

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

ROBINSON ACOSTA VELASCO

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

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

ROBINSON ACOSTA VELASCO

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR EL TÍTULO
DE INGENIERO *DE SISTEMAS*

DIRECTOR:

PAULITA FLOR

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

NOTA DE ACEPTACION

Firma del presidente del jurado

Firma del jurado

Firma del jurado

VALLEDUPAR 28 DE NOVIEMBRE DE 2022

CONTENIDO

LISTA DE TABLAS	5
LISTA DE FIGURAS	6
GLOSARIO	8
RESUMEN.....	9
ABSTRACT.....	10
INTRODUCCIÓN.....	11
DESARROLLO ESCENARIOS.....	13
ESCENARIO 1.....	13
ESCENARIO 2.....	29
CONCLUSIONES	70
BIBLIOGRAFIA.....	71
ANEXOS.....	72

LISTA DE TABLAS

Tabla 1. Direccionamiento IP Escenario 1-----	13
Tabla 2. Configuración R1-----	15
Tabla 3. Configuración S1 -----	17
Tabla 4. Configuración PC-A -----	21
Tabla 5. Configuración PC-B -----	21
Tabla 6. Conexión entre dispositivos -----	22
Tabla 7. VLAN Escenario 2 -----	26
Tabla 8. Asignación de Direcciones IP Escenario 1 -----	27
Tabla 9. Configuración inicial R1 -----	28
Tabla 10. Configuración inicial S1 Y S2 -----	28
Tabla 11. Configuración R1 -----	29
Tabla 12. Configuración S1-----	33
Tabla 13. Configuración S2 -----	36
Tabla 14. Configuración de la infraestructura de red VLAN, Trunking, EtherChannel S1 -----	39
Tabla 15. Configuración de la infraestructura de red VLAN, Trunking, EtherChannel S2 -----	43
Tabla 16. Configurar soporte de host en R1 -----	46

LISTA DE FIGURAS

Figura 1. topología de red escenario 1 -----	13
Figura 2. Ping PC-A a R1 G0/0/0 -----	26
Figura 3. Ping PC-A a R1 G0/0/1 -----	26
Figura 4. Ping PC-A a S1 VLAN 1-----	27
Figura 5. Ping PC-A a PC-B -----	27
Figura 6. Ping PC-B a R1 G0/0/0 -----	28
Figura 7. Ping PC-B a R1 G0/0/1 -----	28
Figura 8. Ping PC-B a S1 VLAN1 -----	29
Figura 9. Topologia de red escenario 2 -----	30
Figura 10. Ping PC-A a R1, G0/0/1.20 IPV4 -----	56
Figura 11. Ping PC-A a R1, G0/0/1.20 IPV6 2001:db8:acad:a: :1 -----	57
Figura 12. Ping PC-A a R1, G0/0/1.30 IPV4 10.37.8.65 -----	57
Figura 13. Ping PC-A a R1, G0/0/1.30 IPV6 2001:db8:acad:b::1 -----	58
Figura 14. Ping PC-A a R1, G0/0/1.40 IPV4 10.37.8.97 -----	58
Figura 15. Ping PC-A a R1, G0/0/1.40 IPV6 2001:db8:acad:c: :1 -----	59
Figura 16. Ping PC-A a S1, VLAN 40 IPv4 10.37.8.98 -----	59
Figura 17. Ping PC-A a S1, VLAN 40 IPv6 2001:db8:acad:c: :98 -----	60
Figura 18. Ping PC-A a S2, VLAN 40 IPv4 10.37.8.99 -----	60
Figura 19. Ping PC-A a S2, VLAN 40 IPv6 2001:db8:acad:c: :99-----	61
Figura 20. Ping PC-A a PC-B IPv4 10.37.8.66 -----	61
Figura 21. Ping PC-A a PC-B IPv6 2001:db8:acad:b::50 -----	62
Figura 22. Ping PC-A a R1 Loopback0 IPv4 209.165.201.1 -----	62
Figura 23. Ping PC-A a R1 Loopback0 IPv6 2001:db8:acad:209::1-----	63
Figura 24. Ping PC-B a R1 Loopback0 IPv4 209.165.201.1 -----	63
Figura 25. Ping PC-B a R1 Loopback0 IPv6 2001:db8:acad:209::1 -----	64

Figura 26. Ping PC-B a R1, G0/0/1.20 IPv4 10.37.8.1 -----	64
Figura 27. Ping PC-B a R1, G0/0/1.20 IPv6 2001:db8:acad:a::1 -----	65
Figura 28. Ping PC-B a R1, G0/0/1.30 IPv4 10.37.8.65 -----	65
Figura 29. Ping PC-B a R1, G0/0/1.30 IPv6 2001:db8:acad:b::1-----	66
Figura 30. Ping PC-B a R1, G0/0/1.40 IPv4 10.37.8.97 -----	66
Figura 31. Ping PC-B a R1, G0/0/1.40 IPv6 2001:db8:acad:c::1 -----	67
Figura 32. Ping PC-B a S1, VLAN 40 IPv4 10.37.8.98 -----	67
Figura 33. Ping PC-B a S1, VLAN 40 IPv6 2001:db8:acad:c::98 -----	68
Figura 34. Ping PC-B a S2, VLAN 40 IPv4 10.37.8.99 -----	68
Figura 35. Ping PC-B a S2, VLAN 40 IPv6 2001:db8:acad:c::99 -----	69

GLOSARIO

BANNER MOTD: Es un comando que especifica el mensaje que se muestra como Mensaje del día, el primer mensaje que se muestra en una conexión entrante. Este comando define solo el mensaje; el comando motd - banner habilita o deshabilita la visualización.¹

DHCP: Significa protocolo de configuración de host dinámico y es un protocolo de red utilizado en redes IP donde un servidor DHCP asigna automáticamente una dirección IP y otra información a cada host en la red para que puedan comunicarse de manera eficiente con otros puntos finales. (Kerravala, 2018).²

GATEWAY: Es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.³

IPV6: Es la nueva versión del protocolo IP (Internet Protocol). Ha sido diseñado por el IETF (Internet Engineering Task Force) para reemplazar en forma gradual a la versión actual, el IPv4.⁴

LÍNEA DE TERMINAL VIRTUAL: En el Router, los puertos vty están enumerados del 0 al 15 y son utilizados para establecer sesiones Telnet. El comando a utilizar es line vty 0 15 así como los subcomandos password y login.⁵

VLAN: Pueden considerarse como dominios de difusión lógica. Una VLAN divide los grupos de usuarios de la red de una red física real en segmentos de redes lógicas.⁶

¹ ALVARO, M. Tipos de Banner en Dispositivos Cisco. (2019)

² MICROSOFT. Protocolo de configuración dinámica de host (DHCP). (2019)

³ WALTON, Alex. Qué es default Gateway.

⁴ FERNÁNDEZ, Yubal. IPv6: qué es, para qué sirve y qué ventajas tiene. (2019)

⁵ García, F. ¿Que son las líneas vty Cisco?. (2018)

⁶ DE LUZ, Sergio. VLANs: Qué son, tipos y para qué sirven. (2022)

RESUMEN

Como parte fundamental para dar solución a dos estudios de caso bajo el uso de tecnología cisco se realiza la configuración de los diferentes dispositivos, la cual se centra en el enrutamiento IPv4 y IPv6, dentro de la configuración de estos dispositivos, se debe tener como punto de partida la restauración a la configuración inicial, así mismo se asignan unos aspectos básicos como lo son el nombre del dispositivo, nombre del dominio, seguridad de acceso a la consola y al modo de configuración y como factor importante que permitan la conexión remota.

Dentro del direccionamiento de las interfaces en los dos escenarios encontramos que los dispositivos se deben configurar para que acepten simultáneamente direcciones IPv6 y IPv4, a su vez se establecen los parámetros de seguridad tanto de acceso como de conectividad, en los dispositivos se crean unas VLAN las cuales cumplirán una determinada función que va desde alojar las interfaces que estarán en funcionamiento a re direccionar las interfaces que están sin uso y apagadas; En los dispositivos se implementara el protocolo de encapsulación dot1q el cual permite que los routers tengan un enlace troncal.

PALABRAS CLAVES: CISCO, CCNA, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

As a fundamental part to solve two case studies under the use of Cisco technology, the configuration of the different devices is carried out, which focuses on IPv4 and IPv6 routing, within the configuration of these devices, it must be taken as a point From the start, the restoration to the initial configuration, likewise, some basic aspects are assigned, such as the name of the device, domain name, security of access to the console and configuration mode, and as an important factor that allows remote connection.

Within the addressing of the interfaces in the two scenarios we find that the devices must be configured to s imultaneously accept IPv6 and IPv4 addresses, in turn the security parameters for both access and connectivity are established, VLANs are created in the devices which which will fulfill a certain function that goes from hosting the interfaces that will be in operation to redirecting the interfaces that are not used and turned off; The dot1q encapsulation protocol will be implemented in the devices, which allows the routers to have a trunk link.

KEY WORDS: CISCO, CCNA, Switching, Routing, Networks, Electronics.

INTRODUCCIÓN

Teniendo en cuenta los avances tecnológicos en cuanto a la conectividad y las diversas formas de comunicación, tanto entre seres humanos, como en dispositivos electrónicos, se evidencia la urgente necesidad como ingeniero en sistemas de conocer dominar y aplicar las diversas formas de diseñar las estructuras de red que permiten transmitir datos entre sistemas y disponer de los recursos de los dispositivos que forman parte de la red, de igual manera, el diseño de red facilita el almacenamiento y procesamiento de la información ya que permite compartir programas, archivos y datos.

Este informe tiene como finalidad presentar el avance del diseño de red planteado en este proyecto, el cual se basa en realizar una topología de red, que consta de un Router, Switch y dos computadores a los cuales, se les realiza una configuración básica y se les asigna la dirección IP, a la cual, previamente se le realizó el subneteo para poder crear las dos subredes necesarias para que cada una de estas trabaje a nivel de envío y recepción de paquetes como una red individual.

Se pretende que las pruebas de conexión entre dispositivos que se realicen en esta red funcionen de forma adecuada cumpliendo con el objetivo del envío y recepción de paquetes, así mismo que permitan realizar pruebas de campo como es la navegación en los diferentes computadores y la corrección de fallas en la configuración de la conectividad.

Con el desarrollo de estos dos ejercicios, se expondrá el aprendizaje de configuración de redes mediante la aplicación de los conceptos y diferentes temas estudiados a través de los diferentes módulos que forman parte del DIPLOMADO DE PROFUNDIZACION CISCO, dentro de esta temática aprendida encontramos la configuración inicial de los dispositivos, el subneteo de redes, asignación de redes de manera manual y por DHCP, re direccionamiento de redes a las diferentes VLAN,

protocolos de red, configuración de seguridad de los dispositivos y demás parámetros de configuración, lo anterior es posible mediante la consola de los dispositivos o mediante un pc conectado directamente al dispositivo a través de una serie de comandos para tal fin.

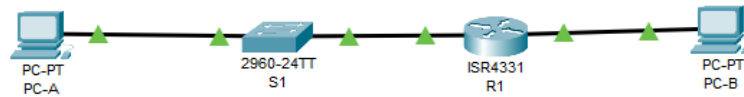
El desarrollo de los escenarios de red nos permite plantear métodos, herramientas y modelos que faciliten el diseño, configuración y la aplicación de nuevas tecnologías de información para el procedimiento de gestión y mejorar los estándares de calidad del funcionamiento de la red, entendiendo que estos estándares de red son una especificación normativa de una tecnología aplicable a internet; es por esta razón que las topologías de red que serán descritas en este documento se caracterizan por su madurez técnica y utilidad que cumpla con los requerimientos del usuario final.

DESARROLLO ESCENARIOS

ESCENARIO 1.

Se procede a construir la red segun los requerimientos de la topologia logica que se plantea en el escenario 1.

Figura 1: topología de red escenario 1



Fuente: Autor

Tabla 1. Direccionamiento IP Escenario 1

Ítem	Requerimiento
Dirección de Red	172.37.3.0 Mascara de red: 255.255.0.0
Requerimiento de host SubredLAN1	60 Sub red 1: IP de Red: 172.37.3.0 /26 Mascara: 255.255.255.192 Primer Host: 172.37.3.1 Ultimo Host: 172.37.3.62
Requerimiento de host SubredLAN2	20 Sub red 2:

	IP de Red: 172.37.3.64/27 Mascara: 255.255.255.224 Primer Host: 172.37.3.65 Ultimo Host: 172.37.3.94
R1 G0/0/1	Última dirección de host de la subred LAN1: 172.37.3.62
R1 G0/0/0	Última dirección de host de la subred LAN2: 172.37.3.94
S1 SVI	Segunda dirección de host de la subred LAN1: 172.37.3.2
PC-A	Décima dirección de host de la subred LAN1: 172.37.3.10
PC-B	Décima dirección de host de la subred LAN2 172.37.3.75

Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 2. Configuración R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del Router	R1 Router(config)#hostname R1

Nombre de dominio	ccna-sa.com R1(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modoEXEC privilegiado	Ciscoenpass R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#enable secret ciscoenpass R1(config)#
Contraseña de acceso a la consola	Ciscoconpass R1(config)#line console 0 R1(config-line) #password ciscoconpass R1(config-line) #login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	10 caracteres R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Contraseña: admin1pass R1(config)#username admin password admin1pass R1(config)#exit
Configure el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 4 R1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexionesSSH	R1(config-line) #transport input ssh R1(config-line)#exit

Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configurar un banner MOTD	<p>Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.</p> <p>R1(config)#banner motd "R1 ROBINSON ALEXANDER ACOSTA VELASCO PROGRAMA: INGENIERIA DE SISTEMAS"</p>
Configuración de interface G0/0/0	<p>Establecer la descripción Establecer la dirección IPv4</p> <p>Activar la interfaz.</p> <p>R1(config)#interface g0/0/0</p> <p>R1(config-if) #ip address 172.37.3.94 255.255.255.224</p> <p>R1(config-if)#no shutdown</p>
Configuración de interface G0/0/1	<p>Establecer la descripción Establecer la dirección IPv4</p> <p>Activar la interfaz.</p> <p>R1(config)#interface g0/0/1</p> <p>R1(config-if) #ip address 172.37.3.62 255.255.255.192</p> <p>R1(config-if)#no shutdown</p>
Generar una clave de cifrado RSA	<p>Módulo de 1024 bits</p> <p>R1(config)#crypto key generate rsa</p> <p>The name for the keys will be: R1.ccna-sa.com</p> <p>Choose the size of the key modulus in the range of 360 to 2048 for your</p> <p>General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.</p>

	How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
--	--

Fuente: Autor

Configuración Router R1

- Para desactivar la búsqueda DNS del Router lo primero que se debe hacer es dar clic en el dispositivo, luego en la pestaña CLI y esperar que el dispositivo permita escribir, posteriormente se utilizan los siguientes comandos para realizar la respectiva configuración

Router>enable **Ingreso al modo privilegiado**

Router#configure terminal **Ingreso al modo de configuración**

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

Router(config)#no ip domain-lookup **Desactivar la búsqueda DNS**

- Como se encuentra en el modo de configuración, se pueden escribir los comandos para asignar el nombre del dispositivo y el nombre del dominio

Router(config)#hostname R1 **Nombre del dispositivo**

R1(config)#ip domain-name ccna-sa.com **Nombre del Dominio**

- Para asignar una contraseña cifrada para el modo EXEC privilegiado, dentro del modo de configuración se escribe el comando:

R1(config)#enable secret ciscoenpass **Contraseña modo privilegiado**

- Para asignar la contraseña Ciscoconpass en el acceso a la consola, dentro del modo de configuración:

R1(config)#line console 0 **Ingreso a la consola**

- Luego, dentro del line console 0, se asigna la contraseña con el siguiente comando, y dar exit para salir de la consola

R1(config-line) #password ciscoconpass **Contraseña acceso a la consola**

R1(config-line) #login

R1(config-line) #exit

- Con el comando `security passwords min-length` dentro del modo de configuración se asigna la longitud mínima para las contraseñas, en este escenario será de 10

R1(config)#security passwords min-length 10 **Longitud minima de contraseña**

- Creación de un usuario administrativo en la base de datos local, dentro del modo de configuración

R1(config)#username admin password admin1pass **Usuario y contraseña**

- Para la configuración del inicio de sesión en las líneas VTY para que use la base de datos local, en el modo de configuración, se ingresa el siguiente comando:

R1(config)#line vty 0 4 **Cambio del modo de configuración
Global a las líneas vty 0 4**

- Dentro del menú de la base local se escribe el siguiente comando para el inicio de sesión

R1(config-line) #login local

- Configuración de la base de datos local para configurar las líneas VTY para que acepten únicamente las conexiones SSH

R1(config-line) #transport input ssh **Configuración VTY solo conexiones ssh**

- Para cifrar las contraseñas, dentro del menú de configuración:

R1(config)#service password-encryption **Cifrado de contraseñas**

Configuración del banner motd, con el nombre del dispositivo, nombre del estudiante y programa continuando en el menú de configuración:

R1(config)#banner motd "R1 ROBINSON ALEXANDER ACOSTA VELASCO
PROGRAMA: INGENIERIA DE SISTEMAS" **Configuración motd banner**

- Configuración de la interface G0/0/0, asignación de IP:

R1(config)#interface g0/0/0 **Acceder a la interface**

R1(config-if) #ip address 172.37.3.94 255.255.255.224 **Dirección IP y máscara de RED**

R1(config-if) #no shutdown **Activación de Puerto**

- Configuración de la interface G0/0/1, asignación de IP:

R1(config)#interface g0/0/1

Acceder a la interface

R1(config-if) #ip address 172.37.3.62 255.255.255.192

de RED

Dirección IP y mascara

R1(config-if) #no shutdown

Activación de Puerto

- Generar una clave de cifrado RSA: 1024 bit

R1(config)#crypto key generate rsa

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 3. Configuración S1

TAREA	ESPECIFICACIÓN
Desactivar la búsqueda DNS	Switch>enable Switch#Configure terminal Enter configuration commands, one per line. Switch(config)#no ip domain-lookup
Nombre del Swtich	S1 Switch(config)#hostname S1
Nombre de dominio	ccna-sa.com S1#configure terminal Enter configuration commands, one per line. S1(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	Ciscoenpass S1(config)#line console 0 S1(config-line) #password ciscoenpass S1(config-line) #login S1(config-line)#exit
Contraseña de acceso a la consola	Ciscoconpass

	<pre>S1(config)#enable secret ciscoconpass S1(config)#exit</pre>
Apagar todos los puertos sin usar	<p>F0/1-4, F0/7-24, G0/1-2</p> <pre>S1(config)#interface range F0/1-4, F0/7-24, G0/1-2 S1(config-if-range) #shutdown</pre>
Crear un usuario administrativo en la base de datos local	<p>Nombre de usuario: admin</p> <p>Contraseña: admin1pass</p> <pre>S1(config)#username admin password admin1pass</pre>
Configure el inicio de sesión en las líneas VTY para que use la base de datos local	<pre>S1(config)#line vty 0 4 S1(config-line) #login local S1(config-line)#exit</pre>
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	<pre>S1(config)#line vty 0 4 S1(config-line) #transport input ssh S1(config-line)#exit</pre>
Cifrar las contraseñas de texto no cifrado	<pre>S1(config)# service password- encryption</pre>
Configurar un banner MOTD	<p>Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.</p> <pre>S1(config)#banner motd " S1 ROBINSON ALEXANDER ACOSTA VELASCO PROGRAMA: INGENIERIA DE SISTEMAS"</pre>
Generar una clave de cifrado RSA	<p>Módulo de 1024 bits</p> <pre>S1(config)#crypto key generate rsa The name for the keys will be: S1.ccn- sa.com Choose the size of the key modulus in the range of 360 to 2048 for your</pre>

	<p>General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.</p> <p>How many bits in the modulus [512]: 1024</p> <p>% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]</p>
<p>Configure la interfaz de administración (SVI) en VLAN1</p>	<p>Establecer la descripción Establecer la dirección IPv4</p> <p>S1(config)# interface vlan1</p> <p>*Mar 1 0:24:35.474: %SSH-5-ENABLED: SSH 1.99 has been enabled</p> <p>S1(config-if) #ip address 172.37.3.2 255.255.255.192</p> <p>S1(config-if) #no shutdown</p>

Fuente: Autor

Configuración Switch S1

- Para desactivar la búsqueda DNS del Switch lo primero que se debe hacer es dar clic en el dispositivo, luego en la pestaña CLI y esperar que el dispositivo permita escribir, posteriormente se utilizan los siguientes comandos para realizar la respectiva configuración

Switch>enable

Ingreso al modo privilegiado

Switch#Configure terminal

Ingreso al modo de configuración

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

Switch(config)#no ip domain-lookup

Desactivar la búsqueda DNS

- Como el dispositivo está en el modo de configuración, se escriben los comandos para asignar el nombre del dispositivo y el nombre del dominio

Router(config)#hostname S1

Nombre del dispositivo

S1(config)#ip domain-name ccna-sa.com

Nombre del Dominio

- Para asignar una contraseña cifrada para el modo EXEC privilegiado, dentro del modo de configuración se escribe el comando:

S1(config)#enable secret ciscoenpass

Contraseña modo privilegiado

- Para asignar la contraseña Ciscoenpass en el acceso a la consola, dentro del modo de configuración:

S1(config)#line console 0

Ingreso a la consola

- Luego, dentro del line console 0, se asigna la contraseña con el siguiente comando, y damos exit para salir de la consola

S1(config-line) #password ciscoconpass

Contraseña acceso a la consola

S1(config-line) #login

S1(config-line) #exit

- Para apagar los puertos que no se van a utilizar en el Switch:

S1(config)#interface range F0/1-4, F0/7-24, G0/1-2 F0/1-4, F0/7-24, G0/1-2

S1(config-if-range) #shutdown

- Creación de un usuario administrativo en la base de datos local, dentro del modo de configuración

S1(config)#username admin password admin1pass

Usuario y contraseña

- Para la configuración del inicio de sesión en las líneas VTY para que use la base de datos local, en el modo de configuración, se ingresa el siguiente comando:

S1(config)#line vty 0 4

Cambio del modo de configuración

Global a las líneas vty 0 4

- Dentro del menú de la base local escribir el siguiente comando para el inicio de sesión

S1(config-line) #login local

- Configuración de la base de datos local para configurar las líneas VTY para que acepten únicamente las conexiones SSH

S1(config-line) #transport input ssh **Configuración VTY solo conexiones ssh**

- Para cifrar las contraseñas, dentro del menú de configuración:

S1(config)#service password-encryption **Cifrado de contraseñas**

- Configuración del banner motd, con el nombre del dispositivo, nombre del estudiante y programa continuando en el menú de configuración:

S1(config)#banner motd "S1 ROBINSON ALEXANDER ACOSTA VELASCO
PROGRAMA: INGENIERIA DE SISTEMAS" **Configuración motd banner**

- Configuración de la interface Vlan1, asignación de IP:

S1(config)# interface vlan1 **Acceso a la VLAN**

*Mar 1 0:24:35.474: %SSH-5-ENABLED: SSH 1.99 has been enabled

S1(config-if) #ip address 172.37.3.2 255.255.255.192 **Asignación IP y Mascara de red**

S1(config-if) #no shutdown **Encender la interface**

- Generar una clave de cifrado RSA: 1024 bit

S1(config)#crypto key generate rsa

The name for the keys will be: S1.ccna-sa.com

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

Paso 2. Configurar los equipos

Tabla 4. Configuración PC-A

Configuración de red de PC-A	
Descripción	PC-A FastEthernet 0
Dirección física	FE80::202:17FF:FE81:1BB
Dirección IPv4	172.37.3.10

Máscara de subred	255.255.255.192
Puerta de enlace IPv4 predeterminada	172.37.3.62

Fuente: Autor

Tabla 5. Configuración PC-B

Configuración de red de PC-B	
Descripción	PC-B FastEthernet 0
Dirección física	FE80::2E0:B0FF:FE73:42A2
Dirección IPv4	172.37.3.75
Máscara de subred	255.255.255.224
Puerta de enlace IPv4 predeterminada	172.37.3.94

Fuente: Autor

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

Tabla 6. Conexión entre dispositivos

Desde	A	Dirección IP	Resultados de ping
PC-A	R1 G0/0/0	172.37.3.94	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	R1 G0/0/1	172.37.3.62	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

	S1 VLAN 1	172.37.3.2	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	PC-B	172.37.3.75	Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
PC-B	R1 G0/0/0	172.37.3.94	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	R1 G0/0/1	172.37.3.62	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	S1 VLAN1	172.37.3.2	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

Fuente: Autor

- Ping PC-A a R1 G0/0/0 172.37.3.94

Figura 2. Ping PC-A a R1 G0/0/0

```

C:\>
C:\>ping 172.37.3.94

Pinging 172.37.3.94 with 32 bytes of data:

Reply from 172.37.3.94: bytes=32 time=349ms TTL=255
Reply from 172.37.3.94: bytes=32 time<lms TTL=255
Reply from 172.37.3.94: bytes=32 time<lms TTL=255
Reply from 172.37.3.94: bytes=32 time<lms TTL=255

Ping statistics for 172.37.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 349ms, Average = 87ms

```

Fuente: Autor

Como se evidencia en la figura 2, el Ping desde el PC-A a R1 G0/0/0 172.37.3.94 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetes enviados los 4 fueron recibidos.

- Ping PC-A a R1 G0/0/1 172.37.3.62

Figura 3. Ping PC-A a R1 G0/0/1

```
C:\>
C:\>ping 172.37.3.62

Pinging 172.37.3.62 with 32 bytes of data:

Reply from 172.37.3.62: bytes=32 time=9ms TTL=255
Reply from 172.37.3.62: bytes=32 time<lms TTL=255
Reply from 172.37.3.62: bytes=32 time<lms TTL=255
Reply from 172.37.3.62: bytes=32 time<lms TTL=255

Ping statistics for 172.37.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 9ms, Average = 2ms

C:\>|
```

Fuente: Autor

En la Figura 3, se puede observar como el Ping del PC-A a R1 G0/0/1 172.37.3.62 Funciona de manera correcta, recibiendo los 4 paquetes que fueron enviados.

- Ping PC-A a S1 VLAN 1 172.37.3.2

Figura 4. Ping PC-A a S1 VLAN 1

```
C:\>
C:\>ping 172.37.3.2

Pinging 172.37.3.2 with 32 bytes of data:

Reply from 172.37.3.2: bytes=32 time<lms TTL=255
Reply from 172.37.3.2: bytes=32 time<lms TTL=255
Reply from 172.37.3.2: bytes=32 time<lms TTL=255
Reply from 172.37.3.2: bytes=32 time<lms TTL=255

Ping statistics for 172.37.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Autor

En la Figura 4, se comprueba la conectividad que se tiene desde el PC-A hasta el Swtich, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-A a PC-B 172.37.3.75

Figura 5. Ping PC-A a PC-B

```
C:\>ping 172.37.3.75

Pinging 172.37.3.75 with 32 bytes of data:

Request timed out.
Reply from 172.37.3.75: bytes=32 time<1ms TTL=127
Reply from 172.37.3.75: bytes=32 time=1ms TTL=127
Reply from 172.37.3.75: bytes=32 time=1ms TTL=127

Ping statistics for 172.37.3.75:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Fuente: Autor

En la Figura 5, se realiza una prueba ping desde los dos PC de esta topología de red, la cual dio un 75%, puesto que se perdió un paquete, pero cabe aclarar que, si se realiza de nuevamente la prueba, esta dará como resultado 100% de conectividad.

- Ping PC-B a R1 G0/0/0 172.37.3.94

Figura 6. Ping PC-B a R1 G0/0/0

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.37.3.94

Pinging 172.37.3.94 with 32 bytes of data:

Reply from 172.37.3.94: bytes=32 time<1ms TTL=255
Reply from 172.37.3.94: bytes=32 time<1ms TTL=255
Reply from 172.37.3.94: bytes=32 time<1ms TTL=255
Reply from 172.37.3.94: bytes=32 time<1ms TTL=255

Ping statistics for 172.37.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Autor

En la Figura 6, la prueba de conectividad entre el PC-B y el Router funciona de manera correcta, obteniendo como resultado 100% de paquetes recibidos, lo que nos demuestra que la configuración de los dispositivos se realizó de manera correcta

- Ping PC-B a R1 G0/0/1 172.37.3.62

Figura 7. Ping PC-B a R1 G0/0/1

```
C:\>ping 172.37.3.62

Pinging 172.37.3.62 with 32 bytes of data:

Reply from 172.37.3.62: bytes=32 time<lms TTL=255
Reply from 172.37.3.62: bytes=32 time<lms TTL=255
Reply from 172.37.3.62: bytes=32 time<lms TTL=255
Reply from 172.37.3.62: bytes=32 time<lms TTL=255

Ping statistics for 172.37.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Autor

En la Figura 7, para comprobar la conectividad entre el los dos dispositivos, PC y Router se enviaron 4 paquetes, los cuales fueron recibidos de manera correcta en su destino en este caso en el Router, demostrando que el direccionamiento de IP es correcto.

- Ping PC-B a S1 VLAN1 172.37.3.2

Figura 8. Ping PC-B a S1 VLAN1

```
C:\>ping 172.37.3.2

Pinging 172.37.3.2 with 32 bytes of data:

Reply from 172.37.3.2: bytes=32 time<lms TTL=254
Reply from 172.37.3.2: bytes=32 time<lms TTL=254
Reply from 172.37.3.2: bytes=32 time<lms TTL=254
Reply from 172.37.3.2: bytes=32 time<lms TTL=254

Ping statistics for 172.37.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Autor

En la Figura 8, en la prueba de conectividad de extremo a extremo, se realizó el ping desde el PC-B al Switch el cual funciono de manera correcta, dando como resultado 4 paquetes recibidos de los 4 enviados.

ESCENARIO 2

Topología

Figura 9. Topología de red escenario 2

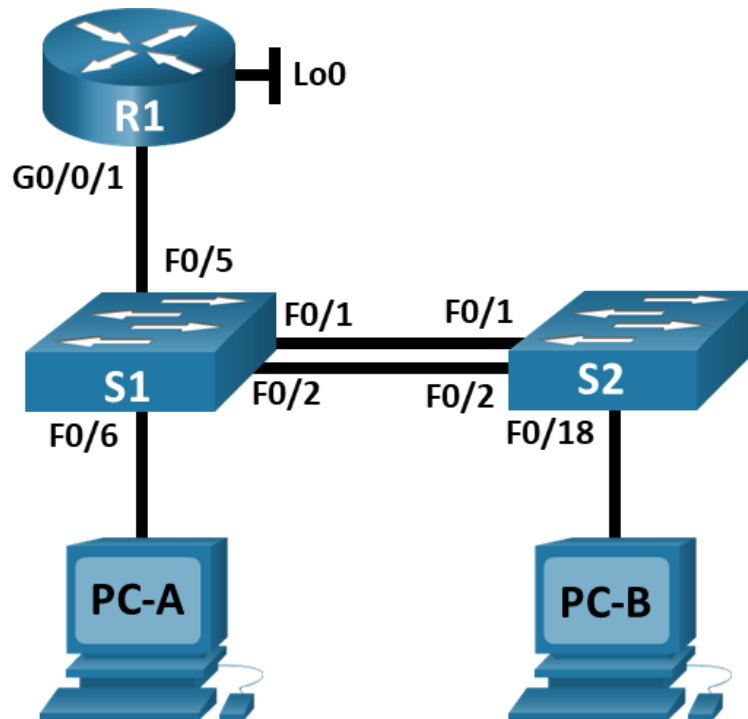


Tabla 7. VLAN Escenario 2

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

Tabla 8. Asignación de Direcciones IP

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.20	10.37.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.30	10.37.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.40	10.37.8.97 /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 4	10.37.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.37.8.99 /29	10.19.8.97
	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

Paso 1: Inicializar y volver a cargar el Router y el switch

- Borre las configuraciones de inicio y las VLAN del Router y del switch y vuelva a cargar los dispositivos.
- Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.

CONFIGURACION DEL ROUTER R1

Tabla 9. Configuración inicial R1

Tarea	Especificación
Eliminar el archivo startup-config de todos los routers	Router>enable Router#erase startup-config
Volver a cargar todos los routers	Router# reload

Fuente: Autor

CONFIGURACION DE LOS SWITCHES S1 Y S2

Tabla 10. Configuración inicial S1 Y S2

Tarea	Especificación
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch#erase startup-config Switch#delete vlan.dat
Volver a cargar ambos switches	Switch#reload
configurar la plantilla SDM para que admita IPv6	Switch#sdm prefer dual-ipv4-and-ipv6 default

Fuente: Autor

Se ingresa al Router 1 a través de la consola en modo privilegiado para borrar cualquier configuración de inicio con el comando **erase startup-config** el cual borra el contenido de la NVRAM, luego con el comando **reload** se reinicia el Router, se repite el mismo procedimiento con los switch 1 y 2 agregándoles el comando **sdm prefer dual-ipv4-and-ipv6 default** para que acepte direcciones ipv4 e ipv6 al tiempo.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11. Configuración R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain lookup
Nombre del Router	Router(config)#hostname R1
Nombre de dominio	R1(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXECprivilegiado	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line) #password cisco R1(config-line)#login
Establecer la longitud mínima para lascontraseñas	R1(config)#security passwords min-length 5
Crear un usuario administrativo en labase de datos local	R1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datoslocal	R1(config)#line vty 015 R1(config-line)#login local
Configurar VTY solo aceptando SSH	R1(config-line) #transport input ssh
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd " R1 ROBINSON ALEXANDER ACOSTA VELASCO INGENIERIA DE SISTEMAS "
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing

<p>Configurar interfaz G0/0/1 y subinterfaces</p>	<pre> R1(config)#int g0/0/1.20 R1(config-subif) #encapsulation dot1q 2 0 R1(config-subif) #description Docentes R1(config-subif) #ip address 10.37.8.1 255.255.255.192 R1(config-subif) #ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 address fe80::1 link- local R1(config-subif)#int g0/0/1.30 R1(config-subif)#encapsulation dot1q30 R1(config-subif)#description Estudiantes R1(config-subif)#ip address 10.37.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address fe80::1 link- local R1(config-subif)#int g0/0/1.40 R1(config-subif)#encapsulation dot1q 40 R1(config-subif)#description Invitados R1(config-subif)#ip address 10.37.8.97 255.255.255.248 R1(config-subif) #ipv6 address 2001:db8: acad:c::1/64 R1(config-subif)#ipv6 address fe80::1 link- local R1(config-subif)#int g0/0/1.56 R1(config-subif)#encapsulation dot1q 6 native R1(config-subif)#description Native R1(config-subif)#int g0/0/1 R1(config-if)#no shutdown </pre>
<p>Configure el Loopback0 interface</p>	<pre> R1(config-if)#int loopback 0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 </pre>

	<pre>R1(config-if)#ipv6 address 2001:db8:acad:209: :1 /64 R1(config-if)#ipv6 address fe80::1 link- local R1(config-if)#description internet R1(config-if)#exit</pre>
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa

Fuente: Autor

Configuración Router R1

- Para desactivar la búsqueda DNS del Router lo primero que se debe hacer es dar clic en el dispositivo, luego en la pestaña CLI y esperar que el dispositivo permita escribir, posteriormente se utilizan los siguientes comandos para realizar la respectiva configuración

Router>enable

Ingreso al modo privilegiado

Router#configure terminal

Ingreso al modo de configuración

Router(config)#no ip domain-lookup

Desactivar la búsqueda DNS

- Como se encuentra en el modo de configuración, se pueden escribir los comandos para asignar el nombre del dispositivo y el nombre del dominio

Router(config)#hostname R1

Nombre del dispositivo

R1(config)#ip domain-name ccna-sa.com

Nombre del Dominio

- Para asignar una contraseña cifrada para el modo EXEC privilegiado, dentro del modo de configuración se escribe el comando:

R1(config)#enable secret ciscoconpass

Contraseña modo privilegiado

- Para asignar la contraseña Ciscoconpass en el acceso a la consola, dentro del modo de configuración:

R1(config)#line console 0

Ingreso a la consola

- Luego, dentro del line console 0, se asigna la contraseña con el siguiente comando, y dar exit para salir de la consola

R1(config-line) #password ciscoconpass

Contraseña acceso a la consola

R1(config-line) #login

R1(config-line) #exit

- Con el comando `security passwords min-length` dentro del modo de configuración se asigna la longitud mínima para las contraseñas, en este escenario será de 10

R1(config)#security passwords min-length 10 **Longitud minima de contraseña**

- Creación de un usuario administrativo en la base de datos local, dentro del modo de configuración

R1(config)#username admin password admin1pass **Usuario y contraseña**

- Para la configuración del inicio de sesión en las líneas VTY para que use la base de datos local, en el modo de configuración, se ingresa el siguiente comando:

R1(config)#line vty 0 15 **Cambio del modo de configuración Global a las líneas vty 0 15**

- Dentro del menú de la base local se escribe el siguiente comando para el inicio de sesión

R1(config-line) #login local

- Configuración de la base de datos local para configurar las líneas VTY para que acepten únicamente las conexiones SSH

R1(config-line) #transport input ssh **Configuración VTY solo conexiones ssh**

Para cifrar las contraseñas, dentro del menú de configuración:

R1(config)#service password-encryption **Cifrado de contraseñas**

- Configuración del banner motd, con el nombre del dispositivo, nombre del estudiante y programa continuando en el menú de configuración:

R1(config)#banner motd "R1 ROBINSON ALEXANDER ACOSTA VELASCO PROGRAMA: INGENIERIA DE SISTEMAS" **Configuración motd banner**

- Configuración del enrutamiento IPv6

R1(config)#ipv6 unicast-routing **Se activa el enrutamiento IPv6**

- Configuración de la interfaz G0/0/1, Sub interfaces y asignación de IPv4 e IPv6:

R1(config)#int g0/0/1.20 **Se accede a la sub interface**
R1(config-subif) #encapsulation dot1q 2 0 **Se establece el modo de encapsulación**

R1(config-subif) #description Docentes **Se asigna una descripción**

R1(config-subif) #ip address 10.37.8.1 255.255.255.192 **se configura la IPv4 con su respectiva mascara de sub red**

R1(config-subif) #ipv6 address 2001:db8:acad:a::1/64 **Asignacion de Ipv6**

R1(config-subif)#ipv6 address fe80::1 link-local **Enlace local de la Ipv6**

- Se repite el anterior procedimiento para las sub interfaces g0/0/1.30, g0/0/1.40 y g0/0/1.56, variando únicamente su direccionamiento IP el cual está establecido en la tabla nº titulada, asignación de direcciones IP

- Configuración de la Interface Loopback0

R1(config-if)#int loopback 0 **Se accede a la Interface**

R1(config-if)#ip address 209.165.201.1 255.255.255.224 **Asignacion de IPv4 con su respectiva mascara de red**

R1(config-if)#ipv6 address 2001:db8:acad:209: :1/64 **Asignacion de IPv6**

R1(config-if)#ipv6 address fe80::1 link-local **Enlace local de IPv6**

R1(config-if)#description internet **Descripcion de la interface**

- Generar una clave de cifrado RSA: 1024 bit

R1(config)#crypto key generate rsa

Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

SWITCH 1:

Tabla 12. Configuración S1

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch(config)#no ip domain lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio	S1(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	S1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd " S1 ROBINSON ALEXANDER ACOSTA VELASCO INGENIERIA DE SISTEMAS "
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa
Configurar la interfaz de administración (SVI)	S1(config)# S1(config)#int vlan 40 S1(config-if)#ip address 10.37.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local

	S1(config-if)#description Administration
Configuración del Gateway predeterminado	S1(config-if)#ip default-gateway 10.37.8.97

Fuente: Autor

Configuración Switch S1

- Para desactivar la búsqueda DNS del Switch lo primero que se debe hacer es dar clic en el dispositivo, luego en la pestaña CLI y esperar que el dispositivo permita escribir, posteriormente se utilizan los siguientes comandos para realizar la respectiva configuración

Switch>enable

Ingreso al modo privilegiado

Switch#Configure terminal

Ingreso al modo de configuración

Switch(config)#no ip domain-lookup

Desactivar la búsqueda DNS

- Como el dispositivo está en el modo de configuración, se escriben los comandos para asignar el nombre del dispositivo y el nombre del dominio

Router(config)#hostname S1

Nombre del dispositivo

S1(config)#ip domain-name ccna-sa.com

Nombre del Dominio

- Para asignar una contraseña cifrada para el modo EXEC privilegiado, dentro del modo de configuración se escribe el comando:

S1(config)#enable secret ciscoenpass

Contraseña modo privilegiado

- Para asignar la contraseña Ciscoconpass en el acceso a la consola, dentro del modo de configuración:

S1(config)#line console 0

Ingreso a la consola

- Luego, dentro del line console 0, se asigna la contraseña con el siguiente comando, y damos exit para salir de la consola

S1(config-line) #password ciscoconpass

Contraseña acceso a la consola

S1(config-line) #login

- Creación de un usuario administrativo en la base de datos local, dentro del modo de configuración

S1(config)#username admin password admin1pass

Usuario y contraseña

- Para la configuración del inicio de sesión en las líneas VTY para que use la base de datos local, en el modo de configuración, se ingresa el siguiente comando:

S1(config)#line vty 0 15 **Cambio del modo de configuración Global a las líneas vty 0 15**

- Dentro del menú de la base local escribir el siguiente comando para el inicio de sesión

S1(config-line) #login local

- Configuración de la base de datos local para configurar las líneas VTY para que acepten únicamente las conexiones SSH

S1(config-line) #transport input ssh **Configuración VTY solo conexiones ssh**

Para cifrar las contraseñas, dentro del menú de configuración:

S1(config)#service password-encryption **Cifrado de contraseñas**

- Configuración del banner motd, con el nombre del dispositivo, nombre del estudiante y programa continuando en el menú de configuración:

S1(config)#banner motd "S1 ROBINSON ALEXANDER ACOSTA VELASCO PROGRAMA: INGENIERIA DE SISTEMAS" **Configuración motd banner**

- Configuración de la interface Vlan 40, asignación de IP:

S1(config)# interface vlan 40 **Se accede a la VLAN**

S1(config-if)#ip address 10.37.8.98 255.255.255.248 **Asignación de IPv4 con máscara de red**

S1(config-if)#ip default-gateway 10.37.8.97 **Configuración del puerto de enlace preterminado para IPv4**

S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 **Asignación de dirección IPv6**

S1(config-if)#ipv6 address fe80::98 link-local **Enlace local de IPv6**

S1(config-if)#description Administration **Se asigna una Descripción**

SWITCH 2

Tabla 13. Configuración S2

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch(config)#no ip domain lookup
Nombre del switch	Switch(config)#hostname S2
Nombre de dominio	S2(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	S2(config)#enable secret class
Contraseña de acceso a la consola	S2(config)#line console 0 S2(config-line)#password cisco S2(config-line)#login
Crear un usuario administrativo en la base de datos local	S2(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 15 S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption
Configurar un MOTD Banner	S2(config)#banner motd " S2 ROBINSON ALEXANDER ACOSTA VELASCO INGENIERIA DE SISTEMAS "
Generar una clave de cifrado RSA	S2(config)#crypto key generate rsa
Configurar la interfaz de administración (SVI)	S2(config)#int vlan 40 S2(config-if)#ip address 10.37.8.99 255.255.255.248 S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#ipv6 address fe80::99 link-local S2(config-if)#description Administracion
Configuración del Gateway predeterminado	S2(config-if)#ip default-gateway 10.37.8.97

	S2(config-if)#no shutdown
--	---------------------------

Fuente: Autor

Configuración Swtich S2

- Para desactivar la búsqueda DNS del Swtich lo primero que se debe hacer es dar clic en el dispositivo, luego en la pestaña CLI y esperar que el dispositivo permita escribir, posteriormente se utilizan los siguientes comandos para realizar la respectiva configuración

Swtich>enable

Ingreso al modo privilegiado

Switch#Configure terminal

Ingreso al modo de configuración

Switch(config)#no ip domain-lookup

Desactivar la búsqueda DNS

- Como el dispositivo está en el modo de configuración, se escriben los comandos para asignar el nombre del dispositivo y el nombre del dominio

Router(config)#hostname S2

Nombre del dispositivo

S2(config)#ip domain-name ccna-sa.com

Nombre del Dominio

- Para asignar una contraseña cifrada para el modo EXEC privilegiado, dentro del modo de configuración se escribe el comando:

S2(config)#enable secret ciscoenpass

Contraseña modo privilegiado

- Para asignar la contraseña Ciscoconpass en el acceso a la consola, dentro del modo de configuración:

S2(config)#line console 0

Ingreso a la consola

- Luego, dentro del line console 0, se asigna la contraseña con el siguiente comando, y damos exit para salir de la consola

S2(config-line) #password ciscoconpass

Contraseña acceso a la consola

S2(config-line) #login

- Creación de un usuario administrativo en labase de datos local, dentro del modo de configuración

S2(config)#username admin password admin1pass

Usuario y contraseña

- Para la configuración del inicio de sesión en las líneas VTY para que use la base de datos local, en el modo de configuración, se ingresa el siguiente comando:

S2(config)#line vty 0 15

**Cambio del modo de configuración
Global a las líneas vty 0 15**

- Dentro del menú de la base local escribir el siguiente comando para el inicio de sesión

S2(config-line) #login local

- Configuración de la base de datos local para configurar las líneas VTY para que acepten únicamente las conexiones SSH

S2(config-line) #transport input ssh

Configuracion VTY solo conexiones ssh

Para cifrar las contraseñas, dentro del menú de configuración:

S2(config)#service password-encryption

Cifrado de contraseñas

- Configuración del banner motd, con el nombre del dispositivo, nombre del estudiante y programa continuando en el menú de configuración:

S2(config)#banner motd "S2 ROBINSON ALEXANDER ACOSTA VELASCO
PROGRAMA: INGENIERIA DE SISTEMAS"

Configuracion motd banner

- Configuración de la interface Vlan 40, asignación de IP:

S2(config)# interface vlan 40

Se accede a la VLAN

S2(config)#int vlan 40

S2(config-if)#ip address 10.37.8.99 255.255.255.248

Asignacion de IPv4 con

mascara de red

S2(config-if)#ip default-gateway 10.37.8.97

Configuracion del puerta

de enlace preterminado para IPv4

S2(config-if)#ipv6 address 2001:db8:acad:c::99/64

Asignacion de direccion

IPv6

S2(config-if)#ipv6 address fe80::99 link-local

Enlace local de IPv6

S2(config-if)#description Administration

Se asigna una descripcion

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

Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 14. Configuración de la infraestructura de red VLAN, Trunking, EtherChannel S1

Tarea	Especificación
Crear VLAN	<pre>S1(config)# S1(config)#vlan 20 S1(config-vlan)#name Docentes S1(config-vlan)#vlan 30 S1(config-vlan)#name Estudiantes S1(config-vlan)#vlan 40 S1(config-vlan)#name Invitados S1(config-vlan)#vlan 50 S1(config-vlan)#name Usuarios S1(config-vlan)#vlan 56 S1(config-vlan)#name Native S1(config-vlan)#exit</pre>
Crear troncos 802.1Q que utilicen la VLAN 56 nativa	<pre>S1(config)#interface fa0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport trunk native vlan 56 S1(config-if)#interface range fa0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport trunk native vlan 56</pre>
Crear un grupo de puertos EtherChannel de	<pre>S1(config)#interface range fa0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#interface Port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q</pre>

Capa 2 que use interfaces F0/1 y F0/2	S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 56
Configurar el puerto de acceso del host para laVLAN 20	S1(config-if)#interface fa0/6 S1(config-if)#switchport mode acces S1(config-if)#switchport acces vlan 20
Configure port-security en los Access ports	S1(config-if)#switchport port-security maximum 4
Asegure todas las interfaces no utilizadas.	S1(config-if-range)#interface range fa0/3-4 S1(config-if-range)#switchport acces vlan 50 S1(config-if-range)#description Sin uso S1(config-if-range)#shutdown S1(config-if-range)#interface range fa0/7-24 S1(config-if-range)#switchport acces vlan 50 S1(config-if-range)#description Sin uso S1(config-if-range)#shutdown S1(config-if-range)#interface range g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#description Sin uso S1(config-if-range)#shutdown

Fuente: Autor

- Creacion de las VLAN, desde la consola en el modo privilegiado, posteriormente en la configuración global con el siguiente comando se proceden a crear las diferentes vlan:

S1(config)#vlan 20

Creación de la vlan 20

S1(config-vlan)#name Docentes

Asignación de Nombre

- Se repite el mismo procedimiento para las vlan, 30- Estudiantes, 40- Invitados, 50- Usuarios, 56-Nativa

- Creación de troncos 802.1Q que utilicen la VLAN 56 nativa en la interfaz fa0/5

S1(config)#interface fa0/5 **Se accede a la interface de conexión con el Router**

S1(config-if)#switchport trunk encapsulation dot1q **Se indica al switch que en la Interfaz debe usar la encapsulación IEEE 802.1Q en las tramas, cuando esta esté configurada como troncal, Se cambia la interface a modo de enlace control permanente**

S1(config-if)#switchport trunk native vlan 56 **Direccionamiento a la VLAN 56**

- Creación de troncos 802.1Q que utilicen la VLAN 56 nativa en la interfaz fa0/1 y fa0/1-2

S1(config-if)#interface range fa0/1-2 **Se accede al rango con las dos interfaces a modificar**

S1(config-if-range)# shutdown **Se apaga el grupo de la interface para realizar la configuración**

S1(config-ifrange)#switchport trunk encapsulation dot1q **Se indica al switch que en la Interfaz debe usar la encapsulación IEEE 802.1Q en las tramas, cuando esta esté configurada como troncal, Se cambia la interface a modo de enlace control permanente**

S1(config-if-range)#switchport trunk native vlan 56 **Se direcciona el rango de la interface a la VLAN 56 native**

- Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2

S1(config)#interface range fa0/1-2 **Se accede al rango con las dos interfaces a modificar**

S1(config-if-range)#channel-group 1 mode active **Luego de que se crea el grupo se realiza su activación**

S1(config-if-range)#interface Port-channel 1 **Se accede a la interface del canal**

S1(config-if)#switchport trunk encapsulation dot1q **Se indica al switch que en la Interfaz debe usar la encapsulación IEEE 802.1Q en las tramas, cuando esta esté configurada como troncal, Se cambia la interface a modo de enlace control permanente**

S1(config-if)#switchport trunk native vlan 56 **Se re direcciona el rango de la interface a la VLAN 56 native**

- Configuración del puerto de acceso del host para la VLAN 20

S1(config-if)#interface fa0/6 **Se accede a la interface**

S1(config-if)#switchport mode acces **Se configura el modo operativo de enlace troncal en una interfaz de capa 2**

S1(config-if)#switchport acces vlan 20 **Se redireccióna la interfaz a la vlan20**

- configuración de seguridad en los puertos de acceso

S1(config-if)#switchport port-security maximum 4 **Se configura la seguridad de los puertos de la interface para que el acceso solo permita 4 direcciones Mac.**

- Interfaces no utilizadas

se aseguran todas las interfaces sin usar, mediante una serie de rangos (fa0/3-4, fa0/7-24, range g0/1-2) para así re direccionarlas a la vlan 50-Usuarios, se asigna una descripción: "sin uso" y finalmente se apagan

```
S1(config-if-range)#interface range fa0/3-4
```

```
S1(config-if-range)#switchport acces vlan 50
```

```
S1(config-if-range)#description Sin uso
```

```
S1(config-if-range)#shutdown
```

```
S1(config-if-range)#interface range fa0/7-24
```

```
S1(config-if-range)#switchport acces vlan 50
```

```
S1(config-if-range)#description Sin uso
```

```
S1(config-if-range)#shutdown
```

```
S1(config-if-range)#interface range g0/1-2
```

S1(config-if-range)#switchport mode access
 S1(config-if-range)#switchport access vlan 50
 S1(config-if-range)#description Sin uso
 S1(config-if-range)#shutdown

Paso 5: Configure el S2.

Entre las tareas de configuración de S2 se incluyen las siguientes

Tabla 15. Configuración de la infraestructura de red VLAN, Trunking, EtherChannel S2

Tarea	Especificación
Crear VLAN	S2(config)# S2(config)#vlan 20 S2(config-vlan)#name Docentes S2(config-vlan)#vlan 30 S2(config-vlan)#name Estudiantes S2(config-vlan)#vlan 40 S2(config-vlan)#name Invitados S2(config-vlan)#vlan 50 S2(config-vlan)#name Usuarios S2(config-vlan)#vlan 56 S2(config-vlan)#name Native S2(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 56 nativa	S2(config)#interface range fa0/1-2 S2(config-if-range)#shutdown S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 56

Crear un grupo de puertos EtherChannel deCapa 2 que use interfaces F0/1 y F0/2	<pre>S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#interface Port-channel 1 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 56</pre>
Configurar el puerto de acceso del host para laVLAN 30	<pre>S2(config-if)# interface fa0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 30</pre>
Configure port-security en los Access ports	<pre>S2(config-if)#switchport port-security maximum 4</pre>
Asegure todas las interfaces no utilizadas.	<pre>S2(config-if)#interface range fa0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 50 S2(config-if-range)#description Sin uso S2(config-if-range)#shutdown S2(config-if-range)#interface range fa0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 50 S2(config-if-range)#description Sin uso S2(config-if-range)#shutdown</pre>

Fuente: Autor

- Creación de las VLAN, desde la consola en el modo privilegiado, posteriormente en la configuración global con el siguiente comando se proceden a crear las diferentes vlan:

S2(config)#vlan 20

Creación de la vlan 20

S2(config-vlan)#name Docentes

Asignación de Nombre

Se repite el mismo procedimiento para las vlan, 30- Estudiantes, 40- Invitados, 50- Usuarios, 56-Nativa

- Creación de troncos 802.1Q que utilicen la VLAN 56 nativa en la interfaz fa0/1 y fa0/1-2

S2(config-if)#interface range fa0/1-2 **Se accede al rango con las dos interfaces a modificar**

S2(config-if-range)# shutdown **Se apaga el grupo de la interface para realizar la configuracion**

S2(config-ifrange)#switchport trunk encapsulation dot1q **Se indica al switch que en la Interfaz debe usar la encapsulacion IEEE 802.1Q en las tramas, cuando esta este configurada como troncal, Se cambia la interface a modo de enlace control permanente**

S2(config-if-range)#switchport trunk native vlan 56 **Se direcciona el rango de la interface a la VLAN 56 native**

- Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2

S2(config)#interface range fa0/1-2 **Se accede al rango con las dos interfaces a modificar**

S2(config-if-range)#channel-group 1 mode active **Luego de que se crea el grupo se realiza su activación**

S2(config-if-range)#interface Port-channel 1 **Se accede a la interface del canal**

S2(config-if)#switchport trunk encapsulation dot1q **Se indica al switch que en la Interfaz debe usar la encapsulacion IEEE 802.1Q en las tramas, cuando esta esté configurada como troncal, Se cambia la interface a modo de enlace control permanente**

S2(config-if)#switchport trunk native vlan 56 **Se redirecciona el rango de la interface a la VLAN 56 native**

- Configuracion del puerto de acceso del host para la VLAN 30

S2(config-if)#interface fa0/18 **Se accede a la interface**

S2(config-if)#switchport mode access **Se configura el modo operativo de enlace trunca en una interfaz de capa 2**

S2(config-if)#switchport access vlan 30 **Se redireccióna la interfaz a la vlan30**

- configuración de seguridad en los puertos de acceso

S2(config-if)#switchport port-security maximum 4 **Se configura la seguridad de los puertos de la interface para que el acceso solo permita 4 direcciones Mac.**

- Interfaces no utilizadas

se aseguran todas las interfaces sin usar, mediante una serie de rangos (fa0/3-17, fa0/19-24, g0/1-2) para así re direccionarlas a la vlan 50-Usuarios, se asigna una descripción: "sin uso" y finalmente se apagan

```
S2(config-if)#interface range fa0/3-17
```

```
S2(config-if-range)#switchport mode access
```

```
S2(config-if-range)#switchport access vlan 50
```

```
S2(config-if-range)#description Sin uso
```

```
S2(config-if-range)#shutdown
```

```
S2(config-if-range)#interface range fa0/19-24
```

```
S2(config-if-range)#switchport mode access
```

```
S2(config-if-range)#switchport access vlan 50
```

```
S2(config-if-range)#description Sin uso
```

```
S2(config-if-range)#shutdown
```

```
S2(config-if-range)#interface range g0/1-2
```

```
S2(config-if-range)#switchport mode access
```

```
S2(config-if-range)#switchport access vlan 50
```

```
S2(config-if-range)#description Sin uso
```

```
S2(config-if-range)#shutdown
```

Parte 2: Configurar soporte de host

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16. Configurar soporte de host en R1

Tarea	Especificación
Configure Default Routing	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0
Configurar IPv4 DHCP para VLAN 20	R1(config)#ip dhcp excluded- address 10.37.8.3 10.37.8.52 R1(config)#ip dhcp pool vlan20- Docentes R1(dhcp-config)#network 10.37.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.37.8.1 R1(dhcp-config)#domain-name unad-ccna-sa.net R1(dhcp-config)#exit
Configurar DHCP IPv4 para VLAN 30	R1(config)#ip dhcp excluded- address 10.37.8.65 10.37.8.84 R1(config)#ip dhcp pool vlan30- Estudiantes R1(dhcp-config)#network 10.37.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.37.8.65 R1(dhcp-config)#domain-name unad-ccna-sb.net R1(dhcp-config)#exit

Fuente: Autor

- Configure Default Routing

Asignación de las rutas predeterminadas IPv4 y IPv6, las cuales direccionan el tráfico a la interfaz LoopBack 0

```
R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
```

```
R1(config)#ipv6 route ::/0 loopback 0
```

Configurar IPv4 DHCP para VLAN 20

R1(config)#ip dhcp excluded-address 10.37.8.3 10.37.8.52 **Comando para excluir el rango de direcciones establecidas**

R1(config)#ip dhcp pool vlan20-Docentes **Configuracion de DHCP en la vlan 20- docentes**

R1(dhcp-config)#network 10.37.8.0 255.255.255.192 **Red y mascara de sub red de la sub interface g0/0/1.20**

R1(dhcp-config)#default-router 10.37.8.1 **Puerta de enlace preterminada**

R1(dhcp-config)#domain-name unad-ccna-sa.net **Nombre del dominio**

- Configurar DHCP IPv4 para VLAN 30

R1(config)#ip dhcp excluded-address 10.37.8.65 10.37.8.84 **Comando para excluir el rango de direcciones establecidas**

R1(config)#ip dhcp pool vlan30-Estudiantes **Configuracion de DHCP en la vlan 20- docentes**

R1(dhcp-config)#network 10.37.8.64 255.255.255.224 **Red y mascara de sub red de la sub interface g0/0/1.30**

R1(dhcp-config)#default-router 10.37.8.65 **Puerta de enlace preterminada**

R1(dhcp-config)#domain-name unad-ccna-sb.net **Nombre del dominio**

Paso 2: Configurar los servidores

Configure los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, registre las configuraciones de red del host con el comando **ipconfig /all**.

Tabla 17. Configuración de red de PC-A

Configuración de red de PC-A	
Descripción	Dirección DHCP
Dirección física	00E0.B069.3E8C
Dirección IP	10.37.8.2
Máscara de subred	255.255.255.192
Gateway predeterminado	10.37.8.1
Gateway predeterminado IPv6	FE80::1

Fuente: Autor

Tabla 18. Configuración de red de PC-B

Configuración de red de PC-B	
Descripción	Dirección por DHCP
Dirección física	0002.1620.219C
Dirección IP	10.37.8.66
Máscara de subred	255.255.255.224
Gateway predeterminado	10.37.8.65
Gateway predeterminado IPv6	FE80::1

Fuente: Autor

Parte 3: Probar y verificar la conectividad de extremo a extremo

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

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 19. Conectividad entre dispositivos

Desde	A		Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.20	IPv4	10.37.8.1 /26	EXITOSO
		IPv6	2001:db8:ac ad:a :1 /64	EXITOSO
	R1, G0/0/1.30	IPv4	10.37.8.65 /27	EXITOSO
		IPv6	2001:db8:ac ad:b :1 /64	EXITOSO
	R1, G0/0/1.40	IPv4	10.37.8.97 /29	EXITOSO
		IPv6	2001:db8:ac ad:c :1 /64	EXITOSO
	S1, VLAN 40	IPv4	10.37.8.98	EXITOSO
		IPv6	2001:db8:ac ad:c :98	EXITOSO
	S2, VLAN 40	IPv4	10.37.8.99 /29	EXITOSO
		IPv6	2001:db8:ac ad:c :99 /64	EXITOSO
	PC-B	IPv4	10.37.8.66	EXITOSO
		IPv6	2001:db8:acad :b :50 /64	EXITOSO
	R1 Loopback0	IPv4	209.165.201 .1 /27	EXITOSO
		IPv6	2001:db8:ac ad:209: :1	EXITOSO

			/64	
PC-B	R1 Loopback0	IPv4	209.165.201 .1 /27	EXITOSO
		IPv6	2001:db8:ac ad:209: :1 /64	EXITOSO
	R1, G0/0/1.20	IPv4	10.37.8.1 /26	EXITOSO
		IPv6	2001:db8:ac ad:a: :1 /64	EXITOSO
	R1, G0/0/1.30	IPv4	10.37.8.65 /27	EXITOSO
		IPv6	2001:db8:ac ad:b: :1 /64	EXITOSO
	R1, G0/0/1.40	IPv4	10.37.8.97 /29	EXITOSO
		IPv6	2001:db8:ac ad:c: :1 /64	EXITOSO
	S1, VLAN 40	IPv4	10.37.8.98	EXITOSO
		IPv6	2001:db8:ac ad:c: :98	EXITOSO
	S2, VLAN 40	IPv4	10.37.8.99	EXITOSO
		IPv6	2001:db8:ac ad:c: :99	EXITOSO

Fuente: Autor

- Ping PC-A a R1, G0/0/1.20 IPV4 10.37.8.1

Figura 10. Ping PC-A a R1, G0/0/1.20 IPV4

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.37.8.1

Pinging 10.37.8.1 with 32 bytes of data:

Reply from 10.37.8.1: bytes=32 time<lms TTL=255
Reply from 10.37.8.1: bytes=32 time<lms TTL=255
Reply from 10.37.8.1: bytes=32 time<lms TTL=255
Reply from 10.37.8.1: bytes=32 time<lms TTL=255

Ping statistics for 10.37.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autor

En la Figura 10, se comprueba la conectividad que se tiene desde el PC-A hasta el a R1, G0/0/1.20, en su dirección Ipv4, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-A a R1, G0/0/1.20 IPV6 2001:db8:acad:a::1

Figura 11. Ping PC-A a R1, G0/0/1.20 IPV6 2001:db8:acad:a::1

```
C:\>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<lms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<lms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=2ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<lms 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 = 2ms, Average = 0ms
```

Fuente: Autor

En la Figura 11, se comprueba la conectividad que se tiene desde el PC-A hasta el R1, G0/0/1.20, en su dirección Ipv6, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-A a R1, G0/0/1.30 IPV4 10.37.8.65

Figura 12. Ping PC-A a R1, G0/0/1.30 IPV4 10.37.8.65

```
C:\>ping 10.37.8.65

Pinging 10.37.8.65 with 32 bytes of data:

Reply from 10.37.8.65: bytes=32 time<1ms TTL=255
Reply from 10.37.8.65: bytes=32 time<1ms TTL=255
Reply from 10.37.8.65: bytes=32 time<1ms TTL=255
Reply from 10.37.8.65: bytes=32 time<1ms TTL=255

Ping statistics for 10.37.8.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Autor

En la Figura 12, se comprueba la conectividad que se tiene desde el PC-A hasta el R1, G0/0/1.30, en su dirección Ipv4, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-A a R1, G0/0/1.30 IPV6 2001:db8:acad:b::1

Figura 13. Ping PC-A a R1, G0/0/1.30 IPV6 2001:db8:acad:b::1

```
C:\>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<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=2ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<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 = 2ms, Average = 0ms
```

Fuente: Autor

En la Figura 13, se comprueba la conectividad que se tiene desde el PC-A hasta el a R1, G0/0/1.30, en su dirección Ipv6, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-A a R1, G0/0/1.40 IPV4 10.37.8.97

Figura 14. Ping PC-A a R1, G0/0/1.40 IPV4 10.37.8.97

```
C:\>ping 10.37.8.97

Pinging 10.37.8.97 with 32 bytes of data:

Reply from 10.37.8.97: bytes=32 time<1ms TTL=255
Reply from 10.37.8.97: bytes=32 time<1ms TTL=255
Reply from 10.37.8.97: bytes=32 time<1ms TTL=255
Reply from 10.37.8.97: bytes=32 time<1ms TTL=255

Ping statistics for 10.37.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autor

En la Figura 14, se comprueba la conectividad que se tiene desde el PC-A hasta el a R1, G0/0/1.24, en su dirección Ipv4, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-A a R1, G0/0/1.40 IPV6 2001:db8:acad:c::1

Figura 15. Ping PC-A a R1, G0/0/1.40 IPV6 2001:db8:acad:c::1

```
C:\>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<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<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
```

Fuente: Autor

En la Figura 15, se comprueba la conectividad que se tiene desde el PC-A hasta el a R1, G0/0/1.40, en su dirección Ipv6, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-A a S1, VLAN 40 IPv4 10.37.8.98

Figura 16. Ping PC-A a S1, VLAN 40 IPv4 10.37.8.98

```
C:\>ping 10.37.8.98

Pinging 10.37.8.98 with 32 bytes of data:

Reply from 10.37.8.98: bytes=32 time<1ms TTL=254
Reply from 10.37.8.98: bytes=32 time<1ms TTL=254
Reply from 10.37.8.98: bytes=32 time=1ms TTL=254
Reply from 10.37.8.98: bytes=32 time<1ms TTL=254

Ping statistics for 10.37.8.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Fuente: Autor

En la Figura 16, se comprueba la conectividad que se tiene desde el PC-A hasta el a S1, VLAN 40, en su dirección Ipv4, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-A a S1, VLAN 40 IPv6 2001:db8:acad:c: :98

Figura 17. Ping PC-A a S1, VLAN 40 IPv6 2001:db8:acad:c: :98

```
C:\>
C:\>ping 2001:db8:acad:c::98

Pinging 2001:db8:acad:c::98 with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::98: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:ACAD:C::98: bytes=32 time<1ms TTL=254
Reply from 2001:DB8:ACAD:C::98: bytes=32 time=11ms TTL=254
Reply from 2001:DB8:ACAD:C::98: bytes=32 time=11ms TTL=254

Ping statistics for 2001:DB8:ACAD:C::98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 5ms
```

Fuente: Autor

En la Figura 17, se comprueba la conectividad que se tiene desde el PC-A hasta el a S1, VLAN 40, en su dirección Ipv6, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-A a S2, VLAN 40 IPv4 10.37.8.99

Figura 18. Ping PC-A a S2, VLAN 40 IPv4 10.37.8.99

```
C:\>ping 10.37.8.99

Pinging 10.37.8.99 with 32 bytes of data:

Reply from 10.37.8.99: bytes=32 time<1ms TTL=254
Reply from 10.37.8.99: bytes=32 time=10ms TTL=254
Reply from 10.37.8.99: bytes=32 time=11ms TTL=254
Reply from 10.37.8.99: bytes=32 time=10ms TTL=254

Ping statistics for 10.37.8.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 7ms

C:\>
```

Fuente: Autor

En la Figura 18, se comprueba la conectividad que se tiene desde el PC-A hasta el a S2, VLAN 40, en su dirección Ipv4, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-A a S2, VLAN 40 IPv6 2001:db8:acad:c: :99

Figura 19. Ping PC-A a S2, VLAN 40 IPv6 2001:db8:acad:c: :99

```
C:\>ping 2001:db8:acad:c::99

Pinging 2001:db8:acad:c::99 with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::99: bytes=32 time<1ms TTL=254
Reply from 2001:DB8:ACAD:C::99: bytes=32 time=10ms TTL=254
Reply from 2001:DB8:ACAD:C::99: bytes=32 time=11ms TTL=254
Reply from 2001:DB8:ACAD:C::99: bytes=32 time=11ms TTL=254

Ping statistics for 2001:DB8:ACAD:C::99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 8ms

C:\>
```

Fuente: Autor

En la Figura 19, se comprueba la conectividad que se tiene desde el PC-A hasta el a S2, VLAN 40, en su dirección Ipv6, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-A a PC-B IPv4 10.37.8.66

Figura 20. Ping PC-A a PC-B IPv4 10.37.8.66

```
C:\>ping 10.37.8.66

Pinging 10.37.8.66 with 32 bytes of data:

Reply from 10.37.8.66: bytes=32 time<lms TTL=127
Reply from 10.37.8.66: bytes=32 time=11ms TTL=127
Reply from 10.37.8.66: bytes=32 time=11ms TTL=127
Reply from 10.37.8.66: bytes=32 time=1ms TTL=127

Ping statistics for 10.37.8.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 5ms

C:\>
```

Fuente: Autor

En la Figura 20, se comprueba la conectividad que se tiene desde el PC-A hasta el al PC-B, en su dirección Ipv4, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-A a PC-B IPv6 2001:db8:acad:b::50

Figura 21. Ping PC-A a PC-B IPv6 2001:db8:acad:b::50

```
C:\>ping 2001:db8:acad:b::50

Pinging 2001:db8:acad:b::50 with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::50: bytes=32 time<lms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=10ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=11ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=11ms TTL=127

Ping statistics for 2001:DB8:ACAD:B::50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 8ms

C:\>
```

Fuente: Autor

En la Figura 21, se comprueba la conectividad que se tiene desde el PC-A hasta el al PC-B, en su dirección Ipv6, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-A a R1 Loopback0 IPv4 209.165.201.1

Figura 22. Ping PC-A a R1 Loopback0 IPv4 209.165.201.1

```
C:\>ping 209.165.201.1

Pinging 209.165.201.1 with 32 bytes of data:

Reply from 209.165.201.1: bytes=32 time<lms TTL=255
Reply from 209.165.201.1: bytes=32 time<lms TTL=255
Reply from 209.165.201.1: bytes=32 time<lms TTL=255
Reply from 209.165.201.1: bytes=32 time<lms 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
```

Fuente: Autor

En la Figura 22, se comprueba la conectividad que se tiene desde el PC-A hasta el R1 Loopback0, en su dirección Ipv4, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-A a R1 Loopback0 IPv6 2001:db8:acad:209::1

Figura 23. Ping PC-A a R1 Loopback0 IPv6 2001:db8:acad:209::1

```
C:\>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=lms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<lms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<lms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<lms 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 = lms, Average = 0ms
```

Fuente: Autor

En la Figura 23, se comprueba la conectividad que se tiene desde el PC-A hasta el R1 Loopback0, en su dirección Ipv6, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-B a R1 Loopback0 IPv4 209.165.201.1

Figura 24. Ping PC-B a R1 Loopback0 IPv4 209.165.201.1

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 209.165.201.1

Pinging 209.165.201.1 with 32 bytes of data:

Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<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
```

Fuente: Autor

En la Figura 24, se comprueba la conectividad que se tiene desde el PC-B hasta el R1 Loopback0, en su dirección Ipv4, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-B a R1 Loopback0 IPv6 2001:db8:acad:209::1

Figura 25. Ping PC-B a R1 Loopback0 IPv6 2001:db8:acad:209::1

```
C:\>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<1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time=12ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<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 = 12ms, Average = 3ms
```

Fuente: Autor

En la Figura 25, se comprueba la conectividad que se tiene desde el PC-B hasta el R1 Loopback0, en su dirección Ipv6, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-B a R1, G0/0/1.20 IPv4 10.37.8.1

Figura 26. Ping PC-B a R1, G0/0/1.20 IPv4 10.37.8.1

```
C:\>ping 10.37.8.1

Pinging 10.37.8.1 with 32 bytes of data:

Reply from 10.37.8.1: bytes=32 time=20ms TTL=255
Reply from 10.37.8.1: bytes=32 time<1ms TTL=255
Reply from 10.37.8.1: bytes=32 time<1ms TTL=255
Reply from 10.37.8.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.37.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 20ms, Average = 5ms
```

Fuente: Autor

En la Figura 26, se comprueba la conectividad que se tiene desde el PC-B hasta el a R1, G0/0/1.20, en su dirección Ipv4, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-B a R1, G0/0/1.20 IPv6 2001:db8:acad:a::1

Figura 27. Ping PC-B a R1, G0/0/1.20 IPv6 2001:db8:acad:a::1

```
C:\>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<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<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<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 = 0ms, Average = 0ms
```

Fuente: Autor

En la Figura 27, se comprueba la conectividad que se tiene desde el PC-B hasta el a R1, G0/0/1.20, en su dirección Ipv6, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-B a R1, G0/0/1.30 IPv4 10.37.8.65

Figura 28. Ping PC-B a R1, G0/0/1.30 IPv4 10.37.8.65

```
C:\>ping 10.37.8.65

Pinging 10.37.8.65 with 32 bytes of data:

Reply from 10.37.8.65: bytes=32 time<1ms TTL=255
Reply from 10.37.8.65: bytes=32 time<1ms TTL=255
Reply from 10.37.8.65: bytes=32 time<1ms TTL=255
Reply from 10.37.8.65: bytes=32 time<1ms TTL=255

Ping statistics for 10.37.8.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autor

En la Figura 28, se comprueba la conectividad que se tiene desde el PC-B hasta el a R1, G0/0/1.30, en su dirección Ipv4, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-B a R1, G0/0/1.30 IPv6 2001:db8:acad:b::1

Figura 29. Ping PC-B a R1, G0/0/1.30 IPv6 2001:db8:acad:b::1

```
C:\>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=10ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<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 = 10ms, Average = 2ms
```

Fuente: Autor

En la Figura 29, se comprueba la conectividad que se tiene desde el PC-B hasta el a R1, G0/0/1.30, en su dirección Ipv6, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-B a R1, G0/0/1.40 IPv4 10.37.8.97

Figura 30. Ping PC-B a R1, G0/0/1.40 IPv4 10.37.8.97

```
C:\>ping 10.37.8.97

Pinging 10.37.8.97 with 32 bytes of data:

Reply from 10.37.8.97: bytes=32 time<1ms TTL=255
Reply from 10.37.8.97: bytes=32 time<1ms TTL=255
Reply from 10.37.8.97: bytes=32 time<1ms TTL=255
Reply from 10.37.8.97: bytes=32 time<1ms TTL=255

Ping statistics for 10.37.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autor

En la Figura 30, se comprueba la conectividad que se tiene desde el PC-B hasta el a R1, G0/0/1.40, en su dirección Ipv4, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-B a R1, G0/0/1.40 IPv6 2001:db8:acad:c::1

Figura 31. Ping PC-B a R1, G0/0/1.40 IPv6 2001:db8:acad:c::1

```
C:\>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<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<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
```

Fuente: Autor

En la Figura 31, se comprueba la conectividad que se tiene desde el PC-B hasta el a R1, G0/0/1.40, en su dirección Ipv6, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-B a S1, VLAN 40 IPv4 10.37.8.98

Figura 32. Ping PC-B a S1, VLAN 40 IPv4 10.37.8.98

```
C:\>ping 10.37.8.98

Pinging 10.37.8.98 with 32 bytes of data:

Reply from 10.37.8.98: bytes=32 time<1ms TTL=254
Reply from 10.37.8.98: bytes=32 time=12ms TTL=254
Reply from 10.37.8.98: bytes=32 time=12ms TTL=254
Reply from 10.37.8.98: bytes=32 time=10ms TTL=254

Ping statistics for 10.37.8.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 8ms
```

Fuente: Autor

En la Figura 32, se comprueba la conectividad que se tiene desde el PC-B hasta el a S1, VLAN 40, en su dirección Ipv4, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-B a S1, VLAN 40 IPv6 2001:db8:acad:c::98

Figura 33. Ping PC-B a S1, VLAN 40 IPv6 2001:db8:acad:c::98

```
C:\>ping 2001:db8:acad:c::98

Pinging 2001:db8:acad:c::98 with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::98: bytes=32 time=70ms TTL=254
Reply from 2001:DB8:ACAD:C::98: bytes=32 time=11ms TTL=254
Reply from 2001:DB8:ACAD:C::98: bytes=32 time=17ms TTL=254
Reply from 2001:DB8:ACAD:C::98: bytes=32 time=11ms TTL=254

Ping statistics for 2001:DB8:ACAD:C::98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 70ms, Average = 27ms
```

Fuente: Autor

En la Figura 33, se comprueba la conectividad que se tiene desde el PC-B hasta el a S1, VLAN 40, en su dirección Ipv6, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-B a S2, VLAN 40 IPv4 10.37.8.99

Figura 34. Ping PC-B a S2, VLAN 40 IPv4 10.37.8.99

```
C:\>ping 10.37.8.99

Pinging 10.37.8.99 with 32 bytes of data:

Reply from 10.37.8.99: bytes=32 time<1ms TTL=254
Reply from 10.37.8.99: bytes=32 time=11ms TTL=254
Reply from 10.37.8.99: bytes=32 time=12ms TTL=254
Reply from 10.37.8.99: bytes=32 time=30ms TTL=254

Ping statistics for 10.37.8.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 30ms, Average = 13ms

C:\>
```

Fuente: Autor

En la Figura 34, se comprueba la conectividad que se tiene desde el PC-B hasta el a S2, VLAN 40, en su dirección Ipv4, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

- Ping PC-B a S2, VLAN 40 IPv6 2001:db8:acad:c :99

Figura 35. Ping PC-B a S2, VLAN 40 IPv6 2001:db8:acad:c :99

```
C:\>ping 2001:db8:acad:c::99

Pinging 2001:db8:acad:c::99 with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::99: bytes=32 time=10ms TTL=254
Reply from 2001:DB8:ACAD:C::99: bytes=32 time=10ms TTL=254
Reply from 2001:DB8:ACAD:C::99: bytes=32 time=11ms TTL=254
Reply from 2001:DB8:ACAD:C::99: bytes=32 time=12ms TTL=254

Ping statistics for 2001:DB8:ACAD:C::99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 12ms, Average = 10ms
```

Fuente: Autor

En la Figura 35, se comprueba la conectividad que se tiene desde el PC-B hasta el a S2, VLAN 40, en su dirección Ipv6, realizando un envío de paquetes el cual da como resultado 100% de envío y recepción.

CONCLUSIONES

A través del presente informe, se ha llegado a comprobar la importancia que radica en la planeación y estructuración de una red, teniendo como punto de partida que para que la conexión entre dispositivos funcione exitosamente como en la práctica anterior se debe realizar el direccionamiento de IP que cumpla con las normas establecidas

De igual manera en la configuración de los dispositivos, se deben cumplir con cada uno de los requerimientos puesto que de no ser así el dispositivo no funcionara de manera correcta, como por ejemplo si no se asigna la dirección IP correcta en el puerto destinado para esa conexión no tendremos comunicación entre dispositivos, es decir el ping no será exitoso.

Al realizar la configuración de los diferentes dispositivos que forman parte de los dos escenarios de red expuestos en este documento, se observó la importancia que trae consigo la correcta configuración de los servidores locales y los remotos mediante los protocolos SSH, así mismo la conectividad física entre las interfaces lógicas y como un ítem de importancia asignarle una contraseña de acceso a los dispositivos con el fin de brindarles la seguridad suficiente para su correcto funcionamiento.

Para concluir con la realización de este informe en el cual se les da solución a dos estudios de caso bajo el uso de tecnología CISCO, se debe tener claro que un factor clave para que estas topologías de red funcionen es elegir de manera correcta los dispositivos a utilizar, puesto que dentro de este simulador (Cisco Packet Tracer) cada dispositivo tiene sus funciones específicas es decir que algunos no permiten ciertos comandos o no son compatibles, es por esta razón que se debe tener claro cuáles serán los requerimientos de la red y luego si determinar cuáles serán los dispositivos a utilizar.

BIBLIOGRAFIA

ÁLVARO, M. Tipos de Banner en Dispositivos Cisco. [sitio web]. [Consultado 23 de noviembre de 2022]. Disponible en: <https://netwgeeks.com/tipos-de-banner-en-dispositivos-cisco/>

CISCO. Asignación de direcciones IPv4. Introducción a las redes. [sitio web]. [Consultado 22 de agosto de 2022]. Disponible en: <https://contenthub.netacad.com/itn/11.0.1>

CISCO. Información sobre los modos de LoopBack en routers de Cisco. [sitio web]. [Consultado 19 de noviembre de 2022]. Disponible en: https://www.cisco.com/c/es_mx/support/docs/asynchronous-transfer-modeatm/permanent-virtual-circuits-pvc-switched-virtual-circuits-svc/6337atmloopback.html

DE LUZ, Sergio. VLANs: Qué son, tipos y para qué sirven. [sitio web]. [Consultado 19 de noviembre de 2022]. Disponible en: <https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/>

GARCIA, Flores. Que son las líneas vty Cisco?. [sitio web]. [Consultado 19 de noviembre de 2022]. Disponible en: <https://la-respuesta.com/preguntas-comunes/Que-son-las-lineas-vty-Cisco/>

GUACA, N. Configuración básica de: Switches. [sitio web]. [Consultado 03 de octubre de 2022] Disponible en: <http://hdl.handle.net/10596/23215>

LOBATO, G. CURSO 7-1 Explicación de protocolo OSPF. [Archivo de Vídeo]. [Consultado el 17 de noviembre de 2022]. Disponible en: https://www.youtube.com/watch?v=dwT5du44t_8

MICROSOFT. Protocolo de configuración dinámica de host (DHCP). [sitio web]. [Consultado el 17 de noviembre de 2022]. Disponible en: <https://learn.microsoft.com/es-es/windows-server/networking/technologies/dhcp/dhcp-top>

WALTON, Alex. Qué es default Gateway. [sitio web]. [Consultado el 17 de noviembre de 2022]. Disponible en: <https://ccnadesdecero.es/que-es-gateway/>

ANEXOS

Link de descarga Escenario 1:

<https://drive.google.com/file/d/1vogfHN4X1aGBXX8jcOKFHgC9mWw4FDrl/view?usp=sharing>

Link de descarga Escenario 2:

https://drive.google.com/file/d/1qdO5vjgo4Js-KqLUET-i11Dj5WF-ImFv/view?usp=share_link