

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

YILMAR GILDARDO RIVERA VELA

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

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

YILMAR GILDARDO RIVERA VELA

Diplomado de opción de grado presentado para optar el título de Ingeniero de
Sistemas

PAULITA FLOR SALAZAR

Director

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

INIRIDA

2022

NOTA DE ACEPTACION

Firma del Presidente del Jurado

Firma del Jurado

Firma del jurado

Inírida, 27 de noviembre de 2022

AGRADECIMIENTOS

Quiero dar las gracias a Dios principalmente, gracias al universo entero y a todas las personas que han hecho parte de este camino, siempre basado en un objetivo principal muy claro y es el de convertirme en ingeniero de sistemas.

Quiero darles las gracias a mis padres Gildardo Rivera y María Vela porque han sido un ejemplo, a mi esposa Yuri Bibiana Aguirre, hermosa mujer con carácter que ha sido mi apoyo y compañera de vida, a mis dos bellas princesas Sara maría e Ivanna Sofía que han sido mi luz y mi fuerza para continuar en esta senda, mil y mil gracias porque la abundancia en mi vida es infinita e ilimitada. Gracias, gracias.

CONTENIDO

AGRADECIMIENTOS.....	4
CONTENIDO.....	5
LISTA DE TABLAS.....	7
LISTA DE FIGURAS.....	8
RESUMEN.....	10
ABSTRACT.....	11
GLOSARIO.....	12
INTRODUCCION.....	13
1. DESARROLLO ESCENARIO 1.....	14
1.1. DESARROLLO ESQUEMA DE DIRECCIONAMIENTO IP.....	15
1.2. CONFIGURE ASPECTOS BÁSICOS.....	17
1.2.1. LAS TAREAS DE CONFIGURACIÓN DE S1.....	19
1.2.2. CONFIGURAR LOS EQUIPO.....	24
1.3. PROBAR Y VERIFICAR LA CONECTIVIDAD DE EXTREMO A EXTREMO.....	27
2. DESARROLLO ESCENARIO 2.....	33
2.1 INICIALIZAR Y RECARGAR Y CONFIGURAR ASPECTOS BÁSICOS DE LOS DISPOSITIVOS.....	36
2.1.1. CONFIGURAR R1.....	38
2.1.2. CONFIGURE S1 Y S2.....	41
2.2. CONFIGURACIÓN DE LA INFRAESTRUCTURA DE RED (VLAN, TRUNKING, ETHERCHANNEL).....	47
2.2.1. CONFIGURAR S1.....	47
2.2.2. CONFIGURE EL S2.....	50
2.3. CONFIGURAR SOPORTE DE HOST.....	53
2.3.1. CONFIGURE R1.....	53
2.3.2 CONFIGURAR LOS SERVIDORES.....	55
2.4. PROBAR Y VERIFICAR LA CONECTIVIDAD DE EXTREMO A EXTREMO.....	57
CONCLUSIONES.....	72

BIBLIOGRAFIA.....73
ANEXOS.....74

LISTA DE TABLAS

ESCENARIO 1

Tabla 1. Direccionamiento Escenario 1-----	15
Tabla 2. Configuración router R1-----	17
Tabla 3. Configuración switch S1-----	21
Tabla 4. Configuración ipv4 PC-A-----	24
Tabla 5. Configuración ipv4 PC-B-----	25
Tabla 6. Verificación de conectividad dispositivos de red-----	27

ESCENARIO 2

Tabla.7 nombre de las VLAN-----	36
Tabla 8. Tabla de asignación de direcciones-----	36
Tabla 9. Configuración router R1-----	37
Tabla 10. Configuración Switch S1 y S2-----	42
Tabla 11. Configuración S1-----	48
Tabla 12. Configuración S2-----	51
Tabla 13. Configuración router R1-----	54
Tabla 14. Configuración de red de PC-A-----	56
Tabla 15. Configuración de PC-B-----	57
Tabla 16. Probar y verificar la conectividad de extremo a extremo-----	58

LISTA DE FIGURAS

DESARROLLO ESCENARIO 1

Figura 1. Topología Escenario 1-----	14
Figura 2. Comando ipconfig /all PC-A-----	24
Figura 3. Comando ipconfig /all-----	26
Figura 4. Ping del PCA a la IP 172.92.3.94 R1 G0/0/0- Última dirección de host de la subred LAN2-----	27
Figura 5. Ping del PCA a la IP 172.92.3.62 R1 G0/0/1- Última dirección de host de la subred LAN1-----	27
Figura 6. ping del PCA a la IP 172.92.3.2 S1 VLAN -----	28
Figura 7. Ping del PCA a la IP 172.92.3.2 S1 PC-B-----	28
Figura 8. Ping del PCB a la IP 172.92.3.94 R1 G0/0/0- Última dirección de host de la subred LAN2-----	29
Figura 9. ping del PCB a la IP 172.92.3.62 R1 G0/0/1- Última dirección de host de la subred LAN1-----	29
Figura 10. Ping del PCB a la IP 172.92.3.2 S1 VLAN 1-----	30
Figura 11. ping del PCB a la IP 172.92.3.10 S1 PC-A-----	30
DESARROLLO ESCENARIO 2	
Figura 12. Topología Escenario 2-----	33
Figura 13. Ping desde PC-A a R1, G0/0/1.20-----	58
Figura 14. Ping desde PC-A a R1, G0/0/1.20 IPv6 2001:db8:acad:a :1-----	58
Figura 15. Ping desde PC-A a R1, G0/0/1.30 Dirección IP 10.19.8.65-----	59
Figura 16. Ping desde PC-A a R1, G0/0/1.30 IPv6 2001:db8:acad:b::1-----	59
Figura 17. Ping desde PC-A a R1, G0/0/1.40 Dirección 10.19.8.97-----	59
Figura 18. Ping desde PC-A a R1, G0/0/1.40 IPv6 2001:db8:acad:c::1-----	60
Figura 19. Ping desde PC-A a S1, VLAN 40 Dirección 10.19.8.98-----	60
Figura 20. Ping desde PC-A a S1 IPv6, VLAN 40-----	61
Figura 21. Ping desde PC-A a S2, VLAN 40-----	61
Figura 22. Ping desde PC-A a S2 IPv6, VLAN 40-----	61

Figura 23. Ping desde PC-A a PC-B, Dirección IP 10.92.8.85-----	61
Figura 24. Ping desde PC-A a PC-B, IPv6 2001:db8:acad:b: :50-----	62
Figura 25. Ping desde PC-A a R1, Bucle 0 Dirección 209.165.201.1-----	62
Figura 26. Ping desde PC-A a R1, Bucle 0 IPv6, 2001:db8:acad:209: :1-----	63
Figura 27. Ping desde PC-B a R1, Bucle 0 Dirección, 209.165.201.1-----	63
Figura 28. Ping desde PC-B a R1, Bucle 0 IPv6 2001:db8:acad:209: :1-----	64
Figura 29. Ping desde PC-B a R1, G0/0/1.20 Dirección 10.19.8.1-----	64
Figura 30. Ping desde PC-B a R1, G0/0/1.20 IPv6 2001:db8:acad:a: :1-----	65
Figura 31. Ping desde PC-B a R1, G0/0/1.30 Dirección IPv4 10.19.8.65-----	65
Figura 32. Ping desde PC-B a R1, G0/0/1.30 IPv6 2001:db8:acad:b: :1-----	65
Figura 33. Ping desde PC-B a R1, G0/0/1.40 Dirección IPv4 10.19.8.97-----	66
Figura 34. Ping desde PC-B a R1, G0/0/1.40 IPv6 2001:db8:acad:c: :1-----	66
Figura 35. Ping desde PC-B a S1, VLAN 40 Dirección 10.19.8.98-----	66
Figura 36. Ping desde PC-B a S1, VLAN 40 IPv6 2001:db8:acad:c: :98-----	67
Figura 37. Ping desde PC-B a S2, VLAN 40 Dirección 10.19.8.99-----	68
Figura 38. Ping de PC-B a S2, VLAN 40 IPv6 2001:db8:acad:c: :99-----	68

RESUMEN

En este primer escenario vamos a identificar y a desarrollar simulaciones de conectividad básica en una red local, mediante la configuración inicial de dispositivos y terminales. Con su respectivo control de seguridad para el acceso al router y los switches, el tipo de cableado que se utilizara, su configuración de direccionamiento IPv4 y configuración de redes LAN, a través de la simulación de escenarios gracias a la herramienta Cisco Packet Tracer, nos ayudara a interpretar la comunicación de datos mediante pruebas que ayudaran a validar su perfecta función.

En el segundo escenario también se realizara una configuración de dispositivos de una red pequeña. Donde se manejara la configuración de un router y se creara rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0, se configuraran dos switches y dos equipos que admitan tanto la conectividad IPv4 también donde se cree un grupo DHCP para VLAN, como IPv6 para los hosts soportados. El router y los switches también deben administrarse de forma segura. Configuraré el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Palabras clave: Loopback, Etherchannel, Dhcp, Enrutamiento, port-security, Redes.

ABSTRACT

In this first scenario we are going to identify and develop simulations of basic connectivity in a local network, through the initial configuration of devices and terminals. With its respective security control for access to the router and switches, the type of cabling to be used, its IPv4 addressing configuration and LAN network configuration, through the simulation of scenarios thanks to the Cisco Packet Tracer tool, we will help to interpret the communication of data through tests that will help to validate its perfect function.

In the second scenario, a configuration of devices of a small network will also be carried out. Where the configuration of a router will be handled and default routes will be created for IPv4 and IPv6 that direct the traffic to the Loopback 0 interface, two switches and two devices that support both IPv4 connectivity will also be configured where a DHCP group for VLANs will be created, as IPv6 for supported hosts. The router and switches must also be managed securely. You will configure routing between VLANs, DHCP, Etherchannel, and port-security.

Keywords: Loopback, Etherchannel, Dhcp, Routing, port-security, Networks.

GLOSARIO

Interfaz de línea de comandos o CLI: Una interfaz de línea de comandos (CLI) es una interfaz de usuario (UI) basada en texto que se utiliza para ver y administrar archivos de computadora.¹

Dirección MAC: Es el identificador único asignado por el fabricante a una pieza de hardware de red (como una tarjeta inalámbrica o una tarjeta Ethernet). «MAC» significa Media Access Control, y cada código tiene la intención de ser único para un dispositivo en particular.²

Capa de aplicación: Capa 7 del modelo OSI; proporciona autenticación, privacidad y restricción de información a los usuarios.³

Dirección IP (protocolo de Internet): Es la que señala que un computador dentro de una red puede recibir información: cada proveedor del servicio de internet asigna una dirección IP a los computadores conectados, dirección de protocolo.⁴

Enrutador: Dispositivo de red que dirige o enruta paquetes a través de las redes. Un enrutador funciona con una dirección de mensajes IP, a fin de determinar la mejor ruta hacia su destino.⁵

¹ ROUSE, Margaret. Interfaz –de- línea- de- comandos-o-CLI (2000).

²MCCANCE, Shaun. Términos-y-consejos-sobre-redes (2010).

³ FUNG, Jacinto. Redes Informáticas: Protocolos de Comunicación, Protocolo de Aplicación y Software. 2da. Edición (2019).

⁴ AVILA, Raul. El bit a las redes sociales (2019).

⁵ TANENBAUN, Andrew s. La capa de red de internet (2003)

INTRODUCCION

Se da inicio a este diplomado y profundización para la comprensión fundamental de la creación, operación y mantenimiento de redes, implementando simulaciones de red usando Packet Tracer y prácticas de laboratorio smartlab. Que nos ayudaran a la comprensión y el desarrollo de dos escenarios propuestos a continuación:

En el escenario 1 se realizara la configuración de una red local, donde se maneja la configuración IPv4 para los switches, el router y las LAN propuestas, con sus respectivas configuraciones de seguridad para cada una de estas LAN tendrán especificaciones en sus hosts de direccionamiento, sus configuraciones de seguridad de acceso a sus consolas, esto con la finalidad de mitigar que algún usuario intruso pueda ingresar y sustraer información.

En el escenario 2 también se realizara una configuración de red local pero a diferencia del escenario 1, se maneja configuración que acepten IPv4 y configuración IPv6 para los switches, el router y las LAN propuestas, su respectivo enrutamiento entre VLAN, DHCP, Etherchannel y port-security que también se deben administrar forma segura con sus respectivas configuraciones de seguridad de acceso a sus consolas.

1. DESARROLLO ESCENARIO 1

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos, diseñar el esquema de direccionamiento IPv4 para las LAN propuestas. El router y el switch también deben administrarse de forma segura.

Figura 1. Topología Escenario 1



Fuente: prueba de habilidades diplomado CCNA.

Para el desarrollo del escenario propuesto se realiza el cálculo de direccionamiento IPv4 en VLSM para poder aprovechar al máximo el espacio de red teniendo en cuenta que la LAN 1 requiere 60 hosts y la LAN 2 requiere 20 hosts.

1.1. DESARROLLO ESQUEMA DE DIRECCIONAMIENTO IP

El espacio de red disponible es 172.92.3.0. Desde allí se parte el subneting con los resultados mostrados en la tabla 1.

Descripción: para esta red local asignamos direcciones ipv4 a las interfaces G0/0/1 y G0/0/0 del router R1, los cuales también estarán configurados con las redes LAN 1, LAN 2, se asignaron direcciones a los respectivos PC1, PC2 donde vamos a desarrollar nuestro esquema.

Tabla 1. Direccionamiento Escenario 1

Item	Requerimiento
Dirección de Red	172.XY.3.0 donde XY corresponde a los últimos dos dígitos de su cédula. 172.92.3.0
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(config)#interface G0/0/1 R1(config-if)#ip address 172.92.3.62 255.255.255.192 R1(config-if)#no shutdown

R1 G0/0/0	Última dirección de host de la subred LAN2 R1(config)#interface G0/0/0 R1(config-if)#ip address 172.92.3.94 255.255.255.224 R1(config-if)#no shutdown
S1 SVI	Segunda dirección de host de la subred LAN1 S1(config)#interface vlan 1 S1(config-if)#ip address 172.92.3.2 255.255.255.192 S1(config-if)#no shutdown
PC-A	Décima dirección de host de la subred LAN1 Red IPv4 numero 172.92.3.10
PC-B	Décima dirección de host de la subred LAN2 Red IPv4 numero 172.92.3.75

Fuente: Autor

1.2. CONFIGURE ASPECTOS BÁSICOS

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

Descripción: una vez realizado el direccionamiento, se procede a realizar la configuración básica de los dispositivos intermediarios, para el router 1 se tuvo en cuenta lo siguiente:

Nombramos al router, también al dominio, se crean claves de acceso modo EXEC privilegiado proporcionando seguridad acceso completo al dispositivo y su configuración a la consola y con longitud mínima para poder mitigar los riesgos de acceso de algún usuario no autorizado, se crea un usuario administrativo en la base de datos local configurando el inicio de sesión en las líneas VTY que acepten únicamente las conexiones SSH, cifrando sus contraseñas, se Configurar un banner MOTD, se realiza configuración de sus interfaces, generamos clave de cifrado.

Tabla 2. Configuración router R1

Tarea	Especificación
Desactivar la búsqueda DNS:	R1(config)#no ip domain-lookup R1(config)#
Nombre del router :	Router(config)#hostname R1
Nombre de dominio :	ccna-sa.com R1(config)#ip domain-name ccna-

	sa.com
Contraseña cifrada para el modo EXEC privilegiado:	ciscoenpass R1(config)#enable password ciscoenpass
Contraseña de acceso a la consola:	Ciscoconpass R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login
Establecer la longitud mínima para las contraseñas	10 caracteres
Crear un usuario administrativo en la base de datos local :	Nombre de usuario: admin Contraseña: admin1pass R1(config)#username admin password admin1pass R1(config)#login local
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 conexiones SSH :	R1(config)#ip ssh version 2 R1(config)#line vty 0 15 R1(config-line)#transport input ssh

	R1(config-line)#login local
Cifrar las contraseñas de texto no cifrado:	R1(config)#service password-encryption
Configurar un banner MOTD: ejecutamos el comando banner motd y entre comillas escribimos “ Cisco Pack Trace,Yilmar Gildardo Rivera Vela,Ingenieria de Sistemas” y damos enter.	Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece. R1(config)#banner motd “ Cisco Pack Trace,Yilmar Gildardo Rivera Vela,Ingenieria de Sistemas”
Configuración de interface G0/0/0:	Establecer la descripción establecer dirección ipv4 activar interfaz. R1(config)#interface gigabitEthernet0/0/0 R1(config-if)#ip address 172.92.3.94 255.255.255.224 R1(config-if)#no shutdown
Configuración de interface G0/0/1	Establecer la descripción establecer dirección ipv4 activar interfaz. R1(config)#interface gigabitEthernet 0/0/1

	<pre>R1(config-if)#ip address 172.92.3.62 255.255.255.192 R1(config-if)#no shutdown</pre>
Generar una clave de cifrado RSA :	<p>Módulo de 1024 bits</p> <pre>R1(config)#crypto key generate rsa</pre> <p>How many bits in the modulus [512]: 1024</p>

Fuente: Autor

1.2.1. LAS TAREAS DE CONFIGURACIÓN DE S1 INCLUYEN LO SIGUIENTE:

Al switch le asignamos nombre también de dominio, se crean claves de acceso modo EXEC privilegiado proporcionando seguridad acceso completo al dispositivo y su configuración a la consola y con longitud mínima para poder mitigar los riesgos de acceso de algún usuario no autorizado, se crea un usuario administrativo en la base de datos local configurando el inicio de sesión en las líneas VTY que acepten únicamente las conexiones SSH, cifrando sus contraseñas, se Configurar un banner MOTD, se realiza configuración de sus interfaces, generamos clave de cifrado.

Tabla 3. Configuración switch S1

Tarea Especificación	Tarea Especificación
Desactivar la búsqueda DNS:	S1(config)#no ip domain-lookup
Nombre del switch:	switch1(config)#hostname S1
Nombre de dominio :	ccna-sa.com S1(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado:	ciscoenpass S1(config)#enable password ciscoenpass
Contraseña de acceso a la consola:	ciscoconpass S1(config)#line 0 S1(config-line)#password ciscoconpass S1(config-line)#login
Apagar todos los puertos sin usar:	F0/1-4, F0/7-24, G0/1-2 S1(config)#interface range fastEthernet 0/1-4

	<pre>S1(config-if-range)#shutdown S1(config)#interface range fastEthernet 0/7-24 S1(config-if-range)#shutdown S1(config)#interface range GigabitEthernet 0/1-2 S1(config-if-range)#shutdown</pre>
Crear un usuario administrativo en la base de datos local:	<pre>Nombre de usuario: admin Contraseña: admin1pass 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</pre>
Configurar las líneas VTY para que acepten únicamente las conexiones SSH:	<pre>S1(config)#ip ssh version 2 S1(config)#line vty 0 15 S1(config-line)#transport input ssh S1(config-line)#login local</pre>
Cifrar las contraseñas de texto no cifrado: ejecutamos el comando conf t	<pre>S1(config)#service password-encryption</pre>

<p>luego ingresamos el comando service password-encryption.</p>	
<p>Configurar un banner MOTD: banner motd y entre comillas escribimos “Cisco Pack Trace,Yilmar Gildardo Rivera Vela,Ingenieria de Sistemas” y damos enter.</p>	<p>Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.</p> <p>S1(config)#banner motd "Cisco Pack Trace,Yilmar Gildardo Rivera Vela,Ingenieria de Sistemas"</p>
<p>Generar una clave de cifrado RSA: Ejecutamos el comando crypto key generate rsa y al final donde dice How many bits in the modulus [512]: agregamos 1024 bits y damos enter.</p>	<p>Módulo de 1024 bits</p> <p>S1(config)#crypto key generate rsa The name for the keys will be: S1.ccna-sa.com</p> <p>How many bits in the modulus [512]: 1024</p>
<p>Configure la interfaz de administración (SVI) en VLAN1:</p>	<p>Establecer la descripción Establecer la dirección IPv4</p> <p>S1(config)#vlan 100 S1(config-vlan)#name SVI S1(config-vlan)#exit S1(config)#interface vlan 100 S1(config-if)#ip address 172.92.3.3</p>

	<pre> 255.255.255.192 S1(config-if)#no shutdown S1(config-if)#ip default-gateway 172.92.3.94 </pre>
--	---

Fuente: Autor

1.2.2. CONFIGURAR LOS EQUIPOS

En este caso se ejecuto el comando ipconfig /all a los equipos PC-A y B, nos muestra un informe de su dirección física, dirección ipv4, mascara de subred y puerta de enlace ipv4 predeterminado.

Tabla 4. Configuración ipv4 PC-A

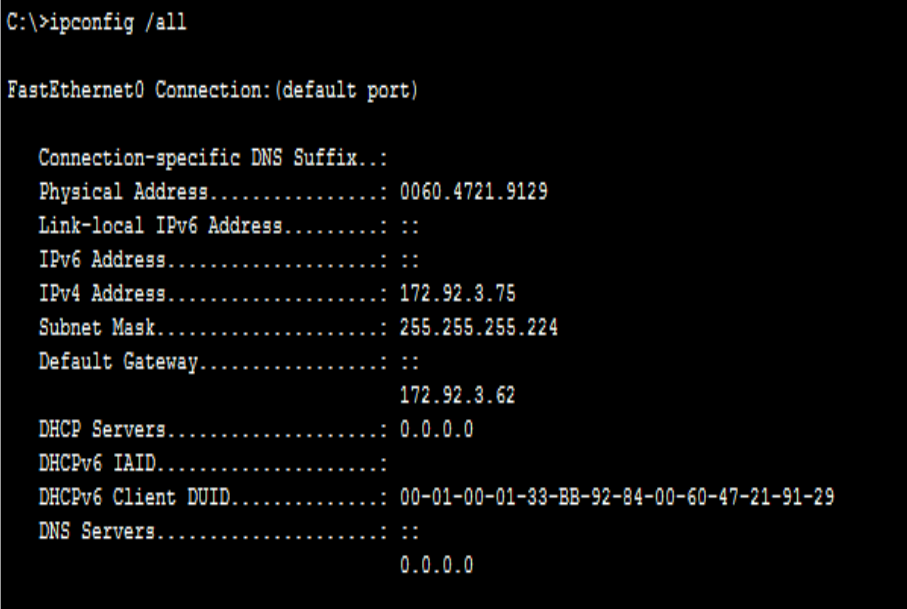
Configuración de red de PC-A	
Descripción	Figura 2. Comando ipconfig /all PC-A

	<pre> C:\>ipconfig /all FastEthernet0 Connection: (default port) Connection-specific DNS Suffix. : Physical Address. : 00D0.5861.EA51 Link-local IPv6 Address. : FE80::2D0:58FF:FE61:EA51 IPv6 Address. : :: IPv4 Address. : 172.92.3.10 Subnet Mask. : 255.255.255.192 Default Gateway. : :: 172.92.3.94 DHCP Servers. : 0.0.0.0 DHCPv6 IAID. : DHCPv6 Client DUID. : 00-01-00-01-5D-1D-18-89-00-D0-58-61-EA-51 DNS Servers. : :: 0.0.0.0 </pre>
Dirección física	00D0.5861.EA51
Dirección IPv4	172.92.3.10
Máscara de subred	255.255.255.192
Puerta de enlace IPv4 predeterminada	172.92.3.94

Fuente: Autor

Tabla 5. Configuración ipv4 PC-B

Configuración de red de PC-B	

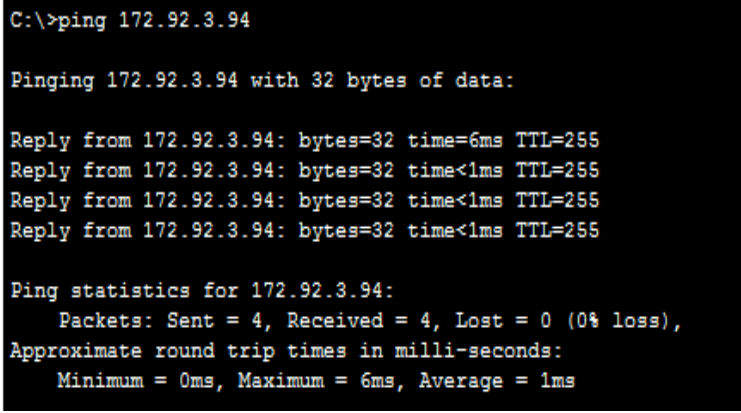
Descripción	<p align="center">Figura 3. comando ipconfig /all PC-B</p>  <pre> C:\>ipconfig /all FastEthernet0 Connection:(default port) Connection-specific DNS Suffix...: Physical Address.....: 0060.4721.9129 Link-local IPv6 Address.....: :: IPv6 Address.....: :: IPv4 Address.....: 172.92.3.75 Subnet Mask.....: 255.255.255.224 Default Gateway.....: :: 172.92.3.62 DHCP Servers.....: 0.0.0.0 DHCPv6 IAID.....: DHCPv6 Client DUID.....: 00-01-00-01-33-BB-92-84-00-60-47-21-91-29 DNS Servers.....: :: 0.0.0.0 </pre>
Dirección física	0060.4721.9129
Dirección IPv4	172.92.3.75
Máscara de subred	255.255.255.224
Puerta de enlace IPv4 predeterminada	172.92.3.62

Fuente: Autor

1.3. PROBAR Y VERIFICAR LA CONECTIVIDAD DE EXTREMO A EXTREMO

Para verificar la correcta implementación del escenario 1, se realizan pruebas de ping desde los dispositivos finales PC a los demás dispositivos de la topología.

Tabla 6. Verificación de conectividad dispositivos de red

Desde	A	Dirección IP	Resultados de ping
PC-A	R1 G0/0/0	172.92.3.94 4	<p>Figura 4. ping del PCA a la IP 172.92.3.94 R1 G0/0/0- Última dirección de host de la subred LAN2</p>  <pre> C:\>ping 172.92.3.94 Pinging 172.92.3.94 with 32 bytes of data: Reply from 172.92.3.94: bytes=32 time=6ms TTL=255 Reply from 172.92.3.94: bytes=32 time<1ms TTL=255 Reply from 172.92.3.94: bytes=32 time<1ms TTL=255 Reply from 172.92.3.94: bytes=32 time<1ms TTL=255 Ping statistics for 172.92.3.94: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 6ms, Average = 1ms </pre>
	R1 G0/0/1	172.92.3.62 2	<p>Figura 5. ping del PCA a la IP 172.92.3.62 R1 G0/0/1- Última dirección de host de la subred LAN1</p>

			<pre> C:\>ping 172.92.3.62 Pinging 172.92.3.62 with 32 bytes of data: Reply from 172.92.3.62: bytes=32 time<1ms TTL=255 Reply from 172.92.3.62: bytes=32 time<1ms TTL=255 Reply from 172.92.3.62: bytes=32 time<1ms TTL=255 Reply from 172.92.3.62: bytes=32 time<1ms TTL=255 Ping statistics for 172.92.3.62: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms </pre>
	S1 VLAN 1	172.92.3.2	<p>Figura 6.ping del PCA a la IP 172.92.3.2 S1 VLAN 1</p> <pre> C:\>ping 172.92.3.2 Pinging 172.92.3.2 with 32 bytes of data: Reply from 172.92.3.2: bytes=32 time<1ms TTL=255 Reply from 172.92.3.2: bytes=32 time<1ms TTL=255 Reply from 172.92.3.2: bytes=32 time<1ms TTL=255 Reply from 172.92.3.2: bytes=32 time<1ms TTL=255 Ping statistics for 172.92.3.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms </pre>
	PC-B	172.92.3.7 5	<p>Figura 7. ping del PCA a la IP 172.92.3.2 S1 PC-B</p>

			<pre> C:\>ping 172.92.3.75 Pinging 172.92.3.75 with 32 bytes of data: Reply from 172.92.3.75: bytes=32 time<1ms TTL=127 Reply from 172.92.3.75: bytes=32 time<1ms TTL=127 Reply from 172.92.3.75: bytes=32 time<1ms TTL=127 Reply from 172.92.3.75: bytes=32 time<1ms TTL=127 Ping statistics for 172.92.3.75: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms </pre>
PC-B	R1 G0/0/0	172.92.3.94 4	<p>Figura 8. ping del PCB a la IP 172.92.3.94 R1 G0/0/0- Última dirección de host de la subred LAN2</p> <pre> C:\>ping 172.92.3.94 Pinging 172.92.3.94 with 32 bytes of data: Reply from 172.92.3.94: bytes=32 time<1ms TTL=255 Reply from 172.92.3.94: bytes=32 time<1ms TTL=255 Reply from 172.92.3.94: bytes=32 time<1ms TTL=255 Reply from 172.92.3.94: bytes=32 time<1ms TTL=255 Ping statistics for 172.92.3.94: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms </pre>
	R1 G0/0/1	172.92.3.62 2	<p>Figura 9. ping del PCB a la IP 172.92.3.62 R1 G0/0/1- Última dirección de host de la subred LAN1</p>

			<pre> C:\>ping 172.92.3.62 Pinging 172.92.3.62 with 32 bytes of data: Reply from 172.92.3.62: bytes=32 time<1ms TTL=255 Reply from 172.92.3.62: bytes=32 time<1ms TTL=255 Reply from 172.92.3.62: bytes=32 time<1ms TTL=255 Reply from 172.92.3.62: bytes=32 time<1ms TTL=255 Ping statistics for 172.92.3.62: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms </pre>
	S1 VLAN 1	172.92.3.2	<p>Figura 10. ping del PCB a la IP 172.92.3.2 S1 VLAN 1</p> <pre> C:\>ping 172.92.3.2 Pinging 172.92.3.2 with 32 bytes of data: Reply from 172.92.3.2: bytes=32 time<1ms TTL=255 Reply from 172.92.3.2: bytes=32 time<1ms TTL=255 Reply from 172.92.3.2: bytes=32 time<1ms TTL=255 Reply from 172.92.3.2: bytes=32 time<1ms TTL=255 Ping statistics for 172.92.3.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms </pre>
	PC-A	172.92.3.10	<p>Figura 11. ping del PCB a la IP 172.92.3.10 S1 PC-A</p>

			<pre>C:\>ping 172.92.3.10 Pinging 172.92.3.10 with 32 bytes of data: Reply from 172.92.3.10: bytes=32 time<1ms TTL=127 Reply from 172.92.3.10: bytes=32 time<1ms TTL=127 Reply from 172.92.3.10: bytes=32 time<1ms TTL=127 Reply from 172.92.3.10: bytes=32 time=13ms TTL=127 Ping statistics for 172.92.3.10: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 13ms, Average = 3ms</pre>
--	--	--	--

Fuente: autor

En la figura 4 se puede evidenciar que el ping del PC –A es exitoso porque la dirección corresponde a la puerta de enlace que está en la última dirección de host de la subred LAN2.

En la figura 5 se puede evidenciar que el ping del PC –A es exitoso porque la dirección corresponde a la puerta de enlace que está en la última dirección de host de la subred LAN1.

En la figura 6 se puede evidenciar que el ping del PC –A es exitoso porque la dirección corresponde al switch S1 de la VLAN.

En la figura 7 se puede evidenciar que el ping del PC –A es exitoso porque la dirección corresponde a la IP del PC-B.

En la figura 8 se puede evidenciar que el ping del PC –B es exitoso porque la dirección corresponde a la última dirección de host de la subred LAN2.

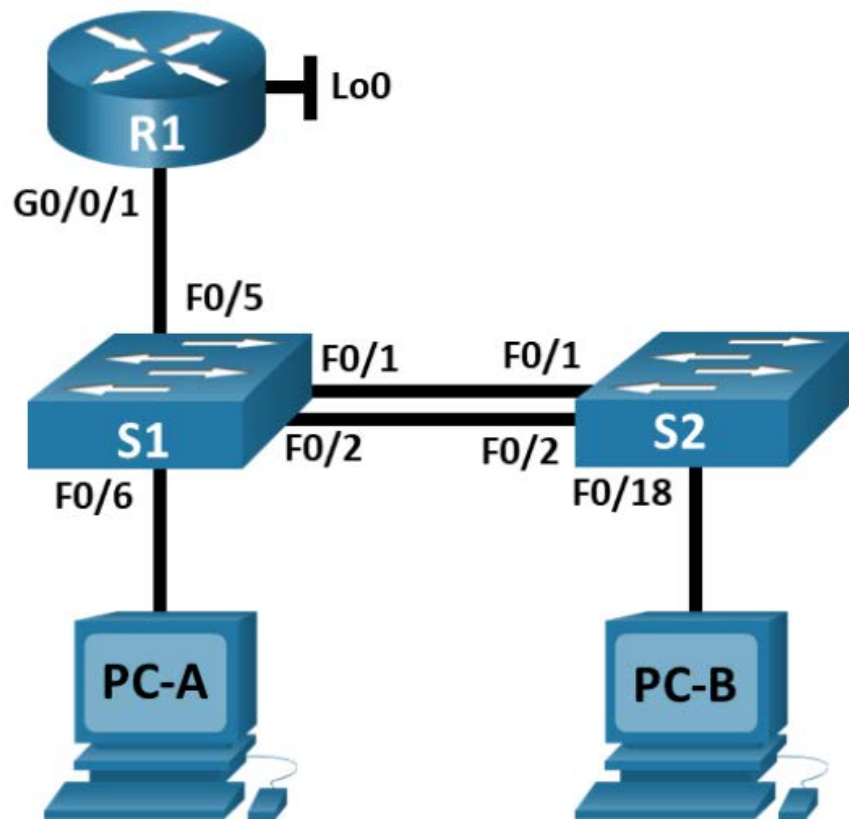
En la figura 9 se puede evidenciar que el ping del PC –B es exitoso porque la dirección corresponde a la última dirección de host de la subred LAN1.

En la figura 10 se puede evidenciar que el ping del PC –A es exitoso porque la dirección corresponde a la última dirección de la swicht S1 VLAN 1.

En la figura 11 se puede evidenciar que el ping del PC –B es exitoso porque la dirección corresponde al swicht S1 de la IP del PC-A.

2. DESARROLLO ESCENARIO 2

Figura 12. Topología Escenario 2



Fuente: prueba de habilidades diplomado CCNA.

En este escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch también deben administrarse de forma segura. Configuraré el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Tabla.7 nombre de las VLAN

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

Fuente: prueba de habilidades diplomado CCNA.

Tabla 8. Tabla de asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.20	10.92.8.1 /26 2001:db8:acad:a::1/64	No corresponde No corresponde
R1 G0/0/1.30	10.92.8.65 /27 2001:db8:acad:b::1/64	No corresponde No corresponde
R1 G0/0/1.40	10.92.8.97 /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 2001:db8:acad:209::1/64	No corresponde No corresponde
S1 VLAN 40	10.92.8.98 /29 2001:db8:acad:c::98/64 fe80::98	10.92.8.97 No corresponde No corresponde
S2 VLAN 40	10.92.8.99 /29 2001:db8:acad:c::99/64 fe80::99	10.92.8.97 No corresponde 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	Dirección DHCP para IPv4 2001:db8:acad:b::50 /64	DHCP para puerta de enlace predeterminada IPv4 fe80::1

Fuente: prueba de habilidades diplomado CCNA.

2.1 INICIALIZAR Y RECARGAR Y CONFIGURAR ASPECTOS BÁSICOS DE LOS DISPOSITIVOS

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.

```
erase startup-config  
reload
```

Nota: se utilizo el comando **startup-config** para eliminar los archivos de los Switches, también mediante el comando `delete vlan.dat` se borro toda la información de las VLAN.

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

para poder configurar la plantilla utilizamos el comando **show sdm prefer** y después reiniciamos la VLAN.

```
Switch#show sdm prefer  
Switch#reload
```

se verifica la correcta configuración de la plantilla SDM para que admita IPv6 Switch1 y Switch 2. También se configura la plantilla SDM para admitir IPv6. Mediante los siguientes comandos:

sdm prefer dual-ipv4-and-ipv6 default.

2.1.1. CONFIGURAR R1

Las tareas de configuración para R1 incluyen las siguientes:

Al router le asignamos nombre, también de dominio, se crean claves de acceso modo EXEC privilegiado proporcionando seguridad acceso completo al dispositivo y su configuración a la consola y con longitud mínima para poder mitigar los riesgos de acceso de algún usuario no autorizado, se crea un usuario administrativo en la base de datos local configurando el inicio de sesión en las líneas VTY que acepten únicamente las conexiones SSH, cifrando sus contraseñas, se Configurar un banner MOTD, se realiza configuración de sus interfaces, GigabitEthernet0/0/1.20, GigabitEthernet0/0/1.30, GigabitEthernet0/0/1.40, GigabitEthernet0/0/1.50, GigabitEthernet0/0/1.56, el Loopback0 generamos clave de cifrado, se habilita el routing IPv6, establecemos dirección IPv4 y la dirección local de enlace.

Tabla 9. Configuración router R1

Tarea	Especificación
Desactivar la búsqueda DNS	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 modo EXEC privilegiado	class R1(config)#enable password class
Contraseña de acceso a la consola	cisco R1(config)#enable secret cisco R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Establecer la longitud mínima para las contraseñas	5 caracteres R1(config)#security passwords min-length 5
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass R1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 15 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	Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece:

	<pre>R1(config)#banner motd "Yilmar Gildardo Rivera Vela,Programa ingenieria de sistemas"</pre>
Habilitar el routing IPv6	<pre>R1(config)#ipv6 unicast-routing</pre>
Configurar interfaz G0/0/1 y subinterfaces	<p>Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como fe80: :1 Establece la dirección IPv6. Activar la interfaz.</p> <pre>R1(config)#interface GigabitEthernet0/0/1.20 R1(config-subif)#encapsulation dot1q 20 R1(config-subif)#description Docentes R1(config-subif)#ip address 10.92.8.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#exit R1(config)# interface GigabitEthernet0/0/1.30</pre>

	<pre> R1(config-subif)#encapsulation dot1q 30 R1(config-subif)#description Estudiantes R1(config-subif)#ip address 10.92.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#exit R1(config-subif)# interface GigabitEthernet0/0/1.40 R1(config-subif)#encapsulation dot1q 40 R1(config-subif)#description Invitados R1(config-subif)#ip address 10.92.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#exit R1(config-subif)#)# interface GigabitEthernet0/0/1.50 R1(config-subif)#encapsulation dot1q 50 </pre>
--	---

	<pre> R1(config-subif)#description Usuarios R1(config-subif)#exit R1(config-subif)# interface GigabitEthernet0/0/1.56 R1(config-subif)#encapsulation dot1q 56 R1(config-subif)#description Native R1(config-subif)#exit R1(config-subif)# interface GigabitEthernet0/0/1 R1(config-if)#no shutdown </pre>
<p>Configure el Loopback0 interface</p>	<p>Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como fe80::1</p> <pre> R1(config-if)interface loopback 0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address fe80::1 link- local R1(config-if)#exit </pre>

Generar una clave de cifrado RSA	Módulo de 1024 bits R1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024
---	---

Fuente: Autor

2.1.2. CONFIGURE S1 Y S2.

Las tareas de configuración incluyen lo siguiente:

Los switches S1 y S2 le asignamos nombre, también de dominio, se crean claves de acceso modo EXEC privilegiado proporcionando seguridad acceso completo al dispositivo y su configuración a la consola y con longitud mínima para poder mitigar los riesgos de acceso de algún usuario no autorizado, se crea un usuario administrativo en la base de datos local configurando el inicio de sesión en las líneas VTY que acepten únicamente las conexiones SSH, cifrando sus contraseñas, se Configurar un banner MOTD, se realiza configuración de sus interfaces, generamos clave de cifrado, configuramos la interfaz de administración (SVI) Establecemos dirección IPv4 de capa 3 con la puerta de enlace predeterminada y dirección local de enlace.

Tabla 10. Configuración Switch S1 y S2

Tarea	Especificación
Desactivar la búsqueda DNS	Nota: estos mismos comandos y procesos los utilizaremos para configurar el Switch S1 y S2 en el orden

	<p>que desee configurarlos.</p> <p>Switch(config)#no ip domain-lookup</p>
Nombre del switch	<p>S1 y S2, de acuerdo a su configuración.</p> <p>Switch(config)#hostname S1</p> <p>Switch(config)#hostname S2</p>
Nombre de dominio	<p>ccna-sa.com</p> <p>S1(config)#ip domain-name ccna-sa.com</p> <p>S2(config)# ip domain-name ccna-sa.com</p>
Contraseña cifrada para el modo EXEC privilegiado	<p>class</p> <p>S1(config)#enable secret class</p> <p>S2(config)#enable secret class</p>
Contraseña de acceso a la consola	cisco

	<pre>S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit S2(config)#line console 0 S2(config-line)#password cisco S2(config-line)#login S2(config-line)#exit</pre>
Establecer la longitud mínima para las contraseñas	5 caracteres
Crear un usuario administrativo en la base de datos local	<pre>Nombre de usuario: admin Password: admin1pass S1(config)# username admin secret admin1pass S2(config)# username admin secret admin1pass</pre>
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	<pre>S1(config)#line vty 0 15 S1(config-line)#login local S2(config)#line vty 0 15 S2(config-line)#login local</pre>
Configurar VTY solo aceptando SSH	<pre>S1(config-line)#transport input ssh S1(config-line)#exit</pre>

	<pre>S2(config-line)#transport input ssh S2(config-line)#exit</pre>
Cifrar las contraseñas de texto no cifrado	<pre>S1(config)#service password-encryption S2(config)#service password-encryption</pre>
Configure un MOTD Banner	<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 "Yilmar Gildardo Rivera Vela,Programa ingenieria de sistemas"</pre>
Generar una clave de cifrado RSA	<p>Módulo de 1024 bits</p> <pre>S1(config)# crypto key generate rsa How many bits in the modulus [512]: 1024 S2(config)# crypto key generate rsa How many bits in the modulus [512]: 1024</pre>
Configurar la interfaz de administración (SVI)	<p>Establecer la dirección IPv4 de capa 3</p> <p>Establezca la dirección local de enlace</p>

	<p>IPv6 como FE80: :98 para S1 y FE80: :99 para S2</p> <p>Establecer la dirección IPv6 de capa 3</p> <p>S1(config)#int vlan40 S1(config-if)#ip address 10.92.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)# ipv6 address fe80::98 link- local S1(config-if)#description Invitados Interface S1(config-if)#no shutdown S1(config-if)#exit</p> <p>S2(config)#int vlan 40 S2(config-if)#ip address 10.92.8.99 255.255.255.248 S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#ipv6 address fe80::99 link- local S2(config-if)#description Invitados Interface S2(config-if)#no shutdown S2(config-if)#exit</p>
--	--

Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.92.8.97 para IPv4 S1(config)#ip default-gateway 10.92.8.97 S2(config)#ip default-gateway 10.92.8.97

Fuente: Autor

2.2. CONFIGURACIÓN DE LA INFRAESTRUCTURA DE RED (VLAN, TRUNKING, ETHERCHANNEL)

2.2.1. CONFIGURAR S1

La configuración del S1 y S2 incluye las siguientes tareas:

Se realiza creación de las Vlan 20,30,40,50 y 56. Se establece comunicación entre los Switch de modo troncal con el fin de manejar el tráfico entre las Vlans, se crearan un grupo de puertos de Capa 2 que use interfaces en un único canal lógico, se configura la seguridad de su puertos de acceso máximo 4 direcciones y se aseguraran todas sus interfaces no utilizadas.

Tabla 11. Configuración S1

Tarea	Especificación
Crear VLAN	VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native S1(config)#vlan 20 S1(config-vlan)#name Docentes S1(config-vlan)#exit S1(config)#vlan 30 S1(config-vlan)#name Estudiantes S1(config-vlan)#exit S1(config)#vlan 40 S1(config-vlan)#name Invitados

	<pre> S1(config-vlan)#exit S1(config)#vlan 50 S1(config-vlan)#name Usuarios S1(config-vlan)#exit S1(config)#vlan 56 S1(config-vlan)#name Native S1(config-vlan)#exit </pre>
<p>Crear troncos 802.1Q que utilicen la VLAN 56 native</p>	<p>Interfaces F0/1, F0/2 y F0/5</p> <pre> S1(config)#int range F0/1-2 S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 56 </pre>
<p>Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2</p>	<p>Usar el protocolo LACP para la negociación</p> <pre> S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#int port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk </pre>

	S1(config-if)#switch trunk native vlan 56
Configurar el puerto de acceso de host para VLAN 20	Interface F0/6 S1(config)#interface F0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 20
Configurar la seguridad del puerto en los puertos de acceso	Permitir 4 direcciones MAC S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 4
Proteja todas las interfaces no utilizadas	Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar S1(config)#interface range F0/3-4 S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#description No esta en Uso S1(config-if-range)#shutdown S1(config)#interface range F0/7-24 S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#description No esta

	en Uso S1(config-if-range)#shutdown
--	--

Fuente: Autor

2.2.2. CONFIGURE EL S2.

Tabla 12. Configuración S2

Tarea	Especificación
Crear VLAN	VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native S2(config)#vlan 20 S2(config-vlan)#name Docentes S2(config-vlan)#exit S2(config)#vlan 30 S2(config-vlan)#name Estudiantes S2(config-vlan)#exit S2(config)#vlan 40 S2(config-vlan)#name Invitados S2(config-vlan)#exit S2(config)#vlan 50 S2(config-vlan)#name Usuarios S2(config-vlan)#exit S2(config)#vlan 56

	<pre>S2(config-vlan)#name Native S2(config-vlan)#exit</pre>
<p>Crear troncos 802.1Q que utilicen la VLAN 56 native</p>	<p>Interfaces F0/1 y F0/2</p> <pre>S2(config)#int range F0/1-2 S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 56</pre>
<p>Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2</p>	<p>Usar el protocolo LACP para la negociación</p> <pre>S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#int port-channel 1 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switch trunk native vlan 56</pre>
<p>Configurar el puerto de acceso del host para la VLAN 30</p>	<p>Interfaz F0/18</p> <pre>S2(config-if)#int F0/18 S2(config-if)#switchport mode access</pre>

	S2(config-if)#switchport access vlan 30
Configure port-security en los access ports	<p>permite 4 MAC addresses</p> <p>S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 4</p>
Asegure todas las interfaces no utilizadas.	<p>Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar</p> <p>S2(config-if)#int range F0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 50 S2(config-if-range)#description No esta en Uso S2(config-if-range)#shutdown</p> <p>S2(config-if-range)#int range F0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 50 S2(config-if-range)#description No esta en Uso S2(config-if-range)#shutdown</p>

Fuente: Autor

2.3. CONFIGURAR SOPORTE DE HOST

2.3.1. CONFIGURE R1

Las tareas de configuración para R1 incluyen las siguientes:

En este caso se crearan unas rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0, se crearan un grupo DHCP para VLAN 20 y otro grupo DHCP para VLAN 30 donde cada uno de ellos este compuesto por las últimas 10 direcciones de la subred solamente y que se les asigne un nombre de dominio especificando de enlace predeterminada como dirección de interfaz del router.

Tabla 13. Configuración router R1

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0 R1(config)#ip router 0.0.0.0 0.0.0.0 loopback 0 R1(config)# ipv6 route ::/0 loopback0 Ambas rutas estáticas para llegar a internet
Configurar IPv4 DHCP para VLAN 20	Cree un grupo DHCP para VLAN 20, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-

	<p>ccna-sa.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada</p> <pre>R1(config)#ip dhcp excluded-address 10.92.8.1 10.92.8.52 R1(config)#ip dhcp pool vlan20- Docentes R1(dhcp-config)#network 10.92.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.92.8.1 R1(dhcp-config)# domain-name unad- ccna-sa.net</pre>
<p>Configurar DHCP IPv4 para VLAN 30</p>	<p>Cree un grupo DHCP para VLAN 30, 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</p> <pre>R1(config)#ip dhcp excluded-address 10.92.8.65 10.92.8.84</pre>

	<pre> R1(config)#ip dhcp pool vlan30- Estudiantes R1(dhcp-config)#network 10.92.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.92.8.65 R1(dhcp-config)# domain-name unad- ccna-sb.net </pre>
--	--

Fuente: Autor

2.3.2 CONFIGURAR LOS SERVIDORES

Se realizara la configuración de 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, registraremos las configuraciones de red del host con el comando `x|`.

Tabla 14. Configuración de red de PC-A

Configuración de red de PC-A	
Descripción	ccna-sa.com
Dirección física	0060.2FAA.6164
Dirección IP	10.92.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.92.8.1

Gateway predeterminado IPv6	<i>FE80::1</i>

Fuente: Autor

Tabla 15. Configuración de PC-B

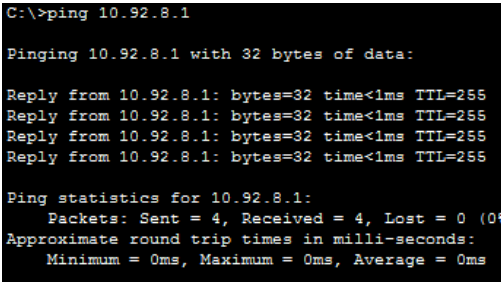
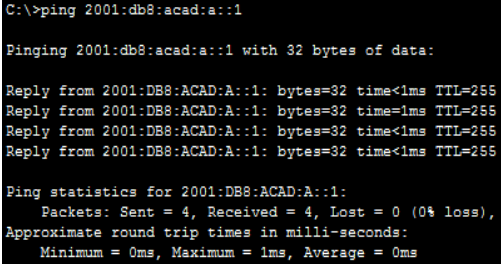
Configuración de red de PC-B	
Descripción	ccna-sa.com
Dirección física	0001.64B1.DE16
Dirección IP	<i>10.92.8.85</i>
Máscara de subred	<i>255.255.255.224</i>
Gateway predeterminado	<i>10.92.8.65</i>
Gateway predeterminado IPv6	FE80::1

Fuente: Autor

2.4. PROBAR Y VERIFICAR LA CONECTIVIDAD DE EXTREMO A EXTREMO

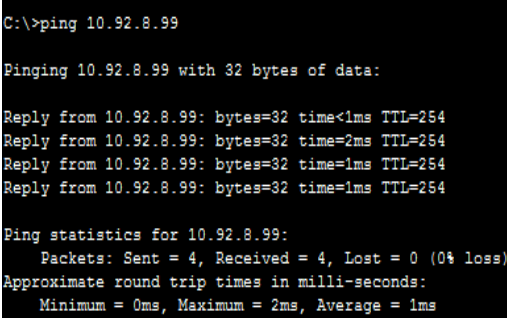
Para verificar la correcta implementación del escenario 2, se realizan pruebas de ping desde los dispositivos finales PC a los demás dispositivos de la topología.

Tabla 16. Probar y verificar la conectividad de extremo a extremo

Desde	A		Dirección IP	Resultados de ping
PC-A	R1, G0/0/1. 20	IPv4	10.92.8.1	<p>Figura 13. Ping desde PC-A a R1, G0/0/1.20</p> 
		IPv6	2001:db8:acad:a::1/64	<p>Figura 14. Ping desde PC-A a R1, G0/0/1.20 IPv6 2001:db8:acad:a::1</p> 

R1, G0/0/1. 30	IPv 4	10.92.8.65	<p>Figura 15. Ping desde PC-A a R1, G0/0/1.30 Dirección IP 10.19.8.65</p>
<pre>C:\>ping 10.92.8.65 Pinging 10.92.8.65 with 32 bytes of data: Reply from 10.92.8.65: bytes=32 time<1ms TTL=255 Reply from 10.92.8.65: bytes=32 time=1ms TTL=255 Reply from 10.92.8.65: bytes=32 time=1ms TTL=255 Reply from 10.92.8.65: bytes=32 time<1ms TTL=255 Ping statistics for 10.92.8.65: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms</pre>			
	IPv 6	2001:db8:acad:b::1/ 64	<p>Figura 16. Ping desde PC-A a R1, G0/0/1.30 IPv6 2001:db8:acad:b: :1</p>
<pre>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<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 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 = 0ms, Average = 0ms</pre>			
R1, G0/0/1. 40	IPv 4	10.92.8.97	<p>Figura 17. Ping desde PC-A a R1, G0/0/1.40 Dirección 10.19.8.97</p>

			<pre>C:\>ping 10.92.8.97 Pinging 10.92.8.97 with 32 bytes of data: Reply from 10.92.8.97: bytes=32 time<1ms TTL=255 Reply from 10.92.8.97: bytes=32 time<1ms TTL=255 Reply from 10.92.8.97: bytes=32 time<1ms TTL=255 Reply from 10.92.8.97: bytes=32 time=1ms TTL=255 Ping statistics for 10.92.8.97: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms</pre>
	IPv6 6	2001:db8:acad:c::1/ 64	<p>Figura 18. Ping desde PC-A a R1, G0/0/1.40 IPv6 2001:db8:acad:c::1</p> <pre>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</pre>
S1, VLAN 40	IPv4 4	10.92.8.98	<p>Figura 19. Ping desde PC-A a S1, VLAN 40 Dirección 10.19.8.98</p> <pre>C:\>ping 10.92.8.98 Pinging 10.92.8.98 with 32 bytes of data: Reply from 10.92.8.98: bytes=32 time<1ms TTL=254 Reply from 10.92.8.98: bytes=32 time=1ms TTL=254 Reply from 10.92.8.98: bytes=32 time<1ms TTL=254 Reply from 10.92.8.98: bytes=32 time<1ms TTL=254 Ping statistics for 10.92.8.98: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms</pre>

	IPv6	2001:db8:acad:c::98/64	<p>Figura 20. Ping desde PC-A a S1, VLAN 40</p> <p>IPv6 2001:db8:acad:c::98</p> <p>Nota: Por temas de actualización en la IOS no es posible hacer ping</p>
S2, VLAN 40	IPv4	10.92.8.99	<p>Figura 21. Ping desde PC-A a S2, VLAN 40</p> <p>Dirección IPv4 10.19.8.99</p>  <pre> C:\>ping 10.92.8.99 Pinging 10.92.8.99 with 32 bytes of data: Reply from 10.92.8.99: bytes=32 time<1ms TTL=254 Reply from 10.92.8.99: bytes=32 time=2ms TTL=254 Reply from 10.92.8.99: bytes=32 time=1ms TTL=254 Reply from 10.92.8.99: bytes=32 time=1ms TTL=254 Ping statistics for 10.92.8.99: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 2ms, Average = 1ms </pre>
	IPv6	2001:db8:acad:c::99/64	<p>Figura 22. Ping desde PC-A a S2, VLAN 40</p> <p>IPv6 2001:db8:acad:c::99</p> <p>Nota: Por temas de actualización en la IOS no es posible hacer ping</p>
PC-B	IPv4	10.92.8.85	<p>Figura 23. Ping desde PC-A a PC-B,</p> <p>Dirección IP 10.92.8.85</p>

			<pre> C:\>ping 10.92.8.85 Pinging 10.92.8.85 with 32 bytes of data: Reply from 10.92.8.85: bytes=32 time<1ms TTL=127 Reply from 10.92.8.85: bytes=32 time<1ms TTL=127 Reply from 10.92.8.85: bytes=32 time<1ms TTL=127 Reply from 10.92.8.85: bytes=32 time<1ms TTL=127 Ping statistics for 10.92.8.85: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms </pre>
	IPv6	2001:db8:acad:b::50/64	<p>Figura 24. Ping desde PC-A a PC-B, IPv6 2001:db8:acad:b :50</p> <pre> 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<1ms TTL=127 Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127 Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127 Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms 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 = 0ms, Average = 0ms </pre>
R1 Bucle 0	IPv4	209.165.201.1	<p>Figura 25. Ping desde PC-A a R1, Bucle 0 Dirección 209.165.201.1</p>

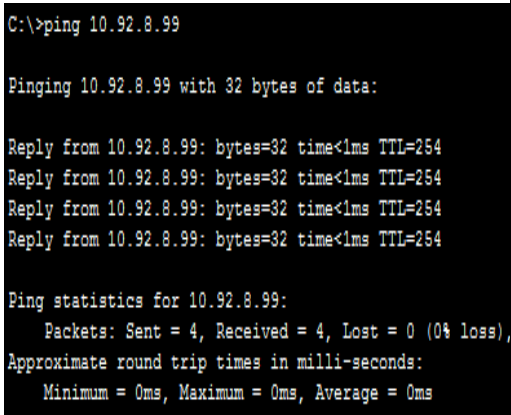
				<pre>C:\>ping 209.165.201.1 Pinging 209.165.201.1 with 32 bytes of data: Reply from 209.165.201.1: bytes=32 time<1ms TTL=255 Reply from 209.165.201.1: bytes=32 time=1ms TTL=255 Reply from 209.165.201.1: bytes=32 time<1ms TTL=255 Reply from 209.165.201.1: bytes=32 time<1ms TTL=255 Ping statistics for 209.165.201.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms</pre>
		IPv6	2001:db8:acad:209::1 /64	<p>Figura 26. Ping desde PC-A a R1, Bucle 0 IPv6, 2001:db8:acad:209::1</p> <pre>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<1ms 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 = 0ms, Average = 0ms</pre>
PC-B	R1 Bucle 0	IPv4	209.165.201.1	<p>Figura 27. Ping desde PC-B a R1, Bucle 0 Dirección, 209.165.201.1</p> <pre>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=22ms 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 = 22ms, Average = 6ms</pre>

		IPv6	2001:db8:acad:209::1/64	<p>Figura 28. Ping desde PC-B a R1, Bucle 0</p> <p>IPv6 2001:db8:acad:209: :1</p> <pre> 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=15ms 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 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 = 15ms, Average = 3ms </pre>
	R1, G0/0/1.20	IPv4	10.92.8.1	<p>Figura 29. Ping desde PC-B a R1, G0/0/1.20 Dirección 10.19.8.1</p> <pre> C:\>ping 10.92.8.1 Pinging 10.92.8.1 with 32 bytes of data: Reply from 10.92.8.1: bytes=32 time=14ms TTL=255 Reply from 10.92.8.1: bytes=32 time<1ms TTL=255 Reply from 10.92.8.1: bytes=32 time<1ms TTL=255 Reply from 10.92.8.1: bytes=32 time=1ms TTL=255 Ping statistics for 10.92.8.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 14ms, Average = 3ms </pre>
		IPv6	2001:db8:acad:a::1/64	<p>Figura 30. Ping desde PC-B a R1, G0/0/1.20 IPv6 2001:db8:acad:a: :1</p>

			<pre> 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 = 1ms, Average = 0ms </pre>
R1, G0/0/1. 30	IPv 4	10.92.8.65	<p>Figura 31. Ping desde PC-B a R1, G0/0/1.30 Dirección IPv4 10.19.8.65</p> <pre> C:\>ping 10.92.8.65 Pinging 10.92.8.65 with 32 bytes of data: Reply from 10.92.8.65: bytes=32 time<1ms TTL=255 Reply from 10.92.8.65: bytes=32 time<1ms TTL=255 Reply from 10.92.8.65: bytes=32 time<1ms TTL=255 Reply from 10.92.8.65: bytes=32 time=1ms TTL=255 Ping statistics for 10.92.8.65: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms </pre>
	IPv 6	2001:db8:acad:b::1/ 64	<p>Figura 32. Ping desde PC-B a R1, G0/0/1.30 IPv6 2001:db8:acad:b::1</p>

			<pre>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<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 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 = 1ms, Average = 0ms</pre>
R1, G0/0/1. 40	IPv 4	10.92.8.97	<p>Figura 33. Ping desde PC-B a R1, G0/0/1.40 Dirección IPv4 10.19.8.97</p> <pre>C:\>ping 10.92.8.97 Pinging 10.92.8.97 with 32 bytes of data: Reply from 10.92.8.97: bytes=32 time<1ms TTL=255 Reply from 10.92.8.97: bytes=32 time=1ms TTL=255 Reply from 10.92.8.97: bytes=32 time=1ms TTL=255 Reply from 10.92.8.97: bytes=32 time<1ms TTL=255 Ping statistics for 10.92.8.97: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms</pre>
	IPv 6	2001:db8:acad:c::1/ 64	<p>Figura 34. Ping desde PC-B a R1, G0/0/1.40 IPv6 2001:db8:acad:c: :1</p>

			<pre>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</pre>
S1, VLAN 40	IPv 4	10.92.8.98	<p>Figura 35. Ping desde PC-B a S1, VLAN 40 Dirección 10.19.8.98</p> <pre>C:\>ping 10.92.8.98 Pinging 10.92.8.98 with 32 bytes of data: Reply from 10.92.8.98: bytes=32 time<1ms TTL=254 Reply from 10.92.8.98: bytes=32 time<1ms TTL=254 Reply from 10.92.8.98: bytes=32 time<1ms TTL=254 Reply from 10.92.8.98: bytes=32 time<1ms TTL=254 Ping statistics for 10.92.8.98: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre>
	IPv 6	2001:db8:acad:c::98 /64	<p>Figura 36. Ping desde PC-B a S1, VLAN 40 IPv6 2001:db8:acad:c: :98</p> <p>Nota: Por temas de actualización en la IOS no es posible hacer ping</p>

S2, VLAN 40	IPv 4	10.92.8.99	<p>Figura 37. Ping desde PC-B a S2, VLAN 40 Dirección 10.19.8.99</p>  <pre> C:\>ping 10.92.8.99 Pinging 10.92.8.99 with 32 bytes of data: Reply from 10.92.8.99: bytes=32 time<1ms TTL=254 Reply from 10.92.8.99: bytes=32 time<1ms TTL=254 Reply from 10.92.8.99: bytes=32 time<1ms TTL=254 Reply from 10.92.8.99: bytes=32 time<1ms TTL=254 Ping statistics for 10.92.8.99: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms </pre>
	IPv 6	2001:db8:acad:c::99 /64	<p>Figura 38. Ping de PC-B a S2, VLAN 40 IPv6 2001:db8:acad:c: :99</p> <p>Nota: Por temas de actualización en la IOS no es posible hacer ping.</p>

En la figura 13 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv4 corresponde a la interfaz del router R1 G0/0/1.20.

En la figura 14 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv6 corresponde a la interfaz del router R1 G0/0/1.20.

En la figura 15 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv4 corresponde a la interfaz del router R1 G0/0/1.30.

En la figura 16 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv6 corresponde a la interfaz del router R1 G0/0/1.30.

En la figura 17 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv4 corresponde a la interfaz del router R1 G0/0/1.40.

En la figura 18 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv6 corresponde a la interfaz del router R1 G0/0/1.40.

En la figura 19 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv4 corresponde al S1 en la VLAN 40.

En la figura 20 se puede evidenciar que el ping del PC –A no es exitoso porque la dirección ipv6 que corresponde al S1 en la VLAN 40. Presenta un error en la configuración de la consola.

En la figura 21 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv4 corresponde al S2 en la VLAN 40.

En la figura 22 se puede evidenciar que el ping del PC –A no es exitoso porque la dirección ipv6 que corresponde al S2 en la VLAN 40. Presenta un error en la configuración de la consola.

En la figura 23 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv4 corresponde al PC-B.

En la figura 24 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv6 corresponde al PC-B.

En la figura 25 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv4 es del Bucle 0 configurado en el router R1.

En la figura 26 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv6 es del Bucle 0 configurado en el router R1.

En la figura 27 se puede evidenciar que el ping del PC –B es exitoso porque la dirección ipv4 es del Bucle 0 configurado en el router R1.

En la figura 28 se puede evidenciar que el ping del PC –B es exitoso porque la dirección ipv6 es del Bucle 0 configurado en el router R1.

En la figura 29 se puede evidenciar que el ping del PC –B es exitoso porque la dirección ipv4 corresponde a la interfaz del router R1 G0/0/1.20.

En la figura 30 se puede evidenciar que el ping del PC –B es exitoso porque la dirección ipv6 corresponde a la interfaz del router R1 G0/0/1.20.

En la figura 31 se puede evidenciar que el ping del PC –B es exitoso porque la dirección ipv4 corresponde a la interfaz del router R1 G0/0/1.30.

En la figura 32 se puede evidenciar que el ping del PC –B es exitoso porque la dirección ipv6 corresponde a la interfaz del router R1 G0/0/1.30.

En la figura 33 se puede evidenciar que el ping del PC –B es exitoso porque la dirección ipv4 corresponde a la interfaz del router R1 G0/0/1.40.

En la figura 34 se puede evidenciar que el ping del PC –B es exitoso porque la dirección ipv6 corresponde a la interfaz del router R1 G0/0/1.40.

En la figura 35 se puede evidenciar que el ping del PC –B es exitoso porque la dirección ipv4 corresponde al S1 en la VLAN 40.

En la figura 36 se puede evidenciar que el ping del PC –B no es exitoso porque la dirección ipv6 que corresponde al S1 en la VLAN 40. Presenta un error en la configuración de la consola.

En la figura 37 se puede evidenciar que el ping del PC –B es exitoso porque la dirección ipv4 corresponde al S2 en la VLAN 40.

En la figura 38 se puede evidenciar que el ping del PC –B no es exitoso porque la dirección ipv6 que corresponde al S2 en la VLAN 40. Presenta un error en la configuración de la consola

CONCLUSIONES

Teniendo muy claro la comprensión de estos dos escenarios, se ejecutaron a cabalidad sus simulaciones y el desarrollo de sus actividades, se mantuvo presente las normas y las configuraciones aprendidas que nos han de llevar a un nivel de aprendizaje más alto, claro, concreto sobre las redes y sus funciones.

Hemos aprendido que para estas técnicas de configuración reconocer las redes IPv4, Ipv6 y sus configuraciones para poder comprender mas a acerca de los Host de una red, como se puede configurar una red y que tipología se podría manejar en cada una de ellas, también en sus niveles de seguridad como configurar cada dispositivo y como poder encriptarlos mediante comandos CLI, sus capas de enlace modo troncal, la configuración de VLAN administrativas, configuración de puertos Etherchannel, en general todo lo que abarca la configuración de estos dispositivos en una red local.

Este diplomado me ha ayudado mucho porque tengo conceptos más claros y espero seguir aprendiendo y seguir mejorando en muchos aspectos seguir creciendo tanto en lo laboral, como en lo personal, muchas gracias.

BIBLIOGRAFIA

ARIGANELLO, E. Redes cisco CCNA Routing y Switching .{en línea } (2016){26 de noviembre de 2022} Disponible en:
https://bibliotecavirtual.unad.edu.co/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=2498326&lang=es&site=ehost-live&ebv=EB&ppid=pp_159

CASTAÑO,R.j y LOPEZ, f.j. Redes locales.Macmillan Iberia S.A. Madrid.{en línea } (2013){26 de noviembre de 2022} Disponible en:
<https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43257?page=215>

CASTAÑO,R.j. y LOPEZ, f.j. Redes locales.Macmillan Iberia S.A. Madrid.{en línea } (2013){26 de noviembre de 2022} Disponible en:
<https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43257?page=233>

CASTAÑO, R. r. j., y López, F. J. Redes locales.Macmillan Iberia S.A. Madrid.{en línea } (2013){26 de noviembre de 2022} Disponible en:
<https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43257?page=193>

PEREZ, Flor. Modelo TCP/IP [OVI].{en línea } (2021){26 de noviembre de 2022} Disponible en:
<https://repository.unad.edu.co/handle/10596/43437>

ANEXOS

ANEXO A. Descarga de archivos de simulación escenario 1

Enlace: https://drive.google.com/file/d/1nyzQ6SyVPqnyluztfmTIm-ShqXN2qsWs/view?usp=share_link

ANEXO B. Descarga de archivos de simulación escenario 2

Enlace: https://drive.google.com/file/d/1x1YrNc33AbFC1ZGOBS2rIZMTeTaXCo60/view?usp=share_link