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

YORK NEY RUIZ PEREZ

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

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

YORK NEY RUIZ PEREZ

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

TUTOR:
RAÚL BAREÑO GUTIERREZ

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

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Sincelejo, 29 de noviembre de 2021.

## AGRADECIMIENTOS

Este trabajo está dedicado a mi esposa Elis Melendres y mi hija Oriana Ruiz, por su apoyo incondicional, son las personas más importantes en mi vida y mi inspiración para salir adelante. Siempre han confiado en mis capacidades y me han motivado mucho para seguir en este proceso de formación y le doy gracias a mi Dios por eso. Por otra parte, de antemano agradecer al cuerpo docente del presente diplomado de profundización CCNA por su desempeño y el valor agregado que les dan a sus tutorías en pro de la mejora continua de superación y aprendizaje de sus estudiantes.

**CONTENIDO**

Pág.

AGRADACIMIENTOS....4
CONTENIDO....5
LISTA DE TABLAS....7
LISTA DE FIGURAS....8
GLOSARIO....10
RESUMEN....11
ABSTRACT....11
INTRODUCCIÓN....12
DESARROLLO....13
1. ESCENARIO 1....13
1.1. Parte 1. Construya red....13
1.2. Parte 2: Desarrolle el esquema de direccionamiento IP....14
1.2.1. Esquema de direcionamiento....14
1.3. Parte 3. Configure aspectos de direcionamiento....14
1.3.1. Configurar los ajustes básicos de R1....14
1.3.1.2. Configuraciones basicas de R1....15
1.3.2. Configura los ajustes basicas de S1....17
1.3.2.1. Configuraciones basicas de S1....18
1.3.3. Configurar los equipos....19
1.3.3.1. Configurar equipo host PC-A....19
1.3.3.2. Configurar equipo host PC-B....20
2. Escenario 2....24
2.2. Creación de la Topología lógica de red....24
2.3. PARTE 1: Iniciación de dispositivos....25
2.3.1. Paso 1: Inicializar y cargar los Routers y los Switches....25
2.4.. PARTE 2: Configuración de los parámetros básicos de los dispositivos....26
2.4.1. Paso 1: Configurar la computadora de Internet....26
2.4.2. Paso 2: Configuración de R1....27

2.4.3. Paso 3: Configuración de R2 ..... 29
2.4.4 Paso 4: Configuración de R3 ..... 32
2.4.5. Paso 5: Configuración de S1 ..... 35
2.4.6. Paso 6: Configuración de S3 ..... 36
2.4.7. Paso 7: Verificación de la conectividad de la red ..... 37
2.5. PARTE 3: Configuración de la seguridad ..... 40
2.5.1. Paso 1: Configuración de S1 ..... 40
2.5.2. Paso 2: Configuración de S3 ..... 42
2.5.3. Paso 3: Configuración de R1 ..... 44
2.5.4. Paso 4: Verificación de la conectividad de la red ..... 48
2.6. PARTE 4: Configuración del protocolo de Routing dinámico OSPF ..... 48
2.6.1. Paso 1 Configurar OSPF en el R1. ..... 48
2.6.2. Paso 2: Configurar OSPF en el R2. ..... 49
2.6.3. Paso 3: Configurar OSPFv3 en el R2 ..... 50
2.6.4. Paso 4: Verificar la información de OSPF ..... 51
2.7. PARTE 5: Implementación DHCP y NAT para IPv4 ..... 53
2.7.1. Paso 1: Configurar el R1 como servidor de DHCP ..... 53
2.7.2. Paso 2: Configuración de la NAT estática y dinámica en el R2 ..... 55
2.7.3. Paso 3: Verificar el protocolo DHCP y la NAT estática ..... 56
2.8. PARTE 6: Configuración de NTP ..... 57
2.9. PARTE 7: Configurar y verificar las listas de control de acceso (ACL) ..... 61
2.9.1. Paso 1: Restringir el acceso a las líneas VTY en el R2. Ver tabla 26 ..... 61
2.9.2 Paso 2: Introducir el comando de CLI ..... 62
CONCLUSIONES ..... 65
BIBLIOGRAFÍA ..... 66

## LISTA DE TABLAS

Pág.

Tabla 1. Direccionamiento IP ..... 14
Tabla 2. Configuración Para R1 ..... 14
Tabla 3. Configuración Para S1 ..... 17
Tabla 4. Direccionamiento IP en PC-A. ..... 19
Tabla 5. Direccionamiento IP en PC-B ..... 20
Tabla 6. Configuración inicial de Routers y Switches. ..... 25
Tabla 7. Configuración de la computadora de internet ..... 26
Tabla 8. Configuración de R1 ..... 28
Tabla 9. Configuración de R2 ..... 29
Tabla 10. Configuración de R3 ..... 32
Tabla 11. Configuración de S1 ..... 35
Tabla 12. Configuración de S3 ..... 36
Tabla 13. Verificación de conectividad en dispositivo. ..... 37
Tabla 14. Configuración de seguridad en S1. ..... 40
Tabla 15. Configuración de seguridad en S3 ..... 42
Tabla 16. Configuración de seguridad en R1. ..... 44
Tabla 17. Verificación de conectividad en dispositivo. ..... 46
Tabla 18. Verificación de conectividad en dispositivo. ..... 48
Tabla 19. Verificación de conectividad en dispositivo. ..... 49
Tabla 20. Verificación de conectividad en dispositivo. ..... 50
Tabla 21. Verificación de OSPF en el dispositivo. ..... 51
Tabla 22. Verificación de OSPF en el dispositivo. ..... 53
Tabla 23. Configuración de la NAT estática y dinámica en el R2. ..... 55
Tabla 24. Verificar el protocolo DHCP y la NAT estática ..... 56
Tabla 25. Verificar el protocolo DHCP y la NAT estática ..... 59
Tabla 26. Restringiendo el acceso a las líneas VTY en el R2. ..... 61
Tabla 27. Resumen de configuración ..... 62

## LISTA DE FIGURAS

Pág

Figura 1. Topología Escenario 1 ..... 13
Figura 2. Conexión de consola de la topología Escenario ..... 13
Figura 3. Comando Ipconfig /all en PC-A. ..... 20
Figura 4. Comando Ipconfig /all en PC-B ..... 21
Figura 5. Ping desde PC-A a PC-B ..... 21
Figura 6. Ping desde PC-B a PC-A ..... 22
Figura 7. Comando Show run en S1 ..... 22
Figura 8. Comando Show run en R1. ..... 23
Figura 9. Topología Escenario 2. ..... 24
Figura 10. Conexión de la topología Escenario 2 ..... 25
Figura 11. Configuración del servidor de internet ..... 27
Figura 12. Ping desde R1 a R2. ..... 38
Figura 13. Ping de R2 a R3 - 172.16.2.2 ..... 38
Figura 14. Ping de R2 a R3 - 2001:DB8:ACAD:2::1. ..... 39
Figura 15. Ping desde PC de internet a Gateway 209.165.200.233. ..... 39
Figura 16. Ping desde PC de internet a Gateway 2001:DB8:ACAD:A::1. ..... 40
Figura 17. Ping de S1 a R1 vlan 99 ..... 46
Figura 18. Ping de S3 a R1 VLAN 99 ..... 47
Figura 19. Ping de S1 a R1 VLAN 21 ..... 47
Figura 20. Figura 20. Ping de S3 a R1 VLAN 23 ..... 48
Figura 21. Show ip protocols en R2. ..... 52
Figura 22. Show ip route ospf en R2 ..... 52
Figura 23. Show ip ospf database en R1. ..... 53
Figura 24. PC-A con DHCP ..... 57
Figura 25. DHCP PC-C ..... 58
Figura 26. Ping de PC-A a PC-C ..... 58
Figura 27. Acceso al servidor web desde el navegador del PCA ..... 59
Figura 28. Comando show clock en R1 ..... 60
Figura 29. Verificación de ingreso a R2 a través de R1. ..... 62

Figura 30. Show access-lists. .....63
Figura 31. Show run para ver access list .....64
Figura 32. Show ip nat translations. .....64

## GLOSARIO

CONSOLA: Es un puerto de administración que proporciona acceso fuera de banda a los dispositivos Cisco. Al realizar la configuración inicial, una PC con software de emulación de terminal se conecta al puerto de consola del dispositivo mediante un cable especial.

DHCP: Protocolo de asignación de direccionamiento IP dinámico de tipo cliente/servidor que consiste en asignar parámetros de dirección IP al host de una red.

DNS: (Domain Name System), Sistema de Nombres de Dominio) es un conjunto de protocolos y servicios que permite a los usuarios utilizar nombres en vez de tener que recordar direcciones IP numéricas

HOST: Computador o dispositivo que se puede conectar a una red y ofrece servicios de transferencia de datos, almacenamiento, conexión remota, etc.

IP: Numero Identificación única y jerárquica que se puede asignar a una interfaz

IPV4: Es la cuarta versión del protocolo de internet IP, usa direcciones de 32 bits y será reemplazado en el futuro por IPV6.

LAN: Es una red de área local pequeña comúnmente es una red de oficina u hogar en la cual se permite enviar y recibir archivos.

ROUTER: Dispositivo que se encarga de encaminar los datos por los diferentes caminos disponibles o configurados dentro de la red. Además, se encarga de interconectar las diferentes redes.

RSA: Es un protocolo SSH permite establecer una sesión de usuario a un dispositivo en la red de forma segura. SSH, a diferencia del protocolo Telnet, encripta el tráfico en tránsito enviado a través de la red. SSH utiliza el puerto 22/TCP.

SWITCH: Es un dispositivo conmutador que permite interconectar muchos dispositivos para formar una red LAN.

SUBNETTING: Es dividir una red IP física en subredes lógicas (redes más pequeñas) para que cada una de estas trabaje a nivel envío y recepción de paquetes como una red individual, aunque todas pertenezcan a la misma red física y al mismo dominio.

VLAN: Es una red de área local virtual, la cual se configura para crear redes lógicas independientes dentro de una red física. Pueden configurarse varias redes VLAN dentro de un mismo escenario físico.

VTY: Es una línea virtual que funciona dentro del software y no requiere hardware adicional para funcionar.

## RESUMEN

A continuación, veremos el desarrollo de una prueba de habilidades, que consta de dos topologías, en el que se buscara dar solución a los parámetros solicitados, mediante la ejecución de comando de consola, análisis de enrutamiento y comprobación de conexión de red.

Para el desarrollo del primer escenario se solicitará la configuración básica de dispositivos de red en una red LAN, con ciertos límites de host, enrutamiento de sus interfaces con direccionamiento IPV4, y verificación de la conexión de los equipos de cómputo con la red.

En el segundo escenario, bajo la ejecución de comandos CLI, se ara la configuración de aspectos básico y direccionamiento IPv4 e IPv6 a los dispositivos de red, crear base de datos VLAN en las interfaces¬, disponer de acceso telnet puertos de acceso, implementar protocolos de routing dinámico OSPF, servicio de protocolo DHCP, mecanismos NAT, para permitir operaciones entre protocolos, sincronizar reloj en los dispositivos con NTP y verificar la conexión de acceso a internet en la topología.



Palabras claves: Acceso, comandos, conexión, datos, dispositivo, enrutamiento, interfaces.



## ABSTRACT

Next, we will see the development of a skills test, which consists of two topologies, in which it will be sought to solve the requested parameters, by executing a console command, routing analysis and checking the network connection.

For the development of the first scenario, the basic configuration of network devices in a LAN network will be requested, with certain host limits, routing of their interfaces with IPV4 addressing, and verification of the connection of the computer equipment with the network.

In the second scenario, under the execution of CLI commands, the configuration of basic aspects and IPv4 and IPv6 addressing to the network devices is done, create a VLAN database on the interfaces, have access to telnet access ports, implement protocols of dynamic routing OSPF, DHCP protocol service, NAT mechanisms, to allow operations between protocols, synchronize clock in the devices with NTP and verify the connection of Internet access in the topology.



Keywords: Access, commands, connection, data, device, routing, interfaces.

# INTRODUCCIÓN

En el presente informe se realizará la documentación de los procesos manejados en las dos etapas realizadas durante el desarrollo de los dos escenarios de prácticas propuestos en la unidad 1,2,3 y 4, del presente curso de profundización en redes Cisco. en el que se expondrá de manera detallada los paso a paso de la creación de redes, subredes, configuraciones de direccionamiento IPv4 e IPV6 enrutamiento y verificación de conectividad entre equipos de red. Así mismo se expondrán, la aplicación de conceptos básico en el manejo de redes, toma de datos, análisis de los mismos, corrección de errores y utilización de comandos de consola y CLI, para ajustes de seguridad, cifrado de contraseñas, creación de usuarios, inicio de sesión configuración de interfaces, conexiones telnet, creación de VLANs, implementación de protocolos de routing dinámico OSPF, protocolos de servicio DHCP, asignaciones POOL, direccionamiento DNS, mecanismos NAT y protocolos NTP.

## DESARROLLO

1. Escenario 1**.**

El primer escenario consta de la construcción y simulación de una red pequeña LAN, con direccionamiento IPv4 para dos (2) subredes, configuración de aspectos básicos de los dispositivos de red, ajustes de seguridad y verificación de conectividad entre equipos. Ver figura 1.

Figura 1. Topología Escenario 1.


Fuente propia.

### 1.1. PARTE 1: Construya la Red.

Se crea la topología lógica de red, con los aspectos básicos de configuración solicitados en el Escenario1, realizando el cableado correspondiente y la conexión de consola a un Router, un switch y dos equipos de cómputo, mediante la herramienta Packet Tracer.

Esta topología, permitirá la configuración del direccionamiento IPv4 y la administración segura de los dispositivos de red. Ver Figura 2.

Figura 2. Conexión de consola de la topología Escenario 1.


Fuente propia.

## 1.2. PARTE 2: Desarrolle el esquema de direccionamiento IP.

El esquema de la red LAN, tendrá los siguientes requisitos de direccionamiento IPv4 en la red, subredes, cantidad requerida de host y asignación IP en los dispositivos de cómputo. Ver tabla 1.

Tabla 1. Direccionamiento IP.

| Ítem | Requerimiento. |
|---|---|
| Dirección de Red | 192.168.79.0/24 |
| Requerimiento de host Subred LAN1 | 192.168.79.0/25 |
| Requerimiento de host Subred LAN2 | 192.168.79.128/26 |
| R1 G0/0/1 | 192.168.79.1/25 |
| R1 G0/0/0 | 192.168.79.129/26 |
| S1 SVI | 192.168.79.2/25 |
| PC-A | 192.168.79.126/25 |
| PC-B | 192.168.79.190/26 |

Fuente propia.

## 1.3. PARTE 3: Configure aspectos básicos.

### 1.3.1. Configurar los ajustes básicos en R1.

Inicialmente se hará el diagnóstico del dispositivo R1 y mediante la conexión de consola se darán las siguientes especificaciones: desactivar la búsqueda DNS, asignar nombre al Router y dominio, contraseña cifrada, contraseña de acceso a la consola, longitud mínima para las contraseñas, usuario administrativo, inicio de sesión y configuración de las interfaces. Ver tabla 2.

Tabla 2. Configuración Para R1.

| Tarea | Especificación |
|---|---|
| Desactivar la búsqueda DNS | |
| Nombre del router | R1 |
| Nombre de dominio | ccna-lab.com |
| Contraseña cifrada para el modo EXEC privilegiado | ciscoenpass |
| Contraseña de acceso a la consola | ciscoconpass |
| Establecer la longitud mínima para las contraseñas | 10 caracteres |
| Crear un usuario administrativo en la base de datos local | Nombre de usuario: admin<br>Password: admin1pass |
| Configurar el inicio de sesión en las | |

| | |
|---|---|
| líneas VTY para que use la base de datos local | |
| Configurar VTY solo aceptando SSH | |
| Cifrar las contraseñas de texto no cifrado | |
| Configure un MOTD Banner | |
| Configurar interfaz G0/0/0 | Establezca la descripción Establece la dirección IPv4.<br>Activar la interfaz. |
| Configurar interfaz G0/0/1 | Establezca la descripción Establece la dirección IPv4.<br>Activar la interfaz. |
| Generar una clave de cifrado RSA | Módulo de 1024 bits |

Fuente propia.

1.3.1.2. Configuraciones básicas en R1.

Se procede a configurar mediante conexión de consola cada uno de los elementos solicitados anteriormente en la tabla 2, Configuración para R1, así:

Primero se empieza entrando al Router desde la PC-B, selecciono Desktop y luego a la configuración del Terminal, e ingreso los siguientes comandos de configuración para cumplir con el requerimiento solicitado para la LAN 1:

Se adjunta código y pantallazos de comprobación del mismo.

Router 1.
Router>en Ingreso a modo privilegiado.
Router#conf t Ingreso a modo de configuración.
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup Desactivo búsqueda DNS.
Router(config)#hostname R1 Asigno nombre al router.
R1(config)#ip domain-name ccna-lab.com Asigno nombre de dominio.
R1(config)#enable secret ciscoenpass Se configura contraseña en modo privilegiado.
R1(config)#line console 0 Se ingresa a la línea de consola.
R1(config-line)#password ciscoenpass Asigno contraseña de acceso a la consola.
R1(config-line)#login Se habilita contraseña, autenticación local.
R1(config-line)#exit Se da un paso atrás.
R1(config)#security password min-length 10 Asigno longitud mínima para contraseña.

R1(config)#username admin password admin1pass Creo usuario y asigno contraseña.
R1(config)#line vty 0 4 Inicio sesión línea vty para uso de la base datos local.
R1(config-line)#password ciscoenpass Asigno contraseña a la línea vty.
R1(config-line)#login local Autenticación local.
R1(config-line)#transport input ssh Configuramos vty aceptando solo protocolo ssh.
R1(config-line)#exit Se da un paso atrás.
R1(config)#service password-encryption Se cifran la contraseña de texto no cifrado.
R1(config)#banner motd #Diplomado de profundización CISCO. UNAD 2021.Area Restringida # Se configura contenido de mensaje de aviso.
R1(config)#int g0/0/0 Configuro interfaz G0/0/0.
R1(config-if)#ip address 192.168.79.129 255.255.255.192 Se Establece la dirección IPv4.
R1(config-if)#description Esta es la interface de la LAN 2 Descripción de la interfaz.
R1(config-if)#no sh Comando para subir la interface.
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 Se da un paso atrás.
R1(config)#int g0/0/1 Configuro interfaz G0/0/1.
R1(config-if)#description Esta es la interface de la LAN 1 Descripción de la interfaz.
R1(config-if)#ip address 192.168.79.1 255.255.255.128 Se Establece la dirección IPv4.
R1(config-if)#no sh Comando para subir la interface.
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 Se da un paso atrás.
R1(config)#ip domain-name ccna-lab.com Se llama el dominio nuevamente.
R1(config)#crypto key generate rsa Se genera una clave de cifrado RSA.
The name for the keys will be: R1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024 Se encripta a 1024 bits.

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#exit Se da un paso atrás.
*Mar 2 2:13:31.878: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#wr Se guarda la configuración.
Building configuration...
[OK]
R1#

### 1.3.2. Configurar los ajustes básicos en S1.

Se realiza el diagnóstico del dispositivo Switch y mediante la conexión de consola se darán las siguientes especificaciones: desactivar la búsqueda DNS, asignar nombre al switch y dominio, contraseña cifrada, contraseña de acceso a la consola, usuario administrativo, inicio de sesión, conexiones SSH, mensaje de aviso y configuración de las interfaces. Ver tabla 3.

Tabla 3. Configuración Para S1.

| Tarea | Especificación |
|---|---|
| Desactivar la búsqueda DNS | |
| Nombre del switch | S1 |
| Nombre de dominio | ccna-lab.com |
| Contraseña cifrada para el modo EXEC privilegiado | ciscoenpass |
| Contraseña de acceso a la consola | ciscoconpass |
| Crear un usuario administrativo en la base de datos local | Nombre de usuario: admin<br>Password: admin1pass |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH | |
| Cifrar las contraseñas de texto no cifrado | |
| Configure un MOTD Banner | |
| Generar una clave de cifrado RSA | Modulo de 1024 bits |
| Configurar la interfaz de administración (SVI) | Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento |
| Configuración del gateway predeterminado | Configure la puerta de enlace predeterminada conforme a la tabla de |

| | |
|---|---|
| | direccionamiento. |

Fuente propia.

1.3.2.1. Configuraciones básicas en S1.

Se procede a configurar mediante conexión de consola cada uno de los elementos solicitados anteriormente en la tabla 3, Configuración para s1, así:

Primero se empieza entrando al Switch desde la PC-A, selecciono Desktop y luego a la configuración del Terminal, e ingreso los siguientes comandos de configuración para cumplir con el requerimiento solicitado para la LAN 2:

Se adjunta código y pantallazos de comprobación del mismo.

**Swich 1**.

Switch>en Ingreso a modo privilegiado.
Switch#conf t Ingreso a modo de configuración.
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup Desactivo búsqueda DNS.
Switch(config)#hostname S1 Asigno nombre al Switch.
S1(config)#ip domain-name ccna-lab.com Asigno nombre de dominio.
S1(config)#enable secret ciscoenpass Se Configura contraseña en modo privilegiado.
S1(config)#line console 0 Se ingresa a la línea de consola.
S1(config-line)#password ciscoenpass Asigno contraseña de acceso a la consola
S1(config-line)#login Se habilita contraseña, se autentica local.
S1(config-line)#exit Se da un paso atrás.
S1(config)#username admin password admin1pass Creo usuario y doy contraseña.
S1(config)#line vty 0 15 Inicio sesión VTY para uso de la base datos local.
S1(config-line)#password ciscoenpass Asigno contraseña a la línea VTY.
S1(config-line)#login local Autenticación local.
S1(config-line)#transport input ssh Configuramos VTY aceptando solo protocolo SSH.
S1(config-line)#exit Se da un paso atrás.
S1(config)#service password-encryption Se cifran la contraseña de texto no cifrado.
S1(config)#banner motd #Diplomado de profundización CISCO. UNAD 2021.Area Restringida S1 # Se configura contenido de mensaje de aviso.

S1(config)#ip domain-name ccna-lab.com Se llama el dominio nuevamente.
S1(config)#crypto key generate rsa Se genera una clave de cifrado RSA.
The name for the keys will be: S1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024 Se encripta a 1024 bits.
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
S1(config)#int vlan 1 Se Configura la interfaz de administración (SVI).
*Mar 2 2:22:53.618: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config-if)#ip address 192.168.79.2 255.255.255.128 Direccionamiento IPv4 capa 3.
S1(config-if)#no sh Comando para subir la interface.
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 Se da un paso atrás.
S1(config)#ip default-gateway 192.168.79.1 Se Configura el Gateway predeterminado.
S1(config)#exit

### 1.3.3. Configurar los equipos.

#### 1.3.3.1. Configuración equipo host PC-A.

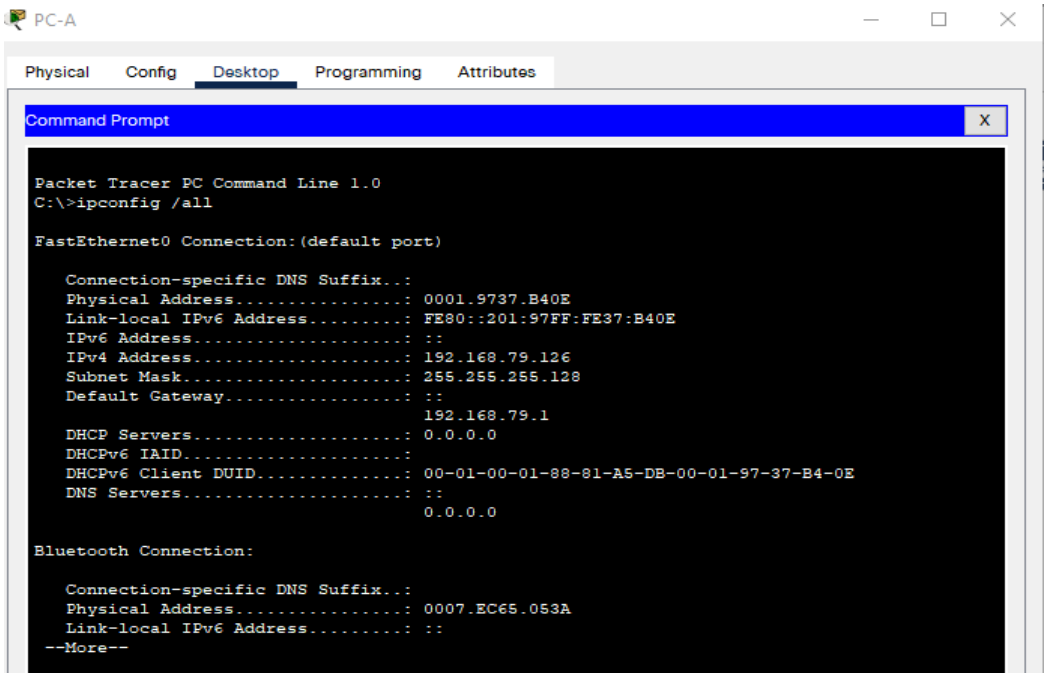
Se ingresa al equipo PC-A, selecciono Desktop, luego entro a la configuración IP y se realiza el direccionamiento especifico del equipo, conforme al direccionamiento suministrado en la tabla 1. Direccionamiento IP, para cumplir con el requerimiento solicitado para la subred LAN 1. Ver tabla 4.

Tabla 4. Direccionamiento IP en PC-A.

| PC-A Network Configuration | |
|---|---|
| Descripción | Este es el PC-A |
| Dirección física | 0001.9737.B40E |
| Dirección IP | 192.168.79.126 |
| Máscara de subred | 255.255.255.128 |
| Gateway predeterminado | 192.168.79.1 |

Fuente propia.

Figura 3. Comando Ipconfig /all en PC-A.




Fuente propia.

1.3.3.2. Configuración equipo host PC-B.

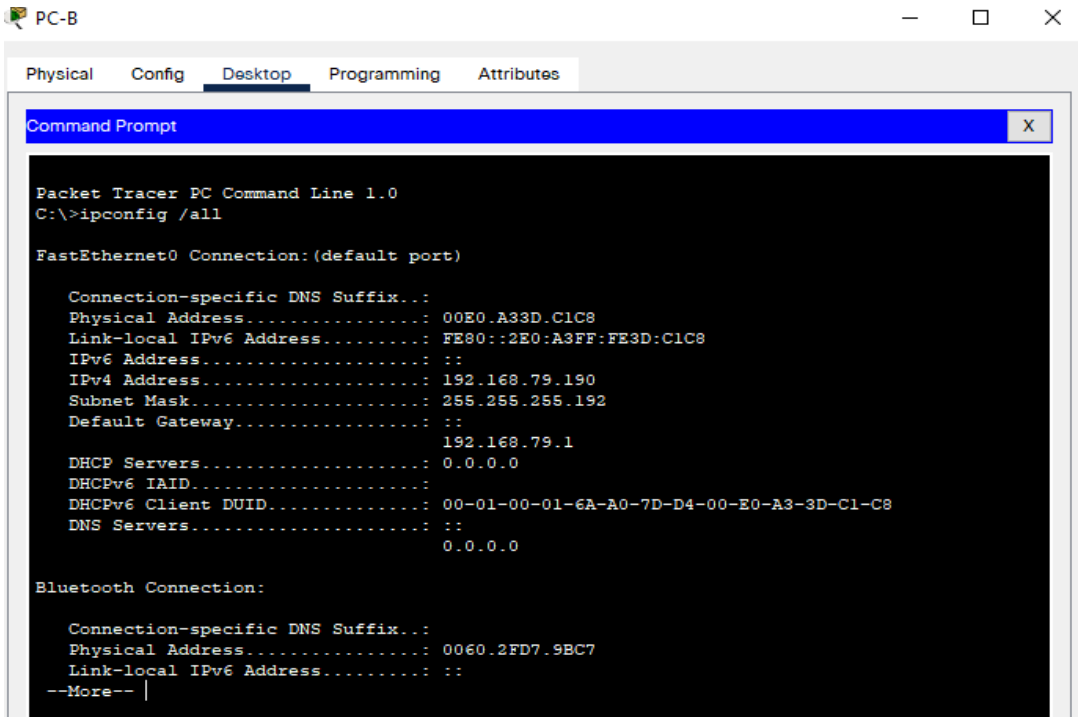
Se ingresa al equipo PC-B, selecciono Desktop, luego entro a la configuración IP y se realiza el direccionamiento especifico del equipo, conforme al direccionamiento suministrado en la tabla 1. Direccionamiento IP, para cumplir con el requerimiento solicitado para la subred LAN 2. Ver tabla 5.

Tabla 5. Direccionamiento IP en PC-B.

| PC-B Network Configuration | |
|---|---|
| Descripción | Este es el PC-B |
| Dirección física | 00E0.A33D.C1C8 |
| Dirección IP | 192.168.79.190 |
| Mascara de subred | 255.255.255.192 |
| Gateway predeterminado | 192.168.79.1 |

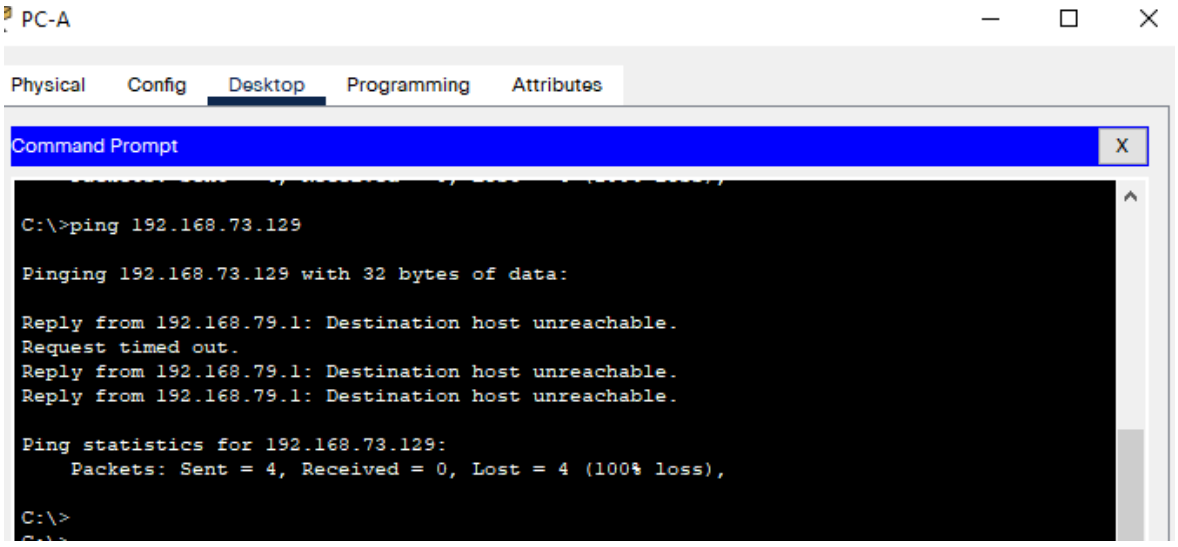
Fuente propia.

Figura 4. Comando Ipconfig /all en PC-B



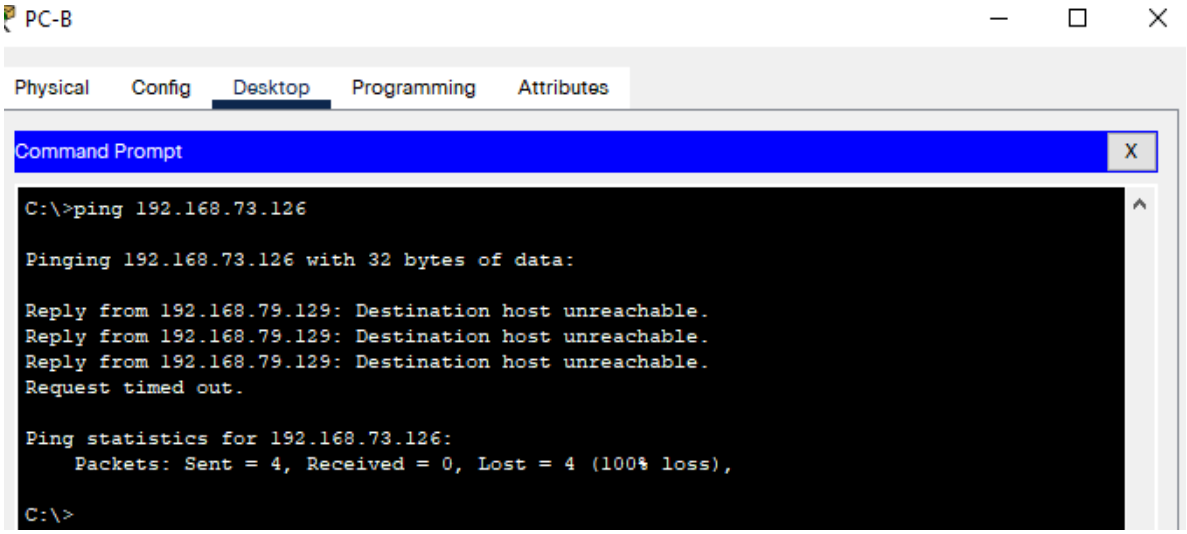

Fuente propia.

Figura 5. Ping desde PC-A a PC-B



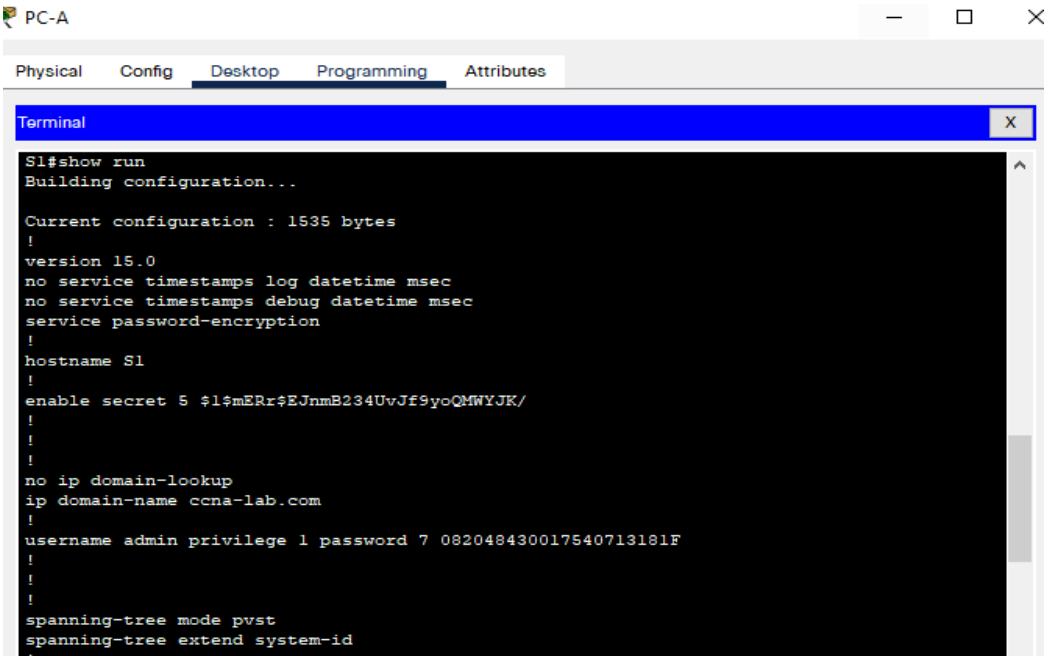

Fuente propia.

Figura 6. Ping desde PC-B a PC-A



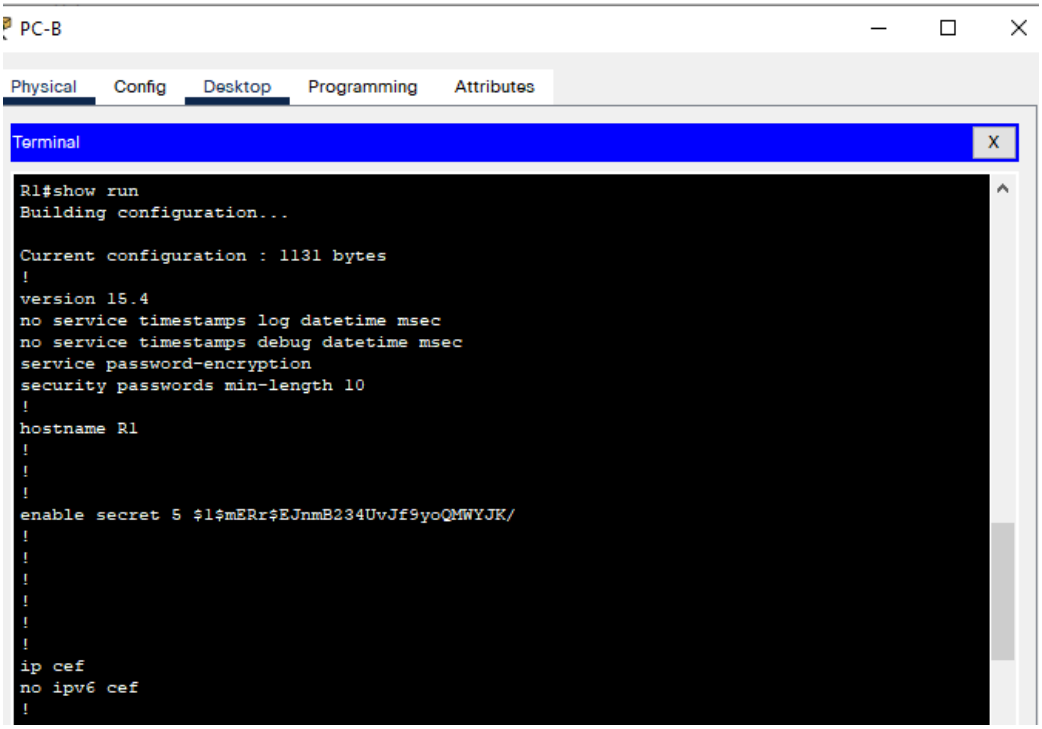

Fuente propia.

Figura 7. Comando Show run en S1.




Fuente propia.

Figura 8. Comando Show run en R1.



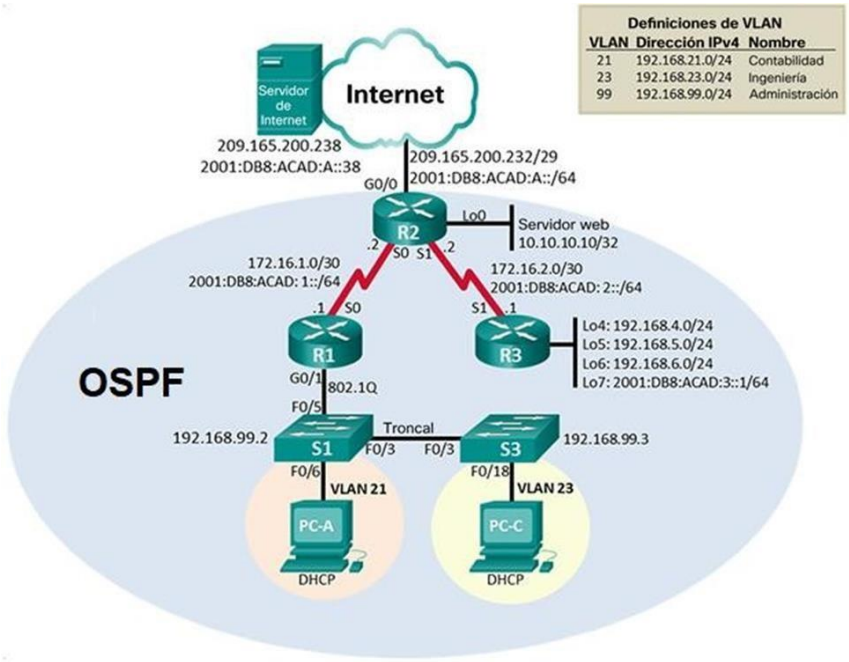

Fuente propia.

# 2. DESARROLLO ESCENARIO 2.

## 2.1. Escenario 2.

Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, 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. Ver figura 9.

Figura 9. Topología Escenario 2.



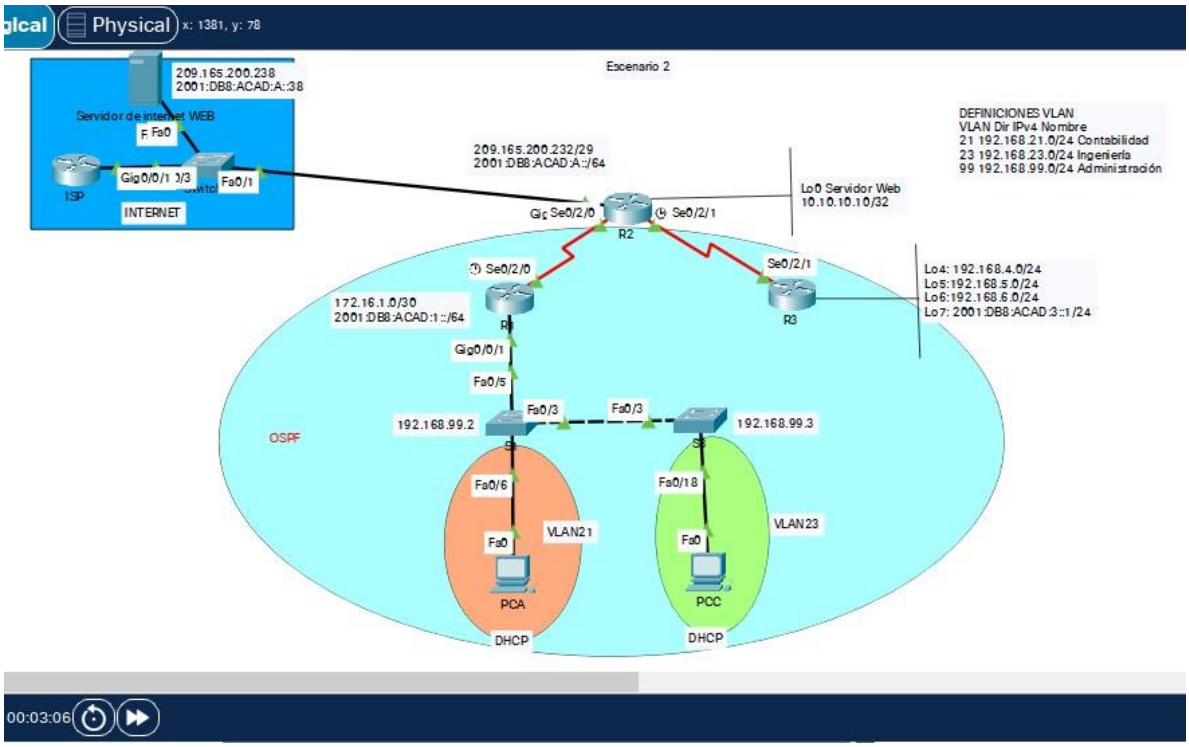

Fuente: Prueba de habilidades prácticas CCNA.

## 2.2. Creación de la Topología lógica de red.

Se crea la topología lógica de red, con los aspectos básicos de configuración solicitados en el Escenario2, realizando el cableado correspondiente y la conexión de un servidor a internet, tres Router, interfaces virtuales, dos switch y dos equipos de cómputo, mediante la herramienta Packet Tracer.

Esta topología, permitirá la configuración del direccionamiento IPv4 e IPv6 en las interfaces y la administración segura de los dispositivos de red. Ver Figura 10.

Figura 10. Conexión de la topología Escenario 2.




Fuente propia.

## 2.3. PARTE 1: Iniciación de dispositivos.

### 2.3.1. Paso 1: Inicializar y cargar los Routers y los Switches.

Mediante la utilización de los comandos comunes de CLI, se hará la eliminación de configuración de inicio y se volverá a cargar los dispositivos de red. Ver tabla 6.

Tabla 6. Configuración inicial de Routers y Switches.

| Tarea | Especificación |
|---|---|
| Eliminar el archivo startup-config de todos los routers | Erase startup-config en todos los routers |
| Volver a cargar todos los routers | Reload en todos los Routers |
| Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior | Erase startup-config en todos los Switches |
| Volver a cargar ambos switches | Reload en todos los Switches |

| | |
|---|---|
| Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches | Show flash en los Switches |

Fuente propia.

## 2.4. PARTE 2: Configuración de los parámetros básicos de los dispositivos.

### 2.4.1. Paso 1: Configurar la computadora de Internet

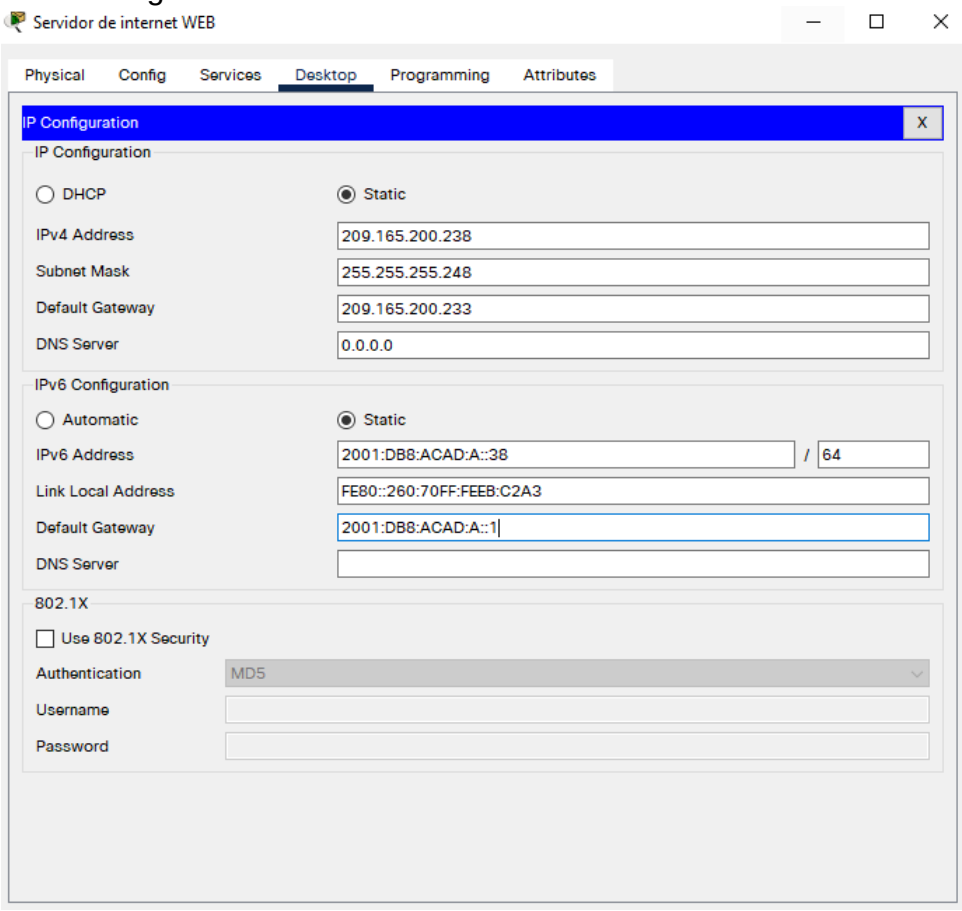
Se procede a configurar el servidor de internet, incluyendo el direccionamiento IPv4 e IPv6, de acuerdo a la topología. Utilizando comandos comunes de CLI. Ver tabla 7.

Tabla 7. Configuración de la computadora de internet.

| Tarea | Especificación |
|---|---|
| Dirección IPv4 | 209.165.200.238/29 |
| Máscara de subred para IPv4 | 255.255.255.248 |
| Gateway predeterminado | 209.165.200.233 |
| Dirección IPv6/subred | 2001:DB8:ACAD:A::38/64 |
| Gateway predeterminado IPv6 | 2001:DB8:ACAD:A::1/64 |

Fuente propia.

Figura 11. Configuración del servidor de internet.




Fuente propia.

Inicialmente se procede a configurar las interfaces del Router ISP. Anexo código de verificación:

Router>enable Se ingresa al modo EXEC privilegiado
Router#confi t Se ingresa al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int g0/0/0 Se ingresa a la interfaz g0/0/0 del router
Router(config-if)#ip address 209.165.200.234 255.255.255.248 Se configura la dirección IP y máscara de subred para esa interfaz
Router(config-if)#no shutdown Se activa la interfaz

### 2.4.2. Paso 2: Configuración de R1.

Se procede a configurar a R1, de acuerdo a la topología, de acuerdo a la topología. Ver tabla 8.

Tabla 8. Configuración de R1.

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | no ip domain-lookup |
| Nombre del router | R1 |
| Contraseña de exec privilegiado cifrada | class |
| Contraseña de acceso a la consola | cisco |
| Contraseña de acceso Telnet | cisco |
| Cifrar las contraseñas de texto no cifrado | |
| Mensaje MOTD | Se prohíbe el acceso no autorizado. |
| Interfaz S0/2/0 | Conexión R1<br>172.16.1.1 255.255.255.252<br>2001:DB8:ACAD:1::1/64<br>Establecer la frecuencia de reloj en 128000<br>Activar la interfaz |
| Rutas predeterminadas | Configurar una ruta IPv4 predeterminada de S0/0/0<br>Configurar una ruta IPv6 predeterminada de S0/0/0 |

Fuente propia.

Anexo código de verificación:

Router>en Ingreso a modo privilegiado.
Router#conf t Ingreso a modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup Desactivo búsqueda DNS.
Router(config)#hostname R1 Asigno nombre al router
R1(config)#enable secret class Se configura contraseña en modo privilegiado
R1(config)#line console 0 Se ingresa a la línea de consola
R1(config-line)#password cisco Asigno contraseña de acceso a la consola
R1(config-line)#login Se habilita contraseña, autenticación local
R1(config-line)#exit Se da un paso atrás

R1(config)#line vty 0 4 Inicio sesión línea vty para uso de la base datos local
R1(config-line)#password cisco Asigno contraseña a la línea vty
R1(config-line)#login Se habilita contraseña
R1(config-line)#exit Se da un paso atrás
R1(config)#service password-encryption Se cifran la contraseña de texto no cifrado
R1(config)#banner motd "Se prohibe el acceso no autorizado" Se configura contenido de mensaje de aviso.
R1(config)#ipv6 unicast-routing Se establece el direccionamiento IPv6
R1(config)#int se0/2/0 Configuro interfaz S0/0/0
R1(config-if)#description interface hacia el router R2 Descripción de la interfaz
R1(config-if)#ip address 172.16.1.1 255.255.255.252 Se Establece la dirección IPv4
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 Se Establece la dirección IPv6
R1(config-if)#clock rate 128000 se establecer la frecuencia de reloj
R1(config-if)#no sh Se sube la interface
%LINK-5-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 Ruta IPv4 predeterminada
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#ipv6 route 2001:DB8:ACAD:1::/64 s0/2/0 Ruta IPv6 predeterminada
R1(config)#

### 2.4.3. Paso 3: Configuración de R2.

Se procede a configurar a R2, de acuerdo a la topología, de acuerdo a la topología. Ver tabla 9.

Tabla 9. Configuración de R2

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | |
| Nombre del router | R2 |
| Contraseña de exec privilegiado cifrada | class |
| Contraseña de acceso a la consola | cisco |

| | |
|---|---|
| Contraseña de acceso Telnet | cisco |
| Cifrar las contraseñas de texto no cifrado | |
| Habilitar el servidor HTTP | Se habilita manualmente servicio HTTP. |
| Mensaje MOTD | Se prohíbe el acceso no autorizado. |
| Interfaz S0/2/0 | Establezca la descripción<br>172.16.1.2 255.255.255.252<br>2001:DB8:ACAD:1::2/64.<br>Activar la interfaz |
| Interfaz S0/2/1 | Establecer la descripción 172.16.2.2 255.255.255.252<br>2001:DB8:ACAD:2::2/64.<br>Establecer la frecuencia de reloj en128000. Activar la interfaz |
| Interfaz G0/0/0 (simulación de Internet) | Establecer la descripción.<br>209.165.200.233 255.255.255.248<br>2001:DB8:ACAD:A::1/64<br>Activar la interfaz |
| Interfaz loopback 0 (servidor web simulado) | Establecer la descripción.<br>Establezca la dirección IPv4. |
| Ruta predeterminada | Configure una ruta IPv4 predeterminada de G0/0/0.<br>Configure una ruta IPv6 predeterminada de G0/0/0. |

Fuente propia.

Anexo código de verificación:

Router>en Ingreso a modo privilegiado
Router#conf t Ingreso a modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup Desactivo búsqueda DNS
Router(config)#hostname R2 Asigno nombre al router
R2(config)#enable secret class Se configura contraseña en modo privilegiado
R2(config)#line console 0 Se ingresa a la línea de consola
R2(config-line)#password cisco Asigno contraseña de acceso a la consola

R2(config-line)#login Se habilita contraseña, autenticación local
R2(config-line)#exit Se da un paso atrás
R2(config)#line vty 0 4 Inicio sesión línea vty para uso de la base datos local
R2(config-line)#password cisco Asigno contraseña a la línea vty
R2(config-line)#login Se habilita contraseña
R2(config-line)#exit Se da un paso atrás
R2(config)#service password-encryption Se cifran la contraseña de texto no cifrado
R2(config)#banner motd "Se prohibe el acceso no autorizado" Se configura contenido de mensaje de aviso
R2(config)#ipv6 unicast-routing Se establece el direccionamiento IPv6
R2(config)#int se0/2/0 Configuro interfaz S0/2/0
R2(config-if)#description Conexion a R1 Descripción de la interfaz
R2(config-if)#ip address 172.16.1.2 255.255.255.252 Se Establece la dirección IPv4
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 Se Establece la dirección IPv6
R2(config-if)#no sh Se sube la interface
R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
R2(config-if)#int s0/2/1 Configuro interfaz S0/2/1
R2(config-if)#description Conexion a R3 Descripción de la interfaz
R2(config-if)#ip address 172.16.2.2 255.255.255.252 Se Establece la dirección IPv4
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 Se Establece la dirección IPv6
R2(config-if)#clock rate 128000 se establecer la frecuencia de reloj
R2(config-if)#no sh Se sube la interfaz
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#
R2(config-if)#exit Se da un paso atrás
R2(config)# ipv6 unicast-routing Se establece el direccionamiento IPv6
R2(config)#int g0/0/0 Configuro interfaz g0/0
R2(config-if)#description Conexion al Servidor Internet Descripción de interfaz
R2(config-if)#ip address 209.165.200.233 255.255.255.248 Se Establece la dirección IPv4

R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 Se Establece la dirección IPv6
R2(config-if)#no sh se activa la interfaz
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
R2(config-if)#exit Se da un paso atrás
R2(config)#int lo0 Configuro interfaz loopback 0
R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R2(config-if)#description Conexión Servidor Web Simulado Descripción de la interfaz
R2(config-if)#ip address 10.10.10.10 255.255.255.255 Se Establece la dirección virtual
R2(config-if)#ip route 0.0.0.0 0.0.0.0 g0/0/0 Se Establece la dirección virtual
%Default route without gateway, if not a point-to-point interface, may impact performance
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0/0 Ruta IPv4 predeterminada
R2(config)# ipv6 route ::/0 G0/0/0 Ruta IPv6 predeterminada
R2(config)#end
R2#

### 2.4.4. Paso 4: Configuración de R3.

Se procede a configurar a R3, de acuerdo a la topología, de acuerdo a la topología. Ver tabla 10.

Tabla 10. Configuración de R3

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | |
| Nombre del router | R3 |
| Contraseña de exec privilegiado cifrada | class |
| Contraseña de acceso a la consola | cisco |
| Contraseña de acceso Telnet | cisco |

| | |
|---|---|
| Cifrar las contraseñas de texto no cifrado | |
| Mensaje MOTD | Se prohíbe el acceso no autorizado. |
| Interfaz S0/2/1 | Establecer la descripción<br>172.16.2.2 255.255.255.252<br>2001:DB8:ACAD:2::1/64<br>Activar la interfaz |
| Interfaz loopback 4 | 192.168.4.1 255.255.255.0 |
| Interfaz loopback 5 | 192.168.5.1 255.255.255.0 |
| Interfaz loopback 6 | 192.168.6.1 255.255.255.0 |
| Interfaz loopback 7 | 2001:DB8:ACAD:3::1/64 |

Fuente propia.

Anexo código de verificación:

Router>en Ingreso a modo privilegiado
Router#conf t Ingreso a modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup Desactivo búsqueda DNS.
Router(config)#hostname R3 Asigno nombre al router
R3(config)#enable secret class Se configura contraseña en modo privilegiado
R3(config)#line console 0 Se ingresa a la línea de consola
R3(config-line)#password cisco Asigno contraseña de acceso a la consola
R3(config-line)#login Se habilita contraseña, autenticación local
R3(config-line)#exit Se da un paso atrás
R3(config)#line vty 0 4 I inicio sesión línea vty para uso de la base datos local
R3(config-line)#password cisco Asigno contraseña a la línea vty
R3(config-line)#login Se habilita contraseña
R3(config-line)#exit Se da un paso atrás
R3(config)#service password-encryption Se cifran la contraseña de texto no cifrado
R3(config)#banner motd "Se prohibe el acceso no autorizado" Se configura contenido de mensaje de aviso
R3(config)#ipv6 unicast-routing Se establece el direccionamiento IPv6

R3(config)#int se0/2/1 Configuro interfaz S0/2/1
R3(config-if)#description Conexion a R2 Descripción de la interfaz
R3(config-if)#ip address 172.16.2.2 255.255.255.252 Se Establece la dirección IPv4
R3(config-if)#
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 Se Establece la dirección IPv6
R3(config-if)#no sh se sube la interfaz
R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
R3(config-if)#exit Se da un paso atrás
R3(config)#int lo4 Configuro interfaz Lo4
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)#exit Se da un paso atrás
R3(config)#int lo4
R3(config-if)#ip address 192.168.4.1 255.255.255.0 se establece la dirección IPv4
R3(config-if)#exit
R3(config)#int lo5 Configuro interfaz Lo5
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)#exit
R3(config)#int lo5
R3(config-if)#ip address 192.168.5.1 255.255.255.0 se establece la dirección IPv4
R3(config-if)#exit Se da un paso atrás
R3(config)#
R3(config)#int lo6 Configuro interfaz Lo6
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up
R3(config-if)#exit
R3(config)#int lo6
R3(config-if)#ip address 192.168.6.1 255.255.255.0 se establece la dirección IPv4

R3(config-if)#exit Se da un paso atrás
R3(config)#int lo7 Configuro interfaz Lo7
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback7, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up
R3(config-if)#exit
R3(config)#int lo7
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 se establece la dirección IPv6
R3(config-if)#exit Se da un paso atrás
R3(config)#ip route 0.0.0.0 0.0.0.0 S0/2/1 Ruta IPv4 predeterminada
%Default route without gateway, if not a point-to-point interface, may impact performance
R3(config)#ipv6 route ::/0 S0/2/1 Ruta IPv6 predeterminada
R3(config)#

### 2.4.5. Paso 5: Configuración de S1.

Se procede a configurar a S1, de acuerdo a la topología, de acuerdo a la topología. Ver tabla 11.

Tabla 11. Configuración de S1.

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

Fuente propia.

Anexo código de verificación:

Switch# Ingreso a modo de configuración
Switch#conf t Ingreso a modo de configuración

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup Desactivo búsqueda DNS.
Switch(config)#hostname S1 Asigno nombre al switch
S1(config)#enable secret class Se configura contraseña en modo privilegiado
S1(config)#line console 0 Se ingresa a la línea de consola
S1(config-line)#password cisco Asigno contraseña de acceso a la consola
S1(config-line)#login Se habilita contraseña, autenticación local
S1(config)#line vty 0 15 Inicio sesión línea vty para acceso a telnet
S1(config-line)#password cisco Asigno contraseña de acceso
S1(config-line)#login Se habilita contraseña
S1(config-line)#exit Se da un paso atrás
S1(config)#service password-encryption Se cifran la contraseña de texto no cifrado
S1(config)#banner motd "Se prohibe el acceso no autorizado" Se configura contenido de mensaje de aviso
S1(config)#

### 2.4.6. Paso 6: Configuración de S3.

Se procede a configurar a S3, de acuerdo a la topología, de acuerdo a la topología. Ver tabla 12.

Tabla 12. Configuración de S3.

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

Fuente propia.

Anexo código de verificación:

Switch# Ingreso a modo de configuración
Switch#conf t Ingreso a modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup Desactivo búsqueda DNS.
Switch(config)#hostname S3 Asigno nombre al switch
S3(config)#enable secret class Se configura contraseña en modo privilegiado
S3(config)#line console 0 Se ingresa a la línea de consola
S3config-line)#password cisco Asigno contraseña de acceso a la consola
S3(config-line)#login Se habilita contraseña, autenticación local
S3(config)#line vty 0 15 Inicio sesión línea VTY para acceso a telnet
S3(config-line)#password cisco Asigno contraseña de acceso
S3(config-line)#login Se habilita contraseña
S3(config-line)#exit Se da un paso atrás
S3(config)#service password-encryption Se cifran la contraseña de texto no cifrado
S3(config)#banner motd "Se prohibe el acceso no autorizado" Se configura contenido de mensaje de aviso
S3(config)#

### 2.4.7. Paso 7: Verificación de la conectividad de la red.

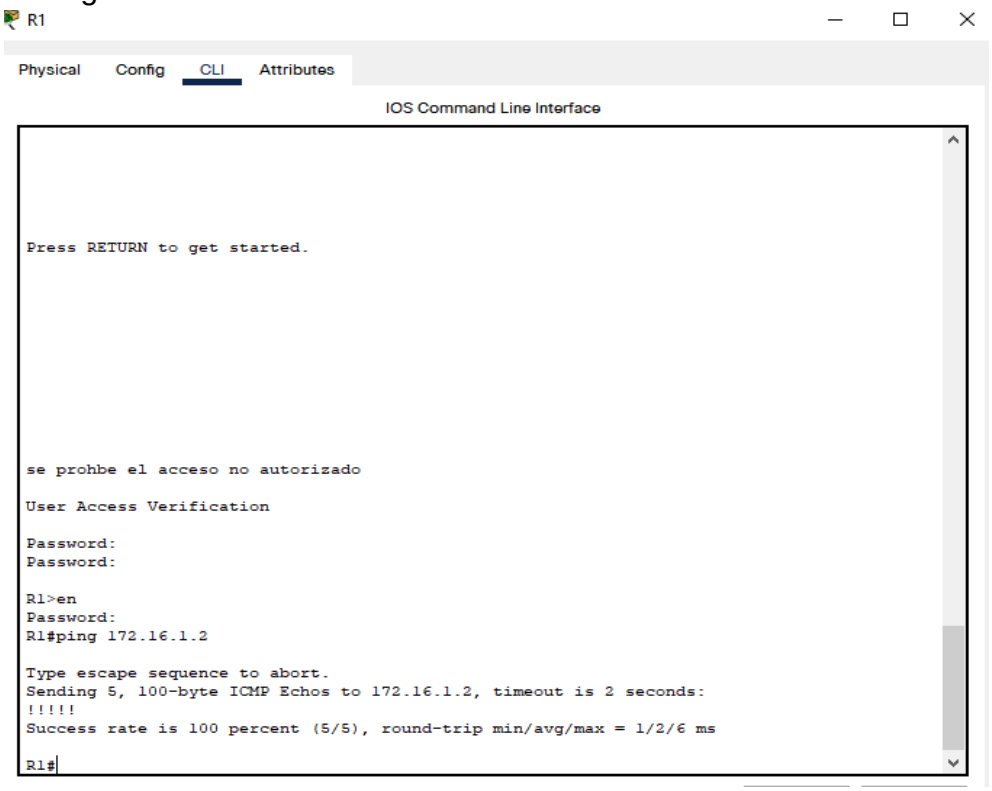
Mediante la utilización de comando ping, Se procede a verificar la conectividad en cada dispositivo de red. Ver tabla 13.

Tabla 13. Verificación de conectividad en dispositivo.

| Desde | A | Dirección IP | Resultados de ping |
|---|---|---|---|
| R1 | R2, S0/2/0 | 172.16.1.2 | 100 porcent (5/5)<br>Exitoso. |
| R2 | R3, S0/2/1 | 172.16.2.1 | 100 porcent (5/5)<br>Exitoso. |
| PC de Internet | Gateway predeterminado | 209.165.200.233<br>2001:DB8:ACAD:A::1 | Send = 4 Received = 4<br>Exitoso.<br>Send = 4 Received = 4<br>Exitoso. |

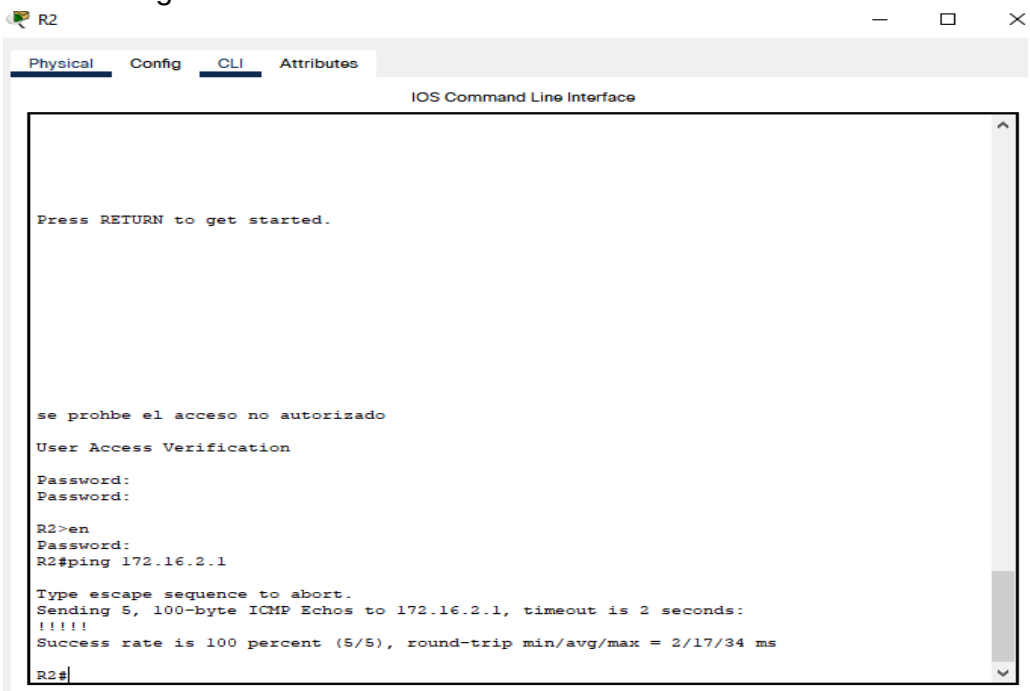
Fuente propia.

Figura 12. Ping desde R1 a R2.



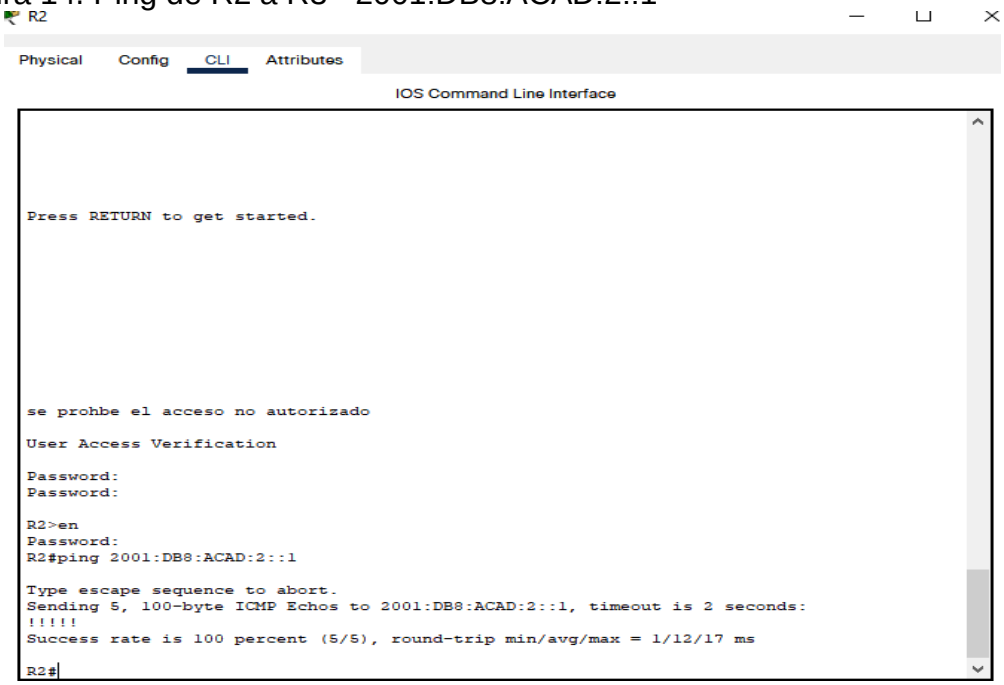

Fuente propia.

Figura 13. Ping de R2 a R3 - 172.16.2.2.



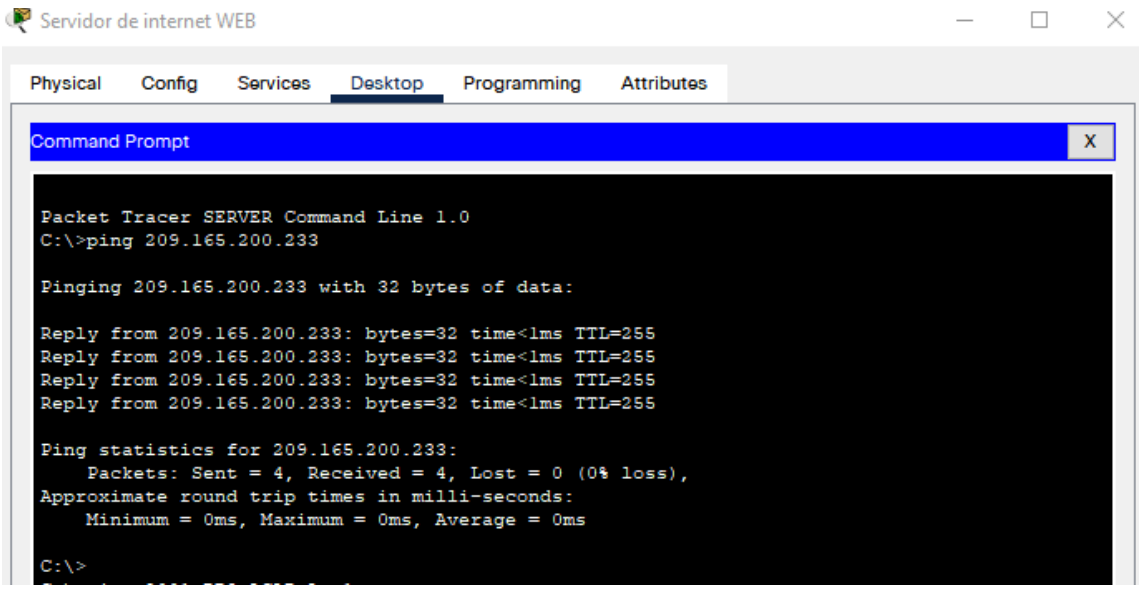

Fuente propia.

Figura 14. Ping de R2 a R3 - 2001:DB8:ACAD:2::1



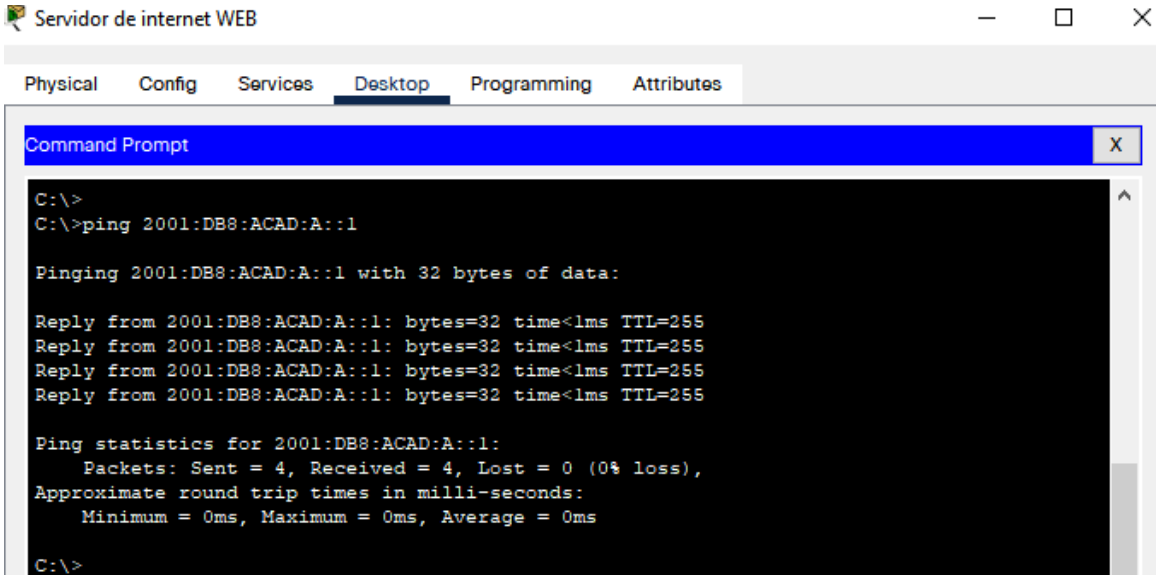

Fuente propia.

Figura 15. Ping desde PC de internet a Gateway 209.165.200.233




Fuente propia.

Figura 16. Ping desde PC de internet a Gateway 2001:DB8:ACAD:A::1.




Fuente propia.

## 2.5. PARTE 3: Configuración de la seguridad del switch, las VLAN y el routing entre VLAN.

### 2.5.1. Paso 1: Configuración de S1.

Se procede a realizar la configuración del S1 incluye las siguientes tareas. Ver tabla 14.

Tabla 14. Configuración de seguridad en S1.

| Elemento o tarea de configuración | Especificación |
|---|---|
| Crear la base de datos de VLAN | Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican |
| Asignar la dirección IP deadministración. | Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama detopología |
| Asignar el gateway predeterminado | Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. |
| Forzar el enlace troncal en la interfazF0/3 | Utilizar la red VLAN 1 como VLAN |

| | |
|---|---|
| | nativa |
| Forzar el enlace troncal en la interfazF0/5 | Utilizar la red VLAN 1 como VLAN nativa |
| Configurar el resto de los puertos comopuertos de acceso | Utilizar el comando interface range |
| Asignar F0/6 a la VLAN 21 | |
| Apagar todos los puertos sin usar | |

Fuente propia.

Anexo código de verificación:

```
S1>en
Password:
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 21                          Se crea la base de datos de VLAN 21
S1(config-vlan)#name CONTABILIDAD           Se asigna nombre de la VLAN
S1(config-vlan)#vlan 23                     Se crea la base de datos de
VLAN 23
S1(config-vlan)#name INGENIERIA             Se asigna nombre de la VLAN
S1(config-vlan)#vlan 99                     Se crea la base de datos de
VLAN 99
S1(config-vlan)#name ADMINISTRACION Se asigna nombre de la VLAN
S1(config-vlan)#exit                                Se da un paso atrás
S1(config)#int vlan 99                              ingreso la interfaz VLAN
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
S1(config-if)#ip address 192.168.99.2 255.255.255.0 Se establece el
direccionamiento IPv4
S1(config-if)#no sh                                 Se active la interfaz
S1(config-if)#exit                                  Se da un paso atrás
S1(config)#ip default-gateway 192.168.99.1          Se establece la gateway
predeterminada
S1(config)#int f0/3                                 Configuro interfaz fa0/3
S1(config-if)#sw mode trunk                 Se fuerza el enlace troncal en la
interfaz
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed
S1(config-if)#sw trunk native vlan 1        Se utiliza la VLAN 1 como enlace
troncal nativa
```

S1(config-if)#exit
Paso atrás
S1(config)#int f0/5 Configuro interfaz fa0/5
S1(config-if)#sw mode trunk Se fuerza el enlace troncal en la interfaz
S1(config-if)#sw trunk native vlan 1 Se utiliza la VLAN 1 como enlace troncal nativa
S1(config-if)#exit
S1(config)#int range f0/1- f0/2 Se ingresa rango de interfaces
S1(config-if-range)#sw mode access Se configura como puertos de acceso
S1(config-if-range)#int range f0/7- f0/24 Se ingresa rango de interfaces
S1(config-if-range)#sw mode access Se configura como puertos de acceso
S1(config-if-range)#exit
S1(config)#int f0/6 Se ingresa la interfaz fa0/5
S1(config-if)#sw mode access Se configuran puertos de acceso
S1(config-if)#sw access vlan 21 Se utiliza la VLAN 1 como enlace troncal nativa
S1(config-if)#exit
S1(config)#int range f0/7- f0/24 Se ingresa rango de interfaces
S1(config-if-range)#shutdown Se apagan los puertos de ese rango sin usar

### 2.5.2. Paso 2: Configuración de S3.

Se procede a realizar la configuración del S2, incluye las siguientes tareas. Ver tabla 15.

Tabla 15. Configuración de seguridad en S3.

| Elemento o tarea de configuración | Especificación |
|---|---|
| Crear la base de datos de VLAN | Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombrea cada VLAN. |
| Asignar la dirección IP de administración | Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama detopología |
| Asignar el gateway predeterminado. | Asignar la primera dirección IP en la subred como gateway predeterminado. |
| Forzar el enlace troncal en la | |

| | |
|---|---|
| interfazF0/3 | Utilizar la red VLAN 1 como VLAN nativa |
| Configurar el resto de los puertos comopuertos de acceso | Utilizar el comando interface range |
| Asignar F0/18 a la VLAN 21 | |
| Apagar todos los puertos sin usar | |

Fuente propia.

Anexo código de verificación:

S3(config)#vlan 21 Se crea la base de datos de VLAN 21
S3(config-vlan)#name CONTABILIDAD Se asigna nombre de la VLAN
S3(config-vlan)#vlan 23 Se crea la base de datos de VLAN 23
S3(config-vlan)#name INGENIERIA Se asigna nombre de la VLAN
S3(config-vlan)#vlan 99 Se crea la base de datos de VLAN 99
S3(config-vlan)#name ADMINISTRACION Se asigna nombre de la VLAN
S3(config-vlan)#exit Se da un paso atrás
S1(config)#int vlan 99 ingresa la interfaz VLAN
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
S3(config-if)#ip address 192.168.99.3 255.255.255.0 Se asigna direcionamiento ipv4 la interfaz
S3(config-if)#no sh Se activa la interfaz
S3(config-if)#exit Se un paso atrás
S3(config)#ip default-gateway 192.168.99.1 Se asigna el gateway predeterminado
S3(config)#int f0/3 Se ingresa a la interfaz f0/3
S3(config-if)#sw mode trunk Se fuerza el enlace troncal en la interfaz
S3(config-if)#sw trunk native vlan 1 Se utiliza la vlan 1 como enlace truncal nativa
S3(config-if)#exit Se sale de la interfaz
S3(config)#int range f0/1 - f0/2 Se ingresa al rango de interfaces
S3(config-if-range)#sw mode access Se configura como puertos de acceso
S3(config-if-range)#int range f0/7 - f0/24 Se ingresa al rango de interfaces
S3(config-if-range)#sw mode access Se configura como puertos de acceso
S3(config-if-range)#exit Se sale de la interfaz
S3(config)#int f0/18 Se ingresa a la interfz f0/18
S3(config-if)#sw access vlan 21 Se asigna la vlan 21 a la interfaz

S3(config-if)#exit — Se sale de la interfaz
S3(config)#int range f0/7 - f0/17 — Se ingresa al rango de interfaces
S3(config-if-range)#shutdown — Se apagan esos puertos
S3(config-if-range)#exit — Se sale de ese rango de interfaces
S3(config)#int range f0/19 - f0/24 — Se ingresa al rango de interfaces
S3(config-if-range)#shutdown — Se apagan esos puertos

### 2.5.3. Paso 3: Configuración de R1.

Se procede a realizar la configuración del R1, incluye las siguientes tareas Ver tabla 16.

Tabla 16. Configuración de seguridad en R1.

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

Fuente propia.

Anexo código de verificación:

```
R1(config)#int g0/0/1                                   Se ingresa a la interfaz g00//1
R1(config-if)#no shutdown                               Se activa la interfaz
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                                      Se sale de la interfaz
R1(config)#int g0/0/1.21                                Se ingresa a la subinterfaz g0/0/1.21
R1(config-subif)#description LAN de CONTABILIDAD se realiza descripción de la interfaz
R1(config-subif)#encapsulation dot1Q 21 Se habilita 802.1Q y asociar una VLAN específica VLAN a la subinterfaz
R1(config-subif)#ip address 192.168.21.1 255.255.255.0 Se Establece la dirección IPv4
R1(config-subif)#exit
R1(config)#int g0/0/1.23                                Se ingresa a la interfaz g0/0/1.23
R1(config-subif)#description LAN de INGENIERIA Se realiza descripción de la interfaz
R1(config-subif)#encapsulation dot1Q 23 Se habilita 802.1Q y asociar una VLAN específica VLAN a la subinterfaz
R1(config-subif)#ip address 192.168.23.1 255.255.255.0 Se Establece la dirección IPv4
R1(config-subif)#exit
R1(config)#int g0/0/1.99                                Se ingresa a la interfaz g0/0/1.99
R1(config-subif)#description LAN de ADMINISTRACION      se realiza descripción de la interfaz
R1(config-subif)#encapsulation dot1Q 99 Se habilita 802.1Q y asociar una VLAN específica VLAN a la subinterfaz
R1(config-subif)#ip address 192.168.99.1 255.255.255.0 Se Establece la dirección IPv4
R1(config-subif)#exit                                   Se da un paso atrás
```

### 2.5.4. Paso 4: Verificación de la conectividad de la red.

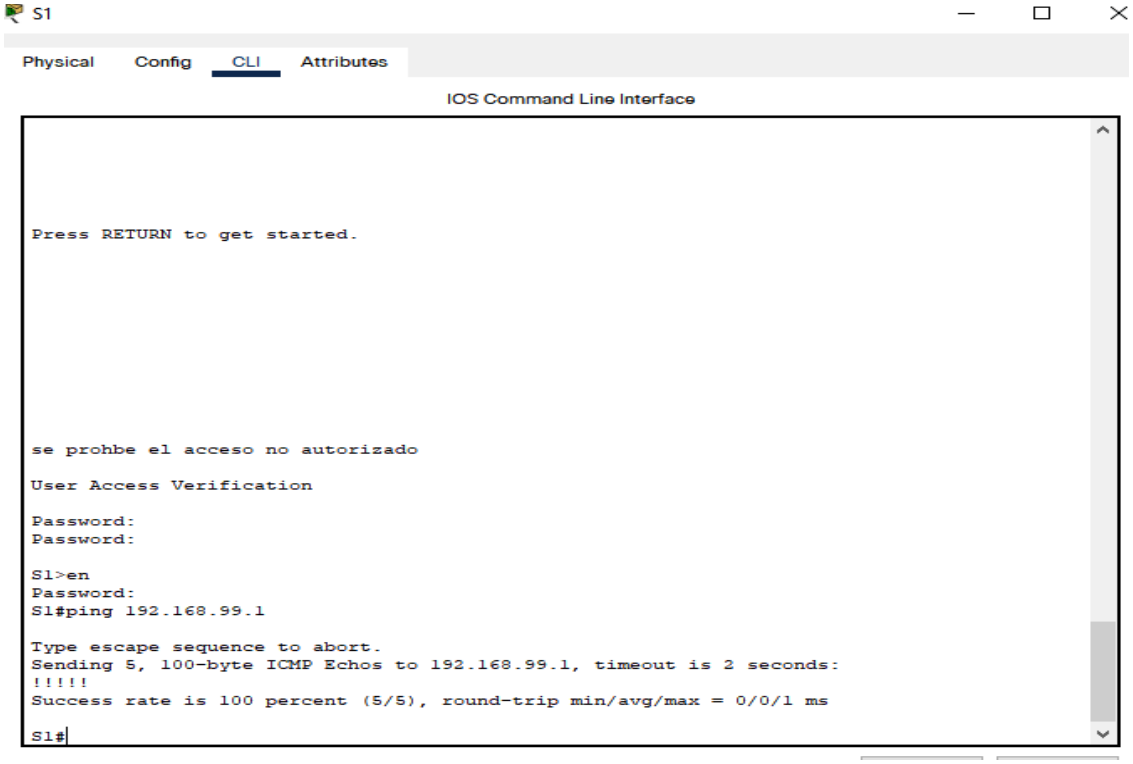
Mediante la utilización de comando ping, Se procede a verificar la conectividad en cada dispositivo de red. Ver tabla 17.

Tabla 17. Verificación de conectividad en dispositivo.

| Desde | A | Dirección IP | Resultados de ping |
|---|---|---|---|
| S1 | R1, dirección VLAN 99 | 192.168.99.1 | 100 porcent (5/5) Exitoso |
| S3 | R1, dirección VLAN 99 | 192.168.99.1 | 100 porcent (5/5) Exitoso |
| S1 | R1, dirección VLAN 21 | 192.168.21.1 | 100 porcent (5/5) Exitoso. |
| S3 | R1, dirección VLAN 23 | 192.168.23.1 | 100 porcent (5/5) Exitoso. |

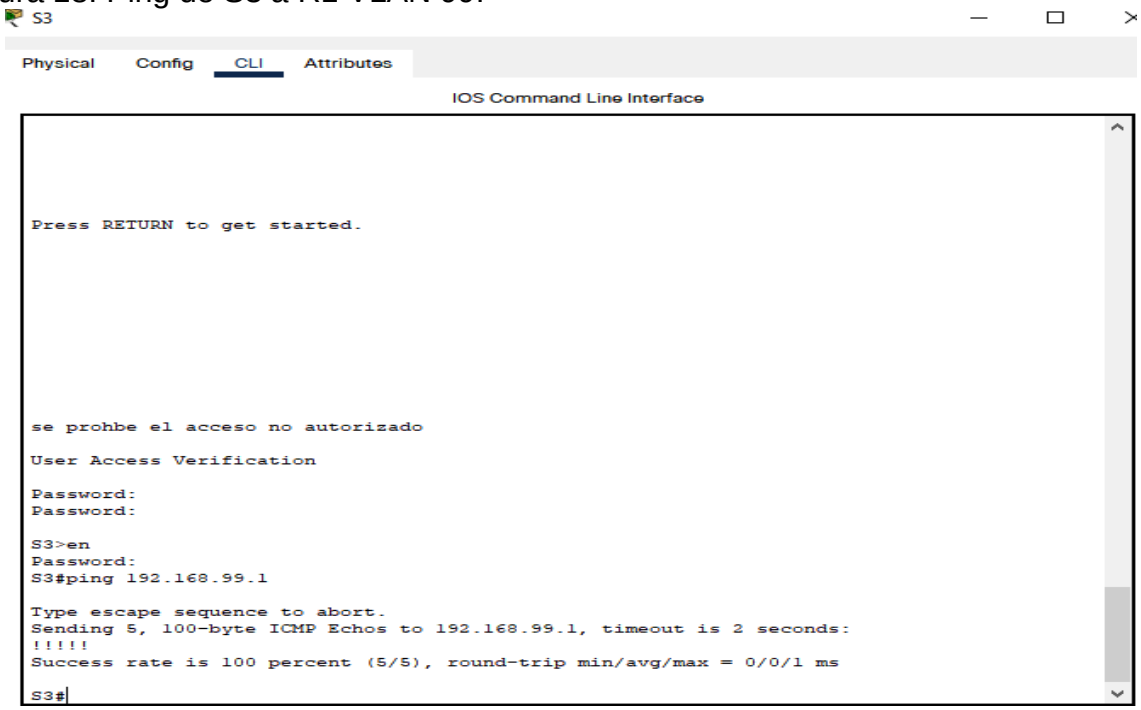
Fuente propia.

Figura 17. Ping de S1 a R1 VLAN 99



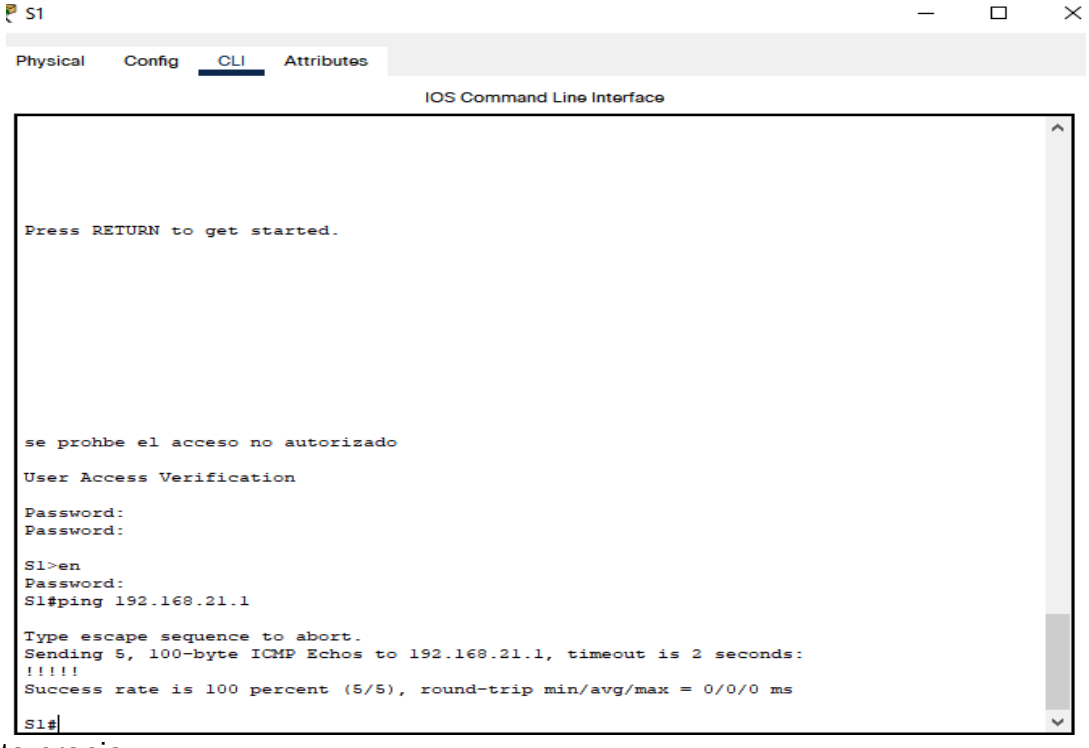

Fuente propia

Figura 18. Ping de S3 a R1 VLAN 99.



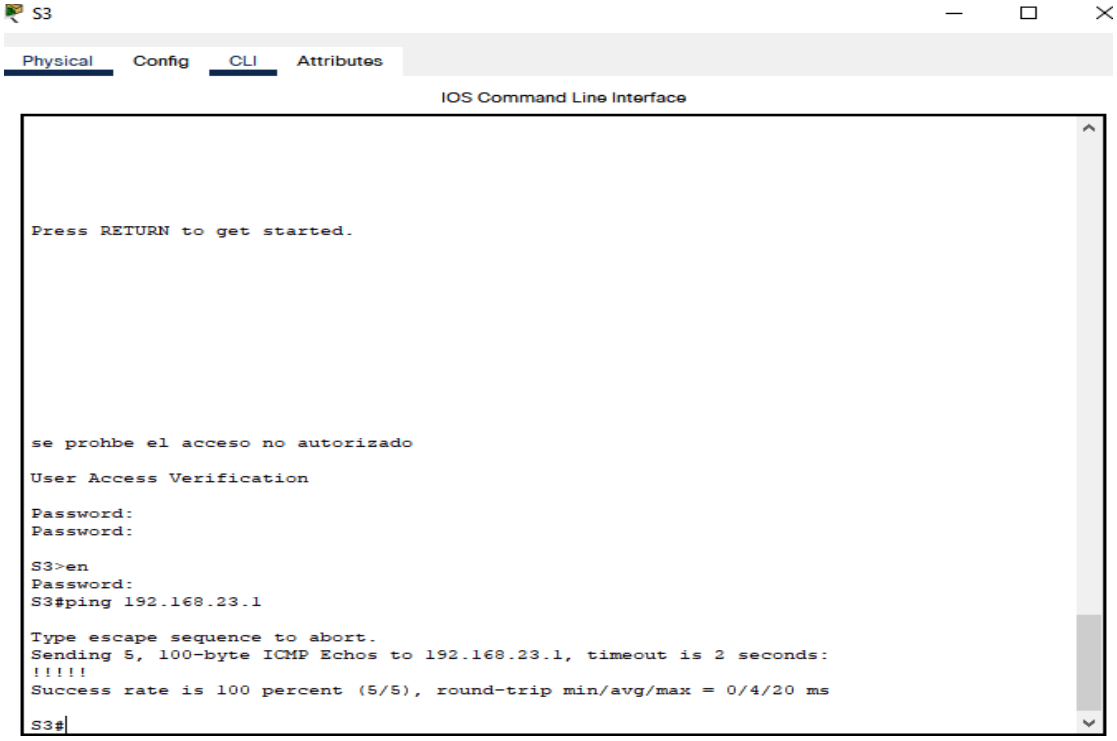

Fuente propia

Figura 19. Ping de S1 a R1 VLAN 21.




Fuente propia

Figura 20. Ping de S3 a R1 VLAN 23.




Fuente propia

## 2.6. PARTE 4: Configuración del protocolo de Routing dinámico OSPF.

### 2.6.1. Paso 1 Configurar OSPF en el R1.

Se procede a configuración de OSPF en R1. Ver tabla 18.

Tabla 18. Verificación de conectividad en dispositivo.

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar OSPF área 0 | |
| Anunciar las redes conectadas directamente | Asigne todas las redes conectadas directamente. |
| Establecer todas las interfaces LAN como pasivas | |
| Desactive la sumarización automática | En este protocolo eso no se hace, porque se coloca la wildcard. |

Fuente propia

Anexo Código de verificación:

R1(config)#router ospf 30 Activar protocolo de enrutamiento ospf en el R1
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 Red conectada y se configura en el área 0
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 Red conectada y se configura en el área 0
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0 Red conectada y se configura en el área 0
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 Red conectada y se configura en el área 0
R1(config-router)#passive-interface g0/0/1 Se establece la interface g0/0/1
R1(config-router)#passive-interface g0/0/1.21 Se establece la interface como pasiva
R1(config-router)#passive-interface g0/0/1.23 Se establece la interface como pasiva
R1(config-router)#passive-interface g0/0/1.99 Se establece la interface como pasiva
R1(config-router)#exit
R1(config)#

### 2.6.2. Paso 2: Configurar OSPF en el R2.

Se procede a configuración de OSPF en R2. Ver tabla 19.

Tabla 19. Verificación de conectividad en dispositivo.

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar OSPF área 0 | |
| Anunciar las redes conectadas directamente | **Nota:** Omitir la red G0/0. |
| Establecer la interfaz LAN (loopback) como pasiva | |
| Desactive la sumarización automática. | En este protocolo eso no se hace, porque se coloca la wildcard. |

Fuente propia.

Anexo código de verificación:

R2(config)#router ospf 30 Activar protocolo de enrutamiento ospf en el R2
R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 Red conectada y se configura en el área 0

R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 Red conectada y se configura en el área 0
R2(config-router)#
00:49:20: %OSPF-5-ADJCHG: Process 30, Nbr 192.168.99.1 on Serial0/2/0 from LOADING to FULL, Loading Done
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 Red conectada y se configura en el área 0
R2(config-router)#passive-interface loopback 0 Se establece la interface como pasiva
R2(config-router)#

### 2.6.3. Paso 3: Configurar OSPFv3 en el R2

Se procede a configuración de OSPFv3 en R2. Ver tabla 20.

Tabla 20. Verificación de conectividad en dispositivo.

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar OSPF área 0 | |
| Anunciar redes IPv4 conectadas directamente | |
| Establecer todas las interfaces de LAN IPv4 (Loopback)como pasivas | |
| Desactive la sumarización automática. | En este protocolo eso no se hace, porque se coloca la wildcard. |

Fuente propia.

Anexo código de verificación:

R3(config)#ipv6 router ospf 31 Activar protocolo de enrutamiento ospfv3 en el R3
R3(config-rtr)#router-id 2.2.2.2 Se identifica el R3 como ospfv3
R3(config-rtr)#exit Salimos de la configuración
R3(config)#int s0/2/1 Se ingresa a la interfaz s0/2/1
R3(config-if)#ipv6 ospf 31 area 0 Se activa protocolo de enrutamiento ospfv3 en la interfaz s0/0/1 y se configura en el área 0
R3(config-if)#exit Salimos de la configuración
R3(config)#int loopback 7 Se ingresa a la interfaz lo7
R3(config-if)#ipv6 ospf 31 area 0 Se activa protocolo de enrutamiento ospfv3 en la interfaz loopback 7 y se configura en el área 0

```
R3(config-if)#exit                                  Salimos de la configuración
R3(config)#ipv6 router ospf 31          Protocolo de enrutamiento ospfv3 en el R3
R3(config-rtr)#passive-interface lo 4 Se establece la interface lo4 como pasiva
R3(config-rtr)#passive-interface lo 5 Se establece la interface lo5 como pasiva
R3(config-rtr)#passive-interface lo 6 Se establece la interface lo6 como pasiva
R3(config-rtr)#exit
R3(config)#
```

### 2.6.4. Paso 4: Verificar la información de OSPF

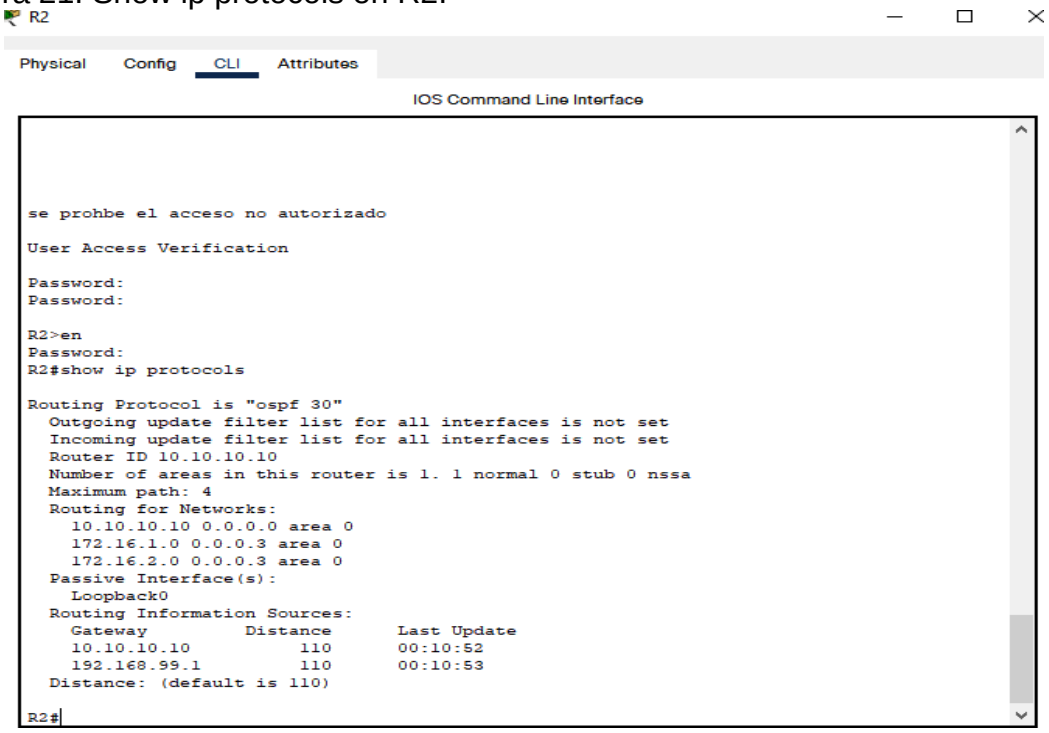
Se procede a verificar la información OSPF en R2. Ver tabla 21.

Tabla 21. Verificación de OSPF en el dispositivo.

| Elemento o tarea de configuración | Especificación |
|---|---|
| ¿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 configuraciónen ejecución? | Show ip ospf database |

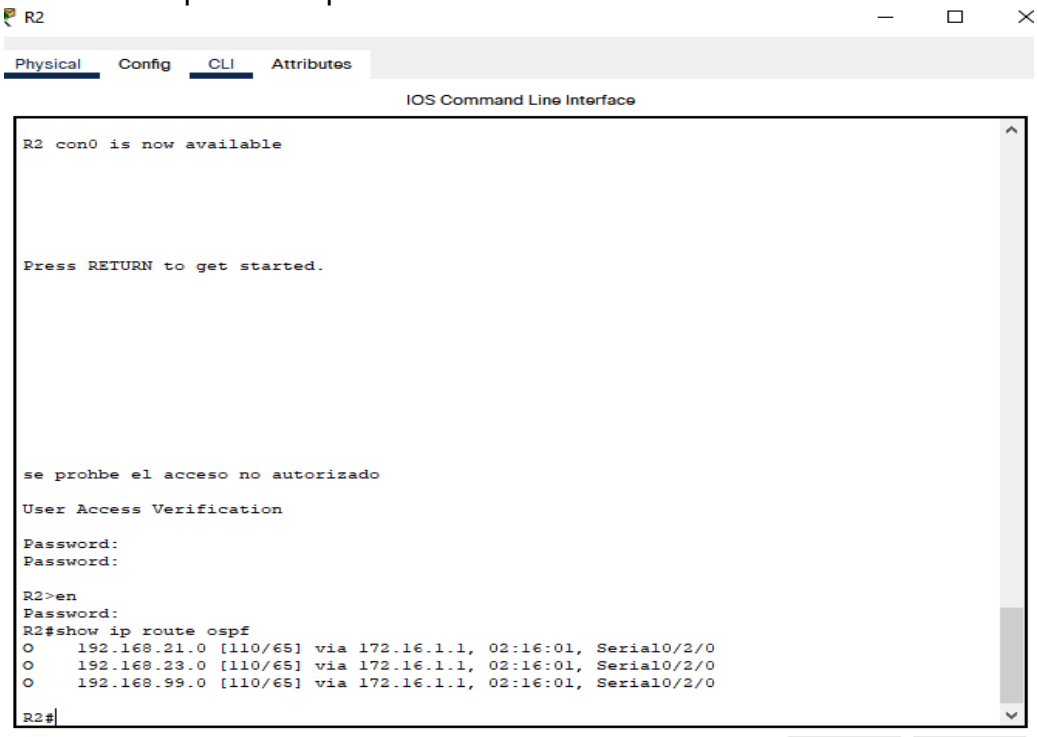
Fuente propia.

Figura 21. Show ip protocols en R2.



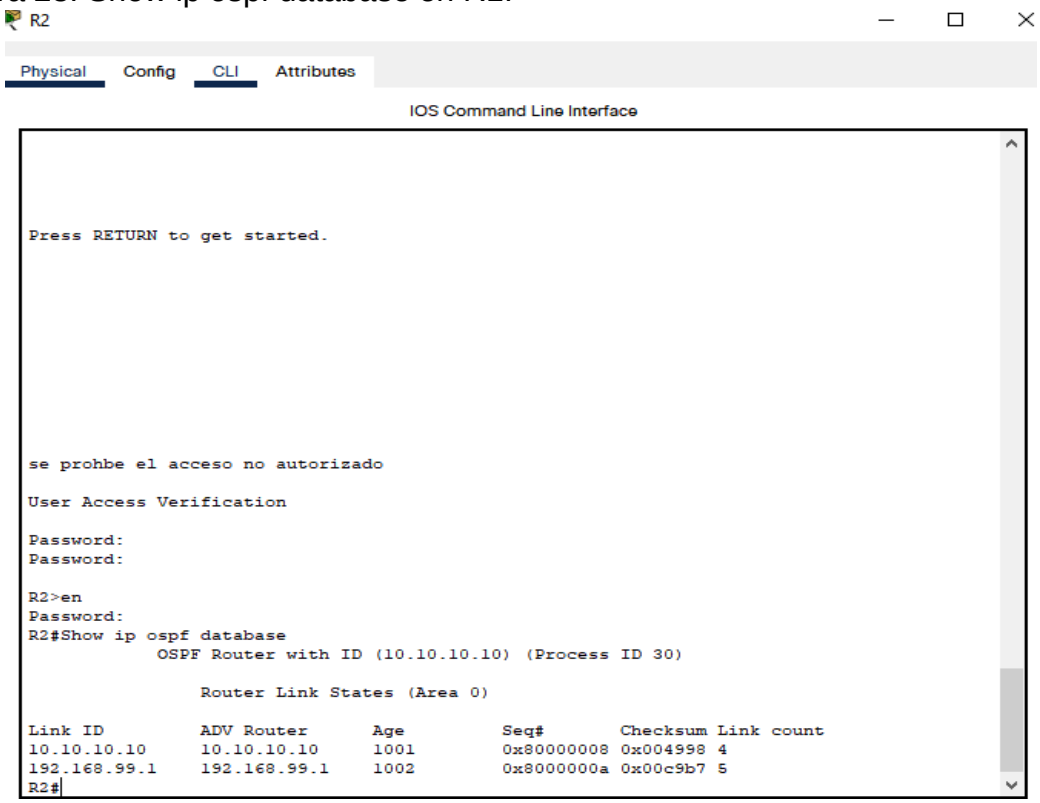

Fuente propia

Figura 22. Show ip route ospf en R2.




Fuente propia

Figura 23. Show ip ospf database en R1.




Fuente propia.

## 2.7. PARTE 5: Implementación DHCP y NAT para IPv4

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

Se procede a configuración de DHCP para las VLANS en R1. Ver tabla 22.

Tabla 22. Verificación de OSPF en el dispositivo.

| Elemento o tarea de configuración | Especificación |
|---|---|
| Reservar las primeras 20 direcciones IP enla VLAN 21 para configuraciones estáticas | |
| Reservar las primeras 20 direcciones IP enla VLAN 23 para configuraciones estáticas | |
| | Nombre: ACCT |

| | |
|---|---|
| Crear un pool de DHCP para la VLAN 21. | Servidor DNS: 10.10.10.10<br>Nombre de dominio: ccna-sa.com<br>Establecer el gateway predeterminado |
| Crear un pool de DHCP para la VLAN 23 | Nombre: ENGNR<br>Servidor DNS: 10.10.10.10<br>Nombre de dominio: ccna-sa.com<br>Establecer el gateway predeterminado |

Fuente propia.

Anexo código de verificación:

R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20 Se reservan las primeras 20 IP en VLAN 21 para configuraciones estáticas
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20 Se reservan las primeras 20 IP en VLAN 23 para configuraciones estáticas
R1(config)#ip dhcp pool ACCT Se crea un pool de DHCP con el nombre ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0 Se establece la Vlan 21 para el pool DHCP
R1(dhcp-config)#domain-name ccna-sa.com Se asigna nombre de dominio
R1(dhcp-config)#dns-server 10.10.10.10 Se establece servidor DNS
R1(dhcp-config)#default-router 192.168.21.1 Se establece el gateway predeterminado
R1(dhcp-config)#exit
R1(config)#ip dhcp pool ENGNR Se crea un pool de DHCP con nombre el ENGNR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0 Se establece la Vlan 23 para el pool DHCP
R1(dhcp-config)#dns-server 10.10.10.10 Se establece servidor DNS
R1(dhcp-config)#domain-name ccna-sa.com Se asigna nombre de dominio
R1(dhcp-config)#default-router 192.168.23.1 Se establece el gateway predeterminado
R1(dhcp-config)#

### 2.7.2. Paso 2: Configuración de la NAT estática y dinámica en el R2.

Se procede a configuración de NAT en R2. Ver tabla 23.

Tabla 23. Configuración de la NAT estática y dinámica en el R2.

| Elemento o tarea de configuración | Especificación |
|---|---|
| Crear una base de datos local con unacuenta de usuario | Nombre de usuario: webuser<br>Contraseña: cisco12345<br>Nivel de privilegio: 15 |
| Habilitar el servicio del servidor HTTP | |
| Configurar el servidor HTTP para utilizar labase de datos local para la autenticación | |
| Crear una NAT estática al servidor web. | Dirección global interna: 209.165.200.229 |
| Asignar la interfaz interna y externa para laNAT estática | |
| Configurar la NAT dinámica dentro de unaACL privada | Lista de acceso: 1<br>Permitir la traducción de las redes de Contabilidad y deIngeniería en el R1<br>Permitir la traducción de un resumen de las redes LAN(loopback) en el R3 |
| Defina el pool de direcciones IP públicasutilizables. | Nombre del conjunto: INTERNET<br>El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228 |
| Definir la traducción de NAT dinámica | |

Fuente propia.

Anexo código de verificación:

R2(config)#username webuser privilege 15 password cisco12345 Se crea base de datos local con nombre de usuario y contraseña

R2(config)#ip nat inside source static 10.10.10.10 209.165.200.233 Se crea una NAT estática
R2(config)#int g0/0/0 Se ingresa a la interfaz g0/0/0
R2(config-if)#ip nat outside Se asigna de NAT externa
R2(config-if)#int S0/2/0 Se ingresa a la interfaz s0/2/0
R2(config-if)#ip nat inside Se asigna de NAT externa
R2(config-if)#int S0/2/1 Se ingresa a la interfaz s0/2/1
R2(config-if)#ip nat inside Se asigna de NAT interna
R2(config-if)#int lo 0 Se ingresa a la interfaz Lo0
R2(config-if)#ip nat inside Se asigna de NAT interna
R2(config-if)#exit Salimos de la configuración
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 Lista de acceso 1 para contabilidad
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 Lista de acceso 1 para ingenieria
R2(config)#access-list 1 permit 192.168.0.0 0.0.3.255 Lista de acceso 1 para redes LAN(loopback) en R3.
R2(config)#ip access-list standard ADMIN-MGT Se configura la lista estándar ADMIN-
MGT
R2(config-std-nacl)#permit host 172.16.1.1 Se permite el host 172.16.1.1
R2(config-std-nacl)#deny any Se deniega el acceso a lo demás
R2(config-std-nacl)#exit
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248 Se define el pool de direccione publicas INTERNET
R2(config)#ip nat inside source list 1 pool INTERNET Se define la traducción NAT dinámica para el pool INTERNET
R2(config)#

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

Se procede a verificar las configuraciones de DHCP y NAT estática. Ver tabla 24.

Tabla 24. Verificar el protocolo DHCP y la NAT estática

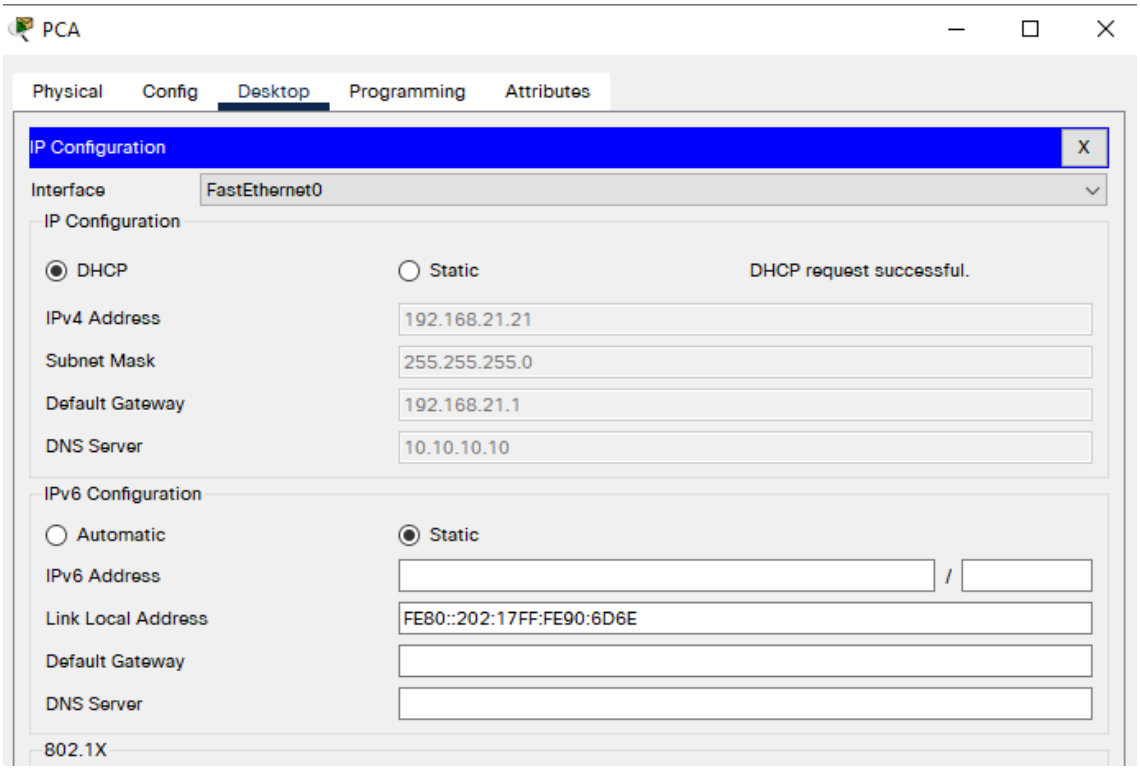
| Elemento o tarea de configuración | Especificación |
|---|---|
| Verificar que la PC-A haya adquirido información de IP del servidor de DHCP | Asigna dirección dhcp 192.168.21.21 |

| | |
|---|---|
| Verificar que la PC-C haya adquirido información de IP del servidor de DHCP | Asigna dirección dhcp 192.168.21.22 |
| Verificar que la PC-A pueda hacer ping ala PC-C<br>Nota: Quizá sea necesario deshabilitar elfirewall de la PC. | Send = 4, Received = 4 |
| Utilizar un navegador web en la computadora de Internet para acceder alservidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345 | Acceso exitoso a http://209.165.200.238 |

Fuente propia.

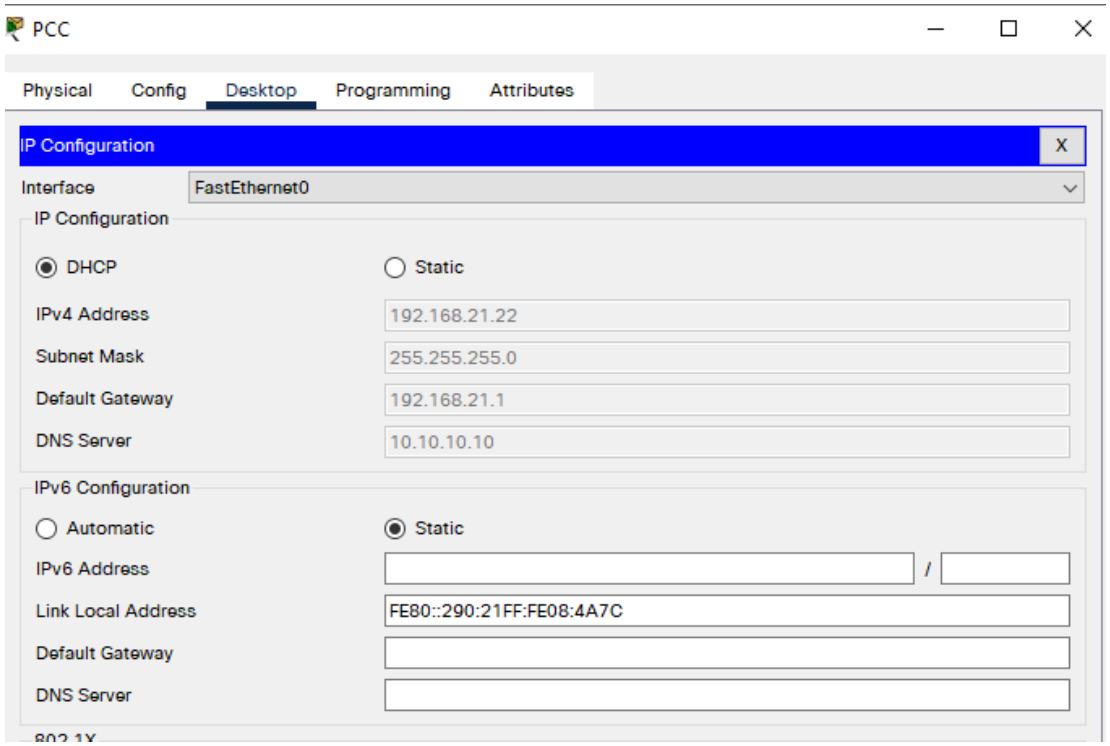
Verificación:

Figura 24. PC-A con DHCP.



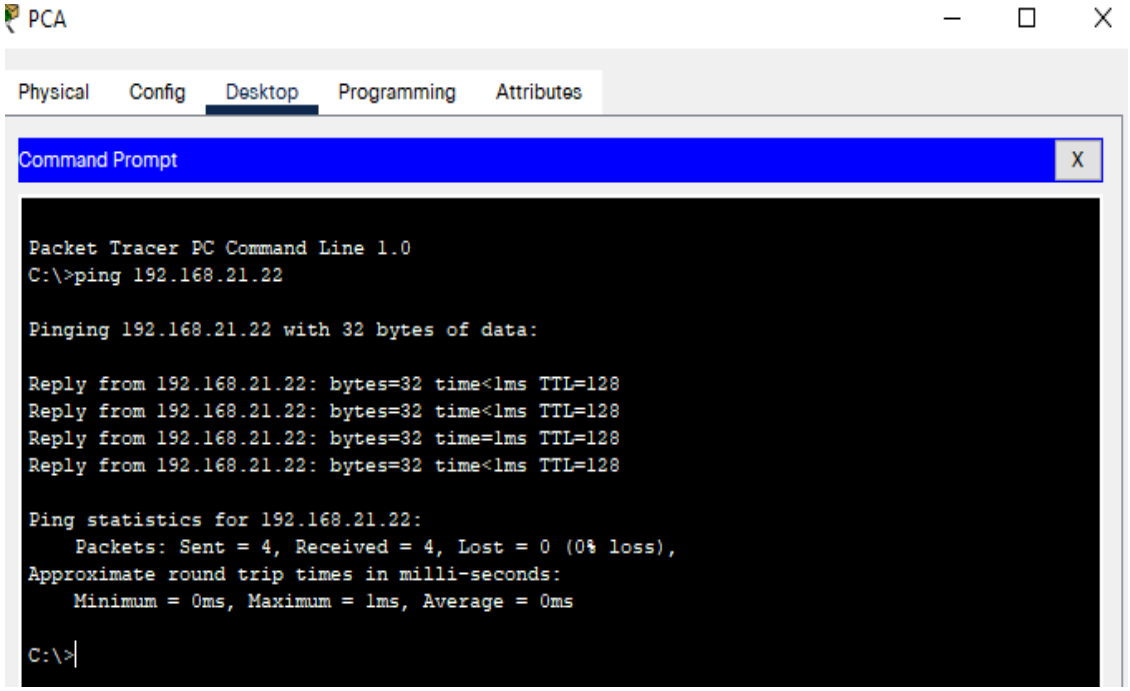

Fuente propia.

Figura 25. DHCP PC-C



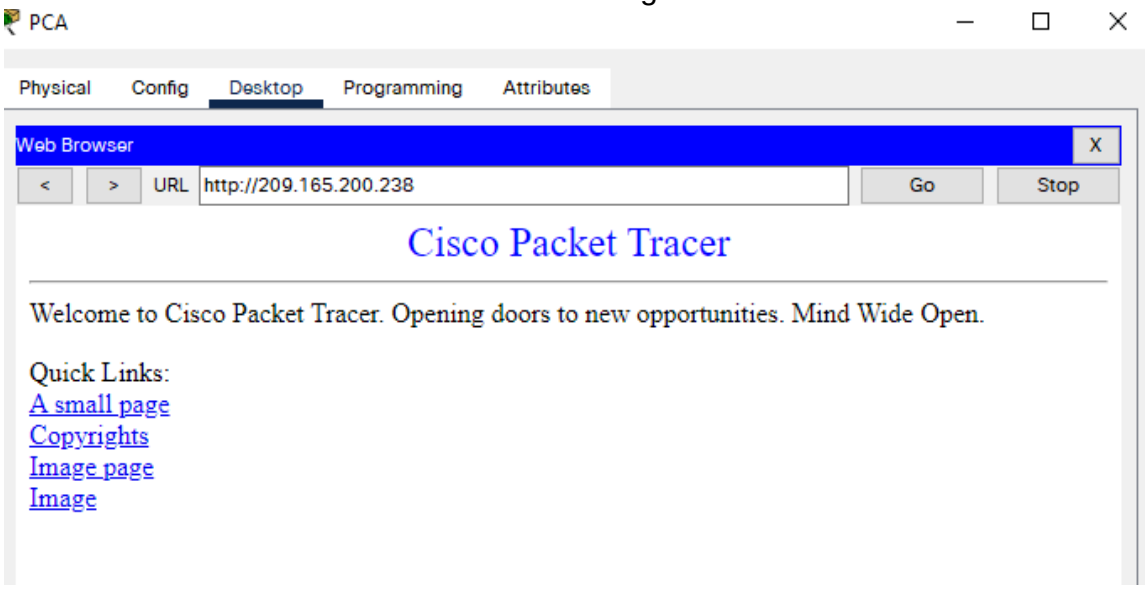

Fuente propia.

Figura 26. Ping de PC-A a PC-C




Fuente propia.

Figura 27. Acceso al servidor web desde el navegador del PCA.




Fuente propia.

## 2.8. PARTE 6: Configuración de NTP.

Se procede a realizar la configuración de NTP en los dispositivos. Ver tabla 25.

Tabla 25. Verificar el protocolo DHCP y la NAT estática

| Elemento o tarea de configuración | Especificación |
|---|---|
| Ajuste la fecha y hora en R2. | 5 de marzo de 2016, 9 a. m. |
| Configure R2 como un maestro NTP. | Nivel de estrato: 5 |
| Configurar R1 como un cliente NTP. | Servidor: R2 |
| Configure R1 para actualizaciones de calendario periódicas con horaNTP. | |
| Verifique la configuración de NTP en R1. | |

Fuente propia.

Anexo código de verificación:

Configuración en R2.
R2#clock set 09:00:00 05 march 2016 Se realiza ajuste de la hora en el R2
R2#conf t Se ingresa a la configuración del terminal

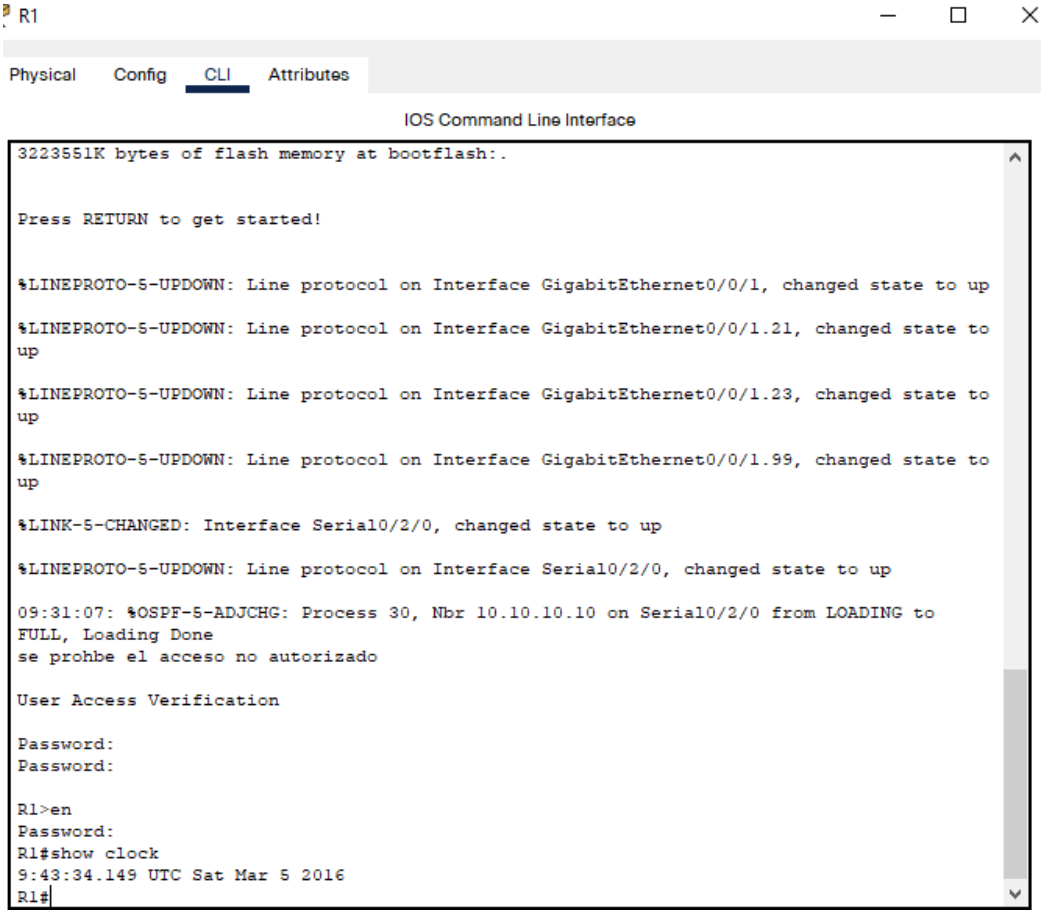
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ntp master 5  Se configura R2 como un maestro NTP nivel 5
R2(config)#

Configuración en R1.
R1(config)#ntp server 172.16.1.2  Se configura R1 como cliente NTP de Servidor R2
R1(config)#ntp update-calendar  Se configuran actualizaciones periódicas con hora NTP
R1(config)#exit  Nos salimos de la configuración
R1#

Se verifica la configuración de NTP en R1.

R1#show clock
9:43:34.149 UTC Sat Mar 5 2016
R1#

Figura 28. Comando show clock en R1.




Fuente propia.

## 2.9. PARTE 7: Configurar y verificar las listas de control de acceso (ACL)

### 2.9.1. Paso 1: Restringir el acceso a las líneas VTY en el R2. Ver tabla 26.

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

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

Fuente propia.

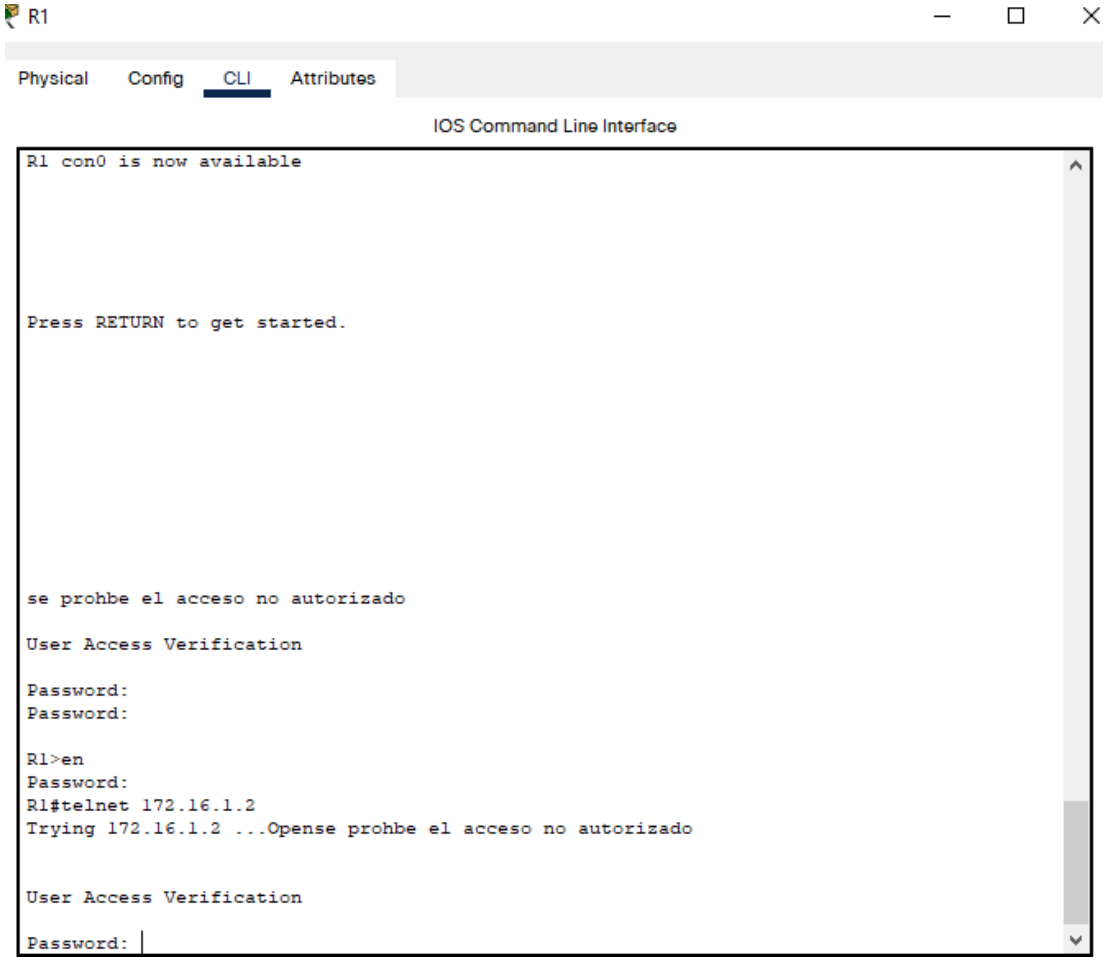
Anexo código de verificación:

```
R2(config)#ip access-list standard ADMIN-MGT Se da nombre a la ACL como ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1 Se permite acceso al host
R2(config-std-nacl)#deny any Se niega acceso a otros
R2(config-std-nacl)#exit Se sale de la configuración ACL
R2(config)#line vty 0 4 Se ingresa a la línea VTY 0 4 del R2
R2(config-line)#ip access-class ADMIN-MGT in Se aplica la ACL con nombre a las líneas VTY
R2(config-line)#transport input telnet Se permite el acceso por telnet
R2(config-line)#
```

Se realiza verificación:

```
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...Open
Se prohbe el acceso no autorizado.
User Access Verification Password:
```

Figura 29. Verificación de ingreso a R2 a través de R1.




Fuente propia.

2.9.2. Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente. Ver tabla 27.

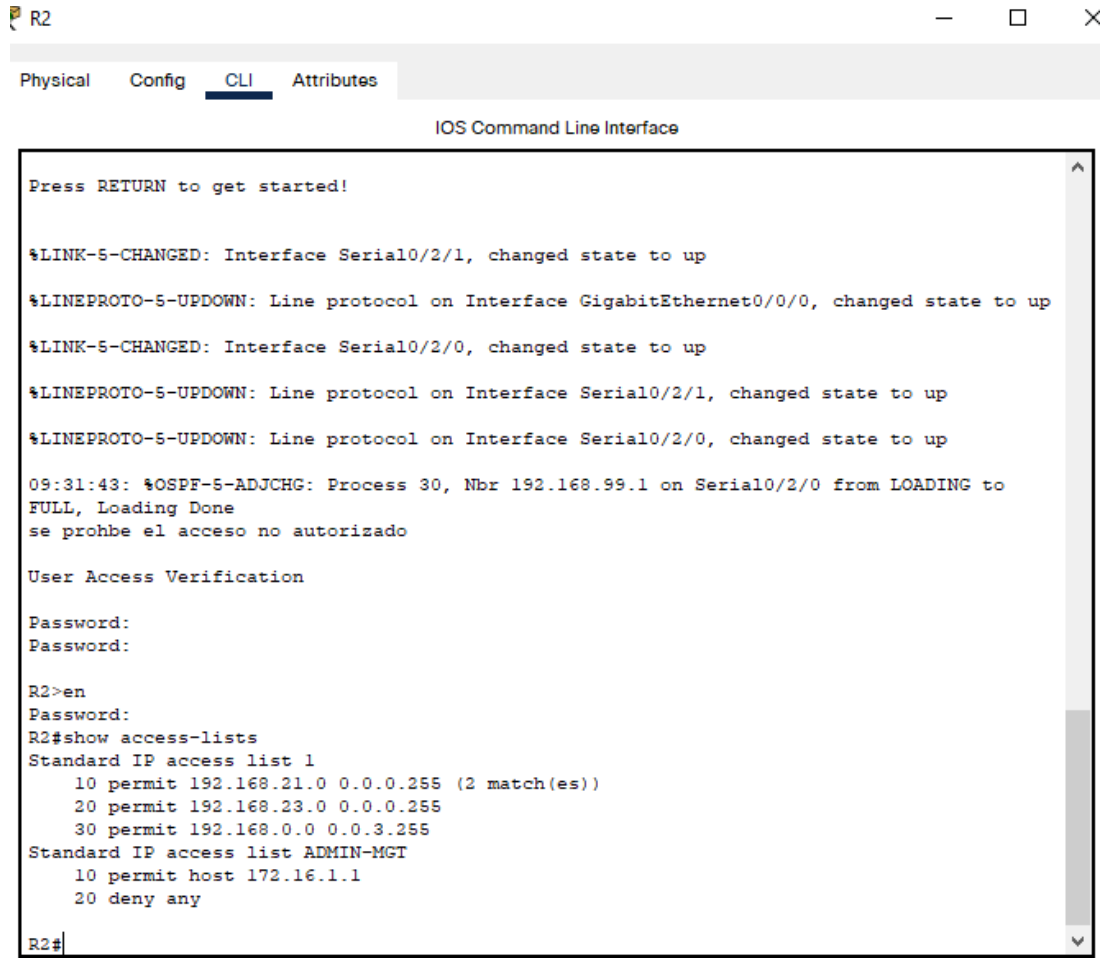
Tabla 27. Resumen de configuración.

| Elemento o tarea de configuración | Especificación |
|---|---|
| Mostrar las coincidencias recibidas poruna lista de acceso desde la última vez que se restableció | sh access-lists |
| Restablecer los contadores de una listade acceso | clear access-list counters |

| | |
|---|---|
| ¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la direcciónen que se aplica? | show run |
| ¿Con qué comando se muestran las traducciones NAT? | show ip nat translations |
| ¿Qué comando se utiliza para eliminarlas traducciones de NAT dinámicas? | clear ip nat translation * |

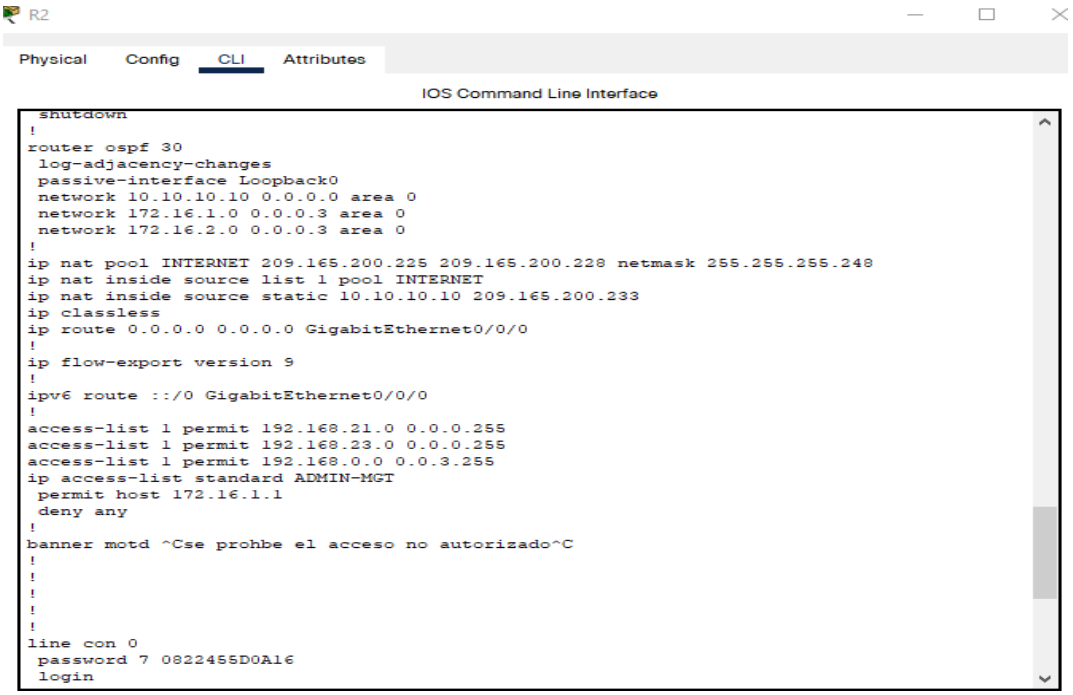
Fuente propia

Figura 30. Show access-lists.



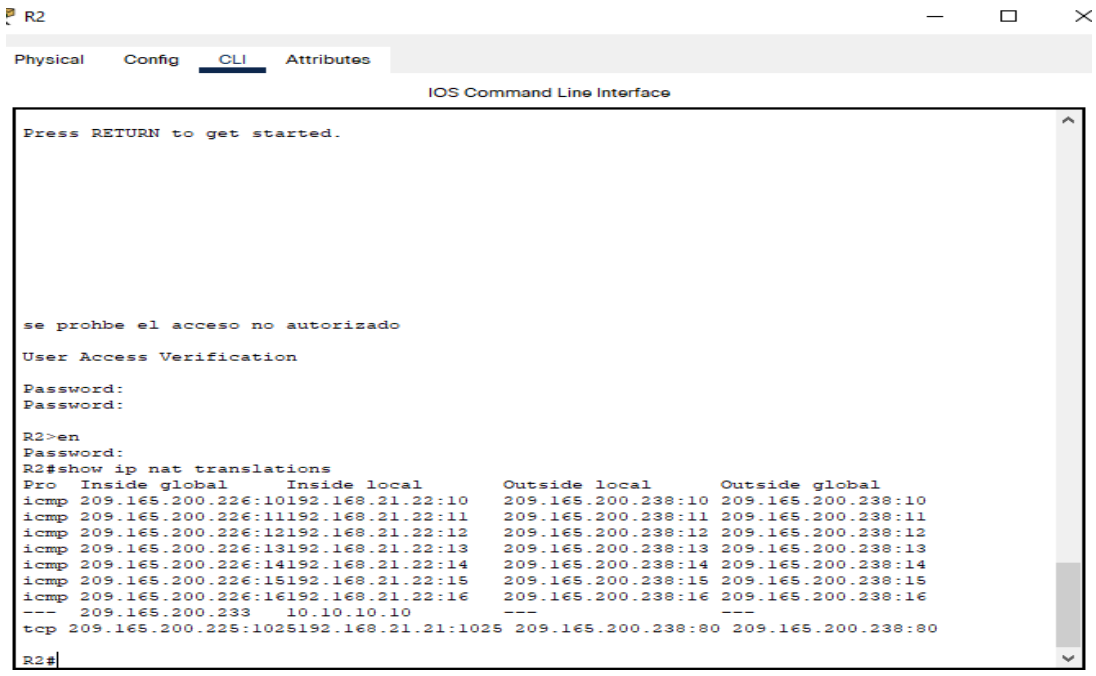

Fuente propia.

Figura 31. Show run para ver access list.




Fuente propia.

Figura 32. Show ip nat translations.




Fuente propia.

## CONCLUSIONES

En la anterior practica de laboratorio pude realizar la configuración básica de dispositivos de red y el correcto direccionamiento de direcciones IPv4 e IPv6 en pequeñas redes LAN, con el que logré corregir ciertos errores de conexión entre las topologías; para ello fue necesario verificar el estado de cada equipo y realizar un diagnóstico previo que me permitiera analizar y configurar de manera adecuada los parámetros solicitados, en el desarrollo de la practica surgieron ciertos inconvenientes, como el modo de enrutar conexiones telnet y configuraciones de puertos troncales, pero pude solucionarlos a través de la investigación de fuentes bibliográficas.

Me llamo mucho la atención y fue la utilización de las VLAN en una red, puesto que estas facilitan crear redes lógicas independientes dentro de la misma red física y ayudan a segmentar el tráfico entre ellas.

También pude reconocer la importancia que tienen la aplicación del protocolo de Routing dinámico OSPF y el manejo que se le dan para la configuración de las interfaces conectadas dentro de un área y establecer estas como pasivas.

De igual manera, aprendí a emplear el protocolo DHCP y NAT para el direccionamiento IPv4 en una red, crear una POOL para las VLAN, dar direccionamiento DNS a un servidor y posteriormente consultar las listas de acceso.

## BIBLIOGRAFIA


[1] 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.

[2] GUTIERREZ, R. B., Urrea, S. C., Núñez, W. N., Sarmiento, H., Acosta, N. D., & Sánchez, G. G.
V. (2015). Análisis de la seguridad en la implementación de servicios corporativos sobre el protocoloIPV. *Revista de Tecnología*, *14*(1), 127-138.

[3] BAREÑO, Gutiérrez, R., Sevillano, A. M. L., Díaz-Piraquive, F. N., & González-Crespo, R. (2021, July). Analysis of WEB Browsers of HSTS Security Under the MITM Management Environment. In *International Conference on Knowledge Management in Organizations* (pp. 331-344). Springer, Cham.

[4] BAREÑO, Gutiérrez, R., Cardenas-Urrea, S. E., Navarro-Nuñez, W., Sarmiento-Osorio, H., & Forero-Paez, N. (2017). Sistema de votación electrónico con características de seguridad SSL/TLS e IPsec en Colombia. *Revista UIS Ingenierías*, *16*(1), 75-84.

[5] BAREÑO Gutiérrez, R. (2013). Elaboración de un estado de arte sobre el protocolo IPV6; y su implementación sobre protocolos de enrutamiento dinámico como RIPNG, EIGRP y OSPF basado sobre la plataforma de equipos cisco.

[6] BAREÑO Raúl, G., & Sevillano, A. M. L. (2017, October). Services cloud under HSTS, Strengths and weakness before an attack of man in the middle MITM. In *2017 Congreso Internacional de Innovacion y Tendencias en Ingenieria (CONIITI)* (pp. 1-5). IEEE.

[7] MOJICA S. Felipe, Andrés, L. V. S., & Raúl, B. G. (2019, October). Risks Found in Electronic Payment Cards on Integrated Public Transport System Applying the ISO 27005 Standard. Case Study Sitp DC Colombia. In *2019 Congreso Internacional de Innovación y Tendencias en Ingenieria(CONIITI)* (pp. 1-6). IEEE.

[8] Boronat Segui, F., & Montagut Climent, M. A. (2013). Direccionamiento e interconexión de redes basada en TCP/IP. Editorial Universitat Politècnica de València.

[9] Rodríguez Gómez, J. D., Ladino Abril, E. Y., Mesa Méndez, C. M., Bejarano Alarcón, J. C., & Quimbayo Calderon, L. F. (2018). Modelo OSI y direccionamiento IP.

[10] Rosero, H. A., & Angulo Palacios, M. K. Soluciones integradas lan–wan) ccna 1 y ccna 2 exploration: fundamentos de networking y principios de enrutamiento.

[11] Dordoigne, J. (2015). Redes informáticas-Nociones fundamentales (5ª

edición):(Protocolos, Arquitecturas, Redes inalámbricas, Virtualización, Seguridad, IP v6...). Ediciones Eni.

[12] Pérez, S. C., Facchini, H. A., & Mercado, G. (2007). Análisis y Determinación de Patrones de Tráfico de Protocolos en redes LAN. In IX Workshop de Investigadores en Ciencias de la Computación.

[13] Paredes, K. R., Ochoa, L. L., & Tejada, J. E. (2017). La Extensión Universitaria como Estrategia para la Aplicación de los Fundamentos de Networking en un Centro de Gestión de Red Empresarial. In Global Partnerships for Development and Engineering Education: Proceedings of the 15th LACCEI International Multi-Conference for Engineering, Education and Technology, July 19-21, 2017, Boca Raton, FL, United States (p. 156). Latin American and Caribbean Consortium of Engineering Institutions.

[14] Stallings, W., Stallings, W., Tanenbaum, A., Fall, K. R., & Stevens, W. R. (2000). Comunicaciones y Redes de Computadores, 6aedición. Prentice-Hall.