SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGIA CISCO

FABIO ALEJANDRO PEREZCARDENAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
TUNJA
2021

SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGIA CISCO

FABIO ALEJANDRO PEREZ CARDENAS

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

TUTORA:
Ing. NANCY AMPARO GUACA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
TUNJA
2021

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Tunja, 12 de diciembre de 2021

AGRADECIMIENTOS

A Dios por darme la oportunidad, a mi familia que ha sido mi motor y fuerza, a la Universidad Nacional Abierta y a Distancia, que han sido una gran compañía todo el proceso formativo, y me han llevado a la culminación exitosa de mi carrera profesional

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Conmutación: Se considera como la acción de establecer una vía, un camino, de extremo a extremo entre dos puntos, un emisor y un receptor a través de nodos o equipos de transmisión.

Ethernet: Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de bus; tiene ancho de banda de 10Mbps, por lo tanto, tiene una elevada velocidad de transmisión y se ha convertido en un estándar de red.

Hosts: El término host o anfitrión se usa en informática para referirse a las computadoras u otros dispositivos conectados a una red que proveen y utilizan servicios de ella.

SSH: Es el nombre de un protocolo y del programa que lo implementa cuya principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada.

Telnet: Telnet es el nombre de un protocolo de red que nos permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. También es el nombre del programa informático que implementa el cliente.

RESUMEN

En este trabajo busca dar solución a los escenarios planteados como parte de la actividad final del diplomado de CISCO, realizado como opción de grado en mi carrera como Ingeniero de Sistemas identificando las herramientas de supervisión y protocolos de administración de red disponibles en el IOS para resolver los problemas de las redes de datos, evaluando el desempeño de routers y switches, mediante el uso de comandos especializados en gestión de redes y compatibles con el protocolo SMNP, propuestos para el escenario 1, donde además se requieren realizar tareas de selección y configuración de dispositivos en el simulador Packet Tracer que nos servirán como base para realizarlos de manera real. Se configuran aspectos básicos de seguridad en los routers y switches, con el ánimo de restringir el manejo por personal distinto a los administradores de la red.

Para el segundo escenario se realizan configuraciones 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.

Se puede concluir que estos escenarios están perfectamente diseñados para aplicación de los conocimientos adquiridos, lo que nos convertirá en grandes administradores de redes en nuestro futuro profesional en el campo de la Ingeniería.

Palabras Claves: Conmutación – Ethernet – Hosts – SSH - Telnet

ABSTRACT

In this work, he seeks to solve the scenarios proposed as part of the final activity of the CISCO diploma, carried out as a degree option in my career as a Systems Engineer, identifying the supervision tools and network administration protocols available in the IOS to solve data network problems, evaluating the performance of routers and switches, through the use of specialized commands in network management and compatible with the SMNP protocol, proposed for scenario 1, where it is also required to perform tasks of selection and configuration of devices in the Packet Tracer simulator that will serve as a basis for realizing them. Basic security aspects are configured in routers and switches, with the aim of restricting handling by personnel other than network administrators.

For the second scenario, IPv4 and IPv6 configurations, switch security, inter-VLAN routing, the dynamic routing protocol OSPF, the dynamic host configuration protocol (DHCP), the translation of dynamic and static network addresses (NAT), Access Control Lists (ACLs) and Network Time Protocol (NTP) server / client. During the evaluation, you will test and register your network using common CLI commands.

It can be concluded that these scenarios are perfectly designed for the application of the acquired knowledge, which will make us great network administrators in our professional future in the field of Engineering.

Keywords: Switching - Ethernet - Hosts - SSH - Telnet

INTRODUCCIÓN

A paso del tiempo la tecnología se ha convertido en una parte fundamental de nuestras vidas, ayudándonos a comprender y responder a cada incógnita que se nos presentan, el internet ha cambiado el mundo la forma de pensar de la gente y ha trasformado sus costumbres y en general su entorno.

Con la implementación de los escenarios 1 y 2, se busca afianzar los conocimientos para el manejo de asignación de direccionamiento IPv4 e IPv6, ruteo para las VLAN, configuración de protocolos dinámicos y estáticos, configuraciones OSPF, NAT, NTP, listas de control de acceso (ACL), entre otros requerimientos solicitados por la guía de actividades.

Este se realiza con el ánimo de aprender e implementar los comandos necesarios que se utilizaran en campo real y que nos llevaran a desenvolvernos en el campo de las redes informáticas.

DESARROLLO

Escenario 1

Aspectos Básicos de la situación

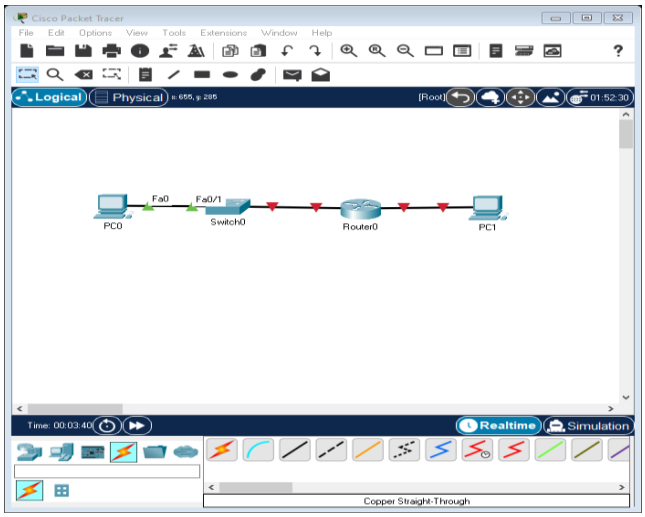
En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos, diseñar el esquema de direccionamiento IPv4 para las LAN propuestas. El router y el switch también deben administrarse de forma segura.

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 como se indica en la topología, y conecte los equipos de cómputo.

Según EL documento guía la conexión entre dispositivos debe realizarse de la siguiente forma del puerto FastEthernet0 de la PC_A, al puerto FastEthernet0/6 del Swicht (S1), esta se definirá como la LAN 1; del puerto GigabitEthernet0/1 del Swicht (S1), al puerto GigabitEthernet0/1 del Router (R1); Finalmente del puerto GigabitEthernet0/0 del Router al puerto FastEthernet0 de la PC_B, definida como LAN 2

Figura 1. Simulación Escenario 1



Fuente: Autoría Propia

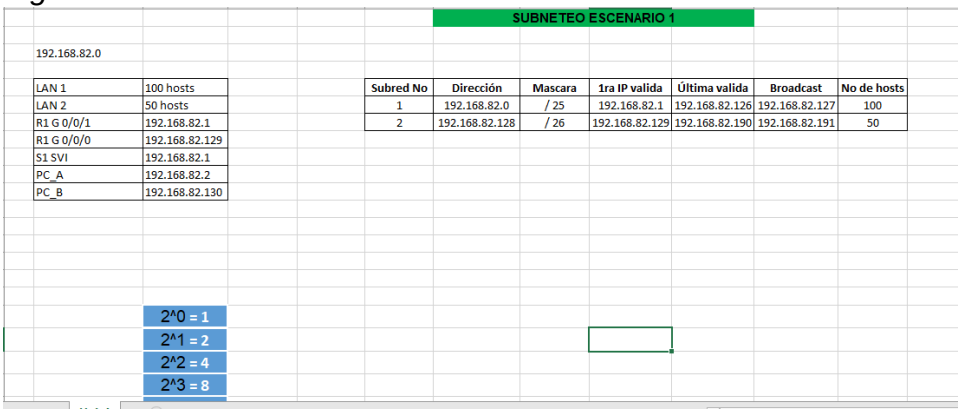
Parte 2: Desarrolle le esquema del direccionamiento IP

Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne la dirección 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 dos últimos dígitos de su cédula.

Para hallar cada una de las direcciones ip, debemos crear el Subneteo, en una hoja de Excel.

Figura 2. Subneteo Escenario 1



SUBNETEO ESCENARIO 1

192.168.82.0

LAN 1	100 hosts
LAN 2	50 hosts
R1 G 0/0/1	192.168.82.1
R1 G 0/0/0	192.168.82.129
S1 SVI	192.168.82.1
PC_A	192.168.82.2
PC_B	192.168.82.130

Subred No	Dirección	Mascara	1ra IP valida	Última valida	Broadcast	No de hosts
1	192.168.82.0	/ 25	192.168.82.1	192.168.82.126	192.168.82.127	100
2	192.168.82.128	/ 26	192.168.82.129	192.168.82.190	192.168.82.191	50

2^0 = 1
2^1 = 2
2^2 = 4
2^3 = 8

Fuente: Autoría Propia

Tabla 1. Direccionamiento Escenario 1

Ítem	Requerimiento
Dirección de Red	192.168.82.0 donde 82 corresponde a los dos últimos dígitos de mi cédula
Requerimiento de host subred LAN 1	192.168.82.0 (100 hosts)
Requerimiento de host subred LAN 2	192.168.82.128 (50 hosts)
R1 G 0/0	192.168.82.1
R1 G 0/1	192.168.82.129
S1 SVI	192.168.82.2
PC_0	192.168.82.126
PC_1	192.168.82.190

Fuente: Autoría Propia

Parte 3: Configure aspectos Básicos

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

Paso 1: Configurar los aspectos básicos

Las tareas de configuración para R1 incluyen las siguientes:

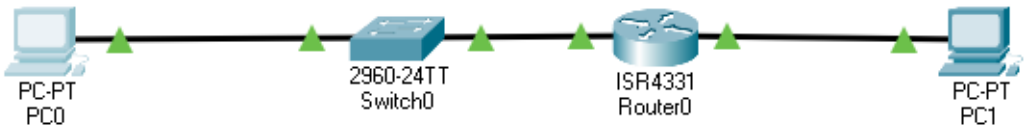
Tabla 2. Configuración de R1

Las tareas de configuración para R1 incluyen las siguientes: Tarea	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R1
Nombre de dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Establecer la longitud mínima para las contraseñas	10 caracteres
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar VTY solo aceptando SSH	
Cifrar las contraseñas de texto no cifrado	
Configure un MOTD Banner	
Configurar interfaz G0/0/0	Establezca la descripción Establece la dirección IPv4. Activar la interfaz.
Configurar interfaz G0/0/1	Establezca la descripción Establece la dirección IPv4. Activar la interfaz.
Generar una clave de cifrado RSA	Módulo de 1024 bits

Fuente: Autoría Propia

1. Escenario 1

Figura 3. escenario1



Fuente: Autoría Propia

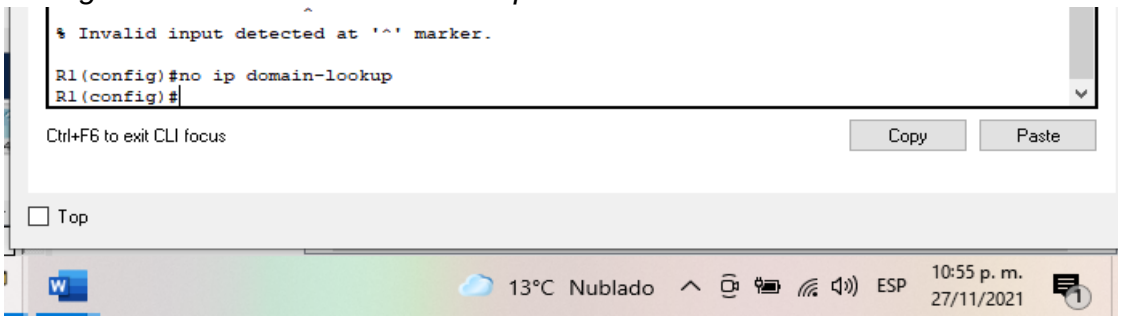
1.1. Aplique las configuraciones iniciales y los protocolos de enrutamiento para el router R1, según el diagrama. No asigne passwords en los routers. Configurar las interfaces con las direcciones que se muestran en la topología de red.

Se procede a configurar cada uno el enrutador. 1
Se asigna nombre y protocolo de comunicación asignados.

Router R1
Router>

Router>enable	Ingreso al modo privilegiado
Router#configure terminal	Ingreso al modo de configuración
Router(config)# No ip domain-lookup	Desactivamos las búsquedas DNS

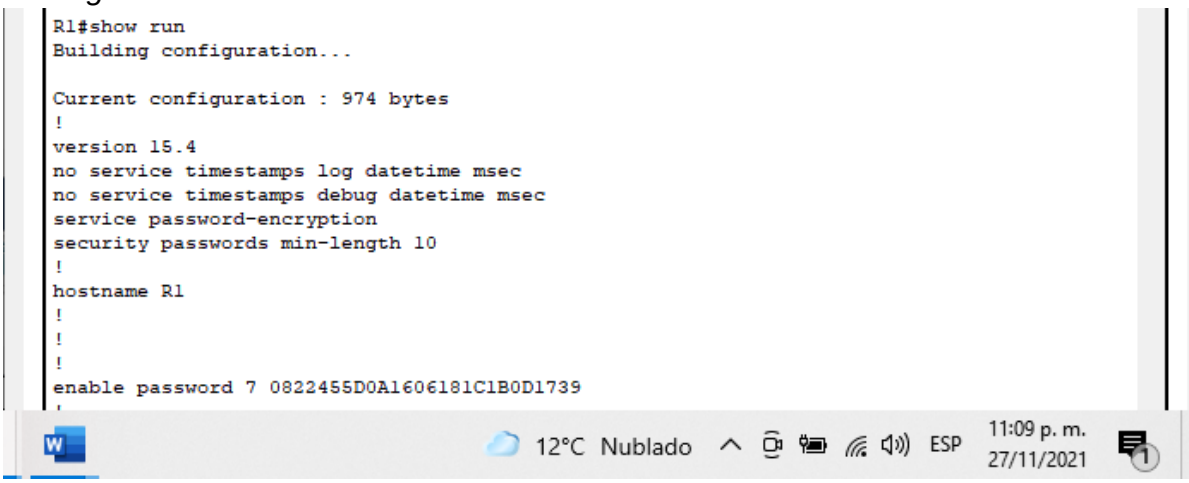
Figura4. Deshabilitar de las búsquedas DNS en R1



Fuente: Autoría Propia

Router(config)#hostname R1 *Se asigna nombre al router*

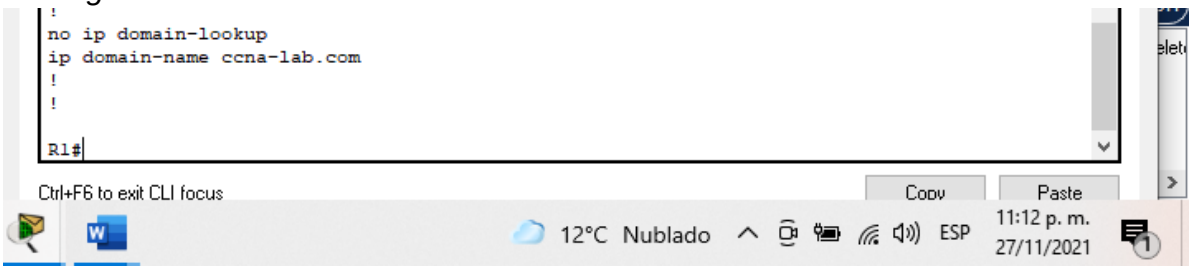
Figura5. Nombre del Router



Fuente: Autoría Propia

R1(config)# ip domain name ccna-lab.com *Se asigna nombre de dominio*

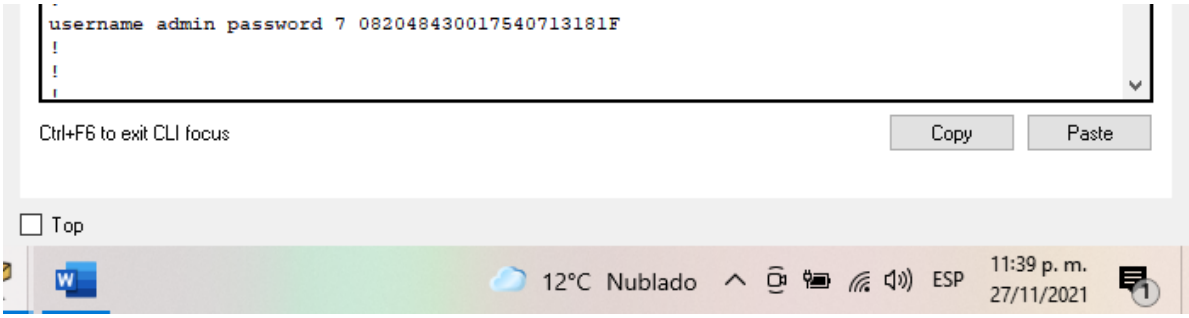
Figura6. Dominio del Router 1



Fuente: Autoría Propia

R1(config)# enable password ciscoconpass	*Se asigna contraseña EXEC en modo privilegiado*
R1(config)# line console 0	*Se* crea contraseña de acceso a la consola
R1(config)# password ciscoenpass	
R1(config)# login	
R1(config)# security password min-length 10	Se establece longitud mínima para las contraseñas
R1(config)# username admin password admin1pass	*Se* crea un usuario administrativo *en la base de datos local*

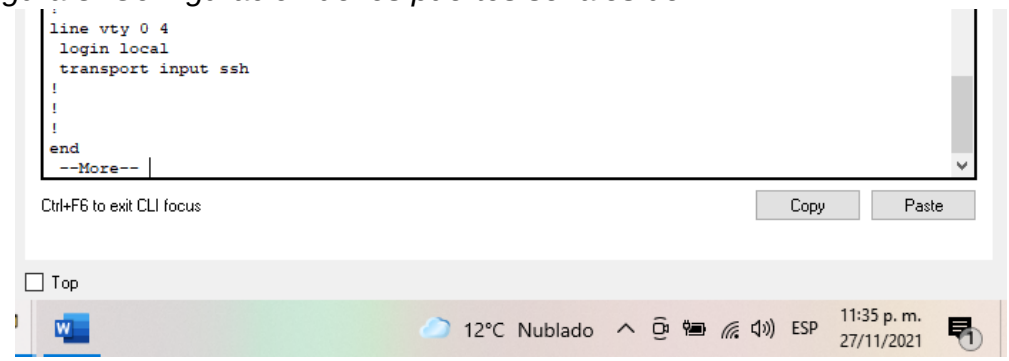
Figura 7. Asignación claves de acceso



Fuente: Autoría Propia

R1(config)# line vty 0 4 R1(config)# login local	Se configura inicio de sesión en las lineas vty para uso de BD local
R1(config)# transport input ssh	Se configura VTY solo aceptando SSH

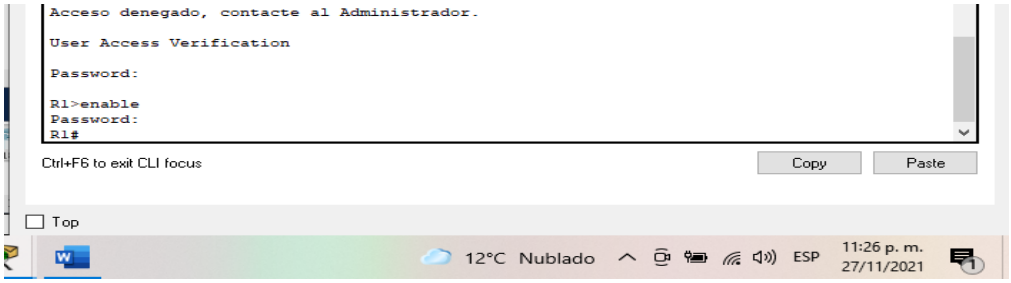
Figura 8. Configuración de los puertos seriales de R1



Fuente: Autoría Propia

R1(config)# service password-encryption Se cifra las contraseñas de texto
R1(config)# banner motd “El Acceso al Configuramos un motd banner
router es restringido. Únicamente personal autorizado”

Figura 9. Solicitud de credenciales de acceso

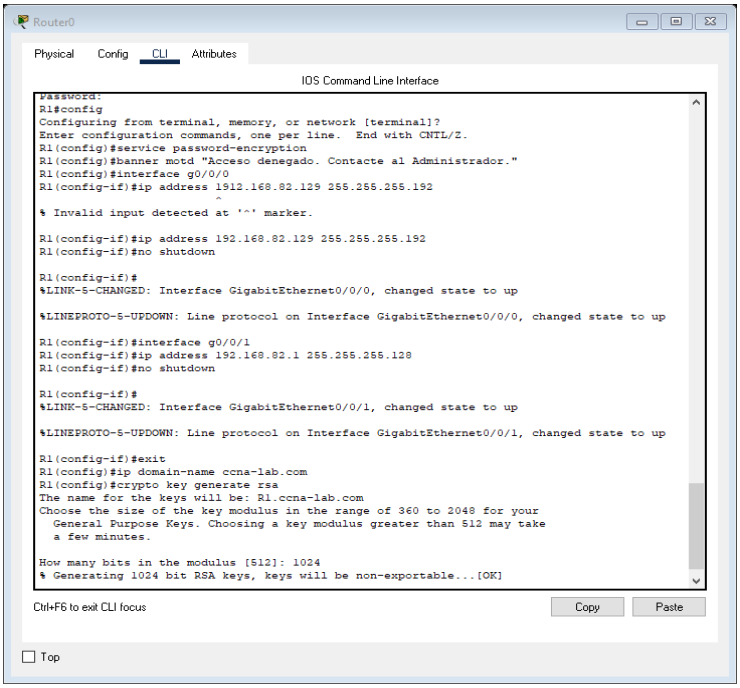


Fuente: Autoría Propia

R1(config)# interfaz G 0/0 Se configura la interface G 0/0
R1(config-if)# ip address 192.168.82.129 255.255.255.192
R1(config-if)# no shutdown

R1(config)# interfaz G 0/0/1 Se configura la interfaz G 0/0/1
R1(config-if)# ip address 192.168.82.1 255.255.255.128
R1(config-if)# no shutdown

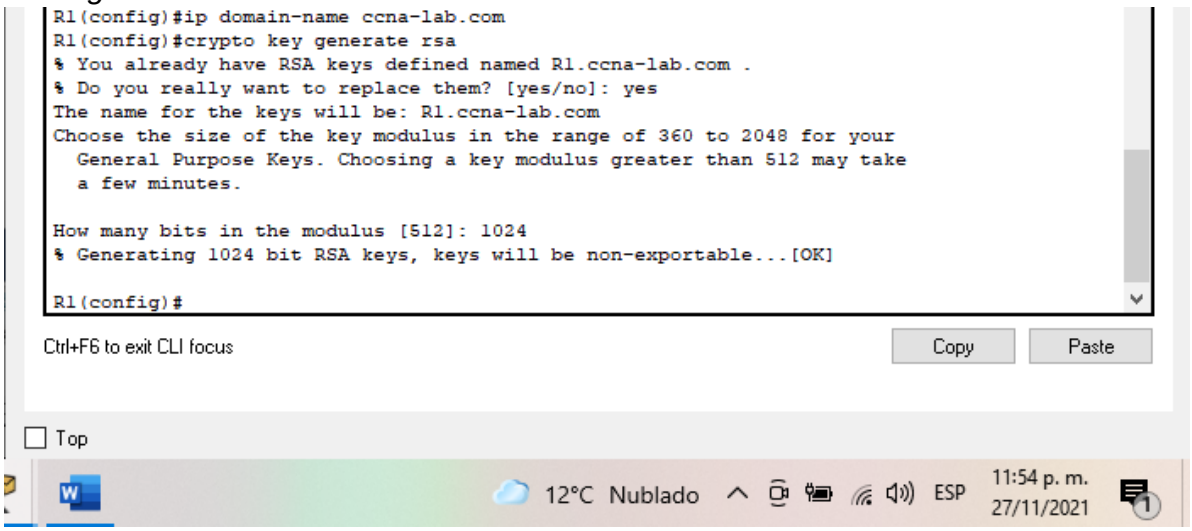
Figura10. Configuración de los puertos GigabitEthernet de R1



Fuente: Autoría Propia

R1(config)# ip domain-name ccna-lab.com	Generamos una clave de cifrado RSA
R1(config)# crypto key generate rsa	
How many bits in the modulus [512]: 1024	

Figura11. Generación clave de cifrado



Fuente: Autoría Propia

Las tareas de configuración del S1 incluyen:

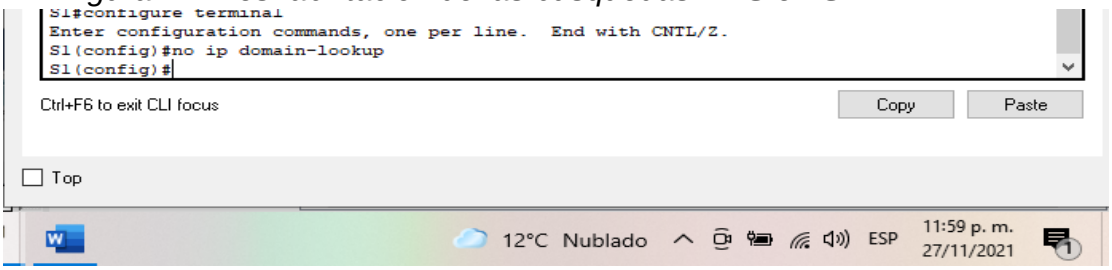
Tabla 3. Configuración de S1

Tarea	Especificación
Desactivar la búsqueda DNS.	
Nombre del switch	S1
Nombre de dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Línea vty 0 4
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Line vty aceptando SSH
Cifrar las contraseñas de texto no cifrado	Ocultar contraseña
Configurar un MOTD Banner	Mensaje de ingreso
Generar una clave de cifrado RSA	Módulo de 1024 bits
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada conforme a la tabla de

Fuente: Autoría Propia

Swicht S1
Swicht>
Swicht>enable — Se ingresa al modo privilegiado
Swicht#configure terminal — Se ingresa al modo de configuración
Swicht(config)# No ip domain-lookup — Se Desactivan las búsquedas DNS

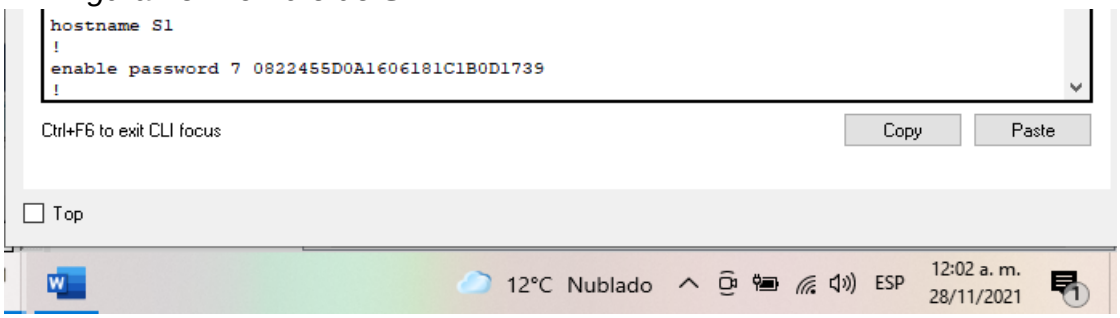
Figura 12. Deshabilitación de las búsquedas DNS en S1



Fuente: Autoría Propia

Swicht(config)#hostname S1 — Se Asigna nombre al Swicht

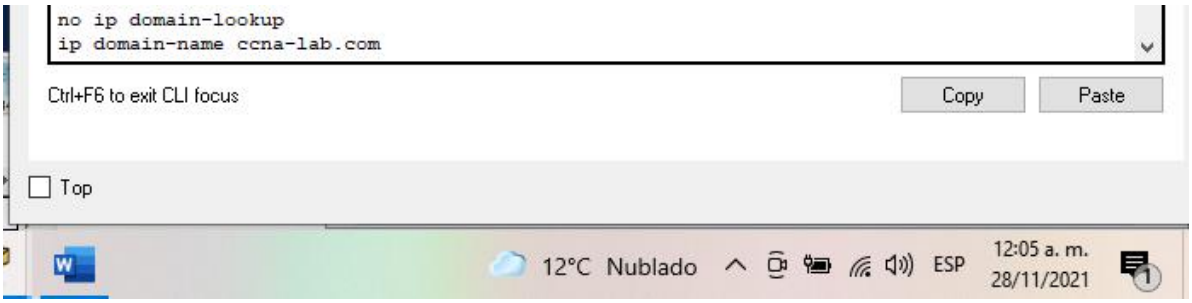
Figura 13. Nombre de S1



Fuente: Autoría Propia

S1(config)# ip domain name ccna-lab.com — Se asigna nombre de dominio

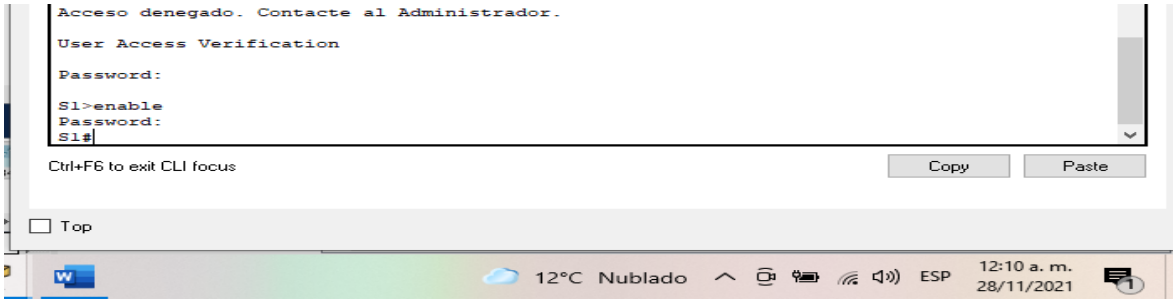
Figura 14. Nombre de dominio de S1



Fuente: Autoría Propia

S1(config)# enable password ciscoconpass	Se asigna contraseña EXEC en modo privilegiado
S1(config)# line console 0	Se crea contraseña de acceso a la consola
S1(config)# password ciscoenpass	
S1(config)# login	

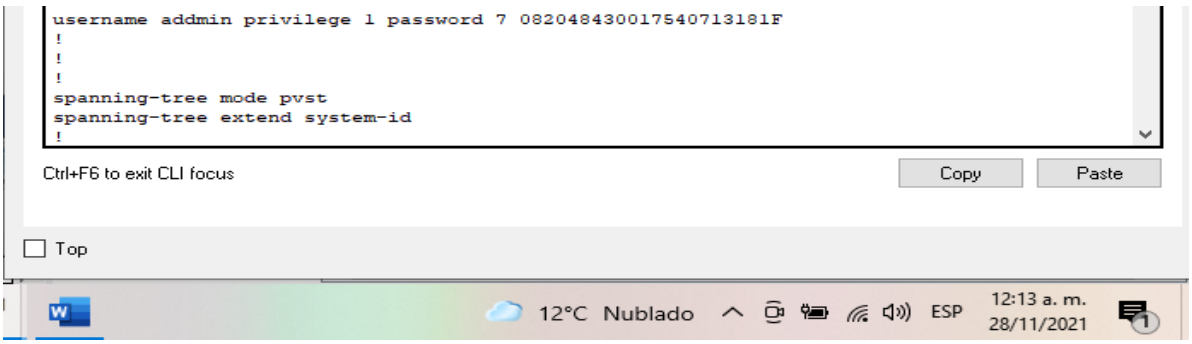
Figura 15. Asignación de claves de acceso a S1



Fuente: Autoría Propia

S1(config)# username admin password admin1pass	Se Crea un usuario adminstrativo en la base de datos local

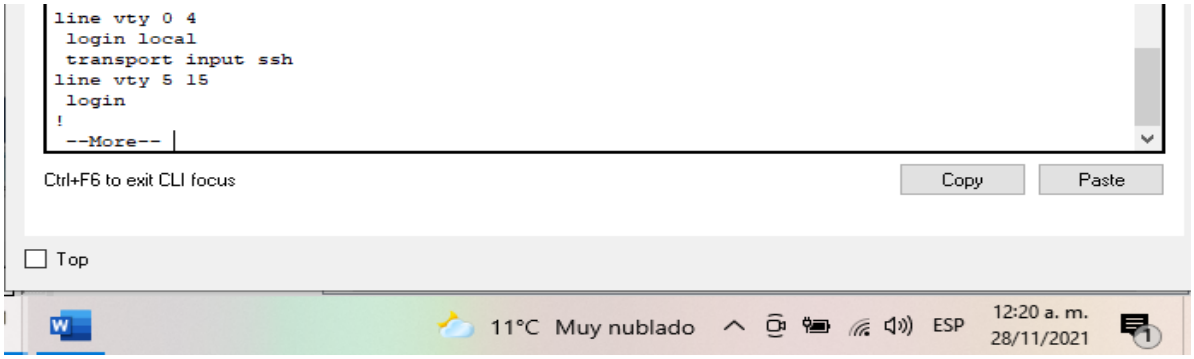
Figura 16. Creación de base de datos local



Fuente: Autoría Propia

S1(config)# line vty 0 4	Se Configura inicio de sesión en las
S1(config)# login local	lineas vty para uso de BD local
S1(config)# transport input ssh	Se Configura VTY solo aceptando SSH
S1(config)# service password-encryption	Se cifra las contraseñas de texto

Figura 17. Verificación de las líneas vty aceptando ssh

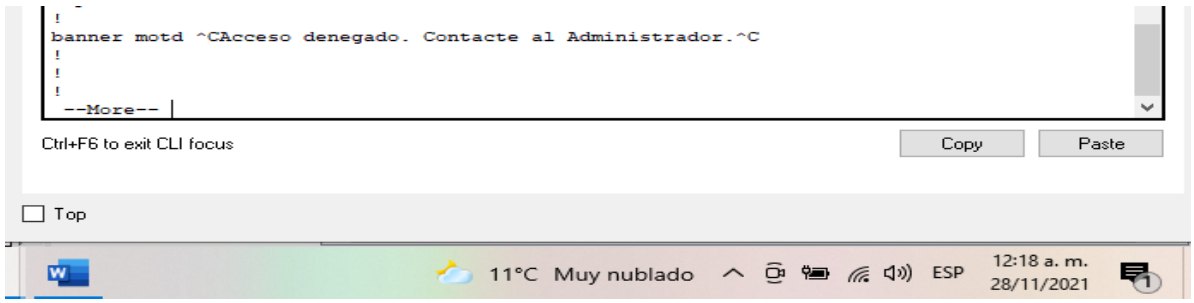


Fuente: Autoría Propia

S1(config)# banner motd “El Acceso al Router es restringido. Únicamente personal autorizado”

Se configura un motd banner

Figura 18. Verificación del banner motd



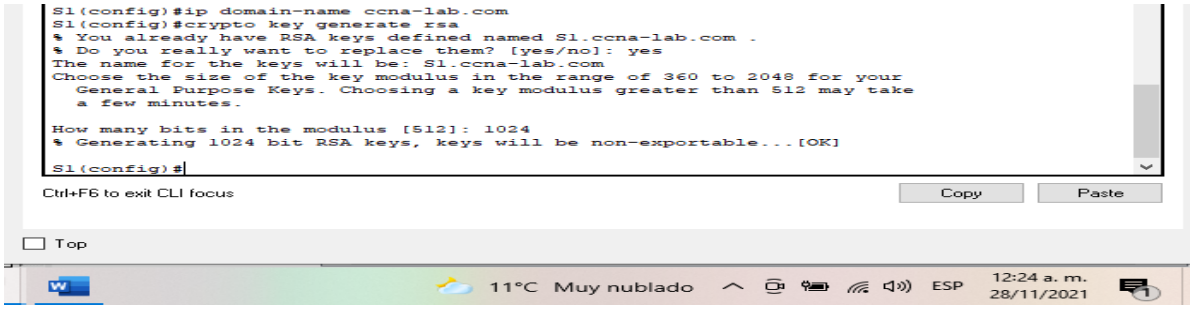
Fuente: Autoría Propia

S1(config)# ip domain-name ccna-lab.com

Se genera una clave de cifrado RSA

S1(config)# crypto key generate rsa
How many bits in the modulus [512]: 1024

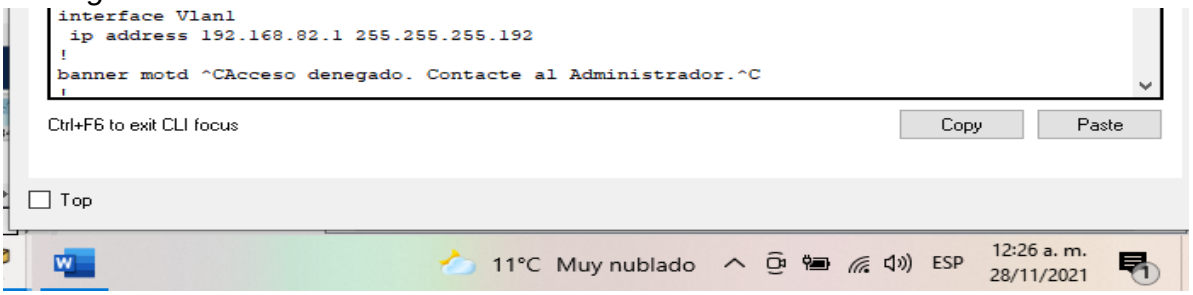
Figura 19. Verificación de clave RSA



Fuente: Autoría Propia

S1(config)# interface S1 SVI Se configura la interface SVI
S1(config-if)# ip address 192.168.82.2 255.255.255.192
S1(config-if)# no shutdown

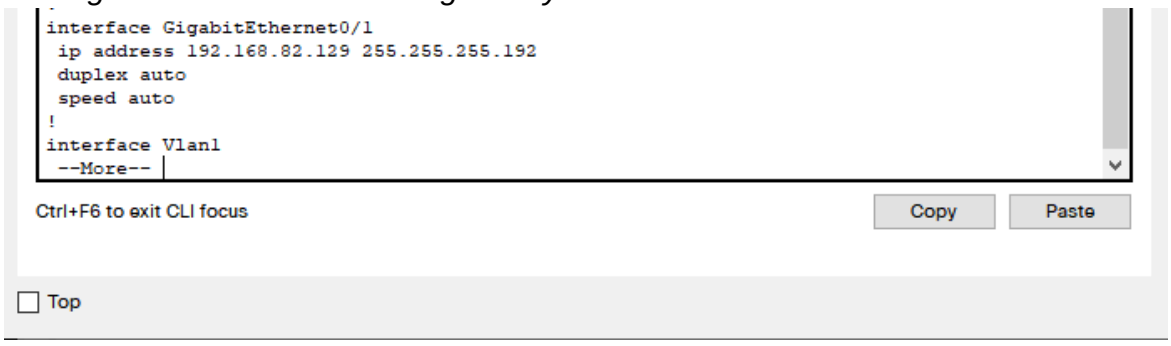
Figura 20. Interface vlan 1



Fuente: Autoría Propia

S1(config)# interface G0/1 Se configura el Gateway
S1(config-if)# ip address 192.168.82.129 255.255.255.192
S1(config-if)# no shutdown

Figura 21. Verificación del gateway



Fuente: Autoría Propia

Paso 2: Configurar los equipos

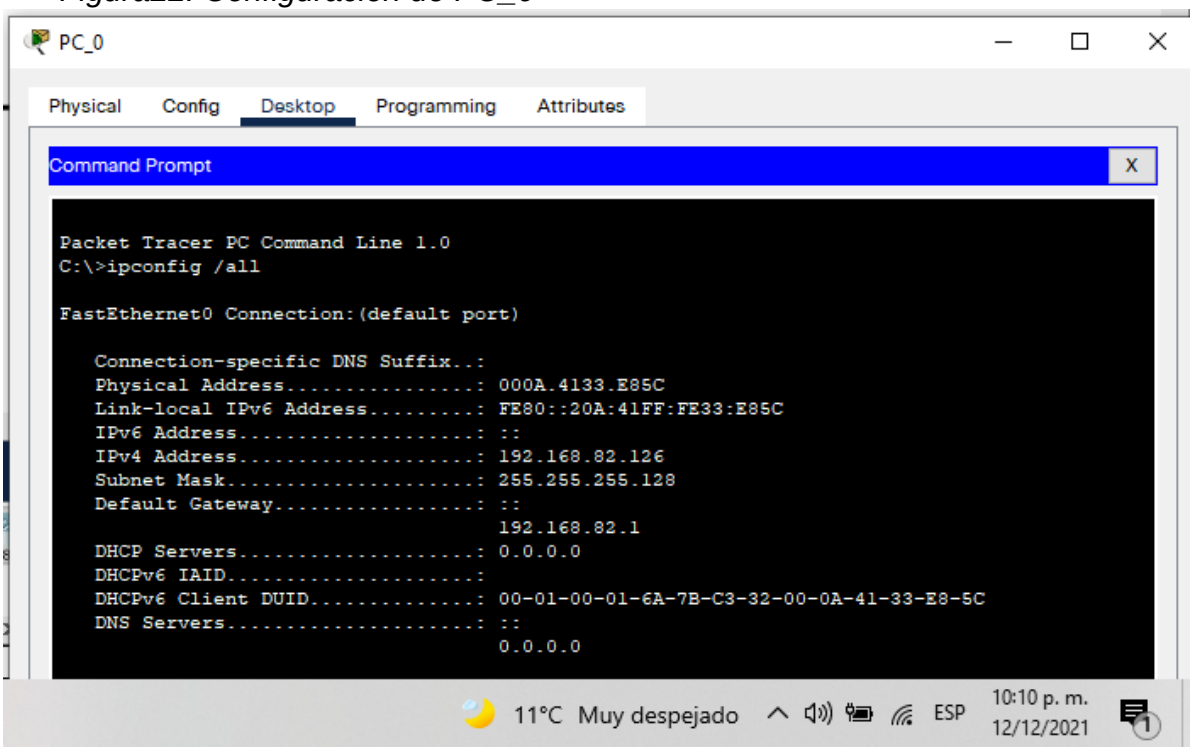
Configure los equipos host PC_A y PC_B conforme a la tabla de direccionamiento, registre las configuraciones de red de los hosts con el comando ipconfig / all

Tabla 4. PC_0 Network Configuration

PC-0 Network Configuration	
Descripción	FastEthernet0 connection: (default port)
Dirección física	*000A.4133.E85C*
Dirección IP	*192.168.82.126*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*192.168.82.1*

Fuente: Autoría Propia

Figura22. Configuración de PC_0



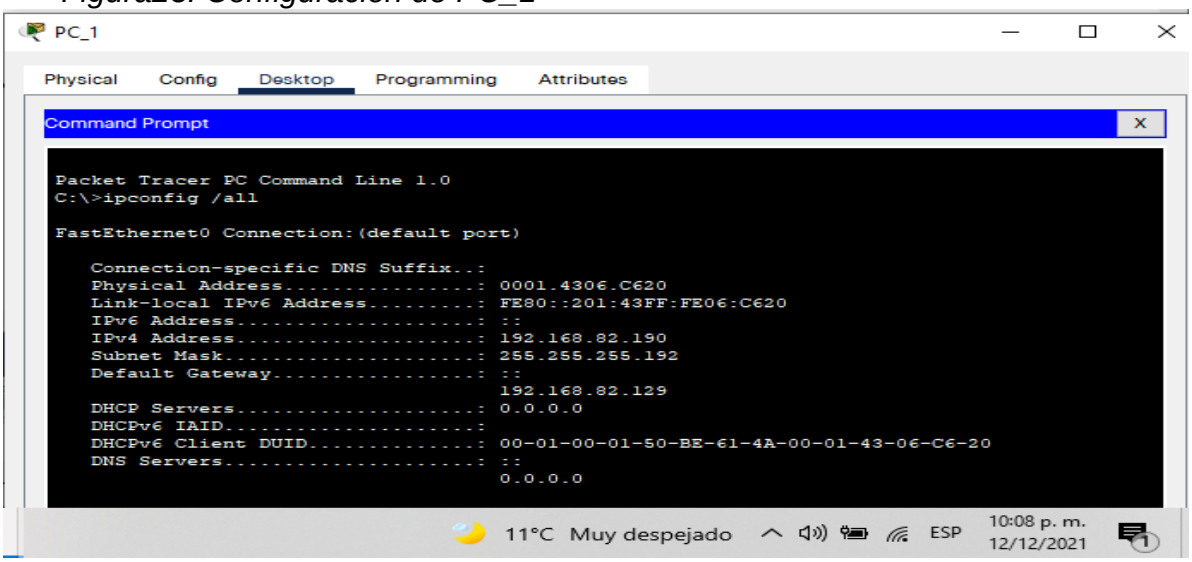
Fuente: Autoría Propia

Tabla 5 .PC_1 Network Configuration

PC-1 Network Configuration	
Descripción	FastEthernet0 connection: (default port)
Dirección física	*0001.4306.620*
Dirección IP	*192.168.82.190*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*192.168.82.129*

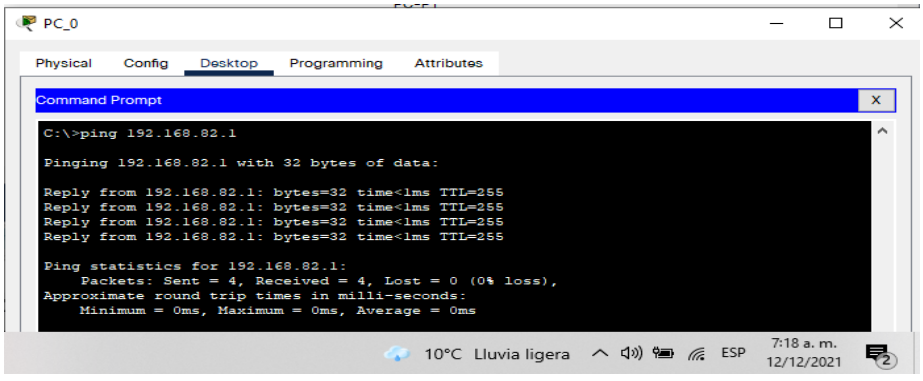
Fuente: Autoría Propia

Figura23. Configuración de PC_1



Fuente: Autoría Propia

Figura24. Prueba de conectividad



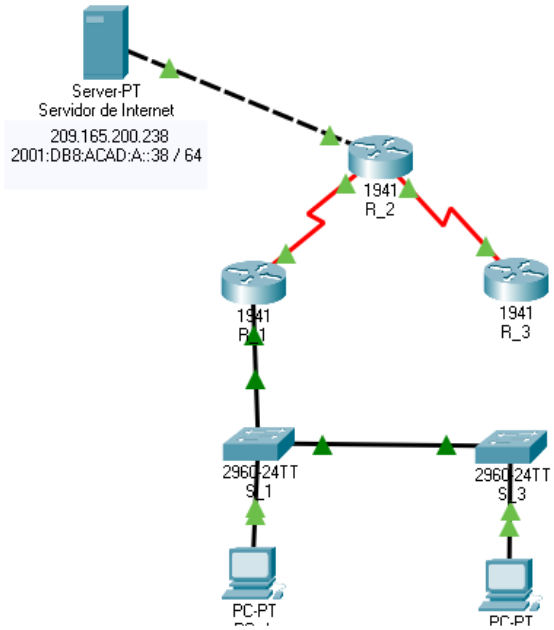
Fuente: Autoría Propia

Escenario 2

Aspectos Básicos de la situación

Vamos a configurar una red pequeña que tenga las siguientes configuraciones y demuestre conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, protocolo de routing dinámico OSPF, protocolo de configuración de hosts dinámicos (DHCP), traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos ingresados por consola

Figura25. Topología escenario 2



Fuente: Autoría Propia

Parte 1: Inicializar los dispositivos

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.

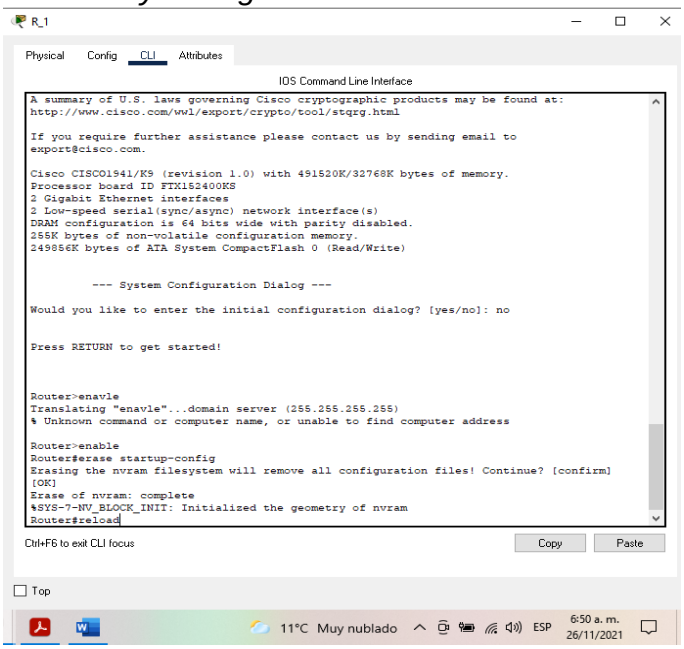
Tabla 6. Inicialización y cargar de routers y switches

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	*Router > enable* *Router# erase startup-config*
Volver a cargar todos los routers	*Router# reload*
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	*switch>enable* *switch#delete vlan.dat* *switch#erase startup-config*
Volver a cargar ambos switches	*swicht#reload*
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	*switch#show flash*

Fuente: Autoría Propia

R1

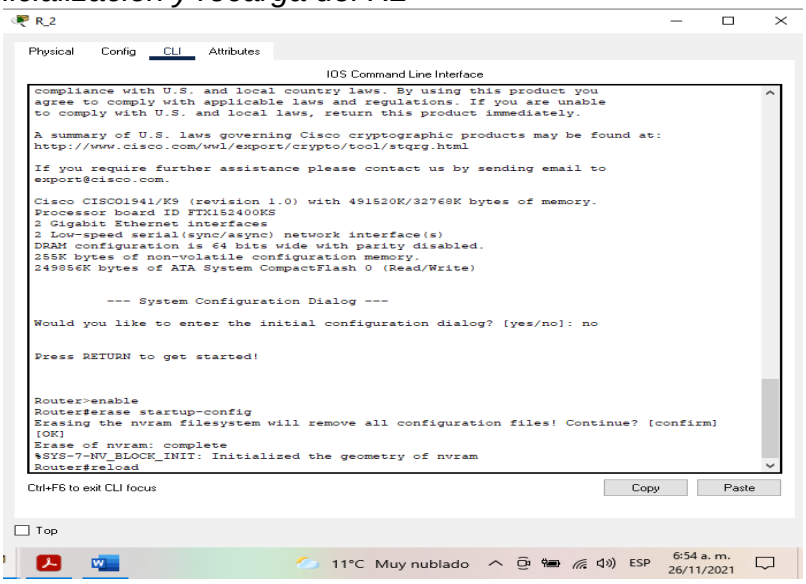
Figura26. Inicialización y recarga del R1



Fuente: Autoría Propia

R2

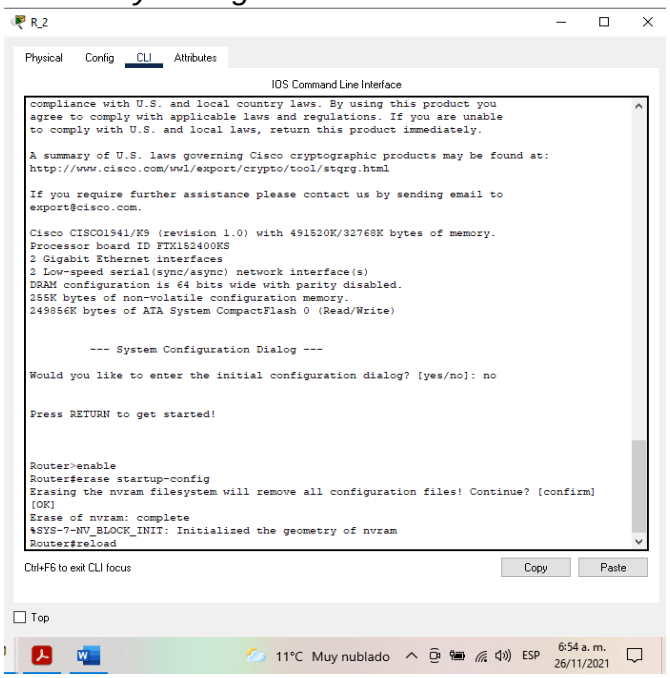
Figura27. Inicialización y recarga del R2



Fuente: Autoría Propia

R3

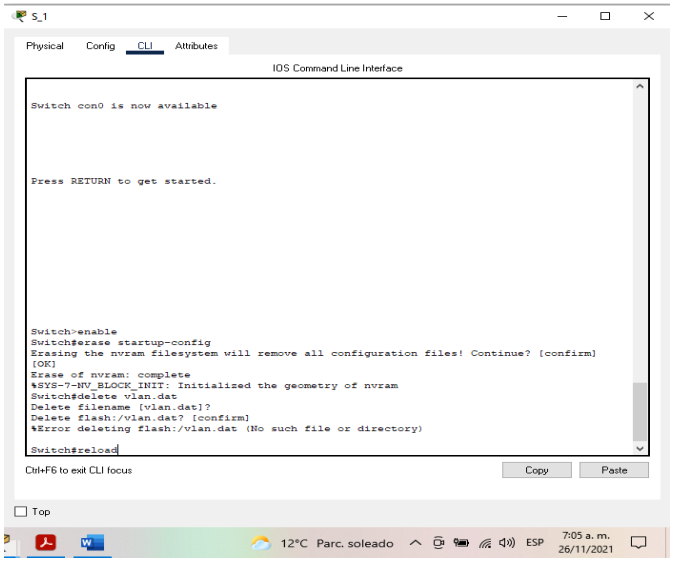
Figura28. Inicialización y recarga del R3



Fuente: Autoría Propia

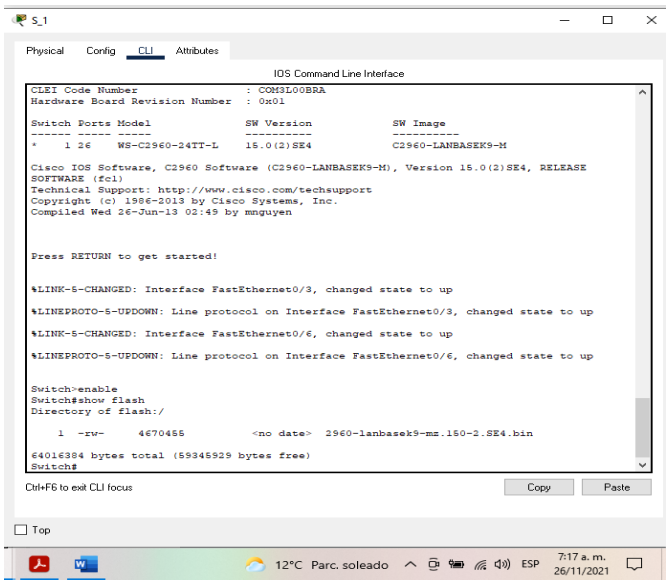
S1

Figura29. Inicialización y recarga del S1



Fuente: Autoría Propia

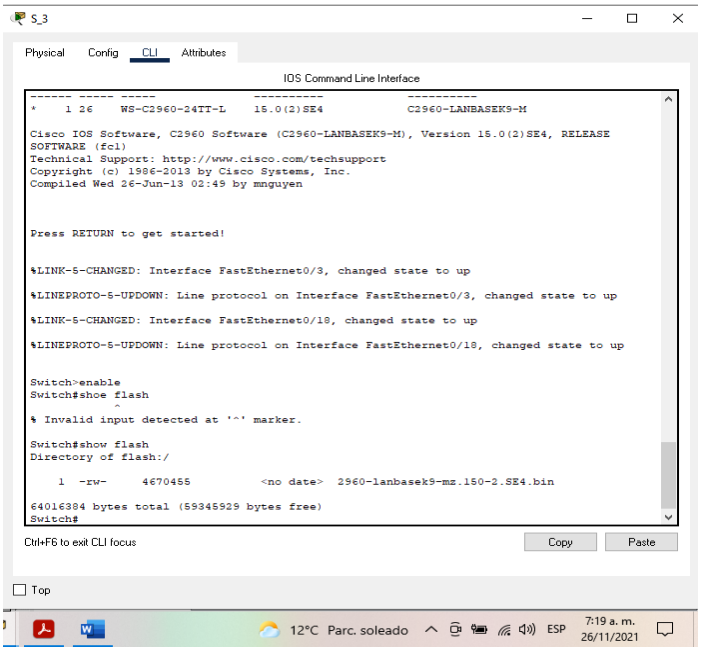
Figura30. Verificación de la memoria flash en S1



Fuente: Autoría Propia

S3

Figura 31. Verificación de la memoria flash en S3



Fuente: Autoría Propia

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 7. Direccionamiento de Servidor de Internet

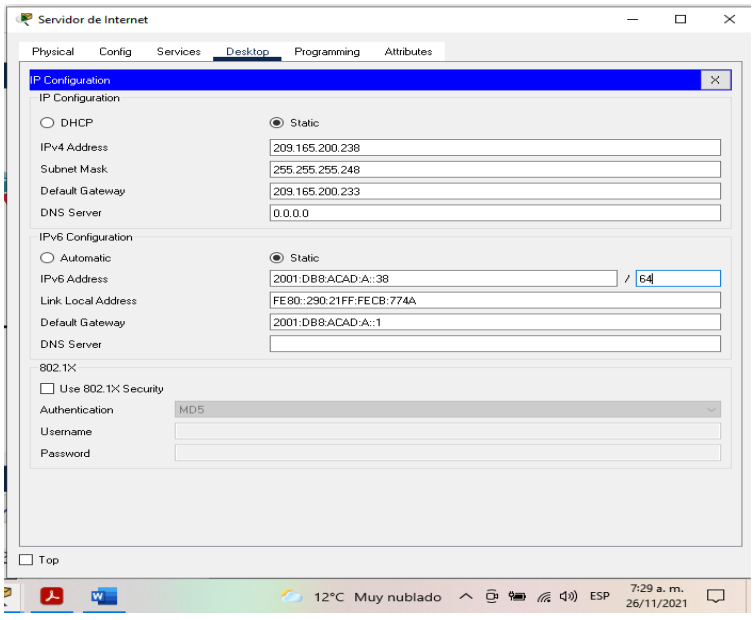
Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38 / 64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Fuente: Autoría Propia

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 32. Configuración de Servidor Web

,



Fuente: Autoría Propia

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

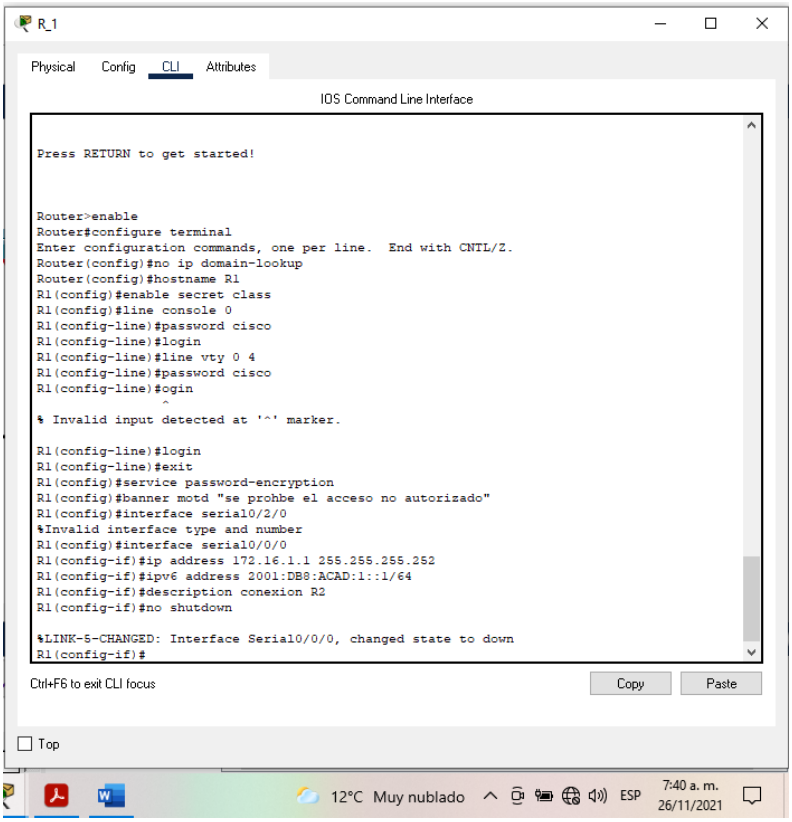
Tabla 8. Configuración de Router 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	*Router(config)#no ip domain-lookup*
Nombre del router	*Router(config)#hostname R1*
Contraseña de exec privilegiado cifrada	*R1(config)#enable secret class*
Contraseña de acceso a la consola	*R1(config)#line console 0* *R1(config-line)#password cisco* *R1(config-line)#login*
Contraseña de acceso Telnet	*R1(config-line)#line vty 0 15* *R1(config-line)#password cisco* *R1(config-line)#login*
Cifrar las contraseñas de texto no cifrado	*R1(config)#service password-encryption*
Mensaje MOTD	*R1(config)#banner motd "Se prohíbe el acceso no autorizado"*
Interfaz S0/0/0	*R1(config)#interface serial0/0/0* *R1(config-if)#ip address 172.16.1.1 255.255.255.252* *R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64* *R1(config-if)#description conexion R2* *R1(config-if)#no shutdown*
Rutas predeterminadas	*R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2* *R1(config)#ipv6 route ::/0 2001:DB8:ACAD:1::2*

Fuente: Autoría Propia

Nota: Todavía no configure G0/1.

Figura 33. Configuración de R1



Fuente: Autoría Propia

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

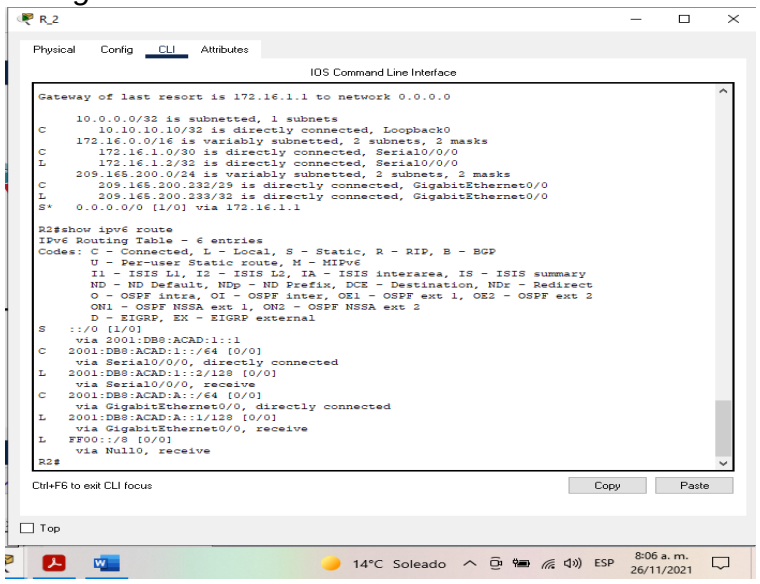
Tabla 9. Configuración de Router 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	*Router(config)#no ip domain-lookup*
Nombre del router	*Router(config)#hostname R2*
Contraseña de exec privilegiado cifrada	*R2(config)#enable secret class*
Contraseña de acceso a la consola	*R2(config)#line console 0* *R2(config-line)#password cisco* *R2(config-line)#login*
Contraseña de acceso Telnet	*R2(config-line)#line vty 0 15* *R2(config-line)#password cisco* *R2(config-line)#login*
Cifrar las contraseñas de texto no cifrado	*R2(config)#service password-encryption*
Habilitar el servidor HTTP	*Ip http server*
Mensaje MOTD	*R2(config)#banner motd "Se prohíbe el acceso no autorizado"*
Interfaz S0/0/0	*R2(config)#interface serial0/0/0* *R2(config-if)#ip address 172.16.1.2 255.255.255.252* *R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64* *R2(config-if)#description conexion R1* *R2(config-if)#clock rate 128000* *R2(config-if)#no shutdown*
Interfaz S0/0/1	*R2(config)#interface Serial0/0/1* *R2(config-if)#ip address 172.16.2.2 255.255.255.252* *R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64* *R2(config-if)#description conexion R3* *R2(config-if)#clock rate 128000* *R2(config-if)#no shutdown*

	R2(config-if)#exit
Interfaz G0/0 (simulación de Internet)	*R2(config)#interface gigabitEthernet0/0* *R2(config-if)#ip address 209.165.200.233 255.255.255.248* *R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64* *R2(config-if)#description conexion servidor* *R2(config-if)#no shutdown*
Interfaz loopback 0 (servidor web simulado)	R2(config)#interface loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description conexion servidor web R2(config-if)#exit
Ruta predeterminada	*R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0* *R2(config)#ipv6 route ::/0 g0/0*

Fuente: Autoría Propia

Figura 34. Configuración de R2



Fuente: Autoría Propia

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas

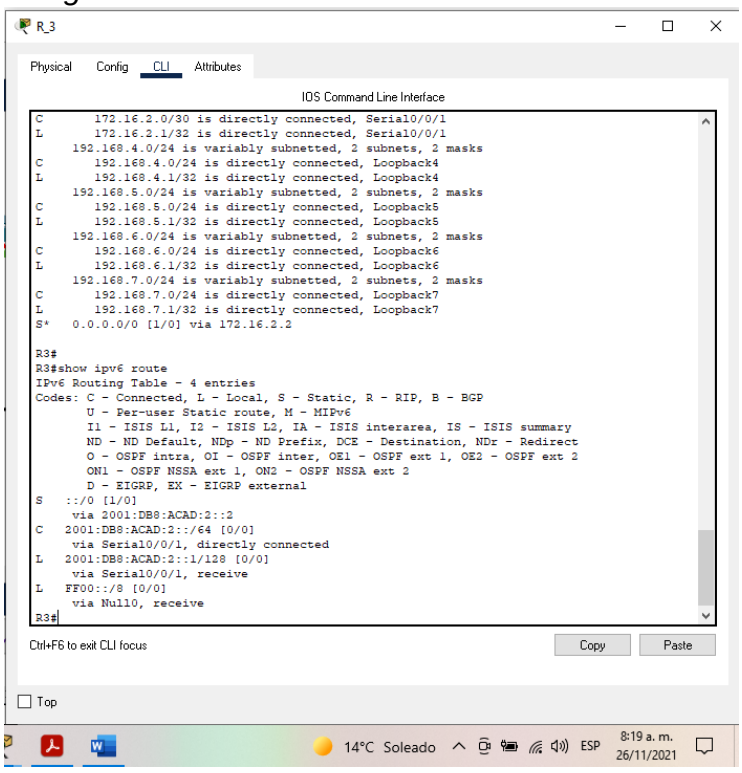
Tabla 10. Configuración de Router 3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	*Router(config)#no ip domain-lookup*
Nombre del router	*Router(config)#hostname R3*
Contraseña de exec privilegiado cifrada	*R3(config)#enable secret class*
Contraseña de acceso a la consola	*R3(config)#line console 0* *R3(config-line)#password cisco* *R3(config-line)#login*
Contraseña de acceso Telnet	*R3(config-line)#line vty 0 15* *R3(config-line)#password cisco* *R3(config-line)#login*
Cifrar las contraseñas de texto no cifrado	*R3(config)#service password-encryption*
Mensaje MOTD	*R3(config)#banner motd "Se prohíbe el acceso no autorizado"*
Interfaz S0/0/1	*R3(config)#interface serial0/2/1* *R3(config-if)#ip address 172.16.2.1 255.255.255.252* *R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64* *R3(config-if)#description conexion R2* *R3(config-if)#no shutdown*
Interfaz loopback 4	*R3(config)#interface loopback 4* *R3(config-if)#ip address 192.168.4.1 255.255.255.0* *R3(config-if)#description loopback 4* *R3(config-if)#exit*
Interfaz loopback 5	*R3(config)#interface loopback 5* *R3(config-if)#ip address 192.168.5.1 255.255.255.0* *R3(config-if)#description loopback 5*

	R3(config-if)#exit
Interfaz loopback 6	*R3(config)#interface loopback 6* *R3(config-if)#ip address 192.168.6.1 255.255.255.0* *R3(config-if)#description loopback 6* *R3(config-if)#exit*
Interfaz loopback 7	*R3(config)#interface loopback 7* *R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64* *R3(config-if)#description loopback 7* *R3(config-if)#exit*
Rutas predeterminadas	*R3(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2* *R3(config)# ipv6 route ::/0 2001:DB8:ACAD:2::2*

Fuente: Autoría Propia

Figura 35. Configuración de R3



Fuente: Autoría Propia

Paso 5: Configurar S1

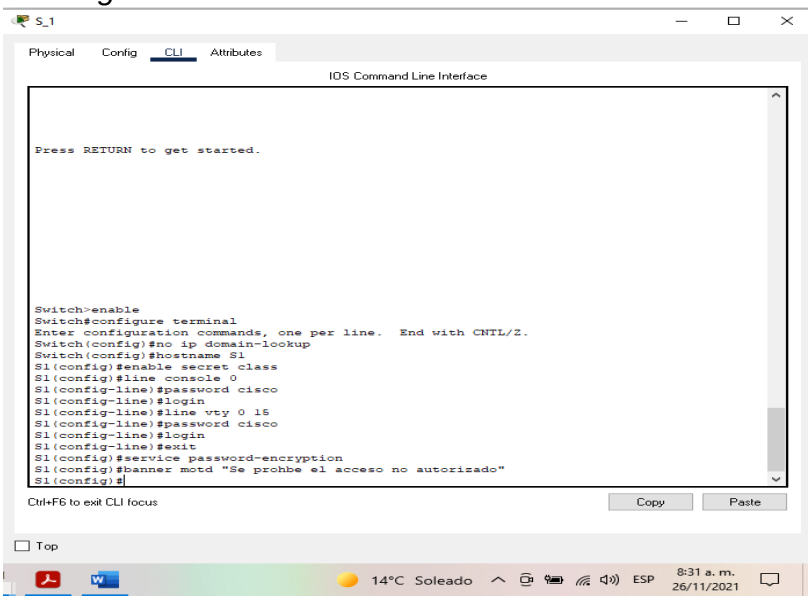
La configuración del S1 incluye las siguientes tareas:

Tabla 11. Configuración del Switch 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	*Switch(config)#no ip domain-lookup*
Nombre del switch	*Switch(config)#hostname S1*
Contraseña de exec privilegiado cifrada	*S1(config)#enable secret class*
Contraseña de acceso a la consola	*S1(config)#line console 0* *S1(config-line)#password cisco* *S1(config-line)#login*
Contraseña de acceso Telnet	*S1(config-line)#line vty 0 15* *S1(config-line)#password cisco* *S1(config-line)#login*
Cifrar las contraseñas de texto no cifrado	*S1(config)#service password-encryption*
Mensaje MOTD	*S1(config)#banner motd "Se prohíbe el acceso no autorizado".*

Fuente: Autoría Propia

Figura 36. Configuración de S1



Fuente: Autoría Propia

Paso 6: Configurar el S3

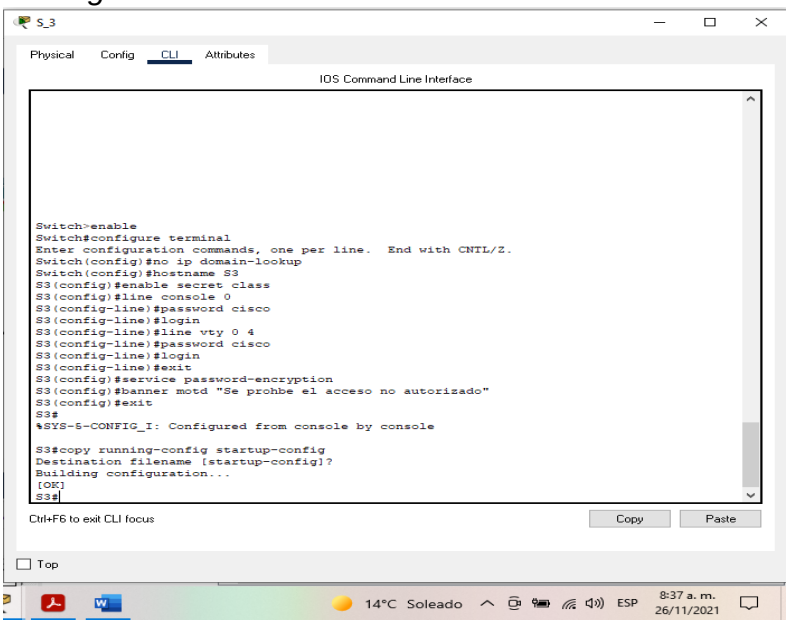
La configuración del S3 incluye las siguientes tareas:

Tabla 12. Configuración de Switch 3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	*Switch(config)#no ip domain-lookup*
Nombre del switch	*Switch(config)#hostname S3*
Contraseña de exec privilegiado cifrada	*S3(config)#enable secret class*
Contraseña de acceso a la consola	*S3(config)#line console 0* *S3(config-line)#password cisco* *S3(config-line)#login*
Contraseña de acceso Telnet	*S3(config-line)#line vty 0 15* *S3(config-line)#password cisco* *S3(config-line)#login*
Cifrar las contraseñas de texto no cifrado	*S3(config)#service password-encryption*
Mensaje MOTD	*S3(config)#banner motd "Se prohíbe el acceso no autorizado".*

Fuente: Autoría Propia

Figura 37. Configuración de S3



Fuente: Autoría Propia

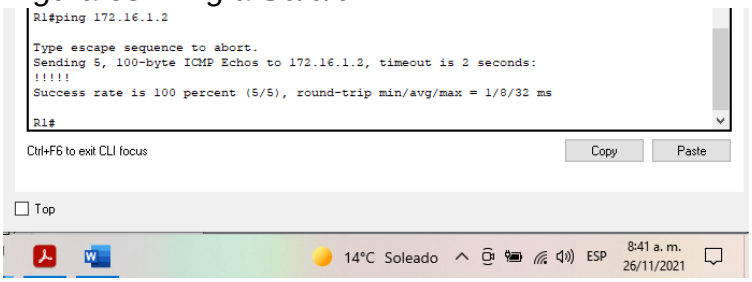
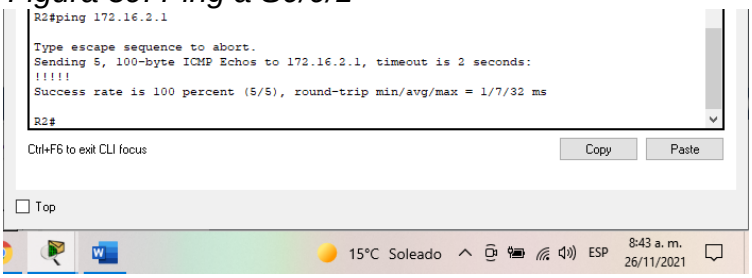
Paso 7: Verificar la conectividad de la red

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.

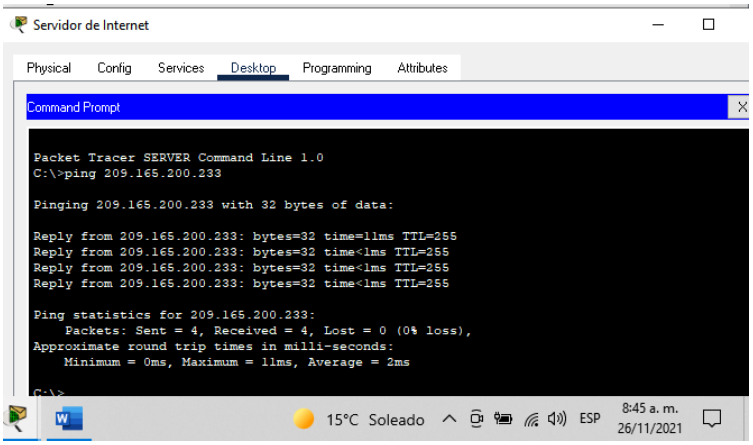
Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 13. Pruebas de conectividad

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Correcto *Figura 38. Ping a S0/0/0*  *Fuente: Autoría Propia*
R2	R3, S0/0/1	172.16.2.1	Correcto *Figura 39. Ping a S0/0/1*  *Fuente: Autoría Propia*

PC de Internet	Gateway predeterminado	209.165.200.233	Correcto

Figura 40. Ping al Gateway predeterminado

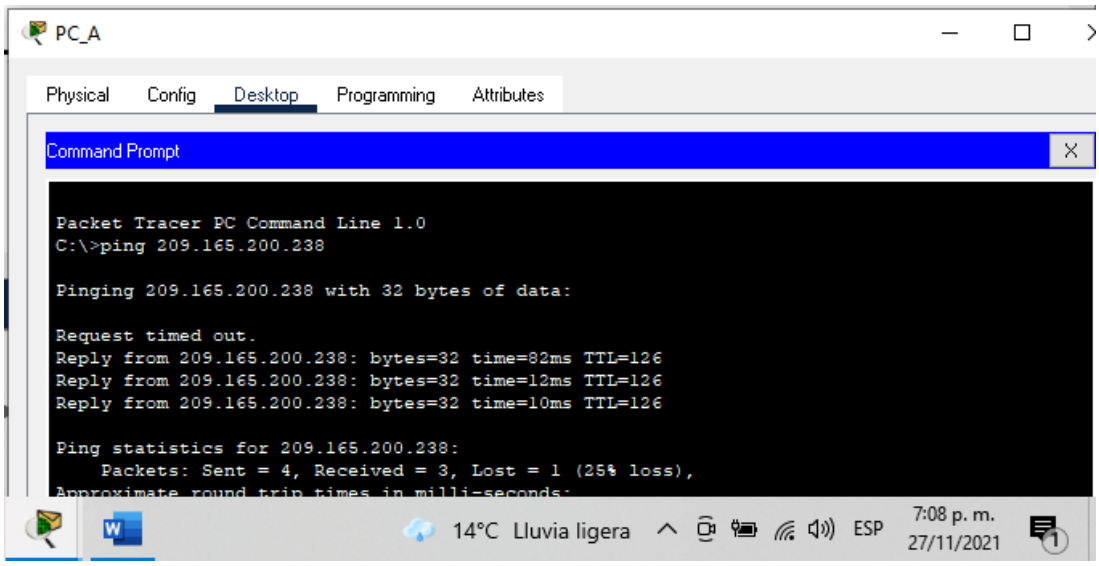


Fuente: Autoría Propia

Fuente: Autoría Propia

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

Figura 41. Ping al servidor web



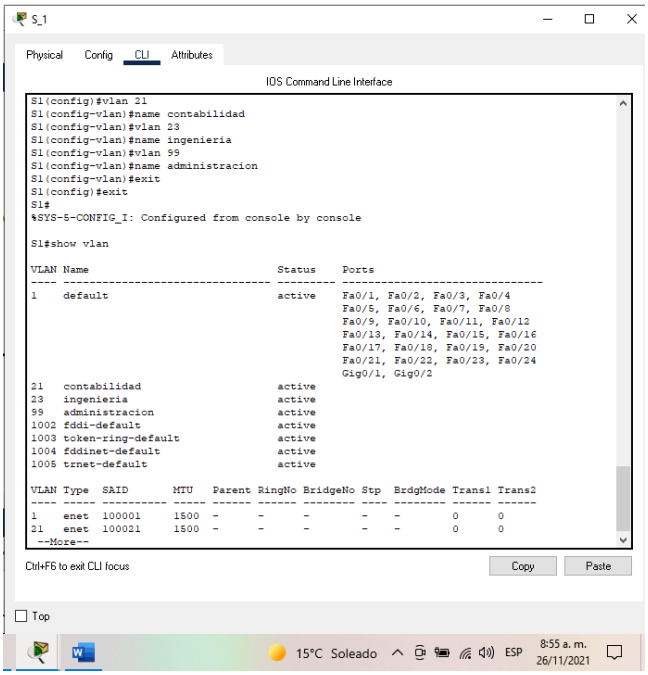
Fuente: Autoría Propia

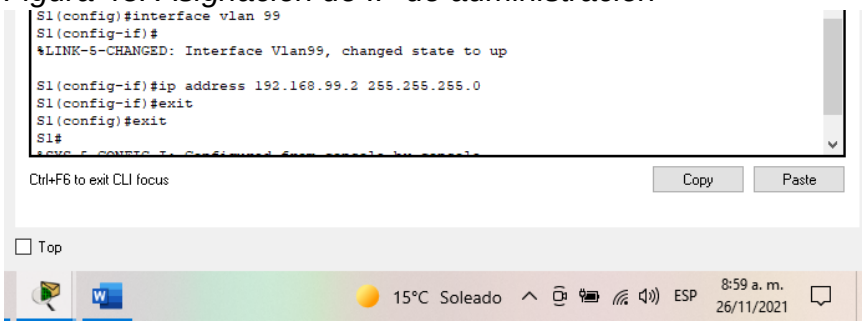
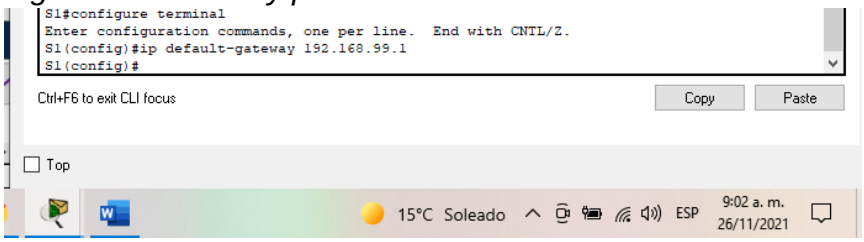
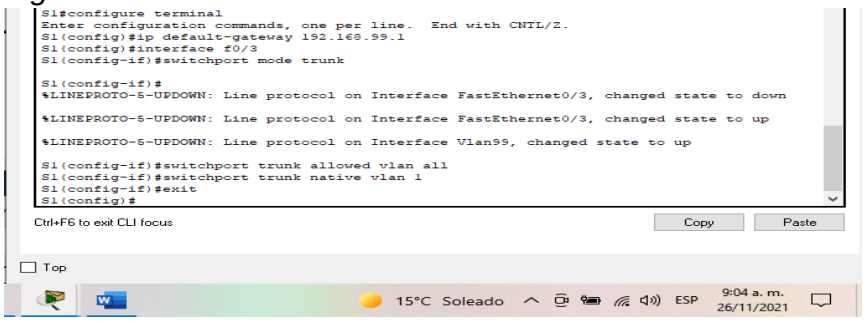
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN

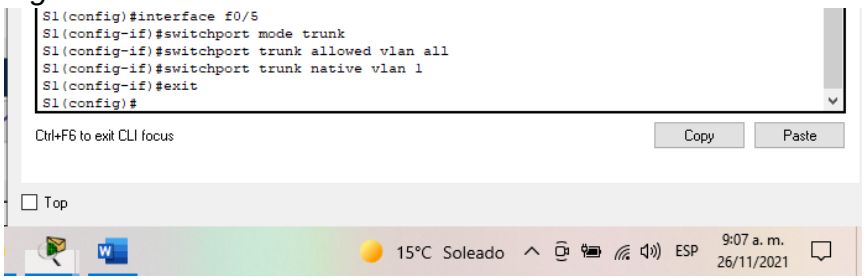
Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 14. configuración del Switch 1 para las vlan

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	*S1(config)#vlan 21* *S1(config-vlan)#name Contabilidad* *S1(config)#vlan 23* *S1(config-vlan)#name Ingenieria* *S1(config)#vlan 99* *S1(config-vlan)#name Administracion* *Figura 42. BD de VLAN 21*  *Fuente: Autoría Propia*

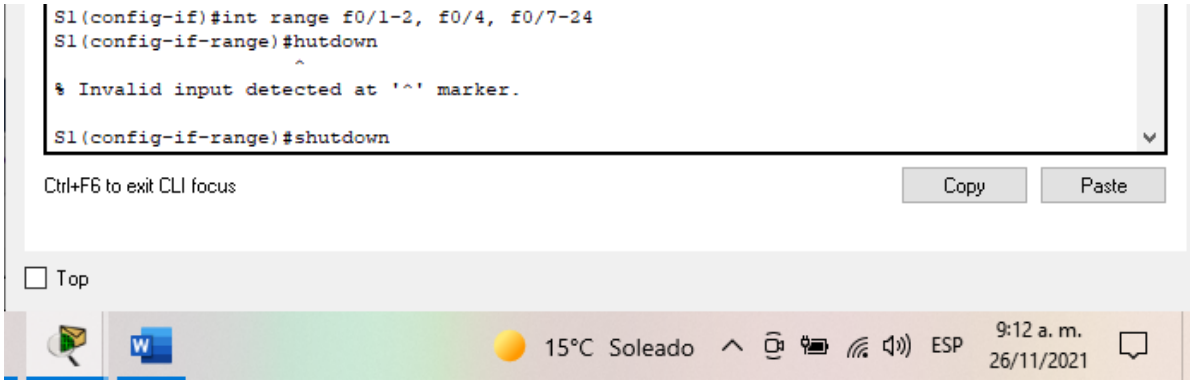
Asignar la dirección IP de administración.	*S1(config)#interface VLAN 99* *S1(config-if)#ip address 192.168.99.2 255.255.255.0* *S1(config-if)#exit* *Figura 43. Asignación de IP de administración*  *Fuente: Autoría Propia*
Asignar el gateway predeterminado	*S1(config)#ip default-gateway 192.168.99.1* *Figura 44. Gateway predeterminado*  *Fuente: Autoría Propia*
Forzar el enlace troncal en la interfaz F0/3	*S1(config)#interface f0/3* *S1(config-if)#switchport mode trunk* *S1(config-if)#switchport trunk allowed vlan all* *S1(config-if)#switchport trunk native vlan 1* *S1(config-if)#exit* *Figura 45. Troncalización del Puerto F0/3*  *Fuente: Autoría Propia*

Forzar el enlace troncal en la interfaz F0/5	*S1(config)#interface f0/5* *S1(config-if)#switchport mode trunk* *S1(config-if)#switchport trunk allowed vlan all* *S1(config-if)#switchport trunk native vlan 1* *S1(config-if)#exit* *Figura 46. Troncalización de la interfaz F0/5*  *Fuente: Autoría Propia*
Configurar el resto de los puertos como puertos de acceso	*S1(config)#int range f0/1-2, f0/4, f0/6-24, g0/1-2* *S1(config-if-range)#switchport mode access* *S1(config-if-range)#no shutdown* *Figura 47. Configuración de puertos de acceso*  *Fuente: Autoría Propia*
Asignar F0/6 a la VLAN 21	*S1(config)#int f0/6* *S1(config-if)#switchport access VLAN 21* *Figura 48. Asignación de F0/6 a VLAN 21*  *Fuente: Autoría Propia*

Apagar todos los puertos sin usar	*S1(config)#int range f0/1-2, f0/4, f0/7-24, g0/1-2* *S1(config-if-range)#shutdown*

Fuente: Autoría Propia

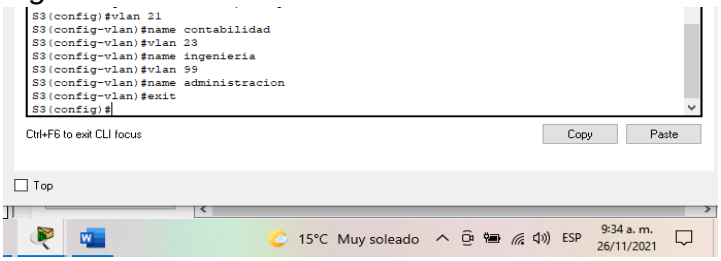
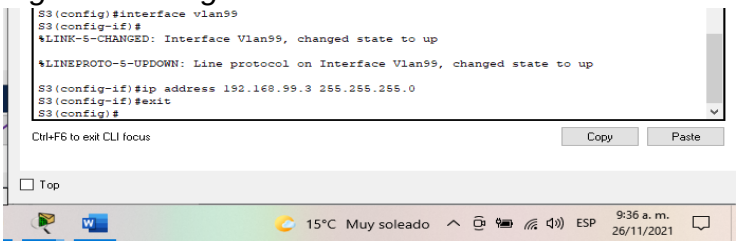
Figura 49. Desactivación de puertos sin uso en S1

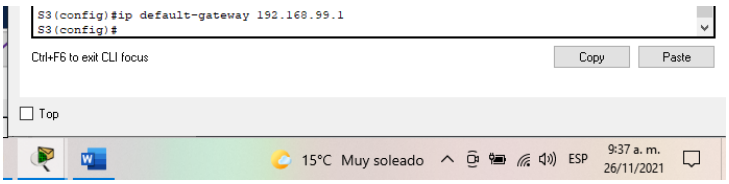
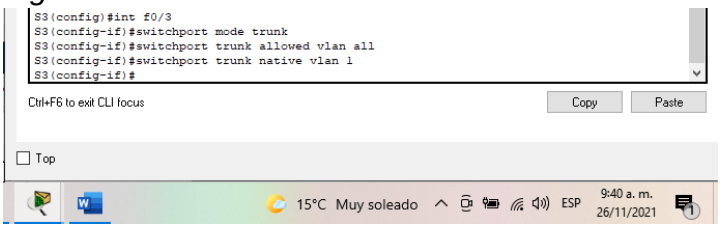
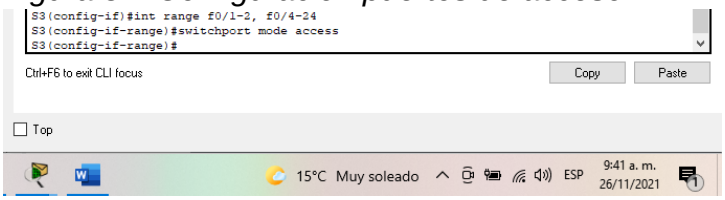
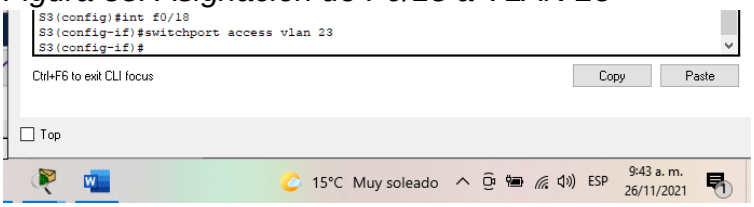


Fuente: Autoría Propia

Paso 2: Configurar el S3
La configuración del S3 incluye las siguientes tareas:

Tabla 15. configuración del Switch 3 para las vlan

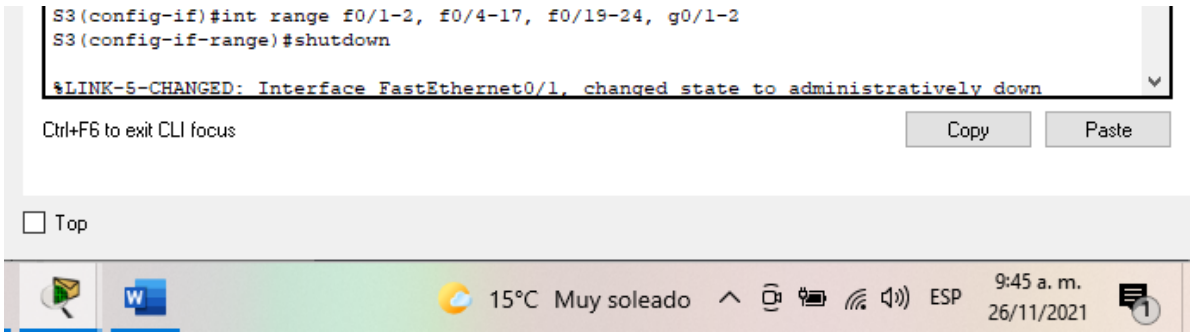
Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	*S3(config)#vlan 21* *S3(config-vlan)#name Contabilidad* *S3(config)#vlan 23* *S3(config-vlan)#name Ingenieria* *S3(config)#vlan 99* *S3(config-vlan)#name administracion* *Figura 50. BD de VLAN 23*  *Fuente: Autoría Propia*
Asignar la dirección IP de administración	*S3(config)#interface VLAN99* *S3(config-if)#ip address 192.168.99.3 255.255.255.0* *S3(config-if)#exit* *Figura 51. Asignación de IP de administración en S3*  *Fuente: Autoría Propia*

Asignar el gateway predeterminado.	*S3(config)#ip default-gateway 192.168.99.1* *Figura 52. Gateway predeterminado*  *Fuente: Autoría Propia*
Forzar el enlace troncal en la interfaz F0/3	*S3(config)#int f0/3* *S3(config-if)#switchport mode trunk* *S3(config-if)#switchport trunk allowed vlan all* *S3(config-if)#switchport trunk native vlan 1* *Figura 53. Troncalización del Puerto F0/3*  *Fuente: Autoría Propia*
Configurar el resto de los puertos como puertos de acceso	*S3(config)#int range f0/1-2, f0/4-24, g0/1-2* *S3(config-if-range)#switchport mode access* *Figura 54. Configuración puertos de acceso*  *Fuente: Autoría Propia*
Asignar F0/18 a la VLAN 23	*S3(config)#int f0/18* *S3(config-if)#switchport access VLAN 23* *Figura 55. Asignación de F0/18 a VLAN 23*  *Fuente: Autoría Propia*

Apagar todos los puertos sin usar	*S3(config)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2* *S3(config-if-range)#shutdown*

Fuente: Autoría Propia

Figura 56. Inhabilitación de los puertos sin usar en S3

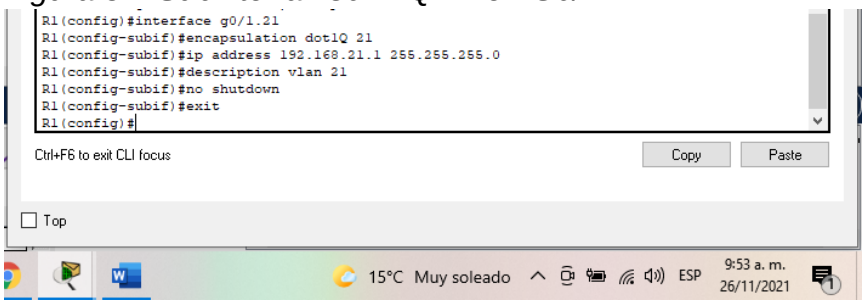
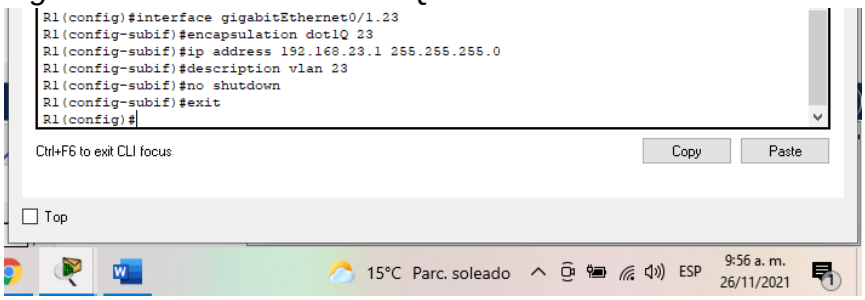


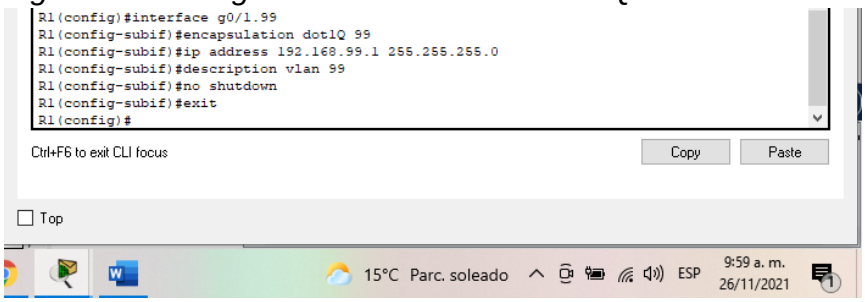
Fuente: Autoría Propia

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

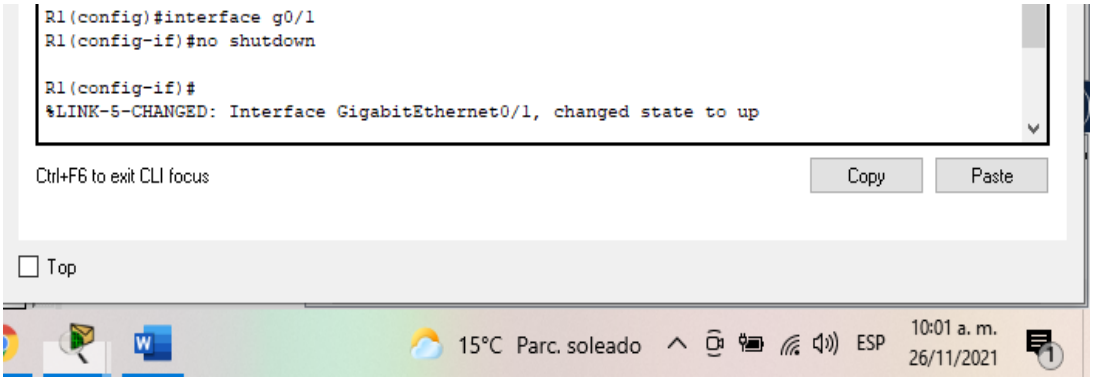
Tabla 16. configuración del R1 para las VLAN

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	*R1(config)#interface g0/1.21* *R1(config-subif)#encapsulation dot1Q 21* *R1(config-subif)#ip address 192.168.21.1 255.255.255.0* *R1(config-subif)#description vlan 21* *R1(config-subif)#no shutdown* *R1(config-subif)#exit* *Figura 57. Subinterfaz 802.1Q.21 en G0/1*  *Fuente: Autoría Propia*
Configurar la subinterfaz 802.1Q .23 en G0/1	*R1(config)#interface gigabitEthernet0/1.23* *R1(config-subif)#encapsulation dot1Q 23* *R1(config-subif)#ip address 192.168.23.1 255.255.255.0* *R1(config-subif)#description vlan 23* *R1(config-subif)#no shutdown* *R1(config-subif)#exit* *Figura 58. Subinterfaz 802.1Q.23 en G0/1*  *Fuente: Autoría Propia*

Configurar la subinterfaz 802.1Q .99 en G0/1	*R1(config)#interface g0/1.99* *R1(config-subif)#encapsulation dot1Q 99* *R1(config-subif)#ip address 192.168.99.1 255.255.255.0* *R1(config-subif)#description vlan 99* *R1(config-subif)#no shutdown* *R1(config-subif)#exit* *Figura 59. Configuración subinterfaz 802.1Q.99 en G0/1*  *Fuente: Autoría Propia*
Activar la interfaz G0/1	*R1(config)#interface g0/1* *R1(config-if)#no shutdown*

Fuente: Autoría Propia

Figura 60. Activación de la interfaz G0/1



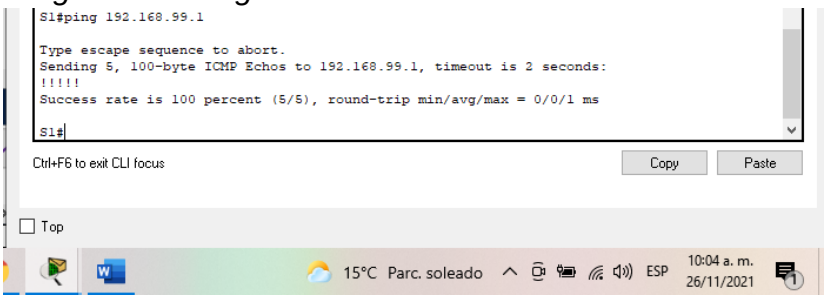
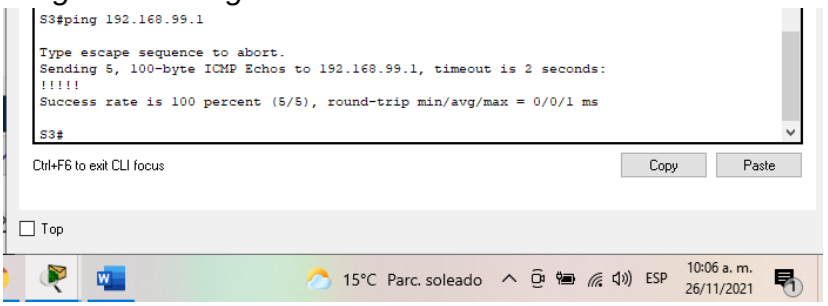
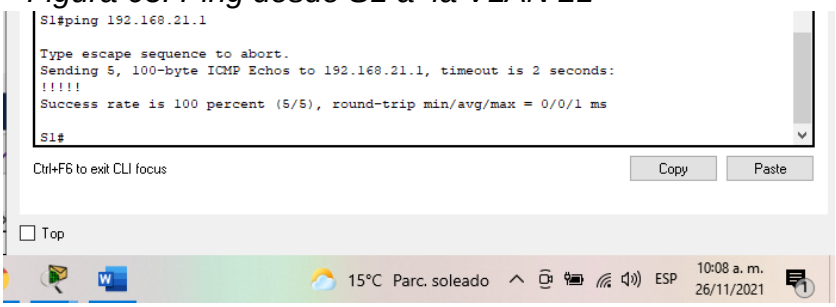
Fuente: Autoría Propia

Paso 4: Verificar la conectividad de la red

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

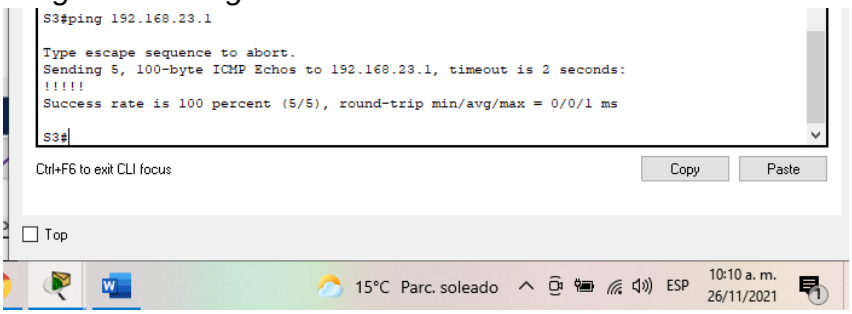
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla17. Resultados de las pruebas realizadas

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Positivo *Figura 61. Ping desde S1 a la VLAN 99*  *Fuente: Autoría Propia*
S3	R1, dirección VLAN 99	192.168.99.1	Positivo *Figura 62. Ping desde S3 a la VLAN 99*  *Fuente: Autoría Propia*
S1	R1, dirección VLAN 21	192.168.21.1	Positivo *Figura 63. Ping desde S1 a la VLAN 21*  *Fuente: Autoría Propia*

S3	R1, dirección VLAN 23	192.168.23.1	Positivo

Figura 64. Ping desde S3 a la VLAN 23



Fuente: Autoría Propia

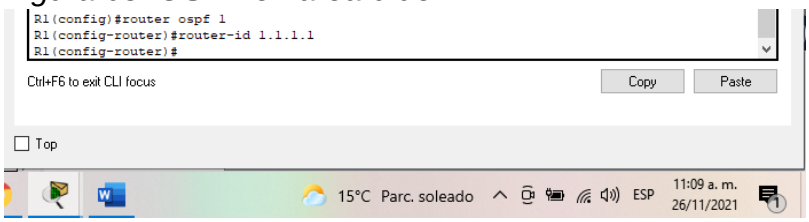
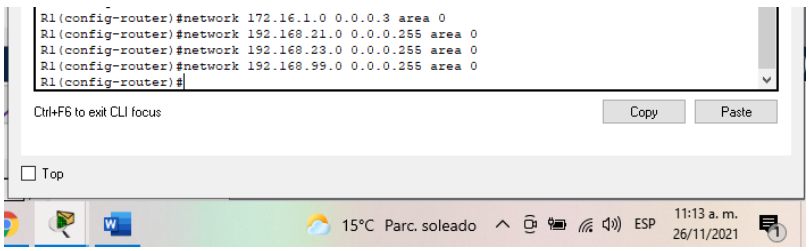
Fuente: Autoría Propia

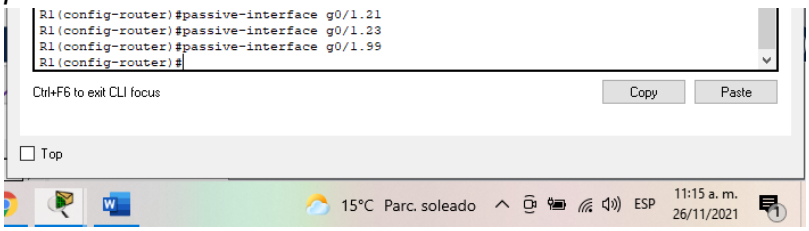
Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18. Configuración de OSPF en el Router 1

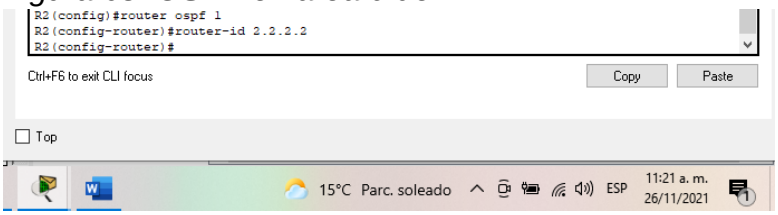
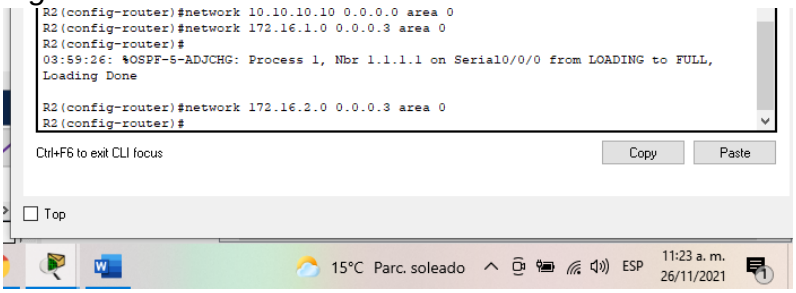
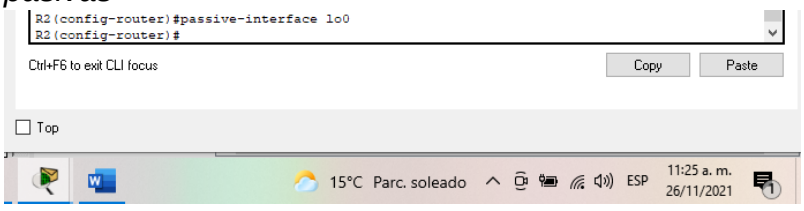
Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	*R1(config)#router ospf 1* *R1(config-router)#router-id 1.1.1.1* *Figura 65. OSPF en área 0 del R1*  *Fuente: Autoría Propia*
Anunciar las redes conectadas directamente	*R1(config-router)#network 172.16.1.0 0.0.0.3 area 0* *R1(config-router)#network 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* *Figura 66. Configuración de redes conectadas directamente*  *Fuente: Autoría Propia*

Establecer todas las interfaces LAN como pasivas	*R1(config-router)#passive-interface g0/1.21* *R1(config-router)#passive-interface g0/1.23* *R1(config-router)#passive-interface g0/1.99* *Figura 67. Establecimiento de interfaces LAN como pasivas*  *Fuente: Autoría Propia*
Desactive la sumarización automática	Solo aplica para RIP

Fuente: Autoría Propia

Paso 2: Configurar OSPF en el R2
La configuración del R2 incluye las siguientes tareas:

Tabla 19. Comandos para la configuración de OSPF en el Router 2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	*R2(config)#router ospf 1* *R2(config-router)#router-id 2.2.2.2* *Figura 68. OSPF en área 0 del R2*  *Fuente: Autoría Propia*
Anunciar las redes conectadas directamente	*R2(config-router)#network 10.10.10.10 0.0.0.0 area 0* *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* *Figura 69. Redes conectadas directamente*  *Fuente: Autoría Propia*
Establecer la interfaz LAN (loopback) como pasiva	*R2(config-router)#passive-interface lo0* *Figura 70. Establecimiento de interfaces LAN como pasivas*  *Fuente: Autoría Propia*

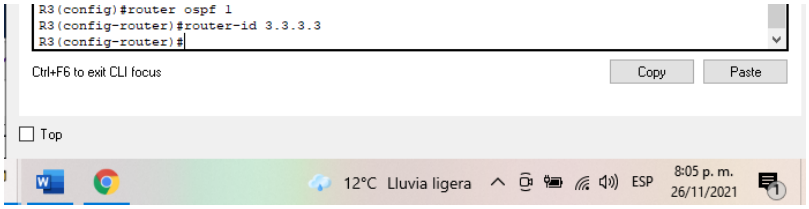
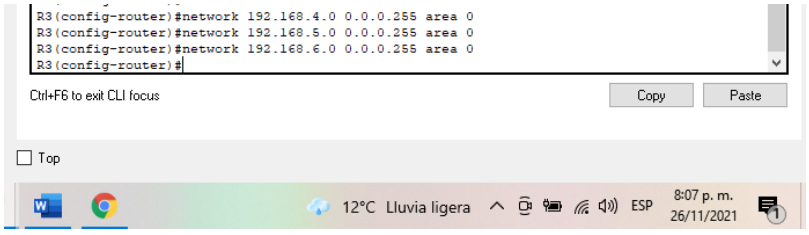
Desactive la sumarización automática.	Solo aplica para RIP

Fuente: Autoría Propia

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 20. Configuración de OSPF en el Router 3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	*R3(config)#router ospf 1* *R3(config-router)#router-id 3.3.3.3* *R3(config-router)#172.16.2.0 0.0.0.3 area 0* *Figura 71. OSPF en área 0 del R3*  *Fuente: Autoría Propia*
Anunciar redes IPv4 conectadas directamente	*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* *Figura 72. Configuración de redes conectadas directamente*  *Fuente: Autoría Propia*

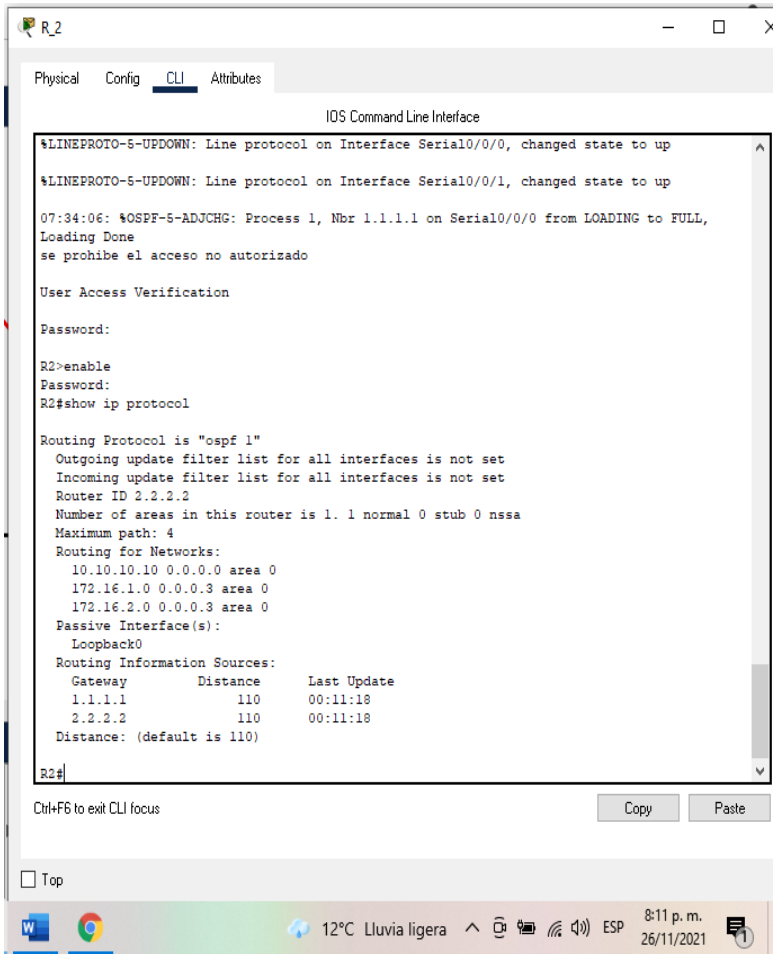
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	*R3(config-router)#passive-interface lo4* *R3(config-router)#passive-interface lo5* *R3(config-router)#passive-interface lo6* *R3(config-router)#passive-interface lo7*
Desactive la sumarización automática.	Solo aplica para RIP

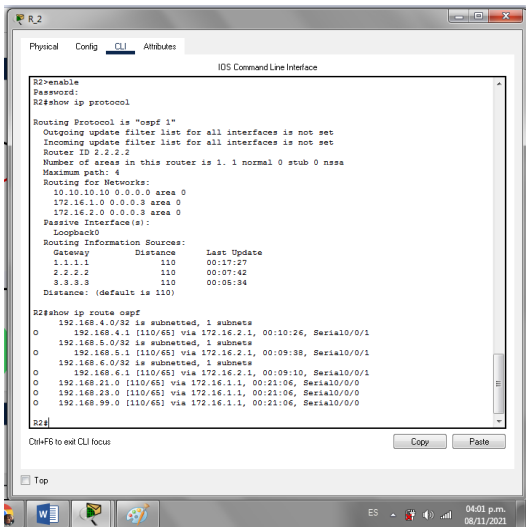
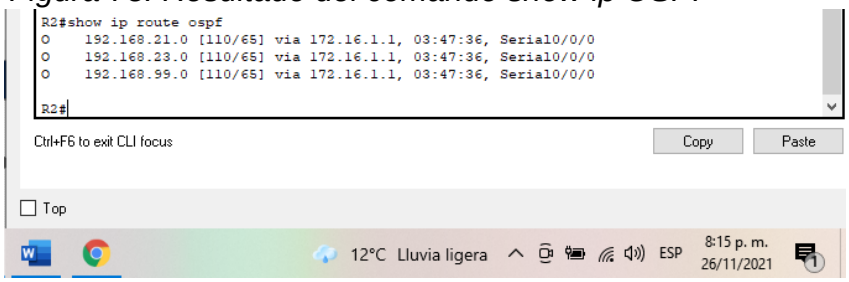
Fuente: Autoría Propia

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. Verificación de configuración 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?	*Figura 73. Comando show ip protocol*  *Fuente: Autoría Propia*

¿Qué comando muestra solo las rutas OSPF?	Show ip route ospf *Figura 74 Resultado del comando show ip route OSPF*  *Fuente: Autoría Propia*
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Show ip ospf *Figura 75. Resultado del comando show ip OSPF*  *Fuente: Autoría Propia*

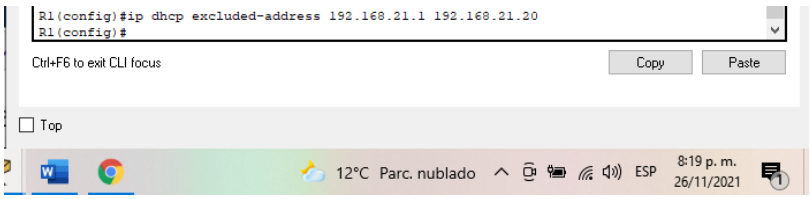
Fuente: Autoría Propia

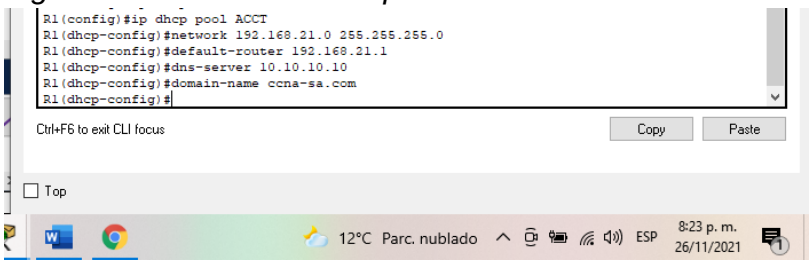
Parte 5: Implementar DHCP y NAT para IPv4

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22. DHCP para las VLAN 23 y 24

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* *Figura 76. Reserva para la configuración de VLAN estática 21*  *Fuente: Autoría Propia*
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* *Figura 77. Reserva para la configuración de VLAN estáticas 23*  *Fuente: Autoría Propia*

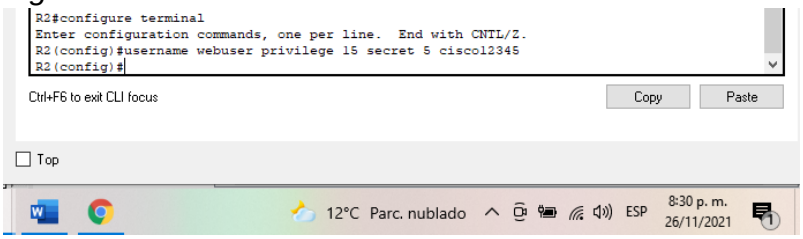
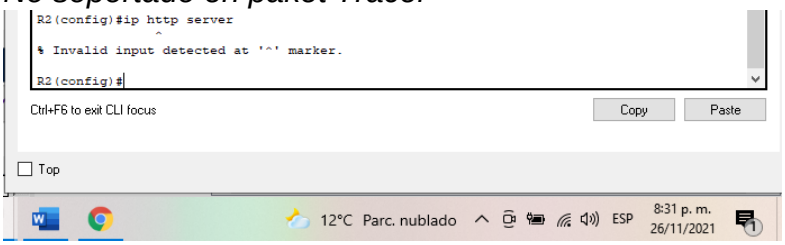
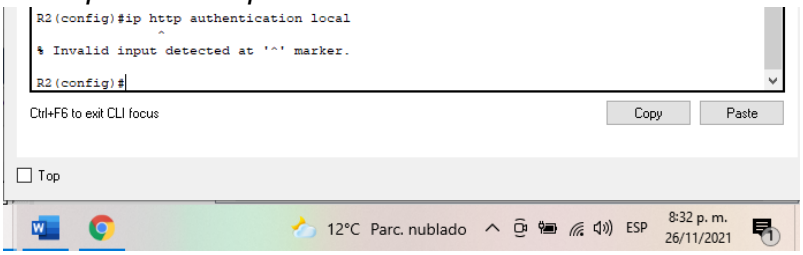
Crear un pool de DHCP para la VLAN 21.	*R1(config)#ip dhcp pool ACCT* *R1(dhcp-config)#network 192.168.21.0 255.255.255.0* *R1(dhcp-config)#default-router 192.168.21.1* *R1(dhcp-config)#dns-server 10.10.10.10* *R1(dhcp-config)#domain-name ccna-sa.com* *Figura 78. Creación de un pool de DHCP en VLAN 21*  *Fuente: Autoría Propia*
Crear un pool de DHCP para la VLAN 23	*R1(config)#ip dhcp pool ENGNR* *R1(dhcp-config)#network 192.168.23.0 255.255.255.0* *R1(dhcp-config)#default-router 192.168.23.1* *R1(dhcp-config)#dns-server 10.10.10.10* *R1(dhcp-config)#domain-name ccna-sa.com* *Figura 79. Creación de un pool de DHCP en VLAN 23*  *Fuente: Autoría Propia*

Fuente: Autoría Propia

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

La configuración del R2 incluye las siguientes tareas:

Tabla 23. Configuración de NAT estática y dinámica en el Router 2

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)#username webuser privilege 15 secret cisco12345 *Figura 80. BD local con cuenta webuser*  *Fuente: Autoría Propia*
Habilitar el servicio del servidor HTTP	*R2(config)#ip http server* *Figura 81. Servicio de servidor HTTP* *No soportado en paket Tracer*  *Fuente: Autoría Propia*
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	*R2(config)#ip http authentication local* *Figura 82 HTTP para la autenticación en la BD local* *No soportado en paket Tracer*  *Fuente: Autoría Propia*

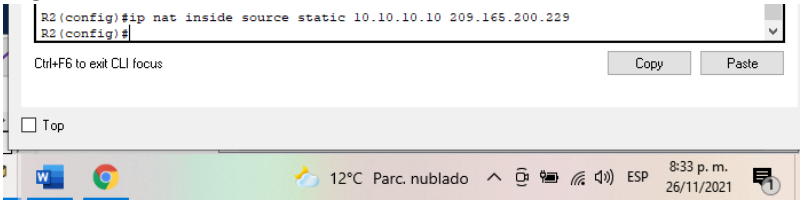
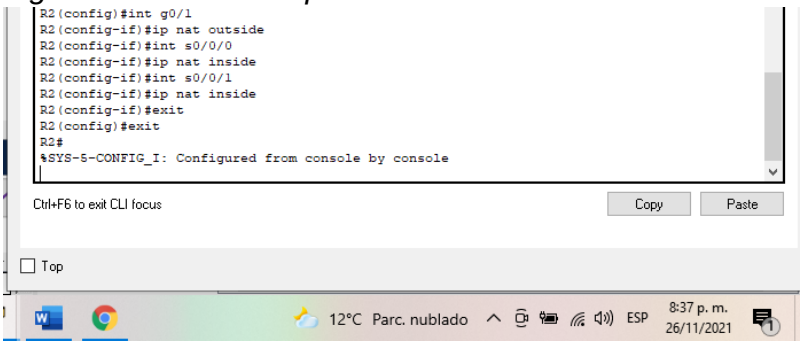
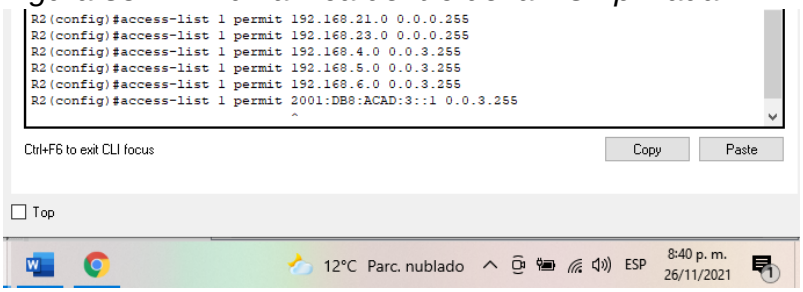
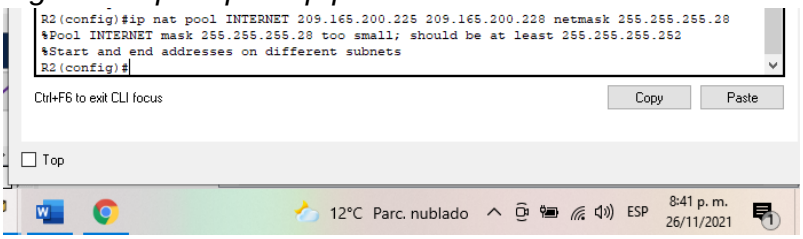
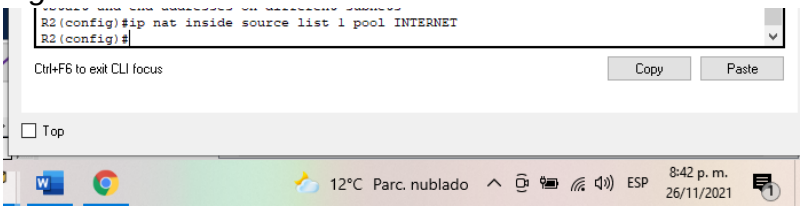
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.229 *R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229* *Figura 83. NAT estática en el servidor web*  *Fuente: Autoría Propia*
Asignar la interfaz interna y externa para la NAT estática	*R2(config)#int g0/1* *R2(config)#ip nat outside* *R2(config)#int s0/0/0* *R2(config)#ip nat inside* *R2(config)#int s0/0/1* *R2(config)#ip nat inside* *R2(config)#exit* *Figura 84. Interfaces para la NAT estática*  *Fuente: Autoría Propia*
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)#access-list 1 permit 192.168.4.0 0.0.3.255* *R2(config)#access-list 1 permit 2001:DB8:ACAD:3::1 0.0.3.255*

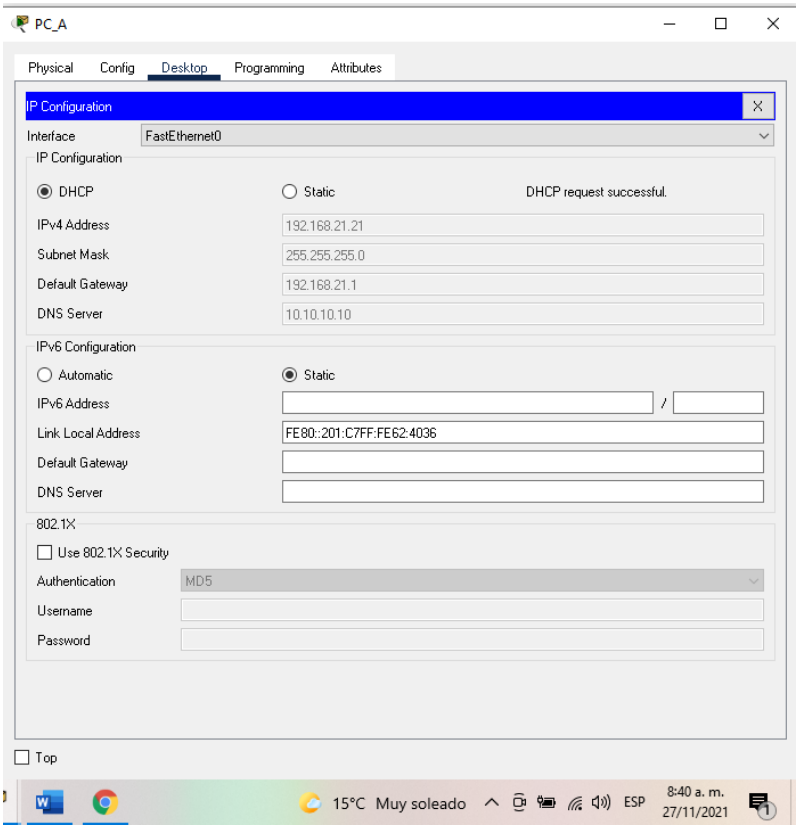
	Figura 85. NAT dinámica dentro de la ACL privada  *Fuente: Autoría Propia*
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228 *R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.252* *Figura 86. pool para ip publica utilizable*  *Fuente: Autoría Propia*
Definir la traducción de NAT dinámica	*R2(config)#ip nat inside source list 1 pool INTERNET* *Figura 87. Traducción de NAT dinámica*  *Fuente: Autoría Propia*

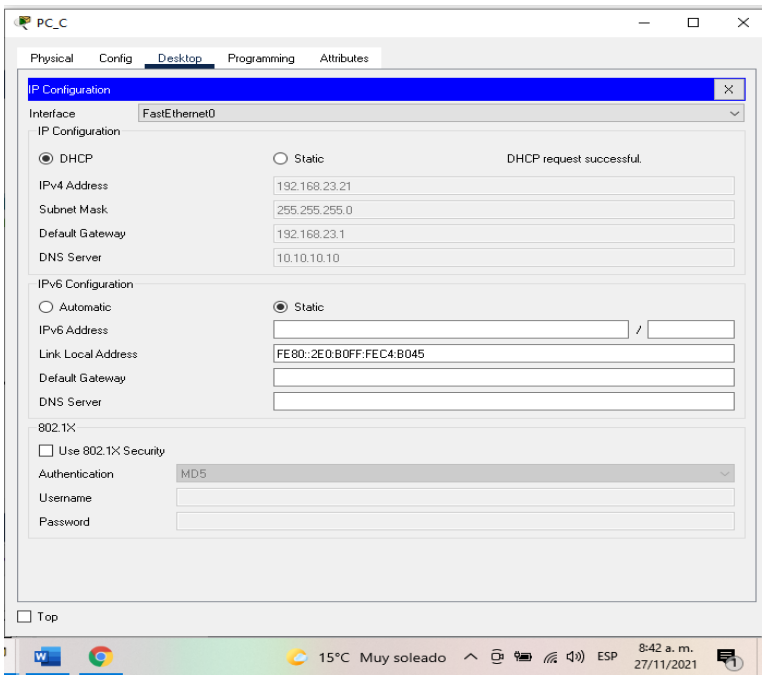
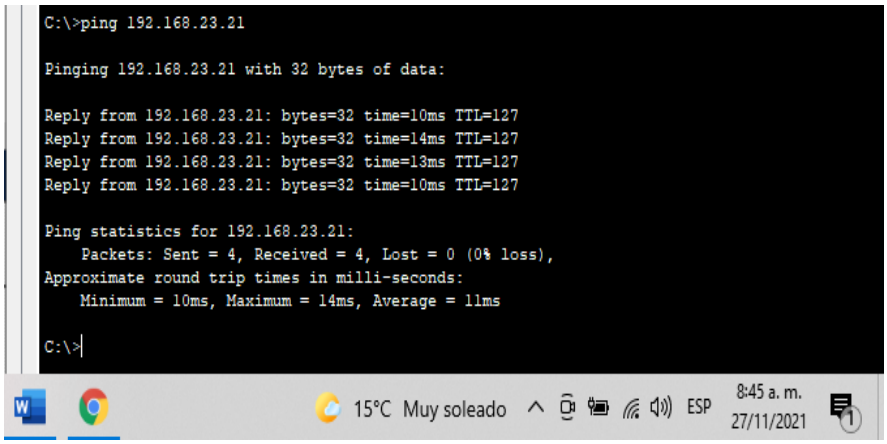
Fuente: Autoría Propia

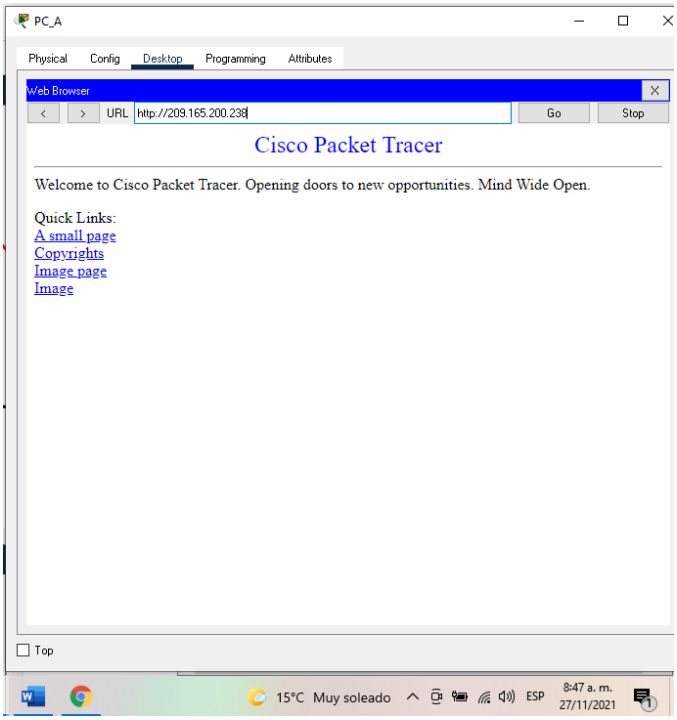
Paso 3: Resultados DHCP y NAT estática

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 24. Verificación de DHCP y NAT

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	*Figura 88. DHCP para PC_A*  *Fuente: Autoría Propia*

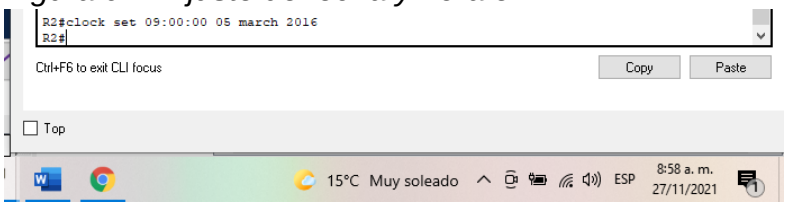
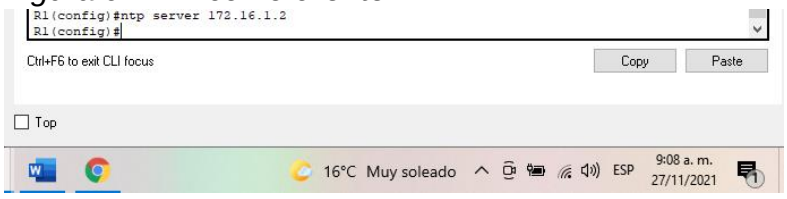
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	*Figura89. DHCP para PC_C*  *Fuente: Autoría Propia*
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	*Figura 90. Ping de PC_ A a PC_C*  *Fuente: Autoría Propia*

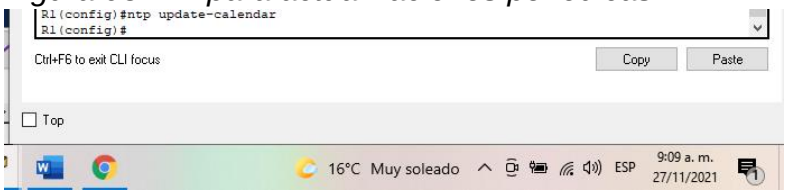
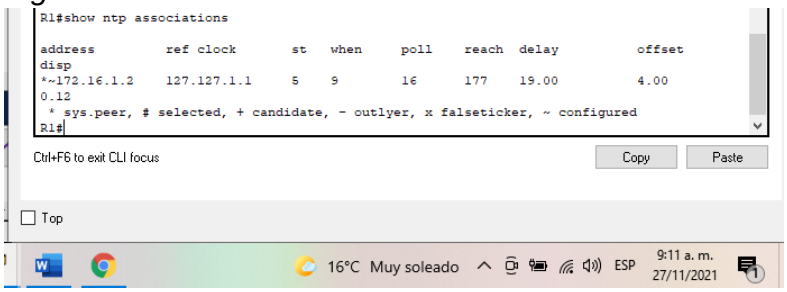
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.238) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	*Figura 91. Conexión de PC_A a internet*  *Fuente: Autoría Propia*

Fuente: Autoría Propia

Parte 6: Configurar NTP

Tabla 25. Configuración de NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	*R2#clock set 09:00:00 05 march 2016* *Figura 92.. Ajuste de fecha y hora en R2*  *Fuente: Autoría Propia*
Configure R2 como un maestro NTP.	*R2(config)#ntp master 5* *Figura 93.NTP como maestro*  *Fuente: Autoría Propia*
Configurar R1 como un cliente NTP.	*R1(config)#ntp server 172.16.1.2* *Figura 94. R1 como cliente NTP*  *Fuente: Autoría Propia*
Configure R1 para actualizaciones de	*R1(config)#ntp update-calendar*

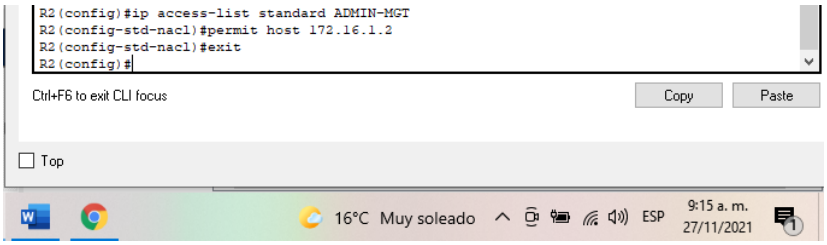
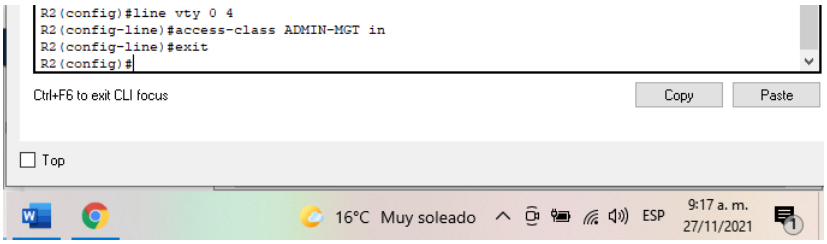
calendario periódicas con hora NTP.	*Figura 95. R1 para actualizaciones periódicas*  *Fuente: Autoría Propia*
Verifique la configuración de NTP en R1.	*R1#show ntp associations* *Figura 96. Verificación de NTP en R1*  *Fuente: Autoría Propia*

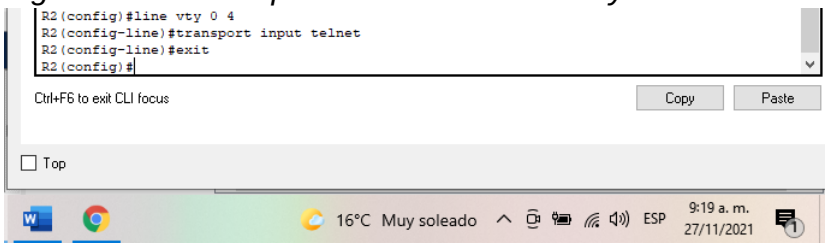
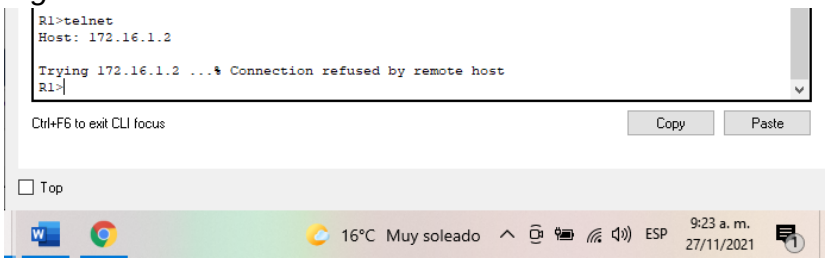
Fuente: Autoría Propia

Parte 7: Configurar y verificar las listas de control de acceso (ACL)

Restringir el acceso a las líneas VTY en el R2

Tabla 26. Verificación Listas de control

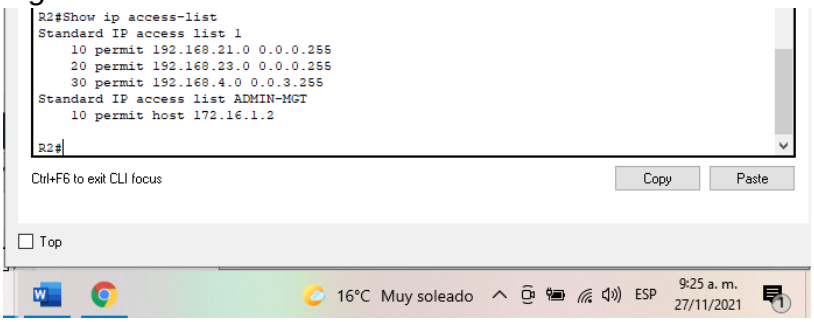
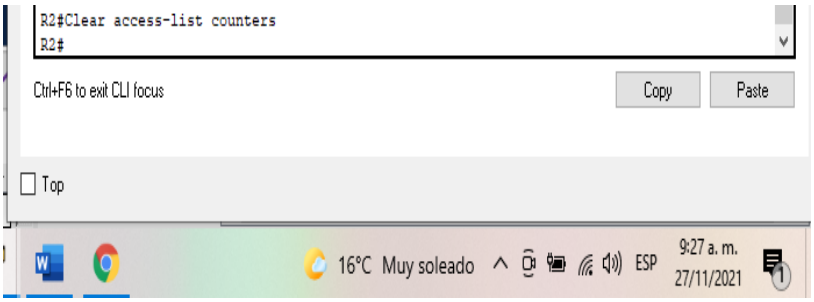
Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	*R2(config)#ip access-list standard ADMIN-MGT* *R2(config-std-nacl)#permit host 172.16.1.2* *R2(config-std-nacl)#exit* *Figura 97. Conexión a telnet de R1 a R2*  *Fuente: Autoría Propia*
Aplicar la ACL con nombre a las líneas VTY	*R2(config)#line vty 0 4* *R2(config-line)#access-class ADMIN-MGT in* *R2(config-line)#exit* *Figura 98. ACL con nombre a las líneas VTY*  *Fuente: Autoría Propia*

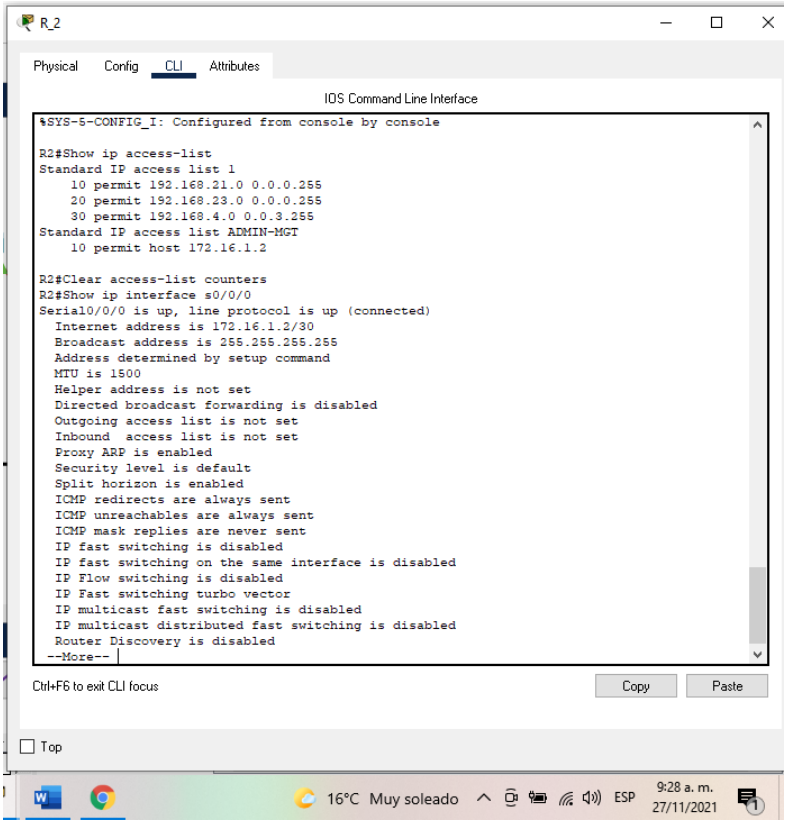
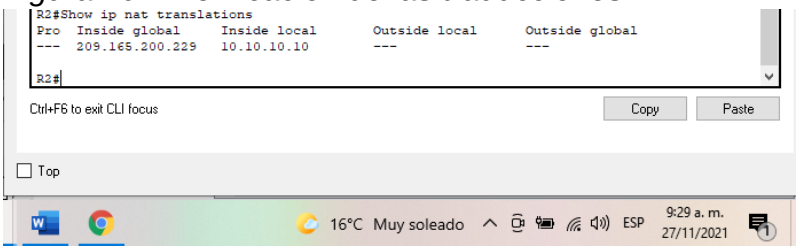
Permitir acceso por Telnet a las líneas de VTY	*R2(config)#line vty 0 4* *R2(config-line)#transport input telnet* *R2(config-line)#exit* *Figura 99. Acceso por telnet a las líneas vty*  *Fuente: Autoría Propia*
Verificar que la ACL funcione como se espera	*R1>telnet* *Host: 172.16.1.2* *Figura100. Verificación de ACL*  *Fuente: Autoría Propia*

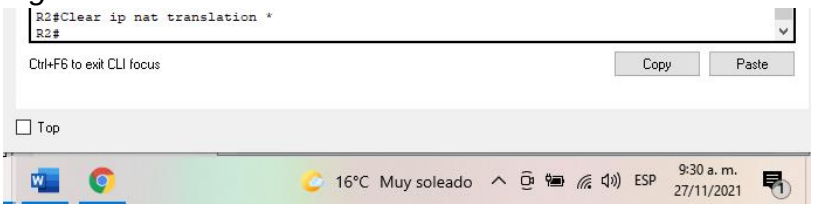
Fuente: Autoría Propia

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

Tabla 27. Comandos 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* *Figura101. Coincidencias de ACL en R2*  *Fuente: Autoría Propia*
Restablecer los contadores de una lista de acceso	*R2#Clear access-list counters* *Figura102. Restablecimiento de contadores de una lista de acceso*  *Fuente: Autoría Propia*

¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	*R2#Show ip interface s0/0/0* *Figura103. ACL a las interfaces y las direcciones donde aplica*  *Fuente: Autoría Propia*
¿Con qué comando se muestran las traducciones NAT?	*R2#Show ip nat translations* 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. *Figura 104. Verificación de las traducciones NAT*  *Fuente: Autoría Propia*

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	*R2#Clear ip nat translation ** *Figura 105. Eliminación de traducciones NAT dinámicas*  *Fuente: Autoría Propia*

Fuente: Autoría Propia

CONCLUSIONES

Se realizan las configuraciones solicitadas y laboratorios de acceso para establecer los escenarios propuestos, para realizar un análisis sobre el comportamiento de los diferentes protocolos y métodos de enrutamiento.

Se identifican las herramientas de supervisión y los protocolos de administración de red disponibles en el IOS para resolver problemas de las redes de datos

Se configuran satisfactoriamente los protocolos de enrutamiento solicitados en el escenario 2, de acuerdo con lo planteado por la guía de actividades y las indicaciones del tutor.

Se resuelven correctamente los problemas de conectividad, asignado seguridad a los dispositivos a través de línea de comandos sore la consola de los dispositivos de la red.

Se logra desarrollar satisfactoriamente cada uno de los requerimientos solicitados por la guía, con el fin de dar soluciones en un entorno real. Permitiendo las buenas prácticas enseñadas.

BIBLIOGRÁFIA

CISCO Networking. (2021). CCNA Routing and Switching: Introducción a las redes (Introduction to Networks). Recuperado de: https://contenthub.netacad.com/legacy/CCNA/ITN/6.0/es/index.html#8.1.1.3

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

López, María (2021). CIPAS Subneting_Diplomado.Capitulo8: División de redes ip en subredes. Recuperado de: https://drive.google.com/file/d/1CmNJEoygio-FsfLe7AG55MbMCFRR27ip/view