

Configuración e Interconexión de una Red WAN

Clara Yadexi Culchac Guerra

Universidad Nacional Abierta y a Distancia
Escuela de Ciencias Básicas Tecnología e Ingeniería
Cauca- Ingeniería de Sistemas- Diplomado de profundización cisco (diseño e
implementación de soluciones integradas LAN/ WAN)

Popayán

2018

Configuración e Interconexión de una Red WAN

Clara Yadexi Culchac Guerra

Trabajo de grado para optar el título de Ingeniería de Sistemas

Director:
Juan Carlos Vesga

Universidad Nacional Abierta y a Distancia
Escuela de Ciencias Básicas Tecnología e Ingeniería
Cauca- Ingeniería de Sistemas- Diplomado de profundización cisco (diseño e
implementación de soluciones integradas LAN/ WAN)

Popayán

2018

Dedicatoria

A mi familia y amigos que siempre estuvieron dispuestos ayudarme, a todos los que me rodearon y me impulsaron a continuar con mis estudios. A los docentes de la institución Educativa La Carbonera que estuvieron pendientes y me apoyaron para que pudiera estudiar en sus salas de internet gratuitamente. A las personas que siempre vieron en mí como un ejemplo a seguir.

A mi novio que me apoyo durante mi carrera y que muchas veces trasnocho junto a mí, y que hoy se siente orgulloso.

Agradecimientos

Agradezco a los tutores de la UNAD que durante mi carrera me orientaron, para sacar adelante cada uno de los cursos. También a mis compañeros que me guiaron y compartieron sus conocimientos conmigo.

Tabla de contenido

Dedicatoria	3
Agradecimientos	4
Introducción	8
Resumen	9
1. Configuración del direccionamiento ip acorde a la topología de red para cada uno de los dispositivos que forman parte del escenario	10
1.1 Configuración R1	13
1.2 Configuración R2	15
1.3 Configuración de Router 3	18
1.4 Configuración del servidor	19
1.5 Configuración S1	19
1.6 Configuración S3	22
1.7 Pruebas de conectividad	24
2. Configuración del protocolo de enrutamiento ospfv2	26
2.2 Configuración R2 bajo el protocolo de enrutamiento OSPFv2 área 0	29
2.3 Configuración R3 bajo el protocolo de enrutamiento OSPFv2 área 0	31
2.4 Verificación de la información OSPF	32
2.4 Se visualiza lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface	34
2.6 Verificación de protocolos	36
2.7 Se visualiza el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router	36
3. Implementar DHCP and NAT para ipv4	38
3.2 Se configura Configurar R1 como servidor DHCP para las VLANs 30 y 40. Y se Reserva las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas	39
3.3 Configuración de NAT estático y dinámico en R2	40
3.4 Verificación de DHCP y NAT estático	41
3.5 Configuración de listas de acceso de tipo estándar para restringir o permitir tráfico	42
3.6 Configuración de listas de acceso de tipo extendido o nombradas a su criterio para restringir o permitir tráfico	45
Bibliografía	52

Lista de Imágenes

Imagen 1. Reinicio de Router 1	11
Imagen 2. Reinicio de Switch 1	12
Imagen 3. Inicio de internet PC	13
Imagen 4. Configuración R1	14
Imagen 5. Configuración R1	15
Imagen 6. Configuración R2	16
Imagen 7. Configuración R2	17
Imagen 8. Configuración R3	18
Imagen 9. Configuración del servidor	19
Imagen 10. Configuración S1	20
Imagen 11. Configuración S1	21
Imagen 12. Configuración S3	22
Imagen 13. Configuración S3	23
Imagen 14. Pruebas de conectividad	24
Tabla 1. Tabla de enrutamiento OSPFv2	26
Imagen 15. Configuración R1 protocolo OSPFv2	27
Imagen 16. Verificación de la configuración R2	28
Imagen 17. Configuración R2 protocolo OSPFv2	29
Imagen 18. Verificación de la configuración r3	30
Imagen 19. Configuración R3 protocolo OSPFv2	31
Imagen 20. Verificación de la información OSPFv2	32
Imagen 21. Verificación de la información OSPFv2 en R1	33
Imagen 22. Verificación de la información OSPFv2 en R2	34
Imagen 23. Verificación de la información OSPFv2 en R2	35
Imagen 24. Visualización del OSPF Process ID	37
Imagen 25. Configuración de R1 como servidor DHCP	39
Imagen 26. Configuración de PC-A como DHCP	40
Imagen 27. Configuración de PC-A como DHCP	40
Imagen 28. Configuración NAT estático y dinámico en R2	41

Imagen 29. Verificación NAT estático y dinámico	42
Imagen 30. Configuración de listas	42
Imagen 31. Verificación de listas	43
Imagen 32. Verificación de listas	43
Imagen 33. Configuración de listas de tipo extendido	46
Imagen 34. Configuración de listas R2.....	47
Imagen 35. Verificación de listas	50

Introducción

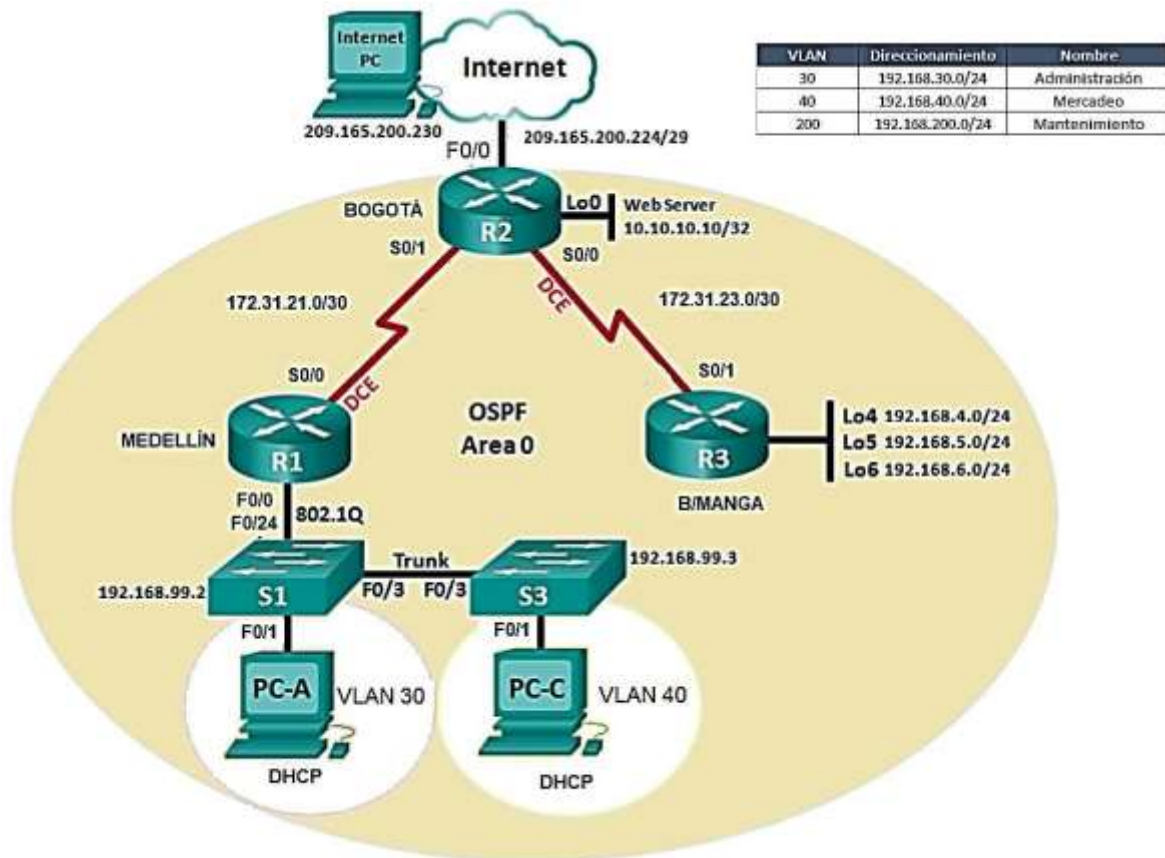
En el presente trabajo se desarrolla la prueba de habilidades prácticas CCNA 2 en la cual se busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado, los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Se realiza la práctica en Packet Tracer y la documentación en un documento de PDF, los respectivos procesos de la solución correspondiente al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante el desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, show ip route entre otros.

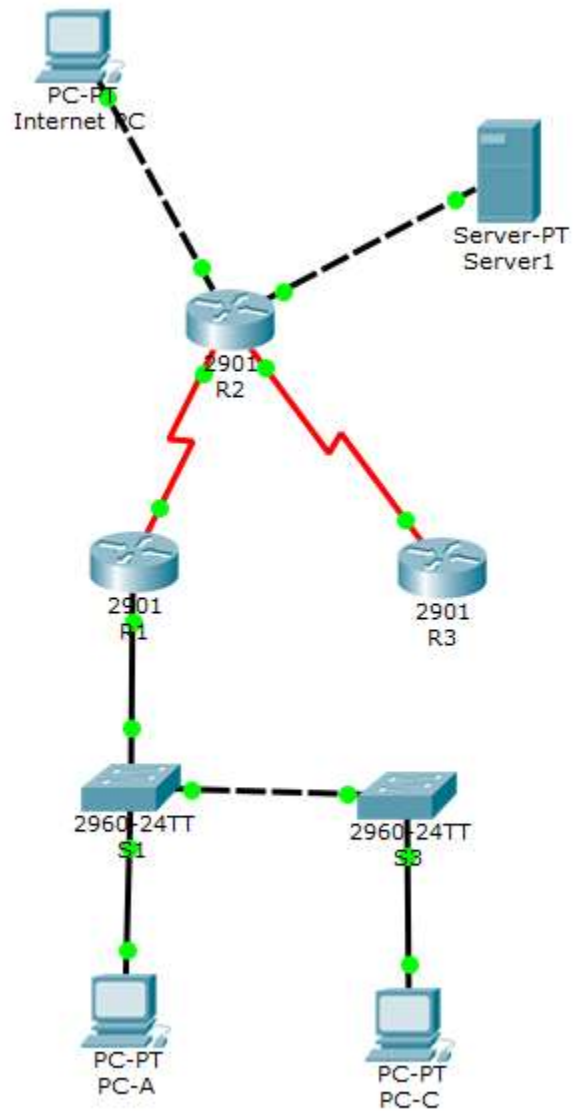
Resumen

Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Bogotá, Medellín y Bucaramanga, en donde se deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

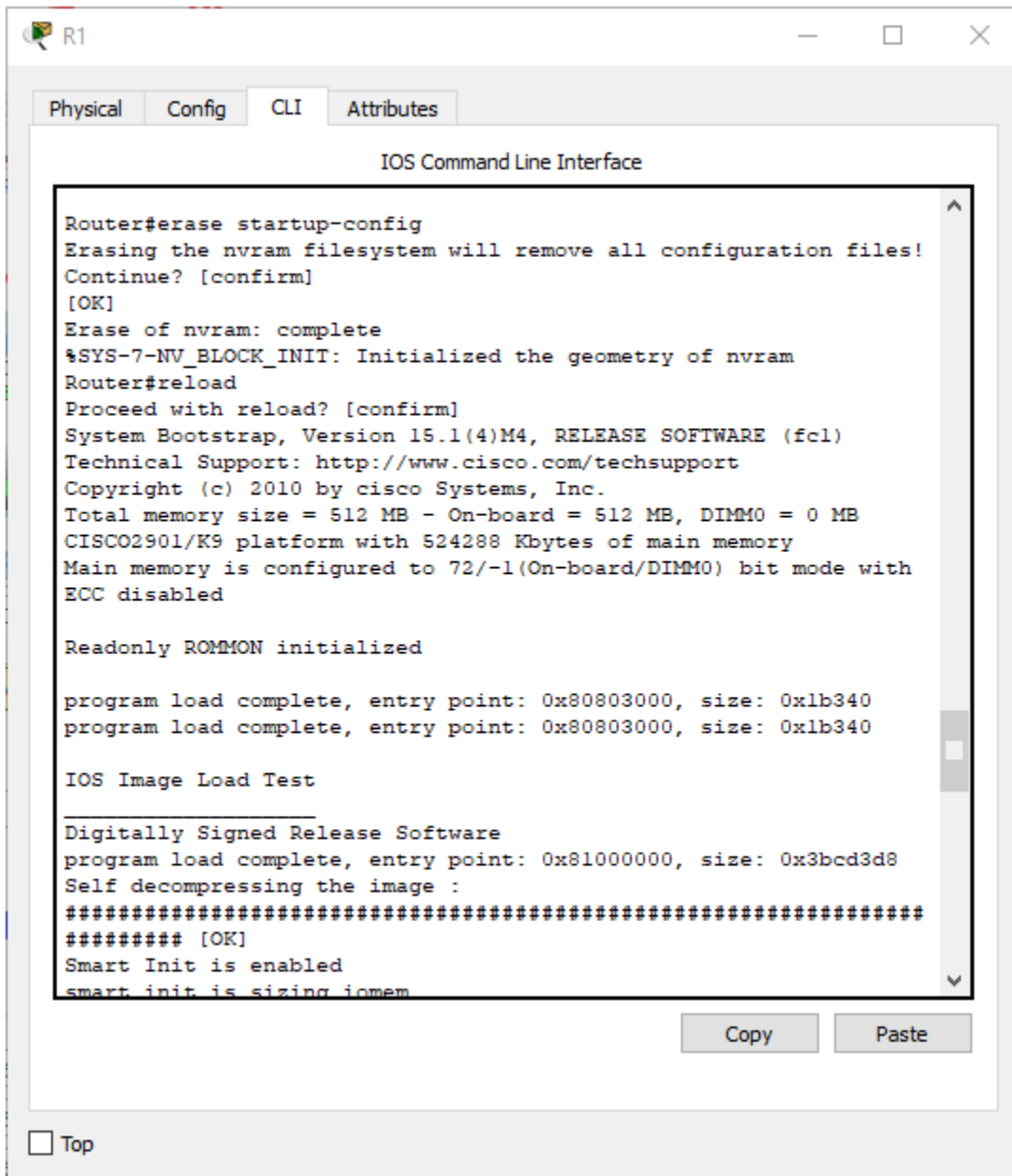
Topología de red



1. CONFIGURACIÓN DEL DIRECCIONAMIENTO IP ACORDE A LA TOPOLOGÍA DE RED PARA CADA UNO DE LOS DISPOSITIVOS QUE FORMAN PARTE DEL ESCENARIO



Una vez creada la topología procedemos a Iniciar y reiniciar los routers y los switches, utilizando el comando **erase start-config** y **reload**.



```
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by Cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO2901/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 72/-1(On-board/DIMM0) bit mode with
ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x3bcd3d8
Self decompressing the image :
#####
##### [OK]
Smart Init is enabled
smart_init is sizing iomem
```

Imagen 1. Reinicio de Router 1

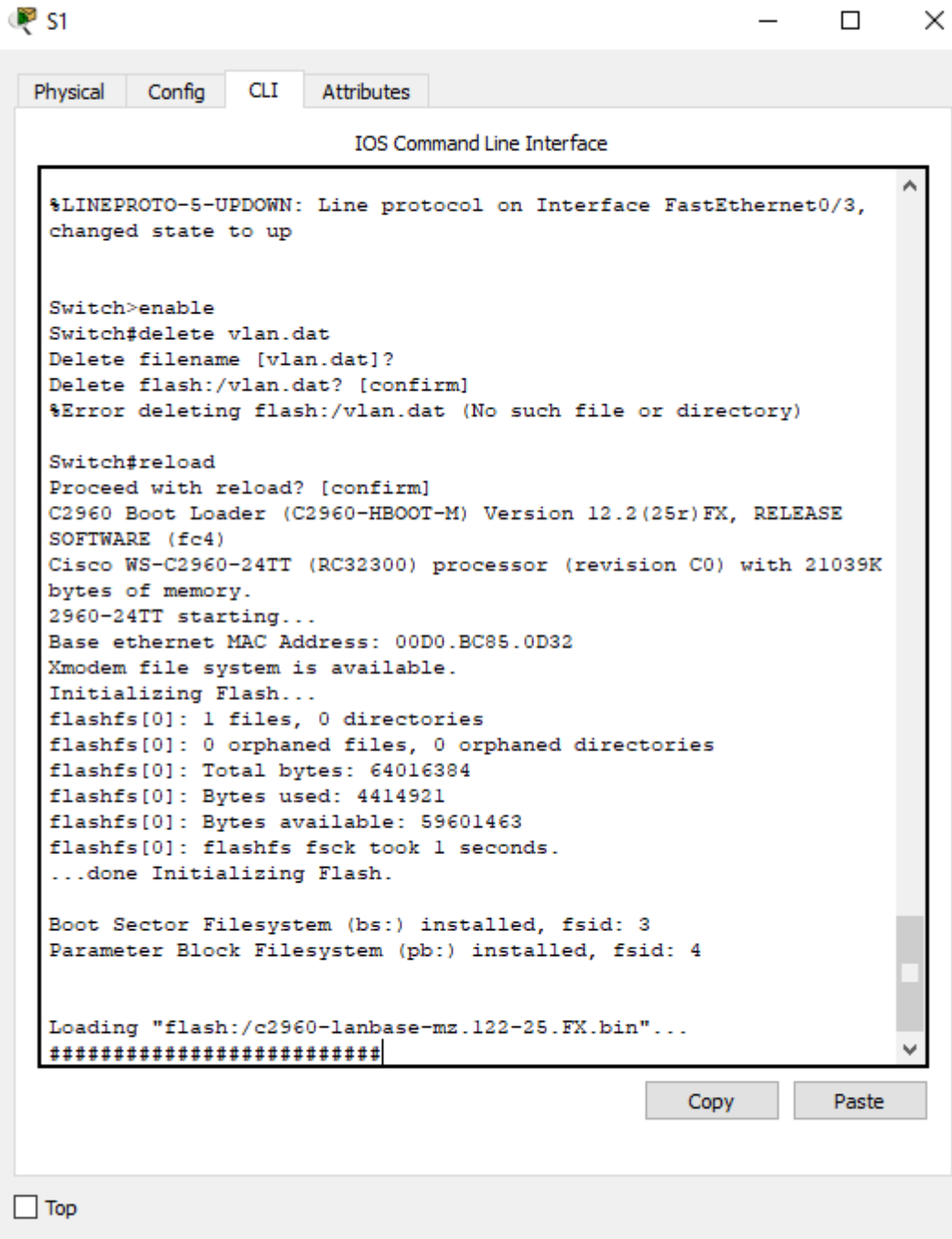


Imagen 2. Reinicio de Switch 1

Iniciamos con la Configuración de internet PC

Internet PC

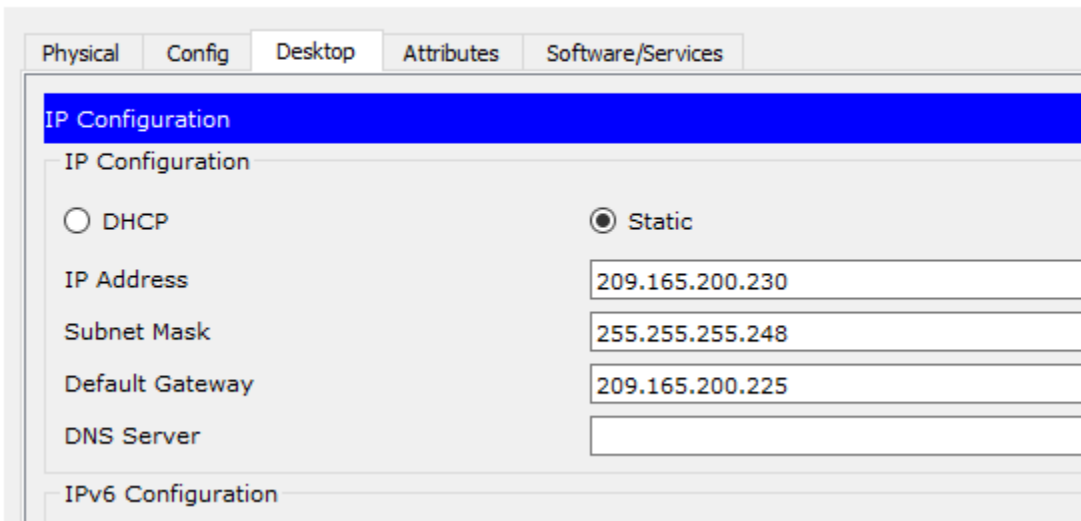


Imagen 3. Inicio de internet PC

1.1 Configuración R1

Para R1 se agrega el nombre del router como R1, se crea una contraseña en modo privilegiado (class), contraseña de acceso a la consola (cisco) y la contraseña de acceso mediante telnet (Cisco). También se crea un mensaje para personas no autorizadas. Se Configura VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.

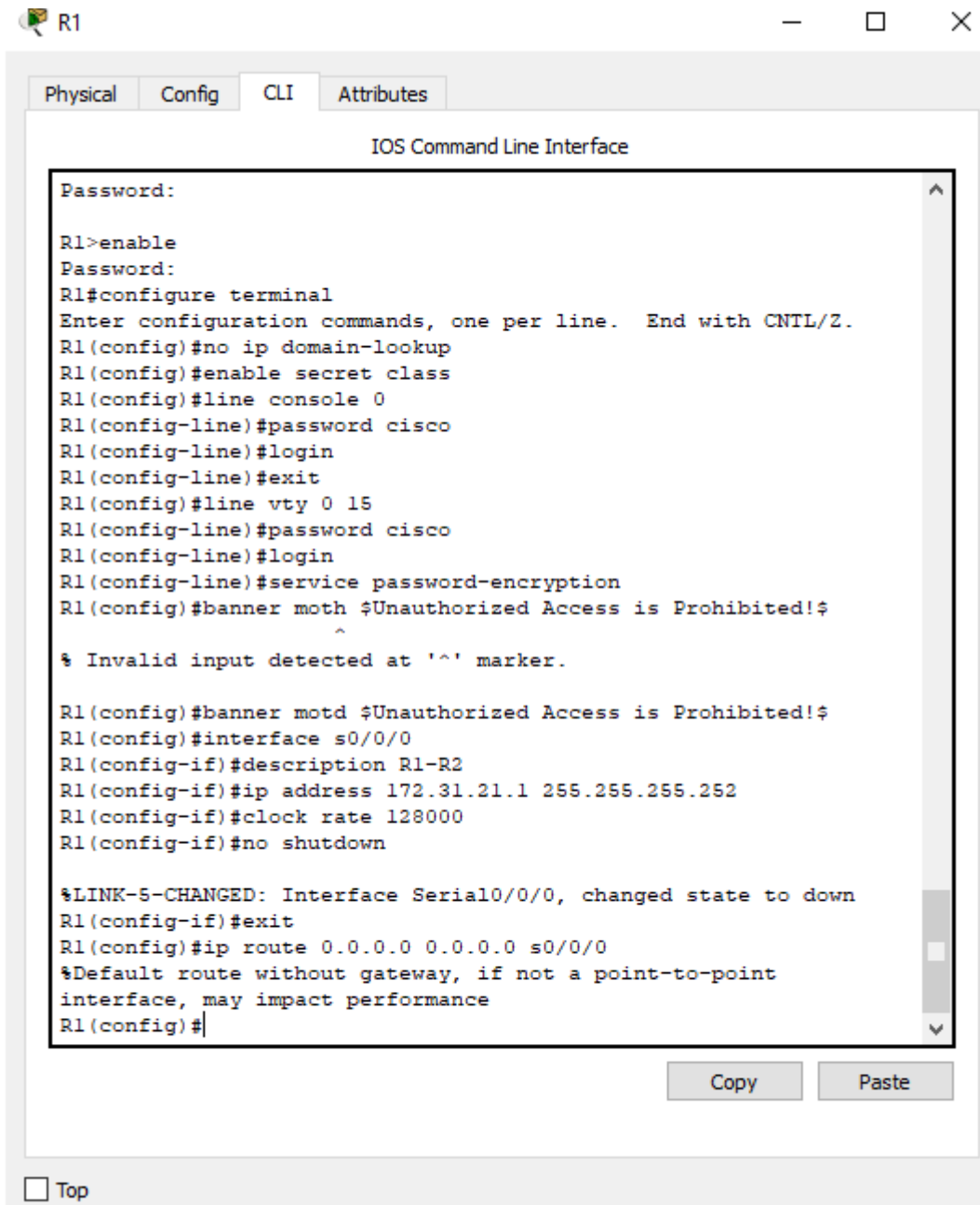


Imagen 4. Configuración R1

```
IOS Command Line Interface

User Access Verification

Password:
Password:

R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/1.30
R1(config-subif)#encapsulation do
% Incomplete command.
R1(config-subif)#description Lan_Adm
R1(config-subif)#encapsulation dot1Q?
dot1Q
R1(config-subif)#encapsulation dot1Q ?
<1-1005> IEEE 802.1Q VLAN ID
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#int g0/1.40
R1(config-subif)#description Lan_Mer
R1(config-subif)#encapsulation dot1Q 40
R1(config-subif)#ip address 192.168.40.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/1.200
R1(config-subif)#description Lan_mant
R1(config-subif)#encapsulation dot1Q 200
R1(config-subif)#ip address 192.168.200.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/1
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.30, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1.30, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.40, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1.40, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.200, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1.200, changed state to up

Copy Paste

 Top
```

Imagen 5. Configuración R1

1.2 Configuración R2

Para R2 se agregó el nombre del router como R2, se creó una contraseña en modo privilegiado (class), contraseña de acceso a la consola (cisco) y la contraseña de acceso mediante telnet (Cisco). También se creó un mensaje para personas no

autorizadas. Se configura VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.

```
R2>enable
Password:
R2#enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2 (config)#no ip domain-lookup
R2 (config)#hostname R2
R2 (config)#enable secret class
R2 (config)#line console 0
R2 (config-line)#password cisco
R2 (config-line)#login
R2 (config-line)#exit
R2 (config)#line vty 0 15
R2 (config-line)#password cisco
R2 (config-line)#login
R2 (config-line)#service password-encryption
R2 (config)#ip http server
^
% Invalid input detected at '^' marker.

R2 (config)#banner motd $Unauthorized Access is Prohibited!$
R2 (config)#interface s0/0/0
R2 (config-if)#description R2-R1
R2 (config-if)#ip address 172.31.21.2 255.255.255.252
R2 (config-if)#no shutdown
R2 (config-if)#exit
R2 (config)#interface s0/0/1
R2 (config-if)#description R2-R3
R2 (config-if)#ip address 172.31.23.1 255.255.255.252
R2 (config-if)#clock rate 128000
This command applies only to DCE interfaces
R2 (config-if)#no shutdown
R2 (config-if)#exit
R2 (config)#interface g0/0
R2 (config-if)#description R2-Internet
R2 (config-if)#ip address 209.165.200.225 255.255.255.252
R2 (config-if)#no shutdown
R2 (config-if)#interface loopback 0
R2 (config-if)#description web_server
R2 (config-if)#ip address 10.10.10.10 255.255.255.255
R2 (config-if)#no shutdown
R2 (config-if)#exit
R2 (config)#
R2 (config)#ip route 0.0.0.0 0.0.0.0 g0/0
R2 (config)#
R2 (config)#
R2 (config)#
R2 (config)#
```

Imagen 6. Configuración R2

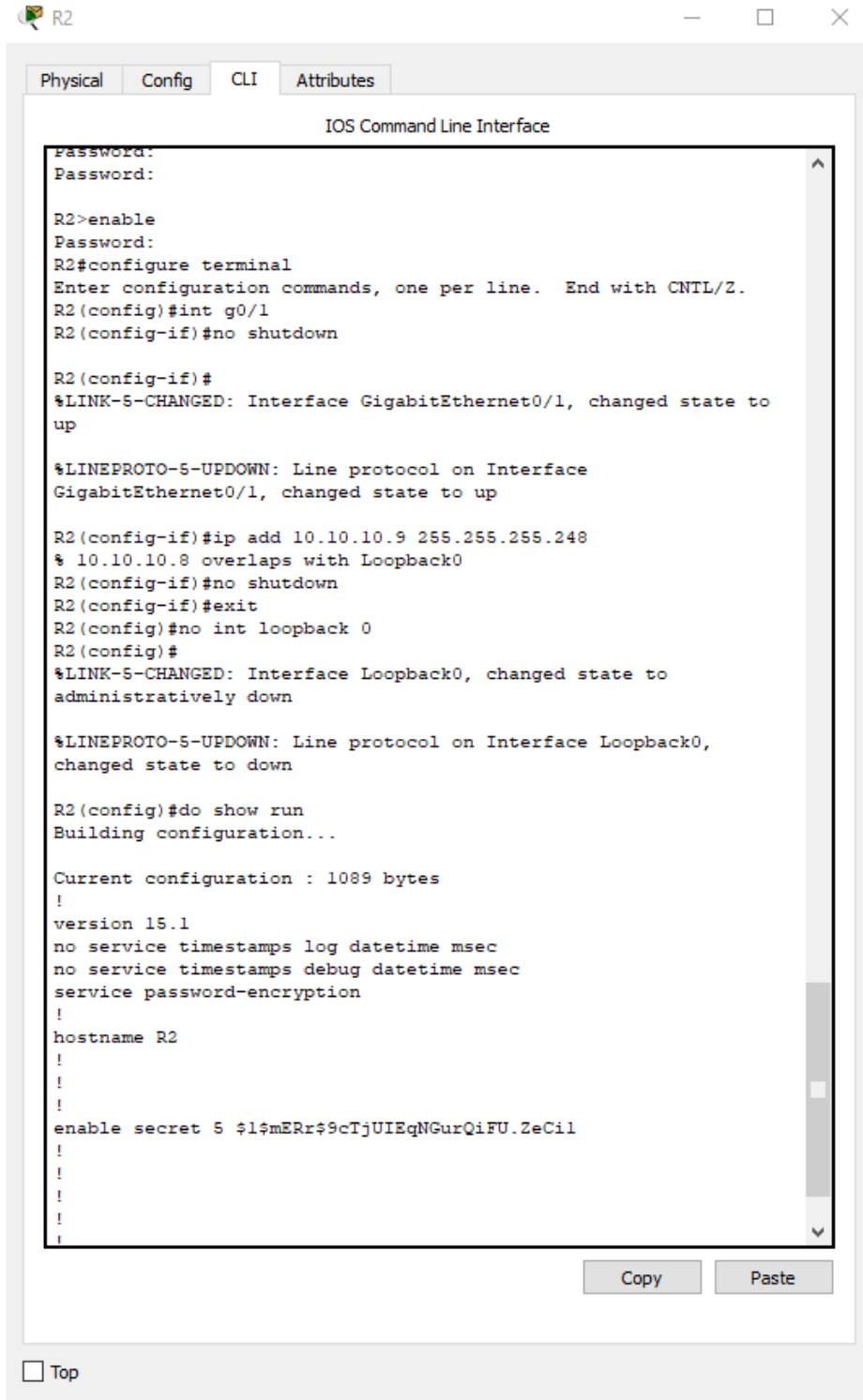


Imagen 7. Configuración R2

1.3 Configuración de Router 3

Para R3 se agregó el nombre del router como R2, se creó una contraseña en modo privilegiado (class), contraseña de acceso a la consola (cisco) y la contraseña de acceso mediante telnet (Cisco). También se crea un mensaje para personas no autorizadas. Se configura VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd $Unauthorized Access is Prohibited!$
R3(config)#interface s0/0/1
R3(config-if)#description R3-R2
R3(config-if)#ip address 172.31.23.2 255.255.255.252
R3(config-if)#no shutdown

R3(config-if)#exit
R3(config)#interface loopback 4
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface loopback 5
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface loopback 6
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

%LINK-5-CHANGED: Interface Loopback4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4,
changed state to up

%LINK-5-CHANGED: Interface Loopback5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5,
changed state to up

%LINK-5-CHANGED: Interface Loopback6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up
```

Imagen 8. Configuración R3

1.4 Configuración del servidor

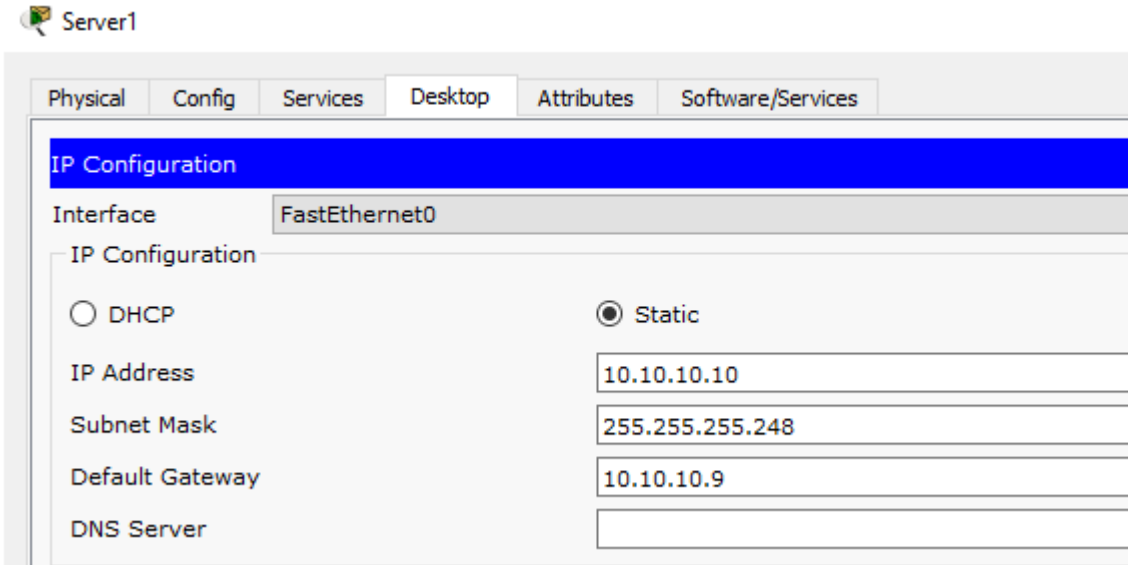


Imagen 9. Configuración del servidor

1.5 Configuración S1

Para el S1 se agrega el nombre del switch como S1, se crea una contraseña en modo privilegiado (class), contraseña de acceso a la consola (cisco) y la contraseña de acceso mediante telnet (Cisco). También se crea un mensaje para personas no autorizadas. Se asigna direcciones IP acorde a los lineamientos. Se configura VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida. Se desactiva todas las interfaces que no son utilizadas en el esquema de red.

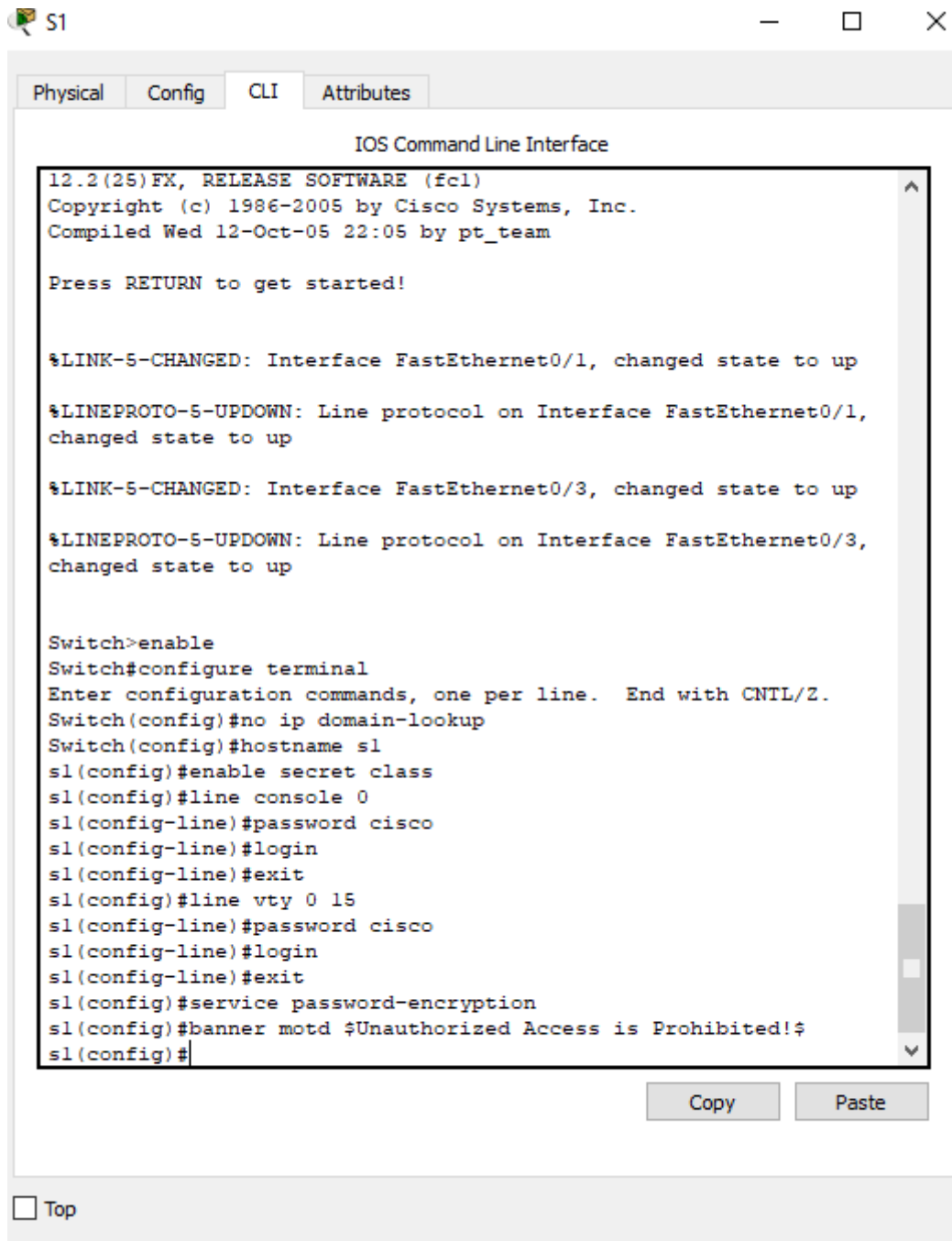


Imagen 10. Configuración S1

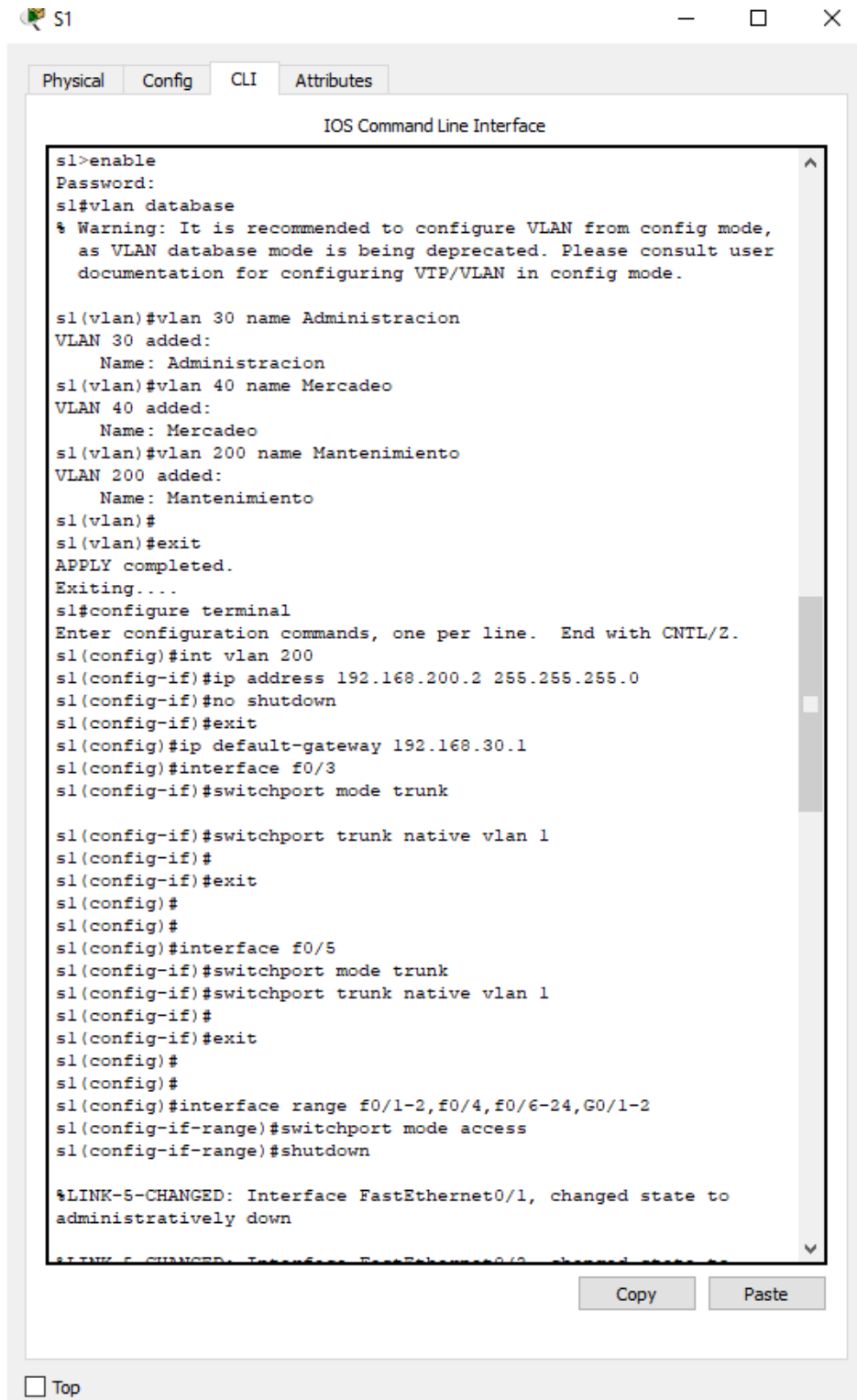


Imagen 11. Configuración S1

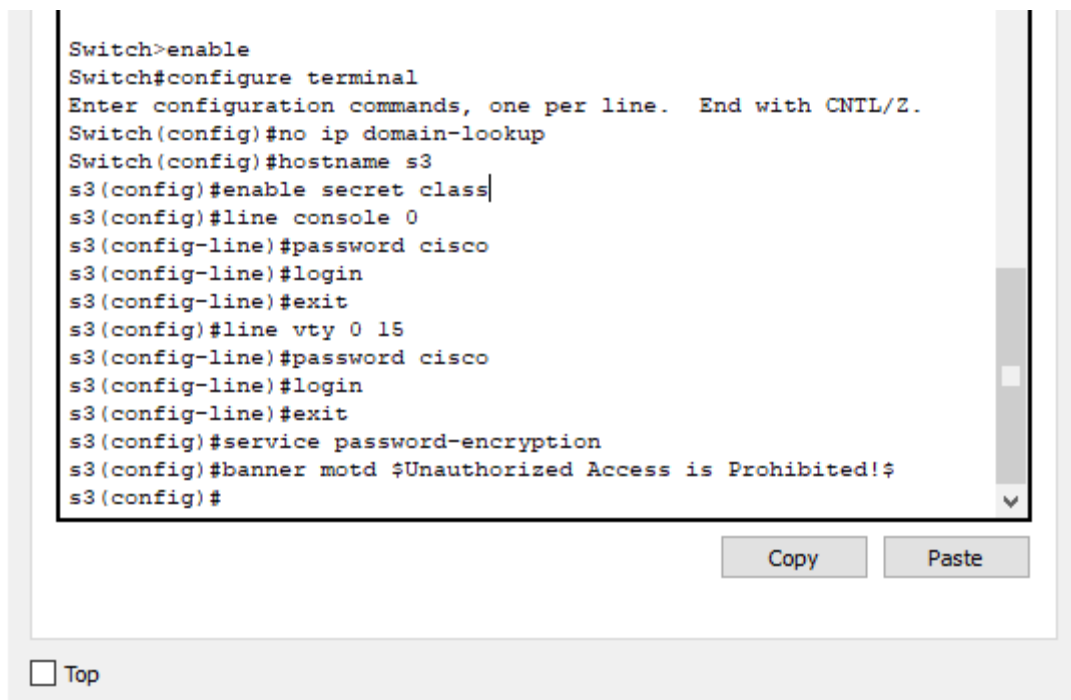
```
s1(config-if-range)#exit
s1(config)#
s1(config)#interface f0/6
s1(config-if)#no shutdown

s1(config-if)#switchport mode access
s1(config-if)#switchport access vlan 30
s1(config-if)#exit
s1(config)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up
```

1.6 Configuración S3

Para el S3 se agrega el nombre del switch como S3, se crea una contraseña en modo privilegiado (class), contraseña de acceso a la consola (cisco) y la contraseña de acceso mediante telnet (Cisco). También se crea un mensaje para personas no autorizadas. Se asigna direcciones IP acorde a los lineamientos. Se configura VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida. Se desactiva todas las interfaces que no son utilizadas en el esquema de red.

. En el Switch S3 se deshabilita el DNS lookup.



```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname s3
s3(config)#enable secret class
s3(config)#line console 0
s3(config-line)#password cisco
s3(config-line)#login
s3(config-line)#exit
s3(config)#line vty 0 15
s3(config-line)#password cisco
s3(config-line)#login
s3(config-line)#exit
s3(config)#service password-encryption
s3(config)#banner motd $Unauthorized Access is Prohibited!$
s3(config)#
```

Copy Paste

Top

Imagen 12. Configuración S3

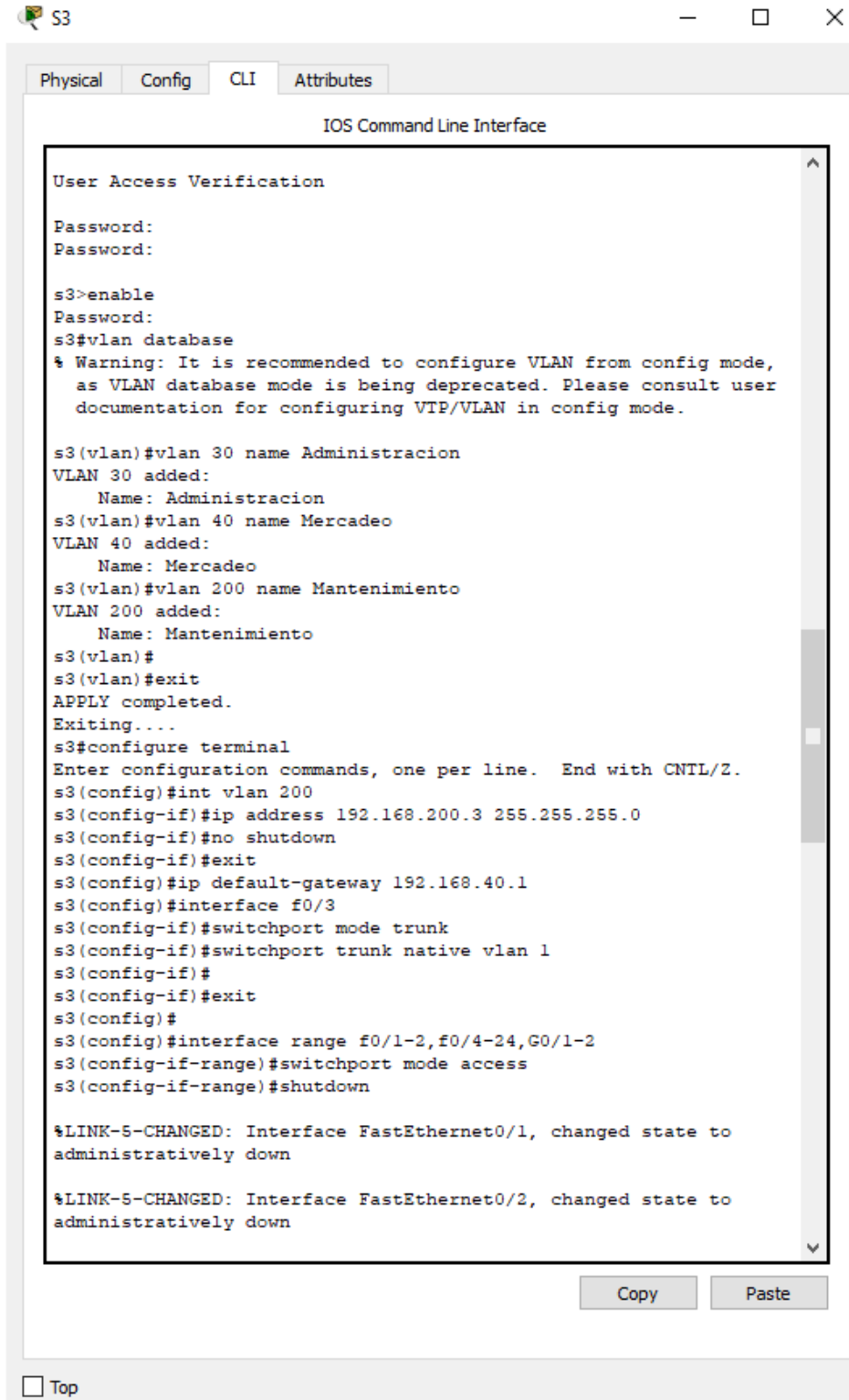


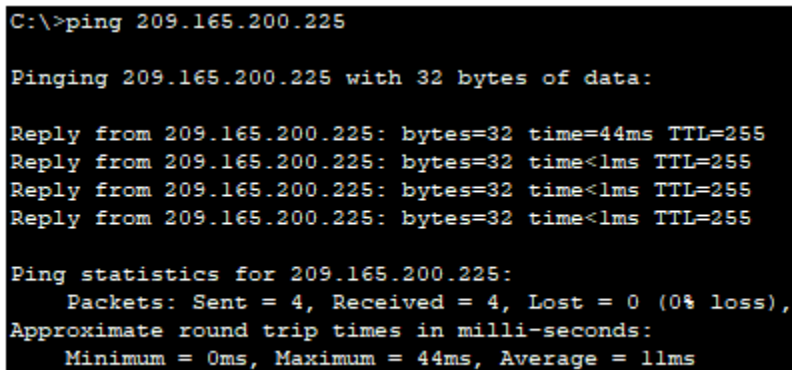
Imagen 13. Configuración S3

```
s3(config-if-range)#exit
s3(config)#
s3(config)#interface f0/18
s3(config-if)#no shutdown

s3(config-if)#switchport mode access
s3(config-if)#switchport access vlan 40
s3(config-if)#exit
%LINK-5-CHANGED: Interface Vlan200, changed state to up
```

1.7 Pruebas de conectividad

R1 a R2 S0/0/0



```
C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=44ms TTL=255
Reply from 209.165.200.225: bytes=32 time<1ms TTL=255
Reply from 209.165.200.225: bytes=32 time<1ms TTL=255
Reply from 209.165.200.225: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 44ms, Average = 11ms
```

Imagen 14. Pruebas de conectividad

R2 a R3 S0/0/1

```
R2#ping 172.31.23.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.2, timeout is 2
seconds:
|
```

S1 to R1 Vlan 200

```
s1#ping 192.168.200.1
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2  
seconds:  
.!!!!  
Success rate is 80 percent (4/5), round-trip min/avg/max =  
0/15/62 ms
```

```
s1#
```

S3 a R1 Vlan 200

```
s3#ping 192.168.200.1
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2  
seconds:  
.!!!!  
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/1/4  
ms
```

```
s3#
```

S1 a R1 Vlan 30

```
s1#ping 192.168.30.1
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2  
seconds:  
.!!!!  
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0  
ms
```

S3 a R1 Vlan 40

```
s3#ping 192.168.40.1
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.40.1, timeout is 2  
seconds:  
.!!!!  
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1  
ms
```

2. CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO OSPFV2

Configuración Ítem	Especificación
Router ID R1	1.1.1.1
Router ID R2	2.2.2.2
Router ID R3	3.3.3.3
Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales en	128Kb/s
Ajustar el costo en la métrica de S0/0 a	7500

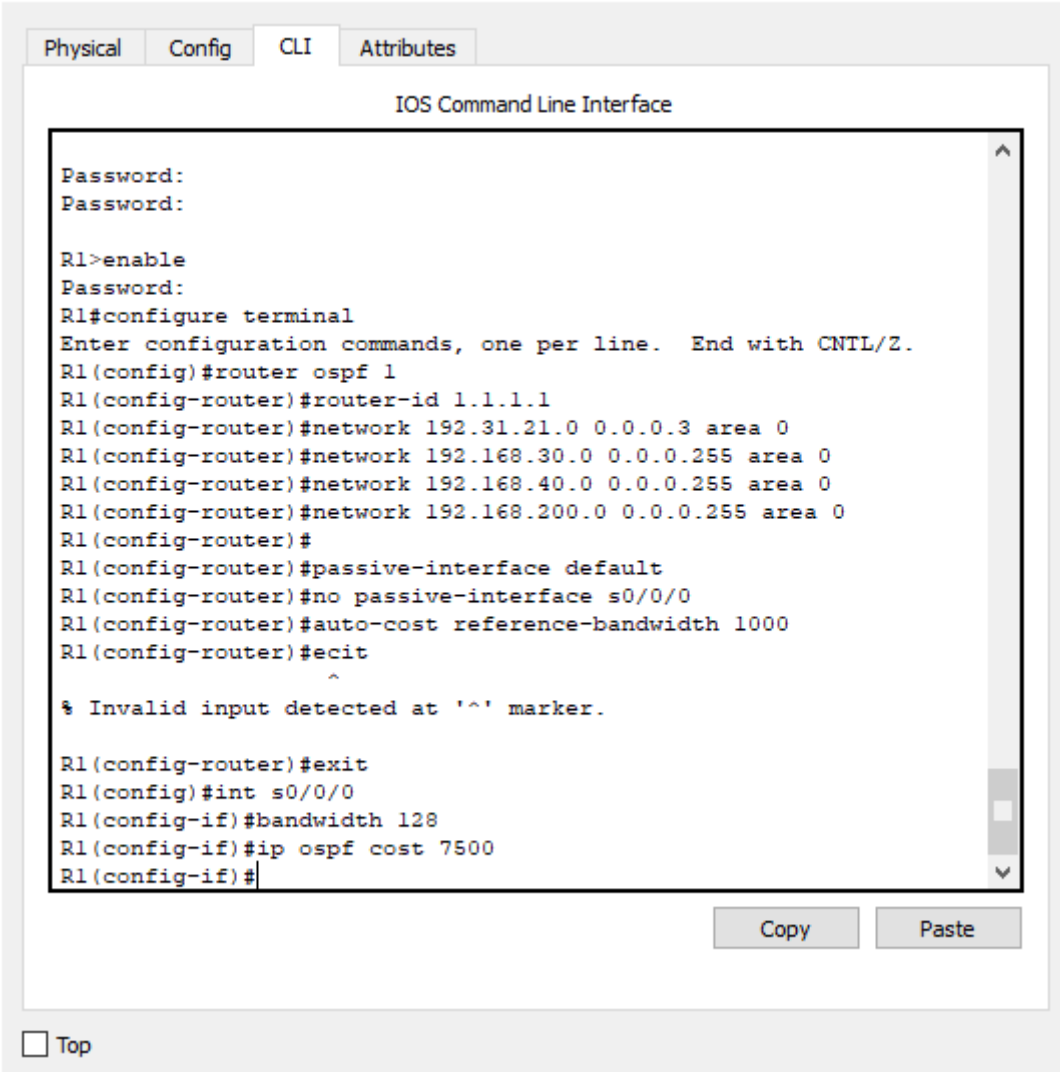
Tabla 1. Tabla de enrutamiento OSPFv2

Se verifica la configuración

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#do show ip route connect
C 172.31.21.0/30 is directly connected, Serial0/0/0
C 192.168.30.0/24 is directly connected,
GigabitEthernet0/1.30
C 192.168.40.0/24 is directly connected,
GigabitEthernet0/1.40
C 192.168.200.0/24 is directly connected,
GigabitEthernet0/1.200

R1(config)#
```

2.1 Configuración R1 bajo el protocolo de enrutamiento OSPFv2 Area 0



```
Physical Config CLI Attributes
IOS Command Line Interface

Password:
Password:

R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 192.31.21.0 0.0.0.3 area 0
R1(config-router)#network 192.168.30.0 0.0.0.255 area 0
R1(config-router)#network 192.168.40.0 0.0.0.255 area 0
R1(config-router)#network 192.168.200.0 0.0.0.255 area 0
R1(config-router)#
R1(config-router)#passive-interface default
R1(config-router)#no passive-interface s0/0/0
R1(config-router)#auto-cost reference-bandwidth 1000
R1(config-router)#exit
^
% Invalid input detected at '^' marker.

R1(config-router)#exit
R1(config)#int s0/0/0
R1(config-if)#bandwidth 128
R1(config-if)#ip ospf cost 7500
R1(config-if)#
```

Copy Paste

Top

Imagen 15. Configuración R1 protocolo OSPFv2

Se verifica la configuración

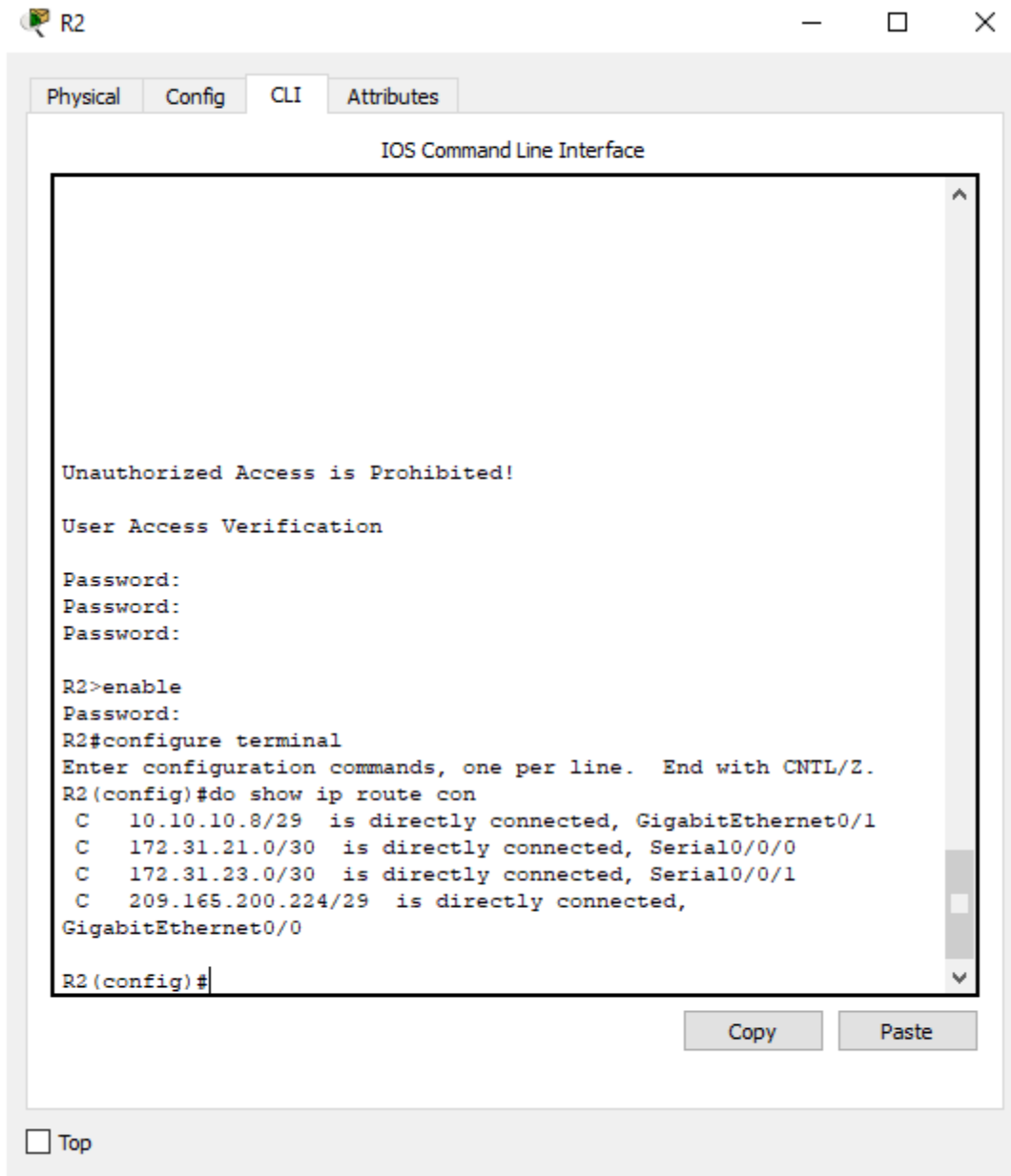
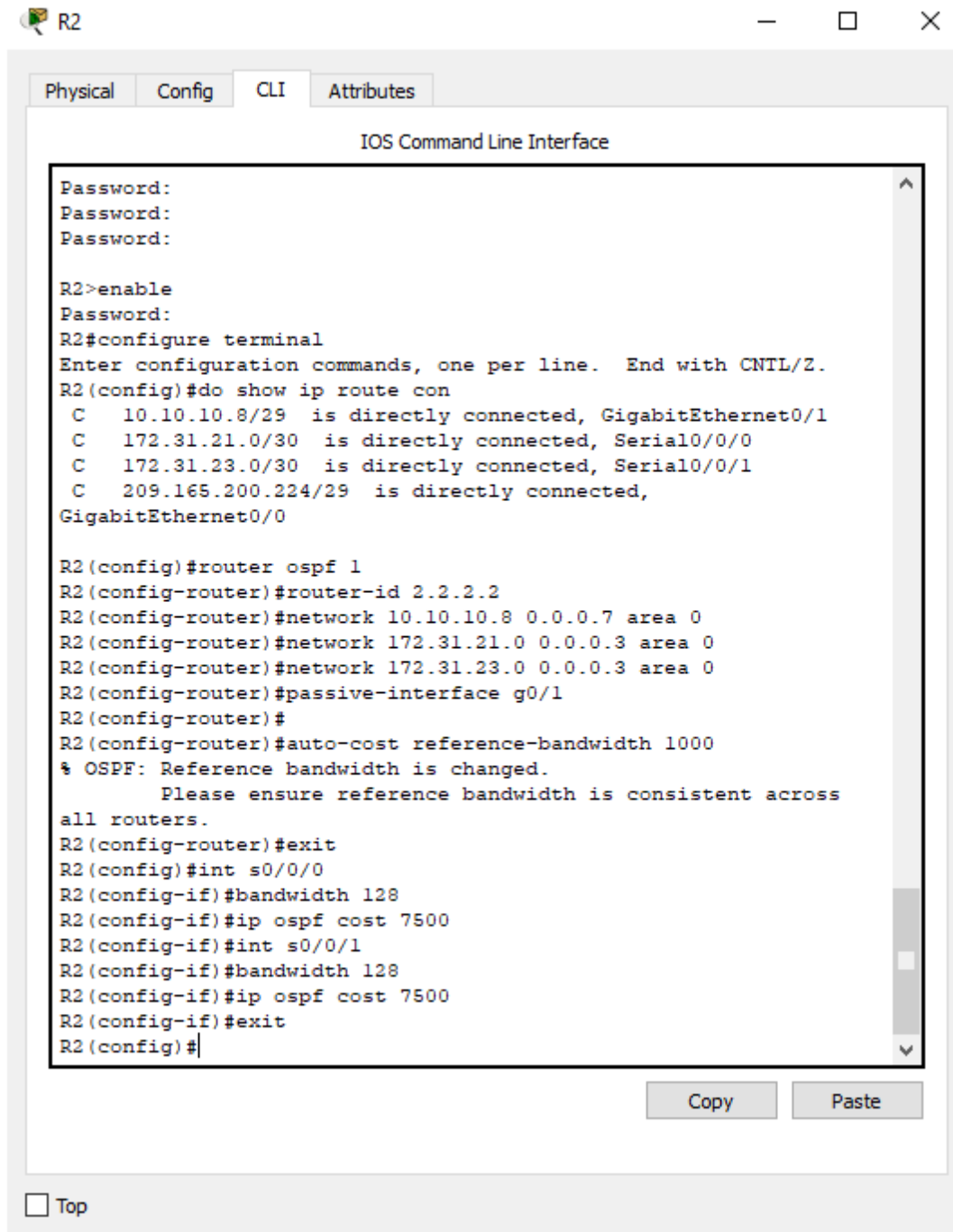


Imagen 16. Verificación de la configuración R2

2.2 Configuración R2 bajo el protocolo de enrutamiento OSPFv2 área 0



```

R2
Physical Config CLI Attributes
IOS Command Line Interface
Password:
Password:
Password:
R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#do show ip route con
C 10.10.10.8/29 is directly connected, GigabitEthernet0/1
C 172.31.21.0/30 is directly connected, Serial0/0/0
C 172.31.23.0/30 is directly connected, Serial0/0/1
C 209.165.200.224/29 is directly connected,
GigabitEthernet0/0
R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 10.10.10.8 0.0.0.7 area 0
R2(config-router)#network 172.31.21.0 0.0.0.3 area 0
R2(config-router)#network 172.31.23.0 0.0.0.3 area 0
R2(config-router)#passive-interface g0/1
R2(config-router)#
R2(config-router)#auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across
all routers.
R2(config-router)#exit
R2(config)#int s0/0/0
R2(config-if)#bandwidth 128
R2(config-if)#ip ospf cost 7500
R2(config-if)#int s0/0/1
R2(config-if)#bandwidth 128
R2(config-if)#ip ospf cost 7500
R2(config-if)#exit
R2(config)#
Copy Paste
Top
```

Imagen 17. Configuración R2 protocolo OSPFv2

Se verifica la configuración

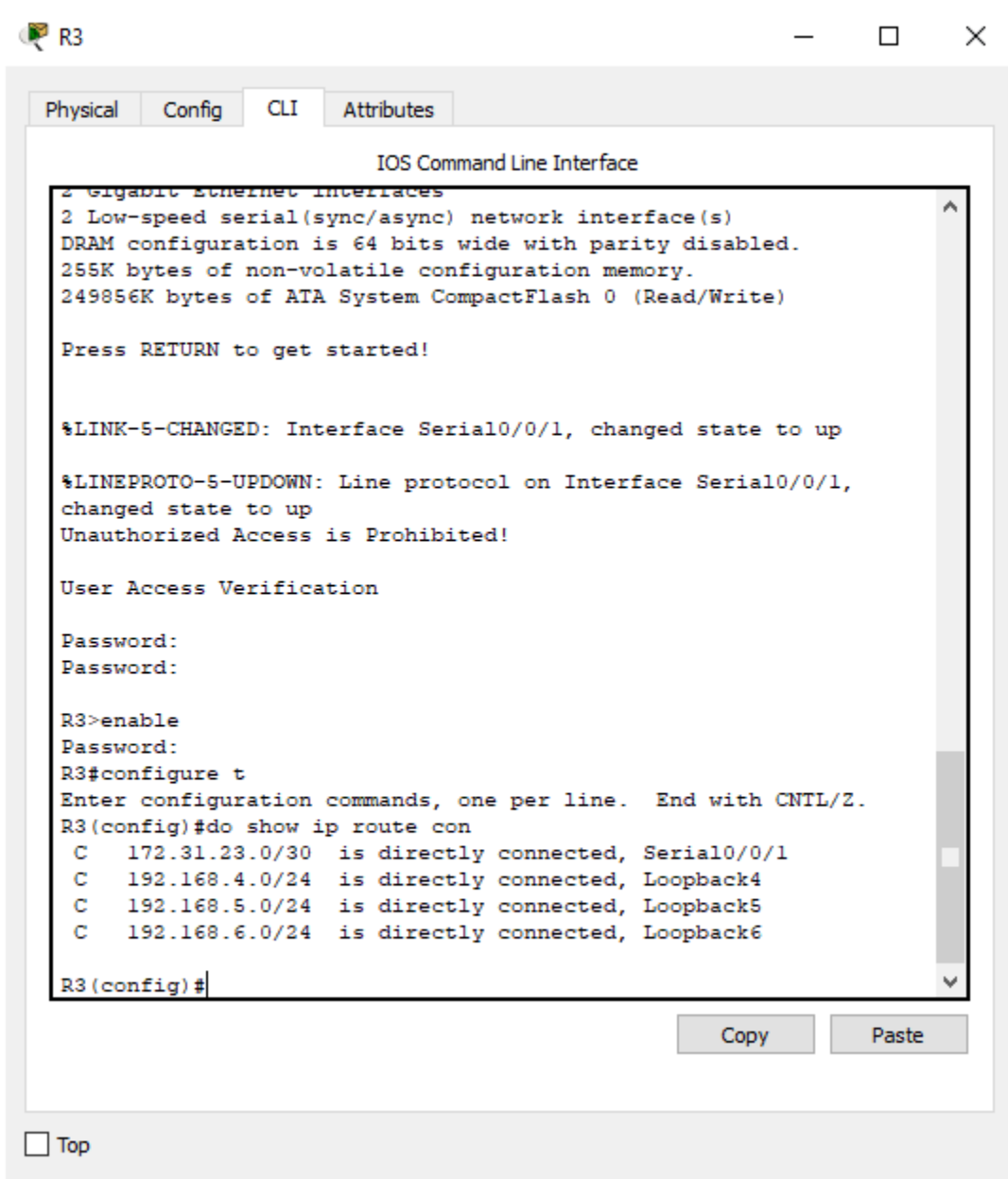
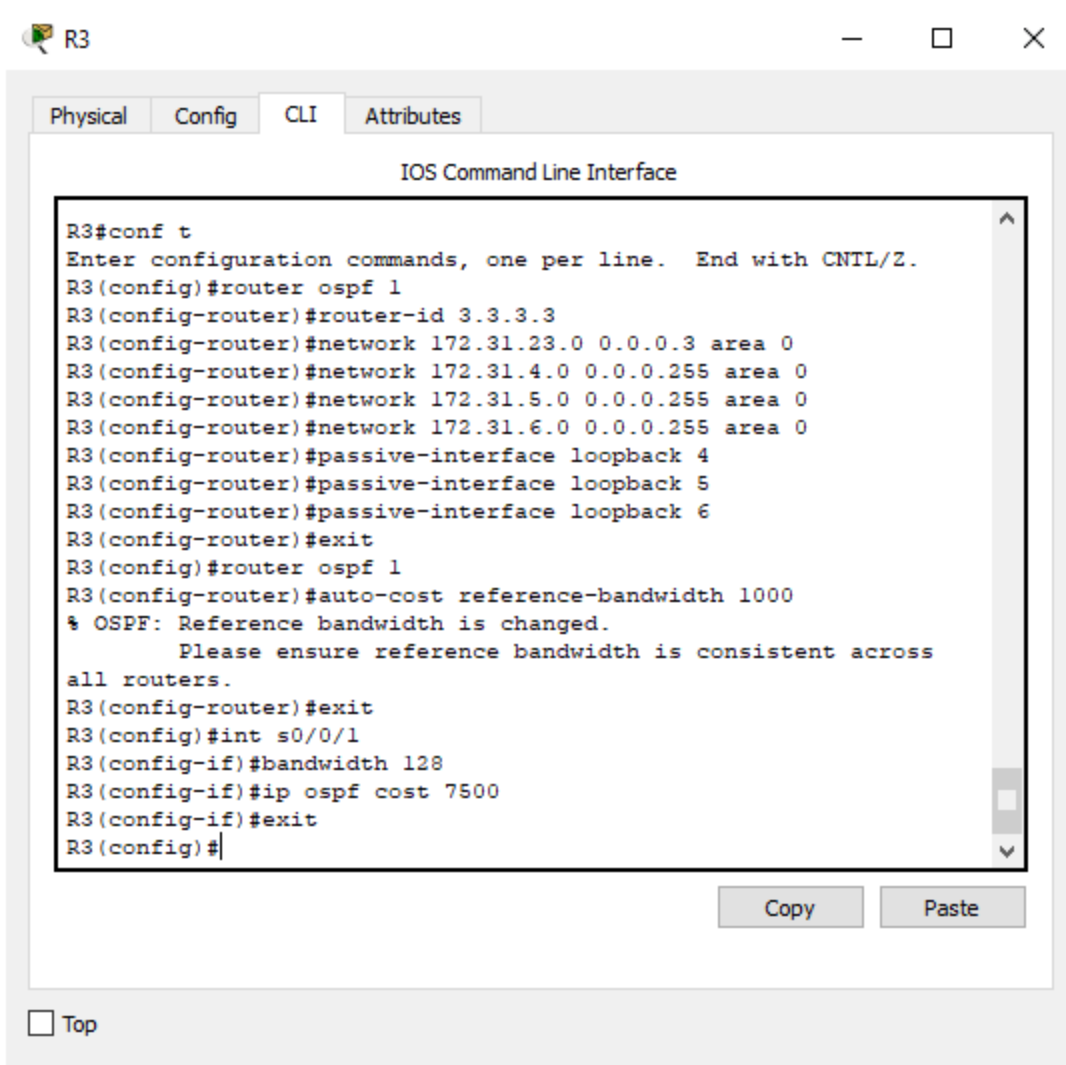


Imagen 18. Verificación de la configuración r3

2.3 Configuración R3 bajo el protocolo de enrutamiento OSPFv2 área 0



```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 172.31.23.0 0.0.0.3 area 0
R3(config-router)#network 172.31.4.0 0.0.0.255 area 0
R3(config-router)#network 172.31.5.0 0.0.0.255 area 0
R3(config-router)#network 172.31.6.0 0.0.0.255 area 0
R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
R3(config-router)#exit
R3(config)#router ospf 1
R3(config-router)#auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across
all routers.
R3(config-router)#exit
R3(config)#int s0/0/1
R3(config-if)#bandwidth 128
R3(config-if)#ip ospf cost 7500
R3(config-if)#exit
R3(config)#
```

Imagen 19. Configuración R3 protocolo OSPFv2

2.4 Verificación de la información OSPF



```
R2#
R2#show ip ospf interface?
interface
R2#show ip ospf interface

GigabitEthernet0/1 is up, line protocol is up
  Internet address is 10.10.10.9/29, Area 0
  Process ID 1, Router ID 2.2.2.2, Network Type BROADCAST, Cost:
  10
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
  Retransmit 5
    No Hellos (Passive interface)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Internet address is 172.31.21.2/30, Area 0
  Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT,
  Cost: 7500
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
  Retransmit 5
    Hello due in 00:00:05
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
  Internet address is 172.31.23.1/30, Area 0
  Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT,
  Cost: 7500
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
  Retransmit 5
    Hello due in 00:00:05
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Suppress hello for 0 neighbor(s)
```

Copy Paste

Top

Imagen 20. Verificación de la información OSPFv2

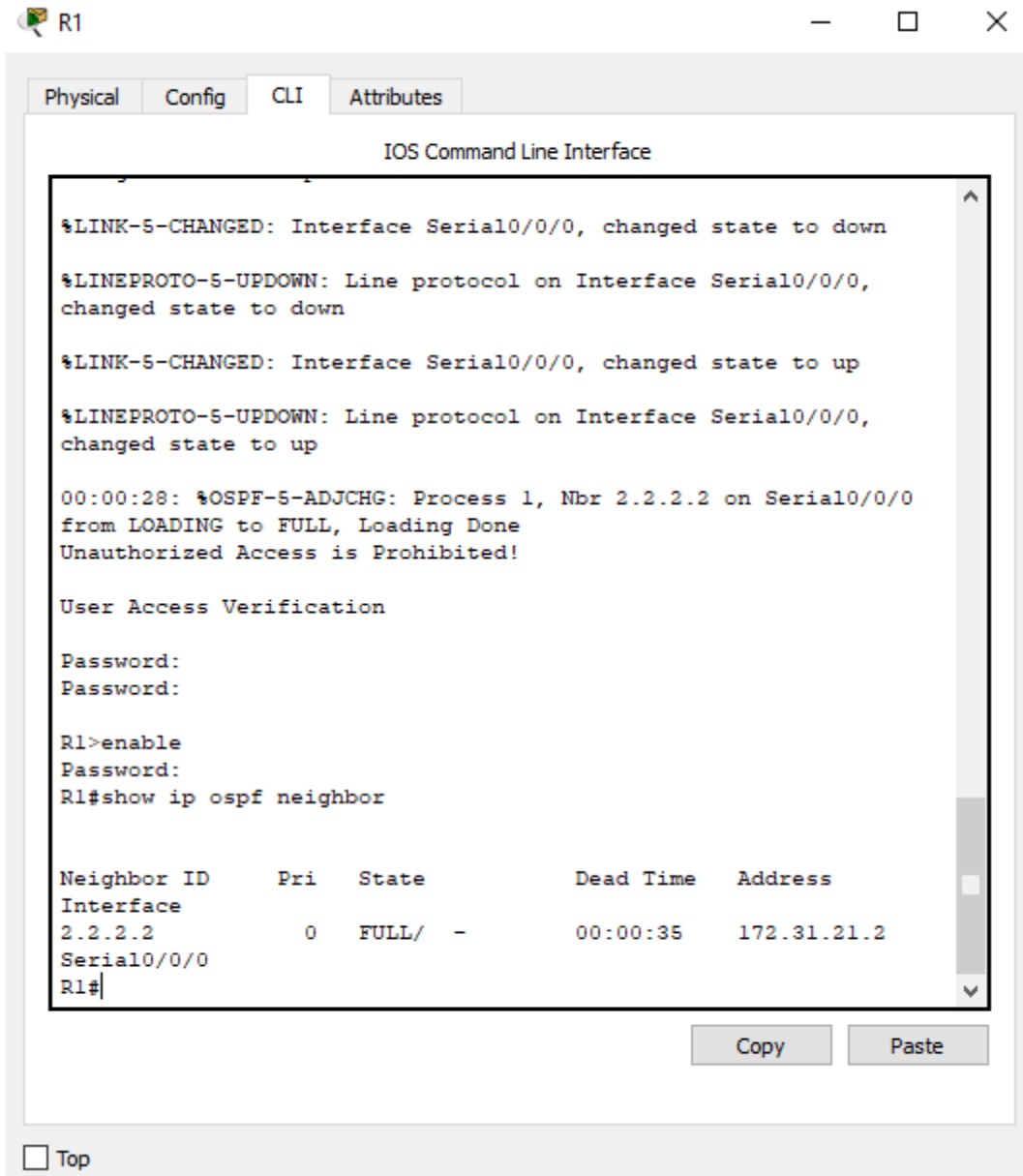


Imagen 21. Verificación de la información OSPFv2 en R1

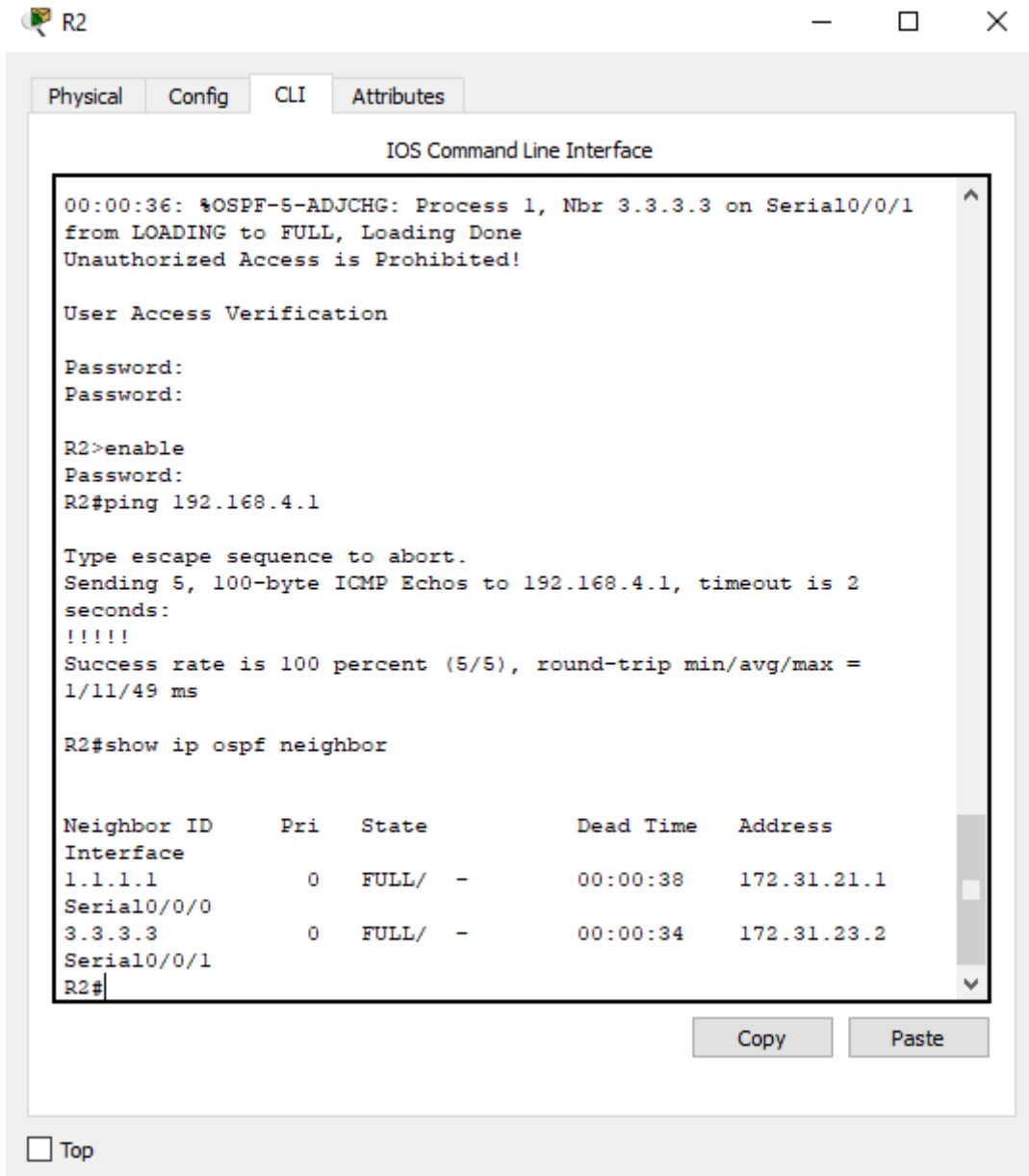


Imagen 22. Verificación de la información OSPFv2 en R2

2.4 Se visualiza lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface

R2

Physical Config CLI Attributes

IOS Command Line Interface

```

R2#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address
Interface
1.1.1.1          0    FULL/ -         00:00:38   172.31.21.1
Serial0/0/0
3.3.3.3          0    FULL/ -         00:00:34   172.31.23.2
Serial0/0/1
R2#show ip ospf interface

GigabitEthernet0/1 is up, line protocol is up
  Internet address is 10.10.10.9/29, Area 0
  Process ID 1, Router ID 2.2.2.2, Network Type BROADCAST, Cost:
  1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 2.2.2.2, Interface address 10.10.10.9
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
  Retransmit 5
  No Hellos (Passive interface)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Internet address is 172.31.21.2/30, Area 0
  Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT,
  Cost: 7500
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
  Retransmit 5
  Hello due in 00:00:09
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 1.1.1.1
  Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
  Internet address is 172.31.23.1/30, Area 0
  Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT,
  Cost: 7500
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
  Retransmit 5
  Hello due in 00:00:02
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 3.3.3.3
  
```

Copy Paste

Top

Imagen 23. Verificación de la información OSPFv2 en R2

2.6 Verificación de protocolos

```
R2#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.10.10.8 0.0.0.7 area 0
    172.31.21.0 0.0.0.3 area 0
    172.31.23.0 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway          Distance      Last Update
    1.1.1.1           110          00:08:24
    2.2.2.2           110          00:08:16
    3.3.3.3           110          00:08:16
  Distance: (default is 110)
```

```
192.168.30.0 [110/7501] via 172.31.21.1, 00:09:40, Serial0/0/0
192.168.40.0 [110/7501] via 172.31.21.1, 00:09:40, Serial0/0/0
192.168.200.0 [110/7501] via 172.31.21.1, 00:09:40, Serial0/0/0
```

2.7 Se visualiza el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.

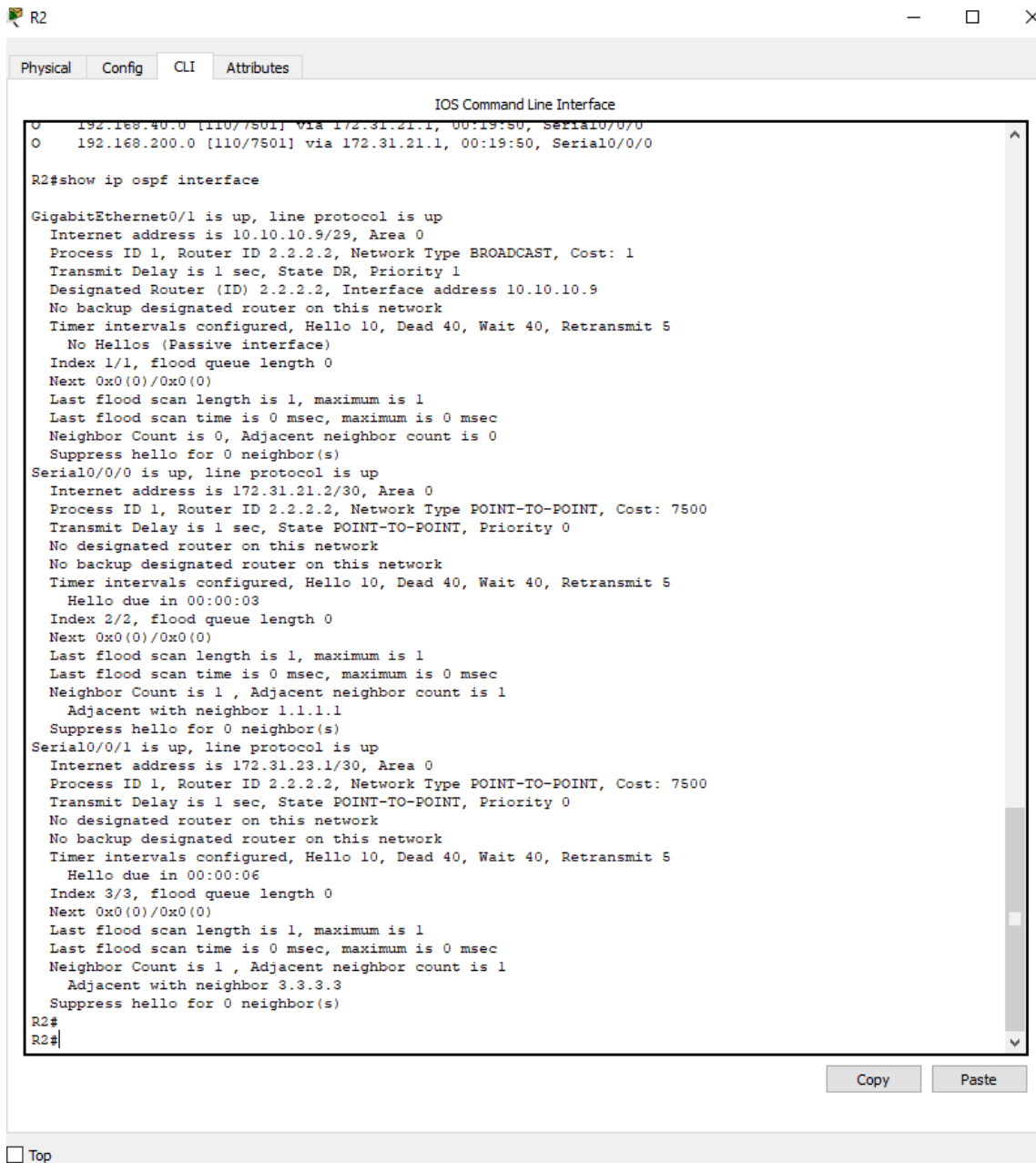


Imagen 24. Visualizacion del OSPF Process ID

Se visualizar tablas de enrutamiento y routers conectados por OSPFv2

```

R2#show run | begin router ospf
router ospf 1
  router-id 2.2.2.2
  log-adjacency-changes
  passive-interface GigabitEthernet0/1
  auto-cost reference-bandwidth 1000
  network 10.10.10.8 0.0.0.7 area 0
  network 172.31.21.0 0.0.0.3 area 0
  network 172.31.23.0 0.0.0.3 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
!
ip flow-export version 9
!
!
!
banner motd ^CUnauthorized Access is Prohibited!^C
!
!
!
line con 0
  password 7 0822455D0A16
  login
!
line aux 0
!
line vty 0 4
  password 7 0822455D0A16
  login
line vty 5 15
  password 7 0822455D0A16
  login
!
!
!
end

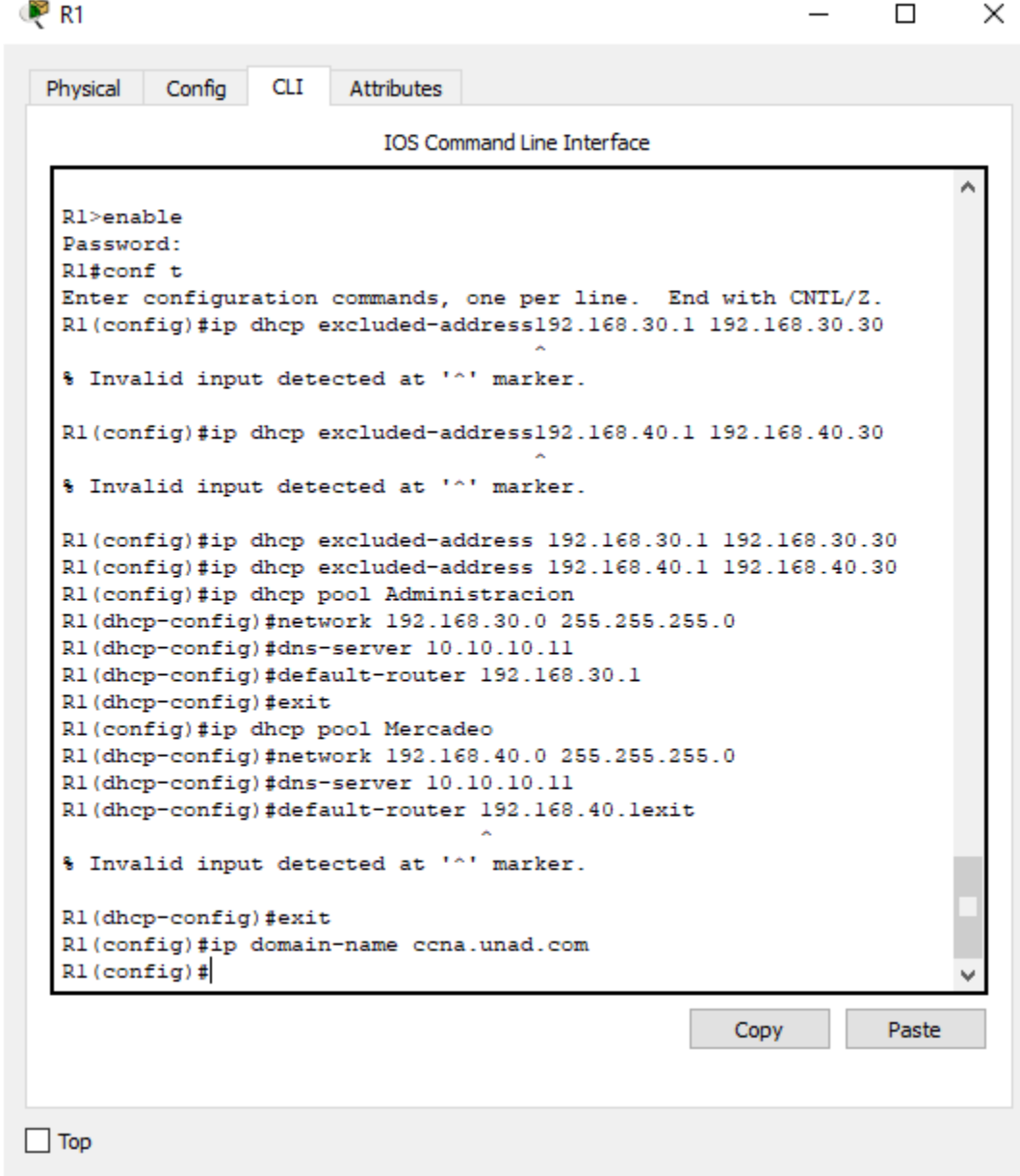
```

3. IMPLEMENTAR DHCP AND NAT PARA IPV4

3.1 Configuración de R1 como servidor DHCP para las VLANs 30 y 40

Configurar DHCP pool para VLAN 30	Name: Administracion DNS-Server : 10.10.10.11 Domain -name: ccna-unad.com Establecer default gateway
Configurar DHCP pool para VLAN 40	Name: Mercadeo DNS-Server : 10.10.10.11 Domain -name: ccna-unad.com Establecer default gateway

3.2 Se configura Configurar R1 como servidor DHCP para las VLANs 30 y 40. Y se Reserva las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.



The screenshot shows the IOS Command Line Interface for R1. The interface has tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the following commands and their outputs:

```
R1>enable
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp excluded-address192.168.30.1 192.168.30.30
^
% Invalid input detected at '^' marker.

R1(config)#ip dhcp excluded-address192.168.40.1 192.168.40.30
^
% Invalid input detected at '^' marker.

R1(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30
R1(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30
R1(config)#ip dhcp pool Administracion
R1(dhcp-config)#network 192.168.30.0 255.255.255.0
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#default-router 192.168.30.1
R1(dhcp-config)#exit
R1(config)#ip dhcp pool Mercadeo
R1(dhcp-config)#network 192.168.40.0 255.255.255.0
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#default-router 192.168.40.1exit
^
% Invalid input detected at '^' marker.

R1(dhcp-config)#exit
R1(config)#ip domain-name ccna.unad.com
R1(config)#
```

At the bottom of the CLI window, there are 'Copy' and 'Paste' buttons. Below the CLI window, there is a 'Top' button.

Imagen 25. Configuración de R1 como servidor DHCP

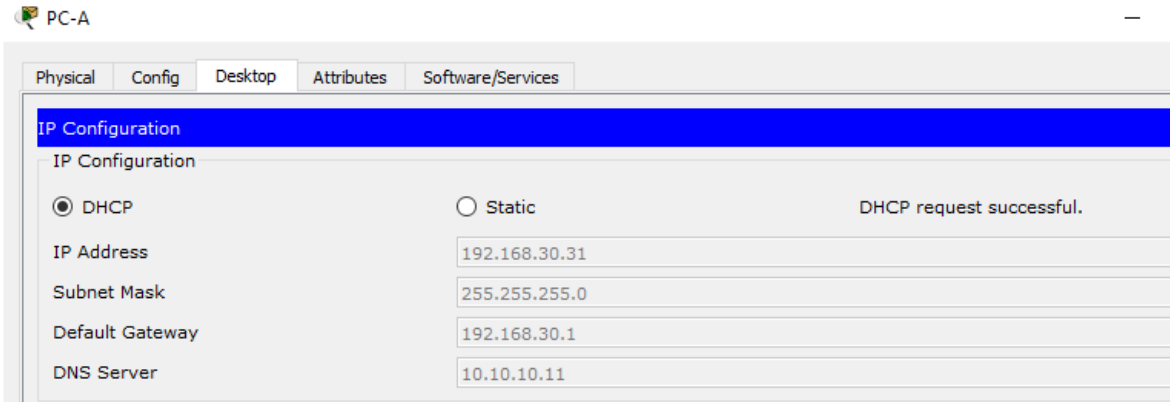


Imagen 26. Configuración de PC-A como DHCP

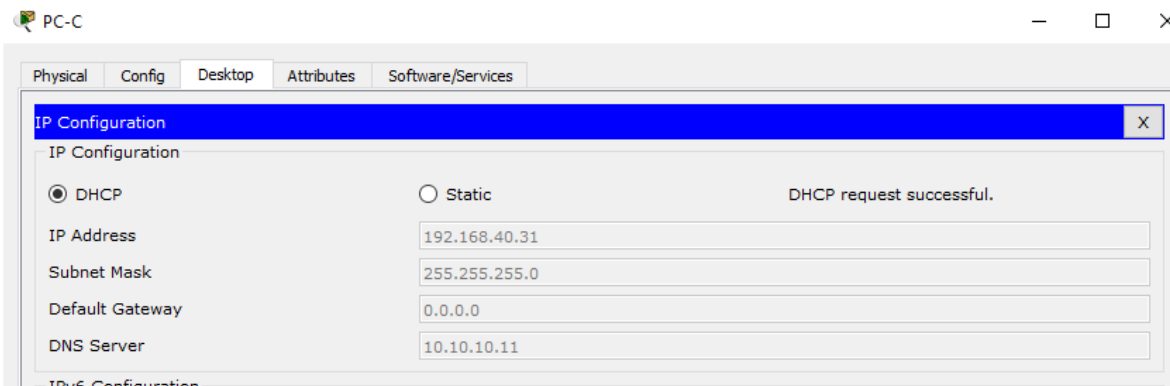


Imagen 27. Configuración de PC-A como DHCP

3.3 Configuración de NAT estático y dinámico en R2

Se configura NAT en R2 para permitir que los host puedan salir a internet

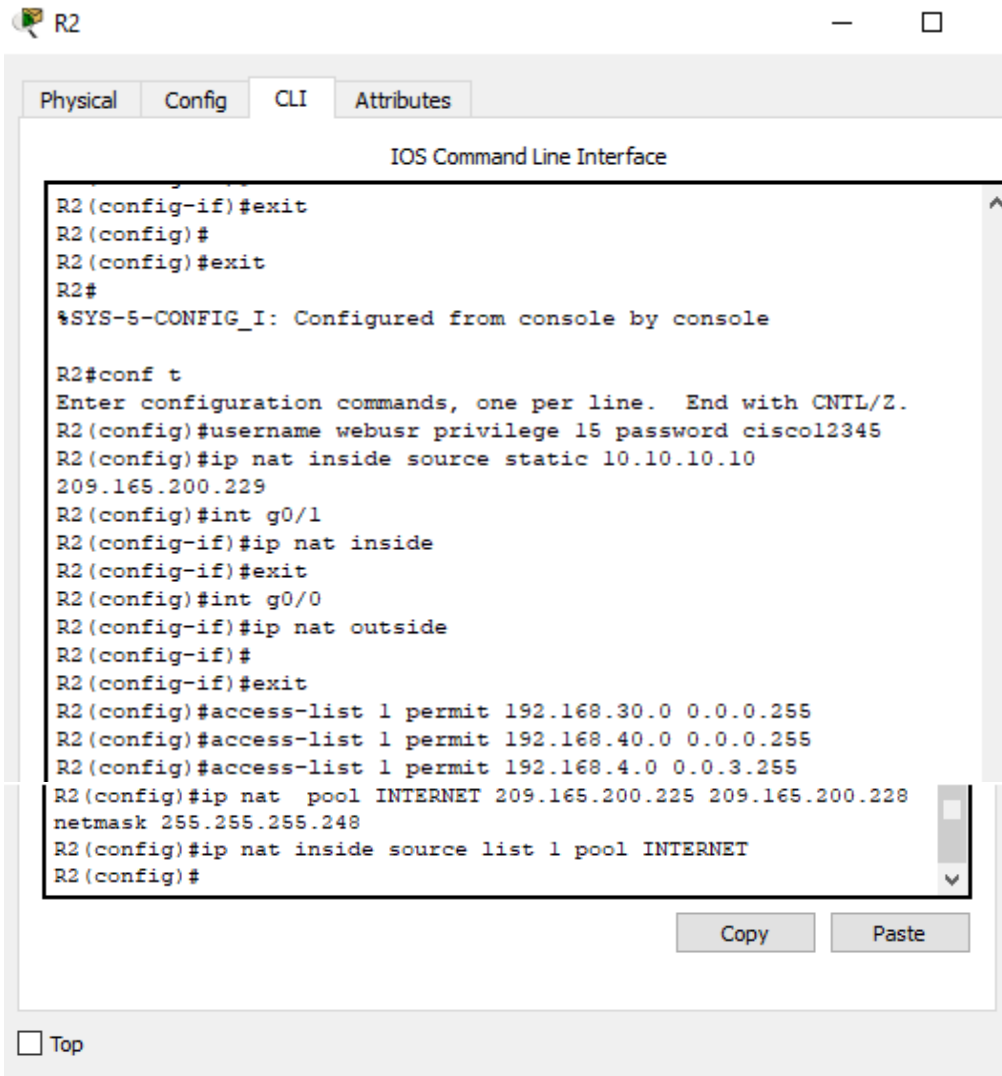


Imagen 28. Configuración NAT estático y dinámico en R2

3.4 Verificación de DHCP y NAT estático



Imagen 29. Verificación NAT estático y dinámico

3.5 Configuración de listas de acceso de tipo estándar para restringir o permitir tráfico

```
R2(config)#ip access-list standard Admin-mgt
R2(config-std-nacl)#permit 172.31.21.1 0.0.0.3
R2(config-std-nacl)#exit
R2(config)#line vty 0 15
R2(config-line)#access-class Admin-mgt in
R2(config-line)#
```



Imagen 30. Configuración de listas

Verificación

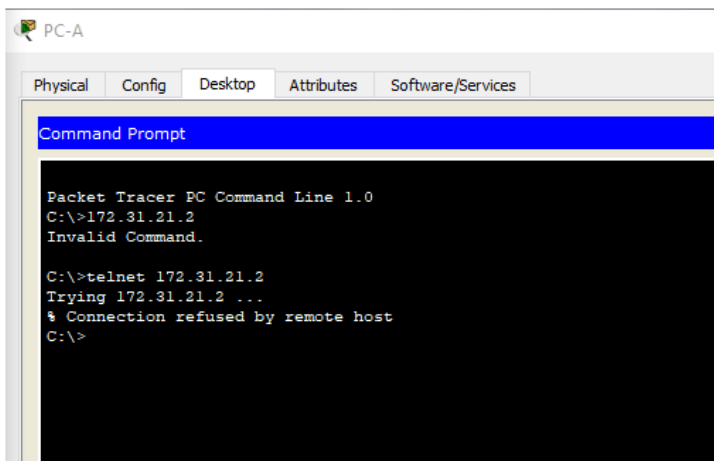


Imagen 31. Verificación de listas

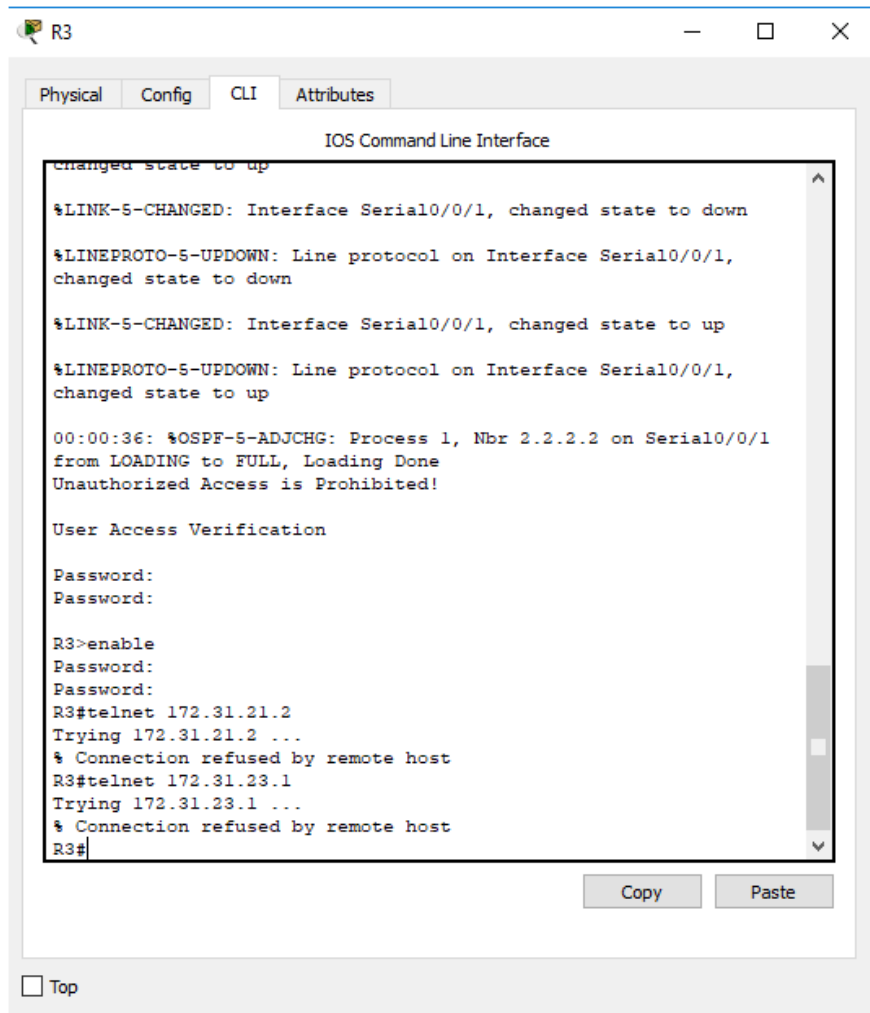


Imagen 32. Verificación de listas

Ping de Internet PC a PCA

```
C:\> ping 192.168.30.31

Pinging 192.168.30.31 with 32 bytes of data:

Reply from 192.168.30.31: bytes=32 time=3ms TTL=126
Reply from 192.168.30.31: bytes=32 time=11ms TTL=126
Reply from 192.168.30.31: bytes=32 time=15ms TTL=126
Reply from 192.168.30.31: bytes=32 time=3ms TTL=126

Ping statistics for 192.168.30.31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 15ms, Average = 8ms
```

Ping PCA a internet PC

```
C:\>ping 209.165.200.230

Pinging 209.165.200.230 with 32 bytes of data:

Reply from 209.165.200.230: bytes=32 time=2ms TTL=126
Reply from 209.165.200.230: bytes=32 time=1ms TTL=126
Reply from 209.165.200.230: bytes=32 time=1ms TTL=126
Reply from 209.165.200.230: bytes=32 time=13ms TTL=126

Ping statistics for 209.165.200.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 13ms, Average = 4ms
```

```
C:\> ping 192.168.30.31

Pinging 192.168.30.31 with 32 bytes of data:

Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.

Ping statistics for 192.168.30.31:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ping de PCA a

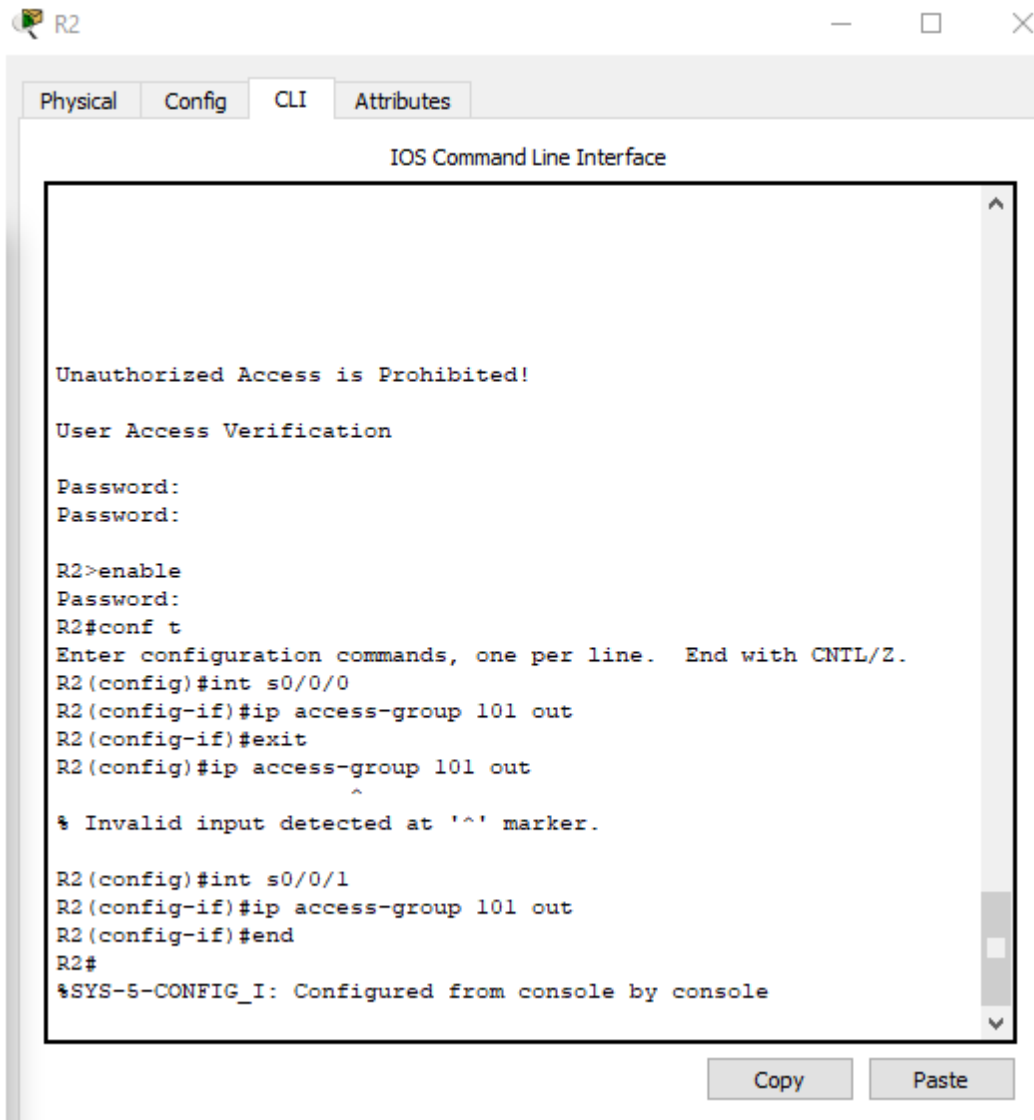
```
C:\>ping 192.168.4.1

Pinging 192.168.4.1 with 32 bytes of data:

Reply from 192.168.4.1: bytes=32 time=4ms TTL=253
Reply from 192.168.4.1: bytes=32 time=17ms TTL=253
Reply from 192.168.4.1: bytes=32 time=11ms TTL=253
Reply from 192.168.4.1: bytes=32 time=14ms TTL=253

Ping statistics for 192.168.4.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 17ms, Average = 11ms
```

3.6 Configuración de listas de acceso de tipo extendido o nombradas a su criterio para restringir o permitir tráfico



The screenshot shows a Cisco IOS Command Line Interface window with tabs for Physical, Config, CLI, and Attributes. The CLI window displays the following text:

```
Unauthorized Access is Prohibited!

User Access Verification

Password:
Password:

R2>enable
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int s0/0/0
R2(config-if)#ip access-group 101 out
R2(config-if)#exit
R2(config)#ip access-group 101 out
^
% Invalid input detected at '^' marker.

R2(config)#int s0/0/1
R2(config-if)#ip access-group 101 out
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

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

Imagen 33. Configuración de listas de tipo extendido

```
C:\> ping 192.168.4.1

Pinging 192.168.4.1 with 32 bytes of data:

Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.

Ping statistics for 192.168.4.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\>ping 192.168.40.31

Pinging 192.168.40.31 with 32 bytes of data:

Request timed out.
Reply from 192.168.40.31: bytes=32 time=11ms TTL=127
Reply from 192.168.40.31: bytes=32 time=12ms TTL=127
Reply from 192.168.40.31: bytes=32 time=10ms TTL=127

Ping statistics for 192.168.40.31:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 12ms, Average = 11ms
```

```
C:\> ping 209.165.200.229

Pinging 209.165.200.229 with 32 bytes of data:

Reply from 209.165.200.229: bytes=32 time<1ms TTL=127
Reply from 209.165.200.229: bytes=32 time<1ms TTL=127
Reply from 209.165.200.229: bytes=32 time=12ms TTL=127
Reply from 209.165.200.229: bytes=32 time<1ms TTL=127

Ping statistics for 209.165.200.229:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 3ms
```

Configuración

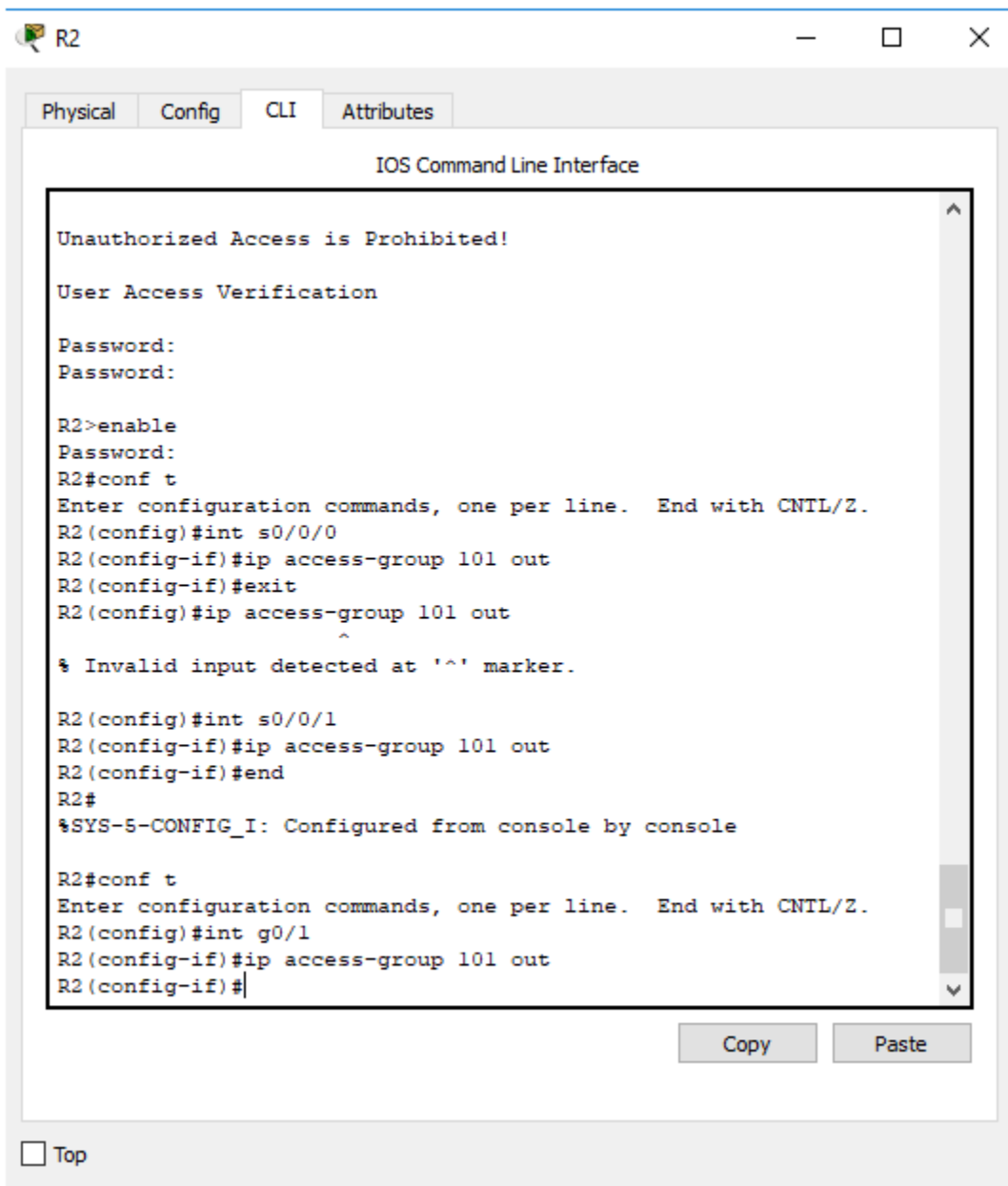


Imagen 34. Configuración de listas R2

Verificación

```
C:\>ping 209.165.200.229

Pinging 209.165.200.229 with 32 bytes of data:

Reply from 209.165.200.229: Destination host unreachable.
Reply from 209.165.200.229: Destination host unreachable.
Reply from 209.165.200.229: Destination host unreachable.
Reply from 209.165.200.229: Destination host unreachable.

Ping statistics for 209.165.200.229:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ping PCA a

```
C:\>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:

Reply from 172.31.21.2: Destination host unreachable.
Reply from 172.31.21.2: Destination host unreachable.
Reply from 172.31.21.2: Destination host unreachable.
Reply from 172.31.21.2: Destination host unreachable.

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ping PCA a

```
C:\>ping 192.168.40.31

Pinging 192.168.40.31 with 32 bytes of data:

Reply from 192.168.40.31: bytes=32 time=1ms TTL=127
Reply from 192.168.40.31: bytes=32 time=13ms TTL=127
Reply from 192.168.40.31: bytes=32 time=13ms TTL=127
Reply from 192.168.40.31: bytes=32 time=13ms TTL=127

Ping statistics for 192.168.40.31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 13ms, Average = 10ms
```

Ping PCA a

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int g0/1
R2(config-if)#ip access-group 101 out
R2(config-if)#exit
R2(config)#int g0/0
R2(config-if)#ip access-group 101 in
R2(config-if)#
```

```
C:\>ping 192.168.4.1

Pinging 192.168.4.1 with 32 bytes of data:

Reply from 172.31.21.2: Destination host unreachable.
Reply from 172.31.21.2: Destination host unreachable.
Reply from 172.31.21.2: Destination host unreachable.
Reply from 172.31.21.2: Destination host unreachable.

Ping statistics for 192.168.4.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

R2

Physical Config CLI Attributes

IOS Command Line Interface

```
!
interface GigabitEthernet0/0
description R2-Internet
ip address 209.165.200.225 255.255.255.248
ip access-group 101 in
ip nat outside
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 10.10.10.9 255.255.255.248
ip access-group 101 out
ip nat inside
duplex auto
speed auto
!
interface Serial0/0/0
description R2-R1
bandwidth 128
ip address 172.31.21.2 255.255.255.252
ip ospf cost 7500
ip access-group 101 out
!
interface Serial0/0/1
description R2-R3
bandwidth 128
ip address 172.31.23.1 255.255.255.252
ip ospf cost 7500
ip access-group 101 out
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
router-id 2.2.2.2
log-adjacency-changes
passive-interface GigabitEthernet0/1
auto-cost reference-bandwidth 1000
network 10.10.10.8 0.0.0.7 area 0
network 172.31.21.0 0.0.0.3 area 0
network 172.31.23.0 0.0.0.3 area 0
!
ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask
255.255.255.248
ip nat inside source list 1 pool INTERNET
ip nat inside source static 10.10.10.10 209.165.200.229
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
!
ip flow-export version 9
!
!
access-list 1 permit 192.168.30.0 0.0.0.255
access-list 1 permit 192.168.40.0 0.0.0.255
access-list 1 permit 192.168.4.0 0.0.3.255
ip access-list standard Admin-mgt
permit 172.31.21.0 0.0.0.3
access-list 101 permit tcp any host 209.165.200.229 eq www
```

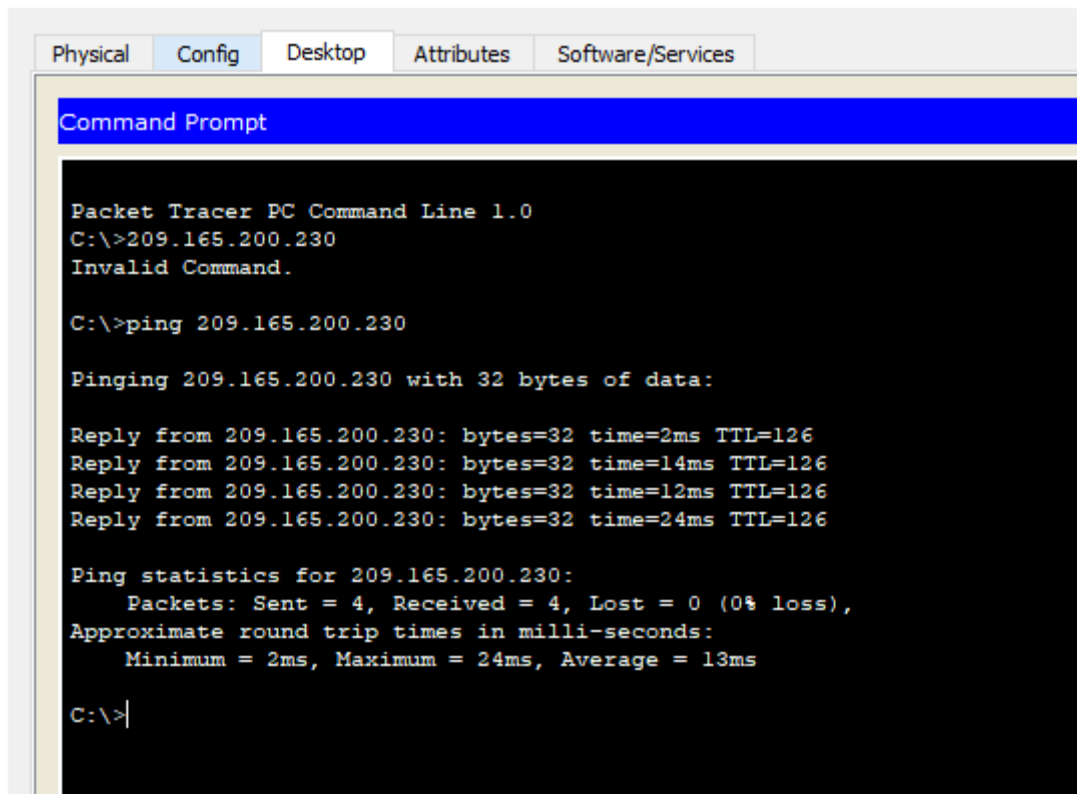
Copy Paste

Top

Imagen 35. Verificación de listas

Ping de PC-C

PC-C



The screenshot shows a Packet Tracer PC Command Line window for PC-C. The window has tabs for Physical, Config, Desktop, Attributes, and Software/Services. The Command Prompt is active, displaying the following text:

```
Packet Tracer PC Command Line 1.0
C:\>209.165.200.230
Invalid Command.

C:\>ping 209.165.200.230

Pinging 209.165.200.230 with 32 bytes of data:

Reply from 209.165.200.230: bytes=32 time=2ms TTL=126
Reply from 209.165.200.230: bytes=32 time=14ms TTL=126
Reply from 209.165.200.230: bytes=32 time=12ms TTL=126
Reply from 209.165.200.230: bytes=32 time=24ms TTL=126

Ping statistics for 209.165.200.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 24ms, Average = 13ms

C:\>
```

Verificación de las listas de acceso estándar y extendido

```
R2#show access-list
Standard IP access list 1
 10 permit 192.168.30.0 0.0.0.255
 20 permit 192.168.40.0 0.0.0.255
 30 permit 192.168.4.0 0.0.3.255
Standard IP access list Admin-mgt
 10 permit 172.31.21.0 0.0.0.3 (4 match(es))
Extended IP access list 101
 10 permit tcp any host 209.165.200.229 eq www
 20 permit icmp any any echo-reply (12 match(es))

R2#clear access-list counters 1
R2#show access-lists
Standard IP access list 1
 10 permit 192.168.30.0 0.0.0.255
 20 permit 192.168.40.0 0.0.0.255
 30 permit 192.168.4.0 0.0.3.255
Standard IP access list Admin-mgt
 10 permit 172.31.21.0 0.0.0.3 (4 match(es))
Extended IP access list 101
 10 permit tcp any host 209.165.200.229 eq www
 20 permit icmp any any echo-reply (12 match(es))
```

Bibliografía

- CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>
- UNAD (2014). Principios de Enrutamiento [OVA]. Recuperado de: https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm
- CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>