

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

VIVIANA MERCADO BENITEZ

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

2022

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

VIVIANA MERCADO BENITEZ

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

Director

PAULITA FLOR

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

2022

Nota de aceptación

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Córdoba, 9 de Diciembre de 2022

CONTENIDO

CONTENIDO	4
LISTA DE TABLAS	5
LISTA DE FIGURAS.....	6
GLOSARIO	7
RESUMEN.....	8
ABSTRACT.....	9
INTRODUCCIÓN.....	10
ESCENARIO 1.....	11
ESCENARIO 2.....	23
CONCLUSIONES	57
BIBLIOGRAFIA.....	58
ANEXOS.....	59

LISTA DE TABLAS

Tabla 1 Tabla de direccionamiento Escenario 1	12
Tabla 2 Tareas configuración R1	13
Tabla 3 Tareas configuración S1	16
Tabla 4 Configuración de red PC-A	18
Tabla 5 Configuración de red PC-B	18
Tabla 6 Verificación de conectividad dispositivos de red	19
Tabla 7 Nombres VLAN Escenario 2	24
Tabla 8 Tabla de direccionamiento Escenario 2	25
Tabla 9 Tareas de configuración R1	29
Tabla 10 Tareas de configuración S1 Y S2.....	33
Tabla 11 Configuración de las VLAN, Trunking, EtherChannel en S1	38
Tabla 12 Configuración de las VLAN, Trunking, EtherChannel en S2	38
Tabla 13 Configuración del soporte de host en R1	43
Tabla 14 Configuración de host PC-A.....	44
Tabla 15 Configuración de host PC-B.....	45
Tabla 16 Verificación de conectividad dispositivos de red	45

LISTA DE FIGURAS

Figura 1 Topología Escenario 1	11
Figura 2 Escenario 1 en Packet Tracer.....	11
Figura 3 Verificación conectividad desde PC-A parte 1	19
Figura 4 Verificación conectividad desde PC-A parte 2	21
Figura 5 Verificación conectividad desde PC-B	22
Figura 6 Topología Escenario 2.....	23
Figura 7 Escenario 2 en Packet Tracer.....	24
Figura 8 Verificación conectividad desde PC-A parte 1	48
Figura 9 Verificación conectividad desde PC-A parte 2	49
Figura 10 Verificación conectividad desde PC-A parte 3	50
Figura 11 Verificación conectividad desde PC-A parte 4	51
Figura 12 Verificación conectividad desde PC-A parte 5	52
Figura 13 Verificación conectividad desde PC-B parte 1	53
Figura 14 Verificación conectividad desde PC-B parte 2	54
Figura 15 Verificación conectividad desde PC-B parte 3	55
Figura 16 Verificación conectividad desde PC-B parte 4	56

GLOSARIO

Dirección IP: Una serie de números que identifican lógicamente un dispositivo en una red. Los dispositivos se conectan entre sí a través de sus direcciones IP, que pueden expresarse en decimal o binario. Hay dos tipos de direcciones IP: IPV4 e IPV6.¹

DHCP: (Protocolo de configuración dinámica de host). Protocolo de configuración de servidor dinámico. Un protocolo que usan las computadoras para obtener información de configuración. DHCP permite asignar direcciones IP a las computadoras sin que los administradores tengan que configurar la información de la computadora en la base de datos del servidor.²

DNS: Sistema de nombres de dominio. DNS es el servicio que asocia nombres de dominio con sus direcciones IP asociadas.³

SSH: un protocolo que admite la comunicación segura entre dos sistemas mediante una arquitectura cliente/servidor, lo que permite a los usuarios conectarse de forma remota a un servidor.⁴

VLAN: (red de área local virtual o LAN virtual) es una red de área local que agrupa las computadoras de forma lógica en lugar de físicamente. De hecho, la arquitectura física administra la comunicación entre diferentes computadoras dentro de una red de área local.⁵

VTY: La serie vty permite el acceso a dispositivos Cisco a través de Telnet. De forma predeterminada, muchos conmutadores de Cisco admiten hasta 16 líneas vty numeradas del 0 al 15.⁶

¹ «Dirección IP: Qué es, para qué sirve y cómo funciona», OpenWebinars.net, 16 de julio de 2021.
<https://openwebinars.net/blog/direccion-ip-que-es-para-que-sirve-y-como-funciona/> (accedido 9 de diciembre de 2022).

² «Protocolo DHCP: Qué es, funcionamiento y ejemplos para configurarlo», *RedesZone*.
<https://www.redeszone.net/tutoriales/internet/que-es-protocolo-dhcp/> (accedido 9 de diciembre de 2022).

³ «Conceptos básicos de DNS - Ayuda de Administrador de Google Workspace».
<https://support.google.com/a/answer/48090?hl=es-419> (accedido 9 de diciembre de 2022).

⁴ «Configuración de SSH en Switch y Router Cisco | eClassVirtual - Cursos Cisco en línea».
<https://eclassvirtual.com/configuracion-ssh-switch-router-cisco/> (accedido 9 de diciembre de 2022).

⁵ «Qué son las VLAN, para qué sirven y cómo funcionan con ejemplos de uso», *RedesZone*.

<https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/> (accedido 9 de diciembre de 2022).

⁶ «TODO SOBRE REDES: VTY», *TODO SOBRE REDES*. <https://todosobreredesdedatos.blogspot.com/p/vty.html>
(accedido 9 de diciembre de 2022).

RESUMEN

Este trabajo analiza la evaluación y resolución de la prueba de habilidades prácticas del diploma Cisco CCNA. Los conocimientos adquiridos durante el transcurso del diploma, como el enrutamiento, los protocolos, las configuraciones básicas y la seguridad en los dispositivos de red se identifican mediante el desarrollo de dos escenarios en el programa Packet Tracer. El primer escenario implica la configuración básica de nombres, asignación de credenciales, encriptación de contraseñas y configuraciones de consola. A continuación, se utiliza VLSM para calcular el direccionamiento basado en una IP fija mediante la alteración de ciertos parámetros, que se describen más adelante. Estos rangos se asignan a las interfaces de los routers y switches y se realizan pruebas de ping para asegurar la conexión entre ellos. En la segunda situación, se siguen los mismos pasos, pero esta vez utilizando sub-interfaces, VLANs y configurando las interfaces para que funcionen en modo troncal, aplicando además el protocolo IPv6 a cada uno de los gadgets.

Palabras Clave: CISCO, CCNA, Conmutación, Enrutamiento, Redes, Protocolos.

ABSTRACT

This paper analyzes the evaluation and resolution of the practical skills test of the Cisco CCNA diploma. The knowledge acquired during the course of the diploma, such as routing, protocols, basic configurations and security in network devices are identified through the development of two scenarios in the Packet Tracer program. The first scenario involves basic naming configuration, credential mapping, password encryption, and console configurations. VLSM is then used to calculate addressing based on a fixed IP by altering certain parameters, which are described below. These ranges are assigned to the interfaces of the routers and switches and ping tests are performed to ensure the connection between them. In the second situation, the same steps are followed, but this time using sub-interfaces, VLANs and configuring the interfaces to work in trunk mode, also applying the IPv6 protocol to each of the gadgets.

Keywords: CISCO, CCNA, Routing, Switching, Networking, Protocols.

INTRODUCCIÓN

El propósito de este trabajo es desarrollar una prueba de habilidad que consta de dos escenarios. El primer escenario usa el esquema de direccionamiento IPv4 para configurar una red pequeña, y el segundo escenario usa conexiones duales IPv4 e IPv6 para enrutar entre VLAN, DHCP, Etherchannels y protección. Se basa en protocolos de Internet con tecnología de red central que permite que las computadoras y otros dispositivos tecnológicos se comuniquen entre sí. Esto funciona con la última versión de IP. La primera es una dirección IPv4, un número de 32 bits que identifica de forma única una interfaz de red en el sistema, escrito en decimal. Actualmente opera en una red global de más de 4 mil millones de dispositivos conectados, cada parte de Internet que conocemos y usamos todos los días. Sin embargo, todas estas conexiones conllevan grandes riesgos. Ahí es donde entra en juego IPv6, conocida como versión 2. Es una nueva versión del Protocolo de Internet que reemplaza a IPv4 y permite más conexiones, brindando a los usuarios más conectividad, seguridad y durabilidad. En otras palabras, ofrece más funciones y ayuda a lograr los objetivos globales, también permite tener más control sobre el tráfico de Internet, asignar direcciones a dispositivos específicos y permite tener más control entre diferentes computadoras. Crear una conexión segura. Tradicionalmente, al diseñar una red, crea subredes dividiendo la red en varias subredes, con cada subred funcionando de forma independiente para mantener los datos en el lugar correcto y de manera eficiente.

En lugar de mejorar la organización de la red, funciona creando redes lógicas separadas mediante la implementación de LAN virtuales (VLAN), un método utilizado para segmentar la infraestructura física pieza por pieza. Por lo tanto, en este trabajo, se desarrolla utilizando la herramienta Packet Tracer para los dos escenarios, uno es diseñar una red con dos LAN con direcciones ipv4, crear esa configuración para cada dispositivo se hará realidad. En cualquier dispositivo que tenga una red desplegada. En el segundo escenario, la red está configurada y administrada de forma segura para admitir la conectividad de enrutamiento dual IPv4/IPv6. Además, se implementan 5 VLAN, se configura 1 EtherChannel para permitir la agregación de diferentes adaptadores Ethernet y se implementa seguridad de puerto adicional para evitar que se reenvíen dispositivos desconocidos.

ESCENARIO 1

En este escenario se pide configurar la topología de red que se muestra en la figura 1.

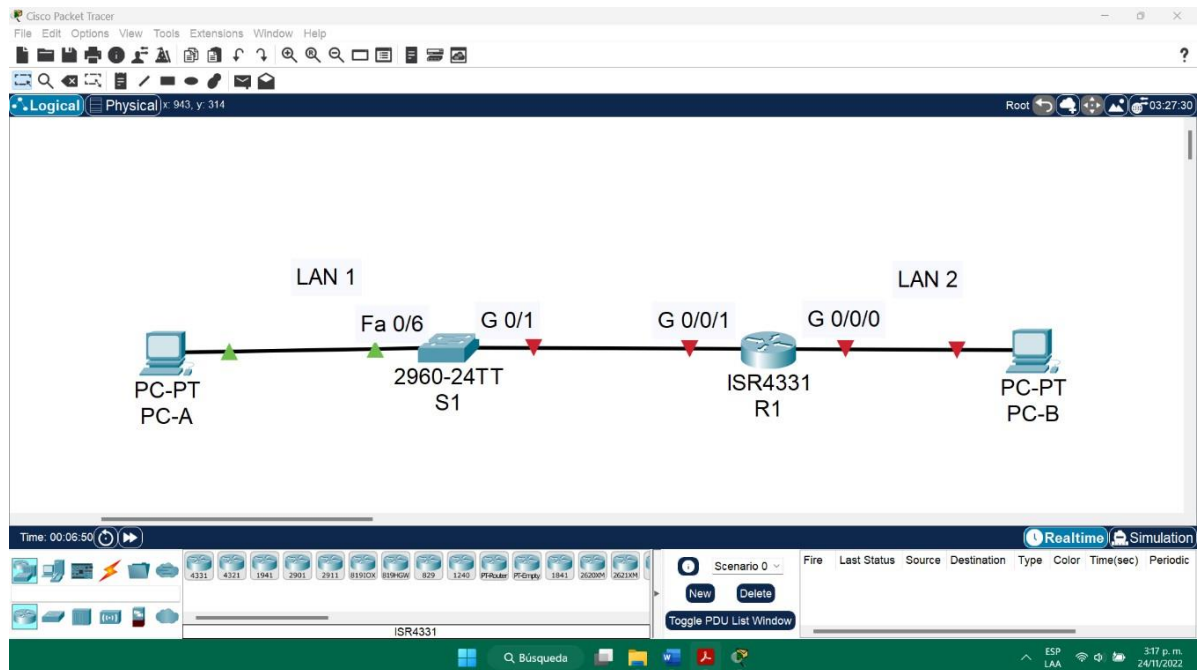
Figura 1 Topología Escenario 1



Fuente: Documento guía

Para el desarrollo de este escenario se usa el software Packet Tracer y se simula la topología como se muestra en la figura 2.

Figura 2 Escenario 1 en Packet Tracer



Fuente: Propia

Lo siguiente es desarrollar el esquema de direccionamiento IPv4, respondiendo los requerimientos de la tabla 1.

Tabla 1 Tabla de direccionamiento Escenario 1

Item	Requerimiento	Desarrollo
Dirección de Red	172.XY.3.0 donde XY corresponde a los dos últimos dígitos de mi cedula	172.19.3.0
Requerimiento de host subred LAN1	60	172.19.3.0/26 172.19.3.1 – 172.19.3.62 255.255.255.192
Requerimiento de host subred LAN2	20	172.19.3.64/27 172.19.3.65 – 172.19.3.94 255.255.255.224
R1 G 0/0/1	Ultima dirección de host de la subred LAN1	172.19.3.62 255.255.255.192
R1 G 0/0/0	Ultima dirección de host de la subred LAN2	172.19.3.94 255.255.255.224
S1 SV1	Segunda dirección de host de la subred LAN1	172.19.3.2 255.255.255.192
PC-A	Decima dirección de host de la subred LAN1	172.19.3.10 255.255.255.192
PC-B	Decima dirección de host de la subred LAN2	172.19.3.74 255.255.255.224

Fuente: Documento guía

En la siguiente parte se configurarán los aspectos básicos de los dispositivos de red R1 y S1, esto se realizará mediante la conexión de consola. En la tabla 2 se indican las tareas a cumplir para configuración de R1.

Tabla 2 Tareas configuración R1

Tarea	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R1
Nombre de dominio	ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Establecer la longitud mínima para las contraseñas	10 caracteres
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Contraseña: admin1pass
Configure el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	
Cifrar las 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.
Configuración de interface G0/0/0	Establecer la descripción Establecer la dirección IPv4 Activar la interfaz.
Configuración de interface G0/0/1	Establecer la descripción Establecer la dirección IPv4 Activar la interfaz.
Generar una clave de cifrado RSA	Módulo de 1024 bits

Fuente: Documento

A continuación, se presenta cada línea de comando usada para la configuración de R1.

```
Router>en
```

```
Router#config t
```

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

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

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

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

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

```
R1(config)#service password-encryption
```

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

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

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

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

```
R1(config)#security password min-length 10
```

```
R1(config)#username admin password admin1pass
```

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

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

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

```
R1(config)#line vty 0 4
```

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

```
R1(config-line)#transport input ssh
```

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

```
R1(config)#service password-encryption
R1(config)#banner motd $ R1 - Nombre completo - Programa: Ingenieria $
R1(config)#int g0/0/0
R1(config-if)#description subred LAN2
R1(config-if)#ip address 172.19.3.94 255.255.255.224
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#int g0/0/1
R1(config-if)#description Subred LAN1
R1(config-if)#ip address 172.19.3.62 255.255.255.192
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#crypto key generate 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]
R1(config)#end
R1#copy running-config startup-config
```

Luego se realizan las configuraciones básicas en S1, cumpliendo las tareas de la tabla 3.

Tabla 3 Tareas configuración S1

Tarea	Especificación
Desactivar la búsqueda DNS	
Nombre del switch	S1
Nombre de dominio	ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Apagar todos los puertos sin usar	F0/1-4, F0/7-24, G0/1-2
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Contraseña: admin1pass
Configure el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	
Cifrar las 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.
Generar una clave de cifrado RSA	Módulo de 1024 bits
Configure la interfaz de administración (SVI) en VLAN1	Establecer la descripción Establecer la dirección IPv4

Fuente: Documento guía

A continuación, se presenta cada línea de comando usada para la configuración de S1.

Switch>en

Switch#config t

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


```
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#ip domain-name ccna-sa.com
S1(config)#enable secret ciscoenpass
S1(config)#service password-encryption
S1(config)#line console 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit
S1(config)#int range f0/1-4, f0/7-24, g0/2
S1(config-if-range)#shutdown
S1(config-if-range)#exit
S1(config)#username admin password admin1pass
S1(config)#line vty 0 4
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd $R1, Nombre completo - Programa: Ingenieria $
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]

S1(config)#int vlan 1

S1(config-if)#description VLAN1

S1(config-if)#ip address 172.19.3.2 255.255.255.192

S1(config-if)#no shutdown

S1(config-if)#exit

S1(config)#ip default-gateway 172.19.3.62

S1(config)#end

S1#copy running-config startup-config

El siguiente paso es configurar los equipos host PC-A y PC-B de acuerdo con la tabla de direccionamiento, esta configuración se verifica con el comando ipconfig /all y se registra en la tabla 4 para el PC-A y en la tabla 5 para el PC-B.

Tabla 4 Configuración de red PC-A

Configuración de red PC-A	
Descripción	PC-A FastEthernet 0
Dirección física	00E0.B088.607D
Dirección IPv4	172.19.3.10
Mascara de subred	255.255.255.192
Puerta de enlace IPv4 predeterminada	172.19.3.62

Fuente: Documento guía

Tabla 5 Configuración de red PC-B

Configuración de red PC-B	
Descripción	PC-B FastEthernet 0
Dirección física	00E0.8F69.780B

Dirección IPv4	172.19.3.74
Mascara de subred	255.255.255.224
Puerta de enlace IPv4 predeterminada	172.19.3.94

Fuente: Documento guía

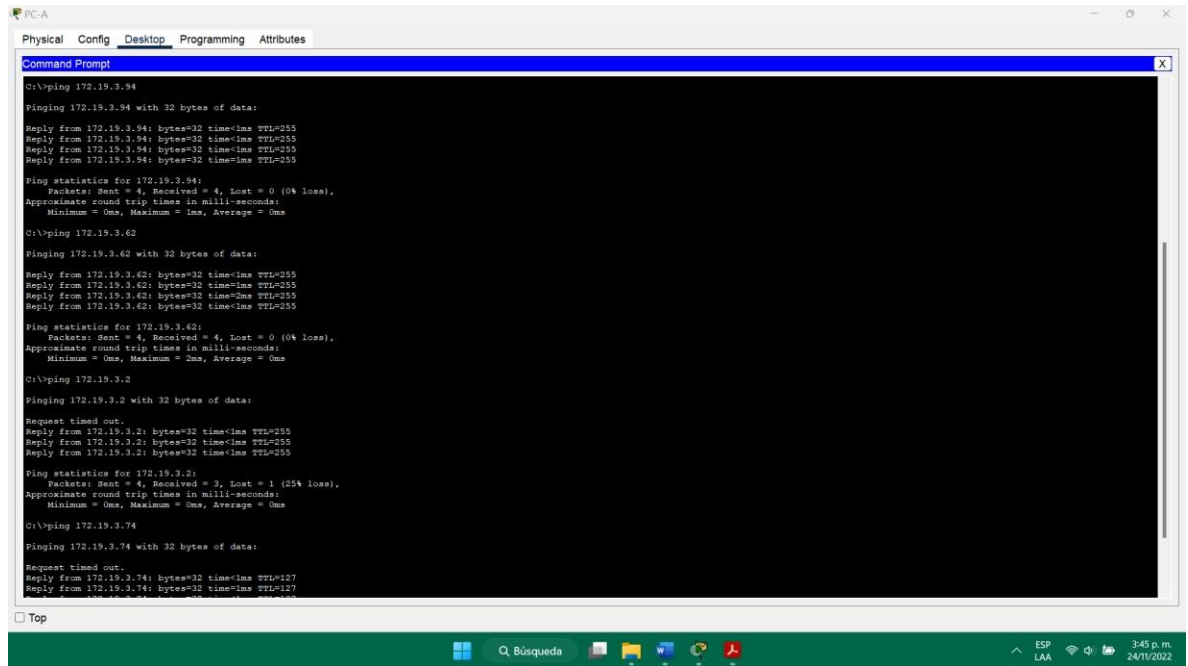
Para terminar con este escenario se procede a probar y verificar la conectividad de extremo a extremo haciendo uso del comando ping, las verificaciones son registradas en la tabla 6.

Tabla 6 Verificación de conectividad dispositivos de red.

Desde	A	Dirección IP	Resultados de ping
PC-A	R1 G 0/0/0	172.19.3.94	Exitoso: 0 paquetes perdidos, ver figura 3.
	R1 G 0/0/1	172.19.3.62	Exitoso: 0 paquetes perdidos, ver figura 3.
	S1 VLAN 1	172.19.3.2	Exitoso: 25% de paquetes perdidos, esto pasa por ser la primera comunicación con ese punto, si se vuelve a ejecutar el ping será 100% exitoso. Ver figura 3.
	PC-B	172.19.3.74	Exitoso: 25% de paquetes perdidos, esto pasa por ser la primera comunicación con ese punto, si se vuelve a ejecutar el ping será 100% exitoso. Ver figura 4.
PC-B	R1 G 0/0/0	172.19.3.94	Exitoso: 0 paquetes perdidos, ver figura 5.
	R1 G 0/0/1	172.19.3.62	Exitoso: 0 paquetes perdidos, ver figura 5.
	S1 VLAN 1	172.19.3.2	Exitoso: 50% de paquetes perdidos, esto pasa por ser la primera comunicación con ese punto, si se vuelve a ejecutar el ping será 100% exitoso. Ver figura 5.

Fuente: Documento guía, Resultados propios

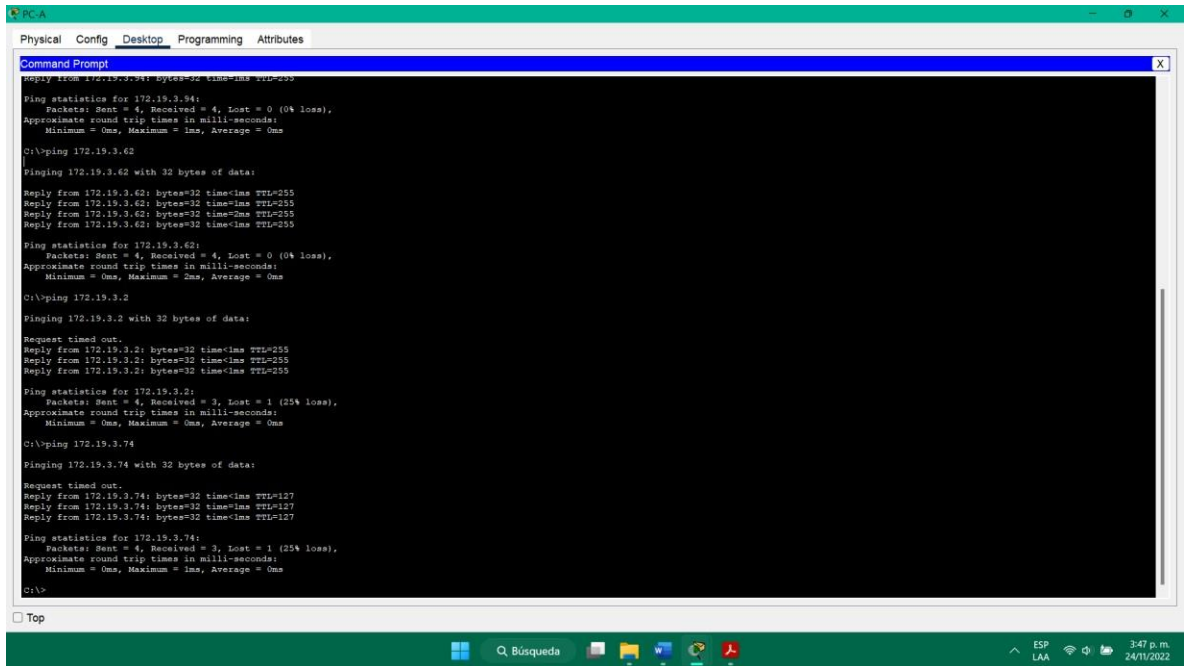
Figura 3 Verificación conectividad desde PC-A parte 1



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.19.3.94
Pinging 172.19.3.94 with 32 bytes of data:
Reply from 172.19.3.94: bytes=32 time<ms TTL=255
Reply from 172.19.3.94: bytes=32 time<ms TTL=255
Reply from 172.19.3.94: bytes=32 time<ms TTL=255
Reply from 172.19.3.94: bytes=32 time<ms TTL=255
Ping statistics for 172.19.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 172.19.3.62
Pinging 172.19.3.62 with 32 bytes of data:
Reply from 172.19.3.62: bytes=32 time<ms TTL=255
Reply from 172.19.3.62: bytes=32 time<ms TTL=255
Reply from 172.19.3.62: bytes=32 time<ms TTL=255
Reply from 172.19.3.62: bytes=32 time<ms TTL=255
Ping statistics for 172.19.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 172.19.3.2
Pinging 172.19.3.2 with 32 bytes of data:
Request timed out.
Reply from 172.19.3.2: bytes=32 time<ms TTL=255
Reply from 172.19.3.2: bytes=32 time<ms TTL=255
Reply from 172.19.3.2: bytes=32 time<ms TTL=255
Ping statistics for 172.19.3.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 172.19.3.74
Pinging 172.19.3.74 with 32 bytes of data:
Request timed out.
Reply from 172.19.3.74: bytes=32 time<ms TTL=127
Reply from 172.19.3.74: bytes=32 time<ms TTL=127
Reply from 172.19.3.74: bytes=32 time<ms TTL=127
Reply from 172.19.3.74: bytes=32 time<ms TTL=127
Ping statistics for 172.19.3.74:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Top
```

Fuente: Propia

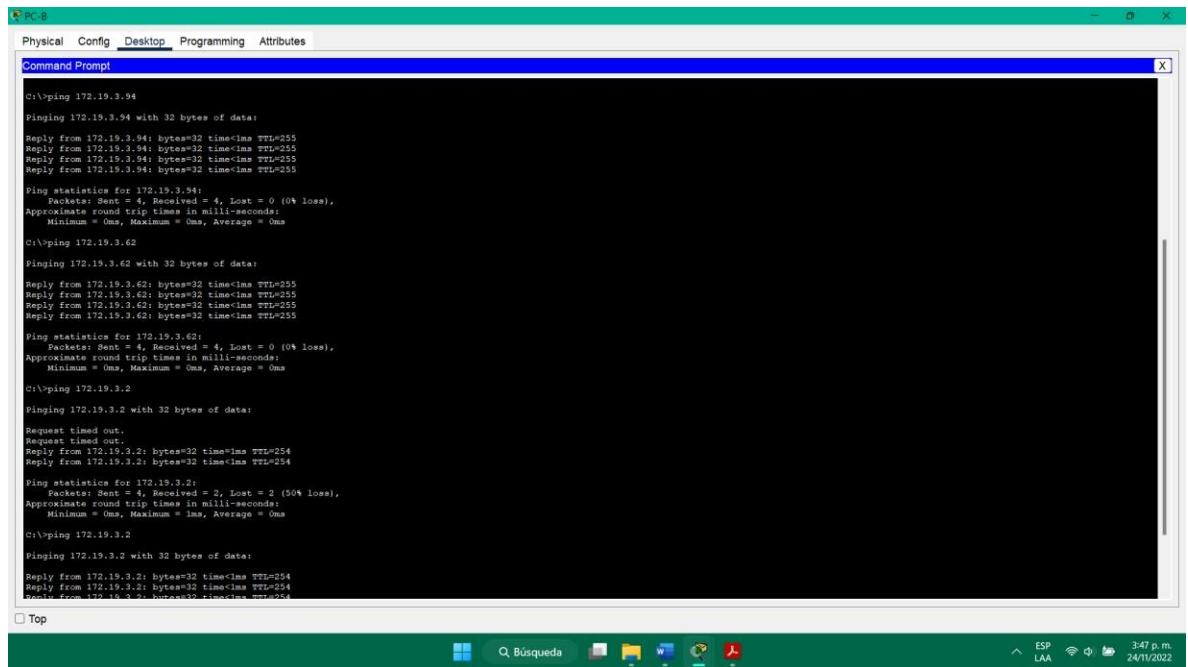
Figura 4 Verificación conectividad desde PC-A parte 2



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 172.19.3.94: bytes=32 time=1ms TTL=255
Ping statistics for 172.19.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 172.19.3.62
Pinging 172.19.3.62 with 32 bytes of data:
Reply from 172.19.3.62: bytes=32 time<1ms TTL=255
Reply from 172.19.3.62: bytes=32 time<1ms TTL=255
Reply from 172.19.3.62: bytes=32 time<1ms TTL=255
Reply from 172.19.3.62: bytes=32 time<1ms TTL=255
Ping statistics for 172.19.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 172.19.3.2
Pinging 172.19.3.2 with 32 bytes of data:
Request timed out.
Reply from 172.19.3.2: bytes=32 time<1ms TTL=255
Reply from 172.19.3.2: bytes=32 time<1ms TTL=255
Reply from 172.19.3.2: bytes=32 time<1ms TTL=255
Ping statistics for 172.19.3.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 172.19.3.74
Pinging 172.19.3.74 with 32 bytes of data:
Request timed out.
Reply from 172.19.3.74: bytes=32 time<1ms TTL=127
Reply from 172.19.3.74: bytes=32 time<1ms TTL=127
Reply from 172.19.3.74: bytes=32 time<1ms TTL=127
Ping statistics for 172.19.3.74:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
```

Fuente: Propia

Figura 5 Verificación conectividad desde PC-B



```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.19.3.94
Pinging 172.19.3.94 with 32 bytes of data:
Reply from 172.19.3.94: bytes=32 time<ms TTL=255
Reply from 172.19.3.94: bytes=32 time<ms TTL=255
Reply from 172.19.3.94: bytes=32 time<ms TTL=255
Reply from 172.19.3.94: bytes=32 time<ms TTL=255
Ping statistics for 172.19.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 172.19.3.62
Pinging 172.19.3.62 with 32 bytes of data:
Reply from 172.19.3.62: bytes=32 time<ms TTL=255
Reply from 172.19.3.62: bytes=32 time<ms TTL=255
Reply from 172.19.3.62: bytes=32 time<ms TTL=255
Reply from 172.19.3.62: bytes=32 time<ms TTL=255
Ping statistics for 172.19.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 172.19.3.2
Pinging 172.19.3.2 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 172.19.3.2: bytes=32 time<ms TTL=254
Reply from 172.19.3.2: bytes=32 time<ms TTL=254
Ping statistics for 172.19.3.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 172.19.3.2
Pinging 172.19.3.2 with 32 bytes of data:
Reply from 172.19.3.2: bytes=32 time<ms TTL=254
Reply from 172.19.3.2: bytes=32 time<ms TTL=254
Reply from 172.19.3.2: bytes=32 time<ms TTL=254
Reply from 172.19.3.2: bytes=32 time<ms TTL=254
Top
```

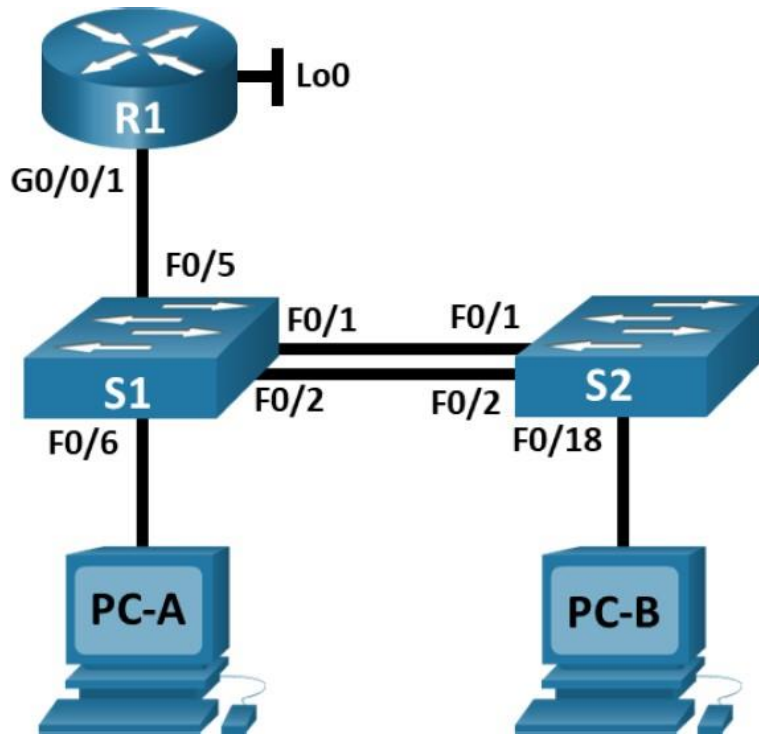
Fuente: Propia

Los resultados muestran que el direccionamiento fue preciso, lo que permite que la red esté preparada para utilizar protocolos alternativos si se requiere ampliar el escenario.

ESCENARIO 2

En este escenario se pide configurar la topología de red que se muestra en la figura 6.

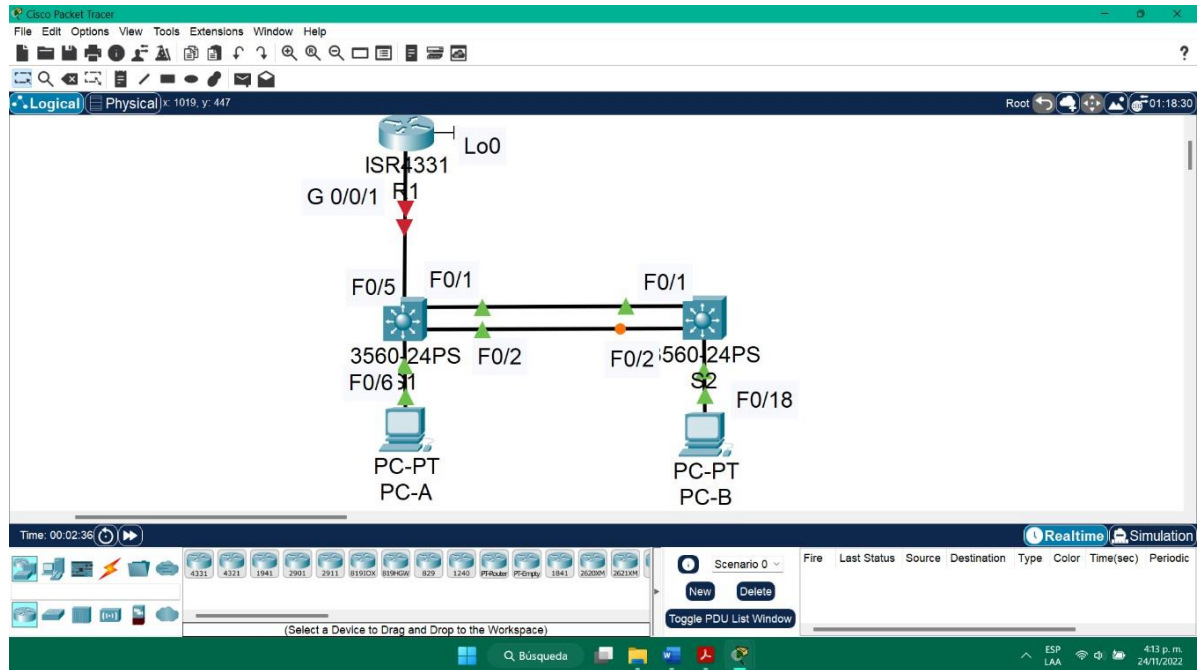
Figura 6 Topología Escenario 2



Fuente: Documento guía

Para el desarrollo de este escenario se usa el software Packet Tracer y se simula la topología como se muestra en la figura 7.

Figura 7 Escenario 2 en Packet Tracer



Fuente: Propia

La guía proporciona una tabla con los nombres de la VLAN del escenario dos, tabla 7, y la tabla de direccionamiento requerida para la configuración de la red, tabla 8.

Tabla 7 Nombres VLAN Escenario 2

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

Fuente: Documento guía

Tabla 8 Tabla de direccionamiento Escenario 2

Dispositivo / Interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G 0/0/1.20	10.19.8.1 /26	No corresponde
	2001:db8:acad:a::1 /64	No corresponde
R1 G 0/0/1.30	10.19.8.65 /27	No corresponde
	2001:db8:acad:b::1 /64	No corresponde
R1 G 0/0/1.40	10.19.8.97 /29	No corresponde
	2001:db8:acad:c::1 /64	No corresponde
R1 G 0/0/1.56	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209::1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c::98 /64	No corresponde
	Fe80::98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8:acad:c::99 /64	No corresponde
	Fe80::99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a::50 /64	Fe80::1
PC-B NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b::50 /64	Fe80::1

Fuente: Documento guía

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

Lo siguiente que hay que hacer inicializar y volver a cargar los R1,S1 y S2. También hay que borrar las configuraciones de inicio y las VLAN de los

dispositivos, para eso se colocan los siguientes comandos en la consola según el dispositivo.

R1

```
Router>enable
```

```
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#delete vlan.dat
```

```
Delete filename [vlan.dat]?
```

```
Delete flash:/vlan.dat? [confirm]
```

```
%Error deleting flash:/vlan.dat (No such file or directory)
```

```
Router#reload
```

S1 y S2

```
Switch>enable
```

```
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#delete vlan.dat
```

Delete filename [vlan.dat]?

Delete flash:/vlan.dat? [confirm]

%Error deleting flash:/vlan.dat (No such file or directory)

Switch#reload

Después de recargar los S1 y S2, se configura la plantilla SDM para que admita IPv6 con los siguientes comandos en cada dispositivo y se vuelven a recargar los dispositivos.

Switch>enable

Switch#show sdm prefer

The current template is "desktop default" template.

The selected template optimizes the resources in the switch to support this level of features for

8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:	6K
number of IPv4 IGMP groups + multicast routes:	1K
number of IPv4 unicast routes:	8K
number of directly-connected IPv4 hosts:	6K
number of indirect IPv4 routes:	2K
number of IPv4 policy based routing aces:	0
number of IPv4/MAC qos aces:	0.5K
number of IPv4/MAC security aces:	1K

Switch#configure terminal

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

```
Switch(config)#sdm prefer ?
```

```
access      Access bias
```

```
default     Default bias
```

```
dual-ipv4-and-ipv6 Support both IPv4 and IPv6
```

```
routing     Unicast bias
```

```
vlan        Vlan bias
```

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

```
Switch(config)#exit
```

```
Switch#reload
```

```
Switch>en
```

```
Switch#show sdm prefer
```

The current template is "desktop IPv4 and IPv6 default" template.

The selected template optimizes the resources in

the switch to support this level of features for

8 routed interfaces and 1024 VLANs.

```
number of unicast mac addresses:          2K
```

```
number of IPv4 IGMP groups + multicast routes: 1K
```

```
number of IPv4 unicast routes:           3K
```

```
number of directly-connected IPv4 hosts:  2K
```

```
number of indirect IPv4 routes:          1K
```

```
number of IPv6 multicast groups:         1.125k
```

number of directly-connected IPv6 addresses:	2K
number of indirect IPv6 unicast routes:	1K
number of IPv4 policy based routing aces:	0
number of IPv4/MAC qos aces:	0.5K
number of IPv4/MAC security aces:	1K
number of IPv6 policy based routing aces:	0
number of IPv6 qos aces:	0.625k
number of IPv6 security aces:	0.5K

El siguiente paso es realizar las configuraciones básicas de R1 cumpliendo las tareas de la tabla 9.

Tabla 9 Tareas de configuración R1

Tarea	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R1
Nombre de dominio	ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	class
Contraseña de acceso a la consola	cisco
Establecer la longitud mínima para las contraseñas	5 caracteres
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar VTY solo aceptando SSH	
Cifrar las contraseñas de texto no cifrado	
Configure un MOTD Banner	Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.
Habilitar el routing IPv6	

Configurar interfaz G0/0/1 y subinterfaces	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como fe80: :1 Establece la dirección IPv6. Activar la interfaz.
Configure el Loopback0 interface	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como fe80::1
Generar una clave de cifrado RSA	Módulo de 1024 bits

Fuente: Documento guía

A continuación, se presenta cada línea de comando usada para la configuración de R1.

Router>en

Router#config t

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

Router(config)#no ip domain-lookup

Router(config)#hostname R1

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

R1(config)#enable password class

R1(config)#service password-encryption

R1(config)#line console 0

R1(config-line)#password cisco

```
R1(config-line)#login
R1(config-line)#exit
R1(config)#security passwords min-length 5
R1(config)#enable password cisco
R1(config)#username admin privilege 15 secret admin1pass
R1(config)#line console 0
R1(config-line)#login local
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd $R1 – Viviana Mercado - Programa: Ingenieria de
sistemas $
R1(config)#ipv6 unicast-routing
R1(config)#interface g0/0/1.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#description Docente
R1(config-subif)#ip address 10.19.8.1 255.255.255.192
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64
R1(config-subif)#no shutdown
```

```
R1(config-subif)#exit
R1(config)#interface g0/0/1.30
R1(config-subif)#description Estudiantes
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 10.19.8.65 255.255.255.224
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#interface g0/0/1.40
R1(config-subif)#description Invitados
R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#ip address 10.19.8.97 255.255.255.248
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#interface g0/0/1.56
R1(config-subif)#encapsulation dot1q 56 native
R1(config-subif)#description Vlan 56 Native
R1(config-subif)#exit
R1(config)#interface g0/0/1
```



```

R1(config-if)#no shutdown

R1(config-if)#exit

R1(config)#interface loopback 0

R1(config-if)#description Loopback 0

R1(config-if)#ip address 209.165.201.1 255.255.255.224

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

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

R1(config-if)#no shutdown

R1(config-if)#exit

R1(config)#crypto key generate rsa

% You already have RSA keys defined named R1.ccna-sa.com .

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]

R1(config)#end

R1#copy running-config startup-config

```

El siguiente paso es realizar las configuraciones básicas en los S1 y S2 cumpliendo las tareas de la tabla 10.

Tabla 10 Tareas de configuración S1 Y S2

Tarea	Especificación
-------	----------------

Desactivar la búsqueda DNS.	
Nombre del switch	S1 o S2, según proceda
Nombre de dominio	ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	class
Contraseña de acceso a la consola	cisco
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	
Cifrar las contraseñas de texto no cifrado	
Configurar un MOTD Banner	Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.
Generar una clave de cifrado RSA	Módulo de 1024 bits
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2 Establecer la dirección IPv6 de capa 3
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4

Fuente: Documento guía

A continuación, se presenta cada línea de comando usada para la configuración de S1.

Switch>en

Switch#config t

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

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

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

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

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

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

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

```
S1(config-line)#login
```

```
S1(config-line)#exit
```

```
S1(config)#username admin password admin1pass
```

```
S1(config)#line vty 0 15
```

```
S1(config-line)#login local
```

```
S1(config-line)#transport input ssh
```

```
S1(config-line)#exit
```

```
S1(config)#service password-encryption
```

```
S1(config)#banner motd $S1 – Viviana Mercado - Programa: Ingenieria de sistemas$
```

```
S1(config)#crypto key generate rsa
```

```
% You already have RSA keys defined named S1.ccna-sa.com .
```

```
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]

S1(config)#interface vlan 40

S1(config-if)#ip address 10.19.8.98 255.255.255.248

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

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

S1(config-if)#no shutdown

S1(config-if)#exit

S1(config)#ip default-gateway 10.19.8.97

S1(config)#end

S1#copy running-config startup-config

A continuación, se presenta cada línea de comando usada para la configuración de S2.

Switch>en

Switch#config t

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

Switch(config)#no ip domain-lookup

Switch(config)#hostname S2

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

S2(config)#enable secret class

S2(config)#line console 0

S2(config-line)#password cisco

```
S2(config-line)#login
S2(config-line)#exit
S2(config)#username admin password admin1pass
S2(config)#line vty 0 15
S2(config-line)#login local
S2(config-line)#transport input ssh
S2(config-line)#exit
S2(config)#service password-encryption
S2(config)#banner motd $S2 – Viviana Mercado - Programa: Ingenieria de
sistemas $
S2(config)#crypto key generate rsa
% You already have RSA keys defined named S2.ccna-sa.com .
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
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
S2(config)#interface vlan 40
S2(config-if)#ip address 10.19.8.99 255.255.255.248
S2(config-if)#ipv6 address fe80::99 link-local
S2(config-if)#ipv6 address 2001:db8:acad:c::99/64
S2(config-if)#no shutdown
```

S2(config-if)#exit

S2(config)#ip default-gateway 10.19.8.97

S2(config)#end

S2#copy running-config startup-config

Lo siguiente es configurar las VLAN, Trunking, EtherChannel cumpliendo las tareas de las tablas 11 y 12 para los dispositivos S1 y S2 respectivamente.

Tabla 11 Configuración de las VLAN, Trunking, EtherChannel en S1

Tarea	Especificación
Crear VLAN	VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6
Configurar la seguridad del puerto en los puertos de acceso	Permitir 4 direcciones MAC
Proteja todas las interfaces no utilizadas	Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar

Fuente: Documento guía

Tabla 12 Configuración de las VLAN, Trunking, EtherChannel en S2

Tarea	Especificación
Crear VLAN	VLAN 20, nombre Docentes

	VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1 y F0/2
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso del host para la VLAN 3	Interfaz F0/18
Configure port-security en los access ports	permite 4 MAC addresses
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar

Fuente: Documento guía

A continuación, se presenta cada línea de comando usada para la configuración de S1.

S1#config t

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

S1(config)#vlan 20

S1(config-vlan)#name Docentes

S1(config-vlan)#exit

S1(config)#vlan 30

S1(config-vlan)#name Estudiantes

S1(config-vlan)#exit

S1(config)#vlan 40

S1(config-vlan)#name Invitados

```
S1(config-vlan)#exit
S1(config)#vlan 50
S1(config-vlan)#name Usuarios
S1(config-vlan)#exit
S1(config)#vlan 56
S1(config-vlan)#name Native
S1(config-vlan)#exit
S1(config)#interface range f0/1-2, f0/5
S1(config-if-range)#switchport trunk encapsulation dot1q
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk Native vlan 56
S1(config-if-range)#interface range f0/1-2
S1(config-if-range)#channel-group 1 mode active
S1(config-if-range)#interface port-channel 1
S1(config-if)#exit
S1(config)#interface f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 20
S1(config-if)#switchport port-security maximum 4
S1(config-if)#exit
S1(config)#interface range f0/3-4, f0/7-24, g0/1-2
S1(config-if-range)#switchport mode access
```



```
S1(config-if-range)#switchport access vlan 50
S1(config-if-range)#description VLAN 50
S1(config-if-range)#shutdown
S1(config-if-range)#exit
S1(config)#interface range f0/1-2
S1(config-if-range)#no shutdown
S1(config-if-range)#end
S1#copy running-config startup-config
```

A continuación, se presenta cada línea de comando usada para la configuración de S2.

```
S2#config t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#vlan 20
S2(config-vlan)#name Docentes
S2(config-vlan)#exit
S2(config)#vlan 30
S2(config-vlan)#name Estudiantes
S2(config-vlan)#exit
S2(config)#vlan 40
S2(config-vlan)#name Invitados
S2(config-vlan)#exit
S2(config)#vlan 50
```

```
S2(config-vlan)#name Usuarios
S2(config-vlan)#exit
S2(config)#vlan 56
S2(config-vlan)#name Native
S2(config-vlan)#exit
S2(config)#interface range f0/1-2
S2(config-if-range)#switchport trunk encapsulation dot1q
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk Native vlan 56
S2(config-if-range)#interface range f0/1-2
S2(config-if-range)#channel-group 1 mode active
S2(config-if-range)#interface port-channel 1
S2(config-if)#exit
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-if)#exit
S2(config)#interface range f0/3-17, f0/19-24, g0/1-2
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 50
S2(config-if-range)#description VLAN 50
```

```

S2(config-if-range)#shutdown

S2(config-if-range)#exit

S2(config)#interface range f0/1-2

S2(config-if-range)#no shutdown

S2(config-if-range)#end

S2#copy running-config startup-config

```

Después se configura el soporte de host en R1 cumpliendo las tareas de la tabla 13.

Tabla 13 Configuración del soporte de host en R1

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0
Configurar IPv4 DHCP para VLAN 2	Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sa.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada
Configurar DHCP IPv4 para VLAN 3	Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sb.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada

Fuente: Documento guía

A continuación, se presenta cada línea de comando usada para la configuración de R1.

```

R1#config t

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

R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0

R1(config)#ipv6 route ::/0 loopback 0

R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52

R1(config)#ip dhcp pool vlan20-Docentes

R1(dhcp-config)#network 10.19.8.0 255.255.255.192

R1(dhcp-config)#default-router 10.19.8.1

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

R1(dhcp-config)#exit

R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84

R1(config)#ip dhcp pool vlan30-Estudiantes

R1(dhcp-config)#network 10.19.8.64 255.255.255.224

R1(dhcp-config)#default-router 10.19.8.65

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

R1(dhcp-config)#end

R1#copy running-config startup-config

```

El siguiente paso es configurar los equipos host PC-A y PC-B de acuerdo con la tabla de direccionamiento, esta configuración se verifica con el comando ipconfig /all y se registra en la tabla 14 para el PC-A y en la tabla 15 para el PC-B.

Tabla 14 Configuración de host PC-A

Configuración de red PC-A	
Descripción	PC-A FastEthernet0

Dirección física	0002.1752.4819
Dirección IPv4	10.19.8.53
Mascara de subred	255.255.255.192
Puerta de enlace IPv4 predeterminada	10.19.8.1
Puerta de enlace IPv6 predeterminada	Fe80::1

Fuente: Documento guía

Tabla 15 Configuración de host PC-B

Configuración de red PC-B	
Descripción	PC-B FastEthernet0
Dirección física	00D0.BA7B.49E9
Dirección IPv4	10.19.8.85
Mascara de subred	255.255.255.224
Puerta de enlace IPv4 predeterminada	10.19.8.65
Puerta de enlace IPv6 predeterminada	Fe80::1

Fuente: Documento guía

Para terminar con este escenario se procede a probar y verificar la conectividad de extremo a extremo haciendo uso del comando ping, las verificaciones son registradas en la tabla 16.

Tabla 16 Verificación de conectividad dispositivos de red

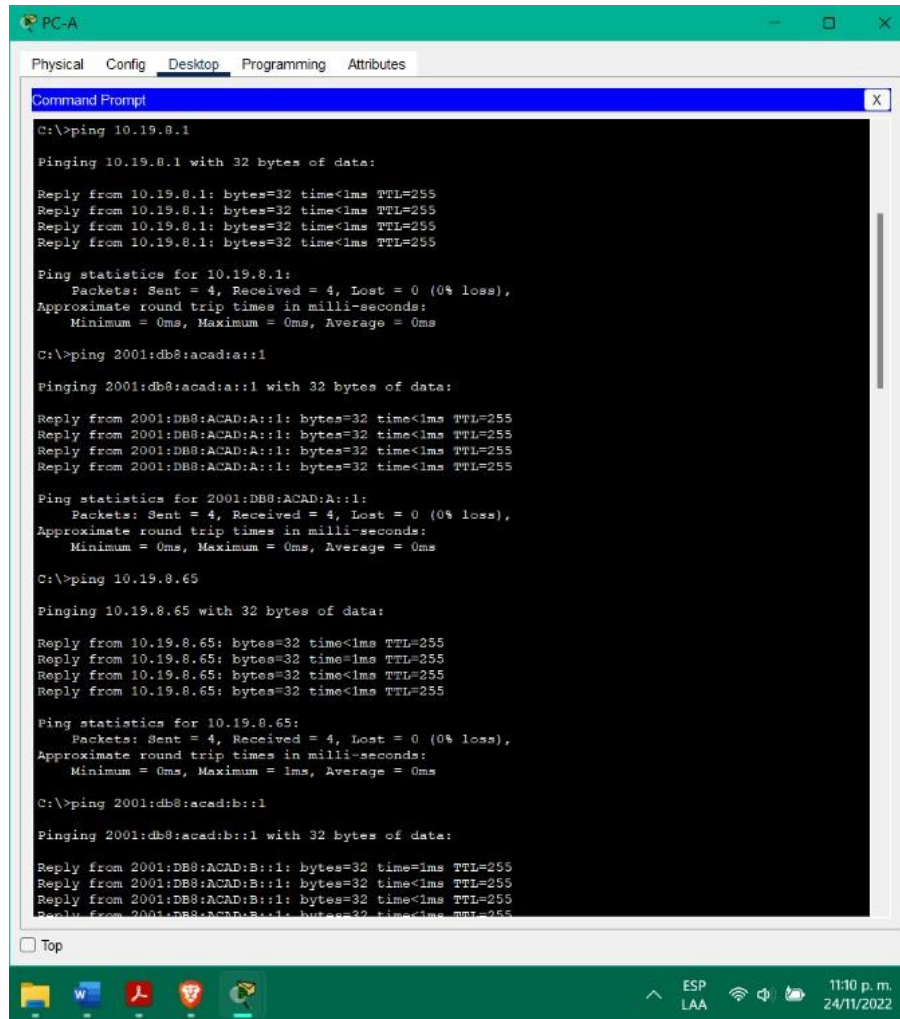
Desde	A		Dirección IP	Resultados de ping
	R1 G 0/0/1.20	IPv4	10.19.8.1	Exitoso: 0% de paquetes perdidos. Ver figura 8.
		IPv6	2001:db8:acad:a::1	Exitoso: 0% de paquetes perdidos. Ver figura 8.
	R1 G 0/0/1.30	IPv4	10.19.8.65	Exitoso: 0% de paquetes perdidos. Ver figura 8.
		IPv6	2001:db8:acad:b::1	Exitoso: 0% de paquetes perdidos. Ver figura 9.
	R1 G 0/0/1.40	IPv4	10.19.8.97	Exitoso: 0% de paquetes perdidos. Ver figura 9.
		IPv6	2001:db8:acad:c::1	Exitoso: 0% de paquetes perdidos. Ver figura 9.
S1	VLAN	IPv4	10.19.8.98	Exitoso: 50% de

	4			paquetes perdidos, esto pasa por ser la primera comunicación con ese punto, si se vuelve a ejecutar el ping será 100% exitoso. Ver figura 10.
		IPv6	2001:db8:acad:c::98	Fallido: 100% de paquetes perdidos. Ver figura 10.
	S2 VLAN 4	IPv4	10.19.8.99	Exitoso: 50% de paquetes perdidos, esto pasa por ser la primera comunicación con ese punto, si se vuelve a ejecutar el ping será 100% exitoso. Ver figura 10.
		IPv6	2001:db8:acad:c::99	Fallido: 100% de paquetes perdidos. Ver figura 11.
	PC-B	IPv4	10.19.8.85	Exitoso: 25% de paquetes perdidos, esto pasa por ser la primera comunicación con ese punto, si se vuelve a ejecutar el ping será 100% exitoso. Ver figura 11.
		IPv6	2001:db8:acad:b::50	Exitoso: 0% de paquetes perdidos. Ver figura 12.
	R1 Bucle 0	IPv4	209.165.201.1	Exitoso: 0% de paquetes perdidos. Ver figura 12.
		IPv6	2001:db8:acad:209::1	Exitoso: 0% de paquetes perdidos. Ver figura 12.
	R1 Bucle 0	IPv4	209.165.201.1	Exitoso: 0% de paquetes perdidos. Ver figura 13.
		IPv6	2001:db8:acad:209::1	Exitoso: 0% de paquetes perdidos. Ver figura 13.

	R1 0/0/1.20	G	IPv4	10.19.8.1	Exitoso: 0% de paquetes perdidos. Ver figura 13.
			IPv6	2001:db8:acad:a::1	Exitoso: 0% de paquetes perdidos. Ver figura 14.
	R1 0/0/1.30	G	IPv4	10.19.8.65	Exitoso: 0% de paquetes perdidos. Ver figura 14.
			IPv6	2001:db8:acad:b::1	Exitoso: 0% de paquetes perdidos. Ver figura 14.
	R1 0/0/1.40	G	IPv4	10.19.8.97	Exitoso: 0% de paquetes perdidos. Ver figura 15.
			IPv6	2001:db8:acad:c::1	Exitoso: 0% de paquetes perdidos. Ver figura 15.
	S1 4	VLAN	IPv4	10.19.8.98	Exitoso: 25% de paquetes perdidos, esto pasa por ser la primera comunicación con ese punto, si se vuelve a ejecutar el ping será 100% exitoso. Ver figura 15.
			IPv6	2001:db8:acad:c::98	Fallido: 100% de paquetes perdidos. Ver figura 16.
	S2 4	VLAN	IPv4	10.19.8.99	Exitoso: 25% de paquetes perdidos, esto pasa por ser la primera comunicación con ese punto, si se vuelve a ejecutar el ping será 100% exitoso. Ver figura 16.
			IPv6	2001:db8:acad:c::99	Fallido: 100% de paquetes perdidos. Ver figura 16.

Fuente: Documento guía. Resultados propios

Figura 8 Verificación conectividad desde PC-A parte 1



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.19.8.1

Pinging 10.19.8.1 with 32 bytes of data:

Reply from 10.19.8.1: bytes=32 time<1ms TTL=255
Reply from 10.19.8.1: bytes=32 time<1ms TTL=255
Reply from 10.19.8.1: bytes=32 time<1ms TTL=255
Reply from 10.19.8.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.19.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>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

C:\>ping 10.19.8.65

Pinging 10.19.8.65 with 32 bytes of data:

Reply from 10.19.8.65: bytes=32 time<1ms TTL=255
Reply from 10.19.8.65: bytes=32 time<1ms TTL=255
Reply from 10.19.8.65: bytes=32 time<1ms TTL=255
Reply from 10.19.8.65: bytes=32 time<1ms TTL=255

Ping statistics for 10.19.8.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

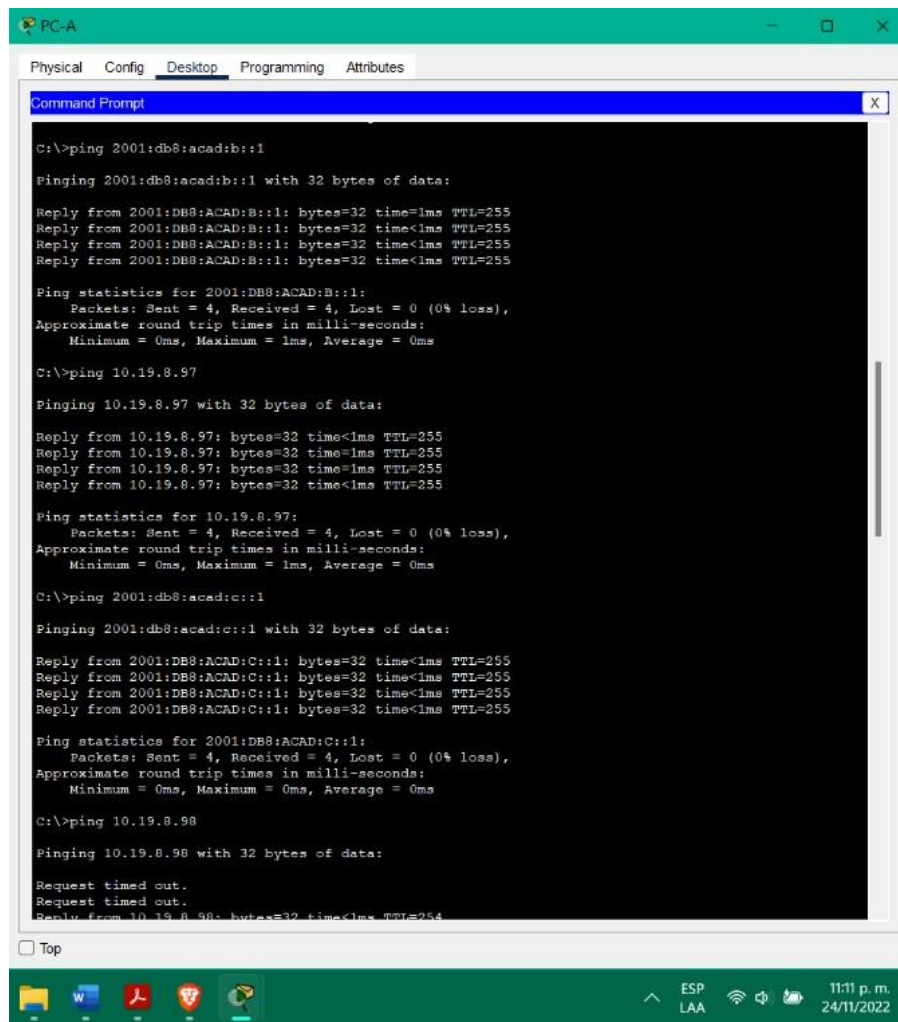
C:\>ping 2001:db8:acad:b::1

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
```

Fuente: Propia

Figura 9 Verificación conectividad desde PC-A parte 2



```
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

C:\>ping 10.19.8.97

Pinging 10.19.8.97 with 32 bytes of data:

Reply from 10.19.8.97: bytes=32 time<1ms TTL=255
Reply from 10.19.8.97: bytes=32 time<1ms TTL=255
Reply from 10.19.8.97: bytes=32 time<1ms TTL=255
Reply from 10.19.8.97: bytes=32 time<1ms TTL=255

Ping statistics for 10.19.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>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

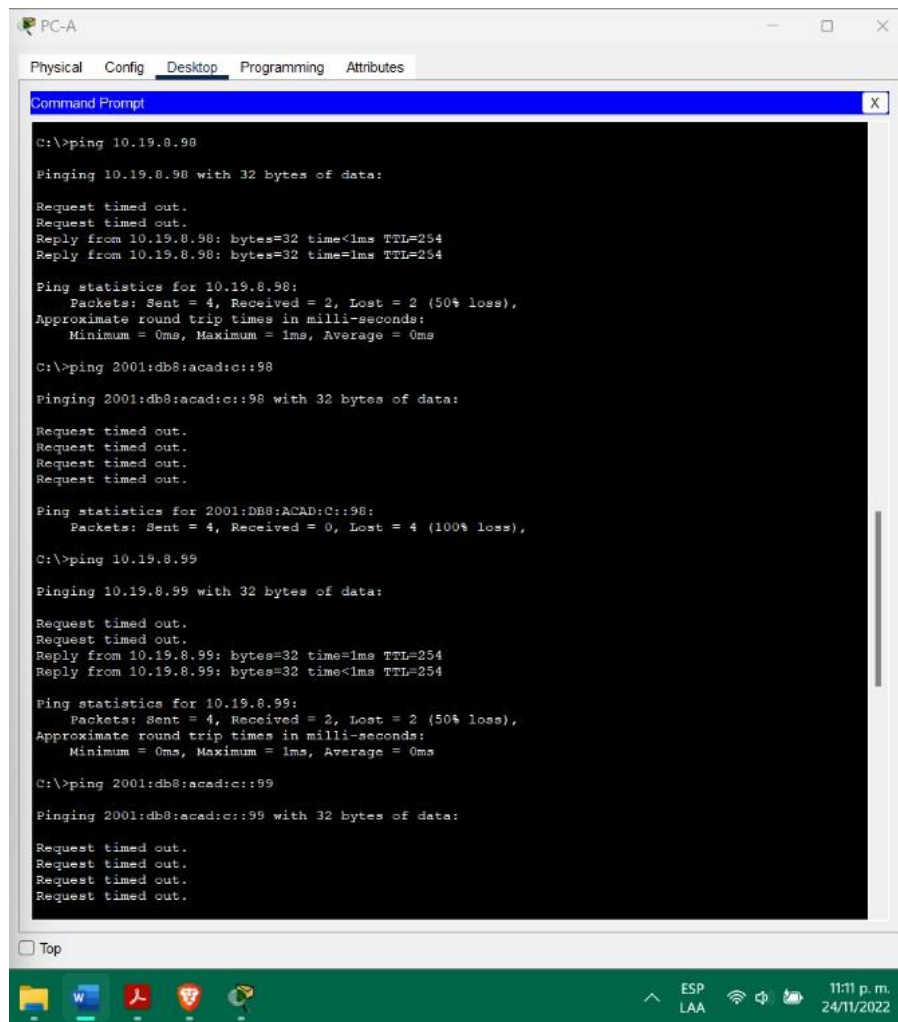
C:\>ping 10.19.8.98

Pinging 10.19.8.98 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.19.8.98: bytes=32 time<1ms TTL=255
```

Fuente: Propia

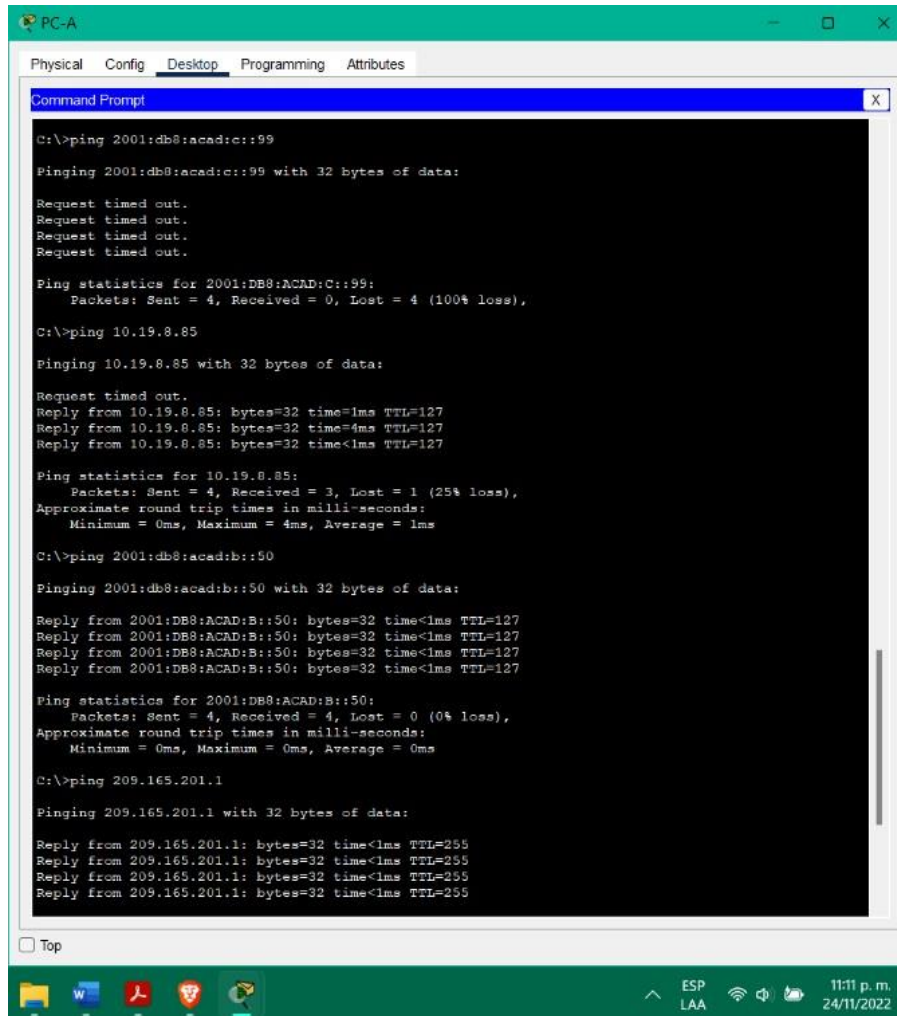
Figura 10 Verificación conectividad desde PC-A parte 3



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.19.8.98
Pinging 10.19.8.98 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 10.19.8.98: bytes=32 time<1ms TTL=254
Reply from 10.19.8.98: bytes=32 time<1ms TTL=254
Ping statistics for 10.19.8.98:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 2001:db8:acad:c::98
Pinging 2001:db8:acad:c::98 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 2001:DB8:ACAD:C::98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 10.19.8.99
Pinging 10.19.8.99 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 10.19.8.99: bytes=32 time<1ms TTL=254
Reply from 10.19.8.99: bytes=32 time<1ms TTL=254
Ping statistics for 10.19.8.99:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 2001:db8:acad:c::99
Pinging 2001:db8:acad:c::99 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Fuente: Propia

Figura 11 Verificación conectividad desde PC-A parte 4



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 2001:db8:acad:c::99
Pinging 2001:db8:acad:c::99 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 2001:DB8:ACAD:C::99:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.19.8.85
Pinging 10.19.8.85 with 32 bytes of data:
Request timed out.
Reply from 10.19.8.85: bytes=32 time=1ms TTL=127
Reply from 10.19.8.85: bytes=32 time=4ms TTL=127
Reply from 10.19.8.85: bytes=32 time<1ms TTL=127
Ping statistics for 10.19.8.85:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>ping 2001:db8:acad:b::50
Pinging 2001:db8:acad:b::50 with 32 bytes of data:
Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127
Ping statistics for 2001:DB8:ACAD:B::50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

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
```

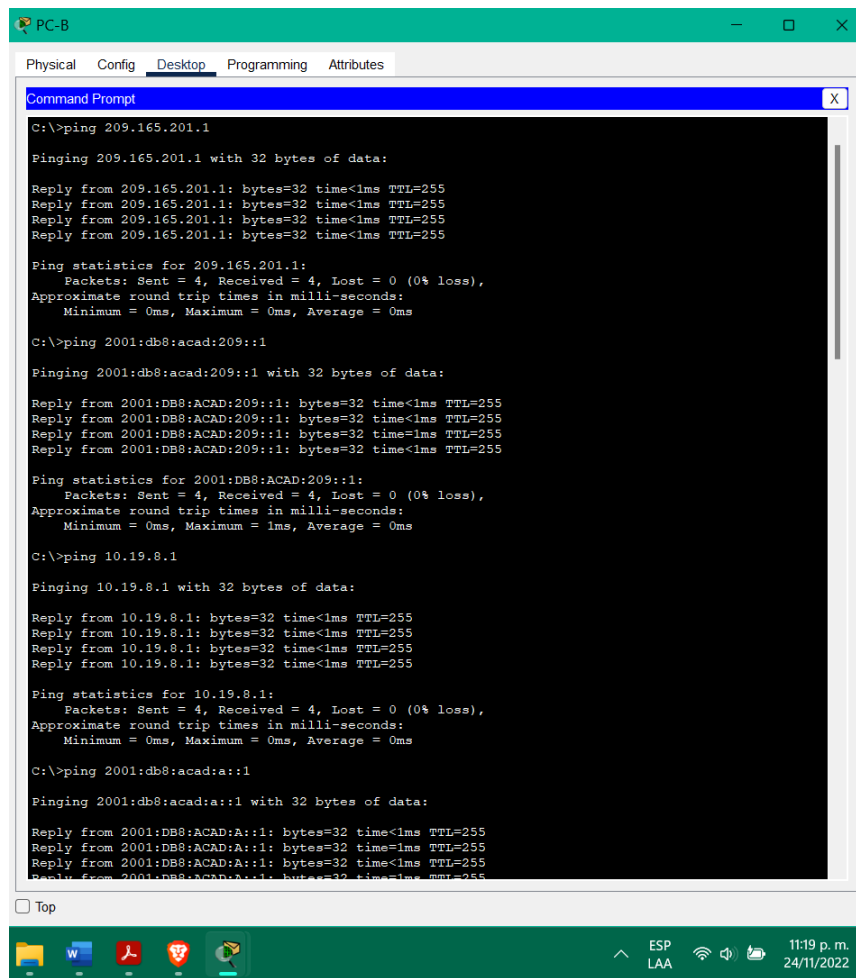
Fuente: Propia

Figura 12 Verificación conectividad desde PC-A parte 5

```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 10.19.8.85: bytes=32 time<1ms TTL=127
Ping statistics for 10.19.8.85:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4ms, Average = 1ms
C:\>ping 2001:db8:acad:b::50
Pinging 2001:db8:acad:b::50 with 32 bytes of data:
Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127
Ping statistics for 2001:DB8:ACAD:B::50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
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
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 = 1ms, Average = 0ms
C:\>
```

Fuente: Propia

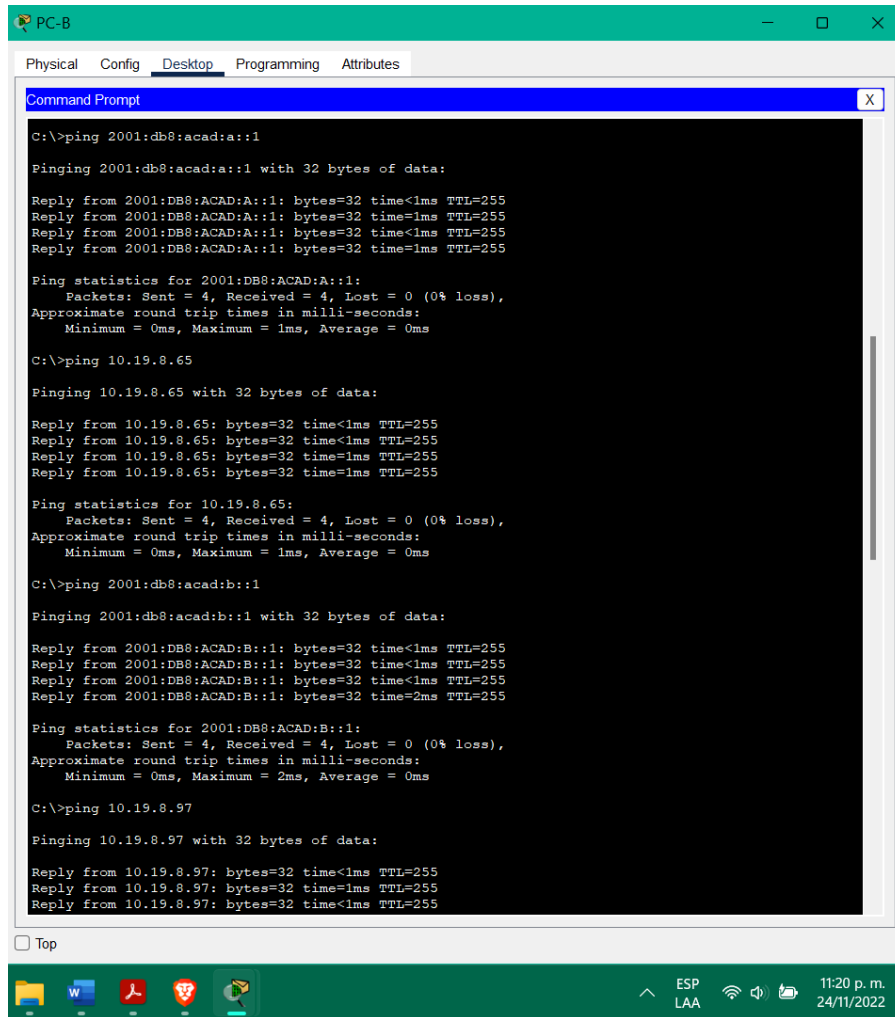
Figura 13 Verificación conectividad desde PC-B parte 1



```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 209.165.201.1
Pinging 209.165.201.1 with 32 bytes of data:
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
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
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 = 1ms, Average = 0ms
C:\>ping 10.19.8.1
Pinging 10.19.8.1 with 32 bytes of data:
Reply from 10.19.8.1: bytes=32 time<1ms TTL=255
Reply from 10.19.8.1: bytes=32 time<1ms TTL=255
Reply from 10.19.8.1: bytes=32 time<1ms TTL=255
Reply from 10.19.8.1: bytes=32 time<1ms TTL=255
Ping statistics for 10.19.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>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
Top
Taskbar: File Explorer, Word, PDF, Security, Network
System tray: ESP LAA, Wi-Fi, Speaker, 11:19 p. m. 24/11/2022
```

Fuente: Propia

Figura 14 Verificación conectividad desde PC-B parte 2



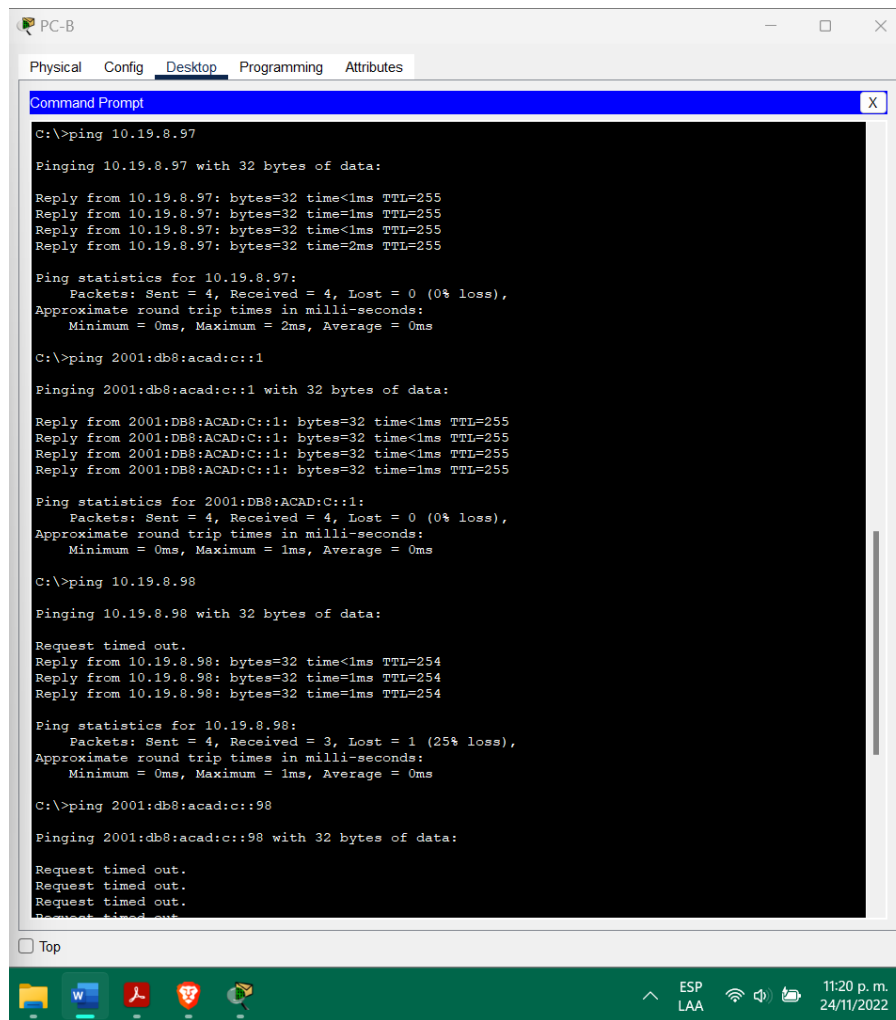
```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 2001:db8:acad:a::1
Pinging 2001:db8:acad:a::1 with 32 bytes of data:
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255
Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 10.19.8.65
Pinging 10.19.8.65 with 32 bytes of data:
Reply from 10.19.8.65: bytes=32 time<1ms TTL=255
Reply from 10.19.8.65: bytes=32 time<1ms TTL=255
Reply from 10.19.8.65: bytes=32 time=1ms TTL=255
Reply from 10.19.8.65: bytes=32 time=1ms TTL=255
Ping statistics for 10.19.8.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
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=2ms 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 = 2ms, Average = 0ms
C:\>ping 10.19.8.97
Pinging 10.19.8.97 with 32 bytes of data:
Reply from 10.19.8.97: bytes=32 time<1ms TTL=255
Reply from 10.19.8.97: bytes=32 time=1ms TTL=255
Reply from 10.19.8.97: bytes=32 time<1ms TTL=255
```

Top

ESP LAA 11:20 p.m. 24/11/2022

Fuente: Propia

Figura 15 Verificación conectividad desde PC-B parte 3



```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.19.8.97

Pinging 10.19.8.97 with 32 bytes of data:

Reply from 10.19.8.97: bytes=32 time<1ms TTL=255
Reply from 10.19.8.97: bytes=32 time=1ms TTL=255
Reply from 10.19.8.97: bytes=32 time<1ms TTL=255
Reply from 10.19.8.97: bytes=32 time=2ms TTL=255

Ping statistics for 10.19.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

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 = 1ms, Average = 0ms

C:\>ping 10.19.8.98

Pinging 10.19.8.98 with 32 bytes of data:

Request timed out.
Reply from 10.19.8.98: bytes=32 time<1ms TTL=254
Reply from 10.19.8.98: bytes=32 time=1ms TTL=254
Reply from 10.19.8.98: bytes=32 time=1ms TTL=254

Ping statistics for 10.19.8.98:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

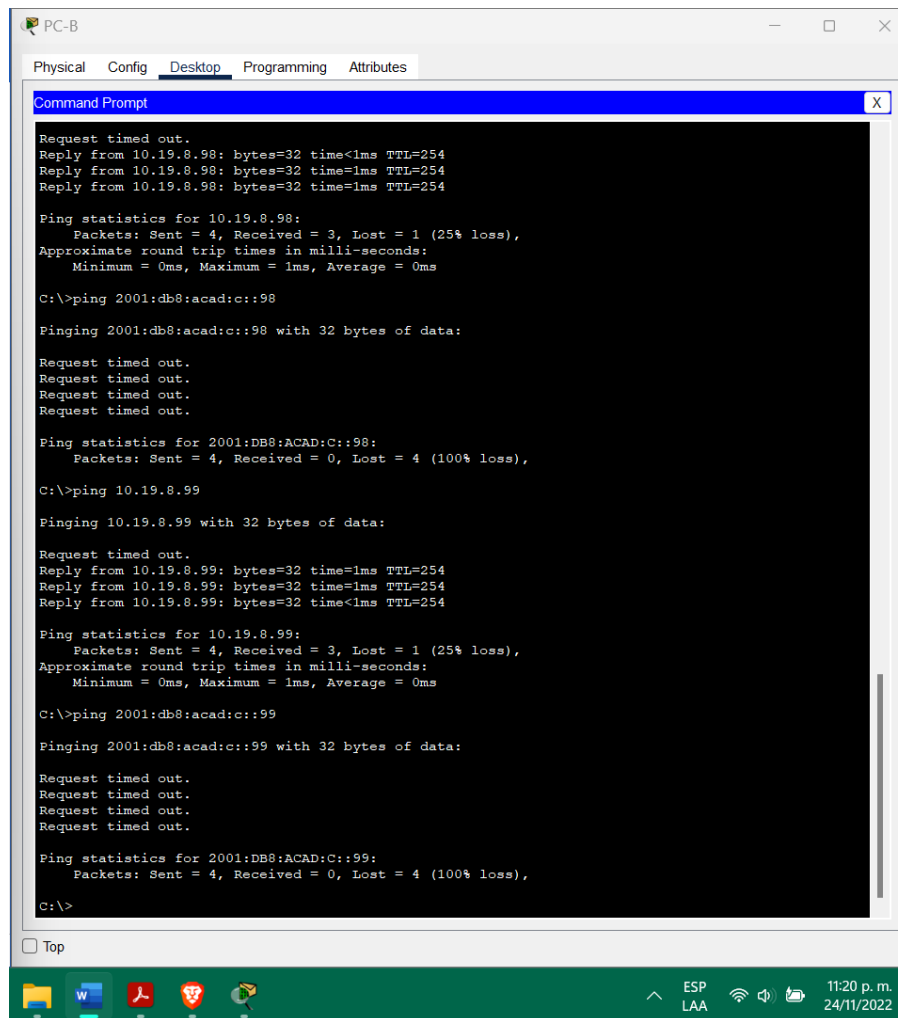
C:\>ping 2001:db8:acad:c::98

Pinging 2001:db8:acad:c::98 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Fuente: Propia

Figura 16 Verificación conectividad desde PC-B parte 4



```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
Request timed out.
Reply from 10.19.8.98: bytes=32 time<1ms TTL=254
Reply from 10.19.8.98: bytes=32 time=1ms TTL=254
Reply from 10.19.8.98: bytes=32 time=1ms TTL=254

Ping statistics for 10.19.8.98:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 2001:db8:acad:c::98

Pinging 2001:db8:acad:c::98 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB8:ACAD:C::98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.19.8.99

Pinging 10.19.8.99 with 32 bytes of data:

Request timed out.
Reply from 10.19.8.99: bytes=32 time=1ms TTL=254
Reply from 10.19.8.99: bytes=32 time=1ms TTL=254
Reply from 10.19.8.99: bytes=32 time<1ms TTL=254

Ping statistics for 10.19.8.99:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 2001:db8:acad:c::99

Pinging 2001:db8:acad:c::99 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB8:ACAD:C::99:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Fuente: Propia

Se estableció que el direccionamiento para ambos protocolos fue preciso, aparte de las pruebas de VLAN40 para IPv6.

CONCLUSIONES

Se logro cumplir con los objetivos de cada escenario propuesto, es esencial pensar en la cantidad de subredes necesarias y en la cantidad de hosts en cada subred antes de asignar las direcciones IP a la red. Esto se debe a que hay que tener en cuenta el direccionamiento y la máscara de subred a la hora de implementar el direccionamiento. Se debe considerar el código utilizado para establecer las subredes necesarias y obtener correctamente las direcciones IP para la configuración de la red y los dispositivos finales que componen la topología.

En el escenario 1, una pequeña LAN IPV4 puede dividirse en subredes utilizando varias fórmulas. Este proceso de división en subredes no afectará a la pertenencia al dominio, y permite dividir la organización en redes más pequeñas. Además, un servidor DHCP no es necesario en esta red ya que hay menos dispositivos y hosts, y más opciones de configuración estática, lo que permite un mayor control sobre las direcciones IP.

El escenario 2 utiliza routers y switches para reforzar la seguridad a través de VLANs, DHCP, EtherChannel y seguridad de puertos, que son métodos eficaces para conceder o denegar el acceso a recursos específicos. La mayor parte de la configuración de los dispositivos se realiza a través de la consola, ya que es más segura y configura procesos no visuales.

BIBLIOGRAFIA

BITACORABYTE. Configurar DHCP en router CISCO. Bitacora Byte. Disponible en <https://bitacorabyte.wordpress.com/2017/07/18/configurar-dhcp-en-router-cisco/>

CISCO. (s. f.-a). Configure InterVLAN Routing on Layer 3 Switches. Cisco. Disponible en <https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html>

CISCO. (s. f.-b). Understand the Ping and Traceroute Commands. Cisco. Disponible en <https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-121-mainline/12778-ping-traceroute.html>

HUCABY, D., & MCQUERRY, S. (s. f.). Trunking > VLANs and Trunking | Cisco Press. Disponible en <https://www.ciscopress.com/articles/article.asp?p=29803&seqNum=3>

JMCRISTOBAL. (2021, enero 22). VLANs y Trunk Ports. JMCristobal. Disponible en <https://jmcristobal.com/2021/01/22/vlans-y-trunk-ports/>

ANEXOS

ANEXO A – Enlace de descarga de las simulaciones de los escenarios

<https://1drv.ms/u/s!AnblQuGc3s9YgR4gAqREuyF5Wfpt?e=gosN4b>