

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS
CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

ANDRES MAURICIO GARAY CRUZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ECBTI
INGENIERÍA DE SISTEMAS
NEIVA
2021

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS
CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

ANDRES MAURICIO GARAY CRUZ

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR EL
TÍTULO DE INGENIERO DE SISTEMAS

DIRECTOR:

MSc. MARÍA ALEJANDRA LOPEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ECBTI
INGENIERÍA DE SISTEMAS
NEIVA
2021

NOTA DE ACEPTACIÓN

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Neiva, 26 de noviembre de 2021

TABLA DE CONTENIDO

GLOSARIO	8
RESUMEN.....	9
ABSTRACT.....	10
INTRODUCCIÓN	11
OBJETIVOS.....	12
Objetivo General.....	12
Específicos.....	12
ESCENARIO.....	13
Escenario 1	13
Paso 1: configurar los ajustes básicos.....	14
Configuración S1	18
Paso 2 configurar los equipos.....	21
Escenario 2.....	25
Topología.....	25
Parte 1: Inicializar dispositivos.....	25
Parte 2: Configurar los parámetros básicos de los dispositivos.....	30
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN	54
Parte 4: Configurar el protocolo de routing OSPF.....	69
Parte 5: Implementar DHCP y NAT para IPv4	74
Parte 6: Configurar NTP.....	84
Parte 7: Configurar y verificar las listas de control de acceso (ACL).....	85
CONCLUSIONES	90
BIBLIOGRAFÍA.....	91

LISTA DE FIGURAS

Figura 1. Topología.....	13
Figura 2. Desactivar búsqueda de DNS.....	15
Figura 3. Configuración password.....	16
Figura 4. Configuración de ip R1.....	16
Figura 5. Configuración Dominio R1	17
Figura 6. Configuración de mínimo 10 caracteres R1	17
Figura 7. Configuración SSh R1.....	17
Figura 8. Configuración banner R1	18
Figura 9. Configuración S1	20
Figura 10. Configuración ip S1.....	21
Figura 11. Guardado de configuración.....	21
Figura 12. Información ip	22
Figura 13. Configuración del PC-A.....	22
Figura 14. Información ip	23
Figura 15. Configuración PC-B	24
Figura 16. Topología tomada de prueba de habilidades CCNA	25
Figura 17. Inicializar y cargar routers.....	27
Figura 18. Inicializar y cargar switches	28
Figura 19. Verificando que la base de datos de VLAN no esté en la memoria.....	29
Figura 20. Configuración del servidor	30
Figura 21. Configuración de R1	33
Figura 22. Configuración de R1 ruta ip	34
Figura 23. Configuración de R1 rutas predeterminadas.....	35
Figura 24. Configuración de R2	39
Figura 25. Configuración de R2 rutas predeterminadas.....	40
Figura 26. Configuración de R3	43
Figura 27. Configuración de R3 interfaces look back.....	44
Figura 28. Configuración de R3 rutas predeterminadas.....	45
Figura 29. Configuración de S1	47

Figura 30. Configuración de S3	49
Figura 31. Verificación de la conexión de la red entre R1 a R2	51
Figura 32. Verificación de la conexión de la red entre R2 a R3	52
Figura 33. Verificación de la conexión de la red entre PC internet a Gateway.....	53
Figura 34. Configuración de seguridad S1	57
Figura 35. Configuración de seguridad S3.....	61
Figura 36. Configuración de seguridad de VLAN R1	63
Figura 37. Verificación de la conectividad de la red desde S1 a R1 VLAN 99	65
Figura 38. Verificación de la conectividad de la red desde S3 a R1 VLAN 99	66
Figura 39. Verificación de la conectividad de la red desde S3 a R1 VLAN 21	67
Figura 40. Verificación de la conectividad de la red desde S1 a R1 VLAN 21	68
Figura 41. Configuración OSPF R1	70
Figura 42. Configuración OSPF R2	72
Figura 43. Configuración OSPFv3 en el R2.....	73
Figura 44. Configuración DHCP en R1	76
Figura 45. Configuración DHCP en R2.....	79
Figura 46. Verificación protocolo DHCP en Pc A.....	81
Figura 47. Verificación protocolo DHCP en Pc C.....	82
Figura 48. Verificación protocolo DHCP en Pc A a Pc C	83
Figura 49. Verificación protocolo DHCP en un buscador.....	83
Figura 50. Configuración ntp R2	84
Figura 51. Configuración ntp R1	85
Figura 52. Configuración ntp R2	89

LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento	13
Tabla 2. Datos de la Subredes.....	14
Tabla 3. Direccionamiento de los dispositivos.....	14
Tabla 4. Configuración PC-A	21
Tabla 5. Configuración PC-B	23
Tabla 6. Inicializar y volver a cargar los routers y los switches.	26
Tabla 7. Configurar la computadora de Internet.....	30
Tabla 8. Configuración R1	31
Tabla 9. Configuración R2	36
Tabla 10. Configuración R3	41
Tabla 11. Configuración S1.....	46
Tabla 12. Configuración S3.....	48
Tabla 13. Verificar la conectividad de la red.....	50
Tabla 14. Configurar la seguridad S1.....	54
Tabla 15. Configurar la seguridad S3.....	58
Tabla 16. Configurar la seguridad VLAN R1	62
Tabla 17. Verificar la conectividad de la red.....	64
Tabla 18. Configurar OSPF en el R1	69
Tabla 19. Configurar OSPF en el R2	71
Tabla 20. Configurar OSPFv3 en el R2.....	72
Tabla 21. Verificar la información de OSPF	74
Tabla 22. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23	74
Tabla 23. Configurar la NAT estática y dinámica en el R2	77
Tabla 24. Verificar el protocolo DHCP y la NAT estática.....	80
Tabla 25. Configurar NTP	84
Tabla 26. Restringir el acceso a las líneas VTY en el R2.....	85
Tabla 27. Introducir el comando de CLI adecuado.....	86

GLOSARIO

Cable: es un cordón que se compone de diferentes conductores, los cuales están aislados entre sí. ... Se denomina cable de red o cable de conexión al elemento físico que permite conectar entre sí a diferentes computadoras (ordenadores) y a otros aparatos informáticos.

Ethernet: es la tecnología LAN predominante en el mundo. Ethernet funciona en la capa de enlace de datos y en la capa física. Los estándares del protocolo Ethernet definen muchos aspectos de la comunicación en red, incluido el formato, el tamaño, la temporización y la codificación de las tramas.

Internet: es un conjunto global de redes interconectadas o se refiere al sistema global de redes de computadoras interconectadas, o World Wide Web.

PACKET TRACER: Es un programa de simulación de topologías de redes, el cual permite verificar correcta configuración de un diseño de red, simular los protocolos de enrutamiento. EL programa es exclusivo de CISCO.

Router: es un dispositivo que ofrece una conexión Wi-Fi, que normalmente está conectado a un módem y que envía información de Internet a tus dispositivos personales, como ordenadores, teléfonos o tablets. Los dispositivos que están conectados a Internet en tu casa conforman tu red de área local (LAN).

Switch: es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3).

VLAN: (Red de Área Local Virtual). Es el método que se usa para la creación de redes lógicas independientes en una misma red.

RESUMEN

En este trabajo se desarrolla una problemática real con dos escenarios en los cuales se aplican diferentes conceptos aprendidos durante en desarrollo del curso CCNA, para la puesta en marcha del diseño y la implementación se requiere de conocimientos básicos y el uso de herramientas de simulación del software Cisco Packet Tracer en el desarrollo de redes (LAN / WAN) donde se realiza un estudio de comportamiento de diferentes protocolos y métricas de enrutamiento para los dos escenarios propuestos, arreglado por diferentes dispositivos para alcanzar una conexión positiva y funcional.

Durante el diplomado de profundización CCNA, se desarrollan habilidades que permiten desarrollar esta actividad de prueba de habilidades practicas para solucionar los diferentes problemas de Networking presentados en los escenarios 1 y 2, donde se muestra la configuración de cada uno de los puntos exigidos gracias a los diferentes espacios académicos como laboratorios, acompañamiento de cipas, y evaluaciones del componente practico obteniendo un resultado positivo, donde se logra dar solución.

En cada escenario se presentará la topología, se realiza la configuración básica en los routers, switches, servidores y los hosts finales. Además, tiene temas de solución como desactivar los DNS de un router, cambio de nombre de los dispositivos, Subneteo de la red, creación de usuario local, creación de contraseñas, encriptación de estas entre otros.

Posteriormente, se soportará el uso de cada comando en los dispositivos de la red, evidenciándolo con su respectiva imagen, también se mostrará la red de Subneteo a implementar en los diferentes dispositivos sustentando el proceso realizado obteniendo con un resultado favorable.

Palabras Clave: CISCO, CCNA, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

In this work, a real problem is developed with two scenarios in which different concepts learned during the development of the CCNA course are applied, for the start-up of the design and implementation, basic knowledge and the use of software simulation tools are required. Cisco Packet Tracer in the development of networks (LAN / WAN) where a behavior study of different protocols and routing metrics is carried out for the two proposed scenarios, arranged by different devices to achieve a positive and functional connection.

During the CCNA deepening diploma, skills are developed that allow to develop this practical skills test activity to solve the different Networking problems submitted in scenarios 1 and 2, where the configuration of each of the required points is shown thanks to the different academic spaces such as laboratories, accompaniment of cipas, and evaluations of the practical component obtaining a positive result, where a solution is achieved.

In each scenario, the topology will be presented, the basic configuration is performed on the routers, switches, servers and the final hosts. In addition, it has solution issues such as deactivating the DNS of a router, renaming the devices, subnetting the network, creating a local user, creating passwords, encryption of these among others.

Subsequently, the use of each command in the network devices will be supported, evidencing it with its respective image, the Subnetting network to be implemented in the different devices is also shown, supporting the process carried out obtaining a favorable result.

Keywords: CISCO, CCNA, Routing, Swicthing, Networking, Electronics.

INTRODUCCIÓN

Como parte de las actividades finales de evaluación final, este trabajo presenta la documentación del desarrollo de forma práctica y configuración de cada uno de los dispositivos de la topología para cada escenario e información del paso a paso evidenciado con imágenes y programación de los dispositivos, se realizará pruebas de conectividad mediante el comando *ping*, *show ip rout*, *show running-config* con el propósito de demostrar el conocimiento adquirido a lo largo del diplomado de profundización cisco (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN).

Su intención es poner en practica lo aprendido por medio del software Cisco Packet Tracer, mediante el desarrollo de las problemáticas planteadas en los escenarios los cuales tienen diferentes tipos de topología según las necesidades de la red, la información que viaja por de las redes debe ser soportada, usando técnicas de configuración, protocolos de comunicaciones y hardware especializado, poniendo a prueba los conocimientos adquiridos para dar soluciones a futuros problemas en nuestro ámbito laboral como ingeniero de sistemas.

Esta actividad corresponde a la evaluación final del Diplomado de Profundización realizado como opción de grado.

OBJETIVOS

OBJETIVO GENERAL

Determinar la solución para cada uno de actividades del diplomado Evaluación-prueba de habilidades practicas CCNA como trabajo final, mediante la implementación y uso de los conocimientos adquiridos en los módulos para los escenarios con diferentes topologías.

OBJETIVOS ESPECÍFICOS

- Aplicar los conocimientos adquiridos en el desarrollo teórico practico del curso de profundización de ccna.
- Analizar la arquitectura propuesta con el fin de implementar su simulación por medio del software Packet Tracer 8.2.
- Registrar cada uno de los procedimientos realizados para la configuración de los dispositivos.
- Realizar la verificación de la conectividad ende cada uno de ellos.

ESCENARIO

Escenario 1

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos, diseñar el esquema de direccionamiento IPv4 para las LAN propuestas. El router y el switch también deben administrarse de forma segura.

Escenario 1

Figura 1. Topología.

Topología



Fuente: Prueba de habilidades CCNA

Tabla 1. Tabla de direccionamiento

Item	Requerimiento
Dirección de Red	192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula.
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	Primera dirección de host de la subred LAN1
R1 G0/0/0	Primera dirección de host de la subred LAN2
S1 SVI	Segunda dirección de host de la subred LAN1
PC-A	Última dirección de host de la subred LAN1
PC-B	Última dirección de host de la subred LAN2

Tabla 2. Datos de la Subredes

Descripción de la subred	Cantidad de host	Direccionamiento de red	Primera dirección utilizable	Ultima dirección utilizable	Dirección de broacast
LAN 1	100	192.168.57.0/25	192.168.57.1	192.168.57.254	192.168.57.255
LAN 2	50	192.168.57.128/26	192.168.57.129	192.168.57.190	192.168.57.191

Se realiza el Subneteo de la red con la dirección ip 192.168.57.0 como resultado salen 2 subredes.

Tabla 3. Direccionamiento de los dispositivos

dispositivo	Interfaz	Dirección	Mascara	Gateway
R 1	G0/0/0/1	192.168.57.1	255.255.255.128	
	G0/0/0/0	192.168.57.129	255.255.255.192	
S1	VLAN1	192.168.57.2	255.255.255.128	192.168.57.1
PC-A	NIC	192.168.57.126	255.255.255.128	192.168.57.1
PC-B	NIC	192.168.57.190	255.255.255.192	192.168.57.129

Se asigna direcciones a cada uno de los dispositivos de la red.

Paso 1: configurar los ajustes básicos

- Desactivar la búsqueda de DNS
- Nombre del router R1
- Nombre de dominio
- Contraseña cifrada para el modo EXEC privilegiado
- Contraseña de acceso a la consola
- Establecer la longitud mínima para las contraseñas
- Crear un usuario administrativo en la base de datos local
- Configurar el inicio de sesión en las líneas VTY para que use la base de datos local
- Configurar VTY solo aceptando el SSH
- Cifrar las contraseñas de texto no cifrado
- Configure un MOTD banner
- Configurar interfaz G0/0/0
- Configurar interfaz G0/0/1
- Generar una clave de cifrado RSA

Router>enable

configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

```

no ip domain-lookup
hostname R1
#interface gigabitEthernet 0/0/1
ip address 192.168.57.1 255.255.255.128
no shut
interface gigabitEthernet 0/0/0
# ip address 192.168.57.129 255.255.255.192
no shut
ip domain-name ccna-lab.com
enable password ciscoenpass
line console 0
Password ciscoconpass
login
security password min-length 10
crypto key generate rsa
ip ssh version 2
line vty 0 15
transport input ssh
login local
username admin secret admin1pass
enable secret admin1pass
banner motd %Se prohíbe el acceso no autorizado.%
service password-encryption
do copy running-config startup-config

```

Figura 2. Desactivar búsqueda de DNS.

```

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no ip domain-lookup
Router(config)#hostname R1
R1(config)#interface gigabitEthernet 0/0/1
R1(config-if)#ip address 192.168.57.1 255.255.255.128
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

R1(config-if)#interface gigabitEthernet 0/0/0
R1(config-if)#ip address 192.168.57.129 255.255.255.192
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

R1(config-if)#ip domain-name ccna-lab.com

```

Ctrl+F6 to exit CLI focus

Fuente: Elaboración propia.

Mediante el código no ip domain-lookup se desactiva la búsqueda de los DNS

Figura 3. Configuración password.



```
Physical  Config  CLI  Attributes
IOS Command Line Interface

R1(config)#login local
^
% Invalid input detected at '^' marker.

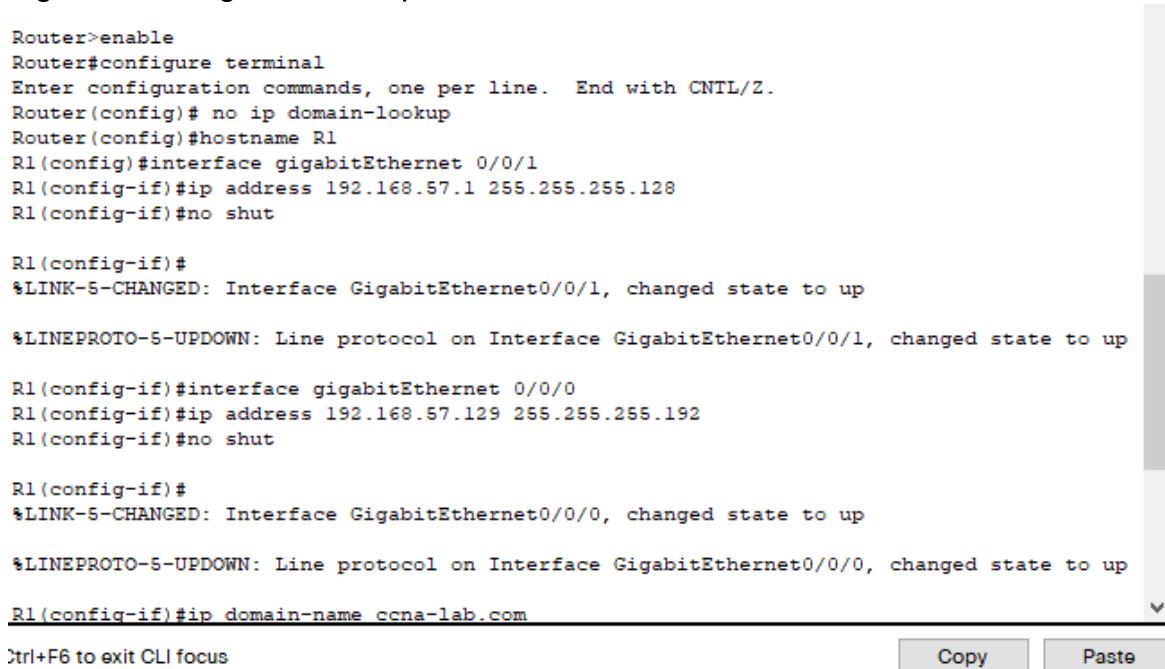
R1(config)#line vty 0 15
R1(config-line)#transport input shh
^
% Invalid input detected at '^' marker.

R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#username admin secret adminipass
R1(config)#enable secret adminipass
R1(config)#enable secret adminipass
R1(config)#banner motd %Se prohíbe el acceso no autorizado%
R1(config)#servicio password-encryption
```

Fuente: Elaboración propia

Mediante el comando line vty 0, password ciscoconpas, line console 0, login

Figura 4. Configuración de ip R1



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no ip domain-lookup
Router(config)#hostname R1
R1(config)#interface gigabitEthernet 0/0/1
R1(config-if)#ip address 192.168.57.1 255.255.255.128
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

R1(config-if)#interface gigabitEthernet 0/0/0
R1(config-if)#ip address 192.168.57.129 255.255.255.192
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

R1(config-if)#ip domain-name ccna-lab.com
```

Ctrl+F6 to exit CLI focus

Copy Paste

Fuente: Elaboración propia.

Mediante el comando de interface gigabitEthernet 0/0/0 y interface gigabitEthernet 0/0/1, ip address 192.168.57.1 255.255.255.128 y ip address 192.168.57.129 255.255.255.192 y no shut se activan las interfases.

Figura 5. Configuración Dominio R1.

```
R1(config)#ip domain-name ccna-lab.com
```

Fuente: Imagen de autoría propia

Se utiliza el comando ip domain-name ccna-lab.com

Figura 6. Configuración de mínimo 10 caracteres R1.

```
R1(config-line)#login
R1(config-line)#security password min-length 10
R1(config)#crypto key generate rsa
```

Fuente: Elaboración propia

Se utiliza el comando security password min-length 10

Figura 7. Configuración SSh R1.

```
R1(config-line)#security password min-length 10
R1(config)#crypto key generate rsa
The name for the keys will be: R1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

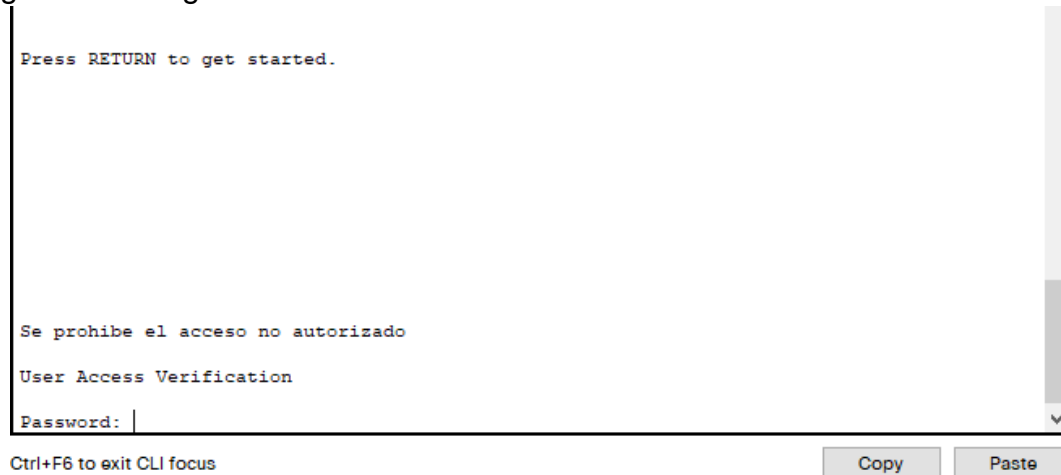
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#ip ssh version 2
*Mar 1 8:2:37.214: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#login local
^
```

Fuente: Elaboración propia

Se utiliza crypto key generate rsa

Figura 8. Configuración banner R1



Fuente: Elaboración propia

Configuración S1

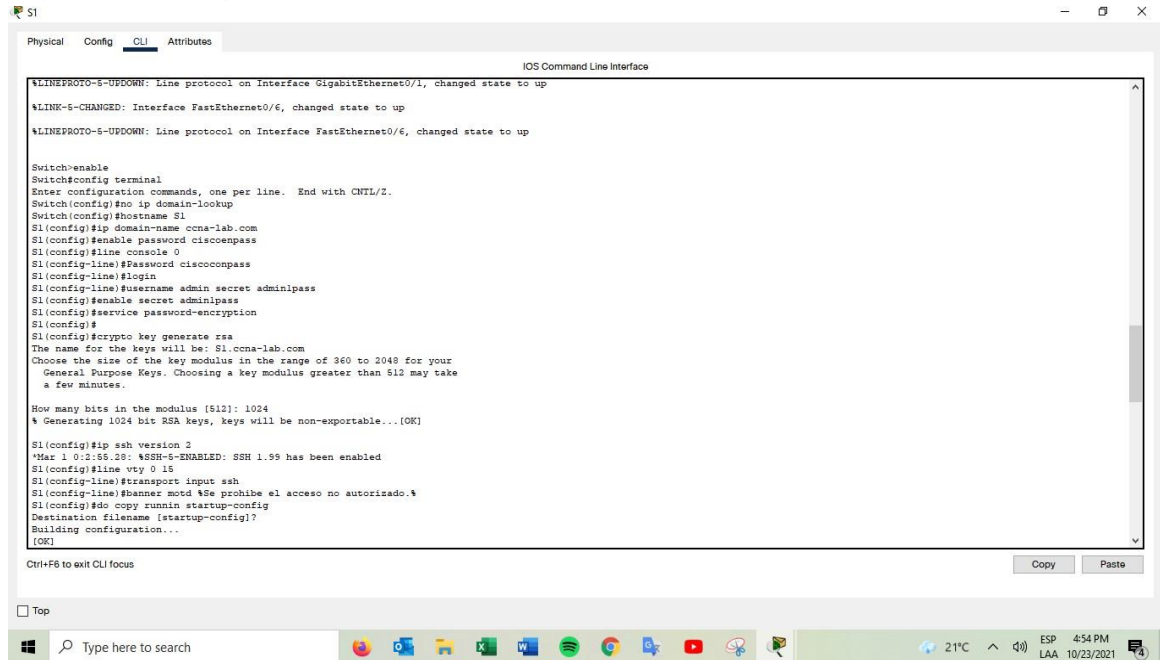
- Desactivar la búsqueda DNS
- Nombre del switch
- Nombre de dominio
- Contraseña cifrada para el modo EXEC privilegiado
- Contraseña de acceso a la consola
- Crear un usuario administrativo en la base de datos local
- Configurar el inicio de sesión en las líneas VTY para que use la base de datos local
- Configurar las líneas VTY para que acepten únicamente las conexiones SSH
- Cifrar las contraseñas de texto no cifrado
- Configurar un MOTD banner
- Generar una clave de cifrado RSA
- Configurar la interfaz de administración (SVI)
- Configuración del Gateway predeterminado

S1

```
enable
config terminal
no ip domain-lookup
hostname S1
ip domain-name ccna-lab.com
enable password ciscoenpass
line console 0
Password ciscoconpass
login
username admin secret admin1pass
enable secret admin1pass
service password-encryption

crypto key generate rsa
ip ssh version 2
line vty 0 15
transport input ssh
banner motd %Se prohíbe el acceso no autorizado.%
exit
interface VLAN1
address 192.168.57.2 255.255.255.128
no shutdown
exit
ip default-gateway 192.168.57.1
copy running-config startup-config
```

Figura 9. Configuración S1.



```
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

Switch#enable
Switch#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#ip domain-name ccna-lab.com
S1(config)#enable password ciscoenpass
S1(config)#line console 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#username admin secret admin1pass
S1(config)#enable secret admin1pass
S1(config)#service password-encryption
S1(config)#
S1(config)#crypto key generate rsa
The name for the keys will be: S1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#ip ssh version 2
*Mar 1 0:05:55.18: SSH-2-ENABLED: SSH 1.99 has been enabled
S1(config)#line vty 0 15
S1(config-line)#transport input ssh
S1(config-line)#banner motd %Se prohíbe el acceso no autorizado.%
S1(config)#do copy running startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

Ctrl+F8 to exit CLI focus
```

Fuente: Elaboración propia

Se utilizaron los siguientes comandos

- enable
- config terminal
- no ip domain-lookup
- hostname S1
- ip domain-name ccna-lab.com
- enable password ciscoenpass
- line console 0
- Password ciscoconpass
- login
- username admin secret admin1pass
- enable secret admin1pass
- service password-encryption
- crypto key generate rsa
- ip ssh version 2
- line vty 0 15

Figura 10. Configuración ip S1.

```
S1(config-if)#ip default 192.168.57.1
S1(config)#interface VLAN1
S1(config-if)#ip address 192.168.57.2 255.255.255.128
S1(config-if)#no shutdown
```

Fuente: Elaboración propia

Se utiliza el comando ip address 192.168.57.2 255.255.255.128

Figura 11. Guardado de configuración.

```
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

trl+F6 to exit CLI focus Copy Paste

Fuente: Elaboración propia

Se utiliza el comando copy running-config startup-config

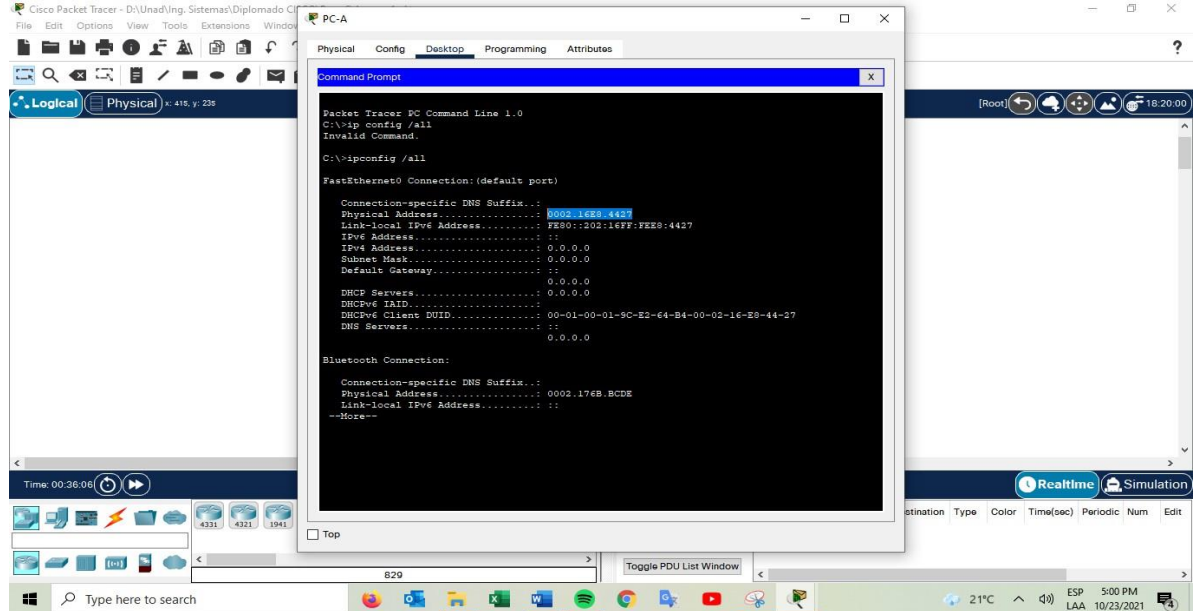
Paso 2 configurar los equipos

Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all**.

Tabla 4. Configuración PC-A

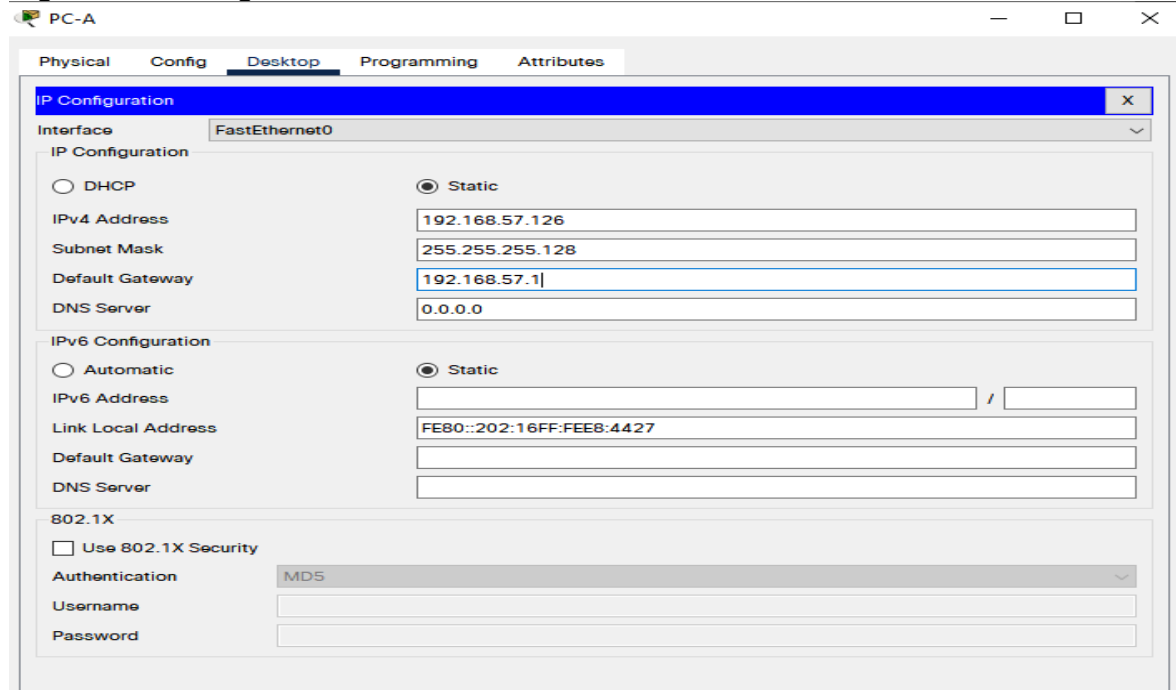
PC-A Network Configuration	
Descripción	
Dirección física	0002.16E8.4427
Dirección IP	192.168.57.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.57.1

Figura 12. Información ip.



Fuente: Elaboración propia

Figura 13. Configuración del PC-A.

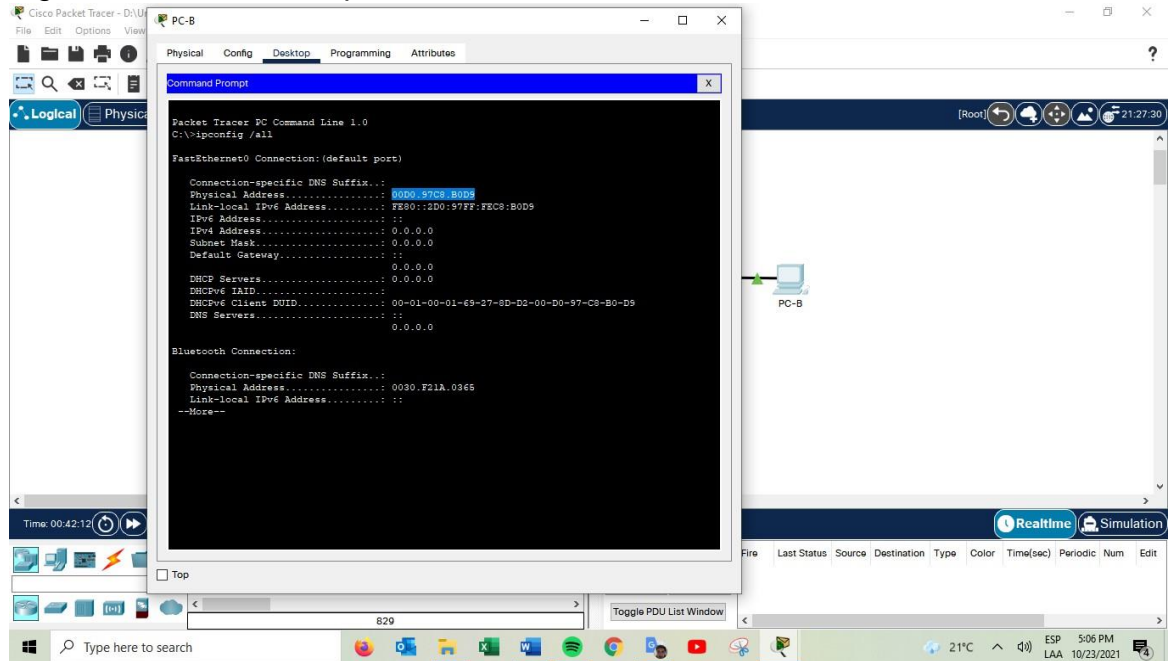


Fuente: Elaboración propia

Tabla 5. Configuración PC-B

PC-B Network Configuration	
Descripción	
Dirección física	00D0.97C8.B0D9
Dirección IP	192.168.57.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.57.1

Figura 14. Información ip.



Fuente: Elaboración propia

Figura 15. Configuración PC-B.

The image shows a configuration window for PC-B with the following details:

- Window title: PC-B
- Navigation tabs: Physical, Config, Desktop (selected), Programming, Attributes
- Section: IP Configuration
- Interface: FastEthernet0
- IP Configuration options:
 - DHCP
 - Static
- Static IP Configuration fields:
 - IPv4 Address: 192.168.57.190
 - Subnet Mask: 255.255.255.192
 - Default Gateway: 192.168.57.1
 - DNS Server: 0.0.0.0
- IPv6 Configuration options:
 - Automatic
 - Static
- Static IPv6 Configuration fields:
 - IPv6 Address: [Empty] / [Empty]
 - Link Local Address: FE80::2D0:97FF:FEC8:B0D9
 - Default Gateway: [Empty]
 - DNS Server: [Empty]
- 802.1X Configuration:
 - Use 802.1X Security
 - Authentication: MD5
 - Username: [Empty]
 - Password: [Empty]
- Bottom button: Top

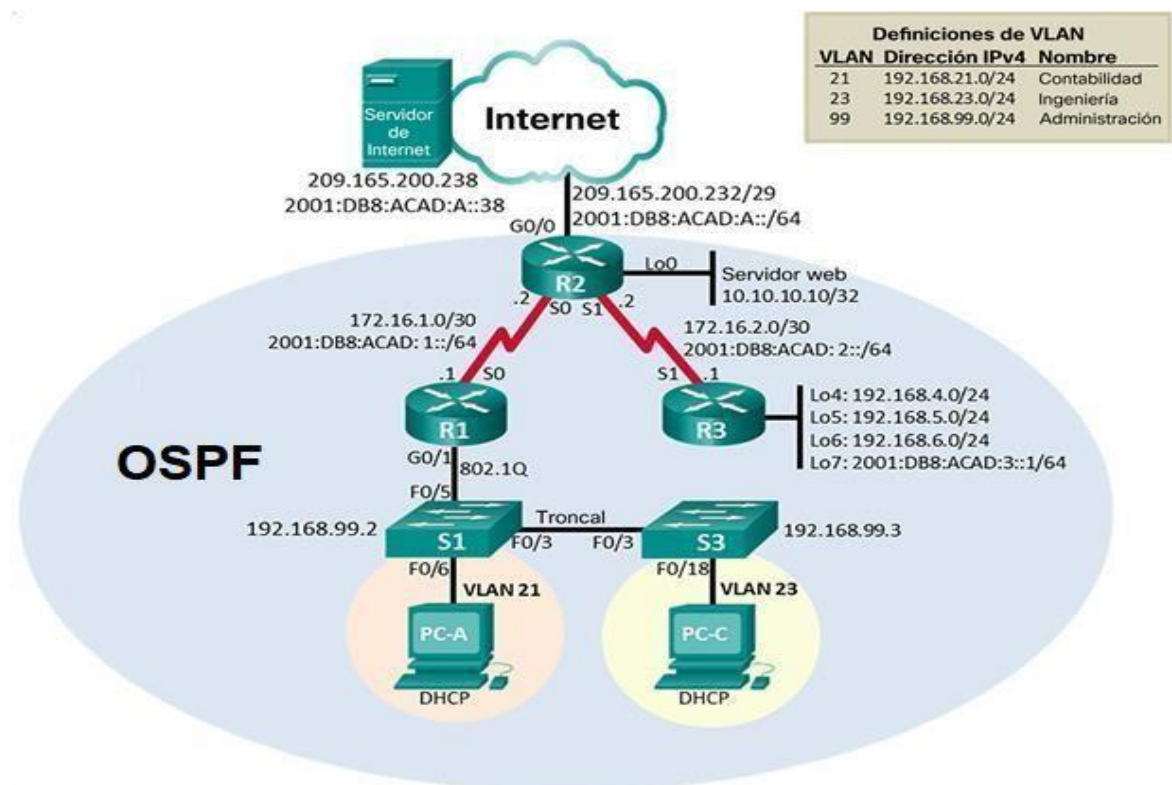
Fuente: Elaboración propia

Escenario 2

Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Topología

Figura 16. Topología tomada de prueba de habilidades CCNA



Fuente: Prueba de habilidades CCNA 2021, Cisco Academy

Parte 1: Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 6. Inicializar y volver a cargar los routers y los switches.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	erase startup-config
Volver a cargar todos los routers	reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	erase startup-config delete vlan.dat
Volver a cargar ambos switches	reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	show flash

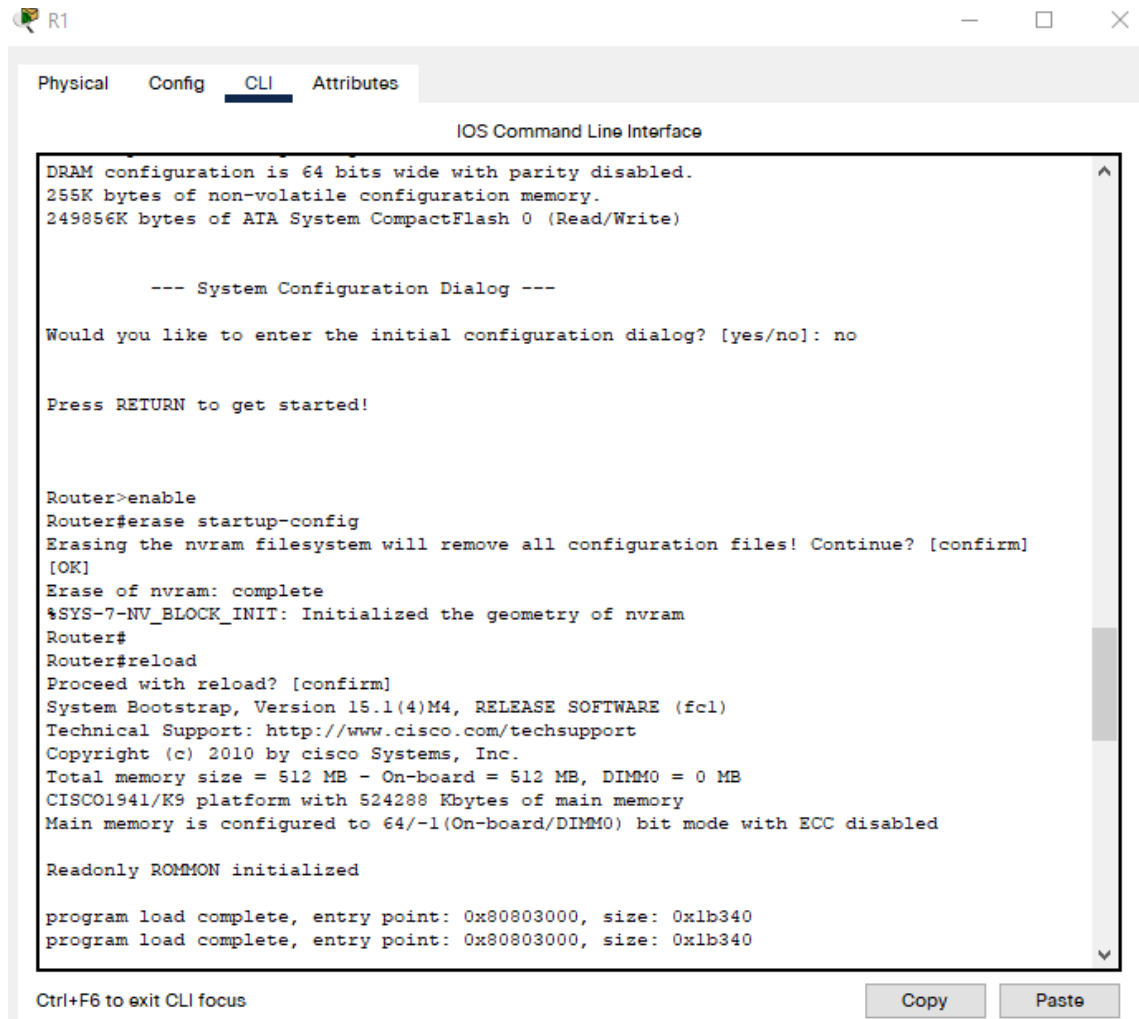
- Inicializar y volver a cargar los routers.

```
Router>enable
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
```

- Inicializar y volver a cargar los switches.

```
Switch>enable
Switch#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
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)
Switch#reload
Switch#show flash
Directory of flash:/  1  -rw-   4670455      <no date> 2960-lanbasek9-mz.150-
2.SE4.bin
```

Figura 17. Inicializar y cargar routers.



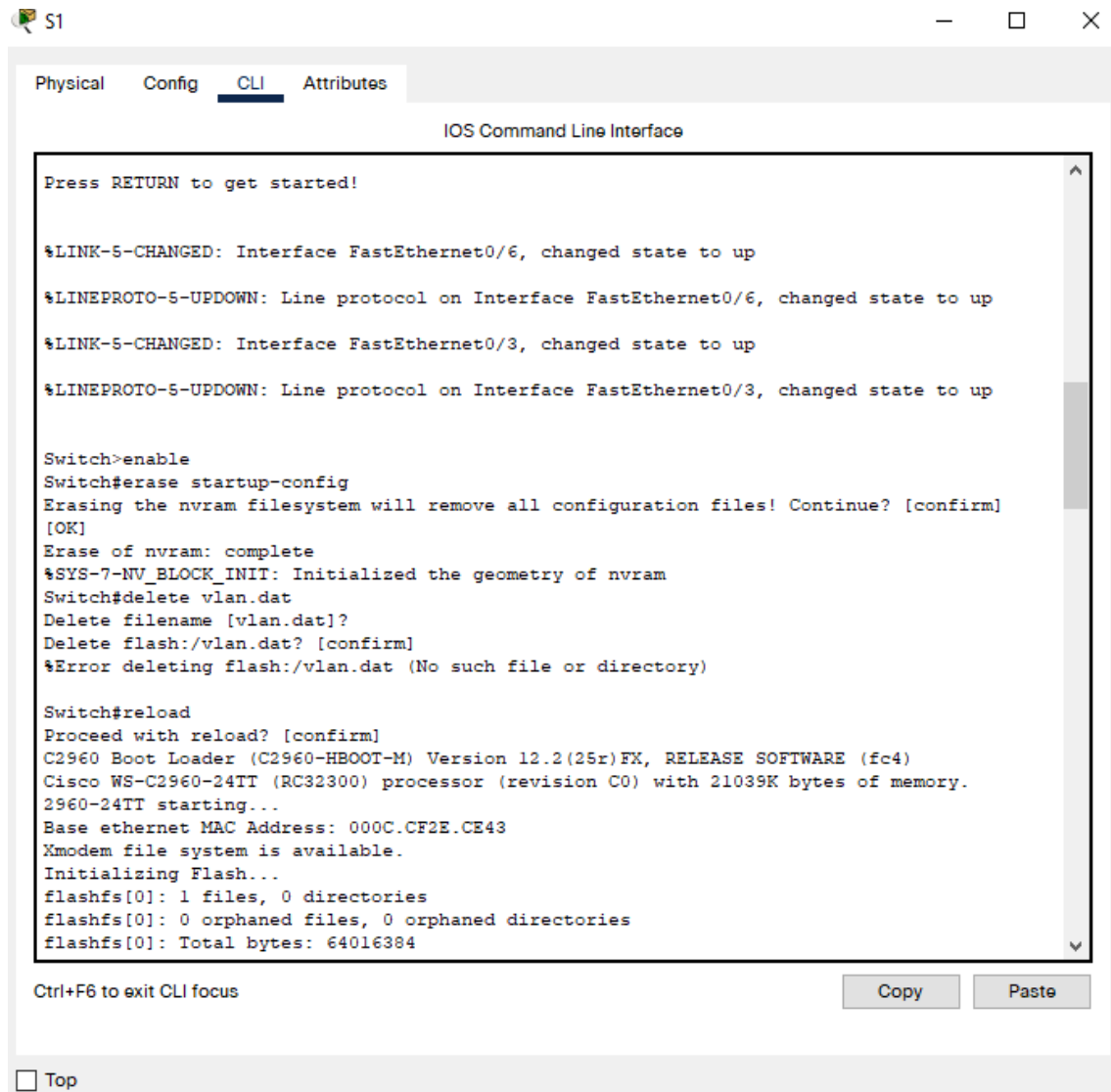
The screenshot shows a window titled "R1" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following sequence of commands and responses:

```
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)  
  
--- System Configuration Dialog ---  
  
Would you like to enter the initial configuration dialog? [yes/no]: no  
  
Press RETURN to get started!  
  
Router>enable  
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#  
Router#reload  
Proceed with reload? [confirm]  
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fcl)  
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  
CISCO1941/K9 platform with 524288 Kbytes of main memory  
Main memory is configured to 64/-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
```

At the bottom of the window, there is a status bar with "Ctrl+F6 to exit CLI focus" on the left and "Copy" and "Paste" buttons on the right.

Fuente: Elaboración propia

Figura 18. Inicializar y cargar switches.



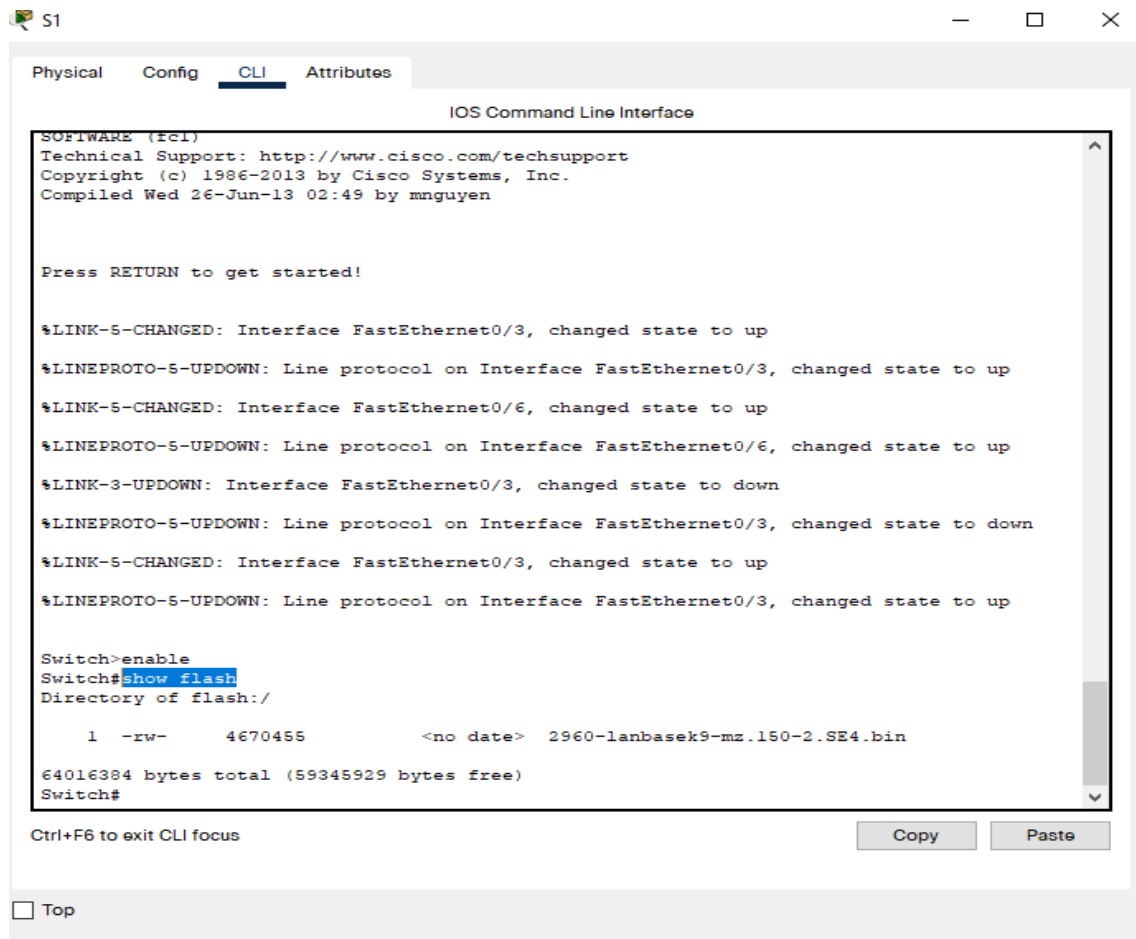
The screenshot shows a window titled "S1" with a tabbed interface. The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following sequence of commands and responses:

```
Press RETURN to get started!  
  
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up  
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up  
  
Switch>enable  
Switch#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  
Switch#delete vlan.dat  
Delete filename [vlan.dat]?  
Delete flash:/vlan.dat? [confirm]  
%Error deleting flash:/vlan.dat (No such file or directory)  
  
Switch#reload  
Proceed with reload? [confirm]  
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)  
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.  
2960-24TT starting...  
Base ethernet MAC Address: 000C.CF2E.CE43  
Xmodem file system is available.  
Initializing Flash...  
flashfs[0]: 1 files, 0 directories  
flashfs[0]: 0 orphaned files, 0 orphaned directories  
flashfs[0]: Total bytes: 64016384
```

At the bottom of the terminal window, there is a prompt "Ctrl+F6 to exit CLI focus" and two buttons labeled "Copy" and "Paste". Below the terminal window, there is a "Top" button.

Fuente: Elaboración propia

Figura 19. Verificando que la base de datos de VLAN no esté en la memoria flash en ambos switches.



```
Switch>enable
Switch#show flash
Directory of flash:/

 1  -rw-      4670455      <no date>  2960-lanbasek9-mz.150-2.SE4.bin

64016384 bytes total (59345929 bytes free)
Switch#
```

Fuente: Elaboración propia

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

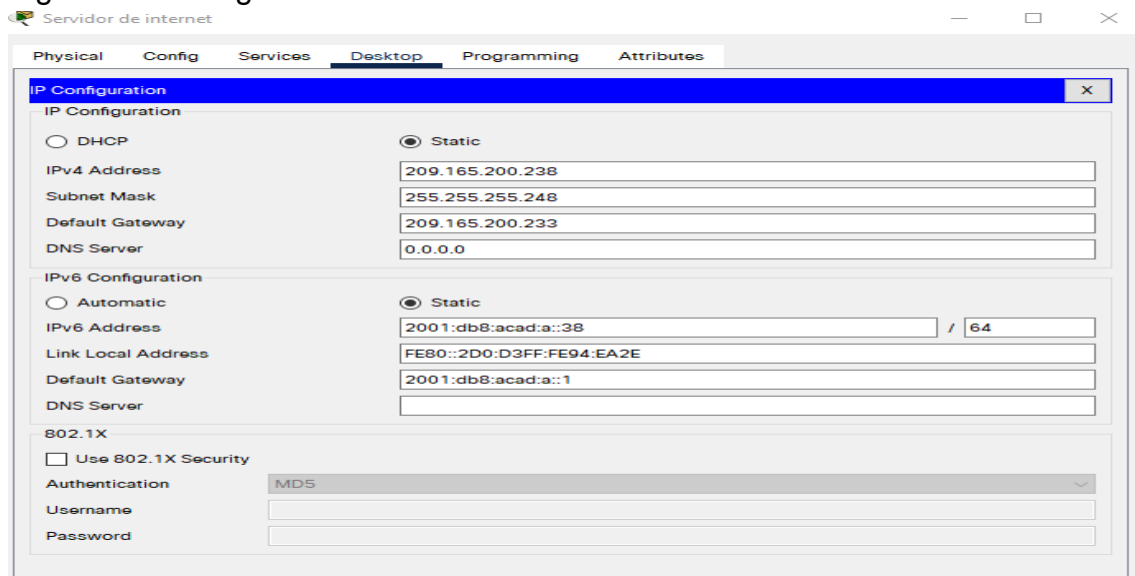
Tabla 7. Configurar la computadora de Internet.

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

En el Gateway predeterminado 209.165.200.225 es incorrecto ya que la primera IP en la red es 209.165.200.233

Figura 20. Configuración del servidor.



Fuente: Elaboración propia

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 8. Configuración R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

Nota: Todavía no configure G0/1.

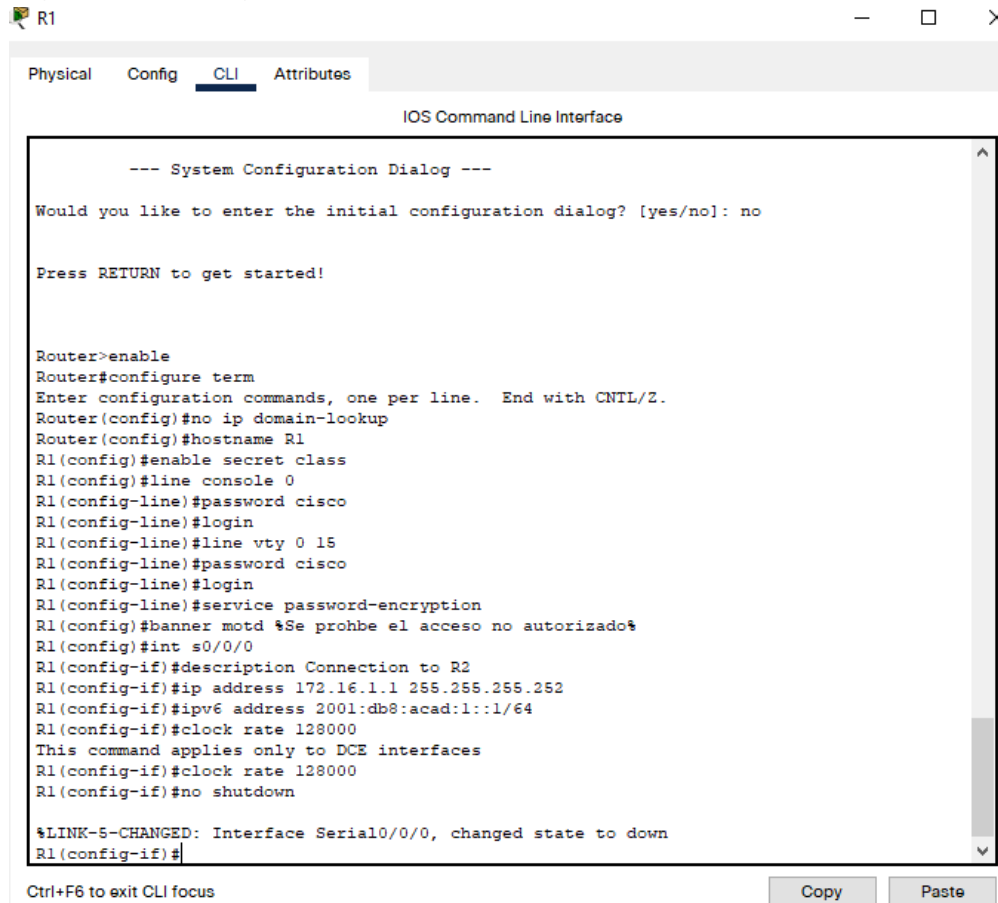
- Configuración R1

```
Router>enable
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
```

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#service password-encryption
R1(config)#banner motd %Se prohbe el acceso no autorizado%
R1(config)#int s0/0/0
R1(config-if)#description connection to R2
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
%Default route without gateway, if not a point-to-point interface, may impact
performance
R1(config)#ipv6 route ::/0 s0/0/0
R1(config)#
```

Figura 21. Configuración de R1.



```
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>enable
Router#configure term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#service password-encryption
R1(config)#banner motd %Se prohbe el acceso no autorizado%
R1(config)#int s0/0/0
R1(config-if)#description Connection to R2
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#clock rate 128000
This command applies only to DCE interfaces
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Fuente: Elaboración propia

Figura 22. Configuración de R1 ruta ip.

```
Physical  Config  CLI  Attributes
IOS Command Line Interface

Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 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!

Se prohbe el acceso no autorizado

User Access Verification

Password:

R1>ip config
^
% Invalid input detected at '^' marker.

R1>enable
Password:
Password:
Password:
% Bad secrets

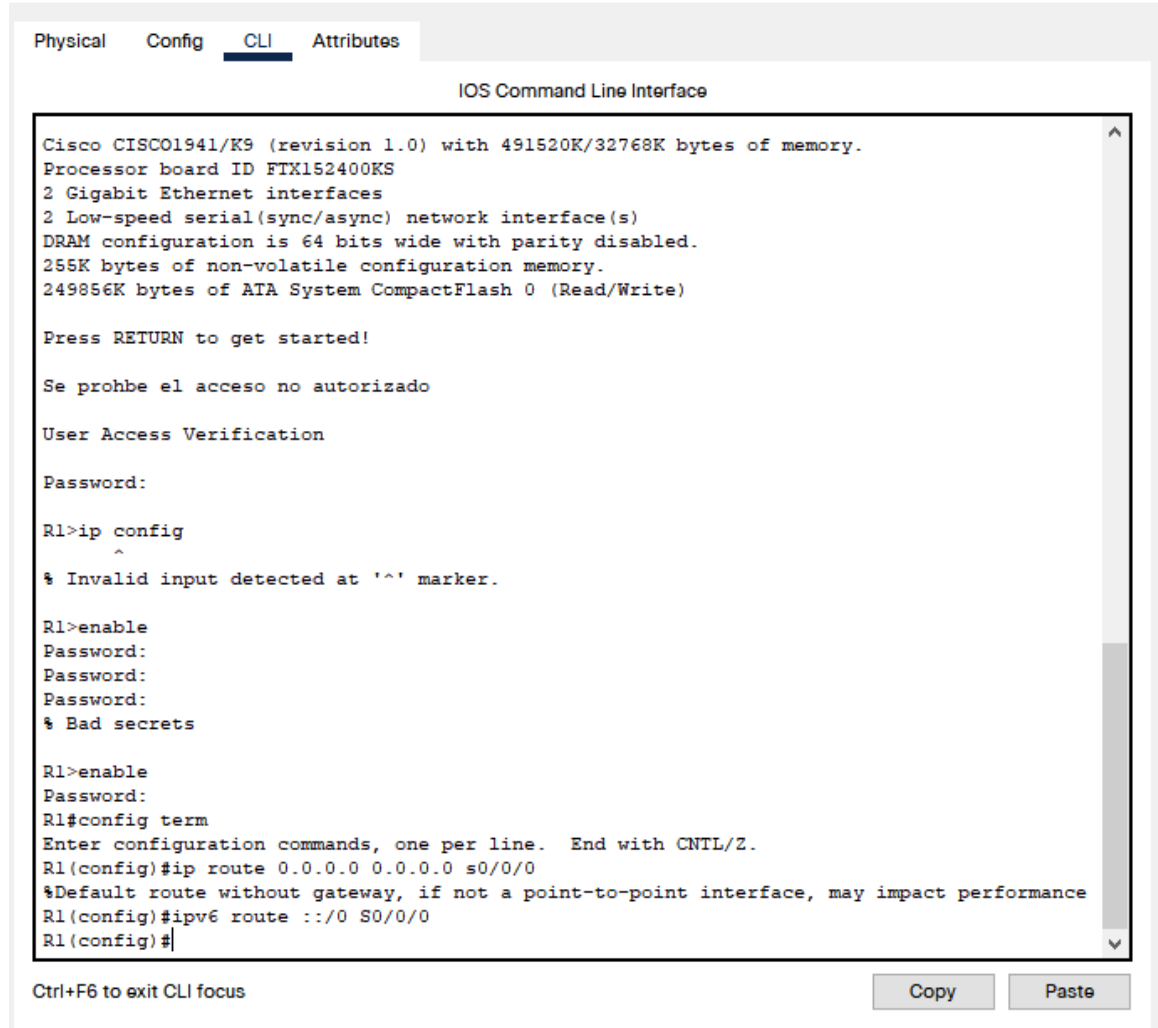
R1>enable
Password:
R1#config term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#ipv6 route ::/0 S0/0/0
R1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Fuente: Elaboración propia

Figura 23. Configuración de R1 rutas predeterminadas.



```
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 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!

Se prohbe el acceso no autorizado

User Access Verification

Password:

R1>ip config
^
% Invalid input detected at '^' marker.

R1>enable
Password:
Password:
Password:
% Bad secrets

R1>enable
Password:
R1#config term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#ipv6 route ::/0 S0/0/0
R1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Fuente: Elaboración propia

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 9. Configuración R2.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Habilitar el servidor HTTP	Packet tracer no soporta este comando
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz

Interfaz G0/0 (simulación de Internet)	<p>Establecer la descripción.</p> <p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <p>Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred.</p> <p>Activar la interfaz</p>
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

- Configuración R2.

```

Router>enable
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(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)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#service password-encryption
R2(config)#ip http server
R2(config)#banner motd %Se prohíbe personal no autorizado%
R2(config)#int s0/0/0
R2(config-if)#description connection to R1
R2(config-if)#ip address 172.16.1.2 255.255.255.252

```

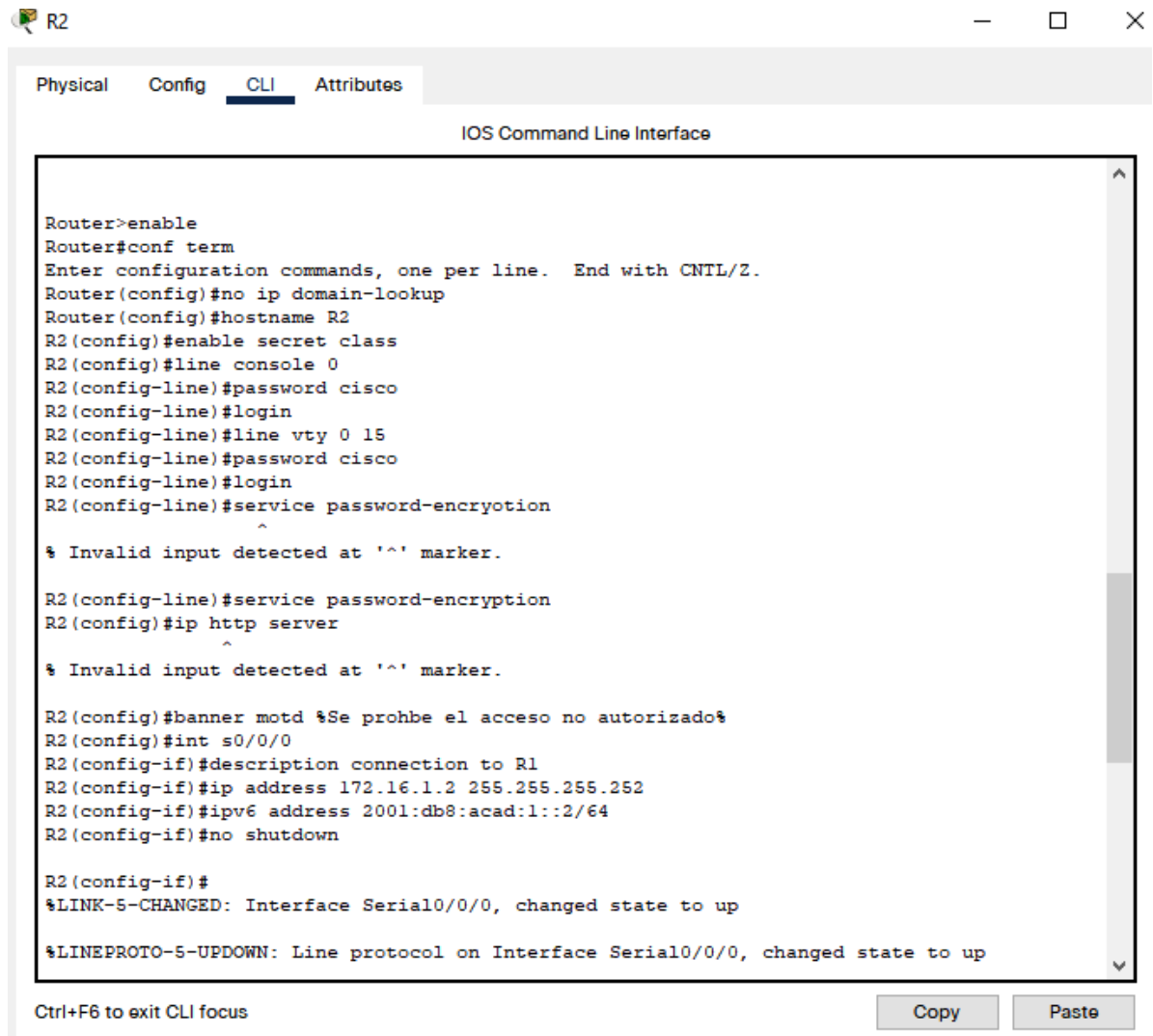
```

R2(config-if)#ipv6 address 2001:db8:acad:1::2/64
R2(config-if)#no shutdown
R2(config-if)#
%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
R2(config-if)#int s0/0/1
R2(config-if)#description connection to R3
R2(config-if)#ip address 172.16.2.2 255.255.255.252
R2(config-if)#ipv6 address 2001:db8:acad:2::2/64
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#int g0/0
R2(config-if)#description connection to Internet
R2(config-if)#ip address 209.165.200.233 255.255.255.248
R2(config-if)#ipv6 address 2001:db8:acad:a::1/64
R2(config-if)#no shutdown
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up

R2(config-if)#int loopback 0
R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state
to up
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#description simulated web server
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0
%Default route without gateway, if not a point-to-point interface, may impact
performance
R2(config)#ipv6 route ::/0 g0/0

```

Figura 24. Configuración de R2.



The screenshot shows a window titled "R2" with a tabbed interface. The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following sequence of commands and responses:

```
Router>enable
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(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)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#service password-encryption
      ^
% Invalid input detected at '^' marker.

R2(config-line)#service password-encryption
R2(config)#ip http server
      ^
% Invalid input detected at '^' marker.

R2(config)#banner motd %Se prohbe el acceso no autorizado%
R2(config)#int s0/0/0
R2(config-if)#description connection to R1
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:db8:acad:1::2/64
R2(config-if)#no shutdown

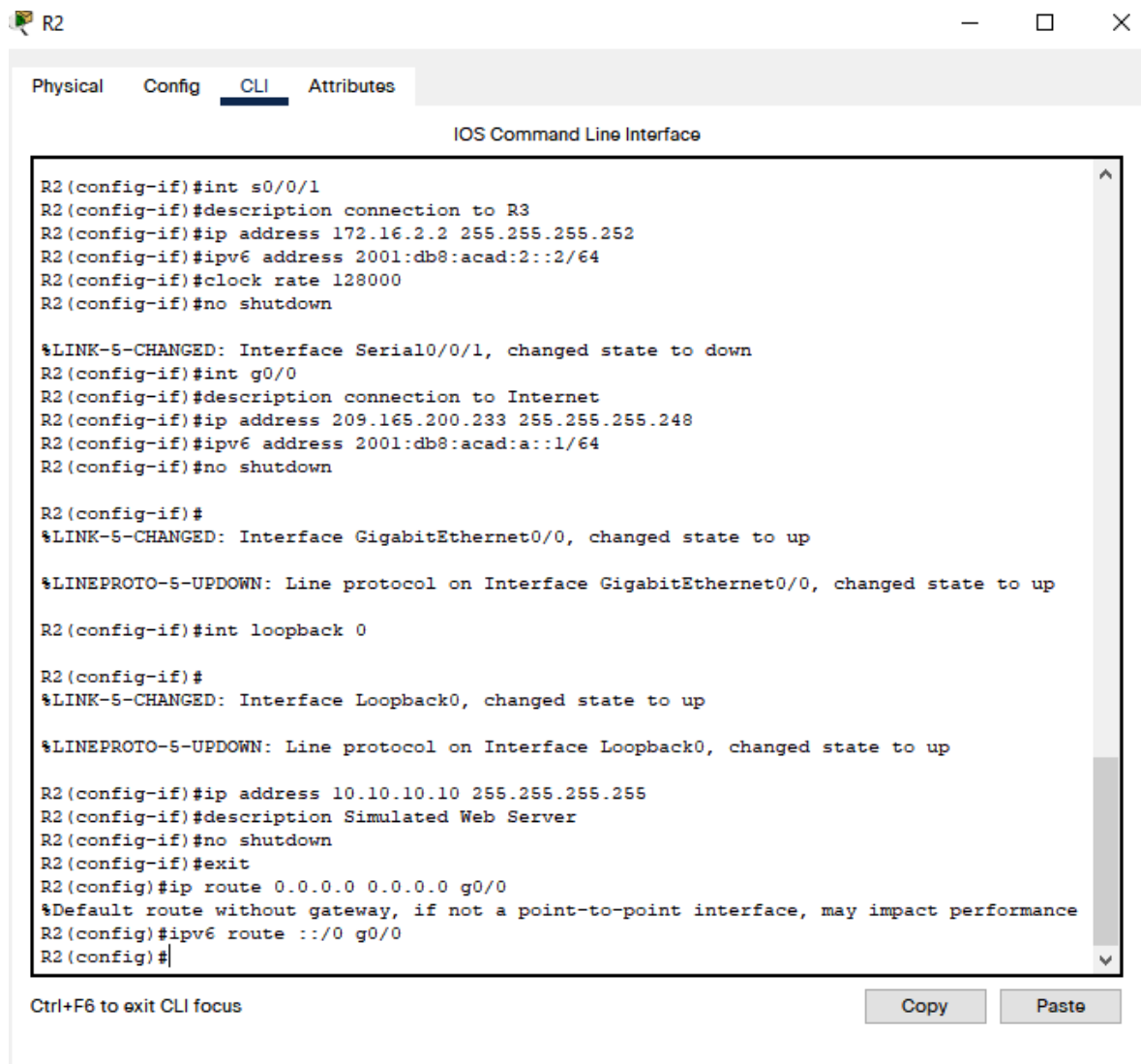
R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

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

At the bottom of the window, there is a status bar with the text "Ctrl+F6 to exit CLI focus" and two buttons labeled "Copy" and "Paste".

Fuente: Elaboración propia

Figura 25. Configuración de R2 rutas predeterminadas.



The screenshot shows a window titled "R2" with a tabbed interface. The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following configuration steps:

```
R2(config-if)#int s0/0/1
R2(config-if)#description connection to R3
R2(config-if)#ip address 172.16.2.2 255.255.255.252
R2(config-if)#ipv6 address 2001:db8:acad:2::2/64
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#int g0/0
R2(config-if)#description connection to Internet
R2(config-if)#ip address 209.165.200.233 255.255.255.248
R2(config-if)#ipv6 address 2001:db8:acad:a::1/64
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R2(config-if)#int loopback 0

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#description Simulated Web Server
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
R2(config)#ipv6 route ::/0 g0/0
R2(config)#
```

At the bottom of the window, there is a status bar with the text "Ctrl+F6 to exit CLI focus" and two buttons: "Copy" and "Paste".

Fuente: Elaboración propia

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 10. Configuración R3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
Rutas predeterminadas	Configure una ruta IPv4 predeterminada de S0/0/1. Configure una ruta IPv6 predeterminada de S0/0/1.

- Configuración R3

```
Router>enable
Router#conf term
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
% Incomplete command.
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#service password-encryption
R3(config)#banner motd %Se prohbe el acceso no autorizado.%
R3(config)#int s0/0/1
R3(config-if)#description connection to R2
R3(config-if)#ip address 172.16.2.1 255.255.255.252
R3(config-if)#ipv6 address 2001:db8:acad:2::1/64
R3(config-if)#no shutdown
R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state
to up
R3(config-if)#int loopback 4
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state
to up
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#int loopback 5
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state
to up
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#int loopback 6
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state
to up
```

```

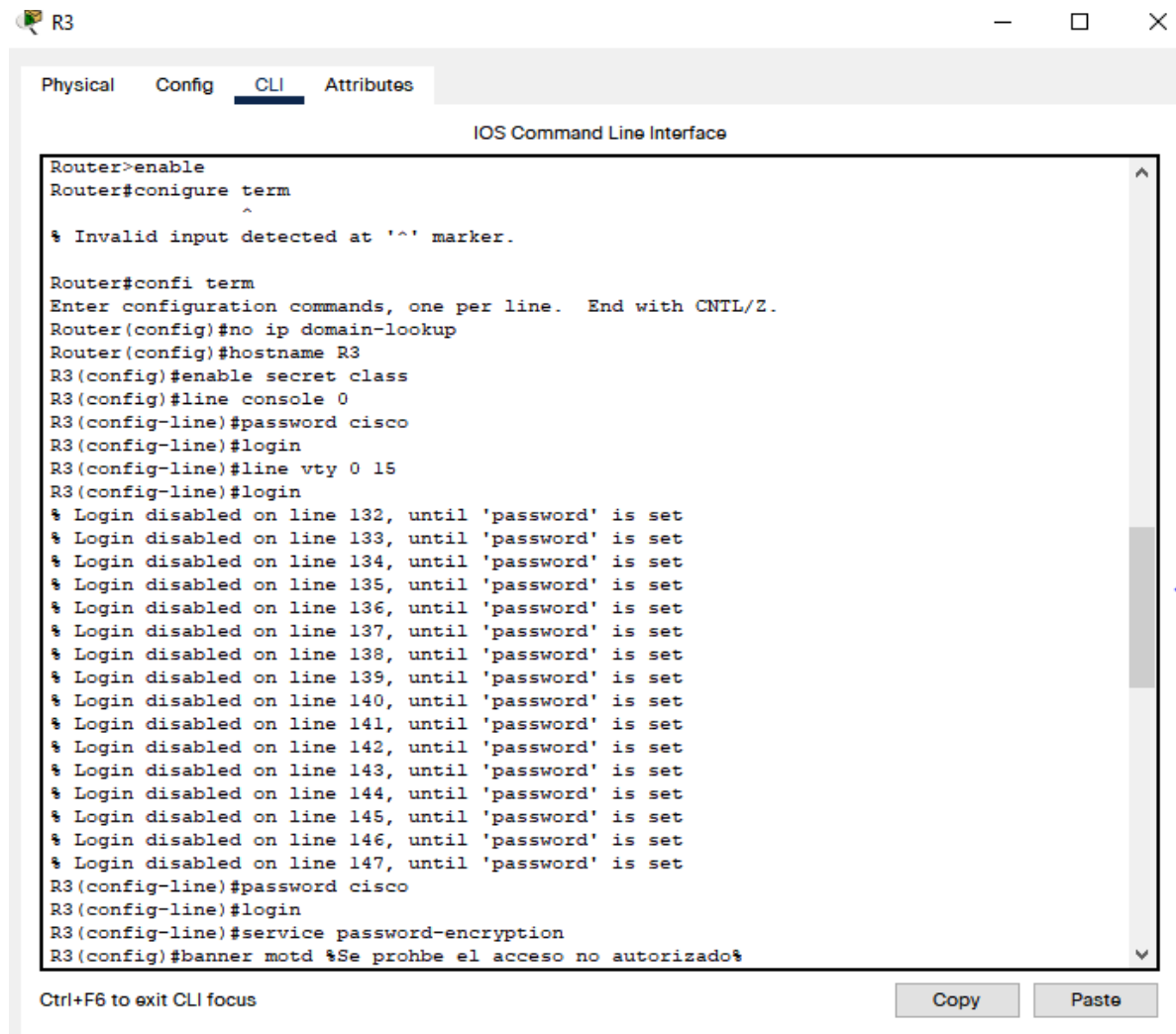
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#int loopback 7
%LINK-5-CHANGED: Interface Loopback7, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state
to up
R3(config-if)#ipv6 address 2001:db8:acad:3::1/64

R3(config-if)#exit

R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
%Default route without gateway, if not a point-to-point interface, may impact
performance
R3(config)#ipv6 route ::/0 s0/0/1

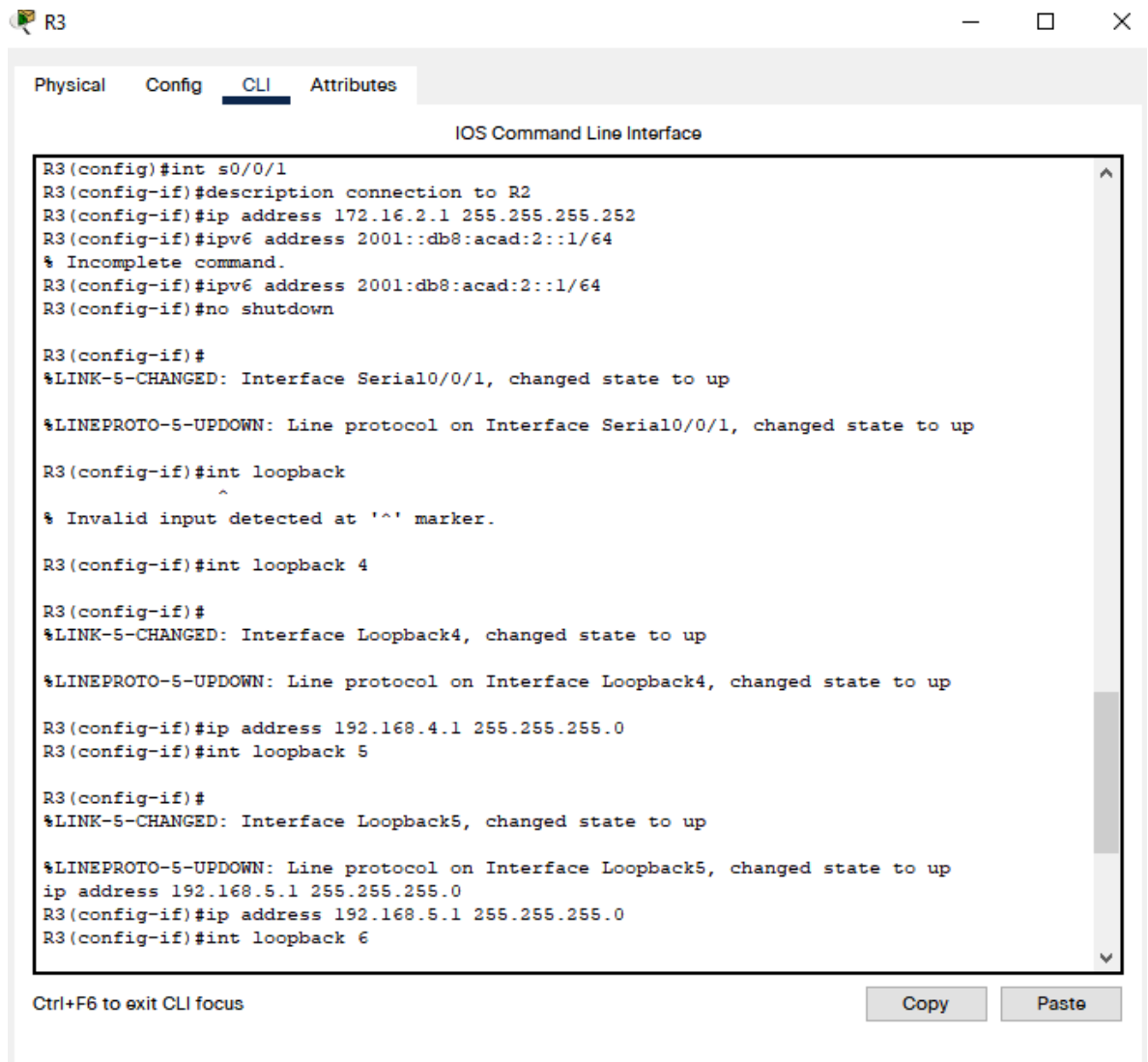
```

Figura 26. Configuración de R3.



Fuente: Elaboración propia.

Figura 27. Configuración de R3 interfaces look back.



The screenshot shows a window titled "R3" with a tabbed interface. The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following commands and responses:

```
R3(config)#int s0/0/1
R3(config-if)#description connection to R2
R3(config-if)#ip address 172.16.2.1 255.255.255.252
R3(config-if)#ipv6 address 2001::db8:acad:2::1/64
% Incomplete command.
R3(config-if)#ipv6 address 2001:db8:acad:2::1/64
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

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

R3(config-if)#int loopback
^
% Invalid input detected at '^' marker.

R3(config-if)#int loopback 4

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up

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

R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#int loopback 5

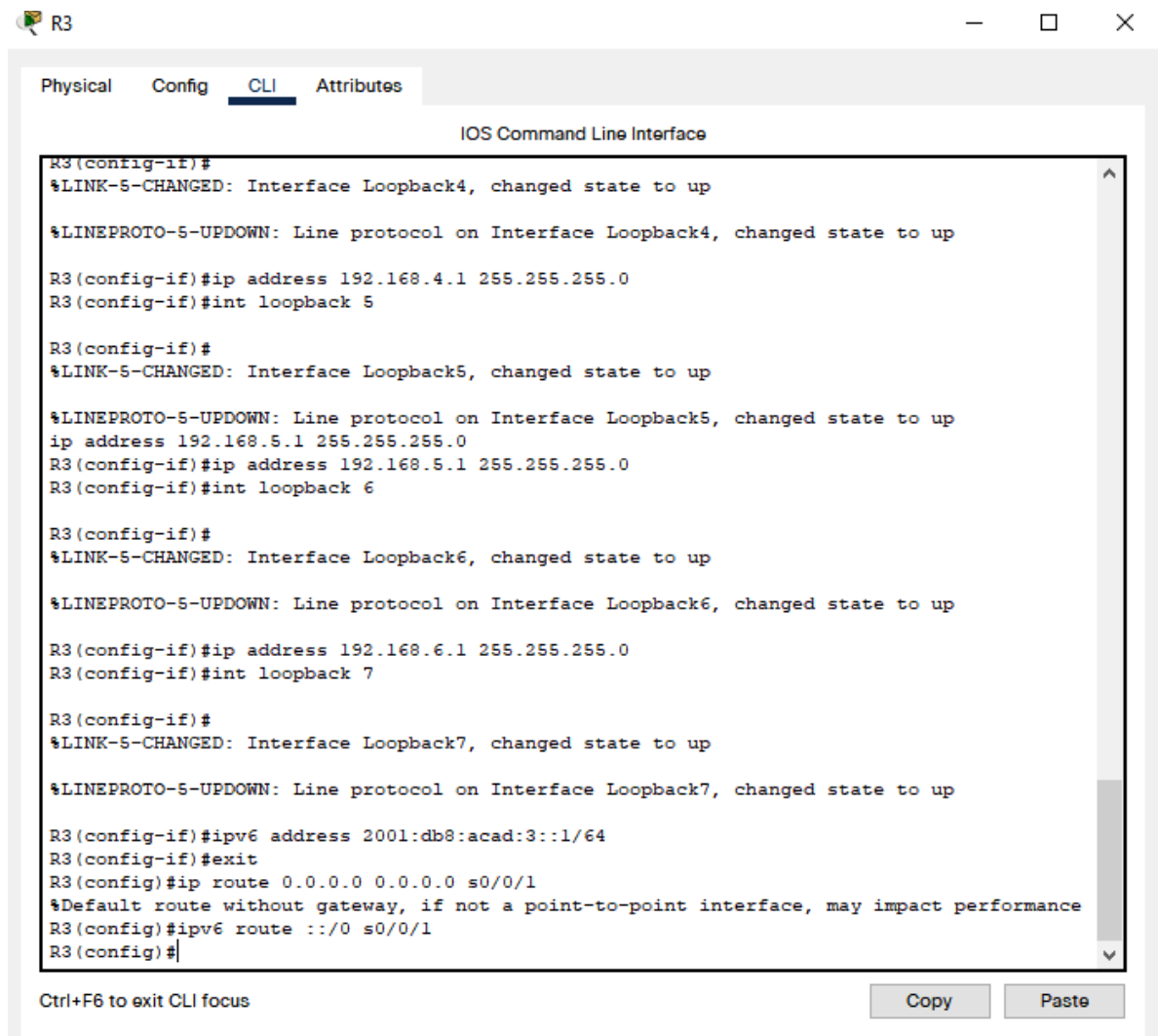
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up
ip address 192.168.5.1 255.255.255.0
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#int loopback 6
```

At the bottom of the window, there is a prompt "Ctrl+F6 to exit CLI focus" and two buttons: "Copy" and "Paste".

Fuente: Elaboración propia.

Figura 28. Configuración de R3 rutas predeterminadas.



The screenshot shows a network configuration window for router R3. The window has tabs for Physical, Config, CLI, and Attributes, with CLI selected. The title is "IOS Command Line Interface". The terminal output shows the configuration of seven loopback interfaces (Loopback4 to Loopback7) and a default route. Each interface is configured with an IP address from the 192.168.4.1 to 192.168.7.1 range and the 255.255.255.0 subnet mask. The configuration includes commands for entering interface configuration mode, setting the IP address, and exiting. Status messages indicate that the link and line protocol are up for each interface. Finally, a default route is configured with the command "ip route 0.0.0.0 0.0.0.0 s0/0/1".

```
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#int loopback 5
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up
ip address 192.168.5.1 255.255.255.0
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#int loopback 6
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#int loopback 7
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback7, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up
R3(config-if)#ipv6 address 2001:db8:acad:3::1/64
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
%Default route without gateway, if not a point-to-point interface, may impact performance
R3(config)#ipv6 route ::/0 s0/0/1
R3(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Fuente: Elaboración propia.

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

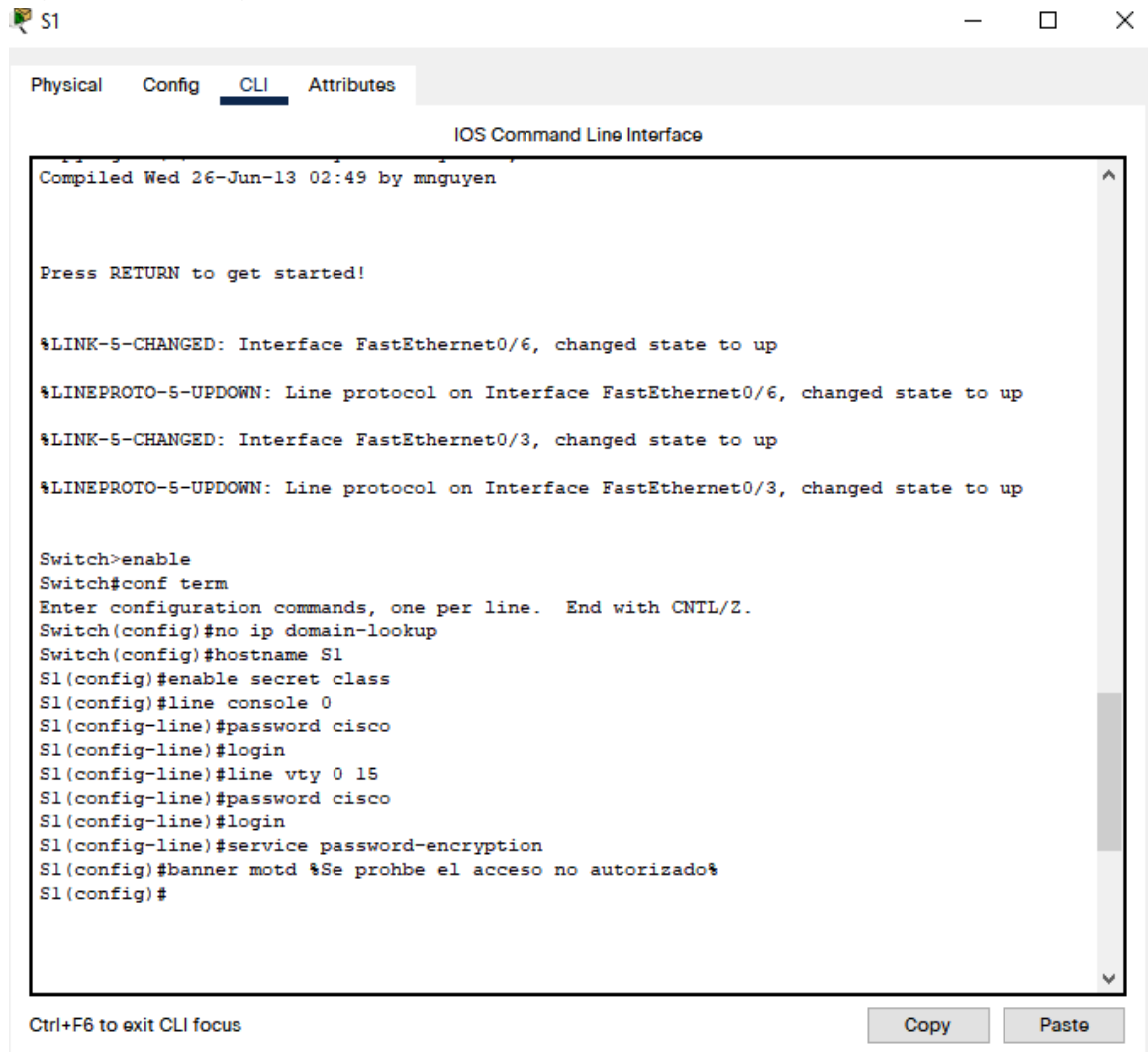
Tabla 11. Configuración S1.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del switch	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

- Código utilizado para la configuración de S1

```
Switch>enable
Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd %Se prohbe el acceso no autorizado%
```

Figura 29. Configuración de S1.



The screenshot shows a window titled 'S1' with a tabbed interface. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal output shows the following configuration steps:

```
Compiled Wed 26-Jun-13 02:49 by mnguyen

Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

Switch>enable
Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd %Se prohbe el acceso no autorizado%
S1(config)#
```

At the bottom of the window, there is a prompt 'Ctrl+F6 to exit CLI focus' and two buttons: 'Copy' and 'Paste'.

Fuente: Elaboración propia.

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

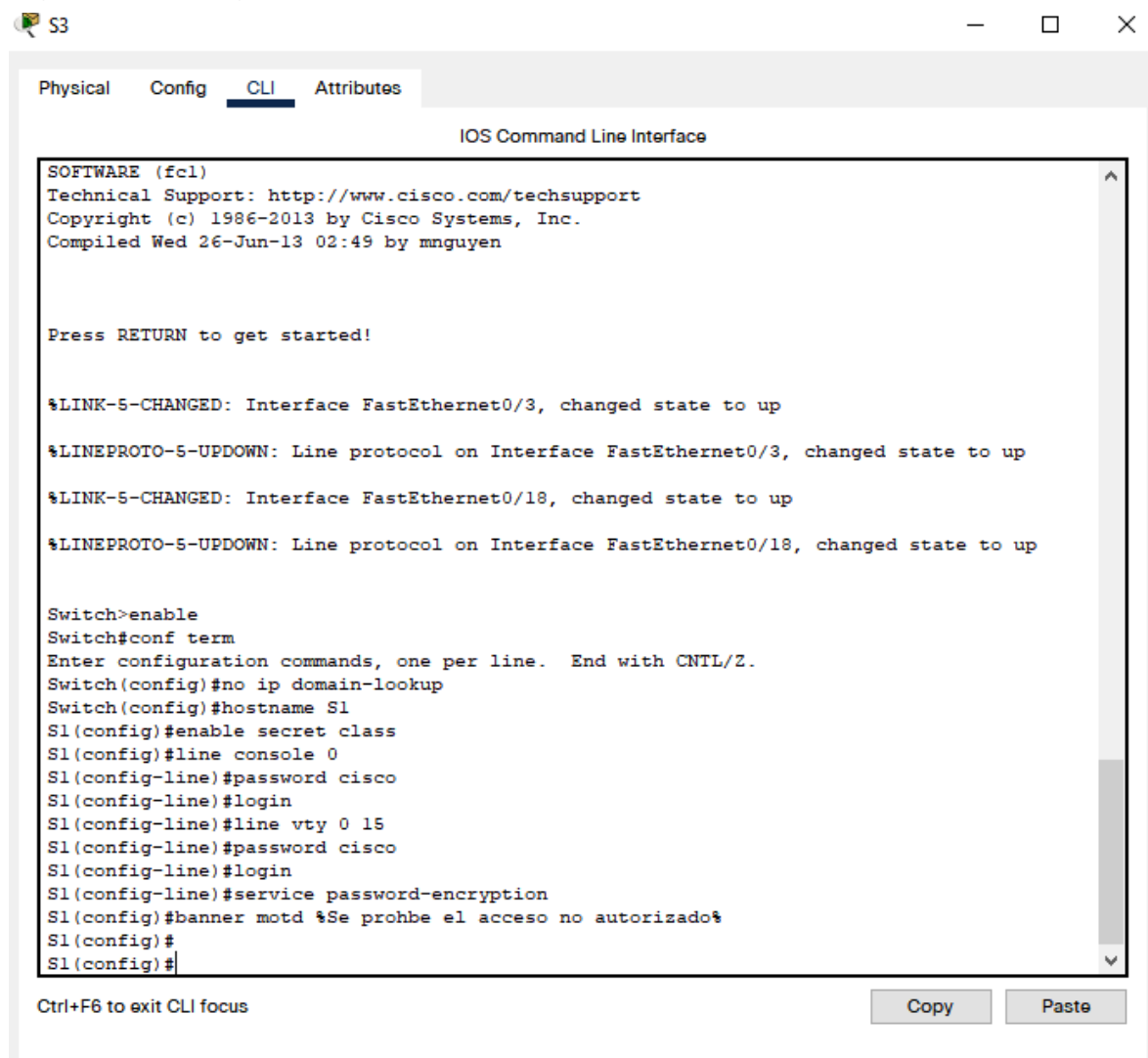
Tabla 12. Configuración S3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

- Código utilizado para la configuración de S3

```
Switch>enable
Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd %Se prohbe el acceso no autorizado%
```

Figura 30. Configuración de S3.



The screenshot shows a window titled "S3" with a tabbed interface. The "CLI" tab is active, displaying the "IOS Command Line Interface". The text in the window is as follows:

```
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen

Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up

Switch>enable
Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd %Se prohbe el acceso no autorizado%
S1(config)#
S1(config)#
```

At the bottom of the window, there is a status bar with the text "Ctrl+F6 to exit CLI focus" and two buttons labeled "Copy" and "Paste".

Fuente: Elaboración propia.

Paso 7: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los dispositivos de red.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 13. Verificar la conectividad de la red.

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Tasa de éxito 100% (5/5), round-trip min/avg/max = 10/16/41 ms
R2	R3, S0/0/1	172.16.2.1	Tasa de éxito 100% (5/5), round-trip min/avg/max = 10/16/41 ms
PC de Internet	Gateway predeterminado	209.165.200.233	Exitoso

- Ping desde R1 a R2.

```
R1>enable
```

```
Password:
```

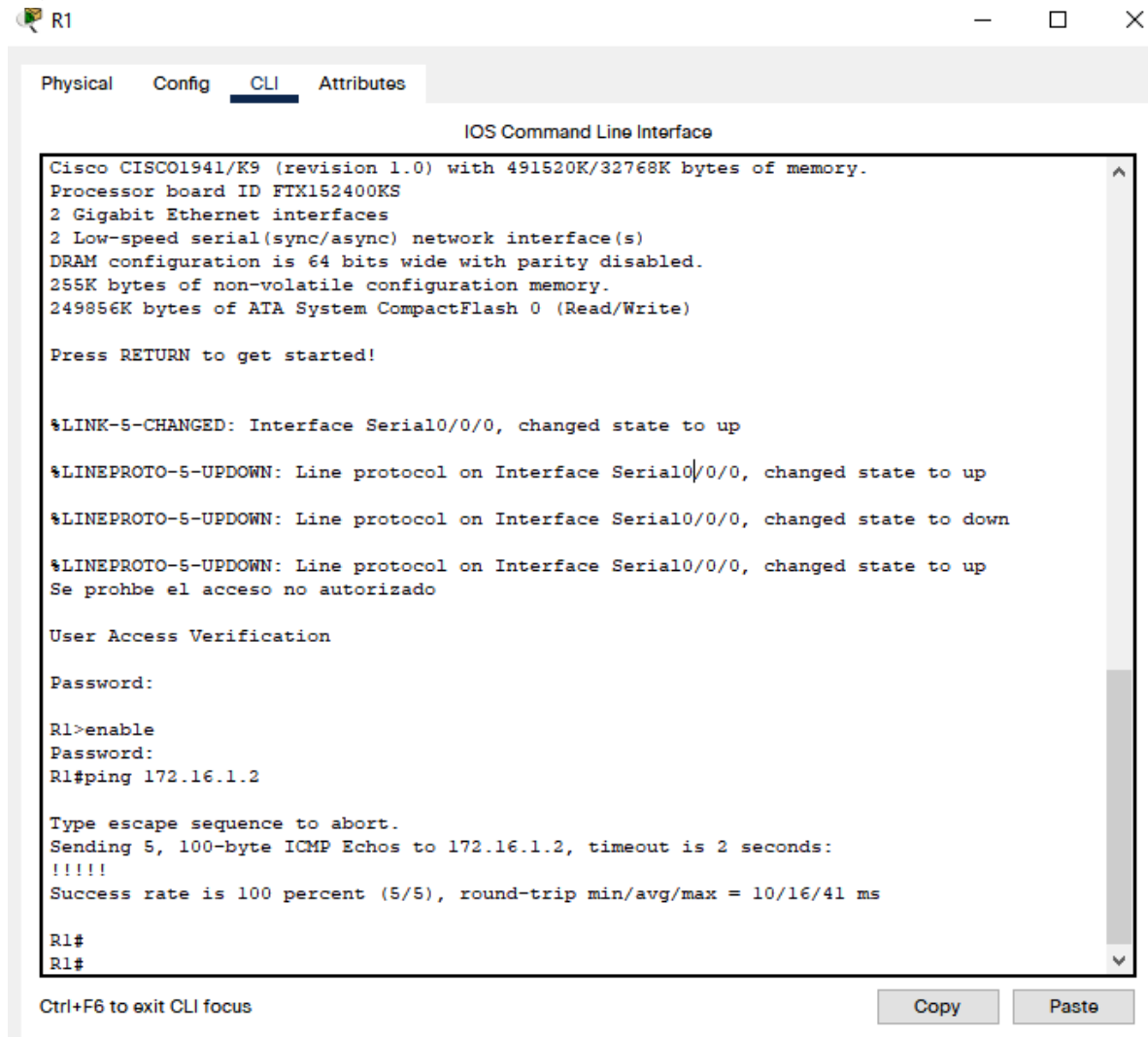
```
R1#ping 172.16.1.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
```

```
!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 6/13/33 ms
```

Figura 31. Verificación de la conexión de la red entre R1 a R2.



```
R1
Physical Config CLI Attributes
IOS Command Line Interface
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 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!

%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
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Se prohbe el acceso no autorizado

User Access Verification

Password:
R1>enable
Password:
R1#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/16/41 ms

R1#
R1#
```

Ctrl+F6 to exit CLI focus

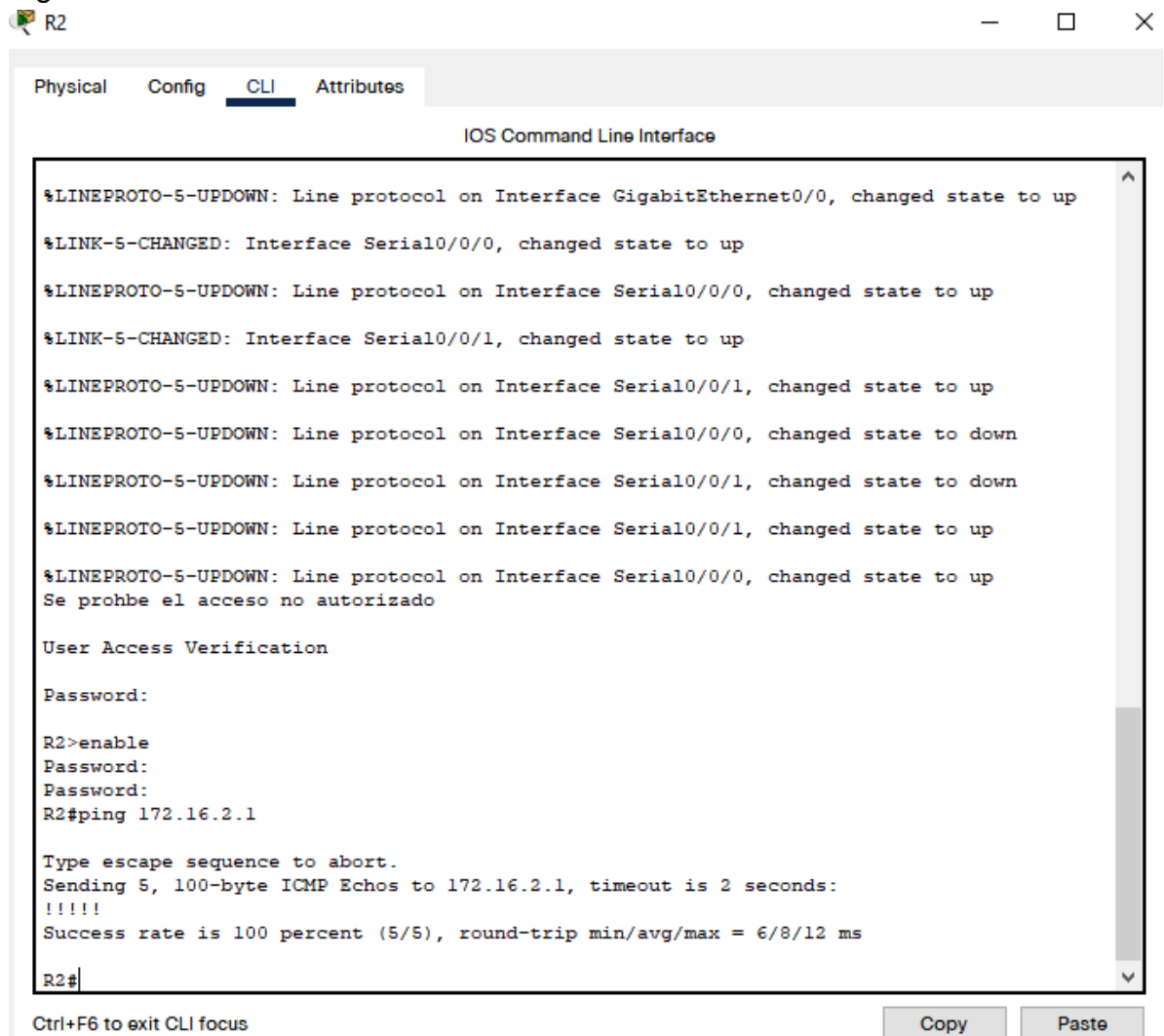
Copy Paste

Fuente: Elaboración propia.

- Ping desde R2 a R3.

```
R2>enable
Password:
R2#ping 172.16.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 6/8/10 ms
```

Figura 32. Verificación de la conexión de la red entre R2 a R3.



The screenshot shows the CLI interface of a Cisco router (R2). The window title is "R2" and it has standard window controls. The interface has tabs for "Physical", "Config", "CLI", and "Attributes", with "CLI" selected. The main area is titled "IOS Command Line Interface" and contains the following text:

```
%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
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Se prohbe el acceso no autorizado

User Access Verification

Password:

R2>enable
Password:
Password:
R2#ping 172.16.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/8/12 ms

R2#
```

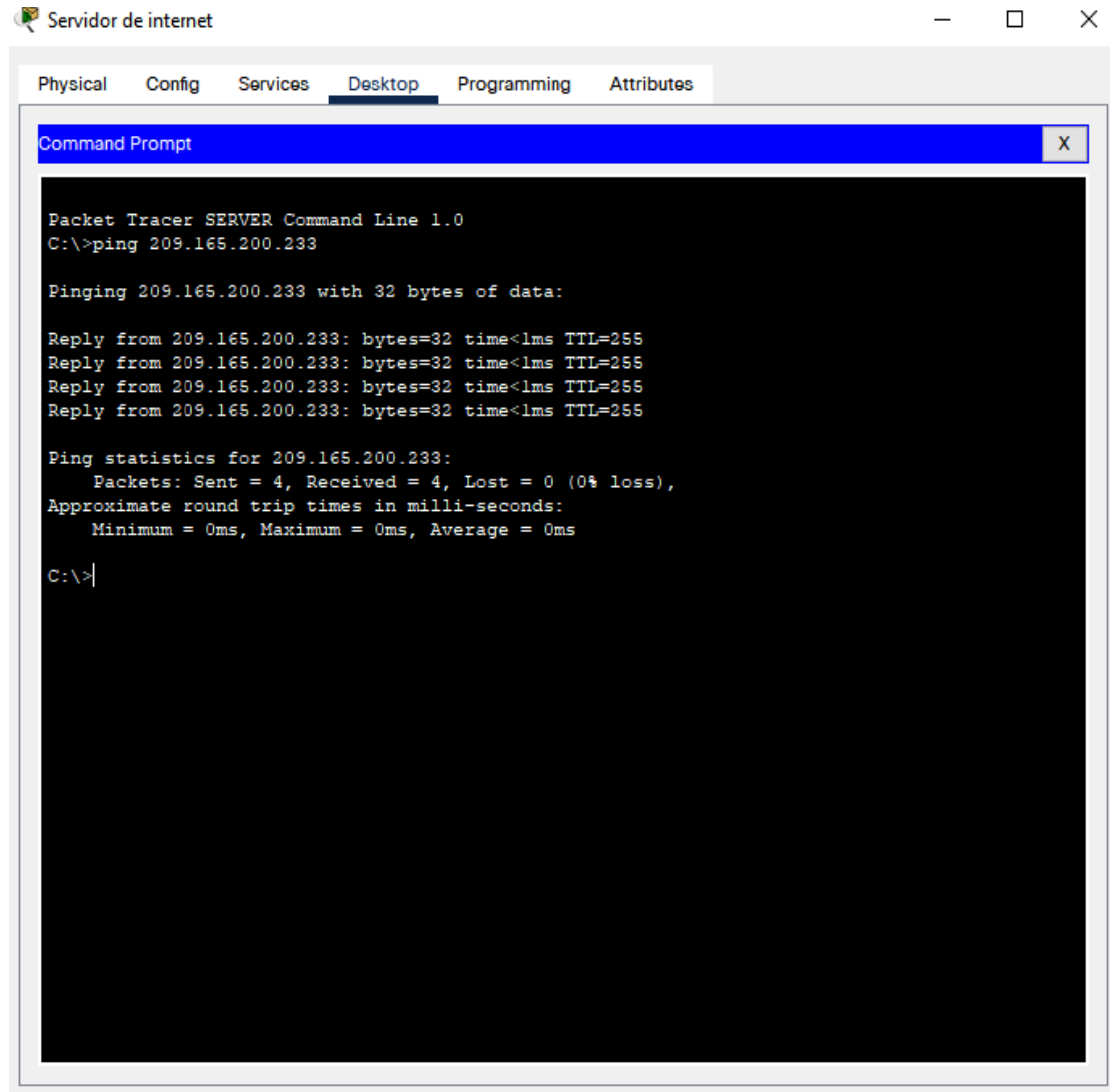
At the bottom of the window, there is a status bar with "Ctrl+F6 to exit CLI focus" on the left and "Copy" and "Paste" buttons on the right.

Fuente: Elaboración propia.

- Ping desde internet PC a Gateway predeterminado.

ping 209.165.200.233

Figura 33. Verificación de la conexión de la red entre PC internet a Gateway predeterminado.



Fuente: Elaboración propia.

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los ping se realicen correctamente.

Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 14. Configurar la seguridad S1.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	Switchport access vlan 21
Apagar todos los puertos sin usar	Int range f0/1-2, f0/4, f0/7-24, g0/1-2

- Código para crear la base de datos de VLAN y demás configuraciones de S1

```
S1>enable
```

```
Password:
```

```
S1#conf term
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
S1(config)#vlan 21
```

```
S1(config-vlan)#name Contabilidad
```

```
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingieneria
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administracion
S1(config-vlan)#int vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.99.1
S1(config)#int f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#int f0/6
S1(config-if)#switchport access vlan 21
```

```
S1(config)#int range f0/1-2, f0/4, f0/7-24, g0/1-2
```

```
S1(config-if-range)#shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
```

```
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
```

```
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
```

```
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
```

```
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
```

```
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
```

```
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
```

```
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down
```

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down

Figura 34. Configuración de seguridad S1.

```

S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.99.1
S1(config)#int f0/3
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2]
S1(config-if-range)#switchport mode access
S1(config-if-range)#int f0/6
S1(config-if)#switchport access vlan 21
S1(config-if)#
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1>show vlan

VLAN Name                Status    Ports
-----
1    default                  active    Fa0/1, Fa0/2, Fa0/4, Fa0/7
                                           Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                           Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                           Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                           Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                           Fa0/24, Gig0/1, Gig0/2

21   Contabilidad             active    Fa0/6
23   Ingenieria               active
99   Administracion           active
1002 fddi-default             active
1003 token-ring-default     active
1004 fddinet-default        active
1005 trnet-default          active

VLAN Type  SAID      MTU   Parent RingNo BridgeNo Stp  BrdgMode Transl  Trans2
-----
1    enet     100001   1500  -     -     -     -     -     C     0
21   enet     100021   1500  -     -     -     -     -     C     0
23   enet     100023   1500  -     -     -     -     -     C     0
--More--

```

Fuente: Elaboración propia.

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 15. Configurar la seguridad S3.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombrea cada VLAN.
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gatewaypredeterminado.
Forzar el enlace troncal en la interfazF0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos comopuertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 23	Switchport access vlan 23
Apagar todos los puertos sin usar	Int range f0/1-2, f0/4-17, f0/19-24, g0/1-2

- Código para la configuración de la seguridad de S3

```
S1>enable
Password:
S1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administracion
S1(config-vlan)#exit
S1(config)#int vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S1(config-if)#ip address 192.168.99.3 255.255.255.0

S1(config-if)#no shutdown

S1(config-if)#exit

S1(config)#ip default-gateway 192.168.99.1

S1(config)#int f0/3

S1(config-if)#switchport mode trunk

S1(config-if)#switchport trunk native vlan 1

S1(config-if)#int range f0/1-2, f0/4-24, g0/1-2

S1(config-if-range)#switchport mode acces

S1(config-if-range)#int f0/18

S1(config-if)#switchport access

% Incomplete command.

S1(config-if)#switchport access vlan 23

S1(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2

S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down

S1(config-if-range)#

Figura 35. Configuración de seguridad S3.

```

S3>enable
Password:
S3#conf term
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vlan 21
S3(config-vlan)#name Contabilidad
S3(config-vlan)#vlan 23
S3(config-vlan)#name Ingenieria
S3(config-vlan)#vlan 99
S3(config-vlan)#name Administracion
S3(config-vlan)#exit
S3(config)#int vlan 99
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1
S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode acces
S3(config-if-range)#int f0/18
S3(config-if)#switchport access
% Incomplete command.
S3(config-if)#switchport access vlan 23
S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2
S3(config-if-range)#shutdown

S3>show vlan

VLAN Name                Status    Ports
-----
1    default                  active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                           Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                           Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                           Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                           Fa0/23, Fa0/24, Gig0/1, Gig0/2

21   Contabilidad             active
23   Ingenieria               active    Fa0/18
99   Administracion           active
1002 fddi-default             active
1003 token-ring-default     active
1004 fddinet-default        active
1005 trnet-default          active

VLAN Type  SAID      MTU   Parent  RingNo  BridgNo  Stp    BrdgMode  Transl  Transl
-----
1    enet   100001   1500  -       -       -      -         -         0       0
21   enet   100021   1500  -       -       -      -         -         0       0
23   enet   100023   1500  -       -       -      -         -         0       0

```

Fuente: Elaboración propia.

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16. Configurar la seguridad VLAN R1.

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 enG0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .23 enG0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .99 enG0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz
Activar la interfaz G0/1	Int g0/1

- Código para la configuración de seguridad de la VLAN R1

```
R1>enable
Password:
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/1.21
R1(config-subif)#description VLAN 21
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#int g0/1.23
R1(config-subif)#description VLAN 23
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#int g0/1.99
```

```

R1(config-subif)#description VLAN 99
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#int g0/1
R1(config-if)#no shutdown
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

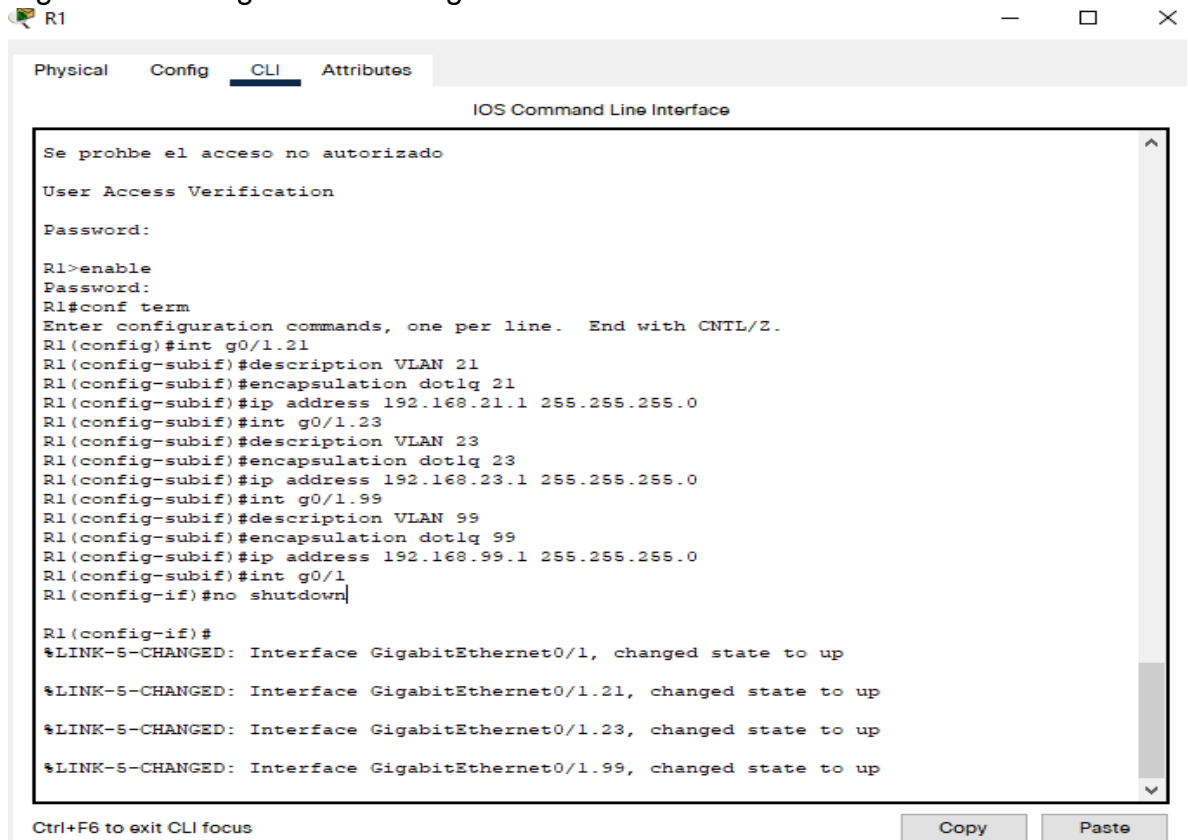
%LINK-5-CHANGED: Interface GigabitEthernet0/1.21, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.23, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.99, changed state to up

```

Figura 36. Configuración de seguridad de VLAN R1.



Fuente: Elaboración propia.

Paso 4: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los switches y el R1.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 17. Verificar la conectividad de la red.

De sde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Exitoso
S3	R1, dirección VLAN 99	192.168.99.1	Exitoso
S1	R1, dirección VLAN 21	192.168.21.1	Exitoso
S3	R1, dirección VLAN 23	192.168.23.1	Exitoso

- Código para realizar las pruebas de conectividad.

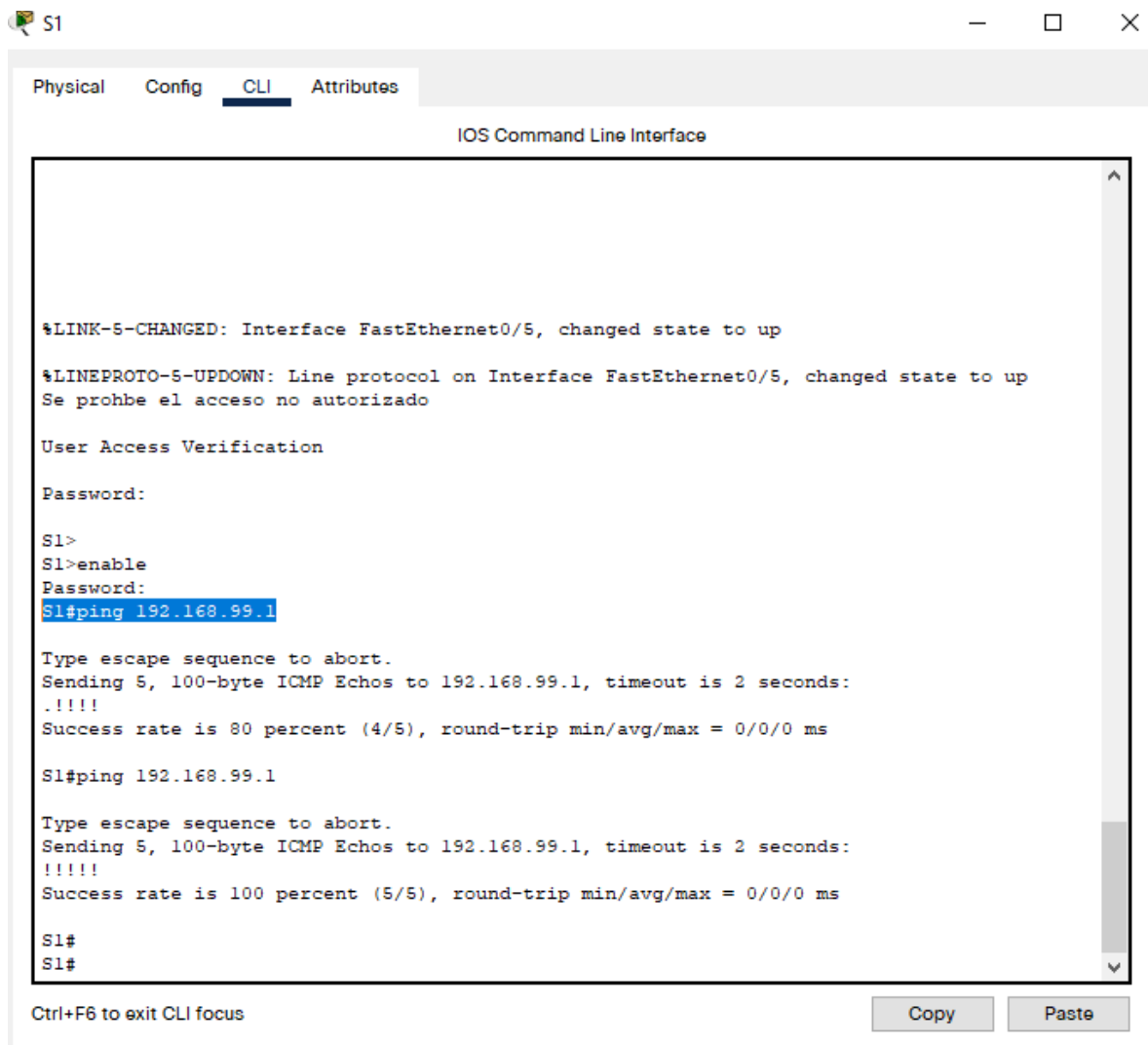
S1#ping 192.168.99.1

S3#ping 192.168.99.1

S1#ping 192.168.21.1

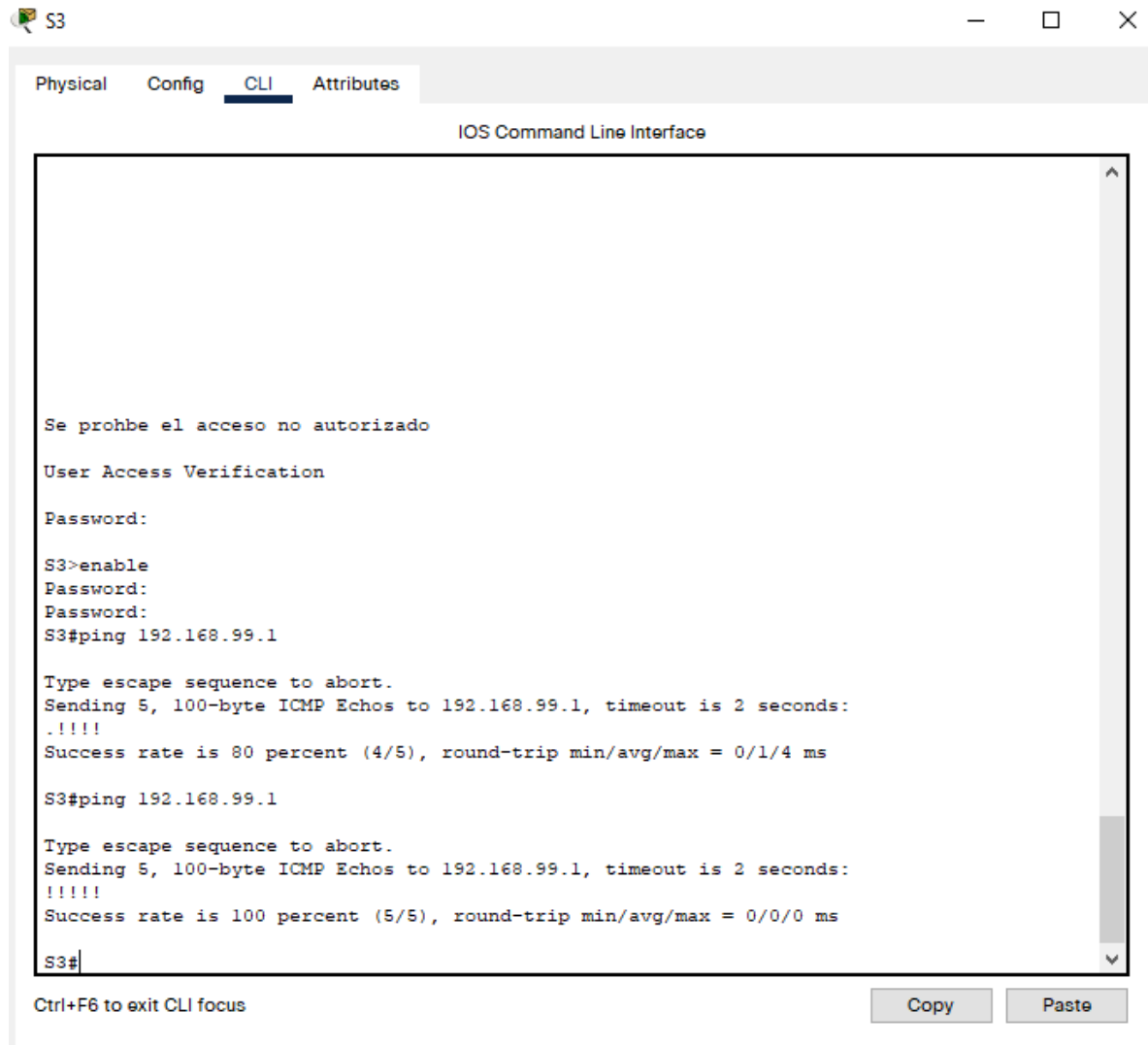
S3#ping 192.168.21.1

Figura 37. Verificación de la conectividad de la red desde S1 a R1 VLAN 99



Fuente: Elaboración propia.

Figura 38. Verificación de la conectividad de la red desde S3 a R1 VLAN 99.



```
Physical  Config  CLI  Attributes
IOS Command Line Interface

Se prohbe el acceso no autorizado
User Access Verification
Password:
S3>enable
Password:
Password:
S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/1/4 ms

S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

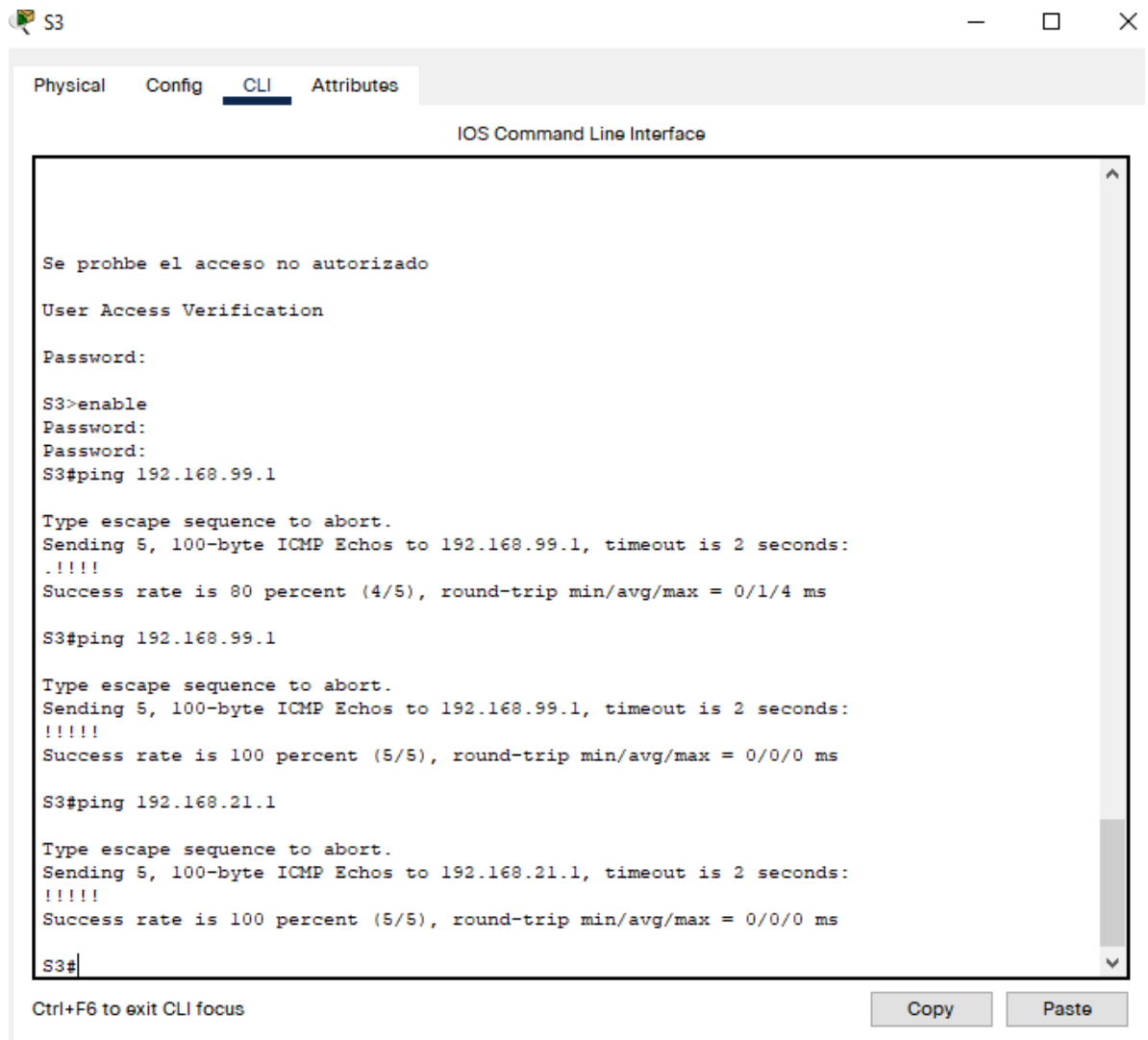
S3#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Fuente: Elaboración propia.

Figura 39. Verificación de la conectividad de la red desde S3 a R1 VLAN 21.



The screenshot shows a network device's CLI interface with the following text:

```
Physical Config CLI Attributes
IOS Command Line Interface

Se prohbe el acceso no autorizado
User Access Verification
Password:
S3>enable
Password:
Password:
S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/1/4 ms

S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

S3#ping 192.168.21.1

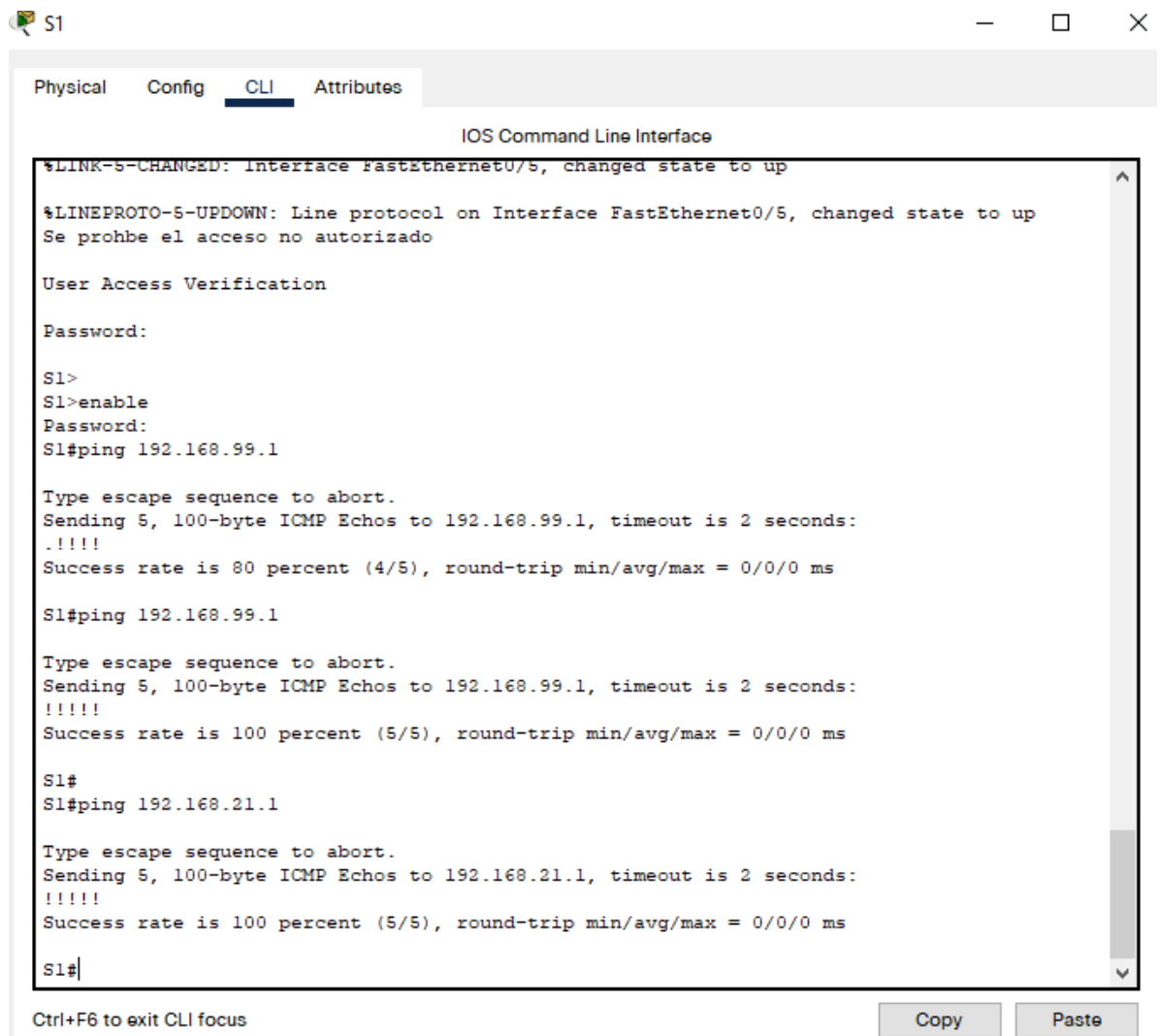
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

S3#
```

At the bottom of the window, there is a status bar with the text "Ctrl+F6 to exit CLI focus" and two buttons labeled "Copy" and "Paste".

Fuente: Elaboración propia.

Figura 40. Verificación de la conectividad de la red desde S1 a R1 VLAN 21



The screenshot shows a terminal window titled "S1" with tabs for "Physical", "Config", "CLI", and "Attributes". The active tab is "CLI", displaying the "IOS Command Line Interface". The terminal output shows the following sequence of commands and responses:

```
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
Se prohbe el acceso no autorizado

User Access Verification

Password:

S1>
S1>enable
Password:
S1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

S1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

S1#
S1#ping 192.168.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

S1#
```

At the bottom of the window, there is a status bar with "Ctrl+F6 to exit CLI focus" on the left and "Copy" and "Paste" buttons on the right.

Fuente: Elaboración propia.

Parte 4: Configurar el protocolo de routing OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18. Configurar OSPF en el R1.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	Router ospf 1
Anunciar las redes conectadas directamente	network 172.16.1.0 network 192.168.21.0 network 192.168.23.0 network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	passive-interface g0/1.21 passive-interface g0/1.23 passive-interface g0/1.99
Desactive la sumarización automática	no auto-summary

- Código para configurar el OSPF

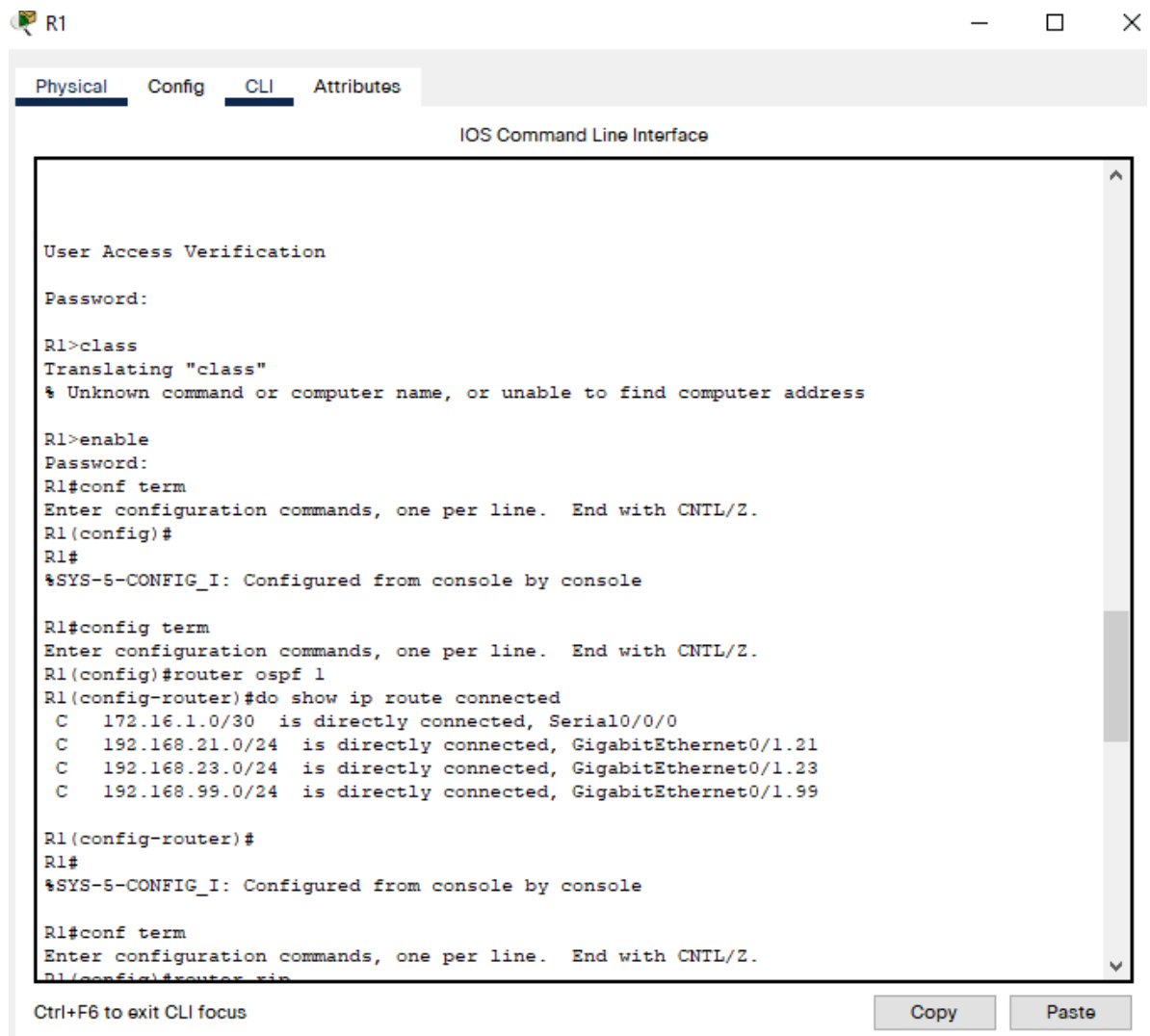
```
R1(config)#router ospf 1
R1(config-router)#do show ip route connected
C 172.16.1.0/30 is directly connected, Serial0/0/0
C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21
C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23
C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99

R1(config-router)#network 172.16.1.0
R1(config-router)#network 192.168.21.0
R1(config-router)#network 192.168.23.0
R1(config-router)#network 192.168.99.0

R1(config-router)#passive-interface g0/1.21

R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
R1(config-router)#no auto-summary
R1(config-router)#
```

Figura 41. Configuración OSPF R1.



The screenshot shows a window titled "R1" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following sequence of commands and responses:

```
User Access Verification

Password:

R1>class
Translating "class"
% Unknown command or computer name, or unable to find computer address

R1>enable
Password:
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#config term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#do show ip route connected
C 172.16.1.0/30 is directly connected, Serial0/0/0
C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21
C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23
C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99

R1(config-router)#
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
```

At the bottom of the window, there is a "Ctrl+F6 to exit CLI focus" message and two buttons labeled "Copy" and "Paste".

Fuente: Elaboración propia.

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 19. Configurar OSPF en el R2.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	Router ospf 1
Anunciar las redes conectadas directamente	network 10.10.10.10 network 172.16.1.0 network 172.16.2.0 Nota: Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	passive-interface loopback 0
Desactive la sumarización automática.	no auto-summary

- Código utilizado para configurar el OSPF

```
R2#conf term
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R2(config)#router ospf 1
```

```
R2(config-router)#do show ip route connected
```

```
C 10.10.10.10/32 is directly connected, Loopback0
```

```
C 172.16.1.0/30 is directly connected, Serial0/0/0
```

```
C 172.16.2.0/30 is directly connected, Serial0/0/1
```

```
C 209.165.200.232/29 is directly connected, GigabitEthernet0/0
```

```
R2(config-router)#network 10.10.10.10
```

```
R2(config-router)#network 172.16.1.0
```

```
R2(config-router)#network 172.16.2.0
```

```
R2(config-router)#passive-interface loopback 0
```

```
R2(config-router)#no auto-summary
```

Figura 42. Configuración OSPF R2.

```

R2(config-router)#do show ip route connected
C 10.10.10.10/32 is directly connected, Loopback0
C 172.16.1.0/30 is directly connected, Serial0/0/0
C 172.16.2.0/30 is directly connected, Serial0/0/1
C 209.165.200.232/29 is directly connected, GigabitEthernet0/0

R2(config-router)#network 10.10.10.10
R2(config-router)#network 172.16.1.0
R2(config-router)#network 172.16.2.0
R2(config-router)#passive-interface loopback 0
R2(config-router)#no auto-summary
R2(config-router)#
R2#
%SYS-5-CONFIG_I: Configured from console by console
    
```

Ctrl+F6 to exit CLI focus

Copy Paste

Fuente: Elaboración propia.

Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 20. Configurar OSPFv3 en el R2.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	Router ospf 1
Anunciar redes IPv4 conectadas directamente	C 172.16.2.0/30 is directly connected, Serial0/0/1 C 192.168.4.0/24 is directly connected, Loopback4 C 192.168.5.0/24 is directly connected, Loopback5 C 192.168.6.0/24 is directly connected, Loopback6
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	passive-interface loopback 4 passive-interface loopback 5 passive-interface loopback 6
Desactive la sumarización automática.	no auto-summary

- Código para la configuración del OSPF.

```
R3(config)#router ospf 1
```

```
R3(config-router)#do show ip route connected  
C 172.16.2.0/30 is directly connected, Serial0/0/1  
C 192.168.4.0/24 is directly connected, Loopback4  
C 192.168.5.0/24 is directly connected, Loopback5  
C 192.168.6.0/24 is directly connected, Loopback6
```

```
R3(config-router)#network 172.16.2.0  
R3(config-router)#network 192.168.4.0  
R3(config-router)#network 192.168.5.0  
R3(config-router)#network 192.168.6.0  
R3(config-router)#passive-interface loopback 4  
R3(config-router)#passive-interface loopback 5  
R3(config-router)#passive-interface loopback 6  
R3(config-router)#no auto-summary
```

Figura 43. Configuración OSPFv3 en el R2.

```
R3(config-router)#do show ip route connected  
C 172.16.2.0/30 is directly connected, Serial0/0/1  
C 192.168.4.0/24 is directly connected, Loopback4  
C 192.168.5.0/24 is directly connected, Loopback5  
C 192.168.6.0/24 is directly connected, Loopback6  
  
R3(config-router)#network 172.16.2.0|  
R3(config-router)#network 192.168.4.0  
R3(config-router)#network 192.168.5.0  
R3(config-router)#network 192.168.6.0  
R3(config-router)#passive-interface loopback 4  
R3(config-router)#passive-interface loopback 5  
R3(config-router)#passive-interface loopback 6  
R3(config-router)#no auto-summary  
R3(config-router)#
```

Ctrl+F6 to exit CLI focus

Copy

Paste

Fuente: Elaboración propia.

Paso 4: Verificar la información de OSPF

Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 21. Verificar la información de OSPF.

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Show ip protocols
¿Qué comando muestra solo las rutas OSPF?	Show ip router OSPF 1
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Show run y después ir a la sección.

Parte 5: Implementar DHCP y NAT para IPv4

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

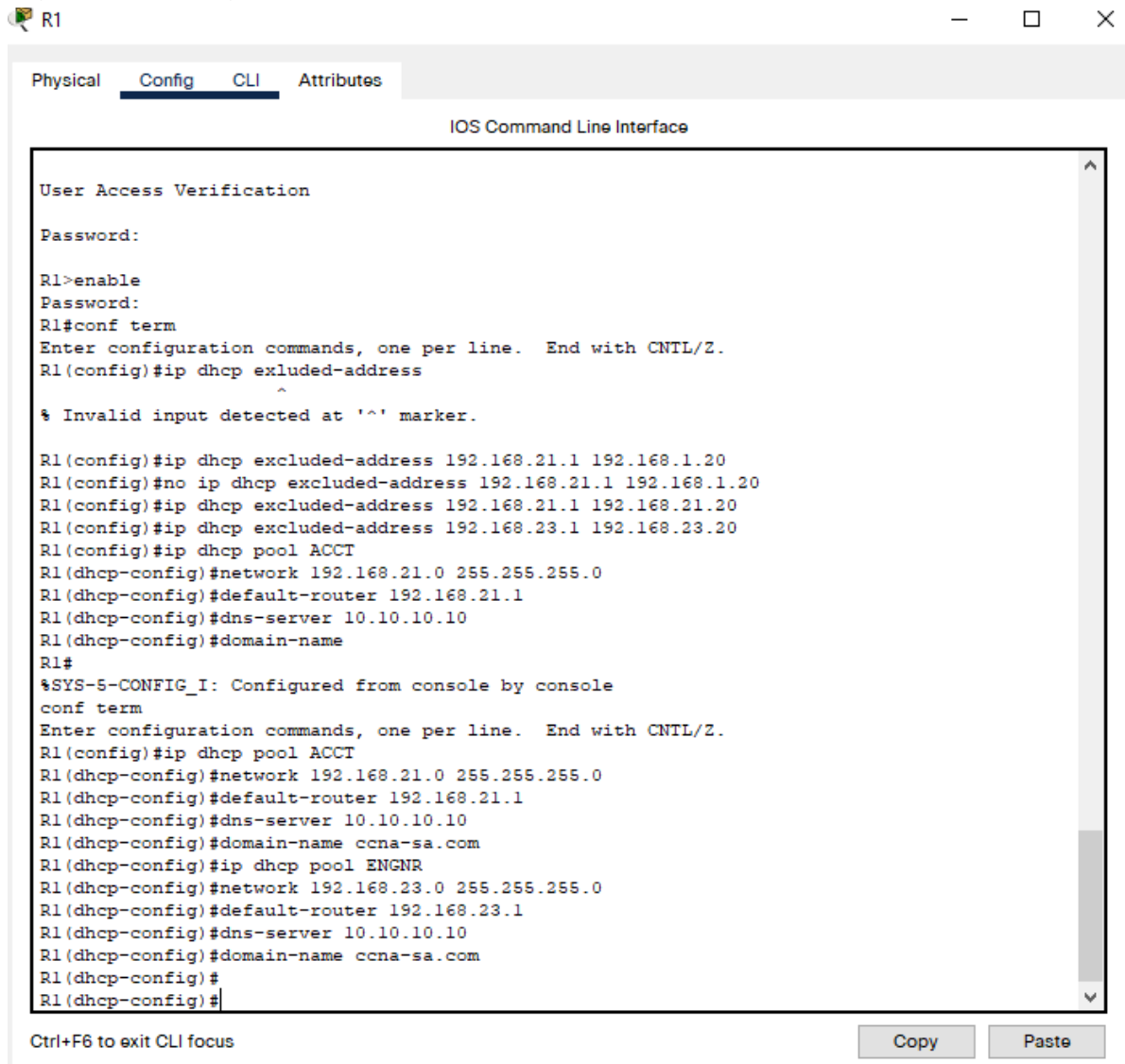
Tabla 22. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23.

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado
Crear un pool de DHCP para la VLAN 23	Nombre: ENGR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

- Código para la configuración de DHCP

```
R1>enable
Password:
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.1.20
R1(config)#no ip dhcp excluded-address 192.168.21.1 192.168.1.20
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name
R1#
%SYS-5-CONFIG_I: Configured from console by console
conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#ip dhcp pool ENGNR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
```

Figura 44. Configuración DHCP en R1.



The screenshot shows the IOS Command Line Interface for router R1. The interface has tabs for Physical, Config, CLI, and Attributes, with CLI selected. The terminal output shows the following sequence of commands and responses:

```
User Access Verification
Password:
R1>enable
Password:
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp excluded-address
      ^
% Invalid input detected at '^' marker.

R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.1.20
R1(config)#no ip dhcp excluded-address 192.168.21.1 192.168.1.20
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name
R1#
%SYS-5-CONFIG_I: Configured from console by console
conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#ip dhcp pool ENGR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#
R1(dhcp-config)#
```

At the bottom of the window, there is a status bar with the text "Ctrl+F6 to exit CLI focus" and two buttons labeled "Copy" and "Paste".

Fuente: Elaboración propia.

Paso 2: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 23. Configurar la NAT estática y dinámica en el R2.

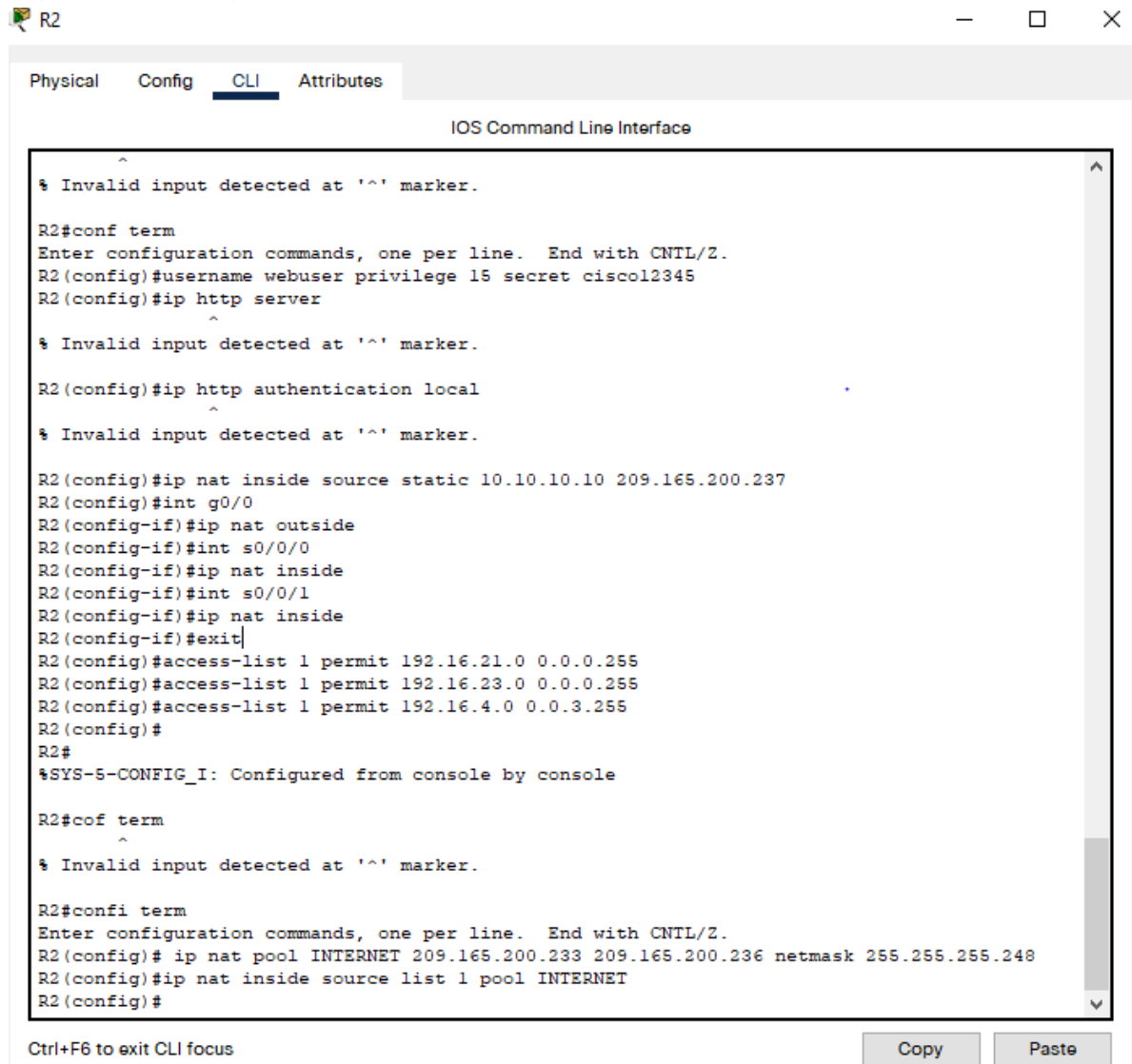
Elemento o tarea de configuración	Especificación
Crear una base de datos local con unacuenta de usuario	Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15
Habilitar el servicio del servidor HTTP	ip http server
Configurar el servidor HTTP para utilizar labase de datos local para la autenticación	ip http authentication local
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.237 ip nat inside source static 10.10.10.10 209.165.200.237
Asignar la interfaz interna y externa para laNAT estática	int g0/0 ip nat outside int s0/0/0 ip nat inside int s0/0/1 ip nat inside
Configurar la NAT dinámica dentro de unaACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y delIngeniería en el R1 Permitir la traducción de un resumen de las redes LAN(loopback) en el R3
Defina el pool de direcciones IP públicasutilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228
Definir la traducción de NAT dinámica	ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248

- Código para la configuración de DHCP R2.

```
R2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#username webuser privilege 15 secret cisco12345
R2(config)#ip http authentication local
^
% Invalid input detected at '^' marker.
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
R2(config)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)#int s0/0/0
R2(config-if)#ip nat inside
R2(config-if)#int s0/0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#access-list 1 permit 192.16.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.16.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.16.4.0 0.0.3.255
R2(config)#
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#cof term
^
% Invalid input detected at '^' marker.
R2#confi term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)# ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask
255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
```

Figura 45. Configuración DHCP en R2.



The screenshot shows the CLI interface of a Cisco router (R2) with the following configuration steps:

```
R2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#username webuser privilege 15 secret cisco12345
R2(config)#ip http server
^
% Invalid input detected at '^' marker.
R2(config)#ip http authentication local
^
% Invalid input detected at '^' marker.
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
R2(config)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)#int s0/0/0
R2(config-if)#ip nat inside
R2(config-if)#int s0/0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#access-list 1 permit 192.16.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.16.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.16.4.0 0.0.3.255
R2(config)#
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#cof term
^
% Invalid input detected at '^' marker.
R2#confi term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)# ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#
```

At the bottom of the window, there is a status bar with the text "Ctrl+F6 to exit CLI focus" and two buttons: "Copy" and "Paste".

Fuente: Elaboración propia.

Paso 3: Verificar el protocolo DHCP y la NAT estática

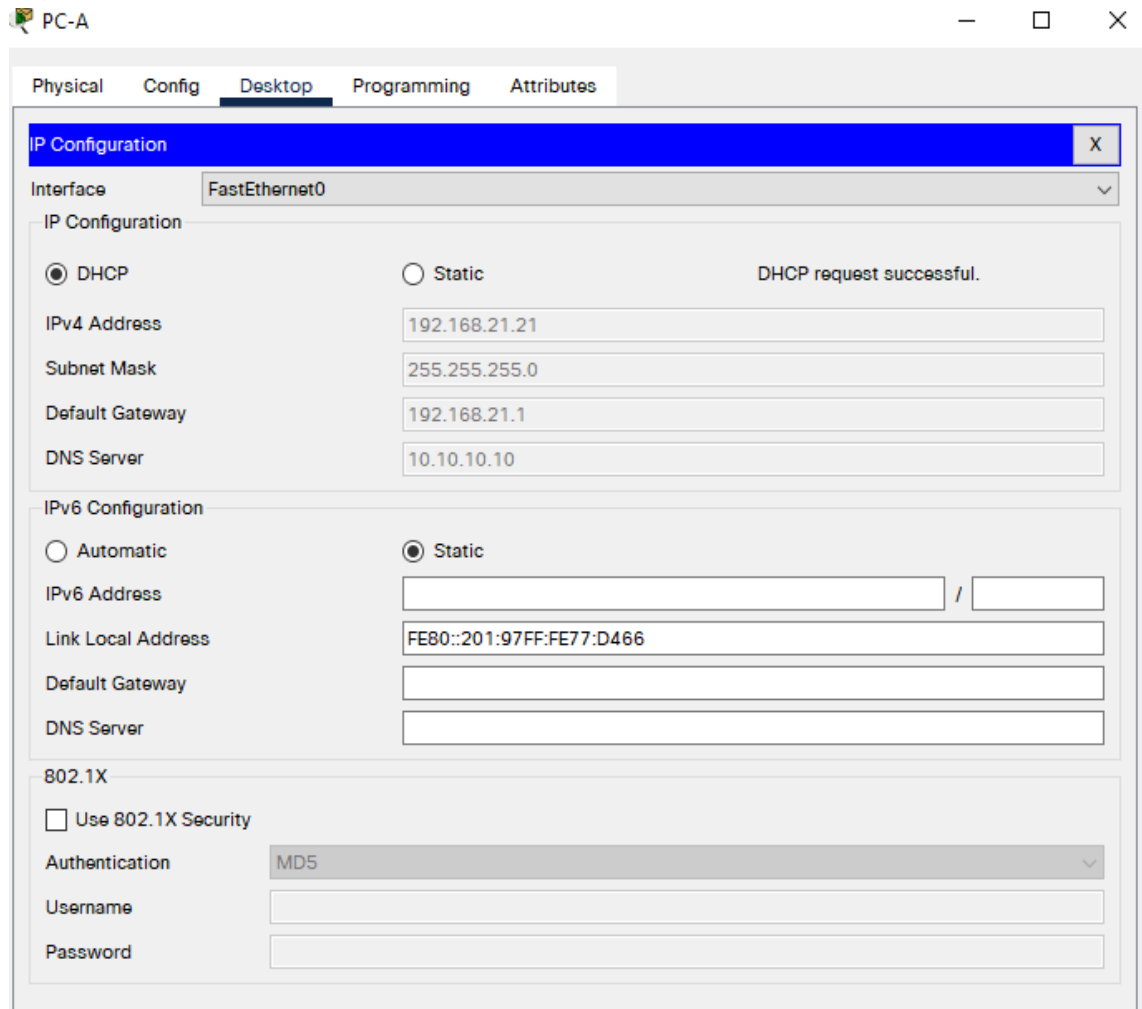
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 24. Verificar el protocolo DHCP y la NAT estática.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Exitoso
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	Fallido Ya que packet tracer no soporta este comando.

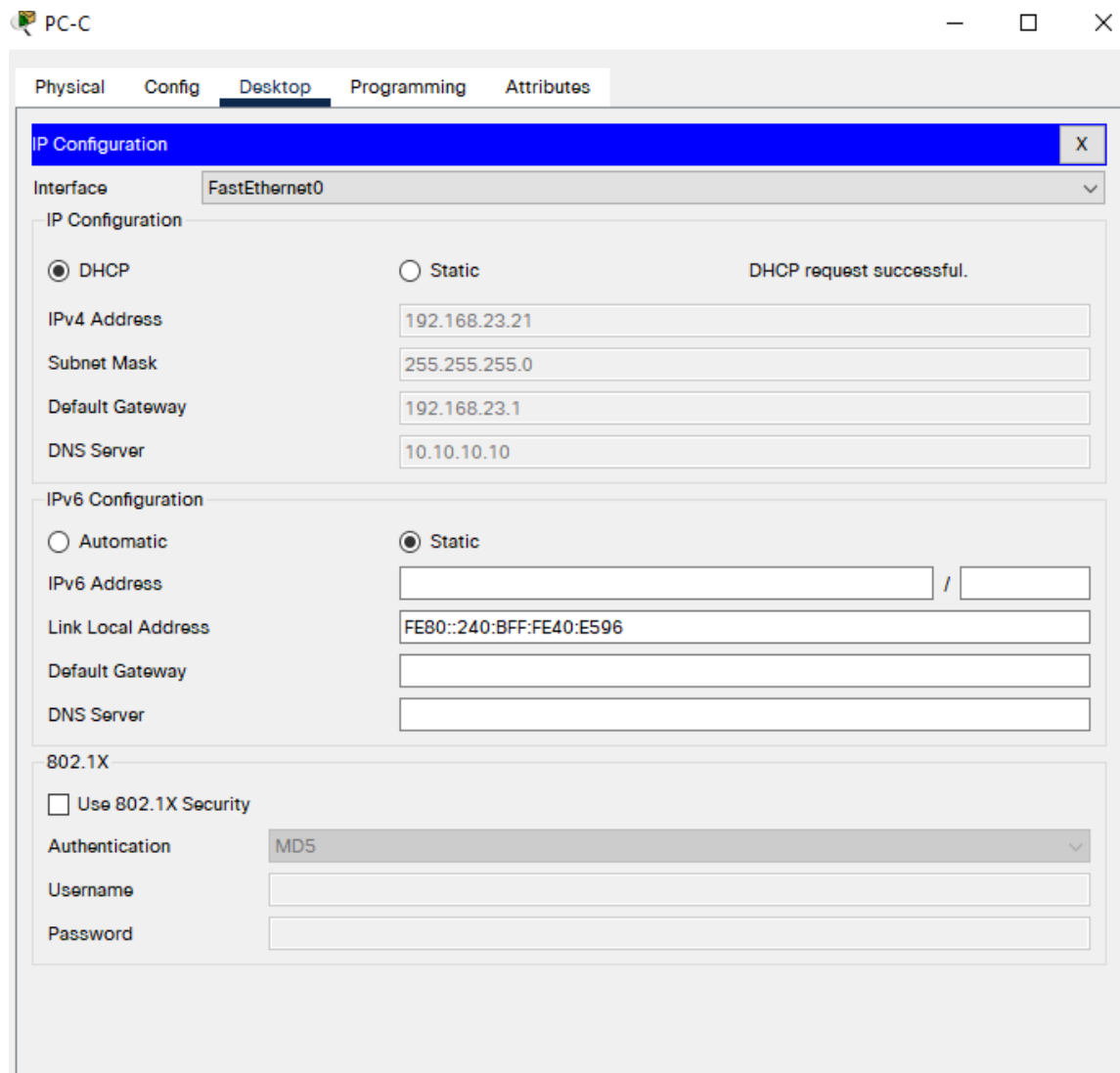
A continuación, las figuras donde se muestra la evidencia de las conexiones:

Figura 46. Verificación protocolo DHCP en Pc A.



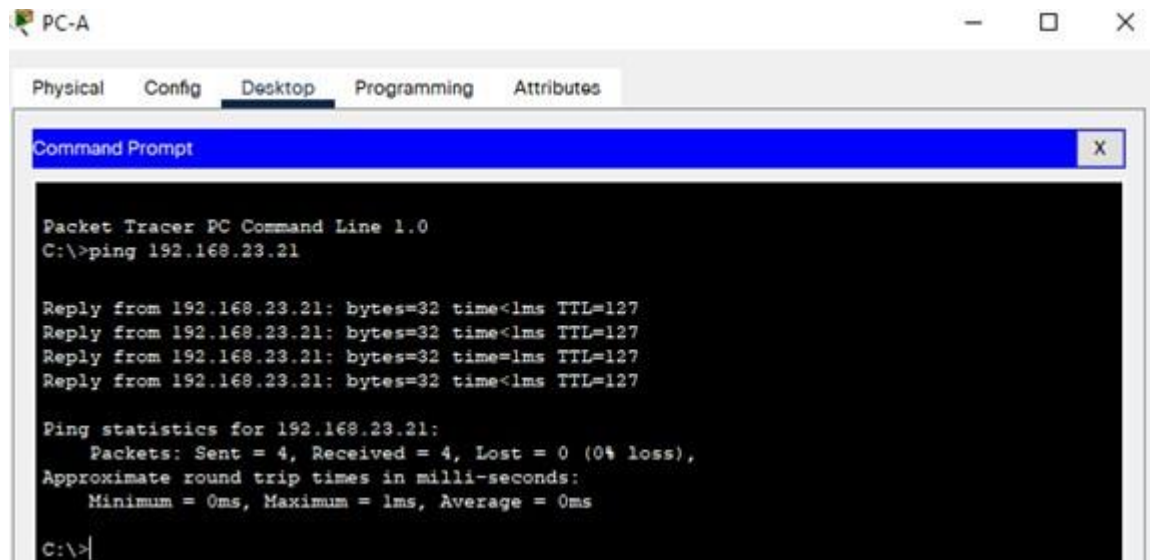
Fuente Elaboración propia.

Figura 47. Verificación protocolo DHCP en Pc C.



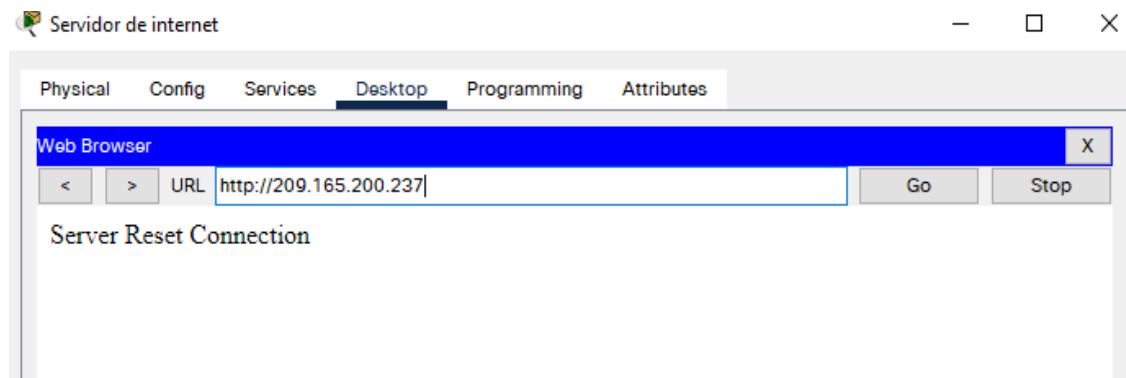
Fuente: Elaboración propia.

Figura 48. Verificación protocolo DHCP en Pc A a Pc C.



Fuente: Elaboración propia.

Figura 49. Verificación protocolo DHCP en un buscador.



Fuente: Elaboración propia.

Parte 6: Configurar NTP

Tabla 25. Configurar NTP.

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	5 de marzo de 2016, 9 a. m.
Configure R2 como un maestro NTP.	Nivel de estrato: 5 No se soporta este comando.
Configurar R1 como un cliente NTP.	Servidor: R2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	ntp server 172.16.1.2
Verifique la configuración de NTP en R1.	show ntp associations

Figura 50. Configuración ntp R2.

```
Se prohíbe personal no autorizado
User Access Verification

Password:

R2>enable
Password:
R2#clock set 09:00:00 march 5 2016
R2#ntp master 5
^
% Invalid input detected at '^' marker.

R2#
```

Ctrl+F6 to exit CLI focus

Copy

Paste

Fuente: Elaboración propia.

Figura 51. Configuración ntp R1.

```
R1>enable
Password:
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp server 172.16.1.2
R1(config)#ntp update-calendar
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ntp associations

address          ref clock      st  when    poll  reach  delay      offset
disp
~172.16.1.2      .INIT.         16  -       64    0      0.00       0.00
0.12
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R1#
```

Ctrl+F6 to exit CLI focus Copy Paste

Fuente: Elaboración propia.

Parte 7: Configurar y verificar las listas de control de acceso (ACL)

Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 26. Restringir el acceso a las líneas VTY en el R2.

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1establezca una conexión Telnet con R2	Nombre de la ACL: ADMIN-MGT
Aplicar la ACL con nombre a las líneas VTY	access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	transport input telnet
Verificar que la ACL funcione como se espera	telnet 172.16.1.2

- Configurar y verificar las listas de control de acceso

```
R2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit
% Incomplete command.
R2(config-std-nacl)#permit host 172.16.1.1
```

```

R2(config-std-nacl)#exit
R2(config)#line vty 0 15
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#transport input telnet

R1>enable
Password:
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenSe prohíbe personal no autorizado
User Access Verification
Password:
R2>exit
[Connection to 172.16.1.2 closed by foreign host]

```

Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 27. Introducir el comando de CLI adecuado.

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	show access-list
Restablecer los contadores de una lista de acceso	clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Show ip interface
¿Con qué comando se muestran las traducciones NAT?	show ip nat translations Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?

clear ip nat translation *

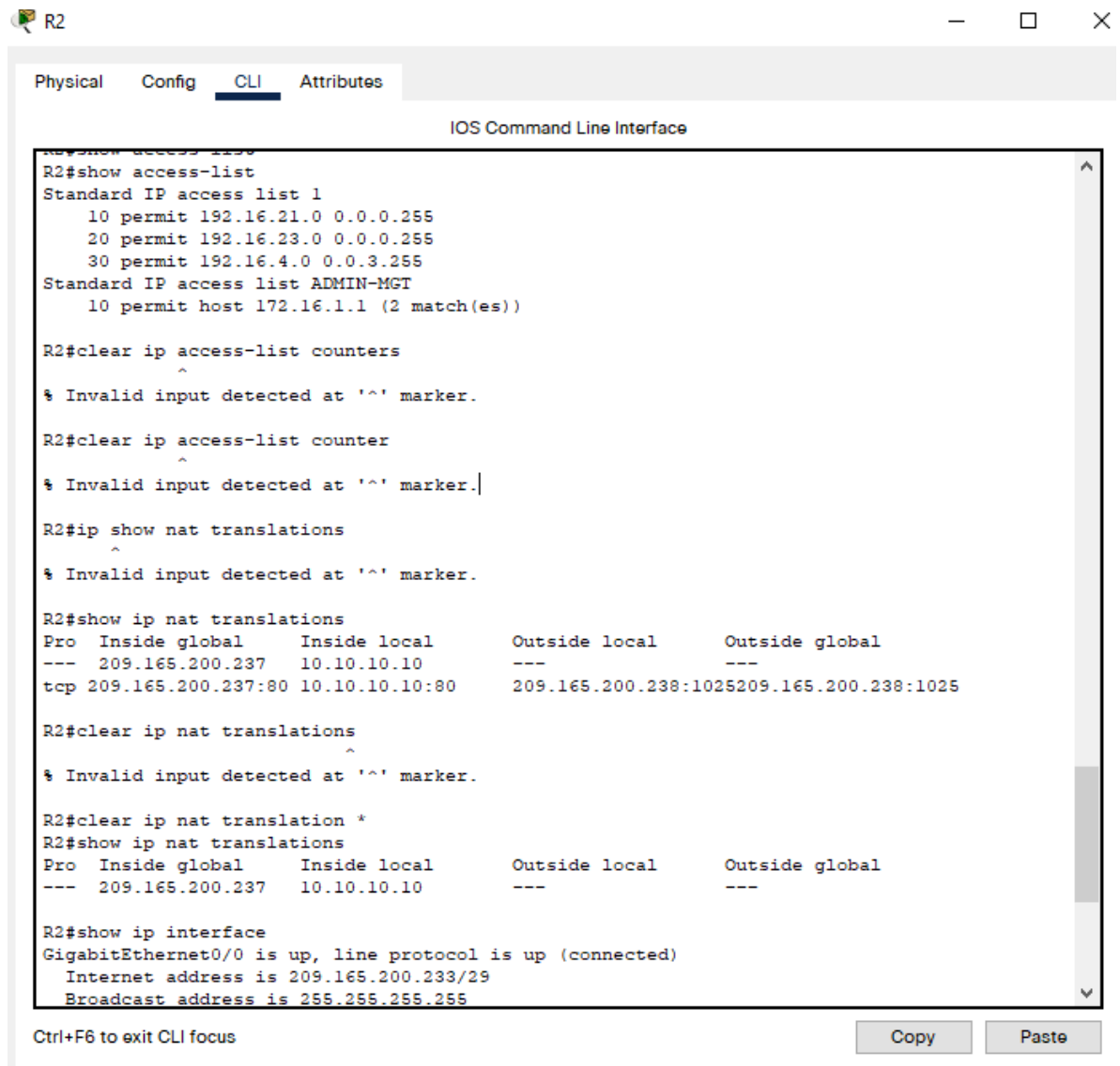
- Código para comandos CLI

```
R2#show access list
R2#show access-list
Standard IP access list 1
10 permit 192.16.21.0 0.0.0.255
20 permit 192.16.23.0 0.0.0.255
30 permit 192.16.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
10 permit host 172.16.1.1 (2 match(es))

R2#clear ip access-list counters
^
% Invalid input detected at '^' marker.
R2#clear ip access-list counter
^
% Invalid input detected at '^' marker.
R2#ip show nat translations
^
% Invalid input detected at '^' marker.
R2#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.237 10.10.10.10 --- ---
tcp 209.165.200.237:80 10.10.10.10:80
209.165.200.238:1025 209.165.200.238:1025
R2#clear ip nat translations
^
% Invalid input detected at '^' marker.
R2#clear ip nat translation *
R2#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.237 10.10.10.10 --- ---
R2#show ip interface
GigabitEthernet0/0 is up, line protocol is up (connected)
Internet address is 209.165.200.233/29
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 not set
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
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled

Figura 52. Configuración ntp R2.



The screenshot shows the CLI interface of a router named R2. The interface has tabs for Physical, Config, CLI (selected), and Attributes. The main window displays the following commands and their outputs:

```
R2#show access-list
Standard IP access list 1
 10 permit 192.16.21.0 0.0.0.255
 20 permit 192.16.23.0 0.0.0.255
 30 permit 192.16.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
 10 permit host 172.16.1.1 (2 match(es))

R2#clear ip access-list counters
^
% Invalid input detected at '^' marker.

R2#clear ip access-list counter
^
% Invalid input detected at '^' marker.

R2#ip show nat translations
^
% Invalid input detected at '^' marker.

R2#show ip nat translations
Pro  Inside global   Inside local   Outside local   Outside global
---  209.165.200.237   10.10.10.10    ---             ---
tcp  209.165.200.237:80 10.10.10.10:80 209.165.200.238:1025 209.165.200.238:1025

R2#clear ip nat translations
^
% Invalid input detected at '^' marker.

R2#clear ip nat translation *
R2#show ip nat translations
Pro  Inside global   Inside local   Outside local   Outside global
---  209.165.200.237   10.10.10.10    ---             ---

R2#show ip interface
GigabitEthernet0/0 is up, line protocol is up (connected)
 Internet address is 209.165.200.233/29
 Broadcast address is 255.255.255.255
```

At the bottom of the window, there is a prompt "Ctrl+F6 to exit CLI focus" and two buttons: "Copy" and "Paste".

Fuente: Elaboración propia.

CONCLUSIONES

Se documentó el desarrollo de dos escenarios paso a paso acompañado con su respectiva evidencia del proceso realizado en cada uno de los dispositivos de la red, realizando pruebas de conectividad donde el resultado fue satisfactorio.

Se logró hallar la solución para cada uno de las actividades del diplomado Evaluación-prueba de habilidades prácticas CCNA como trabajo final, mediante la implementación y uso de los conocimientos adquiridos en los módulos para los escenarios con diferentes topologías.

Se adquirió el conocimiento necesario para realizar la configuración básica y de seguridad de diferentes dispositivos en el simulador Packet Tracer con el uso de diferentes comandos, códigos y tipografías que permitieron el aprendizaje de este.

Finalmente, se implementó los diferentes comandos que permiten a los dispositivos y las redes un nivel de seguridad suficiente para que no sean vulnerados por agentes externos.

BIBLIOGRAFÍA

Configuración de VLAN [Comandos]» CCNA desde Cero. (2020, junio 10). CCNA desde Cero. <https://ccnadesdecero.es/configuracion-vlan/>

Configurar EtherChannel» CCNA desde Cero. (2020, junio 13). CCNA desde Cero. <https://ccnadesdecero.es/configurar-etherchannel/>

CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1>

CISCO. (2017). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1>

CISCO. (2017). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1>

CISCO. (2017). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://staticcourseassets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1>

Rodrigo. Conexiones telnet y configuración de contraseñas. {En línea}. {03 de marzo de 2012}. Disponible en: <https://todopacketracer.com/2011/06/21/conexionestelnet-y-configuracion-de-contrasenas/>

ROSALES, Delfi. Configuraciones Básicas de un Router o Switch Cisco. {En línea}. Disponible en: <https://delfirosales.blogspot.com/2011/02/configuraciones-basicasde-un-router-o.html>