

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

JHON ALEXANDER ARAQUE CONTRERAS

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

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

JHON ALEXANDER ARAQUE CONTRERAS

Diplomado de opción de grado presentado para optar el  
título de INGENIERO DE SISTEMAS

DIRECTOR:  
MSc. NANCY AMPARO GUACA GIRON

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

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

---

Firma del Presidente del Jurado

---

Firma del Jurado

---

Firma del Jurado

Pamplona, 1 diciembre de 2021

## **AGRADECIMIENTOS**

Mi agradecimiento a Dios, mi madre y la Universidad Nacional Abierta y a Distancia, institución en la cual estudio, que me brindó la oportunidad a través del Programa de Ingeniería de Sistemas, para realizar mis estudios de pregrado en la que he recibido apoyo.

Al MSc. Nancy Amparo Guaca

Directora del Diplomado de Profundización en CCNA CISCO

Por su cotutoria en trabajos académicos y brindarme su valioso tiempo.

Al Ing. Raúl Barreño Gutiérrez

Tutor del Diplomado de Profundización en CCNA CISCO

Por sus valiosas asesorías y comentarios.

Al Ps. Nidia Yasmin Duque Barajas

Directora de CCAV Pamplona

Por brindarme su apoyo incondicional en todo momento.

En general, a todas las instituciones, organismos, archivos, bibliotecas, que de alguna manera contribuyeron a facilitarme acceso a la información requerida para alcanzar los objetivos trazados del diplomado.

En especial a Dios, mi madre y la Universidad Nacional Abierta y a Distancia de los cuales siempre recibí su apoyo.

Finalmente, a todas aquellas personas, colegas y amigos que me brindaron su apoyo, tiempo e información para el logro de mis objetivos.

## CONTENIDO

|                        |    |
|------------------------|----|
| AGRADECIMIENTOS.....   | 4  |
| CONTENIDO .....        | 5  |
| LISTA DE TABLAS .....  | 6  |
| LISTA DE FIGURAS ..... | 7  |
| GLOSARIO .....         | 10 |
| RESUMEN.....           | 11 |
| ABSTRACT.....          | 12 |
| INTRODUCCIÓN .....     | 13 |
| DESARROLLO .....       | 14 |
| 1. Escenario 1 .....   | 14 |
| 2. Escenario 2 .....   | 24 |
| CONCLUSIONES .....     | 64 |
| BIBLIOGRAFÍA.....      | 65 |

## LISTA DE TABLAS

|  |    |
|--|----|
| Tabla 1. Tabla de direccionamiento IP .....            | 15 |
| Tabla 2. Tabla de LANs.....                            | 15 |
| Tabla 3. Tabla direcciones del Servidor .....          | 29 |
| Tabla 4. Tabla de Conectividad Routers .....           | 40 |
| Tabla 5. Tabla de Conectividad Routers y Switchs ..... | 47 |

## LISTA DE FIGURAS

|   |    |
|---|----|
| Figura 1. Escenario 1 .....                           | 14 |
| Figura 2. Simulación de Escenario 1 .....             | 15 |
| Figura 3. Configuración R1 .....                      | 17 |
| Figura 4. Configuración interfaces.....               | 18 |
| Figura 5. Configuración S1 .....                      | 20 |
| Figura 6. Configuración VLAN.....                     | 20 |
| Figura 7. Configuración de los equipos host PC-A..... | 21 |
| Figura 8. Visualización direcciones IP PC-A .....     | 21 |
| Figura 9. Configuración de los equipos host PC-B..... | 22 |
| Figura 10. Visualización direcciones IP PC-B .....    | 22 |
| Figura 11. Conectividad PC-B-PC-A .....               | 23 |
| Figura 12. Conectividad PC-A-PC-B .....               | 23 |
| Figura 13. Verificación de interfaces R1.....         | 24 |
| Figura 14. Escenario 2 .....                          | 25 |
| Figura 15. Simulación de Escenario 2.....             | 26 |
| Figura 16. Reiniciar Configuración .....              | 27 |
| Figura 17. Eliminar VLAN.....                         | 28 |
| Figura 18. VLAN.....                                  | 28 |
| Figura 19. Asignación direcciones Servidor Web .....  | 29 |
| Figura 20. Configuración básica de R1 .....           | 31 |
| Figura 21. Configuración básica de R2 .....           | 33 |
| Figura 22. Configuración interfaces R2 .....          | 34 |

|   |    |
|---|----|
| Figura 23. Configuración Loopbacks R2 ..... | 34 |
| Figura 25. Configuración Loopbacks R3 ..... | 37 |
| Figura 26. Configuración S1 .....           | 38 |
| Figura 27. Configuración S3.....            | 40 |
| Figura 28. Conectividad R1-R2 .....         | 41 |
| Figura 29. Conectividad R2-R3 .....         | 41 |
| Figura 30. Conectividad Servidor .....      | 42 |
| Figura 31. Configuración Trunk S1.....      | 44 |
| Figura 32. Configuración Trunk S3.....      | 46 |
| Figura 33. Configuración Subinterfaz .....  | 47 |
| Figura 34. Conectividad S1-R1 .....         | 48 |
| Figura 36. Conectividad R1-S1 .....         | 49 |
| Figura 37. Conectividad R1-S3 .....         | 50 |
| Figura 38. Configuración OSPF en R1 .....   | 51 |
| Figura 39. Configurar OSPF en R2 .....      | 52 |
| Figura 40. Configuración OSPFv3 en R3 ..... | 53 |
| Figura 41. Ver IP Protocolos .....          | 54 |
| Figura 42. Ver IP Routers.....              | 54 |
| Figura 43. Ver OSPF .....                   | 55 |
| Figura 44. Configuración DHCP .....         | 56 |
| Figura 45. NAT .....                        | 58 |
| Figura 46. DHCP PC-A .....                  | 58 |
| Figura 47. DHCP PC-B .....                  | 59 |
| Figura 49. NTP .....                        | 60 |

|  |    |
|--|----|
| Figura 51. Acceso verificación.....      | 62 |
| Figura 52. Verificación ACL.....         | 63 |
| Figura 53. Verificación interfaces ..... | 63 |

## GLOSARIO

**Conectividad:** Es la capacidad de un dispositivo de ordenador personal, periférico, PDA, móvil, robot, electrodoméstico, automóvil de conectarse y comunicarse con otro, con el fin de intercambiar información o establecer una conexión directa a base de información digital.

**Conmutación:** Son los que permite establecer un camino entre dos puntos, un transmisor y un receptor a través de equipos de transmisión para trasladar los datos de un nodo al otro hasta alcanzar el destino final entran a la red conmutada y se encaminan hasta la estación de destino conmutándolos de nodo en nodo

**Direccionamiento:** Especifica la forma de calcular las direcciones IP de memoria efectiva de un operando mediante el uso de la información contenida en registros y/o constantes, contenida dentro de una instrucción de la máquina o en otra parte.

**Enrutamiento:** Es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad. Dado que se trata de encontrar la mejor ruta posible, lo primero será definir qué se entiende por mejor ruta y en consecuencia cuál es la métrica que se debe utilizar para medirla.

**Topología:** Mapa físico o lógico de una red para intercambiar datos en otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico como conjunto de nodos interconectados en nodos del punto en el que la curva se intercepta a sí misma que concretamente depende del tipo de red en cuestión.

## **RESUMEN**

El desarrollo de este trabajo trata de identificar los conceptos adquiridos en el Diplomado CISCO, que articula la estrategia de construir redes de comunicación con el simulador Packet Tracer en la Gestión de Sistemas y Servicios de Telecomunicaciones en los protocolos de conectividad de internet de LAN y WAN donde se realiza el desarrollo los escenarios, cada uno con diferente tipología las cuales se crea en el simulador implementan diferentes topologías, en donde se diseña, configura e implementa una red eficaz y escalable para supervisar y solucionar problemas en los equipos electrónicos pertenecientes a la infraestructura con las diferentes funcionalidades por medio de la certificación CCNA; creando una redes compuestas por un Routers, Switch y PCs para realizar configuraciones de enrutamiento entre VLAN y DHCP requeridos por los dispositivos, que verifica por comandos en la configuración correcta para que la redes funcione como es solicitada que se realiza la seguridad de la red admita conectividad IPv4 e IPv6, generando routing entre VLAN, que cuente con el protocolos OSPF, DHCP, NAT, ACL y NTP.

Palabras Clave: CISCO, CCNA, Enrutamiento, Redes, Sistemas.

## **ABSTRACT**

The development of this work tries to identify the concepts acquired in the Diploma CISCO, which articulates the strategy of building communication networks with the Packet Tracer simulator in the Management of Telecommunications Systems and Services in the LAN and WAN internet connectivity protocols where The scenarios are developed, each one with a different typology which is created in the simulator and implements different topologies, where an efficient and scalable network is designed, configured and implemented to monitor and solve problems in the electronic equipment belonging to the infrastructure with the different functionalities through the CCNA certification; creating a network composed of routers, switches and PCs to perform routing configurations between VLAN and DHCP required by the devices, which verifies by commands in the correct configuration so that the network works as requested that the security of the networks is supported IPv4 and IPv6 connectivity, generating routing between VLANs, which has the OSPF, DHCP, NAT, ACL and NTP protocols.

Keywords: CISCO, CCNA, Routing, Networks, Systems.

## INTRODUCCIÓN

El presente trabajo académico administra la proyección de redes de comunicaciones mediante equipos y simuladores con sus respectivos protocolos de seguridad en los diferentes laboratorios cumplieron con el propósito de evidenciar lo aprendido identificando comandos básicos de configuración y comandos avanzados, detallando el paso a paso de cada una de las etapas realizadas soluciones integradas en las redes de área local y las redes de área mundial.

El Escenario 1 presenta una Topología con un Router un Switch y dos Computadores con la respectiva configuración de terminales para el manejo de codificación evidenciando los resultados de conectividad de redes.

El Escenario 2 presenta una Topología con tres Router, dos Switch y dos Computadores con la respectiva configuración de terminales para el manejo de codificación evidenciando resultados de comandos como ping, traceroute, show, IP, route, entre otros con su funcionalidad de la red con direcciones IPV4 y IPV6.

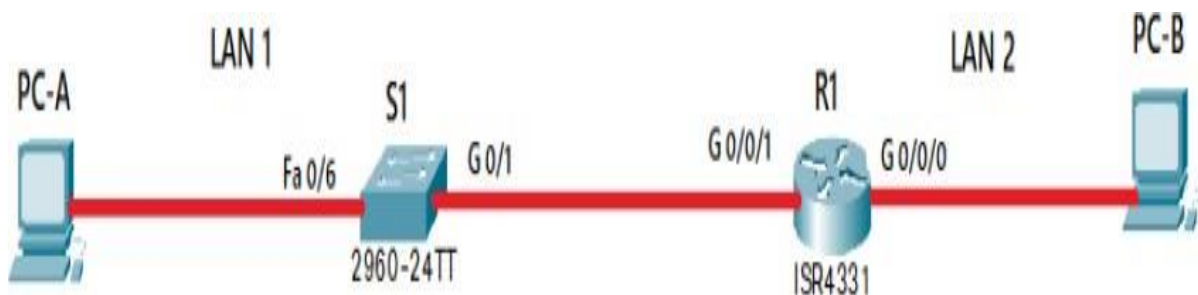
## DESARROLLO

### 1. 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.

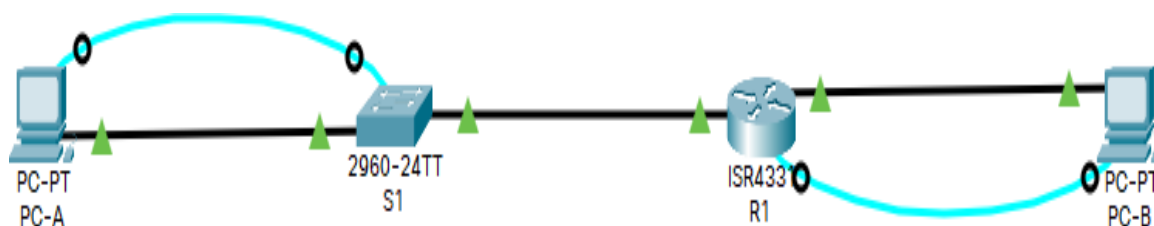
En el desarrollo del caso de estudio se implementa la topología mostrada en la figura y configura el Router R1 y el switch S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

Figura 1. Escenario 1



Fuente: Guía de actividades

Figura 2. Simulación de Escenario 1



Fuente: Elaboración propia

Tabla 1. Tabla de direccionamiento IP

| Item                              | Requerimiento      |
|-----------------------------------|--------------------|
| Dirección de Red                  | 192.168.19.0 /24   |
| Requerimiento de host Subred LAN1 | 192.168.19.0 /25   |
| Requerimiento de host Subred LAN2 | 192.168.19.128 /26 |
| R1 G0/0/0                         | 192.168.19.129 /26 |
| R1 G0/0/1                         | 192.168.19.1 /25   |
| S1 SVI                            | 192.168.19.2 /25   |
| PC-A                              | 192.168.19.126 /25 |
| PC-B                              | 192.168.19.190 /25 |

Fuente: Elaboración propia

Tabla 2. Tabla de LANs

| Subredes        | Dirección red  | Mascara         | IP Inicial     | IP Final       | # de salto |
|-----------------|----------------|-----------------|----------------|----------------|------------|
| LAN 1 = 100HOST | 192.168.19.0   | 255.255.255.128 | 192.168.19.1   | 192.168.19.126 | 128        |
| LAN 2 = 50 HOST | 192.168.19.128 | 255.255.255.192 | 192.168.19.129 | 192.168.19.190 | 64         |

Fuente: Elaboración propia

## Paso 1: Configurar los ajustes básicos R1

- Desactivar la búsqueda DNS  
Router(config)# no ip domain-lookup
- Nombre del router R1  
Router(config)#hostname R1
- Nombre de dominio ccna-lab.com  
R1(config)#ip domain-name ccna-lab.com
- Contraseña cifrada para el modo EXEC privilegiado  
R1(config)#enable secret ciscoenpass
- Contraseña de acceso a la consola  
R1(config)#line console 0  
R1(config-line)#password ciscoconpass  
R1(config-line)#login  
R1(config-line)#exit
- Establecer la longitud mínima para las contraseñas 10 caracteres  
R1(config)#security passwords min-length 10
- Crear un usuario administrativo en la base de datos local  
R1(config)#username admin password admin1pass I
- Configurar el inicio de sesión en las líneas VTY para que use la base de datos  
R1(config)#line vty 0 4  
R1(config-line)#password ciscocisco  
R1(config-line)#login local
- Configurar VTY solo aceptando SSH  
R1(config-line)# transport input ssh
- Cifrar las contraseñas de texto no cifrado  
R1(config)#service password-encryption

- Configurar un MOTD Banner

```
R1(config)#banner motd # personal autorizado de la UNAD #
```

- Configurar interfaz G0/0/0

```
R1(config)#int g0/0/0
R1(config-if)#ip address 192.168.19.129 255.255.255.192
R1(config-if)#description interfaz LAN2
R1(config-if)#no shutdown
```

- Configurar interfaz G0/0/1

```
R1(config)#int g0/0/1
R1(config-if)#ip address 192.168.19.1 255.255.255.128
R1(config-if)#description interfaz LAN1
R1(config-if)#no shutdown
```

- Generar una clave de cifrado RSA Módulo de 1024 bits

```
R1(config)#ip domain name ccna-lab.com
R1(config)#crypto key generate rsa
```

Figura 3. Configuración R1

```

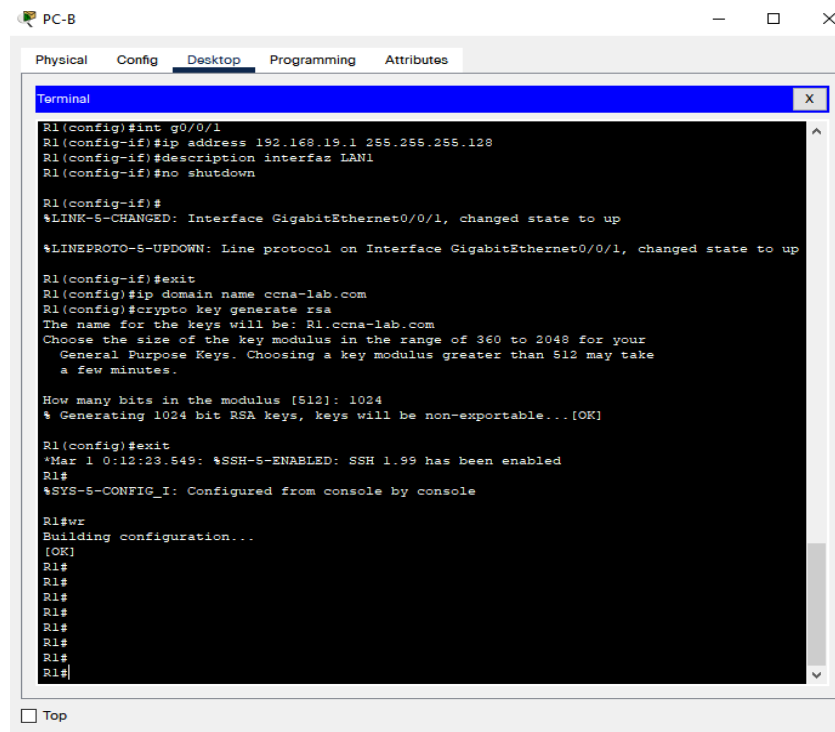
PC-B
Physical Config Desktop Programming Attributes
Terminal
Press RETURN to get started!

Router>enable
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#ho R1
R1(config)#ip domain-name ccna-lab.com
R1(config)#enable secret ciscoenpass
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit
R1(config)#security passwords min-length 10
R1(config)#username admin password adminpass
R1(config)#line vty 0 4
R1(config-line)#password ciscocisco
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd #Router de personal autorizado de la UNAD cualquier instruccion
tendra efectos legales de acuerdo a la ley#
R1(config)#int g0/0/0
R1(config-if)#ip address 192.168.19.129 255.255.255.192
R1(config-if)#description interfaz LAN2
R1(config-if)#no shutdown

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)#exit
  
```

Fuente: Elaboración propia

Figura 4. Configuración interfaces



```
PC-B
Physical Config Desktop Programming Attributes
Terminal
R1(config)#int g0/0/1
R1(config-if)#ip address 192.168.19.1 255.255.255.128
R1(config-if)#description interfaz LAN1
R1(config-if)#no shutdown

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)#exit
R1(config)#ip domain name ccna-lab.com
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)#exit
*Mar 1 0:12:23.549: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1#
%SYS-5-CONFIG_I: Configured from console by console

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

Fuente: Elaboración propia

## Paso 2: Configurar los ajustes básicos S1

- Desactivar la búsqueda DNS  
Switch(config)#no ip domain-lookup
- Nombre del switch S1  
Switch(config)#hostname S1
- Nombre de dominio ccna-lab.com  
S1(config)#ip domain-name ccna-lab.com
- Contraseña cifrada para el modo EXEC privilegiado  
S1(config)#enable secret ciscoenpass
- Contraseña de acceso a la consola  
S1(config)#line console 0
- Establecer la longitud mínima para las contraseñas 10 caracteres

S1(config)#security passwords min-length 10

- Crear un usuario administrativo en la base de datos local

```
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit
```

- Crear un usuario administrativo en la base de datos local

S1(config)#username admin password admin1pass

- Configurar el inicio de sesión en las líneas VTY para que use la base de datos local

```
S1(config)#line vty 0 15
S1(config-line)#password ciscocisco
S1(config-line)#login local
```

- Configurar VTY solo aceptando SSH

```
S1(config-line)#transport input ssh
S1(config-line)#exit
```

- Cifrar las contraseñas de texto no cifrado

```
S1(config)#service password-encryption
```

- Configure un MOTD Banner

S1(config)#banner motd #Switch de personal autorizado de la UNAD cualquier instruccion tendra efectos legales de acuerdo a la ley#

- Generar una clave de cifrado RSA Módulo de 1024 bits

```
S1(config)#ip domain name ccna-lab.com
S1(config)#crypto key generate rsa
```

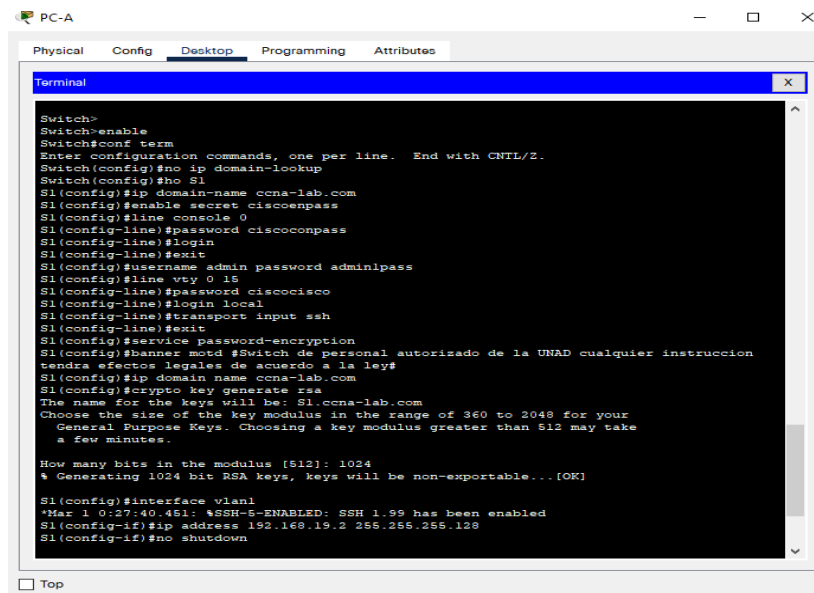
- Configurar la interfaz de administración (SVI)

```
S1(config)#interface vlan1
S1(config-if)# ip address 192.168.19.2 255.255.255.128
S1(config-if)#no shutdown
S1(config-if)#exit
```

- Configuración del gateway predeterminado.

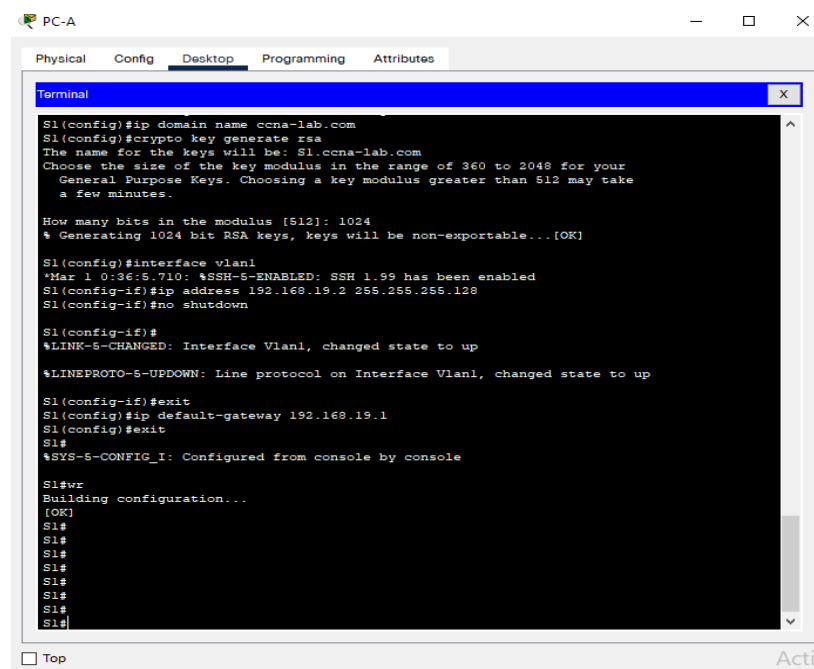
```
S1(config)#ip default-gateway 192.168.19.1
S1(config)#exit
S1#wr
```

Figura 5. Configuración S1



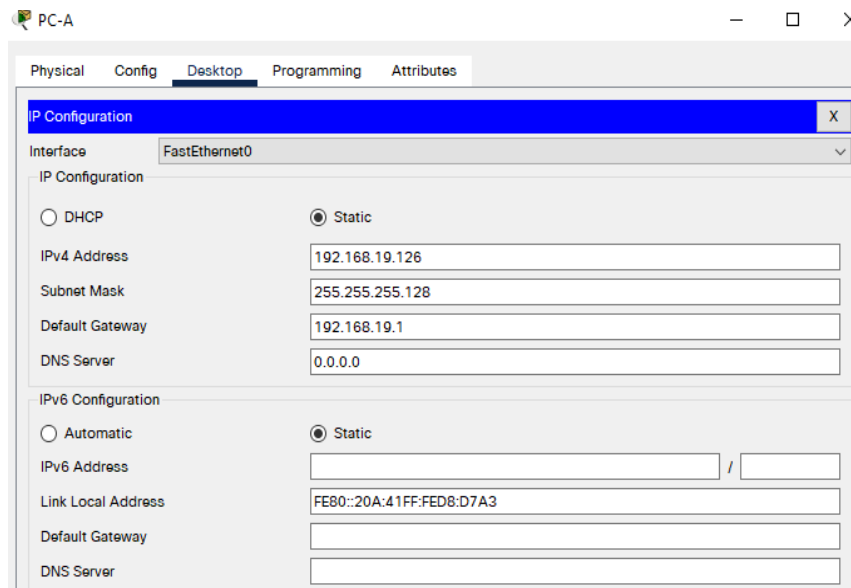
Fuente: Elaboración propia

Figura 6. Configuración VLAN



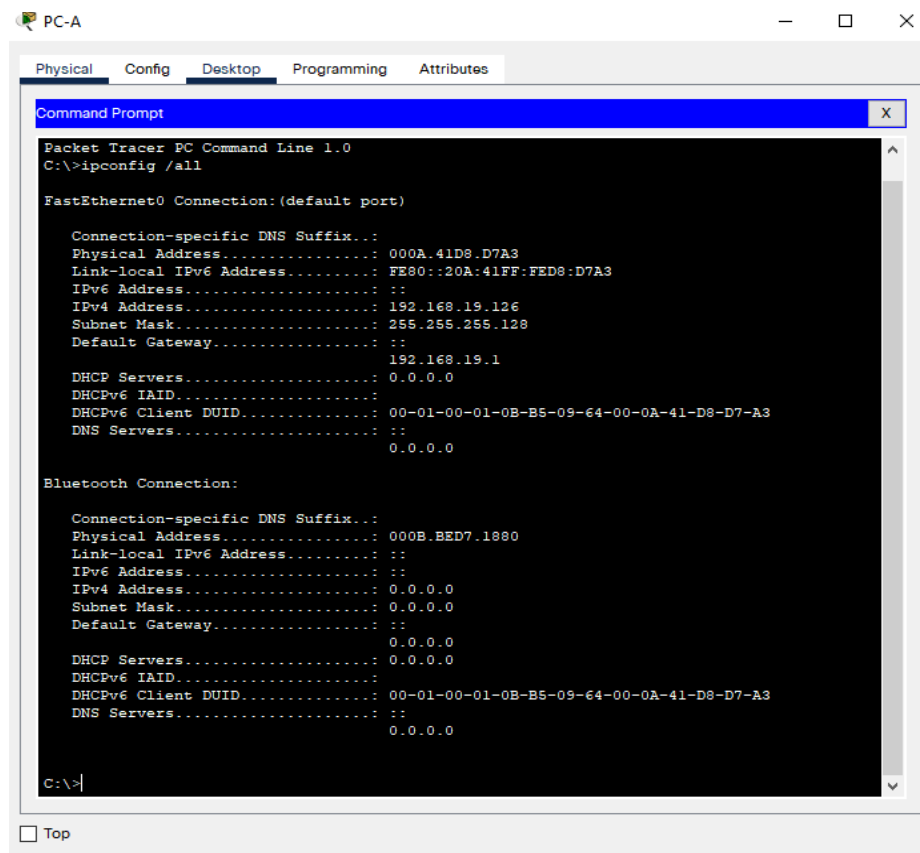
Fuente: Elaboración propia

Figura 7. Configuración de los equipos host PC-A



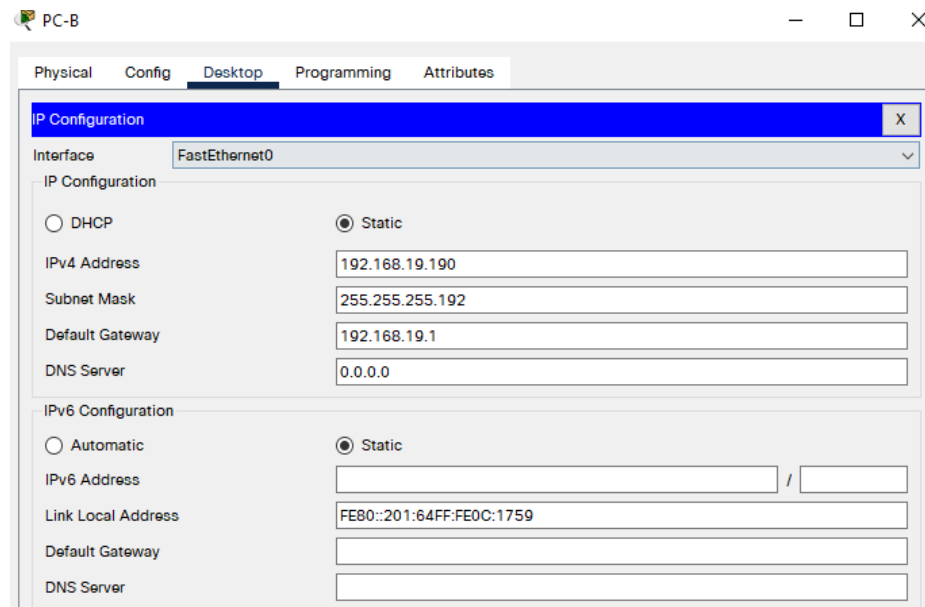
Fuente: Elaboración propia

Figura 8. Visualización direcciones IP PC-A



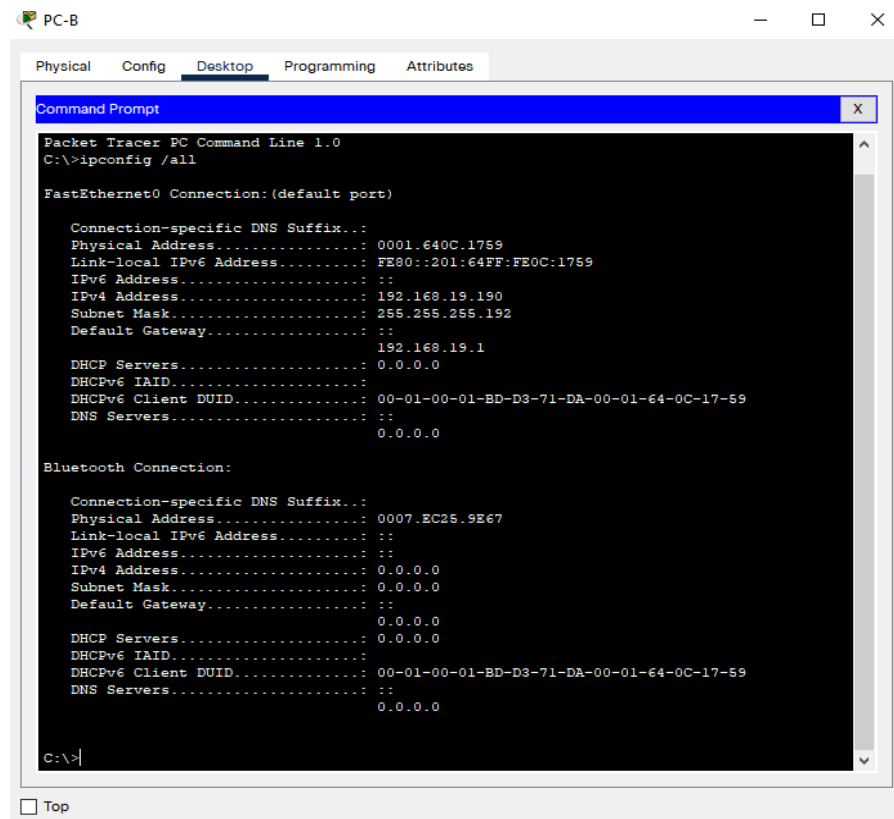
Fuente: Elaboración propia

Figura 9. Configuración de los equipos host PC-B



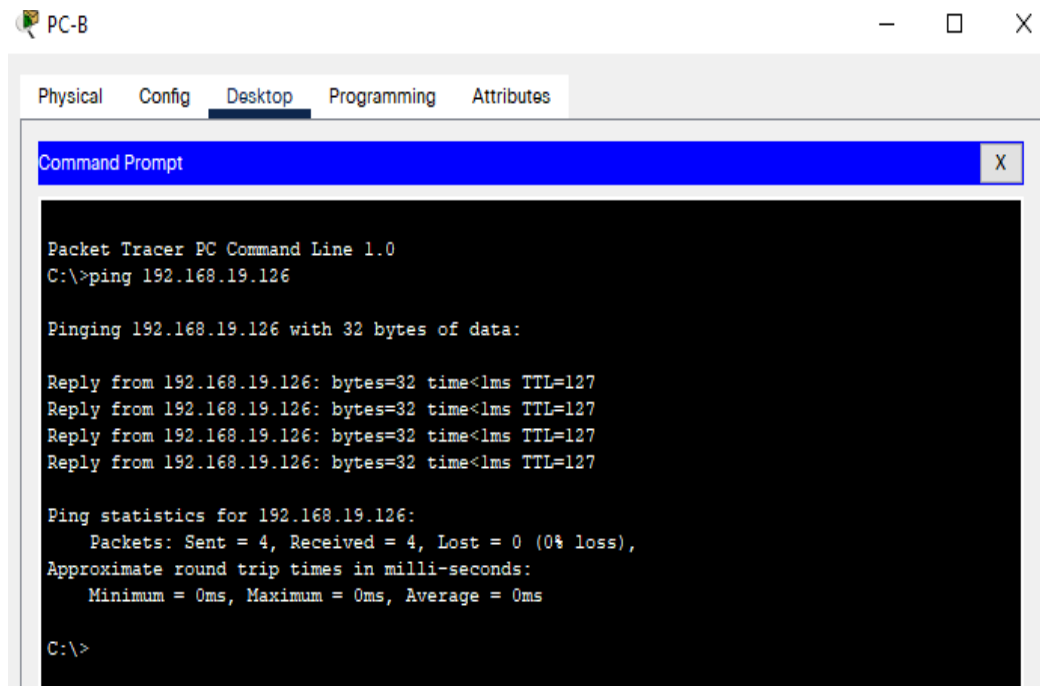
Fuente: Elaboración propia

Figura 10. Visualización direcciones IP PC-B



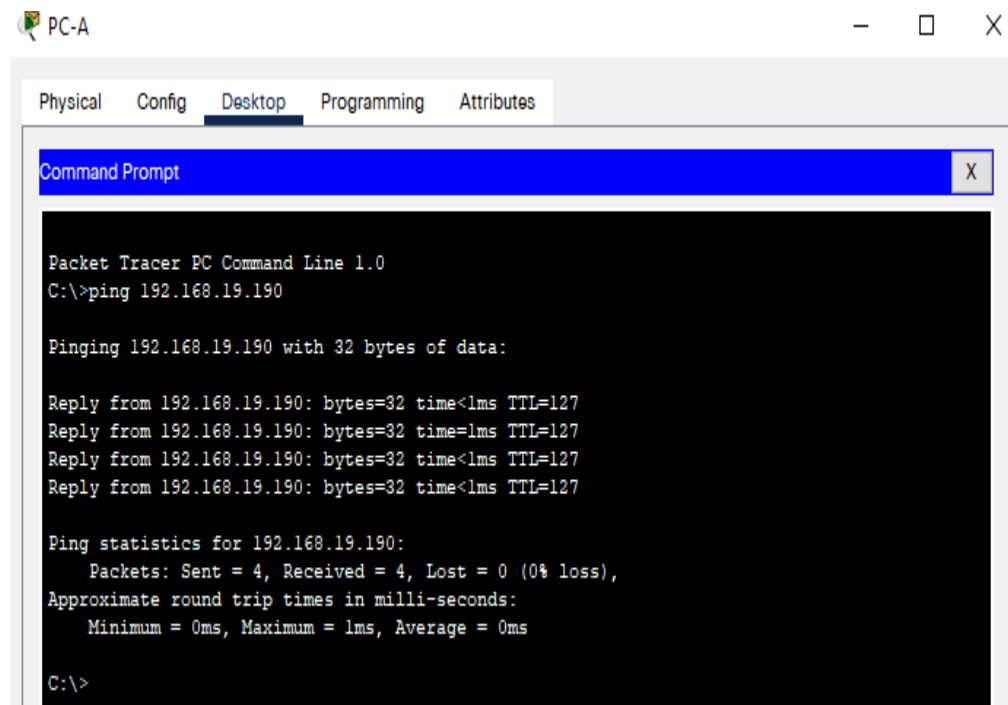
Fuente: Elaboración propia

Figura 11. Conectividad PC-B-PC-A



Fuente: Elaboración propia

Figura 12. Conectividad PC-A-PC-B



Fuente: Elaboración propia

Figura 13. Verificación de interfaces R1

```

PC-B
Physical Config Desktop Programming Attributes
Terminal
Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up
Router de personal autorizado de la UNAD cualquier instruccion tendra efectos legales de acuerdo a la ley

User Access Verification

Password:

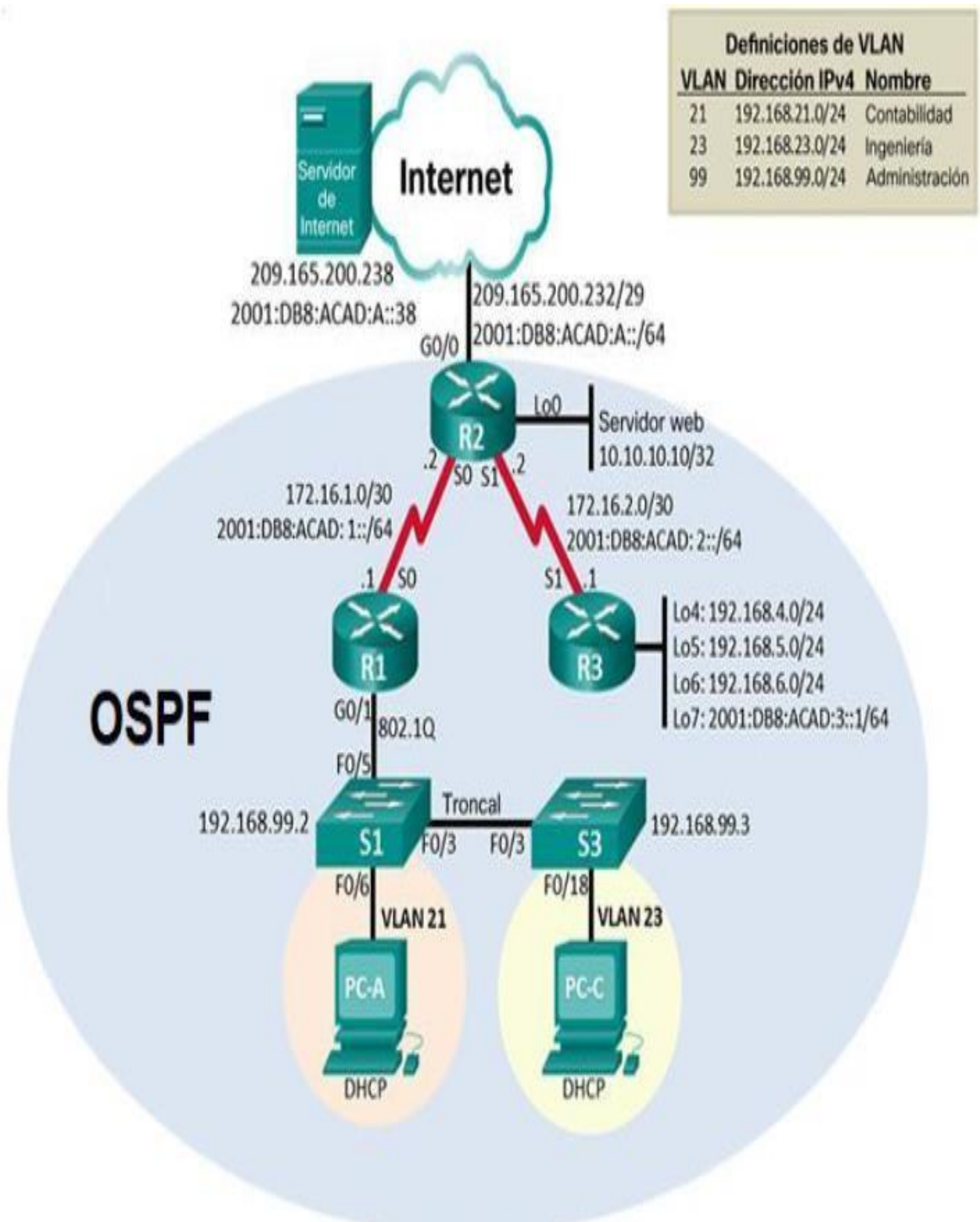
R1>enable
Password:
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/0/1
R1(config-if)#description conexion LAN 1 - PC-A
R1(config-if)#ip address 192.168.19.1 255.255.255.128
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#int g0/0/0
R1(config-if)#description conexion LAN 2 - PC-B
R1(config-if)#ip address 192.168.19.129 255.255.255.192
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#do show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0/0     192.168.19.129 YES manual up          up
GigabitEthernet0/0/1     192.168.19.1   YES manual up          up
GigabitEthernet0/0/2     unassigned      YES unset  administratively down down
Vlan1                    unassigned      YES unset  administratively down down
R1(config)#
R1(config)#
  
```

Fuente: Elaboración propia

## 2. ESCENARIO 2

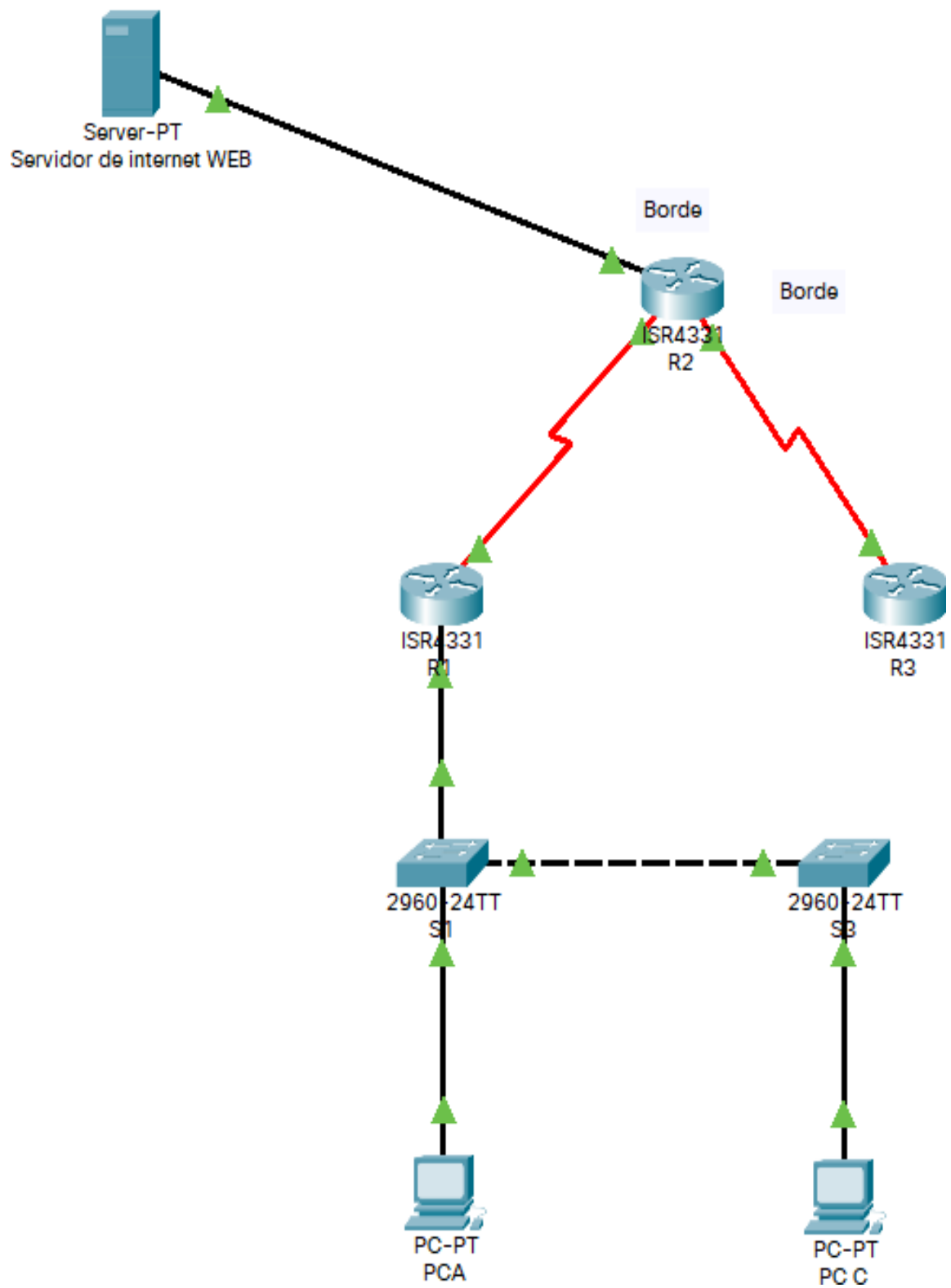
Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de 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.

Figura 14. Escenario 2



Fuente: Guía de actividades

Figura 15. Simulación de Escenario 2



## Parte 1: Inicializar dispositivos

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

- Eliminar el archivo startup-config de todos los routers

```
Router#erase startup-config
```

- Volver a cargar todos los routers

```
Router#reload
```

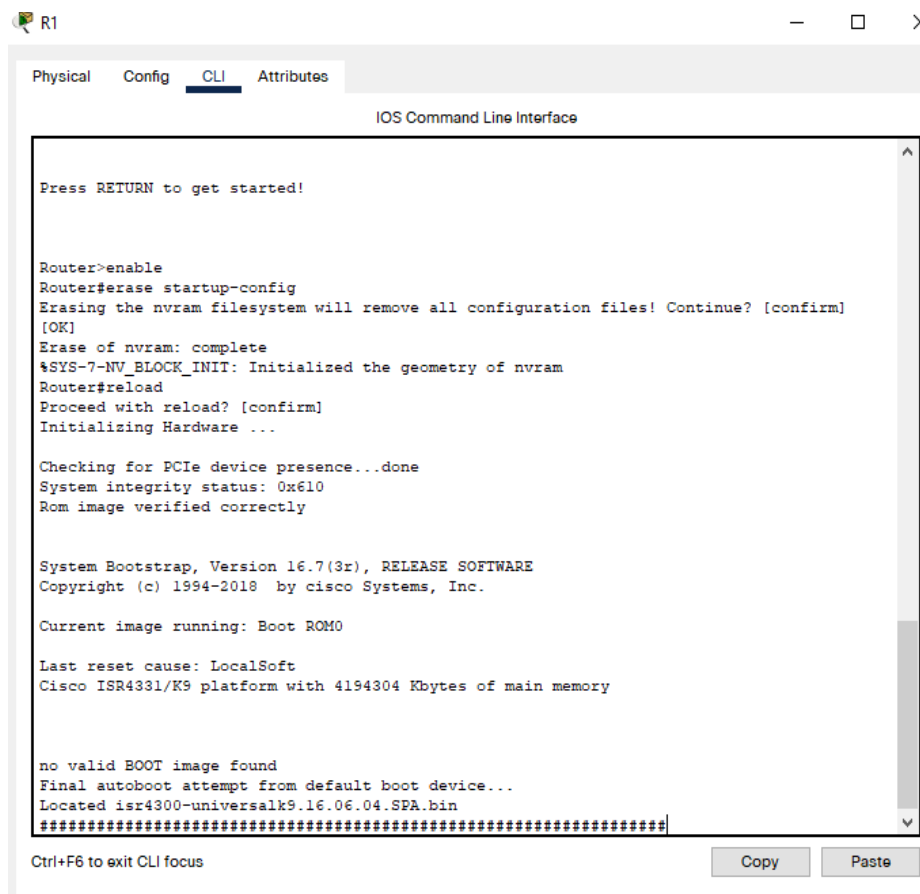
```
Router# delete vlan.dat
```

- Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches

```
Router# show vlan brief
```

```
Router# show flash
```

Figura 16. Reiniciar Configuración



```
R1
Physical Config CLI Attributes
IOS Command Line Interface

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#reload
Proceed with reload? [confirm]
Initializing Hardware ...

Checking for PCIe device presence...done
System integrity status: 0x610
Rom image verified correctly

System Bootstrap, Version 16.7(3r), RELEASE SOFTWARE
Copyright (c) 1994-2018 by cisco Systems, Inc.

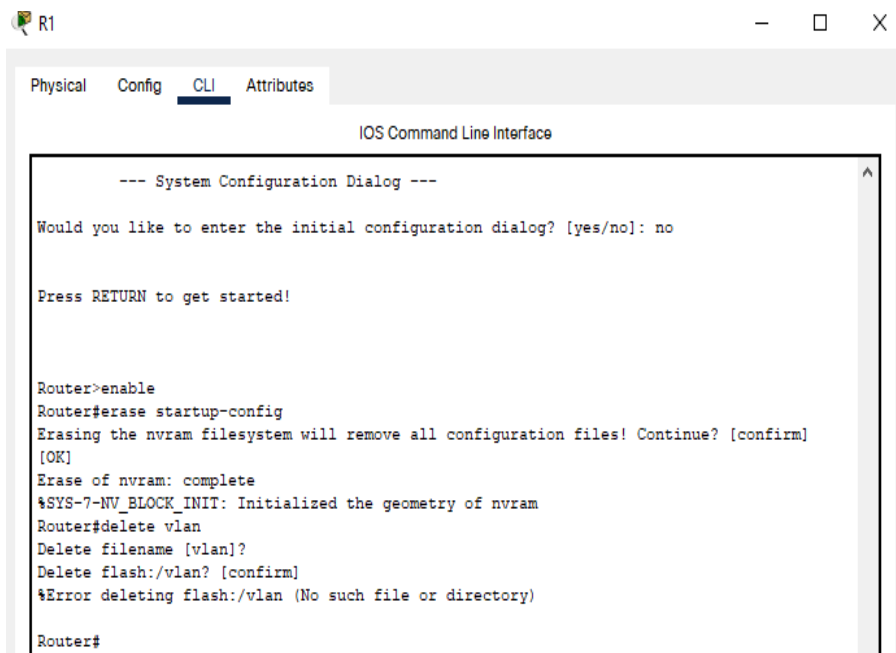
Current image running: Boot ROM0

Last reset cause: LocalSoft
Cisco ISR4331/K9 platform with 4194304 Kbytes of main memory

no valid BOOT image found
Final autoboot attempt from default boot device...
Located isr4300-universalk9.16.06.04.SPA.bin
*****
Ctrl+F6 to exit CLI focus
```

Fuente: Elaboración propia

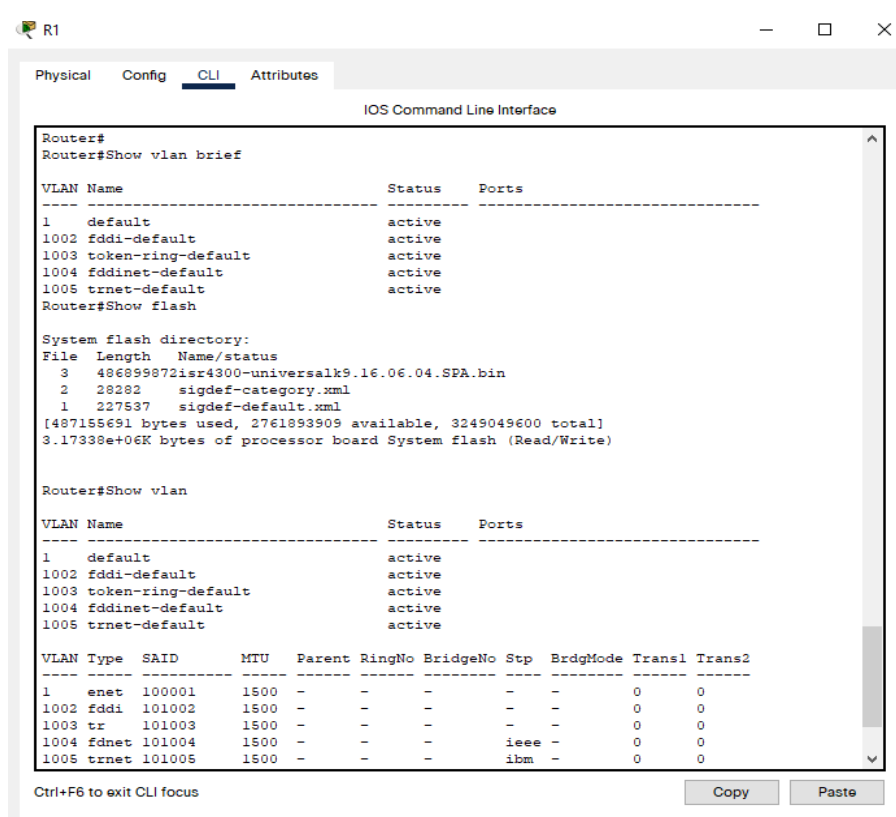
Figura 17. Eliminar VLAN



```
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#delete vlan
Delete filename [vlan]?
Delete flash:/vlan? [confirm]
%Error deleting flash:/vlan (No such file or directory)
Router#
```

Fuente: Elaboración propia

Figura 18. VLAN



```
Router#
Router#Show vlan brief

VLAN Name                Status    Ports
-----
1    default                active
1002 fddi-default          active
1003 token-ring-default    active
1004 fddinet-default       active
1005 trnet-default         active
Router#Show flash

System flash directory:
File Length Name/status
3 486899872lsr4300-universalk9.16.06.04.SPA.bin
2 28282 sigdef-category.xml
1 227537 sigdef-default.xml
[487155691 bytes used, 2761893909 available, 3249049600 total]
3.17338e+06K bytes of processor board System flash (Read/Write)

Router#Show vlan

VLAN Name                Status    Ports
-----
1    default                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 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
1003 tr 101003 1500 - - - - - 0 0
1004 fdnet 101004 1500 - - - - - ieee 0 0
1005 trnet 101005 1500 - - - - - ibm 0 0
```

Fuente: Elaboración propia

## Parte 2: Configurar los parámetros básicos de los dispositivos

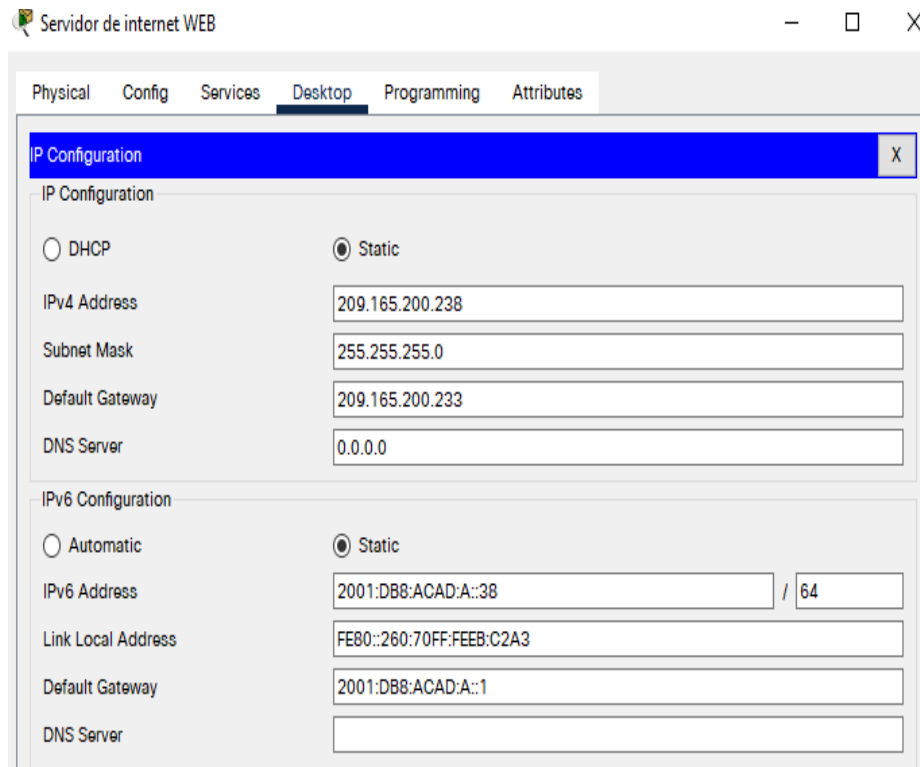
### Paso 1: Configurar la computadora de Internet

Tabla 3.Tabla direcciones del Servidor

| Elemento o Tarea de Configuración | Especificación         |
|-----------------------------------|------------------------|
| Dirección IPv4                    | 209.165.200.238        |
| Máscara de subred para IPv4       | 255.255.255.248        |
| Gateway predeterminado            | 209.165.200.225        |
| Dirección IPv6/subred             | 2001:DB8:ACAD:A::38/64 |
| Gateway predeterminado IPv6       | 2001:DB8:ACAD:2::1     |

Fuente: Elaboración propia

Figura 19. Asignación direcciones Servidor Web



Fuente: Elaboración propia

## Parte 2: Configurar los parámetros básicos de los dispositivos

### Paso 2: Configurar R1

- Desactivar la búsqueda DNS

Router(config)#no ip domain-lookup

- Nombre del router  
Router(config)#hostname R1
- Contraseña de exec privilegiado cifrada  
R1(config)#enable secret class
- Contraseña de acceso a la consola  
R1(config)#line console 0  
R1(config-line)#password cisco  
R1(config-line)#login
- Contraseña de acceso Telnet  
R1(config-line)#line vty 0 4  
R1(config-line)#password cisco  
R1(config-line)#login  
R1(config-line)#exit
- Cifrar las contraseñas de texto no cifrado  
R1(config)#service password-encryption
- Mensaje MOTD  
R1(config)#banner motd #Se prohíbe el acceso no autorizado#
- Interfaz S0/0/0  
R1(config)#int s0/2/0  
R1(config-if)#description interface Hacia el Router R2  
R1(config-if)#exit
- Configurar rutas predeterminadas  
R1(config)#ipv6 unicast-routing  
R1(config)#int s0/2/0  
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  
R1(config-if)#exit  
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/2/0  
R1(config)#ipv6 route ::/0 s0/2/0

Figura 20. Configuración básica de R1

```
Press RETURN to get started!

Router>enable
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#ho 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 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd #se prohíbe el acceso no autorizado#
R1(config)#int s0/2/0
R1(config-if)#description interface hacia el router R2
R1(config-if)#exit
R1(config)#ipv6 unicast-routing
R1(config)#int s0/2/0
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 Serial0/2/0, changed state to down
R1(config-if)#ip route 0.0.0.0 0.0.0.0 S0/2/0
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#ipv6 route ::/0 S0/2/0
R1(config)#
```

Fuente: Elaboración propia

### Paso 3: Configurar R2.

- Desactivar la búsqueda DNS  
Router(config)#no ip domain-lookup
- Nombre del router  
Router(config)#hostname R2
- Contraseña de exec privilegiado cifrada  
R2(config)#enable secret class

- Contraseña de acceso a la consola

```
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
```

- Contraseña de acceso Telnet

```
R2(config-line)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
```

- Cifrar las contraseñas de texto no cifrado

```
R2(config)#service password-encryption
```

- Mensaje MOTD

```
R2(config)#banner motd #Se prohíbe el acceso no autorizado#
```

- Interfaz S0/0/0

```
R2(config)#ipv6 unicast-routing
R2(config)#int s0/2/0
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)#description Conexion entre R2-R1
R2(config-if)#exit
```

- Interfaz S0/0/1

```
R2(config)#int s0/2/1
R2(config-if)#ip address 172.16.2.1 255.255.255.252
R2(config-if)#ipv6 add 2001:DB8:ACAD:2::2/64
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown
R2(config-if)#exit
```

- Interfaz G0/0

```
R2(config)#int g0/0/0
R2(config-if)#description interface Hacia Internet
R2(config-if)#exit
```

```

R2(config)#ipv6 unicast-routing
R2(config)#int g0/0/0
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)#exit

```

- Interfaz loopback 0

```

R2(config)#int loopback 0
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#description DNS Server
R2(config-if)#exit

```

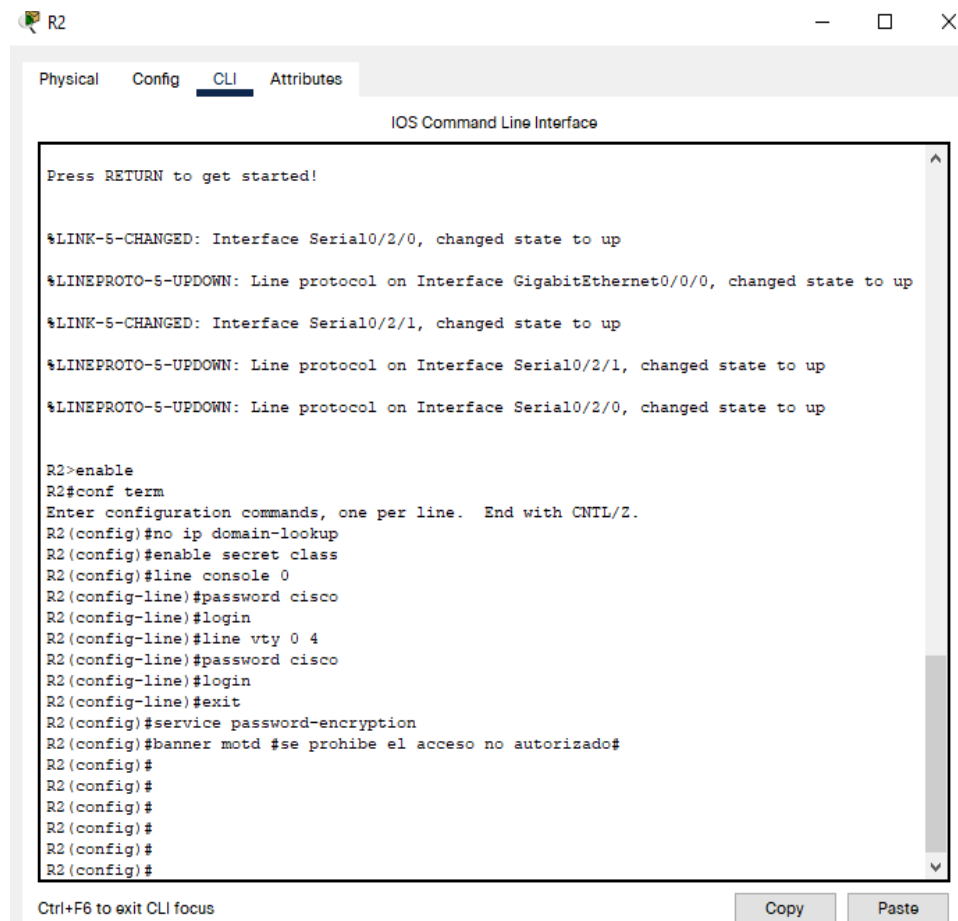
- Rutas predeterminadas

```

R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0/0
R2(config)#ipv6 route ::/0 g0/0/0

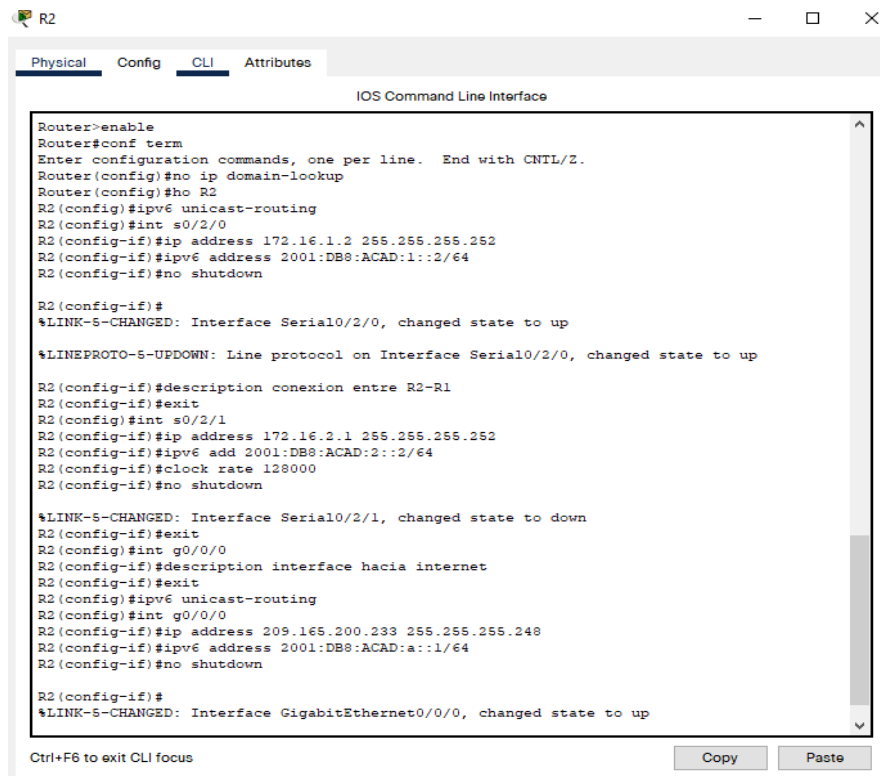
```

Figura 21. Configuración básica de R2



Fuente: Elaboración propia

Figura 22. Configuración interfaces R2



```

Router>enable
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#ho R2
R2(config)#ipv6 unicast-routing
R2(config)#int s0/2/0
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 Serial0/2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed state to up

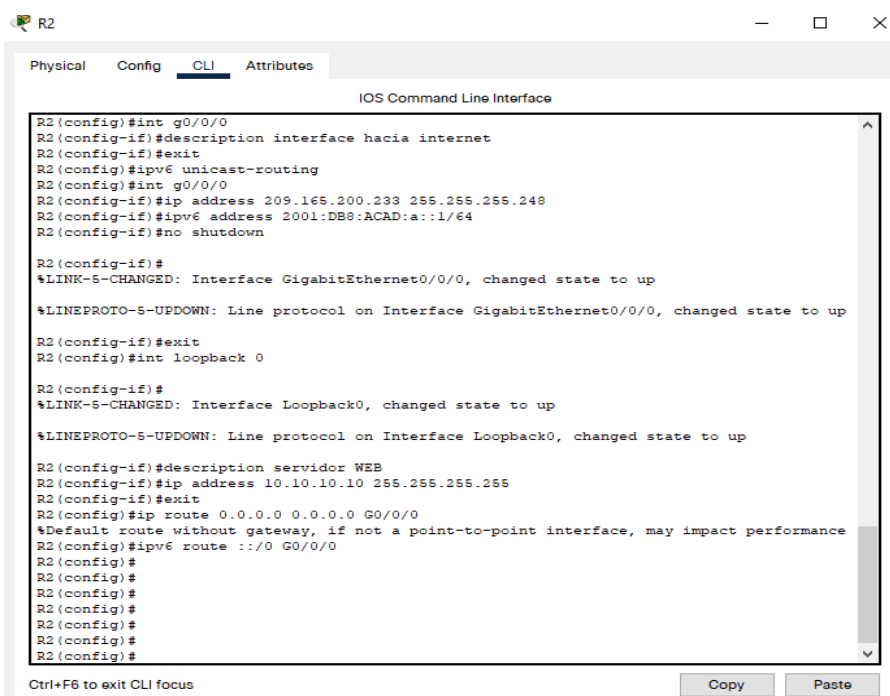
R2(config-if)#description conexion entre R2-R1
R2(config-if)#exit
R2(config)#int s0/2/1
R2(config-if)#ip address 172.16.2.1 255.255.255.252
R2(config-if)#ipv6 add 2001:DB8:ACAD:2::2/64
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/2/1, changed state to down
R2(config-if)#exit
R2(config)#int g0/0/0
R2(config-if)#description interface hacia internet
R2(config-if)#exit
R2(config)#ipv6 unicast-routing
R2(config)#int g0/0/0
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 GigabitEthernet0/0/0, changed state to up
  
```

Fuente: Elaboración propia

Figura 23. Configuración Loopbacks R2



```

R2(config)#int g0/0/0
R2(config-if)#description interface hacia internet
R2(config-if)#exit
R2(config)#ipv6 unicast-routing
R2(config)#int g0/0/0
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 GigabitEthernet0/0/0, changed state to up

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

R2(config-if)#exit
R2(config)#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)#description servidor WEB
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 G0/0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
R2(config)#ipv6 route ::0 G0/0/0
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
  
```

Fuente: Elaboración propia

#### Paso 4: Configurar R3

- Desactivar la búsqueda DNS  
Router(config)#no ip domain-lookup
- Nombre del router  
Router(config)#hostname R3
- Contraseña de exec privilegiado cifrada  
R3(config)#enable secret class
- Contraseña de acceso a la consola  
R3(config)#line console 0  
R3(config-line)#password cisco  
R3(config-line)#login
- Contraseña de acceso Telnet  
R3(config-line)#line vty 0 4  
R3(config-line)#password cisco  
R3(config-line)#login
- Cifrar las contraseñas de texto no cifrado  
R3(config)#service password-encryption
- Mensaje MOTD  
R3(config)#banner motd #Se prohíbe el acceso no autorizado#
- Interfaz S0/0/1  
R3(config)#ipv6 unicast-routing  
R3(config)#int s0/2/1  
R3(config-if)#ip address 172.16.2.2 255.255.255.252  
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64  
R3(config-if)#no shutdown
- Interfaz loopback 4  
R3(config)#int loopback 4

R3(config-if)#ip address 192.168.4.1 255.255.255.0

- Interfaz loopback 5

R3(config)#int loopback 5

R3(config-if)#ip address 192.168.5.1 255.255.255.0

- Interfaz loopback 6

R3(config)#int loopback 6

R3(config-if)#ip address 192.168.6.1 255.255.255.0

- Interfaz loopback 7

R3(config)#int loopback 7

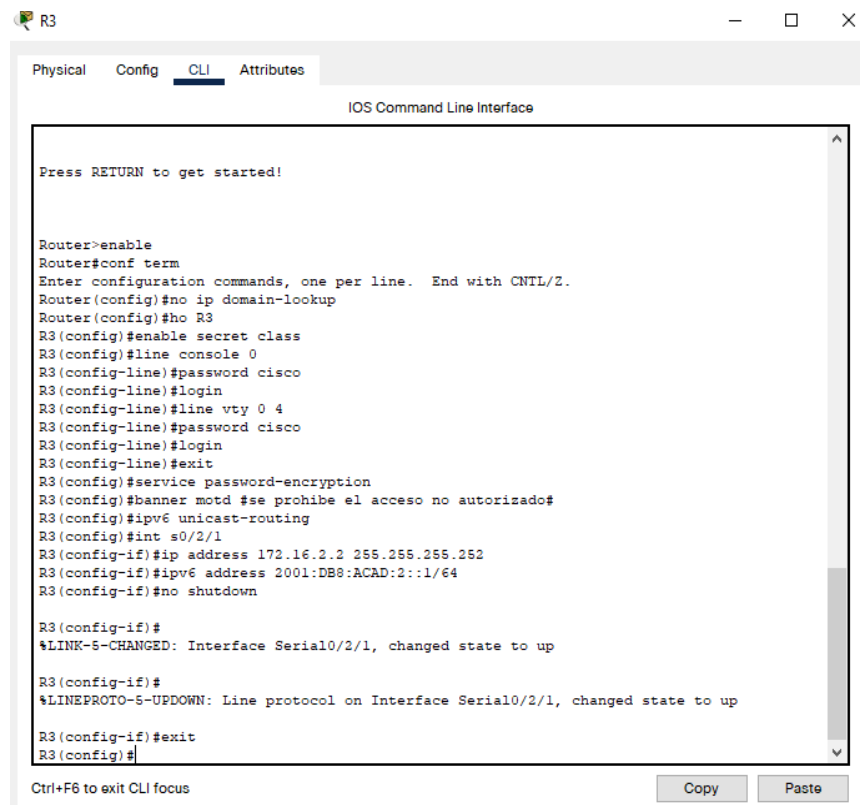
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64

- Rutas predeterminadas

R3(config)#ip route 0.0.0.0 0.0.0.0 S0/2/1

R3(config)#ipv6 route ::0 S0/2/1

Figura 24. Configuración básica de R3



The screenshot shows a window titled 'R3' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The text in the window shows the following commands and their outputs:

```
Press RETURN to get started!

Router>enable
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#ho R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd #se prohíbe el acceso no autorizado#
R3(config)#ipv6 unicast-routing
R3(config)#int s0/2/1
R3(config-if)#ip address 172.16.2.2 255.255.255.252
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64
R3(config-if)#no shutdown

R3(config-if)#
%LINK-6-CHANGED: Interface Serial0/2/1, changed state to up

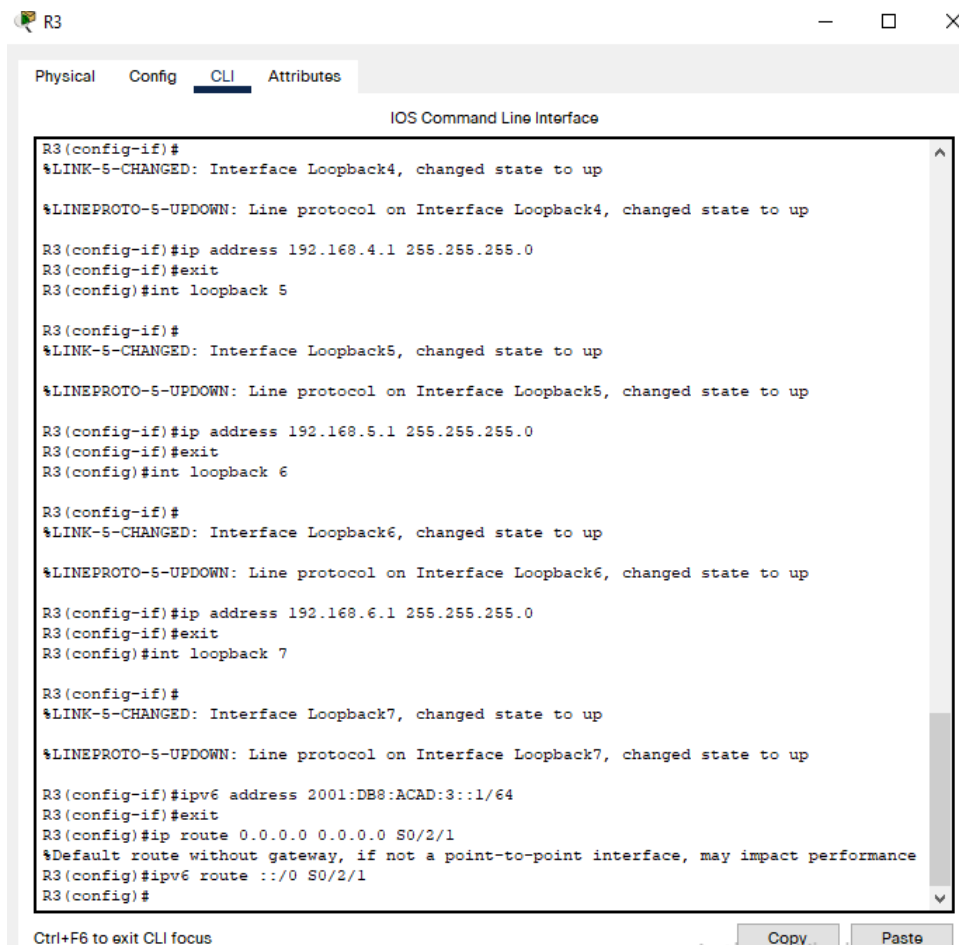
R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/1, changed state to up

R3(config-if)#exit
R3(config)#
```

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

Fuente: Elaboración propia

Figura 25. Configuración Loopbacks R3



The screenshot shows a window titled 'R3' 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 commands and responses:

```
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)#exit  
R3(config)#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)#exit  
R3(config)#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)#exit  
R3(config)#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 S0/2/1  
%Default route without gateway, if not a point-to-point interface, may impact performance  
R3(config)#ipv6 route ::/0 S0/2/1  
R3(config)#
```

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

Fuente: Elaboración propia

### Paso 5: Configurar S1

- Desactivar la búsqueda DNS  
Switch (config)#no ip domain-lookup
- Nombre del switch  
Switch (config)#hostname S1
- Contraseña de exec privilegiado cifrada  
S1(config)#enable secret class
- Contraseña de acceso a la consola  
S1(config)#line console 0

```
S1(config-line)#password cisco
S1(config-line)#login
```

- Contraseña de acceso Telnet

```
S1(config-line)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
```

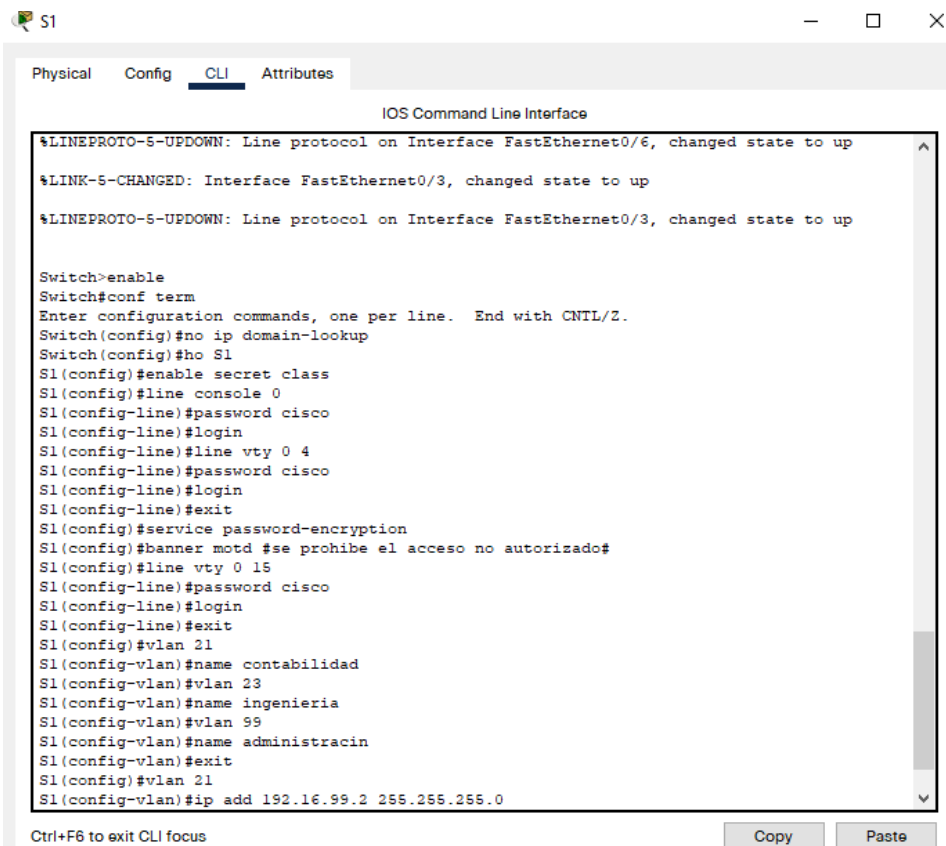
- Cifrar las contraseñas de texto no cifrado

```
S1(config)#service password-encryption
```

- Mensaje MOTD

```
S1(config)#banner motd #Se prohíbe el acceso no autorizado#
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
```

Figura 26. Configuración S1



Fuente: Elaboración propia

## Paso 6: Configurar el S3

- Desactivar la búsqueda DNS

Switch (config)#no ip domain-lookup

- Nombre del switch

Switch (config)#hostname S3

- Contraseña de exec privilegiado cifrada

S3 (config)#enable secret class

- Contraseña de acceso a la consola

S3 (config)#line console 0

S3 (config-line)#password cisco

S3 (config-line)#login

- Contraseña de acceso Telnet

S3 (config-line)#password cisco

S3 (config-line)#login

- Cifrar las contraseñas de texto no cifrado

S3(config)#service password-encryption

- Mensaje MOTD

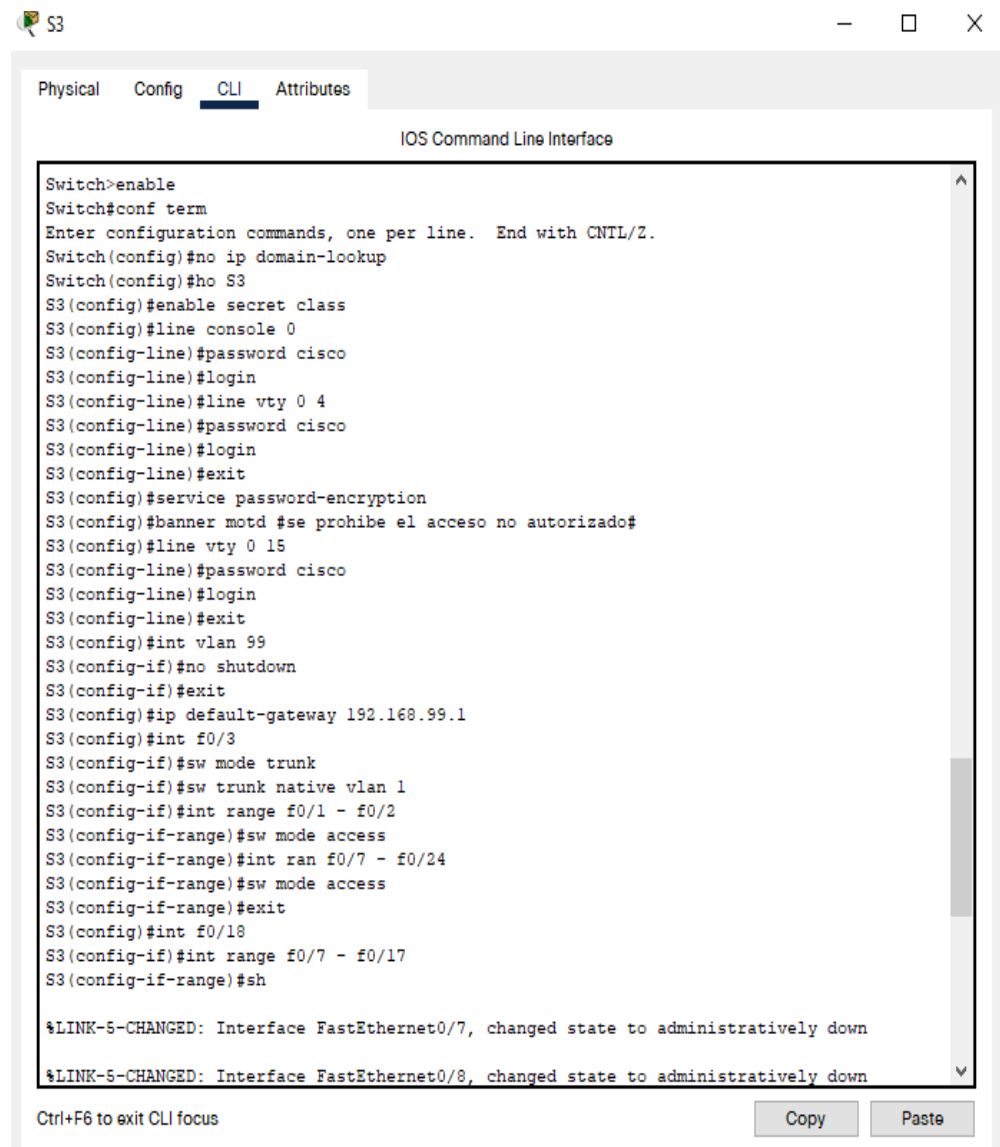
S3(config)#banner motd #Se prohíbe el acceso no autorizado#

S3(config)#line vty 0 15

S3(config-line)#password cisco

S3(config-line)#login

Figura 27. Configuración S3



The screenshot shows a window titled 'S3' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The interface shows a series of configuration commands entered for a switch named S3. The commands include enabling the switch, configuring terminal settings, disabling domain lookup, setting the host name to S3, enabling secret class, configuring console and vty lines with passwords and login, enabling password encryption, setting a MOTD banner, configuring VLAN 99, setting a default gateway, and configuring interfaces f0/3 through f0/17. The interface also shows two status messages: '%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down' and '%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down'. At the bottom, there is a 'Ctrl+F6 to exit CLI focus' message and 'Copy' and 'Paste' buttons.

```
Switch>enable
Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#ho S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd #se prohíbe el acceso no autorizado#
S3(config)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#int vlan 99
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)#sw mode trunk
S3(config-if)#sw trunk native vlan 1
S3(config-if)#int range f0/1 - f0/2
S3(config-if-range)#sw mode access
S3(config-if-range)#int ran f0/7 - f0/24
S3(config-if-range)#sw mode access
S3(config-if-range)#exit
S3(config)#int f0/18
S3(config-if)#int range f0/7 - f0/17
S3(config-if-range)#sh

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

Ctrl+F6 to exit CLI focus
```

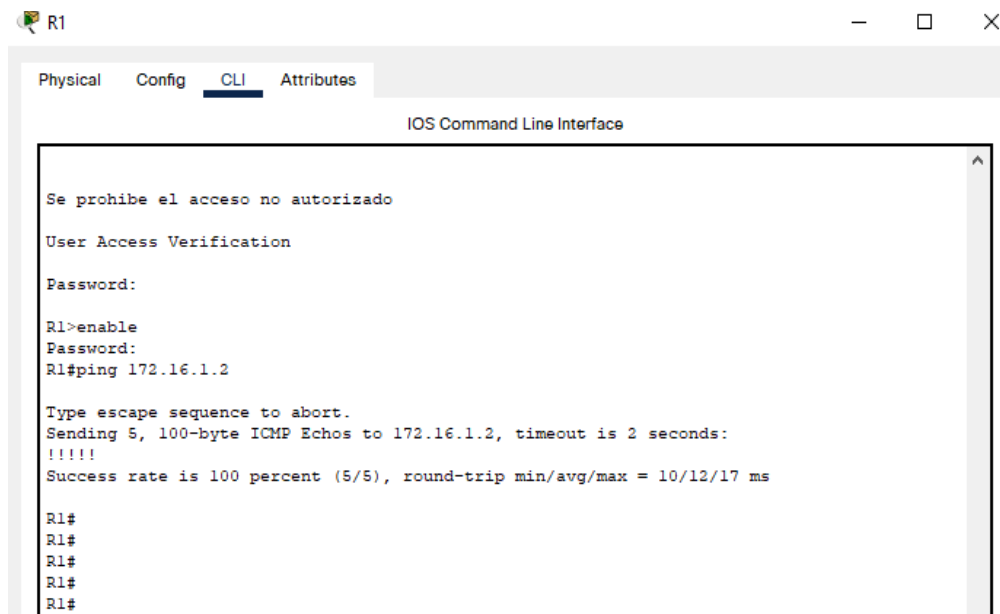
Fuente: Elaboración propia

Tabla 4. Tabla de Conectividad Routers

| Desde | A                      | Dirección IP    | Resultados |
|-------|------------------------|-----------------|------------|
| R1    | R2, S0/0/0             | 172.16.1.2      | Correcto   |
| R2    | R3, S0/0/1             | 172.16.2.1      | Correcto   |
| PC    | Gateway predeterminado | 209.165.200.233 | Correcto   |

Fuente: Elaboración propia

Figura 28. Conectividad R1-R2



The screenshot shows the CLI window for router R1. The window has tabs for Physical, Config, CLI (selected), and Attributes. The title bar says 'R1'. The main area is titled 'IOS Command Line Interface'. The text in the window is as follows:

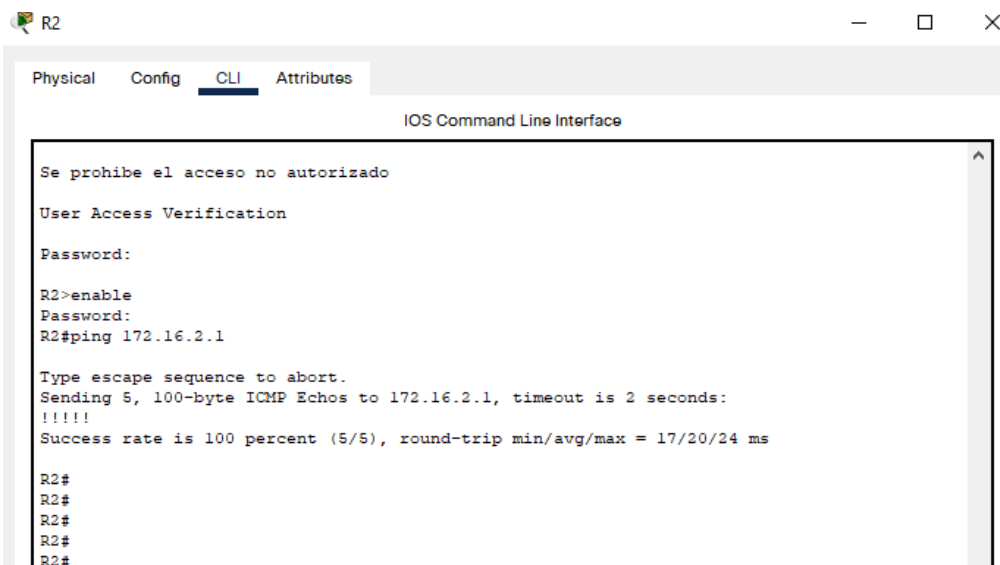
```
Se prohíbe el acceso no autorizado
User Access Verification
Password:
R1>enable
Password:
R1#ping 172.16.1.2

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 = 10/12/17 ms

R1#
R1#
R1#
R1#
R1#
```

Fuente: Elaboración propia

Figura 29. Conectividad R2-R3



The screenshot shows the CLI window for router R2. The window has tabs for Physical, Config, CLI (selected), and Attributes. The title bar says 'R2'. The main area is titled 'IOS Command Line Interface'. The text in the window is as follows:

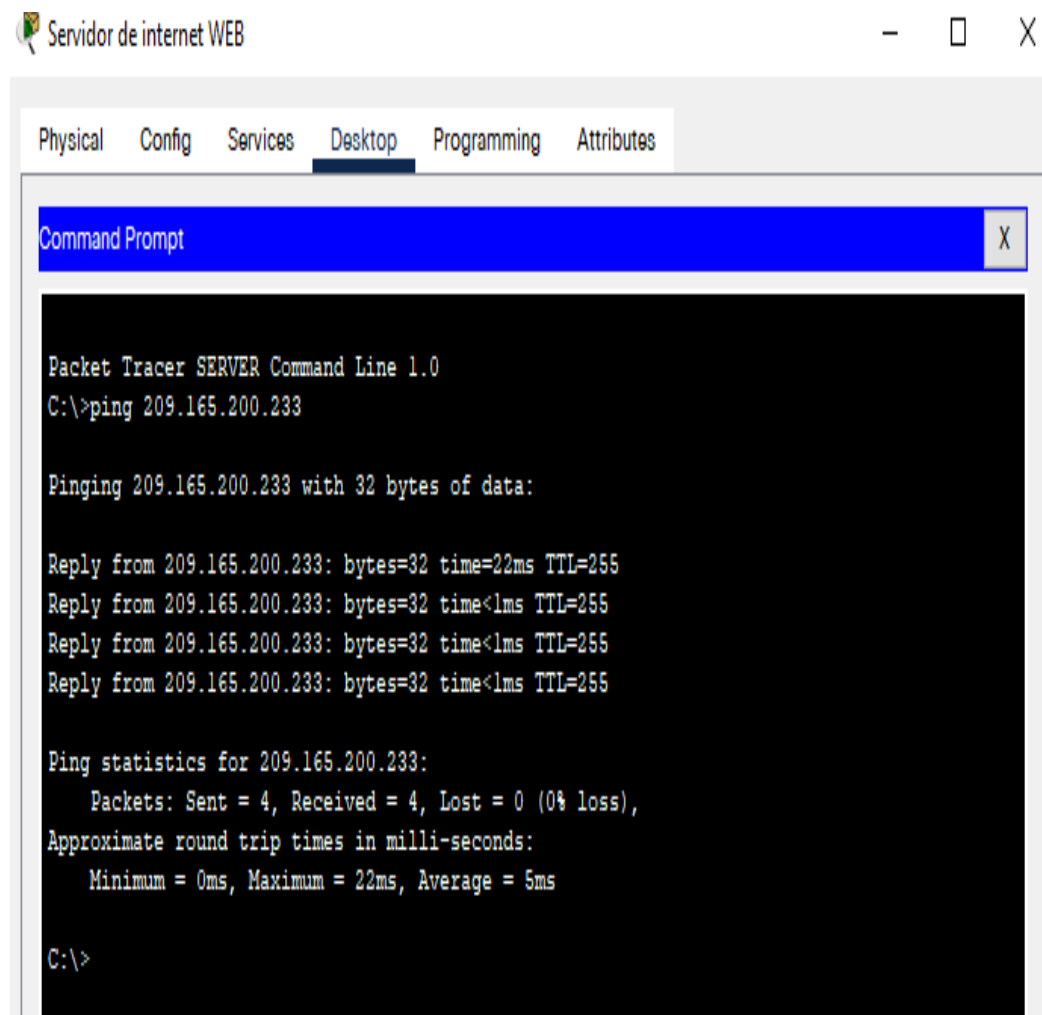
```
Se prohíbe el acceso no autorizado
User Access Verification
Password:
R2>enable
Password:
R2#ping 172.16.2.1

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 = 17/20/24 ms

R2#
R2#
R2#
R2#
R2#
```

Fuente: Elaboración propia

Figura 30. Conectividad Servidor



Fuente: Elaboración propia

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

#### Paso 1: Configurar S1

- Crear la base de datos de VLAN
- ```
S1(config-vlan)#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
```

- Asignar la dirección IP de administración

```
S1(config)#int vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
```

- Asignar el gateway predeterminado

```
S1(config)#ip default-gateway 192.168.99.1
```

- Forzar el enlace troncal en la interfaz F0/3

```
S1(config)#int f0/3
S1(config-if)#sw mode trunk
S1(config-if)#switchport trunk native vlan 1
```

- Forzar el enlace troncal en la interfaz F0/5

```
S1(config)#int f0/5
S1(config-if)#sw mode trunk
S1(config-if)#switchport trunk native vlan 1
```

- Configurar el resto de los puertos como puertos de acceso

```
S1(config)#int range f0/1- f0/2
S1(config-if-range)#sw mode access
```

```
S1(config)#int range f0/7- f0/24
S1(config-if-range)#sw mode access
```

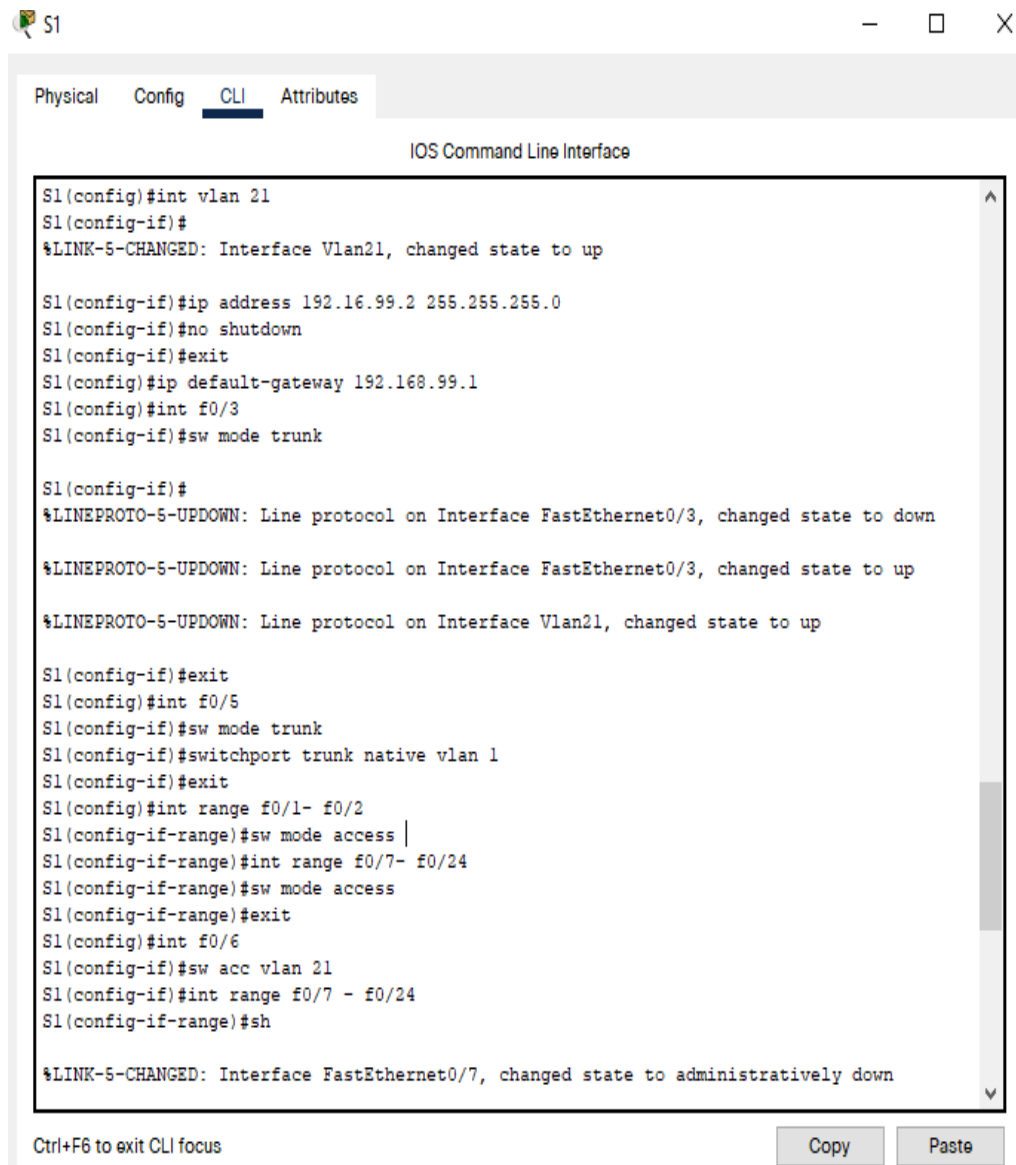
- Asignar f0/6 a la VLAN 21

```
S1(config)#int f0/6
S1(config-if)#sw acc vlan 21
```

- Apagar todos los puertos sin usar

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

Figura 31. Configuración Trunk S1



```
S1
Physical Config CLI Attributes
IOS Command Line Interface

S1(config)#int vlan 21
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan21, 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)#sw 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 Vlan21, changed state to up

S1(config-if)#exit
S1(config)#int f0/5
S1(config-if)#sw mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
S1(config)#int range f0/1- f0/2
S1(config-if-range)#sw mode access
S1(config-if-range)#int range f0/7- f0/24
S1(config-if-range)#sw mode access
S1(config-if-range)#exit
S1(config)#int f0/6
S1(config-if)#sw acc vlan 21
S1(config-if)#int range f0/7 - f0/24
S1(config-if-range)#sh

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

Ctrl+F6 to exit CLI focus
```

Fuente: Elaboración propia

## Paso 2: Configurar el S3

- Crear la base de datos de VLAN

```
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 Administración
```

- Asignar la dirección IP de administración

```
S3(config)#int vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown
```

- Asignar el gateway predeterminado

```
S3(config)#ip default-gateway 192.168.99.1
```

- Forzar el enlace troncal en la interfaz F0/3

```
S3(config)#int f0/3
S3(config-if)#sw mode trunk
S3(config-if)#sw trunk native vlan 1
```

- Configurar el resto de los puertos como puertos de acceso

```
S3(config)#int range f0/1 - f0/2
S3(config-if-range)#sw mode access
S3(config-if-range)#int range f0/7 - f0/24
S3(config-if-range)#sw mode access
```

- Asignar f0/18 a la VLAN 23

```
S3(config)#int f0/18
S3(config-if)#sw acc vlan 23
S3(config)#int range f0/7 - f0/17
S3(config-if-range)#sh
```

- Apagar todos los puertos sin usar

```
S3(config)# int range f0/1-2,f0/4,f0/7-24,g0/1-2
S3(config-if-range)#sh
```

Figura 32. Configuración Trunk 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 Administracin
S3(config-vlan)#exit
S3(config)#int vlan 99
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)#sw mode trunk
S3(config-if)#sw trunk native vlan 1
S3(config-if)#int range f0/1 - f0/2
S3(config-if-range)#sw mode access
S3(config-if-range)#int range f0/7 - f0/24
S3(config-if-range)#sw mode access
S3(config-if-range)#int f0/18
S3(config-if)#exit
S3(config)#int f0/18
S3(config-if)#sw acc vlan 23
S3(config-if)#int range f0/7 - f0/17
S3(config-if-range)#sh
S3(config-if-range)#exit
S3(config)#int range f0/1-2,f0/4,f0/7-24,g0/1-2
S3(config-if-range)#sh

S3(config-if-range)#
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administrati
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed

```

Fuente: Elaboración propia

### Paso 3: Configurar R1

- Configurar la subinterfaz 802.1Q .21 en G0/1

```

R1(config)#int g0/0/1.21
R1(config-subif)#description LAN Contabilidad
R1(config-subif)#enc dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#exit

```

- Configurar la subinterfaz 802.1Q .23 en G0/1

```
R1(config)#int g0/0/1.23
R1(config-subif)#desc LAN Ingenieria
R1(config-subif)#en dot1q 23
R1(config-subif)#ip add 192.168.23.1 255.255.255.0
```

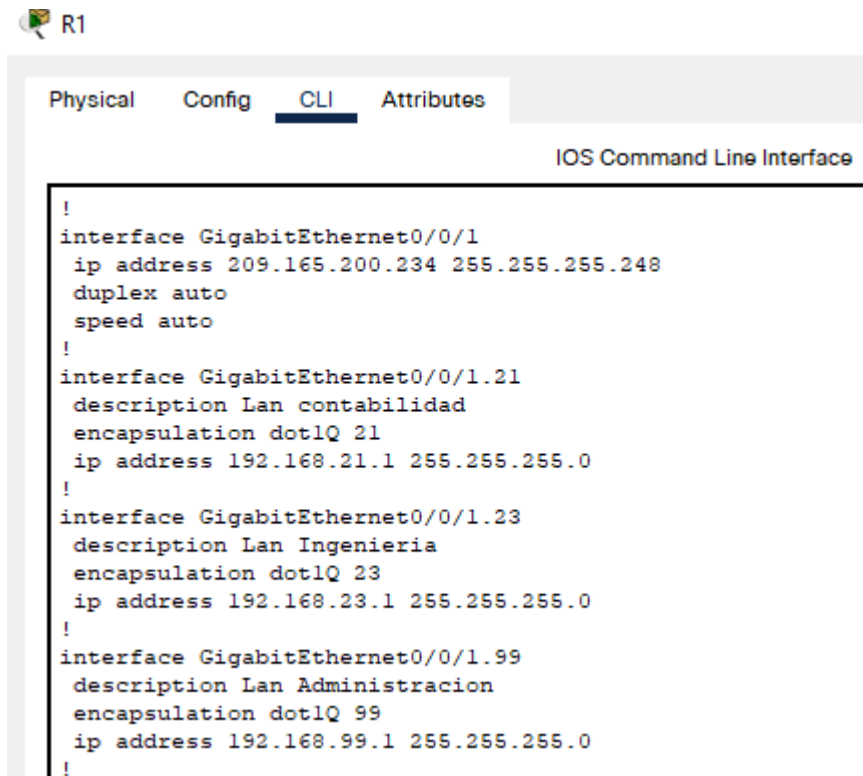
- Configurar la subinterfaz 802.1Q .99 en G0/1

```
R1(config)#int g0/0/1.99
R1(config-subif)#description LAN Administracion
R1(config-subif)#en dot1q 99
R1(config-subif)#ip add 192.168.99.1 255.255.255.0
```

- Activar la interfaz G0/1

```
R1(config-subif)#int g0/0/1
R1(config-if)#no shutdown
```

Figura 33. Configuración Subinterfaz



```
R1
Physical  Config  CLI  Attributes
IOS Command Line Interface

!
interface GigabitEthernet0/0/1
 ip address 209.165.200.234 255.255.255.248
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/1.21
 description Lan contabilidad
 encapsulation dot1Q 21
 ip address 192.168.21.1 255.255.255.0
!
interface GigabitEthernet0/0/1.23
 description Lan Ingenieria
 encapsulation dot1Q 23
 ip address 192.168.23.1 255.255.255.0
!
interface GigabitEthernet0/0/1.99
 description Lan Administracion
 encapsulation dot1Q 99
 ip address 192.168.99.1 255.255.255.0
!
```

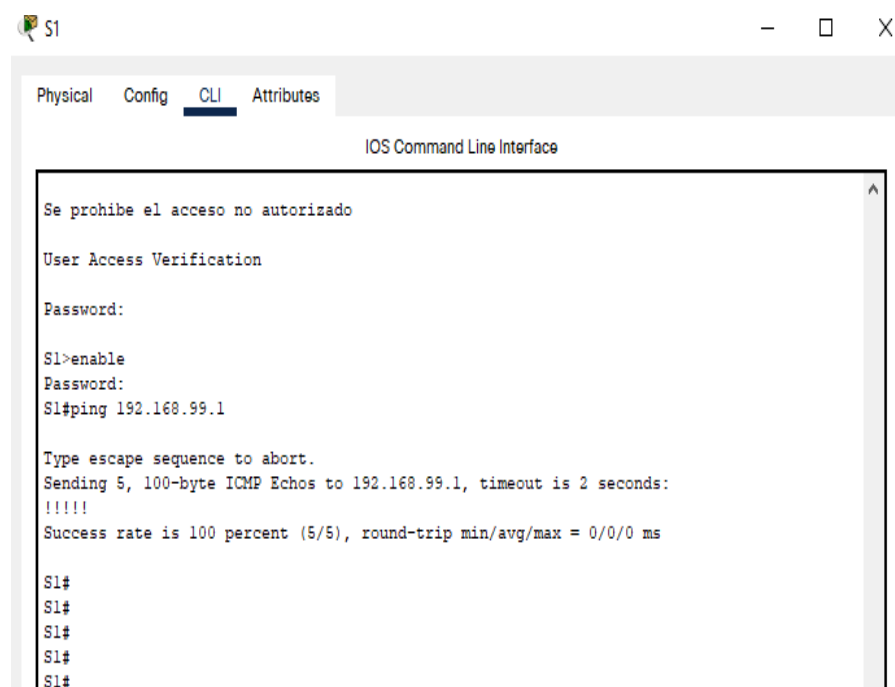
Fuente: Elaboración propia

Tabla 5. Tabla de Conectividad Routers y Switchs

| Desde     | A                     | Dirección IP | Resultados |
|-----------|-----------------------|--------------|------------|
| <b>S1</b> | R1, dirección VLAN 99 | 192.168.99.1 | Correcto   |
| <b>S3</b> | R1, dirección VLAN 99 | 192.168.99.1 | Correcto   |
| <b>S1</b> | R1, dirección VLAN 21 | 192.168.21.1 | Correcto   |
| <b>S3</b> | R1, dirección VLAN 23 | 192.168.21.1 | Correcto   |

Fuente: Elaboración propia

Figura 34. Conectividad S1-R1



```

S1
Physical Config CLI Attributes
IOS Command Line Interface

Se prohíbe el acceso no autorizado

User Access Verification

Password:

S1>enable
Password:
S1#ping 192.168.99.1

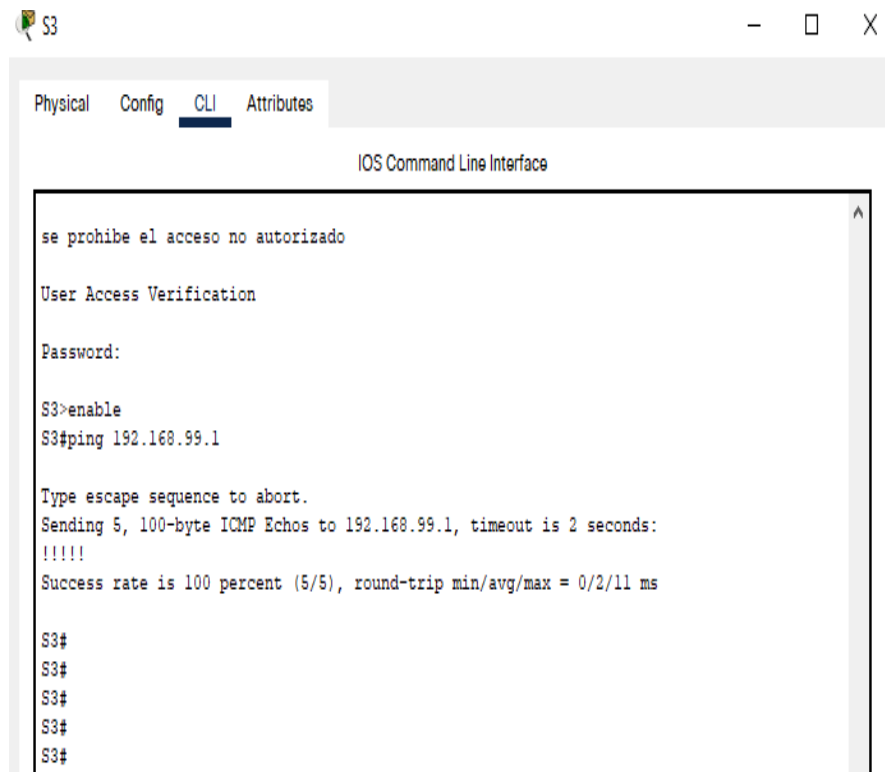
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

S1#
S1#
S1#
S1#
S1#

```

Fuente: Elaboración propia

Figura 35. Conectividad S3-R1



The screenshot shows a terminal window titled 'S3' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The text in the terminal is as follows:

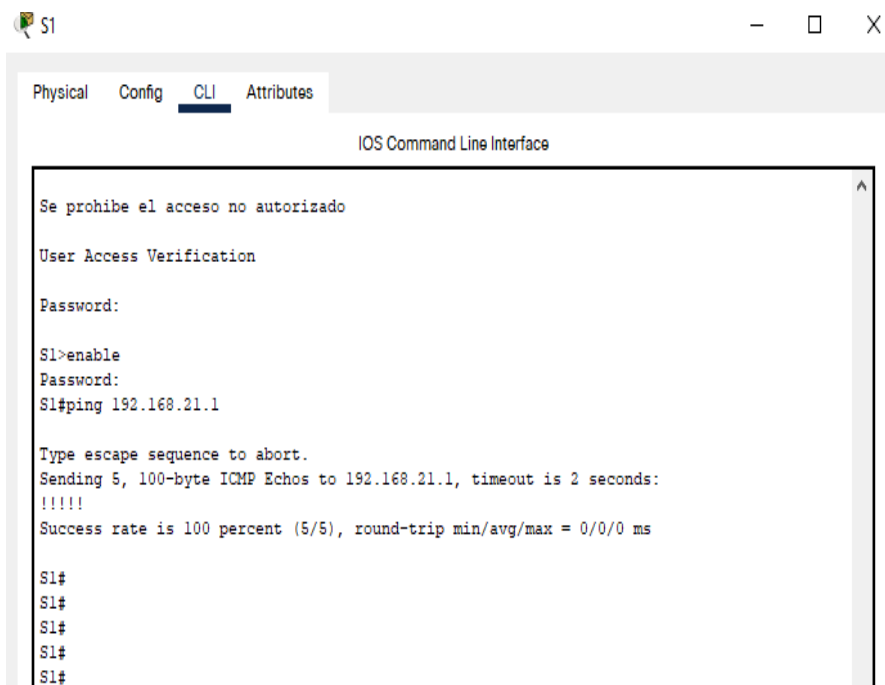
```
se prohíbe el acceso no autorizado
User Access Verification
Password:
S3>enable
S3#ping 192.168.99.1

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 = 0/2/11 ms

S3#
S3#
S3#
S3#
S3#
```

Fuente: Elaboración propia

Figura 36. Conectividad R1-S1



The screenshot shows a terminal window titled 'S1' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The text in the terminal is as follows:

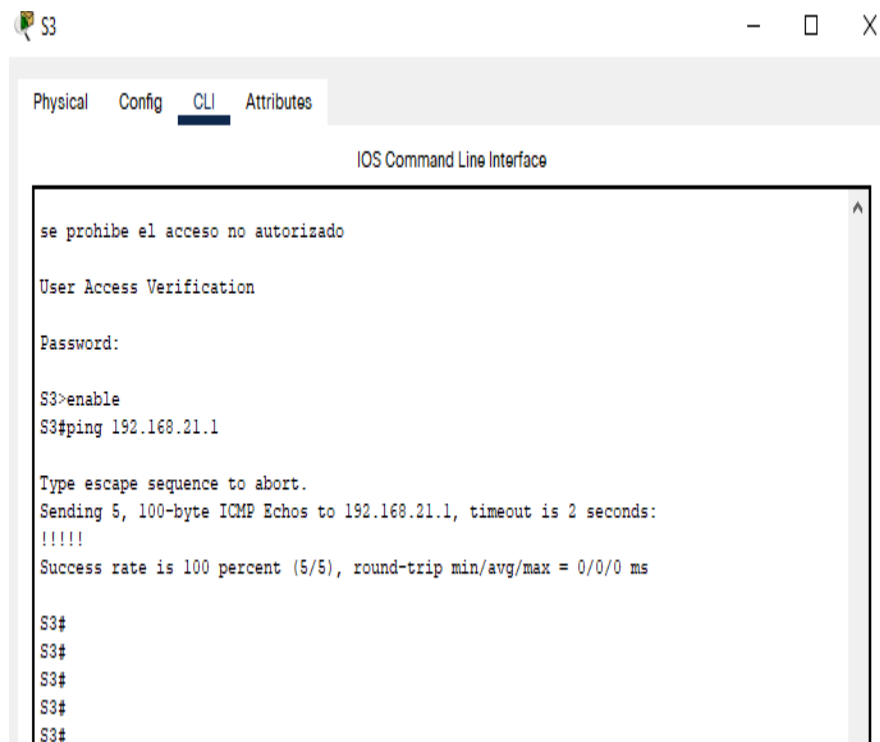
```
Se prohíbe el acceso no autorizado
User Access Verification
Password:
S1>enable
Password:
S1#ping 192.168.21.1

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#
S1#
S1#
S1#
S1#
```

Fuente: Elaboración propia

Figura 37. Conectividad R1-S3



Fuente: Elaboración propia

#### Parte 4: Configurar el protocolo de routing dinámico OSPF

##### Paso 1: Configurar OSPF en R1

- Configurar OSPF área 1

```
R1(config)#router ospf 1
```

- Anunciar las redes conectadas directamente

```
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0
```

```
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0
```

```
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
```

```
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
```

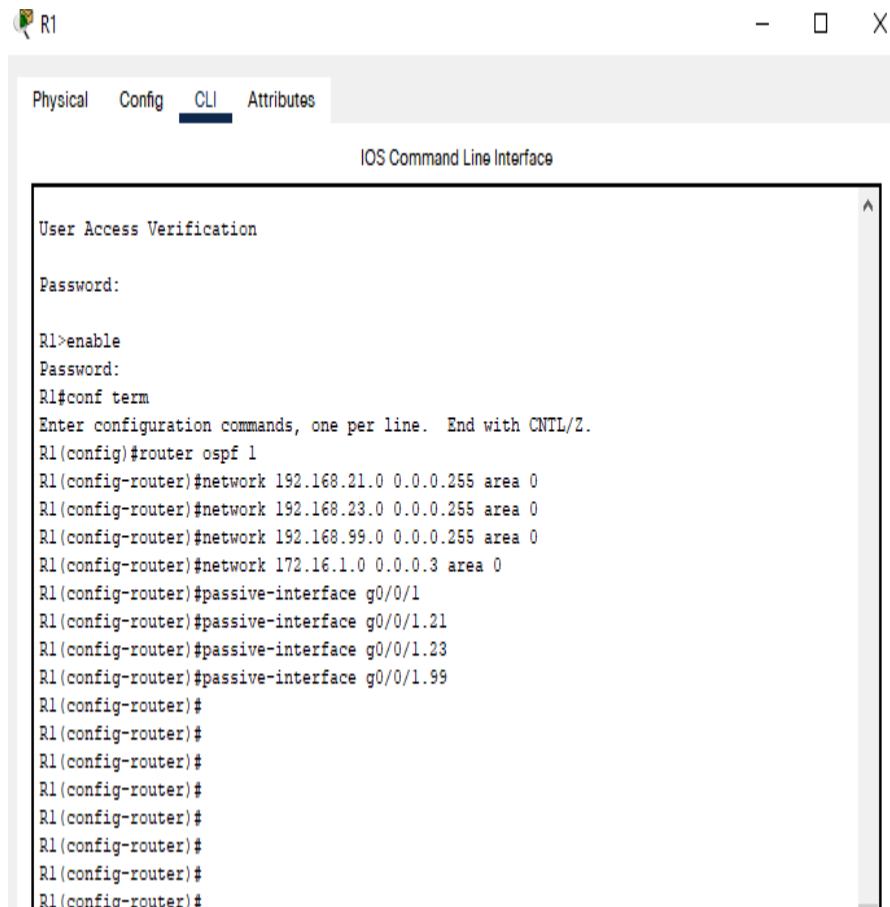
- Establecer todas las interfaces LAN como pasivas

```
R1(config-router)#passive-interface g0/0/1.21
```

```
R1(config-router)#passive-interface g0/0/1.23
```

```
R1(config-router)#passive-interface g0/0/1.99
```

Figura 38. Configuración OSPF en R1



The screenshot shows the CLI of router R1. The tabs at the top are Physical, Config, CLI (selected), and Attributes. The title bar says 'IOS Command Line Interface'. The terminal output is as follows:

```
User Access Verification

Password:

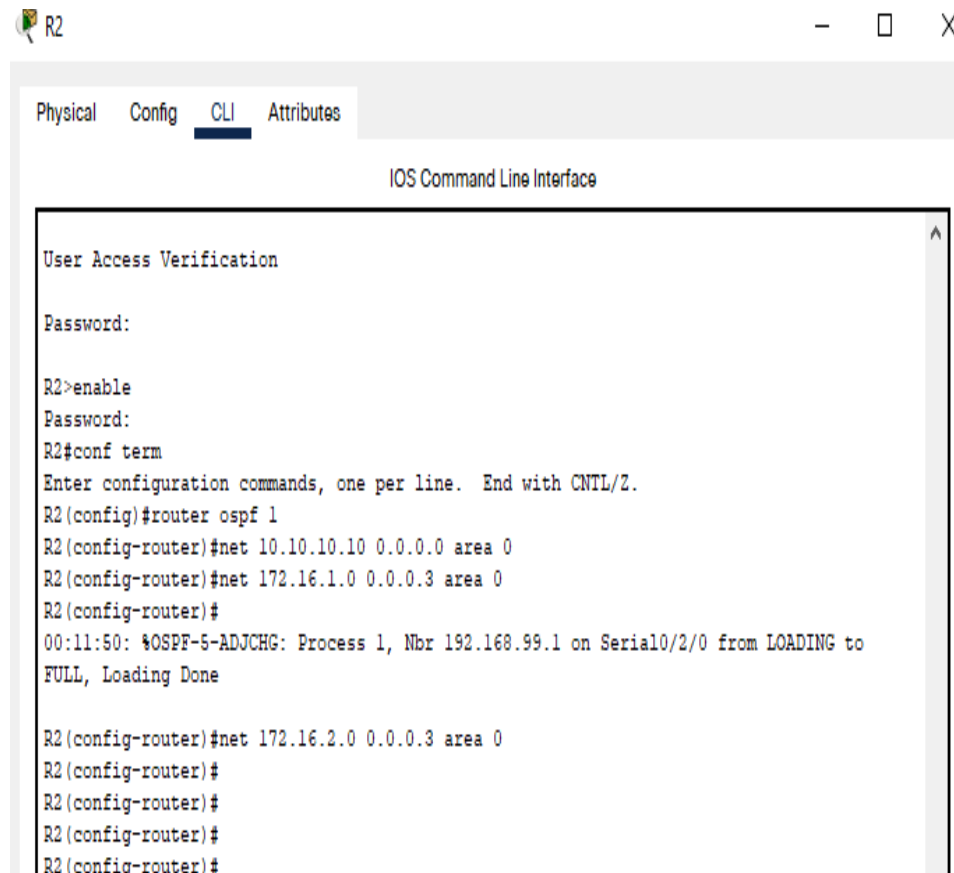
R1>enable
Password:
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
R1(config-router)#passive-interface g0/0/1
R1(config-router)#passive-interface g0/0/1.21
R1(config-router)#passive-interface g0/0/1.23
R1(config-router)#passive-interface g0/0/1.99
R1(config-router)#
R1(config-router)#
R1(config-router)#
R1(config-router)#
R1(config-router)#
R1(config-router)#
R1(config-router)#
R1(config-router)#
```

Fuente: Elaboración propia

## Paso 2: Configurar OSPF en R2

- Configurar OSPF área 1  
R2(config)#router ospf 1
- Anunciar las redes conectadas directamente  
R2(config-router)#network 10.10.10.10 0.0.0.0 area 0  
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0  
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
- Establecer todas las interfaces LAN como pasivas  
R2(config-rtr)#passive-interface loopback 0

Figura 39. Configurar OSPF en R2



The screenshot shows a terminal window titled 'R2' 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:

R2>enable
Password:
R2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#net 10.10.10.10 0.0.0.0 area 0
R2(config-router)#net 172.16.1.0 0.0.0.3 area 0
R2(config-router)#
00:11:50: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.99.1 on Serial0/2/0 from LOADING to FULL, Loading Done
R2(config-router)#net 172.16.2.0 0.0.0.3 area 0
R2(config-router)#
R2(config-router)#
R2(config-router)#
R2(config-router)#
```

Fuente: Elaboración propia

### Paso 3: Configurar OSPFv3 en el R3

- Configurar OSPFv3 área 0

```
R3(config)#router ospf 1
R3(config-rtr)#router-id 3.3.3.3
R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
```

### Anunciar redes IPv6 conectadas directamente

```
R3(config)#int s0/2/0
R3(config-if)#ipv6 ospf 2 area 0
```

- Establecer todas las interfaces LAN

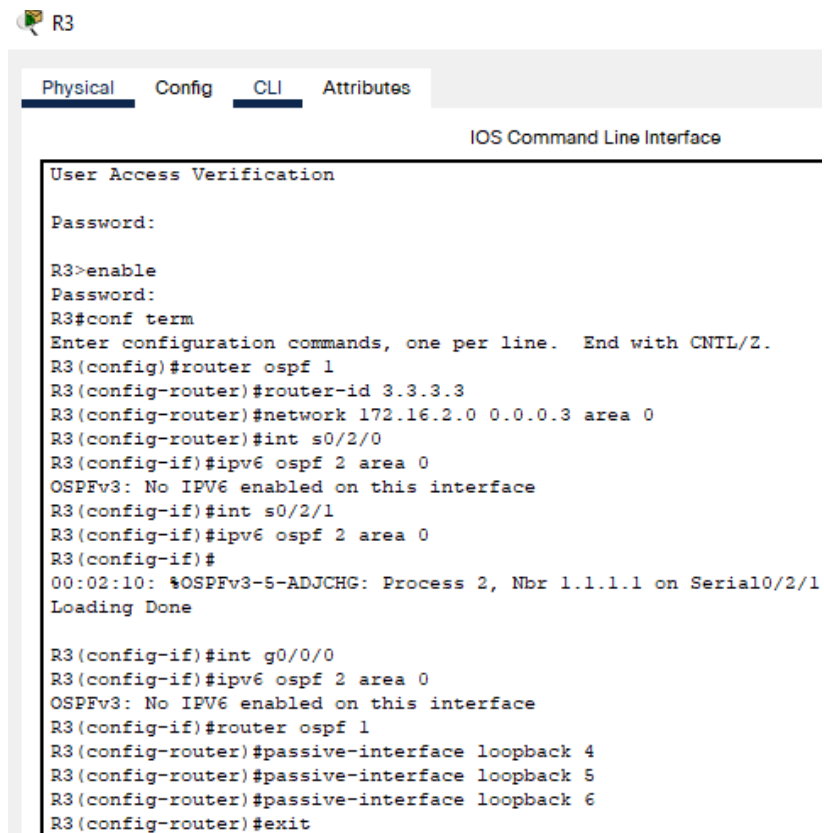
```
R3(config)#int s0/2/1
R3(config-if)#ipv6 ospf 2 area 0
```

```
R3(config)#int g0/0/0
R3(config-if)#ipv6 ospf 2 area 0
```

- Establecer todas las interfaces LAN como pasivas

```
R3(config-rtr)#passive-interface loopback 4
R3(config-rtr)#passive-interface loopback 5
R3(config-rtr)#passive-interface loopback 6
```

Figura 40. Configuración OSPFv3 en R3



```
R3
Physical Config CLI Attributes
IOS Command Line Interface

User Access Verification

Password:

R3>enable
Password:
R3#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
R3(config-router)#int s0/2/0
R3(config-if)#ipv6 ospf 2 area 0
OSPFv3: No IPV6 enabled on this interface
R3(config-if)#int s0/2/1
R3(config-if)#ipv6 ospf 2 area 0
R3(config-if)#
00:02:10: %OSPFv3-5-ADJCHG: Process 2, Nbr 1.1.1.1 on Serial0/2/1
Loading Done

R3(config-if)#int g0/0/0
R3(config-if)#ipv6 ospf 2 area 0
OSPFv3: No IPV6 enabled on this interface
R3(config-if)#router ospf 1
R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
R3(config-router)#exit
```

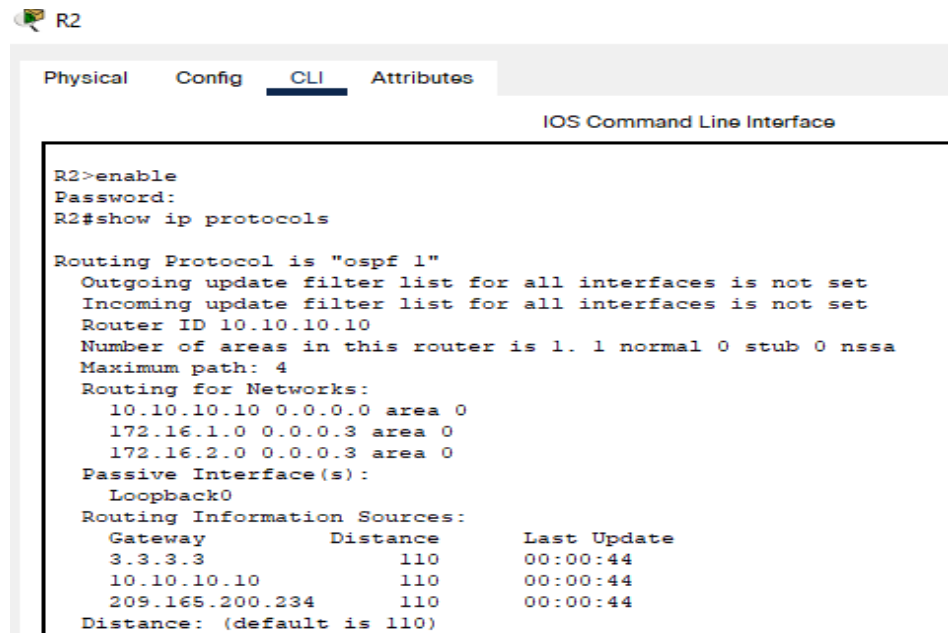
Fuente: Elaboración propia

#### 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:

¿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?

Figura 41. Ver IP Protocolos



```

R2
Physical Config CLI Attributes
IOS Command Line Interface

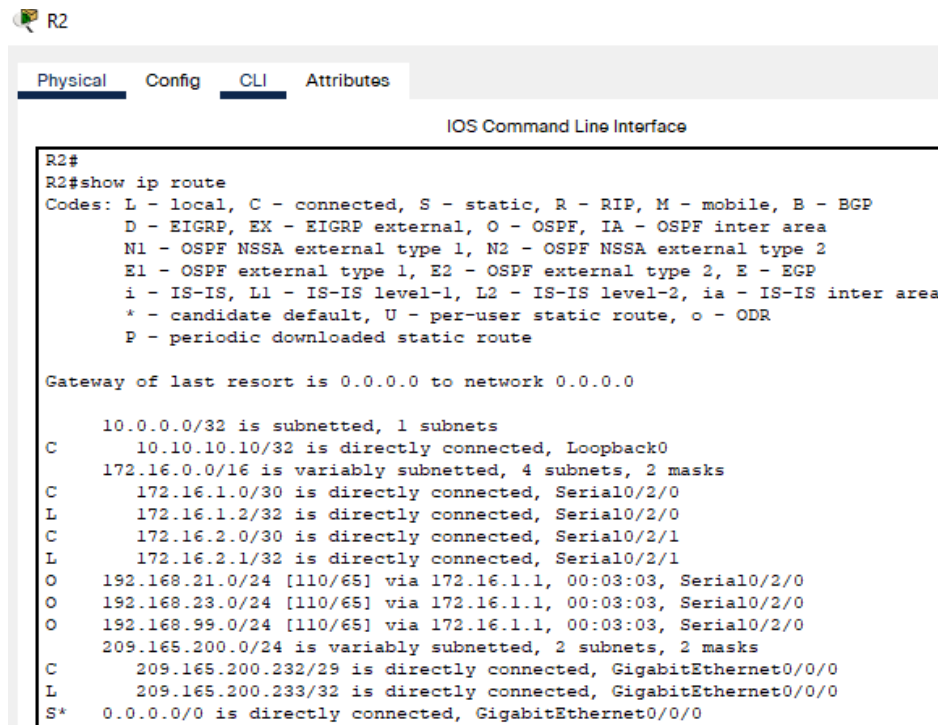
R2>enable
Password:
R2#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.10.10.10
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.10.10.10 0.0.0.0 area 0
    172.16.1.0 0.0.0.3 area 0
    172.16.2.0 0.0.0.3 area 0
  Passive Interface(s):
    Loopback0
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3          110           00:00:44
    10.10.10.10      110           00:00:44
    209.165.200.234  110           00:00:44
  Distance: (default is 110)
  
```

Fuente: Elaboración propia

¿Qué comando muestra solo las rutas OSPF?

Figura 42. Ver IP Routers



```

R2#
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

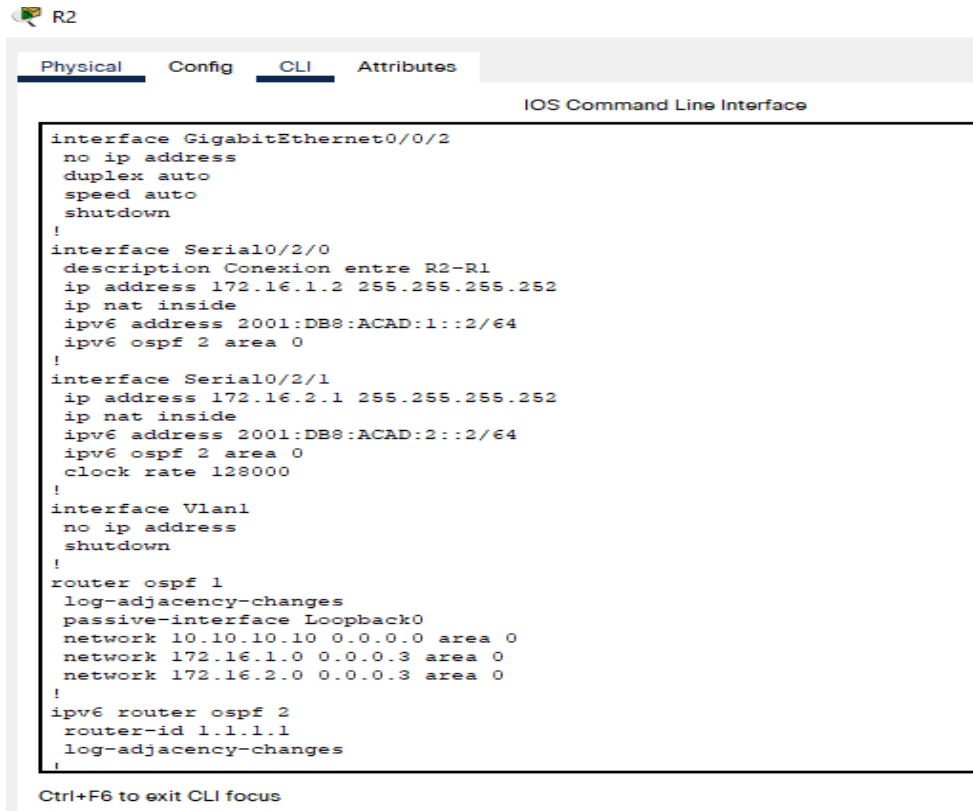
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

    10.0.0.0/32 is subnetted, 1 subnets
C      10.10.10.10/32 is directly connected, Loopback0
    172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C      172.16.1.0/30 is directly connected, Serial0/2/0
L      172.16.1.2/32 is directly connected, Serial0/2/0
C      172.16.2.0/30 is directly connected, Serial0/2/1
L      172.16.2.1/32 is directly connected, Serial0/2/1
O      192.168.21.0/24 [110/65] via 172.16.1.1, 00:03:03, Serial0/2/0
O      192.168.23.0/24 [110/65] via 172.16.1.1, 00:03:03, Serial0/2/0
O      192.168.99.0/24 [110/65] via 172.16.1.1, 00:03:03, Serial0/2/0
    209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C      209.165.200.232/29 is directly connected, GigabitEthernet0/0/0
L      209.165.200.233/32 is directly connected, GigabitEthernet0/0/0
S*    0.0.0.0/0 is directly connected, GigabitEthernet0/0/0
  
```

Fuente: Elaboración propia

¿Qué comando muestra la sección de OSPF de la configuración en ejecución?

Figura 43. Ver OSPF



```

R2
Physical Config CLI Attributes
IOS Command Line Interface

interface GigabitEthernet0/0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/2/0
description Conexion entre R2-R1
ip address 172.16.1.2 255.255.255.252
ip nat inside
ipv6 address 2001:DB8:ACAD:1::2/64
ipv6 ospf 2 area 0
!
interface Serial0/2/1
ip address 172.16.2.1 255.255.255.252
ip nat inside
ipv6 address 2001:DB8:ACAD:2::2/64
ipv6 ospf 2 area 0
clock rate 128000
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
passive-interface Loopback0
network 10.10.10.10 0.0.0.0 area 0
network 172.16.1.0 0.0.0.3 area 0
network 172.16.2.0 0.0.0.3 area 0
!
ipv6 router ospf 2
router-id 1.1.1.1
log-adjacency-changes
!

```

Ctrl+F6 to exit CLI focus

Fuente: Elaboración propia

## Parte 5: Implementar DHCP y NAT para IPv4

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

- Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas

R1(config)#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

R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20

- Crear un pool de DHCP para la VLAN 21

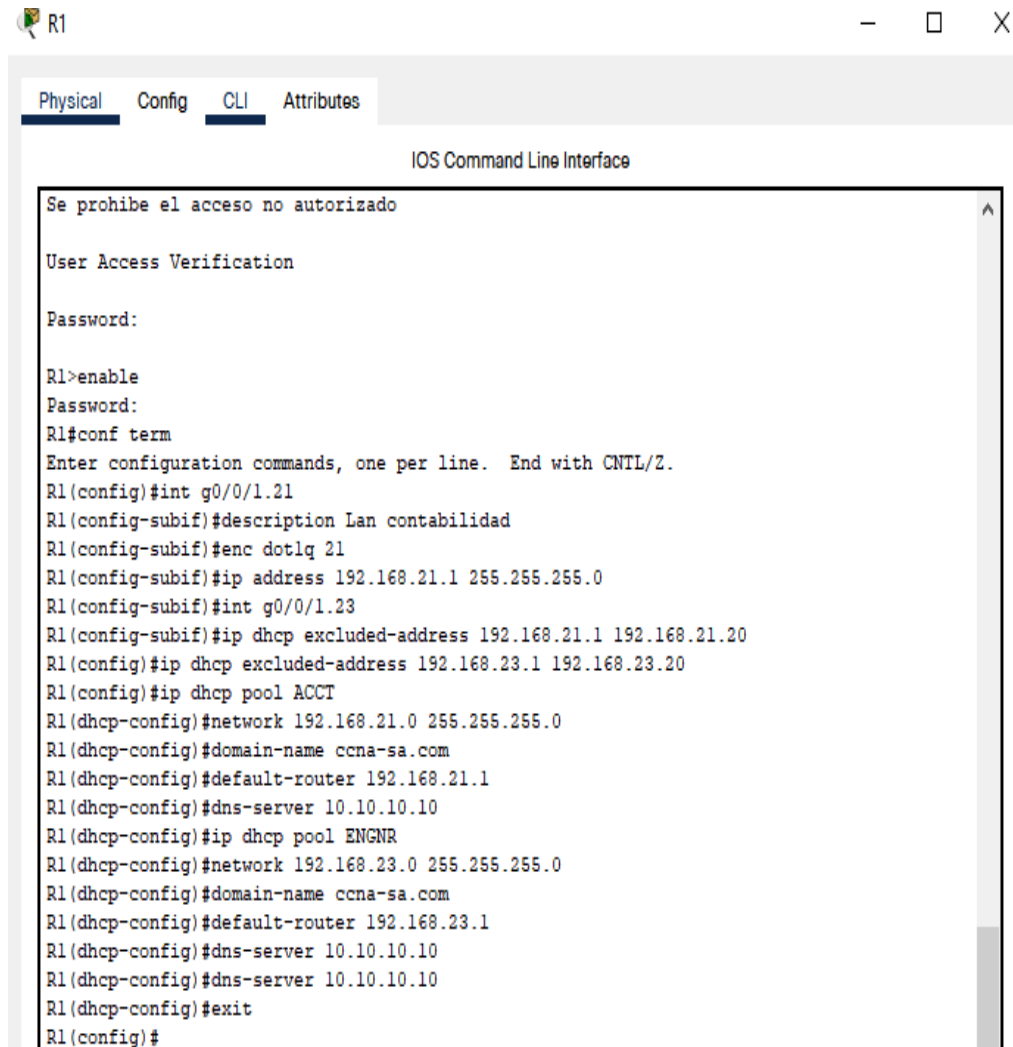
R1(config)#ip dhcp pool ACCT

```
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10
```

- Crear un pool de DHCP para la VLAN 23

```
R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#dns-server 10.10.10.10
```

Figura 44. Configuración DHCP

The image is a screenshot of a network device's command-line interface (CLI) for a router named R1. The window has a title bar with 'R1' and standard window controls. Below the title bar are tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' being the active tab. The main area is titled 'IOS Command Line Interface'. It shows a series of commands entered at the prompt 'R1>' and the corresponding system responses. The commands include enabling privileged EXEC mode, entering global configuration mode, configuring interfaces g0/0/1.21 and g0/0/1.23 with IP addresses and descriptions, and configuring two DHCP pools: 'ACCT' for the 192.168.21.0/24 network and 'ENGNR' for the 192.168.23.0/24 network. Both pools are configured with the domain 'ccna-sa.com', a default router of 192.168.21.1 (for ACCT) or 192.168.23.1 (for ENGNR), and DNS servers at 10.10.10.10. The session ends with the 'exit' command, returning to the 'R1(config)#' prompt.

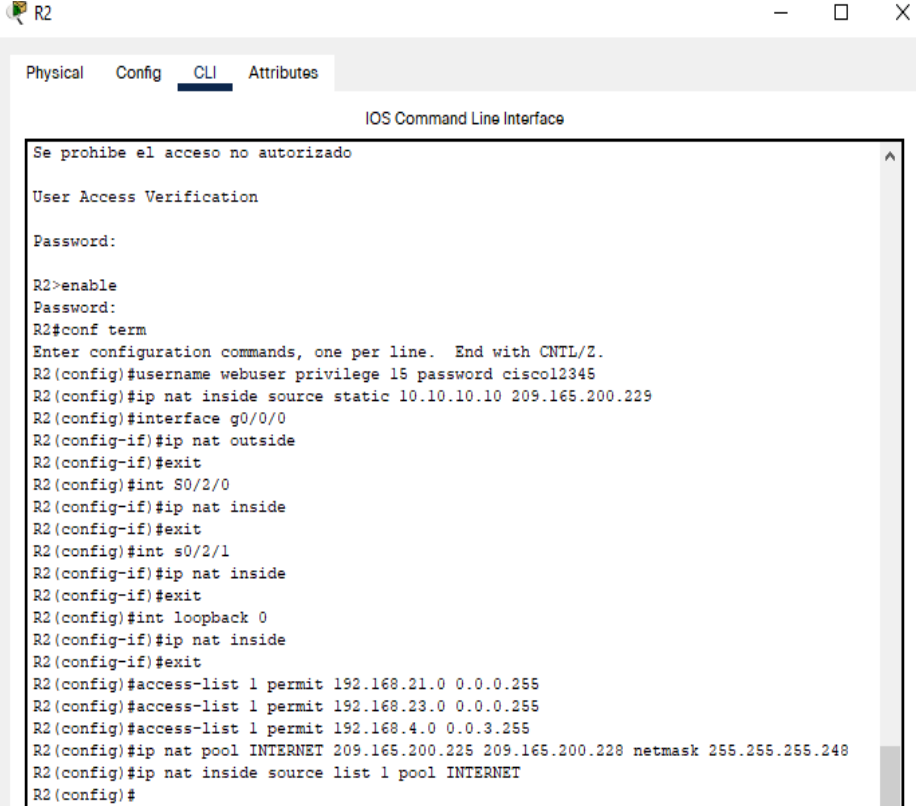
```
R1>enable
Password:
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/0/1.21
R1(config-subif)#description Lan contabilidad
R1(config-subif)#enc dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#int g0/0/1.23
R1(config-subif)#ip 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)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#ip dhcp pool ENGNR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#exit
R1(config)#
```

Fuente: Elaboración propia

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

- Crear una base de datos local con una cuenta de usuario  
R2(config)#username webuser privilege 15 password cisco12345
- Habilitar el servicio del servidor HTTP No soportado Packet Tracer  
R2(config)#ip http server
- Configurar el servidor HTTP para utilizar la base de datos local para la autenticación  
R2(config)#ip http authentication local No soportado Packet Tracer
- Crear una NAT estática al servidor web.  
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
- Asignar la interfaz interna y externa para la NAT estática  
R2(config)#interface g0/0/0  
R2(config-if)#ip nat outside  
R2(config-if)#exit  
  
R2(config)#int S0/2/0  
R2(config-if)#ip nat inside  
R2(config-if)#exit  
  
R2(config)#int s0/2/1  
R2(config-if)#ip nat inside  
R2(config-if)#exit  
  
R2(config)#int loopback 0  
R2(config-if)#ip nat inside
- Configurar la NAT dinámica dentro de una ACL privada  
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255  
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255  
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
- Defina el pool de direcciones IP públicas utilizables.  
R2(config)#ip nat inside source list 1 pool INTERNET

Figura 45. NAT

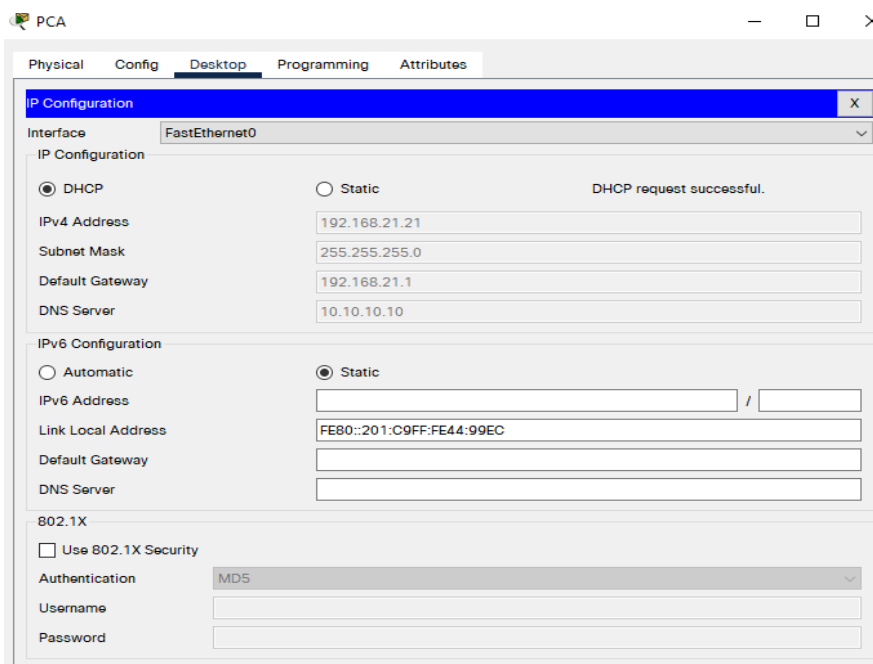


```

R2
Physical Config CLI Attributes
IOS Command Line Interface
Se prohíbe el acceso no autorizado
User Access Verification
Password:
R2>enable
Password:
R2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#username webuser privilege 15 password cisco12345
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
R2(config)#interface g0/0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#int s0/2/0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#int s0/2/1
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#int loopback 0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#
  
```

Fuente: Elaboración propia

Figura 46. DHCP PC-A



PCA

Physical Config Desktop Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☒ DHCP ☐ Static DHCP request successful.

IPv4 Address: 192.168.21.21

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.21.1

DNS Server: 10.10.10.10

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::201:C9FF:FE44:99EC

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

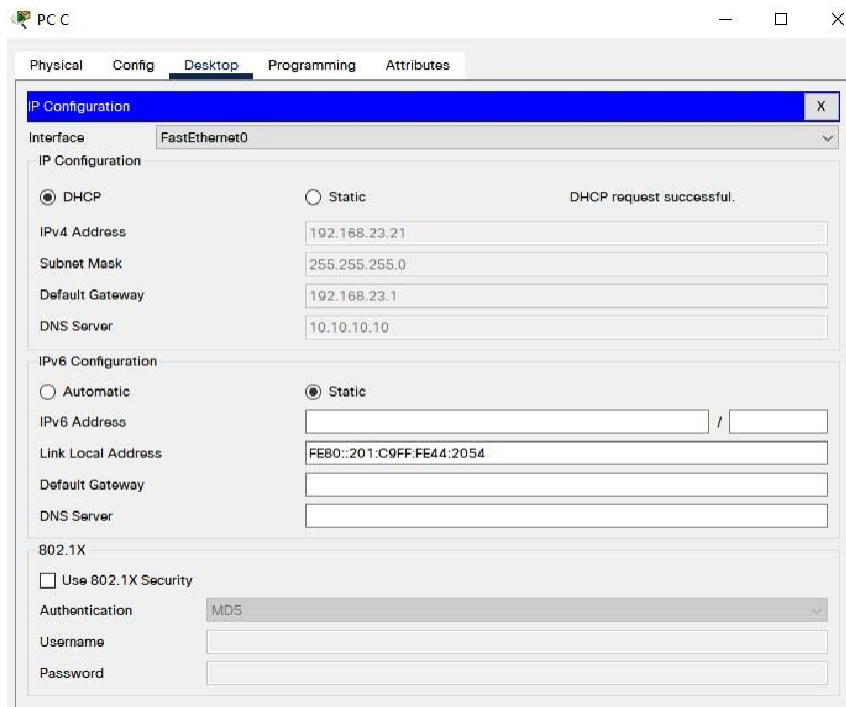
Authentication: MD5

Username:

Password:

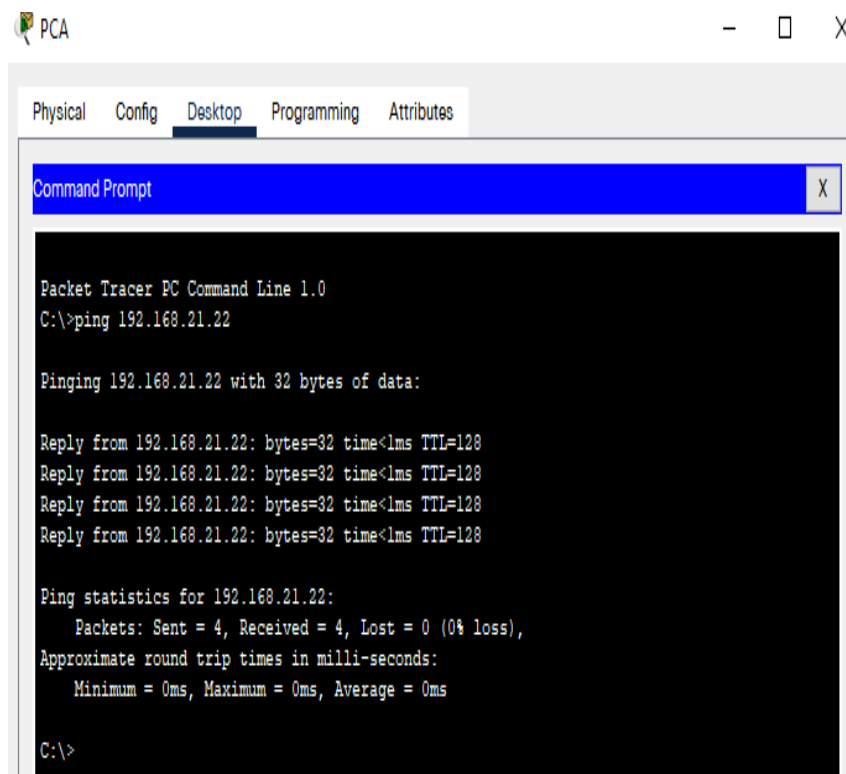
Fuente: Elaboración propia

Figura 47. DHCP PC-B



Fuente: Elaboración propia

Figura 48. Conectividad S-PC



Fuente: Elaboración propia

## Parte 6: Configurar NTP

- Ajuste la fecha y hora en R2  
R2(config)#clock set 09:00:00 05 march 2016
- Configure R2 como un maestro NTP.  
R2(config)#ntp master 5
- Configurar R1 como un cliente NTP.  
R1(config)#ntp server 172.16.1.2
- Configure R1 para actualizaciones de calendario periódicas con hora NTP.  
R1(config)#ntp update-calendar
- Verifique la configuración de NTP en R1  
R2#sh clock

Figura 49. NTP



The screenshot shows a terminal window titled 'R2' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The text in the terminal is as follows:

```
Se prohíbe el acceso no autorizado
User Access Verification
Password:
R2>enable
Password:
R2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp server 172.16.1.2
R2(config)#ntp update-calendar
R2(config)#ntp master 5
```

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

- Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2

```
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#deny any
```

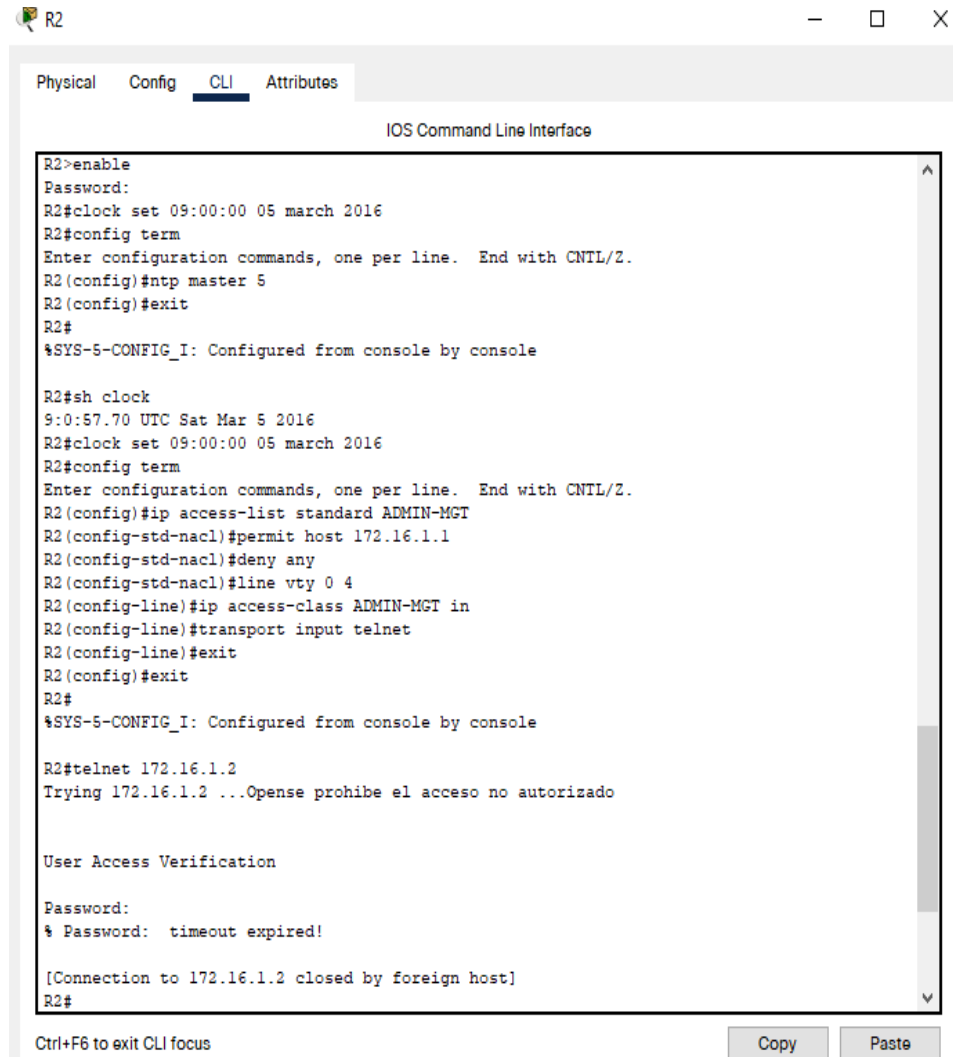
- Aplicar la ACL con nombre a las líneas VTY

```
R2(config)#line vty 0 4
R2(config-line)#ip access-class ADMIN-MGT in
```

- Permitir acceso por Telnet a las líneas de VTY

```
R2(config-line)#transport input telnet
```

Figura 50. Telnet



```
R2>enable
Password:
R2#clock set 09:00:00 05 march 2016
R2#config term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp master 5
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#sh clock
9:0:57.70 UTC Sat Mar 5 2016
R2#clock set 09:00:00 05 march 2016
R2#config term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#deny any
R2(config-std-nacl)#line vty 0 4
R2(config-line)#ip access-class ADMIN-MGT in
R2(config-line)#transport input telnet
R2(config-line)#exit
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#telnet 172.16.1.2
Trying 172.16.1.2 ...Opense prohíbe el acceso no autorizado

User Access Verification

Password:
% Password: timeout expired!

[Connection to 172.16.1.2 closed by foreign host]
R2#
```

Fuente: Elaboración propia

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

- Verificar que la ACL funcione como se espera

```
R2#sh access-lists
```

- Restablecer los contadores de una lista de acceso

```
R2#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?

```
R2 (config)#interface fa0/1  
R2 (config-if)#ip access-group 1 out
```

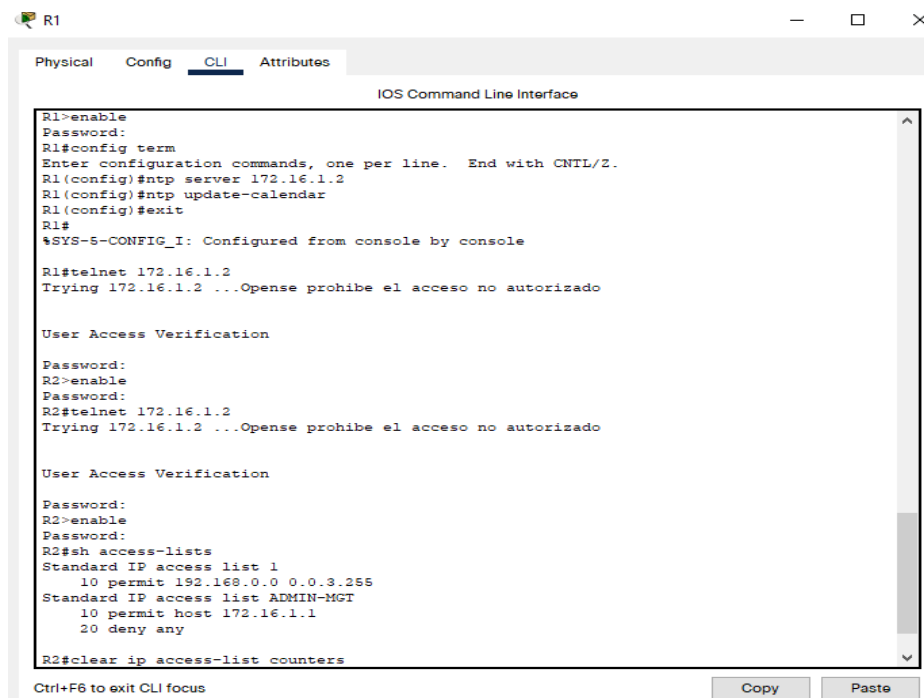
- ¿Con qué comando se muestran las traducciones NAT?

```
R2 (config)#show ip nat translations
```

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

```
R2(config)#clear ip nat translation
```

Figura 51. Acceso verificación



```
R1>enable
Password:
R1#config 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)#exit
R1#
*SYS-5-CONFIG_I: Configured from console by console

R1#telnet 172.16.1.2
Trying 172.16.1.2 ...Opense prohíbe el acceso no autorizado

User Access Verification

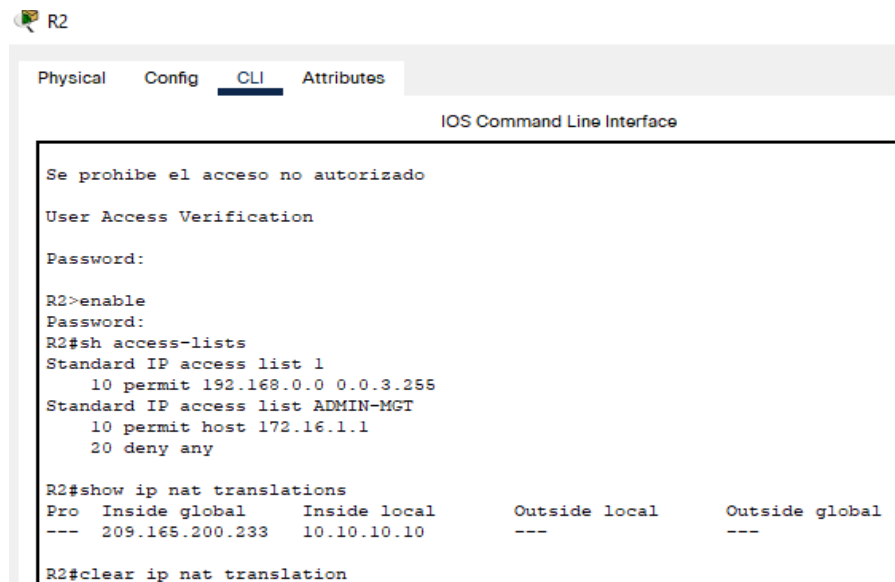
Password:
R2>enable
Password:
R2#telnet 172.16.1.2
Trying 172.16.1.2 ...Opense prohíbe el acceso no autorizado

User Access Verification

Password:
R2>enable
Password:
R2#sh access-lists
Standard IP access list 1
 10 permit 192.168.0.0 0.0.3.255
Standard IP access list ADMIN-MGT
 10 permit host 172.16.1.1
 20 deny any
R2#clear ip access-list counters
```

Fuente: Elaboración propia

Figura 52. Verificación ACL



```

R2
Physical Config CLI Attributes
IOS Command Line Interface

Se prohíbe el acceso no autorizado
User Access Verification
Password:

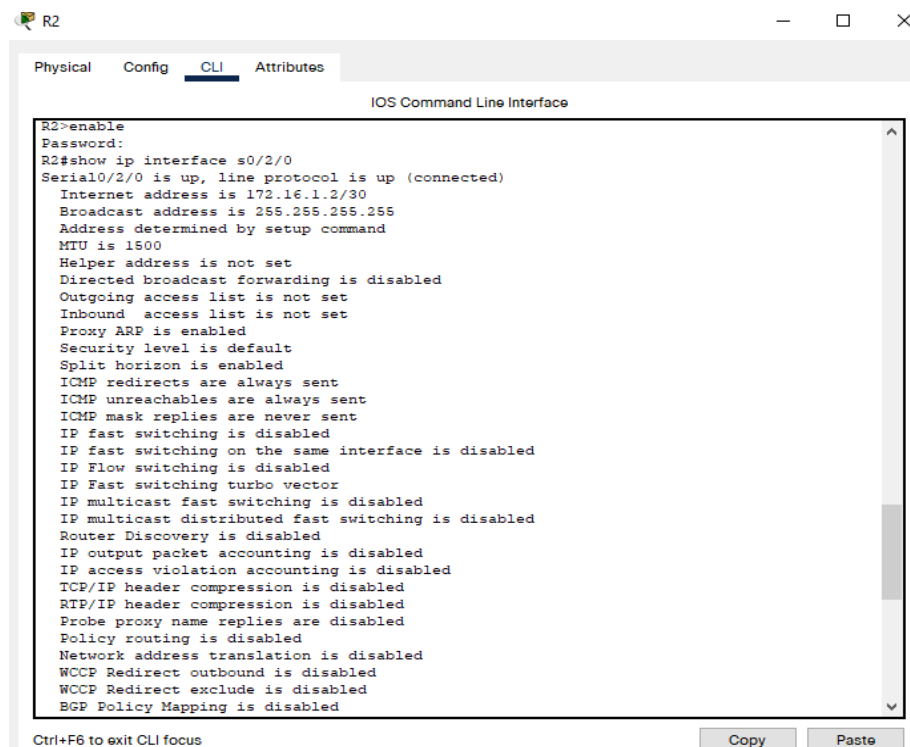
R2>enable
Password:
R2#sh access-lists
Standard IP access list 1
  10 permit 192.168.0.0 0.0.3.255
Standard IP access list ADMIN-MGT
  10 permit host 172.16.1.1
  20 deny any

R2#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
---  209.165.200.233      10.10.10.10      ---                ---

R2#clear ip nat translation
  
```

Fuente: Elaboración propia

Figura 53. Verificación interfaces



```

R2
Physical Config CLI Attributes
IOS Command Line Interface

R2>enable
Password:
R2#show ip interface s0/2/0
Serial0/2/0 is up, line protocol is up (connected)
  Internet address is 172.16.1.2/30
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500
  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
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
  
```

Fuente: Elaboración propia

## **CONCLUSIONES**

En el desarrollo de las prácticas de laboratorio de redes, se adquiere conocimientos importantes con muchas ventajas, porque administra las direcciones IP de manera práctica para ser eficaz evitando el riesgo de duplicidad de las IP en la red en los problemas de conexión.

Con esta actividad, se pone en práctica las configuraciones de conectividad de redes internet con las diferentes topologías en los dispositivos en cada red, se conoce los comandos fundamentales para el funcionamiento correcto de cada dispositivo.

Por las temáticas del curso, se profundiza los escenarios en las configuraciones dadas direccionamiento, segmentación y seguridad, para realizar las respectivas simulaciones de conectividad por medio de la codificación requerida para el funcionamiento de la red.

El diplomado CCNA CISCO es muy importante para la sociedad en el desarrollo en los entornos de redes comunicaciones con sus características y funcionalidades en las diferentes topologías.

## BIBLIOGRAFÍA

BAREÑO, Gutiérrez, R., Núñez, W. N., Urrea, S. C., Osorio, H. S., & Acosta, N. D. (2016). Revisión de la seguridad en la implementación de servicios sobre IPv6. Inge Cuc, 12(1), 86-93.

BAREÑO, Gutiérrez, R., Urrea, S. C., Núñez, W. N., Sarmiento, H., Acosta, N. D., & Sánchez, G. G. V. (2015). Análisis de la seguridad en la implementación de servicios corporativos sobre el protocolo IPV. Revista de Tecnología, 14(1), 127-138.

CISCO. (2019). Exploración de la red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1>

CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3>

CISCO. (2019). Capa de red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6>

CISCO. (2019). Direccionamiento IP. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7>

CISCO. (2019). División de redesIP en subredes. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8>

CISCO. (2019). Routing Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#3>

CISCO. (2019). Redes Conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4>

CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5>

CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6>

CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7>

CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8>

CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9>

CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10>