

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

XENIA XIMENA TIBADUIZA CRUZ

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

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

XENIA XIMENA TIBADUIZA CRUZ

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

DIRECTOR:

MSc. MARIA ALEJANDRA LOPEZ

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

NOTA DE ACEPTACIÓN:

Firma del presidente del jurado

Firma del jurado

Firma del jurado

SOGAMOSO, 24 de Octubre de 2021

DEDICATORIA

Este trabajo está dedicado a Dios, a mi familia, y a mis dos hijos los cuales son mi inspiración para salir adelante, y mis docentes de la UNAD, los cuales me orientaron en este proceso hasta lograr el resultado de estudiar el plan de ingeniería de sistemas y cursos de profundización de Cisco Ccna.

AGRADECIMIENTOS

Primero que todo quiero dar gracias a Dios por ser mi guía, por darme la sabiduría y perseverancia para alcanzar mi carrera como Ingeniera de Sistemas.

A mi papa y mama que me ayudaron y apoyaron económicamente a lo largo de esta carrera, dándome fuerza para resistir y no desfallecer en este camino, mis hermanos quienes me guiaron con sus consejos y conocimientos.

A mi familia, mi esposo y mis dos hijos, quienes fueron mi principal motivo para culminar mis estudios, los cuales son mi motor para salir adelante y a quienes debo dar ejemplo.

A mis amigos y amigas con los cuales compartí, nos apoyamos en este proceso que todos iniciamos con el mismo objetivo, a sí mismo a mis tutores gracias por el apoyo, paciencia y el conocimiento aprendido.

CONTENIDO

NOTA DE ACEPTACION.....	3
DEDICATORIA.....	4
AGRADECIMIENTOS.....	5
CONTENIDO	6
LISTA DE TABLAS	8
LISTA DE FIGURAS	9
GLOSARIO.....	11
RESUMEN.....	12
ABSTRACT	12
INTRODUCCIÓN	13
DESARROLLO	14
Escenario 1	14
Parte 1: Construir en el simulador la Red.....	15
Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2	16
Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta	17
Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1	18
Parte 5: Configurar los hosts y verificar la conectividad entre los equipos	18
Escenario 2	37
ESCENARIO 2.....	37
Topología.....	37
Parte 1: Inicializar dispositivos	38
Paso 1. Inicializar y volver a cargar los routers y los switches.....	38
Parte 2: Configurar los parámetros básicos de los dispositivos	42
Paso 1. Configurar la computadora de Internet.....	42
Paso 2. Configurar R1.....	43
Paso 3. Configurar R2.....	45
Paso 4. Configurar R3.....	49
Paso 5. Configurar S1.....	50
Paso 6: Configurar el S3	54
Paso 7. Verificar la conectividad de la red	56
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN	58
Paso 1. Configurar S1.....	58
Paso 2. Configurar el S3.....	61
Paso 3. Configurar R1.....	63
Paso 4. Verificar la conectividad de la red	65
Parte 4: Configurar el protocolo de routing dinámico OSPF.....	67
Paso 1. Configurar OSPF en el R1	67
Paso 2. Configurar OSPF en el R2	69
Paso 3. Configurar OSPFv3 en el R3	70
Paso 4. Verificar la información de OSPF	71
Parte 5: Implementar DHCP y NAT para IPv4	72

Paso 1. Configurar el R1 como servidor de DHCP	73
Paso 2. Configurar la NAT estática y dinámica en el R2.....	73
Paso 3. Verificar el protocolo DHCP y la NAT estática	76
Parte 6: Configurar NTP	78
Parte 7: Configurar y verificar las listas de control de acceso (ACL).....	80
Paso 1. Restringir el acceso a las líneas VTY en el R2	80
Paso 2: CLI adecuado que se necesita para mostrar lo siguiente	82
CONCLUSIONES	87
BIBLIOGRAFÍA	88

LISTA DE TABLAS

Tabla 1. Tabla de Direccionamiento.....	15
Tabla 2. Direccionamiento de la LAN 1.....	16
Tabla 3. Direccionamiento de la LAN 2.....	17
Tabla 4. Direccionamiento conexión.....	17
Tabla 5. Configuración de R1.....	18
Tabla 6. Configuración en S1.....	25
Tabla 7. Configuración del PC-A.....	32
Tabla 8. Configuración del PC-B.....	33
Tabla 9: Inicializar y volver a cargar los routers y los switches.....	38
Tabla 10: Configurar la computadora de Internet.....	42
Tabla 11: de subnet IPV4.....	43
Tabla 12: de subnet IPV6.....	43
Tabla 13: Configurar R1.....	44
Tabla 14: Configuración R2.....	46
Tabla 15: Configuración R3.....	49
Tabla 16: Configuración S1.....	53
Tabla 17: Configuración S3.....	54
Tabla 18: Verificar la conectividad de la red.....	56
Tabla 19: Configurar S3.....	61
Tabla 21 : Configuración R1.....	63
Tabla 22: Verificar la conectividad de la red.....	65
Tabla 23: Configurar OSPF en el R1.....	67
Tabla 24: Configurar OSPF en el R2.....	69
Tabla 24: Configurar OSPFv3 en el R3.....	70
Tabla 25: Verificar la información de OSPF.....	71
Tabla 26: Configurar el R1 como servidor de DHCP.....	72
Tabla 27: Configurar la NAT estática y dinámica en el R2.....	74
Tabla 28: Verificar el protocolo DHCP y la NAT estática.....	76
Tabla 29: Configurar NTP.....	78
Tabla 30: Restringir el acceso a las líneas VTY en el R2.....	80
Tabla 31: Introducir el comando de CLI adecuado.....	82

LISTA DE FIGURAS

Figura 1. Escenario 1	14
Figura 2. Simulación Escenario 1	14
Figura 3. Construcción de la red.....	16
Figura 4. Desactivar DNS	20
Figura 5. Nombre del router	20
Figura 6. Nombre de dominio.....	20
Figura 7. Contraseña cifrada.....	21
Figura 8. Contraseña consola.....	21
Figura 9. Longitud contraseña	21
Figura 10. Crear usuario	22
Figura 11. Configurar vty	22
Figura 12. Configurar vty-ssh	23
Figura 13. Cifrar contraseñas.....	23
Figura 14. Configurar MOTD.....	24
Figura 15. Configurar G0/0/0.....	24
Figura 16. Configurar G0/0/1.....	25
Figura 17. Desactivar DNS S1	27
Figura 18. Nombre S1.....	27
Figura 19. Nombre dominio S1	28
Figura 20. Contraseña cifrada S1.....	28
Figura 21. Contraseña consola S1.....	28
Figura 22. Crear usuario S1.....	29
Figura 23. Configurar vty S1	29
Figura 24. Configurar vty-ssh S1.....	30
Figura 25. Cifrar contraseña S1	30
Figura 26. Configurar Motd S1.....	31
Figura 27. Generar RSA S1	31
Figura 28. Configurar interfaz S1	31
Figura 29. Configurar gateway S1	32
Figura 30. Configuración de PC-A	33
Figura 31. Configuración de PC-B.....	34
Figura 32. Ping PC-B	35
Figura 33. Ping PC-A	36
Figura 34: Topología.....	37
Figura 35: R1 Eliminar el archivo startup-config y volver a cargarlos.....	38
Figura 36: R2 Eliminar el archivo startup-config y volver a cargarlos.....	39
Figura 37: R3 Eliminar el archivo startup-config y volver a cargarlos.....	39
Figura 38: S1 Eliminar el archivo startup-config y volver a cargarlos.....	40
Figura 39: S1 Verificar que la base de datos de VLAN.....	40
Figura 40: S3 Eliminar el archivo startup-config y volver a cargarlos.....	41
Figura 41: S3 Verificar que la base de datos de VLAN.....	41

Figura 42: Configurar la computadora de Internet	42
Figura 43: Configuración R1	45
Figura 44: Configuración R2	48
Figura 45: Configuración R2	48
Figura 46: Configuración R3	51
Figura 47: Configuración R3	51
Figura 48: Configuración R3	52
Figura 49: Configuración S1	54
Figura 50: Configuración S3	55
Figura 51: Ping de R1 a R2	57
Figura 52: Ping de R2 a R3	57
Figura 53: Ping de Pc de Internet a Gateway predeterminado	57
Figura 54: Configuración S1	59
Figura 55: Configuración S1	60
Figura 56: Configuración S3	62
Figura 57: Configuración S3	63
Figura 58: Configuración R1	64
Figura 59: Ping de S1 a R1	66
Figura 60: Ping de S3 a R1	67
Figura 61: Ping de S1 a R1	67
Figura 62: Ping de S3 a R1	67
Figura 63: Configurar OSPF en el R1	68
Figura 64: Configurar OSPF en el R2	69
Figura 65: Configurar OSPFv3 en el R3	71
Figura 66: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23	73
Figura 67: Configurar la NAT estática y dinámica en el R2	75
Figura 68: Verificar que la PC-A A IP del servidor de DHCP	76
Figura 69: Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	77
Figura 70: Verificar que la PC-A pueda hacer ping a la PC-C	77
Figura 71: Ajuste la fecha y hora en R2	78
Figura 72: Configure R2 como un maestro NTP	79
Figura 73: Restringir el acceso a las líneas VTY en el R2	80
Figura 74: Verificar que la ACL funcione como se espera	81
Figura 75: Verificar conexión	81
Figura 76: Mostrar las coincidencias recibidas	83
Figura 77: Restablecer los contadores de una lista de acceso	83
Figura 78: Con qué comando se muestran las traducciones NAT?	84
Figura 79: Prueba de ping al Servidor de Internet desde la PC-A	84
Figura 80: Prueba de ping al Servidor de Internet desde la PC-C	85
Figura 81: Prueba de acceso al Servidor de Web desde PC-A	85
Figura 82: Eliminar las traducciones de NAT dinámicas	86
Figura 83: Topología de red escenario 2 - Cisco Packet Tracer	86

GLOSARIO

CONEXIÓN: Una conexión de red designa la conexión entre un equipo informático y una red informática. Es un enlace entre un emisor y un receptor a través del cual se envía un mensaje.

DIRECCION IP: Este protocolo es un conjunto de reglas para la comunicación a través de Internet, ya sea el envío de correo electrónico, la transmisión de vídeo o la conexión a un sitio web. Una dirección IP identifica una red o dispositivo en Internet.

HOST: también conocido como hosting, hospedaje o anfitrión, es cualquier computadora o máquina conectada a una red mediante un número de IP definido y un dominio, que ofrece recursos, información y servicios a sus usuarios.

INTERFACE: Se conoce como la interfaz de usuario al medio que permite a una persona comunicarse con una máquina. La interfaz, en este caso, está compuesta por los puntos de contacto entre un usuario y el ordenador.

MASCARA DE SUBRED: Permite a nuestro sistema reconocer cuál parte de nuestra dirección IP identifica a nuestra red y cuál a los equipos.

ROUTER: Un router es un dispositivo que ofrece una conexión Wi-Fi, que normalmente está conectado a un módem y que envía información de Internet a tus dispositivos personales, como ordenadores, teléfonos o tablets. Los dispositivos que están conectados a Internet en tu casa conforman tu red de área local (LAN).

SWITCH: Un switch o conmutador es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet.

RESUMEN

En el programa de Ingeniería de Sistemas se tomó como opción de grado el diplomado de profundización Cisco (diseño e implementación de soluciones integradas lan / wan), configurando los Routing y switching de CCNA: aprendiendo los Principios básicos de routing y switching,

Por medio de la elaboración de laboratorios tanto en packet tracer como en Smarlab se practicó las diferentes formas de conmutación y enrutamiento de diferentes redes, se conocieron los dispositivos las clases de ellos, los tipos de conexión electrónica de cada uno de ellos, y a plantear la solución de un problema propuesto.

Para poder aprobar la certificación CCNP se practicaron mecanismos de comunicación, acceso a la red, comunicaciones sobre Ethernet, direccionamiento ip, subnetting, enrutamiento estatico, gestión de equipos networking; por medio de las simulaciones se establecieron conexiones entre equipos, ping entre las pc, envío de paquetes, en cada uno de los escenarios propuestos dando solución a cada uno de ellos.

Palabras Clave: CISCO, CCNP, CONMUTACIÓN, ENRUTAMIENTO, REDES, ELECTRÓNICA.

ABSTRACT

In the Systems Engineering program, the Cisco deepening diploma (design and implementation of integrated lan / wan solutions) was taken as a degree option, configuring CCNA routing and switching: learning the basic principles of routing and switching,

Through the elaboration of laboratories both in packet tracer and in Smarlab, the different forms of switching and routing of different networks were practiced, the devices were known, their classes, the types of electronic connection of each one of them, and to raise the solution of a proposed problem.

In order to pass the CCNP certification, communication mechanisms, network access, communications over Ethernet, IP addressing, subnetting, static routing, networking equipment management were practiced; Through the simulations, connections between computers were established, pinging between the PCs, sending packets, in each of the proposed scenarios, providing a solution to each one of them.

Keywords: CISCO, CCNP, ROUTING, SWICTHING, NETWORKING, ELECTRONICS

INTRODUCCION

El Diplomado Cisco CCNP permite desarrollar la capacidad de planificar, implementar, verificar y solucionar problemas de redes empresariales locales y de amplia y trabajar en colaboración con especialistas en soluciones avanzadas de seguridad, voz, redes inalámbricas y video.

El objetivo del diplomado es aprender a realizar redes en las cuales se deben configurar tanto switch, router, establecer conexiones, configurar los dispositivos con el fin de solucionar una problemática por medio de la Simulación donde se realizar pines para probar la conectividad entre ellos.

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.

En el escenario 2 Se debe configurar una red pequeña para que admita de conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el 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.

DESARROLLO

1. ESCENARIO 1

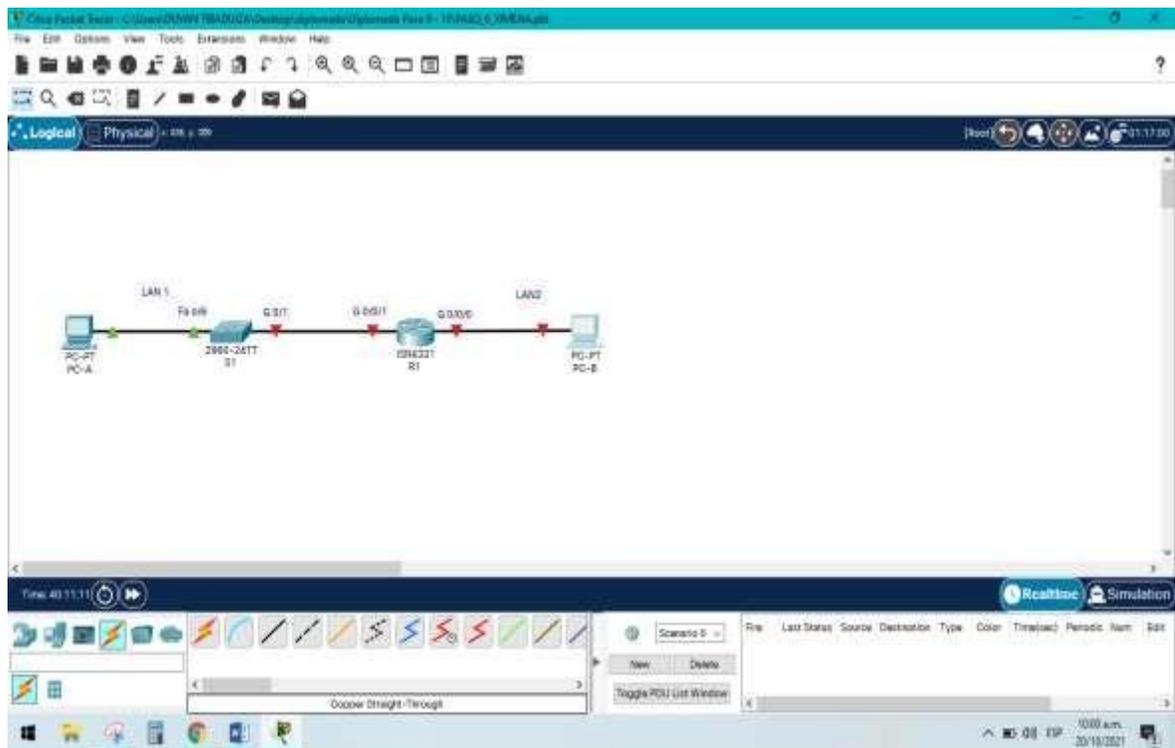
Figura 1: Escenario 1

Topología



Fuente: Prueba de habilidades CCNA II-2021

Figura 2. Simulación de 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 5: 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 switch S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

Tabla 1: Tabla de Direccionamiento

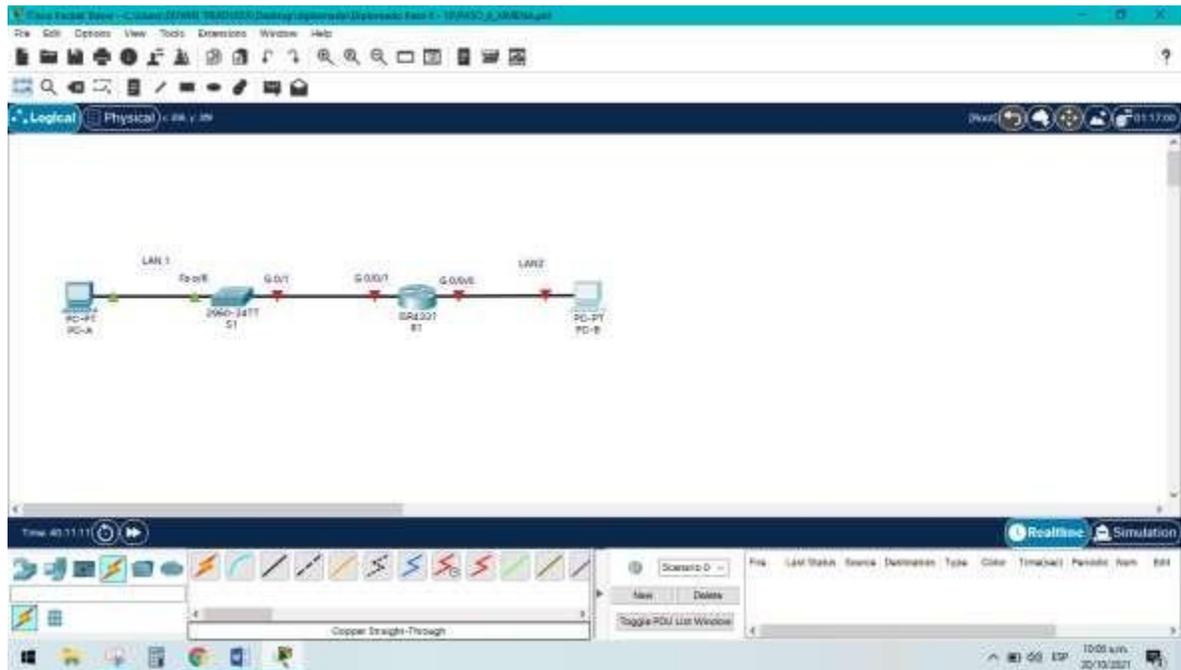
RED	HOST	MASCARA DE SUBRED	DIRECCION IP	PRIMERA IP UTIL	ULTIMA IP UTIL	BROADCAST	HOST DISPONIBLE
LAN 1	100	255.255.255.128	192.168.57.0/25	192.168.57.1	192.168.57.126	192.168.57.127	126
LAN 2	50	255.255.255.192	192.168.57.128/26	192.168.57.129	192.168.57.190	192.168.57.191	62

Fuente: Elaboración propia.

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 3. Construcción de la red



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.

Tabla 2: Direccionamiento de la LAN 1

Red	LAN 1
Host	100
Mascara de subred	255.255.255.128
Dirección IP	192.168.57.0/25
Primera IP útil	192.168.57.1
Ultima IP útil	192.168.57.126
Broadcast	192.168.57.127
Host disponible	126

Fuente: Elaboración propia.

Tabla 3: Direccionamiento de LAN 2

Red	LAN 2
Host	50
Mascara de subred	255.255.255.192
Dirección IP	192.168.57.128/26
Primera IP útil	192.168.57.129
Ultima IP útil	192.168.57.190
Broadcast	192.168.57.191
Host disponible	62

Fuente: Elaboración propia.

Tabla de direccionamiento

Ítem	Requerimiento
Dirección de Red	192.168.57.0 donde X corresponde a los últimos dos dígitos de su cédula.
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	192.168.57.1
R1 G0/0/0	192.168.57.129
S1 SVI	192.168.57.2
PC-A	192.168.57.126
PC-B	192.168.57.190

Fuente: Prueba de Habilidades CCNA II-2021

Mi número de cedula es 1.58.274.857 por lo tanto utilicé los dos últimos dígitos para la red que son 57.

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 5. Configuración de R1

Tarea	Especificación
Desactivar la búsqueda DNS	R1>enable R1#configure terminal R1(config)#no ip domain-lookup
Nombre del router	R1 R1(config)#hostname R1
Nombre de dominio	ccna-lab.com R1(config)#ip domain-name ccna-lab.com
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)#exit
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)#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]

	<pre>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#</pre>
Cifrar las contraseñas de texto no cifrado	<pre>R1(config)#service password-encryption</pre>
Configure un MOTD Banner	<pre>R1(config)#banner motd ¡SOLO PERSONAL AUTORIZADO DE LA UNAD!</pre>
Configurar interfaz G0/0/0	<p>Establezca la descripción Establece la dirección IPv4. Activar la interfaz.</p> <pre>R1(config)#interface gigabitethernet 0/0/0 R1(config-if)#ip address 192.168.57.129 255.255.255.128 R1(config-if)#no shutdown R1(config-if)#exit</pre>
Configurar interfaz G0/0/1	<p>Establezca la descripción Establece la dirección IPv4. Activar la interfaz.</p> <pre>R1(config)#interface gigabitethernet 0/0/1 R1(config-if)#ip address 192.168.57.1 255.255.255.128 R1(config-if)#no shutdown R1(config-if)#exit</pre>
Generar una clave de cifrado RSA	<p>Módulo de 1024 bits</p> <pre>R1(config)#crypto key generate rsa</pre> <p>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.</p>

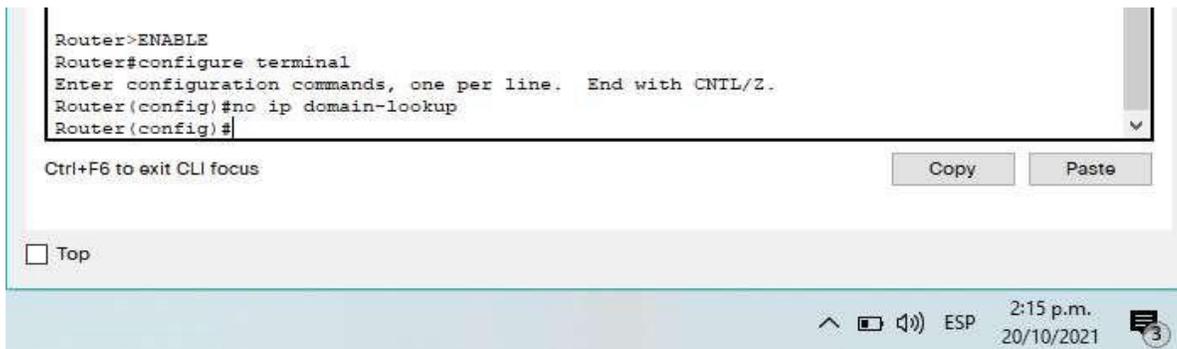
	How many bits in the modulus [512]: 10% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
--	---

Fuente: Prueba de Habilidades CCNA II-2021

Pantallazos de evidencia del código:

Figura 4. Desactivar DNS

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
Router(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

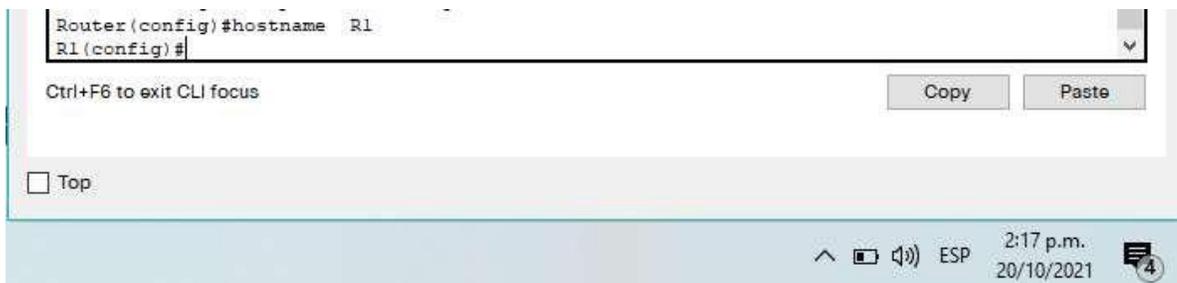
Top

2:15 p.m. 20/10/2021

Fuente: Elaboración propia.

Figura 5: Nombre del router

Nombre del router



```
Router(config)#hostname R1
R1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

2:17 p.m. 20/10/2021

Fuente: Elaboración propia.

Figura 6: Nombre de dominio

Nombre de dominio



```
R1(config)#ip domain-name ccna-lab.com
R1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

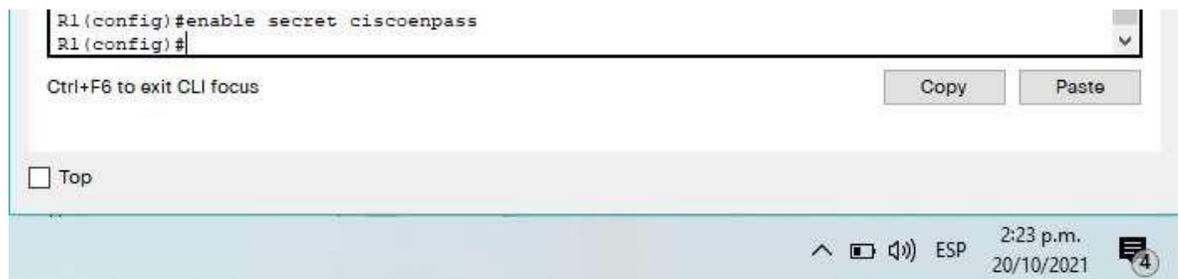
Top

ESP 2:20 p.m. 20/10/2021

Fuente: Elaboración propia.

Figura 7: Contraseña cifrada

Contraseña cifrada para el modo EXECprivilegiado



```
R1(config)#enable secret ciscoconpass
R1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

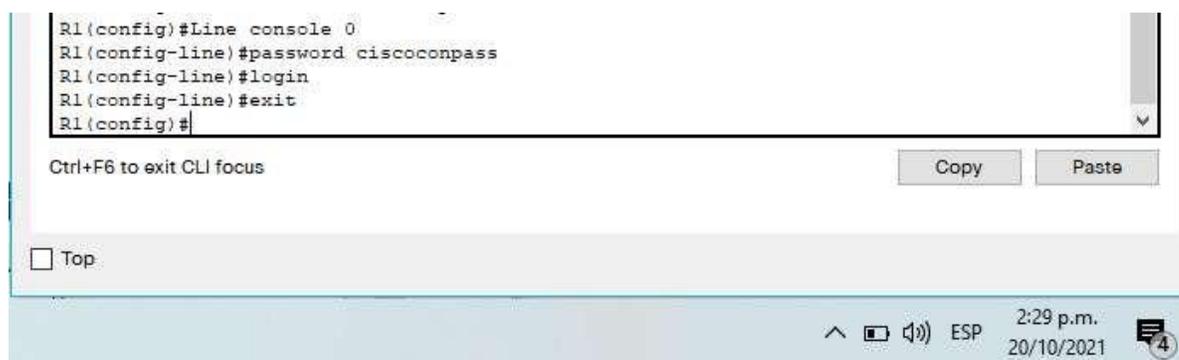
Top

ESP 2:23 p.m. 20/10/2021

Fuente: Elaboración propia.

Figura 8: Contraseña consola

Contraseña de acceso a la consola



```
R1(config)#Line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

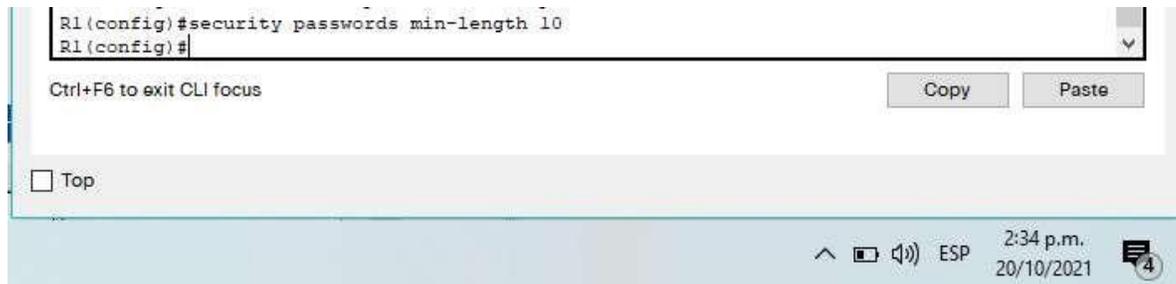
Top

ESP 2:29 p.m. 20/10/2021

Fuente: Elaboración propia.

Figura 9. Longitud contraseña

Establecer la longitud mínima para las contraseñas



```
R1(config)#security passwords min-length 10
R1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

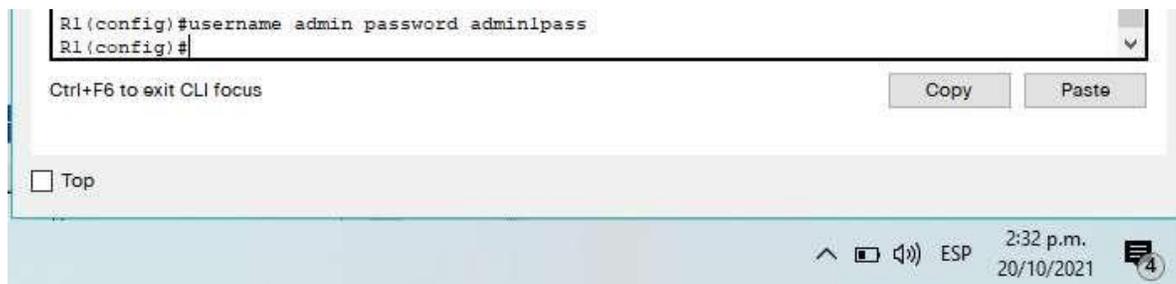
Top

ESP 2:34 p.m. 20/10/2021

Fuente: Elaboración propia.

Figura 10: Crear usuario

Crear un usuario administrativo en la base de datos local



```
R1(config)#username admin password adminpass
R1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

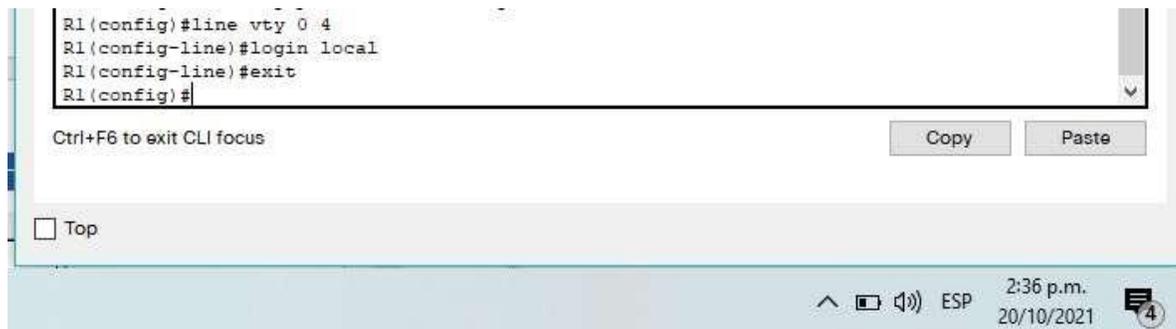
Top

ESP 2:32 p.m. 20/10/2021

Fuente: Elaboración propia.

Figura 11: Configurar vty

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)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

ESP 2:36 p.m. 20/10/2021

Fuente: Elaboración propia.

Figura 12: Configurar vty-ssh

Configurar VTY solo aceptando SSH

```
Router(config)#hostname R1
R1(config)#ip domain-name ccna-lab.com
R1(config)#enable secret ciscoenpass
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit
R1(config)#username admin password adminpass
R1(config)#security passwords min-length 10
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#exit
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 260 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 2 20:49:14.419: %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 adminpass
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

ESP 2:46 p.m. 20/10/2021

Fuente: Elaboración propia.

Figura 13: Cifrar contraseñas

Cifrar las contraseñas de texto no cifrado

```
R1(config)#service password-encryption
R1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

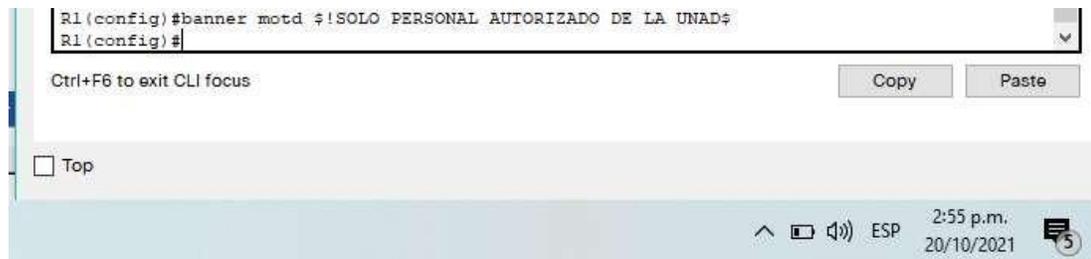
Top

ESP 2:52 p.m. 20/10/2021

Fuente: Elaboración propia.

Figura 14: Configurar MOTD

Configure un MOTD Banner



```
R1(config)#banner motd #!SOLO PERSONAL AUTORIZADO DE LA UNAD#
R1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

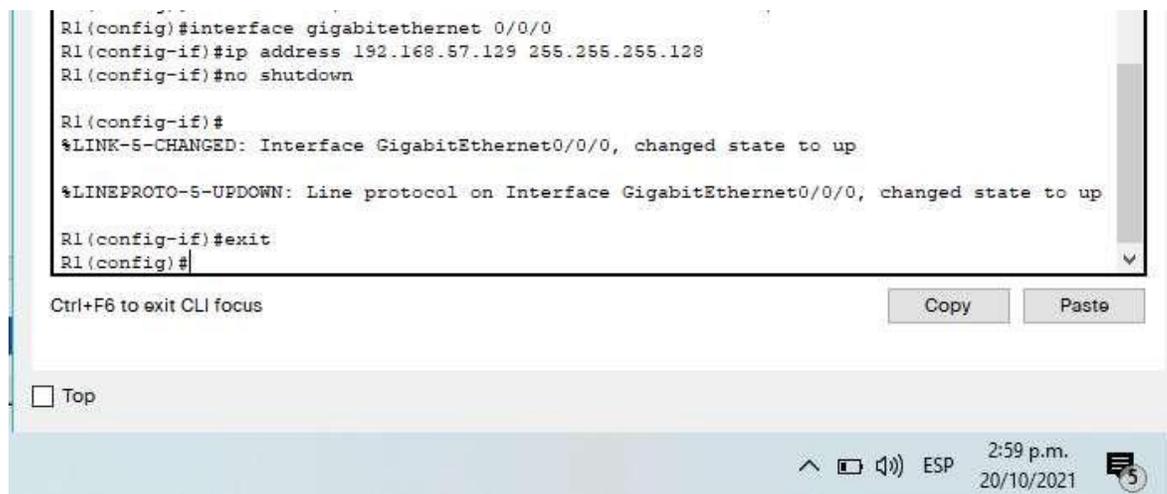
^ [] [] ESP 2:55 p.m. 20/10/2021 [5]

Detailed description: This screenshot shows a terminal window with a network device's CLI. The user has entered the command 'banner motd #!SOLO PERSONAL AUTORIZADO DE LA UNAD#' and is now at the 'R1(config)#' prompt. The interface includes a 'Copy' and 'Paste' button, a 'Top' link, and a system tray at the bottom right showing the time as 2:55 p.m. on 20/10/2021 and a notification icon with the number 5.

Fuente: Elaboración propia.

Figura 15: Configurar G0/0/0

Configurar interfaz G0/0/0



```
R1(config)#interface gigabitethernet 0/0/0
R1(config-if)#ip address 192.168.57.129 255.255.255.128
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

R1(config-if)#exit
R1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

^ [] [] ESP 2:59 p.m. 20/10/2021 [5]

Detailed description: This screenshot shows a terminal window with a network device's CLI. The user has configured interface GigabitEthernet0/0/0 with IP address 192.168.57.129 and subnet mask 255.255.255.128, and has disabled shutdown. The interface is now up. The user has exited the interface configuration mode and returned to the 'R1(config)#' prompt. The interface includes a 'Copy' and 'Paste' button, a 'Top' link, and a system tray at the bottom right showing the time as 2:59 p.m. on 20/10/2021 and a notification icon with the number 5.

Fuente: Elaboración propia.

Figura 16: Configurar G0/0/1

Configurar interfaz G0/0/1

```

R1(config)#interface gigabitethernet 0/0/1
R1(config-if)#ip address 192.168.57.1 255.255.255.128
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

R1(config-if)#exit
R1(config)#

```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

ESP 3:59 p.m. 20/10/2021

Fuente: Elaboración propia.

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 6. Configuración de S1

Tarea	Especificación
Desactivar la búsqueda DNS.	S1>enable S1#configure terminal S1(config)#no ip domain-lookup
Nombre del switch	S1 S1(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	Nombre de usuario: admin Password: admin1pass S1#configure terminal

datos local	S1(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 las líneas VTY para que acepten únicamente las conexiones 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 AUTORIZADO POR LA UNAD\$
Generar una clave de cifrado RSA	Módulo de 1024 bits 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]
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento S1(config)#int vlan 1 S1(config-if)#ip address 192.168.57.2 255.255.255.128 S1(config-if)#no shutdown 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 192.168.57.1

Fuente: Prueba de Habilidades CCNA II-2021

Figura 17: Desactivar DNS S1

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
Switch(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

ESP 4:32 p.m. 20/10/2021

Fuente: Elaboración propia.

Figura 18: Nombre S1

Nombre del switch

```
Switch(config)#hostname S1
S1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

ESP 4:33 p.m. 20/10/2021

Fuente: Elaboración propia

Figura 19: Nombre dominio S1

Nombre de dominio

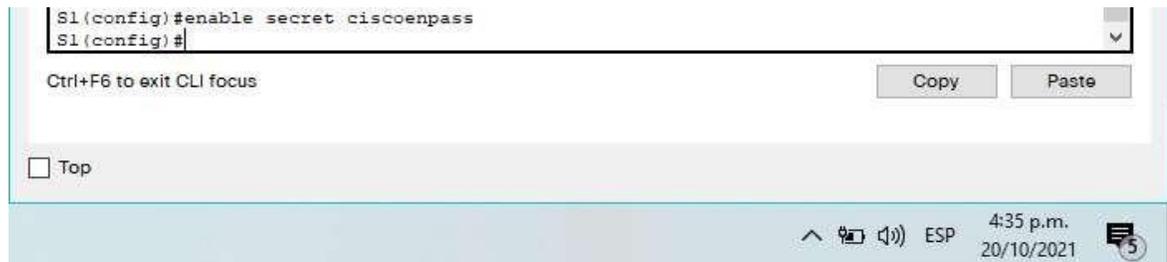


The screenshot shows a Cisco CLI window with the following text: `S1(config)#ip domain-name ccna-lab.com` and `S1(config)#`. Below the terminal area, there is a 'Top' button and a system tray at the bottom right showing the time as 4:34 p.m. on 20/10/2021.

Fuente: Elaboración propia

Figura 20: Contraseña cifrada S1

Contraseña cifrada para el modo EXEC privilegiado

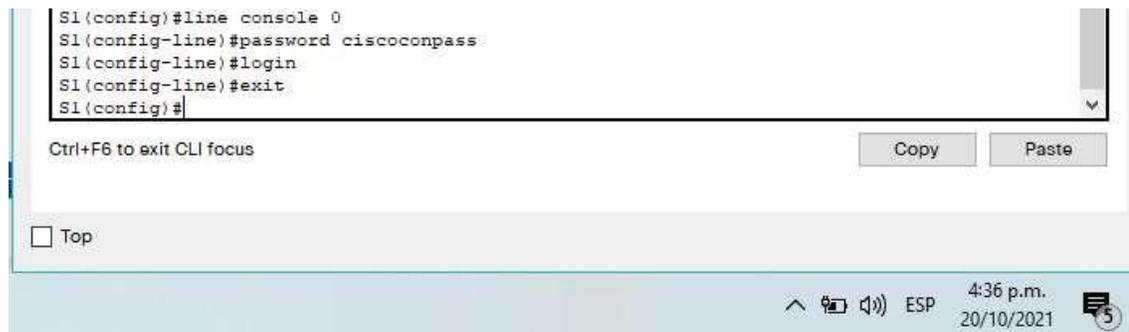


The screenshot shows a Cisco CLI window with the following text: `S1(config)#enable secret ciscoenpass` and `S1(config)#`. Below the terminal area, there is a 'Top' button and a system tray at the bottom right showing the time as 4:35 p.m. on 20/10/2021.

Fuente: Elaboración propia

Figura 21: Contraseña consola S1

Contraseña de acceso a la consola

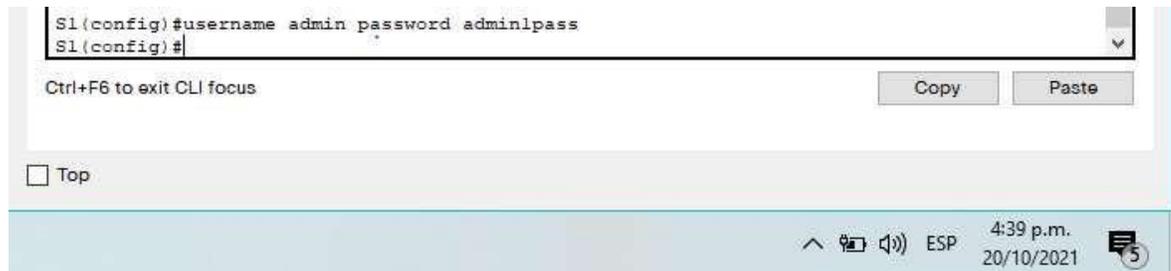


The screenshot shows a Cisco CLI window with the following text: `S1(config)#line console 0`, `S1(config-line)#password ciscoconpass`, `S1(config-line)#login`, `S1(config-line)#exit`, and `S1(config)#`. Below the terminal area, there is a 'Top' button and a system tray at the bottom right showing the time as 4:36 p.m. on 20/10/2021.

Fuente: Elaboración propia

Figura 22: Crear usuario S1

Crear un usuario administrativo en la base de datos local



```
S1(config)#username admin password adminpass
S1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

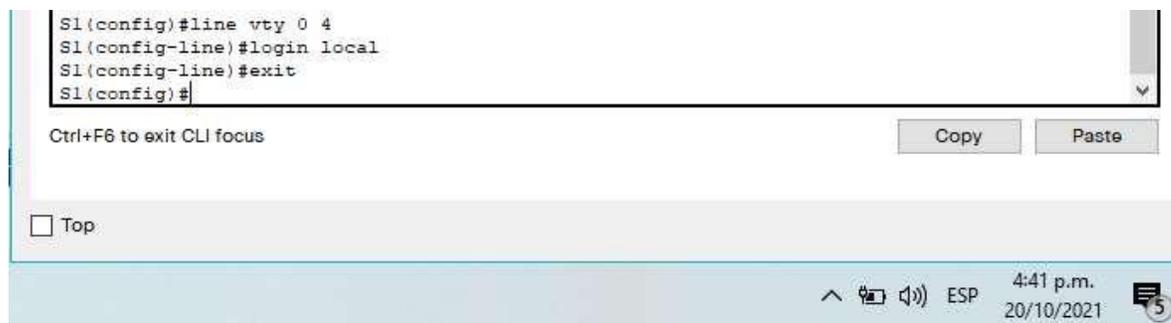
Top

^ [network icon] [volume icon] ESP 4:39 p.m. 20/10/2021 [notifications icon]

Fuente: Elaboración propia

Figura 23: Configurar vty S1

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local



```
S1(config)#line vty 0 4
S1(config-line)#login local
S1(config-line)#exit
S1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

^ [network icon] [volume icon] ESP 4:41 p.m. 20/10/2021 [notifications icon]

Fuente: Elaboración propia

Figura 24: Configurar vty-ssh S1

Configurar las líneas VTY para que acepten únicamente las conexiones SSH

```
S1(config)#enable secret ciscoenpass
S1(config)#line console 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit
S1(config)#configure terminal
^
% Invalid input detected at '^' marker.
S1(config)#username admin password adminpass
S1(config)#line vty 0 4
S1(config-line)#login local
S1(config-line)#exit
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 2 22:46:46.73: %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 adminpass
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

4:44 p.m. 20/10/2021

Fuente: Elaboración propia

Figura 25: Cifrar contraseña S1

Cifrar las contraseñas de texto no cifrado

```
S1(config)#service password-encryption
S1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

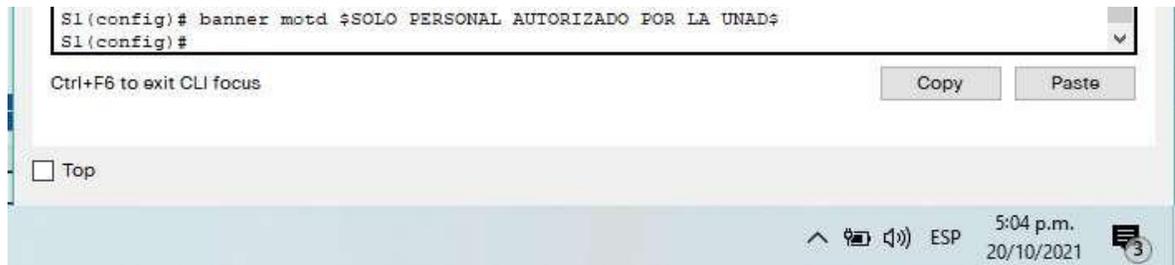
Top

4:47 p.m. 20/10/2021

Fuente: Elaboración propia

Figura 26: Configurar Motd S1

Configure un MOTD Banner



```
S1(config)# banner motd $SOLO PERSONAL AUTORIZADO POR LA UNAD$
S1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

5:04 p.m. 20/10/2021

Fuente: Elaboración propia

Figura 27: Generar RSA S1

Generar una clave de cifrado RSA



```
S1(config)#crypto key generate rsa
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

5:07 p.m. 20/10/2021

Fuente: Elaboración propia

Figura 28. Configurar interfaz S1

Configurar la interfaz de administración (SVI)



```
S1(config)#int vlan 1
S1(config-if)#ip address 192.168.57.2 255.255.255.128
S1(config-if)#no shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#exit
S1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

5:09 p.m. 20/10/2021

Fuente: Elaboración propia

Figura 29. Configurar gateway S1

Configuración del gateway predeterminado



```
S1 (config) #ip default-gateway 192.168.57.1
S1 (config) #
```

Fuente: Elaboración propia

Paso 2. Configurar los equipos

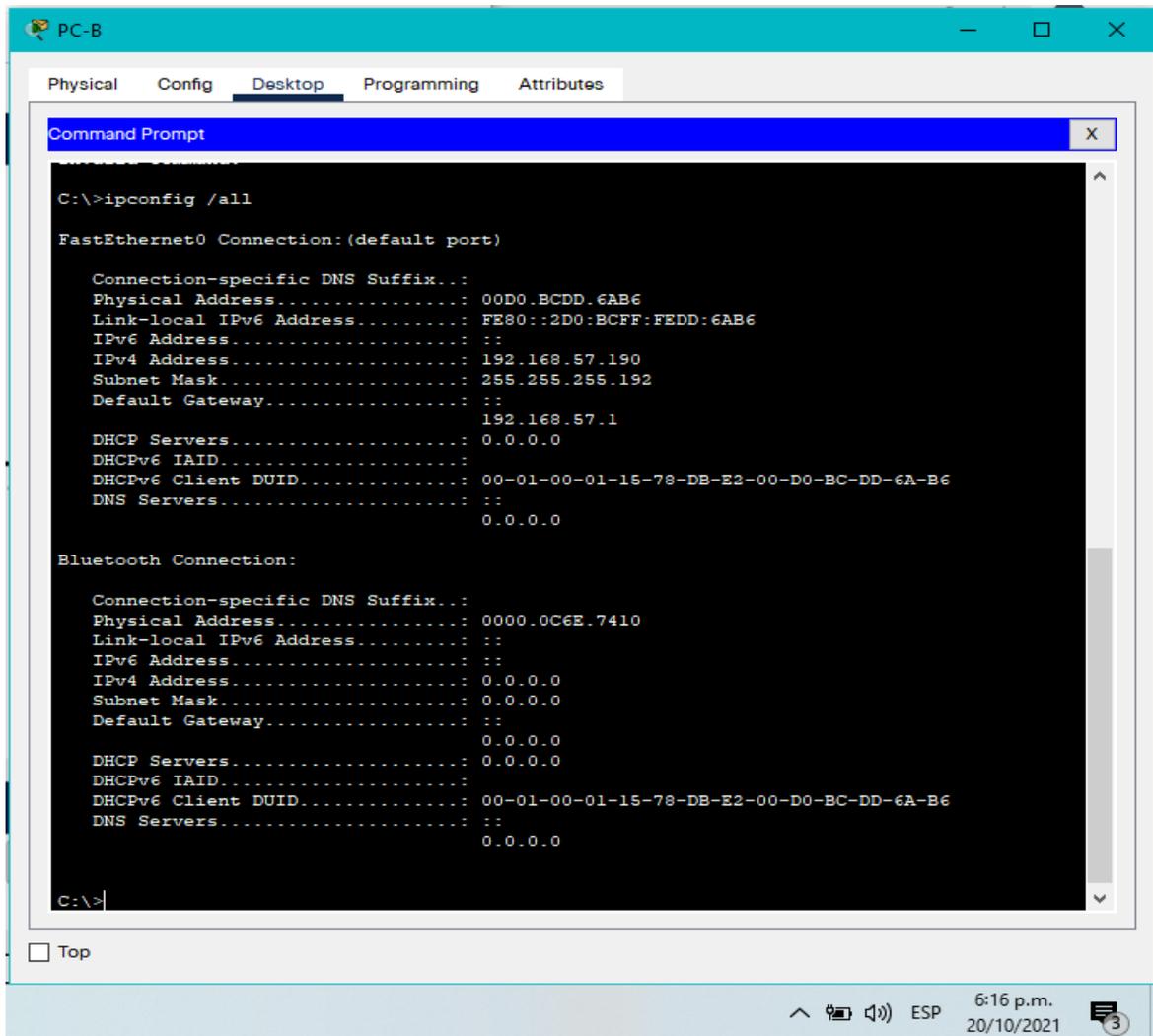
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all**.

Tabla 7. Configuración de PC-A

PC-A Network Configuration	
Descripción	El PC-A esta configurado y conectado a una red Lan 1, con las siguientes características que se mencionan.
Dirección física	0001.9722.1175
Dirección IP	192.168.57.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.57.1

Fuente: Prueba de Habilidades CCNA II-2021

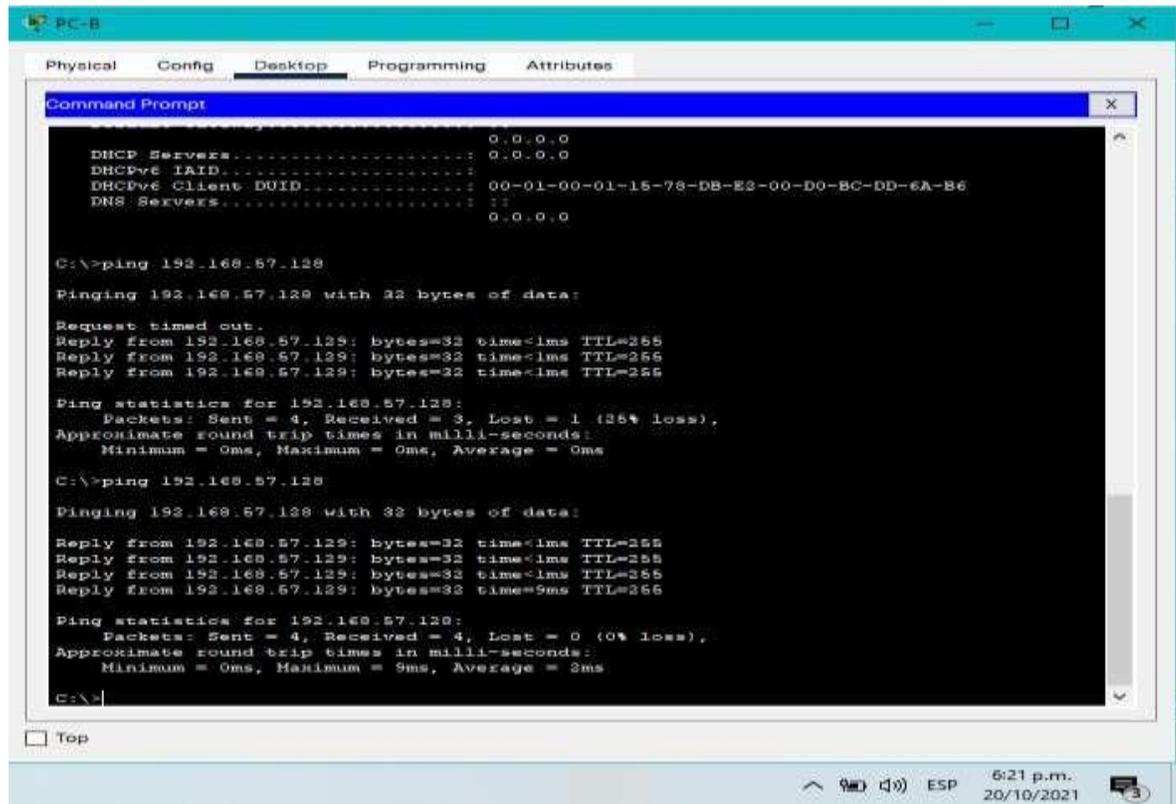
Figura 31: Configuración de PC-B



Fuente: Elaboración propia

Ping del PC-B al PC-A para probar la conectividad

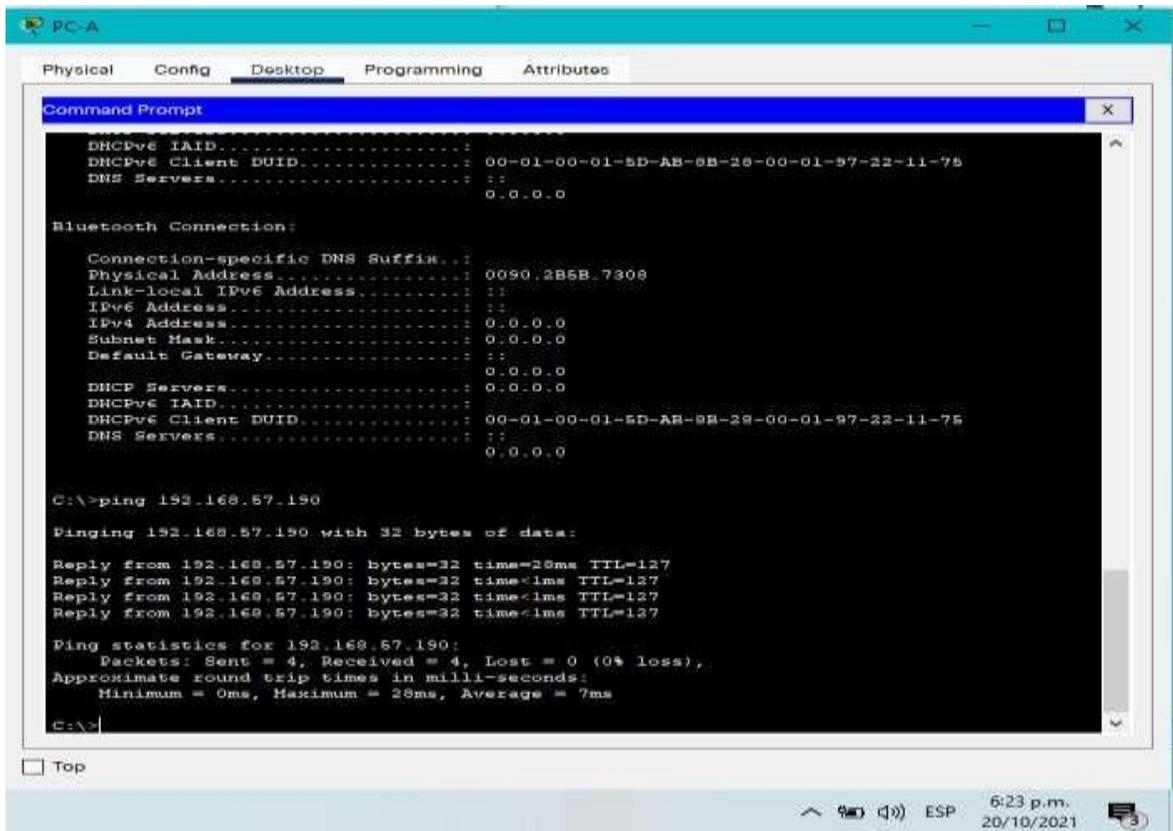
Figura 32: Ping PC-B



Fuente: Elaboración propia

Ping del PC-A al PC-B para probar la conectividad

Figura 33: Ping PC-A



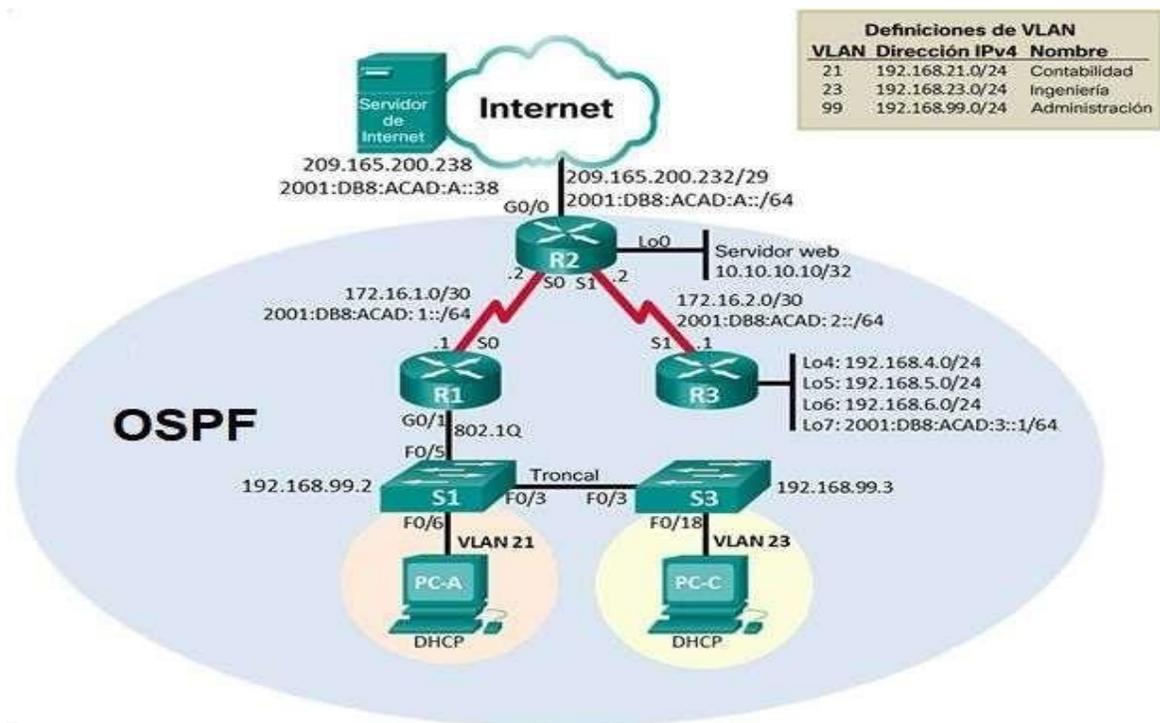
Fuente: Elaboración propia

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

Topología

Figura 34: Topología



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 9: Inicializar y volver a cargar los routers y los switches

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

Fuente: Prueba de Habilidades CCNA II-2021

Figura 35: R1 Eliminar el archivo startup-config y volver a cargarlos

```
RouterD>enable
RouterD#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
RouterD#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by Cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DRAM = 0 MB
CISC01341/RS platform with 524288 Bytes of main memory
Main memory is configured to 64/-1 (On-board/DRAM) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x00000000, size: 0x1b340
program load complete, entry point: 0x00000000, size: 0x1b340

IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x01000000, size: 0x2bb1c50
Self decompressing the image :
##### [OK]
Smart Init is enabled
Smart Init is taking 10mem
-----
TYPE          MEMORY_REQ      Onboard devices :
-----
HWIC Slot 0   0x00200000
buffer pools 0x01E0F000
-----
TOTAL:        0x03EEF000

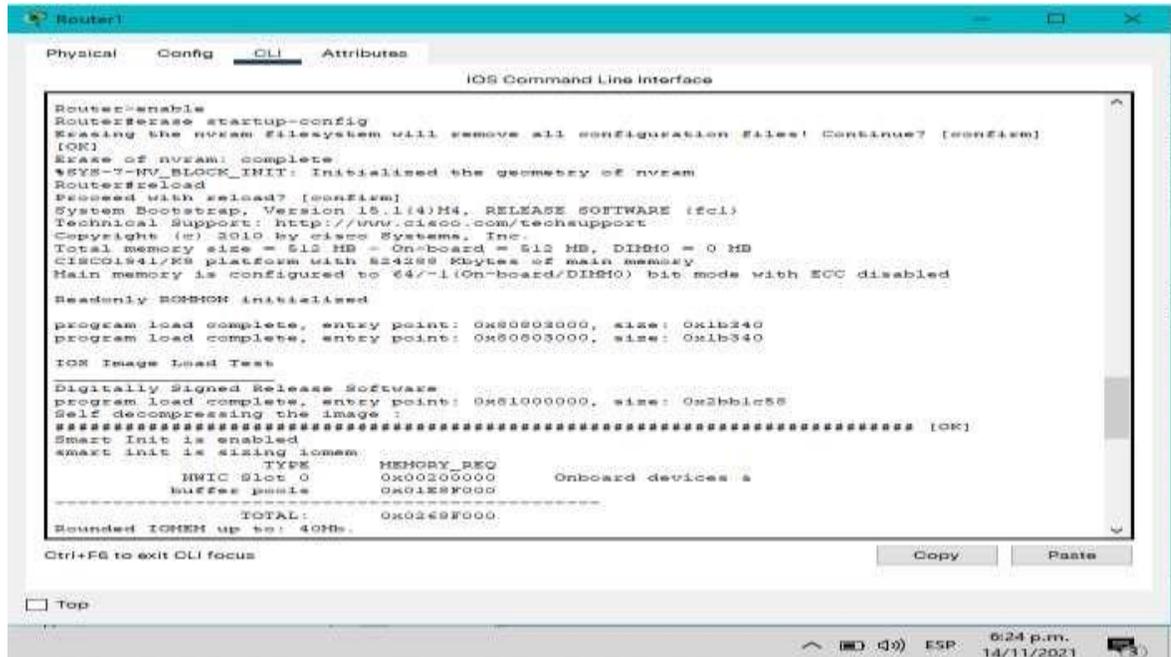
Rounded ROMEM up to: 4096.
Using a percent 10mem: {4096/512MB}

Restricted Rights Legend
Use, duplication, or disclosure by the Government is
prohibited.

Ctrl+F6 to exit CLI focus
```

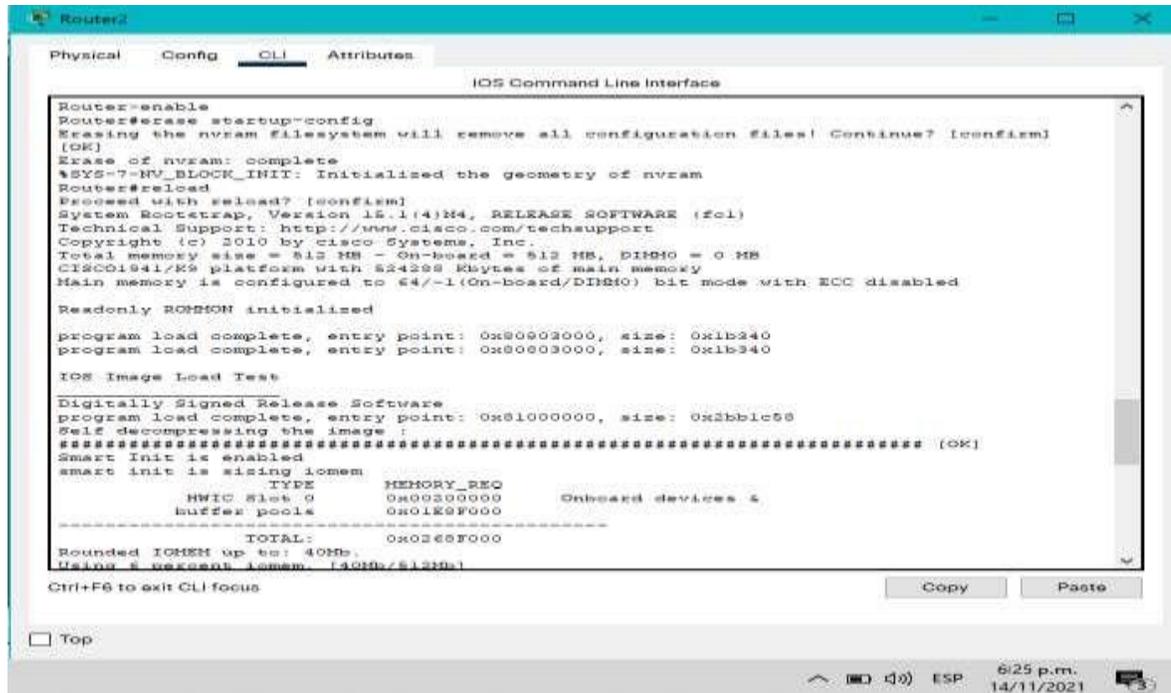
Fuente: Elaboración propia.

Figura 36: R2 Eliminar el archivo startup-config y volver a cargarlos



Fuente: Elaboración propia.

Figura 37: R3 Eliminar el archivo startup-config y volver a cargarlos



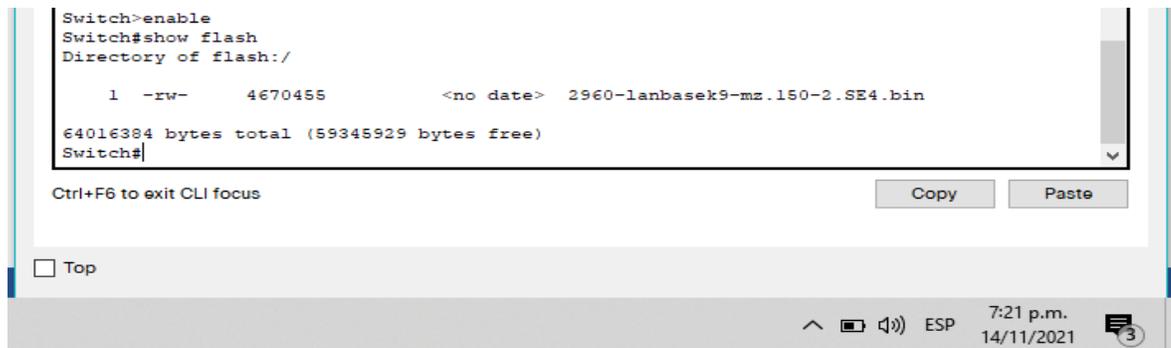
Fuente: Elaboración propia

Figura 38: S1 Eliminar el archivo startup-config y volver a cargarlos



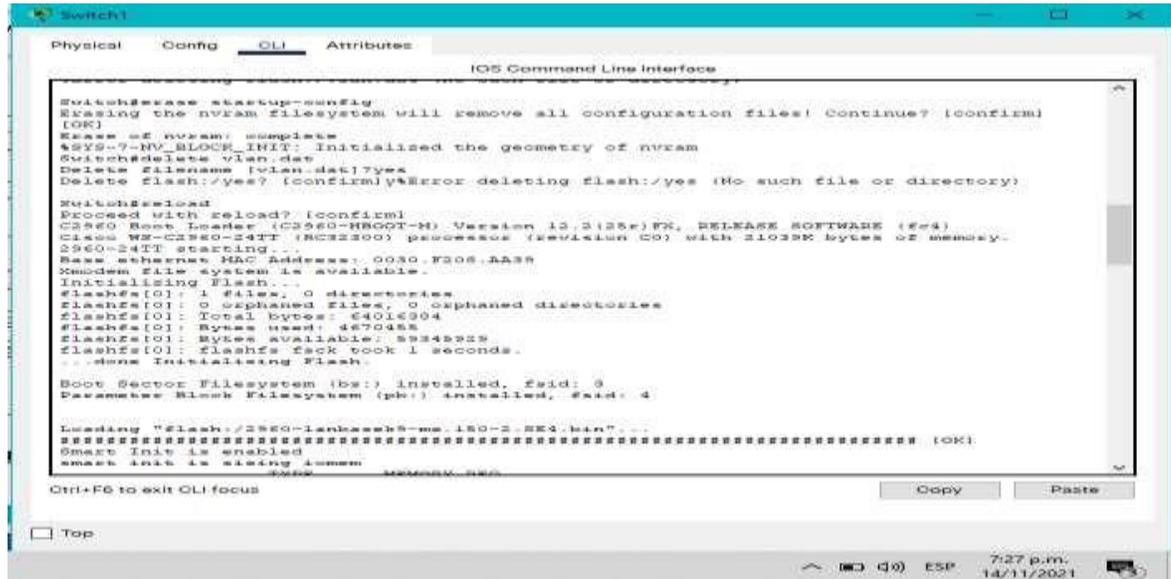
Fuente: Elaboración propia.

Figura 39: S1 Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches



Fuente: Elaboración propia.

Figura 40: S3 Eliminar el archivo startup-config y volver a cargarlos



Fuente: Elaboración propia.

Figura 41: S3 Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches



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):

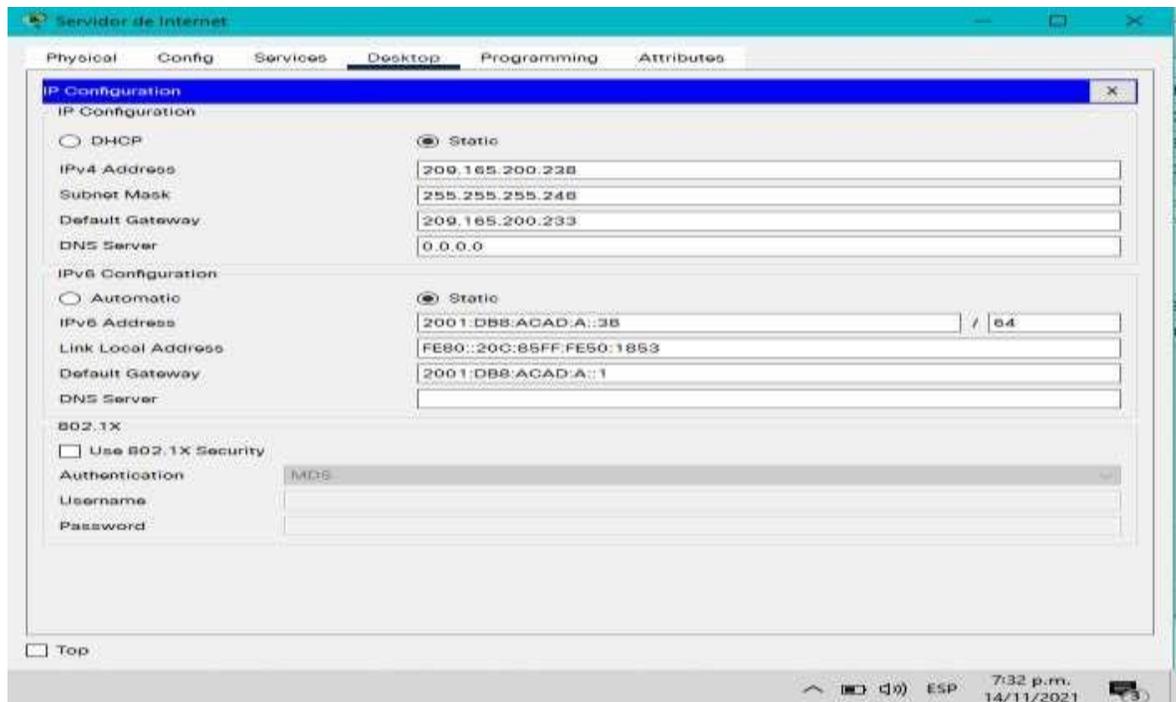
Tabla 10: Configurar la computadora de Internet

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:A::1

Fuente: Prueba de Habilidades CCNA II-2021

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

Figura 42: Configurar la computadora de Internet



Fuente: Elaboración propia.

TABLA 11: DE SUBNET IPV4

Elemento o tarea de configuración	Especificación
ID address:	209.165.200.232
Network Address:	209.165.200.232
Usable Host Ip Range:	209.165.200.233-209.165.200.238
Broadcast Address:	209.165.200.239
Total Number of Hosts:	8
Number of Usable:	6
Subnet mask:	255.255.255.248
Wildcard Mask:	0.0.0.7
Binary subnet Mask:	11111111.11111111.11111111.111110
Ip Type:	PUBLICIP-CLASS C

Fuente: Elaboración propia.

TABLA 12: DE SUBNET IPV6

Elemento o tarea de configuración	Especificación
ID address:	2001.db8:a cad:a::38/64
Full Ip Address:	2001:0db8:acad:000a:0000:0000:0000:0038
Total Ip Address:	18.446.744.073.709.551.616
Network	2001:0db8:acad:000a:: /64 2001:0db8:acad:000a:0000:0000:0000:0000/
Ip Range	2001:db8:acad:a::1 2001:0db8:acad:000a:0000:0000:0000:0001 2001:db8:acad:a:ffff:ffff:ffff:ffff 2001:0db8:acad:000a:ffff:ffff:ffff:ffff
Ip Type:	GLOBAL UNICAST

Fuente: Elaboración propia.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 13: Configurar R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#conf term Router(config)#no ip domain-lookup
Nombre del router	R1Router(config)#hostname R1 R1(config)#
Contraseña de exec privilegiado cifrada	Class R1(config)#enable secret class
Contraseña de acceso a la consola	Cisco R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#
Contraseña de acceso Telnet	Cisco R1(config-Line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. R1(config)#banner motd 'Prohibido 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 R1(config)# interface 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

	R1(config-if)#exit
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0 R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)# ipv6 route ::/0 s0/0/0

Fuente: Elaboración propia.

Nota: Todavía no configure G0/1.

Figura 43: Configuración R1

```

R1
Physical  Config  CLI  Attributes
IOS Command Line Interface

Press RETURN to get started!

Router>enable
Router#conf term
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)#exit
R1(config)#service password-encryption
R1(config)#banner motd 'prohibido el acceso no autorizado'
R1(config)#interface s0/0/0
R1(config-if)#description Conexion 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)#
  
```

Fuente: Elaboración propia.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 14: Configuración R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#conf term Router(config)#no ip domain-lookup
Nombre del router	R2 Router(config)#hostname R2 R2(config)#
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)#
Contraseña de acceso Telnet	Cisco R2(config-Line)#line vty 0 15 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	R2(config)#ip http server
Mensaje MOTD	Se prohíbe el acceso no autorizado. R2(config)#banner motd 'Prohibido 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)# interface 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)# clock rate 128000 R2(config-if)#no shutdown

<p>Interfaz S0/0/1</p>	<p>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-if)# interface 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</p>
<p>Interfaz G0/0 (simulación de Internet)</p>	<p>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-if)# interface 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</p>
<p>Interfaz loopback 0 (servidor web simulado)</p>	<p>Establecer la descripción. Establezca la dirección IPv4. R2(config-if)# interface loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description Simulated Web Server R2(config-if)#exit</p>
<p>Ruta predeterminada</p>	<p>Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0. R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)# ipv6 route ::/0 g0/0</p>

Fuente: Prueba de Habilidades CCNA II-2021

Figura 44: Configuración R2

```
Router>enable
Router#conf term
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)#exit
R2(config)#service password-encryption
R2(config)#ip http server

% Invalid input detected at '^' marker.

R2(config)#banner motd 'Prohibido el acceso no autorizado'
R2(config)#interface 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)#clock rate 120000
R2(config-if)#no shutdown

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R2(config-if)#interface 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
```

Fuente: Elaboración propia.

Figura 45: Configuración R2

```
R2(config-if)#interface 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 120000
This command applies only to DCE interfaces
R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down

R2(config-if)#interface g0/0
R2(config-if)#description Connection to Internet
R2(config-if)#ip address 209.166.200.233 255.255.255.240
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)#interface 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)#
```

Fuente: Elaboración propia.

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 15: Configuración R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#conf term Router(config)#no ip domain-lookup
Nombre del router	R3 Router(config)#hostname R3(config)#
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)#
Contraseña de acceso Telnet	Cisco R3(config-line)#line vty 0 15 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 'Prohibido 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)# int s0/0/1 R3(config-if)#description Connection to R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252

	<pre>R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#no shutdown R3(config-if)#</pre>
Interfaz loopback 4	<p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <pre>R3(config-if)# int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#exit</pre>
Interfaz loopback 5	<p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <pre>R3(config)# int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#exit</pre>
Interfaz loopback 6	<p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <pre>R3(config-if)# int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#exit</pre>
Interfaz loopback 7	<p>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.</p> <pre>R3(config-if)# int loopback 7 R3(config-if)# ipv6 address 2001:db8:acad:3::1/64 R3(config-if)#exit</pre>
Rutas predeterminadas	<pre>R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)# ipv6 route ::/0 s0/0/1</pre>

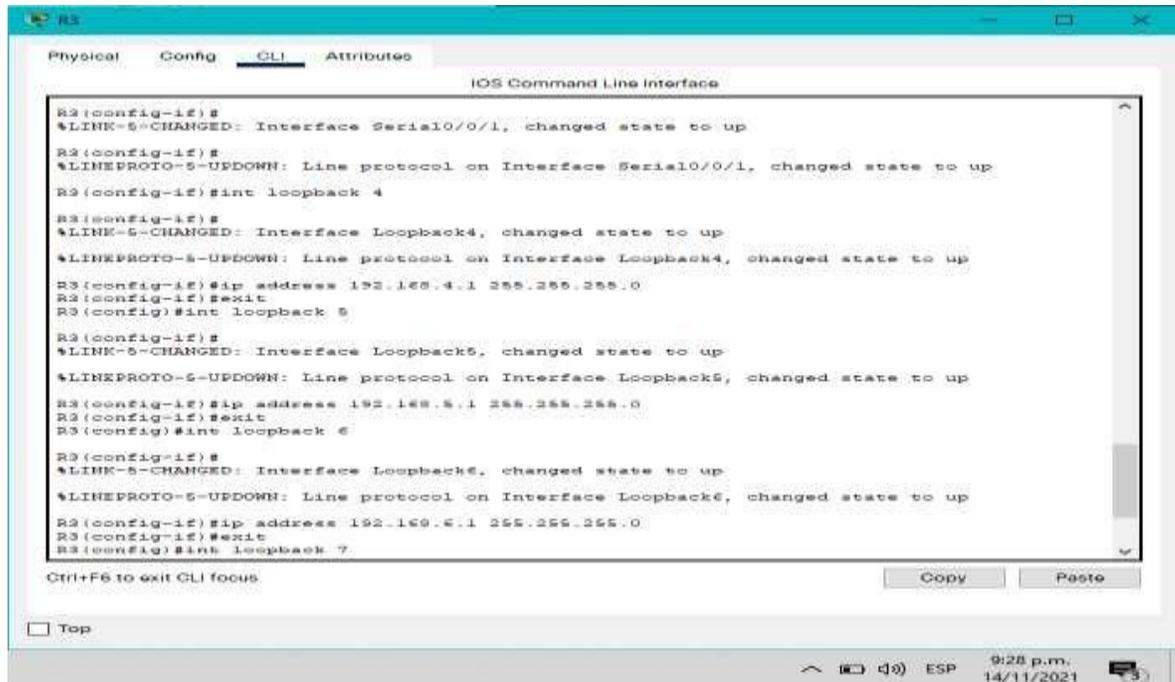
Fuente: Prueba de Habilidades CCNA II-2021

Figura 46: Configuración R3



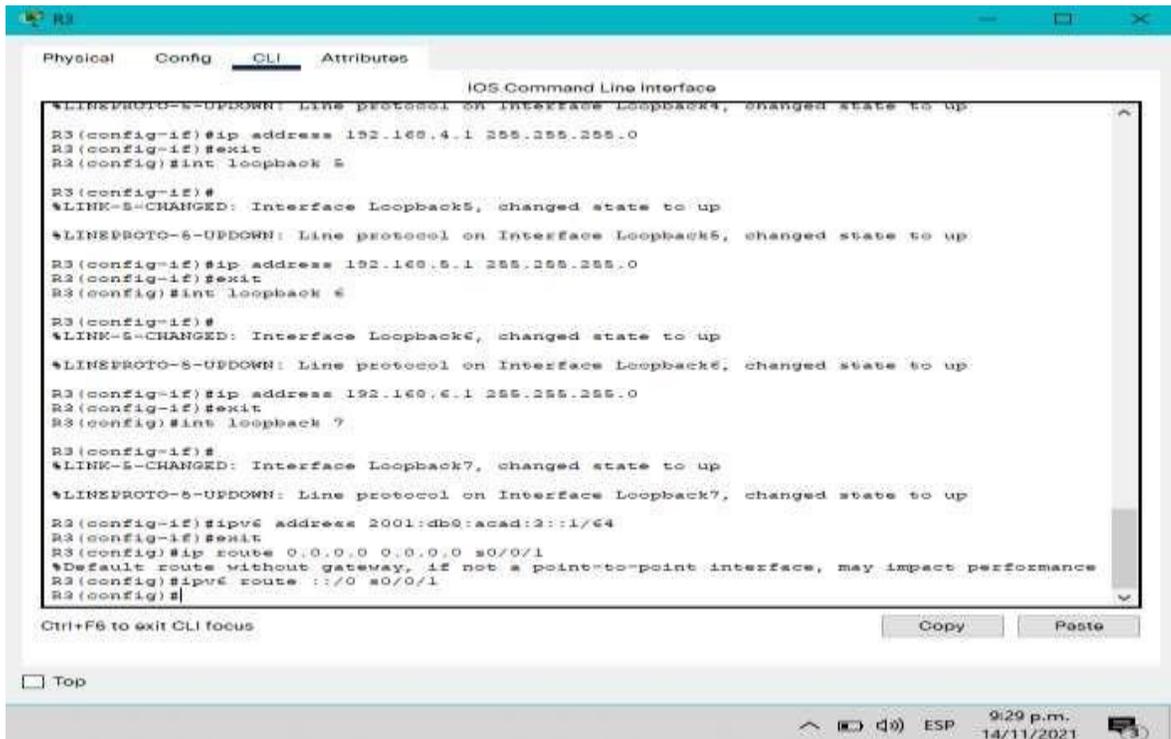
Fuente: Elaboración propia.

Figura 47: Configuración R3



Fuente: Elaboración propia.

Figura 48: Configuración R3



```
Physical  Config  CLI  Attributes
IOS Command Line Interface
%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)#exit
R3(config)#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)#exit
R3(config)#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)#exit
R3(config)#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:db0:acad:2::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)#
Ctrl+F8 to exit CLI focus
Copy Paste
Top
9:29 p.m.
14/11/2021
```

Fuente: Elaboración propia.

Paso 5: Configurar S1

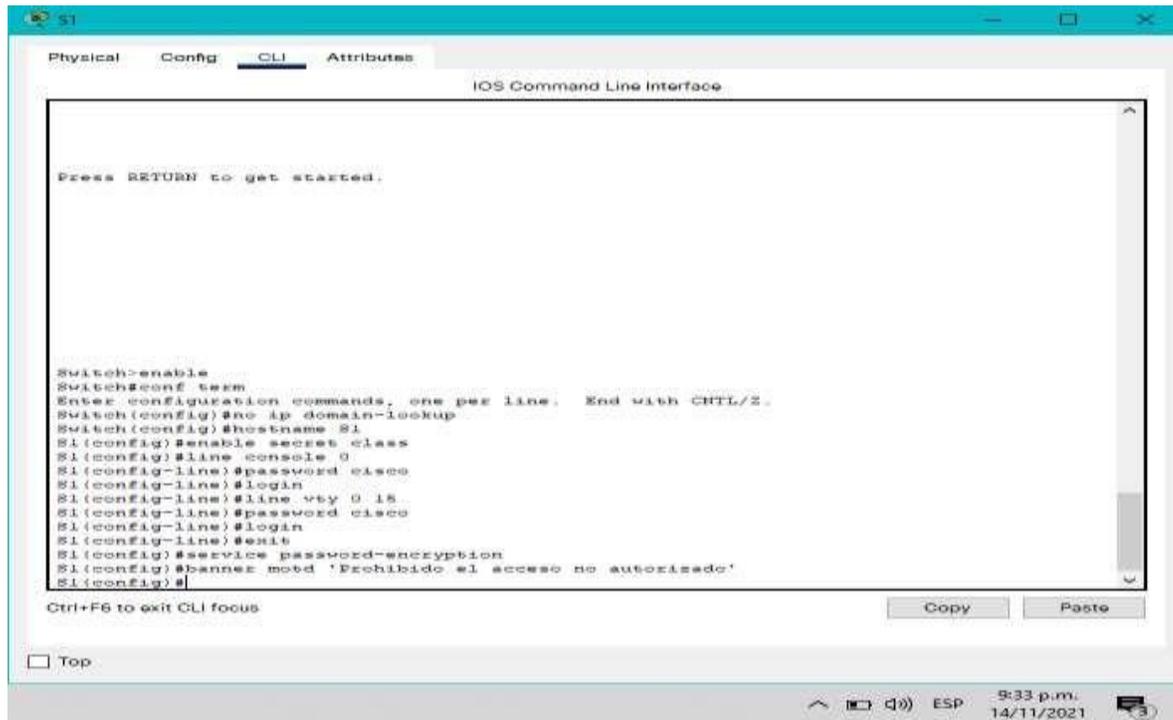
La configuración del S1 incluye las siguientes tareas:

Tabla 16: Configuración S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#conf term Switch(config)#no ip domain-lookup
Nombre del switch	S1 Switch(config)#hostname S1 S1(config)#
Contraseña de exec privilegiado cifrada	Class S1(config)#enable secret class
Contraseña de acceso a la consola	Cisco S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#
Contraseña de acceso Telnet	Cisco S1(config-line)#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	Se prohíbe el acceso no autorizado. S1(config)#banner motd 'Prohibido el acceso no autorizado' S1(config)#

Fuente: Prueba de Habilidades CCNA II-2021

Figura 49: Configuración S1



Fuente: Elaboración propia.

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 17: Configuración S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#conf term 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)#
Contraseña de acceso Telnet	Cisco S3(config-line)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. S3(config)#banner motd 'Prohibido el acceso no autorizado'

Fuente: Prueba de Habilidades CCNA II-2021

Figura 50: Configuración S3

```

Switch#enable
Switch#conf term
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)#exit
S3(config)#service password-encryption
S3(config)#banner motd 'Prohibido el acceso no autorizado'
S3(config)#

```

Fuente: Elaboración propia.

Paso 7: Verificar la conectividad de la red

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

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

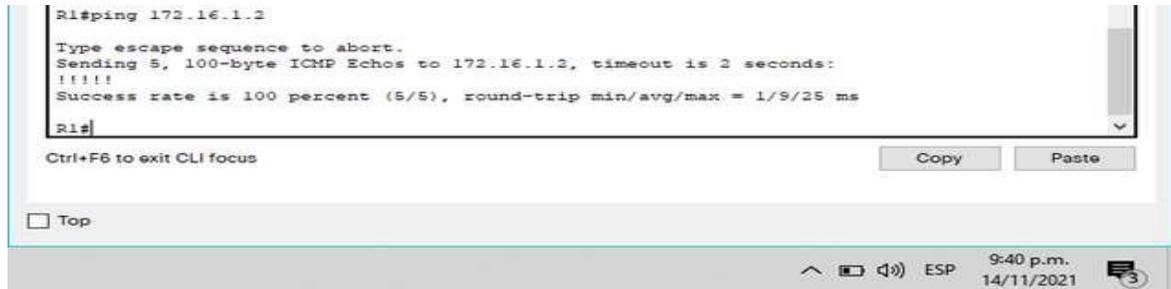
Tabla 18: Verificar la conectividad de la red

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 = 1/1/2 ms
R2	R3, S0/0/1	172.16.2.1	R2#ping 172.16.2.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/7 ms
PC de Internet	Gateway predeterminado	209.165.200.233	

Fuente: Prueba de Habilidades CCNA II-2021

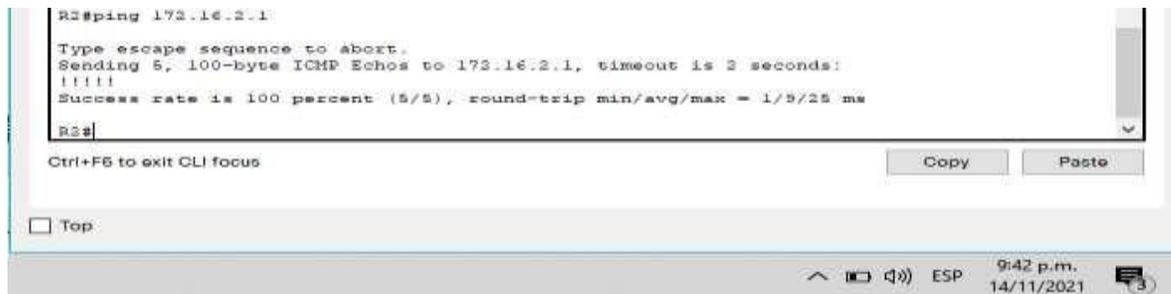
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Figura 51: Ping de R1 a R2



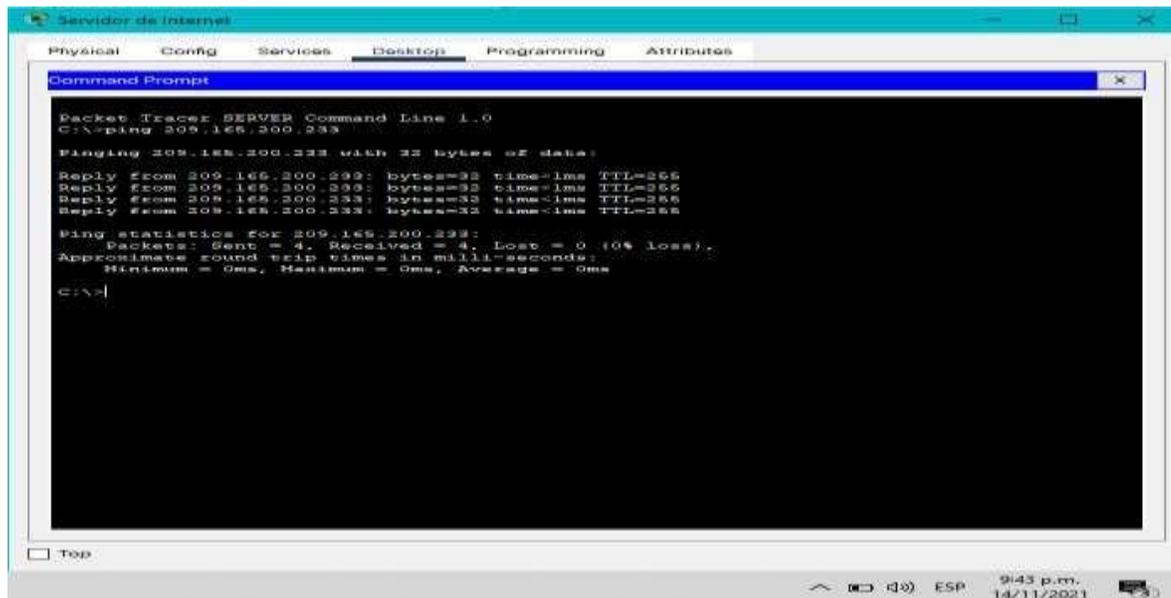
Fuente: Elaboración propia

Figura 52: Ping de R2 a R3



Fuente: Elaboración propia.

Figura 53: Ping de Pc de Internet a Gateway predeterminado



Fuente: Elaboración propia.

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 19: Configurar S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican S1>enable S1#conf term 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)#
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología S1(config)#int 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	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. S1(config)#ip default-gateway 192.168.99.1 S1(config)#
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk

	S1(config-if)#switchport trunk native vlan 1 S1(config-if)#
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range 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)#
Asignar F0/6 a la VLAN 21	S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21 S1(config-if)#
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 S1(config-if-range)#

Fuente: Prueba de Habilidades CCNA II-2021

Figura 54: Configuración S1

```

S1>enable
Password:
S1#conf term
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)#int 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

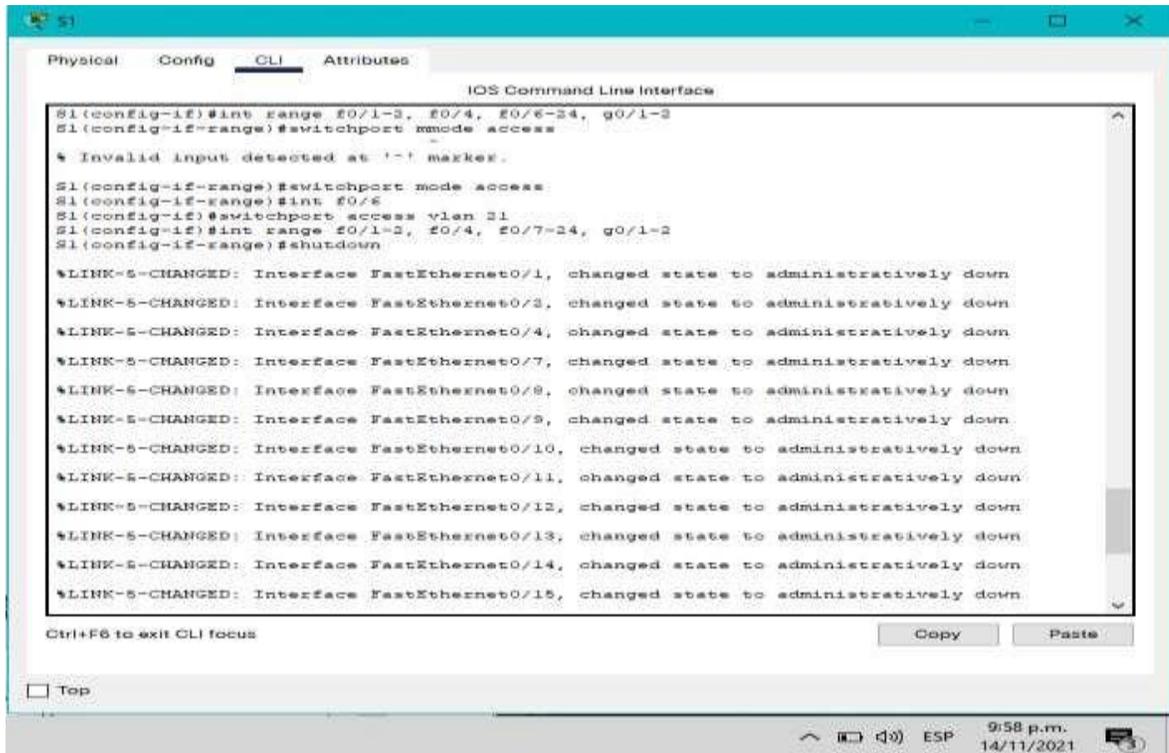
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

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

```

Fuente: Elaboración propia.

Figura 55: Configuración S1



The screenshot shows a network switch configuration window titled "S1". The window has tabs for "Physical", "Config", "CLI", and "Attributes", with "CLI" selected. The main area is titled "IOS Command Line Interface" and displays the following text:

```
S1(config-if)#int range f0/1-3, f0/4, f0/6-24, g0/1-2
S1(config-if-range)#switchport mode access

% Invalid input detected at '!-' marker.

S1(config-if-range)#switchport mode access
S1(config-if-range)#int f0/8
S1(config-if)#switchport access vlan 31
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 FastEthernet0/3, 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
```

Below the text, there are "Copy" and "Paste" buttons. At the bottom left, there is a "Top" button. At the bottom right, there is a system tray showing "ESP", "9:58 p.m.", and "14/11/2021".

Fuente: Elaboración propia.

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 20: Configuración S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombrea cada VLAN. S3>enable S3#conf term 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)#
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 detopología S3(config)#int 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 gatewaypredeterminado. S3(config)#ip default-gateway 192.168.99.1 S3(config)#
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range 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 S3(config-if)#

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

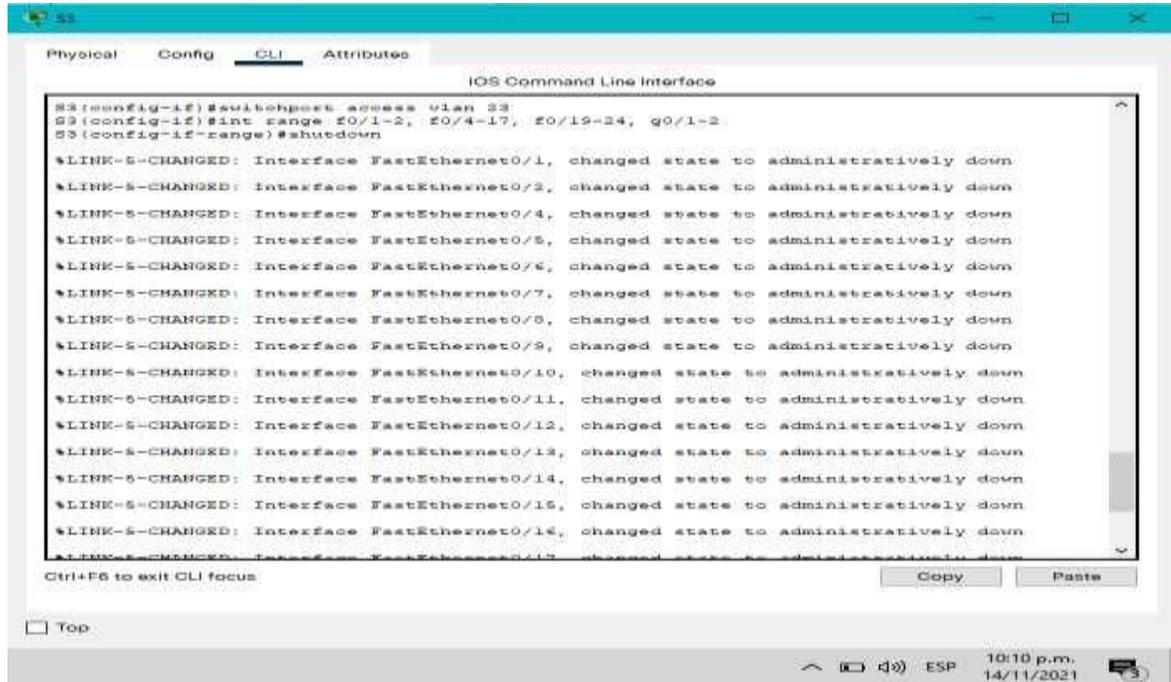
Fuente: Prueba de Habilidades CCNA II-2021

Figura 56: Configuración S3



Fuente: Elaboración propia.

Figura 57: Configuración S3



Fuente: Elaboración propia.

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 21: Configuración R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz R1>enable R1#conf term 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)#

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-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)#
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-subif)#int g0/1.99 R1(config-subif)#description LAN de Administracion R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#
Activar la interfaz G0/1	R1(config-if)#int g0/1 R1(config-if)#no shutdown

Fuente: Prueba de Habilidades CCNA II-2021

Figura 58: Configuración R1

```

R1#
R1#config term
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 Administracion
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-S-CHANGED: Interface GigabitEthernet0/1, changed state to up
*LINEPROTO-S-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
*LINK-S-CHANGED: Interface GigabitEthernet0/1.21, changed state to up
*LINEPROTO-S-UPDOWN: Line protocol on Interface GigabitEthernet0/1.21, changed state to up
*LINK-S-CHANGED: Interface GigabitEthernet0/1.23, changed state to up
*LINEPROTO-S-UPDOWN: Line protocol on Interface GigabitEthernet0/1.23, changed state to up
*LINK-S-CHANGED: Interface GigabitEthernet0/1.99, changed state to up

```

Fuente: Elaboración propia.

Paso 4: Verificar la conectividad de la red

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

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

Tabla 22: 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 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 99	192.168.99.1	S3# 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 80 percent (4/5), round-trip min/avg/max = 0/0/3 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 = 0/0/1 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 = 0/1/6 ms

Fuente: Prueba de Habilidades CCNA II-2021

Figura 59: Ping de S1 a R1

```

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 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
S1#

```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

ESP 10:32 p.m. 14/11/2021

Fuente: Elaboración propia.

Figura 60: Ping de S3 a R1

```

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 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
S3#

```

Ctrl+F6 to exit CLI focus

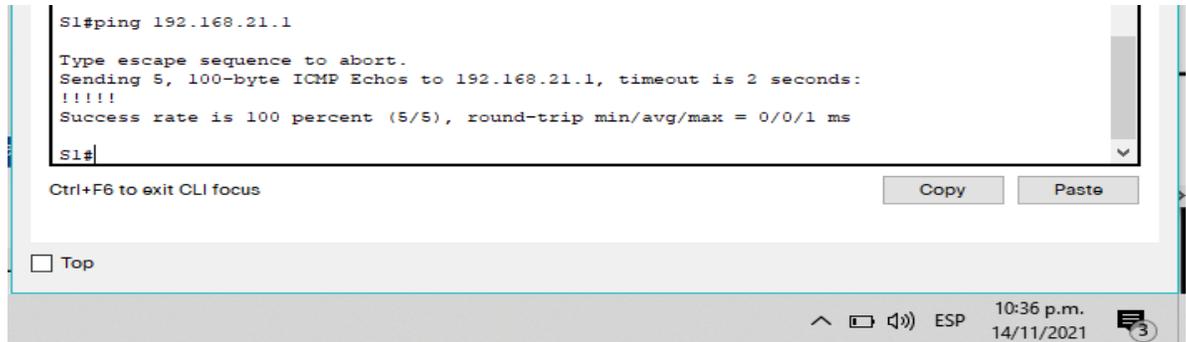
Copy Paste

Top

ESP 10:34 p.m. 14/11/2021

Fuente: Elaboración propia.

Figura 61: Ping de S1 a R1



```
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#
```

Ctrl+F6 to exit CLI focus

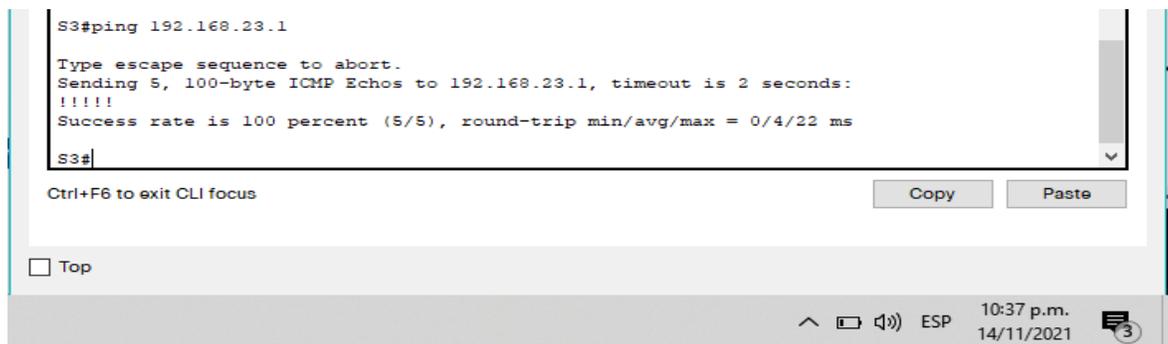
Copy Paste

Top

ESP 10:36 p.m. 14/11/2021

Fuente: Elaboración propia.

Figura 62: Ping de S3 a R1



```
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 = 0/4/22 ms
S3#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

ESP 10:37 p.m. 14/11/2021

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 23: Configurar OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1>enable R1#conf term R1(config)#router ospf 1 R1(config-router)#

<p>Anunciar las redes conectadas directamente</p>	<p>Asigne todas las redes conectadas directamente. R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0 R1(config-router)#</p>
<p>Establecer todas las interfaces LAN como pasivas</p>	<p>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)#exit</p>
<p>Desactive la sumarización automática</p>	<p>R1(config)#router rip R1(config-router)#no auto-summary R1(config-router)#exit</p>

Fuente: Prueba de Habilidades CCNA II-2021

Figura 63: Configurar OSPF en el R1



Fuente: Elaboración propia.

Paso 3: Configurar OSPFv3 en el R3

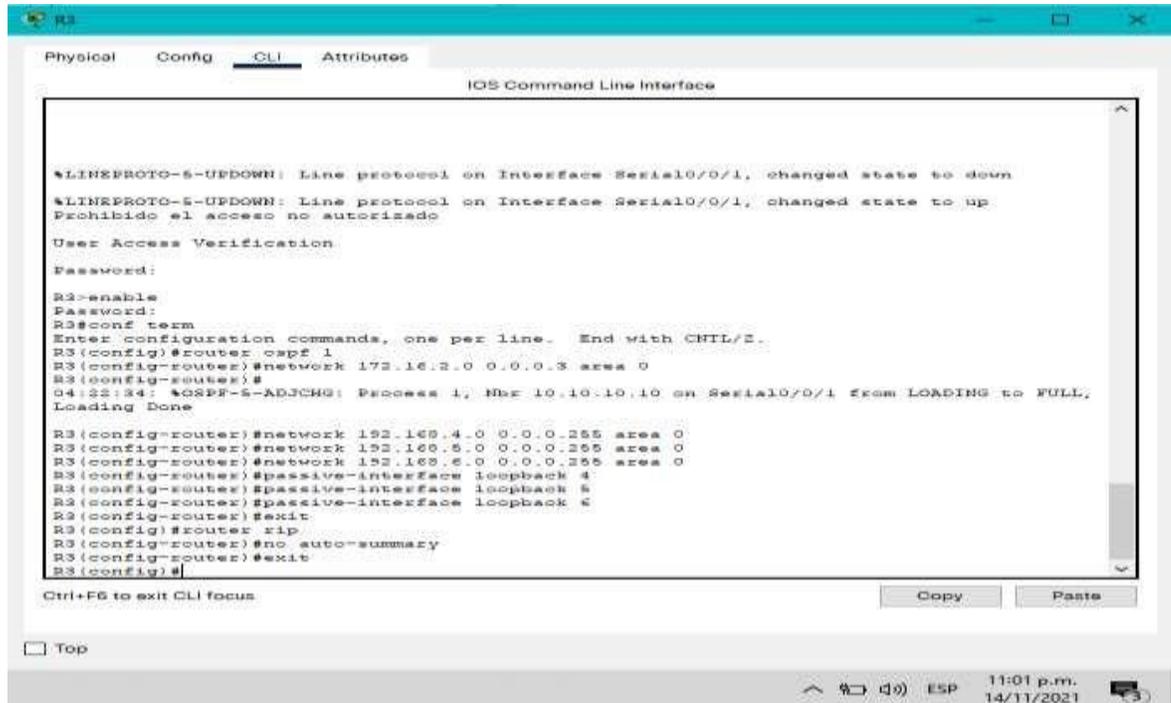
La configuración del R3 incluye las siguientes tareas:

Tabla 24: Configurar OSPFv3 en el R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3>enable R3#conf term R3(config)#router ospf 1 R3(config-router)#
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 R3(config-router)#
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)#exit
Desactive la sumarización automática.	R3(config)#router rip R3(config-router)#no auto-summary R3(config-router)#exit

Fuente: Prueba de Habilidades CCNA II-2021

Figura 65: Configurar OSPFv3 en el R3



Fuente: Elaboración propia.

Paso 4: Verificar la información de OSPF

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

Tabla 25: 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 running-config show run begin ospf

Fuente: Prueba de Habilidades CCNA II-2021

Parte 5: Implementar DHCP y NAT para IPv4

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

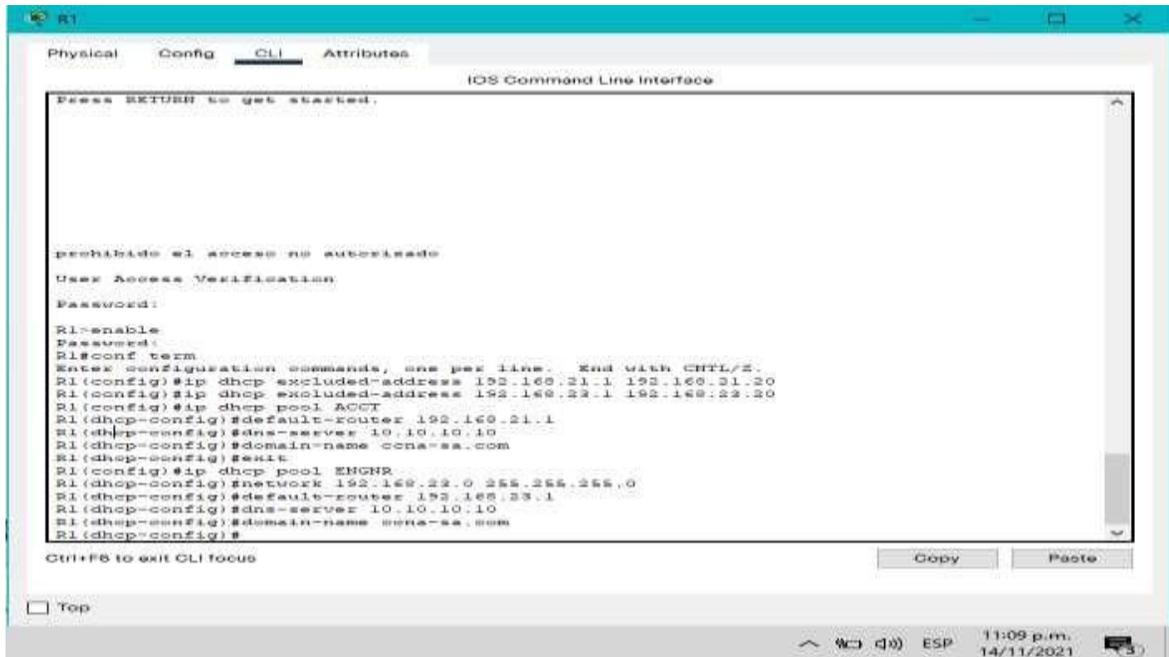
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 26: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

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

Fuente: Prueba de Habilidades CCNA II-2021

Figura 66: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23



```

R1
-----
Physical  Config  CLI  Attributes
IOS Command Line Interface

Press RETURN to get started.

prohibido el acceso no autorizado
User Access Verification
Password:
R1-enable
Password:
R1#conf term
Enter configuration commands, one per line. End with CTRL/Z.
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)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#exit
R1(config)#ip dhcp pool ENCHR
R1(dhcp-config)#network 192.168.22.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#
Ctrl+F8 to exit CLI focus
Copy Paste
 Top
ESP 11:09 p.m. 14/11/2021

```

Fuente: Elaboración propia.

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

La configuración del R2 incluye las siguientes tareas:

Tabla 27: Configurar la NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15 R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)# ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)# ip http authentication local
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.229 R2(config)#ip nat inside source static 10.10.10.10 209.165.200.238
Asignar la interfaz interna y externa para la NAT estática	R2(config)#int g0/0 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R1(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)#
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 209.165.200.232 209.165.200.237 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Fuente: Prueba de Habilidades CCNA II-2021

Figura 67: Configurar la NAT estática y dinámica en el R2

```

R2
Physical Config CLI Attributes
IOS Command Line Interface

Prohibido el acceso no autorizado
User Access Verification
Password:
R2>enable
Password:
R2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#user webuser privilege 15 secret cisco12345
R2(config)#ip http server
^
* Invalid input detected at '^' marker.

R2(config)#ip http authentication local
* Ambiguous command: "ip http authentication local"
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.238
R2(config)#int g0/0
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)#

```

Fuente: Elaboración propia.

Paso 3: Verificar el protocolo DHCP y la NAT estática

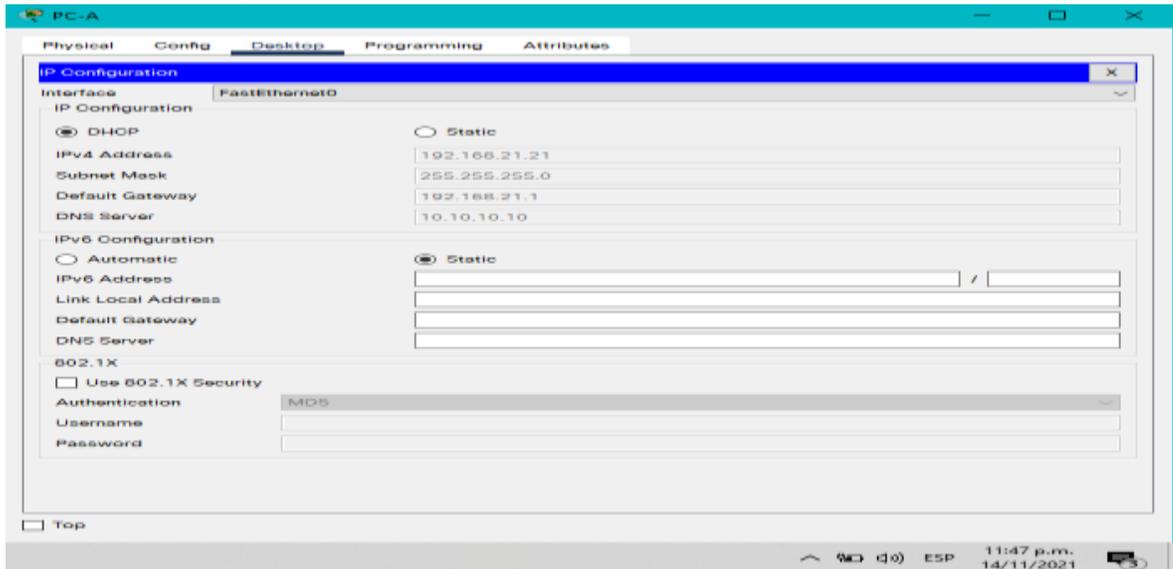
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 28: Verificar el protocolo DHCP y la NAT estática

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

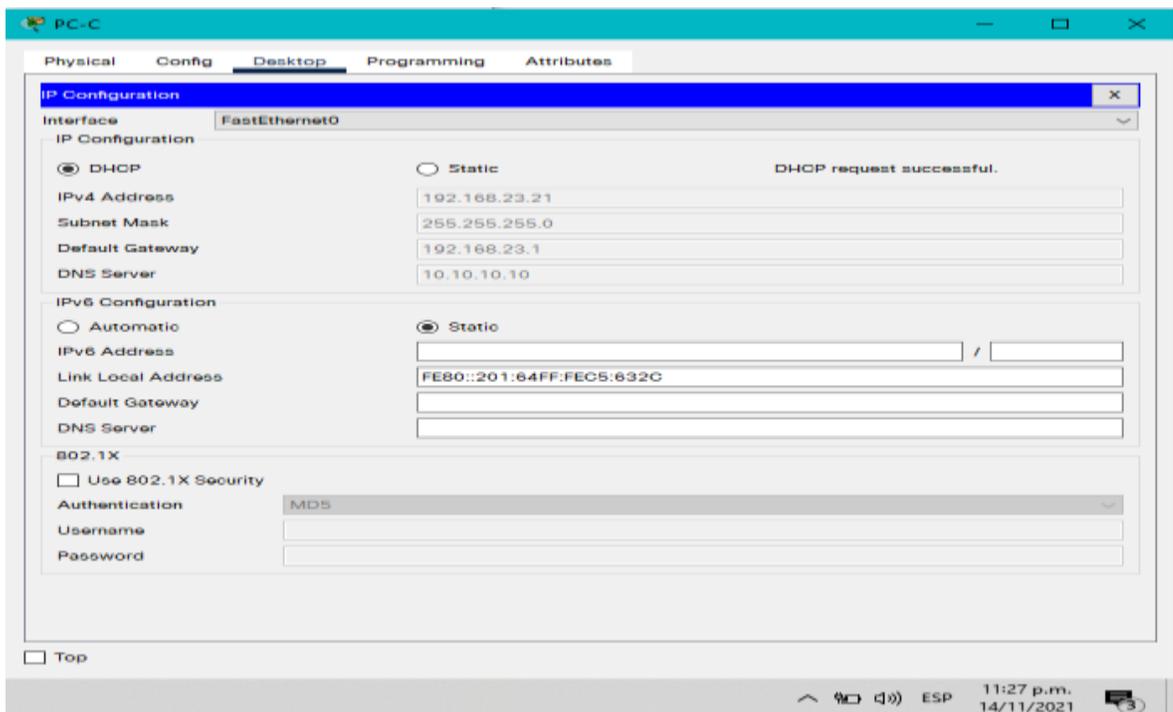
Fuente: Prueba de Habilidades CCNA II-2021

Figura 68: Verificar que la PC-A haya adquirido información de IP del servidor de DHCP



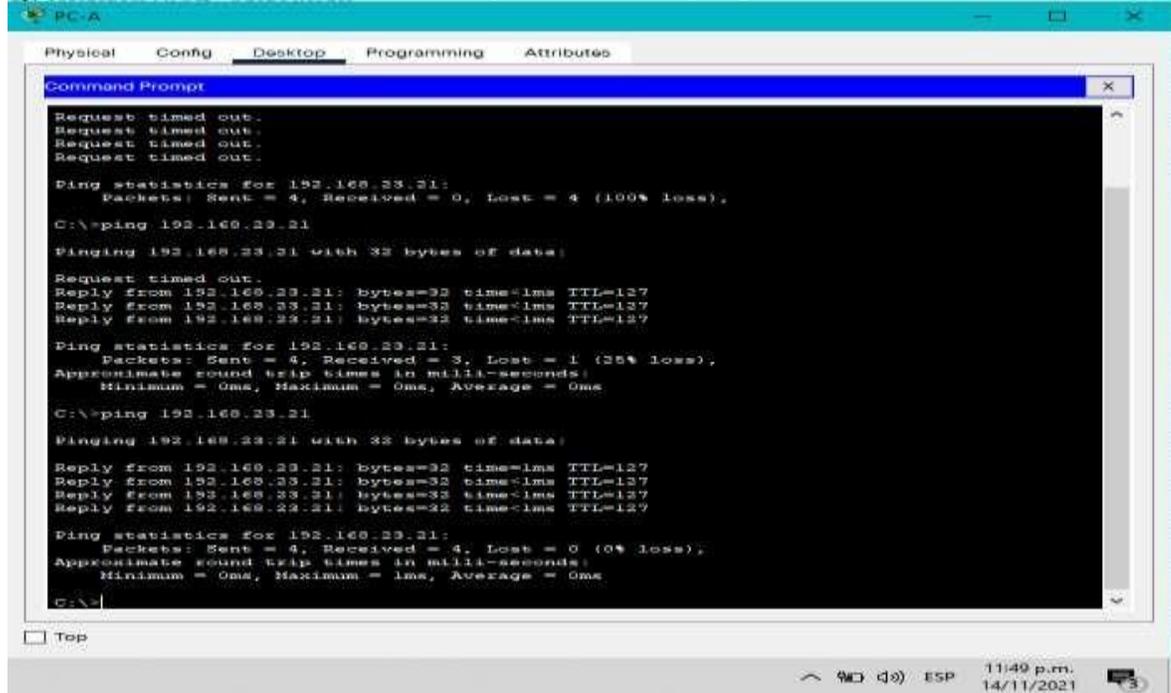
Fuente: Elaboración propia.

Figura 69: Verificar que la PC-C haya adquirido información de IP del servidor de DHCP



Fuente: Elaboración propia.

Figura 70: Verificar que la PC-A pueda hacer ping ala PC-C



Fuente: Elaboración propia.

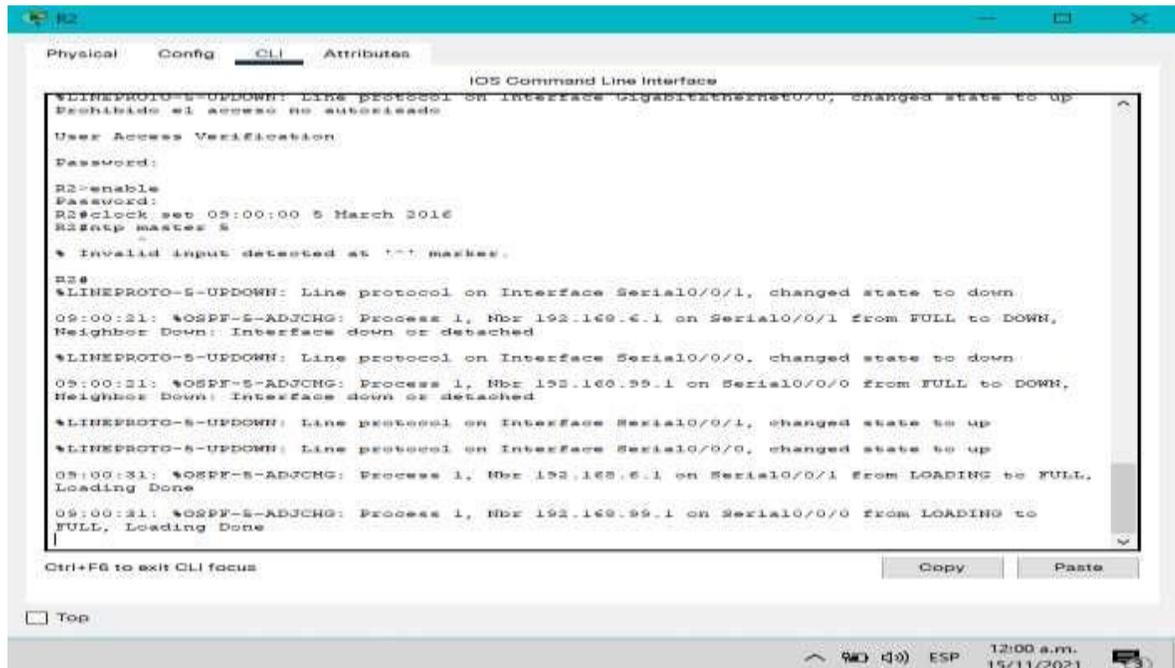
Parte 6: Configurar NTP

Tabla 29: Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	5 de marzo de 2016, 9 a. m. R2#clock set 09:00:00 5 March 2016
Configure R2 como un maestro NTP.	Nivel de estrato: 5 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 horaNTP.	R1(config)# ntp update-calendar
Verifique la configuración de NTP en R1.	R1# show ntp associations

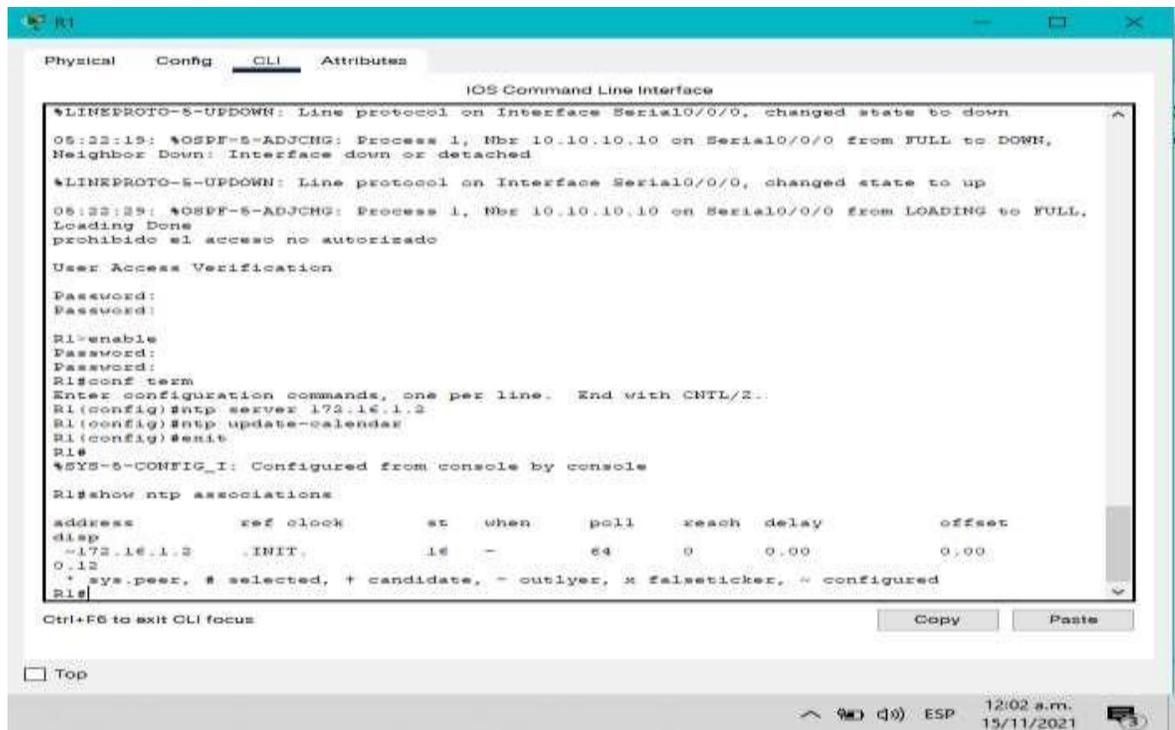
Fuente: Prueba de Habilidades CCNA II-2021

Figura 71: Ajuste la fecha y hora en R2.



Fuente: Elaboración propia

Figura 72: Configure R2 como un maestro NTP



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 30: 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	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)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 Trying 172.16.1.2 OpenSe prohíbe el acceso no Elaboración propiaizado.

Fuente: Prueba de Habilidades CCNA II-2021

Figura 73: Restringir el acceso a las líneas VTY en el R2

```

IOS Command Line Interface

Press RETURN to get started.

Prohibido el acceso no autorizado
User Access Verification
Password:
R2#enable
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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)#

Ctrl+F6 to exit CLI focus.
    
```

Fuente: Elaboración propia

Figura 74: Verificar que la ACL funcione como se espera



Fuente: Elaboración propia

Figura 75: Verificar conexión



Fuente: Elaboración propia

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

Tabla 31: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-lists
Restablecer los contadores de una lista de acceso	clear ip access-list counters R2#clear ip access-list counters R2#clear ip
¿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?	Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red. R2# show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#show ip nat translations

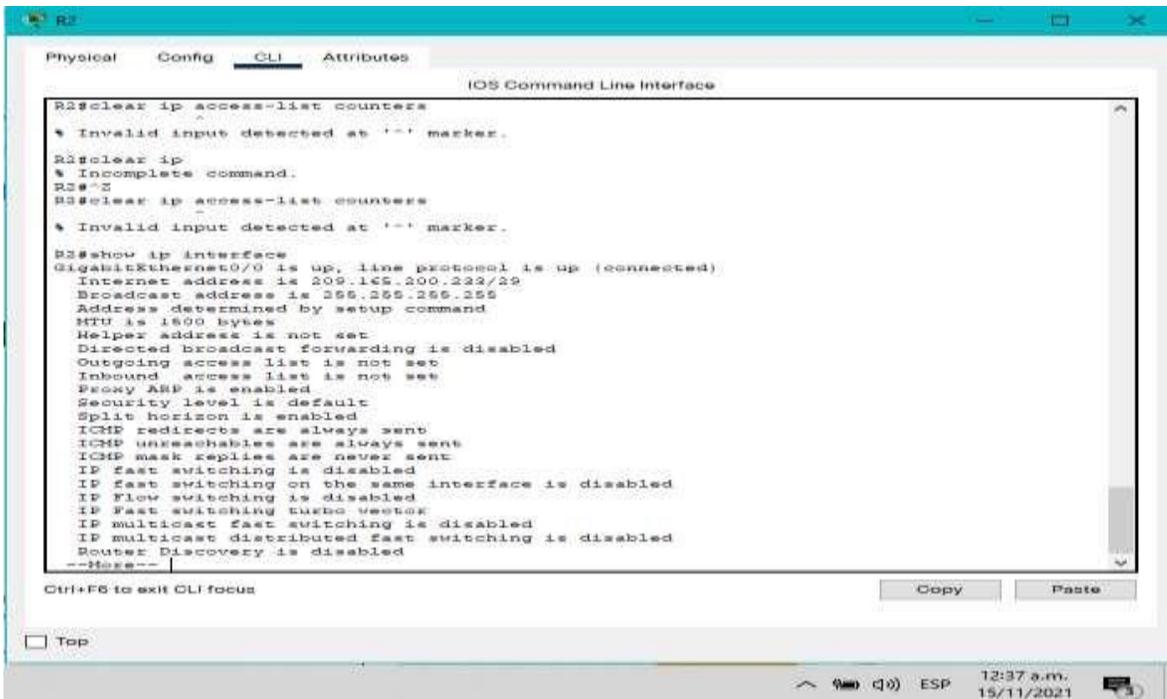
Fuente: Prueba de Habilidades CCNA II-2021

Figura 76: Mostrar las coincidencias recibidas



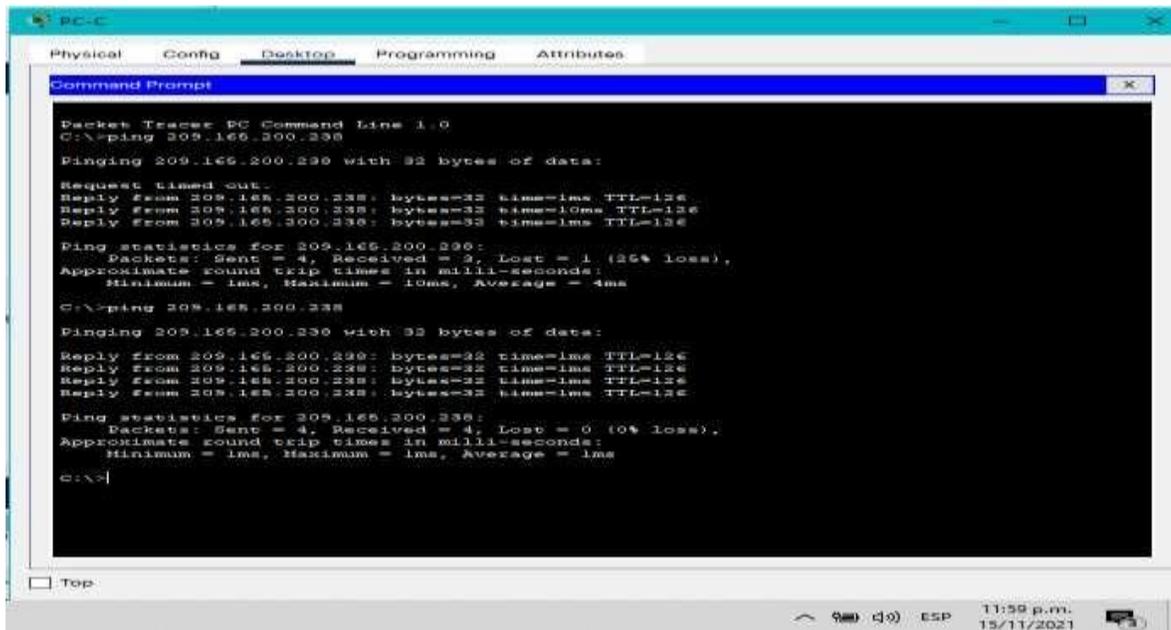
Fuente: Elaboración propia

Figura 77: Restablecer los contadores de una listade acceso



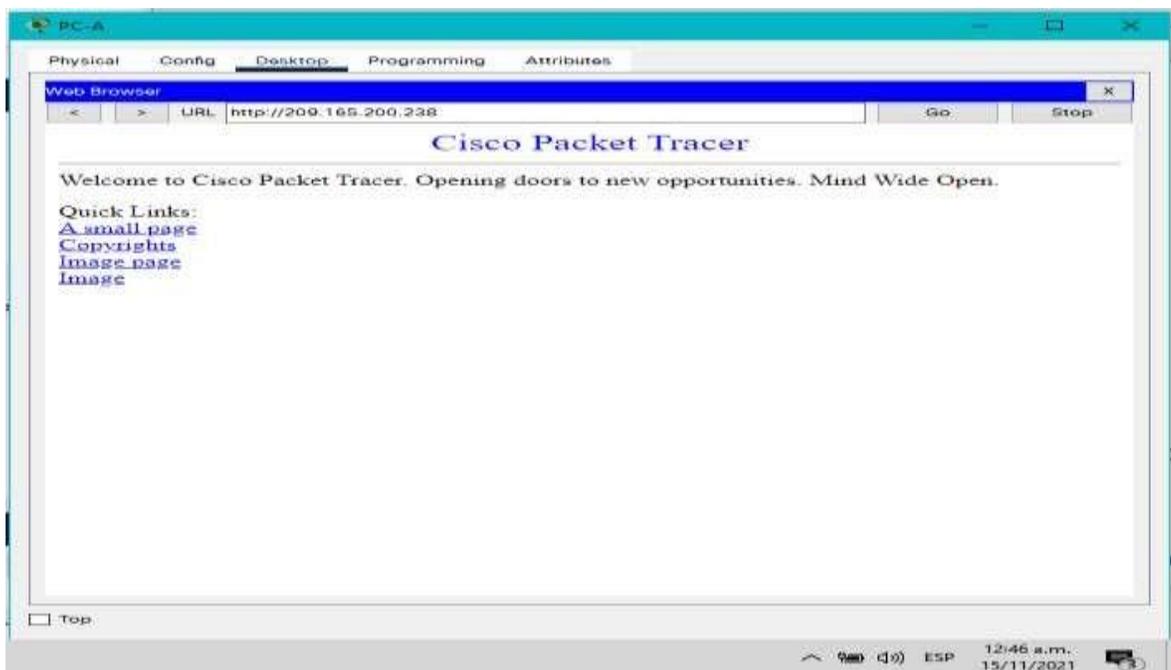
Fuente: Elaboración propia

Figura 80: Prueba de ping al Servidor de Internet desde la PC-C.



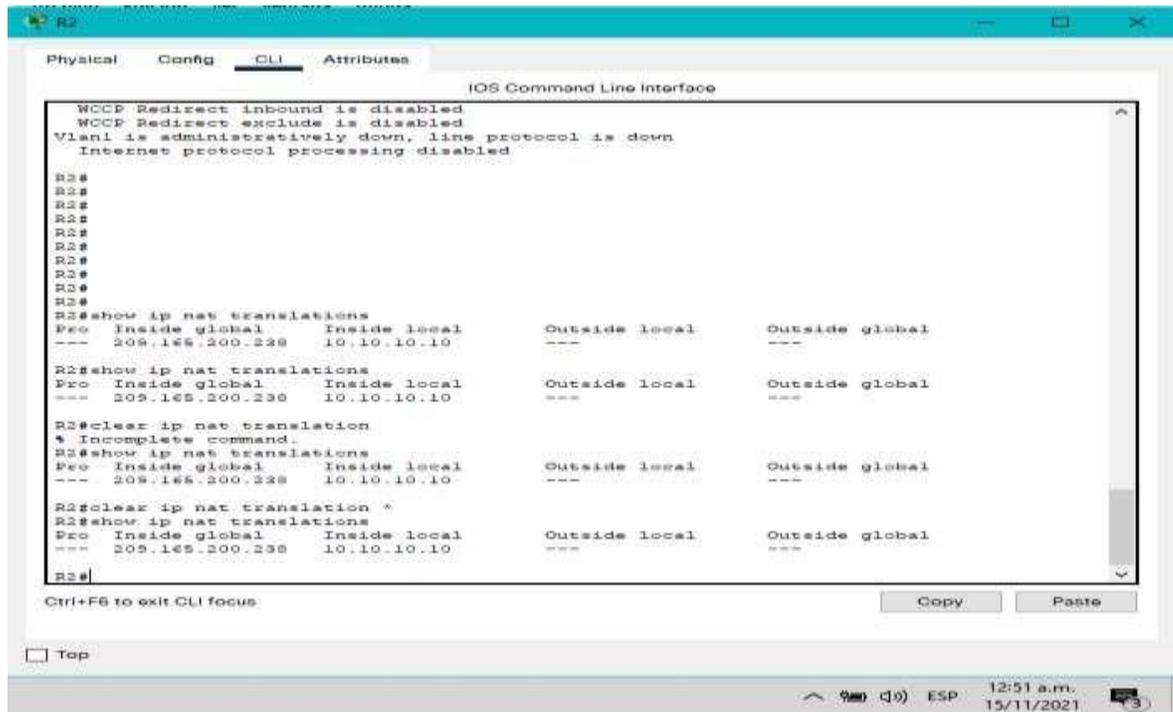
Fuente: Elaboración propia

Figura 81: Prueba de acceso al Servidor de Web desde PC-A.



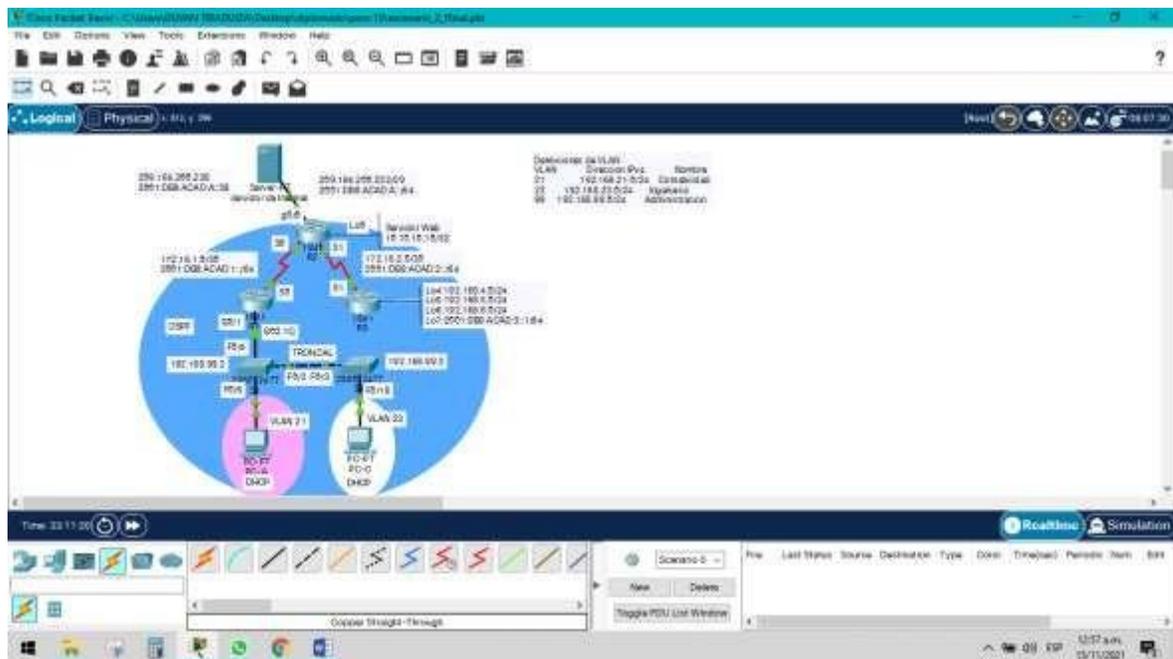
Fuente: Elaboración propia

Figura 82: Eliminar las traducciones de NAT dinámicas



Fuente: Elaboración propia

Figura 83: Topología de red escenario 2 - Cisco Packet Tracer.



Fuente: Elaboración propia

CONCLUSIONES

Por medio de este diplomado conocí y configure cada uno de los dispositivos de Packet Tracer, interactúe con los diferentes tipos de conexión, puertos, se hicieron pruebas de conectividad, se hicieron simulaciones en este mismo y en el laboratorio remoto smarlab.

Debido a los problemas y laboratorios planteados se practicó de una manera muy dinámica, acorde a los problemas actuales, en los cuales se hicieron una serie de pasos hasta llegar a la solución de la red y probar conectividad y la eficiencia de ella.

Es muy importante garantizar la seguridad de los routers, a través de cuentas de usuarios y sus respectivas contraseñas, así mismo la encriptación de estas, para poder acceder a él, ya que no garantiza la seguridad y evitamos la pérdida de configuración y de información.

La tecnología en redes de Cisco ayuda a su implementación de topologías, por medio de la configuración de cada uno de sus dispositivos, nos permite configurar y mostrar errores para poder corregirlos y que haya una excelente conectividad en la red que estamos desarrollando.

Se desarrollaron dos casos de estudio, donde se configuró su topología física, calculando su direccionamiento, y configurando paso a paso cada uno de los dispositivos, hasta obtener la solución y conectividad de la red.

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

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 redes IP 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>

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

Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCl_pLtPD9