SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

ALEJANDRO CALDERON RIOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
CALI
2021

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

ALEJANDRO CALDERON RIOS

Diplomado de opción de grado presentado para optar el título de

INGENIERO DE SISTEMAS

DIRECTOR:
MSc. NANCY GUACA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
CALI
2021

NOTA DE ACEPTACION

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Cali, 17 de octubre del 2021

AGRADECIMIENTOS

A Dios, por permitir gozar de salud, fuerzas y voluntad de superación como parte de mi proyecto de vida en esta etapa final como profesional. A mi familia quien siempre ha estado presente con su apoyo incondicional y como motor e impulso para seguir en constante formación. A todo el gran equipo de la Universidad Nacional Abierta y a Distancia como excelentes tutores y directores dando ánimo y brindando ese acompañamiento día a día para que el alumno cumpla y finalice sus responsabilidades universitarias como profesional.

CONTENIDO

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

GLOSARIO

IPV4: Es un sistema de direccionamiento conformado por 32 bits, estos se usan para identificar un dispositivo en una red. Este a su vez es contenido por 4 octetos de 8 bits cada uno.

LAN: Red de área local, en el cual se conectan dispositivos o equipos informáticos.

VLAN: Tecnología de segmentación de tráfico en un mismo segmento de una ip, usualmente se configura en switch para agrupar interfaces físicas en un mismo dominio de broadcast.

PING: Comando usado para determinar el estado de un host remoto, por medio del protocolo ICMP.

ROUTER: Dispositivo para conectar computadoras y otros dispositivos a internet, funciona como un despachador y elige la ruta de mayor acceso para la conectividad.

SWITCH: Dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de are local (LAN) IEEE 802.3.

SUBNETEO: dividir una red ipv física en subredes lógicas, redes más pequeñas. De esta manera trabajarían de forma individual, pero pertenecen a la misma red física y al mismo dominio.

RESUMEN

Documentación de 02 escenarios, usando la herramienta de simulación packet tracer, donde para el escenario 1, se realizó subneteo con ipv4 “192.168.81.0”. El cual se crearon 02 subredes LAN 1 con 100 host y LAN 2 con 50 host. La configuración básica y necesaria de acuerdo con cada requerimiento y el uso de comando especiales para dar respuesta a esta red, posterior a esto que todos los dispositivos de esta topología puedan hacer conectividad.

Para el escenario 2, se complementaron esquemas, configuraciones y comandos ajustados para cumplir de acuerdo con los parámetros dados para el desarrollo de los temas vistos en el diplomado; tales como enrutamiento ipv6, OSPF, VLAN, DHCP, ACL, NAT. Aplicando los respectivos ajustes desde comandos la validación de cada dispositivo y confirmando por medio de las pruebas de conectividad.

Palabras Clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes.

ABSTRACT

Documentation of 02 scenarios, using the packet tracer simulation tool, where for scenario 1, subnetting with ipv4 “192.168.81.0” was performed. Which created 02 subnets LAN 1 with 100 hosts and LAN 2 with 50 hosts. The basic and necessary configuration according to each requirement and the use of special commands to respond to this network, after which all the devices in this topology can make connectivity.

For scenario 2, schemes, configurations and commands adjusted to comply with the parameters given for the development of the topics seen in the diploma were complemented; such as ipv6 routing, OSPF, VLAN, DHCP, ACL, NAT. Applying the respective settings from commands the validation of each device and confirming through the connectivity tests.

Keywords: CISCO, CCNP, Switching, Routing, Networks.

INTRODUCCION

Este trabajo como opción de grado del diplomado de profundización cisco CCNA1 y CCNA 2. Demuestra las habilidades, conceptos y desarrollos comprendidos desde el inicio del curso hasta la finalización de este, ahondando y fortaleciendo el aprendizaje en los contenidos y capítulos permitiendo obtener una experiencia positiva y en el transcurso de cada planteamiento e implementación a ejecutar con el visto, el apoyo y orientación por parte del tutor.

De acuerdo con esto, se mostrará la evidencia y soportes de lo aprendido estableciendo escenarios LAN/WAN, permitiendo hacer diagnóstico y análisis con los diferentes protocolos de enrutamiento, protocolos de administración de red desde IOS, también poder detectar y resolver problemas en una red, evaluar funcionalidad de routers y switches mediante el uso de los comandos para cada dispositivo.

Como respuesta a la estructura de implementación se usó el simulador packet tracer, apropiando lo visto en redes pequeñas desde la creación de direccionamiento ipv4 y ipv6, subredes, configuración inicial, básica y segura para los diferentes dispositivos y demás protocolos como OSPF, DHCP, ACL, NAT. Estos con el fin de dar una mayor confiablidad, escalabilidad, seguridad, funcionamiento, orden y control a una red, donde en esta actividad tenemos respuesta al escenario 1 y el escenario 2.

Desarrollo

1. Escenario 1

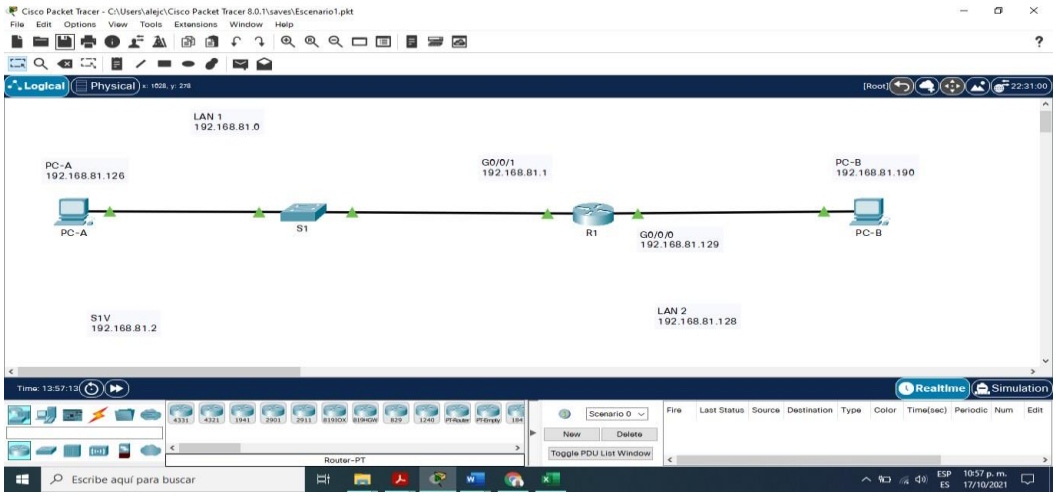
Figura 1. Topología por desarrollar

Fuente: Autor cisco networking academy prueba de habilidades

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos, diseñar el esquema de direccionamiento IPv4 para las LAN propuestas. El router y el switch también deben administrarse de forma segura.

1.1 Construcción de la red

Figura 2. creación escenario 1 en packet tracer 8.0



Fuente: Elaboración propia

1.2 Desarrollo del 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.

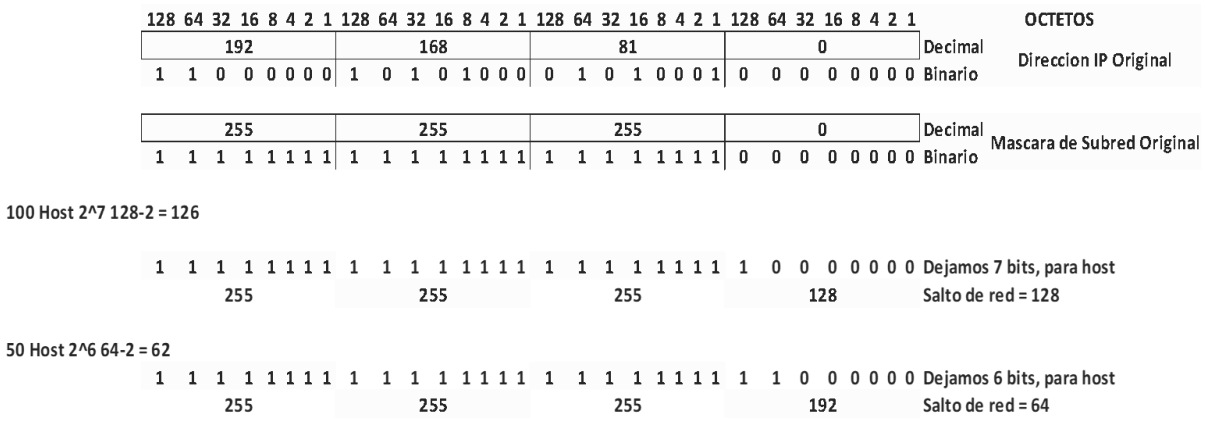
Cada estudiante tomará el direccionamiento 192.168.**X**.0 donde X corresponde a los últimos dos dígitos de su cédula.

Tabla 1. Crear direccionamiento

Item	***Requerimiento***
Dirección de Red	*192.168.81.0*
Requerimiento de host Subred LAN1	*100*
Requerimiento de host Subred LAN2	*50*
R1 G0/0/1	*Primera dirección de host de la subred LAN1*
R1 G0/0/0	*Primera dirección de host de la subred LAN2*
S1 SVI	*Segunda dirección de host de la subred LAN1*
PC-A	*Última dirección de host de la subred LAN1*
PC-B	*Última dirección de host de la subred LAN2*

Creación de las subredes, con la dirección ipv4 192.168.81.0 con una máscara de subred 255.255.255.0 con prefijo de /24

Figura 3. Creación de 02 subredes ipv4



Fuente: Elaboración propia

Figura 4. Datos en Subneteo realizado

Host Encontrados	Red	Host - Inicial	Host - Final	Broadcast	LAN
126	**192.168.81.0**	**192.168.81.1**	**192.168.81.126**	**192.168.81.127**	**1**
62	**192.168.81.128**	**192.168.81.129**	**192.168.81.190**	**192.168.81.191**	**2**

Fuente: Elaboración propia

Tabla 2. Desarrollo del esquema de direccionamiento ipv4

Item	Requerimiento
Direccion de Red	192.168.81.0 / 24
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	Primera direccion subred LAN1 192.168.81.1
R1 G0/0/0	Primera dirección de host de la subred LAN2 192.168.81.129
S1 SVI	Segunda dirección de host de la subred LAN1 192.168.81.2
PC-A	Ultima direccion de host de la subred LAN1 192.168.81.126
PC-B	Última dirección de host de la subred LAN2 192.168.81.190

1.3 Configuración aspectos básicos de dispositivos de la red propuesta

1.3.1 Router

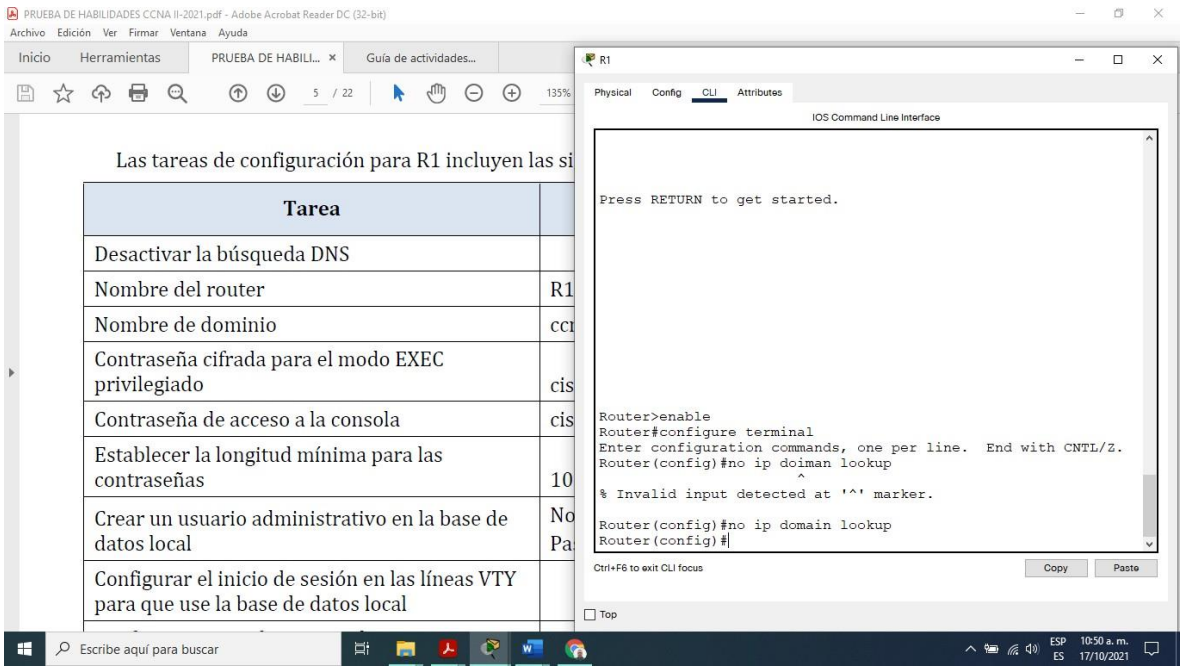
Tabla 3. Configuración básica R1

Tarea	Especificación
Desactivar la búsqueda DNS	no ip domain lookup
Nombre del router	hostname R1
Nombre de dominio	no ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	enable secret ciscoenpass
Contraseña de acceso a la consola	line console 0 password cinscoconpass login exit
Establecer la longitud mínima para las contraseñas	10 caracteres security password min-length 10
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** username admin secret admin1pass

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	line vty 0 15 login local
Configurar VTY solo aceptando SSH	transport input ssh exit
Cifrar las contraseñas de texto no cifrado	service password-encryption
Configure un MOTD Banner	service password-encryption banner motd $Solo Personal Autorizado. .....!!!$
Configurar interfaz G0/0/0	int g0/0/0 description Primera Direccion LAN2 ip address 192.168.81.129 255.255.255.192 no shutdown
Configurar interfaz G0/0/1	int g0/0/1 description Primera Direccion LAN1 ip address 192.168.81.1 255.255.255.128 no shutdown
Generar una clave de cifrado RSA	Módulo de 1024 bits crypto key generate rsa general-key modulos 1024

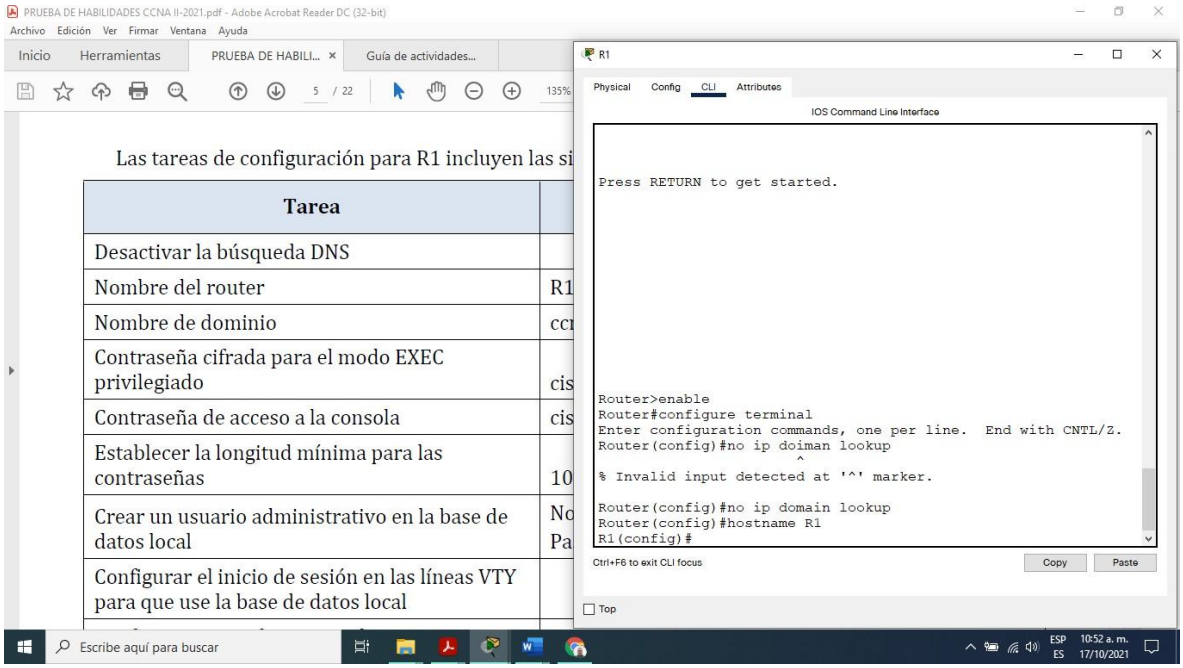
1.3.2 Evidencia de la tabla configuración R1

Figura 5. Desactivar búsqueda DNS



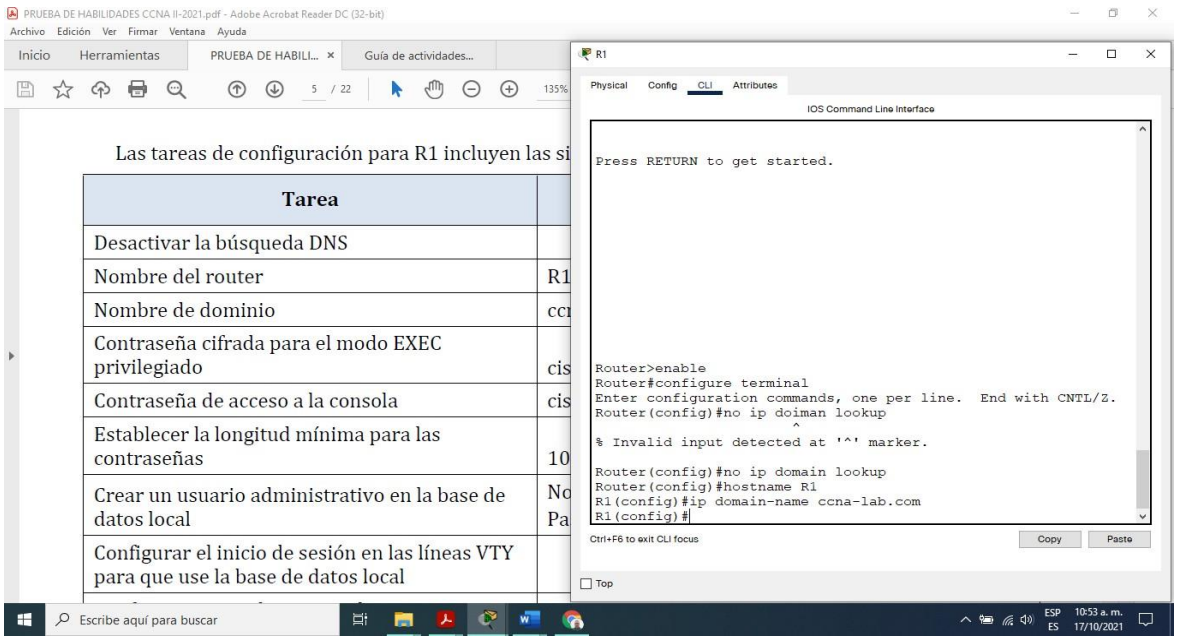
Fuente: Elaboración propia

Figura 6. Nombre del Router



Fuente: Elaboración propia

Figura 7. Nombre del dominio



Fuente: Elaboración propia

Contraseña cifrada para el modo EXCEC privilegiado **ciscoenpass**

Figura 8. Contraseña Cifrada

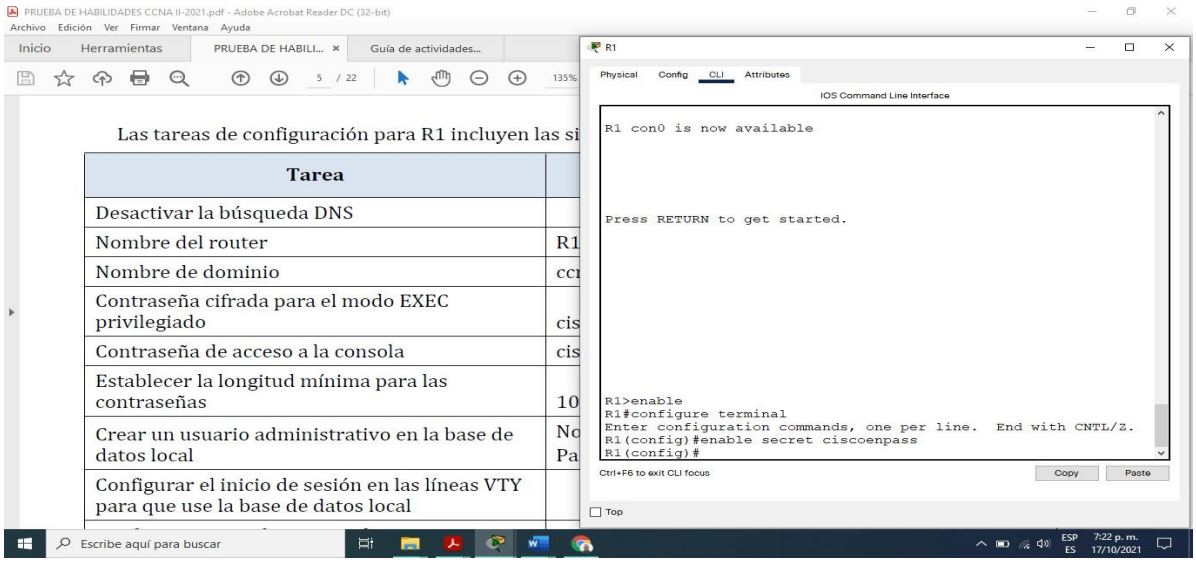
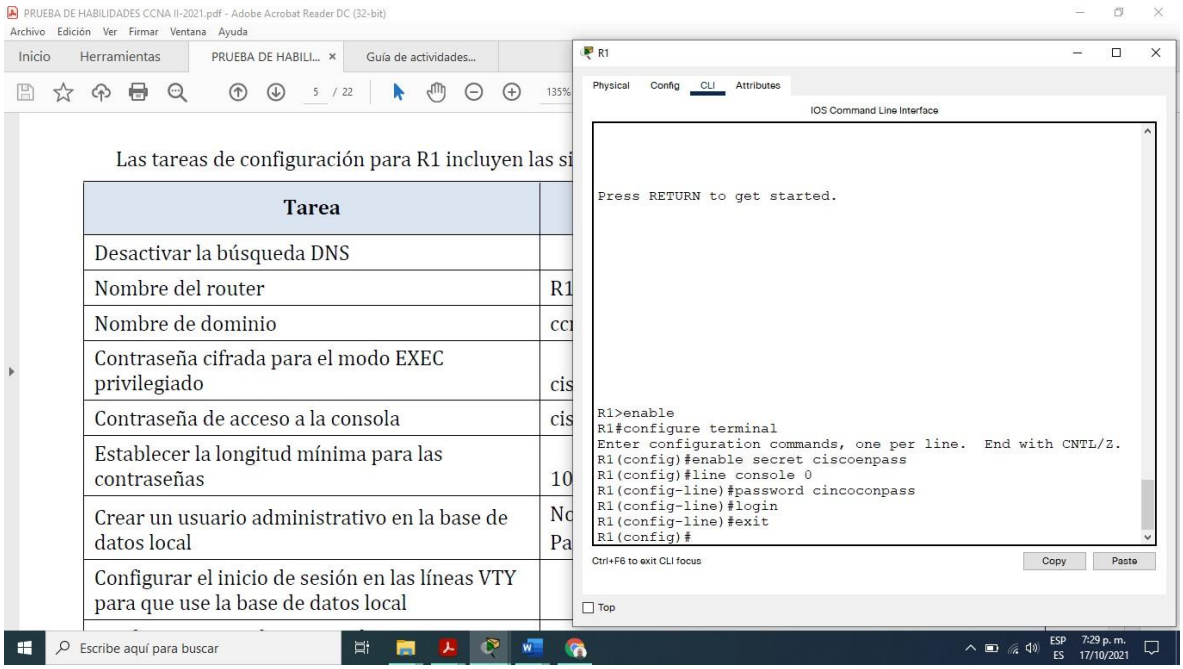
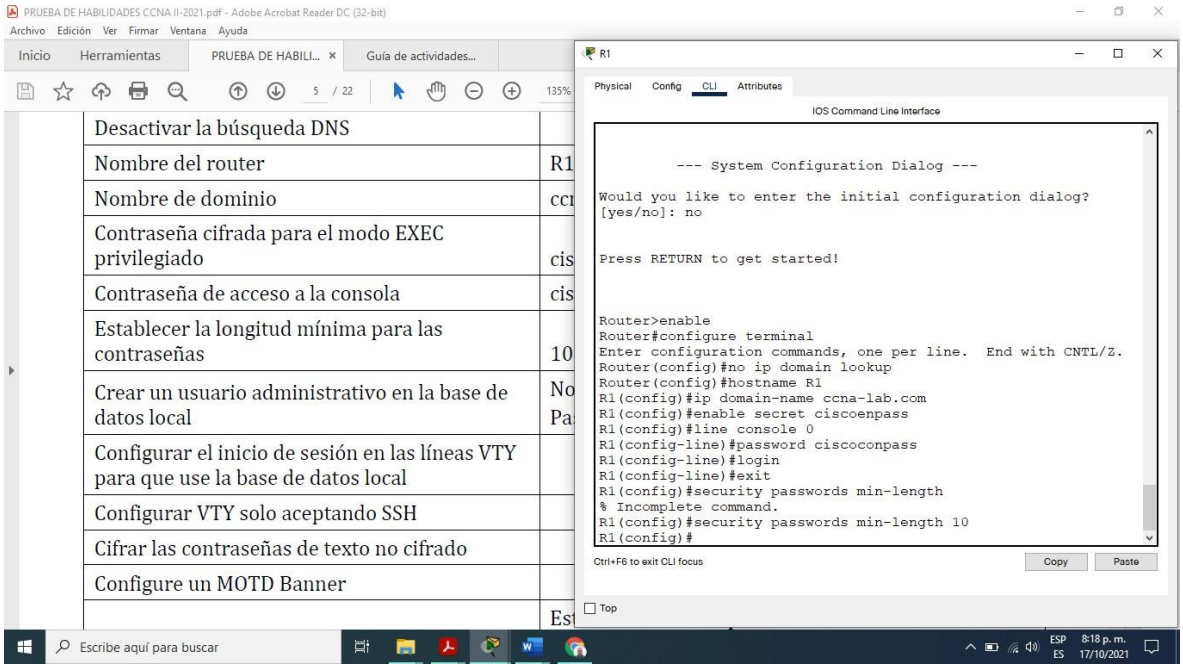


Figura 9.Contraseña de acceso a la consola ciscoconpass



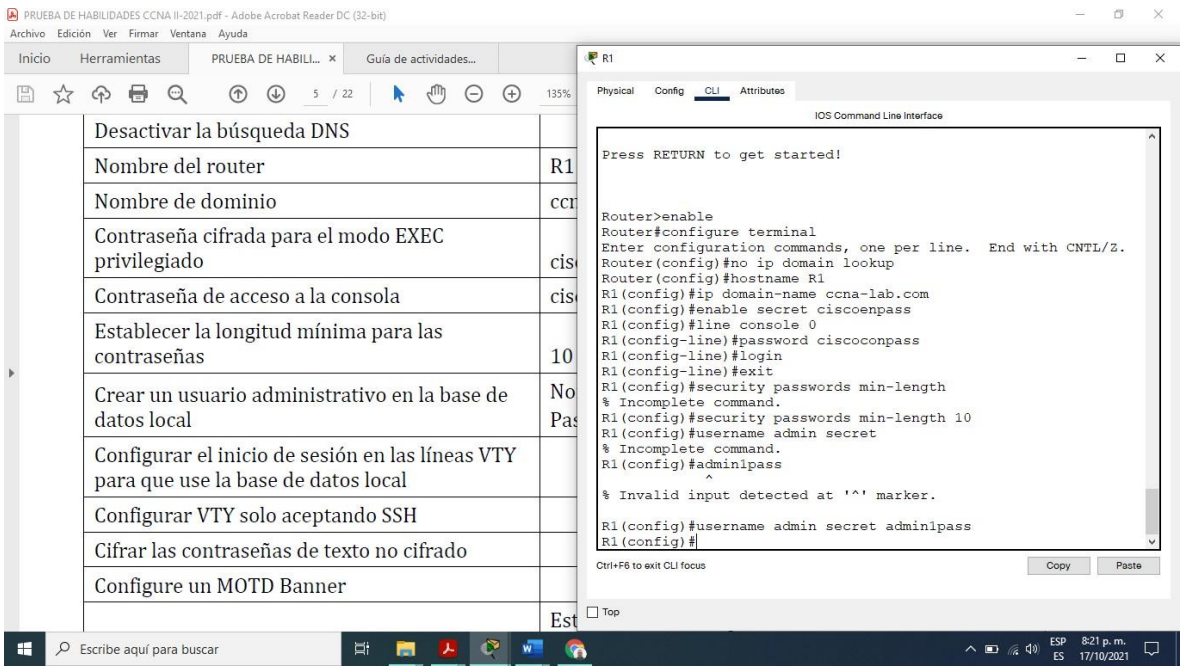
Fuente: Elaboración propia

Figura 10. Establecer longitud mínima de contraseña de 10 caracteres



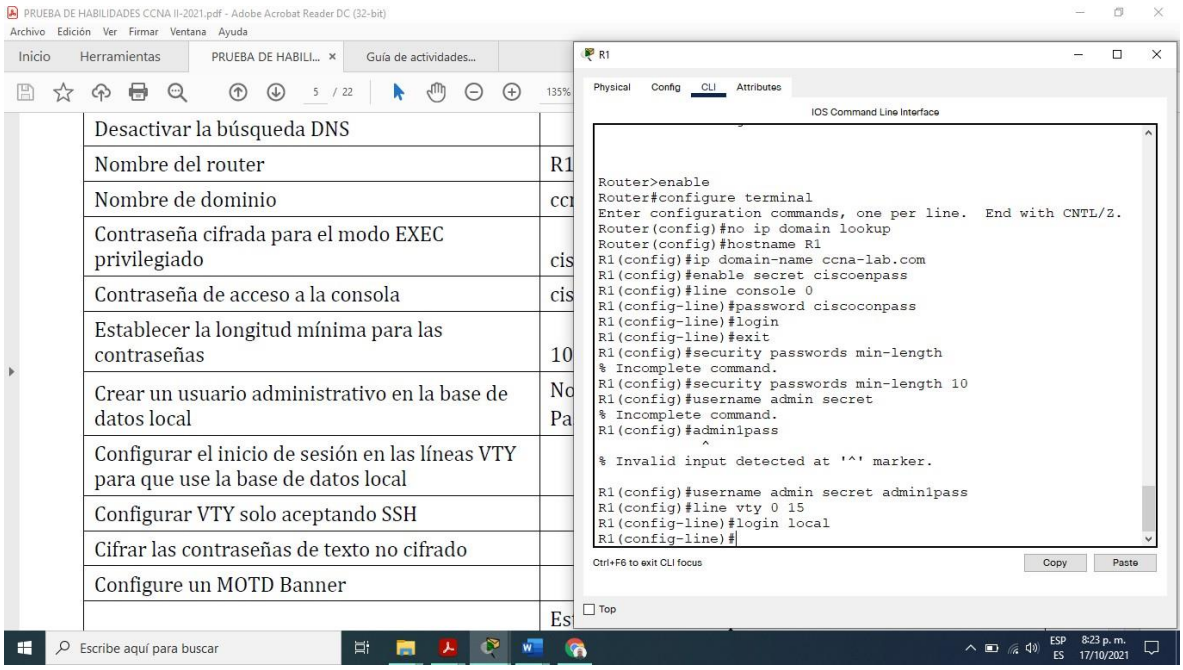
Fuente: Elaboración propia

Figura 11.Crear un usuario administrativo en la base de datos local



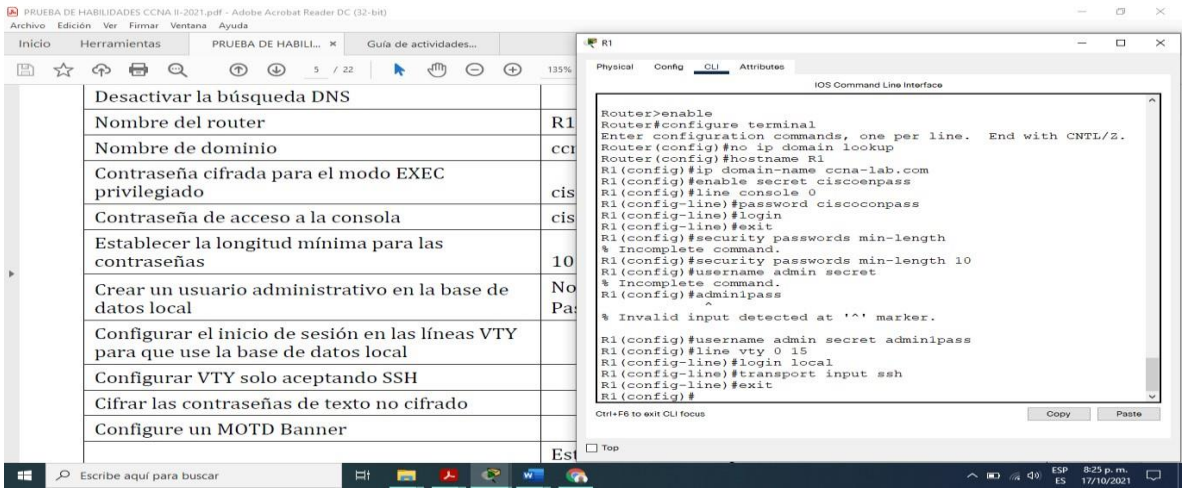
Fuente: Elaboración propia

Figura 12.Configurar líneas VTY para usar base de datos local



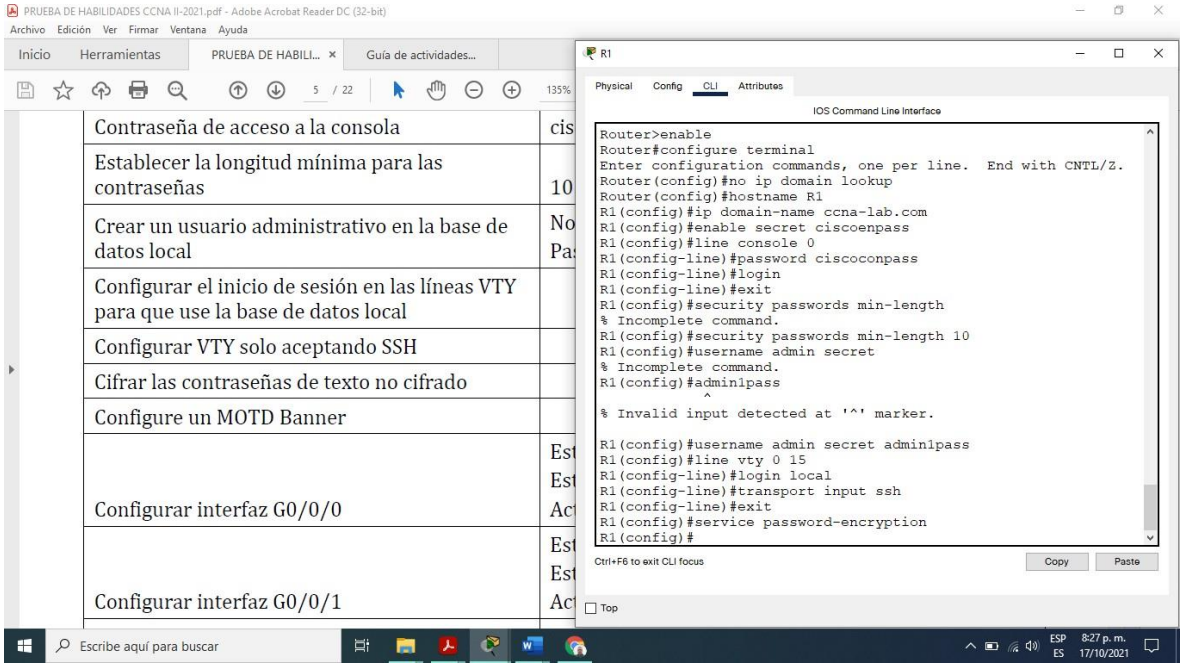
Fuente: Elaboración propia

Figura 13.Configurar VTY solo aceptando SSH



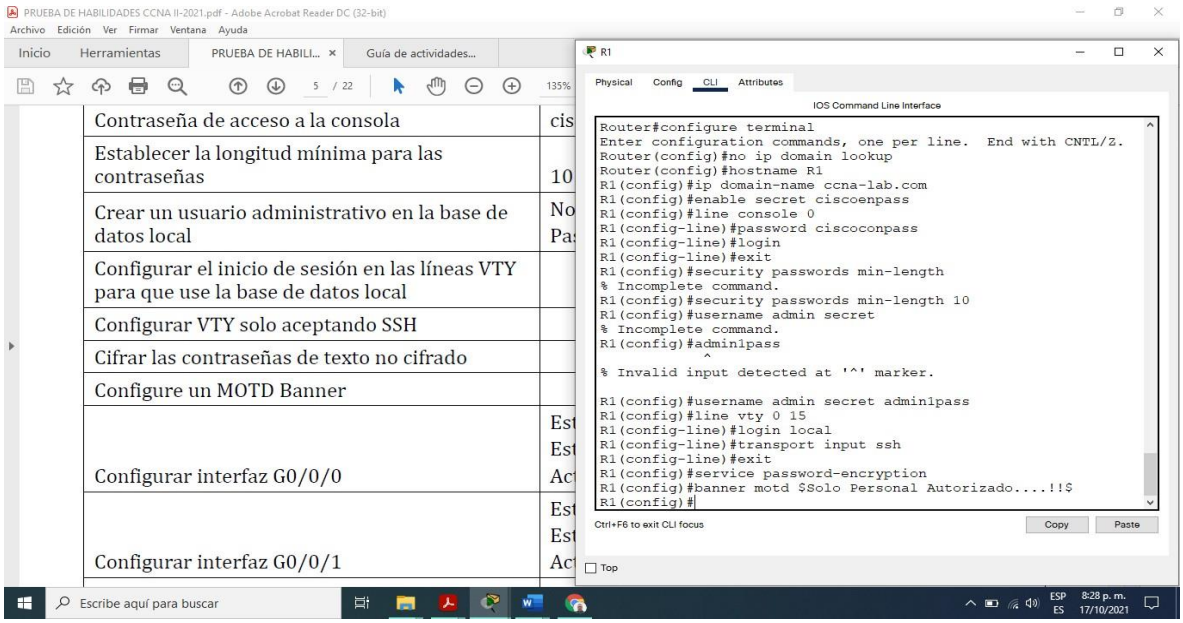
Fuente: Elaboración propia

Figura 14.Cifrar las contraseñas de texto no cifrado



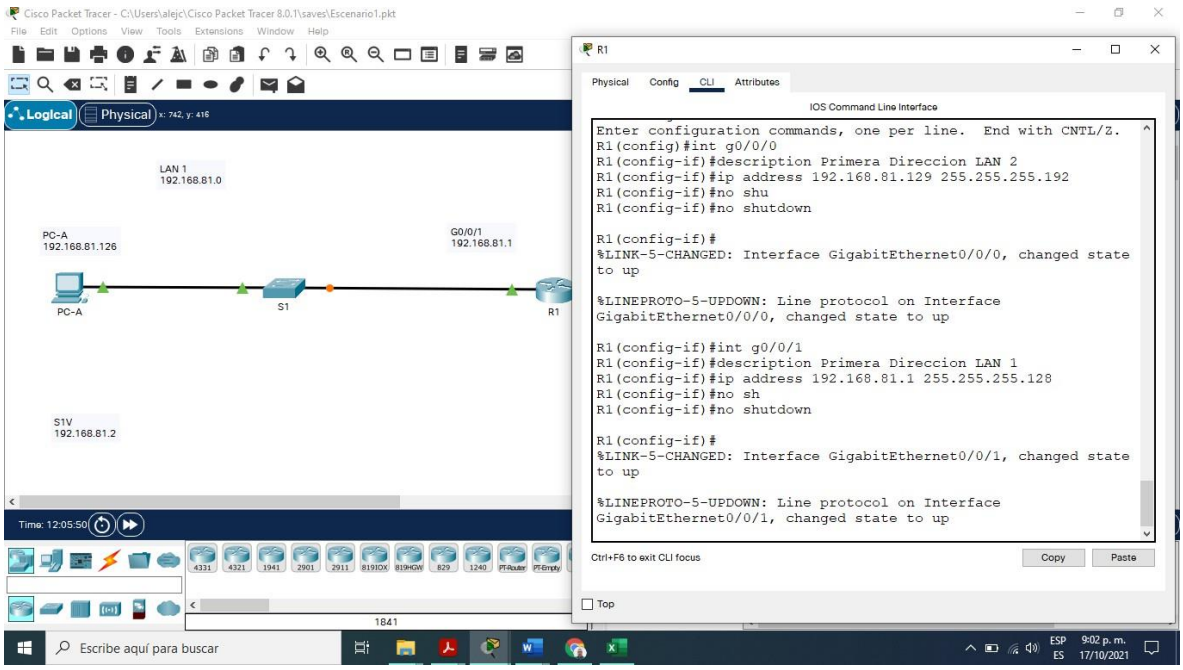
Fuente: Elaboración propia

Figura 15.Configure un MOTD Banner



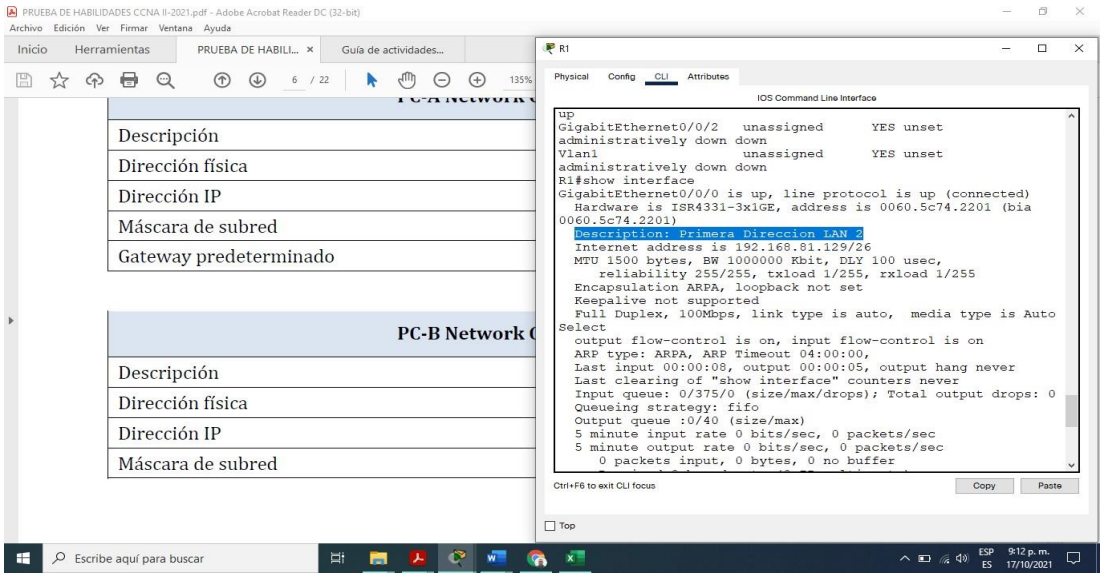
Fuente: Elaboración propia

Figura 16.Configuración de la interfaz g0/0/0 – g0/0/1 del R1



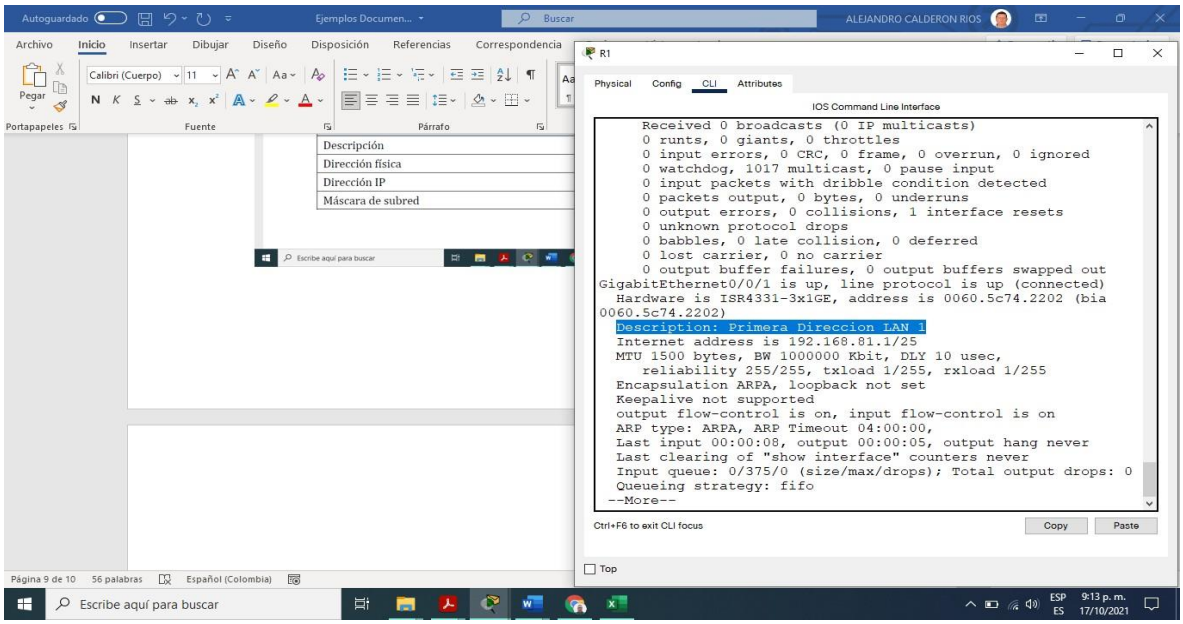
Fuente: Elaboración propia

Figura 17. Comando show interface



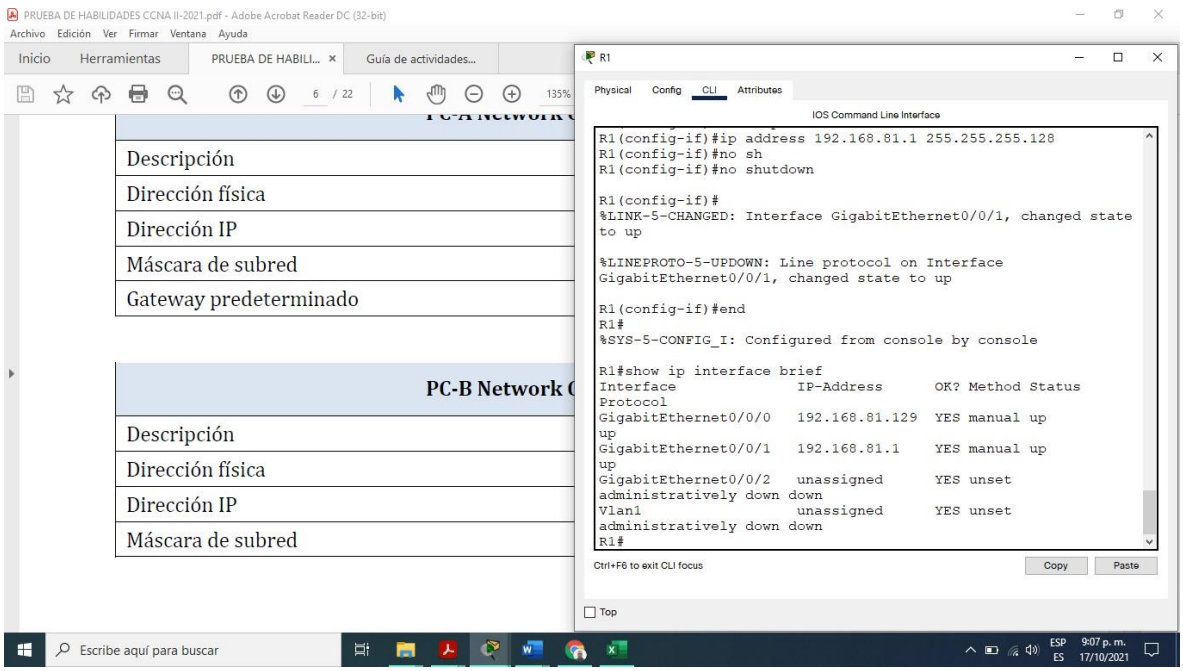
Fuente: Elaboración propia

Figura 18. Comando show interface, descripción de la interfaz LAN 1



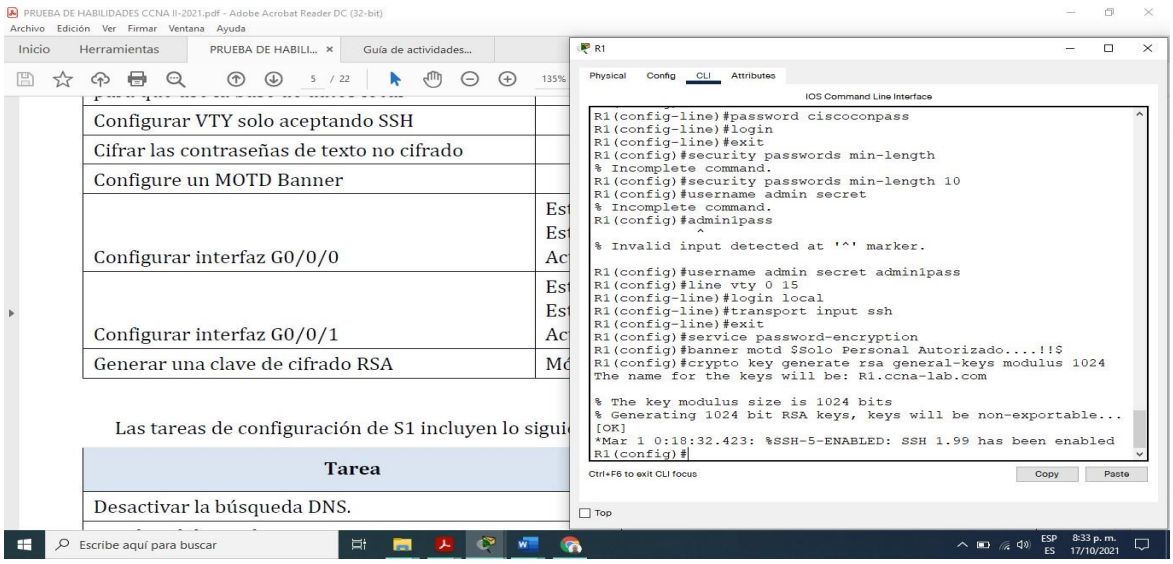
Fuente: Elaboración propia

Figura 19. Uso de comando show ip interface brief



Fuente: Elaboración propia

Figura 20.Generar una clave de cifrado RSA módulo de 1024 bits



Fuente: Elaboración propia

1.4. Configuración básica Switch

1.4.1 S1

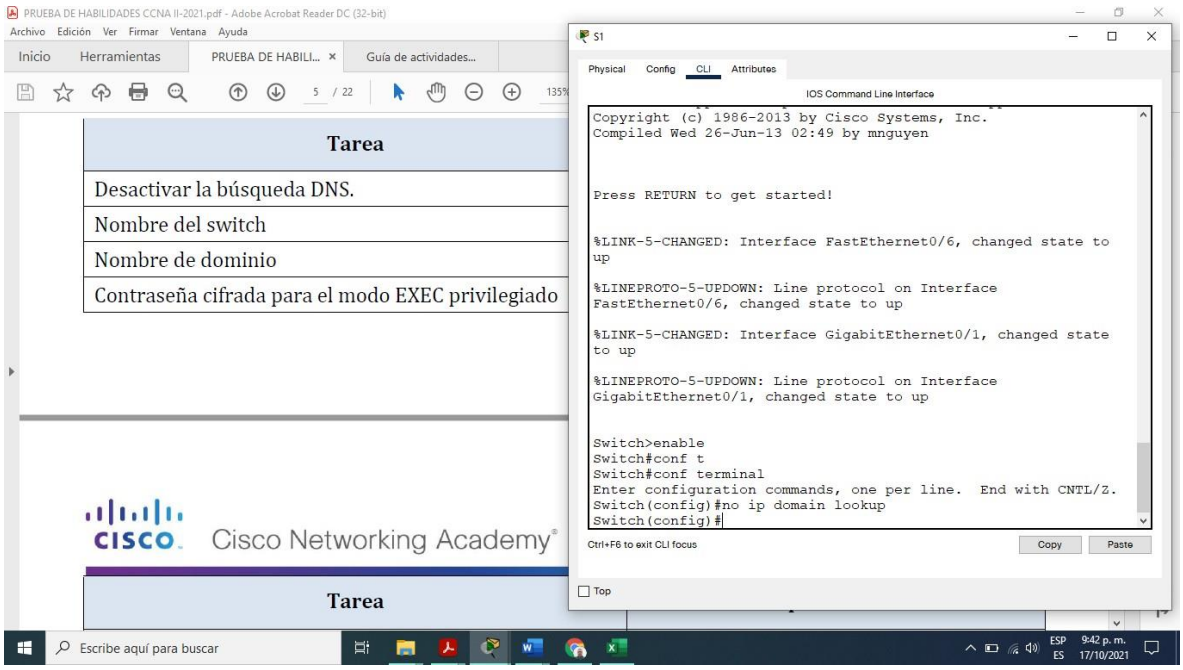
Tabla 4. Configuración Básica S1

Tarea	Especificación
Desactivar la búsqueda DNS.	no ip domain lookup
Nombre del switch	hostname S1
Nombre de dominio	no ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	enable secret ciscoenpass
Contraseña de acceso a la consola	line console 0 password cinscoconpass login exit
Crear un usuario administrativo en la base de datos local	username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	line vty 0 15 login local

Configurar las líneas VTY para que acepten únicamente las conexiones SSH	transport input ssh exit
Cifrar las contraseñas de texto no cifrado	service password-encryption
Configurar un MOTD Banner	banner motd $Solo Personal Autorizado.....!!!$
Generar una clave de cifrado RSA	crypto key generate rsa general-key modulos 1024
Configurar la interfaz de administración (SVI)	int vlan1 descripcion 2da direccion LAN1 ip address 102.168.81.2 255.255.255.128 no shutdown
Configuración del gateway predeterminado	ip default-gateway 192.168.81.1

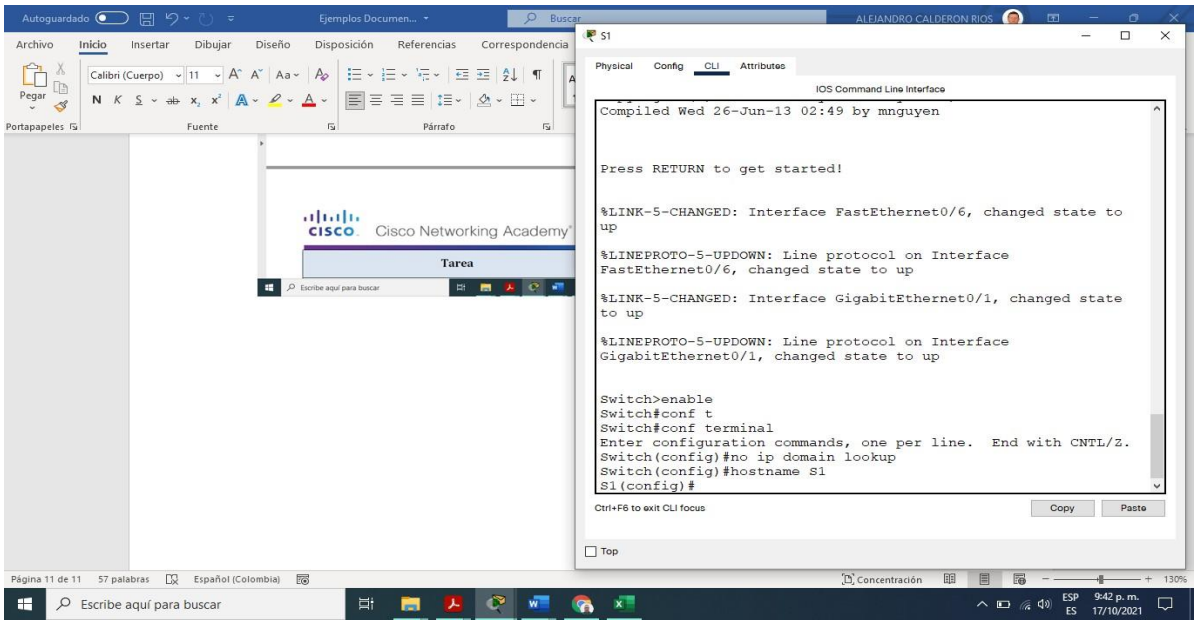
1.4.2 Evidencia de la tabla configuración S1

Figura 21.Desactivar la búsqueda DNS



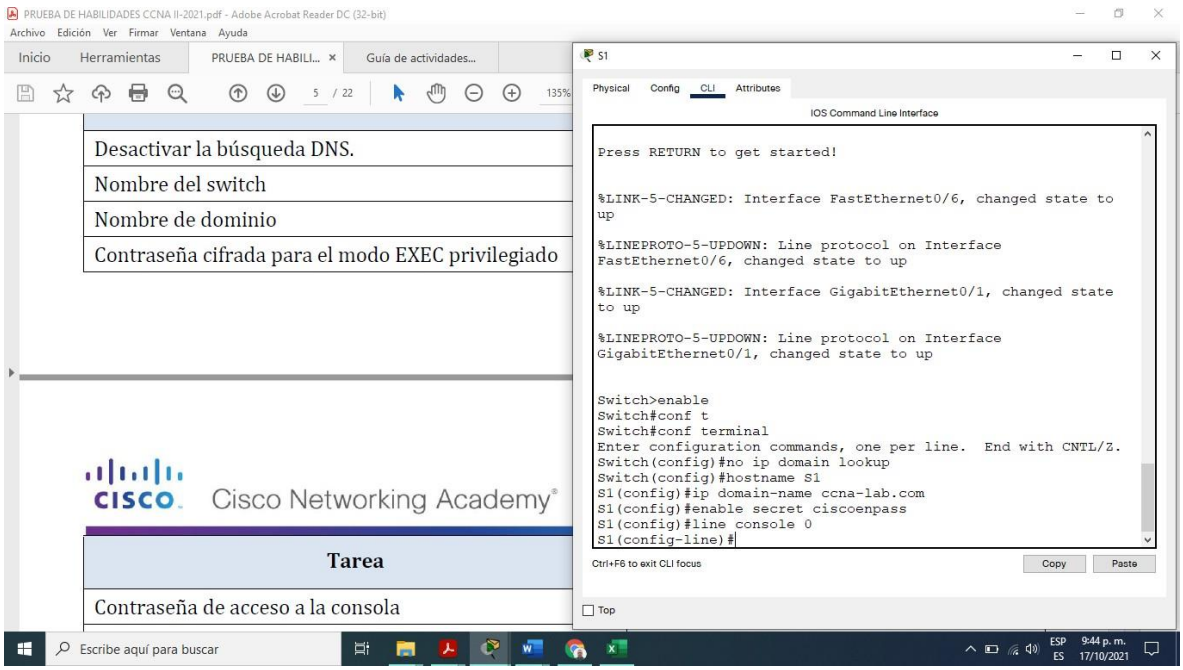
Fuente: Elaboración propia

Figura 22.Nombre del Switch S1



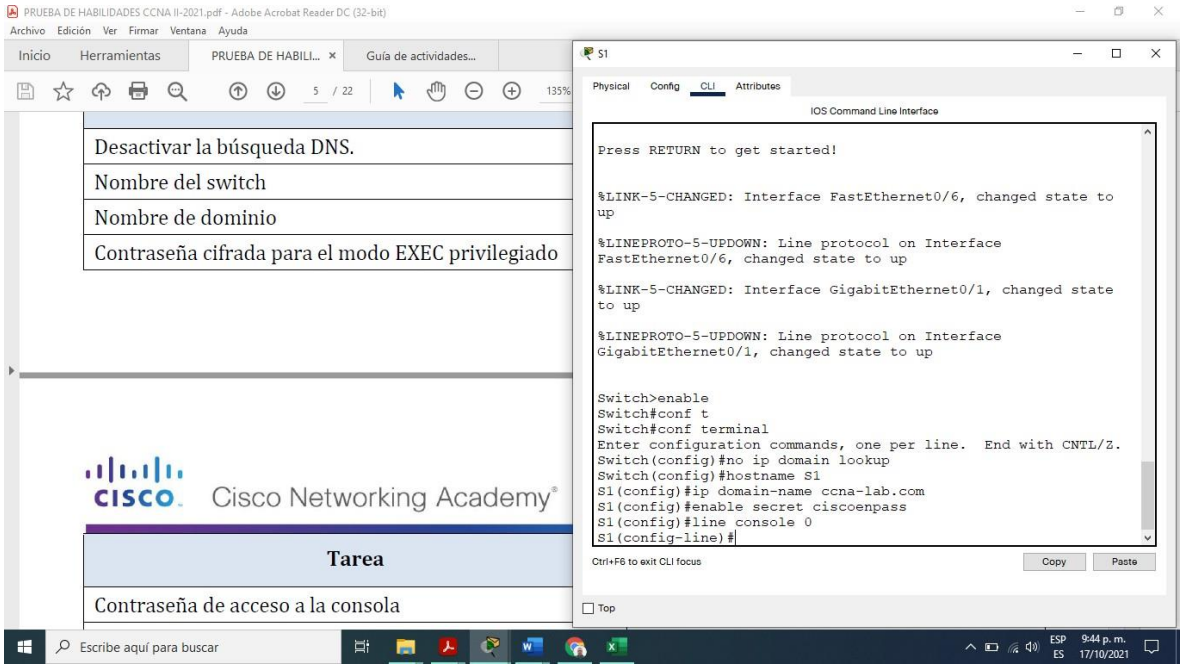
Fuente: Elaboración propia

Figura 23.Nombre del dominio



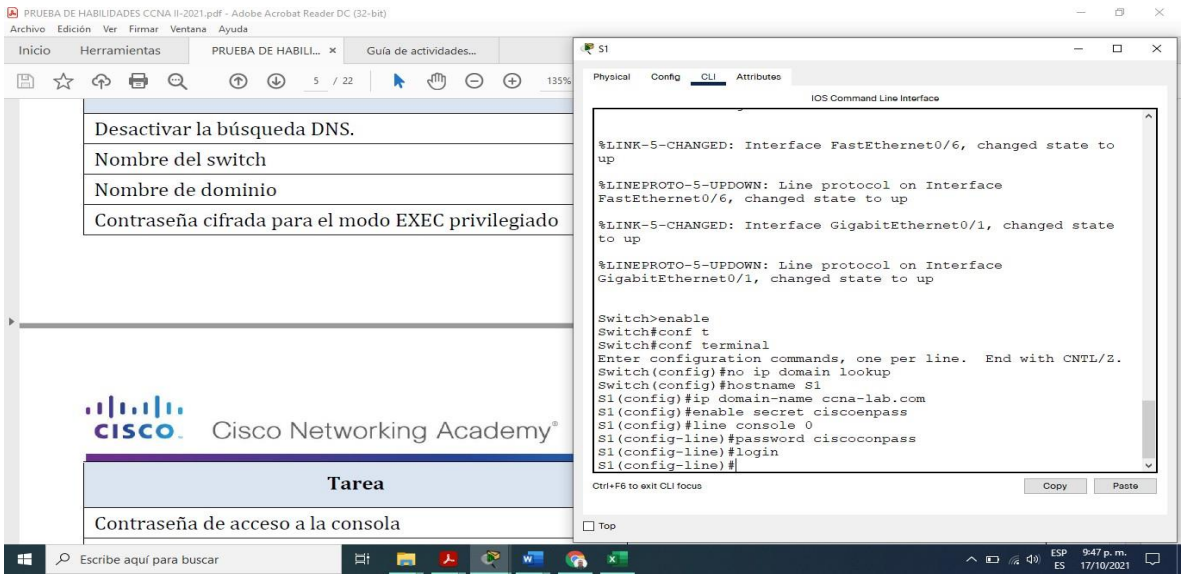
Fuente: Elaboración propia

Figura 24. Contraseña cifrada para el modo EXEC privilegiado



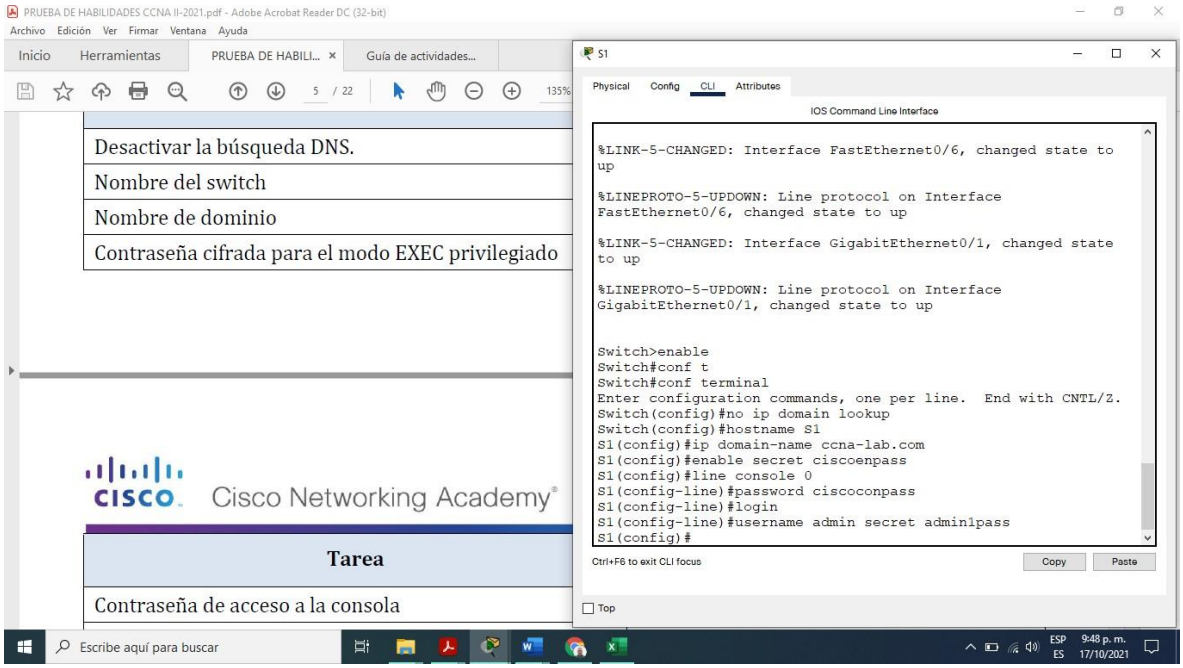
Fuente: Elaboración propia

Figura 25. Contraseña de acceso a la consola



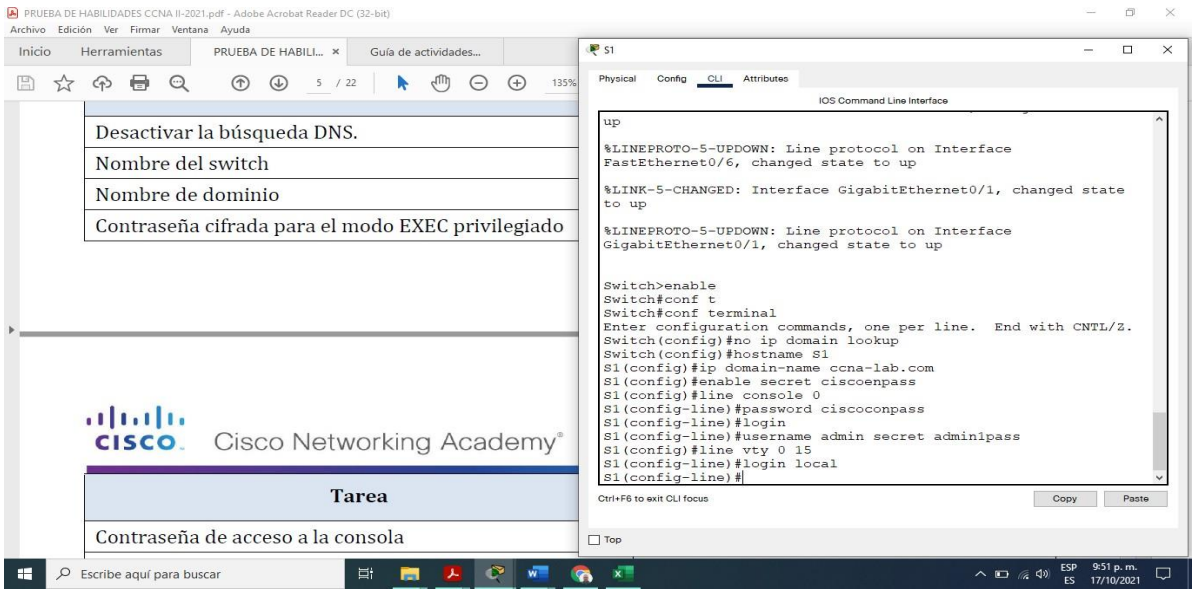
Fuente: Elaboración propia

Figura 26. Crear un usuario administrativo en la base de datos local



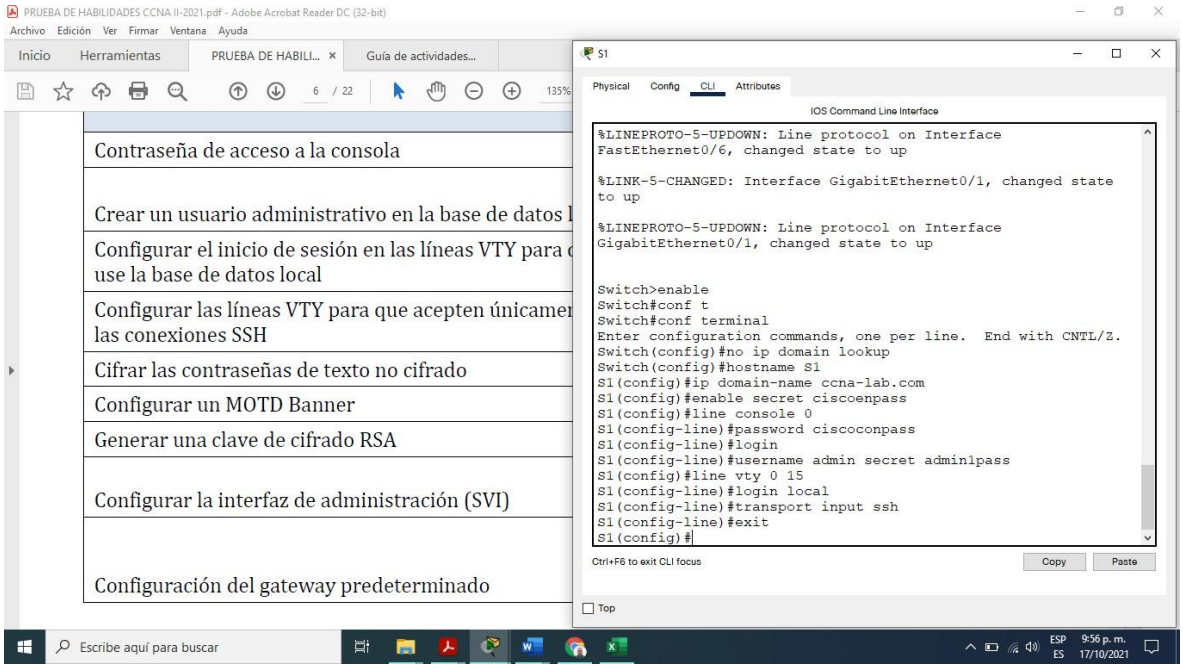
Fuente: Elaboración propia

Figura 27. Configurar el inicio de sesión en las líneas VTY



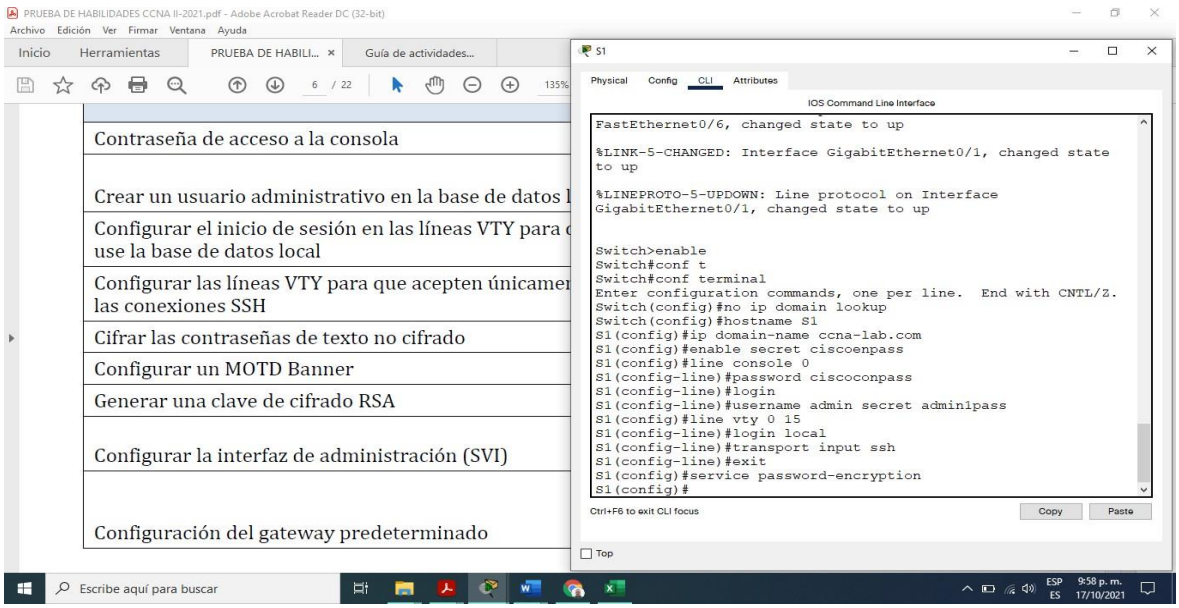
Fuente: Elaboración propia

Figura 28. Configurar las líneas VTY



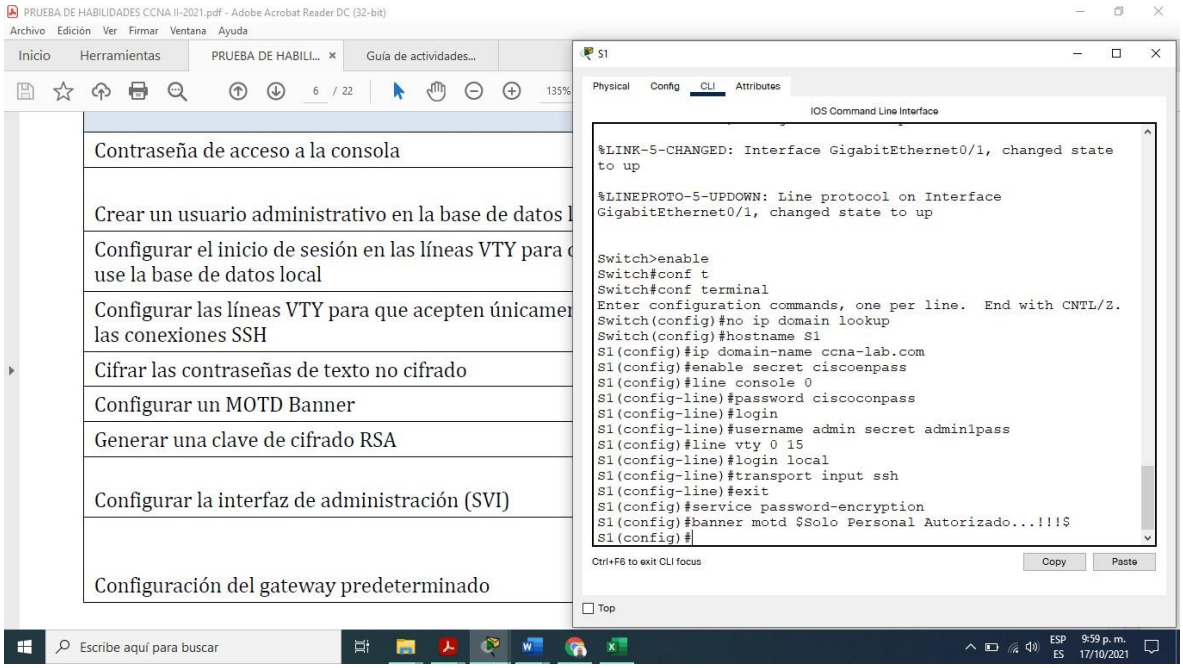
Fuente: Elaboración propia

Figura 29. Cifrar las contraseñas de texto no cifrado



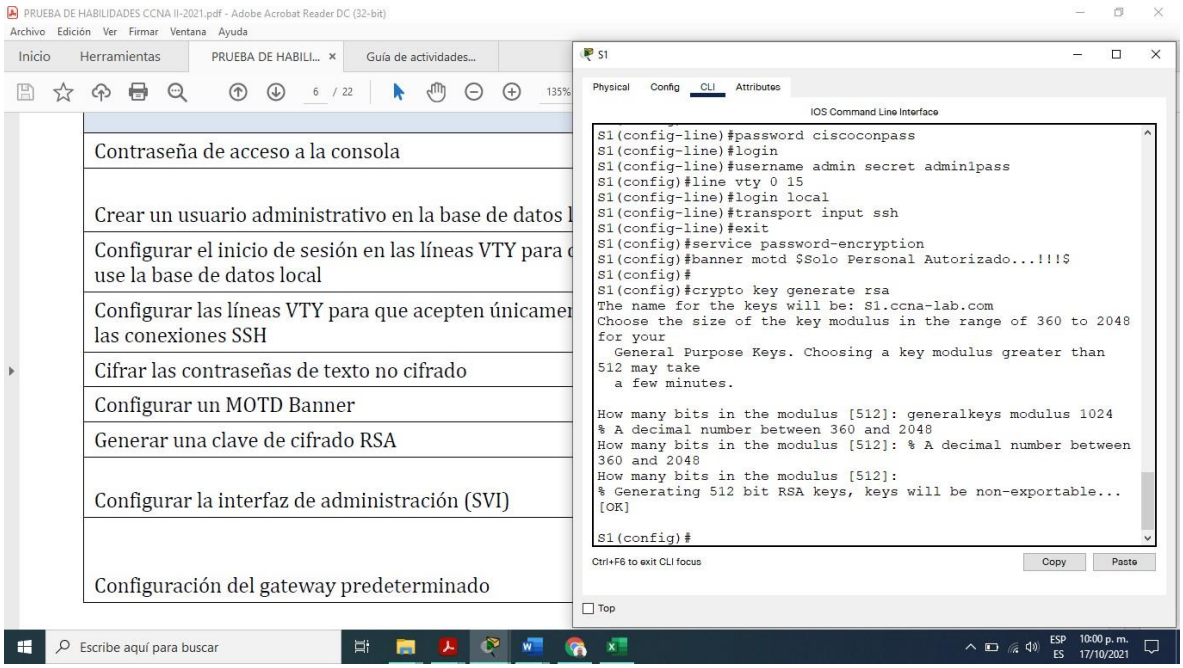
Fuente: Elaboración propia

Figura 30. Configurar un MOTD Banner



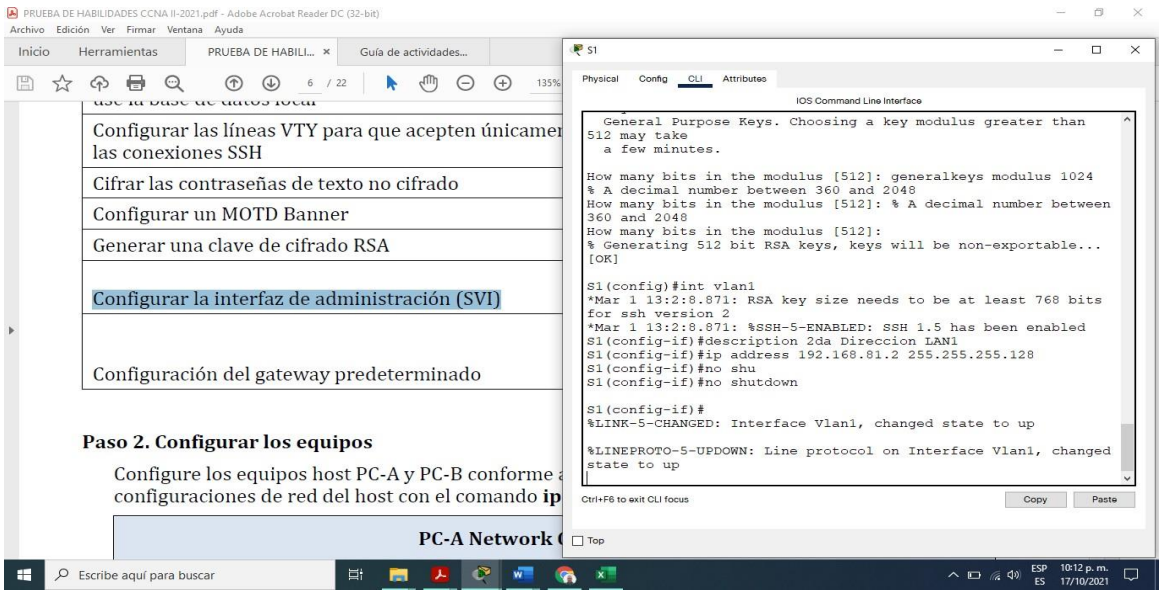
Fuente: Elaboración propia

Figura 31. Generar una clave de cifrado RSA módulo de 1024 bits



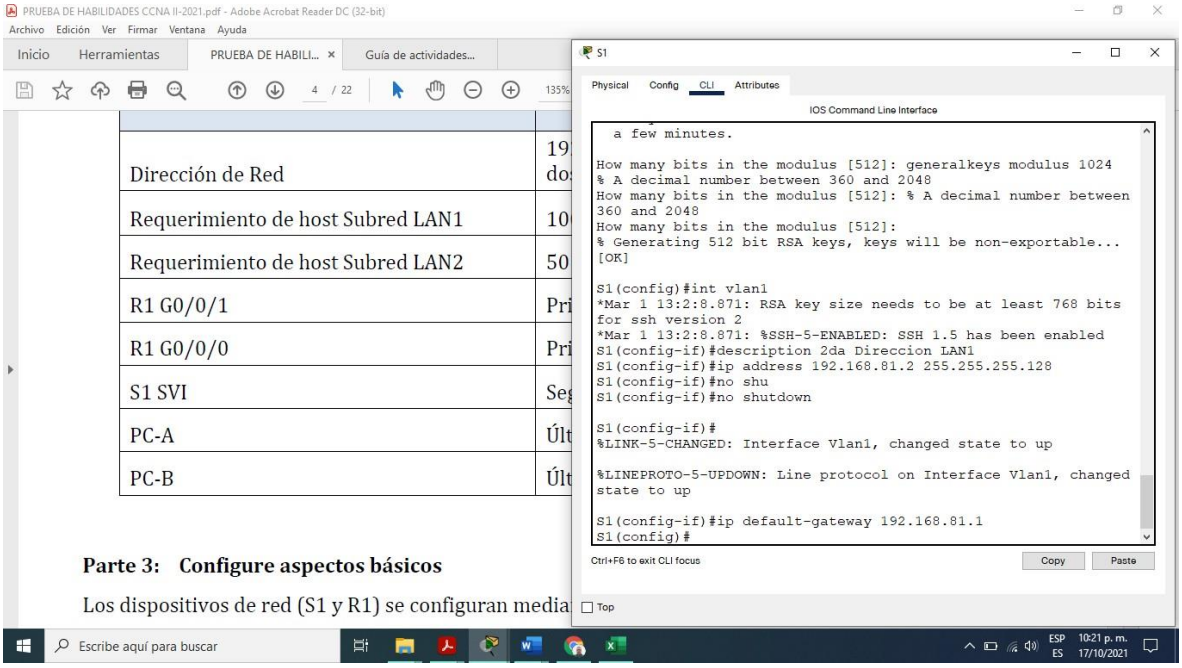
Fuente: Elaboración propia

Figura 32. Configurar la interfaz de administración (SVI)



Fuente: Elaboración propia

Figura 33. Configuración del gateway predeterminado



Fuente: Elaboración propia

1.5 Configuración de equipos host

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

Tabla 5. Registro de configuración PC-A ipconfig /all.

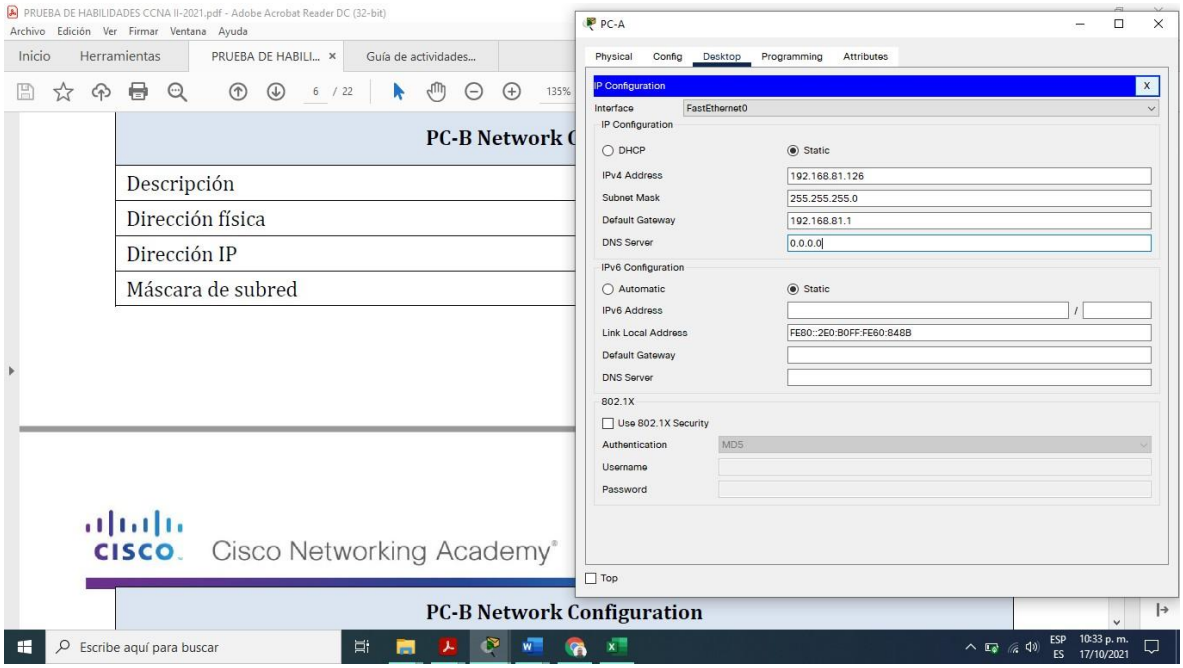
PC-A Network Configuration	
Descripción	Connection-specific DNS Suffix
Dirección física	00E0.B060.848B
Dirección IP	192.168.81.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.81.1

Tabla 6. Registro de configuración PC-B comando ipconfig /all

PC-B Network Configuration	
Descripción	Connection-specific DNS Suffix
Dirección física	00D0.BAE2.55E7
Dirección IP	192.168.81.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.81.1

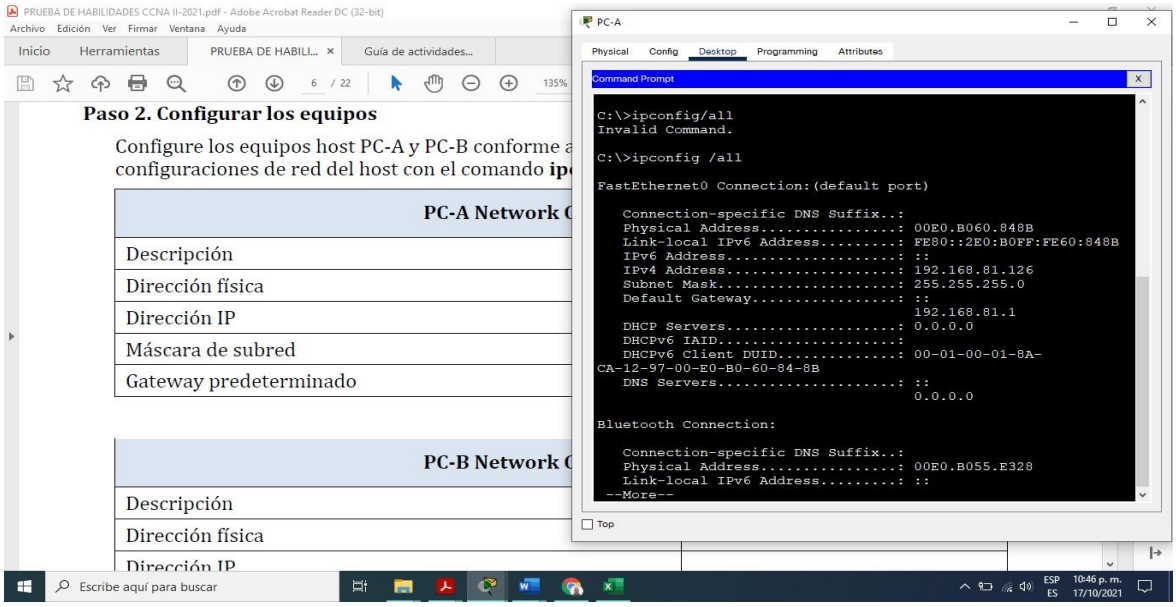
1.5.1 Host PC-A

Figura 34. Configuración Manual PC-A



Fuente: Elaboración propia

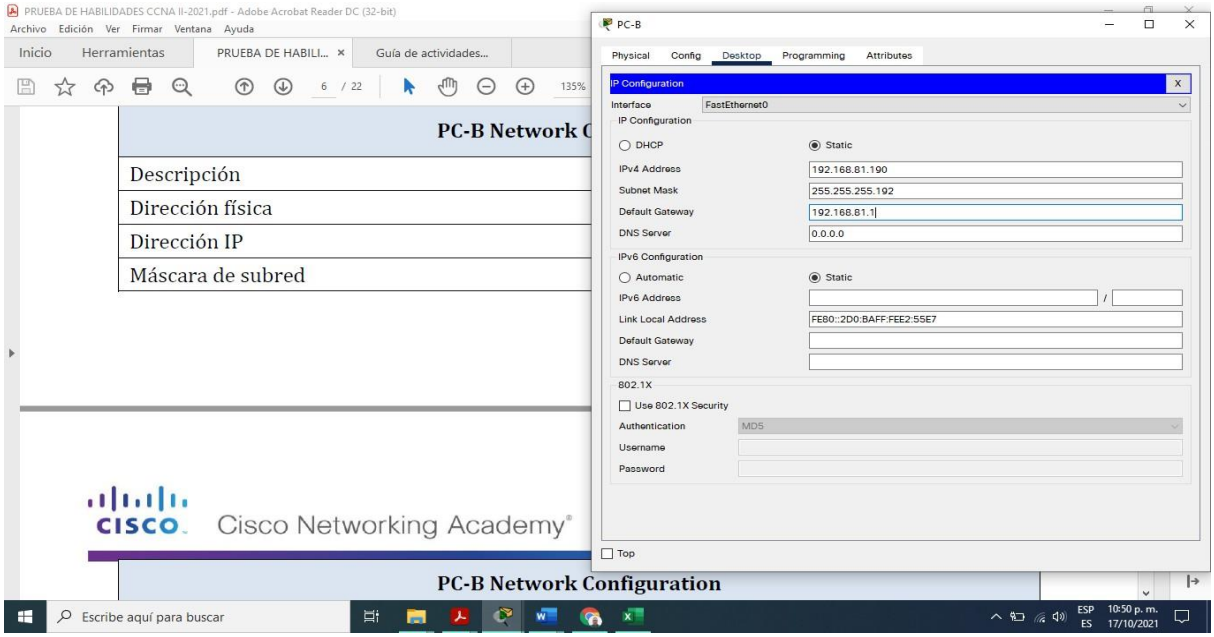
Figura 35. Uso de comando ipconfig /all host PC-A



Fuente: Elaboración propia

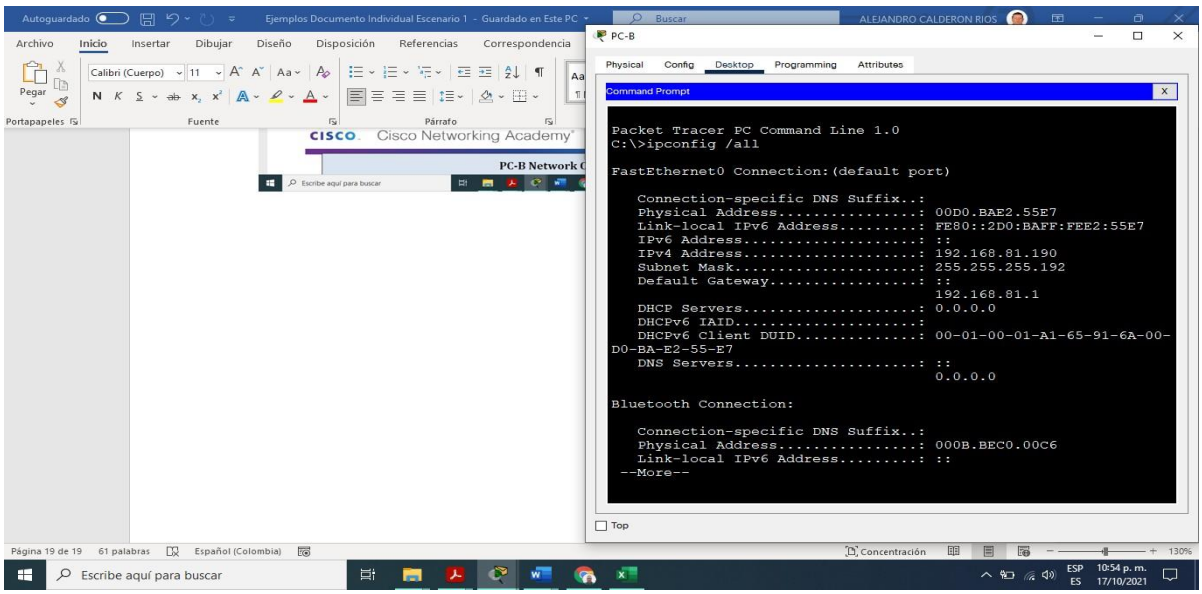
1.5.2 Host PC-B

Figura 36. Configuración Manual PC-B



Fuente: Elaboración propia

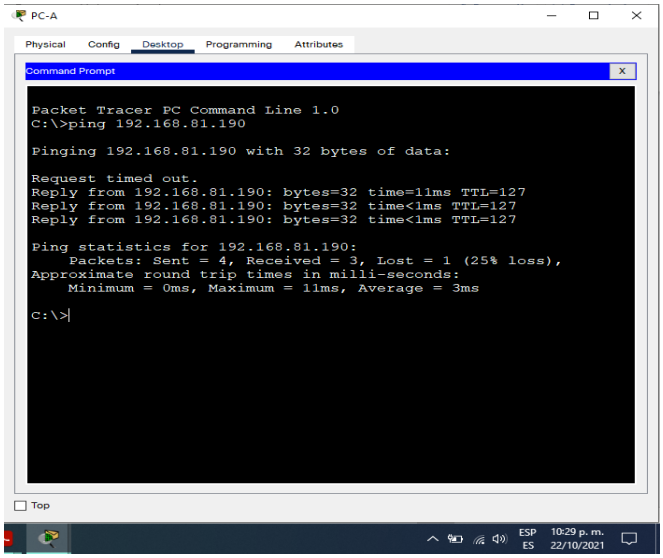
Figura 37. Uso del comando ipconfig /all. PC-B



Fuente: Elaboración propia

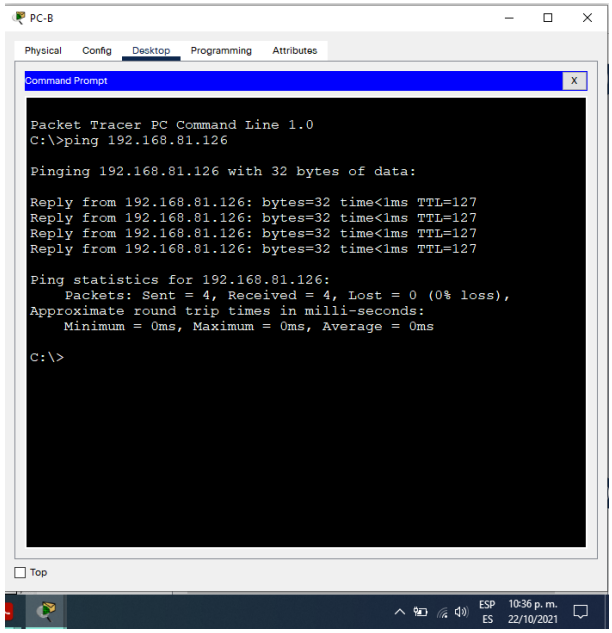
1.6 Pruebas de conectividad

Figura 38. Conectividad comando ping PC-A a PC_B



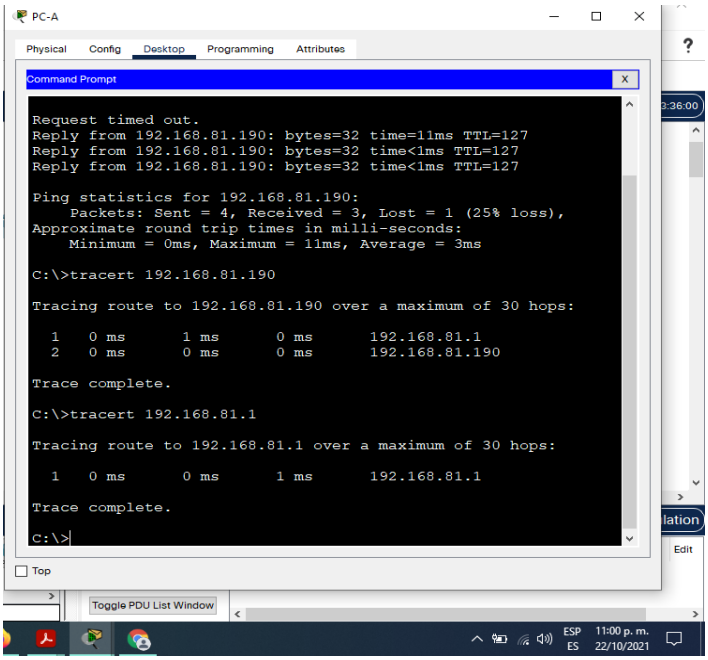
Fuente: Elaboración propia

Figura 39. Conectividad comando ping PC-B a PC-A



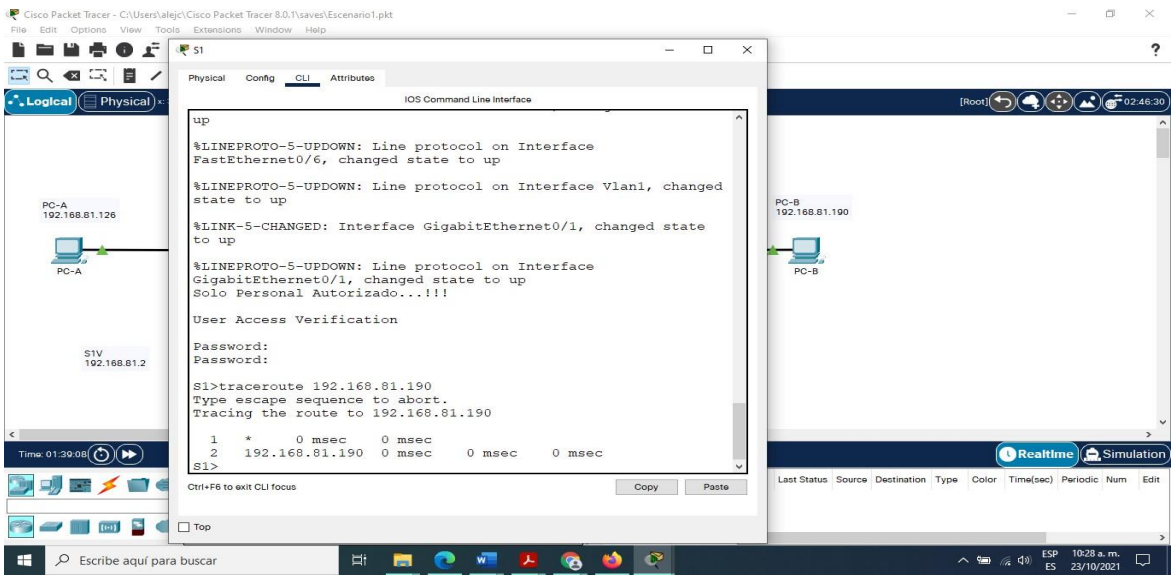
Fuente: Elaboración propia

Figura 40. Comando tracert de PC-A a PC-B



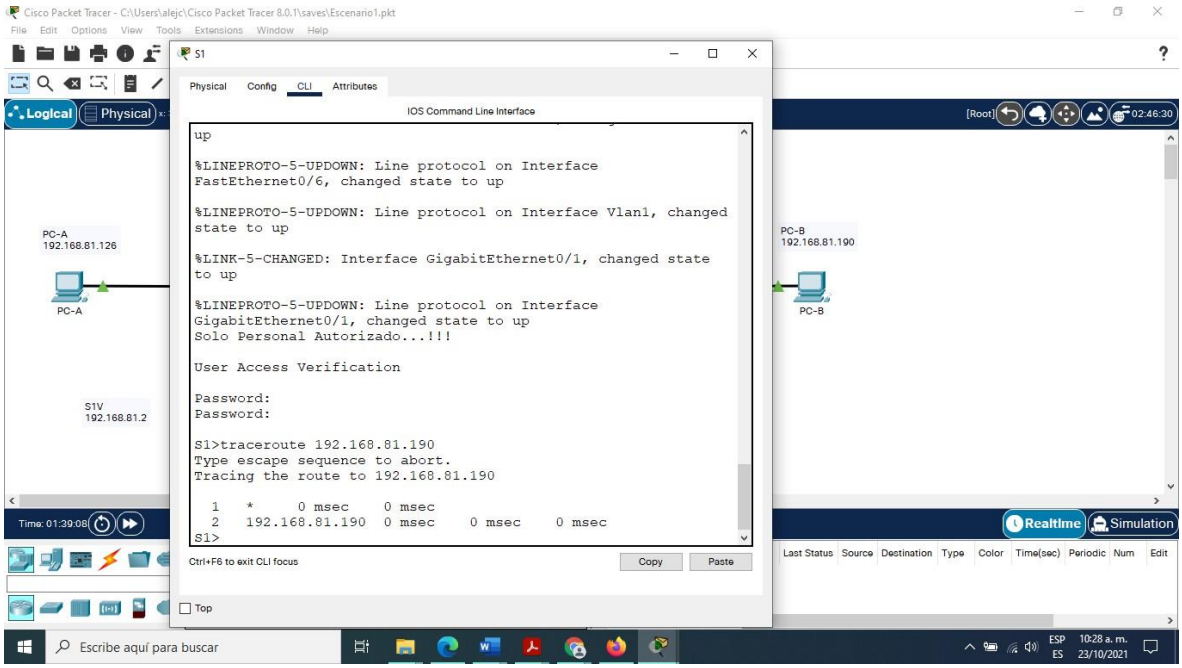
Fuente: Elaboración propia

Figura 41. Comando traceroute desde CLI S1 a PC-B



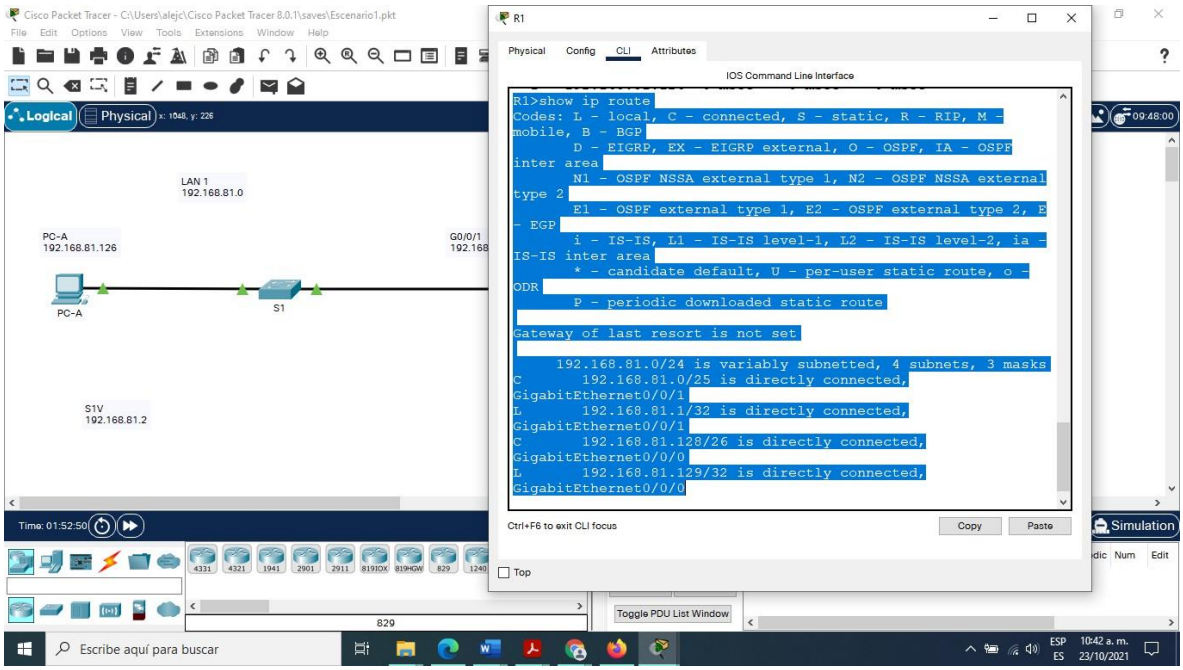
Fuente: Elaboración propia

Figura 42. Comando traceroute desde R1 a PC-A



Fuente: Elaboración propia

Figura 43. Comando show ip route desde R1

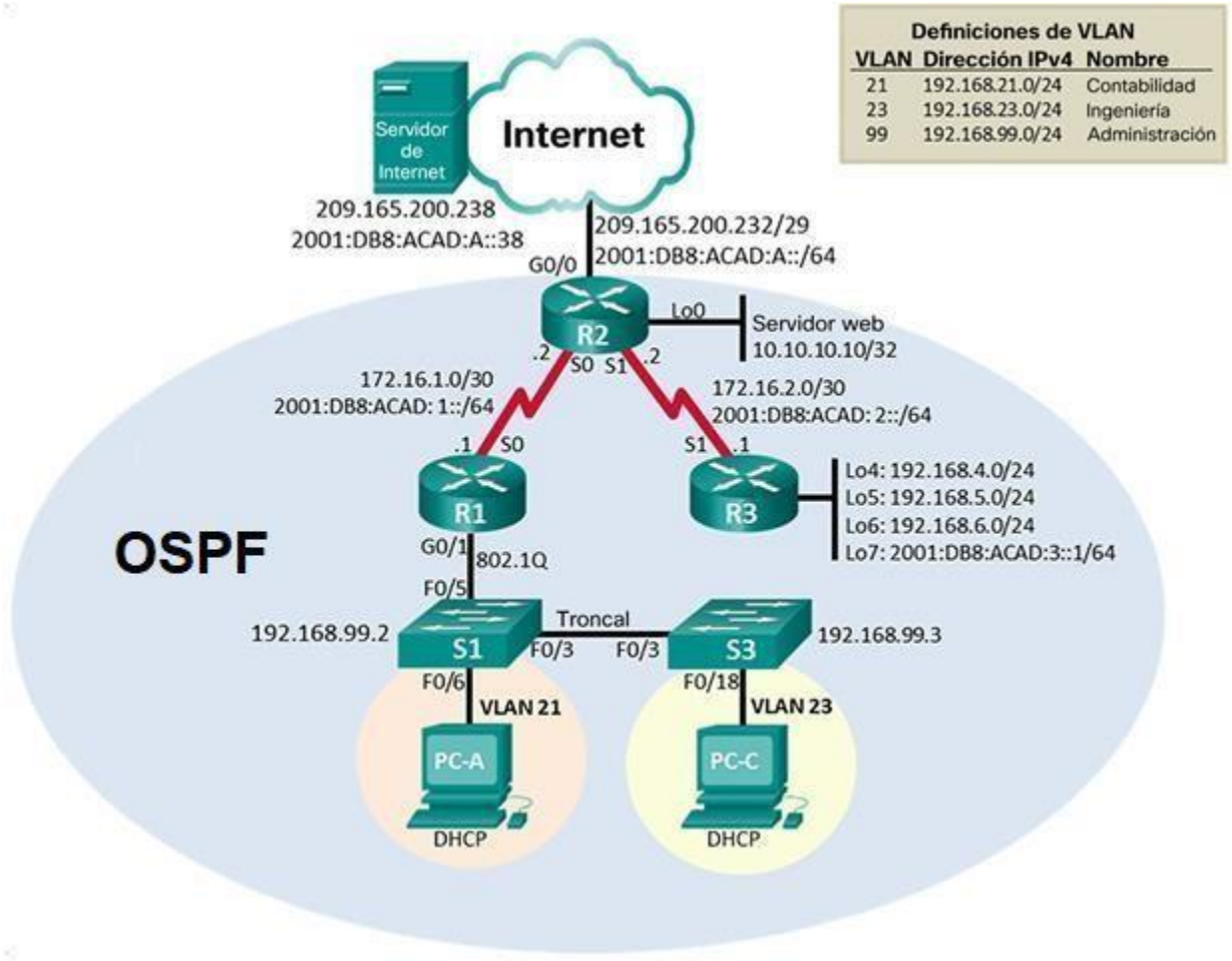


Fuente: Elaboración propia

2. Escenario 2

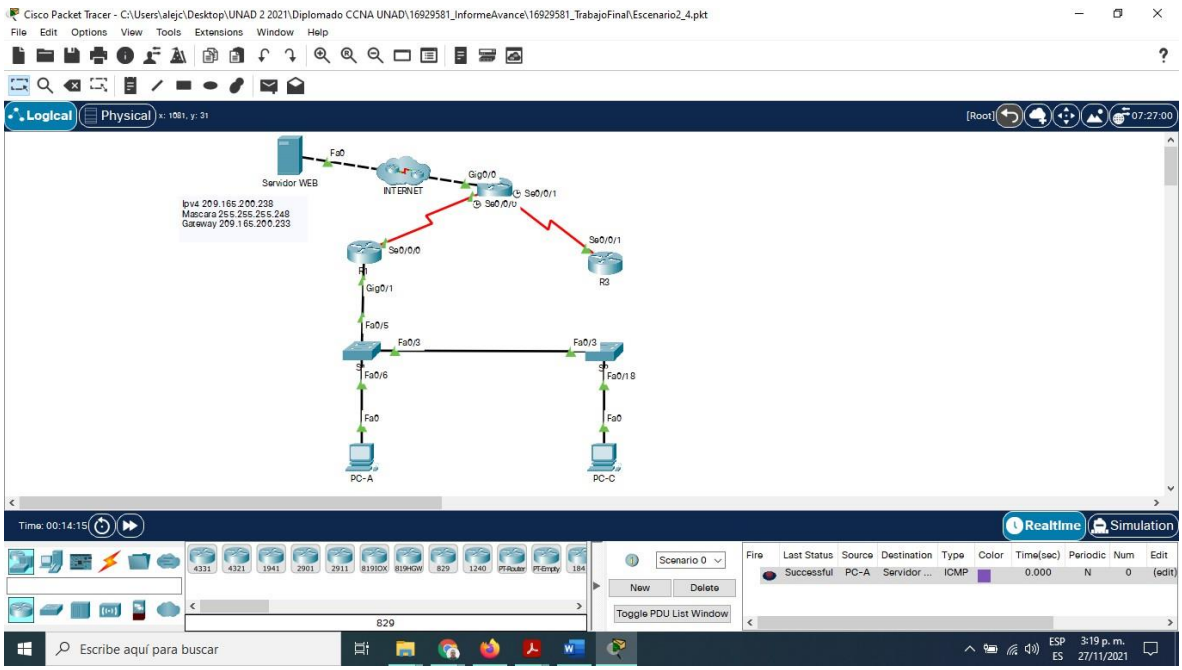
Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Figura 37. Topología inicial



Fuente: Autor cisco networking academy prueba de habilidades

Figura 38. Escenario y su implementación a desarrollar



Fuente: Elaboración propia

Parte 1: Inicializar dispositivos

2.1 Paso 1: Inicializar y volver a cargar los routers y los switches

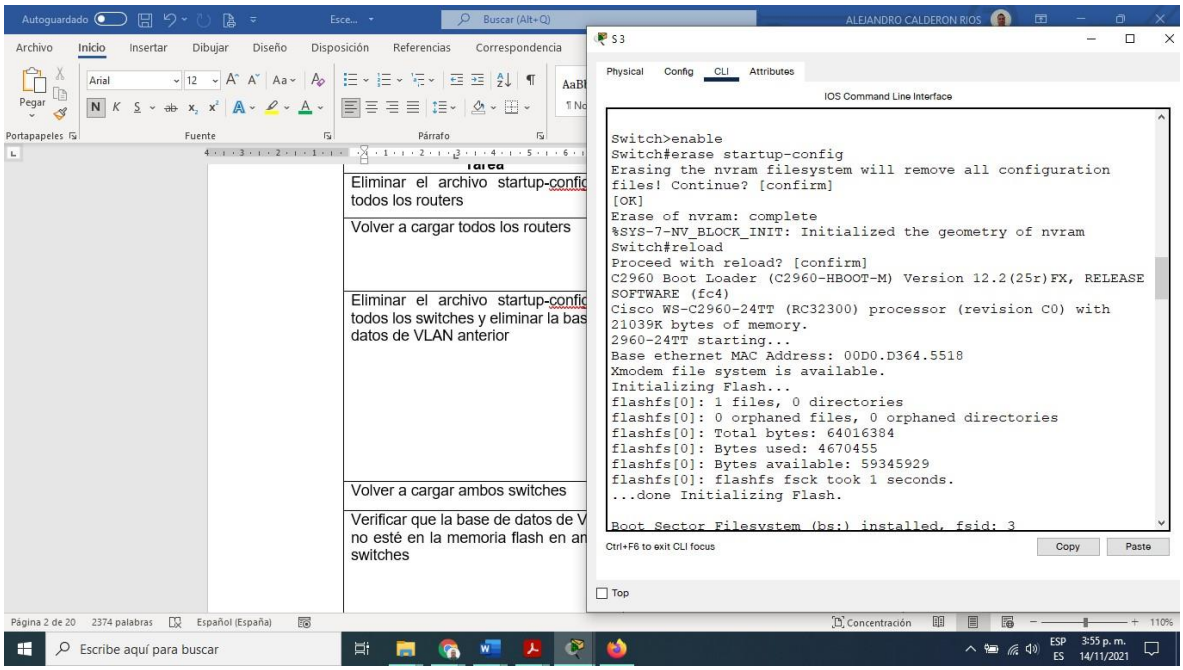
Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 7. Inicializando router

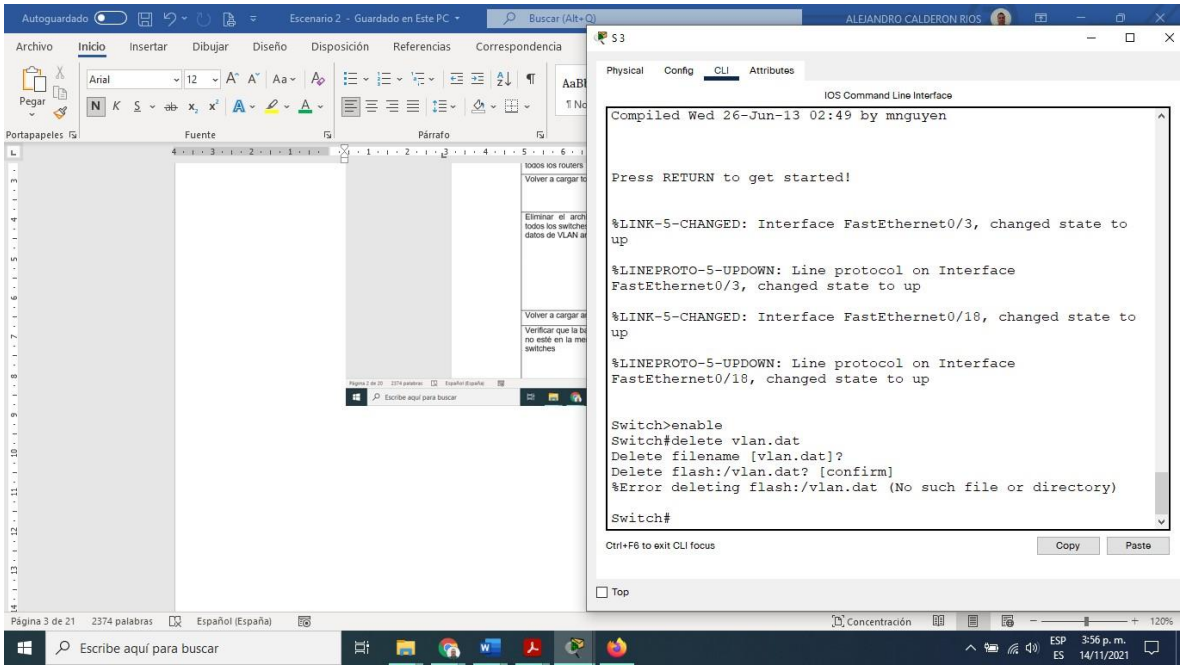
Tarea	Comandos
Eliminar el archivo startup-config de todos los routers	Router>enable Router#erase startup-config
Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm] Would you like to enter the initial configuration dialog? [yes/no]: no
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Switch# Switch#delete vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm]
Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm]
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>enable Switch#show flash Directory of flash:/ 1 -rw- 4670455 <no date> 2960-lanbasek9-mz.150-2.SE4.bin 64016384 bytes total (59345929 bytes free) Switch#

Figura 39. Comando startup-config S3



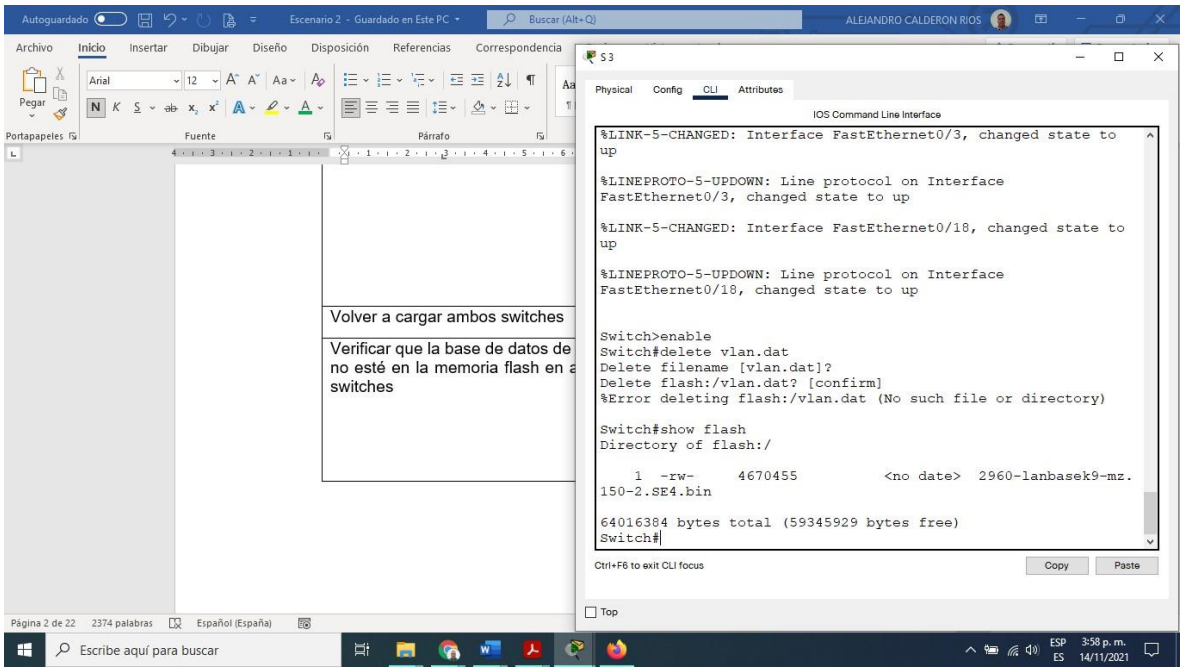
Fuente: Elaboración propia

Figura 40. Comando delete vlan.dat



Fuente: Elaboración propia

Figura 41. Verificación de base de datos comando show flash



Fuente: Elaboración propia

Parte 2: Configurar los parámetros básicos de los dispositivos

2.2 Paso 1: Configurar la computadora de Internet

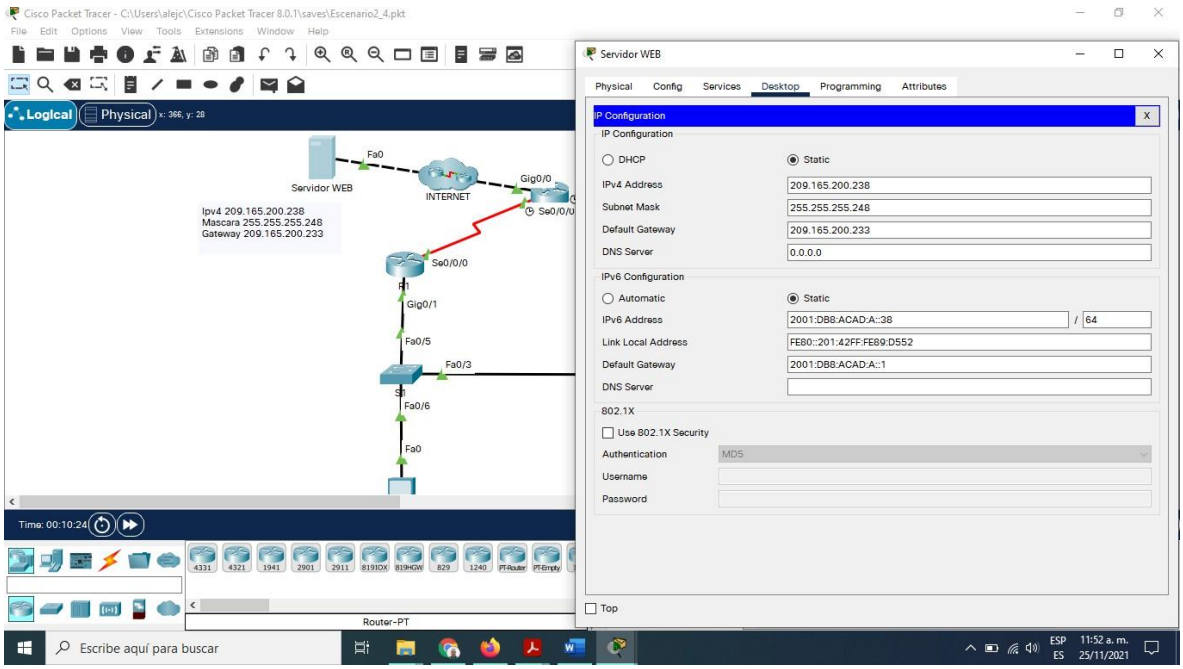
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 8. Configuración servidor web

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1/64

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Figura 42. Servidor web



Fuente: Elaboración propia

2.3.1 Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

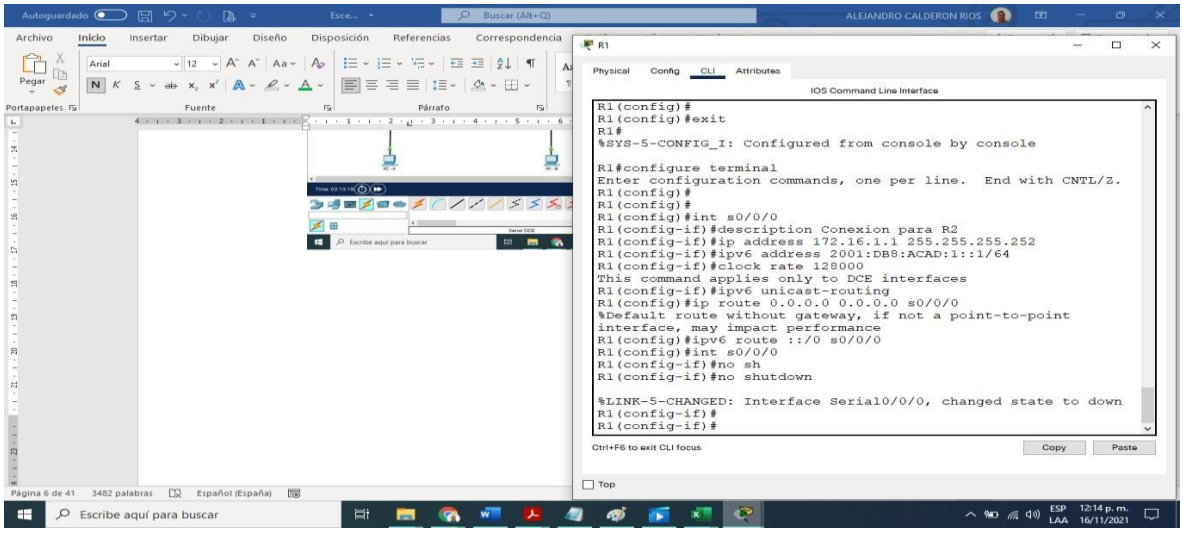
Tabla 9. Configuración R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#no ip domain-lookup
Nombre del router	R1 Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	class R1(config)#enable secret class

Contraseña de acceso a la consola	cisco R1(config)#line con 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	cisco R1(config)#line vty 04 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. R1(config)#banner motd $Se Prohibe el Acceso No Autorizado...!!$
Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

Nota: Todavía no configure G0/1.

Figura 43. Configuración de interfaz s/0/0/0



Fuente: Elaboración propia

2.3.2 La configuración del R2 incluye las siguientes tareas:

Tabla 10. Paso 3: Configurar R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	*Router(config)#no ip domain-lookup*
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Habilitar el servidor HTTP	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz

Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

Figura 44. Configuración R2 parte 1

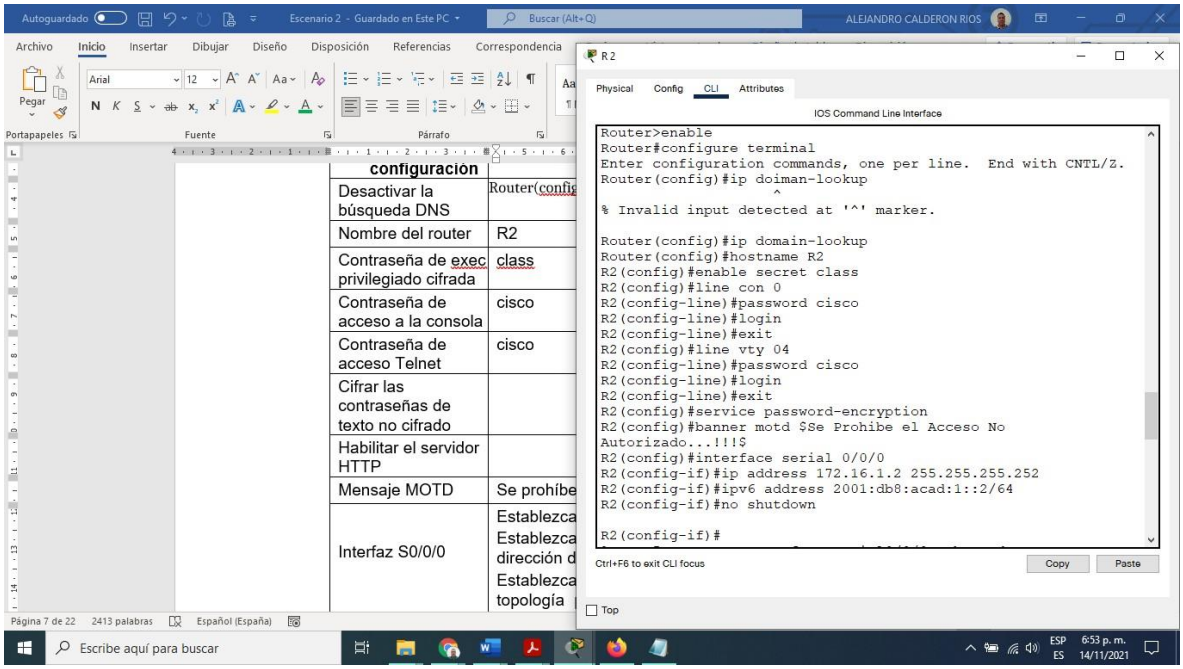
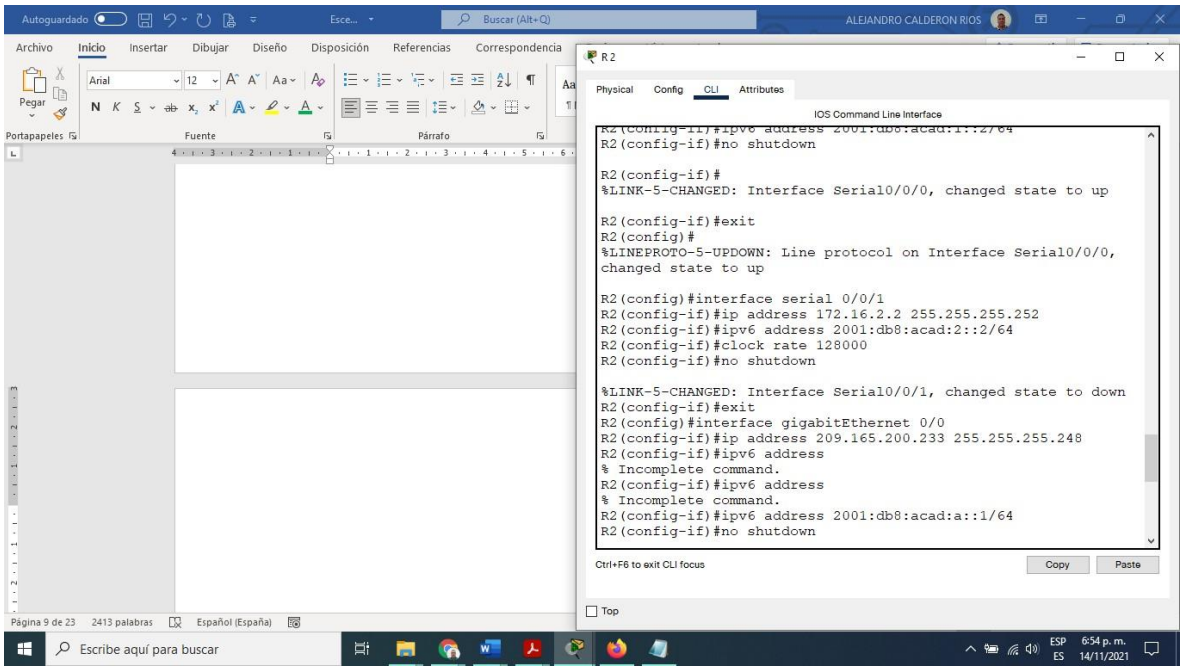
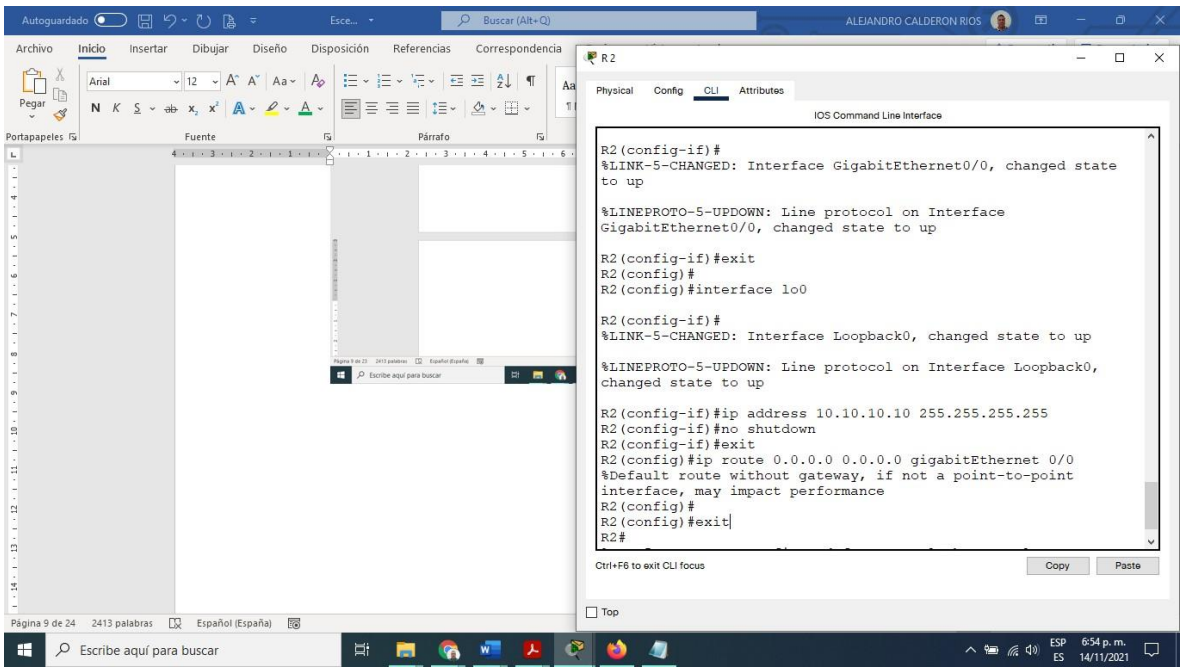


Figura 45. Configuración R2 parte 2 – interface gigabitEthernet 0/0



Fuente: Elaboración propia

Figura 46. Descripción y servidor web R2



Fuente: Elaboración propia

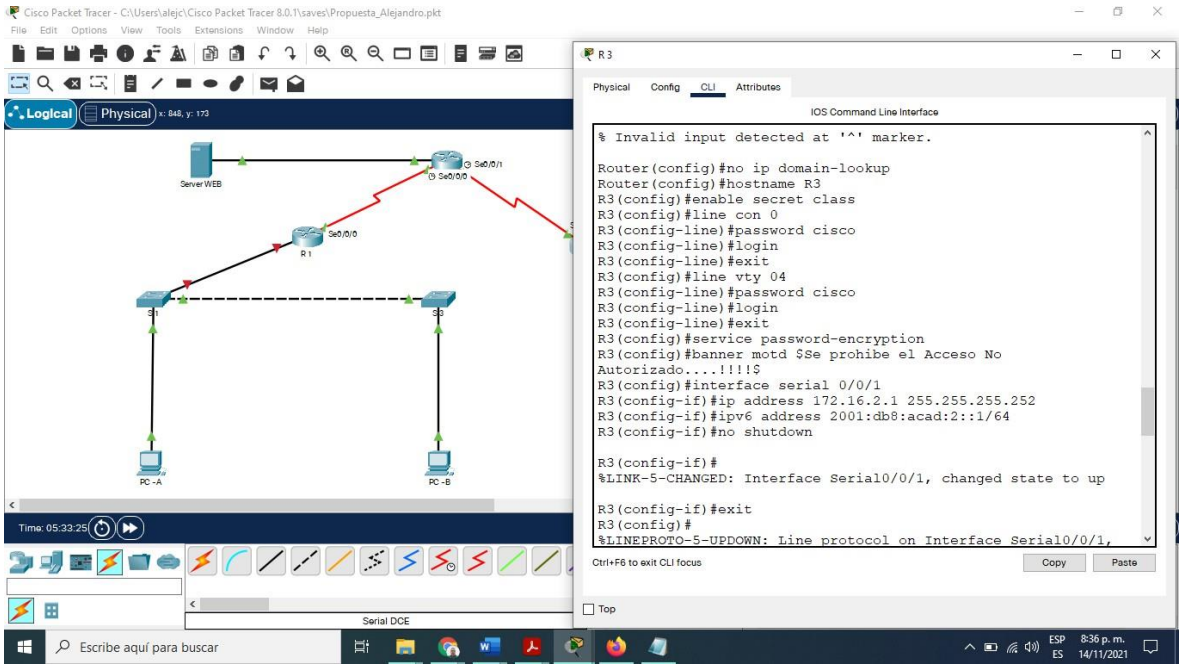
2.3.3 La configuración del R3 incluye las siguientes tareas:

Tabla 11. Paso 4: Configurar R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.

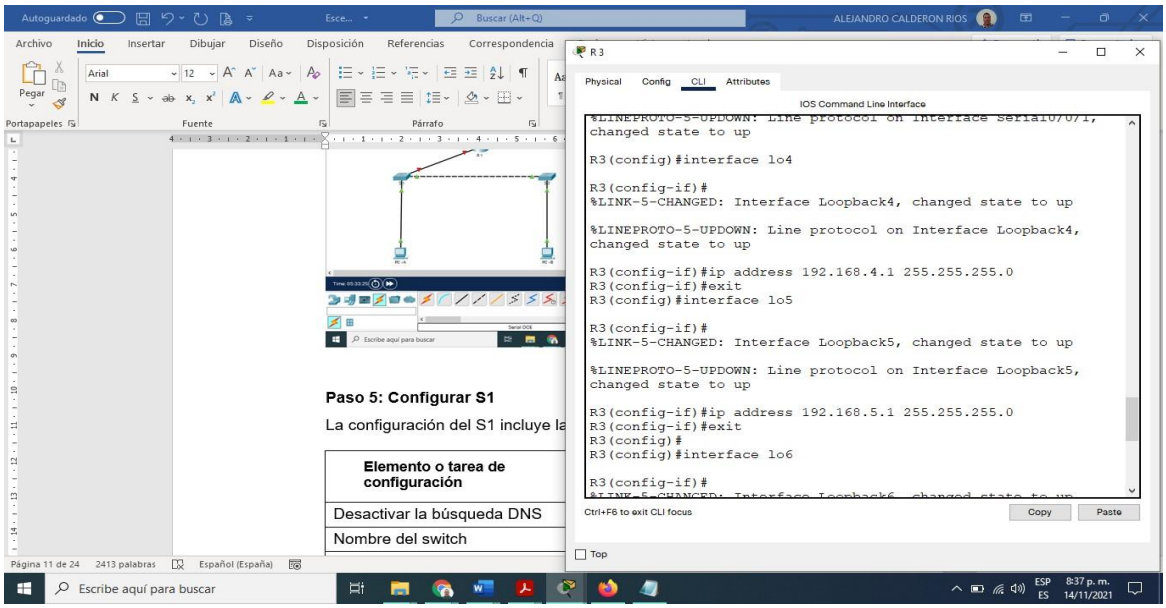
Rutas predeterminadas

Figura 47. Configuración R3



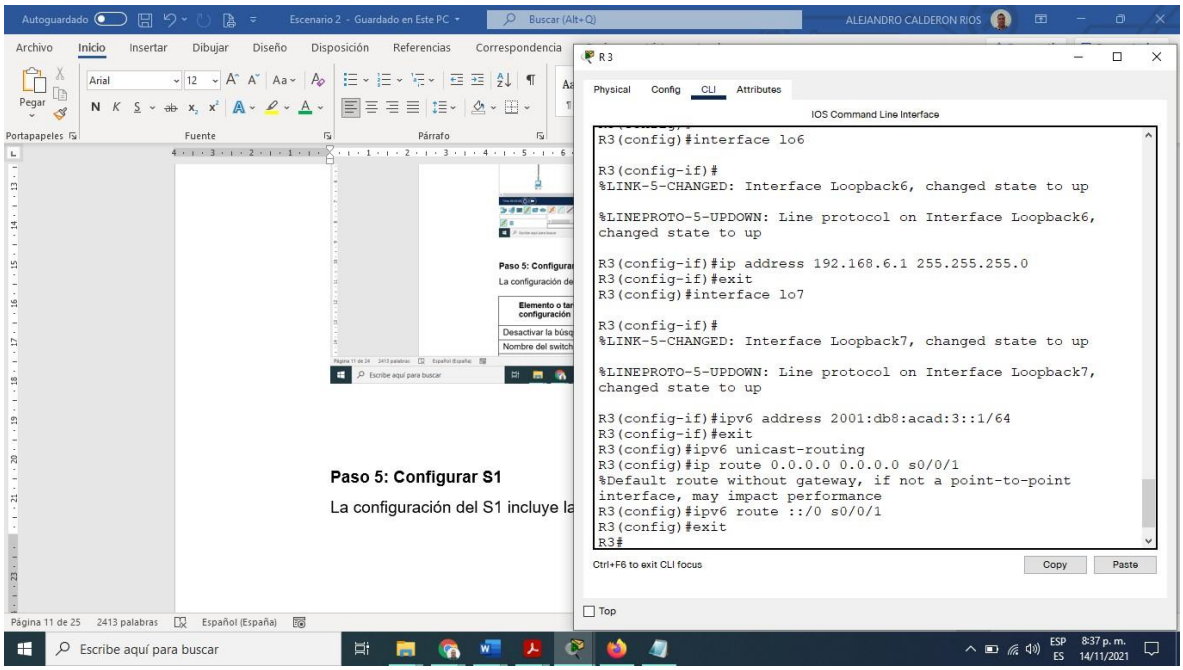
Fuente: Elaboración propia

Figura 48. Configuración R3 parte 2 loopback 4 - 6



Fuente: Elaboración propia

Figura 49. Ipv6 y loopback 7 R3



Fuente: Elaboración propia

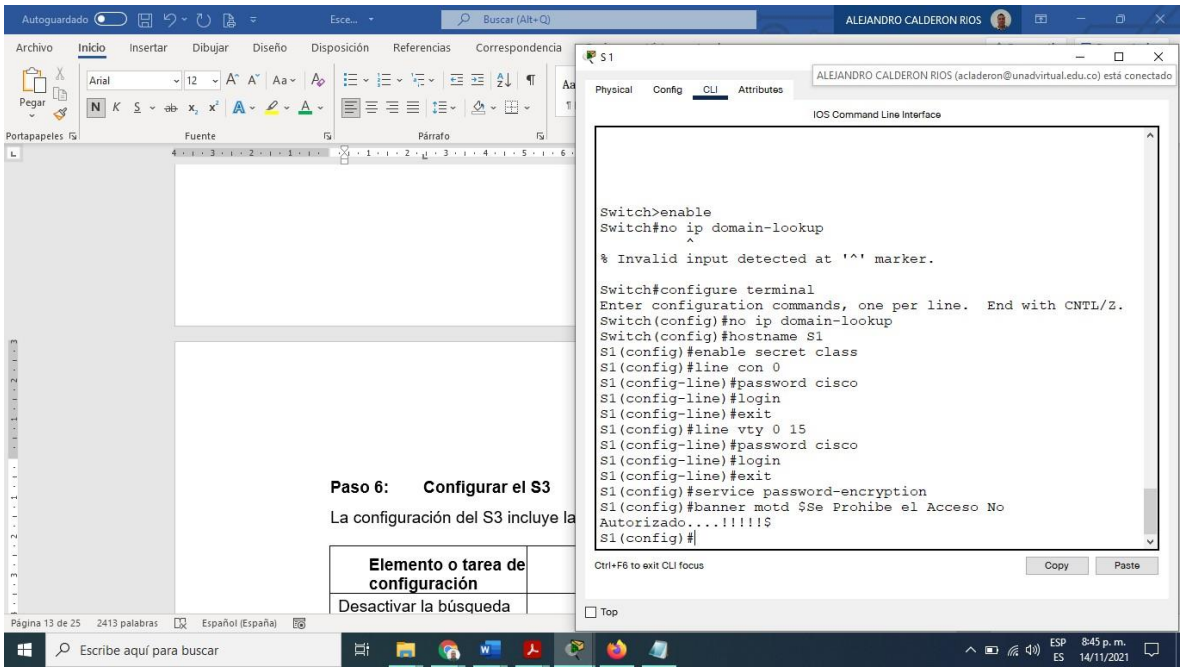
2.4.1 La configuración del S1 incluye las siguientes tareas:

Tabla 12. Paso 5: Configurar S1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	
Nombre del switch	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	

Mensaje MOTD	Se prohíbe el acceso no autorizado.

Figura 50. Configuración S1, paso 5



Fuente: Elaboración propia

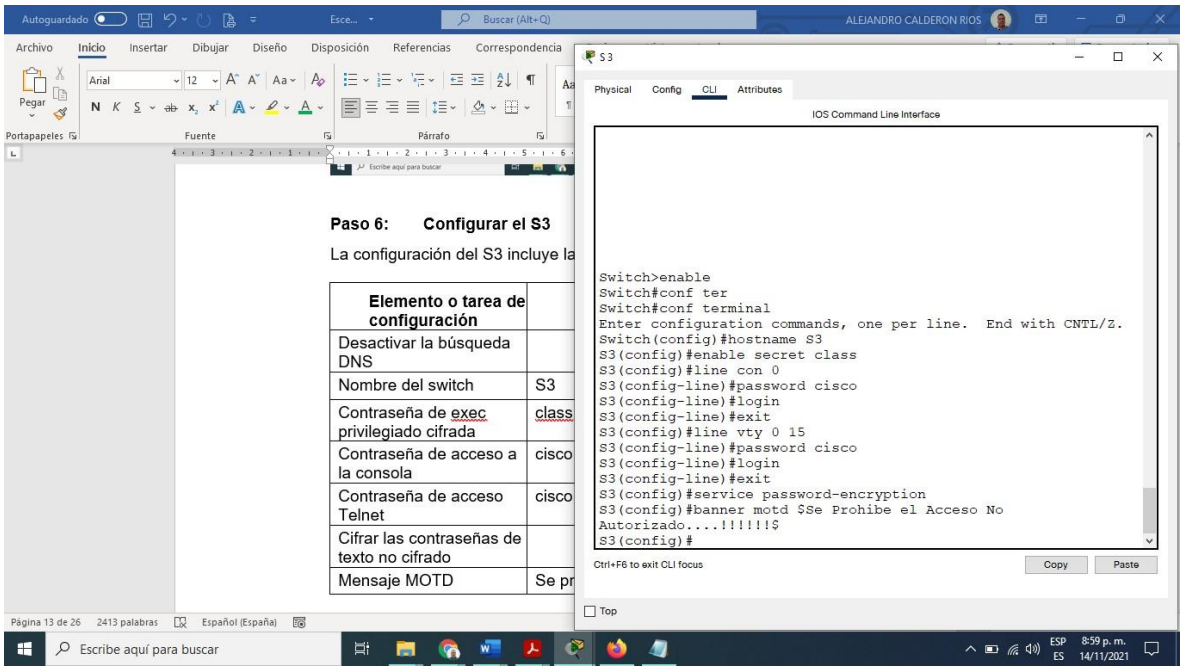
2.4.2 La configuración del S3 incluye las siguientes tareas:

Tabla 13. Paso 6: Configurar el S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso	cisco

Telnet	
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Figura 51. Configuración S3, paso 6



Fuente: Elaboración propia

2.5 Paso 7: Verificar la conectividad de la red

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

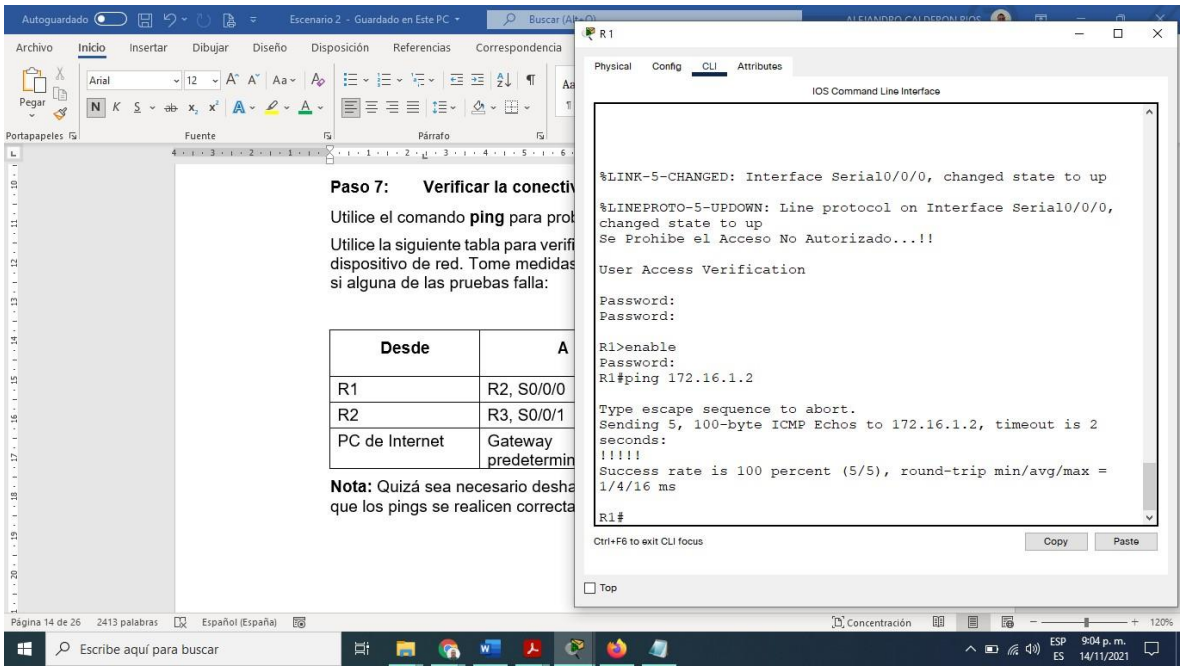
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 14. Conectividad

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms
R2	R3, S0/0/1	*172.16.2.1*	Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/13 ms
PC de Internet	Gateway predeterminado	209.165.200.233	Pinging 209.165.200.233 with 32 bytes of data: Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Ping statistics for 209.165.200.233: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms

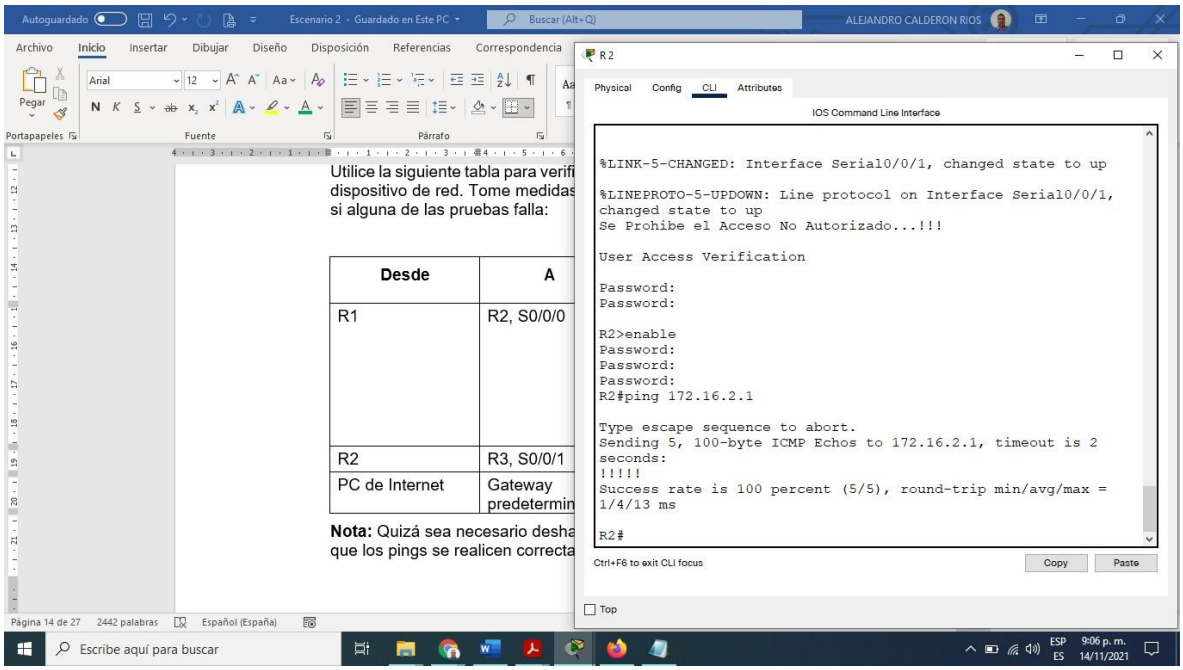
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Figura 52. Conectividad de R1 a R2 s0/0/0 172.16.1.2



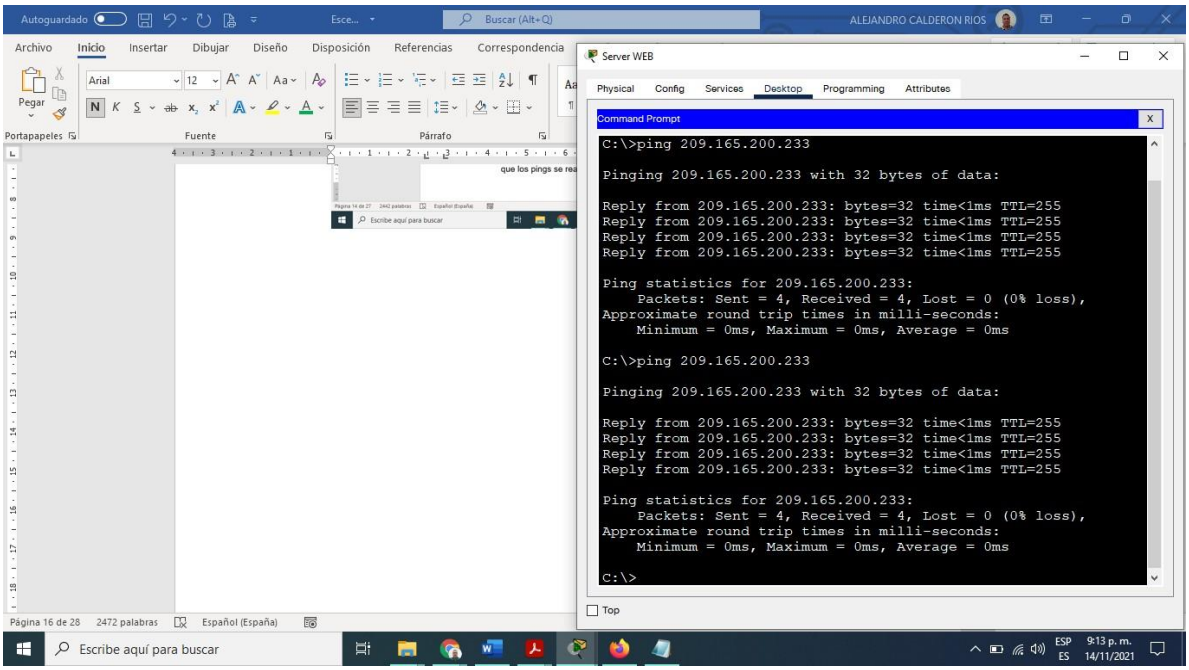
Fuente: Elaboración propia

Figura 53. Conectividad de R2 a R3 s0/0/0 172.16.2.1



Fuente: Elaboración propia

Figura 54. Ping PC internet a gateway predeterminado 209.165.200.233



Fuente: Elaboración propia

2.6 Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN Paso 1: Configurar S1

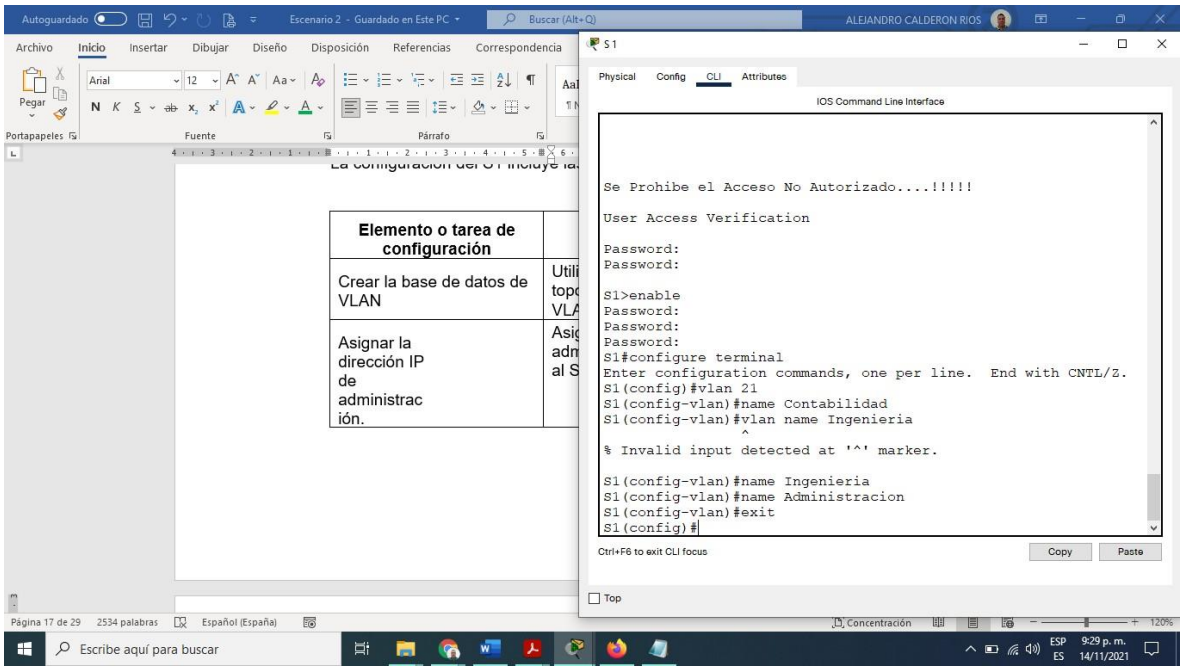
La configuración del S1 incluye las siguientes tareas:

Tabla 15. Configuración de vlan S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)# %LINK-5-CHANGED: Interface Vlan99, changed state to up S1(config-vlan)#name Administracion VLAN #21 and #99 have an identical name: Administracion S1(config-vlan)#

	S1(config-vlan)#exit
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#exit
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. S1(config)#ip default-gateway 192.168.99.1 S1(config)#
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S1(config)#interface fastEthernet 0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trun native vlan 1 S1(config-if)#exit
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa S1(config)#interface fastEthernet 0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit S1(config)#
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S1(config)#interface range fa0/1-2, fa0/4, fa0/6-24 S1(config-if-range)#switchport access vlan 21 S1(config-if-range)#exit S1(config)#
Asignar F0/6 a la VLAN 21	S1(config)#interface range fa0/6 S1(config-if-range)#switchport access vlan 21 S1(config-if-range)#exit
Apagar todos los puertos sin usar	S1(config)#interface range fa0/1-2, fa0/4, fa0/7-24, gi0/1-2 S1(config-if-range)#shutdown

Figura 55. Vlan S1



Fuente: Elaboración propia

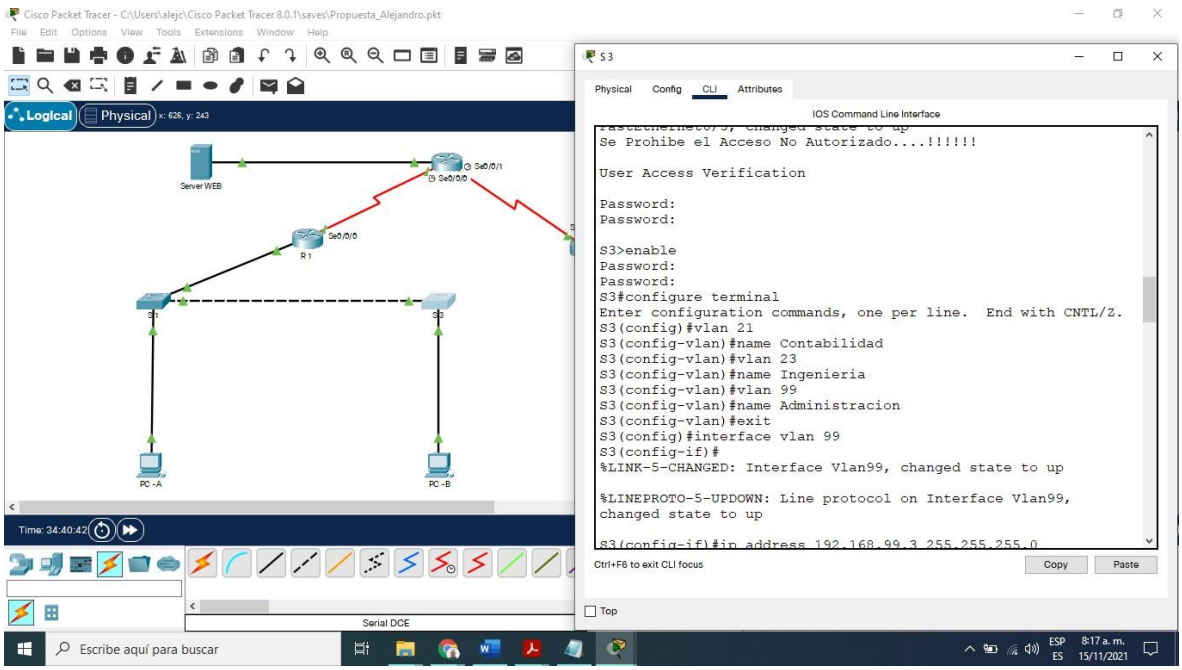
2.6.1 La configuración del S3 incluye las siguientes tareas:

Tabla 16. Paso 2: Configurar el S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN. S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología S3(config)#interface vlan 99 S3(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up

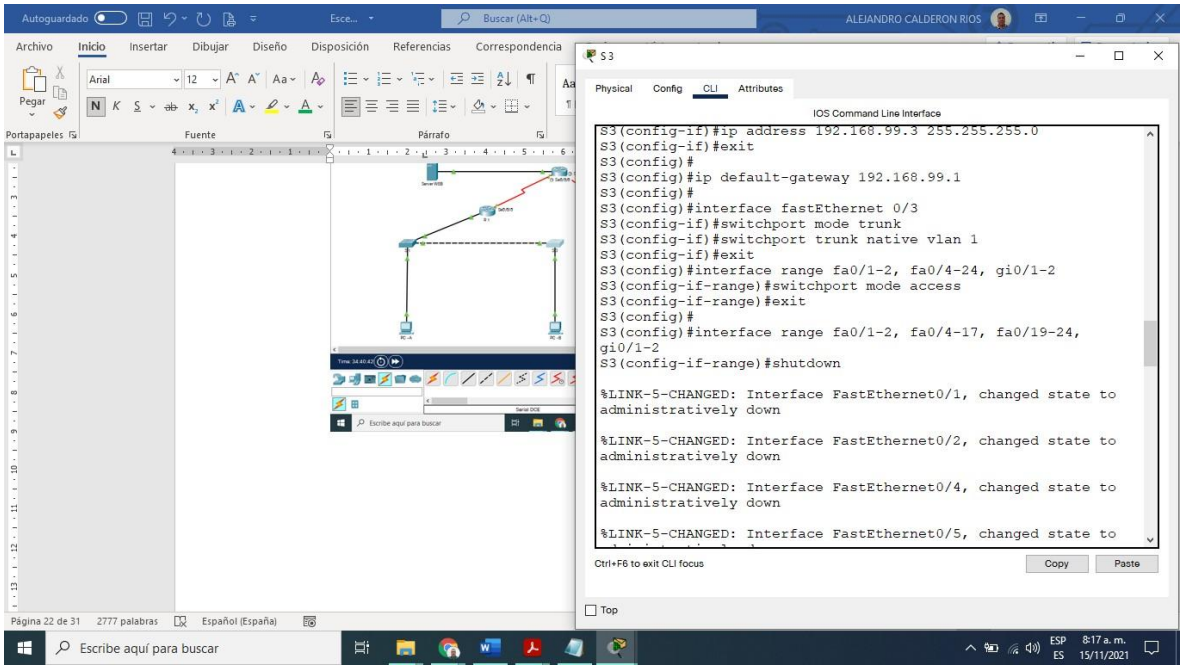
	%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#exit
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. S3(config)#ip default-gateway 192.168.99.1 S3(config)#
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S3(config)#interface fastEthernet 0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S3(config)#interface range fa0/1-2, fa0/4-24, gi0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#exi
Asignar F0/18 a la VLAN 21	S3(config)#interface fastEthernet 0/18 S3(config-if)#switchport access vlan 21 S3(config-if)#exit
Apagar todos los puertos sin usar	S3(config)#interface range fa0/1-2, fa0/4-17, fa0/19-24, gi0/1-2 S3(config-if-range)#shutdown

Figura 56. Vlan S3 parte 1



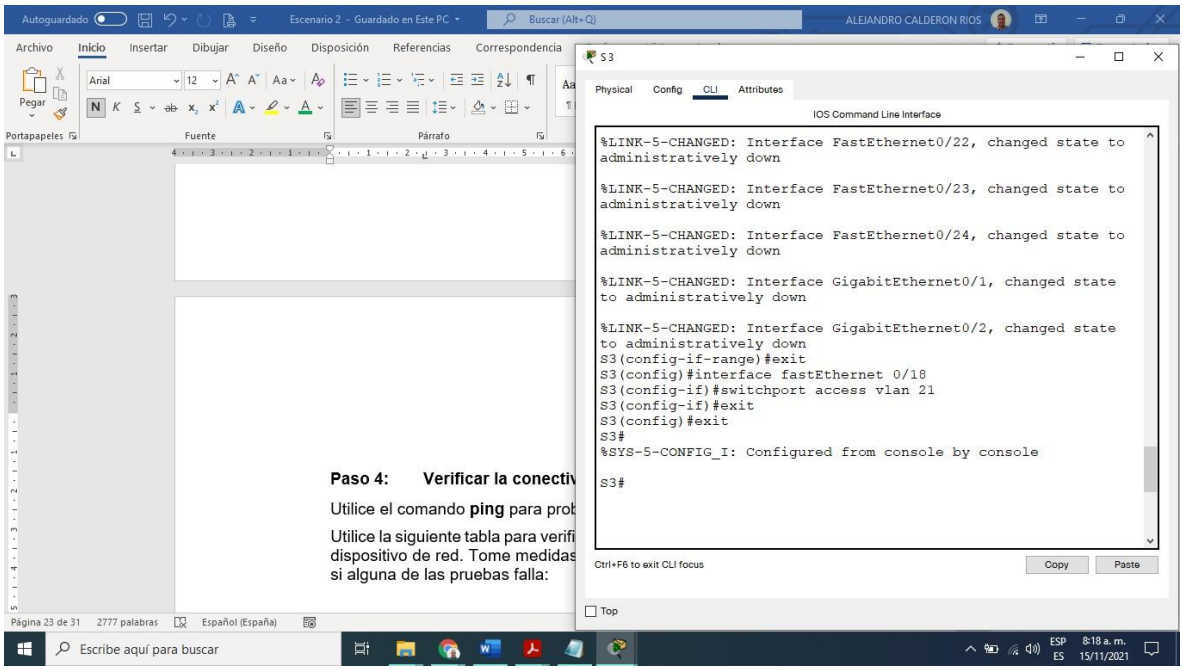
Fuente: Elaboración propia

Figura 57. Vlan S3 parte 2



Fuente: Elaboración propia

Figura 58. Vlan S3 parte 3



Fuente: Elaboración propia

2.6.2 Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17. Configuraciones de subinterfaces vlan 21, 23 y 99 R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz R1(config)#interface gigabitEthernet 0/1.21 R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#exit

Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz R1(config)#interface gigabitEthernet 0/1.23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz R1(config)#interface gigabitEthernet 0/1.99 R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#exit
Activar la interfaz G0/1	R1(config)#interface gigabitEthernet 0/1 R1(config-if)#no shutdown

2.7 Paso 4: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los switches y el R1.

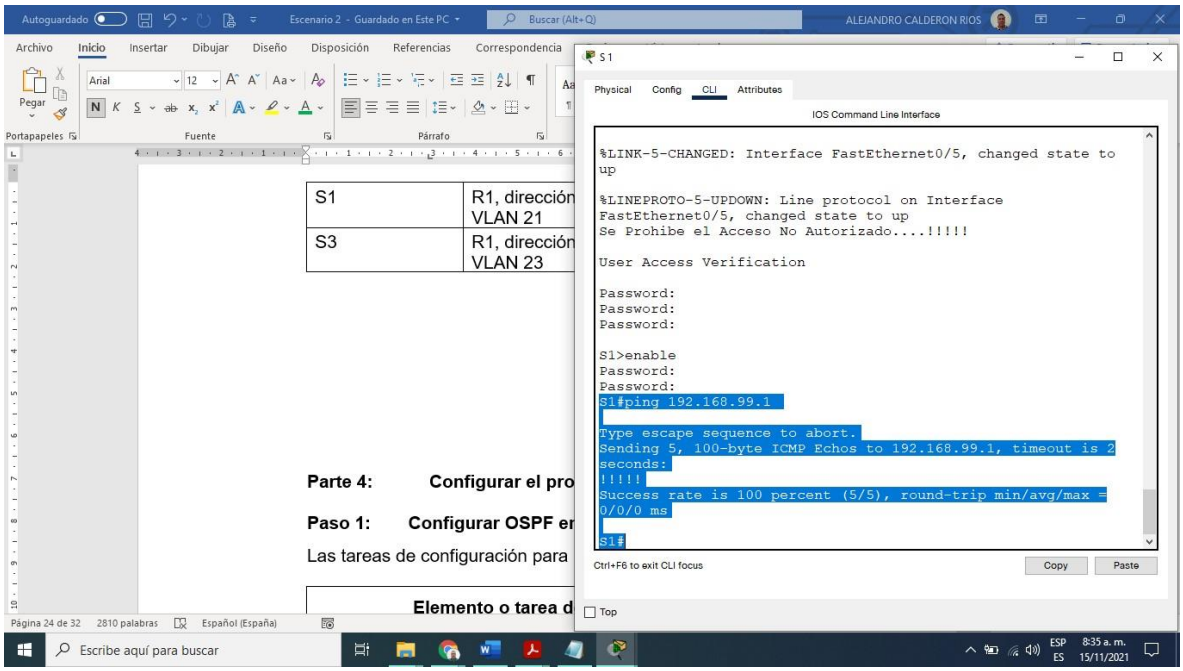
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 18. Conectividad en la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms S1#
S3	R1, dirección VLAN 99	192.168.99.1	S3#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!!

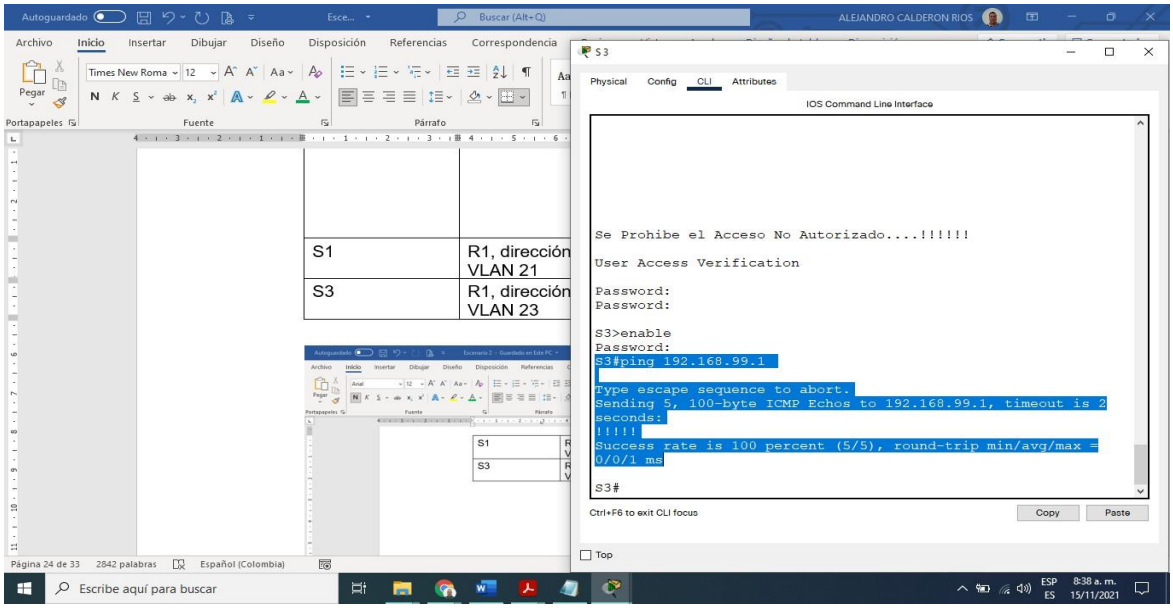
			Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S1	R1, dirección VLAN 21	192.168.21.1	S1#ping 192.168.21.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 23	192.168.23.1	S3#ping 192.168.23.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

Figura 59. Ping 192.168.99.1 desde S1 a R1 vlan 99



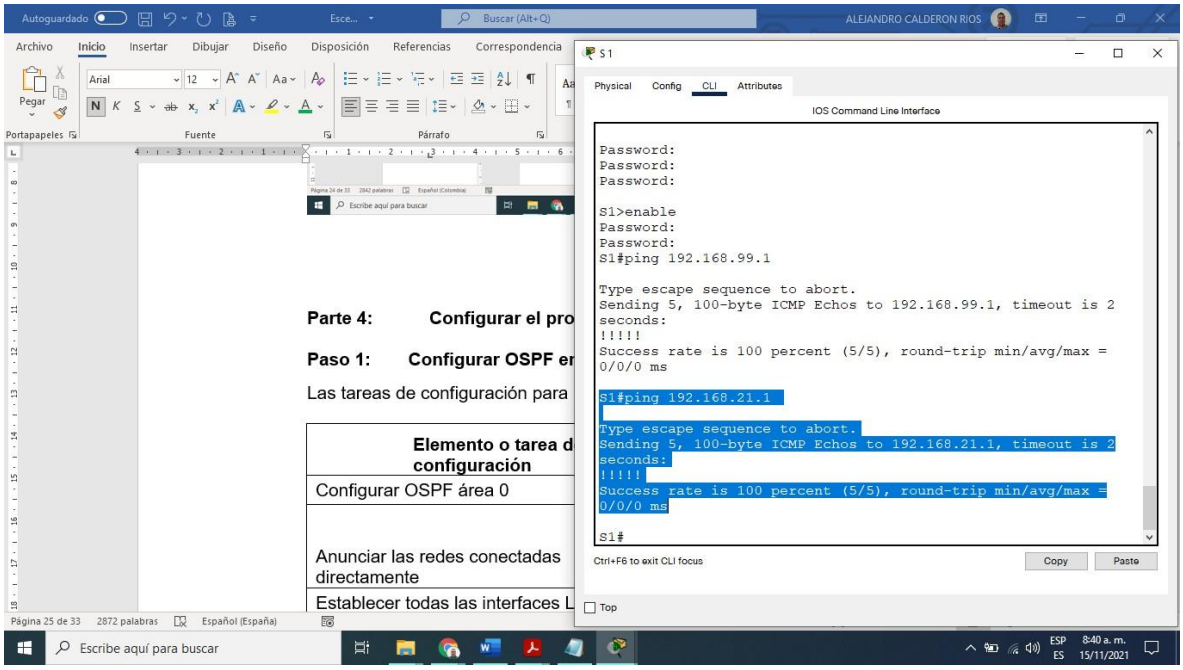
Fuente: Elaboración propia

Figura 60. Ping 192.168.99.1 desde S3 a R1 vlan 99



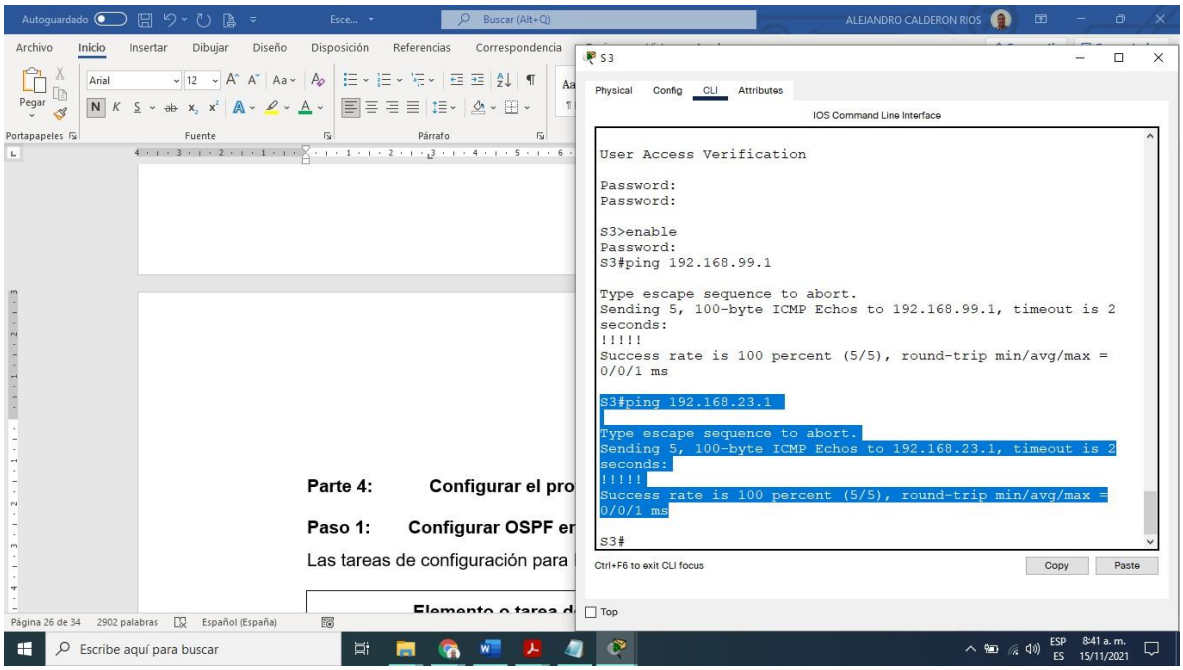
Fuente: Elaboración propia

Figura 61. S1 a R1 vlan 21 192.168.21.1



Fuente: Elaboración propia

Figura 62. S3 a R1 Vlan 23 192.168.23.1



Fuente: Elaboración propia

2.8 Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

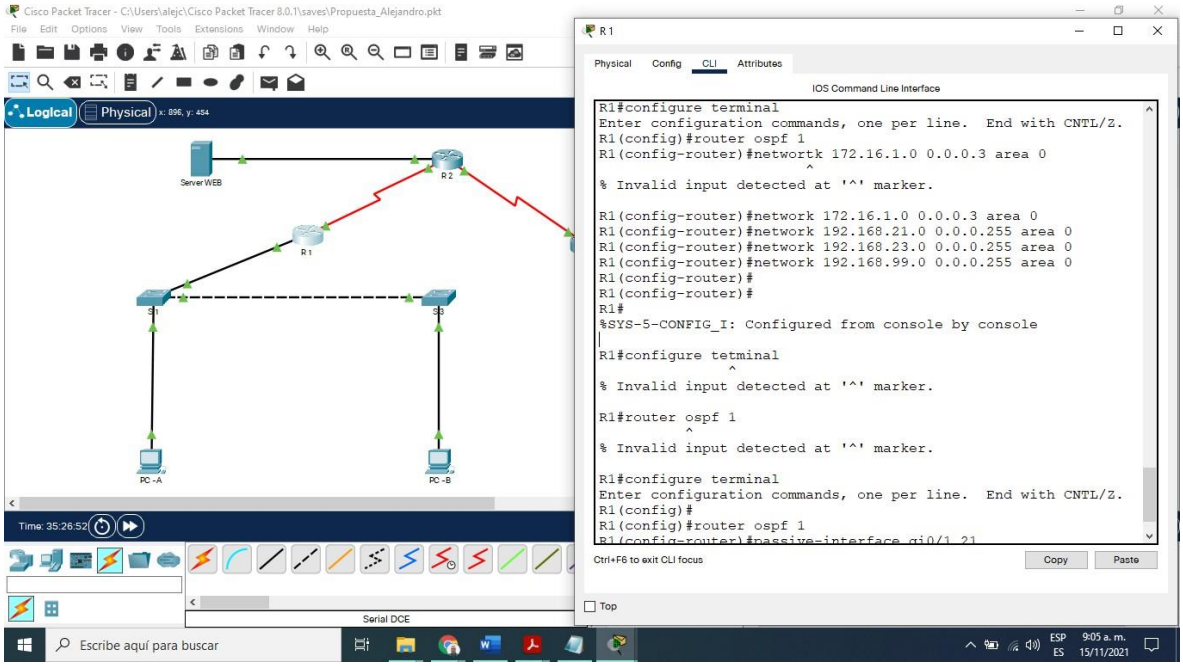
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 19. OSPF para R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 81, inicialmente lo había configurado con el numero (1) y después lo modifique al (81)
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. R1(config-router)#network 172.16.1.0 0.0.0.3 area 0

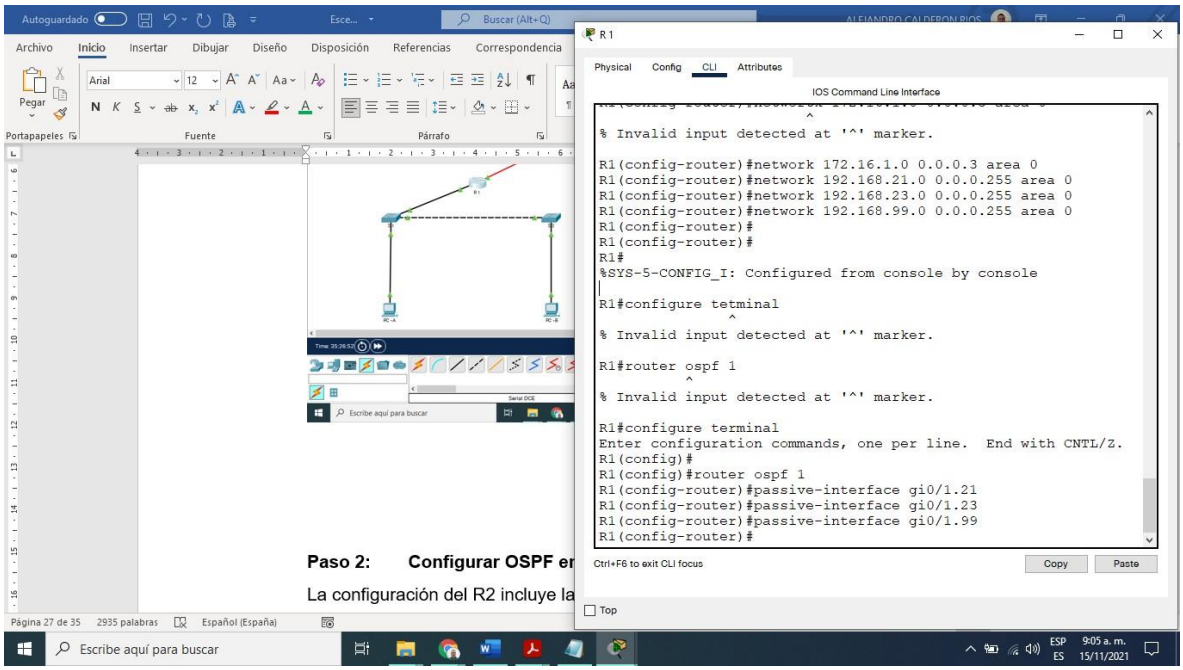
	R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0 R1(config-router)#
Establecer todas las interfaces LAN como pasivas	R1(config)#router ospf 81 R1(config-router)#passive-interface gi0/1.21 R1(config-router)#passive-interface gi0/1.23 R1(config-router)#passive-interface gi0/1.99
Desactive la sumarización automática	No se puede hacer en OSPF

Figura 63. Configuración de ospf en R1



Fuente: Elaboración propia

Figura 64. Configuración ospf LAN líneas pasivas



Fuente: Elaboración propia

2.8.1 Paso 2: Configurar OSPF en el R2

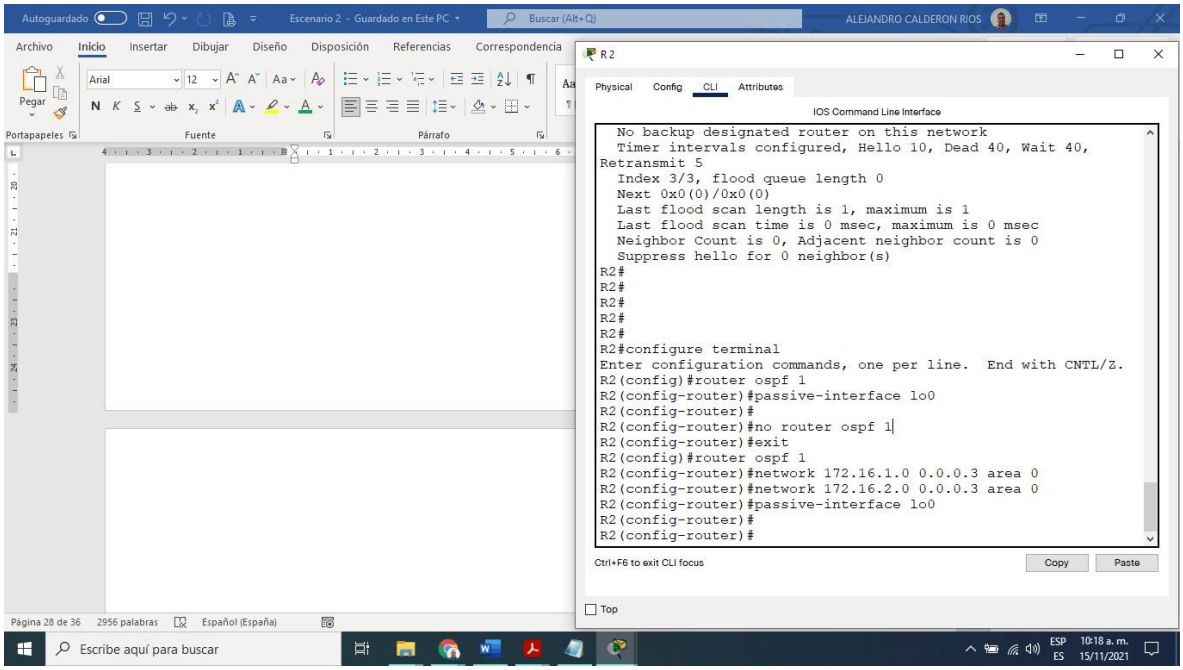
La configuración del R2 incluye las siguientes tareas:

Tabla 20. OSPF R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 81 Colocar los últimos dígitos preguntar al tutor del grupo
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. R2(config)#router ospf 1 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config)#router ospf 1 R2(config-router)#passive-interface lo0

Desactive la sumarización automática.	Para ospf no se puede realizar

Figura 65. Configuración tabla OSPF R2



Fuente: Elaboración propia

2.8.2 Paso 3: Configurar OSPFv3 en el R2

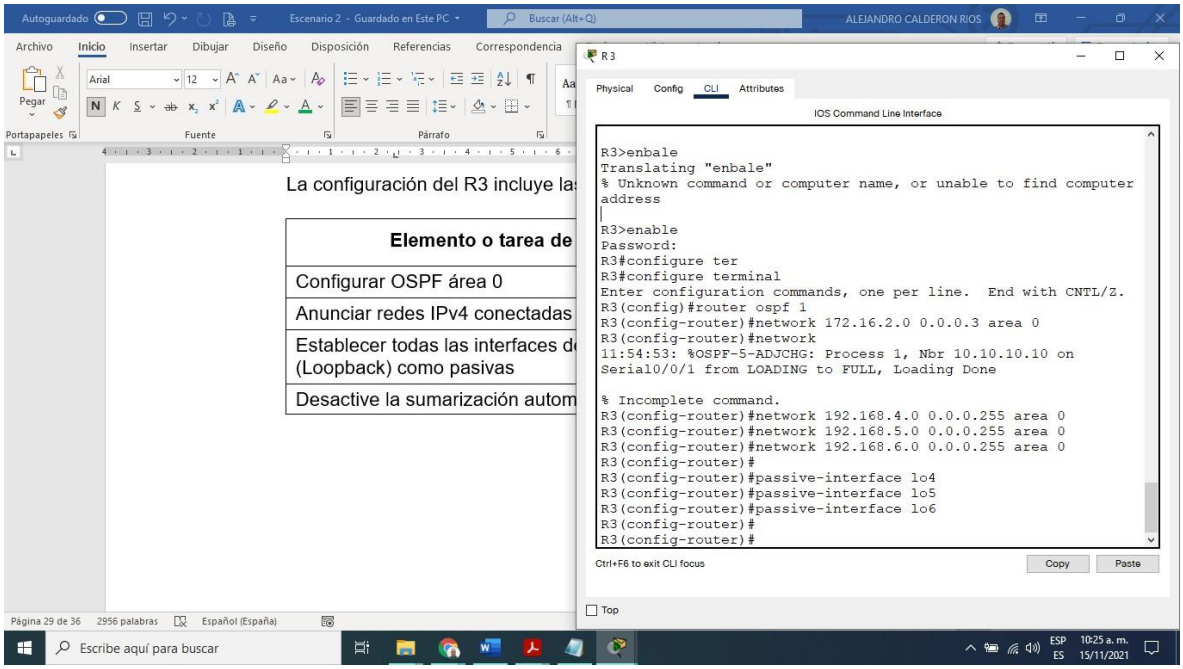
La configuración del R3 incluye las siguientes tareas:

Tabla 21. OSPF R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 81
Anunciar redes IPv6 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 11:54:53: %OSPF-5-ADJCHG: Process 1, Nbr 10.10.10.10 on Serial0/0/1 from LOADING to FULL, Loading Done % Incomplete command.

	R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router) #passive-interface lo6
Desactive la sumarización automática.	No se puede hacer en ipv6.

Figura 66. Configuración tabla OSPF R3



Fuente: Elaboración propia

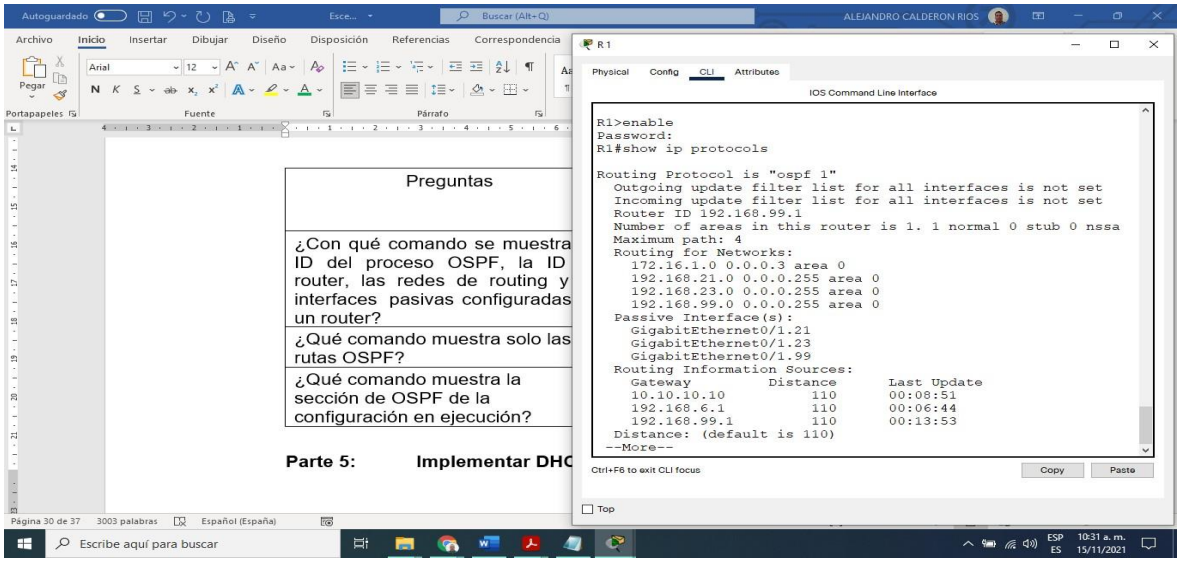
2.8.3 Paso 4: Verificar la información de OSPF

Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 22. resultados OSPF

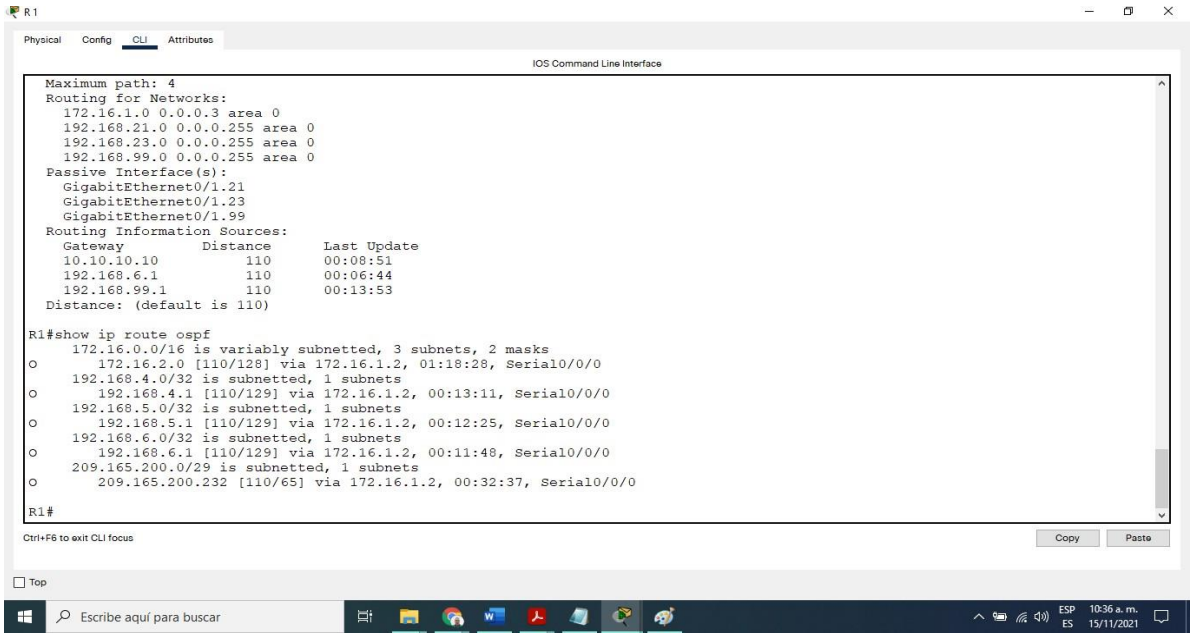
Preguntas	Respuestas
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	show ip protocols
¿Qué comando muestra solo las rutas OSPF?	R1#show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R1#show ip ospf database

Figura 67. Verificación comando show ip protocols



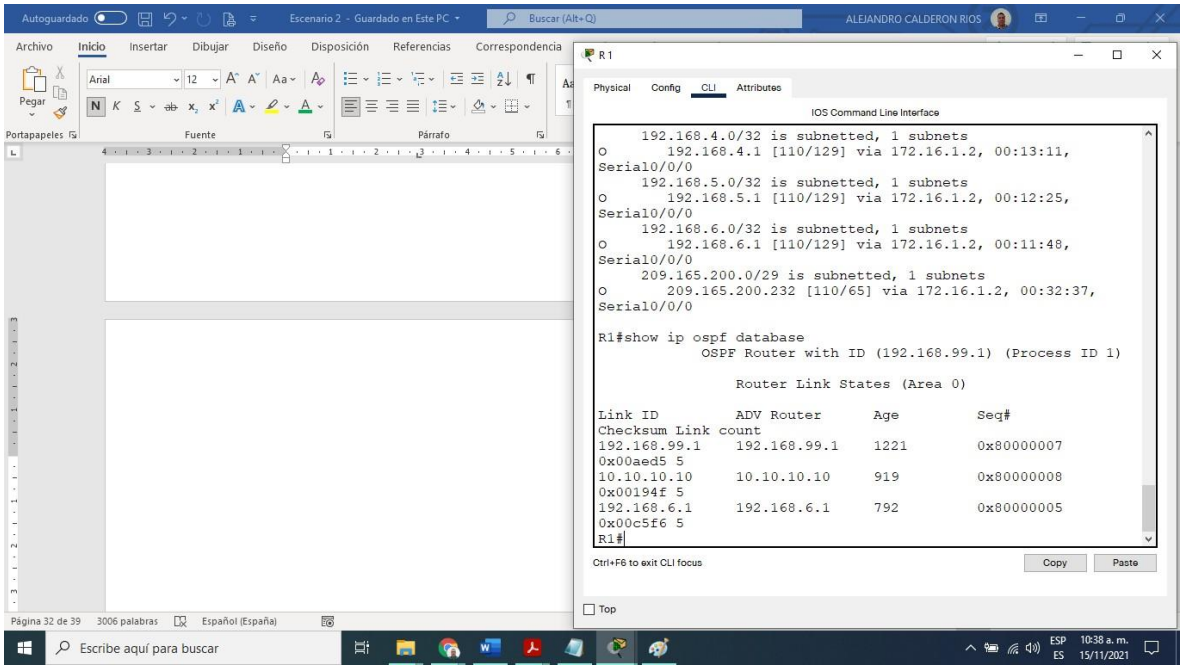
Fuente: Elaboración propia

Figura 68. Show ip route ospf



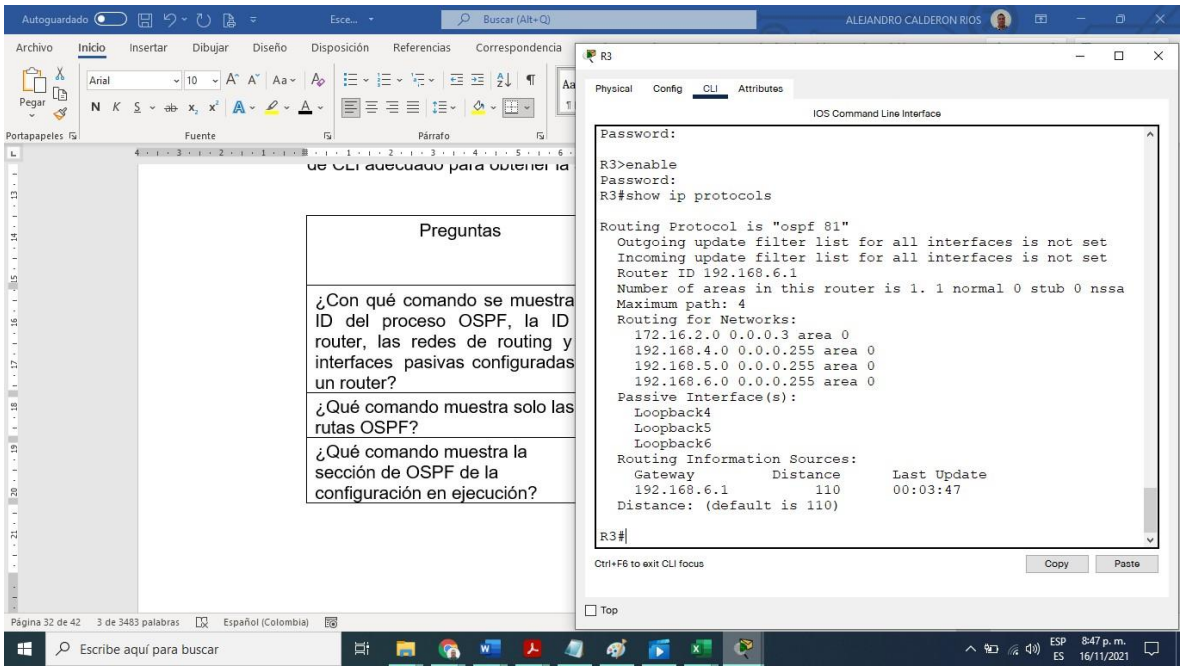
Fuente: Elaboración propia

Figura 69. Comando show ip ospf database



Fuente: Elaboración propia

Figura 70. Show ip protocols R3



Fuente: Elaboración propia

2.9 Parte 5: Implementar DHCP y NAT para IPv4

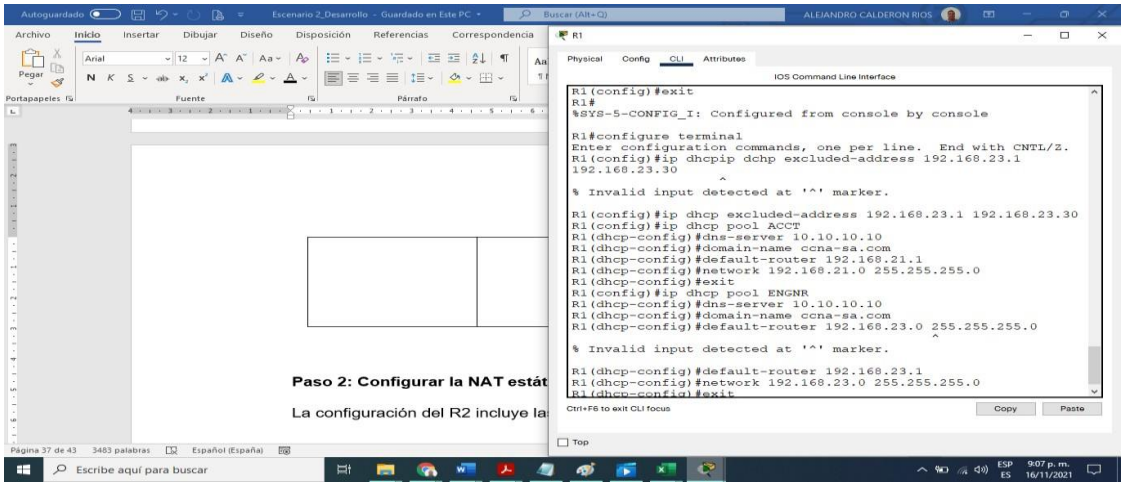
Las tareas de configuración para R1 incluyen las siguientes; para las Vlan 21 y 23

Tabla 23.Paso 1: Configurar el R1 como servidor de DHCP

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20

Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#exit
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#exit

Figura 71. Configuración de R1 como servidor de DHCP



Fuente: Elaboración propia

2.9.1 Paso 2: Configurar la NAT estática y dinámica en el R2

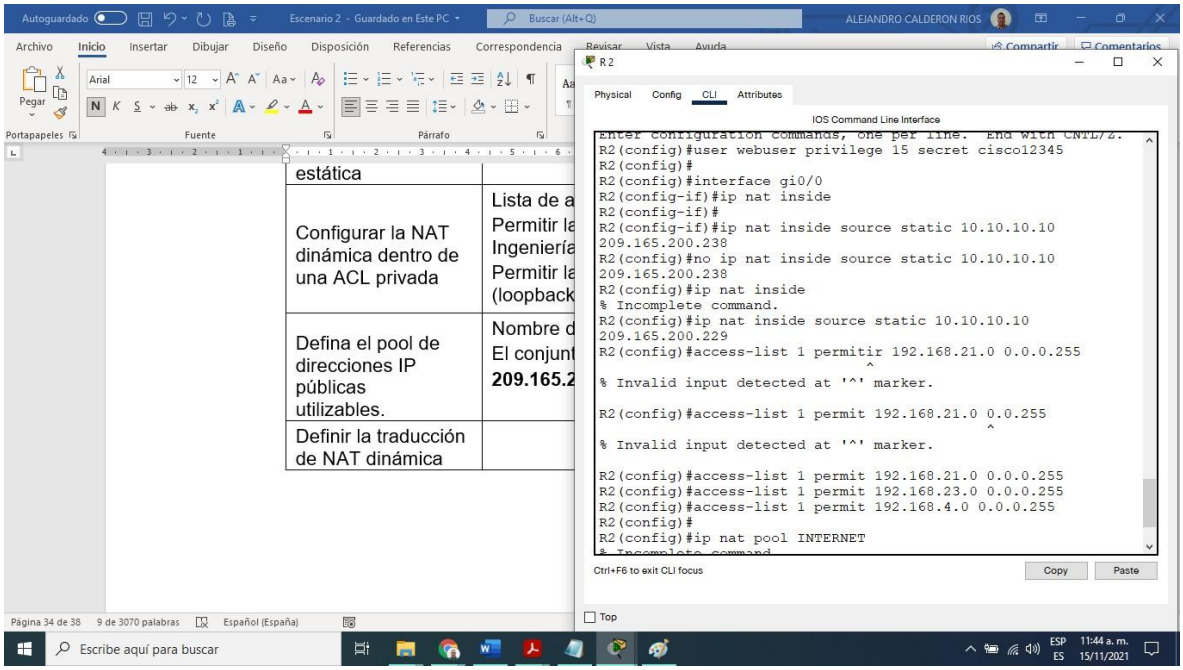
La configuración del R2 incluye las siguientes tareas:

Tabla 24. NAT estática – dinámica R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	No soportado en el simulador packet tracer
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	No soportado en el simulador packet tracer
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.229 con el ultimo octeto genero error se cambió por 233 y funciono R2(config)#ip nat inside source static 10.10.10.10 209.165.200.233
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface gi0/0 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#acce R2(config)#access-list 1 permit 192.168.0.0 0.0.7.255 R2(config)#no access-list 1 permit 192.168.0.0 0.0.7.255 R2(config)#access-list 1 permit 192.168.0.0 0.0.3.255

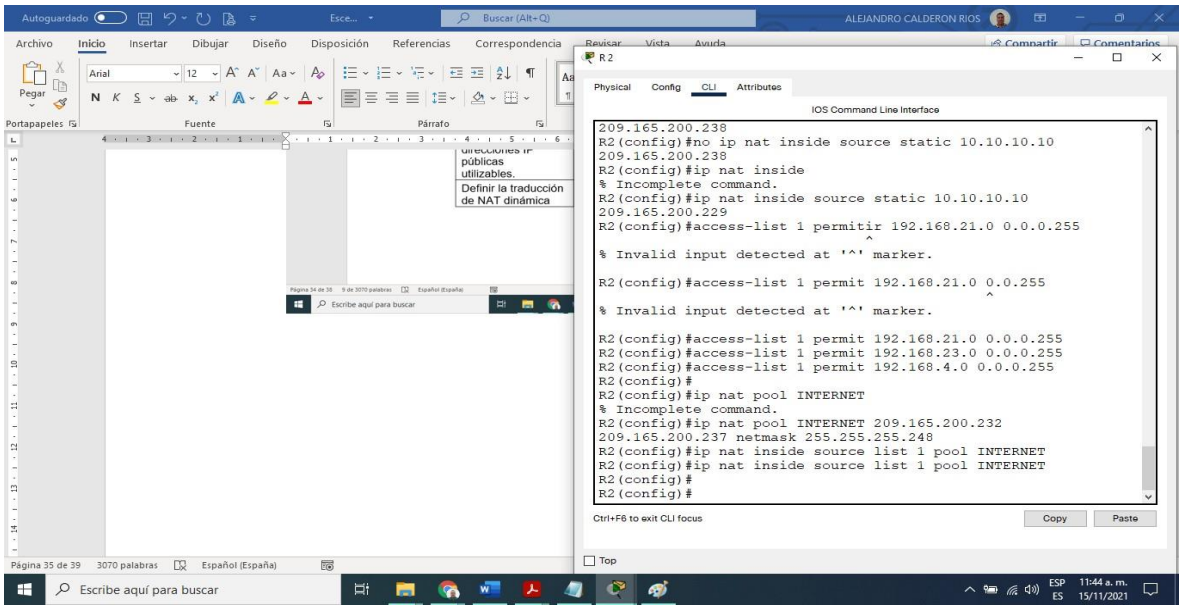
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228** R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Figura 72. Configuración tabla NAT estática – dinámica R2 parte 1



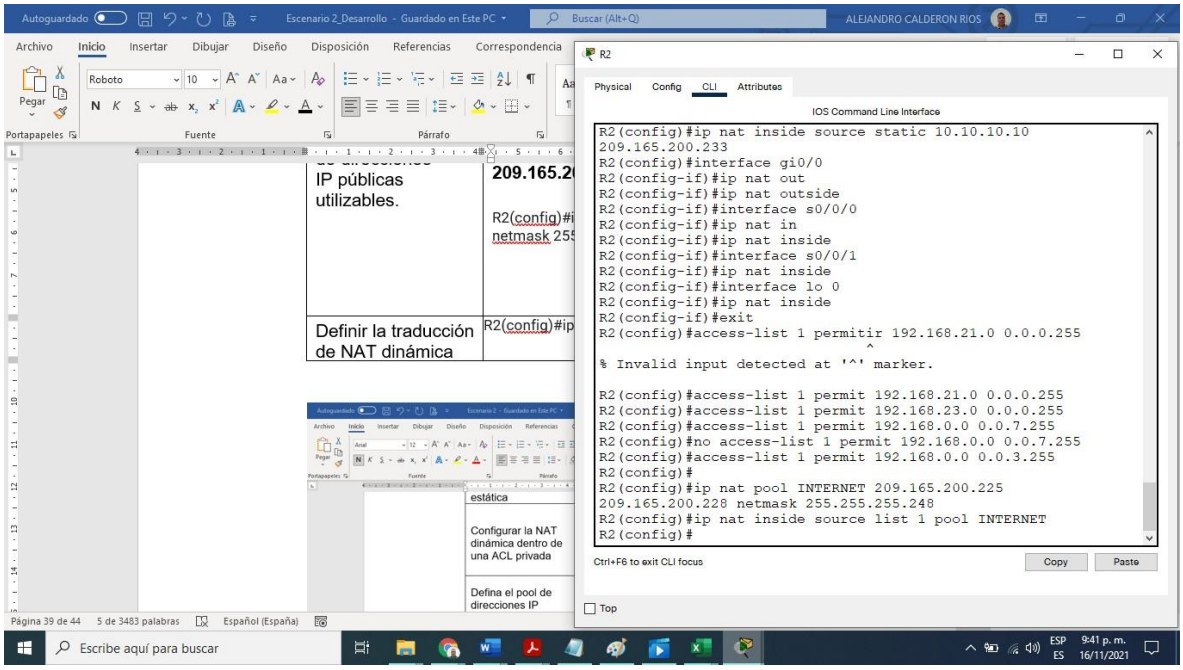
Fuente: Elaboración propia

Figura 73. Configuración tabla NAT estática – dinámica R2 parte 2



Fuente: Elaboración propia

Figura 74. Configuración tabla NAT estática – dinámica R2 parte 3



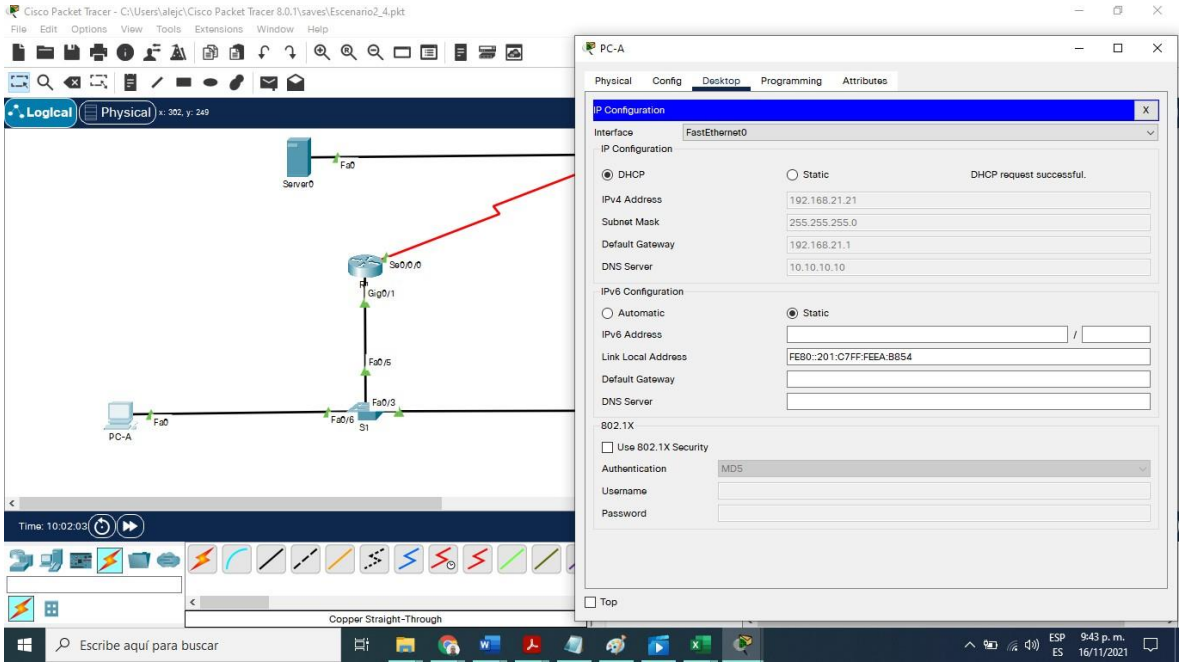
Fuente: Elaboración propia

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 25. Verificar protocolo DHCP y la NAT estática

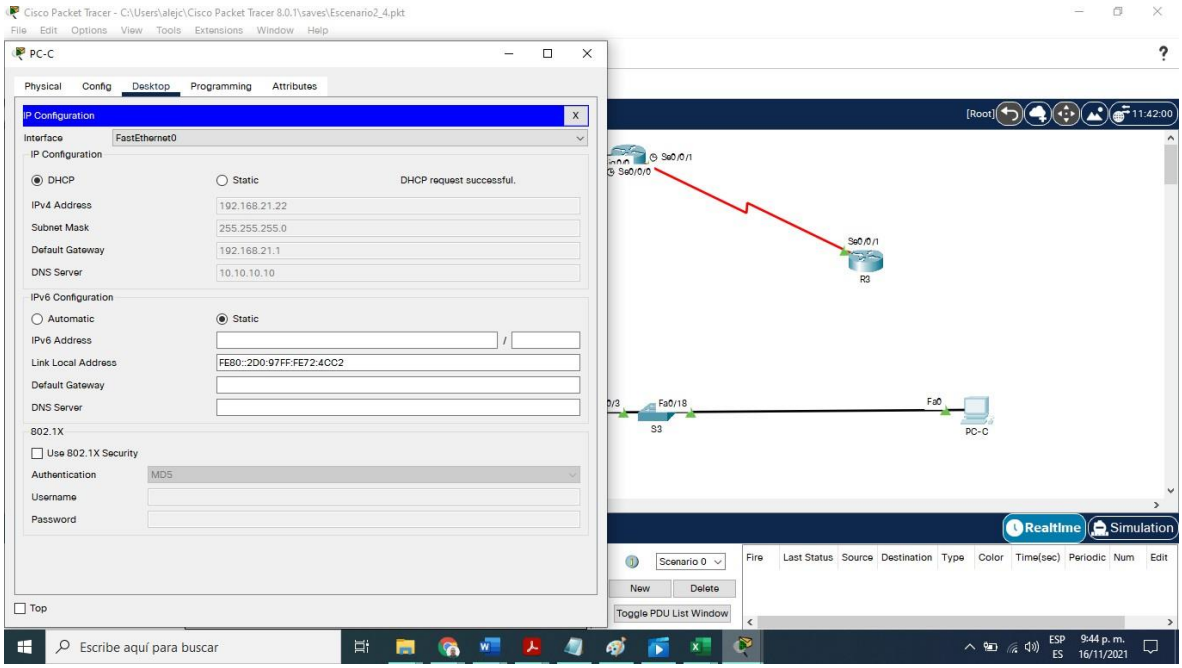
Pruebas	**Resultados**
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Ver ilustración Información del servidor DCHP – PC-A.
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Ver ilustración Información del servidor DCHP – PC-C
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	C:\>ping 192.168.21.22 Pinging 192.168.21.22 with 32 bytes of data: Reply from 192.168.21.22: bytes=32 time<1ms TTL=128 Reply from 192.168.21.22: bytes=32 time<1ms TTL=128 Reply from 192.168.21.22: bytes=32 time=2ms TTL=128 Reply from 192.168.21.22: bytes=32 time<1ms TTL=128
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Al probar con esta ip 209.165.200.229 genera error. Se realizo con esta y es exitoso la conexión al servidor 209.165.200.238

Figura 75. Información del servidor DCHP – PC-A



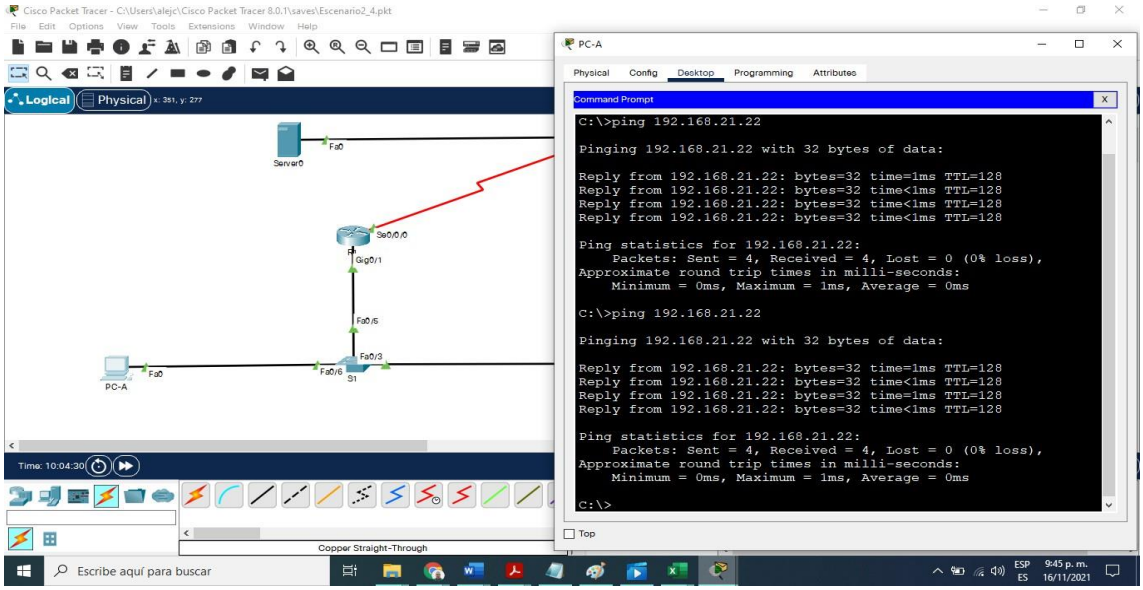
Fuente: Elaboración propia

Figura 76. Información del servidor DCHP – PC-C



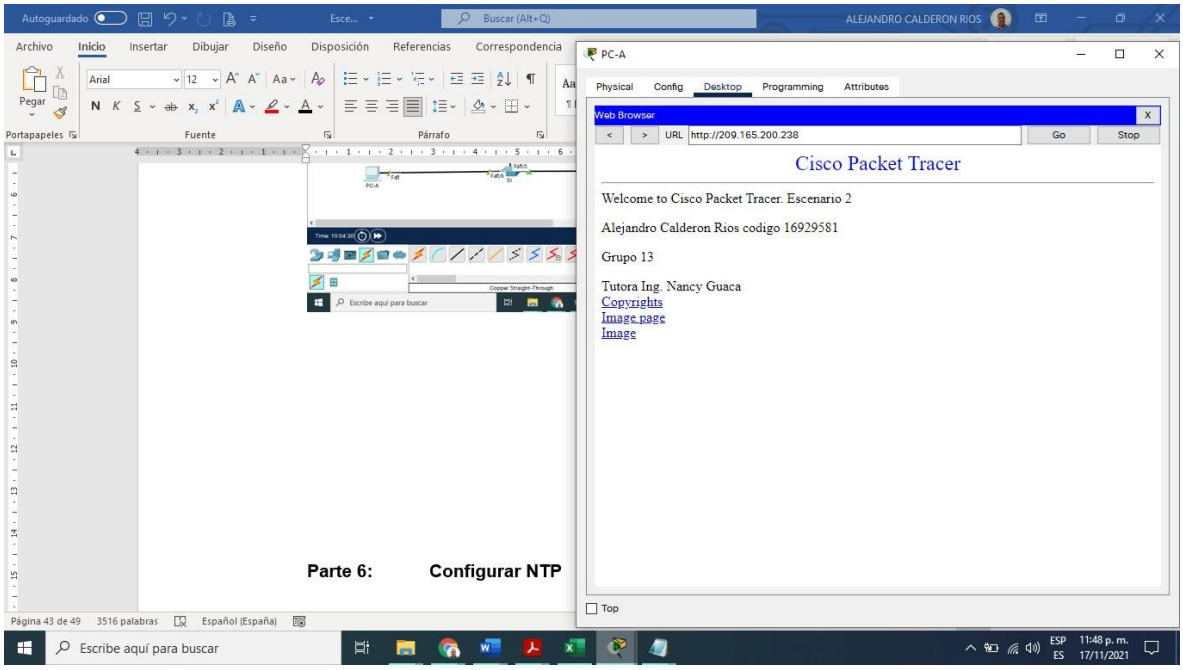
Fuente: Elaboración propia

Figura 77.Ping 192.168.21.22 PC-A – PC-C



Fuente: Elaboración propia

Figura 78. Conexión navegador de PC-A al servidor web

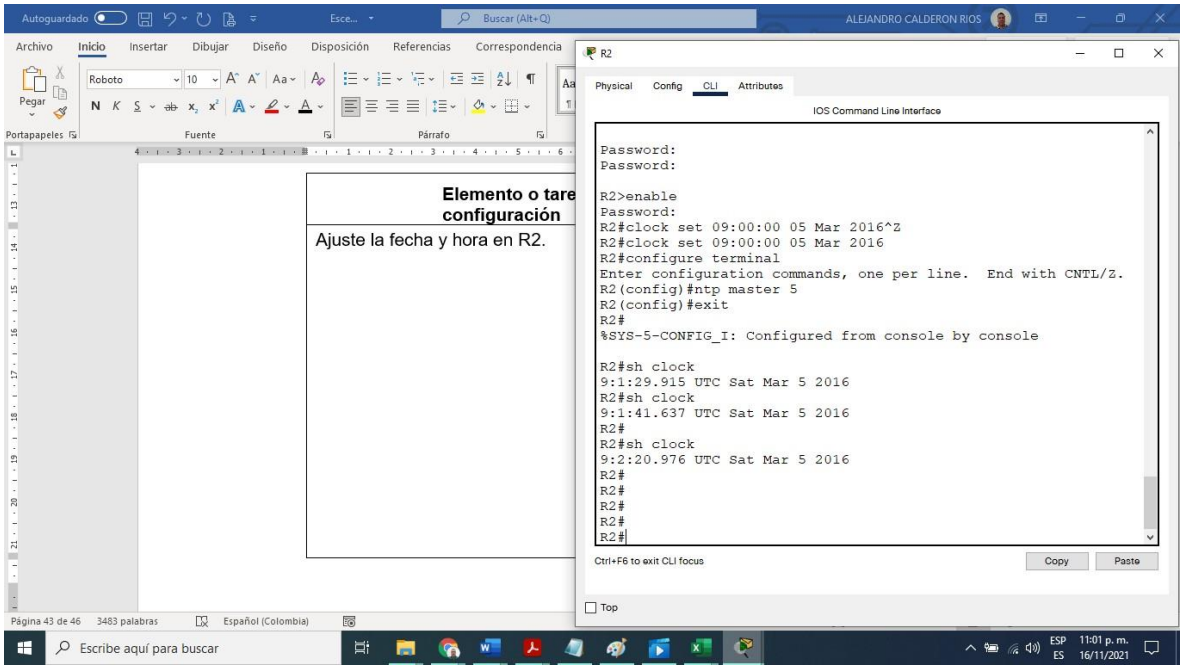


Fuente: Elaboración propia

Tabla 26. Parte 6: Configurar NTP

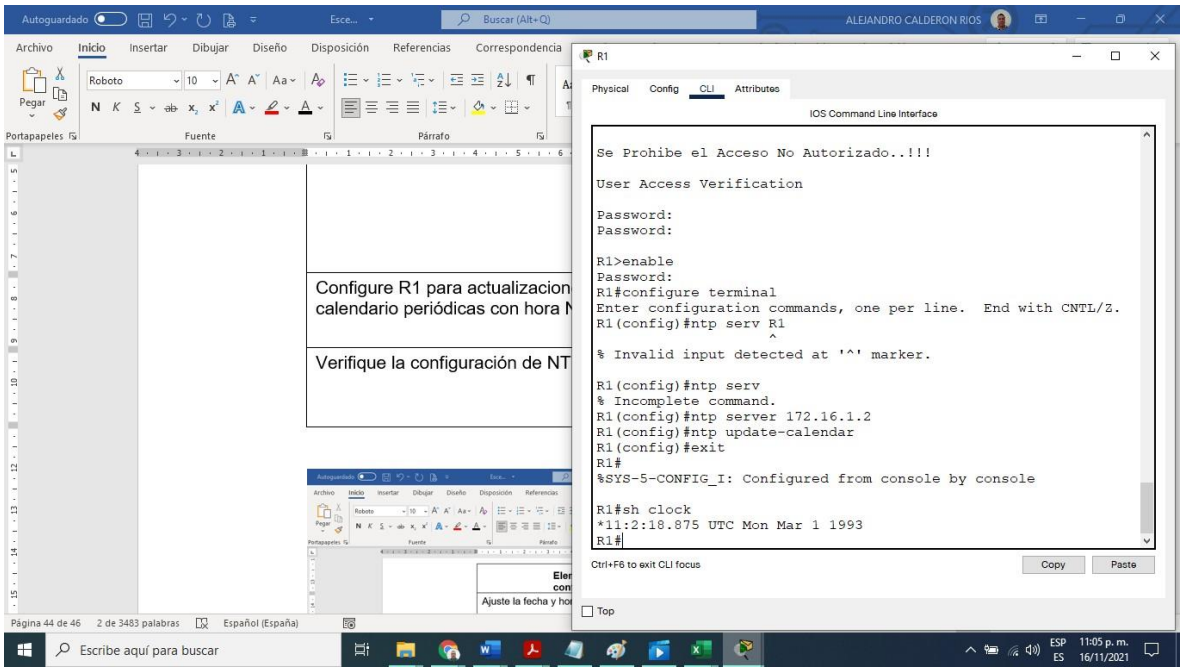
Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.**
Configure R2 como un maestro NTP.	Nivel de estrato: **5** R2(config)#ntp master 5 R2(config)#exit
Configurar R1 como un cliente NTP.	Servidor: **R2** R1(config)#ntp serv R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp upd R1(config)#ntp update-calendar R1(config)#exit

Figura 79. Ajuste la fecha, hora y maestro NTP R2



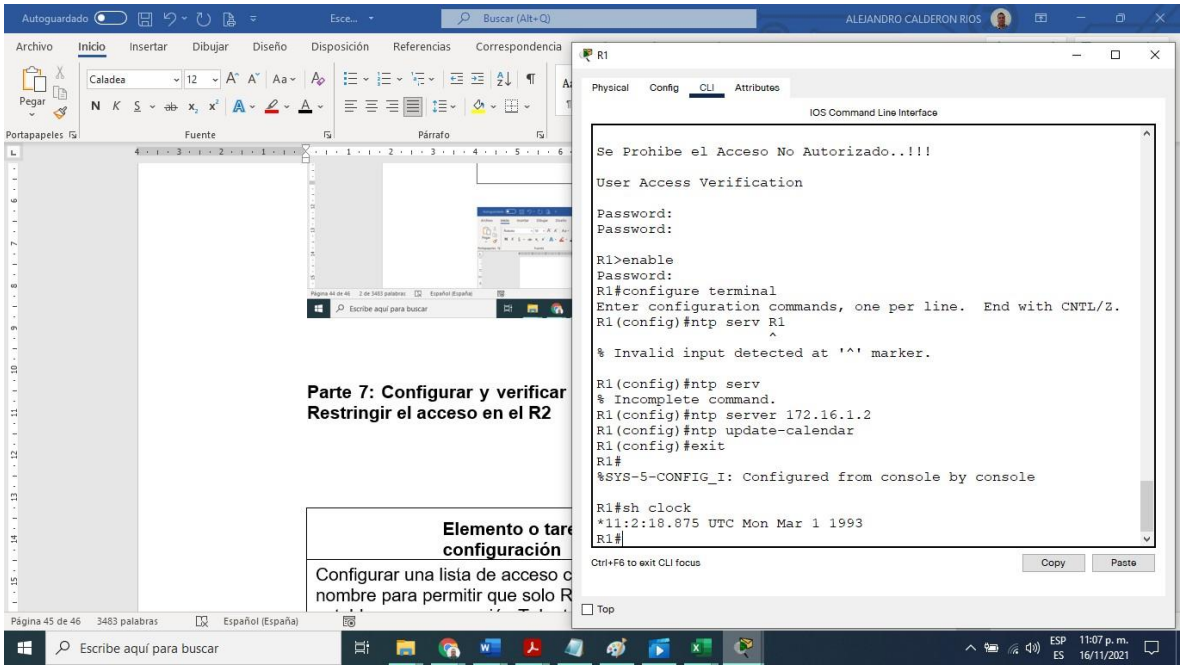
Fuente: Elaboración propia

Figura 80. R1 como un cliente NTP



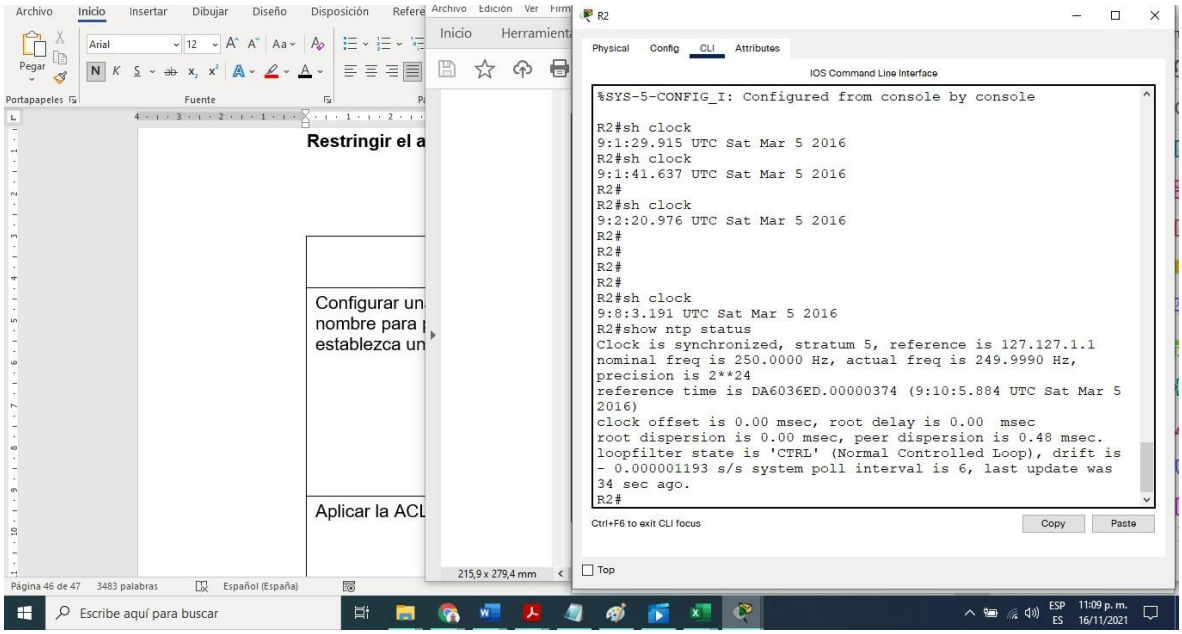
Fuente: Elaboración propia

Figura 81. Actualizaciones de calendario periódicas NTP en R1



Fuente: Elaboración propia

Figura 82. Comando show clock en R2



Parte 7
paso 1: Restringir el acceso en el R2

Tabla 27. Configurar y verificar las listas de control de acceso (ACL)

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN- MGT** R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#perm R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#deny an R2(config-std-nacl)#deny any R2(config-std-nacl)#
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4 R2(config-line)#ip a

	R2(config-line)#ip access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.1 Trying 172.16.1.1 ...Open [Connection to 172.16.1.1 closed by foreign host] R1#

Tabla 28. Paso 2: Introducir el comando de CLI

Descripción del comando	**Entrada del estudiante (comando)**
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show ip access-list Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 20 deny any Standard IP access list 1 10 permit 192.168.0.0 0.0.3.255
Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Show ip interface
¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red. R1 (config)#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R1(config)#clear ip nat translation

CONCLUSIONES

Se aplico los conocimientos aprendidos durante el curso de profundización, dando desarrollo a cada una de las actividades propuestas, realizando diferentes tipos de configuración en cada dispositivo en una red, se validó la conectividad y funcionamiento de cada escenario puesto en práctica, fortaleciendo los conceptos de seguridad en una red, haciendo filtro al personal no autorizado generando una experiencia y habilidad en el manejo e implementación de una red.

Se da la importancia en este curso, llevando a cabo las prácticas en los diferentes escenarios y simuladores para adquirir el conocimiento como packet tracer y el laboratorio remoto Smartlab. Desarrollando para el escenario 1 esquema de direccionamiento ip para cada LAN, configuración de aspectos básicos iniciales en cada dispositivo, protocolos de seguridad en routers y switches, parámetros de host etc. Para el escenario 2 de adiciona implementación de direcciones ipv6, routing entre VLAN permitiendo que la conexión sea más segura y efectiva, OSPF permitiendo el intercambio de paquetes en una red, direccionamiento de host por parte de DHCP, traducción de direcciones de red estáticas NAT, creación de listados de acceso ACL.

Estos protocolos durante el desarrollo y la implementación, por medio de comandos especiales se verificando la existencia, funcionalidad, nombres, descripción, las interfaces y su direccionamiento, tráfico de paquetes etc.

BIBLIOGRAFIA

CISCO. (2019). Capa de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5

CISCO. (2019). Direccionamiento IP. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7

CISCO. (2019). División de redesIP en subredes. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9