

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA  
CISCO

SANDRA MILENA BUSTOS BACCA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERIA DE SISTEMAS  
PASTO  
2022

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA  
CISCO

SANDRA MILENA BUSTOS BACCA

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

DIRECTORA:  
PAULITA FLOR SALAZAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERIA DE SISTEMAS  
PASTO  
2022

NOTA DE ACEPTACION

---

---

---

---

---

---

---

---

Firma del Presidente del Jurado

---

Firma del Jurado

---

Firma del Jurado

San Juan de Pasto, 27 de noviembre de 2022

## **AGRADECIMIENTOS**

En el transcurso de la carrera se presentan varios momentos, es por ello, que mi principal agradecimiento es para Dios, porque logre continuar y realizar cada etapa que me llevo a finalizar la carrera, colocó en mi camino a las personas correctas que me ayudaron a continuar y lograr este paso tan importante en mi vida.

También agradezco a mi familiar, que me apoyo para seguir adelante, con el fin de mirarme realizar uno de mis logros propuestos y obtener el título de la carrera por la cual luché y me esforcé cada día.

A mis amigos, tutores y compañeros por su interés, dedicación y enseñanza, que estuvieron conmigo durante todo este proceso de conocimiento y crecimiento personal y profesional.

El fruto del esfuerzo son los buenos resultados que se obtiene de la disciplina, la responsabilidad y la dedicación.

## CONTENIDO

|  |    |
|--|----|
| AGRADECIMIENTOS.....   | 4  |
| CONTENIDO .....  | 5  |
| LISTA DE TABLAS .....  | 7  |
| LISTA DE FIGURAS .....   | 8  |
| GLOSARIO .....   | 9  |
| RESUMEN.....   | 10 |
| ABSTRACT.....  | 10 |
| INTRODUCCIÓN.....  | 11 |
| ESCENARIO 1.....   | 12 |
| Topología.....   | 12 |
| Parte 1: Construya la red.....   | 12 |
| Parte 2: Desarrolle el esquema de direccionamiento IP .....                        | 12 |
| Parte 3: Configure aspectos básicos .....  | 14 |
| Paso 1: Configurar los ajustes básicos.....  | 14 |
| Paso 2. Configurar los equipos.....  | 21 |
| Parte 4: Probar y verificar la conectividad de extremo a extremo.....              | 24 |
| ESCENARIO 2.....   | 30 |
| Topología.....   | 30 |
| Parte 1: Inicializar, recargar y configurar aspectos básicos de los dispositivos.. | 33 |
| Paso 1: Inicializar y volver a cargar el router y el switch.....                   | 33 |
| Borrado de configuración y VLAN en los switches .....                              | 33 |

|   |    |
|---|----|
| Paso 2: Configurar R1 .....   | 34 |
| Paso 3: Configure S1 y S2. ....   | 38 |
| Configuración en Switch 1 .....   | 38 |
| Configuración en Switch 2 .....   | 41 |
| Parte 2: Configuración de la infraestructura de red (VLAN, Trunking,<br>EtherChannel) ..... | 44 |
| Paso 4: Configurar S1 .....   | 44 |
| Paso 5: Configure el S2.....  | 46 |
| Parte 3: Configurar soporte de host.....  | 49 |
| Paso 1: Configure R1 .....  | 49 |
| Paso 2: Configurar los servidores.....  | 50 |
| Parte 4: Probar y verificar la conectividad de extremo a extremo.....                       | 51 |
| Capturas de pantalla de verificación de conectividad .....                                  | 55 |
| CONCLUSIONES .....  | 69 |
| BIBLIOGRAFÍA.....   | 71 |
| ANEXOS .....  | 73 |

## LISTA DE TABLAS

|          |   |    |
|----------|---|----|
| Tabla 1  | Tabla de direccionamiento .....                   | 13 |
| Tabla 2  | Configuración de Router 1 .....                   | 15 |
| Tabla 3  | Configuración de Switch 1 .....                   | 18 |
| Tabla 4  | Configuración de red PC-A .....                   | 21 |
| Tabla 5  | Configuración de red PC-B .....                   | 23 |
| Tabla 6  | Resultados Ping PC-A y PC-B .....                 | 25 |
| Tabla 7  | Tabla de asignación de VLAN.....                  | 31 |
| Tabla 8  | Tabla de direccionamiento IPV4 e IPV6.....        | 32 |
| Tabla 9  | Configuración Router 1 .....                      | 34 |
| Tabla 10 | configuración en Switch 1 .....                   | 38 |
| Tabla 11 | Configuración en Switch 2 .....                   | 41 |
| Tabla 12 | Configuración de infraestructura en Switch 1..... | 44 |
| Tabla 13 | Configuración de infraestructura en Switch 2..... | 47 |
| Tabla 14 | Configuración de servicio DHCP en Router 1 .....  | 49 |
| Tabla 15 | Configuración de red en PC-A .....                | 51 |
| Tabla 16 | Configuración de red en PC-B .....                | 51 |
| Tabla 17 | Verificación de conectividad.....                 | 51 |
| Tabla 18 | Captura de pantalla con comando Ping .....        | 56 |

## LISTA DE FIGURAS

|  |    |
|--|----|
| Figura 1 Topología escenario 1 .....               | 12 |
| Figura 2 Simulación escenario 1 .....              | 12 |
| Figura 3 Comando ipconfig/ all en PC-A.....        | 22 |
| Figura 4 Comando ipconfig /all en PC-B.....        | 23 |
| Figura 5 Ping de PC-A hacia interfaz G0/0/0 .....  | 25 |
| Figura 6 Ping de PC-A hacia interfaz G0/0/1 .....  | 25 |
| Figura 7 Ping de PC-A hacia interfaz VLAN 1 .....  | 26 |
| Figura 8 Ping de PC-A hacia PC-B .....             | 27 |
| Figura 9 Ping de PC-B hacia interfaz G0/0/0 .....  | 27 |
| Figura 10 Ping de PC-B hacia interfaz G0/0/1 ..... | 28 |
| Figura 11 Ping de PC-B hacia interfaz VLAN 1.....  | 29 |
| Figura 12 Topología escenario 2 .....              | 30 |
| Figura 13 Simulación escenario 2.....              | 31 |
| Figura 14 Ping desde PC-A a G0/0/1.2.....          | 56 |
| Figura 15 Ping desde PC-A a G0/0/1.3.....          | 57 |
| Figura 16 Ping desde PC-A a G0/0/1.4.....          | 58 |
| Figura 17 Ping desde PC-A a SVI – S1 .....         | 59 |
| Figura 18 Ping desde PC-A a SVI – S2 .....         | 60 |
| Figura 19 Ping desde PC-A a PC-B.....              | 61 |
| Figura 20 Ping desde PC-A a Bucle0 .....           | 62 |
| Figura 21 Ping desde PC-B a Bucle0 .....           | 63 |
| Figura 22 Ping desde PC-B a G0/0/1.2.....          | 64 |
| Figura 23 Ping desde PC-B a G0/0/1.3.....          | 65 |
| Figura 24 Ping desde PC-B a G0/0/1.4.....          | 66 |
| Figura 25 Ping desde PC-B a SVI – S1 .....         | 67 |
| Figura 26 Ping desde PC-B a SVI – S2 .....         | 68 |



## GLOSARIO

**CIFRADO:** mecanismo empleado para asegurar información, mediante el uso de algoritmos matemáticos que transforman los datos originales. Como resultado se obtienen datos indescifrables para usuarios no autorizados. Es utilizado para la protección de claves de acceso.<sup>1</sup>

**CLI:** interfaz de línea de comandos. Interfaz de usuario empleada para configurar, monitorear y mantener a los equipos. Provee una ejecución directa y simple de los comandos utilizados para realizar diferentes funciones.<sup>2</sup>

**DIRECCIONAMIENTO IP:** conjunto de números que identifica de manera lógica a un dispositivo de una red. Los dispositivos se conectan entre sí mediante sus respectivas direcciones IP que pueden ser representadas en sistema decimal o en sistema binario. Existen dos tipos de direcciones IP, IPV4 e IPV6.<sup>3</sup>

**ENRUTAMIENTO:** proceso que facilita a dispositivos de interconexión disponer de la mejor ruta para enviar y recibir mensajes. Esta ruta se la puede obtener mediante el dispositivo de red router.<sup>4</sup>

**VLAN:** red de área local virtual es un grupo de dispositivos que se encuentran en diferente ubicación de una red de área local pero que se comunican como si estuvieran en el mismo segmento físico.<sup>5</sup>

---

<sup>1</sup> SORIANO, Miguel. Seguridad en redes y seguridad de la información. (2014)

<sup>2</sup> FERNÁNDEZ TERÁN, Pablo David. Desarrollo de un programa que permita generar archivos de configuración para routers CISCO mediante la simulación de la Interfaz de Línea de Comandos (CLI). (2005)

<sup>3</sup> GONZÁLEZ LAFORGA, Belén. Servicio interactivo de asignación de direcciones IP. (2021)

<sup>4</sup> LOPEZ BULLA, Ricardo. Enrutamiento y configuración de redes. (2018)

<sup>5</sup> CAPELLA HERNÁNDEZ, Juan Vicente. Características y configuraciones básicas de VLANs. (2012)

## **RESUMEN**

El presente trabajo consiste en el desarrollo de dos escenarios que forman parte de las pruebas de habilidades de los temas mirados en el transcurso del diplomado. Los temas a tratar son direccionamiento IPV4 e IPV6 en redes LAN, configuración de aspectos básicos en los dispositivos de red, configuración de ajustes básicos de seguridad en routers, enrutamiento entre VLAN, DHCP, Etherchannel entre otros temas importantes que integran a los escenarios. Con lo aprendido en la plataforma de Cisco, se coloca en práctica los conocimientos en cada uno de los temas de los escenarios, empleando el simulador Packet Tracer se lograr un mejor entendimiento del funcionamiento, configuración y diseño de una red Cisco.

Palabras claves: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

## **ABSTRACT**

The present work consists of the development of two scenarios that are part of the skills tests of the topics studied in the course of the diploma course. The topics to be discussed are IPV4 and IPV6 addressing in LAN networks, configuration of basic aspects in network devices, configuration of basic security settings in routers, routing between VLANs, DHCP, Etherchannel, among other important topics that make up the scenarios. With what is learned in the Cisco platform, the knowledge in each of the scenario topics is put into practice, using the Packet Tracer simulator to achieve a better understanding of the operation, configuration and design of a Cisco network.

Keywords: CISCO, CCNP, Switching, Routing, Networks, Electronics.

## INTRODUCCIÓN

El diplomado en profundización Cisco, desarrolla habilidades en el empleo de diversos comandos, los cuales permiten crear y configurar funciones necesarias para el correcto funcionamiento de una red. Es importante mencionar que el conocimiento adquirido acerca de la configuración de los diferentes dispositivos de red Cisco, otorga beneficios en el desarrollo del perfil profesional, puesto que temas como la seguridad o protección en el ingreso de dispositivo, direccionamiento IPV4 e IPV6, enrutamiento y creación de VLAN, servicio DHCP, Etherchannel entre otros temas relevantes, aportan información requerida en el ámbito laboral.

Por consiguiente, para el desarrollo de las topologías propuestas en los dos escenarios, se utilizan dispositivos de red como routers y switches de capa 2 y capa 3 de Cisco, los cuales se ingresan de manera segura y con privilegios para llevar a cabo las configuraciones presentadas, es más, se utilizó el programa de simulación Packet Tracer, que permite realizar el diseño de la red, comprobación de conectividad y la aplicación general de los conocimientos adquiridos en el diplomado.

Finalmente, este trabajo muestra en detalle los procesos llevados a cabo para configurar los dispositivos que conforman una red, como son los router, switch y host, al tiempo que se emplean comandos para la creación de enlaces y verificación de configuración y conectividad, a fin de validar el funcionamiento óptimo de la red Cisco.

## ESCENARIO 1

### Topología

Figura 1 Topología escenario 1

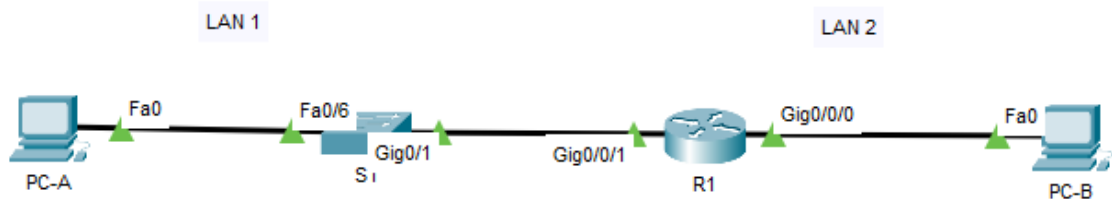


Fuente: Prueba de habilidades CCNA II

### Parte 1: Construya la red

Se realiza la topología propuesta en el escenario 1, para ello se emplea el programa de simulación Packet Tracer en su última versión, como se observa en la Figura 2.

Figura 2 Simulación escenario 1



Fuente: Autor

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

Se desarrolla el esquema de direccionamiento IPV4, se crean las dos subredes, LAN1 conformada con 60 hosts y LAN2 con 20 hosts. Se tiene en cuenta que en el direccionamiento 172.XY.3.0 el valor de XY es reemplazado por los dos últimos dígitos de la cédula. Como se observa en la tabla 1.

Tabla 1 Tabla de direccionamiento

| Item                              | Requerimiento   |
|-----------------------------------|---|
| Dirección de Red                  | <b>172.53.3.0</b>   |
| Requerimiento de host Subred LAN1 | <b>60</b>   |
| Requerimiento de host Subred LAN2 | <b>20</b>   |
| R1 G0/0/1                         | <p>Para la asignación de la dirección IPV4 a la interfaz G0/0/0 del router 1, se ingresa las siguientes líneas de comandos, se tiene en cuenta que es la última dirección de host de la subred LAN1, 172.53.3.62</p> <p><b>R1(config)#interface g0/0/1</b></p> <p><b>R1(config-if)#ip address 172.53.3.62</b></p> <p><b>255.255.255.192</b></p> <p><b>R1(config-if)#no shutdown</b></p>   |
| R1 G0/0/0                         | <p>Para la asignación de la dirección IPV4 a la interfaz G0/0/0 del router 1, se ingresa las siguientes líneas de comandos, se tiene en cuenta que es la última dirección de host de la subred LAN2, 172.53.3.158</p> <p><b>R1(config)#interface g0/0/0</b></p> <p><b>R1(config-if)#ip address 172.53.3.158</b></p> <p><b>255.255.255.224</b></p> <p><b>R1(config-if)#no shutdown</b></p> |

|        |   |
|--------|---|
| S1 SVI | Para la asignación de la dirección IPV4 a VLAN1 del switch1, se ingresa las siguientes líneas de comandos, se tiene en cuenta la segunda dirección de host de la subred LAN1, 172.53.3.2<br><b>S1(config)#interface vlan 1</b><br><b>S1(config-if)#ip address 172.53.3.2</b><br><b>255.255.255.192</b><br><b>S1(config-if)#ip default-gateway 172.53.3.62</b><br><b>S1(config-if)#no shutdown</b> |
| PC-A   | Para la asignación de la dirección IPV4 al PC-A, se ingresa las siguientes líneas de comandos, y se tiene en cuenta que es la décima dirección de host de la subred LAN1, 172.53.3.10   |
| PC-B   | Para la asignación de la dirección IPV4 al PC-A, se ingresa las siguientes líneas de comandos y se tiene en cuenta que es la décima dirección de host de la subred LAN2, 172.53.3.138   |

Fuente: Autor

### Parte 3: Configure aspectos básicos

La configuración de dispositivos de red como switch y router, se realiza mediante conexión de consola, empleando los comandos necesarios para el ingreso a configuración global y para los ajustes requeridos.

#### Paso 1: Configurar los ajustes básicos

Para realizar las tareas de configuración del R1, es necesario ingresar a configuración global desde consola y aplicar los comandos de ajuste básico como se muestra en la tabla 2.

Tabla 2 Configuración de Router 1

| Tarea  | Especificación   |
|--|--|
| Desactivar la búsqueda DNS                       | <p>Para desactivar la búsqueda de DNS, se ingresa la siguiente línea de comandos en el router1</p> <p><b>R1&gt;enable</b></p> <p><b>R1#configure terminal</b></p> <p><b>R1(config)#no ip domain-lookup</b></p>   |
| Nombre del router                                | <p>Para cambiar el nombre del dispositivo de red se ingresa la siguiente línea de comando en el router 1</p> <p><b>Route(config)#hostname R1</b></p>   |
| Nombre de dominio                                | <p>Para ingresar el nombre de dominio en el router 1, se ingresa la siguiente línea de comando, especificando el dominio ccna-sa.com</p> <p><b>R1(config)#ip domain-name ccna-sa.com</b></p>   |
| Contraseña cifrada para el modoEXEC privilegiado | <p>Para cifrar la contraseña para el ingreso a modo EXEC privilegiado en el router 1, se ingresa el siguiente comando especificando la contraseña ciscoenpass</p> <p><b>R1(config)#enable secret ciscoenpass</b></p>   |
| Contraseña de acceso a la consola                | <p>Para configurar la contraseña de acceso a la consola del router 1, se inserta las siguientes líneas de comandos, especificando el usuario: admin y la contraseña: ciscoconpass</p> <p><b>R1(config)#line console 0</b></p> <p><b>R1(config-line)#password ciscoconpass</b></p> <p><b>R1(config-line)#login</b></p> <p><b>R1(config-line)#exit</b></p> |

|  |   |
|--|---|
| <p>Establecer la longitud mínima para contraseñas</p>                                    | <p>Para establecer la longitud mínima de 10 en las contraseñas ingresadas, se inserta las siguientes líneas de comandos en el router 1</p> <p><b>R1(config)#security password min-length 10</b><br/> <b>R1(config)#end</b></p>  |
| <p>Crear un usuario administrativo en labase de datos local</p>                          | <p>Para la creación de un usuario administrativo en la base de datos local, se ingresa las siguientes líneas de comandos en el router 1, especificando nombre de usuario: admin y la contraseña: admin1pass</p> <p><b>R1(config)#username admin password admin1pass</b><br/> <b>R1(config)#line console 0</b><br/> <b>R1(config-line)#login local</b></p> |
| <p>Configure el inicio de sesión en laslíneas VTY para que use la base dedatos local</p> | <p>Para la configuración de inicio de sesión en las líneas VTY para el uso de la base de datos local, se ingresa los siguientes comandos en el router</p> <p><b>R1#configure terminal</b><br/> <b>R1(config)#line vty 0 4</b><br/> <b>R1(config-line)#login local</b></p>   |
| <p>Configurar las líneas VTY para que acepten únicamente las conexionesSSH</p>           | <p>Para la configuración de las líneas VTY en el router 1 que acepten únicamente las conexiones SSH, se ingresa los siguientes comandos</p> <p><b>R1(config)#line vty 0 4</b><br/> <b>R1(config-line)#transport input ssh</b><br/> <b>R1(config-line)#login local</b></p>   |



|  |  |
|--|--|
| Cifrar las contraseñas de texto no cifrado | <p>Para el cifrado de las contraseñas de texto no cifrado, se ingresa los siguientes comandos en el router 1</p> <p><b>R1(config)#service password-encryption</b></p>  |
| Configurar un banner MOTD                  | <p>El banner MOTD permite la creación de comentarios o mensajes para los usuarios que ingresen en la configuración del dispositivo, para ello se ingresa el siguiente comando</p> <p><b>R1(config)#banner motd #R1, Sandra Milena Bustos Bacca, Ingeniería de sistemas#</b></p>  |
| Configuración de interface G0/0/0          | <p>Para la configuración de la interfaz G0/0/0 del router 1, se ingresa los siguientes comandos, especificando la dirección IPV4, mascara de subred y su respectiva descripción.</p> <p><b>R1(config)#interface g0/0/0</b></p> <p><b>R1(config)#description Line0 R1</b></p> <p><b>R1(config)#ip address 172.53.3.158 255.255.255.224</b></p> <p><b>R1(config)#no shutdown</b></p> |
| Configuración de interface G0/0/1          | <p>Para la configuración de la interfaz G0/0/1 del router 1, se ingresa los siguientes comandos, especificando la dirección IPV4, mascara de subred y su respectiva descripción.</p> <p><b>R1(config)#interface g0/0/1</b></p> <p><b>R1(config)#description Line1 R1</b></p> <p><b>R1(config)#ip address 172.53.3.62 255.255.255.192</b></p> <p><b>R1(config)#no shutdown</b></p>  |

|                                  |  |
|----------------------------------|--|
| Generar una clave de cifrado RSA | <p>Para generar la clave de cifrado RSA, se ingresa la línea de comando en el router 1, especificando el módulo de 1024 bits</p> <p><b>R1(config)#crypto key generate rsa</b></p> <p><b>How many bits in the modulus [512]: 1024</b></p> |
|----------------------------------|--|

Fuente: Autor

Se realiza las tareas de configuración del switch 1 (S1), para lo cual se ingresa a la consola del dispositivo, en configuración global se insertan los comandos de ajuste básico, como se observa en la tabla 3.

Tabla 3 Configuración de Switch 1

| Tarea                      | Especificación  |
|----------------------------|---|
| Desactivar la búsqueda DNS | <p>Para desactivar la búsqueda DNS en el switch 1, se ingresa la siguiente línea de comando</p> <p><b>S1(config)#no ip domain-lookup</b></p>  |
| Nombre del switch          | <p>Para el cambio de nombre en el dispositivo switch 1 a S1, se ingresa la siguiente línea de comando</p> <p><b>Switch#configure terminal</b></p> <p><b>Switch(config)#hostname S1</b></p>    |
| Nombre de dominio          | <p>Para el ingreso de nombre del dominio en el switch1, se inserta la siguiente línea de comando especificando el dominio ccna-sa.com</p> <p><b>S1(config)#ip domain-name ccna-sa.com</b></p> |

|  |   |
|--|---|
| <p>Contraseña cifrada para el modoEXEC privilegiado</p>          | <p>Para cifrar la contraseña en el modo EXEC privilegiado en el switch 1, se ingresa la siguiente línea de comando, especificando la contraseña ciscoenpass</p> <p><b>S1(config)#enable secret ciscoenpass</b></p>  |
| <p>Contraseña de acceso a la consola</p>                         | <p>Para ingresar la contraseña de acceso a la consola del switch 1, se inserta las siguientes líneas de comandos, especificando la contraseña ciscoconpass</p> <p><b>S1(config)#line console 0</b><br/> <b>S1(config-line)#password ciscoconpass</b><br/> <b>S1(config-line)#login</b><br/> <b>S1(config-line)#end</b></p>  |
| <p>Apagar todos los puertos sin usar</p>                         | <p>Para realizar el proceso de apagar los puertos sin usar en el switch 1, se ingresa los siguientes comandos seguido de la interfaz y el rango</p> <p><b>S1(config)#interface range F0/1-4</b><br/> <b>S1(config-if-range)#shutdown</b><br/> <b>S1(config)#interface range F0/7-24</b><br/> <b>S1(config-if-range)#shutdown</b><br/> <b>S1(config)#interface range G0/2</b><br/> <b>S1(config-if-range)#shutdown</b></p> |
| <p>Crear un usuario administrativo en la base de datos local</p> | <p>Para la creación de un usuario administrativo en la base de datos local en el switch 1, se ingresa los siguientes comandos, especificando el usuario: admin y contraseña admin1pass</p> <p><b>S1(config)#username admin password</b></p>   |

|   |   |
|---|---|
|   | <b>admin1pass</b><br><b>S1(config)#line console 0</b><br><b>S1(config-line)#login local</b>   |
| Configure el inicio de sesión en las líneas VTY para que use la base de datos local | Para la configuración de inicio de sesión en las líneas VTY en la base de datos local, se realiza ingresando las siguientes líneas de comandos<br><b>S1(config)#line vty 0 15</b><br><b>S1(config-line)#login local</b>                                     |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH            | Para configurar las líneas VTY que acepten únicamente las conexiones SSH en el switch 1, se ingresa los siguientes comandos<br><b>S1(config)#line vty 0 15</b><br><b>S1(config-line)#transport input ssh</b><br><b>S1(config-line)#login local</b>          |
| Cifrar las contraseñas de texto no cifrado  | Para cifrar las contraseñas de texto sin cifrar en el switch 1, se ingresa el siguiente comando<br><b>S1(config)#service password-encryption</b>  |
| Configurar un banner MOTD   | Para la creación de un comentario o mensaje en el switch 1, se emplea el comando banner motd, se encierra el mensaje entre símbolos que no pertenezcan al mensaje<br><b>S1(config)#benner most #S1, Sandra Milena Bustos Bacca, Ingeniería de Sistemas#</b> |
| Generar una clave de cifrado RSA  | Para la generación de una clave de cifrado RSA en el dispositivo switch 1, se ingresa el  |

|  |  |
|--|--|
|  | <p>siguiente comando, especificando el módulo de 1024 bits</p> <p><b>S1(config)#crypto key generate rsa</b></p> <p><b>How many bits in the modulus [512]: 1024</b></p>   |
| Configure la interfaz de administración (SVI) en VLAN1 | <p>Para la configuración de la interfaz de administración en la VLAN1, se ingresa los siguientes comandos especificando la dirección IPV4, la máscara de subred y la descripción</p> <p><b>S1(config)#interface vlan1</b></p> <p><b>S1(config-if)#description SVI S1</b></p> <p><b>S1(config-if)#ip address 172.53.3.255.255.255.192</b></p> <p><b>S1(config-if)#default-gateway 172.53.3.62</b></p> <p><b>S1(config-if)#no shutdown</b></p> |

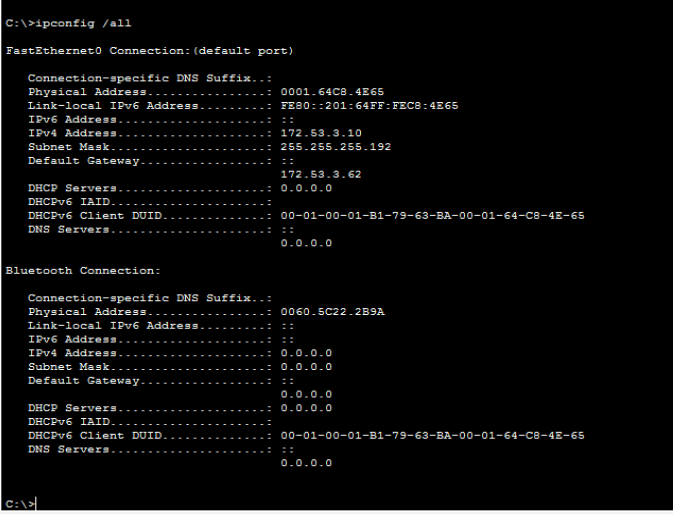
Fuente: Autor

## Paso 2. Configurar los equipos

Se lleva a cabo la configuración de los equipos host PC-A y PC-B conforme a la tabla de direccionamiento (Tabla 1), se realiza el registro de las configuraciones de red de cada host empleando el comando ipconfig /all. Se muestra el resultado obtenido del PC-A en la tabla 4.

Tabla 4 Configuración de red PC-A

| <b>Configuración de red de PC-A</b> |   |
|-------------------------------------|---|
| Descripción                         | Al emplear el comando ipconfig/all en el PC-A, se logra identificar la dirección IPV4 asignada, además de la máscara de subred, el Link-Local |

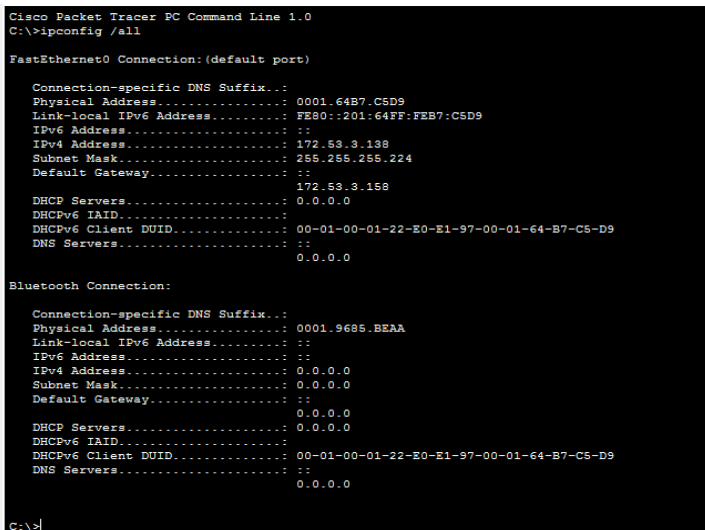
|   |   |
|---|---|
|   | <p>de IPV6, la dirección física y el Gateway. Mediante el uso de este comando se obtiene información específica de la configuración de la red del equipo.</p> <p>Figura 3 Comando ipconfig/ all en PC-A</p>  <pre> C:\&gt;ipconfig /all  FastEthernet0 Connection: (default port)      Connection-specific DNS Suffix. . . :      Physical Address. . . . . : 0001.64C8.4E65     Link-local IPv6 Address . . . . . : FE80::201:64FF:FEC8:4E65     IPv6 Address. . . . . :      IPv4 Address. . . . . : 172.53.3.10     Subnet Mask . . . . . : 255.255.255.192     Default Gateway . . . . . :      DHCP Servers. . . . . : 172.53.3.62     DHCPv6 IAID. . . . . : 0.0.0.0     DHCPv6 Client DUID. . . . . : 00-01-00-01-B1-79-63-BA-00-01-64-C8-4E-65     DNS Servers . . . . . :      . . . . . : 0.0.0.0  Bluetooth Connection:      Connection-specific DNS Suffix. . . :      Physical Address. . . . . : 0060.5C22.2B9A     Link-local IPv6 Address . . . . . :      IPv6 Address. . . . . :      IPv4 Address. . . . . : 0.0.0.0     Subnet Mask . . . . . : 0.0.0.0     Default Gateway . . . . . :      DHCP Servers. . . . . : 0.0.0.0     DHCPv6 IAID. . . . . : 0.0.0.0     DHCPv6 Client DUID. . . . . : 00-01-00-01-B1-79-63-BA-00-01-64-C8-4E-65     DNS Servers . . . . . :      . . . . . : 0.0.0.0  C:\&gt; </pre> |
|   | <p>Fuente: Autor</p>  |
| <p>Dirección física</p>                     | <p>La dirección física asignada para el PC-A y que se obtiene mediante el comando ipconfig/all es <b>0001.64C8.4E65</b></p>   |
| <p>Dirección IPv4</p>                       | <p>La dirección IPV4 asignada para la primera subred en el equipo PC-A es la siguiente <b>172.53.3.10</b></p>   |
| <p>Máscara de subred</p>                    | <p>La máscara de subred a la que pertenece el equipo PC-A es la siguiente <b>255.255.255.192</b></p>  |
| <p>Puerta de enlace IPv4 predeterminada</p> | <p>La puerta de enlace IPV4 predeterminada, permite al equipo PC-A la comunicación o conexión con otra red.</p>   |

|  |   |
|--|---|
|  | Se obtiene la siguiente<br><b>172.53.3.62</b> |
|--|---|

Fuente: Autor

También se realiza el registro de la configuración de red del host PC-B, empleando el comando ipconfig /all. Se muestra el resultado obtenido del PC-B en la tabla 5.

Tabla 5 Configuración de red PC-B

| <b>Configuración de red de PC-B</b> |   |
|-------------------------------------|---|
| Descripción                         | <p>Al emplear el comando ipconfig/all en el PC-B, se logra identificar la dirección IPV4 asignada, además de la máscara de subred, el Link-Local de IPV6, la dirección física y el Gateway. Mediante este comando se obtiene información específica de la configuración de la red del equipo.</p> <p style="text-align: center;">Figura 4 Comando ipconfig /all en PC-B</p>  <pre> Cisco Packet Tracer PC Command Line 1.0 C:\&gt;ipconfig /all  FastEthernet0 Connection:(default port)  Connection-specific DNS Suffix. . . :  Physical Address. . . . . : 0001.64B7.C5D9 Link-local IPv6 Address. . . . . : FE80::201:64FF:FEB7:C5D9 IPv6 Address. . . . . : :: IPv4 Address. . . . . : 172.53.3.138 Subnet Mask. . . . . : 255.255.255.224 Default Gateway. . . . . : ::                                 172.53.3.158 DHCP Servers. . . . . : 0.0.0.0 DHCPv6 IAID. . . . . :  DHCPv6 Client DUID. . . . . : 00-01-00-01-22-E0-E1-97-00-01-64-B7-C5-D9 DNS Servers. . . . . : ::                                 0.0.0.0  Bluetooth Connection:  Connection-specific DNS Suffix. . . :  Physical Address. . . . . : 0001.9685.BEAA 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 DHCPv6 IAID. . . . . :  DHCPv6 Client DUID. . . . . : 00-01-00-01-22-E0-E1-97-00-01-64-B7-C5-D9 DNS Servers. . . . . : ::                                 0.0.0.0  C:\&gt; </pre> |
|                                     | Fuente: Autor   |
| Dirección física                    | La dirección física asignada para PC-B es la  |

|                                      |   |
|--------------------------------------|---|
|                                      | siguiente<br><b>0001.64B7.C5D9</b>  |
| Dirección IPv4                       | La dirección IPV4 asignada en la red para el equipo PC-B que pertenece a la segunda subred es la siguiente<br><b>172.53.3.138</b>   |
| Máscara de subred                    | La máscara de subred a la que pertenece el equipo PC-B es la siguiente<br><b>255.255.255.224</b>  |
| Puerta de enlace IPv4 predeterminada | La puerta de enlace IPV4 predeterminada, permite al equipo PC-B la comunicación o conexión con otra red. La configurada y mostrada por el comando ipconfig/all es la siguiente<br><b>172.53.3.158</b> |

Fuente: Autor

#### **Parte 4: Probar y verificar la conectividad de extremo a extremo**

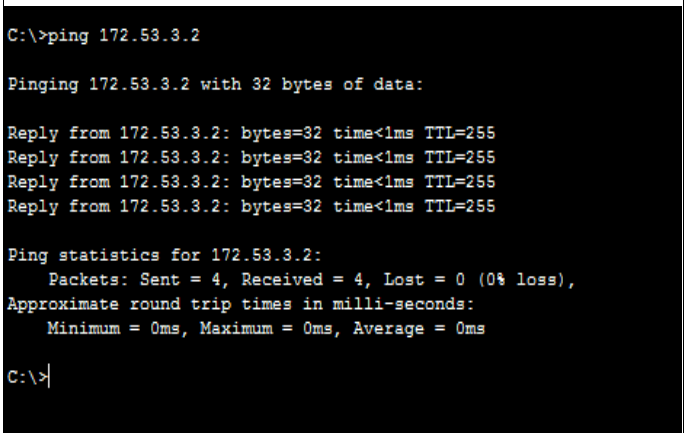
Para llevar a cabo la verificación se emplea el comando ping, que permite probar la conectividad entre todos los dispositivos de red configurados. Es importante tener en cuenta que, si los pings a los servidores fallan, es recomendable deshabilitar temporalmente el firewall del equipo y volver a realizar la verificación.

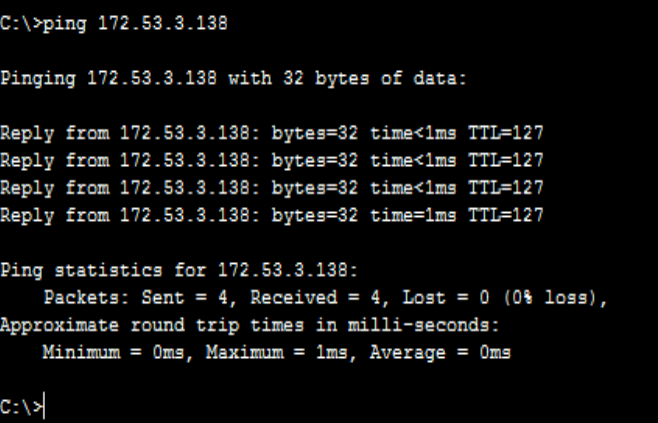
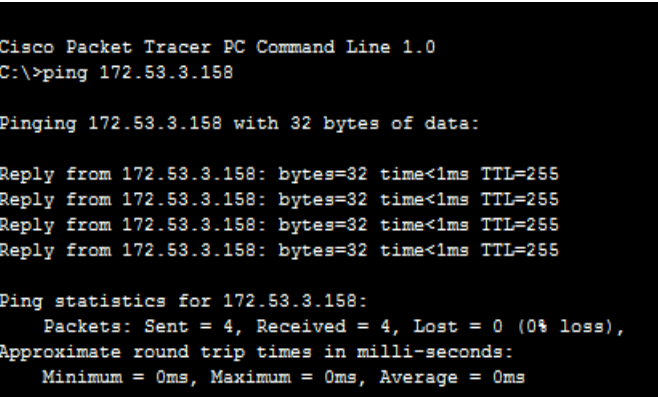
En la tabla 6 se muestra los resultados de verificación de conectividad obtenidos con cada dispositivo de red.

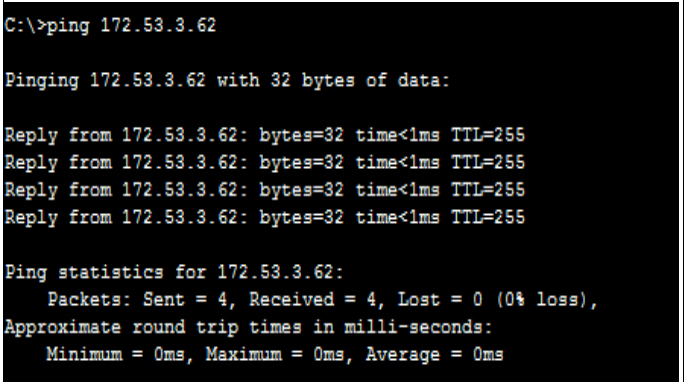


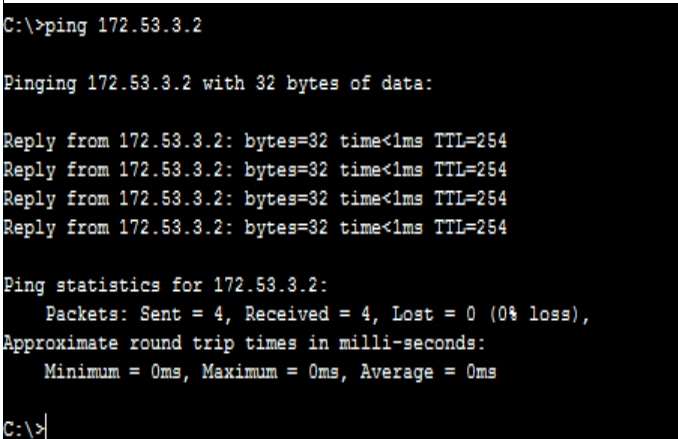
Tabla 6 Resultados Ping PC-A y PC-B

| Desde | A         | Dirección IP                | Resultados de ping   |
|-------|-----------|-----------------------------|--|
| PC-A  | R1 G0/0/0 | 172.53.3.10<br>172.53.3.158 | <p>Figura 5 Ping de PC-A hacia interfaz G0/0/0</p> <pre data-bbox="797 436 1455 800"> C:\&gt;ping 172.53.3.158  Pinging 172.53.3.158 with 32 bytes of data:  Reply from 172.53.3.158: bytes=32 time&lt;1ms TTL=255 Reply from 172.53.3.158: bytes=32 time&lt;1ms TTL=255 Reply from 172.53.3.158: bytes=32 time&lt;1ms TTL=255 Reply from 172.53.3.158: bytes=32 time&lt;1ms TTL=255  Ping statistics for 172.53.3.158:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 0ms, Average = 0ms                     </pre> <p>Fuente: Autor</p> <p>Al emplear el comando <b>ping</b> para probar la conectividad entre el PC-A y la interfaz G0/0/0 del router 1, muestra que se obtiene respuestas eco, el tiempo entre el momento en que se envío la solicitud y el momento en que se recibió la respuesta, la cantidad de paquetes enviados, los recibidos y si hubo paquetes perdidos. De acuerdo con el resultado obtenido se logra evidenciar que existe una conexión exitosa.</p> |
|       | R1 G0/0/1 | 172.53.3.10<br>172.53.3.62  | <p>Figura 6 Ping de PC-A hacia interfaz G0/0/1</p> <pre data-bbox="797 1413 1455 1797"> Cisco Packet Tracer PC Command Line 1.0 C:\&gt;ping 172.53.3.62  Pinging 172.53.3.62 with 32 bytes of data:  Reply from 172.53.3.62: bytes=32 time&lt;1ms TTL=255 Reply from 172.53.3.62: bytes=32 time&lt;1ms TTL=255 Reply from 172.53.3.62: bytes=32 time&lt;1ms TTL=255 Reply from 172.53.3.62: bytes=32 time=1ms TTL=255  Ping statistics for 172.53.3.62:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 1ms, Average = 0ms  C:\&gt;                      </pre> <p>Fuente: Autor</p>  |

|           |                                   |   |
|-----------|-----------------------------------|---|
|           |                                   | <p>Al emplear el comando <b>ping</b> para probar la conectividad entre el PC-A y la interfaz G0/0/1 del router 1, muestra que se obtiene respuestas eco, el tiempo entre el momento en que se envío la solicitud y el momento en que se recibió la respuesta, la cantidad de paquetes enviados, los recibidos y si hubo paquetes perdidos. De acuerdo con el resultado obtenido se logra evidenciar que existe una conexión exitosa.</p>  |
| S1 VLAN 1 | <p>172.53.3.10<br/>172.53.3.2</p> | <p>Figura 7 Ping de PC-A hacia interfaz VLAN 1</p>  <p>Fuente: Autor</p> <p>Al emplear el comando <b>ping</b> para probar la conectividad entre el PC-A y la interfaz VLAN 1 del switch 1 con la IPV4 172.53.3.2, muestra que se obtiene respuestas eco, el tiempo entre el momento en que se envío la solicitud y el momento en que se recibió la respuesta, la cantidad de paquetes enviados, los recibidos y si hubo paquetes perdidos. De acuerdo con el resultado obtenido se logra evidenciar que existe una conexión exitosa.</p> |

|      |   |  |
|------|---|--|
| PC-B | 172.53.3.10<br>172.53.3.138               | <p>Figura 8 Ping de PC-A hacia PC-B</p>  <pre>C:\&gt;ping 172.53.3.138  Pinging 172.53.3.138 with 32 bytes of data:  Reply from 172.53.3.138: bytes=32 time&lt;1ms TTL=127 Reply from 172.53.3.138: bytes=32 time&lt;1ms TTL=127 Reply from 172.53.3.138: bytes=32 time&lt;1ms TTL=127 Reply from 172.53.3.138: bytes=32 time=1ms TTL=127  Ping statistics for 172.53.3.138:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:     Minimum = 0ms, Maximum = 1ms, Average = 0ms  C:\&gt; </pre> <p>Fuente: Autor</p> <p>Al emplear el comando <b>ping</b> para probar la conectividad entre el PC-A y PC-B, muestra que se obtiene respuestas eco, así como el tiempo entre el momento en que se envió la solicitud y el momento en que se recibió la respuesta, la cantidad de paquetes enviados, los recibidos y si hubo paquetes perdidos. De acuerdo con el resultado obtenido se logra evidenciar que existe una conexión exitosa entre los equipos que pertenecen a diferentes redes.</p> |
| PC-B | R1 G0/0/0<br>172.53.3.138<br>172.53.3.158 | <p>Figura 9 Ping de PC-B hacia interfaz G0/0/0</p>  <pre>Cisco Packet Tracer PC Command Line 1.0 C:\&gt;ping 172.53.3.158  Pinging 172.53.3.158 with 32 bytes of data:  Reply from 172.53.3.158: bytes=32 time&lt;1ms TTL=255 Reply from 172.53.3.158: bytes=32 time&lt;1ms TTL=255 Reply from 172.53.3.158: bytes=32 time&lt;1ms TTL=255 Reply from 172.53.3.158: bytes=32 time&lt;1ms TTL=255  Ping statistics for 172.53.3.158:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:     Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> <p>Fuente: Autor</p>  |

|           |                             |   |
|-----------|-----------------------------|---|
|           |                             | <p>Al emplear el comando <b>ping</b> para probar la conectividad entre el PC-B y la interfaz G0/0/0 del router 1, muestra que se obtiene respuestas eco, así como el tiempo entre el momento en que se envió la solicitud y el momento en que se recibió la respuesta, la cantidad de paquetes enviados, los recibidos y si hubo paquetes perdidos. De acuerdo con el resultado obtenido se logra evidenciar que existe una conexión exitosa.</p>   |
| R1 G0/0/1 | 172.53.3.138<br>172.53.3.62 | <p>Figura 10 Ping de PC-B hacia interfaz G0/0/1</p>  <pre> C:\&gt;ping 172.53.3.62  Pinging 172.53.3.62 with 32 bytes of data:  Reply from 172.53.3.62: bytes=32 time&lt;1ms TTL=255 Reply from 172.53.3.62: bytes=32 time&lt;1ms TTL=255 Reply from 172.53.3.62: bytes=32 time&lt;1ms TTL=255 Reply from 172.53.3.62: bytes=32 time&lt;1ms TTL=255  Ping statistics for 172.53.3.62:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 0ms, Average = 0ms </pre> <p>Fuente: Autor</p> <p>Al emplear el comando <b>ping</b> para probar la conectividad entre el PC-B y la interfaz G0/0/1 del router 1, muestra que se obtiene respuestas eco, el tiempo entre el momento en que se envió la solicitud y el momento en que se recibió la respuesta, la cantidad de paquetes enviados, los recibidos y si hubo paquetes perdidos. De acuerdo con el resultado obtenido se logra</p> |

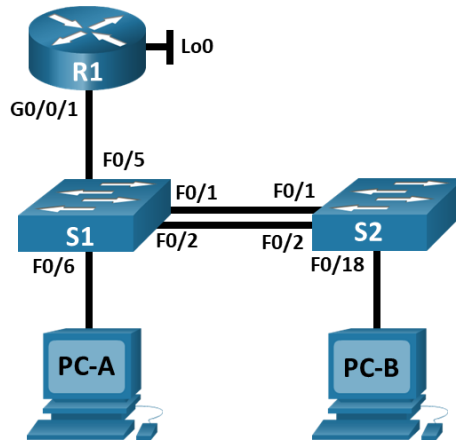
|  |  |   |
|--|--|---|
|  |  | evidenciar que existe una conexión exitosa.   |
|  | S1 VLAN1<br>172.53.3.138<br>172.53.3.2 | <p>Figura 11 Ping de PC-B hacia interfaz VLAN 1</p>  <pre> C:\&gt;ping 172.53.3.2  Pinging 172.53.3.2 with 32 bytes of data:  Reply from 172.53.3.2: bytes=32 time&lt;1ms TTL=254 Reply from 172.53.3.2: bytes=32 time&lt;1ms TTL=254 Reply from 172.53.3.2: bytes=32 time&lt;1ms TTL=254 Reply from 172.53.3.2: bytes=32 time&lt;1ms TTL=254  Ping statistics for 172.53.3.2:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 0ms, Average = 0ms  C:\&gt; </pre> <p>Fuente: Autor</p> <p>Al emplear el comando <b>ping</b> para probar la conectividad entre el PC-B y la interfaz VLAN 1 del switch 1 con la IPV4 172.53.3.2, muestra que se obtiene respuestas eco, así como el tiempo entre el momento en que se envió la solicitud y el momento en que se recibió la respuesta, la cantidad de paquetes enviados, los recibidos y si hubo paquetes perdidos. De acuerdo con el resultado obtenido se logra evidenciar que existe una conexión exitosa</p> |

Fuente: Autor

## ESCENARIO 2

### Topología

Figura 12 Topología escenario 2



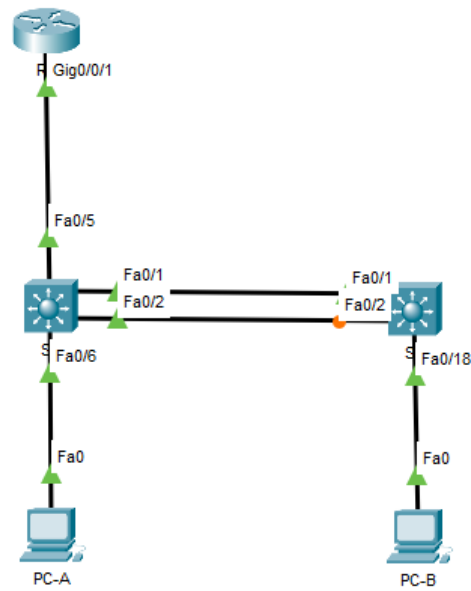
Fuente: Prueba de habilidades CCNA II

En este escenario se configura los dispositivos de una red pequeña, conformada por un router, dos switches (capa 3) y dos hosts. Se tiene en cuenta que los hosts admitan tanto la conectividad IPv4 entregada por servidor DHCP e IPv6 ingresada de manera manual. Para el caso del router y de los switches, se configuran para ser administrados de forma segura.

El enrutamiento se realiza entre las VLAN respectivas y el Etherchannel configurado entre los dispositivos de red. También se tiene en cuenta la habitación de seguridad del puerto mediante port-security.

Se presenta la topología propuesta en el escenario 2, para ello emplea el programa de simulación Packet Tracer en su última versión.

Figura 13 Simulación escenario 2



Fuente: Autor

Para el desarrollo del escenario 2 se tiene en cuenta la tabla 7, que corresponde a las VLAN a crear durante la ejecución de la actividad.

Tabla 7 Tabla de asignación de VLAN

| <b>VLAN</b> | <b>Nombre de la VLAN</b> |
|-------------|--------------------------|
| 20          | Docentes                 |
| 30          | Estudiantes              |
| 40          | Invitados                |
| 50          | Usuarios                 |
| 56          | Native                   |

Fuente: Prueba de habilidades CCNA II

Es importante mencionar el direccionamiento IPV4 e IPV6 que se emplea para las respectivas configuraciones de los dispositivos, de muestra en la Tabla 8.

Tabla 8 Tabla de direccionamiento IPV4 e IPV6

| <b>Dispositivo / interfaz</b> | <b>Dirección IP / Prefijo</b> | <b>Puerta de enlace predeterminada</b>         |
|-------------------------------|-------------------------------|--|
| R1 G0/0/1.20                  | 10.53.8.1 /26                 | No corresponde                                 |
|                               | 2001:db8:acad:a: :1 /64       | No corresponde                                 |
| R1 G0/0/1.30                  | 10.53.8.65 /27                | No corresponde                                 |
|                               | 2001:db8:acad:b: :1 /64       | No corresponde                                 |
| R1 G0/0/1.40                  | 10.53.8.97 /29                | No corresponde                                 |
|                               | 2001:db8:acad:c: :1 /64       | No corresponde                                 |
| R1 G0/0/1.56                  | No corresponde                | No corresponde                                 |
| R1 Loopback0                  | 209.165.201.1 /27             | No corresponde                                 |
|                               | 2001:db8:acad:209: :1 /64     | No corresponde                                 |
| S1 VLAN 40                    | 10.53.8.98 /29                | 10.53.8.97                                     |
|                               | 2001:db8:acad:c: :98 /64      | No corresponde                                 |
|                               | fe80: :98                     | No corresponde                                 |
| S2 VLAN 40                    | 10.53.8.99 /29                | 10.53.8.97                                     |
|                               | 2001:db8:acad:c: :99 /64      | No corresponde                                 |
|                               | fe80: :99                     | No corresponde                                 |
| PC-A NIC                      | Dirección DHCP para IPv4      | DHCP para puerta de enlace predeterminada IPv4 |
|                               | 2001:db8:acad:a: :50 /64      | fe80::1  |
| PC-B NIC                      | DHCP para dirección IPv4      | DHCP para puerta de enlace predeterminada IPv4 |
|                               | 2001:db8:acad:b: :50 /64      | fe80::1  |

Fuente: Prueba de habilidades CCNA II



## **Parte 1: Inicializar, recargar y configurar aspectos básicos de los dispositivos**

### **Paso 1: Inicializar y volver a cargar el router y el switch**

Se realiza la eliminación de las configuraciones de inicio del router y de cada uno de los switches, después de realizar este procedimiento se reinicia cada uno de los dispositivos de red con el comando **Reload**.

En el router se ingresa la siguiente línea de comandos para eliminar las configuraciones previas y para el reinicio del dispositivo.

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

### **Borrado de configuración y VLAN en los switches**

Para borrar las configuraciones previas en cada uno de los switches se ingresa las siguientes líneas de comandos. Es importante mencionar que con la eliminación del archivo vlan.dat, todas las VLAN creadas anteriormente ya no estarán presentes.

```
Switch#delete vlan.dat  
Switch#erase startup-config  
Switch#reload
```

Después de recargar los switches, se realiza la configuración de la plantilla SDM en cada uno de los switches (Switch1 y Switch 2) es necesario ingresar las siguientes líneas de comandos. Adicional se puede emplear la línea de comandos **show adm prefer** para observar si existen características de IPV6 habilitadas en la plantilla SDM antes de iniciar con la respectiva configuración.

```
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default  
Switch(config)#exit  
Switch#reload
```

## Paso 2: Configurar R1

Para llevar a cabo las tareas de configuración del Router 1 (R1), se tiene en cuenta los comandos empleados en el escenario 1. Se realiza las configuraciones de seguridad en el acceso y la creación y configuración de las subinterfaces de acuerdo con la Tabla 8 de direccionamiento. En la tabla 9 se muestran las líneas de comandos de cada tarea.

Tabla 9 Configuración Router 1

| Tarea  | Especificación  |
|--|---|
| Desactivar la búsqueda DNS                       | Para desactivar la búsqueda DNS en el router, se ingresa la siguiente línea de comando.<br><b>Router(config)#no ip domain-lookup</b>  |
| Nombre del router                                | Para cambiar el nombre del dispositivo de red a R1, se ingresa la siguiente línea de comando.<br><b>Router(config)#hostname R1</b>  |
| Nombre de dominio                                | Para ingresar el nombre de dominio <b>ccna-sa.com</b> en el router, se ingresa la siguiente línea de comando<br><b>R1(config)#ip domain-name ccna-sa.com</b>  |
| Contraseña cifrada para el modo EXECprivilegiado | Para cifrar la contraseña en modo EXEC privilegiado, se incorpora la siguiente línea de comando, especificando la contraseña class.<br><b>R1(config)#enable secret class</b>  |
| Contraseña de acceso a la consola                | Para la creación de la contraseña de acceso a consola, se ingresa las siguientes líneas de comandos, especificando la contraseña cisco<br><b>R1(config)#line console 0</b><br><b>R1(config-line)#password cisco</b> |

|  |  |
|--|--|
|  | <b>R1(config-line)#login</b>   |
| Establecer la longitud mínima para las contraseñas                                   | Para definir la longitud mínima en las contraseñas, es necesario ingresar la siguiente línea de comando, especificando la cantidad de caracteres requeridos.<br><b>R1(config)#security passwords min-length 5</b>  |
| Crear un usuario administrativo en la base de datos local                            | Para la creación de usuario y contraseña en la base de datos local, se ingresa las siguientes líneas de comandos, especificando el nombre de usuario <b>admin</b> y contraseña <b>admin1pass</b> .<br><b>R1(config)#username admin password admin1pass</b><br><b>R1(config)#line console 0</b><br><b>R1(config-line)#login local</b> |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | Para la configuración de inicio de sesión en las líneas VTY en la base de datos local, se ingresa las siguientes líneas de comandos.<br><b>R1(config)#line vty 0 4</b><br><b>R1(config-line)#login local</b>   |
| Configurar VTY solo aceptando SSH  | Para la configuración de las líneas VTY que solo acepten conexiones remotas SSH, se ingresan las siguientes líneas de comandos.<br><b>R1(config)#line vty 0 4</b><br><b>R1(config-line)#transport input ssh</b><br><b>R1(config-line)#login local</b>  |
| Cifrar las contraseñas de texto no cifrado   | Para el cifrado de las contraseñas de texto que se encuentran sin cifrar, se ingresa la línea de comando siguiente.<br><b>R1(config)#service password-encryption</b>   |

|  |  |
|--|--|
| Configure un MOTD Banner                   | <p>Para la creación del banner que contiene el nombre del router, el nombre del estudiante y el programa académico, se incorpora la siguiente línea de comando.</p> <p><b>R1(config)#banner motd#R1, Sandra Milena Bustos Bacca, Ingeniería de Sistemas#</b></p>   |
| Habilitar el routing IPv6                  | <p>Para habilitar el routing del Protocolo de Internet versión 6 en el router, se ingresa la siguiente línea de comando.</p> <p><b>R1(config)#ipv6 unicast-routing</b></p>   |
| Configurar interfaz G0/0/1 y subinterfaces | <p>Inicialmente se configura las respectivas interfaces, de acuerdo con la Tabla 8 de direccionamiento.</p> <p><b>R1(config)#int g0/0/1.20</b><br/> <b>R1(config-subif)#description vlan Docentes</b><br/> <b>R1(config-subif)#encapsulation dot1q 20</b><br/> <b>R1(config-subif)#ip add 10.53.8.1</b><br/> <b>255.255.255.192</b><br/> <b>R1(config-subif)#ipv6 add</b><br/> <b>2001:db8:acad:a::1/64</b><br/> <b>R1(config-subif)#ipv6 add fe80::1 link-local</b></p> <p><b>R1(config)#int g0/0/1.30</b><br/> <b>R1(config-subif)#description vlan</b><br/> <b>Estudiantes</b><br/> <b>R1(config-subif)#encapsulation dot1q 30</b><br/> <b>R1(config-subif)#ip add 10.53.8.65</b><br/> <b>255.255.255.224</b></p> |

|                                  |   |
|----------------------------------|---|
|                                  | <pre> R1(config-subif)#ipv6 add 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 add fe80::1 link-local  R1(config)#int g0/0/1.40 R1(config-subif)#description vlan Invitados R1(config-subif)#encapsulation dot1q 40 R1(config-subif)#ip add 10.53.8.97 255.255.255.248 R1(config-subif)#ipv6 add 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 add fe80::1 link-local  R1(config)#int g0/0/1.56 R1(config-subif)#description vlan native R1(config-subif)#encapsulation dot1q 56 R1(config-subif)#ipv6 add fe80::1 link-local  Configuración de la interfaz G0/0/1 R1(config)#int g0/0/1 R1(config-subif)#description enlace troncal a S1 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#no shut R1(config-subif)#exit </pre> |
| Configure el Loopback0 interface | <p>Para la configuración de la interfaz Loopback0 en el router, se ingresa las siguientes líneas de comando, teniendo en cuenta la Tabla 8 de direccionamiento.</p> <pre> R1(config)# int loopback0 R1(config-if)#description Loopback0 </pre>  |

|                                  |  |
|----------------------------------|--|
|                                  | <b>R1(config-if)#ip add 209.165.201.1<br/>255.255.255.224</b><br><b>R1(config-if)#ipv6 add<br/>2001:db8:acad:209::1/64</b><br><b>R1(config-if)#ipv6 add fe80::1 link-local</b><br><b>R1(config-if)#no shut</b> |
| Generar una clave de cifrado RSA | Para generar la clave de cifrado RSA, con módulo de 1024 bits, se ingresar la siguiente línea de comando.<br><br><b>R1(config)#crypto key generate rsa</b><br><b>How many bits in the modulus [512]: 1024</b>  |

Fuente: Autor

### **Paso 3: Configure S1 y S2.**

Para llevar a cabo las tareas de configuración de los switches que conforman la red, se requiere de los comandos empleados en el escenario 1. Se realiza la respectiva configuración de seguridad y de la interfaz de administración (SVI) con su respectiva Gateway.

#### **Configuración en Switch 1**

Se realiza las tareas requeridas para el Switch 1 (S1) que incluye configuración de seguridad en el acceso y configuración de interfaz de administración (SVI) con direccionamiento IPV4 e IPV6 asignada en la Tabla 8 de direccionamiento.

Tabla 10 configuración en Switch 1

| <b>Tarea</b>                | <b>Especificación</b>  |
|-----------------------------|--|
| Desactivar la búsqueda DNS. | Para desactivar la búsqueda DNS en el switch 1, se ingresa la siguiente línea de comando.<br><br><b>Switch(config)#no ip domain-lookup</b> |

|  |  |
|--|--|
| Nombre del switch  | Para cambiar el nombre del dispositivo de red a S1, se ingresa la línea de comando siguiente.<br><b>Switch(config)#hostname S1</b>   |
| Nombre de dominio  | Para ingresar el nombre de dominio <b>ccna-sa.com</b> en el switch, se ingresa la siguiente línea de comando.<br><b>S1(config)#ip domain-name ccna-sa.com</b>  |
| Contraseña cifrada para el modo EXEC privilegiado                                    | Para cifrar la contraseña en modo EXEC privilegiado, se incorpora la siguiente línea de comando, especificando la contraseña class.<br><b>S1(config)#enable secret class</b>   |
| Contraseña de acceso a la consola  | Para la creación de la contraseña de acceso a la consola, se ingresa las siguientes líneas de comandos, especificando la contraseña cisco.<br><b>S1(config)#line console 0</b><br><b>S1(config-line)#password cisco</b><br><b>S1(config-line)#login</b>  |
| Crear un usuario administrativo en la base de datos local                            | Para la creación de usuario y contraseña en la base de datos local, se ingresa las siguientes líneas de comandos, especificando el nombre de usuario <b>admin</b> y contraseña <b>admin1pass</b> .<br><b>S1(config)#username admin password admin1pass</b><br><b>S1(config)#line console 0</b><br><b>S1(config-line)#login local</b> |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | Para la configuración de inicio de sesión en las líneas VTY en la base de datos local, se ingresa las siguientes líneas de comandos.   |

|  |   |
|--|---|
|  | <b>S1(config)#line vty 0 4</b><br><b>S1(config-line)#login local</b>  |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH | Para la configuración de las líneas VTY que solo acepten conexiones remotas SSH, se ingresan las siguientes líneas de comandos.<br><b>S1(config)#line vty 0 4</b><br><b>S1(config-line)#transport input ssh</b><br><b>S1(config-line)#login local</b> |
| Cifrar las contraseñas de texto no cifrado                               | Para el cifrado de las contraseñas de texto no cifradas, se ingresa la línea de comando siguiente.<br><b>S1(config)#service password-encryption</b>   |
| Configurar un MOTD Banner  | Para la creación del banner que contiene el nombre del switch, el nombre del estudiante y el programa académico, se incorpora la siguiente línea de comando.<br><b>S1(config)#banner motd#S1, Sandra Milena Bustos Bacca, Ingeniería de Sistemas#</b> |
| Generar una clave de cifrado RSA   | Para generar la clave de cifrado RSA, con módulo de 1024 bits, es necesario ingresar la siguiente línea de comando.<br><b>S1(config)#crypto key generate rsa</b><br><b>How many bits in the modulus [512]: 1024</b>                                   |
| Configurar la interfaz de administración (SVI)                           | Para la configuración de la interfaz de administración (SVI) del switch 1. Se ingresa las siguientes líneas de comando, teniendo en cuenta la Tabla 8 de direccionamiento.<br><b>S1(config)#int vlan 40</b><br><b>S1(config-if)#ip add 10.53.8.98</b> |



|  |   |
|--|---|
|  | <b>255.255.255.248</b><br><b>S1(config-if)#ipv6 add</b><br><b>2001:db8:acad:c::98/64</b><br><b>S1(config-if)#ipv6 add fe80::98 link-local</b><br><b>S1(config-if)#description vlan 40, S1</b><br><b>S1(config-if)#no shut</b> |
| Configuración del Gateway predeterminado | Para la configuración del Gateway predeterminado en la VLAN 40, se ingresa las siguientes líneas de comandos.<br><br><b>S1(config)#int vlan 40</b><br><br><b>S1(config-if)#ip default-gateway 10.53.8.97</b>                  |

Fuente: Autor

## Configuración en Switch 2

Se realiza la configuración en el Switch 2 (S2) con los comandos empleados anteriormente. Se lleva a cabo la configuración de acceso seguro y la creación de la interfaz de administración (SVI) con el direccionamiento IPV4 e IPV6 asignado en la Tabla 8 de direccionamiento.

Tabla 11 Configuración en Switch 2

| Tarea                       | Especificación   |
|-----------------------------|--|
| Desactivar la búsqueda DNS. | Para desactivar la búsqueda DNS en el switch 2, se ingresa la siguiente línea de comando.<br><br><b>Switch(config)#no ip domain-lookup</b> |
| Nombre del switch           | Para cambiar el nombre del dispositivo de red a S2, se ingresa la línea de comando siguiente.<br><br><b>Switch(config)#hostname S2</b>     |
| Nombre de dominio           | Para ingresar el nombre de dominio <b>ccna-</b>  |

|   |  |
|---|--|
|   | <p><b>sa.com</b> en el switch, se ingresa la siguiente línea de comando.</p> <p><b>S2(config)#ip domain-name ccna-sa.com</b></p>   |
| <p>Contraseña cifrada para el modo EXEC privilegiado</p>                                    | <p>Para cifrar la contraseña en modo EXEC privilegiado, se incorpora la siguiente línea de comando, especificando la contraseña <b>class</b>.</p> <p><b>S2(config)#enable secret class</b></p>   |
| <p>Contraseña de acceso a la consola</p>  | <p>Para la creación de la contraseña de acceso a la consola, se ingresa las siguientes líneas de comandos, especificando la contraseña <b>cisco</b>.</p> <p><b>S2(config)#line console 0</b><br/> <b>S2(config-line)#password cisco</b><br/> <b>S2(config-line)#login</b></p>  |
| <p>Crear un usuario administrativo en la base de datos local</p>                            | <p>Para la creación de usuario y contraseña en la base de datos local, se ingresa las siguientes líneas de comandos, especificando el nombre de usuario <b>admin</b> y contraseña <b>admin1pass</b>.</p> <p><b>S2(config)#username admin password admin1pass</b><br/> <b>S2(config)#line console 0</b><br/> <b>S2(config-line)#login local</b></p> |
| <p>Configurar el inicio de sesión en las líneas VTY para que use la base de datos local</p> | <p>Para la configuración de inicio de sesión en las líneas VTY en la base de datos local, se ingresa las siguientes líneas de comandos.</p> <p><b>S2(config)#line vty 0 4</b><br/> <b>S2(config-line)#login local</b></p>  |
| <p>Configurar las líneas VTY para que acepten únicamente</p>                                | <p>Para la configuración de las líneas VTY que solo acepten conexiones remotas SSH, se ingresan</p>  |

|  |   |
|--|---|
| las conexiones SSH                             | <p>las siguientes líneas de comandos.</p> <p><b>S2(config)#line vty 0 4</b></p> <p><b>S2(config-line)#transport input ssh</b></p> <p><b>S2(config-line)#login local</b></p>   |
| Cifrar las contraseñas de texto no cifrado     | <p>Para el cifrado de las contraseñas de texto no cifradas, se ingresa la línea de comando siguiente.</p> <p><b>S2(config)#service password-encryption</b></p>  |
| Configurar un MOTD Banner                      | <p>Para la creación del banner que contiene el nombre del switch, el nombre del estudiante y el programa académico, se incorpora la siguiente línea de comando.</p> <p><b>S2(config)#banner motd#S1, Sandra Milena Bustos Bacca, Ingeniería de Sistemas#</b></p>  |
| Generar una clave de cifrado RSA               | <p>Para generar la clave de cifrado RSA, con módulo de 1024 bits, es necesario ingresar la siguiente línea de comando.</p> <p><b>S2(config)#crypto key generate rsa</b></p> <p><b>How many bits in the modulus [512]: 1024</b></p>  |
| Configurar la interfaz de administración (SVI) | <p>Para la configuración de la interfaz de administración (SVI) del switch 2. Se ingresa las siguientes líneas de comandos, teniendo en cuenta la Tabla 8 de direccionamiento.</p> <p><b>S2(config)#int vlan 40</b></p> <p><b>S2(config-if)#ip add 10.53.8.99</b></p> <p><b>255.255.255.248</b></p> <p><b>S2(config-if)#ipv6 add</b></p> <p><b>2001:db8:acad:c::99/64</b></p> |

|  |  |
|--|--|
|  | <b>S2(config-if)#ipv6 add fe80::99 link-local</b><br><b>S2(config-if)#description vlan 40, S2</b><br><b>S2(config-if)#no shut</b>  |
| Configuración del Gateway predeterminado | Para la configuración del Gateway predeterminado en la VLAN 40, se ingresa las siguientes líneas de comandos.<br><br><b>S2(config)#int vlan 40</b><br><br><b>S2(config-if)#ip default-gateway 10.53.8.97</b> |

Fuente: Autor

## Parte 2: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

### Paso 4: Configurar S1

Para realizar las configuraciones del Switch 1 (S1), se empleó los comandos necesarios para la creación de VLAN, para ello, se tiene en cuenta la Tabla 7 de asignación de VLAN. También se crea troncos 802.1Q y se emplea port-security para la protección de los respectivos puertos.

En la Tabla 12 se muestra las líneas de comandos requeridos para llevar a cabo las tareas.

Tabla 12 Configuración de infraestructura en Switch 1

| Tarea      | Especificación   |
|------------|--|
| Crear VLAN | Para la creación de las VLAN en el switch 1, se requiere ingresar las siguientes líneas de comandos, teniendo en cuenta la Tabla 7 de asignación de VLAN.<br><br><b>S1(config)#vlan 20</b><br><b>S1(config-vlan)#name Docentes</b><br><b>S1(config-vlan)#vlan 30</b> |

|  |  |
|--|--|
|  | <b>S1(config-vlan)#name Estudiantes</b><br><b>S1(config-vlan)#vlan 40</b><br><b>S1(config-vlan)#name Invitados</b><br><b>S1(config-vlan)#vlan 50</b><br><b>S1(config-vlan)#name Usuarios</b><br><b>S1(config-vlan)#vlan 56</b><br><b>S1(config-vlan)#name Native</b>   |
| <p>Crear troncos 802.1Q que utilicen la VLAN 56 nativa</p>                             | <p>Para la creación de troncos 802.1Q que utilicen la VLAN nativa 56 en las interfaces F0/1, F0/2 y F0/5, se ingresa las siguientes líneas de comandos.</p> <b>S1(config)#int range f0/1-2, f0/5</b><br><b>S1(config-if-range)#switchport trunk native vlan 56</b><br><b>S1(config-if-range)#switchport trunk encapsulation dot1q</b><br><b>S1(config-if-range)#switchport mode trunk</b><br><b>S1(config-if-range)#switchport nonegotiate</b><br><b>S1(config-if-range)#no shut</b> |
| <p>Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2</p> | <p>Para la creación del grupo de puertos Etherchannel de capa 2, usando las interfaces F0/1, F0/2 y el protocolo LACP para la negociación. Se emplean las siguientes líneas de comandos.</p> <b>S1(config)#int range f0/1-2</b><br><b>S1(config-if-range)#channel-group 2 mode active</b>  |
| <p>Configurar el puerto de acceso de host para VLAN 20</p>                             | <p>Para la configuración del puerto de acceso en la interfaz F0/6 que pertenece a la VLAN 20, se ingresa las siguientes líneas de comandos.</p> <b>S1(config)#int f0/6</b>   |

|   |  |
|---|--|
|   | <b>S1(config-if)#switchport mode access</b><br><b>S1(config-if)#swirchport access vlan 20</b><br><b>S1(config-if)#no shut</b>  |
| Configurar la seguridad del puerto en los puertos de acceso | Para configurar la seguridad en el puerto de acceso con 4 direcciones MAC, se ingresa las siguientes líneas de comandos.<br><b>S1(config)#int f0/6</b><br><b>S1(config-if)#switchport por-security</b><br><b>S1(config-if)#switchport port-security maximum 4</b>  |
| Proteja todas las interfaces no utilizadas                  | Para proteger todas las interfaces no utilizadas en el switch 1 y asignar a la VLAN 50, se ingresa las siguientes líneas de comandos.<br><b>S1(config)#int range f0/3-4, f0/7-24, g0/1-2</b><br><b>S1(config-if-range)#switchport mode access</b><br><b>S1(config-if-range)#switchport access vlan 50</b><br><b>S1(config-if-range)#switchport port-security</b><br><b>S1(config-if-range)#switchport port-security violation shutdown</b><br><b>S1(config-if-range)#description Interfaces no utilizadas</b><br><b>S1(config-if-range)#shut</b> |

Fuente: Autor

### **Paso 5: Configure el S2.**

En el Switch 2 (S2) se realiza las configuraciones iguales a las del Switch 1 (S1). Se crean las VLAN respectivas teniendo en cuenta la Tabla 7 de asignación de VLAN y se crea y configura los troncos 802.1Q que utiliza la VLAN nativa 56. También se protege los puertos empleando port-security y se asegura las interfaces no utilizadas en el Switch.

En la Tabla 13 se muestra las líneas de comandos empleadas para llevar a cabo las tareas.

Tabla 13 Configuración de infraestructura en Switch 2

| Tarea   | Especificación  |
|---|---|
| Crear VLAN  | <p>Para la creación de las VLAN en el switch 2, se requiere ingresar las siguientes líneas de comandos, teniendo en cuenta la Tabla 7 de asignación de VLAN.</p> <p><b>S2(config)#vlan 20</b><br/> <b>S2(config-vlan)#name Docentes</b><br/> <b>S2(config-vlan)#vlan 30</b><br/> <b>S2(config-vlan)#name Estudiantes</b><br/> <b>S2(config-vlan)#vlan 40</b><br/> <b>S2(config-vlan)#name Invitados</b><br/> <b>S2(config-vlan)#vlan 50</b><br/> <b>S2(config-vlan)#name Usuarios</b><br/> <b>S2(config-vlan)#vlan 56</b><br/> <b>S2(config-vlan)#name Native</b></p> |
| Crear troncos 802.1Q que utilicen la VLAN 56 nativa | <p>Para la creación de troncos 802.1Q que utilicen la VLAN nativa 56 en las interfaces F0/1 y F0/2, se ingresan las siguientes líneas de comandos.</p> <p><b>S2(config)#int range f0/1-2</b><br/> <b>S2(config-if-range)#switchport trunk native vlan 56</b><br/> <b>S2(config-if-range)#switchport trunk encapsulation dot1q</b><br/> <b>S2(config-if-range)#switchport mode trunk</b><br/> <b>S2(config-if-range)#switchport nonegotiate</b></p>  |

|   |  |
|---|--|
| <p>Crear un grupo de puertos EtherChannel deCapa 2 que use interfaces F0/1 y F0/2</p> | <p>Para la creación del grupo de puertos Etherchannel de capa 2, usando las interfaces F0/1, F0/2 y el protocolo LACP para la negociación. Se emplea las siguientes líneas de comandos.</p> <p><b>S2(config)#int range f0/1-2</b><br/> <b>S2(config-if-range)#channel-group 2</b><br/> <b>mode active</b></p>  |
| <p>Configurar el puerto de acceso del host para la VLAN 30</p>                        | <p>Para la configuración del puerto de acceso en la interfaz F0/18 que pertenece a la VALN 30, se ingresa las siguientes líneas de comandos.</p> <p><b>S2(config)#int f0/18</b><br/> <b>S2(config-if)#switchport mode access</b><br/> <b>S2(config-if)#swirchport access vlan 30</b></p>   |
| <p>Configure port-security en los access ports</p>                                    | <p>Para configurar la seguridad en el puerto de acceso, con 4 direcciones MAC, se ingresa las siguientes líneas de comandos.</p> <p><b>S2(config)#int f0/18</b><br/> <b>S2(config-if)#switchport por-security</b><br/> <b>S2(config-if)#switchport port-security maximum 4</b></p>   |
| <p>Asegure todas las interfaces no utilizadas.</p>                                    | <p>Para proteger todas las interfaces no utilizadas en el switch 2, y asignar a la VLAN 50, se ingresa las siguientes líneas de comandos.</p> <p><b>S2(config)#int range f0/3-17, f0/19-24, g0/1-2</b><br/> <b>S2(config-if-range)#switchport mode access</b><br/> <b>S2(config-if-range)#switchport access vlan 50</b><br/> <b>S2(config-if-range)#switchport port-security</b><br/> <b>S2(config-if-range)#switchport port-security violation shutdown</b><br/> <b>S2(config-if-range)#description Interfaces no</b></p> |



|  |  |
|--|--|
|  | <b>utilizadas</b><br><b>S2(config-if-range)#shut</b> |
|--|--|

Fuente: Autor

### Parte 3: Configurar soporte de host

#### Paso 1: Configure R1

La configuración en el Router 1 (R1) se realiza empleando los comandos necesarios para la creación de un grupo DHCP para IPV4 en las VLAN 20 y 30. Se tiene en cuenta el nombre de dominio y el rango de direcciones IPV4 excluidas para cada VLAN de acuerdo con las especificaciones de las tareas.

En la Tabla 14 se observa las líneas de comandos utilizadas para la configuración del Router 1.

Tabla 14 Configuración de servicio DHCP en Router 1

| <b>Tareas</b>                     | <b>Especificación</b>   |
|-----------------------------------|---|
| Configure Default Routing         | Para la creación de rutas predeterminadas para IPV4 e IPV6 que dirija el tráfico a la interfaz Loopback0, se ingresa las siguientes líneas de comando.<br><b>R1(config)#ip route 0.0.0.0 0.0.0.0 loopback0</b><br><b>R1(config)#ipv6 route ::/0 loopback0</b>   |
| Configurar IPv4 DHCP para VLAN 20 | Para la creación de un grupo DHCP compuesto por las 10 últimas direcciones de la subred y asignación de nombre de dominio unad-ccna-sa.net para la VLAN 20, se ingresa las siguientes líneas de comandos.<br><b>R1(config)#ip dhcp pool vlan20</b><br><b>R1(dhcp-config)#network 10.53.8.0</b><br><b>255.255.255.192</b><br><b>R1(dhcp-config)#default-router 10.53.8.1</b> |

|  |  |
|--|--|
|  | <pre> R1(dhcp-config)#domain-name unad-ccna- sa.net R1(dhcp-config)#exit R1(config)#ip dhcp excluded-address 10.53.8.1 10.53.8.52 </pre>   |
| <p>Configurar DHCP IPv4 para VLAN 30</p> | <p>Para la creación de un grupo DHCP compuesto por las 10 ultimas direcciones de la subred y asignación de nombre de dominio unad-ccna-sa.net para la VLAN 30, se ingresa las siguientes líneas de comandos.</p> <pre> R1(config)#ip dhcp pool vlan30 R1(dhcp-config)#network 10.53.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.53.8.65 R1(dhcp-config)#domain-name unad-ccna- sb.net R1(dhcp-config)#exit R1(config)#ip dhcp excluded-address 10.53.8.65 10.53.8.84 </pre> |

Fuente: Autor

## Paso 2: Configurar los servidores

La configuración en los hosts (PC-A y PC-B) se realiza al ingresar y configura la dirección IPV6 GUA y Link Local de manera estática. Para el direccionamiento IPV4 se habilita la opción DHCP para que se utilice el servicio DHCP anteriormente configurado.

Después, con el comando **ipconfig /all** se verifica las configuraciones de red realizadas en cada host. En la Tabla 15 se muestra las configuraciones del PC-A y en la Tabla 16 las configuraciones del PC-B.

Tabla 15 Configuración de red en PC-A

| <b>Configuración de red de PC-A</b> |                       |
|-------------------------------------|-----------------------|
| Descripción                         | Datos tomados en PC-A |
| Dirección física                    | 00D0.BA48.952C        |
| Dirección IP                        | 10.53.8.53            |
| Máscara de subred                   | 255.255.255.192       |
| Gateway predeterminado              | 10.53.8.1             |
| Gateway predeterminado IPv6         | FE80::1               |

Fuente: Autor

Tabla 16 Configuración de red en PC-B

| <b>Configuración de red de PC-B</b> |                       |
|-------------------------------------|-----------------------|
| Descripción                         | Datos tomados en PC-B |
| Dirección física                    | 00D0.D38C.0B43        |
| Dirección IP                        | 10.53.8.85            |
| Máscara de subred                   | 255.255.255.224       |
| Gateway predeterminado              | 10.53.8.65            |
| Gateway predeterminado IPv6         | FE80::1               |

Fuente: Autor

#### **Parte 4: Probar y verificar la conectividad de extremo a extremo**

Se realiza la comprobación de conectividad usando el comando ping para probar la conectividad en IPv4 e IPv6 entre todos los dispositivos que conforman la red.

En la Tabla 17 se muestra los resultados obtenidos de conectividad entre los hosts y las interfaces de los dispositivos de red.

Tabla 17 Verificación de conectividad

| Desde | A            |      | Dirección IP | Resultados de ping                      |
|-------|--------------|------|--------------|---|
| PC-A  | R1, G0/0/1.2 | IPv4 | 10.53.8.1    | Ping de PC-A a subinterfaz G0/0/1.2 con |

|  |              |      |                     |   |
|--|--------------|------|---------------------|---|
|  |              |      |                     | direccionamiento IPV4 se realizo con éxito.   |
|  |              | IPv6 | 2001:db8:acad:a::1  | Ping de PC-A a subinterfaz G0/0/1.2 con direccionamiento IPV6 se realizo con éxito.             |
|  | R1, G0/0/1.3 | IPv4 | 10.53.8.65          | Ping de PC-A a subinterfaz G0/0/1.3 con direccionamiento IPV4 se realizo con éxito.             |
|  |              | IPv6 | 2001:db8:acad:b::1  | Ping de PC-A a subinterfaz G0/0/1.3 con direccionamiento IPV6 se realizo con éxito.             |
|  | R1, G0/0/1.4 | IPv4 | 10.53.8.97          | Ping de PC-A a subinterfaz G0/0/1.4 con direccionamiento IPV4 se realizo con éxito.             |
|  |              | IPv6 | 2001:db8:acad:c::1  | Ping de PC-A a subinterfaz G0/0/1.4 con direccionamiento IPV6 se realizo con éxito.             |
|  | S1, VLAN 40  | IPv4 | 10.53.8.98          | Ping de PC-A a interfaz SVI con direccionamiento IPV4 se realizo con éxito.                     |
|  |              | IPv6 | 2001:db8:acad:c::98 | Ping de PC-A a interfaz SVI con direccionamiento IPV6 no se realizo con exitosa por motivos del |

|             |              |                      |  |
|-------------|--------------|----------------------|--|
|             |              |                      | IOS.   |
| S2, VLAN 40 | IPv4         | 10.53.8.99           | Ping de PC-A a interfaz SVI con direccionamiento IPV4 se realizo con éxito.                          |
|             | IPv6         | 2001:db8:acad:c::99  | Ping de PC-A a interfaz SVI con direccionamiento IPV6 no se realizo con exitosa por motivos del IOS. |
| PC-B        | IPv4         | 10.53.8.85           | Ping de PC-A a PC-B con direccionamiento IPV4 se realizo con éxito.                                  |
|             | IPv6         | 2001:db8:acad:a::50  | Ping de PC-A a PC-B con direccionamiento IPV6 se realizo con éxito.                                  |
| R1 Bucle 0  | IPv4         | 209.165.201.1        | Ping de PC-A a Bucle 0 con direccionamiento IPV4 se realizo con éxito.                               |
|             | IPv6         | 2001:db8:acad:209::1 | Ping de PC-A a Bucle 0 con direccionamiento IPV6 se realizo con éxito.                               |
| PC-B        | R1 Bucle 0   | IPv4                 | 209.165.201.1  |
|             |              | IPv6                 | 2001:db8:acad:209::1   |
|             | R1, G0/0/1.2 | IPv4                 | 10.53.8.1  |
|             |              |                      | Ping de PC-B a subinterfaz G0/0/1.2 con  |

|  |              |      |                     |   |
|--|--------------|------|---------------------|---|
|  |              |      |                     | direccionamiento IPV4 se realizo con éxito.   |
|  |              | IPv6 | 2001:db8:acad:a::1  | Ping de PC-B a subinterfaz G0/0/1.2 con direccionamiento IPV6 se realizo con éxito.             |
|  | R1, G0/0/1.3 | IPv4 | 10.53.8.65          | Ping de PC-B a subinterfaz G0/0/1.3 con direccionamiento IPV4 se realizo con éxito.             |
|  |              | IPv6 | 2001:db8:acad:b::1  | Ping de PC-B a subinterfaz G0/0/1.3 con direccionamiento IPV6 se realizo con éxito.             |
|  | R1, G0/0/1.4 | IPv4 | 10.53.8.97          | Ping de PC-B a subinterfaz G0/0/1.4 con direccionamiento IPV4 se realizo con éxito.             |
|  |              | IPv6 | 2001:db8:acad:c::1  | Ping de PC-B a subinterfaz G0/0/1.4 con direccionamiento IPV6 se realizo con éxito.             |
|  | S1, VLAN 40  | IPv4 | 10.53.8.98          | Ping de PC-B a interfaz SVI con direccionamiento IPV4 se realizo con éxito.                     |
|  |              | IPv6 | 2001:db8:acad:c::98 | Ping de PC-B a interfaz SVI con direccionamiento IPV6 no se realizo con exitosa por motivos del |

|  |             |      |                     |  |
|--|-------------|------|---------------------|--|
|  |             |      |                     | IOS.   |
|  | S2, VLAN 40 | IPv4 | 10.53.8.99          | Ping de PC-B a interfaz SVI con direccionamiento IPV4 se realizo con éxito.                          |
|  |             | IPv6 | 2001:db8:acad:c::99 | Ping de PC-B a interfaz SVI con direccionamiento IPV6 no se realizo con exitosa por motivos del IOS. |

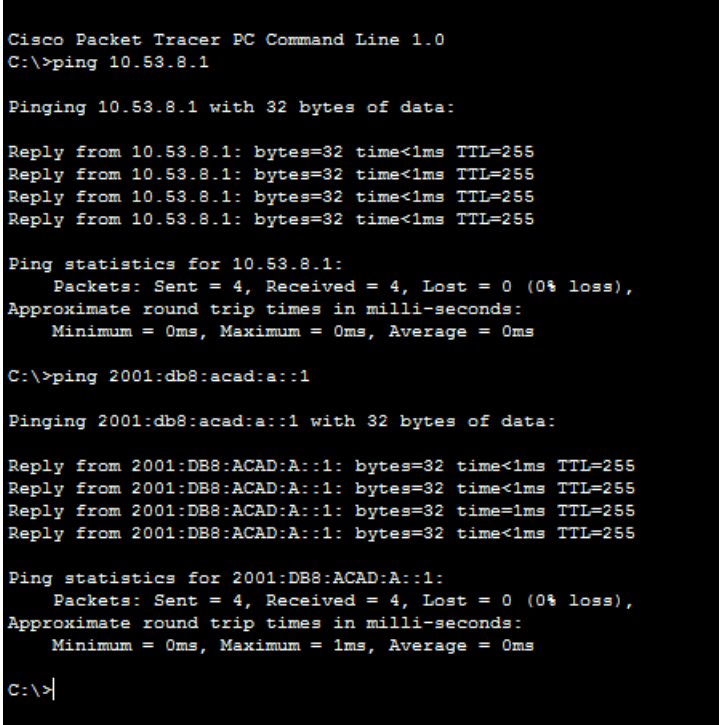
Fuente: Autor

### **Capturas de pantalla de verificación de conectividad**

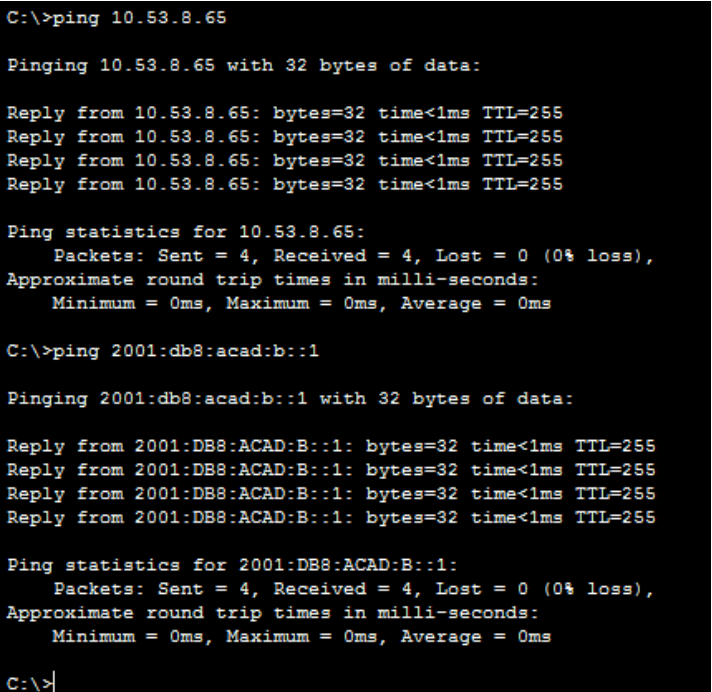
Para realizar la verificación de conectividad entre los diferentes dispositivos que conforman la red, se emplea el comando **ping** que se ejecuta en la interfaz de línea de comandos del PC-A y PC-B.

En la Tabla 18 se observa las respuestas obtenidas desde los hosts a las diferentes interfaces configuradas con direccionamiento IPV4 e IPV6.

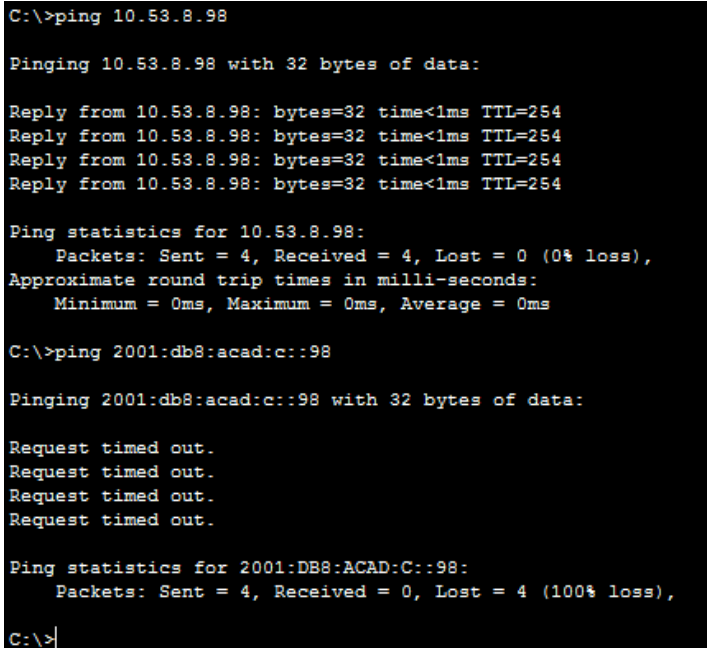
Tabla 18 Captura de pantalla con comando Ping

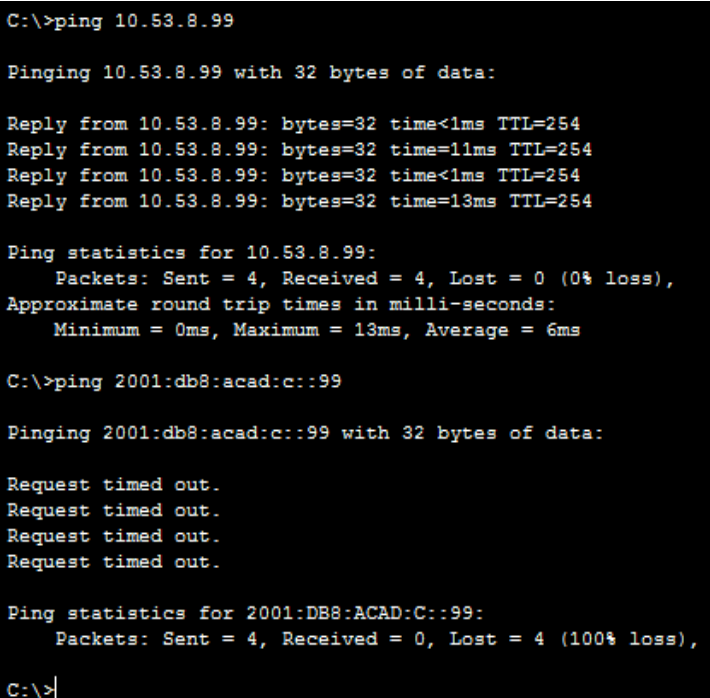
| Interfaces |               | Captura de pantalla   |
|------------|---------------|---|
| PC-A       | R1 - G0/0/1.2 | <p>Figura 14 Ping desde PC-A a G0/0/1.2</p>  <pre> Cisco Packet Tracer PC Command Line 1.0 C:\&gt;ping 10.53.8.1  Pinging 10.53.8.1 with 32 bytes of data:  Reply from 10.53.8.1: bytes=32 time&lt;1ms TTL=255 Reply from 10.53.8.1: bytes=32 time&lt;1ms TTL=255 Reply from 10.53.8.1: bytes=32 time&lt;1ms TTL=255 Reply from 10.53.8.1: bytes=32 time&lt;1ms TTL=255  Ping statistics for 10.53.8.1:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:     Minimum = 0ms, Maximum = 0ms, Average = 0ms  C:\&gt;ping 2001:db8:acad:a::1  Pinging 2001:db8:acad:a::1 with 32 bytes of data:  Reply from 2001:DB8:ACAD:A::1: bytes=32 time&lt;1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time&lt;1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time&lt;1ms TTL=255  Ping statistics for 2001:DB8:ACAD:A::1:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:     Minimum = 0ms, Maximum = 1ms, Average = 0ms  C:\&gt;  </pre> |
|            |               | <p>Fuente: Autor</p> <p>Se realiza la prueba de conectividad utilizando el comando Ping entre el host PC-A y la subinterfaz g0/0/1.2 del Router 1. En el resultado que se obtiene se observa los paquetes enviados (4), los recibidos (4) y los perdidos (0), lo cual indica que la conexión es exitosa tanto para el direccionamiento IPV4 como para IPV6. Permite la comunicación, transmisión y envió de paquetes entre el PC–A y la subinterfaz g0/0/1.2 del Router.</p>  |

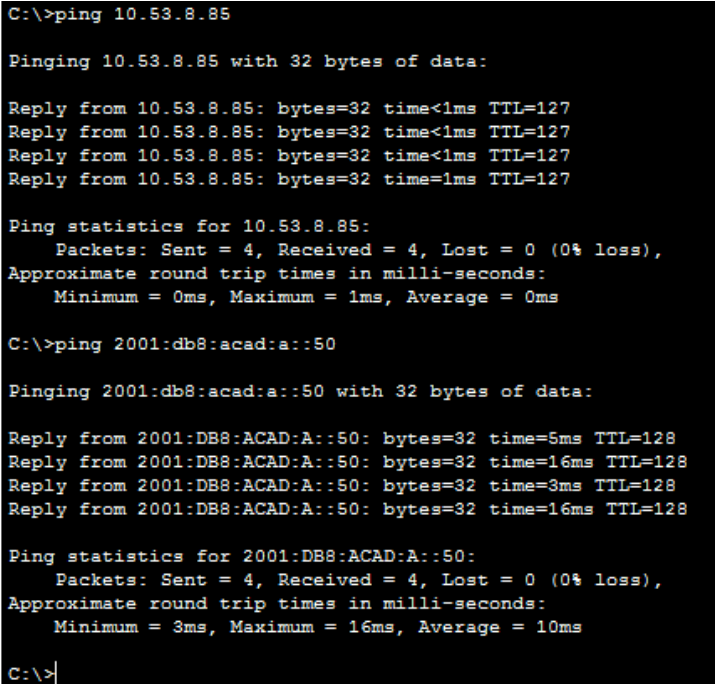


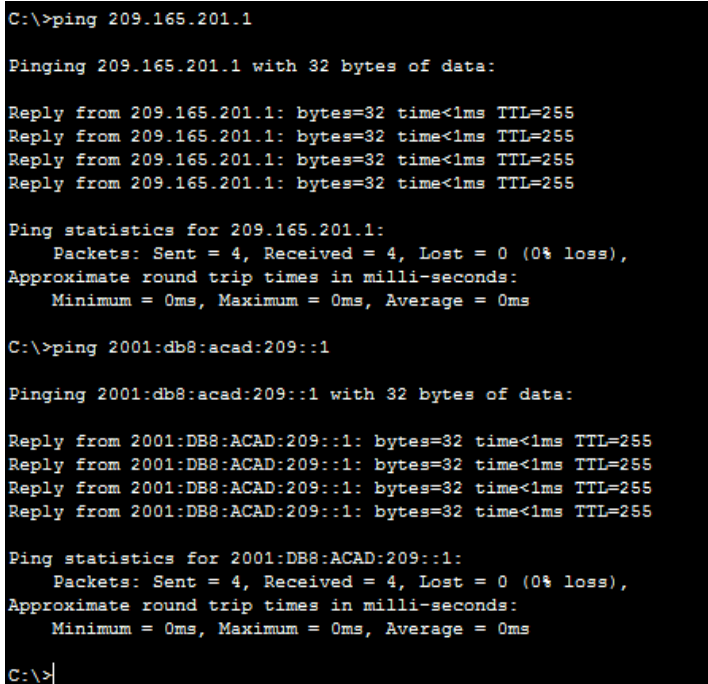
|  |               |  |
|--|---------------|--|
|  | R1 - G0/0/1.3 | <p>Figura 15 Ping desde PC-A a G0/0/1.3</p>  <pre> C:\&gt;ping 10.53.8.65  Pinging 10.53.8.65 with 32 bytes of data:  Reply from 10.53.8.65: bytes=32 time&lt;1ms TTL=255 Reply from 10.53.8.65: bytes=32 time&lt;1ms TTL=255 Reply from 10.53.8.65: bytes=32 time&lt;1ms TTL=255 Reply from 10.53.8.65: bytes=32 time&lt;1ms TTL=255  Ping statistics for 10.53.8.65:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 0ms, Average = 0ms  C:\&gt;ping 2001:db8:acad:b::1  Pinging 2001:db8:acad:b::1 with 32 bytes of data:  Reply from 2001:DB8:ACAD:B::1: bytes=32 time&lt;1ms TTL=255 Reply from 2001:DB8:ACAD:B::1: bytes=32 time&lt;1ms TTL=255 Reply from 2001:DB8:ACAD:B::1: bytes=32 time&lt;1ms TTL=255 Reply from 2001:DB8:ACAD:B::1: bytes=32 time&lt;1ms TTL=255  Ping statistics for 2001:DB8:ACAD:B::1:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 0ms, Average = 0ms  C:\&gt; </pre> <p>Fuente: Autor</p> <p>Se realiza la prueba de conectividad utilizando el comando Ping entre el host PC-A y la subinterfaz g0/0/1.3 del Router 1. En el resultado que se obtiene se observa los paquetes enviados (4), los recibidos (4) y los perdidos (0), lo cual indica que la conexión es exitosa tanto para el direccionamiento IPV4 como para IPV6. Permite la comunicación, transmisión y envío de paquetes entre el PC-A y la subinterfaz g0/0/1.3 del Router.</p> |
|--|---------------|--|

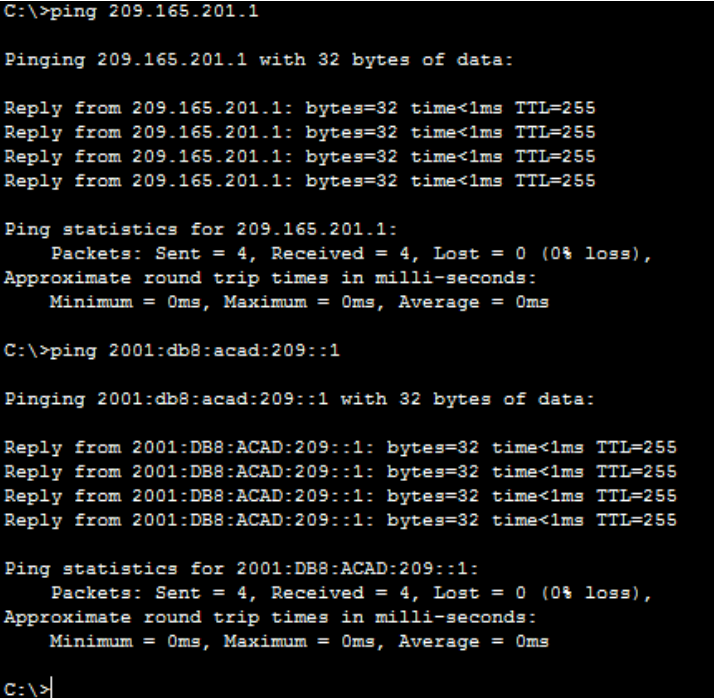
|  |               |  |
|--|---------------|--|
|  | R1 - G0/0/1.4 | Figura 16 Ping desde PC-A a G0/0/1.4   |
|  |               | <pre> C:\&gt;ping 10.53.8.97  Pinging 10.53.8.97 with 32 bytes of data:  Reply from 10.53.8.97: bytes=32 time&lt;1ms TTL=255 Reply from 10.53.8.97: bytes=32 time&lt;1ms TTL=255 Reply from 10.53.8.97: bytes=32 time&lt;1ms TTL=255 Reply from 10.53.8.97: bytes=32 time&lt;1ms TTL=255  Ping statistics for 10.53.8.97:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:     Minimum = 0ms, Maximum = 0ms, Average = 0ms  C:\&gt;ping 2001:db8:acad:c::1  Pinging 2001:db8:acad:c::1 with 32 bytes of data:  Reply from 2001:DB8:ACAD:C::1: bytes=32 time&lt;1ms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time&lt;1ms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time&lt;1ms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time&lt;1ms TTL=255  Ping statistics for 2001:DB8:ACAD:C::1:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:     Minimum = 0ms, Maximum = 0ms, Average = 0ms  C:\&gt;  </pre> <p>Fuente: Autor</p> <p>Se realiza la prueba de conectividad utilizando el comando Ping entre el host PC-A y la subinterfaz g0/0/1.4 del Router 1. En el resultado que se obtiene se observa los paquetes enviados (4), los recibidos (4) y los perdidos (0), lo cual indica que la conexión es exitosa tanto para el direccionamiento IPV4 como para IPV6. Permite la comunicación, transmisión y envío de paquetes entre el PC-A y la subinterfaz g0/0/1.4 del Router.</p> |

|  |              |   |
|--|--------------|---|
|  | S1 - VLAN 40 | Figura 17 Ping desde PC-A a SVI – S1  |
|  |              |  <pre> C:\&gt;ping 10.53.8.98  Pinging 10.53.8.98 with 32 bytes of data:  Reply from 10.53.8.98: bytes=32 time&lt;1ms TTL=254 Reply from 10.53.8.98: bytes=32 time&lt;1ms TTL=254 Reply from 10.53.8.98: bytes=32 time&lt;1ms TTL=254 Reply from 10.53.8.98: bytes=32 time&lt;1ms TTL=254  Ping statistics for 10.53.8.98:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 0ms, Average = 0ms  C:\&gt;ping 2001:db8:acad:c::98  Pinging 2001:db8:acad:c::98 with 32 bytes of data:  Request timed out. Request timed out. Request timed out. Request timed out.  Ping statistics for 2001:DB8:ACAD:C::98:     Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  C:\&gt; </pre> <p>Fuente: Autor</p> <p>Se realiza la prueba de conectividad utilizando el comando Ping entre el host PC-A y la interfaz de administración (SVI) configurada en la VLAN 40 del Switch 1. En el resultado que se obtiene se observa los paquetes enviados (4), los recibidos (4) y los perdidos (0), para el direccionamiento IPV4, lo cual indica que la conexión es exitosa, sin embargo, para el direccionamiento IPV6, se obtiene paquetes enviados (4), recibidos (0) y perdidos (4), indica que se perdió la conexión con la interfaz empleando el direccionamiento IPV6 en consecuencia por el IOS del dispositivo.</p> |

|  |              |  |
|--|--------------|--|
|  | S2 – VLAN 40 | Figura 18 Ping desde PC-A a SVI – S2   |
|  |              |  <pre> C:\&gt;ping 10.53.8.99  Pinging 10.53.8.99 with 32 bytes of data:  Reply from 10.53.8.99: bytes=32 time&lt;1ms TTL=254 Reply from 10.53.8.99: bytes=32 time=11ms TTL=254 Reply from 10.53.8.99: bytes=32 time&lt;1ms TTL=254 Reply from 10.53.8.99: bytes=32 time=13ms TTL=254  Ping statistics for 10.53.8.99:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 13ms, Average = 6ms  C:\&gt;ping 2001:db8:acad:c::99  Pinging 2001:db8:acad:c::99 with 32 bytes of data:  Request timed out. Request timed out. Request timed out. Request timed out.  Ping statistics for 2001:DB8:ACAD:C::99:     Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  C:\&gt; </pre> <p>Fuente: Autor</p> <p>Se realiza la prueba de conectividad utilizando el comando Ping entre el host PC-A y la interfaz de administración (SVI) configurada en la VLAN 40 del Switch 2. En el resultado que se obtiene se observa los paquetes enviados (4), los recibidos (4) y los perdidos (0), para el direccionamiento IPV4, lo cual indica que la conexión es exitosa, sin embargo, para el direccionamiento IPV6, se obtiene paquetes enviados (4), recibidos (0) y perdidos (4), indica que se perdió la conexión con la interfaz empleando el direccionamiento IPV6 en consecuencia por el IOS del dispositivo.</p> |

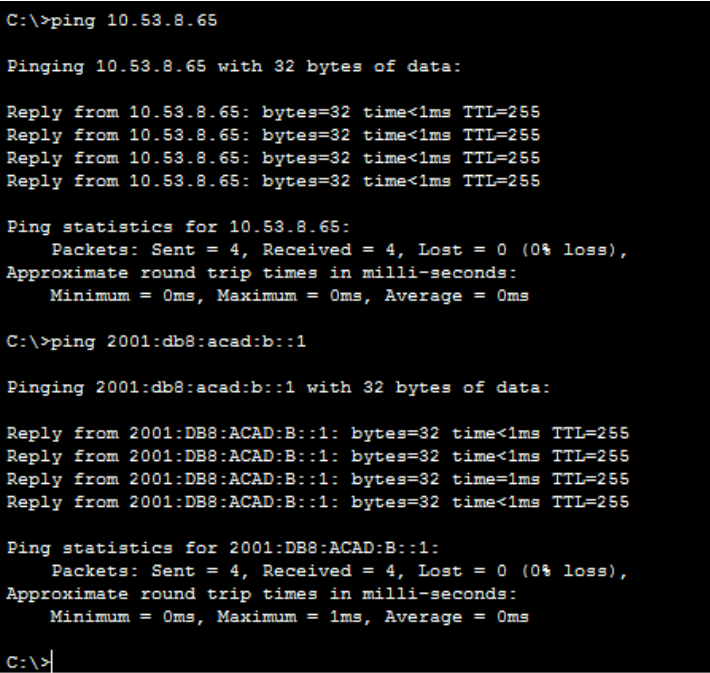
|  |      |   |
|--|------|---|
|  | PC-B | <p>Figura 19 Ping desde PC-A a PC-B</p>  <pre> C:\&gt;ping 10.53.8.85  Pinging 10.53.8.85 with 32 bytes of data:  Reply from 10.53.8.85: bytes=32 time&lt;1ms TTL=127 Reply from 10.53.8.85: bytes=32 time&lt;1ms TTL=127 Reply from 10.53.8.85: bytes=32 time&lt;1ms TTL=127 Reply from 10.53.8.85: bytes=32 time=1ms TTL=127  Ping statistics for 10.53.8.85:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 1ms, Average = 0ms  C:\&gt;ping 2001:db8:acad:a::50  Pinging 2001:db8:acad:a::50 with 32 bytes of data:  Reply from 2001:DB8:ACAD:A::50: bytes=32 time=5ms TTL=128 Reply from 2001:DB8:ACAD:A::50: bytes=32 time=16ms TTL=128 Reply from 2001:DB8:ACAD:A::50: bytes=32 time=3ms TTL=128 Reply from 2001:DB8:ACAD:A::50: bytes=32 time=16ms TTL=128  Ping statistics for 2001:DB8:ACAD:A::50:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 3ms, Maximum = 16ms, Average = 10ms  C:\&gt; </pre> <p>Fuente: Autor</p> <p>Se realiza la prueba de conectividad utilizando el comando Ping entre el host PC-A y el host PC-B. En el resultado que se obtiene se observa los paquetes enviados (4), los recibidos (4) y los perdidos (0), lo cual indica que la conexión es exitosa tanto para el direccionamiento IPV4 como para IPV6. Permite la comunicación, transmisión y envío de paquetes entre ellos hosts PC-A y PC-B.</p> |
|--|------|---|

|  |             |   |
|--|-------------|---|
|  | R1 – Bucle0 | <p><b>Figura 20 Ping desde PC-A a Bucle0</b></p>  <pre> C:\&gt;ping 209.165.201.1  Pinging 209.165.201.1 with 32 bytes of data:  Reply from 209.165.201.1: bytes=32 time&lt;1ms TTL=255 Reply from 209.165.201.1: bytes=32 time&lt;1ms TTL=255 Reply from 209.165.201.1: bytes=32 time&lt;1ms TTL=255 Reply from 209.165.201.1: bytes=32 time&lt;1ms TTL=255  Ping statistics for 209.165.201.1:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 0ms, Average = 0ms  C:\&gt;ping 2001:db8:acad:209::1  Pinging 2001:db8:acad:209::1 with 32 bytes of data:  Reply from 2001:DB8:ACAD:209::1: bytes=32 time&lt;1ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time&lt;1ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time&lt;1ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time&lt;1ms TTL=255  Ping statistics for 2001:DB8:ACAD:209::1:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 0ms, Average = 0ms  C:\&gt; </pre> <p>Fuente: Autor</p> <p>Se realiza la prueba de conectividad utilizando el comando Ping entre el host PC-A y la interfaz loopback0 del Router 1. En el resultado que se obtiene se observa los paquetes enviados (4), los recibidos (4) y los perdidos (0), lo cual indica que la conexión es exitosa tanto para el direccionamiento IPV4 como para IPV6. La comunicación, transmisión y envío de paquetes desde el host PC-A hacia el bucle0 del Router 1 se realiza de manera correcta.</p> |
|--|-------------|---|

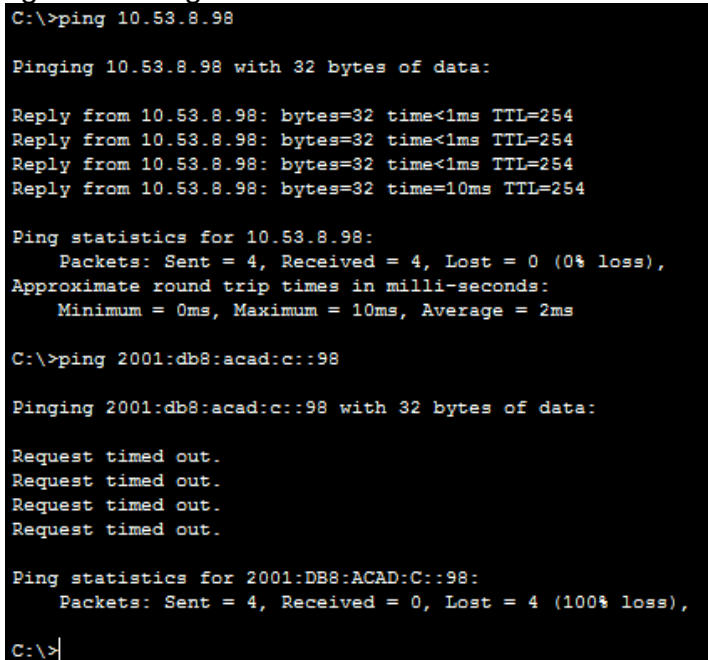
|             |                    |   |
|-------------|--------------------|---|
| <b>PC-B</b> | <b>R1 - Bucle0</b> | <b>Figura 21 Ping desde PC-B a Bucle0</b>   |
|             |                    |  <pre> C:\&gt;ping 209.165.201.1  Pinging 209.165.201.1 with 32 bytes of data:  Reply from 209.165.201.1: bytes=32 time&lt;1ms TTL=255 Reply from 209.165.201.1: bytes=32 time&lt;1ms TTL=255 Reply from 209.165.201.1: bytes=32 time&lt;1ms TTL=255 Reply from 209.165.201.1: bytes=32 time&lt;1ms TTL=255  Ping statistics for 209.165.201.1:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 0ms, Average = 0ms  C:\&gt;ping 2001:db8:acad:209::1  Pinging 2001:db8:acad:209::1 with 32 bytes of data:  Reply from 2001:DB8:ACAD:209::1: bytes=32 time&lt;1ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time&lt;1ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time&lt;1ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time&lt;1ms TTL=255  Ping statistics for 2001:DB8:ACAD:209::1:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 0ms, Average = 0ms  C:\&gt;  </pre> <p>Fuente: Autor</p> <p>Se realiza la prueba de conectividad utilizando el comando Ping entre el host PC-B y la interfaz loopback0 del Router 1. En el resultado que se obtiene se observa los paquetes enviados (4), los recibidos (4) y los perdidos (0), lo cual indica que la conexión es exitosa tanto para el direccionamiento IPV4 como para IPV6. La comunicación, transmisión y envío de paquetes desde el host PC-B hacia el bucle0 del Router 1 se realiza de manera correcta.</p> |

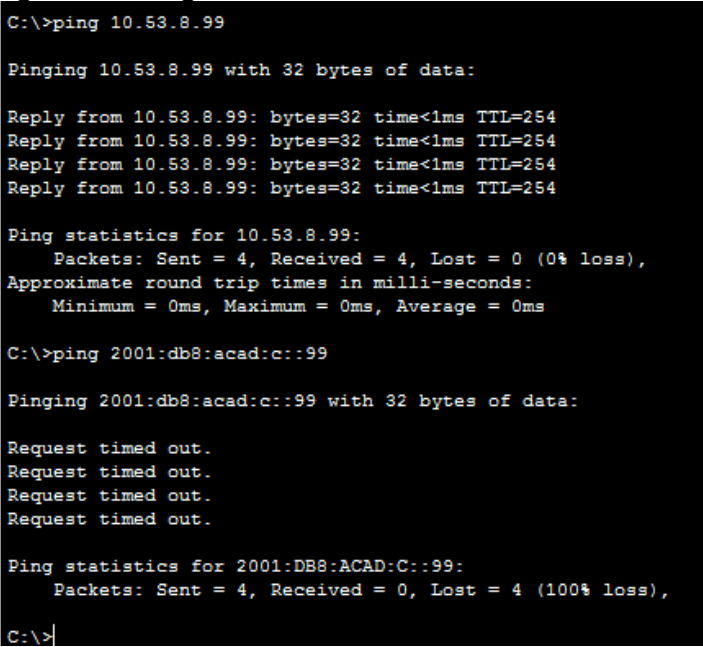
|               |   |
|---------------|---|
| R1 – G0/0/1.2 | Figura 22 Ping desde PC-B a G0/0/1.2  |
|               | <pre> C:\&gt;ping 10.53.8.1  Pinging 10.53.8.1 with 32 bytes of data:  Reply from 10.53.8.1: bytes=32 time&lt;1ms TTL=255 Reply from 10.53.8.1: bytes=32 time&lt;1ms TTL=255 Reply from 10.53.8.1: bytes=32 time&lt;1ms TTL=255 Reply from 10.53.8.1: bytes=32 time&lt;1ms TTL=255  Ping statistics for 10.53.8.1:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 0ms, Average = 0ms  C:\&gt;ping 2001:db8:acad:a::1  Pinging 2001:db8:acad:a::1 with 32 bytes of data:  Reply from 2001:DB8:ACAD:A::1: bytes=32 time&lt;1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time&lt;1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time=22ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time&lt;1ms TTL=255  Ping statistics for 2001:DB8:ACAD:A::1:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 22ms, Average = 5ms  C:\&gt; </pre> <p>Fuente: Autor</p> <p>Se realiza la prueba de conectividad utilizando el comando Ping entre el host PC-B y la subinterfaz g0/0/1.2 del Router 1. En el resultado que se obtiene se observa los paquetes enviados (4), los recibidos (4) y los perdidos (0), lo cual indica que la conexión es exitosa tanto para el direccionamiento IPV4 como para IPV6. Permite la comunicación, transmisión y envió de paquetes entre el PC–B y la subinterfaz g0/0/1.2 del Router.</p> |



|               |  |
|---------------|--|
| R1 – G0/0/1.3 | Figura 23 Ping desde PC-B a G0/0/1.3   |
|               |  <pre> C:\&gt;ping 10.53.8.65  Pinging 10.53.8.65 with 32 bytes of data:  Reply from 10.53.8.65: bytes=32 time&lt;1ms TTL=255 Reply from 10.53.8.65: bytes=32 time&lt;1ms TTL=255 Reply from 10.53.8.65: bytes=32 time&lt;1ms TTL=255 Reply from 10.53.8.65: bytes=32 time&lt;1ms TTL=255  Ping statistics for 10.53.8.65:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 0ms, Average = 0ms  C:\&gt;ping 2001:db8:acad:b::1  Pinging 2001:db8:acad:b::1 with 32 bytes of data:  Reply from 2001:DB8:ACAD:B::1: bytes=32 time&lt;1ms TTL=255 Reply from 2001:DB8:ACAD:B::1: bytes=32 time&lt;1ms TTL=255 Reply from 2001:DB8:ACAD:B::1: bytes=32 time&lt;1ms TTL=255 Reply from 2001:DB8:ACAD:B::1: bytes=32 time&lt;1ms TTL=255  Ping statistics for 2001:DB8:ACAD:B::1:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 1ms, Average = 0ms  C:\&gt; </pre> <p>Fuente: Autor</p> <p>Se realiza la prueba de conectividad utilizando el comando Ping entre el host PC-B y la subinterfaz g0/0/1.3 del Router 1. En el resultado que se obtiene se observa los paquetes enviados (4), los recibidos (4) y los perdidos (0), lo cual indica que la conexión es exitosa tanto para el direccionamiento IPV4 como para IPV6. Permite la comunicación, transmisión y envío de paquetes entre el PC-B y la subinterfaz g0/0/1.3 del Router.</p> |

|  |               |   |
|--|---------------|---|
|  | R1 – G0/0/1.4 | <p><b>Figura 24 Ping desde PC-B a G0/0/1.4</b></p> <pre> C:\&gt;ping 10.53.8.97  Pinging 10.53.8.97 with 32 bytes of data:  Reply from 10.53.8.97: bytes=32 time&lt;1ms TTL=255 Reply from 10.53.8.97: bytes=32 time=1ms TTL=255 Reply from 10.53.8.97: bytes=32 time&lt;1ms TTL=255 Reply from 10.53.8.97: bytes=32 time=1ms TTL=255  Ping statistics for 10.53.8.97:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:     Minimum = 0ms, Maximum = 1ms, Average = 0ms  C:\&gt;ping 2001:db8:acad:c::1  Pinging 2001:db8:acad:c::1 with 32 bytes of data:  Reply from 2001:DB8:ACAD:C::1: bytes=32 time=5ms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time&lt;1ms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time=10ms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time&lt;1ms TTL=255  Ping statistics for 2001:DB8:ACAD:C::1:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:     Minimum = 0ms, Maximum = 10ms, Average = 3ms  C:\&gt;  </pre> <p>Fuente: Autor</p> <p>Se realiza la prueba de conectividad utilizando el comando Ping entre el host PC-B y la subinterfaz g0/0/1.4 del Router 1. En el resultado que se obtiene se observa los paquetes enviados (4), los recibidos (4) y los perdidos (0), lo cual indica que la conexión es exitosa tanto para el direccionamiento IPV4 como para IPV6. Permite la comunicación, transmisión y envió de paquetes entre el PC-B y la subinterfaz g0/0/1.4 del Router.</p> |
|--|---------------|---|

|  |              |   |
|--|--------------|---|
|  | S1 – VLAN 40 | <p><b>Figura 25 Ping desde PC-B a SVI – S1</b></p>  <pre> C:\&gt;ping 10.53.8.98  Pinging 10.53.8.98 with 32 bytes of data:  Reply from 10.53.8.98: bytes=32 time&lt;1ms TTL=254 Reply from 10.53.8.98: bytes=32 time&lt;1ms TTL=254 Reply from 10.53.8.98: bytes=32 time&lt;1ms TTL=254 Reply from 10.53.8.98: bytes=32 time=10ms TTL=254  Ping statistics for 10.53.8.98:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 10ms, Average = 2ms  C:\&gt;ping 2001:db8:acad:c::98  Pinging 2001:db8:acad:c::98 with 32 bytes of data:  Request timed out. Request timed out. Request timed out. Request timed out.  Ping statistics for 2001:DB8:ACAD:C::98:     Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  C:\&gt; </pre> <p>Fuente: Autor</p> <p>Se realiza la prueba de conectividad utilizando el comando Ping entre el host PC-B y la interfaz de administración (SVI) configurada en la VLAN 40 del Switch 1. En el resultado que se obtiene se observa los paquetes enviados (4), los recibidos (4) y los perdidos (0), para el direccionamiento IPV4, lo cual indica que la conexión es exitosa, sin embargo, para el direccionamiento IPV6, se obtiene paquetes enviados (4), recibidos (0) y perdidos (4), indica que se perdió la conexión con la interfaz empleando el direccionamiento IPV6 en consecuencia por el IOS del dispositivo.</p> |
|--|--------------|---|

|  |              |  |
|--|--------------|--|
|  | S2 – VLAN 40 | <p><b>Figura 26 Ping desde PC-B a SVI – S2</b></p>  <pre> C:\&gt;ping 10.53.8.99  Pinging 10.53.8.99 with 32 bytes of data:  Reply from 10.53.8.99: bytes=32 time&lt;1ms TTL=254 Reply from 10.53.8.99: bytes=32 time&lt;1ms TTL=254 Reply from 10.53.8.99: bytes=32 time&lt;1ms TTL=254 Reply from 10.53.8.99: bytes=32 time&lt;1ms TTL=254  Ping statistics for 10.53.8.99:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 0ms, Average = 0ms  C:\&gt;ping 2001:db8:acad:c::99  Pinging 2001:db8:acad:c::99 with 32 bytes of data:  Request timed out. Request timed out. Request timed out. Request timed out.  Ping statistics for 2001:DB8:ACAD:C::99:     Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  C:\&gt; </pre> <p>Fuente: Autor</p> <p>Se realiza la prueba de conectividad utilizando el comando Ping entre el host PC-B y la interfaz de administración (SVI) configurada en la VLAN 40 del Switch 2. En el resultado que se obtiene se observa los paquetes enviados (4), los recibidos (4) y los perdidos (0), para el direccionamiento IPV4, lo cual indica que la conexión es exitosa, sin embargo, para el direccionamiento IPV6, se obtiene paquetes enviados (4), recibidos (0) y perdidos (4), indica que se perdió la conexión con la interfaz empleando el direccionamiento IPV6 en consecuencia por el IOS del dispositivo.</p> |
|--|--------------|--|

## CONCLUSIONES

Se logra concluir con el desarrollo de este trabajo de prueba de habilidades que, es importante tener en cuenta antes de direccionar una red, la cantidad de subredes que se requiere y la cantidad de host por cada una de ellas, puesto que, en la realización de la tabla de direccionamiento se debe tener en cuenta la dirección de red y la máscara de subred que nos otorgan para dar inicio al subneteo requerido y obtener de manera correcta las direcciones IP para la configuración de los dispositivos de red y finales que conforman la topología.

Tener conocimiento de los comandos para llevar a cabo los procesos requeridos en la configuración de interfaces en el router y en el switch, es importante para el correcto desarrollo y puesta en práctica de los conocimientos adquiridos en las diferentes lecturas. El empleo de los comandos para la seguridad, para la verificación de conectividad entre los diferentes dispositivos de la red, para la asignación de direcciones IP y dominio, para cambio de nombre del dispositivo entre otros, permiten realizar comprobación, protección y una correcta configuración de los dispositivos de red y finales.

La asignación de direcciones IPV4 e IPV6 de manera estática o dinámica es de mucha responsabilidad, puesto que, cada equipo debe contar con una dirección única y la repetición de esta en dos equipos diferentes traerán problemas en el funcionamiento de la red. Por esta razón es recomendable emplear una tabla de direccionamiento, para llevar una organización en la asignación de las direcciones entre los diferentes dispositivos que conforman la red.

Para el desarrollo del escenario 2, se emplearon switches de capa 3 los cuales fueron configurados de acuerdo a los requerimientos solicitados, en la verificación de conectividad utilizando el comando PING, y realizando la comprobación en la interfaz de administración (SVI) se notó que no da respuesta exitosa con IPV6, a pesar que la configuración es correcta, no permite la verificación de conectividad

con este direccionamiento, dando como resultado que es el IOS del dispositivo que impide realizar la comprobación.

El diseño de una red requiere de organización, eficiencia y seguridad, es por ello que, la creación de VLAN, configuración básica de seguridad en los dispositivos de red, creación de Etherchannel, subinterfaces entre otros, permiten la administración de red de una manera segura y confiable.

Finalmente, se concluye, que es primordial y necesario contar con los conocimientos requeridos para una administración correcta de una red LAN y WAN. El uso adecuado de la consola y de los comandos, permite tener una respuesta exitosa en el momento de verificar la conexión empleando el comando ping entre los dispositivos, además, de contar con un esquema de direccionamiento preciso para la asignación de direcciones en cada subred.

## BIBLIOGRAFÍA

CAPELLA HERNANDEZ, Juan Vicente. Características y configuración básica de VLANs. {En línea}. (2012). {20 noviembre de 2022}. Disponible en: <http://hdl.handle.net/10251/16310>

CISCO. Asignación de direcciones IPv4. {En línea}. (2020). {4 octubre de 2022}. Disponible en: <https://contenthub.netacad.com/itn/11.0.1>

CISCO. Configuración básica de dispositivos. {En línea}. (2020). {4 octubre de 2022}. Disponible en: <https://contenthub.netacad.com/srwe/1.0.1>

CISCO. Conceptos de Switching. {En línea}. (2020). {4 octubre de 2022}. Disponible en: <https://contenthub.netacad.com/srwe/2.0.1>

CISCO. Configuración básica de un router. {En línea}. (2020). {4 octubre de 2022}. Disponible en: <https://contenthub.netacad.com/itn/10.0.1>

CISCO. VLANs. {En línea}. (2020). {10 noviembre de 2022}. Disponible en: <https://contenthub.netacad.com/srwe/3.0.1>

CISCO. Enrutamiento inter VLAN. {En línea}. (2020). {10 noviembre de 2022}. Disponible en: <https://contenthub.netacad.com/srwe/4.0.1>

CISCO. Configuración en seguridad en switches. {En línea}. (2020). {10 noviembre de 2022}. Disponible en: <https://contenthub.netacad.com/srwe/11.0.1>

CISCO. Enrutamiento estático. {En línea}. (2020). {10 noviembre de 2022}. Disponible en: <https://contenthub.netacad.com/srwe/15.0.1>

FERNANDEZ TERAN, Pablo David. Desarrollo de un programa que permita generar archivos de configuración para routers CISCO mediante la simulación de la Interfaz de Línea de Comandos (CLI). {En línea}. (2005). {20 noviembre de 2022}. Disponible en: <http://bibdigital.epn.edu.ec/handle/15000/5496>

GONZÁLEZ LAFORGA, Belén. Servicio interactivo de asignación de direcciones IP. {En línea}. (2021). {20 noviembre de 2022}. Disponible en: <https://oa.upm.es/cgi/export/eprint/68052/HTML/upm-eprint-68052.html>

GUACA, Nancy. Configuración básica de Switches [OVI]. {En línea}. (2018). {11 noviembre 2022}. Disponible en: <http://hdl.handle.net/10596/23215>

LOPEZ BULLA, Ricardo. Enrutamiento y configuración de redes. {En línea}. (2018). {20 noviembre de 2022}. Disponible en: <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://digitk.areandina.edu.co/bitstream/handle/areandina/1495/74%20ENRUTAMIENTO%20Y%20CONFIGURACION%20DE%20REDES.pdf?sequence=1>

SORIANO, Miguel. Seguridad en redes y seguridad de la información. {En línea}. (2014). {20 noviembre de 2022}. Disponible en: [chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://psm.fei.stuba.sk/pages/47/Seguridad de Red e Informacion.pdf](chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://psm.fei.stuba.sk/pages/47/Seguridad_de_Red_e_Informacion.pdf)

TAPIAS BAENA, Juan. Introducción a las VLAN [OVI]. {En línea}. (2022). {11 noviembre de 2022}. Disponible en: <https://repository.unad.edu.co/handle/10596/49452>



## ANEXOS

**ANEXO A:** Descarga de archivos de simulación

<https://drive.google.com/drive/folders/1oNPfNcphEUyacxSqm9vOWK4jPDzjPj6E?usp=sharing>