INFORME - PRUEBA DE HABILIDADES PRACTICAS

ELIECER ADOLFO GUZMAN BARRIOS

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

Cartagena de Indias
2022

INFORME - PRUEBA DE HABILIDADES PRACTICAS

ELIECER ADOLFO GUZMAN BARRIOS

Diplomado como opción de grado para optar al título de INGENIERO DE SISTEMAS

PAULITA FLOR SALAZAR

TUTORA

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

Cartagena de Indias
2022

Nota de aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Cartagena de Indias, 13 de diciembre de 2022

AGRADECIMIENTOS

Agradezco principalmente a Dios, por su amor, su bondad y sus bendiciones, quien ha hecho posible el poder llegar donde estoy hoy. Gracias infinitas a mis abuelos, David y Tulia (QEPD), por enseñarme valores y educarme con tanto amor, a mi compañera de vida por ser siempre mi apoyo en todo en momento, a los profesores y a esta universidad por guiarme y formarme profesionalmente, y a mis compañeros de estudio por todo su apoyo.

Hoy, a un paso de obtener mi título como profesional en Ingeniería de Sistemas en la Universidad Nacional Abierta y a Distancia, solo tengo infinito agradecimiento hacia aquellos que han aportado a mi proceso profesional y a mi vida personal.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

DHCP: “es un protocolo cliente/servidor que proporciona automáticamente un host de Protocolo de Internet (IP) con su dirección IP y otra información de configuración relacionada, como la máscara de subred y la puerta de enlace predeterminada” [1]

IP: “es una representación numérica del punto de Internet donde está conectado un dispositivo. Se usa para identificar dónde hay algo y, en cierto modo, qué es. Comprender los fundamentos de las direcciones IP es esencial para desenvolverse por Internet. Aprenda cómo funcionan las direcciones IP y por qué es tan importante proteger la suya” [2]

ROUTER: “es un dispositivo que nos permite conectar diferentes tipos de equipos que funcionan en una red, esta red puede ser de manera cableada o inalámbrica entonces el router nos ayuda a crear la ruta que enviara cada paquete de datos a la red”[3]

SWITCH: “son dispositivos que crean una red que conecta diferentes dispositivos, pero solo en una red local, los switches envían la información a un solo equipo y estos no tiene la facultad de replicarse en los demás dispositivos, al switch le configuramos la MAC del equipo al cual queremos enviarle información y este no le enviara la información a ningún equipo más” [4]

VTY: “Que significa línea de terminal virtual, las líneas vty nos brindan el acceso a los dispositivos CISCO a través de Telnet de forma predeterminada, en los router estos puertos pueden ir del 0 al 15, para poder utilizarlo tenemos que usar el comando line vty 0 15 y también usamos los subcomandos password y login”[5]

[1] Microsoft. (29 de septiembre de 2022). Protocolo de configuración dinámica de host (DHCP). Obtenido de https://learn.microsoft.com/es-es/windows-server/networking/technologies/dhcp/dhcp-top

[2] Avast. (14 de Julio de 2022). ¿Qué es una dirección IP? Obtenido de https://www.avast.com/es-es/c-what-is-an-ipaddress

[3] 3 Cisco. (s.f.). ¿Qué es un router? Obtenido de https://www.cisco.com/c/es_mx/solutions/small-business/resourcecenter/networking/what-is-a-router.html

[4] Movistar. (2021). Switch de red: ¿cómo facilita las telecomunicaciones en tu hogar? Obtenido de https://www.movistar.es/blog/alarmas/alarma-conectada-vigilancia-constante/

[5] CISCO, Netacad. Introducción a las redes – Configuración de interfaz virtual de switch (2022) {3 de noviembre de 2022}. Disponible en https://contenthub.netacad.com/itndl/2.7.4

RESUMEN

Estudiaremos dos topologías diferentes separadas por dos escenarios, en cual se muestra la manera en la cual se deben configurar estos dos tipos de redes, ésta creación de redes estará bajo la plataforma de redes CISCO que nos brinda un programa que es una herramienta de simulación y configuración de redes y demás funciones.

El primer escenario es la configuración de una red pequeña, donde utilizaremos equipos como el switch, router y computadores, debemos diseñarla configuración de red para estos a través de las LAN y utilizando el protocolo de red IPV4.

Para el segundo escenario y aunque la red es pequeña abordaremos temas y veremos la configuración como la IPV6, VLAN t DHCP, cada uno de estos comandos siempre van a ir conectados entre sí por los diferentes protocolos, lo que nos hará el correcto funcionamiento de la red.

Para los dos escenarios estará plasmado el paso a paso utilizados para el correcto funcionamiento de la red, al final veremos unas pruebas de ping utilizadas para demostrar que las redes están conectadas entre sí.

PALABRAS CLAVES: Redes, Protocolo, LAN, Cisco, Redes.

ABSTRACT

We will study two different topologies separated by two scenarios, which showsthe way in which these two types of networks should be configured, this networking will be under the CISCO networking platform that gives us a program that is a tool for simulation and network configuration and other functions.

The first scenario is the configuration of a small network, where we will use equipment such as the switch, router and computers, we must design the network configuration for these through the LAN and using the IPV4 network protocol.

For the second scenario and although the network is small, we will address issues and see the configuration as the IPV6, VLAN and DHCP, each of thesecommands will always be connected to each other by different protocols, whichwill make us the proper functioning of the network.

For the two scenarios will be captured step by step used for the correct operation of the network, at the end we will see some ping tests used to demonstrate that the networks are connected to each other.

KEY WORDS: Networks, Protocol, LAN, Cisco, Networks.

INTRODUCCIÓN

Si bien es cierto que el uso de internet se ha vuelto en estos tiempos algo muy popular y aunque pensemos que el usar esta herramienta es solo poner la clave en nuestro dispositivo como Smartphone, Tablet, Laptop, Tv etc., conectarnos y empezar a consumir del internet, estamos un poco errados ya que esto es un poco más complejo y para entender cómo es que ese internet o como esa información llega a nuestro dispositivo es que este trabajo nos va a servir.

En este documento está plasmado los conocimientos adquiridos durante este tiempo, y que nos permitirá a posterior entender conceptos claves en la configuración de una red, crear una buena práctica del uso correcto de la armada de una red, y aunque las redes que se mostraran son sencillas, se manejan todos los conceptos con los cuales se puede configurar cualquier red.

Los dos escenarios abordados en esta práctica de CCNA se trabajarán bajo el simulador de PACKET TRACER herramienta bastante robusta y que nos dará todas las herramientas necesarias para el correcto manejo de esta práctica.

Se dejará un paso a paso detallado de la manera en la cual se usó los diferentes protocolos, además de la configuración que se utiliza desde la configuración de 0 de un switch o router, también podemos ver las pruebas de Ping echas en los equipos los cuales nos brindan una idea de lo acertado que fue hacer esa configuración en cada equipo.

DESARROLLO ESCENARIO 1

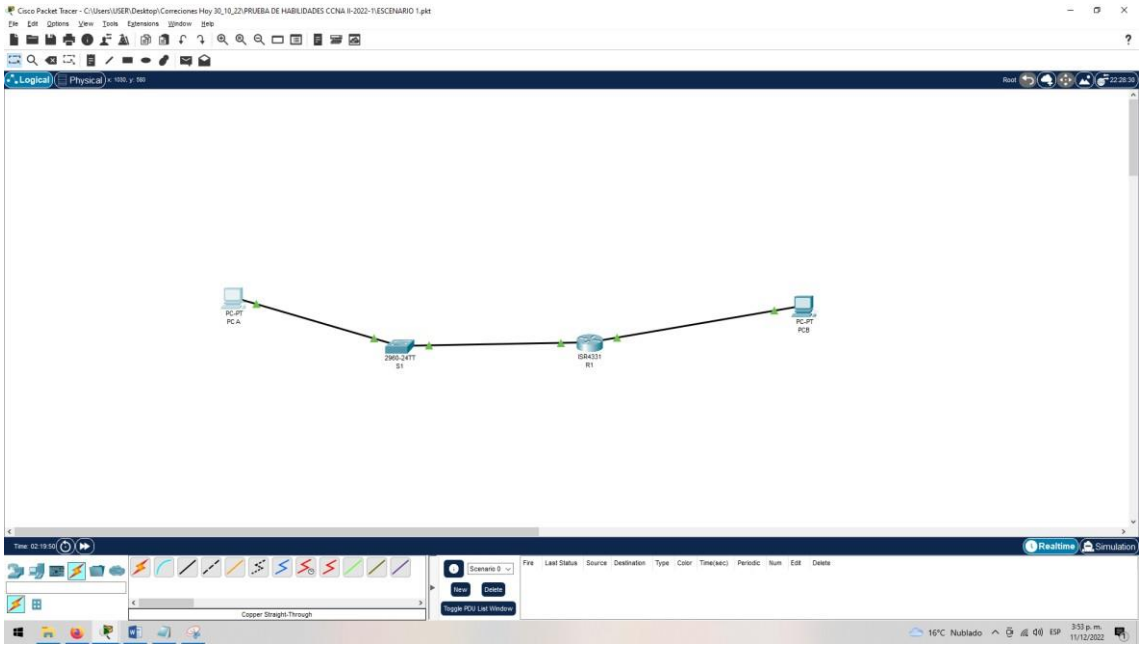
En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un Reuter, un switch y equipos, diseñar el esquema de direccionamiento IPv4 para las LAN propuestas. El Router y el switch también deben administrarse de forma segura.

Topología

Figura 1 Topología primer escenario

Fuente: Prueba de habilidades CCNA

Figura 2 topología escenario 1 en Packet Tracer



Fuente. Elaboración 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/situación.

En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el swich S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (60 host) y la LAN2 (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, cablee conforme se indica en la topología, y conéctelos equipos de cómputo.

Parte 2: Desarrolle el 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 tomará el direccionamiento 172.XY.3.0 donde XY corresponde a los últimos dos dígitos de su cédula, en este caso y como mi número de documento termina en 19 la dirección que utilizare para trabajar será 172.43.3.0

Tabla 1 direccionamiento IP

Ítem	Requerimiento
Dirección de Red	172.43.3.0 donde XY corresponde a los últimos dos dígitos de su cédula.
Requerimiento de host Subred LAN1	60
Requerimiento de host Subred LAN2	20
R1 G0/0/1	172.43.3.62 / 255.255.255.192
R1 G0/0/0	172.43.3.94 / 255.255.255.224
S1 SVI	172.43.3.4 / 255.255.255.192
PC-A	172.43.3.10 / 255.255.255.192
PC-B	172.43.3.75 / 255.255.255.224

Fuente. Elaboración propia

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

Paso 1: configurar los ajustes básicos
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 2 Configuración router 1 R1

	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure t Router#configure terminal **Router(config)#no ip domain-lookup** Router(config)#
Nombre del router	**Router(config)#hostname R1** R1(config)#
Nombre de dominio	**R1(config)#ip domain name ccna-sa.com** R1(config)#
Contraseña cifrada para el modo EXEC privilegiado	**R1(config)#enable secret ciscoenpass** R1(config)#
Contraseña de acceso a laconsola	**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	**R1(config)#security passwords min-length 10** R1(config)#
Crear un usuario administrativo en la base de datos local	R1(config)#username admin secret admin1pass R1(config)#
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 R1(config-line)#

Configurar las líneas VTY para que acepten únicamente las conexiones SSH	R1(config-line)#transport input ssh R1(config-line)#exit R1(config)#
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption R1(config)#
Configurar un banner MOTD	R1(config)#banner motd ' R1-ELIECER GUZMAN-INGENIERIA DE SISTEMAS ' R1(config)#
Configuración de interface G0/0/0	R1(config)#interface g R1(config)#interface gigabitEthernet 0/0/0 R1(config-if)#ip address 172.43.3.94 255.255.255.224 R1(config-if)#no shutdown
Configuración de interface G0/0/1	R1(config)#interface g R1(config)#interface gigabitEthernet 0/0/1 R1(config-if)#ip address 172.43.3.62 255.255.255.192 R1(config-if)#no shutdown
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa general-keys modulus 1024

Fuente. Elaboración propia

Lo primero que hacemos es desactivar la búsqueda el DNS, iniciamos el router con el comando Router>enable después entramos a la configuración de la terminal de configuración con el comando Router#configure terminal y después agregamos el comando para desactivar los DNS del router con el comando Router(config)#no ip domain-lookup.

Continuamos con la asignación del nombre del router en este caso nombramos R1 con el comando Router(config)#hostname R1.

Agregamos el dominio al router con el comando R1(config)#ip domain name ccna-sa.com es decir que cuando se quiera comunicara este router R1 podemos acceder a través de ccna-sa.com desde el navegador y el router se nos va a conectar para hacerle la configuración o lo que necesitamos hacer.

Procedemos a cifrar nuestra contraseña con el comando R1(config)#enable secret ciscoenpass.

Continuamos con la configuración de consola para colocarle la contraseña de acceso y para esto utilizaremos el comando para entrar primero a la consola que sería R1(config)#line console 0 después agregamos el comando para agregar la contraseña R1(config-line) #password ciscoconpass y escribimos el comando R1(config-line) #login para que esta contraseña se nos active.

Procedemos a establecer la longitud mínima para las contraseñas que en este caso es de 10 caracteres y colocaremos el comando R1(config)#security passwords min-length 10.

Continuamos creando el usuario administrativo del router que en este caso sería admin y la contraseña admin1pass y lo configuramos con el comando R1(config)#username admin secret admin1pass.

Procedemos a configurar las líneas VTY que a la hora de iniciar sesión nos use la base de datos local y para esto utilizaremos el comando R1(config)#line vty 0 4 seguido del comando R1(config-line) #login local para iniciarla.

Configuramos las líneas VTY para que solo nos utilice las conexionesSSH, utilizamos el comando R1(config-line) #transport input ssh y con el comando R1(config-line) #exit salimos del modo de configuración delas líneas VTY.

Y procedemos a cifrar la contraseña de texto con el comando R1(config)# service password-encryption.

Agregamos el banner del router, este banner nos saldrá al inicio del router podemos la información que queramos y para este utilizaremos el comando R1(config)#banner motd y agregamos entre comillas simples el mensaje que queremos que se nos muestre en este caso colocamos ' R1-ELIECER GUZMAN-INGENIERÍA DE SISTEMAS '.

Y ahora continuamos con la configuración de las interfaces empezamos con la interfaz G0/0/0 con el siguiente comando R1(config)#interface gigabit Ethernet 0/0/0 y agregamos la dirección IP seguida de la máscara de red con el siguiente comando R1(config- if) #ip address 172.43.3.94 255.255.255.224 y al finalizar colocamos el comando R1(config-if) #no shutdown y este lo utilizamos para activar el puerto.

Y después configuramos la interfaz G0/0/1 con el siguiente comando R1(config)#interface gigabit Ethernet 0/0/1 y agregamos la dirección IP seguida de la máscara de red con el siguiente R1(config-if) #ip address 172.43.3.62 255.255.255.192 y al finalizar colocamos el comando R1(config- if) #no shutdown y este lo utilizamos para activar el puerto en este caso G0/0/1.

Y por último configuramos la clave de cifrado RSA con el siguiente comando R1(config)#crypto key generate rsa general-keys modulus1024

Tabla 3 Configuración del switch 1 S1

Tarea	**Especificación**
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal . Switch(config)#no ip domain-lookup Switch(config)#
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio	S1(config)#ip domain name ccna-sa.com S1(config)#
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass S1(config)#
Contraseña de acceso a la consola	S1(config)#line 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit S1(config)#

Apagar todos los puertos sin usar	Los puertos sin usar siempre van a estar apagados y siempre que queramos activar uno de esos puertos debemos usar el comando no shutdown o conectarle algo a eseswitch.
Crear un usuario administrativo en la base de datos local	S1(config)#username admin secret admin1pass
	S1(config)#
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)#login local S1(config-line)#exit S1(config)#
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)#line vty 0 4 S1(config-line)#transport input ssh S1(config-line)#exit S1(config)#
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption S1(config)#
Configurar un banner MOTD	S1(config)#banner motd ' S1-ELICER GUZMAN- INGENIERIA DE SISTEMAS ' S1(config)#
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)#interface vlan 1 S1(config-if)#des S1(config-if)#description S1-ELIECER GUZMAN-CONEXION RED VIRTUAL-SUBRED A S1(config-if)#ip address 172.43.3.4 255.255.255.192 S1(config-if)#no shutdown S1(config)#ip default-gateway 172.43.3.1 S1(config)#exit

Fuente. Elaboración propia

Lo primero que hacemos es desactivar la búsqueda el DNS, iniciamos el switch con el comando Switch>enable, después entramos a la configuración de la terminal de configuración con el comando Switch#configure terminal y después agregamos el comando para desactivar los DNS del switch con el comando Switch(config)#no ip domain-lookup.

Continuamos con la asignación del nombre del switch en este caso le colocaremos S1 con el comando Switch(config)#hostname S1 y en la siguiente línea de código ya nos muestra el nuevo nombre asignado.

Procedemos a agregar el dominio del switwch en este caso utilizaremos el comando S1(config)#ip domain name ccna-sa.com.

Agregamos la contraseña cifrada para el modo EXEC privilegiado utilizando el comando S1(config)#enable secret ciscoenpass.

Continuamos con la configuración de consola para colocarle la contraseña de acceso y para esto utilizaremos el comando para entrar primero a la consola que sería S1(config)#line 0 después agregamos el comando para agregar la S1(config- line) #password ciscoconpass y escribimos el comando S1(config-line)#login para que esta contraseñase nos active.

En los switches los puertos siempre estarán apagados solo existen dos maneras para activarlos, las primeras serian conectándolo algún dispositivo por uno de sus puertos y la segunda haciéndole un no shutdown por consola.

Continuamos creando el usuario administrativo y para esto utilizaremos el comando S1(config)#username admin secretadmin1pass.

Configuramos el inicio de sesión en las líneas VTY para que use la base de datos local y para esto escribimos el comando S1(config)#linevty 0 4 y después escribimos S1(config-line) #login local para iniciarlo y por ultimo escribimos S1(config-line) #exit para salir de este modo.

Procedemos a configurar las líneas VTY para que solo nos acepte las conexiones SSH y para esto utilizamos el comando S1(config)#line vty 0 4 seguido del comando S1(config-line) #transport input ssh y finalizamos S1(config-line) #exit para salir de ese modo.

Para cifrar las contraseñas de texto no cifrado utilizamos el comando S1(config)#service password-encryption.

Configuramos el banner del switch, este banner nos saldrá al inicio del switch en este ponemos la información que queramos y para este utilizaremos el comando S1(config)#banner motd y agregamos entre comillas simples el mensaje que queremos que se nos muestre en este caso colocamos ' S1-ELIECER GUZMAN-INGENIERÍA DE SISTEMAS '.

Continuamos configurando la clave de cifrado RSA con el código S1(config)#crypto key generate rsa general-keys modulus 1024 y debemos tener en cuenta que al final se agrega el número de bits queen este caso es 1024.

Y ya por último configuramos la descripción de nuestro switch en este caso utilizaremos el comando S1(config)#interface vlan 1 seguido de S1(config-if)#description S1-ELIECER GUZMAN-CONEXION RED VIRTUAL-SUBRED A y ya finalizando establecemos la dirección IP con su mascara de red utilizando el comando S1(config-if)#ip address 172.43.3.2 255.255.255.192 la inicializamos con el comando S1(config-if)#no shutdown y por ultimo también configuramos el Gateway de esta red y para esto Utilizamos el comando S1(config)#ipdefault-gateway 172.43.3.1 .

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 Configuración de red PC-A

Configuración de red de PC-A	
Descripción	FastEthernet0 connection: (default port)
Dirección física	FE80::205:5EFF:FEEB:17AE
Dirección IPv4	172.43.3.10
Máscara de subred	255.255.255.192

Puerta de enlace IPv4 predeterminada	172.43.3.62

Fuente. Elaboración propia

Para la configuración del PC-A debemos tener en cuenta la tabla de direccionamiento, puesto que hay encontraremos las direcciones que utilizaremos para configurar este pc, en el apartado descripción colocaremos el puerto en el cual se está conectando este equipo es decir el puertoFastEthernet0 este sería el puerto donde llegaría nuestro cable de red, la dirección fisca la sacamos por comando y para esto utilizaremos el comando ipconfig /all, la dirección, la máscara y la puerta de enlace directamente con la tabla.

Tabla 5 Configuración de red PC-B

Configuración de red de PC-B	
Descripción	FastEthernet0 connection: (default port)
Dirección física	FE80::207:ECFF:FE6C:D85C
Dirección IPv4	172.43.3.75
Máscara de subred	255.255.255.224
Puerta de enlace IPv4 predeterminada	172.43.3.94

Fuente. Elaboración propia

Al igual que para el PC-A para llenar estos campos utilizaremos los mismos pasos que se utilizaron para ese pc pero obviamente colocando los datos correspondientes al PC-B que serían tener en cuenta la tabla de direccionamiento, puesto que hay encontraremos las direcciones que utilizaremos para configurar este pc, en el apartado descripción colocaremos el puerto en el cual se está conectando este equipo es decir el puerto FastEthernet0 este sería el puerto donde llegaría nuestro cable de red, la dirección fisca la sacamos por comando y para esto utilizaremos el comando ipconfig /all, la dirección, la máscara y la puerta de enlace directamente con la tabla.

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

Utilice el comando ping para probar la conectividad entre todos los dispositivos de red. Nota: Si los pings a los servidores fallan, deshabilite temporalmente el firewall del equipo y vuelva a realizar la verificación. Utilícela siguiente tabla para

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

Tabla 6 Prueba de ping

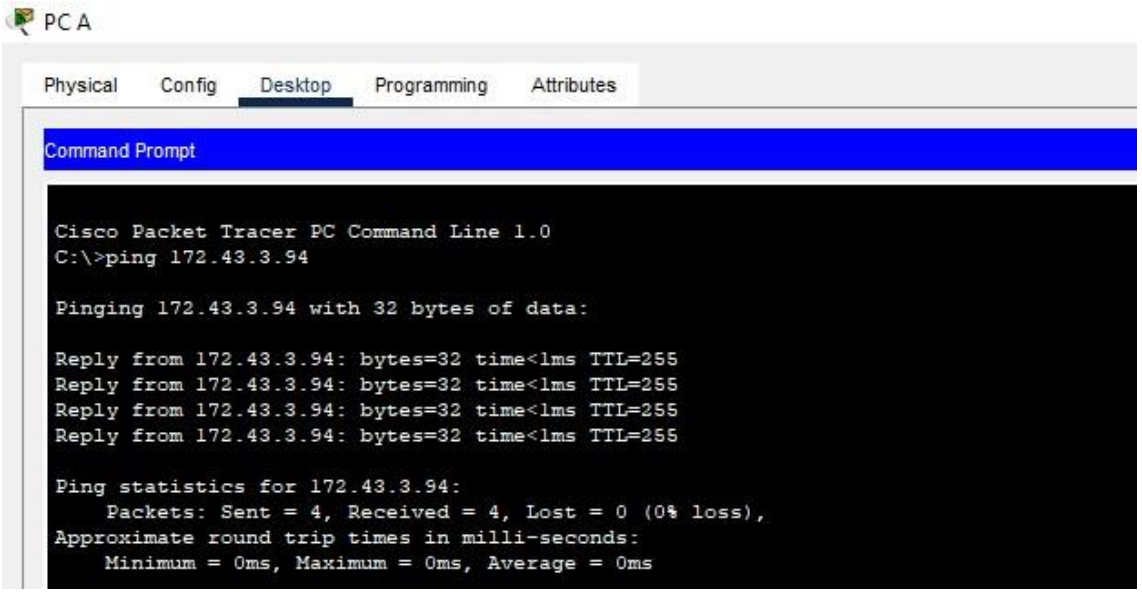
Desde	A	Dirección IP	Resultados deping
PC-A	R1 G0/0/0	172.43.3.94	CORRECTO
	R1 G0/0/1	172.43.3.62	CORRECTO
	S1 VLAN 1	172.43.3.4	CORRECTO
	PC-B	172.43.3.75	CORRECTO
PC-B	R1 G0/0/0	172.43.3.94	CORRECTO
	R1 G0/0/1	172.43.3.62	CORRECTO
	S1 VLAN1	172.43.3.4	CORRECTO

Fuente. Elaboración propia

Para la prueba de ping utilizamos la consola, ya que esta nos permite escribir el comando con lo cual podemos verificar la conexión de los equipos y de esta manera saber que la configuración que se hizo fue correcta, el comando que se utiliza es ping seguido de la dirección del equipo que se quiere verificar la conexión.

PRUEBAS DE PING ESCENARIO 1

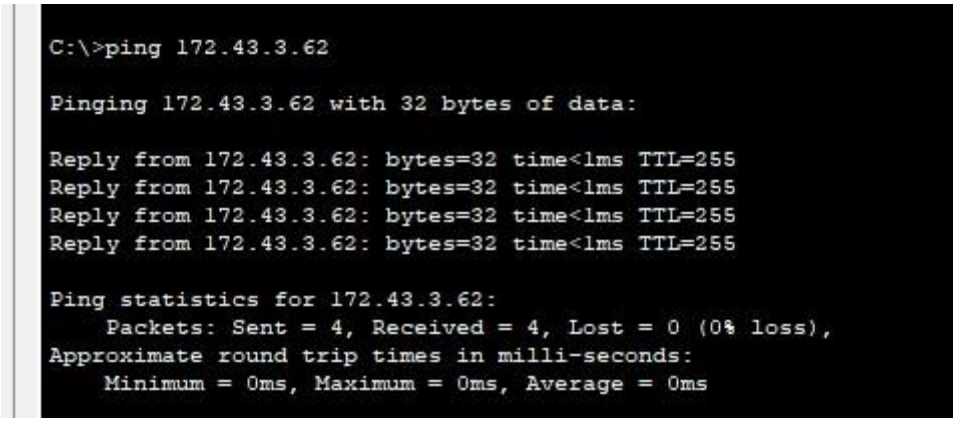
Figura 3 Prueba de ping PC-A a R1 G0/0/0



Fuente. Elaboración propia

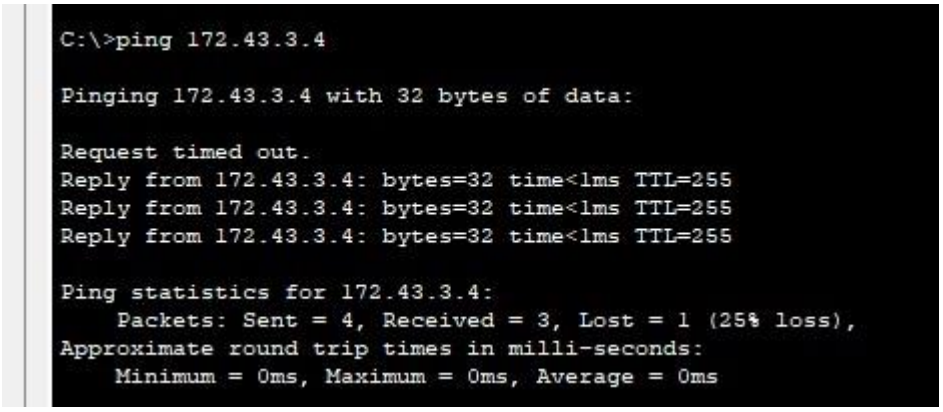
En la primera prueba de ping que realizamos seria del PC-A al R1 G0/0/0 y para esta utilizamos la dirección IP 172.43.3.94 la cual nos muestra un resultado de cuatro paquetes enviados y 4 recibidos lo que quiere decir que la comunicación se efectuó con éxito.

Figura 4 Prueba de ping PC-A a R1 G0/0/1



La siguiente prueba de ping se hizo desde el PC-A al R1 G0/0/1 y para esta se utilizó la dirección IP 172.43.3.62 y esta prueba nos arrojó un total de 4 paquetes enviados y 4 recibidos lo cual nos dice que el ping se realizó correctamente.

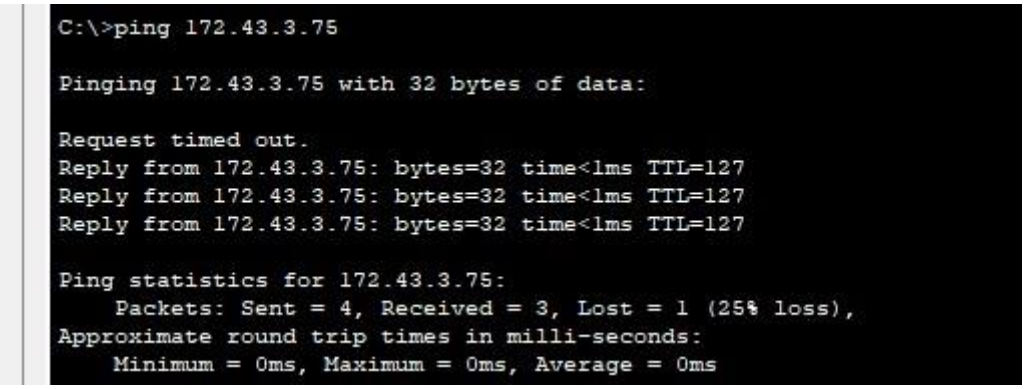
Figura 5 prueba ping a S1 VLAN 1



Fuente. Elaboración propia

En esta prueba de ping el resultado fue de 4 paquetes enviados y 3 paquetes recibidos lo que quiere decir que la conexión quedo medianamente correcta y el ping salió correcto en un 75%, este ping pertenece al PC-A al S1 en el puerto S1 VLAN 1 utilizando la dirección 172.43.3.4

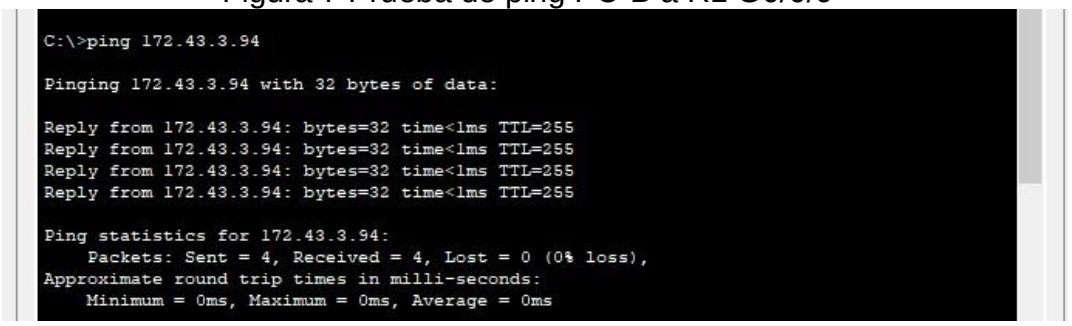
Figura 6 Prueba de ping PC-A a PC-B



Fuente. Elaboración propia

Esta es la última prueba de ping que se hace desde el PC-A y fue hacia el PC-B utilizando la dirección IP 172.43.3.75 y esta prueba nos arrojó 4 paquetes enviados y 3 paquetes recibidos lo que quiere decir que la conexión es medianamente correcta.

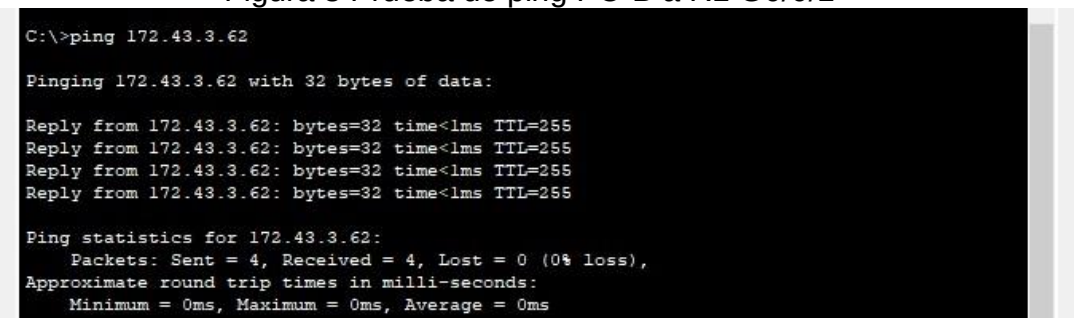
Figura 7 Prueba de ping PC-B a R1 G0/0/0



Fuente. Elaboración propia

Para la prueba de ping entre el PC-B y el router R1 se utilizó el puerto G0/0/0 con la dirección IP 172.43.3.94 Dándonos un resultado de 4 paquetes enviados y 4 paquetes recibidos lo que quiere decir que la prueba esta correcta.

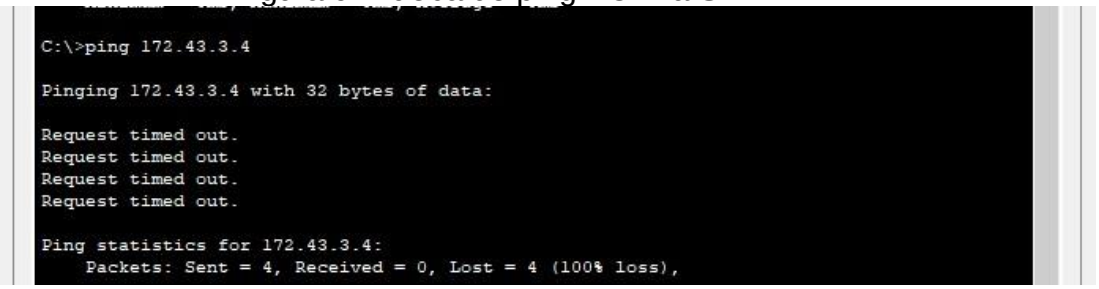
Figura 8 Prueba de ping PC-B a R1 G0/0/1



Fuente. Elaboración propia

Para esta prueba se utilizaron los dispositivos PC-B y el router R1 y este a su vez utilizando el puerto G0/0/1 con un resultado de 4 paquetes enviados, 4 paquetes recibidos y 0 paquetes perdidos lo que nos quiere decir que el ping y la configuración de los dispositivos son correctos.

Figura 9 Prueba de ping PC-B a S1 VLAN1

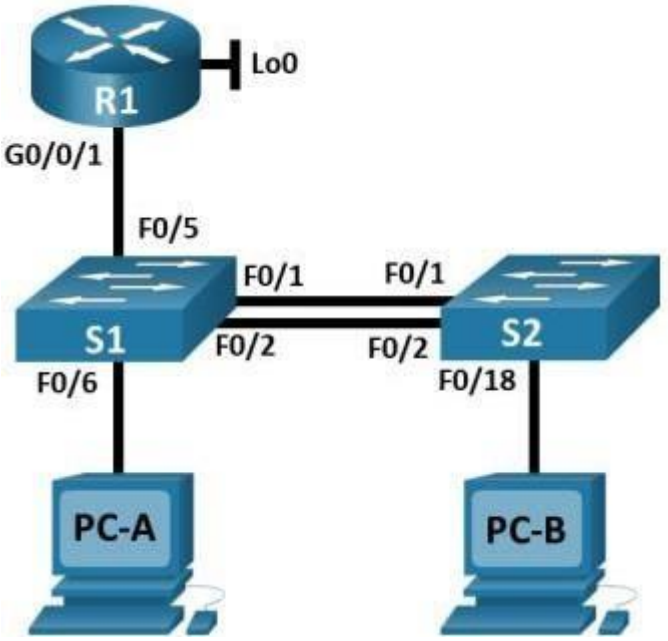


Fuente. Elaboración propia

En esta prueba se envían 4 paquetes y se reciben 0 paquetes y un total de 4 paquetes perdidos, se revisa configuración, pero no se encuentra ningún error ya que desde el PC-B hacia el puerto S1 VLAN1 con la dirección IP 172.43.3.4 la configuración esta correcta.

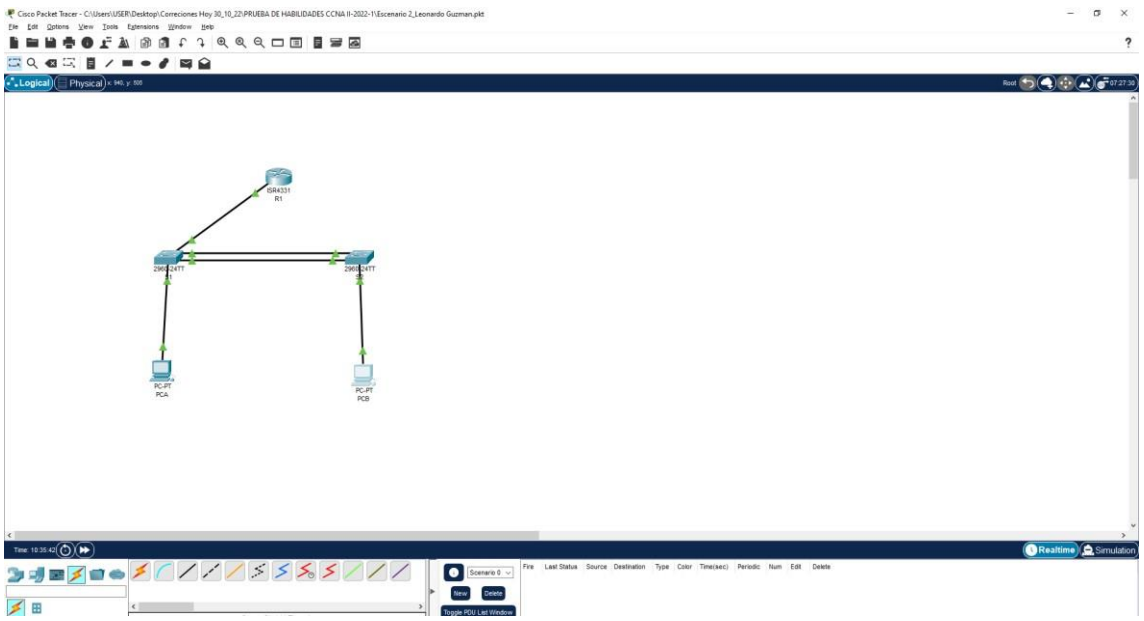
DESARROLLO ESCENARIO 2

Figura 10. Topología escenario 2



Fuente. Elaboración propia

Figura 11 Topología escenario 2 en Packet Tracer



Fuente. Elaboración propia

Topología

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.

Tabla 7 Tabla de la vlan

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

Autor. Prueba de habilidades CCNA

Tabla de asignación de direcciones

En este apartado según la guía donde estaba XY se debía remplazar por los últimos dos dígitos de mi número de identificación que son 43.

Tabla 8 Asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.20	10.43.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.30	10.43.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.40	10.43.8.97 /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	10.43.8.98 /29	10.43.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 40	10.43.8.99 /29	10.43.8.97
	2001:db8:acad:c: :99/64	No corresponde
	fe80: :99	No corresponde

PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminadaIPv4
	2001:db8:acad:a: :50/64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminadaIPv4
	2001:db8:acad:b: :50/64	fe80::1

Autor. Prueba de habilidades CCNA

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

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

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

Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos.

Después de recargar el switch, configure la plantilla SDM para que admitaIPv6 según sea necesario y vuelva a cargar el switch.

Empezamos con la inicialización y cargar nuevamente el router, esto es importante ya que el router puede tener configuración antigua que nos puede dar error a la hora de iniciar una nueva configuración.

Tabla 9 Inicializar y Recargar R1

Tarea	Especificación - Comando
Iniciamos el modo privilegiado.	Router>enable
Eliminamos la configuración de inicio.	Router#erase startup-config
Presionamos enter y empezara el proceso	Erasing the nvram filesystem willremove all configuration files! Continue? [confirm]
Eliminamos la configuración de la memoria antigua	Router#reload
Presionamos enter para confirmar la recarga	Proceed with reload? [confirm]

Fuente. Elaboración propia

Continuamos con la inicialización y la carga del switch 1 y switch 2, que al igual que el router se debe tener los switches libres de cualquier configuración para que a la hora de nosotros ingresar la nueva configuración no tengamos ningún tipo de error, además de lo anterior al switch se le debe configurar la plantilla SDM para que nos admitan IPV6.

Tabla 10 Inicializar y Recargar S1

Tarea	Especificación - Comando
Iniciamos el modo privilegiado.	Switch>enable
Determinamos si hay VLAN creadas	Switch#show flash *Determinamos si hay VLAN creadas* System flash directory: File Length Name/status 3 8662192 c3560-advipservicesk9-mz.122-37.SE1.bin 2 28282 sigdef-category.xml 1 227537 sigdef-default.xml [8918011 bytes used, 55098373 available, 64016384 total] 63488K bytes of processor board System flash (Read/Write) Como no encontramos ningún archivo vlan.dat continuamos con elproceso de borrar el archivo de configuración de la NVRAM

Eliminamos la configuración de la memoria antigua	Switch# erase startup-config
Le damos enter para confirmar la orden	Erasing the nvram filesystem willremove all configuration files! Continue? [confirm]
Volvemos a cargar el switwch Confirmamos la orden	Switch#reload Proceed with reload? [confirm]
Iniciamos nuevamente Entramos al modo de configuración *Se configura la plantilla SDM* *Salimos del modo de configuracion*	Switch>enable Switch#configure t Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#sdm prefer dual-ipv4-and-ipv6 default Changes to the running SDM preferences have been stored, butcannot take effect until the next reload. Use 'show sdm prefer' to see what SDM preference is currently active. [OK]

Fuente. Elaboración propia

Hacemos la misma configuración para el switch 2

Tabla 11 Inicializar y Recargar S2

Tarea	Especificación - Comando
Iniciamos el modo privilegiado.	Switch>enable

Determinamos si hay VLAN creadas	Switch#show flash *Determinamos si hay VLAN creadas* System flash directory: File Length Name/status 3 8662192 c3560-advipservicesk9-mz.122-37.SE1.bin 2 28282 sigdef-category.xml 1 227537 sigdef-default.xml [8918011 bytes used, 55098373 available, 64016384 total] 63488K bytes of processor board System flash (Read/Write) Como no encontramos ningún archivo vlan.dat continuamos con elproceso de borrar el archivo de configuración de la NVRAM
Eliminamos la configuración de la memoria antigua	Switch# erase startup-config
Le damos enter para confirmar la orden	Erasing the nvram filesystem willremove all configuration files! Continue? [confirm]
Volvemos a cargar el switwch Confirmamos la orden	Switch#reload Proceed with reload? [confirm]

Iniciamos nuevamente Entramos al modo de configuración	Switch>enable Switch#configure t Switch#configure terminal
Se configura la plantilla SDM *Salimos del modo de configuracion* *Recargamos el switch*	Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#sdm prefer dual-ipv4-and-ipv6 default Changes to the running SDM preferences have been stored, butcannot take effect until the next reload. Use 'show sdm prefer' to see what SDM preference is currently active.Switch(config)#end Switch# %SYS-5-CONFIG_I: Configuredfrom console by console Switch#reload System configuration has beenmodified. Save? [yes/no]:yes Building configuration... [OK]

Fuente. Elaboración propia

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Para el Router R1 debemos configurar, la búsqueda de DNS, le damos nombre al dispositivo, asígnanos el dominio necesario para la comunicación con todos los dispositivos que estén en red, establecemos usuarios y contraseñas, configuramos las interfaces y además de eso el loopback0.

Tabla 12 Configuración del Router R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router#enable Router#configure t Router#configure terminal Enter configuration commands, oneper line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#
Nombre del router	Router(config)#hostname R1 R1(config)#
Nombre de dominio	R1(config)#ip domain name ccna-sa.com R1(config)#
Contraseña cifrada para el modoEXEC privilegiado	R1(config)#enable secret class R1(config)#
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit R1(config)#
Establecer la longitud mínima para las contraseñas	R1(config)#security passwords min-length 5 R1(config)#
Crear un usuario administrativo en la base de datos local	R1(config)#username admin secret admin1pass R1(config)#
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 R1(config-line)#
Configurar VTY solo aceptando SSH	R1(config-line)#transport input ssh R1(config-line)#exit R1(config)#
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption R1(config)#

Configure un MOTD Banner	R1(config)#banner motd ' R1-ELIECER GUZMAN-INGENIERIA DE SISTEMAS ' R1(config)#
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing R1(config)# shutdown
Configurar interfaz G0/0/1 y sub interfaces Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 comofe80: :1 Establece la dirección IPv6. Activar la interfaz.	R1(config-subif)#exit
Configure el Loopback0 interface	R1(config)#interface Loopback0 R1(config-if)#description loopback0 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::1link-local R1(config-if)#no shutdown R1(config-if)#exit
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa general-keys modulus 1024 The name for the keys will be: R1.ccna-sa.com % The key modulus size is 1024 bits% Generating 1024 bit RSA keys,keys will be non-exportable...[OK] *Mar 1 0:22:54.70: %SSH-5-ENABLED: SSH 1.99 has been enabled R1(config)#

Fuente. Elaboración propia

Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Para la configuración de los switch S1 y S2 se deben seguir los pasos especificados en la tablas, que serían empezar desactivando la búsqueda de DNS, entremos a la consola y entramos a la configuración de terminal,

agregamos un nombre al switch S1 para el primero y S2 para el segundo, configuramos el nombre de switch que queremos mostrar, agregamos el dominio, creamos las contraseña privilegiada y le agregamos el comando secret, establecemos el dominio para que este tenga comunicación con los demás equipos conectados en la red, creamos la contraseña de acceso a la consola creamos la contraseña y el usuario administrativo de la base local, configuramos las líneas VTY, agregamos el banner que este caso nos solicita el nombre del switch, nombre del estudiante y carrera esto es lo que observara el usuario al entrar a modificar cualquier apartado de los switch, generamos una clave de cifrado de 1024 bits, configuramos la interfaz de administración establecemos la dirección IPV4 que será de capa 3 y establecemos también la dirección de IPV6, por ultimo configuramos el Gateway.

Tabla 13 Configuración S1

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch#configure t Switch#configure terminal Switch(config)#no ip domain-lookup Switch(config)#
Nombre del switch	Switch(config)#hostname S1 S1(config)#
Nombre de dominio	S1(config)#ip domain name ccna-sa.com S1(config)#
Contraseña cifrada para el modoEXEC privilegiado	S1(config)#enable secret class S1(config)#
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#LOGIN S1(config-line)#exit S1(config)#
Crear un usuario administrativo en la base de datos local	S1(config)#username admin secret admin1pass S1(config)#
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local S1(config-line)#
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh S1(config-line)#exit S1(config)#

Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption S1(config)#
Configurar un MOTD Banner	S1(config)#banner motd ' S1-ELIECER GUZMAN-INGENIERIA DE SISTEMAS ' S1(config)#
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa general-keys modulus 1024 The name for the keys will be: S1.ccna-sa.com % The key modulus size is 1024 bits % Generating 1024 bit RSA keys,keys will be non-exportable...[OK] *Mar 1 0:9:28.896: %SSH-5-ENABLED: SSH 1.99 has been enabled S1(config)#
Configurar la interfaz de administración (SVI)	S1(config)#interface vlan 4 S1(config-if)#ip address 10.43.8.98 255.255.255.248 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 S1(config-if)#no shutdown S1(config-if)#exit S1(config)#
Configuración del gateway predeterminado	S1(config)#ip default-gateway 10.43.8.97 S1(config)#

Fuente. Elaboración propia

Para la configuración es básicamente los pasos hechos en switch S1 ya que estos dos switches tienen la misma configuración, claro está que las direcciones cambian de uno al otro.

Tabla 14 Configuración del switch S2

Tarea	Especificación

Desactivar la búsqueda DNS.	Switch>enable Switch#configure terminal Switch(config)#ip domain-lookup Switch(config)#
Nombre del switch	Switch(config)#hostname S2 S2(config)#
Nombre de dominio	S2(config)#ip domain name ccna-sa.com S2(config)#
Contraseña cifrada para el modo EXEC privilegiado	S2(config)#enable secret class S2(config)#
Contraseña de acceso a la consola	S2(config)#line console 0 S2(config-line)#password cisco S2(config-line)#LOGIN S2(config-line)#exit S2(config)#
Crear un usuario administrativo en la base de datos local	S2(config)#username admin secret admin1pass S2(config)#
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 15 S2(config-line)#login local S2(config-line)#
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config-line)#transport input ssh S2(config-line)#exit S2(config)#
Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption S2(config)#
Configurar un MOTD Banner	S2(config)#banner motd ' S2-ELIECER GUZMAN-INGENIERIA DE SISTEMAS ' S2(config)#
Generar una clave de cifrado RSA	S2(config)#crypto key generate rsa general-keys modulus 1024 The name for the keys will be: S1.ccna-sa.com % The key modulus size is 1024 bits % Generating 1024 bit RSA keys,keys will be non-exportable...[OK] *Mar 1 0:9:28.896: %SSH-5- ENABLED: SSH 1.99 has been enabled S2(config)#

Configurar la interfaz de administración (SVI)	S2(config)#interface vlan 4 S2(config-if)#ip address 10.43.8.99 255.255.255.248 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 S2(config-if)#no shutdown S2(config-if)#exit S2(config)#
Configuración del gateway predeterminado	S2(config)#ip default-gateway 10.43.8.97 S2(config)#

Fuente. Elaboración propia

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

Paso 4: Configurar S1.

La configuración del S1 incluye las siguientes tareas:

En este apartado configuramos la infraestructura de red, creamos las VLAN con cada una de sus nombres, asignamos los troncos 802.1Q y estos utilizarán la VLAN 56, creamos el grupo delos puertos EtherChannel de Capa 2 bajo el protocolo LACP, agregamos el puerto de acceso al host parala VLAN 20 además de esto configuramos la seguridad en los puertos para que solo nos permita 4 direcciones MAC y protegemos las interfaces no utilizadas y las asignamos a la VLAN 50 le debemos asignar una descripción ya apagarlas.

Tabla 15 Configuración de la infraestructura de red S1

Tarea	Especificación

rear VLAN VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native	S1#configure terminal Enter configuration commands, oneper line. End with CNTL/Z. 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 S1(config)#
Crear troncos 802.1Q que utilicen la VLAN 56 nativa	S1(config)#interface range f0/1, f0/2, f0/5 S1(config-if-range)#switchport mode trunk S1(config-if-range)#encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 56 S1(config-if-range)#switchport trunk allowed vlan 20,30,40,50,56 S1(config-if)#exit

Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1(config)#interface range fa0/1,fa0/2 S1(config-if-range)#channel-protocol lacp S1(config-if-range)#channel-group 2 mode active S1(config-if-range)#Creating a port-channel interfacePort-channel 2
Configurar el puerto de acceso dehost para VLAN 20	S1(config)#interface f0/6 S1(config-if)#switchport modeaccess S1(config-if)#switchport access vlan20 S1(config-if)#no shutdown
Configurar la seguridad del puertoen los puertos de acceso	S1(config-if)#switchport port-security maximum 4 S1(config-if)#switchport port-security violation shutdown S1(config-if)#no shutdown
Proteja todas las interfaces no utilizadas	S1(config)#interface range f0/3-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchportaccess vlan 50 S1(config-if-range)#descriptionunused interfaces S1(config-if-range)#shutdown S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#description unused interfaces

	S1(config-if-range)#shutdown S1(config)#interface range g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#description unused interfaces S1(config-if-range)#shutdown

Fuente. Elaboración propia

Paso 5: Configure el S2

Entre las tareas de configuración de S2 se incluyen las siguientes:

Configurar switch 2 básicamente con la misma configuración del switch excepto que en la configuración del puerto de acceso al host será para laVLAN 30 por lo demás toda la configuración es la misma, claro está que cada switch tiene sus direcciones diferentes.

Tabla 16 Configuración de la infraestructura de red 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 S2(config-vlan)#name Native S2(config-vlan)#exit S2(config)#

Crear troncos 802.1Q que utilicen la VLAN 56 nativa	S2(config)#interface range fa0/1,fa0/2 S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 56 S2(config-if-range)#switchport trunk allowed vlan 20,30,40,50,56 S2(config-if-range)#exit S2(config)#
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S2(config)#interface range fa0/1,fa0/2 S2(config-if-range)#channel-protocol lacp S2(config-if-range)#channel-group 2 mode active S2(config-if-range)#Creating a port-channel interfacePort-channel 2
Configurar el puerto de acceso del host para la VLAN 30	S2(config)#interface f0/18 S2(config-if)#switchport modeaccess S2(config-if)#switchport access vlan30 S2(config-if)#no shutdown S2(config-if)#exit

Configure port-security en losaccess ports	S2(config-if)#switchport port-security maximum 4 S2(config-if)#switchport port-security violation shutdown
Asegure todas las interfaces no utilizadas.	S2(config)#interface range f0/3-17, f0/19-24, g0/1-2 S2(config-if-range)#switchport acces vlan 50 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport nonegotiate S2(config-if-range)#description SW2-of S2(config-if-range)#sh

Fuente. Elaboración propia

Parte 3: Configurar soporte de host Paso 6: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Esta configuración la realizamos solo en Router y empezaremos creando las rutas predeterminadas tanto para IPV4 como IPV6 y debemos tener en cuenta que todo el tráfico se debe enviar por el Loopback 0, continuamos con la creación del grupo DHCP para la VLAN 20 y a este le asignamos las ultimas 10 direcciones de la subred, creamos el dominio y especificamos al puerta deenlace, también configuramos el DHCP para la VLAN 30 básicamente la misma configuración echa en la VLAN 20 claro está que con las direcciones asignadas para cada uno.

Tabla 17 Configuración soporte de host en R1

Tarea	Especificación
Configure Default Routing	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 %Default route without gateway, ifnot a point-to-point interface, may impact performance R1(config)#ipv6 route ::/0 loopback 0 R1(config)#
Configurar IPv4 DHCP para VLAN20	R1(config)#ip dhcp excluded-address 10.47.8.1 10.47.8.52 R1(config)#ip dhcp pool vlan20-Docentes R1(dhcp-config)#network 10.43.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.43.8.1 R1(dhcp-config)#domain-nameunad-ccna-sa.net
Configurar DHCP IPv4 para VLAN30	R1(config)#ip dhcp excluded-address 10.43.8.65 10.19.8.8 R1(config)#ip dhcp pool vlan30-Estudiantes R1(dhcp-config)#network 10.43.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.43.8.65 R1(dhcp-config)#domain-nameunad-ccna-sb.net R1(dhcp-config)#exit

Fuente. Elaboración propia

Paso 7: Configurar los servidores

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

Empezamos la configuración de los equipos es decir el PC-A agregamos la descripción. La dirección física para esto utilizamos el comando ipconfig /all, configuramos la dirección en IPV4 la dejamos que asigne las ip de manera estativa, agregamos la mascar y el Gateway.

Tabla 18 Configuración de red PC-A

Configuración de red de PC-A	
Descripción	FastEthernet0 connection
Dirección física	FE80::240:BFF:FE6A:A353
Dirección IP	Ipv4 10.43.8.53 Ipv6 2001:DB8:ACAD:A::50
Máscara de subred	255.255.255.192
Gateway predeterminado	10.43.8.1
Gateway predeterminado IPv6	2001:db8:acad:a::1

Fuente. Elaboración propia

Para el PC-B dejamos que la IPV4 se asigne de manera estática y la IPV6 si la agregamos de manera manual.

Tabla 19 Configuración de red PC-B.

Configuración de red de PC-B	
Descripción	FastEthernet0 connection
Dirección física	FE80::2E0:F7FF:FEB8:1668
Dirección IP	Ipv4 10.43.8.66 Ipv6 2001:DB8:ACAD:B::50/64
Máscara de subred	255.255.255.224
Gateway predeterminado	10.43.8.65
Gateway predeterminado IPv6	2001:db8:acad:b::1

Fuente. Elaboración propia

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

Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 20 Pruebas de Ping

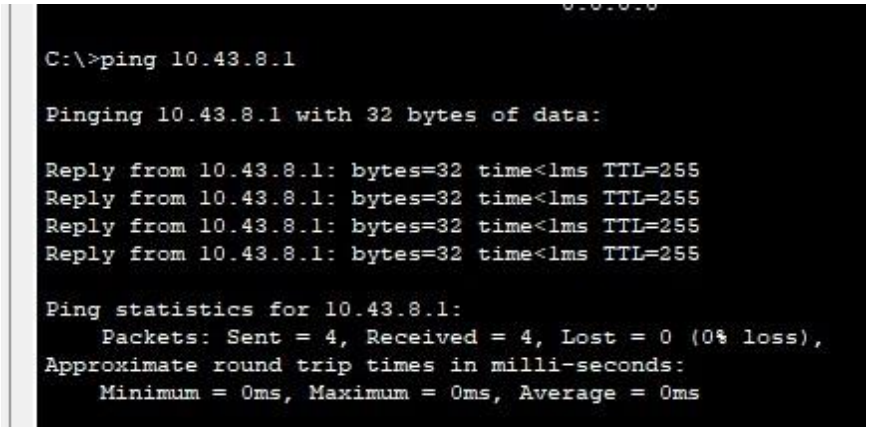
Desde	A		Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.20	IPv4	10.43.8.1 /26	CORRECTO
		IPv6	2001:DB8:ACAD:A::1/64	CORRECTO
	R1, G0/0/1.30	IPv4	10.43.8.65 /27	CORRECTO
		IPv6	2001:db8:acad:b::1/64	CORRECTO
	R1, G0/0/1.40	IPv4	10.43.8.97 /29	CORRECTO
		IPv6	2001:db8:acad:c::1/64	CORRECTO

	S1, VLAN 4	IPv4	10.43.8.98 /29	CORRECTO
	0	IPv6	2001:db8:acad:c::98/64	CORRECTO
	S2, VLAN 4	IPv4	10.43.8.99 /29	CORRECTO
	0	IPv6	2001:db8:acad:c::99/64	CORRECTO
	PC - B	IPv4	10.43.8.53	CORRECTO
		IPv6	2001:DB8:ACAD:A::50/64	CORRECTO
PC - B	R1, G0/0/1.20	IPv4	10.43.8.1 /26	CORRECTO
		IPv6	2001:db8:acad:a::1/64	CORRECTO
	R1, G0/0/1.30	IPv4	10.43.8.65 /27	CORRECTO
		IPv6	2001:db8:acad:b::1/64	CORRECTO
	R1, G0/0/1.40	IPv4	10.43.8.97 /29	CORRECTO
		IPv6	2001:db8:acad:c::1/64	CORRECTO
	S1, VLAN 4	IPv4	10.43.8.98 /29	CORRECTO
	0	IPv6	2001:db8:acad:c::98/64	CORRECTO
	S2, VLAN 4	IPv4	10.43.8.99 /29	CORRECTO
	0	IPv6	2001:db8:acad:c::99/64	CORRECTO

Fuente. Elaboración propia

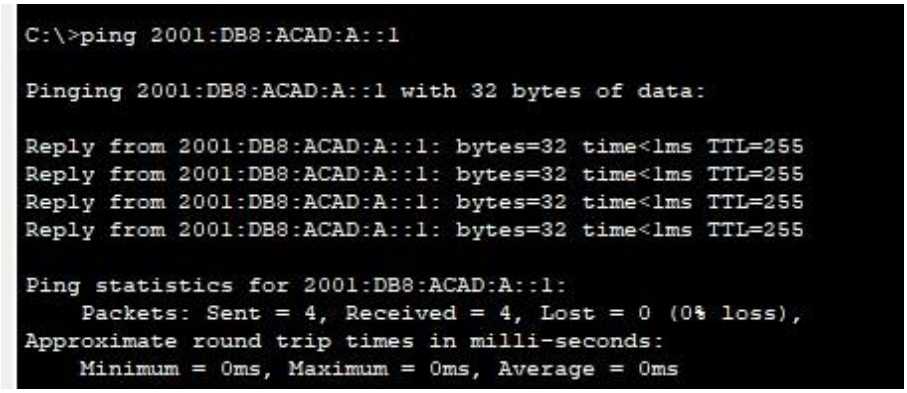
PRUEBAS DE PING ESCENARIO 2

Figura 12. Ping de PC-A a R1, G0/0/1.20 IPV4



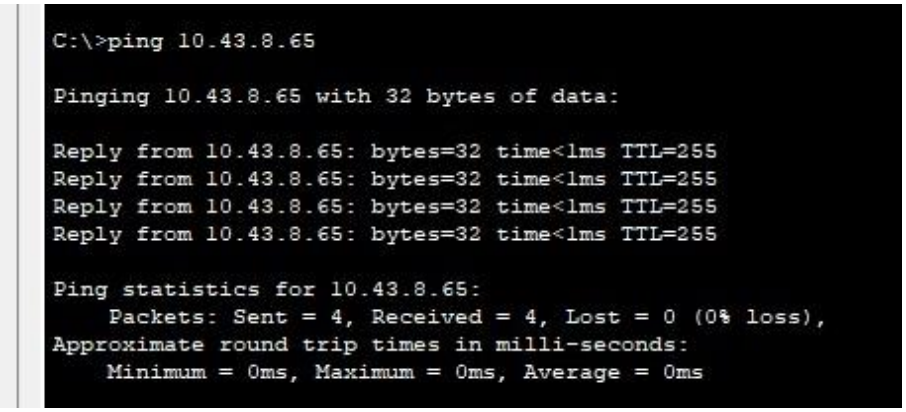
Fuente. Elaboración propia

Figura 13. Ping de PC-A a R1, G0/0/1.20 IPV6



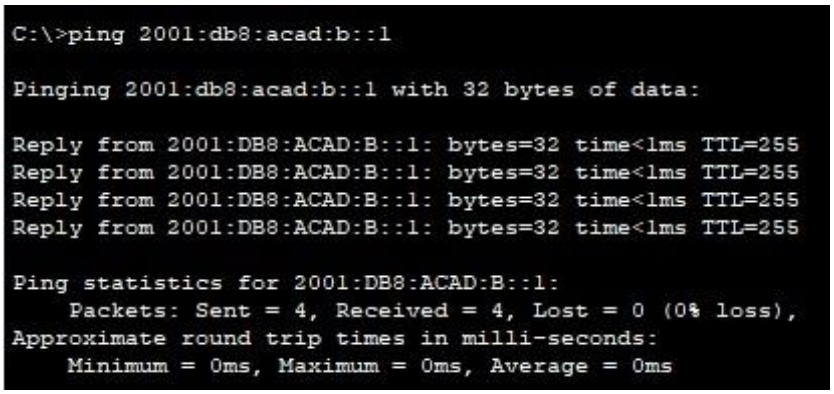
Fuente. Elaboración propia

Figura 14. Ping de PC-A a R1, G0/0/1.30 IPV4



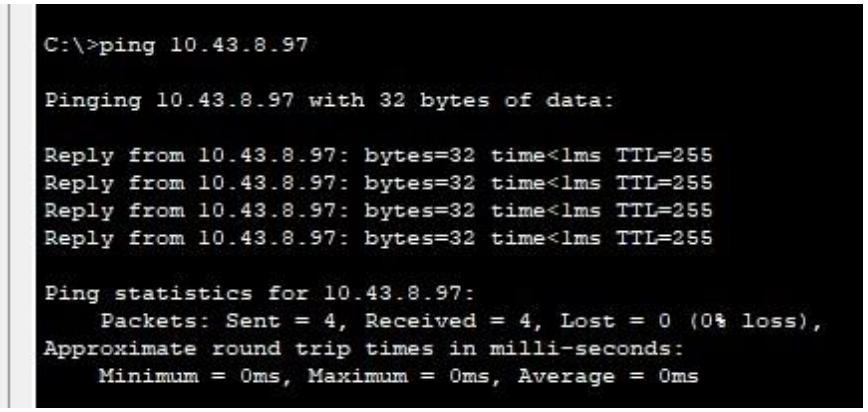
Fuente. Elaboración propia

Figura 15. Ping de PC-A a R1, G0/0/1.30 IPV6



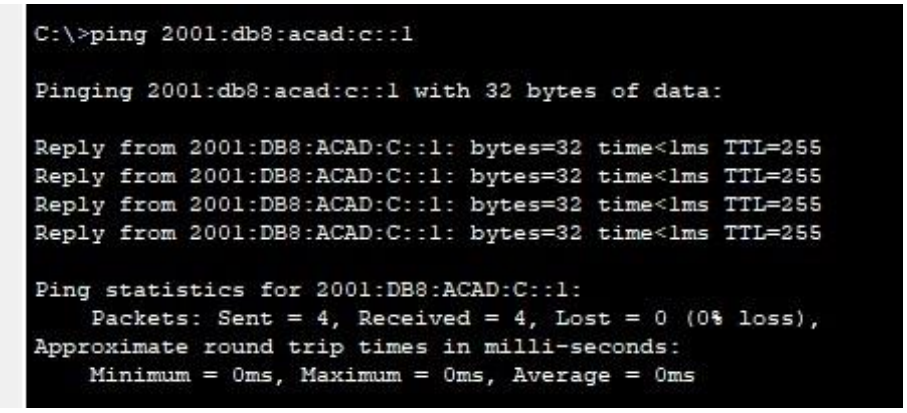
Fuente. Elaboración propia

Figura 16. Ping de PC-A a R1, R1, G0/0/1.40 IPV4



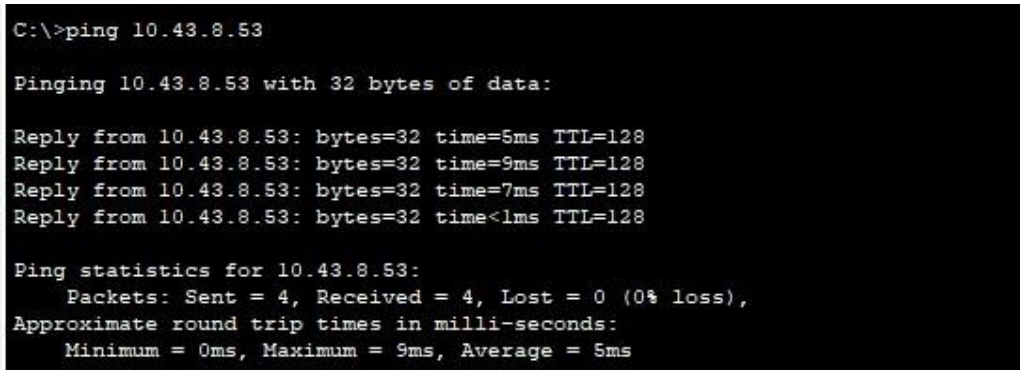
Fuente. Elaboración propia

Figura 17. Ping de PC-A a R1, R1, G0/0/1.40 IPV6



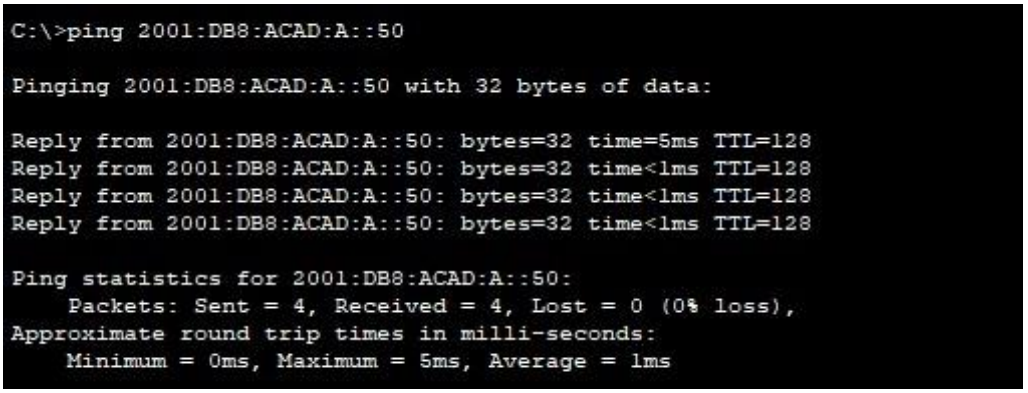
Fuente. Elaboración propia

Figura 18. Ping de PC-A a PC – B IPV4



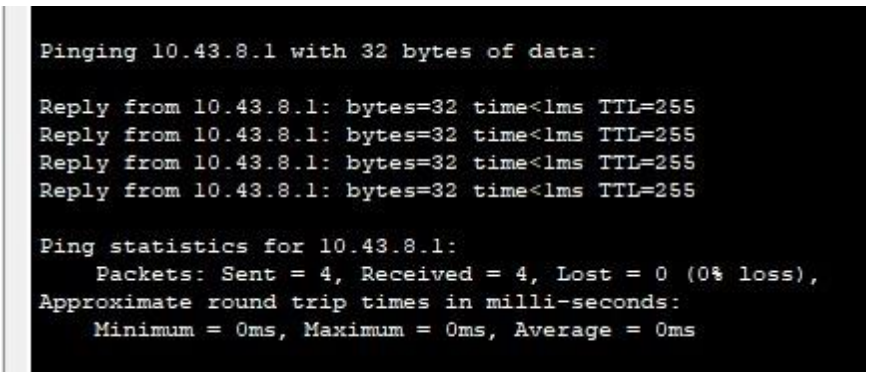
Fuente. Elaboración propia

Figura 19. Ping de PC-A a PC – B IPV6



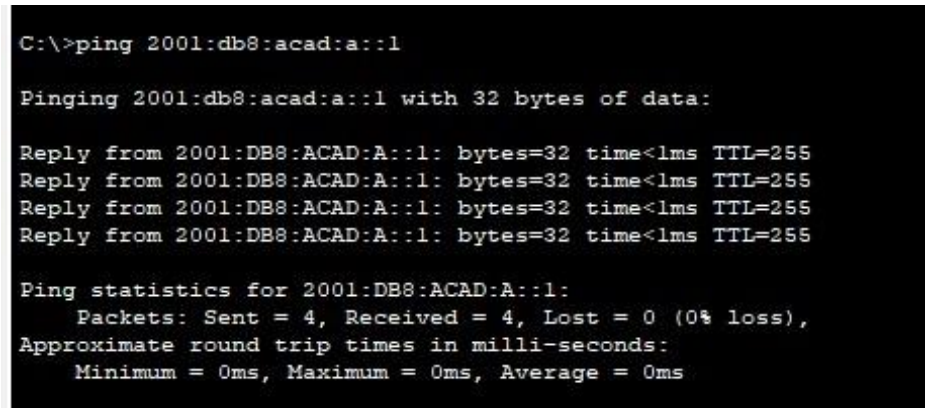
Fuente. Elaboración propia

Figura 20. Ping de PC – B a R1, G0/0/1.2 0 IPV4



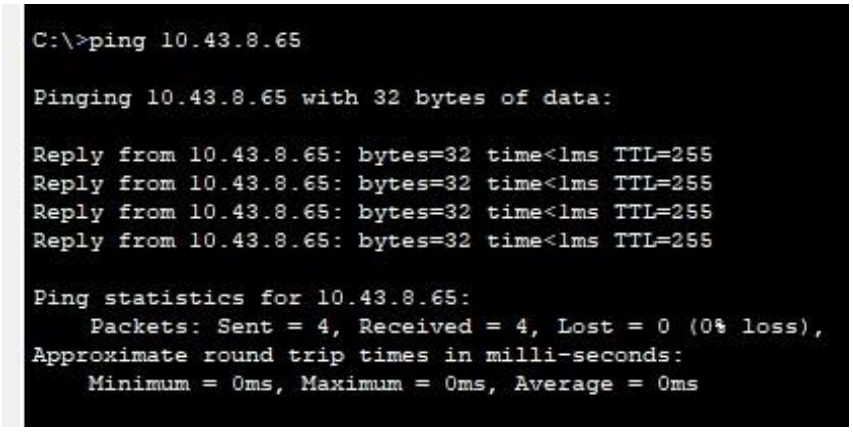
Fuente. Elaboración propia

Figura 21. Ping de PC – B a R1, G0/0/1.2 0 IPV6



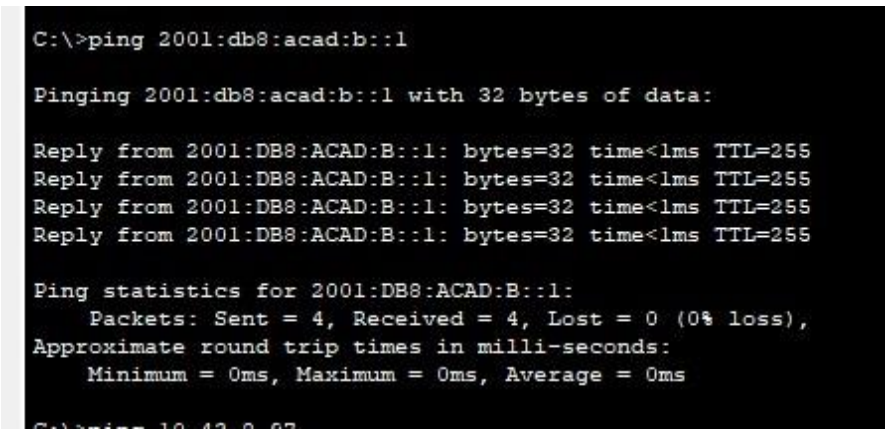
Fuente. Elaboración propia

Figura 22. Ping de PC – B a R1, R1, G0/0/1.3 0 IPV4



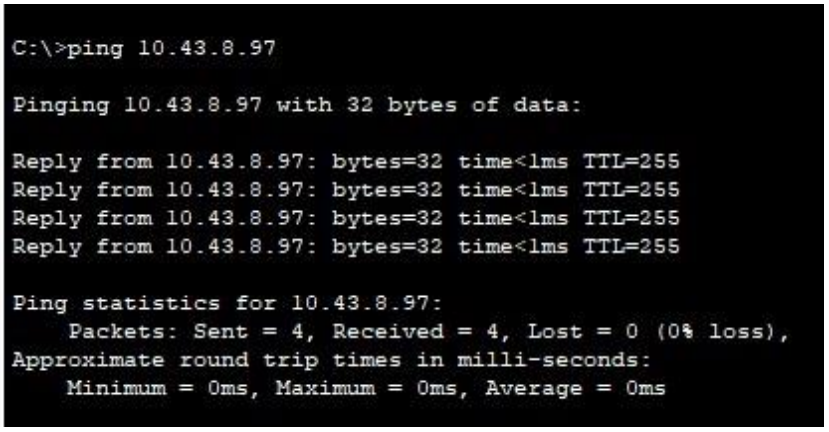
Fuente. Elaboración propia

Figura 23. Ping de PC – B a R1, R1, G0/0/1.3 0 IPV6



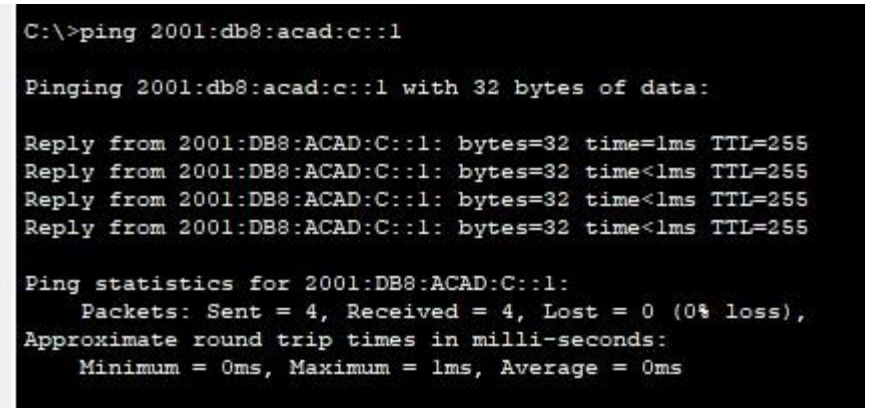
Fuente. Elaboración propia

Figura 24. Ping de PC – B a R1, R1, G0/0/1.4 0 IPV4



Fuente. Elaboración propia

Figura 25. Ping de PC – B a R1, R1, G0/0/1.4 0 IPV6



Fuente. Elaboración propia

CONCLUSIONES

Los dos escenarios realizados son la muestra de lo que se encuentra en una red ya sea en un hogar o una empresa, el desarrollo de la práctica permitió afianzar conceptos a cerca de: configuraciones, protocolos, dispositivos que utilizamos a la hora de configurar una red.

Dos escenarios con topologías diferentes, se pudo evidenciar en ambos escenarios problemas de conmutación y enrutamiento, vemos que el soporte de los modelos de arquitectura en la comunicación, nos ayudan a resolver los problemas que se obtiene a la hora de la configuración, del enrutamiento y de la conectividad.

Por medio de la realización de la práctica se pudo comprender el funcionamiento de una red, problemas que pueden ocurrir en el ámbito laboral cuando estos realizando enrutamiento de redes.

Con el uso de la herramienta tecnológica CISCO PACKET TRACER se realizó la simulación y configuración en tiempo real de los equipos, lo que ayudo a facilitar la comprensión del ejercicio y la apropiación del conocimiento.

BIBLIOGRAFÍA

Avast . (14 de Julio de 2022). ¿Qué es una dirección IP? Obtenido de https://www.avast.com/es-es/c-what-is-an-ip-address

ISCO, Netacad. Introducción a las redes – LAN y WAN (2022) {28 de octubre de 2022}. Disponible en https://contenthub.netacad.com/itn-dl/1.4.2

CISCO, Netacad. Introducción a las redes - Estructura básica de comandos de IOS (2022) {30 de octubre de 2022}. Disponible en https://contenthub.netacad.com/itn-dl/2.3.1

CISCO, Netacad. Introducción a las redes – Encriptación de las contraseñas (2022) {3 de noviembre de 2022}. Disponible en https://contenthub.netacad.com/itn- dl/2.4.4

CISCO, Netacad. Introducción a las redes – Configuración de interfaz virtual de switch (2022) {3 de noviembre de 2022}. Disponible en https://contenthub.netacad.com/itndl/2.7.4

CISCO, Netacad. Introducción a las redes – Protocolos (2022) {4 de noviembre de 2022}. Disponible en https://contenthub.netacad.com/itn-dl/3.2.1

CISCO, Netacad. Introducción a las redes – Dirección MAC de Ethernet (2022) {5 de noviembre de 2022}. Disponible en https://contenthub.netacad.com/itn-dl/7.2.2

CISCO, Netacad. Introducción a las redes – Paquete IPv4 (2022) {5 de noviembre de 2022}. Disponible en https://contenthub.netacad.com/itn-dl/8.2.1

CISCO, Netacad. Introducción a las redes – Paquete IPv6 (2022) {5 de noviembre de 2022}. Disponible en https://contenthub.netacad.com/itn-dl/8.3.1

CISCO, Netacad. Introducción a las redes – Mensajes ICMP (2022) {10 de noviembre de 2022}. Disponible en https://contenthub.netacad.com/itn- dl/13.1.1

Cisco. (s.f.). ¿Qué es un router? Obtenido de https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html

Microsoft. (29 de Septiembree de 2022). Protocolo de configuración dinámica de host (DHCP). Obtenido de https://learn.microsoft.com/es-es/windows-server/networking/technologies/dhcp/dhcp-top

Movistar. (2021). Switch de red: ¿cómo facilita las telecomunicaciones en tu hogar? Obtenido de https://www.movistar.es/blog/alarmas/alarma-conectada-vigilancia-constante/

ANEXOS

Enlace de descarga Escenario 1 y Escenario 2

https://1drv.ms/u/s!Am7QVmoKpsWKgsYkfgygkSuFgNJRhg?e=t1KHDM