

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

LIBARDO POTOSI SANDOVAL

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

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

LIBARDO POTOSÍ SANDOVAL

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

DIRECTORA:  
ING. NANCY AMPARO GUACA GIRON

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

## NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

POPAYÁN, 28 de noviembre de 2021

## **AGRADECIMIENTOS**

Gracias Dios por todos los esfuerzos y logros alcanzados en el proceso académico, cada uno de los cuales es importante para continuar con nuestros proyectos de vida.

Expreso mis más sinceros agradecimiento a la directora de este proyecto Ing. Nancy Amparo Guaca por su acompañamiento que nos ha brindado en el transcurso de este Diplomado, también al cuerpo de tutores por ser parte de mi proceso formativo.

Expreso mi más sincera gratitud a la Universidad Nacional Abierta y a Distancia UNAD, por haberme permitido crecer de manera integral en lo profesional y en el personal.

Por ultimo agradecemos a la base de todo, a nuestro familiares, en especial a nuestros padres, que son el motor de arranque y nuestra mejor motivación, muchas gracias por su paciencia, compresión y colaboración.

## **CONTENIDO**

|                        |    |
|------------------------|----|
| AGRADECIMIENTOS .....  | 4  |
| CONTENIDO.....         | 5  |
| LISTA DE TABLAS .....  | 6  |
| LISTA DE FIGURAS ..... | 7  |
| GLOSARIO .....         | 9  |
| RESUMEN .....          | 10 |
| ABSTRACT .....         | 11 |
| INTRODUCCIÓN .....     | 12 |
| DESARROLLO.....        | 13 |
| 1. ESCENARIO 1 .....   | 13 |
| 2. ESCENARIO 2 .....   | 27 |
| CONCLUSIONES .....     | 64 |
| BIBLIOGRAFÍA .....     | 65 |

## LISTA DE TABLAS

|  |    |
|--|----|
| Tabla 1. Direccionamiento del escenario 1 .....                            | 14 |
| Tabla 2. Subnetting .....  | 16 |
| Tabla 3. Tareas de configuración para el Router R1.....                    | 16 |
| Tabla 4. Tareas de configuración para el Switch S1 .....                   | 19 |
| Tabla 5. Configuración de red de la PC-A.....                              | 21 |
| Tabla 6. Configuración de red de la PC-B.....                              | 22 |
| Tabla 7. Reinicio y verificación de Router y Switches del escenario 2..... | 28 |
| Tabla 8. Configuración del servidor.....                                   | 28 |
| Tabla 9. Configuración del Router R1 .....                                 | 29 |
| Tabla 10. Configuración del Router R2 .....                                | 31 |
| Tabla 11. Configuración del Router R3 .....                                | 34 |
| Tabla 12. Configuración del Switch S1 .....                                | 36 |
| Tabla 13. Configuración del Switch S3 .....                                | 38 |
| Tabla 14. Verificación de la conectividad de los dispositivos .....        | 40 |
| Tabla 15. Configuración de la seguridad del Switch S1 .....                | 42 |
| Tabla 16. Configuración de la seguridad del Switch S3 .....                | 44 |
| Tabla 17. Configuración de la seguridad del Router R1.....                 | 45 |
| Tabla 18. Verificación de la conectividad entre switches y R1 .....        | 45 |
| Tabla 19. Configuración OSPF en el Router R1 .....                         | 48 |
| Tabla 20. Configuración OSPF en el Router R2 .....                         | 49 |
| Tabla 21. Verificación información de OSPFv3 en el Router R2.....          | 51 |
| Tabla 22. Verificación información de OSPFv3 en el Router R3.....          | 51 |
| Tabla 23. Verificación información de OSPF .....                           | 52 |
| Tabla 24. Configuración R1 como servidor DHCP para VLAN 21 y 23.....       | 54 |
| Tabla 25. Configuración NAT estática y dinámica en R2 .....                | 56 |
| Tabla 26. Verificación del protocolo DHCP y NAT estática .....             | 58 |
| Tabla 27. Configuración NTP en R1 .....                                    | 60 |
| Tabla 28. Restringir el acceso a las líneas VTY en Router R2.....          | 61 |
| Tabla 29. Comandos de verificación .....                                   | 63 |

## LISTA DE FIGURAS

|   |    |
|---|----|
| Figura 1. Topología Escenario 1 .....                               | 13 |
| Figura 2. Construcción de la red de acuerdo con la topología .....  | 13 |
| Figura 3. Configuración para el Router R1 .....                     | 18 |
| Figura 4. Configuración para el Switch S1 .....                     | 20 |
| Figura 5. Red del host con el comando ipconfig /all de la PC-A..... | 22 |
| Figura 6. Red del host con el comando ipconfig /all de la PC-B..... | 23 |
| Figura 7. Configuración host PC-A.....                              | 23 |
| Figura 8. Configuración host PC-B.....                              | 24 |
| Figura 9. Conectividad desde LAN 1- PC-A a todos los equipos .....  | 24 |
| Figura 10. Conectividad desde LAN 1- S1 a todos los equipos.....    | 25 |
| Figura 11. Conectividad desde LAN 2- R1 a todos los equipos .....   | 25 |
| Figura 12. Ping desde LAN 2- PC-B a todos los equipos .....         | 26 |
| Figura 13. Acceso remoto desde PC-B a R1.....                       | 26 |
| Figura 14. Acceso remoto desde PC-A a S1.....                       | 26 |
| Figura 15. Topología del escenario 2 .....                          | 27 |
| Figura 16. Configuración del servidor.....                          | 29 |
| Figura 17. Configuración inicial R1.....                            | 30 |
| Figura 18. Configuración inicial R2.....                            | 32 |
| Figura 19. Configuración inicial R3.....                            | 35 |
| Figura 20. Configuración inicial S1 .....                           | 37 |
| Figura 21. Configuración inicial S3 .....                           | 39 |
| Figura 22. Ping de R1 a R2 .....                                    | 41 |
| Figura 23. Ping de R2 a R3 .....                                    | 41 |
| Figura 24. Conectividad PC a Gateway predeterminado .....           | 42 |
| Figura 25. Ping S1 a VLAN Administración .....                      | 46 |
| Figura 27. Ping de S1 a VLAN 21 .....                               | 47 |
| Figura 28. Ping de S3 a la VLAN 23.....                             | 47 |
| Figura 29. Configuración OSPF en el R1 .....                        | 48 |
| Figura 30. Configuración OSPF en el R2 .....                        | 50 |
| Figura 31. Comando para ver ID del proceso OSPF .....               | 53 |
| Figura 32. Comando para mostrar solo las rutas OSPF.....            | 53 |

|   |    |
|---|----|
| Figura 33. Show ip ospf database en R1 .....                              | 54 |
| Figura 34. Configuración R1 como servidor de DHCP para VLAN 21 y 23 ..... | 55 |
| Figura 35. Configuración NAT estática y dinámica de R2 .....              | 57 |
| Figura 36. PC-A con DHCP .....  | 58 |
| Figura 37. PC-C con DHCP .....  | 58 |
| Figura 38. Ping PC-A a PC-C .....   | 59 |
| Figura 39. Acceder al servidor web desde PC-A .....                       | 59 |
| Figura 40. Acceder al servidor web desde PC-C .....                       | 60 |
| Figura 41. Configuración de NTP en R1 .....                               | 61 |
| Figura 42. Verificación de ACL .....                                      | 62 |
| Figura 43. Verificación desde R1 A R2 mediante conexión SSH .....         | 62 |
| Figura 44. Verificación R3 A R2 mediante conexión SSH .....               | 62 |

## GLOSARIO

**IP:** Es una forma particular de expresar las direcciones de red y sus máscaras a partir de identificar solamente la cantidad de bits que se encuentran en uno en la máscara de subred.

**DNS:** La sigla DNS proviene de la expresión inglesa Domain Name System: es decir, Sistema de Nombres de Dominio. Se trata de un método de denominación empleado para nombrar a los dispositivos que se conectan a una red a través del IP (Internet Protocol o Protocolo de Internet).

**VLAN:** Es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.

**DHCP:** Es un servidor que usa protocolo de red de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

**SUBRED:** Una subred es un rango de direcciones lógicas.

**OSPF:** Es un protocolo de direccionamiento de tipo enlace estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta (SPF). OSPF es un protocolo de pasarela interior (IGP). OSPF puede recalcular las rutas en muy poco tiempo cuando cambia la topología de la red.

**NAT:** En redes, NAT significa Network Adress Translation o Traducción de direcciones de red en español. Se trata de un sistema que se utiliza en las redes bajo el protocolo IP y que nos permite el intercambio de paquetes entre dos redes que tienen asignadas mutuamente direcciones IP incompatibles.

**LÍNEA VTY:** son las líneas de terminal virtual del router, que se utilizan solamente para controlar las conexiones Telnet entrantes. Son virtuales en el sentido que son una función de software; no hay hardware relacionado con ellas. Aparecen en la configuración como line vty 0 4.

## RESUMEN

Hoy en día las telecomunicaciones se encuentra en la gran mayoría de las organizaciones y de acuerdo a unas políticas deben tener cierto nivel de seguridad y estabilidad para soportar un sistema, para el ejercicio la directora a cargo del grupo propone dos escenarios con características y requerimientos específicos mediante el cual se pone en práctica las competencias y conocimientos adquiridos durante curso.

Durante el proceso se tiene en cuenta saber identificar las herramientas de supervisión y protocolos de administración de redes disponibles en el IOS para resolver los problemas de las redes de datos, evaluando dos subredes con la cantidad requerida de hosts por medio de la configuración de los siguientes dispositivos router, switch, y PC en esquema de direccionamiento en IPv4 utilizando la herramienta de simulación Cisco Packet Tracer.

Al desarrollar el escenario dos se conceptualiza y se aplica la temática de conectividad IPv4 e IPv6, seguridad de switch enrutamiento inter VLAN, OSPFv2, DHCP, NAT dinámica / estática y listas de control de acceso (ACL).

**Palabras Clave:** CISCO, Protocolos, Switch, Router, Redes, OSPFv2, IPv4, IPv6, Hosts, Packet Tracer.

## ABSTRACT

Today telecommunications is found in the vast majority of organizations and according to some policies they must have a certain level of security and stability to support a system, for the exercise director in charge of the group proposes scenarios with specific characteristics and requirements through which puts into practice the skills and knowledge acquired during the course.

During the process, knowing how to identify the monitoring tools and network management protocols available in the IOS is taken into account to solve data network problems, evaluating two subnets with the required number of hosts by configuring the following router, switch, and PC devices in IPv4 addressing scheme using the Cisco Packet Tracer simulation tool.

When developing scenario two, the themes of IPv4 and IPv6 connectivity, switch security, routing between VLANs, OSPFv2, DHCP, dynamic / static NAT and access control lists (ACLs) are conceptualized and applied.

**Keywords:** CISCO, Protocols, Switch, Router, Networks, OSPFv2, IPv4, IPv6, Hosts, Packet Tracer.

## INTRODUCCIÓN

Este proyecto se crea en base al diseño e implementación de soluciones integradas LAN / WAN, las cuales son las bases primordiales hoy en día para el desarrollo de los futuros trabajos con lo cual se fortalecerá cada una de las distintas competencias cognitivas para nuestro desempeño profesional, permitiéndonos dar soluciones en el área de redes informáticas, implementando tecnologías como CISCO.

El análisis se cumple teniendo en cuenta la topología del primer escenario, que consta mediante la configuración de dos subredes donde se le realizará el respectivo direccionamiento y uso de subnetting de LAN1 con 100 host y la LAN2 50 hosts, haciendo uso de los siguientes dispositivos un router, un switch y equipos PC, el cual se debe diseñar el esquema de direccionamiento en IPv4.

Dentro del cuerpo del informe se encuentra el segundo escenario donde se verá evidenciado soluciones a situaciones o ejercicios previos, usando comandos de configuración IOS en router con direccionamiento IPv4 e IPv6 donde se prioriza en la seguridad de switch, enrutamiento inter VLAN, OSPFv2, DHCP, NAT dinámica / estática y listas de control de acceso (ACL) previo a la configuración de dispositivos de networking.

Logrando una aplicación directa a las situaciones dadas por la tutoría del curso, permitiéndonos adquirir nuevos conocimientos, habilidades y destrezas a través del software Packet Tracer, donde es una herramienta de aprendizaje y simulación de redes interactiva de Cisco CCNA y la UNAD donde se llevó a cabo los dos escenarios propuestos a continuación.

# DESARROLLO

## 1. ESCENARIO 1

Figura 1. Topología Escenario 1



Fuente: Tomado de Prueba de habilidades CCNA 2021, Cisco Academy

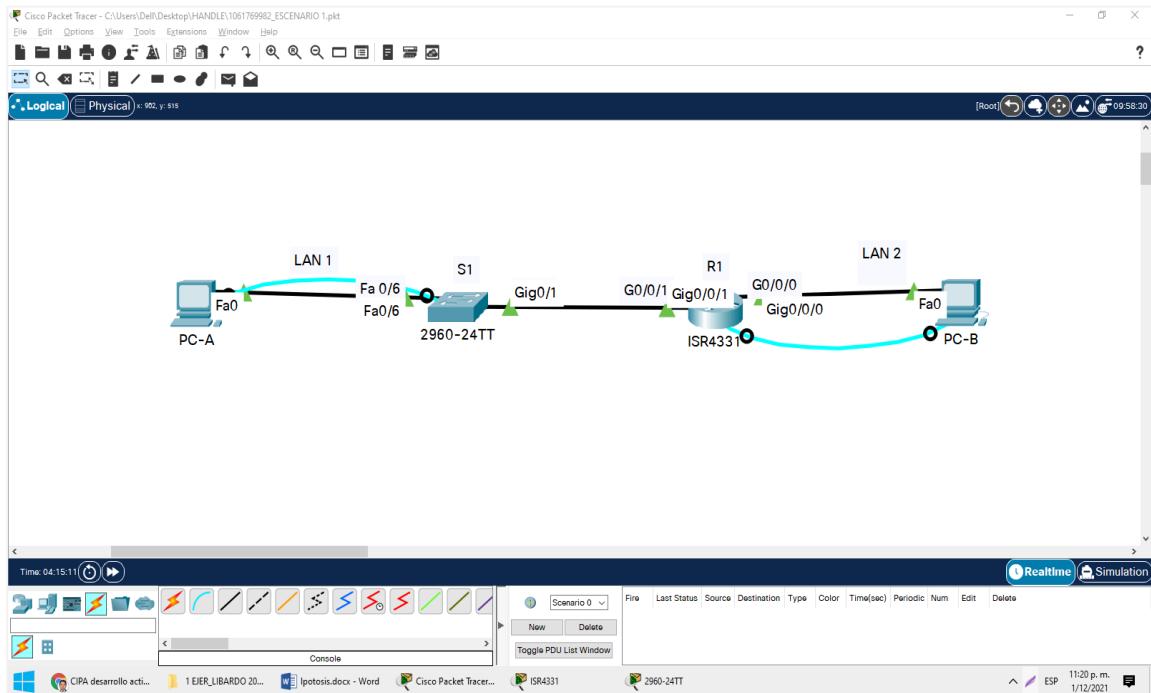
## Aspectos básicos de la situación

En el desarrollo del caso de estudio usted 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).

## Parte 1: Construya la Red

En el simulador construya la red de acuerdo con la topología lógica que se plantea en la figura 1, cablee conforme se indica en la topología, y conecte los equipos de

Figura 2. Construcción de la red de acuerdo con la topología



Fuente: Elaboración propia

**Parte 2: Desarrolle el esquema de direccionamiento IP**

Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento.

Tabla 1. Direccionamiento del escenario 1

| <b>Ítem</b>                       | <b>Requerimiento</b>   |
|-----------------------------------|--|
| Dirección de Red                  | 192.168.82.0 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<br>192.168.82.1              |
| R1 G0/0/0                         | Primera dirección de host de la subred LAN2<br>192.168.82.129            |
| S1 SVI                            | Segunda dirección de host de la subred LAN1<br>192.168.82.2              |
| PC-A                              | Última dirección de host de la subred LAN1<br>192.168.82.126             |
| PC-B                              | Última dirección de host de la subred LAN2<br>192.168.82.190             |

Fuente: Elaboración propia

Se tiene en cuenta que los dos últimos dígitos de la cédula 82

192.168.82.0 /24

Para la LAN 1 se tiene en cuenta 100 host por lo tanto para satisfacer los 100 host

$$\begin{array}{cccccccc} 2^7 & 2^6 & 2^5 & 2^4 & 2^3 & 2^2 & 2^1 & 2^0 \\ 128 & 64 & 32 & 16 & 8 & 4 & 2 & 1 \end{array}$$

Por lo anterior se tiene en cuenta  $2^7 - 2 = 126$  host

$$\begin{array}{c|ccccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \text{Subred} & & & & & & & & 7 \text{ host} \end{array}$$

La nueva máscara de subred es la siguiente:

1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 . 1 0 0 0 0 0 0 0  
255 . 255 . 255 . 128

Debido a esto la dirección de la red es la siguiente:

192.168.82.0 /25

Para la LAN 1 de 100 host la dirección es 192.168.82.0, y para la LAN 2 de 50 host la dirección de red es 192.168.82.128, se toma  $256-128=128$  donde es el incremento para la siguiente subred.

Para la LAN 2 de 50 host se tiene en cuenta la dirección de red 192.168.82.128, como se debe satisfacer los 50 host

$$\begin{array}{cccccccc} 2^7 & 2^6 & 2^5 & 2^4 & 2^3 & 2^2 & 2^1 & 2^0 \\ 128 & 64 & 32 & 16 & 8 & 4 & 2 & 1 \end{array}$$

Se tiene en cuenta  $2^6 - 2 = 62$  host

$$\begin{array}{c|ccccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \text{Subred} & & & & & & & & 6 \text{ host} \end{array}$$

Nueva máscara de subred es la siguiente:

1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 . 1 1 0 0 0 0 0 0  
255 . 255 . 255 . 192

Debido a esto la dirección de la red es la siguiente:

192.168.82.128 /25

Tabla 2. Subnetting

| Host | Dirección de red  | Máscara         | Primer IP disponible | Último IP disponible | Broadcast      |
|------|-------------------|-----------------|----------------------|----------------------|----------------|
| 100  | 192.168.82.0/25   | 255.255.255.128 | 192.168.82.1         | 192.168.82.126       | 192.168.82.127 |
| 50   | 192.168.82.128/26 | 255.255.255.192 | 192.168.82.129       | 192.168.82.190       | 192.168.82.191 |
|      | 192.168.82.192    |                 |                      |                      |                |

Fuente: Elaboración propia

### Parte 3: Configure aspectos básicos

Los dispositivos de red (S1 y R1) se configuran mediante conexión de consola.

#### Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3. Tareas de configuración para el Router R1

| Tarea  | Especificación  |
|--|---|
| Desactivar la búsqueda DNS                         | Router(config)#no ip domain-lookup  |
| Nombre del router                                  | Router(config)#hostname R1  |
| Nombre de dominio                                  | 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<br>R1(config-line)#password ciscoconpass<br>R1(config-line)#login<br>R1(config-line)#exit |
| Establecer la longitud mínima para las contraseñas | R1(config)#security passwords min-length 10   |

|  |  |
|--|--|
| Crear un usuario administrativo en la base de datos local                            | R1(config)#username admin privilege 15 secret<br>admin1pass  |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | R1(config)#line vty 0 4<br>R1(config-line)#login local<br>R1(config-line)#exit   |
| Configurar VTY solo aceptando SSH  | R1(config)#line vty 0 4<br>R1(config-line)#transport input ssh<br>R1(config-line)#login local<br>R1(config-line)#exit  |
| Cifrar las contraseñas de texto no cifrado   | R1(config)#service password-encryption   |
| Configure un MOTD Banner   | R1(config)#banner motd #ACCESO NO AUTORIZADO#  |
| Configurar interfaz G0/0/0   | R1(config)#int GigabitEthernet0/0/0<br>R1(config)#description HACIA PCB<br>R1(config-if)#ip add 192.168.82.129<br>255.255.255.192<br>R1(config-if)#no shutdown<br>R1(config-if)#exit |
| Configurar interfaz G0/0/1   | R1(config)#int GigabitEthernet0/0/1<br>R1(config)#description HACIA S1<br>R1(config)#ip add 192.168.82.1<br>255.255.255.128<br>R1(config-if)#no shutdown<br>R1(config-if)#exit       |
| Generar una clave de cifrado RSA   | R1(config)# crypto key generate rsa general-keys modulus 1024  |

Fuente: Elaboración propia

Figura 3. Configuración para el Router R1

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname 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 privilege 15 secret adminpass
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd #ACCESO NO AUTORIZADO#
R1(config)#int GigabitEthernet0/0/0
R1(config-if)#description HACIA PCB
R1(config-if)#ip add 192.168.82.129 255.255.255.192
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
R1(config)#int GigabitEthernet0/0/1
R1(config-if)#description HACIA SI
R1(config-if)#ip add 192.168.82.1 255.255.255.128
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)#crypto key generate rsa general-keys modulus 1024
```

Ctrl+F6 to exit CLI focus      Copy      Paste

Top Cisco Packet ... ISR4331 2960-24TT PC-A ESP 9:14 a.m. 5/12/2021

Fuente: Elaboración propia

A continuación se anexa el código de configuración de R1:

```
Router>en
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname 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 privilege 15 secret admin1pass
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd #ACCESO NO AUTORIZADO#
R1(config)#int GigabitEthernet0/0/0
R1(config-if)#description HACIA PCB
R1(config-if)#ip add 192.168.82.129 255.255.255.192
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#int GigabitEthernet0/0/1
R1(config-if)#description HACIA S1
R1(config-if)#ip add 192.168.82.1 255.255.255.128
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#crypto key generate rsa general-keys modulus 1024

```

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 4. Tareas de configuración para el Switch S1

| Tarea  | Especificación  |
|--|---|
| Desactivar la búsqueda DNS.  | Switch(config)#no ip domain-lookup  |
| Nombre del switch  | Switch(config)#hostname S1  |
| Nombre de dominio  | 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<br>S1(config-line)#password ciscoconpass<br>S1(config-line)#login<br>S1(config-line)#exit |
| Crear un usuario administrativo en la base de datos local                            | S1(config)#username admin privilege 15 secret admin1pass  |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | S1(config)#line vty 0 4<br>S1(config-line)#login local<br>S1(config-line)#exit                                      |

|  |   |
|--|---|
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH | S1(config)#line vty 0 4<br>S1(config-line)#transport input ssh<br>S1(config-line)#login local<br>S1(config-line)#exit             |
| Cifrar las contraseñas de texto no cifrado                               | S1(config)#service password-encryption  |
| Configurar un MOTD Banner  | S1(config)#banner motd #ACCESO NO AUTORIZADO#   |
| Generar una clave de cifrado RSA   | S1(config)#crypto key generate rsa general-keys modulus 1024  |
| Configurar la interfaz de administración (SVI)                           | S1(config)#interface vlan 1<br>S1(config-if)#ip address 192.168.82.2 255.255.255.128<br>S1(config-if)#no sh<br>S1(config-if)#exit |
| Configuración del gateway predeterminado                                 | S1(config)#ip default-gateway 192.168.82.1  |

Fuente: Elaboración propia

Figura 4. Configuración para el Switch S1

```

Switch>
Switch>en
Switch>enable
Switch>conf t
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 secret ciscoconpass
S1(config)#line console 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit
S1(config)#username admin privilege 15 secret admin1pass
S1(config)#line vty 0 4
S1(config-line)#login local
S1(config-line)#exit
S1(config)#line vty 0 4
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd #ACCESO NO AUTORIZADO#
S1(config)#crypto key generate rsa general-keys modulus 1024
* You already have RSA keys defined named S1.CCNA-Lab.com
* They will be replaced.

* The key modulus size is 1024 bits
* Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
* Mar 1 0:31:17.666: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.82.2 255.255.255.128
S1(config-if)#no sh

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#exit
S1(config)#ip default-gateway 192.168.82.1

```

Fuente: Elaboración propia

A continuación se anexa el código de configuración de S1:

```
Switch>en
Switch>enable
Switch#conf t
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 secret ciscoenpass
S1(config)#line console 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit
S1(config)#username admin privilege 15 secret admin1pass
S1(config)#line vty 0 4
S1(config-line)#login local
S1(config-line)#exit
S1(config)#line vty 0 4
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd #ACCESO NO AUTORIZADO#
S1(config)#crypto key generate rsa general-keys modulus 1024
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.82.2 255.255.255.128
S1(config-if)#no sh
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.82.1
```

#### 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 5. Configuración de red de la PC-A

| PC-A Network Configuration |                 |
|----------------------------|-----------------|
| Descripción                | HACIA S1        |
| Dirección física           | 0001.429B.E573  |
| Dirección IP               | 192.168.82.126  |
| Máscara de subred          | 255.255.255.128 |
| Gateway predeterminado     | 192.168.82.1    |

Fuente: Elaboración propia

Figura 5. Red del host con el comando ipconfig /all de la PC-A

```
Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix..:
Physical Address.....: 0001.429B.E573
Link-local IPv6 Address....: FE80::201:42FF:FE9B:E573
IPv6 Address.....: ::
IPv4 Address.....: 192.168.82.126
Subnet Mask.....: 255.255.255.128
Default Gateway.....: ::
                           192.168.82.1
DHCP Servers.....: 0.0.0.0
DHCPv6 IAID.....: :
DHCPv6 Client DUID.....: 00-01-00-01-A6-7B-5D-54-00-01-42-9B-E5-73
DNS Servers.....: ::
                           0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix..:
Physical Address.....: 0090.0C27.9DE8
Link-local IPv6 Address....: ::

--More--
```

Fuente: Elaboración propia

Tabla 6. Configuración de red de la PC-B

| PC-B Network Configuration |                 |
|----------------------------|-----------------|
| Descripción                | HACIA R1        |
| Dirección física           | 0000.0CCB.B9A0  |
| Dirección IP               | 192.168.82.190  |
| Máscara de subred          | 255.255.255.192 |
| Gateway predeterminado     | 192.168.82.1    |

Fuente: Elaboración propia

Figura 6. Red del host con el comando ipconfig /all de la PC-B

```
C:\> ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0000.0CCB.B9A0
Link-local IPv6 Address....: FE80::200:CFE:FECA:B9A0
IPv6 Address.....: ::
IPv4 Address.....: 192.168.82.190
Subnet Mask.....: 255.255.255.192
Default Gateway.....: ::
                           192.168.82.1
DHCP Servers.....: 0.0.0.0
DHC Pv6 IAID.....:
DHC Pv6 Client DUID.....: 00-01-00-01-D2-71-D2-63-00-00-0C-CB-B9-A0
DNS Servers.....: ::
                           0.0.0.0

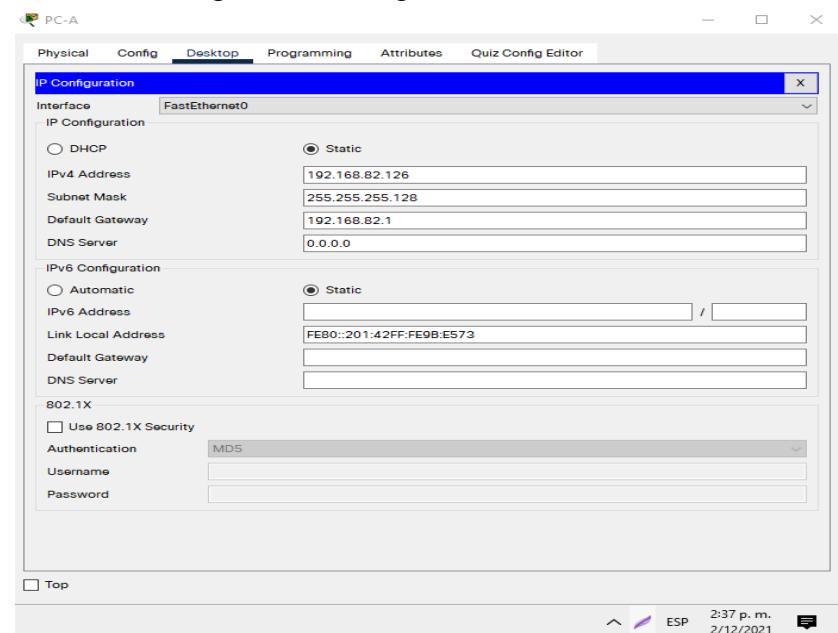
Bluetooth Connection:

Connection-specific DNS Suffix...:
Physical Address.....: 0060.3E6C.C261
Link-local IPv6 Address....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
                           0.0.0.0
DHCP Servers.....: 0.0.0.0
DHC Pv6 IAID.....:
DHC Pv6 Client DUID.....: 00-01-00-01-D2-71-D2-63-00-00-0C-CB-B9-A0
DNS Servers.....: ::
                           0.0.0.0

C:\>
```

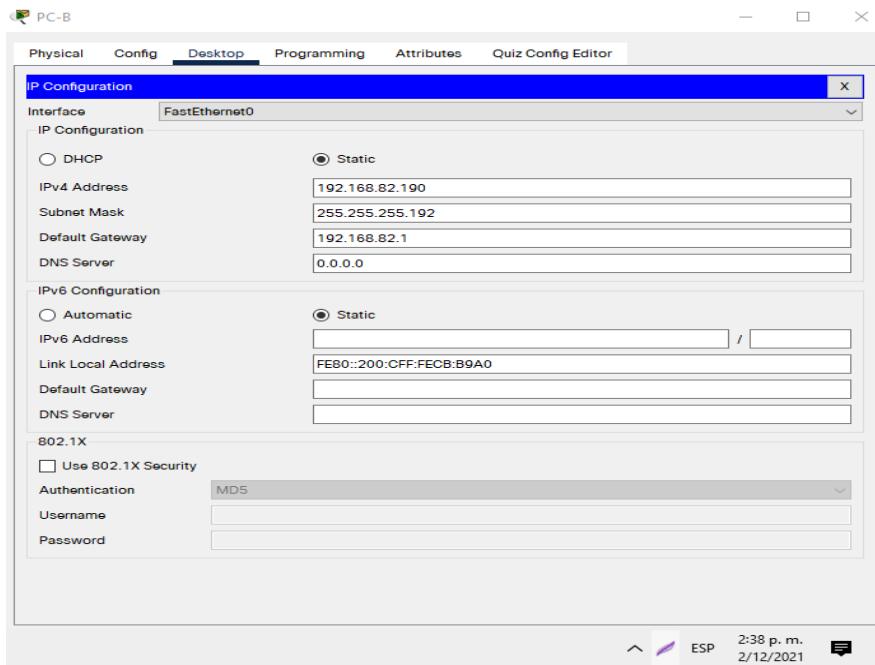
Fuente: Elaboración propia

Figura 7. Configuración host PC-A



Fuente: Elaboración propia

Figura 8. Configuración host PC-B



Fuente: Elaboración propia

Figura 9. Conectividad desde LAN 1- PC-A a todos los equipos

```
C:\>
C:\>ping 192.168.82.2
Pinging 192.168.82.2 with 32 bytes of data:
Reply from 192.168.82.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.82.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.82.129
Pinging 192.168.82.129 with 32 bytes of data:
Reply from 192.168.82.129: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.82.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.82.129
Pinging 192.168.82.129 with 32 bytes of data:
Reply from 192.168.82.129: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.82.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.82.190
Pinging 192.168.82.190 with 32 bytes of data:
Reply from 192.168.82.190: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.82.190:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Fuente: Elaboración propia

Figura 10. Conectividad desde LAN 1- S1 a todos los equipos

Fuente: Elaboración propia

Figura 11. Conectividad desde LAN 2- R1 a todos los equipos

Fuente: Elaboración propia

Figura 12. Ping desde LAN 2- PC-B a todos los equipos

The screenshot shows a Cisco Packet Tracer interface titled "PC-B". A "Command Prompt" window is open, displaying the output of a ping command. The command "ping 192.168.82.129" was run, followed by "ping 192.168.82.2". Both pings were successful, with four packets sent and received, no loss, and a round-trip time of 0ms. The timestamp at the bottom right is 5:15 p.m. on 5/12/2021.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.82.129
Pinging 192.168.82.129 with 32 bytes of data:
Reply from 192.168.82.129: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.82.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.82.2
Pinging 192.168.82.2 with 32 bytes of data:
Reply from 192.168.82.2: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.82.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Elaboración propia

Figura 13. Acceso remoto desde PC-B a R1

The screenshot shows a Cisco Packet Tracer interface titled "PC-B". A "Command Prompt" window is open, showing an attempt to log in via SSH to host "R1". The user "admin" is specified, but the password is left blank. The response "ACCESO NO AUTORIZADO" (Access denied) is displayed. The timestamp at the bottom right is 10:33 a.m. on 5/12/2021.

```
C:\>ssh -l admin 192.168.82.129
Password:
ACCESO NO AUTORIZADO
R1#
```

Fuente: Elaboración propia

Figura 14. Acceso remoto desde PC-A a S1

The screenshot shows a Cisco Packet Tracer interface titled "PC-A". A "Command Prompt" window is open, showing an attempt to log in via SSH to host "S1". The user "admin" is specified, but the password is left blank. The response "ACCESO NO AUTORIZADO" (Access denied) is displayed. The timestamp at the bottom right is 10:28 a.m. on 5/12/2021.

```
C:\>ssh -l admin 192.168.82.2
Password:
ACCESO NO AUTORIZADO
S1#
```

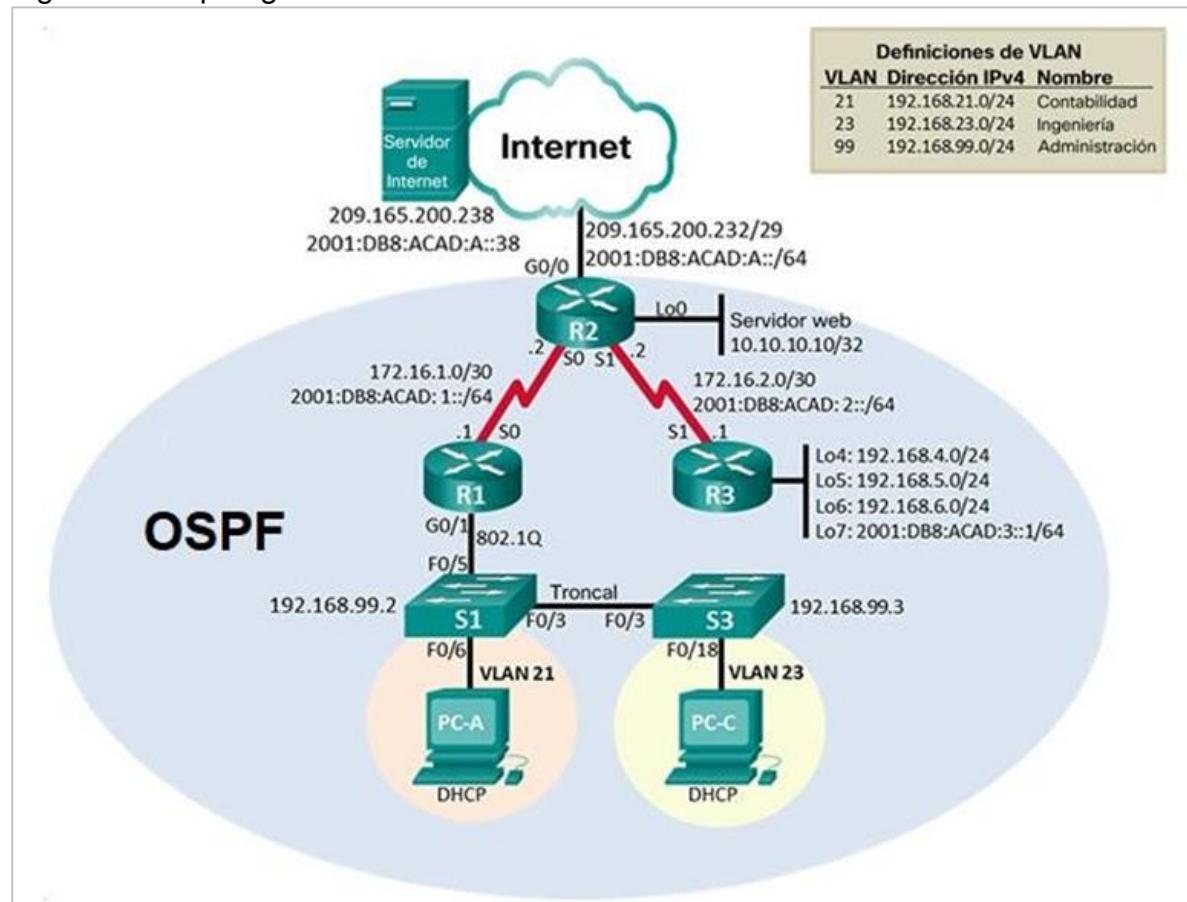
Fuente: Elaboración propia

## 2. ESCENARIO 2

Escenario: 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 15. Topología del escenario 2



Fuente: Tomado de 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 7. Reinicio y verificación de Router y Switches del escenario 2

| Tarea   | Comando de IOS  |
|---|---|
| Eliminar el archivo startup-config de todos los routers   | Router#erase startup-config   |
| Volver a cargar todos los routers   | Router#reload   |
| Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior | Switch#erase startup-config   |
| Volver a cargar ambos switches  | Switch#reload   |
| Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches                  | Switch#show flash<br>Directory of flash:/<br>1 -rw- 4670455 <no date><br>2960-lanbasek9-mz.150-2.SE4.bi |

Fuente: Elaboración propia

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

### Paso 1: Configurar la computadora de Internet

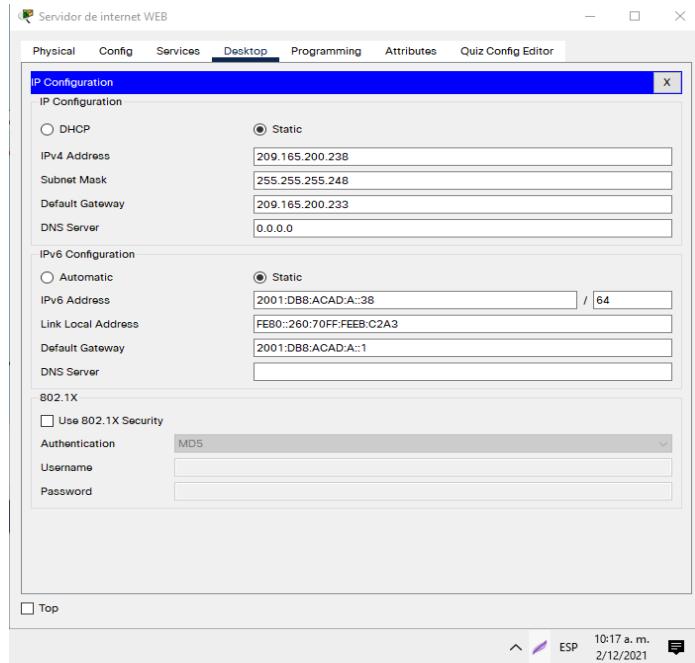
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 8. Configuración 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            | 209.165.200.233     |
| Dirección IPv6/subred             | 2001:DB8:ACAD:A::38 |
| Gateway predeterminado IPv6       | 2001:DB8:ACAD:A::1  |

Fuente: Elaboración propia

Figura 16. Configuración del servidor



Fuente: Elaboración propia

## Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 9. Configuración del Router R1

| Elemento o tarea de configuración          | Especificación   |
|--|--|
| 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<br>R1(config-line)#password cisco<br>R1(config-line)#login<br>R1(config-line)#exit |
| Contraseña de acceso Telnet                | R1(config)#line vty 0 4<br>R1(config-line)#password cisco<br>R1(config-line)#login<br>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 S0/2/0       | R1(config)#interface s0/2/0<br>R1(config-if)#description interface hacia el router R2<br>R1(config-if)#ip address 172.16.1.1<br>255.255.255.252<br>R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64<br>R1(config-if)#clock rate 128000<br>R1(config-if)#no sh |
| Rutas predeterminadas | R1(config)#ip route 0.0.0.0 0.0.0.0 S0/2/0<br>R1(config)#ipv6 route ::/0 S0/2/0   |

Fuente: Elaboración propia

Figura 17. Configuración inicial R1

```

Router>en
Router>enable
Router#conf t
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)
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#$ Se prohíbe el acceso no autorizado#
# Ambiguo comando: "Se prohíbe el acceso no autorizado"
R1(config)#banner motd #Se prohíbe el acceso no autorizado#
R1(config)#interface S0/2/0
R1(config-if)#description interface hacia el router 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 sh

#LINK--CHANGED: Interface Serial0/2/0, changed state to down
R1(config-if)#
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

A continuación se anexa el código de configuración de R1:

```

Router>en
Router>enable
Router#conf t
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 con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#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)#interface S0/2/0
R1(config-if)#description interface hacia el router 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 sh
R1(config-if)#ip route 0.0.0.0 0.0.0.0 S0/2/0
R1(config)#ipv6 route ::/0 S0/2/0

```

### Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 10. Configuración del Router R2

| <b>Elemento o tarea de configuración</b>   | <b>Especificación</b>  |
|--|--|
| Desactivar la búsqueda DNS                 | Router(config)#no ip domain lookup   |
| Nombre del router                          | Router(config)#hostname R2   |
| Contraseña de exec                         | R2(config)#enable secret class   |
| Contraseña de acceso a la consola          | R2(config)#line console 0<br>R2(config-line)#password cisco<br>R2(config-line)#login<br>R2(config-line)#exit               |
| Contraseña de acceso Telnet                | R2(config)#line vty 0 4<br>R2(config-line)#password cisco<br>R2(config-line)#login<br>R2(config-line)#exit                 |
| Cifrar las contraseñas de texto no cifrado | R2(config)#service password-encryption   |
| Habilitar el servidor HTTP                 | R2(config)#ip http server<br>(Comando que no sirve en ninguno de los routers en esta versión 8.0.1 de Cisco Packet Tracer) |

|   |   |
|---|---|
| Mensaje MOTD                                | R2(config)#banner motd #Se prohíbe el acceso no autorizado#   |
| Interfaz S0/2/0                             | R2(config)#interface serial 0/2/0<br>R1(config-if)#description conexión entre R2-R1<br>R2(config-if)#ip address 172.16.1.2 255.255.255.252<br>R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64  |
| Interfaz S0/2/1                             | R2(config)#interface serial 0/2/1<br>R2(config-if)#description R2 a R3<br>R2(config-if)#ip address 172.16.2.1 255.255.255.252<br>R2(config-if)#ipv6 add 2001:DB8:ACAD:2::2/64<br>R2(config-if)#clock rate 128000<br>R2(config-if)#no sh |
| Interfaz G0/0/0 (simulación de Internet)    | R2(config)#interface gigabitEthernet 0/0/0<br>R2(config-if)#description servidor WEB<br>R2(config-if)#ip address 209.165.200.233<br>255.255.255.248<br>R2(config-if)#ipv6 address 2001:DB8:ACAD:a::1/64<br>R2(config-if)#no sh          |
| Interfaz loopback 0 (servidor web simulado) | R2(config)#interface lo0<br>R2(config-if)#description servidor WEB<br>R2(config-if)#ip address 10.10.10.10 255.255.255.255  |
| Ruta predeterminada                         | R2(config)#ip route 0.0.0.0 0.0.0.0 G0/0/0<br>R2(config)#ipv6 route ::/0 G0/0/0   |

Fuente: Elaboración propia

Figura 18. Configuración inicial R2

```

Router>en
Router>enable
Router>config
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 con 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#ip http server

* Invalid input detected at '^' marker.

R2(config)#banner motd #Se prohíbe el acceso no autorizado#
R2(config)#interface serial 0/2/0
R2(config-if)#description conexión entre R2-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)#interface serial 0/2/1
R2(config-if)#description R2 a R3
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 sh

R2(config-if)#
*LINK-5-CHANGED: Interface Serial0/2/1, changed state to up

```

The screenshot shows the Cisco IOS CLI interface with the configuration commands entered. The configuration includes setting the banner motd, configuring interfaces (S0/2/0, S0/2/1, G0/0/0, and loopback 0), and defining a default route.

Fuente: Elaboración propia

A continuación se anexa el código de configuración de R2:

```
Router>en
Router>enable
Router#conf t
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 con 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#ip http server (Comando que no sirve en ninguno de los router en esta
versión 8.0.1 de Cisco Packet Tracer)
R2(config)#banner motd #Se prohíbe el acceso no autorizado#
R2(config)#interface serial 0/2/0
R2(config-if)#description conexión entre R2-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)#interface serial 0/2/1
R2(config-if)#description R2 a R3
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 sh
R2(config-if)#interface gigabitEthernet 0/0/0
R2(config-if)#description servidor WEB
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 sh
R2(config-if)#interface lo0
R2(config-if)#description servidor WEB
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#ip route 0.0.0.0 0.0.0.0 G0/0/0
R2(config)#ipv6 route ::/0 G0/0/0
```

## Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 11. Configuración del Router R3

| <b>Elemento o tarea de configuración</b>   | <b>Especificación</b>  |
|--|--|
| 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          | R2(config)#line con 0<br>R2(config-line)#password cisco<br>R2(config-line)#login<br>R2(config-line)#exit   |
| Contraseña de acceso Telnet                | R3(config)#line vty 0 4<br>R3(config-line)#password cisco<br>R3(config-line)#login<br>R3(config-line)#exit   |
| 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 S0/2/1                            | R3(config)#interface serial 0/2/1<br>R3(config-if)#description R3 a R2<br>R3(config-if)#ip address 172.16.2.2<br>255.255.255.252<br>R3(config-if)#ipv6 address<br>2001:DB8:ACAD:2::1/64<br>R3(config-if)#no sh |
| Interfaz loopback 4                        | R3(config)#int loopback 4<br>R3(config-if)#ip address 192.168.4.1<br>255.255.255.0<br>R3(config-if)#exit   |
| Interfaz loopback 5                        | R3(config)#int loopback 5<br>R3(config-if)#ip address 192.168.5.1<br>255.255.255.0<br>R3(config-if)#exit   |
| Interfaz loopback 6                        | R3(config)#int loopback 6<br>R3(config-if)#ip address 192.168.6.1<br>255.255.255.0<br>R3(config-if)#exit   |

|                       |  |
|-----------------------|--|
| Interfaz loopback 7   | R3(config)#interface loopback 7<br>R3(config-if)#ipv6 address<br>2001:DB8:ACAD:3::1/64<br>R3(config-if)#exit |
| Rutas predeterminadas | R3(config)#ip route 0.0.0.0 0.0.0.0<br>S0/2/1<br>R3(config)#ipv6 route ::/0 S0/2/1<br>R3(config)#            |

Fuente: Elaboración propia

Figura 19. Configuración inicial R3

```

Router>en
Router#conf t
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 con 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#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)#interface serial 0/2/1
R3(config-if)#description R3 a R2
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 sh

R3(config-if)#
*LINK-5-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)#
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)#
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)#
R3(config-if)ip address 192.168.4.1 255.255.255.0
R3(config-if)#
R3(config-if)int loopback 6

```

Fuente: Elaboración propia

A continuación se anexa el código de configuración de R3:

```

Router>en
Router#conf t
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 con 0

```

```

R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#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)#interface serial 0/2/1
R3(config-if)#description R3 a R2
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 sh
R3(config-if)#int loopback 4
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#int loopback 5
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)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#interface loopback 7
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
R3(config-if)#ip route 0.0.0.0 0.0.0.0 S0/2/1
R3(config)#ipv6 route ::/0 S0/2/1
R3(config)#

```

#### Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

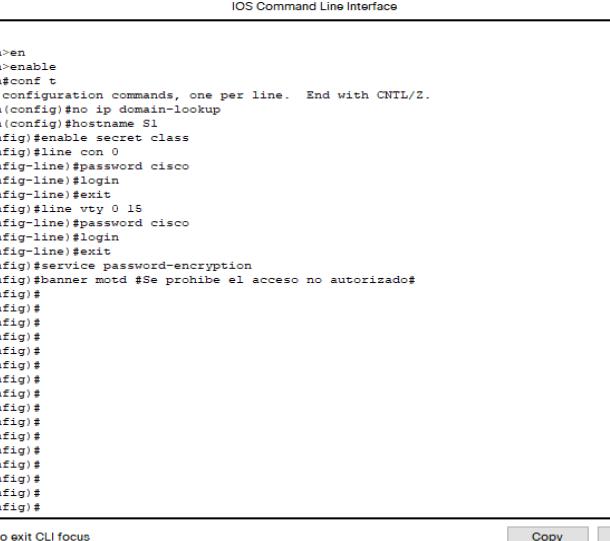
Tabla 12. Configuración del Switch S1

| Elemento o tarea de configuración       | Especificación   |
|---|--|
| 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 con 0<br>S1(config-line)#password cisco<br>S1(config-line)#login<br>S1(config-line)#exit |

|  |   |
|--|---|
| Contraseña de acceso Telnet                | S1(config)#line vty 0 15<br>S1(config-line)#password cisco<br>S1(config-line)#login<br>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#   |

Fuente: Elaboración propia

Figura 20. Configuración inicial S1



The screenshot shows a Cisco IOS CLI interface with the following details:

- Tab Bar:** Physical, Config, **CLI**, Attributes.
- Title Bar:** IOS Command Line Interface.
- Text Area:** Displays the configuration commands entered by the user. The commands include:
  - Switch>en
  - Switch>enable
  - Switch#conf t
  - 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 con 0
  - S1(config-line)#password cisco
  - S1(config-line)#login
  - S1(config-line)#exit
  - S1(config)#line vty 0 15
  - S1(config-line)#password cisco
  - S1(config-line)#login
  - S1(config-line)#exit
  - S1(config)#service password-encryption
  - S1(config)#banner motd #Se prohíbe el acceso no autorizado#
  - S1(config)#
  - S1(config)#
- Bottom Status Bar:** Ctrl+F6 to exit CLI focus, Copy, Paste.
- Bottom Right Corner:** Icons for TnN, 9:06 p.m., 2/12/2021, ESP, and a message bubble.

Fuente: Elaboración propia

A continuación se anexa el código de configuración de S1

Switch>en

Switch>enable

Switch#conf t

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

Enter configuration commands, one per line.  
Switch(config)#no ip domain-lookup

Switch(config)#no ip domain

S1(config)#enable secret class

S1(config)#line con 0

S1(config-line)#passw

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

31(config-line)#login

```

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

```

#### Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 13. Configuración del Switch S3

| Elemento o tarea de configuración          | Especificación  |
|--|---|
| 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 con 0<br>S3(config-line)#password cisco<br>S3(config-line)#login<br>S3(config-line)#exit    |
| Contraseña de acceso Telnet                | S3(config)#line vty 0 15<br>S3(config-line)#password cisco<br>S3(config-line)#login<br>S3(config-line)#exit |
| Cifrar las contraseñas de texto no cifrado | S3(config)#service password-encryption  |
| Mensaje MOTD                               | S3(config)#banner motd #Se prohíbe el acceso no autorizado#   |

Fuente: Elaboración propia

Figura 21. Configuración inicial S3

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line con 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd #Se prohíbe el acceso no autorizado#
S3(config)#
```

Fuente: Elaboración propia

A continuación se anexa el código de configuración de S3

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line con 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd #Se prohíbe el acceso no autorizado#
```

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 14. Verificación de la conectividad de los dispositivos

| <b>Desde</b>   | <b>A</b>               | <b>Dirección IP</b> | <b>Resultados de ping</b>   |
|----------------|------------------------|---------------------|---|
| R1             | R2, S0/2/0             | 172.16.1.2          | <p>Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:<br/>!!!!</p> <p>Success rate is 100 percent (5/5), round-trip min/avg/max = 20/22/25 ms</p>    |
| R2             | R3, S0/2/1             | 172.16.2.1          | <p>Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:<br/>!!!!</p> <p>Success rate is 100 percent (5/5), round-trip min/avg/max = 12/18/21 ms</p>    |
| PC de Internet | Gateway predeterminado | 209.165.200.233     | <p>Sending 5, 100-byte ICMP Echos to 209.165.200.233, timeout is 2 seconds:<br/>!!!!</p> <p>Success rate is 100 percent (5/5), round-trip min/avg/max = 1/9/14 ms</p> |

Fuente: Elaboración propia

Figura 22. Ping de R1 a R2

R1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
export@r1:~$
```

cisco ISR4331/K9 (IRU) processor with 1795955K/6147K bytes of memory.  
Processor board ID FLM332010G0  
3 Gigabit Ethernet interfaces  
2 Serial interfaces  
32768K bytes of non-volatile configuration memory.  
4194304K bytes of physical memory.  
3207167K bytes of flash memory at bootflash:.  
OK bytes of WebUI ODM Files at webui:.

Press RETURN to get started!

#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  
Se prohíbe el acceso no autorizado

User Access Verification

Password:

```
R1>en
R1>enable
R1>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 = 8/15/33 ms

R1#

Ctrl+F6 to exit CLI focus

Top

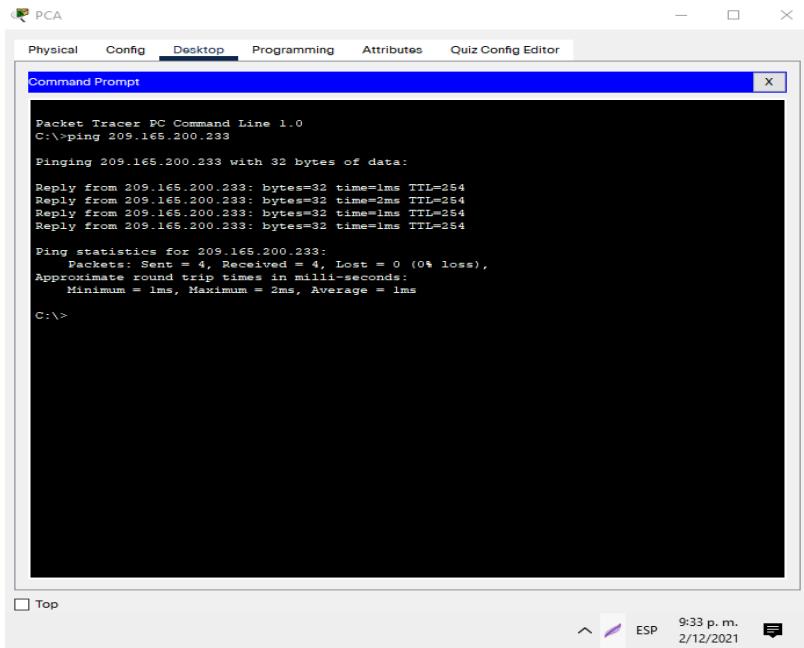
 Gmail: Co...  Cisco Pac...  S1  R1  ESP 2:00 p.m. 18/11/2021 

Fuente: Elaboración propia

Figura 23. Ping de R2 a R3

Fuente: Elaboración propia

Figura 24. Conectividad PC a Gateway predeterminado



```

Packet Tracer PC Command Line 1.0
C:\>ping 209.165.200.233

Pinging 209.165.200.233 with 32 bytes of data:
Reply from 209.165.200.233: bytes=32 time=1ms TTL=254
Reply from 209.165.200.233: bytes=32 time=2ms TTL=254
Reply from 209.165.200.233: bytes=32 time=1ms TTL=254
Reply from 209.165.200.233: bytes=32 time=1ms TTL=254

Ping statistics for 209.165.200.233:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>

```

Elaboración propia

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 15. Configuración de la seguridad del Switch S1

| Elemento o tarea de configuración | Especificación   |
|-----------------------------------|--|
| Crear la base de datos de VLAN    | <pre> S1&gt;enable S1#conf t 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 </pre> |

|   |   |
|---|---|
| Asignar la dirección IP de administración.                | S1(config)#int vlan 99<br>S1(config-if)#ip add 192.16.99.2<br>255.255.255.0<br>S1(config-if)#no sh<br>S1(config-if)#exit  |
| Asignar el gateway predeterminado                         | S1(config)#ip default-gateway 192.168.99.1<br>S1(config)#int f0/3   |
| Forzar el enlace troncal en la interfaz F0/3              | S1(config-if)#int f0/3<br>S1(config-if)#sw mode trunk<br>S1(config-if)#switchport trunk native vlan 1<br>1S1(config-if)#exit  |
| Forzar el enlace troncal en la interfaz F0/5              | S1(config-if)#int f0/5<br>S1(config-if)#sw mode trunk<br>S1(config-if)#switchport trunk native vlan 1<br>S1(config-if)# exit  |
| Configurar el resto de los puertos como puertos de acceso | S1(config-if)#int range f0/1- f0/2<br>S1(config-if-range)#sw mode access<br>S1(config-if-range)#int range f0/7- f0/24<br>S1(config-if-range)#sw mode access<br>S1(config-if-range)#exit |
| Asignar F0/6 a la VLAN 21                                 | S1(config-if)#int f0/6<br>S1(config-if)#sw mode access<br>S1(config-if)#sw access vlan 21   |
| Apagar todos los puertos sin usar                         | S1(config-if)#int range f0/7 - f0/24<br>S1(config-if-range)#sh<br>S1(config-if-range)#exit  |

Fuente: Elaboración propia

## Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 16. Configuración de la seguridad del Switch S3

| Elemento o tarea de configuración                         | Especificación   |
|---|--|
| Crear la base de datos de VLAN                            | <pre> Switch&gt;en Switch&gt;enable Switch#conf t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#ho S3 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 </pre> |
| Asignar la dirección IP de administración                 | <pre> S3(config)#int vlan 99 S3(config-if)#ip add 192.168.99.3 255.255.255.0 S3(config-if)#no sh S3(config-if)#exit </pre>   |
| Asignar el gateway predeterminado.                        | <pre> S3(config)#ip default-gateway 192.168.99.1 </pre>  |
| Forzar el enlace troncal en la interfaz F0/3              | <pre> S3(config)#int f0/3 S3(config-if)#sw mode trunk S3(config-if)#sw trunk native vlan 1 </pre>  |
| Configurar el resto de los puertos como puertos de acceso | <pre> S3(config)#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 </pre>  |
| Asignar F0/18 a la VLAN 21                                | <pre> S3(config)#int f0/18 S3(config-if)#sw acc vlan 21 </pre>   |
| Apagar todos los puertos sin usar                         | <pre> S3(config)#int range f0/7 - f0/17 S3(config-if-range)#sh S3(config-if-range)#exit </pre>   |

Fuente: Elaboración propia

### Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17. Configuración de la seguridad del Router R1

| Elemento o tarea de configuración            | Especificación  |
|--|---|
| Configurar la subinterfaz 802.1Q .21 en G0/1 | R1(config-subif)#enc dot1q 21<br>R1(config-subif)#ip address 192.168.21.1 255.255.255.0   |
| Configurar la subinterfaz 802.1Q .23 en G0/1 | R1(config-subif)#desc LAN ingenieira<br>R1(config-subif)#en dot1q 23<br>R1(config-subif)#ip add 192.168.23.1 255.255.255.0            |
| Configurar la subinterfaz 802.1Q .99 en G0/1 | R1(config-subif)#description LAN administracion<br>R1(config-subif)#en dot1q 99<br>R1(config-subif)#ip add 192.168.99.1 255.255.255.0 |
| Activar la interfaz G0/1                     | R1(config)#interface gigabitEthernet 0/1<br>R1(config-if)#no shutdown<br>R1(config-if)#exit   |

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 18. Verificación de la conectividad entre switches y R1

| Desde | 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 | 192.168.21.1 | Exitoso            |

Fuente: Elaboración propia

Figura 25. Ping S1 a VLAN Administración

The screenshot shows the Cisco IOS CLI interface for router S1. The configuration includes setting a password for the console and creating VLAN 99 with an IP address of 192.168.99.2. A ping command is then issued to 192.168.99.1, resulting in a success rate of 80 percent (4/5). The terminal window has a red box highlighting the ping output.

```
line Vty 5 15
password cisco
login
!
!
!
end

S1#
S1>conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#
S1(config)# interface vlan 99
S1(config-if)# ip add
S1(config-if)# ip address 192.168.99.2 255.255.255.0
S1(config-if)# no sh
S1(config-if)# exit
S1(config)#{ping 192.168.99.1
% Invalid input detected at '^' marker.

S1(config)#exit
S1#
*SYS-5-CONFIG_I: Configured from console by console

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#
```

Elaboración propia

Figura 26. Ping S3 a VLAN Administración

The screenshot shows the Cisco IOS CLI interface for router S3. After booting up, it displays various system logs. Then, it enters configuration mode and performs a ping to 192.168.99.1, achieving a 80 percent success rate (4/5). The terminal window has a red box highlighting the ping output.

```
(S3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1996-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 03:49 by mnnguyen

Press RETURN to get started!

*LINK-3-UPDOWN: Interface Vlan99, changed state to down
*LINK-5-CHANGED: Interface Vlan99, 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
*LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
*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

S3>en
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 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

S3#
```

Fuente: Elaboración propia

Figura 27. Ping de S1 a VLAN 21

```
%LINK-5-CHANGED: Interface Vlan99, 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
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%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
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

S1>en
S1>enable
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 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

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#
```

### Elaboración propia

Figura 28. Ping de S3 a la VLAN 23

```
S3 con0 is now available

Press RETURN to get started.

S3>en
S3>enable
S3#ping 192.168.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

S3#
```

Fuente: Elaboración propia

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

## Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 19. Configuración OSPF en el Router R1

| Elemento o tarea de configuración                | Especificación  |
|--|---|
| Configurar OSPF área 0                           | R1(config)#router ospf 82   |
| Anunciar las redes conectadas directamente       | R1(config-router)#network 192.168.21.0<br>0.0.0.255 area 0<br>R1(config-router)#network 192.168.23.0<br>0.0.0.255 area 0<br>R1(config-router)#network 192.168.99.0<br>0.0.0.255 area 0<br>R1(config-router)#net 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<br>R1(config-router)#passive-interface g0/0/1.21<br>R1(config-router)#passive-interface g0/0/1.23<br>R1(config-router)#passive-interface g0/0/1.99   |
| Desactive la summarización automática            | R1(config-router)#no auto-summary<br>(Error de comandos en OSPF, no se puede hacer)   |

Fuente: Elaboración propia

Figura 29. Configuración OSPF en el R1

Fuente: Elaboración propia

A continuación se anexa el código de configuración de OSPF en el R1

```
R1#conf t
```

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

```
R1(config)#router ospf 82
```

```
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)#net 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)#no auto-summary (Error de comandos en OSPF, no se puede hacer)
```

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 20. Configuración OSPF en el Router R2

| Elemento o tarea de configuración                 | Especificación   |
|---|--|
| Configurar OSPF área 0                            | R2(config)#router ospf 82  |
| Anunciar las redes conectadas directamente        | R2(config-router)#net 10.10.10.10<br>0.0.0.0 area 0<br>R2(config-router)#net 172.16.1.0<br>0.0.0.3 area 0<br>R2(config-router)#net 172.16.2.0<br>0.0.0.3 area 0<br>03:21:23: %OSPF-5-ADJCHG:<br>Process 82, Nbr 192.168.99.1 on<br>Serial0/2/0 from LOADING to FULL,<br>Loading Done |
| Establecer la interfaz LAN (loopback) como pasiva | R2(config-router)#passive-interface<br>loopback 0<br>R2(config-router)#exit  |
| Desactive la summarización automática.            | R3(config-router)#no auto-summary<br>(Error de comandos en OSPF, no se puede hacer)  |

Fuente: Elaboración propia

Figura 30. Configuración OSPF en el R2

The screenshot shows the Cisco Network Assistant interface for router R2. The window title is "R2". The tabs at the top are "Physical", "Config", "CLI" (which is selected), and "Attributes". The main area is titled "IOS Command Line Interface". The configuration code is as follows:

```
!
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 28 area 0
 clock rate 128000
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 82
 log-adjacency-changes
 passive-interface Loopback0
 network 10.10.10.10 0.0.0.0 area 0
 network 10.10.10.8 0.0.0.3 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 28
 router-id 1.1.1.1
 log-adjacency-changes
!
ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
ip nat inside source list 1 pool INTERNET
ip nat inside source static 10.10.10.10 209.165.200.233
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0/0
!
ip flow-export version 9
!
ipv6 route ::/0 GigabitEthernet0/0/0
!
access-list 1 permit 192.168.21.0 0.0.0.255
```

At the bottom of the CLI window, there are "Copy" and "Paste" buttons. A checkbox labeled "Top" is checked. In the bottom right corner, there is a timestamp: "10:20 p.m. 2/12/2021".

Fuente: Elaboración propia

A continuación se anexa el código de configuración de OSPF en el R2

R2#conf t

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

R2(config)#router ospf 82

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)#net 172.16.2.0 0.0.0.3 area 0

03:21:23: %OSPF-5-ADJCHG: Process 82, Nbr 192.168.99.1 on Serial0/2/0 from  
LOADING to FULL, Loading Done

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

R2(config-router)#exit

Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 21. Verificación información de OSPFv3 en el Router R2

| Elemento o tarea de configuración                                   | Especificación   |
|---|--|
| Configurar OSPF área 0  | R2(config)#ipv6 router ospf 28<br>R2(config-rtr)#router-id 1.1.1.1   |
| Anunciar redes IPv4 conectadas directamente                         | R2(config)#ipv6 router ospf 28<br>R2(config-rtr)#router-id 1.1.1.1<br>R2(config-rtr)#int s0/2/0<br>R2(config-if)#ipv6 ospf 28 area 0<br>R2(config-if)#exit<br>R2(config)#int s0/2/1<br>R2(config-if)#ipv6 ospf 28 area 0<br>R2(config-if)#exit<br>R2(config)#int g0/0/0<br>R2(config-if)#ipv6 ospf 28 area 0<br>R2(config-if)#exit |
| Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas | La loopback no tiene direcciones bajo IPV6.  |
| Desactive la summarización automática.                              | R2(config-router)#no auto-summary<br>(En este protocolo eso no se hace para, eso se coloca la wildcard y en IPV6 no se hace)   |

Fuente: Elaboración propia

La configuración del R3 incluye las siguientes tareas:

Tabla 22. Verificación información de OSPFv3 en el Router R3

| Elemento o tarea de configuración | Especificación  |
|-----------------------------------|---|
| Configurar OSPF área 0            | R3(config)#ipv6 router ospf 28<br>R3(config-rtr)#router-id 2.2.2.2<br>R3(config-rtr)#exit |

|   |  |
|---|--|
| Anunciar redes IPv4 conectadas directamente                         | R3(config)#int s0/2/1<br>R3(config-if)#ipv6 ospf 28 area 0<br>04:52:14: %OSPFv3-5-ADJCHG: Process 2, Nbr 1.1.1.1 on Serial0/2/1 from FULL to DOWN, Neighbor Down: Interface down or detached<br>R3(config-if)#exit   |
| Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas | R3(config)#int lo<br>R3(config)#int loopback 7<br>R3(config-if)#ipv6 ospf 28 area 0<br>R3(config-if)#exit<br>R3(config)#ipv6 router ospf 28<br>R3(config-rtr)#pas<br>R3(config-rtr)#passive-interface lo 4<br>R3(config-rtr)#passive-interface lo 5<br>R3(config-rtr)#passive-interface lo 6 |
| Desactive la summarización automática.                              | R3(config-router)#no auto-summary<br>(En este protocolo no se hace, para eso se coloca la wildcard y en IPV6 no aplica)  |

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 23. Verificación 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 route ospf    |
| ¿Qué comando muestra la sección de OSPF de la configuración en ejecución?   | show ip ospf database |

Fuente: Elaboración propia

Figura 31. Comando para ver ID del proceso OSPF

```
R1#show ip protocols
    OSPF Router with ID (192.168.99.1) (Process ID 82)
        Router Link States (Area 0)

Link ID      ADV Router      Age      Seq#      Checksum Link count
192.168.99.1 192.168.99.1  1316      0x8000000e 0x00c1bb 5
10.10.10.10  10.10.10.10  1316      0x8000000c 0x00419c 4
R1#
R1$show ip protocols
Routing Protocol is "ospf 82"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.99.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.2.0 0.0.0.255 area 0
    192.168.99.0 0.0.0.255 area 0
    192.168.99.0 0.0.0.255 area 0
    172.16.1.0 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0/1
    GigabitEthernet0/0/1.21
    GigabitEthernet0/0/1.23
    GigabitEthernet0/0/1.99
  Routing Information Sources:
    Gateway          Distance      Last Update
    10.10.10.10      110          00:24:04
    192.168.99.1     110          00:24:04
    Distance: (default is 110)
R1$
```

Fuente: Elaboración propia

Figura 32. Comando para mostrar solo las rutas OSPF

```
R1#show ip route ospf
  10.0.0.0/32 is subnetted, 1 subnets
  o  10.10.10.10 [110/65] via 172.16.1.2, 04:26:37, Serial0/2/0
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
  o  172.16.2.0 [110/128] via 172.16.1.2, 04:26:37, Serial0/2/0
R1#
R1$show ip route ospf
  10.0.0.0/32 is subnetted, 1 subnets
  o  10.10.10.10 [110/65] via 172.16.1.2, 04:26:37, Serial0/2/0
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
  o  172.16.2.0 [110/128] via 172.16.1.2, 04:26:37, Serial0/2/0
R1$
```

Fuente: Elaboración propia

Figura 33. Show ip ospf database en R1

```

R1
Physical Config CLI Attributes
IOS Command Line Interface
Incoming update filter list for all interfaces is not set
Router ID 192.168.99.1
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
 192.168.21.0 0.0.0.255 area 0
 192.168.20.0 0.0.0.255 area 0
 192.168.99.0 0.0.0.255 area 0
 172.16.1.0 0.0.0.3 area 0
Passive Interface(s):
 GigabitEthernet0/0/1
 GigabitEthernet0/0/1.21
 GigabitEthernet0/0/1.23
 GigabitEthernet0/0/1.99
Routing Information Sources:
   Gateway          Distance      Last Update
   10.10.10.10      110          00:24:04
   192.168.99.1     110          00:24:04
Distance: (default is 110)

R1#show ip route ospf
  10.0.0.0/32 is subnetted, 1 subnets
o  10.10.10.10 [110/65] via 172.16.1.2, 04:25:37, Serial0/2/0
  172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
o  172.16.2.0 [110/128] via 172.16.1.2, 04:25:37, Serial0/2/0

R1#show ip ospf database
OSPF Router with ID (192.168.99.1) (Process ID 82)

Router Link States (Area 0)
Link ID        ADV Router      Age      Seq#      Checksum Link count
192.168.99.1  192.168.99.1  1595      0x8000000e 0x00c1bb 5
10.10.10.10   10.10.10.10   1595      0x8000000c 0x00419c 4
R1#

```

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  
Las tareas de configuración para R1 incluyen las siguientes:

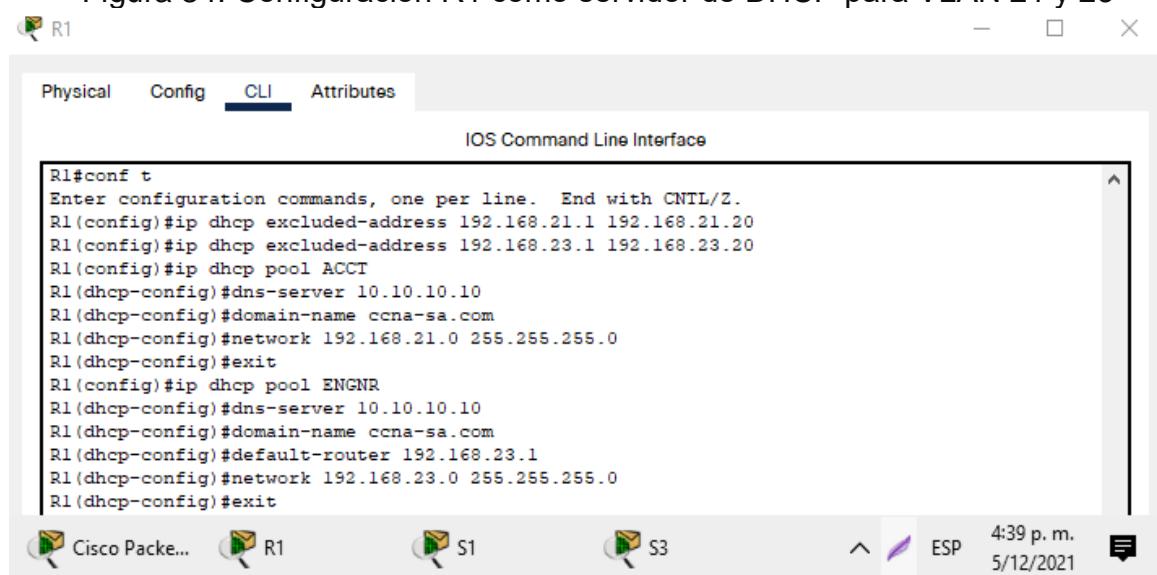
Tabla 24. Configuración R1 como servidor DHCP para VLAN 21 y 23

| Elemento o tarea de configuración  | Especificación  |
|--|---|
| Reservar las primeras 20 direcciones IP en la VLAN 21 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<br>R1(dhcp-config)#dns-server 10.10.10.10<br>R1(dhcp-config)#domain-name ccna-sa.com<br>R1(dhcp-config)#network 192.168.21.0 255.255.255.0<br>R1(dhcp-config)#exit |

|                                       |  |
|---------------------------------------|--|
| Crear un pool de DHCP para la VLAN 23 | R1(config)#ip dhcp pool ENGNR<br>R1(dhcp-config)#dns-server 10.10.10.10<br>R1(dhcp-config)#domain-name ccna-sa.com<br>R1(dhcp-config)#default-router 192.168.23.1<br>R1(dhcp-config)#network 192.168.23.0<br>255.255.255.0<br>R1(dhcp-config)#exit |
|---------------------------------------|--|

Fuente: Elaboración propia

Figura 34. Configuración R1 como servidor de DHCP para VLAN 21 y 23



The screenshot shows the CLI interface for router R1. The tab bar at the top has 'Physical', 'Config', 'CLI' (which is selected), and 'Attributes'. Below the tabs is the title 'IOS Command Line Interface'. The main window displays the configuration commands entered by the user:

```

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#exit
R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#exit

```

The bottom status bar shows the session name 'Cisco Pack...', the interface 'R1', port 'S1', port 'S3', and the timestamp '4:39 p. m. 5/12/2021'.

Fuente: Elaboración propia

A continuación se anexa el código de configuración de OSPF en el R1

```

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#exit
R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#exit

```

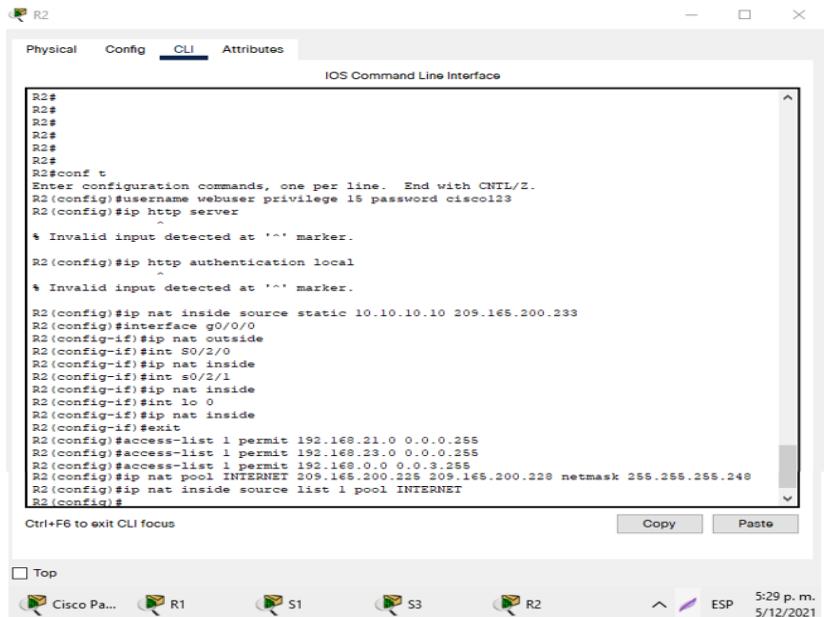
Paso 2: Configurar la NAT estática y dinámica en el R2  
La configuración del R2 incluye las siguientes tareas:

Tabla 25. Configuración NAT estática y dinámica en R2

| Elemento o tarea de configuración  | Especificación  |
|--|---|
| Crear una base de datos local con una cuenta de usuario                                | R2(config)#username webuser privilege 15 password cisco123  |
| Habilitar el servicio del servidor HTTP  | R2(config)#ip http server (error literal de comando)  |
| Configurar el servidor HTTP para utilizar la base de datos local para la autenticación | R2(config)#ip http authentication local (error literal de comando)  |
| Crear una NAT estática al servidor web.  | R2(config)#ip nat inside source static 10.10.10.10 209.165.200.233  |
| Asignar la interfaz interna y externa para la NAT estática                             | R2(config)#interface g0/0/0<br>R2(config-if)#ip nat outside<br>R2(config-if)#int S0/2/0<br>R2(config-if)#ip nat inside<br>R2(config-if)#int s0/2/1<br>R2(config-if)#ip nat inside<br>R2(config-if)#int lo 0<br>R2(config-if)#ip nat inside<br>R2#exit |
| Configurar la NAT dinámica dentro de una ACL privada                                   | R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255<br>R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255<br>R2(config)#access-list 1 permit 192.168.0.0 0.0.3.255   |
| Defina el pool de direcciones IP públicas utilizables.                                 | R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248   |
| Definir la traducción de NAT dinámica  | R2(config)#ip nat inside source list 1 pool INTERNET  |

Fuente: Elaboración propia

Figura 35. Configuración NAT estática y dinámica de R2



Fuente: Elaboración propia

A continuación se anexa el código de Configuración NAT estática y dinámica R2

R2#conf t

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

R2(config)#username webuser privilege 15 password cisco123

R2(config)#ip http server (error literal de comando)

R2(config)#ip http authentication local (error literal de comando)

R2(config)#ip nat inside source static 10.10.10.10 209.165.200.233

R2(config)#interface g0/0/0

R2(config-if)#ip nat outside

R2(config-if)#int S0/2/0

R2(config-if)#ip nat inside

R2(config-if)#int s0/2/1

R2(config-if)#ip nat inside

R2(config-if)#int lo 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 192.168.0.0 0.0.3.255

R2(config)#ip nat pool INTERNET

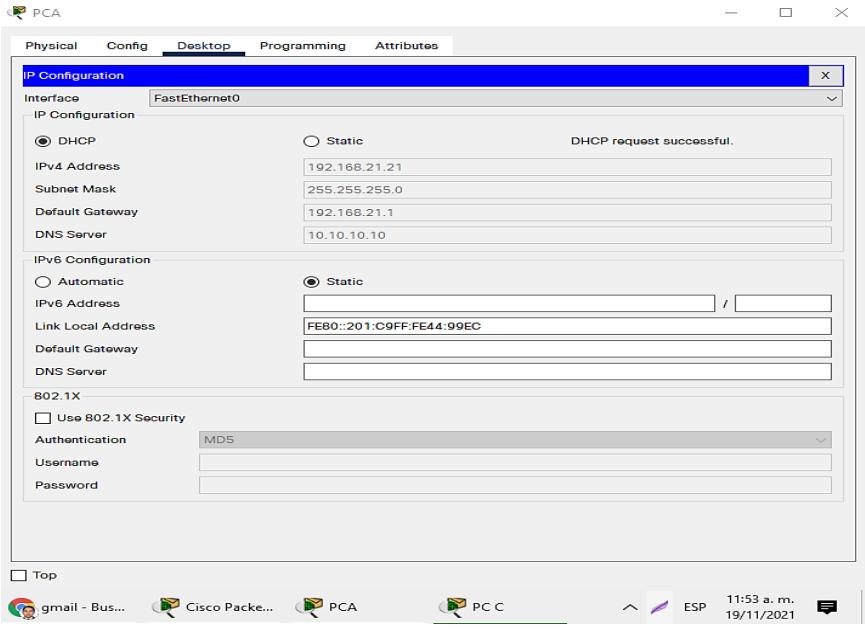
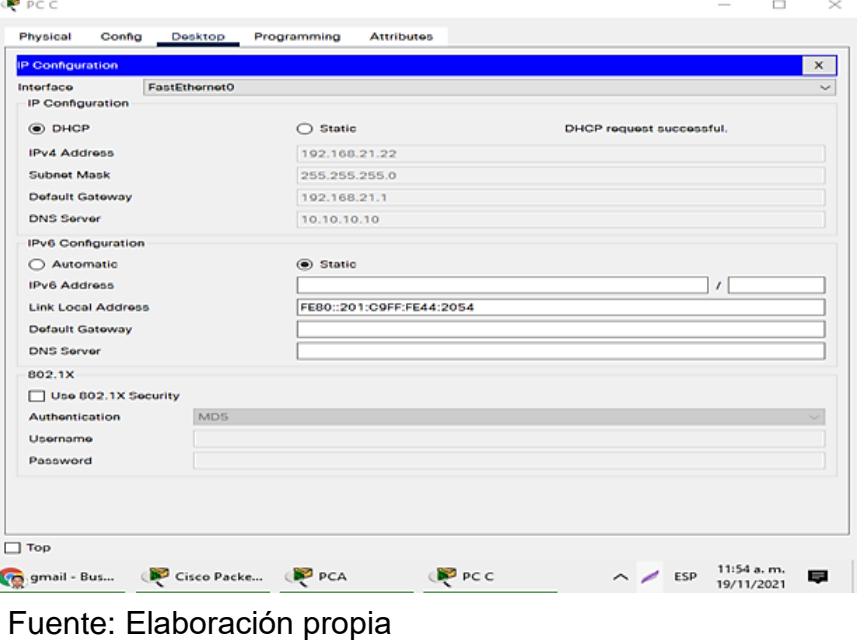
% Incomplete command.

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

### Paso 3: Verificar el protocolo DHCP y la NAT estática

Tabla 26. Verificación del protocolo DHCP y NAT estática

| Prueba  | Resultados   |
|---|--|
| verificar que la PC-A haya adquirido información de IP del servidor de DHCP | <p>Figura 36. PC-A con DHCP</p>  <p>Fuente: Elaboración propia</p>  |
| Verificar que la PC-C haya adquirido información de IP del servidor de DHCP | <p>Figura 37. PC-C con DHCP</p>  <p>Fuente: Elaboración propia</p> |

Verificar que la PC-A pueda hacer ping a la PC-C

Nota: Quizá sea necesario deshabilitar el firewall de la PC.

Figura 38. Ping PC-A a PC-C

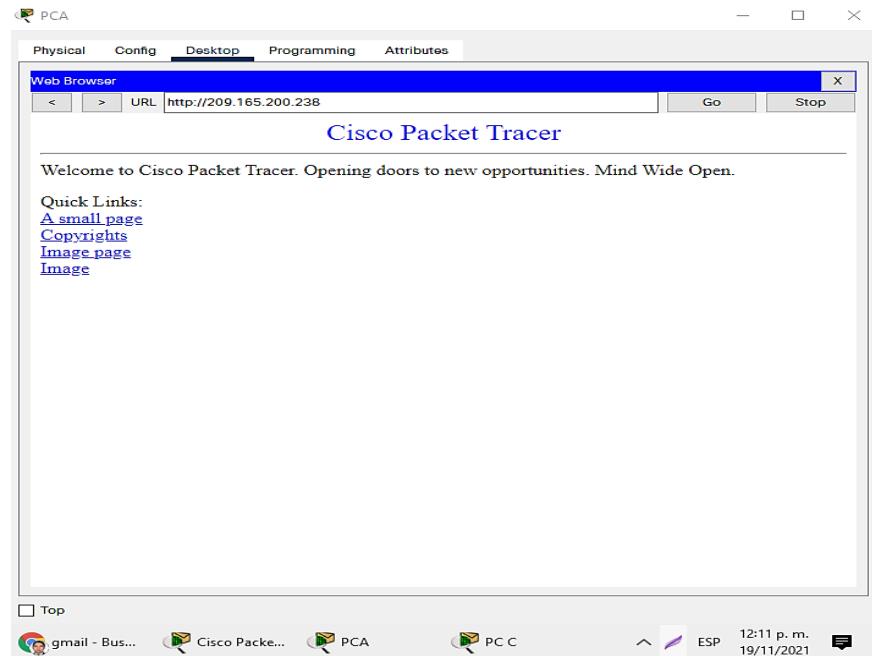
The screenshot shows a Cisco Packet Tracer Command Prompt window titled "Command Prompt". The command entered is "C:\>ping 192.168.21.22". The output shows four successful ping responses to the IP address 192.168.21.22. Below the responses, ping statistics are displayed, indicating 4 packets sent, 4 received, 0 lost, and 0% loss. The timestamp at the bottom right of the window is 11:58 a.m. on 19/11/2021.

Fuente: Elaboración propia

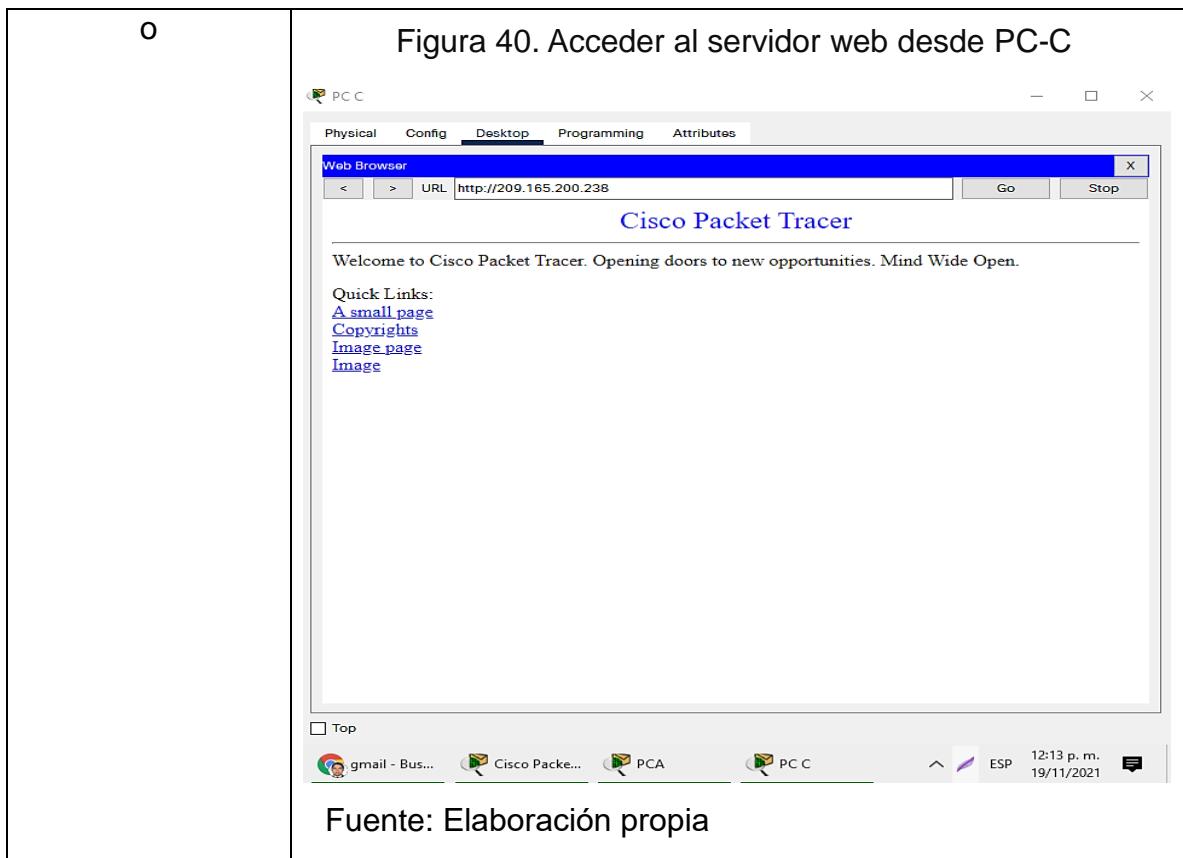
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.238)

Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345

Figura 39. Acceder al servidor web desde PC-A



Fuente: Elaboración propia



## Parte 6: Configurar NTP

Tabla 27. Configuración NTP en R1

| Elemento o tarea de configuración  | Especificación   |
|--|--|
| Ajuste la fecha y hora en R2.  | R2#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<br>R1#sh clock<br>*5:18:29.487 UTC Mon Mar 1 1993<br>R1#sh clock<br>*5:18:31.788 UTC Mon Mar 1 1993 |
| Verifique la configuración de NTP en R1.                                 | R1#sh clock<br>*9:9:0.319 UTC Sat Mar 5 2016<br>R1#sh clock<br>9:9:5.514 UTC Sat Mar 5 2016  |

Fuente: Elaboración propia

Figura 41. Configuración de NTP en R1

The screenshot shows the Cisco Network Assistant interface with Router R1 selected. The top navigation bar has tabs for Physical, Config, CLI, and Attributes, with CLI being the active tab. Below the tabs is the IOS Command Line Interface window. The command history shows the configuration of NTP on R1:

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp master 5
R2(config)#ntp server 172.16.1.2
R2(config)#ntp update-calendar
R2(config)#exit
R2#
*SYS-5-CONFIG_I: Configured from console by console

R2#sh clock
*9:13:28.869 UTC Sat Mar 5 2016
R2#
```

The bottom status bar shows the network diagram with nodes Cisco P..., R1, S1, S3, R2, R3, and ESP, along with the date and time (6:35 p.m. 5/12/2021).

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 28. Restringir el acceso a las líneas VTY en Router R2

| Elemento o tarea de configuración   | Especificación   |
|---|--|
| Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 | Nombre de la ACL: <b>ADMIN- MGT</b><br>R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255<br>R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255<br>R2(config)#access-list 1 permit 192.168.0.0 0.0.3.255<br>R2(config)#ip access-list standard ADMIN-MGT<br>R2(config-std-nacl)#permit host 172.16.1.1<br>R2(config-std-nacl)#deny any<br>R2(config-std-nacl)#exit |
| Aplicar la ACL con nombre a las líneas VTY  | R2(config)#line vty 0 4  |
| Permitir acceso por Telnet a las líneas de VTY  | R2(config-line)#ip access-class ADMIN-MGT in<br>R2(config-line)#transport input telnet   |
| Verificar que la ACL funcione como se espera  | R1#telnet 172.16.1.2<br>Trying 172.16.1.2 ...Open<br>User Access Verification<br>Password:<br>R2>ena<br>Password:<br>Password:<br>R2#  |

Fuente: Elaboración propia

Figura 42. Verificación de ACL

```
R2#show access-lists
Standard IP access list 1
 10 permit 192.168.21.0 0.0.0.255
 20 permit 192.168.23.0 0.0.0.255
 30 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
```

Fuente: Elaboración propia

Figura 43. Verificación desde R1 A R2 mediante conexión SSH

```
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...Open

User Access Verification

Password:
R2>en
Password:
Password:
Password:
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
```

Fuente: Elaboración propia

Figura 44. Verificación R3 A R2 mediante conexión SSH

```
R3>en
Password:
Password:
Password:
R3#telnet 172.16.1.2
Trying 172.16.1.2 ...Open

User Access Verification

Password:
R2>en
Password:
Password:
R2#
R2#
```

Fuente: Elaboración propia

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

Tabla 29. Comandos de verificación

| <b>Descripción del comando</b>   | <b>Entrada del estudiante (comando)</b> |
|--|---|
| Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció | R1(config) #show access-list            |
| 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#show run                             |
| ¿Con qué comando se muestran las traducciones NAT?   | R2#sh ip nat translations               |
| ¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?                           | R1(config)#clear ip nat translation     |

Fuente: Elaboración propia

## CONCLUSIONES

Mediante las topologías de red se logró verificar las diferentes configuraciones del dispositivo en cuanto a tecnologías y protocolos de commutación y enrutamiento sobre IP, articulando políticas básicas de seguridad de la información de esta manera se puede verificar el desempeño del desarrollo de un buen trabajo, y lo más importante, enriquecer el conocimiento para nuestra vida diaria.

El subneteo es una herramienta muy útil al momento de hacer Redes, el cual nos permite hacer la división que parte de una red dentro de varias subredes, como se llevo a cabo dentro de la configuración inicial del primer escenario, permitiendo llevar un mejor control sobre ellas y una transferencia de archivos más rápida.

Mediante el segundo escenario se logró conceptualizar con claridad el protocolo OSP, el cual nos facilita la escalabilidad de la red y simplifica su administración, donde se comprobó mediante la práctica, que todos los routers de la misma área mantienen la misma información topológica en su base de datos de estado enlace, de esta manera la red no tiene por qué afectar a toda ella.

Es de buena práctica que se implemente ACL en routers para proteger la red de ataques remotos, permitiendo el acceso a direcciones IP específicas, asegurándose de que solo la computadora del administrador tenga derecho a acceder al enrutador a través de telnet o SSH.

Se configuran servidores DHCP principal protocolo para ahorrar tiempo en la gestión de direcciones IP en redes grandes comprendiendo la importancia que cumple los agentes de retransmisión DHCP.

## BIBLIOGRAFÍA

GUTIERREZ, R. B., 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.

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

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

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

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

CISCO. (2019). Conceptos de Routing. Principios de Enrutamiento y Comutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#1>

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