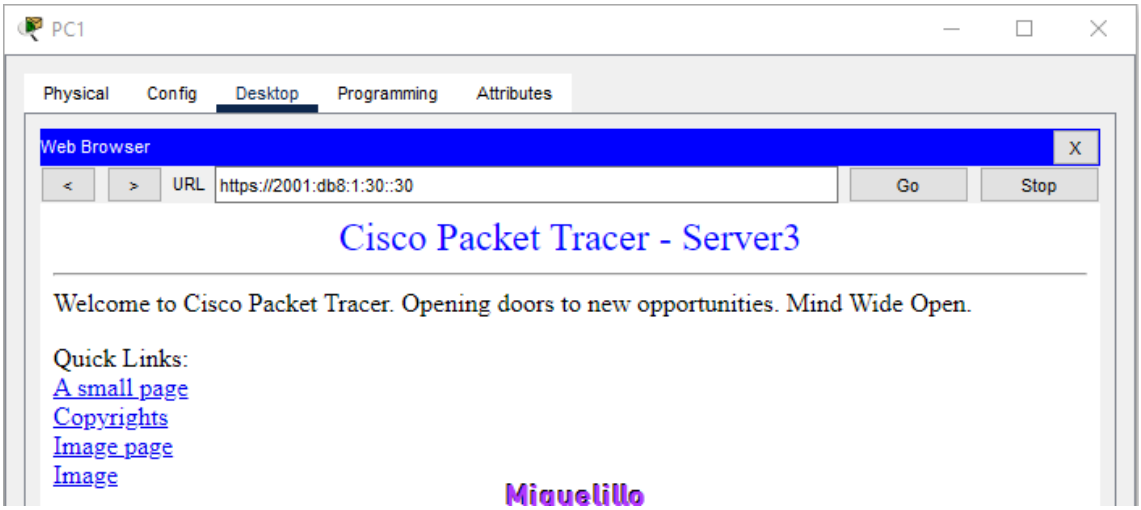
Paso 3: Verificar la implementación del ACL.

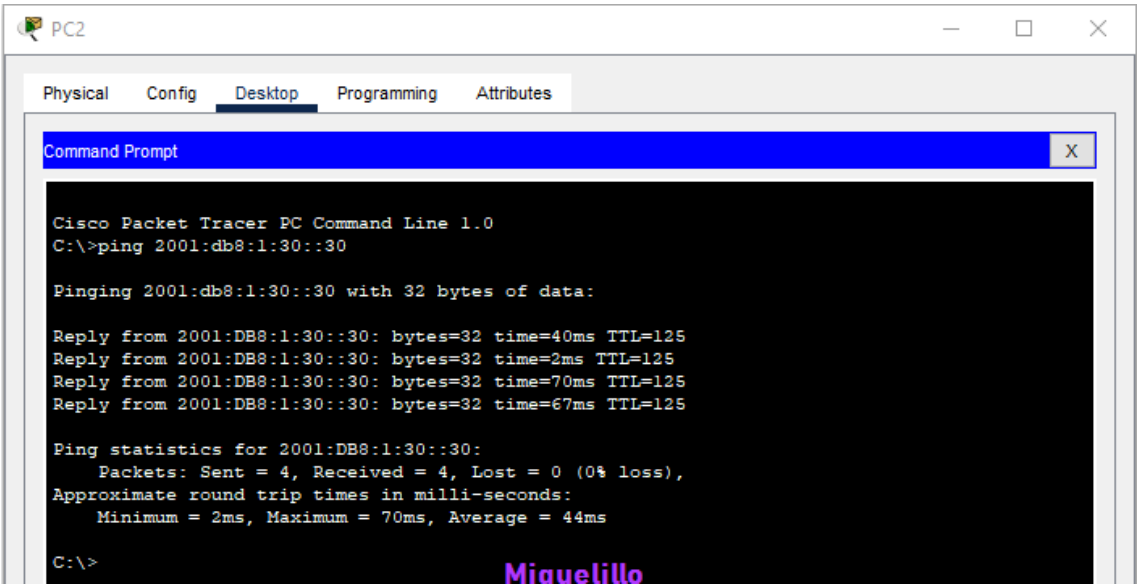
Abre el navegador web de PC1 a http://2001:db8:1:30::30 o https://2001:db8:1:30::30. El sitio web debería aparecer.

Abre el navegador web de PC2 a http://2001:db8:1:30::30 o https://2001:db8:1:30::30. El sitio web debería estar bloqueado.

Realiza un ping desde PC2 a 2001:db8:1:30::30. El ping debería ser exitoso.


PC2
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
https://2001:db8:1:30::30
Go
Stop
Miguelillo

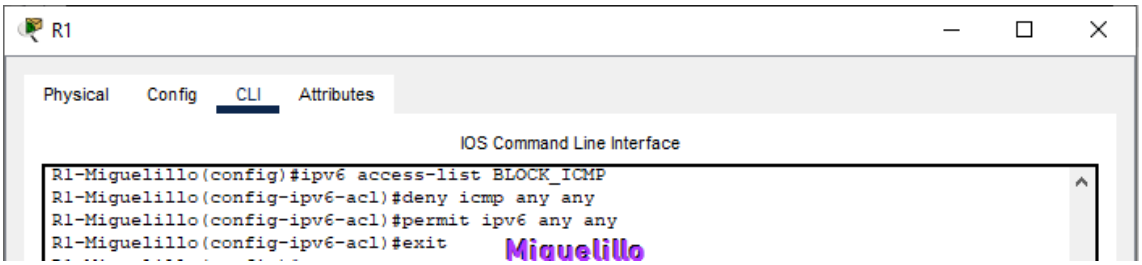

PC1
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
https://2001:db8:1:30::30
Go
Stop
Cisco Packet Tracer - Server3
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image
Miguelillo


PC2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 2001:db8:1:30::30
Pinging 2001:db8:1:30::30 with 32 bytes of data:
Reply from 2001:DB8:1:30::30: bytes=32 time=40ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=70ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=67ms TTL=125
Ping statistics for 2001:DB8:1:30::30:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 70ms, Average = 44ms
C:\>
Miguelillo

Parte 2: Configurar, Aplicar y Verificar un Segundo ACL IPv6

Los registros ahora indican que tu servidor está recibiendo pings desde muchas direcciones IPv6 diferentes en un ataque de Denegación de Servicio Distribuido (DDoS). Debes filtrar las solicitudes de ping ICMP a tu servidor.

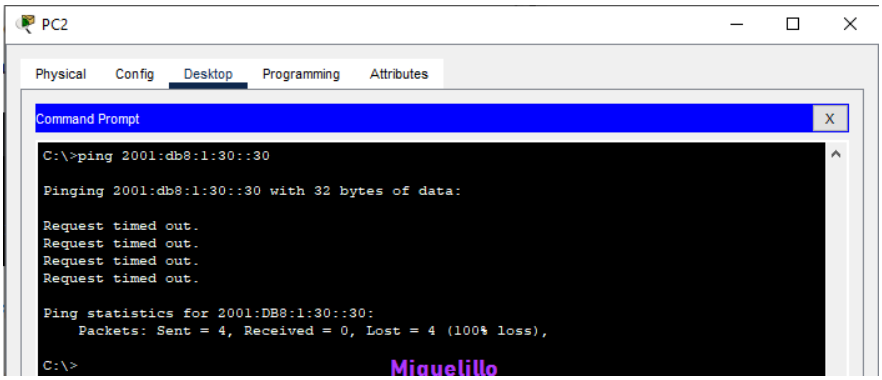
Paso 1: Crear una lista de acceso para bloquear ICMP.



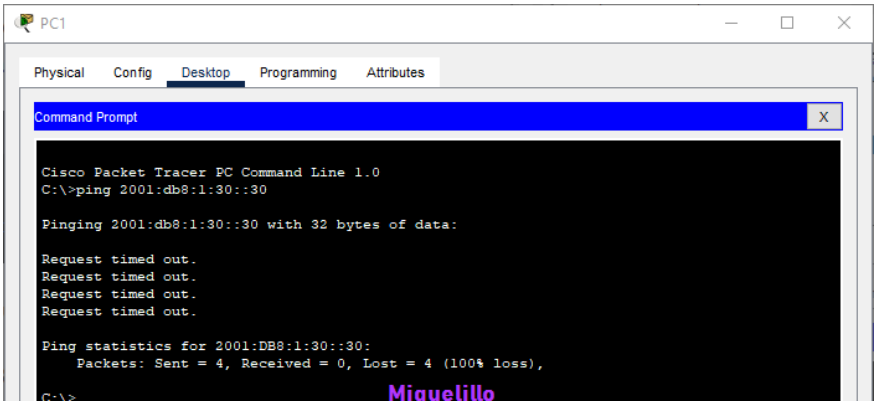
Paso 2: Aplicar el ACL en la interfaz correcta.

Paso 3: Verificar que la lista de acceso funcione correctamente.

a. Realiza un ping desde PC2 a 2001:db8:1:30::30. El ping debería fallar.



b. Realiza un ping desde PC1 a 2001:db8:1:30::30. El ping debería fallar.



c. Abre el navegador web de PC1 a http://2001:db8:1:30::30 o https://2001:db8:1:30::30. El sitio web debería mostrarse.