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

ANTONY JHAN PIERE MARIN QUIJANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA EN INGENIERÍA – ECBTI

INGENIERÍA DE SISTEMAS

SANTIAGO DE CALI

2022

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

ANTONY JHAN PIERE MARIN QUIJANO

Diplomado como opción de grado para optar el título de Ingeniero de Sistemas.

PAULITA FLOR SALAZAR

Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA EN INGENIERÍA – ECBTI

INGENIERÍA DE SISTEMAS

SANTIAGO DE CALI

2022

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Santiago de Cali, 27 de Noviembre de 2022.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

BYTE: El byte es la unidad de información estándar utilizada en informática y en telecomunicaciones. Un byte equivale a un conjunto ordenado de 8 bits.[1]

CISCO: Cisco es una empresa de origen estadounidense fabricante de dispositivos para redes locales y externa, también presta el servicio de soluciones de red, su objetivo es conectar a todos y demostrar las cosas asombrosas que se pueden lograr con una visión clara del futuro.[2]

DNS: Es el acrónimo para “Domain Name System” (sistema de nombre de dominio) servicio que habilita un enlace entre nombres de dominio y direcciones IP con la que están asociados.[3]

INTERNET: Internet es una red de computadoras interconectadas a nivel mundial en forma de tela de araña. Consiste en servidores (o "nodos") que proveen información a aproximadamente 100 millones de personas que están conectadas entre ellas a través de las redes de telefonía y cable.[4]

PROTOCOLO: Conjunto de reglas que se establecen en el proceso de comunicación entre dos sistemas.[5]

RED: interconexión de un número determinado de computadores (o de redes, a su vez) mediante dispositivos alámbricos o inalámbricos que, mediante impulsos eléctricos, ondas electromagnéticas u otros medios físicos, les permiten enviar y recibir información en paquetes de datos, compartir sus recursos y actuar como un conjunto organizado.[6]

ROUTER: recibe y envía datos en redes informáticas. Los ROUTERS a veces se confunden con los concentradores de red, los módems o los SWITCH de red. No obstante, los ROUTERS pueden combinar las funciones de estos componentes y conectarse con estos componentes para mejorar el acceso a Internet o ayudar a crear redes empresariales.[7]

---

[1] JVS Informática. ¿Qué es un Byte?.(2020)
[2] NETEC, Expertos enseñando a expertos. ¿Qué es CISCO? (2021)
[3] AT INTERNET. Glosario DNS. (2022)
[4] RAMIREZ, Helena. ¿Qué es internet? (1999)
[5] REAL ACADEMIA ESPAÑOLA. Protocolo. (2021)
[6] CONCEPTO.de. ¿Qué es una red? (2021)
[7] CISCO. ¿Qué es un ROUTER? (2022)

SERVIDOR: tiene dos significados en el ámbito informático. El primero hace referencia al ordenador que pone recursos a disposición a través de una red, y el segundo se refiere al programa que funciona en dicho ordenador.[8]

SWITCH: son los encargados de la interconexión de equipos dentro de una misma red, o lo que es lo mismo, son los dispositivos que, junto al cableado, constituyen las redes de área local o LAN.[9]

VTY: Línea de Terminal Virtual, los puertos VTY están enumerados del 0 al 15 y son utilizados para establecer sesiones Telnet. El comando para utilizar es line VTY 0 15 así como los subcomandos PASSWORD y LOGIN.[10]

WEB: World Wide Web, o simplemente Web, es el universo de información accesible a través de Internet, una fuente inagotable del conocimiento humano. El componente más usado en el Internet es definitivamente el Web. Su característica sobresaliente es el texto remarcado, un método para referencias cruzadas instantáneas. En la mayoría de los Sitios Web, ciertas palabras aparecen en texto de otro color diferente al resto del documento. Por lo general, este texto es subrayado. Al seleccionar una palabra o frase, uno es transferido al sitio o página relacionado a esa frase.[11]

[8] IONOS, Digital Guide. ¿Qué es un servidor? (2020)
[9] GONZALEZ. El SWITCH: ¿Cómo funciona y sus principales características? (2013)
[10] UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO. Configurando un acceso administrativo seguro. (2010)
[11] MILENIUM. Web. (2022)

RESUMEN

En el presente documento encontraremos el desarrollo de dos escenarios en los cuales se configuran diferentes tipos de redes; se da solución al primer escenario propuesto el cual corresponde a la configuración completa de una red pequeña construida con un ROUTER, un SWITCH y dos equipos de cómputo; para iniciar personalizamos los nombres de nuestros equipos para que sea mucho más fácil identificarlos y realizar la configuración, luego diseñamos el esquema de direccionamiento IPv4 en esta caso para LAN1 y LAN2 en nuestro ROUTER y SWITCH, por último configuramos nuestros hosts disponibles (PC-A y PC-B) con el direccionamiento asignado y pasamos a verificar conectividad entre ellos haciendo ping lo cual debe resultar exitoso. El escenario número dos corresponde a la configuración de una red construida con un ROUTER, dos SWITCH y dos equipos de cómputo, como debemos hacer siempre antes de iniciar a configurar nuestra red asignamos los nombres personalizados a cada uno de los equipos para tener una configuración más ordenada y clara, cuando tengamos esto pasamos a diseñar nuestro esquema de direccionamiento el cual debe ser para el segundo escenario en IPv4 e IPv6; para asegurarnos de que nuestros enlaces cuenten con una seguridad alta debemos utilizar el enrutamiento PORT-SECURITY junto con grupos ETHERCHANNEL y DHCP, por último configuramos los equipos de cómputo (PC-A y PC-B) para que obtengan su IPv4 por medio de DHCP y la IPv6 sea estática; rectificamos que todos los equipos que conforman nuestra red están interconectados correctamente por medio de pings, los cuales deben resultar exitosos.

Palabras clave: CISCO, CCNA, CONMUTACIÓN, ENRUTAMIENTO, REDES, ELECTRÓNICA, ROUTER, SWITCH, LAN, IPV4.

ABSTRACT

In this document we will find the development of two scenarios in which different types of networks are configured; a solution is given to the first proposed scenario which corresponds to the complete configuration of a small network built with a ROUTER, a SWITCH and two computers; to start we customize the names of our computers to make it much easier to identify them and perform the configuration, then we design the IPv4 addressing scheme in this case for LAN1 and LAN2 in our ROUTER and SWITCH, finally we configure our available hosts (PC-A and PC-B) with the assigned addressing and we verify connectivity between them by pinging which should be successful. Scenario number two corresponds to the configuration of a network built with a ROUTER, two SWITCH and two computers, as we must always do before starting to configure our network we assign custom names to each of the computers to have a more orderly and clear configuration, when we have this we go to design our addressing scheme which should be for the second scenario in IPv4 and IPv6; to ensure that our links have a high security we must use PORT-SECURITY routing along with ETHERCHANNEL and DHCP groups, finally we configure the computers (PC-A and PC-B) to obtain their IPv4 through DHCP and IPv6 is static; we rectify that all the computers that make up our network are properly interconnected through pings, which must be successful.

Keywords: CISCO, CCNA, SWITCHING, ROUTING, NETWORKING, ELECTRONICS, ROUTER, SWITCH, LAN, IPV4.

INTRODUCCIÓN

Con el desarrollo de este documento se sustenta lo aprendido en el diplomado de profundización; se logra realizar la configuración completa de redes locales y corporativas simuladas; con la finalización de este trabajo se puede decir que se tiene el conocimiento para afrontar casos de la vida real en donde haya que desarrollar redes básicas según la necesidad garantizando una excelente seguridad y efectividad al momento de realizar optimizaciones o mantenimiento en ellas.

En el primer escenario propuesto se construye una red pequeña la cual simula un escenario local, en ella se debe configurar un direccionamiento IPv4 para lograr la correcta comunicación entre todos los equipos de la red, adicional a esto cabe mencionar que se realiza la configuración en un nivel básico al ROUTER y SWITCH.

En el segundo escenario se crea una red que simula un escenario más corporativo, con mucha más seguridad en comparación con el primer escenario, uno de los cambios más notorios entre una y otra es que se debe utilizar enrutamiento en IPv6, hacer uso de grupos DHCP y EtherChannel junto con el comando Port-security para asegurar un nivel alto de confidencialidad; con el desarrollo de este segundo escenario se puede afirmar que se cumple con el objetivo de interconectar dos lugares que están alejados.

DESARROLLO DEL TRABAJO.

Escenario 1.

Escenario: En este primer escenario se configurará una simulación de red LAN pequeña, está construida con un ROUTER, un SWITCH y 2 equipos de cómputo, se desarrollará también el esquema de direccionamiento IPv4 para cada una de las LAN.

Figura 1. Escenario 1.

Fuente: Prueba de habilidades práctica CCNA 2022.

Objetivos:

-Parte 1: Armar la red en Packer Tracer como lo indica la figura 1.

-Parte 2: Llenar la tabla 1 con las direcciones IP correspondientes.

-Parte 3: Realizar configuración básica a los equipos que componen la red.

-Parte 4: Asegurar la buena configuración de la seguridad en R1 y S1.

-Parte 5: Realizar la configuración en PC-A y PC-B para terminar realizando ping entre los equipos y confirmar su conectividad.

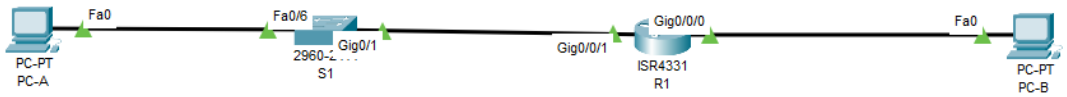
Aspectos básicos/situación:

En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el ROUTER R1 y el SWICH S1, y los PCs. Con la dirección suministrada realizará el SUBNETTING y cumplirá el requerimiento para la LAN1 (60 host) y la LAN2 (20 hosts).

Parte 1: Construya la Red:

En Packet Tracer se crea la red tal cual lo indica la Figura 1.

Figura 2.Simulación de escenario 1.



Fuente: Autoría propia.

Parte 2: Desarrolle el esquema de direccionamiento IP:

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. Cada estudiante tomará el direccionamiento 192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula.

Tabla 1. Tabla de direccionamiento escenario 1

ITEM	REQUERIMIENTO	SOLUCIÓN
Dirección de Red	172.XY.3.0 donde XY corresponde a los últimos dos dígitos de su cédula.	172.80.3.0
Requerimiento de host Subred LAN1	60	172.80.3.0/26
Requerimiento de host Subred LAN2	20	172.80.3.0/27
R1 G0/0/1	Última dirección de host de la subred LAN1	172.80.3.62/26
R1 G0/0/0	Última dirección de host de la subred LAN2	172.80.3.94/27
S1 SVI	Segunda dirección de host de la subred LAN1	172.80.3.2/26
PC-A	Décima dirección de host de la subred LAN1	172.80.3.10/26
PC-B	Décima dirección de host de la subred LAN2	172.80.3.74/27

Fuente: Autoría propia.

Parte 3: Configure aspectos básicos:

Para lograr configurar los dispositivos S1 y R1 se ingresa por medio de consola a realizar la configuración básica.

1.3.1- Las tareas de configuración para R1 incluyen las siguientes:

Tabla 2. Comandos para configuración del ROUTER R1 por consola.

TAREA	EXPLICACIÓN	COMANDO
Desactivar la búsqueda DNS	Se desactiva la búsqueda DNS para evitar demoras al ingresar comandos de configuración.	R1(config)#no ip domain-lookup
Cambiar nombre del ROUTER: **R1**	Suministramos el nombre del ROUTER personalizado el cual seguiremos usando para seguir con nuestra configuración.	Router>enable Router#configure terminal Router(config)#hostname R1 R1(config)#
Cambiar nombre de Dominio: **ccna-sa.com**	Asignamos el nombre de dominio al ROUTER.	R1#configure terminal R1(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado: **ciscoenpass**	Se asigna una contraseña para poder acceder a la configuración del ROUTER en modo privilegiado.	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola: **ciscoconpass**	Se asigna una contraseña para poder acceder a la configuración del ROUTER por medio de consola.	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas: **10 caracteres**	Configuramos que solo acepte contraseñas con mínimo 10 caracteres.	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local: Nombre de usuario: **admin** Contraseña: **admin1pass**	Se crea el usuario y la contraseña del usuario que va a tener acceso a la base de datos local.	R1(config)#username admin password admin1pass

Configure el inicio de sesión en las líneas VTY para que use la base de datos local	Debemos subir las líneas 0 15 para que estas puedan usar la base de datos local.	R1(config)#line vty 0 15 R1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Se debe aceptar únicamente SSH para garantizar la NO pérdida de paquetes y la seguridad de estos.	R1(config-line)#transport input SSH
Cifrar las contraseñas de texto no cifrado	Aumentamos la seguridad de contraseñas cifrándolas.	R1(config)#service password-encryption
Configurar un banner MOTD: Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.	Establecemos el mensaje que va a aparecer cuando una persona no esté autorizada para ingresar a la configuración.	R1(config)#banner motd "R1, Antony Jhan Piere Marin Quijano Ingenieria de sistemas"
Configuración de interface G0/0/0 Establecer la descripción Establecer la dirección IPv4 Activar la interfaz.	Le asignamos una IP y una máscara de subred a nuestro primer puerto Giga del ROUTER.	R1(config-if)#ip address 172.80.3.94 255.255.255.192 R1(config-if)#description Interfaz LAN1 R1(config-if)#no shutdown
Configuración de interface G0/0/1 Establecer la descripción Establecer la dirección IPv4 Activar la interfaz.	Le asignamos una IP y una máscara de subred a nuestro primer puerto Giga del ROUTER.	R1(config-if)#exit R1(config)#int gigabitEthernet 0/0/1 R1(config-if)#ip address 172.80.3.62 255.255.255.192 R1(config-if)#description Interfaz LAN1 R1(config-if)#no shutdown

Generar una clave de cifrado RSA: Módulo de 1024 bits	El RSA es un sistema de encriptación, es el más recomendado por su seguridad, y los 1024 bits son la longitud de la clave encriptada.	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]

Fuente: Autoría propia.

1.3.2- Se realizan las siguientes configuraciones expresadas en la tabla 3 para el S1:

Tabla 3. Comandos para configuración del Switch S1 por consola.

TAREA	EXPLICACIÓN	COMANDO
Desactivar la búsqueda DNS	Se desactiva la búsqueda DNS para evitar demoras al ingresar comandos de configuración.	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch: **S1**	Suministramos el nombre del SWITCH personalizado el cual seguiremos usando para seguir con nuestra configuración.	Switch#configure terminal Switch(config)#hostname S1
Nombre de dominio: **ccna-sa.com**	Asignamos el nombre de dominio al SWITCH.	S1(config)#ip domain-name ccna-sa.com

Contraseña cifrada para el modo EXEC privilegiado: **ciscoenpass**	Se asigna una contraseña para poder acceder a la configuración del SWITCH en modo privilegiado.	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola: **ciscoconpass**	Se asigna una contraseña para poder acceder a la configuración del SWITCH por medio de consola.	S1#configure terminal S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit
Apagar todos los puertos sin usar: F0/1-4, F0/7-24, G0/1-2	Se apagan todos los puertos no usados, en esta parte del ejercicio por error se apagan todos los puertos y toca volver a encender los que se usan para la conexión al PC y al Router.	S1(config)#interface range f0/1-4,f0/7-24,g0/1-2 S1(config-if-range)#shutdown
Crear un usuario administrativo en la base de datos local: Nombre de usuario: **admin** Contraseña: **admin1pass**	Se crea el usuario y la contraseña del usuario que va a tener acceso a la base de datos local.	S1(config)#username admin password admin1pass
Configure el inicio de sesión en las líneas VTY para que use la base de datos local.	Debemos subir las líneas 0 15 para que estas puedan usar la base de datos local.	S1(config)#line vty 0 15 S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Se debe aceptar únicamente SSH para garantizar la NO pérdida de paquetes y la seguridad de estos.	S1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	Aumentamos la seguridad de contraseñas cifrándolas.	S1(config-line)#transport input ssh

Configurar un banner MOTD: Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.	Establecemos el mensaje que va a aparecer cuando una persona no esté autorizada para ingresar a la configuración.	S1(config)#banner motd "S1, Antony Jhan Piere Marin Quijano Ingenieria de sistemas"
Generar una clave de cifrado RSA: Módulo de 1024 bits	El RSA es un sistema de encriptación, es el más recomendado por su seguridad, y los 1024 bits son la longitud de la clave encriptada.	S1(config)#crypto key generate rsa The name for the keys will be: S1.ccna-sa.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Configure la interfaz de administración (SVI) en VLAN1: Establecer la descripción Establecer la dirección IPv4	Le asignamos una IP y una máscara de subred a nuestro primer puerto Giga del SWITCH.	S1(config)#int vlan 1 S1(config-if)#ip address 172.80.3.2 255.255.255.128 S1(config-if)#description Interfaz VLAN1

Fuente: Autoría propia.

Paso 2. Configurar los equipos:

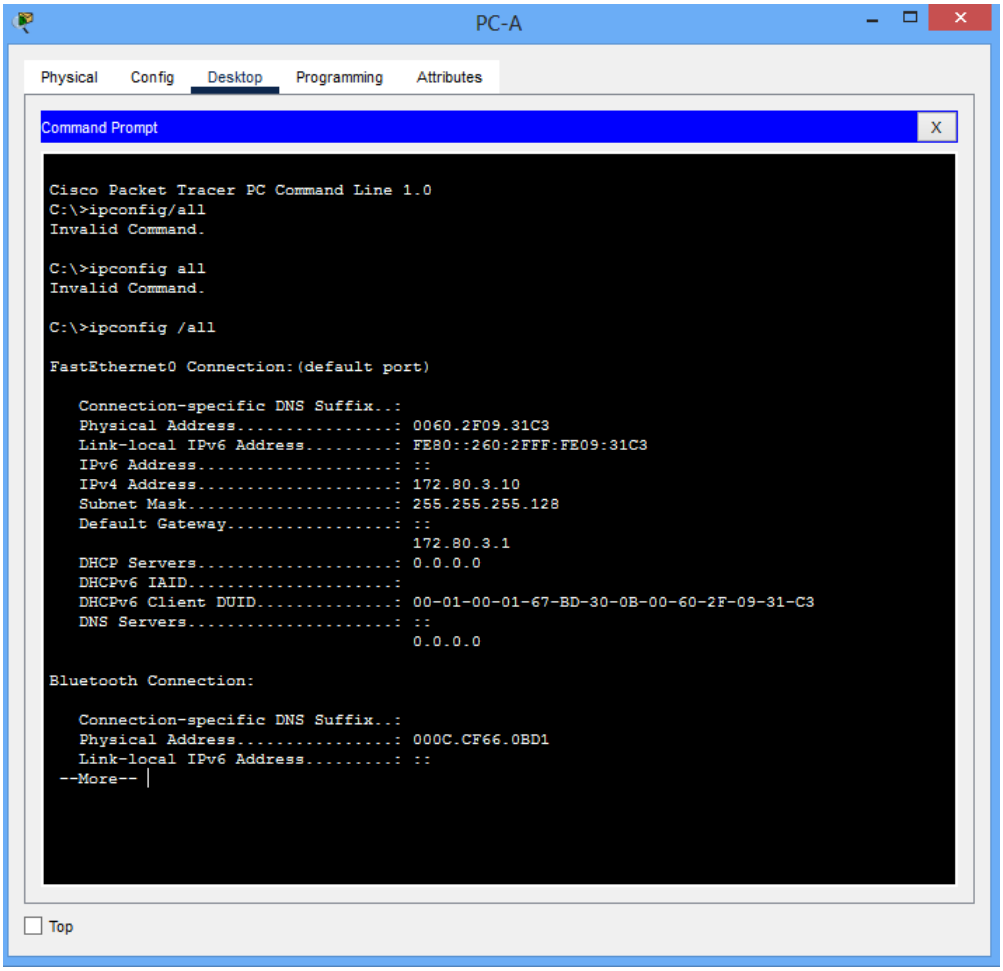
Se configuran los equipos PC-A y PC-B de acuerdo a lo estipulado en la tabla 1. Se utiliza el comando ipconfig /all para cnfirmar que estén bien configurados los equipos.

Tabla 4. Configuración de red PC-A.

Configuración de red de PC-A	
Descripción	
Dirección física	
Dirección IPv4	172.80.3.10/26
Máscara de subred	255.255.255.128
Puerta de enlace IPv4 predeterminada	172.80.3.1

Fuente: Autoría propia.

Figura 3. Evidencia de la configuración PC-A.



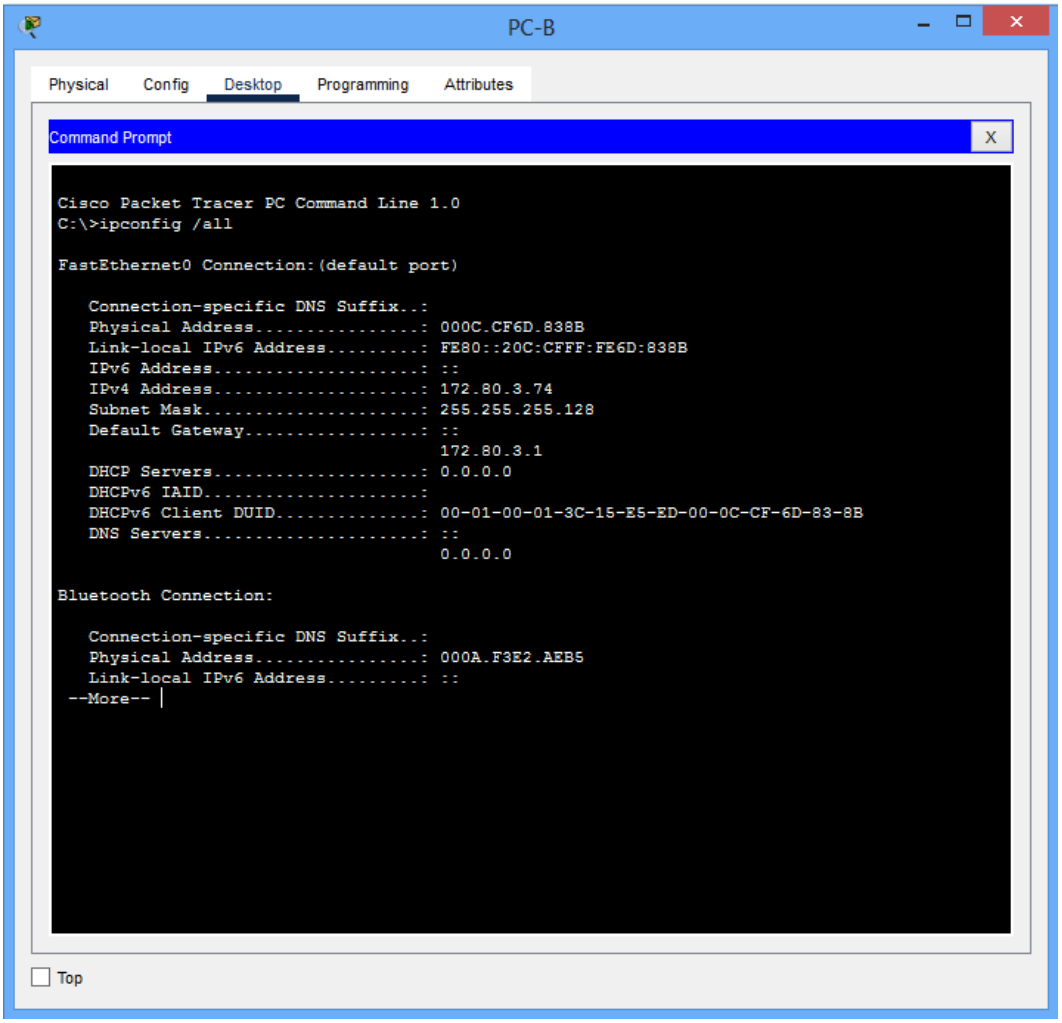
Fuente: Autoría propia.

Tabla 5. Configuración de red PC-B.

Configuración de red de PC-B	
Descripción	
Dirección física	
Dirección IPv4	172.80.3.74/27
Máscara de subred	255.255.255.128
Puerta de enlace IPv4 predeterminada	172.80.3.1

Fuente: Autoría propia.

Figura 4. Evidencia de la configuración PC-B.

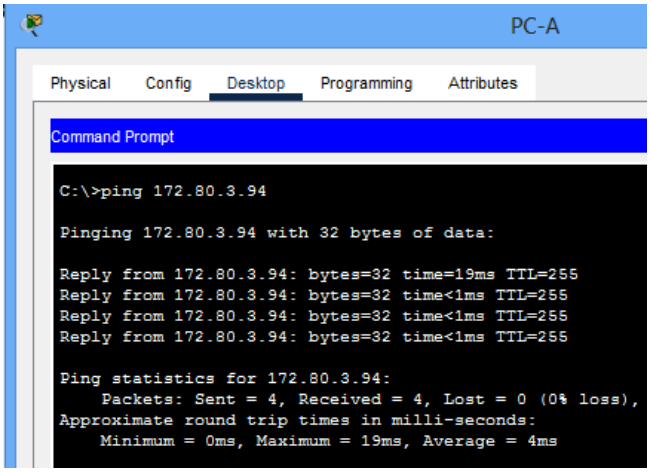
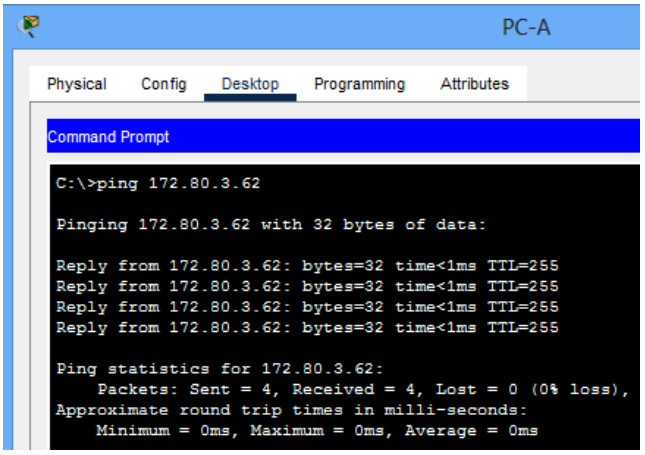


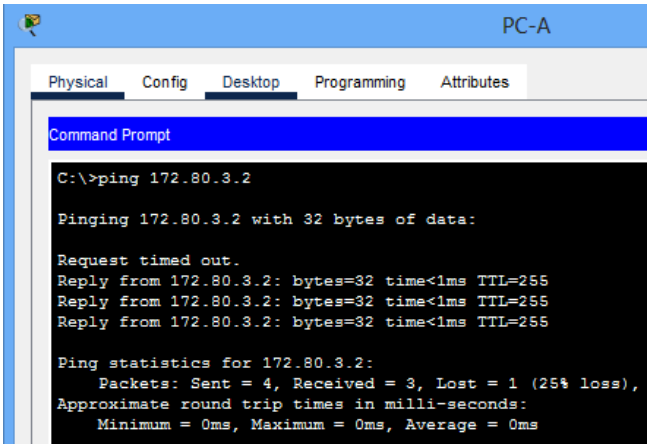
Fuente: Autoría propia.

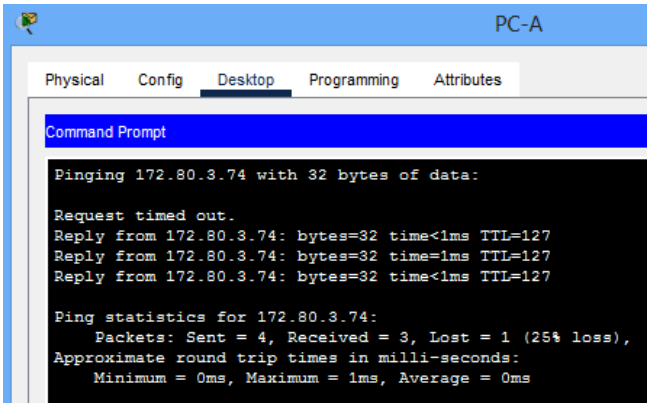
Parte 4. Probar y verificar la conectividad de extremo a extremo:

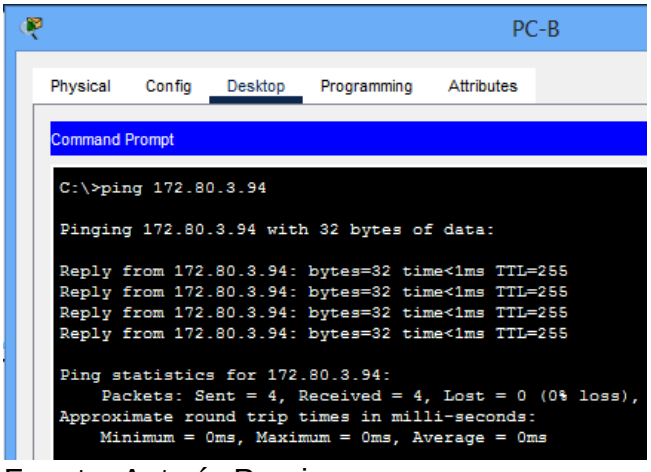
Se realiza un ping entre cada uno de los equipos que conforman la red para verificar su buen funcionamiento.
Se utiliza la Tabla 6 para ir evidenciando mediante capturas de pantalla la conectividad exitosa de cada uno de los equipos que componen la red.

Tabla 6. Conectividad entre dispositivos de red.

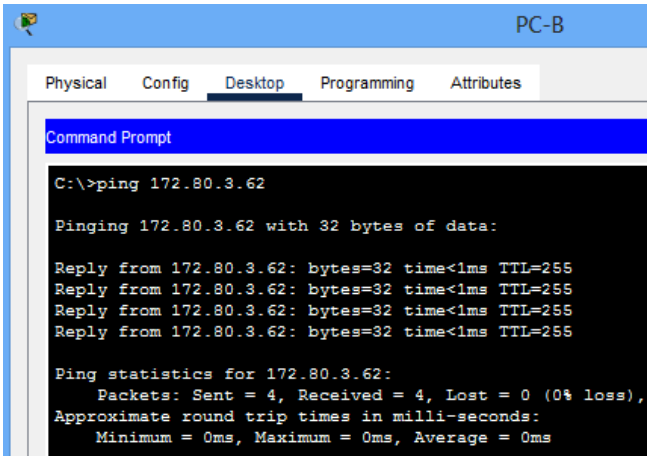
DESDE	A	DIRECCIÓN IP	RESULTADO PING
PC-A	R1 G0/0/0	172.80.3.94/27	Figura 5. Ping PC-A / R1 G0/0/0.  Fuente: Autoría Propia.
	R1 G0/0/1	172.80.3.62/26	Figura 6. Ping PC-A / R1 G0/0/1.  Fuente: Autoría Propia.

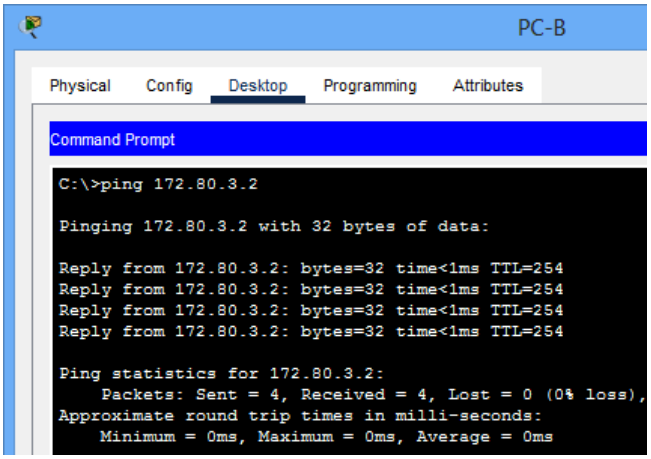
<table>
<tr><td rowspan="2">PC-A</td><td>S1 VLAN 1</td><td>172.80.3.2/26</td><td>Figura 7. Ping PC-A / S1 VLAN 1.
 

Fuente: Autoría Propia.</td></tr>
<tr><td>PC-B</td><td>172.80.3.74/27</td><td>Figura 8. Ping PC-A / PC-B.
 

Fuente: Autoría Propia.</td></tr>
<tr><td>PC-B</td><td>R1 G0/0/0</td><td>172.80.3.94/27</td><td>Figura 9. Ping PC-B / R1 G0/0/0.
 

Fuente: Autoría Propia.</td></tr>
</table>

<table>
<tr><td rowspan="2">PC-B</td><td>R1
G0/0/1</td><td>172.80.3.62/26</td><td>Figura 10. Ping PC-B / R1 G0/0/1.
 

Fuente: Autoría Propia.</td></tr>
<tr><td>S1
VLAN1</td><td>172.80.3.2/26</td><td>Figura 11. Ping PC-B / S1 VLAN1.
 

Fuente: Autoría Propia.</td></tr>
</table>

Fuente: Autoría propia.

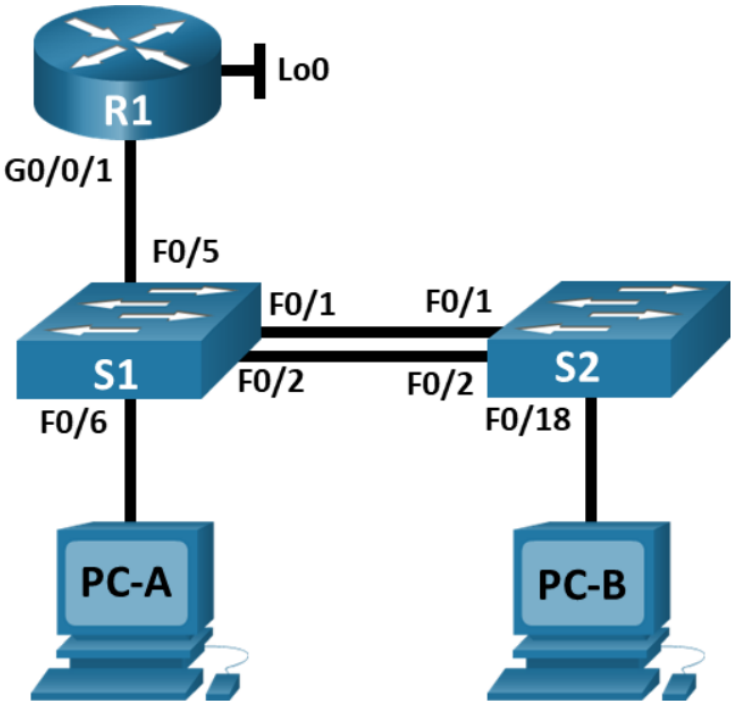
CONCLUSION ESCENARIO 1.

Se crea y configura una red muy básica con IPv4, el objetivo principal es lograr que se puedan comunicar entre todos los dispositivos que conforman la red, para que dicha conexión sea exitosa debemos configurar un dominio que va a funcionar como canal para la interconexión, todos los equipos deben tener una dirección IP o nombre con el cual van a acceder al dominio y van a poder ver los demás dispositivos que también ingresaron a dicha red con un nombre y las credenciales del dominio.

Escenario 2.

Escenario: Para este segundo escenario tenemos un caso el cual simula una red de tipo corporativo, contiene un ROUTER, dos SWITCHS y dos equipos de cómputo, estos deben funcionar con IPv4 e IPv6, la novedad es que utilizaremos enrutamientos entre VLAN, DHCP, ETHERCHANNEL y PORT-SECURITY.

Figura 12. Escenario 2.



Fuente: Prueba de habilidades práctica CCNA 2022

Tabla 7. Tabla de VLAN escenario 2.

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

Fuente: Prueba de habilidades práctica CCNA 2022.

Tabla 8. Tabla de asignación de direcciones escenario 2.

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.20	10.80.8.1 /26 2001:db8:acad:a: :1/64	No corresponde No corresponde
R1 G0/0/1.30	10.80.8.65 /27 2001:db8:acad:b: :1/64	No corresponde No corresponde
R1 G0/0/1.40	10.80.8.97 /29 2001:db8:acad:c: :1/64	No corresponde No corresponde
R1 G0/0/1.56	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27 2001:db8:acad:209: :1/64	No corresponde No corresponde
S1 VLAN 4	10.80.8.98 /29 2001:db8:acad:c: :98 /64 fe80: :98	10.80.8.97 No corresponde No corresponde
S2 VLAN 4	10.80.8.99 /29 2001:db8:acad:c: :99 /64 fe80: :99	10.80.8.97 No corresponde No corresponde
PC-A NIC	Dirección DHCP para IPv4 2001:db8:acad:a: :50 /64	DHCP para puerta de enlace predeterminada IPv4 fe80::1
PC-B NIC	DHCP para dirección IPv4 2001:db8:acad:b: :50 /64	DHCP para puerta de enlace predeterminada IPv4 fe80::1

Fuente: Prueba de habilidades practica CCNA 2022.

Instrucciones.

Paso1: Inicializar y volver a cargar el ROUTER y el SWITCH

• Se borran las configuraciones predeterminadas y VLANS tanto del ROUTER como del SWITCH y los reiniciamos.

Router#enable

Router#erase startup-config

Router#reaload

Switch>enable

Switch#erase startup-config

Switch#reaload

Switch>enable

Switch#erase startup-config

Switch#reaload

• Una vez se hecho el paso anterior debemos configurar la plantilla SDM que nos permitirá trabajar de este punto en adelante con IPV6.

Switch#configure terminal

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

Switch#configure terminal

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

Paso 2: Configurar R1

Las configuraciones que se deben realizar en el R1 se detallan en la Tabla 9:

Tabla 9. Tabla de tareas configuración R1.

TAREA	EXPLICACIÓN	COMANDO
Desactivar la búsqueda DNS	Se desactiva la búsqueda DNS para evitar demoras al ingresar comandos de configuración.	Router#configure terminal Router(config)#no ip domain-lookup
Nombre del ROUTER: R1	Suministramos el nombre del ROUTER personalizado el cual seguiremos usando para seguir con nuestra configuración.	Router#configure terminal Router(config)#hostname R1
Nombre de dominio: ccna-sa.com	Asignamos el nombre de dominio al ROUTER	R1(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC Privilegiado: class	Se asigna una contraseña para poder acceder a la configuración del ROUTER en modo privilegiado.	R1(config)#enable secret class
Contraseña de acceso a la consola: cisco	Se asigna una contraseña para poder acceder a la configuración del ROUTER por medio de consola.	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: 5 caracteres	Configuramos que solo acepte contraseñas con mínimo 5 caracteres.	R1(config)#security passwords min-length 5

Crear un usuario administrativo en lav base de datos local: Nombre de usuario: **admin** Password: **admin1pass**	Se crea el usuario y la contraseña del usuario que va a tener acceso a la base de datos local.	R1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local.	Debemos subir las líneas 0 4 para que estas puedan usar la base de datos local.	R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	Se debe aceptar únicamente SSH para garantizar la NO pérdida de paquetes y la seguridad de estos.	R1(config)#line vty 0 4 R1(config-line)#transport input ssh R1(config-line)#login local R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado.	Aumentamos la seguridad de contraseñas cifrándolas.	R1(config)#service password-encryption
Configure un MOTD Banner: Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.	Establecemos el mensaje que va a aparecer cuando una persona no esté autorizada para ingresar a la configuración.	R1(config)#banner motd "R1, Antony Jhan Piere Marin Quijano, Ingenieria en sistemas"
Habilitar el ROUTING IPv6.	Se habilita para poder configurar IPv6.	R1(config)#ipv6 unicast-routing
	En este paso debemos darle un nombre a cada una de las subredes y utilizar	R1(config)#interface g0/0/1.20 R1(config-subif)#encapsulation dot1Q 20 R1(config-subif)#description Docentes R1(config-subif)#ip address 10.80.8.1 255.255.255.192

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.	la encapsulación dot1Q para el enrutamiento entre las Vlans. En este paso debemos darle un nombre a cada una de las subredes y utilizar la encapsulación dot1Q para el enrutamiento entre las Vlans. En este paso debemos darle un nombre a cada una de las subredes y utilizar la encapsulación dot1Q para el enrutamiento entre las Vlans. En este paso debemos darle un nombre a cada una de las	R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface g0/0/1.30 R1(config-subif)#encapsulation dot1Q 30 R1(config-subif)#description Estudiantes R1(config-subif)#ip address 10.80.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface g0/0/1.40 R1(config-subif)#encapsulation dot1Q 40 R1(config-subif)#ip address 10.80.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#description Invitados R1(config-subif)#no shutdown R1(config-subif)#exit

	subredes y utilizar la encapsulación dot1Q para el enrutamiento entre las Vlans.	R1(config)#interface g0/0/1.56 R1(config-subif)#encapsulation dot1Q 56 R1(config-subif)#description Native R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#int g0/0/1 R1(config-if)#no shutdown
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	Configuramos la interfaz loopback que nos permite proporcionar direcciones IP a routers y switches capa 3.	R1(config)#interface lo0 R1(config-if)#description loopback0 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)#exit
Generar una clave de cifrado RSA: Módulo de 1024 bits.	El RSA es un sistema de encriptación, es el más recomendado por su seguridad, y los 1024 bits son la longitud de la clave encriptada.	R1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Fuente: Autoría propia.

Paso 3: Configure S1 y S2.

Las configuraciones que se deben aplicar al S1 y S2 se detallan en la Tabla 10:

Tabla 10. Tabla de tareas configuración S1 y S2.

TAREA	EXPLICACIÓN	COMANDO
Desactivar la búsqueda DNS	Se desactiva la búsqueda DNS para evitar demoras al ingresar comandos de configuración.	Switch(config)#no ip domain-lookup Switch(config)#no ip domain-lookup
Nombre del SWITCH: S1 o S2, según proceda	Suministramos el nombre de los SWITCHS personalizados los cual seguiremos usando para seguir con nuestra configuración.	Switch(config)#hostname S1 Switch(config)#hostname S2
Nombre de dominio: ccna-sa.com	Asignamos el nombre de dominio a los SWITCHES.	S1(config)#ip domain-name ccna-sa.com S2(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado: class	Se asigna una contraseña para poder acceder a la configuración de los SWITCHS en modo privilegiado.	S1(config)#enable secret class S2(config)#enable secret class
Contraseña de acceso a la consola: cisco	Se asigna una contraseña para poder acceder a la configuración del ROUTER por medio de consola.	S1(config)#line con 0 S1(config-line)# password cisco S1(config-line)#login S1(config-line)#exit S2(config)#line con 0 S2(config-line) #password cisco S2(config-line)#login S2(config-line)#exit

Crear un usuario administrativo en la base de datos local: Nombre de usuario: **admin** Password: **admin1pass**	Se crea el usuario y la contraseña del usuario que va a tener acceso a la base de datos local.	S1(config)#username admin secret admin1pass S2(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local.	Debemos subir las líneas 0 15 para que estas puedan usar la base de datos local.	S1(config)#line vty 0 15 S1(config-line)#login local S1(config-line)#exit 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	Se debe aceptar únicamente SSH para garantizar la NO pérdida de paquetes y la seguridad de estos.	S1(config)#line vty 0 15 S1(config-line)#transport input ssh S1(config-line)#login local S1(config-line)#exit S2(config)#line vty 0 15 S2(config-line)#transport input ssh S2(config-line)#login local S2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	Aumentamos la seguridad de contraseñas cifrándolas.	S1(config)#service password-encryption S2(config)#service password-encryption
Configurar un MOTD Banner: Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa	Establecemos el mensaje que va a aparecer cuando una persona no esté autorizada para ingresar a la configuración.	S1(config)# banner motd “S1, Antony Jhan Piere marin Quijano, Ingenieria de sistemas.” S2(config)#banner motd "S1, Antony Jhan Piere marin Quijano, Ingenieria de sistemas."

académico al que pertenece.		
Generar una clave de cifrado RSA: Módulo de 1024 bits	El RSA es un sistema de encriptación, es el más recomendado por su seguridad, y los 1024 bits son la longitud de la clave encriptada.	S1(config)#crypto key generate rsa S2(config)#crypto key generate rsa
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.	En este paso asignamos las IPv4 e IPv6 correspondientes a cada VLAN.	S1(config)#interface vlan 4 S1(config-if)#ip address 10.80.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#no shutdown S1(config-if)#exit S2(config)#interface vlan 4 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 fe80::99 link-local S2(config-if)#no shutdown S2(config-if)#exit
Configuración del GATEWAY predeterminado: Configure la puerta de enlace predeterminada como 10.80.8.97 para IPv4	Asignamos una puerta de enlace predeterminada al S1 el S2.	S1(config)#ip default-gateway 10.80.8.97 S2(config)#ip default-gateway 10.80.8.97

Fuente: Autoría propia.

Parte 3: Inicializar y recargar y configurar aspectos básicos de los dispositivos Configuración de la infraestructura de red (VLAN, TRUNKING, EtherChannel).

Paso 4: Configurar S1

La configuración a aplicar al S1 se detalla en la Tabla 11:

Tabla 11. Tabla de tareas configuración S1.

TAREA	EXPLICACIÓN	COMANDO
Crear VLAN: VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native	Creamos todas las VLAN solicitadas en el S1 para comenzar a configurar los demás puntos.	S1(config)#vlan 20 S1(config-vlan)#name Docentes S1(config-vlan)#exit S1(config)#vlan 30 S1(config-vlan)#name Estudiantes S1(config-vlan)#exit S1(config)#vlan 40 S1(config-vlan)#name Invitados S1(config-vlan)#exit S1(config)#vlan 50 S1(config-vlan)#name Usuarios S1(config-vlan)#exit S1(config)#vlan 56 S1(config-vlan)#name Native S1(config-vlan)#exit

Crear troncos 802.1Q que utilicen la VLAN 6
Nativa:
Interfaces F0/1, F0/2 y F0/5
	Configuramos los puertos de nuestro S1 modo TRUNK y le decimos que VLAN es la que va a pasar por cada puerto.	S1(config)#interface fa0/1
		S1(config-if)#switchport mode trunk
		S1(config-if)#switchport trunk native vlan 56
		S1(config-if)
		#switchport trunk encapsulation dot1q
		
		S1(config)#interface fa0/2
		S1(config-if)#switchport mode trunk
		S1(config-if)#switchport trunk native vlan 56
		S1(config-if)#switchport trunk encapsulation dot1q
		
		S1(config)#interface fa0/5
		S1(config-if)#switchport mode trunk
		S1(config-if)#switchport trunk native vlan 56
		S1(config-if)#switchport trunk encapsulation dot1q

Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2: Usar el protocolo LACP para la negociación	Creamos un grupo de puertos los cuales vana utilizar la configuración realizada en el paso anterior. Usamos LACP (Link Aggregation Control Protocol) para unir las	S1(config-if)#int range fa0/1-2 S1(config-if-range)#channel-group 2 mode active S1(config-if-range)# Creating a port-channel interface Port-channel 2 S1(config-if-range)#exit S1(config)#interface port-channel 2 S1(config-if)#switchport trunk encapsulation dot1q

	conexiones de red en una virtual y mejorar la velocidad del acceso.	S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 56
Configurar el puerto de acceso de host para VLAN 2: Interface F0/6	Indicamos a nuestro S1 que VLAN va a pasar por el puerto f0/6.	S1(config)#interface fa0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 20 S1(config-if)#no shutdown S1(config-if)#exit
Configurar la seguridad del puerto en los puertos de acceso: Permitir 4 direcciones MAC	En este paso le decimos al S1 que acepte el paso de máximo 4 direcciones MAC diferentes por el puerto f0/6.	S1(config)#interface fa0/6 S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 4
Proteja todas las interfaces no utilizadas: Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar	A todos los puertos que no vamos a utilizar le vamos a asignar la VLAN 50, esto como una forma de seguridad y protección a nuestra red.	S1(config)#interface range fa0/3- 4, fa0/7-24, gi0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#description Puertos sin utilizar S1(config-if-range)#shutdown

Fuente: Autoría propia.

Paso 5: Configurar S2

Las configuraciones que se deben aplicar la S" se detallan en la Tabla 12:

Tabla 12. Tabla de tareas configuración S2.

TAREA	EXPLICACIÓN	COMANDO
Crear VLAN: VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native	Creamos todas las VLAN solicitadas en el S2 para comenzar a configurar los demás puntos.	S2(config)#vlan 20 S2(config-vlan)#name Docentes S2(config-vlan)#exit S2(config)#vlan 30 S2(config-vlan)#name Estudiantes S2(config-vlan)#exit S2(config)#vlan 40 S2(config-vlan)#name Invitados S2(config-vlan)#exit S2(config-vlan)#vlan 50 S2(config-vlan)#name Usuarios S2(config-vlan)#exit S2(config)#vlan 56 S2(config-vlan)#name Native S2(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 Nativa: Interfaces F0/1 y F0/2	Configuramos los puertos de nuestro S2 modo TRUNK y le decimos que VLAN es la que va a pasar por cada puerto.	S2(config)#interface range fa0/1-2 S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport trunk native vlan 56

Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2: Usar el protocolo LACP para la negociación	Creamos un grupo de puertos los cuales van a utilizar la configuración realizada en el paso anterior. Usamos LACP (Link Aggregation Control Protocol) para unir las conexiones de red en una virtual y mejorar la	S2(config)#interface port S2(config)#interface port-channel 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 S2(config)#interface range fa0/1-2 S2(config)#channel-group 2 mode passive S2(config-if-range)#no shutdown
Configurar el puerto de acceso de host para VLAN 3: Interface F0/18	Indicamos a nuestro S2 que VLAN va a pasar por el puerto f0/18.	S2(config)#interface fa0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 30 S2(config-if)#exit
Configure PORT-SECURITY en los ACCESS PORTS: Permitir 4 direcciones MAC	En este paso le decimos al S2 que acepte el paso de máximo 4 direcciones MAC diferentes por el puerto f0/18.	S2(config)#int fa0/18 S2(config-if)#switchport port-security maximum 4 S2(config-if)#switchport port-security S2(config-if)#
Asegure todas las interfaces no utilizadas.: Asignar a VLAN 50,	A todos los puertos que no vamos a utilizar le vamos a asignar la VLAN 50,	S2(config)#interface range fa0/3-17, fa0/19-24, gi0/1-2 S2(config-if-range)#switchport mode access

Establecer en modo de acceso, agregar una descripción y apagar	esto como una forma de seguridad y protección a nuestra red.	S2(config-if-range)#switchport access vlan 50 S2(config-if-range)#description puertos no utilizados S2(config-if-range)#shutdown

Fuente: Autoría propia.

Parte 2: Configurar soporte de host

Paso 1: Configure R1

La configuración que se aplica al R1 se detallan en la Tabla 13:

Tabla 13. Tabla de tareas configuración R1.

TAREA	EXPLICACIÓN	COMANDO
Configure Default Routing:	Creamos las rutas predeterminadas para que la IPv4 e IPv6 dirijan el tráfico a la interfaz Loopback 0	R1(config)#ip route 0.0.0.0 0.0.0.0 lo0
Configurar IPv4 DHCP para VLAN 2: Configurar IPv4 DHCP para VLAN 20	Creamos el grupo DHCP para la VLAN 20, compuesto por las últimas 10 direcciones de la subred solamente. Asignamos el nombre de dominio unad-ccna-sa.net y especificamos la dirección de la puerta de enlace predeterminada como dirección de interfaz del ROUTER para la subred involucrada.	R1(config)#ip dhcp pool vlan20 R1(dhcp-config)#network 10.80.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.80.8.1 R1(dhcp-config)#domain-name unad-ccna-sa.net R1(dhcp-config)#exit R1(config)#ip dhcp excluded-address 10.80.8.2 10.80.8.51

Configurar DHCP IPv4 para VLAN 30	Creamos el grupo DHCP para la VLAN 30, compuesto por las últimas 10 direcciones de la subred solamente. Asignamos el nombre de dominio unad-ccna-sa.net y especificamos la dirección de la puerta de enlace predeterminada como dirección de interfaz del ROUTER para la subred involucrada.	R1(config)#ip dhcp pool vlan30 R1(dhcp-config)#network 10.80.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.80.8.65 R1(dhcp-config)#domain-name unad-ccna-sa.net R1(dhcp-config)#exit R1(config)#ip dhcp excluded-address 10.80.8.66 10.80.8.83

Fuente: Autoría propia.

Paso 2: Configurar los servidores

Se configuran los equipos de cómputo (PC-A y PC-B) para que obtengan IPv4 por medio de DHCP y la IPv6 sea estática, utilizamos ipconfig/all y con la información presentada se llena la Tabla 14 y Tabla 15.

Tabla 14. Tabla de tareas configuración servidores PC-A.

Configuración de red de PC-A	
Descripción	ccna-sa.com
Dirección física	00E0.8FB0.4D34
Dirección IP	10.80.8.2
Máscara de subred	255.255.255.192
Gateway predeterminado	10.80.8.1
Gateway predeterminado IPv6	FE80::1

Fuente: Autoría propia.

Tabla 15. Tabla de tareas configuración servidores PC-B.

Configuración de red de PC-B	
Descripción	ccna-sa.com
Dirección física	000B.BE9B.5BDB
Dirección IP	10.80.8.66
Máscara de subred	255.255.255.224
Gateway predeterminado	10.80.8.65
Gateway predeterminado IPv6	FE80::1

Fuente: Autoría propia.

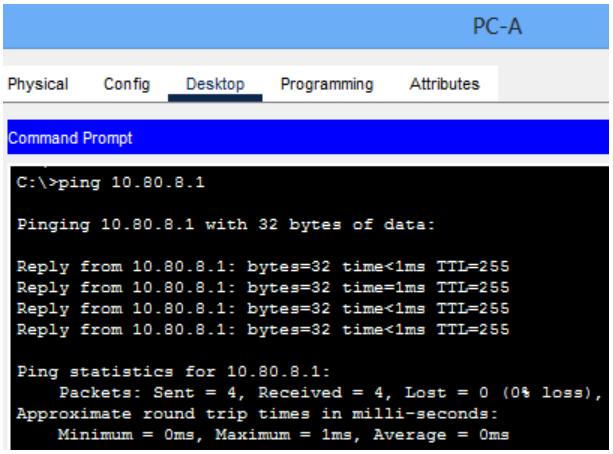
Parte 3: Probar y verificar la conectividad de extremo a extremo.

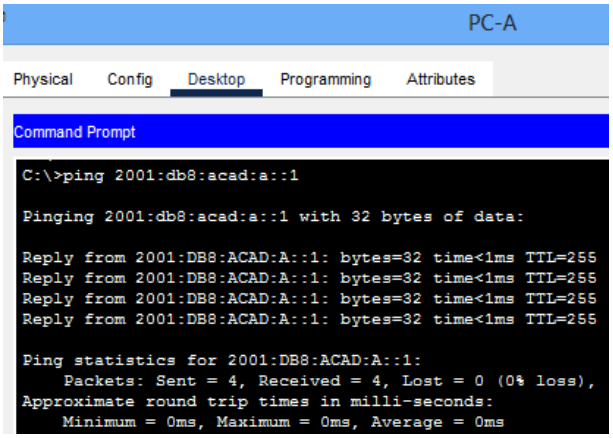
Se utiliza el comando PING para verificar la conectividad exitosa entre los equipos que conforman la red, esto lo hacemos para probar IPv4 e IPv6.

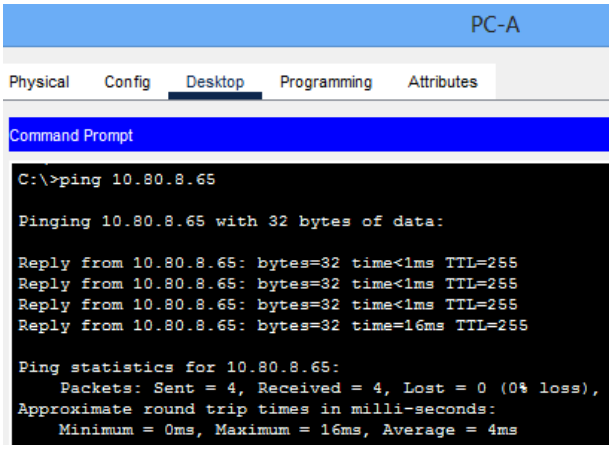
Se utiliza la Tabla 16 para almacenar las capturas de pantalla que soportan la conectividad exitosa entre los dispositivos de la red:

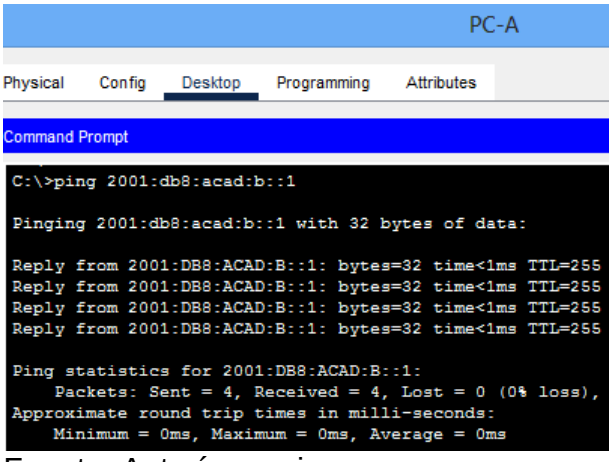
Nota: En la Tabla 16 podemos evidenciar que todas nuestras pruebas PING fueron exitosas ya que no tenemos perdida de paquetes al momento de solicitarlos al otro dispositivo.

Tabla 16. Tabla de pruebas y verificación de conectividad.

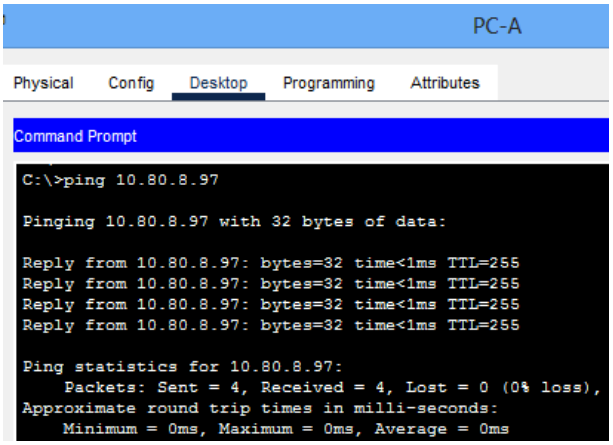
DE	A		DIRECCION IP	RESULTADOS DE PING
PC-A	R1, G0/0/1.2	IPv4	10.80.8.1 /26	Figura 13. Ping PC-A / R1 G0/0/1.2 IPv4.  Fuente: Autoría propia.

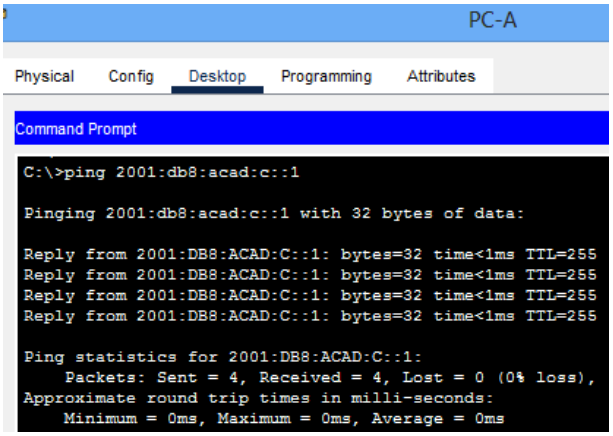
<table>
<tr><td rowspan="3"></td><td></td><td>IPv6</td><td>2001:db8:acad:a::1/64</td><td>Figura 14. Ping PC-A / R1 G0/0/1.2 IPv6.
 

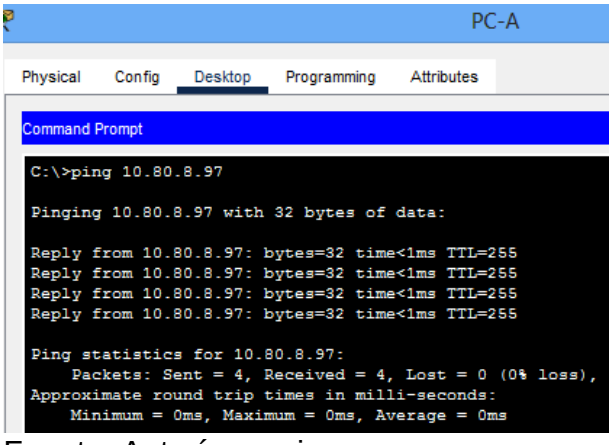
Fuente: Autoría propia.</td></tr>
<tr><td>R1, G0/0/1.3</td><td>IPv4</td><td>10.80.8.65 /27</td><td>Figura 15. Ping PC-A / R1 G0/0/1.3 IPv4.
 

Fuente: Autoría propia.</td></tr>
<tr><td></td><td>IPv6</td><td>2001:db8:acad:b::1/64</td><td>Figura 16. Ping PC-A / R1 G0/0/1.3 IPv6.
 

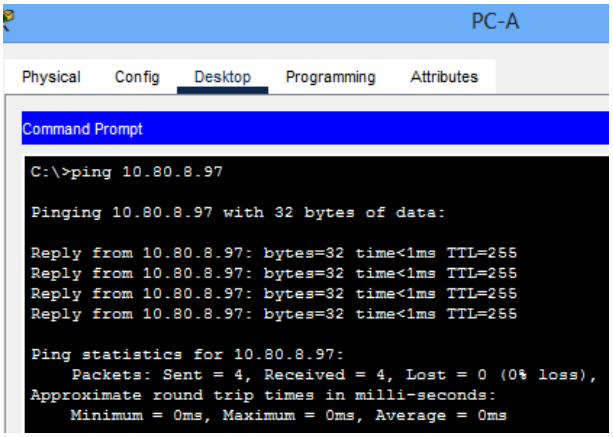
Fuente: Autoría propia.</td></tr>
</table>

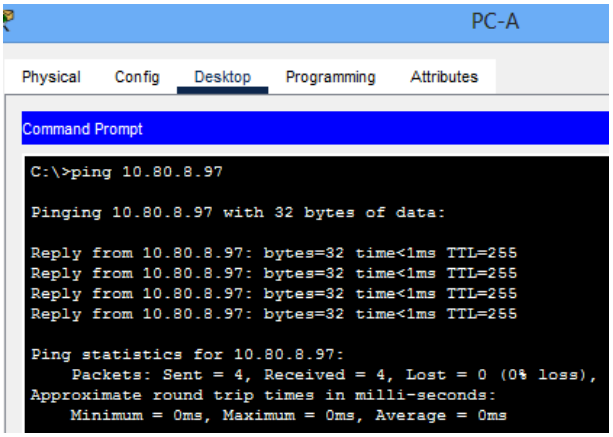
<table>
<tr><td rowspan="3"></td><td rowspan="2">R1, G0/0/1.4</td><td>IPv4</td><td>10.80.8.97 /29</td><td>Figura 17. Ping PC-A / R1 G0/0/1.4 IPv4.
 

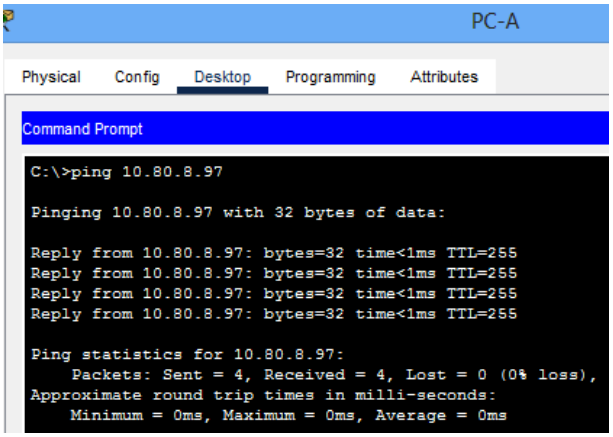
Fuente: Autoría propia.</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:c::1/64</td><td>Figura 18. Ping PC-A / R1 G0/0/1.4 IPv6.
 

Fuente: Autoría propia.</td></tr>
<tr><td>S1, VLAN 4</td><td>IPv4</td><td>10.80.8.97</td><td>Figura 19. Ping PC-A / S1, VLAN 4 IPv4.
 

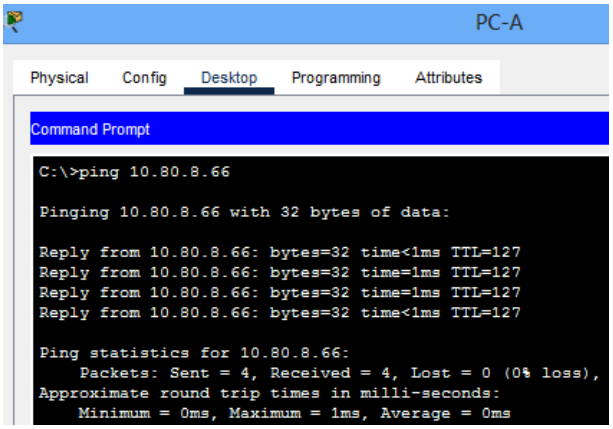
Fuente: Autoría propia.</td></tr>
</table>

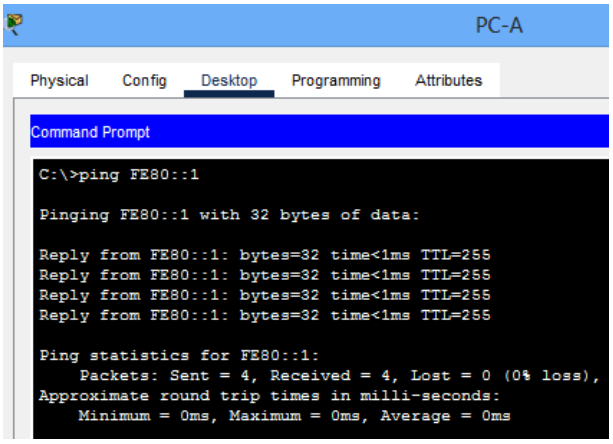
<table>
<tr><td rowspan="3"></td><td></td><td>IPv6</td><td>2001:db8:acad:c::98
/64
fe80: :98</td><td>Figura 20. Ping PC-A / S1, VLAN 4 IPv6.
 

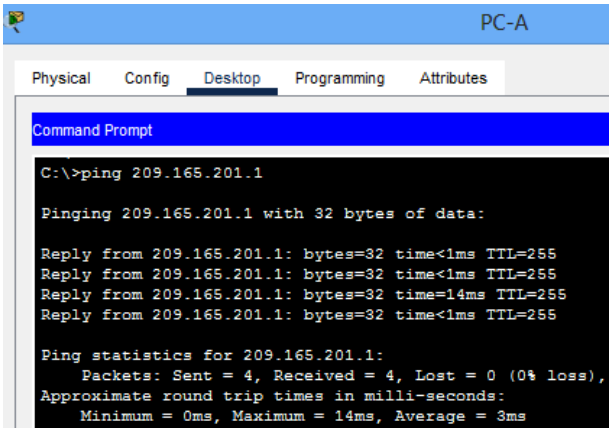
Fuente: Autoría propia.</td></tr>
<tr><td rowspan="2">S2,
VLAN 4</td><td>IPv4</td><td>10.80.8.97</td><td>Figura 21. Ping PC-A / S2, VLAN 4 IPv4.
 

Fuente: Autoría propia.</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:c::99
/64
fe80: :99</td><td>Figura 22. Ping PC-A / S2, VLAN 4 IPv6.
 

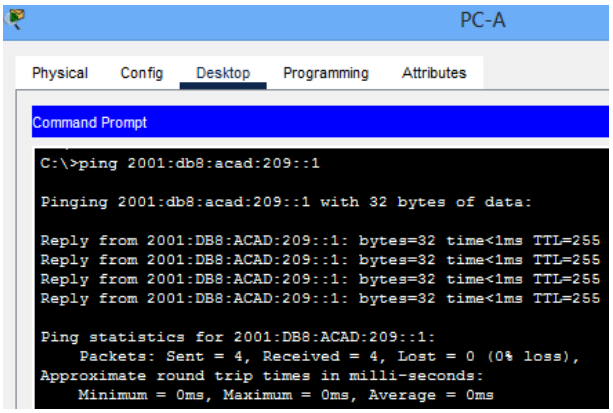
Fuente: Autoría propia.</td></tr>
</table>

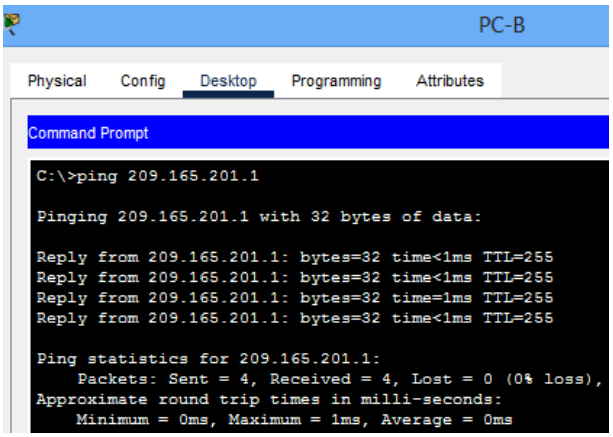
<table>
<tr><td rowspan="3"></td><td rowspan="2">PC-B</td><td>IPv4</td><td>10.80.8.66</td><td>Figura 23. Ping PC-A / PC-B IPv4.
 

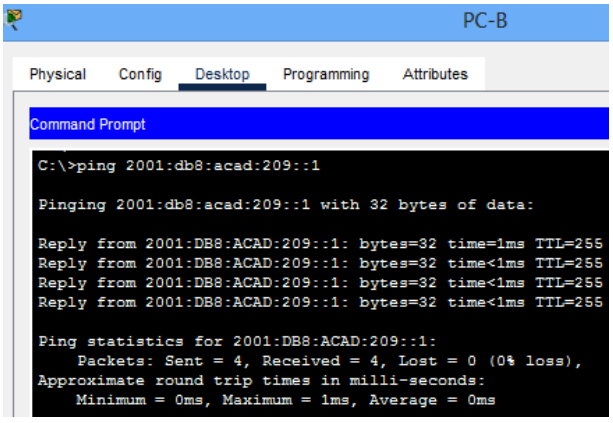
Fuente: Autoría propia.</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:b::50 /64</td><td>Figura 24. Ping PC-A / PC-B IPv6.
 

Fuente: Autoría propia.</td></tr>
<tr><td>R1 Bucle 0</td><td>IPv4</td><td>209.165.201.1 /27</td><td>Figura 25. Ping PC-A / R1 Bucle 0 IPv4.
 

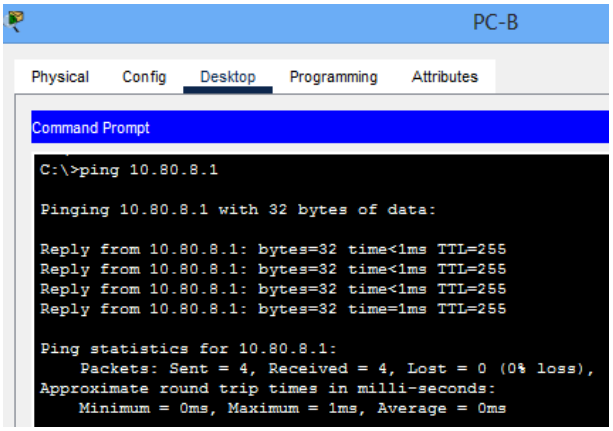
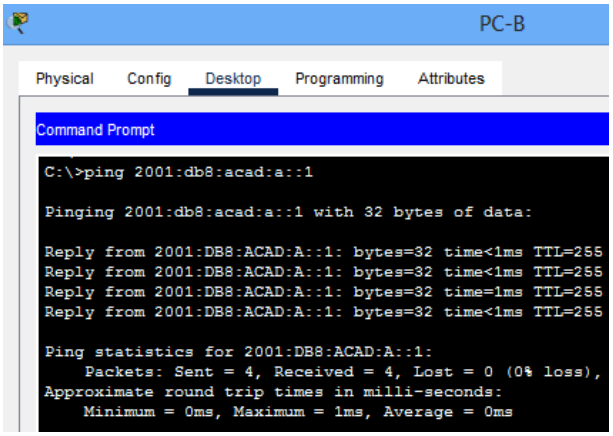
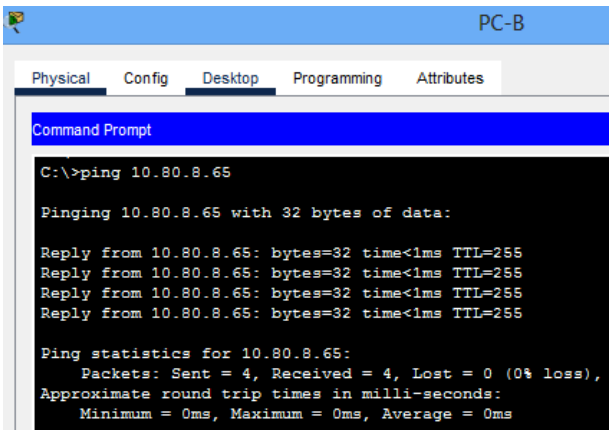
Fuente: Autoría propia.</td></tr>
</table>

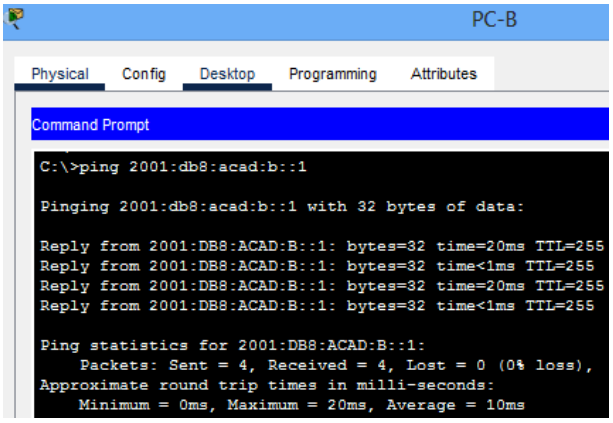
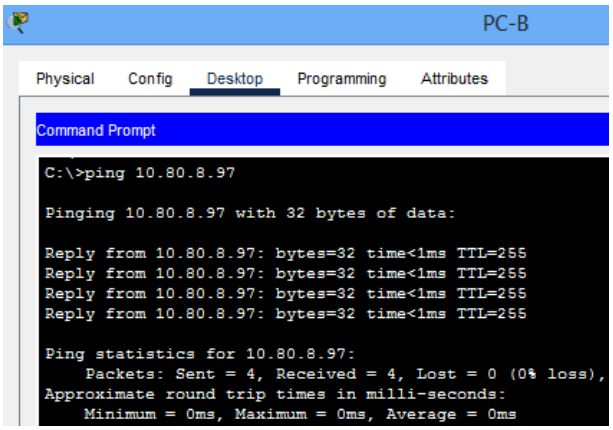
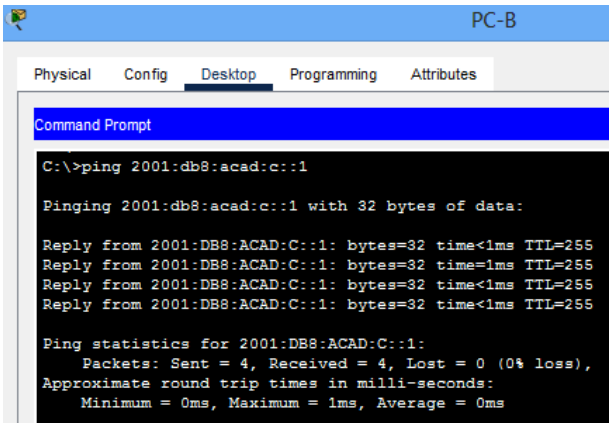
<table>
<tr><td></td><td></td><td>IPv6</td><td>2001:db8:acad:209::1/64</td><td>Figura 26. Ping PC-A / R1 Bucle 0 IPv6.
 

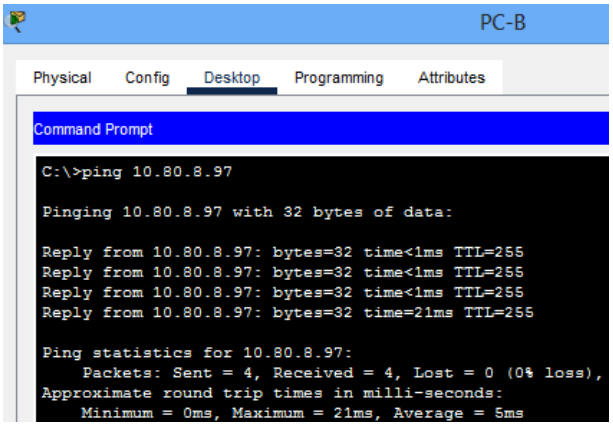
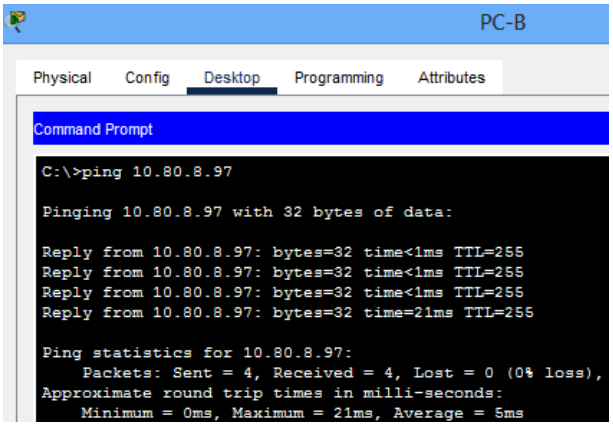
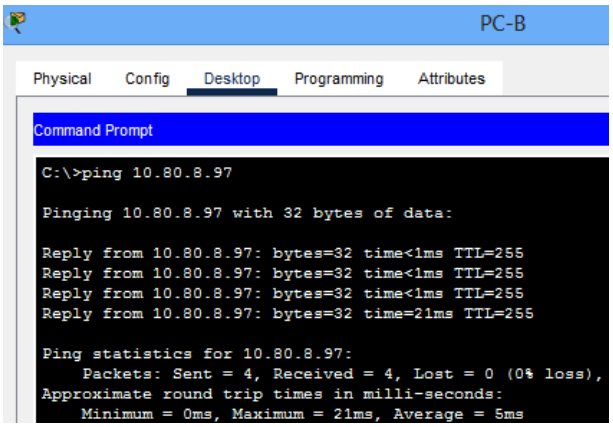
Fuente: Autoría propia.</td></tr>
<tr><td rowspan="2">PC-B</td><td>R1 Bucle 0</td><td>IPv4</td><td>209.165.201.1 /27</td><td>Figura 27. Ping PC-B / R1 Bucle 0 IPv4.
 

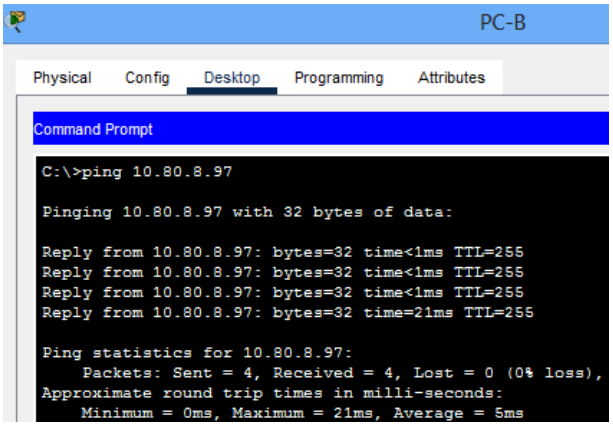
Fuente: Autoría propia.</td></tr>
<tr><td></td><td>IPv6</td><td>2001:db8:acad:209::1/64</td><td>Figura 28. Ping PC-B / R1 Bucle 0 IPv6.
 

Fuente: Autoría propia.</td></tr>
</table>

	R1, G0/0/1.2	IPv4	10.80.8.1 /26	Figura 29. Ping PC-B / R1, G0/0/1.2 IPv4.  Fuente: Autoría propia.
		IPv6	2001:db8:acad:a::1/64	Figura 30. Ping PC-B / R1, G0/0/1.2 IPv6.  Fuente: Autoría propia.
	R1, G0/0/1.3	IPv4	10.80.8.65 /27	Figura 31. Ping PC-B / R1, G0/0/1.3 IPv4.  Fuente: Autoría propia.

		IPv6	2001:db8:acad:b::1/64	Figura 32. Ping PC-B / R1, G0/0/1.3 IPv6.  Fuente: Autoría propia.
	R1, G0/0/1.4	IPv4	10.80.8.97 /29	Figura 33. Ping PC-B / R1, G0/0/1.4 IPv4.  Fuente: Autoría propia.
		IPv6	2001:db8:acad:c::1/64	Figura 34. Ping PC-B / R1, G0/0/1.4 IPv6.  Fuente: Autoría propia.

	S1, VLAN 4	IPv4	10.80.8.97	Figura 35. Ping PC-B / S1, VLAN 4 IPv4.  Fuente: Autoría propia.
		IPv6	2001:db8:acad:c::98 /64 fe80: :98	Figura 36. Ping PC-B / S1, VLAN 4 IPv6.  Fuente: Autoría propia.
	S2, VLAN 4	IPv4	10.80.8.97	Figura 37. Ping PC-B / S2, VLAN 4 IPv4.  Fuente: Autoría propia.

		IPv6	2001:db8:acad:c::99 /64 fe80: :99	Figura 38. Ping PC-B / S2, VLAN 4 IPv6.  Fuente: Autoría propia.

Fuente: Autoría propia.

CONCLUSION ESCENARIO 2.

Para el segundo escenario se debe crear desde cero una red mucho mas corporativa, un poco más robusta que la anterior, en esta red se debe utilizar enrutamiento IPv6 con otro tipo de comandos que nos ayudan a mejorar la seguridad de la misma como lo son PORT-SECURITY junto con grupos ETHERCHANNEL y DHCP, en esta red se configura que tipo de VLAN se va a aceptar que pasen por que puerto de los SWITCHES, es decir se van a armar grupos los cuales van a tener permisos para pasar por unos puertos y por otros no, esto también se realiza pensando en la privacidad de los datos que se envíen en la red.

CONCLUSIONES

Al momento de realizar las subredes se debe tener en cuenta que, después de crear nuestra primera subred dependiendo de la cantidad de host la segunda subred debe iniciar con el número de host siguiente al host con el que termina la primera subred.

Realizando los dos escenarios propuestos se logra identificar las herramientas básicas y protocolos de configuración disponibles para realizar una red.

Después de asignar una contraseña para poder acceder a la configuración del equipo por medio de consola debemos escribir en la siguiente línea “LOGIN” para guardar esta información y que entre en funcionamiento.

En las anteriores páginas se logró configurar como lo indica la guía los equipos enlistados y pudimos lograr simular el escenario de redes LAN y WAN sin problema alguno, para ello utilizamos todas las herramientas dispuestas para poder revisar y entender este tipo de red.

Fortalecimos el uso de la configuración por medio de comandos, recordemos que hoy en día son mucho menos los equipos que se configuran de esta forma y gracias a ello se nos va olvidando el proceso por códigos.

REFERENCIA BIBLIOGRAFICAS

AT INTERNET. GLOSARIO DNS. {En línea}. (2022) {27 de noviembre de 2022} disponible en: https://www.atinternet.com/es/glosario/dns/

CISCO. ¿Qué es un ROUTER? {En línea}.(2022) {26 de noviembre de 2022} disponible en: https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html

CONCEPTO.de. ¿Qué es una red?. {En línea}. (2021) {24 de noviembre de 2022} disponible en: https://concepto.de/red-2/

IONOS, digital guide. ¿Qué es un servidor? {En línea}.(2020) {27 de noviembre de 2022} disponible en: https://www.ionos.es/digitalguide/servidores/know-how/que-es-un-servidor-un-concepto-dos-definiciones/

JVS Informática. ¿Qué es un BYTE? {En línea}. (2020) {25 de noviembre de 2022} disponible en: https://www.jvs-informatica.com/blog/glosario/byte/

MILENIUM. Web. {En línea}. (2022) {27 de noviembre de 2022} disponible en: https://www.informaticamilenium.com.mx/es/temas/que-es-el-web.html

Ms.gonzalez. El SWITCH: ¿Cómo funciona? y sus principales características. {En línea}. (2013) {24 de noviembre de 2022} disponible en: https://redestelematicas.com/el-switch-como-funciona-y-sus-principales-caracteristicas/

NETEC expertos enseñando a expertos. ¿Qué es CISCO? {En línea}. (2021) {27 de noviembre de 2022} disponible en: https://www.netec.com/que-es-cisco

RAMIREZ, Helena. ¿Qué es internet? {En línea}. (1999) {27 noviembre de 2022} disponible en: https://ccp.ucr.ac.cr/cursoweb/112que.htm

REAL ACADEMIA ESPAÑOLA. Protocolo. {En línea}. (2021) {25 de noviembre de 2022} disponible en: https://dle.rae.es/protocolo

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO. Configurando un acceso administrativo seguro. {En línea}. (2010) {24 de noviembre de 2022} disponible en: https://www.uaeh.edu.mx/scige/boletin/tepeji/n8/e1.html#:~:text=L%C3%ADnea%20de%20terminal%20virtual,los%20subcomandos%20password%20y%20login

ANEXOS

Anexo A – Descarga de archivo de simulación Escenario 1.

Enlace:

https://drive.google.com/file/d/1Ud4as3z_Zpc1K9YswI4Pef7JZgOigXMX/view?usp=sharing

Anexo B – Descarga de archivo de simulación Escenario 2.

Enlace:

https://drive.google.com/file/d/1vnyclVciz13ccBG7mfCbXI8iNg7snm5O/view?usp=sharing