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

KEVEN STEVE VEGA VALENCIA

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

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

KEVEN STEVE VEGA VALENCIA

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

TUTOR:
MARIA ALEJANDRA LOPEZ

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

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Villavicencio, 28 de noviembre de 2021

AGRADECIMIENTOS

Agradezco a mis padres y a mi familia por apoyarme, por su sacrificio y creen en mí y a Dios por permitir seguir adelante pese a las adversidades a mis compañeros de estudio y profesores que guiaron mi formación como profesional.

TABLA DE CONTENIDO

AGRADECIMIENTOS 4

CONTENIDO 5

LISTA DE TABLAS 6

LISTA DE IMAGENES 7

GLOSARIO 8

RESUMEN 9

ABSTRACT 9

INTRODUCCIÓN 10

DESARROLLO 11

1. Escenario 1 11
2. Escenario 2 24

CONCLUSIONES 54

BIBLIOGRÁFIA 55

LISTA DE TABLAS

Escenario 1
Tabla 1. Tabla de Direccionamiento 12
Tabla 2. Tabla de Subredes 13
Tabla 3. Tabla de Configuración R1 14
Tabla 4. Tabla de Configuración S1 17
Tabla 5. PC-A Network Configuración 22
Tabla 6. PC-B Network Configuración 23

Escenario 2
Tabla 7. Inicialización de dispositivos switches y routers 25
Tabla 8. Configuracion Servidor de Internet 26
Tabla 9. Configuracion Parámetros básicos en R1 26
Tabla 10. Configuracion Parámetros básicos en R2 29
Tabla 11. Configuracion Parámetros básicos en R3 32
Tabla 12. Configuracion Parámetros básicos en S1 35
Tabla 13. Configuracion Parámetros básicos en S3 36
Tabla 14. Verificación de Red 38
Tabla 15. Configuracion de las Vlan y el routing entre VLAN en S1 38
Tabla 16. Configuracion de las Vlan y el routing entre VLAN en S3 42
Tabla 17. Configuracion Subinterfaces G0/1 en R1 43
Tabla 18. Verificación de la red 45
Tabla 19. Configuracion protocolo OSPF en R1 46
Tabla 20. Configuracion protocolo OSPF en R2 47
Tabla 21. Configuracion protocolo OSPF en R3 48
Tabla 22. verificación protocolo OSPF 48
Tabla 23. Configuracion DHCP en R1 50
Tabla 24. Configuracion NAT estática y dinámica en R2 52
Tabla 25. Verificación protocolo DHCP y la NAT estática 53
Tabla 26. Configuracion protocolo Network Time Protocol en R2 54
Tabla 27. Configuracion listas de control de acceso 55
Tabla 28. Verificación ACL 56

LISTA DE FIGURAS

Escenario 1
Figura 1. Escenario 1 11
Figura 2. Simulación de escenario 1 12
Figura 3. Aplicando código R1 16
Figura 4. Aplicando código R1 16
Figura 5. Aplicando código R1 17
Figura 6. Aplicando código S1 20
Figura 7. Aplicando código S1 20
Figura 8. Aplicando código S1 21
Figura 9. Network Configuration PC-A 22
Figura 10. Network Configuration PC-A 23
Figura 11. Show Ip route en R1 24

Escenario 2
Figura 12. Escenario 2 25
Figura 13. Aplicando código en R1 29
Figura 14. Aplicando código en R2 32
Figura 15. Show run en R3 34
Figura 16. Aplicando Código en S1 36
Figura 17. Aplicando Código en S3 37
Figura 18. show interface trunk en S1 41
Figura 19. Aplicando Código en S3 43
Figura 20. Show ip interface brief en R1 45
Figura 21. show ip ospf interface en R3 49
Figura 22. show ip route ospf en R1 49
Figura 23. show ip protocols en R2 50
Figura 24. Aplicando código en R3 52
Figura 25. Verificación de NTP 55
Figura 26. show access-lists en R2 57
Figura 27. show ip nat translations en R2 58
Figura 28. show ip route en R1 59
Figura 29. show ip route en R2 59

GLOSARIO

CISCO IOS: Es el Sistema operativo Internetwork utilizado en los dispositivos red Cisco
intermedios como routers y switches.

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

DIRECCION DE RED: Un número decimal con puntos que representa una única dirección IP

ROUTING: El proceso de envío de paquetes a hosts en una red remota.

SUBNETTING: Esta técnica se usa para dividir una red extensa en pequeñas redes o subredes con el fin de hacerla más manejable administrativamente.

SVI: Interfaz lógica que se utiliza para administrar un switch de manera remota a través de una red IPv4,

RESUMEN

En el desarrollo del presente trabajo se abordan dos escenarios que se resolvieron con las temáticas abordadas en el diplomado de profundización de CNNA: las temáticas abordadas son direccionamiento IPV4 e IPV6, VLANS, ACL, OSPF, NAT entre otros protocolos donde de igual forma se resalta la importancia de configurar los parámetros básicos de los dispositivos intermediarios switch y routers estableciendo contraseñas cifradas y deshabilitando las interfaces que no están en funcionamiento, estableciendo puertos troncales y asignando las Vlans en las interfaces respectivas finalmente se realiza la verificación del funcionamiento de la red y las configuraciones establecidas.

Palabras claves: CISCO, CNNA, IPV4, IPV6, VLANS.

ABSTRACT

In the development of this work, two scenarios are addressed that were resolved with the issues addressed in the CNNA deepening diploma: the issues addressed are IPV4 and IPV6 addressing, VLANS, ACL, OSPF, NAT among other protocols where in the same way it is highlighted the importance of configuring the basic parameters of the intermediate switch devices and routers, establishing encrypted passwords and disabling the interfaces that are not in operation, establishing trunk ports and assigning the Vlans in the respective interfaces, finally, the verification of the operation of the network and the established settings.

Keywords: CISCO, CNNA, IPV4, IPV6, VLANS.

INTRODUCCION

En el primer escenario se desarrolla un esquema de direccionamiento, se realiza la tabla de direccionamiento y la tabla de subredes para la conexión de dos redes LAN 1 de 100 y LAN 2 de 50 host respectivamente se configuran los dispositivos intermediarios Switch 1 y Router 1 para su segura administración.

En los dispositivos R1 y S1 mediante conexión de consola se inició la configuración se les denomino un nombre, se restringe el acceso al modo Exec usuario y Exec privilegiado asignando contraseñas y encriptándolas, así mismo se configura un mensaje de advertencia para usuarios no autorizados se abstengan del ingreso.

Se realiza la configuración de las interfaces Gigabit Ethernet 0/0/0 y Gigabit Ethernet 0/0/1 del R1 con el fin conectar el switch y la PC-B se configuran las direcciones IP, la máscara de subred y descripciones en cada interfaz para determinar a qué dispositivo va conectada.

El desarrollo del segundo escenario es mas complejo inicialmente se configuran los parámetros básicos de seguridad en los dispositivos R1, R2, R3, S1 y S3 posterior se configura el direccionamiento IPV4 e IPV6, se crean y asignan las vlan para que permita el routing, seguidamente se configura el protocolo de routing dinámico OSPF en los routers, 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, de igual forma se documentan los comandos que se ejecutaron para realizar las configuraciones antes mencionadas.

DESARROLLO

Figura 1. Escenario 1

Fuente: Elaboración propia

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.

Objetivos

Parte 1: Construir en el simulador la Red
Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2
Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta.
Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1
Parte 4: Configurar los hosts y verificar la conectividad entre los equipos

Aspectos básicos/situación

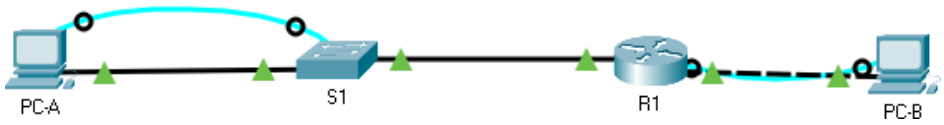
En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el swicth S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

192.168.34.0/24
100 host 192.168.34.0/25 255.255.255.128
50 host 192.168.34.128/26 255.255.255.192

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. Simulación de escenario 1



Fuente: Elaboración propia

Parte 2: Desarrolle el esquema de direccionamiento IP

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

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

En mi caso **192.168.34.0**

Tabla 1. Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0/0	192.168.34.129/26	255.255.255.192	No aplicable
	G0/0/1	192.168.34.1/25	255.255.255.128	No aplicable
S1	VLAN 1	192.168.34.2	255.255.255.128	192.168.34.1
PC-A	NIC	192.168.34.126	255.255.255.128	192.168.34.1
PC-B	NIC	192.168.34.190	255.255.255.192	192.168.34.129

Tabla 2. Tabla de Subredes

subred	hosts	Dirección de red/CIDR	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
LAN 1	100	192.168.34.0/25	192.168.34.1	192.168.34.126	192.168.34.127
LAN 2	50	192.168.34.128/26	192.168.34.129	192.168.34.190	192.168.34.191
Enlace WAN	2	192.168.34.192/28	192.168.34.193	192.168.34.194	192.168.34.195

Parte 3: Configure aspectos básicos

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

Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3. Tabla de Configuración R1

Tarea/ Especificación	Comandos
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip doma Router(config)#no ip domain-lookup Router(config)#
Nombre del router / R1	Router(config)#hostname R1 R1(config)#
Nombre de dominio / ccna-lab.com	R1(config)#ip domain-name ccna-lab.com R1(config)#
Contraseña cifrada para el modo EXEC privilegiado / ciscoenpass	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola / ciscoconpass	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#
Establecer la longitud mínima para las contraseñas / 10 caracteres	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local / Nombre de usuario: **admin** Password: **admin1pass**	R1(config)#username admin password admin1pass

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 4 R1(config-line)#password ciscocisco R1(config-line)#login local R1(config-line)#
Configurar VTY solo aceptando SSH	R1(config-line)#transport input SSH
Cifrar las contraseñas de texto no cifrado	R1(config)#service pass R1(config)#service password-encryption R1(config)#
Configure un MOTD Banner	R1(config)#banner motd #Este es el router de la UNAD. cualquier intrusion tendra efectos legales # R1(config)#
Configurar interfaz G0/0/0 Establezca la descripción Establece la dirección IPv4. Activar la interfaz.	R1(config)#interface g R1(config)#interface gigabitEthernet 0/0/0 R1(config-if)#ip address 192.168.34.129 255.255.255.192 R1(config-if)#des R1(config-if)#description Esta es la interfaz de la LAN 2 R1(config-if)#no shut R1(config-if)#no shutdown R1(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up
Configurar interfaz G0/0/1 / Establezca la descripción Establece la dirección IPv4.	R1(config)#interface gigabitEthernet 0/0/1 R1(config-if)#ip address 192.168.34.1 255.255.255.128 R1(config-if)#des R1(config-if)#description

Activar la interfaz.	Esta es la interfaz de la LAN 1 R1(config-if)#no shutdown R1(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
Generar una clave de cifrado RSA / Módulo de 1024 bits	R1(config)#crypto key generate RSA The name for the keys will be: R1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] R1(config)#

Se adjunta código y pantallazos con veracidad del código.

R1

Ingresar a modo privilegiado
Router>enable
Ingresar a modo de configuración
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Desactivar la búsqueda DNS
Router(config)#no ip domain-lookup
Asignar nombre al router
Router(config)#hostname R1
Definir el nombre de dominio

R1(config)#ip domain-name ccna-lab.com
Establecer una contraseña cifrada
R1(config)#enable secret ciscoenpass
ingresar al modo de configuración de la consola
R1(config)#line console 0
asignar una contraseña sin encriptar
R1(config-line)#password ciscoconpass
configurar autenticación al iniciar sesión
R1(config-line)#login
Salir del modo de modo de configuración de la consola
R1(config-line)#exit
Establecer la longitud mínima para las contraseñas
R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local
R1(config)#username admin password admin1pass

Configuro el inicio de sesión en las líneas VTY 0 4 para el uso de la base de datos local solo aceptando SSH y estableciendo una contraseña.

R1(config)#line vty 0 4
R1(config-line)#password ciscocisco
R1(config-line)#login local
R1(config-line)#transport input SSH
R1(config-line)#exit

Cifrar todas las contraseñas
R1(config)#service password-encryption
Configurar un MOTD Banner
R1(config)#banner motd #Este es el router de la UNAD. cualquier intrusion tendra efectos legales #

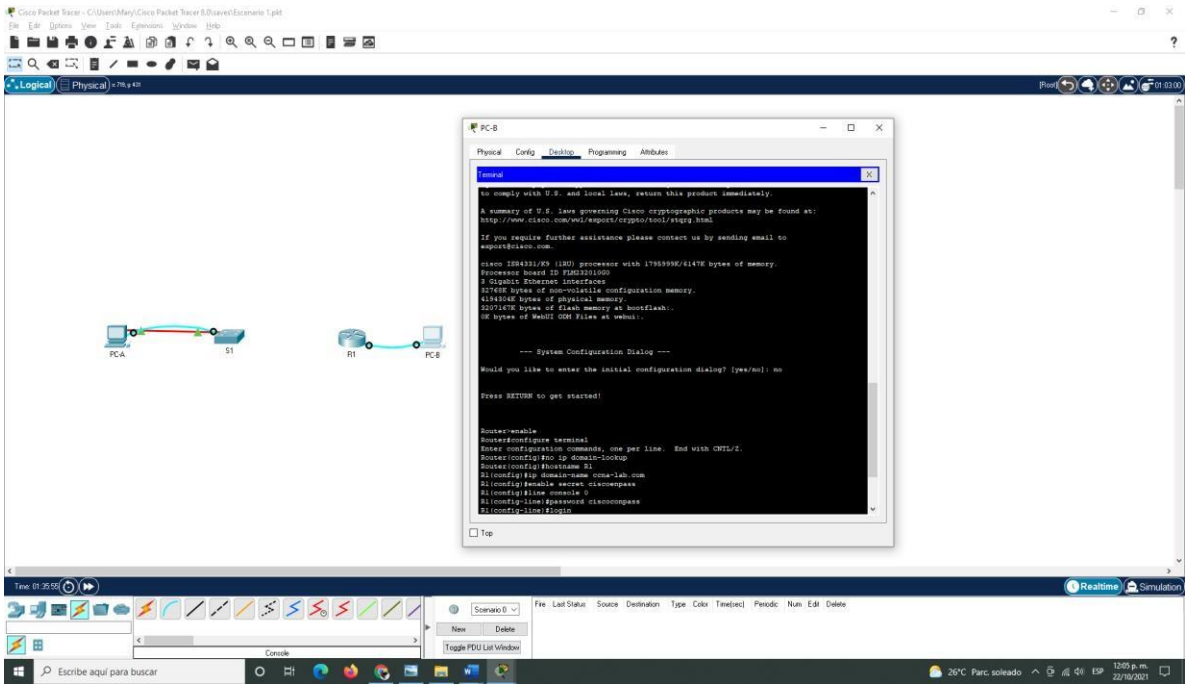
Configuración de la interfaz GigabitEthernet 0/0/0 se asigna dirección IPV4 Mascara de sub red, agrega una descripción y se habilita la interfaz.

R1(config)#interface g
R1(config)#interface gigabitEthernet 0/0/0
R1(config-if)#ip address 192.168.34.129 255.255.255.192
R1(config-if)#description Esta es la interfaz de la LAN 2
R1(config-if)#no shutdown
R1(config-if)#exit

Configuración de la interfaz GigabitEthernet 0/0/1 se asigna dirección IPV4 Mascara de sub red, agrega una descripción y se habilita la interfaz.

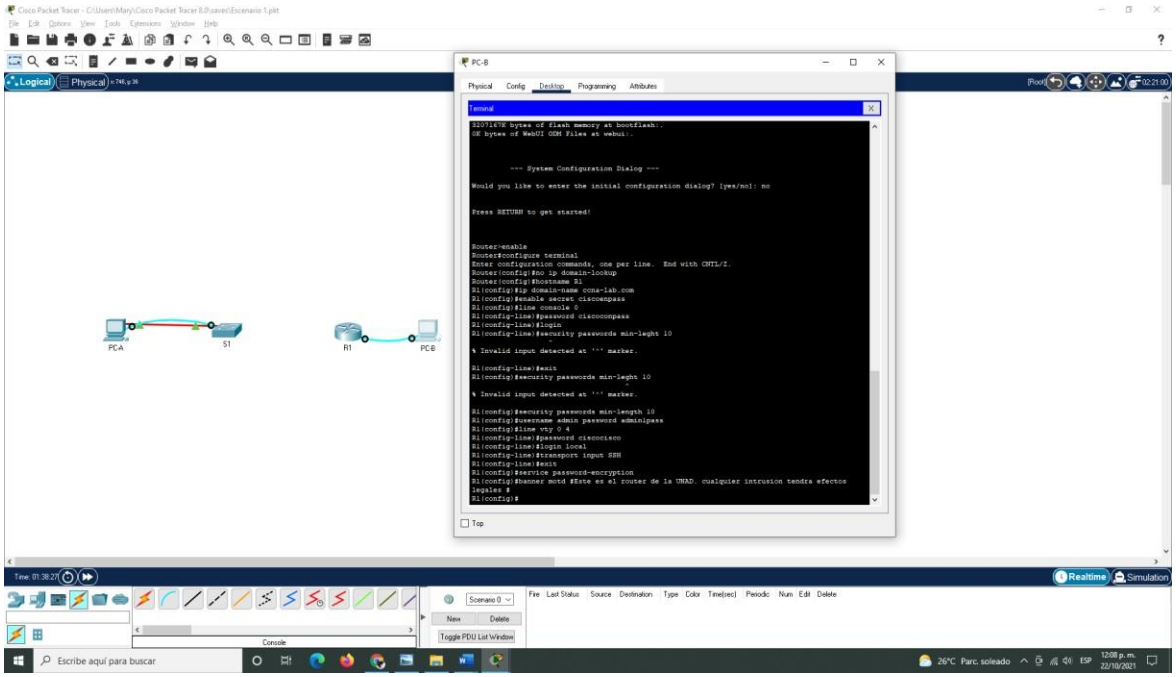
R1(config)#interface gigabitEthernet 0/0/1
R1(config-if)#ip address 192.168.34.1 255.255.255.128
R1(config-if)#description Esta es la interfaz de la LAN 1
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#ip domain-name ccna-lab.com
Generar una clave de cifrado RSA con Módulo de 1024 bits
R1(config)#crypto key generate RSA

Figura 3. Aplicando código R1



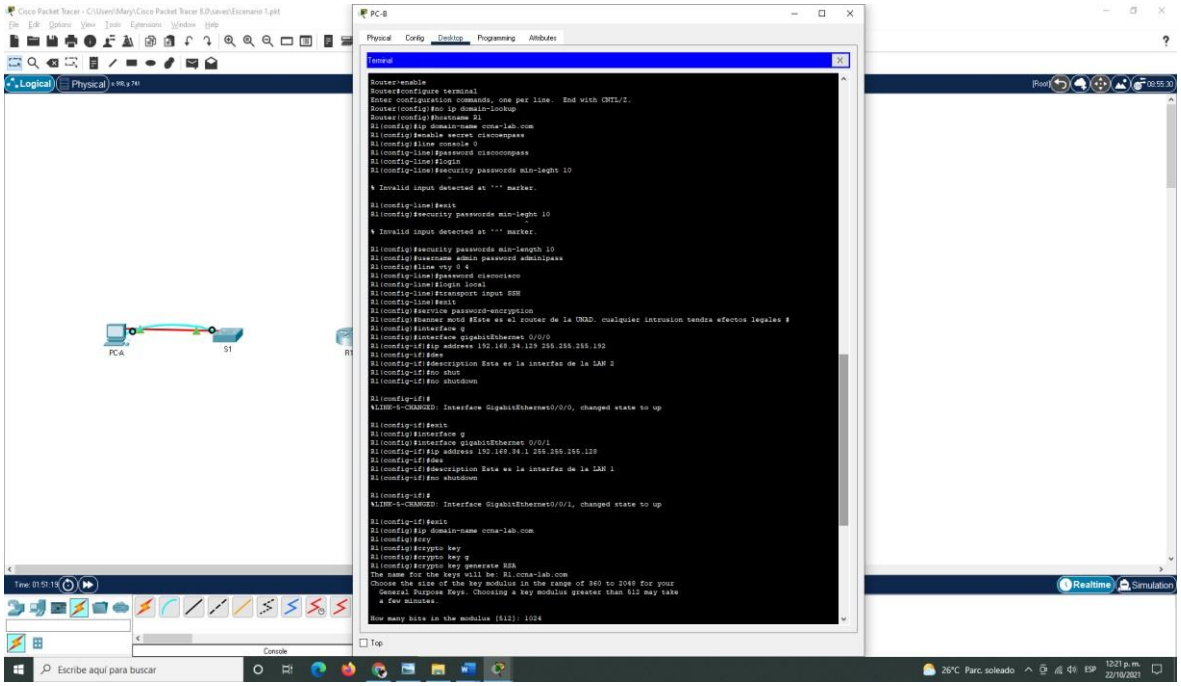
Fuente: Elaboración propia

Figura 4. Aplicando código R1



Fuente: Elaboración propia

Figura 5. Aplicando código R1



Fuente: Elaboración propia

En las imágenes anteriores se refleja la ejecución de los comandos y el avance del desarrollo lo que corresponde a la configuración del Router(R1) mediante la conexión consola.

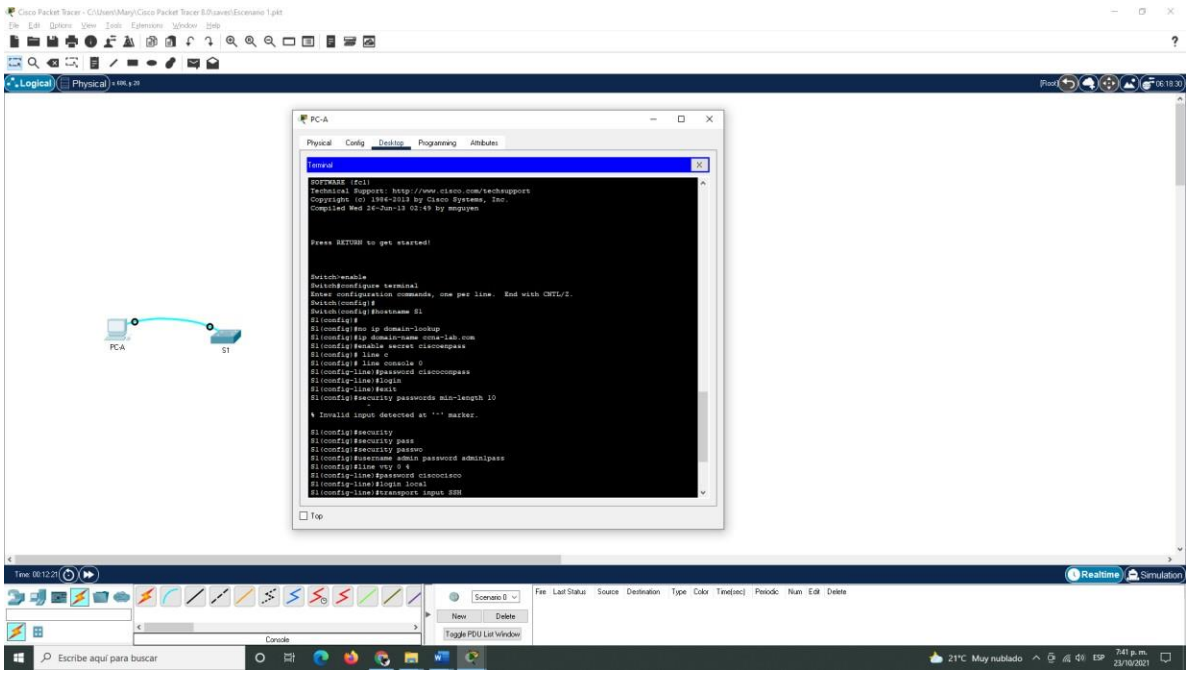
Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 4. Tabla de Configuración S1

Tarea / Especificación	Comandos
Desactivar la búsqueda DNS.	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch / S1	Switch(config)#hostname S1
Nombre de dominio / ccna-lab.com	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado / Ciscoenpass	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola/ ciscoconpass	S1(config)# line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base de datos local/ Nombre de usuario: admin Password: admin1pass	S1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#password ciscocisco S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input SSH S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd #Este es el Swicth de la UNAD. cualquier intrusion tendra efectos legales #

Generar una clave de cifrado RSA / Módulo de 1024 bits	S1(config)#crypto key generate RSA
Configurar la interfaz de administración (SVI) / Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento	S1(config)#interface vlan 1 S1(config-if)#ip address 192.168.34.2 255.255.255.128 S1(config-if)#no shutdown S1(config-if)#%LINK-5-CHANGED: Interface Vlan1, changed state to up S1(config-if)#exit
Configuración del gateway predeterminado/ Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento.	S1(config)#ip default-gateway 192.168.34.1

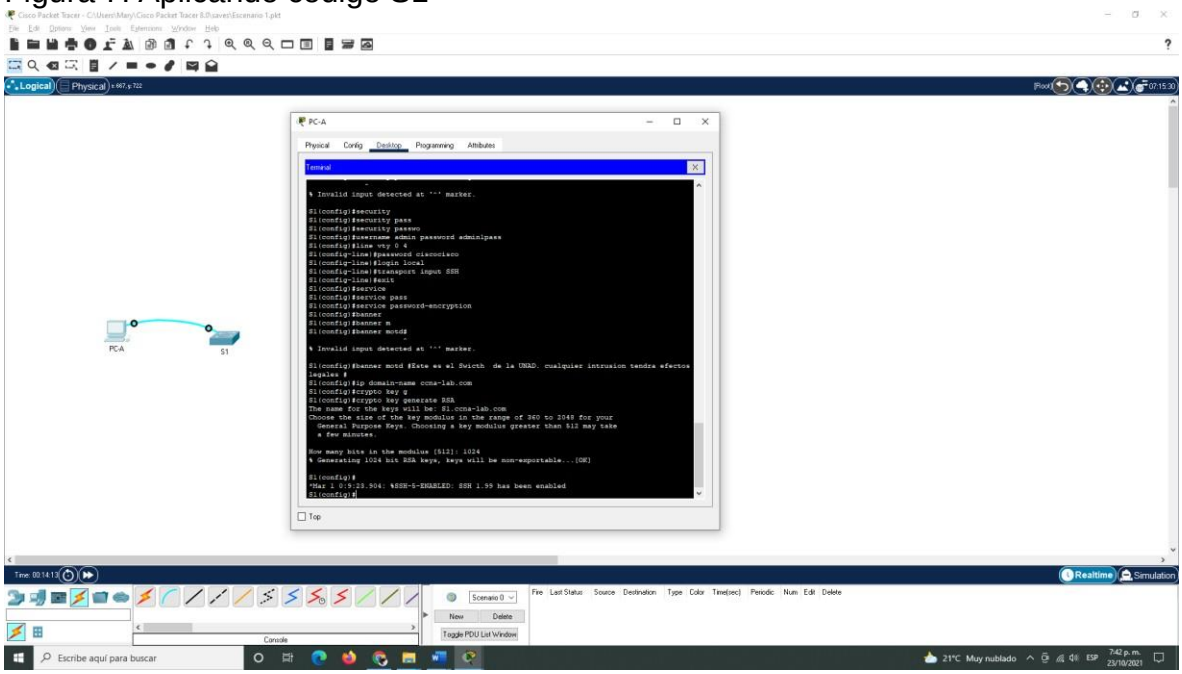
Figura 6. Aplicando código S1



Fuente: Elaboración propia

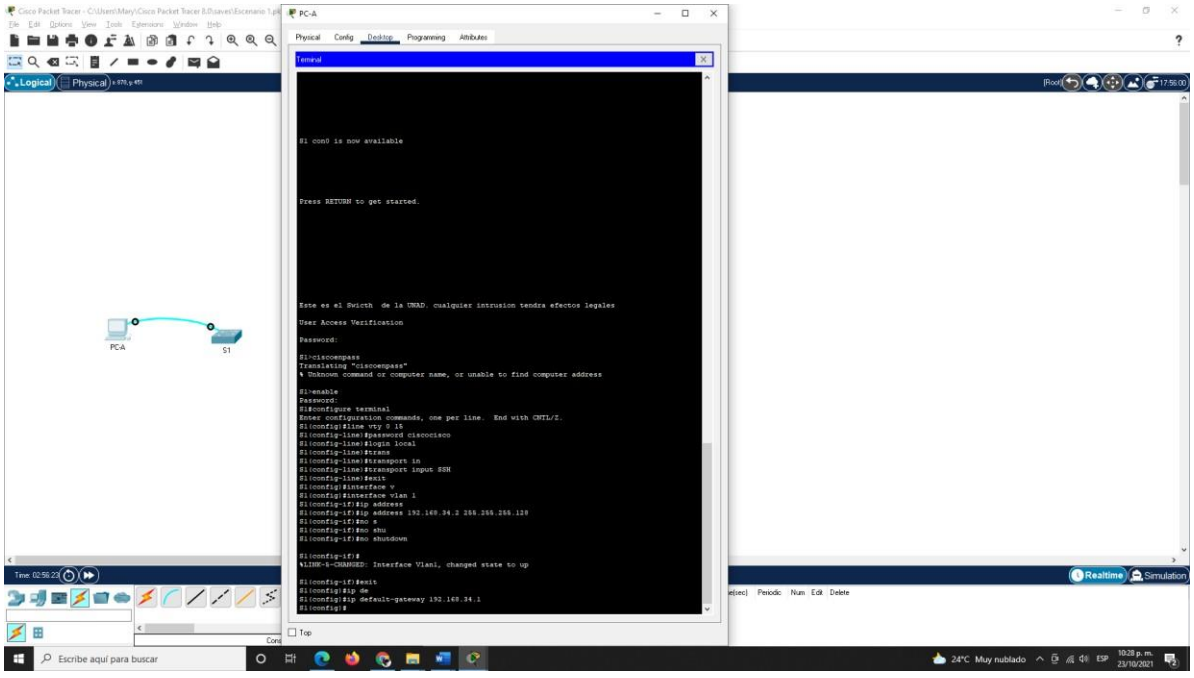
En las imágenes a continuación se refleja la ejecución de los comandos y el avance del desarrollo lo que corresponde a la configuración del Switch(S1) mediante la conexión consola.

Figura 7. Aplicando código S1



Fuente: Elaboración propia

Figura 8. Aplicando código S1

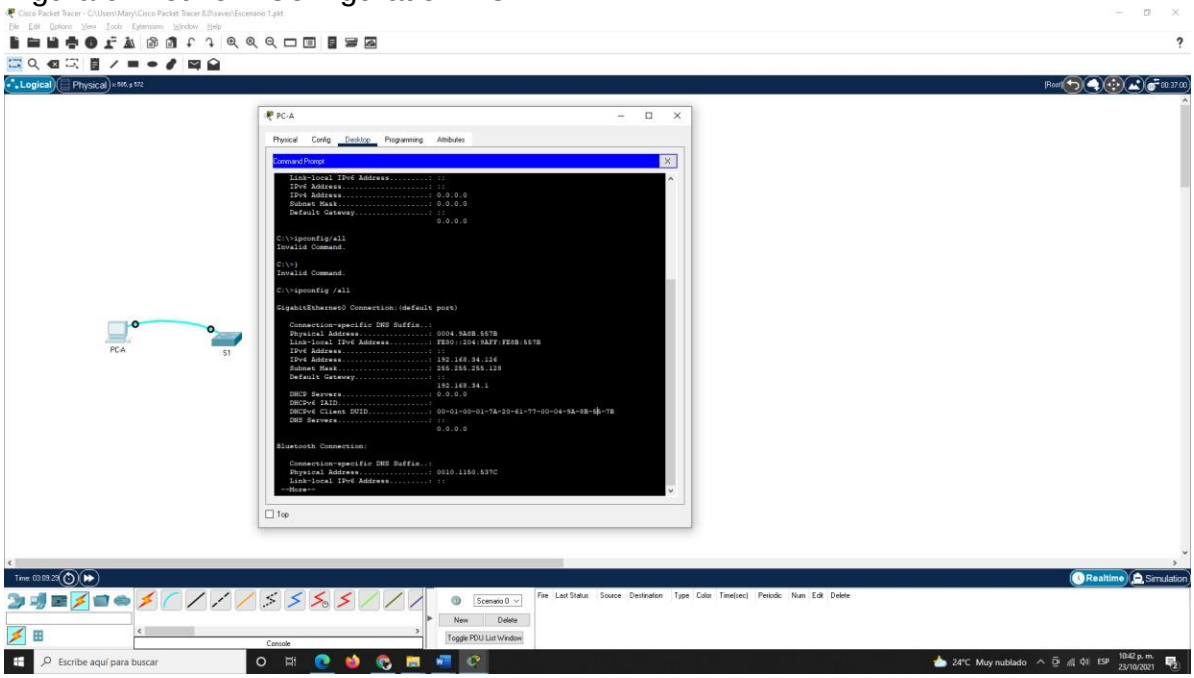


Fuente: Elaboración propia

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 del host con el comando ipconfig /all.

Figura 9. Network Configuration PC-A

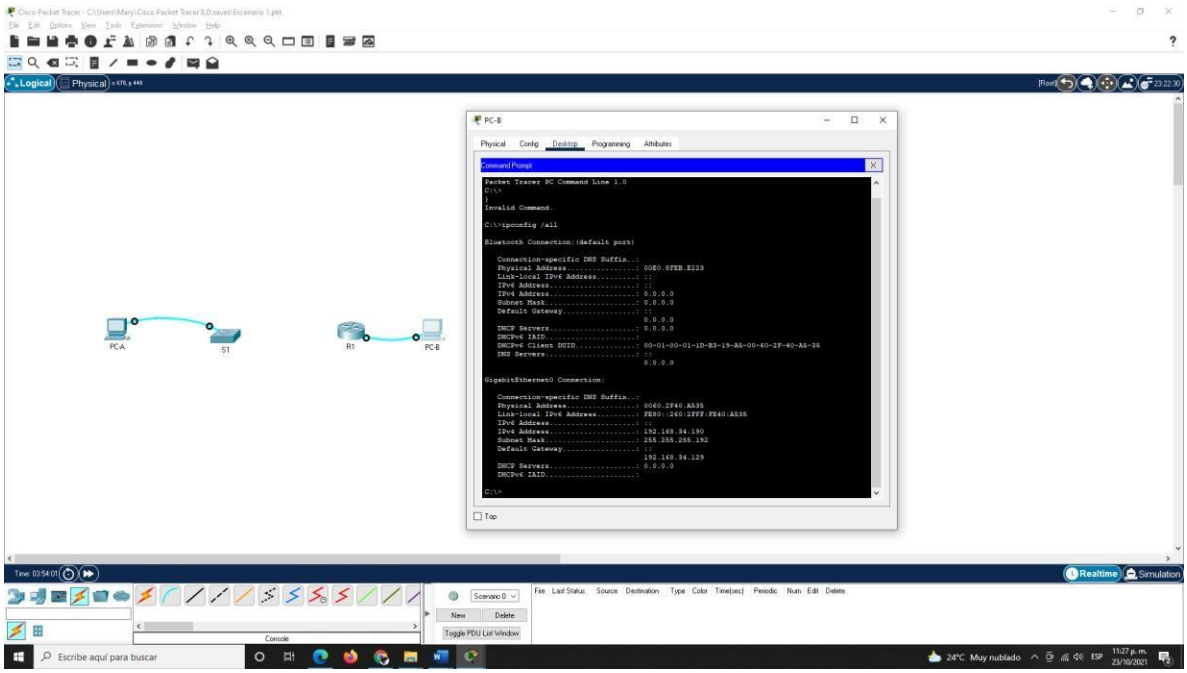


Fuente: Elaboración propia

Tabla 5. PC-A Network Configuration

	PC-A Network Configuration
Descripción	Conexión LAN1
Dirección física	0004.9A8B.557B
Dirección IP	192.168.34.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.34.1

Figura 10. Network Configuration PC-A



Fuente: Elaboración propia

Tabla 6. PC-B Network Configuration

PC-B Network Configuration	
Descripción	Conexión LAN 2
Dirección física	00E0.8FEB.E223
Dirección IP	192.168.34.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.34.129

Parte Cuarta. Verificar la conectividad entre los dispositivos

Se ejecuta el comando Show Ip route para mostrar el contenido de la tabla de enrutamiento en R1, se refleja que hay 2 rutas conectadas (utilizan el código C)

C 192.168.34.0/25 is directly connected, GigabitEthernet0/0/1
C 192.168.34.128/26 is directly connected, GigabitEthernet0/0/0

El router solo enviara paquetes a redes indicadas en la tabla de enrutamiento.

Figura 11. Show Ip route en R1

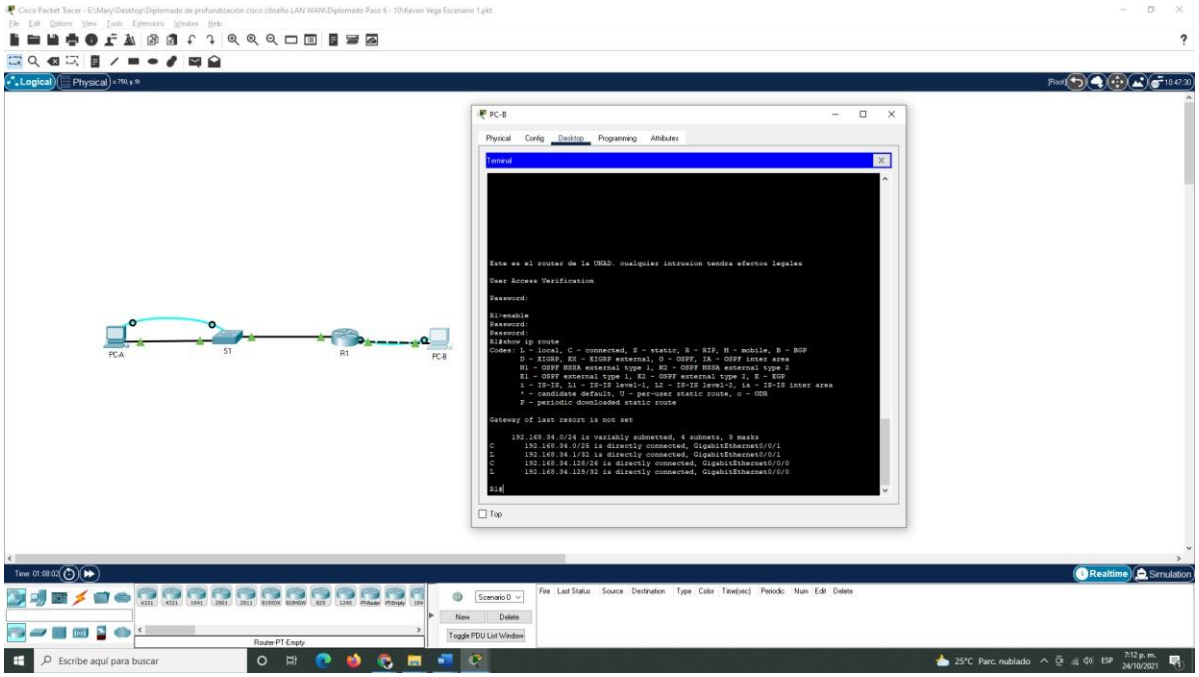
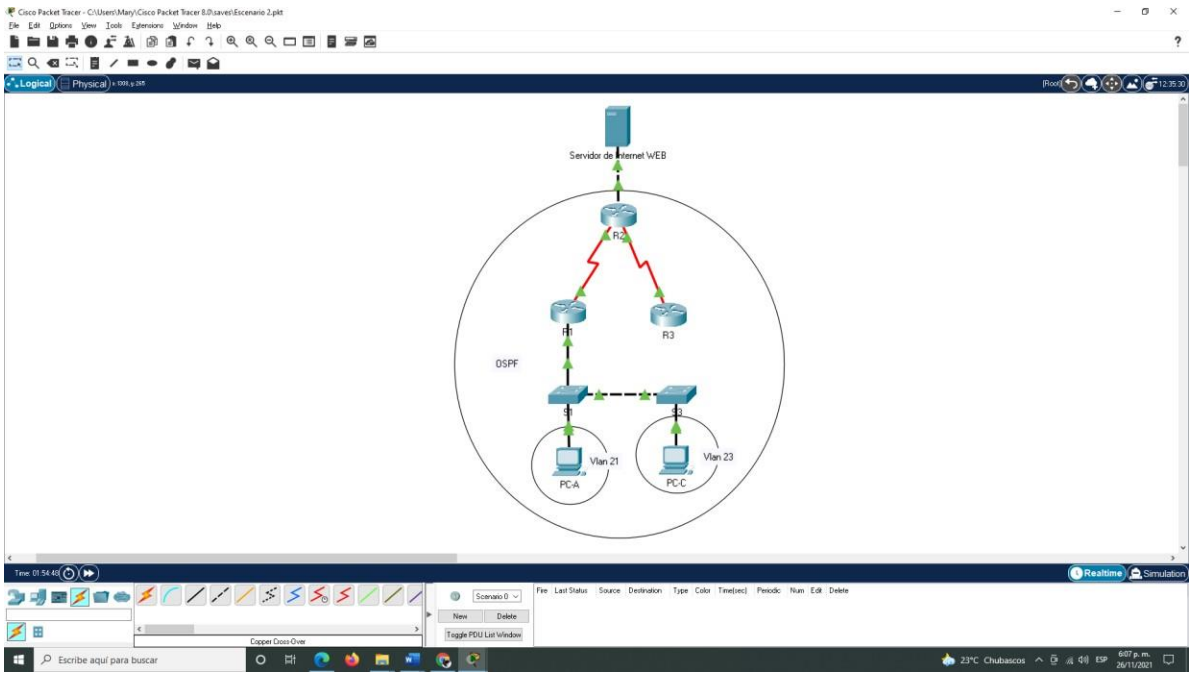


Figura 12. Escenario 2



Fuente: Elaboración propia

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

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos. Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 7. Inicialización de dispositivos switches y routers S1, S3, R1, R2, y R3

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 Proceed with reload? [confirm] enter
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch#erase startup-config
Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm] enter

Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#sh flash Switch#show vlan brief

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 8. Configuracion Servidor de Internet

Elemento o tarea de configuración	**Especificación**
Dirección IPv4	209.165.200.228
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1/64

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 9. Configuracion Parámetros básicos en R1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	
Nombre del router	R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no

	autorizado.
Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

Se adjunta código y pantallazos con veracidad del código.

R1
Ingresar al modo privilegiado
Router>enable
Ingresar al modo de configuracion global
Router#configure terminal
Desactivar la búsqueda del DNS
Router(config)#no ip domain-lookup
Asignar nombre al router
Router(config)#hostname R1
Establecer una contraseña cifrada
R1(config)#enable secret class
Ingresar al modo de configuración de la consola
R1(config)#line console 0
Asignar una contraseña sin encriptar
R1(config-line)#password cisco
Autenticación al iniciar sesión
R1(config-line)#login
Salir del modo de configuración de la consola
R1(config-line)#exit
Ingresar a la configuracion remota telnet
R1(config)#line vty 0 4
Asignar una contraseña sin encriptar

R1(config-line)#password cisco
Autenticación al iniciar sesión
R1(config-line)#login
Salir del modo de configuracion remota telnet
R1(config-line)#exit
Cifrar todas las contraseñas
R1(config)#service password-encryption
Configurar un Banner MOTD
R1(config)#banner motd #Se prohíbe el acceso no autorizado#
Habilitar el routing IPv6
R1(config)#ipv6 unicast-routing

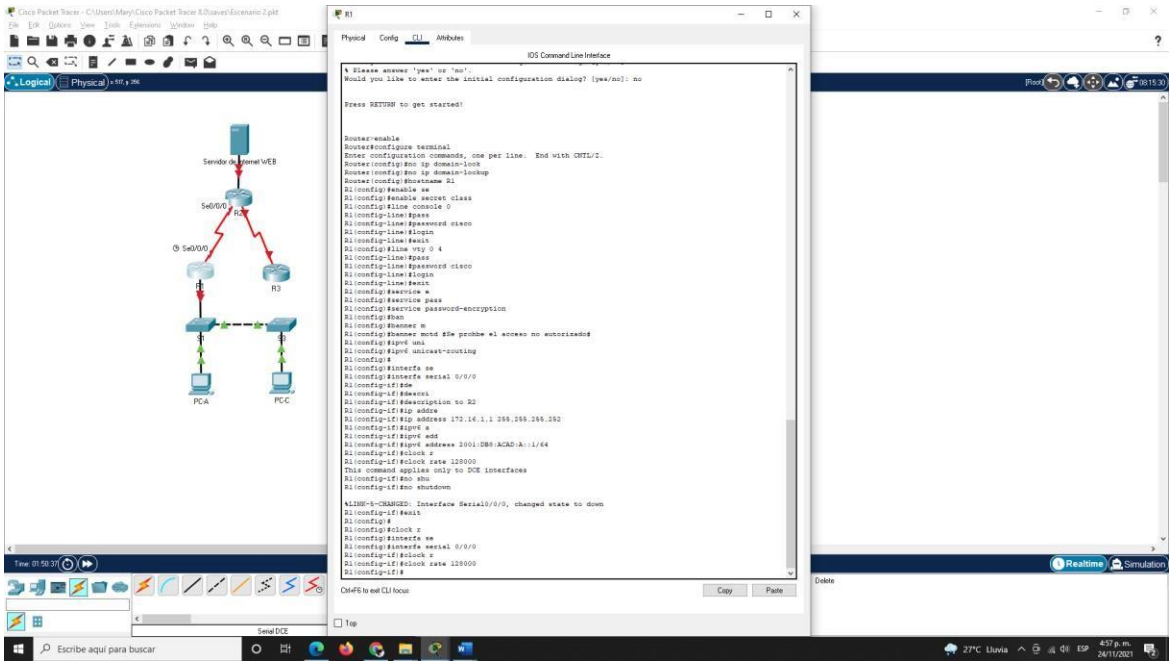
Configuración de la interfaz serial 0/0/0 que conecta al Router 2 se asigna dirección IPV4 Mascara de sub red, se establece la dirección IPv6, la frecuencia de reloj en 128000 y se habilita la interfaz.

R1(config)#interfa serial 0/0/0
R1(config-if)#description to R2
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R1(config-if)#no shutdown
R1(config-if)#exit

Establecer la frecuencia del reloj en 128000
R1(config)#interfa serial 0/0/0
R1(config-if)#clock rate 128000

Se configura una ruta predeterminada Ipv4 y Ipv6 para S0/0/0
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#ipv6 route ::/0 s0/0/0

Figura 13. Aplicando código en R1



Fuente: Elaboración propia

En la anterior figura se refleja la ejecución de los comandos y el avance del desarrollo lo que corresponde a la configuración del Router(R1)

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

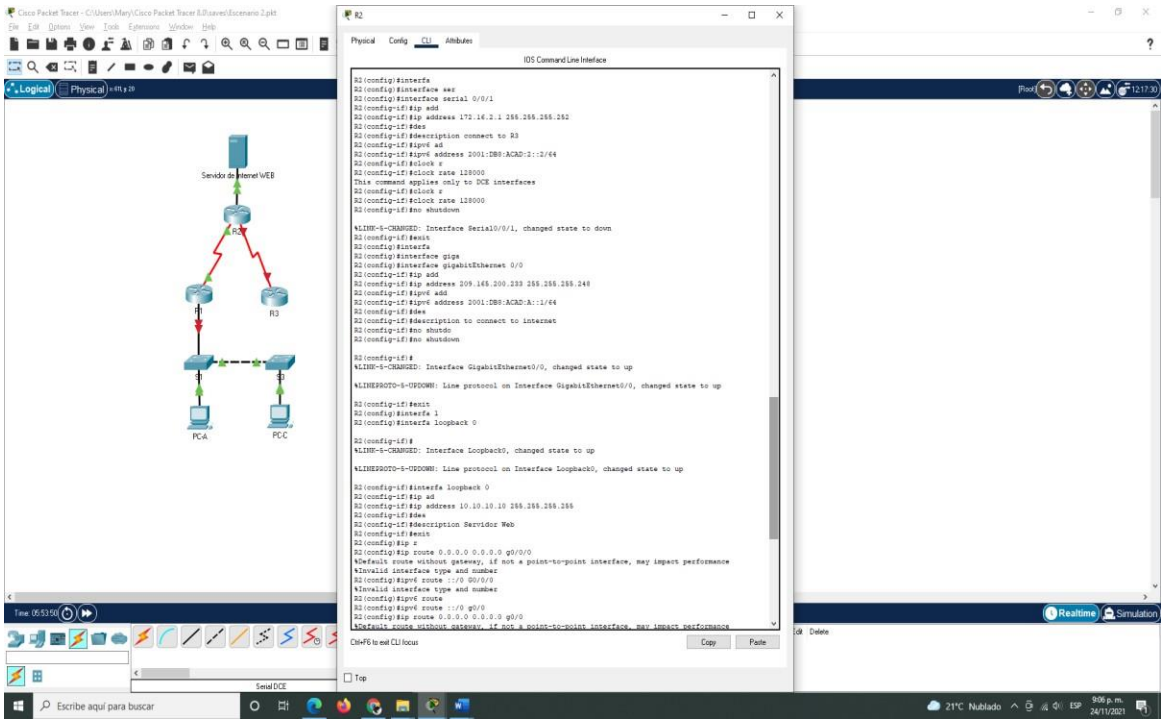
Tabla 10. Configuracion Parámetros básicos en R2

Elemento o tarea de configuración/ Especificación	**Comandos**
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router/ R2	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada/ class	R2(config)#enable secret class
Contraseña de acceso a la consola/ cisco	R2(config)#line console 0 R2(config-line)#password cisco

	R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet/ cisco	R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	Packet tracer no lo soporta
Mensaje MOTD/ Se prohíbe el acceso no autorizado.	R2(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/0/0 Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	R2(config)#ipv6 unicast-routing R2(config)#interf serial 0/0/0 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#description connect to R1 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown R2(config-if)#exit
Interfaz S0/0/1/ Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz	R2(config)#interface serial 0/0/1 R2(config-if)#ip address 172.16.2.1 255.255.255.252 R2(config-if)#description connect to R3 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown R2(config-if)#exit

Interfaz G0/0 (simulación de Internet)/ Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz	R2(config)#interface gigabitEthernet 0/0 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 to connect to internet R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)/ Establecer la descripción. Establezca la dirección IPv4.	R2(config-if)#interfa loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description Servidor Web R2(config-if)#exit
Ruta predeterminada/ Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.	R2(config)#ipv6 route ::/0 g0/0 R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 %Default route without gateway, if not a point-to-point interface, may impact performance R2(config)#

Figura 14. Aplicando código en R2



Fuente: Elaboración propia

Se ejecutan los comandos para la configuracion de los parámetros básicos del router R2 y la configuracion de las interfaces serial 0/0/0 y 0/0/1 GigabitEthernet 0/0 y Loopback 0

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

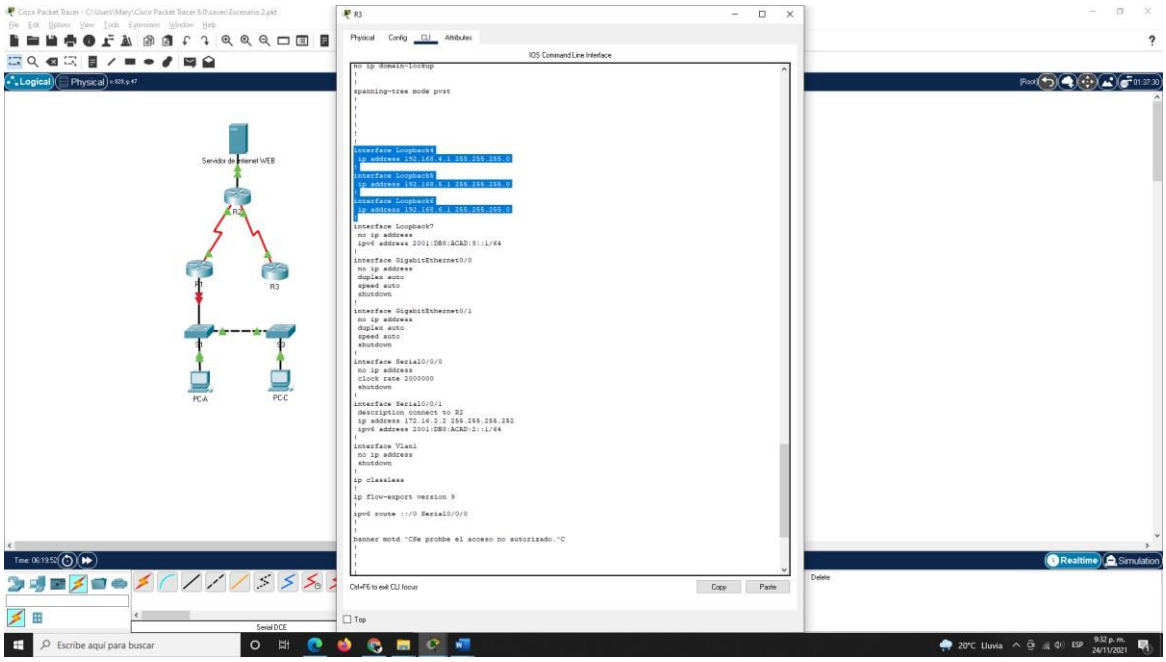
Tabla 11. Configuracion Parámetros básicos en R3

Elemento o tarea de configuración / Especificación	**Comandos**
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup

Nombre del router/ R3	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada/ class	R3(config)#enable secret class
Contraseña de acceso a la consola/ cisco	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Contraseña de acceso Telnet/ cisco	R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD / Se prohíbe el acceso no autorizado.	R3(config)#banner motd #Se prohibe el acceso no autorizado.#
Interfaz S0/0/1 / Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	R3(config)#ipv6 unicast-routing R3(config)#interfa serial 0/0/1 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 connect to R2 R3(config-if)#no shutdown
Interfaz loopback 4/ Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config)#interfa loopback 4 R3(config)# ip address 192.168.4.1 255.255.255.0 R3(config)#exit

Interfaz loopback 5 / Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config)#interfa loopback 5 R3(config)# ip address 192.168.5.1 255.255.255.0 R3(config)#exit
Interfaz loopback 6 / Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config)#interfa loopback 6 R3(config)# ip address 192.168.6.1 255.255.255.0 R3(config)#exit
Interfaz loopback 7/ Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.	R3(config)#interfa loopback 7 R3(config-if)#ipv6 add R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#exit
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 %Default route without gateway, if not a point-to-point interface, may impact performance R3(config)#ipv6 route ::/0 s0/0/0

Figura 15. Show run en R3



Fuente: Elaboración propia

Se muestra las configuracion establecidas en la ejecución de los comandos de cada una de las interfaces serial 0/01 y Loopback 4, 5, 6 y 7.

Paso 5: Configurar S1

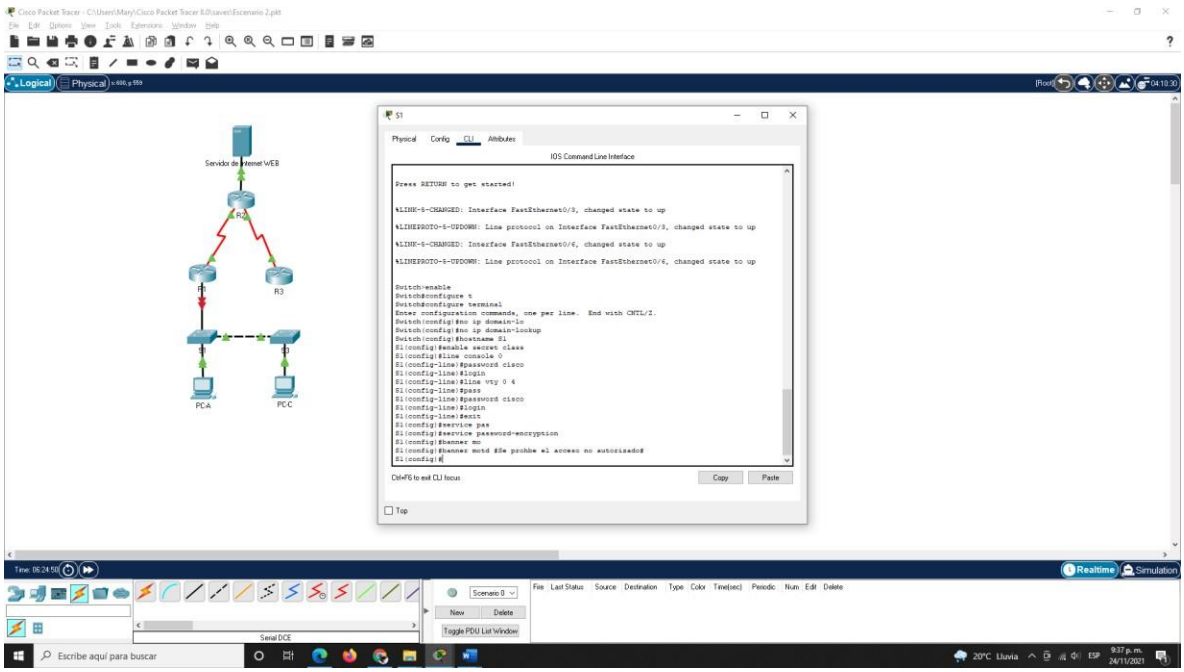
La configuración del S1 incluye las siguientes tareas:

Tabla 12. Configuracion Parámetros básicos en S1

Elemento o tarea de configuración/ Especificación	**Comandos**
Desactivar la búsqueda DNS	Switch>enable Switch#configure t Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup
Nombre del switch / S1	Switch(config)#hostname S1
Contraseña de exec privilegiado	S1(config)#enable secret class

cifrada / class	S1(config)#
Contraseña de acceso a la consola / cisco	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet / cisco	S1(config-line)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD / Se prohíbe el acceso no autorizado.	S1(config)#banner motd #Se prohbe el acceso no autorizado#

Figura 16. Aplicando Código en S1



Fuente: Elaboración propia

Se ejecutan los comandos para la configuracion de los parámetros básicos en S1

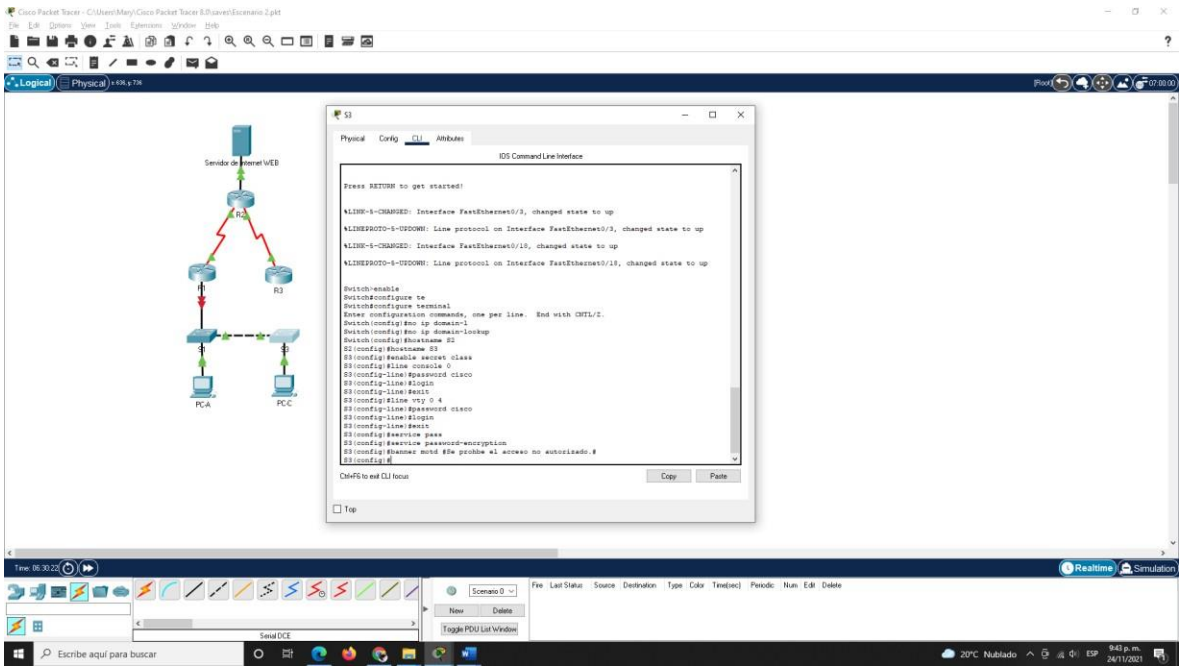
Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 13. Configuracion Parámetros básicos en S3

Elemento o tarea de configuración / Especificación	**Comandos**
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup
Nombre del switch / S3	Switch(config)#hostname S3 S3(config)#
Contraseña de exec privilegiado cifrada / class	S3(config)#enable secret class
Contraseña de acceso a la consola / cisco	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Contraseña de acceso Telnet / cisco	S3(config)#line vty 0 4 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S3(config)#service pass S3(config)#service password-encryption
Mensaje MOTD / Se prohíbe el acceso no autorizado.	S3(config)#banner motd #Se prohíbe el acceso no autorizado.#

Figura 17. Aplicando Código en S3



Fuente: Elaboración propia

Se ejecutan los comandos para la configuracion de los parámetros básicos en S3.

Paso 7: Verificar la conectividad de la red

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

Tabla 14. Verificación de Red

Desde	**A**	**Dirección IP**	**Resultados de ping**
R1	R2, S0/0/0	172.16.1.2	R1#ping 172.16.1.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max =

			3/20/35 ms
R2	R3, S0/0/1	172.16.2.1	R2#ping 172.16.2.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/17/32 ms
PC de Internet	Gateway predeterminado	209.165.200.233	

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 15. Configuracion de las Vlan y el routing entre VLAN en S1

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican
Asignar la dirección IP de de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología administración.
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3 /	Utilizar la red VLAN 1 como VLAN nativa

Forzar el enlace troncal en la interfaz F0/5 /	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	
Apagar todos los puertos sin usar	

Se adjunta código y pantallazos con veracidad del código.

S1

Se ejecutan los siguientes comandos desde la configuración global modo Exec privilegiado para crear y asignar los nombres alas Vlans

S1(config)#vlan 21
S1(config-vlan)#name contabilidad
S1(config-vlan)#exit
S1(config)#vlan 23
S1(config-vlan)#name ingenieria
S1(config-vlan)#exit
S1(config)#vlan 99
S1(config-vlan)#name administracion
S1(config-vlan)#exit

Asignar la dirección IPv4 a la VLAN de administración

S1(config)#interfa vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit

Asignar el gateway predeterminado
S1(config)#ip default-gateway 192.168.99.1

Se Configura el puerto F0/3 en el S1 como puerto de enlace troncal

S1(config)#interfa fastEthernet 0/3
Establecer como puerto de enlace troncal
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit

Se Configura el puerto F0/5 en el S1 como puerto de enlace troncal

```
S1(config)#interfa fastEthernet 0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
```

Se Configurar el resto de los puertos como puertos de acceso

```
S1(config)#inter range f0/1-2, f0/4, f0/6-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#exit
```

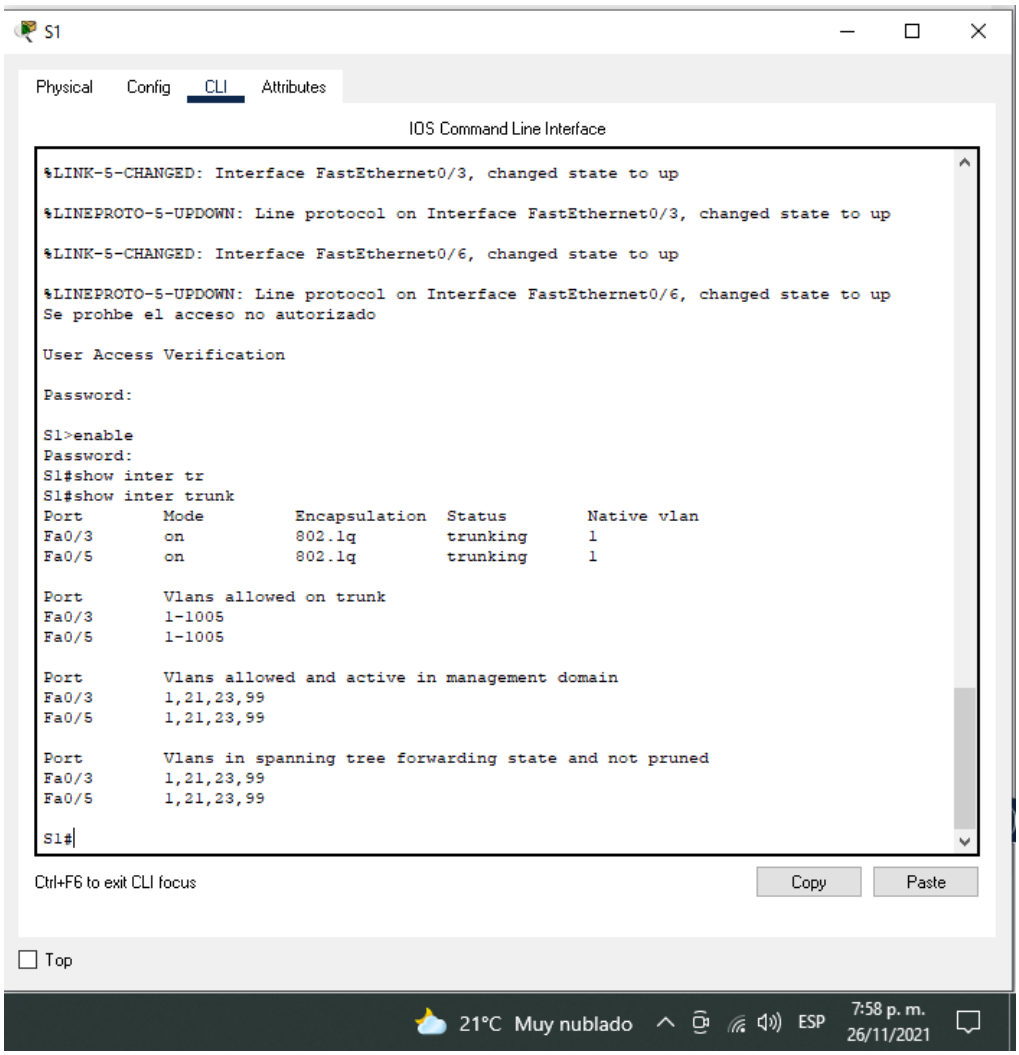
Asignar fastEthernet 0/6 a la VLAN 21

```
S1(config)#inter fastEthernet 0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 21
S1(config-if)#exit
```

Se Desactivaron todos los puertos físicos sin utilizar

```
S1(config)#inter range f0/1-2, f0/4, f0/7-24, g0/1-2
S1(config-if-range)#shutdown
```

Figura 18. show interface trunk en S1



Fuente: Elaboración propia

La anterior figura se puede verificar la configuracion realizada se establecieron los enlaces troncales

Paso 2: Configurar el S3

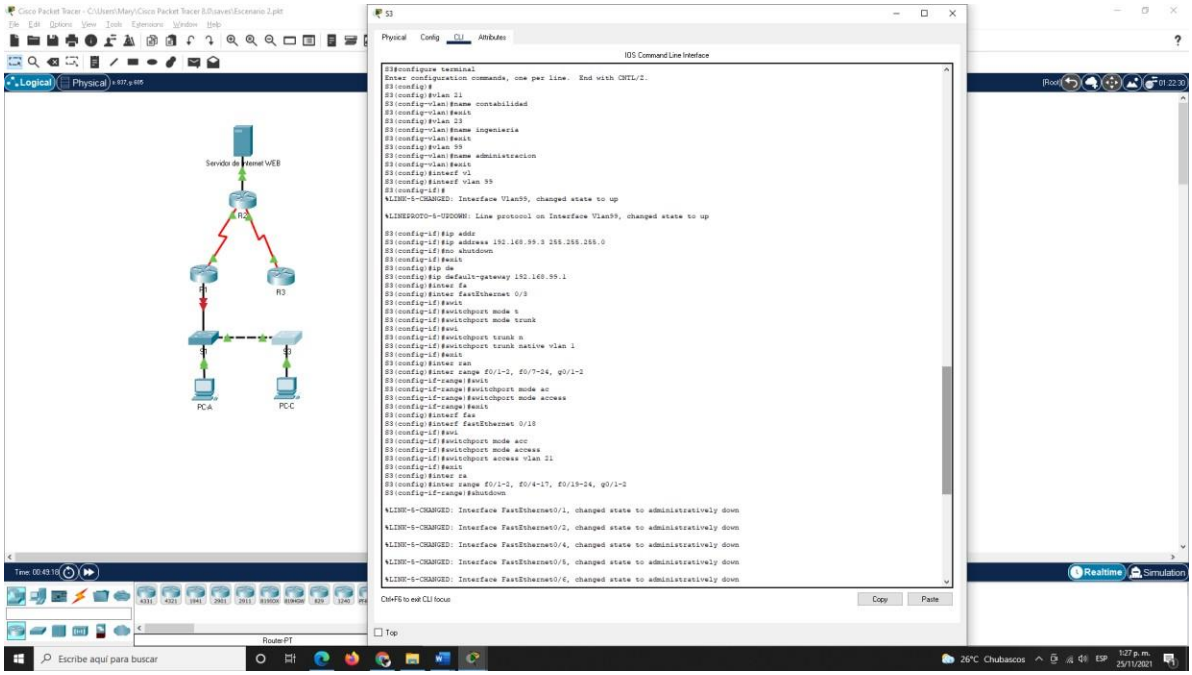
La configuración del S3 incluye las siguientes tareas:

Tabla 16. Configuracion de las Vlan y el routing entre VLAN en S3

Elemento o tarea de configuración/ Especificación	**Comandos**
Crear la base de datos de VLAN / Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.	S3(config)#vlan 21 S3(config-vlan)#name contabilidad S3(config-vlan)#exit S3(config)#vlan 23 S3(config-vlan)#name ingenieria S3(config-vlan)#exit S3(config)#vlan 99 S3(config-vlan)#name administracion S3(config-vlan)#exit
Asignar la dirección IP de administración/ Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología	S3(config)#interf vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#exit
Asignar el gateway predeterminado. / Asignar la primera dirección IP en la subred como gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3 / Utilizar la red VLAN 1 como VLAN nativa	S3(config)#inter fastEthernet 0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#exit
Configurar el resto de los puertos como puertos de acceso / Utilizar el comando interface range	S3(config)#inter range f0/1-2, f0/7-24, g0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#exit
Asignar F0/18 a la VLAN 21	S3(config)#interf fastEthernet 0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 21 S3(config-if)#exit
Apagar todos los puertos sin usar	S3(config)#inter range f0/1-2, f0/4-

	17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Figura 19. Aplicando Código en S3



Fuente: Elaboración propia

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

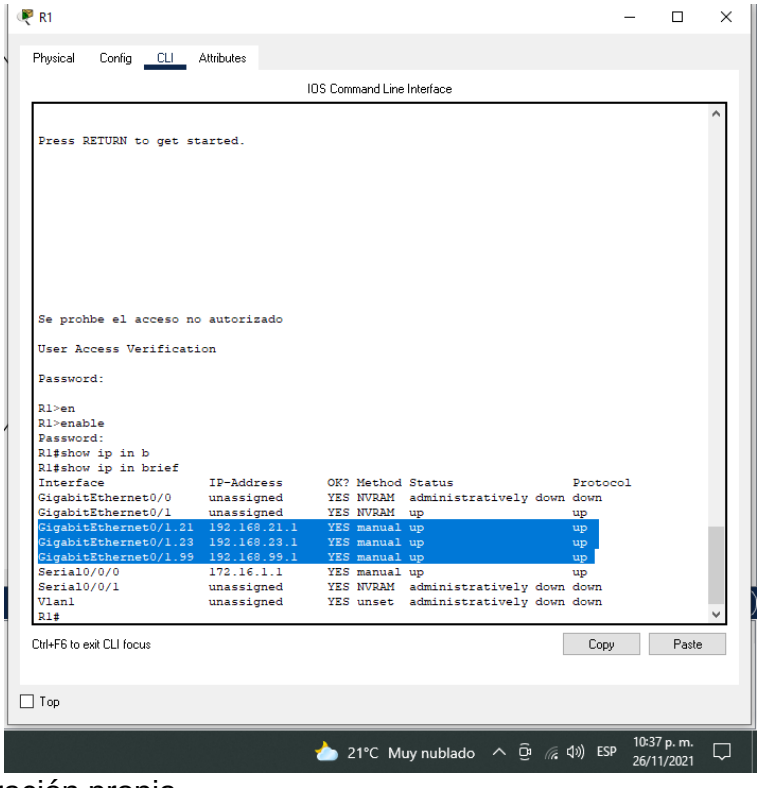
Tabla 17. Configuracion Subinterfaces G0/1 en R1

Elemento o tarea de configuración/ Especificación	**Comandos**
Configurar la subinterfaz 802.1Q .21 en G0/1/ Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz	R1(config)#interfa gigabitEthernet 0/1.21 R1(config-subif)#des R1(config-subif)#description vlan 21 R1(config-subif)#encap dot1Q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#exit

Configurar la subinterfaz 802.1Q .23 en G0/1/ Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz	R1(config)#interfa gigabitEthernet 0/1.23 R1(config-subif)#description vlan 23 R1(config-subif)#encapsulation dot R1(config-subif)#encapsulation dot1Q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .99 en G0/1/ Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz	R1(config)#interfa gigabitEthernet 0/1.99 R1(config-subif)#description Vlan 99 R1(config-subif)#encapsulation dot R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#exit
Activar la interfaz G0/1	R1(config)#inter gigabitEthernet 0/1 R1(config-if)#no shutdown R1(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up %LINK-5-CHANGED: Interface GigabitEthernet0/1.21, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.21, changed state to up

	%LINK-5-CHANGED: Interface GigabitEthernet0/1.23, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.23, changed state to up %LINK-5-CHANGED: Interface GigabitEthernet0/1.99, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.99, changed state to up

Figura 20. show ip interface brief en R1



Fuente: Elaboración propia

Se muestra las configuracion establecidas en la ejecución de los comandos de cada una de las subinterfaces G0/1.21, G0/1.23 y G0/1.91 con información de direccionamiento IP y los estados de interfaz.

Paso 4: Verificar la conectividad de la red

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

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

Tabla 18. Verificación de la red

Desde	**A**	**Dirección IP**	**Resultados de ping**
S1	R1, dirección VLAN 99	192.168.99.1	S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 99	192.168.99.1	S3#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/13 ms
S1	R1, dirección VLAN 21	192.168.21.1	S1#ping 192.168.21.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 23	192.168.23.1	S3#ping 192.168.23.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to

			192.168.23.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

En la anterior tabla se pueden observar los resultados de ejecutar el comando ping para verificar la conectividad entre los Switches S1 y S3, se puede concluir que la configuracion entre los dispositivos es óptima y no es necesario tomar medidas correctivas.

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 19. Configuracion protocolo OSPF en R1

Elemento o tarea de configuración/ Especificación	**Comandos**
Configurar OSPF área 0	R1(config)#router ospf 1
Anunciar las redes conectadas directamente/ Asigne todas las redes conectadas directamente.	R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0 R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface gigabitEthernet 0/1 R1(config-router)#passive-interface gigabitEthernet 0/1.21 R1(config-router)#passive-interface gigabitEthernet 0/1.23 R1(config-router)#passive-interface gigabitEthernet 0/1.99
Desactive la sumarización automática	**No aplica para el protocolo OSPF**

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 20. Configuracion protocolo OSPF en R2

Elemento o tarea de configuración/Especificación	**Comandos**
Configurar OSPF área 0	R2(config)#router ospf 1
Anunciar las redes conectadas directamente/ **Nota:** Omitir la red G0/0.	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
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	**No aplica para el protocolo OSPF**

Paso 3: Configurar OSPF en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 21. Configuracion protocolo OSPF en R3

Elemento o tarea de configuración/ Especificación	**Comandos**
Configurar OSPF área 0	R3(config)#router ospf 1 R3(config-router)#router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6 R3(config-router)#passive-interface

	loopback 7
Desactive la sumarización automática.	**No aplica para el protocolo OSPF**

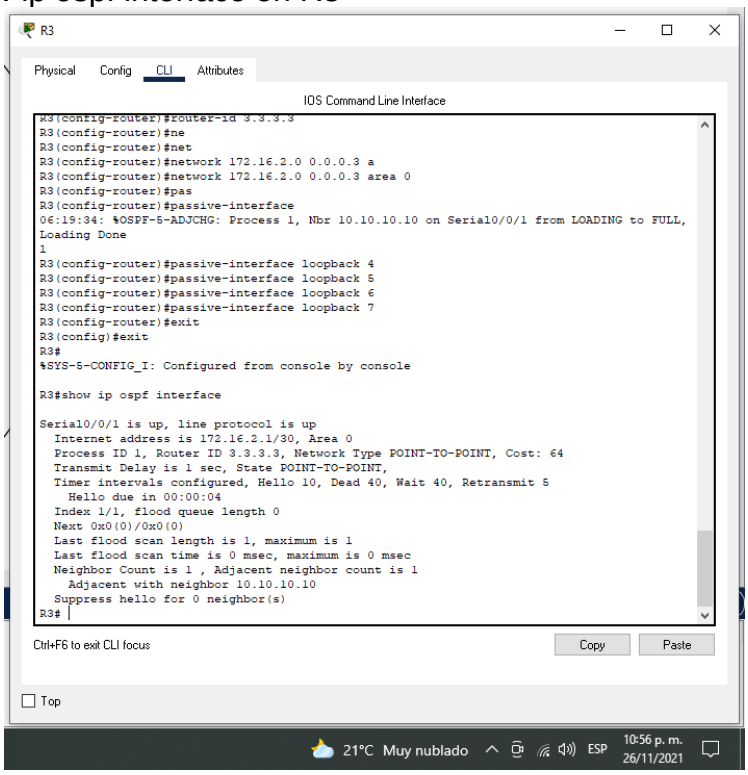
Paso 4: Verificar la información de OSPF

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

Tabla 22. verificación protocolo OSPF

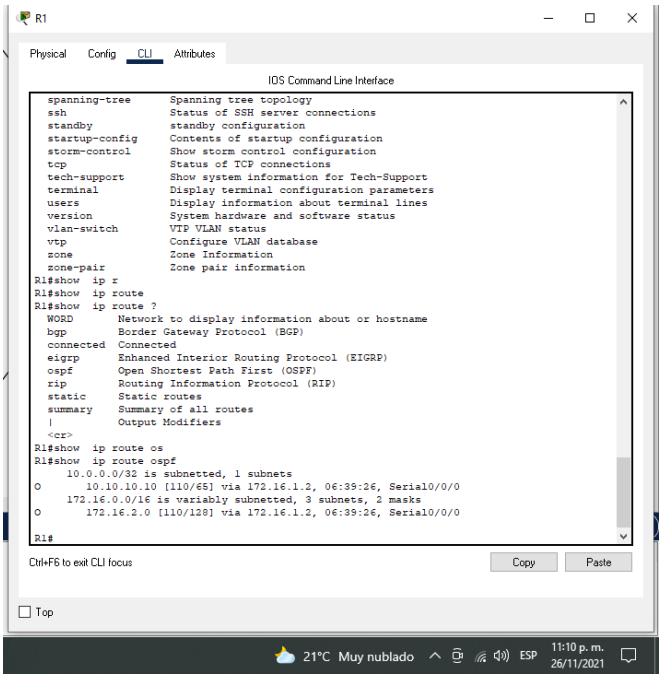
Pregunta	**Respuesta**
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	show ip protocols
¿Qué comando muestra solo las rutas OSPF?	show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración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

Figura 21. show ip ospf interface en R3



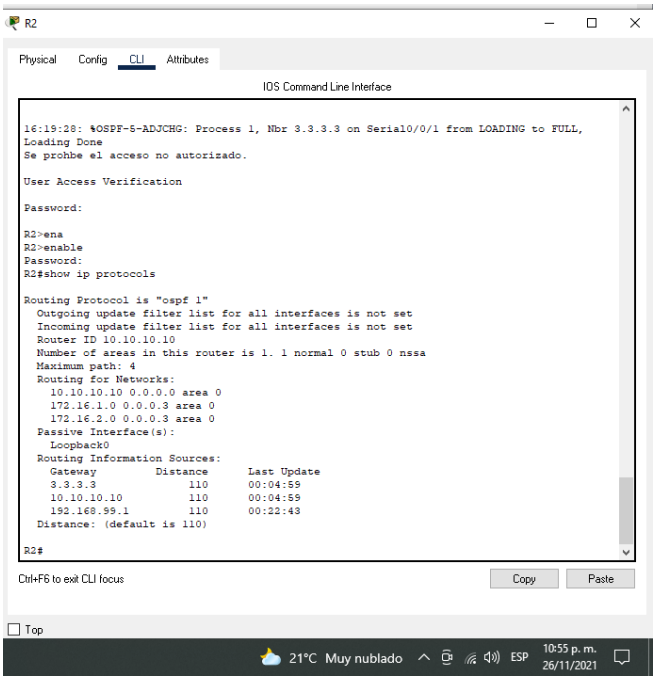
Fuente: Elaboración propia

Figura 22. show ip route ospf en R1



Fuente: Elaboración propia

Figura 23. show ip protocols en R2



Fuente: Elaboración propia

La ejecución de este comando muestra la información de los protocolos de routing

configurados. Incluyendo OSPF incluye la ID del proceso OSPF, la ID del router, las redes que anuncia el router, los vecinos de los que el router recibe actualizaciones y la distancia administrativa predeterminada, que para OSPF es 110.

Parte 5: Implementar DHCP y NAT para IPv4

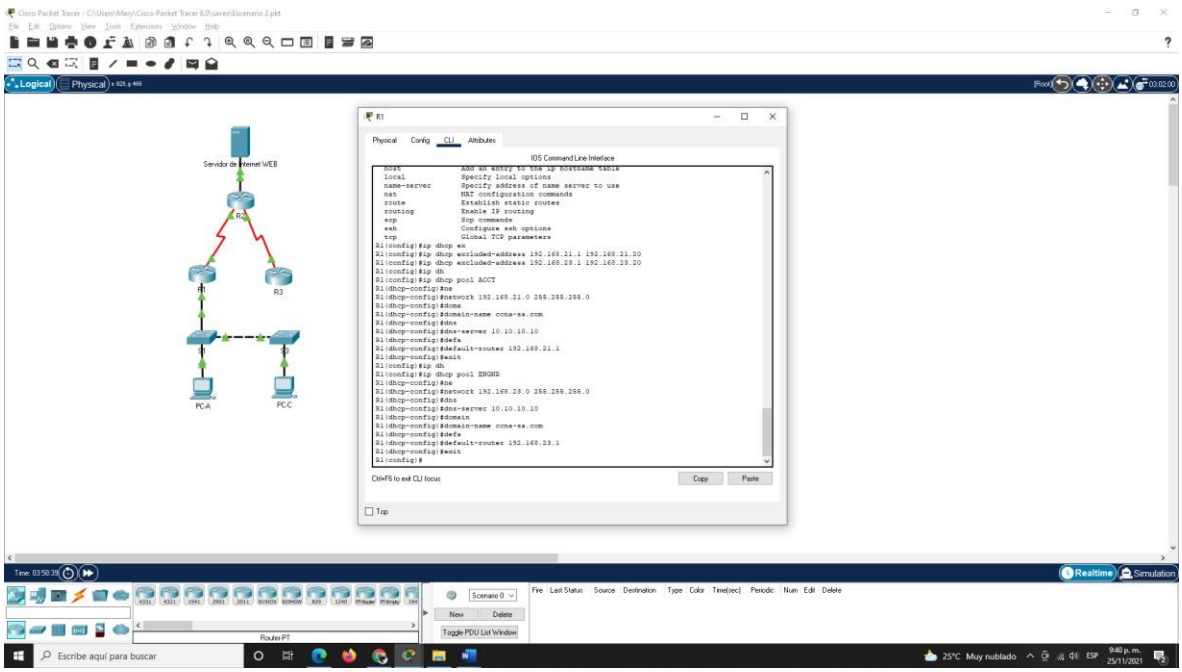
Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 23. Configuracion DHCP en R1

Elemento o tarea de configuración/ Especificación	**Comandos**
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21. / Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna- sa.com Establecer el gateway predeterminado	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#ne R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#doma R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#dns R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#defa R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#exit
Crear un pool de DHCP para la VLAN 23/ Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna- sa.com	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#ne R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#dns R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain R1(dhcp-config)#domain-name ccna-sa.com

Establecer el gateway predeterminado	R1(dhcp-config)#defa R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#exit

Figura 24. Aplicando código en R3



Fuente: Elaboración propia

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

La configuración del R2 incluye las siguientes tareas:

Tabla 24. Configuracion NAT estática y dinámica en R2

Elemento o tarea de configuración/ Especificación	**Comandos**
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 password cisco12345

Habilitar el servicio del servidor HTTP	packet tracer no soporta este comando
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	packet tracer no soporta este comando
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	R2(config)#inter gigabitEthernet 0/0 R2(config-if)#ip nat outside R2(config-if)#exit R2(config)#interfa serial 0/0/0 R2(config-if)#ip nat inside R2(config-if)#exit R2(config)#interfa serial 0/0/1 R2(config-if)#ip nat inside R2(config-if)#exit
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
Defina el pool de direcciones IP públicas utilizables. / Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye:**209.165.200.225** – **209.165.200.228**	R2(config)#ip nat pool INTERNET **209.165.200.225 209.165.200.228** netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

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 25. Verificación protocolo DHCP y la NAT estática

Prueba	**Resultados**
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Exitoso automáticamente se asigna la dirección IP
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Exitoso automáticamente se asigna la dirección IP
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Los pings fueron exitosos
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**	Request Timeout – se agotó el tiempo de espera el Acceso al servidor web no fue satisfactorio debido a que Packet tracer no soporta HTTP en R2

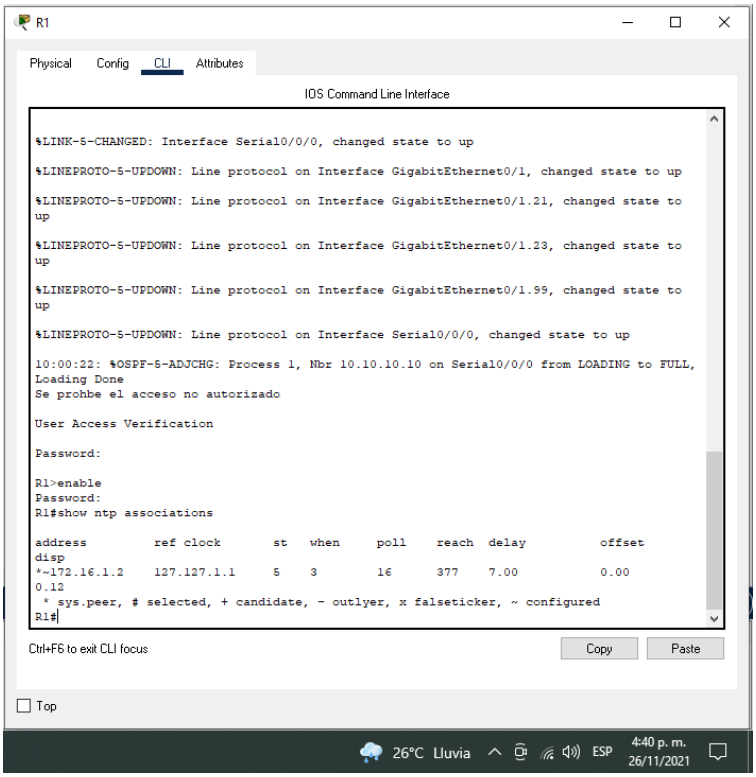
Parte 6: Configurar NTP

Tabla 26. Configuracion protocolo Network Time Protocol en R2

Elemento o tarea de configuración/ Especificación	**Comandos**
Ajuste la fecha y hora en R2./ **5 de marzo de 2016, 9 a. m.**	R2#clock set 09:00:00 05 March 2016
Configure R2 como un maestro NTP./ Nivel de estrato: **5**	R2#configure terminal Enter configuration commands, one per line. End

	with CNTL/Z. R2(config)#ntp master 5
Configurar R1 como un cliente NTP./ Servidor: **R2**	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 associations

Figura 25. Verificación de NTP



Fuente: Elaboración propia

La ejecución de este comando se usa para determinar si NTP (Network Time Protocol) se comunica y si está funcionando correctamente.

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

Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 27. Configuracion listas de control de acceso

Elemento o tarea de configuración / Especificación	**Comandos**
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 - Nombre de la ACL: **ADMIN- MGT**	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#deny any R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4 R2(config-line)#ip access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R2#telnet 172.16.1.2 Trying 172.16.1.2 ...OpenSe prohbe el acceso no autorizado. User Access Verification Password:

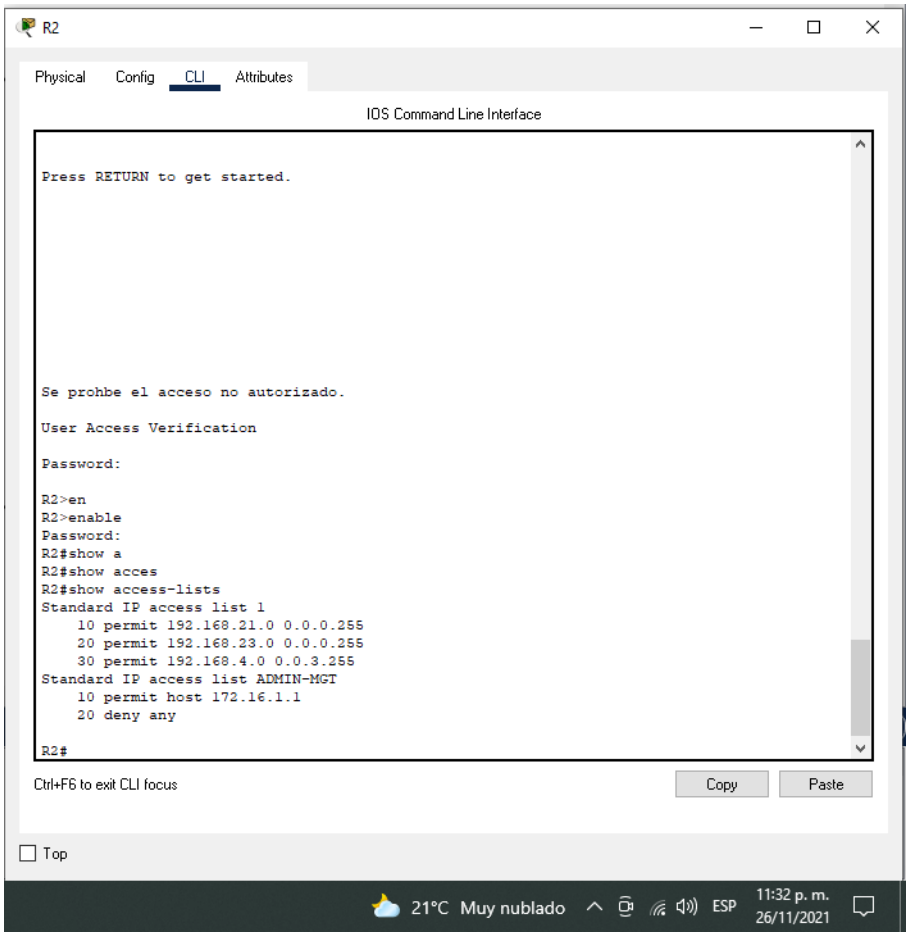
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 28. Verificación ACL

Descripción del comando	**Entrada del estudiante (comando)** Los comandos a continuación se ejecutan en el modo Exec Privilegiado #
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	show access-lists
Restablecer los contadores de una lista de acceso	clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	show run / show ip interface

¿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 *

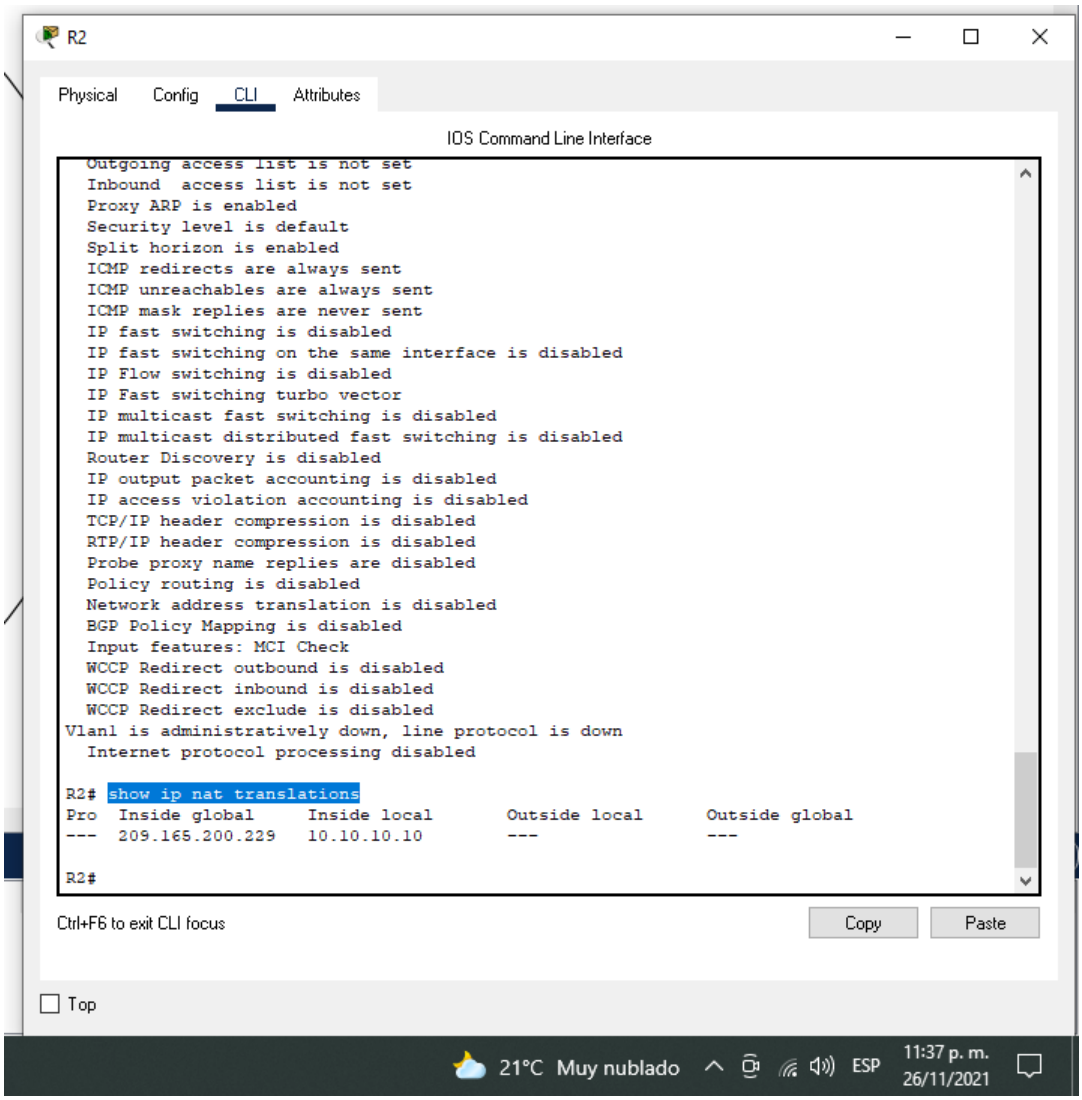
Figura 26. show access-lists en R2



Fuente: Elaboración propia

show access-lists Muestra las coincidencias recibidas por una lista de acceso desde la última vez que se restableció.

Figura 27. show ip nat translations en R2

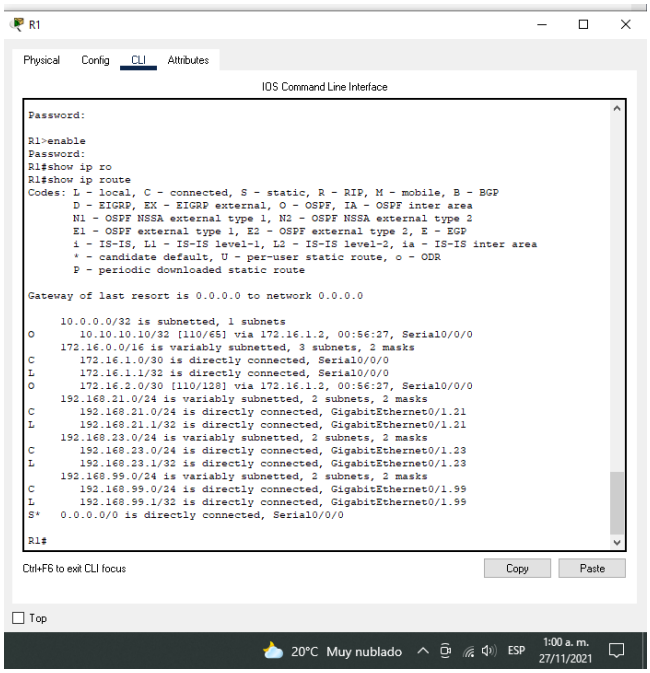


Fuente: Elaboración propia

show ip nat translations muestran las traducciones NAT

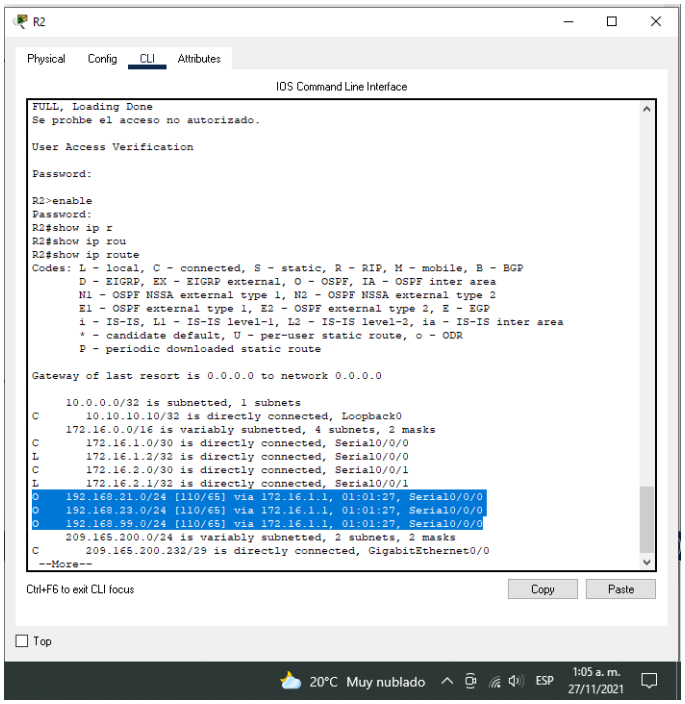
A continuación, se ejecuta el comando **show ip route** el cual muestra las configuraciones de las direcciones Ip asignadas de la red, las configuraciones directamente conectadas y la interfaz respectiva. Igualmente, las conectadas usando el protocolo OSPF (Open Shortest Path First).

Figura 28. show ip route en R1



Fuente: Elaboración propia

Figura 29. show ip route en R2



Fuente: Elaboración propia

CONCLUSIONES

Packet tracer es una herramienta de simulación que nos permite realizar la construcción de una red, la configuración de dispositivos Routers y Switches mediante Consola u otro tipo de acceso, la configuración de direccionamiento de los hosts entre muchas más opciones,

Packet Tracer es de gran utilidad tanto en el proceso formativo como en la práctica para administrar una red y detectar fallas.

Se resalta la importancia de la configuracion de los parámetros básicos de seguridad de todos los dispositivos routers y switches lo relacionado a establecer contraseñas en los modos Exec Privilegiado, telnet y consola, encriptación de contraseñas y la configuracion de un banner Motd.

En cuanto a seguridad Si bien se desactivan los puertos sin utilizar en los switches es recomendable como medida de seguridad ejecutar el comando **switchport nonegotiate** con el fin de desactivar la auto negociación debido que las troncales de los switches Cisco están en auto negociación, entonces se pueden encender y establecer un enlace troncal.

BIBLIOGRAFIA

Vesga, J. (2017). Ping y Tracer como estrategia en los procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3

CISCO. (2019). Acceso a la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4

CISCO. (2019). Ethernet. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5

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

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

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

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

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

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

CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10