

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

RICARDO AGREDO TRUJILLO

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

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

RICARDO AGREDO TRUJILLO

Diplomado de opción de grado presentado para optar el
título de INGENIERO DE SISTEMAS

PAULITA FLOR SALAZAR
DIRECTOR

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

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Calarcá, 27 de octubre de 2022

DEDICATORIA

El siguiente trabajo representa la finalización de un largo proceso académico, por esta razón está dedicado a mi familia quienes siempre me han demostrado su apoyo incondicional, compartiendo su amor, cariño y comprensión en cada meta que me he propuesto, brindándome su granito de arena en este proyecto de vida.

A mi madre Diana Trujillo Castro por su amor incondicional desde el momento en que nací, brindándome una infancia llena de amor y felicidad, teniendo paciencia para educarme, fortaleza y autoridad para corregirme en los momentos oportunos, estando siempre dispuesta a escucharme y transformando todos los momentos de amargura en procesos de reflexión, enseñándome que cada acción tiene una consecuencia ya sea buena o mala, que mentir es lo peor que puede decir una persona, qué con el esfuerzo y sacrificio que ha realizado a lo largo de todos estos años han permitido formarme como profesional.

A mi abuela Omaira Castro de Trujillo, por sus incesantes oraciones desde el momento en el que nací, las cuales se han transformado en fortaleza en los momentos de flaqueza, bendiciones en los momentos de felicidad, y tranquilidad en los momentos de tristeza, por estar siempre dispuesta a preparar mi comida favorita sin importar la hora del día, por consentirme tanto en infinidad de ocasiones, necesitando todas las estrellas del universo y granos de arena del mundo para lograr contarlas, y finalmente por permitir que me convierta en su bordón de la vejez en honor a aquél que ya no está con nosotros.

A mi abuelo Darío Trujillo Celis (q.d.e.p) quien fue mi ejemplo a seguir desde una edad temprana, el cual me inculcó los valores que ahora son para mí una regla de vida grabándose a fuego en mi interior, quién siempre me puso como prioridad ante cualquier situación, ofreciéndome lo mejor dentro de las posibilidades, velando por mi seguridad y calidad de vida haciendo que no me faltará nada incluso después del momento en el que fue llamado por Dios, inculcándome un

sin fin de valores, entre ellos, la confianza, la autoridad y la más importante de todos la responsabilidad, demostrándome desde muy pequeño que la única forma de cumplir los sueños y metas es no desistir, que si llegado el momento se debe retroceder, que sea para tomar impulso y finalmente por ser él mi bordón en la niñez.

A mi padre José Eduardo Agredo Hernández, quien pese a la distancia siempre tiene la disposición y tiempo para escucharme, brindándome su sabiduría y consejos, convirtiéndose en ese *amigo* que todo hijo necesita, por apoyarme y celebrar cada logro que he realizado, a mis abuelos paternos Lilia Hernández y José Ignacio Agredo Rojas, por recibirme siempre con las puertas y brazos abiertos en cada momento, por ayudarme de diferentes maneras desde tan lejos, a mi hermana Katerin Agredo Ruiz por convertir muchas navidades en momentos de felicidad que jamás olvidaré, por todas las travesuras que hicimos desde pequeños, por ese cariño de hermanos que nos une.

A quienes considero que puedo llamar amigos, y compartieron conmigo de manera altruista sus consejos, palabras de motivación, momentos de distracción, de felicidad y un sinfín de cosas, Camilo Sánchez Perdomo, Carolina Herrera Zabala, Daniel Beltrán Gómez, Daniel Gerardo, Jonathan Coronado, Juan Luis Duarte, Karen B. Ibarra, Laura Fernanda (*Lu Fer*) y Néider Alejandro Cárdenas García, de igual forma a todos mis familiares, pero especialmente a mis primos Javier Alejandro Ibarra y Jhon Freddy Gómez quienes siempre me brindaron un espacio cuando lo necesitaba.

A todos ustedes infinitas gracias.

AGRADECIMENTOS

Un agradecimiento especial a la Universidad Nacional Abierta y a Distancia – UNAD y su programa de formación a distancia, la cual sin este no me hubiera permitido culminar mi carrera profesional, por permitirme hacer uso de sus diferentes instituciones, laboratorios e instrumentos de educación, por brindarme excelentes tutores quienes tienen la paciencia y vocación para instruir.

A la Ingeniera de Telecomunicaciones y directora de curso del diplomado de profundización Cisco 2022 (Diseño e implementación de soluciones integradas LAN/WAN) Paulita Flor por compartir sus conocimientos de CCNA, resolver inquietudes, y brindarnos los diferentes espacios de capacitación para poder ejercer esta noble profesión.

Al Ingeniero químico Wilberth Daniel Diaz Prada por su constante asesoría y tutoría académica en mis inicios de la carrera profesional, quien siempre resolvió mis dudas por más absurdas que fueran y fue un faro en el ámbito matemático, ayudándome a desarrollar mi lado lógico – matemático.

Al Ingeniero de Sistemas y Computación Daniel Beltrán Gómez quien fue mi primer amigo en el transcurso de esta profesión, brindándome su amistad y compartiendo su conocimiento en el ámbito de programación, quien me acompañó “*sin peros*” en altas horas de la noche mientras buscábamos donde me faltaba un punto y coma.

A todos ustedes infinitas gracias.

CONTENIDO

	Página
DEDICATORIA	4
AGRADECIMIENTOS	6
CONTENIDO	7
LISTA DE TABLAS	9
LISTA DE FIGURAS.....	10
GLOSARIO	12
RESUMEN.....	13
ABSTRACT	13
INTRODUCCION.....	14
DESARROLLO	15
1. ESCENARIO 1	15
1.1 DIRECCIONAMIENTO	16
1.2 ROUTER “R1”	18
1.3 SWITCH “S1”	19
1.4 CONFIGURACIÓN BÁSICA ROUTER “R1”	19
1.5 CONFIGURACIÓN BÁSICA SWITCH “S1”	26
1.6 CONFIGURACIÓN DE LOS DISPOSITIVOS FINALES PC – A Y PC - B	33
1.7 PRUEBA CONECTIVIDAD EXTREMO A EXTREMO	34
2. ESCENARIO 2	43
2.1 PREPARAR LOS DISPOSITIVOS.....	46
2.2 CONFIGURACIÓN ROUTER R1	48
2.3 CONFIGURACIÓN S1 Y S2	53

2.4	CONFIGURACIÓN DE LA INFRAESTRUCTURA DE RED	60
2.5	CONFIGURACIÓN DE SOPORTE PARA LOS HOSTS.....	64
2.6	CONFIGURAR LOS EQUIPOS HOST	66
2.7	VERIFICAR LA CONECTIVIDAD DE EXTREMO A EXTREMO.....	67
	CONCLUSIONES.....	92
	LISTA DE REFERENCIA.....	93
	ANEXOS.....	95

LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento IPv4.....	16
Tabla 2. Posición y valor de bits.	16
Tabla 3. Ajustes básicos para R1	20
Tabla 4. Configuración básica para S1.....	27
Tabla 5. Configuración PC - A	33
Tabla 6. Configuración PC - B	33
Tabla 7. Tabla de verificación.	42
Tabla 8. Tabla de VLAN.....	44
Tabla 9. Tabla de asignación de direcciones escenario 2	45
Tabla 10. Configuración red equipo A.....	67
Tabla 11. Configuración red equipo B.....	67
Tabla 12. Conectividad de extremo a extremo.	68

LISTA DE FIGURAS

Figura 1. Topología Escenario 1.....	15
Figura 2. Cuarto octeto de la máscara de subred LAN 1.....	16
Figura 3. Cuarto octeto para la máscara de subred LAN 2.....	17
Figura 4. Ping desde PC-A hacia G/0/0/0.....	34
Figura 5. Ping desde PC - A hacia G0/0/1.....	36
Figura 6. Ping desde PC - A hacia SVI.....	37
Figura 7. Ping desde PC - A hacia PC - B.....	38
Figura 8. Ping desde PC - B hacia G0/0/1.....	39
Figura 9. Ping desde PC - B hacia G/0/0/1.....	40
Figura 10. Ping desde PC - B hacia S1 SVI.....	41
Figura 11. Topología Escenario 2.....	44
Figura 12. Ping desde PC - A hacia G0/0/1.20 por IPv4.....	70
Figura 13. Ping desde PC - A hacia G0/0/1.20 por IPv6.....	71
Figura 14. Ping hacia G0/0/1.30 por IPv4.....	72
Figura 15. Ping desde PC - A hacia G0/0/1.30 por IPv6.....	73
Figura 16. Ping desde PC - A hacia G0/0/1.41 por IPv4.....	74
Figura 17. Ping desde PC - A hacia G0/0/1.40 por IPv6.....	75
Figura 18. Ping desde PC - A hacia VLAN 40 del S1 por IPv4.....	76
Figura 19. Ping desde PC - A hacia VLAN 40 del S2 por IPv4.....	77
Figura 20. Ping desde PC - A hacia PC - B por IPv4.....	78
Figura 21. Ping desde PC - A hacia PC - B por IPv6.....	79
Figura 22. Ping desde PC - A hacia Loopback 0 por IPv4.....	80
Figura 23. Ping desde PC - A hacia Loopback 0 por IPv6.....	81
Figura 24. Ping desde PC - B hacia el Loopback 0 por IPv4.....	82
Figura 25. Ping desde PC - B hacia el Loopback 0 por IPv6.....	83
Figura 26. Ping desde PC - B hacia G0/0/1.20 por IPv4.....	84
Figura 27. Ping desde PC - B hacia G0/0/1.20 por IPv6.....	85
Figura 28. Ping desde PC - B hacia G0/0/1.30 por IPv4.....	86
Figura 29. Ping desde PC - B hacia G0/0/1.30 por IPv6.....	87

Figura 30. Ping desde PC - B hacía G0/0/1.41 por IPv4.....	88
Figura 31. Ping desde PC - B hacía G0/0/1.40 por IPv6.....	89
Figura 32. Ping desde PC - B hacía VLAN 40 del S1	90
Figura 33. Ping desde PC - B hacía VLAN 40 del S2	91

GLOSARIO

CIDR¹: Enrutamiento entre dominios sin clases (Classless Inter-Domain Routing) Hace referencia a una de las grandes mejoras que realizó el IETF para la interpretación de las direcciones IP.

DHCP²: Protocolo de configuración dinámica de host (Dynamic Host Configuration Protocol) Es un protocolo de red del tipo Cliente/Servidor el cual está configurado para asignar de manera dinámica las direcciones IP para la comunicación entre diferentes dispositivos de la red.

MODELO DE PROTOCOLO TCP/IP³: Protocolo para las comunicaciones de Internet el cual describe las funciones que ocurren en cada capa siendo este un modelo de referencia para los diferentes modelos.

MODELO DE REFERENCIA OSI⁴: Amplia lista de funciones y/o servicios que pueden surgir en cada “Capa”, describiendo que proceso debe realizar cada capa sin forzar una metodología en específica.

MULTIDIFUSIÓN⁵: Hace referencia a cuando un único host envía un único paquete a un grupo de host seleccionados que están debidamente configurados al grupo de multidifusión.

PREFIJOS⁶: Creación por parte del CIDR, el cual agrega diferentes prefijos en el supernetting permitiendo la reducción significativamente del número de rutas en los enrutadores.

VLSM⁷: Máscara de subred de tamaño variable (Variable Length Subnet Mask) permite subdividir una subred, es una de las diferentes soluciones que se implementaron para cuando se está llegando al límite de direcciones IP en IPv4.

¹ ARIGANELLO, Ernesto. Redes Cisco (2015)

² BORONAT, Fernando. Funcionamiento del protocolo DHCP (2013)

³ ERASO ERASO, O. Modelos TCP/IP y OSI (2019)

⁴ ERASO ERASO, O. Modelos TCP/IP y OSI (2019)

⁵ GALVÁN B, Implementación de redes IP Multicast (2008)

⁶ ARIGANELLO, Erenesto, Redes Cisco 4ª edición (2016)

⁷ CRESPO, M. R. G., RIVERA, M. I. H., CRUZ, L. O. C., & MÉNDEZ, L. N. H. Ahorrando direcciones IP en la red de datos UJAT. (S.F)

RESUMEN

Se plantean dos escenarios para su desarrollo donde el primer escenario plantea una pequeña red de la cual se debe realizar el direccionamiento aplicando VLSM para dos subredes con sus respectivas direcciones, de igual forma se configura los aspectos básicos de seguridad para cada dispositivo, seguidamente se llevará el control mediante las diferentes tablas y finalmente se valida que la conexión es exitosa por medio del respectivo comando.

Para el segundo escenario se plantea una red pequeña, para la cual se deben de realizar las configuraciones por ambos tipos de conectividad, para uno de estos se utiliza el protocolo DHCP y el restante utiliza un direccionamiento estático, de igual forma algunos dispositivos intermedios son configurados para implementar el modo de enlace troncal utilizando el protocolo de estándar abierto LACP.

Palabras Clave: CISCO, CCNA, Enrutamiento, Switching, Redes.

ABSTRACT

Two scenarios are proposed for its development where the first scenario presents a small network of which the addressing must be done by applying VLSM for two subnets with their respective addresses, likewise the basic security aspects are configured for each device, then the control is carried out through the different tables and finally the connection is validated as successful by means of the respective command.

For the second scenario a small network is proposed, for which the configurations must be made for both types of connectivity, for one of these the DHCP protocol is used and the remaining one uses static addressing, likewise some intermediate devices are configured to implement the trunk link mode using the open standard LACP protocol.

Keywords: CISCO, CCNA, Routing, Swicthing, Networking.

INTRODUCCION

Con la finalidad de aplicar los conocimientos adquiridos mediante el diplomado CCNA se simulan dos diferentes escenarios para el desarrollo de habilidades que están enfocadas en el diseño e implementación para redes LAN/WAN:

Para el primer escenario se plantea una pequeña red que consta de dos subredes, la cual cuenta con dos dispositivos finales, un router y un switch, por lo se a realiza la tabla de direccionamiento con la finalidad de conocer el rango que se tiene disponible entre todos los hosts para cada subred, de igual forma se realiza una configuración a cada dispositivo implementando los protocolos de seguridad.

Para el segundo escenario se plantea una red que consta de tres dispositivos intermedios y dos dispositivos finales, los cuales permiten la conectividad tanto IPv4 como IPv6, ambos dispositivos intermedios tendrán configurado diferentes protocolos de seguridad al igual que en el escenario 1, sus respectivas VLAN según la tabla 8, se implementa el protocolo de configuración de host dinámico (DHCP), se realiza los enlaces troncales para la comunicación interna entre las VLANS aplicando el estándar IEEE 802.1Q o dot1Q para las redes virtuales, finalmente se verifica la conectividad mediante el comando ping.

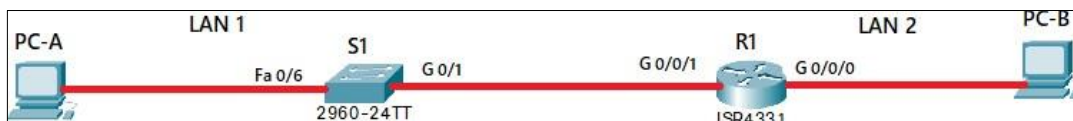
DESARROLLO

1. Escenario 1

Para el primer escenario que se plantea, está conformado por un router, un switch y dos equipos, tal como se muestra en la figura 1 presentando el diseño de una red de tamaño pequeño, por lo que es se debe diseñar un esquema de direccionamiento IPv4 basado en el protocolo VLSM para maximizar la eficiencia al momento de realizar el direccionamiento tal como se muestra la tabla 1, siendo un requisito tener dos subredes con nombre LAN 1 y LAN 2.

Para LAN 1 el requisito es de 60 Host mientras que para LAN 2 es de 20 Host, de igual forma se implementan protocolos básicos de seguridad para el router y el switch.

Figura 1. Topología Escenario 1.



Fuente: Prueba de habilidades práctica CCNA – 2022.

Dando cumplimiento a las siguientes indicaciones:

La dirección de red debe ser *172.71.3.0*

Para R1, la dirección IP para la interfaz G0/0/1 es la última dirección de host de la subred LAN 1, mientras que para la interfaz G0/0/0 es la última dirección de host de la subred LAN 2.

Para el SVI del Switch S1 su dirección de host es la segunda disponible de la subred LAN 1.

Para el PC-A se asigna la décima dirección de host de la subred LAN 1.

Para el PC-B se asigna la décima dirección de host de la subred LAN 2.

1.1 DIRECCIONAMIENTO

Tabla 1. Tabla de direccionamiento IPv4.

Nombre	Dirección de red	Mascara de subred	Primera IP utilizable	Ultima IP utilizable	Dirección de broadcast
LAN 1	172.71.3.0/26	255.255.255.192	172.71.3.1	172.71.3.62	172.71.3.63
LAN 2	172.71.3.64/27	255.255.255.224	172.71.3.65	172.71.3.94	172.71.3.95

Fuente: Autoría propia.

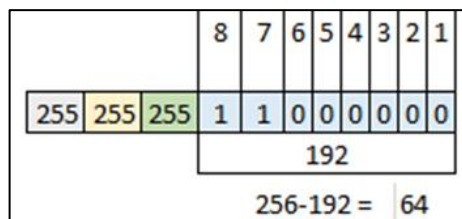
La dirección IP asignada es 172.71.3.0 por lo que está ubicada dentro del rango de 128.0.0.0 hasta 191.255.255.255 indicando que es una dirección de clase B, el requerimiento para LAN 1 es de 60 Hosts e implementando el protocolo VLSM se observa que el número de host para que cumple con este requisito es de 64 como se observa en la tabla 2, indicando que para el ultimo octeto es necesario dejar seis ceros como se muestra en la figura 2 con la finalidad de conocer la máscara de subred para LAN 1.

Tabla 2. Posición y valor de bits.

Posición	7	6	5	4	3	2	1	0
Valor	128	64	32	16	8	4	2	1

Fuente: Autoría propia

Figura 2. Cuarto octeto de la máscara de subred LAN 1



Fuente: Autoría propia

Sabiendo que cada bit cuenta con un valor diferente como se indica en la tabla 2, se suma los bits que quedaron con un valor de uno, por lo que $128 + 64 = 192$, identificando la dirección de la máscara de subred siendo 255.255.255.192, de los cuatro octetos, se cuenta con 26 bits con valor de 1, por lo que el prefijo es de /26, finalmente para conocer la siguiente dirección de red se resta el valor de la máscara de subred que es de 192 con 256 siendo este último un valor proporcionado por el protocolo, por lo que $256 - 192 = 64$ indicando que la siguiente dirección de red es 172.71.3.64.

Finalmente con la siguiente dirección de red, se procede a restarle 1 al valor encontrado, esto es reservado para la dirección de broadcast por lo que para la subred "LAN 1" de 60 host que fueron solicitados se tienen disponibles 64, el prefijo de la red es /26, la máscara de red es 255.255.255.192, la primera dirección IP utilizable es de 172.71.3.1, la dirección de broadcast es 172.71.3.63 por lo que la última dirección IP disponible es de 172.71.3.62 tal como se registra en la tabla 1.

Continuando con la subred "LAN 2" se solicitan 20 host, revisando la tabla 2 se observa que el número de host que cumple con este requisito es de 32 indicando que para el último octeto es necesario dejar cinco ceros como se muestra en la figura 3.

Figura 3. Cuarto octeto para la máscara de subred LAN 2

				8	7	6	5	4	3	2	1
255	255	255	1	1	1	0	0	0	0	0	0
			224								

Fuente: Autoría propia.

De igual forma cada bit cuenta con un valor diferente como se indica en la tabla 2, se suma los bits que quedaron con un valor de uno por lo que $128 + 64 + 32 = 224$ identificando la dirección de la máscara de subred 255.255.255.224, de los cuatro octetos, se cuenta con 27 bits con valor de 1, por lo que el prefijo es de /27, finalmente para conocer la siguiente dirección de red se resta el valor de la anterior máscara de subred que es de 192 (LAN 1) con el valor encontrado que es 32 (LAN 2) por lo que $192 - 32 = 96$ indicando que la siguiente dirección de red es 172.71.3.96.

Finalmente con la siguiente dirección de red, se procede a restarle 1 al valor encontrado, esto es reservado para la dirección de broadcast por lo que para la subred "LAN 2" de 30 host que fueron solicitados se tienen disponibles 32, el prefijo de la red es /27, la máscara de red es 255.255.255.224, la primera dirección IP utilizable es de 172.71.3.65, la dirección de broadcast es 172.71.3.95 por lo que la última dirección IP disponible es de 172.71.3.94 tal como se registra en la tabla 1.

Una vez completado el direccionamiento por VLSM se procede a realizar la configuración básica de los dispositivos intermediarios.

Para configurar las interfaces de R1 y S1 se utilizan las siguientes líneas de comando:

```
1.2ROUTER "R1"
```

```
Router>enable
```

```
Router#
```

```
Router#configure terminal
```

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

```
Router(config)#interface GigabitEthernet0/0/1
```

```
Router(config-if)#ip address 172.71.3.62 255.255.255.192
```

```
Router(config)#interface GigabitEthernet0/0/0
```

```
Router(config-if)#ip address 172.71.3.94 255.255.255.224
```

```
Router(config-if)#
```

1.3 SWITCH "S1"

Switch#config terminal

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

Switch(config)#interface vlan 1

Switch(config-if)#no shutdown

Switch(config-if)#exit

Switch(config)#vlan 1

Switch(config-if)#ip address 172.71.3.2 255.255.255.192

Switch(config-if)#exit

1.4 CONFIGURACIÓN BÁSICA ROUTER "R1"

Inicialmente se desactiva la búsqueda por DNS por diferentes razones siendo una de esas que no se implementará ningún servidor de este tipo, sumado a que si se llega a ingresar un comando con algún error, por configuración del dispositivo este genera una búsqueda por DNS procediendo a bloquear el teclado y generando un incremento de tiempo a la hora de configurar por lo que se procede a desactivar de forma manual.

A continuación se asigna el nombre del router como *R1*, su nombre de dominio como *ccna-sa.com*, en el apartado de seguridad se asigna una contraseña para el modo EXEC privilegiado ya que en este modo se tiene acceso a todos los comandos disponibles para el Router, de igual forma se asigna una contraseña diferente para el acceso a la consola del Router, estas contraseñas serán diferentes para cumplir con el estándar de seguridad mínimo, en caso de que se fueran a agregar más usuarios a futuro, mediante el modo privilegiado se configura que las contraseñas contarán con un mínimo de 10 caracteres, sin embargo se crea un usuario con permisos administrativos en la base de datos local siendo el nombre de usuario *admin* y su contraseña *admin1pass*, una vez configurada las contraseñas se proceden a cifrar de manera local y se genera una clave de cifrado RSA que es utilizada para intercambiar mensajes cifrados sin una clave privada.

Todo esto con la finalidad de que terceros no accedan a esta información, por esta misma razón se procede a dejar una advertencia en la consola del router indicando que el acceso es restringido a personal no autorizado sin embargo por temas del ejercicio se dejará un mensaje con la información del administrador.

De igual forma para el conjunto de puertos virtuales, se configura que únicamente acepten conexiones vía SSH, que es uno de los protocolos más seguros para el acceso remoto.

Finalmente ya se puede iniciar a configurar las diferentes interfaces del Router activando la interfaz G0/0/0, por la cual se establece una descripción y su dirección IPv4 que para el ejercicio dicha dirección IP es la última disponible de LAN 2, de igual forma para la interfaz G0/0/1 únicamente cambiando la dirección IPv4 siendo está la última disponible de LAN 1, que dichos valores son encontrados en la tabla 1.

Lo anterior se realiza con las siguientes líneas de comando:

Tabla 3. Ajustes básicos para R1

Tarea	Especificación	Comando
Desactivar la búsqueda DNS		Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	R1	Router#configure terminal Router(config)#hostname R1
Nombre de dominio	ccna-sa.com	R1(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass	R1(config)#enable password ciscoenpass

Contraseña de acceso a la consola	ciscoconpass	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	10 caracteres	R1(config)#security password min-length 10
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Contraseña: admin1pass	R1(config)#username admin password admin1pass
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)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH		R1(config)#ip ssh version 2 *Mar 1 0:8:2.692: %SSH-5-ENABLED: SSH 1.99 has been enabled R1(config)#line vty 0 15 R1(config-line)#transport input ssh R1(config-line)#login local
Cifrar las		R1(config)#service password-encryption

contraseñas de texto no cifrado		
Configurar un banner MOTD	Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.	<pre>R1(config)#banner motd # Enter TEXT message. End with the character '#'. Nombre Dispositivo: R1 Nombre Estudiante: Ricardo Agredo Trujillo Programa Academico: Ingenieria de Sistemas #</pre>
Configuración de interface G0/0/0	<p>Establecer la descripción</p> <p>Establecer la dirección IPv4</p> <p>Activar la interfaz.</p>	<pre>R1(config)#interface gigabitEthernet 0/0/0 R1(config-if)#description Interfaz 0/0/0 Router(config-if)#ip address 172.71.3.94 255.255.255.224</pre>
Configuración de interface G0/0/1	<p>Establecer la descripción</p> <p>Establecer la dirección IPv4</p> <p>Activar la interfaz.</p>	<pre>R1(config-if)#interface gigabitEthernet 0/0/1 R1(config-if)#description interfaz 0/0/1 Router(config-if)#ip address 172.71.3.62 255.255.255.192</pre>
Generar una clave de cifrado RSA	Módulo de 1024 bits	<pre>R1(config)#crypto key generate rsa The name for the keys will be: R1.ccna- sa.com How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]</pre>

Fuente: Autoría Propia.

Se explican los comandos utilizados anteriormente con su comentario correspondiente:

```
Router>enable
```

```
//Se activa el modo EXEC.
```

```
Router#configure terminal
```

```
//Se configura la terminal.
```

```
Router(config)#no ip domain-lookup
```

```
//Se desactiva la búsqueda DNS.
```

```
Router#configure terminal
```

```
//Se configura la terminal.
```

```
Router(config)#hostname R1
```

```
//Se cambia el nombre del HOST a R1.
```

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

```
//Se cambia el nombre del Dominio.
```

```
R1(config)#enable password ciscoenpass
```

```
//Se activa la contraseña para el modo EXEC.
```

```
R1(config)#line console 0
```

```
//Se configura la Línea 0 de la consola.
```

```
R1(config-line)#password ciscoconpass
```

```
//Se configura la contraseña para el acceso a consola.
```

R1(config-line)#login

//Se configura que la consola requiera validar la contraseña.

R1(config)#security password min-length 10

//Se establece la longitud mínima de caracteres a 10.

R1(config)#username admin privilege 15 password admin1pass

//Se crea un usuario y contraseña de nivel 15.

R1(config)#line vty 0 4

//Se accede a las líneas VTY 0 4.

R1(config-line)#login local

//Se activa la verificación del login de manera local.

R1(config)#ip ssh version 2

//Se activa el protocolo SSH Versión 2 (Es necesario antes crear una clave RSA).

R1(config)#line vty 0 15

//Se accede a las líneas VTY 0 15.

R1(config-line)#transport input ssh

//Se activa la conexión SSH únicamente.

R1(config-line)#login local

//Se validan las credenciales de manera local.

R1(config)#service password-encryption

//Se activa el cifrado de contraseñas.


```
R1(config)#banner motd #  
//Mensaje para la consola, Se finaliza con #.
```

```
R1(config)#interface gigabitEthernet 0/0/0  
//Se accede a la interfaz G0/0/0.
```

```
R1(config-if)#description Interfaz 0/0/0  
//Se da una descripción.
```

```
Router(config-if)#ip address 172.71.3.94 255.255.255.224  
//Se configura la IP y SubNet Mask.
```

```
R1(config-if)#interface gigabitEthernet 0/0/1  
//Se accede a la interfaz G0/0/1.
```

```
R1(config-if)#description interfaz 0/0/1  
//Se da una descripción.
```

```
Router(config-if)#ip address 172.71.3.62 255.255.255.192  
//Se configura la IP y SubNet Mask.
```

```
R1(config)#crypto key generate rsa  
//Se configura una clave de cifrado RSA
```

The name for the keys will be: **R1.ccna-sa.com** Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys.

Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: **1024**

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

1.5 CONFIGURACIÓN BÁSICA SWITCH “S1”

De igual forma se desactiva la búsqueda por DNS, a continuación se asigna el nombre del switch como *S1*, su nombre de dominio como *ccna-sa.com*, en el apartado de seguridad se asigna una contraseña para el modo EXEC privilegiado, de igual forma se asigna una contraseña diferente para el acceso a la consola del Router, se apaga todos los puertos que no se utilizan para aumentar la seguridad del dispositivo intermediario, estos puertos son F0/1 al F0/4, F0/7 al F0/24 y G0/2, también se crea un usuario con permisos administrativos en la base de datos local siendo el nombre de usuario *admin* y su contraseña *admin1pass*, una vez configurada las contraseñas se proceden a cifrar de manera local y se genera una clave de cifrado RSA que es utilizada para intercambiar mensajes cifrados sin una clave privada.

Todo esto con la finalidad de que terceros no accedan a esta información, por esta misma razón se procede a dejar una advertencia en la consola del router indicando que el acceso es restringido a personal no autorizado, sin embargo por temas del ejercicio se dejará un mensaje con la información del administrador.

De igual forma para el conjunto de puertos virtuales, se configura que únicamente acepten conexiones vía SSH, que es uno de los protocolos más seguros para el acceso remoto.

Finalmente se procede a configurar la interfaz de administración SVI en la VLAN1, la cual cuenta con su respectiva descripción y su dirección IPv4.

Lo anterior se realiza con las siguientes líneas de comando

Tabla 4. Configuración básica para S1.

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

Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Contraseña: admin1pass	S1(config)#username admin privilege 15 password admin1pass
Configure el inicio de sesión en las líneas VTY para que use la base de datos local		S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH		S1(config)#ip ssh version 2 *Mar 1 0:8:2.692: %SSH-5-ENABLED: SSH 1.99 has been enabled S1(config)#line vty 0 15 S1(config-line)#transport input ssh S1(config-line)#login local
Cifrar las contraseñas de texto no cifrado		S1(config)#service password-encryption
Configurar un banner MOTD	Debe contener el nombre del dispositivo, el	S1(config)#banner motd # Enter TEXT message. End with the character '#'. #

	nombre completo del estudiante y el programa académico al que pertenece.	Nombre Dispositivo: S1 Nombre Estudiante: Ricardo Agredo Trujillo Programa Academico: Ingenieria de Sistemas #
Generar una clave de cifrado RSA	Módulo de 1024 bits	S1(config)#crypto key generate rsa The name for the keys will be: S1.ccna-sa.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Configure la interfaz de administración (SVI) en VLAN1	Establecer la descripción Establecer la dirección IPv4	S1(config-if)#description Interfaz de Administracion VLAN 1 Rkt S1(Config-if)#ip address 172.71.3.2 255.255.255.192

Fuente: Autoría propia.

Se explican los comandos utilizados anteriormente con su comentario correspondiente:

Switch>enable

//Se activa el modo EXEC.

Switch#configure terminal

//Se configura la terminal.

Switch(config)#no ip domain-lookup
//Se desactiva la búsqueda DNS.

Switch#configure terminal
//Se configura la terminal.

Switch(config)#hostname S1
//Se cambia el nombre del HOST a S1.

S1(config)#ip domain-name ccna-sa.com
//Se cambia el nombre del Dominio.

S1(config)#enable password ciscoenpass
//Se activa la contraseña para el modo Enable.

S1(config)#line console 0
//Se configura la Línea 0 de la consola.

S1(config-line)#password ciscoconpass
//Se configura la contraseña para la consola.

S1(config-line)#login
//Se configura que la consola requiera login.

S1(config)#interface range f0/1-4
//Se selecciona la interfaz FA0/1 hasta F0/4.

S1(config-if)#shut
//Se apaga el puerto.

S1(config)#interface range G0/2

//Se selecciona la interfaz G0/2.

S1(config-if)#shut

//Se apaga el puerto.

S1(config)#interface range f0/7-24

//Se selecciona la interfaz F0/7 hasta F0/24.

S1(config-if-range)#shut

//Se apaga la Interfaz.

S1(config)#username admin privilege 15 password admin1pass

//Se crea un usuario y contraseña con privilegio 15.

S1(config)#line vty 0 4

//Se accede a las líneas VTY 0 4.

S1(config-line)#login local

//Se activa el login de manera local.

S1(config)#ip ssh version 2

//Se activa el protocolo SSH Versión 2.

S1(config)#line vty 0 15

//Se accede a las líneas VTY 0 15.

S1(config-line)#transport input ssh

//Se activa la conexión SSH únicamente.

S1(config-line)#login local
//Se validan las credenciales de manera local.

S1(config)#service password-encryption
//Se activa el cifrado de contraseñas.

S1(config)#banner motd #
//Se inicia un mensaje para la consola, Se finaliza con #.

S1(config)#crypto key generate rsa
//Se configura una clave de cifrado RSA.

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

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys.

Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: **1024**

//Se ingresa el rango de Bits.

% Generating **1024** bit RSA keys, keys will be non-exportable...[OK]

S1(config-if)#description Interfaz de Administracion VLAN 1 Rkt
//Se da una descripción a la interfaz Vlan1

S1(Config-if)#ip address 172.71.3.2 255.255.255.128
//Se asigna la IP y la SubNet Mask.

S1(Config)#ip default-gateway 172.71.3.255
//Se asigna el Gateway por defecto.

1.6 CONFIGURACIÓN DE LOS DISPOSITIVOS FINALES PC – A Y PC - B

Una vez realizada la configuración de los dispositivos intermedios se continua con la configuración de los equipos host PC-A y PC-B cuya información se plasma en la tabla 5, en la cual se registra las configuraciones de red del host proporcionadas con el comando ipconfig /all.

Tabla 5. Configuración PC - A

Configuración de red de PC- A	
Descripción	Equipo de Cómputo ubicado en la LAN 1
Dirección física	0060.3E19.2AC7
Dirección IPv4	172.71.3.10
Máscara de subred	255.255.255.192
Puerta de enlace IPv4 Predeterminada	172.71.3.63

Fuente: Autoría propia.

Tabla 6. Configuración PC - B

Configuración de red de PC- B	
Descripción	Equipo de Cómputo ubicado en la LAN 2
Dirección física	0001.4294.5124
Dirección IPv4	172.71.3.75
Máscara de subred	255.255.255.224
Puerta de enlace IPv4 Predeterminada	172.71.3.95

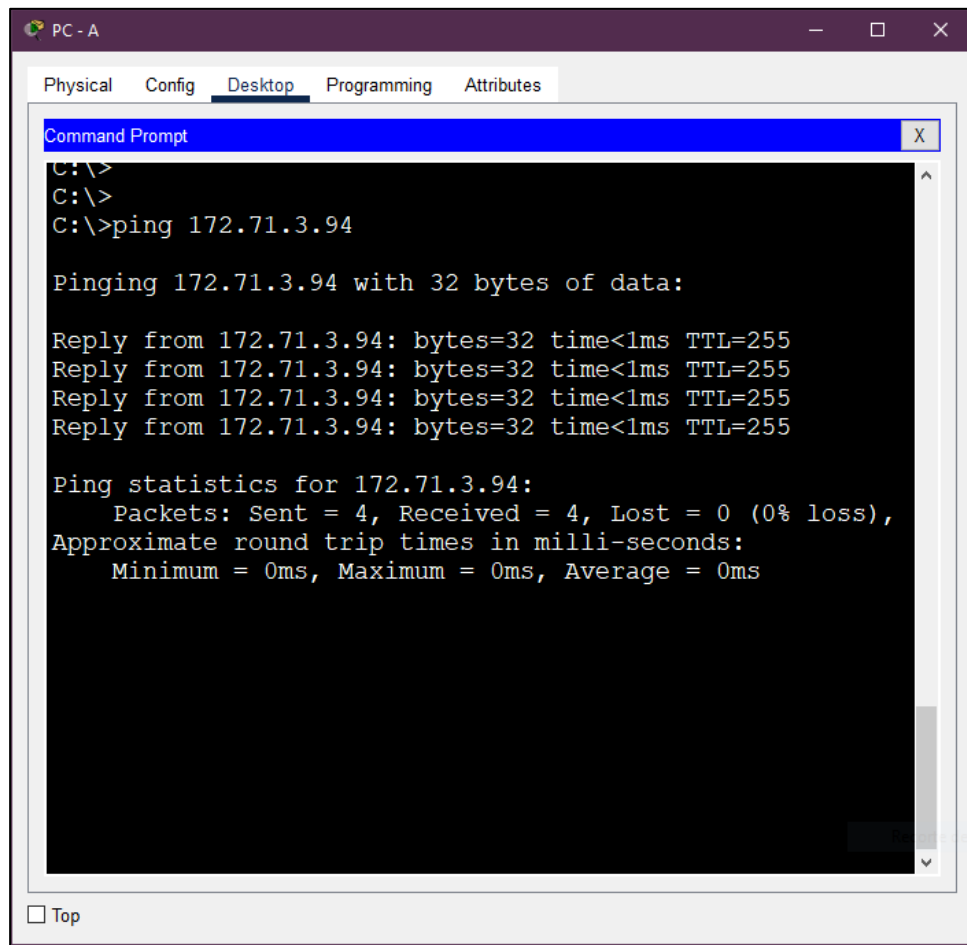
Fuente: Autoría propia.

Ambos dispositivos se configuran desde la pestaña Desktop > Configuración de IP.

1.7 PRUEBA CONECTIVIDAD EXTREMO A EXTREMO

Se utiliza el comando ping para probar la conectividad entre todos los dispositivos de red, este comando lo que hace es enviar un mensaje ICMP Echo Request o un mensaje de solicitud de eco, por lo que si este mensaje llega al Host nos reenvía un ICMP Echo Replay o mensaje de respuesta de eco, indicando que existe la conexión entre nuestro host y el host de destino incluso mostrando el tiempo de respuesta en milisegundos que tarda en viajar el paquete de datos, dado el caso en que el host de destino no envíe un ICMP Echo Replay se puede interpretar que existe un fallo hacia el host.

Figura 4. Ping desde PC-A hacia G/0/0/0



```
PC - A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>ping 172.71.3.94

Pinging 172.71.3.94 with 32 bytes of data:

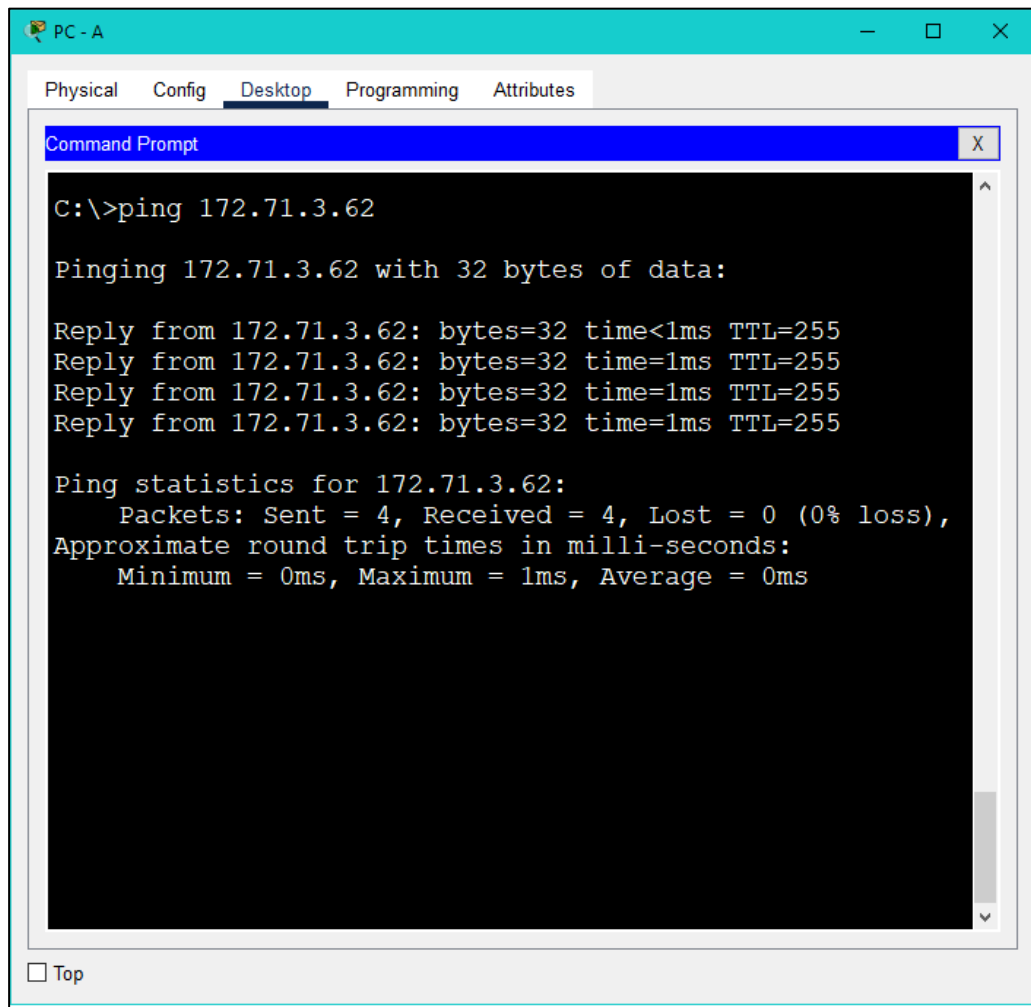
Reply from 172.71.3.94: bytes=32 time<1ms TTL=255
Reply from 172.71.3.94: bytes=32 time<1ms TTL=255
Reply from 172.71.3.94: bytes=32 time<1ms TTL=255
Reply from 172.71.3.94: bytes=32 time<1ms TTL=255

Ping statistics for 172.71.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autoría propia.

Al ejecutar el comando ping hacia la dirección 172.71.3.94 que según la tabla 7, corresponde a la interfaz G0/0/0 perteneciente a R1, los resultados del ping de la figura 4 nos indica que los 4 paquetes fueron enviados y recibidos de manera exitosa indicando que la puerta de enlace es correcta permitiendo el tráfico de datos por S1 que es de una subred diferente y finalmente llegando a su destino el cual contesta el protocolo ICMP indicando que la conexión es exitosa.

Figura 5. Ping desde PC - A hacia G0/0/1



```
C:\>ping 172.71.3.62

Pinging 172.71.3.62 with 32 bytes of data:

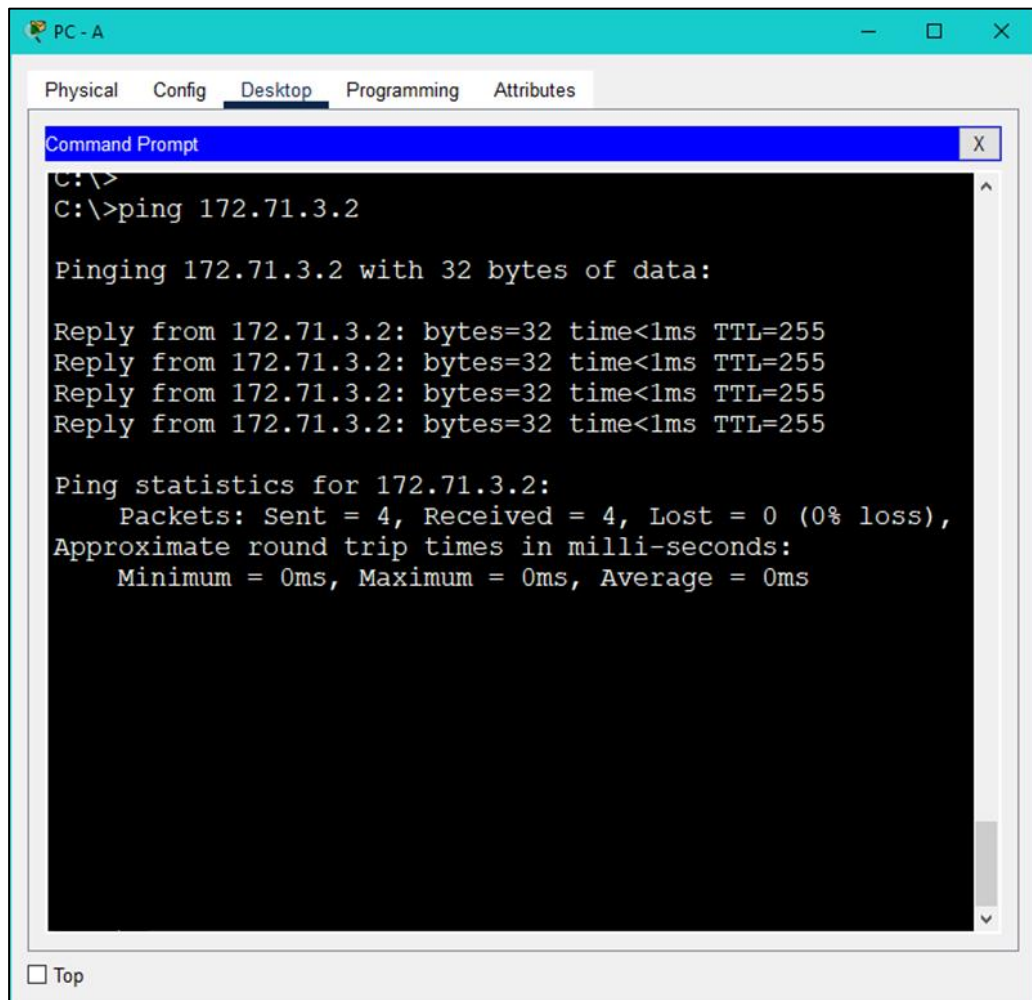
Reply from 172.71.3.62: bytes=32 time<1ms TTL=255
Reply from 172.71.3.62: bytes=32 time=1ms TTL=255
Reply from 172.71.3.62: bytes=32 time=1ms TTL=255
Reply from 172.71.3.62: bytes=32 time=1ms TTL=255

Ping statistics for 172.71.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Fuente: Autoría propia.

Continuando con la figura 5 se observa que la conexión entre el host y la dirección de destino 172.71.3.62 que según la tabla 7 pertenece a la interfaz G/0/0/1 de R1 es exitosa y no existe ninguna pérdida de datos.

Figura 6. Ping desde PC - A hacia SVI.



```
PC - A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>ping 172.71.3.2

Pinging 172.71.3.2 with 32 bytes of data:

Reply from 172.71.3.2: bytes=32 time<1ms TTL=255
Reply from 172.71.3.2: bytes=32 time<1ms TTL=255
Reply from 172.71.3.2: bytes=32 time<1ms TTL=255
Reply from 172.71.3.2: bytes=32 time<1ms TTL=255

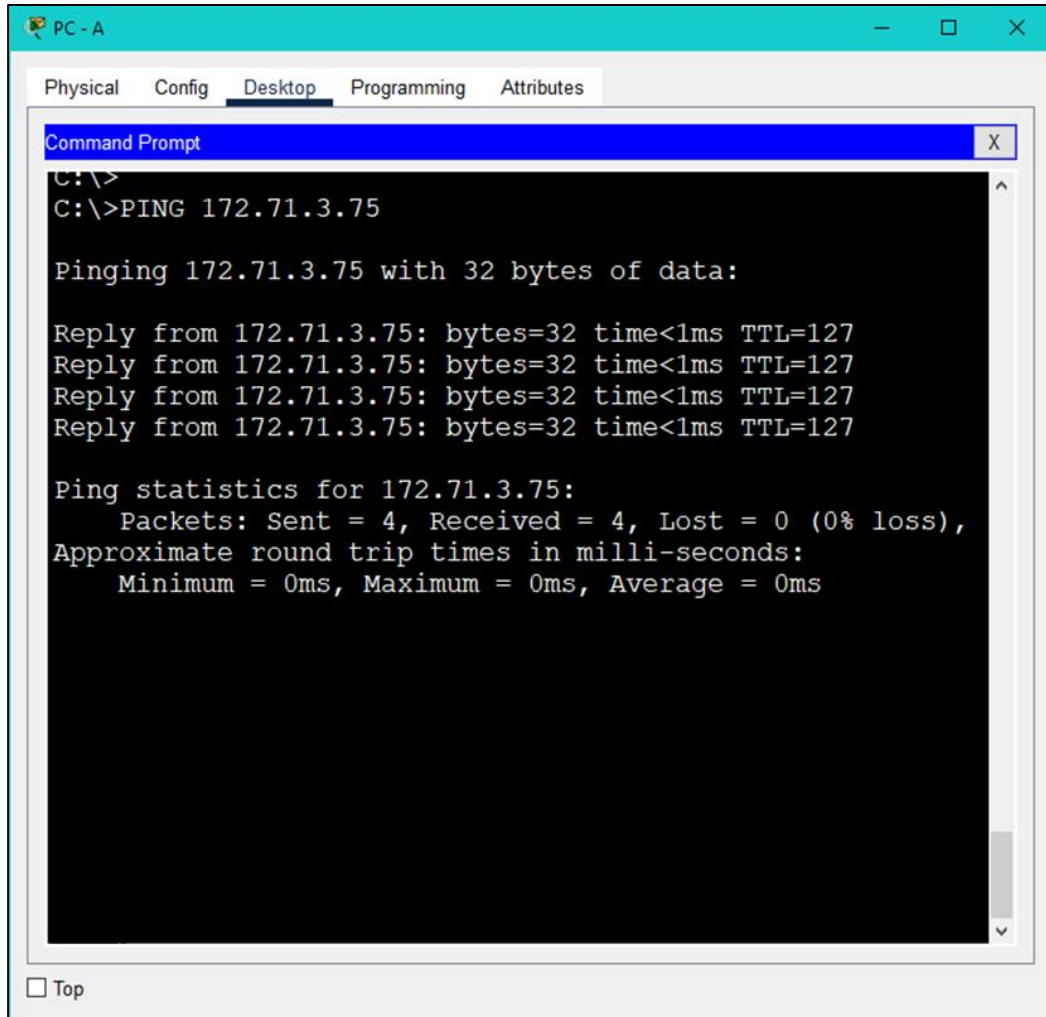
Ping statistics for 172.71.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

 Top
```

Fuente: Autoría propia.

De la figura 6 se puede observar que para este caso tanto el Host como el destino pertenecen a la misma subred visualmente se identifica por la IP indicando que la conexión entre estos dos dispositivos es correcta.

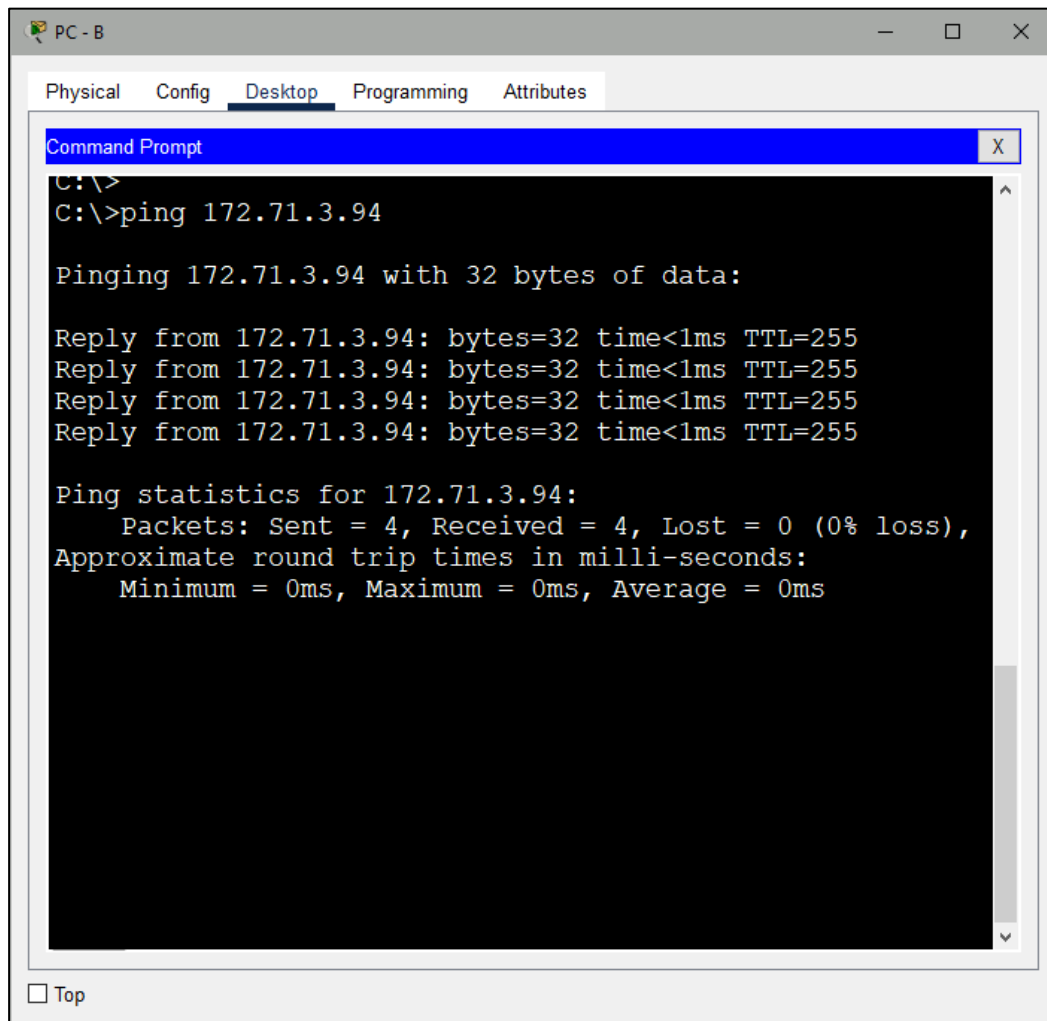
Figura 7. Ping desde PC - A hacia PC - B.



Fuente: Autoría propia.

Finalmente se realiza el ping entre los dos dispositivos finales, los cuales están en dos subredes diferentes, indicando que existe un tráfico correcto entre el PC - A, S1, R1 y finalizando en PC - B el cual replica el mensaje proveniente desde PC - A como se observa en la figura 7.

Figura 8. Ping desde PC - B hacia G0/0/1



```
PC - B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>ping 172.71.3.94

Pinging 172.71.3.94 with 32 bytes of data:

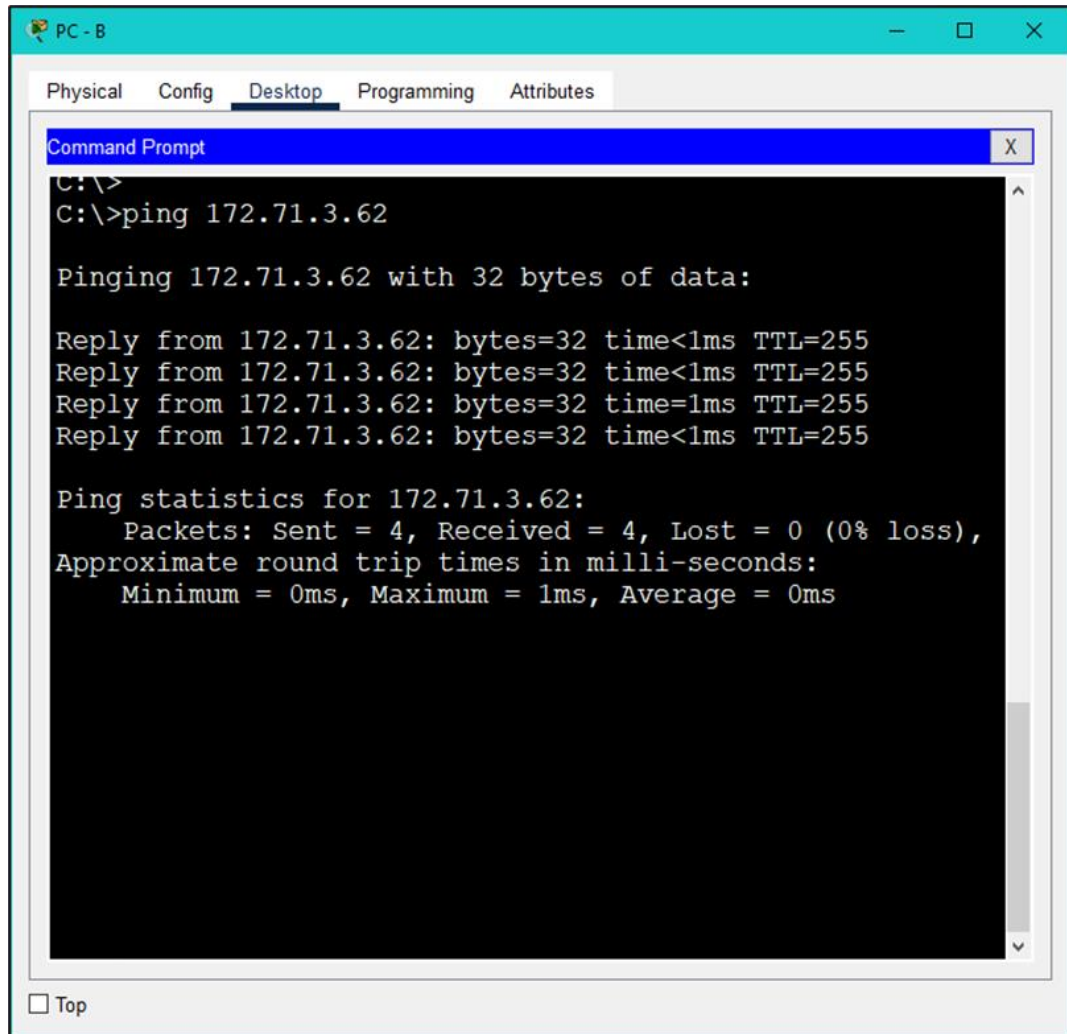
Reply from 172.71.3.94: bytes=32 time<1ms TTL=255
Reply from 172.71.3.94: bytes=32 time<1ms TTL=255
Reply from 172.71.3.94: bytes=32 time<1ms TTL=255
Reply from 172.71.3.94: bytes=32 time<1ms TTL=255

Ping statistics for 172.71.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autoría propia.

Para este caso ambos dispositivos pertenecen a la misma subred y por medio del comando ping se verifica que dicha conexión es estable, por lo que existe conexión entre el PC – B y G0/0/0 tal como lo muestra la figura 8.

Figura 9. Ping desde PC - B hacia G/0/0/1



```
PC - B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>ping 172.71.3.62

Pinging 172.71.3.62 with 32 bytes of data:

Reply from 172.71.3.62: bytes=32 time<1ms TTL=255
Reply from 172.71.3.62: bytes=32 time<1ms TTL=255
Reply from 172.71.3.62: bytes=32 time=1ms TTL=255
Reply from 172.71.3.62: bytes=32 time<1ms TTL=255

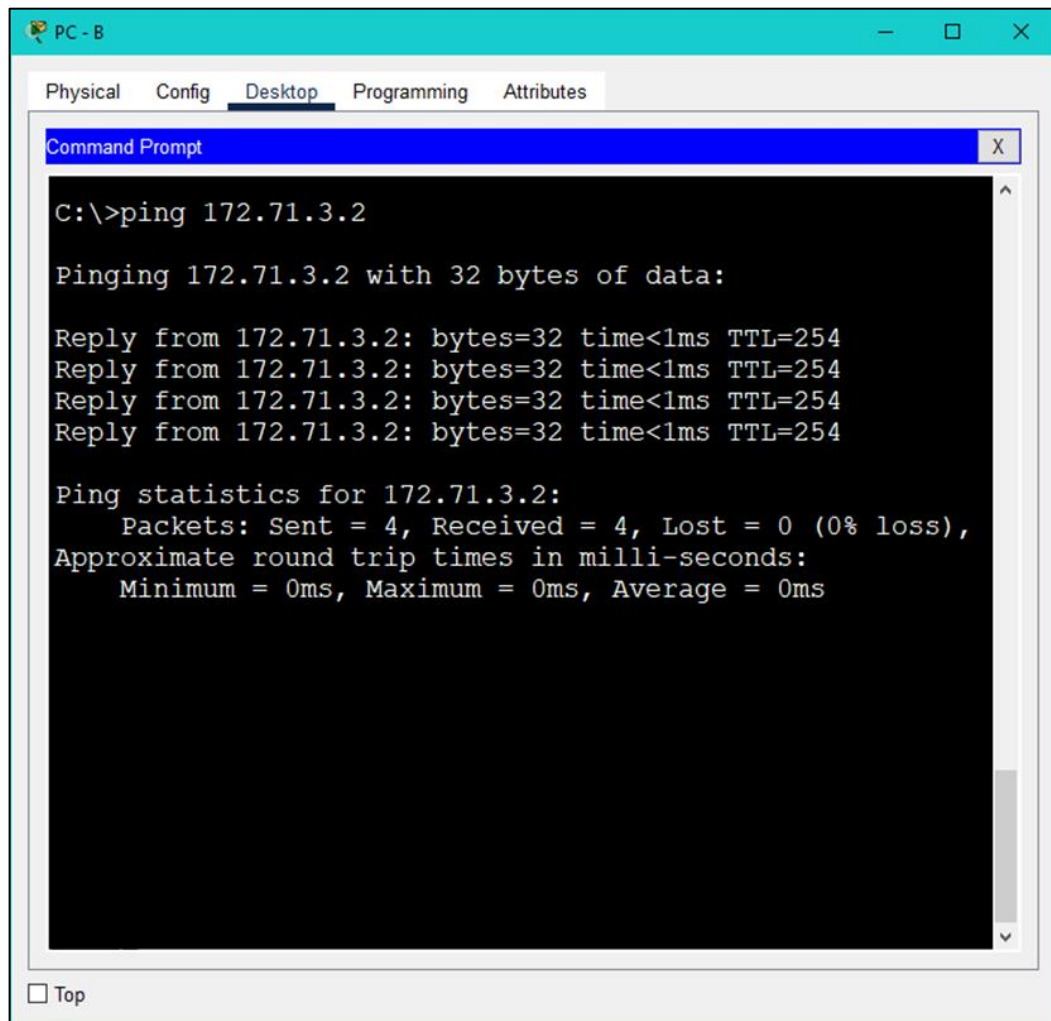
Ping statistics for 172.71.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

 Top
```

Fuente: Autoría propia.

De igual forma que en el caso anterior y como se observa en la figura 9 ambos dispositivos pertenecen a la misma subred y por medio del comando ping se verifica que dicha conexión es estable, por lo que existe conexión entre el PC – B y G0/0/1.

Figura 10. Ping desde PC - B hacia S1 SVL.



```
PC - B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.71.3.2

Pinging 172.71.3.2 with 32 bytes of data:

Reply from 172.71.3.2: bytes=32 time<1ms TTL=254
Reply from 172.71.3.2: bytes=32 time<1ms TTL=254
Reply from 172.71.3.2: bytes=32 time<1ms TTL=254
Reply from 172.71.3.2: bytes=32 time<1ms TTL=254

Ping statistics for 172.71.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autoría propia.

Finalmente se realiza el ping al último dispositivo por comprobar que para este caso es una VLAN perteneciente a S1, como se observa en la figura 10 dicha conexión es exitosa.

Se utiliza la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de la red.

Tabla 7. Tabla de verificación.

Desde	A	Dirección IP	Resultados de ping
PC-A	R1 G0/0/0	172.71.3.94	✓
	R1 G0/0/1	172.71.3.62	✓
	S1 VLAN 1	172.71.3.2	✓
	PC-B	172.71.3.75	✓
PC-B	R1 G0/0/0	172.71.3.94	✓
	R1 G0/0/1	172.71.3.62	✓
	S1 VLAN1	172.71.3.2	✓

Fuente: Autoría propia.

De la tabla 7 se puede concluir que efectivamente la red quedo dividida conforme las especificaciones, igual mente la conexión entre los diferentes dispositivos fue exitosa, por lo que la implementación es correcta.

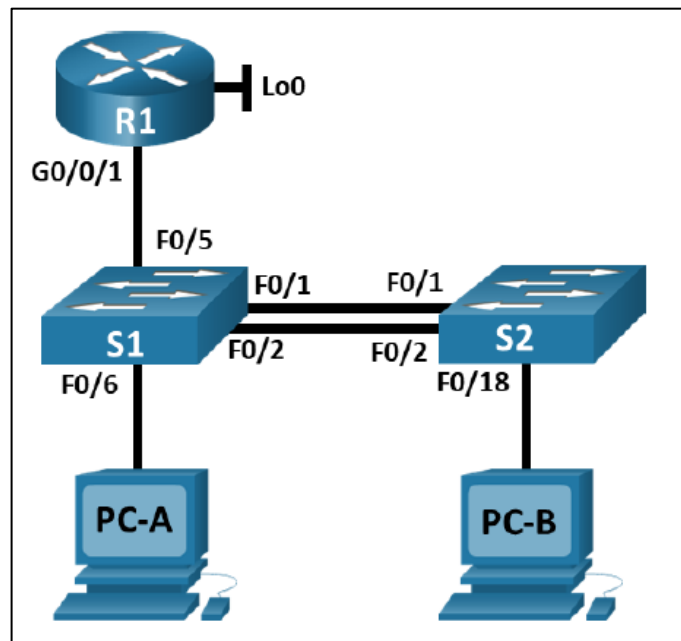
2. ESCENARIO 2

El segundo escenario plantea, una configuración de diferentes dispositivos conformados para una red pequeña, entre los cuales está conformado por tres dispositivos intermedios que son un router, dos switches y dos dispositivos finales que son dos computadores, se realiza el diseño tal como se plantea en la figura 11, estos dispositivos deben de admitir las diferentes conectividades IPv4 como IPv6 como se muestra en la tabla 8, cumpliendo de igual forma los diferentes protocolos de seguridad para asegurar el enrutamiento entre las diferentes VLAN que son proporcionadas en la tabla 8, activar el grupo de DHCP para las VLAN correspondientes indicando un grupo exacto de direcciones IPv4, de igual forma se configura el EtherChannel que es una tecnología desarrollada por Cisco, la cual permite la agrupación de puertos Fa/E y puertos Gi/E que son puertos lógicos en un puerto virtual denominado PortChannel.

Para implementar el EtherChannel se cuenta con dos protocolos de negociación tanto el PAgP como el LACP siendo éste último de estándar abierto mientras que PAgP es exclusivo de Cisco, por lo que se implementa el protocolo de negociación LACP ya que es basado en IEEE implementándose a nivel mundial en mayor medida.

Finalmente se pone en marcha una seguridad de Capa 2 que según el modelo de Capa OSI - TCP/IP autoriza únicamente las direcciones MAC que se hayan establecido para que estas tengan acceso de comunicación por medio del puerto lógico del dispositivo intermedio dicha seguridad se implementara por medio del uso del comando Port-security.

Figura 11. Topología Escenario 2



Fuente: Prueba de habilidades práctica CCNA – 2022

Tabla 8. Tabla de VLAN.

VLAN	NOMBRE DE LA VLAN
20	Docentes
30	Estudiantes
40	Invitados
50	Usuarios
56	Native

Tabla 9. Tabla de asignación de direcciones escenario 2

Dispositivo/Interfaz	Dirección IP / Prefijo	Default Gateway
R1 G0/0/1.20 Docentes	10.71.8.1/26	No corresponde
	2001:db8:acad:a::1/64	No corresponde
R1 G0/0/1.30 Estudiantes	10.71.8.65 /27	No corresponde
	2001:db8:acad:b::1/64	No corresponde
R1 G0/0/1.40 Invitados	10.71.8.97 /29	No corresponde
	2001:db8:acad:c::1/64	No corresponde
R1 G0/0/1.56 Native	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209::1/64	No corresponde
S1 VLAN 40	10.71.8.98/29	10.71.8.97
	2001:db8:acad:c: :98/64	No corresponde
	fe80::98	No corresponde
S2 VLAN 40	10.71.8.99/29	10.71.8.97
	2001:db8:acad:c: :99/64	No corresponde
	fe80::99	No corresponde
PC-A NIC	Dirección DHCP IPv4 2001:db8:acad:a::50/64	DHCP para puerta de enlace predeterminada IPv4 fe80::1
PC-B NIC	Dirección DHCP IPv4 2001:db8:acad:b::50/64	DHCP para puerta de enlace predeterminada IPv4 Fe80::1

Fuente: Prueba de habilidades práctica CCNA – 2022

2.1 Preparar los dispositivos

Inicialmente se va a configurar los aspectos básicos de los dispositivos intermedios, así que se procede a borrar las configuraciones que traen los dispositivos por defecto, incluyendo las VLAN del router y del switch, con el propósito de eliminar cualquier configuración previa que entorpezca los nuevos ajustes.

Para los dispositivos "Switch" será necesario habilitar el soporte de conectividad IPv6 por lo que ambos deben aplicarse correctamente y dando a lugar su recargar la configuración para conservar los cambios que aplicaron, todo lo anterior se realiza con la siguiente línea de comando:

ROUTER

```
Router>en
```

```
Router#erase startup-config
```

```
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
```

```
[OK]
```

```
Erase of nvram: complete
```

```
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

```
Router#reload
```

```
Proceed with reload? [confirm]
```

```
Initializing Hardware ...
```

```
System integrity status: 00000610
```

```
Rom image verified correctly
```

```
--- System Configuration Dialog ---
```

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

```
Press RETURN to get started!
```

SWITCH S1 Y S2

Switch>en

Switch#erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Switch#reload

Proceed with reload? [confirm]

C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)

Una vez inicializado todos los dispositivos se procede a activar el soporte de IPv6 para ambos switches.

Switch>en

Switch#conf t

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

Changes to the running SDM preferences have been stored, but cannot take effect until the next reload.

Use 'show sdm prefer' to see what SDM preference is currently active.

Switch(config)#exit

Switch#reload

%SYS-5-CONFIG_I: Configured from console by console

System configuration has been modified. Save? [yes/no]:yes

Building configuration...

[OK]

Proceed with reload? [confirm]

2.2 CONFIGURACIÓN ROUTER R1

Se desactiva la búsqueda por DNS debido a que no se implementará ningún servidor de este tipo, y para no entorpecer la configuración del dispositivo ya que si esta activa y se ingresa un comando erróneo dicho dispositivo genera una búsqueda por DNS inhabilitando el teclado aumentando el tiempo de configuración, una vez desactivada la búsqueda se procede a cambiar el nombre del router por *R1*, su nombre de dominio como *ccna-sa.com*, para el apartado de seguridad se configura la contraseña como *class* para el modo EXEC que es el que permite tener acceso a todos los comandos sin restricciones, de igual forma para ingresar a la consola del router se configura la contraseña como *cisco*, cumpliendo así con un protocolo básico de seguridad el cual recomienda manejar contraseñas diferentes aunque más robustas para los diferentes niveles, seguido de esto cualquier contraseña nueva que intente registrar deberá de cumplir con una longitud mínima de cinco (5) caracteres, se contará con un usuario administrativo o de privilegio 15 siendo su nombre de usuario *admin* y su contraseña *admin1pass*, de igual forma las contraseñas deberán de estar cifradas en el dispositivo.

Una vez configurado estos aspectos, se continúa a proteger las líneas de acceso VTY las cuales deberán de validar las credenciales de manera local y su acceso remoto será por el protocolo SSH, por lo que también es necesario generar una clave de cifrado RSA de al menos 1024 bits.

Por estándar se debe de mostrar un mensaje cada vez que se acceda al router, por lo general dicho mensaje debe de informar que el acceso a personal no autorizado está prohibido, pero por motivos del ejercicio se reemplazara con la información del administrador, seguido de esto se debe de activar que el dispositivo acepte la configuración de conectividad por IPv6, todo esto con la finalidad de configurar la interfaz G0/0/1 y las sub interfaces, por lo que cada una de esta contará con su dirección IPv4 e IPv6, su descripción, su default gateway IPv6, de igual forma se configura la interfaz loopback0 tanto para IPv4 como para

IPv6 con la finalidad de verificar el funcionamiento TCP/IP.

Todo lo anterior se realiza por medio de los siguientes comandos:

```
Router>en
```

```
//Se activa el modo EXEC.
```

```
Router#conf t
```

```
//Se accede para configurar la terminal.
```

```
Router(config)#no ip domain lookup
```

```
//Se desactiva la búsqueda por DNS.
```

```
Router(config)#hostname R1
```

```
//Se cambia el nombre del Host a R1.
```

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

```
//Se cambia el nombre del Dominio.
```

```
R1(config)#enable secret class
```

```
//Se configura la contraseña para el modo EXEC.
```

```
R1(config)#line con 0
```

```
//Se configura la línea 0 de la consola.
```

```
R1(config-line)#password cisco
```

```
//Se configura la contraseña para la consola.
```

```
R1(config-line)#login
```

```
//Se configura para que la consola requiera login.
```

R1(config)#security password min-length 5
//Se establece una longitud mínima de 5 caracteres.

R1(config)#username admin privilege 15 password admin1pass
//Se crea un usuario y contraseña de nivel 15.

R1(config)#line vty 0 15
//Se accede a las líneas VTY 0 al 15.

R1(config-line)#login local
//Se configura el login de manera local.

R1(config-line)#transport input ssh
//Se activa el protocolo SSH.

R1(config)#service password-encryption
//Se activa el cifrado de contraseña.

R1(config)#banner motd #
Nombre Dispositivo: R1
Nombre Estudiante: Ricardo Agredo Trujillo
Programa Academico: Ingenieria de Sistemas
//Mensaje para la consola, se finaliza con #.

R1(config)#ipv6 unicast-routing
//Se activa la conectividad para los medios tipo IPv6.

R1(config)#interface g0/0/1
//Se accede a la interfaz G/0/1.

```
R1(config-if)#no shut
//Se activa la interfaz.
```

Debido a que los siguientes comandos son los mismos exceptuando que cambia la interfaz y la dirección se explica una vez el funcionamiento para uno de ellos:

```
R1(config)#interface g0/0/1.20
//Se selecciona la subinterfaz .20 de la interfaz G0/0/1.
```

```
R1(config-subif)#encapsulation dot1Q 20
//Se activa el encapsulamiento dot1Q para la VLAN con ID 20.
```

```
R1(config-subif)#description Docentes
//Se asigna una descripción para facilitar la identificación.
```

```
R1(config-subif)#ip add 10.71.8.1 255.255.255.192
//Se añade la dirección IPv4 proporcionada por la tabla 9.
```

```
R1(config-subif)#ipv6 add fe80::1 link-local
//Se añade la dirección de enlace local.
```

```
R1(config-subif)#ipv6 add 2001:db8:acad:a::1/64
//Se añade la dirección IPv6 proporcionada por la tabla 9.
```

```
R1(config-subif)#no shut
//Se activa la sub interfaz.
```

```
R1(config-subif)#exit
//Se finaliza la configuración de la sub interfaz
```

```
R1(config)#interface g0/0/1.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#description Estudiantes
R1(config-subif)#ip add 10.71.8.65 255.255.255.224
R1(config-subif)#ipv6 add fe80::1 link-local
R1(config-subif)#ipv6 add 2001:db8:acad:b::1/64
R1(config-subif)#no shut
R1(config-subif)#exit
```

```
R1(config)#interface g0/0/1.40
R1(config-subif)#encapsulation dot1Q 40
R1(config-subif)#description Invitados
R1(config-subif)#ip add 10.71.8.97 255.255.255.248
R1(config-subif)#ipv6 add fe80::1 link-local
R1(config-subif)#ipv6 add 2001:db8:acad:c::1/64
R1(config-subif)#no shut
R1(config-subif)#exit
```

```
R1(config)#interface g0/0/1.56
R1(config-subif)#encapsulation dot1Q 56
R1(config-subif)#description Native
R1(config-subif)#exit
```

```
R1(config)#interface Loopback 0
//Se accede a la interfaz Loopback 0
```

```
R1(config-if)#description Loopback 0
//Se deja una descripción para su identificación
```

```
R1(config-if)#ip add 209.165.201.1 255.255.255.224
```

```
//Se configura la IPv4 proporcionada por la tabla 9
```

```
R1(config-if)#ipv6 add 2001:db8:acad:209::1/64
```

```
//Se configura la IPv6 proporcionada por la tabla 9
```

```
R1(config-if)#ipv6 add fe80::1 link-local
```

```
//Se configura la dirección de enlace local
```

```
R1(config)#crypto key generate RSA
```

```
//Se genera una clave de cifrado RSA
```

```
The name for the keys will be: R1.ccna-sa.com
```

```
How many bits in the modulus [512]: 1024
```

```
//Se especifica que la clave debe de ser de 1024 Bits
```

```
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

2.3 CONFIGURACIÓN S1 Y S2

Continuando con la configuración para los dispositivos switch S1 y S2, se desactiva la búsqueda por DNS, se cambia el nombre del dispositivo, se configura el nombre de dominio a *ccna-sa.com*, para el modo EXEC se establece la contraseña *class* y para el acceso a la consola la contraseña es *cisco*, de igual forma se debe de crear un usuario administrativo cuyo usuario es *admin* y su contraseña es *admin1pass*, para el inicio de sesión de las líneas VTY se debe de validar las credenciales de manera local mientras que para la conexión remota únicamente se aceptara por SSH, de igual forma se cifraran las contraseñas y se dejará los datos del administrador en la ventana de acceso a la consola.

A continuación se creará una clave de cifrado RSA de 1024 bits, mientras que la interfaz virtual de la LAN 40 de los dos switches se deberá de establecer la

dirección de IPv4 e IPv6 proporcionadas en la tabla 9, mientras que para S1 su dirección de enlace local de IPv6 debe de ser FE80::98 para S2 será FE80::99, finalmente se configura el gateway predeterminado tal como lo indica en la tabla 9. Toda la configuración anterior se realiza por medio de los siguientes comandos:

Switch S1

```
Switch>en
```

```
//Se activa el modo EXEC.
```

```
Switch#conf t
```

```
//Se accede a la configuración de la terminal.
```

```
Switch(config)#no ip domain-lookup
```

```
//Se desactiva la búsqueda por DNS.
```

```
Switch(config)#hostname S1
```

```
//Se cambia el nombre de host a S1.
```

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

```
//Se configura el nombre de dominio.
```

```
S1(config)#enable secret class
```

```
//Se configura la contraseña para el modo EXEC.
```

```
S1(config)#line con 0
```

```
//Se accede a la línea 0 de la consola.
```

```
S1(config-line)#password cisco
```

```
//Se configura la contraseña de acceso a la consola.
```

S1(config-line)#login

//Se activa que se requiera validar credenciales al acceso de la consola.

S1(config-line)#exit

//Se finaliza la configuración actual.

S1(config)#username admin privilege 15 password admin1pass

//Se crea un usuario y contraseña de nivel 15.

S1(config)#line vty 0 15

//Se accede a las líneas VTY.

S1(config-line)#login local

//Se activa la validación de credenciales de manera local.

S1(config-line)#transport input ssh

//Se activa que únicamente se acepten conexiones por SSH.

S1(config)#service password-encryption

//Se cifran las contraseñas que se encuentran en el Switch.

S1(config)#banner motd #

//Se configura un mensaje de la consola.

Nombre Dispositivo: S1

Nombre Estudiante: Ricardo Agredo Trujillo

Programa Academico: Ingenieria de Sistemas

S1(config)#crypto key generate rsa

//Se genera una clave encriptada RSA.

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

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

How many bits in the modulus [512]: 1024

//Se especifica que la clave RSA debe ser de 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#interface vlan 40

//Se accede la interfaz VLAN 40.

S1(config-if)#ip add 10.71.8.98 255.255.255.248

//Se configura la dirección Ipv4 proporcionada por la tabla 9.

S1(config-if)#ipv6 add fe80::98 link-local

//Se configura la dirección Ipv6 de enlace local.

S1(config-if)#ipv6 add 2001:db8:acad:c::98/64

//Se configura la dirección Ipv6 proporcionada por la tabla 9.

S1(config-if)#description Invitados

//Se deja una descripción para su visualización.

S1(config-if)#no shut

//Se activa la interfaz.

S1(config)#ip default-gateway 10.71.8.97

//Se configura el default gateway proporcionado por la tabla 9.

Switch S2

Switch>en

//Se accede al modo EXEC.

Switch#conf t

//Se accede a la configuración de la terminal.

Switch(config)#no ip domain-lookup

//Se desactiva la búsqueda por DNS.

Switch(config)#hostname S2

//Se cambia el nombre de host a S2.

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

//Se configura el nombre de dominio.

S2(config)#enable secret class

//Se configura la contraseña para el modo EXEC.

S2(config)#line con 0

//Se accede a la línea 0 de la consola.

S2(config-line)#password cisco

//Se configura la contraseña de acceso a la consola.

S2(config-line)#login

//Se activa que se requiera validar credenciales al acceso de la consola.

S2(config-line)#exit

//Se finaliza la configuración actual.

S2(config)#username admin privilege 15 password admin1pass
//Se crea un usuario y contraseña de nivel 15.

S2(config)#line vty 0 15
//Se accede a las líneas VTY.

S2(config-line)#login local
//Se activa la validación de credenciales de manera local.

S2(config-line)#transport input ssh
//Se activa que únicamente se acepten conexiones por SSH.

S2(config)#service password-encryption
//Se cifran las contraseñas del Switch.

S2(config)#banner motd #
//Se configura un mensaje de la consola.
Enter TEXT message. End with the character '#'.
Nombre Dispositivo: S2
Nombre Estudiante: Ricardo Agredo Trujillo
Programa Academico: Ingenieria de Sistemas

S2(config)#crypto key generate rsa
//Se genera una clave encriptada RSA.

The name for the keys will be: S2.ccna-sa.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024

//Se especifica que la clave RSA debe ser de 1024 bits.
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S2(config)#interface vlan 40
//Se accede a la interfaz VLAN 40.

S2(config-if)#ip add 10.71.8.99 255.255.255.248
//Se configura la dirección Ipv4 proporcionada por la tabla 9.

S2(config-if)#ipv6 add fe80::99 link-local
//Se configura la dirección Ipv6 de enlace local.

S2(config-if)#ipv6 add 2001:db8:acad:c::99/64
//Se configura la dirección Ipv6 proporcionada por la tabla 9.

S2(config-if)#description Invitados
//Se deja una descripción para su visualización.

S2(config-if)#no shut
//Se activa la interfaz.

S2(config)#ip default-gateway 10.71.8.97
//Se configura el default gateway proporcionado por la tabla 9.

2.4 CONFIGURACIÓN DE LA INFRAESTRUCTURA DE RED

Una vez finalizada las configuraciones de los dispositivos intermediarios se crearán las VLAN'S para ambos Switches tal como lo indica la tabla 8, por lo que también se configura los enlaces troncales tal que para los switches S1 y S2 las interfaces serán F0/1, F0/2 y F0/5 de igual forma el protocolo de negociación será LACP y se utilizará la VLAN 56 como una VLAN nativa.

Para switch S1 el puerto de acceso de host para la VLAN 20 será por medio de la interfaz F0/6 mientras que para el switch S2 el puerto de acceso para la VLAN 30 será por medio de la interfaz F0/18, ambos switches deberán permitir únicamente 4 direcciones MAC para dar cumplimiento con los protocolos de seguridad establecidos inicialmente, seguidamente para las interfaces restantes que no son utilizadas se asignarán a la VLAN 50 de usuarios, para lo cual se asignará una descripción con el propósito de facilitar su identificación y seguidamente se apagarán dichas interfaces.

Lo anterior se aplicará con las siguientes líneas de comando:

Se explica el primer segmento y se omitirá para los siguientes pues lo único que cambia es el identificador o ID.

Configuración switch S1

```
S1(config)#vlan 20
```

```
//Se crea la VLAN con ID 20
```

```
S1(config-vlan)#name Docentes
```

```
//Se asigna el nombre a la VLAN
```

```
S1(config)#vlan 30
```

```
S1(config-vlan)#name Estudiantes
```

```
S1(config)#vlan 40
```

```
S1(config-vlan)#name Invitados
```

```
S1(config)#vlan 50
S1(config-vlan)#name Usuarios
```

```
S1(config)#vlan 56
S1(config-vlan)#name Native
```

```
S1(config)#interface range F0/1-2
//Se selecciona el rango desde F0/1 hasta F0/2
```

```
S1(config-if-range)#switchport mode trunk
//Se activa el modo troncal en el puerto
```

```
S1(config-if-range)#switchport trunk native vlan 56
//Se configura la VLAN 56 como vlan troncal nativa.
```

```
S1(config-if-range)#switchport trunk allowed vlan 20,30,40,50,56
//Se añaden las VLAN'S que utilizaran el modo de enlace troncal
```

```
S1(config)#interface f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 56
S1(config-if)#switchport trunk allowed vlan 20,30,40,50,56
```

```
S1(config)#interface range f0/1-2
S1(config-if-range)#channel-group 1 mode active
//Se activa el channel group para utilizar unicamente LACP (mode active)
```

```
S1(config)#interface f0/6
S1(config-if)#switchport mode access
//Se configura el modo de acceso
```

```
S1(config-if)#switchport access vlan 20
//El acceso será únicamente por la VLAN 20
```

```
S1(config-if)#switchport port-security maximum 4
//Se configura la seguridad del puerto en máximo 4 direcciones MAC
```

```
S1(config)#interface range f0/3-4
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 50
S1(config-if-range)#description Interfaces no utilizadas
S1(config-if-range)#shut
```

```
S1(config)#interface range f0/7-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 50
S1(config-if-range)#description Interfaces no utilizadas
S1(config-if-range)#shut
```

```
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 Interfaces no utilizadas
S1(config-if-range)#shut
```

Configuración switch S2

```
S2(config)#vlan 20
S2(config-vlan)#name Docentes
S2(config)#vlan 30
S2(config-vlan)#name Estudiantes
S2(config)#vlan 40
S2(config-vlan)#name Invitados
S2(config)#vlan 50
S2(config-vlan)#name Usuarios
S2(config)#vlan 56
S2(config-vlan)#name Native

S2(config)#interface range f0/1-2
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)#channel-group 1 mode active

S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 30
S2(config-if)#switchport port-security maximum 4

S2(config)#interface range f0/3-17
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 50
S2(config-if-range)#description Interfaces no utilizadas
S2(config-if-range)#shut
```

```
S2(config)#interface range f0/19-24
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 50
S2(config-if-range)#description Interfaces no utilizadas
S2(config-if-range)#shut
```

```
S2(config-if-range)#interface range g0/1-2
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 50
S2(config-if-range)#description Interfaces no utilizadas
S2(config-if-range)#shut
```

2.5 CONFIGURACIÓN DE SOPORTE PARA LOS HOSTS

Una vez creada la infraestructura de la red y estando debidamente configurada se continua con la configuración para el soporte de los hosts, dicha configuración debe ser aplicada en el router R1, la cual consta de especificar que la ruta predeterminada para la conectividad Ipv4 e Ipv6 debe ser por la interfaz donde se encuentra configurado el Loopback0, a continuación siguiendo los requerimientos establecidos se debe crear un grupo DHCP o pool DHCP para la VLAN 20 la cual constará de las ultimas 10 direcciones de la subred, también se configura el nombre de dominio como *unad-ccna-sa.net*, se especifica el default gateway para dicha interfaz, mientras que para la VLAN 30 la configuración es la misma únicamente cambiando el nombre de dominio a *unad-ccna-sb.net*, lo anterior se puede identificar y calcular mediante la tabla 9.

Para identificar las 10 últimas direcciones se hace el siguiente procedimiento:

Se indica que deben de estar disponible las últimas diez direcciones IP para la VLAN 20, por lo que según la tabla 9 la VLAN 20 pertenece a la interfaz G0/0/1.20 cuya primera dirección es 10.71.8.1/26, mientras que VLAN 30 su dirección es 10.71.8.65/27 siendo la primera IP utilizable por lo que se identifica que la dirección de red es 10.71.8.64 y la dirección de broadcast es 10.71.8.63, siendo estas dos últimas direcciones reservadas, así que la última IP disponible para la VLAN 20 es 10.71.8.62 y separando las 10 últimas direcciones IP se identifica que el rango de direcciones que se deben de excluir va desde 10.71.8.1 hasta 10.71.8.52.

De igual forma para la VLAN 30, se conoce que la primera dirección disponible para la VLAN 40 es 10.71.8.97/29 por lo que la dirección de red es 10.71.8.96, la dirección de broadcast es 10.71.8.95 y la última IP disponible es 10.71.8.94 por lo que el rango que se debe de excluir va desde 10.71.8.65 hasta 10.8.84.

De igual forma se explica el procedimiento para la VLAN 20 y se omite para la VLAN 30 debido a que el procedimiento es el mismo, únicamente se cambia las últimas diez direcciones y el nombre de dominio.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
//Se establece la dirección Ipv4 para el loopback
```

```
R1(config)#ipv6 route ::/0 loopback 0
//Se establece la dirección IPv6 para el loopback
```

```
R1(config)#ip dhcp excluded-address 10.71.8.1 10.71.8.52
//Se excluye el rango de direcciones para el protocolo DHCP
```

```
R1(config)#ip dhcp pool VLAN20-Docentes
```

```
//Se activa el protocolo DHCP para la VLAN 20
```

```
R1(dhcp-config)#network 10.71.8.0 255.255.255.192
```

```
//Se configura la red para el protocolo DHCP
```

```
R1(dhcp-config)#default-router 10.71.8.1
```

```
//Se establece la puerta de enlace predeterminada como dirección de interfaz
```

```
R1(dhcp-config)#domain-name unad-ccna-sa.net
```

```
//Se establece el nombre del dominio
```

```
R1(config)#ip dhcp excluded-address 10.71.8.65 10.71.8.84
```

```
R1(config)#ip dhcp pool VLAN30-Estudiantes
```

```
R1(dhcp-config)#network 10.71.8.64 255.255.255.224
```

```
R1(dhcp-config)#default-router 10.71.8.65
```

```
R1(dhcp-config)#domain-name unad-ccna-sb.net
```

```
R1(dhcp-config)#exit
```

2.6 CONFIGURAR LOS EQUIPOS HOST

Finalmente la infraestructura esta realizada, así que se continua con la configuración de los dispositivos finales, se debe de configurar que para la conexión por Ipv4 se utilice el protocolo DHCP para ambos equipos, las direcciones Ipv6 y de enlace local se deben de configurar de manera estática tal como lo indica la tabla 9, por lo que se realiza por medio de la pestaña Desktop y en la sección de configuración de IP, se activa el protocolo DHCP y se ingresan dichos datos en la configuración de Ipv6 , de igual forma se guarda la información mostrada por medio del comando *ipconfig /all* en la tabla 10 para el PC – A y en la tabla 11 para el PC – B.

Tabla 10. Configuración red equipo A

CONFIGURACIÓN DE RED DE PC - A	
Descripción	FastEthernet0 (Default Port)
Dirección física	0001.64D4.D07A
Dirección IP	10.71.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.71.8.1
Gateway predeterminado IPv6	FE80::1

Fuente: Autoría propia.

Tabla 11. Configuración red equipo B

CONFIGURACIÓN DE RED DE PC - B	
Descripción	FastEthernet0 (Default Port)
Dirección física	0060.2FB5.B88C
Dirección IP	10.71.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.71.8.65
Gateway predeterminado IPv6	FE80::1

Fuente: Autoría propia.

2.7 VERIFICAR LA CONECTIVIDAD DE EXTREMO A EXTREMO

Una vez finalizada toda la configuración para la red y con la finalidad de verificar metódicamente la conectividad entre todos los dispositivos por medio del comando ping, esta información se registra en la tabla 12.

Tabla 12. Conectividad de extremo a extremo.

Desde	A		Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.20	IPv4	10.71.8.1/26	✓
		IPv6	2001:DB8:ACAD:A::1/64	✓
	R1, G0/0/1.30	IPv4	10.71.8.65/24	✓
		IPv6	2001:DB8:ACAD:B::1/64	✓
	R1, G0/0/1.40	IPv4	10.71.8.97/29	✓
		IPv6	2001:DB8:ACAD:C::1/64	✓
	S1, VLAN 40	IPv4	10.71.8.98/29	✓
		IPv6	2001:DB8:ACAD:C::98/64	Error C.P.T ⁸
	S2, VLAN 40	IPv4	10.71.8.99/29	✓
		IPv6	2001:DB8:ACAD:C::99/64	Error C.P.T
	PC-B	IPv4	DHCP (10.71.8.86)	✓
		IPv6	2001:DB8:ACAD:B::50/64	✓
	R1 Bucle 0	IPv4	209.165.201.1/27	✓
		IPv6	2001:DB8:ACAD:209::1/64	✓
PC-B	R1 Bucle 0	IPv4	209.165.201.1/27	✓
		IPv6	2001:DB8:ACAD:209::1/64	✓
	R1, G0/0/1.20	IPv4	10.71.8.1/26	✓
		IPv6	2001:DB8:ACAD:A::1/64	✓
	R1, G0/0/1.30	IPv4	10.71.8.65/24	✓
		IPv6	2001:DB8:ACAD:B::1/64	✓
	R1,	IPv4	10.71.8.97/29	✓

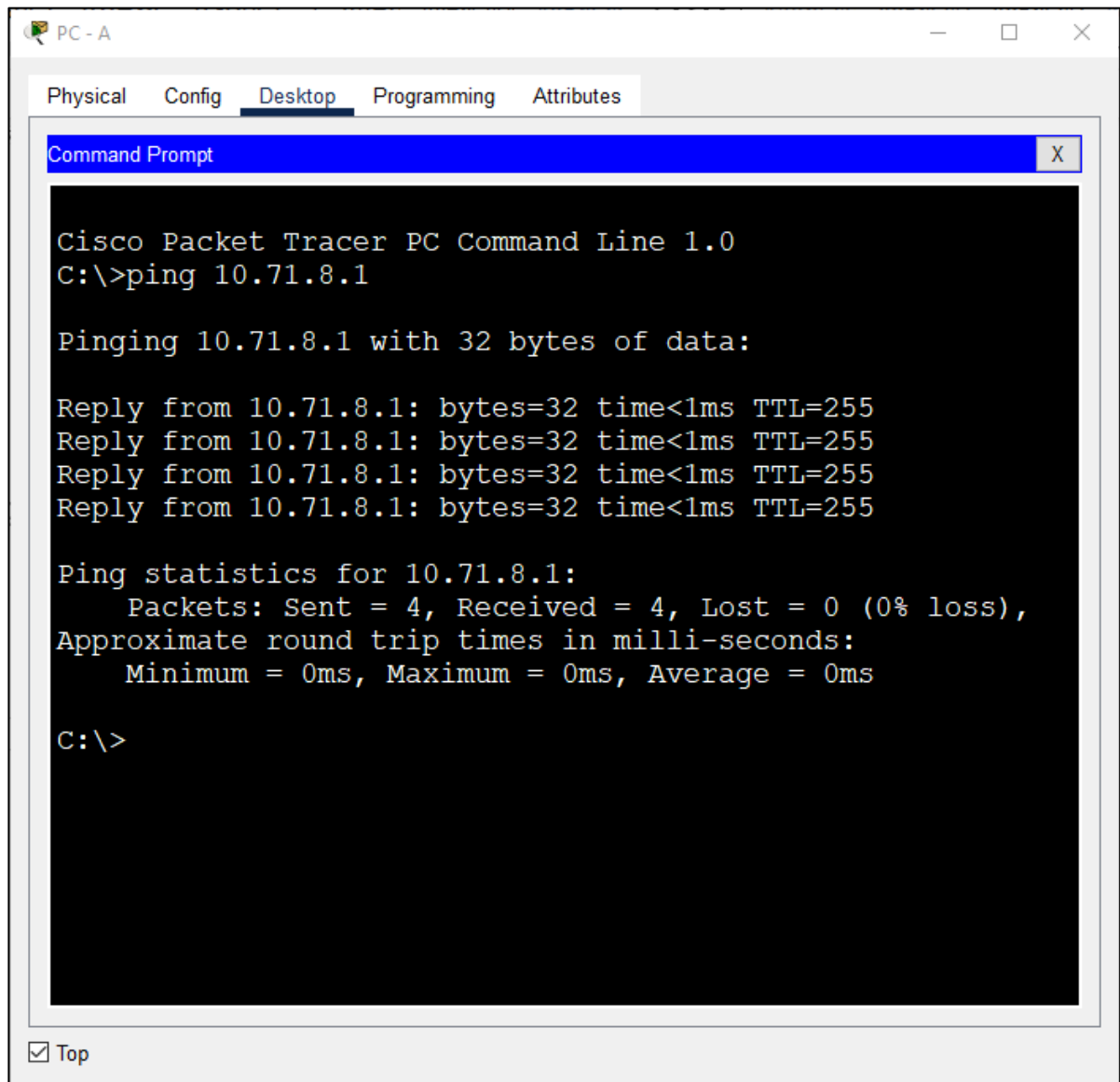
* Error C.P.T : Error por parte de Cisco Packet Tracer

	G0/0/1.40	IPv6	2001:DB8:ACAD:C::1/64	✓
	S1, VLAN 40	IPv4	10.71.8.98/29	✓
		IPv6	2001:DB8:ACAD:C::98/64	Error C.P.T
	S2, VLAN 40	IPv4	10.71.8.99/29	✓
		IPv6	2001:DB8:ACAD:C::99/64	Error C.P.T

Fuente: Autoría propia.

El ping para los dispositivos S1 VLAN 40 y S2 VLAN 40 por medio de IPv6 presenta un error C.P.T, ya que al ser un simulador todo lo está ejecutando desde un único dispositivo final, de igual forma también contribuye que surja debido al sistema que se implementa para dichos switches.

Figura 12. Ping desde PC - A hacia G0/0/1.20 por IPv4



The image shows a screenshot of a Cisco Packet Tracer PC Command Prompt window. The window title is "PC - A" and it has tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, and a "Command Prompt" window is open. The text in the Command Prompt is as follows:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.71.8.1

Pinging 10.71.8.1 with 32 bytes of data:

Reply from 10.71.8.1: bytes=32 time<1ms TTL=255
Reply from 10.71.8.1: bytes=32 time<1ms TTL=255
Reply from 10.71.8.1: bytes=32 time<1ms TTL=255
Reply from 10.71.8.1: bytes=32 time<1ms TTL=255

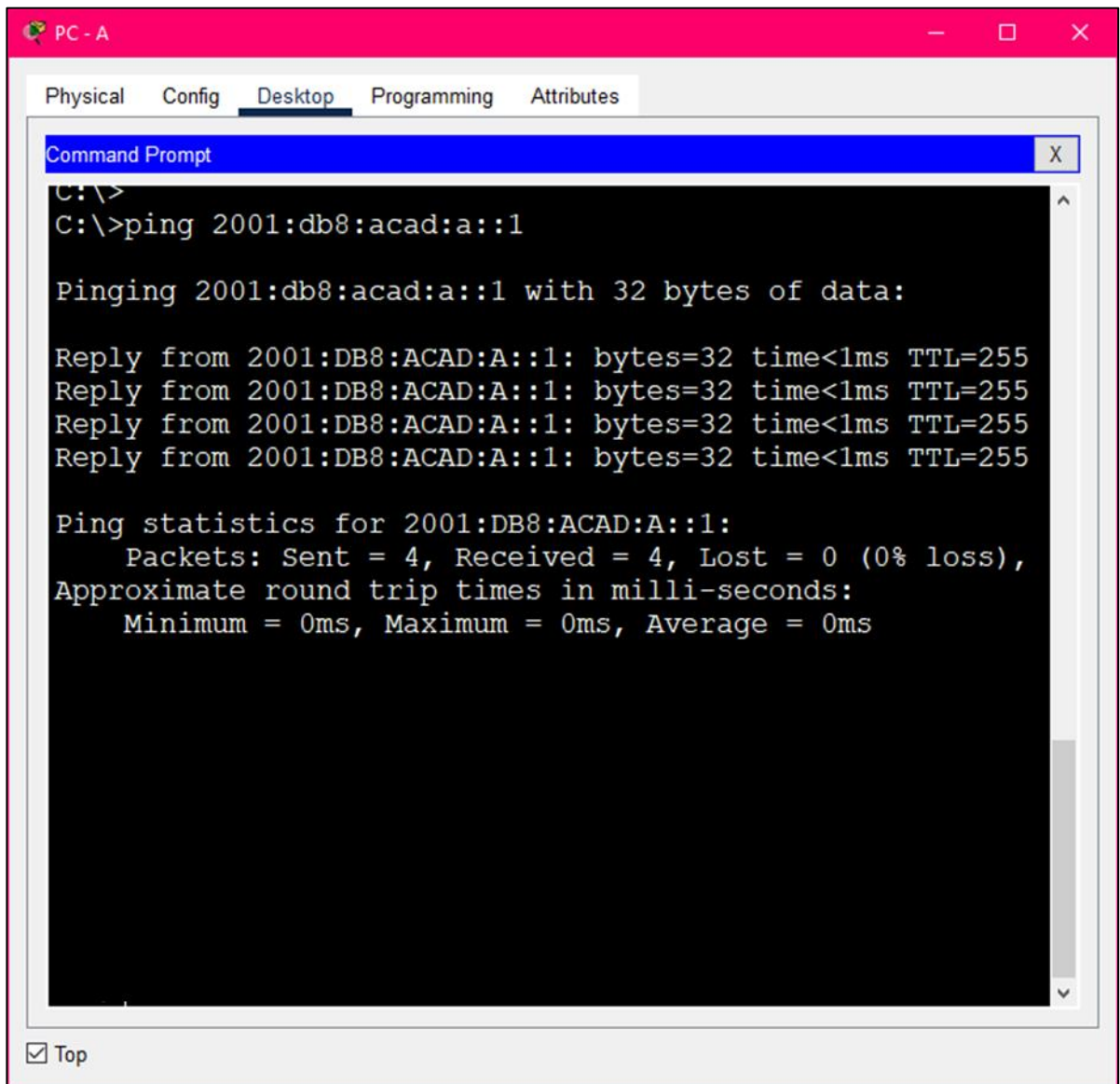
Ping statistics for 10.71.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

At the bottom left of the Command Prompt window, there is a checkbox labeled "Top" which is checked.

Fuente: Autoría propia.

Figura 13. Ping desde PC - A hacía G0/0/1.20 por IPv6



The image shows a screenshot of a PC-A desktop environment. The window title is "PC - A" and it has tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, and a "Command Prompt" window is open. The command prompt shows the following text:

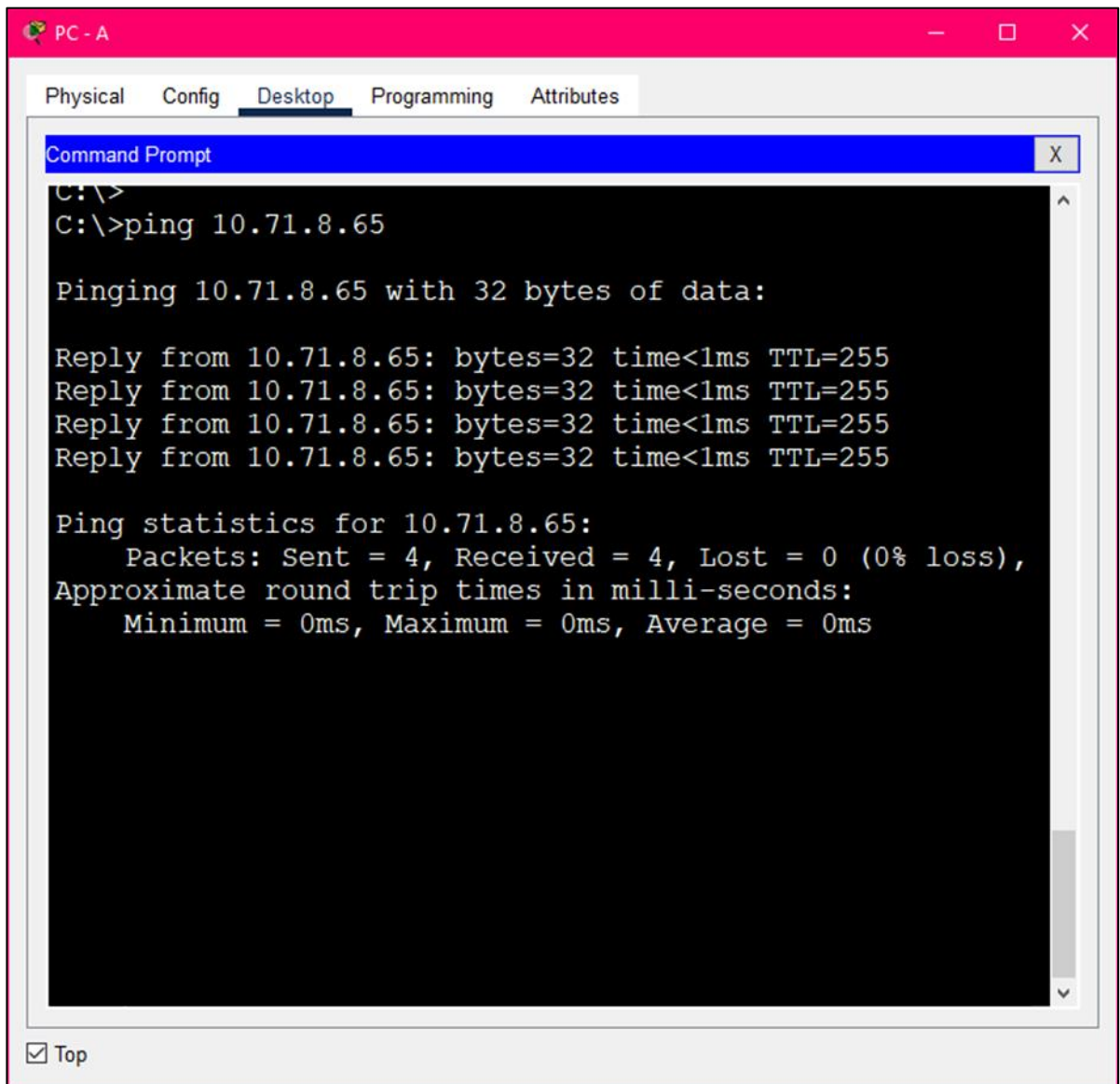
```
C:\>  
C:\>ping 2001:db8:acad:a::1  
  
Pinging 2001:db8:acad:a::1 with 32 bytes of data:  
  
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255  
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255  
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255  
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255  
  
Ping statistics for 2001:DB8:ACAD:A::1:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

At the bottom left of the Command Prompt window, there is a checkbox labeled "Top" which is checked.

Fuente: Autoría propia.

De la figura 13 se concluye que

Figura 14. Ping hacia G0/0/1.30 por IPv4



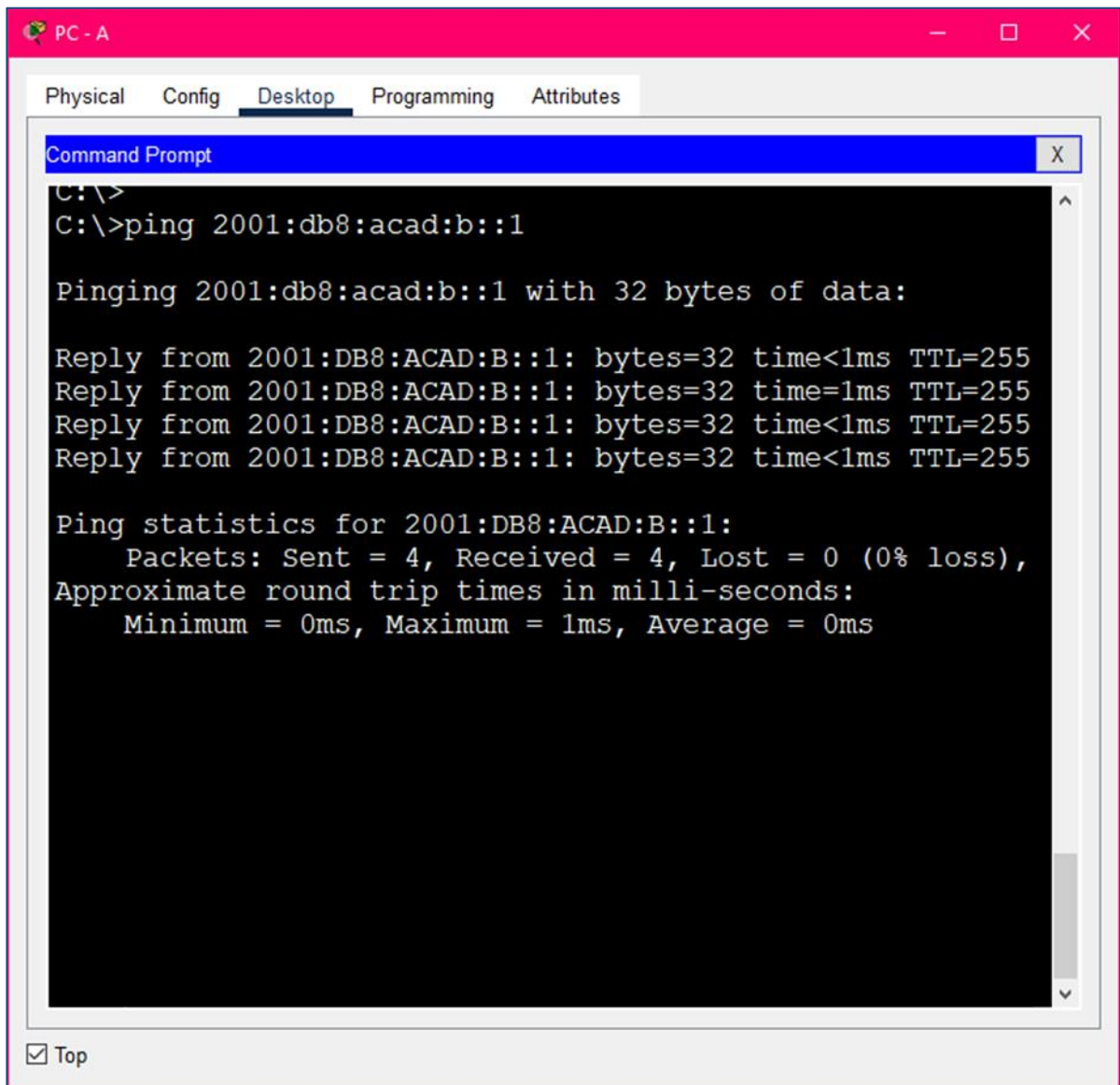
The image shows a screenshot of a PC-A Desktop environment. The window title is "PC - A" and it has standard Windows window controls (minimize, maximize, close). The desktop environment includes tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, displaying a "Command Prompt" window. The Command Prompt shows the following text:

```
C:\>  
C:\>ping 10.71.8.65  
  
Pinging 10.71.8.65 with 32 bytes of data:  
  
Reply from 10.71.8.65: bytes=32 time<1ms TTL=255  
Reply from 10.71.8.65: bytes=32 time<1ms TTL=255  
Reply from 10.71.8.65: bytes=32 time<1ms TTL=255  
Reply from 10.71.8.65: bytes=32 time<1ms TTL=255  
  
Ping statistics for 10.71.8.65:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

At the bottom left of the Command Prompt window, there is a checkbox labeled "Top" which is checked.

Fuente: Autoría propia.

Figura 15. Ping desde PC - A hacía G0/0/1.30 por IPv6



The image shows a screenshot of a PC-A window with a red title bar. Inside, there are tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the execution of a ping command to the IPv6 address 2001:db8:acad:b::1. The output indicates that four packets were sent and received successfully with 0% loss and a round trip time of less than 1ms.

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

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

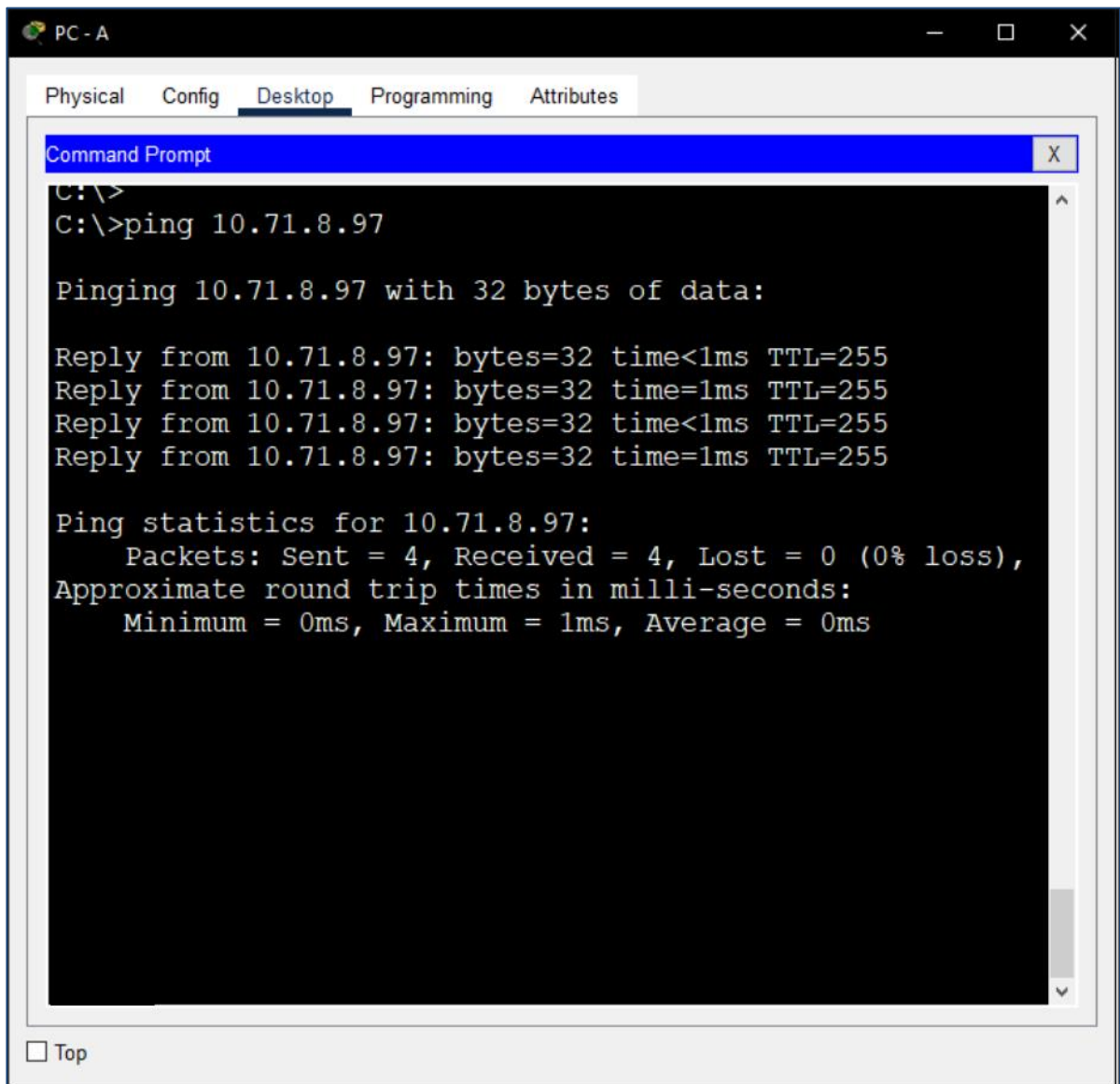
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255

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

Top

Fuente: Autoría propia.

Figura 16. Ping desde PC - A hacía G0/0/1.41 por IPv4



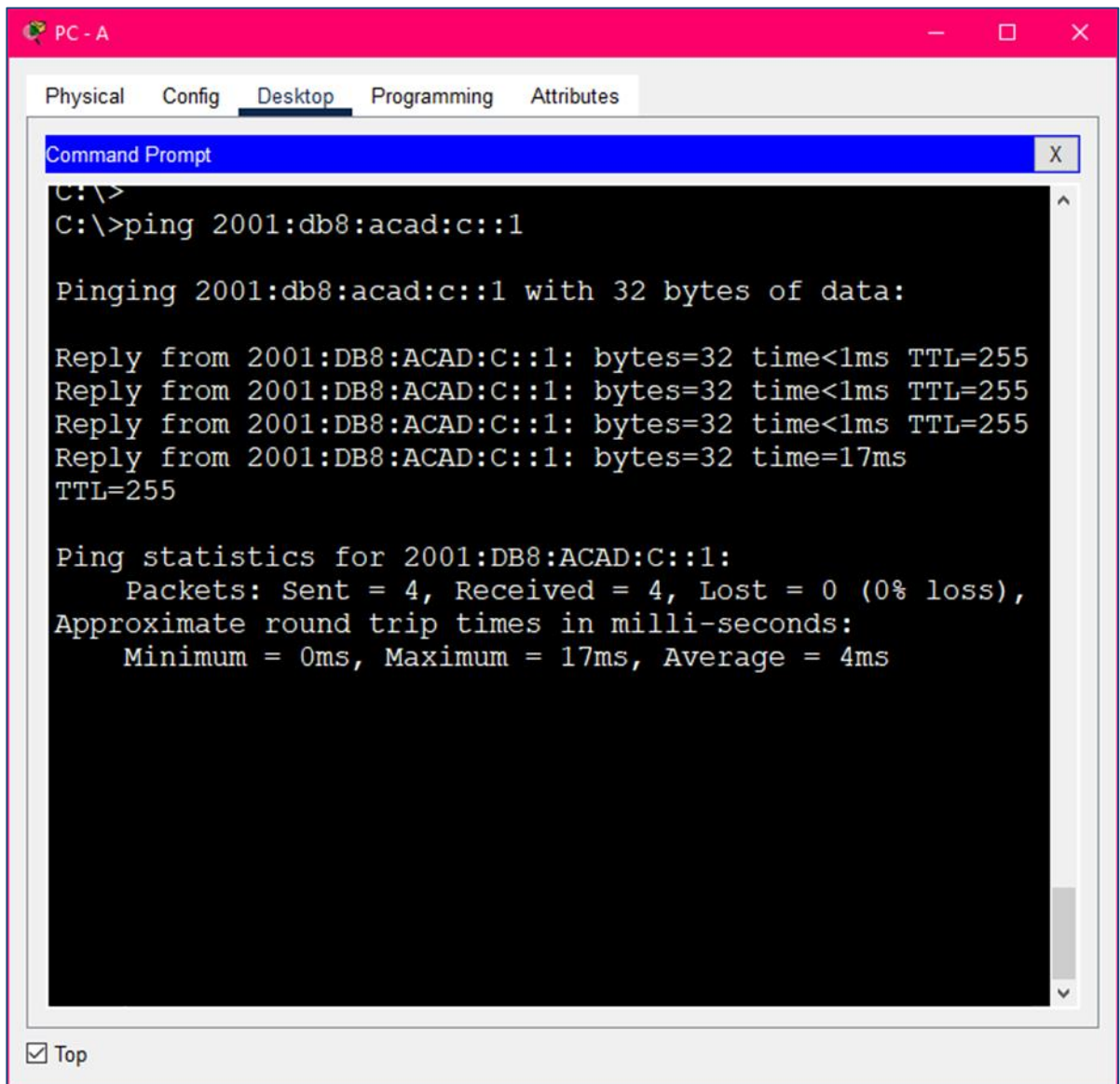
The image shows a screenshot of a Command Prompt window titled "PC - A" with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active. The Command Prompt shows the following text:

```
C:\>  
C:\>ping 10.71.8.97  
  
Pinging 10.71.8.97 with 32 bytes of data:  
  
Reply from 10.71.8.97: bytes=32 time<1ms TTL=255  
Reply from 10.71.8.97: bytes=32 time=1ms TTL=255  
Reply from 10.71.8.97: bytes=32 time<1ms TTL=255  
Reply from 10.71.8.97: bytes=32 time=1ms TTL=255  
  
Ping statistics for 10.71.8.97:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

At the bottom left of the window, there is a "Top" button with a small square icon.

Fuente: Autoría propia.

Figura 17. Ping desde PC - A hacía G0/0/1.40 por IPv6



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

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

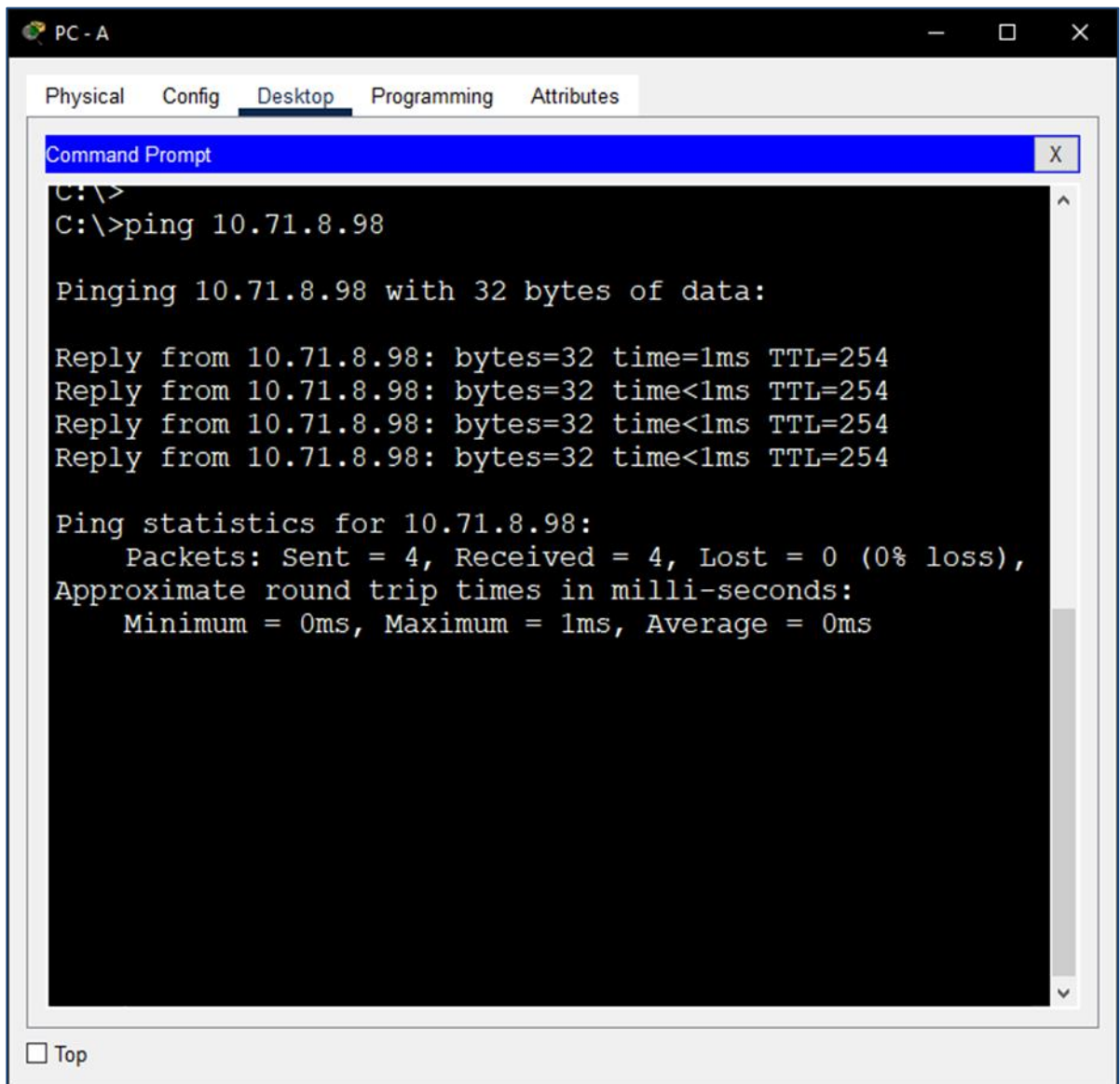
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time=17ms
TTL=255

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 = 17ms, Average = 4ms
```

Top

Fuente: Autoría propia.

Figura 18. Ping desde PC - A hacía VLAN 40 del S1 por IPv4



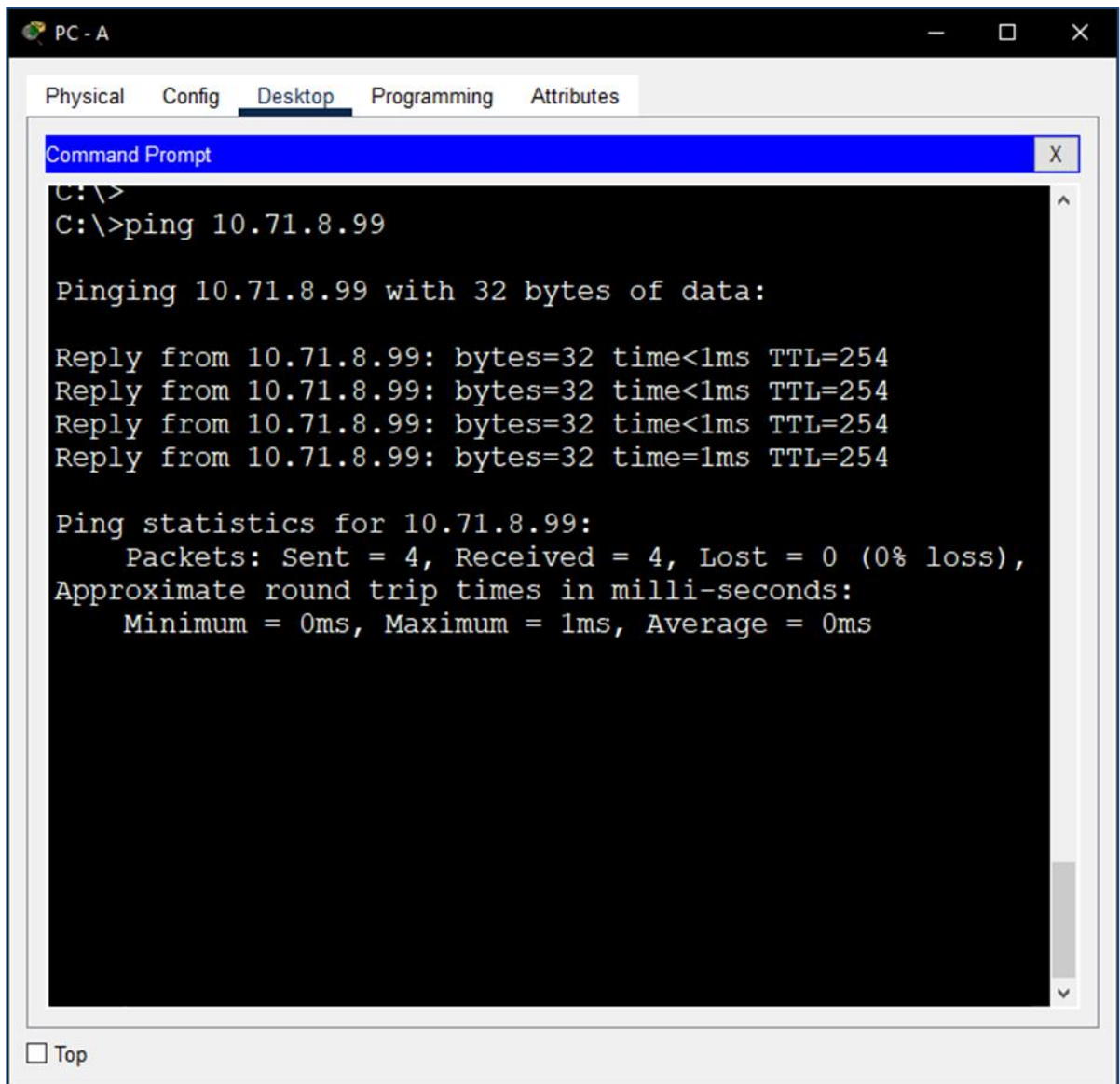
The image shows a screenshot of a Command Prompt window titled "PC - A" with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active. The Command Prompt shows the following text:

```
C:\>  
C:\>ping 10.71.8.98  
  
Pinging 10.71.8.98 with 32 bytes of data:  
  
Reply from 10.71.8.98: bytes=32 time=1ms TTL=254  
Reply from 10.71.8.98: bytes=32 time<1ms TTL=254  
Reply from 10.71.8.98: bytes=32 time<1ms TTL=254  
Reply from 10.71.8.98: bytes=32 time<1ms TTL=254  
  
Ping statistics for 10.71.8.98:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

At the bottom left of the window, there is a "Top" button.

Fuente: Autoría propia.

Figura 19. Ping desde PC - A hacía VLAN 40 del S2 por IPv4



The image shows a screenshot of a Command Prompt window titled "PC - A" with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active. The Command Prompt shows the following text:

```
C:\>ping 10.71.8.99

Pinging 10.71.8.99 with 32 bytes of data:

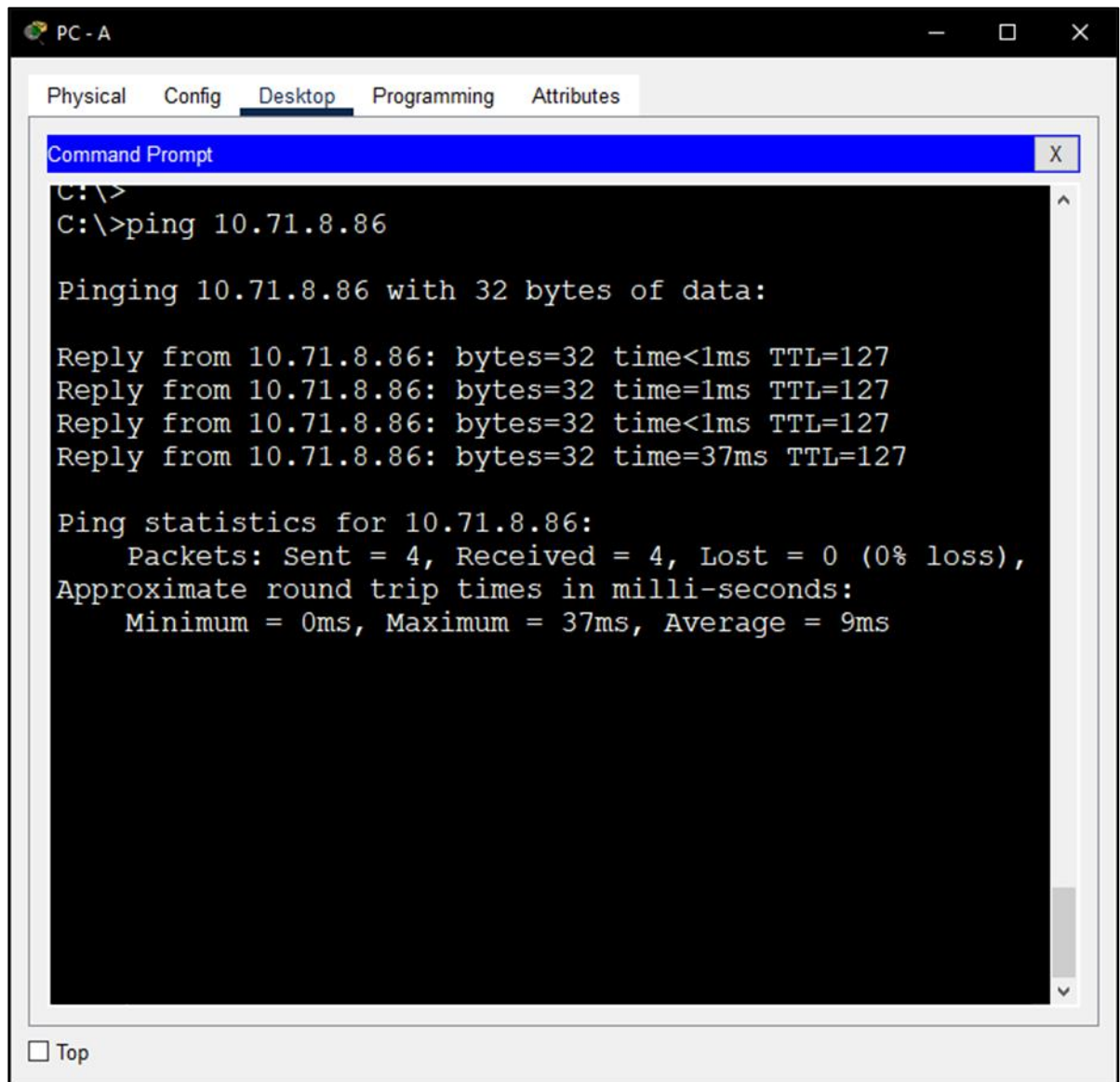
Reply from 10.71.8.99: bytes=32 time<1ms TTL=254
Reply from 10.71.8.99: bytes=32 time<1ms TTL=254
Reply from 10.71.8.99: bytes=32 time<1ms TTL=254
Reply from 10.71.8.99: bytes=32 time=1ms TTL=254

Ping statistics for 10.71.8.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

At the bottom left of the window, there is a "Top" button.

Fuente: Autoría propia.

Figura 20. Ping desde PC - A hacía PC - B por IPv4



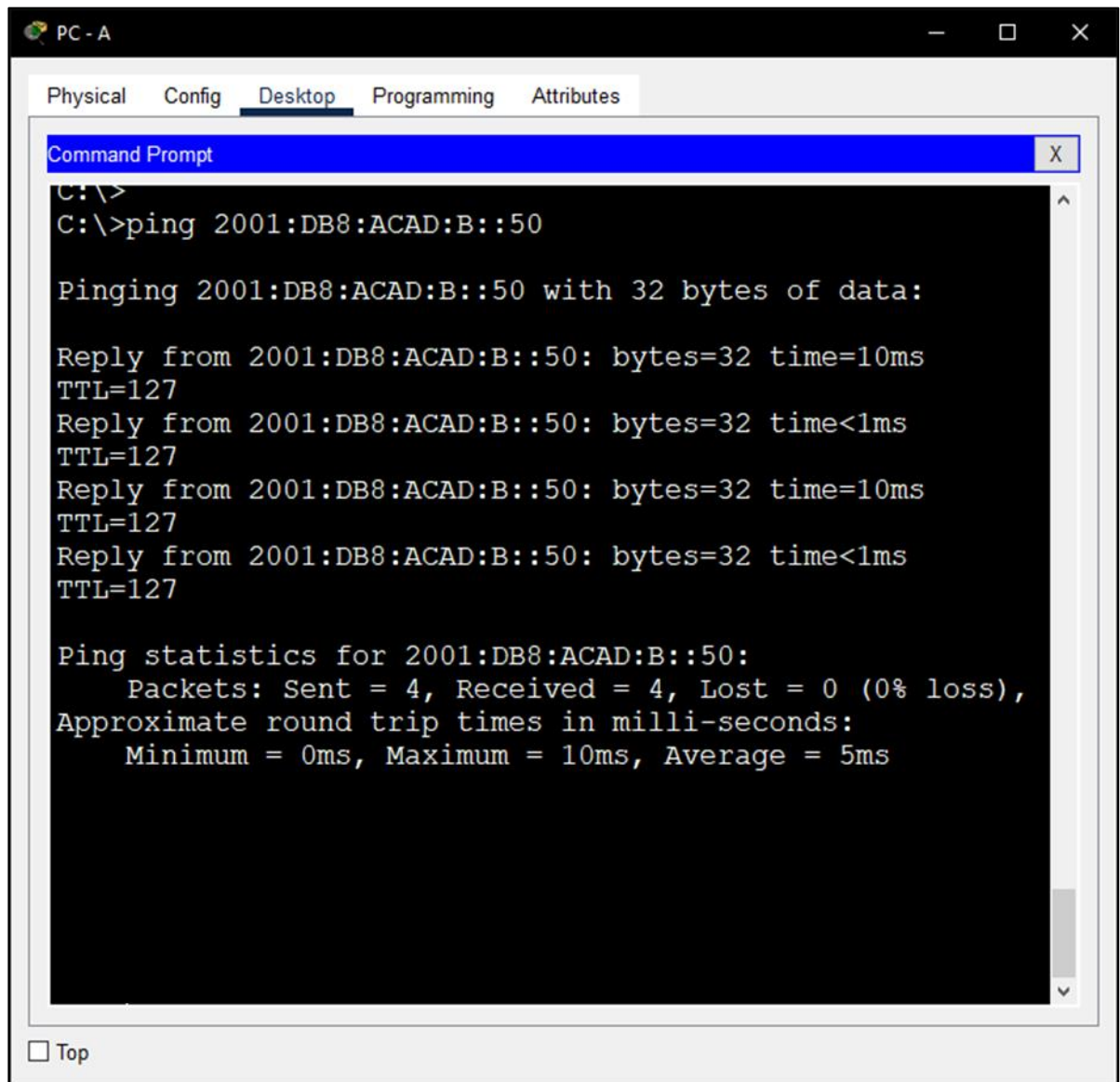
The image shows a screenshot of a Windows Command Prompt window titled "PC - A". The window has a menu bar with "Physical", "Config", "Desktop", "Programming", and "Attributes". The Command Prompt itself has a title bar "Command Prompt" and a close button "X". The text in the Command Prompt is as follows:

```
C:\>  
C:\>ping 10.71.8.86  
  
Pinging 10.71.8.86 with 32 bytes of data:  
  
Reply from 10.71.8.86: bytes=32 time<1ms TTL=127  
Reply from 10.71.8.86: bytes=32 time=1ms TTL=127  
Reply from 10.71.8.86: bytes=32 time<1ms TTL=127  
Reply from 10.71.8.86: bytes=32 time=37ms TTL=127  
  
Ping statistics for 10.71.8.86:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 37ms, Average = 9ms
```

At the bottom left of the window, there is a "Top" button with a small square icon.

Fuente: Autoría propia.

Figura 21. Ping desde PC - A hacía PC - B por IPv6



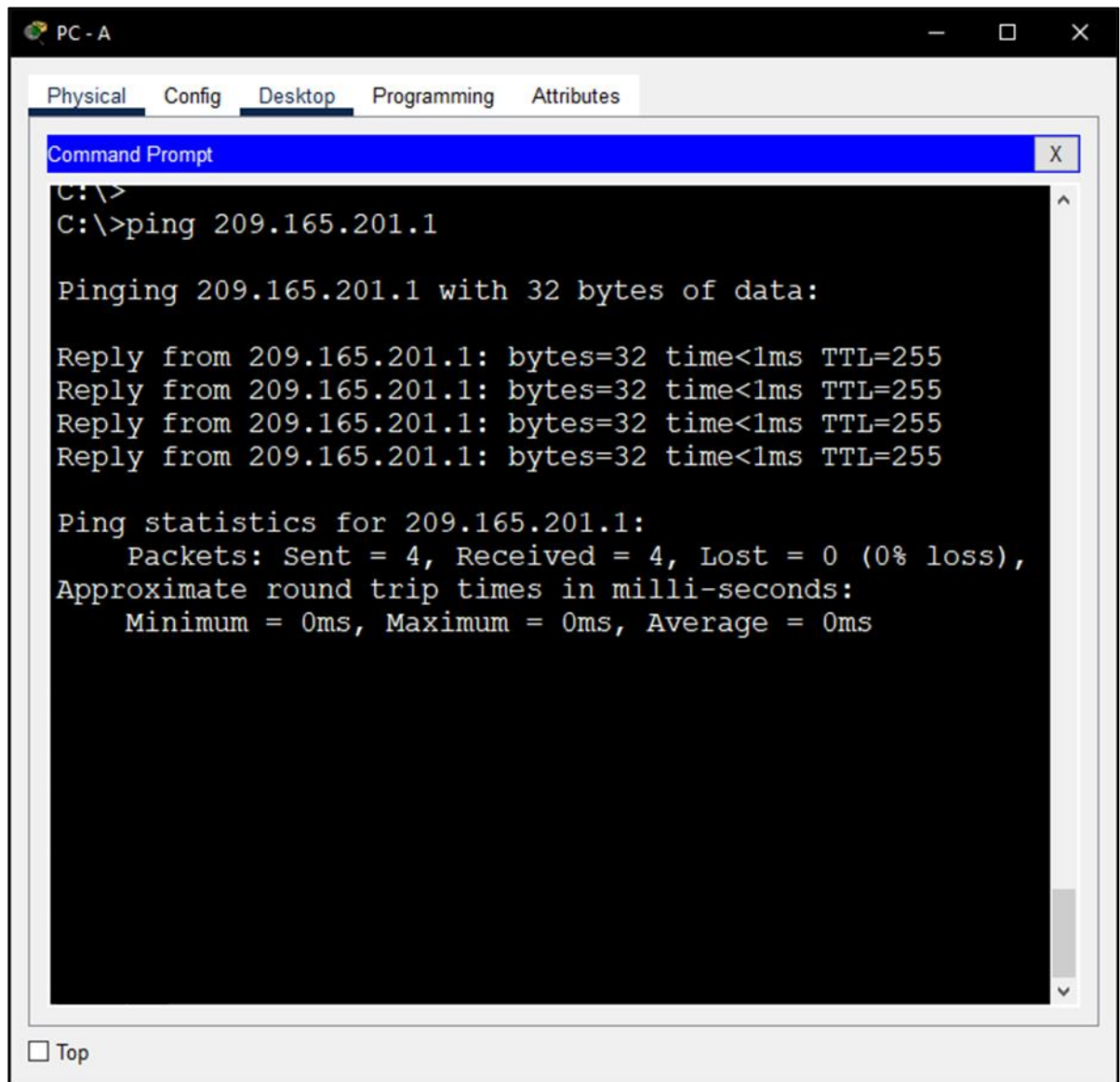
The image shows a screenshot of a Command Prompt window titled "PC - A". The window has tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes", with "Desktop" selected. The Command Prompt shows the following text:

```
C:\>  
C:\>ping 2001:DB8:ACAD:B::50  
  
Pinging 2001:DB8:ACAD:B::50 with 32 bytes of data:  
  
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=10ms  
TTL=127  
Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms  
TTL=127  
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=10ms  
TTL=127  
Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms  
TTL=127  
  
Ping statistics for 2001:DB8:ACAD:B::50:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 10ms, Average = 5ms
```

At the bottom left of the window, there is a "Top" button.

Fuente: Autoría propia.

Figura 22. Ping desde PC - A hacía Loopback 0 por IPv4



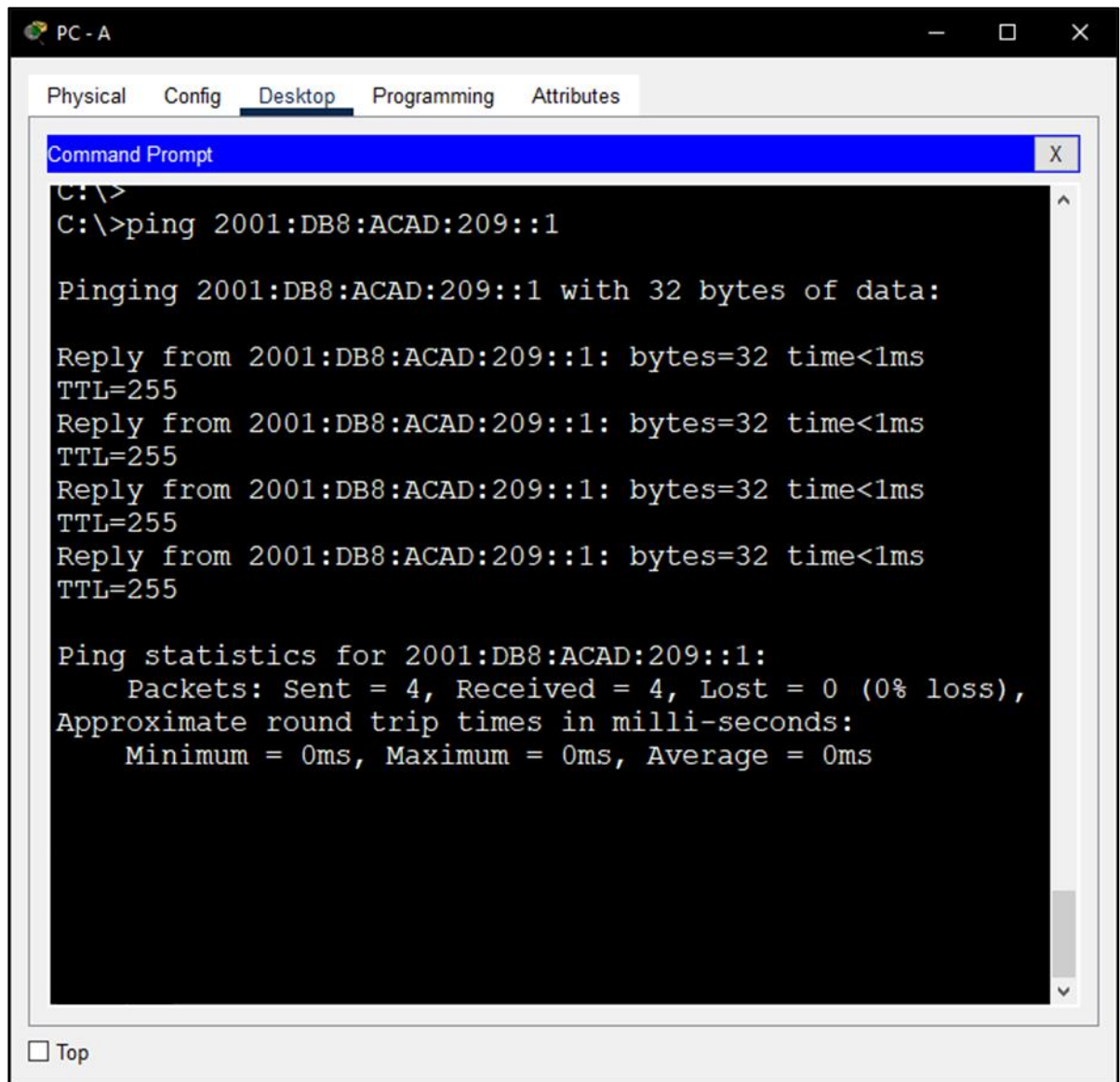
The image shows a screenshot of a Command Prompt window titled "PC - A". The window has tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes", with "Desktop" selected. The Command Prompt shows the following text:

```
C:\>  
C:\>ping 209.165.201.1  
  
Pinging 209.165.201.1 with 32 bytes of data:  
  
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255  
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255  
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255  
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255  
  
Ping statistics for 209.165.201.1:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

At the bottom left of the window, there is a "Top" button.

Fuente: Autoría propia.

Figura 23. Ping desde PC - A hacía Loopback 0 por IPv6



```
PC - A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>ping 2001:DB8:ACAD:209::1

Pinging 2001:DB8:ACAD:209::1 with 32 bytes of data:

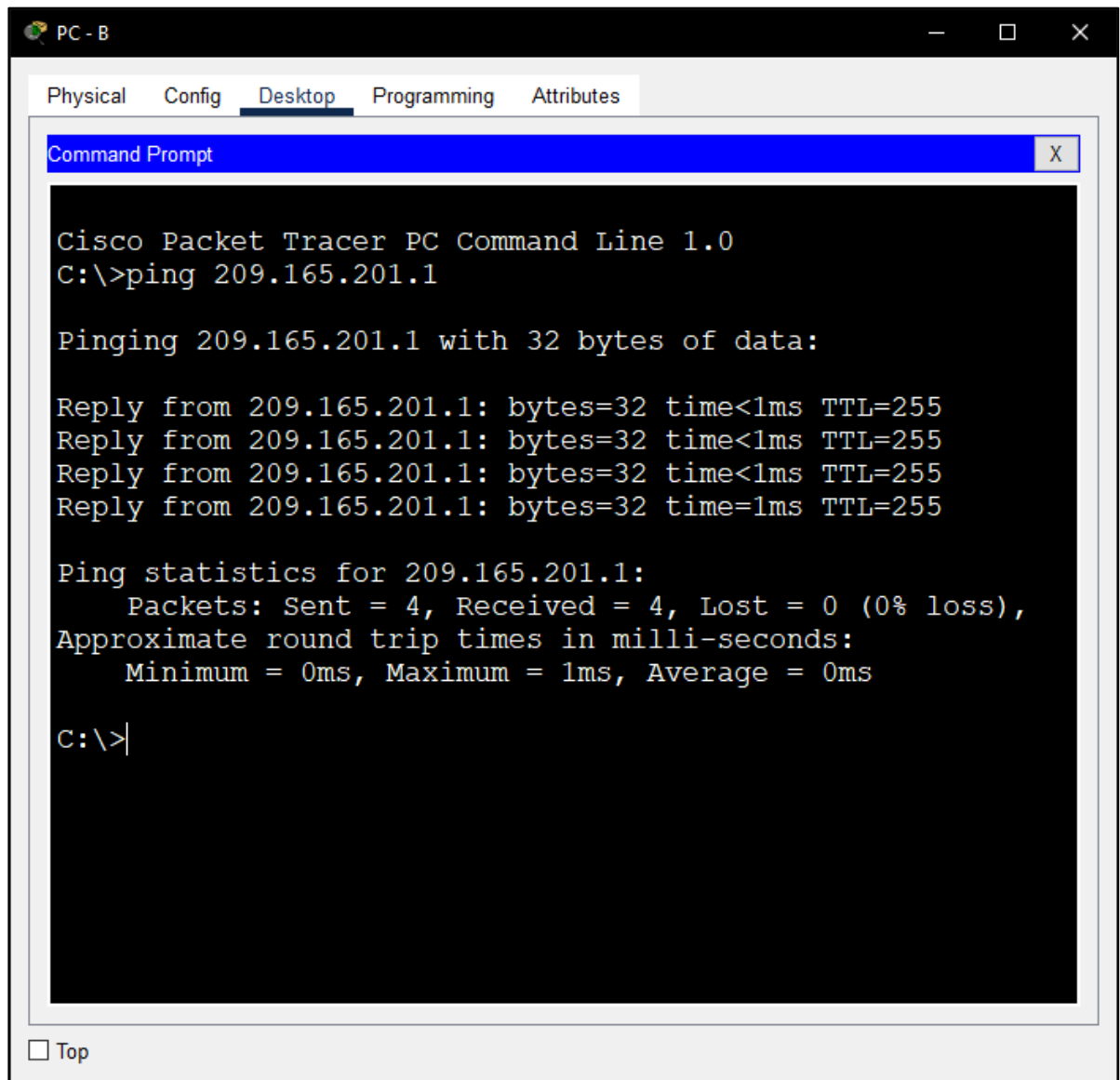
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms
TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms
TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms
TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms
TTL=255

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

 Top
```

Fuente: Autoría propia.

Figura 24. Ping desde PC - B hacía el Loopback 0 por IPv4



The image shows a screenshot of a Cisco Packet Tracer PC Command Prompt window. The window title is "PC - B" and it has tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, and a "Command Prompt" window is open. The text in the Command Prompt is as follows:

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

Pinging 209.165.201.1 with 32 bytes of data:

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

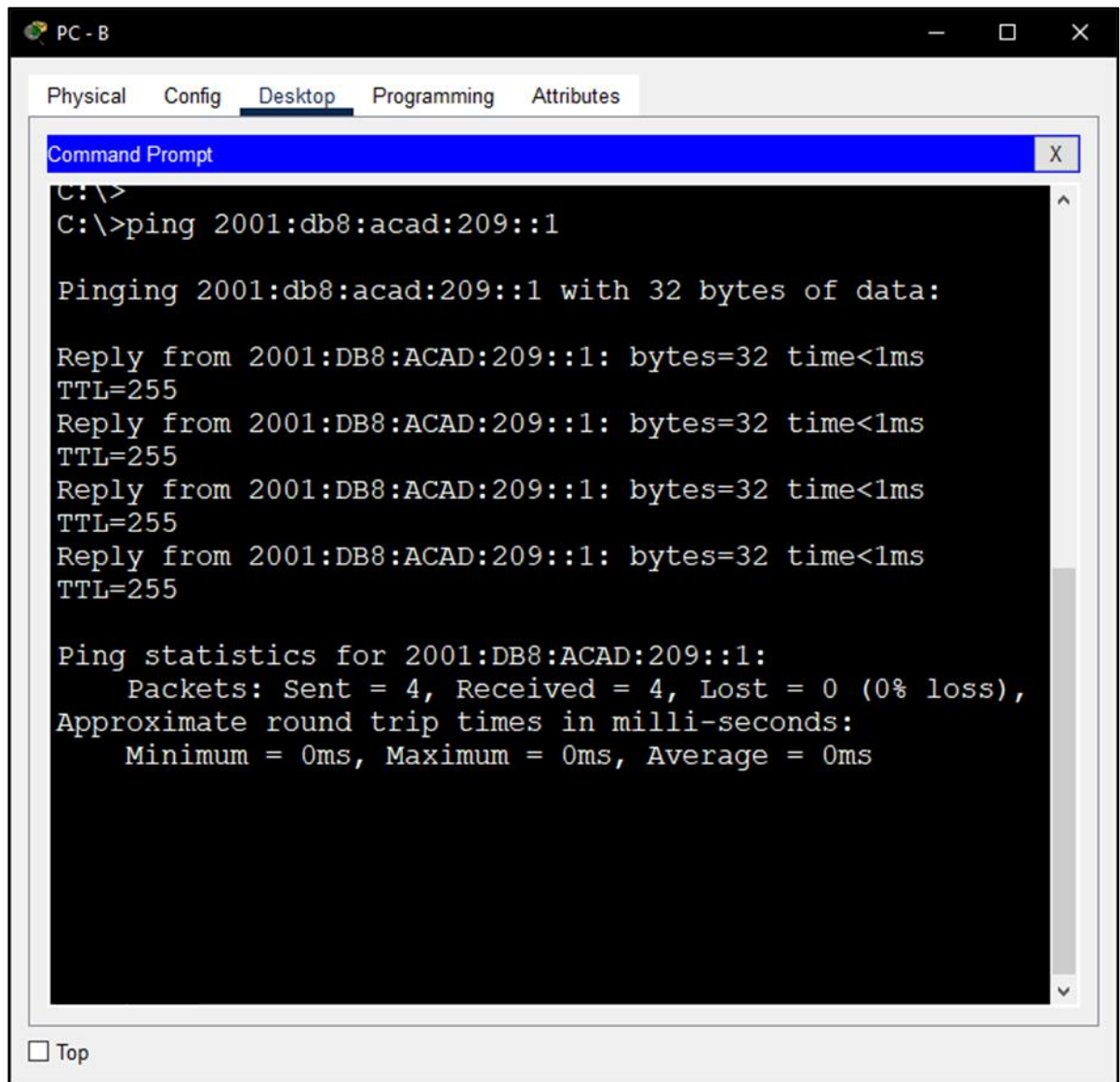
Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

At the bottom left of the Command Prompt window, there is a "Top" button.

Fuente: Autoría propia.

Figura 25. Ping desde PC - B hacía el Loopback 0 por IPv6



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

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

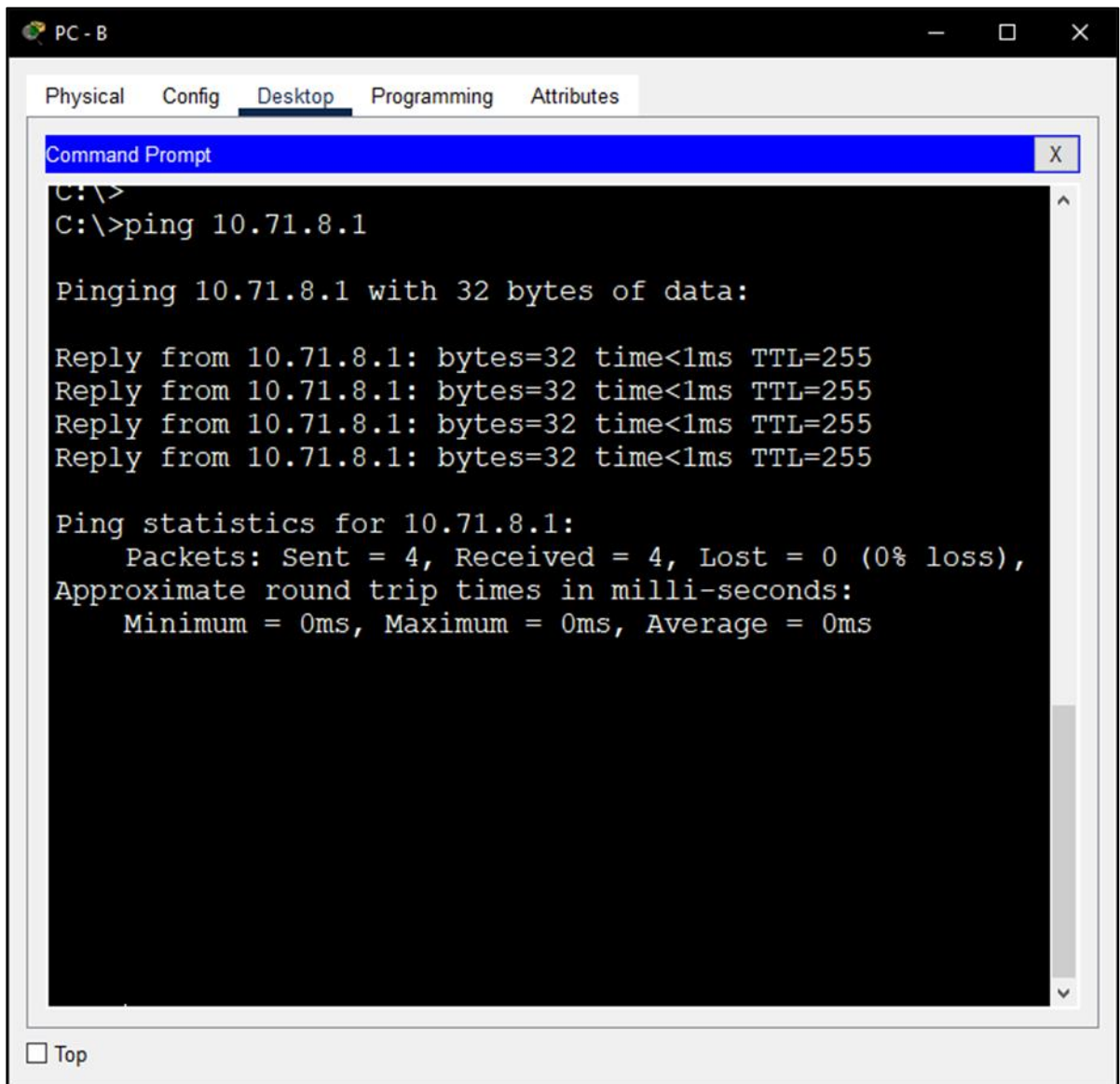
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms
TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms
TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms
TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms
TTL=255

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

 Top
```

Fuente: Autoría propia.

Figura 26. Ping desde PC - B hacía G0/0/1.20 por IPv4



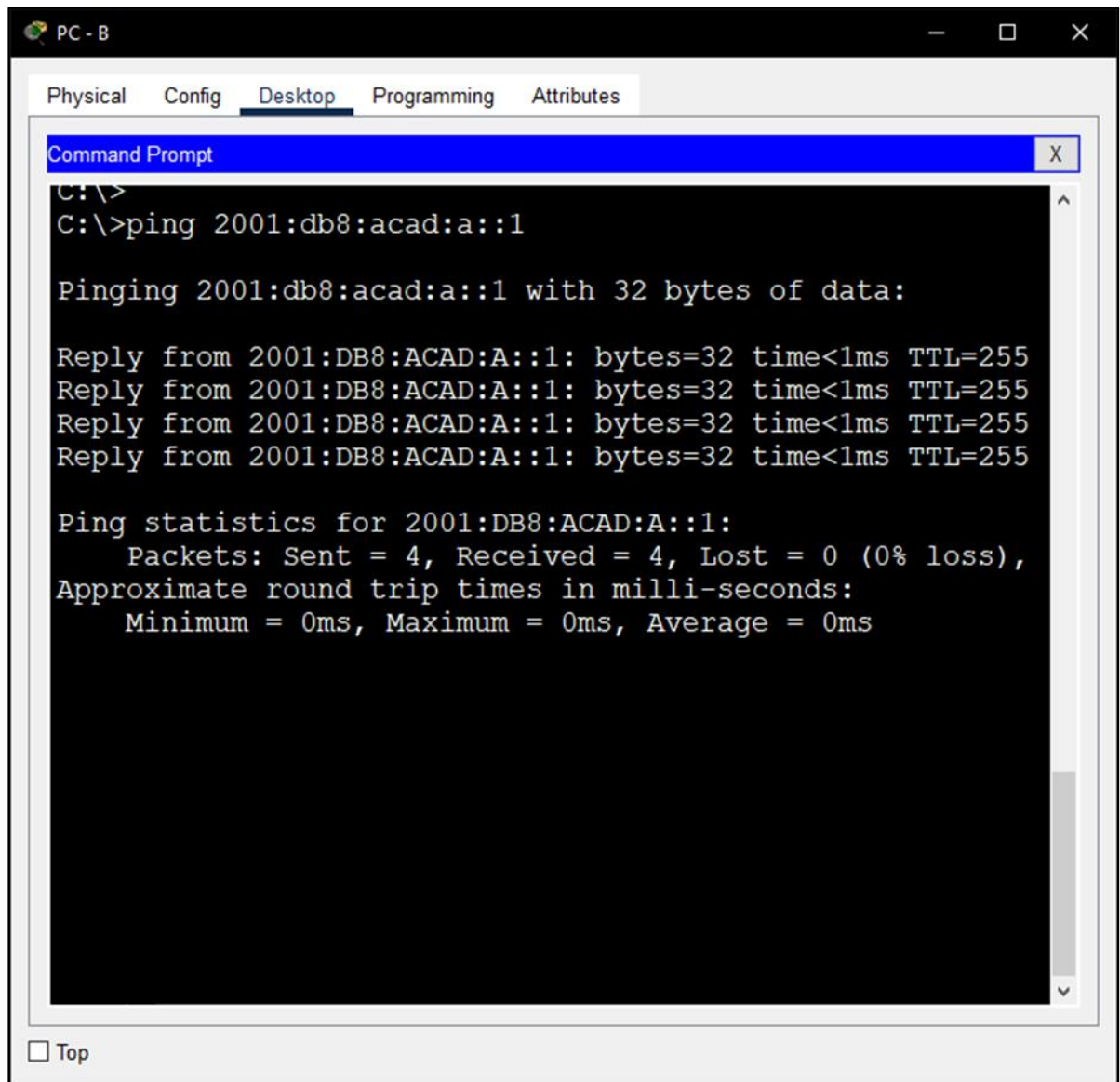
The image shows a screenshot of a PC-B Desktop environment. The window title is "PC - B" and it has standard Windows window controls (minimize, maximize, close). The desktop environment includes tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, displaying a "Command Prompt" window. The Command Prompt shows the following text:

```
C:\>  
C:\>ping 10.71.8.1  
  
Pinging 10.71.8.1 with 32 bytes of data:  
  
Reply from 10.71.8.1: bytes=32 time<1ms TTL=255  
Reply from 10.71.8.1: bytes=32 time<1ms TTL=255  
Reply from 10.71.8.1: bytes=32 time<1ms TTL=255  
Reply from 10.71.8.1: bytes=32 time<1ms TTL=255  
  
Ping statistics for 10.71.8.1:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

At the bottom left of the Command Prompt window, there is a "Top" button.

Fuente: Autoría propia.

Figura 27. Ping desde PC - B hacía G0/0/1.20 por IPv6



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

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

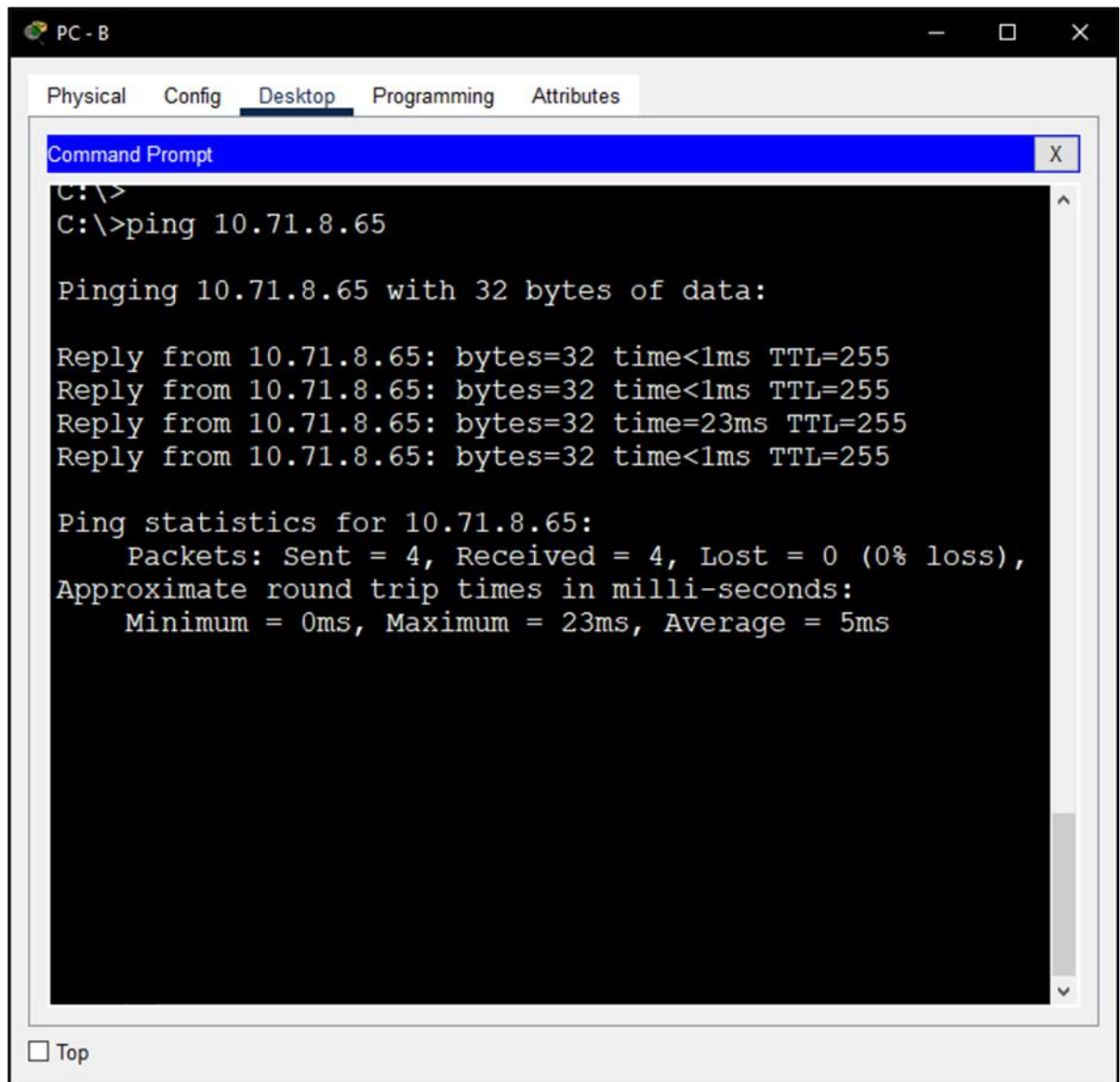
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255

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

 Top
```

Fuente: Autoría propia.

Figura 28. Ping desde PC - B hacía G0/0/1.30 por IPv4



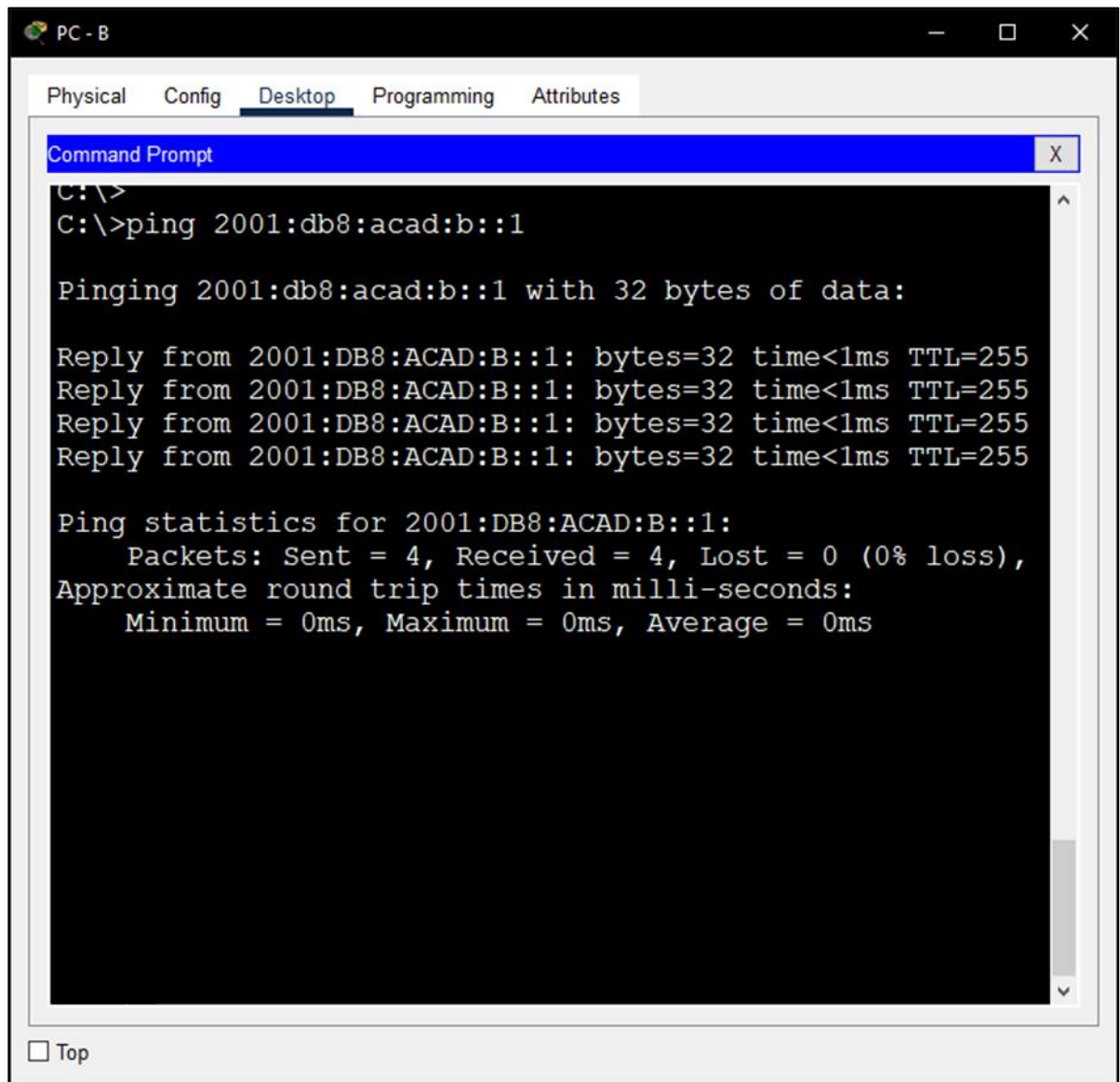
The image shows a screenshot of a PC-B desktop environment. The desktop has several tabs: Physical, Config, Desktop (selected), Programming, and Attributes. A Command Prompt window is open, displaying the following text:

```
C:\>  
C:\>ping 10.71.8.65  
  
Pinging 10.71.8.65 with 32 bytes of data:  
  
Reply from 10.71.8.65: bytes=32 time<1ms TTL=255  
Reply from 10.71.8.65: bytes=32 time<1ms TTL=255  
Reply from 10.71.8.65: bytes=32 time=23ms TTL=255  
Reply from 10.71.8.65: bytes=32 time<1ms TTL=255  
  
Ping statistics for 10.71.8.65:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 23ms, Average = 5ms
```

At the bottom left of the Command Prompt window, there is a checkbox labeled "Top".

Fuente: Autoría propia.

Figura 29. Ping desde PC - B hacía G0/0/1.30 por IPv6



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

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

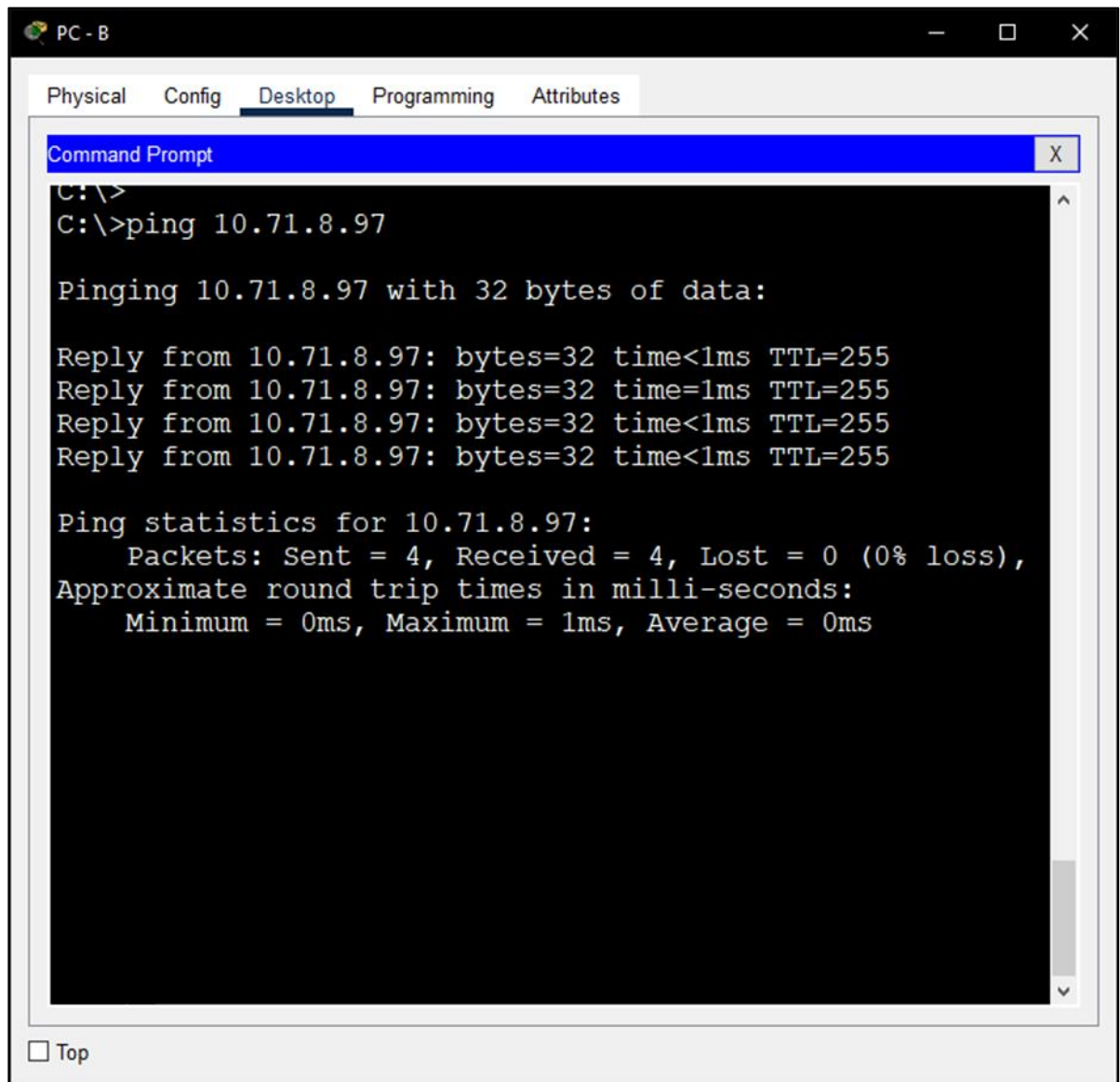
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255

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

 Top
```

Fuente: Autoría propia.

Figura 30. Ping desde PC - B hacía G0/0/1.41 por IPv4



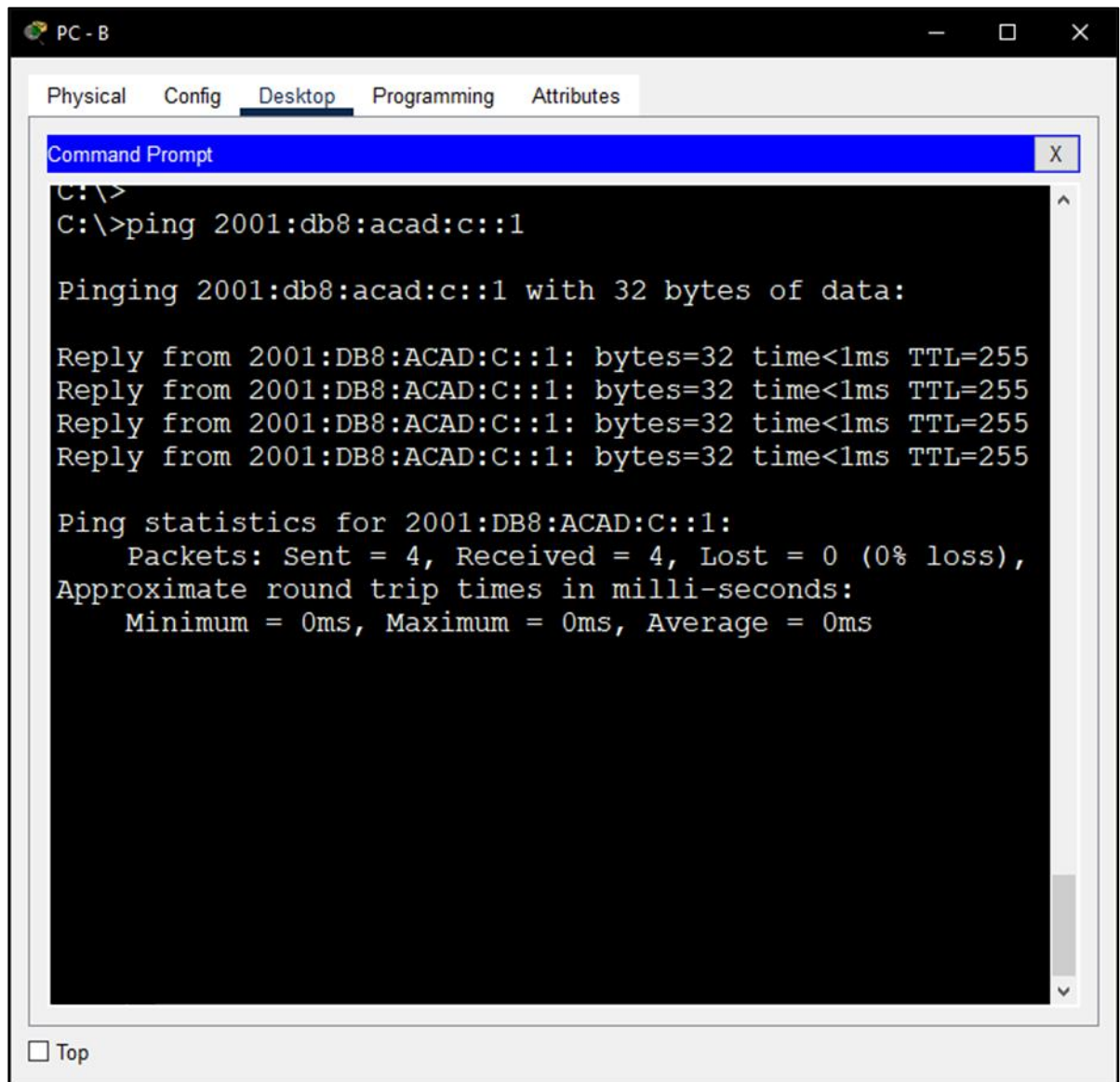
The image shows a screenshot of a PC-B desktop environment. The desktop has a menu bar with 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. A 'Command Prompt' window is open, displaying the following text:

```
C:\>  
C:\>ping 10.71.8.97  
  
Pinging 10.71.8.97 with 32 bytes of data:  
  
Reply from 10.71.8.97: bytes=32 time<1ms TTL=255  
Reply from 10.71.8.97: bytes=32 time=1ms TTL=255  
Reply from 10.71.8.97: bytes=32 time<1ms TTL=255  
Reply from 10.71.8.97: bytes=32 time<1ms TTL=255  
  
Ping statistics for 10.71.8.97:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

At the bottom left of the window, there is a 'Top' button.

Fuente: Autoría propia.

Figura 31. Ping desde PC - B hacía G0/0/1.40 por IPv6



The image shows a screenshot of a Command Prompt window titled "PC - B". The window has tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes", with "Desktop" selected. The Command Prompt shows the following text:

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

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

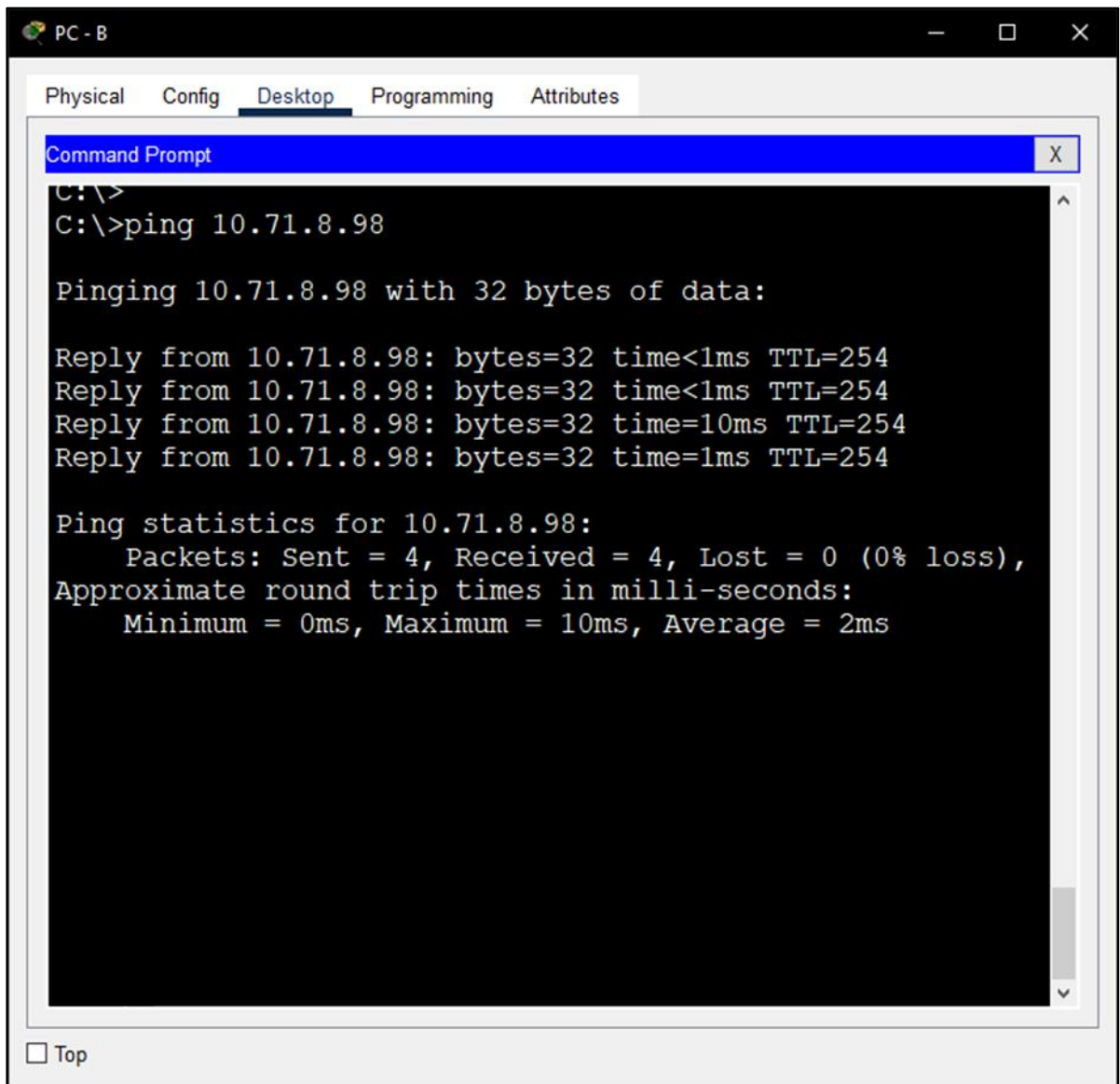
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255

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

At the bottom left of the window, there is a "Top" button.

Fuente: Autoría propia.

Figura 32. Ping desde PC - B hacía VLAN 40 del S1



The image shows a screenshot of a PC-B desktop environment. The desktop has several tabs: Physical, Config, Desktop (selected), Programming, and Attributes. A Command Prompt window is open, displaying the following text:

```
C:\>
C:\>ping 10.71.8.98

Pinging 10.71.8.98 with 32 bytes of data:

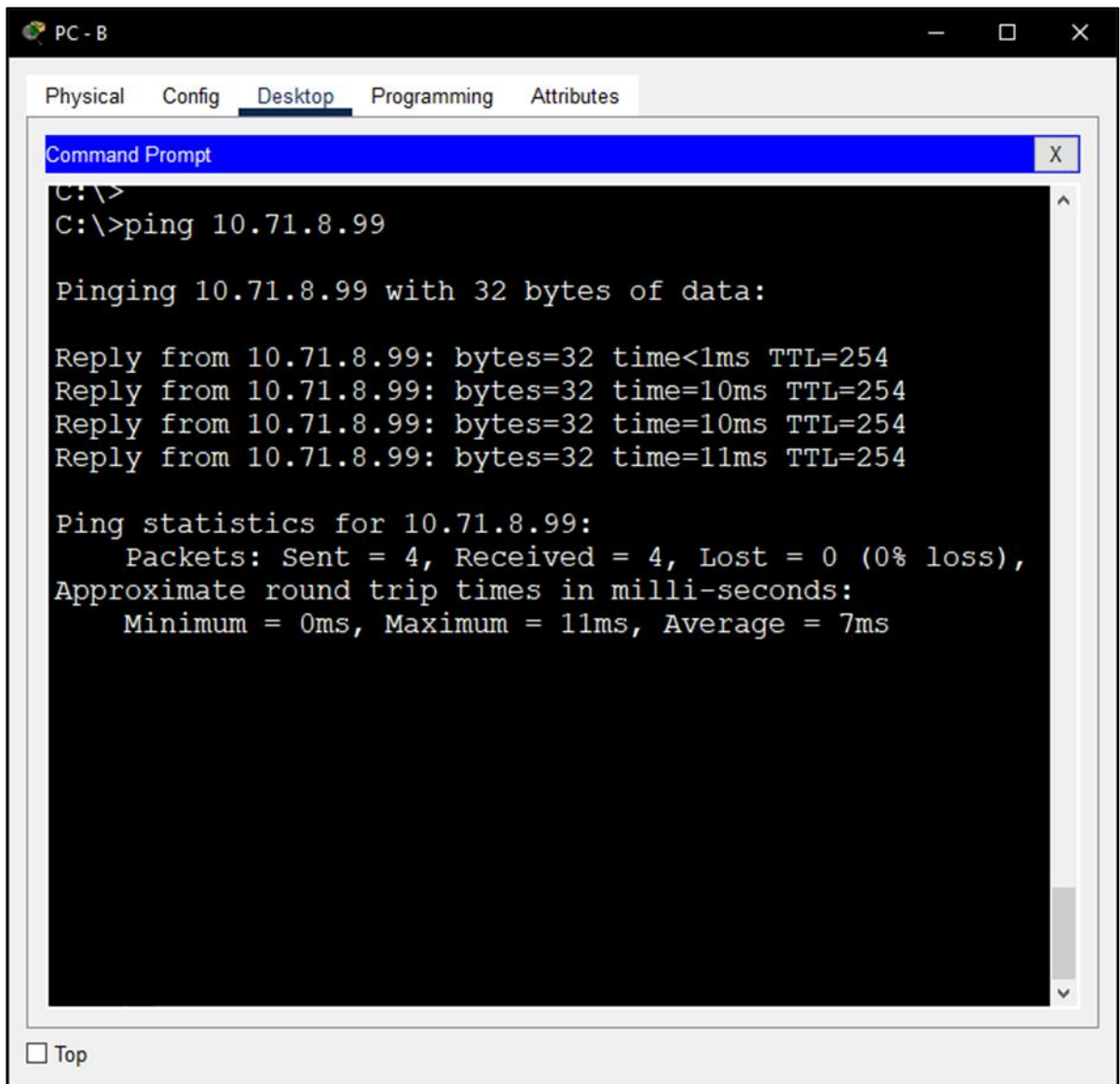
Reply from 10.71.8.98: bytes=32 time<1ms TTL=254
Reply from 10.71.8.98: bytes=32 time<1ms TTL=254
Reply from 10.71.8.98: bytes=32 time=10ms TTL=254
Reply from 10.71.8.98: bytes=32 time=1ms TTL=254

Ping statistics for 10.71.8.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

At the bottom left of the Command Prompt window, there is a checkbox labeled "Top".

Fuente: Autoría propia.

Figura 33. Ping desde PC - B hacía VLAN 40 del S2



```
PC - B
Physical  Config  Desktop  Programming  Attributes
Command Prompt
C:\>
C:\>ping 10.71.8.99

Pinging 10.71.8.99 with 32 bytes of data:

Reply from 10.71.8.99: bytes=32 time<1ms TTL=254
Reply from 10.71.8.99: bytes=32 time=10ms TTL=254
Reply from 10.71.8.99: bytes=32 time=10ms TTL=254
Reply from 10.71.8.99: bytes=32 time=11ms TTL=254

Ping statistics for 10.71.8.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 7ms

 Top
```

Fuente: Autoría propia.

De la figura 12 hasta la 33 se concluye que la conexión entre los diferentes dispositivos es correcta y el direccionamiento implementado tanto para IPv4 como IPv6 se ejecuta sin ningún problema, la creación del grupo DHCP para para la conectividad por IPv4 se aplicó correctamente.

CONCLUSIONES

La realización de los diferentes escenarios tuvo como objetivo el implementar los diferentes procedimientos que se realizan al momento de configurar una red con todo lo que esto conlleva, esto mediante un entorno que simula toda la metodología lo más fiel a la realidad posible.

Con el primer escenario se observa la importancia de implementar el Subneteo con VLSM ya que por medio de este se logra maximizar el uso de la red, adaptándola conforme las necesidades van surgiendo, llegando a escalar la red de manera óptima a diferencia del Subneteo tradicional, de igual forma el utilizar las diferentes metodologías de seguridad robustas ya sea por medio del acceso físico o virtual asegurando los dispositivos a posibles cambios no autorizados.

Finalmente para el desarrollo del escenario se observa la importancia de configurar el EtherChannel, comprendiendo que por medio de este si se conectan dos dispositivos intermedios directamente sin activar dicha función la conexión no se realizará ya que en caso de no estar configurado correctamente se puede generar diferentes problemas, sobrecarga de la red, tormenta de broadcast o un generar bucle infinito de envío de tramas, para esto se utiliza el modo de negociación LACP que permite al switch valga su redundancia negociar con el EtherChannel e implementarse en el momento que se considera oportuno.

LISTA DE REFERENCIA

CISCO SYSTEM INC. “Asignación de direcciones IPv4.” [Sitio Web] [Consulta: 19 de octubre de 2022]. Disponible en : <https://contenthub.netacad.com/itn/11.0.1>

CISCO SYSTEM INC. “Asignación de direcciones IPv6.” [Sitio Web] [Consulta: 19 de octubre de 2022]. Disponible en : <https://contenthub.netacad.com/itn/12.0.1>

CISCO SYSTEM INC. “Capa de aplicación.” [Sitio Web] [Consulta: 19 de octubre de 2022]. Disponible en : <https://contenthub.netacad.com/itn/15.0.1>

CISCO SYSTEM INC. “Capa de enlace de datos.” [Sitio Web] [Consulta: 19 de octubre de 2022]. Disponible en : <https://contenthub.netacad.com/itn/6.0.1>

CISCO SYSTEM INC. “Capa de red.” [Sitio Web] [Consulta: 19 de octubre de 2022]. Disponible en : <https://contenthub.netacad.com/itn/8.0.1>

CISCO SYSTEM INC. “Capa de transporte.” [Sitio Web] [Consulta: 19 de octubre de 2022]. Disponible en : <https://contenthub.netacad.com/itn/14.0.1>

CISCO SYSTEM INC. “Configuración básica de un router.” [Sitio Web] [Consulta: 19 de octubre de 2022]. Disponible en <https://contenthub.netacad.com/itn/10.0.1>

CISCO SYSTEM INC. “Crear una red pequeña.” [Sitio Web] [Consulta: 19 de octubre de 2022]. Disponible en : <https://contenthub.netacad.com/itn/17.0.1>

CISCO SYSTEM INC. “Fundamentos de seguridad de la red.” [Sitio Web] [Consulta: 19 de octubre de 2022]. Disponible en : <https://contenthub.netacad.com/itn/16.0.1>

CISCO SYSTEM INC. “ICMP.” [Sitio Web] [Consulta: 19 de octubre de 2022]. Disponible en : <https://contenthub.netacad.com/itn/13.0.1>

CISCO SYSTEM INC. “Las redes en la actualidad.” [Sitio Web] [Consulta: 19 de octubre de 2022]. Disponible en : <https://contenthub.netacad.com/itn/5.0.1>

CISCO SYSTEM INC. “Resolución de dirección.” [Sitio Web] [Consulta: 19 de octubre de 2022]. Disponible en : <https://contenthub.netacad.com/itn/9.0.1>

CISCO SYSTEM INC. “Switching Ethernet.” [Sitio Web] [Consulta: 19 de octubre de 2022]. Disponible en : <https://contenthub.netacad.com/itn/7.0.1>

CISCO SYSTEM INC. “Capa física.” [Sitio Web] [Consulta: 19 de octubre de 2022]. Disponible en : <https://contenthub.netacad.com/itn/4.0.1>

CISCO SYSTEM INC. “Configuración básica de switches y terminales.” [Sitio Web] [Consulta: 19 de octubre de 2022]. Disponible en <https://contenthub.netacad.com/itn/2.0.1>

CISCO SYSTEM INC. “Las redes en la actualidad.” [Sitio Web] [Consulta: 19 de octubre de 2022]. Disponible en <https://contenthub.netacad.com/itn/1.0.1>

CISCO SYSTEM INC. “Protocolos y modelos.” [Sitio Web] [Consulta: 19 de octubre de 2022]. Disponible en : <https://contenthub.netacad.com/itn/3.0.1>

ANEXOS

Anexo A: Descarga de archivos de simulación escenario A

Enlace:

https://unadvirtualedu-my.sharepoint.com/:u:/g/personal/ragredot_unadvirtual_edu_co/Ee3amWODM9xCgyq9SUJ3mikBy465hzmra3uqcOml6mEcfw?e=QWxp2a

Anexo B: Descarga de archivos de simulación escenario B

Enlace:

https://unadvirtualedu-my.sharepoint.com/:u:/g/personal/ragredot_unadvirtual_edu_co/EWtAcmWPFUpCjYtWfgNwDloBmrQZy2OEDje8FMOpPEXPBQ?e=RYJYKg