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

JONATHAN FERNANDO RAMIREZ VALENCIA

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

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

JONATHAN FERNANDO RAMIREZ VALENCIA

Diplomado de opción de grado presentado para optar el título de
Ingeniero de Sistemas

Asesora:
Magister MARIA ALEJANDRA LOPEZ HURTADO

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

CÚCUTA, 28 de noviembre de 2021

DEDICATORIA

Este trabajo está dedicado a Dios, a mi familia, en especial a mi esposa que me brinda gran motivación para lograr todas mis metas establecidas, a mis docentes de la UNAD. Este es el resultado de estudiar el plan de ingeniería de sistemas y el curso de profundización de Cisco.

AGRADECIMIENTOS

Después de un potente período de cuatro meses, hoy es el día en el que escribo este apartado de agradecimientos para concluir mi proyecto de fin de grado. Ha sido una época de aprendizaje intenso no solo en el campo académico sino también a nivel personal. Escribir este trabajo ha tenido un gran impacto en mi persona y por ello me gustaría dar las gracias a todas aquellas personas que me han ayudado y apoyado durante este proceso.

En primer lugar, me gustaría agradecer a mis compañeros de prácticas, por su colaboración. Me han dado todo su apoyo enormemente y siempre han estado ahí para ayudarme cuando lo he necesitado.

Además, me gustaría dar las gracias a mis tutores por su valiosa ayuda. Definitivamente me han ofrecido todas las herramientas necesarias para completar mi proyecto de fin de grado de forma satisfactoria.

También me gustaría agradecer a mi esposa y a mis padres por sus sabios consejos y su comprensión. Siempre han estado ahí cuando los he necesitado. Finalmente, mis amigos. No solo han estado a mi lado para apoyarnos entre nosotros en los momentos más complicados, sino que también hemos tenido conversaciones sobre otras cosas no relacionadas con universidades y artículos académicos.

CONTENIDO

LISTADO DE TABLAS

LISTADO DE FIGURAS

GLOSARIO

DNS: La sigla DNS proviene de la expresión inglesa Domain Name System: es decir, Sistema de Nombres de Dominio. Se trata de un método de denominación empleado para nombrar a los dispositivos que se conectan a una red a través del IP (Internet Protocol o Protocolo de Internet).

INTERFAZ: Se denomina interfaz a cualquier medio que permita la interconexión de dos procesos diferenciados con un único propósito común. Se conoce como Interfaz Física a los medios utilizados para la conexión de un computador con el medio de transporte de la red.

MÁSCARA DE SUBRED: La máscara de subred es particularmente necesaria al momento de señalar la dirección de red correspondiente a cada subred, y que es la que se encuentra referenciada en la tabla de enrutamiento.

PREFIJO IP: Es una forma particular de expresar las direcciones de red y sus máscaras a partir de identificar solamente la cantidad de bits que se encuentran en uno en la máscara de subred.

PROTOCOLOS DE RED: Los protocolos de red son un conjunto de reglas que gobiernan la comunicación entre dispositivos que están conectados a una red. Dichas reglas se constituyen de instrucciones que permiten a los dispositivos identificarse y conectarse entre sí, además de aplicar reglas de formateo, para que los mensajes viajen de la forma adecuada de principio a fin. Dichas reglas de formateo determinan si los datos son recibidos correctamente o si son rechazados o ha habido algún tipo de problema en la transferencia de la información.

ROUTER: Dispositivo hardware o software de interconexión de redes de computadores que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras.

RESUMEN

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

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.

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

PALABRAS CLAVE: CISCO, Conmutación, Enrutamiento, Redes, Sistemas.

ABSTRACT

The evaluation called "Test of practical skills" is part of the evaluative activities of the CCNA Deepening Diploma, and seeks to identify the degree of development of skills and abilities that were acquired throughout the diploma. The essential thing is to test the levels of understanding and problem solving related to various aspects of Networking.

In this first scenario, the devices of a small network will be configured. You must configure a router, a switch and equipment, design the IPv4 addressing scheme for the proposed LANs. The router and switch must also be managed securely.

For the second scenario, a small network must be configured to support IPv4 and IPv6 connectivity, switch security, inter-VLAN routing, OSPF dynamic routing protocol, Dynamic Host Configuration Protocol (DHCP), address translation dynamic and static network (NAT), access control lists (ACL), and network time protocol (NTP) server / client. During the evaluation, you will test and register your network using common CLI commands.

KEY WORDS: CISCO, Switching, Routing, Networks, Systems.

INTRODUCCIÓN

El contenido de este documento tiene como fin desarrollar el escenario 1 como avance documento final de grado del Diplomado de Profundización Cisco respecto a la guía de actividades entregada por la UNAD en el entorno aprendizaje unidad 5 paso 6, aplicando los conceptos aprendidos en el curso en línea El desarrollo del primer ejercicio nos ayudara a mejorar las competencias mediante el uso adecuado de estrategias basadas en comandos del IOS y estadísticas de tráfico en las interfaces. Adicional a esto se desarrolló simulación del ejercicio propuestos en el simulador PACKET TRACER.

La solución de este ejercicio nos brindara un conocimiento en el uso de comandos de configuración ya que con las simulaciones aprendemos a usarlos correctamente, así como los niveles de seguridad que se pueden configurar para diseñar soluciones tecnológicas innovadoras para satisfacer las necesidades de las compañías.

Teniendo en cuenta que la Prueba de habilidades está conformada por dos (2) escenarios, el estudiante deberá realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: Packet Tracer o GNS3.

Al final, cada proceso está debidamente documentado y consta de una evidencia que determina la operación y aplicación de cada una de las instrucciones requeridas para el cumplimiento de lo solicitado en cada uno de los escenarios y además de verificar el funcionamiento y el comportamiento de la red a medida que se va implementando cada uno de los cambios y configuración de los dispositivos.

DESARROLLO

Escenario 1

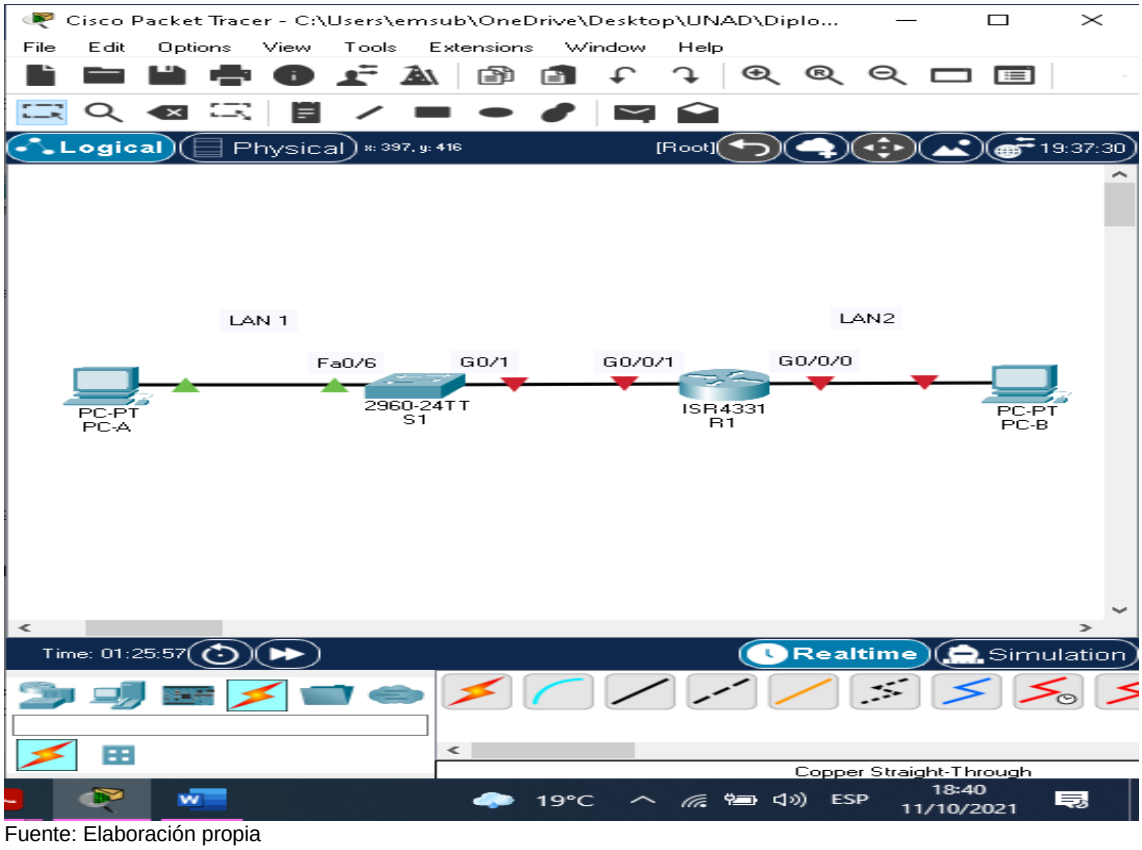
Topología

Figura 1: Topología escenario 1

Fuente: PRUEBA DE HABILIDADES CCNA II-2021

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.

Figura 2: topología en PT.



Fuente: Elaboración propia

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 swich S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts)

Parte 1: Construya la Red

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

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.

Tabla 1: Tabla de direccionamiento

Item	Requerimiento
Dirección de red	192.168.22.0
Requerimiento de host LAN 1	100 (126)
Requerimiento de host LAN 2	50 (62)
R1 G0/0/1	192.168.22.1
R1 G0/0/0	192.168.22.129
S1 SVI	192.168.22.2
PC-A	192.168.22.126
PC-B	192.168.22.190

Fuente: Elaboración propia

Mi número de CC es 1.073.322.122 = 192.168.22.0

Entonces la red quedaría de la siguiente manera 192.168.22.0/24, el 24 es porque los primeros 3 puntos van a estar encendidos, esta red la vamos a dividir en dos subredes las cuales van a quedar cada una con 126 host, ya que por cada subred se reservan dos para la red y el broadcast.

Como en la Lan 2 solo necesitamos 50 host procederemos a dividir la segunda red en dos redes mas cada una con 64 host y 62 utilizables quedando una red disponible para futuro ampliación de la red.

En este orden de ideas la red quedaría así:

IP: 192.168.22.0 LAN1
Mascara: 255.255.255.0 /24 Bits
Sub mascara: 255.255.255.128 /25 Bits

IP: 192.168.22.128 LAN2
Mascara: 255.255.255.128 /25 Bits
Sub mascara: 255.255.255.192 /26 Bits

Tabla 2: Subneteo de redes requeridas.

No	Red	Rango Host	Broadcast
1	**192.168.22.0/25**	**192.168.22.1--192.168.22.126**	**192.168.22.127**
2	**192.168.22.128/26**	**192.168.22.129--192.168.22.190**	**192.168.22.191**

Fuente: Elaboración propia

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: Configuraciones R1

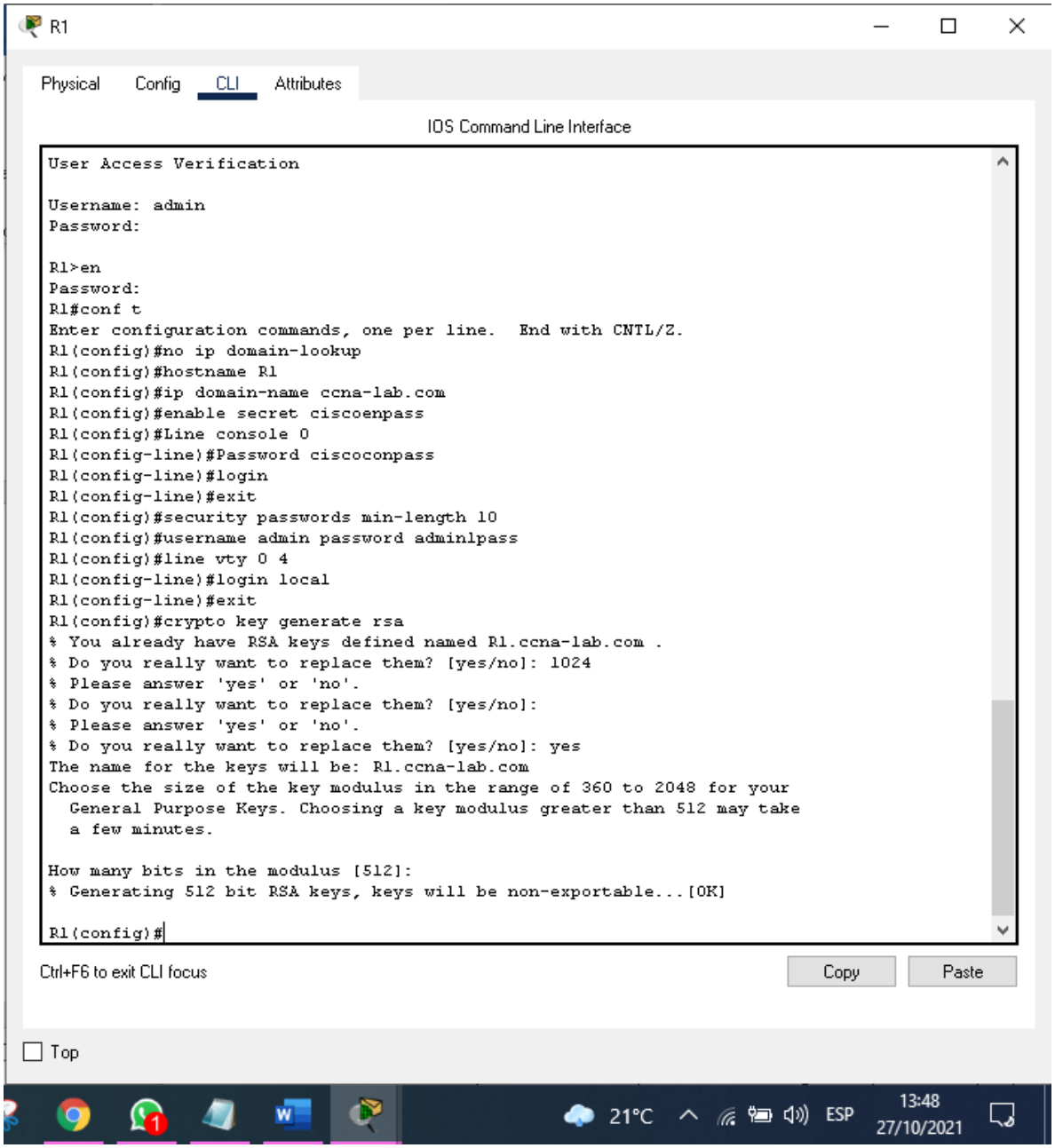
Tarea	Especificación
Desactivar la búsqueda DNS	R1>enable R1#configure terminal R1(config)#no ip domain-lookup
Nombre del router	R1(config)#hostname R1

Nombre de dominio	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC Privilegiado	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config)#Line console 0 R1(config-line)#Password ciscoconpass R1(config-line)#login 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**
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)#login local R1(config-line)#exit R1(config)#
Configurar VTY solo aceptando SSH	R1(config)#hostname R1 R1(config)#ip domain-name ccna-lab.com 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)#ip ssh version 2 *Mar 5 1:18:9.131: %SSH-5-ENABLED: SSH 1.99 has been enabled R1(config)#line vty 0 15 R1(config-line)#login local R1(config-line)#exit R1(config)#username admin password admin1pass R1(config)#exit R1#

	%SYS-5-CONFIG_I: Configured from console by console R1#
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd $SOLO PERSONAL DE LA UNAD!$
Configurar interfaz G0/0/0	R1(config)#interface gigabitethernet 0/0/0 R1(config-if)#ip address 192.168.22.129 255.255.255.128 R1(config-if)#no shutdown R1(config-if)#exit
Configurar interfaz G0/0/1	R1(config)#interface gigabitethernet 0/0/1 R1(config-if)#ip address 192.168.22.1 255.255.255.0 R1(config-if)#no shutdown R1(config-if)#exit
Generar una clave de cifrado RSA	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]

Fuente: Elaboración propia

Figura 3: Configuraciones R1



Fuente: Elaboración propia

Figura 4: Configuraciones R1

Fuente: Elaboración propia

Las tareas de configuración de S1 incluyen lo siguiente:

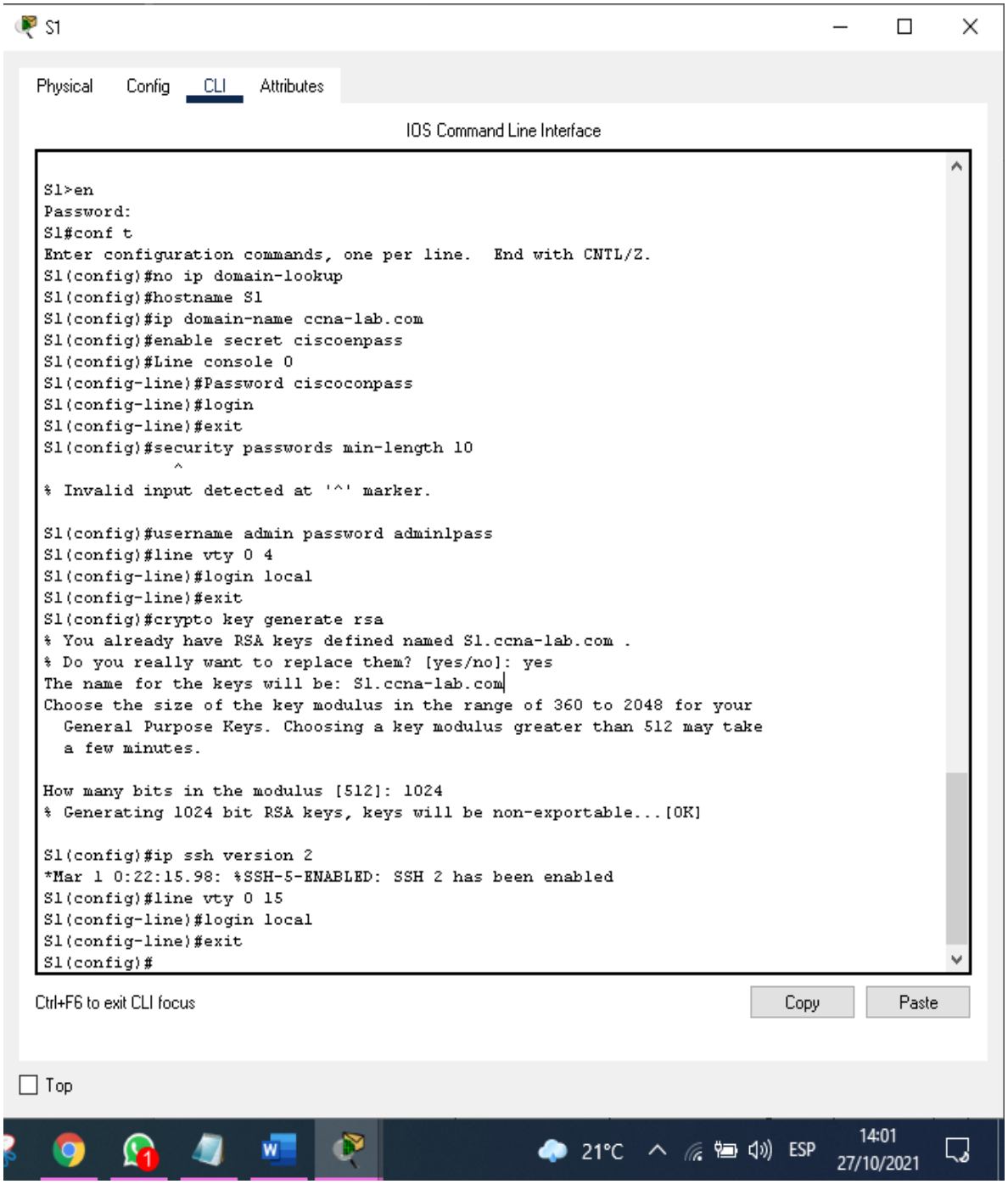
Tabla 4: configuración S1

Tarea	Especificación
Desactivar la búsqueda DNS	S1>enable S1#configure terminal S1(config)#no ip domain-lookup
Nombre del switch	S1(config)#hostname S1
Nombre de dominio	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC Privilegiado	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#Line console 0 S1(config-line)#Password ciscoconpass S1(config-line)#login S1(config-line)#exit
Establecer la longitud mínima para las Contraseñas	S1(config)#security passwords min-length 10 10 caracteres
Crear un usuario administrativo en la base de datos local	R1#configure terminal R1(config)#username **admin** password **admin1pass**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1#configure terminal S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line)#exit S1(config)#
Configurar VTY solo aceptando SSH	S1(config)#hostname S1 S1(config)#ip domain-name ccna-lab.com S1(config)#crypto key generate rsa The name for the keys will be: S1.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] S1(config)#ip ssh version 2 *Mar 5 1:22:19.227: %SSH-5-ENABLED: SSH 1.99 has been enabled

	S1(config)#line vty 0 15 S1(config-line)#login local S1(config-line)#exit S1(config)#username admin password admin1pass S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console S1#
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configure un MOTD Banner	S1(config)#banner motd $SOLO PERSONAL DE LA UNAD!$
Configurar la interfaz de administración (SVI)	S1(config)#int vlan 1 S1(config-if)#ip address 192.168.22.2 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#exit
Generar una clave de cifrado RSA	S1(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]
Configuración del gateway predeterminado	S1(config)#ip default-gateway 192.168.22.1

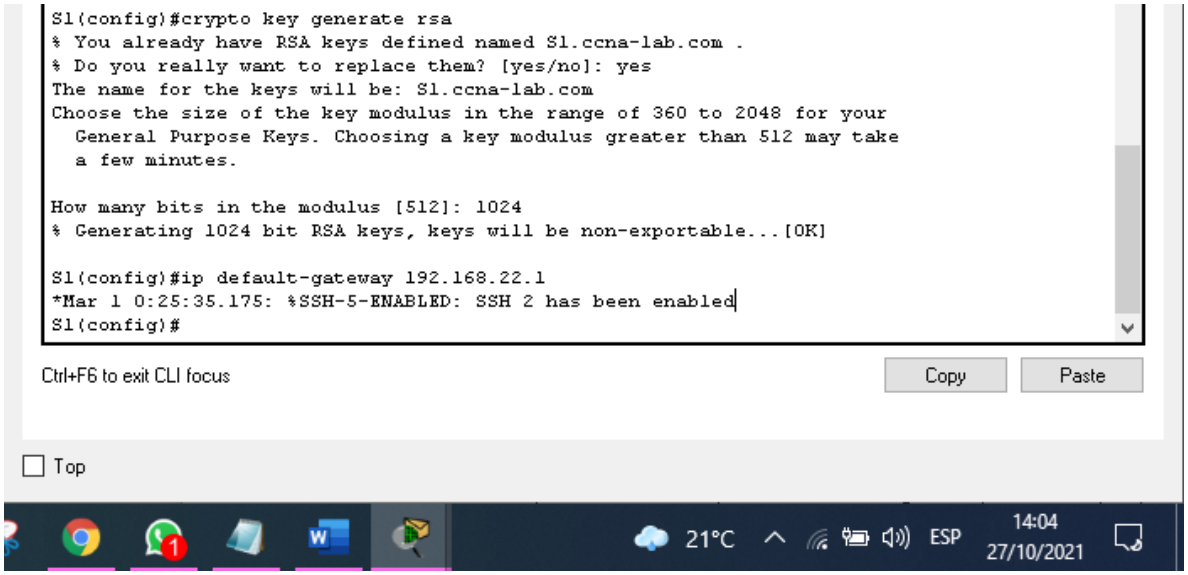
Fuente: Elaboración propia

Figura 5: Configuraciones S1



Fuente: Elaboración propia

Figura 6: Configuraciones S1



Fuente: Elaboración propia

Paso 2. Configurar los equipos

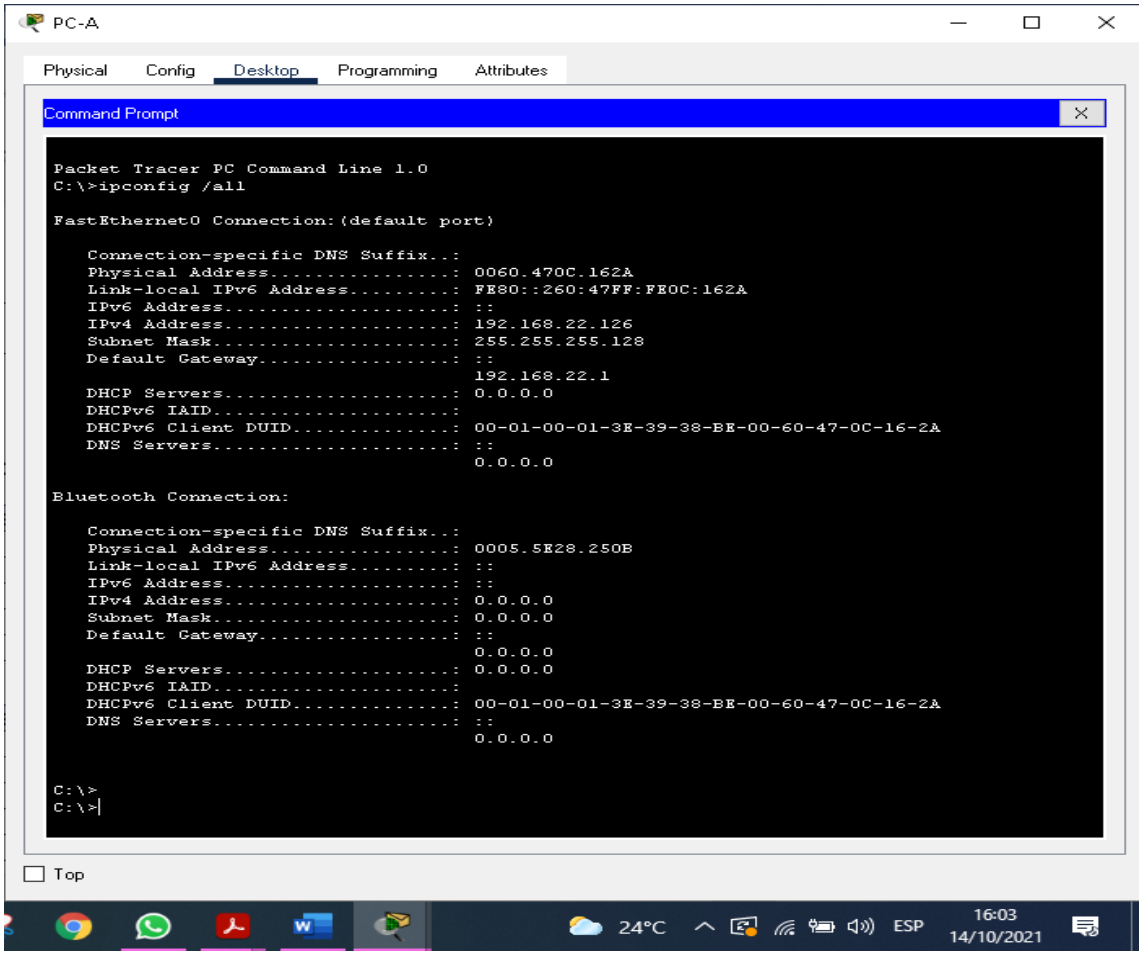
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando ipconfig /all.

Tabla 5: configuración PC-A

PC-A Network Configuration	
Descripción	Este PC-A esta conectado a una red la cual cuenta con 126 host utilizables, esta conectado al ultimo host como su dirección ip, su puerta de enlace es la ip conexión del R1 en el g0/0/1 192.168.22.1
Dirección física	0060.470C.162A
Dirección IP	192.168.22.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.22.1

Fuente: Elaboración propia

Figura 7: comando ipconfig /all en PC-A



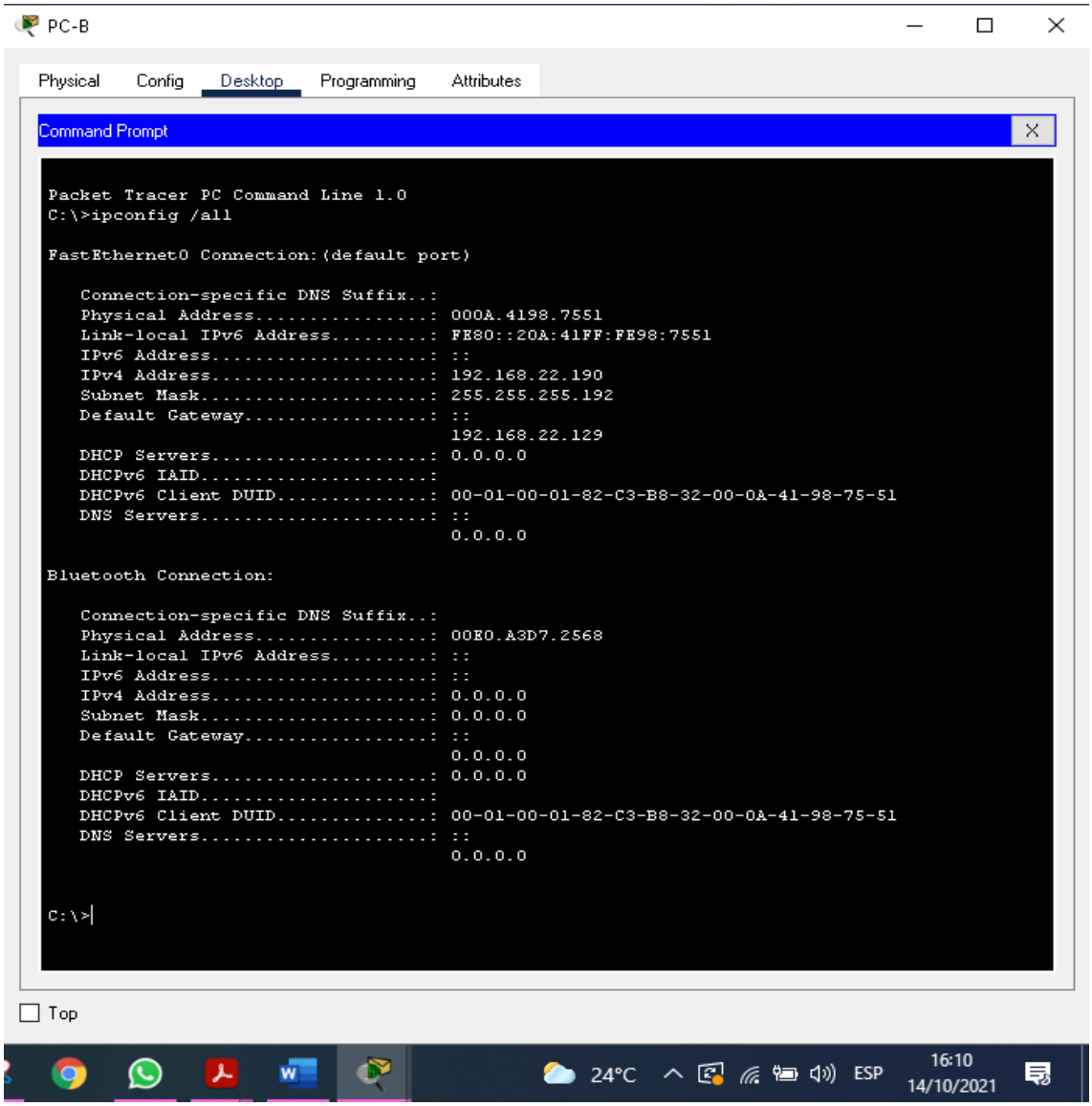
Fuente: Elaboración propia

Tabla 6: configuración PC-B

PC-B Network Configuration	
Descripción	Este PC-B esta conectado a una red la cual cuenta con 62 host utilizables, esta conectado al ultimo host como su dirección ip, su puerta de enlace es la ip conexión del R1 en el g0/0/0 192.168.22.129
Dirección física	000A.4198.7551
Dirección IP	192.168.22.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.22.129

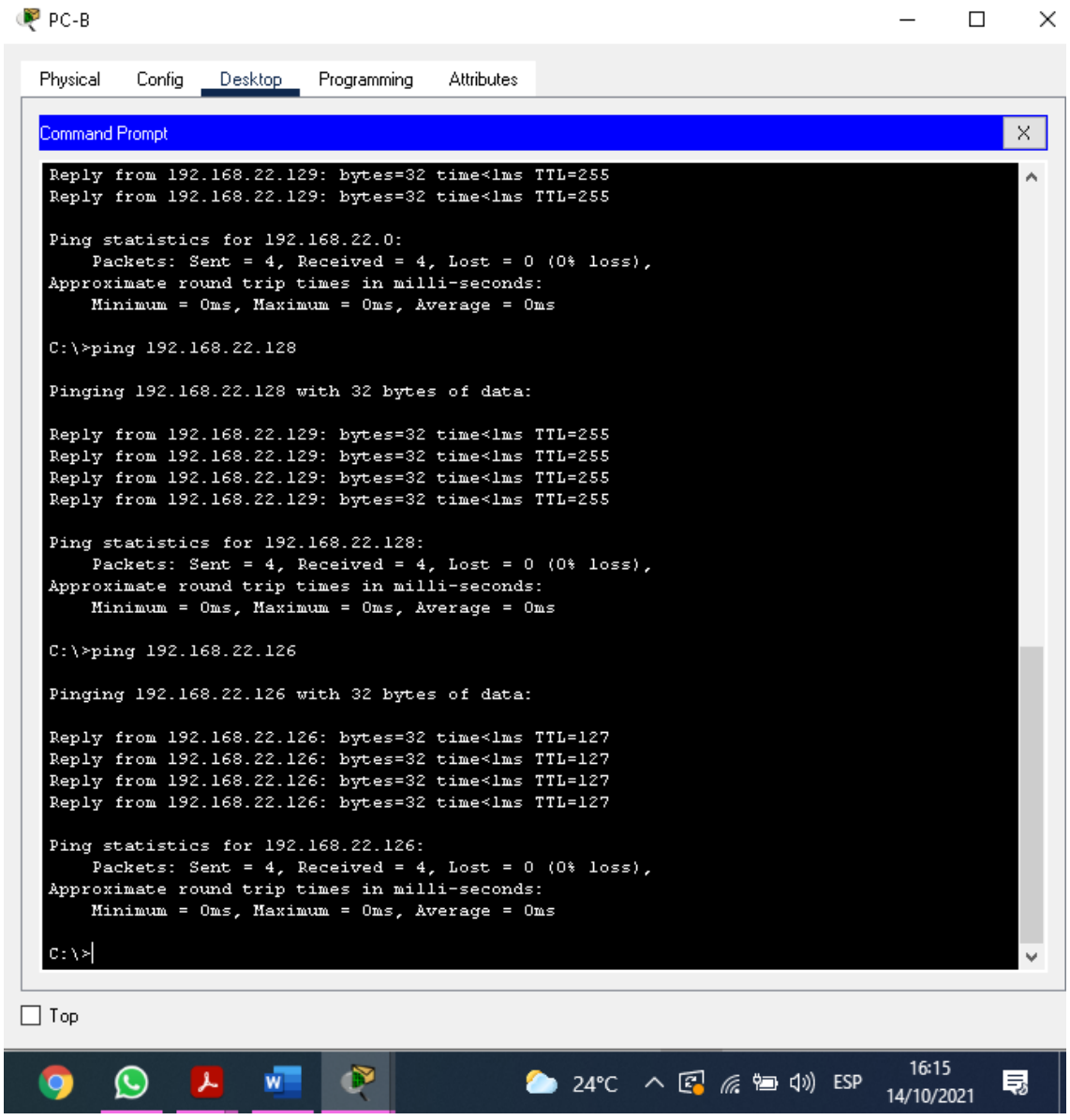
Fuente: Elaboración propia

Figura 8: comando ipconfig /all en PC-B



Fuente: Elaboración propia

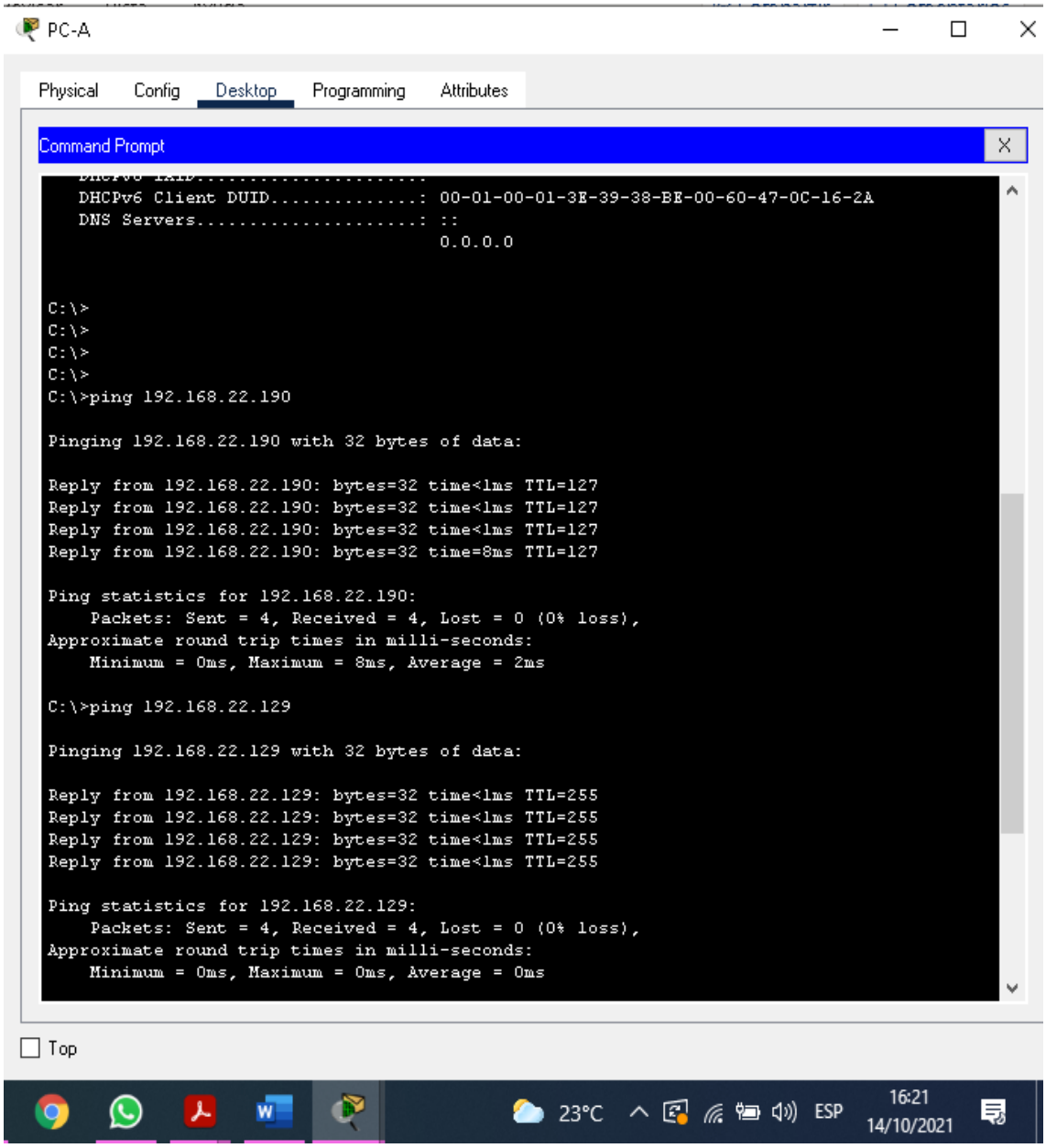
Figura 9: ping PC-B a PC-A



Fuente: Elaboración propia

Desde el PC-B se realiza ping al PC-A y demás IP de la topografía con 0 perdidas y envió de paquetes completos.

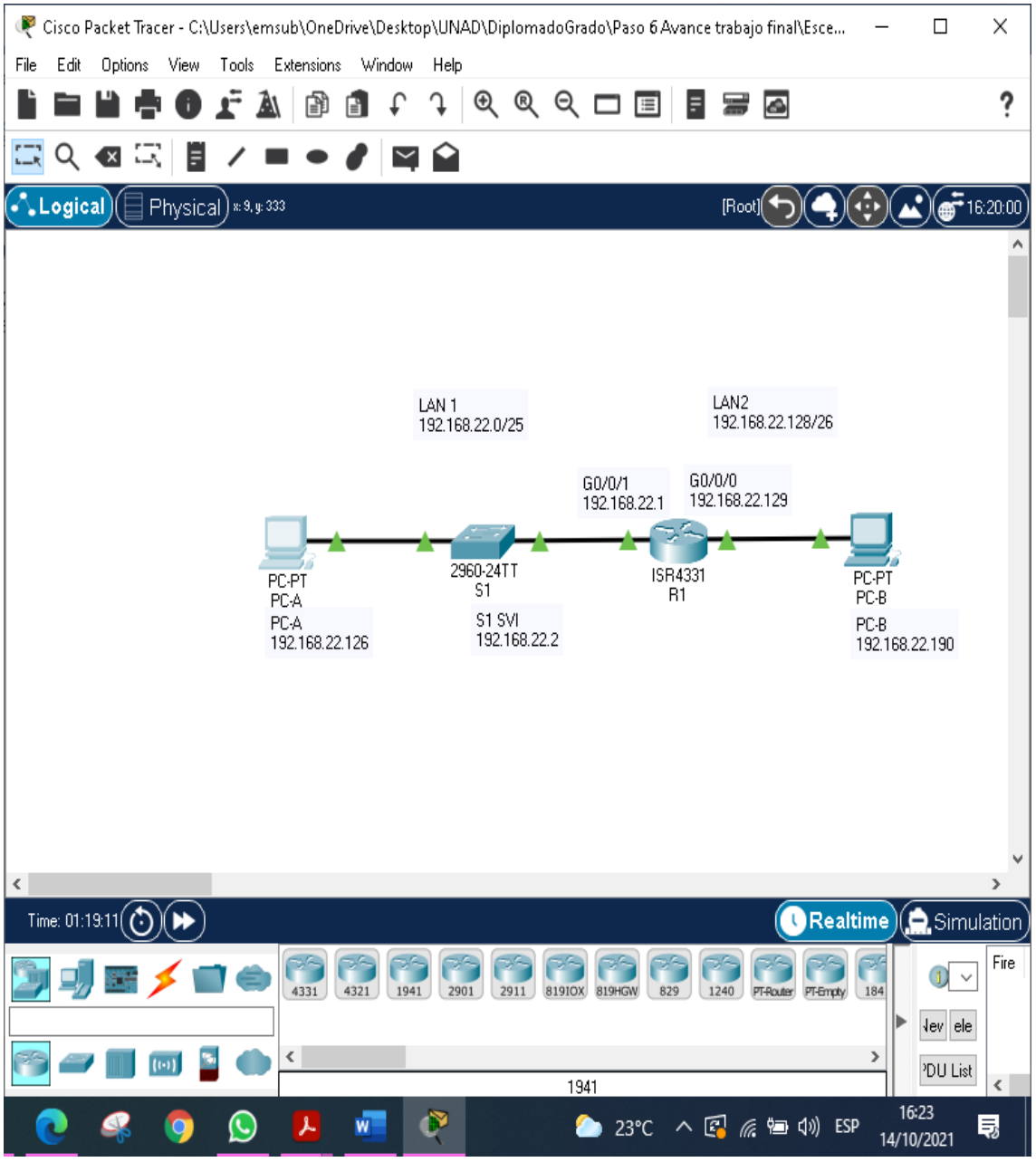
Figura 10: ping PC-A a PC-B



Fuente: Elaboración propia

Con el PC-A se realiza ping al PC-B y las puetas de enlace del Router todas con 0 perdidas de paquetes.

Figura 11: Topología escenario 1 completamente funcional.

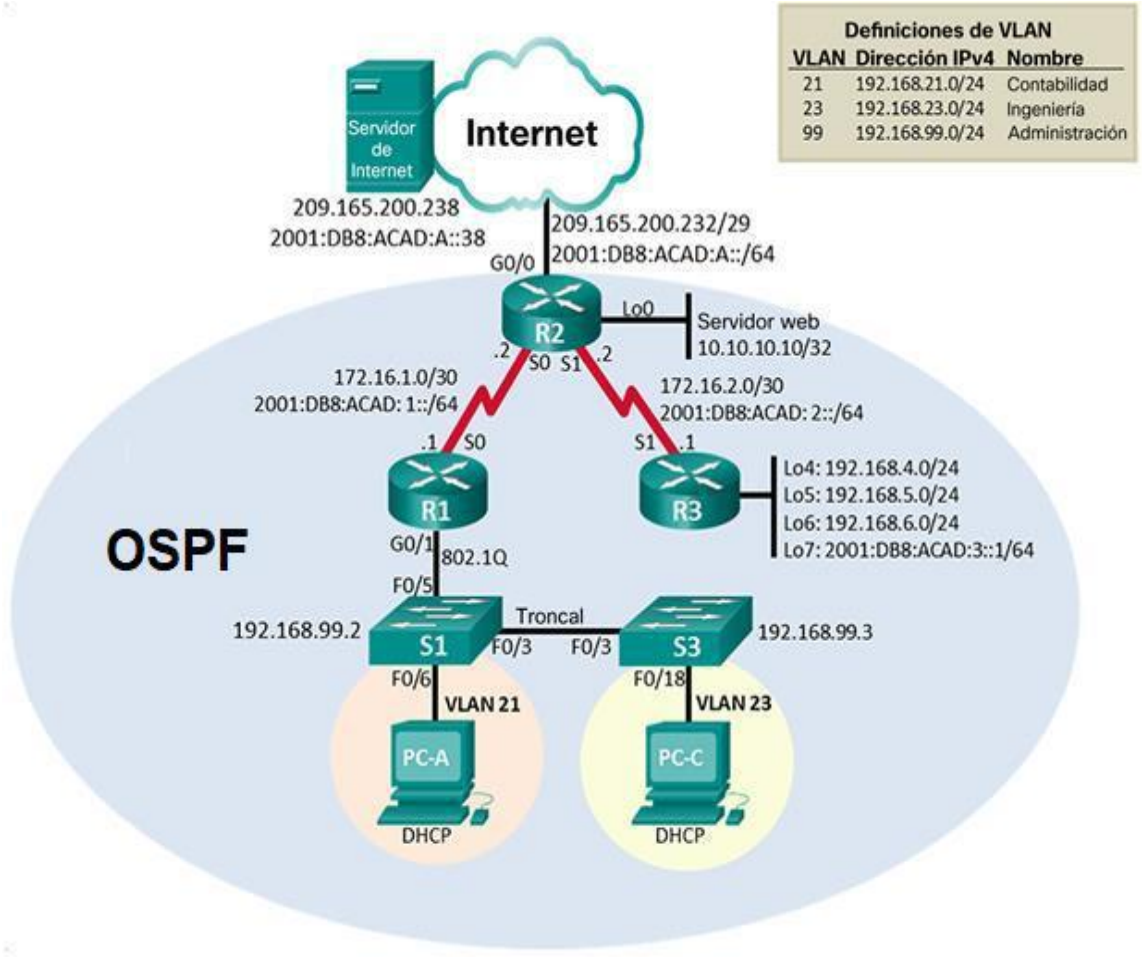


Fuente: Elaboración propia

Escenario 2

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

Figura 12: Topología escenario 2.



Fuente: PRUEBA DE HABILIDADES CCNA II-2021

Parte 1: Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los routers y los switches
Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

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

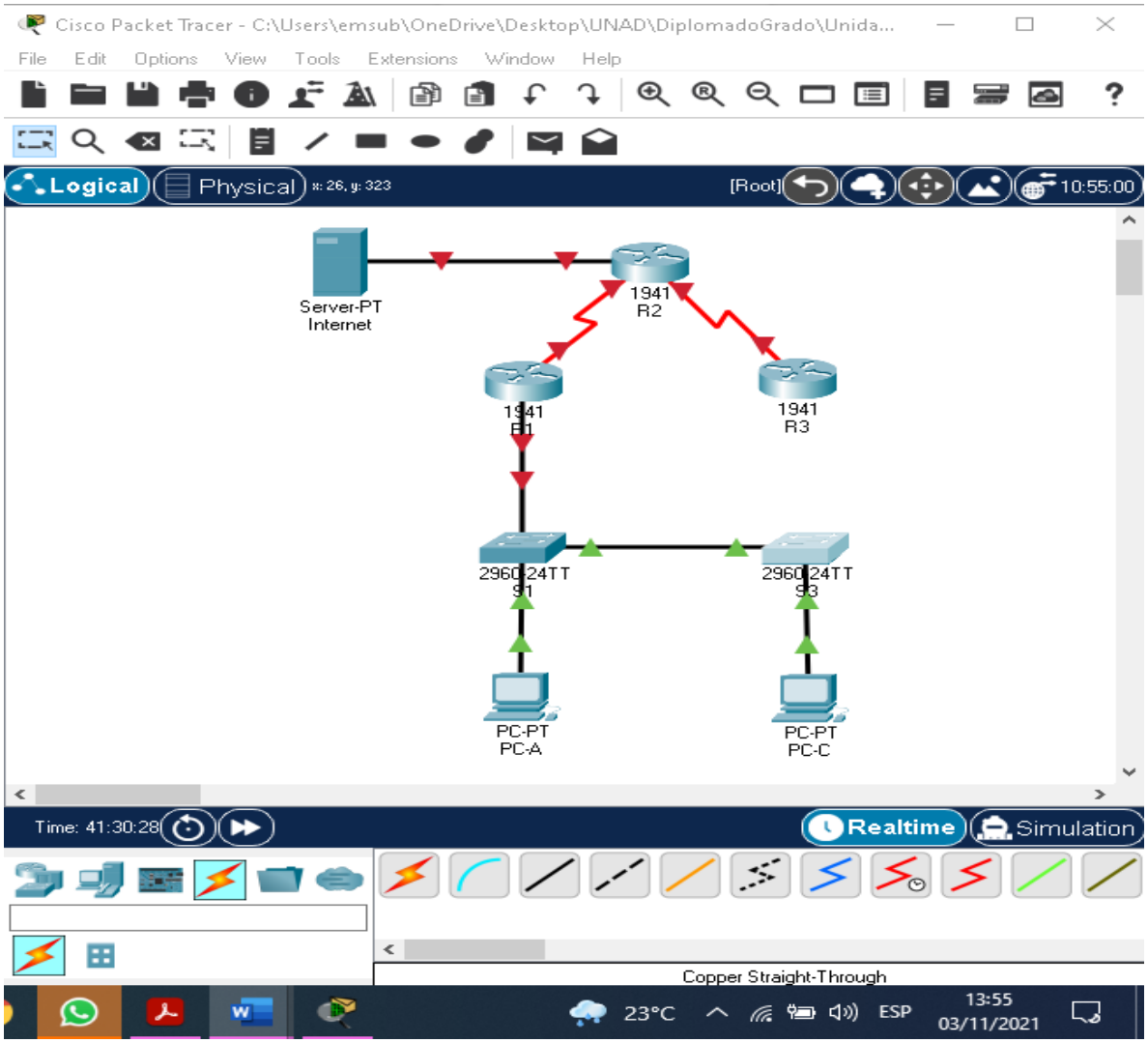
Tabla 7: inicialización de Routers y Switches.

Tarea	Comando de IOS
Eliminar el archivo startup-configde todos los routers	Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete Router#
Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm]
Eliminar el archivo startup-configde todos los switches y eliminar la base de datos de VLAN anterior	Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete Switch#
Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm]
Verificar que la base de datos deVLAN no esté en la memoria flash en ambos switches	Switch#show flash: Directory of flash:/ 1 -rw- 4670455 <no date> 2960-lanbasek9-mz.150-2.SE4.bin 64016384 bytes total

	(59345929 bytes free) Switch#

Fuente: Elaboración propia

Figura 13: Topología escenario 2 PT.



Fuente: Elaboración propia

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

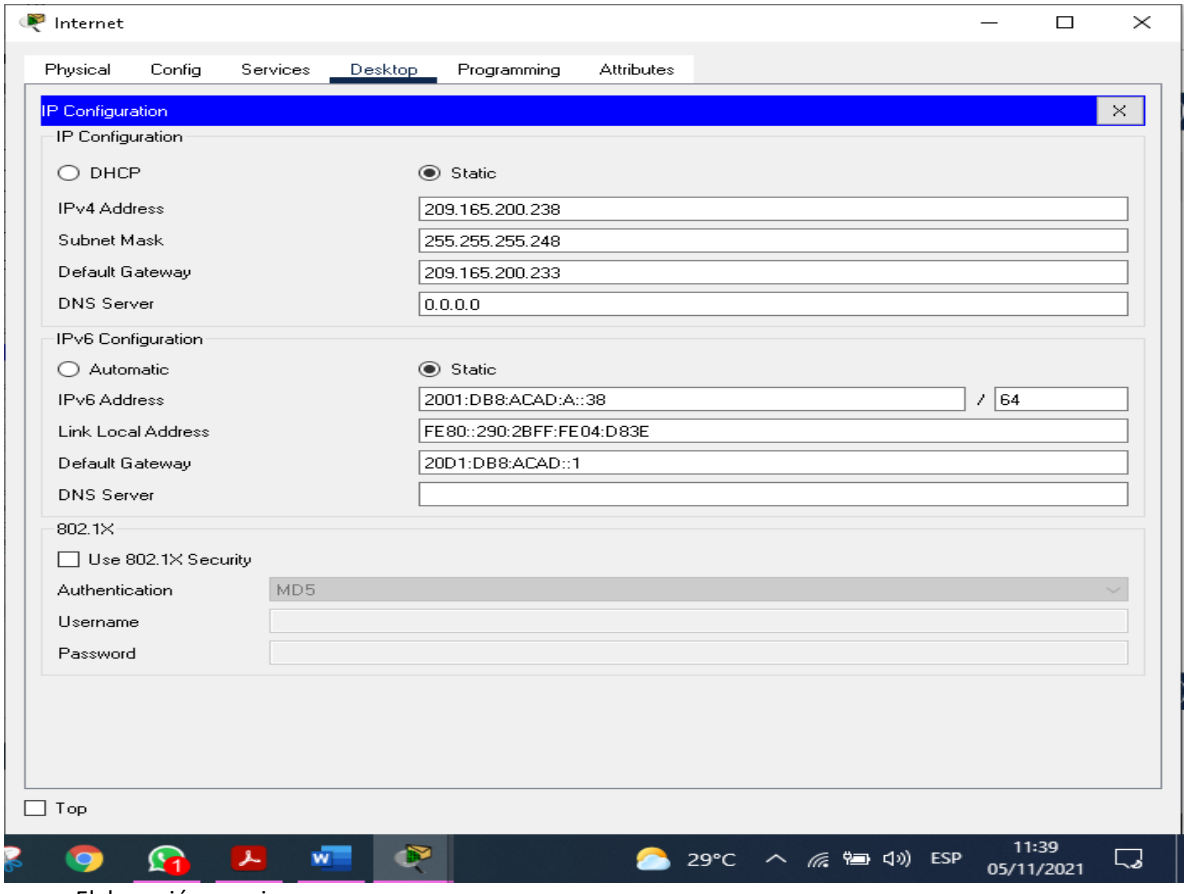
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 8: Configurar la computadora 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::1

Fuente: Elaboración propia

Figura 14: Configurar la computadora de Internet



Fuente: Elaboración 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.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 9: Configuraciones R1

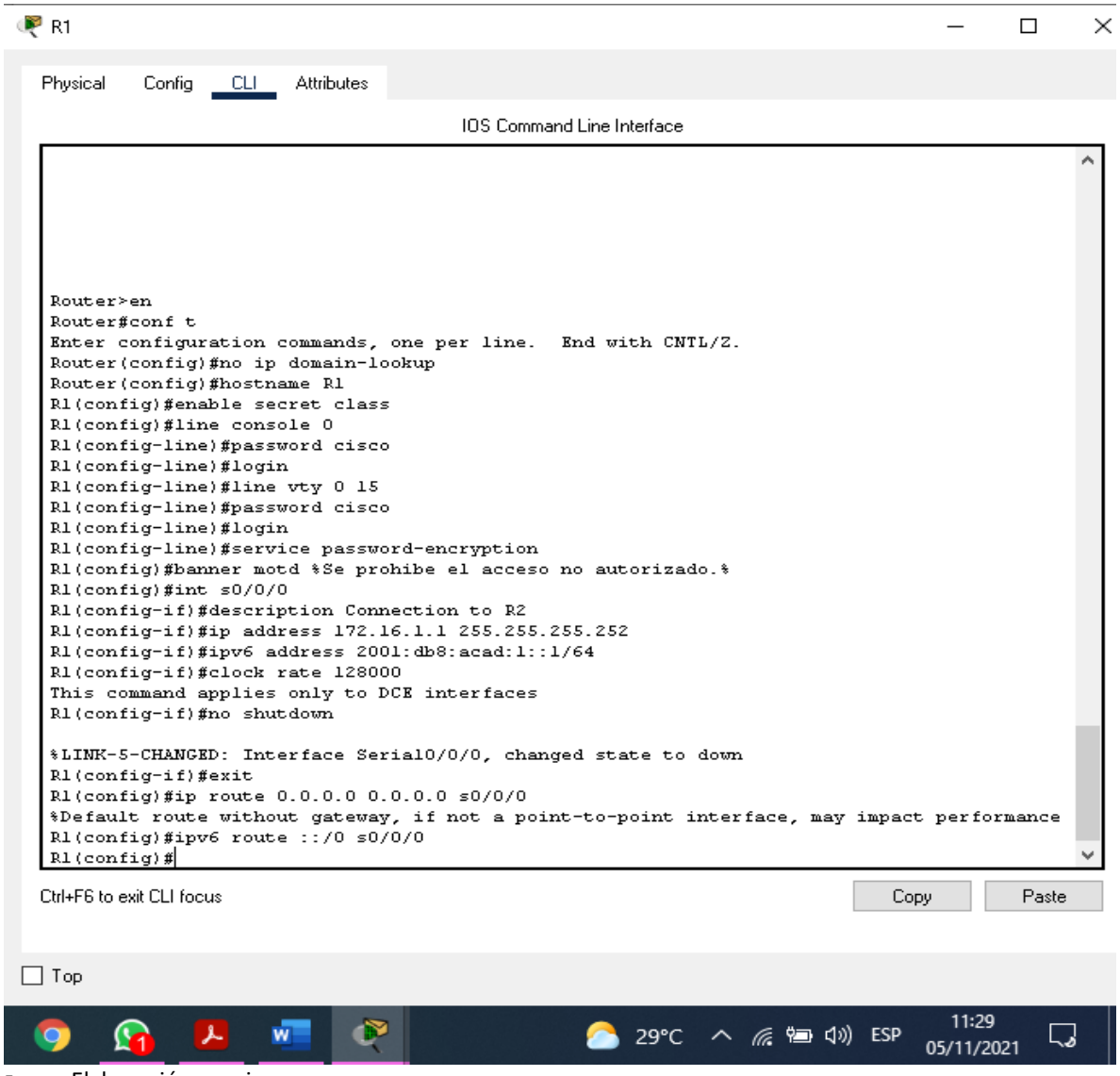
Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line con 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#passwordcisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)# banner motd %Se prohibe el acceso no autorizado.%
Interfaz S0/0/0	R1(config)#int s0/0/0 R1(config-if)#description Connection to R2 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)#clock rate 128000 R1(config-if)#no shutdown %LINK-5-CHANGED: Interface Serial0/0/0, changed state to down R1(config-if)#exit

Rutas predeterminadas	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 R1(config)#

Fuente: Elaboración propia

Nota: Todavía no configure G0/1.

Figura 15: Configuraciones R1



Fuente: Elaboración propia

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#service password-encryption
R1(config)#banner motd %Se prohibe el acceso no autorizado.%
R1(config)#int s0/0/0
R1(config-if)#description Connection to R2
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)#clock rate 128000
This command applies only to DCE interfaces
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit
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
R1(config)#
```

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 10: Configuraciones R2

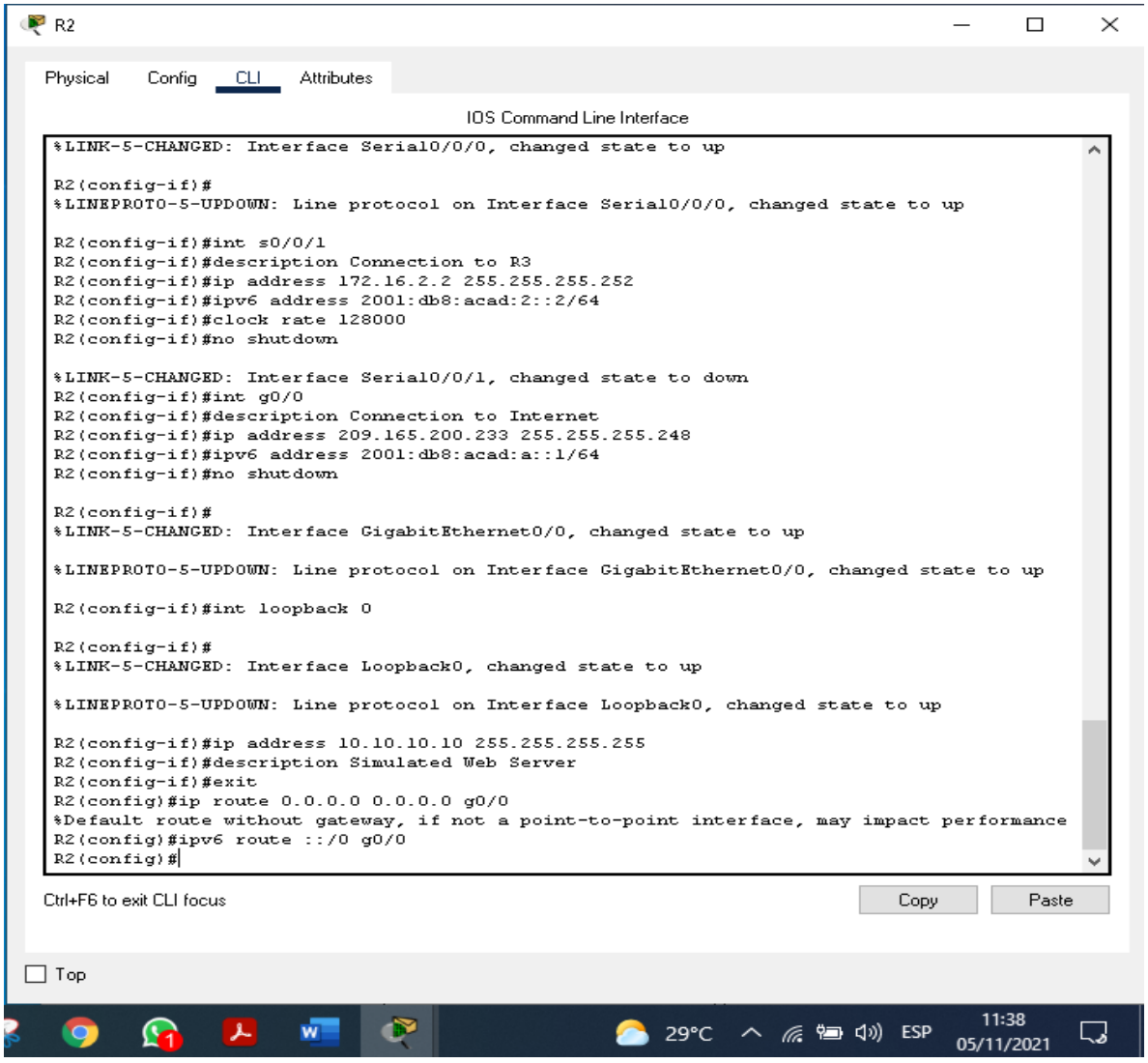
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class

Contraseña de acceso a la consola	R2(config)#line con 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	R2(config)#ip http server (No soportado)
Mensaje MOTD	R2(config)# banner motd %Se prohibe el acceso no autorizado.%
Interfaz S0/0/0	R2(config)#int s0/0/0 R2(config-if)#description Connection to R1 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)#no shutdown R2(config-if)# %LINK-5-CHANGED: Interface Serial0/0/0, changed state to up R2(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Interfaz S0/0/1	R2(config-if)#int s0/0/1 R2(config-if)#description Connection to R3 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)#clock rate 128000 R2(config-if)#no shutdown %LINK-5-CHANGED: Interface Serial0/0/1, changed state to down

Interfaz G0/0 (simulación de Internet)	R2(config-if)#int g0/0 R2(config-if)#description Connection to Internet 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)#no shutdown R2(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
Interfaz loopback 0 (servidor web simulado)	R2(config-if)#int loopback 0 R2(config-if)# %LINK-5-CHANGED: Interface Loopback0, changed state to up %LINEPROTO-5-UPDOWN: Line Interface Loopback0, changed state to up R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description Simulated Web Server R2(config-if)#exit
Ruta predeterminada	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)#ipv6 route ::/0 g0/0 R2(config)#

Fuente: Elaboración propia

Figura 16: Configuraciones R2



Fuente: Elaboración propia

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 15
R2(config-line)#password cisco
```

```
R2(config-line)#login
R2(config-line)#service password-encryption
R2(config)#ip http server
           ^
% Invalid input detected at '^' marker.

R2(config)#banner motd %Se prohibe el acceso no autorizado.%
R2(config)#int s0/0/0
R2(config-if)#description Connection to R1
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)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R2(config-if)#int s0/0/1
R2(config-if)#description Connection to R3
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)#clock rate 128000
R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#int g0/0
R2(config-if)#description Connection to Internet
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)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R2(config-if)#int loopback 0

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#description Simulated Web Server
R2(config-if)#exit
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)#ipv6 route ::/0 g0/0
R2(config)#

Paso 4: Configurar R3
La configuración del R3 incluye las siguientes tareas:

Tabla 11: Configuraciones R3

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 con 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 prohibe el acceso no autorizado.%

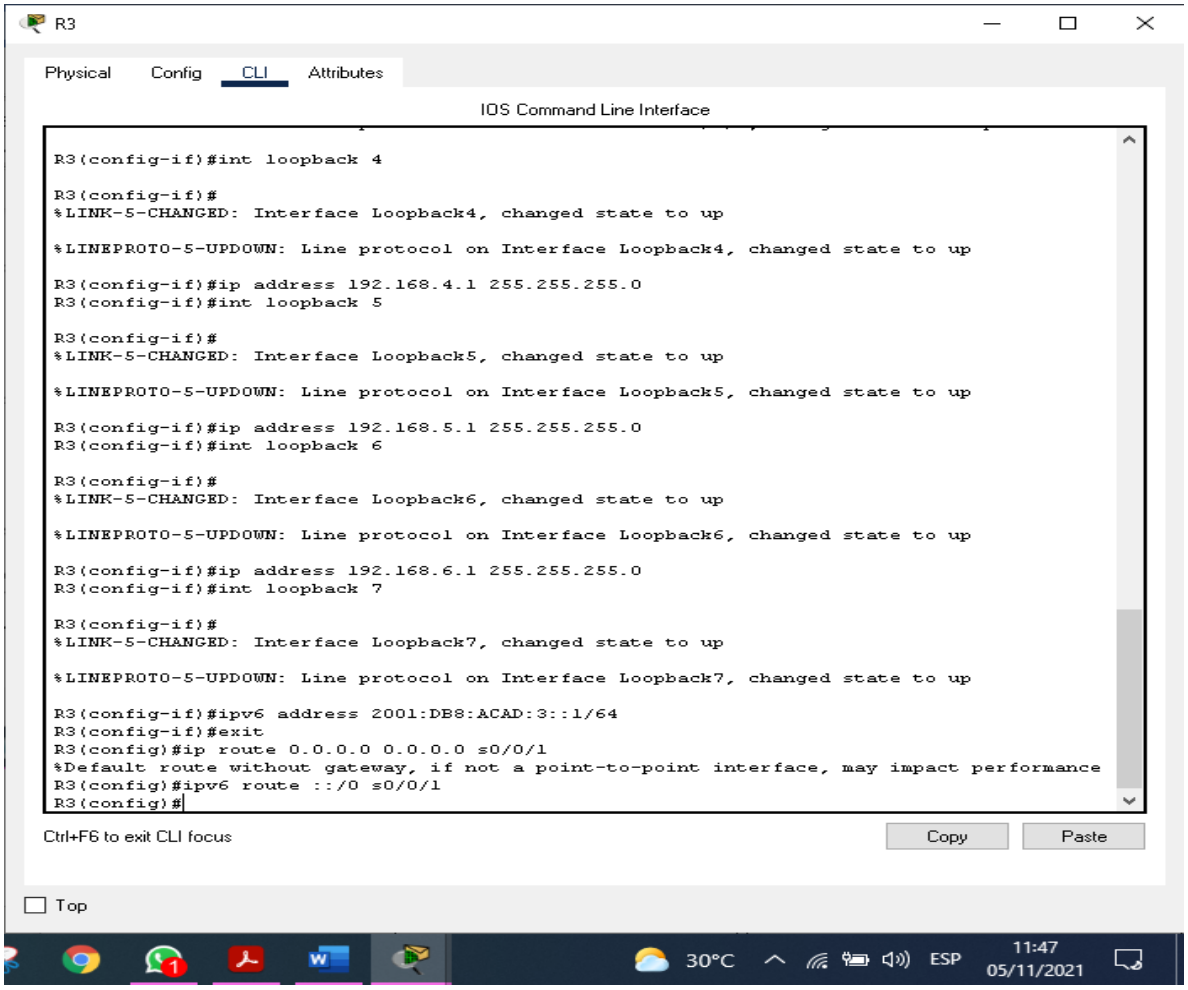
Interfaz S0/0/1	R3(config)#int s0/0/1 R3(config-if)#description Connection to R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#no shutdown R3(config-if)# %LINK-5-CHANGED: Interface Serial0/0/1, changed state to up R3(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
Interfaz loopback 4	R3(config-if)#int loopback 4 R3(config-if)# %LINK-5-CHANGED: Interface Loopback4, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config-if)#int loopback 5 R3(config-if)# %LINK-5-CHANGED: Interface Loopback5, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed

	state to up R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config-if)#int loopback 6 R3(config-if)# %LINK-5-CHANGED: Interface Loopback6, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config-if)#int loopback 7 R3(config-if)# %LINK-5-CHANGED: Interface Loopback7, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up 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 performance R3(config)#ipv6 route ::/0 s0/0/1 R3(config)#

Fuente: Elaboración propia

Figura 17: Configuraciones R3



Fuente: Elaboración propia

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
```

```
R3(config-line)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#service password-encryption
R3(config)#banner motd %Se prohibe el acceso no autorizado.%
R3(config)#int s0/0/1
R3(config-if)#description Connection to R2
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)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state
to up

R3(config-if)#int loopback 4

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state
to up

R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#int loopback 5

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state
to up

R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#int loopback 6

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state
to up

R3(config-if)#ip address 192.168.6.1 255.255.255.0
```

R3(config-if)#int loopback 7

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback7, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up

R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
R3(config-if)#exit
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 s0/0/1
R3(config)#

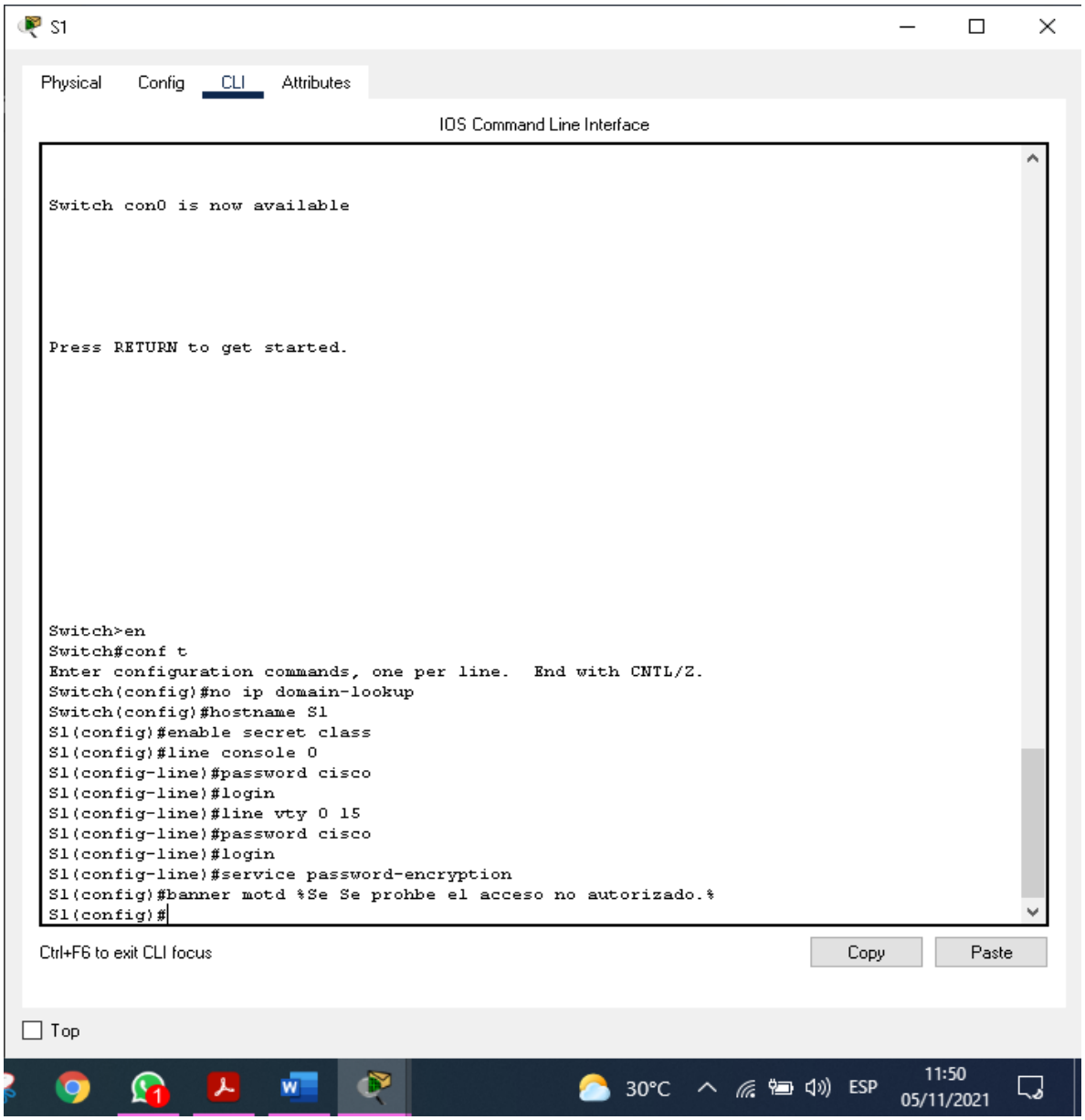
Paso 5: Configurar S1
La configuración del S1 incluye las siguientes tareas:

Tabla 12: Configuraciones S1

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 con 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config)#line vty 0 15 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	S1(config)# banner motd %Se Se prohíbe el acceso no autorizado.%

Fuente: Elaboración propia

Figura 18: Configuraciones S1



Fuente: Elaboración propia

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class

S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd %Se Se prohbe el acceso no autorizado.%
S1(config)#

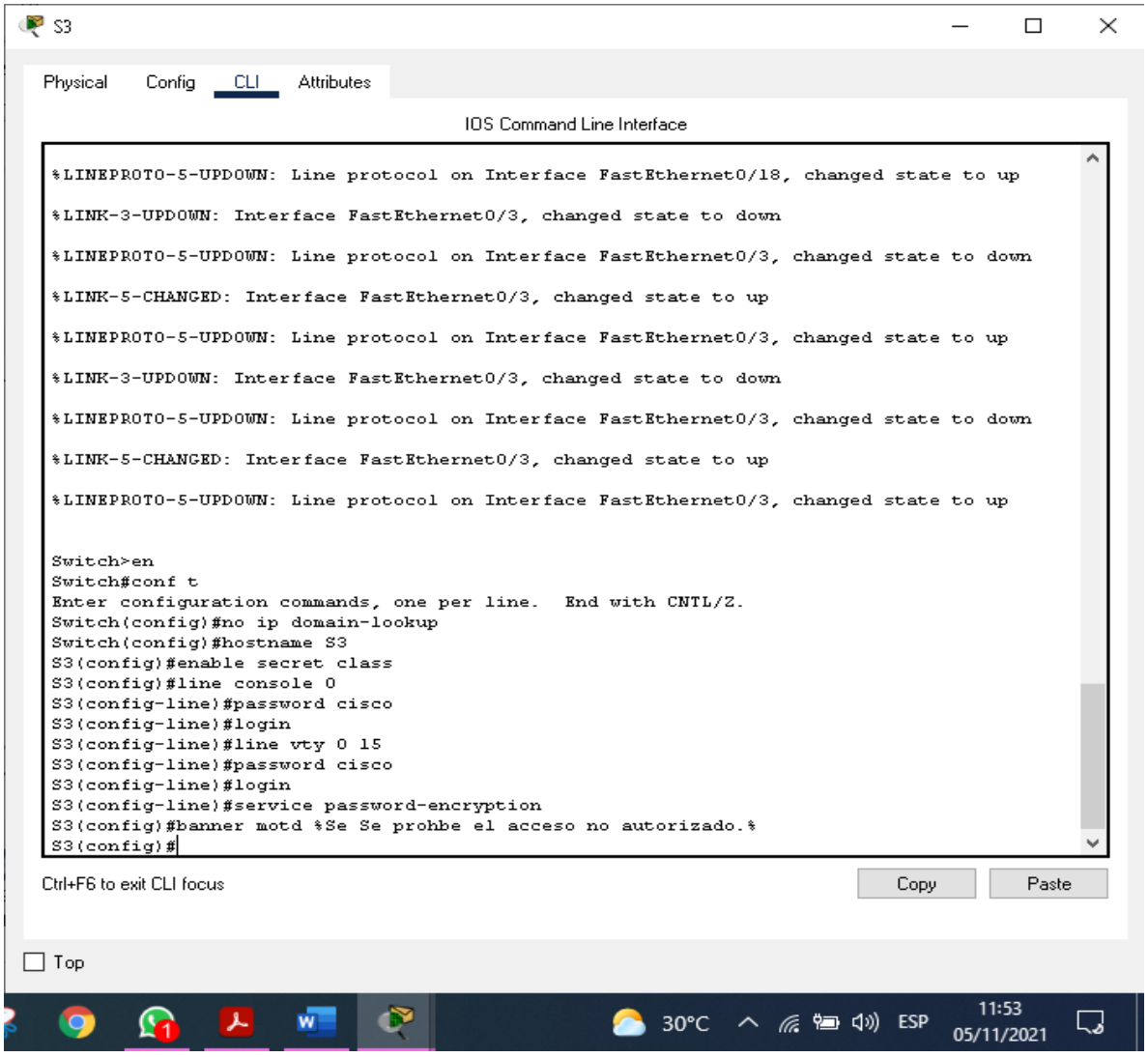
Paso 6: Configurar el S3
La configuración del S3 incluye las siguientes tareas:

Tabla 13: Configuraciones S3

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 con 0 S3(config-line)#password ciscoS3(config-line)#login
Contraseña de acceso Telnet	S3(config)#line vty 0 15 S3(config-line)#password ciscoS3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)# banner motd %Se Se prohíbe el acceso no autorizado.%

Fuente: Elaboración propia

Figura 19: Configuraciones S3



Fuente: Elaboración propia

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
```

S3(config-line)#service password-encryption
S3(config)#banner motd %Se Se prohbe el acceso no autorizado.%
S3(config)#

Paso 7: Verificar la conectividad de la red

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

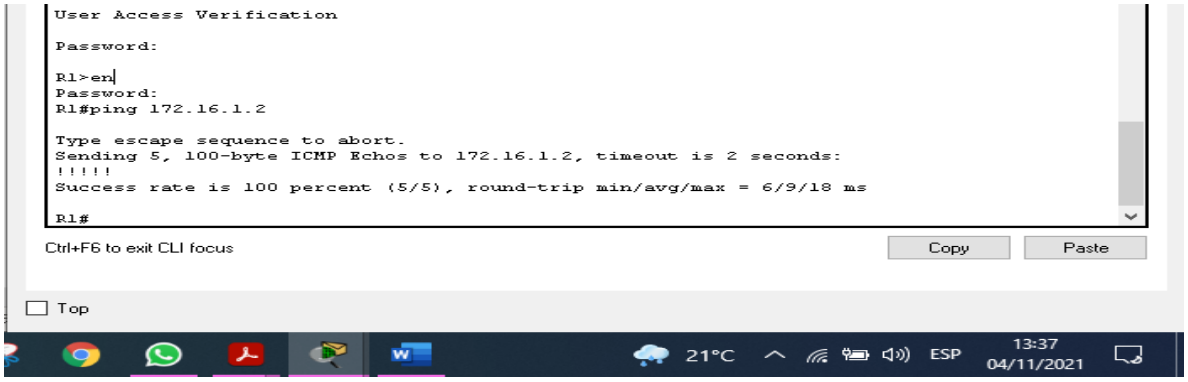
Tabla 14: Verificar la conectividad de la red

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 = 6/9/18 ms R1#
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 = 7/9/18 ms R2#

PC de Internet	Gateway predeterminado	209.165.200.233	C:\>ping 209.165.200.233 Pinging 209.165.200.233 with 32 bytes of data: Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time=5ms TTL=255 Ping statistics for 209.165.200.233: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 5ms, Average = 1ms C:\>

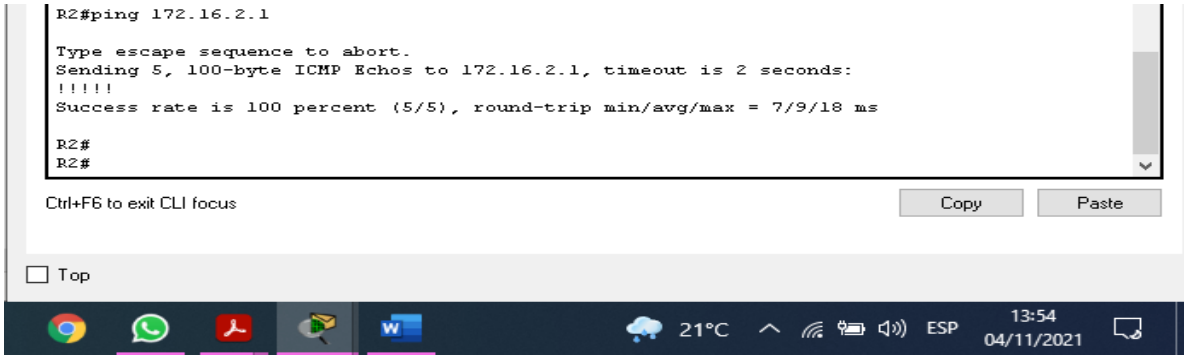
Fuente: Elaboración propia

Figura 20: ping 172.16.1.2 en R1



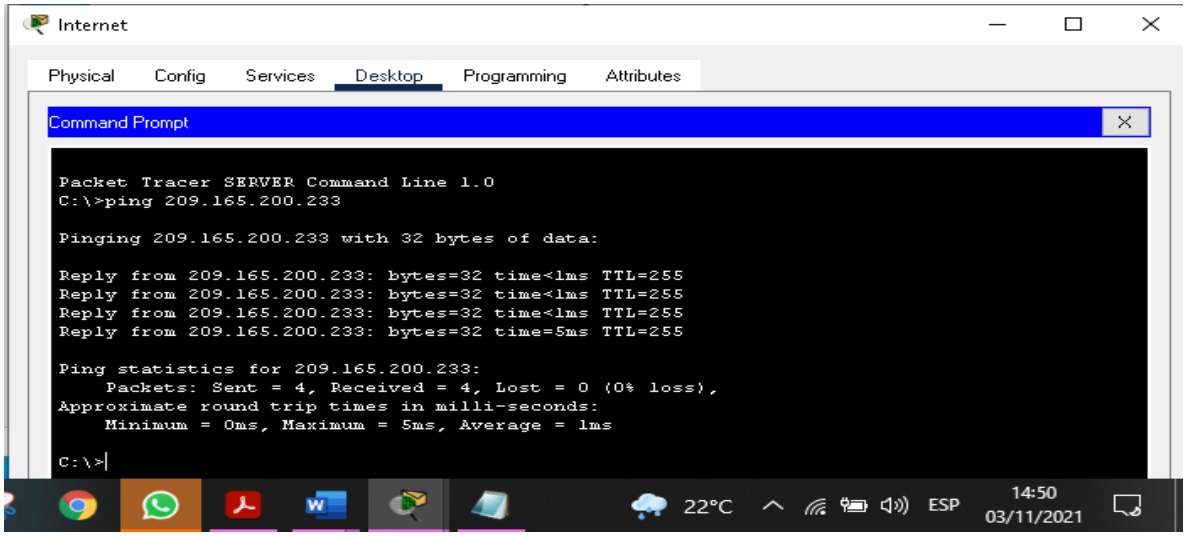
Fuente: Elaboración propia

Figura 21: ping 172.16.2.1 en R2



Fuente: Elaboración propia

Figura 22: ping 209.168.200.233 en PC-Internet



Fuente: Elaboración propia

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:

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

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:

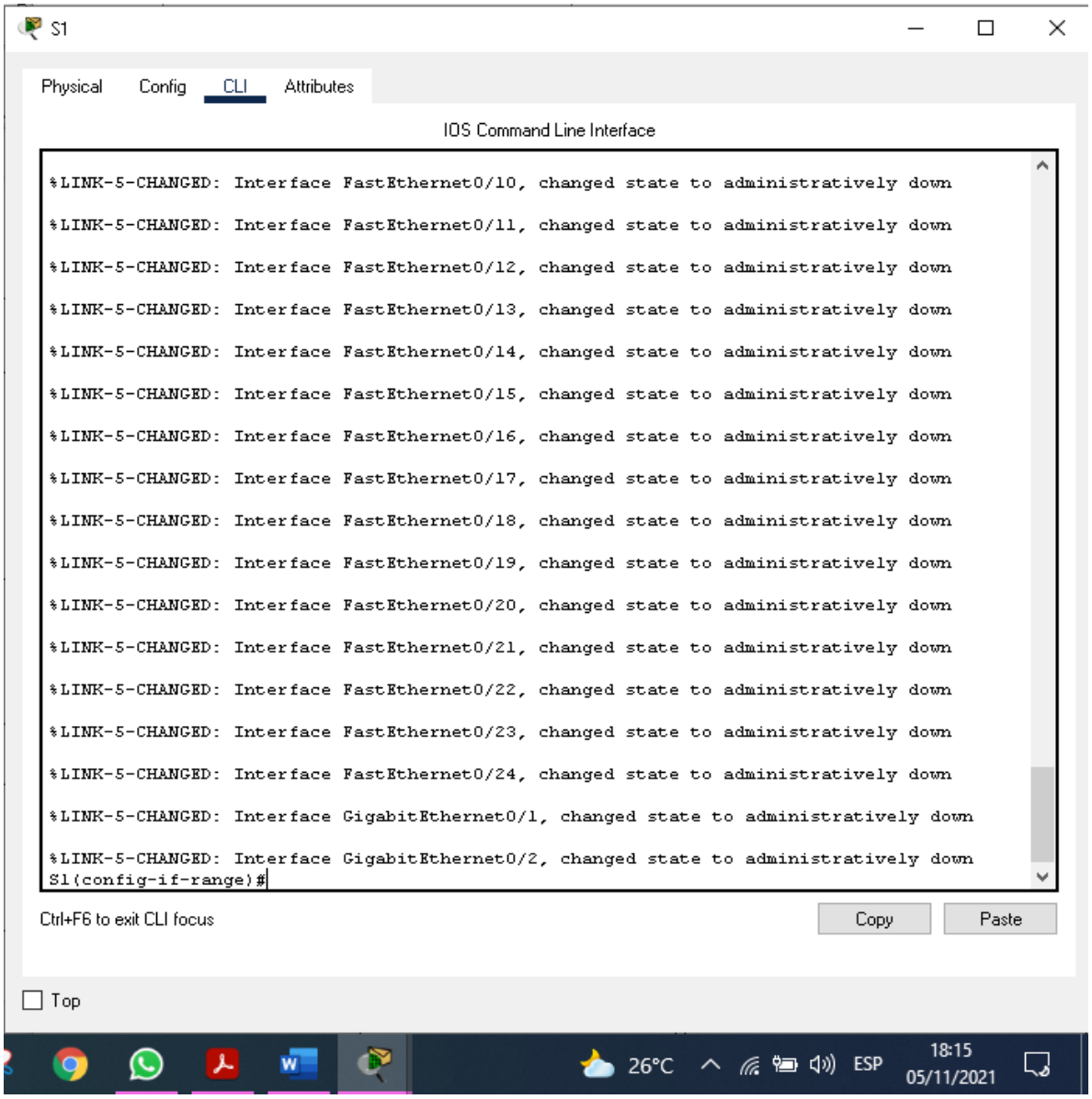
Tabla 15: Configuraciones S1 tareas

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)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit
Asignar la dirección IP de administración.	S1(config)#interface vlan 99 S1(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up 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.

Forzar el enlace troncal en la interfaz F0/3	S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Fuente: Elaboración propia

Figura 23: Configuraciones S1 tareas



Fuente: Elaboración propia

Se Se prohbe el acceso no autorizado.

User Access Verification

Password:

S1>en
Password:

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administracion
S1(config-vlan)#exit
S1(config)#interface vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.99.1
S1(config)#int f0/3
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#int f0/6
S1(config-if)#switchport access vlan 21
S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
```

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
S1(config-if-range)#

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

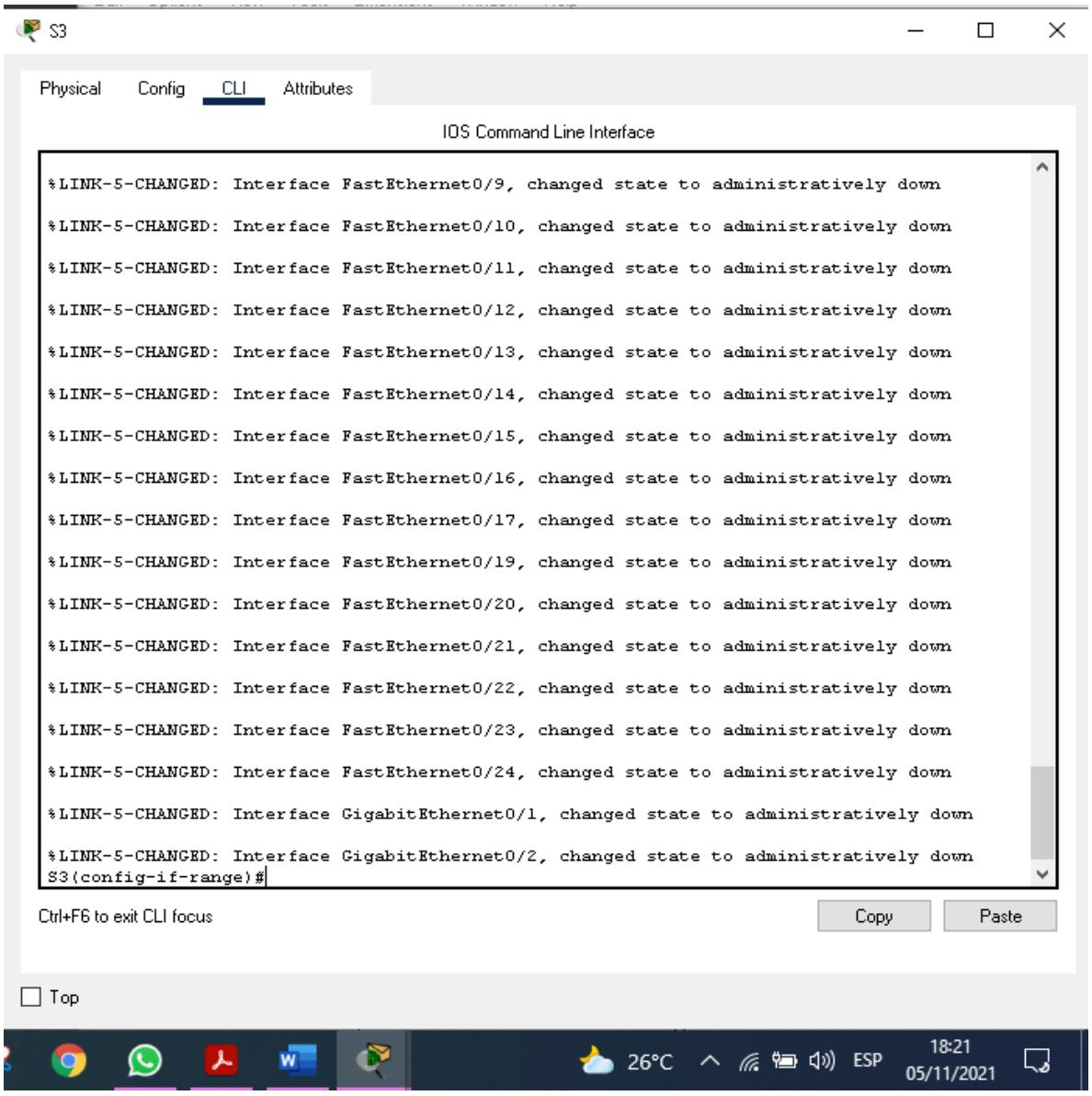
Tabla 16: Configuraciones S3 tareas

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)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit
Asignar la dirección IP de administración	S3(config)#int vlan 99 S3(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up %LINEPROTO-5-

	UPDOWN: Line protocol on Interface Vlan99, changed state to up S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#exit
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
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 native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode Access
Asignar F0/18 a la VLAN 21	S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if- range)#shutdown

Fuente: Elaboración propia

Figura 24: Configuraciones S3 tareas



Fuente: Elaboración propia

Se Se prohbe el acceso no autorizado.

User Access Verification

Password:

S3>en
Password:
S3#conf t

Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vlan 21
S3(config-vlan)#name Contabilidad
S3(config-vlan)#vlan 23
S3(config-vlan)#name Ingenieria
S3(config-vlan)#vlan 99
S3(config-vlan)#name Administracion
S3(config-vlan)#exit
S3(config)#int vlan 99
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1
S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode Access
S3(config-if-range)#int f0/18
S3(config-if)#switchport access vlan 23
S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2
S3(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
S3(config-if-range)#

Paso 3: Configurar R1
Las tareas de configuración para R1 incluyen las siguientes:

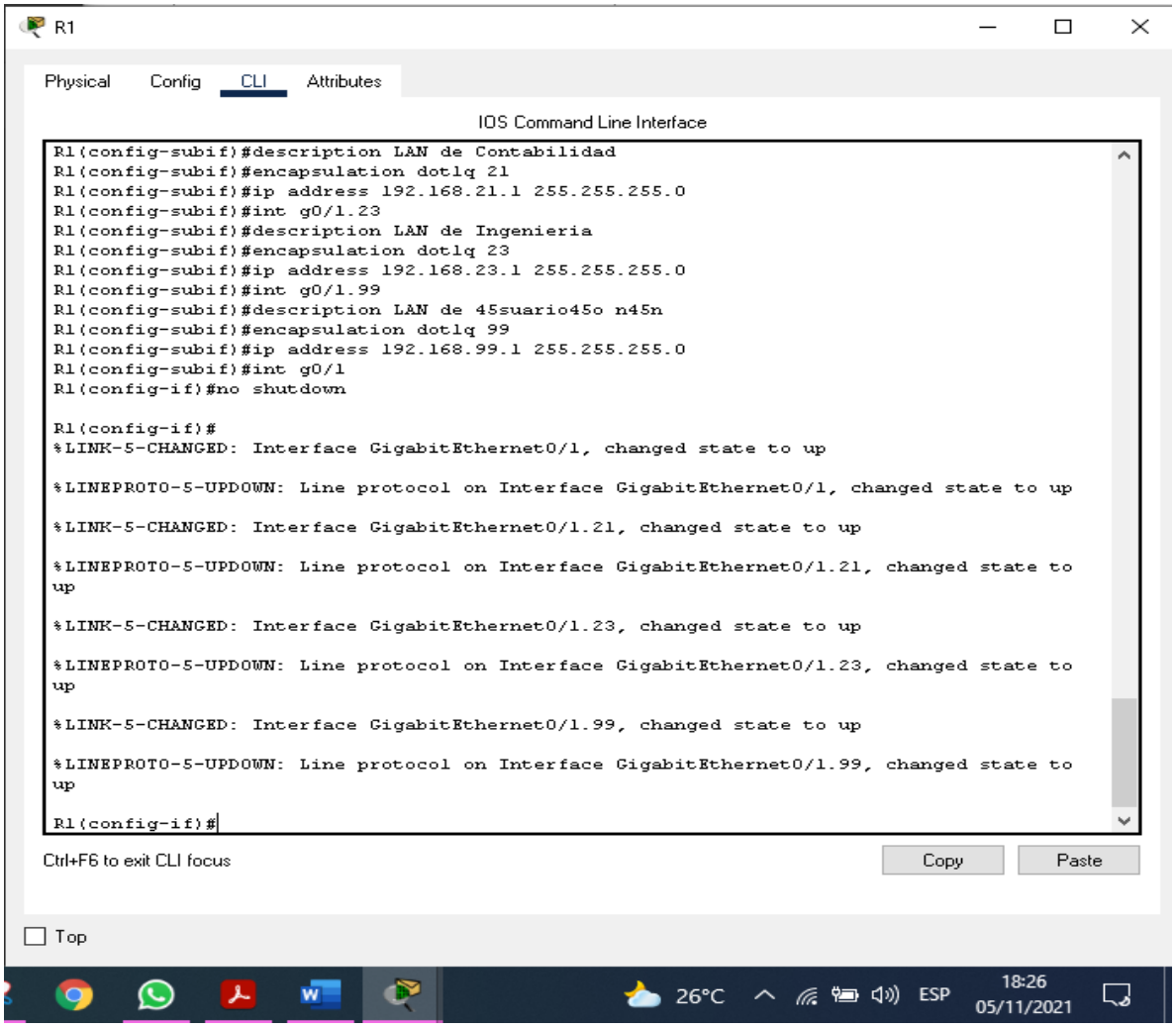
Tabla 17: Configuraciones R1 tareas

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#int g0/1.21 R1(config-subif)#description LAN de Contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#int g0/1.23 R1(config-subif)#description LAN de Ingenieria R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config-subif)#int g0/1.99 R1(config-subif)#description LAN de 45suario45o n45ón R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0

Activar la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shutdown

Fuente: Elaboración propia

Figura 25: Configuraciones R1 tareas



Fuente: Elaboración propia

Se prohibe el acceso no autorizado.

User Access Verification

Password:

R1>en

```
Password:
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int g0/1.21
R1(config-subif)#description LAN de Contabilidad
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#int g0/1.23
R1(config-subif)#description LAN de Ingenieria
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#int g0/1.99
R1(config-subif)#description LAN de 45suario45o n45n
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#int g0/1
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

R1(config-if)#
```

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: Verificar la conectividad de la red

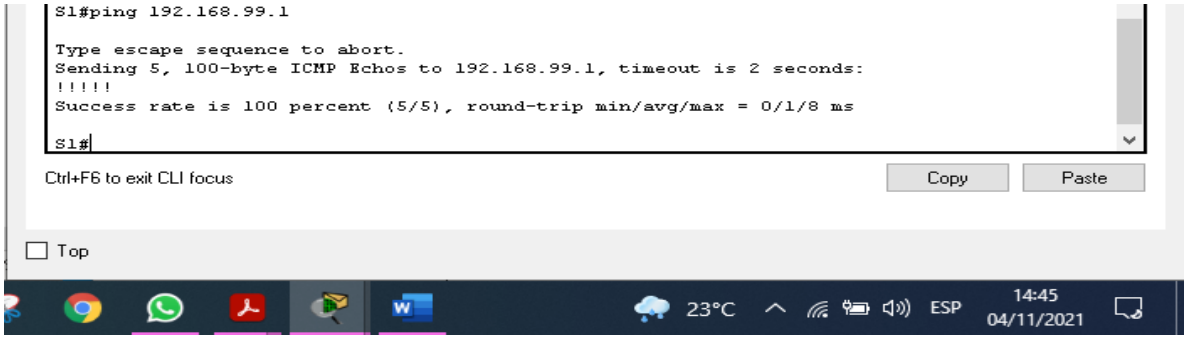
Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/8 ms S1#
S3	R1, dirección VLAN 99	192.168.99.1	S3#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte

			ICMP Echos to 192.168.99.1 , timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms S3#
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 = 0/0/1 ms S1#

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 S3#

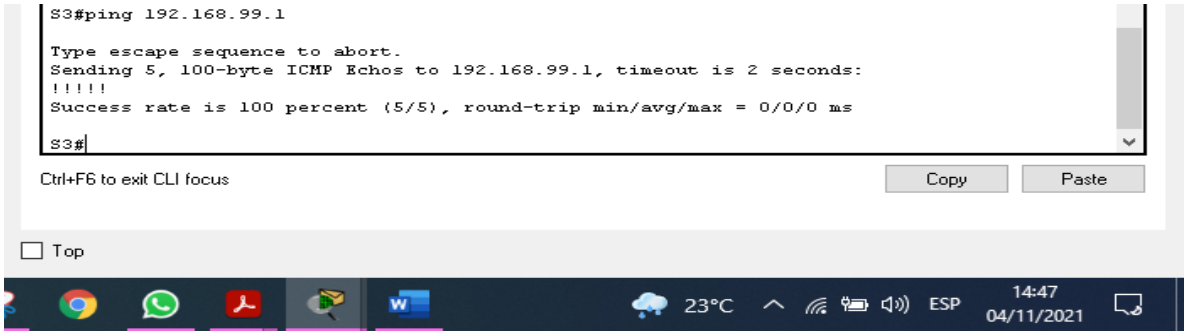
Fuente: Elaboración propia

Figura 26: ping 192.168.99.1 en S1



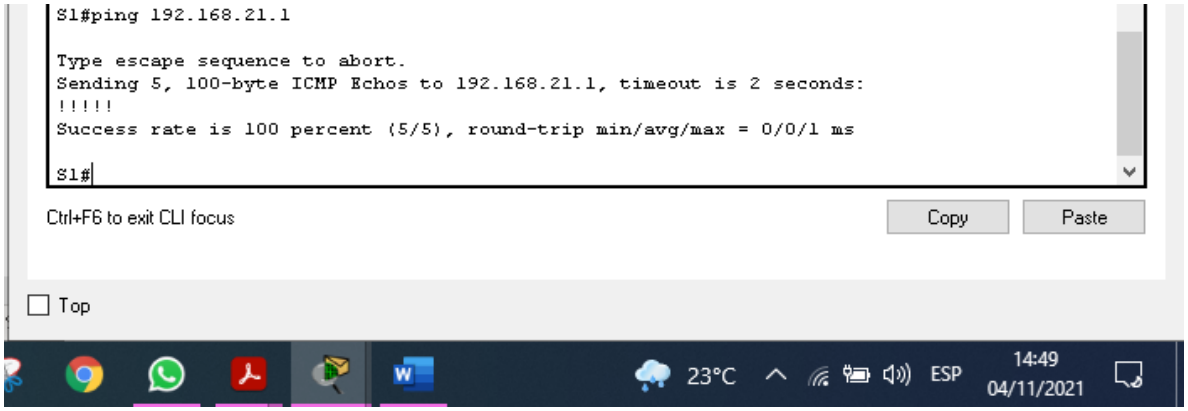
Fuente: Elaboración propia

Figura 27: ping 192.168.99.1 en S3



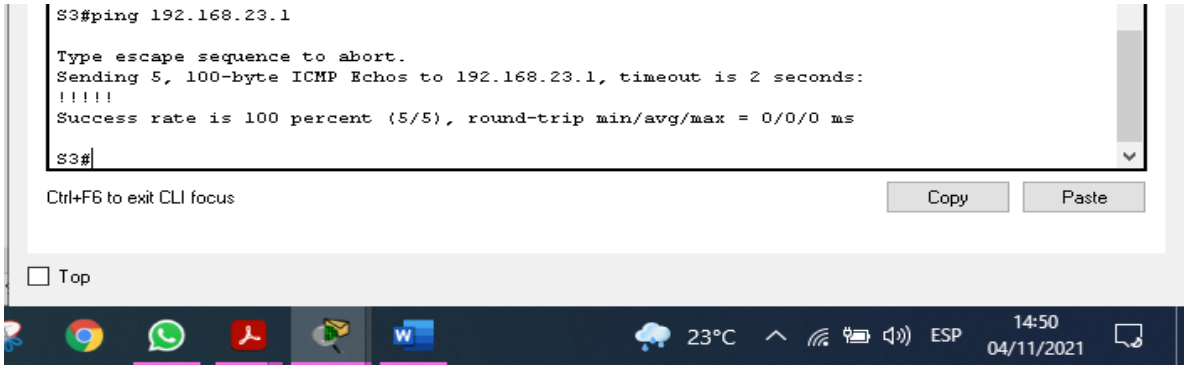
Fuente: Elaboración propia

Figura 28: ping 192.168.21.1 en S1



Fuente: Elaboración propia

Figura 29: ping 192.168.23.1 en S3



Fuente: Elaboración 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:

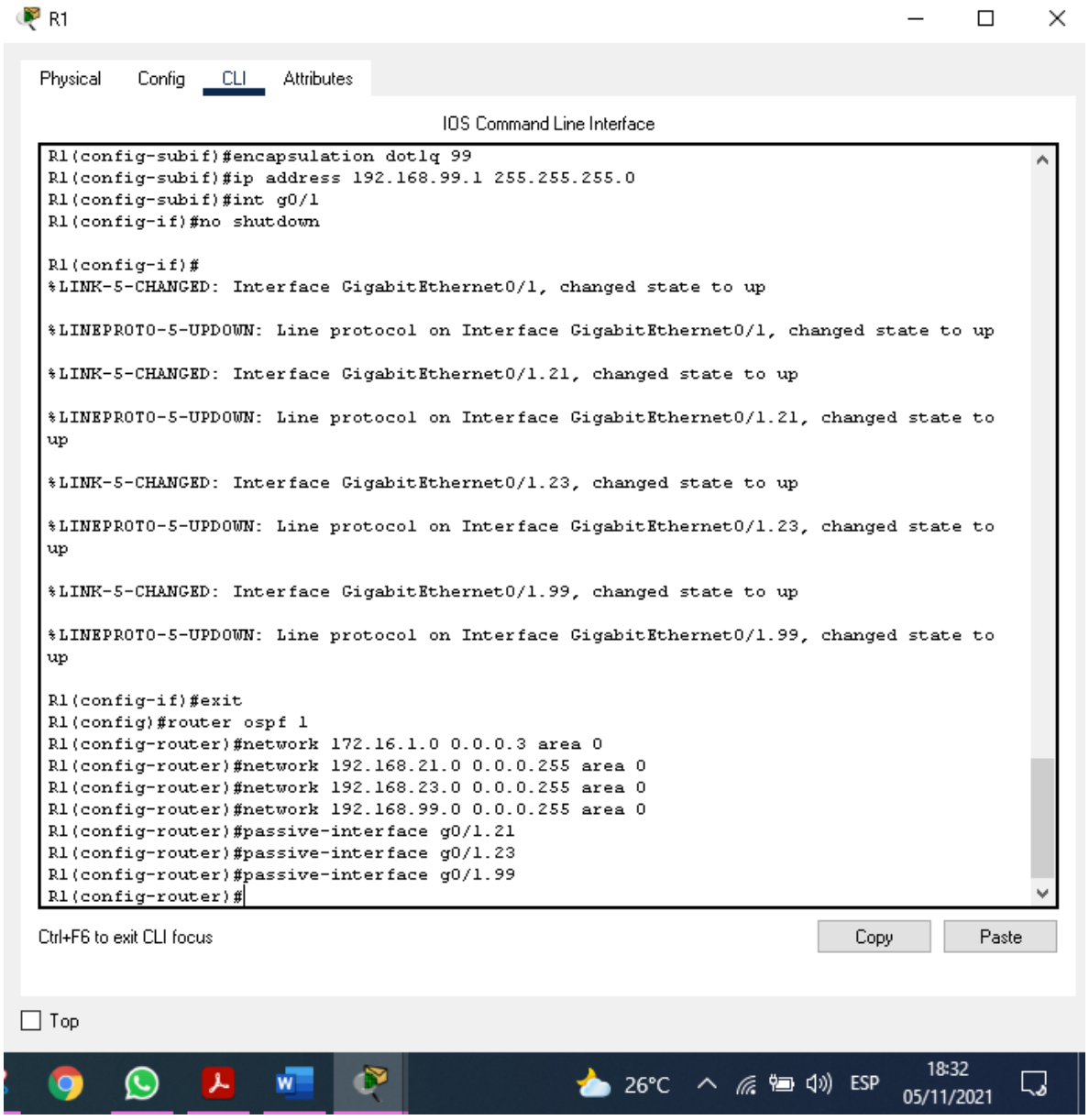
Tabla 19: Configurar OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1

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
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
Desactive la sumarización automática	R1(config-router)#no auto-summary (no soportado)

Fuente: Elaboración propia

Figura 30: Configurar OSPF en el R1



Fuente: Elaboración propia

R1(config)#router ospf 1
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
R1(config-router)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23

R1(config-router)#passive-interface g0/1.99
R1(config-router)#

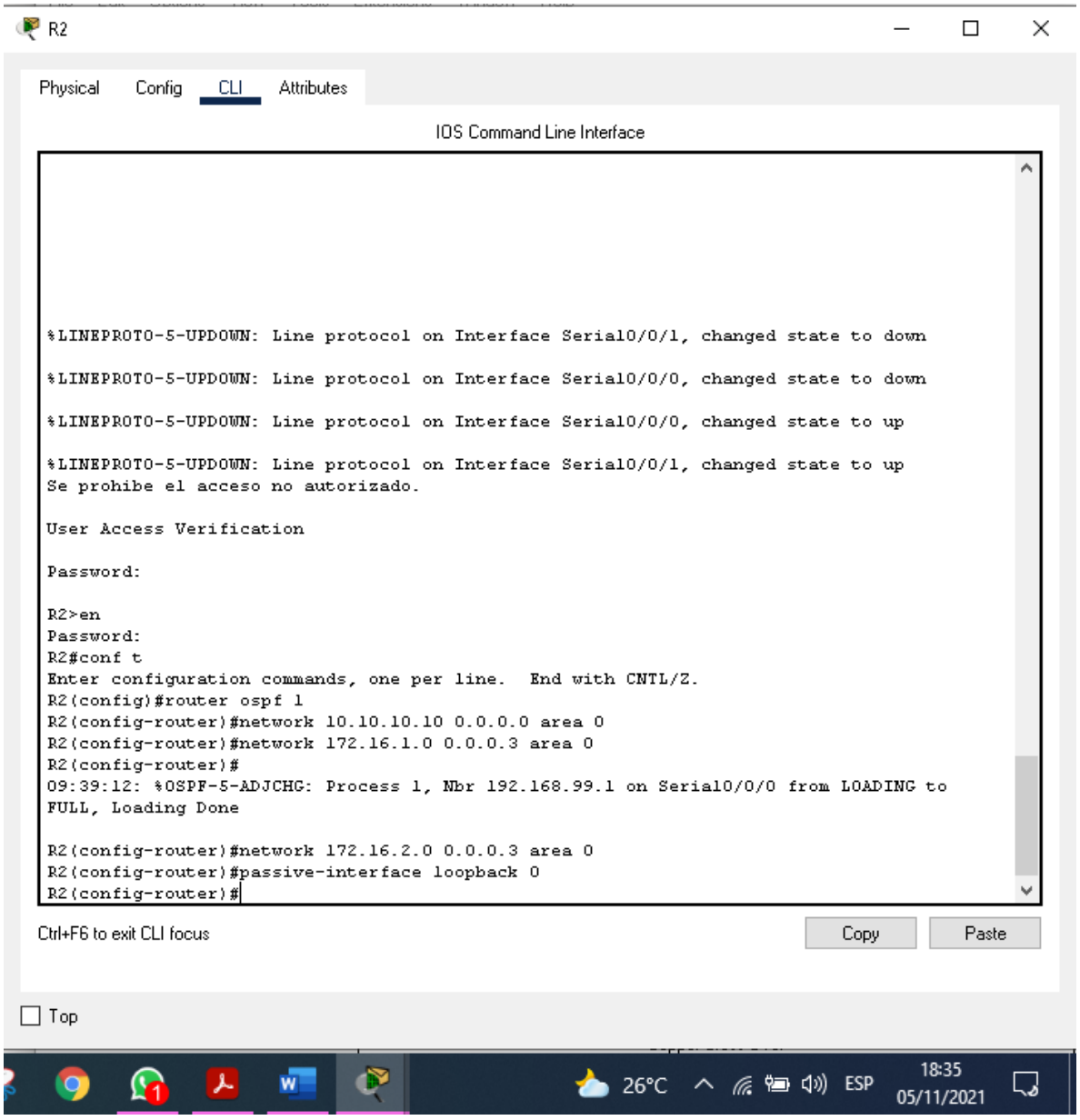
Paso 2: Configurar OSPF en el R2
La configuración del R2 incluye las siguientes tareas:

Tabla 20: Configurar OSPF en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1
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
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary (no soportado)

Fuente: Elaboración propia

Figura 31: Configurar OSPF en el R2



Fuente: Elaboración propia

Se prohibe el acceso no autorizado.

User Access Verification

Password:

R2>en

Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
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)#
09:39:12: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.99.1 on Serial0/0/0 from LOADING to FULL, Loading Done

R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
R2(config-router)#passive-interface loopback 0
R2(config-router)#

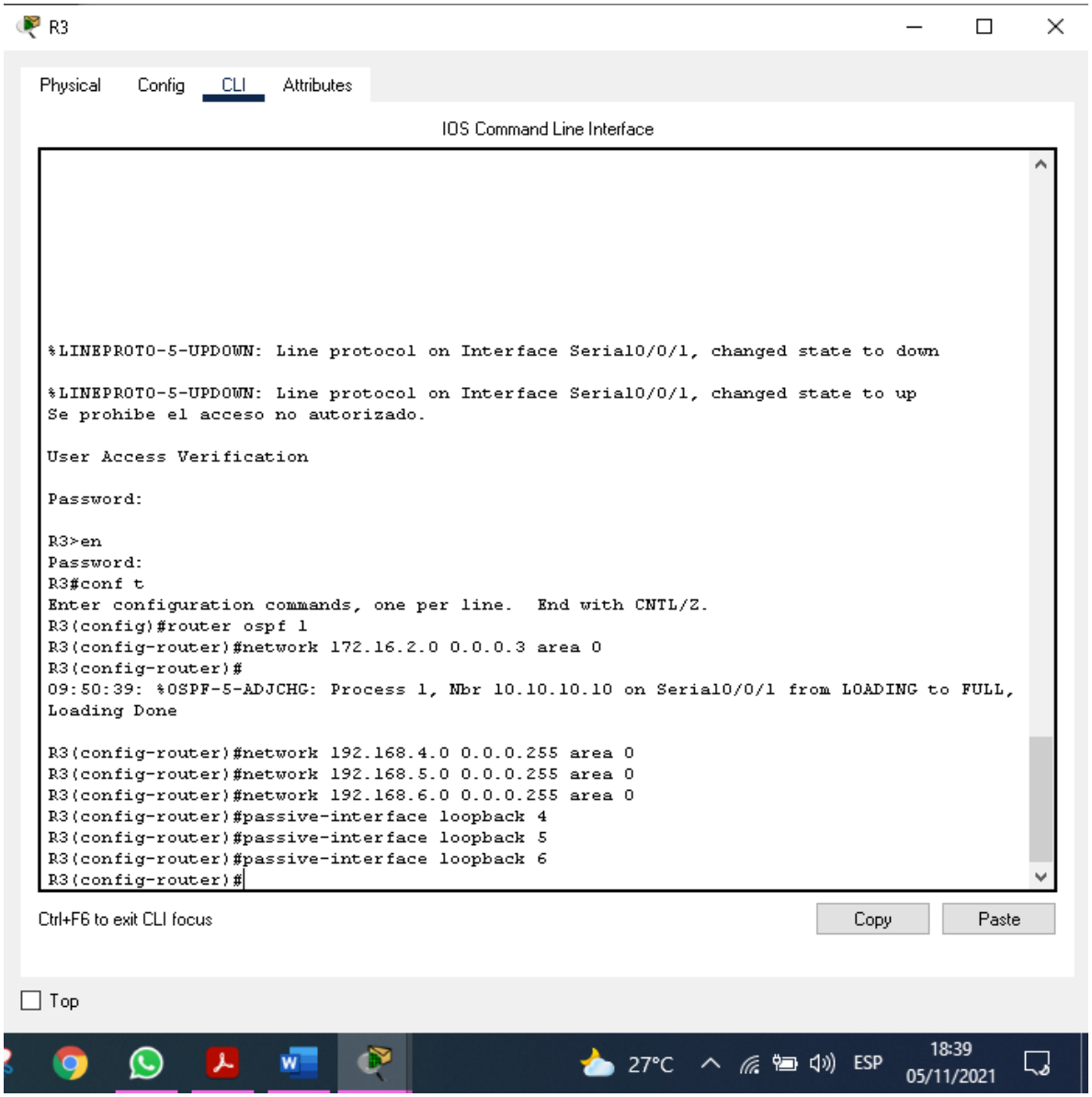
Paso 3: Configurar OSPFv3 en el R3
La configuración del R3 incluye las siguientes tareas:

Tabla 21: Configurar OSPF en el R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 1
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	R3(config-router)#no auto-summary (no soportado)

Fuente: Elaboración propia

Figura 32: Configurar OSPF en el R3



Fuente: Elaboración propia

Se prohibe el acceso no autorizado.

User Access Verification

Password:

R3>en
Password:
R3#conf t

Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
R3(config-router)#
09:50:39: %OSPF-5-ADJCHG: Process 1, Nbr 10.10.10.10 on Serial0/0/1 from LOADING to FULL, Loading Done

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
R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
R3(config-router)#

Paso 4: Verificar la información de OSPF

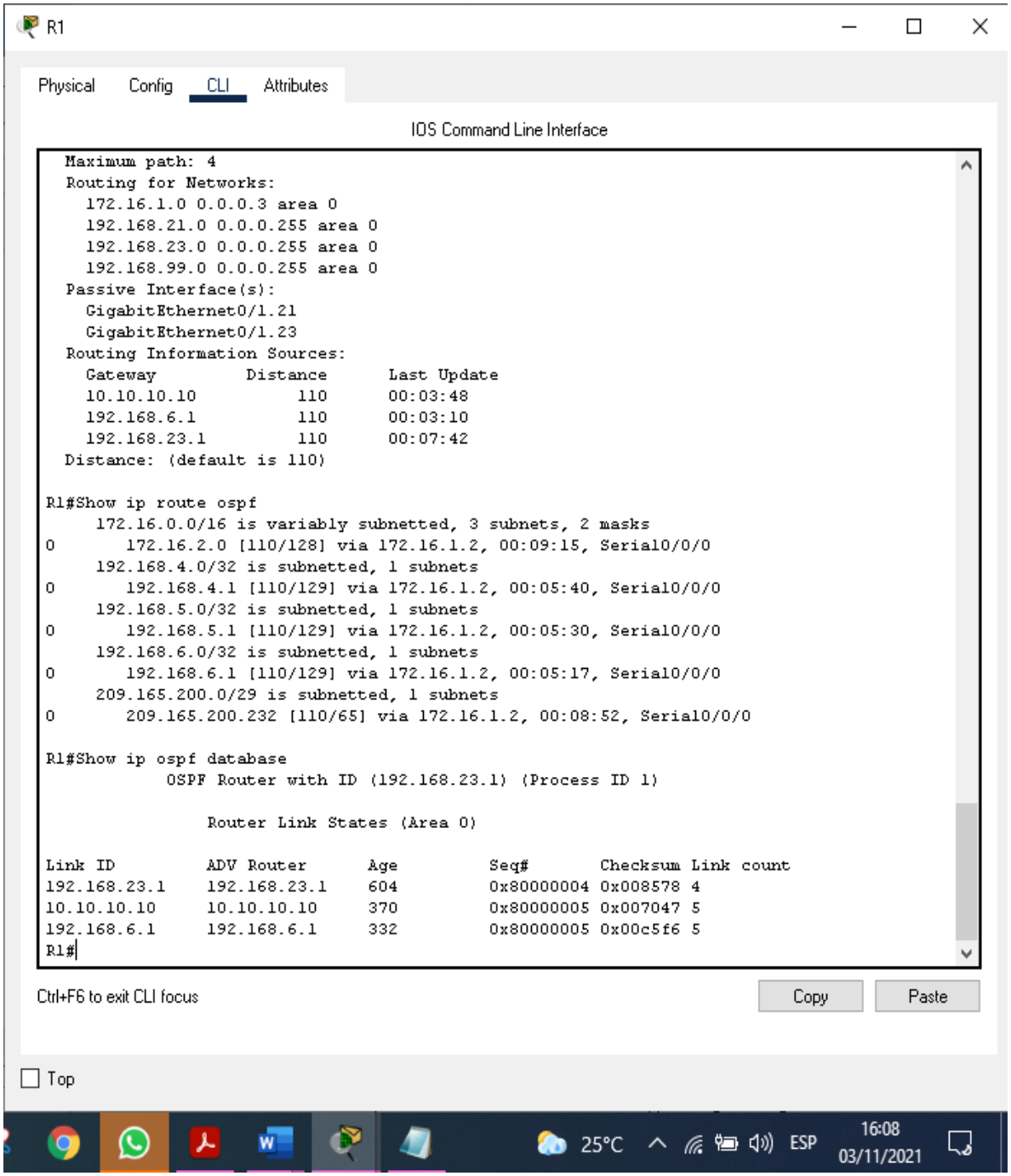
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 22: Verificar la información de OSPF

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

Fuente: Elaboración propia

Figura 33: R1 Verificar la información de OSPF



Fuente: Elaboración propia

Parte 5: Implementar DHCP y NAT para IPv4

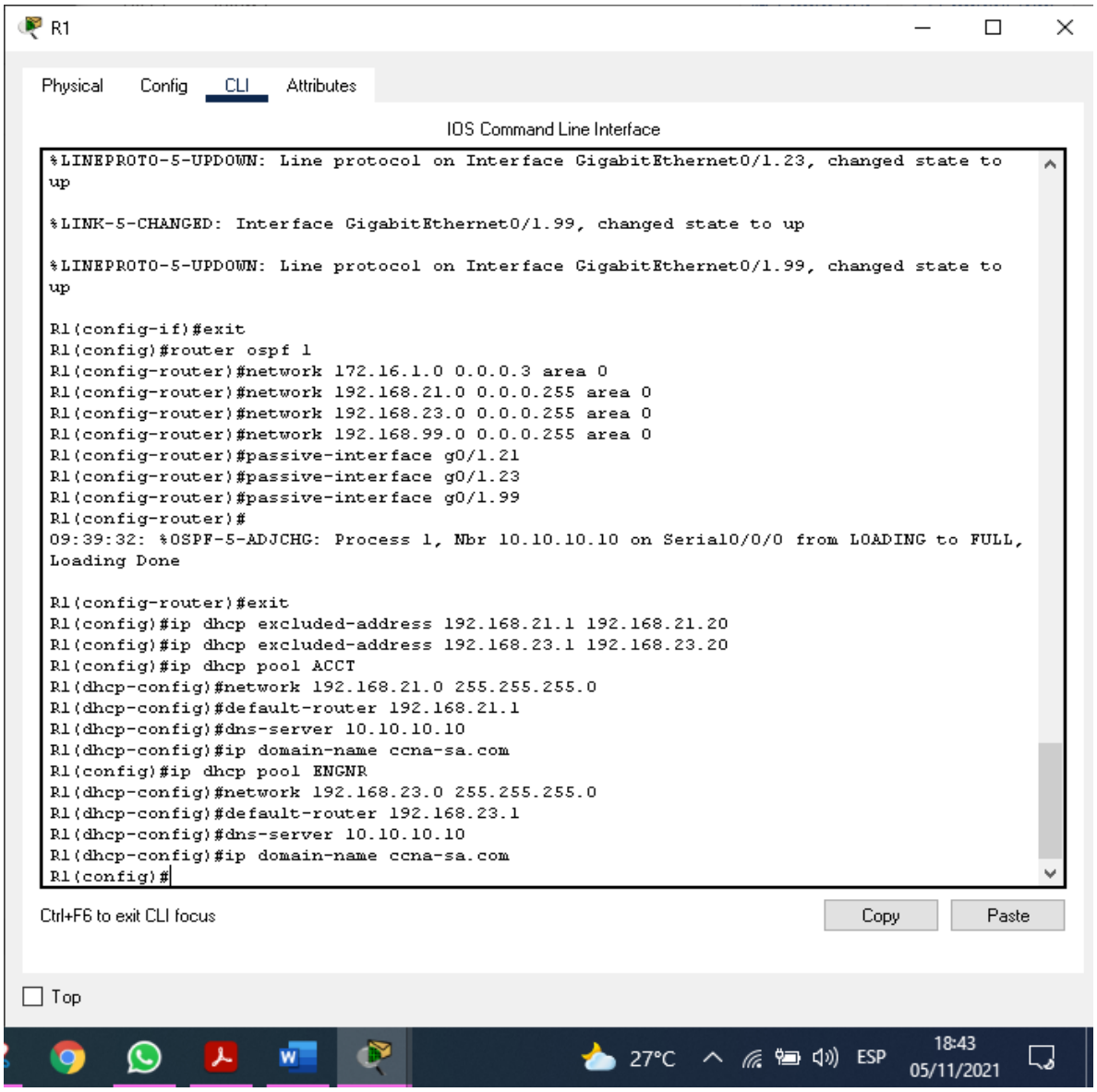
Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 23: Implementar DHCP y NAT para IPv4

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	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)#ip domain-name ccna-sa.com
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)#ip domain-name ccna-sa.com

Fuente: Elaboración propia

Figura 34: Implementar DHCP y NAT para IPv4 en R1



Fuente: Elaboración propia

R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
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)#ip domain-name ccna-sa.com
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)#ip domain-name ccna-sa.com
R1(config)#

Paso 2: Configurar la NAT estática y dinámica en el R2
La configuración del R2 incluye las siguientes tareas:

Tabla 24: Configurar la NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server ^ % Invalid input detected at '^' marker. (No soportado)
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local % Invalid input detected at '^' marker. (No soportado)
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.238
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface gi0/0 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	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 0.0.0.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.232 209.165.200.237 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Fuente: Elaboración propia

Figura 35: Configurar la NAT estática y dinámica en el R2

Fuente: Elaboración propia

Se prohibe el acceso no autorizado.

User Access Verification

Password:

```
R2>en
Password:
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#user webuser privilege 15 secret cisco12345
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.238
R2(config)#interface gi0/0
R2(config-if)#ip nat inside
R2(config-if)#access-list 1 permit 192.168.21.0 0.0.0.255
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 0.0.0.255
R2(config)#ip nat pool INTERNET 209.165.200.232 209.165.200.237 netmask
255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#
```

Nota: Los siguientes comandos no son compatibles con Packet Tracer.
Ip http server
Ip http authentication local
Ip http secure-server

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.

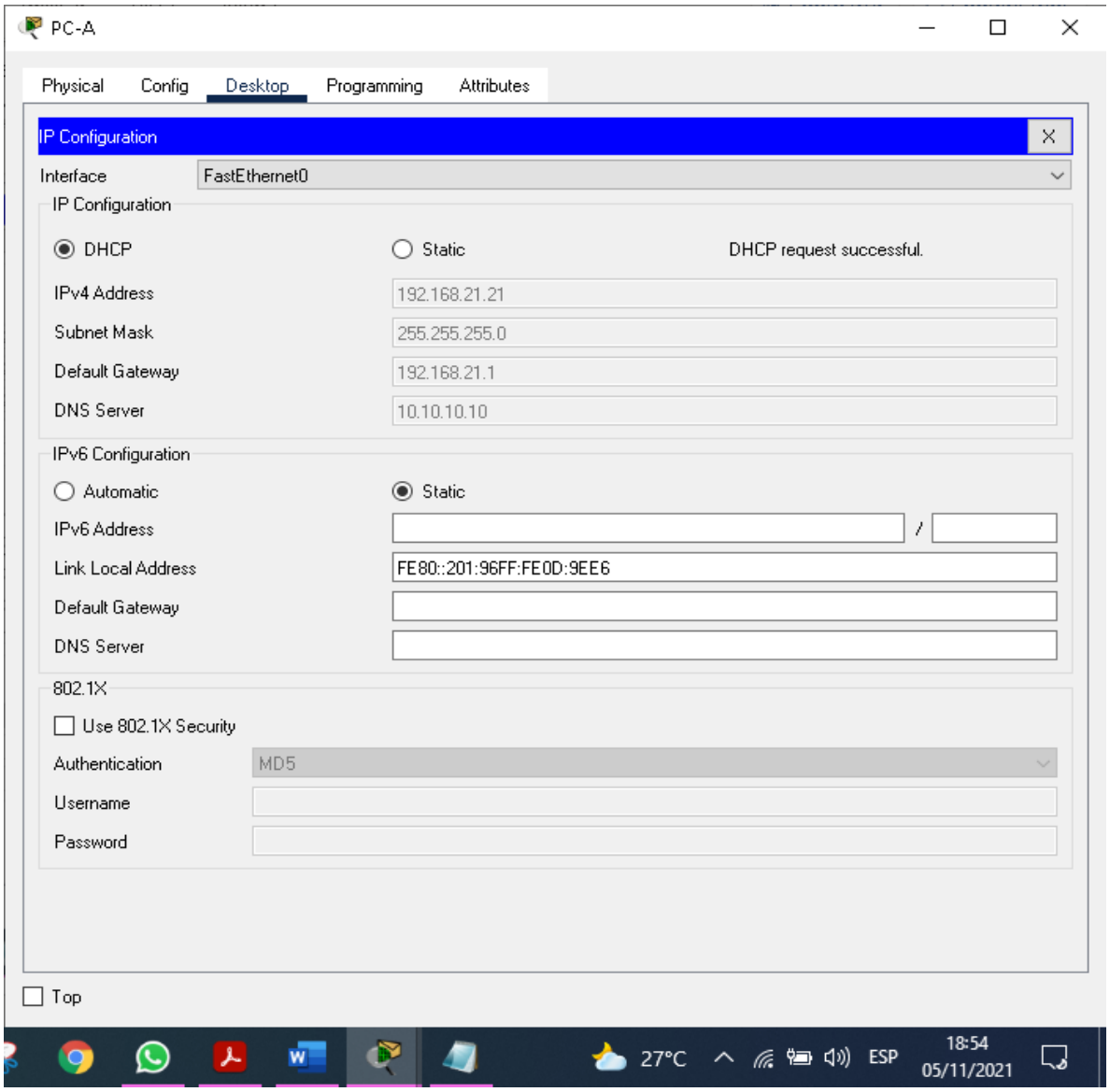
Tabla 25: Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	

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**	

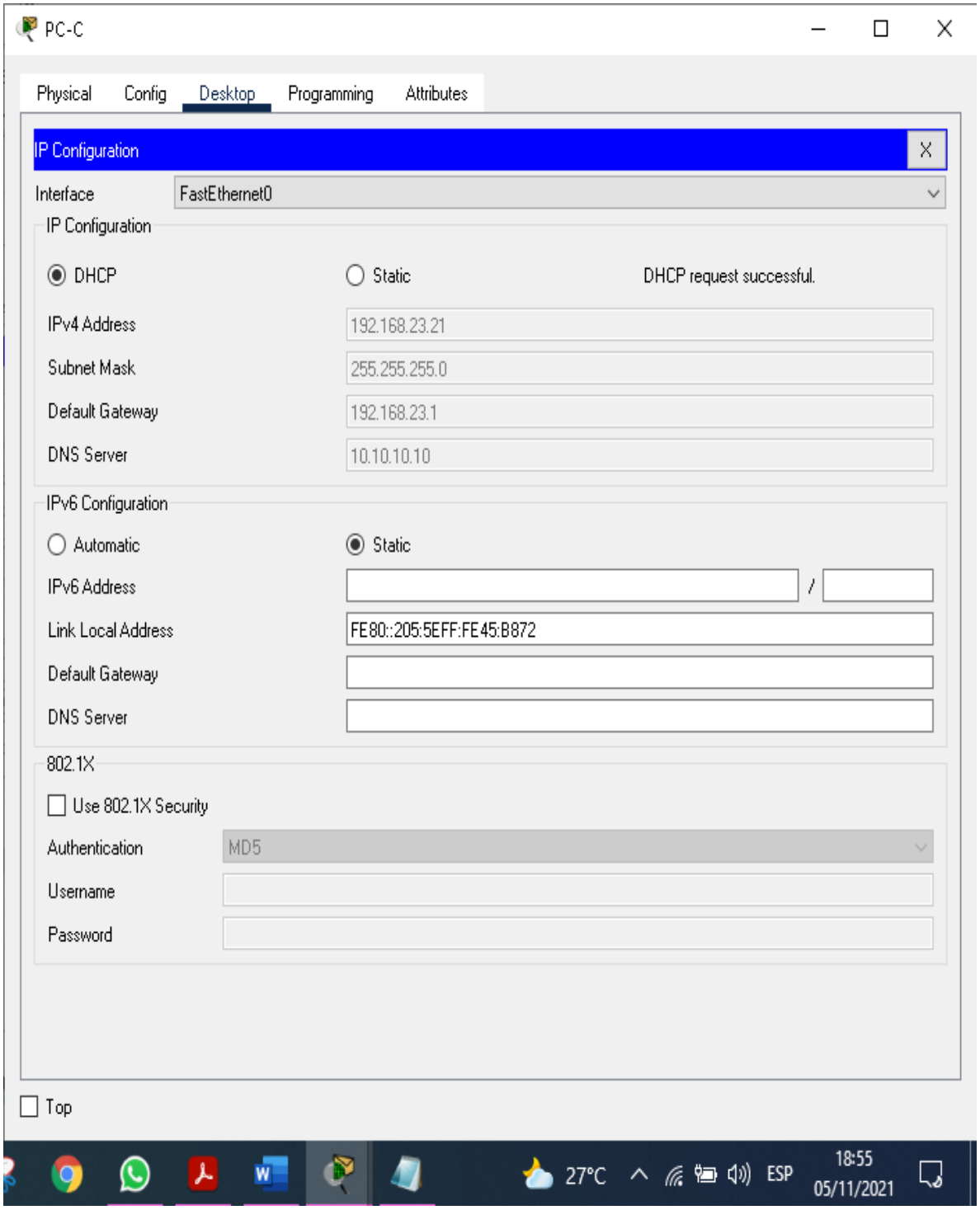
Fuente: Elaboración propia

Figura 36: Verificar el protocolo DHCP y la NAT estática PC-A



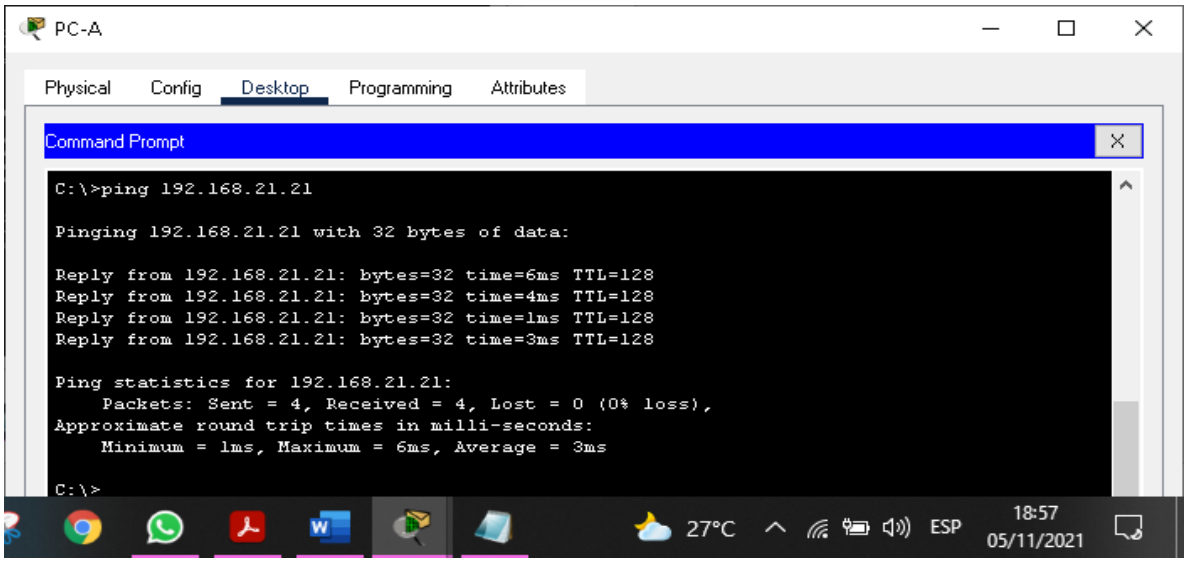
Fuente: Elaboración propia

Figura 37: Verificar el protocolo DHCP y la NAT estática PC-C



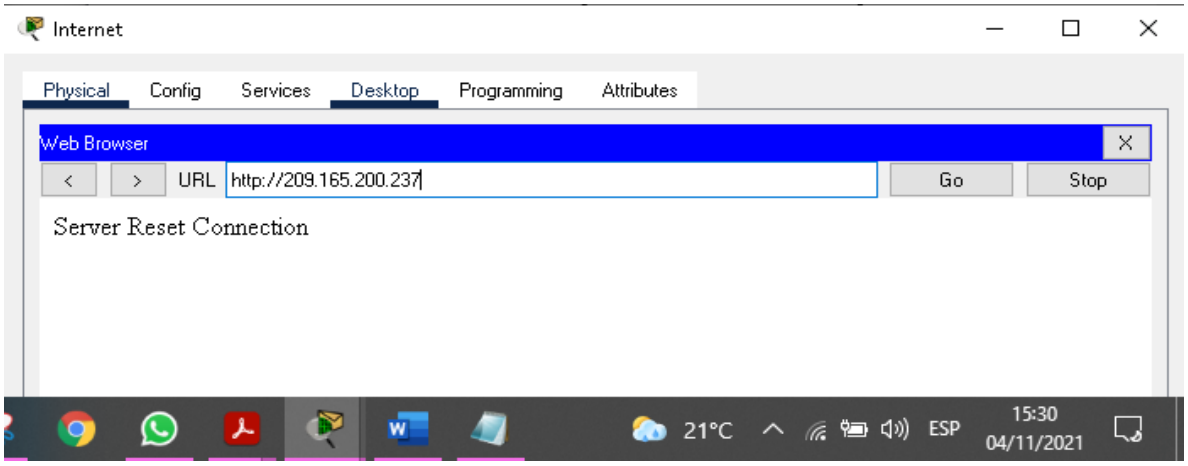
Fuente: Elaboración propia

Figura 38: ping 192.168.21.21 en PC-A



Fuente: Elaboración propia

Figura 39: acceder al servidor web (209.165.200.237)



Fuente: Elaboración propia

Parte 6: Configurar NTP

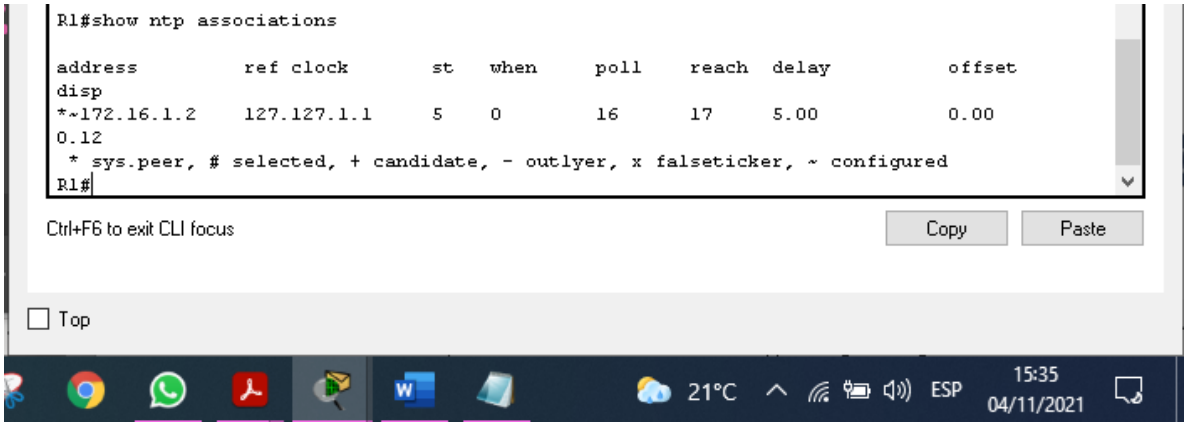
Tabla 26: Configurar NTP en R1 y R2

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 15:35:00 04 November 2021
Configure R2 como un maestro NTP.	R2(config)#ntp master 5

	^% Invalid input detected at '^' marker.
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1#show ntp associations

Fuente: Elaboración propia

Figura 40: show ntp associations



Fuente: Elaboración propia

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

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

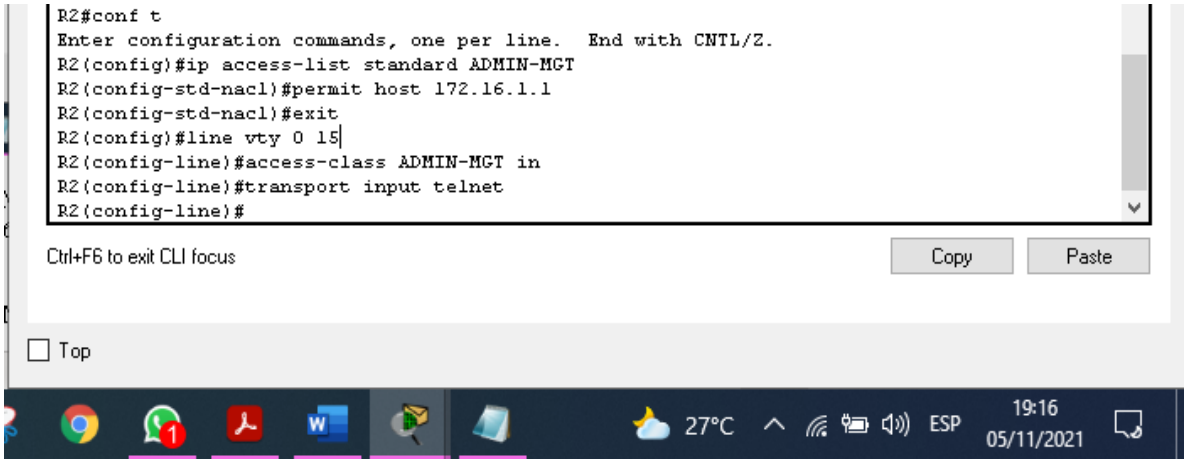
Tabla 27: Restringir el acceso a las líneas VTY en el R2

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
Aplicar la ACL con nombre a las líneas VTY	R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit

Permitir acceso por Telnet a las líneas de VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 Trying 172.16.1.2 …OpenSe prohibe el acceso no Elaboración propiaizado. User Access Verification Password: R2>exit [Connection to 172.16.1.2 closed by foreign host] R1#

Fuente: Elaboración propia

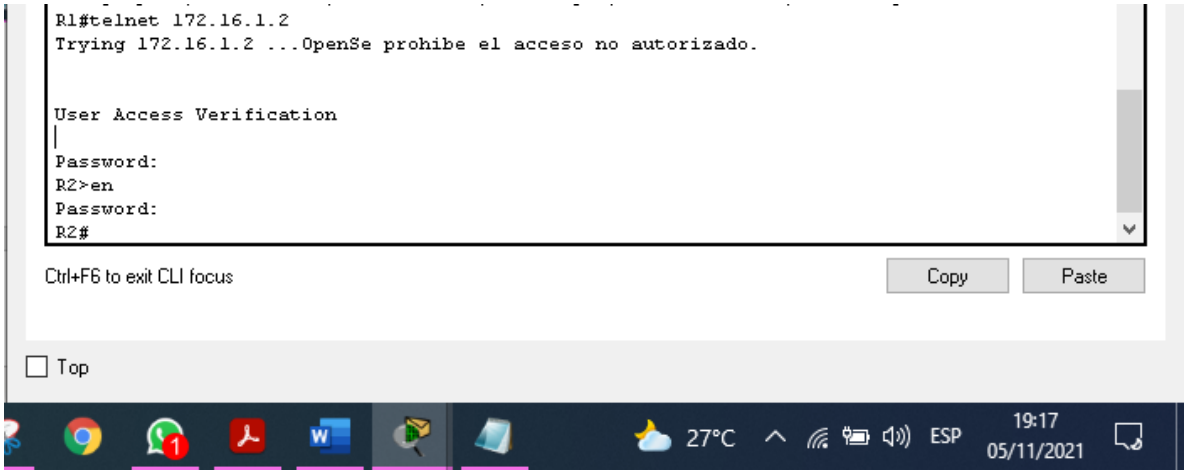
Figura 41: Restringir el acceso a las líneas VTY en el R2



Fuente: Elaboración propia

R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#exit
R2(config)#line vty 0 15
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#transport input telnet
R2(config-line)#

Figura 42: telnet 172.16.1.2 desde el R1 al R2



Fuente: Elaboración propia

R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenSe prohibe el acceso no autorizado.

User Access Verification

Password:
R2>en
Password:
R2#

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

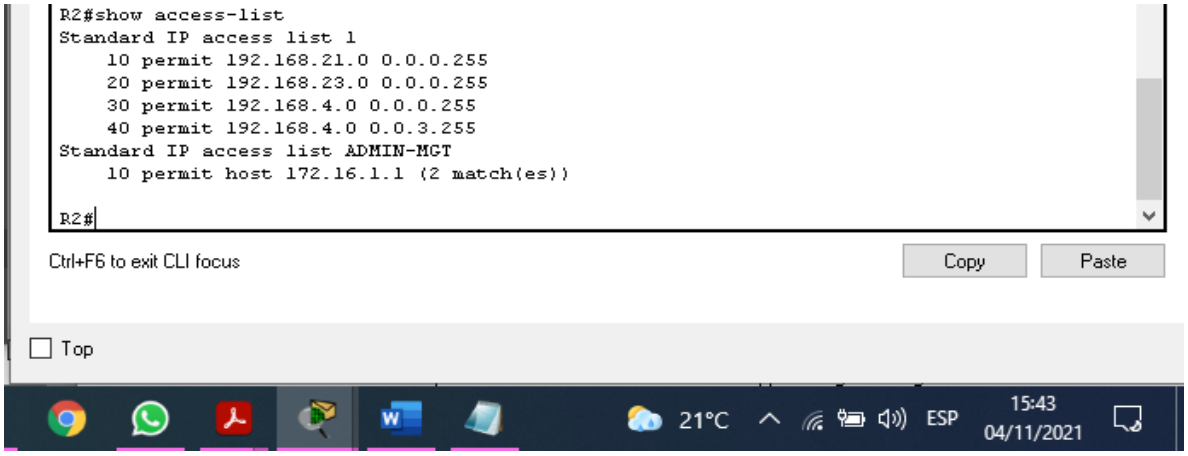
Tabla 28: Comandos solicitados

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 access-list
Restablecer los contadores de una lista de acceso	R2#clear access-list counters (no soportado)
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface

¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation *

Fuente: Elaboración propia

Figura 43: Comandos solicitados show access-list

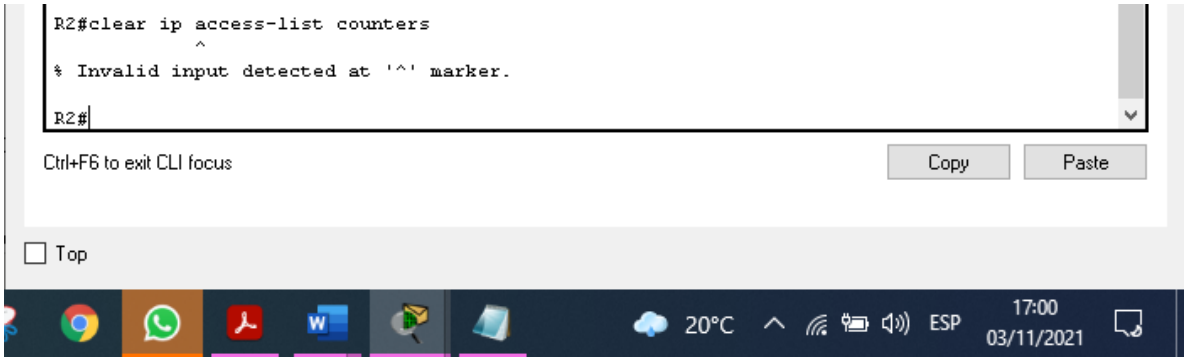


Fuente: Elaboración propia

R2#show access-list
Standard IP access list 1
10 permit 192.168.21.0 0.0.0.255
20 permit 192.168.23.0 0.0.0.255
30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
10 permit host 172.16.1.1 (2 match(es))

R2#

Figura 44: Comandos solicitados clear ip access-list counters



Fuente: Elaboración propia

Restablecer los contadores de una lista de acceso

R2#clear ip access-list counters
R2#clear ip
bgp Clear BGP connections
dhcp Delete items from the DHCP database
nat Clear NAT
ospf OSPF clear commands
route Delete route table entries

Comando show ip interface en R2

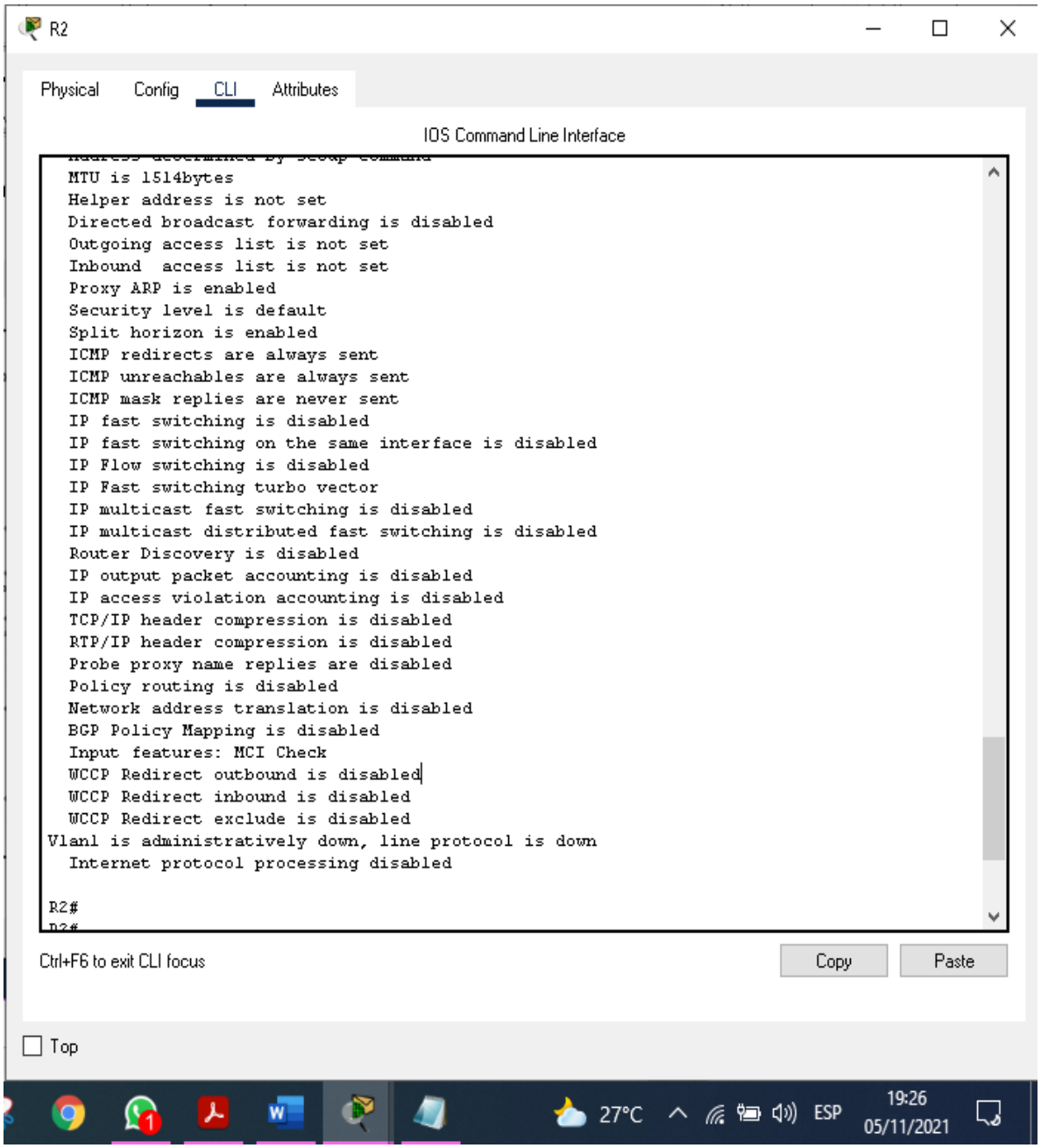
R2#show ip interface
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 209.165.200.233/29
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled

  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: MCI Check
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
GigabitEthernet0/1 is administratively down, line protocol is down (disabled)
  Internet protocol processing disabled
Serial0/0/0 is up, line protocol is up (connected)
  Internet address is 172.16.1.2/30
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled

```
  WCCP Redirect outbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
Serial0/0/1 is up, line protocol is up (connected)
  Internet address is 172.16.2.2/30
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
Loopback0 is up, line protocol is up (connected)
  Internet address is 10.10.10.10/32
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1514bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
```

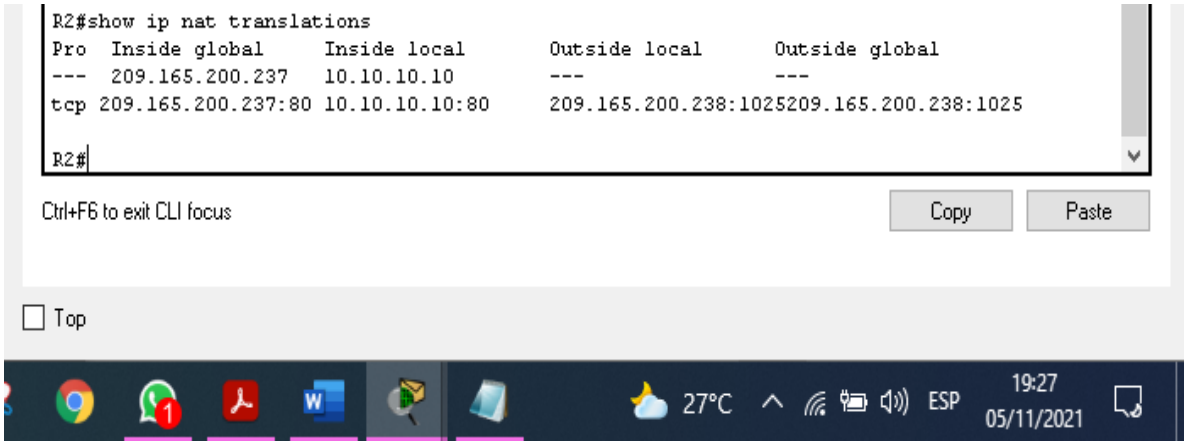
```
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: MCI Check
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
Vlan1 is administratively down, line protocol is down
  Internet protocol processing disabled

R2#
```

Figura 45: comando show ip interface en R2



Fuente: Elaboración propia

Figura 46: comando show ip nat translation en R2

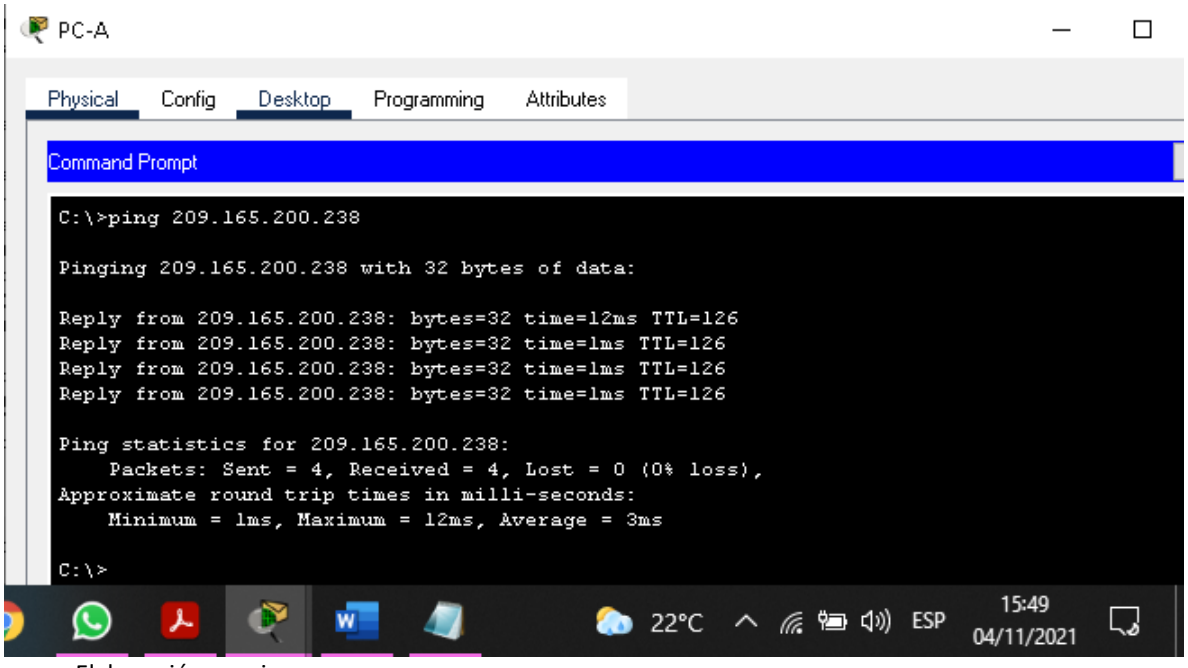


Fuente: Elaboración propia

R2#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.237 10.10.10.10 --- ---
tcp 209.165.200.237:80 10.10.10.10:80
209.165.200.238:1025209.165.200.238:1025

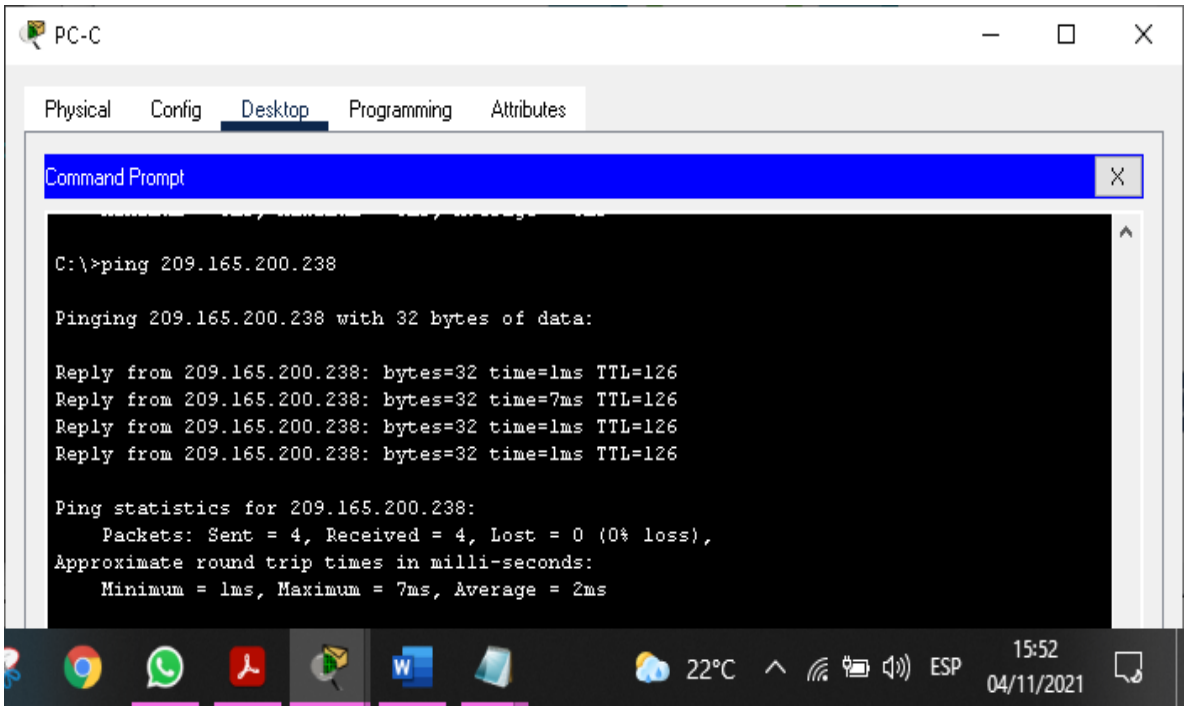
R2#

Figura 47: ping PC-A al PC Internet



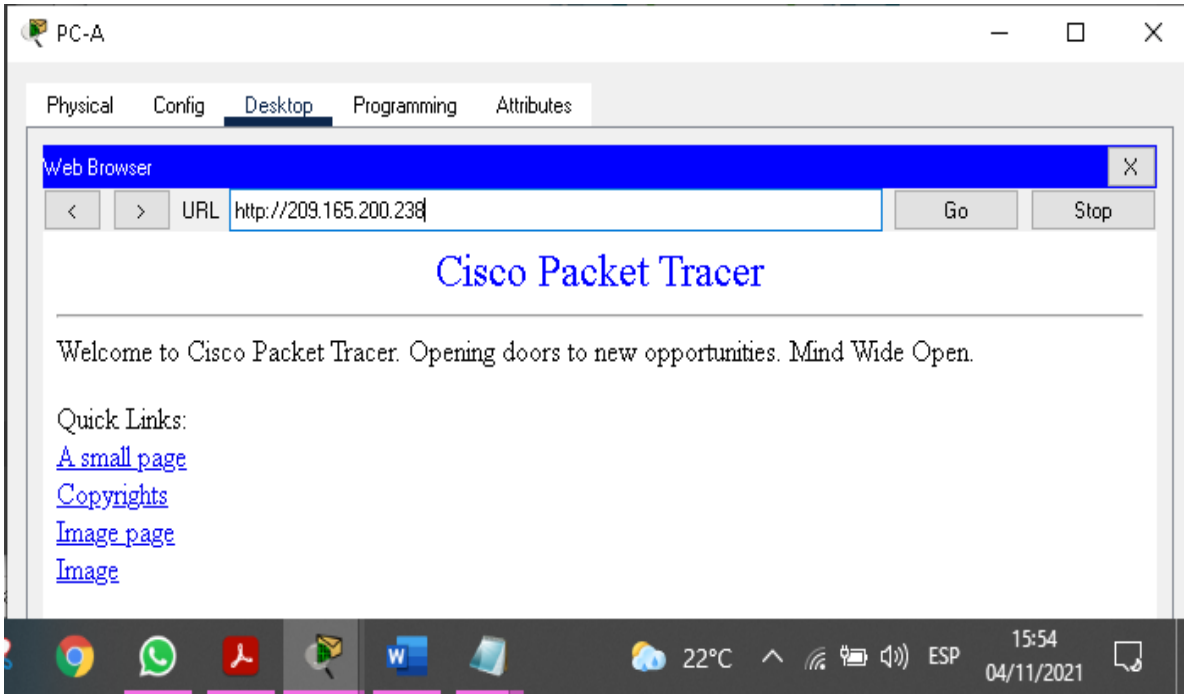
Fuente: Elaboración propia

Figura 48: ping PC-C al PC Internet



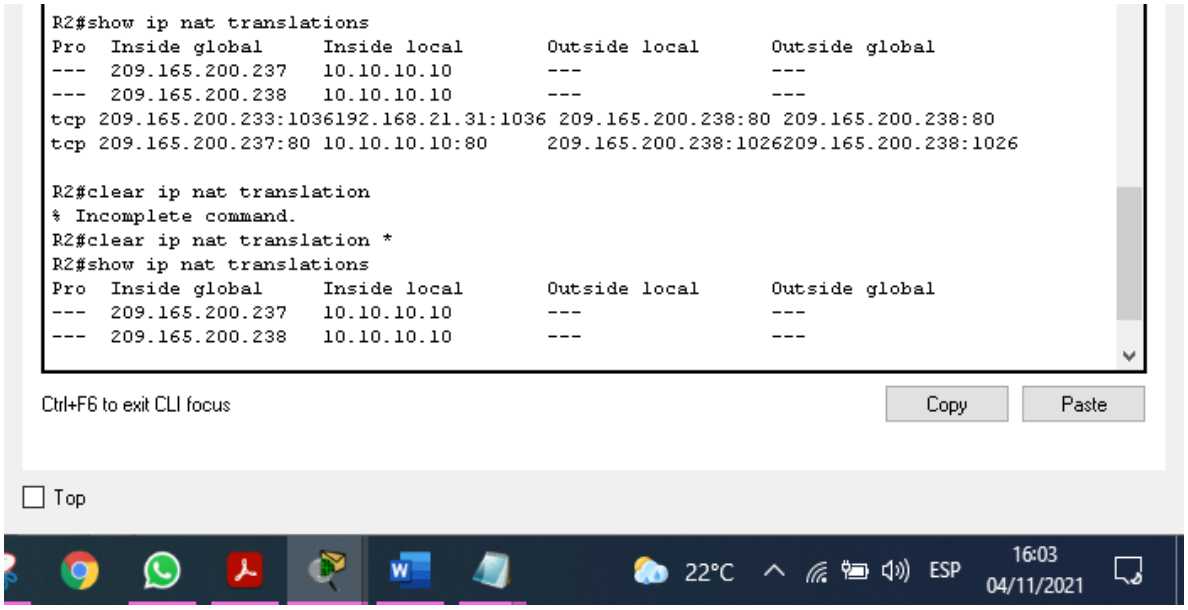
Fuente: Elaboración propia

Figura 49: prueba de acceso del PC-A al servidor web



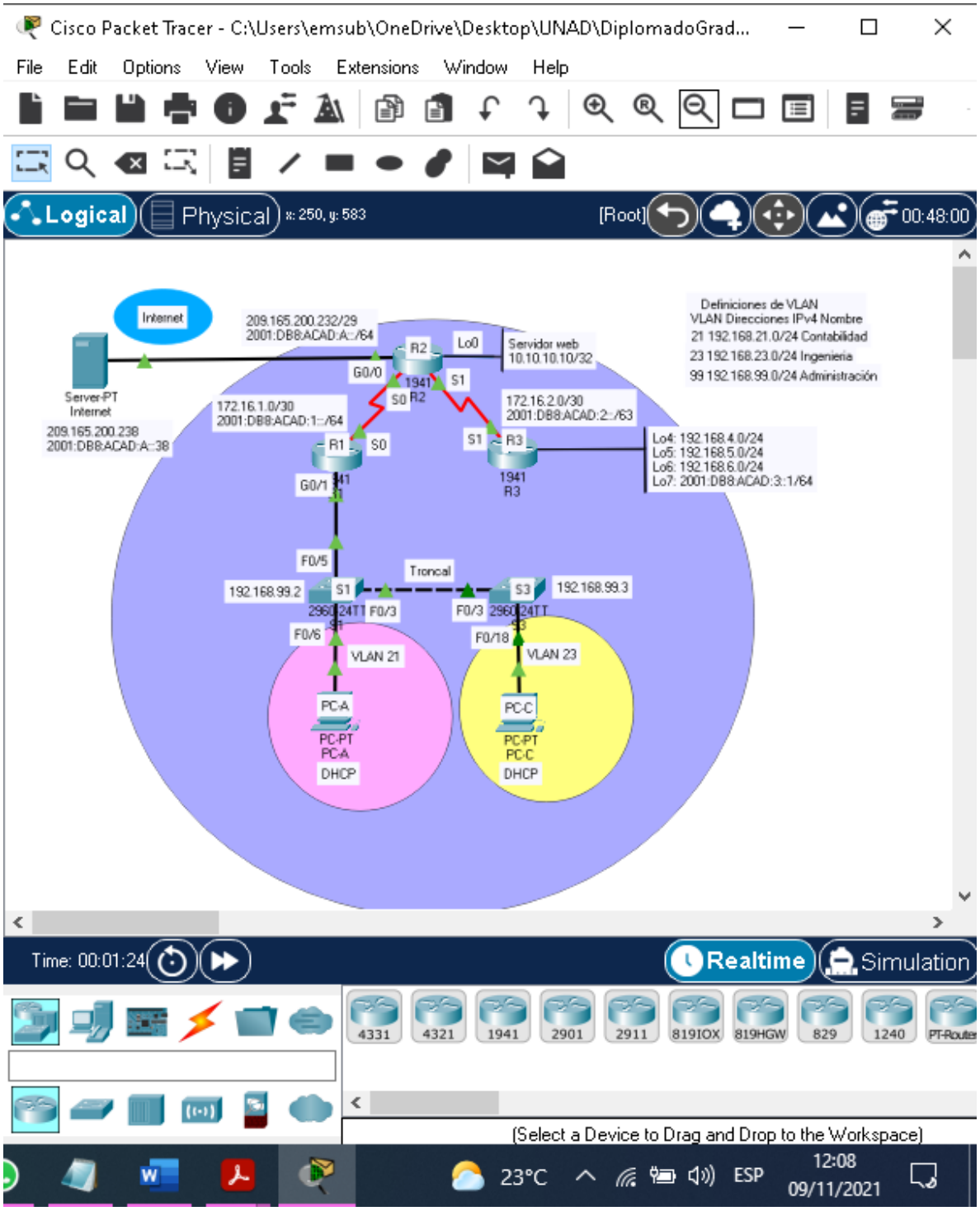
Fuente: Elaboración propia

Figura 50: comando clear ip nat translation en R2



Fuente: Elaboración propia

Figura 51: topología completa y funcional escenario 2.



Fuente: Elaboración propia

CONCLUSIONES

Mediante la utilización de herramientas de simulación se permitió realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento, mediante el uso de comandos de administración de tablas de enrutamiento.

Se identifico problemas propios de conmutación y enrutamiento, mediante el uso adecuado de estrategias basadas en comandos del IOS y estadísticas de tráfico en las interfaces, soportado en modelos de arquitecturas de comunicación, con el fin de resolver problemas de configuración, conectividad y enrutamiento

Se adquirió habilidades de gestión de redes orientadas hacia el mundo profesional y corporativo, además necesarios para planificar, implementar, asegurar, mantener y solucionar problemas de redes convergentes.

Se logro entender el funcionamiento de un sistema de enrutamiento avanzado y su importancia a la hora de implementar en una red de datos.

Con el estudio de estos dos escenarios como trabajo final, se configuro su topología física calculando el direccionamiento adecuado que cumple con las necesidades solicitadas por la guía, finalizando con la implementación en el Packet Tracer.

BIBLIOGRAFIA

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2

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

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

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

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

CISCO. (2019). Exploración de la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1

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

Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

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

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