

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNA

BRAYAN EMILIO BENAVIDES PANTOJA

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNA

BRAYAN EMILIO BENAVIDES PANTOJA

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

DIRECTOR:
MSc. HECTOR JULIAN PARRA MOGOLLON

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

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

PASTO - NARIÑO 26 de junio de 2022

AGRADECIMIENTOS

Agradezco a Dios por haberme permitido alcanzar este extraordinario momento en la vida, soportándome con amor, salud, paz y sabiduría para afrontar los retos venideros.

A mis padres: Maria del Carmen Pantoja Mesa y Emilio Marcial Benavides Vela por otorgarme la vida, por su esmero incondicional de forjar una gran persona y un gran profesional.

A mis amigos y familiares, al personal de tutores y directores de la universidad por su paciencia y profesionalismo, ustedes me encausaron por los senderos correctos para alcanzar la formación como Ingeniero de sistemas, centrada en el servicio a la sociedad.

Y finalmente a todas las personas que de algún modo realizaron acciones en pos de la consecución de mi objetivo, compañeros de carrera con los cuales compartimos muchos momentos tanto dentro como fuera de la institución.

CONTENIDO

CONTENIDO.....	6
LISTA DE TABLAS.....	8
LISTA DE FIGURAS	9
RESUMEN	12
ABSTRACT	13
OBJETIVOS	15
DESARROLLO.....	16
Escenario propuesto N° 1	16
Parte 1: Construya la Red	16
Parte 2: Desarrolle el esquema de direccionamiento IP.....	17
Parte 3: Configure aspectos básicos.....	18
Paso 1: configurar los ajustes básicos.....	18
Paso 2. Configurar los equipos	23
Escenario 2	25
Parte 1: Inicializar dispositivos	26
Paso 1: Inicializar y volver a cargar los routers y los switches	26
Parte 2: Configurar los parámetros básicos de los dispositivos.....	27
Paso 1: Configurar la computadora de Internet.....	27
Paso 2: Configurar R1	28
Paso 3: configurar R2.....	29
Paso 4: configurar R3.....	31
Paso 5: Configurar S1	32
Paso 6: Configurar el S3	34
Paso 7: Verificar la conectividad de la red	35
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN.....	36
Paso 1: Configurar S1	37
Paso 1: Configurar S3.....	38
Paso 3: Configurar R1	39
Paso 4: Verificar la conectividad de la red.....	40

Parte 4: Configurar el protocolo de routing dinámico OSPF	41
Paso 1: Configurar OSPF en el R1.....	41
Paso 1: OSPF en el Configurar R2.....	42
Paso 3: Configurar OSPFv3 en el R2.....	42
Paso 4: Verificar la información de OSPF	43
Parte 5: Implementar DHCP y NAT para IPv4	44
Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23.....	45
Paso 2: Configurar la NAT estática y dinámica en el R2	46
Paso 3: Verificar el protocolo DHCP y la NAT estática.....	47
Parte 6: Configurar NTP	48
Parte 7: Configurar y verificar las listas de control de acceso (ACL)	49
Paso 1: Restringir el acceso a las líneas VTY en el R2.....	49
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente.....	50
CONCLUSIONES.....	51
REFERENCIAS.....	52

LISTA DE TABLAS

Tabla 1. Direccionamiento general.	17
Tabla 2. Subredes LAN1.....	17
Tabla 3. Subredes LAN2.....	18
Tabla 4. Proceso de configuración de R1	18
Tabla 5. Proceso de configuración de Switch 1.....	20
Tabla 6. Configuración del PC-A.....	23
Tabla 7. Configuración del PC-B.....	23
Tabla 8. Eliminación de las configuraciones de inicio y volver a cargar los hosts.....	26
Tabla 9. Configuraciones del servidor.....	27
Tabla 10. Configuración de router 1	28
Tabla 11. Configuración de router 2.....	29
Tabla 12. Configuración de router 3.....	31
Tabla 13. Configuración del Switch 1	32
Tabla 13. Configuración del Switch 3.....	34
Tabla 13. De Verificación la conectividad de la red	35
Tabla 14. Configurar seguridad y Vlans en switch	37
Tabla 15. Configurar seguridad y Vlans en switch 3	38
Tabla 16. Configurar las sub-interfaces 802.1Q en las Vlans	39
Tabla 17. De Verificación la conectividad de la red	40
Tabla 18. Configurar OSPF en el R1	41
Tabla 19. Configurar OSPF en el R2	42
Tabla 20. Configurar OSPFv3 en el R2.....	42
Tabla 21. Verificar la información de OSPF.	43
Tabla 21. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23.....	45
Tabla 22. Configurar la NAT estática y dinámica en el R2.....	46
Tabla 24. Verificar el protocolo DHCP y la NAT estática.....	48
Tabla 25. Restringir el acceso a las líneas VTY en el R2.....	49
Tabla 26. Comando de CLI adecuado que se necesita para mostrar lo siguiente	50

LISTA DE FIGURAS

Figura 1. Topología Escenario 1	16
Figura 2. Construcción de la red.....	16
Figura 3. Configuración del Router.	19
Figura 4. Guardado de configuración en la NVRAM.	20
Figura 5. Configuración del switch 1	22
Figura 6. Guardado de la configuración del S1 en la NVRAM	22
Figura 7. Prueba de conexión PC-A.	24
Figura 8. Prueba de conexión PC-B.	24
Figura 9. Topología Escenario 2.....	25
Figura 10. Construcción de la red.....	26
Figura 11. Borrado de la NVRAM	27
Figura 12. Configuraciones del servidor de internet.....	28
Figura 13. Configuración del router 1.....	29
Figura 14. Configuración del router 2.....	30
Figura 15. Configuración del router 3.....	32
Figura 16. Borrado de la NVRAM S1	33
Figura 17. Configuración del switch 1	33
Figura 18. Configuración del switch 3.....	34
Figura 19. Ping de R1 a R2.....	35
Figura 20. Ping de R2 a R3.....	36
Figura 21. Configurar seguridad y Vlans en switch 1	37
Figura 22. Configurar seguridad y Vlans en switch 3.....	39
Figura 23. Verificación de conectividad	40
Figura 24. Configurar OSPF en el R1	41
Figura 25. Configurar OSPFv3 en el R2	42
Figura 26. Verificar la información de OSPFv3.....	43
Figura 27. Verificar la información de OSPFv3.....	44
Figura 28. Configurar el R1 como servidor de DHCP para las VLAN.	45
Figura 29. Configurar la NAT estática y dinámica en el R2.....	46
Figura 30. Verificar el protocolo DHCP y la NAT estática	48
Figura 31. Verificar el protocolo DHCP y la NAT estática	48
Figura 32. Restringir el acceso a las líneas VTY en el R2	49

GLOSARIO

ACL: las listas de control de acceso se utilizan para permitir o denegar el tráfico de los paquetes de la red según un criterio, como dirección de origen, de destino, protocolos y números de puerto, además pueden clasificar el tráfico para darle prioridad en la línea.

Cisco Packet Tracer: es un programa de Networking Academy para simular el comportamiento de redes, que proporciona a los estudiantes interacción y aprendizaje de conceptos tecnológicos complejos. Su interfaz permite a los estudiantes realizar el diseño de topologías con una cantidad ilimitada de dispositivos, como también la configuración de estos, este entorno práctico, incluye la detección y corrección de errores en sistemas de redes de comunicaciones, lo cual, fortalece el desarrollo de habilidades tales como el pensamiento creativo, crítico y la toma de decisiones.

DHCP: es un protocolo que se desarrolló como solución para redes de gran envergadura y ordenadores portátiles para asignar automáticamente direcciones de red reutilizables y por la existencia de posibilidades de configuración adicionales.

Enlace troncal o trunk: es un enlace que se configura en uno o más puertos de un switches o un router para que por este se pueda enviar y recibir el tráfico de las varias VLANs que se han configurado.

IPv4: Es cuarta versión del Internet Protocol (IP), se diseñó antes de que se produjera la gran demanda de direcciones, crecimiento exponencial de Internet ha agotado el suministro de direcciones IP.

IPv6: Es una actualización más extensible y escalable del IP, diseñado para resolver el problema de agotamiento de direcciones que utiliza 128 bits en lugar de los 32 bits que en la actualidad utiliza el IPv4. IPv6 utiliza números hexadecimales para representar los 128 bits lo que proporciona 640 sextillones de direcciones.

RESUMEN

El presente documento corresponde al trabajo final del curso de profundización CISCO, en la prueba de habilidades prácticas. En este documento se pueden encontrar soluciones resueltos a través de Packet Tracer, además de configuraciones básicas en cuanto a: OSPF, DHCPv4, etc. Además de distintas pruebas de conexiones entre los distintos dispositivos de la topología empleada.

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

ABSTRACT

This document corresponds to the final work of the CISCO deepening course, in the practical skills test. In this document you can find solutions resolved through Packet Tracer, in addition to basic configurations regarding: OSPF, DHCPv4, etc. In addition to different connection tests between the different devices of the topology used.

Keywords: CISCO, CCNP, Routing, Swicthing, Networking, Electronics.

INTRODUCCION

En un mundo interconectado de forma tan amplia se debe tener presente que las redes forman parte de un papel muy importante dentro de las distintas sociedades. Es por eso que mediante el uso de protocolos como TCP/IP y OSI, configuración de redes soportadas en VLANs y demás dispositivos se hace posible la interconexión entre varias redes.

Se realizarán prácticas sobre equipos reales, con el simulador de Cisco Networking Academy y con Packet Tracer; el cual tiene como objetivo la adquisición y la formalización de habilidades para el mejor acceso a los equipos y realizar una configuración básica de los distintos aspectos físicos (hardware) y lógicos (software).

Para finalizar, se toma nota de cada uno de los comandos necesarios para realizar las mencionadas configuraciones, y de igual forma los pantallazos correspondientes a los resultados obtenidos luego de verificar las distintas interconexiones.

1. ESCENARIO 1

DESARROLLO

Figura 1. Topología Escenario 1



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.

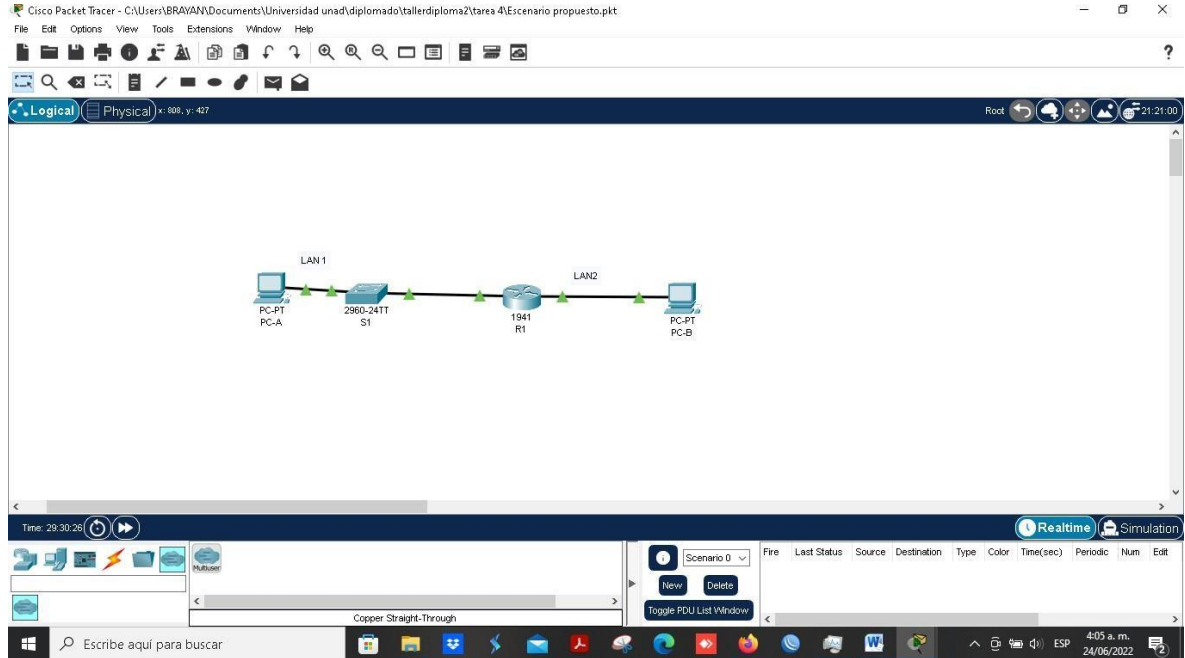
Aspectos básicos/situación

En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el switch S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

Parte 1: Construya la Red

En el simulador construya la red de acuerdo con la topología lógica que se plantea en la figura 1, cablee conforme se indica en la topología, y conecte los equipos de cómputo.

Figura 2. Construcción de la red



Fuente Autor.

Parte 2: Desarrolle el esquema de direccionamiento IP

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

Tabla 1. Direccionamiento general.

Item	Requerimiento
Dirección de Red	192.168.47.0
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/1	Primera dirección de host de la subred LAN1
R1 G0/0	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

Fuente Guía de Actividades.

Tabla 2. Subredes LAN1.

Tabla de subredes LAN1	
IP de red	192.168.47.0/25
Host	100
Mascara subred	255.255.255.128
Primera IP útil	192.168.47.1
Ultima IP útil	192.168.47.126
Broadcast	192.168.47.127
Host disponibles	126

Fuente Autor.

Tabla 3. Subredes LAN2.

Tabla de subredes LAN2	
IP de red	192.168.47.0/26
Host	50
Mascara subred	255.255.255.192
Primera IP útil	192.168.47.129
Ultima IP útil	192.168.47.190
Broadcast	192.168.47.191
Host disponibles	62

Fuente Autor.

Parte 3: Configure aspectos básicos.

Los dispositivos de red (S1 y R1) se configuran mediante conexión de consola.

Paso 1: configurar los ajustes básicos.

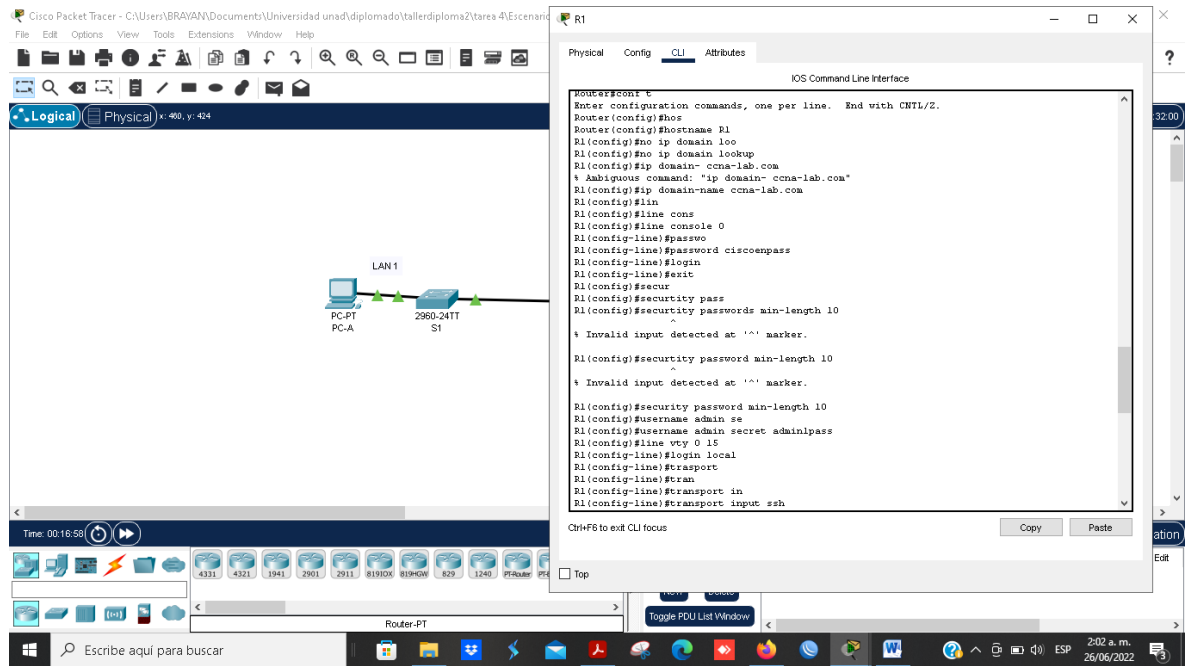
Tabla 4. Proceso de configuración de R1

Host	Especificación
R1>en	Ingreso modo privilegiado
R1#config t	Ingreso a modo configuración global
Enter configuration commands, one per line. End with CNTL/Z.	
R1(config)#hostname R1	Asignar nombre al Router
R1(config)#no ip domain lookup	Desactiva la búsqueda DNS
R1(config)#ip domain-name ccna-lab.com	Asignar el nombre de dominio
R1(config)#line console 0	Ingreso al modo de configura de línea consola
R1(config-line)#password ciscoenpass	Asignar contraseña acceso consola
R1(config-line)#login	Activar la autenticación de inicio
R1(config-line)#exit	Salir

R1(config)#security passwords min-length 10	Establecer la longitud mínima para las contraseñas mínimo 10 caracteres
R1(config)#username admin secret admin1pass	Crear un usuario administrativo en la base de datos local
R1(config)#line vty 0 15	Ingreso a la configuración en las líneas VTY
R1(config-line)#login local	Activar la autenticación de inicio a la base de datos local
R1(config-line)#transport input ssh	Configurado de VTY para que solo acepte SSH
R1(config-line)#exit	Salir
R1(config)#service password-encryption	Cifrado para las contraseñas
R1(config)#banner motd \$el acceso a personal no autorizado está prohibido!\$	Configurar un mensaje para inicio de sesión
R1(config)#int g0/1	Configurar interfaz G0/1
R1(config-if)#ip address 192.168.47.1 255.255.255.128	Establecer la dirección IPv4.
R1(config-if)#no shut	Enciende la interface
R1(config-if)#exit	Salir
R1(config)#int g0/0	Configurar interfaz G0/0
R1(config-if)#ip address 192.168.47.129 255.255.255.192	Establecer la dirección IPv4.
R1(config-if)#no shut	Enciende la interface
R1(config-if)#exit	Salir
R1(config)# crypto key generate rsa	Genera clave de cifrado tamaño del módulo en bits
R1(config)#exit	Salir del modo de configuración global
R1#	
%SYS-5-CONFIG_I: Configured from console by console	
R1#copy running-config startup-config	Guardar configuración de ejecución del router en la NVRAM
Destination filename [startup-config]?	
Building configuration...	
[OK]	

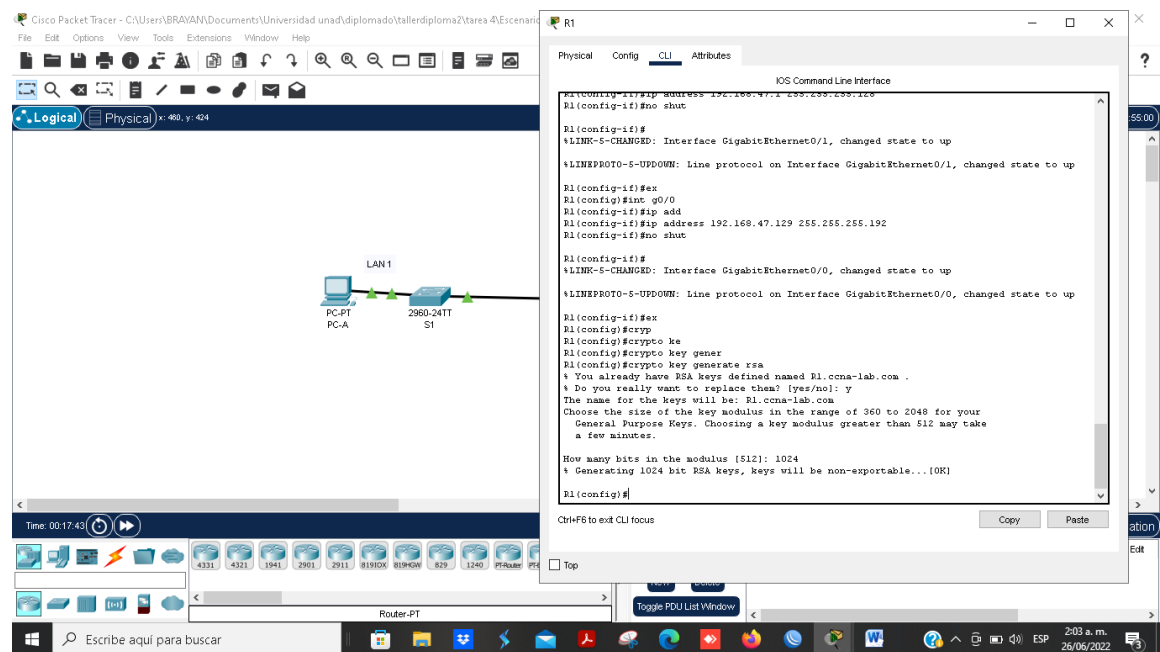
Fuente Autor.

Figura 3. Configuración del Router.



Fuente Autor.

Figura 4. Guardado de configuración en la NVRAM.



Fuente Autor.

Tabla 5. Proceso de configuración de Switch 1

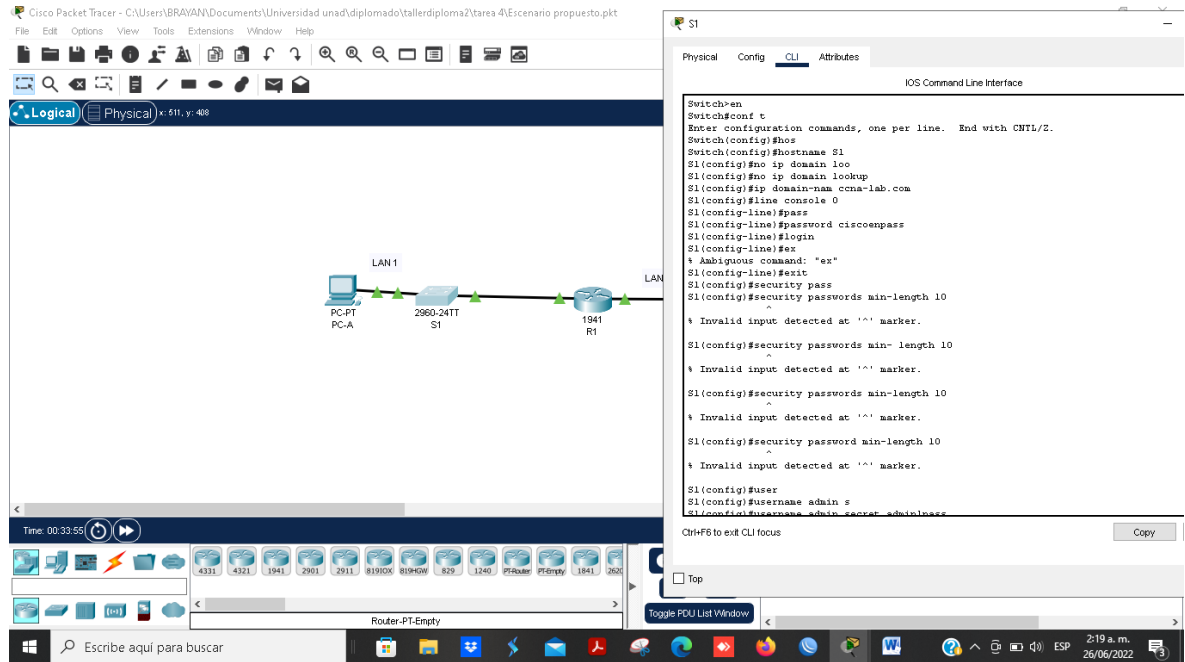
Host	Especificación
S1>en	Ingreso modo privilegiado
S1#config t	Ingreso a modo configuración global
Enter configuration commands, one per line. End with CNTL/Z.	
S1(config)#hostname S1	Asignar nombre al Router
S1(config)#no ip domain lookup	Desactiva la búsqueda DNS
S1(config)#ip domain-name ccna-lab.com	Asignar el nombre de dominio
S1(config)#line console 0	Ingreso al modo de configura de línea consola
S1(config-line)#password ciscoenpass	Asignar contraseña acceso consola
S1(config-line)#login	Activar la autenticación de inicio
S1(config-line)#exit	Salir
S1(config)#security passwords min-length 10	Establecer la longitud mínima para las contraseñas mínimo 10 caracteres
S1(config)#username admin secret admin1pass	Crear un usuario administrativo en la base de datos local
S1(config)#line vty 0 15	Ingreso a la configuración en las líneas VTY
S1(config-line)#login local	Activar la autenticación de inicio a la base de datos local
S1(config-line)#transport input ssh	Configurado de VTY para que solo acepte SSH
S1(config-line)#exit	Salir
S1(config)#service password-encryption	Cifrado para las contraseñas
S1(config)#banner motd \$el acceso a personal no autorizado está prohibido!\$	Configurar un mensaje para inicio de sesión
S1(config)# int vlan1	Configurar interfaz vlan1
S1(config-if)# ip address 192.168.47.2 255.255.255.128	Establecer la dirección IPv4.
S1(config-if)#no shut	Enciende la interface
S1(config-if)#exit	Salir
S1(config)# ip default-gateway 192.168.47.1	Configuración de la puerta de enlace predeterminada
S1(config-if)#exit	Salir
S1(config)# crypto key generate rsa	Generar clave de cifrado tamaño del módulo en 1024 bits
S1(config)#exit	Salir del modo de configuración global

S1#	
%SYS-5-CONFIG_I: Configured from console by console	
S1#copy running-config startup-config	Guardar configuración de ejecución del router en la NVRAM

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

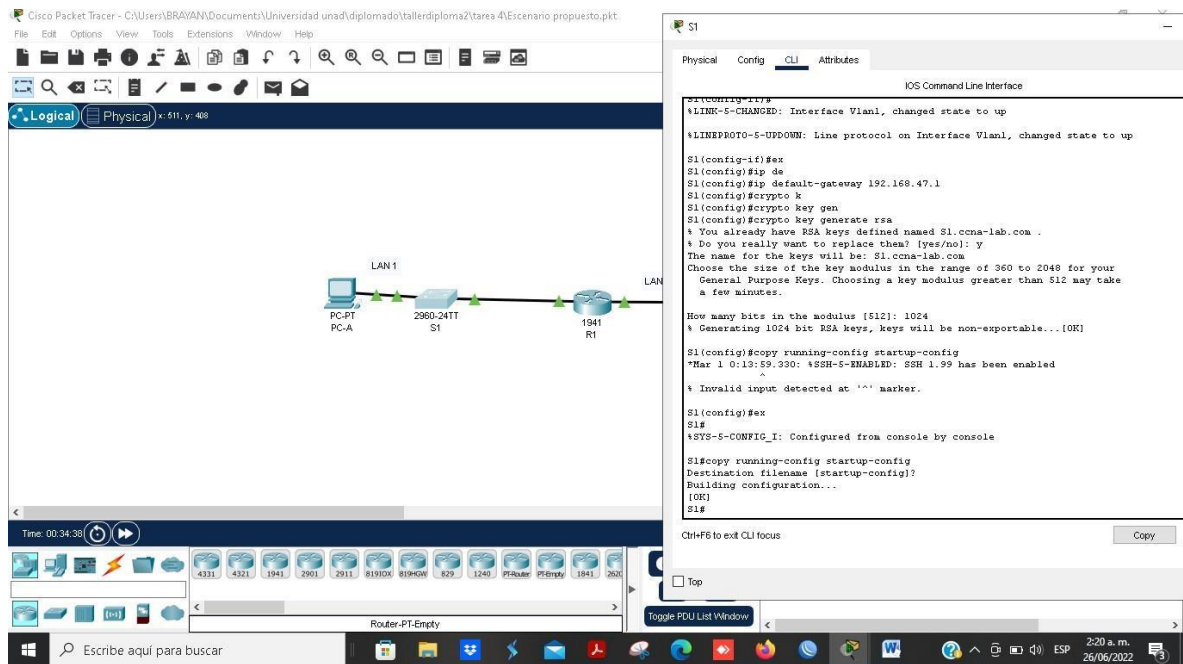
Fuente Autor.

Figura 5. Configuración del switch 1.



Fuente Autor.

Figura 6. Guardado de la configuración del S1 en la NVRAM.



Fuente Autor.

Paso 2. Configurar los equipos

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

Tabla 6. Configuración del PC-A

PC-A Network Configuration	
Descripción	Fastethernet 0
Dirección física	FE80::202:16FF:FE3D:19D
Dirección IP	192.168.47.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.47.1

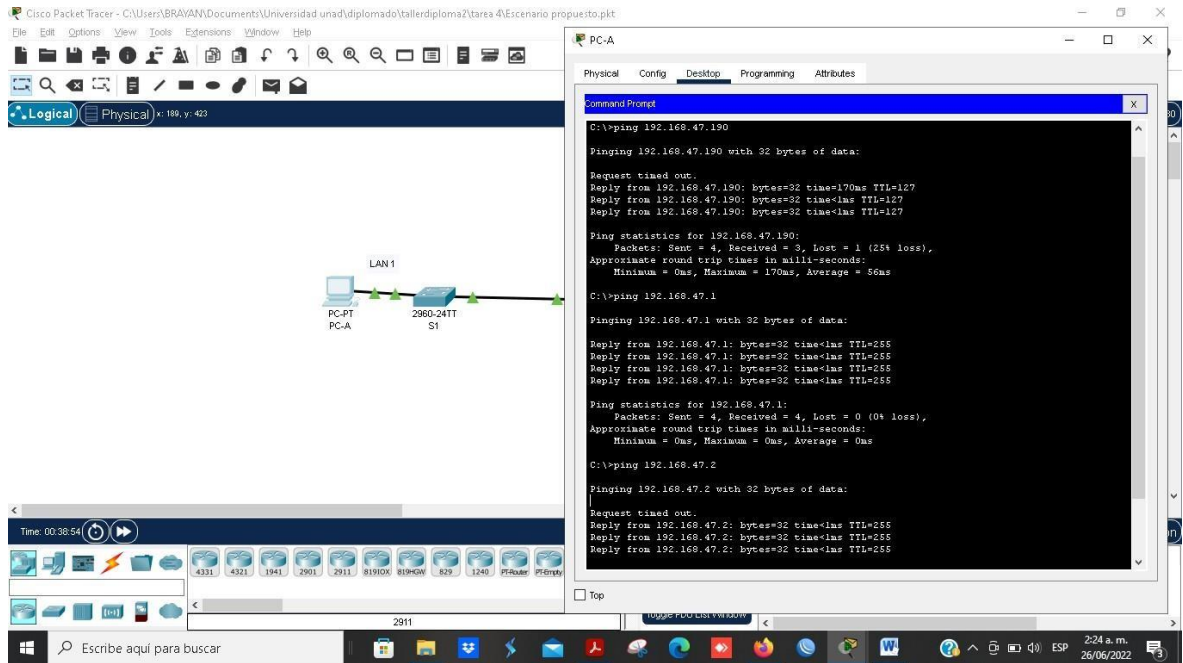
Fuente Autor.

Tabla 7. Configuración del PC-B

PC-B Network Configuration	
Descripción	Fastethernet 0
Dirección física	FE80::201:C9FF:FE2A:D489
Dirección IP	192.168.47.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.47.129

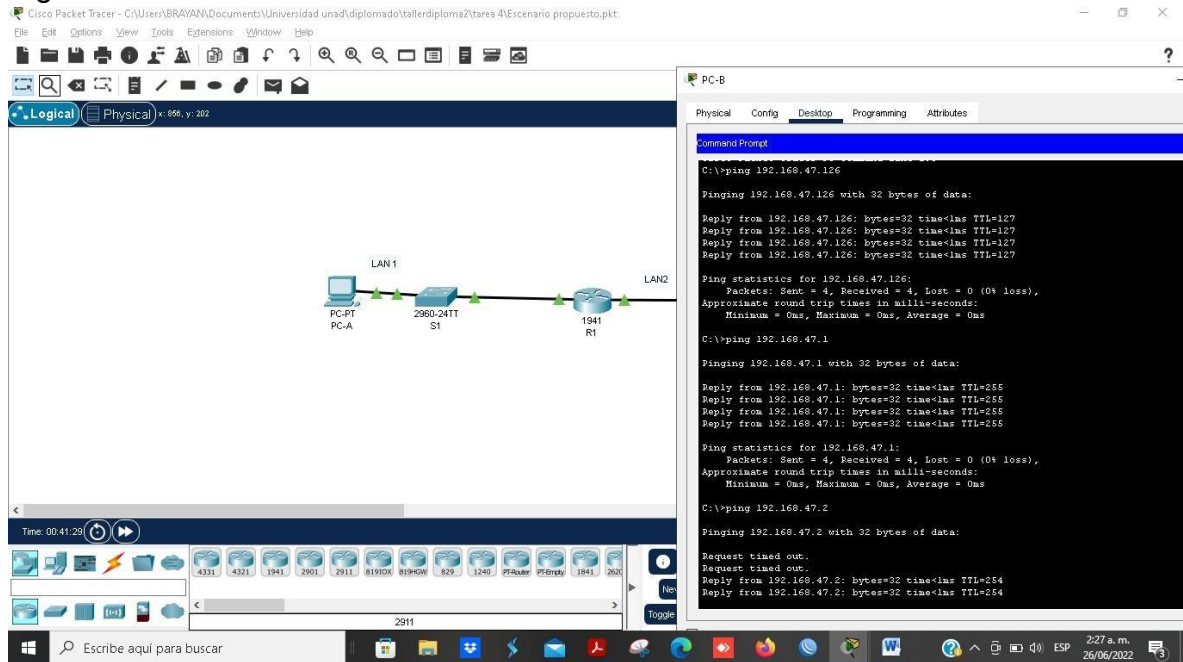
Fuente Autor.

Figura 7. Prueba de conexión PC-A.



Fuente Autor.

Figura 8. Prueba de conexión PC-B.



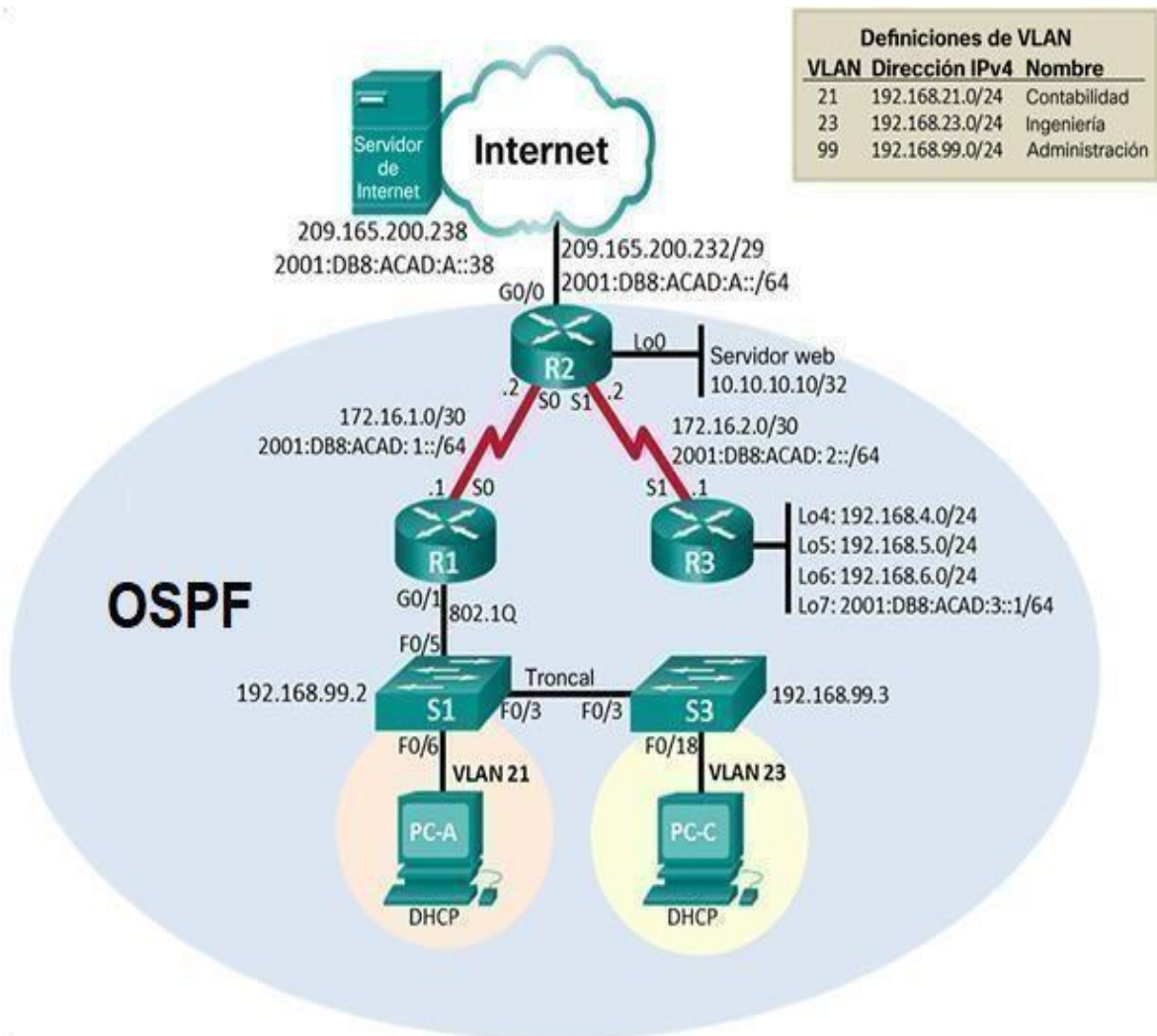
Fuente Autor.

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

Topología

Figura 9. Topología Escenario 2.



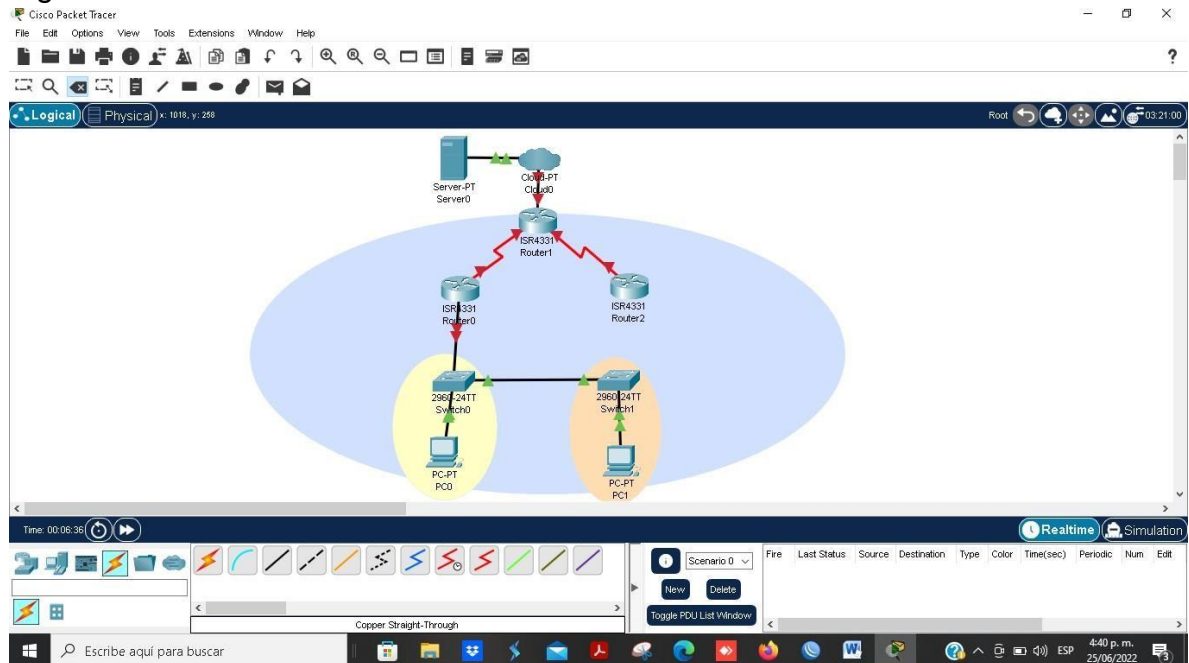
Fuente guía de actividades.

Parte 1: Inicializar dispositivos

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

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

Figura 10. Construcción de la red.



Fuente Autor.

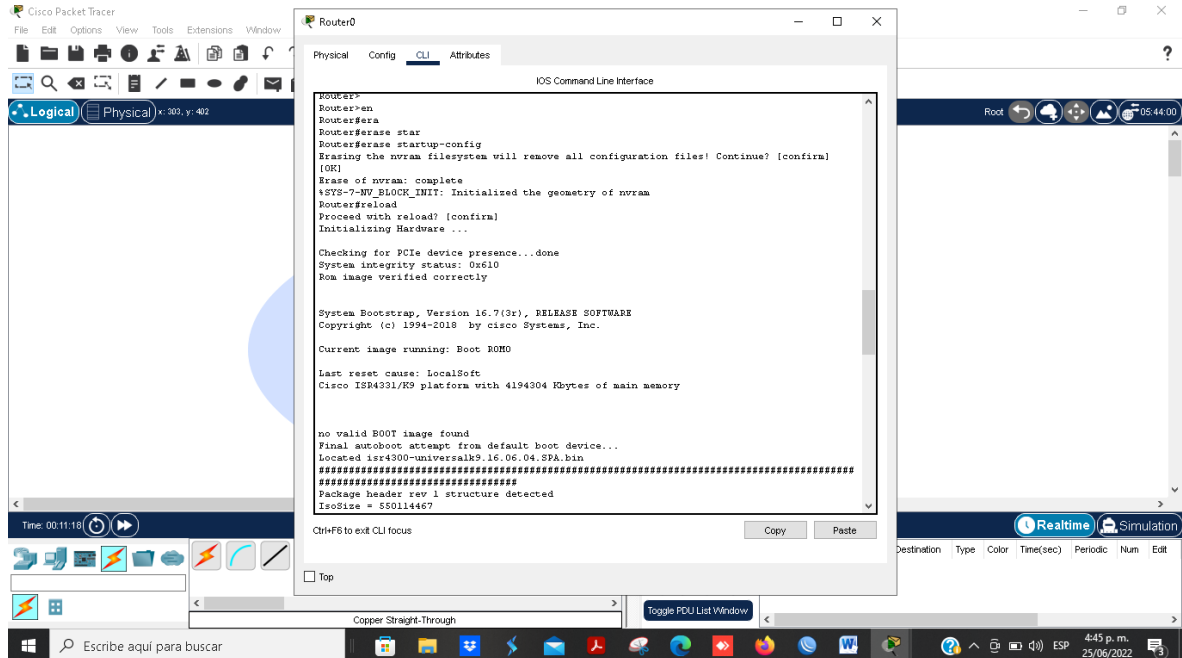
Tabla 8. Eliminación de las configuraciones de inicio y volver a cargar los dispositivos

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router Enable Erase startup-config
Volver a cargar todos los routers	Reload
Salir	Exit
Eliminar el archivo startup-config de todos los switches	Switch Enable Erase startup-config
Eliminar la base de datos de VLAN anterior	Delete vlan.dt
Volver a cargar ambos switches	Reload

Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches

Fuente Autor.

Figura 11. Borrado de la NVRAM.



Fuente Autor.

Parte 2: Configurar los parámetros básicos de los dispositivos

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 9. Configuraciones del servidor

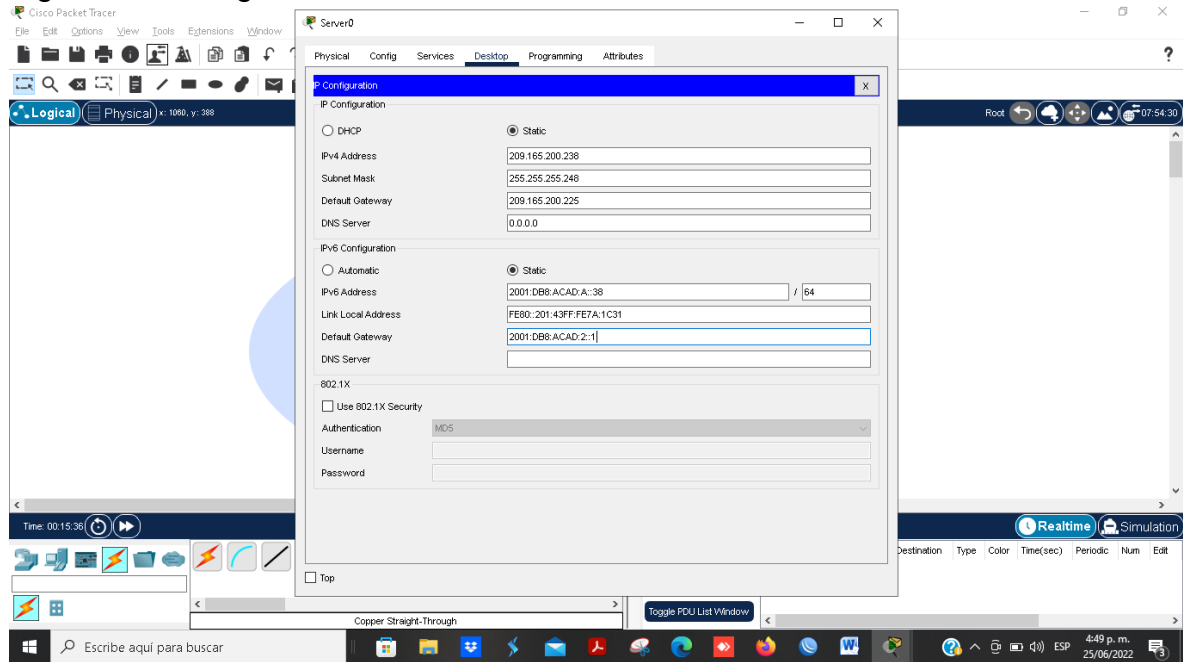
Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Fuente Autor.

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.

Inicialmente configuramos del servidor de internet, con la puerta de enlace Ipv4 predeterminada 209.165.200.233, y luego la configuración IPv6 con la dirección 2001:DB8:ACAD:A::38.

Figura 12. Configuraciones del servidor de internet



Fuente Autor.

Paso 2: Configurar R1

La configuración para R1 incluye las siguientes:

Tabla 10. Configuración de router 1

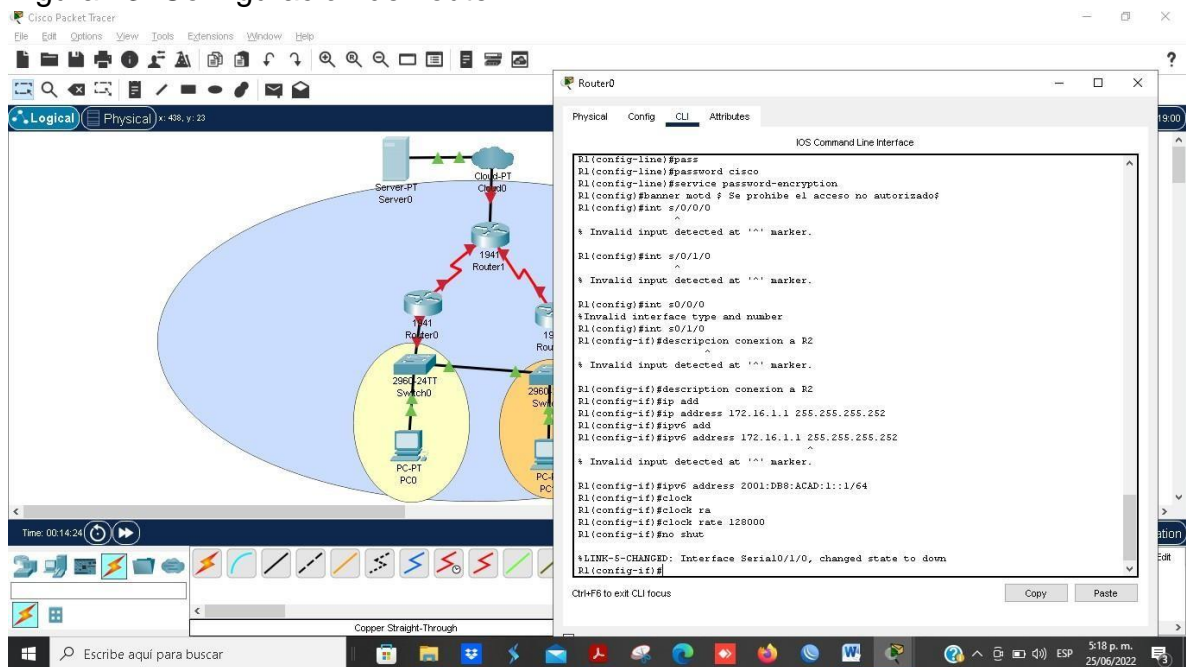
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain lookup
Nombre del router	R1
Contraseña de exec privilegiado cifrada	enable secret class
Contraseña de acceso a la consola	line console 0 password cisco
Contraseña de acceso Telnet	line vty 0 15 password cisco

Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interface Serial S0/0/0	Conexión a R2
Ipv4 address	172.16.1.1 255.255.255.252
Ipv6 address	2001:DB8:ACAD:1::1/64
Clock rate	128000
Rutas predeterminadas	ip route 0.0.0.0 0.0.0.0 172.16.1.2 ipv6 route ::/0 2001:DB8:ACAD:1::2

Fuente Autor.

Nota: Todavía no configure G0/1.

Figura 13. Configuración del router 1.



Fuente Autor.

Paso 3: configurar R2

La configuración para R2 incluye las siguientes:

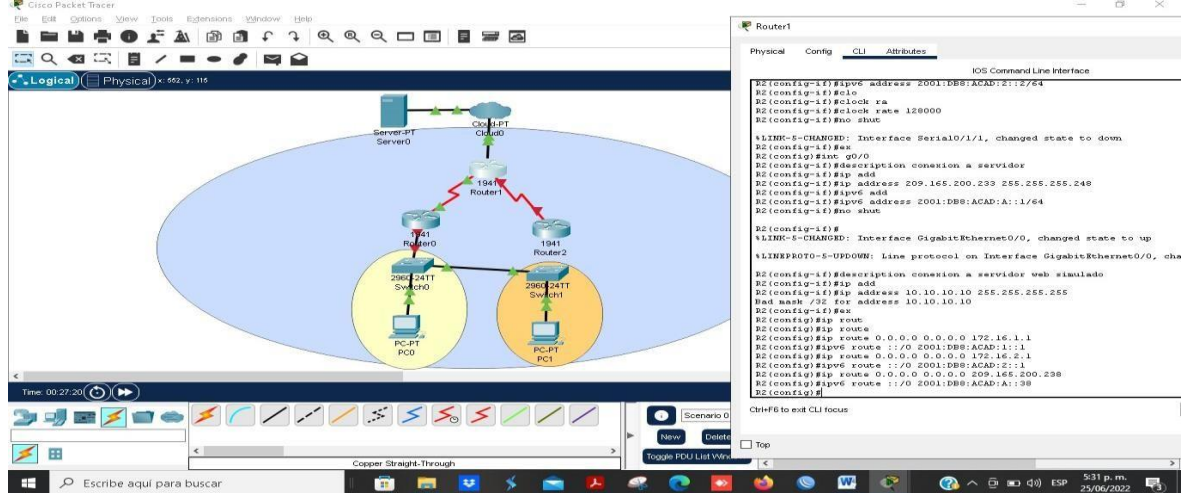
Tabla 11. Configuración de router 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain lookup

Nombre del router	R2
Contraseña de exec privilegiado cifrada	enable secret class
Contraseña de acceso a la consola	line console 0 password cisco
Contraseña de acceso Telnet	line vty 0 15 password cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interface Serial S0/0/0	Conexión a R1
Ipv4 address	172.16.1.2 255.255.255.252
Ipv6 address	2001:DB8:ACAD:1::2/64
Interface Serial S0/0/1	Conexión a R3
Ipv4 address	172.16.2.2 255.255.255.252
Ipv6 address	2001:DB8:ACAD:2::2/64
Clock rate	128000
Interface GigabitEthernet 0/0	Conexión a servidor
Ipv4 address	209.165.200.233 255.255.255.248
Ipv6 address	2001:DB8:ACAD:A::1/64
Interface Loopback 0	Conexión a servidor web simulado
Ipv4 address	10.10.10.10 255.255.255.255
Rutas predeterminadas	ip route 0.0.0.0 0.0.0.0 172.16.1.1 ipv6 route ::/0 2001:DB8:ACAD:1::1 ip route 0.0.0.0 0.0.0.0 172.16.2.1 ipv6 route ::/0 2001:DB8:ACAD:2::1 ip route 0.0.0.0 0.0.0.0 209.165.200.238 ipv6 route ::/0 2001:DB8:ACAD:A::38

Fuente Autor.

Figura 14. Configuración del router 2.



Fuente Autor.

Paso 4: configurar R3

La configuración para R3 incluye las siguientes:

Tabla 12. Configuración de router 3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain lookup
Nombre del router	R1
Contraseña de exec privilegiado cifrada	enable secret class
Contraseña de acceso a la consola	line console 0 password cisco
Contraseña de acceso Telnet	line vty 0 15 password cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interface Serial S0/0/1	Conexión a R2
Ipv4 address	172.16.2.1 255.255.255.252
Ipv6 address	2001:DB8:ACAD:2::1/64
Interface Loopback 4	

Ipv4 address	192.168.4.1 255.255.255.0
Interface Loopback 5	
Ipv4 address	192.168.5.1 255.255.255.0
Interface Loopback 6	
Ipv4 address	192.168.6.1 255.255.255.0
Interface Loopback 7	
Ipv6 address	2001:DB8:ACAD:3::1/64
Rutas predeterminadas	ip route 0.0.0.0 0.0.0.0 172.16.2.2 ipv6 route ::/0 2001:DB8:ACAD:2::2

Fuente Autor.

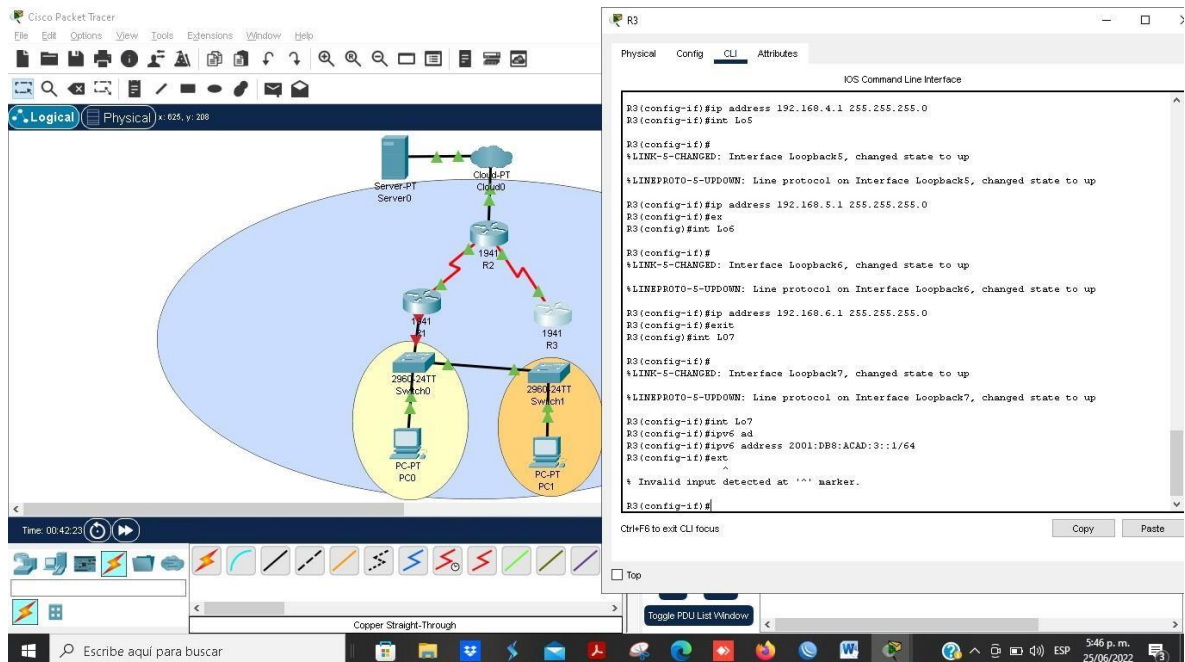


Figura 15. Configuración del router 3.

Fuente Autor.

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

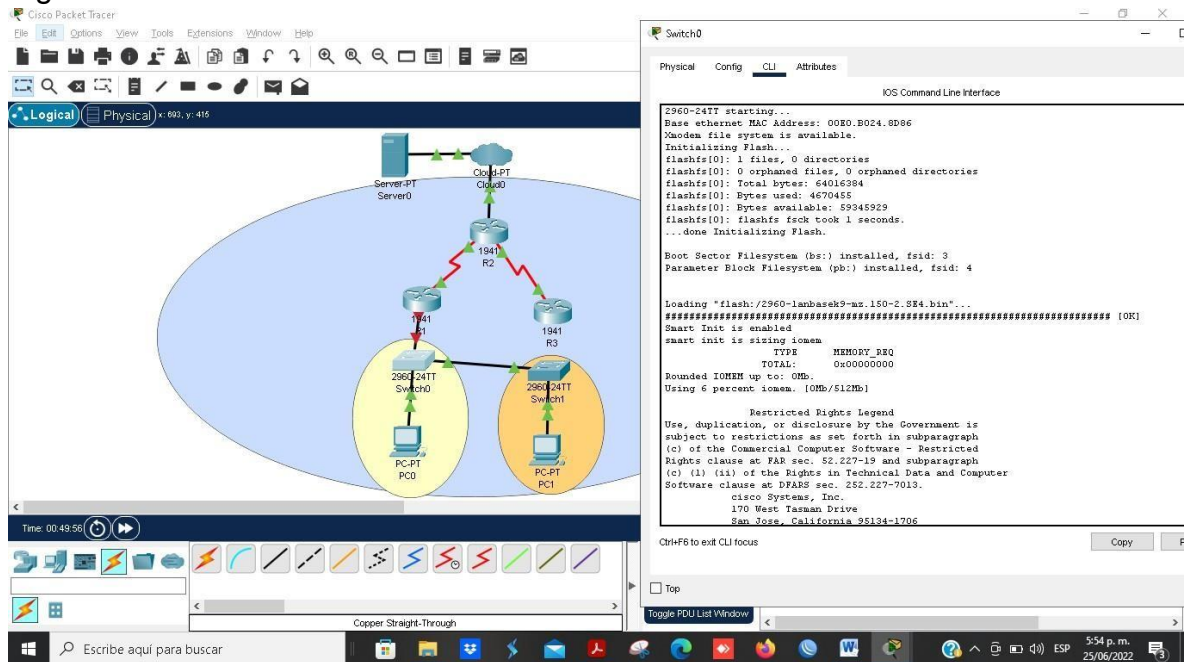
Tabla 13. Configuración del Switch 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain lookup

Nombre del switch	Hostname S1
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	line console 0 password cisco
Contraseña de acceso Telnet	line vty 0 15 password cisco
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

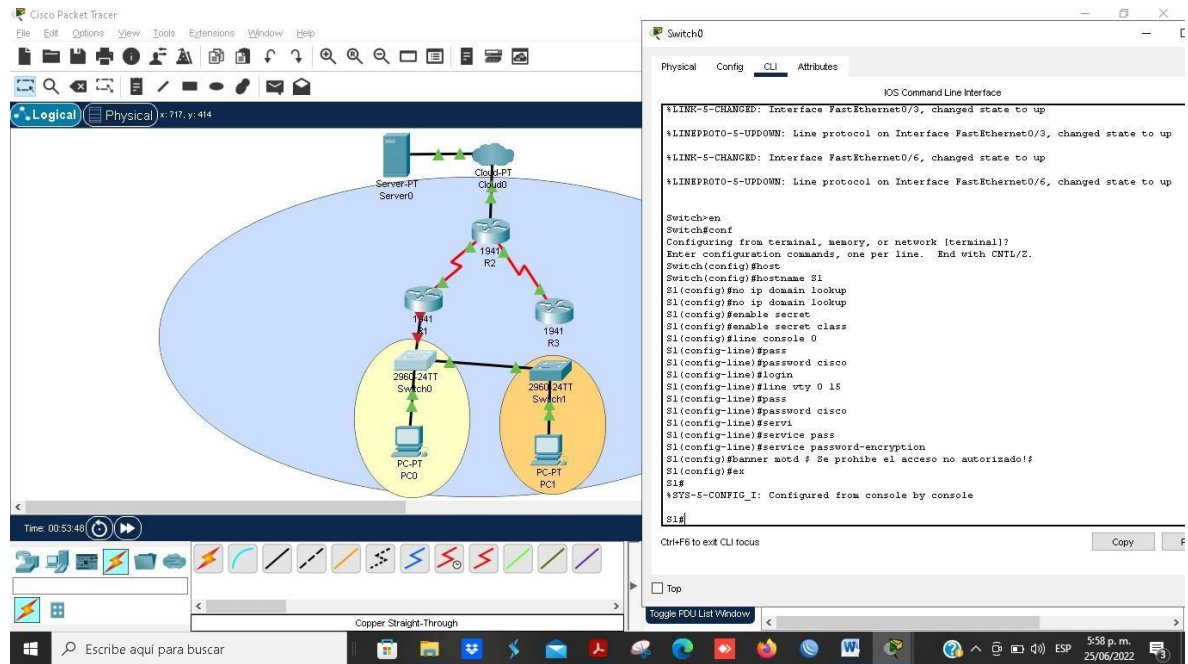
Fuente Autor.

Figura 16. Borrado de la NVRAM S1.



Fuente Autor.

Figura 17. Configuración del switch 1.



Fuente Autor.

Paso 6: Configurar el S3

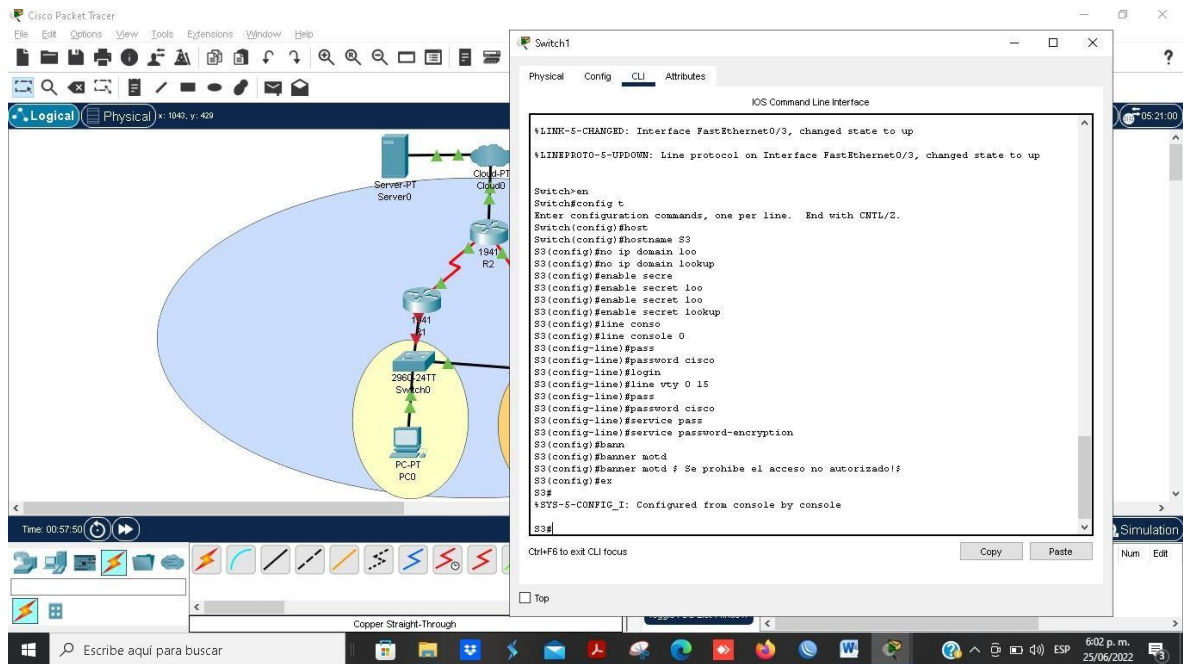
La configuración del S3 incluye las siguientes tareas:

Tabla 13. Configuración del Switch 3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain lookup
Nombre del switch	Hostname S3
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	line console 0 password cisco
Contraseña de acceso Telnet	line vty 0 15 password cisco
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente Autor.

Figura 18. Configuración del switch 3.



Fuente Autor.

Paso 7: Verificar la conectividad de la red

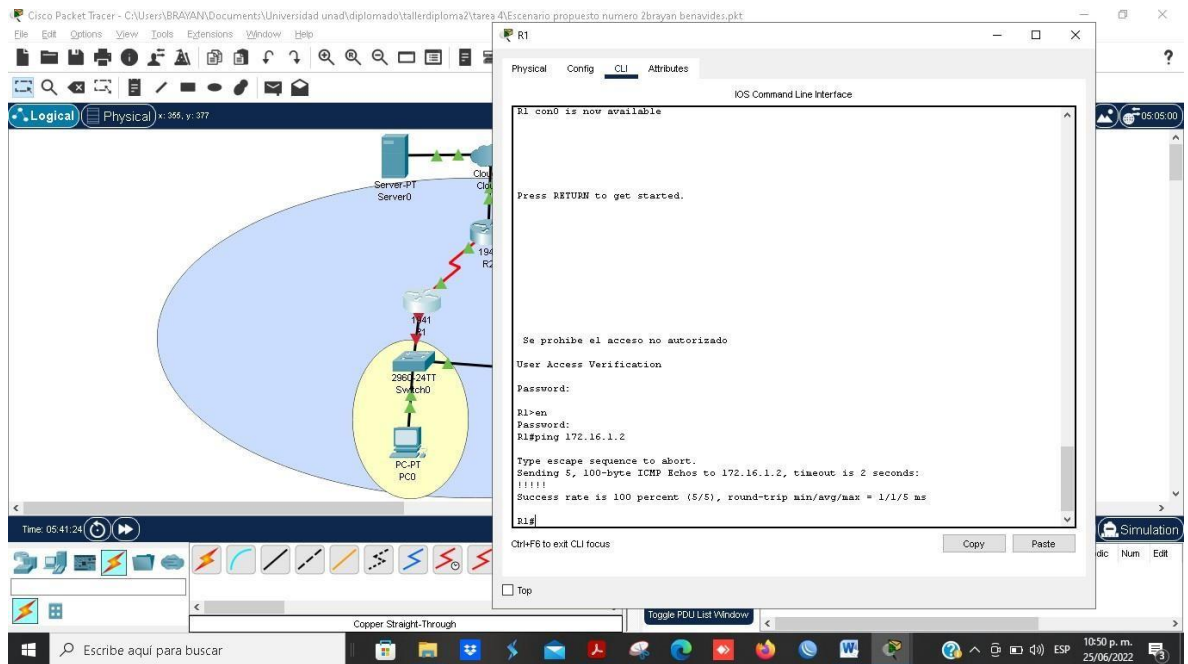
Utilice el comando **ping** para probar la conectividad entre los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 13. De Verificación la conectividad de la red.

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/1/0	172.16.1.2	Ok
R2	R3, S0/1/1	172.16.2.1	Ok
PC de Internet	Gateway predeterminado	209.165.200.225	No

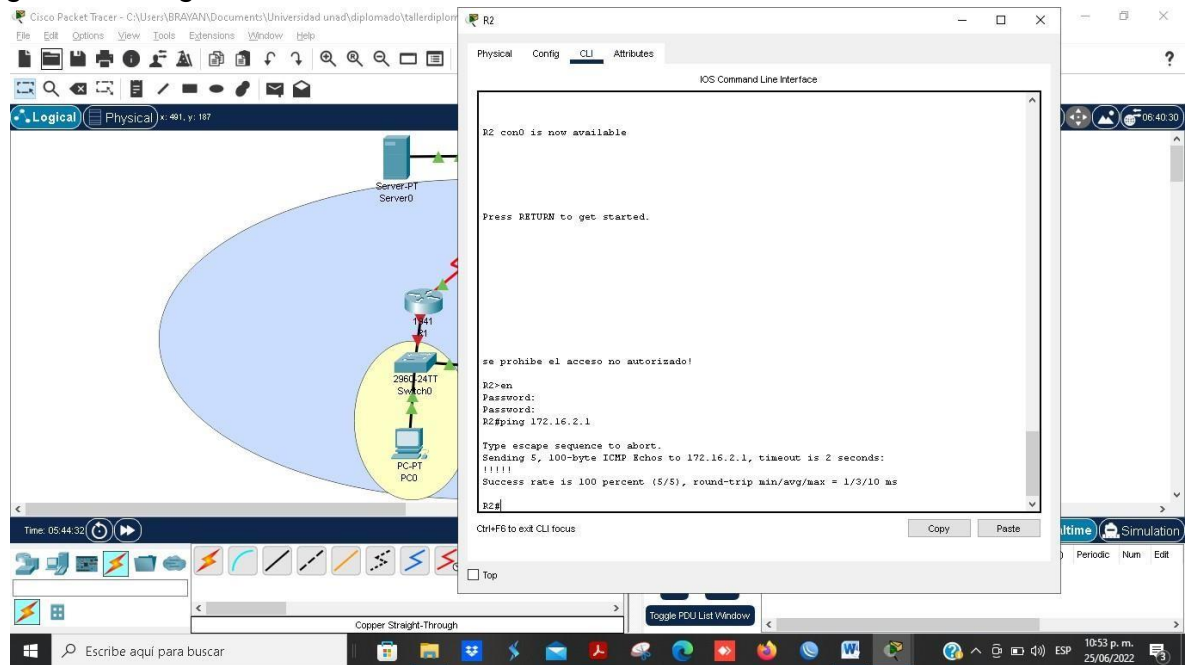
Fuente Autor.

Figura 19. Ping de R1 a R2.



Fuente Autor.

Figura 20. Ping de R2 a R3.



Fuente Autor.

Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN

Paso 1: Configurar S1

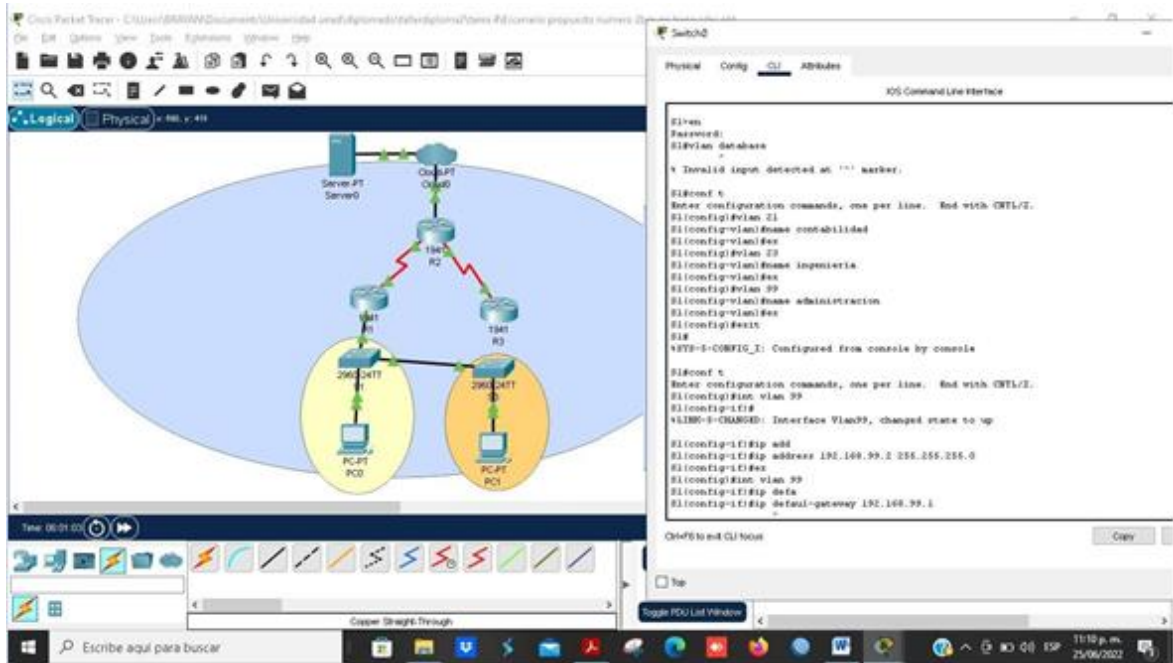
La configuración del S1 incluye las siguientes tareas:

Tabla 14. Configurar seguridad y Vlans en switch

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	vlan database vlan 21 name contabilidad vlan 23 name Ingenieria vlan 99 name Administracion
Asignar la dirección IP de administración.	interface Vlan 99 ip address 192.168.99.2 255.255.255.0 exit
Asignar el gateway predeterminado	ip default-gateway 192.168.99.1 exit
Forzar el enlace troncal en la interfaz F0/3	int f0/3 switchport mode trunk switchport trunk native vlan 1 exit
Forzar el enlace troncal en la interfaz F0/5	int f0/5 switchport mode trunk switchport trunk native vlan 1 no shutdown exit
Configurar el resto de los puertos como puertos de acceso	int range f0/1-2, f0/4, f0/6-24, g0/1-2 switchport mode access exit
Asignar F0/6 a la VLAN 21	interface fastEthernet 0/6 switchport access vlan 21 no shutdown exit
Apagar todos los puertos sin usar	interface range fastEthernet 0/1-2, f0/4, f0/7-24, g0/1-2 shutdown

Fuente Autor.

Figura 21. Configurar seguridad y Vlans en switch 1.



Fuente Autor.

Paso 1: Configurar S3

La configuración del S3 incluye las siguientes tareas:

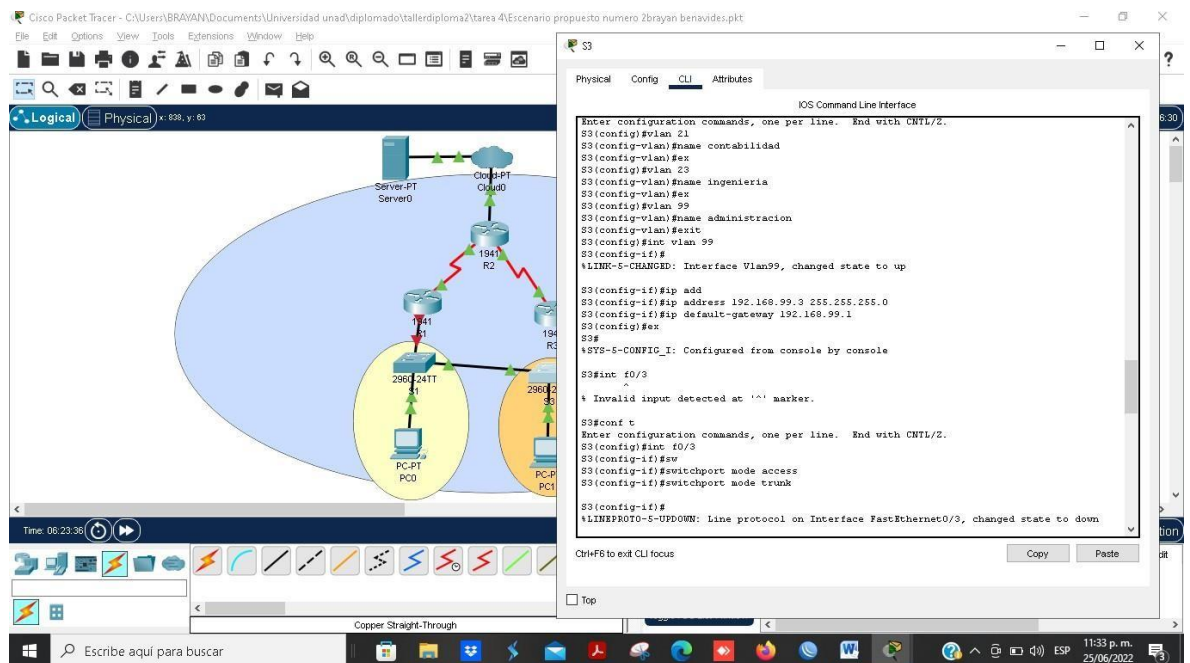
Tabla 15. Configurar seguridad y Vlans en switch 3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	<pre> vlan 21 name Contabilidad vlan 23 name Ingenieria vlan 99 name Administracion exit </pre>
Asignar la dirección IP de administración.	<pre> interface Vlan 99 ip address 192.168.99.3 255.255.255.0 exit </pre>
Asignar el gateway predeterminado	<pre> ip default-gateway 192.168.99.1 exit </pre>
Forzar el enlace troncal en la interfaz F0/3	<pre> int f0/3 switchport mode trunk switchport trunk native vlan 1 exit </pre>
Configurar el resto de los puertos como puertos de acceso	<pre> int range f0/1-2, f0/4-24, g0/1-2 switchport mode access </pre>

	exit
Asignar F0/18 a la VLAN 23	interface f0/18 switchport access vlan 23 exit
Apagar todos los puertos sin usar	interface range f0/1-2, f0/4, f0/7-24, g0/1-2 shut

Fuente Autor.

Figura 22. Configurar seguridad y Vlans en switch 3.



Fuente Autor.

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16. Configurar las sub-interfaces 802.1Q en las Vlans

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	int g0/1.21 description LAN Contabilidad encapsulation dot1Q 21 ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	int g0/1.23 description LAN 23 Ingenieria encapsulation dot1Q 23

	ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	g0/1.99 description LAN 99 Administracion encapsulation dot1Q 99 ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	int g0/1 no shut

Fuente Autor.

Paso 4: Verificar la conectividad de la red

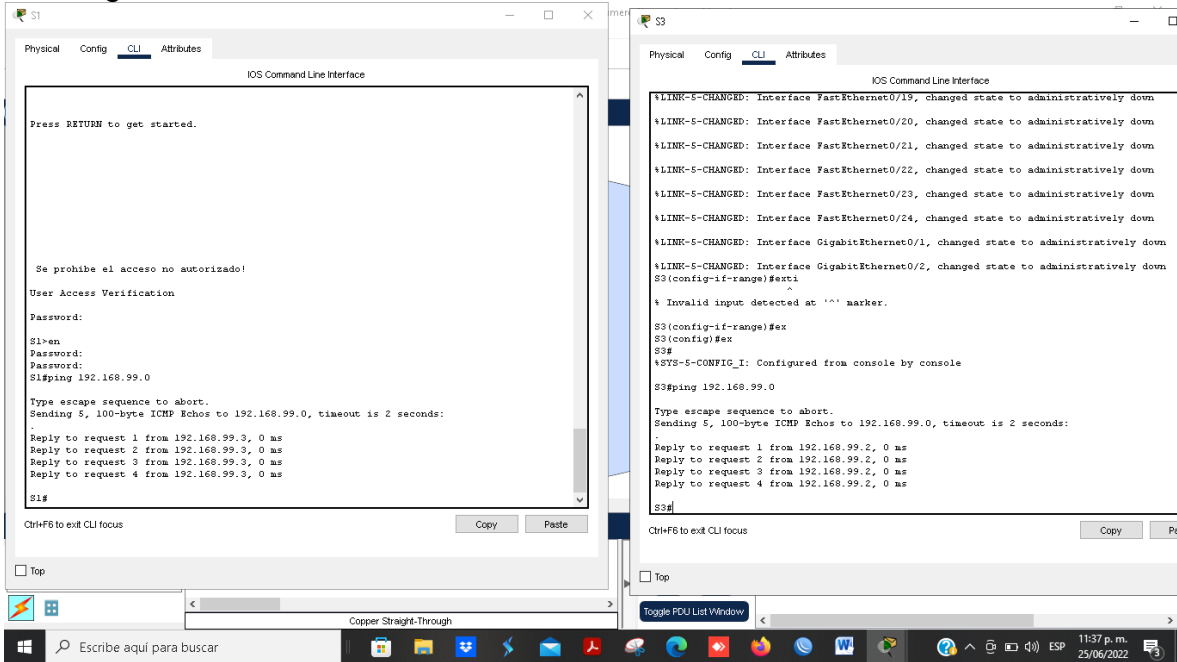
Utilice el comando ping para probar la conectividad entre los switches y el R1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla.

Tabla 17. De Verificación la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.0	Ok
S3	R1, dirección VLAN 99	192.168.99.0	Ok
S1	R1, dirección VLAN 21	192.168.21.0	Ok
S3	R1, dirección VLAN 23	192.168.23.0	Ok

Fuente Autor.

Figura 23. Verificación de conectividad.



Fuente Autor.

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 18. Configurar OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	router ospf 1
Anunciar las redes conectadas directamente	router-id 1.1.1.1 network 192.168.21.0 0.0.0.255 area 0 network 192.168.23.0 0.0.0.255 area 0 network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	passive-int g0/1.21 passive-int g0/1.23 passive-int g0/1.99
Desactive la sumarización automática	router rip no auto-summary

Fuente Autor.

Figura 24. Configurar OSPF en el R1.

Paso 1: OSPF en el Configurar R2

Las tareas de configuración para R2 incluyen las siguientes:

Tabla 19. Configurar OSPF en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	router ospf 1
Anunciar las redes conectadas directamente	router-id 2.2.2.2 network 10.10.10.10 0.0.0.255 area 0 network 172.16.1.0 0.0.0.255 area 3 network 172.16.2.0 0.0.0.255 area 3
Establecer todas las interfaces LAN como pasivas	passive-int loopback 0
Desactive la sumarización automática	router rip no auto-summary

Fuente Autor.

Paso 3: Configurar OSPFv3 en el R2

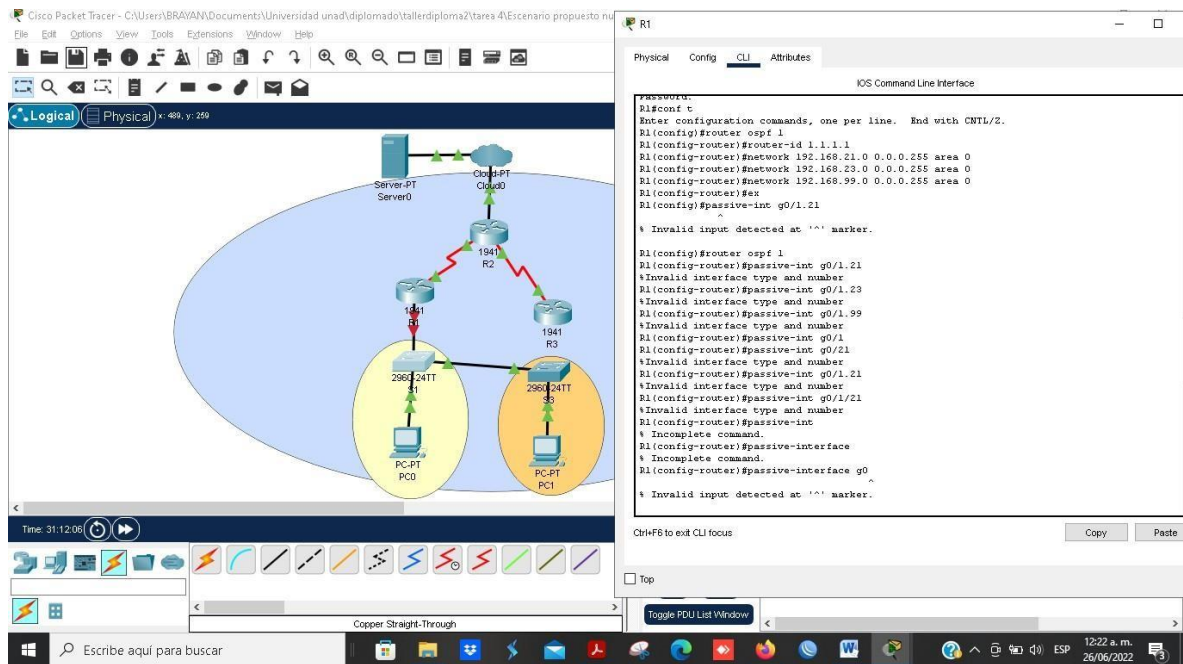
La configuración del R3 incluye las siguientes tareas:

Tabla 20. Configurar OSPFv3 en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	ipv6 unicast-routing
Anunciar redes IPv4 conectadas directamente	network 10.10.10.10 0.0.0.255 area 0 network 172.16.1.0 0.0.0.255 area 3 network 172.16.2.0 0.0.0.255 area 3
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	No permite
Desactive la sumarización automática.	No permite el comando “no auto-summary”

Fuente Autor.

Figura 25. Configurar OSPFv3 en el R2.



Fuente Autor.

Paso 4: Verificar la información de OSPF

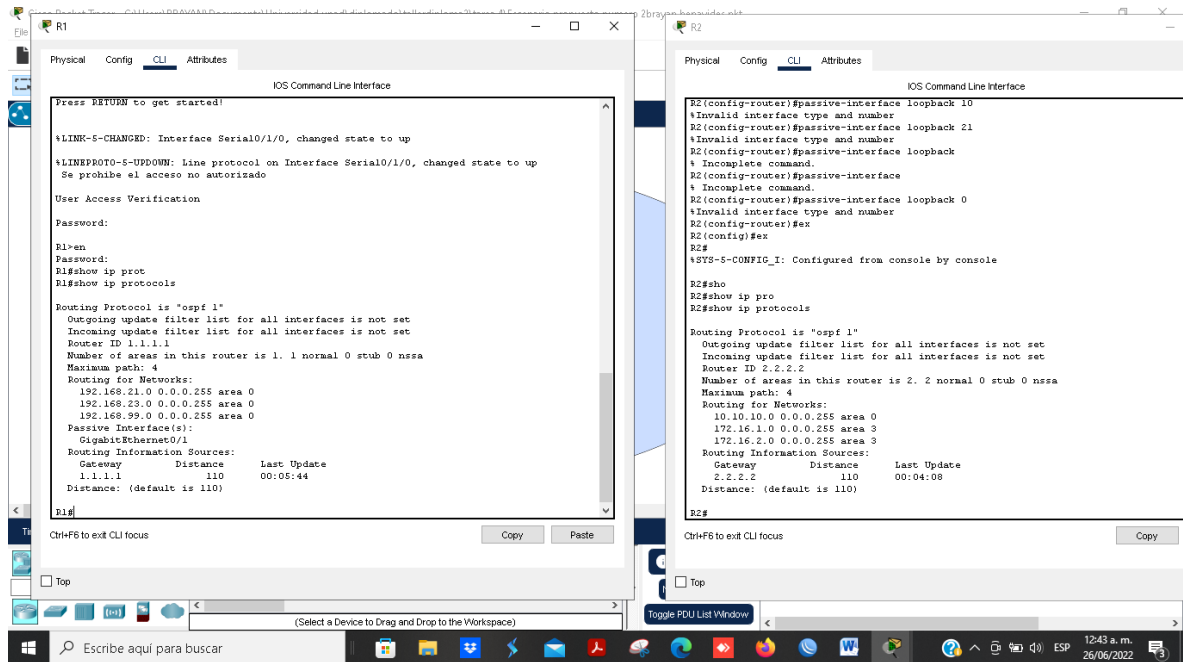
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 21. Verificar la información de OSPF.

Pregunta	Respuesta
¿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?	Show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Show ip ospf

Fuente Autor.

Figura 26. Verificar la información de OSPFv3.



Fuente Autor.

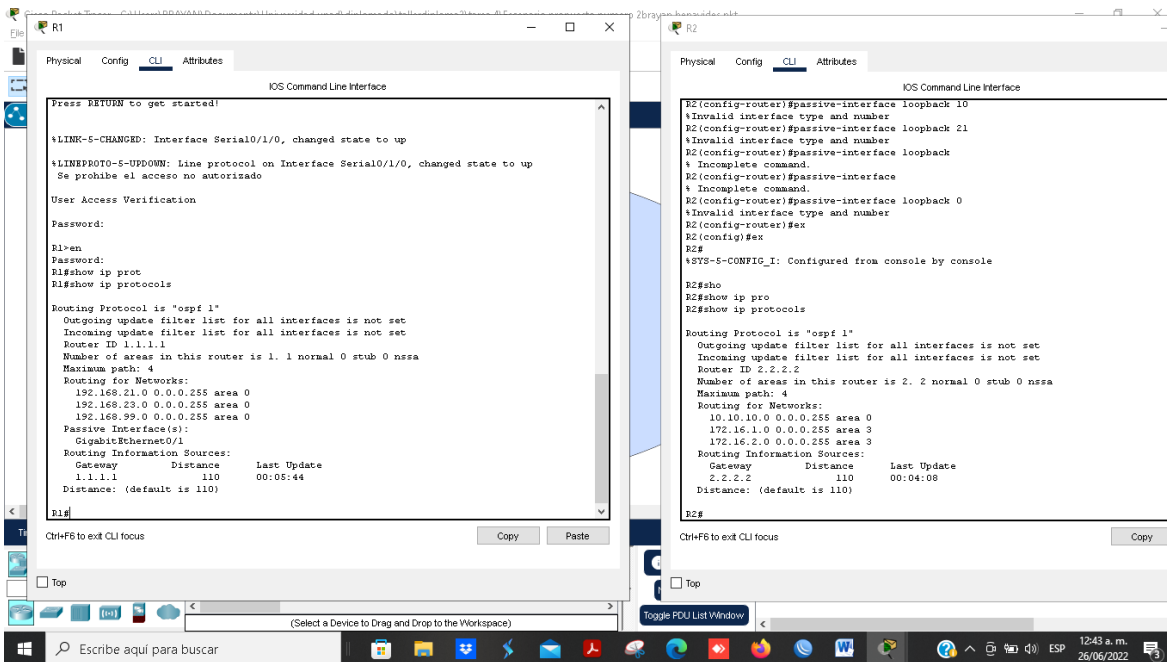
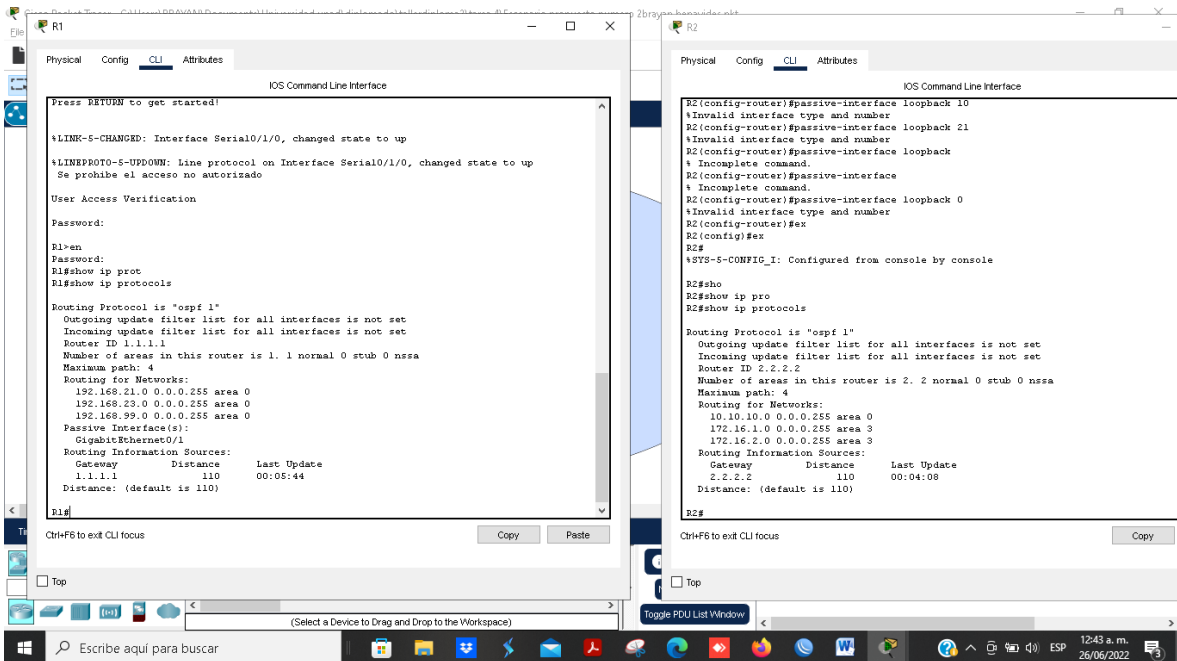


Figura 27.

Verificar la información de OSPFv3.



Fuente Autor.

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

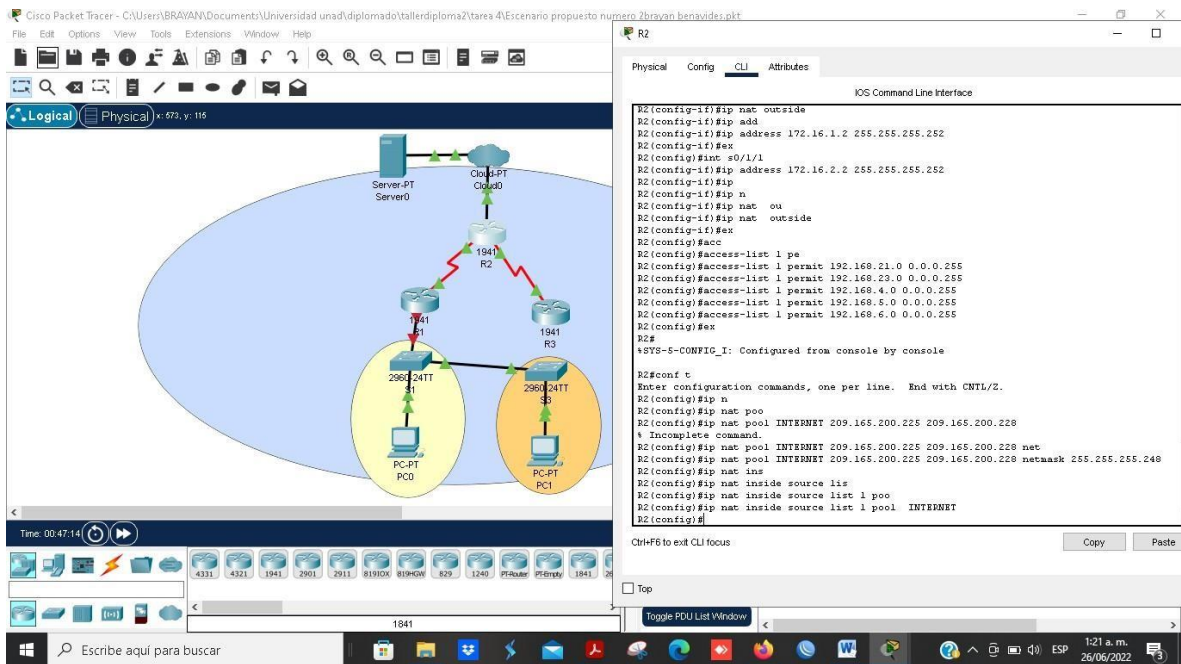
La configuración del R2 incluye las siguientes tareas:

Tabla 22. Configurar la NAT estática y dinámica en el 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	
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.229 R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	int g0/0 ip nat inside exit int lo0 ip nat outside
Configurar la NAT dinámica dentro de una ACL privada	access-list 1 permit 192.168.21.0 0.0.0.255 access-list 1 permit 192.168.23.0 0.0.0.255 access-list 1 permit 192.168.4.0 0.0.0.255 access-list 1 permit 192.168.5.0 0.0.0.255 access-list 1 permit 192.168.6.0 0.0.0.255
Defina el pool de direcciones IP públicas utilizables.	ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	ip nat inside source list 1 pool INTERNET

Fuente Autor.

Figura 29. Configurar la NAT estática y dinámica en el R2



Fuente Autor.

Paso 3: Verificar el protocolo DHCP y la NAT estática

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 23. Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Ok
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Ok
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	No se pudo
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	No se pudo

Fuente Autor.

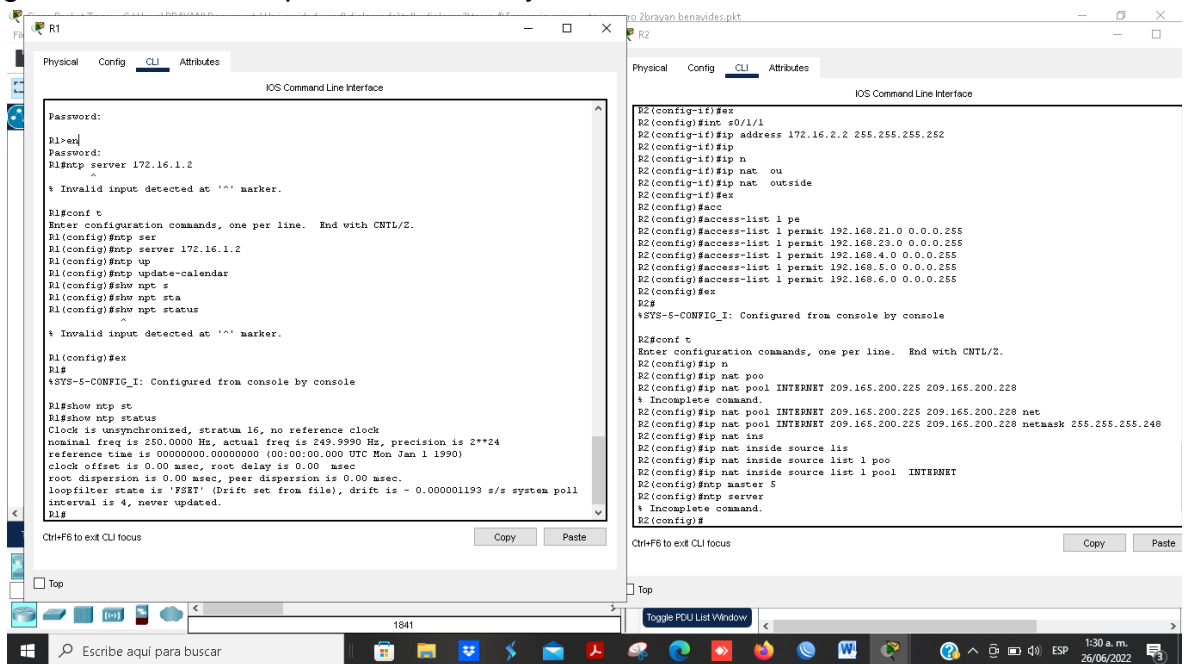
Parte 6: Configurar NTP

Tabla 24. Verificar el protocolo DHCP y la NAT estática

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00:00 05 march 2016
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1#show ntp status R1#show ntp associations

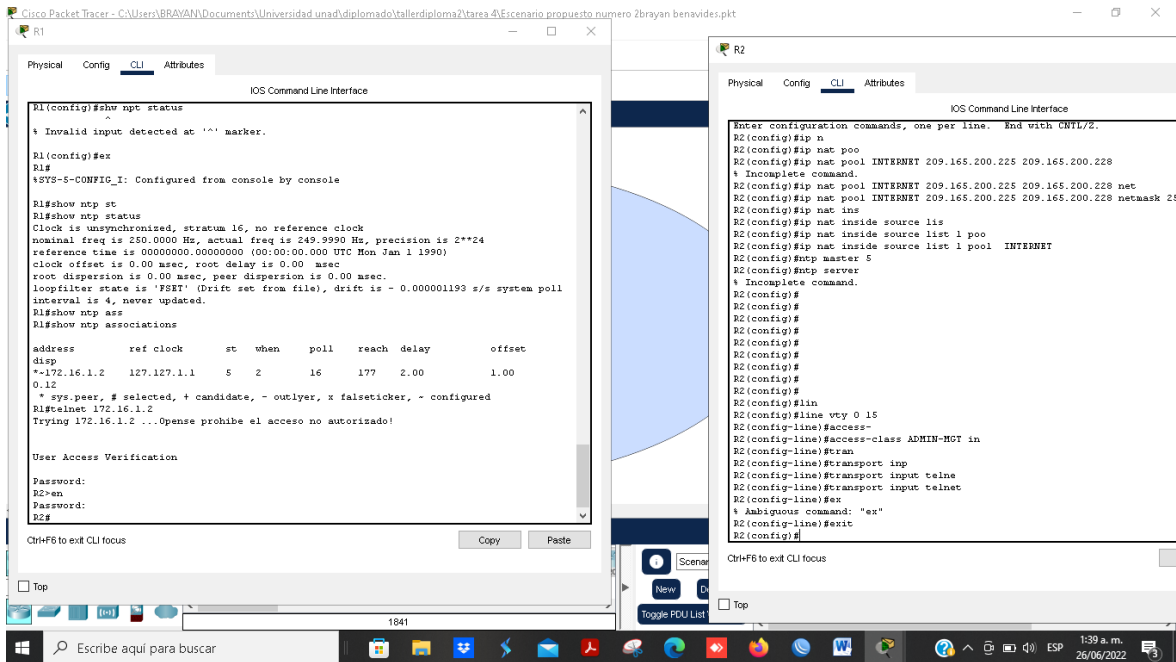
Fuente Autor.

Figura 30. Verificar el protocolo DHCP y la NAT estática



Fuente Autor.

Figura 31. Verificar el protocolo DHCP y la NAT estática



Fuente Autor.

Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrarlo siguiente

Tabla 26. Comando de CLI adecuado que se necesita para mostrar lo siguiente

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	show access-list
Restablecer los contadores de una lista de acceso	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 access-list
¿Con qué comando se muestran las traducciones NAT?	show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat translation

Fuente Autor.

CONCLUSIONES

El haber desarrollado este primer escenario del Diplomado de Profundización CCNA como opción de grado, profundiza el aprendizaje y permite al ingeniero obtener las competencias necesarias para implementar soluciones básicas o complejas en campo de las redes Networking.

El empleo de comandos para conectividad IPv4 e IPv6, enrutamiento Vlan, DHC y demás, los cuales, permiten la configuración dispositivos de redes en forma real mediante software, evitando realizar una costosa arquitectura, y finalmente se presenta como evidencia este documento diplomado NETWORKIN CCNA CISCO, como opción de grado, en el cual se evidencian los resultados obtenidos en el curso.

Escenario 2 se diseña enrutamiento dinámico OSPF, bajo un esquema de direccionamiento IP, para poder dar solución al diseño propuesto, se arma la topología de la red con varias Vlan y un enlace troncal entre switches, con la cual se puede llegar a proteger la red de datos en caso que se produzca una falla en las interfaces, se logró realizar la mayoría de las configuraciones existentes en switch y a un router, se aumentó la seguridad.

REFERENCIAS

- CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2>
- CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3>
- CISCO. (2019). Acceso a la red. Fundamentos de Networking. <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4>
- CISCO. (2019). Ethernet. Fundamentos de Networking. <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5>
- CISCO. (2019). Capa de red. Fundamentos de Networking. <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6>
- CISCO. (2019). Direccionamiento IP. Fundamentos de Networking <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7>
- CISCO. (2019). División de redes IP en subredes. Fundamentos de Networking. <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8>
- CISCO. (2019). Capa de transporte. Fundamentos de Networking. <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9>
- CISCO. (2019). Capa de aplicación. Fundamentos de Networking. <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10>
- CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11>
- CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10>