INFORME– PRUEBA DE HABILIDADES PRÁCTICA

PAOLA ANDREA MARTINEZ AGUIRRE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

INGENIERÍA DE SISTEMAS

CALI

2022

INFORME– PRUEBA DE HABILIDADES PRÁCTICA

PAOLA ANDREA MARTINEZ AGUIRRE

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

PAULITA FLOR SALAZAR
DIRECTOR

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

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____
_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

CALI, 11 de diciembre de 2022

AGRADECIMIENTOS

Doy gratitud a mi familia por darme su ejemplo de persistencia y de paciencia para lograr mis objetivos propuestos, también agradezco a mi esposo por apoyarme en este camino y a mi hija que le dedico este logro diciéndole “que no se fácil no significa que sea imposible.

CONTENIDO

LISTA DE TABLAS

TABLA DE ILUSTRACIONES

GLOSARIO

BROADCAST: Es un mensaje que se transmite a todos los usuarios de una red sin necesitar una acción de retroalimentación. Un ordenador conectado a la red envía un paquete de datos a todos los demás usuarios en la red de forma simultánea y, en cuanto a las direcciones de destino, el emisor no tiene que especificar ninguna.[1]

COMANDO PING: Se usa para determinar el estado de un host remoto. Al ejecutar el comando ping, el protocolo ICMP envía al host un determinado datagrama para solicitar una respuesta.[2]

CONSOLA: Un puerto físico de un dispositivo Cisco que proporciona acceso al dispositivo a través de un canal de administración exclusivo, también conocido como acceso fuera de banda.[3]

EXTRANET: Una red privada y controlada de ordenadores que utiliza la tecnología de Internet para conectar entre sí a un grupo definido de usuarios externos y otorgar acceso a la red. Una extranet se utiliza para poner ciertos recursos a disposición de un círculo autorizado**,** pero no al público general.[4]

INTERNET: La Red es un conjunto global y abierto de redes de ordenadores. No es una red homogénea, sino que está compuesta por muchas redes, con frecuencia muy diferentes.[5]

INTRANET: La intranet es una red corporativa que conecta a varios participantes entre sí y permite, de esta forma, el intercambio interno.[6]

---

[1] IONOS, ¿qué es y cómo funciona?, (2022)
[2] ORACLE. Sondeo de hosts remotos con el comando ping, (2022)
[3] WALTON Alex, CCNA desde Cero, (2020)
[4] IONOS, La extranet y sus beneficios para las empresas, (2022)
[5] IONOS, La extranet y sus beneficios para las empresas, (2022)
[6] IONOS, La extranet y sus beneficios para las empresas, (2022)

LAN: Si una red está formada por más de un ordenador, esta recibe el nombre de Local Area Network (LAN). Una red local de tales características puede incluir a dos ordenadores en una vivienda privada o a varios miles de dispositivos en una empresa.[7]

PDU: Es un bloque específico de información transferida a través de una red. A menudo se usa en referencia a la Modelo OSI, ya que describe los diferentes tipos de datos que se transfieren desde cada capa.[8]

SSH: Es un protocolo que tiene como función ofrecer acceso remoto a un servidor. [9]

[7] IONOS, Conoce los tipos de redes más importantes, (2022)
[8] TECHLIB. Definición de PDU, (2022)
[9] JIMENEZ, Javier. Qué es y para qué sirve el SSH, (2021)

RESUMEN

En el informe siguiente se abordarán el desarrollo de dos escenarios en los cuales aplicaremos los conceptos aprendidos como configuraciones básicas, seguridad para los switches y routers, con estos escenarios aprenderemos a tener habilidades y destreza para resolver problemas futuros en Networking.

Para el desarrollo de los escenarios utilizaremos la herramienta Packet Tracer, en la cual podemos replicar los escenarios y hacer todo el direccionamiento propuesto como el seguimiento de la configuración por ejemplo con el comando show ip route, y por último comprobar la configuración con el comando ping

Palabras Clave: CCNA, Networking, Direccionamiento, Conectividad, Packet Tracer, Comandos básicos.

ABSTRACT

In the following report, the development of two scenarios will be addressed in which we will apply the concepts learned such as basic configurations, security for switches and routers, with these scenarios we will learn to have skills and abilities to solve future problems in Networking.

For the development of the scenarios, we will use the Packet Tracer tool, in which we can replicate the scenarios and do all the proposed addressing such as configuration monitoring, for example with the show ip route command, and finally check the configuration with the ping command.

Keywords: CCNA, Networking, Addressing, Connectivity, Packet Tracer, Basic Commands.

INTRODUCCIÓN

La actividad de las pruebas de habilidades practicas CCNA, corresponde a los conocimientos aprendidos durante el curso del diplomado de profundización CCNA en los cuales con evaluaciones en la plataforma de CISCO o con trabajos colaborativos podemos adquirir habilidades de manejo de configuraciones, protocolos de enrutamiento para crear una topología de red interconectada de acuerdo a los requerimientos definidos.

Para el desarrollo de las pruebas de habilidades se utiliza la herramienta Packet Tracer, para poder demostrar nuestras habilidades y seguir aprendiendo como en nuestra vida se aplica las redes de telecomunicación.

En el escenario 1 aprenderemos hacer un direccionamiento IPv4 dándonos una dirección IP y los hosts necesarios para implementar la red la cual consta de dos pc, un switch y un router, esto lo haremos con la ayuda del software Packet Tracer.

En el escenario 2 aprenderemos a hacer una configuración de una pequeña red, la cual aceptará direcciones ipv4 y ipv6 para todos los hosts, se ampliará el conocimiento sobre el EtherChannel.

DESARROLLO

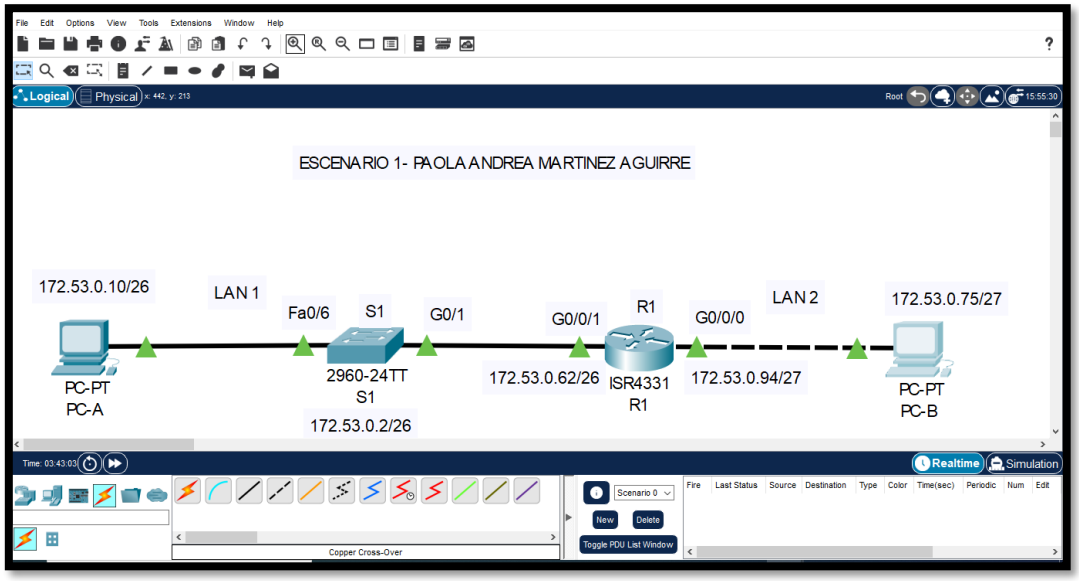
1. ESCENARIO 1

1.1 Topología Escenario 1

Figura 1 Topología Escenario 1

Fuente: Autor

Figura 2 Simulación de escenario 1



Fuente: Autor

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

Ítem	Requerimiento
Dirección de Red	172.53.3.0/16
Requerimiento de host Subred LAN1	60
Requerimiento de host Subred LAN2	20
R1 G0/0/1	172.53.0.62/26
R1 G0/0/0	172.53.0.94/27
S1 SVI	172.53.0.2/26
PC-A	172.53.0.10/26
PC-B	172.53.0.75/27

Fuente: Autor

1.2 Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Desactivaremos la búsqueda DNS, ya que está habilitada por defecto y así evitaremos al escribir comandos con errores. Este los haremos con el comando no ip domain-lookup	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#exit Router#

	%SYS-5-CONFIG_I: Configured from console by console
Ahora le daremos al nombre al router de R1 con el comando hostname R1	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#hostname R1 R1(config)#exit R1# %SYS-5-CONFIG_I: Configured from console by console
Ahora le daremos un nombre al dominio ccna-sa.com con el comando ip domain-name ccna-sa.com	R1>enable R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ip domain-name ccna-sa.com R1(config)#exit R1# %SYS-5-CONFIG_I: Configured from console by console
Guardaremos en la configuración del router la contraseña ciscoenpass encriptada con el comando enable secret ciscoenpass	R1>enable R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#enable secret ciscoenpass R1(config)#exit R1#

	%SYS-5-CONFIG_I: Configured from console by console
Protegeremos la consola con una contraseña de consola ciscoconpass con el comando password ciscoconpass	R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit R1(config)#exit R1# %SYS-5-CONFIG_I: Configured from console by console
Crearemos un mínimo de longitud para proteger nuestro router con un mínimo de 10 de caracteres, utilizaremos el comando security passwords min-length 10	User Access Verification Password: R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#security passwords min-length 10 R1(config)#exit R1# %SYS-5-CONFIG_I: Configured from console by console

Para mantener la seguridad a la hora de autenticarnos crearemos el usuario admin y de contraseña admin1pass con el comando username admin secret admin1pass	User Access Verification Password: R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#username admin secret admin1pass R1(config)#exit R1# %SYS-5-CONFIG_I: Configured from console by console
Vamos activar los puertos virtuales VTY del 0 al 15 con el comando line vty 0 15, en este caso se debe tener en cuenta que una mala configuración del VTY causa un riesgo de seguridad.	User Access Verification Password: R1>enable Password: R1#enable R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#line vty 0 15 R1(config-line)#login local R1(config-line)#exit R1(config)#exit R1# %SYS-5-CONFIG_I: Configured from console by console

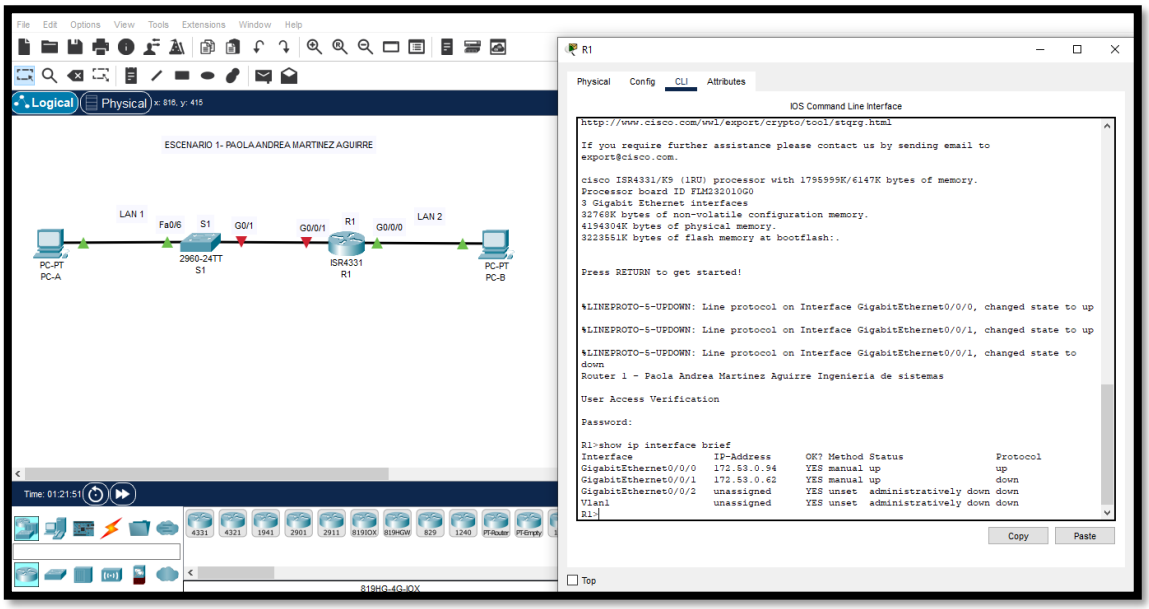
Configuraremos el acceso remoto seguro de los puertos virtuales VTY con el protocolo SSH con el comando transport input ssh	User Access Verification Password: R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#line vty 0 15 R1(config-line)#transport input ssh R1(config-line)#login local R1(config-line)#exit R1(config)#exit R1# %SYS-5-CONFIG_I: Configured from console by console
Para proteger las contraseñas que estén sin encriptar en el router utilizaremos el comando service password-encryption	User Access Verification Password: R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#service password-encryption R1(config)#exit R1# %SYS-5-CONFIG_I: Configured from console by console
	User Access Verification

Crearemos un cartel de aviso al iniciar el entorno de trabajo del router utilizando el comando banner motd # Router 1 - Paola Andrea Martínez Aguirre Ingeniería de sistemas #	Password: R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#banner motd # Router 1 - Paola Andrea Martínez Aguirre Ingeniería de sistemas # R1(config)#exit R1# %SYS-5-CONFIG_I: Configured from console by console
Para que nuestro router sea accesible vamos a configurar de interface G0/0/0 con el comando int g0/0/0, ip address 172.53.0.94 y no shutdown	Router 1 - Paola Andrea Martinez Aguirre Ingenieria de sistemas User Access Verification Password: R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#int g0/0/0 R1(config-if)#ip address 172.53.0.94 255.255.255.224 R1(config-if)#no shutdown R1(config-if)#

	%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up
Para que nuestro router sea accesible vamos a configurar la interface G0/0/1con el comando int g0/0/1, ip address 172.53.0.62 y no shutdown	Router 1 - Paola Andrea Martinez Aguirre Ingenieria de sistemas User Access Verification Password: R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#int g0/0/1 R1(config-if)#ip address 172.53.0.62 255.255.255.192 R1(config-if)#no shutdown R1(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface

	GigabitEthernet0/0/1, changed state to up
Vamos a crear un sistema de cifrado para el router con el sistema RSA y utilizaremos el comando crypto key generate rsa y de longitud del módulo será de 1024.	Router 1 - Paola Andrea Martinez Aguirre Ingenieria de sistemas User Access Verification Password: R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#crypto key generate rsa The name for the keys will be: R1.ccna-sa.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Figura 3 Verificación R1 con comando show ip interface brief



Fuente: Autor

Las tareas de configuración de S1 incluyen lo siguiente:

Tarea	Especificación
Desactivaremos la búsqueda DNS, ya que está habilitada por defecto y así evitaremos al escribir comandos con errores. Este los haremos con el comando no ip domain-lookup	Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup Switch(config)#exit Switch# %SYS-5-CONFIG_I: Configured from console by console

Ahora le daremos al nombre al switch de S1 con el comando hostname S1	Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#hostname S1 S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console
Ahora le daremos un nombre al dominio ccna-sa.com con el comando ip domain-name ccna-sa.com	S1>enable S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#ip domain-name ccna-sa.com S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console
Guardaremos en la configuración del switch la contraseña ciscoenpass encriptada con el comando enable secret ciscoenpass	S1>enable S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#enable secret ciscoenpass S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console

Protegeremos la consola con una contraseña de consola ciscoconpass con el comando password ciscoconpass	S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console
Hay puertos que no se van usar, utilizaremos el comando interface range para desactivar en un rango los puertos sin uso los cuales son F0/1-4, F0/7-24, G0/1-2	**F0/1-4** User Access Verification Password: S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#interface range fastEthernet 0/1-4 S1(config-if-range)#shutdown %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

	%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down S1(config-if-range)#exit S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console **F0/7-24** User Access Verification Password: S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#interface range fastEthernet 0/7-24

	S1(config-if-range) #shutdown %LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

	%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

	%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down S1(config-if-range) #exit S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console **G0/1-2** User Access Verification Password: S1>enable Password: S1#configure terminal

	Enter configuration commands, one per line. End with CNTL/Z. S1(config)#interface range gigabitEthernet 0/1-2 S1(config-if-range)#shutdown %LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down S1(config-if-range)# %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down S1(config-if-range)#exit S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console
Para mantener la seguridad a la hora de autenticarnos crearemos el usuario admin y de contraseña	User Access Verification Password: S1>enable Password: S1#configure terminal

admin1pass con el comando username admin secret admin1pass	Enter configuration commands, one per line. End with CNTL/Z. S1(config)#username admin secret admin1pass S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console
Vamos activar los puertos virtuales VTY del 0 al 15 con el comando line vty 0 15, en este caso se debe tener en cuenta que una mala configuración del VTY causa un riesgo de seguridad.	User Access Verification Password: S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#line vty 0 15 S1(config-line)#login local S1(config-line)#exit S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console
Configuraremos el acceso remoto seguro de los puertos virtuales VTY con el protocolo SSH con el comando transport input ssh	User Access Verification Password: S1>enable Password: S1#configure terminal

	Enter configuration commands, one per line. End with CNTL/Z. S1(config)#line vty 0 15 S1(config-line)#transport input ssh S1(config-line)#login local S1(config-line)#exit S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console
Para proteger las contraseñas que estén sin encriptar en el switch utilizaremos el comando service password-encryption	User Access Verification Password: S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#service password-encryption S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console
Crearemos un cartel de aviso al iniciar el entorno de trabajo del switch utilizando el comando banner motd # Switch 1 - Paola Andrea Martínez Aguirre - Ingeniería de sistemas #	User Access Verification Password: S1>enable Password: S1#configure terminal

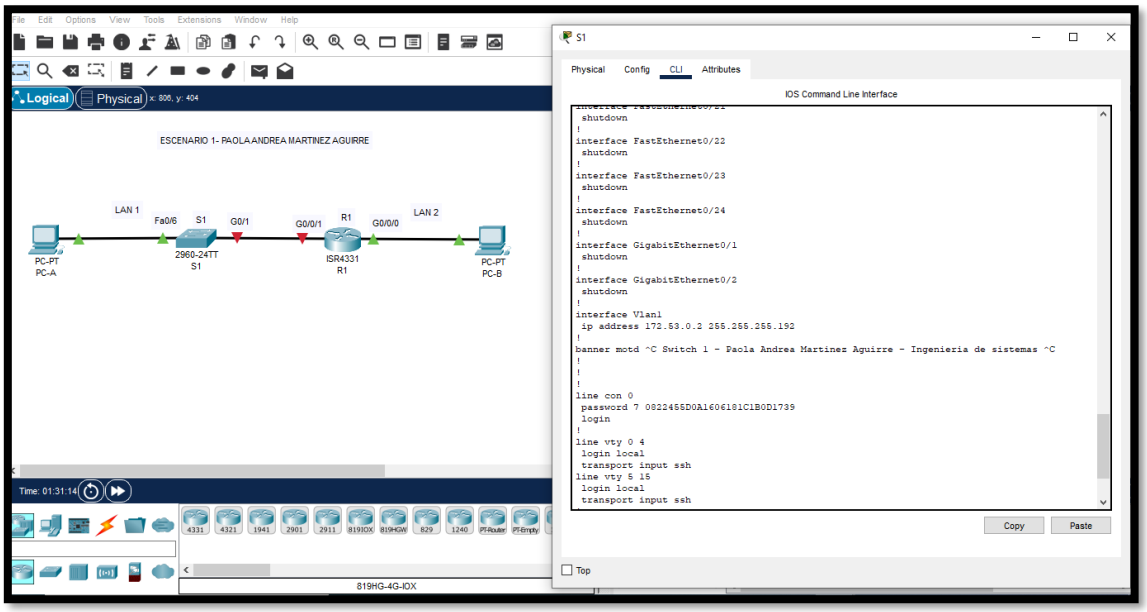
	Enter configuration commands, one per line. End with CNTL/Z. S1(config)#banner motd # Switch 1 - Paola Andrea Martinez Aguirre - Ingenieria de sistemas # S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console
Vamos a crear un sistema de cifrado para el switch con el sistema RSA y utilizaremos el comando crypto key generate rsa y de longitud del módulo será de 1024.	Switch 1 - Paola Andrea Martinez Aguirre - Ingenieria de sistemas User Access Verification Password: S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#no ip domain-lookup S1(config)#crypto key generate rsa The name for the keys will be: S1.ccna-sa.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

	How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] S1(config)#exit *Mar 1 1:3:56.977: %SSH-5-ENABLED: SSH 1.99 has been enabled S1# %SYS-5-CONFIG_I: Configured from console by console
Vamos a configurar la VLAN1 en una interfaz virtual SVI la cual nos soporta los protocolos de enrutamiento, utilizaremos el comando interface vlan1, ip address 172.53.0.2 y no shutdown	Switch 1 - Paola Andrea Martinez Aguirre - Ingenieria de sistemas User Access Verification Password: S1>enable Password: S1#enable S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#interface vlan1 S1(config-if)#ip address 172.53.0.2 255.255.255.192 S1(config-if)#no shutdown S1(config-if)# %LINK-5-CHANGED: Interface Vlan1, changed state to up

	%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up S1(config-if)#exit S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console
Para que nuestro switch sea accesible vamos a configurar la interface G0/1 con el comando interface GigabitEthernet0/1 y así levantar el puerto para la comunicación con el router.	Switch 1 - Paola Andrea Martinez Aguirre - Ingenieria de sistemas User Access Verification Password: S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)# S1(config)#interface GigabitEthernet0/1 S1(config-if)#no shutdown S1(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

	%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
Para que nuestros pc se puedan comunicar entre ellos debemos configurar la puerta de enlace por defecto con el comando ip default-gateway	Switch 1 - Paola Andrea Martinez Aguirre - Ingenieria de sistemas User Access Verification Password: S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#ip default-gateway 172.53.0.62 S1(config)#exit

Figura 4 Verificación S1 con comando show runing-config



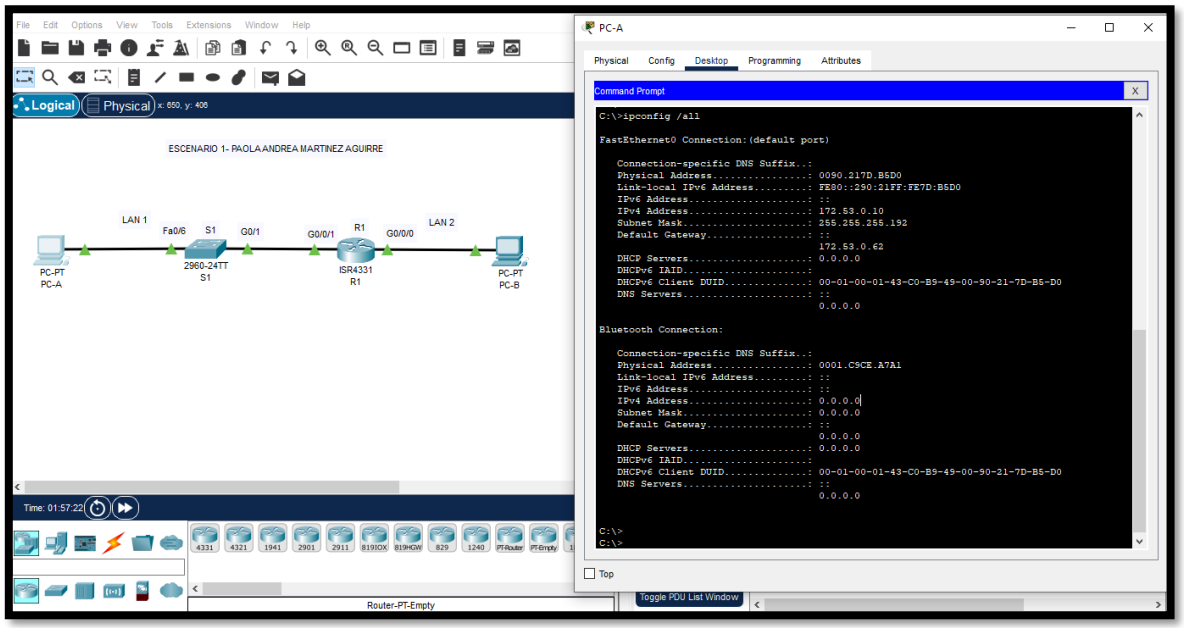
Fuente: Autor

1.3 Paso 2. Configurar los equipos

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

Configuración de red de PC-A	
Descripción	PC-A
Dirección física	0090.217D.B5D0
Dirección IPv4	172.53.0.10
Máscara de subred	255.255.255.192
Puerta de enlace IPv4 predeterminada	172.53.0.62

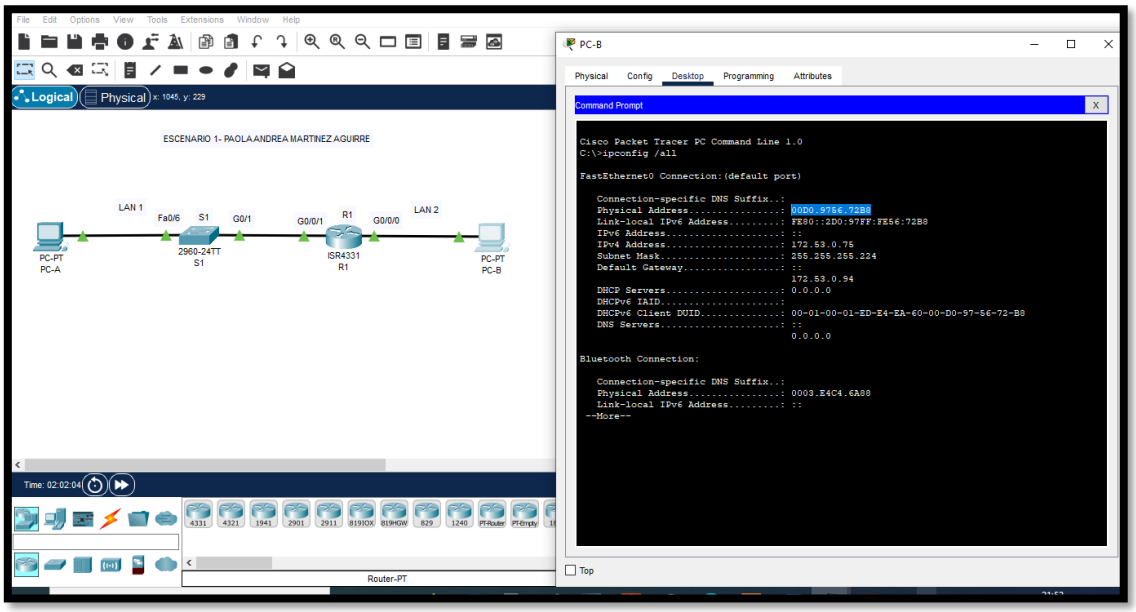
Figura 5 Verificación PC-A con comando ipconfig /all



Fuente: Autor

Configuración de red de PC-B	
Descripción	PC-B
Dirección física	00D0.9756.72B8
Dirección IPv4	172.53.0.75
Máscara de subred	255.255.255.224
Puerta de enlace IPv4 predeterminada	172.53.0.94

Figura 6 Verificación PC-B con comando ipconfig /all



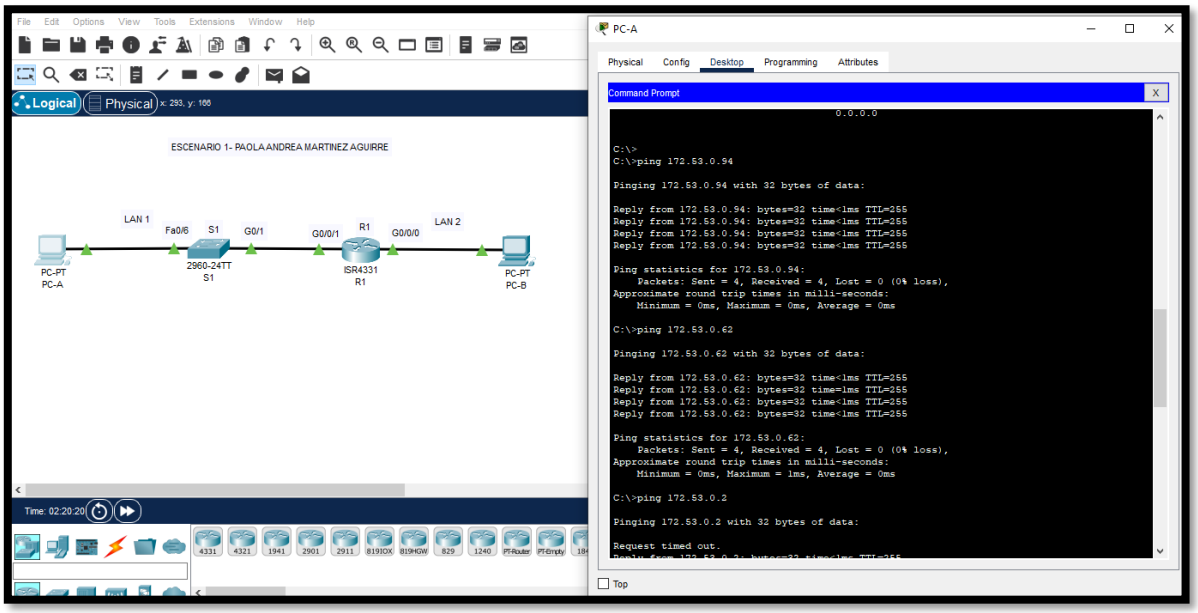
Fuente: Autor

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

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

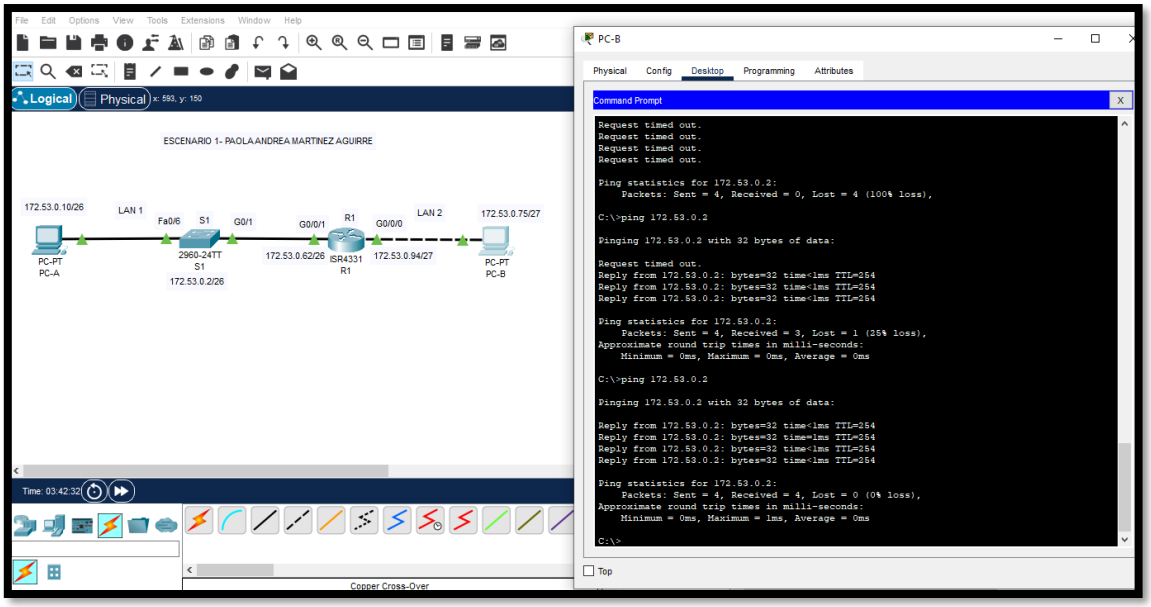
Desde	A	Dirección IP	Resultados de ping
PC-A	R1 G0/0/0	172.53.0.94	El ping se realizó correctamente
	R1 G0/0/1	172.53.0.62	El ping se realizó correctamente
	S1 VLAN 1	172.53.0.2	El ping se realizó correctamente
	PC-B	172.53.0.75	El ping se realizó correctamente
PC-B	R1 G0/0/0	172.53.0.94	El ping se realizó correctamente
	R1 G0/0/1	172.53.0.62	El ping se realizó correctamente
	S1 VLAN1	172.53.0.2	El ping se realizó correctamente

Figura 7 Verificación PC-A con comando ping



Fuente: Autor

Figura 8 Verificación PC-B con comando ping

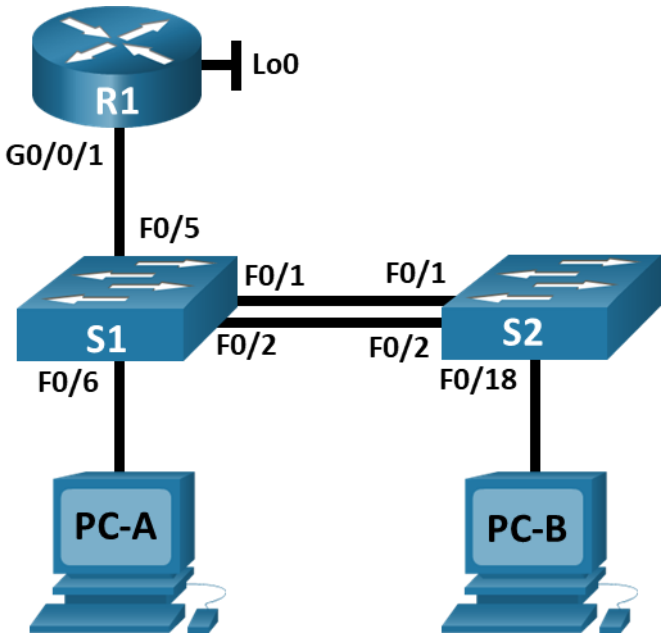


Fuente: Autor

2. ESCENARIO 2

2.1 Topología Escenario 2

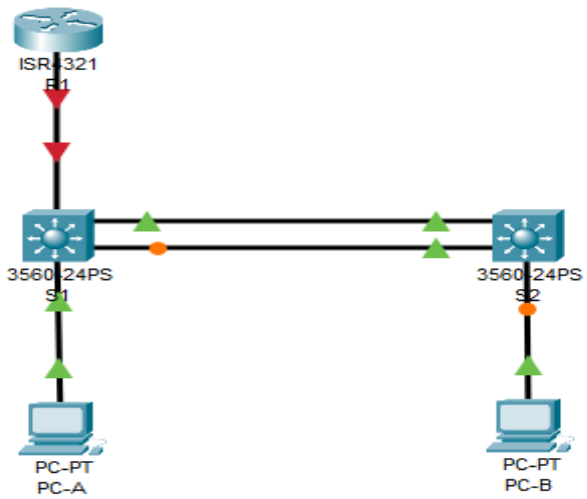
Figura 9 Topología Escenario 2



Fuente: Autor

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

Figura 10 Topología Creada Escenario 2



Fuente: Autor

Tabla 2 Tabla de VLAN

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

Fuente: Autor

Tabla 3 Tabla de asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.20	10.53.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.30	10.53.8.65 /27	No corresponde
R1 G0/0/1.3	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.40	10.53.8.97 /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	10.53.8.98 /29	10.53.8.97
VLAN S1 4	2001:db8:acad:c: :98 /64	No corresponde
S1 VLAN 4	fe80: :98	No corresponde
S2 VLAN 4	10.53.8.99 /29	10.53.8.97
	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: Autor

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

2.2 Instrucciones

2.3 2.3 Parte 1: Inicializar y Recargar y Configurar aspectos básicos de los dispositivos

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

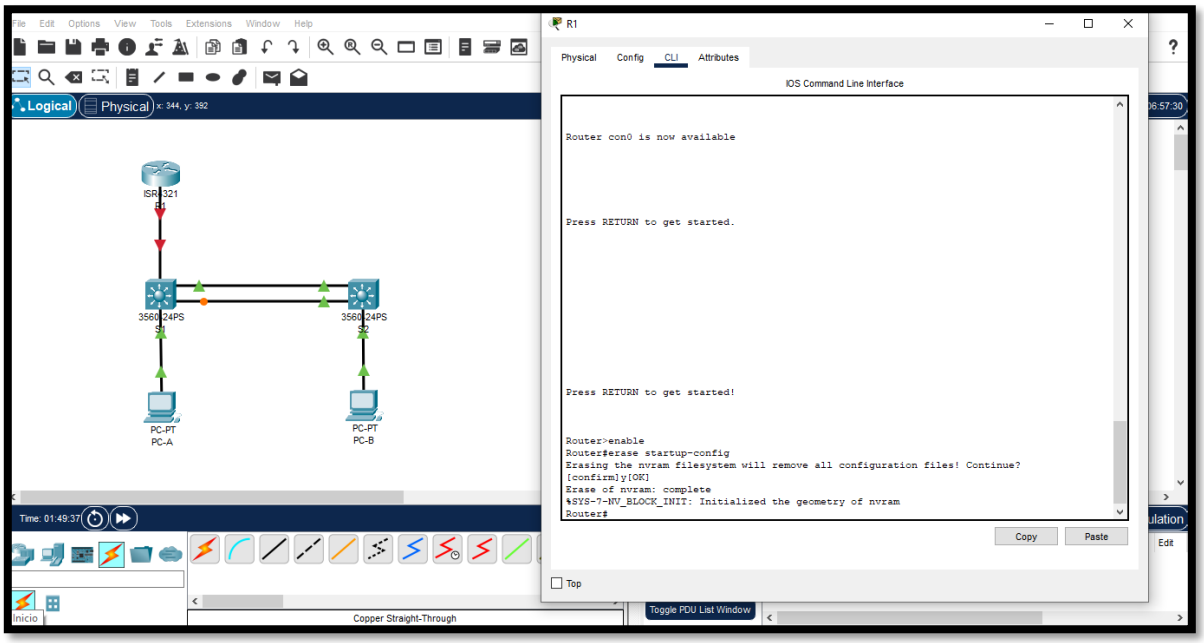
- Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos.

Tarea	Especificación
Eliminar archivos configuración R1	Router>enable Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]y[OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Cargar archivos R1	Router>enable Router#reload System configuration has been modified. Save? [yes/no]: y Building configuration... [OK] Proceed with reload? [confirm] Initializing Hardware ...
Eliminar archivos configuración S1 y datos VLAN	Switch>enable Switch#delete vlan.dat Delete filename [vlan.dat]? y Delete flash:/y? [confirm] %Error deleting flash:/y (No such file or directory) Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]y[OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Cargar archivos S1	Switch>enable Switch#reload Proceed with reload? [confirm] C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(25r) SEC, RELEASE SOFTWARE (fc4)

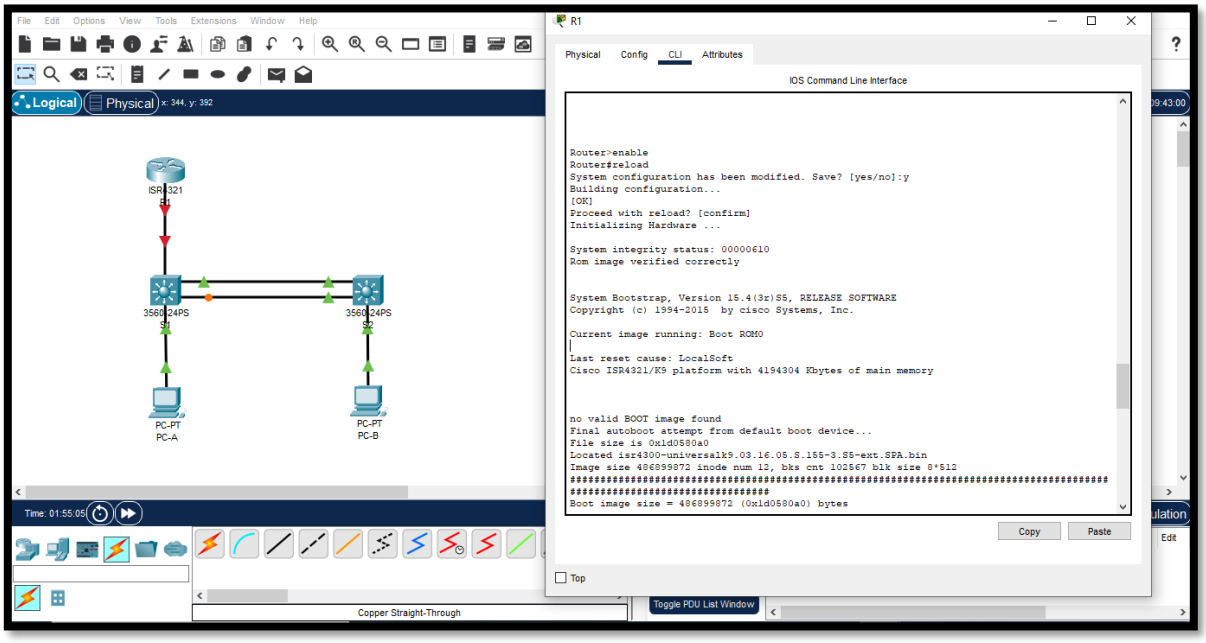
Eliminar archivos configuración S2 y datos VLAN	Switch>enable Switch#delete vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm]y%Error deleting flash:/vlan.dat (No such file or directory) Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]y[OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Cargar archivos S2	Switch>enable Switch#reload Proceed with reload? [confirm] C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(25r) SEC, RELEASE SOFTWARE (fc4)

Figura 11 Eliminar archivos configuración R1



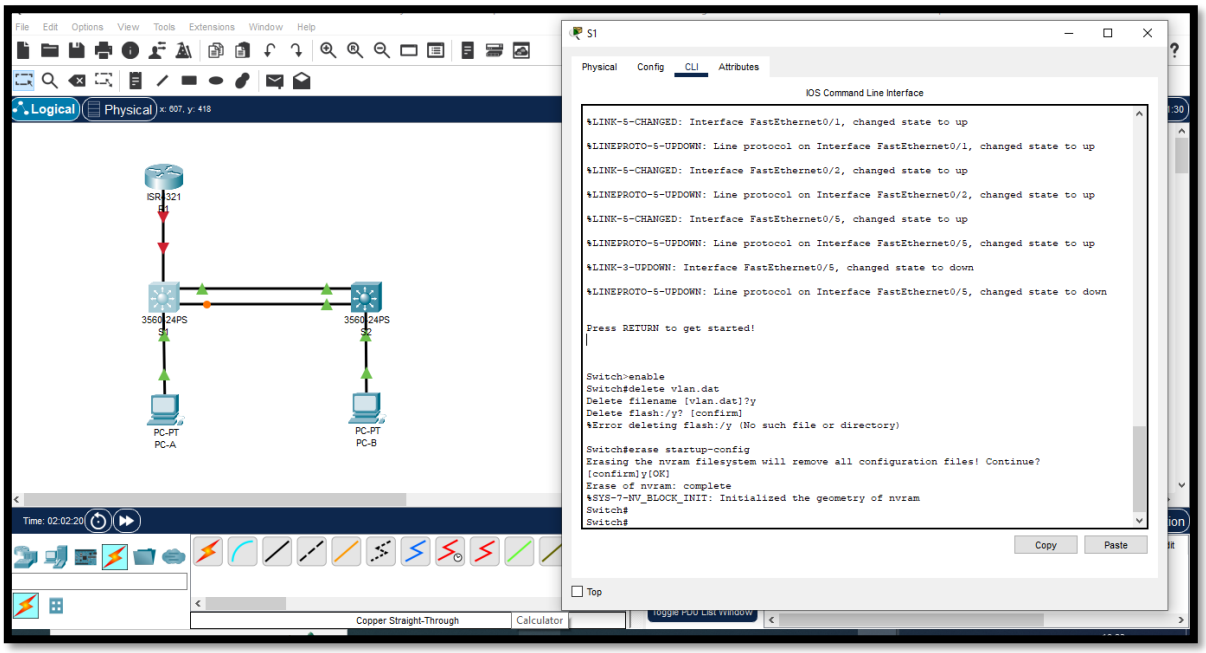
Fuente: Autor

Figura 12 Cargar archivos R1



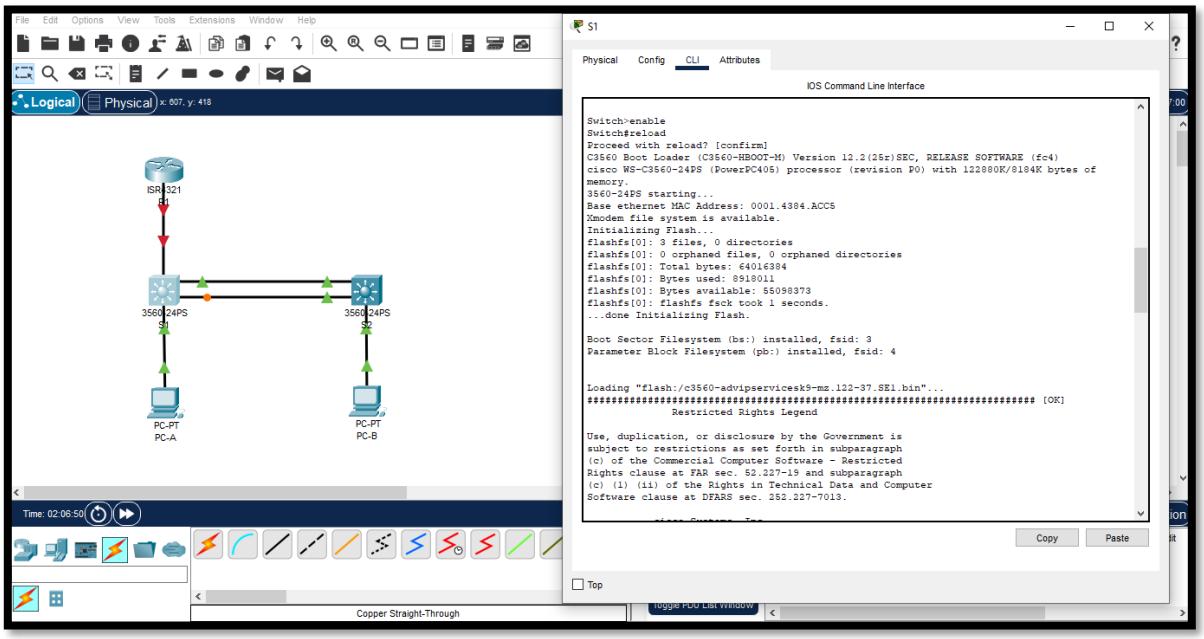
Fuente: Autor

Figura 13 Eliminar archivos configuración S1 y datos VLAN



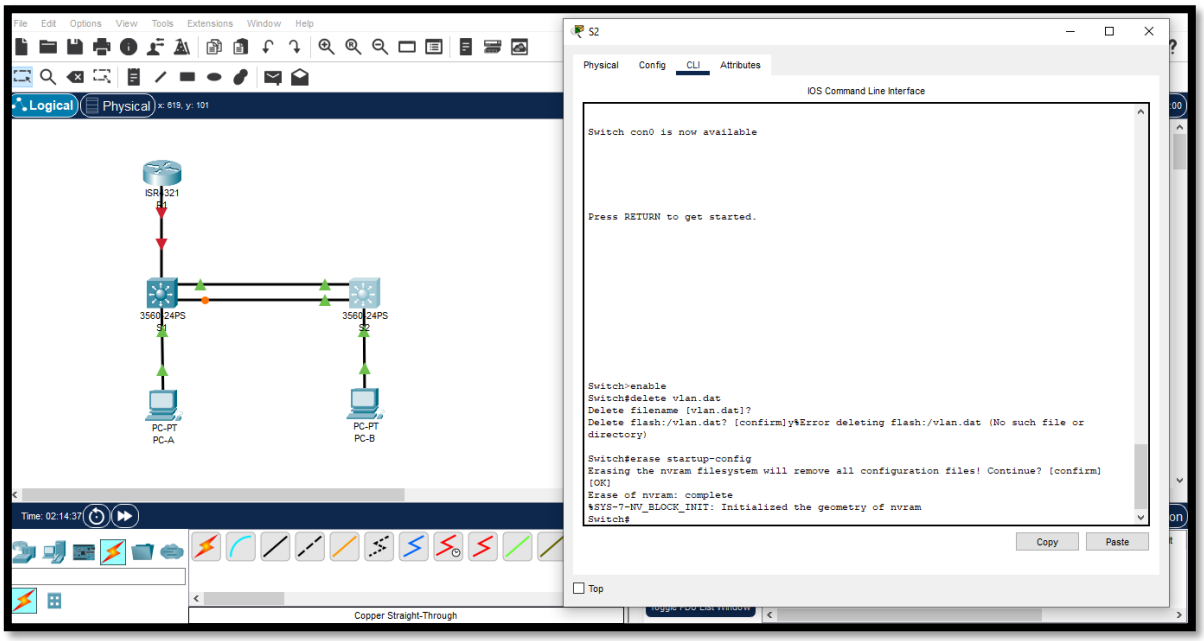
Fuente: Autor

Figura 14 Cargar archivos S1



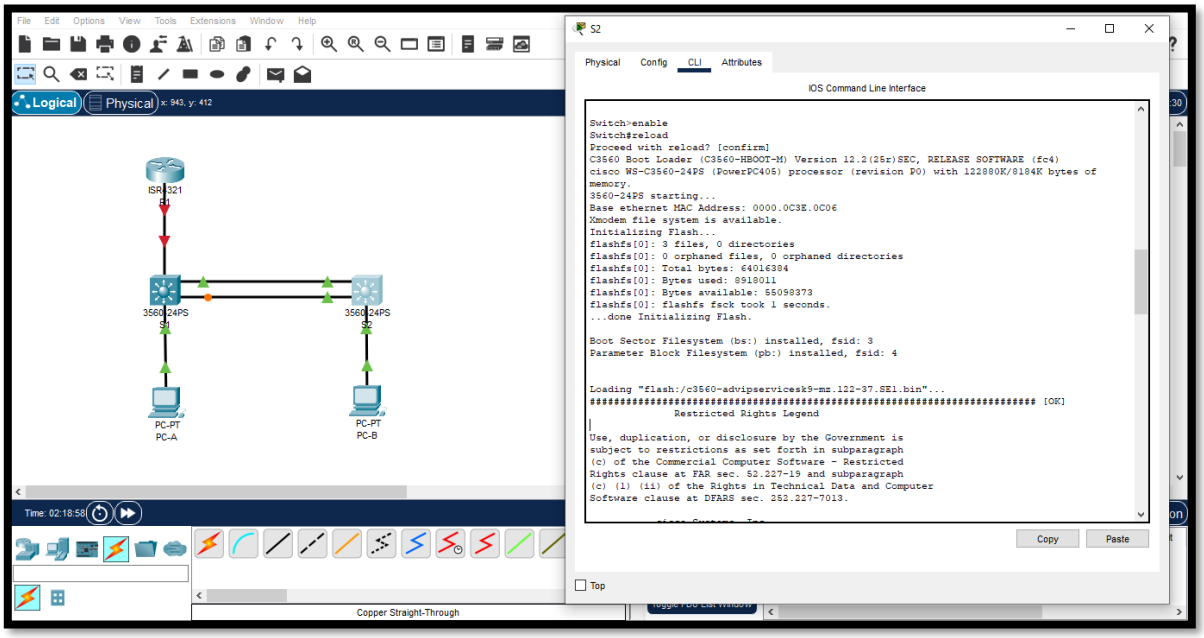
Fuente: Autor

Figura 15 Eliminar archivos configuración S2 y datos VLAN



Fuente: Autor

Figura 16 Cargar archivos S2

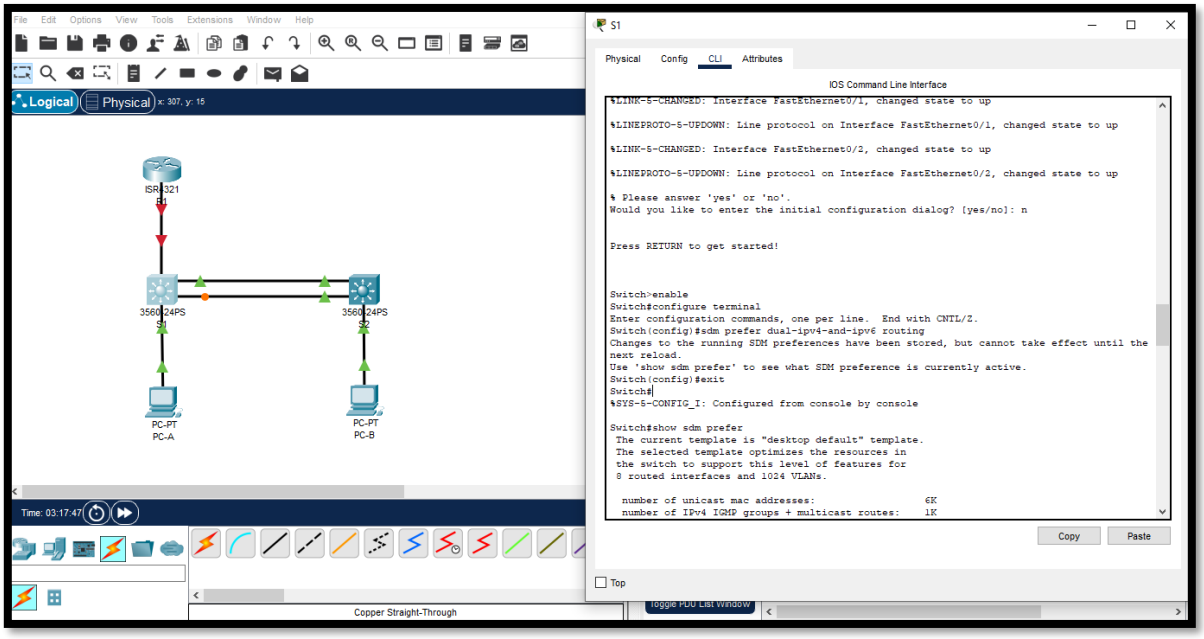


Fuente: Autor

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

Tarea	Especificación
Cargar plantilla SDM en S1	Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#sdm prefer dual-ipv4-and-ipv6 routing Changes to the running SDM preferences have been stored, but cannot take effect until the next reload.

Figura 17 Cargar plantilla SDM en S1



Fuente: Autor

2.5 Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#
Nombre del router	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#hostname R1 R1(config)#
Nombre de dominio	R1>enable R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ip domain-name ccna-sa.com R1(config)#
Contraseña cifrada para el modo EXEC privilegiado	R1>enable R1#configure terminal

	Enter configuration commands, one per line. End with CNTL/Z. R1(config)# enable secret class R1(config)#
Contraseña de acceso a la consola	R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit R1(config)#
Establecer la longitud mínima para las contraseñas	User Access Verification Password: R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#security passwords min-length 5 R1(config)#
Crear un usuario administrativo en la base de datos local	User Access Verification Password: R1>enable Password:

	R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#username admin password admin1pass R1(config)#
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	User Access Verification Password: R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#line vty 0 15 R1(config-line)#login local R1(config-line)#exit R1(config)#
Configurar VTY solo aceptando SSH	User Access Verification Password: R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#line vty 0 15 R1(config-line)#transport input ssh R1(config-line)#exit

	R1(config)#
Tarea	**Especificación**
Cifrar las contraseñas de texto no cifrado	User Access Verification Password: R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#service password-encryption R1(config)#exit R1#
Configure un MOTD Banner	User Access Verification Password: R1>enable Password: R1#enable R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#banner motd #R1 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas# R1(config)#exit R1#

Habilitar el routing IPv6	R1 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password: R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ipv6 unicast-routing R1(config)#exit R1#
Configurar interfaz G0/0/1 y subinterfaces	R1 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password: R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#interface gigabitEthernet 0/0/1.20 R1(config-subif)#encapsulation dot1Q 20 R1(config-subif)#description vlan Docentes R1(config-subif)#ip address 10.53.8.1 255.255.255.192

	R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#exit R1(config)#interface gigabitEthernet 0/0/1.30 R1(config-subif)#encapsulation dot1Q 30 R1(config-subif)#description vlan Estudiantes R1(config-subif)#ip address 10.53.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#exit R1(config)#interface gigabitEthernet 0/0/1.40 R1(config-subif)#encapsulation dot1Q 40 R1(config-subif)#description vlan Invitados R1(config-subif)#ip address 10.53.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64

	R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#exit R1(config)#interface gigabitEthernet 0/0/1.56 R1(config-subif)#encapsulation dot1Q 56 R1(config-subif)#description vlan Native R1(config-subif)#exit R1(config)#interface gigabitEthernet 0/0/1 R1(config-if)#no shutdown
Configure el Loopback0 interface	R1 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password: R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#interface loopback 0 R1(config-if)# %LINK-5-CHANGED: Interface Loopback0, changed state to up

	%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#description Loopback R1(config-if)#exit
Generar una clave de cifrado RSA	R1 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password: R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#crypto key generate rsa The name for the keys will be: R1.ccna-sa.com Choose the size of the key modulus in the range of 360 to 2048 for your

	General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non- exportable...[OK] R1(config)#

2.6 Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente: **S1**

Tarea	**Especificación**
Desactivar la búsqueda DNS.	Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain- lookup Switch(config)#exit Switch#
Nombre del switch	Switch> Switch>enable

	Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#hostname S1 S1(config)#
Nombre de dominio	S1>enable S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#ip domain-name ccna-sa.com S1(config)#exit S1#
Contraseña cifrada para el modo EXEC privilegiado	S1>enable S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#enable secret class S1(config)#exit S1#
Contraseña de acceso a la consola	S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login

	S1(config-line)#exit S1(config)#exit S1#
Crear un usuario administrativo en la base de datos local	User Access Verification Password: S1>enable Password: Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#username admin password admin1pass S1(config)#exit S1#
Tarea	**Especificación**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	User Access Verification Password: S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#line vty 0 15 S1(config-line)#login local S1(config-line)#exit S1(config)#exit

	S1#
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	User Access Verification Password: S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#line vty 0 15 S1(config-line)#transport input ssh S1(config-line)#exit S1(config)#exit S1#
Cifrar las contraseñas de texto no cifrado	User Access Verification Password: S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#service password-encryption S1(config)#exit S1#
Configurar un MOTD Banner	User Access Verification Password: S1>enable

	Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#banner motd #S1 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas# S1(config)#exit S1#
Generar una clave de cifrado RSA	S1 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password: S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#crypto key generate rsa The name for the keys will be: S1.ccna-sa.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

	How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] S1(config)#
Configurar la interfaz de administración (SVI)	S1 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password: S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#interface vlan 40 S1(config-if)#ip address 10.53.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#description vlan Invitados S1(config-if)#no shutdown S1(config)#
Configuración del gateway predeterminado	S1 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas

	User Access Verification Password: S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#ip default-gateway 10.53.8.97 S1(config)#exit S1#

Las tareas de configuración incluyen lo siguiente: **S2**

Tarea	**Especificación**
Desactivar la búsqueda DNS.	Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup Switch(config)#exit Switch#
Nombre del switch	Switch> Switch>enable Switch#configure terminal

	Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#hostname S1 S2(config)#
Nombre de dominio	S2>enable S2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S2(config)#ip domain-name ccna-sa.com S2(config)#exit S2#
Contraseña cifrada para el modo EXEC privilegiado	S2>enable S2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S2(config)#enable secret class S2(config)#exit S2#
Contraseña de acceso a la consola	S2>enable Password: S2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S2(config)#line console 0 S2(config-line)#password cisco S2(config-line)#login S2(config-line)#exit

	S2(config)#exit S2#
Crear un usuario administrativo en la base de datos local	User Access Verification Password: S2>enable Password: Password: S2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S2(config)#username admin password admin1pass S2(config)#exit S2#
Tarea	**Especificación**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	User Access Verification Password: S2>enable Password: S2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S2(config)#line vty 0 15 S2(config-line)#login local S2(config-line)#exit S2(config)#exit S2#

Configurar las líneas VTY para que acepten únicamente las conexiones SSH	User Access Verification Password: S2>enable Password: S2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S2(config)#line vty 0 15 S2(config-line)#transport input ssh S2(config-line)#exit S2(config)#exit S2#
Cifrar las contraseñas de texto no cifrado	User Access Verification Password: S2>enable Password: S2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S2(config)#service password-encryption S2(config)#exit S2#
Configurar un MOTD Banner	User Access Verification Password: S2>enable Password: S2#configure terminal

	Enter configuration commands, one per line. End with CNTL/Z. S2(config)#banner motd #S2 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas# S2(config)#exit S2#
Generar una clave de cifrado RSA	S2 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password: S2>enable Password: S2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S2(config)#crypto key generate rsa The name for the keys will be: S2.ccna-sa.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024

	% Generating 1024 bit RSA keys, keys will be non-exportable...[OK] S2(config)#
Configurar la interfaz de administración (SVI)	S2 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password: S1>enable Password: S2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S2(config)#interface vlan 40 S2(config-if)#ip address 10.53.8.99 255.255.255.248 S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#ipv6 address fe80::99 link-local S2(config-if)#description vlan Invitados S2(config-if)#no shutdown S2(config-if)#exit
Configuración del gateway predeterminado	S2 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password:

	S2>enable Password: S2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S2(config)#ip default-gateway 10.53.8.97 S2(config)#exit S2#

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

2.8 Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tarea	Especificación
Crear VLAN	S1 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password: S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#vlan 20 S1(config-vlan)#name Docentes S1(config-vlan)#exit S1(config)#vlan 30

	S1(config-vlan)#name Estudiantes S1(config-vlan)#exit S1(config)#vlan 40 S1(config-vlan)#name Invitados S1(config-vlan)#exit S1(config)#vlan 50 S1(config-vlan)#name Usuarios S1(config-vlan)#exit S1(config)#vlan 56 S1(config-vlan)#name Native S1(config-vlan)#exit S1(config)#
Tarea	**Especificación**
Crear troncos 802.1Q que utilicen la VLAN 56 nativa	S1 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password: S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z S1(config)#interface fastEthernet 0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 56 S1(config-if)#shutdown

	S1(config)#interface range fastEthernet 0/1-2 S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if)#switchport trunk native vlan 56 S1(config-if)#shutdown
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password: S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#int range f0/1-2 S1(config-if-range)#channel-protocol lacp S1(config-if-range)#channel-group 1 mode active S1(config-if-range)# Creating a port-channel interface Port-channel 1 %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

	%EC-5-CANNOT_BUNDLE2: Fa0/1 is not compatible with Po1 and will be suspended (vlan mask is different) %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down %EC-5-CANNOT_BUNDLE2: Fa0/2 is not compatible with Po1 and will be suspended (vlan mask is different) S1(config-if-range)#exit S1(config)#
Configurar el puerto de acceso de host para VLAN 20	S1 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password: S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#int f0/6 S1(config-if)#switchport mode access

	S1(config-if)#switchport access vlan 20 S1(config-if)#exit S1(config)#exit S1#
Configurar la seguridad del puerto en los puertos de acceso	S1 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password: S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#int f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport port-security maximum 4 S1(config-if)#switchport port-security violation shutdown S1(config-if)#exit S1(config)#exit S1#
Proteja todas las interfaces no utilizadas	S1 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password: S1>enable

	Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#interface range f0/3-4,f0/7-9,f0/11-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#description " Asignacion de seguridad VLAN 50 " S1(config-if-range)#shutdown %LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

	%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

	%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

	%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down S1(config-if-range)# S1(config-if-range)#exit S1(config)#

2.9 Paso 5: Configure el S2.

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

Tarea	Especificación
Crear VLAN	S2 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password: S2>enable Password: S2# %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up S2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S2(config)#vlan 20 S2(config-vlan)#name Docentes S2(config-vlan)#exit S2(config)#vlan 30 S2(config-vlan)#name Estudiantes S2(config-vlan)#exit S2(config)#vlan 40 S2(config-vlan)#name Invitados S2(config-vlan)#exit S2(config)#vlan 50 S2(config-vlan)#name Usuarios S2(config-vlan)#exit S2(config)#vlan 56 S2(config-vlan)#name Native S2(config-vlan)#exit S2(config)#
Crear troncos 802.1Q que utilicen la VLAN 56 nativa	S2 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password: S2>enable

	Password: S2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S2(config)#interface range f0/1,f0/2 S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk allowed vlan 56 S2(config-if-range)#exit S2(config)#
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S2 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password: S2>enable Password: S2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S2(config)#int range f0/1-2 S2(config-if-range)#channel-protocol lacp S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#

	Creating a port-channel interface Port-channel 1 %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down %EC-5-CANNOT_BUNDLE2: Fa0/1 is not compatible with Po1 and will be suspended (vlan mask is different) %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down %EC-5-CANNOT_BUNDLE2: Fa0/2 is not compatible with Po1 and will be suspended (vlan mask is different) S2(config-if-range)#exit S2(config)#
Configurar el puerto de acceso del host para la VLAN 30	S2 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password:

	S2>enable Password: S2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S2(config)#int f0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 30 S2(config-if)#exit S2(config)#
Tarea	**Especificación**
Configure port-security en los access ports	S2 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password: S2>enable Password: S2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S2(config)#int f0/18 S2(config-if)#switchport port-security Maximum 4 S2(config-if)#switchport port-security

	S2(config-if)#switchport port-security violation shutdown S2(config-if)#exit S2(config)#
Asegure todas las interfaces no utilizadas.	S2 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password: S2>enable Password: S2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S2(config)#int range f0/3-17,f0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 50 S2(config-if-range)#exit

2.10 Parte 2: Configurar soporte de host

2.11 Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Configure Default Routing	R1 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password: R1>enable Password: R1#configure terminal R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0 R1(config)#
Configurar IPv4 DHCP para VLAN 20	R1 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password: R1>enable Password: R1#configure terminal R1(config)#ip dhcp excluded-address 10.53.8.1 10.53.8.53 R1(config)#ip dhcp pool vlan20-Docentes R1(dhcp-config)#network 10.53.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.53.8.1 R1(dhcp-config)#domain-name unad-ccna-sa.net R1(dhcp-config)#exit

Configurar DHCP IPv4 para VLAN 30	R1 - Paola Andrea Martinez Aguirre - Ingenieria de Sistemas User Access Verification Password: R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(dhcp-config)#ip dhcp excluded-address 10.53.8.65 10.53.8.84 R1(config)#ip dhcp pool vlan30-Estudiantes R1(dhcp-config)#network 10.53.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.53.8.56 R1(dhcp-config)#ip domain-name unad-ccna-sb.net

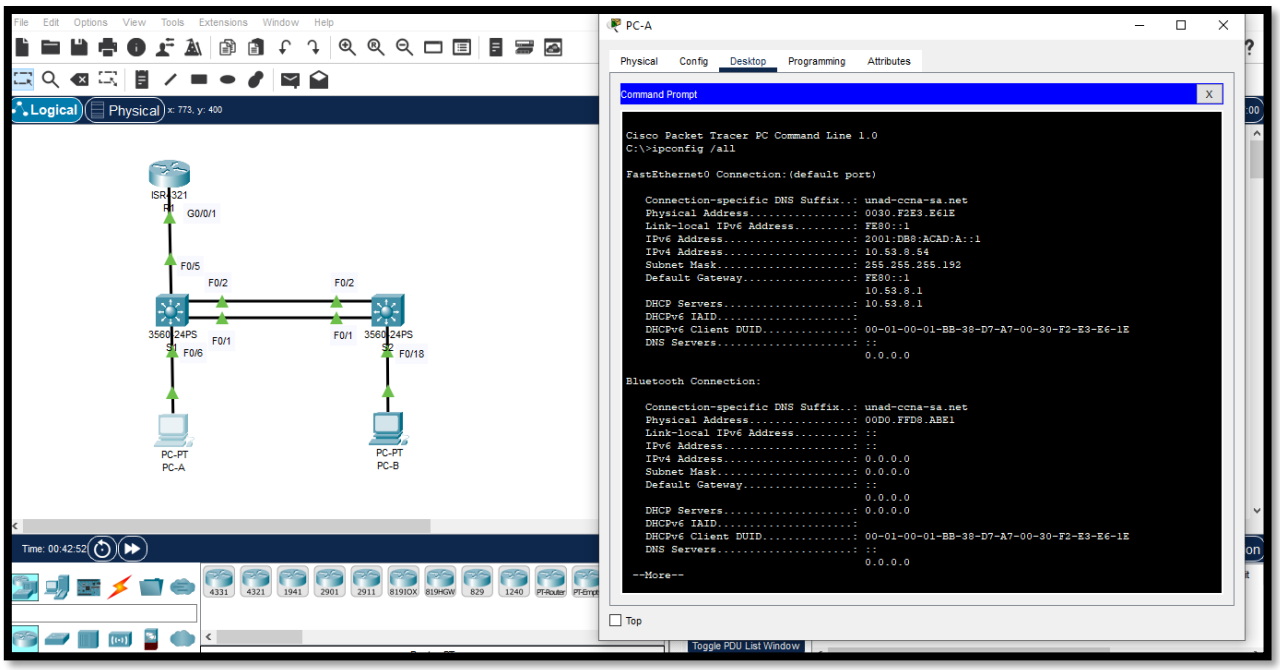
2.12 Paso 2: Configurar los servidores

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

Configuración de red de PC-A	
Descripción	**PC-A**
Dirección física	0030.F2E3.E61E

Dirección IP	10.53.8.54 - 2001:DB8:ACAD:A::1
Máscara de subred	255.255.255.192
Gateway predeterminado	10.53.8.1
Gateway predeterminado IPv6	FE80::1

Figura 18 Ipconfig/all en PC-A

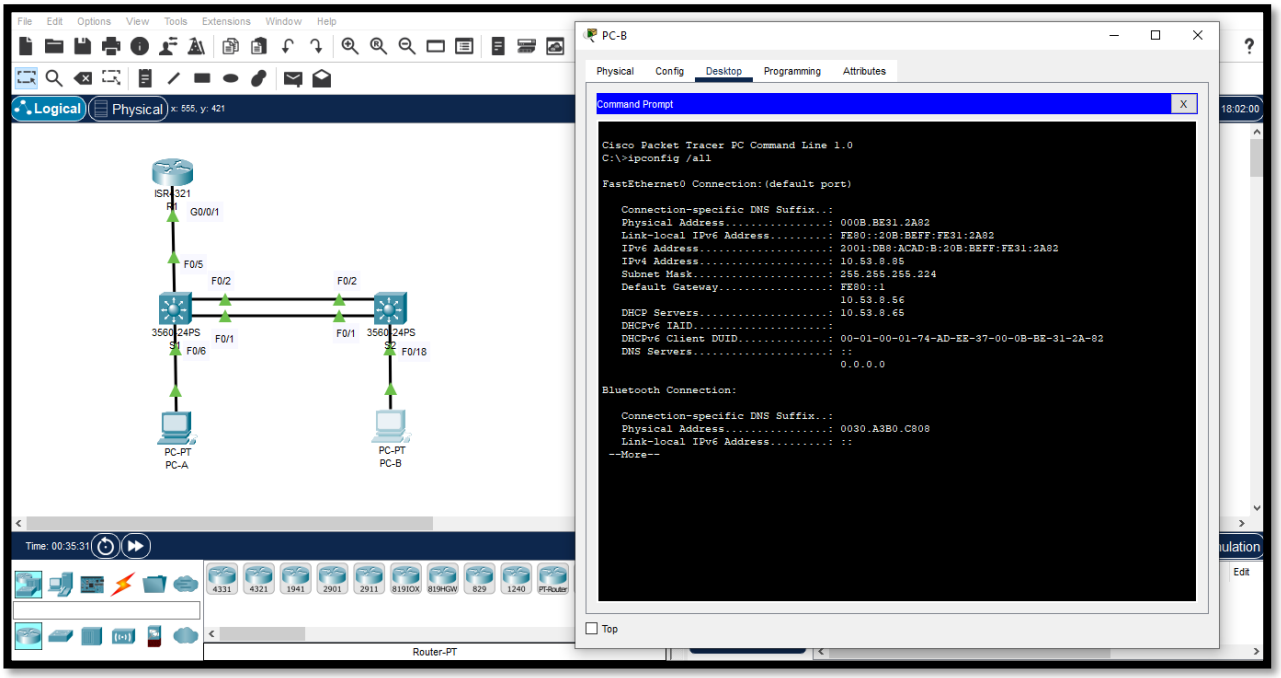


Fuente: Autor

Configuración de red de PC-B	
Descripción	**PC-B**
Dirección física	000B.BE31.2A82
Dirección IP	2001:DB8:ACAD:B:20B:BEFF:FE31:2A82 10.53.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.53.8.65

Gateway predeterminado IPv6	FE80::1

Figura 19 Ipconfig/all en PC-B



Fuente: Autor

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

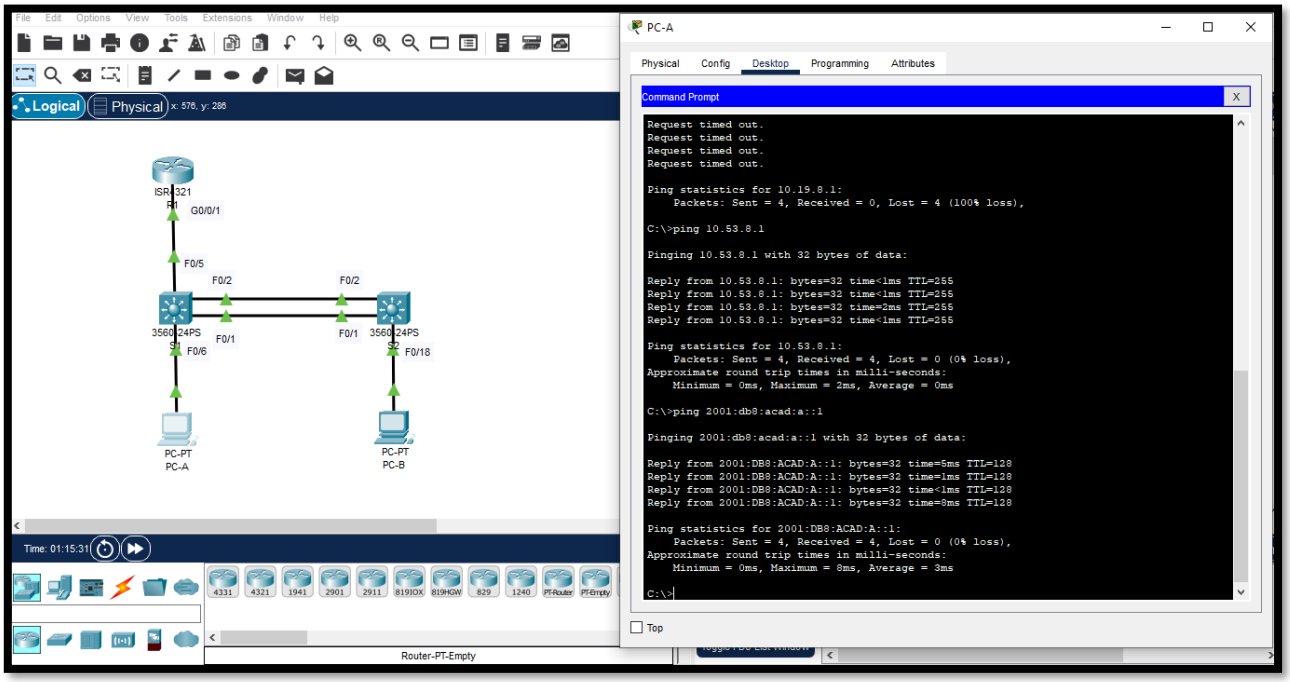
Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

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

Desde	A		Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.20	IPv4	10.53.8.1	Correcto
		IPv6	2001:db8:acad:a::1	Correcto
	R1, G0/0/1.30	IPv4	10.53.8.65	Correcto
		IPv6	2001:db8:acad:b::1	No correcto
	R1, G0/0/1.40	IPv4	10.53.8.97	Correcto
		IPv6	2001:db8:acad:c: :1	No Correcto
	S1, VLAN 40	IPv4	10.53.8.98	Correcto
		IPv6	2001:db8:acad:c: :98	No correcto
Desde	**A**		**Dirección IP**	**Resultados de ping**
	S2, VLAN 40	IPv4	10.53.8.99	Correcto
		IPv6	2001:db8:acad:c: :99	No Correcto
	PC-B	IPv4	10.53.8.85	Correcto
		IPv6	2001:DB8:ACAD:B:20B:BEFF:FE31:2A82	No Correcto
	R1 Bucle 0	IPv4	209.165.201.1	Correcto
		IPv6	2001:db8:acad:209::1	No correcto
PC-B	R1 Bucle 0	IPv4	209.165.201.1	Correcto
		IPv6	2001:db8:acad:209::1	Correcto
		IPv4	10.53.8.1	Correcto

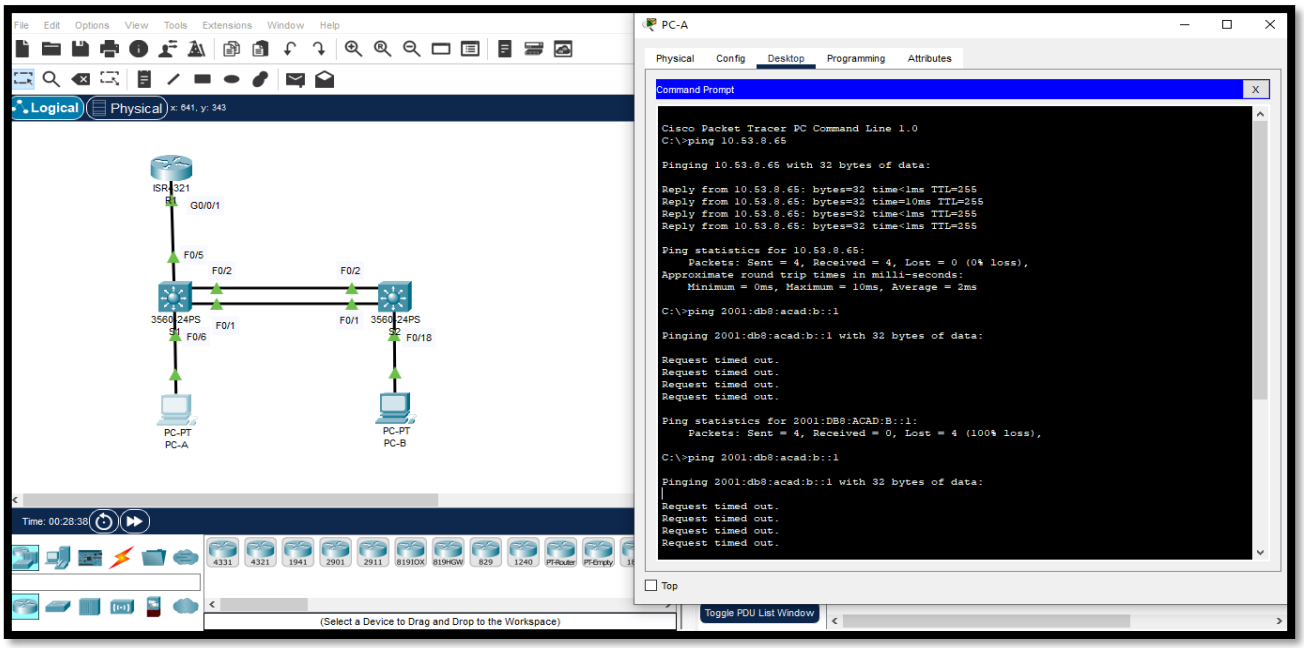
	R1, G0/0/1.20	IPv6	2001:db8:acad:a: :1	Correcto
	R1, G0/0/1.30	IPv4	10.53.8.65	Correcto
		IPv6	2001:db8:acad:b: :1	Correcto
	R1, G0/0/1.40	IPv4	10.53.8.97	Correcto
		IPv6	2001:db8:acad:c: :1	Correcto
	S1, VLAN 40	IPv4	10.53.8.98	Correcto
		IPv6	2001:db8:acad:c: :98	No correcto
	S2, VLAN 40	IPv4	10.53.8.99	Correcto
		IPv6	2001:db8:acad:c: :99	No correcto

Figura 20 Conectividad desde PC-A a IP 10.53.8.1 e IP 2001:db8:acad:a::1



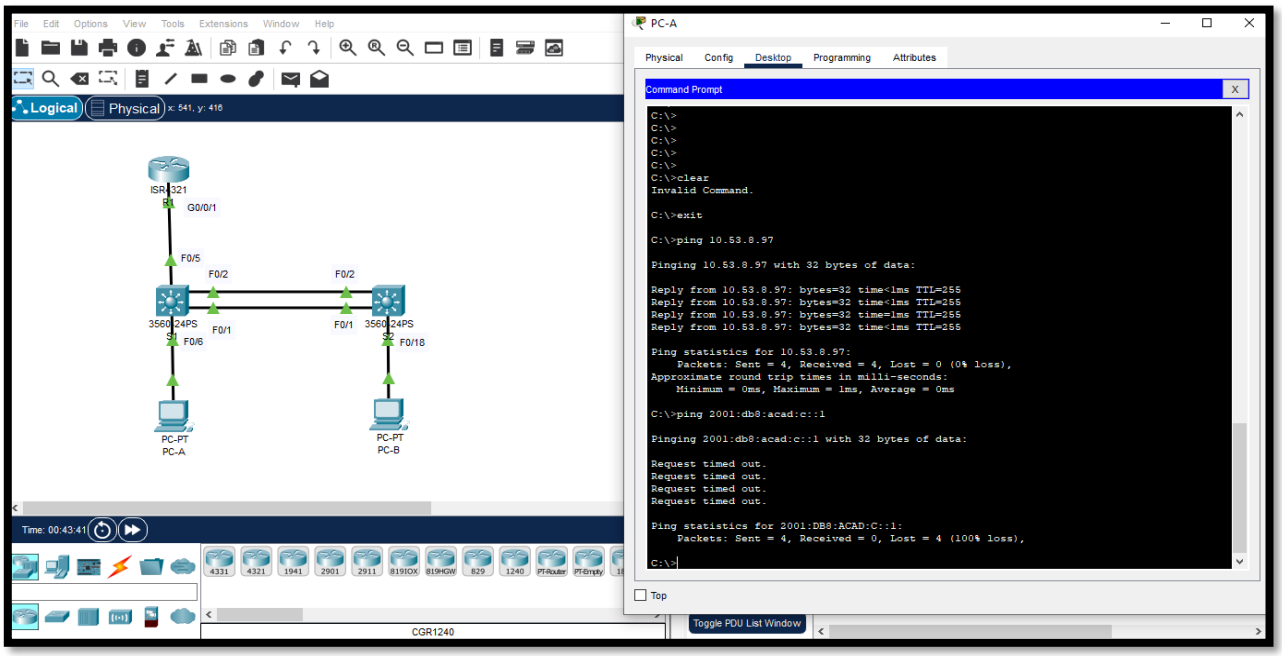
Fuente: Autor

Figura 21 Conectividad desde PC-A a IP 10.53.8.65 e IP 2001:db8:acad:b::1



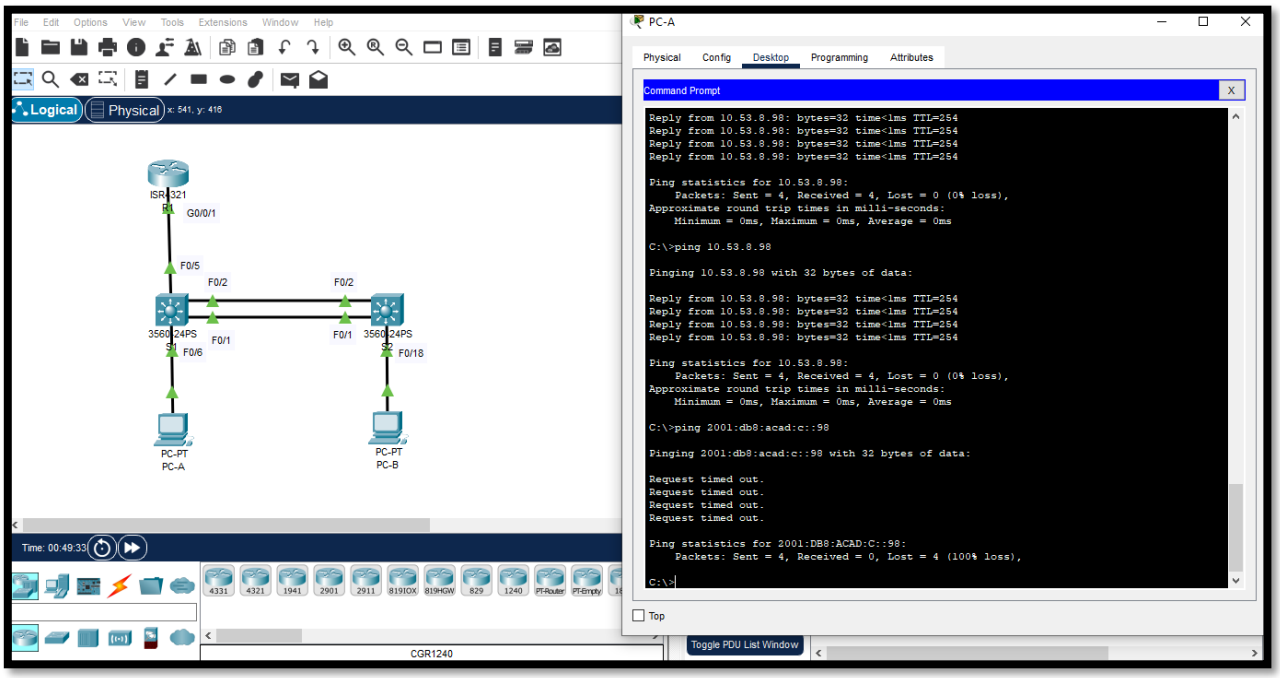
Fuente: Autor

Figura 22 Conectividad desde PC-A a IP 10.53.8.97 e IP 2001:db8:acad:c::1



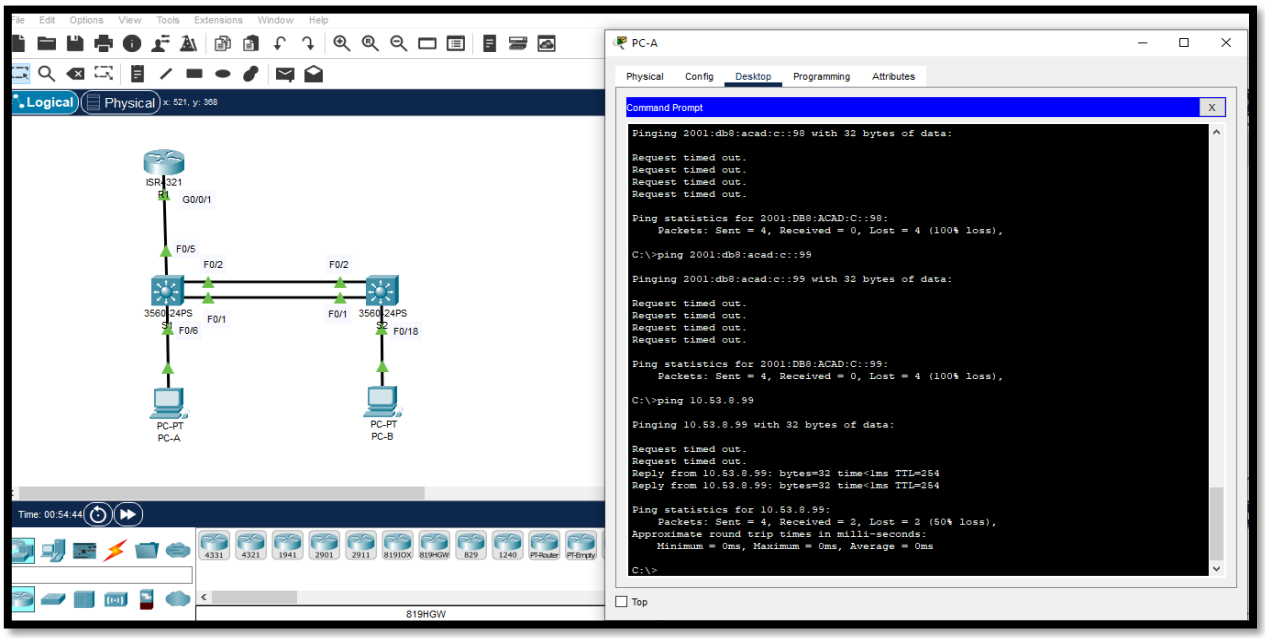
Fuente: Autor

Figura 23 Conectividad desde PC-A a IP 10.53.8.98 e IP 2001:db8:acad:c::98



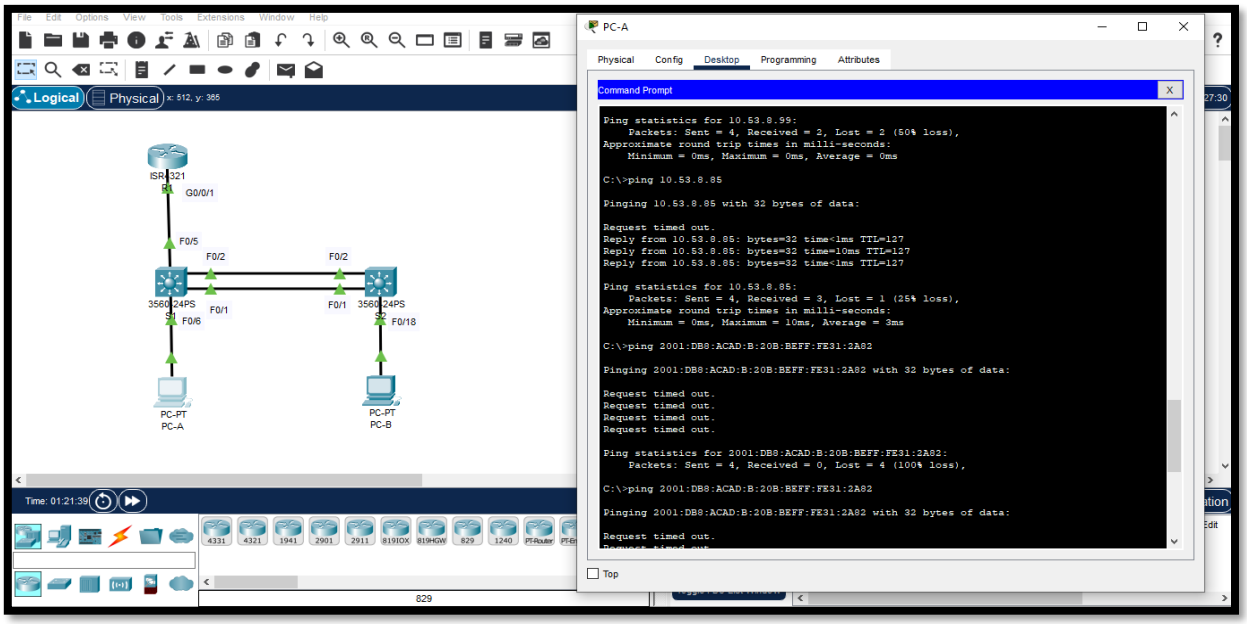
Fuente: Autor

Figura 24 Conectividad desde PC-A a IP 10.53.8.99 e IP 2001:db8:acad:c::99



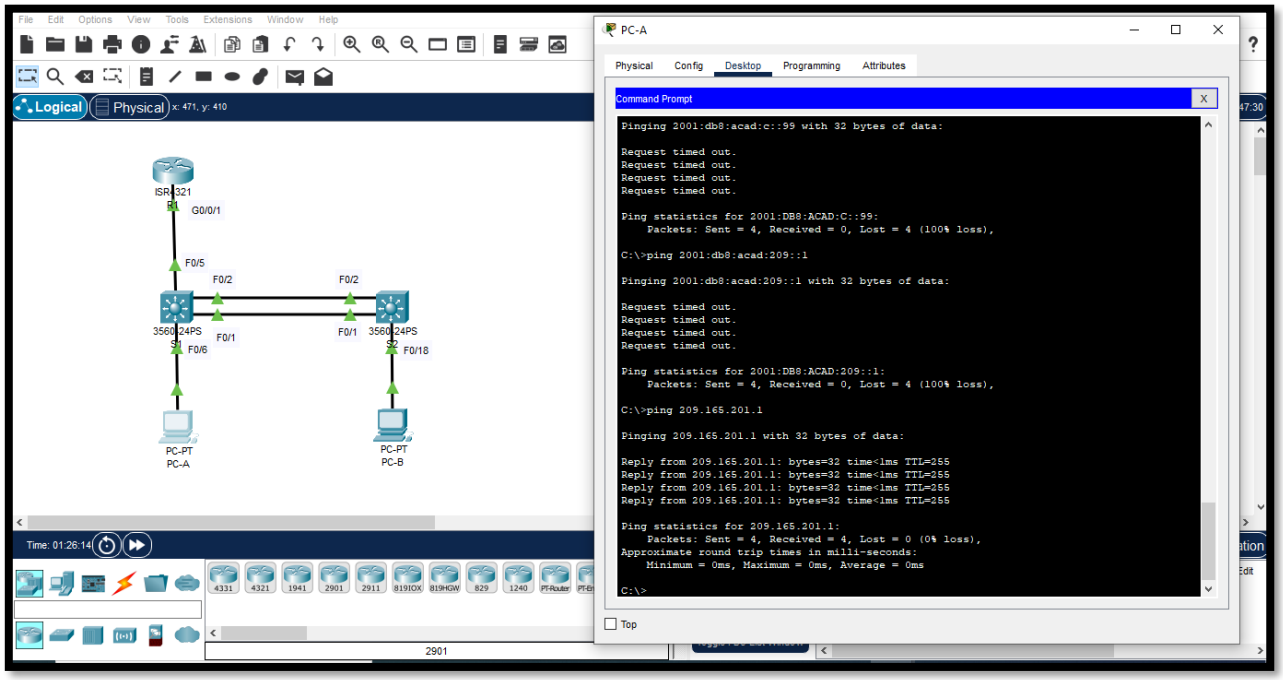
Fuente: Autor

Figura 25 Conectividad desde PC-A a IP 10.53.8.85 e IP 2001:DB8:ACAD:B:20B:BEFF:FE31:2A82



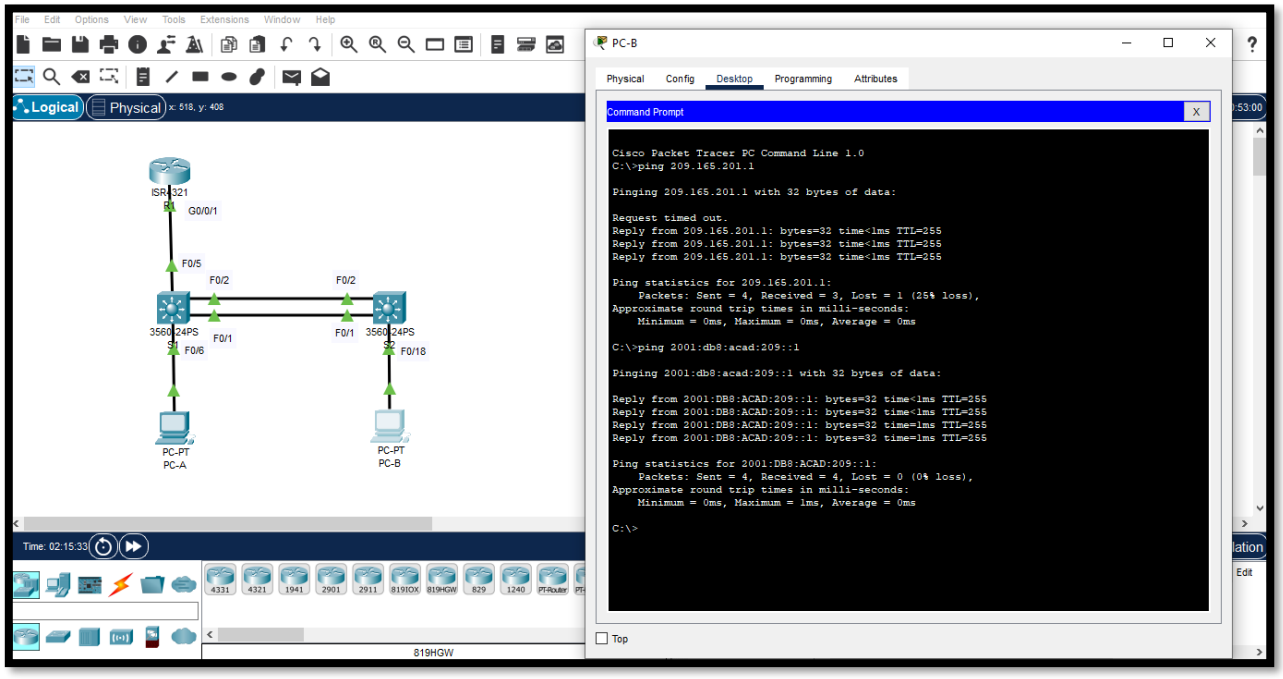
Fuente: Autor

Figura 26 Conectividad desde PC-A a IP 209.165.201.1 e IP 2001:db8:acad:209::1



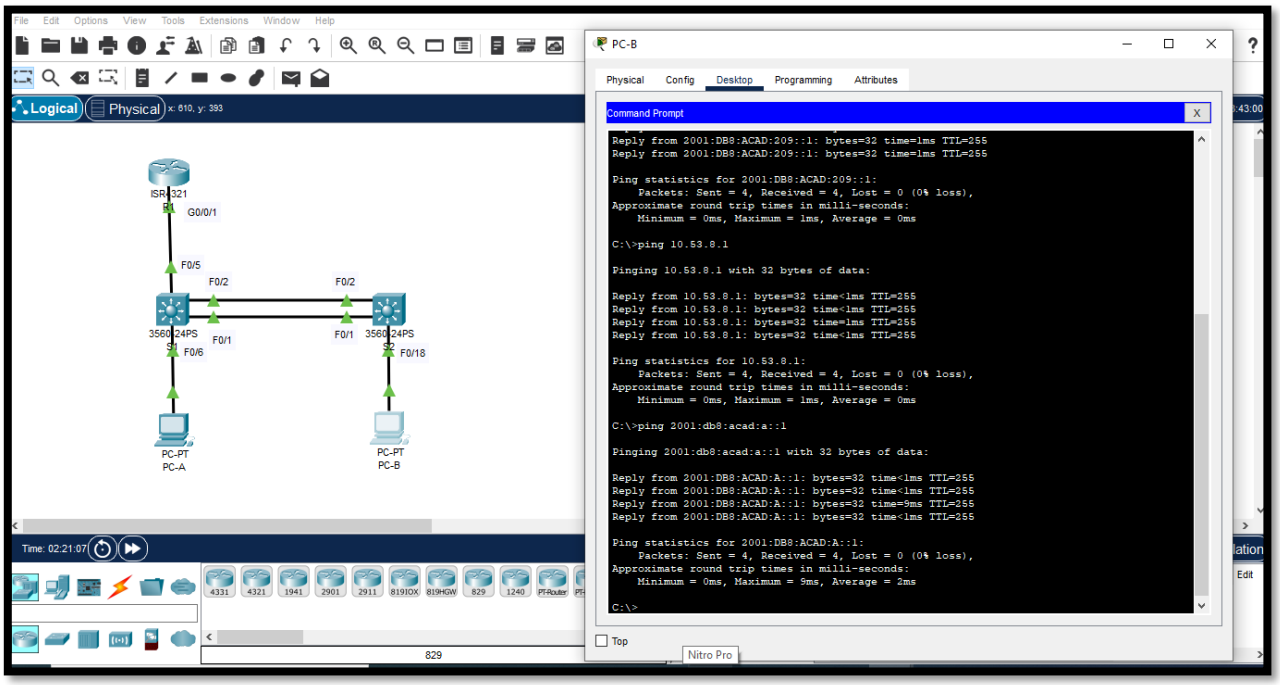
Fuente: Autor

Figura 27 Conectividad desde PC-B a IP 209.165.201.1 e IP 2001:db8:acad:209::1



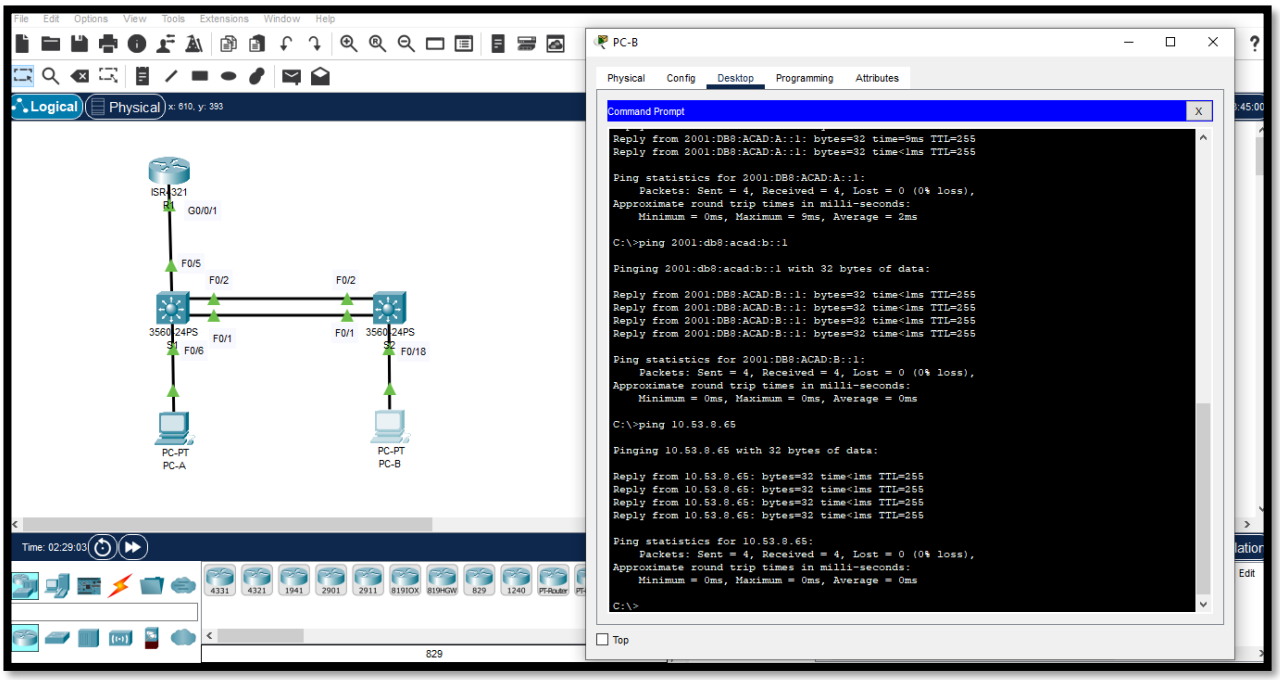
Fuente: Autor

Figura 28 Conectividad desde PC-B a IP 10.53.8.1 e IP 2001:db8:acad:a::1



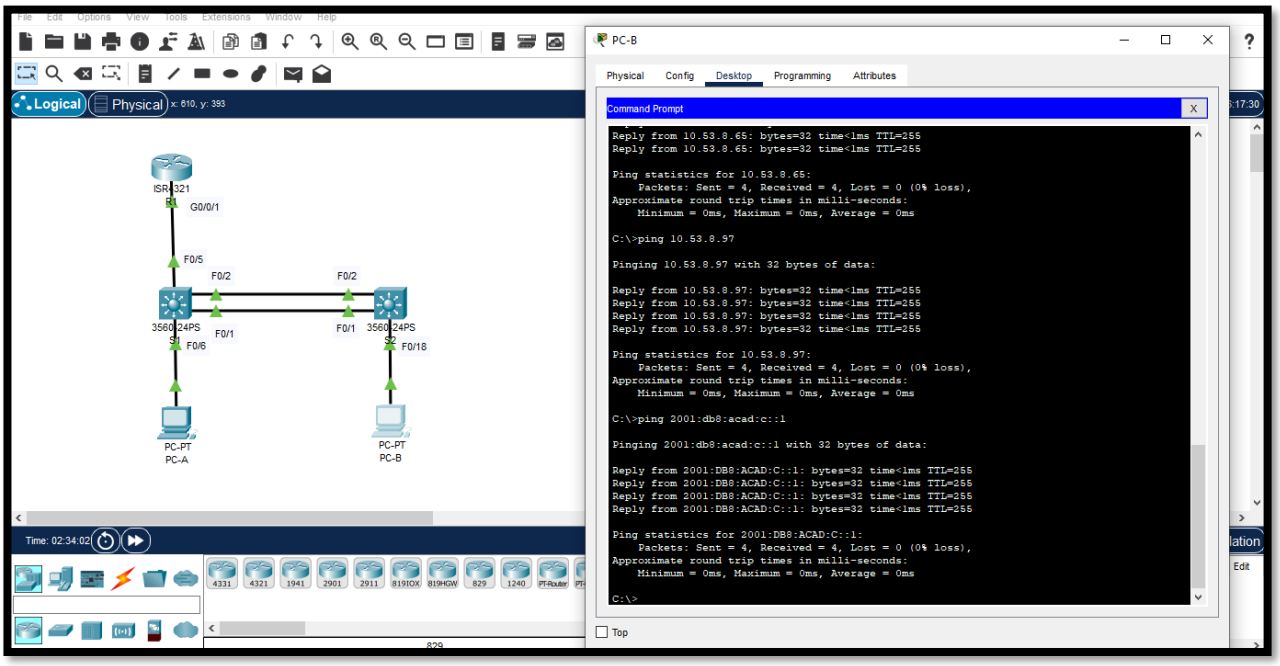
Fuente: Autor

Figura 29 Conectividad desde PC-B a IP 10.53.8.65 e IP 2001:db8:acad:b::1



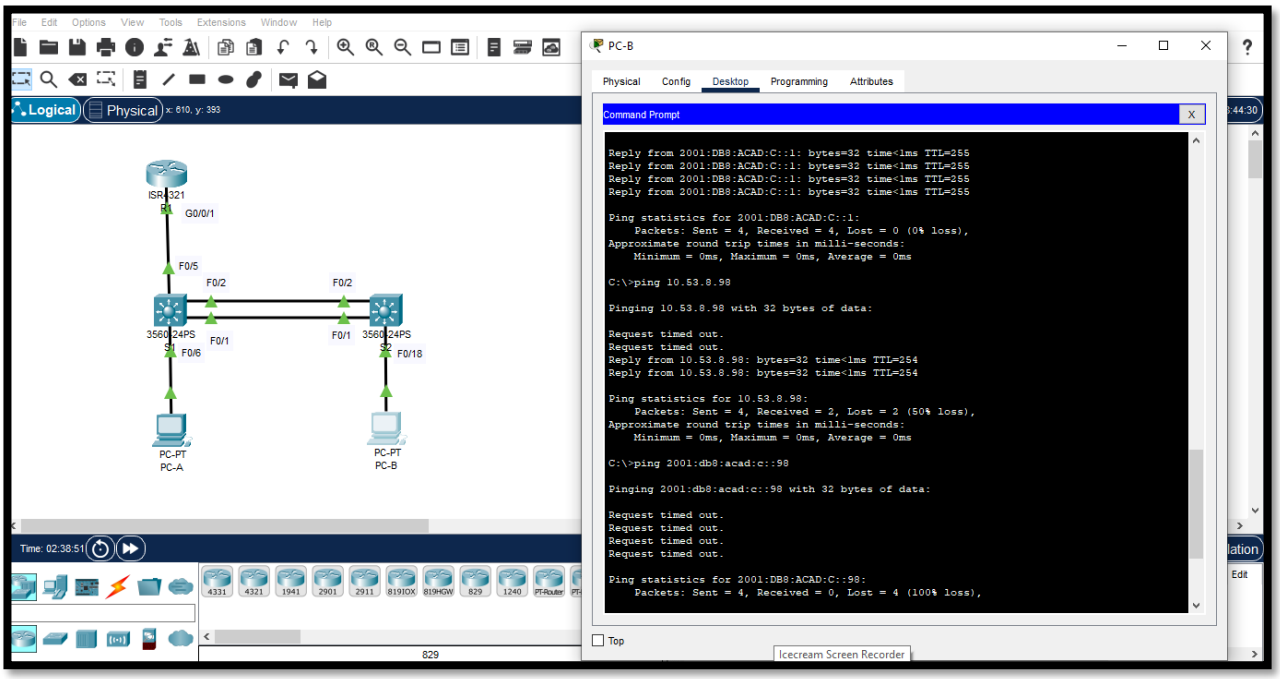
Fuente: Autor

Figura 30 Conectividad desde PC-B a IP 10.53.8.97 e IP 2001:db8:acad:c::1



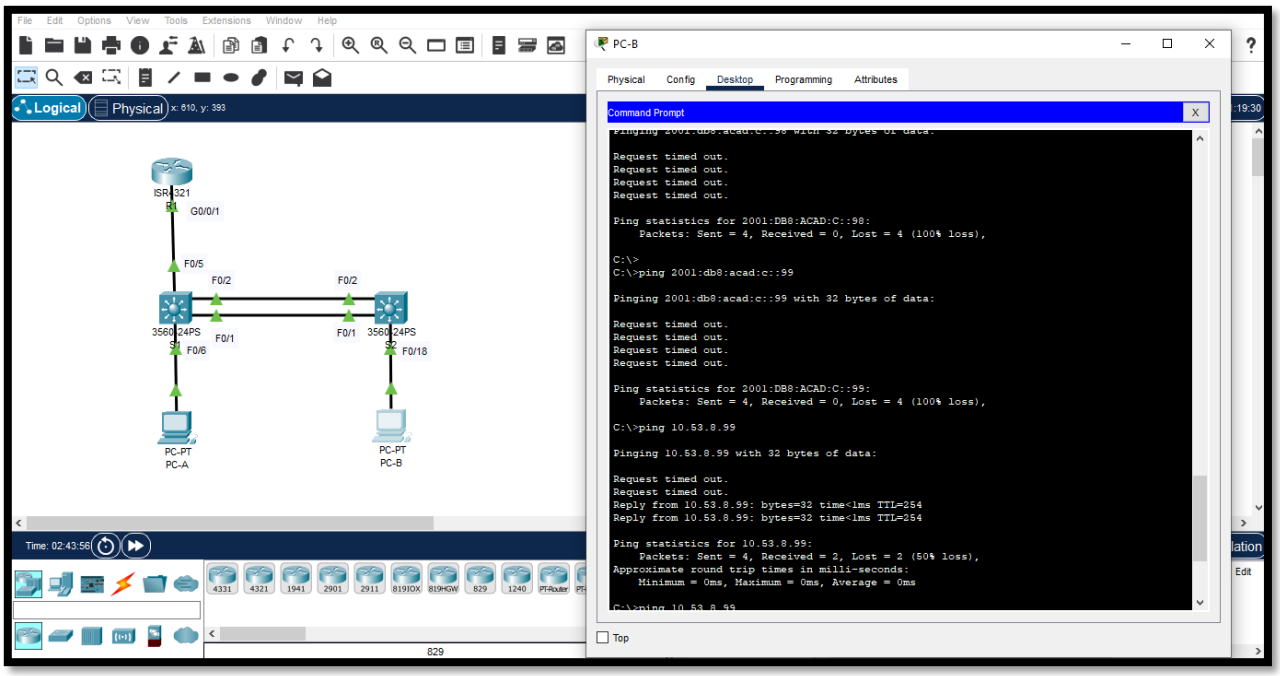
Fuente: Autor

Figura 31 Conectividad desde PC-B a IP 10.53.8.98 e IP 2001:db8:acad:c::98



Fuente: Autor

Figura 32 Conectividad desde PC-B a IP 10.53.8.99 e IP 2001:db8:acad:c::99



Fuente: Autor

CONCLUSIONES

Con el primer escenario podemos observar que las configuraciones básicas en el router y el switch son para mejorar la seguridad entre ellos como la optimización de la red, esto nos garantiza que cuando se quiera conectar vía telnet o a través de la consola podamos trabajar con seguridad.

Por medio de las verificaciones podemos garantizar que los enrutamientos que se realizaron el router y switch este correctas y al hacer ping desde los dispositivos de la red el porcentaje de comunicación es el 100% de datos recibidos.

Se aprendió que con el uso subredes por medio del manejo de Vlan podemos ampliar el numero de equipos haciendo el uso del encapsulamiento Do1Q y del modo Trunk, para hacer una mejor comunicación como la ampliación de elementos en una red.

REFERENCIAS BIBLIOGRAFICAS

CISCO. “División de redes IP en subredes. Fundamentos de Networking”. {En línea}. (2019). {25 noviembre de 2020}. Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

IONOS, Digital Guide. ¿qué es y cómo funciona? {18 de octubre de 2020} Disponible en: https://www.ionos.es/digitalguide/servidores/know-how/broadcast/

IONOS, Digital Guide. Conoce los tipos de redes más importantes. {18 de octubre de 2022} Disponible en: https://www.ionos.es/digitalguide/servidores/know-how/los-tipos-de-redes-mas-conocidos/

IONOS, Startupguide. La extranet y sus beneficios para las empresas. {18 de octubre de 2022} Disponible en: https://www.ionos.es/startupguide/productividad/extranet/

IONOS, Startupguide. La extranet y sus beneficios para las empresas. {18 de octubre de 2022} Disponible en: https://www.ionos.es/startupguide/productividad/extranet/

IONOS, Startupguide. La extranet y sus beneficios para las empresas. {18 de octubre de 2022} Disponible en: https://www.ionos.es/startupguide/productividad/extranet/

JIMÉNEZ, Javier. Qué es y para qué sirve el SSH. RedesZone. {13 de octubre de 2021} Disponible en: https://www.redeszone.net/tutoriales/internet/protocolo-ssh-usos/

ORACLE. Sondeo de hosts remotos con el comando ping. {18 de octubre de 2022} Disponible en: https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-admintasks-53/index.html

TECHLIB. Definición de PDU (Unidad de datos de protocolo) {18 de octubre de 2022} Disponible en: https://techlib.net/definition/pdu.html

VESGA, J. Diseño y configuración de redes con Packet Tracer [OVA]. {En línea}. (2014). {25 de noviembre de 2020}. Disponible en: https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

WALTON, Alex. Acceso a Cisco IOS. CCNA desde Cero. { 4 de julio de 2020} Disponible en: https://ccnadesdecero.es/acceso-a-cisco-ios/

ANEXOS

Anexo A - Descarga de archivos de simulación.

Enlace:
https://drive.google.com/drive/folders/1OiavwOTBnwsmF4PxJjF7liENO5uqgrmE?usp=sharing