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

LUIS FERNANDO MONROY GOMEZ

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

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

LUIS FERNANDO MONROY GOMEZ

Diplomado de opción de grado presentado para optar el título de
INGENIERO DESISTEMAS

DIRECTOR:
PAULITA FLOR

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

TUNJA, 5 de diciembre de 2022

AGRADECIMIENTOS

Agradezco primeramente a Dios por darme la vida, fuerza y sabiduría para la realización de las actividades, en segundo lugar, a mis padres por el apoyo económico e incondicional para el desarrollo de este proceso de formación, en tercer lugar a la Universidad UNAD por brindarme todo el apoyo a través de los tutores, que gracias a su enseñanza me permitieron fortalecer mis conocimientos en el campo de los sistemas, las redes informáticas y la programación, así como ofrecerme la oportunidad de ser e-monitor y dar todo lo mejor de sí al estamento estudiantil y con ello aprender habilidades que antes no tenía y los beneficios que esta estrategia tiene y por lo cual me siento muy orgulloso de mi universidad, mis tutores y la comunidad en general.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ACL (Lista de Control de acceso): es una colección secuencial de condiciones de permiso y denegación que se aplican a un paquete IP.[1]

CCNA: La certificación en (Cisco Certified Networking Associate) demuestra que usted tiene conocimiento de las tecnologías fundamentales y asegura que se mantenga relevante con los conjuntos de habilidades necesarios para la adopción de tecnologías de próxima generación.[2]

DHCP (Dynamic Host Configuration Protocol): Es un protocolo de red que utiliza una arquitectura cliente-servidor. Este asigna direcciones IP y otra información de configuración de red dinámicamente[3]

DNS (Sistema de Nombres de Dominio): es un sistema de nombres jerárquico que permite la comunicación entre dispositivos en una red.[4]

DPT (Protocolo de Enlace Troncal Dinámico): DTP es un protocolo exclusivo de Cisco que se habilita de manera automática en los switches de las series Catalyst 2960 y Catalyst 3560.[5]

ETHERCHANNEL: es una tecnología de agregación de enlaces que agrupa varios enlaces Ethernet físicos en un único enlace lógico. Se utiliza para proporcionar tolerancia a fallos, uso compartido de carga, mayor ancho de banda y redundancia entre switches, routers y servidores.[6]

ENRUTAMIENTO: Proceso que en el que los enrutadores aprenden sobre redes remotas, encuentran todas las rutas posibles para llegar a ellas y luego escogen las mejores rutas, es decir, las más rápidas para intercambiar datos entre las mismas.[7]

FTP: (Protocolo de Transferencia de archivos) se trata de un protocolo que permite transferir archivos directamente de un dispositivo a otro[8]

HSRP: (Hot Standby Router Protocol) Es el protocolo FHRP exclusivo de Cisco

[1] CISCO, Configurar ACL de IP de uso común (2022)
[2] CISCO, Las redes en la actualidad. Introducción a Redes (2020)
[3] CISCO, Conceptos de DHCPv4. Switching, Routing, y Wireless Essentials. (2020)
[4] CCNA DE CERO, ¿Qué es DNS? (2020)
[5] CISCO, Introducción a DTP. Switching, Routing, y Wireless Essentials. (2020)
[6] CCNA DE CERO, Funcionamiento de EtherChannel (2020)
[7] CISCO, Community. Conceptos Fundamentales de enrutamiento. (S.f)
[8] FERNÁNDEZ, Yúbal. FTP: qué es y cómo funciona. (2021)

diseñado para permitir la conmutación por falla transparente de los dispositivos IPv4 de primer salto[9]

LAN (Red de área local): Es una infraestructura de red que proporciona acceso a usuarios y dispositivos finales en un área geográfica pequeña. Normalmente, una LAN se utiliza en un departamento dentro de una empresa, un hogar o una red de pequeñas empresas.[10]

LÍNEAS VTY (Líneas de Terminal Virtual): Los puertos vty están enumerados del 0 al 15 y son utilizados para establecer sesiones Telnet.[11]

LLC: (Capa Lógica de Control de Enlace) Subcapa de la capa de Enlace, encargada de corregir y/o detectar errores en las tramas, se asegura de que las tramas lleguen en la secuencia correcta e implementa el control de flujo.[12]

NORMA IEEE 802: Estándar de redes y prácticas recomendadas para redes locales, metropolitanas y de otras áreas, utilizando un proceso abierto y acreditado.[13]

MAC: (Capa de Control de Acceso al Medio) Subcapa de la capa de Enlace, encargada de encapsular el acceso al medio, la cual existe siempre y cuando haya conexiones basadas en canales.[14]

MODELO OSI: Es un modelo desarrollado por ISO: International Standards Organization. OSI significa: Open Systems Interconection (Interconexión de Sistemas Abiertos).[15]

SMTP (Protocolo Simple De Transferencia De Correo Electrónico): Es aquel que provee los mecanismos para la transmisión de correos electrónicos desde la máquina cliente hasta el servidor.[16]

SSL (Secure Socket Layer): es un protocolo que dispone un nivel seguro de transporte entre el servicio clásico de transporte en internet (TCP) y las aplicaciones que se comunican a través de él.[17]

---

[9] CISCO. Conceptos de FHRP. Switching, Routing, y Wireless Essentials. (2020)
[10] CISCO. Tipos comunes de Redes. Introducción a las redes. (2020)
[11] RINCON V, Liliana y ANDRADE MUÑOZ, Jesús. Configurando un acceso administrativo seguro. Universidad Autónoma del Estado de Hidalgo: UAEH. (2017)
[12] CAFFA, Angel. Conceptos de redes de computadoras (2005)
[13] IEEE. Norma IEEE 802.x (2022)
[14] CAFFA, Angel. Conceptos de redes de computadoras (2005)
[15] CAFFA, Angel. Conceptos de redes de computadoras (2005)
[16] NIÑO, Elías. Fundamentos para el desarrollo de aplicaciones en la red. (2012)
[17] NIÑO, Elías. Fundamentos para el desarrollo de aplicaciones en la red. (2012)

RESUMEN

El propósito de este informe es presentar el desarrollo de dos escenarios de práctica utilizando el software de simulación Cisco Packet Tracer, donde en el primer escenario se realiza la configuración básica del router y switch utilizando el direccionamiento IPv4 a través de VLSM, lo que permite un mejor aprovechamiento de la red, de igual forma se realiza la configuración del host y se ejecutan las pruebas de conectividad; En el segundo escenario se configuran las subinterfaces mediante direccionamiento IPv4 e IPv6, así como enrutamiento dinámico en el router, finalmente se configura la infraestructura de red (VLAN, Trunking, Ether Channel y Port-security) en los switches, y los hosts. en PCs de forma dinámica para IPv4 y estática para IPv6 para que exista comunicación entre los diferentes dispositivos de la red con ambos protocolos.

Palabras Clave: CISCO, CCNA, Enrutamiento, Conmutación, Redes, EtherChannel, DHCP, VLAN.

ABSTRACT

The purpose of this report is to present the development of two practice scenarios using the Cisco Packet Tracer simulation software, where in the first scenario the basic configuration of the router and switch is performed using it IPv4 addressing through VLSM, which allows a better use of the network, in the same way, the host configuration is carried out and connectivity tests are executed; In the second scenario, the sub interfaces are configured through IPv4 and IPv6 addressing, as well as dynamic routing in the router, finally the network infrastructure (VLAN, Trunking, Ether Channel and Port-security) is configured in the switches, and the hosts in PCs dynamically for IPv4 and static for IPv6 so that there is communication between the different devices on the network with both protocols.

Keywords: CISCO, CCNA, Routing, Switching, Networking, Ether Channel, DHCP, VLAN.

INTRODUCCIÓN

El diplomado en CISCO CNNA tiene como objetivo profundizar en el diseño y construcción de redes locales y corporativas seguras y escalables, a través de la configuración de dispositivos en red que permita su optimización y resolución de problemas en entornos reales de redes LAN y WLAN. En este sentido, los estudiantes deben tener la capacidad de usar adecuadamente los protocolos de diseño y configuración aplicándolos en cada uno de los escenarios de practica propuestos, con el uso de la herramienta de simulación de redes Cisco Packet Tracer, la cual permite utilizar diferentes dispositivos finales, intermedios y el cableado adecuado según el medio de transmisión para realizar la configuración correspondiente de acuerdo con el diseño lógico y físico.

Por otra parte, en el desarrollo del escenario 1 se realiza la configuración de los dispositivos de una red pequeña, donde se diseñó la topología de red, el esquema de direccionamiento IP para la LAN1 y la LAN2 configurando los aspectos básicos de los dispositivos de la red, los ajustes básicos de seguridad en el R1 y S1 y los hosts de conectividad entre los equipos presentando un análisis de los resultados de ping. De igual forma, en el escenario 2 se inicializan, recargan y configuran aspectos básicos de los dispositivos R1, S1 y S2 con la creación de subinterfaces y loopback0 en R1 y la interfaz de administración SVI en cada Switch, así mismo, se configura la infraestructura de red (VLAN, Trunking, EtherChannel), el soporte de host en R1 y los servidores DHCP en los PC. Por último, se realizan las pruebas de conectividad de un dispositivo a otro a través del comando ping tanto para ipv4 como para ipv6 y se efectúa la evaluación de los resultados de ping.

Finalmente, durante este diplomado se logra profundizar en el modelo OSI y TCP/IP a través de las diferentes configuraciones desarrolladas en ambos escenarios, teniendo en cuenta el proceso de conmutación, enrutamiento, direccionamiento IP, identificación, mitigación de amenazas de seguridad de una

red, conectividad de dispositivos y direccionamiento sin clase, logrando generar redundancia y confiabilidad en redes locales corporativas LAN y WAN.

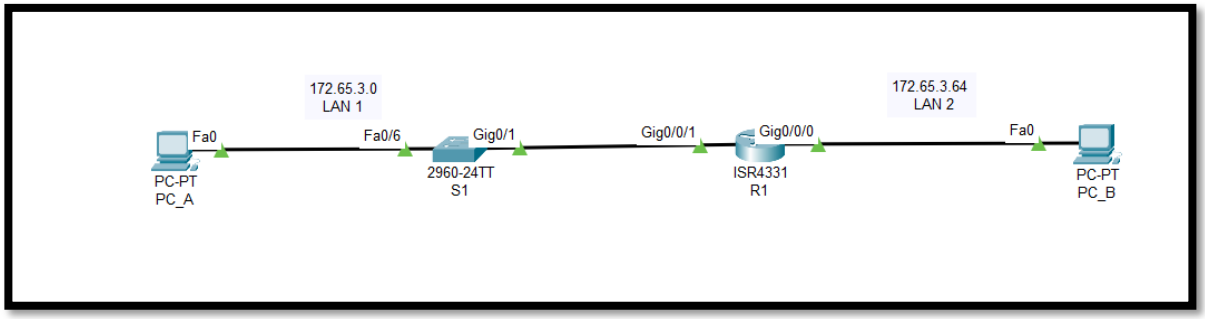
DESARROLLO

1. 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.

Topología

Figura 1. Escenario 1



Fuente: Autoría propia

Objetivos

Parte 1: Construir en el simulador la Red

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

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

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

Parte 5: Configurar los hosts y verificar la conectividad entre los equipos

Aspectos básicos de la situación

En el desarrollo de caso de estudio usted implementa la topología mostrada en la figura y configurara el Router 1, el Switch 1 y los 2 PC's. Con la dirección suministrada se realizará el Subneteo y cumplirá con los requerimientos de la LAN 1 (60 hosts) y la LAN 2 (20 hosts).

Parte 1: Construya la Red

En el simulador construya la red de acuerdo con la topología lógica que se plantea en la figura 1, cable como se indica en la topología, y conecte los equipos de cómputo.

Según el documento guía la conexión entre dispositivos debe realizarse de la siguiente forma del puerto FastEthernet0 de la PC_A, al puerto FastEthernet0/6 del Switch (S1), esta se definirá como la LAN 1; del puerto GigabitEthernet0/1 del Switch (S1), al puerto GigabitEthernet0/0/1 del Router (R1); Finalmente del puerto GigabitEthernet0/0/0 del Router al puerto FastEthernet0 de la PC_B, definida como LAN2

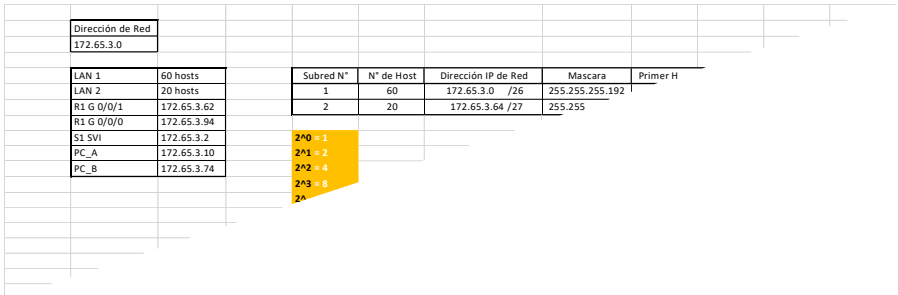
Parte 2: Desarrollo del esquema de direccionamiento IP

Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento

Cada estudiante tomara el direccionamiento 172.XY.3.0 donde XY corresponde a los dos últimos dígitos de su cédula

Para hallar cada una de las direcciones IP, debemos crear el Subneteo a través de VLSM a través de una hoja Excel como se muestra a continuación:

Figura 2. Subneteo Escenario 1



Dirección de Red
172.65.3.0

LAN 1	60 hosts
LAN 2	20 hosts
R1 G 0/0/1	172.65.3.62
R1 G 0/0/0	172.65.3.94
S1 SVI	172.65.3.2
PC_A	172.65.3.10
PC_B	172.65.3.74

Subred N°	N° de Host	Dirección IP de Red	Mascara	Primer H
1	60	172.65.3.0 /26	255.255.255.192	
2	20	172.65.3.64 /27	255.255	

2^0	1
2^1	2
2^2	4
2^3	8
2^	

Fuente: Autoría propia

Tabla 1. Esquema de Direccionamiento

Ítem	Requerimiento
Dirección de Red	172.65.3.0 donde XY corresponde a los últimos dos dígitos de mi cédula.
Requerimiento de host Subred LAN1	172.65.3.0 (60 hosts)
Requerimiento de host Subred LAN2	172.65.3.64 (20 host)
R1 G0/0/1	172.65.3.62
R1 G0/0/0	172.65.3.94
S1 SVI	172.65.3.2
PC-A	172.65.3.10
PC-B	172.65.3.74

Fuente: Autoría propia

Parte 3: Configure aspectos básicos

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

Paso 1: Configurar los ajustes básicos

Esta configuración se realiza a través de los parámetros básicos que debe llevar todos los dispositivos intermedios tales como: desactivar el DNS, esto con el fin de que no llame a otro dominio, se da el nombre al router, se establecen contraseñas para la protección de este, así como la creación del usuario administrativo, el mensaje de advertencia de acuerdo a lo solicitado, y se configuran las respectivas interfaces del router con su respectivo direccionamiento IP como se muestra a continuación:

Tabla 2. Configuración aspectos básicos R1

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

Contraseña cifrada para el modo EXEC privilegiado	Asignamos la contraseña en modo EXEC Privilegiado R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	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	Se establece la longitud mínima de 10 caracteres para la contraseña R1(config)#security password min-length 10
Crear un usuario administrativo en la base de datos local Nombre de usuario: **admin** Contraseña: **admin1pas**	R1(config)#username admin password admin1pass
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)#password cisco R1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	R1(config-line)#transport input ssh R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	Ciframos las contraseñas de texto R1(config)#service password-encryption
Configurar un banner MOTD	R1(config)#banner motd #R1_LUIS FERNANDO MONROY Ingenieria de Sistemas #
Configuración de interfaz G0/0/1	Acceso a la interfaz G0/0/1 R1(config)#int G0/0/1 R1(config-if)#description RED LAN 1 R1(config-if)#ip add 172.65.3.62 255.255.255.192 R1(config-if)#no shut
Configuración de interface G0/0/0	R1(config)#int G0/0/0 R1(config-if)#description RED LAN 2 R1(config-if)#ip add 172.65.3.94 255.255.255.224 R1(config-if)#no shut
Generar una clave de cifrado RSA	R1(config)# crypto key generate rsa general-keys modulus 1024

Fuente: Autoría propia

Las tareas de configuración de S1 incluyen lo siguiente:

Esta configuración se realiza a través de los parámetros básicos que debe llevar todos los dispositivos intermedios tales como: desactivar el DNS, esto con el fin de que no llame a otro dominio, se da el nombre del switch, el nombre de dominio, contraseñas para la protección de estos, creación del usuario administrativo en la base de datos local, configuración del inicio de sesión en las líneas VTY tanto para base de datos local como para que acepte únicamente las conexiones SSH, generar clave de cifrado RSA, interfaz de administración (SVI) y el Gateway predeterminado.

Tabla 3. Configuración aspectos básicos del S1

Tarea	**Especificación**
Desactivar la búsqueda DNS	Switch>en Switch#conf t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup
Nombre del switch	S1 Switch(config)#hostname S1
Nombre de dominio	ccna-sa.com S1(config)#ip domain name ccna-sa.com
Contraseña cifrada para el modoEXEC privilegiado	ciscoenpass S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit
Apagar todos los puertos sin usar	F0/1-4, F0/7-24 S1(config)#int range Fa 0/1-4 S1(config-if-range)#shut S1(config)#int range Fa 0/7-24 S1(config-if-range)#shut S1(config)#int range G0/2 S1(config-if-range)#shut

Crear un usuario administrativoen la base de datos local	Nombre de usuario: **admin** Contraseña: **admin1pass** S1(config)#username admin password admin1pass
Configure el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un banner MOTD	S1(config)#banner motd #S1_LUIS FERNANDO MONROY Ingenieria de Sistemas#
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa general-keys modulus 1024
Configure la interfaz de administración (SVI) en VLAN1	S1(config)#int vlan 1 S1(config-if)#ip add 172.65.3.2 255.255.255.192 S1(config-if)#no shut
Configuración del Gateway predeterminado	S1(config)#ip default-gateway 172.65.3.62

Fuente: Autoría propia

Paso 2: Configurar los equipos

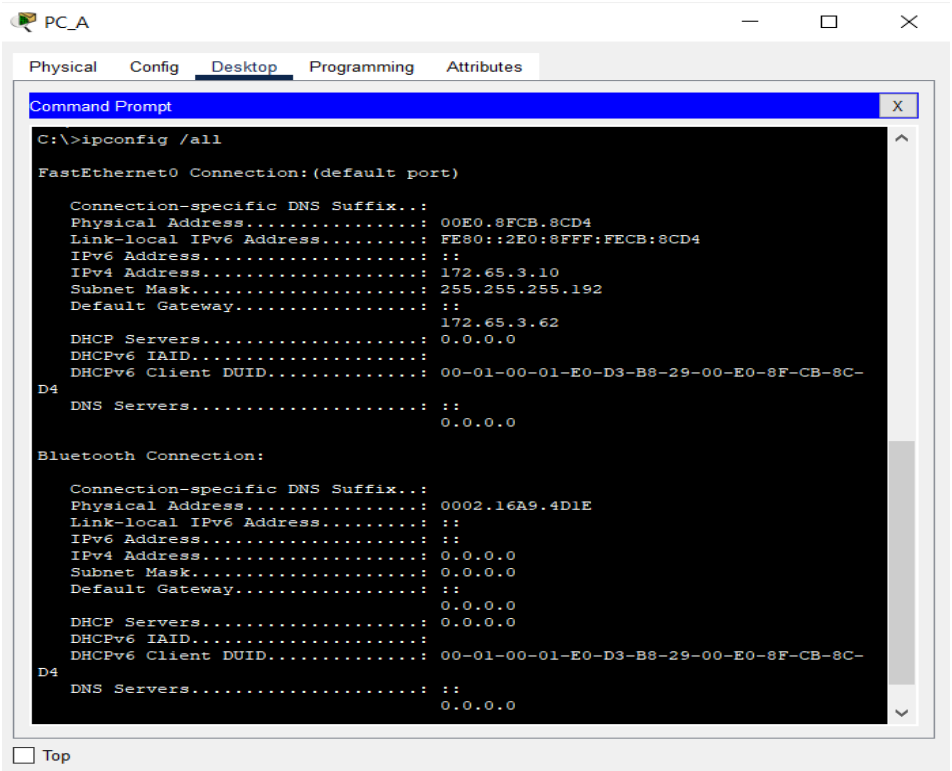
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all**

Tabla 4. Network Configuration - PC-A

Configuración de red - PC-A	
Descripción	PC-A
Dirección física	00E0.8FCB.8CD4
Dirección IPv4	172.65.3.10
Máscara de subred	255.255.255.192
Puerta de enlace IPv4predeterminada	172.65.3.62

Fuente: Autoría propia

Figura 3. Configuración física del PC-A



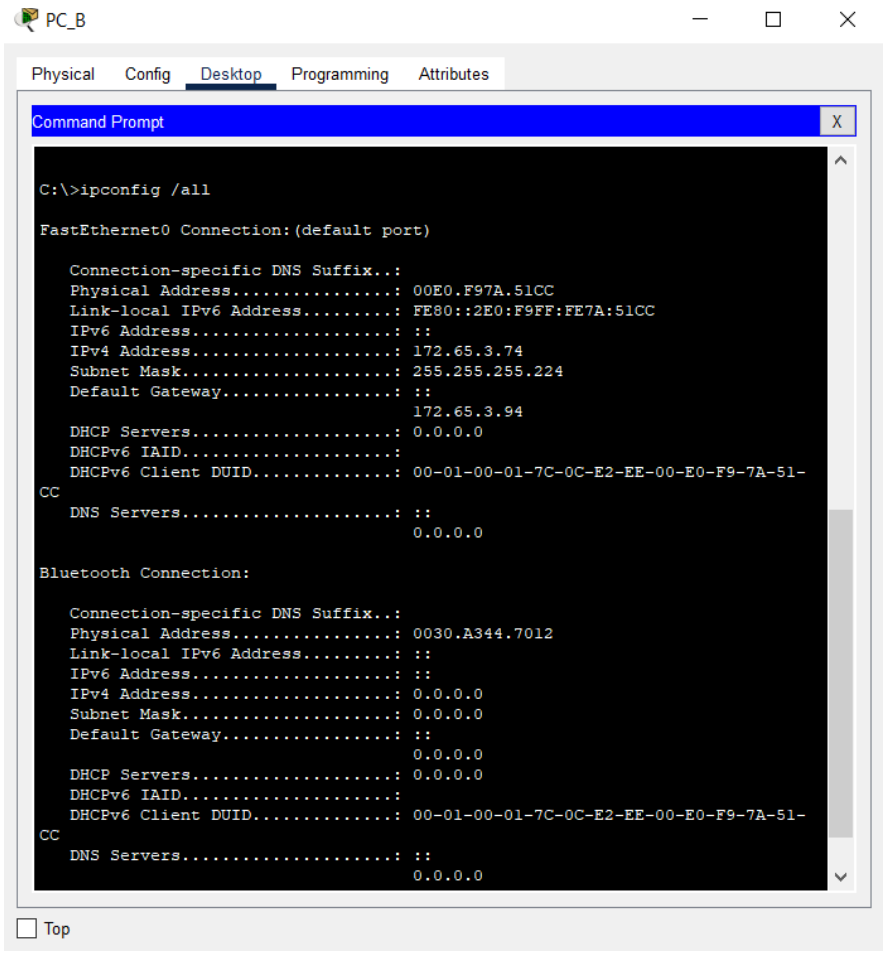
Fuente: Autoría propia

Tabla 5. Network Configuration - PC-B

Configuración de red - PC-A	
Descripción	FastEthernet0 connection: (defaultport)
Dirección física	00E0.F97A.51CC
Dirección IPv4	172.65.3.74
Máscara de subred	255.255.255.224
Puerta de enlace IPv4 predeterminada	172.65.3.94

Fuente: Autoría propia

Figura 4. Configuración física PC-B



Fuente: Autoría propia

Paso 3: pruebas de conectividad

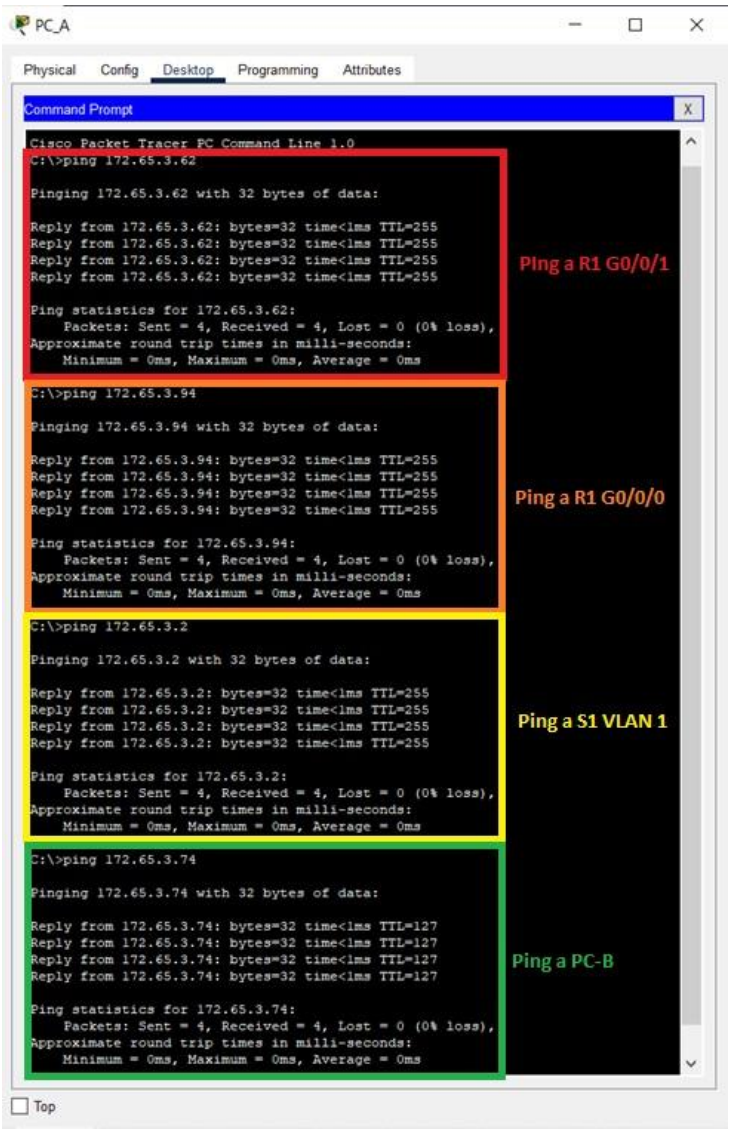
Para verificar la correcta implementación del escenario 1, se realizan pruebas de ping desde los dispositivos finales PC hacia los demás dispositivos de la topología.

Tabla 6. Verificación de conectividad extremo a extremo

Desde	A	Dirección IP	Resultados de ping
PC-A	R1 G0/0/1	172.65.3.62	Exitoso
	R1 G0/0/0	172.65.3.94	Exitoso
	S1 VLAN1	172.65.3.2	Exitoso
	PC-B	172.65.3.74	Exitoso
PC-B	R1 G0/0/1	172.65.3.62	Exitoso
	R1 G0/0/0	172.65.3.94	Exitoso
	S1 VLAN1	172.65.3.2	Exitoso
	PC-A	172.65.3.10	Exitoso

Fuente: Autoría propia

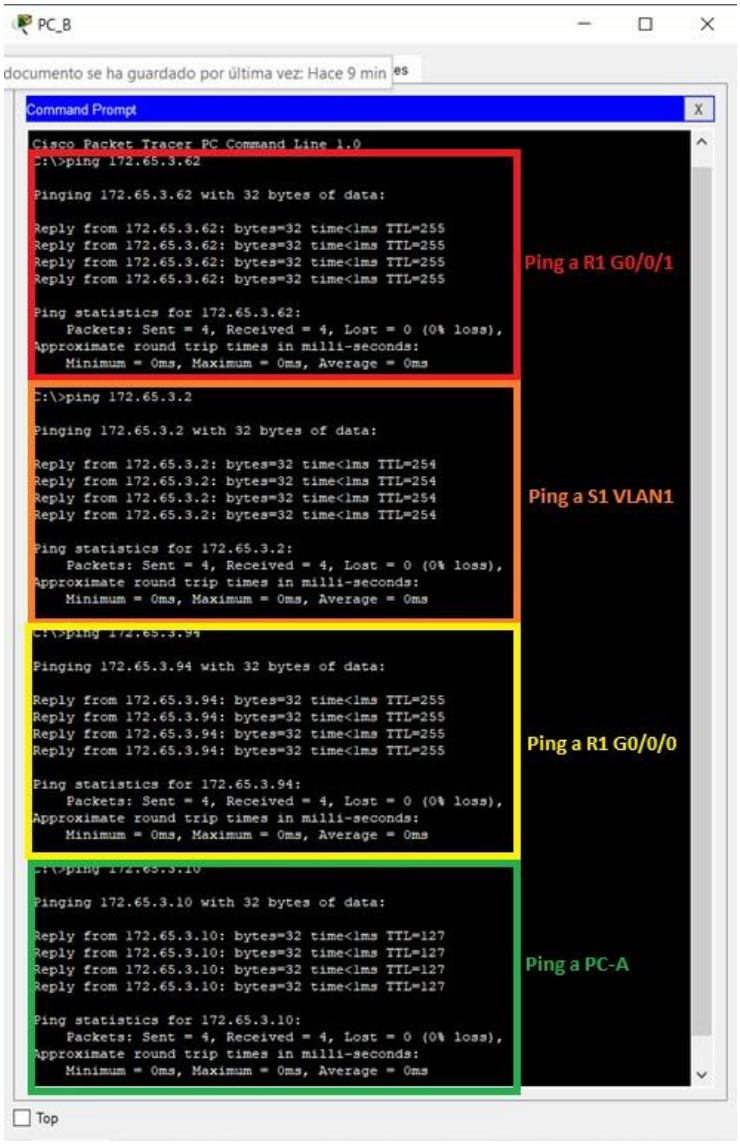
Figura 5. Prueba de conectividad PC-A a los diferentes dispositivos de la red



Fuente: Autoría propia

En la figura 5, se puede observar que los diferentes pings realizados son exitosos, ya que la dirección corresponde a la puerta de enlace del mismo pc y a su vez, están en la misma subred.

Figura 6. Prueba de conectividad PC-B a los diferentes dispositivos de la red



Fuente: Autoría propia

En la figura 6, se puede observar que los diferentes pings realizados son exitosos, ya que la dirección corresponde a la puerta de enlace del mismo pc y a su vez, están en la misma subred.

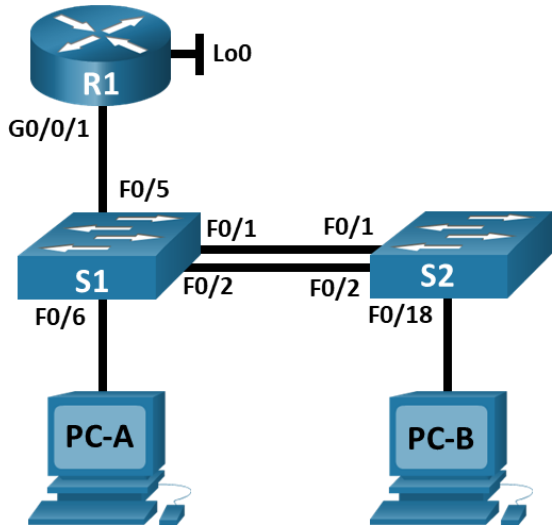
2. Escenario 2

2.1. Topología

Los dispositivos requeridos para esta red son los siguientes

- Un Router Cisco ISR 4331
- Dos Switches Cisco Multilayer C3560-24PS
- 2 PC de escritorio

Figura 7. Escenario 2



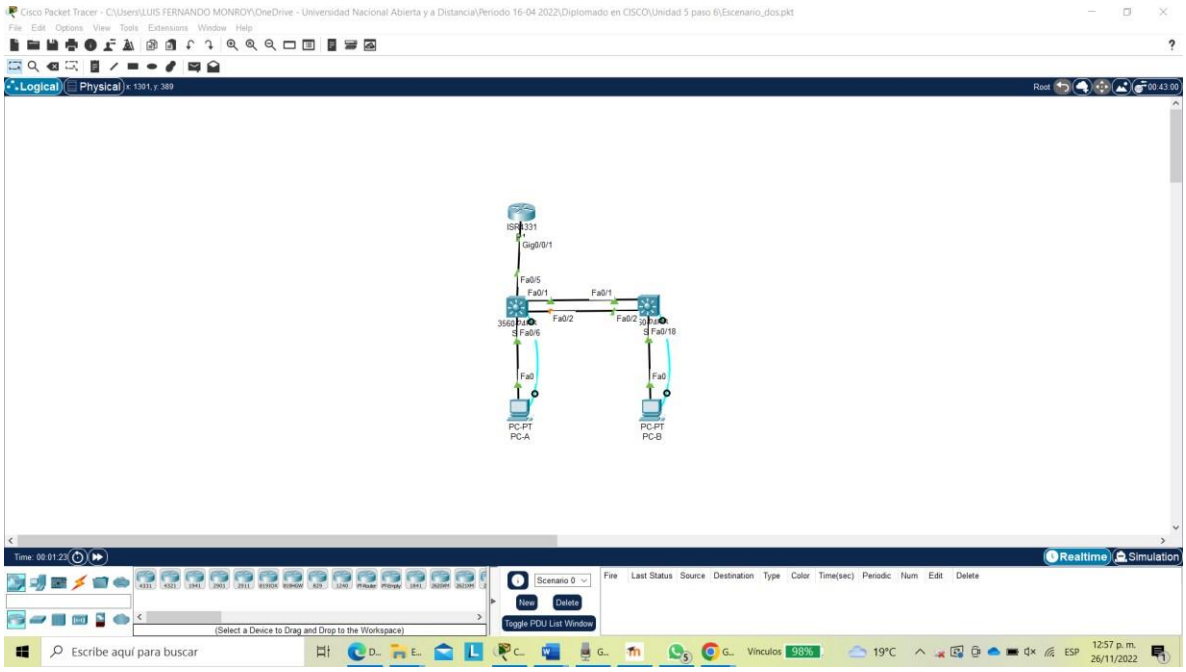
Fuente: Guía Prueba de habilidades practicas CCNA

Aspectos básicos de la situación

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. Configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security. Entre tanto inicialmente se debe identificar los dispositivos, consecutivamente se crea la topología, se procede a realizar las respectivas configuraciones en el router, los switches y los equipos de cómputo, por último, se realizará las respectivas pruebas de conectividad de toda la red.

Para ello se agregan a la pantalla del simulador Cisco Packet Tracer los dispositivos requeridos, después se conectan por medio de cable directo y/o UTP según corresponda el puerto como se muestra en la siguiente topología:

Figura 8. Realización de la topología en Cisco Packet Tracer



Fuente: Autoría propia

Las VLAN que se deben crear en cada switch son:

Tabla 7. VLAN

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

Fuente: Guía Prueba de habilidades practicas CCNA

Tabla 8. Asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.20	10.65.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.30	10.65.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.40	10.65.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.56	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1/64	No corresponde
S1 VLAN 40	10.65.8.98 /29	10.65.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 40	10.65.8.99 /29	10.65.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

Fuente: Guía Prueba de habilidades practicas CCNA.

DESARROLLO DEL ESCENARIO 2

Instrucciones

Parte 1: Inicializar y Recargar y Configurar aspectos básicos de los dispositivos

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

Para el desarrollo de este escenario 2 hay que tener en cuenta que se deben borrar las configuraciones de inicio de las VLAN del Router y el switch y se reinician los dispositivos utilizando los comandos que se muestran a continuación:

Tabla 9. Comandos básicos para inicializar y reiniciar el router y los switches

Tarea	Comando de IOS
Eliminar el archivo start-up-config del router.	Router > enable Router# erase startup-config
Volver a cargar el router.	Router# reload
el archivo startup-config de todos los switches y eliminar la base de datos, develan anterior.	switch>enable switch#delete vlan.dat switch#erase startup-config
Volver a cargar ambos switches.	swicht#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos Switches.	switch#show flash

Fuente: Autoría propia

Habiendo realizado las instrucciones mencionadas en la tabla anterior, se procede a realizar la activación y/o configuración de la plantilla SDM en ambos switches por medio del comando "*sdm prefer dual-ipv4-and-ipv6 default"*, con el fin de que estos admitan el direccionamiento IPv4 e Ipv6. Entre tanto, hay que tener presente que para este paso se debe estar en la configuración global, entre tanto, después de haber hecho esto se emite el comando reload desde el modo privilegiado, el cual permite activar la nueva configuración establecida.

Switches (S1 y S2)

Switch>en

Switch#conf t

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

Switch(config)#exit

Switch#reload

Systemconfigurationhasbeenmodified.Save?[yes/no]:yes

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Esta configuración se realiza a través de los parámetros básicos que debe llevar todos los dispositivos intermedios tales como: desactivar el DNS, esto con el fin de que no llame a otro dominio, se da el nombre al router, se establecen contraseñas para la protección de este, así como la creación del usuario administrativo, el mensaje de advertencia de acuerdo a lo solicitado, se habilita el routing IPv6 y se configuran las respectivas interfaces del router con su respectivo direccionamiento IP como se muestra a continuación:

Tabla 10. Configuración del R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#no ip domain-lookup
Nombre de dominio ccna-sa.com	R1(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXECprivilegiado: class	R1(config)#enable secret class
Contraseña de acceso a la consola: cisco	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit

Establecer la longitud mínima para las contraseñas: 5 Caracteres	R1(config)#security password min-length 5
Crear un usuario administrativo en la base de datos local Nombre de usuario: admin Password: admin1pass	R1(config)#username admin privilege 15 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)#password cisco R1(config-line)#login local
Configurar VTY solo aceptando SSH	R1(config-line)#transport input ssh R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd #R1_Luis Fernando Monroy Gomez_Ingenieria de Sistemas#
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces incluye: Establezca la descripción Establece la dirección IPv4 Establezca la dirección local de enlace IPv6 como fe80: :1 Establece la dirección IPv6 Activar la interfaz	R1(config)#int G0/0/1.20 R1(config-subif)#encapsulation dot1q 20 R1(config-subif)#description LAN to VLAN20 Docentes R1(config-subif)#ip add 10.65.8.1 255.255.255.192 R1(config-subif)#ipv6 add 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#no shut R1(config-subif)#exit
	R1(config)#int G0/0/1.30 R1(config-subif)#encapsulation dot1q 30 R1(config-subif)#description LAN to VLAN30 Estudiantes R1(config-subif)#ip add 10.65.8.65 255.255.255.224 R1(config-subif)#ipv6 add 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#no shut R1(config-subif)#exit

	R1(config)#int G0/0/1.40 R1(config-subif)#encapsulation dot1q 40 R1(config-subif)#description LAN to VLAN40 Invitados R1(config-subif)#ip add 10.65.8.97 255.255.255.248 R1(config-subif)#ipv6 add 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#no shut R1(config-subif)#exit
	R1(config)#int G0/0/1.56 R1(config-subif)#encapsulation dot1q 56 R1(config-subif)#description VLAN56 Native R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#no shut
Configure el Loopback0 interface • Establezca la descripción • Establece la dirección IPv4 • Establece la dirección IPv6 • Establezca la dirección local de enlace IPv6 como fe80::1	R1(config)#int loopback0 R1(config-if)#ip add 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 add 2001:db8:acad:209::1/64 R1(config-if)#ipv6 add fe80::1 link-local R1(config-if)#no shut R1(config-if)#exit
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa 1024 R1(config)#exit R1#copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK]

Fuente: Autoría propia

Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Esta configuración se realiza a través de los parámetros básicos que debe llevar todos los dispositivos intermedios tales como: desactivar el DNS, esto con el fin de que no llame a otro dominio, se da el nombre del switch, el nombre de dominio,

contraseñas para la protección de estos, creación del usuario administrativo en la base de datos local, configuración del inicio de sesión en las líneas VTY tanto para base de datos local como para que acepte únicamente las conexiones SSH, generar clave de cifrado RSA y por ultimo configurar la interfaz administrativa (SVI).

Tabla 11. Configuración del S1

Tarea	**Especificación**
Desactivar la búsqueda DNS.	Switch>en Switch#conf t Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio • ccna-sa.com	S1(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado • class	S1(config)#enable secret class
Contraseña de acceso a la consola • cisco	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 • Nombre de usuario: admin • Password: admin1pass	S1(config)#username admin privilege 15 password 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)#password cisco S1(config-line)#login local S1(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)#line vty 0 15 S1(config-line)#transport input ssh S1(config-line)#login local S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption

Configurar un MOTD Banner	S1(config)#banner motd #S1_Luis Fernando Monroy Gomez_Ingenieria de Sistemas#
Generar una clave de cifrado RSA y asignarle el Módulo de 1024 bits	S1(config)#crypto key generate rsa 1024
Configurar la interfaz de administración (SVI) • Establecer la dirección IPv4 de capa 3 • Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 • Establecer la dirección IPv6 de capa 3	S1(config)#int vlan40 S1(config-if)#ip add 10.65.8.98 255.255.255.248 S1(config-if)#ipv6 add 2001:db8:acad:c::98/64 S1(config-if)#ipv6 add fe80::98 link-local S1(config-if)#description VLAN40 Invitados S1(config-if)#no shut S1(config-if)#exit
Configuración del gateway predeterminado • Configure la puerta de enlace predeterminada como 10.65.8.97 para IPv4	S1(config)#ip default-gateway 10.65.8.97 S1(config)#do wr Building configuration... [OK]

Fuente: Autoría propia

En el siguiente paso, se vuelven a realizar las mismas tareas que se configuraron previamente en el S1

Tabla 12. Configuración del S2

Tarea	**Especificación**
Desactivar la búsqueda DNS.	Switch>en Switch#conf t Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S2
Nombre de dominio • ccna-sa.com	S2(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado • class	S2(config)#enable secret class

Contraseña de acceso a la consola • cisco	S2(config)#line console 0 S2(config-line)#password cisco S2(config-line)#login S2(config-line)#exit
Crear un usuario administrativo en la base de datos local • Nombre de usuario: admin • Password: admin1pass	S2(config)#username admin privilege 15 password 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)#password cisco S2(config-line)#login local S2(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config)#line vty 0 15 S2(config-line)#transport input ssh S2(config-line)#login local S2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption
Configurar un MOTD Banner	S2(config)#banner motd #S2_Luis Fernando Monroy Gomez_Ingenieria de Sistemas#
Generar una clave de cifrado RSA y asignarle el Módulo de 1024 bits	S2(config)#crypto key generate rsa 1024
Configurar la interfaz de administración (SVI) Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80::99 para S2 Establecer la dirección IPv6 de capa 3	S2(config)#int vlan40 S2(config-if)#ip add 10.65.8.99 255.255.255.248 S2(config-if)#ipv6 add 2001:db8:acad:c::99/64 S2(config-if)#ipv6 add fe80::99 link-local S2(config-if)#description VLAN40 Invitados S2(config-if)#no shut S2(config-if)#exit
Configuración del gateway predeterminado • Configure la puerta de enlace predeterminada como 10.65.8.97 para IPv4	S2(config)#ip default-gateway 10.65.8.97 S2(config)#do wr Building configuration... [OK]

Fuente: Autoría propia

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

En esta sección de configuración troncal se realiza la creación de VLAN con sus respectivos nombres y direccionamiento, creando los respectivos enlaces trocales 802.1Q que maneje la VLAN 56 nativa y la cual permite enrutar los paquetes de varias VLAN que viajan a través de los switches.

Tabla 13. Configuración de la infraestructura de red en 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 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
Crear troncos 802.1Q que utilicen la VLAN 56 nativa en Interfaces F0/1, F0/2 y F0/5	S1(config)#int Fa0/5 S1(config-if)#sw t encapsulation dot1q S1(config-if)#sw mo t S1(config-if)#sw t native vlan 56 S1(config-if)#sw t allowed vlan 20,30,40,56 S1(config-if)#exit

	S1(config)#int range Fa0/1-2 S1(config-if-range)#sw t encapsulation dot1q S1(config-if-range)#sw mo t S1(config-if)#sw t native vlan 56 S1(config-if)#sw t allowed vlan 20,30,40,56 S1(config-if)#exit
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2, para ello usar el protocolo LACP para la negociación	S1(config)#int range fa0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#channel-protocol lacp S1(config-if-range)#int port-channel 1 S1(config-if)#sw t encapsulation dot1q S1(config-if)#sw mo t S1(config-if)#sw t native vlan 56 S1(config-if)#exit
Configurar el puerto de acceso de host para VLAN 20 en la Interface F0/6	S1(config)#int fa0/6 S1(config-if)#sw mo access S1(config-if)#sw access vlan 20 S1(config-if)#exit
Configurar la seguridad del puerto en los puertos de acceso, para que permita 4 direcciones MAC	S1(config)#int Fa0/6 1(config-if)#sw port-security maximum 4 S1(config-if)#exit
Proteja todas las interfaces no utilizadas, para esto hay que: • Asignar a VLAN 50 • Establecer en modo de acceso, agregar una descripción y apagar	1(config)#int range Fa0/3-4,Fa0/7-24,G0/1-2 S1(config-if-range)#sw mo access S1(config-if-range)#sw access vlan 50 S1(config-if-range)#description #Puertos sin utilizar# S1(config-if-range)#shut S1(config-if-range)#exit S1(config)#do wr Building configuration... [OK]

Fuente: Autoría propia

Paso 2: Configure el S2.

En este paso se vuelven a realizar las mismas tareas del S1 y se crea un conjunto de puertos EtherChannel de la capa 2 para que se utilice en las interfaces F0/1 y F0/2.

Tabla 14. configuración de la infraestructura de red en 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)#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)#do wr Building configuration... [OK]
Crear troncales 802.1Q que utilicen la VLAN 56 nativa en las Interfaces F0/1 y F0/2	S2(config)#int range Fa0/1-2 S2(config-if-range)#sw t encapsulation dot1q S2(config-if-range)#sw mo t S2(config-if-range)#sw t native vlan 56 S2(config-if-range)#sw t allowed vlan 20,30,40,56 S2(config-if-range)#exit
Crear un grupo de puertos EtherChannel deCapa 2 que use interfaces F0/1 y F0/2, para ello se debe usar el protocolo LACP para lanegociación.	S2(config)#int range Fa0/1-2 S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#channel-protocol lacp S2(config-if-range)#int port-channel 1 S2(config-if)#sw t encapsulation dot1q S2(config-if)#sw mo t S2(config-if)#sw t native vlan 56

	S2(config-if)#
Configurar el puerto de acceso del host para laVLAN 30 en la Interfaz F0/18	S2(config)#int Fa0/18 S2(config-if)#sw mo access S2(config-if)#sw access vlan 30 S2(config-if)#exit
Configurar la seguridad del puerto en los puertos de acceso, para que permita 4 direcciones MAC	S2(config)#int Fa0/18 S2(config-if)#sw mo access S2(config-if)#sw port-security maximum 4 S2(config-if)#do wr Building configuration... [OK]
Asegure todas las interfaces no utilizadas, para esto hay que: • Asignar a VLAN 50 • Establecer en modo de acceso, agregar una descripción y apagar	S2(config)#int range Fa0/3-17,Fa0/19-24, G0/1-2 S2(config-if-range)#sw mo access S2(config-if-range)#sw access vlan 50 S2(config-if-range)#sw port-security violation shut S2(config-if-range)#description #Puertos sin utilizar# S2(config-if-range)#shut S2(config-if-range)#do wr Building configuration... [OK]

Fuente: Autoría propia

Parte 3: Configurar soporte de host

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes: Se realiza la configuración del router R1 con DHCP con el fin de que al momento efectuar la conexión con los hosts estos asignen automáticamente la dirección IP en los dispositivos, sin necesidad de configurar manualmente estos, para ello se crea una ruta predeterminada para IPv4 e IPv6 que permita enviar el tráfico a la interfaz loopback 0 y consecutivamente se configura ipv4 DHCP para la VLAN 20 y 30.

Tabla 15. Configuración del soporte de host de R1

Tarea	Especificación
Configure Default Routing, para ello hay que: Crear rutas predeterminadas para ipv4 e ipv6 que dirijan el trafico a la interfaz Loopback 0	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 %Default route without gateway, if not a point-to-point interface, may impact performance R1(config)#ipv6 route ::/0 loopback 0
Configurar IPv4 DHCP para VLAN 20: Cree un grupo de DHCP para VLAN 20 compuesto por las 10 ultimas direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sa.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada.	R1(config)#ip dhcp excluded-address 10.65.8.1 10.65.8.52 R1(config)#ip dhcp pool vlan20-Docentes R1(dhcp-config)#network 10.65.8.1 255.255.255.192 R1(dhcp-config)#default-router 10.65.8.1 R1(dhcp-config)#domain-name unad-ccna-sa.net R1(dhcp-config)#exit
Configurar DHCP IPv4 para VLAN 30: 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	R1(config)#ip dhcp excluded-address 10.65.8.65 10.65.8.84 R1(config)#ip dhcp pool vlan30-Estudiantes R1(dhcp-config)#network 10.65.8.65 255.255.255.224 R1(dhcp-config)#default-router 10.65.8.65 R1(dhcp-config)#domain-name unad.ccna-sb.net R1(dhcp-config)#exit R1(config)#do wr

Fuente: Autoría propia

Paso 2: Configurar los servidores

Esta configuración está compuesta por la dirección física e IP la cual lleva su respectiva mascara de subred y el Gateway predeterminado tanto para IPv4 como para IPv6, el cual permite que pasando por si mismo, ir hacia otra red. Donde, después de configurar cada servidor, se procede a registrar las

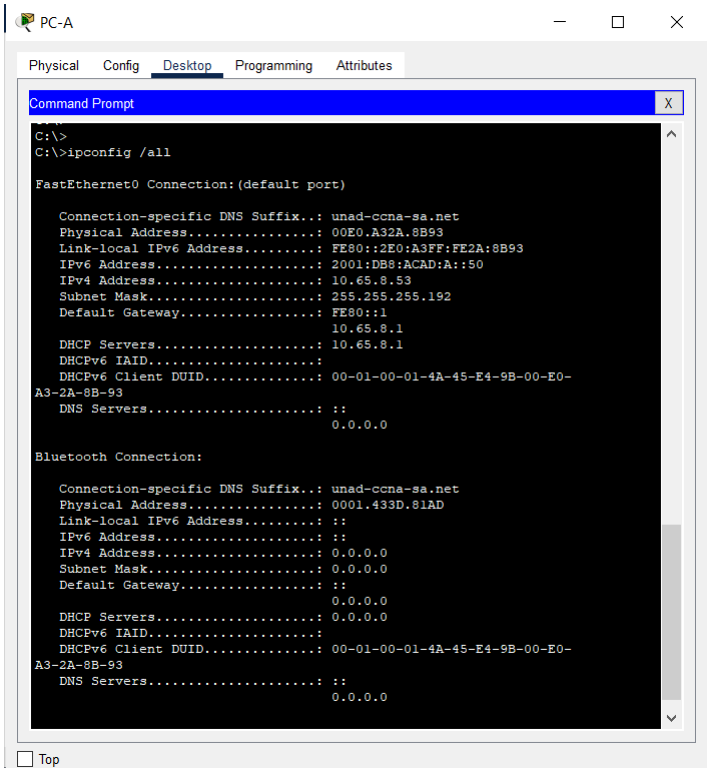
configuraciones de red del host a través del comando ipconfig /all.

Tabla 16. Configuración de red del PC-A

Configuración de red de PC-A	
Descripción	PC-A
Dirección física	00E0.A32A.8B93
Dirección IP	10.65.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.65.8.1
Gateway predeterminado IPv6	FE80::1

Fuente: Autoría propia.

Figura 9. Registro de las configuraciones de red en PC-A



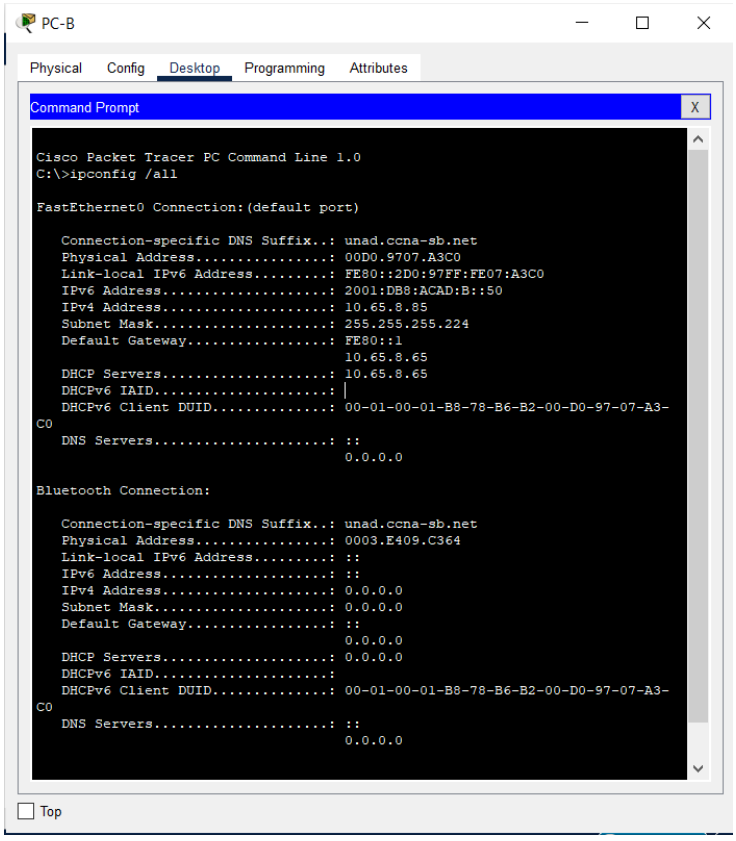
Fuente: Autoría propia

Tabla 17. Configuración de red del PC-B

Configuración de red de PC-B	
Descripción	PC-B
Dirección física	00D0.9707.A3C0
Dirección IP	10.65.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.65.8.65
Gateway predeterminado IPv6	FE80::1

Fuente: Autoría propia

Figura 10. Registro de las configuraciones de red en PC-B



Fuente: Autoría propia

Parte 4: Probar y verificar la conectividad

En esta parte se realiza de un dispositivo a otro a través del comando ping tanto para ipv4 como para ipv6, para ello se accede a la consola de comandos y se digita el comando ping seguido de la dirección IP del host.

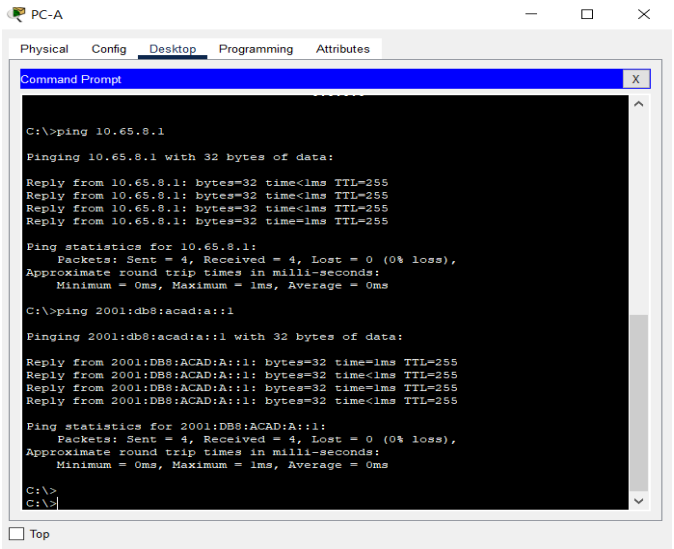
Tabla 18. Pruebas de conectividad de red

Desde	A		Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.20	IPv4	10.65.8.1	Exitoso (Figura 11)
		IPv6	2001:db8:acad:a::1	Exitoso (Figura 11)
	R1, G0/0/1.30	IPv4	10.65.8.65	Exitoso (Figura 12)
		IPv6	2001:db8:acad:b::1	Exitoso (Figura 12)
	R1, G0/0/1.40	IPv4	10.65.8.97	Exitoso (Figura 13)
		IPv6	2001:db8:acad:c::1	Exitoso Figura (13)
	S1, VLAN 40	IPv4	10.65.8.98	Exitoso (Figura 14)
		IPv6	2001:db8:acad:c::98	Fallido (Figura 14)
	S2, VLAN 40	IPv4	10.65.8.99	Exitoso (Figura 15)
		IPv6	2001:db8:acad:c::99	Fallido (Figura 15)
	PC-B	IPv4	10.65.8.85	Exitoso (Figura 16)
		IPv6	2001:db8:acad:b::50	Exitoso (Figura 16)
	R1 Bucle 0	IPv4	209.165.201.1	Exitoso (Figura 17)
		IPv6	2001:db8:acad:209::1	Exitoso (Figura 17)
PC-B	R1 Bucle 0	IPv4	209.165.201.1	Exitoso (Figura 18)
		IPv6	2001:db8:acad:209::1	Exitoso (Figura 18)

	R1, G0/0/1.20	IPv4	10.65.8.1	Exitoso (Figura 19)
		IPv6	2001:db8:acad:a::1	Exitoso (Figura 19)
	R1, G0/0/1.30	IPv4	10.65.8.65	Exitoso (Figura 20)
		IPv6	2001:db8:acad:b::1	Exitoso (Figura 20)
	R1, G0/0/1.40	IPv4	10.65.8.97	Exitoso (Figura 21)
		IPv6	2001:db8:acad:c::1	Exitoso (Figura 21)
	S1, VLAN 40	IPv4	10.65.8.98	Exitoso (Figura 22)
		IPv6	2001:db8:acad:c::98	Fallido (Figura 22)
	S2, VLAN 40	IPv4	10.65.8.99	Exitoso (Figura 23)
		IPv6	2001:db8:acad:c::99	Fallido (Figura 23)
	PC-A	IPv4	10.65.8.53	Exitoso (Figura 24)
		IPv6	2001:db8:acad:a::50	Exitoso (Figura 24)

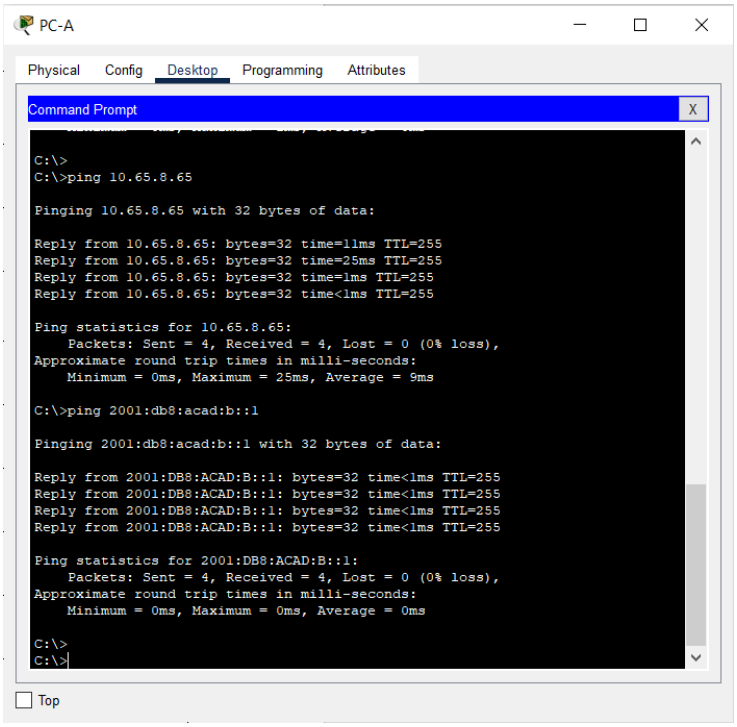
Fuente: Guía Prueba de habilidades practicas CCNA.

Figura 11. Prueba de conectividad desde PC-A a R1 (G0/0/1.20)



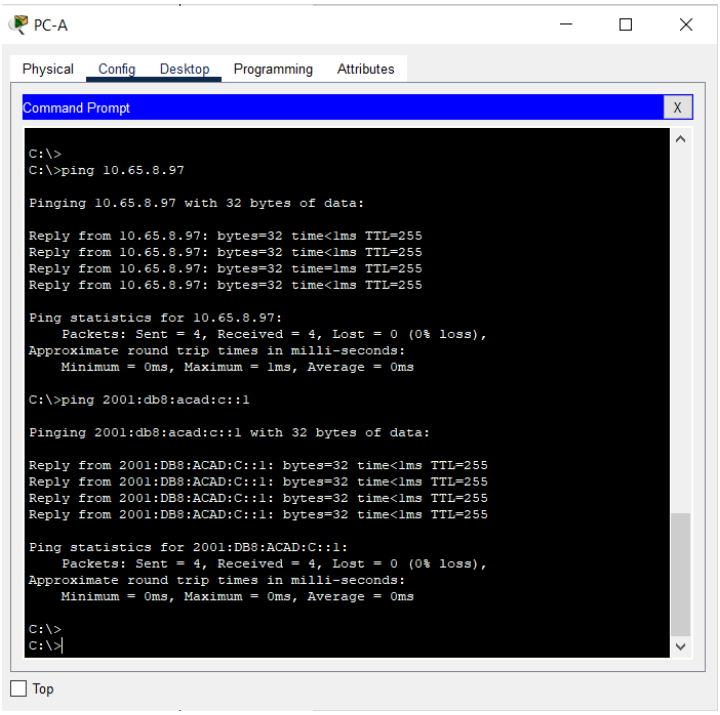
Fuente: Autoría propia

Figura 12. Prueba de conectividad desde PC-A a R1 (G0/0/1.30)



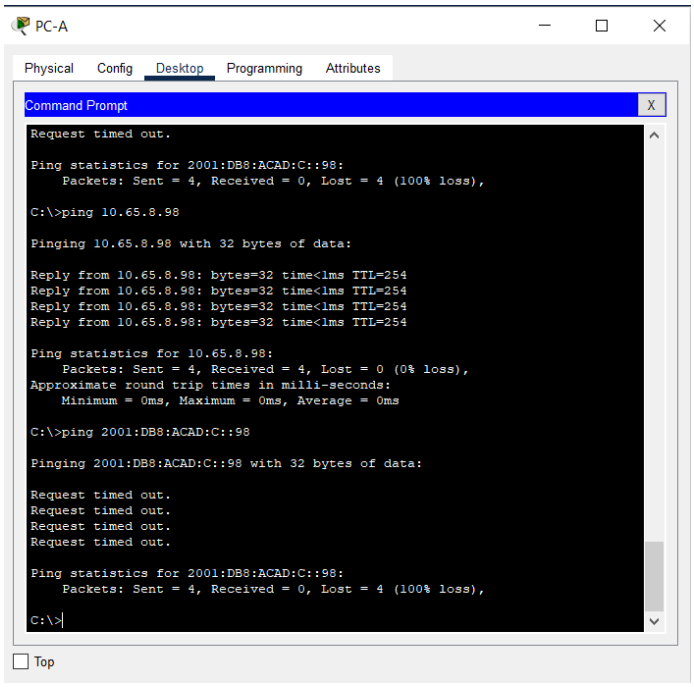
Fuente: Autoría propia

Figura 13. Prueba de conectividad desde PC-A a R1 (G0/0/1.40)



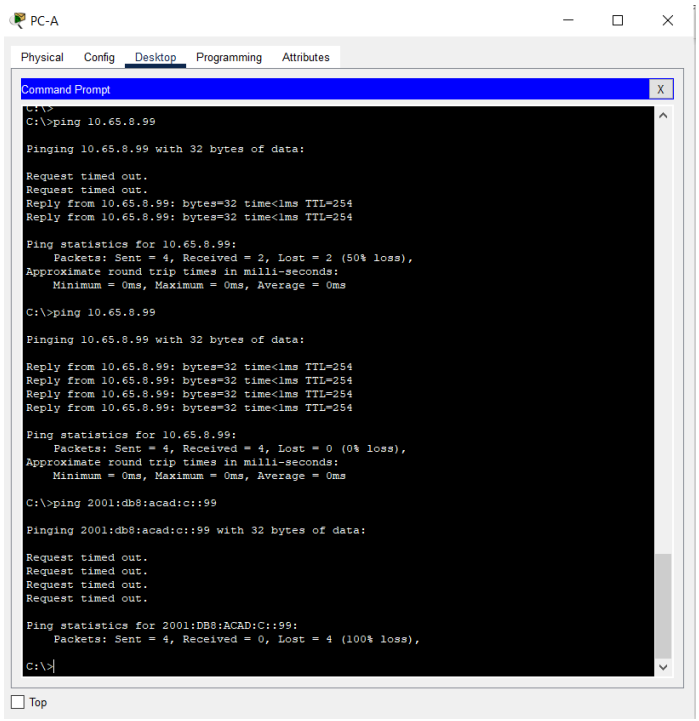
Fuente: Autoría propia

Figura 14. Prueba de conectividad desde PC-A a S1 (VLAN 40)



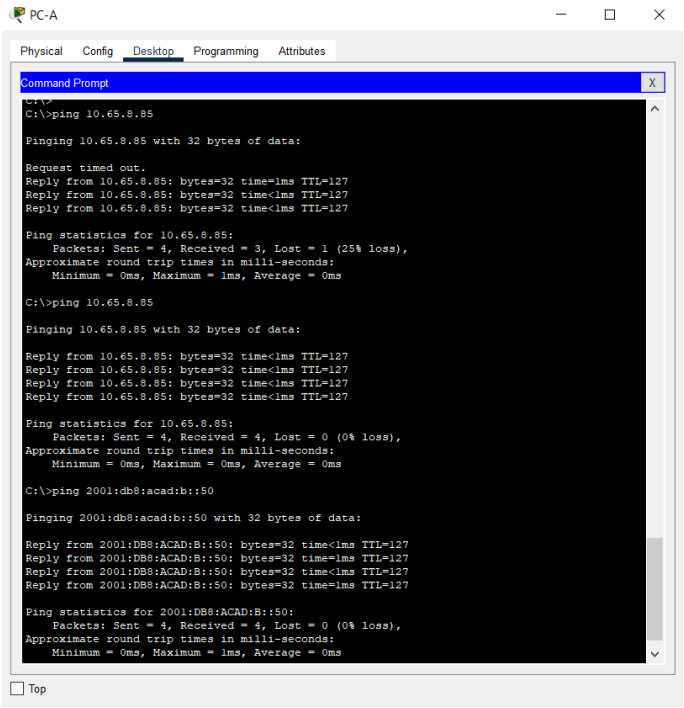
Fuente: Autoría propia

Figura 15. Prueba de conectividad desde PC-A a S2 (VLAN 40)



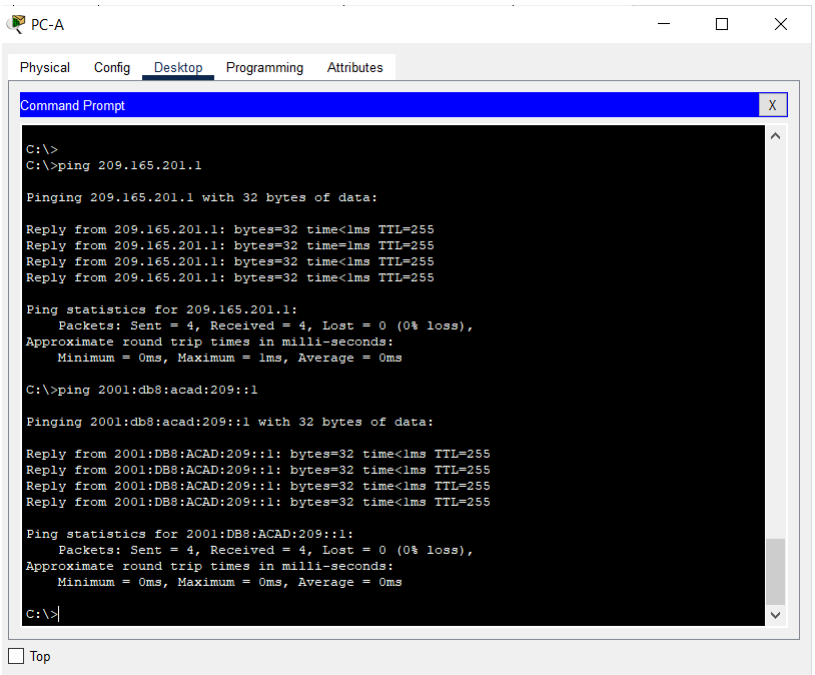
Fuente: Autoría propia

Figura 16. Prueba de conectividad desde PC-A a PC-B



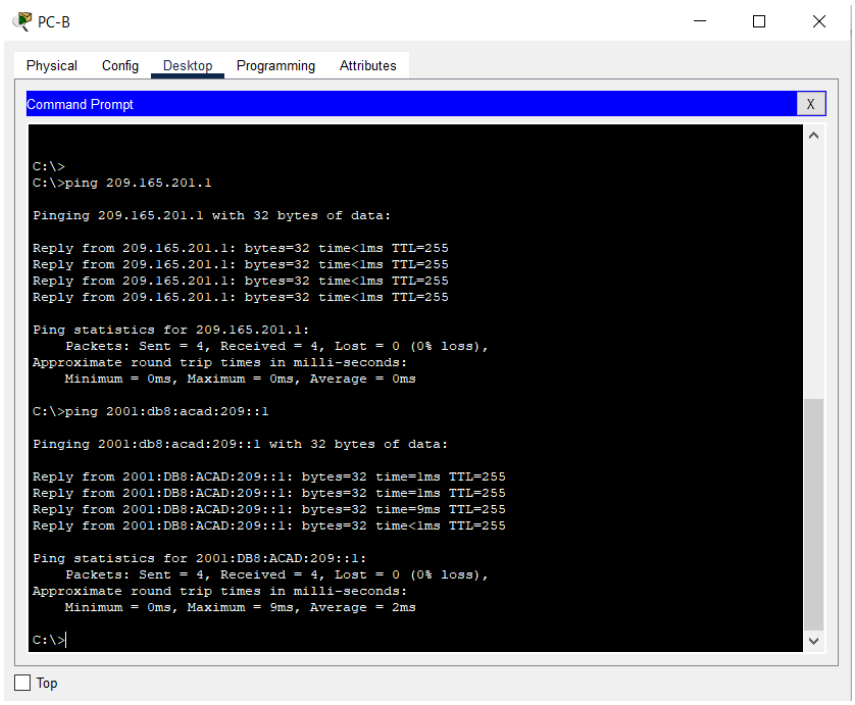
Fuente: Autoría propia

Figura 17. Prueba de conectividad desde PC-A a R1 (Bucle 0)



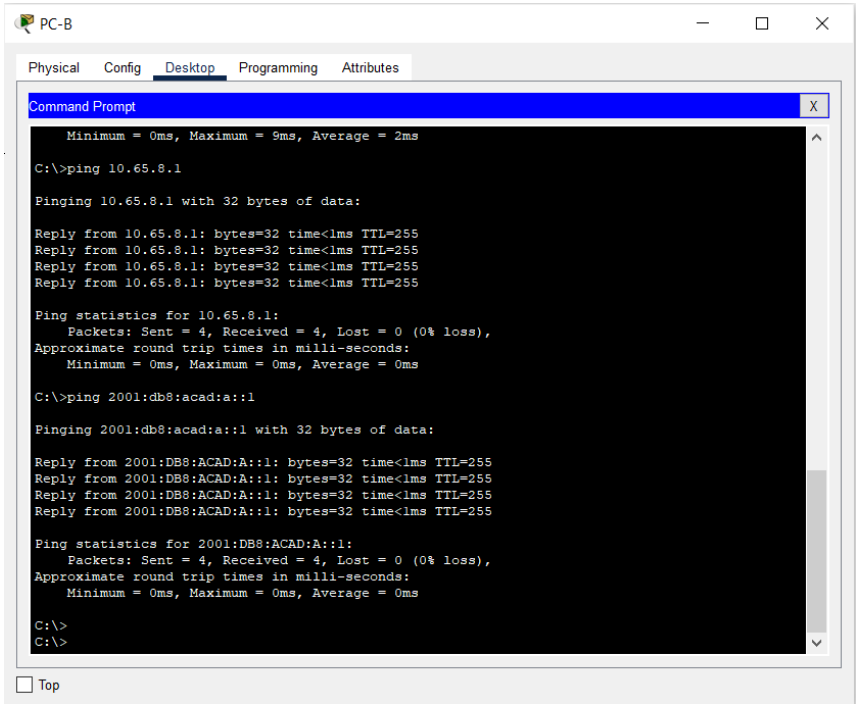
Fuente: Autoría propia

Figura 18. Prueba de conectividad desde PC-B a R1 (Bucle 0)



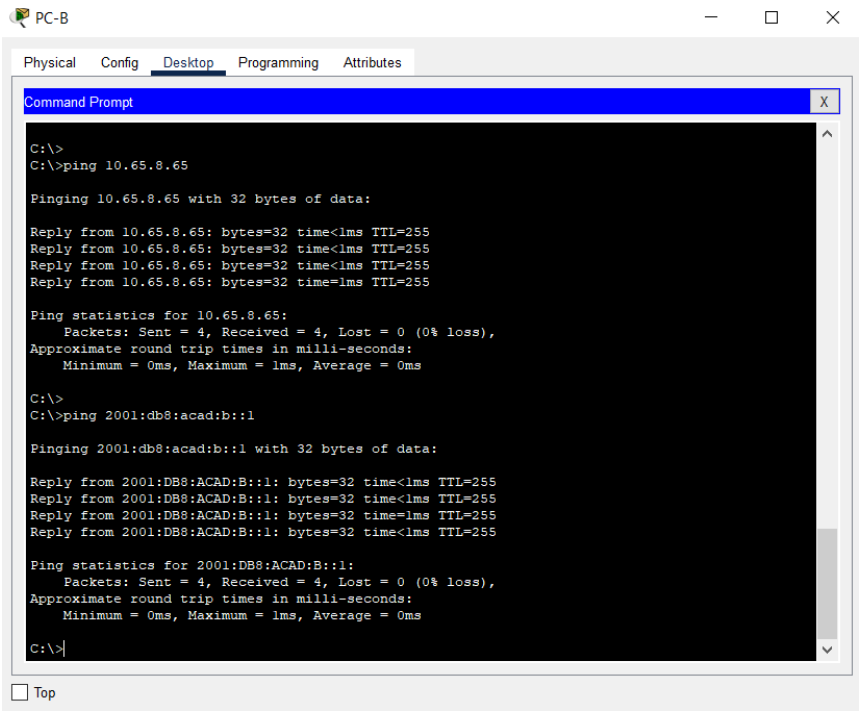
Fuente: Autoría propia

Figura 19. Prueba de conectividad desde PC-B a R1 (G0/0/1.20)



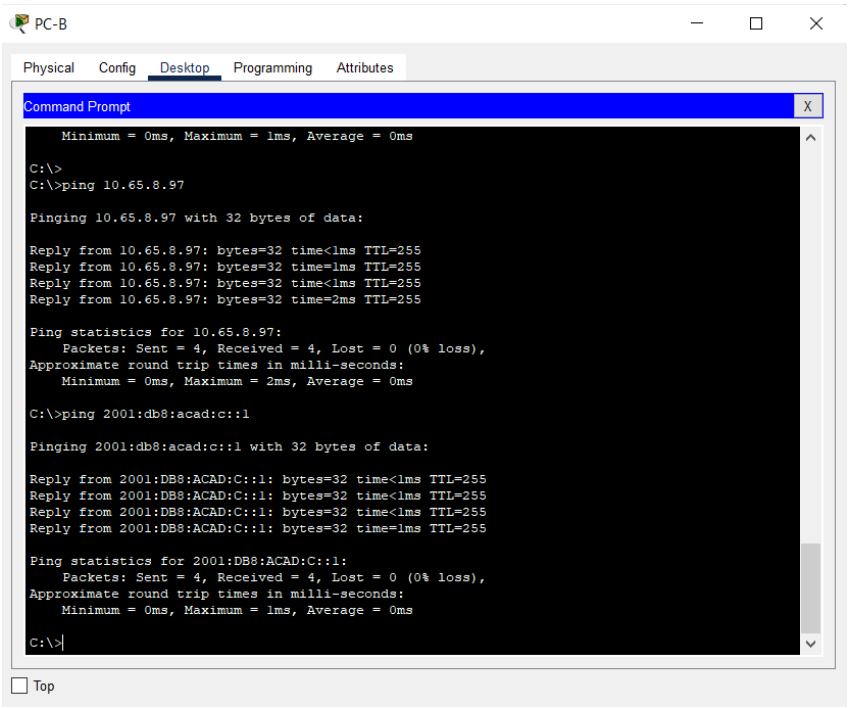
Fuente: Autoría propia

Figura 20. Prueba de conectividad desde PC-B a R1 (G0/0/1.30)



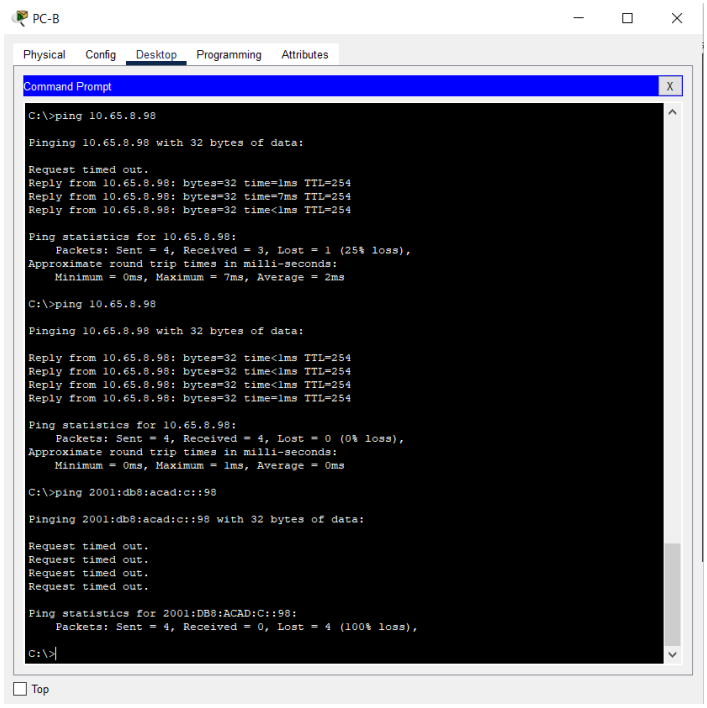
Fuente: Autoría propia

Figura 21. Prueba de conectividad desde PC-B a R1 (G0/0/1.40)



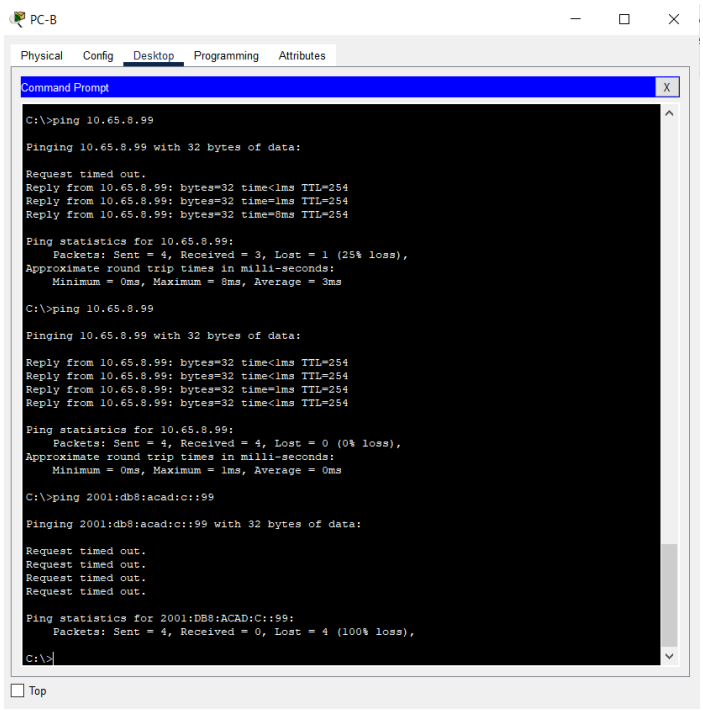
Fuente: Autoría propia

Figura 22.Prueba de conectividad desde PC-B a S1 (VLAN 40)



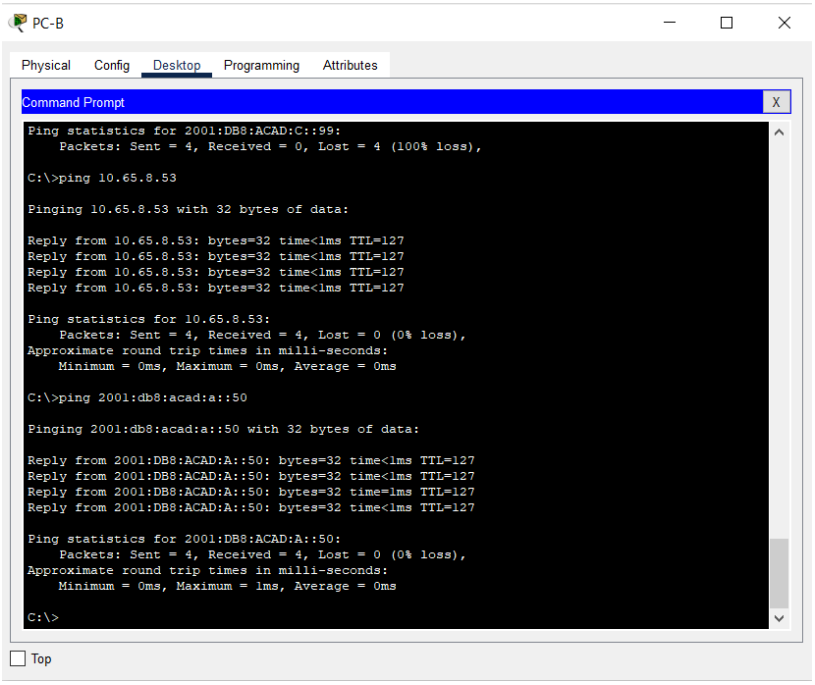
Fuente: Autoría propia

Figura 23. Prueba de conectividad desde PC-B a S2 (VLAN 40)



Fuente: Autoría propia

Figura 24. Prueba de conectividad desde PC-B a PC-A



Fuente: Autoría propia

A través de las anteriores imágenes se evidencia la conectividad desde un dispositivo a otro, para ello se abre la consola de comandos y se escribe el comando ping seguido de la dirección IP según corresponda (ver tabla 18).

Es de tener presente que si el ping en protocolo IPv6 de las SVI de los swich (VLAN40) fallaron esto se debe a que es la interfaz de administración del switch

CONCLUSIONES

El cálculo del Subneteo a través de VLSM nos permite en el escenario 1 tener un mejor aprovechamiento de la red, ya que por otro método como el FSLM se desperdiciarían grandes direcciones IP.

Mediante el uso de uso de herramientas de simulación, se desarrolla dos escenarios LAN/WAN, el cual permite realizar un estudio sobre los diferentes protocolos, métricas de enrutamiento y evaluación de riesgos en las redes informáticas.

La configuración básica realizada en los dispositivos intermedios, así como la distribución de la infraestructura de red en los switches y de soporte host en el router, permite asignar direcciones IP aleatoria por DHCPv4 en los dispositivos finales, lo cual, al momento de realizar los ping de verificación de conectividad se identifica que todos los ping en las diferentes interfaces y VLAN son exitosos, sin embargo, los ping en protocolo IPv6 aplicados en la SVI (VLAN40) de los switches fallan, por tanto, esto se debe a que ésta es la interfaz de administración de los switches.

BIBLIOGRAFIA

CAFFA, Angel. Conceptos de redes de computadoras [en línea]. Montevideo: Udelar.CSEP, (2005) [consultado el 27, noviembre, 2022]. 75 p. Disponible en https://hdl.handle.net/20.500.12008/9583

CASTAÑO, R. y LOPEZ, F. Redes locales [en línea]. Madrid: Macmillan Iberia, S.A. [Consultado el 27, noviembre, 2022]. Disponible https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43257?page=133

CCNA DE CERO, ¿Qué es DNS? [en línea] (2020) [Consultado 26 de noviembre de 2022] Disponible en: https://ccnadesdecero.es/que-es-dns/

CCNA DE CERO, Funcionamiento de EtherChannel [en línea] (2020) [Consultado 26 de noviembre de 2022] Disponible en: https://ccnadesdecero.es/funcionamiento-etherchannel/#2_EtherChannel

CISCO. Configurar ACL de IP de uso general. [en línea] (2022) [Consultado 25 de noviembre de 2022] Disponible en https://www.cisco.com/c/es_mx/support/docs/ip/access-lists/26448-ACLsamples.html

CISCO. Las redes en la actualidad. Introducción a Redes [en línea] (2020) [Consultado 25 de noviembre de 2022] Disponible en: https://contenthub.netacad.com/itn-dl/1.9.1

CISCO, Conceptos de DHCPv4. Switching, Routing, y Wireless Essentials. [en línea] (2020) [Consultado 26 de noviembre de 2022] Disponible en: https://contenthub.netacad.com/srwe-dl/7.1.1

CISCO, Introducción a DTP. Switching, Routing, and Wireless Essentials [en línea] (2020) [Consultado 26 de noviembre de 2022] Disponible en: https://contenthub.netacad.com/srwe-dl/3.5.1

CISCO, Community. Conceptos Fundamentales de enrutamiento. [documento en linea] (S.f) [Consultado 26 de noviembre de 2022] Disponible en: https://community.cisco.com/legacyfs/online/attachments/document/enrutamiento-conceptos_basicos.pdf

CISCO. Conceptos de FHRP. Switching, Routing, y Wireless Essentials. [en línea] (2020) [Consultado el 27, noviembre, 2022]. Disponible en: https://contenthub.netacad.com/srwe-dl/9.2.1

CISCO. Tipos comunes de Redes. Introducción a las redes. [en línea] (2020) [Consultado el 27, noviembre, 2022]. Disponible en: https://contenthub.netacad.com/itn-dl/1.4.2

FERNÁNDEZ, Yúbal. FTP: qué es y cómo funciona. Xataka [en línea]. (15, julio, 2021). [Consultado el 27, noviembre, 2022]. Disponible en: https://www.xataka.com/basics/ftp-que-como-funciona

NIÑO, Elías. Fundamentos para el desarrollo de aplicaciones en la red. Universidad del Norte [página web]. (2012). [Consultado el 27, noviembre, 2022]. Disponible en: https://manglar.uninorte.edu.co/bitstream/handle/10584/2205/Modelo%20cliente%20servidor.pdf?sequence=2

RINCON V, Liliana y ANDRADE M, Jesús. Configurando un acceso administrativo seguro. Universidad Autónoma del Estado de Hidalgo: UAEH. [página web]. (2017). [Consultado el 27, noviembre, 2022]. Disponible en: https://www.uaeh.edu.mx/scige/boletin/tepeji/n8/e1.html#:~:text=Línea%20de%20terminal%20virtual,los%20subcomandos%20password%20y%20login.

ANEXOS

ANEXO – A

Escenario 1

Escenario 2