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

ALVARO JOSE MUÑOZ GALARZA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DECIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA SISTEMAS
SANTANDER DE QUILICHAO
2022

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USODE TECNOLOGÍA CISCO

ALVARO JOSE MUÑOZ GALARZA

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

DIRECTOR:
PAULITA FLOR SALAZAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DECIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA SISTEMAS
SANTANDER DE QUILICHAO
2022

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Santander de Quilichao, 25 de noviembre de 2022

AGRADECIMIENTOS

Quiero agradecer principalmente a Dios por darme la vida, la salud y la fortaleza para culminar mi carrera profesional.

A mis Padres darme los valores y los principios fundamentales que me han permitido seguir en la vida por el buen camino y por haber sido mis guías en momentos difíciles.

También quiero agradecer a mis Hermanos y mi a Tía por el amor y apoyo que me han brindado en todas las etapas de mi vida.

A mi Esposa por el amor, paciencia, comprensión y apoyo incondicional brindado en las etapas importantes de mi vida, para cumplir con mis metas académicas y profesionales.

A la Universidad Nacional Abierta y a Distancia (UNAD), a sus docentes; por darme la oportunidad de homologar mis estudios Tecnológicos y así obtener mi título de Ingeniero de Sistemas.

Finalmente, a demás familiares y amigos que estuvieron pendientes de mí en el transcurso de la carrera, dándome ánimo para no desfallecer en este proceso académico.

CONTENIDO

LISTADE TABLAS

LISTA DE FIGURAS

GLOSARIO

LAN: Es una infraestructura de red que proporciona acceso a usuarios y dispositivos finales en un área geográfica pequeña. Normalmente, una LAN se utiliza en un departamento dentro de una empresa, un hogar o una red de pequeñas empresas. Las infraestructuras LAN interconectan terminales en un área limitada, como una casa, un lugar de estudios, un edificio de oficinas o un campus.

WAN: Es una infraestructura de red que proporciona acceso a otras redes en un área geográfica amplia, que generalmente es propiedad y está administrada por una corporación más grande o un proveedor de servicios de telecomunicaciones. Las infraestructuras WAN interconectan LAN a través de áreas geográficas extensas, por ejemplo, entre ciudades, estados, provincias, países o continentes, y la administración de las WAN está a cargo de varios proveedores de servicios.

CONSOLA: Es un puerto de administración físico que proporciona acceso fuera de banda a un dispositivo de Cisco. El acceso fuera de banda hace referencia al acceso por un canal de administración exclusivo que se usa únicamente con fines de administración del dispositivo. Para una conexión de consola se requiere un equipo con software de emulación de terminal y un cable de consola especial para conectarse al dispositivo.

GATEWAY (Puerta de enlace): es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red, al protocolo usado en la red de destino.

DISPOSITIVOS FINALES: Son los dispositivos de red con los que las personas están más familiarizados. Para distinguir un dispositivo final de otro, cada dispositivo final de una red tiene una dirección. Cuando un dispositivo final inicia la comunicación, utiliza la dirección del dispositivo final de destino para especificar dónde entregar el mensaje.

INTERFAZ: Puertos especializados en un dispositivo de red que se conecta a redes individuales. Debido a que los routers conectan redes, los puertos en un router se denominan interfaces de red.

DIRECCIÓN IP: Una IP (Internet Protocol) es una dirección única que identifica a un dispositivo en una red. Esta se encuentra formada por cuatro números de hasta tres cifras separados por un punto, comprendidos cada uno de ellos entre 0 y 255 (ejemplo:192.168.10.3). Estas direcciones Ip se dividen en públicas y privadas, a su vez pueden ser fijas y dinámicas.

RESUMEN

Cisco es una empresa líder en comunicaciones, redes de datos y TI, fabricante de dispositivos de red, como routers, firewalls de hardware, productos de telefonía IP, etc. Además, posee varios programas educativos que brindan la formación y certificación de personal profesional en el área de TI y redes informáticas.

Es por ello que los diplomados CCNA, nos brindan la oportunidad de obtener los conocimientos y habilidades prácticas para diagnosticar y dar solución en problemas de redes. Además, son de gran ayuda para prepararnos y lograr obtener la certificación CCNA (Cisco Certified Networking Associate); la cual es de las más importantes dentro de la industria de la Tecnología de la Información y tiene reconocimiento internacional por su reputación y credibilidad.

Con el desarrollo de esta actividad se busca prepararse y obtener los conocimientos y las habilidades necesarias para afrontar cualquier tipo de trabajo que se pueda presentar en el área de TI. Las competencias de los ingenieros de redes hoy en día son muy importantes y necesarias, es por ello que la certificación Cisco Certified Network Associate (CCNA) demuestra que el profesional tiene y asegura la idoneidad requerida para la adopción de tecnologías de próxima generación.

Debemos tener presente el método integrado de enrutamiento y conmutación adoptado, de acuerdo al tipo de redes y topologías planteadas, ya que permitirá que todos los usuarios de la red tengan el mismo acceso a las aplicaciones, las comunicaciones y videoconferencias, incluidos los usuarios de otras redes y dependencias. Cisco acepta que la red crezca en el tiempo, agregándole funcionalidades y dispositivos a medida que los necesite.

Para desarrollar todo el direccionamiento IP y configuración de los dispositivos, se hace bajo la estandarización de la Organización de Electrónica e Ingeniería Eléctrica (Institute of Electrical and Electronics Engineers IEEE), dedicada a avanzar en la innovación tecnológica y en elaborar estándares para sectores como: servicios de salud, telecomunicaciones y redes. Algunos estándares de red IEEE son 802.3 Ethernet y 802.11 WLAN.

Palabras clave: Configuración, consola, Interfaz, LAN, Redes.

ABSTRACT

Cisco is a leading company in communications, data networks and IT, manufacturer of network devices, such as routers, hardware firewalls, IP telephony products, etc. In addition, it has several educational programs that provide training and certification of professional personnel in the area of IT and computer networks.

That is why the CCNA graduates provide us with the opportunity to obtain the knowledge and practical skills to diagnose and solve network problems. In addition, they are of great help to prepare and achieve the CCNA certification (Cisco Certified Networking Associate); which is one of the most important within the Information Technology industry and has international recognition for its reputation and credibility.

The development of this activity seeks to prepare and obtain the knowledge and skills necessary to face any type of work that may arise in the IT area. The competencies of network engineers today are very important and necessary, that is why the Cisco Certified Network Associate (CCNA) certification demonstrates that the professional has and ensures the required suitability for the adoption of next generation technologies.

We must keep in mind the integrated routing and switching method adopted, according to the type of networks and topologies proposed, since it will allow all network users to have the same access to applications, communications and videoconferencing, including users of other networks and dependencies. Cisco accepts that the network grows over time, adding functionalities and devices as you need them.

To develop all IP addressing and configuration of devices, it is done under the standardization of the Institute of Electrical and Electronics Engineers (IEEE), dedicated to advancing technological innovation and developing standards for sectors such as: health services, telecommunications and networks. Some IEEE network standards are 802.3 Ethernet and 802.11 WLAN.

Keywords: configuración, console, Interface, LAN, Networks.

INTRODUCCIÓN

En el desarrollo del escenario 1 y con base en los conocimientos obtenidos durante el diplomado, se diseña la red propuesta en el simulador packet tracer, de acuerdo a la topología lógica planteada y se conectan los equipos con el cableado correspondiente.

Para la comunicación e interconexión de los diferentes dispositivos se crea un esquema de direccionamiento IP, cumpliendo con los requerimientos y haciendo uso de VLSM para un mayor aprovechamiento del espacio de red.

La configuración de los dispositivos de red S1 y R1 se realiza utilizando código por medio de la conexión por consola y para la configuración y direccionamiento Ip de los hosts se asigna la dirección IPv4, mascara de subred y puerta de enlace.

La utilización del comando ping, permite probar y verificar la conectividad entre los dispositivos de la red, desde cualquier dispositivo hacia una dirección Ip específica de cada interface y/o dispositivo de red, el cual permite diagnosticar si la red tiene o no fallas.
Debido a la escasez de direcciones IPv4 es necesario implementar el protocolo IPv6 a corto plazo, pero las organizaciones, proveedores, servidores de Internet no han hecho la migración debido a que dispositivos, software y demás deben soportar el nuevo protocolo. En el caso de los dispositivos CISCO y sistemas operativos ya se encuentran actualizados y soportan el uso de IPv6.

Para la implementación y configuración del protocolo IPv6 se habilita el uso de IPv6 tanto en el router como en el switch. En cuanto al mejoramiento de la administración, la seguridad y la optimización del rendimiento de la red se crean las VLAN. En la comunicación interVlan es indispensable que se habilite el uso de los enlaces troncales, configurando las interfaces respectivas en cada switch y especificando las Vlan que se permiten en el enlace troncal.

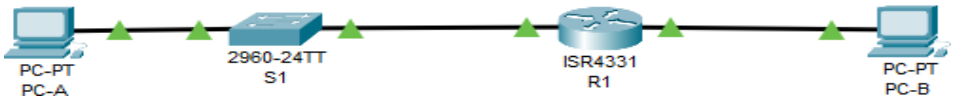
1. ESCENARIO 1

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

Figura 1. Topología del escenario 1

Fuente: Prueba de habilidades diplomado profundización CCNA

Figura 2. Simulación de la topología del escenario 1



Fuente: Autor

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

Tabla 1. Esquema de direccionamiento

Item	Requerimiento
Dirección de Red	172.46.3.0 donde XY corresponde a los últimos dos dígitos de su cédula.
Requerimiento de host Subred LAN1	60
Requerimiento de host Subred LAN2	20
R1 G0/0/1	Última dirección de host de la subred LAN1 172.46.3.62 255.255.255.192

R1 G0/0/0	Última dirección de host de la subred LAN2 172.46.3.94 255.255.255.224
S1 SVI	Segunda dirección de host de la subred LAN1 172.46.3.2
PC-A	Décima dirección de host de la subred LAN1 172.46.3.10 255.255.255.192
PC-B	Décima dirección de host de la subred LAN2 172.46.3.74 255.255.255.224

Se hace el cálculo de las subredes por medio de VLSM, partiendo con la red LAN 1 que requiere el mayor número de hosts (60), dando como resultado las subredes que se detallan a continuación:

Tabla 2. Direccionamiento IPv4 de Subredes

Subred	**Dirección de subred**	**Mascara de subred**	**Primera dirección** **Última dirección de host utilizable**	**Dirección Broadcast**
LAN 1	172.46.3.0/26	255.255.255.192	172.46.3.1 172.46.3.62	172.46.3.63
LAN 2	172.46.3.64/27	255.255.255.224	172.46.3.65 172.46.3.94	172.46.3.95
LAN 3	172.46.3.96/30	255.255.255.252	172.46.3.97 172.46.3.98	172.46.3.99

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

Configurar los ajustes básicos

1.2.1 Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3. . Código de configuración Router R1

Tarea	Especificación
Desactivar la búsqueda DNS	Comandos utilizados enable: permite ingresar al modo privilegiado configure terminal: se accede al modo de configuración del router no ip domain-lookup: por defecto la búsqueda DNS está activa y con este comando se desactiva, ejecutando las siguientes instrucciones en el Router. Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	Con la ejecución de los siguientes comandos, cambiamos el nombre del Router a R1 Router>enable Router#configure terminal Router(config)#hostname R1
Nombre de dominio	Ingresamos al modo de configuración del Router y con la siguiente línea de comandos asignamos a R1 el nombre de dominio: ccna-sa.com R1(config)#ip domain name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	enable password: Activa una contraseña para restringir el ingreso al modo EXEC privilegiado

	service password-encryption: Habilita un cifrado débil a las contraseñas sin cifrar Ingresamos al modo de configuración del Router y ejecutamos los siguientes comandos para cifrar y asignar la contraseña: ciscoenpass R1>enable R1#configure terminal R1(config)#enable password ciscoenpass R1(config)#service password-encryption R1(config)#exit
Contraseña de acceso a la consola	Los comandos utilizados son: line console 0: Configuración de consola. password: Establece la contraseña login: Activa la contraseña Ingresamos al modo de configuración de R1, luego accedemos al modo de configuración de consola, ejecutamos la contraseña y finalmente por medio de las siguientes líneas de comandos activamos la contraseña: ciscoconpass R1#configure terminal R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima paralas contraseñas	security passwords min-length: Establece la longitud mínima de caracteres en las contraseñas

	En el modo de configuración de R1 ejecutamos los siguientes comandos para establecer la longitud mínima de caracteres y de nuevo la contraseña de modo privilegiado. 10 caracteres R1#configure terminal R1(config)#security passwords min-length 10 R1(config)#enable password ciscoenpass
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Contraseña: **admin1pass** username y password: Son los comandos utilizados para acceder a R1 con usuario y clave. login local: Activa la base de datos local para el ingreso a la línea de consola Con la ejecución de los siguientes comandos en el modo de configuración de R1, se asigna el nombre de usuario y contraseña para la base de datos local: R1#configure terminal R1(config)#username admin password admin1pass R1(config)#line console 0 R1(config-line)#login local
Configure el inicio de sesión en las líneas VTY para que use la base de datos local	line vty 0 4: Acceder a la interfaz telnet con permiso para 5 conexiones múltiples login local: Habilita la base de datos local para la conexión.

	Con la ejecución de los siguientes comandos en el modo de configuración de R1, accedemos a la interfaz telnet para la base de datos local. R1#configure terminal 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	transport input SSH: Permite solamente acceso por medio del protocolo SSH en el modo de configuración line vty En el modo de configuración de R1 ejecutamos los siguientes comandos para permitir solamente el acceso a las conexiones SSH en las líneas VTY. R1#configure terminal R1(config)#line vty 0 4 R1(config-line)#transport input ssh R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	Ingresamos al modo de configuración para cifrar todas las contraseñas no cifradas en R1. R1#configure terminal R1(config)#service password-encryption
Configurar un banner MOTD	Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece. En el modo de configuración de R1 ejecutamos el comando: banner motd, para establecer un mensaje en consola, de la siguiente manera:

	R1#configure terminal R1(config)#banner motd "R1 - Alvaro Jose Munoz Galarza - Programa: Ingenieria de Sistemas"
Configuración de interface G0/0/0	Establecer la descripción Establecer la dirección IPv4 Activar la interfaz. interface: Selecciona la interfaz y entra al modo de configuración description: Dar una descripción a la interfaz ip address: Establece una dirección IP y una máscara de subred no shutdown: Activa la interfaz En el modo de configuración de interface de R1, se ejecutan los siguientes comandos para seleccionar la interfaz G0/0/0 y darle una descripción, asignarle la dirección IP y activarla. R1#configure terminal R1(config)#interface g0/0/0 R1(config-if)#description Subred LAN2 R1(config-if)#ip address 172.46.3.94 255.255.255.224 R1(config-if)#no shutdown
Configuración de interface G0/0/1	Establecer la descripción Establecer la dirección IPv4 Activar la interfaz. En el modo de configuración de interface de R1, se ejecutan los siguientes comandos para seleccionar la interfaz G0/0/1 y darle una descripción, asignarle

	la dirección IP y activarla. R1#configure terminal R1(config)#interface g0/0/1 R1(config-if)#description Subred LAN1 R1(config-if)#ip address 172.46.3.62 255.255.255.192 R1(config-if)#no shutdown
Generar una clave de cifrado RSA	crypto key generate rsa general-keys modulus: Para crear una clave de encriptación con un tamaño específico En el modo de configuración de R1 ejecutamos los siguientes comandos para crear la clave de encriptación con tamaño de: Módulo de 1024 bits R1#configure terminal R1(config)#crypto key generate rsa general-keys modulus 1024 The name for the keys will be: R1.ccna-sa.com % The key modulus size is 1024 bits % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] *Mar 1 1:54:36.916: %SSH-5-ENABLED: SSH 1.99 has been enabled

1.2.2. Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 4. Código de configuración Switch S1

Tarea	**Especificación**
Desactivar la búsqueda DNS	Ingresamos al modo de configuración

	y ejecutamos los siguientes comandos para desactivar la búsqueda DNS en el Switch. Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch	Con la ejecución de los siguientes comandos, cambiamos el nombre del Switch a S1. Switch>enable Switch#configure terminal Switch(config)#hostname S1 S1(config)#
Nombre de dominio	Ingresamos al modo de configuración del Switch y con la siguiente línea de comandos asignamos a S1 el nombre de dominio: ccna-sa.com S1#enable S1#configure terminal S1(config)#ip domain name ccna-sa.com
Contraseña cifrada para el modoEXEC privilegiado	Ingresamos al modo de configuración del Switch y ejecutamos los siguientes comandos para cifrar y asignar la contraseña: ciscoenpass S1>enable S1#configure terminal S1(config)#enable secret ciscoenpass

	S1(config)#service password-encryption S1(config)#exit
Contraseña de acceso a la consola	Ingresamos al modo de configuración de S1, luego accedemos al modo de configuración de consola, ejecutamos la contraseña y finalmente por medio de las siguientes líneas de comandos activamos la contraseña: ciscoconpass S1>enable S1#configure terminal S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit
Apagar todos los puertos sin usar	interface range: Se utiliza para configurar un grupo de interfaces de igual tipo y con los mismos parámetros shutdown: Desactiva la interfaz seleccionada En el modo de configuración de interface de S1, con los siguientes comandos se apagan los grupos de puertos seleccionados: F0/1-4, F0/7-24, G0/1-2 S1>enable S1#configure terminal

	S1(config)#interface range F0/1-4, F0/7-24, G0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#exit S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Contraseña: **admin1pass** Con la ejecución de los siguientes comandos en el modo de configuración de S1, se asigna el nombre de usuario y contraseña para la base de datos local. S1>enable S1#configure terminal S1(config)#username admin password admin1pass
Configure el inicio de sesión en las líneas VTY para que use la base de datos local	Con la ejecución de los siguientes comandos en el modo de configuración de S1, accedemos a la interfaz telnet para la base de datos local. S1>enable S1#configure terminal S1(config)#line vty 0 4 S1(config-line)#exit S1(config)#

Configurar las líneas VTY para que acepten únicamente las conexiones SSH	En el modo de configuración de S1 ejecutamos los siguientes comandos para que las líneas VTY solo acepte las conexiones SSH. S1>enable S1#configure terminal S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line)#transport input ssh S1(config-line)#exit S1(config)#
Cifrar las contraseñas de texto nocifrado	En el modo de configuración con el comando siguiente se cifra todas las contraseñas no cifradas en S1 S1(config)#service password-encryption
Configurar un banner MOTD	Debe contener el nombre del dispositivo, el nombre completodel estudiante y el programa académico al que pertenece. Ingresamos al modo de configuración de S1 y ejecutamos el comando: banner motd, para establecer el mensaje en consola, con los parámetros dados: S1#configure terminal S1(config)#banner motd "R1 - Alvaro Jose Munoz Galarza - Programa: Ingenieria de Sistemas"
Generar una clave de cifrado RSA	En el modo de configuración de S1

	ejecutamos los siguientes comandos para crear la clave de encriptación con tamaño de: Módulo de 1024 bits S1#configure terminal S1(config)#crypto key generate rsa general-keys modulus 1024 The name for the keys will be: S1.ccna-sa.com % The key modulus size is 1024 bits % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] *Mar 1 0:19:29.766: %SSH-5-ENABLED: SSH 1.99 has been enabled S1(config)#
Configure la interfaz de administración (SVI) en VLAN1	Establecer la descripción Establecer la dirección IPv4 ip default-gateway: Para configurar el gateway predeterminado del switch. En el modo de configuración de interface de S1, se ejecutan los siguientes comandos para seleccionar la interfaz vlan1 y darle una descripción, asignarle la dirección IP y activar la interfaz, luego en el modo de configuración de S1 se ejecuta el comando para asignar la puerta de enlace. S1>enable S1#configure terminal

	S1(config)#interface vlan 1 S1(config-if)#description VLAN1 S1(config-if)#ip address 172.46.3.2 255.255.255.192 S1(config-if)#no shutdown Asignamos la puerta enlace S1>enable S1#configure terminal S1(config)#ip default-gateway 172.46.3.62

1.3 Configurar los equipos

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

En el aplicativo Packet Tracer, seleccionamos Desktop, en la opción Command Prompt del equipo PC-A, digitamos el comando C:\>ipconfig /all, con el cual podemos visualizar toda la información que se detalla en la siguiente tabla.

Tabla 5. Configuración PC-A

Configuración de red de PC-A	
Descripción	PC-A
Dirección física	000C.85E1.BD59
Dirección IPv4	172.46.3.10
Máscara de subred	255.255.255.192
Puerta de enlace IPv4predeterminada	172.46.3.62

En el aplicativo Packet Tracer, seleccionamos Desktop, en la opción Command Prompt del equipo PC-B, digitamos el comando C:\>ipconfig /all, con el cual podemos visualizar toda la información que se detalla en la siguiente tabla.

Tabla 6. Configuración PC-B

Configuración de red de PC-B	
Descripción	PC-B
Dirección física	00E0.A3C2.6EDA
Dirección IPv4	172.46.3.74
Máscara de subred	255.255.255.224
Puerta de enlace IPv4predeterminada	172.46.3.94

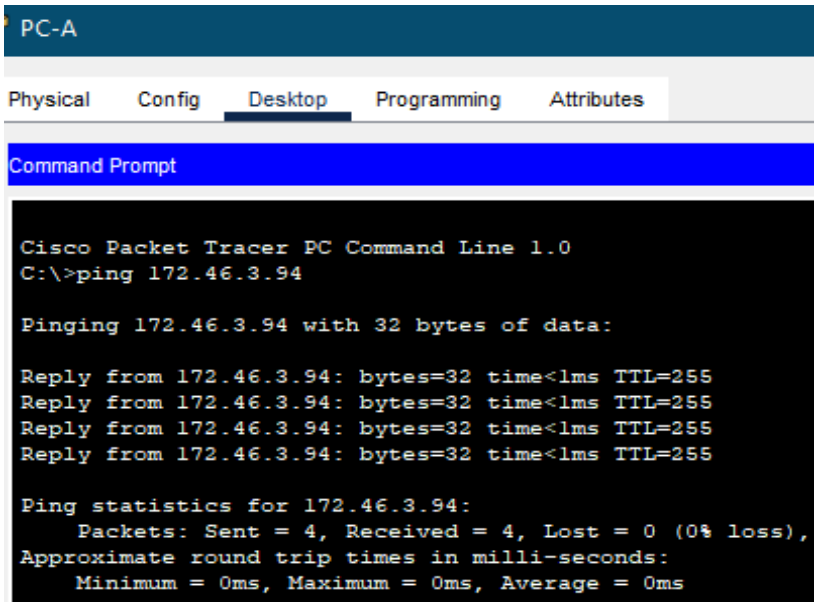
1.4 Probar y verificar la conectividad de extremo a extremo

Utilice el comando ping para probar la conectividad entre todos los dispositivos de red.

Tabla 7. Pruebas de conectividad entre dispositivos

Desde	A	Dirección IP	Resultados de ping
PC-A	R1 G0/0/0	172.46.3.94	Exitoso - Figura 3
	R1 G0/0/1	172.46.3.62	Exitoso - Figura 4
	S1 VLAN 1	172.46.3.2	Exitoso - Figura 5
	PC-B	172.46.3.74	Exitoso - Figura 6
PC-B	R1 G0/0/0	172.46.3.94	Exitoso - Figura 7
	R1 G0/0/1	172.46.3.62	Exitoso - Figura 8
	S1 VLAN1	172.46.3.2	Exitoso - Figura 9

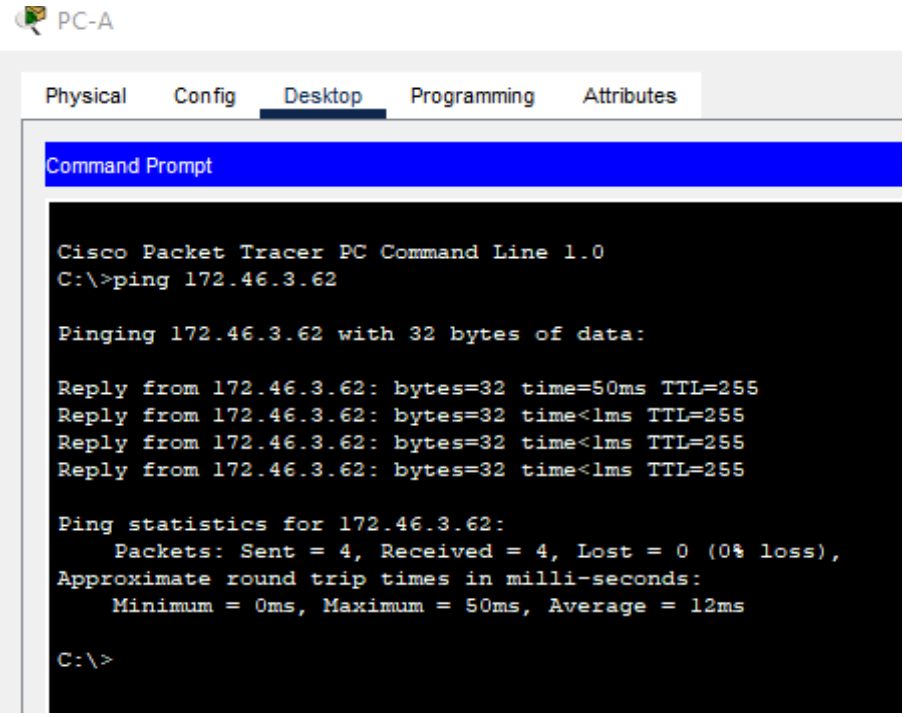
Figura 3. Conectividad de PC-A a R1 G0/0/0



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-A a la interfaz G0/0/0 de R1 con dirección IP 172.46.3.94, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-A y ejecutamos la instrucción C:\>ping 172.46.3.94, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta de 1ms.

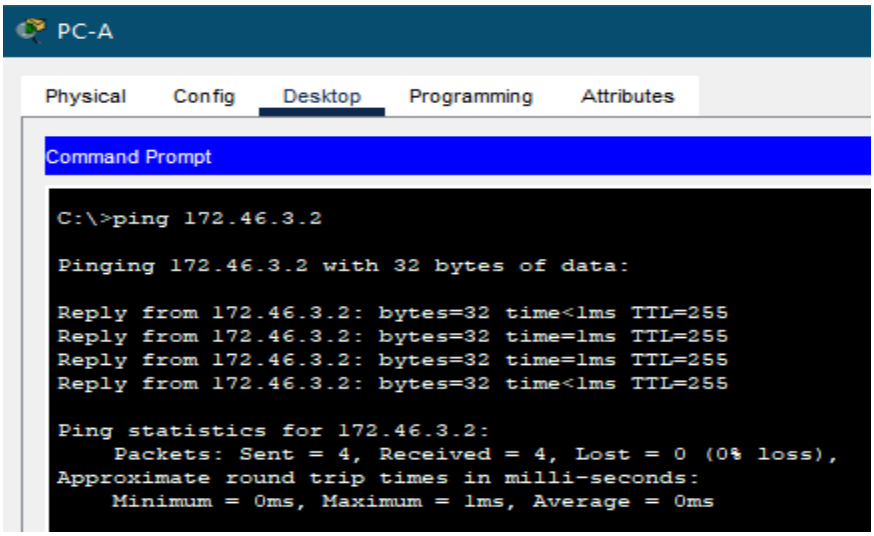
Figura 4. Conectividad de PC-A a R1 G0/0/1



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-A a la interfaz G0/0/1 de R1 con dirección IP 172.46.3.62, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-A y ejecutamos la instrucción C:\>ping 172.46.3.62, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta de 1ms.

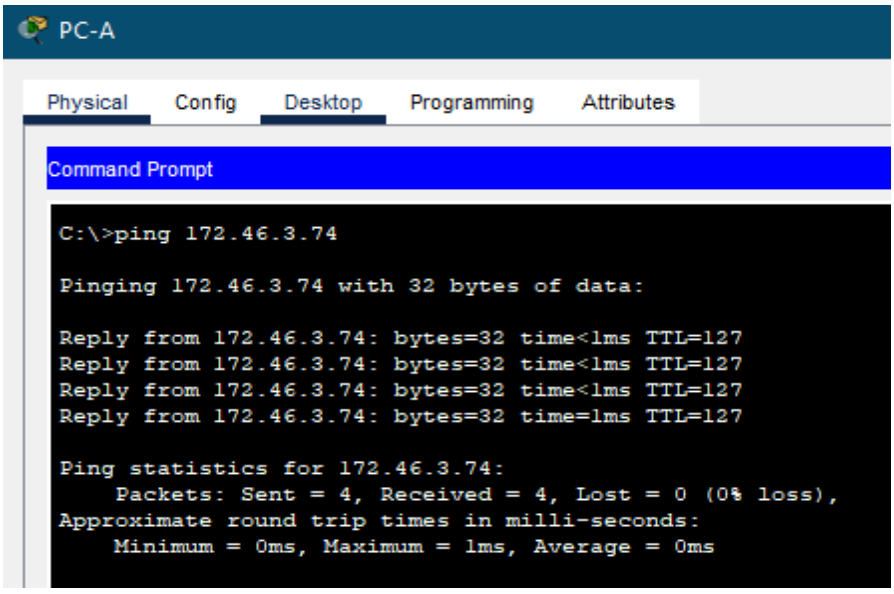
Figura 5. Conectividad de PC-A a S1 VLAN 1



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-A a la interfaz VLAN1 de S1 con dirección IP 172.46.3.2, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-A y ejecutamos la instrucción C:\>ping 172.46.3.2, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta de 1ms.

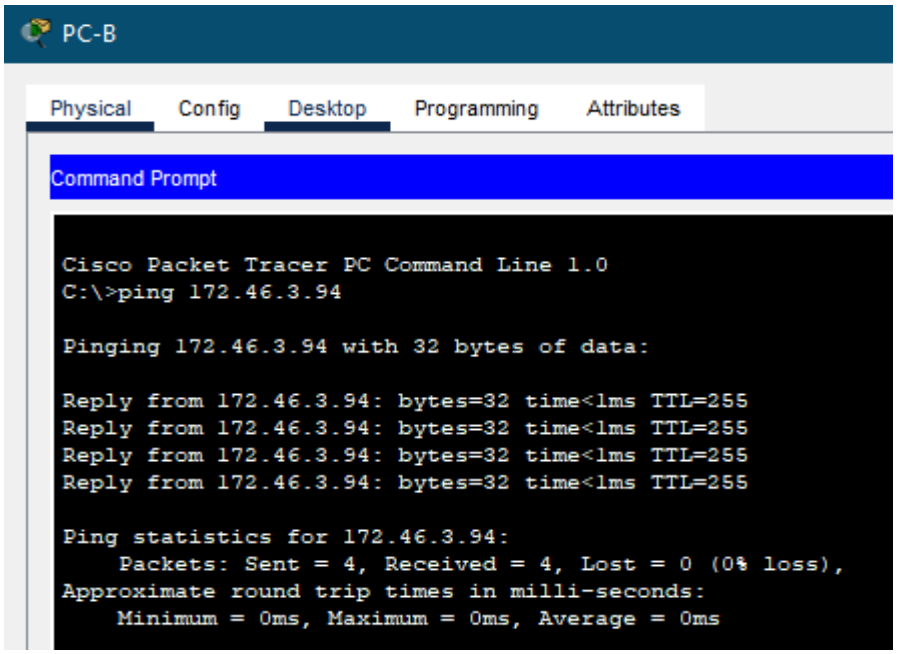
Figura 6. Conectividad de PC-A a PC-B



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-A a PC-B con dirección IP 172.46.3.74, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-A y ejecutamos la instrucción C:\>ping 172.46.3.74, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta de 1ms.

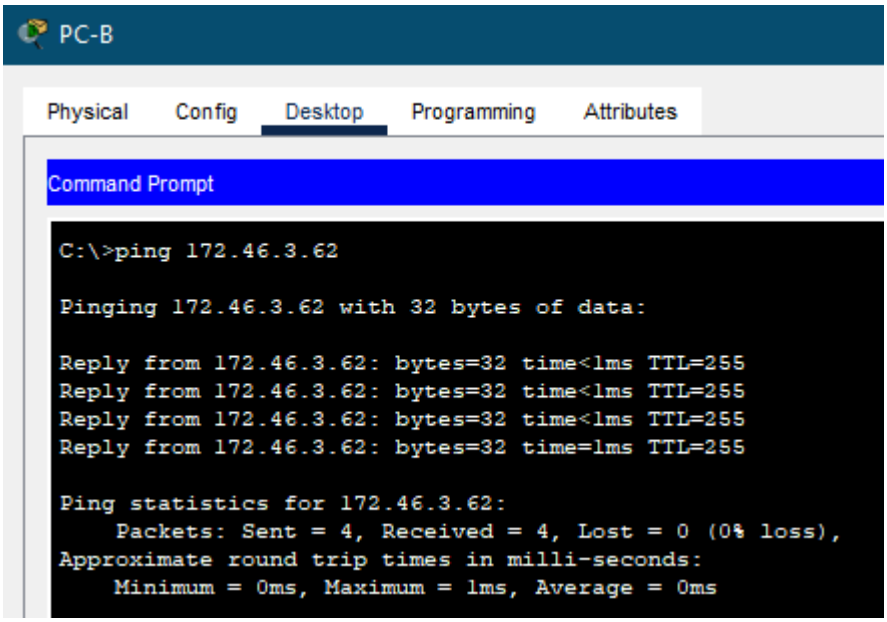
Figura 7. Conectividad de PC-B a R1 G0/0/0



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-B a la interfaz G0/0/0 de R1 con dirección IP 172.46.3.94, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-B y ejecutamos la instrucción C:\>ping 172.46.3.94, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta de 1ms.

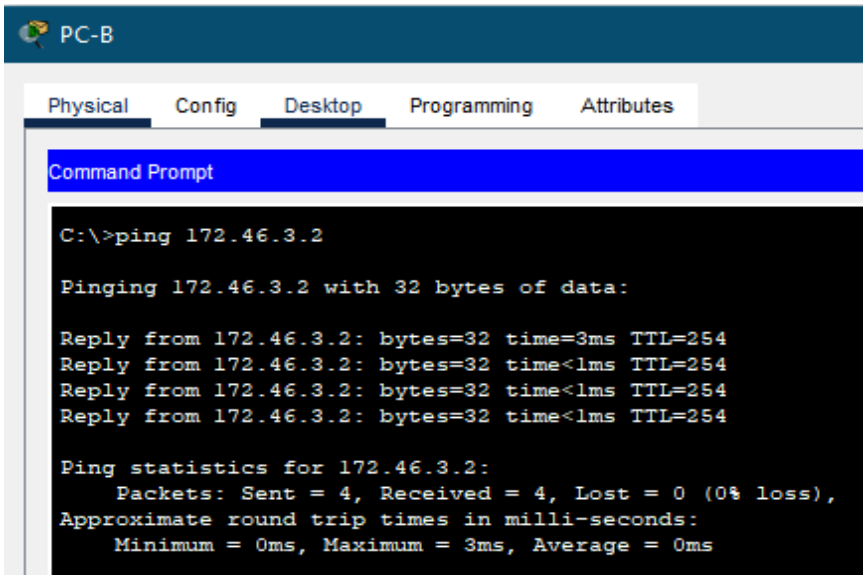
Figura 8. Conectividad de PC-B a R1 G0/0/1



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-B a la interfaz G0/0/1 de R1 con dirección IP 172.46.3.62, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-B y ejecutamos la instrucción C:\>ping 172.46.3.62, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta de 1ms.

Figura 9. Conectividad de PC-B a S1 VLAN1

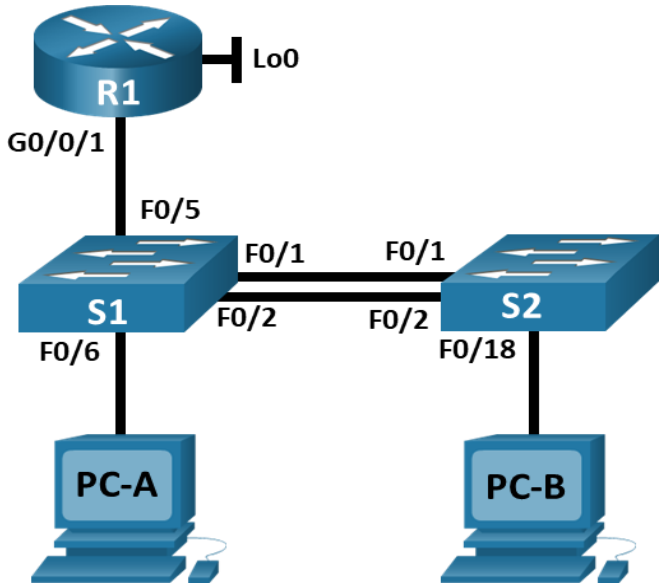


Fuente: Autor

Se realiza la prueba de conectividad desde el PC-B a la interfaz VLAN1 de S1 con dirección IP 172.46.3.2, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-B y ejecutamos la instrucción C:\>ping 172.46.3.2, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta de 1ms.

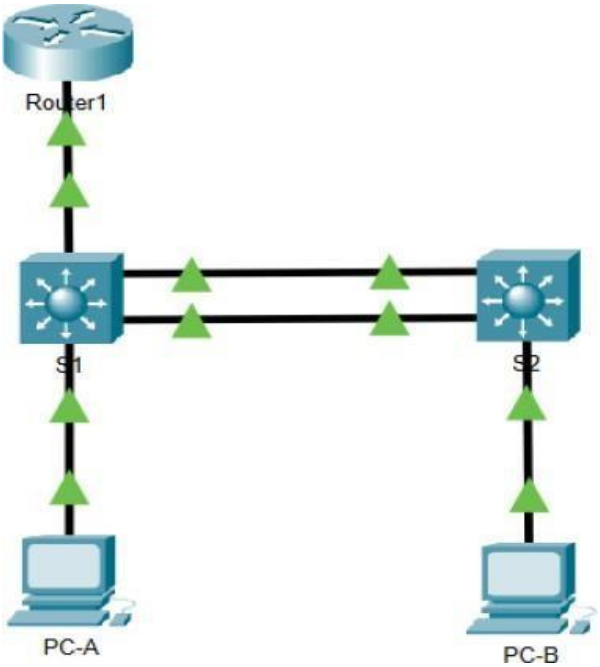
2. ESCENARIO 2

Figura 10. Topología del escenario 2



Fuente: Prueba de habilidades diplomado profundización CCNA

Figura 11. Simulación de la topología del escenario 2



Fuente: Autor

En este escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch también deben administrarse de forma segura. Configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Tabla 8.Tabla de VLAN

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

Tabla de asignación de direcciones

Para el desarrollo del escenario 2 se toma la red 10.46.8.0 y a partir de allí se hace el direccionamiento que se detalla a continuación.

Tabla 9. Asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.20	10.46.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.30	10.46.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.40	10.46.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.56	No corresponde	No corresponde

R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1/64	No corresponde
S1 VLAN 40	10.46.8.98 /29	10.46.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 40	10.46.8.99 /29	10.46.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP paraIPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

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

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

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

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

Para borrar la configuración de inicio en la NVRAM en el Router se utiliza el comando: **erase startup-config.**

Router>enable

Router#erase startup-config

Una vez ejecutado el comando, el sistema pregunta si confirma la eliminación de los archivos de configuración, al continuar el proceso se confirma que se borró la configuración de la NVRAM.

Para borrar las VLAN creadas en el Router se utiliza el comando**: delete vlan.dat**
Router#delete vlan.dat

Al ejecutar el comando me pide la confirmación para borrar el archivo de configuración vlan.dat y para borrarlo de la memoria flash; al no encontrar el archivo Vlan, muestra el siguiente mensaje: **%Error deleting flash:/vlan.dat (No such file or directory)**

Se utilizan los mismos comandos en los Switches para borrar la configuración de inicio en la NVRAM y para borrar las VLAN.

Switch>enable
Switch#erase startup-config
Switch#delete vlan.dat

Se ejecuta el comando para borrar la configuración de inicio en la NVRAM en los Switches y el proceso se realiza correctamente, seguidamente se ejecuta el comando para eliminar las VLAN, pero no es posible borrar el archivo Vlan ya que no se encuentra en los switches.

- Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.

Para recargar el Router y los Switches se utiliza el siguiente comando: **reload**
Router>enable
Router#reload

Switch>enable
Switch#reload

Al ejecutar este comando, el sistema pregunta si confirma el proceso de recarga e inicializa el dispositivo correctamente.

Paso siguiente es verificar la configuración de la plantilla SDM, luego vemos las opciones que se pueden aplicar a la plantilla, posteriormente se habilitan y se

configuran por defecto en la plantilla SDM los protocolos IPv4 e IPv6, recargamos de nuevo la configuración y confirmamos que los cambios se hayan realizado correctamente, mediante los siguientes comandos:

Switch>enable

Switch#show sdm prefer

Switch#configure terminal

Switch(config)#sdm prefer ?

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

Switch(config)#exit

Switch#reload

Switch>enable

Switch#show sdm prefer

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 10. Código de configuración Router R1

Tarea	Especificación
Desactivar la búsqueda DNS	Para la desactivación de DNS utilizamos los siguientes comandos: enable: se ingresa al modo privilegiado configure terminal: se accede al modo de configuración del router no ip domain-lookup: por defecto la búsqueda DNS está activa y con este comando se desactiva, ejecutando las siguientes instrucciones en el Router. Router>enable Router#configure terminal

	Router(config)#no ip domain-lookup
Nombre del router	Con la ejecución de los siguientes comandos, cambiamos el nombre del Router a R1 Router>enable Router#configure terminal Router(config)#hostname R1
Nombre de dominio	Ingresamos al modo de configuración del Router y con la siguiente línea de comandos asignamos a R1 el nombre de dominio: ccna-sa.com R1(config)#ip domain name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	Ingresamos al modo de configuración del Router y ejecutamos los siguientes comandos para cifrar y asignar la contraseña: class enable password: Activa una contraseña para restringir el ingreso al modo EXEC privilegiado service password-encryption: Habilita un cifrado débil a las contraseñas sin cifrar R1>enable R1#configure terminal R1(config)#enable password class R1(config)#service password-encryption R1(config)#exit
Contraseña de acceso a la consola	Ingresamos al modo de configuración de R1, luego accedemos al modo de configuración de consola, ejecutamos la

	contraseña y finalmente por medio de las siguientes líneas de comandos activamos la contraseña: cisco Los comandos utilizados son: line console 0: Configuración de consola. password: Establece la contraseña login: Activa la contraseña R1#configure terminal R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	Ingresamos al modo de configuración de R1 y ejecutamos los siguientes comandos para establecer la longitud mínima de caracteres y la contraseña a modo privilegiado: 5 caracteres security passwords min-length: Establece la longitud mínima de caracteres en las contraseñas R1#configure terminal R1(config)#security passwords min-length 5 R1(config)#enable password cisco
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** username y password: Son los comandos utilizados para acceder a R1 con usuario y clave.

	login local: Activa la base de datos local para el ingreso a la línea de consola Se debe ingresar al modo de configuración de R1, asignar el nombre de usuario y contraseña para la base de datos local, mediante las siguientes líneas de comandos: R1#configure terminal R1(config)#username admin password admin1pass R1(config)#line console 0 R1(config-line)#login local
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Los comandos utilizados son los siguientes: line vty 0 4: Acceder a la interfaz telnet con permiso para 5 conexiones múltiples login local: Habilita la base de datos local para la conexión Las siguientes líneas de comandos en el modo de configuración de R1, nos permiten acceder a la interfaz telnet para la base de datos local. R1#configure terminal R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	Con el comando: transport input SSH, en el modo de configuración de R1 configuramos que solo se permita el acceso a las conexiones SSH en las

	líneas VTY. R1#configure terminal R1(config)#line vty 0 4 R1(config-line)#transport input ssh R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	En el modo de configuración ciframos las contraseñas no cifradas, mediante el siguiente comando para el R1. R1#configure terminal R1(config)#service password-encryption
Configure un MOTD Banner	Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece. Para establecer un mensaje en consola entramos al modo de configuración de R1 y ejecutamos el comando: banner motd, con los siguientes comandos: R1#configure terminal R1(config)#banner motd "R1 - Alvaro Jose Munoz Galarza - Programa: Ingenieria de Sistemas"
Habilitar el routing IPv6	Para habilitar el protocolo de routing IPv6 ingresamos al modo de configuración de R1, mediante los siguientes comandos: R1#configure terminal R1(config)#ipv6 unicast-routing

Configurar interfaz G0/0/1 y subinterfaces	Por medio de los comandos: interface, description, ip address, ipv6 address, ipv6 address link-local-address link-local, no shutdown, en el modo de configuración podemos seleccionar la interfaz, dar una descripción a la interfaz, establecer una dirección IPv4, establecer la dirección IPv6, dirección link-local y activar la interfaz respectivamente, tal como lo vemos a continuación: Selecciono la interfaz y la activo R1#configure terminal R1(config)#interface g0/0/1 R1(config-if)#no shutdown R1(config-if)#interface g0/0/1.20 R1(config-subif)#encapsulation dot1q 20 R1(config-subif)#description Vlan 20 Establezco la dirección IPv4 R1(config-subif)#ip address 10.46.8.1 255.255.255.192 Establezco la dirección local de enlace IPv6, la dirección IPv6 y activo la interfaz R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#no shutdown R1(config-if)#interface g0/0/1.30 R1(config-if)#description Vlan 30 R1(config-subif)#encapsulation dot1q 30 Establezco la dirección IPv4

	R1(config-if)#ip address 10.46.8.65 255.255.255.224 Establezco la dirección local de enlace IPv6, la dirección IPv6 y activo la interfaz R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#no shutdown R1(config-if)#interface g0/0/1.40 R1(config-if)#description Vlan 40 R1(config-subif)#encapsulation dot1q 40 Establezco la dirección IPv4 R1(config-if)#ip address 10.46.8.97 255.255.255.248 Establezco la dirección local de enlace IPv6, la dirección IPv6 y activo la interfaz R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#no shutdown R1(config-if)#interface g0/0/1.56 R1(config-subif)#encapsulation dot1q 56 native R1(config-if)#description Vlan 56 Nativa
Configure el Loopback0 interface	loopback: habilita una interfaz lógica, es un comando utilizado para probar y administrar un dispositivo Cisco IOS, las líneas de comandos son:

	Selecciono la interfaz loopback, doy la descripción y establezco la dirección IPv4 R1#configure terminal R1(config)#interface loopback 0 R1(config-if)#description Loopback 0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 Establezco la dirección local de enlace IPv6, la dirección IPv6 y activo la interfaz 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
Generar una clave de cifrado RSA	En el modo de configuración de R1 ejecutamos los siguientes comandos para crear la clave de encriptación con un módulo de 1024 bits R1#configure terminal R1(config)#crypto key generate rsa general-keys modulus 1024

Paso 3: Configure S1 y S2.

Las tareas de configuración para S1 incluyen lo siguiente:

Tabla 11. Código de configuración Switch S1

Tarea	Especificación
Desactivar la búsqueda DNS.	Ingresamos al modo de configuración y ejecutamos los siguientes

	comandos para desactivar la búsqueda DNS en el Switch. Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch	Con la ejecución de los siguientes comandos, cambiamos el nombre del Switch a S1. Switch>enable Switch#configure terminal Switch(config)#hostname S1 S1(config)#
Nombre de dominio	Ingresamos al modo de configuración del Switch y con la siguiente línea de comandos asignamos a S1 el nombre de dominio: ccna-sa.com S1#enable S1#configure terminal S1(config)#ip domain name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	Ingresamos al modo de configuración del Switch y ejecutamos los siguientes comandos para cifrar y asignar la contraseña: class S1>enable S1#configure terminal S1(config)#enable secret class S1(config)#service password-encryption S1(config)#exit

Contraseña de acceso a la consola	Ingresamos al modo de configuración de S1, luego accedemos al modo de configuración de consola, ejecutamos la contraseña y finalmente por medio de las siguientes líneas de comandos activamos la contraseña: cisco S1>enable S1#configure terminal S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base dedatos local	Nombre de usuario: **admin** Password: **admin1pass** Con la ejecución de los siguientes comandos en el modo de configuración de S1, se asigna el nombre de usuario y contraseña para la base de datos local. S1>enable S1#configure terminal S1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Con la ejecución de los siguientes comandos en el modo de configuración de S1, accedemos a la interfaz telnet para la base de datos local. S1>enable S1#configure terminal S1(config)#line vty 0 4

	S1(config-line)#exit S1(config)#
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	En el modo de configuración de S1 ejecutamos los siguientes comandos para que las líneas VTY solo acepte las conexiones SSH. S1>enable S1#configure terminal S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line)#transport input ssh S1(config-line)#exit S1(config)#
Cifrar las contraseñas de texto no cifrado	Ingresamos al modo de configuración y ejecutamos el comando siguiente para cifrar todas las contraseñas no cifradas en S1 S1(config)#service password-encryption
Configurar un MOTD Banner	Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece. Ingresamos al modo de configuración de S1 y ejecutamos el comando: banner motd, para establecer el mensaje en consola, con los parámetros dados: S1#configure terminal S1(config)#banner motd "S1 - Alvaro Jose Munoz Galarza - Programa:

	Ingenieria de Sistemas"
Generar una clave de cifrado RSA	En el modo de configuración de S1 ejecutamos los siguientes comandos para crear la clave de encriptación con tamaño: Módulo de 1024 bits S1#configure terminal S1(config)#crypto key generate rsa general-keys modulus 1024
Configurar la interfaz de administración (SVI)	En el modo de configuración de interface de SVI de S1, ejecutamos los siguientes comandos para seleccionar la interfaz vlan40, damos una descripción, establecemos las direcciones IPv4, IPv6 capa 3, la dirección local de enlace IPv6 **FE80: :98** y finalmente activamos la interfaz S1>enable S1#configure terminal S1(config)#interface vlan 40 S1(config-if)#description VLAN40 S1(config-if)#ip address 10.46.8.98 255.255.255.248 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
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.46.8.97 para IPv4

	El comando utilizado para configurar el gateway predeterminado de un switch es: ip default-gateway, mediante la siguiente línea de comandos: S1>enable S1#configure terminal S1(config)#ip default-gateway 10.46.8.97

Las tareas de configuración para S2 incluyen lo siguiente:

Tabla 12. Código de configuración Switch S2

Tarea	**Especificación**
Desactivar la búsqueda DNS.	Ingresamos al modo de configuración y ejecutamos los siguientes comandos para desactivar la búsqueda DNS en el Switch. Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch	Con la ejecución de los siguientes comandos, cambiamos el nombre del Switch a S2. Switch>enable Switch#configure terminal Switch(config)#hostname S2 S2(config)#
Nombre de dominio	Ingresamos al modo de configuración del Switch y con la siguiente línea de comandos asignamos a S2 el nombre

	de dominio: ccna-sa.com S2#enable S2#configure terminal S2(config)#ip domain name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	Ingresamos al modo de configuración del Switch y ejecutamos los siguientes comandos para cifrar y asignar la contraseña: class S2>enable S2#configure terminal S2(config)#enable secret class S2(config)#service password-encryption S2(config)#exit
Contraseña de acceso a la consola	Ingresamos al modo de configuración de S2, luego accedemos al modo de configuración de consola, ejecutamos la contraseña y finalmente por medio de las siguientes líneas de comandos activamos la contraseña: cisco S2>enable S2#configure terminal S2(config)#line console 0 S2(config-line)#password cisco S2(config-line)#login S2(config-line)#exit
Crear un usuario administrativo en la base dedatos local	Nombre de usuario: **admin** Password: **admin1pass** Con la ejecución de los siguientes comandos en el modo de

	configuración de S2, se asigna el nombre de usuario y contraseña para la base de datos local. S2>enable S2#configure terminal S2(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Con la ejecución de los siguientes comandos en el modo de configuración de S2, accedemos a la interfaz telnet para la base de datos local. S2>enable S2#configure terminal S2(config)#line vty 0 4 S2(config-line)#exit S2(config)#
Configurar las líneas VTY para que aceptenúnicamente las conexiones SSH	En el modo de configuración de S2 ejecutamos los siguientes comandos para que las líneas VTY solo acepte las conexiones SSH. S2>enable S2#configure terminal S2(config)#line vty 0 4 S2(config-line)#login local S2(config-line)#transport input ssh S2(config-line)#exit S2(config)#
Cifrar las contraseñas de texto no cifrado	Ingresamos al modo de configuración y ejecutamos el comando siguiente para cifrar todas las contraseñas no cifradas en S2

	S2(config)#service password-encryption
Configurar un MOTD Banner	Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece. Ingresamos al modo de configuración de S2 y ejecutamos el comando: banner motd, para establecer el mensaje en consola, con los parámetros dados: S2#configure terminal S2(config)#banner motd "S2 - Alvaro Jose Munoz Galarza - Programa: Ingenieria de Sistemas"
Generar una clave de cifrado RSA	En el modo de configuración de S2 ejecutamos los siguientes comandos para crear la clave de encriptación con tamaño: Módulo de 1024 bits S2#configure terminal S2(config)#crypto key generate rsa general-keys modulus 1024
Configurar la interfaz de administración (SVI)	En el modo de configuración de interface de SVI de S2, ejecutamos los siguientes comandos para seleccionar la interfaz vlan40, damos una descripción, establecemos las direcciones IPv4, IPv6 capa 3, la dirección local de enlace IPv6

	FE80: :99 y finalmente activamos la interfaz S2>enable S2#configure terminal S2(config)#interface vlan 40 S2(config-if)#description VLAN40 S2(config-if)#ip address 10.46.8.99 255.255.255.248 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
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.46.8.97 para IPv4 El comando utilizado para configurar el gateway predeterminado de S2 es: ip default-gateway, mediante la siguiente línea de comandos: S2>enable S2#configure terminal S2(config)#ip default-gateway 10.46.8.97

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

Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 13. Configuración de infraestructura de red del Switch S1

Tarea	Especificación
Crear VLAN	Los siguientes comandos permiten crear y dar un nombre a las VLAN relacionadas, mediante las siguientes instrucciones: S1>enable S1#configure terminal Creo VLAN 20, nombre Docentes S1(config)#vlan 20 S1(config-vlan)#name Docentes Creo VLAN 30, nombre Estudiantes S1(config)#vlan 30 S1(config-vlan)#name Estudiantes Creo VLAN 40, nombre Invitados S1(config)#vlan 40 S1(config-vlan)#name Invitados Creo VLAN 50, nombre Usuarios S1(config)#vlan 50 S1(config-vlan)#name Usuarios Creo VLAN 56, nombre Native S1(config)#vlan 56 S1(config-vlan)#name Native S1(config-vlan)#exit S1(config)#end Con el siguiente comando confirmo que se hayan creado las VLAN: S1#show vlan brief

Crear troncos 802.1Q que utilicen la VLAN 56 nativa	Interfaces F0/1, F0/2 y F0/5 switchport mode trunk: permite configurar un puerto de switch en modo de enlace troncal permanente. switchport trunk native: especifica la vlan nativa para enlace troncal 802.1Q Ingresamos al modo de configuración de interfaz, configuramos el puerto en modo troncal, especificamos la vlan 56 como nativa con enlace troncal 802.1Q, finalmente volvemos al modo exec privilegiado, mediante las siguientes líneas de comandos: S1>enable S1#configure terminal S1(config)#interface range f0/1, f0/2 S1(config-if-range)#switchport trunk native vlan 56 S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#no shutdown S1(config-if-range)#exit S1(config)#interface f0/5 S1(config-if)#switchport trunk native vlan 56 S1(config-if)#switchport mode trunk S1(config-if-range)#no shutdown S1(config-if)#end S1#

Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación Se ingresa al modo de configuración de interfaz, seleccionamos las interfaces para crear el grupo de puertos Etherchannel y lo activamos. S1>enable S1#configure terminal S1(config)#interface range f0/1,f0/2 S1(config-if-range)#channel-group 1 mode active
Configurar el puerto de acceso de host paraVLAN 20	Interface F0/6 Ingresamos al modo de configuración de interfaz, seleccionamos la interfaz f0/6 y configuramos el puerto de acceso de host para Vlan 20, mediante los siguientes comandos: S1>enable S1#configure terminal S1(config)#interface f0/6 S1(config-if)#no shutdown S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 20
Configurar la seguridad del puerto en los puertos de acceso	Permitir 4 direcciones MAC switchport mode access: permite establecer la interfaz en modo de acceso switchport port-security: comando para permitir la seguridad de puerto a la interfaz seleccionada Ingresamos al modo de configuración

	de interfaz, seleccionamos el puerto a configurar la seguridad de acceso F0/6, establecemos a la interfaz el modo de acceso y la seguridad, asignamos la cantidad máxima de 4 direcciones MAC permitidas y finalmente se habilita el aprendizaje por persistencia, mediante los siguientes comandos configuramos la seguridad en el puerto: S1>enable S1#configure terminal S1(config)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 4 S1(config-if)#switchport port-security mac-address sticky
Proteja todas las interfaces no utilizadas	Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar Se ingresa al modo de configuración de interfaz, seleccionamos las interfaces, damos el modo de acceso a los puertos escogidos, los asignamos a la Vlan 50, apagamos la interfaz y finalmente damos una descripción. Esta configuración se hace mediante los siguientes comandos: S1>enable S1#configure terminal 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)#shutdown S1(config-if-range)#description Puertos no utilizados S1(config-if-range)#end S1#

Paso 5: Configure el S2.

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

Tabla 14. Configuración de infraestructura de red del Switch S2

Tarea	Especificación
Crear VLAN	Los siguientes comandos permiten crear y dar un nombre a las VLAN relacionadas, mediante las siguientes instrucciones: S2>enable S2#configure terminal Creo VLAN 20, nombre Docentes S2(config)#vlan 20 S2(config-vlan)#name Docentes Creo VLAN 30, nombre Estudiantes S2(config)#vlan 30 S2(config-vlan)#name Estudiantes Creo VLAN 40, nombre Invitados S2(config)#vlan 40 S2(config-vlan)#name Invitados

	Creo VLAN 50, nombre Usuarios S2(config)#vlan 50 S2(config-vlan)#name Usuarios Creo LAN 56, nombre Native S2(config)#vlan 56 S2(config-vlan)#name Native S2(config-vlan)#exit S2(config)#end Con el siguiente comando confirmo que se hayan creado las VLAN: S2#show vlan brief
Crear troncos 802.1Q que utilicen la VLAN 56 nativa	Interfaces F0/1 y F0/2 Ingresamos al modo de configuración de interfaz, configuramos el puerto en modo troncal, especificamos la vlan 56 como nativa con enlace troncal 802.1Q, finalmente volvemos al modo exec privilegiado, mediante las siguientes líneas de comandos: S2>enable S2#configure terminal S2(config)#interface range f0/1, f0/2 S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 56 S2(config-if-range)#no shutdown S2(config-if)#end S2#

Crear un grupo de puertos EtherChannel deCapa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación Se ingresa al modo de configuración de interfaz, seleccionamos las interfaces para crear el grupo de puertos Etherchannel y lo activamos. S2>enable S2#configure terminal S2(config)#interface range f0/1,f0/2 S2(config-if-range)#channel-group 1 mode active
Configurar el puerto de acceso del host para laVLAN 30	Interfaz F0/18 Ingresamos al modo de configuración de interfaz, seleccionamos la interfaz f0/18 y configuramos el puerto de acceso de host para Vlan 30, mediante los siguientes comandos: S2>enable S2#configure terminal S2(config)#interface f0/18 S2(config-if)#no shutdown S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 30
Configure port-security en los access ports	Permite 4 direcciones MAC Ingresamos al modo de configuración de interfaz, seleccionamos el puerto a configurar la seguridad de acceso F0/18, establecemos a la interfaz el modo de acceso y la seguridad, asignamos la cantidad máxima de 4 direcciones MAC permitidas y

	finalmente se habilita el aprendizaje por persistencia, mediante los siguientes comandos configuramos la seguridad en el puerto: S2>enable S2#configure terminal S2(config)#interface f0/18 S2(config-if)#switchport mode access S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 4 S2(config-if)#switchport port-security mac-address sticky
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar Ingresamos al modo de configuración de interfaz, seleccionamos las interfaces, damos el modo de acceso a los puertos escogidos, los asignamos a la Vlan 50, apagamos la interfaz y finalmente damos una descripción. Esta configuración se hace mediante los siguientes comandos: S2>enable S2#configure terminal 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)#shutdown S2(config-if-range)#description Puertos

	no utilizados S2(config-if)#end S1#

Parte 2: Configurar soporte de host

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 15. Configuración de soporte de host en Router R1

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0 ip route: configura la ruta por defecto de forma estática en el router. Ingresamos al modo de configuración de R1, se configura la ruta estática predeterminada para IPv4 e IPv6 para dirigir el tráfico a la interfaz Loopback 0, mediante los siguientes comandos: R1>enable R1#configure terminal R1(config)#ip route 0.0.0.0 0.0.0.0 loopback0 R1(config)#ipv6 route ::/0 loopback0
Configurar IPv4 DHCP para VLAN 20	Cree un grupo DHCP para VLAN 20, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sa.net yespecifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada ip dhcp excluded-address: este comando se

	utiliza para excluir direcciones IPv4 estáticas específicas. ip dhcp pool: Comando para ingresar al router en el modo de configuración DHCPv4 y crear un pool con el nombre especificado. network: instrucción que permite definir el rango de direcciones ip disponibles default-router: es utilizado para definir el router de gateway predeterminado Ingresamos al modo de configuración de R1, excluimos las direcciones que serán utilizadas por otros dispositivos como servidores, entramos al modo de configuración DHCP, asignamos el nombre LAN POOL VLAN20 al pool y definimos el rango de direcciones ip, configuramos la puerta de enlace y por último le damos el nombre de dominio unad-ccna-sa.net, mediante las siguientes líneas de comandos: R1>enable R1#configure terminal R1(config)#ip dhcp excluded-address 10.46.8.1 10.46.8.52 R1(config)#ip dhcp excluded-address 10.46.8.63 R1(config)#ip dhcp pool LAN_POOL_VLAN20 R1(dhcp-config)#network 10.46.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.46.8.1 R1(dhcp-config)#domain-name unad-ccna-sa.net R1(dhcp-config)#exit
Configurar DHCP IPv4 para VLAN 30	Cree un grupo DHCP para VLAN 30, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sb.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada

	Ingresamos al modo de configuración de R1, excluimos las direcciones que serán utilizadas por otros dispositivos como servidores, entramos al modo de configuración DHCP, asignamos el nombre LAN POOL VLAN30 al pool y definimos el rango de direcciones ip, configuramos la puerta de enlace y por último le damos el nombre de dominio unad-ccna-sb.net, mediante las siguientes líneas de comandos: R1>enable R1#configure terminal R1(config)#ip dhcp excluded-address 10.46.8.65 10.46.8.84 R1(config)#ip dhcp excluded-address 10.46.8.95 R1(config)#ip dhcp pool LAN_POOL_VLAN30 R1(dhcp-config)#network 10.46.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.46.8.65 R1(dhcp-config)#domain-name unad-ccna-sb.net R1(dhcp-config)#exit

Paso 2: Configurar los servidores

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

Tabla 16. Configuración de host PC-A

Configuración de red de PC-A	
Descripción	PC-A
Dirección física	0030.A32E.2DC8
Dirección IP	10.46.8.53

Máscara de subred	255.255.255.192
Gateway predeterminado	10.46.8.1
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Tabla 17. Configuración de host PC-B

Configuración de red de PC-B	
Descripción	PC-B
Dirección física	0007.ECC1.CB1C
Dirección IP	10.46.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.46.8.65
Gateway predeterminado IPv6	2001:DB8:ACAD:B::1

Parte 3: Probar y verificar la conectividad de extremo a extremo

Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

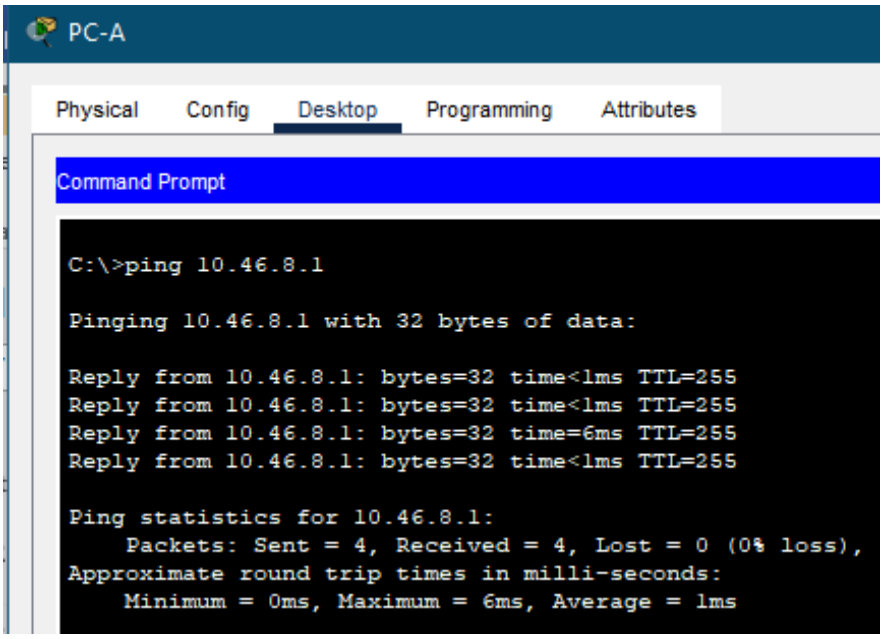
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 18. Pruebas de conectividad entre dispositivos

Desde	**A**		**Dirección IP**	**Resultados de ping**
PC-A	R1, G0/0/1.2	IPv4	10.46.8.1	Exitoso – Figura 12
		IPv6	2001:db8:acad:a::1	Exitoso – Figura 13
	R1, G0/0/1.3	IPv4	10.46.8.65	Exitoso – Figura 14
		IPv6	2001:db8:acad:b::1	Exitoso – Figura 15
	R1, G0/0/1.4	IPv4	10.46.8.97	Exitoso – Figura 16
		IPv6	2001:db8:acad:c::1	Exitoso – Figura 17
	S1, VLAN 40	IPv4	10.46.8.98	Exitoso – Figura 18

		IPv6	2001:db8:acad:c::98	Fallido – Figura 19
	S2, VLAN 40	IPv4	10.46.8.99	Exitoso – Figura 20
		IPv6	2001:db8:acad:c::99	Fallido – Figura 21
	PC-B	IPv4	10.46.8.85	Exitoso – Figura 22
		IPv6	2001:db8:acad:b::50	Exitoso – Figura 23
	R1 Bucle 0	IPv4	209.165.201.1	Exitoso – Figura 24
		IPv6	2001:db8:acad:209::1	Exitoso – Figura 25
PC-B	R1 Bucle 0	IPv4	209.165.201.1	Exitoso – Figura 26
		IPv6	2001:db8:acad:209::1	Exitoso – Figura 27
	R1, G0/0/1.2	IPv4	10.46.8.1	Exitoso – Figura 28
		IPv6	2001:db8:acad:a::1	Exitoso – Figura 28
	R1, G0/0/1.3	IPv4	10.46.8.65	Exitoso – Figura 30
		IPv6	2001:db8:acad:b::1	Exitoso – Figura 31
	R1, G0/0/1.4	IPv4	10.46.8.97	Exitoso – Figura 32
		IPv6	2001:db8:acad:c::1	Exitoso – Figura 33
	S1, VLAN 40	IPv4	10.46.8.98	Exitoso – Figura 34
		IPv6	2001:db8:acad:c::98	Fallido – Figura 35
	S2, VLAN 40	IPv4	10.46.8.99	Exitoso – Figura 36
		IPv6	2001:db8:acad:c::99	Fallido – Figura 37

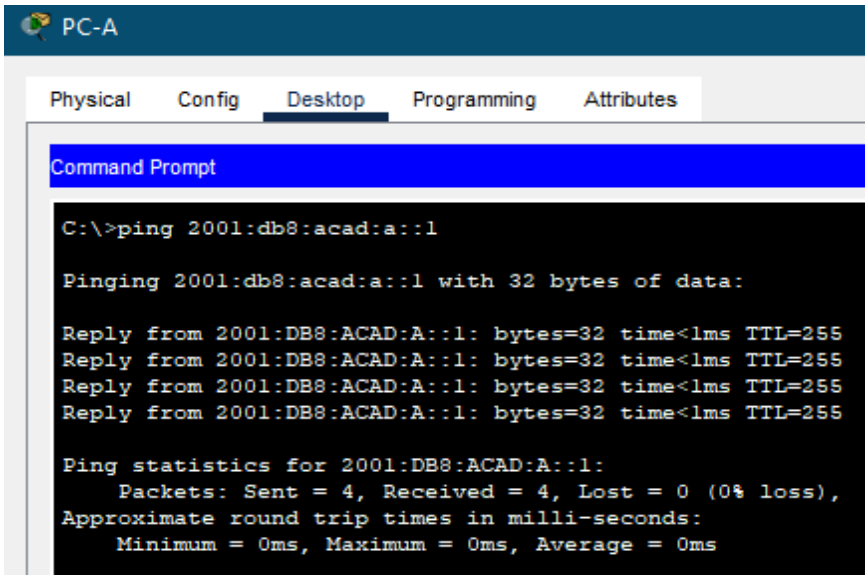
Figura 12. Conectividad de PC-A a R1 G0/0/1.2 IPv4



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-A a la interfaz G0/0/1.2 de R1 con dirección IP 10.46.8.1, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-A y ejecutamos la instrucción C:\>ping 10.46.8.1, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta promedio de 1ms.

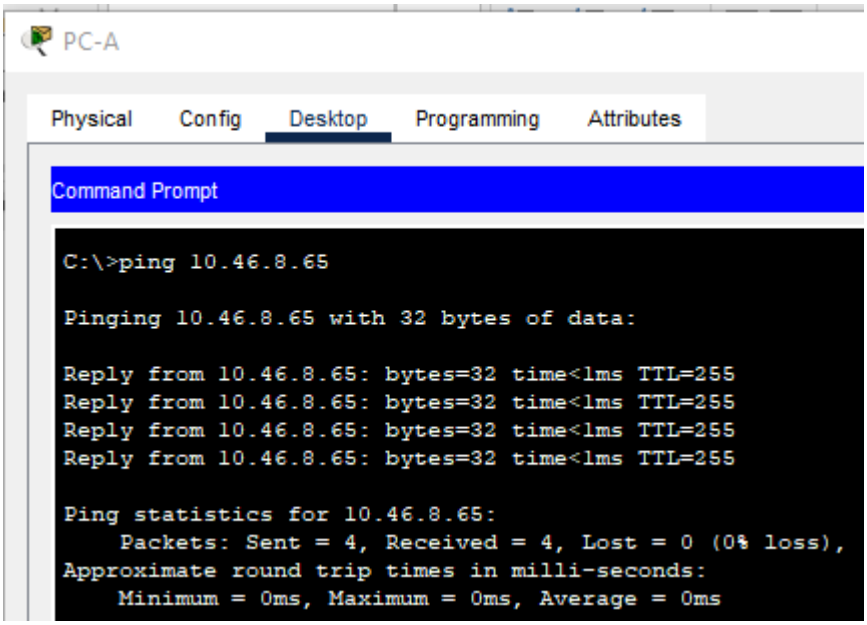
Figura 13. Conectividad de PC-A a R1 G0/0/1.2 IPv6



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-A a la interfaz G0/0/1.2 de R1 con dirección IP 2001:db8:acad:a::1, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-A y ejecutamos la instrucción C:\>ping 2001:db8:acad:a::1, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta de 1ms.

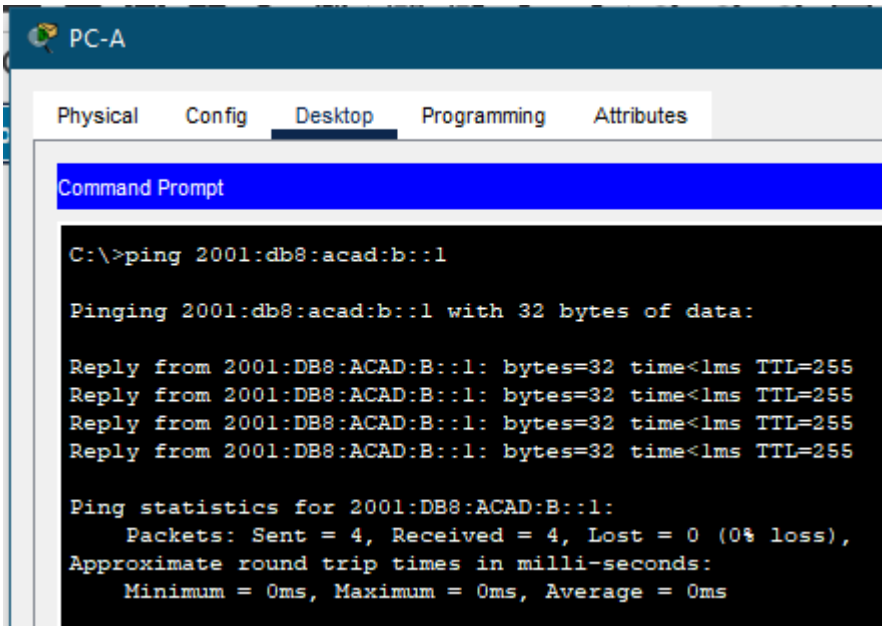
Figura 14. Conectividad de PC-A a R1 G0/0/1.3 IPv4



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-A a la interfaz G0/0/1.3 de R1 con dirección IP 10.46.8.65, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-A y ejecutamos la instrucción C:\>ping 10.46.8.65, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta de 1ms.

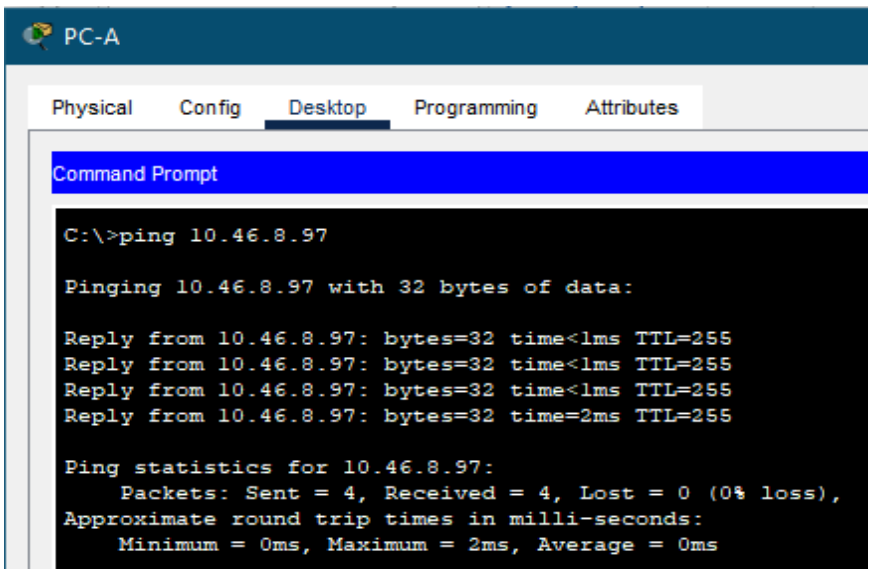
Figura 15. Conectividad de PC-A a R1 G0/0/1.3 IPv6



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-A a la interfaz G0/0/1.3 de R1 con dirección IP 2001:db8:acad:b::1, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-A y ejecutamos la instrucción C:\>ping 2001:db8:acad:b::1, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta de 1ms.

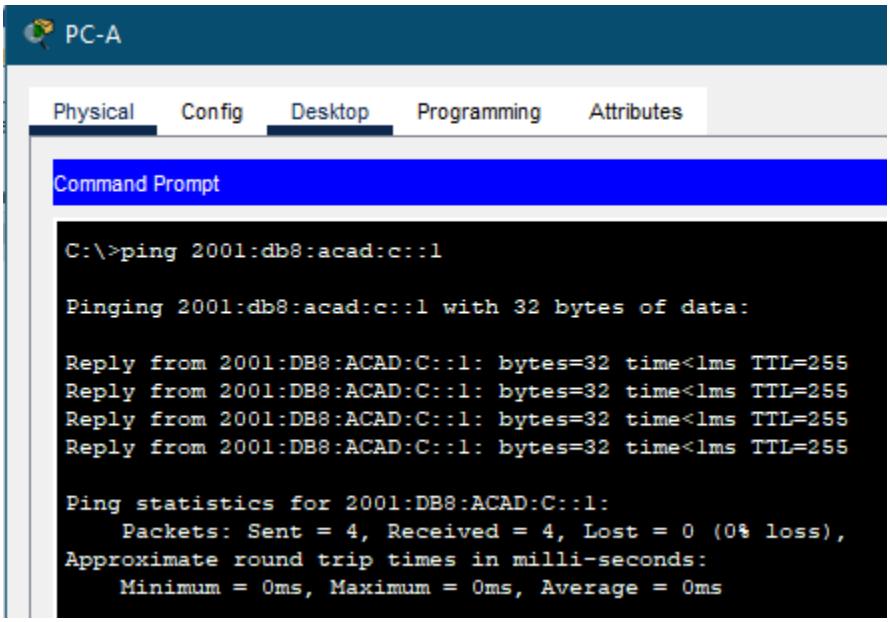
Figura 16. Conectividad de PC-A a R1 G0/0/1.4 IPv4



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-A a la interfaz G0/0/1.4 de R1 con dirección IP 10.46.8.97, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-A y ejecutamos la instrucción C:\>ping 10.46.8.97, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta de 1ms.

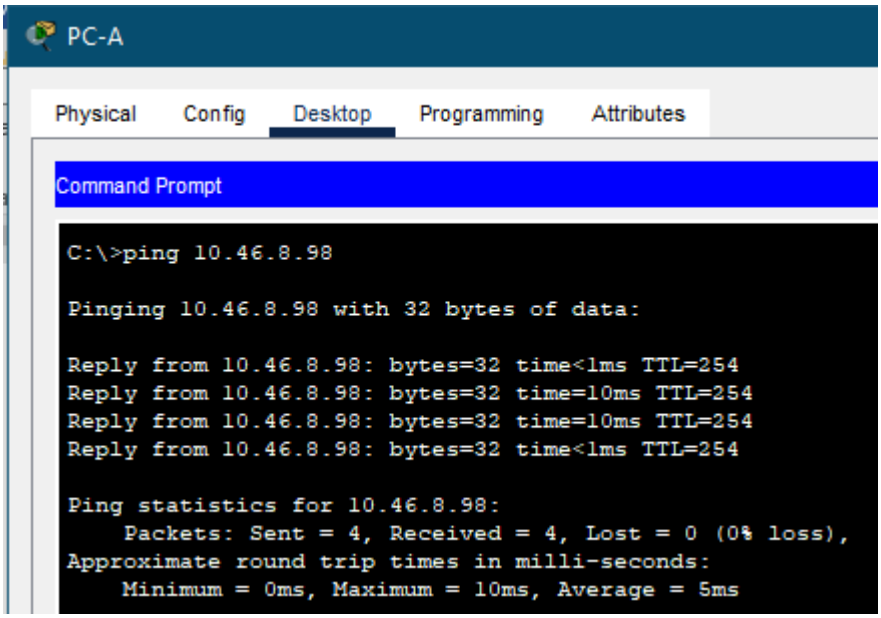
Figura 17. Conectividad de PC-A a R1 G0/0/1.4 IPv6



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-A a la interfaz G0/0/1.4 de R1 con dirección IP 2001:db8:acad:c::1, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-A y ejecutamos la instrucción C:\>ping 2001:db8:acad:c::1, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta de 1ms.

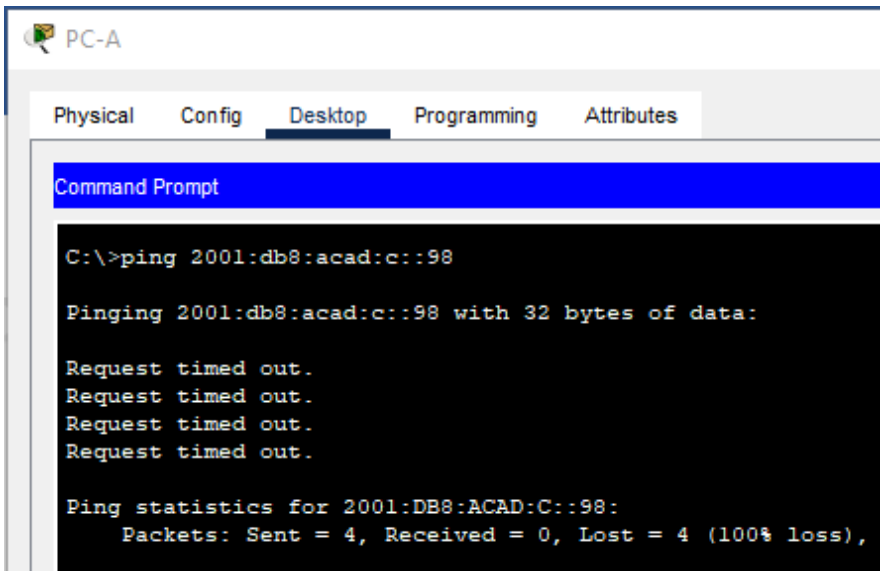
Figura 18. Conectividad de PC-A a S1 VLAN 40 IPv4



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-A a la SVI VLAN 40 de S1 con dirección IP 10.46.8.98, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-A y ejecutamos la instrucción C:\>ping 10.46.8.98, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta promedio de 5ms.

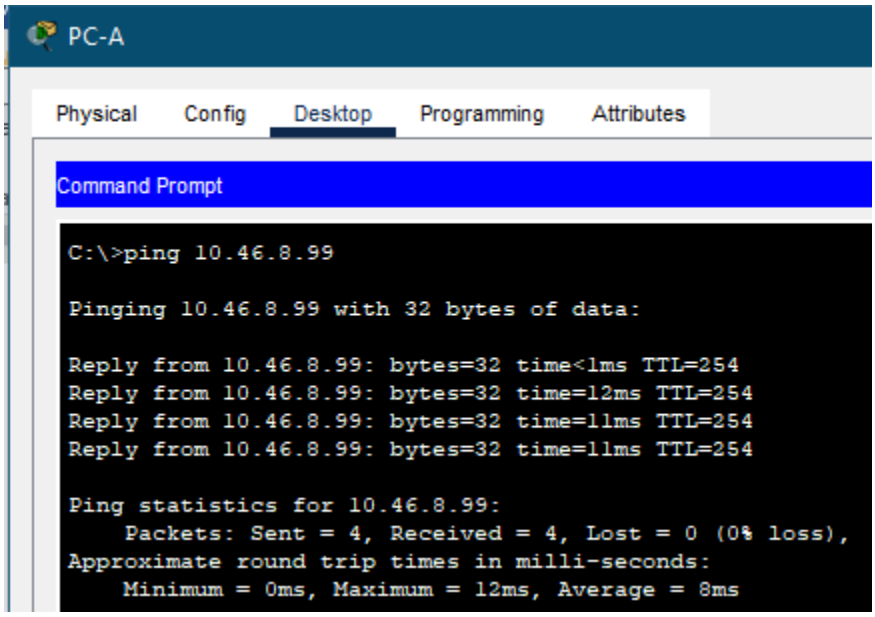
Figura 19. Conectividad de PC-A a S1 VLAN 40 IPv6



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-A a la SVI VLAN 40 de S1 con dirección IPv6 2001:db8:acad:c::98, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-A y ejecutamos la instrucción C:\>ping 2001:db8:acad:c::98, sin obtener respuesta del host de destino con 4 paquetes enviados y 4 paquetes perdidos. Teniendo en cuenta que la configuración para el protocolo IPv6 se encuentra habilitado y las pruebas con otras interfaces y dispositivos se ejecutaron exitosamente, se deduce que el error que se presenta en la prueba de conectividad es debido al simulador utilizado.

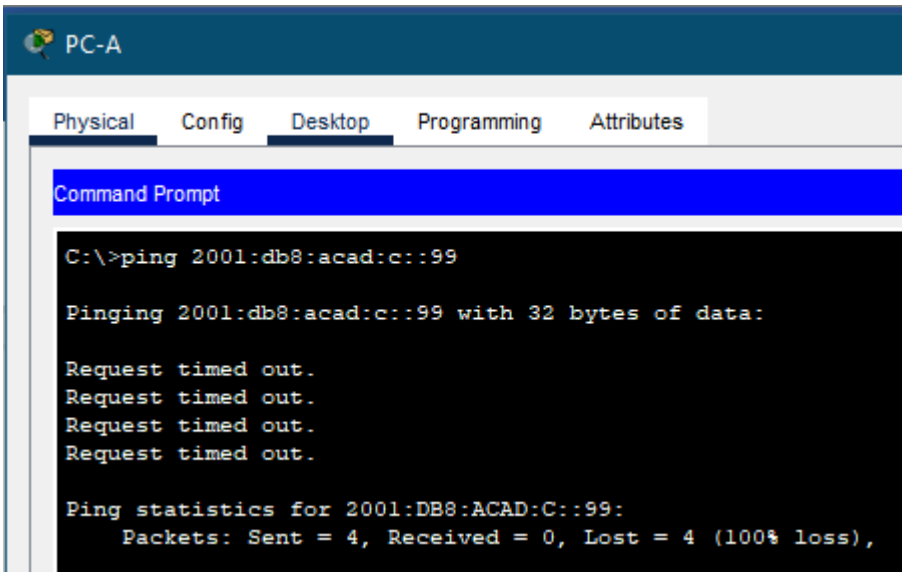
Figura 20. Conectividad de PC-A a S2 VLAN 40 IPv4



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-A a la SVI VLAN 40 de S2 con dirección IP 10.46.8.99, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-A y ejecutamos la instrucción C:\>ping 10.46.8.99, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta promedio de 8ms.

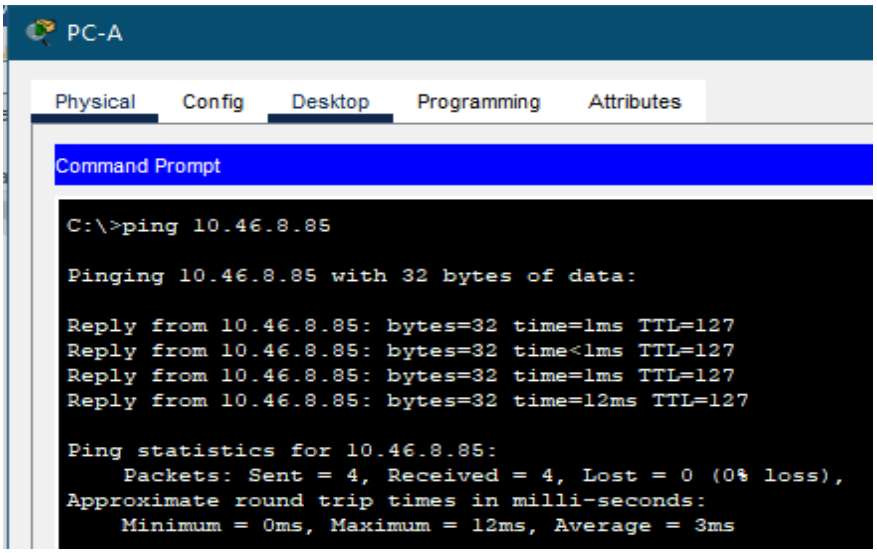
Figura 21. Conectividad de PC-A a S2 VLAN 40 IPv6



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-A a la SVI VLAN 40 de S2 con dirección IPv6 2001:db8:acad:c::99, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-A y ejecutamos la instrucción C:\>ping 2001:db8:acad:c::99, sin obtener respuesta del host de destino con 4 paquetes enviados y 4 paquetes perdidos. Teniendo en cuenta que la configuración para el protocolo IPv6 se encuentra habilitado y las pruebas con otras interfaces y dispositivos se ejecutaron exitosamente, se deduce que el error que se presenta en la prueba de conectividad es debido al simulador utilizado.

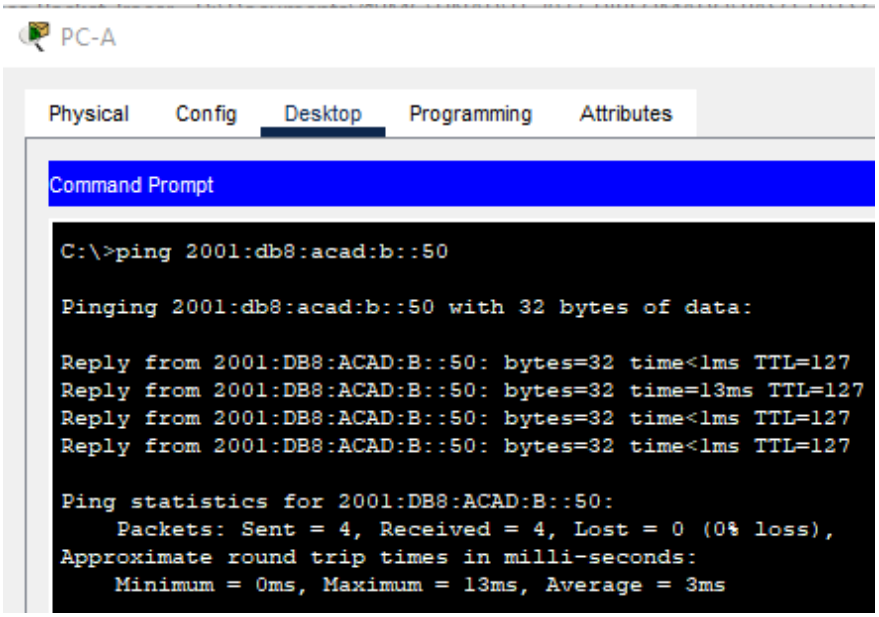
Figura 22.Conectividad de PC-A a PC-B IPv4



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-A a PC-B con dirección IP 10.46.8.85, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-A y ejecutamos la instrucción C:\>ping 10.46.8.85, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta promedio de 3ms.

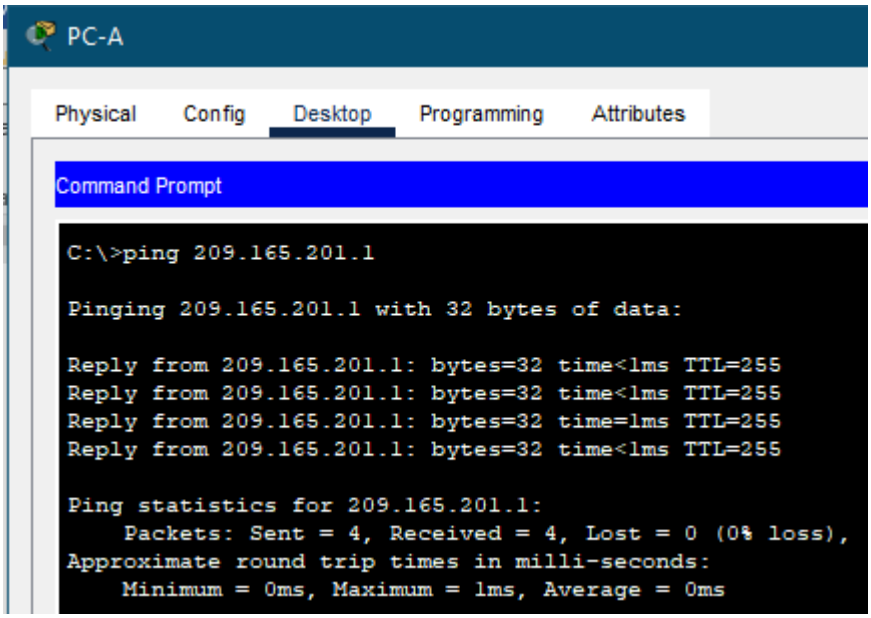
Figura 23. Conectividad de PC-A a PC-B IPv6



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-A a PC-B con dirección IP 2001:db8:acad:b::50, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-A y ejecutamos la instrucción C:\>ping 2001:db8:acad:b::50, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta promedio de 3ms.

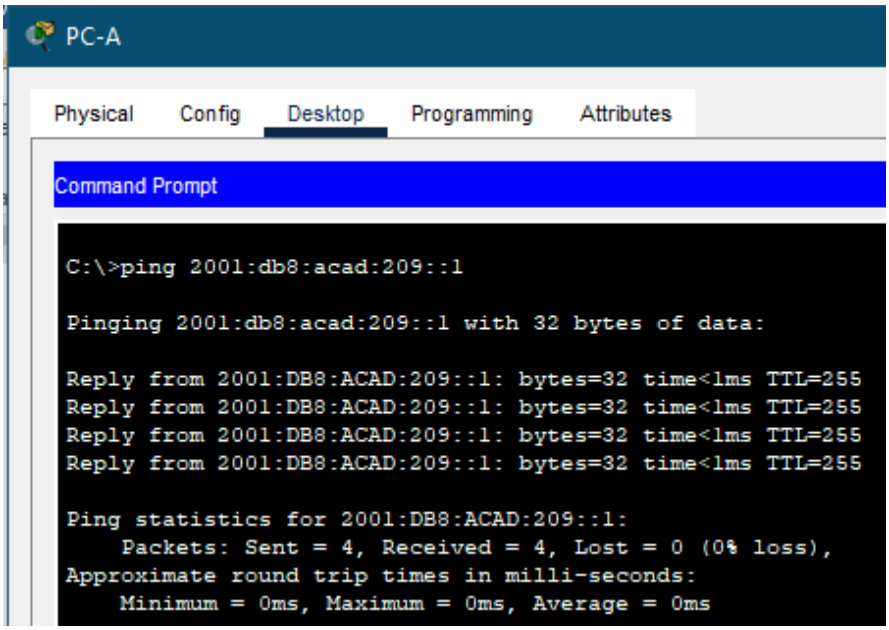
Figura 24. Conectividad de PC-A a R1 Loopback 0 IPv4



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-A a Loopback 0 de R1 con dirección IP 209.165.201.1, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-A y ejecutamos la instrucción C:\>ping 209.165.201.1, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta de 1ms.

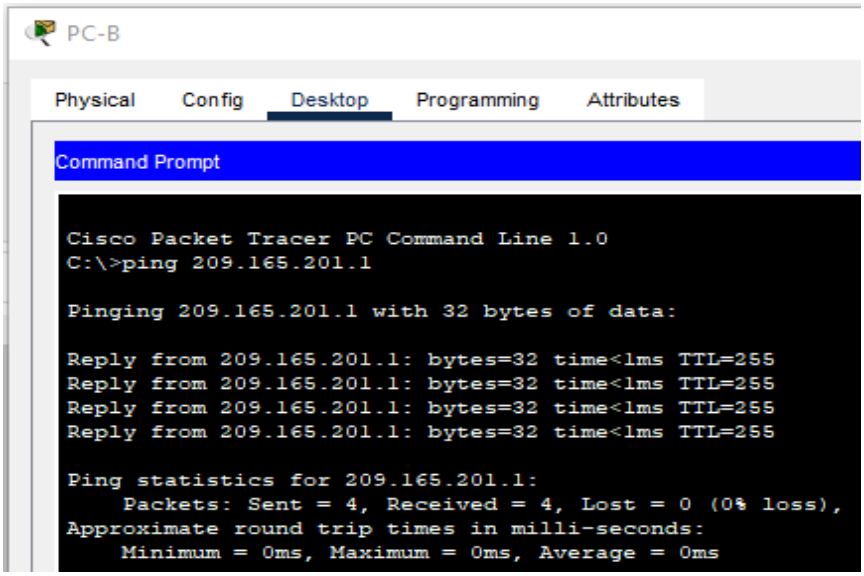
Figura 25. Conectividad de PC-A a R1 Loopback 0 IPv6



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-A a Loopback 0 de R1 con dirección IP 2001:db8:acad:209::1, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-A y ejecutamos la instrucción C:\>ping 2001:db8:acad:209::1, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta de 1ms.

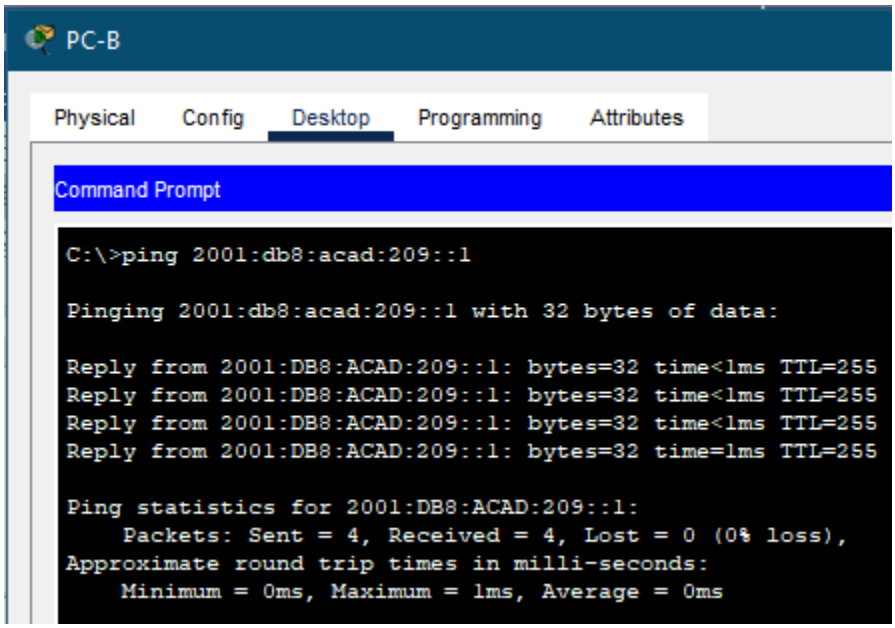
Figura 26. Conectividad de PC-B a R1 Loopback 0 IPv4



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-B a Loopback 0 de R1 con dirección IP 209.165.201.1, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-B y ejecutamos la instrucción C:\>ping 209.165.201.1, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta de 1ms.

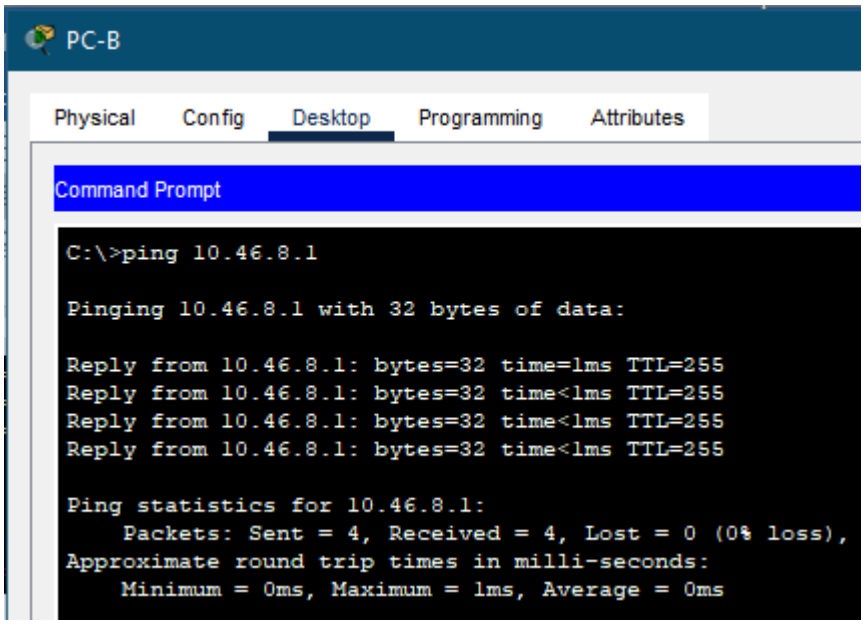
Figura 27. Conectividad de PC-B a R1 Loopback 0 IPv6



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-B a Loopback 0 de R1 con dirección IP 2001:db8:acad:209::1, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-B y ejecutamos la instrucción C:\>ping 2001:db8:acad:209::1, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta de 1ms.

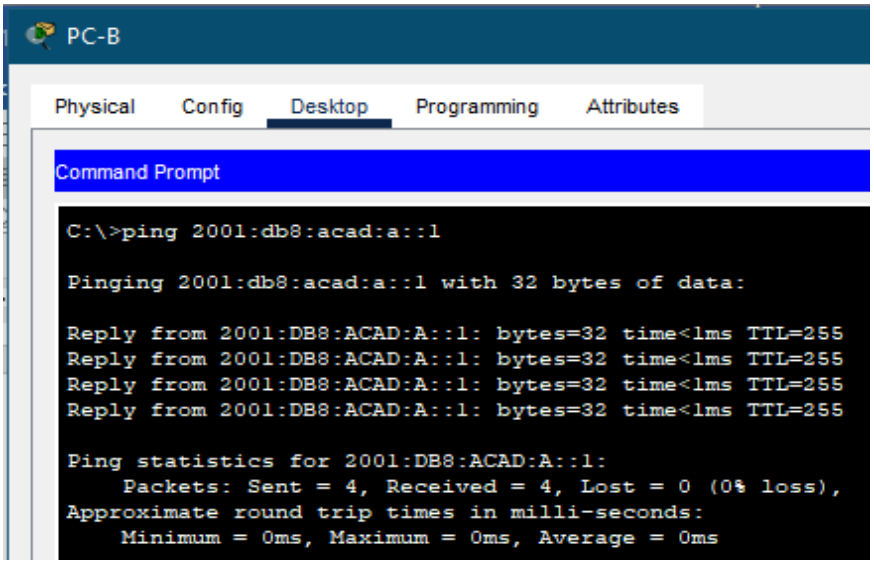
Figura 28. Conectividad de PC-B a R1 G0/0/1.2 IPv4



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-B a la interfaz G0/0/1.2 de R1 con dirección IP 10.46.8.1, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-B y ejecutamos la instrucción C:\>ping 10.46.8.1, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta de 1ms.

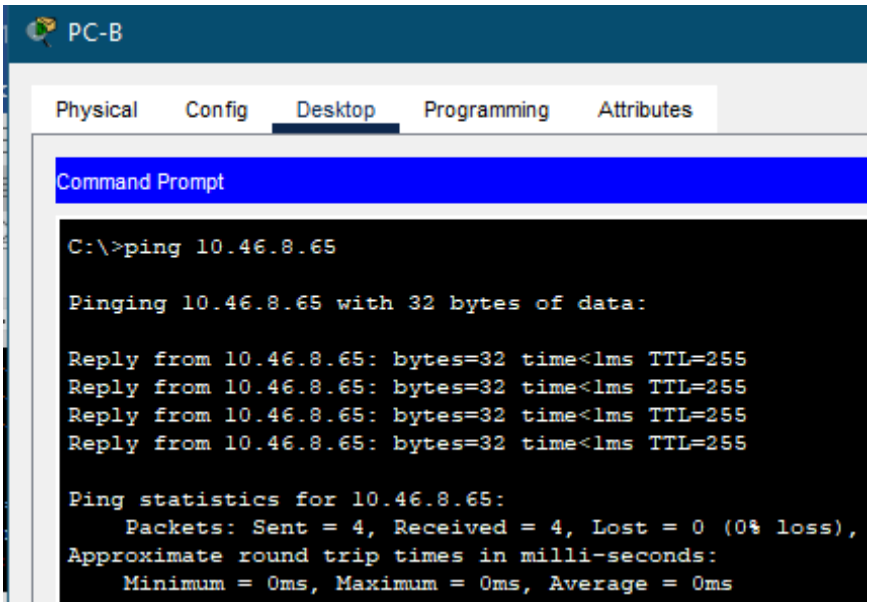
Figura 29. Conectividad de PC-B a R1 G0/0/1.2 IPv6



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-B a la interfaz G0/0/1.2 de R1 con dirección IP 2001:db8:acad:a::1, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-B y ejecutamos la instrucción C:\>ping 2001:db8:acad:a::1, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta de 1ms.

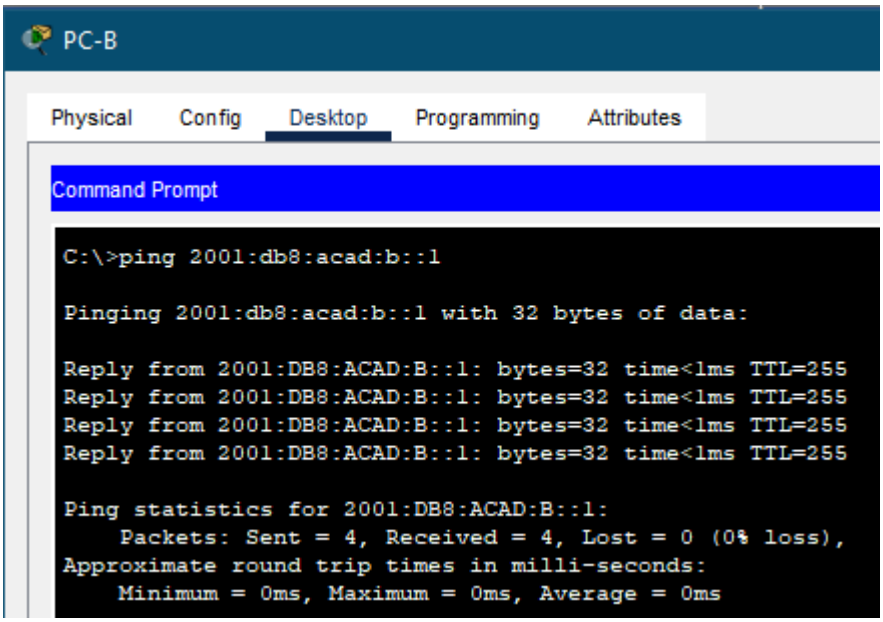
Figura 30. Conectividad de PC-B a R1 G0/0/1.3 IPv4



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-B a la interfaz G0/0/1.3 de R1 con dirección IP 10.46.8.65, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-B y ejecutamos la instrucción C:\>ping 10.46.8.65, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta de 1ms.

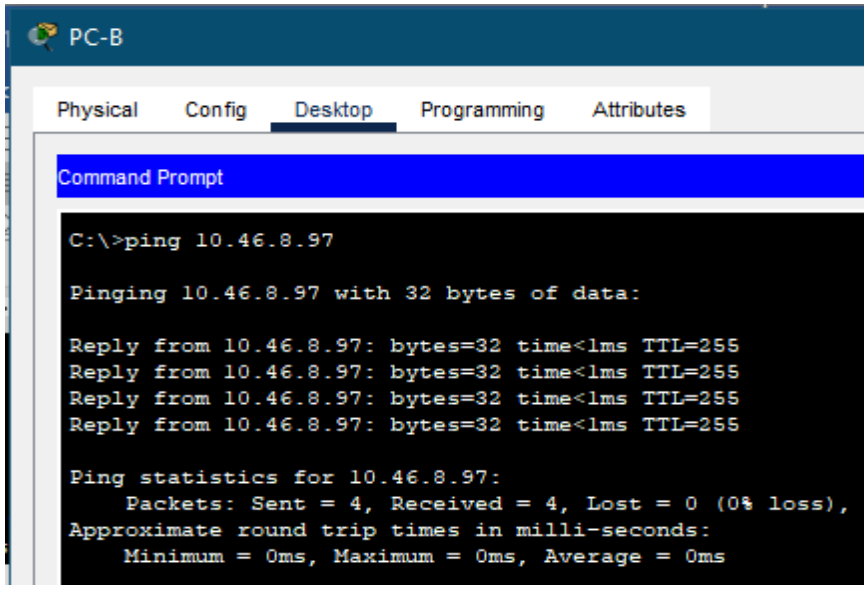
Figura 31. Conectividad de PC-B a R1 G0/0/1.3 IPv6



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-B a la interfaz G0/0/1.3 de R1 con dirección IP 2001:db8:acad:b::1, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-B y ejecutamos la instrucción C:\>ping 2001:db8:acad:b::1, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta de 1ms.

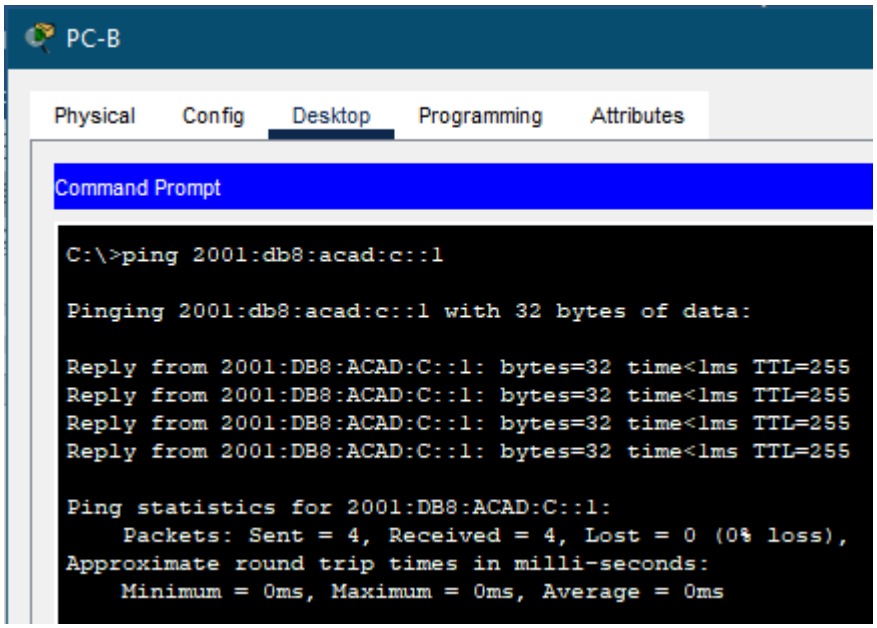
Figura 32. Conectividad de PC-B a R1 G0/0/1.4 IPv4



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-B a la interfaz G0/0/1.4 de R1 con dirección IP 10.46.8.97, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-B y ejecutamos la instrucción C:\>ping 10.46.8.97, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta de 1ms.

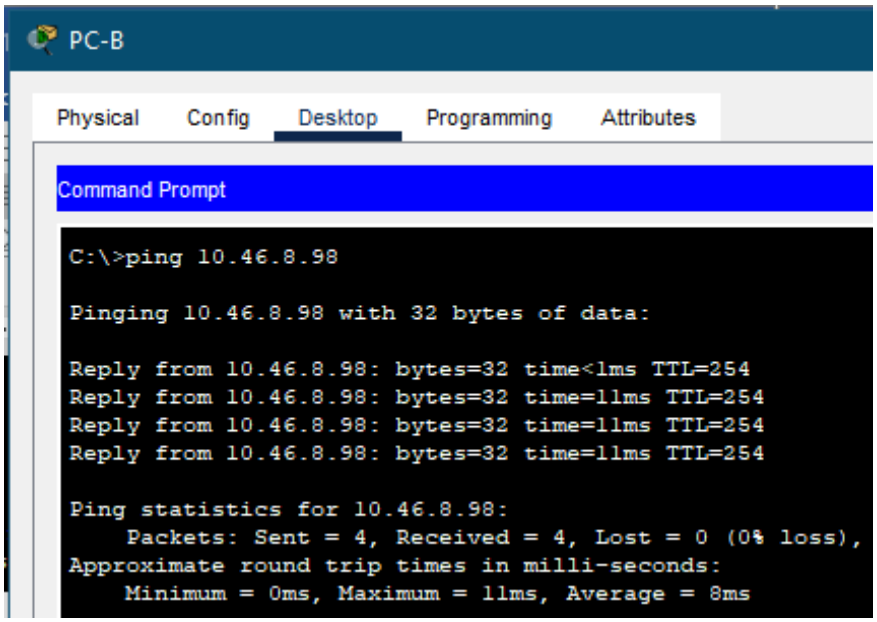
Figura 33. Conectividad de PC-B a R1 G0/0/1.4 IPv6



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-B a la interfaz G0/0/1.4 de R1 con dirección IP 2001:db8:acad:c::1, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-B y ejecutamos la instrucción C:\>ping 2001:db8:acad:c::1, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta de 1ms.

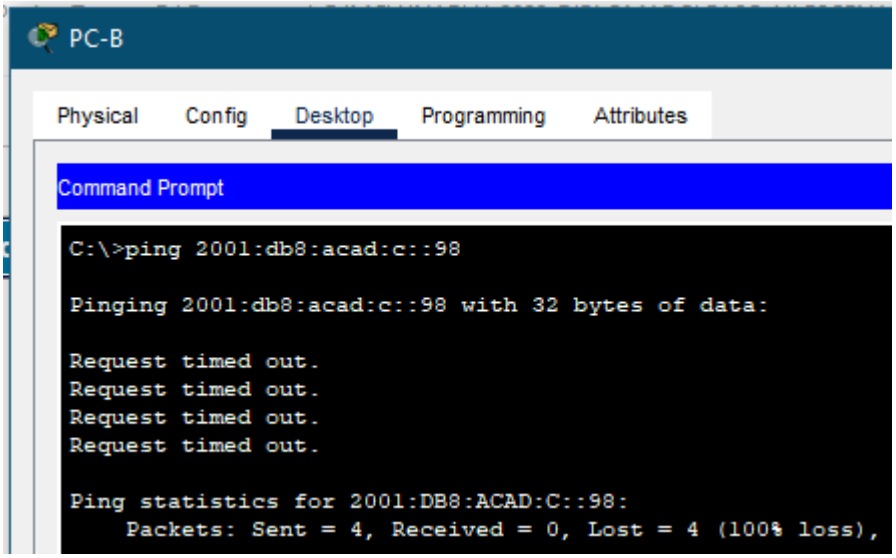
Figura 34. Conectividad de PC-B a S1 VLAN 40 IPv4



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-B a la SVI VLAN 40 de S1 con dirección IP 10.46.8.98, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-B y ejecutamos la instrucción C:\>ping 10.46.8.98, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta promedio de 8ms.

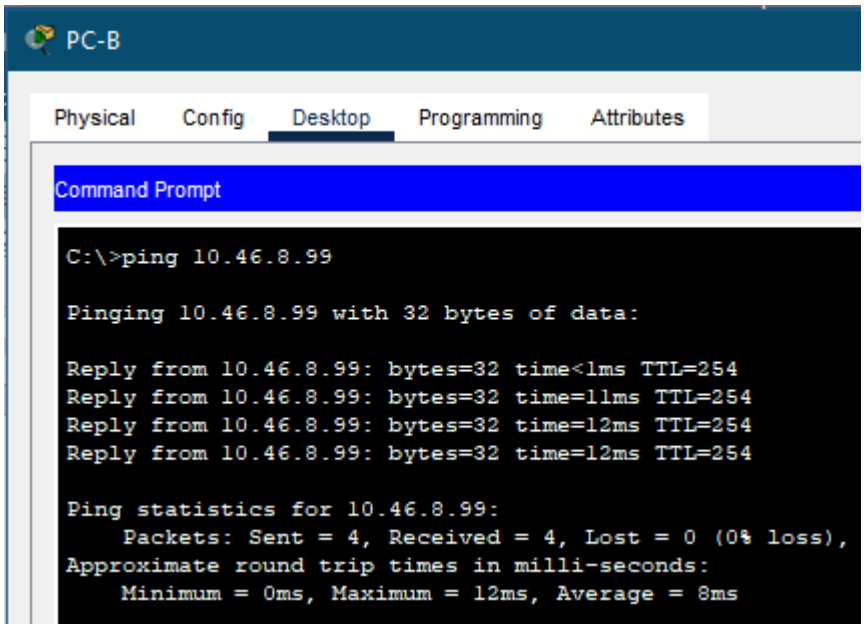
Figura 35. Conectividad de PC-B a S1 VLAN 40 IPv6



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-A a la SVI VLAN 40 de S1 con dirección IPv6 2001:db8:acad:c::98, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-A y ejecutamos la instrucción C:\>ping 2001:db8:acad:c::98, sin obtener respuesta del host de destino con 4 paquetes enviados y 4 paquetes perdidos. Teniendo en cuenta que la configuración para el protocolo IPv6 se encuentra habilitado y las pruebas con otras interfaces y dispositivos se ejecutaron exitosamente, se deduce que el error que se presenta en la prueba de conectividad es debido al simulador utilizado.

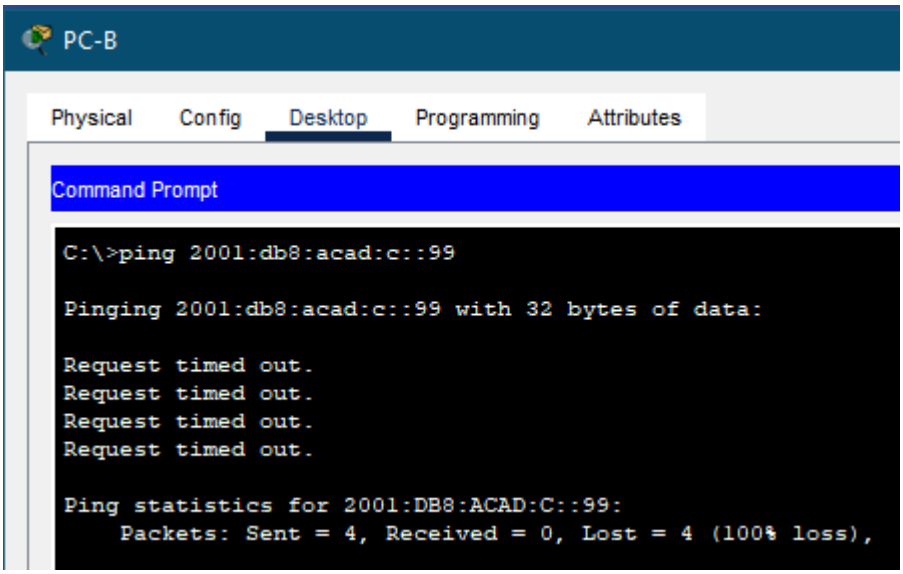
Figura 36. Conectividad de PC-B a S2 VLAN 40 IPv4



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-B a la SVI VLAN 40 de S2 con dirección IP 10.46.8.99, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-B y ejecutamos la instrucción C:\>ping 10.46.8.99, obteniendo respuesta del host de destino con 4 paquetes enviados y 4 paquetes recibidos con un tiempo de respuesta promedio de 8ms.

Figura 37. Conectividad de PC-B a S2 VLAN 40 IPv6



Fuente: Autor

Se realiza la prueba de conectividad desde el PC-A a la SVI VLAN 40 de S2 con dirección IPv6 2001:db8:acad:c::99, utilizando el comando ping. Abrimos el Command Prompt del equipo PC-A y ejecutamos la instrucción C:\>ping 2001:db8:acad:c::99, sin obtener respuesta del host de destino con 4 paquetes enviados y 4 paquetes perdidos. Teniendo en cuenta que la configuración para el protocolo IPv6 se encuentra habilitado y las pruebas con otras interfaces y dispositivos se ejecutaron exitosamente, se deduce que el error que se presenta en la prueba de conectividad es debido al simulador utilizado.

CONCLUSIONES

Se construye la red en el simulador, creando y calculando las subredes utilizando VLSM, lo cual nos permite aprovechar al máximo el espacio de red. Con la anterior metodología de direccionamiento IPv4 se desperdicia demasiado espacio en las redes, ya que solo se usa una máscara de subred y ello impide el crecimiento de la red en grandes empresas. El subneteo aplicando VLSM permite utilizar más de una máscara de subred dentro del mismo grupo de direcciones ip en una red, optimizando el direccionamiento y creando subredes de acuerdo a la cantidad de hosts requeridos.

El comando **ping** es una herramienta para diagnosticar la conectividad de los dispositivos en las redes. Para este trabajo fue de gran ayuda este comando ya que los resultados de las pruebas que realicé, me permitieron hacer la configuración de la puerta de enlace de S1 y del PC-A con el direccionamiento de la interfaz G/0/0/1 del R1 y así tener conexión con todos los dispositivos de las 2 subredes.

Se ponen en práctica algunos de los comandos utilizados para la configuración por consola de los dispositivos de red. Para optimizar la seguridad e impedir el acceso no autorizado a los puertos que no se utilizan, se pueden inhabilitar uno a uno los puertos, pero también se puede inactivar un rango de puertos por medio del comando **interface range**, y con ello estamos cerrando las puertas a usuarios no autorizados que puedan hacer daño en nuestra red.

Para hacer un esquema de direccionamiento con IPv6 en necesario configurar la plantilla SDM, la cual puede habilitarse para permitir algunas funciones según se requiera usar el switch en la red. Para el caso del escenario 2 que se requiere el protocolo IPv6, el comando utilizado para la plantilla es dual-ipv4-and-ipv6 default.

La seguridad en las redes es de vital importancia, es por ello que, para evitar el acceso de usuarios no autorizados a las redes y dispositivos, es recomendable que todos los puertos no utilizados de un switch se inhabiliten utilizando en comando **shutdown.**

Para la creación de un grupo de puertos EtherChannel se hay que tener en cuenta que las características de los puertos individuales deben ser las mismas, es decir se deben seleccionar el mismo tipo de puertos: FastEthernet o Gigabit en ambos dispositivos. Si los puertos en un switch se configuran como enlaces troncales, los

puertos físicos en el otro switch también se deben configurar como enlaces troncales en la misma VLAN.

BIBLIOGRAFIA

Asignación de puertos a las redes VLAN. Institut Sa Palomera – ESO [página web]. Disponible en Internet: <https://www.sapalomera.cat/moodlecf/RS/2/course/module3/3.2.1.3/3.2.1.3.html>

CISCO. Configuración básica de switches y terminales. Introducción a las redes [página web]. (2020). Disponible en Internet: <https://contenthub.netacad.com/itn-dl/2.1.4>

CISCO. Dispositivos finales. Introducción a las redes [página web]. (2020). Disponible en Internet: <https://contenthub.netacad.com/itn-dl/1.2.3>

CISCO. Las redes en la actualidad. Introducción a las redes [página web]. (2020). Disponible en Internet: <https://contenthub.netacad.com/itn-dl/1.3.1>

CISCO. Las redes en la actualidad. Introducción a las redes [página web]. (2020). Disponible en Internet: <https://contenthub.netacad.com/itn-dl/1.4.1>

CISCO. Poniendo las bases de la red. (2006). Disponible en Internet: <https://www.cisco.com/c/dam/global/es_es/assets/acelera/pdf/poniendo-las-bases-de-la-red-enrutamiento-y-conmutacion-sin-problemas.pdf>

COBOS, Antonio. Qué es la Certificación Cisco CCNA y cuáles son sus ventajas. Openwebinars [página web]. (2017). Disponible en Internet: https://openwebinars.net/blog/que-es-la-certificacion-cisco-ccna-y-cuales-son-sus-ventajas/

Configuración de enlaces troncales IEEE 802.1Q. Institut Sa Palomera – ESO [página web]. Disponible en Internet: <https://www.sapalomera.cat/moodlecf/RS/2/course/module3/3.2.2.1/3.2.2.1.html>

Configuración de un servidor de DHCPv4 básico. Institut Sa Palomera – ESO [página web]. Disponible en Internet: <https://www.sapalomera.cat/moodlecf/RS/2/course/module10/10.1.2.1/10.1.2.1.html>

Configuración de una interfaz loopback IPv4 [Anónimo]. Institut Sa Palomera – ESO [página web]. Disponible en Internet:

<https://www.sapalomera.cat/moodlecf/RS/2/course/module4/4.1.3.4/4.1.3.4.html>

Corporación de Estudios Tecnológicos del Norte del Valle [página web]. Disponible en Internet: <https://www.cotecnova.edu.co/index.php/diplomado-en-redes-cisco/#tab-id-3>

ECURED CONTRIBUTORS. Puerta de enlace. Ecured. (2012). Disponible en Internet: https://www.ecured.cu/index.php?title=Puerta_de_enlace&oldid=1491740

Funcionamiento de EtherChannel » CCNA desde Cero. CCNA desde Cero [página web]. Disponible en Internet: <https://ccnadesdecero.es/funcionamiento-etherchannel/#2_EtherChannel>

La importancia del Protocolo IPv6. Grupo iLabora Formación [página web]. Disponible en Internet: <https://ilabora.com/la-importancia-del-protocolo-ipv6/#Motivos_por_los_que_aun_no_se_ha_adoptado_IPv6>

LIMONES, Elena. Redes y Sistemas. Openwebinars [página web]. (2021). Disponible en Internet: <https://openwebinars.net/blog/direccion-ip-que-es-para-que-sirve-y-como-funciona/>

Seguridad de puertos: configuración. Institut Sa Palomera – ESO [página web]. Disponible en Internet: https://www.sapalomera.cat/moodlecf/RS/2/course/module2/2.2.4.5/2.2.4.5.html

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER. Deshabilitar puertos en desuso. Disponible en Internet: <http://giret.ufps.edu.co/cisco/modulos/5.0/m2/course/module2/2.2.4.1/2.2.4.1.html>

ANEXOS

Anexo A

Enlace de descarga para el archivo de simulación del escenario 1:

https://drive.google.com/file/d/1DWo-JFF_3FnL29kXjwCCmRQRHTZY9Q_8/view?usp=share_link

Anexo B

Enlace de descarga para el archivo de simulación del escenario 2:

https://drive.google.com/file/d/165FruA9miegnmLX9-Y8p5e2sIm6So5Et/view?usp=share_link