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

CRISTIAN ESNEIDER MUÑOZ ÑAÑEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA EN SISTEMAS
PITALITO - HUILA
2022

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

CRISTIAN ESNEIDER MUÑOZ ÑAÑEZ

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

DIRECTOR:
PAULITA FLOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA EN SISTEMAS
PITALITO - HUILA
2022

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____
_____
_____
_____

Firma del Presidente del jurado

Firma del Jurado

Firma del Jurado

Pitalito Huila, 27 de Noviembre de 2022

AGRADECIMIENTOS

A culmino de mi carrera, extiendo mi agradecimiento a quienes han hecho parte de este caminar, aquellos (as) que han aportado a mi construcción personal y académica: Dios, mis padres, familiares y profesores (as) que día a día plasmaron en mi valores y conocimiento, tesoros que, aunque intangibles son indudablemente invaluables. En la vida, además de aprender, es necesario y casi inevitable desaprender, el lograr avanzar, mejorar, edificarse a si mismo es un proceso, -a modo personal- extenso pero enriquecedor, y ustedes son quienes en mi lo han hecho posible.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Cisco: Empresa de comunicaciones líder en el mundo de las redes de datos y TI, una compañía muy importante que fabrica componentes de red, como routers, firewalls de hardware, productos de telefonía IP, entre otros, estos dispositivos son bastantes robustos y conocidos en todo el mundo.[1]

Cnna: Certificaciones más importantes dentro de la industria de la Tecnología de la Información. Esta certificación es de nivel asociado y está diseñada para desarrollar habilidades prácticas para detectar y resolver problemas de red específicos.[2]

Conmutación: Se entiende el término conmutación como el modo que posibilita que una señal arribe a su destino después de salir de su origen.[3]

Router: Conocido también como enrutador o ruteador, permite interconectar computadoras que funcionan dentro de una red.[4]

Interface: El entorno que permite a una persona interactuar con las máquinas se denomina interfaz de usuario.[5]

Host: Es una tecnología que ofrece distintos servicios a todos los demás equipos conectados a la red por medio de un equipo que funciona como su "huésped".[6]

---

[1] ORTEGO DELGADO Daniel. ¿Qué es la Certificación Cisco CCNA?. OpenWebinars {En línea}. (27 de 08 de 2017). {27/10/2022} Obtenido de: https://openwebinars.net/blog/que-es-la-certificacion-cisco-ccna-200-125/

[2] ORTEGO DELGADO Daniel. ¿Qué es la Certificación Cisco CCNA?. OpenWebinars {En línea}. (27 de 08 de 2017). {27/10/2022} Obtenido de: https://openwebinars.net/blog/que-es-la-certificacion-cisco-ccna-200-125/

[3] PEREZ PORTO, J., Merino, M. Definición de conmutación - Qué es, Significado y Concepto.{En línea} (2 de diciembre de 2016). {23/11/2022} Disponible en: https://definicion.de/conmutacion/

[4] PEREZ PORTO, J., Merino, M. Definición de router - Qué es, Significado y Concepto. {En línea} (15 de enero de 2010). {23/11/2022} Definicion.de. Recuperado el 23 de noviembre de 2022 de https://definicion.de/router/

[5] PEREZ PORTO, J., Merino, M. Definición de interfaz - Qué es, Significado y Concepto. {En línea} (3 de mayo de 2011). {23/11/2022} Definición.de. Recuperado el 23 de noviembre de 2022 de: https://definicion.de/interfaz/

[6] VELAZQUEZ QUINTERO Jorge. Qué es Host. {En línea} (13 de 07 de 2021). {23/11/2022} Pág. 2. Obtenido de DocerArgentina: https://docer.com.ar/doc/xs1550x

Enrutamiento: Proceso de reenviar paquetes entre redes, siempre buscando la mejor ruta. Para encontrar esa ruta más óptima, se debe tener en cuenta la tabla de enrutamiento y algunos otros parámetros como la métrica.[7]

Switch: Un switch es el dispositivo analógico que permite interconectar redes operando en la capa 2 o de nivel de enlace de datos del modelo OSI u Open Systems Interconnection.[8]

[7] BARRIO DAVID, Fundamentos y Protocolos, Enrutamiento {En linea} (2020d, julio 10). {24/11/2022}, Obtenido de: https://eltallerdelbit.com/enrutamiento-fundamentos-y-protocolos/

[8] BEMBIBRE, Victoria. Definición de Switch. Definición ABC {En línea}. (enero, 2009). {27/10/2022}. Obtenido de: https://www.definicionabc.com/tecnologia/switch.php

RESUMEN

La importancia de las redes informáticas abarca varios aspectos de nuestro entorno digital y tecnológico. Cisco es una empresa de comunicaciones líder en el mundo de las redes de datos y TI que en conjunto con CNNA una de las certificaciones más importantes dentro de la industria de la tecnología de la información, asociada a prácticas en el diagnóstico y soluciones específicos de redes, ayudando así al entendimiento sobre las tecnologías de la comunicación.

El software Cisco Packet Tracer herramienta de simulación de redes donde se configuran, simulan enrutamientos y conmutaciones mediante una interfaz de usuario permitiendo arrastrar y soltar dispositivos de red y simular de una mejor manera una red.

Palabras Clave: CISCO, CNNA, Conmutación, Enrutamiento, Redes

ABSTRACT

The importance of computer networks includes various aspects of our digital and technological environment. Cisco is the leading company in the world of communications, data networks and IT, that together with CNNA one of the most important certifications in the information technology industry, associated with internships in network-specific diagnostics and solutions; They help understand communication technologies.

"Cisco Packet Tracer" software is a network simulation tool, which allows you to configure, simulate routing and switching through a user interface, in which you can drag and drop network devices and simulate it in the best possible way

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

INTRODUCCIÓN

Las redes se han convertido en un medio de comunicación y de intercambio de información relevante en el día a día, estando presentes desde la red informática de casa hasta la red global (internet).

En el presente trabajo se muestra la simulación de dos escenarios con su diferente topología de red, trabajo optado como modalidad de grado en Ingeniería en Sistemas en la Universidad Nacional Abierta y a Distancia (UNAD). El primer escenario consta de configurar algunos dispositivos en una red pequeña, un router, un switch y dos equipos de cómputo, diseñando un esquema de direccionamiento IPv4 y conexión para la LAN propuesta.

El segundo escenario consiste en una red que contiene un router, un switch y equipos que se debe configurar y hacer la respectiva conexión tanto con red IPv4 como red IPv6 para los hosts soportados, adicional el router y el switch también deben administrarse de forma segura con sus respectivas configuraciones para ello.

DESARROLLO

1. ESCENARIO 1

Escenario: En el primer escenario se configuran los dispositivos de una red pequeña, conformada por un router, un switch y equipos, los cuales deben configurarse, diseñar el esquema de direccionamiento IPv4 para las LAN propuestas.

Topología

Figura 1-Topología Escenario 1

Fuente: Prueba de habilidades ccna ii-2022

Objetivos

Parte 1: Construir en el simulador la Red

Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2

Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta.

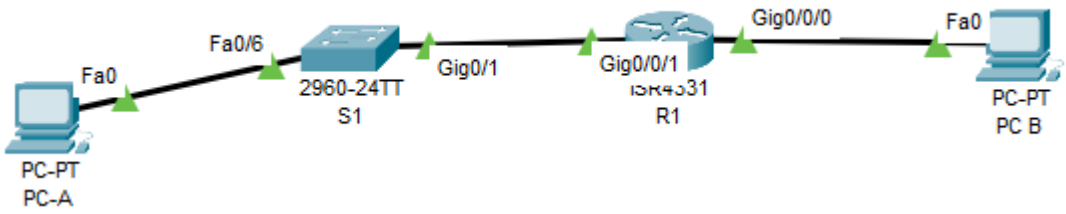
Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1

Parte 4: Configurar los hosts y verificar la conectividad entre los equipos

Parte 1: Construcción de la Red

En el simulador Packet Tracer se construye la red de acuerdo con la topología lógica que se plantea en la figura 1, para posteriormente conectar los equipos de cómputo.

Figura 2-Conexión de equipos



Fuente: Elaboración propia

Parte 2: Desarrollo del esquema de direccionamiento IP

Se desarrolla el esquema de direccionamiento IP, según la tabla de direccionamientos.

Tabla 1 - Tabla de direccionamiento

ITEM	REQUERIMIENTO
Dirección de Red	**172.64.3.0**
Requerimiento de host Subred LAN1	60
Requerimiento de host Subred LAN2	20
R1 G0/0/1	Última dirección de host de la subred LAN1
R1 G0/0/0	Última dirección de host de la subred LAN2
S1 SVI	Segunda dirección de host de la subred LAN1
PC-A	Décima dirección de host de la subred LAN1
PC-B	Décima dirección de host de la subred LAN2

Fuente: Elaboración propia

DIRECCION DE RED: 172.64.3.0

Se pide prestado **1 bit,** el necesario para abarcar las 2 subredes presentes en la topología.

$$\mathbf{2^1 = 2}$$

LAN 1. (60 Host)

Se verifica la fórmula $\mathbf{2^6 - 2 = 62\ Host}$, donde se indica cuántos bits se deben tomar prestados para cumplir con la cantidad de hosts que se crean por subred. En este caso son **6** bits.

Obtener nueva máscara:

La máscara que permite conectar los 62 host requeridos es la siguiente:

Tabla 2-Máscara de Red 1

BINARIO.	DECIMAL	PREFIJO DE RED	No. HOST
11111111.11111111.11111111.11000000	255.255.255.192	/26	**62**

Fuente: Elaboración propia

Se calculan el rengo de Hosts para la LAN 1.

Tabla 3 - LAN 1

LAN 1		
RED	RANGO DE HOSTS	BROADCAST
172.64.3.0/26	172.64.3.1 -- 172.64.3.62	172.64.3.63

Fuente: Elaboración propia

LAN 2. (20 Host)

Se verifica $\mathbf{2^5 - 2 = 30\ Host}$, donde se indica cuántos bits se deben tomar prestados para cumplir con la cantidad de hosts que se crean por subred. En este caso son **5**.

Obtener nueva máscara:

La máscara que permite conectar los 20 host requeridos es la siguiente:

Tabla 4-Máscara de red 2

BINARIO.	DECIMAL	PREFIJO DE RED	No. HOST
11111111.11111111.11111111.11100000	255.255.255.224	/27	**30**

Fuente: Elaboración propia

Se inicia la segunda sub red con la dirección IP siguiente al BROADCAST calculado en la primera sub red.

Tabla 5-LAN 2

LAN 2		
RED	RANGO DE HOSTS	BROADCAST
172.64.3.**64**/27	172.64.3.65 --172.64.3.94	172.64.3.95

Fuente: Elaboración propia

Por último, se obtienen todos los resultados:

Tabla 6- Resultados Obtenidos

ITEM	**REQUERIMIENTO**
Dirección de Red	**172.64.3.0**
Requerimiento de host Subred LAN1	**172.64.3.0/ 26**
Requerimiento de host Subred LAN2	**172.64.3.64/ 27**
R1 G0/0/1	**172.64.3.62**
R1 G0/0/0	**172.64.3.94**

S1 SVI	**172.64.3.2**
PC-A	**172.64.3.10**
PC-B	**175.64.3.75**

Fuente: Elaboración propia

Parte 3: Configuración de los aspectos básicos

Se procede a realizar la configuración de los dispositivos de red (S1 y R1), los cuales se configuran mediante conexión de consola.

Paso 1: Configuración de los ajustes básicos

La configuración para R1 incluye:

CONFIGURACION R1

1. Se desactiva la búsqueda **DNS,** para ello realizamos lo siguiente:

Router> Se accede al router
Router>enable Ingreso al modo privilegiado
Router#configure terminal Ingreso a modo de configuración
Router(config)#no ip domain-lookup Desactivación de búsqueda DNS
Router(config)#

2. Se establece un nombre al Router, mediante el comando Hostname llamarlo como **R1.**

Router>enable Ingreso al modo privilegiado
Router#configure terminal Ingreso a modo de configuración
Router(config)#hostname R1 Configuración nombre del router
R1(config)#

3. Se añade un nombre de dominio el cual se llamará **ccna-sa.com.**

R1>enable Ingreso a modo privilegiado
R1#configure terminal Ingreso a modo de configuración
R1(config)#ip domain name ccna-sa.com Nombre de dominio
R1(config)#

4. Se configura una contraseña cifrada para el modo EXEC privilegiado: **ciscoenpass**

R1>enable	Ingreso a modo privilegiado
R1#configure terminal	Ingreso a modo de configuración
R1(config)#enable secret ciscoenpass	**C**ontraseña cifrada modo EXEC
R1(config)#	

5. Se configura una contraseña de acceso a la consola, para ello se utilizará la siguiente: **ciscoconpass**

R1#configure terminal	Ingreso a modo de configuración
R1(config)#line console 0	Se selecciona consola
R1(config-line)# pass	
R1(config-line)# password ciscoconpass	Ingreso de contraseña.
R1(config-line)#login	Se solicita el comando loguin para pedir la contraseña.

6. Se establece una longitud mínima para las contraseñas de **10 caracteres:**

R1#configure terminal	Ingreso al modo de configuración
R1(config)#security pass	
R1(config)#security passwords min-length 10	
R1(config)#	

Se habilita el comando para la longitud mínima para las contraseñas con passwords min-length.

7. Se crea un usuario administrativo en la base de datos local con los siguientes requerimientos:

- **Nombre de usuario: admin**
- **Contraseña: admin1pass**

R1#configure terminal	Ingreso a modo de configuración
R1(config)#username admin secret admin1pass	
R1(config)#	

Se configura el nombre del usuario administrativo con su contraseña, utilizando el comando username admin secret.

8. Se configura el inicio de sesión en las líneas VTY para usar la base de datos local

R1#
R1#configure terminal Ingreso a modo de configuración
R1(config)# line vty 0 4 Ingreso a la línea vty 0 4
R1(config-line)#login local Habilitado de login en las líneas VTY
R1(config-line)#

9. Se configuran las líneas VTY para que acepten conexiones SSH únicamente.

R1(config-line)# Ingreso de configuración de líneas
R1(config-line)#transport input ssh Conexión solo por ssh
R1(config-line)#

10. Se procede a cifrar las contraseñas de texto no cifrado, de la siguiente forma:

R1(config)**#** Ingreso a modo de configuración
R1(config)#service pass
R1(config)#service password-encryption Se cifran las contraseñas
R1(config)#

11. Se configura un banner MOTD, donde se visualiza el nombre del dispositivo, el nombre completo de quien configura y el programa académico al que pertenece.

R1(config)#banner motd #
Enter TEXT message. End with the character '#'.
R1 - CRISTIAN ESNEIDER MUNOZ NANEZ - INGENIERIA DE SISTEMAS
#
R1(config)#EXIT
Se ingresó a banner motd,

12. Se procede a realizar la configuración de la interface G0/0/0, estableciendo:

La descripción, dirección IPv4 y por último la activación de la interfaz

R1(config)#
R1(config)# interface gigabitEthernet 0/0/0
R1(config-if)#
R1(config-if)#ip address 172.64.3.94 255.255.255.224
R1(config-if)#no shutdown
Se configuró la interfaz G0/0/0 con ip y máscara de subred de la LAN 2.

13. Se configura la interface G0/0/1, con su respectiva descripción, su dirección IPv4 y por último activando la interfaz para su funcionamiento.

R1(config)#
R1(config)#interface gigabitEthernet 0/0/1
R1(config-if)#
R1(config-if)#ip address 172.64.3.62 255.255.255.192
R1(config-if)#no shutdown

Se configura la interfaz G0/0/0 con ip y máscara de subred de la LAN 1.

14. Se genera una clave de cifrado RSA: **Módulo de 1024 bits**

R1(config)#
R1(config)#crypto key generate r
R1(config)#crypto key generate rsa general-keys mo
R1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.ccna-sa.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
***Mar 1 1:45:27.100: %SSH-5-ENABLED: SSH 1.99 has been enabled**
R1(config)#

Se genera la clave de cifrado ingresando al módulo de configuración, y con la configuración: crypto key generate rsa general-keys modulus 1024.

La configuración de S1 incluye lo siguiente:

CONFIGURACIÓN S1

1. Se desactiva la búsqueda **DNS,** ejecutando el siguiendo comando:

Switch>	
Switch>enable	Ingreso a modo privilegiado
Switch#configure terminal	Ingreso a modo de configuración
Switch(config)#no ip domain-lookup	Desactivo la búsqueda DNS
Switch(config)#	

2. Se configura un nombre al switch, en este caso es: **S1**

Switch>enable	Ingreso a modo privilegiado
Switch#configure terminal	Ingreso a modo de configuración
Switch(config)#hostname S1	Configuración nombre del switch
S1(config)#	

3. Se le da un nombre de dominio, llamado en este caso **ccna-sa.com**

S1>enable	Ingreso a modo privilegiado
S1#configure terminal	Ingreso a modo de configuración
S1(config)#ip domain name ccna-sa.com	Nombre del dominio
S1(config)#	

4. Se establece la contraseña cifrada para el modo EXEC privilegiado: **ciscoenpass**

S1>enable	Ingreso a modo privilegiado
S1#configure terminal	Ingreso a modo de configuración
S1(config)#enable secret ciscoenpass	Contraseña cifrada modo
S1(config)#	

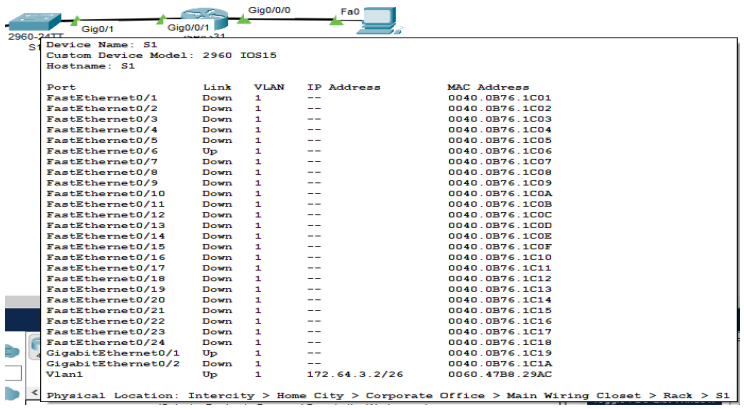
5. Se configura la contraseña de acceso a la consola: **ciscoconpass**

S1(config)#	Ingreso a modo de configuración
S1(config)#line console 0	Se selecciona la consola
S1(config-line)#password ciscoconpass	Ingresamos contraseña
S1(config-line)#login	Comando login para habilitar la contraseña

Se dejan apagados todos los puertos sin usar: **F0/1-4, F0/7-24, G0/1-2**

Los puertos sin usar se encuentran apagados.

Figura 3-Puertos sin usar



Fuente: Elaboración propia

6. Se crea un usuario administrativo en la base de datos local, con los siguientes requerimientos:

Nombre de usuario: admin
Contraseña: admin1pass

S1#configure terminal Ingreso a modo de configuración
S1(config)#username admin secret admin1pass
S1(config)#

Se configura un usuario administrativo admin con su contraseña.

7. Se configura el inicio de sesión en las líneas VTY para que use la base de datos local

S1(config)# Ingreso al modo configuración
S1(config)#line vty 0 4 Ingreso a la línea vty 04
S1(config-line)#login local Habilitado de login en las líneas VTY
S1(config-line)#

8. Se configura las líneas VTY para que acepten solamente las conexiones SSH

S1(config)# Ingreso al modo configuración
S1(config)#line vty 0 4 Ingreso a la línea vty 04
S1(config-line)#transport input ssh Conexión solo por ssh

9. Se cifran las contraseñas de texto no cifrado

S1(config)# Ingreso al modo configuración
S1(config)#service password-encryption Cifrado de contraseñas

10. Se procede a configurar un banner **MOTD,** donde se observa el nombre del dispositivo, el nombre completo de quien configura y el programa académico, así:

S1(config)#banner mot
S1(config)#banner motd #
Enter TEXT message. End with the character '#'.
S1 - CRISTIAN ESNEIDER MUNOZ NANEZ - INGENIERIA DE SISTEMAS
#
S1(config)#exit

Se configura el banner motd con lo requerido para el switch.

11. Se genera una clave de cifrado RSA; Módulo de 1024 bits

S1(config)#
S1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: S1.ccna-sa.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
***Mar 1 5:21:39.107: %SSH-5-ENABLED: SSH 1.99 has been enabled**

Se ingreso al modo configuración, realizando el cifrado RSA, módulo 1024 bits.

12. Por último, se configura la interfaz de administración (SVI) en VLAN1, con su descripción y dirección IPv4.

S1(config)#
S1(config)#interface vlan 1
S1(config-if)#description CONEXION RED VIRTUAL SUBRED A
S1(config-if)#ip address 172.64.3.2 255.255.255.192
S1(config-if)#

Se estableció la dirección ip al S1, asignando la ip con el comando ip addres dentro de la configuración de la interfaz vlan 1

Paso 2. Configuración de los equipos PC-A y PC-B.

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

Tabla 7- Configuración de red PC-A

Configuración de red de PC-A	
Descripción	PC-A
Dirección física	000A.41AA.176D
Dirección IPv4	172.64.3.10
Máscara de subred	255.255.255.192
Puerta de enlace IPv4 predeterminada	172.64.3.62

Fuente: Elaboración propia

Tabla 8- Configuración de red PC-B

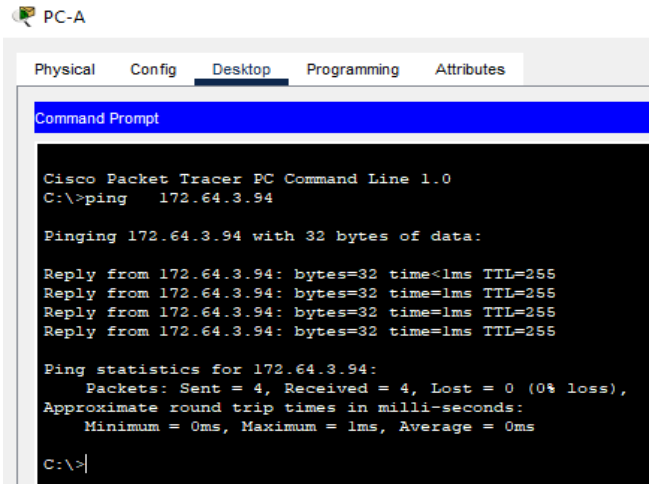
Configuración de red de PC-B	
Descripción	PC-B
Dirección física	00E0.F72D.1480
Dirección IPv4	175.64.3.75
Máscara de subred	255.255.255.224
Puerta de enlace IPv4 predeterminada	175.64.3.94

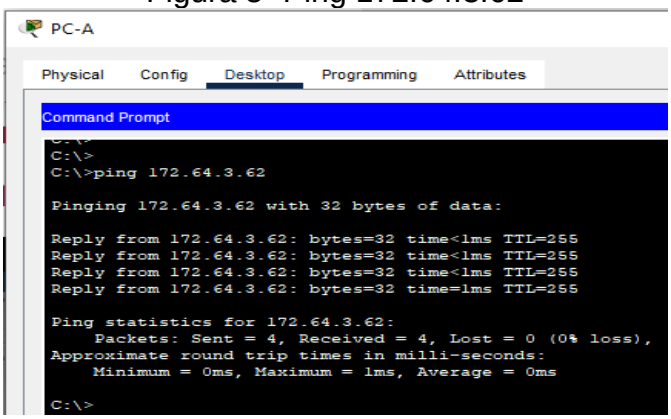
Fuente: Elaboración propia

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

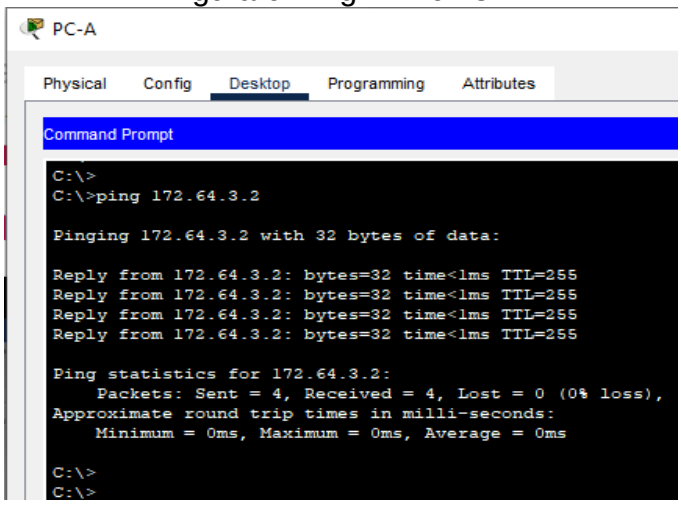
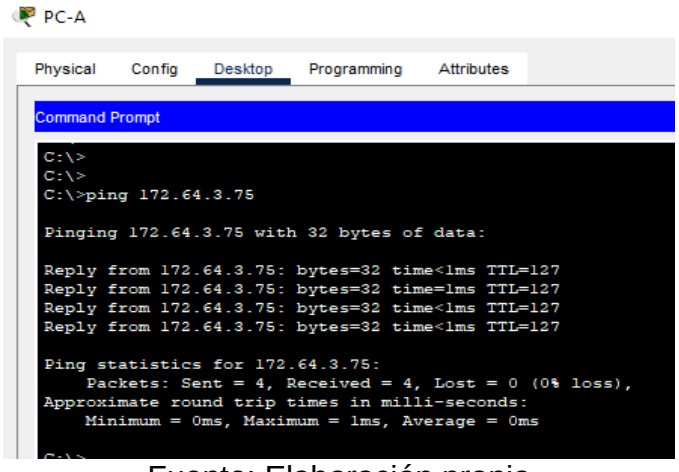
Para probar la conectividad entre todos los dispositivos de red, se utiliza el comando ping para las diferentes direcciones IP de la siguiente manera:

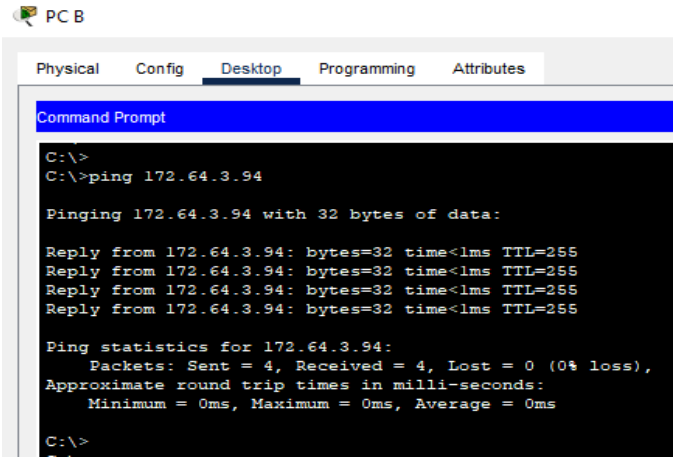
Tabla 9-Verificación de conectividad

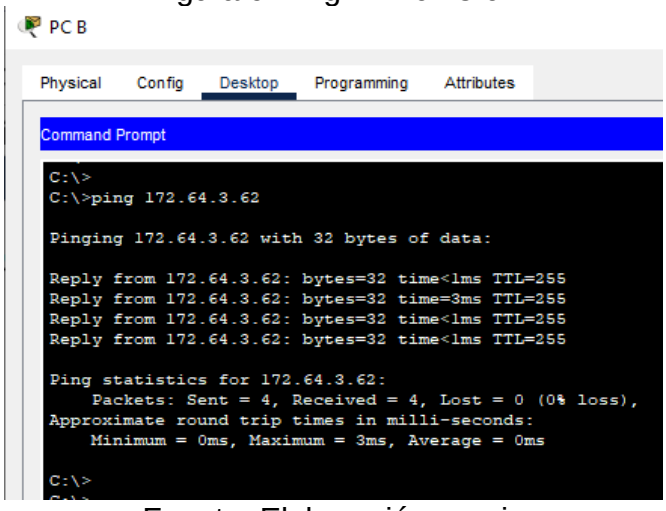
<table>
<tr><th>Desde</th><th>A</th><th>Dirección IP</th><th>Resultados de ping</th></tr>
<tr><td rowspan="2">PC-A</td><td>R1 G0/0/0</td><td>172.64.3.94</td><td>Exitoso
Figura 4-Ping 172.64.3.94
 

Fuente: Elaboración propia
Se establece un ping desde el PC-A (Host origen) dirigido a R1 con interfaz G0/0/0 (Host destino) cual corresponde la IP 172.64.3.94. En este caso ha sido satisfactorio ya que los cuatro paquetes de la prueba que se han enviado, se han recibido correctamente en un tiempo estimado de 0ms.</td></tr>
<tr><td>R1 G0/0/1</td><td>172.64.3.62</td><td>Exitoso.
Figura 5 -Ping 172.64.3.62
 

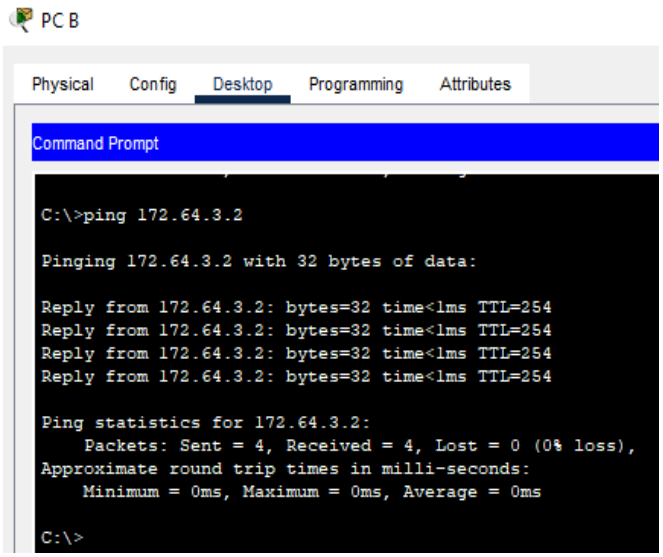
Fuente: Elaboración propia
Se establece un ping desde el PC-A (Host origen) dirigido a R1 a la interfaz G0/0/1, (Host</td></tr>
</table>

			destino) con dirección IP 172.64.3.62. El pin es exitoso pues el host de destino es accesible desde otro host, en este caso PC-A (Host origen).
	S1 VLAN 1	**172.64.3.2**	**Exitoso.** Figura 6-Ping 172.64.3.2  Fuente: Elaboración propia Se establece un ping desde el PC-A dirigido a S1 a la VLAN1, con la dirección IP 172.64.3.2. El ping es exitoso ya que el paquete de 32 bytes que es enviado por el PC-A, es recibido con respuesta exitosa desde el host de destino, y no hay pérdida de ninguno de estos.
	PC-B	**172.64.3.75**	**Exitoso** Figura 7-Ping 175.64.3.75  Fuente: Elaboración propia Se establece un ping desde el PC-A dirigido a PC-B, con la dirección IP 172.64.3.75. Ping

<table>
<tr><td></td><td></td><td></td><td>exitoso ya que los cuatro paquetes que han sido enviados por PC-A (Host origen) tienen una contestación exitosa de parte del host de destino, no hay pérdida de paquetes.</td></tr>
<tr><td rowspan="2">PC-B</td><td>R1
G0/0/0</td><td>172.64.3.94</td><td>Exitoso
Figura 8-Ping 172.64.3.94
 

Fuente: Elaboración propia
Se establece un ping desde el PC-B dirigido a R1, a la interfaz G0/0/0, con la dirección IP 172.64.3.94. Se evidencia un ping exitoso ya que el host de origen envía y recibe exitosamente paquetes, esto como respuesta de acceso al host de destino.</td></tr>
<tr><td>R1
G0/0/1</td><td>172.64.3.62</td><td>Exitoso
Figura 9-Ping 172.64.3.62
 

Fuente: Elaboración propia
Se establece un ping desde el PC-B dirigido a R1, a la interfaz G0/0/1, con la dirección IP</td></tr>
</table>

<table>
<tr><td rowspan="2"></td><td></td><td></td><td>172.64.3.62. El ping es exitoso ya que el PC-B como host de origen envía paquetes hacia la dirección ip indicada, el host destino responde a la de manera exitosa respondiendo y reenviando respuesta.</td></tr>
<tr><td>S1 VLAN 1</td><td>172.64.3.2</td><td>Exitoso
Figura 10-Ping 172.64.3.2
 

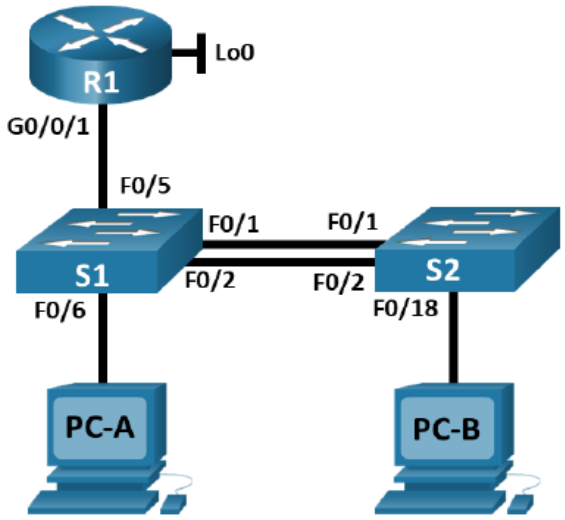
Fuente: Elaboración propia
Se establece un ping desde el PC-B dirigido a S1, a la VLAN1, con la dirección IP 172.64.3.2. El ping es exitoso ya que se envía un paquete de solicitud de eco a la dirección indicada y el host remoto al recibir la solicitud de eco, responde con un paquete de respuesta de eco.</td></tr>
</table>

Fuente: Elaboración propia

2. ESCENARIO 2

Topología

Figura 11-Topología escenario 2



Fuente: Prueba de habilidades ccna ii-2022

En este escenario de configuran dispositivos en una red pequeña, conformada por un Router, dos switch y dos equipos. Se admitirá tanto la conectividad IPV4 como IPV6 para los hosts soportados.

Tabla de VLAN

Tabla 10 - Tabla de VLAN

VLAN	Nombre de la VLAN
20	Docentes
30	Estudiantes
40	Invitados
50	Usuarios
56	Native

Fuente: Elaboración propia

Tabla de asignación de direcciones

Tabla 11-Tabla de asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.20	10.**64**.8.1 /26	No corresponde
R1 G0/0/1.2	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.30	10.**64**.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.40	10.**64**.8.97 /29	No corresponde
R1 G0/0/1.4	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
R1 Loopback0	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 40	10.**64**.8.98 /29	10.64.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 40	10.**64**.8.99 /29	10.64.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4 2001:db8:acad:a: :50 /64	DHCP para puerta de enlace predeterminada IPv4 fe80::1
PC-B NIC	DHCP para dirección IPv4 2001:db8:acad:b: :50 /64	DHCP para puerta de enlace predeterminada IPv4 fe80::1

Fuente: Elaboración propia.

Nota: No hay ninguna interfaz en el router que admita VLAN 50.

Parte 1. Se inicia construyendo la red, configurando los aspectos básicos de cada dispositivo.

Paso1. Contrucción de la red.

- Se borra las configuraciones de inicio y las VLAN del router y del switch y se vuelven a cargar los dispositivos.

Se ingresa el siguiente comando para borrar las configuraciones de inicio y cargue de los dispositivos:

Enable	Ingreso a modo privilegiado
Erase startup-config	Borrado de configuración
Delete flash:vlans.dat	Borrado de las VLAN
Reload.	Recargamos los dispositivos

- Después de recargar el switch, se configura la plantilla SDM para que admita IPv6 según sea necesario y vuelve a cargar el switch.

Se configura configura la plantilla SDM para que admita IPv6 en los dos switch, ingresando el siguiente comando:

Switch(config)#
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Changes to the running SDM preferences have been stored, but cannot take effect until the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
Switch(config)#
Switch(config)#exit
Switch#reload

Se accede al modo privilegiado del Switch, luego dentro de la configuración del terminal se ejecuta el comando **sdm prefer dual-ipv4-and-ipv6 default,** así se admite IPv4 e IPv6 en el dispositivo.

Paso 2. Configurar R1

La configuración para R1 incluye:

CONFIGURACION R1

1. Se desactivan las búsquedas **DNS,** para ello realizamos lo siguiente:

Router>	Se accede al router
Router>enable	Ingreso al modo privilegiado
Router#configure terminal	Ingreso a modo de configuración
Router(config)#no ip domain-lookup	Desactivación de búsqueda DNS
Router(config)#	

2. Se establece un nombre al Router, mediante el comando Hostname llamarlo como **R1.**

Router>enable	Ingreso al modo privilegiado
Router#configure terminal	Ingreso a modo de configuración
Router(config)#hostname R1	Configuración nombre del router
R1(config)#	

3. Se añade un nombre de dominio el cual se llamará **ccna-sa.com.**

R1>enable	Ingreso a modo privilegiado
R1#configure terminal	Ingreso a modo de configuración
R1(config)#ip domain name ccna-sa.com	Nombre de dominio
R1(config)#	

4. Se configura una contraseña cifrada para el modo EXEC privilegiado: **class.**

R1>enable	Ingreso a modo privilegiado
R1#configure terminal	Ingreso a modo de configuración
R1(config)#enable secret class	**C**ontraseña cifrada modo EXEC
R1(config)#	

5. Se configura una contraseña de acceso a la consola, para ello se utilizará la siguiente: **cisco**

R1#configure terminal	Ingreso a modo de configuración
R1(config)#line console 0	Se selecciona consola
R1(config-line)# pass	
R1(config-line)# password cisco	Ingreso de contraseña.
R1(config-line)#login	Se solicita el comando loguin para pedir la contraseña.

6. Se establece una longitud mínima para las contraseñas de 5 **caracteres:**

R1#configure terminal Ingreso al modo de configuración
R1(config)#security pass
R1(config)#security passwords min-length 5
R1(config)#

Se habilita el comando para la longitud mínima para las contraseñas con passwords min-length.

7. Se crea un usuario administrativo en la base de datos local con los siguientes requerimientos:

- **Nombre de usuario: admin**
- **Contraseña: admin1pass**

R1#configure terminal Ingreso a modo de configuración
R1(config)#username admin secret admin1pass
R1(config)#

Se configura el nombre del usuario administrativo con su contraseña, utilizando el comando username admin secret.

8. Se configura el inicio de sesión en las líneas VTY para usar la base de datos local

R1#
R1#configure terminal Ingreso a modo de configuración
R1(config)# line vty 0 4 Ingreso a la línea vty 0 4
R1(config-line)#login local Habilitado de login en las líneas VTY
R1(config-line)#

9. Se configuran las líneas VTY para que acepten conexiones SSH únicamente.

R1(config-line)# Ingreso de configuración de líneas
R1(config-line)#transport input ssh Conexión solo por ssh
R1(config-line)#

10. Se procede a cifrar las contraseñas de texto no cifrado, de la siguiente forma:

R1(config)# Ingreso a modo de configuración
R1(config)#service pass
R1(config)#service password-encryption Se cifran las contraseñas
R1(config)#

11. Se configura un banner MOTD, donde se visualiza el nombre del dispositivo, el nombre completo de quien configura y el programa académico al que pertenece.

R1(config)#banner motd #
Enter TEXT message. End with the character '#'.
R1 - CRISTIAN ESNEIDER MUNOZ NANEZ - INGENIERIA DE SISTEMAS
#
R1(config)#EXIT

Se ingresó dentro de la configuración del terminal el comando banner motd, el cual ayuda a ejecutar el mensaje banner.

12. Se procede a habilitar el routing IPv6.

R1(config)# Ingreso al modo de configuración
R1(config)#ipv6 unicast-routing Habilitado routing IPv6
R1(config)#exit Salida de modo configuración
R1#wr Guardado de la configuración

13. Se realiza la configuración de la interface G0/0/1, estableciendo:

La descripción, dirección IPv4,
La dirección local de enlace IPv6 como fe80::1,
Se establece la dirección IPv6,
Y por último la activación de la interfaz

IPV4

R1(config)#	Ingreso al modo de configuración
R1(config)#int g0/0/1.20	Ingreso a la interfaz g0/0/1.20
R1(config-subif)#encapsulation dot1q 20	Encapsulamiento
R1(config-subif)#ip add 10.64.8.1 255.255.255.192	Ingreso de la IP
R1(config-subif)#no shut	Activación de interfaz
R1(config-subif)#exit	
R1(config)#int g0/0/1.30	Ingreso a la interfaz g0/0/1.30
R1(config-subif)#encapsulation dot1q 30	Encapsulamiento
R1(config-subif)#ip add 10.64.8.65 255.255.255.224	Ingreso de la IP
R1(config-subif)#no shut	Activación de interfaz
R1(config-subif)#exit	
R1(config)#int g0/0/1.40	Ingreso a la interfaz g0/0/1.40
R1(config-subif)#encapsulation dot1q 40	Encapsulamiento
R1(config-subif)#ip add 10.64.8.97 255.255.255.248	Ingreso de la IP
R1(config-subif)#no shut	Activación de interfaz
R1(config-subif)#exit	
R1(config)#int g0/0/1.56	Ingreso a la interfaz g0/0/1.56
R1(config-subif)#no shut	Activación de interfaz
R1(config-subif)#exit	
R1(config)#int g0/0/1	Ingreso a la interfaz g0/0/1
R1(config-if)#no shut	Activación de interfaz
R1(config-if)#	

IPV6

R1#(config)#	Ingreso al modo de configuración
R1(config)#int g0/0/1.20	Ingreso a la interfaz g0/0/1.20
R1(config-subif)#ipv6 add fe80::1 link-local	Dirección local de enlace
R1(config-subif)#ipv6 add 2001:db8:acad:a::1/64	Ingreso de dirección IP
R1(config-subif)#exit	
R1(config)#int g0/0/1.30	Ingreso a la interfaz g0/0/1.20
R1(config-subif)#ipv6 add fe80::1 link-local	Dirección local de enlace
R1(config-subif)#ipv6 add 2001:db8:acad:b::1/64	Ingreso de dirección IP
R1(config-subif)#exit	
R1(config)#int g0/0/1.40	Ingreso a la interfaz g0/0/1.20
R1(config-subif)#ipv6 add fe80::1 link-local	Dirección local de enlace
R1(config-subif)#ipv6 add 2001:db8:acad:c::1/64	Ingreso de dirección IP
R1(config-subif)#exit	
R1(config)#	

14. Se configura el Loopback0 interface, estableciendo:

La descripción, dirección IPv4,
Se establece la dirección IPv6,
La dirección local de enlace IPv6 como fe80: :1

R1(config)# Ingreso al modo de configuración
R1(config)#int loopback0 Ingreso a loopback0
R1(config-if)#

%LINK-5-CHANGED: Interface Loopback0, changed state to up

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

R1(config-if)#no shut Activación de interfaz
R1(config-if)#ip add 209.165.201.1 255.255.255.224 Ingreso de dirección IPv4
R1(config-if)#ipv6 add fe80::1 link-local Dirección local de enlace
R1(config-if)#ipv6 add 2001:db8:acad:209::1/64 Ingreso de dirección IPv6
R1(config-if)#exit
R1(config)#

15. Se genera una clave de cifrado RSA: **Módulo de 1024 bits**

R1(config)#
R1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.ccna-sa.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
***Mar 1 1:45:27.100: %SSH-5-ENABLED: SSH 1.99 has been enabled**
R1(config)#

Se genera la clave de cifrado ingresando al módulo de configuración, y con la configuración: crypto key generate rsa general-keys modulus 1024.

Paso 3. Configurar S1 y S2.

La configuración de los dos Switch, incluye:

CONFIGURACION S1 Y S2

1. Se desactiva la búsqueda **DNS,** ejecutando el siguiendo comando para los dos switches:

Switch>	
Switch>enable	Ingreso a modo privilegiado
Switch#configure terminal	Ingreso a modo de configuración
Switch(config)#no ip domain-lookup	Desactivo la búsqueda DNS
Switch(config)#	

2. Se configura un nombre al switch, en este caso es: **S1 y S2.**

Switch>enable	Ingreso a modo privilegiado
Switch#configure terminal	Ingreso a modo de configuración
Switch(config)#hostname S1	Configuración nombre del switch1
S1(config)#	

Switch>enable	Ingreso a modo privilegiado
Switch#configure terminal	Ingreso a modo de configuración
Switch(config)#hostname S2	Configuración nombre del switch2
S2(config)#	

3. Se le da un nombre de dominio, llamado en este caso **ccna-sa.com** para los dos switches.

S1>enable	Ingreso a modo privilegiado
S1#configure terminal	Ingreso a modo de configuración
S1(config)#ip domain name ccna-sa.com	Nombre del dominio en switch 1
S1(config)#	

S2>enable	Ingreso a modo privilegiado
S2#configure terminal	Ingreso a modo de configuración
S2(config)#ip domain name ccna-sa.com	Nombre del dominio en switch 2
S2(config)#	

4. Se establece la contraseña cifrada para el modo EXEC privilegiado: **class.**

S1>enable	Ingreso a modo privilegiado
S1#configure terminal	Ingreso a modo de configuración
S1(config)#enable secret class	Contraseña cifrada modo
S1(config)#	

S2>enable Ingreso a modo privilegiado
S2#configure terminal Ingreso a modo de configuración
S2(config)#enable secret class Contraseña cifrada modo
S2(config)#

5. Se configura la contraseña de acceso a la consola: **cisco**

S1(config)# Ingreso a modo de configuración
S1(config)#line console 0 Se selecciona la consola
S1(config-line)#password cisco Ingresamos contraseña
S1(config-line)#login Comando login

S2(config)# Ingreso a modo de configuración
S2(config)#line console 0 Se selecciona la consola
S2(config-line)#password cisco Ingresamos contraseña
S2(config-line)#login Comando login para habilitar la contraseña

6. Se crea un usuario administrativo en la base de datos local, con los siguientes requerimientos:

Nombre de usuario: admin
Contraseña: admin1pass

S1#configure terminal Ingreso a modo de configuración
S1(config)#username admin secret admin1pass
S1(config)#

S2#configure terminal Ingreso a modo de configuración
S2(config)#username admin secret admin1pass
S2(config)#

Se configura un usuario administrativo con su contraseña para el Switch 1 y 2.

7. Se configura el inicio de sesión en las líneas VTY para que use la base de datos local

S1(config)# Ingreso al modo configuración
S1(config)#line vty 0 4 Ingreso a la línea vty 04
S1(config-line)#login local Habilitado de login en las líneas VTY
S1(config-line)#

S2(config)# Ingreso al modo configuración
S2(config)#line vty 0 4 Ingreso a la línea vty 04
S2(config-line)#login local Habilitado de login en las líneas VTY

S2(config-line)#

8. Se configura las líneas VTY para que acepten solamente las conexiones SSH

S1(config)#	Ingreso al modo configuración
S1(config)#line vty 0 4	Ingreso a la línea vty 04
S1(config-line)#transport input ssh	Conexión solo por ssh

S2(config)#	Ingreso al modo configuración
S2(config)#line vty 0 4	Ingreso a la línea vty 04
S2(config-line)#transport input ssh	Conexión solo por ssh

9. Se cifran las contraseñas de texto no cifrado

S1(config)#	Ingreso al modo configuración
S1(config)#service password-encryption	Cifrado de contraseñas

S2(config)#	Ingreso al modo configuración
S2(config)#service password-encryption	Cifrado de contraseñas

10. Se procede a configurar un banner **MOTD,** donde se observa el nombre del dispositivo, el nombre completo de quien configura y el programa académico, así:

S1(config)#banner mot
S1(config)#banner motd #
Enter TEXT message. End with the character '#'.
S1 - CRISTIAN ESNEIDER MUNOZ NANEZ - INGENIERIA DE SISTEMAS
#
S1(config)#exit

S2(config)#banner mot
S2(config)#banner motd #
Enter TEXT message. End with the character '#'.
S2 - CRISTIAN ESNEIDER MUNOZ NANEZ - INGENIERIA DE SISTEMAS
#
S2(config)#exit

Se configura el banner motd con lo requerido para el switch 1 y 2.

11. Se genera una clave de cifrado RSA; Módulo de 1024 bits

S1(config)#
S1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: S1.ccna-sa.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
***Mar 1 5:21:39.107: %SSH-5-ENABLED: SSH 1.99 has been enabled**

S2(config)#
S2(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: S2.ccna-sa.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
***Mar 1 5:21:39.107: %SSH-5-ENABLED: SSH 1.99 has been enabled**

Se ingreso al modo configuración, realizando el cifrado RSA, módulo 1024 bits para el switch 1 y 2.

12. Se configura la interfaz de administración (SVI) donde se establece:

La dirección IPv4 de capa 3

La dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2

Establecer la dirección IPv6 de capa 3

S1(config)#	Ingreso a modo configuración
S1(config)#interface vlan 40	Ingreso a la interfaz vlan 40
S1(config-if)#ip address 10.64.8.98 255.255.255.248	Se asigna la IP.
S1(config-if)#ipv6 address fe80::98 link-local	Se establece el link-local
S1(config-if)#ipv6 add 2001:db8:acad:c::98/64	Se asigna la dirección IPv6
S1(config-if)#no shutdown	Se enciende la interfaz.
S1(config-if)#exit	

S2(config)#	Ingreso a modo configuración
S2(config)#interface vlan 40	Ingreso a la interfaz vlan 40
S2(config-if)#ip address 10.64.8.99 255.255.255.248	Se asigna la IP.
S2(config-if)#ipv6 address fe80::99 link-local	Se establece el link-local
S2(config-if)#ipv6 add 2001:db8:acad:c::99/64	Se asigna la dirección IPv6

S2(config-if)#no shutdown	Se enciende la interfaz.
S2(config-if)#exit	

13. Se configura el gateway predeterminado, puerta de enlace predeterminada como **10.64.8.97** para IPv4

S1(config)#	Ingreso al modo configuración
S1(config)#int vlan 40	**I**ngreso a la vlan 40
S1(config-if)#ip default-gateway 10.64.8.97	Se establece la puerta de enlace
S1(config)#exit	

S2(config)#	Ingreso al modo configuración
S2(config)#int vlan 40	**I**ngreso a la vlan 40
S2(config-if)#ip default-gateway 10.64.8.97	Se establece la puerta de enlace
S2(config)#exit	

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

Paso 4: Configuración de S1

1. Se crean las siguientes VLAN:

   VLAN 20, nombre Docentes; VLAN 30, nombre Estudiantes
   VLAN 40, nombre Invitados; VLAN 50, nombre Usuarios
   VLAN 56, nombre Native

S1(config)#	Ingreso al modo de configuración
S1(config)#vlan 20	Ingreso a la vlan 20
S1(config-vlan)#name Docentes	Se le asigna un nombre a la vlan 20
S1(config-vlan)#vlan 30	Ingreso a la vlan 20
S1(config-vlan)#name Estudiantes	Se le asigna un nombre a la vlan 30
S1(config-vlan)#vlan 40	Ingreso a la vlan 40
S1(config-vlan)#name Invitados	Se le asigna un nombre a la vlan 40
S1(config-vlan)#vlan 50	Ingreso a la vlan 50
S1(config-vlan)#name Usuarios	Se le asigna un nombre a la vlan 50
S1(config-vlan)#vlan 56	Ingreso a la vlan 56
S1(config-vlan)#name Native	Se le asigna un nombre a la vlan 56
S1(config-vlan)#exit	

2. Se procede a crear los troncos 802.1Q que utilicen la VLAN 56 nativa para las Interfaces F0/1, F0/2 y F0/5.

S1(config)# Ingreso al modo de configuración
S1(config)#interface fastEthernet 0/1 Acceso a la interfaz FastE. 0/1
S1(config-if)#switchport mode trunk Se habilita el modo trunk
S1(config-if)#switchport trunk native vlan 56
Se especifica una VLAN nativa para los enlaces troncales 802.1Q

S1(config)#interface fastEthernet 0/2 Acceso a la interfaz FastE. 0/2
S1(config-if)#switchport mode trunk Se habilita el modo trunk
S1(config-if)#switchport trunk native vlan 56
Se especifica una VLAN nativa para los enlaces troncales 802.1Q

S1(config)#interface fastEthernet 0/5 Acceso a la interfaz FastE. 0/5
S1(config-if)#switchport mode trunk Se habilita el modo trunk
S1(config-if)#switchport trunk native vlan 56
Se especifica una VLAN nativa para los enlaces troncales 802.1Q

3. Se crea un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2, usando el protocolo LACP para la negociación.

S1(config)#interface fastEthernet 0/1 Acceso a la interfaz FastE. 0/1
S1(config-if)#channel-protocol lacp Se utiliza el modo LACP
S1(config-if)#channel-group 1 mode active Se activa el canal channel-g
S1(config-if)#

S1(config)#interface fastEthernet 0/2 Acceso a la interfaz FastE. 0/2
S1(config-if)#channel-protocol lacp Se utiliza el modo LACP
S1(config-if)#channel-group 1 mode active Se activa el canal channel-g
S1(config-if)#

4. Se configura el puerto de acceso de host para VLAN 20, para la Interface F0/6, de la siguiente forma:

S1(config)# Ingreso al modo de configuración
S1(config)#interface fastEthernet 0/6 Se ingresa a la interfaz FastE. 0/6
S1(config-if)#switchport acces vlan 20 Se habilita el acceso por VLAN 20
S1(config-if)#switchport mode access Se activa el acceso
S1(config-if)#

5. Se configura la seguridad del puerto en los Access ports, permitiendo 4 direcciones MAC.

S1(config)#interface range fastEthernet 0/3-4 Se acceden a las interfaces
S1(config-if-range)#switchport port-security Se habilita la seguridad
Command rejected: FastEthernet0/3 is a dynamic port.
Command rejected: FastEthernet0/4 is a dynamic port.
S1(config-if-range)#switchport port-security maximum 4
Se permiten solo 4 direcciones MAC
S1(config)#interface range fastEthernet 0/7-24 Se acceden a las interfaces
S1(config-if-range)#switchport port-security Se habilita la seguridad
Command rejected: FastEthernet0/7 is a dynamic port.
Command rejected: FastEthernet0/8 is a dynamic port.
Command rejected: FastEthernet0/9 is a dynamic port.
Command rejected: FastEthernet0/10 is a dynamic port.
Command rejected: FastEthernet0/11 is a dynamic port.
Command rejected: FastEthernet0/12 is a dynamic port.
Command rejected: FastEthernet0/13 is a dynamic port.
Command rejected: FastEthernet0/14 is a dynamic port.
Command rejected: FastEthernet0/15 is a dynamic port.
Command rejected: FastEthernet0/16 is a dynamic port.
Command rejected: FastEthernet0/17 is a dynamic port.
Command rejected: FastEthernet0/18 is a dynamic port.
Command rejected: FastEthernet0/19 is a dynamic port.
Command rejected: FastEthernet0/20 is a dynamic port.
Command rejected: FastEthernet0/21 is a dynamic port.
Command rejected: FastEthernet0/22 is a dynamic port.
Command rejected: FastEthernet0/23 is a dynamic port.
Command rejected: FastEthernet0/24 is a dynamic port.
S1(config-if-range)#switchport port-security maxi
S1(config-if-range)#switchport port-security maximum 4
Se permiten solo 4 direcciones MAC

S1(config)#interface range gigabitEthernet 0/1-2 Se acceden a las interfaces
S1(config-if-range)#switchport port-security Se habilita la seguridad
Command rejected: GigabitEthernet0/1 is a dynamic port.
Command rejected: GigabitEthernet0/2 is a dynamic port.
S1(config-if-range)#switchport port-security maximum 4
Se permiten solo 4 direcciones MAC

6. Se procede a proteger todas las interfaces no utilizadas, asignándolas a VLAN 50, Estableciendo en modo de acceso, agregando una descripción y por último apagar.

S1(config)# Se accede al modo configuración
S1(config)#interface range FastEthernet 0/3-4 Se acceden a las interfaces
S1(config-if-range)#description DOWN-SECURITY Se agrega una descripción
S1(config-if-range)#switchport access vlan 50 Se asigna a la VLAN 50
S1(config-if-range)#switchport mode access Se activa el acceso
S1(config-if-range)#switchport port-security Se habilita la seguridad
S1(config-if-range)#switchport port-security maximum 4
Se permiten solo 4 direcciones MAC
S1(config-if-range)#shutdown Se apagan las interfaces

S1(config)# Se accede al modo configuración
S1(config)#interface range FastEthernet 0/7-24 Se acceden a las interfaces
S1(config-if-range)#description DOWN-SECURITY Se agrega una descripción
S1(config-if-range)#switchport access vlan 50 Se asigna a la VLAN 50
S1(config-if-range)#switchport mode access Se activa el acceso
S1(config-if-range)#switchport port-security Se habilita la seguridad
S1(config-if-range)#switchport port-security maximum 4
Se permiten solo 4 direcciones MAC
S1(config-if-range)#shutdown Se apagan las interfaces

S1(config)# Se accede al modo configuración
S1(config)#interface range gigabitEthernet 0/1-2 Se acceden a las interfaces
S1(config-if-range)#description DOWN-SECURITY Se agrega una descripción
S1(config-if-range)#switchport access vlan 50 Se asigna a la VLAN 50
S1(config-if-range)#switchport mode access Se activa el acceso
S1(config-if-range)#switchport port-security Se habilita la seguridad
S1(config-if-range)#switchport port-security maximum 4

Se permiten solo 4 direcciones MAC
S1(config-if-range)#shutdown Se apagan las interfaces

Paso 5: Configuración de S2.

1. Se crean las siguientes VLAN:
   VLAN 20, nombre Docentes; VLAN 30, nombre Estudiantes
   VLAN 40, nombre Invitados; VLAN 50, nombre Usuarios
   VLAN 56, nombre Native

S2(config)# Ingreso al modo de configuración
S2(config)#vlan 20 Ingreso a la vlan 20
S2(config-vlan)#name Docentes Se le asigna un nombre a la vlan 20
S2(config-vlan)#vlan 30 Ingreso a la vlan 30
S2(config-vlan)#name Estudiantes Se le asigna un nombre a la vlan 30
S2(config-vlan)#vlan 40 Ingreso a la vlan 40
S2(config-vlan)#name Invitados Se le asigna un nombre a la vlan 40
S2(config-vlan)#vlan 50 Ingreso a la vlan 50
S2(config-vlan)#name Usuarios Se le asigna un nombre a la vlan 50
S2(config-vlan)#vlan 56 Ingreso a la vlan 56
S2(config-vlan)#name Native Se le asigna un nombre a la vlan 56
S2(config-vlan)#exit

2. Se procede a crear los troncos 802.1Q que utilicen la VLAN 56 nativa para las Interfaces F0/1, F0/2.

S2(config)# Ingreso al modo de configuración
S2(config)#interface fastEthernet 0/1 Ingreso a la interfas FastE. 0/1
S2(config-if)#switchport mode trunk Se habilita en modo Trunk
S2(config-if)#switchport trunk native vlan 56

Se especifica una VLAN nativa para los enlaces troncales 802.1Q

S2(config)#interface fastEthernet 0/2 Ingreso a la interfas FastE. 0/2
S2(config-if)#switchport mode trunk Se habilita en modo Trunk
S2(config-if)#switchport trunk native vlan 56

Se especifica una VLAN nativa para los enlaces troncales 802.1Q

3. Se crea un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2, usando el protocolo LACP para la negociación.

S2(config)#interface fastEthernet 0/1 Ingreso a la interfaz FastE. 0/1
S2(config-if)#channel-protocol lacp Se activa el protocolo LACP
S2(config-if)#channel-group 1 mode passive Se activa el canal channel-g
S2(config-if)#

S2(config)#interface fastEthernet 0/2 Ingreso a la interfaz FastE. 0/1
S2(config-if)#channel-protocol lacp Se activa el protocolo LACP
S2(config-if)#channel-group 1 mode passive Se activa el canal channel-g
S2(config-if)#

4. Se configura el puerto de acceso de host para VLAN 30, para la Interface F0/18, de la siguiente forma:

S2(config)# Ingreso al modo de configuración
S2(config)#interface fastEthernet 0/18 Acceso a la interfaz FastE. 0/18
S2(config-if)#switchport acces vlan 30 Se activa el acceso a la Vlan 30
S2(config-if)#switchport mode access Se habilita el modo de acceso
S2(config-if)#

5. Se configura la seguridad del puerto en los Access ports, permitiendo 4 direcciones MAC.

S2(config)# Ingreso al modo de configuración
S2(config)#interface range fastEthernet 0/3-24 Ingreso a las interfaces
S2(config-if-range)#switchport port-security Se activa la seguridad
Command rejected: FastEthernet0/3 is a dynamic port.
Command rejected: FastEthernet0/4 is a dynamic port.
Command rejected: FastEthernet0/5 is a dynamic port.
Command rejected: FastEthernet0/6 is a dynamic port.
Command rejected: FastEthernet0/7 is a dynamic port.
Command rejected: FastEthernet0/8 is a dynamic port.
Command rejected: FastEthernet0/9 is a dynamic port.

Command rejected: FastEthernet0/10 is a dynamic port.
Command rejected: FastEthernet0/11 is a dynamic port.
Command rejected: FastEthernet0/12 is a dynamic port.
Command rejected: FastEthernet0/13 is a dynamic port.
Command rejected: FastEthernet0/14 is a dynamic port.
Command rejected: FastEthernet0/15 is a dynamic port.
Command rejected: FastEthernet0/16 is a dynamic port.
Command rejected: FastEthernet0/17 is a dynamic port.
Command rejected: FastEthernet0/19 is a dynamic port.
Command rejected: FastEthernet0/20 is a dynamic port.
Command rejected: FastEthernet0/21 is a dynamic port.
Command rejected: FastEthernet0/22 is a dynamic port.
Command rejected: FastEthernet0/23 is a dynamic port.
Command rejected: FastEthernet0/24 is a dynamic port.
S2(config-if-range)#switchport port-security maximum 4
Se permiten solo 4 direcciones MAC
S2(config-if-range)#
S2(config)#interface range gigabitEthernet 0/1-2 Ingreso a las interfaces
S2(config-if-range)#switchport port-security Se activa la seguridad
Command rejected: GigabitEthernet0/1 is a dynamic port.
Command rejected: GigabitEthernet0/2 is a dynamic port.
S2(config-if-range)#switchport port-security maximum 4
Se permiten solo 4 direcciones MAC
S2(config-if-range)#

6. Se procede a proteger todas las interfaces no utilizadas, asignándolas a VLAN 50, Estableciendo en modo de acceso, agregando una descripción y por último apagar.

S2(config)# Ingreso al modo configuración
S2(config)#interface range FastEthernet 0/3-17 Ingreso a las interfaces
S2(config-if-range)#description DOWN-SECURITY Una descripción
S2(config-if-range)#switchport access vlan 50 Acceso a la VLAN 50
S2(config-if-range)#switchport mode access Se activa el acceso
S2(config-if-range)#switchport port-security Se habilita la seguridad
S2(config-if-range)#switchport port-security maximum 4
Se permiten solo 4 direcciones MAC
S2(config-if-range)#shutdown Se apagan las interfaces

S2(config)# Ingreso al modo configuración
S2(config)#interface range FastEthernet 0/19-24 Ingreso a las interfaces
S2(config-if-range)#description DOWN-SECURITY Asigna una descripción
S2(config-if-range)#switchport access vlan 50 Acceso a la VLAN 50
S2(config-if-range)#switchport mode access Se activa el acceso
S2(config-if-range)#switchport port-security
S2(config-if-range)#switchport port-security maximum 4
Se permiten solo 4 direcciones MAC
S2(config-if-range)#shutdown Se apagan las interfaces

S2(config)# Ingreso al modo configuración
S2(config)#interface range gigabitEthernet 0/1-2 Ingreso a las interfaces
S2(config-if-range)#description DOWN-SECURITY Asigna una descripción
S2(config-if-range)#switchport access vlan 50 Acceso a la VLAN 50
S2(config-if-range)#switchport mode access Se activa el acceso
S2(config-if-range)#switchport port-security Se activa el acceso
S2(config-if-range)#switchport port-security maximum 4
Se permiten solo 4 direcciones MAC
S2(config-if-range)#shutdown Se apagan las interfaces

Parte 3: Configuración de soporte de host

Paso 1. Se configura el R1.

La configuración de R1, se incluyen los siguientes términos:

1. Se configura en Default Routing, creando rutas predeterminadas par IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0, para este caso serán las siguientes:

R1(config)# Ingreso a modo de configuración
R1(config)#ip route 0.0.0.0 0.0.0.0 Loopback 0 Ruta predeterminada Ipv4
R1(config)#ipv6 route ::/0 Loopback 0 Ruta predeterminada Ipv6
R1(config)#

2. Se configura IPv4 DHCP para la Vlan 20, creando un grupo DHCP para VLAN 20, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sa.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada.

R1#
R1#configure terminal Ingreso a modo de configuración
R1(config)#ip dhcp pool VLAN20 Se crea un grupo DHCP para VLAN20
R1(dhcp-config)#network 10.64.8.0 255.255.255.192 Se establece la IP
R1(dhcp-config)#default-router 10.64.8.1 Se establece la puerta de enlace
R1(dhcp-config)#domain-name unad-ccna-sa.net Nombre del dominio
R1(dhcp-config)#ip dhcp excluded-address 10.64.8.1 10.64.8.52
Se componen las últimads 10 direcciones IP de la subred.
R1(config)#
R1(config)#end
R1#

3. Se configura DHC IPv4 para la VLAN 30, creando un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sb.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada

R1#
R1#configure terminal Ingreso a modo de configuración
R1(config)#ip dhcp pool Vlan30 Se crea un grupo DHCP para VLAN30
R1(dhcp-config)#network 10.64.8.64 255.255.255.224 Se establece la IP
R1(dhcp-config)#default-router 10.64.8.65 Se establece la puerta de enlace
R1(dhcp-config)#domain-name unad-ccna-sb.net Nombre del dominio
R1(dhcp-config)#ip dhcp excluded-address 10.64.8.65 10.64.8.84
Se componen las últimads 10 direcciones IP de la subred.
R1(config)#end
R1#

Paso 2: Configuración de los servidores

Se configuran los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y se asignan estáticamente las direcciones IPv6 GUA y Link Local.

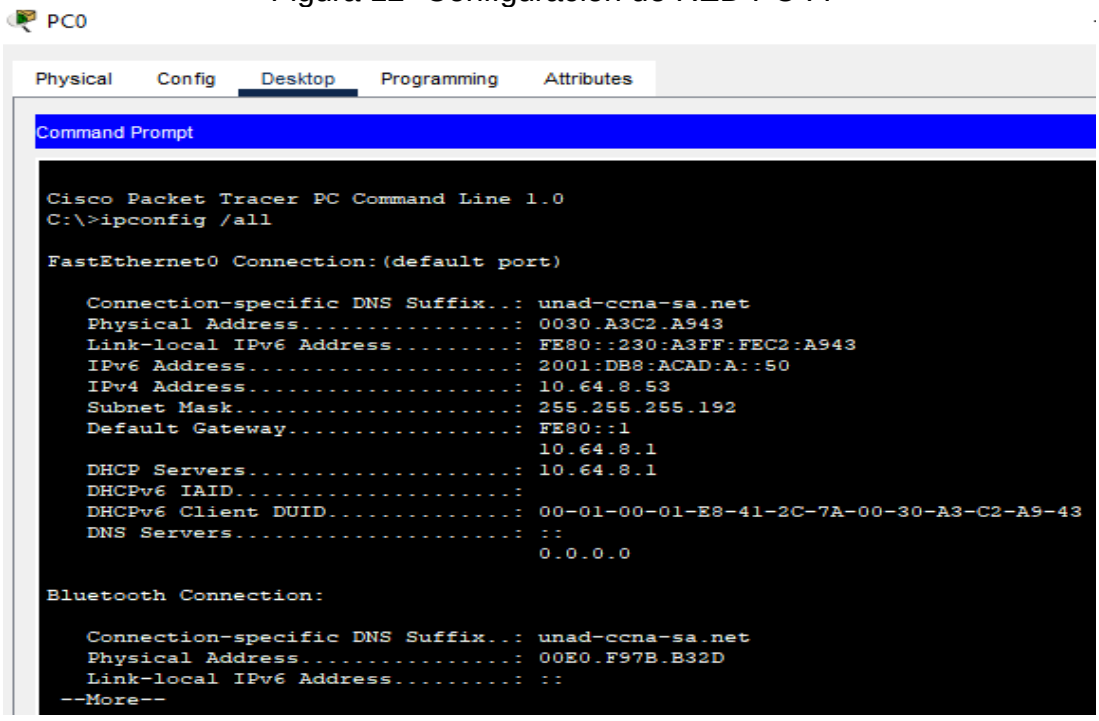
Después de configurar cada servidor, se registran las configuraciones de red del host con el comando ipconfig /all.

- **Configuración de red de PC-A**

  Descripción: FastEthernet0 Connection:(default port)
  Dirección Física: 0030.A3C2.A943
  Dirección IP: 10.64.8.53
  Máscara de subred: 255.255.255.192
  Gateway predeterminado: 10.64.8.1
  Gateway predeterminado IPv6: FE80::1

  PC-A Comando ipconfig/all:

Figura 12- Configuración de RED PC-A



Fuente: Elaboración propia

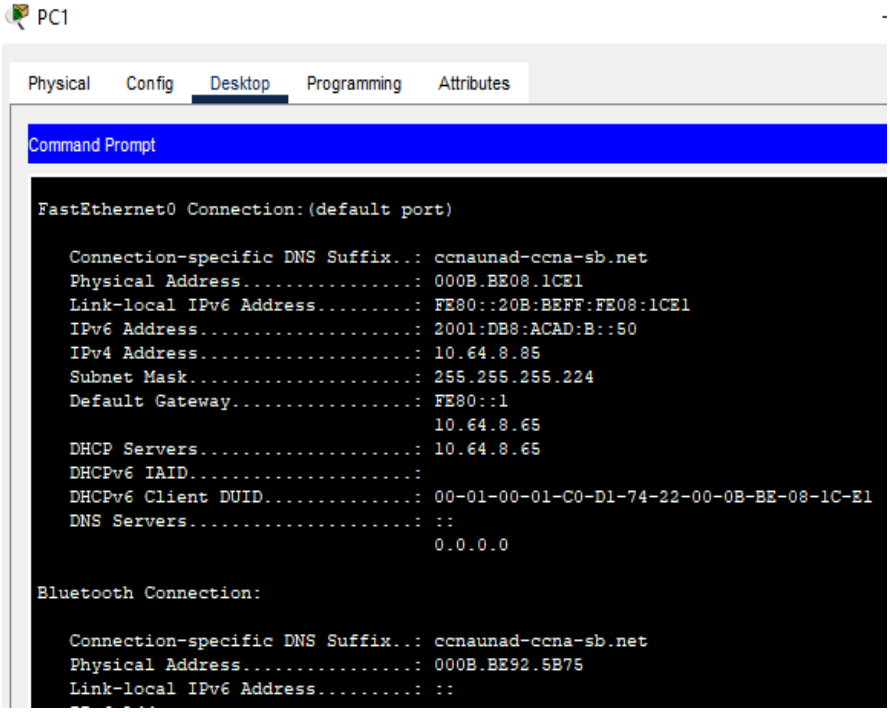
- **Configuración de red de PC-B**

  Descripción: FastEthernet0 Connection:(default port)

Dirección Física: 000B.BE08.1CE1
Dirección IP: 10.64.8.85
Máscara de subred: 255.255.255.224
Gateway predeterminado: 10.64.8.65
Gateway predeterminado IPv6: FE80::1

PC-B Comando ipconfig/all:

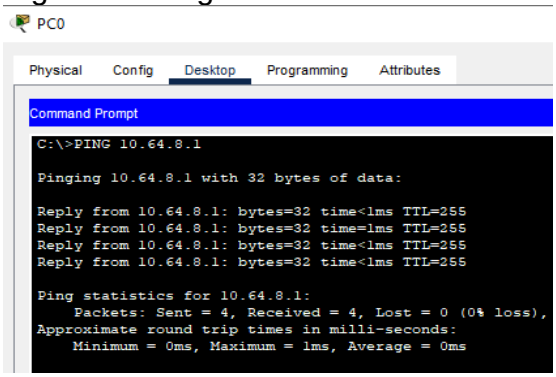
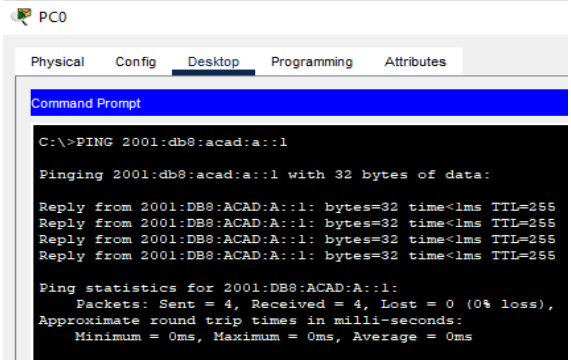
Figura 13-Configuración de RED PC-B

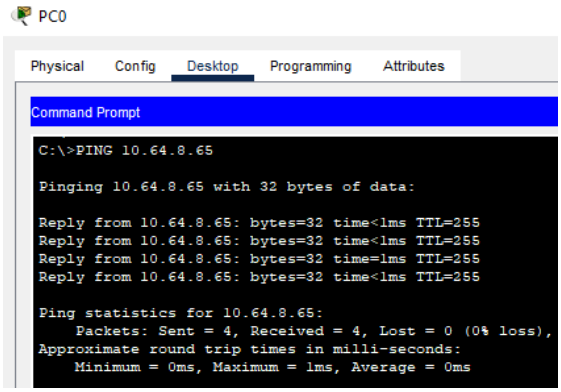


Fuente: Elaboración propia

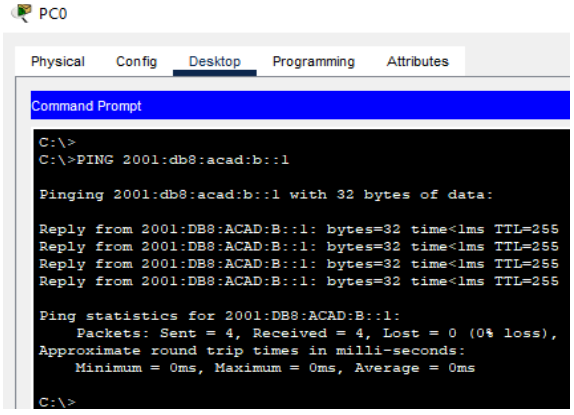
Parte 3: Verificación de la conectividad de extremo a extremo:

Se verifica usando el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

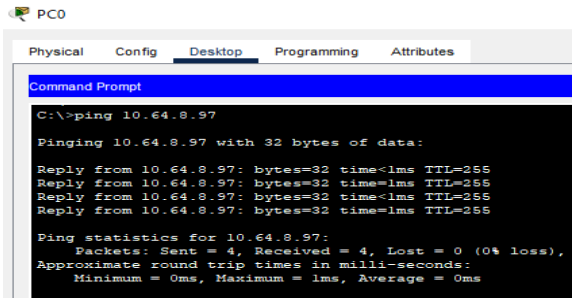
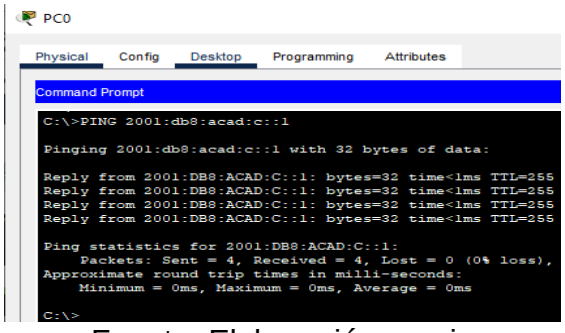
Desde	A	Dirección IP	Resultados de ping
PC-A (PC0)	R1, G0/0/1.20 R1, G0/0/1.2	10.**64**.8.1	**Exitoso.** Figura 14-Ping de PCA a IP 10.64.8.1  Fuente: Elaboración propia Se establece un ping desde el PC-A dirigido a R1, con la dirección IP 10.**64**.8.1, perteneciente a la interfaz G0/0/1.20. El ping es exitoso ya que se envía un paquete de solicitud de eco a la dirección indicada y el host remoto al recibir la solicitud de eco, responde con un paquete de respuesta de eco.
		2001:db8:acad:a::1	**Exitoso.** Figura 15-Ping de PCA a IPv6 2001:db8:acad:a::1  Fuente: Elaboración propia Se establece un ping desde el PC-A dirigido a R1, con la dirección IPv6 2001:db8:acad:a::1, perteneciente a la interfaz G0/0/1.20. Ping exitoso ya que los cuatro paquetes que han sido

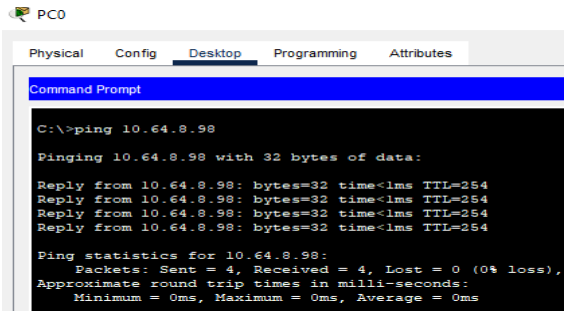
<table>
<tr><td></td><td></td><td></td><td>enviados por PC-A (Host origen) tienen una contestación exitosa de parte del host de destino, no hay pérdida de paquetes.</td></tr>
<tr><td rowspan="2"></td><td rowspan="2">R1, G0/0/1.30
R1, G0/0/1.3</td><td>10.64.8.65</td><td>Exitoso.
Figura 16-Ping de PCA a IP 10.64.8.65
 

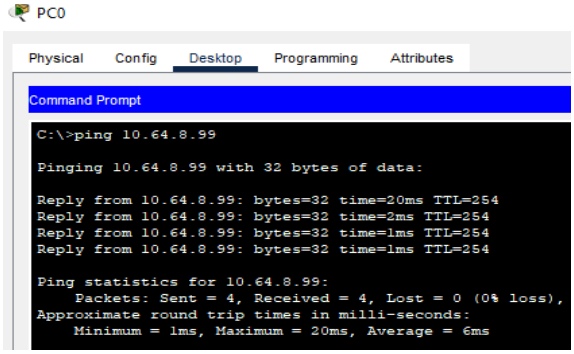
Fuente: Elaboración propia

Se establece un ping desde el PC-A dirigido a S1 a la R1, con la dirección IP 172.64.3.2, perteneciente a la interfaz G0/0/1.30. El ping es exitoso ya que el paquete de 32 bytes que es enviado por el PC-A, es recibido con respuesta exitosa desde el host de destino, y no hay pérdida de ninguno de estos.</td></tr>
<tr><td>2001:db8:acad:b::1</td><td>Exitoso.
Figura 17-Ping de PCA a IPv6 2001:db8:acad:b::1
 

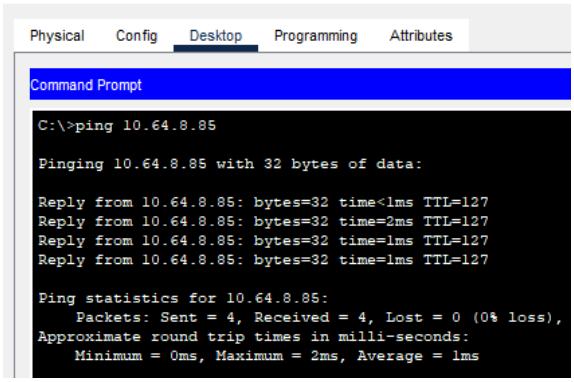
Fuente: Elaboración propia</td></tr>
</table>

			Se establece un ping desde el PC-A dirigido a R1, a la interfaz G0/0/1.30, con la dirección IPv6 2001:db8:acad:b::1. El ping es exitoso ya que el PC-A como host de origen envía paquetes hacia la dirección ip indicada, el host destino responde a la de manera exitosa respondiendo y reenviando respuesta.
	R1, G0/0/1.40 R1, G0/0/1.4	10.**64**.8.97	**Exitoso** Figura 18 - Ping de PCA a IP 10.64.8.97  Fuente: Elaboración propia Se establece un ping desde el PC-A dirigido a R1, con la dirección IP 10.64.8.97, perteneciente a la interfaz G0/0/1.40. El ping exitoso ya que los cuatro paquetes que han sido enviados por PC-A (Host origen) tienen una contestación exitosa de parte del host de destino, no hay pérdida de paquetes.
		2001:db8:acad:c::1	**Exitoso** Figura 19- Ping de PCA a IPv6 2001:db8:acad:c::1  Fuente: Elaboración propia Se establece un ping desde el PC-A dirigido a R1, con la dirección IPv6

			2001:db8:acad:c::1, perteneciente a la interfaz G0/0/1.40. El ping es exitoso ya que se envía un paquete de solicitud de eco a la dirección indicada y el host remoto al recibir la solicitud de eco, responde con un paquete de respuesta de eco.
	S1, VLAN 40 S1, VLAN 4	10.**64**.8.98	**Exitoso** Figura 20-Ping de PCA a IP10.64.8.98  Fuente: Elaboración propia Se establece un ping desde el PC-A dirigido a S1, con la dirección IP 10.64.8.98, perteneciente a la VLAN 40. El ping es exitoso ya que se envía un paquete de solicitud de eco a la dirección indicada y el host remoto al recibir la solicitud de eco, responde con un paquete de respuesta de eco.
		2001:db8:acad:c::98	El ping IPv6 no es Exitoso debido a una falla en el software Packet Tracer.
	S2, VLAN 40	10.**64**.8.99	**Exitoso**.

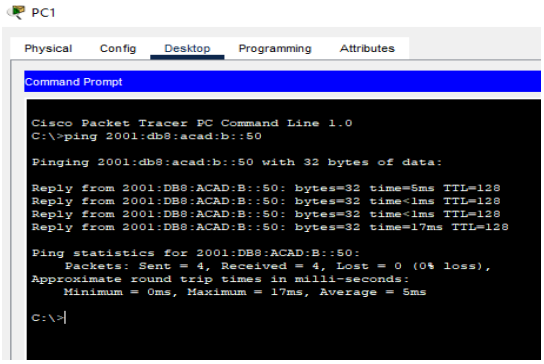
<table>
<tr><td></td><td></td><td></td><td>Figura 21-Ping de PCA a IP 10.64.8.99
 

Fuente: Elaboración propia

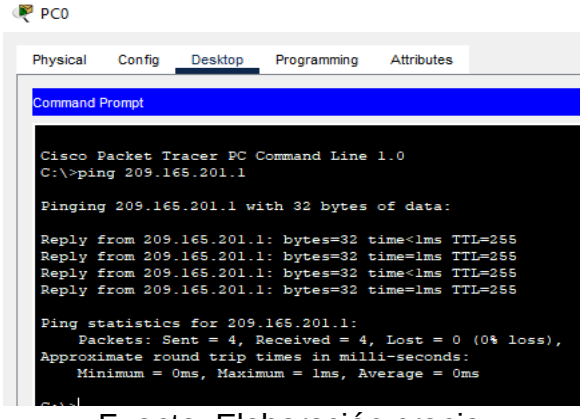
Se establece un ping desde el PC-A dirigido a S1, con la dirección IP 10.64.8.99, perteneciente a la VLAN 40. El ping es exitoso ya que se envía un paquete de solicitud de eco a la dirección indicada y el host remoto al recibir la solicitud de eco, responde con un paquete de respuesta de eco.</td></tr>
<tr><td></td><td></td><td>2001:db8:acad:c::99</td><td>El ping IPv6 no es Exitoso debido a una falla en el software Packet Tracer.</td></tr>
<tr><td></td><td>PC-B</td><td>IPv4-DHCP 10.64.8.85</td><td>Exitoso
Figura 22-Ping de PCA a IP 10.64.8.85
 

Fuente: Elaboración propia

Se establece un ping desde el PC-A dirigido a PC-B, con la dirección IP 10.64.8.97, perteneciente a la interfaz G0/0/1.40. El ping exitoso ya que los cuatro paquetes que han sido enviados por PC-A (Host origen) tienen una</td></tr>
</table>

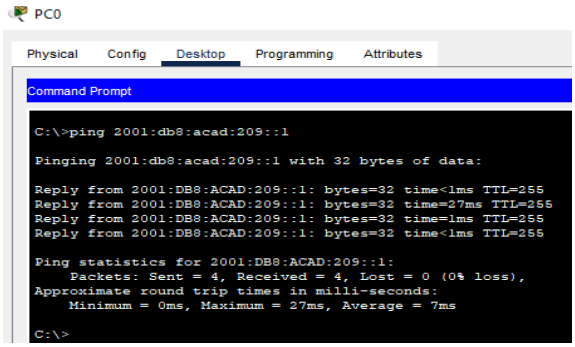
<table>
<tr><td></td><td></td><td></td><td>contestación exitosa de parte del host de destino, no hay pérdida de paquetes.</td></tr>
<tr><td></td><td></td><td>2001:db8:acad:b::50</td><td>Exitoso
Figura 23-Ping de PCA a IP 2001:db8:acad:b::50
 

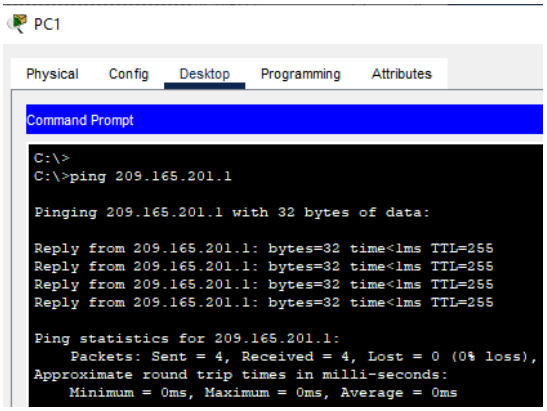
Fuente: Elaboración propia

Se establece un ping desde el PC-B dirigido a PC-B, con la dirección IPv6 2001:db8:acad:b::50. El ping exitoso ya que los cuatro paquetes que han sido enviados por PC-B (Host origen) tienen una contestación exitosa de parte del host de destino, no hay pérdida de paquetes.</td></tr>
<tr><td></td><td>R1 Bucle 0
R1 Bucle 0</td><td>209.165.201.1</td><td>Exitoso.
Figura 24-Ping de PCA a IP 209.165.201.1
 

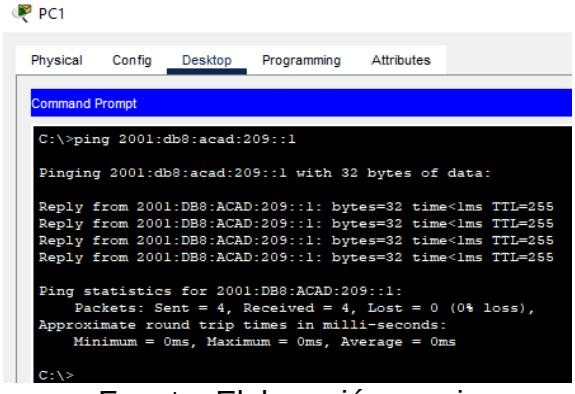
Fuente: Elaboración propia

Se establece un ping desde el PC-A dirigido a R1, con la dirección IP</td></tr>
</table>

			10.64.8.97, perteneciente a la interfaz G0/0/1.40. El ping exitoso ya que los cuatro paquetes que han sido enviados por PC-A (Host origen) tienen una contestación exitosa de parte del host de destino, no hay pérdida de paquetes.
		2001:db8:acad:209::1	**Exitoso.** Figura 25-Ping de PCA a IPv6 2001:db8:acad:209::1  Fuente: Elaboración propia Se establece un ping desde el PC-A dirigido a R1, con la dirección IPv6 2001:db8:acad:c::1, perteneciente a la interfaz G0/0/1.40. El ping es exitoso ya que se envía un paquete de solicitud de eco a la dirección indicada y el host remoto al recibir la solicitud de eco, responde con un paquete de respuesta de eco.
PC-B	R1 Bucle 0	209.165.201.1	**Exitoso.**

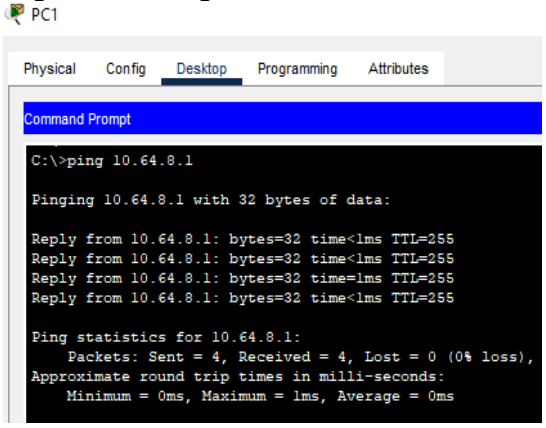
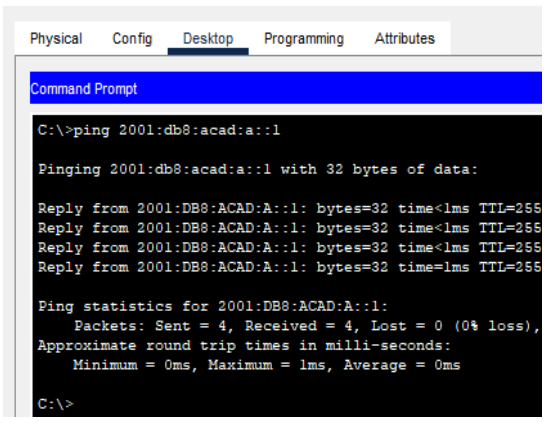
<table>
<tr><td rowspan="3">PC-B</td><td rowspan="2"></td><td>10.64.8.1</td><td>Figura 26-Ping de PCB a IP 209.165.201.1
 

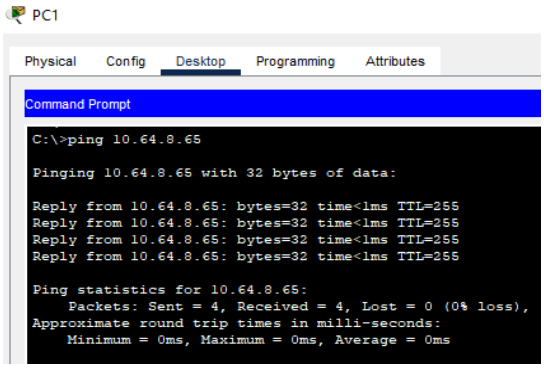
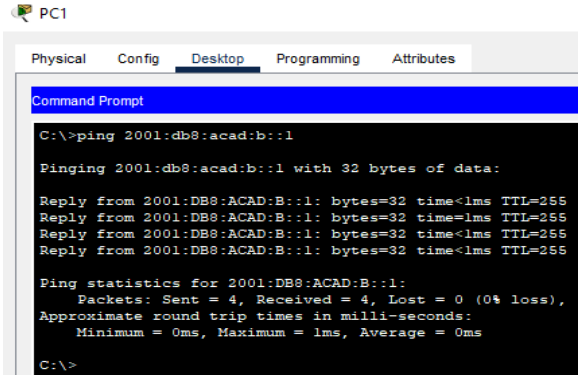
Fuente: Elaboración propia

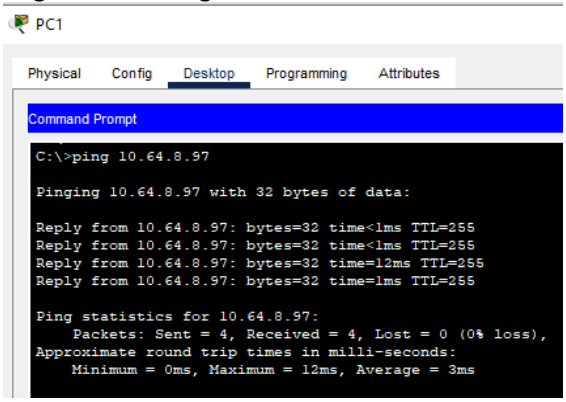
Se establece un ping desde el PC-B dirigido a R1, con la dirección IP 209.165.201.1. El ping exitoso ya que los cuatro paquetes que han sido enviados por PC-B (Host origen) tienen una contestación exitosa de parte del host de destino, no hay pérdida de paquetes.</td></tr>
<tr><td>2001:db8:acad:209::1</td><td>Exitoso.
Figura 27-Figura 28-Ping de PCB a IPv6 2001:db8:acad:209::1
 

Fuente: Elaboración propia

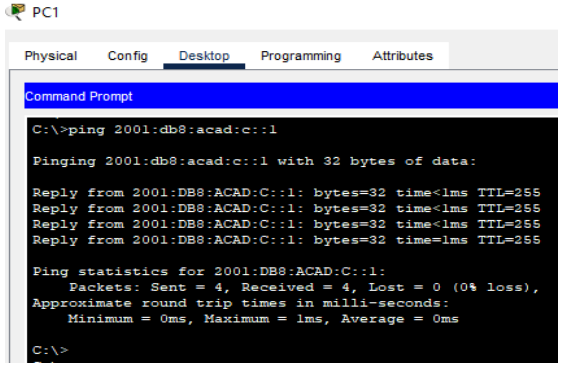
Se establece un ping desde el PC-B dirigido a R1, con la dirección IPv6 2001:db8:acad:209::1. El ping exitoso ya que los cuatro paquetes que han sido enviados y recibido de manera exitosa.</td></tr>
<tr><td></td><td>10.64.8.1</td><td>Exitoso.</td></tr>
</table>

	R1, G0/0/1.20 R1, G0/0/1.2		Figura 28-Ping de PCB a IP 10.64.8.1  Fuente: Elaboración propia. Se establece un ping desde el PC-B dirigido a R1, con la dirección IP 10.64.8.1, perteneciente a la interfaz G0/0/1.20. El ping exitoso ya que los cuatro paquetes que han sido enviados por PC-B tienen una respuesta exitosa de parte del host de destino, no hay pérdida de paquetes.
		2001:db8:acad:a::1	**Exitoso.** Figura 29-Ping de PCB a IPv6 2001:db8:acad:a::1  Fuente: Elaboración propia. Se establece un ping desde el PC-B dirigido a R1, con la dirección IPv6 2001:db8:acad:a::1, perteneciente a la interfaz G0/0/1.20. El ping exitoso ya que los cuatro paquetes que han sido

			enviados por PC-B tienen una respuesta exitosa de parte del host de destino.
	R1, G0/0/1.30 R1, G0/0/1.3	10.**64**.8.65	**Exitoso.** Figura 30-Ping de PCB a IP 10.64.8.65  Fuente: Elaboración propia Se establece un ping desde el PC-B dirigido a R1, con la dirección IP 10.64.8.65, perteneciente a la interfaz G0/0/1.30. El ping exitoso ya que los cuatro paquetes que han sido enviados por PC-B (Host origen) tienen una contestación exitosa de parte del host de destino, no hay pérdida de paquetes.
		2001:db8:acad:b::1	**Exitoso.** Figura 31-Ping de PCB a IPv6 2001:db8:acad:b::1  Fuente: Elaboración propia Se establece un ping desde el PC-B dirigido a R1, con la dirección IPv6

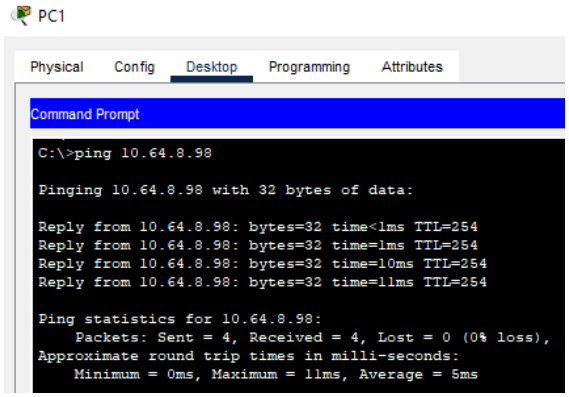
<table>
<tr><td></td><td></td><td></td><td>2001:db8:acad:b::1. El ping exitoso ya que los cuatro paquetes que han sido enviados y recibido de manera exitosa.</td></tr>
<tr><td rowspan="2"></td><td rowspan="2">R1, G0/0/1.40
R1, G0/0/1.4</td><td>10.64.8.97</td><td>Exitoso
Figura 32-Ping de PCB a IP 10.64.8.97
 

Fuente: Elaboración propia

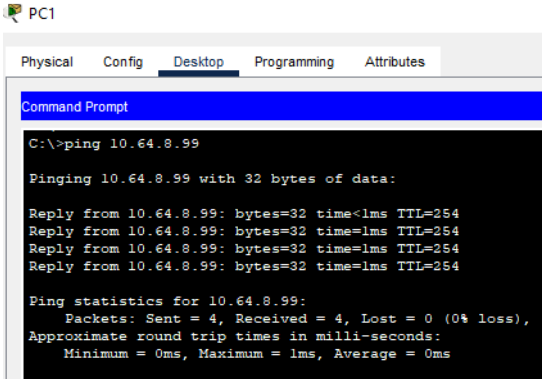
Se establece un ping desde el PC-B dirigido a R1, con la dirección IP 10.64.8.97, perteneciente a la interfaz G0/0/1.40. El ping exitoso ya que los cuatro paquetes que han sido enviados por PC-B tienen una contestación exitosa de parte del host de destino, no hay pérdida de paquetes.</td></tr>
<tr><td>2001:db8:acad:c::1</td><td>Exitoso.
Figura 33-Ping de PCB a IPv6 2001:db8:acad:c::1
 

Fuente: Elaboración propia

Se establece un ping desde el PC-B dirigido a R1, con la dirección IPv6 2001:db8:acad:c::1, perteneciente a la</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td>interfaz G0/0/1.40. El ping es exitoso ya que se envía un paquete de solicitud de eco a la dirección indicada y el host remoto al recibir la solicitud de eco, responde con un paquete de respuesta de eco.</td></tr>
<tr><td></td><td>S1, VLAN 40
S1, VLAN 4</td><td>10.64.8.98</td><td>Exitoso.
Figura 34-Ping de PCB a IP 10.64.8.98
 

Fuente: Elaboración propia

Se establece un ping desde el PC-B dirigido a S1, con la dirección IP 10.64.8.98. El ping exitoso ya que los cuatro paquetes que han sido enviados y recibido de manera exitosa.</td></tr>
<tr><td></td><td></td><td>2001:db8:acad:c::98</td><td>No hay ping a las VLAN 40 por IPV6 debido a una falla en el software.</td></tr>
<tr><td></td><td>S2, VLAN 40
S2, VLAN 4</td><td>10.64.8.99</td><td>Exitoso.
Figura 35-Ping de PCB a IP 10.64.8.99
 

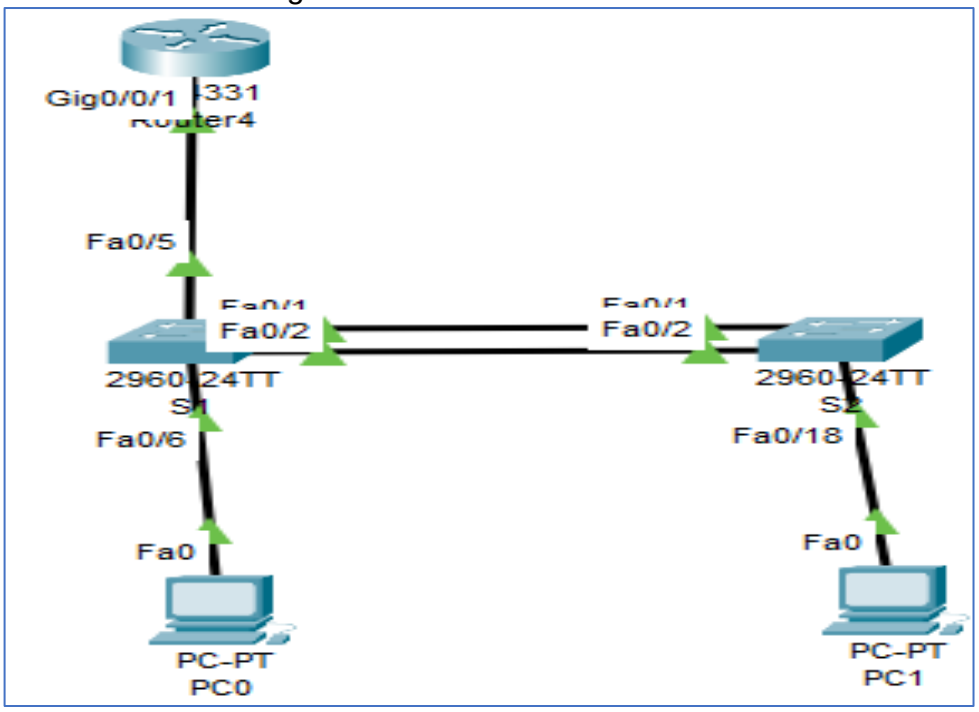
Fuente: Elaboración propia

Se establece un ping desde el PC-B dirigido a S1, con la dirección IP</td></tr>
</table>

			10.64.8.99, perteneciente a la VLAN 40. El ping exitoso ya que los cuatro paquetes que han sido enviados por PC-B (Host origen) tienen una contestación exitosa de parte del host de destino, no hay pérdida de paquetes.
		2001:db8:acad:c::99	No hay ping a las VLAN 40 por IPV6 debido a una falla en el software.

Fuente: Elaboración propia

Figura 36-Conexión Escenario 2



Fuente: Elaboración propia

CONCLUSIONES

Mediante el desarrollo de este trabajo, se realizaron los ajustes básicos de configuraciones para la conexión de una red LAN pequeña.

En el primer escenario se realizó el proceso de configuración de diversos dispositivos en una red pequeña conformada por un router, un switch y dos equipos de escritorio, el cual esboza un esquema de direccionamiento IPv4, dividido en dos redes LAN, se configuró la seguridad básica entre el Router y switch permitiendo entonces la interconexión entre los hosts conectados. Los switches son un elemento fundamental en el mundo de las redes, por lo que entender su funcionamiento es un requisito fundamental. El uso de los elementos tratados en este escenario es muy importante en las redes empresariales para lograr una escalabilidad, un rendimiento, una seguridad, una gestión mas adecuada y eficaz.

En el escenario 2 se simula la conectividad básica de redes mediante la configuración inicial de dispositivos de red y dispositivos finales que permitan la conexión IPv4 e IPv6 para los diferentes hosts presentados en la red. Se configuran el enrutamiento entre VLAN, DHCP. Se realiza la configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) configurando los puertos para el acceso de los hosts para las VLAN. La implementación adecuada de VTP garantiza que la administración de las VLAN en la red se simplifique al duplicar la configuración entre los conmutadores, lo que reduce los errores de administración y configuración.

Para finalizar podemos señalar que el material de apoyo que brinda el Diplomado de profundización cisco, es de gran ayuda pues influye a desarrollar las actitudes necesarias para planificar e implementar pequeñas redes con diversas aplicaciones.

BIBLIOGRAFIAS

BEMBIBRE, Victoria. Definición de Switch. Definición ABC {En línea}. (enero, 2009). {27/10/2022}. Obtenido de: https://www.definicionabc.com/tecnologia/switch.php

BARRIO DAVID, Fundamentos y Protocolos, Enrutamiento {En linea} (2020d, julio 10). {24/11/2022}, Obtenido de: https://eltallerdelbit.com/enrutamiento-fundamentos-y-protocolos/

ORTEGO DELGADO Daniel. ¿Qué es la Certificación Cisco CCNA?. OpenWebinars {En línea}. (27 de 08 de 2017). {27/10/2022} Obtenido de: https://openwebinars.net/blog/que-es-la-certificacion-cisco-ccna-200-125/

PEDROZA Scarlet. Host. Muy Tecnológicos. {En línea} (12 de 09 de 2021). {28/10/2022} Disponible en Muy Tecnológicos: https://muytecnologicos.com/diccionario-tecnologico/host

PEREZ PORTO, J., Merino, M. Definición de interfaz - Qué es, Significado y Concepto. {En línea} (3 de mayo de 2011). {23/11/2022} Definición.de. Recuperado el 23 de noviembre de 2022 de: https://definicion.de/interfaz/

PEREZ PORTO, J., Merino, M. Definición de router - Qué es, Significado y Concepto. {En línea} (15 de enero de 2010). {23/11/2022} Definicion.de. Recuperado el 23 de noviembre de 2022 de https://definicion.de/router/

PEREZ PORTO, J., Merino, M. Definición de conmutación - Qué es, Significado y Concepto.{En línea} (2 de diciembre de 2016). {23/11/2022} Disponible en: https://definicion.de/conmutacion/

VELAZQUEZ QUINTERO Jorge. Qué es Host. {En línea} (13 de 07 de 2021). {23/11/2022} Pág. 2. Obtenido de DocerArgentina: https://docer.com.ar/doc/xs1550x

ANEXO A

Descarga de archivos de simulación de los escenarios.

https://drive.google.com/drive/folders/1AqvNlig_IwNPRgSEeZslSiUp5eO9aPsl?usp=share_link