

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

CRISTHIAN LEONARDO BARONA MORENO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICA, TECNOLOGÍA E INGENIERÍA -ECBTI
INGENIERÍA DE SISTEMAS
PALMIRA
2022

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

CRISTHIAN LEONARDO BARONA MORENO

DIPLOMADO DE OPCION DE GRADO PRESENTADO PARA OPTAR EL
TITULO DE INGENIERO DE SISTEMAS

DIRECTOR
PAULITA FLOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICA, TECNOLOGIA E INGENIERIA -ECBTI
INGENIERÍA DE SISTEMAS
PALMIRA
2022

NOTA DE ACEPTACION

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Palmira 27 noviembre 2022

DEDICATORIA

El presente trabajo se lo dedico primero que todo a Dios que siempre estuvo a mi lado guiándome y dándome la fuerza para continuar y no desistir en este largo proceso educativo, a mis padres que gracias a su esfuerzo y apoyo incondicional que me brindaron tanto en los buenos momentos como en los malos, de este proceso, sin ustedes no hubiera sido posible culminar este camino que arduo y difícil y a todas las personas que estuvieron cerca brindándome su apoyo en todo momento para poder obtener este título.

AGRADECIMIENTOS

Agradezco a mis padres que fueron un apoyo incondicional en esta etapa de mi vida y de mi proceso formativo gracias a ellos y a su cariño me han impulsado siempre a perseguir mis metas y nunca abandonarlas frente a las adversidades, hoy cuando concluyo mis estudios, les dedico a ustedes este logro, como una meta más conquistada.

Gracias a Dios por darme la fuerza y la perseverancia para continuar y no desistir en los momentos difíciles porque esos momentos me enseñaron a un sin fin de respuesta que me ayudaron a crecer como persona y como profesional.

Agradezco también a los tutores gracias a ellos y a sus orientaciones en cada uno de los temas, no hubiera sido posible llegar hasta donde estoy, gracias por su paciencia, por compartir sus conocimientos de manera profesional e invaluable, por su dedicación perseverancia, tolerancia y dedicación gracias a todos aquellos tutores que han hecho parte de mi camino universitario.

Gracias a todos por creer en mí.

TABLA DE CONTENIDO

	Pág.
DEDICATORIA	4
AGRADECIMIENTOS.....	5
LISTA DE TABLAS	8
LISTA DE FIGURAS	9
GLOSARIO	10
RESUMEN.....	11
ABSTRACT.....	11
INTRODUCCION	12
ESCENARIO 1	13
PARTE 1: CONSTRUCCION DE LA RED.....	13
PARTE 2: ESQUEMA DE DIRECCIONAMIENTO IP	13
PARTE 3: CONFIGURE ASPECTOS BÁSICOS.....	16
PASO 1: CONFIGURAR LOS AJUSTES BÁSICOS.....	16
PASO 2. CONFIGURAR LOS EQUIPOS.....	29
PARTE 4: PROBAR Y VERIFICAR LA CONECTIVIDAD DE EXTREMO A EXTREMO	30
ESCENARIO 2.....	38
PARTE 1: INICIALIZAR Y RECARGAR Y CONFIGURAR ASPECTOS BASICOS DE LOS DISPOSITIVOS:.....	39
PASO 1: INICIALIZAR Y VOLVER A CARGAR EL ROUTER Y EL SWITCH	39
PASO 2: CONFIGURAR R1	43
PASO 3: CONFIGURE S1 Y S2.....	51
PARTE 2: CONFIGURACIÓN DE LA INFRAESTRUCTURA DE RED (VLAN, TRUNKING, ETHERCHANNEL).....	60
PASO 4: CONFIGURAR S1.....	60
PARTE 2: CONFIGURAR SOPORTE DE HOST	69
PASO 1: CONFIGURE R1	69
PASO 2: CONFIGURAR LOS SERVIDORES	71
PARTE 3: PROBAR Y VERIFICAR LA CONECTIVIDAD DE EXTREMO A EXTREMO	72

CONCLUSIONES84
REFERENCIAS85
ANEXOS86

LISTA DE TABLAS

Pág.

Tabla 1. Direccionamiento Ip	14
Tabla 2. Direcciones	15
Tabla 3. Configuración Router	16
Tabla 4. Configuración Switch	23
Tabla 5. Configuración PC-A	29
Tabla 6. Configuración PC-B	29
Tabla 7. Prueba de Conectividad.....	30
Tabla 8. Tabla de Vlan.....	38
Tabla 9. Asignación De Direcciones	39
Tabla 10. Configuración Router	43
Tabla 11. Configuración Switch 1 y Switch 2	51
Tabla 12. Configuración Switch 1	61
Tabla 13. Configuración Switch 2	65
Tabla 14. Configuración Router	69
Tabla 15. Configuración PCA.....	71
Tabla 16. Configuración PCB.....	71
Tabla 17. Prueba De Conectividad	72

LISTA DE FIGURAS

Pág.

Figura 1. Construcción de la red	13
Figura 2. Ping desde PCA a router	31
Figura 3. Ping desde PCA a router	32
Figura 4. Ping desde PCA a switch.....	33
Figura 5. Ping desde PCA a PCB	34
Figura 6. Ping desde PCB a router	35
Figura 7. Ping desde PCB a router	36
Figura 8. Ping desde PCB a switch.....	37
Figura 9. Topología.....	38
Figura 10. Ping de PCA a Interface Giga0/0/1.20 del Router	73
Figura 11. Ping de PCA a Interface Giga0/0/1.30 del Router	73
Figura 12. Ping de PCA a Interface Giga0/0/1.40 del Router	74
Figura 13. Ping de PCA a Vlan 40 del Switch 1 con ipv4.....	75
Figura 14. ping de PCA a Vlan 40 del switch 1 con ipv6.....	75
Figura 15. Ping de PCA a Vlan 40 del switch 2 con ipv4	76
Figura 16. Ping de PCA a Vlan 40 del switch 2 con ipv6	77
Figura 17. Ping de PCA a PCB	77
Figura 18. Ping de PCA a Bucle 0 router	78
Figura 19. Ping de PCB a Bucle 0 Router.....	79
Figura 20. Ping de PCB a Interface Giga0/0/1.20 del Router	79
Figura 21. Ping de PCB a Interface Giga0/0/1.30 del Router	80
Figura 22. Ping de PCB a Interface Giga0/0/1.40 del Router	80
Figura 23. Ping de PCB a Vlan 40 del switch 1 con ipv4	81
Figura 24. Ping de PCB a Vlan 40 del switch 1 con ipv6	81
Figura 25. ping de PCB a Vlan 40 del switch 2 con ipv4.....	82
Figura 26. ping de PCB a Vlan 40 del switch 2 con ipv6.....	82

GLOSARIO

Direccionamiento: El direccionamiento permite identificar los distintos dispositivos que se encuentran conectados a un mismo medio compartido¹.

Router: Es el encargado de delimitar cada una de las redes existentes y como llegan los paquetes de una red a otra².

Switch: Se utilizan para conectar varios dispositivos a través de la misma red, puede conectar varias computadoras, impresoras y servidores para crear una red de servicios compartidos dentro de una oficina o edificio.

Enrutamiento: Para que un dispositivo de capa tres pueda determinar la ruta hacia un destino debe tener conocimiento de las diferentes rutas hacia él y cómo hacerlo. El aprendizaje y la determinación de estas rutas se lleva a cabo mediante un proceso de enrutamiento dinámico a través de cálculos y algoritmos que se ejecutan en la red o enrutamiento estático ejecutado manualmente por el administrador o incluso ambos métodos³.

Interfaces: 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 red⁴.

Dirección Ip: Son utilizadas para identificar a un dispositivo en internet o en una red local y que permite el envío de información entre diferentes dispositivos en una red.

¹ CASTAÑO RIBES, Rafael Jesús. Redes locales. Madrid: Macmillan Iberia, S.A. [En línea] (2013). [27 noviembre 2022]. 322 p. Disponible en: <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43257?page=137>.

² CISCO. Las redes en la actualidad. Introducción a las redes. [En línea] (2020). [27 noviembre 2022]. <https://contenthub.netacad.com/itn/1.0.1>

³ ERNESTO, Ariganello. REDES CISCO. Guía de estudio para la certificación CCNA Routing y Switching. España RA-MA 4ª edición actualizada. [En línea] (2016). [27 noviembre 2022]. 561p. Disponible en:

<https://web-s-ebsohost-com.bibliotecavirtual.unad.edu.co/ehost/ebookviewer/ebook/bmxlYmtfXzl0OTgzMjZfX0FO0?sid=d9d99d0e-2b15-46c1-a251-246f19fc1868%40redis&vid=0&format=EB&rid=1>

⁴ Ibid., p. 159

RESUMEN

El presente trabajo abarca los conocimientos adquiridos en este proceso formativo, la exploración de dos escenarios que permitieron aplicar y practicar cada una de las fases del diplomado de cisco networking, donde se logró solucionar varias simulaciones con el propósito de entender cómo funciona es mundo de las redes y los retos que plantea, en cada uno de estos escenarios implementamos el direccionamiento ip, la configuración de los diferentes dispositivos, el enrutamiento de dispositivos, etc. Esto con el fin de conocer como es el proceso de configuración de estos dispositivos y preparándonos para abarcar un caso real.

Palabras clave: Enrutamiento, Vlan, Networking, Redes, Ipv4, Iv6, CCNA, Direccionamiento.

ABSTRACT

The present work covers the knowledge acquired in this training process, the exploration of 2 scenarios that allowed applying and practicing each of the phases of the cisco networking diploma and where it was possible to solve several simulations with the purpose of understanding how the world of networks and the challenges it poses, in each of these scenarios we implement IP addressing, the configuration of the different devices, device routing, etc. This in order to know how is the configuration process of these devices and preparing ourselves to cover a real case.

Keywords: Routing, Vlan, Networking, Networks, Ipv4, Iv6, CCNA, Addressing.

INTRODUCCION

Hoy en día el mundo de las redes ha crecido exponencialmente, las amenazas y las vulnerabilidades pueden generar que se pierda información o que personas no autorizadas puedan acceder fácilmente a estas, es por eso que se hace necesario que los profesionales conozcan de manera clara y precisa los aspectos necesarios para la configuración y la seguridad de los dispositivos ciscos.

El presente trabajo se realizó con el fin de que los profesionales tengan los conceptos claros a la hora de configurar un dispositivo real, es necesario que el profesional tenga en cuenta cómo funciona y se configuran los distintos dispositivos, mediante una serie de pasos que estos realizan de manera clara y que documentan con código, se puede observar cómo se comportan estos cuando están configurados y desconfigurados.

En este primer escenario se realizó la construcción y configuración de una red en donde se realizó la tabla de direccionamiento con su respectiva máscara de red dependiendo de la cantidad de host que cada subred necesitará, se configuraron los dispositivos router y switch utilizando los conceptos vistos en las temáticas de cisco con el fin de mantener los más altos niveles de seguridad en el dispositivo aplicando ipv4, enrutamiento, encriptación de contraseñas mensajes de consola etc. Que garantizan la seguridad y confidencialidad de la información suministrada o transportada.

En el segundo escenario se realizó la construcción de una red con su respectiva configuración aplicando las técnicas de configuración vistas anteriormente en los diferentes dispositivos, como son los router, switches y los pcs, esto con la finalidad de garantizar la seguridad y la integridad de los datos en cada uno de ellos, fue necesario configurar el direccionamiento ipv4 y ipv6 en cada uno de estos dispositivos, se utilizó el enrutamiento DHCP para asignar las direcciones ipv4 de nuestros pcs de manera dinámica, además de configurar nuestras interfaces vlan que nos permitirá dividir nuestra red de manera más estructurada, todo esto realizado desde la línea de comandos y respectivamente documentando el paso a paso de cada proceso.

ESCENARIO 1

PARTE 1: CONSTRUCCION DE LA RED

Figura 1. Construcción de la red



PARTE 2: ESQUEMA DE DIRECCIONAMIENTO IP

De acuerdo a que mi cedula es 1115075508 y mis dos últimos dígitos de mi documento terminan en 08 entonces la dirección Ip quedaría de la siguiente forma 172.08.3.0

Ahora calculamos nuestras subredes.

Dirección Ip que usara.

Ip: 172.08.3.0/24

Para obtener las subredes primero debemos calcularla y para eso realizaremos Subneteo.

Tomamos los bits prestados de la porción de hosts y debemos verificar la cantidad de bit a tomar prestados, para eso aplicamos la siguiente formula

$$2^n - 2 \geq \text{cantidad subredes}$$

En la formula se le resta 2 ya que en cada subred se pierden 2 direcciones una de red y otra de broadcast

Cantidad de subredes: 2

$$\begin{aligned} 2^2 - 2 &\geq 2 \\ 4 - 2 &= 2 \end{aligned}$$

Entonces son 2 la cantidad bits que debemos tomar prestados

128 64 32 16 8 4 2 1
 1 1 0 0 0 0 0 0

Sumamos los resultados de los 2 bits

128+64 = 192

Nuestra Ip y nuestra nueva mascara nos queda así

Ip: 172.08.3.0/26

Máscara: 255.255.255.192 / 26.

Después de haber hallado nuestra nueva Ip y nuestra nueva mascara debemos ahora realizar nuestro esquema y nuestro direccionamiento Ip; lo primero que debemos tener en cuenta son los requisitos de host para cada subred, en nuestro caso se nos pide que la primera subred debe tener mínimo 60 host y para nuestra segunda subred nos piden como requisito que debe tener mínimo 20 host.

A continuación, se muestra la tabla con el direccionamiento Ip dependiendo de la cantidad de host:

Tabla 1. Direccionamiento Ip

			172.08.3.0/24	255.255.255.0			
Requisitos	Nombre Subred	Subred	Inicial	Final	Broadcast	Máscara	Máscara decimal
60	LAN 1	172.08.3.0	172.08.3.1	172.08.3.62	172.08.3.63	26	255.255.255.192
20	LAN 2	172.08.3.64	172.08.3.65	172.08.3.94	172.08.3.95	27	255.255.255.224
		192.168.72.96					

Fuente: Autoría propia

TABLA DE DIRECCIONES

Tabla 2. Direcciones

Ítem	Requerimiento
Dirección de Red	172.08.3.0
Requerimiento de host Subred LAN1	60
Requerimiento de host Subred LAN2	20
R1 G0/0/1	172.08.3.62
R1 G0/0/0	172.08.3.94
S1 SVI	172.08.3.2
PC-A	172.08.3.10
PC-B	172.08.3.75

Fuente: Autoría propia

PARTE 3: CONFIGURE ASPECTOS BÁSICOS

PASO 1: CONFIGURAR LOS AJUSTES BÁSICOS

Tabla 3. Configuración Router

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

Desactivar la búsqueda DNS

Para deshabilitar la búsqueda DNS es necesario utilizar el comando `no ip domain-lookup` que detendrá la búsqueda automática que viene por defecto la configuración del router.

```
Router>enable
```

```
Router#configure terminal
```


Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup

Nombre del router

Utilizamos el comando Hostname con el fin de establecer el nombre que se le dará al dispositivo en nuestro caso es R1 y presionamos intro.

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

Nombre de dominio

Habilitamos el ip dominio lookup y utilizamos el comando ip domain-name para establecer el nombre de dominio en nuestro caso es **ccna-sa.com** para que el usuario pueda acceder a esta sin problema.

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

Contraseña cifrada para el modo EXEC privilegiado

Establecemos una contraseña cifrada para evitar los ingresos que puedan modificar nuestra configuración privilegiada de nuestro dispositivo.

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

Contraseña de acceso a la consola

Establecemos nuestra contraseña para el acceso a la consola para evitar que intrusos no autorizados ingresen a nuestra IOS del dispositivo.

```
R1(config)#line console 0  
R1(config-line)#password ciscoconpass  
R1(config-line)#login  
R1(config-line)#end  
R1#  
%SYS-5-CONFIG_I: Configured from console by console
```

Establecer la longitud mínima para las contraseñas

Establecemos una cantidad mínima de caracteres para nuestra contraseña para si evitar que establezcan contraseñas débiles y fáciles de descifrar y que tienen que ser iguales a 10 o superiores a 10 caracteres.

```
R1#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.
```

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

Crear un usuario administrativo en la base de datos local

Se creo un usuario administrativo en nuestra base de datos local de nuestro dispositivo utilizando el siguiente comando.

```
R1(config)#username admin password admin1pass
R1(config)#line console 0
R1(config-line)#login local
R1(config-line)#exit
```

Configure el inicio de sesión en las líneas VTY para que use la base de datos local

Habilite el inicio de sesión de las líneas VTY (Línea de tiempo virtual) que están habilitadas de 0 15, utilizando el usuario administrativo creado previamente para establecer la sesiones telnet

```
R1(config)#line vty 0 15
R1(config-line)#login local
R1(config-line)#exit
```

Configurar las líneas VTY para que acepten únicamente las conexiones SSH

Para configurar las líneas vty para que acepten las conexiones ssh es necesario generar una llave encriptada esto nos mostrará el nombre de las llaves y el rango que esta soporta luego implementamos en la entrada de transporte ssh y por último lo activamos la conexión para que funcione con nuestro administrador creado previamente.

```
R1(config)#crypto key generate?
  rsa Generate RSA keys
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)#line vty 0 15
*Mar 1 0:7:33.992: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config-line)#transport input ssh
```

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

Cifrar las contraseñas de texto no cifrado

Encriptamos todas las contraseñas configuradas en el dispositivo con el fin de que sean difícil de detectar para los intrusos.

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

Configurar un banner MOTD

Configuramos nuestro mensaje de acceso al dispositivo con el siguiente comando.

```
R1(config)#banner motd #R1 Cristhian Leonardo Barona Moreno Ingeniería de
Sistemas#
```

Configuración de interface G0/0/0

Configuramos nuestras interfaces giga con la dirección Ip asignadas en el cuadro anterior.

```
R1(config)#inteface gi
R1(config)#inteface giga
R1(config)#interface giga
R1(config)#interface gigabitEthernet 0/0/0
R1(config-if)#description Conexion LAN 2
R1(config-if)#ip address 172.08.3.94 255.255.255.224
R1(config-if)#no shutdown
```

```
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
changed state to up
```

Configuración de interface G0/0/1

```
R1(config-if)#exit
R1(config)#interface giga
R1(config)#interface gigabitEthernet 0/0/1
R1(config-if)#description Conexion LAN 1
R1(config-if)#ip address
% Incomplete command.
R1(config-if)#ip address 172.08.3.62 255.255.255.192
```

```
R1(config-if)#no shutdown
```

```
R1(config-if)#
```

```
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1,  
changed state to up
```

Generar una clave de cifrado RSA

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

```
rsa Generate RSA keys
```

```
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]
```

Código completo de la consola

```
Router>enable
```

```
Router#configure terminal
```

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

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

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

```
R1(config)#ip domain lookup
```

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

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

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

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

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

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

```
R1#
```

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

```
R1#configure terminal
```

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

```
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 15
R1(config-line)#login local
R1(config-line)#exit
R1(config)#crypto key generate?
  rsa Generate RSA keys
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)#line vty 0 15
*Mar 1 0:7:33.992: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#do show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
R1(config)#banner motd #R1 Cristhian Leonardo Barona Moreno Ingeniería de
Sistemas#
R1(config)#interface gi
R1(config)#interface giga
R1(config)#interface giga
R1(config)#interface gigabitEthernet 0/0/0
R1(config-if)#description Conexion LAN 2
R1(config-if)#ip address 172.08.3.94 255.255.255.224
R1(config-if)#no shutdown
```

```
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
changed state to up
```

```
R1(config-if)#exit
R1(config)#interface giga
R1(config)#interface gigabitEthernet 0/0/1
R1(config-if)#description Conexion LAN 1
R1(config-if)#ip address
% Incomplete command.
```

```
R1(config-if)#ip address 172.08.3.62 255.255.255.192
R1(config-if)#no shutdown
```

```
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1,
changed state to up
```

```
R1(config-if)#copy running-con
R1(config-if)#copy running-confi
R1(config-if)#copy running-config start
R1(config-if)#exit
R1(config)#copy runnig
R1(config)#copy running
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
R1#copy runni
R1#copy running-config startup-con
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Switch

Tabla 4. Configuración Switch

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

Desactivar la búsqueda DNS

Para deshabilitar la búsqueda DNS es necesario utilizar el comando `no ip domain-lookup` que detendrá la búsqueda automática que viene por defecto la configuración del switch.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
```

Nombre del switch

Utilizamos el comando Hostname con el fin de establecer el nombre que se le dará al dispositivo en nuestro caso es R1 y presionamos intro.

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

Nombre de dominio

Habilitamos el ip dominio lookup y utilizamos el comando ip domain-name para establecer el nombre de dominio en nuestro caso es **ccna-sa.com** para que el usuario pueda acceder a esta sin problema.

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

Contraseña cifrada para el modo EXEC privilegiado

Establecemos una contraseña cifrada para evitar los ingresos que puedan modificar nuestra configuración privilegiada de nuestro dispositivo.

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

Contraseña de acceso a la consola

Establecemos nuestra contraseña para el acceso a la consola para evitar que intrusos no autorizados ingresen a nuestra IOS del dispositivo.

```
S1(config)#line console 0  
S1(config-line)#password ciscoconpass  
S1(config-line)#login  
S1(config-line)#exit
```

Apagar todos los puertos sin usar

Para apagar los puertos sin usar utilizamos el comando interface range ingresando las interfaces que deseamos apagar de nuestro rango.

```
S1(config)#interface range fastEthernet 0/1-4  
S1(config-if-range)#shutdown
```

```
S1(config-if-range)#exit  
S1(config)#interface gig  
S1(config)#interface gigabitEthernet 0/1-2
```

```
^  
% Invalid input detected at '^' marker.
```

Crear un usuario administrativo en la base de datos local

Para crear un usuario administrativo en nuestra base de datos local de nuestro dispositivo utilizamos el siguiente comando.

```
S1(config)#username admin password admin1pass
S1(config)#line console 0
S1(config-line)#login local
S1(config-line)#exit
```

Configure el inicio de sesión en las líneas VTY para que use la base de datos local

Se habilito el inicio de sesión de las líneas VTY (Línea de tiempo virtual) que están habilitadas de 0 15, utilizando el usuario administrativo creado previamente para establecer la sesiones telnet

```
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#exit
```

Configurar las líneas VTY para que acepten únicamente las conexiones SSH

Para configurar las líneas vty para que acepten las conexiones ssh es necesario generar una llave encriptada esto nos mostrara el nombre de las llaves y el rango que esta soporta luego implementamos en la entrada de transporte ssh y por último lo activamos la conexión para que funcione con nuestro administrador creado previamente.

```
S1(config)#crypto key generate ?
  rsa  Generate RSA keys
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)#line vty 0 15
*Mar 1 0:23:49.364: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#exit
```

Cifrar las contraseñas de texto no cifrado

Para encriptar todas las contraseñas utilizamos el comando service password encryption esto con el fin de proporcionar seguridad a nuestro dispositivo y no queden las contraseñas en texto plano.

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

Configurar un banner MOTD

Configuramos nuestro mensaje de acceso al dispositivo con el siguiente comando

```
S1(config)#banner motd #S1 Cristhian Leonardo Barona Moreno Ingeniería de Sistemas#
```

Configure la interfaz de administración (SVI) en VLAN1

```
S1(config)#interfcae vlan 1
      ^
```

```
% Invalid input detected at '^' marker.
```

```
S1(config)#interface vlan 1
S1(config-if)#ip address 172.08.3.2 255.255.255.192
S1(config-if)#no shutdown
```

```
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

```
S1(config-if)#description Conexion Vlan 1
S1(config-if)#exit
S1(config)#copy runnig-config startup-config
      ^
```

```
% Invalid input detected at '^' marker.
```

```
S1(config)#copy running-config startup-config
      ^
```

```
% Invalid input detected at '^' marker.
```

```
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
S1#copy running-config startup-config
```

Destination filename [startup-config]?
Building configuration...
[OK]

Código completo de configuración del Switch

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#ip domain lookup
S1(config)#ip domain-name ccna-sa.com
S1(config)#enable secret ciscoenpass
S1(config)#line console 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit
S1(config)#interface range fastEthernet 0/1-4
S1(config-if-range)#shutdown

S1(config-if-range)#exit
S1(config)#interface gig
S1(config)#interface gigabitEthernet 0/1-2
      ^
% Invalid input detected at '^' marker.

S1(config)#username admin password admin1pass
S1(config)#line console 0
S1(config-line)#login local
S1(config-line)#exit
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#exit
S1(config)#crypto key generate ?
  rsa  Generate RSA keys
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)#line vty 0 15
*Mar 1 0:23:49.364: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd #S1 Cristhian Leonardo Barona Moreno Ingenieria de
Sistemas#
S1(config)#interfcae vlan 1
      ^
% Invalid input detected at '^' marker.

S1(config)#interface vlan 1
S1(config-if)#ip address 172.08.3.2 255.255.255.192
S1(config-if)#no shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#description Conexion Vlan 1
S1(config-if)#exit
S1(config)#copy runnig-config startup-config
      ^
% Invalid input detected at '^' marker.

S1(config)#copy running-config startup-config
      ^
% Invalid input detected at '^' marker.

S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

```

PASO 2. CONFIGURAR LOS EQUIPOS

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

Tabla 5. Configuración PC-A

Configuración de red de PC-A	
Descripción	PC de escritorio con antena para conexión wifi
Dirección física	0060.3E8D.719B
Dirección IPv4	172.8.3.10
Máscara de subred	255.255.255.192
Puerta de enlace IPv4 predeterminada	172.08.3.62

Fuente: Autoría propia

Tabla 6. Configuración PC-B

Configuración de red de PC-B	
Descripción	PC de escritorio con antena para conexión wifi
Dirección física	0001.9636.7568
Dirección IPv4	172.8.3.75
Máscara de subred	255.255.255.224
Puerta de enlace IPv4 predeterminada	172.8.3.94

Fuente: Autoría propia

PARTE 4: PROBAR Y VERIFICAR LA CONECTIVIDAD DE EXTREMO A EXTREMO

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

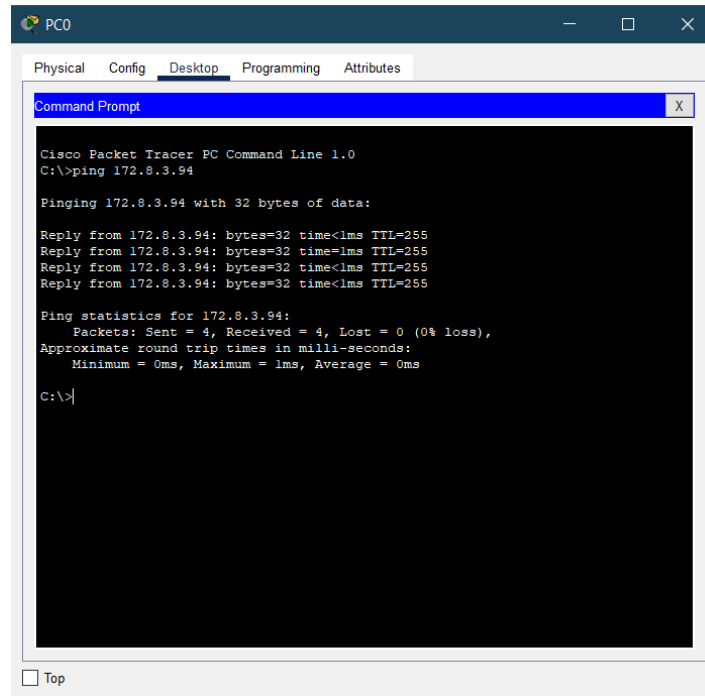
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 7. Prueba de Conectividad

Desde	A	Dirección IP	Resultados de ping
PC-A	R1 G0/0/0	172.8.3.94	Si hay conexión
	R1 G0/0/1	172.8.3.62	Si hay conexión
	S1 VLAN 1	172.8.3.2	Si hay conexión
	PC-B	172.8.3.75	Si hay conexión
PC-B	R1 G0/0/0	172.8.3.94	Si hay conexión
	R1 G0/0/1	172.8.3.62	Si hay conexión
	S1 VLAN 1	172.8.3.2	No hay conexión

Fuente: Autoría propia

Figura 2. Ping desde PCA a router



```
PCO
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.8.3.94

Pinging 172.8.3.94 with 32 bytes of data:

Reply from 172.8.3.94: bytes=32 time<1ms TTL=255
Reply from 172.8.3.94: bytes=32 time<1ms TTL=255
Reply from 172.8.3.94: bytes=32 time<1ms TTL=255
Reply from 172.8.3.94: bytes=32 time<1ms TTL=255

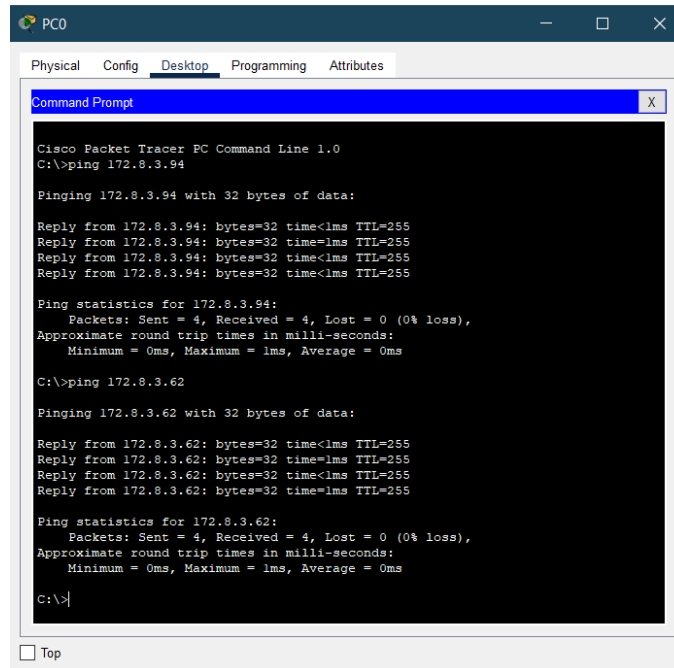
Ping statistics for 172.8.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Fuente: Autoría propia

En la figura 2 podemos evidenciar que hay conectividad desde el PCA hacia el router ya que al hacer ping este nos genera una respuesta positiva al enviar los datos.

Figura 3. Ping desde PCA a router



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.8.3.94

Pinging 172.8.3.94 with 32 bytes of data:

Reply from 172.8.3.94: bytes=32 time<1ms TTL=255
Reply from 172.8.3.94: bytes=32 time<1ms TTL=255
Reply from 172.8.3.94: bytes=32 time<1ms TTL=255
Reply from 172.8.3.94: bytes=32 time<1ms TTL=255

Ping statistics for 172.8.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 172.8.3.62

Pinging 172.8.3.62 with 32 bytes of data:

Reply from 172.8.3.62: bytes=32 time<1ms TTL=255
Reply from 172.8.3.62: bytes=32 time<1ms TTL=255
Reply from 172.8.3.62: bytes=32 time<1ms TTL=255
Reply from 172.8.3.62: bytes=32 time<1ms TTL=255

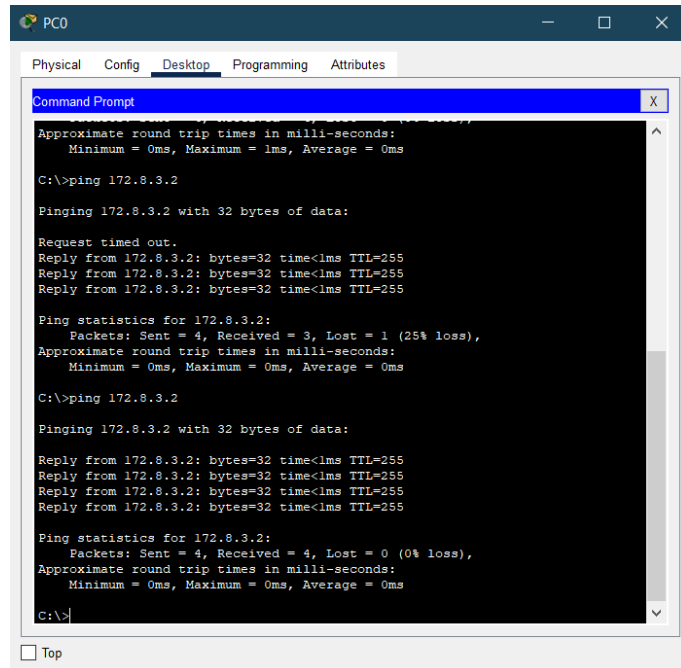
Ping statistics for 172.8.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Fuente1: Autoría propia

En la figura 3 podemos evidenciar que hay conectividad desde el PCA hacia el router por medio de la interface giga0/0/1 ya que al hacer ping este nos genera una respuesta positiva al enviar los datos.

Figura 4. Ping desde PCA a switch

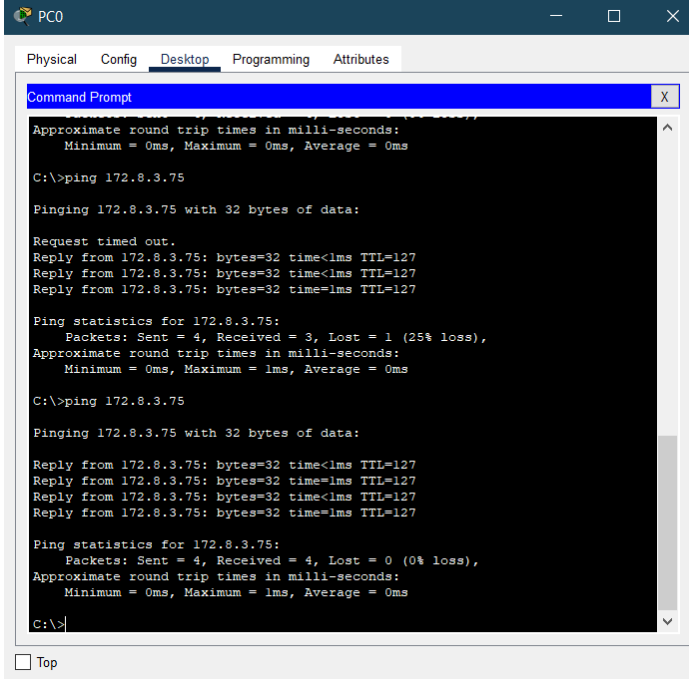


```
PCO
Physical Config Desktop Programming Attributes
Command Prompt
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 172.8.3.2
Pinging 172.8.3.2 with 32 bytes of data:
Request timed out.
Reply from 172.8.3.2: bytes=32 time<1ms TTL=255
Reply from 172.8.3.2: bytes=32 time<1ms TTL=255
Reply from 172.8.3.2: bytes=32 time<1ms TTL=255
Ping statistics for 172.8.3.2:
  Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 172.8.3.2
Pinging 172.8.3.2 with 32 bytes of data:
Reply from 172.8.3.2: bytes=32 time<1ms TTL=255
Reply from 172.8.3.2: bytes=32 time<1ms TTL=255
Reply from 172.8.3.2: bytes=32 time<1ms TTL=255
Reply from 172.8.3.2: bytes=32 time<1ms TTL=255
Ping statistics for 172.8.3.2:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Fuente: Autoría propia

En la figura 4 podemos evidenciar que hay conectividad desde el PCA hacia el switch ya que al hacer ping este nos genera una respuesta positiva al enviar los datos.

Figura 5. Ping desde PCA a PCB



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.8.3.75

Pinging 172.8.3.75 with 32 bytes of data:

Request timed out.
Reply from 172.8.3.75: bytes=32 time<1ms TTL=127
Reply from 172.8.3.75: bytes=32 time<1ms TTL=127
Reply from 172.8.3.75: bytes=32 time<1ms TTL=127

Ping statistics for 172.8.3.75:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
      Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 172.8.3.75

Pinging 172.8.3.75 with 32 bytes of data:

Reply from 172.8.3.75: bytes=32 time<1ms TTL=127
Reply from 172.8.3.75: bytes=32 time<1ms TTL=127
Reply from 172.8.3.75: bytes=32 time<1ms TTL=127
Reply from 172.8.3.75: bytes=32 time<1ms TTL=127

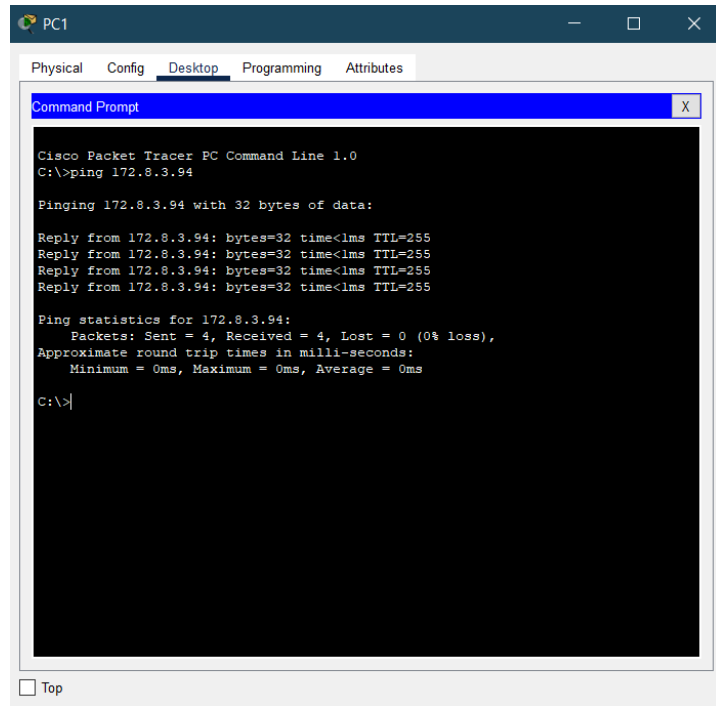
Ping statistics for 172.8.3.75:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
      Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Fuente: Autoría propia

En la figura 5 podemos evidenciar que hay conectividad desde el PCA hacia el PCB ya que al hacer ping este nos genera una respuesta positiva al enviar los datos.

Figura 6. Ping desde PCB a router

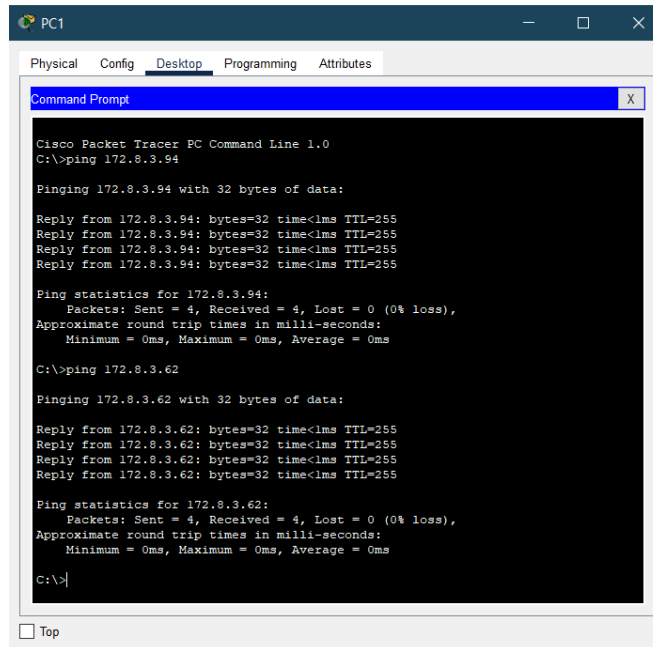


```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.8.3.94
Pinging 172.8.3.94 with 32 bytes of data:
Reply from 172.8.3.94: bytes=32 time<1ms TTL=255
Reply from 172.8.3.94: bytes=32 time<1ms TTL=255
Reply from 172.8.3.94: bytes=32 time<1ms TTL=255
Reply from 172.8.3.94: bytes=32 time<1ms TTL=255
Ping statistics for 172.8.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Fuente: Autoría propia

En la figura 6 podemos evidenciar que hay conectividad desde el PCB hacia el router ya que al hacer ping este nos genera una respuesta positiva al enviar los datos.

Figura 7. Ping desde PCB a router



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.8.3.94

Pinging 172.8.3.94 with 32 bytes of data:

Reply from 172.8.3.94: bytes=32 time<ms TTL=255
Reply from 172.8.3.94: bytes=32 time<ms TTL=255
Reply from 172.8.3.94: bytes=32 time<ms TTL=255
Reply from 172.8.3.94: bytes=32 time<ms TTL=255

Ping statistics for 172.8.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.8.3.62

Pinging 172.8.3.62 with 32 bytes of data:

Reply from 172.8.3.62: bytes=32 time<ms TTL=255
Reply from 172.8.3.62: bytes=32 time<ms TTL=255
Reply from 172.8.3.62: bytes=32 time<ms TTL=255
Reply from 172.8.3.62: bytes=32 time<ms TTL=255

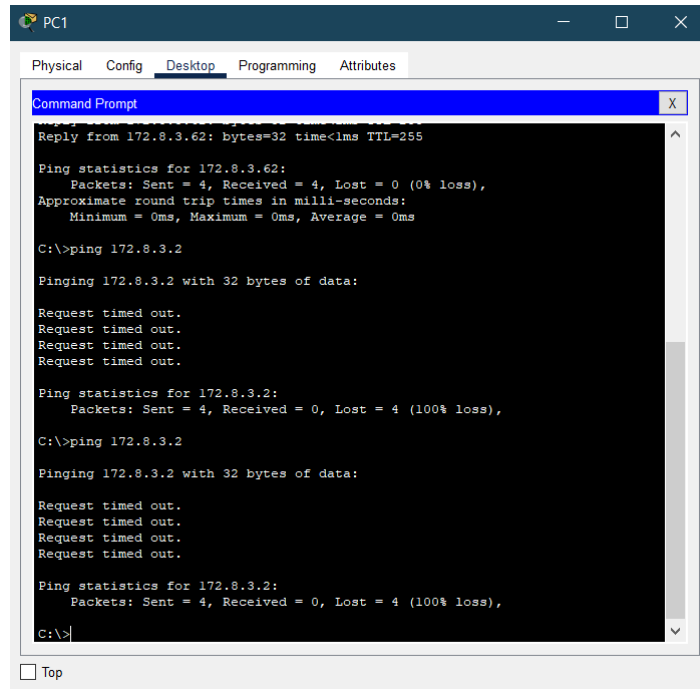
Ping statistics for 172.8.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Autoría propia

En la figura 7 podemos evidenciar que hay conectividad desde el PCB hacia el router por medio de la interface giga0/0/1, ya que al hacer ping este nos genera una respuesta positiva al enviar los datos.

Figura 8. Ping desde PCB a switch



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Replay from 172.8.3.62: bytes=32 time<lms TTL=255
Ping statistics for 172.8.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 172.8.3.2
Pinging 172.8.3.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 172.8.3.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 172.8.3.2
Pinging 172.8.3.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 172.8.3.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

Fuente2: Autoría propia

En la figura 8 podemos evidenciar que hay conectividad desde el PCB hacia el switch ya que al hacer ping este nos genera una respuesta positiva al enviar los datos.

ESCENARIO 2

TOPOLOGIA:

Figura 9. Topología

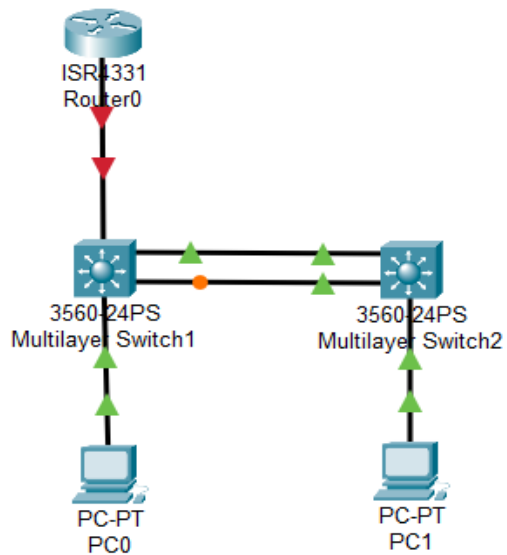


TABLA DE VLAN

Tabla 8. Tabla de Vlan

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

TABLA DE ASIGNACION DE DIRECCIONES:

Tabla 9. Asignación De Direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.20	10.08.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.30	10.08.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.40	10.08.8.97 /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 4	10.08.8.98 /29	10.08.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.08.8.99 /29	10.08.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4 2001:db8:acad:a: :50 /64	DHCP para puerta de enlace predeterminada IPv4 fe80::1
	DHCP para dirección IPv4 2001:db8:acad:b: :50 /64	DHCP para puerta de enlace predeterminada IPv4 fe80::1

Fuente3: Autoría propia

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.

R//

Para eliminar la configuración de inicio de la memoria de acceso aleatorio del router es necesario utilizar el comando erase startup-config y se implementa el comando reload para eliminar la antigua configuración de la memoria es necesario aplicar los siguientes comandos

Router

```
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#reload
Proceed with reload? [confirm]
Initializing Hardware ...
```

Para eliminar la configuración de inicio de la memoria de acceso aleatorio del switch primero verificamos si existen vlan creadas anteriormente con el comando show flash, es necesario utilizar el comando delete vlan.dat para eliminar de la memoria flash las vlans, luego usamos el comando erase startup-config para borrar los archivos de la memoria y se implementa el comando reload para eliminar la antigua configuración de la memoria es necesario aplicar los siguientes comandos.

Switch 1

```
Switch>enable
Switch#show flash

System flash directory:
File Length Name/status
3 8662192 c3560-advipservicesk9-mz.122-37.SE1.bin
2 28282 sigdef-category.xml
1 227537 sigdef-default.xml
[8918011 bytes used, 55098373 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)
```

```
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)
```

```
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
```


[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload
Proceed with reload? [confirm]

Switch 2

Switch>enable
Switch#show flash

System flash directory:
File Length Name/status
3 8662192 c3560-advipservicesk9-mz.122-37.SE1.bin
2 28282 sigdef-category.xml
1 227537 sigdef-default.xml
[8918011 bytes used, 55098373 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)

Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload
Proceed with reload? [confirm]

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

R//

Switch 1

Switch>enable
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 routing
Changes to the running SDM preferences have been stored, but cannot take effect
until the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
Switch(config)#do reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]
```

Switch 2

```
Switch>enable
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 routing
Changes to the running SDM preferences have been stored, but cannot take effect
until the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
Switch(config)#do reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]
```

PASO 2: CONFIGURAR R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 10. Configuración Router

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

Desactivar la búsqueda DNS

Para deshabilitar la búsqueda DNS es necesario utilizar el comando `no ip domain-lookup` que detendrá la búsqueda automática que viene por defecto la configuración del router.

```
Router>enable
```

```
Router#configure terminal
```

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

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

Nombre del router

Utilizamos el comando `Hostname` con el fin de establecer el nombre que se le dará al dispositivo en nuestro caso es R1 y presionamos enter.

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

Nombre de dominio

Habilitamos el `ip domain lookup` y utilizamos el comando `ip domain-name` para establecer el nombre de dominio en nuestro caso es `ccna-sa.com` para que el usuario pueda acceder a esta sin problema.

```
R1(config)#ip domain lookup
```

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

Contraseña cifrada para el modo EXEC privilegiado

Establecemos una contraseña cifrada para evitar los ingresos que puedan modificar nuestra configuración privilegiada de nuestro dispositivo.

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

Contraseña de acceso a la consola

Establecemos nuestra contraseña para el acceso a la consola para evitar que intrusos no autorizados ingresen a nuestra IOS del dispositivo.

```
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

Establecemos una cantidad mínima de caracteres para nuestra contraseña para si evitar que establezcan contraseñas débiles y fáciles de descifrar y que tienen que ser iguales a 5 o superiores a 5 caracteres.

```
R1(config)#security password min-length 5
```

Crear un usuario administrativo en la base de datos local

Se creo un usuario administrativo en nuestra base de datos local de nuestro dispositivo utilizando el siguiente comando.

```
R1(config)#username admin password admin1pass
R1(config)#line console 0
R1(config-line)#login local
R1(config-line)#exit
```

Configure el inicio de sesión en las líneas VTY para que use la base de datos local

Habilite el inicio de sesión de las líneas VTY (Línea de tiempo virtual) que están habilitadas de 0 15, utilizando el usuario administrativo creado previamente para establecer la sesiones telnet

```
R1(config)#line vty 0 15
R1(config-line)#login local
R1(config-line)#exit
```

Configurar las líneas VTY para que acepten únicamente las conexiones SSH

Para configurar las líneas vty para que acepten las conexiones ssh es necesario generar una llave encriptada esto nos mostrara el nombre de las llaves y el rango que esta soporta luego implementamos en la entrada de transporte ssh y por último lo activamos la conexión para que funcione con nuestro administrador creado previamente.

```
R1(config)#crypto key generate?
  rsa Generate RSA keys
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)#line vty 0 15
*Mar 1 0:7:33.992: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
```

Cifrar las contraseñas de texto no cifrado

Encriptamos todas las contraseñas configuradas en el dispositivo con el fin de que sean difícil de detectar para los intrusos.

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

Configurar un banner MOTD

Configuramos nuestro mensaje de acceso al dispositivo con el siguiente comando.

```
R1(config)#banner motd #R1 Cristhian Leonardo Barona Moreno Ingeniería de
Sistemas#
```

Habilitar el routing IPv6

```
R1(config)#ipv6 unicast-routing
```

Configuración de interface G0/0/1

Configuramos nuestras interfaces giga con la direcciones Ipv4 y Ipv6 asignadas en el cuadro anterior.

```
R1(config)#ipv6 unicast-routing
R1(config)#interface giga
R1(config)#interface gigabitEthernet 0/0/1
R1(config-if)#description Conexion router a switch 1
R1(config-if)#interface gi0/0/1.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 10.08.8.1 255.255.255.192
R1(config-subif)#exit
```

```
R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit
```

```
R1(config)#interface gi
R1(config)#interface gigabitEthernet 0/0/1
```

```
R1(config-if)#interface gi0/0/1.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 10.08.8.65 255.255.255.224
```

```
R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
```

```
R1(config)#interface gig
R1(config)#interface gigabitEthernet 0/0/1
R1(config-if)#interface g0/0/1.40
R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#ip address 10.08.8.97 255.255.255.248
R1(config-subif)#exit
```

```
R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit
R1(config)#interface gi
R1(config)#interface gigabitEthernet 0/0/1
R1(config-if)#no shutdown
```

Configure el Loopback0 interface

```
R1(config)#interface loopback 0
```

```
R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
```

```
R1(config-if)#ip address 209.165.201.1 255.255.255.224
R1(config-if)#ipv6 address 2001:db8:acad:209::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shutdown
R1(config-if)#exit
```

Generar una clave de cifrado RSA

```
R1(config)#crypto key generate?
  rsa Generate RSA keys
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]

Código completo

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#ip domain lookup
R1(config)#ip domain-name ccna-sa.com
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#security password min-length 5
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 15
R1(config-line)#login local
R1(config-line)#exit
R1(config)#crypto key generate ?
  rsa  Generate RSA keys
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)#line vty 0 15
*Mar 1 0:7:55.194: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
R1(config)#service password encryption
      ^
% Invalid input detected at '^' marker.
```



```
R1(config)#service password-encryption
R1(config)#banner motd#R1 Cristhian Leonardo Barona Moreno Ingenieria De
Sistemas#
```

^

% Invalid input detected at '^' marker.

```
R1(config)#banner motd #R1 Cristhian Leonardo Barona Moreno Ingenieria De
Sistemas#
```

```
R1(config)#ipv6 unicast-routing
```

```
R1(config)#interface gig
```

```
R1(config)#interface gigabitEthernet 0/0/1
```

```
R1(config-if)#description Conexion router a switch 1
```

```
R1(config-if)#interface giga0/0/1.20
```

```
R1(config-subif)#ip address 10.08.8.1 255.255.255.192
```

% Configuring IP routing on a LAN subinterface is only allowed if that subinterface is already configured as part of an IEEE 802.10, IEEE 802.1Q, or ISL vLAN.

```
R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64
```

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

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

```
R1(config)#interface gi
```

```
R1(config)#interface gigabitEthernet 0/0/1
```

```
R1(config-if)#interface giga0/0/1.30
```

```
R1(config-subif)#ip address 10.08.8.65 255.255.255.224
```

% Configuring IP routing on a LAN subinterface is only allowed if that subinterface is already configured as part of an IEEE 802.10, IEEE 802.1Q, or ISL vLAN.

```
R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64
```

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

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

```
R1(config)#interface gi
```

```
R1(config)#interface gi
```

```
R1(config)#interface gigabitEthernet 0/0/1
```

```
R1(config-if)#interface giga0/0/1.40
```

```
R1(config-subif)#ip address 10.08.8.97 255.255.255.248
```

% Configuring IP routing on a LAN subinterface is only allowed if that subinterface is already configured as part of an IEEE 802.10, IEEE 802.1Q, or ISL vLAN.

```
R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit
R1(config)#interface gi
R1(config)#interface gigabitEthernet 0/0/1
R1(config-if)#no shutdown
```

```
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1,
changed state to up
```

```
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.20, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.20,
changed state to up
```

```
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.30, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.30,
changed state to up
```

```
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.40, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.40,
changed state to up
```

```
R1(config-if)#exit
R1(config)#interface loopback 0
```

```
R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state
to up
```

```
R1(config-if)#ip address 209.165.201.1 255.255.255.224
R1(config-if)#ipv6 address 2001:db8:acad:209::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shutdown
R1(config-if)#exit
```

PASO 3: CONFIGURE S1 Y S2.

Las tareas de configuración incluyen lo siguiente:

Tabla 11. Configuración Switch 1 y Switch 2

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.XY.8.97 para IPv4

Switch 1

Desactivar la búsqueda DNS

Para deshabilitar la búsqueda DNS es necesario utilizar el comando no ip domain-lookup que detendrá la búsqueda automática que viene por defecto la configuración del switch 1.

```
Switch>enable
```

```
Switch#configure terminal
```

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

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

Nombre del switch

Utilizamos el comando Hostname con el fin de establecer el nombre que se le dará al dispositivo en nuestro caso es S1 y presionamos enter.

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

Nombre de dominio

Habilitamos el ip dominio lookup y utilizamos el comando ip domain-name para establecer el nombre de dominio en nuestro caso es ccna-sa.com para que el usuario pueda acceder a esta sin problema.

```
S1(config)#ip domain lookup
```

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

Contraseña cifrada para el modo EXEC privilegiado

Establecemos una contraseña cifrada para evitar los ingresos que puedan modificar nuestra configuración privilegiada de nuestro dispositivo.

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

Contraseña de acceso a la consola

Establecemos nuestra contraseña para el acceso a la consola para evitar que intrusos no autorizados ingresen a nuestra IOS del dispositivo.

```
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 de datos local

Se creo un usuario administrativo en nuestra base de datos local de nuestro dispositivo utilizando el siguiente comando.

```
S1(config)#username admin password admin1pass
S1(config)#line console 0
S1(config-line)#login local
S1(config-line)#exit
```

Configure el inicio de sesión en las líneas VTY para que use la base de datos local

Habilite el inicio de sesión de las líneas VTY (Línea de tiempo virtual) que están habilitadas de 0 15, utilizando el usuario administrativo creado previamente para establecer la sesiones telnet

```
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#exit
```

Configurar las líneas VTY para que acepten únicamente las conexiones SSH

Para configurar las líneas vty para que acepten las conexiones ssh es necesario generar una llave encriptada esto nos mostrara el nombre de las llaves y el rango que esta soporta luego implementamos en la entrada de transporte ssh y por último lo activamos la conexión para que funcione con nuestro administrador creado previamente.

```
S1(config)#crypto key generate?
  rsa Generate RSA keys
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)#line vty 0 15
*Mar 1 0:7:33.992: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#exit
```

Cifrar las contraseñas de texto no cifrado

Encriptamos todas las contraseñas configuradas en el dispositivo con el fin de que sean difícil de detectar para los intrusos.

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

Configurar un banner MOTD

Configuramos nuestro mensaje de acceso al dispositivo con el siguiente comando.

```
S1(config)#banner motd #S1 Cristhian Leonardo Barona Moreno Ingeniería de Sistemas#
```

Generar una clave de cifrado RSA

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

```
rsa Generate RSA keys
```

```
S1(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]
```

Configurar la interfaz de administración (SVI)

Configuramos nuestra interface de administración para generar la comunicación entre los dos switches.

```
S1(config)#ipv6 unicast-routing
```

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

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

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

```
S1(config-if)#
```

```
%LINK-5-CHANGED: Interface Vlan40, changed state to up
```

```
S1(config-if)#ip address 10.08.8.98 255.255.255.248
```

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

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

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

```
S1(config)#ip default-gateway 10.08.8.97
```

```
S1(config)#
```

Código completo

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#ip domain lookup
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)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#enable
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#username admin password admin1pass
S1(config)#line console 0
S1(config-line)#login local
S1(config-line)#exit
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#exit
S1(config)#crypto key generate ?
  rsa  Generate RSA keys
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)#line vty 0 15
*Mar 1 0:9:7.27: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd #S1 Cristhian Leonardo Barona Moreno Ingenieria De
Sistemas#
```

```
S1(config)#ipv6 unicast-routing
S1(config)#vlan 40
S1(config-vlan)#exit
S1(config)#interface vlan 40
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan40, changed state to up
```

```
S1(config-if)#ip address 10.08.8.98 255.255.255.248
S1(config-if)#ipv6 address 2001:db8:acad:c::98/64
S1(config-if)#ipv6 address fe80::98 link-local
S1(config-if)#exit
S1(config)#ip default-gateway 10.08.8.97
S1(config)#
```

Switch 2

Desactivar la búsqueda DNS

Para deshabilitar la búsqueda DNS es necesario utilizar el comando `no ip domain-lookup` que detendrá la búsqueda automática que viene por defecto la configuración del router.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
```

Nombre del switch

Utilizamos el comando `Hostname` con el fin de establecer el nombre que se le dará al dispositivo en nuestro caso es S2 y presionamos enter.

```
Switch(config)#hostname S2
```

Nombre de dominio

Habilitamos el ip dominio lookup y utilizamos el comando `ip domain-name` para establecer el nombre de dominio en nuestro caso es `ccna-sa.com` para que el usuario pueda acceder a esta sin problema.

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

Contraseña cifrada para el modo EXEC privilegiado

Establecemos una contraseña cifrada para evitar los ingresos que puedan modificar nuestra configuración privilegiada de nuestro dispositivo.

```
S2(config)#enable secret class
```

Contraseña de acceso a la consola

Establecemos nuestra contraseña para el acceso a la consola para evitar que intrusos no autorizados ingresen a nuestra IOS del dispositivo.

```
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 de datos local

Se creo un usuario administrativo en nuestra base de datos local de nuestro dispositivo utilizando el siguiente comando.

```
S2(config)#username admin password admin1pass
S2(config)#line console 0
S2(config-line)#login local
S2(config-line)#exit
```

Configure el inicio de sesión en las líneas VTY para que use la base de datos local

Habilite el inicio de sesión de las líneas VTY (Línea de tiempo virtual) que están habilitadas de 0 15, utilizando el usuario administrativo creado previamente para establecer la sesiones telnet

```
S2(config)#line vty 0 15
S2(config-line)#login local
S2(config-line)#exit
```

Configurar las líneas VTY para que acepten únicamente las conexiones SSH

Para configurar las líneas vty para que acepten las conexiones ssh es necesario generar una llave encriptada esto nos mostrara el nombre de las llaves y el rango que esta soporta luego implementamos en la entrada de transporte ssh y por último lo activamos la conexión para que funcione con nuestro administrador creado previamente.

```
S2(config)#crypto key generate?
```

```
rsa Generate RSA keys
S2(config)#crypto key generate rsa
The name for the keys will be: S2.ccna-sa.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.
```

```
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

```
S2(config)#line vty 0 15
*Mar 1 0:7:33.992: %SSH-5-ENABLED: SSH 1.99 has been enabled
S2(config-line)#transport input ssh
S2(config-line)#login local
S2(config-line)#exit
```

Cifrar las contraseñas de texto no cifrado

Encriptamos todas las contraseñas configuradas en el dispositivo con el fin de que sean difícil de detectar para los intrusos.

```
S2(config)#service password-encryption
```

Configurar un banner MOTD

Configuramos nuestro mensaje de acceso al dispositivo con el siguiente comando.

```
S2(config)#banner motd #S2 Cristhian Leonardo Barona Moreno Ingeniería de
Sistemas#
```

Generar una clave de cifrado RSA

```
S2(config)#crypto key generate?
  rsa Generate RSA keys
S2(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]
```

Configurar la interfaz de administración (SVI)

```
S2(config)#ipv6 unicast-routing
```

```
S2(config)#vlan 40
S2(config-vlan)#exit
S2(config)#interface vlan 40
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan40, changed state to up
```

```
S2(config-if)#ip address 10.08.8.99 255.255.255.248
S2(config-if)#ipv6 address 2001:db8:acad:c::99/64
S2(config-if)#ipv6 address fe80::99 link-local
S2(config-if)#exit
S2(config)#ip default-gateway 10.08.8.97
S2(config)#
```

Codigo completo

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S2
S2(config)#ip domain lookup
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 console 0
S2(config-line)#login local
S2(config-line)#exit
S2(config)#line vty 0 15
S2(config-line)#login local
S2(config-line)#exit
S2(config)#crypto key generate ?
  rsa  Generate RSA keys
S2(config)#crypto key generate rsa
The name for the keys will be: S2.ccna-sa.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

```
S2(config)#line vty 0 15
*Mar 1 1:13:3.352: %SSH-5-ENABLED: SSH 1.99 has been enabled
S2(config-line)#transport input ssh
S2(config-line)#login local
S2(config-line)#exit
S2(config)#service password-encryption
S2(config)#banner motd #S1 Cristhian Leonardo Barona Moreno Ingenieria De
Sistemas#
S2(config)#ipv6 unicast-routing
S2(config)#vlan 4
S2(config-vlan)#exit
S2(config)#interface vlan 4
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan4, changed state to up

S2(config-if)#ip address 10.08.8.99 255.255.255.248
S2(config-if)#ipv6 address 2001:db8:acad:c::99/64
S2(config-if)#ipv6 address fe80::99 link-local
S2(config-if)#exit
S2(config)#ip default-gateway 10.19.8.97
S2(config)#
```

PARTE 2: CONFIGURACIÓN DE LA INFRAESTRUCTURA DE RED (VLAN, TRUNKING, ETHERCHANNEL)

PASO 4: CONFIGURAR S1

La configuración del S1 incluye las siguientes tareas:

Tabla 12. Configuración Switch 1

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

Crear VLAN

Para crear las vlans de nuestro switch utilizamos el comando vlan más el número que se desea asignar (vlan 1) luego procedemos a nombrar nuestra vlan con el comando name mas el nombre que se le va a dar (name ejemplo).

S1 Cristhian Leonardo Barona Moreno Ingenieria De Sistemas

User Access Verification

Username: admin

Password:

S1>enable

Password:

Password:

S1#configure terminal

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

S1(config)#vlan 20

S1(config-vlan)#name Docentes

S1(config-vlan)#

S1(config-vlan)#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)#

```

```
S1#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
4 VLAN0004	active	
20 Docentes	active	
30 Estudiantes	active	
40 Invitados	active	
50 Usuarios	active	
56 Native	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Crear troncos 802.1Q que utilicen la VLAN 56 nativa

Creamos nuestros troncos y los encapsulamos con los siguientes comandos.

```

S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface f0/1
S1(config-if)#switchport trunk encapsulation ?
  dot1q Interface uses only 802.1q trunking encapsulation when trunking
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 56

```

```
S1(config-if)#exit
S1(config)#interface f0/2
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 56
S1(config-if)#exit
S1(config)#interface f0/5
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 56
S1(config-if)#exit
S1(config)#
```

Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2

```
S1(config)#interface range f0/1 - 2
S1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1
S1(config-if-range)#no shutdown
S1(config-if-range)#exit
S1(config-if)#exit
S1(config)#interface port-channel 1
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk allowed vlan 20,30,40,50,56
S1(config-if)#exit
S1(config)#
```

Configurar el puerto de acceso de host para VLAN 20

```
S1(config)#interface f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan
S1(config-if)#switchport access vlan 20
S1(config-if)#exit
S1(config)#
```

Configurar la seguridad del puerto en los puertos de acceso

```
S1(config)#interface f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security maximum 4
S1(config-if)#switchport port-security violation shutdown
```

```
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#exit
```

Proteja todas las interfaces no utilizadas

```
S1(config)#interface range g0/1-2
S1(config-if-range)#description interface vlan 50
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 50
S1(config-if-range)#
S1(config-if-range)#switchport port-security violation shutdown
S1(config-if-range)#exit
S1(config)#interface range f0/3-4
S1(config-if-range)#description interface vlan 50
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 50
S1(config-if-range)#switchport port-security violation shutdown
S1(config-if-range)#exit
S1(config)#interface range f0/7-24
S1(config-if-range)#description interface vlan 50
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 50
S1(config-if-range)#switchport port-security violation shutdown
S1(config-if-range)#exit
```


Paso 5: Configure el S2.

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

Tabla 13. Configuración Switch 2

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

Crear VLAN

Para crear las vlans de nuestro switch utilizamos el comando vlan más el número que se desea asignar (vlan 1) luego procedemos a nombrar nuestra vlan con el comando name mas el nombre que se le va a dar (name ejemplo).

S1 Cristhian Leonardo Barona Moreno Ingenieria De Sistemas

User Access Verification

Username: admin

Password:

S2>enable

Password:

S2#configure terminal

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

S2(config)#vlan 20

S2(config-vlan)#name Docentes

S2(config-vlan)#vlan 30

S2(config-vlan)#name Estudiantes

S2(config-vlan)#vlan 40

```

S2(config-vlan)#name Invitados
S2(config-vlan)#vlan 50
S2(config-vlan)#name Usuarios
S2(config-vlan)#vlan 56
S2(config-vlan)#name Native
S2(config-vlan)#exit
S2(config)#

```

```
S2#show vlan brief
```

```

VLAN Name                Status  Ports
-----
1  default                  active  Fa0/3, Fa0/4, Fa0/5, Fa0/6
                               Fa0/7, Fa0/8, Fa0/9, Fa0/10
                               Fa0/11, Fa0/12, Fa0/13, Fa0/14
                               Fa0/15, Fa0/16, Fa0/17, Fa0/18
                               Fa0/19, Fa0/20, Fa0/21, Fa0/22
                               Fa0/23, Fa0/24, Gig0/1, Gig0/2
4  VLAN0004                 active
20 Docentes                 active
30 Estudiantes             active
40 Invitados               active
50 Usuarios                 active
56 Native                  active
1002 fddi-default          active
1003 token-ring-default    active
1004 fddinet-default       active
1005 trnet-default         active
S2#

```

Crear troncos 802.1Q que utilicen la VLAN 6 nativa

```

S2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface f0/1
S2(config-if)#switchport trunk encapsulation ?
dot1q Interface uses only 802.1q trunking encapsulation when trunking
S2(config-if)#switchport trunk encapsulation dot1q
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 56
S2(config-if)#exit
S2(config)#interface f0/2
S2(config-if)#switchport trunk encapsulation dot1q
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 56

```

```
S2(config-if)#exit
```

Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2

```
S2(config)#interface range f0/1-2
S2(config-if-range)#channel-group 1 mode active
S2(config-if-range)#
Creating a port-channel interface Port-channel 1
S2(config-if-range)#no shutdown
S2(config-if-range)#exit
S2(config)#interface port-channel 1
S2(config-if)#switchport trunk encapsulation dot1q
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk allowed vlan 20,30,40,50,56
S2(config-if)#exit
S2(config)#
```

Configurar el puerto de acceso del host para la VLAN 3

```
S2#configure terminal
```

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

```
S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 30
S2(config-if)#exit
S2(config)#
```

Configure port-security en los access ports

```
S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport port-security maximum 4
S2(config-if)#switchport port-security violation shutdown
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#exit
```

S2(config)#

Asegure todas las interfaces no utilizadas.

S2(config)#interface range g0/1-2, f0/3-4, f0/7-17, f0/19-24

S2(config)#interface range g0/1-2

S2(config-if-range)#description interface vlan 50

S2(config-if-range)#switchport mode access

S2(config-if-range)#switchport access vlan 50

S2(config-if-range)#switchport port-security violation shutdown

S2(config-if-range)#exit

S2(config)#interface range f0/3-4

S2(config-if-range)#description interface vlan 50

S2(config-if-range)#switchport mode access

S2(config-if-range)#switchport access vlan 50

S2(config-if-range)#switchport port-security violation shutdown

S2(config-if-range)#exit

S2(config)#interface range f0/7-17

S2(config-if-range)#description interface vlan 50

S2(config-if-range)#switchport mode access

S2(config-if-range)#switchport access vlan 50

S2(config-if-range)#switchport port-security violation shutdown

S2(config-if-range)#exit

S2(config)#interface range f0/19-24

S2(config-if-range)#description interface vlan 50

S2(config-if-range)#switchport mode access

S2(config-if-range)#switchport access vlan 50

S2(config-if-range)#switchport port-security violation shutdown

```

S2(config-if-range)#exit
S2(config)#interface range f0/5-6
S2(config-if-range)#description interface vlan 50
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 50
S2(config-if-range)#switchport port-security violation shutdown
S2(config-if-range)#exit

```

PARTE 2: CONFIGURAR SOPORTE DE HOST

PASO 1: CONFIGURE R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 14. Configuración Router

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

Configure Default Routing

Username: admin

Password:

R1>enable

Password:

R1#configure terminal

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

R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0

%Default route without gateway, if not a point-to-point interface, may impact performance

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

Configurar IPv4 DHCP para VLAN 20

R1(config)#service dhcp

R1(config)#ip dhcp pool Dhcpvlan20

R1(dhcp-config)#network 10.08.8.0 255.255.255.192

R1(dhcp-config)#ip dhcp excluded-address 10.08.8.1 10.08.8.52

R1(config)#ip dhcp pool Dhcpvlan20

R1(dhcp-config)#default-router 10.08.8.1

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

R1(dhcp-config)#exit

Configurar DHCP IPv4 para VLAN 30

R1(config)#service dhcp

R1(config)#ip dhcp pool Dhcpvlan30

R1(dhcp-config)#network 10.08.8.64 255.255.255.224

R1(dhcp-config)#ip dhcp excluded-address 10.08.8.65 10.08.8.84

R1(config)#ip dhcp pool Dhcpvlan30

R1(dhcp-config)#default-router 10.08.8.65

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 15. Configuración PCA

Configuración de red de PC-A	
Descripción.	unad-ccna-sa.net
Dirección física.	0002.4A38.653D
Dirección IP	10.8.8.53 2001:DB8:ACAD:A::50
Mascara de subred	255.255.255.192
Gateway predeterminado	10.8.8.1
Gateway predeterminado ipv6	2001:DB8:ACAD:A::1

Fuente: Autoría propia

Tabla 16. Configuración PCB

Configuración de red de PC-B	
Descripción.	unad-ccna-sb.net
Dirección física.	0003.E4E9.6B9A
Dirección IP	10.8.8.85 2001:DB8:ACAD:B::50
Mascara de subred	255.255.255.224
Gateway predeterminado	10.8.8.65
Gateway predeterminado ipv6	2001:DB8:ACAD:B::1

Fuente: Autoría propia

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.

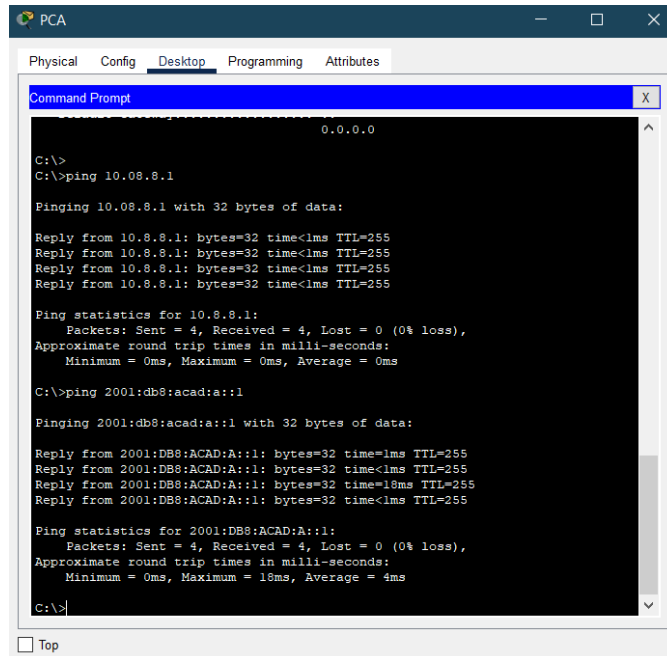
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 17. Prueba De Conectividad

Desde	A	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.20	IPv4	Hay conexión
		IPv6	Hay conexión
	R1, G0/0/1.30	IPv4	Hay conexión
		IPv6	Hay conexión
	R1, G0/0/1.40	IPv4	Hay conexión
		IPv6	Hay conexión
	S1, VLAN 4	IPv4	Hay conexión
		IPv6	No hay conexión
	S2, VLAN 4	IPv4	Hay conexión
		IPv6	No hay conexión
	PC-B	IPv4	Hay conexión
		IPv6	Hay conexión
R1 Bucle 0	IPv4	Hay conexión	
	IPv6	Hay conexión	
PC-B	R1 Bucle 0	IPv4	Hay conexión
		IPv6	Hay conexión
	R1, G0/0/1.20	IPv4	Hay conexión
		IPv6	Hay conexión
	R1, G0/0/1.30	IPv4	Hay conexión
		IPv6	Hay conexión
	R1, G0/0/1.40	IPv4	Hay conexión
		IPv6	Hay conexión
	S1, VLAN 4	IPv4	Hay conexión
		IPv6	No hay conexión
	S2, VLAN 4	IPv4	Hay conexión
		IPv6	No hay conexión

Fuente: Autoría propia

Figura 10. Ping de PCA a Interface Giga0/0/1.20 del Router

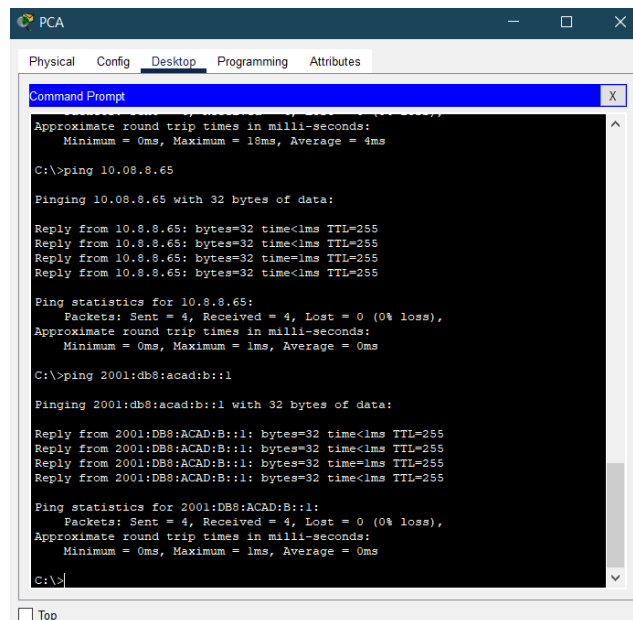


```
PCA
Physical Config Desktop Programming Attributes
Command Prompt
0.0.0.0
C:\>
C:\>ping 10.08.8.1
Pinging 10.08.8.1 with 32 bytes of data:
Reply from 10.08.8.1: bytes=32 time<1ms TTL=255
Reply from 10.08.8.1: bytes=32 time<1ms TTL=255
Reply from 10.08.8.1: bytes=32 time<1ms TTL=255
Reply from 10.08.8.1: bytes=32 time<1ms TTL=255
Ping statistics for 10.08.8.1:
    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=18ms 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 = 18ms, Average = 4ms
C:\>
```

Fuente: Autoría propia

En la figura 10 podemos evidenciar que hay conectividad desde el PCA hacia el router con interface giga0/0/1.20 tanto en ipv4 como en ipv6, ya que al hacer ping este nos genera una respuesta positiva al enviar los datos.

Figura 11. Ping de PCA a Interface Giga0/0/1.30 del Router

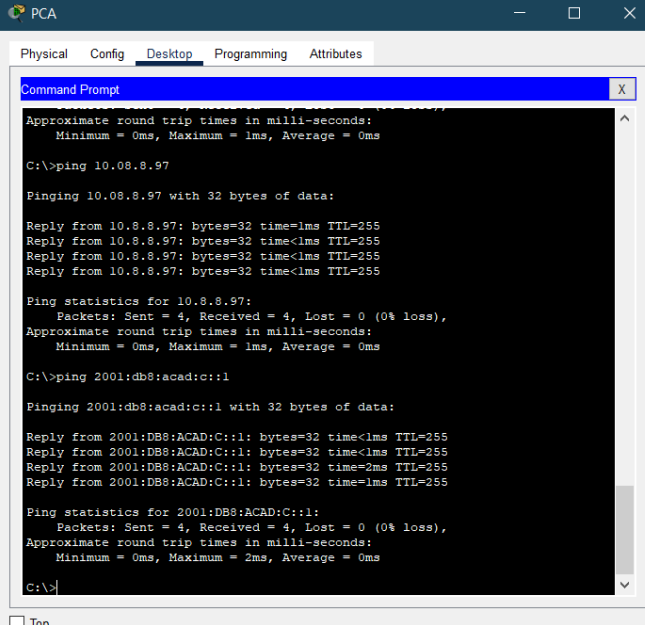


```
PCA
Physical Config Desktop Programming Attributes
Command Prompt
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 18ms, Average = 4ms
C:\>ping 10.08.8.65
Pinging 10.08.8.65 with 32 bytes of data:
Reply from 10.08.8.65: bytes=32 time<1ms TTL=255
Reply from 10.08.8.65: bytes=32 time<1ms TTL=255
Reply from 10.08.8.65: bytes=32 time=1ms TTL=255
Reply from 10.08.8.65: bytes=32 time<1ms TTL=255
Ping statistics for 10.08.8.65:
    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
Ping statistics for 2001:DB8:ACAD:B::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
```

Fuente: Autoría propia

En la figura 11 podemos evidenciar que hay conectividad desde el PCA hacia el router con interface giga0/0/1.30 tanto en ipv4 como en ipv6, ya que al hacer ping este nos genera una respuesta positiva al enviar los datos.

Figura 12. Ping de PCA a Interface Giga0/0/1.40 del Router



```
PCA
Physical Config Desktop Programming Attributes
Command Prompt
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 10.08.8.97
Finging 10.08.8.97 with 32 bytes of data:

Reply from 10.08.8.97: bytes=32 time<1ms TTL=255
Reply from 10.08.8.97: bytes=32 time<1ms TTL=255
Reply from 10.08.8.97: bytes=32 time<1ms TTL=255
Reply from 10.08.8.97: bytes=32 time<1ms TTL=255

Ping statistics for 10.08.8.97:
    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
Finging 2001:db8:acad:c::1 with 32 bytes of data:

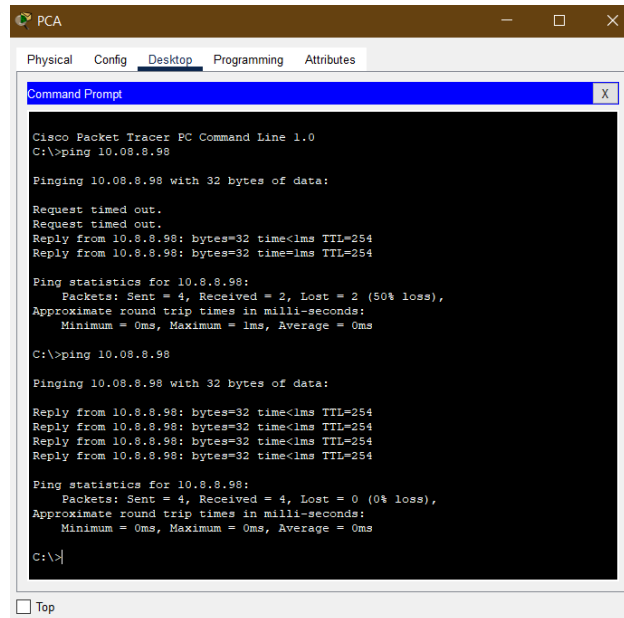
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time=2ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time=1ms TTL=255

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 = 2ms, Average = 0ms
C:\>
```

Fuente: Autoría propia

En la figura 12 podemos evidenciar que hay conectividad desde el PCA hacia el router con interface giga0/0/1.40 tanto en ipv4 como en ipv6, ya que al hacer ping este nos genera una respuesta positiva al enviar los datos.

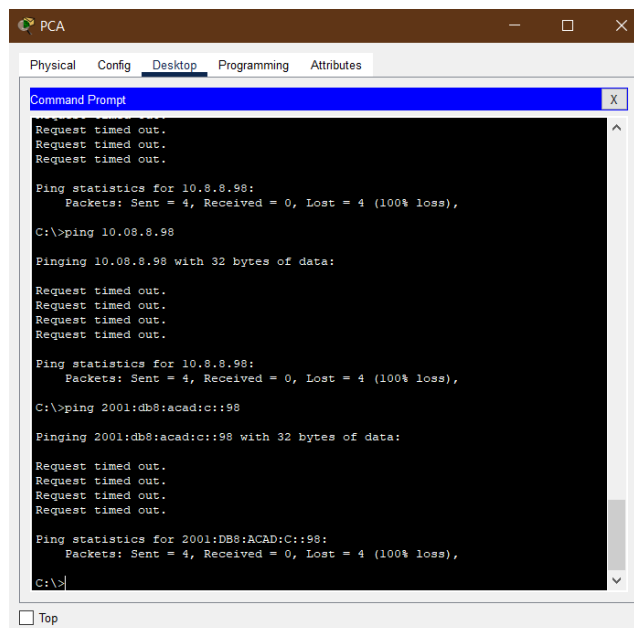
Figura 13. Ping de PCA a Vlan 40 del Switch 1 con ipv4



Fuente: autoría propia

En la figura 13 podemos evidenciar que hay conectividad desde el PCA hacia la vlan 40 del switch 1 en ipv4, ya que al hacer ping este nos genera una respuesta positiva al enviar los datos.

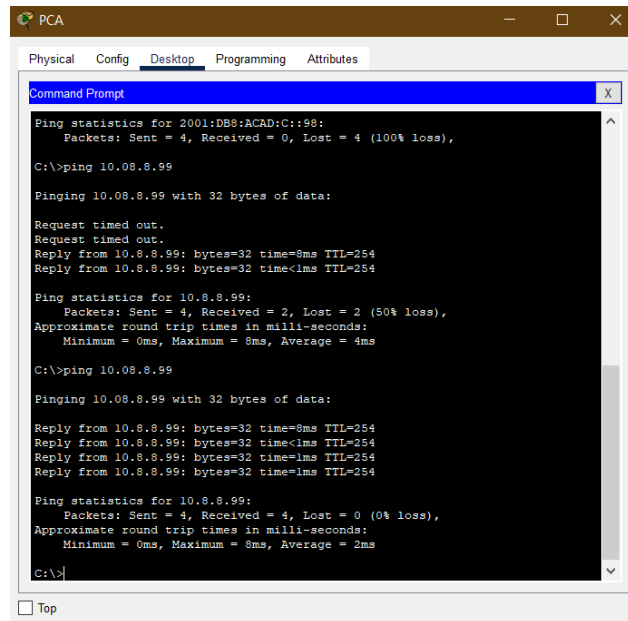
Figura 14. ping de PCA a Vlan 40 del switch 1 con ipv6



Fuente: Autoría propia

En la figura 14 podemos evidenciar que no hay conectividad desde el PCA hacia la vlan 40 del switch 1 en ipv6, ya que al hacer ping este nos genera una pérdida total de los datos.

Figura 15. Ping de PCA a Vlan 40 del switch 2 con ipv4



```
PCA
Physical Config Desktop Programming Attributes
Command Prompt
Ping statistics for 2001:DB8:ACAD:C::98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.08.0.99

Pinging 10.08.0.99 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.08.0.99: bytes=32 time=8ms TTL=254
Reply from 10.08.0.99: bytes=32 time<1ms TTL=254

Ping statistics for 10.08.0.99:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 4ms

C:\>ping 10.08.0.99

Pinging 10.08.0.99 with 32 bytes of data:

Reply from 10.08.0.99: bytes=32 time=8ms TTL=254
Reply from 10.08.0.99: bytes=32 time<1ms TTL=254
Reply from 10.08.0.99: bytes=32 time=1ms TTL=254

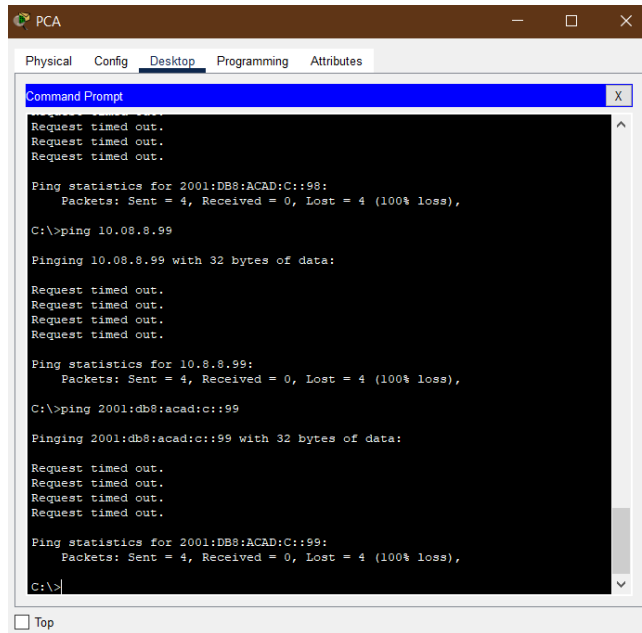
Ping statistics for 10.08.0.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms

C:\>
```

Fuente: Autoría propia

En la figura 15 podemos evidenciar que hay conectividad desde el PCA hacia la vlan 40 del switch 2 en ipv4, ya que al hacer ping este nos genera una respuesta positiva al enviar los datos.

Figura 16. Ping de PCA a Vlan 40 del switch 2 con ipv6



```
PCA
Physical Config Desktop Programming Attributes
Command Prompt
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 10.08.8.99

Pinging 10.08.8.99 with 32 bytes of data:

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

Ping statistics for 10.08.8.99:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

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.

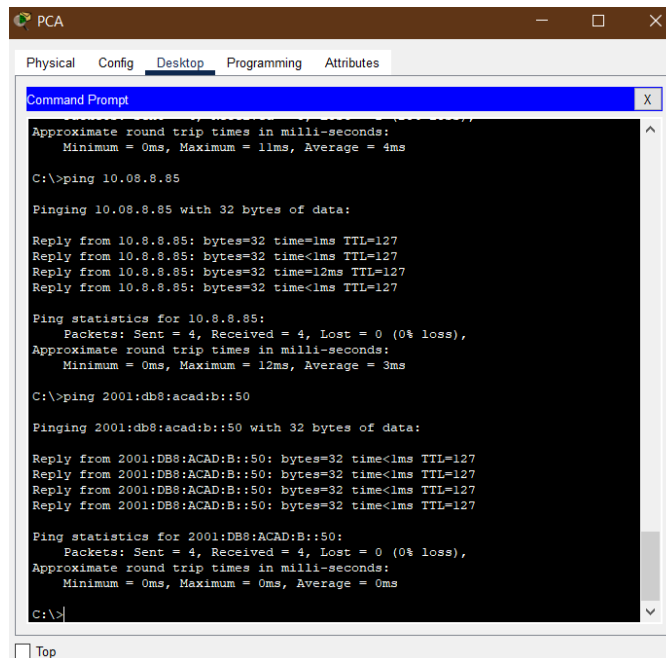
Ping statistics for 2001:DB8:ACAD:C:99:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Fuente: Autoría propia

En la figura 16 podemos evidenciar que no hay conectividad desde el PCA hacia la vlan 40 del switch 2 en ipv6, ya que al hacer ping este nos genera una perdida de los datos.

Figura 17. Ping de PCA a PCB



```
PCA
Physical Config Desktop Programming Attributes
Command Prompt
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 4ms

C:\>ping 10.08.8.85

Pinging 10.08.8.85 with 32 bytes of data:

Reply from 10.08.8.85: bytes=32 time=1ms TTL=127
Reply from 10.08.8.85: bytes=32 time<1ms TTL=127
Reply from 10.08.8.85: bytes=32 time=12ms TTL=127
Reply from 10.08.8.85: bytes=32 time<1ms TTL=127

Ping statistics for 10.08.8.85:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 3ms

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

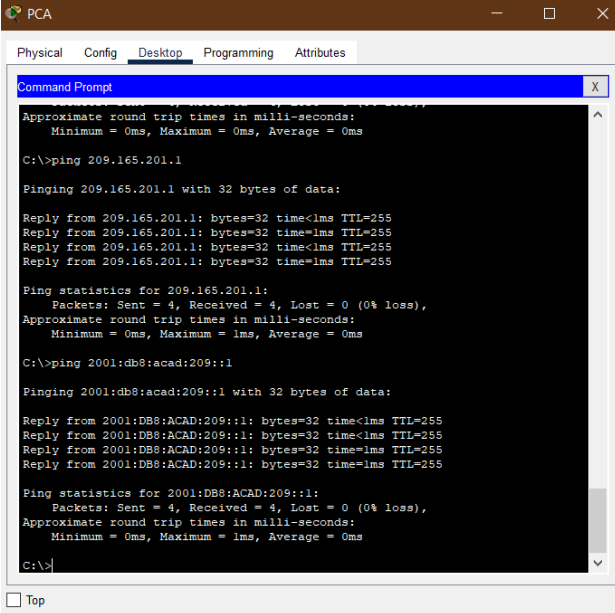
Ping statistics for 2001:DB8:ACAD:B::50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente4: Autoría propia

En la figura 17 podemos evidenciar que hay conectividad desde el PCA hacia el PCB tanto en ipv4 como en ipv6, ya que al hacer ping este nos genera una respuesta positiva al enviar los datos.

Figura 18. Ping de PCA a Bucle 0 router



```
PCA
Physical Config Desktop Programming Attributes
Command Prompt
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 = 1ms, 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

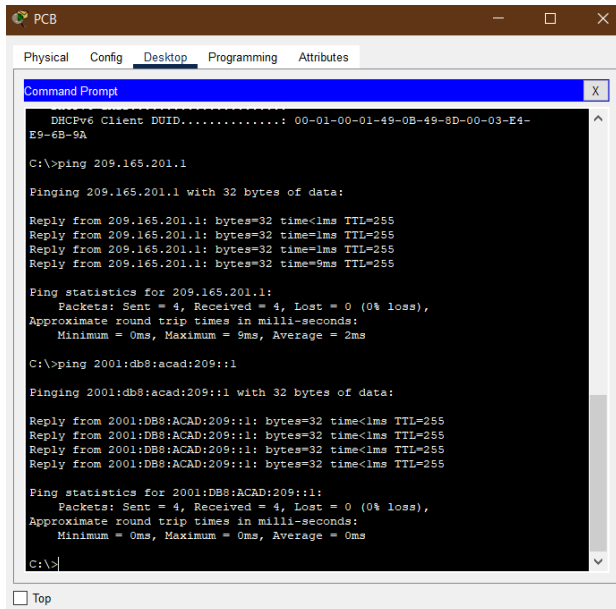
Ping statistics for 2001:DB8:ACAD:209::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
      Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Fuente: Autoría propia

En la figura 18 podemos evidenciar que hay conectividad desde el PCA hacia el router con bucle 0 tanto en ipv4 como en ipv6, ya que al hacer ping este nos genera una respuesta positiva al enviar los datos.

Figura 19. Ping de PCB a Bucle 0 Router

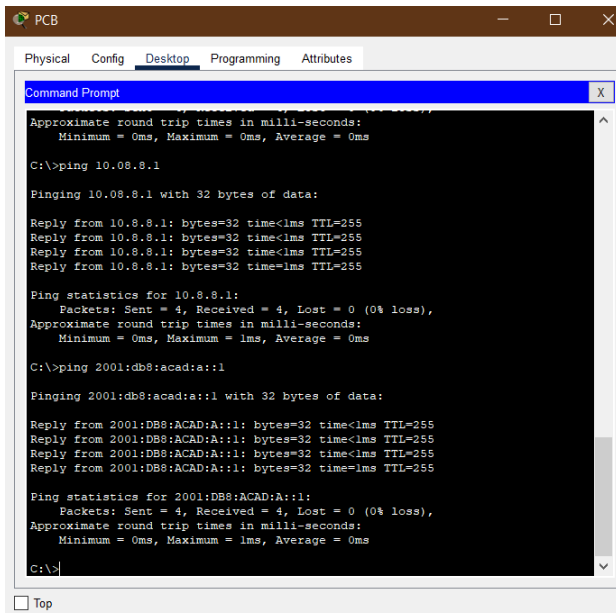


```
PCB
Physical Config Desktop Programming Attributes
Command Prompt
DHCPv6 Client DUID.....: 00-01-00-01-49-0B-49-8D-00-03-E4-
E9-6B-9A
C:\>ping 209.165.201.1
Pinging 209.165.201.1 with 32 bytes of data:
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time=9ms 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 = 9ms, Average = 2ms
C:\>ping 2001:db8:acad:209::1
Pinging 2001:db8:acad:209::1 with 32 bytes of data:
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255
Ping statistics for 2001:DB8:ACAD:209::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Fuente: Autoría propia

En la figura 19 podemos evidenciar que hay conectividad desde el PCB hacia el router con bucle 0 tanto en ipv4 como en ipv6, ya que al hacer ping este nos genera una respuesta positiva al enviar los datos.

Figura 20. Ping de PCB a Interface Giga0/0/1.20 del Router

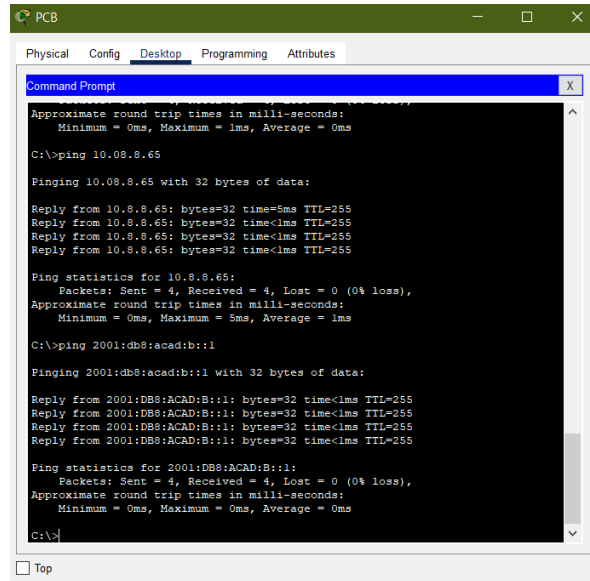


```
PCB
Physical Config Desktop Programming Attributes
Command Prompt
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 10.08.8.1
Pinging 10.08.8.1 with 32 bytes of data:
Reply from 10.8.8.1: bytes=32 time<1ms TTL=255
Reply from 10.8.8.1: bytes=32 time<1ms TTL=255
Reply from 10.8.8.1: bytes=32 time<1ms TTL=255
Reply from 10.8.8.1: bytes=32 time<1ms TTL=255
Ping statistics for 10.8.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 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:\>
```

Fuente: Autoría propia

En la figura 20 podemos evidenciar que hay conectividad desde el PCB hacia el router con interface giga0/0/1.20 tanto en ipv4 como en ipv6, ya que al hacer ping este nos genera una respuesta positiva al enviar los datos.

Figura 21. Ping de PCB a Interface Giga0/0/1.30 del Router



```
PCB
Physical Config Desktop Programming Attributes
Command Prompt
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.08.8.65

Pinging 10.08.8.65 with 32 bytes of data:

Reply from 10.08.8.65: bytes=32 time<1ms TTL=255
Reply from 10.08.8.65: bytes=32 time<1ms TTL=255
Reply from 10.08.8.65: bytes=32 time<1ms TTL=255
Reply from 10.08.8.65: bytes=32 time<1ms TTL=255

Ping statistics for 10.08.8.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
      Minimum = 0ms, Maximum = 5ms, Average = 1ms

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

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

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

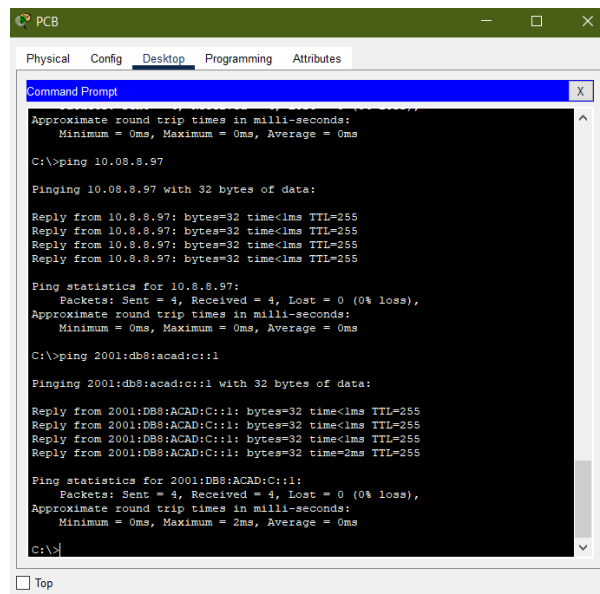
Ping statistics for 2001:DB8:ACAD:B::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
      Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente5: Autoría propia

En la figura 21 podemos evidenciar que hay conectividad desde el PCB hacia el router con interface giga0/0/1.30 tanto en ipv4 como en ipv6, ya que al hacer ping este nos genera una respuesta positiva al enviar los datos.

Figura 22. Ping de PCB a Interface Giga0/0/1.40 del Router



```
PCB
Physical Config Desktop Programming Attributes
Command Prompt
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.08.8.97

Pinging 10.08.8.97 with 32 bytes of data:

Reply from 10.08.8.97: bytes=32 time<1ms TTL=255
Reply from 10.08.8.97: bytes=32 time<1ms TTL=255
Reply from 10.08.8.97: bytes=32 time<1ms TTL=255
Reply from 10.08.8.97: bytes=32 time<1ms TTL=255

Ping statistics for 10.08.8.97:
    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: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=2ms TTL=255

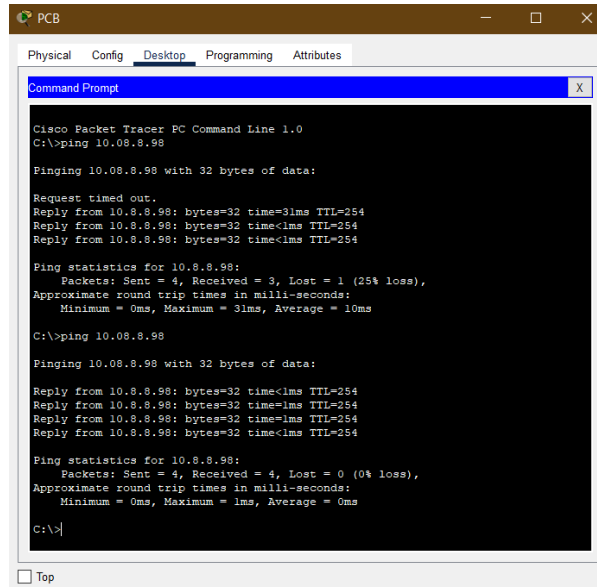
Ping statistics for 2001:DB8:ACAD:C::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
      Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>
```

Fuente: Autoría propia

En la figura 22 podemos evidenciar que hay conectividad desde el PCB hacia el router con interface giga0/0/1.40 tanto en ipv4 como en ipv6, ya que al hacer ping este nos genera una respuesta positiva al enviar los datos.

Figura 23. Ping de PCB a Vlan 40 del switch 1 con ipv4



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.08.8.98

Pinging 10.08.8.98 with 32 bytes of data:

Request timed out.
Reply from 10.08.8.98: bytes=32 time=31ms TTL=254
Reply from 10.08.8.98: bytes=32 time<1ms TTL=254
Reply from 10.08.8.98: bytes=32 time<1ms TTL=254

Ping statistics for 10.08.8.98:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 31ms, Average = 10ms

C:\>ping 10.08.8.98

Pinging 10.08.8.98 with 32 bytes of data:

Reply from 10.08.8.98: bytes=32 time<1ms TTL=254
Reply from 10.08.8.98: bytes=32 time=1ms TTL=254
Reply from 10.08.8.98: bytes=32 time=1ms TTL=254
Reply from 10.08.8.98: bytes=32 time<1ms TTL=254

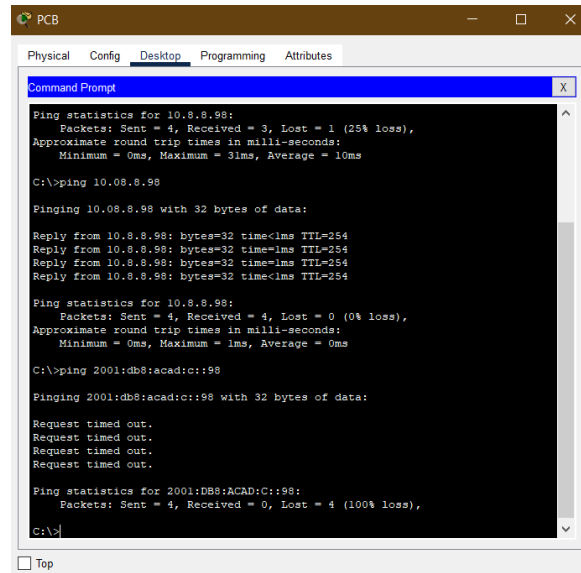
Ping statistics for 10.08.8.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Fuente: Autoría propia

En la figura 23 podemos evidenciar que hay conectividad desde el PCB hacia la vlan 40 del switch 1 en ipv4 ya que al hacer ping este nos genera una respuesta positiva al enviar los datos.

Figura 24. Ping de PCB a Vlan 40 del switch 1 con ipv6



```
Ping statistics for 10.08.8.98:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 31ms, Average = 10ms

C:\>ping 10.08.8.98

Pinging 10.08.8.98 with 32 bytes of data:

Reply from 10.08.8.98: bytes=32 time<1ms TTL=254
Reply from 10.08.8.98: bytes=32 time=1ms TTL=254
Reply from 10.08.8.98: bytes=32 time=1ms TTL=254
Reply from 10.08.8.98: bytes=32 time<1ms TTL=254

Ping statistics for 10.08.8.98:
    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::98

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

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

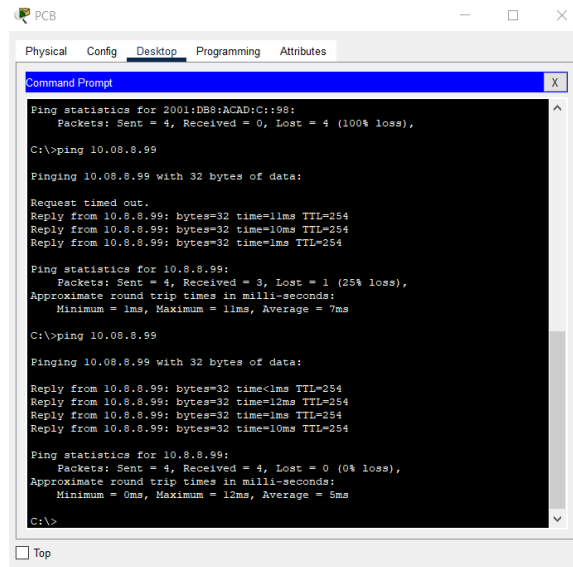
Ping statistics for 2001:DB8:ACAD:C::98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Fuente: Autoría propia

En la figura 24 podemos evidenciar que no hay conectividad desde el PCB hacia la vlan 40 del switch 1 en ipv6, ya que al hacer ping este nos genera una pérdida de datos.

Figura 25. ping de PCB a Vlan 40 del switch 2 con ipv4



```

C:\>ping 2001:db8:acad:c::99
    Ping statistics for 2001:db8:acad:c::99:
        Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.0.8.99
    Pinging 10.0.8.99 with 32 bytes of data:
    Request timed out.
    Reply from 10.0.8.99: bytes=32 time=1ms TTL=254
    Reply from 10.0.8.99: bytes=32 time=10ms TTL=254
    Reply from 10.0.8.99: bytes=32 time=1ms TTL=254

    Ping statistics for 10.0.8.99:
        Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 7ms

C:\>ping 10.0.8.99
    Pinging 10.0.8.99 with 32 bytes of data:
    Reply from 10.0.8.99: bytes=32 time=1ms TTL=254
    Reply from 10.0.8.99: bytes=32 time=12ms TTL=254
    Reply from 10.0.8.99: bytes=32 time=1ms TTL=254
    Reply from 10.0.8.99: bytes=32 time=10ms TTL=254

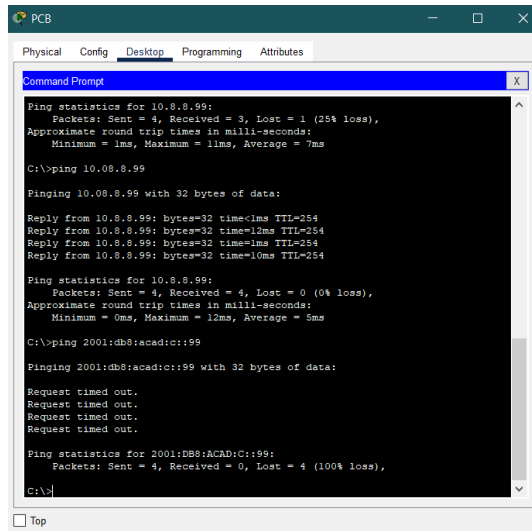
    Ping statistics for 10.0.8.99:
        Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 5ms

C:\>
    
```

Fuente: Autoría propia

En la figura 25 podemos evidenciar que hay conectividad desde el PCB hacia la vlan 40 del switch 2 en ipv4 ya que al hacer ping este nos genera una respuesta positiva al enviar los datos.

Figura 26. ping de PCB a Vlan 40 del switch 2 con ipv6



```

C:\>ping 10.0.8.99
    Ping statistics for 10.0.8.99:
        Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 7ms

C:\>ping 10.0.8.99
    Pinging 10.0.8.99 with 32 bytes of data:
    Reply from 10.0.8.99: bytes=32 time=1ms TTL=254
    Reply from 10.0.8.99: bytes=32 time=12ms TTL=254
    Reply from 10.0.8.99: bytes=32 time=1ms TTL=254
    Reply from 10.0.8.99: bytes=32 time=10ms TTL=254

    Ping statistics for 10.0.8.99:
        Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 5ms

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: Autoría propia

En la figura 26 podemos evidenciar que no hay conectividad desde el PCB hacia la vlan 40 del switch 2 en ipv6, ya que al hacer ping este nos genera una pérdida de datos.

CONCLUSIONES

Después de analizar y desarrollar el primer escenario podemos observar cómo funciona el mundo de las redes de comunicación, esto debido a como el profesional interactúa con esta área de una manera mucho más compleja, aplicando los conocimientos adquiridos en el diplomado de cisco y realizando las diferentes configuraciones para cada uno de los dispositivos presentes en este primer escenario debido a esto el profesional adquiere la capacidad para resolver problemas de configuración, enrutamiento y de seguridad brindando las garantías necesarias para que las redes operen de manera segura y satisfactorias.

La solución de este primer escenario se basó en la configuración desde cero de una topología de red cumpliendo con cada uno de las instrucciones necesarias para lograr dar solución a este problema esto aplicando los diferentes conceptos adquiridos en las diferentes temáticas que se encuentra en la plataforma de netacad que fueron de gran ayuda a la hora de abordar estos temas.

Después de analizar y desarrollar el segundo escenario se logró evidenciar algunas características de configuración utilizadas anteriormente que permiten brindar la seguridad a nuestra red, utilizando los comandos necesarios para desarrollar la configuración de la red, observando los cambios en la conectividad de la red y cómo cada proceso influye en el funcionamiento correcto de nuestra red, garantizando que esta funcione en completa armonía.

Podemos concluir que estos dos escenarios fue necesario aplicar los conocimientos básicos hasta los más avanzados en los diferentes escenarios planteados lo que nos permite fortalecer nuestros conocimientos para lograr cumplir los objetivos que generan las tecnologías en especial las redes ya que son un campo completamente extenso y de mucho cuidado por la información que estas manejan.

REFERENCIAS

ABAD DOMINGO, Alfredo. Redes locales. Madrid: McGraw-Hill. [En línea] (2013) [27 noviembre 2022]. 250p. Disponible en:

<https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/50228?page=1>.

CASTAÑO RIBES, Rafael Jesús, y LOPEZ FERNANDEZ, Jesús. Redes locales. Madrid: Macmillan Iberia. [En línea] (2013) [27 noviembre 2022]. 322p Disponible en:

<https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43257?page=1>.

CASTAÑO RIBES, Rafael Jesús. Redes locales. Madrid: Macmillan Iberia S.A. [En línea] (2013) [27 noviembre 2022]. 322p. Disponible en:

<https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43257?page=1>.

ERNESTO, Ariganello. Redes ciscos. Guía de estudio para la certificación CCNA Routing y Switching. España RA-MA 4ª edición actualizada. [En línea] (2016) [27 noviembre 2022]. 561p. Disponible en:

<https://web-s-ebshost-com.bibliotecavirtual.unad.edu.co/ehost/ebookviewer/ebook/bmxlYmtfXzI0OTgzMjZfX0FO0?sid=d9d99d0e-2b15-46c1-a251-246f19fc1868%40redis&vid=0&format=EB&rid=1>

Flor, Paulita. Modelo TCP/IP. Objeto virtual de Información OVI. [En línea] (2021) [27 noviembre 2022]. Disponible en:

<https://repository.unad.edu.co/handle/10596/43437>

Guaca, Nancy. Configuración básica Switches. Objeto virtual de Información OVI. [En línea] (2018) [27 noviembre 2022]. Disponible en:

<https://repository.unad.edu.co/handle/10596/23215>

TAPIAS, Juan. Esteban. Introducción a las VLAN. Objeto virtual de Información OVI. (2022) [27 noviembre 2022]. Disponible en:

<https://repository.unad.edu.co/handle/10596/49452>

ANEXOS

Anexo A

[ESCENARIOS](#)