

Índice:

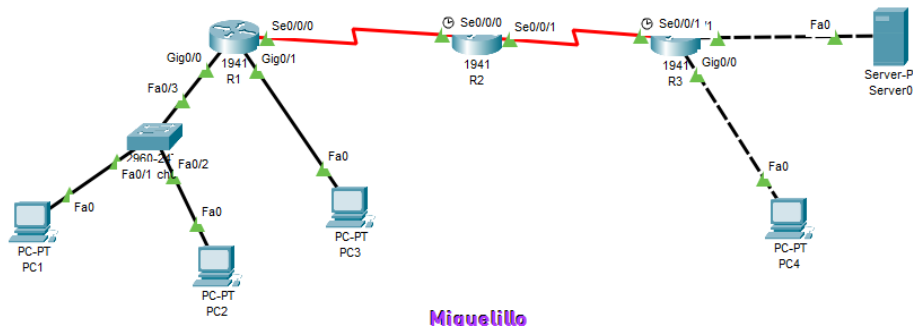
Ejercicio ACL Cisco	2
a) 8.1.5-packet-tracer---acl-demonstration	2
b) 8.5.5-packet-tracer---configure-named-standard-ipv4-acls	6
c) 8.5.6-packet-tracer---configure-numbered-standard-ipv4-acls	9
d) 8.5.12-packet-tracer---configure-extended-ipv4-acls---scenario-1	13
e) 8.5.13-packet-tracer---configure-extended-ipv4-acls---scenario-2	20
f) 8.6.5-packet-tracer---configure-ip-acls-to-mitigate-attacks	26
g) 8.7.4-packet-tracer---configure-ipv6-acls	34

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 bloquea a esa red cuando sale por el serial0/0/0

```

C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.11:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

Control-C
^C
C:\>ping 192.168.11.10

Pinging 192.168.11.10 with 32 bytes of data:

Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.11.10:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
  
```

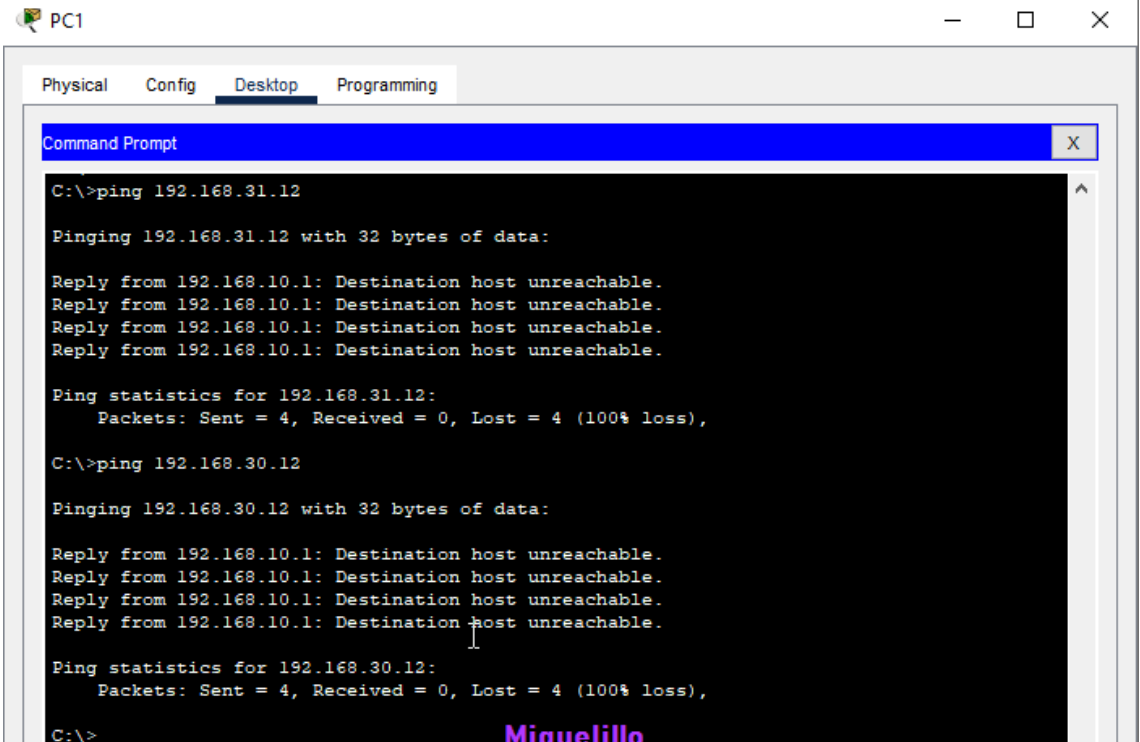
Miquelillo

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

- Desde PC1, haz ping a PC4.
- 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



The screenshot shows a PC1 desktop environment with a 'Command Prompt' window open. The window displays the results of two ping commands. Both pings failed with 100% loss. The first ping was to 192.168.31.12 and the second was to 192.168.30.12. The output for both is identical: 'Pinging 192.168.10.1: Destination host unreachable.' followed by 'Ping statistics for 192.168.10.1: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),'. The name 'Miguelillo' is written in purple at the bottom right of the window.

```
C:\>ping 192.168.31.12

Pinging 192.168.31.12 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.31.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.30.12

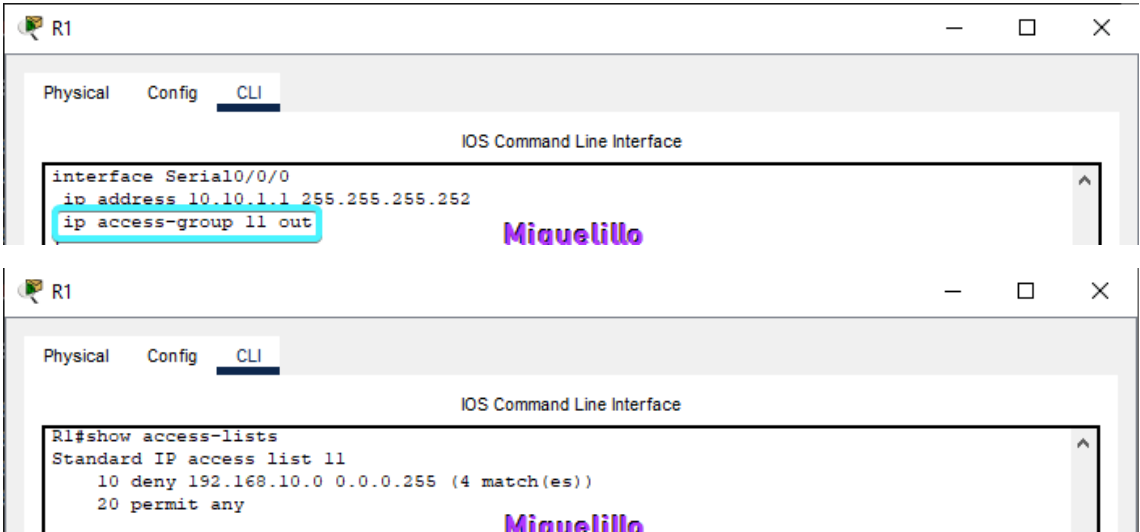
Pinging 192.168.30.12 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.30.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

ACL implicada



The first screenshot shows the configuration of an ACL on R1. The CLI shows the command 'ip access-group 11 out' being entered under the 'interface Serial0/0/0' configuration. The name 'Miguelillo' is written in purple at the bottom right. The second screenshot shows the verification of the ACL configuration using the 'show access-lists' command. The output shows 'Standard IP access list 11' with two entries: '10 deny 192.168.10.0 0.0.0.255 (4 match(es))' and '20 permit any'. The name 'Miguelillo' is written in purple at the bottom right.

```
interface Serial0/0/0
ip address 10.10.1.1 255.255.255.252
ip access-group 11 out
```

```
R1#show access-lists
Standard IP access list 11
 10 deny 192.168.10.0 0.0.0.255 (4 match(es))
 20 permit any
```

PARTE 2

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

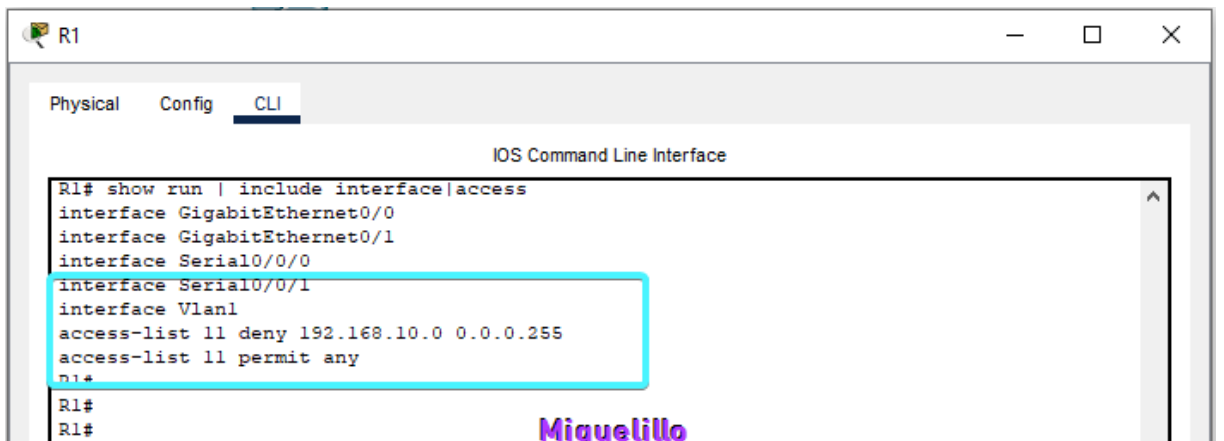
a) Utilizar comandos show para investigar la configuración de la ACL



```
R1#show access-lists ?
<1-199>  ACL number
WORD      ACL name
|         Output Modifiers
<cr>
R1#show access-lists
Standard IP access list 11
 10 deny 192.168.10.0 0.0.0.255 (15 match(es))
 20 permit any
```

Miguelillo

b) para ver las interfaces que tiene una ACL asignada

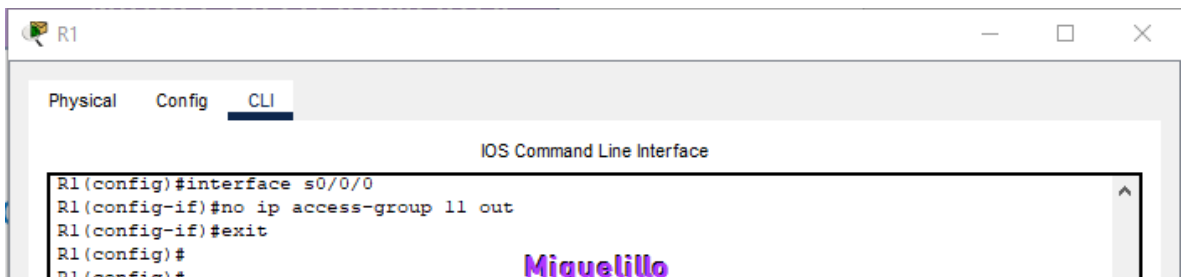


```
R1# show run | include interface|access
interface GigabitEthernet0/0
interface GigabitEthernet0/1
interface Serial0/0/0
interface Serial0/0/1
interface Vlan1
access-list 11 deny 192.168.10.0 0.0.0.255
access-list 11 permit any
R1#
```

Miguelillo

Paso 2

a) Quitamos la ACL



```
R1(config)#interface s0/0/0
R1(config-if)#no ip access-group 11 out
R1(config-if)#exit
R1(config)#
```

Miguelillo

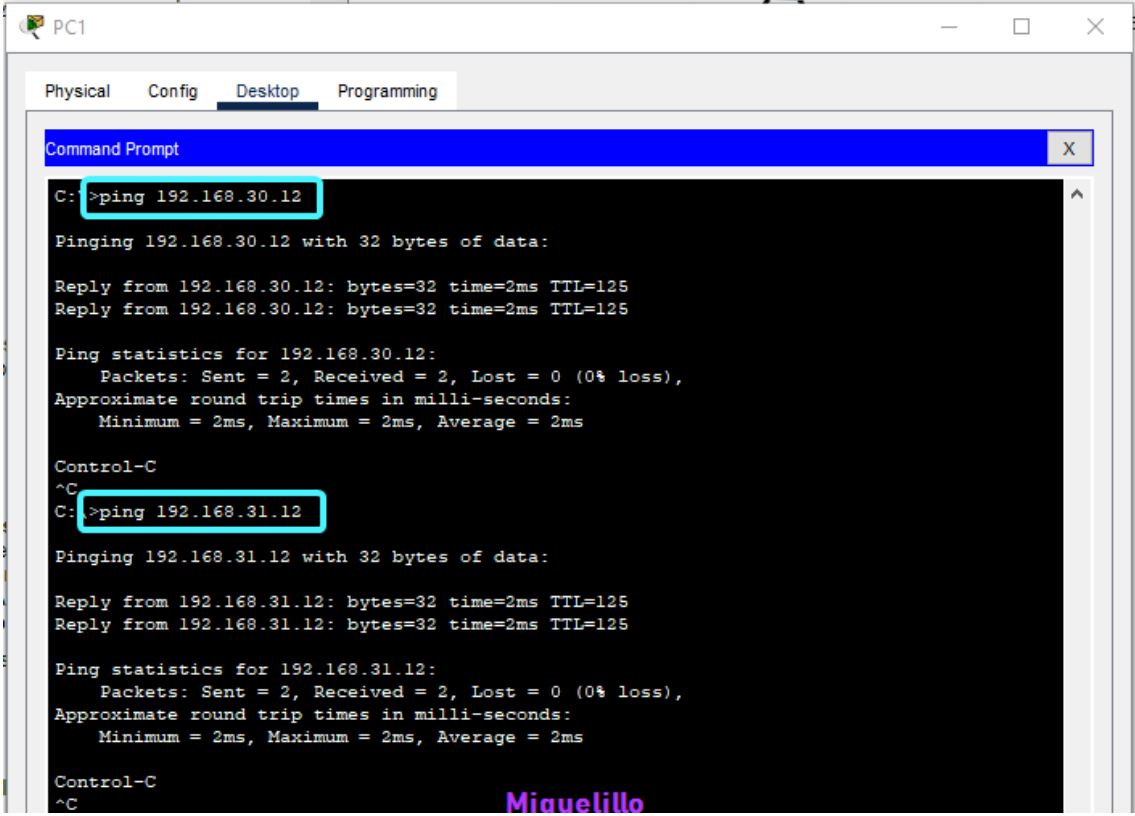
b) En modo de configuración global, elimina la ACL



```
R1(config)#no access-list 11
R1(config)#
```

Miguelillo

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



The screenshot shows a Packet Tracer interface with a PC1 icon in the top left. The 'Desktop' tab is selected, displaying a 'Command Prompt' window. The window has a blue title bar with 'Command Prompt' and a close button. The command prompt shows two ping commands being executed. The first command is 'ping 192.168.30.12', which is highlighted with a red rectangle. The output shows successful pings with 2ms response times. The second command is 'ping 192.168.31.12', also highlighted with a red rectangle. The output shows successful pings with 2ms response times. The text 'Miguelillo' is written in red at the bottom right of the command prompt window.

```
C:\>ping 192.168.30.12

Pinging 192.168.30.12 with 32 bytes of data:

Reply from 192.168.30.12: bytes=32 time=2ms TTL=125
Reply from 192.168.30.12: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.30.12:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

Control-C
^C
C:\>ping 192.168.31.12

Pinging 192.168.31.12 with 32 bytes of data:

Reply from 192.168.31.12: bytes=32 time=2ms TTL=125
Reply from 192.168.31.12: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.31.12:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

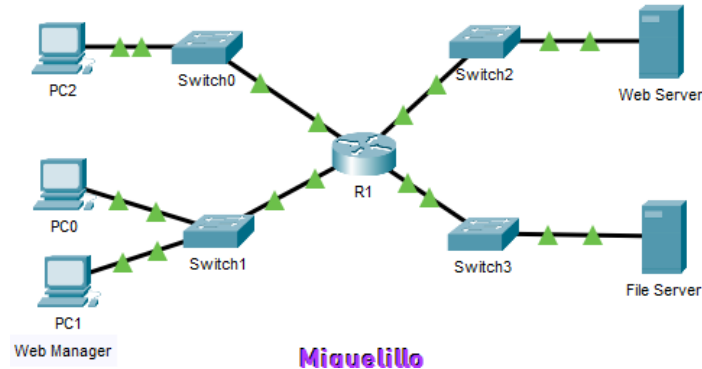
Control-C
^C
```

Miguelillo

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

Solución:

Escenario



Parte 1

Paso 1 Verificar 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.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

Control-C
^C
C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=27ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 27ms, Average = 13ms

Control-C
^C
C:\>ping 192.168.10.3

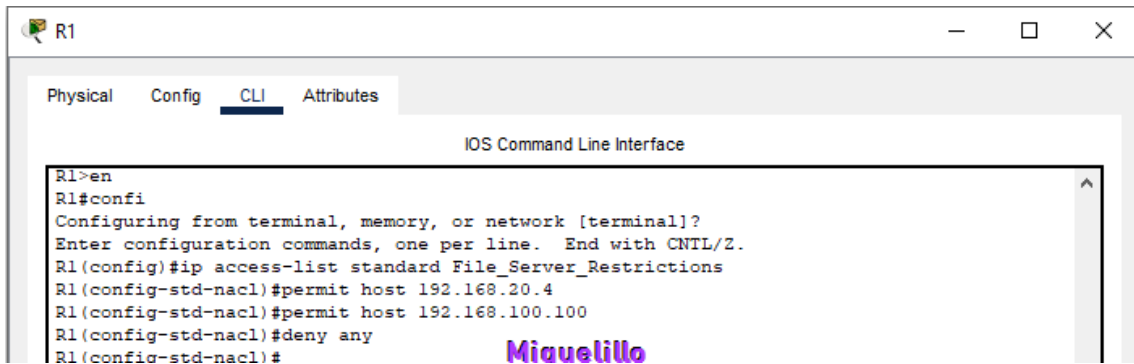
Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time=7ms TTL=127
Reply from 192.168.10.3: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.10.3:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
  
```

Paso 2 configura la ACL

a. Configura la siguiente ACL nombrada en R1.



```
R1>en
R1#confi
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip access-list standard File_Server_Restrictions
R1(config-std-nacl)#permit host 192.168.20.4
R1(config-std-nacl)#permit host 192.168.100.100
R1(config-std-nacl)#deny any
R1(config-std-nacl)#
```

Miquelillo

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

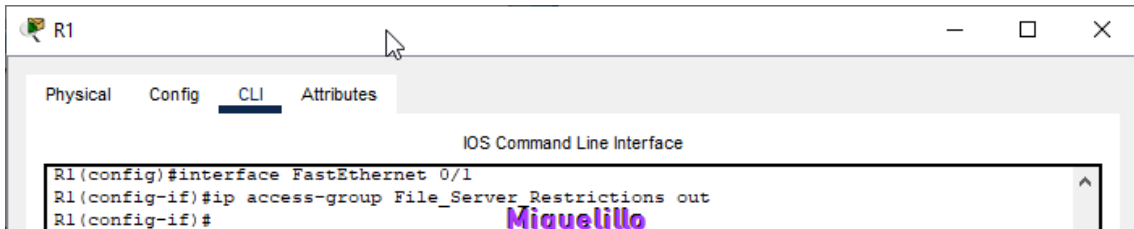


```
R1#show access-lists
Standard IP access list File_Server_Restrictions
 10 permit host 192.168.20.4
 20 permit host 192.168.100.100
 30 deny any
```

Miquelillo

Paso 3: Aplicar la ACL nombrada.

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



```
R1(config)#interface FastEthernet 0/1
R1(config-if)#ip access-group File_Server_Restrictions out
R1(config-if)#
```

Miquelillo

b. Guarda la configuración.



```
R1#write
Building configuration...
[OK]
```

Miquelillo

Parte 2

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

```

R1#show access-lists
Standard IP access list File_Server_Restrictions
 10 permit host 192.168.20.4
 20 permit host 192.168.100.100
 30 deny any

R1#show run | include interface | access
interface FastEthernet0/0
interface FastEthernet0/1
ip access-group File_Server_Restrictions out
interface Ethernet0/0/0
interface Ethernet0/1/0
interface Vlan1
ip access-list standard File_Server_Restrictions
R1#
  
```

Miguelillo

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)

Miguelillo

```

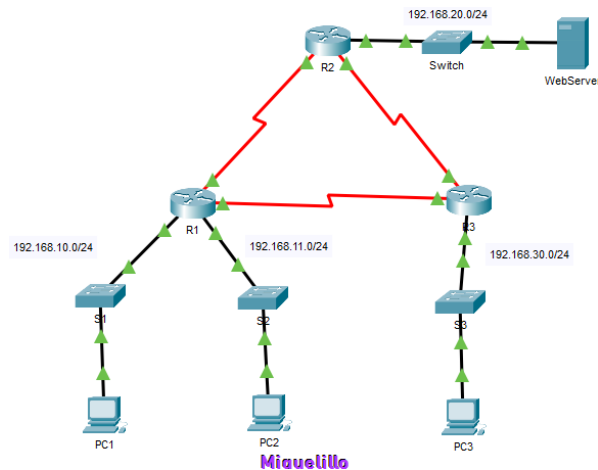
R1#show access-lists
Standard IP access list File_Server_Restrictions
 10 permit host 192.168.20.4 (2 match(es))
 20 permit host 192.168.100.100 (1 match(es))
 30 deny any (3 match(es))
  
```

Miguelillo

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)

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.

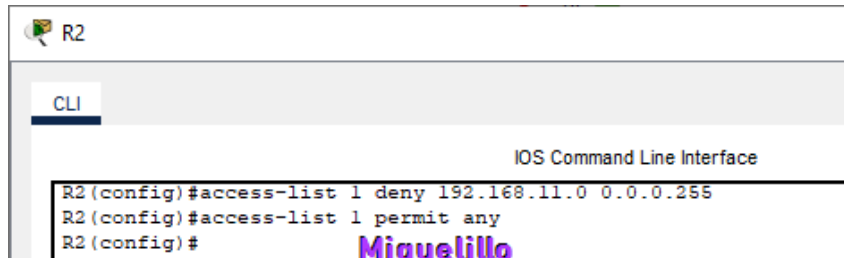
R3

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

Se permite todo otro acceso.

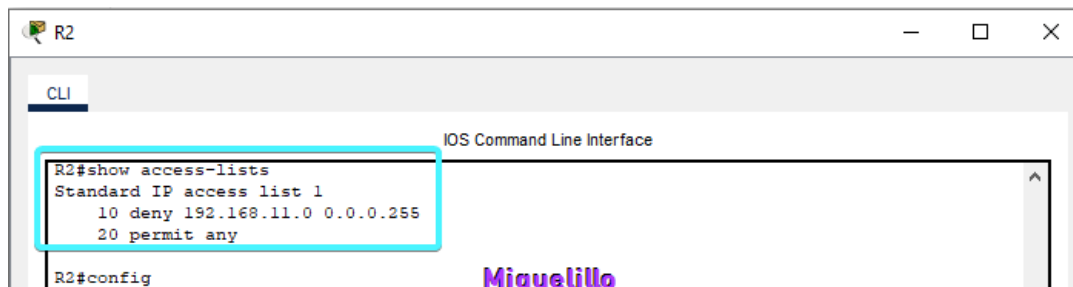
Parte 2 Configurar, Aplicar y Verificar una ACL Estándar Numerada**Paso 1:** Configurar y aplicar una ACL estándar numerada en R2.

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



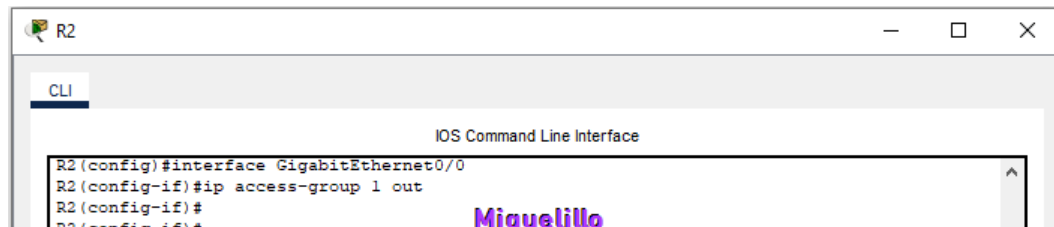
```
R2
CLI
IOS Command Line Interface
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 1 permit any
R2(config)#
```

- 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.



```
R2
CLI
IOS Command Line Interface
R2#show access-lists
Standard IP access list 1
  10 deny 192.168.11.0 0.0.0.255
  20 permit any
R2#config
```

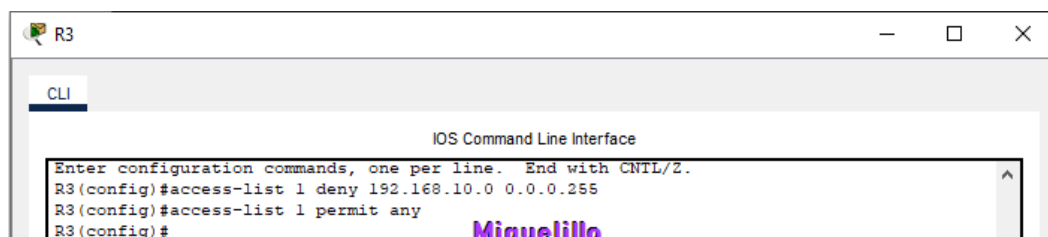
- Aplica la ACL colocándola para el tráfico de salida en la interfaz GigabitEthernet 0/0.



```
R2
CLI
IOS Command Line Interface
R2(config)#interface GigabitEthernet0/0
R2(config-if)#ip access-group 1 out
R2(config-if)#
```

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

- 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.
- 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.



```
R3
CLI
IOS Command Line Interface
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 1 deny 192.168.10.0 0.0.0.255
R3(config)#access-list 1 permit any
R3(config)#
```

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



```

R3#show access-lists
Standard IP access list 1
 10 deny 192.168.10.0 0.0.0.255
 20 permit any
  
```

Miguelillo

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



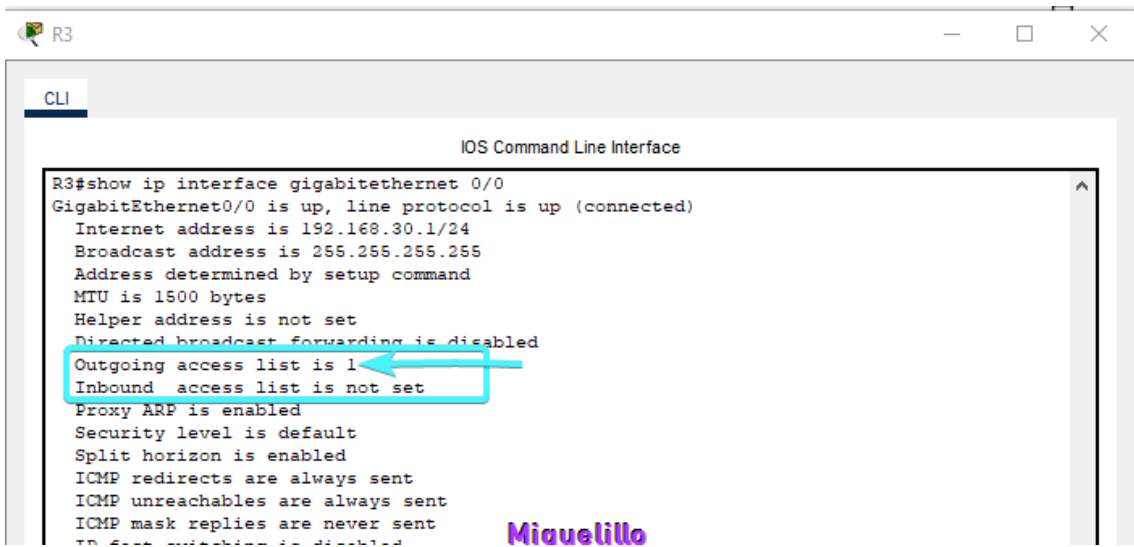
```

R3(config)#
R3(config)#interface GigabitEthernet0/0
R3(config-if)#ip access-group 1 out
R3(config-if)#
  
```

Miguelillo

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.



```

R3#show ip interface gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
 Internet address is 192.168.30.1/24
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Outgoing access list is 1
 Inbound access list is not set
 Proxy ARP is enabled
 Security level is default
 Split horizon is enabled
 ICMP redirects are always sent
 ICMP unreachable are always sent
 ICMP mask replies are never sent
  
```

Miguelillo

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

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

Miguelillo

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.



The image displays two screenshots of router CLI interfaces, one for R2 and one for R3. Both show the output of the `show access-lists` command, which lists the configured access lists and the number of matches for each line.

R2 CLI Output:

```
R2#show access-lists
Standard IP access list 1
 10 deny 192.168.11.0 0.0.0.255 (1 match(es))
 20 permit any (2 match(es))
```

R3 CLI Output:

```
R3#show access-lists
Standard IP access list 1
 10 deny 192.168.10.0 0.0.0.255 (1 match(es))
 20 permit any (2 match(es))
```

Both screenshots include a purple signature "Miguelillo" at the bottom right of the CLI window.

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

Solución:

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

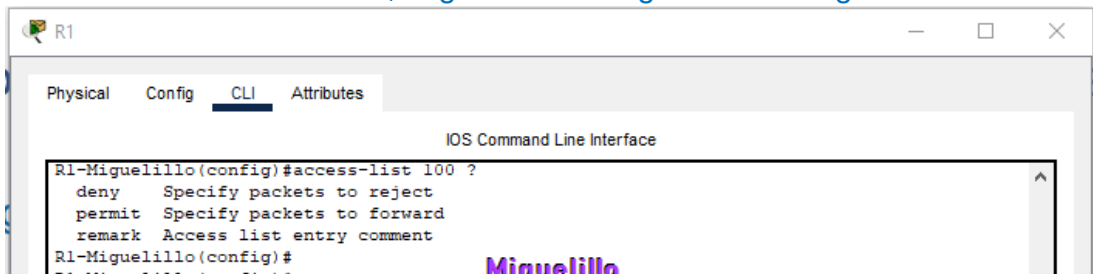
Paso 1: Configurar una ACL para permitir FTP e ICMP desde la LAN de PC1.

- 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.



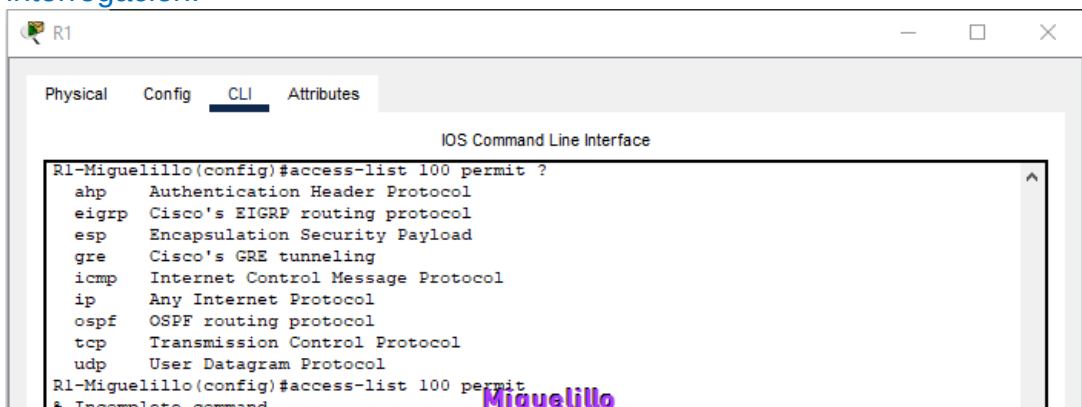
```
R1-Miguelillo(config)#access-list ?
<1-99>      IP standard access list
<100-199>   IP extended access list
R1-Miguelillo(config)#access-list
```

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



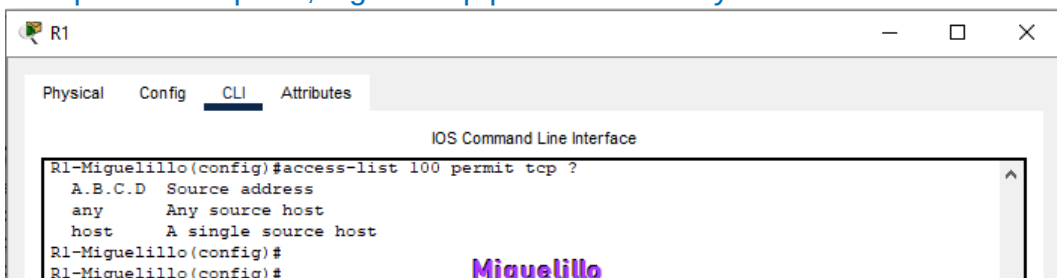
```
R1-Miguelillo(config)#access-list 100 ?
deny        Specify packets to reject
permit      Specify packets to forward
remark      Access list entry comment
R1-Miguelillo(config)#
```

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



```
R1-Miguelillo(config)#access-list 100 permit ?
ahp         Authentication Header Protocol
eigrp       Cisco's EIGRP routing protocol
esp         Encapsulation Security Payload
gre         Cisco's GRE tunneling
icmp        Internet Control Message Protocol
ip          Any Internet Protocol
ospf        OSPF routing protocol
tcp         Transmission Control Protocol
udp         User Datagram Protocol
R1-Miguelillo(config)#access-list 100 permit
* Incomplete command
```

- 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.



```
R1-Miguelillo(config)#access-list 100 permit tcp ?
A.B.C.D     Source address
any         Any source host
host        A single source host
R1-Miguelillo(config)#
R1-Miguelillo(config)#
```

- 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. Ingresar esta dirección de red, seguida de un signo de interrogación.



```

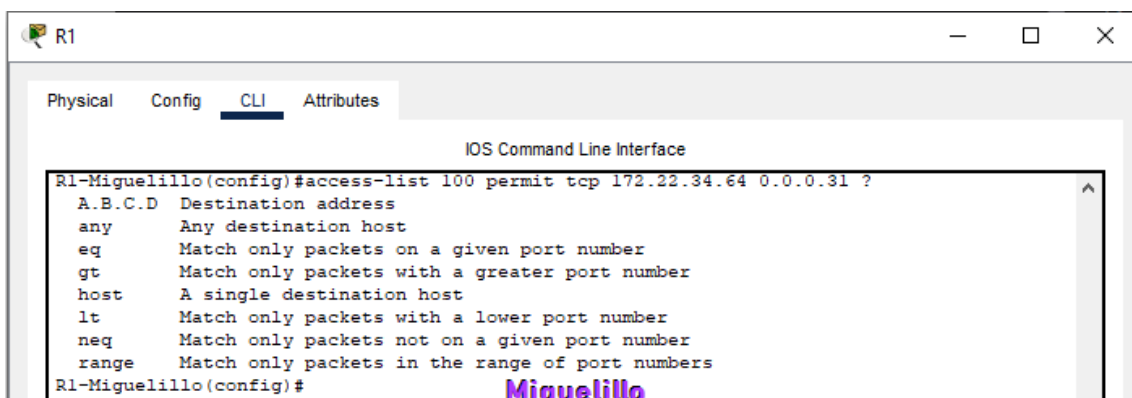
R1-Miguelillo(config)#access-list 100 permit tcp 172.22.34.64 ?
A.B.C.D Source wildcard bits
R1-Miguelillo(config)#
  
```

- 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

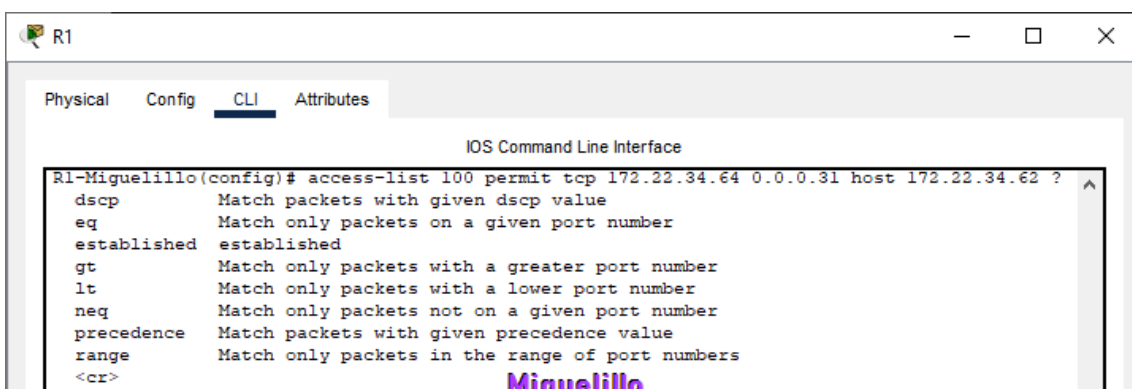
- g. Ingresar la máscara wildcard, seguida de un signo de interrogación.



```

R1-Miguelillo(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 ?
A.B.C.D Destination address
any Any destination host
eq Match only packets on a given port number
gt Match only packets with a greater port number
host A single destination host
lt Match only packets with a lower port number
neq Match only packets not on a given port number
range Match only packets in the range of port numbers
R1-Miguelillo(config)#
  
```

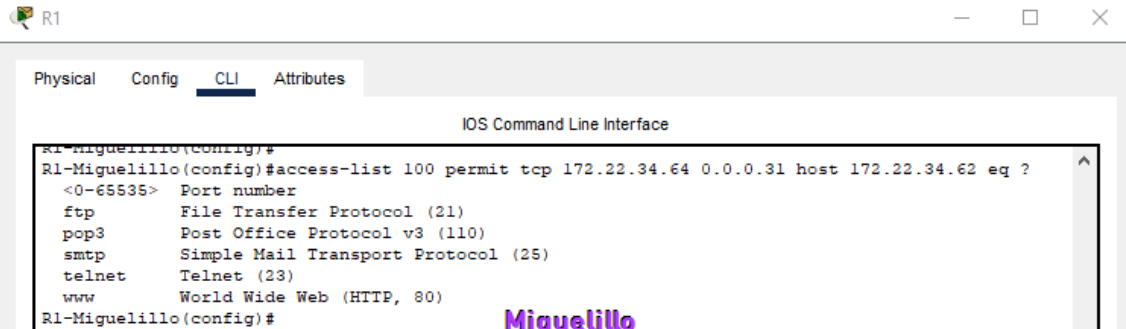
- h. Configura la dirección de destino. Ingresar la palabra clave host seguida de la dirección IP del servidor seguida de una interrogación



```

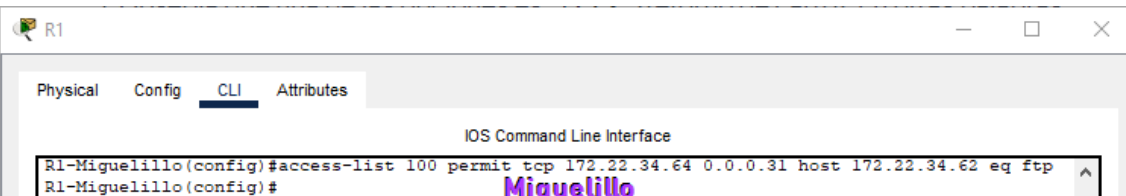
R1-Miguelillo(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 ?
dscp Match packets with given dscp value
eq Match only packets on a given port number
established established
gt Match only packets with a greater port number
lt Match only packets with a lower port number
neq Match only packets not on a given port number
precedence Match packets with given precedence value
range Match only packets in the range of port numbers
<cr>
R1-Miguelillo(config)#
  
```

- 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.



```

R1-Miguelillo(config)#
R1-Miguelillo(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ?
<0-65535> Port number
ftp      File Transfer Protocol (21)
pop3     Post Office Protocol v3 (110)
smtp     Simple Mail Transport Protocol (25)
telnet   Telnet (23)
www      World Wide Web (HTTP, 80)
R1-Miguelillo(config)#
  
```



```

R1-Miguelillo(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
R1-Miguelillo(config)#
  
```

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



```

R1-Miguelillo(config)#access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
R1-Miguelillo(config)#
  
```

- k. Todo otro tráfico se deniega por defecto. Con lo cual no tenemos que poner ninguna directiva
- l. Ejecuta el comando show access-list y verifica que la lista de acceso 100 contiene las declaraciones correctas.



```

R1-Miguelillo#show access-lists
Extended IP access list 100
 10 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
 20 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
R1-Miguelillo#
  
```

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



```

R1-Miguelillo(config)#interface gigabitEthernet 0/0
R1-Miguelillo(config-if)#ip access-group 100 in
R1-Miguelillo(config-if)#exit
  
```

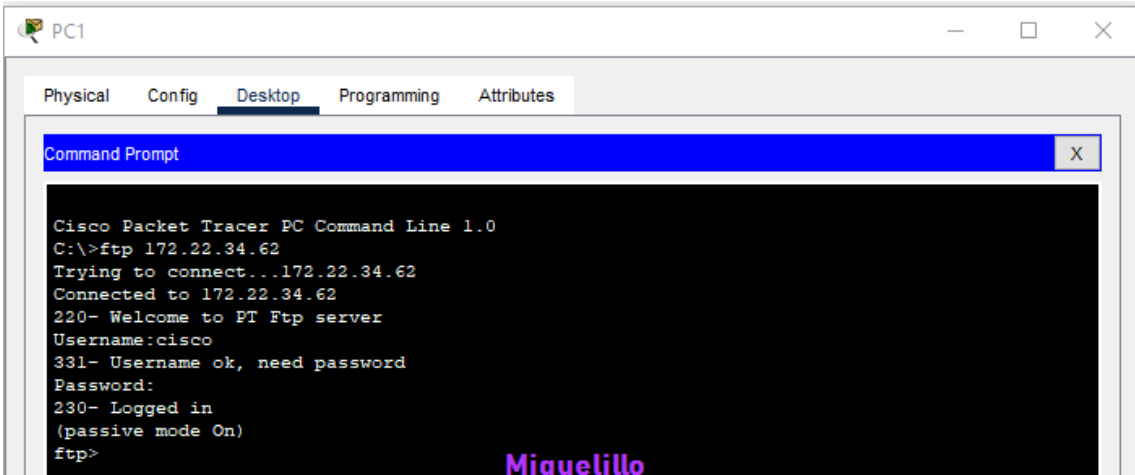
Paso 3: Verificar la implementación de la ACL.

- a. Realiza un ping desde PC1 hasta el servidor.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC1	Server	ICMP		0.000	N	0	(edit)	(delete)

Miguelillo

- b. Realiza un FTP desde PC1 hasta el servidor

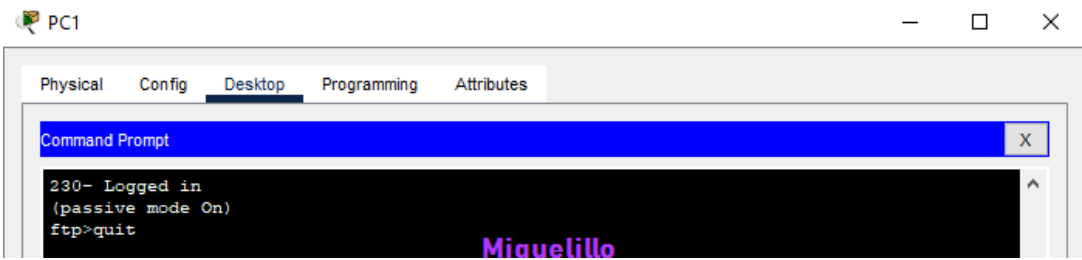


```

Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 172.22.34.62
Trying to connect...172.22.34.62
Connected to 172.22.34.62
220- Welcome to FT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
  
```

Miguelillo

- c. Sal del servicio FTP.



```

230- Logged in
(passive mode On)
ftp>quit
  
```

Miguelillo

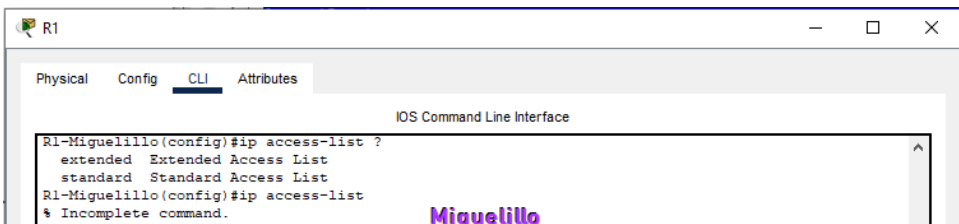
- d. Realiza un ping desde PC1 hasta PC2. El host de destino debe ser inalcanzable por la ACL

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC1	Server	ICMP		0.000	N	0	(edit)	
	Failed	PC1	PC2	ICMP		0.000	N	1	(edit)	

Miguelillo

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

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

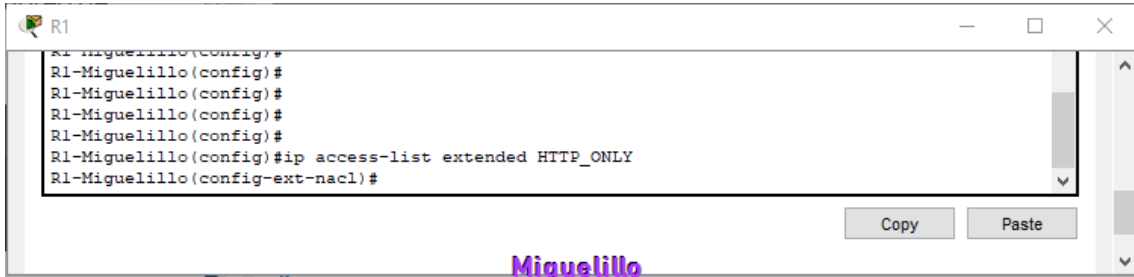


```

R1-Miguelillo(config)#ip access-list ?
  extended Extended Access List
  standard Standard Access List
R1-Miguelillo(config)#ip access-list
% Incomplete command.
  
```

Miguelillo

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

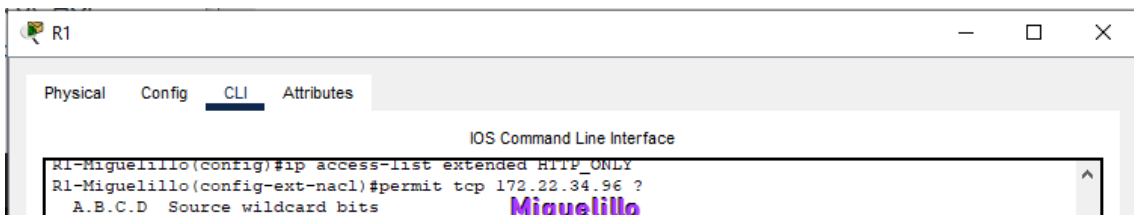


```

R1-Miguelillo(config)#
R1-Miguelillo(config)#
R1-Miguelillo(config)#
R1-Miguelillo(config)#
R1-Miguelillo(config)#ip access-list extended HTTP_ONLY
R1-Miguelillo(config-ext-nacl)#
  
```

Miguelillo

- 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.

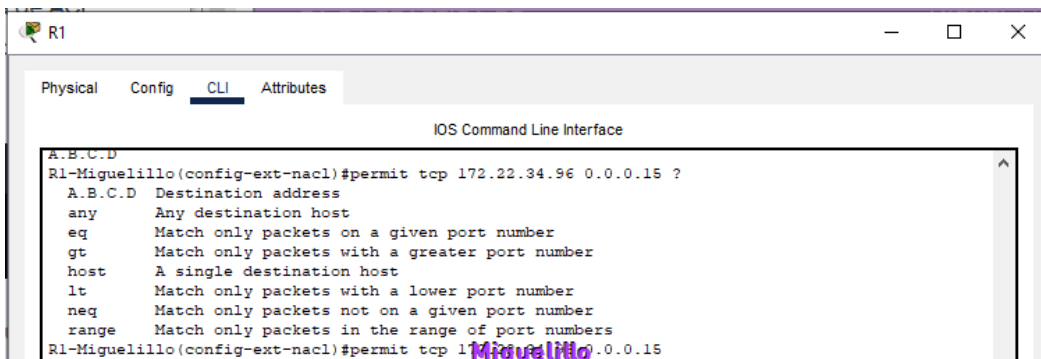


```

R1-Miguelillo(config)#ip access-list extended HTTP_ONLY
R1-Miguelillo(config-ext-nacl)#permit tcp 172.22.34.96 ?
A.B.C.D Source wildcard bits
  
```

Miguelillo

- d. Calculamos la wildcard



```

R1-Miguelillo(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 ?
A.B.C.D Destination address
any Any destination host
eq Match only packets on a given port number
gt Match only packets with a greater port number
host A single destination host
lt Match only packets with a lower port number
neq Match only packets not on a given port number
range Match only packets in the range of port numbers
R1-Miguelillo(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15
  
```

Miguelillo

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



```

R1-Miguelillo(config-ext-nacl)#
R1-Miguelillo(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
R1-Miguelillo(config-ext-nacl)#
  
```

Miguelillo

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



```

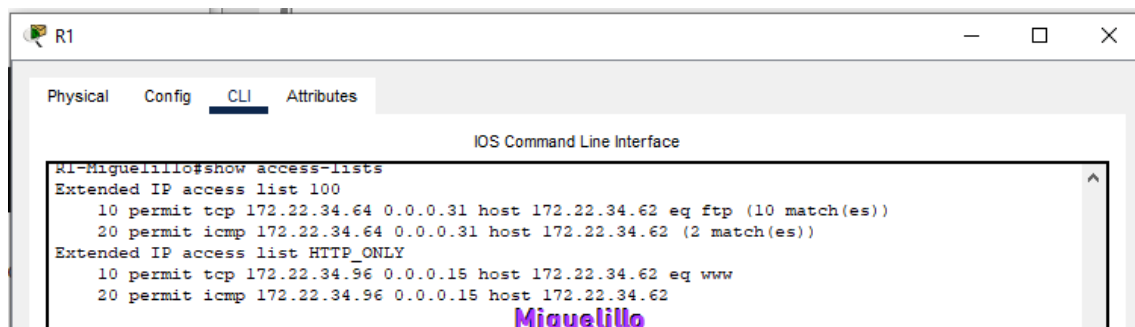
R1-Miguelillo(config-ext-nacl)#
R1-Miguelillo(config-ext-nacl)#permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
R1-Miguelillo(config-ext-nacl)#
  
```

Miguelillo

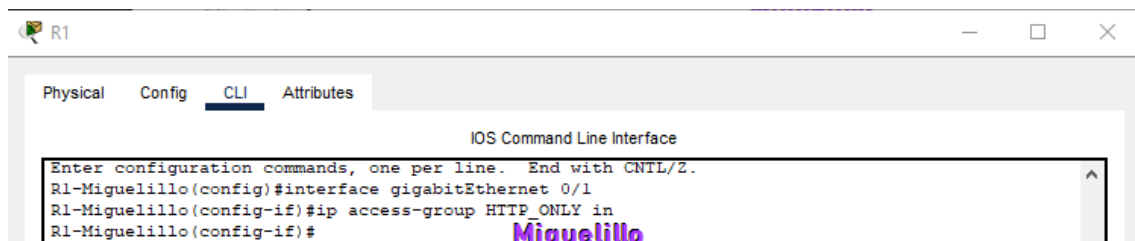
- g. Todo otro tráfico se deniega por defecto. Sal del modo de configuración de ACL con nombre extendida.



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

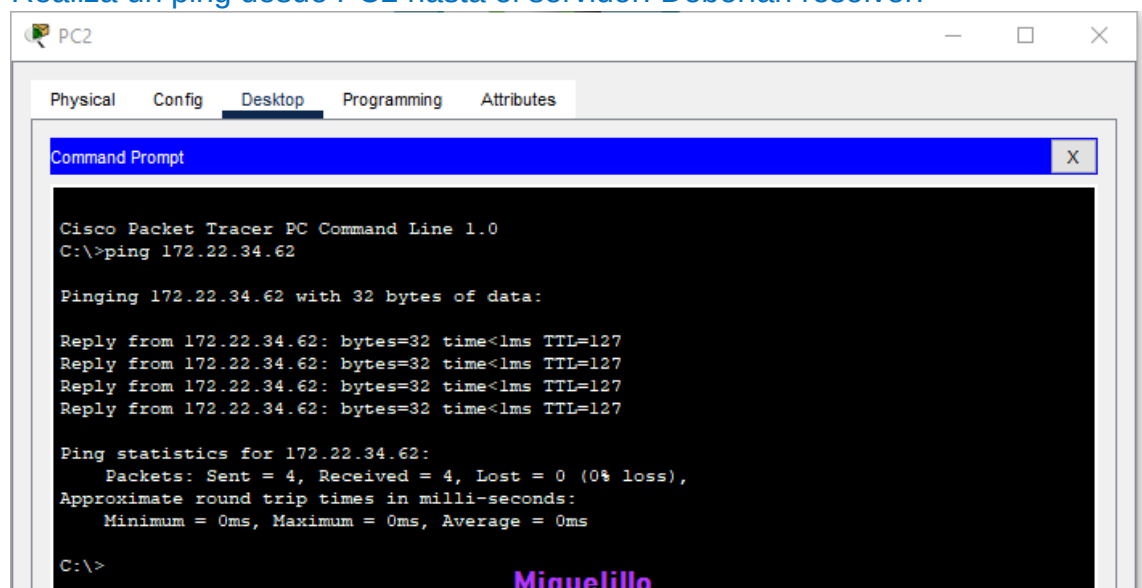


Paso 2: Aplicar la ACL en la interfaz correcta para filtrar el tráfico.

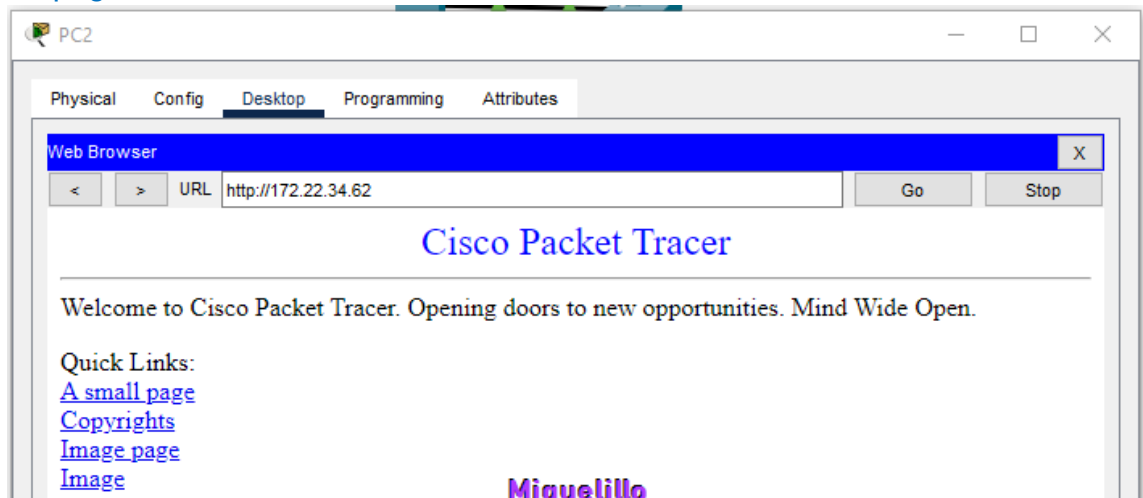


Paso 3: Verificar la Implementación de la ACL.

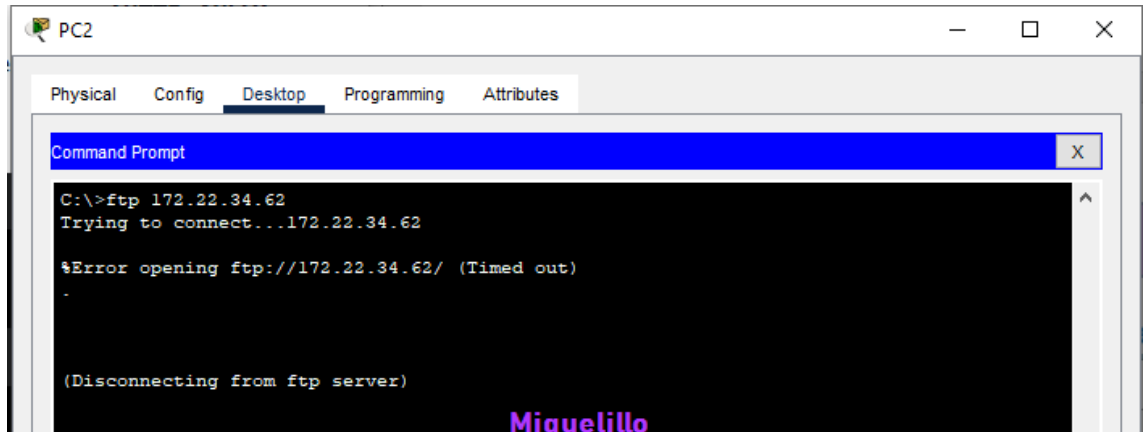
- a. Realiza un ping desde PC2 hasta el servidor. Deberían resolver.



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



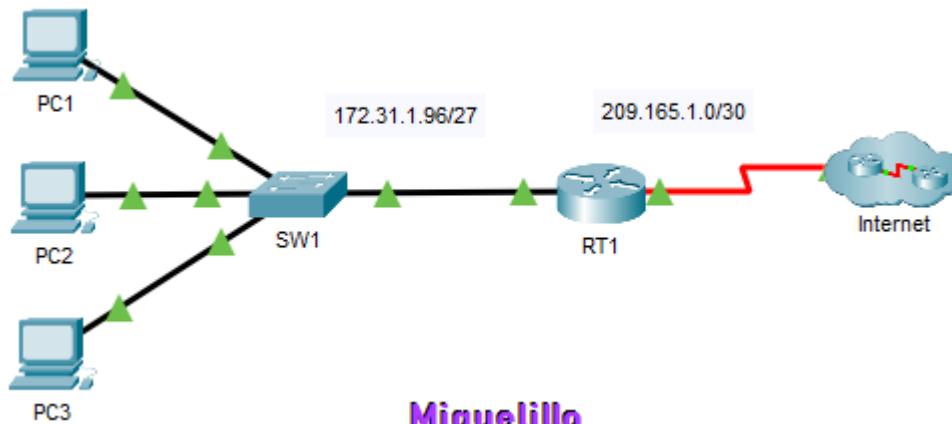
- c. Intenta hacer FTP desde PC2 hasta el servidor. La conexión debería fallar.



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.

- Crea una lista de acceso extendida con nombre en el router RT1. Usa el nombre ACL para la lista de acceso con nombre.
- 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).
- 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.

```

RT1-Miguelillo(config)#ip access-list extended ACL
RT1-Miguelillo(config-ext-nacl)#deny tcp host 172.31.1.101 host 64.101.255.254 eq 80
RT1-Miguelillo(config-ext-nacl)#deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
RT1-Miguelillo(config-ext-nacl)#deny tcp host 172.31.1.101 host 64.103.255.254 eq 80
RT1-Miguelillo(config-ext-nacl)#deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
RT1-Miguelillo(config-ext-nacl)#

```

Miguelillo

- 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.

```

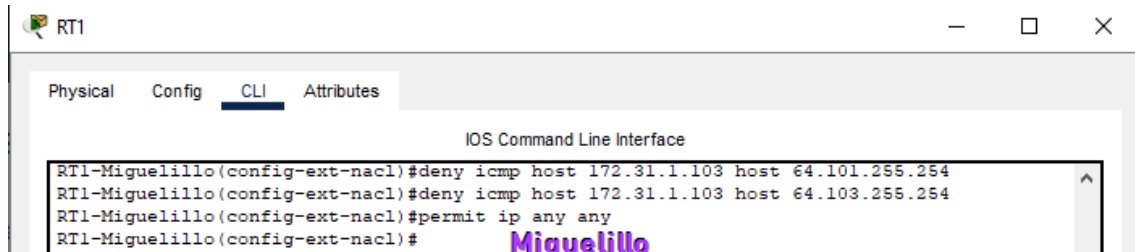
RT1-Miguelillo(config-ext-nacl)#deny tcp host 172.31.1.102 host 64.101.255.254 eq 21
RT1-Miguelillo(config-ext-nacl)#deny tcp host 172.31.1.102 host 64.103.255.254 eq 21
RT1-Miguelillo(config-ext-nacl)#

```

Miguelillo

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

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

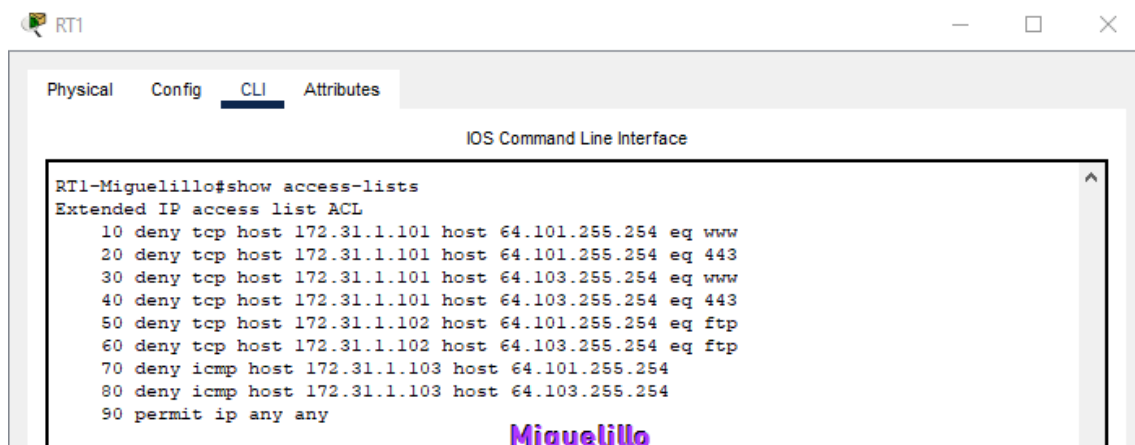


```

RT1-Miguelillo(config-ext-nacl)#deny icmp host 172.31.1.103 host 64.101.255.254
RT1-Miguelillo(config-ext-nacl)#deny icmp host 172.31.1.103 host 64.103.255.254
RT1-Miguelillo(config-ext-nacl)#permit ip any any
RT1-Miguelillo(config-ext-nacl)#
  
```

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.

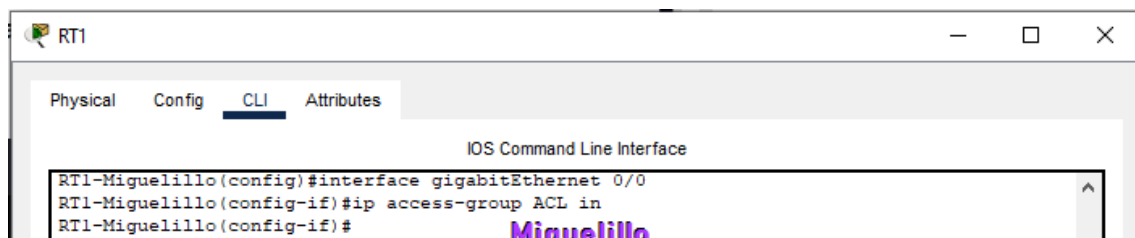


```

RT1-Miguelillo#show access-lists
Extended IP access list ACL
 10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www
 20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
 30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
 40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
 50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
 60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
 70 deny icmp host 172.31.1.103 host 64.101.255.254
 80 deny icmp host 172.31.1.103 host 64.103.255.254
 90 permit ip any any
  
```

Parte 2: Aplicar y Verificar la ACL Extendida

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

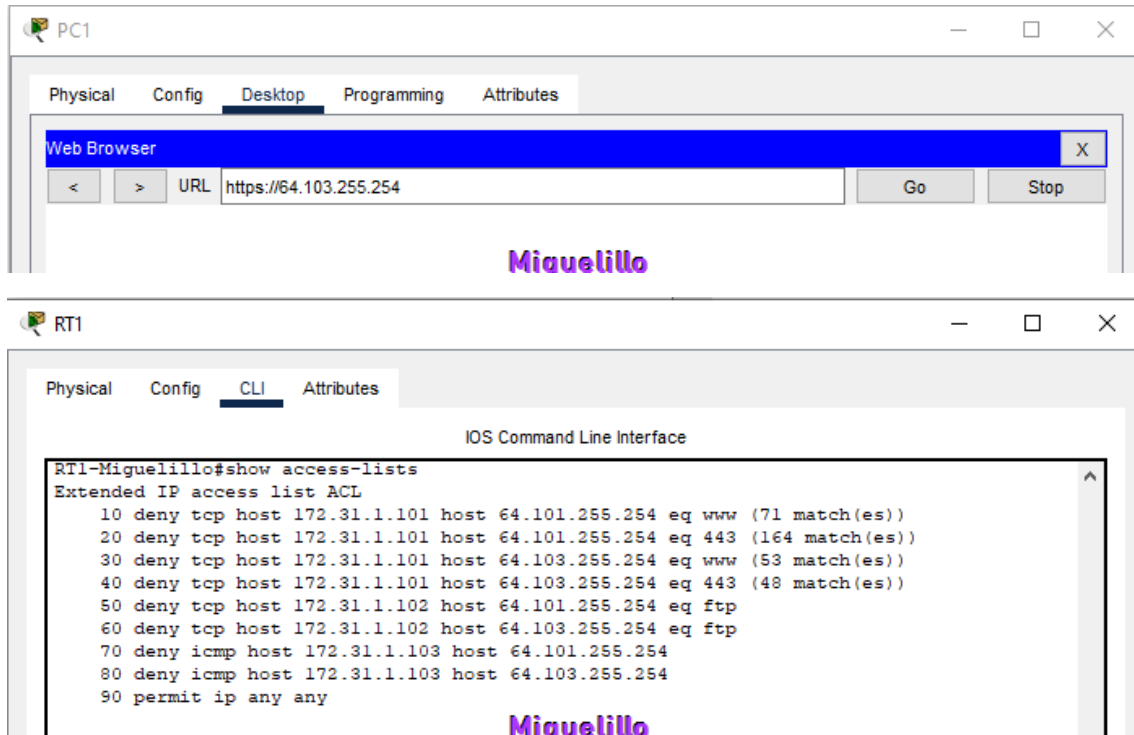


```

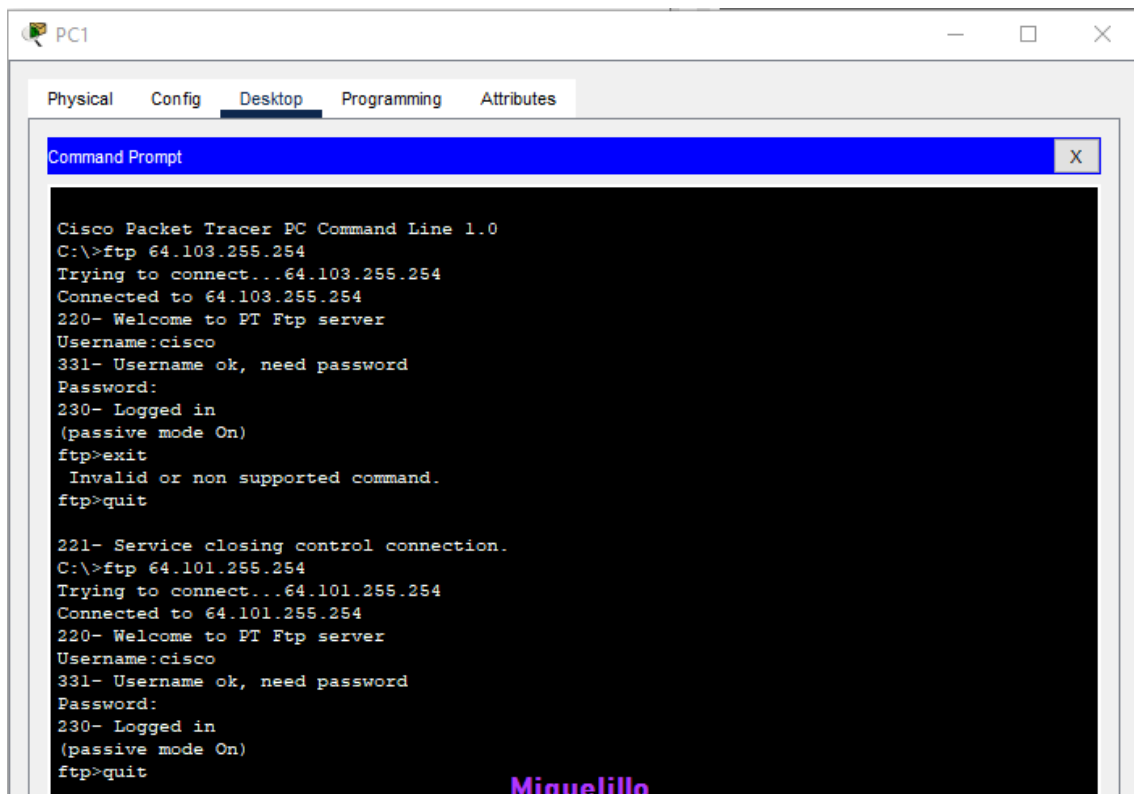
RT1-Miguelillo(config)#interface gigabitEthernet 0/0
RT1-Miguelillo(config-if)#ip access-group ACL in
RT1-Miguelillo(config-if)#
  
```

Paso 2: Probar el acceso para cada PC.

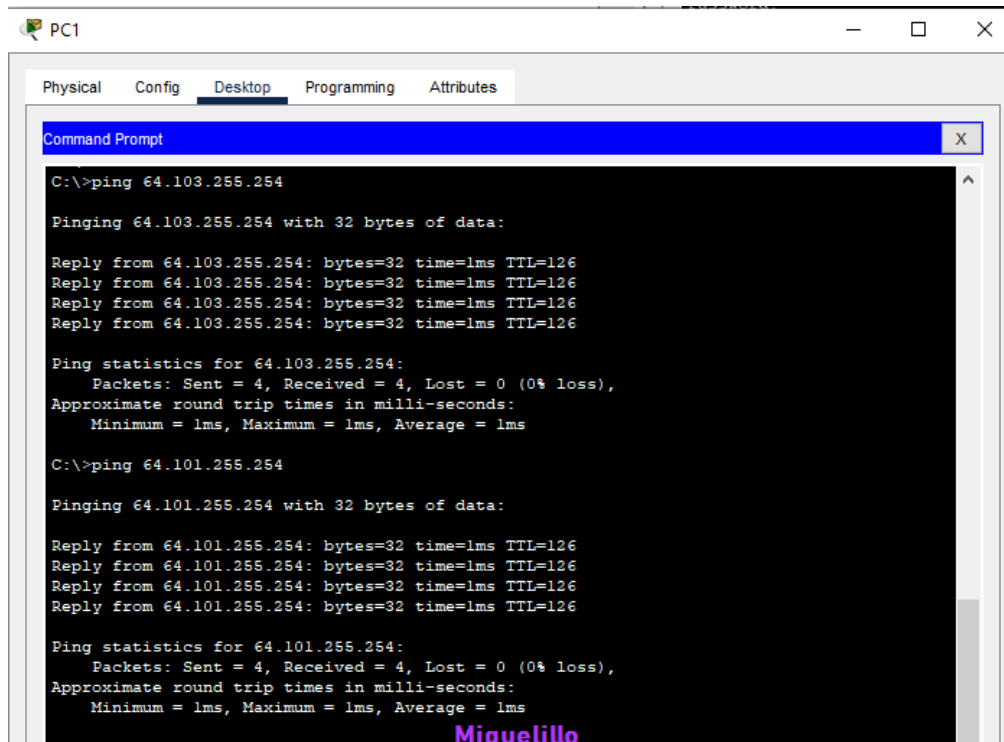
- Accede a los sitios web de Server1 y Server2 desde el navegador de PC1, utilizando tanto HTTP como HTTPS. Usa show access-lists para ver qué declaración de la lista de acceso permitió o denegó el tráfico.



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

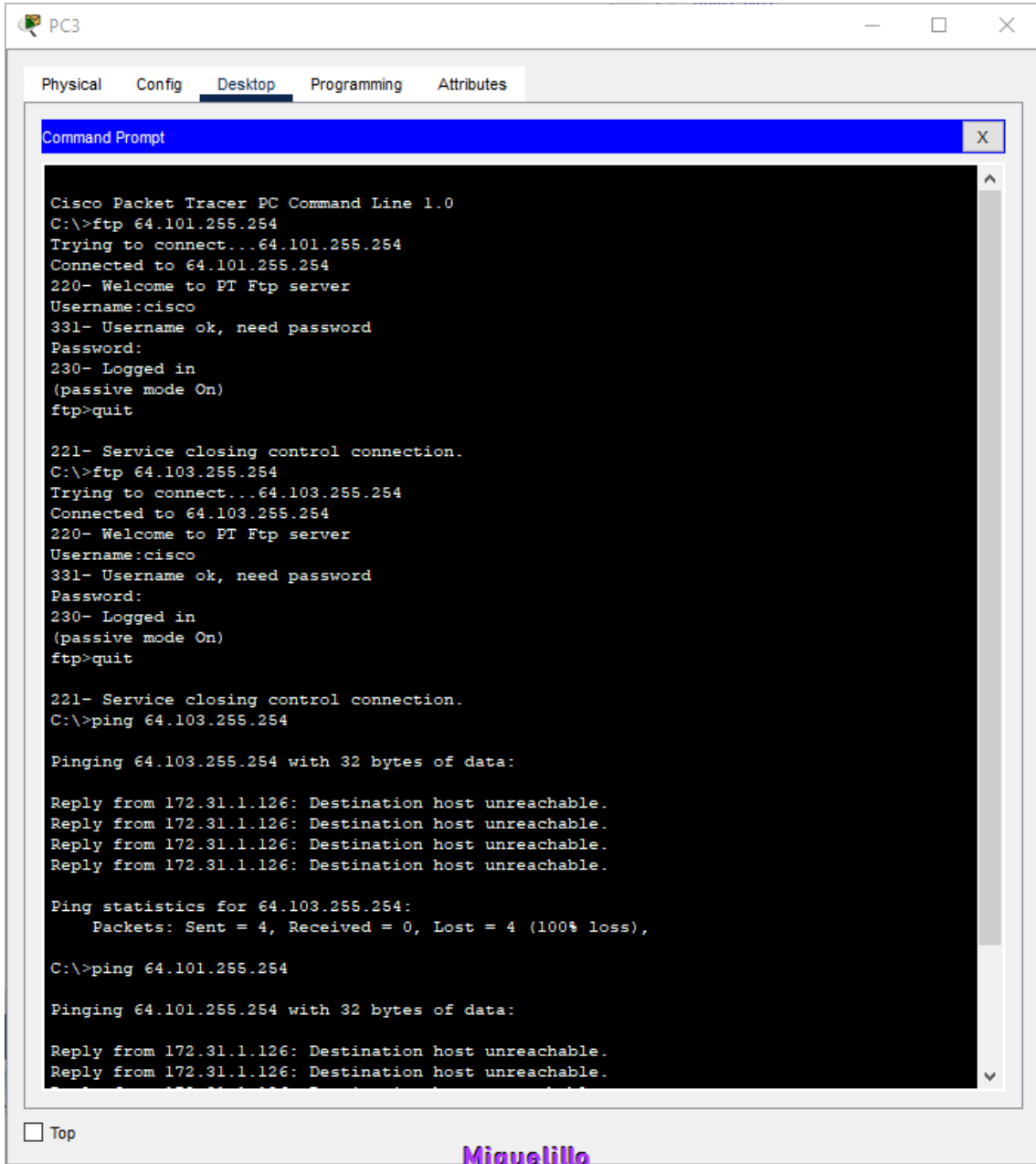


c. Realiza un ping a Server1 y Server2 desde PC1.



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





The screenshot shows a Cisco Packet Tracer PC Command Line window for a PC named 'PC3'. The window has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes', with 'Desktop' selected. The Command Prompt shows the following sequence of commands and outputs:

```
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 FT 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 FT 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.

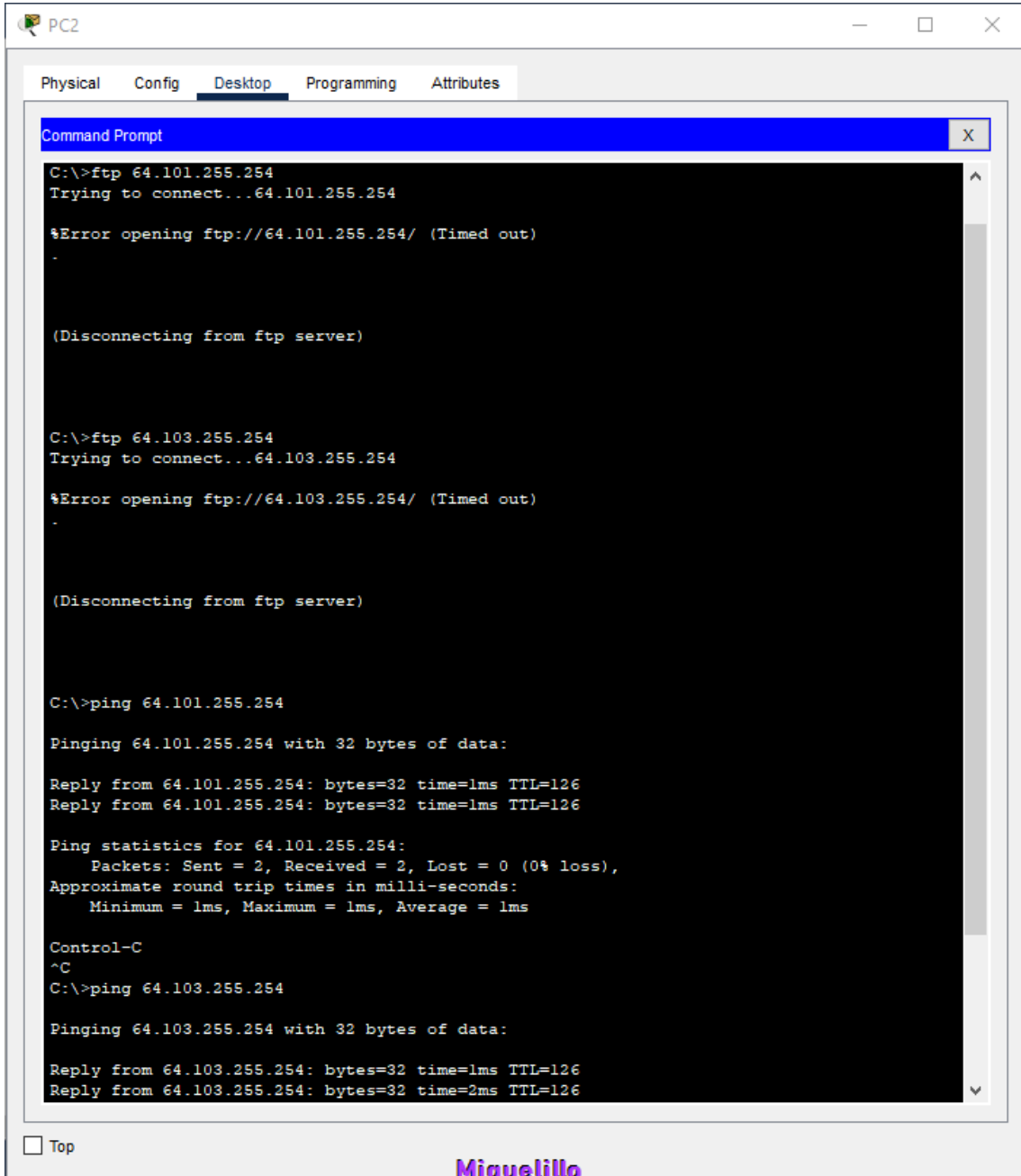
Ping statistics for 64.103.255.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

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.
```

At the bottom left of the window, there is a checkbox labeled 'Top' which is currently unchecked. At the bottom center, the name 'Miguelillo' is written in a purple, stylized font.



PC2

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ftp 64.101.255.254
Trying to connect...64.101.255.254

%Error opening ftp://64.101.255.254/ (Timed out)

.

(Disconnecting from ftp server)

C:\>ftp 64.103.255.254
Trying to connect...64.103.255.254

%Error opening ftp://64.103.255.254/ (Timed out)

.

(Disconnecting from ftp server)

C:\>ping 64.101.255.254

Pinging 64.101.255.254 with 32 bytes of data:

Reply from 64.101.255.254: bytes=32 time=1ms TTL=126
Reply from 64.101.255.254: bytes=32 time=1ms TTL=126

Ping statistics for 64.101.255.254:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

Control-C
^C
C:\>ping 64.103.255.254

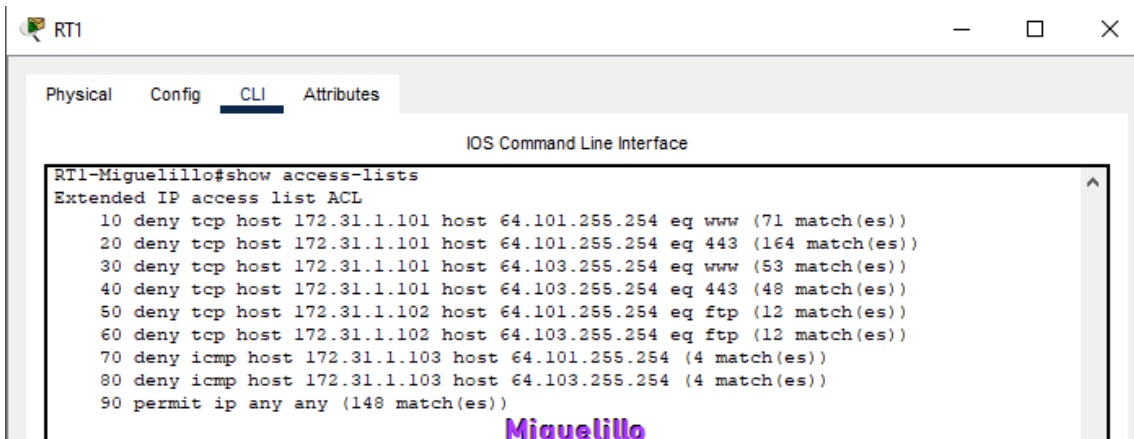
Pinging 64.103.255.254 with 32 bytes of data:

Reply from 64.103.255.254: bytes=32 time=1ms TTL=126
Reply from 64.103.255.254: bytes=32 time=2ms TTL=126
```

☐ Top

Miguelillo

Comprobamos los matches



RT1

Physical Config CLI Attributes

IOS Command Line Interface

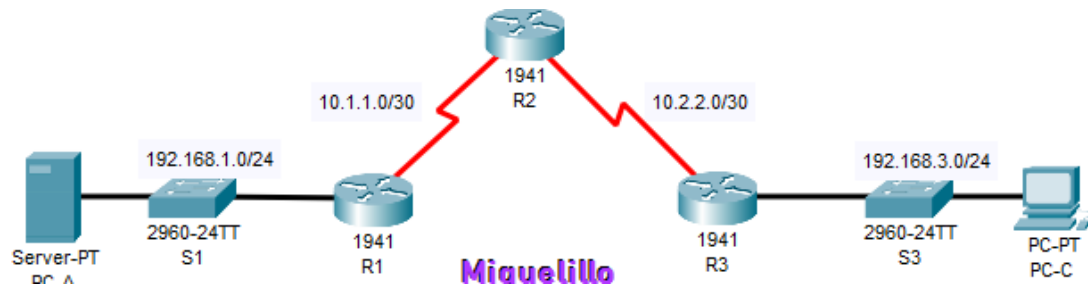
```
RT1-Miguelillo#show access-lists
Extended IP access list ACL
 10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www (71 match(es))
 20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443 (164 match(es))
 30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www (53 match(es))
 40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443 (48 match(es))
 50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp (12 match(es))
 60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp (12 match(es))
 70 deny icmp host 172.31.1.103 host 64.101.255.254 (4 match(es))
 80 deny icmp host 172.31.1.103 host 64.103.255.254 (4 match(es))
 90 permit ip any any (148 match(es))
```

Miguelillo

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).

```

C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
C:\>
  
```

- 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:\>ssh -l SSHadmin 192.168.2.1

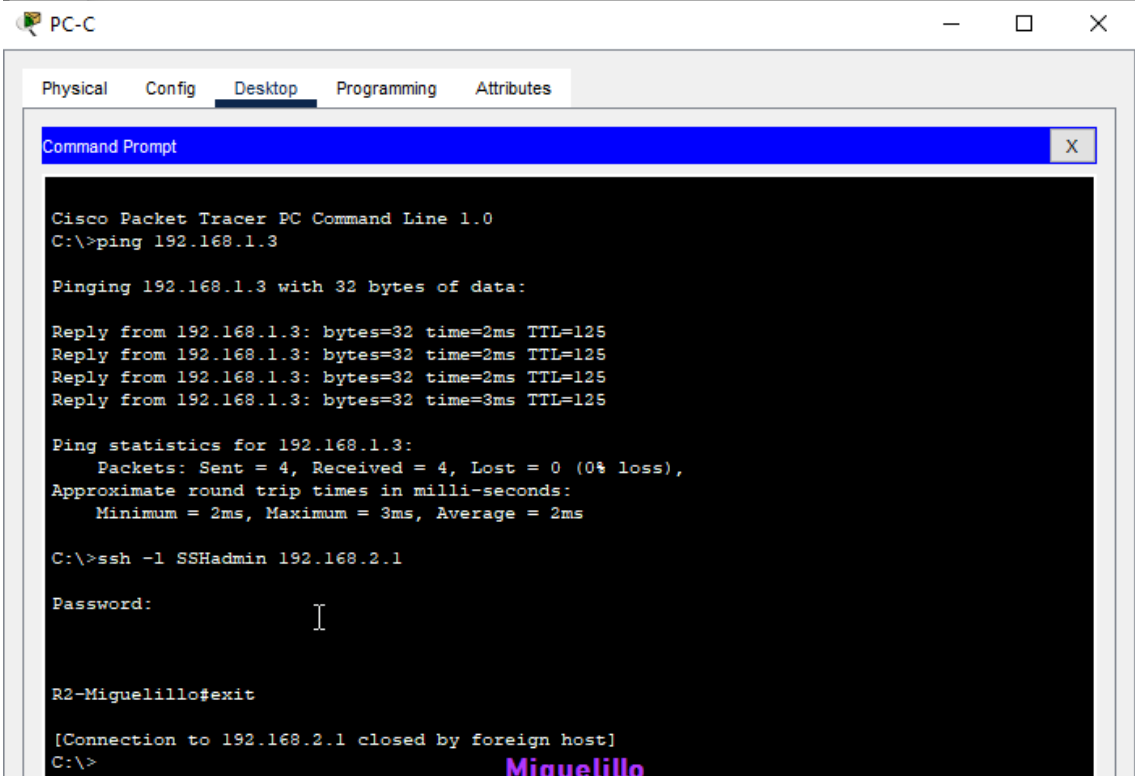
Password:

R2-Miguelillo#exit

[Connection to 192.168.2.1 closed by foreign host]
C:\>
  
```

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

- Desde la línea de comandos, realiza un ping a PC-A (192.168.1.3).
- 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.



The screenshot shows the 'PC-C' window in Packet Tracer. The 'Desktop' tab is selected, and a 'Command Prompt' window is open. The command prompt displays the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=3ms TTL=125

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

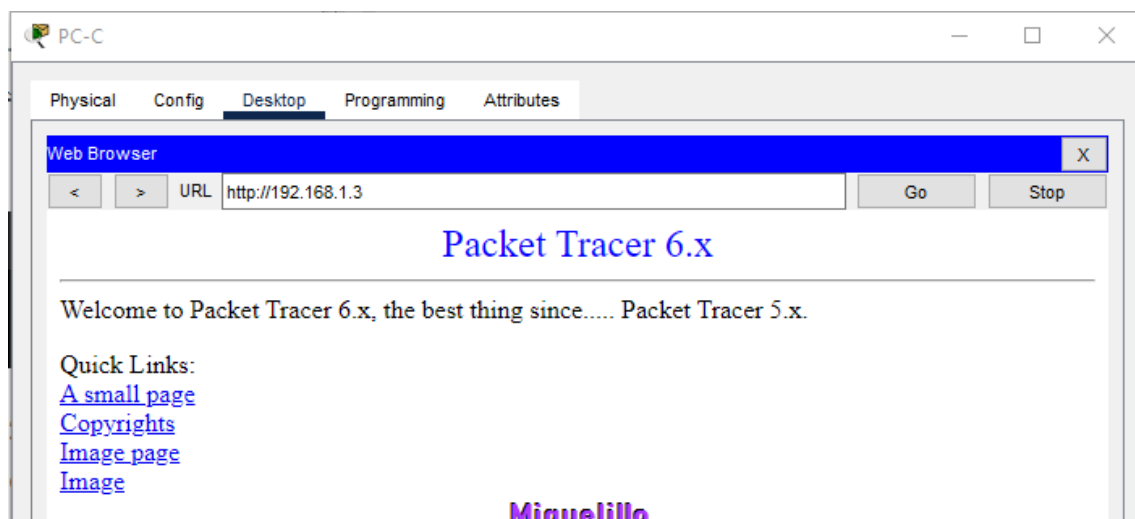
C:\>ssh -l SSHadmin 192.168.2.1

Password:
R2-Miguelillo#exit

[Connection to 192.168.2.1 closed by foreign host]
C:\>
```

The name 'Miguelillo' is written in purple at the bottom right of the command prompt window.

- 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.

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



```
R1-Miguelillo(config)#access-list 10 permit 192.168.3.3
R1-Miguelillo(config)#access-list 10 deny any
R1-Miguelillo(config)#

R2-Miguelillo(config)#access-list 10 permit 192.168.3.3
R2-Miguelillo(config)#access-list 10 deny any
R2-Miguelillo(config)#

R3-Miguelillo(config)#access-list 10 permit 192.168.3.3
R3-Miguelillo(config)#access-list 10 deny any
R3-Miguelillo(config)#
```

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



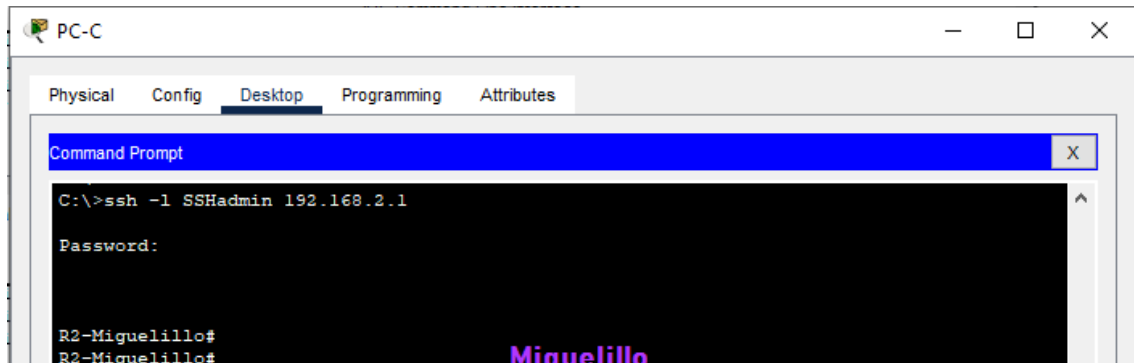
```
R1-Miguelillo(config)#line vty 0 15
R1-Miguelillo(config-line)#access-class 10 in
R1-Miguelillo(config-line)#

R2-Miguelillo(config)#line vty 0 15
R2-Miguelillo(config-line)#access-class 10 in
R2-Miguelillo(config-line)#

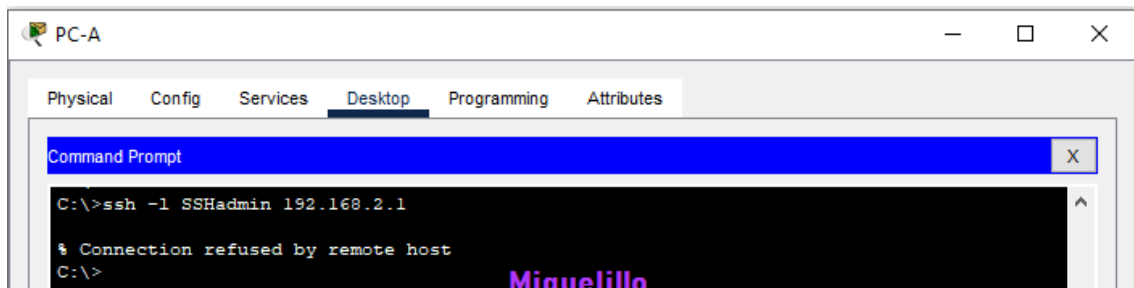
R3-Miguelillo(config)#line vty 0 15
R3-Miguelillo(config-line)#access-class 10 in
R3-Miguelillo(config-line)#
```

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).



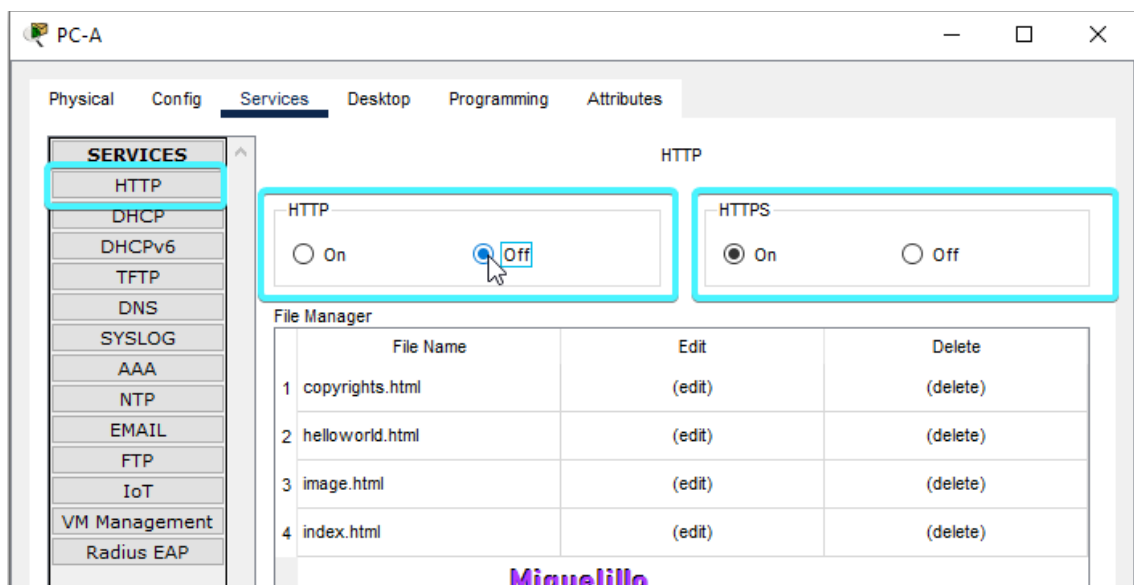
- b. Establece una sesión SSH a 192.168.2.1 desde PC-A (debería fallar).

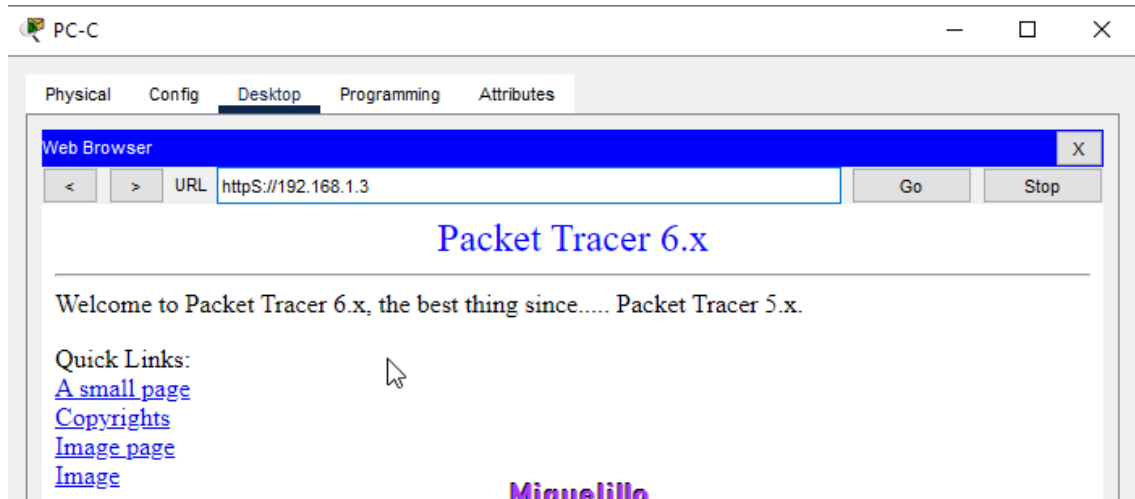


Parte 3: Crea una ACL Numerada 120 en R1

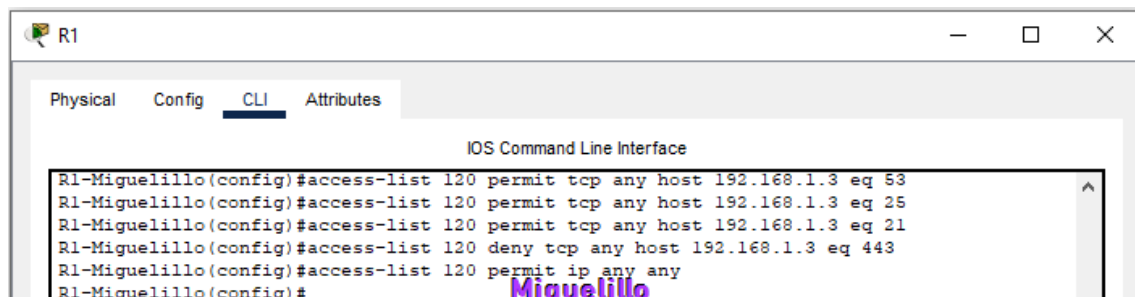
- Permitir que cualquier host externo acceda a los servicios DNS, SMTP y FTP en el servidor PC-A.
- Denegar el acceso de cualquier host externo a los servicios HTTPS en PC-A.
- Permitir a PC-C acceder a R1 a través de SSH.

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

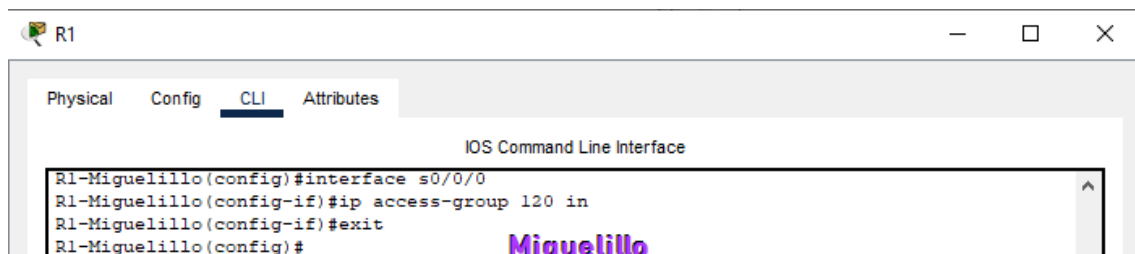




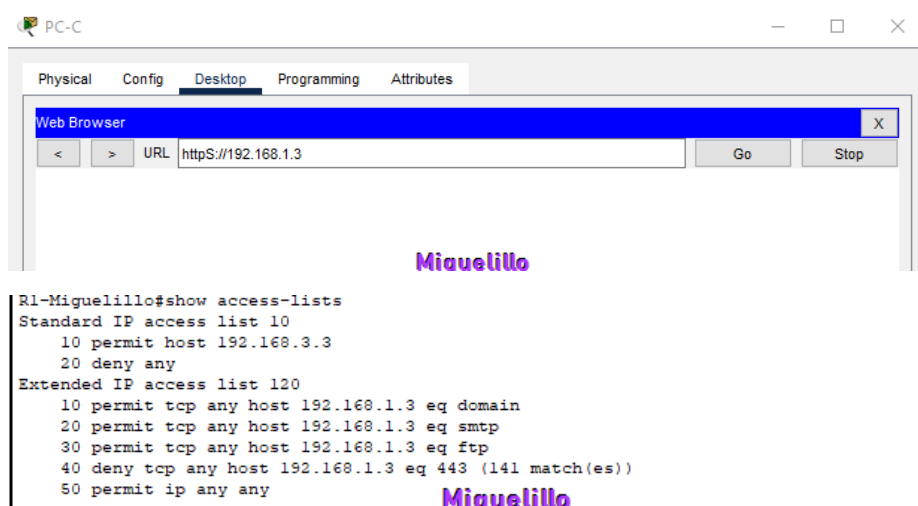
Paso 2: Configura la ACL 120 para permitir y denegar específicamente el tráfico.



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



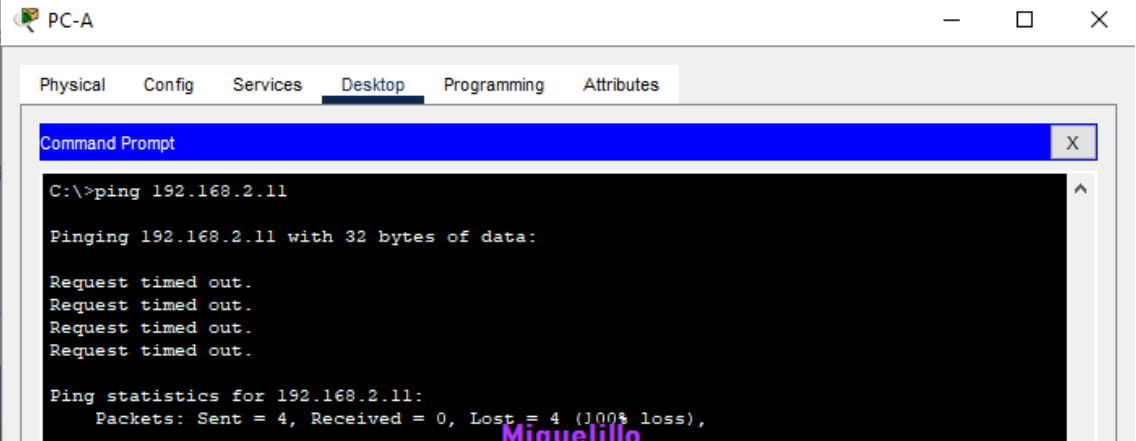
Paso 4: Verifica que PC-C no pueda acceder a PC-A a través de HTTPS usando el navegador web.



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.



The screenshot shows a Windows Command Prompt window titled "PC-A". The "Desktop" tab is selected. The command prompt shows the following output:

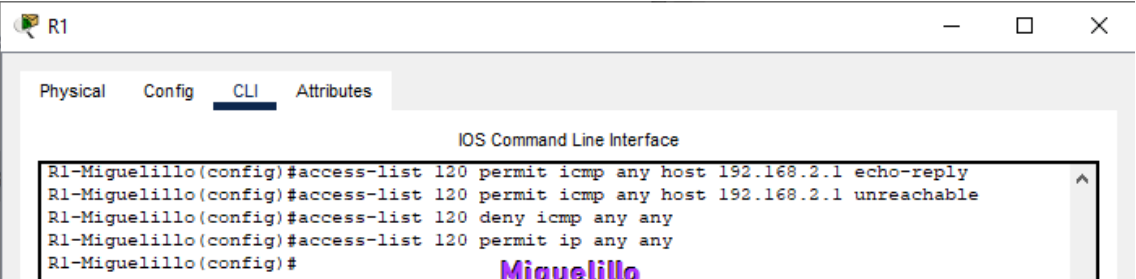
```
C:\>ping 192.168.2.11

Pinging 192.168.2.11 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

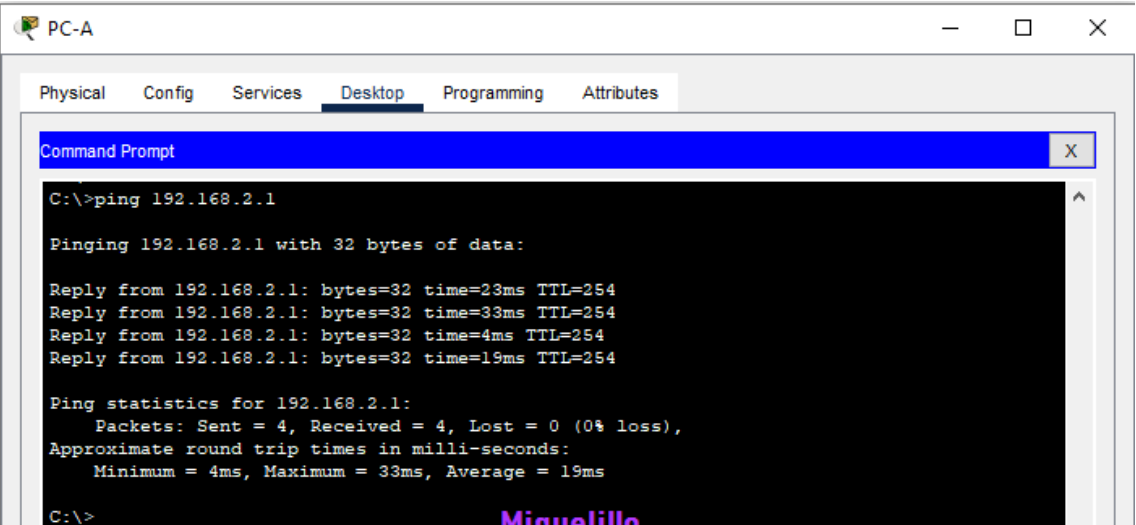
Paso 2: Realiza los cambios necesarios en la ACL 120 para permitir y denegar el tráfico especificado.



The screenshot shows the IOS Command Line Interface for R1-Miguelillo. The "CLI" tab is selected. The following commands are entered:

```
R1-Miguelillo(config)#access-list 120 permit icmp any host 192.168.2.1 echo-reply
R1-Miguelillo(config)#access-list 120 permit icmp any host 192.168.2.1 unreachable
R1-Miguelillo(config)#access-list 120 deny icmp any any
R1-Miguelillo(config)#access-list 120 permit ip any any
R1-Miguelillo(config)#
```

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



The screenshot shows a Windows Command Prompt window titled "PC-A". The "Desktop" tab is selected. The command prompt shows the following output:

```
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=23ms TTL=254
Reply from 192.168.2.1: bytes=32 time=33ms TTL=254
Reply from 192.168.2.1: bytes=32 time=4ms TTL=254
Reply from 192.168.2.1: bytes=32 time=19ms TTL=254

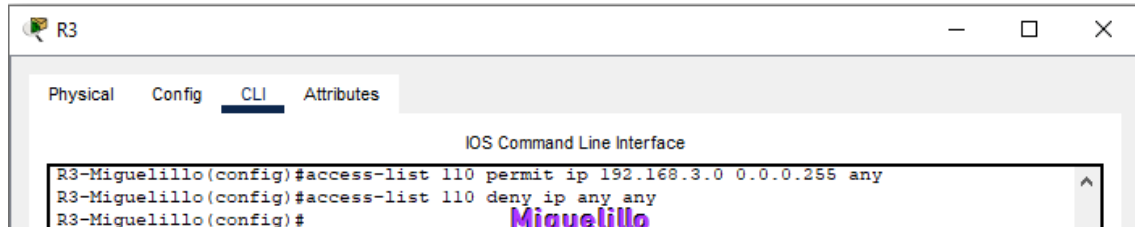
Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 33ms, Average = 19ms

C:\>
```

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.



The screenshot shows the R3 CLI interface with the following commands entered:

```
R3-Miguelillo(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
R3-Miguelillo(config)#access-list 110 deny ip any any
R3-Miguelillo(config)#
```

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



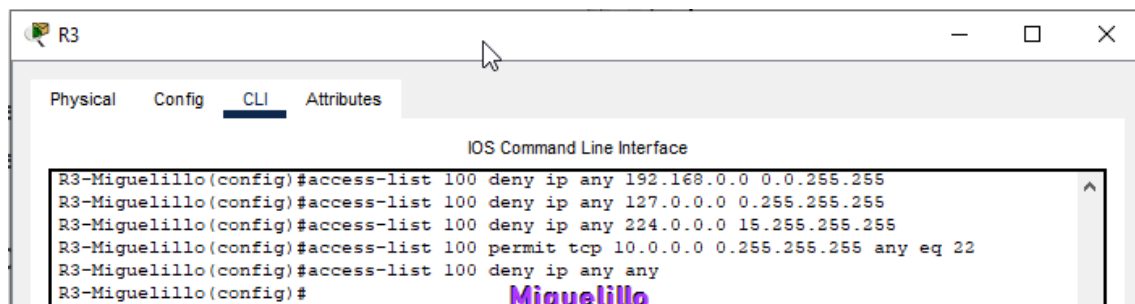
The screenshot shows the R3 CLI interface with the following commands entered:

```
R3-Miguelillo(config)#interface g0/1
R3-Miguelillo(config-if)#ip access-group 110 in
R3-Miguelillo(config-if)#exit
```

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.

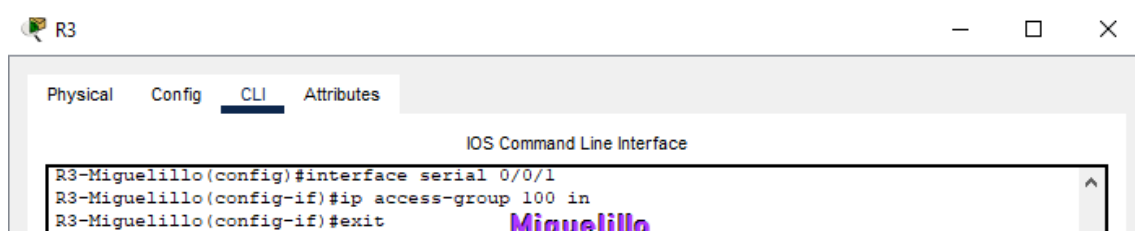
Paso 1: Configurar la ACL 100 para bloquear todo el tráfico especificado desde la red externa.



The screenshot shows the R3 CLI interface with the following commands entered:

```
R3-Miguelillo(config)#access-list 100 deny ip any 192.168.0.0 0.0.255.255
R3-Miguelillo(config)#access-list 100 deny ip any 127.0.0.0 0.255.255.255
R3-Miguelillo(config)#access-list 100 deny ip any 224.0.0.0 15.255.255.255
R3-Miguelillo(config)#access-list 100 permit tcp 10.0.0.0 0.255.255.255 any eq 22
R3-Miguelillo(config)#access-list 100 deny ip any any
R3-Miguelillo(config)#
```

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

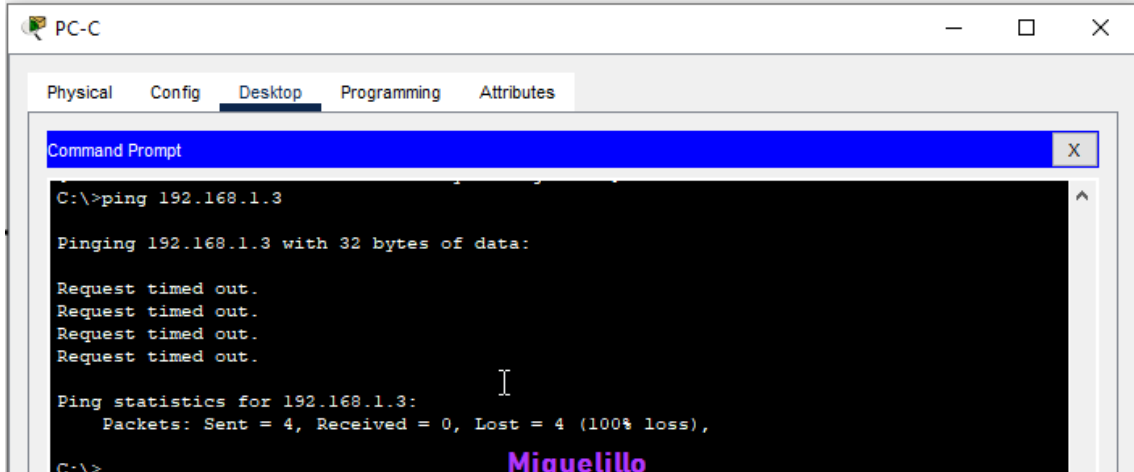


The screenshot shows the R3 CLI interface with the following commands entered:

```
R3-Miguelillo(config)#interface serial 0/0/1
R3-Miguelillo(config-if)#ip access-group 100 in
R3-Miguelillo(config-if)#exit
```


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)



The screenshot shows a window titled "PC-C" with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, displaying a "Command Prompt" window. The command prompt shows the execution of the command `C:\>ping 192.168.1.3`. The output indicates that the ping failed, showing "Request timed out." four times and "Ping statistics for 192.168.1.3: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)". A cursor is visible on the line "Ping statistics for 192.168.1.3:". The name "Miguelillo" is written in pink at the bottom right of the command prompt window.

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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



The screenshot shows a window titled "PC-C" with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, displaying a "Command Prompt" window. The command prompt shows the execution of the command `C:\>ssh -l SSHadmin 192.168.2.1`. The output indicates that the connection timed out, showing "Connection timed out; remote host not responding". The name "Miguelillo" is written in pink at the bottom right of the command prompt window.

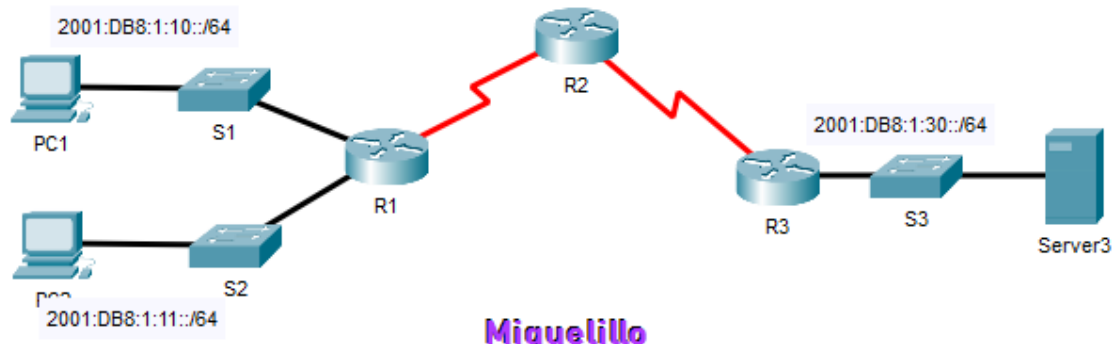
```
C:\>ssh -l SSHadmin 192.168.2.1

Connection timed out; remote host not responding
C:\>
```

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.

```

R1
Physical Config CLI Attributes
IOS Command Line Interface
R1-Miguelillo(config)#ipv6 access-list BLOCK_HTTP
R1-Miguelillo(config-ipv6-acl)#deny tcp any host 2001:db8:1:30::30 eq www
R1-Miguelillo(config-ipv6-acl)#deny tcp any host 2001:db8:1:30::30 eq 443
R1-Miguelillo(config-ipv6-acl)#permit ipv6 any any
R1-Miguelillo(config-ipv6-acl)#exit

```

Paso 2: Aplicar el ACL en la interfaz correcta.

```

R1
Physical Config CLI Attributes
IOS Command Line Interface
R1-Miguelillo(config)#interface GigabitEthernet 0/1
R1-Miguelillo(config-if)#ipv6 traffic-filter BLOCK_HTTP in
R1-Miguelillo(config-if)#exit

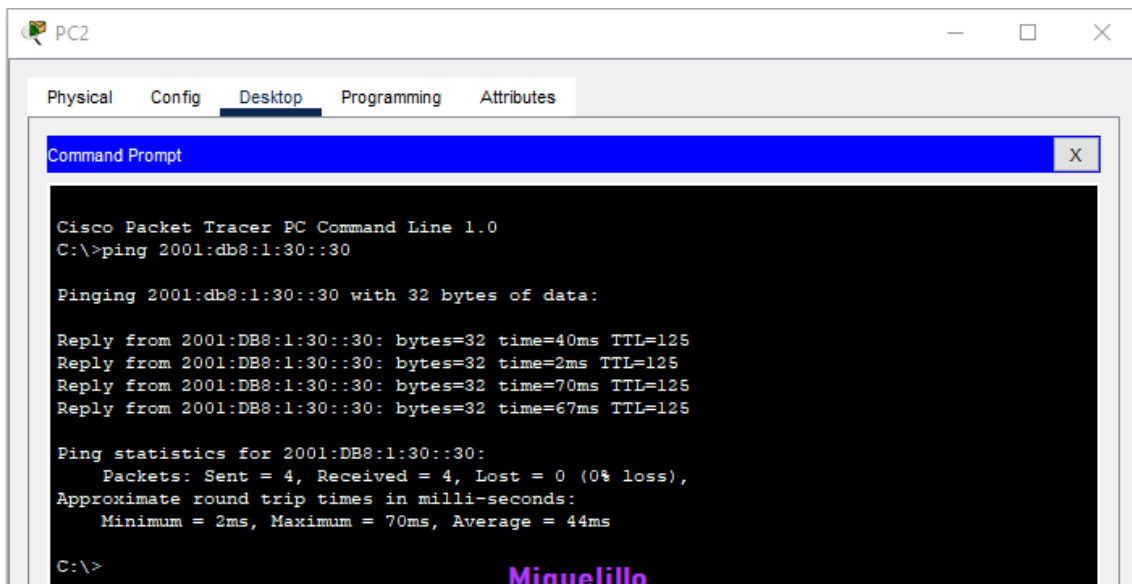
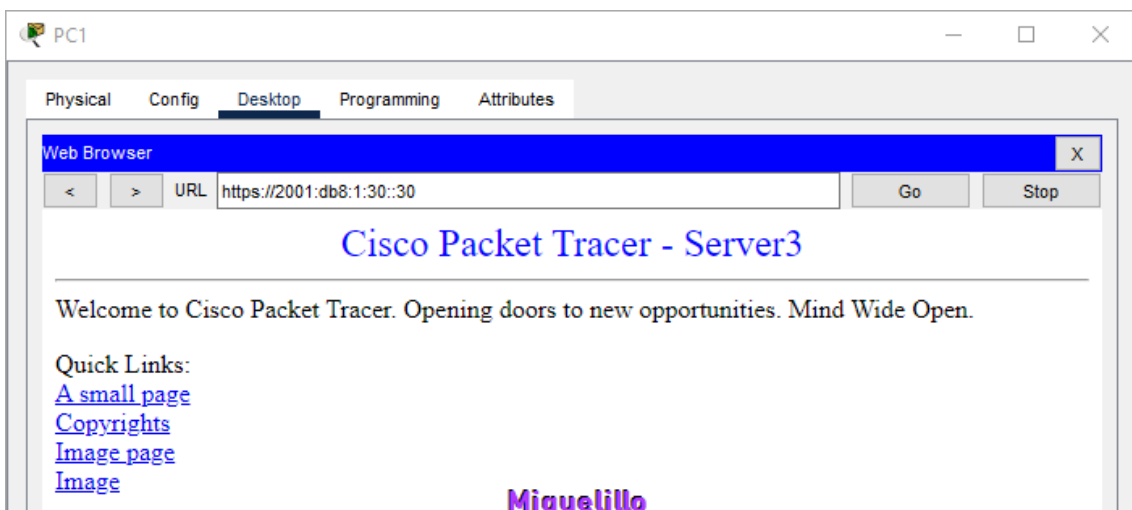
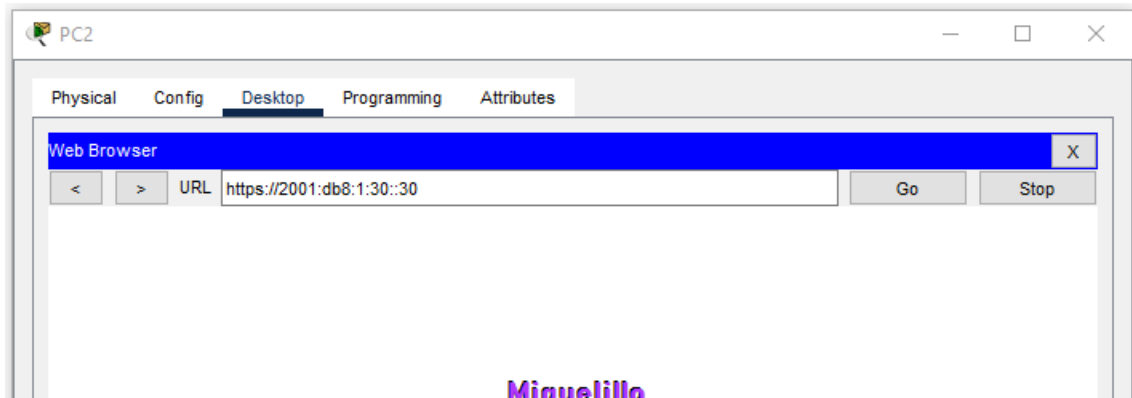
```

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.

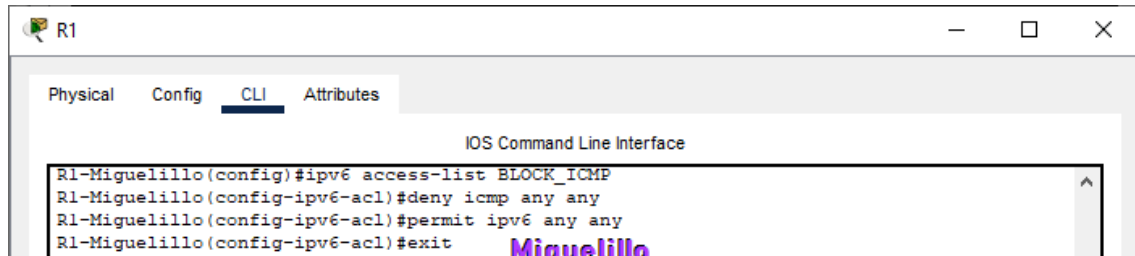
Realiza un ping desde PC2 a 2001:db8:1:30::30. El ping debería ser exitoso.



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.

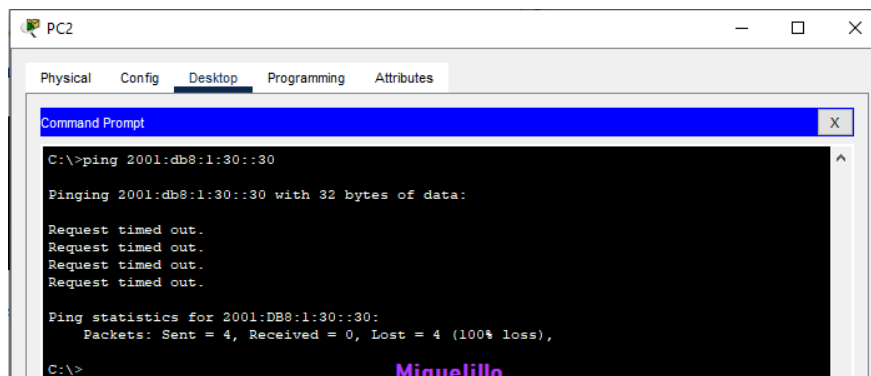


Paso 2: Aplicar el ACL en la interfaz correcta.

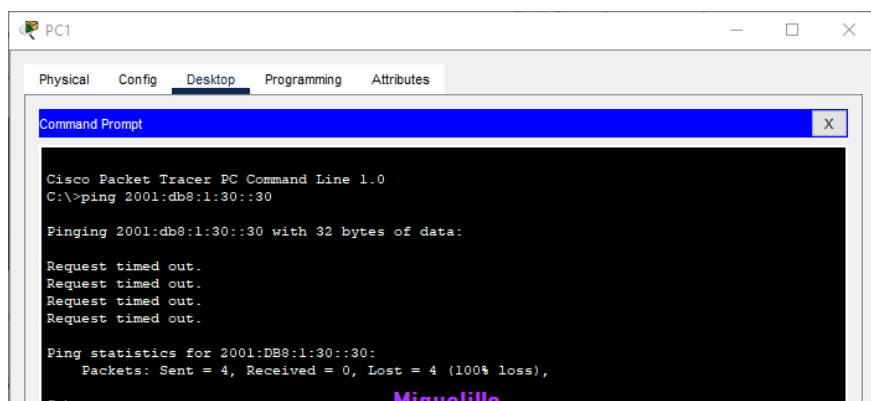


Paso 3: Verificar que la lista de acceso funcione correctamente.

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



- 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.

