

PRUEBAS DE HABILIDADES PRÁCTICA

ANDRES FERNANDO PAEZ

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

PRUEBAS DE HABILIDADES PRÁCTICA

ANDRES MAURICIO PEREZ

Diplomado De Opción De Grado Presentado Para Optar El
Título De Ingeniero De Sistemas

Director:
Paulita Flor

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

NOTA DE ACEPTACIÓN:

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Bogotá, 17 de diciembre de 2022

CONTENIDO

LISTA DE FIGURAS	5
LISTA DE TABLAS	7
GLOSARIO	8
RESUMEN	9
ABSTRACT	10
INTRODUCCION	11
DESARROLLO DE LAS TOPOLOGIAS DE RED	12
1. Topología de red/ Escenario 1	12
1.1. Paso 1. Construcción en la simulación de red.....	12
1.2. Paso 2. Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2	13
1.3. Paso 3. Configure aspectos básicos	14
1.4. Paso 4. Configure los host PC-A y PC-B.....	16
1.5. Parte 5: Verificar la conectividad en la red	17
2. Topología de red/ Escenario 2	19
2.1. Parte 1. Inicializar, recargar y configurar aspectos básicos de los dispositivos	21
2.2. Parte 2. Configuración básica de R1, S1 y S2	22
2.3. Parte 3. Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) en S1 y S2	27
2.4. Parte 4. Configurar soporte de host en R1	31
2.5. Parte 5. Configurar los equipos de red	32
2.6. Parte 6. Probar y verificar la conectividad de extremo a extremo.....	34
CONCLUSIONES	49
BIBLIOGRAFÍA	50
ANEXOS	51

LISTA DE FIGURAS

Figura 1. Primera topología de red a desarrollar.....	12
Figura 2. Simulación realizada para la primera topología de red	12
Figura 3. Direccionamiento IPv4 para el PC-A.....	16
Figura 4. Direccionamiento IPv4 para el PC-B.....	17
Figura 5. Verificación de conexión por ping desde PC-A a G0/0/0	17
Figura 6. Verificación de conexión por ping desde PC-A a G0/0/1	18
Figura 7. Verificación de conexión por ping desde PC-A a la IP de la VLAN.....	18
Figura 8. Verificación de conexión extremo-extremo por ping desde PC-A a PC-B.	19
Figura 9. Segunda topología de red a desarrollar.....	20
Figura 10. Direcciones de las subinterfaces en R1	26
Figura 11. Uso de show run para observar algunas configuraciones realizadas en S2	26
Figura 12. Visualización de VLAN's configuradas en S2.....	30
Figura 13. Visualización de VLAN's configuradas en S1	30
Figura 14. Segunda topología de red resultante	32
Figura 15. Información total de dirección para PC-A.....	33
Figura 16. Información total de dirección para PC-B.....	34
Figura 17. Prueba de ping desde PC-A a R1 G0/0/1.20 para IPv4	35
Figura 18. Prueba de ping desde PC-A a R1 G0/0/1.20 para IPv6	35
Figura 19. Prueba de ping desde PC-A a R1 G0/0/1.30 para IPv4	36
Figura 20. Prueba de ping desde PC-A a R1 G0/0/1.30 para IPv6	36
Figura 21. Prueba de ping desde PC-A a R1 G0/0/1.40 para IPv4	37
Figura 22. Prueba de ping desde PC-A a R1 G0/0/1.40 para IPv6	37
Figura 23. Prueba de ping desde PC-A a Loopback 0 para IPv4.....	38
Figura 24. Prueba de ping desde PC-A a Loopback 0 para IPv6.....	38
Figura 25. Prueba de ping desde PC-A a S1 VLAN 40.....	39
Figura 26. Prueba de ping desde PC-A a S2 VLAN 40.....	39
Figura 27. Prueba de ping desde PC-A a PC-B para IPv4.....	40
Figura 28. Prueba de ping desde PC-A a PC-B para IPv6.....	40

Figura 29. Prueba de ping desde PC-B a R1 G0/0/1.20 para IPv4	42
Figura 30. Prueba de ping desde PC-B a R1 G0/0/1.20 para IPv6	42
Figura 31. Prueba de ping desde PC-A a R1 G0/0/1.30 para IPv4	43
Figura 32. Prueba de ping desde PC-A a R1 G0/0/1.30 para IPv6	43
Figura 33. Prueba de ping desde PC-A a R1 G0/0/1.40 para IPv4	44
Figura 34. Prueba de ping desde PC-A a R1 G0/0/1.40 para IPv6	44
Figura 35. Prueba de ping desde PC-A a Loopback 0 para IPv4.....	45
Figura 36. Prueba de ping desde PC-A a Loopback 0 para IPv6.....	45
Figura 37. Prueba de ping desde PC-B a S1 VLAN 40.....	46
Figura 38. Prueba de ping desde PC-B a S2 VLAN 40.....	46
Figura 39. Prueba de ping desde PC-B a PC-A para IPv4.....	47
Figura 40. Prueba de ping desde PC-B a PC-A para IPv6.....	47

LISTA DE TABLAS

Tabla 1. Direccionamiento para la LAN1 y LAN2 en la primera topología.....	13
Tabla 2. Asignación de direcciones para las interfaces de los dispositivos.....	13
Tabla 3. Comandos empleados para la configuración en R1	14
Tabla 4. Comandos empleados para la configuración en S1	15
Tabla 5. Direccionamiento especificadas para las subinterfaces, VLAN's y hosts.	20
Tabla 6. Nombre y números de VLAN para el segundo escenario	21
Tabla 7. Comandos para borrado, recarga y habilitación de IPv6.....	21
Tabla 8. Comandos de configuración básica para R1 #1.....	22
Tabla 9. Comandos de configuración básica para R1 #2.....	23
Tabla 10. Comandos de configuración básica para S1	24
Tabla 11. Comandos de configuración básica para S2.....	25
Tabla 12. Comandos de configuración para la infraestructura de red en S1 #1.....	27
Tabla 13. Comandos de configuración para la infraestructura de red en S1 #2.....	27
Tabla 14. Comandos de configuración para la infraestructura de red en S2 #1.....	28
Tabla 15. Comandos de configuración para la infraestructura de red en S2 #2.....	29
Tabla 16. Comandos de configuración para el servicio DHCP desde R1.	31
Tabla 17. Información de direccionamiento en PC-A.	32
Tabla 18. Información de direccionamiento en PC-B.	33
Tabla 19. Resultados de pruebas de ping desde PC-A.	41
Tabla 20. Resultados de pruebas de ping desde PC-B.	41

GLOSARIO

PING: El ping es una herramienta o utilidad de diagnóstico para redes en la cual se puede llegar a comprobar la latencia de dicha red o comprobar el estado de la comunicación entre varios dispositivos de dicha red.

DHCP: El DHCP es un servicio o protocolo que permite configurar los parámetros de TCP/IP, como la dirección IP y la máscara de subred en los clientes o hosts dispuestos en una topología de red.

VLAN: Las VLAN son consideradas redes virtuales que trabajan sobre una red de área local y tiene como finalidad generar o crear grupos de manera independiente dentro de dicha red siendo útil para seccionar usuarios o dominios dentro una topología de red en cuestión.

CIFRADO: En redes, consiste en el proceso de codificación de información que ya bien pueden ser contraseñas, paquetes, ficheros o información dispuesta en una base de datos con el fin de garantizar mayor seguridad en dicho escenario.

TOPOLOGIA: Una topología en la temática de redes hace alusión a la disposición de varios equipos o dispositivos en un mapa físico de red los cuales se encuentran interconectados y que realizan tareas de enrutamiento y/o conmutación, así como la comunicación entre los mismos.

RESUMEN

En el presente documento se expone la solución al trabajo “Evaluación – Prueba de habilidades práctica CCNA” mediante el programa de simulación de redes Packet Tracer, con este, se lleva a cabo la solución de dos escenarios de redes los cuales disponen de dispositivos de comunicación, transmisión y recepción de paquetes o información en una red como routers, switches y hosts, a partir de estos, en ambos escenarios se realizan configuraciones básicas sobre estos como asignación de usuario y contraseña, identificación por nombre y uso de servicios de seguridad, de igual manera, se realiza el calculo de direccionamiento con una IP especifica y a partir de esto se realiza la relación de dichas direcciones con las interfaces o puertos de cada dispositivo, relación con las VLAN's o redes virtuales configuradas y los distintos protocolos empleados en este caso como DHCP, LAAC, 802.11 entre otros, a partir del uso de protocolos dispuestos por CISCO para la edición de redes, se realizan estas configuraciones y se verifican mediante pruebas de ping respectivas.

Palabras clave: CISCO, COMUNICACIÓN, DHCP, DIRECCIONAMIENTO, LAAC, VLAN

ABSTRACT

This document presents the solution to the work "Evaluation - CCNA practical skills test" through the Packet Tracer network simulation program, with this, the solution of two network scenarios is carried out, which have communication devices , transmission and reception of packets or information in a network such as routers, switches and hosts, from these, in both scenarios basic configurations are made on these such as user and password assignment, identification by name and use of security services, of In the same way, the addressing calculation is made with a specific IP and from this the relationship of said addresses with the interfaces or ports of each device is made, relationship with the VLANs or virtual networks configured and the different protocols used in this case as DHCP, LAAC, 802.11 among others, from the use of protocols provided by CISCO for network editing, these c configurations and are verified by respective ping tests.

Keywords: CISCO, COMMUNICATION, DHCP, ADDRESSING, LAAC, VLAN

INTRODUCCION

El estudio de las redes y las comunicaciones al día de hoy es una temática que es ampliamente abordada, por ello es pertinente, realizar investigaciones, consulta y estudios para llevar a cabo un continuo aprendizaje y que a partir del diplomado de profundización en Cisco CCNA se puede llevar a cabo de manera eficiente y sencilla, durante el transcurso del diplomado se logra adquirir los conocimientos mas esenciales y básicos pero no por ello menos importantes en cuanto a la comunicación y funcionamiento básico de los dispositivos en una red, como estos interactúan y bajo que estándares están regidos como el caso del modelo OSI.

El desarrollo de este trabajo precisamente hace parte de las actividades de carácter evaluativo del curso y permite como tal, listar y demostrar los conocimientos adquiridos en el transcurso del curso, realizando a partir de un fichero o interfaz en blanco de Packet Tracer, la búsqueda, asignación y configuración de los dispositivos necesarios empleando exclusivamente los conocimientos adquiridos y llegar como tal a la finalidad de garantizar la conexión a partir de IPv4 e IPv6.

Además, no solo la actividad tiene como finalidad, evaluar dichos conocimientos sobre comprensión y solución de errores en networking, a partir de la solución de estas topologías de red se puede llevar a cabo el planteamiento y observación de implementar mejoras en dichas redes usando protocolos mas actuales o investigar sobre nuevas temáticas que permiten comprender de mejor manera redes de mayor nivel, más extensas y más complejas.

DESARROLLO DE LAS TOPOLOGIAS DE RED

1. Topología de red/ Escenario 1

1.1. Paso 1. Construcción en la simulación de red.

Para la primera topología del trabajo, se presenta la siguiente disposición de dispositivos de red.

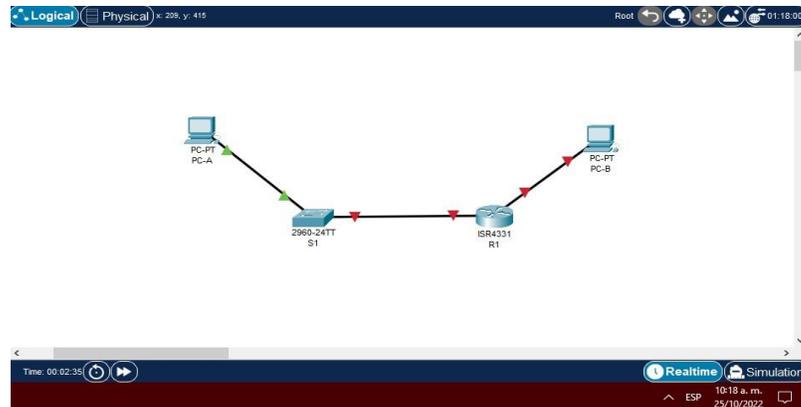
Figura 1. Primera topología de red a desarrollar.



Fuente: Prueba de habilidades.

Respecto al análisis de la figura anterior, se identifica que es necesario el uso de un switch 2960-TT, un router ISR4331 y dos PC host's, luego de asignarlos en Packet Tracer se conectan mediante cobre directo y se obtiene la siguiente simulación.

Figura 2. Simulación realizada para la primera topología de red.



Fuente: Autor.

1.2. Paso 2. Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2

Como segundo paso, se realiza el cálculo de direccionamiento para cada dispositivo de las LAN's respectivas, teniendo en cuenta el numero "42" el cual es el resultado de los dos últimos dígitos del documento, con ello claro la dirección IP será:

- 172.XY.3.0 = 172.42.3.0.

El documento guía menciona que para la LAN1 y LAN2 se requieren 80 host divididos en 60 para la primera LAN y 20 para la segunda LAN, con esto claro, se sabe que el ultimo octeto puede almacenar hasta 254 hosts, por ello el direccionamiento resultante se observa en la siguiente tabla.

Tabla 1. Direccionamiento para la LAN1 y LAN2 en la primera topología.

Nombre	LAN1	LAN2
Dirección de red	172.42.3.0	172.42.3.64
Mascara de red	255.255.255.192	255.255.255.224
Prefijo de red	26	27
Host	64	32
IP host disponibles	172.42.3.1-172.42.3.62	172.42.3.65-172.42.3.94
Gateway	172.42.3.0	172.42.3.64
Broadcast	172.42.3.63	172.42.3.95

Fuente: Autor.

Con el conteo de los hosts totales en ambas LAN's y la segmentación de la dirección IP a desarrollar se establecen las direcciones de las interfaces como lo requiere la guía.

Tabla 2. Asignación de direcciones para las interfaces de los dispositivos.

Nombre	Dirección
Requerimiento hosts LAN1	60
Requerimiento hosts LAN2	20
R1 G0/0/1	172.42.3.62/26
R1 G0/0/0	172.42.3.94/27
PC-A	172.42.3.11/26
PC-B	172.42.3.75/27

Fuente: Autor.

1.3. Paso 3. Configure aspectos básicos

Las configuraciones del router y del switch en la topología deben cumplir con las siguientes características o parámetros:

- Desactivar la búsqueda DNS.
- Nombre del router: R1
- Nombre de dominio.
- Contraseña cifrada para el modo EXEC privilegiado: ciscoenpass
- Contraseña de acceso a la consola: ciscoconpass
- Establecer la longitud mínima para las contraseñas: 10 caracteres
- Crear un usuario administrativo en la base de datos local: admin; admin1pass
- Configurar el inicio de sesión en las líneas VTY para que use la base de datos local.
- Cifrar las contraseñas de texto no cifradas
- Configure un banner MOTD
- Configuración de interfaz G0/0/0
- Configuración de interfaz G0/0/1
- Generar una clave de cifrado RSA.

Los comandos empleados para dichas tareas se observan en la tabla 3 a continuación:

Tabla 3. Comandos empleados para la configuración en R1.

Comandos	Función
conf terminal	Entrar a la terminal
hostname R1	Asignacion de nombre
int g0/0/0	Entrar a la interfaz especificada
ip address 172.42.3.94	Asignar dirección especificada
255.255.255.224	.
no shutdown	Habilitar la interfaz
exit	
int g0/0/1	Entrar a la interfaz especificada
ip address 172.42.3.62	Asignar dirección especificada
255.255.255.192	.
no shutdown	Habilitar la interfaz
exit	
no ip domain-lookup	
security passwords min-length 10	Asignacion de longitud de contraseña
username admin password admin1pass	Asignacion de nombre y contraseña

line console 0 login local exit	Acceso a la primera línea de consola Autenticación local
line vty 0 4 login local exit	Acceso a las líneas virtuales 0 4
enable secret ciscoenpass	Asignacion contraseña cifrada
line console 0 password ciscoconpass exit	Asignacion de contraseña a consola
ip domain name ccna-sa.com	Asignacion de nombre de dominio
crypto key generate rsa	Uso del servicio de cifrado
banner motd & Ingenieria de sistemas Andres Fernando Paez Router R1 &	Creación del mensaje diario
ip ssh version 2	Asignacion de versión SSH
line vty 0 4 transport input ssh login local exit exit	Asignacion de solo conexión SSH
copy running-config startup-config	Guardado de configuración en NVRAM

Fuente: Autor.

De igual manera, los comandos empleados para las configuraciones del switch se pueden detallar en la tabla 4 a continuación.

Tabla 4. Comandos empleados para la configuración en S1.

Comandos	Funciones
conf terminal	Entrar a la terminal
hostname S1	Asignacion de nombre
no ip domain-lookup	Asignacion de nombre y contraseña
username admin password admin1pass	
line console 0	Acceso a la primera línea de consola
login local	Autenticación local
exit	
line vty 0 4	Acceso a las líneas virtuales 0 4
login local	
exit	
enable secret ciscoenpass	Asignacion contraseña cifrada
line console 0 password ciscoconpass	Asignacion de contraseña a consola

<pre> exit ip domain name ccna-sa.com banner motd % Ingenieria de sistemas Andres Fernando Paez Switch S1 % ip ssh version 2 crypto key generate rsa line vty 0 4 transport input ssh login local exit int vlan 1 ip address 172.42.3.5 255.255.255.192 no shutdown exit ip default-gateway 172.42.3.0 exit copy running-config startup-config </pre>	<p>Asignacion de nombre de dominio Creación del mensaje diario</p> <p>Asignacion de versión SSH Uso del servicio de cifrado</p> <p>Asignacion de solo conexión SSH</p> <p>Entrar a la interfaz especificada Asignacion de dirección especificada</p> <p>Asignacion de gateway</p> <p>Guardado de configuración en NVRAM</p>
---	---

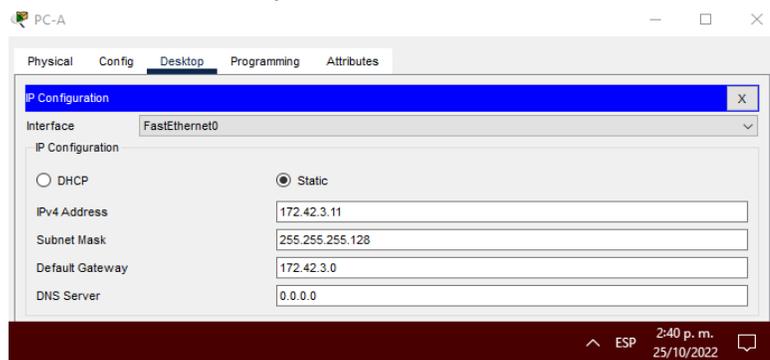
Fuente: Autor.

1.4. Paso 4. Configure los host PC-A y PC-B.

Para el cuarto paso, se accede a los hosts desde su interfaz gráfica en la opción de direccionamiento se procede a configurar los siguientes parámetros:

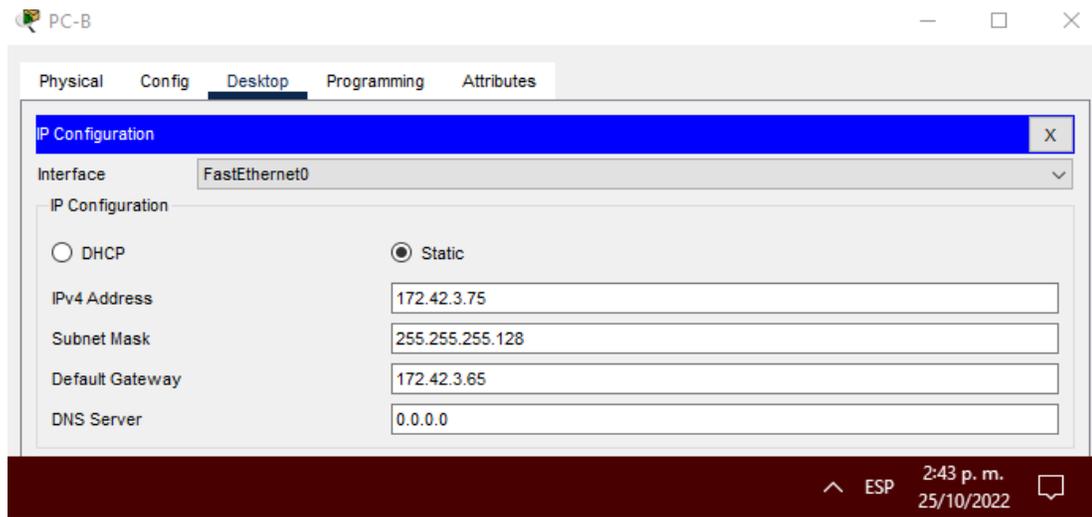
- Dirección física.
- Dirección IP.
- Mascara de red.
- Gateway predeterminado

Figura 3. Direccionamiento IPv4 para el PC-A.



Fuente: Autor.

Figura 4. Direccionamiento IPv4 para el PC-B.



Fuente: Autor.

1.5. Parte 5: Verificar la conectividad en la red.

Para verificar que el direccionamiento fue correcto se accede al command prompt de ambos hosts y se analiza una a una cada de las direcciones asignadas.

Figura 5. Verificación de conexión por ping desde PC-A a G0/0/0.

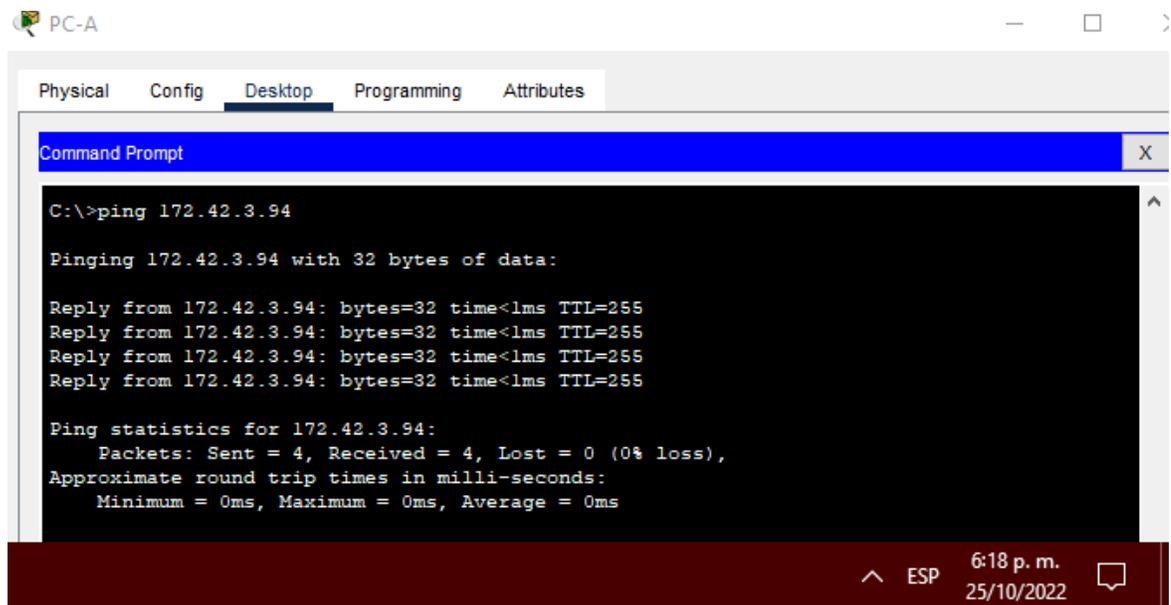
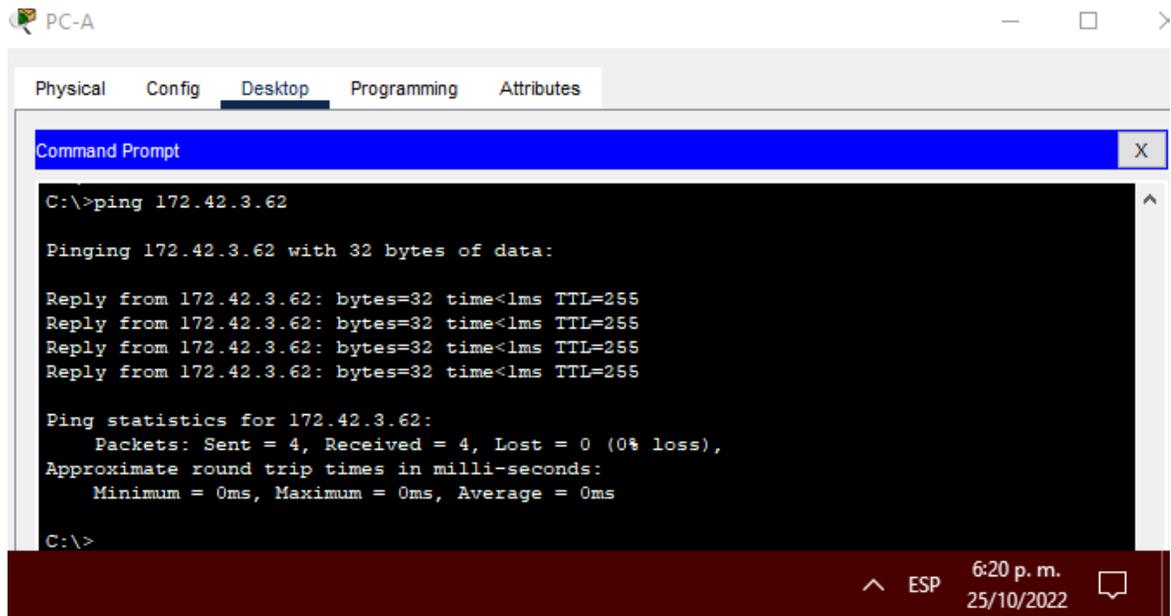
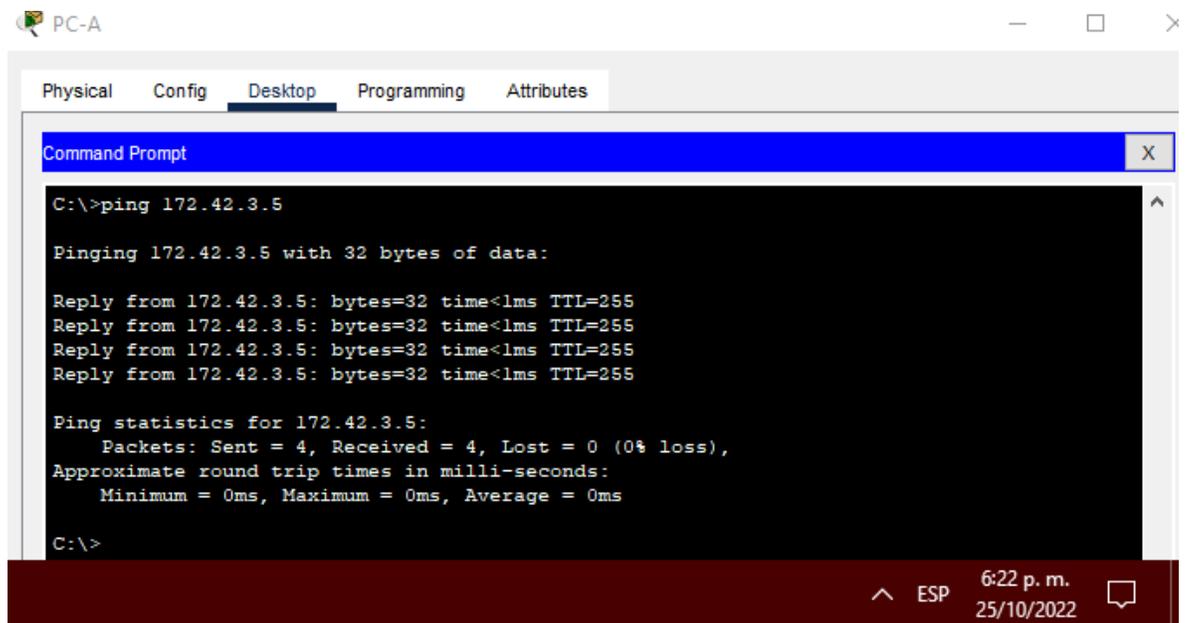


Figura 6. Verificación de conexión por ping desde PC-A a G0/0/1.



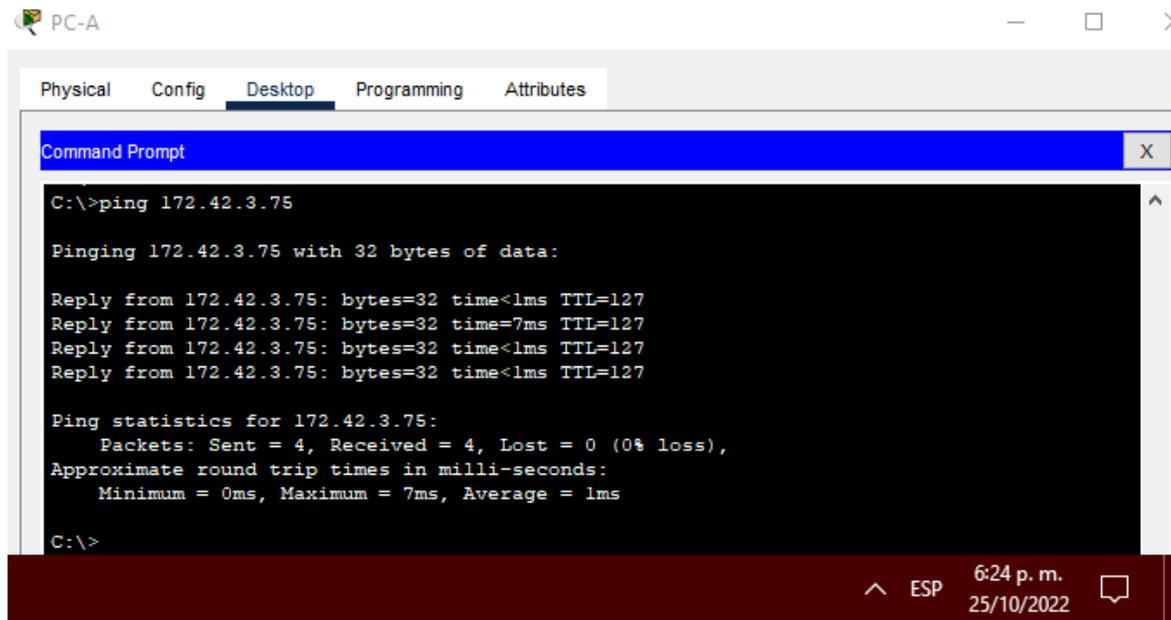
Fuente: Autor.

Figura 7. Verificación de conexión por ping desde PC-A a la IP de la VLAN.



Fuente: Autor.

Figura 8. Verificación de conexión extremo-extremo por ping desde PC-A a PC-B.



Fuente: Autor.

Como se detalla, los pings fueron satisfactorios lo que indica que el direccionamiento y la configuración básica en cada uno de los dispositivos fue correcta.

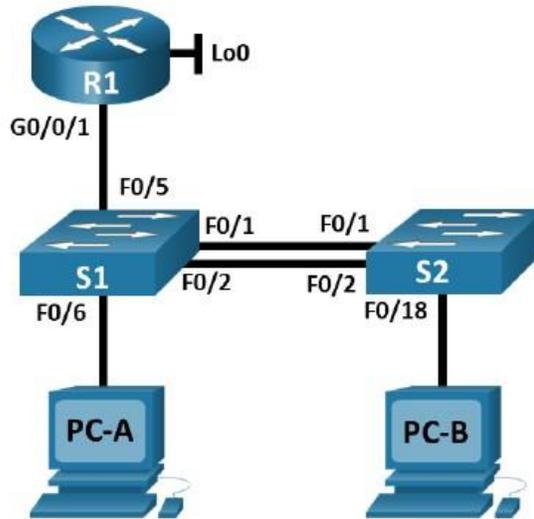
2. Topología de red/ Escenario 2

Para la segunda topología de red se configurarán los dispositivos de una red pequeña para que admitan tanto la conectividad IPv4 como IPv6, así mismo se debe garantizar administración de forma segura en el router y el switch, así mismo, se configura el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Para la segunda topología del trabajo, se presenta la siguiente disposición de dispositivos de red.

Figura 9. Segunda topología de red a desarrollar.

Topología



Fuente: Prueba de habilidades.

La guía de trabajo expone las siguientes tablas con información para direccionamiento IPv4 e IPv6.

Tabla 5. Direccionamiento especificadas para las subinterfaces, VLAN's y hosts.

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.20	10.42.8.1 /26 2001:db8:acad:a: :1 /64	--
R1 G0/0/1.30	10.42.8.65 /27 2001:db8:acad:b: :1 /64	--
R1 G0/0/1.40	10.42.8.97 /29 2001:db8:acad:c: :1 /64	--
R1 G0/0/1.60	--	--
R1 Loopback0	209.165.201.1 /27 2001:db8:acad:209: :1 /64	--

S1 VLAN 4	10.42.8.98 /29 2001:db8:acad:c: :98 /64 fe80: :98	10.19.8.97
S2 VLAN 4	10.42.8.99 /29 2001:db8:acad:c: :99 /64 fe80: :99	10.19.8.97
PC-A NIC	Dirección DHCP para IPv4 2001:db8:acad:a: :50 /64	DHCP para puerta de enlace predeterminada IPv4 e80::1
PC-B NIC	DHCP para dirección IPv4 2001:db8:acad:b: :50 /64	DHCP para puerta de enlace predeterminada IPv4 fe80::1

Fuente: Autor.

Tabla 6. Nombre y números de VLAN para el segundo escenario.

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

Fuente: Autor.

2.1. Parte 1. Inicializar, recargar y configurar aspectos básicos de los dispositivos

Para esta primera parte se realiza un borrado de las configuraciones de VLAN del router y de los switches, seguido se realiza la recarga de los dispositivos, además se asegura de cargar la plantilla de tipo SDM para que los switches puedan trabajar con el protocolo IPv6.

Tabla 7. Comandos para borrado, recarga y habilitación de IPv6.

Comandos	Funcion
erase startup-config	Borrar la configuración

reload	Recargar el dispositivo
delete vlan.dad	Borrar las vlans
reload	Recargar el dispositivo
sdm prefer dual-ipv4-and-ipv6 default	Habilitar IPv6
reload	Recargar el dispositivo

Fuente: Autor.

2.2. Parte 2. Configuración básica de R1, S1 y S2.

Para esta segunda parte, las configuraciones básicas de R1, S1 y S2 se listan en tablas dispuestas en el documento guía, en este caso se presentan dichas tablas con los comandos empleados en la parte derecha, así mismo, se presenta el registro visual de las configuraciones realizadas mediante el uso de comandos tipo show

Tabla 8. Comandos de configuración básica para R1 #1.

Tarea	Comandos empleados
Desactivar la búsqueda DNS	enable conf ter no ip domain lookup
Nombre del router	hostname R1
Nombre de dominio	ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC	enable password class enable secret class
Contraseña de acceso a la consola	line console 0 password cisco login
Longitud mínima para las contraseñas	security passwords min-length 5
Usuario administrativo en base de datos local	username admin secret admin1pass
Configuración inicio sesión en líneas VTY	line vty 0 15 login local
Configuración líneas VTY para solo SSH	transport input ssh
Cifrar contraseñas de texto no cifrado	service password-encryption
Configure un banner	banner motd & Ingenieria de Sistemas R1 Andres Fernando Paez &

Habilitar routing IPv6	ipv6 unicast-routing
------------------------	----------------------

Fuente: Autor.

Tabla 9. Comandos de configuración básica para R1 #2.

Tarea	Comandos empleados
Configuración interfaz g0/0/1	<pre> int g0/0/1.20 encapsulation dot1q 20 description Docentes ip address 10.42.8.1 255.255.255.192 ipv6 address 2001:db8:acad:a::1/64 ipv6 address fe80::1 link-local int g0/0/1.30 description Estudiantes ip address 10.42.8.65 255.255.255.224 encapsulation dot1q 30 ip address 10.42.8.65 255.255.255.224 ipv6 address 2001:db8:acad:b::1/64 ipv6 address fe80::1 link-local int g0/0/1.40 encapsulation dot1q 40 description Invitados ip address 10.42.8.97 255.255.255.248 ipv6 address 2001:db8:acad:c::1/64 ipv6 address fe80::1 link-local int g0/0/1.60 encapsulation dot1q 60 description Native int g0/0/1 no shutdown </pre>
Configuración Loopback0 interface	<pre> int loopback 0 ip address 209.165.201.1 255.255.255.224 ipv6 address 2001:db8:acad:209::1/64 ipv6 address fe80::1 link-local description Internet </pre>
Generar clave de cifrado RSA	<pre> exit crypto key generate rsa do wr </pre>

Fuente: Autor.

Para los switches S1 y S2 se ingresaron los siguientes comandos para las tareas listadas.

Tabla 10. Comandos de configuración básica para S1.

Tarea	Especificación
Desactivar la búsqueda DNS	enable conf ter no ip domain lookup
Nombre del switch	hostname S1
Nombre de dominio	ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC	enable secret class
Contraseña de acceso a la consola	line console 0 password cisco login
Usuario administrativo en base de datos local	exit username admin secret admin1pass
Configuración inicio sesión en líneas VTY	line vty 0 15 login local
Configuración líneas VTY para solo SSH	transport input ssh exit
Cifrar contraseñas de texto no cifrado	service password-encryption
Configure un banner	banner motd & Ingenieria de Sistemas S1 Andres Fernando Paez &
Generar clave de cifrado	crypto key generate rsa
Configuración interfaz SVI	int vlan 40 ip address 10.42.8.98 255.255.255.248 ipv6 address 2001:db8:acad:c::98/64 ipv6 address fe80::98 link-local description Interfaz Invitados no shutdown
Configuración gateway predeterminado	exit ip default-gateway 10.42.8.97 exit do wr

Fuente: Autor.

Tabla 11. Comandos de configuración básica para S2.

Tarea	Especificación
Desactivar la búsqueda DNS	enable conf ter no ip domain lookup
Nombre del switch	hostname S2
Nombre de dominio	ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC	enable secret class
Contraseña de acceso a la consola	line console 0 password cisco login
Usuario administrativo en base de datos local	exit username admin secret admin1pass
Configuración inicio sesión en líneas VTY	line vty 0 15 login local
Configuración líneas VTY para solo SSH	transport input ssh exit
Cifrar contraseñas de texto no cifrado	service password-encryption
Configure un banner	banner motd & Ingenieria de Sistemas S2 Andres Fernando Paez &
Generar clave de cifrado	crypto key generate rsa
Configuración interfaz SVI	int vlan 40 ip address 10.42.8.99 255.255.255.248 ipv6 address 2001:db8:acad:c::99/64 ipv6 address fe80::99 link-local description Interfaz Invitados no shutdown
Configuración gateway predeterminado	exit ip default-gateway 10.42.8.97 do wr

Fuente: Autor.

2.3. Parte 3. Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) en S1 y S2.

Para esta tercera parte, se presentan las configuraciones en S1 y S2 con base a las tablas dispuestas en el documento guía, en este caso se presentan dichas tablas con los comandos empleados en la parte derecha, así mismo, se presenta el registro visual de las configuraciones realizadas mediante el uso de comandos tipo show.

Tabla 12. Comandos de configuración para la infraestructura de red en S1 #1.

Tarea	Especificación
Crear VLAN	<pre> conf ter vlan 20 name Docentes vlan 30 name Estudiantes vlan 40 name Invitados vlan 50 name Usuarios vlan 60 name Native exit </pre>
Crear troncales 802.1Q que utilicen la VLAN 60 nativa	<pre> int f0/5 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 60 int range f0/1-2 channel-group 1 mode active int port-channel 1 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 60 </pre>

Fuente: Autor.

Tabla 13. Comandos de configuración para la infraestructura de red en S1 #2

Tarea	Especificación
Crear un grupo de puertos	<pre> int range f0/1-2 </pre>

EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	switchport trunk allowed vlan 20,30,40,50,60
Configurar el puerto de acceso de host para VLAN 20	inter f0/6 switchport mode access switchport access vlan 20
Configurar la seguridad del puerto en los puertos de acceso	switchport port-security switchport port-security maximum 4
Proteja todas las interfaces no utilizadas	int range f0/3-4 switchport mode access switchport access vlan 50 description Sin Uso shutdown int range f0/7-24 switchport mode access switchport access vlan 50 description Sin Uso shutdown int range g0/1-2 switchport mode access switchport access vlan 50 description Sin Uso shutdown

Fuente: Autor.

Tabla 14. Comandos de configuración para la infraestructura de red en S2 #1.

Tarea	Especificación
Crear VLAN	conf ter vlan 20 name Docentes vlan 30 name Estudiantes vlan 40 name Invitados vlan 50 name Usuarios vlan 60 name Native

Fuente: Autor.

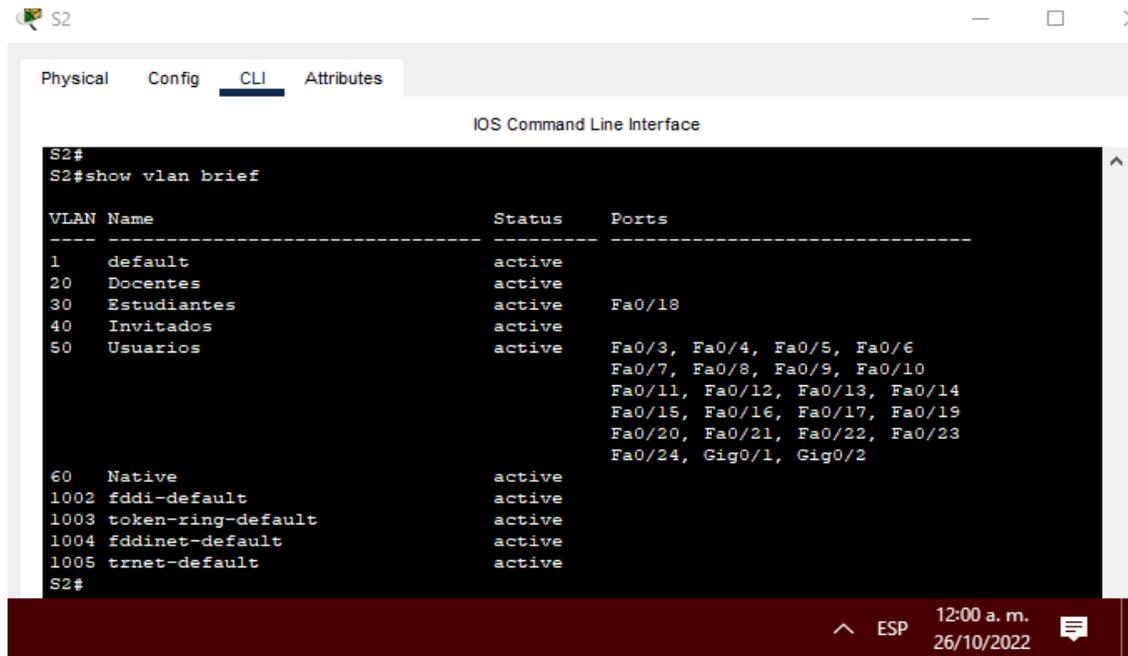
Tabla 15. Comandos de configuración para la infraestructura de red en S2 #2.

Tarea	Especificación
Crear troncales 802.1Q que utilicen la VLAN 60 nativa	int range f0/1-2 channel-group 1 mode active int port-channel 1 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 60
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	int range f0/1-2 switchport trunk allowed vlan 20,30,40,50,60
Configurar el puerto de acceso de host para VLAN 30	inter f0/18 switchport mode access switchport access vlan 30
Configurar la seguridad del puerto en los puertos de acceso	switchport port-security switchport port-security maximum 4
Proteja todas las interfaces no utilizadas	int range f0/3-17 switchport mode access switchport access vlan 50 description Sin Uso shutdown int range f0/19-24 switchport mode access switchport access vlan 50 description Sin Uso shutdown int range g0/1-2 switchport mode access switchport access vlan 50 description Sin Uso shutdown

Fuente: Autor.

Con los comandos ingresados en cada switch, mediante el comando show vlan brief se pueden observar las VLAN's creadas y los puertos especificados en cuestión.

Figura 12. Visualización de VLAN's configuradas en S2.

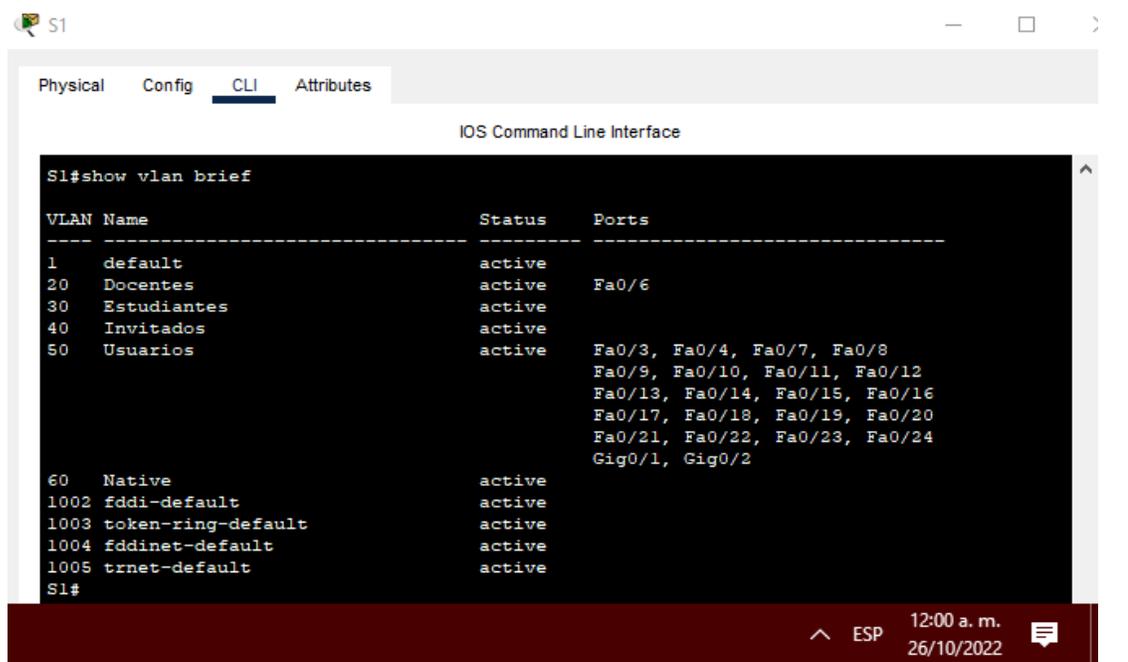


The screenshot shows the CLI of switch S2 with the command 'show vlan brief' executed. The output is a table with three columns: VLAN Name, Status, and Ports. The table lists several VLANs, including the default VLAN (1) and various user-defined VLANs (20, 30, 40, 50, 60) with their respective active statuses and associated ports.

```
S2#  
S2#show vlan brief  
  
VLAN Name                Status    Ports  
-----  
1    default                 active  
20   Docentes                 active  
30   Estudiantes              active    Fa0/18  
40   Invitados                active  
50   Usuarios                 active    Fa0/3, Fa0/4, Fa0/5, Fa0/6  
                                           Fa0/7, Fa0/8, Fa0/9, Fa0/10  
                                           Fa0/11, Fa0/12, Fa0/13, Fa0/14  
                                           Fa0/15, Fa0/16, Fa0/17, Fa0/19  
                                           Fa0/20, Fa0/21, Fa0/22, Fa0/23  
                                           Fa0/24, Gig0/1, Gig0/2  
  
60   Native                   active  
1002 fddi-default             active  
1003 token-ring-default     active  
1004 fddinet-default        active  
1005 trnet-default          active  
S2#
```

Fuente: Autor.

Figura 13. Visualización de VLAN's configuradas en S1.



The screenshot shows the CLI of switch S1 with the command 'show vlan brief' executed. The output is a table with three columns: VLAN Name, Status, and Ports. The table lists several VLANs, including the default VLAN (1) and various user-defined VLANs (20, 30, 40, 50, 60) with their respective active statuses and associated ports.

```
S1#show vlan brief  
  
VLAN Name                Status    Ports  
-----  
1    default                 active  
20   Docentes                 active    Fa0/6  
30   Estudiantes              active  
40   Invitados                active  
50   Usuarios                 active    Fa0/3, Fa0/4, Fa0/7, Fa0/8  
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12  
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16  
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20  
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24  
                                           Gig0/1, Gig0/2  
  
60   Native                   active  
1002 fddi-default             active  
1003 token-ring-default     active  
1004 fddinet-default        active  
1005 trnet-default          active  
S1#
```

Fuente: Autor.

2.4. Parte 4. Configurar soporte de host en R1.

Para esta cuarta y última parte de configuración por consola de comandos, se presentan las configuraciones en R1 con base a las tablas dispuestas en el documento guía, se presentan los comandos empleados en la parte derecha, así mismo, se presenta el registro visual de las configuraciones realizadas mediante el uso de comandos tipo show, como tal, en esta parte, se realiza la configuración para generar el servicio DHCP para los hosts.

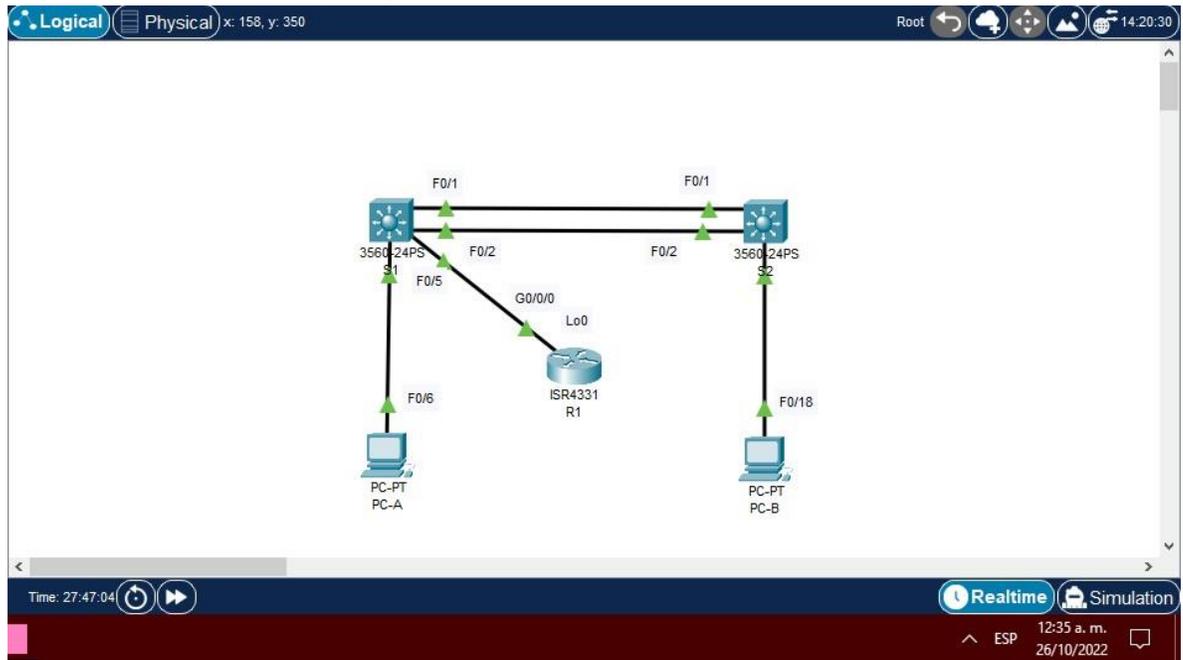
Tabla 16. Comandos de configuración para el servicio DHCP desde R1.

Tarea	Especificación
Configure Default Routing	conf ter ip route 0.0.0.0 0.0.0.0 loopback 0 ipv6 route ::/0 loopback 0
Configurar IPv4 DHCP para la VLAN 20	ip dhcp pool VLAN20 network 10.42.8.0 255.255.255.192 default-router 10.42.8.1 domain-name unad-ccna-sa.net ip dhcp excluded-address 10.42.8.2 10.42.8.51
Configurar DHCP IPv4 para la VLAN 30	ip dhcp pool VLAN30 network 10.42.8.64 255.255.255.224 default-router 10.42.8.65 domain-name unad-ccna-sb.net ip dhcp excluded-address 10.42.8.66 10.42.8.83 exit

Fuente: Autor.

Luego de realizar las configuraciones de las cuatro primeras partes, el escenario resultante en el programa Packet Tracer se observa en la figura 14 a continuación.

Figura 14. Segunda topología de red resultante.



Fuente: Autor.

2.5. Parte 5. Configurar los equipos de red.

Para la quinta parte se realiza el direccionamiento en los equipos PC-A y PC-B empelando DHCP previamente configurado en R1 para IPv4 e IPv6 de forma manual con base a los datos de la tabla 5, con ello se tiene:

Tabla 17. Información de direccionamiento en PC-A.

Configuración de red de PC-A	
Descripción	PC-A
Dirección física	00D0.BCE3.D7D7
Dirección IP	10.42.8.2
Mascara de subred	255.255.255.192
Gateway predeterminado	10.42.8.1
Gateway predeterminado IPv6	FE80::1

Fuente: Autor.

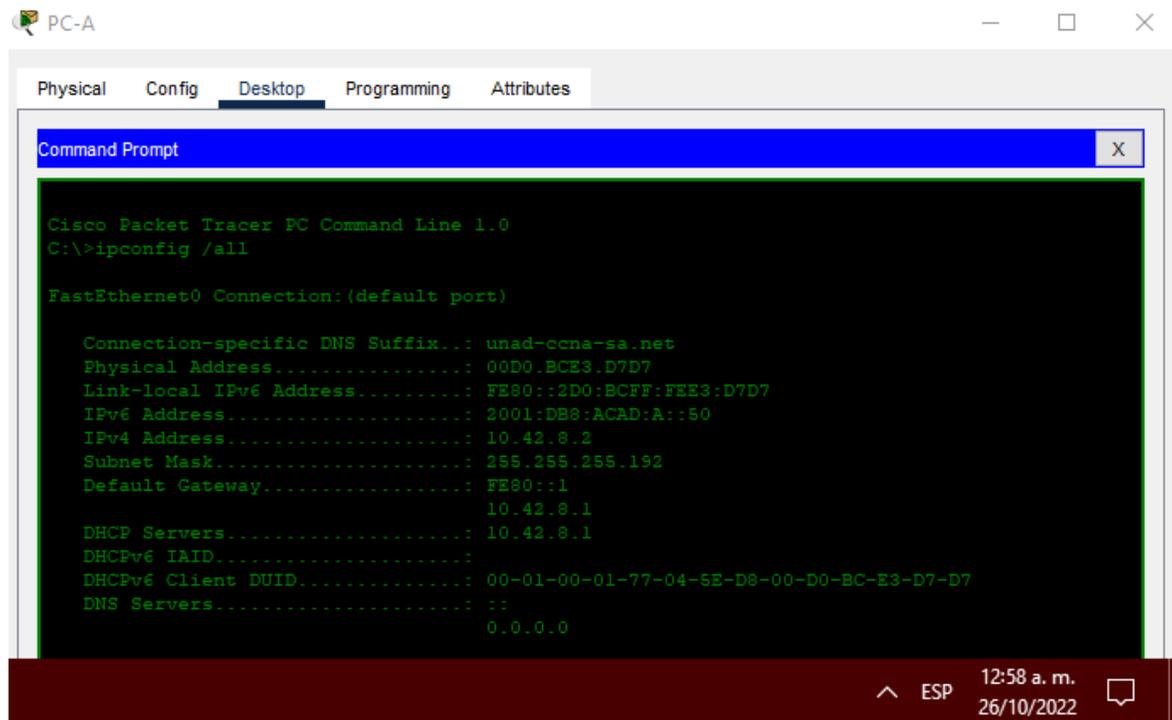
Tabla 18. Información de direccionamiento en PC-B.

Configuración de red de PC-B	
Descripción	PC-B
Dirección física	0050.0F11.5640
Dirección IP	10.42.8.66
Mascara de subred	255.255.255.224
Gateway predeterminado	10.42.8.65
Gateway predeterminado IPv6	FE80::1

Fuente: Autor.

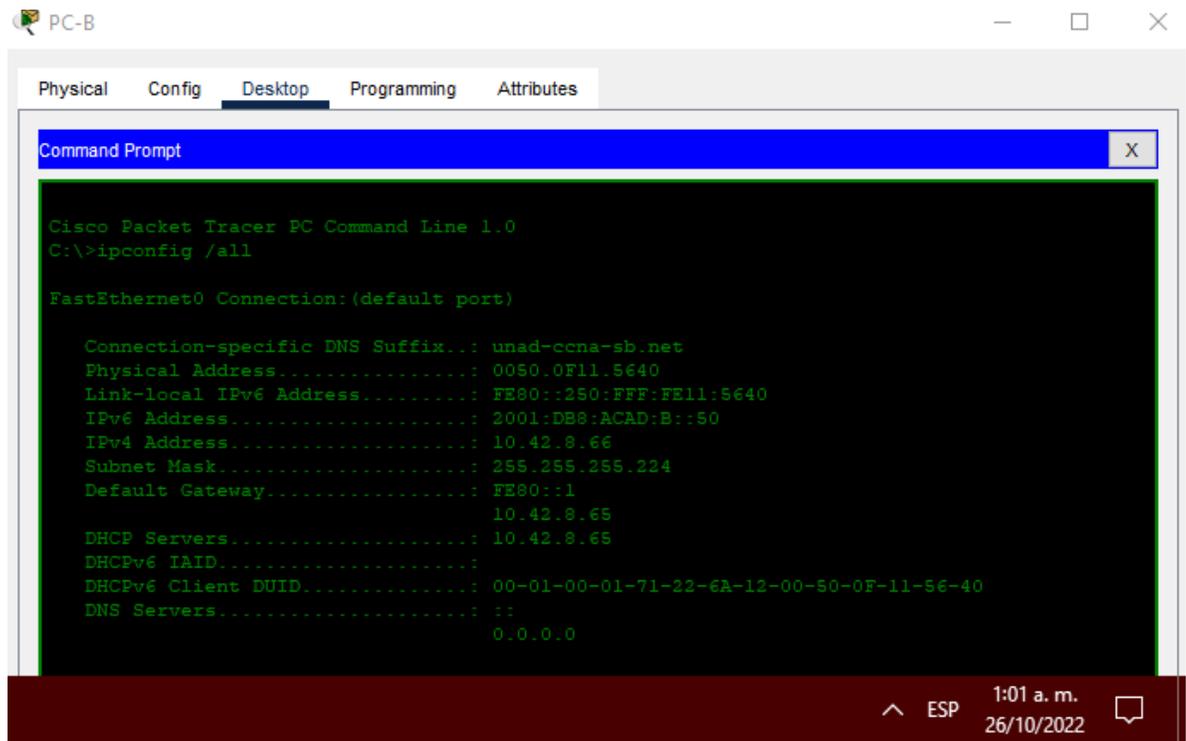
Dicha información se puede constatar al revisar la información de dichos PC's mediante el comando ipconfig /all.

Figura 15. Información total de dirección para PC-A.



Fuente: Autor.

Figura 16. Información total de dirección para PC-B.

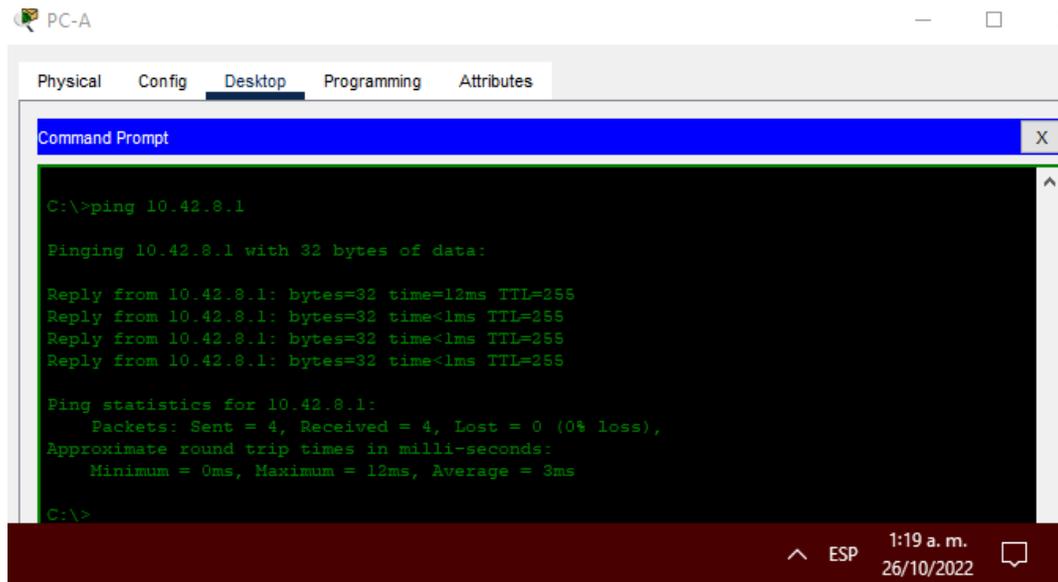


Fuente: Autor.

2.6. Parte 6. Probar y verificar la conectividad de extremo a extremo

Finalmente, la guía dispone de una tabla para listar las múltiples pruebas de ping que se pueden realizar en la red para detallar la conexión IPv4 e IPv6 en la segunda topología de red. Por cuestiones de ajuste de tabla y visualización de las imágenes, se omite la tabla y se presenta una a una las pruebas realizadas.

Figura 17. Prueba de ping desde PC-A a R1 G0/0/1.20 para IPv4.



```
C:\>ping 10.42.8.1

Pinging 10.42.8.1 with 32 bytes of data:

Reply from 10.42.8.1: bytes=32 time=12ms TTL=255
Reply from 10.42.8.1: bytes=32 time<1ms TTL=255
Reply from 10.42.8.1: bytes=32 time<1ms TTL=255
Reply from 10.42.8.1: bytes=32 time<1ms TTL=255

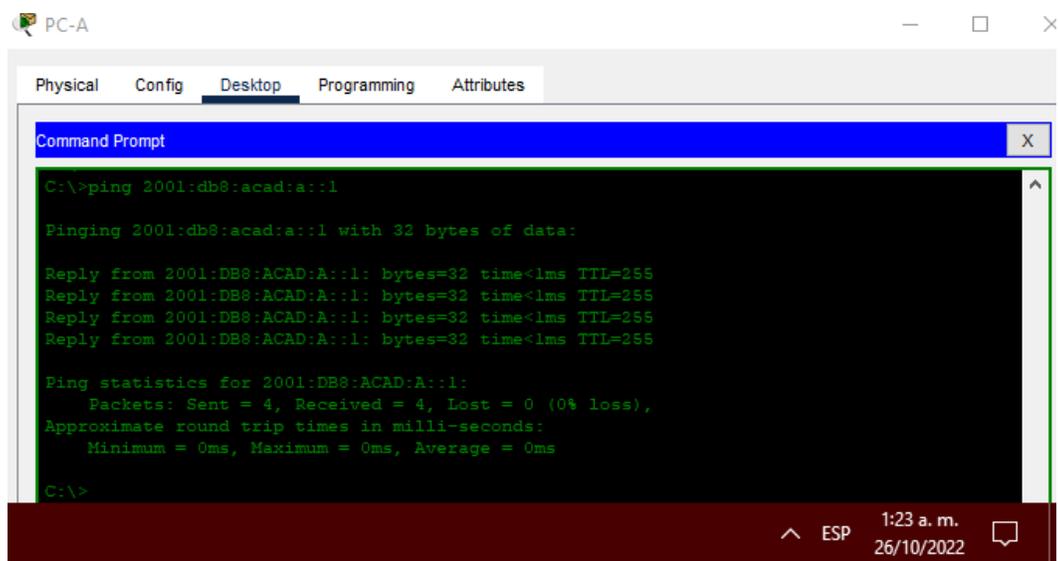
Ping statistics for 10.42.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 3ms

C:\>
```

Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz.

Figura 18. Prueba de ping desde PC-A a R1 G0/0/1.20 para IPv6.



```
C:\>ping 2001:db8:acad:a::1

Pinging 2001:db8:acad:a::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255

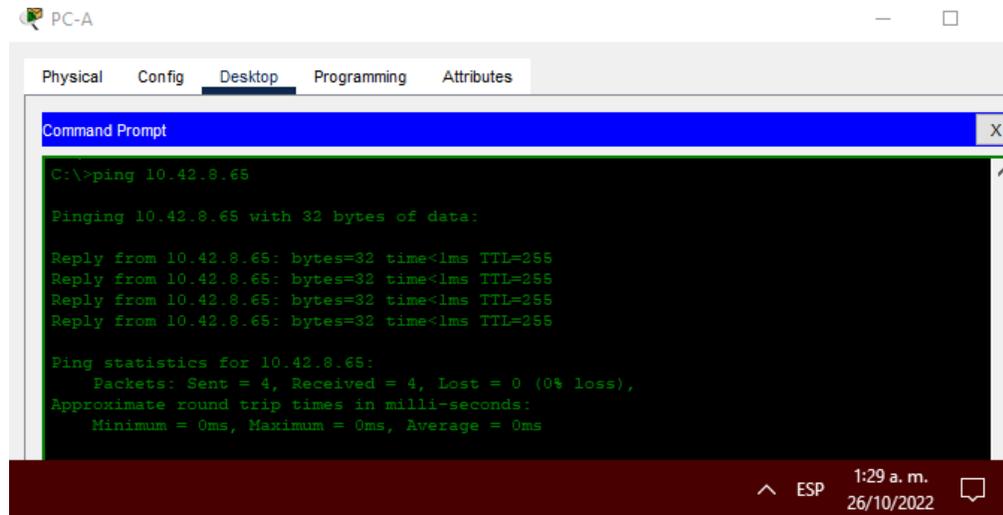
Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz.

Figura 19. Prueba de ping desde PC-A a R1 G0/0/1.30 para IPv4.



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.42.8.65

Pinging 10.42.8.65 with 32 bytes of data:

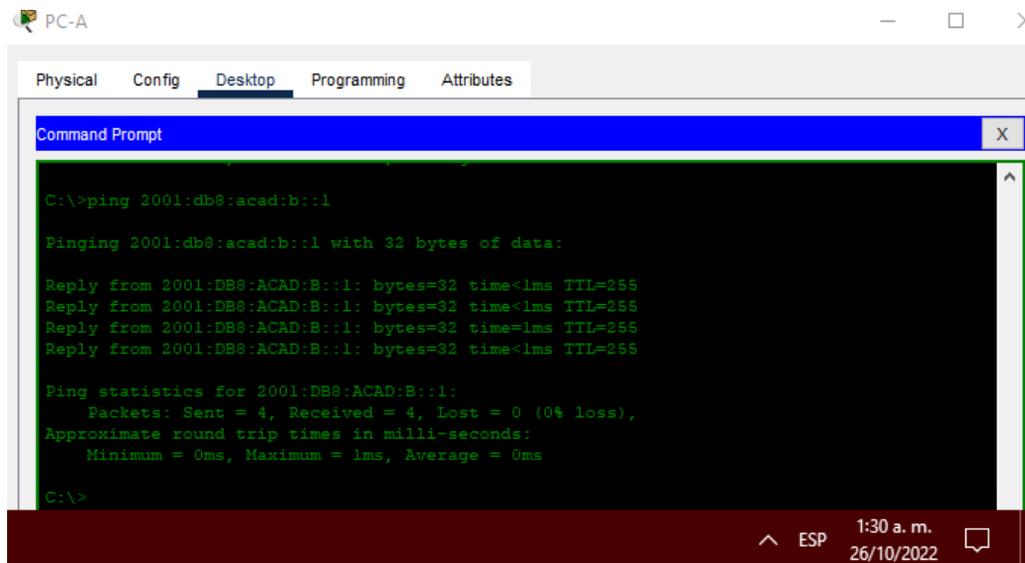
Reply from 10.42.8.65: bytes=32 time<lms TTL=255

Ping statistics for 10.42.8.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz.

Figura 20. Prueba de ping desde PC-A a R1 G0/0/1.30 para IPv6.



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 2001:db8:acad:b::1

Pinging 2001:db8:acad:b::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::1: bytes=32 time<lms TTL=255

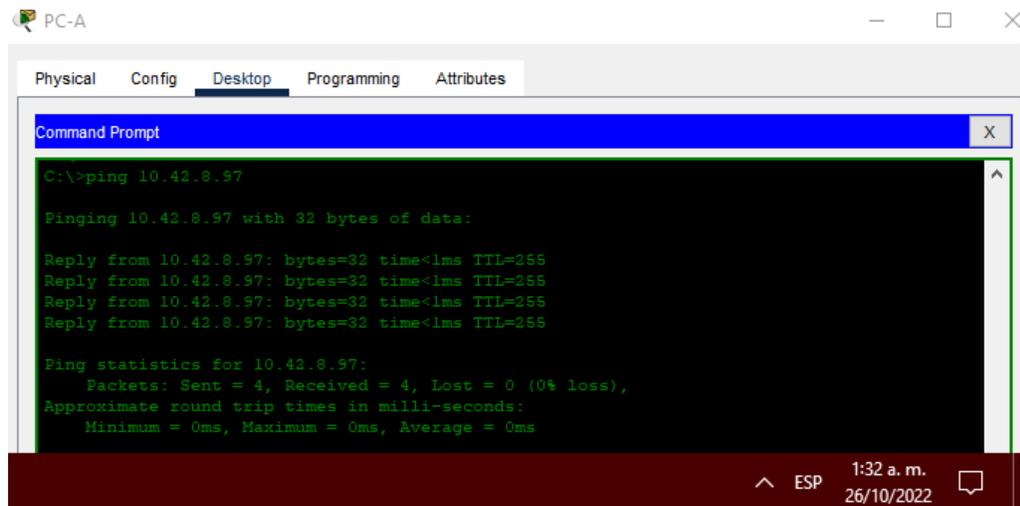
Ping statistics for 2001:DB8:ACAD:B::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz.

Figura 21. Prueba de ping desde PC-A a R1 G0/0/1.40 para IPv4.



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.42.8.97

Pinging 10.42.8.97 with 32 bytes of data:

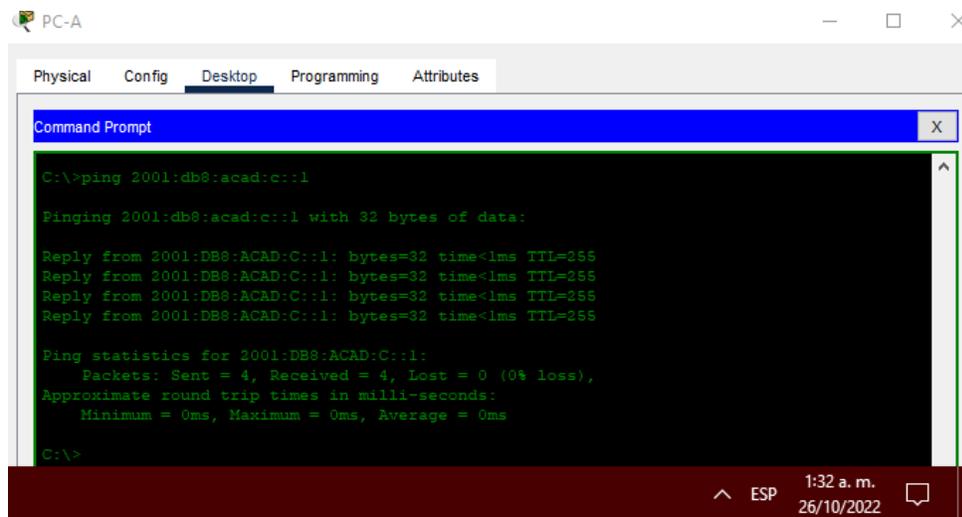
Reply from 10.42.8.97: bytes=32 time<1ms TTL=255

Ping statistics for 10.42.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz.

Figura 22. Prueba de ping desde PC-A a R1 G0/0/1.40 para IPv6.



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 2001:db8:acad:c::1

Pinging 2001:db8:acad:c::1 with 32 bytes of data:

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

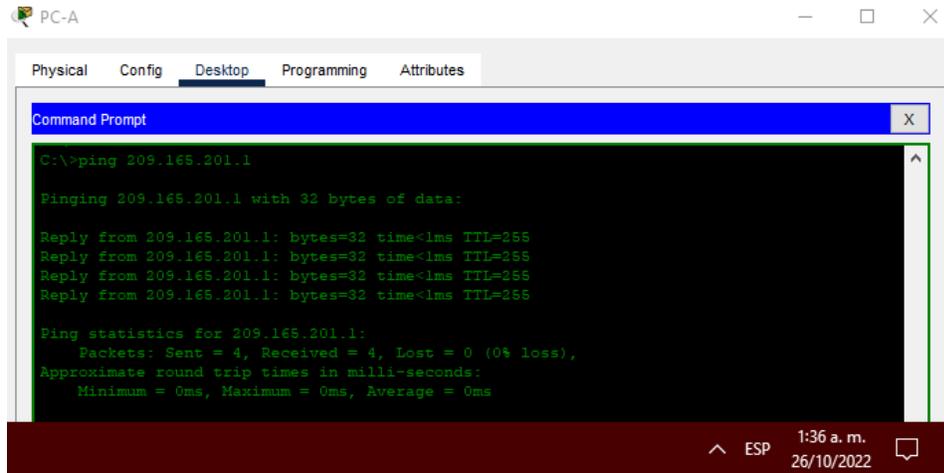
Ping statistics for 2001:DB8:ACAD:C::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz.

Figura 23. Prueba de ping desde PC-A a Loopback 0 para IPv4.



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 209.165.201.1

Pinging 209.165.201.1 with 32 bytes of data:

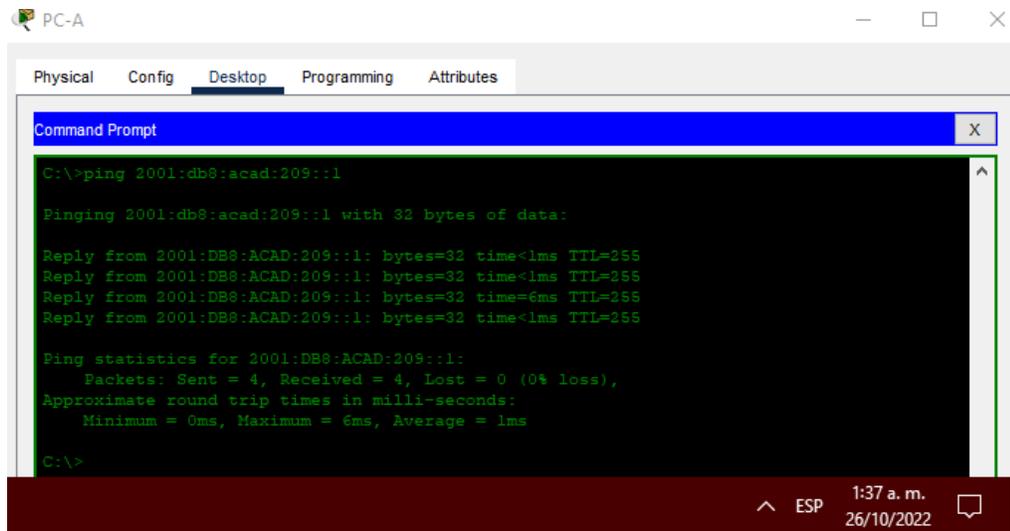
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz.

Figura 24. Prueba de ping desde PC-A a Loopback 0 para IPv6.



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 2001:db8:acad:209::1

Pinging 2001:db8:acad:209::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time=6ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255

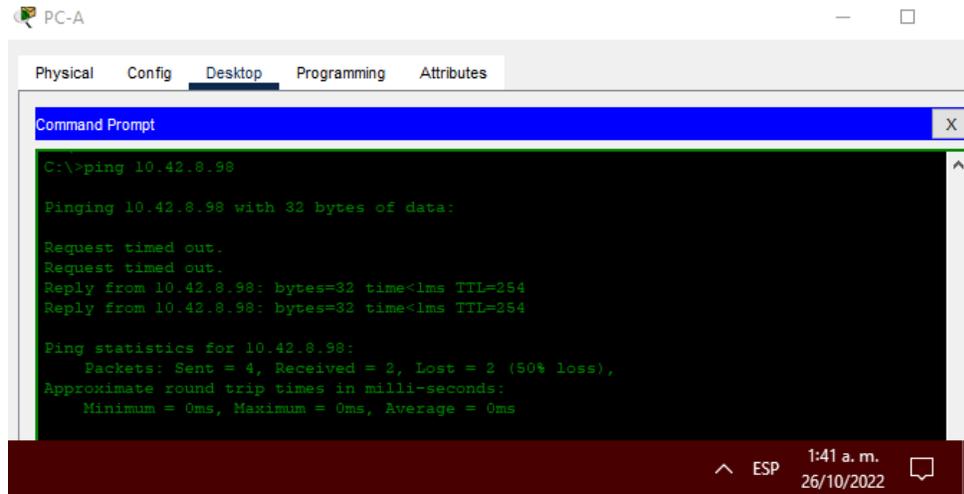
Ping statistics for 2001:DB8:ACAD:209::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms

C:\>
```

Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz.

Figura 25. Prueba de ping desde PC-A a S1 VLAN 40.



```
C:\>ping 10.42.8.98

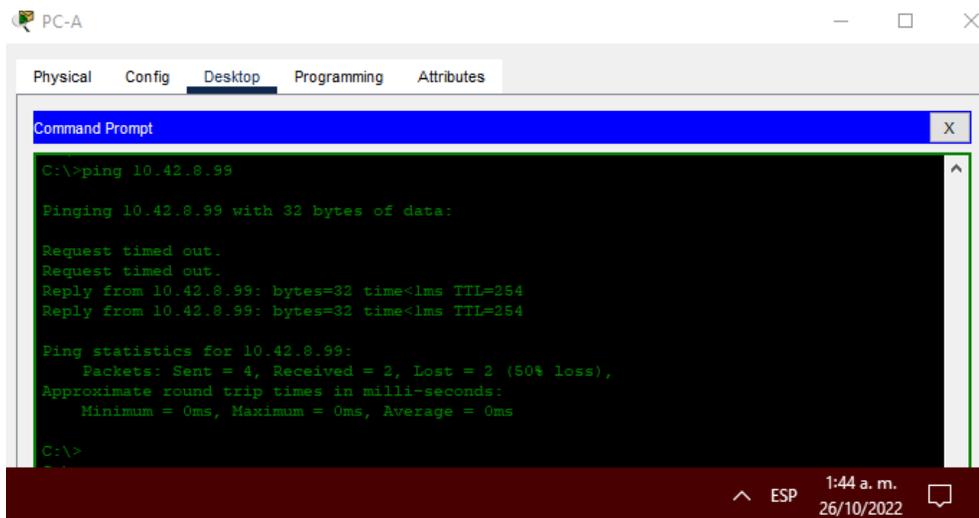
Pinging 10.42.8.98 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 10.42.8.98: bytes=32 time<1ms TTL=254
Reply from 10.42.8.98: bytes=32 time<1ms TTL=254

Ping statistics for 10.42.8.98:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz para IPv4, pero no para IPv6.

Figura 26. Prueba de ping desde PC-A a S2 VLAN 40.



```
C:\>ping 10.42.8.99

Pinging 10.42.8.99 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 10.42.8.99: bytes=32 time<1ms TTL=254
Reply from 10.42.8.99: bytes=32 time<1ms TTL=254

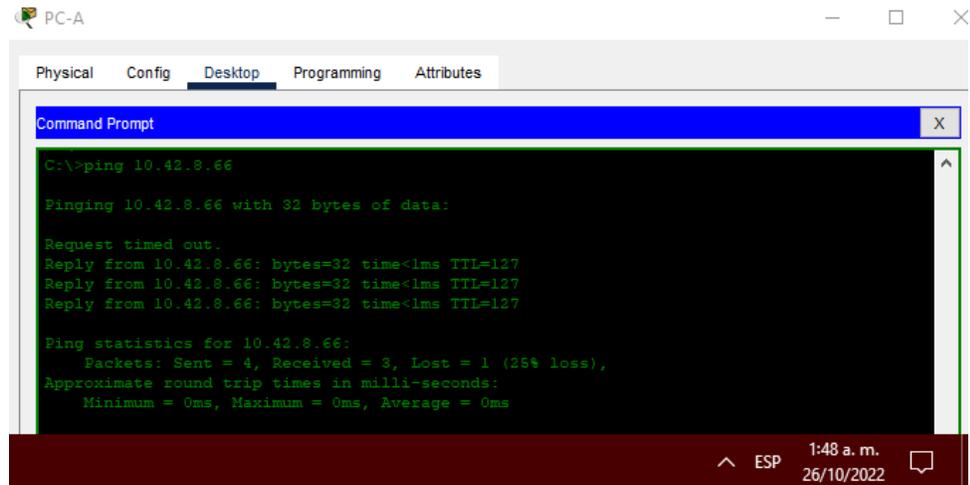
Ping statistics for 10.42.8.99:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz para IPv4 pero no para IPv6.

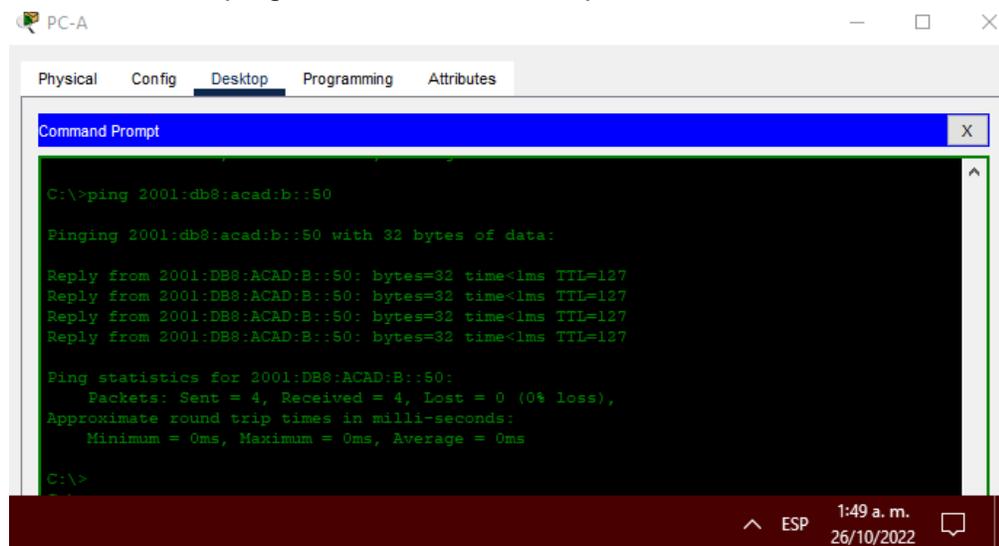
Figura 27. Prueba de ping desde PC-A a PC-B para IPv4.



Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz.

Figura 28. Prueba de ping desde PC-A a PC-B para IPv6.



Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz.

Al igual se realizan las pruebas de ping empleando las mismas direcciones de las interfaces o sub-interfaces desde PC-B obteniendo los resultados de la siguiente tabla:

Tabla 19. Resultados de pruebas de ping desde PC-A.

Desde	A	Protocolo	Resultado
PC-A	R1 G0/0/1.20	IPv4	Satisfactorio
		IPv6	Satisfactorio
	R1 G0/0/1.30	IPv4	Satisfactorio
		IPv6	Satisfactorio
	R1 G0/0/1.40	IPv4	Satisfactorio
		IPv6	Satisfactorio
	S1 VLAN 40	IPv4	Satisfactorio
		IPv6	Fallido
	S2 VLAN 40	IPv4	Satisfactorio
		IPv6	Fallido
	PC-B	IPv4	Satisfactorio
		IPv6	Satisfactorio
R1 Loopback 0	IPv4	Satisfactorio	
	IPv6	Satisfactorio	

Fuente: Autor.

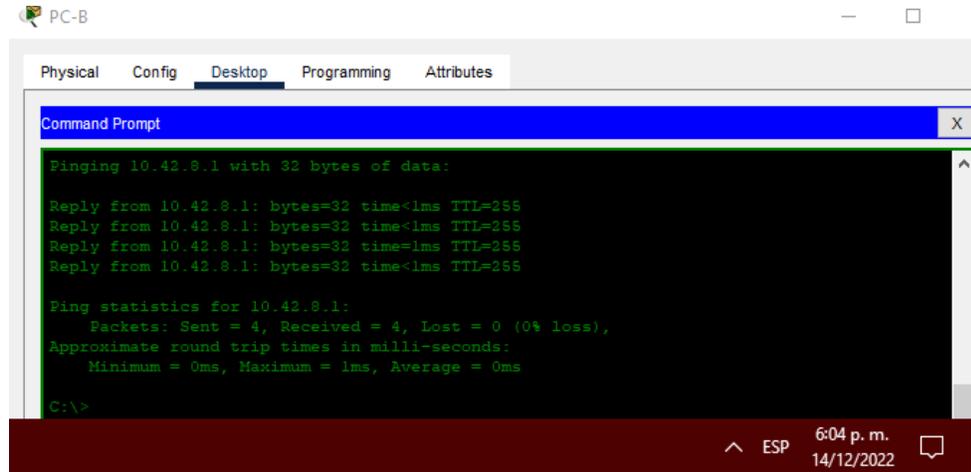
Tabla 20. Resultados de pruebas de ping desde PC-B.

Desde	A	Protocolo	Resultado
PC-B	R1 G0/0/1.20	IPv4	Satisfactorio
		IPv6	Satisfactorio
	R1 G0/0/1.30	IPv4	Satisfactorio
		IPv6	Satisfactorio
	R1 G0/0/1.40	IPv4	Satisfactorio
		IPv6	Satisfactorio
	S1 VLAN 40	IPv4	Satisfactorio
		IPv6	Fallido
	S2 VLAN 40	IPv4	Satisfactorio
		IPv6	Fallido
	R1 Loopback 0	IPv4	Satisfactorio
		IPv6	Satisfactorio

Fuente: Autor.

Las pruebas listadas en la tabla 20 se observan a continuación:

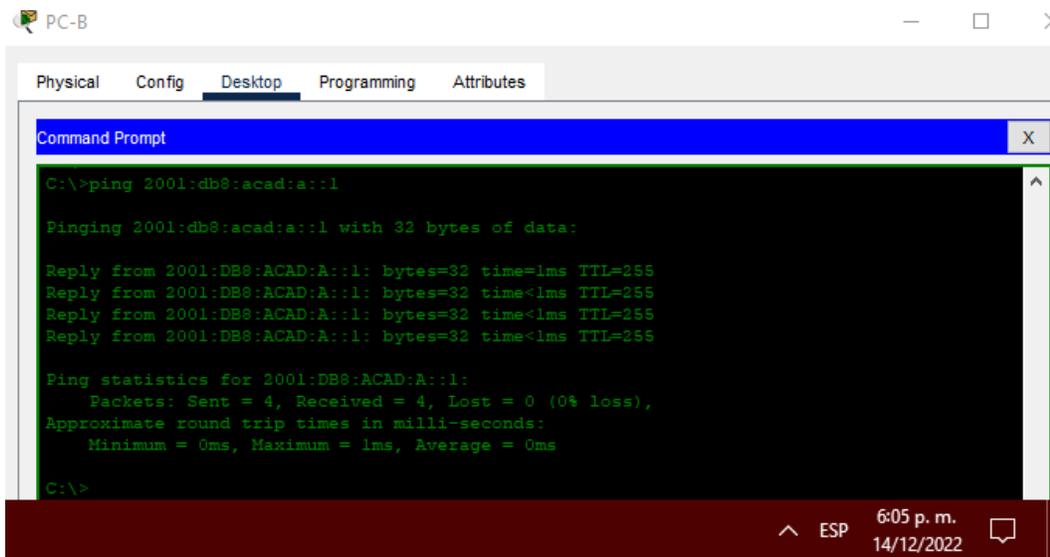
Figura 29. Prueba de ping desde PC-B a R1 G0/0/1.20 para IPv4.



Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz.

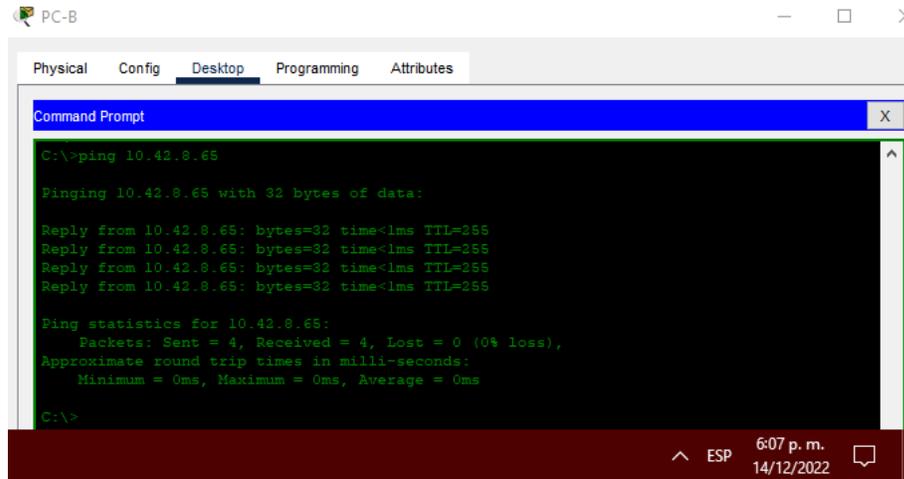
Figura 30. Prueba de ping desde PC-B a R1 G0/0/1.20 para IPv6.



Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz.

Figura 31. Prueba de ping desde PC-B a R1 G0/0/1.30 para IPv4.

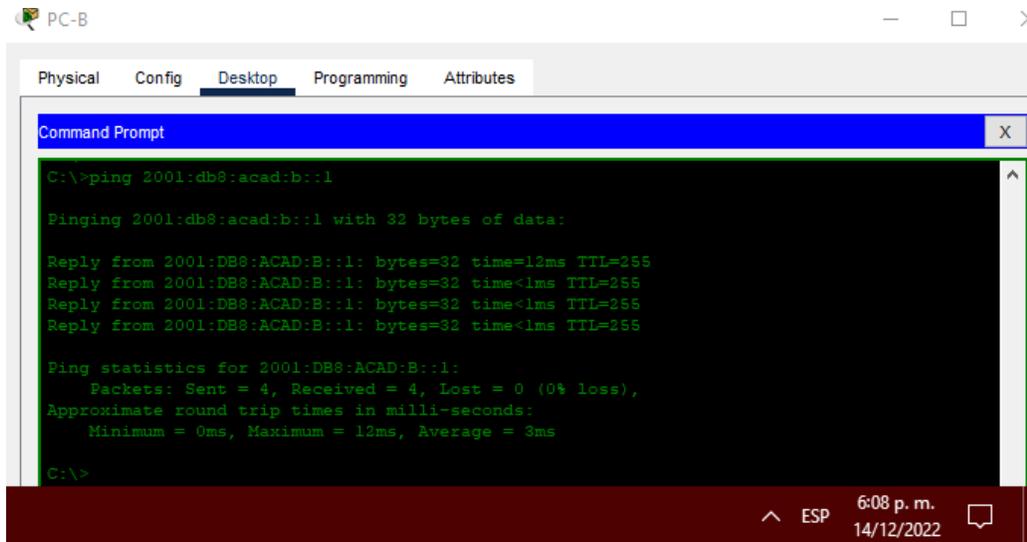


```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.42.8.65
Pinging 10.42.8.65 with 32 bytes of data:
Reply from 10.42.8.65: bytes=32 time<1ms TTL=255
Ping statistics for 10.42.8.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz.

Figura 32. Prueba de ping desde PC-B a R1 G0/0/1.30 para IPv6.

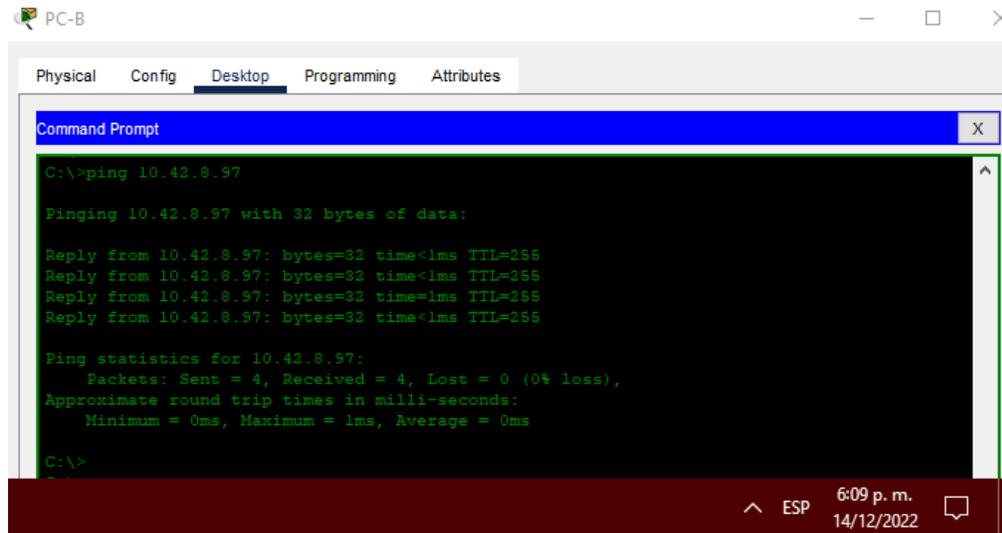


```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 2001:db8:acad:b::1
Pinging 2001:db8:acad:b::1 with 32 bytes of data:
Reply from 2001:DB8:ACAD:B::1: bytes=32 time=12ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Ping statistics for 2001:DB8:ACAD:B::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 3ms
C:\>
```

Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz.

Figura 33. Prueba de ping desde PC-B a R1 G0/0/1.40 para IPv4.



```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.42.8.97

Pinging 10.42.8.97 with 32 bytes of data:

Reply from 10.42.8.97: bytes=32 time<1ms TTL=255

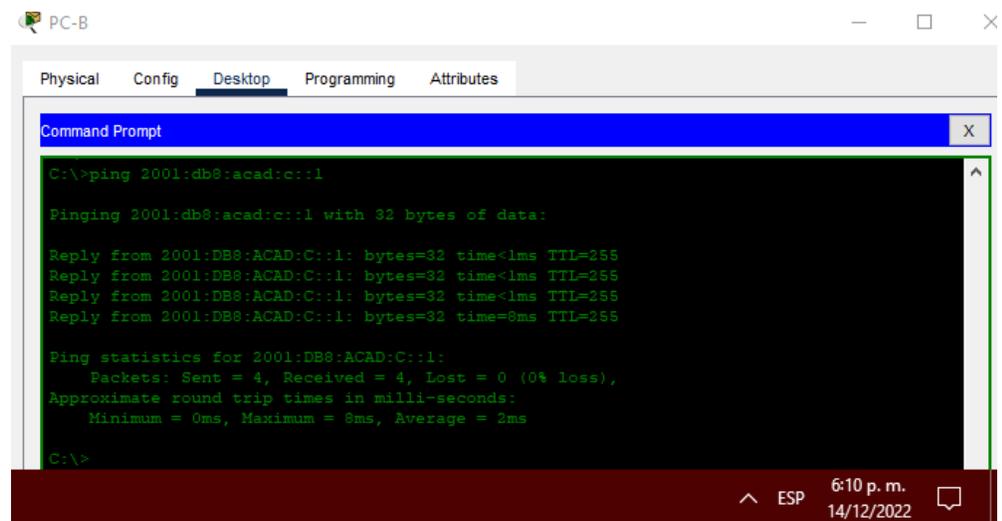
Ping statistics for 10.42.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz.

Figura 34. Prueba de ping desde PC-B a R1 G0/0/1.40 para IPv6.



```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 2001:db8:acad:c::1

Pinging 2001:db8:acad:c::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time=8ms TTL=255

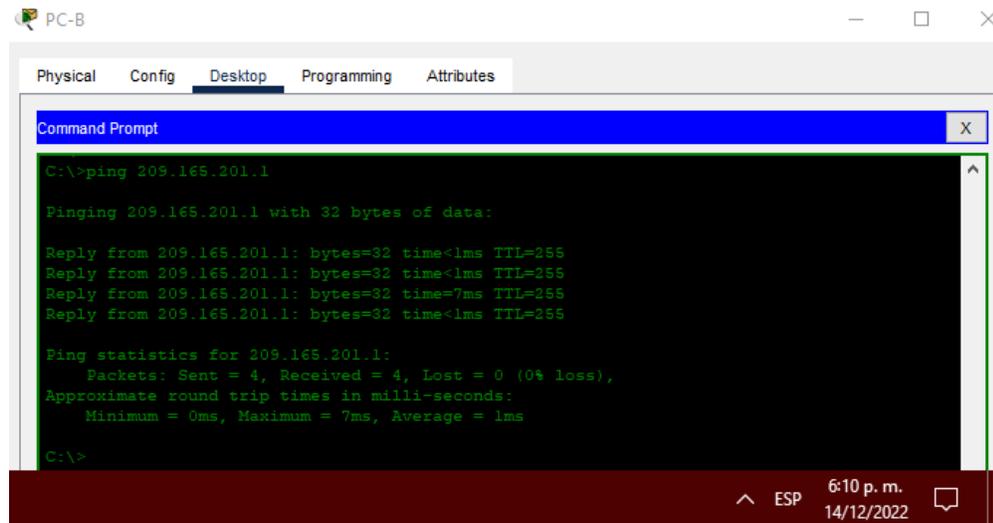
Ping statistics for 2001:DB8:ACAD:C::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms

C:\>
```

Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz.

Figura 35. Prueba de ping desde PC-B a Loopback 0 para IPv4.



```
C:\>ping 209.165.201.1

Pinging 209.165.201.1 with 32 bytes of data:

Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time=7ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255

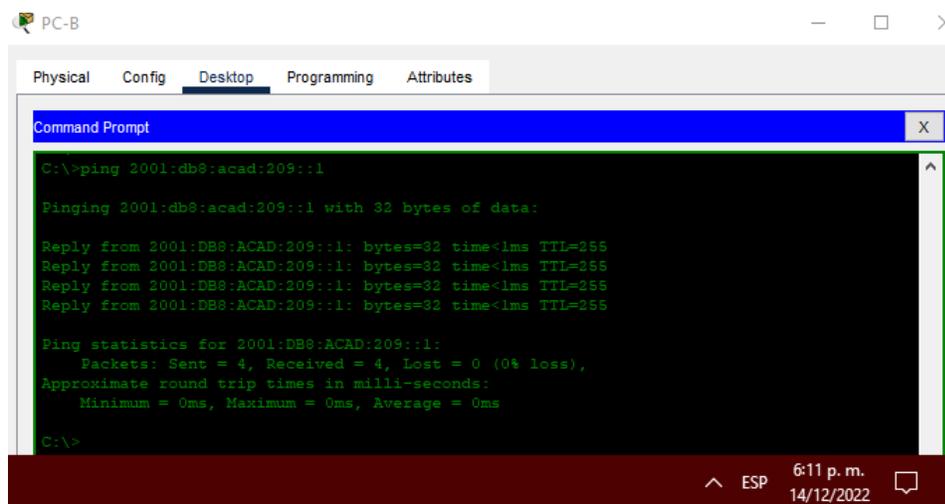
Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 1ms

C:\>
```

Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz.

Figura 36. Prueba de ping desde PC-B a Loopback 0 para IPv6.



```
C:\>ping 2001:db8:acad:209::1

Pinging 2001:db8:acad:209::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255

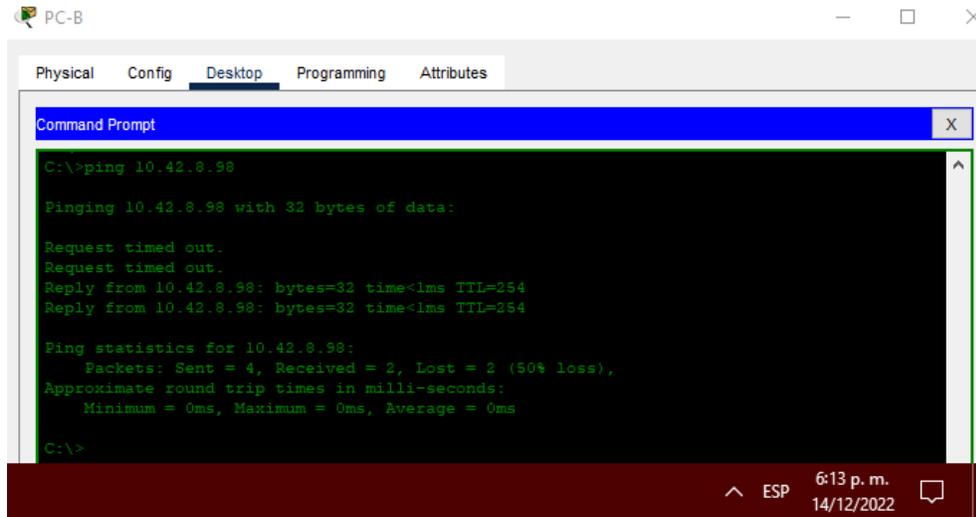
Ping statistics for 2001:DB8:ACAD:209::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz.

Figura 37. Prueba de ping desde PC-B a S1 VLAN 40.



```
C:\>ping 10.42.8.98

Pinging 10.42.8.98 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.42.8.98: bytes=32 time<1ms TTL=254
Reply from 10.42.8.98: bytes=32 time<1ms TTL=254

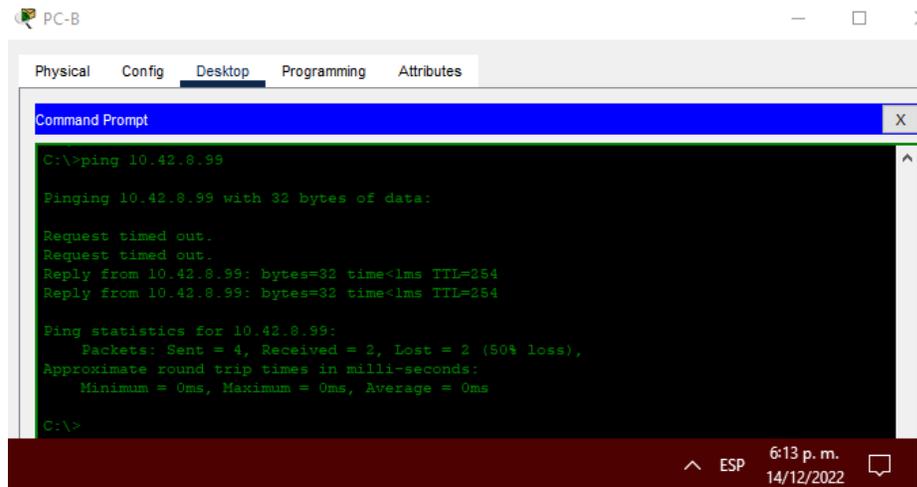
Ping statistics for 10.42.8.98:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz para IPv4, pero no para IPv6.

Figura 38. Prueba de ping desde PC-B a S2 VLAN 40.



```
C:\>ping 10.42.8.99

Pinging 10.42.8.99 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.42.8.99: bytes=32 time<1ms TTL=254
Reply from 10.42.8.99: bytes=32 time<1ms TTL=254

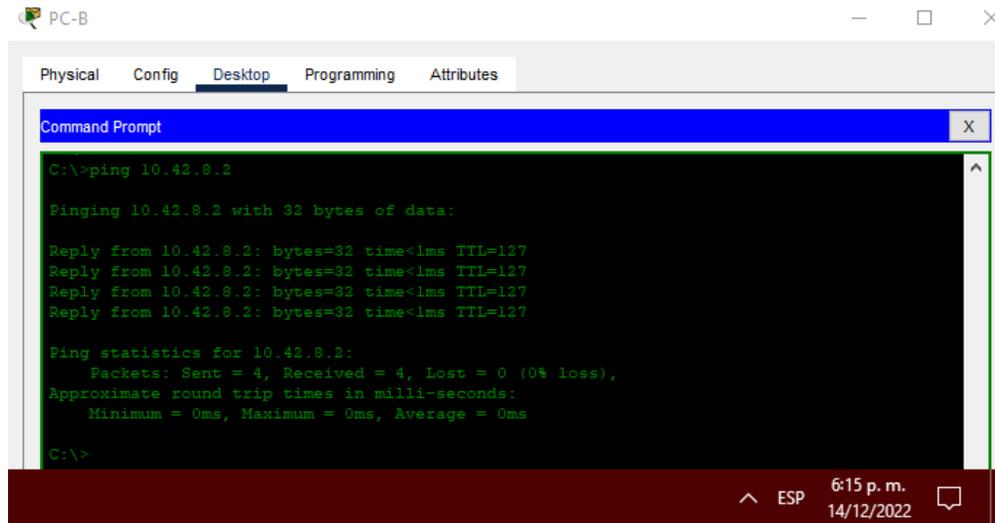
Ping statistics for 10.42.8.99:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz para IPv4 pero no para IPv6.

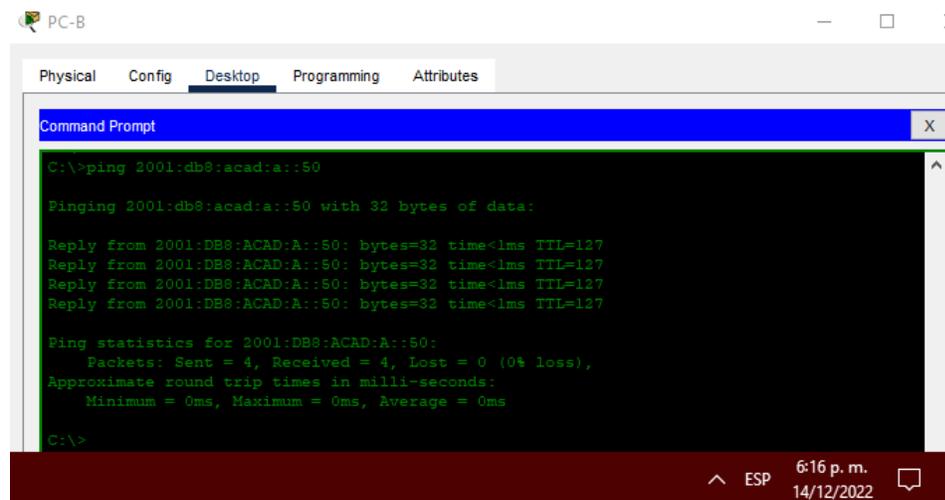
Figura 39. Prueba de ping desde PC-B a PC-A para IPv4.



Fuente: Autor.

Como se observa en la figura anterior, el resultado es eficaz.

Figura 40. Prueba de ping desde PC-B a PC-A para IPv6.



Fuente: Autor.

Esto permite detallar que el direccionamiento para ambos protocolos de dirección fue correcto también para el host PCB, exceptuando las pruebas a la VLAN40 por IPv6 que más adelante se explicara en las conclusiones.

CONCLUSIONES

La realización de direccionamiento empleando conocimientos como VLSM permite detallar la importancia de realizar una correcta segmentación de direcciones para garantizar y ofrecer el máximo número de hosts en una red, así como asignar correctamente las gateway y máscaras de red en los dispositivos ya que como se observó, suelen ser alguna de las problemáticas cuando los equipos no se pueden conectar o comunicar en una red, esto muy importante cuando se direcciona con IPv4 debido a la escasez de sus direcciones y que puede ser ampliamente mejorado empleando el protocolo DHCP ya bien sea con servidores o routers.

Las pruebas de ping permitieron identificar un método eficiente para encontrar y categorizar problemáticas en una red ya bien sea mediante pruebas de latencia o trazado de rutas pero que al ser un método sencillo no se debe siempre estar totalmente confiando de los resultados que entrega.

Finalmente, la configuración de enlaces troncales permite identificar la facilidad para la inter comunicación entre las VLAN's configuradas en una topología, así como compartir dicha información entre la red, lo que permite observar también que elimina la necesidad de emplear un enlace físico para cada VLAN lo cual puede llegar a ser muy tedioso cuando se maneja un numero alto de redes virtuales o VLAN's en una topología de red.

BIBLIOGRAFÍA

CISCO. Configuración de IPv4 e IPv6 en un punto de acceso inalámbrico. {En línea} (2018) {26 de octubre de 2022}. Disponible en: https://www.cisco.com/c/es_mx/support/docs/smb/wireless/cisco-small-business-100-series-wireless-access-points/smb5176-configure-ipv4-and-ipv6-on-a-wireless-access-point.html.

CISCO. Configure InterVLAN routing on Layer 3 switches. {En línea} (2020) {26 de octubre de 2022}. Disponible en: <https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html>

ENI. Routers y switches de nivel 3. Ediciones-eni. {En línea} (2019) {26 de octubre de 2022}. Disponible en: <https://www.ediciones-eni.com/open/mediabook.aspx?idR=c8e579cf5beae0192df4f95dde0d93a3>

FERNANDEZ, Lorena. Así puedes configurar un enlace trunk en un switch gestionable. RedesZone. {En línea} (2020) {26 de octubre de 2022}. Disponible en: <https://www.redeszone.net/tutoriales/redes-cable/configurar-enlace-troncal-switch/>

MARTINEZ, Cristóbal. VLANs y Trunk ports. JMCristobal. {En línea} (2021) {26 de octubre de 2022}. Disponible en: <https://jmcristobal.com/2021/01/22/vlans-y-trunk-ports/>

SEPULVEDA, Manuel. Configuración de DHCP en Cisco Router - eClassVirtual - Cursos Cisco en línea. eClassVirtual. {En línea} (2019) {26 de octubre de 2022}. Disponible en: <https://eclassvirtual.com/configuracion-de-dhcp-en-cisco-router/>

ANEXOS

Anexo A: Simulaciones

[https://drive.google.com/drive/folders/1PgnorPoJPnijpZioUFtcRvQTO86hb5Fm?usp=share link](https://drive.google.com/drive/folders/1PgnorPoJPnijpZioUFtcRvQTO86hb5Fm?usp=share_link)