

ACTIVIDAD 5.4.13. CONFIGURACIÓN DE LISTAS ACL IPV4 EXTENDIDAS

Memoria Técnica

Ignacio Andrade Salazar

7 A IELC

CONTENIDO

- 1. Antecedentes
 - 1.1. Objetivo
 - 1.2. Alcance
 - 1.3. Descripción técnica de la solución
- 2. Esquema General
- 3. Script CTC
- 4. Pruebas

I. ANTECEDENTES

- I.1. Objetivos

- **Parte 1: Configure una ACL extendida con nombre**
- **Parte 2: Aplique y verifique la ACL extendida**

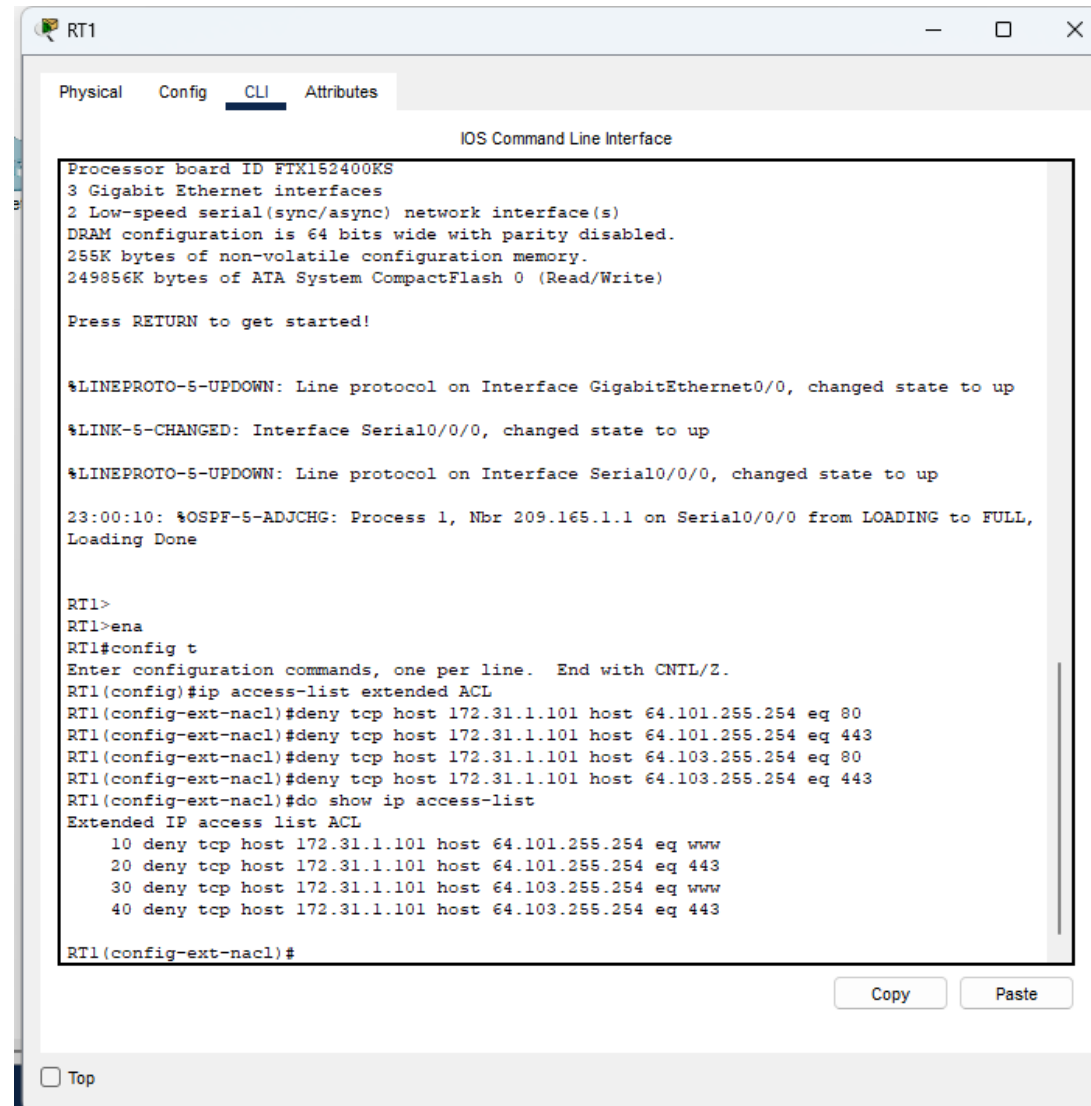
- I.2. Alcance

- En este escenario, se permiten dispositivos específicos en la LAN a varios servicios en servidores ubicados en Internet.

2. DESCRIPCIÓN TÉCNICA DE LA SOLUCIÓN

**Part 1: Configure a Named
Extended ACL**

**PASO 1: DENEGAR A
LA PCI EL ACCESO
A LOS SERVICIOS
HTTP Y HTTPS EN
EL SERVIDOR1 Y EL
SERVIDOR2.**



The screenshot shows a network device CLI window titled 'RT1'. The 'CLI' tab is selected. The window displays the following text:

```
Processor board ID FTX152400KS
3 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

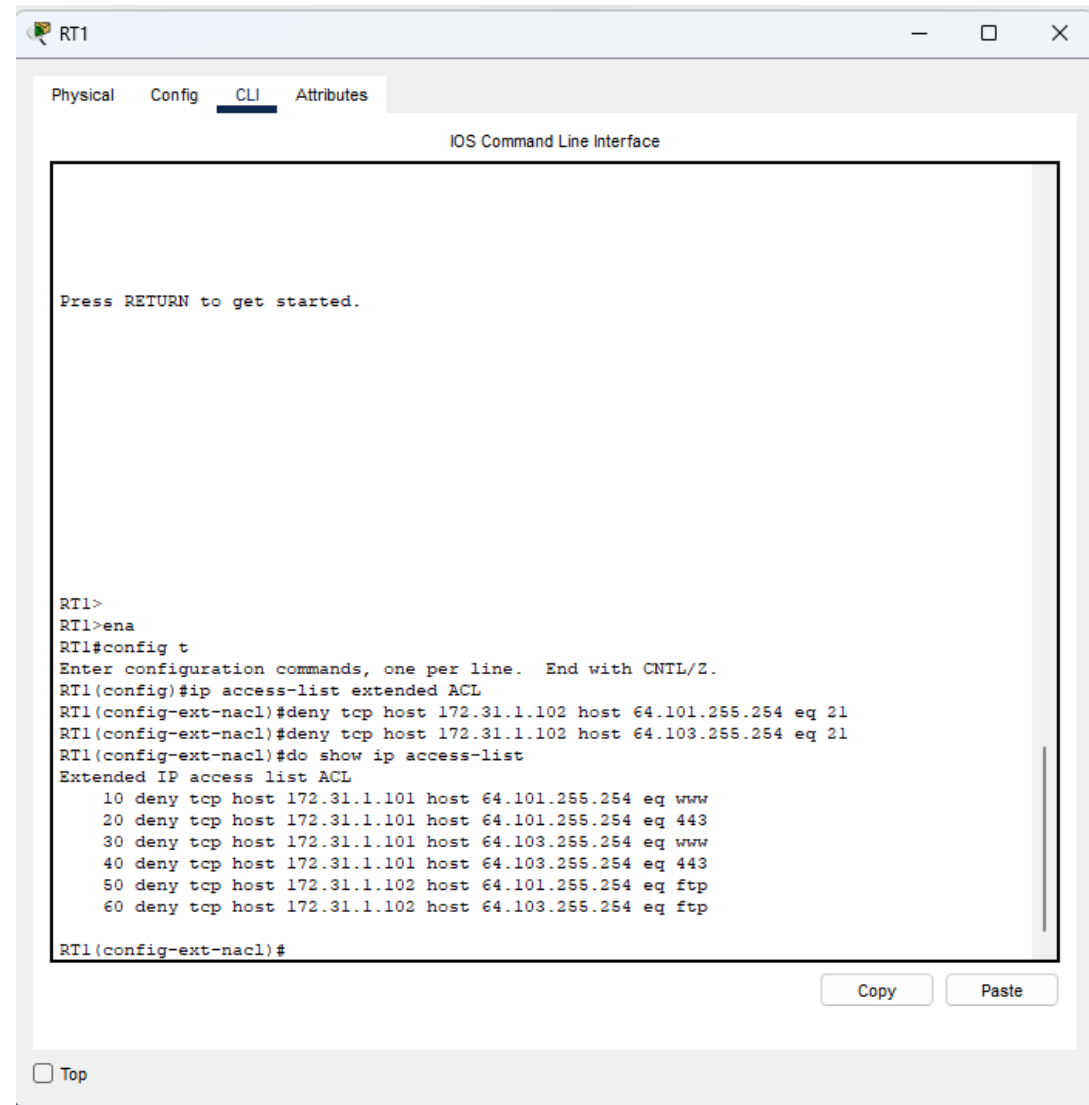
Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
23:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done

RT1>
RT1>ena
RT1#config t
Enter configuration commands, one per line. End with CNTL/Z.
RT1(config)#ip access-list extended ACL
RT1(config-ext-nacl)#deny tcp host 172.31.1.101 host 64.101.255.254 eq 80
RT1(config-ext-nacl)#deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
RT1(config-ext-nacl)#deny tcp host 172.31.1.101 host 64.103.255.254 eq 80
RT1(config-ext-nacl)#deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
RT1(config-ext-nacl)#do show ip access-list
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
RT1(config-ext-nacl)#
```

At the bottom of the window, there are 'Copy' and 'Paste' buttons, and a 'Top' link.

**PASO 2: DENEGAR A
LA PC2 EL ACCESO
A LOS SERVICIOS
FTP EN EL
SERVIDOR1 Y EL
SERVIDOR2.**

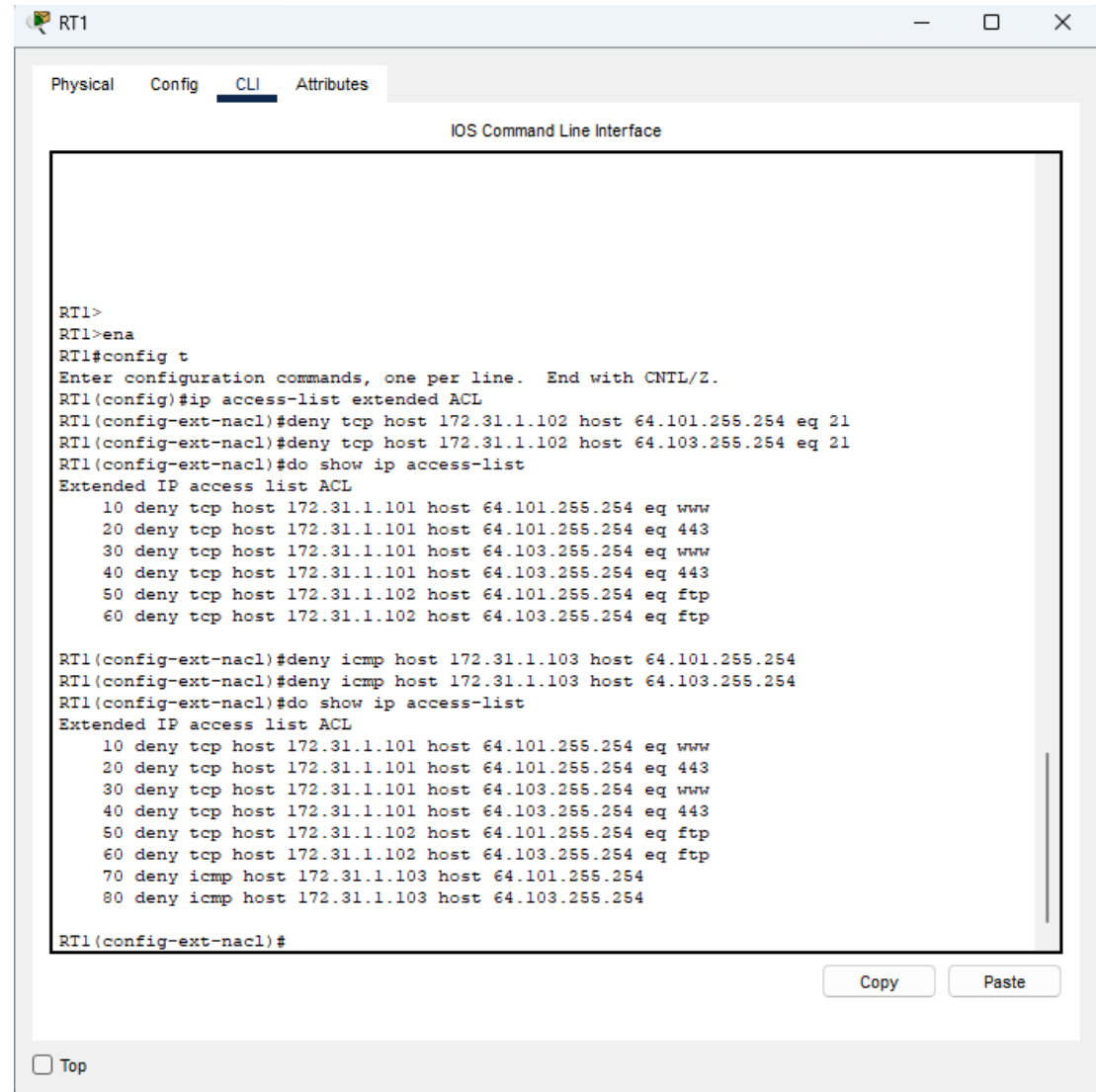


The screenshot shows the CLI interface of a router named RT1. The 'CLI' tab is selected. The interface displays the following commands and output:

```
RT1>
RT1>ena
RT1#config t
Enter configuration commands, one per line. End with CNTL/Z.
RT1(config)#ip access-list extended ACL
RT1(config-ext-nacl)#deny tcp host 172.31.1.102 host 64.101.255.254 eq 21
RT1(config-ext-nacl)#deny tcp host 172.31.1.102 host 64.103.255.254 eq 21
RT1(config-ext-nacl)#do show ip access-list
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
RT1(config-ext-nacl)#
```

At the bottom of the window, there are 'Copy' and 'Paste' buttons, and a 'Top' link.

PASO 3: DENEGAR A LA PC3 QUE HAGA PING A SERVIDOR1 AL SERVIDOR2.

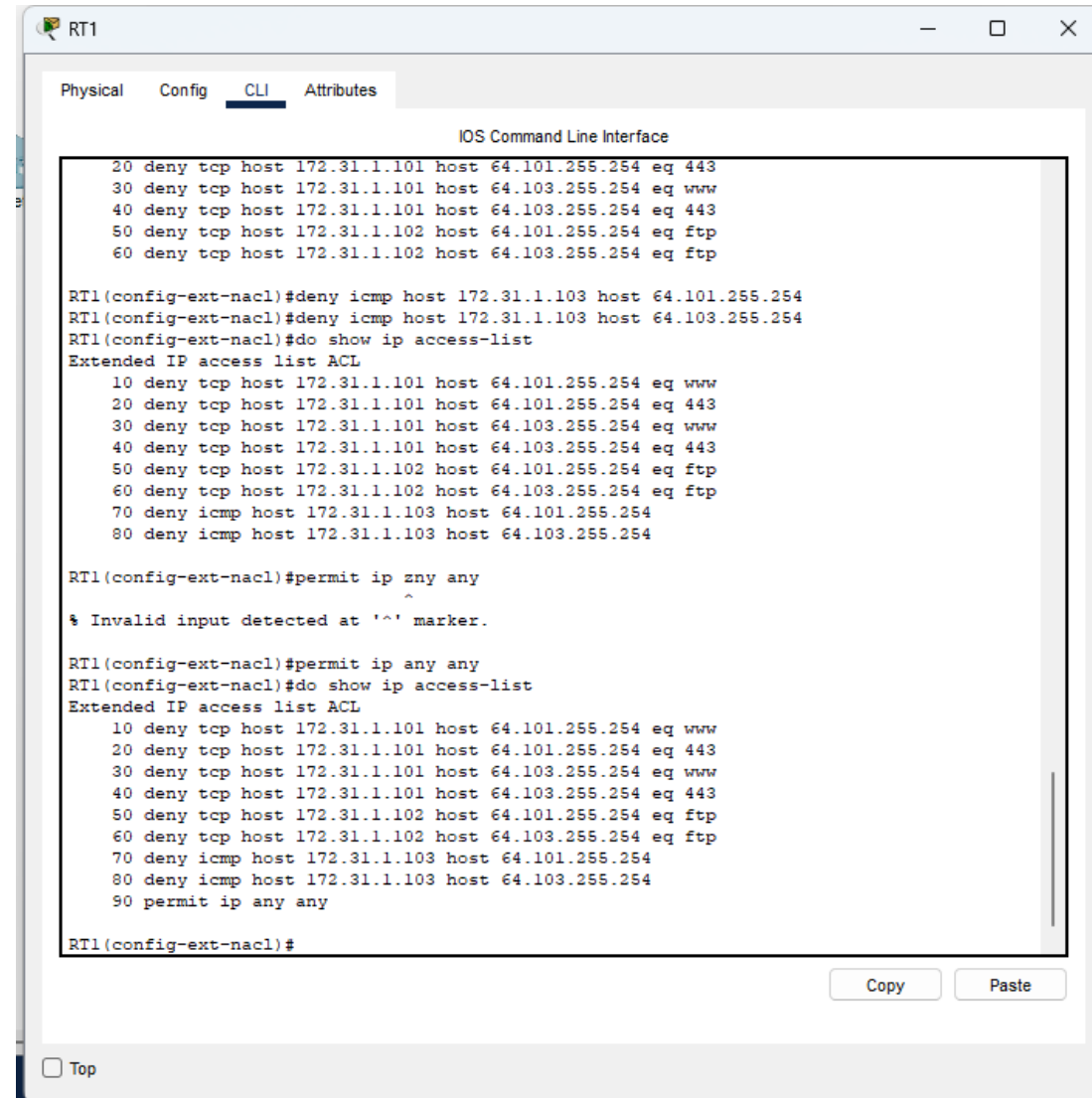


```
RT1>
RT1>ena
RT1#config t
Enter configuration commands, one per line. End with CNTL/Z.
RT1(config)#ip access-list extended ACL
RT1(config-ext-nacl)#deny tcp host 172.31.1.102 host 64.101.255.254 eq 21
RT1(config-ext-nacl)#deny tcp host 172.31.1.102 host 64.103.255.254 eq 21
RT1(config-ext-nacl)#do show ip access-list
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

RT1(config-ext-nacl)#deny icmp host 172.31.1.103 host 64.101.255.254
RT1(config-ext-nacl)#deny icmp host 172.31.1.103 host 64.103.255.254
RT1(config-ext-nacl)#do show ip access-list
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

RT1(config-ext-nacl)#
```

PASO 4: PERMITIR EL RESTO DEL TRÁFICO IP.



```
RT1
Physical Config CLI Attributes
IOS Command Line Interface
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

RT1(config-ext-nacl)#deny icmp host 172.31.1.103 host 64.101.255.254
RT1(config-ext-nacl)#deny icmp host 172.31.1.103 host 64.103.255.254
RT1(config-ext-nacl)#do show ip access-list
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

RT1(config-ext-nacl)#permit ip any any
^
% Invalid input detected at '^' marker.

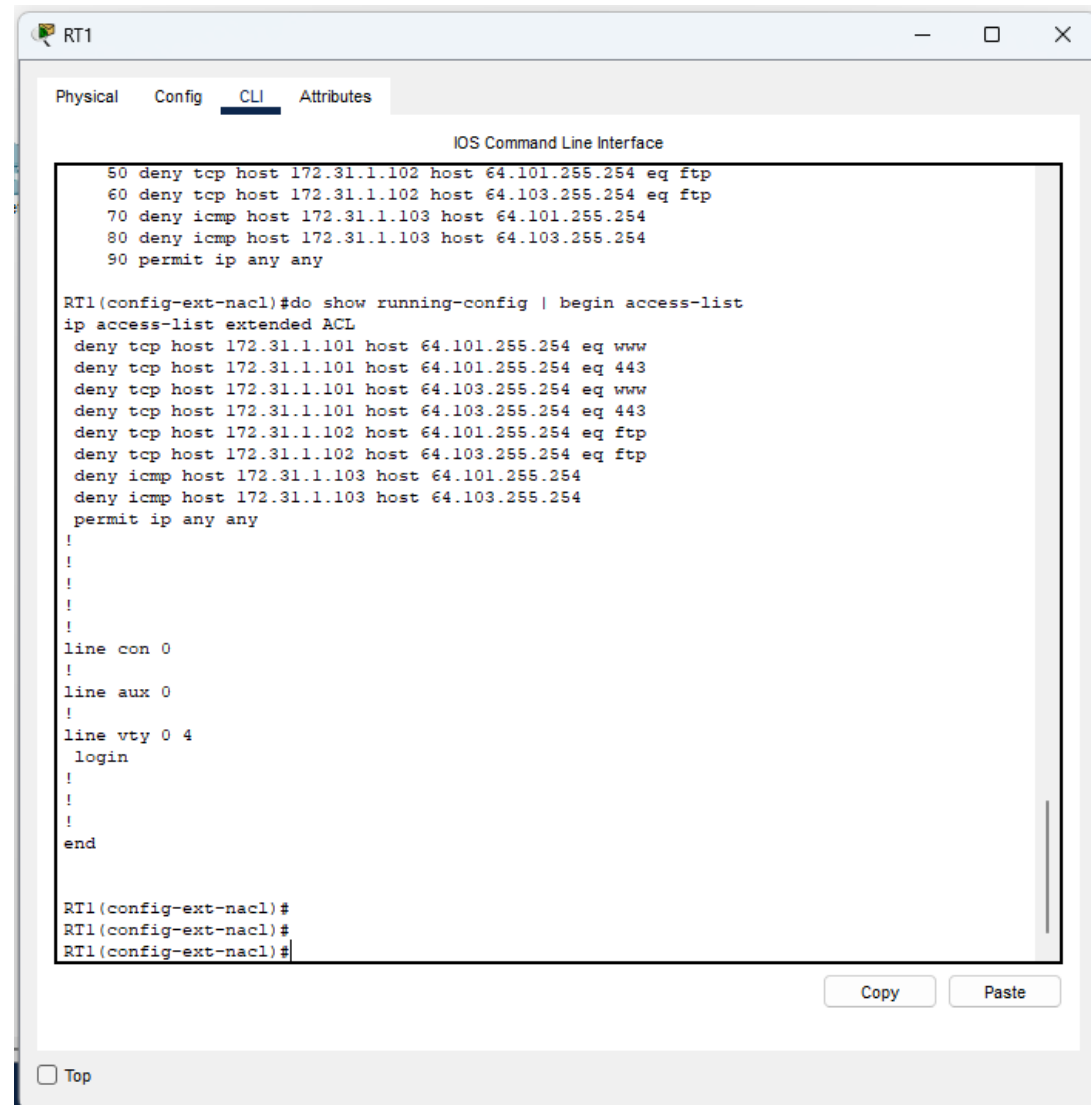
RT1(config-ext-nacl)#permit ip any any
RT1(config-ext-nacl)#do show ip access-list
Extended IP access list ACL
10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www
20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
40 deny tcp host 172.31.1.101 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

RT1(config-ext-nacl)#
```

Copy Paste

☐ Top

PASO 5: VERIFIQUE LA CONFIGURACIÓN DE LA LISTA DE ACCESO ANTES DE APLICARLA A UNA INTERFAZ.



The screenshot shows a network device CLI window titled "RT1". The window has tabs for "Physical", "Config", "CLI", and "Attributes", with "CLI" selected. The main area displays the "IOS Command Line Interface". The configuration shows an extended ACL with the following rules:

```
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
```

The user enters the command `RT1(config-ext-nacl)#do show running-config | begin access-list`, and the output shows the ACL configuration and other configuration lines:

```
ip access-list extended ACL
deny tcp host 172.31.1.101 host 64.101.255.254 eq www
deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
deny tcp host 172.31.1.101 host 64.103.255.254 eq www
deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
deny icmp host 172.31.1.103 host 64.101.255.254
deny icmp host 172.31.1.103 host 64.103.255.254
permit ip any any
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end

RT1(config-ext-nacl)#
RT1(config-ext-nacl)#
RT1(config-ext-nacl)#
```

At the bottom of the window, there are "Copy" and "Paste" buttons, and a "Top" button.

2. DESCRIPCIÓN TÉCNICA DE LA SOLUCIÓN

**Parte 2: Aplicar y verificar la ACL
Extendida**

PC1

Physical Config Desktop Programming Attributes

Command Prompt

```
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:\>ping 64.101.255.254

Pinging 64.101.255.254 with 32 bytes of data:

Reply from 64.101.255.254: bytes=32 time=12ms TTL=126
Reply from 64.101.255.254: bytes=32 time=2ms TTL=126
Reply from 64.101.255.254: bytes=32 time=29ms TTL=126
Reply from 64.101.255.254: bytes=32 time=28ms TTL=126

Ping statistics for 64.101.255.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 29ms, Average = 17ms

C:\>ping 64.103.255.254

Pinging 64.103.255.254 with 32 bytes of data:

Request timed out.
Reply from 64.103.255.254: bytes=32 time=28ms TTL=126
Reply from 64.103.255.254: bytes=32 time=29ms TTL=126
Reply from 64.103.255.254: bytes=32 time=28ms TTL=126

Ping statistics for 64.103.255.254:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 28ms, Maximum = 29ms, Average = 28ms

C:\>
```

☐ Top

PC3

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 34.103.255.254
Trying to connect...34.103.255.254

C:\>
C:\>
C:\>
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:\>ping 34.103.255.254

Pinging 34.103.255.254 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.

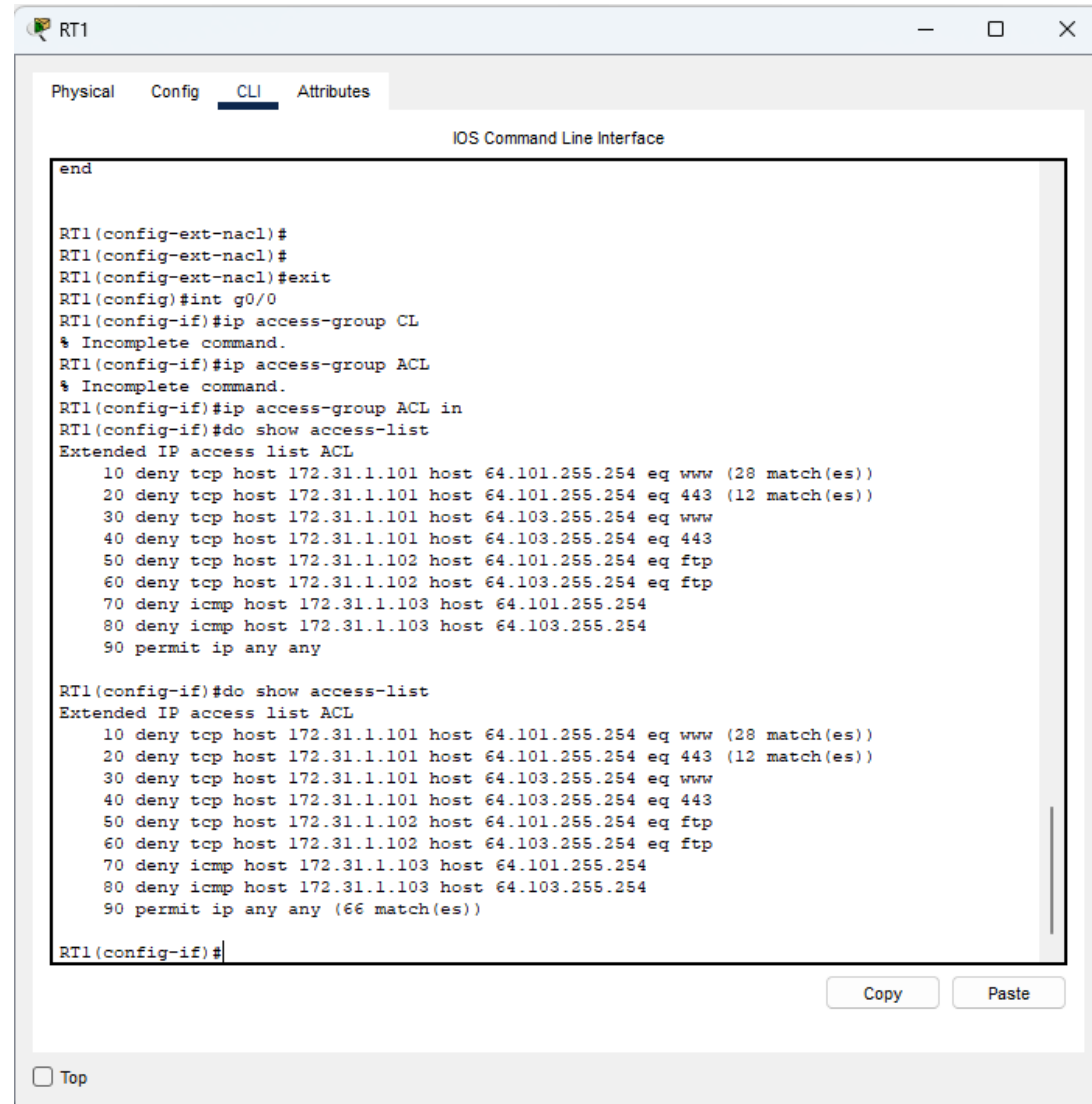
Ping statistics for 34.103.255.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

☐ Top

PASO I: APLICAR LA ACL A LA INTERFAZ APROPIADA EN EL SENTIDO CORRECTO.

PASO 2: PRUEBA EL ACCESO PARA CADA PC.



The screenshot shows a network simulator window titled "RT1" with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the "IOS Command Line Interface". The terminal output shows the configuration of an extended ACL named "ACL" on interface "g0/0". The ACL denies traffic from 172.31.1.101 to 64.101.255.254 (www) and 64.101.255.254 (443), denies traffic from 172.31.1.101 to 64.103.255.254 (www) and 64.103.255.254 (443), denies traffic from 172.31.1.102 to 64.101.255.254 (ftp) and 64.103.255.254 (ftp), denies traffic from 172.31.1.103 to 64.101.255.254 and 64.103.255.254, and permits traffic from any source to any destination. The output also shows the number of matches for each rule.

```
end

RT1(config-ext-nacl)#
RT1(config-ext-nacl)#
RT1(config-ext-nacl)#exit
RT1(config)#int g0/0
RT1(config-if)#ip access-group CL
% Incomplete command.
RT1(config-if)#ip access-group ACL
% Incomplete command.
RT1(config-if)#ip access-group ACL in
RT1(config-if)#do show access-list
Extended IP access list ACL
 10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www (28 match(es))
 20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443 (12 match(es))
 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

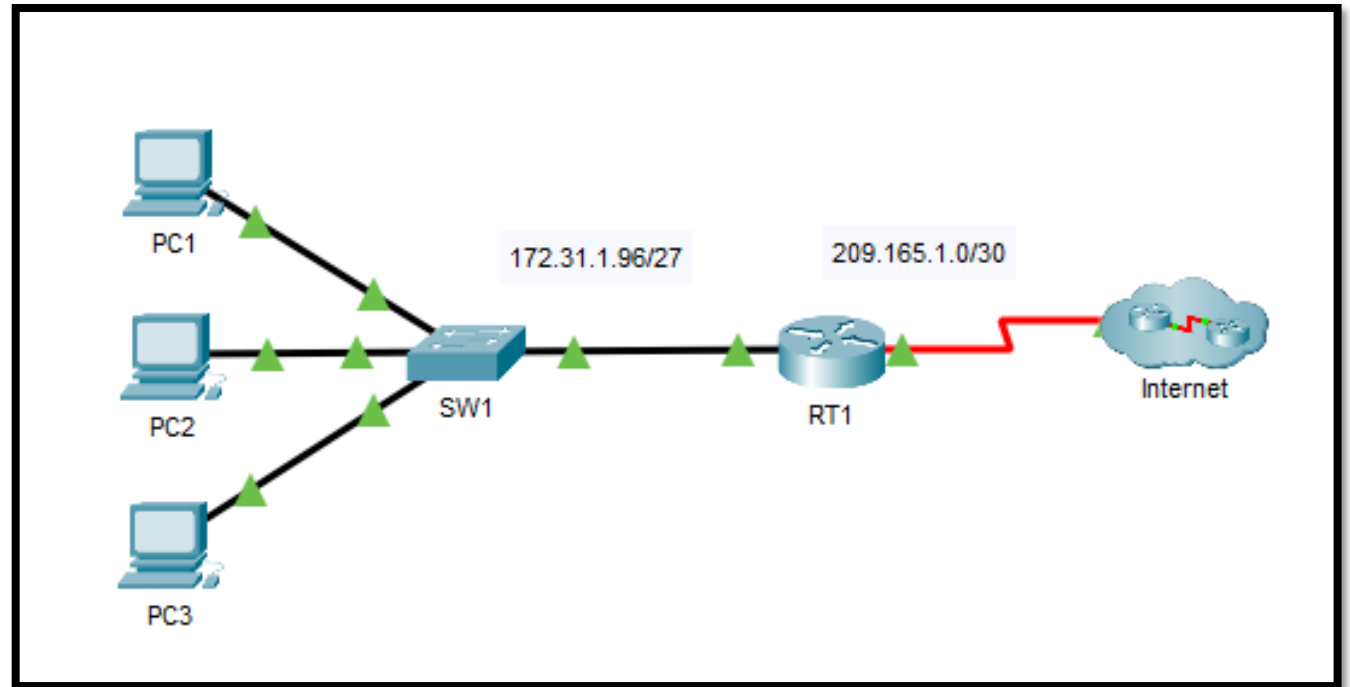
RT1(config-if)#do show access-list
Extended IP access list ACL
 10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www (28 match(es))
 20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443 (12 match(es))
 30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
 40 deny tcp host 172.31.1.101 host 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 (66 match(es))

RT1(config-if)#
```

Copy Paste

☐ Top

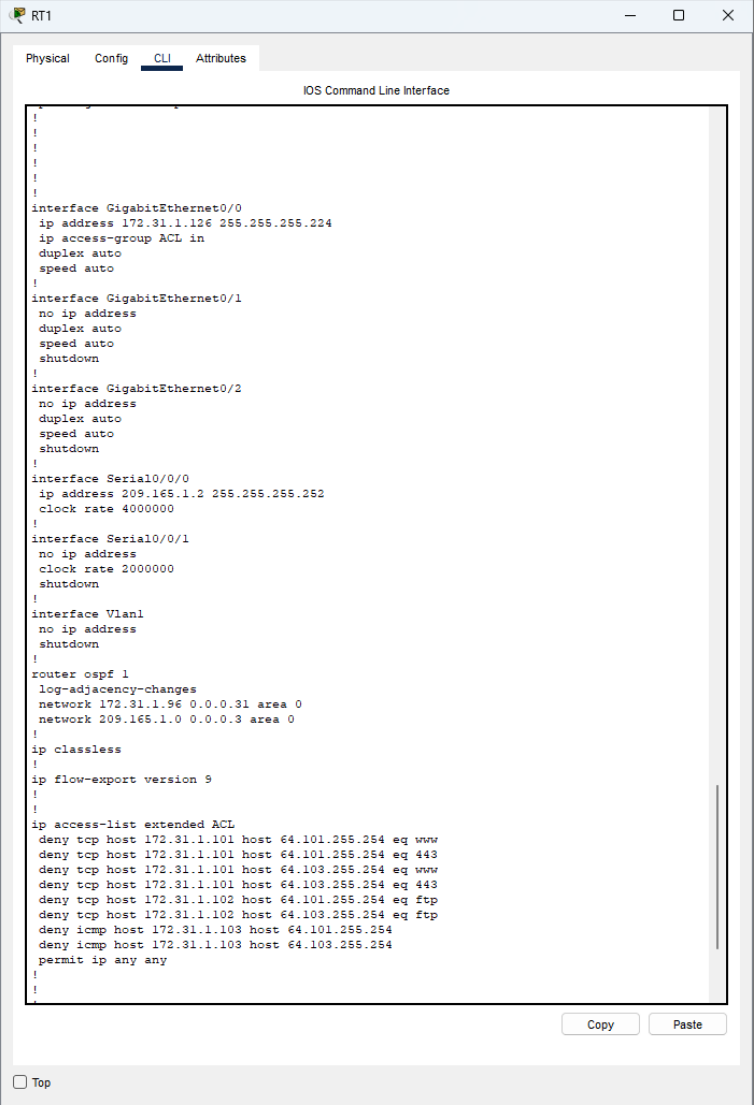
3.ESQUEMA GENERAL



4.SCRIPT CTC

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Puerta de enlace predeterminada
RT1	G0/0	172.31.1.126	255.255.255.224	N/D
	S0/0/0	209.165.1.2	255.255.255.252	
PC1	NIC	172.31.1.101	255.255.255.224	172.31.1.126
PC2	NIC	172.31.1.102	255.255.255.224	172.31.1.126
PC3	NIC	172.31.1.103	255.255.255.224	172.31.1.126
Servidor1	NIC	64.101.255.254		
Servidor2	NIC	64.103.255.254		

5. PRUEBAS



```
!
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 172.31.1.126 255.255.255.224
ip access-group ACL in
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
ip address 209.165.1.2 255.255.255.252
clock rate 4000000
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 172.31.1.96 0.0.0.31 area 0
network 209.165.1.0 0.0.0.3 area 0
!
ip classless
!
ip flow-export version 9
!
!
ip access-list extended ACL
deny tcp host 172.31.1.101 host 64.101.255.254 eq www
deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
deny tcp host 172.31.1.101 host 64.103.255.254 eq www
deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
deny icmp host 172.31.1.103 host 64.101.255.254
deny icmp host 172.31.1.103 host 64.103.255.254
permit ip any any
!
!
```

☐ Top