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

ELKIN PEREZ PEREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA *DE SISTEMAS*
CARTAGENA
2022

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

CARTAGENA, 27 de Noviembre de 2022

AGRADECIMIENTOS

Al ver el resultado logrado con este proyecto, solamente se me ocurre una palabra: ¡Gracias!, Todo el trabajo realizado fue posible gracias al apoyo incondicional de Dalia, mi esposa, que estuvo a mi lado en los momentos difíciles, y a mis hijos, Dania y Dhael, cuya paciencia fue puesta a prueba en incontables ocasiones. Gracias, también, a mi padre y a madre, que me dieron todo lo que necesité, y a mis amigos, que me dieron su contención. Nada de esto hubiera sido posible sin ustedes. Este trabajo es el resultado de un sinfín de acontecimientos que poco tuvieron que ver con lo académico, sino más bien, con el amor. Gracias infinitas a ustedes y, por supuesto, a Dios, por ponerlos en mi camino.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

LAN: Es una infraestructura de la red que abarca un área geográfica pequeña. Las LANs tienen características específicas:
Las LANs interconectan terminales en un área limitada, como una casa, un lugar de estudios, un edificio de oficinas o un campus.
Por lo general, la administración de las LAN está a cargo de una única organización o persona. El control administrativo se aplica a nivel de red y rige las políticas de seguridad y control de acceso.[1]
Direccionamiento de dispositivos finales: los dispositivos finales deben configurarse con una dirección IP única para la identificación en la red.[2]
Switching de almacenamiento y envío: Este método de reenvío de trama recibe la trama completa y calcula el CRC. La CRC utiliza una fórmula matemática basada en la cantidad de bits (números uno) de la trama para determinar si esta tiene algún error. Si la CRC es válida, el switch busca la dirección de destino, que determina la interfaz de salida. Luego, la trama se reenvía desde el puerto correcto.[3]
Enrutamiento: La capa de red proporciona servicios para dirigir los paquetes a un host de destino en otra red. Para transferir un paquete a otras redes, debe procesarlo un router. La función del router es seleccionar la mejor ruta y dirigir los paquetes al host de destino en un proceso que se denomina "enrutamiento". Un paquete puede cruzar muchos routers antes de llegar al host de destino. Se denomina "salto" a cada router que cruza un paquete antes de alcanzar el host de destino.[4]
Puerta de Enlace Predeterminada: La puerta de enlace predeterminada es el dispositivo de red (es decir, el router o el switch de capa 3) que puede enrutar el tráfico a otras redes. Si se piensa en una red como si fuera una habitación, el gateway predeterminado es como la puerta. Si desea ingresar a otra habitación o red, debe encontrar la puerta.[5]

[1] MCCANCE, Shaun. Términos-y-consejos-sobre-redes (2010).
[2] ROUSE, Margaret**.** Interfaz –de- línea- de- comandos-o-CLI (2000).
[3] FUNG, Jacinto. Redes Informáticas: Protocolos de Comunicación, Protocolo de Aplicación
[4] TANENBAUN, Andrew s. La capa de red de internet (2003)
[5] AVILA, Raul. El bit a las redes sociales (2019).

RESUMEN

Esta actividad tiene como objetivo dar solución a dos escenarios planteados, en cada uno de los escenarios utilizaremos dispositivos Cisco , los cuales se configuraran de manera exitosa mediante todos los comandos que nos brinda el curso en la plataforma de Cisco de tal manera que todo quede funcional de manera optime según lo requerido, los dispositivos procederemos a configurar serán , Router , Switch y dispositivos finales como pc de escritorio , todo esto realizado en el Simulador Packet tracert.

Para la ejecución de esta actividad comprenderemos y implementaremos conceptos como Vlans , Subneting ,Routing Port Security IPV4 e IPV6 ,EtherChannel , interVlans , y finalizaremos con la verificación de la conectividad entre los dispositivos mediante los protocolos Ipv4 e Ipv6 a través del comando Ping, esto nos permitirá comprobar que la solución esta correctamente funcional y que los equipos fueron configurados de manera correcta.

Palabras Clave: VLSM,VLAN,EtherChannel,Enrutamiento,PortSecurity, SSH.

ABSTRACT

The purpose of this activity is to provide a solution to two proposed scenarios, in each of the scenarios we will use Cisco devices, which will be successfully configured using all the commands provided by the course on the Cisco platform in such a way that everything remains functional. optimally as required, the devices we will proceed to configure will be Router, Switch and end devices such as desktop PCs, all this done in the Packet tracert Simulator.

For the execution of this activity we will understand and implement concepts such as Vlans, Subneting, Routing Port Security IPV4 and IPV6, EtherChannel, interVlans, and we will finish with the verification of the connectivity between the devices through the IPv4 and Ipv6 protocols through the Ping command, this It will allow us to verify that the solution is correctly functional and that the equipment was configured correctly.

Keywords: VLSM,VLAN, EtherChannel ,Routing ,Port Securiry, SSH.

INTRODUCCIÓN

Con el fin de garantizar una mejor comunicación, la humanidad ha realizado un sin número de progreso tecnológico lo cual ha mejorado la comunicación para tener un mejor estilo de vida y mayormente las empresas han sido las mayores beneficiadas con este mejoramiento tecnológico ya que el intercambio de información entre departamento se hace de manera eficiente esto debió al concetos de rede de datos, partiendo de esto , procedernos a colocar todos nuestros conocimientos adquiridos en este diplomado para la realización de dos escenarios los cuales describiremos continuación :

En el escenario 1 se procederá a realizar la configuración de una red local, donde se manejara la configuración IPv4 para los switches, el Router y las LAN propuestas, con sus respectivas configuraciones de seguridad para cada una de estas LAN tendrán especificaciones en sus hosts de direccionamiento, sus configuraciones de seguridad de acceso a sus consolas, esto con la finalidad de mitigar que algún usuario intruso pueda ingresar y sustraer información , al finalizas todos los dispositivos te intercomunicaran entre si .

.

En el escenario 2 se procederá a realizar la configuración de una red local , se manejara la configuración que acepten los protocolos IPv4 y configuración IPv6 en los dispositivos (Router, Switch y PC) ,se realizará el respectivo enrutamiento entre VLAN, DHCP, Etherchannel y port-security que también se deben administrar forma segura con sus respectivas configuraciones de seguridad de acceso a sus consolas.

1. ESCENARIO 1

Figura 1. Escenario 1

Fuente: prueba de habilidades diplomado CCNA 2022.

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

Tabla 1. Esquema de direccionamiento

Item	**Requerimiento**
Dirección de Red	172.XY.3.0 donde XY corresponde a los últimos dos dígitos de su cédula.
Requerimiento de host Subred LAN1	60
Requerimiento de host Subred LAN2	20
R1 G0/0/1	172.80.3.62
R1 G0/0/0	172.80.3.94
S1 SVI	172.80.3.2
PC-A	172.80.3.10
PC-B	172.80.3.72

1.2 Configuración de aspectos básicos (S1 Y R1)

Tabla 2. Configuración de R1

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

Fuente: prueba de habilidades diplomado CCNA2022.

Item	Comandos	Explicación
Configurar nombre	Router> Router>enable Router#configureterminal Router(config)#hostname R1	Ingresamos a modo configuración global y a través del comando hostname se le agrega un nombre y así identificar nuestro dispositivo en la red.
Desactivar búsqueda DNS	R1(config)#no ip domain-lookup	Ingresamos a modo configuración global y a través del comando desactivamos la búsqueda de DNS , para que al equivocarnos en alguna palabra no demore unos segundos buscando algún nombre de host.
Nombre de dominio	R1(config)#ip domain-name ccna-sa.com	Ingresamos al modo configuración global y mediante el comando y le asociamos un nombre de dominio el cual queda asociada a la ip que se le configura, donde se llame a este nombre se resolverá al equipo determinado.
Configurar contraseña cifrada modo exec privilegiado	R1(config)#enable secret ciscoenpas	Ingresamos al modo Exec privilegiado y mediate el comando configuramos una contraseña debido a que en este modo podemos acceder a muchos comandos privilegiados que modifican parámetros operativos.
Configurar contraseña de acceso a consola	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login	Ingresamos a modo configuración, mediante los comandos en mención agregamos una contraseña para poder ingresar a la consola del dispositivo.
Establecer longitud mínima para contraseñas	R1(config)#security passwords min-length 10	Ingresamos al modo de configuración global, a través de este comando le indicamos una longitud máxima.
Crear un usuario administrativo en la BD Local	R1(config)#username admin password admin1pass R1(config)#line console 0 R1(config-line)#login local	Ingresamos al modo configuración global, agregamos el comando en mención el cual nos permite tener un usuario y

		una contraseña, luego para que el se asocié a el acceso por consola, ingresamos al modo línea de consola en el mismo como de configuración global, y el login se lo agregamos con la etiqueta loca.
Configure el inicio de sesión en las líneas VTY para que use la base de datos local.	R1#configure terminal R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit	Ingresamos al modo de configuración global mediante el comando configure terminal, luego con el comando de línea vty que nos indica que activamos el protocolo de línea virtual, le asociamos al login el usuario que configuramos en la base de datos local , mediate el comando local.
Configurar las líneas VTY para que acepten únicamente las conexiones SSH.	R1(config)#line vty 0 4 R1(config-line)#login R1(config-line)#login local R1(config-line)#transport input ssh	Luego de ingresar al modo configuración global, ingresamos al modo línea vty, y le decimos que el protocolo ssh estará protegido con el usuario y contraseña que configuramos en la base de datos local del dispositivo.
Cifrar las contraseñas de texto no cifrado.	R1(config)#service password-encryption	Ingresamos al modo de configuración global, luego mediante el comando, encriptamos todas las contraseñas lo cual es muy importante para la seguridad de la red y es una buena práctica.
Configurar un banner MOTD	R1(config)#banner motd #Elkin Perez Perez / Ingenieria de sistemas#	Ingresamos al modo de configuración y mediante el comando banner motd , asociamos un mensaje de bienvenida o advertencia para todo aquel que tiene la intención de ingresar al equipo lo cual es una buena práctica de configuración básica.
Configuración de interface G0/0/0	R1#configure terminal R1(config)#interface gigabitEthernet 0/0/0 R1(config-if)#description LAN2 R1(config-if)#ip address 172.80.3.62 255.255.255.224 R1(config-if)#no shutdown	Luego de ingresar al modo de configuración global, procedemos a ingresar al la interface ggigabte 0/0/0 , luego mediante el comando desctiption agregamos una descripción que vaya relacionada con la función de la interface en este caso como es la puerta de salida o enlace de la lan 2 , le colocamos LAN 2,

		para asociar una ip de esa subred usamos el comando ip address seguido de la ip y la mascara de red para luego activarla mediante el comando no shudown.
Configuración de interface G0/0/1	R1(config)#interface gigabitEthernet 0/0/1 R1(config-if)#ip address 172.80.3.62 255.255.255.192 R1(config-if)#description LAN 1 R1(config-if)#no shutdown	Luego de ingresar al modo de configuración global, procedemos a ingresar a la interface ggigabte 0/0/1, luego mediante el comando desctiption agregamos una descripción que vaya relacionada con la función de la interface en este caso como es la puerta de salida o enlace de la lan 2 , le colocamos LAN 1, para asociar una ip de esa subred usamos el comando ip address seguido de la ip y la máscara de red para luego activarla mediante el comando no shudown.
Generar una clave de cifrado RSA	R1(config-if)#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)#	Ingresamos al modo de configuración global, luego ingresamos el comando crypto key generate rsa para generar las claves RSA , luego le damos un tamaño al módulo de mínimo 1024 bits y así activar el protocolo ssh..
Configurar enrutamiento estático para poder comunicarse por ssh.	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 gigabitEthernet 0/0/1	Para poder tener comunicación con el switch, fue necesario realizar un enrutamiento estático ingresando al modo de configuración global mediante el comando ip route indicando la red que se enrutará por dicha interface de salida.

Fuente: prueba de habilidades diplomado CCNA2022.

Tabla 3. Configuración de S1

Tarea	Especificación
Desactivar la búsqueda DNS	
Nombre del switch	S1
Nombre de dominio	ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Apagar todos los puertos sin usar	F0/1-4, F0/7-24, G0/1-2
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Contraseña: **admin1pass**
Configure el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	
Cifrar las contraseñas de texto no cifrado	
Configurar un banner MOTD	Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.
Generar una clave de cifrado RSA	Módulo de 1024 bits
Configure la interfaz de administración (SVI) en VLAN1	Establecer la descripción Establecer la dirección IPv4

Fuente: prueba de habilidades diplomado CCNA2022.

Item	Comandos	Explicación
Configurar nombre	S1(config)#host S1(config)#hostname S1	Ingresamos a modo configuración global y a través del comando hostname se le agrega un nombre y así identificar nuestro dispositivo en la red.
Desactivar búsqueda DNS	S1(config)#ip domain-name ccna-sa.com	Ingresamos a modo configuración global y a través del comando desactivamos la búsqueda de DNS , para que al equivocarnos en alguna palabra no demore unos segundos buscando algún nombre de host.
Nombre de dominio	S1(config)#ip domain-name ccna-sa.com	Ingresamos al modo configuración global y mediante el comando y le asociamos un nombre de dominio el cual queda asociada a la ip que se le configura, donde se llame a este nombre se resolverá al equipo determinado.
Configurar contraseña cifrada modo exec privilegiado	S1(config)#enable secret ciscoenpas	Ingresamos al modo Exec privilegiado y mediate el comando configuramos una contraseña debido a que en este modo podemos acceder a muchos comandos privilegiados que modifican parámetros operativos.
Configurar contraseña de acceso a consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login	Ingresamos a modo configuración, mediante los comandos en mención agregamos una contraseña para poder ingresar a la consola del dispositivo.
Establecer longitud mínima para contraseñas	S1(config)#security passwords min-length 10	Ingresamos al modo de configuración global, a través de este comando le indicamos una longitud máxima.
Crear un usuario administrativo en la BD Local	S1(config)#username admin password admin1pass S1(config)#line console 0 S1(config-line)#login	Ingresamos al modo configuración global, agregamos el comando en mención el cual nos permite tener un usuario

	local	y una contraseña, luego para que el se asocié a el acceso por consola, ingresamos al modo línea de consola en el mismo como de configuración global, y el login se lo agregamos con la etiqueta loca.
Configure el inicio de sesión en las líneas VTY para que use la base de datos local.	S1#configure terminal S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line)#exit	Ingresamos al modo de configuración global mediante el comando configure terminal, luego con el comando de línea vty que nos indica que activamos el protocolo de línea virtual, le asociamos al login el usuario que configuramos en la base de datos local , mediate el comando local.
Configurar las líneas VTY para que acepten únicamente las conexiones SSH.	S1(config)#line vty 0 4 S1(config-line)#login S1(config-line)#login local S1(config-line)#transport input ssh	Luego de ingresar al modo configuración global, ingresamos al modo línea vty, y le decimos que el protocolo ssh estará protegido con el usuario y contraseña que configuramos en la base de datos local del dispositivo.
Cifrar las contraseñas de texto no cifrado.	S1(config)#service password-encryption	Ingresamos al modo de configuración global, luego mediante el comando, encriptamos todas las contraseñas lo cual es muy importante para la seguridad de la red y es una buena práctica.
Configurar un banner MOTD	S1(config)#banner motd #Elkin Perez Perez / Ingenieria de sistemas#	Ingresamos al modo de configuración y mediante el comando banner motd , asociamos un mensaje de bienvenida o advertencia para todo aquel que tiene la intención de ingresar al equipo lo cual es una buena práctica de configuración básica.
Generar una clave de cifrado RSA	R1(config-if)#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	Ingresamos al modo de configuración global , luego ingresamos el comando crypto key generate rsa para generar las claves RSA , luego le damos un tamaño al modulo de mínimo 1024 bits y así activar el protocolo ssh..

	a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] R1(config)#	
	S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#vlan 1 S1(config)#interface vlan 1 S1(config-if)#ip address 172.80.3.2 255.255.255.192 S1(config-if)#no shutdown S1(config)#ip default-gateway 172.80.3.94	Ingresamos al modo de configuración global, luego ingresamos a la interface virtual Vlan1 , le asociamos la ip determinada de la LAN1 y su mascara de red, luego activamos la interface. Para que los equipos de la subred LAN2 puedan acceder remotamente al switch se debe asociar la puerta de enlace de esa subred lo cual se hizo mediante el comando ip default-gateway.

Fuente: prueba de habilidades diplomado CCNA2022.

1.3 Configuración del PCA Y PCB

Tabla 4. Configuración PCA

Configuración de red de PC-A	
Descripción	PCA
Dirección física	FE80::201:63FF:FEC0:CD19
Dirección IPv4	172.80.3.10
Máscara de subred	255.255.255.192
Puerta de enlace IPv4 predeterminada	172.80.3.62

Fuente: prueba de habilidades diplomado CCNA2022.

Tabla 5. Configuración PCB

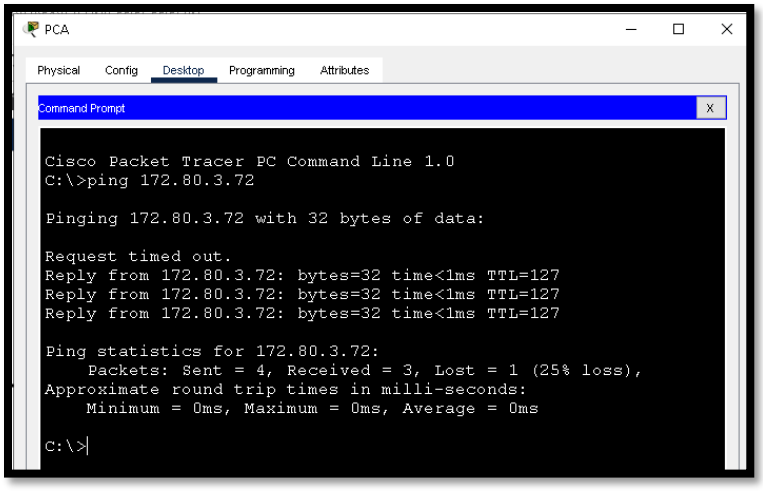
Configuración de red de PC-B	
Descripción	PC B
Dirección física	FE80::202:4AFF:FEE1:BB15
Dirección IPv4	172.80.3.72
Máscara de subred	255.255.255.224
Puerta de enlace IPv4 predeterminada	172.80.3.94

Fuente: prueba de habilidades diplomado CCNA2022.

1.4 Probar y verificar la conectividad de extremo a extremo

- **Ping PCA a PCB**

Figura 2. Ping PCA a PCB

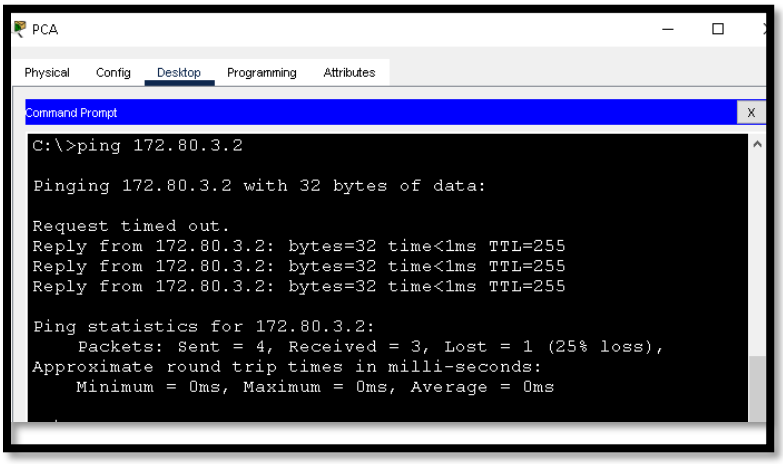


Fuente: Elaboración propia

Se evidencia que hay conectividad entre las dos subredes LAN1 y LAN2, lo cual indica que las configuraciones realizadas en todos los dispositivos de la red están ok

- **PING de PCA A SVI**

Figura 3. PING de PCA A SVI

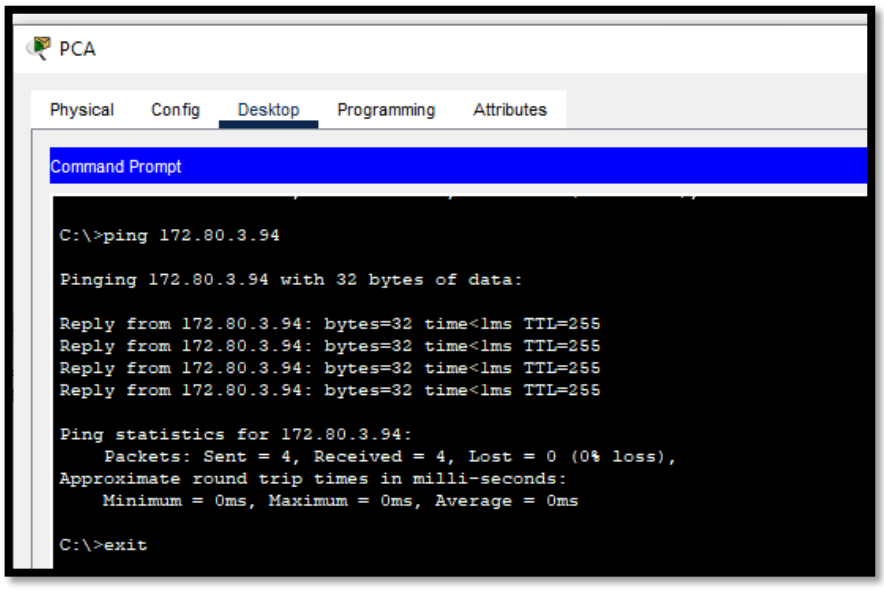


Fuente: Elaboración propia

Se puede evidenciar que hay conectividad entre la Lan1 y entre interface virtual hay conectividad, lo que nos permitirá conectarnos mediante protocolos de conectividad remota al switch y así poder configurar o modificar .

- **Ping PCA a R1 G0/0/0**

Figura 4. Ping PCA a R1 G0/0/0

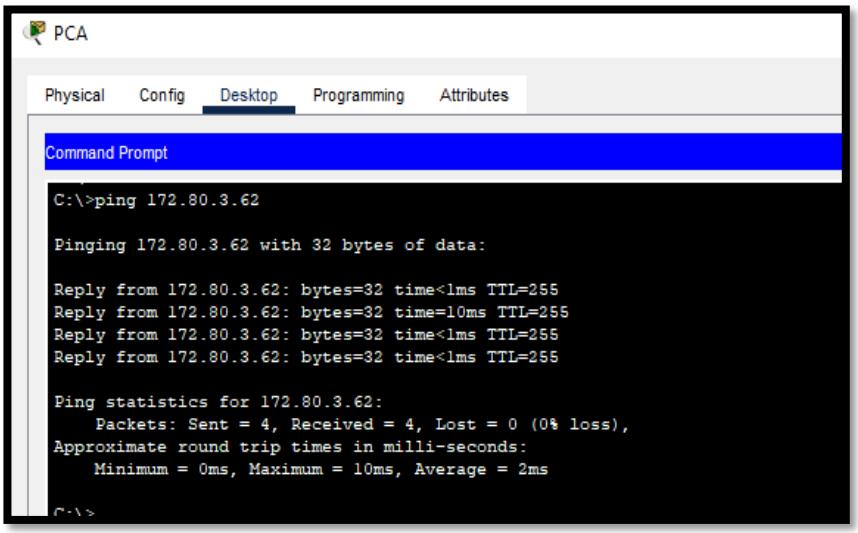


Fuente: Elaboración propia

Se puede evidenciar que hay conectividad entre la LAN1 y la LAN2 mediante la puerta de enlace 0/0/0 que permitirá la salida de los paquetes enviados de la LAN2 a la LAN1.

- **Ping PCA a R1 G0/0/0/1**

Figura 5. Ping PCA a R1 G0/0/0/1

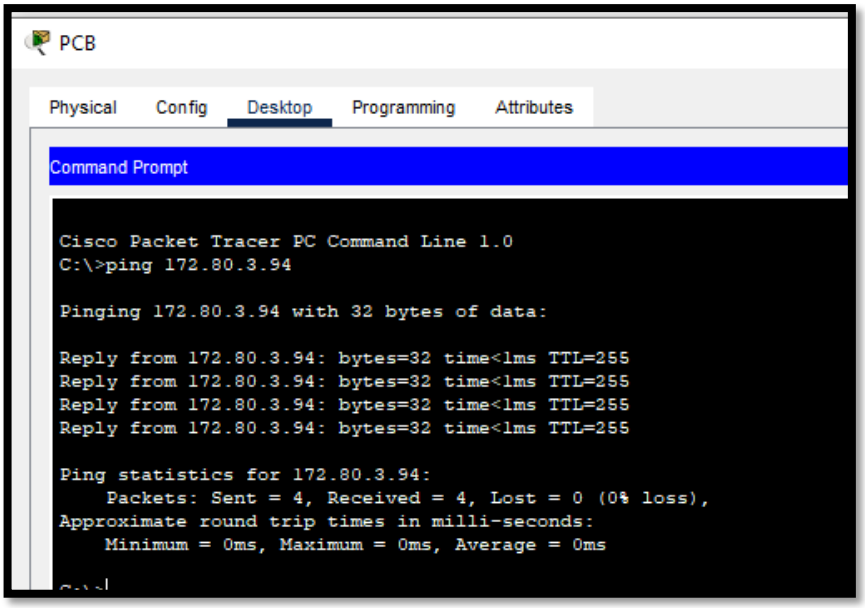


Fuente: Elaboración propia

Se puede evidenciar que hay conectividad entre la LAN1 y la LAN2 mediante la puerta de enlace 0/0/1 que permitirá la salida de los paquetes enviados de la LAN1 a la LAN2.

- **Ping PCB a R1 G0/0/0**

Figura 6.Ping PCB a R1 G0/0/0

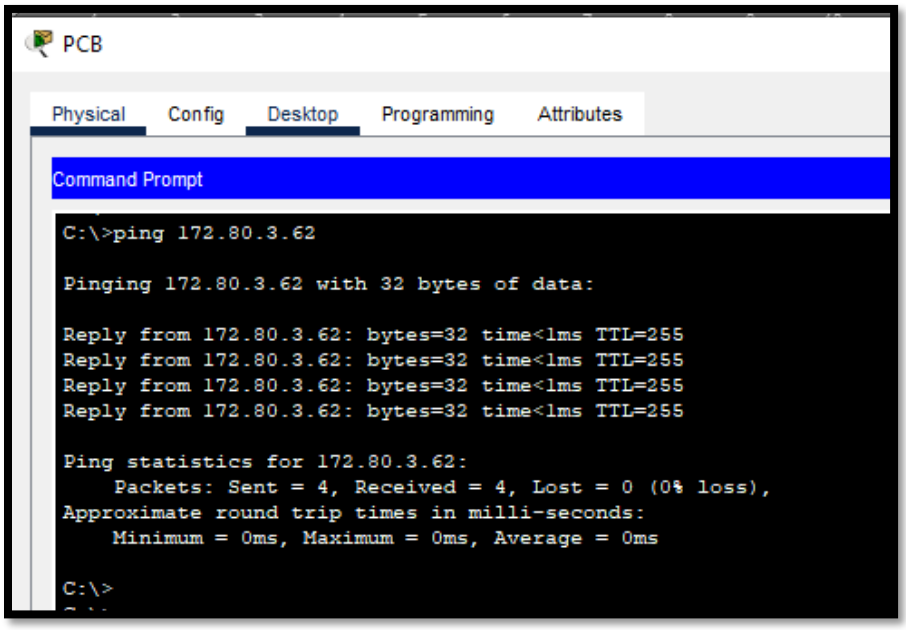


Fuente: Elaboración propia

Se puede evidenciar que hay conectividad entre la LAN2 y la LAN1 mediante la puerta de enlace 0/0/0 que permitirá la salida de los paquetes enviados de la LAN2 a la LAN1.

- **Ping PCB a R1 G/0/0/1**

Figura 7.Ping PCB a R1 G/0/0/1

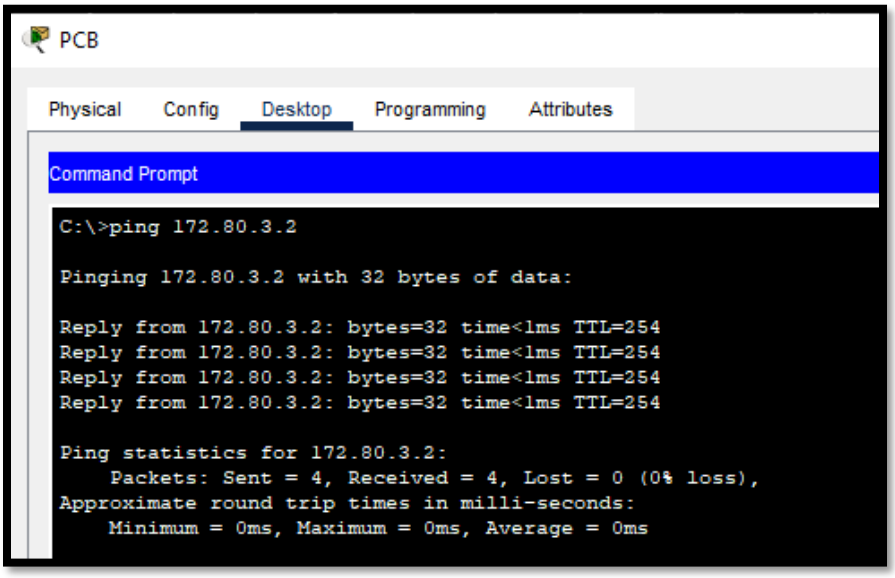


Fuente: Elaboración propia

Se puede evidenciar que hay conectividad entre la LAN2 y la LAN1 mediante la puerta de enlace 0/0/1 que permitirá la salida de los paquetes enviados de la LAN1 a la LAN2.

- **Ping PCB a SVI**

Figura 8. Ping PCB a SVI



Fuente: Elaboración propia

Se puede evidenciar que hay conectividad entre la Lan2 y entre interface virtual hay conectividad, lo que nos permitirá conectarnos mediante protocolos de conectividad remota ssh al switch y así poder configurar o modificar parámetros .

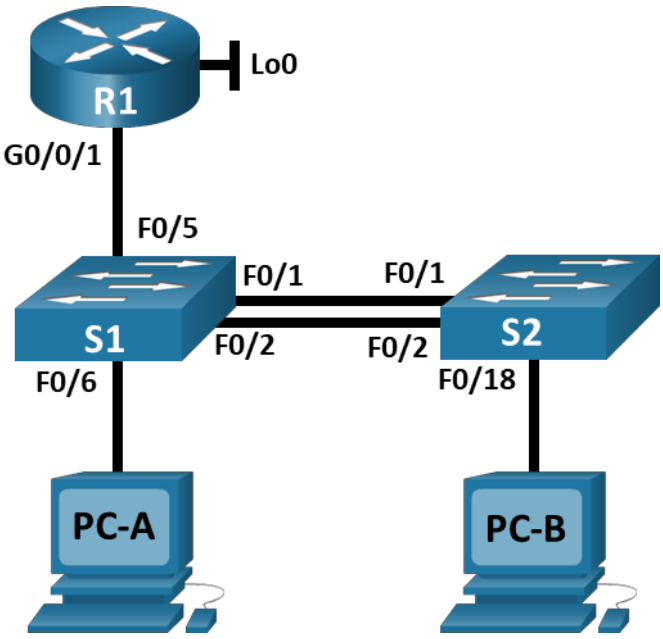
		Dirección IP	Resultados de ping
PC-A	R1 G0/0/0	172.80.3.94	CONECTADO
	R1 G0/0/1	172.80.3.62	CONECTADO
	S1 VLAN 1	172.80.3.2	CONECTADO
	PC-B	172.80.3.72	CONECTADO
PC-B	R1 G0/0/0	172.80.3.94	CONECTADO
	R1 G0/0/1	172.80.3.62	CONECTADO
	S1 VLAN1	172.80.3.2	CONECTADO

Tabla 6. Conectividad

Fuente: prueba de habilidades diplomado CCNA 2022.

2. ESCENARIO 2

Figura 2. Escenario 2



Fuente: prueba de habilidades diplomado CCNA 2022.

Tabla 7. de direccionamiento Escenario 2

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.20	10.80.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.30	10.80.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.40	10.80.8.97 /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	10.80.8.98 /29	10.80.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.80.8.99 /29	10.80.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

Fuente: prueba de habilidades diplomado CCNA 2022.

Tabla 8. Configurar R1

Tarea	Especificación
Nombre del router	R1
Desactivar la búsqueda DNS	
Nombre de dominio	ccna-sa.com
Contraseña cifrada para el modo EXECprivilegiado	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 datoslocal	
Configurar VTY solo aceptando SSH	
Cifrar las contraseñas de texto nocifrado	
Configure un MOTD Banner	Debe contener el nombre del dispositivo, elnombre 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 IPv6como **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 IPv6como **fe80::1**
Generar una clave de cifrado RSA	Módulo de 1024 bits

Fuente: prueba de habilidades diplomado CCNA 2022.

Item	Comandos	Explicación
Configurar nombre	Router> Router>enable Router#configureterminal Router(config)#hostname R1	Ingresamos a modo configuración global y a través del comando hostname se le agrega un nombre y así identificar nuestro dispositivo en la red.
Desactivar búsqueda DNS	R1(config)#no ip domain-lookup	Ingresamos a modo configuración global y a través del comando desactivamos la búsqueda de DNS , para que al equivocarnos en alguna palabra no demore unos segundos buscando algún nombre de host.
Nombre de dominio	R1(config)#ip domain-name ccna-sa.com	Ingresamos al modo configuración global y mediante el comando y le asociamos un nombre de dominio el cual queda asociada a la ip que se le configura, donde se llame a este nombre se resolverá al equipo determinado.
Configurar contraseña cifrada modo exec privilegiado	R1(config)#enable secret class	Ingresamos al modo Exec privilegiado y mediate el comando configuramos una contraseña debido a que en este modo podemos acceder a muchos comandos privilegiados que modifican parámetros operativos.
Configurar contraseña de acceso a consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login	Ingresamos a modo configuración, mediante los comandos en mención agregamos una contraseña para poder ingresar a la consola del dispositivo.
Establecer longitud mínima para contraseñas	R1(config)#security passwords min-length 5	Ingresamos al modo de configuración global, a través de este comando le indicamos una longitud máxima.
Crear un usuario administrativo en la BD Local	R1(config)#username admin password admin1pass R1(config)#line console 0 R1(config-line)#login local	Ingresamos al modo configuración global, agregamos el comando en mención el cual nos permite tener un usuario y una contraseña, luego para que el se asocié a el acceso por consola, ingresamos al modo línea de consola en el mismo como de configuración global, y el login se lo agregamos con la

		etiqueta loca.
Configure el inicio de sesión en las líneas VTY para que use la base de datos local.	R1#configure terminal R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit	Ingresamos al modo de configuración global mediante el comando configure terminal, luego con el comando de línea vty que nos indica que activamos el protocolo de línea virtual, le asociamos al login el usuario que configuramos en la base de datos local , mediate el comando local.
Configurar las líneas VTY para que acepten únicamente las conexiones SSH.	R1(config)#line vty 0 4 R1(config-line)#login R1(config-line)#login local R1(config-line)#transport input ssh	Luego de ingresar al modo configuración global, ingresamos al modo línea vty, y le decimos que el protocolo ssh estará protegido con el usuario y contraseña que configuramos en la base de datos local del dispositivo.
Cifrar las contraseñas de texto no cifrado.	R1(config)#service password-encryption	Ingresamos al modo de configuración global, luego mediante el comando, encriptamos todas las contraseñas lo cual es muy importante para la seguridad de la red y es una buena práctica.
Configurar un banner MOTD	R1(config)#banner motd #Elkin Perez Perez / Ingenieria de sistemas#	Ingresamos al modo de configuración y mediante el comando banner motd , asociamos un mensaje de bienvenida o advertencia para todo aquel que tiene la intención de ingresar al equipo lo cual es una buena práctica de configuración básica.
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing	Este comando que se ejecuta en el modo de configuración global , nos permite trabajar con los protocolos ipv4 e ipv6
Configurar interfaz G0/0/1 ysubinterfaces	Enter configuration commands, one per line. End with CNTL/Z. R1(config)#interface gigabitEthernet 0/0/1.20 R1(config-if)#DEScription puesta enlace vlan 20 R1(config-subif)#encapsulation dot1Q 20 R1(config-subif)#ip address 10.80.8.1 255.255.255.192 R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface	Luego de ingresar al modo de configuración global, procedemos a crear las intervlan mediante los comandos mencionas , seguidos de la descripción y el protocolo de encapsulamiento Dot1q.

	gigabitEthernet 0/0/1.30 R1(config-if)#DEScription puesta enlace vlan 30 R1(config-subif)#encapsulation dot1Q 30 R1(config-subif)#ip address 10.80.8.65 255.255.255.224 R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface gigabitEthernet 0/0/1.40 R1(config-if)#DEScription puesta enlace vlan 40 R1(config-subif)#encapsulation dot1Q 40 R1(config-subif)#ip address 10.80.8.97 255.255.255.248 R1(config-subif)#no shutdown R1(config)#interface gigabitEthernet 0/0/1.56 R1(config-if)#DEScription vlan native R1(config-subif)#exit R1(config-if)#interface loopback0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#no shutdown R1(config-subif)#exit R1(config)#interface gigabitEthernet 0/0/1.20 R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#exit R1(config)#interface gigabitEthernet 0/0/1.30 R1(config-subif)#ipv	

	R1(config-subif)#ipv6 ad R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#exit R1(config)#interface gigabitEthernet 0/0/1.40 R1(config-subif)#ipv6 ad R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#exit R1(config)#interface g0/0/1 R1(config-if)#ipv6 address fe80::1 link-local	
Configure el Loopback0 interface	R1(config)#INTERface LOopback0 R1(config-if)#ipv6 address 2001:Db8:Acad:209::1/64 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#no shutdown R1(config-subif)#exit R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#exit	Luego de ingresar a modo de configuración global se procede a crear la inteface virtual loopback , a la cual le asiganamos la ip añadiendo también la mascara y la el link local para ipv6.
Generar una clave de cifrado RSA	R1(config-if)#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)#	Ingresamos al modo de configuración global, luego ingresamos el comando crypto key generate rsa para generar las claves RSA , luego le damos un tamaño al módulo de mínimo 1024 bits y así activar el protocolo ssh..

Fuente: Elaboración Propia

Tabla 9. Configuración de S1 y S2

Tarea	Especificación
Desactivar la búsqueda DNS.	
Nombre del switch	S1 o S2, según proceda
Nombre de dominio	ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	class
Contraseña de acceso a la consola	cisco
Crear un usuario administrativo en la base dedatos local	Nombre de usuario: **admin** Password: **admin1pass**
Configurar el inicio de sesión en las líneas VTYpara que use la base de datos local	
Configurar las líneas VTY para que aceptenúnicamente las conexiones SSH	
Cifrar las contraseñas de texto no cifrado	
Configurar un MOTD Banner	Debe contener el nombre del dispositivo, el nombre completo delestudiante y el programa académicoal que pertenece.
Generar una clave de cifrado RSA	**Módulo de 1024 bits**
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa3 Establezca la dirección local de enlace IPv6 como **FE80: :98 para S1y FE80: :99 para S2** Establecer la dirección IPv6 de capa3
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.XY.8.97para IPv4

Fuente: prueba de habilidades diplomado CCNA 2022.

Item	Comandos	Explicación
Configurar nombre	S1(config)#hostname S1 S2(config)# hostname S2	Ingresamos a modo configuración global y a través del comando hostname se le agrega un nombre y así identificar nuestro dispositivo en la red.
Desactivar búsqueda DNS	S1(config)#no ip domain-name S2(config)#no ip domain-name	Ingresamos a modo configuración global y a través del comando desactivamos la búsqueda de DNS , para que al equivocarnos en alguna palabra no demore unos segundos buscando algún nombre de host.
Nombre de dominio	S1(config)#ip domain-name ccna-sa.com S2(config)#ip domain-name ccna-sa.com	Ingresamos al modo configuración global y mediante el comando y le asociamos un nombre de dominio el cual queda asociada a la ip que se le configura, donde se llame a este nombre se resolverá al equipo determinado.
Configurar contraseña cifrada modo exec privilegiado	S1(config)#enable secret class S2(config)#enable secret class	Ingresamos al modo Exec privilegiado y mediate el comando configuramos una contraseña debido a que en este modo podemos acceder a muchos comandos privilegiados que modifican parámetros operativos.
Configurar contraseña de acceso a consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S2(config)#line console 0 S2(config-line)#password cisco S2(config-line)#login	Ingresamos a modo configuración, mediante los comandos en mención agregamos una contraseña para poder ingresar a la consola del dispositivo.
Establecer longitud mínima para contraseñas	S1(config)#security passwords min-length 5 S2(config)#security passwords min-length 5	Ingresamos al modo de configuración global, a través de este comando le indicamos una longitud máxima.
Crear un usuario administrativo en la BD Local	S1(config)#username admin password admin1pass S1(config)#line console 0 S1(config-line)#login local S2(config)#username admin password admin1pass S2(config)#line console 0 S2(config-line)#login local	Ingresamos al modo configuración global, agregamos el comando en mención el cual nos permite tener un usuario y una contraseña, luego para que el se asocié a el acceso por consola, ingresamos al modo línea de consola en el mismo como de configuración global, y el login se lo agregamos con la etiqueta loca.
Configure el inicio de sesión en las líneas VTY para que use la base de datos local.	S1#configure terminal S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line)#exit S2#configure terminal S2(config)#line vty 0 4	Ingresamos al modo de configuración global mediante el comando configure terminal, luego con el comando de línea vty que nos indica que activamos el protocolo de línea virtual, le asociamos al login el usuario que configuramos en la base de datos

	S2(config-line)#login local S2(config-line)#exit	local , mediate el comando local.
Configurar las líneas VTY para que acepten únicamente las conexiones SSH.	S1(config)#line vty 0 4 S1(config-line)#login S1(config-line)#login local S1(config-line)#transport input ssh	Luego de ingresar al modo configuración global, ingresamos al modo línea vty, y le decimos que el protocolo ssh estará protegido con el usuario y contraseña que configuramos en la base de datos local del dispositivo.
Cifrar las contraseñas de texto no cifrado.	S1,S2(config)#service password-encryption	Ingresamos al modo de configuración global, luego mediante el comando, encriptamos todas las contraseñas lo cual es muy importante para la seguridad de la red y es una buena práctica.
Configurar un banner MOTD	S1,S2(config)#banner motd #Elkin Perez Perez / Ingenieria de sistemas#	Ingresamos al modo de configuración y mediante el comando banner motd ¸ asociamos un mensaje de bienvenida o advertencia para todo aquel que tiene la intención de ingresar al equipo lo cual es una buena práctica de configuración básica.
Configurar la interfaz de administración (SVI)	S1(config)#interface vlan 40 S1(config-if)#ip address 10.80.8.98 255.255.255.248 (config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#no shutdown S1(config-if)#ipv6 address fe80::98 link-local S2(config)#interface vlan 40 S2(config-if)# %LINK-5-CHANGED: Interface Vlan40, changed state to up S2(config-if)#ip address 10.80.8.99 255.255.255.248 S2(config-if)#ipv6 address 2001:db8:acad:c::99 /64 S2(config-if)#ipv6 address 2001:db8:acad:c::/64 S2(config-if)#ipv6 address fe80::99 link-local	Luedo de ingresar al modo de configuración global procedemos a ingrar el comando para crear la interface que estará asociada a la vlan 40 , la cual nos permitirá la administración vía ssh a los sw.
Generar una clave de cifrado RSA	S1,S2(config-if)#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]	Ingresamos al modo de configuración global , luego ingresamos el comando crypto key generate rsa para generar las claves RSA , luego le damos un tamaño al modulo de mínimo 1024 bits y así activar el protocolo ssh..

Configuración del gateway predeterminado	S1(config)ip default-gateway 10.80.8.97 S2(Config) ip default-gateway 10.80.8.97	Ingresamos al modo de configuración global , luego agregamos el gateway predeterminado .

Fuente: Elaboración propia.

Tabla 10. configuración S1

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

Fuente: prueba de habilidades diplomado CCNA 2022.

Item	**Comandos**	**Explicación**
Crear vlans	S1#configure terminal End with CNTL/Z.	Luego de ingresar al modo de configuración global,

	S1(config)#vl S1(config)#vlan 20 S1(config-vlan)#name Docentes S1(config-vlan)#vlan S1(config-vlan)#exit S1(config)#vlan 30 S1(config-vlan)#name Estudiantes S1(config-vlan)#exit S1(config)#vlan 40 S1(config-vlan)#na S1(config-vlan)#name Invitados S1(config-vlan)#exit S1(config)#nam S1(config)#vl S1(config)#vlan 50 S1(config-vlan)#nad S1(config-vlan)#na S1(config-vlan)#name Usuarios S1(config-vlan)#exit S1(config)#vlan 56 S1(config-vlan)#name Native S1(config-vlan)#exit S1(config)#	procedemos a crear cada vlan , que se exige en la guía , a su ves se le asigna un nombre a cada unas de ellas .
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S1(config)#interface range f0/1-2 S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport access vlan 56 S1(config)#interface fastEthernet 0/5 S1(config-if)#switchport mode trunk 56 S1(config-if)#exit. S1(config-if-range)#switchport access vlan 56	Luego de ingresar al modo de configuración global, procedemos a crear las intervlan mediante los comandos mencionas , seguidos de la descripción y el protocolo de encapsulamiento Dot1q.
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1(config)#interface range fastEthernet 0/1-2 channel-group channel-protocol S1(config-if-range)#channel-group 1 mode active S1(config-if-range)# Creating a port-channel interface Port-channel 1 S1(config-if-range)#exit S1(config)#interface port-channel 1 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk allowed vlan 20,30,40	Luego de ingresar al modo de configuración global , procedemos a crear el etherchanel , configurando los puertos solicitados de manera troncal para luego activar el portchanel e indicarles de pasaran por las vlan correspondientes.
Configurar el puerto de acceso de host	S1(config)#interface fastEthernet 0/6	Luego de ingresar al modo de configuración global,

para VLAN 20	S1(config-if)#switchport access vlan 20	procedemos a crear a configurar la interface del sw f0/6 de tal manera que este asociado a la vlan 20
Configurar la seguridad del puerto en los puertos de acceso	S1(config)#interface range fastEthernet 0/1-2 S1(config-if-range)#switchport port-security maximum 4 S1(config-if-range)#exit	Luego de ingresar al modo de configuración global, procedemos a crear a indicar que los puertos de los dispositivos locales tengan un máximo de 4 mac asociadas.
Proteja todas las interfaces no utilizadas	S1(config)#interface range f0/3-4 ,f0/7-24,g0/1-2 S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#switchport mode access S1(config-if-range)#description Interfaces apagadas S1(config-if-range)#shutdown	Luego de ingresar al modo de configuración global, procedemos a indicarle al sw que los puertos en los cuales no se están utilizando se procedan a apagar para de esta manera tener una mayor seguridad.

Fuente: elaboración propia.

Tabla 11. de Configuración S2

Tareas	**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 6nativa	Interfaces F0/1, F0/2 y F0/5
Crear un grupo de puertos EtherChannel deCapa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación

Configurar el puerto de acceso de host paraVLAN 30	Interface F0/18
Configurar la seguridad del puerto en lospuertos de acceso	Permitir 4 direcciones MAC
Proteja todas las interfaces no utilizadas	Asignar a VLAN 50, Establecer en modode acceso, agregar una descripción y apagar

Fuente: prueba de habilidades diplomado CCNA 2022.

Item	Comandos	Explicación
	S2#configure terminal End with CNTL/Z. S2(config)#vl S2(config)#vlan 20 S2(config-vlan)#name Docentes S2(config-vlan)#vlan S2(config-vlan)#exit S2(config)#vlan 30 S2(config-vlan)#name Estudiantes S2(config-vlan)#exit S2(config)#vlan 40 S2(config-vlan)#na S2(config-vlan)#name Invitados S2(config-vlan)#exit S2(config)#nam S2(config)#vl S2(config)#vlan 50 S2(config-vlan)#nad S2(config-vlan)#na S2(config-vlan)#name Usuarios S2config-vlan)#exit S2(config)#vlan 56 S2(config-vlan)#name Native S2(config-vlan)#exit S2(config)#	Luego de ingresar al modo de configuración global, procedemos a crear cada vlan , que se exige en la guía , a su ves se le asigna un nombre a cada unas de ellas .
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S2(config)#interface range f0/1-2 S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport access vlan 56 S2(config-if)#switchport mode trunk 56 S2(config-if)#exit. S2(config-if-range)#switchport access vlan 56	Luego de ingresar al modo de configuración global, procedemos a crear las intervlan mediante los comandos mencionas , seguidos de la descripción y el protocolo de encapsulamiento Dot1q.
Crear un grupo de puertos EtherChannel de Capa 2 que use	S2(config)#interface range fastEthernet 0/1-2 channel-group channel-	Luego de ingresar al modo de configuración global , procedemos a crear el

interfaces F0/1 y F0/2	protocol 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)#exit S2(config)#interface port-channel 1 S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk allowed vlan 20,30,40	etherchanel , configurando los puertos solicitados de manera troncal para luego activar el portchanel e indicarles de pasaran por las vlan correspondientes.
Configurar el puerto de acceso de host para VLAN 30	S2(config)#interface fastEthernet 0/18 S2(config-if)#switchport access vlan 30	Luego de ingresar al modo de configuración global, procedemos a crear a configurar la interface del sw f0/18 de tal manera que este asociado a la vlan 30
Configurar la seguridad del puerto en los puertos de acceso	S2(config)#interface range fastEthernet 0/1-2 S2(config-if-range)#switchport port-security maximum 4 S2(config-if-range)#exit S2(config)#interface f0/18 S2(config-if)#switchport port-security maximum 4	Luego de ingresar al modo de configuración global, procedemos a crear a indicar que los puertos de los dispositivos locales tengan un máximo de 4 mac asociadas.
Proteja todas las interfaces no utilizadas	S2(config)#interface range f0/3-17,f0/19-24,g0/1-2 S2(config-if-range)#switchport access vlan 50 S2(config-if-range)#shutdown	Luego de ingresar al modo de configuración global, procedemos a indicarle al sw que los puertos en los cuales no se están utilizando se procedan a apagar para de esta manera tener una mayor seguridad.

Fuente: elaboración propia .

Tabla 12. Configurar Soporte de host

Tarea	**Especificación**

Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0
Configurar IPv4 DHCP paraVLAN 20	Cree un grupo DHCP para VLAN 20, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sa.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada
Configurar DHCP IPv4 paraVLAN 30	Cree un grupo DHCP para VLAN 30, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sb.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada

Fuente: prueba de habilidades diplomado CCNA 2022.

Item	Comandos	Explicación
Configure Default Routing	R1(config)#ipv6 route ::/0 loopback0 R1(config)#ip route 0.0.0.0 0.0.0.0 loopback0	
Configurar IPv4 DHCP paraVLAN 20	R1(dhcp-config)#default-router 10.80.8.97 R1(dhcp-config)#network 10.80.8.0 255.255.255.192 R1(config)#ip dhcp excluded-address 10.80.8.1 10.80.8.51 R1(config)#ip dhcp pool POOL-VLAN20 R1(dhcp-config)#domain-name unad-ccna-sa.net R1(dhcp-config)#exit	
Configurar DHCP IPv4 paraVLAN 30	R1(config)#ip dhcp pool POOL-VLAN30 R1(dhcp-config)#default-router 10.80.8.97 R1(dhcp-config)#domain-name unad-ccna-sb.net R1(dhcp-config)#network 10.80.8.64 255.255.255.224 R1(config)#ip dhcp excluded-address 10.80.8.65 10.80.8.83	

Fuente: elaboración propia .

Tabla 13. Configuracion de PC A

Configuración de red de PC-A	
Descripción	PC A
Dirección física	00D0.BC66.0C51
Dirección IP	10.80.8.52
Máscara de subred	255.255.255.192
Gateway predeterminado	10.80.8.97
Gateway predeterminado IPv6	FE80::1

Fuente: prueba de habilidades diplomado CCNA 2022.

Tabla 14. Configuracion de PC B

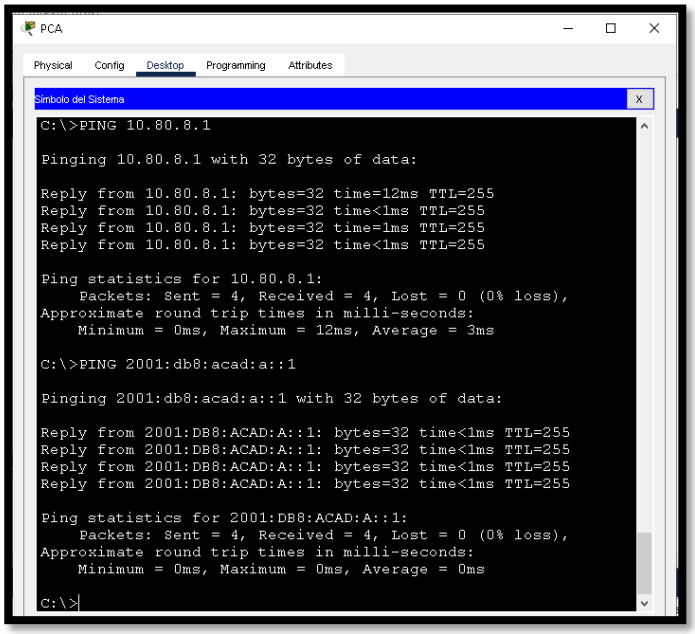
Configuración de red de PC-B	
Descripción	PC B
Dirección física	0001.6344.A46C
Dirección IP	10.80.8.84
Máscara de subred	255.255.255.224
Gateway predeterminado	10.80.8.97
Gateway predeterminado IPv6	FE80::1

Fuente: prueba de habilidades diplomado CCNA 2022.

Probar y verificar la conectividad de extremo a extremo

- **Ping PC-A - R1, G0/0/1.20 – IPV4 e IPV6**

Figura 9 Ping PC-A - R1, G0/0/1.20 – IPV4 e IPV6

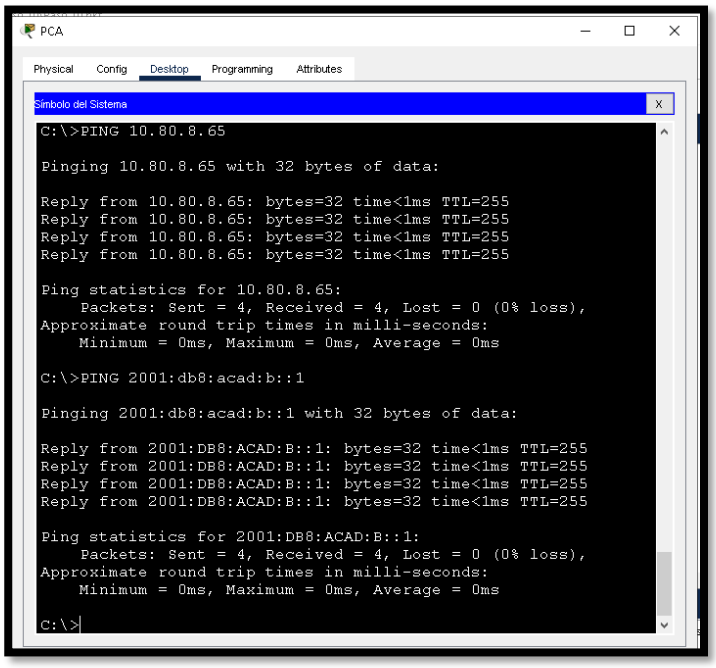


Fuente: Elaboración propia

Se puede evidenciar que hay Conectividad entre la puertas de enlace que hacen permiten coactividad para los dispositivos de la vlan 20 (Docentes)que se encuentran en la interface del router de las

- **Ping PC-A - R1, G0/0/1.30 – IPV4 e IPV6**

Figura 10 Ping PC-A - R1, G0/0/1.30 – IPV4 e IPV6

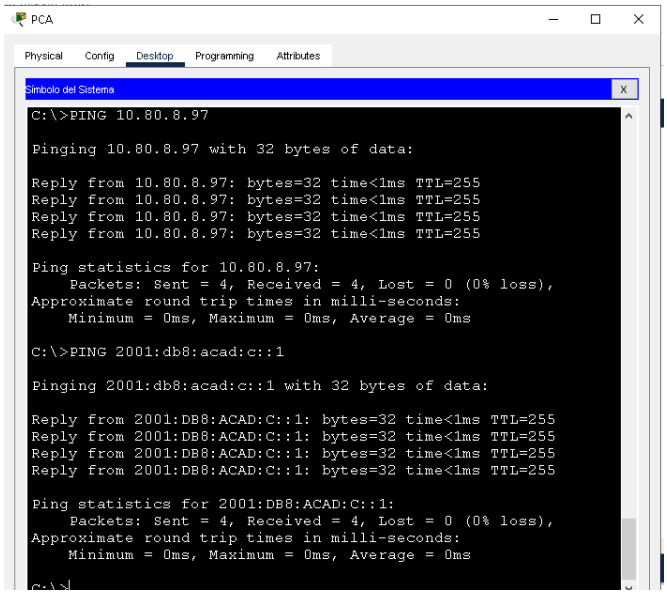


Fuente: Elaboración propia

Se puede evidenciar que hay Conectividad entre la puertas de enlace que hacen permiten coactividad para los dispositivos de la vlan 30 (Estudiantes)que se encuentran en la interface del router de las

- **Ping PC-A - R1, G0/0/1.40 – IPV4 e IPV6**

Figura 11 Ping PC-A - R1, G0/0/1.40 – IPV4 e IPV6

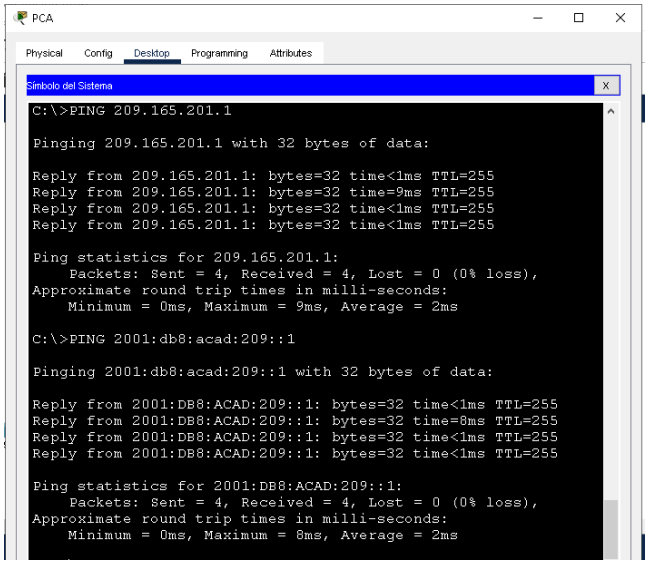


Fuente: Elaboración propia

Se puede evidenciar que hay Conectividad entre la puertas de enlace que hacen permiten coactividad para los dispositivos de la vlan 40 (Invitados)que se encuentran en la interface del router de las

- **Ping PC-A - R1, Loopback0– IPV4 e IPV6**

Figura 12 Ping PC-A - R1, Loopback0– IPV4 e IPV6

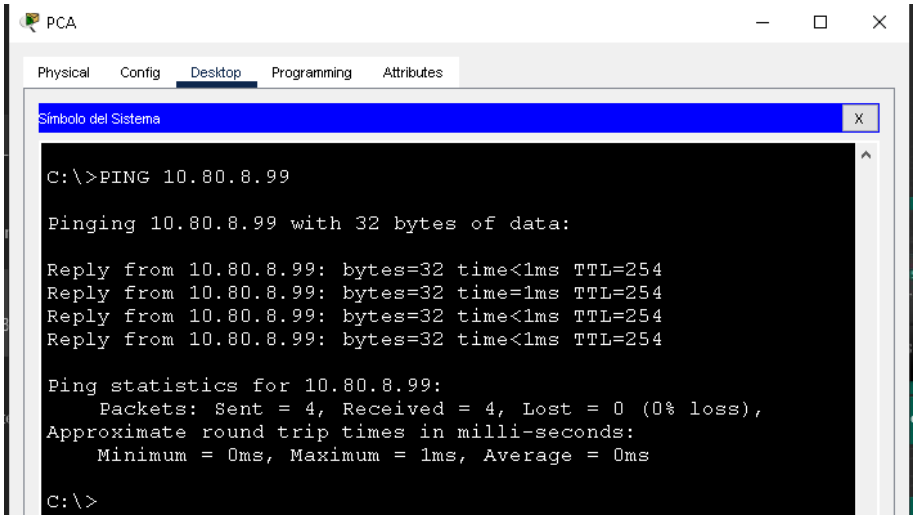


Fuente: Elaboración proia

Se puede evidenciar que hay Conectividad entre la interface loopback y el pc- A, lo cual le permite al Router tener una interface virtual.

- **Ping PC-A - S1, VLAN40– IPV4 e IPV6**

Figura 13 Ping PC-A - S1, VLAN40– IPV4 e IPV6

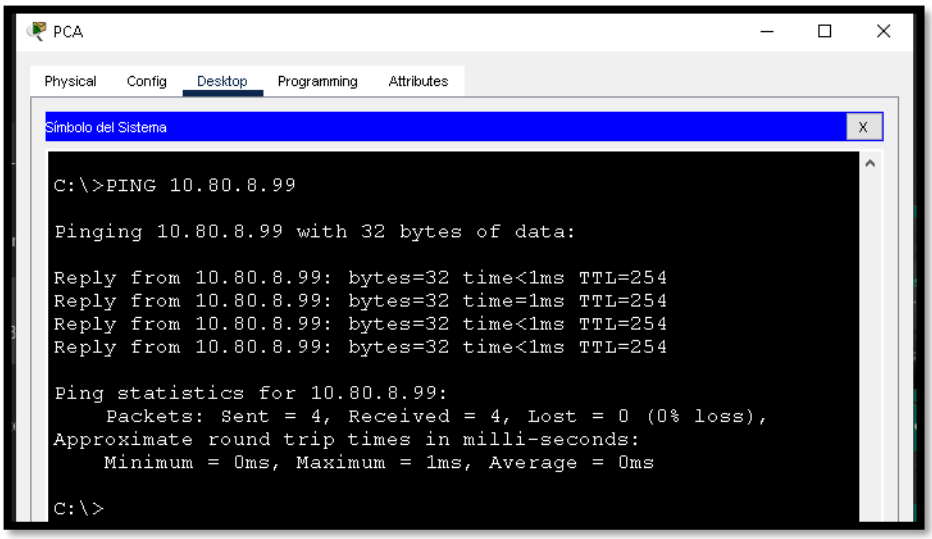


Fuente: Elaboración propia

Se puede evidenciar que hay Conectividad entre entre la interface de administración de los sw mediante la ipv4 , la ipv6 no se logra alcanzar por motivos de desactualización del ios en el software packet Tracert.

- **Ping PC-A – S2, VLAN40– IPV6**

Figura 14 Ping PC-A – S2, VLAN40– IPV6

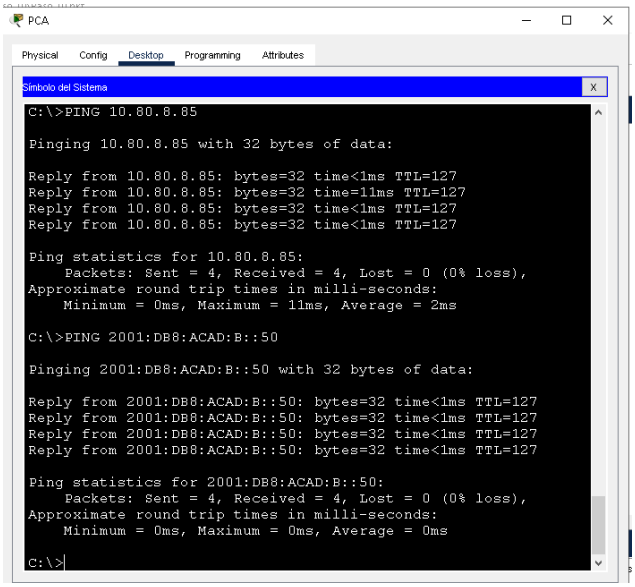


Fuente: Elaboración propia

Se puede evidenciar que hay Conectividad entre entre la interface de administración de los sw mediante la ipv4 , la ipv6 no se logra alcanzar por motivos de desactualización del ios en el software packet Tracert.

- **Ping PC-A – PC-B– IPV4 e IPV6**

Figura 15 Ping PC-A – PC-B– IPV4 e IPV6

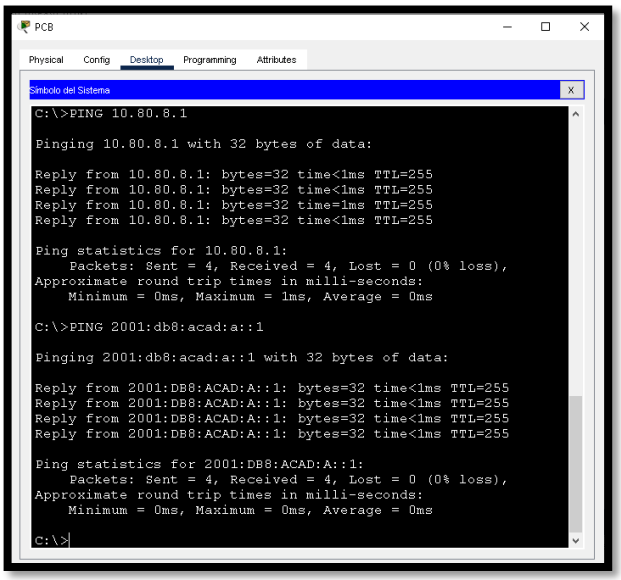


Fuente: Elaboración propia

Se puede evidenciar que hay Conectividad entre entre las vlas 20 y 30 .

- **Ping PC-B - R1, G0/0/1.20 – IPV4 e IPV6**

Figura 15 Ping PC-B - R1, G0/0/1.20 – IPV4 e IPV6

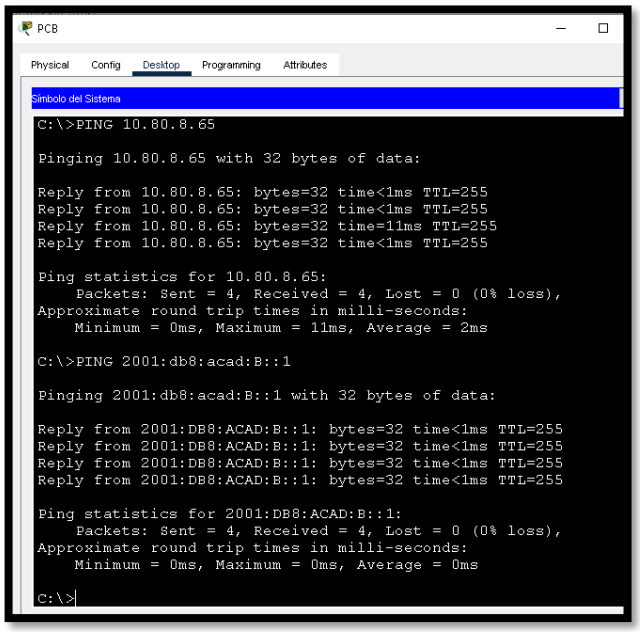


Fuente: Elaboración propia

Se puede evidenciar que hay Conectividad entre la puertas de enlace que hacen permiten coactividad para los dispositivos de la vlan 20 (Docentes)que se encuentran en la interface del router de las

- **Ping PC-B - R1, G0/0/1.30 – IPV4 e IPV6**

Figura 17 Ping PC-B - R1, G0/0/1.30 – IPV4 e IPV6

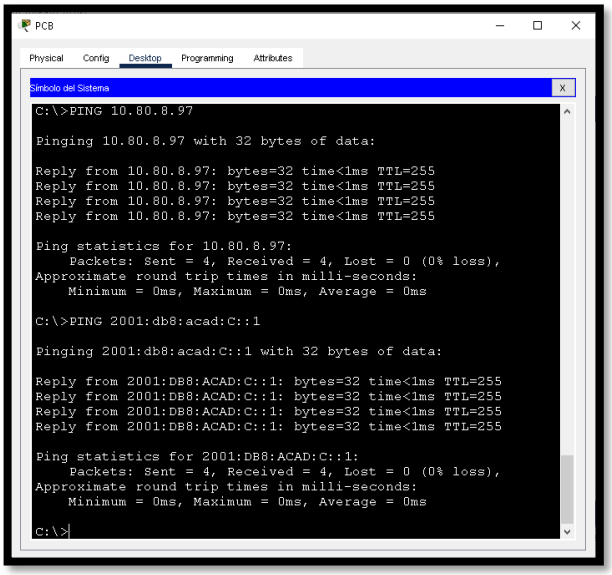


Fuente: Elaboración propia

Se puede evidenciar que hay Conectividad entre la puertas de enlace que hacen permiten coactividad para los dispositivos de la vlan 30 (Estuadiantes)que se encuentran en la interface del router de las

- **Ping PC-B - R1, G0/0/1.40 – IPV4 e IPV6**

Figura 18 Ping PC-B - R1, G0/0/1.40 – IPV4 e IPV6

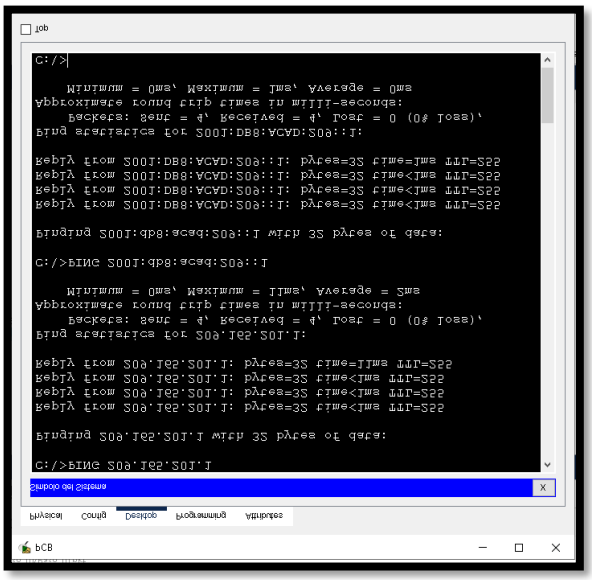


Fuente: Elaboración propia

Se puede evidenciar que hay Conectividad entre la puertas de enlace que hacen permiten coactividad para los dispositivos de la vlan 40 (Invitados)que se encuentran en la interface del router de las

- **Ping PC-B - R1, Loopback– IPV4 e IPV6**

Figura 19 Ping PC-B - R1, Loopback– IPV4 e IPV6

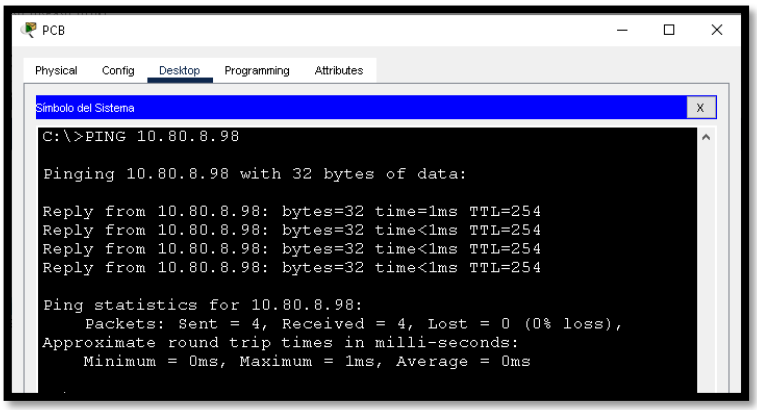


Fuente: Elaboración propia

Se puede evidenciar que hay Conectividad entre la interface loopback y el pc- A, lo cual le permite al Router tener una interface virtual.

- **Ping PC-B – S1, VLAN40 – IPV4 e IPV6**

Figura 20 Ping PC-B – S1, VLAN40 – IPV4 e IPV6

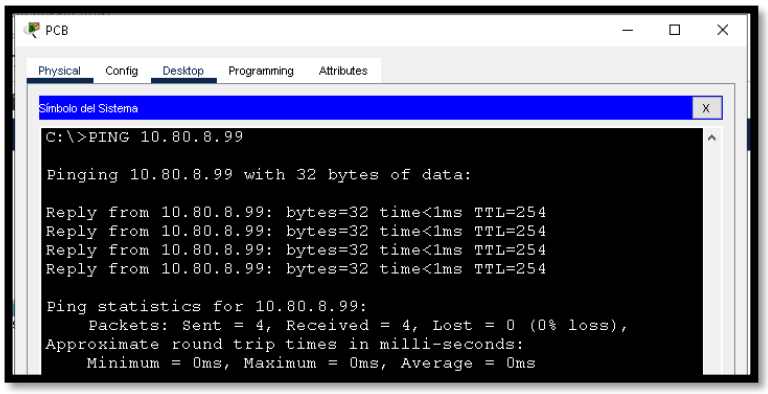


Fuente: Elaboración propia

Se puede evidenciar que hay Conectividad entre entre la interface de administración de los sw mediante la ipv4 , la ipv6 no se logra alcanzar por motivos de desactualización del ios en el software packet Tracert.

- **Ping PC-B – S2,VLAN40 – IPV4 e IPV6**

Figura 21 Ping PC-B -S2,VLAN40 -IPV4 IPV6



Fuente: Elaboración propia

Se puede evidenciar que hay Conectividad entre entre la interface de administración de los sw mediante la ipv4 , la ipv6 no se logra alcanzar por motivos de desactualización del ios en el software packet Tracert.

Tabla 15. Probar y verificar la conectividad de extremo a extremo

Desde	A		Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.20	IPv4	10.80.8.1	Exitoso
		IPv6	2001:db8:acad:a: :1 /64	Exitoso
	R1, G0/0/1.30	IPv4	10.80.8.65	Exitoso
		IPv6	2001:db8:acad:b::1/64	Exitoso
	R1, G0/0/1.40	IPv4	10.80.8.97	Exitoso
		IPv6	2001:db8:acad:c::1/64	Exitoso
	S1, VLAN 40	IPv4	2001:db8:acad:c: :98 /64	No aplica
		IPv6	2001:db8:acad:c: :98 /64	No aplica
	S2, VLAN 40	IPv4	10.80.8.99	No aplica
		IPv6	2001:db8:acad:c: :98 /64	No aplica
	PC-B	IPv4	10.80.8.84	Exitoso
		IPv6	2001:DB8:ACAD:B::50	Exitoso
	R1 Bucle 0	IPv4	209.165.201.1	Exitoso
		IPv6	2001:db8:acad:209: :1 /64	Exitoso
PC-B	R1 Bucle 0	IPv4	209.165.201.1	Exitoso
		IPv6	2001:db8:acad:209: :1 /64	Exitoso
	R1, G0/0/1.20	IPv4	10.80.8.1	Exitoso
		IPv6	2001:db8:acad:a: :1 /64	Exitoso
	R1, G0/0/1.30	IPv4	10.80.8.65	Exitoso
		IPv6	2001:db8:acad:b::1/64	Exitoso
	R1, G0/0/1.40	IPv4	10.80.8.97	Exitoso
		IPv6	2001:db8:acad:c::1/64	Exitoso

	S1, VLAN 40	IPv4	10.80.8.98	Exitoso
		IPv6	2001:db8:acad:c: :98 /64	Exitoso
	S2, VLAN 40	IPv4	10.80.8.99	Exitoso
		IPv6	2001:DB8:ACAD:C: :99 /64	Exitoso

Fuente: Prueba de habilidades diplomado CCNA.

CONCLUSIONES

Comprendiendo y aplicando de manera optima las configuraciones en los dos escenarios propuestos , se ejecutaron de manera exitosa todos las simulaciones y el desarrollo de los solicitado ,se tuvo en cuenta todas las normativas y configuración vistas , las cuales nos permitieron tener una mejor comprensión y un nivel de claridad mas alto de las redes de datos en tecnología cisco.

Se aprendió a ejecutar las técnicas de configuraciones respecto a los protocolos establecidos en cada dispositivo , partiendo particularmente con la seguridad de los dispositivos , se procedió a realizar la configuración de un usuario y contraseña local , la cual se deberá ingresar al momento de acceder a cualquier Switch o Router , a su ves se permitió la opción de que se permita conectar a e ellos mediante el protocolo SSH , habilitando la líneas vty.

Logramos la optimización y control del trafico de las redes locales mediante las configuración en los switches mediante Vlans , las cuales son asignadas a las interfaces establecidas.

Se establecieron políticas de seguridad en las interfaces de los Switchs , determinando de manera correcta el numero de conexiones que se permitirán en ellas , e inhabilitando las que no se usaran.

Por ultimo logramos en cada escenario realizar la conectividad de manera satisfactoria de los dispositivos asociados en las diferentes subredes , aplicando no solo el protocolo ipv4 , si no también el ipv6 , esto se comprobó con el comando ping en cada dispositivo Final.

BIBLIOGRAFIA

Castaño, R. R. J., y López, F. J. (2013). *Redes locales.* Madrid, ES: Macmillan Iberia, S.A. (pp. 214 - 227). https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43257?page=215

Castaño, R. R. J., y López, F. J. (2013). *Redes locales.* Madrid, ES: Macmillan Iberia, S.A. (pp. 232 - 247).

Cobos, A. (16 de octubre de 2017). ¿Qué es la Certificación Cisco CCNA y cuáles son sus ventajas? openwebinars. https://openwebinars.net/blog/que-es-la-certificacion-cisco-ccna-y-cuales-son-sus-ventajas/

DIRECCIONAMIENTO Y subredes TCP/IP - Windows Client [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. [Consultado el 20, octubre, 2022]. Disponible en Internet: <https://learn.microsoft.com/es-es/troubleshoot/windows-client/networking/tcpip-addressing-and-subnetting>.

González, M. (8 de noviembre de 2013). *El switch: cómo funciona y sus principales características | Redes Telemáticas*. Redes telemáticas. https://redestelematicas.com/el-switch-como-funciona-y-sus-principales-caracteristicas/

Terol, M. (13 de septiembre de 2022). *Gateway: ¿por qué debes conocer su funcionalidad?* Blogthinkbig.com. https://blogthinkbig.com/gateway-por-que-debes-conocer-su-funcionalidad

ANEXOS

ANEXO A. Descarga de archivo de simulación de escenario 1

https://drive.google.com/file/d/1fefGGY8eC5kZvY0eyhVzuwHnlCmEtSmT/view?usp=sharing

ANEXO B. Descarga de archivo de simulación de escenario 2

https://drive.google.com/file/d/1u63NlmWMQ3kbWbeejP10DK6cUJQa5hc1/view?usp=sharing