

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

OMAR HERNANDO ROJAS GARCIA

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

TUNJA

2021

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

OMAR HERNANDO ROJAS GARCIA

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

TUTOR:
Ing. JAVIER RICARDO VASQUEZ

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

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

TUNJA, 29 de noviembre de 2021

AGRADECIMIENTOS

En el proceso de formación realizado durante toda la carrera profesional, debo dar las gracias a mis tutores que con sus enseñanzas permitieron afianzar mis conocimientos en el campo de los sistemas y las redes informáticas, debo dar gracias a mis padres quienes me animaron a no desfallecer ni bajar la guardia y sacar adelante este proyecto de vida que decidí realizar; a las personas que me colaboraron directa e indirectamente, a Dios por darme fuerza y sabiduría para realizar cada una de mis actividades. No ha sido fácil, pero con mucha disciplina he podido realizar lo solicitado y he aprendido todo lo necesario para convertirme en un gran profesional y dejar en alto las enseñanzas adquiridas por lo cual me siento muy orgulloso de mi universidad y mis tutores.

Muchas gracias

CONTENIDO

NOTA DE ACEPTACION.....	3
AGRADECIMIENTOS.....	4
CONTENIDO.....	5
LISTA DE TABLAS	6 - 7
LISTA DE FIGURAS	8 - 13
GLOSARIO	14 - 15
RESUMEN	16
ABSTRACT	17
INTRODUCCIÓN	18
DESARROLLO	19 - 86
1. Escenario 1.....	19 - 35
2. Escenario 2.....	36 - 86
CONCLUSIONES	87
BIBLIOGRAFÍA.....	88

LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento	20
Tabla 2. Configuración aspectos básicos R1	21
Tabla 3. Configuración aspectos básicos S1	28
Tabla 4. PC_A Network Configuration	34
Tabla 5. PC_B Network Configuration	35
Tabla 6. Comandos básicos para inicializar Routers y Switches	37
Tabla 7. Tabla de direccionamiento del Servidor de internet	41
Tabla 8. Comandos para la configuración de R1	42
Tabla 9. Comandos para la configuración de R2	44 - 45
Tabla 10. Comandos para la configuración de R3	46 - 47
Tabla 11. Comandos para la configuración de S1	49
Tabla 12. Comandos para la configuración de S3	50
Tabla 13. Tabla de resultados prueba de conectividad	52 - 53
Tabla 14. Comandos para la configuración de S1	55 - 57
Tabla 15. Comandos para la configuración de S3	58 - 60
Tabla 16. Comandos para la configuración de R1	62 - 63
Tabla 17. Tabla de resultados prueba de conectividad	64 - 65
Tabla 18. Tabla de conexión OSPF en R1	66 - 67
Tabla 19. Tabla de conexión OSPF en R2	68
Tabla 20. Tabla de conexión OSPF en R3	69 - 70

Tabla 21. Tabla de verificación de resultados OSPF -----	70 – 71
Tabla 22. Tabla de configuración de R1 como servidor DHCP para las VLAN 21 y 23 _____	72 - 73
Tabla 23. Tabla de configuración de NAT estática y dinámica en R2-----	74 - 76
Tabla 24. Verificación del protocolo DHCP y la NAT estática-----	77 - 79
Tabla 25. Tabla de configuración NTP -----	80 - 81
Tabla 26. Tabla de comandos para restringir el acceso a las líneas VTY en R2	82 – 83
Tabla 27. Tabla de comandos para realizar pruebas de configuración-----	84 - 86

LISTA DE FIGURAS

Figura 1. Escenario 1 _____	19
Figura 2. Subneteo escenario 1 _____	20
Figura 3. Simulación de escenario 1 _____	22
Figura 4. Desactivación de las búsquedas DNS R1 -----	23
Figura 5. Asignación de nombre a R1 _____	23
Figura 6. Asignación nombre de dominio a R1 -----	23
Figura 7. Asignación de contraseña EXEC en modo privilegiado a R1 -----	23
Figura 8. Creación de contraseña de acceso a la consola R1-----	24
Figura 9. Establecimiento longitud de caracteres de contraseña R1 -----	24
Figura 10. Creación de usuario administrativo en R1 -----	24
Figura 11. Configuración vty para uso de BD local en R1 -----	25
Figura 12. Configuración vty aceptando ssh en R1 -----	25
Figura 13. Ciframos contraseñas de texto en R1 -----	25
Figura 14. Configuramos un motd banner en R1 -----	25
Figura 15. Configuramos interfaz G0/0/0 en R1 -----	26
Figura 16. Configuramos interfaz G0/0/1 en R1 -----	26
Figura 17. Generamos clave de cifrado RSA en R1 -----	27
Figura18. Pantallazo verificación de credenciales de acceso a R1 -----	27
Figura 19. Desactivación de las búsquedas DNS en S1 -----	28
Figura 20. Asignación de nombre a S1 _____	29
Figura 21. Asignación nombre del dominio de S1 -----	29
Figura 22. Asignación de contraseña EXEC en modo privilegiado a S1 -----	30
Figura 23. Creación de contraseña de acceso a la consola S1 -----	30
Figura 24. Creación de usuario administrativo en S1 -----	30

Figura 25. Configuración vty para uso de BD local en S1 -----	31
Figura 26. Configuración vty aceptando ssh en S1 -----	31
Figura 27. Ciframos contraseñas de texto en S1 -----	31
Figura 28. Creamos un motd banner _____	32
Figura 29. Generamos clave de cifrado RSA en S1 -----	32
Figura 30. Configuramos interfaz vlan 1 -----	33
Figura 31. Configuramos el Gateway -----	33
Figura 32. Configuración de PC_A _____	34
Figura 33. Configuración de PC_B _____	35
Figura.34 Topología Escenario_2 _____	36
Figura35. Inicialización y recarga del R1 -----	37
Figura36. Inicialización y recarga del R2 -----	38
Figura37. Inicialización y recarga del R3 -----	38
Figura38. Inicialización y recarga del S1 -----	39
Figura39. Verificación de la BD del S1 _____	39
Figura40. Inicialización y recarga del S3 -----	40
Figura41. Verificación de la BD del S3 _____	40
Figura42. Configuración de Servidor Web -----	41
Figura43. Configuración de R1 _____	43
Figura44. Configuración de R2 _____	46
Figura45. Configuración de R3 _____	48
Figura46. Configuración de S1 -----	49

Figura47. Configuración de S3	50
Figura48. Ping a S0/2/0	52
Figura49. Ping a S0/2/1	52
Figura50. Ping al Gateway predeterminado	53
Figura51. Ping simulado de R1 a R2	53
Figura52. Ping simulado de R2 a R3	54
Figura53. Ping al servidor web	54
Figura54. Creación BD de VLAN21	55
Figura55. Asignación de IP de administración	55
Figura56. Asignación del Gateway predeterminado	56
Figura57. Troncalización del puerto F0/3	56
Figura58. Troncalización de la interfaz F0/5	56
Figura59. Configuración de los puertos de acceso	57
Figura60. Asignación de F0/6 a VLAN 21	57
Figura61. Inhabilitación de los puertos sin usar en S1	58
Figura62. Creación BD de VLAN23	59
Figura63. Asignación de IP de administración	59
Figura64. Asignación del Gateway predeterminado	59
Figura65. Troncalización del puerto F0/3	60
Figura66. Configuración de puertos de acceso	60
Figura67. Asignación de F0/18 a VLAN 23	60
Figura68. Apagado de los puertos sin uso	61

Figura69. Configuración subinterfaz 802.1Q.21 en G0/0/1 -----	62
Figura70. Configuración subinterfaz 802.1Q.23 en G0/0/1 -----	62
Figura71. Configuración subinterfaz 802.1Q.99 en G0/0/1 -----	63
Figura72. Activación de la interfaz G0/0/1 -----	63
Figura73. Resultado de ping desde S1 a VLAN 99-----	64
Figura74. Resultado de ping desde S3 a VLAN 99-----	64
Figura75. Resultado de ping desde S1 a VLAN 21-----	64
Figura76. Resultado de ping desde S3 a VLAN 23-----	65
Figura77. Configuración de OSPF en área 0 del R1-----	66
Figura78. Configuración de redes conectadas directamente -----	66
Figura79. Establecimiento de interfaces LAN como pasivas-----	67
Figura80. Desactivación de la sumarización automática-----	67
Figura81. Configuración de OSPF en área 0 del R2-----	68
Figura82. Configuración de redes conectadas directamente -----	68
Figura83. Establecimiento de interfaces LAN como pasivas-----	68
Figura84. Configuración de OSPF en área 0 del R3-----	69
Figura85. Configuración de redes conectadas directamente -----	69
Figura86. Establecimiento de interfaces LAN como pasivas-----	69
Figura87. Resultado del comando show ip protocol-----	70
Figura88. Resultado del comando show ip route OSPF-----	71
Figura89. Resultado del comando show ip OSPF-----	71

Figura90. Comando de reserva para la configuración de las VLAN estáticas 21---	72
Figura91. Comando de reserva para la configuración de las VLAN estáticas 23---	72
Figura92. Comando para crear un pool de DHCP en VLAN 21 -----	73
Figura93. Comando para crear un pool de DHCP en VLAN 23-----	73
Figura94. Creación de BD local con cuenta de usuario-----	74
Figura95. Habilitación del servicio http_____	74
Figura96. Configuración de http para la autenticación en la BD local -----	74
Figura97. Creación de una NAT estática en el servidor web -----	75
Figura98. Asignación de interfaces para la NAT estática -----	75
Figura99. Configuración de la NAT dinámica dentro de la ACL privada-----	76
Figura100. Definición del pool en Ips públicas utilizadas -----	76
Figura101. Definición de la traducción de NAT dinámica -----	76
Figura102. Asignación de DHCP a la PC_A -----	77
Figura103. Asignación de DHCP a la PC_C -----	78
Figura104. Ping de PC_A a PC_C_____	78
Figura105. Accesibilidad de PC_A a internet -----	79
Figura106. Ajuste de fecha y hora en R2 -----	80
Figura107. Configuración de NTP como maestro -----	80
Figura108. Configuración de R1 como cliente NTP -----	80
Figura 109. Configuración de R1 para actualizaciones periódicas -----	81
Figura110. Verificación de NTP en R1 _____	81
Figura111. Configuración de la conexión a telnet de R1 a R2-----	82

Figura112. Aplicación de ACL con nombre de líneas VTY -----	82
Figura113. Acceso por telnet a las líneas VTY -----	83
Figura114. Verificación de ACL_____-----	83
Figura115. Coincidencias recibidas por ACL en R2	84
Figura116. Restablecimiento de contadores de una ACL -----	84
Figura117. Verificación de ACL a las interfaces y las direcciones donde aplica-----	85
Figura118. Verificación de las traducciones NAT -----	85
Figura119. Eliminación de las traducciones NAT -----	86

GLOSARIO

CCNP (Cisco Certified Design Professional): Proporcionan conocimientos avanzados en el diseño de redes LAN, WAN, grandes redes y redes de conexión telefónica, tanto enrutadas como conmutadas.

CISCO: Empresa principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

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

DNS: Es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada.

Dominio: Es un nombre único que identifica a una subárea de internet. El propósito principal de los nombres de dominio en Internet y del sistema de nombres de dominio, es traducir las direcciones IP de cada activo en la red, a términos memorizables y fáciles de encontrar.

Direccionamiento: Es la forma en que se interpretan los bits de un campo de dirección de una instrucción para localizar el operando y/o la dirección destino del resultado de la instrucción.

Electrónica: Es una rama de la física aplicada que comprende la física, la ingeniería, la tecnología y las aplicaciones que tratan con la emisión, el flujo y el control de los electrones —u otras partículas cargadas eléctricamente— en el vacío y la materia.

Enrutamiento: El enrutamiento o ruteo es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad.

Interfaz: Se utiliza en informática para nombrar a la conexión funcional entre dos sistemas, programas, dispositivos o componentes de cualquier tipo, que proporciona una comunicación de distintos niveles, permitiendo el intercambio de información.

Networking: Es, literalmente, crear relaciones desde un punto de vista laboral o de negocio. Consiguiendo, gracias a la interacción entre personas que comparten intereses comunes, soluciones a sus problemas o potenciar sus habilidades en busca de un beneficio común.

Redes: Es un conjunto de equipos nodos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Routing: Es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad.

RSA: Es un sistema criptográfico de clave pública desarrollado en 1979, que utiliza factorización de números enteros. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.

Simulación: Es el artificio contextual que hace referencia a la investigación de una hipótesis o un conjunto de hipótesis de trabajo utilizando modelos un método perfecto para la enseñanza y aprendizaje.

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

Switching: Es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI.

VTY: Permiten el acceso a un dispositivo Cisco a través de Telnet. De manera predeterminada, muchos switches Cisco admiten hasta 16 líneas vty que se numeran del 0 al 15.

RESUMEN

El siguiente trabajo tiene como propósito desarrollar la temática como alternativa de grado, donde se proponen dos escenarios con características y requerimientos específicos, en donde el primer escenario será desarrollado acorde a las temáticas del módulo1.

La guía solicita la configuración de los dispositivos, diseñar el esquema de direccionamiento IPv4 para las redes LAN propuestas, y la administración del Router y el Switch de forma segura. Además, tiene como objetivos construir en el simulador la red, desarrollar el esquema de direccionamiento IP, enrutar para las LAN 1 y 2, configurar los aspectos básicos de los dispositivos de la red propuesta, configura los ajustes básicos de seguridad y conmutación, en el R1 y S1, y finalmente configurar los hosts y verificar la conectividad entre los equipos.

La segunda parte consta de 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. Basándose en la normatividad y los protocolos solicitados en la guía y ajustados en los escenarios simulados en la herramienta Packet Tracer.

ABSTRACT

The purpose of the following work is to develop the theme as an alternative degree, where two scenarios with specific characteristics and requirements are proposed, where the first scenario will be developed according to the themes of module1.

The guide requests the configuration of the devices, design the IPv4 addressing scheme for the proposed LAN networks, and the administration of the Router and the Switch in a secure way. In addition, its objectives are to build the network in the simulator, develop the IP addressing scheme, route for LANs 1 and 2, configure the basic aspects of the proposed network devices, configure the basic security and switching settings, in the R1 and S1, and finally configure the hosts and verify the connectivity between the computers.

The second part consists of configuring a small network to support IPv4 and IPv6 connectivity, switch security, inter-VLAN routing, OSPF dynamic routing protocol, Dynamic Host Configuration Protocol (DHCP), dynamic network address translation and static (NAT), access control lists (ACL) and the server / client Network Time Protocol (NTP). During the evaluation, you will test and register your network using common CLI commands. Based on the regulations and protocols requested in the guide and adjusted in the simulated scenarios in the Packet Tracer tool.

INTRODUCCIÓN

La información como fuente de enriquecimiento personal para el aprendizaje se puede transmitir mediante distintas formas y en distintos medios, la más utilizada actualmente para la comunicación global en todo el mundo es la utilización de las redes informáticas (Networking), y sus aplicaciones de red, pues las utilizamos para compartir información que pueden observar distintas personas alrededor del mundo y con quienes deseamos compartirla; pero poder dar buen uso de las normas debemos conocer cómo implementarlas y asegurarlas.

Los estudiantes de este diplomado CISCO CCNP debemos estar en la capacidad de dar buen uso a los protocolos de diseño y configuración, que se aprendieron durante el periodo, para poder aplicarlos en la simulación de cada uno de los escenarios propuestos para este trabajo, bajo la herramienta Packet Tracer; configurando correctamente cada uno de los dispositivos solicitados para su diseño, como equipos PC, Routers, Switches, cableado adecuado y otros dispositivos manejados en el medio, además utilizando los respectivos comandos de configuración de equipo por medio de consola en cada dispositivo, y detallando el paso a paso de cada una de estas, logrando así el objetivo de la actividad.

Finalmente se espera cumplir a satisfacción los requerimientos solicitados en la guía de actividades del paso 6, "Entrega avance documento final"; ya que contiene información fundamental en nuestro camino profesional en el área de la ingeniería, más exactamente en la implementación y configuración de redes cableadas e inalámbricas CISCO.

DESARROLLO

Escenario 1

Aspectos Básicos de la situación

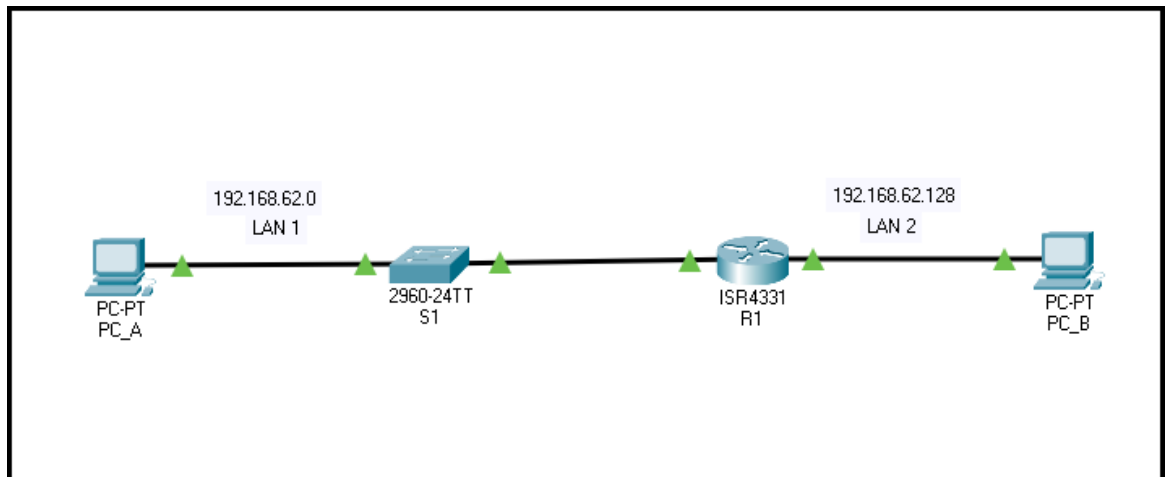
En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configurara el Router 1 y el Swicht 1 y los PC's. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN 1 (100 hosts) y la LAN 2 (50 hosts).

Parte 1: Construya la Red

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

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

Figura 1. Escenario 1



Fuente: Elaborado por Omar Hernando Rojas García, modelo de la red que se trabajara en la herramienta de simulación Packet Tracer.

Parte 2: Desarrolle le esquema del direccionamiento IP

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

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

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

Figura 2. Subneteo Escenario 1

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1		192.168.62.0													
2															
3		LAN 1	100 hosts			Subred No	Dirección	Mascara	1ra IP valida	Última valida	Broadcast	No de hosts			
4		LAN 2	50 hosts			1	192.168.62.0	/ 25	192.168.62.1	192.168.62.126	192.168.62.127	100			
5		R1 G 0/0/1	192.168.62.1			2	192.168.62.128	/ 26	192.168.62.129	192.168.62.190	192.168.62.191	50			
6		R1 G 0/0/0	192.168.62.129												
7		S1 SVI	192.168.62.1												
8		PC_A	192.168.62.2												
9		PC_B	192.168.62.130												
10															
11															
12															
13															
14															
15															
16			2 ⁰ = 1												
17			2 ¹ = 2												
18			2 ² = 4												
19			2 ³ = 8												
20			2 ⁴ = 16												
21			2 ⁵ = 32												

Fuente: Elaborado por Omar Hernando Rojas García, Desarrollo del direccionamiento IP bajo una hoja de cálculo Excel

Tabla 1. Tabla de direccionamiento

Ítem	Requerimiento
Dirección de Red	192.168.62.0 donde 62 corresponde a los dos últimos dígitos de mi cédula
Requerimiento de host subred LAN 1	192.168.62.0 (100 hosts)
Requerimiento de host subred LAN 2	192.168.62.128 (50 hosts)
R1 G 0/0/1	192.168.62.1
R1 G 0/0/0	192.168.62.129
S1 SVI	192.168.62.1
PC_A	192.168.62.2
PC_B	192.168.62.130

Fuente: Elaborado por Omar Hernando Rojas García,

Parte 3: Configure aspectos Básicos

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

Paso 1: Configurar los aspectos básicos

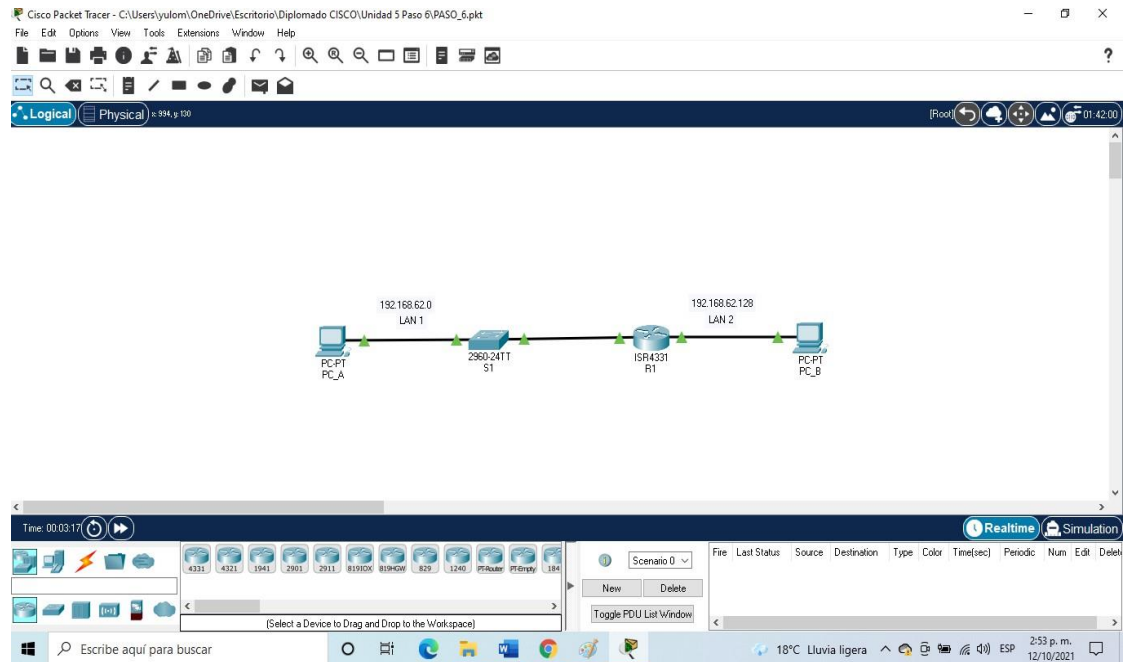
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 2. Configuración aspectos básicos R1

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

ESCENARIO 1

Figura 3. Simulación escenario1



Fuente: Elaborado por Omar Hernando Rojas García, Implementación de la red en el programa Packet Tracer

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

Se procede a configurar cada uno el enrutador. 1

Se asigna nombre y protocolo de comunicación mediante EIGRP que fueron asignados.

Router R1

Router>

Router>enable

Router#configure terminal

Router(config)# No ip domain-lookup

Ingreso al modo privilegiado

Ingreso al modo de configuración

Desactivamos las búsquedas DNS

Figura4.Desactivación de las búsquedas DNS en R1

```
Press RETURN to get started!  
El Acceso al Router es restringido. Unicamente personal autorizado.  
User Access Verification  
Password:  
R1>enable  
Password:  
R1#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)#No ip domain-lookup  
R1(config)#
```

Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

Router(config)#hostname R1 *Asignamos nombre al router*

Figura5.Asignación de nombre a R1

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

Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

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

Figura6.Asignación nombre del dominio de R1

```
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)#No ip domain-lookup  
R1(config)#hostname R1  
R1(config)#ip domain name ccna-lab.com  
R1(config)#
```

Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

R1(config)# enable password ciscocompass *Asignamos contraseña EXEC en modo privilegiado*

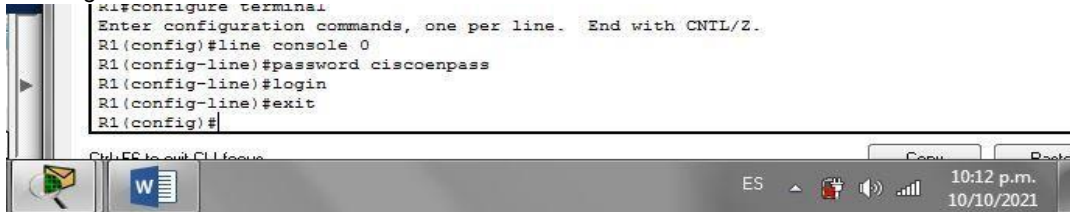
Figura7.Asignación de contraseña EXEC en modo privilegiado a R1

```
R1(config)#No ip domain-lookup  
R1(config)#hostname R1  
R1(config)#ip domain name ccna-lab.com  
R1(config)#enable password ciscocompass  
R1(config)#exit  
R1#  
%SYS-5-CONFIG_I: Configured from console by console  
R1#
```

Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

```
R1(config)# line console 0 Creamos contraseña de acceso a la consola
R1(config)# password ciscoenpass
R1(config)# login
```

Figura8. Creación de contraseña de acceso a la consola R1

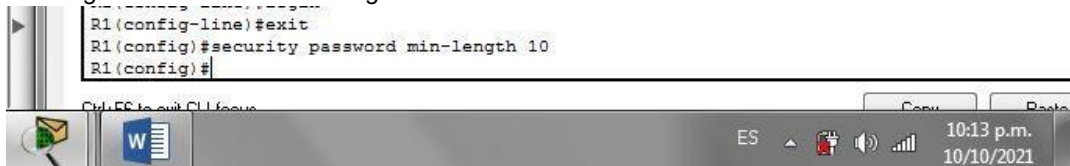


```
R1(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# line console 0
R1(config-line)# password ciscoenpass
R1(config-line)# login
R1(config-line)# exit
R1(config)#
```

Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

```
R1(config)# security password min-length 10 Establecemos longitud mínima para
las contraseñas
```

Figura9. Establecimiento longitud de caracteres de contraseña R1

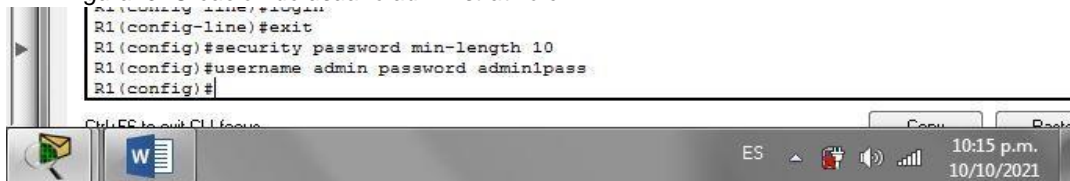


```
R1(config-line)# exit
R1(config)# security password min-length 10
R1(config)#
```

Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

```
R1(config)# username admin password admin1pass Creamos un usuario administrativo
admin1pass en la base de datos local
```

Figura10. Creación de usuario administrativo en R1

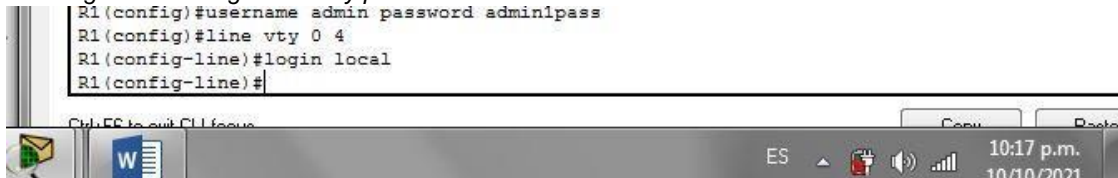


```
R1(config-line)# exit
R1(config)# security password min-length 10
R1(config)# username admin password admin1pass
R1(config)#
```

Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

```
R1(config)# line vty 0 4 Configuramos inicio de sesión en las
R1(config)# login local líneas vty para uso de BD local
```

Figura11. Configuración vty para uso de BD local en R1



```
R1(config)# username admin password admin1pass
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)#
```

Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

R1(config)# transport input ssh

Configurar VTY solo aceptando SSH

Figura12. Configuración vty aceptando ssh en R1

```
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#
```



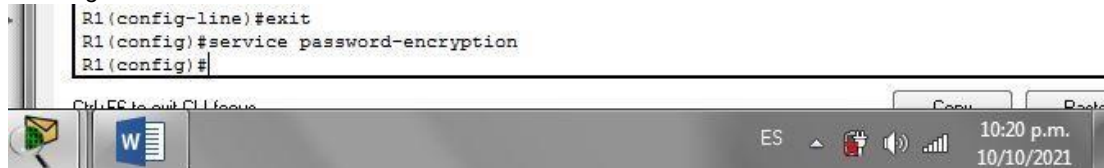
Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

R1(config)# service password-encryption

Ciframos las contraseñas de texto

Figura13. Ciframos contraseñas de texto en R1

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



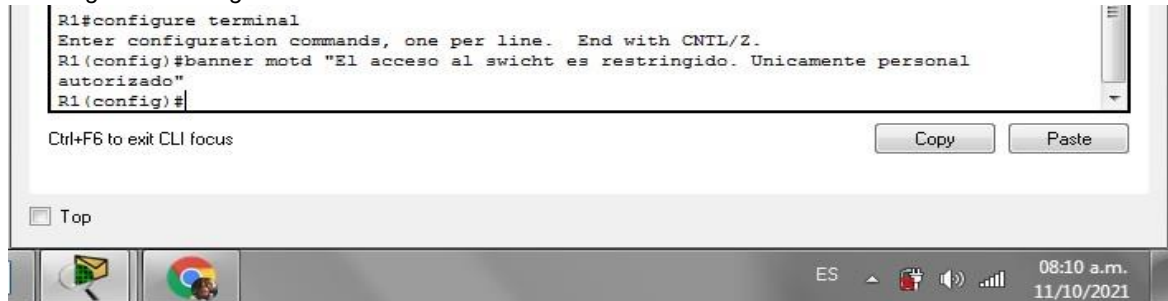
Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

R1(config)# banner motd "El Acceso al
router es restringido. Únicamente personal autorizado"

Configuramos un motd banner

Figura14. Configuramos un motd banner en R1

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#banner motd "El acceso al swicht es restringido. Unicamente personal
autorizado"
R1(config)#
```



Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

R1(config)# interface G 0/0/0

Configuramos la interfaz G 0/0/0

R1(config-if)# ip address 192.168.62.129 255.255.255.192

R1(config-if)# no shutdown

Figura15. Configuramos interfaz G0/0/0 en R1

```
R1(config)#interface G 0/0/0
R1(config-if)#ip address 192.168.62.129 255.255.255.192
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

ES 08:13 a.m. 11/10/2021

Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

```
R1(config)# interface G 0/0/1          Configuramos la interface G 0/0/1
R1(config-if)# ip address 192.168.62.1 255.255.255.128
R1(config-if)# no shutdown
```

Figura16. Configuramos interfaz G0/0/1 en R1

```
R1(config)#interface G 0/0/1
R1(config-if)#ip address 192.168.62.1 255.255.255.128
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

ES 08:16 a.m. 11/10/2021

Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

```
R1(config)# ip domain-name ccna-lab.com  Generamos una clave de cifrado
R1(config)# crypto key generate rsa      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]
```

Figura17. Generamos clave de cifrado RSA en R1

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip domain-name ccna-lab.com
R1(config)#crypto key generate rsa
The name for the keys will be: R1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#
```

Ctrl+F6 to exit CLI focus

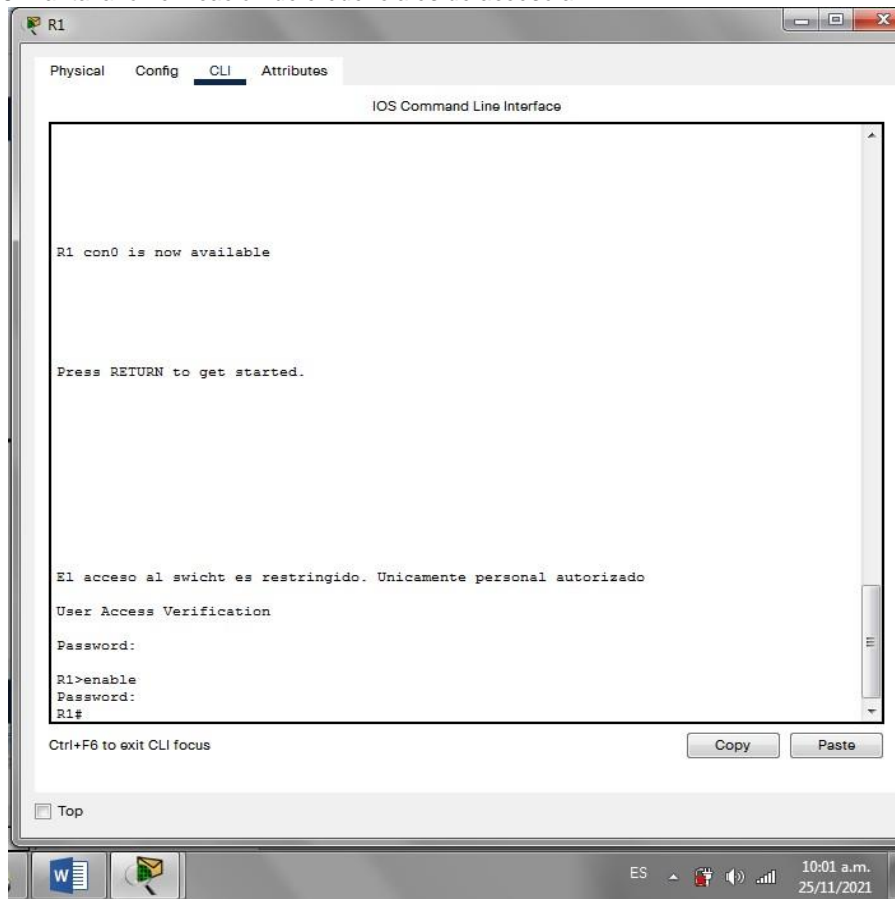
Copy Paste

Top

ES 08:35 a.m. 11/10/2021

Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

Figura18. Pantallazo verificación de credenciales de acceso a R1



Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

Las tareas de configuración del S1 incluyen:

Tabla 3. Configuración aspectos básicos S1

Tarea	Especificación
Desactivar las búsquedas DNS	
Nombre del Swicht	S1
Nombre del dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Ciscoenpass
Contraseña de acceso a la consola	Ciscoconpass
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar las líneas VTY para que acepten únicamente SSH	
Cifrar las contraseñas de texto no cifrado	
Configure un MOTD Banner	
Generar una clave de cifrado RSA	Módulo de 1024 bits
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento
Configuración del Gateway predeterminado	Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento.

Fuente: Elaborado por Omar Hernando Rojas García

Swicht S1

Swicht>

Swicht>enable

Swicht#configure terminal

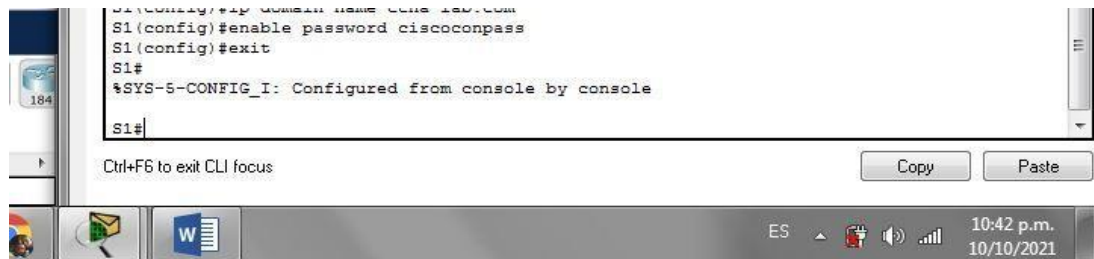
Swicht(config)# No ip domain-lookup

Ingreso al modo privilegiado

Ingreso al modo de configuración

Desactivamos las busquedas DNS

Figura22. Asignación de contraseña EXEC en modo privilegiado a S1



Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

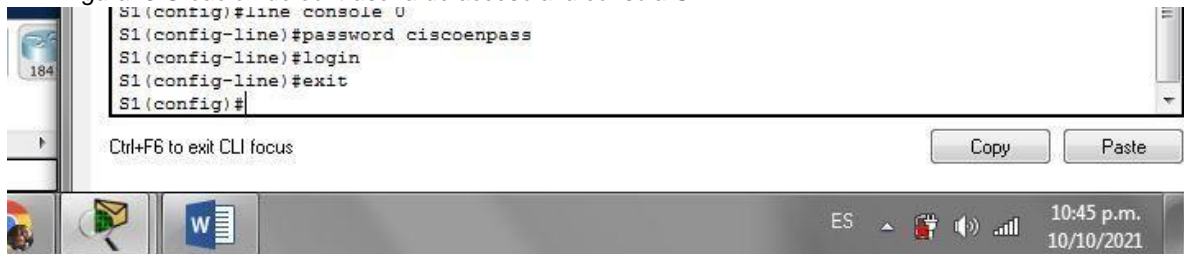
S1(config)# line console 0

Creamos contraseña de acceso a la consola

S1(config)# password ciscoenpass

S1(config)# login

Figura23. Creación de contraseña de acceso a la consola S1

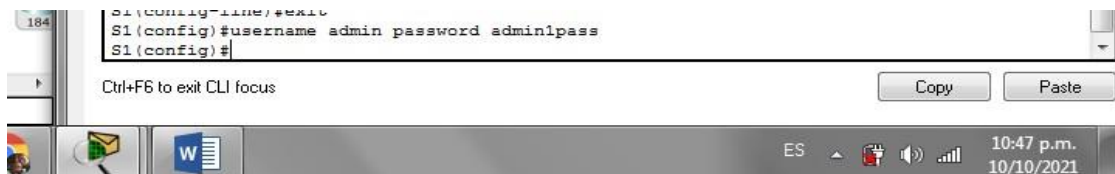


Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

S1(config)# username admin password admin1pass Creamos un usuario administrativo en la base de datos local

Figura24. Creación de usuario administrativo en S1

Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

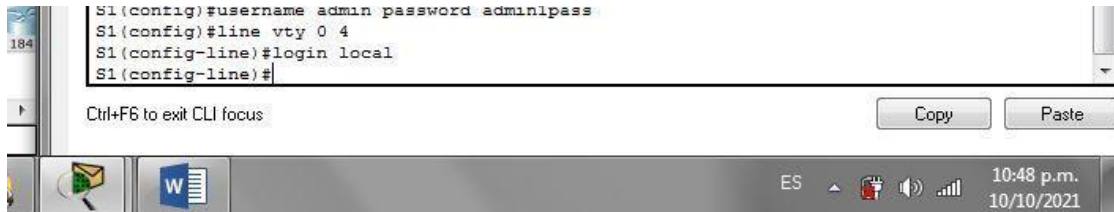


Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

S1(config)# line vty 0 4
S1(config)# login local

Configuramos inicio de sesión en las líneas vty para uso de BD local

Figura25. Configuración vty para uso de BD local en S1



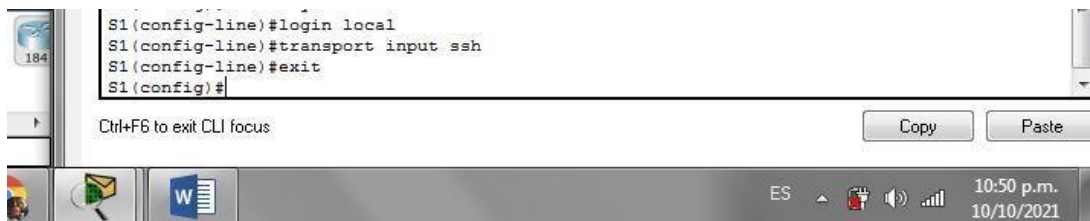
```
S1(config)#username admin password adminpass
S1(config)#line vty 0 4
S1(config-line)#login local
S1(config-line)#
```

Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

S1(config)# transport input ssh

Configurar VTY solo aceptando SSH

Figura26. Configuración vty aceptando ssh en S1



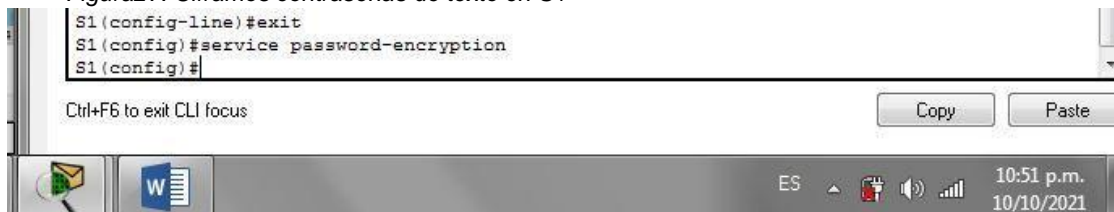
```
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config-line)#exit
S1(config)#
```

Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

S1(config)# service password-encryption

Ciframos las contraseñas de texto

Figura27. Ciframos contraseñas de texto en S1



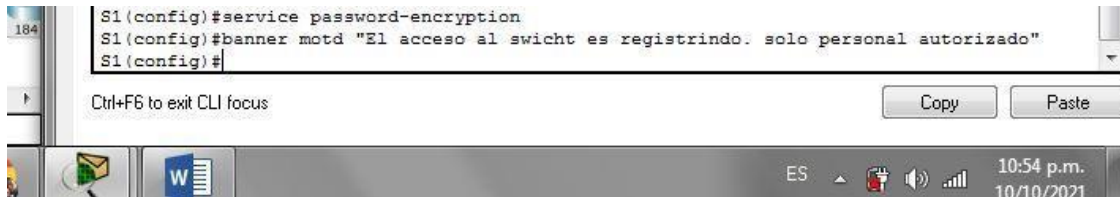
```
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#
```

Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

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

Configuramos un motd banner

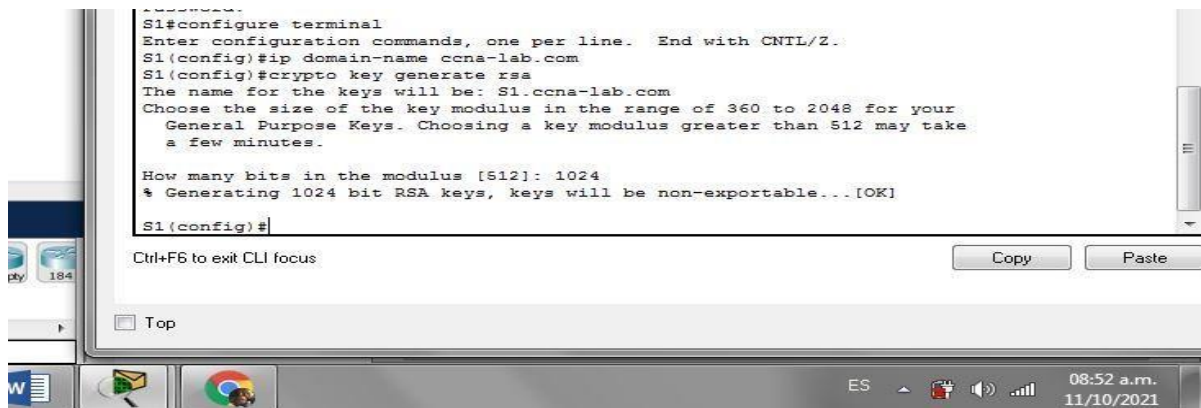
Figura28. Configuramos un motd banner en S1



Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

```
S1(config)# ip domain-name ccna-lab.com      Generamos una clave de cifrado
S1(config)# crypto key generate rsa         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]
```

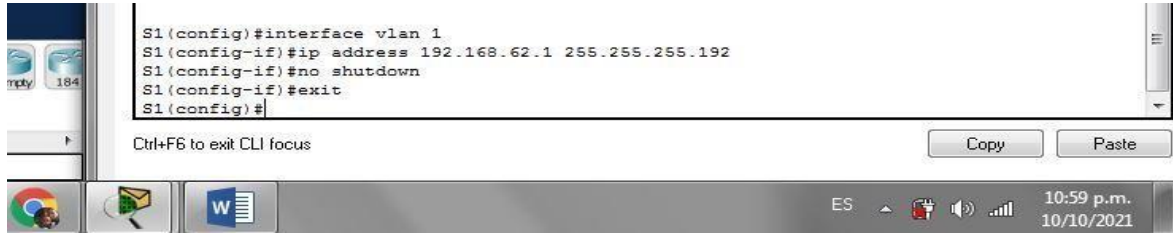
Figura29. Generamos clave de cifrado RSA en S1



Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

```
S1(config)# interface S1 SVI                Configuramos la interface vlan 1
S1(config-if)# ip address 192.168.62.1 255.255.255.192
S1(config-if)# no shutdown
```

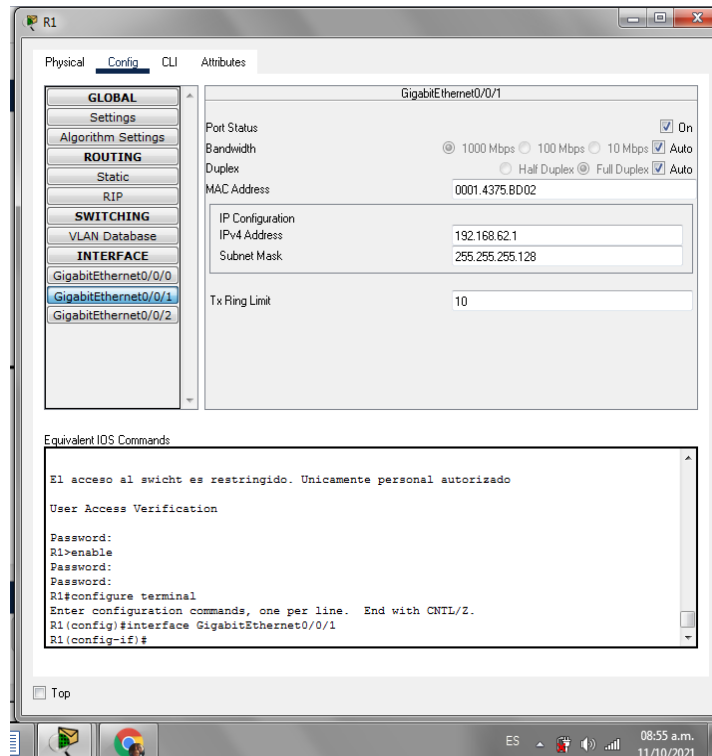
Figura30. Configuramos interfaz vlan 1



Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por consola CLI

S1(config)# interface GE0/1 Configuramos el Gateway
S1(config-if)# ip address 192.168.62.1 255.255.255.192
S1(config-if)# no shutdown

Figura31. Configuramos Gateway



Fuente: Elaborado por Omar Hernando Rojas García, Ingreso del código por interfaz gráfica

Paso 2: Configurar los equipos

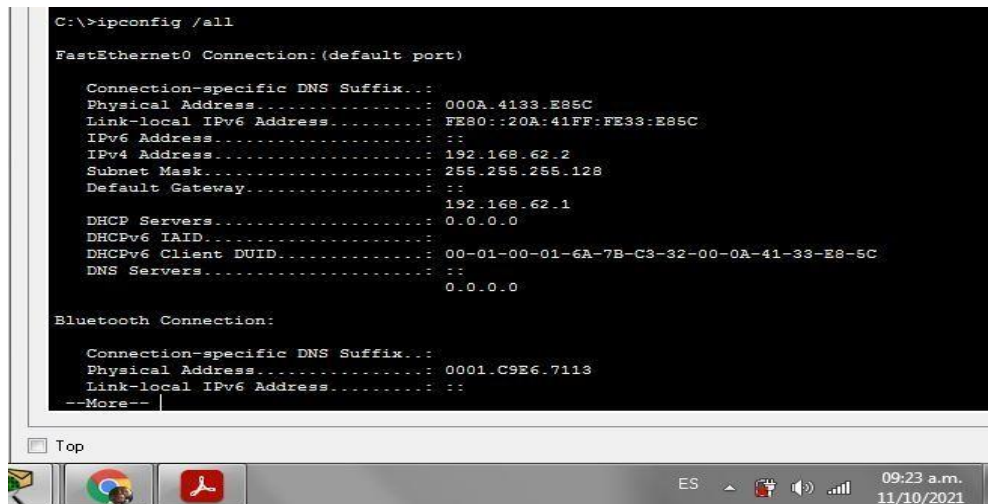
Configure los equipos host PC_A y PC_B conforme a la tabla de direccionamiento, registre las configuraciones de red de los hosts con el comando **ipconfig / all**

Tabla 4. PC A Network Configuration

PC_A Network Configuration	
Descripción	FastEthernet0 connection: (default port)
Dirección física	000A.4133.E85C
Dirección IP	192.168.62.2
Mascara de subred	255.255.255.128
Gateway predeterminado	192.168.62.1

Fuente: Elaborado por Omar Hernando Rojas García,

Figura32. Configuración de PC_A



```
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix... : 
    Physical Address. . . . . : 000A.4133.E85C
    Link-local IPv6 Address . . . . . : FE80::20A:41FF:FE33:E85C
    IPv6 Address. . . . . : 
    IPv4 Address. . . . . : 192.168.62.2
    Subnet Mask . . . . . : 255.255.255.128
    Default Gateway . . . . . : 
    DHCP Servers . . . . . : 192.168.62.1
    DHCPv6 IAID. . . . . : 0.0.0.0
    DHCPv6 Client DUID. . . . . : 00-01-00-01-6A-7B-C3-32-00-0A-41-33-E8-5C
    DNS Servers . . . . . : 
    . . . . . : 0.0.0.0

Bluetooth Connection:

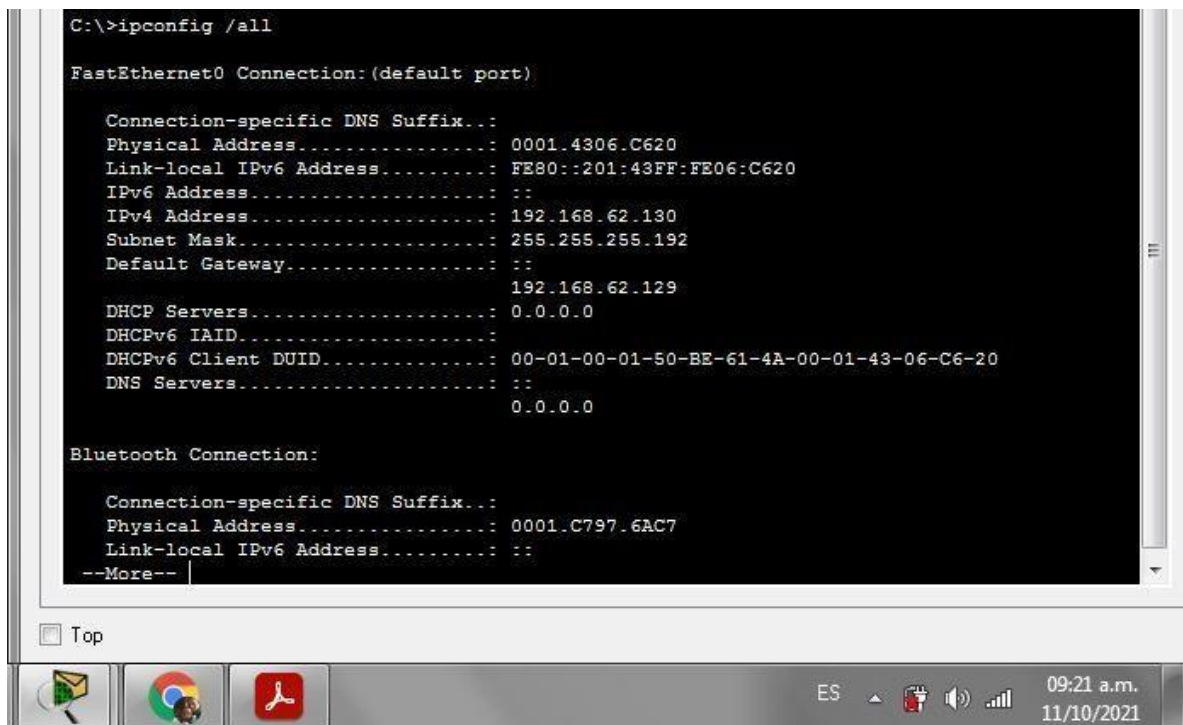
    Connection-specific DNS Suffix... : 
    Physical Address. . . . . : 0001.C9E6.7113
    Link-local IPv6 Address . . . . . : 
    --More--
```

Fuente: Elaborado por Omar Hernando Rojas García, Aplicación del comando **ipconfig /all** por command prompt

Tabla 5. PC B Network Configuration

PC_B Network Configuration	
Descripción	FastEthernet0 connection: (default port)
Dirección física	0001.4306.C620
Dirección IP	192.168.62.130
Mascara de subred	255.255.255.192
Gateway predeterminado	192.168.62.129

Figura33. Configuración de PC_B



```
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Physical Address. . . . .: 0001.4306.C620
    Link-local IPv6 Address . . . . .: FE80::201:43FF:FE06:C620
    IPv6 Address. . . . .: ::
    IPv4 Address. . . . .: 192.168.62.130
    Subnet Mask . . . . .: 255.255.255.192
    Default Gateway. . . . .: ::
                                192.168.62.129
    DHCP Servers. . . . .: 0.0.0.0
    DHCPv6 IAID. . . . .:
    DHCPv6 Client DUID. . . . .: 00-01-00-01-50-BE-61-4A-00-01-43-06-C6-20
    DNS Servers. . . . .: ::
                                0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Physical Address. . . . .: 0001.C797.6AC7
    Link-local IPv6 Address . . . . .: ::
    --More--
```

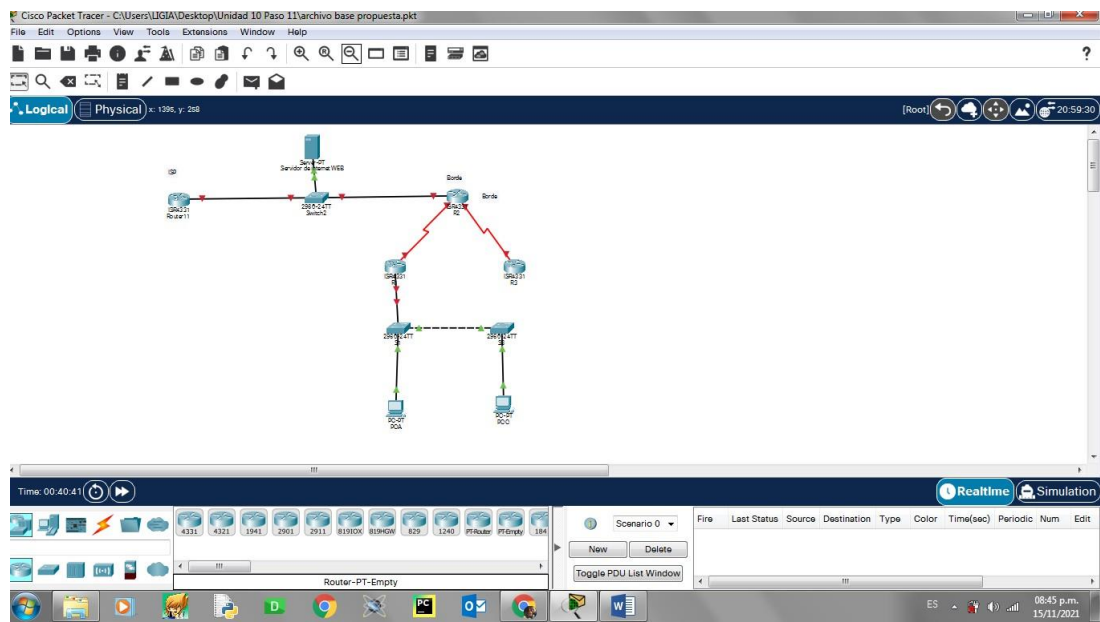
Fuente: Elaborado por Omar Hernando Rojas García, Aplicación del comando ipconfig /all por command prompt

Escenario 2

Aspectos Básicos de la situación

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.

Figura34. Topología escenario 2



Fuente: Elaborado por Omar Hernando Rojas García, Implementación de la red en el programa Packet Tracer

Parte 1: Inicializar los dispositivos

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

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

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

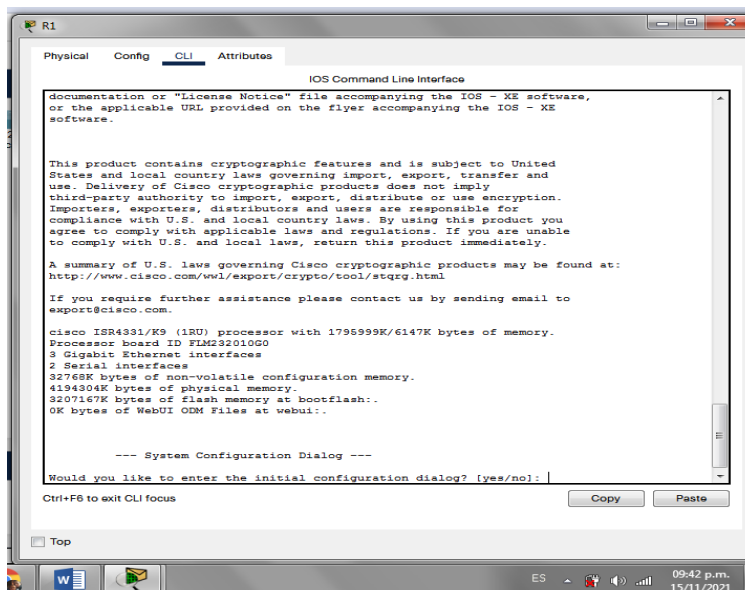
Tabla 6. Comandos básicos par inicializar y reiniciar Routers y switches

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

Fuente: Elaborado por Omar Hernando Rojas García,

R1

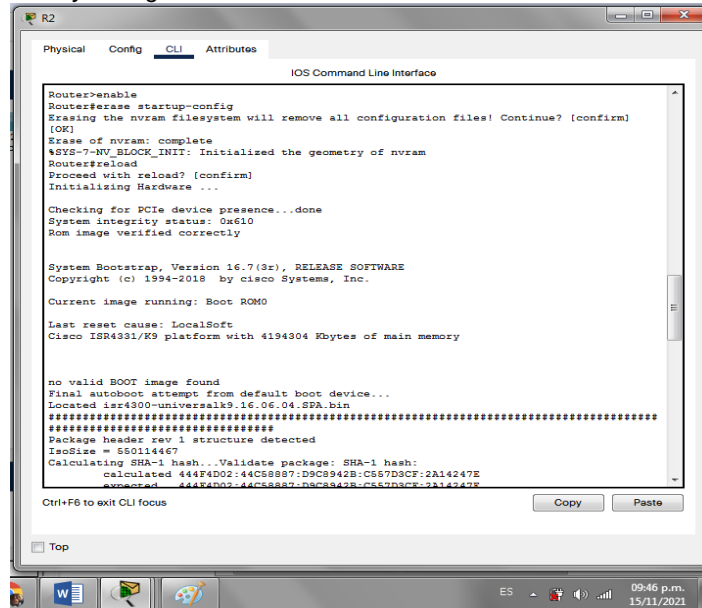
Figura35. Inicialización y recarga del R1



Fuente: Elaborado por Omar Hernando Rojas García, Configuración de comandos por consola

R2

Figura36. Inicialización y recarga del R2



```
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]
Initializing Hardware ...

Checking for PCIe device presence...done
System integrity status: 0x610
Rom image verified correctly

System Bootstrap, Version 16.7(3z), RELEASE SOFTWARE
Copyright (c) 1994-2018 by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft
Cisco ISR4331/K9 platform with 4194304 Kbytes of main memory

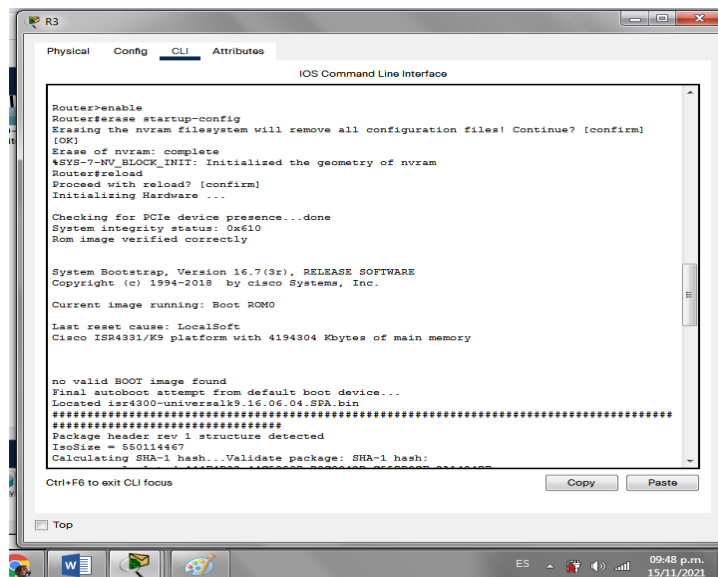
no valid BOOT image found
Final autoboot attempt from default boot device...
Located isr4300-universalk9.16.06.04.SPA.bin
#####
Package header rev 1 structure detected
IsoSize = 560114467
Calculating SHA-1 hash...Validate package: SHA-1 hash:
  calculated 444F4D02:44C68897:D9C942B:C567D3CF:2A14247E
  expected  444F4D02:44C68897:D9C942B:C567D3CF:2A14247E

Ctrl+F8 to exit CLI focus
```

Fuente: Elaborado por Omar Hernando Rojas García, Configuración de comandos por consola

R3

Figura37. Inicialización y recarga del R3



```
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]
Initializing Hardware ...

Checking for PCIe device presence...done
System integrity status: 0x610
Rom image verified correctly

System Bootstrap, Version 16.7(3z), RELEASE SOFTWARE
Copyright (c) 1994-2018 by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft
Cisco ISR4331/K9 platform with 4194304 Kbytes of main memory

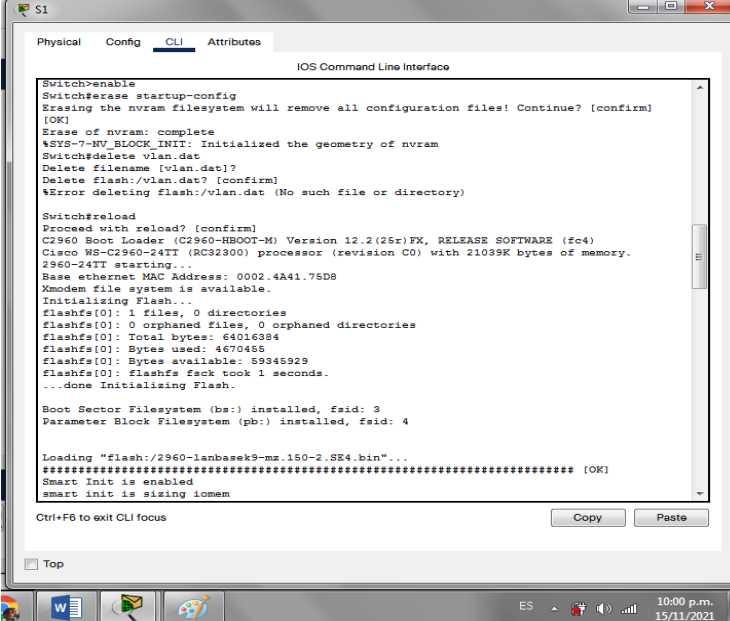
no valid BOOT image found
Final autoboot attempt from default boot device...
Located isr4300-universalk9.16.06.04.SPA.bin
#####
Package header rev 1 structure detected
IsoSize = 560114467
Calculating SHA-1 hash...Validate package: SHA-1 hash:
  calculated 444F4D02:44C68897:D9C942B:C567D3CF:2A14247E
  expected  444F4D02:44C68897:D9C942B:C567D3CF:2A14247E

Ctrl+F8 to exit CLI focus
```

Fuente: Elaborado por Omar Hernando Rojas García, Configuración de comandos por consola

S1

Figura38. Inicialización y recarga del S1



```
Switch>enable
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 0002.4A41.75D8
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4670455
flashfs[0]: Bytes available: 59345929
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

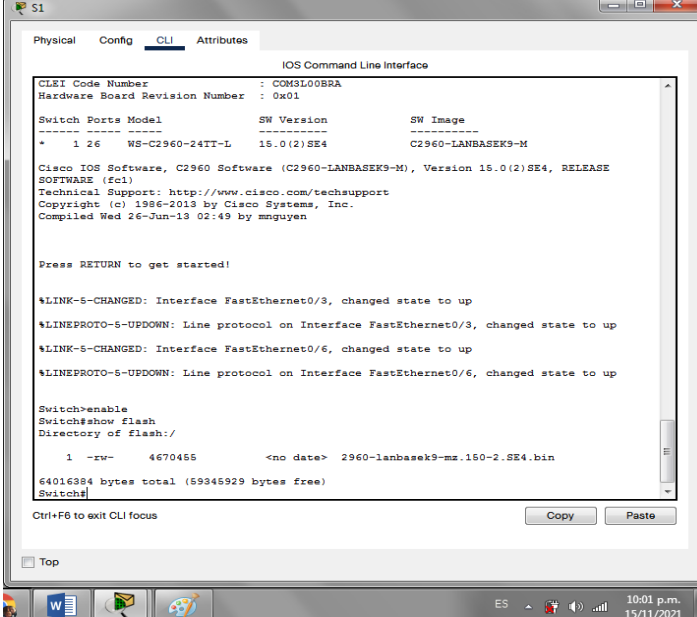
Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4

Loading "flash:/2960-lanbasek9-mz.150-2.SE4.bin"...
***** [OK]
Smart Init is enabled
smart init is sizing iomem

Ctrl+F8 to exit CLI focus
```

Fuente: Elaborado por Omar Hernando Rojas García, Configuración de comandos por consola

Figura39. Verificación de la BD del S1



```
CLEI Code Number : COM3L00BRA
Hardware Board Revision Number : 0x01

Switch Ports Model SW Version SW Image
-----
* 1 26 WS-C2960-24TT-L 15.0(2)SE4 C2960-LANBASEK9-M

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE
SOFTWARE (fzl)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mguyen

Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

Switch#enable
Switch#show flash
Directory of flash:/

 1 -rw- 4670455 <no date> 2960-lanbasek9-mz.150-2.SE4.bin

64016384 bytes total (59345929 bytes free)
Switch#
```

Fuente: Elaborado por Omar Hernando Rojas García, Configuración de comandos por consola

Figura40. Inicialización y recarga del S3

```

Switch>enable
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25c)FX, RELEASE SOFTWARE (fc4)
Cisco WS-C2960-24TT (RCS2300) processor (revision C0) with 21039K bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 0001.637B.EC16
Modem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4670455
flashfs[0]: Bytes available: 59345929
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4

Loading "flash:/2960-lanbasek9-mz.150-2.SE4.bin"...
***** [OK]
Smart Init is enabled
smart init is sizing iomem

Ctrl+F6 to exit CLI focus
  
```

Fuente: Elaborado por Omar Hernando Rojas García, Configuración de comandos por consola

Figura41. Verificación de la BD del S3

```

CLI Code Number      : COM3L00BRA
Hardware Board Revision Number : 0x01

Switch Ports Model          SW Version        SW Image
-----
 1 26 WS-C2960-24TT-L 15.0(2)SE4      C2960-LANBASEK9-M

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen

Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up

Switch>enable
Switch#show flash
Directory of flash:/

 1  -rw-  4670455      <no date>  2960-lanbasek9-mz.150-2.SE4.bin
64016384 bytes total (59345929 bytes free)
Switch#
  
```

Fuente: Elaborado por Omar Hernando Rojas García, Configuración de comandos por consola

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

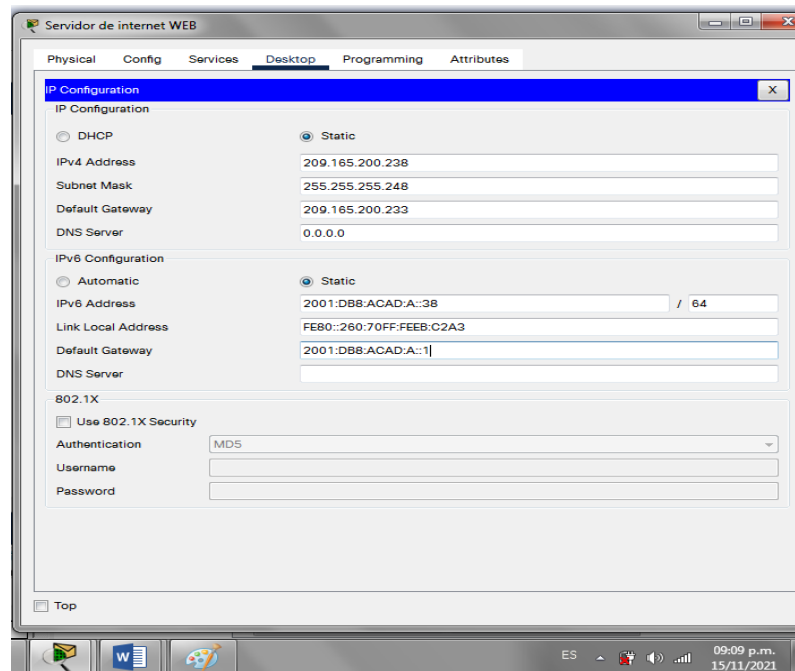
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 7. Tabla de direccionamiento del servidor de internet

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

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.

Figura42. Configuración de Servidor Web



Fuente: Elaborado por Omar Hernando Rojas García, Configuración del servidor web por interfaz grafica

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

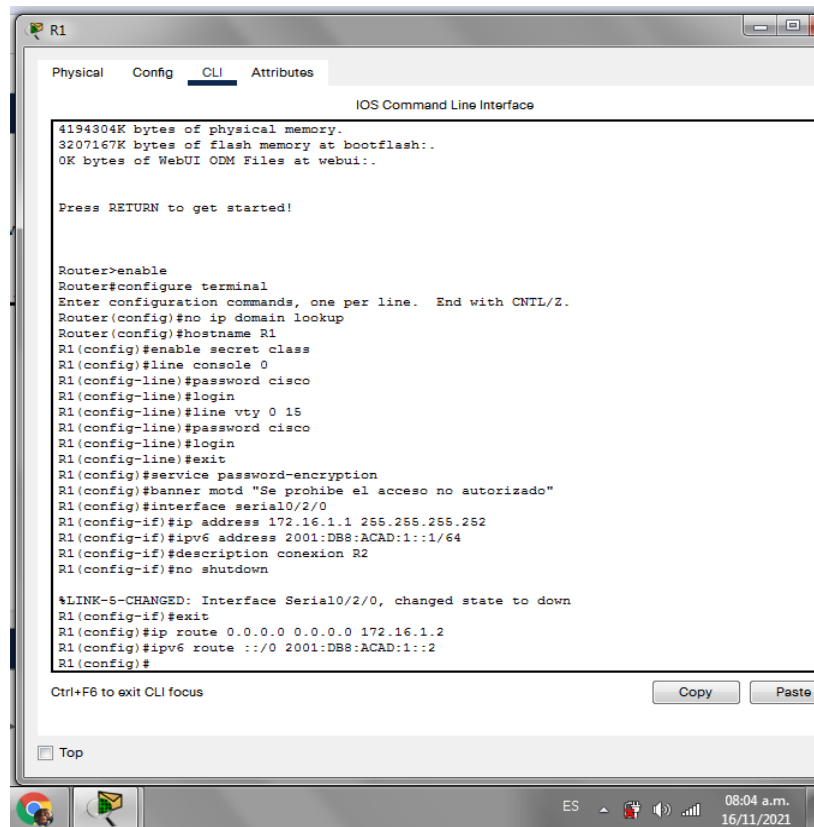
Tabla 8. Comandos para la configuración de R1

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

Nota: Todavía no configure G0/0/1.

Fuente: Elaborado por Omar Hernando Rojas García,

Figura43. Configuración de R1



```
R1
Physical Config CLI Attributes
IOS Command Line Interface
4194304K bytes of physical memory.
3207167K bytes of flash memory at bootflash:.
0K bytes of WebUI ODM Files at webui:.

Press RETURN to get started!

Router>enable
Router#configure terminal
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 "Se prohíbe el acceso no autorizado"
R1(config)#interface serial0/2/0
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64
R1(config-if)#description conexion conexion R2
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/2/0, changed state to down
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2
R1(config)#ipv6 route ::/0 2001:DB8:ACAD:1::2
R1(config)#

Ctrl+F6 to exit CLI focus
Copy Paste
Top
ES 08:04 a.m.
16/11/2021
```

Fuente: Elaborado por Omar Hernando Rojas García, Configuración de R1 por consola CLI

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

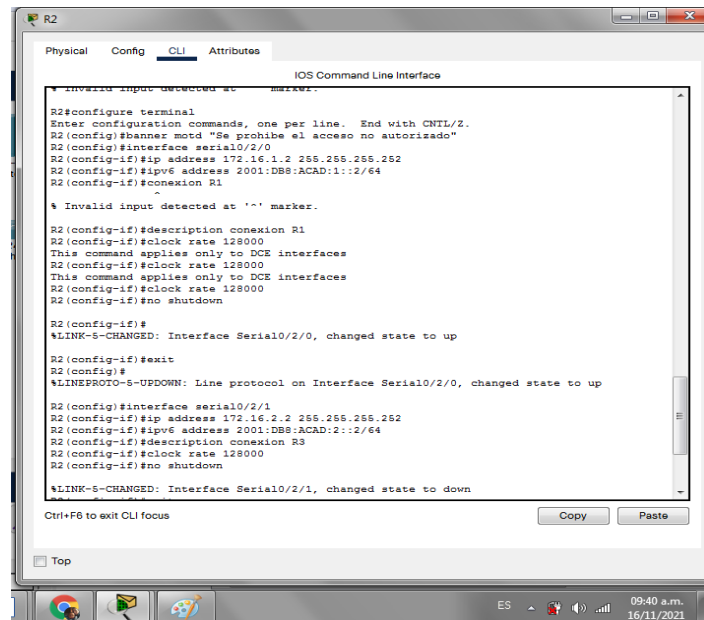
Tabla 9. Comandos para la configuración de R2

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

	<i>R2(config-if)#exit</i>
Interfaz G0/0 /0 (simulación de Internet)	<i>R2(config)#interface gigabitEthernet0/0 R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#description conexion servidor R2(config-if)#no shutdown</i>
Interfaz loopback 0 (servidor web simulado)	<i>R2(config)#interface loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description conexion servidor web R2(config-if)#exit</i>
Ruta predeterminada	<i>R2(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.1 R2(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.1 R2(config)#ipv6 route ::/0 2001:DB8:ACAD:1::1 R2(config)#ipv6 route ::/0 2001:DB8:ACAD:2::1</i>

Fuente: Elaborado por Omar Hernando Rojas García

Figura44. Configuración de R2



Fuente: Elaborado por Omar Hernando Rojas García, Configuración de R2 por consola CLI

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

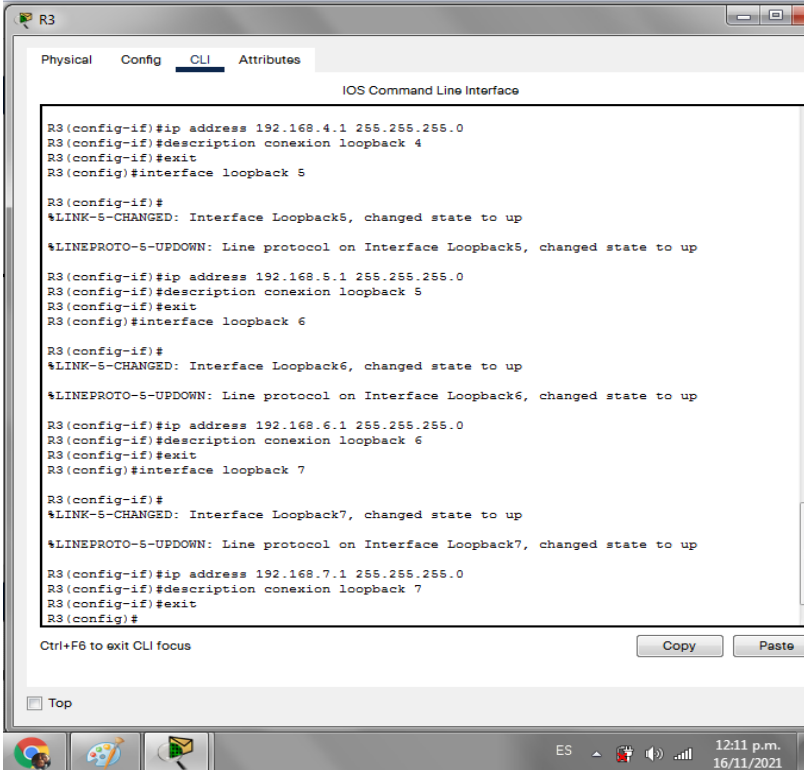
Tabla 10. Comandos para la configuración de R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	<i>Router(config)#no ip domain-lookup</i>
Nombre del router	<i>Router(config)#hostname R3</i>
Contraseña de exec privilegiado cifrada	<i>R3(config)#enable secret class</i>
Contraseña de acceso a la consola	<i>R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login</i>
Contraseña de acceso Telnet	<i>R3(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login</i>
Cifrar las contraseñas de texto no cifrado	<i>R3(config)#service password-encryption</i>

Mensaje MOTD	<i>R3(config)#banner motd "Se prohíbe el acceso no autorizado"</i>
Interfaz S0/2/1	<i>R3(config)#interface serial0/2/1 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#description conexion R2 R3(config-if)#no shutdown</i>
Interfaz loopback 4	<i>R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#description loopback 4 R3(config-if)#exit</i>
Interfaz loopback 5	<i>R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#description loopback 5 R3(config-if)#exit</i>
Interfaz loopback 6	<i>R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#description loopback 6 R3(config-if)#exit</i>
Interfaz loopback 7	<i>R3(config)#interface loopback 7 R3(config-if)#ip address 192.168.7.1 255.255.255.0 R3(config-if)#description loopback 7 R3(config-if)#exit</i>
Rutas predeterminadas	<i>R3(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2 R3(config)# ipv6 route ::/0 2001:DB8:ACAD:2::2</i>

Fuente: Elaborado por Omar Hernando Rojas García

Figura45. Configuración de R3



```
R3
Physical Config CLI Attributes
IOS Command Line Interface

R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#description conexion loopback 4
R3(config-if)#exit
R3(config)#interface 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)#description conexion loopback 5
R3(config-if)#exit
R3(config)#interface 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)#description conexion loopback 6
R3(config-if)#exit
R3(config)#interface 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)#ip address 192.168.7.1 255.255.255.0
R3(config-if)#description conexion loopback 7
R3(config-if)#exit
R3(config)#

Ctrl+F8 to exit CLI focus
Copy Paste
Top
```

Fuente: Elaborado por Omar Hernando Rojas García, Configuración de R3 por consola CLI

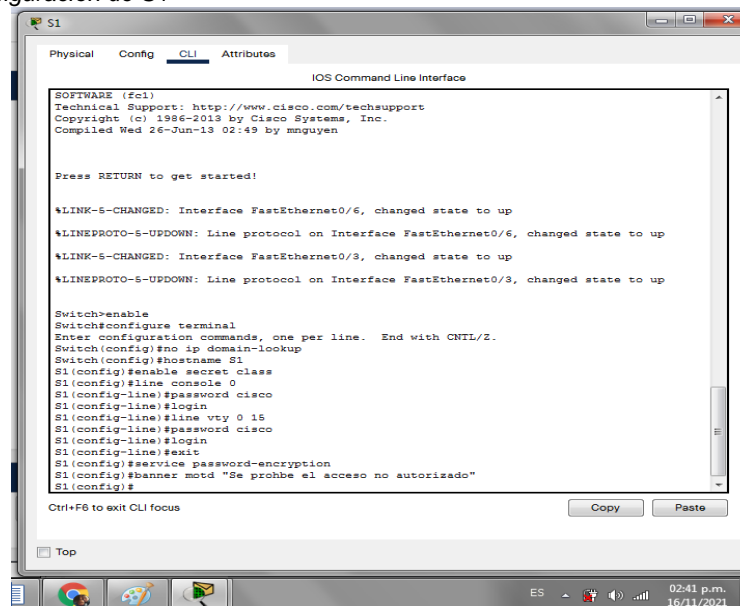
Paso 5: Configurar S1

La configuración de S1 incluye las siguientes tareas:

Tabla 11. Comandos para la configuración de S1

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

Figura46. Configuración de S1



```
SOFTWARE (Scl)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnquyen

Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd "Se prohíbe el acceso no autorizado"
S1(config)#
```

Fuente: Elaborado por Omar Hernando Rojas García, Configuración de S1 por consola CLI

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 12. Comandos para la configuración de S3

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

Figura47. Configuración de S3

```

S3
Physical Config CLI Attributes
IOS Command Line Interface

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

Switch>enable
Switch#configure terminal
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 "Se prohíbe el acceso no autorizado"
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S3#
  
```

Fuente: Elaborado por Omar Hernando Rojas García, Configuración de S3 por consola CLI

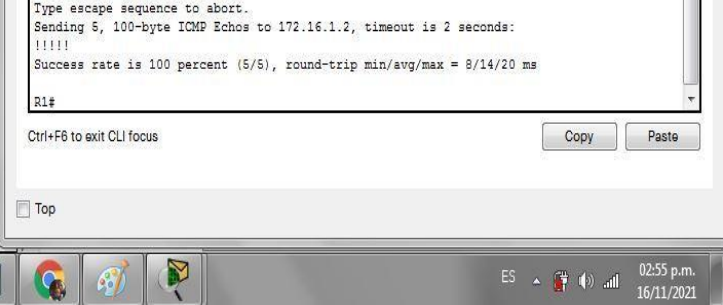
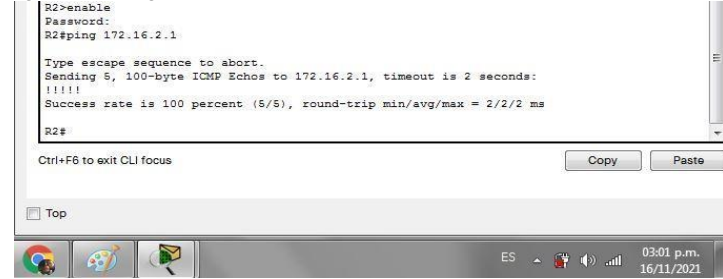
Paso 7: Verificar la conectividad de la red

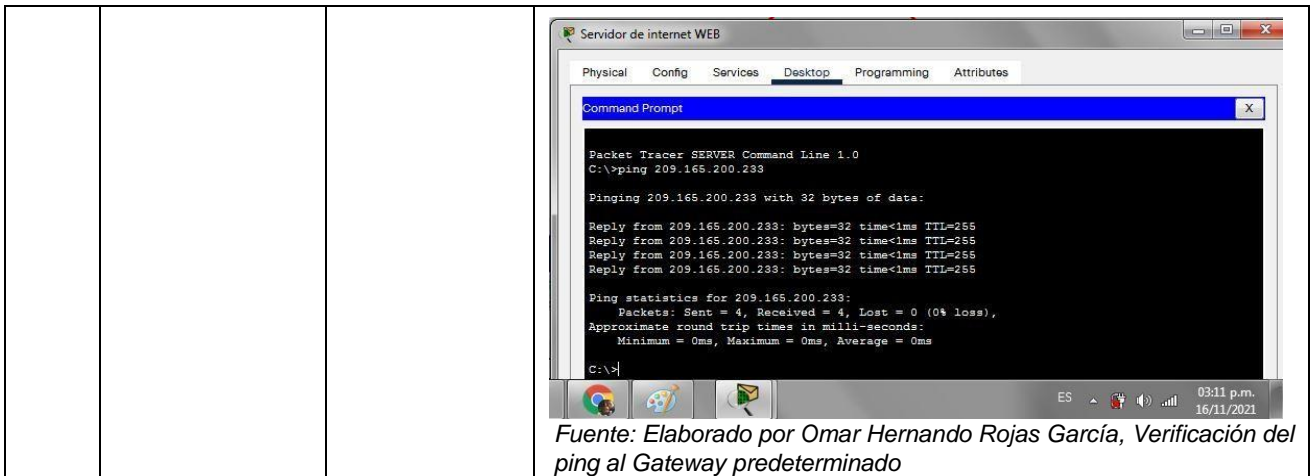
Utilice el comando **ping** para probar la conectividad entre los dispositivos de red.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.

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

Tabla 13. Tabla de resultados prueba de conectividad

Des de	A	Dirección IP	Resultados de ping
R1	R2, S0/2/0	172.16.1.2	<p><u>Correcto</u> <i>Figura48. Ping a S0/2/0</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García, Verificación del ping al puerto solicitado</i></p>
R2	R3, S0/2/1	172.16.2.1	<p><u>Correcto</u> <i>Figura49. Ping a S0/2/1</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García, Verificación del ping al puerto solicitado</i></p>
PC de Internet	Gateway predeterminado	209.165.200.233	<p><u>Correcto</u> <i>Figura50. Ping al Gateway predeterminado</i></p>



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

Figura51. Ping simulado de R1 a R2

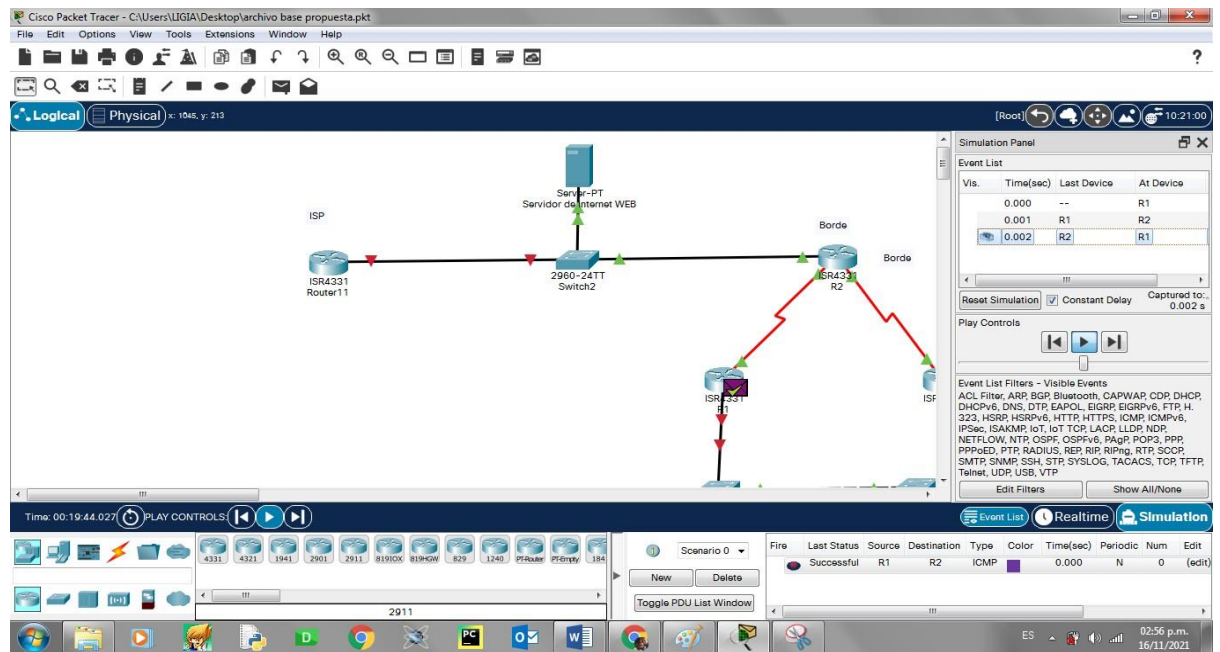
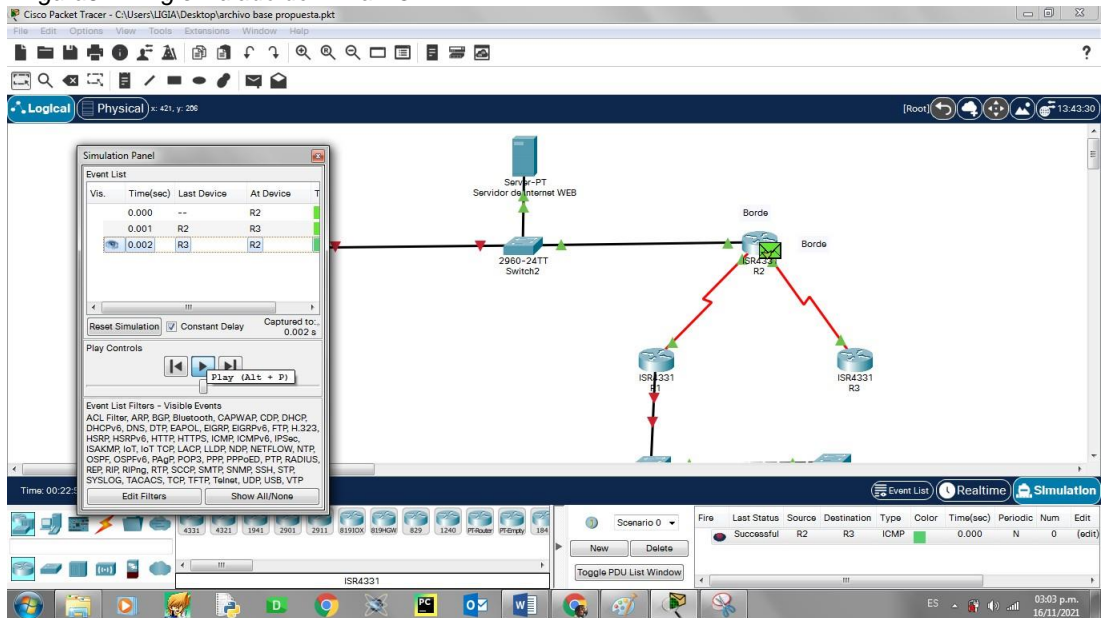
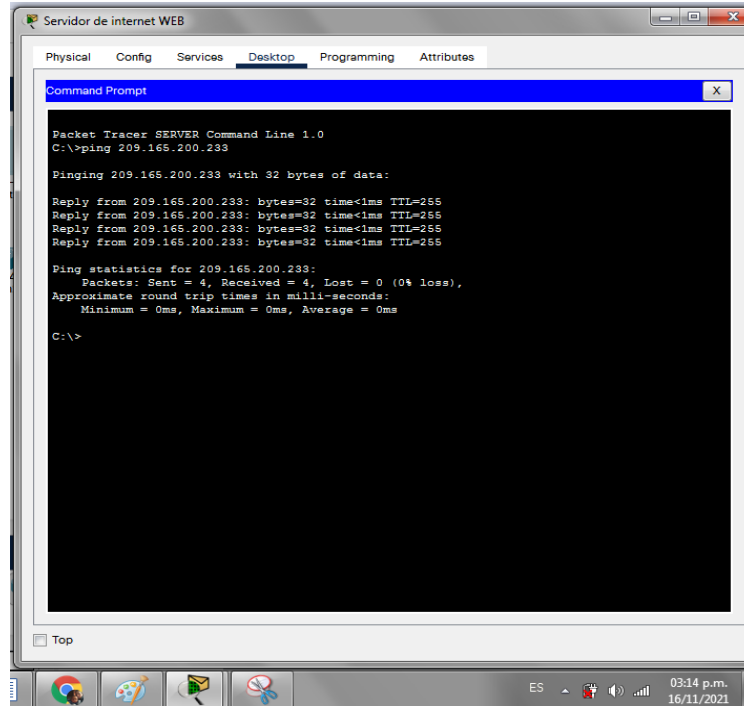


Figura52. Ping simulado de R2 a R3



Fuente: Elaborado por Omar Hernando Rojas García, Verificación de la simulación en Packet Tracer

Figura53. Ping al servidor web



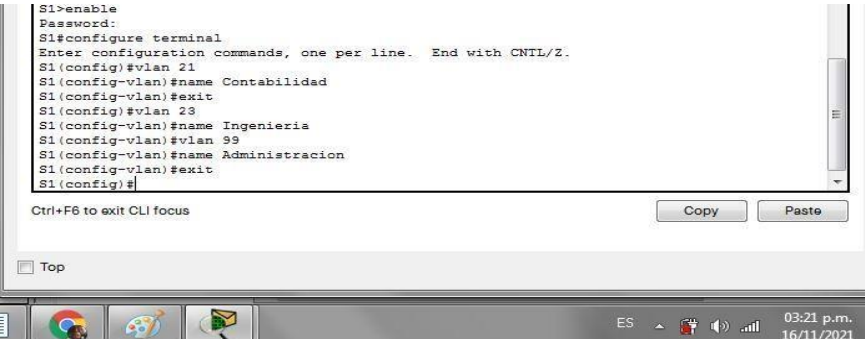
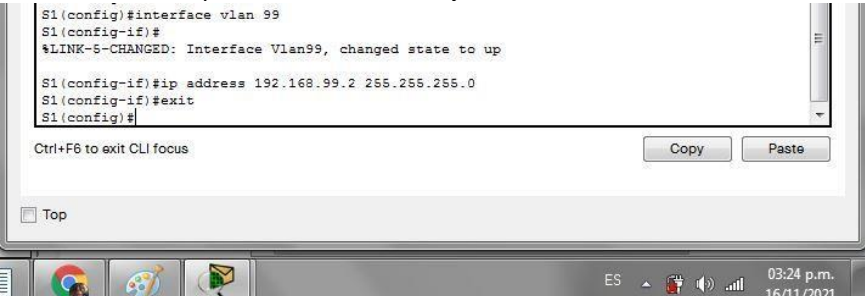
Fuente: Elaborado por Omar Hernando Rojas García, Verificación del ping por command prompt

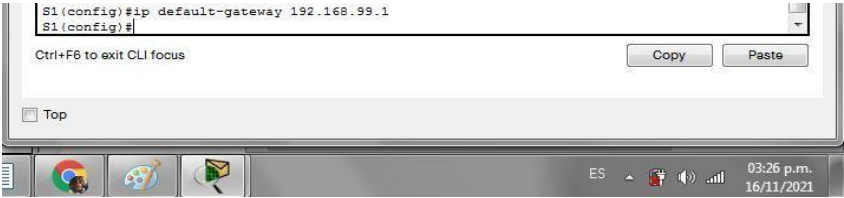
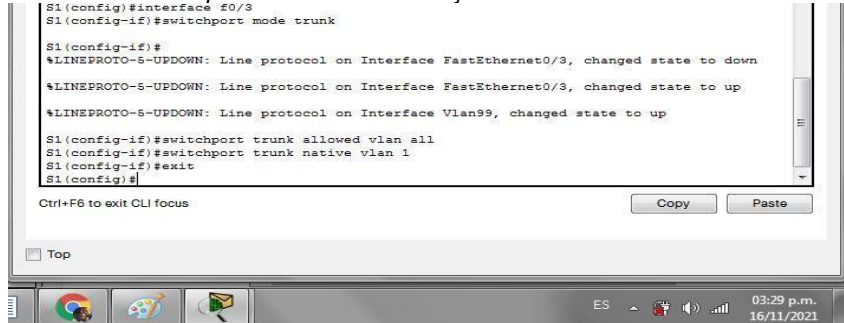
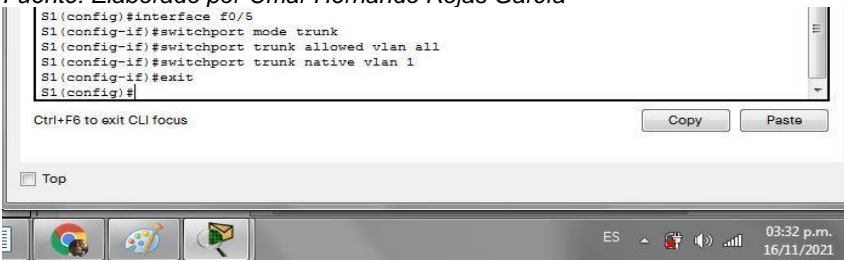
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN

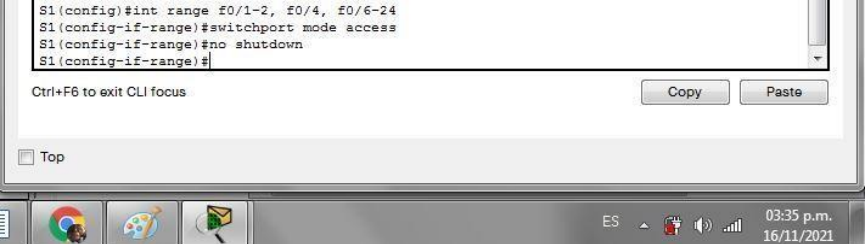
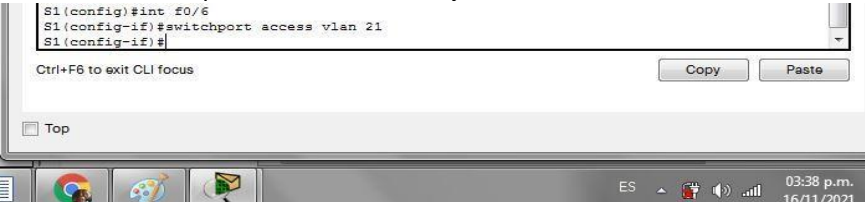
Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 14. Comandos para la configuración de S1

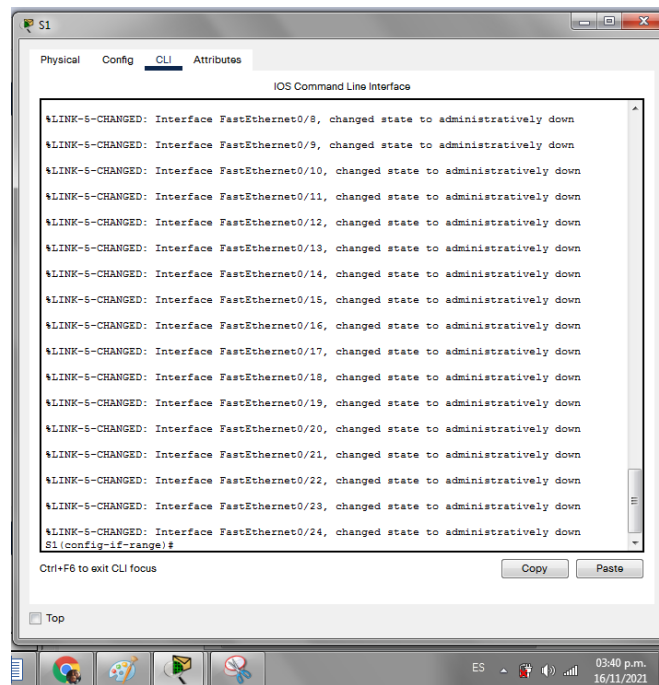
Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	<pre>S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config)#vlan 23 S1(config-vlan)#name Ingenieria S1(config)#vlan 99 S1(config-vlan)#name Administracion</pre> <p><i>Figura54. Creación de una BD de VLAN 21</i> <i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>  <pre>S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#exit S1(config)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit S1(config)#</pre>
Asignar la dirección IP de administración.	<pre>S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#exit</pre> <p><i>Figura55. Asignación de IP de administración</i> <i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>  <pre>S1(config)#interface vlan 99 S1(config-if)# %LINK-S-CHANGED: Interface Vlan99, changed state to up S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#exit S1(config)#</pre>

<p>Asignar el gateway predeterminado</p>	<pre>S1(config)#ip default-gateway 192.168.99.1</pre> <p><i>Figura56. Asignación del Gateway predeterminado</i> Fuente: Elaborado por Omar Hernando Rojas García</p> 
<p>Forzar el enlace troncal en la interfaz F0/3</p>	<pre>S1(config)#interface f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk allowed vlan all S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit</pre> <p><i>Figura57 Troncalización del Puerto F0/3</i> Fuente: Elaborado por Omar Hernando Rojas García</p> 
<p>Forzar el enlace troncal en la interfaz F0/5</p>	<pre>S1(config)#interface f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk allowed vlan all S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit</pre> <p><i>Figura58. Troncalización de la interfaz F0/5</i> Fuente: Elaborado por Omar Hernando Rojas García</p> 

<p>Configurar el resto de los puertos como puertos de acceso</p>	<pre>S1(config)#int range f0/1-2, f0/4, f0/6-24 S1(config-if-range)#switchport mode access S1(config-if-range)#no shutdown</pre> <p><i>Figura59. Configuración de los puertos de acceso</i> Fuente: Elaborado por Omar Hernando Rojas García</p> 
<p>Asignar F0/6 a la VLAN 21</p>	<pre>S1(config)#int f0/6 S1(config-if)#switchport access vlan 21</pre> <p><i>Figura60. Asignación de F0/6 a la VLAN 21</i> Fuente: Elaborado por Omar Hernando Rojas García</p> 
<p>Apagar todos los puertos sin usar</p>	<pre>S1(config)#int range f0/1-2, f0/4, f0/7-24 S1(config-if-range)#shutdown</pre>

Fuente: Elaborado por Omar Hernando Rojas García

Figura61. Inhabilitación de los puertos sin usar en S1

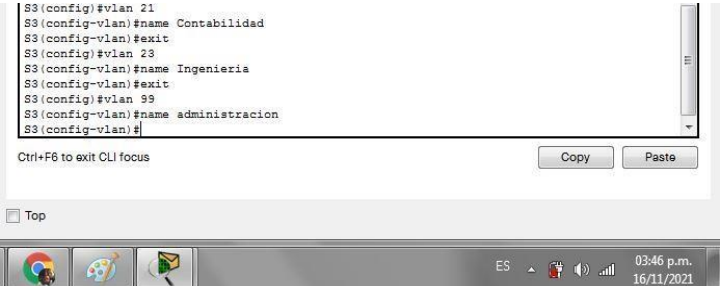
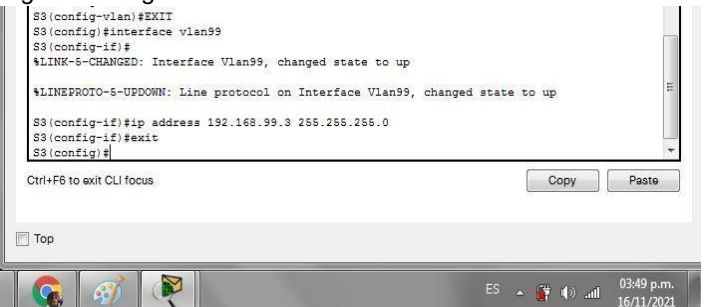


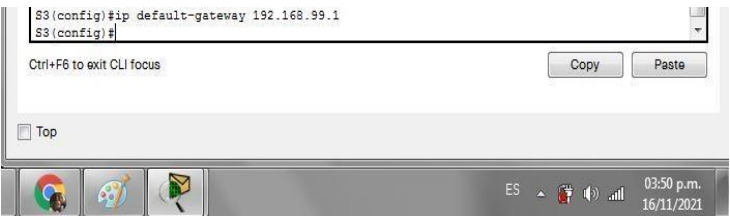
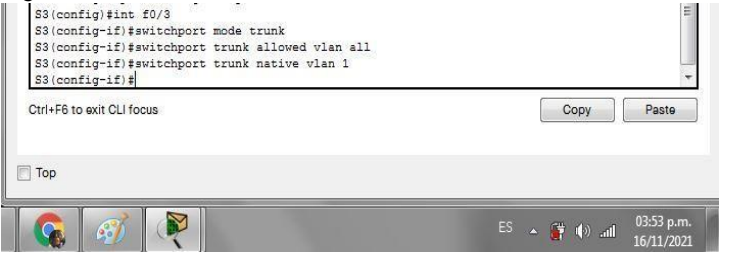
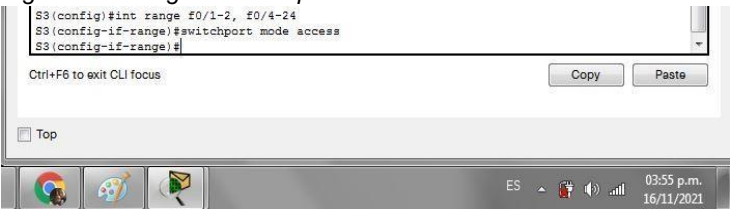

Fuente: Elaborado por Omar Hernando Rojas García, Configuración de S1 por consola CLI

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 15. Comandos para la configuración de S3

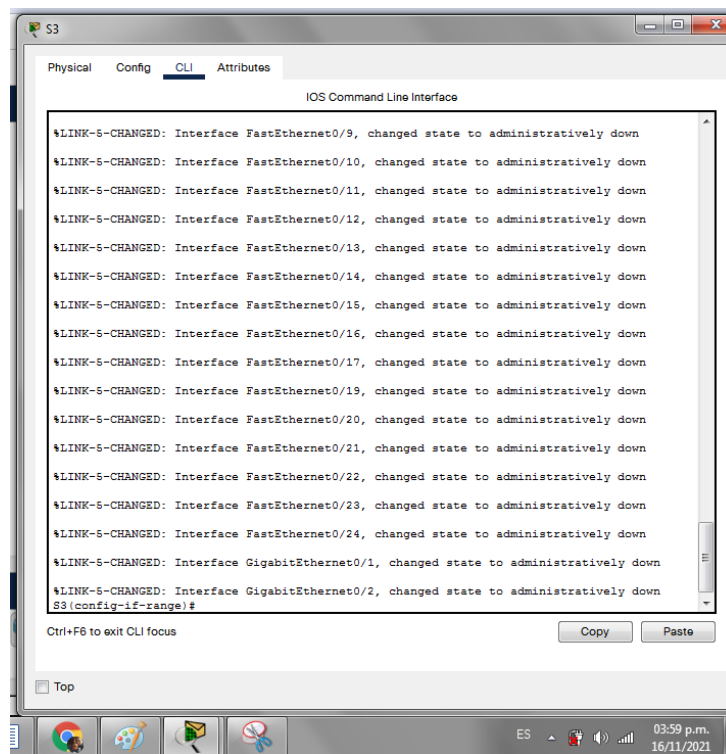
Elemento o tarea de configuración	Especificación
<p>Crear la base de datos de VLAN</p>	<pre>S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#exit S3(config)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#exit S3(config)#vlan 99 S3(config-vlan)#name administracion S3(config-vlan)#</pre> <p><i>Figura62. Creación de una BD de VLAN 23</i></p>  <p>Fuente: Elaborado por Omar Hernando Rojas García</p>
<p>Asignar la dirección IP de administración</p>	<pre>S3(config)#interface vlan99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#exit</pre> <p><i>Figura63. Asignación de IP de administración</i></p>  <p>Fuente: Elaborado por Omar Hernando Rojas García</p>
<p>Asignar el gateway predeterminado.</p>	<pre>S3(config)#ip default-gateway 192.168.99.1</pre> <p><i>Figura64. Asignación del Gateway predeterminado</i></p>

	 <p>Fuente: Elaborado por Omar Hernando Rojas García</p>
<p>Forzar el enlace troncal en la interfaz F0/3</p>	<pre>S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk allowed vlan all S3(config-if)#switchport trunk native vlan 1</pre> <p><i>Figura65. Troncalización del Puerto F0/3</i></p>  <p>Fuente: Elaborado por Omar Hernando Rojas García</p>
<p>Configurar el resto de los puertos como puertos de acceso</p>	<pre>S3(config)#int range f0/1-2, f0/4-24 S3(config-if-range)#switchport mode access</pre> <p><i>Figura66. Configuración de puertos de acceso</i></p>  <p>Fuente: Elaborado por Omar Hernando Rojas García</p>
<p>Asignar F0/18 a la VLAN 23</p>	<pre>S3(config)#int f0/18 S3(config-if)#switchport access vlan 23</pre> <p><i>Figura67. Asignación de F0/18 a VLAN 23</i></p>  <p>Fuente: Elaborado por Omar Hernando Rojas García</p>

Apagar todos los puertos
sin usar

```
S3(config)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2  
S3(config-if-range)#shutdown
```

Figura68. Inhabilitación de los puertos sin usar en S3

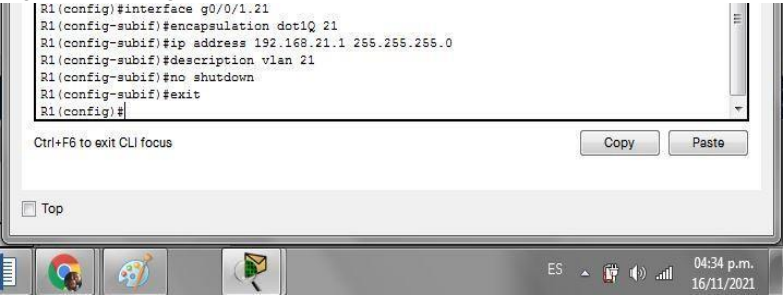


Fuente: Elaborado por Omar Hernando Rojas García, Configuración de S3 por consola CLI

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16. Comandos para la configuración de R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/0/1	<pre>R1(config)#interface g0/0/1.21 R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#description vlan 21 R1(config-subif)#no shutdown R1(config-subif)#exit</pre> <p><i>Figura69. Configuración subinterfaz 802.1Q.21 en G0/0/1</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>
Configurar la subinterfaz 802.1Q .23 en G0/0/1	<pre>R1(config)#interface gigabitEthernet0/0/1.23 R1(config-subif)#encapsulation dot1Q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#description vlan 23 R1(config-subif)#no shutdown R1(config-subif)#exit</pre> <p><i>Figura70. Configuración subinterfaz 802.1Q.23 en G0/0/1</i></p>

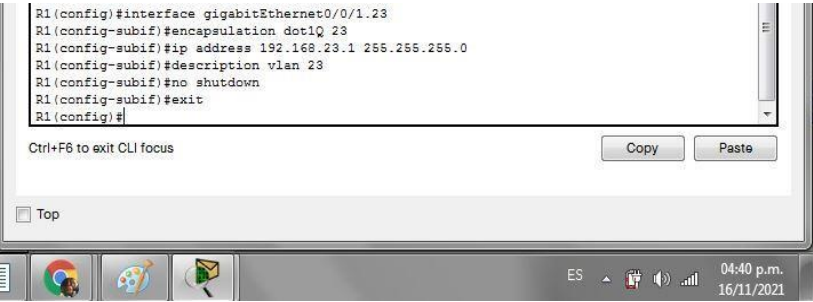
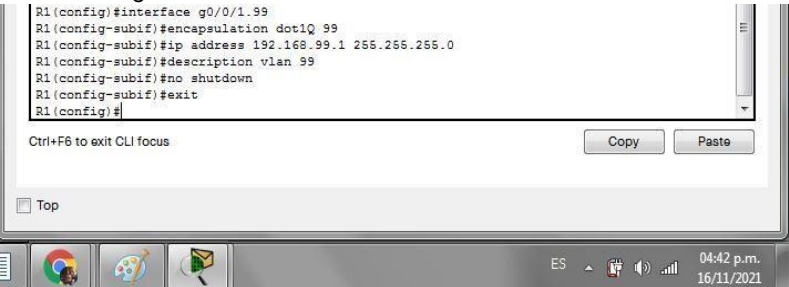
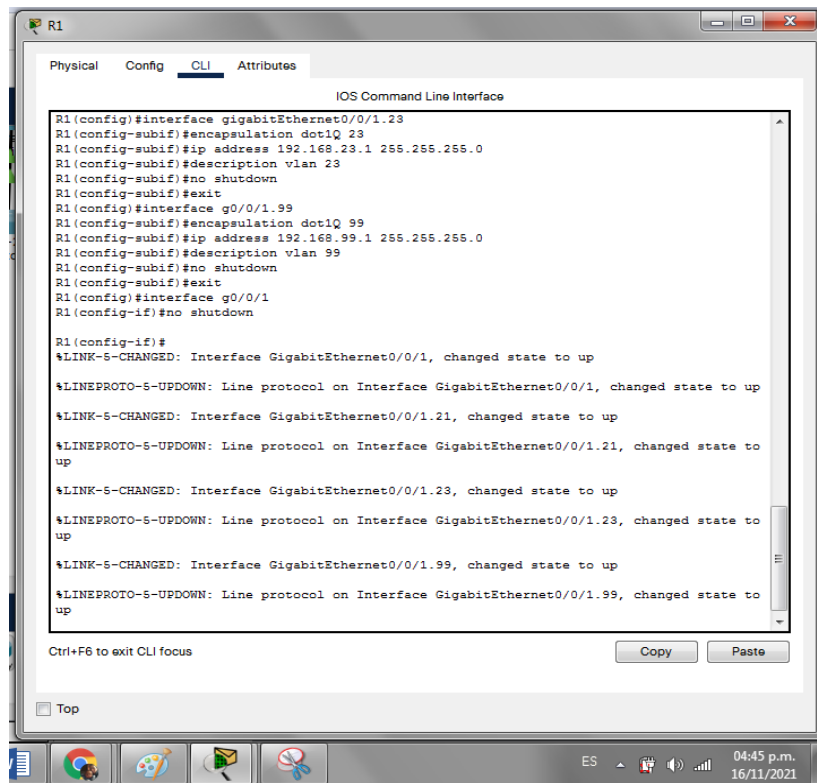
	 <p>Fuente: Elaborado por Omar Hernando Rojas García</p>
<p>Configurar la subinterfaz 802.1Q .99 en G0/1</p>	<pre>R1(config)#interface g0/0/1.99 R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#description vlan 99 R1(config-subif)#no shutdown R1(config-subif)#exit</pre> <p><i>Figura71. Configuración subinterfaz 802.1Q.99 en G0/0/1</i></p>  <p>Fuente: Elaborado por Omar Hernando Rojas García</p>
<p>Activar la interfaz G0/0/1</p>	<pre>R1(config)#interface g0/0/1 R1(config-if)#no shutdown</pre>

Figura72. Activación de la interfaz G0/0/1



```
R1
Physical Config CLI Attributes
IOS Command Line Interface
R1(config)#interface gigabitEthernet0/0/1.23
R1(config-subif)#encapsulation dot1Q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#description vlan 23
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#interface g0/0/1.99
R1(config-subif)#encapsulation dot1Q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#description vlan 99
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#interface g0/0/1
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
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.21, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.21, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.23, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.23, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.99, changed state to up

Ctrl+F6 to exit CLI focus
Copy Paste
Top
```

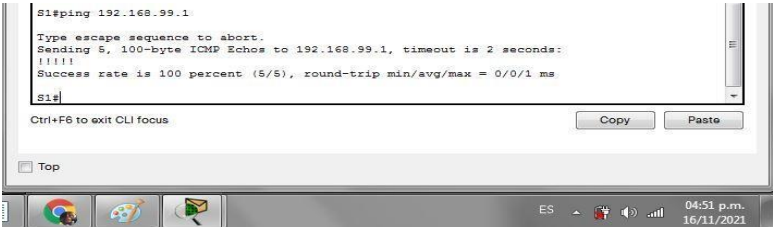
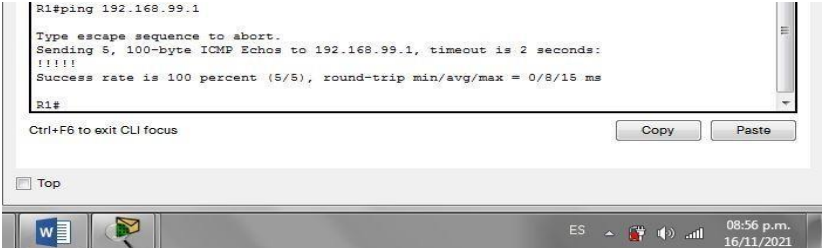
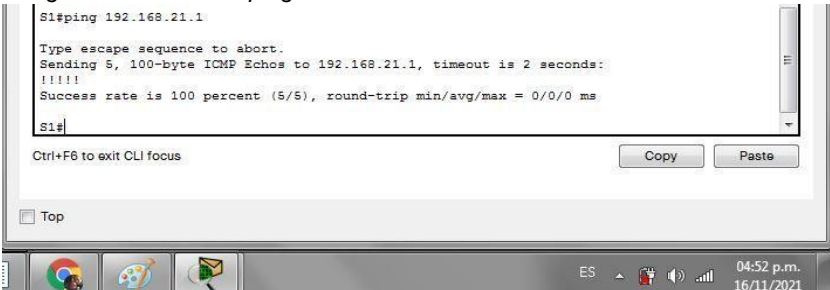
Fuente: Elaborado por Omar Hernando Rojas García, Configuración de S3 por consola CLI

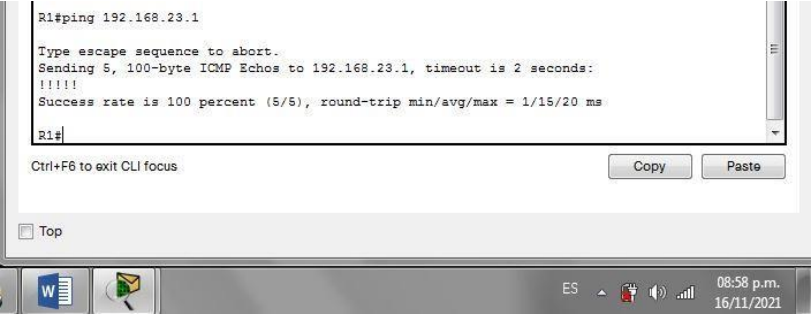
Paso 4: Verificar la conectividad de la red

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

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

Tabla 17. Tabla de resultados prueba de conectividad

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	<p>Positivo <i>Figura73. Resultado ping desde S1 a la VLAN 99</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>
S3	R1, dirección VLAN 99	192.168.99.1	<p>Positivo <i>Figura74. Resultado ping desde S3 a la VLAN 99</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>
S1	R1, dirección VLAN 21	192.168.21.1	<p>Positivo <i>Figura75. Resultado ping desde S1 a la VLAN 21</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>

S3	R1, dirección VLAN 23	192.168.23.1	<p>Positivo <i>Figura76. Resultado ping desde S3 a la VLAN 23</i></p>  <pre>R1#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 = 1/15/20 ms R1#</pre> <p>Ctrl+F6 to exit CLI focus</p> <p>Copy Paste</p> <p>Top</p> <p>ES 08:58 p.m. 16/11/2021</p>
----	-----------------------------	--------------	--

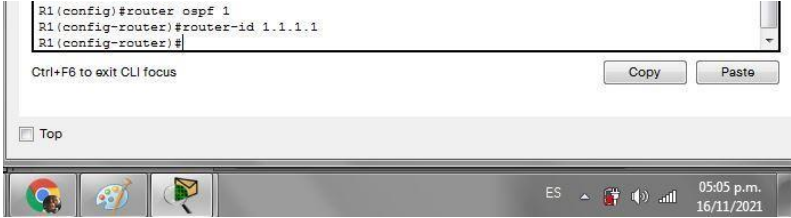
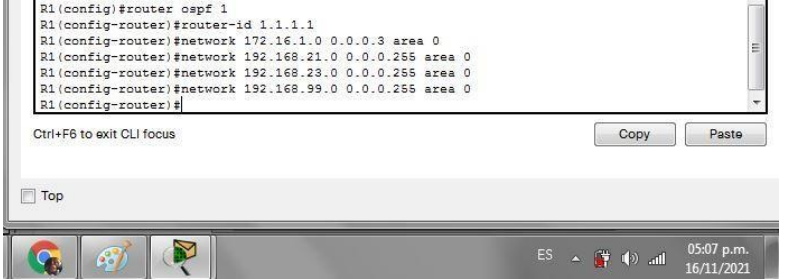
Fuente: Elaborado por Omar Hernando Rojas García

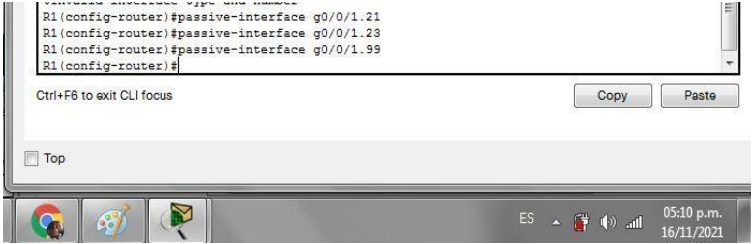
Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

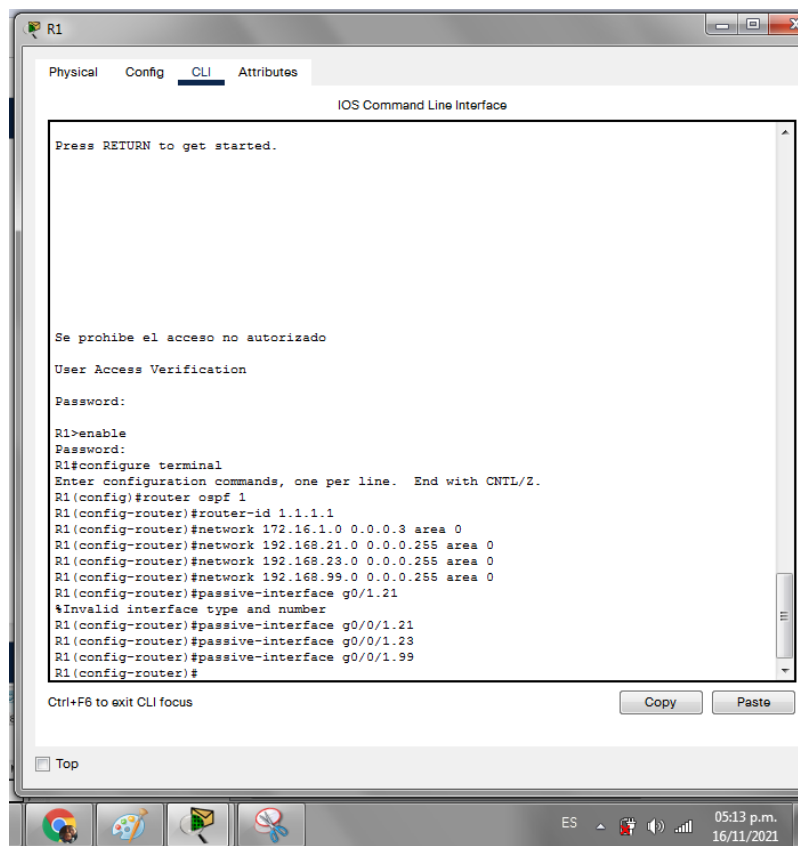
Tabla 18. Tabla de conexión OPSF en R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	<pre>R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1</pre> <p><i>Figura77. Configuración de OSPF en área 0 del R1</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>
Anunciar las redes conectadas directamente	<pre>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</pre> <p><i>Figura78. Configuración de redes conectadas directamente</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>
Establecer todas las interfaces LAN como pasivas	<pre>R1(config-router)#passive-interface g0/0/1.21 R1(config-router)#passive-interface g0/0/1.23 R1(config-router)#passive-interface g0/0/1.99</pre>

	<p><i>Figura79. Establecimiento de interfaces LAN como pasivas</i></p>  <p>Fuente: Elaborado por Omar Hernando Rojas García</p>
<p>Desactive la sumarización automática</p>	<p>N.A</p>

Fuente: Elaborado por Omar Hernando Rojas García

Figura80. Desactivación de la sumarización automática

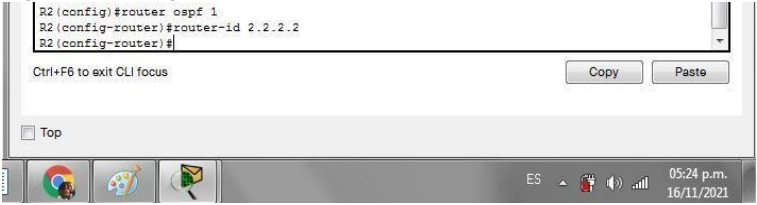
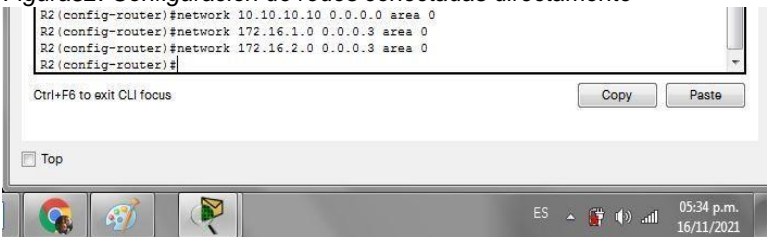



Fuente: Elaborado por Omar Hernando Rojas García, Desactivación de la sumarización por consola CLI

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

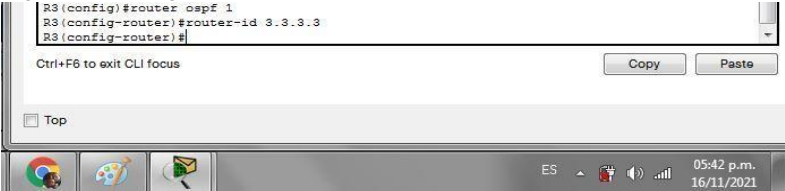
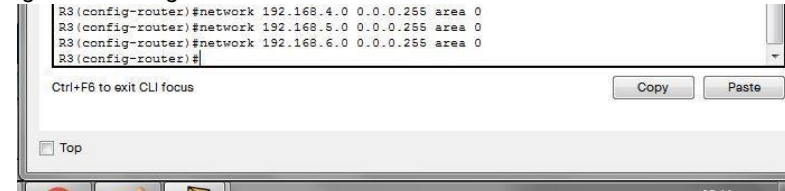
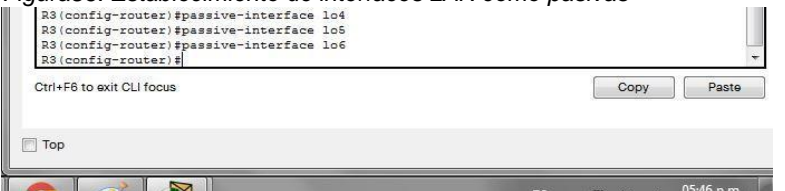
Tabla 19. Tabla de conexión OPSF en R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	<pre>R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2</pre> <p><i>Figura81. Configuración de OSPF en área 0 del R2</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>
Anunciar las redes conectadas directamente	<pre>R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0</pre> <p><i>Figura82. Configuración de redes conectadas directamente</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>
Establecer la interfaz LAN (loopback) como pasiva	<pre>R2(config-router)#passive-interface lo0</pre> <p><i>Figura83. Establecimiento de interfaces LAN como pasivas</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>
Desactive la summarización automática.	N.A

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 20. Tabla de conexión OPSF en R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	<p><i>R3(config)#router ospf 1</i> <i>R3(config-router)#router-id 3.3.3.3</i></p> <p><i>Figura84. Configuración de OSPF en área 0 del R3</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>
Anunciar redes IPv4 conectadas directamente	<p><i>R3(config-router)#network 192.168.4.0 0.0.0.255 area 0</i> <i>R3(config-router)#network 192.168.5.0 0.0.0.255 area 0</i> <i>R3(config-router)#network 192.168.6.0 0.0.0.255 area 0</i></p> <p><i>Figura85. Configuración de redes conectadas directamente</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	<p><i>R3(config-router)#passive-interface lo4</i> <i>R3(config-router)#passive-interface lo5</i> <i>R3(config-router)#passive-interface lo6</i></p> <p><i>Figura86. Establecimiento de interfaces LAN como pasivas</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>

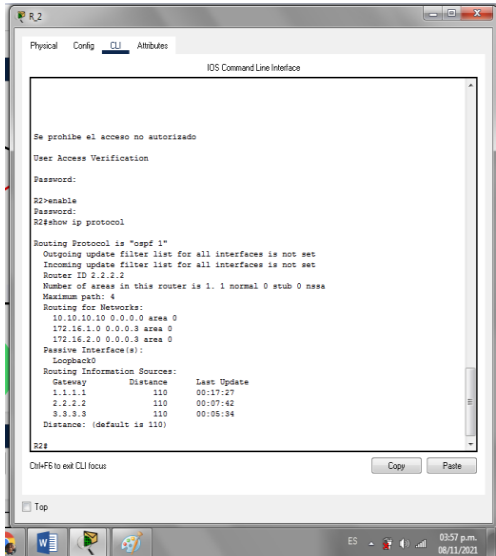
Desactive la sumarización automática.	N.A
---	-----

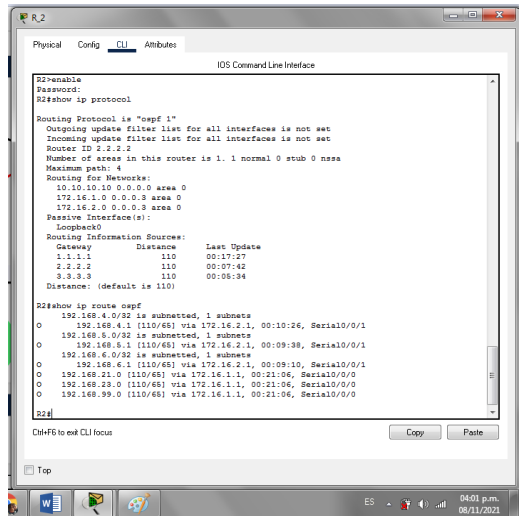
Fuente: Elaborado por Omar Hernando Rojas García,

Paso 4: Verificar la información de OSPF

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

Tabla 21. Tabla de verificación de resultados 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?	<p>Show ip protocol</p> <p><i>Figura87. Resultado del comando show ip protocol</i></p>  <pre> R2# Physical Config CLI Attributes IOS Command Line Interface Se prohíbe el acceso no autorizado User Access Verification Password: R2#enable Password: R2#show ip protocol Routing Protocol is "ospf 1" Outgoing update filter list for all interfaces is not set Incoming update filter list for all interfaces is not set Router ID 2.2.2.2 Number of areas in this router is 1. 1 normal 0 stub 0 nssa Maximum path: 4 Routing for Networks: 10.10.10.0 0.0.0.0 area 0 172.16.1.0 0.0.0.0 area 0 172.16.2.0 0.0.0.0 area 0 Passive Interface(s): Loopback0 Routing Information Sources: Gateway Distance Last Update 1.1.1.1 110 00:17:27 2.2.2.2 110 00:17:42 3.3.3.3 110 00:18:34 Distance: (default is 110) R2# </pre> <p>Fuente: Elaborado por Omar Hernando Rojas García,</p>
¿Qué comando muestra solo las rutas OSPF?	<p>Show ip route ospf</p> <p><i>Figura88 Resultado del comando show ip route OSPF</i></p>

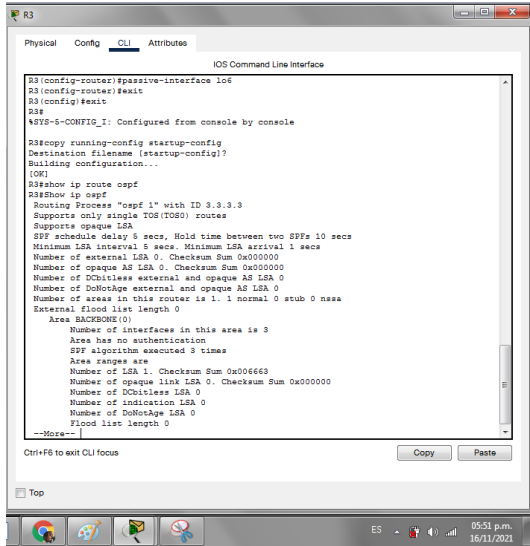


Fuente: Elaborado por Omar Hernando Rojas García,

¿Qué comando muestra la sección de OSPF de la configuración en ejecución?

Show ip ospf

Figura89. Resultado del comando show ip OSPF



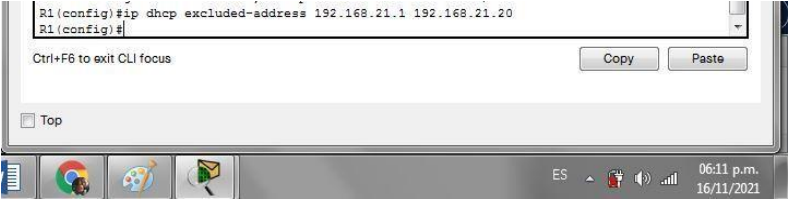
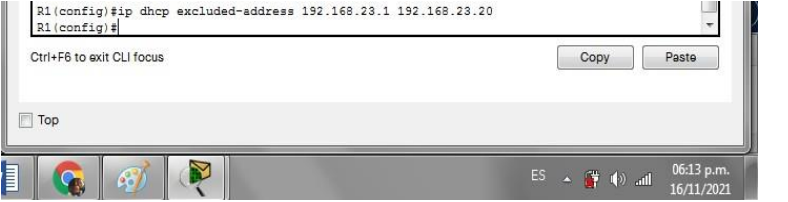
Fuente: Elaborado por Omar Hernando Rojas García,


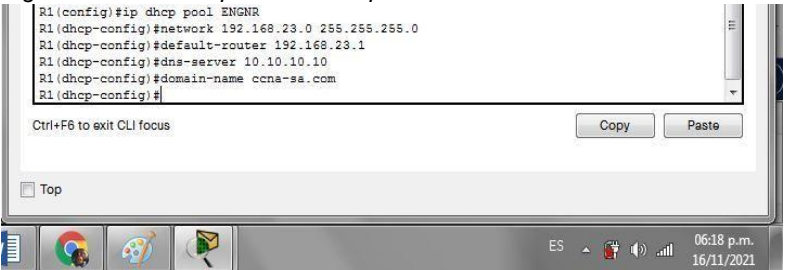
Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22. Tabla de configuración de R1 como servidor 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	<p><i>R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20</i></p> <p><i>Figura90. Comando de reserva para la configuración de VALN estáticas 21</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	<p><i>R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20</i></p> <p><i>Figura91. Comando de reserva para la configuración de VALN estáticas 23</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>
Crear un pool de DHCP para la VLAN 21.	<p><i>R1(config)#ip dhcp pool ACCT</i> <i>R1(dhcp-config)#network 192.168.21.0 255.255.255.0</i> <i>R1(dhcp-config)#default-router 192.168.21.1</i> <i>R1(dhcp-config)#dns-server 10.10.10.10</i> <i>R1(dhcp-config)#domain-name ccna-sa.com</i></p> <p><i>Figura92. Comando para crear un pool de DHCP en VLAN 21</i></p>

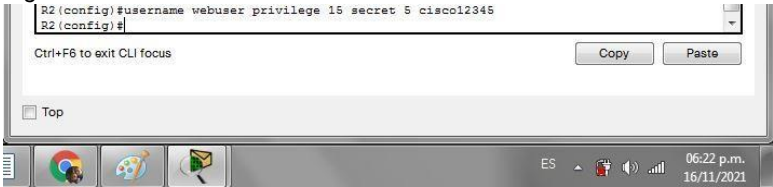
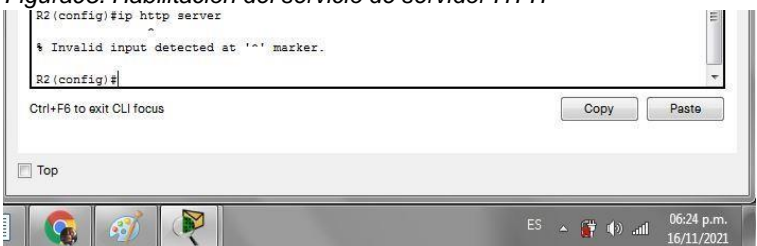
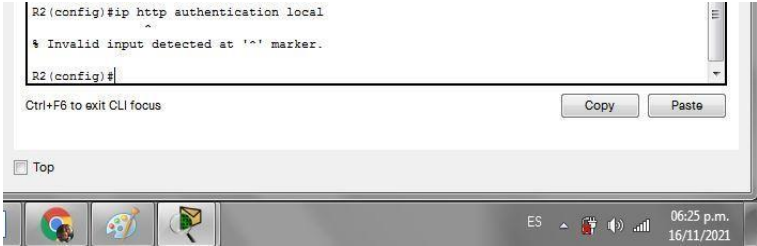
	 <p>Fuente: Elaborado por Omar Hernando Rojas García</p>
<p>Crear un pool de DHCP para la VLAN 23</p>	<pre>R1(config)#ip dhcp pool ENGR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com</pre> <p><i>Figura93. Comando para crear un pool de DHCP en VLAN 23</i></p>  <p>Fuente: Elaborado por Omar Hernando Rojas García</p>

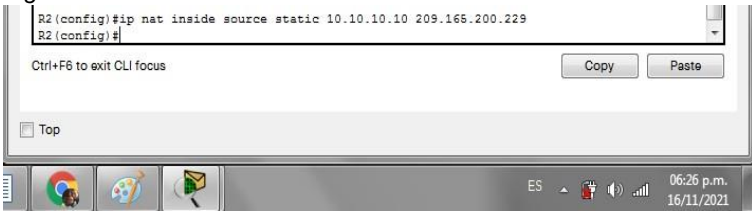
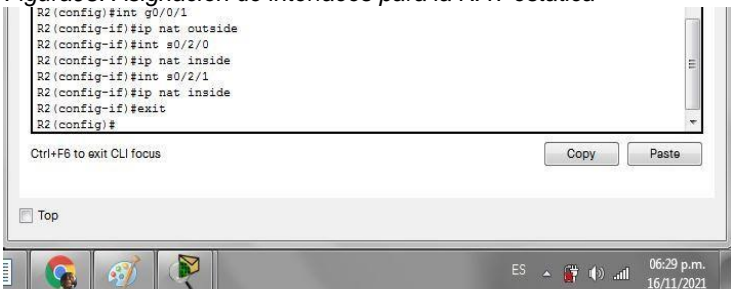
Fuente: Elaborado por Omar Hernando Rojas García

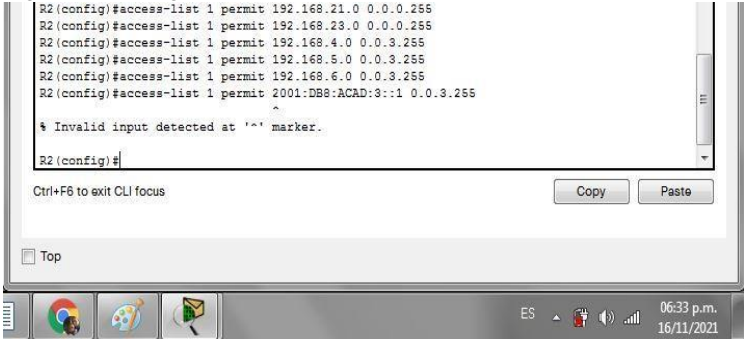
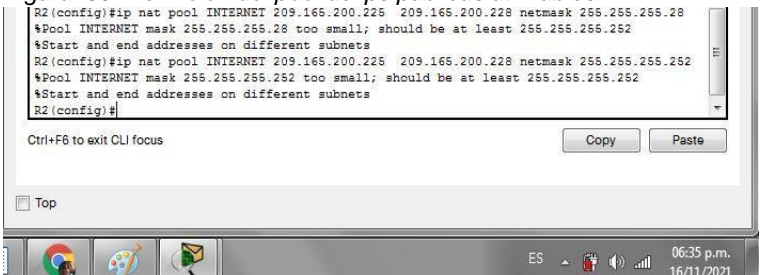
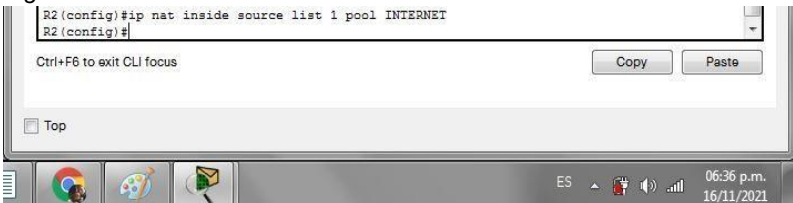
Paso 2: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 23. Tabla de configuración de NAT estática y dinámica en R2

Elemento o tarea de configuración	Especificación
<p>Crear una base de datos local con una cuenta de usuario</p>	<p>Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15 R2(config)#username webuser privilege 15 secret 5 cisco12345</p> <p><i>Figura94. Creación de BD local con cuenta de usuario</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>
<p>Habilitar el servicio del servidor HTTP</p>	<p>R2(config)#ip http server</p> <p><i>Figura95. Habilitación del servicio de servidor HTTP</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>
<p>Configurar el servidor HTTP para utilizar la base de datos local para la autenticación</p>	<p>R2(config)#ip http authentication local</p> <p><i>Figura96. Configuración de HTTP para la autenticación en la BD local</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>

<p>Crear una NAT estática al servidor web.</p>	<p>Dirección global interna: 209.165.200.229 <code>R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229</code></p> <p><i>Figura97. Creación de una NAT estática en el servidor web</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>
<p>Asignar la interfaz interna y externa para la NAT estática</p>	<pre>R2(config)#int g0/0/1 R2(config)#ip nat outside R2(config)#int s0/2/0 R2(config)#ip nat inside R2(config)#int s0/2/1 R2(config)#ip nat inside R2(config)#exit</pre> <p><i>Figura98. Asignación de interfaces para la NAT estática</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>
<p>Configurar la NAT dinámica dentro de una ACL privada</p>	<p>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</p> <pre>R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255 R2(config)#access-list 1 permit 192.168.5.0 0.0.3.255 R2(config)#access-list 1 permit 192.168.6.0 0.0.3.255 R2(config)#access-list 1 permit 2001:DB8:ACAD:3::1 0.0.3.255</pre>

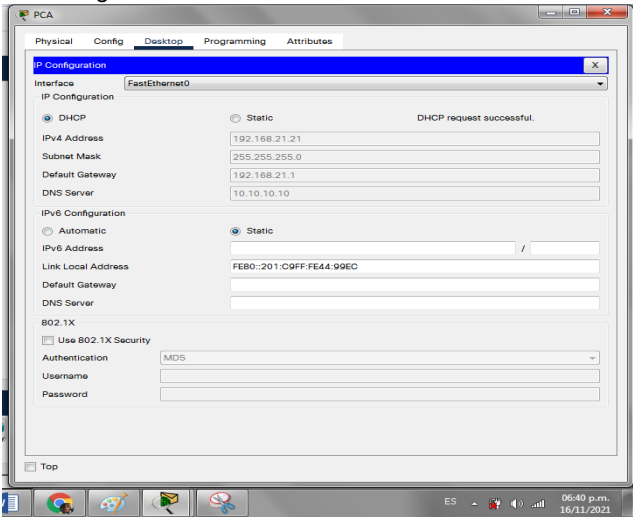
	<p><i>Figura99. Configuración de la NAT dinámica dentro de la ACL privada</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>
<p>Defina el pool de direcciones IP públicas utilizables.</p>	<p>Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228 <i>R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.28</i></p> <p><i>Figura100. Definición del pool de ips publicas utilizables</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas Garcí</i></p>
<p>Definir la traducción de NAT dinámica</p>	<p><i>R2(config)#ip nat inside source list 1 pool INTERNET</i></p> <p><i>Figura101. Definición de la traducción de NAT dinámica</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>

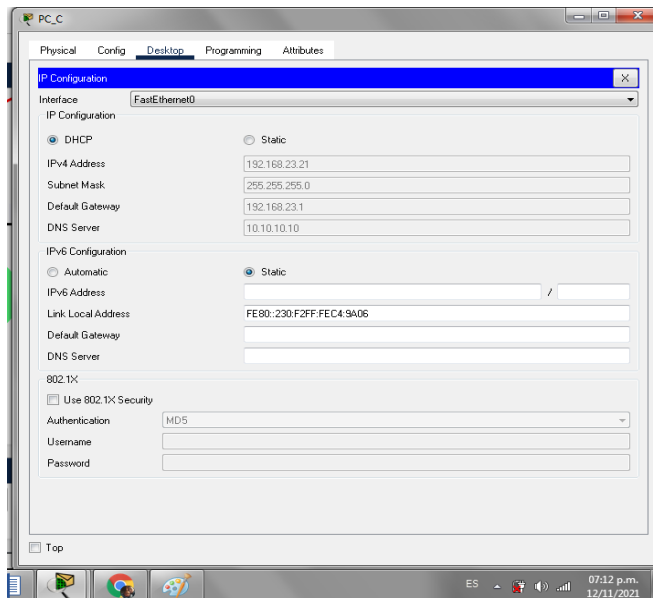
Fuente: Elaborado por Omar Hernando Rojas García

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 24. Tabla de verificación del protocolo DHCP y la NAT estática

Prueba	Resultados
<p>Verificar que la PC-A haya adquirido información de IP del servidor de DHCP</p>	<p><i>Figura102. Asignación de DHCP a PC_A</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García. Asignación de DHCP</i></p>
<p>Verificar que la PC-C haya adquirido información de IP del servidor de DHCP</p>	<p><i>Figura1023 Asignación de DHCP a PC_C</i></p>

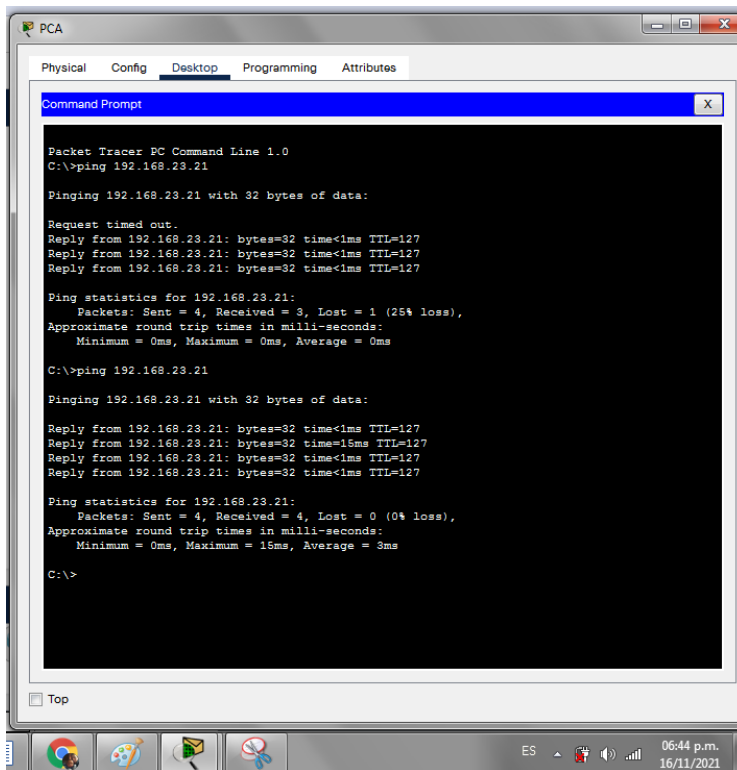


Fuente: Elaborado por Omar Hernando Rojas García. Asignación de DHCP a PC_C

Verificar que la PC-A pueda hacer ping a la PC-C

Nota: Quizá sea necesario deshabilitar el firewall de la PC.

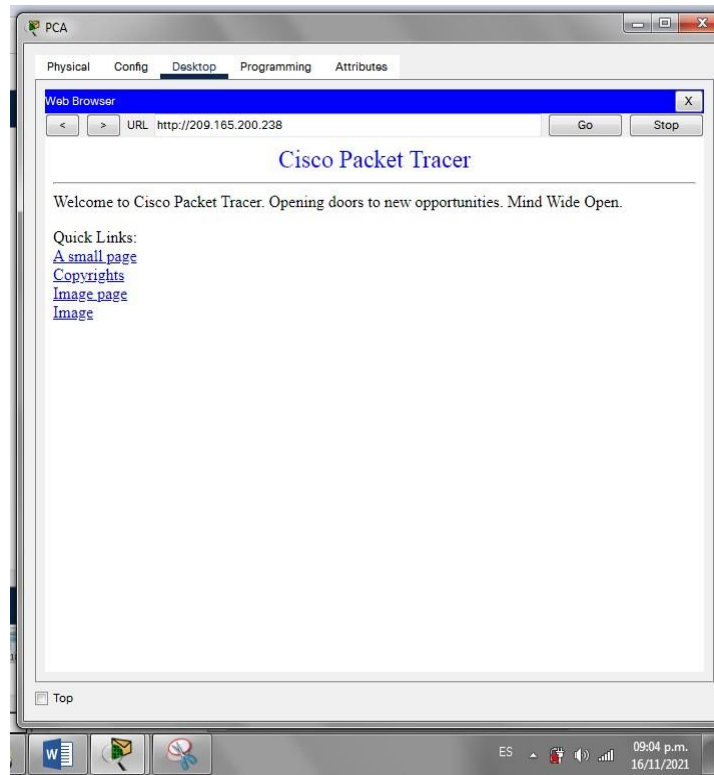
Figura104 Ping de PC_A a PC_C



Fuente: Elaborado por Omar Hernando Rojas García. Comprobación del ping realizado entre PC_A y PC_C

Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.238) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**

Figura105. Accesibilidad de PC_A a internet



Fuente: Elaborado por Omar Hernando Rojas García. Comprobación de accesibilidad de PC_A a internet

Fuente: Elaborado por Omar Hernando Rojas García

Parte 6: Configurar NTP

Tabla 25. Tabla de configuración de NTP

Elemento o tarea de configuración	Especificación
<p>Ajuste la fecha y hora en R2.</p>	<p><i>R2#clock set 09:00:00 05 march 2016</i></p> <p><i>Figura106. Ajuste de fecha y hora en R2</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García.</i></p>
<p>Configure R2 como un maestro NTP.</p>	<p><i>R2(config)#ntp master 5</i></p> <p><i>Figura107. Configuración de NTP como maestro</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García.</i></p>
<p>Configurar R1 como un cliente NTP.</p>	<p><i>R1(config)#ntp server 172.16.1.2</i></p> <p><i>Figura108. Configuración de R1 como un cliente NTP</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>
<p>Configure R1 para actualizaciones de calendario periódicas con hora NTP.</p>	<p><i>R1(config)#ntp update-calendar</i></p> <p><i>Figura109. Configuración de R1 para actualizaciones periódicas</i></p>

R1(config)#ntp update-calendar
R1(config)#

Ctrl+F6 to exit CLI focus

Copy Paste

Top

ES 07:11 p.m.
16/11/2021

Fuente: Elaborado por Omar Hernando Rojas García

Verifique la configuración de NTP en R1.

R1#show ntp associations

Figura 110 Verificación de NTP en R1

```
R1#show ntp associations
address      ref clock    st  when  poll  reach  delay  offset
disp
*-172.16.1.2 127.127.1.1 5   4     16   37    27.00  7.00
0.12
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

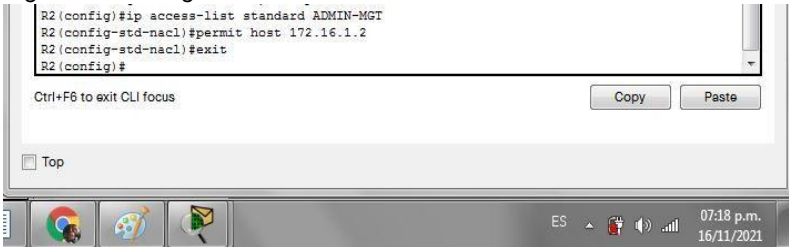
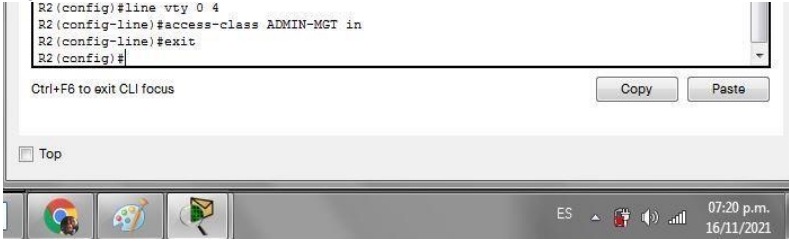
ES 07:13 p.m.
16/11/2021

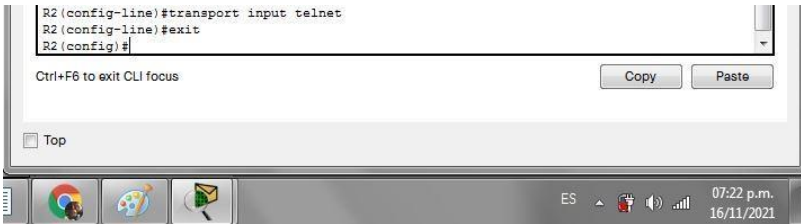
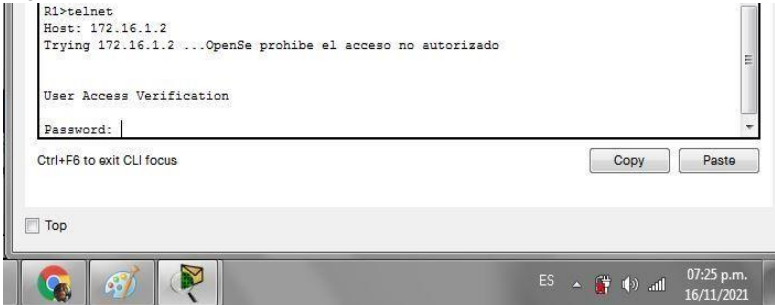
Fuente: Elaborado por Omar Hernando Rojas García

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

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

Tabla 26. Tabla de comandos para restringir el acceso a las líneas VTY en R2

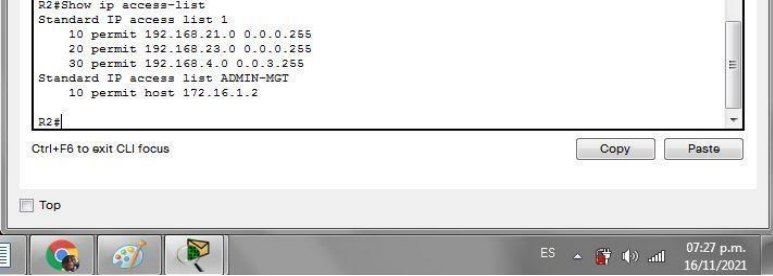
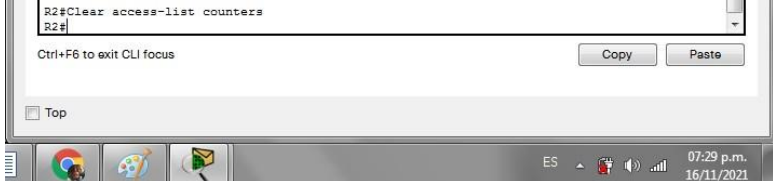
Elemento o tarea de configuración	Especificación
<p>Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2</p>	<pre>R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.2 R2(config-std-nacl)#exit</pre> <p><i>Figura 111. Configuración de la conexión a telnet de R1 a R2</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>
<p>Aplicar la ACL con nombre a las líneas VTY</p>	<pre>R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in R2(config-line)#exit</pre> <p><i>Figura 112. Aplicación de ACL con nombre a las líneas VTY</i></p>  <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>
<p>Permitir acceso por Telnet a las líneas de VTY</p>	<pre>R2(config)#line vty 0 4 R2(config-line)#transport input telnet R2(config-line)#exit</pre> <p><i>Figura 113. Acceso por telnet a las líneas vty</i></p>

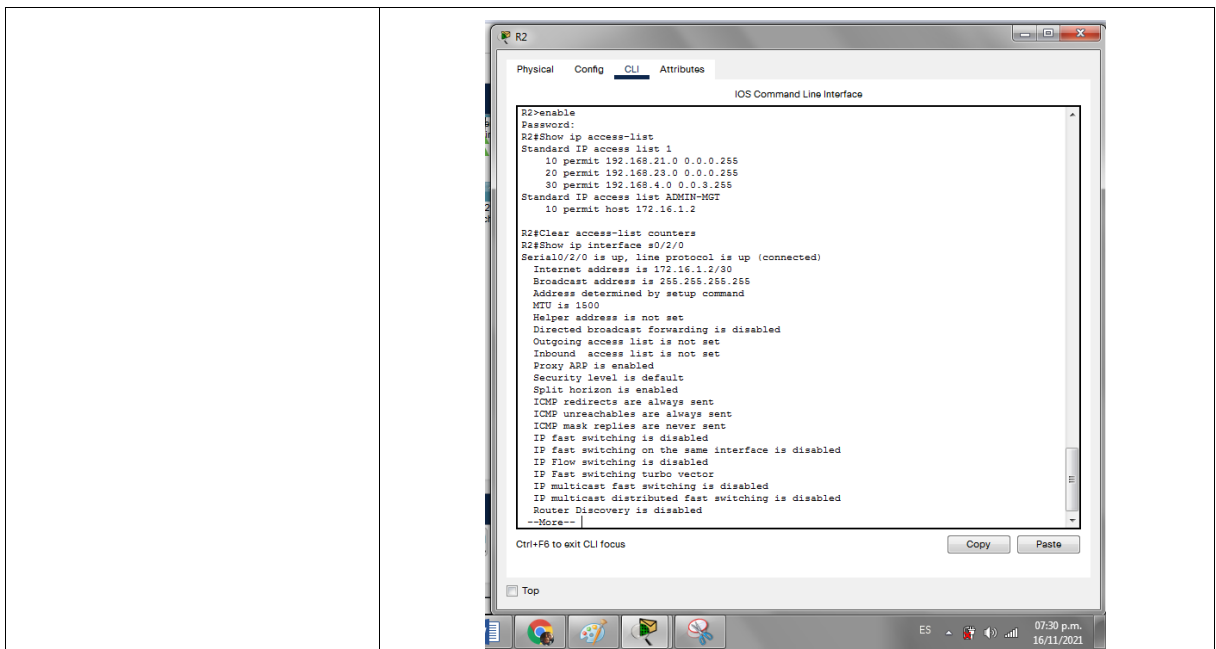
	 <pre>R2 (config-line)#transport input telnet R2 (config-line)#exit R2 (config)#</pre> <p>Ctrl+F6 to exit CLI focus</p> <p>Copy Paste</p> <p>Top</p> <p>ES 07:22 p.m. 16/11/2021</p> <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>
<p>Verificar que la ACL funcione como se espera</p>	<p><i>R1>telnet</i> <i>Host: 172.16.1.2</i></p> <p><i>Figura 114. Verificación de ACL</i></p>  <pre>R1>telnet Host: 172.16.1.2 Trying 172.16.1.2...OpenSe prohíbe el acceso no autorizado User Access Verification Password:</pre> <p>Ctrl+F6 to exit CLI focus</p> <p>Copy Paste</p> <p>Top</p> <p>ES 07:25 p.m. 16/11/2021</p> <p><i>Fuente: Elaborado por Omar Hernando Rojas García</i></p>

Fuente: Elaborado por Omar Hernando Rojas García

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

Tabla 27. Tabla de comandos para realizar pruebas de configuración

Descripción del comando	Entrada del estudiante (comando)
<p>Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció</p>	<p><i>R2#Show ip access-list</i></p> <p><i>Figura115. Coincidencias recibidas por ACL en R2</i></p>  <p>Fuente: Elaborado por Omar Hernando Rojas García</p>
<p>Restablecer los contadores de una lista de acceso</p>	<p><i>R2#Clear access-list counters</i></p> <p><i>Figura116. Restablecimiento de contadores de una lista de acceso</i></p>  <p>Fuente: Elaborado por Omar Hernando Rojas García</p>
<p>¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?</p>	<p><i>R2#Show ip interface s0/2/0</i></p> <p><i>Figura117. Verificación de ACL a las interfaces y las direcciones donde aplica</i></p>



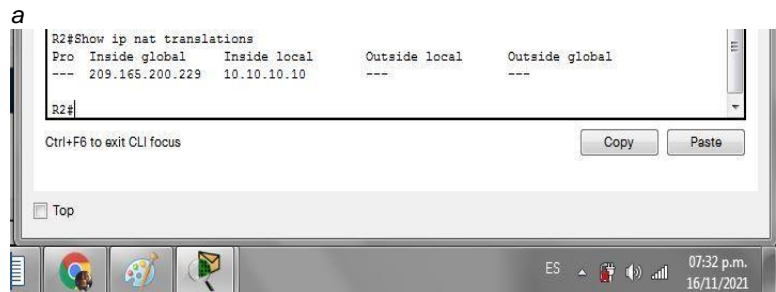
Fuente: Elaborado por Omar Hernando Rojas García

¿Con qué comando se muestran las traducciones NAT?

R2#Show ip nat translations

Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.

Figura118. Verificación de las traducciones NAT

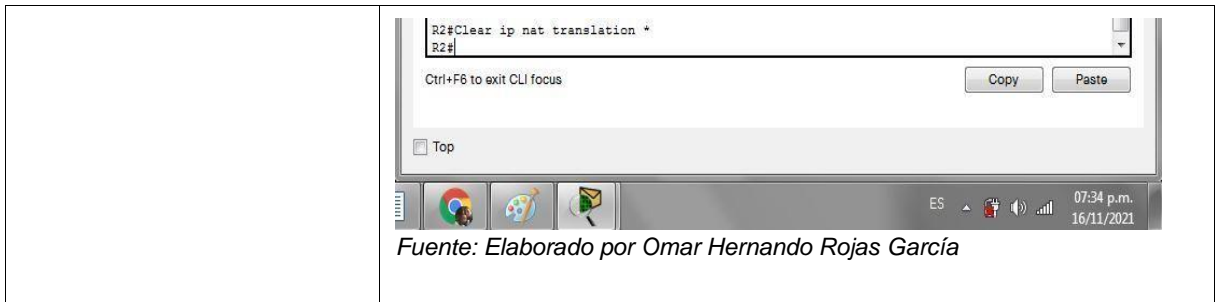


Fuente: Elaborado por Omar Hernando Rojas García

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?

*R2#Clear ip nat translation **

Figura119. Eliminación de traducciones NAT dinámicas



Fuente: Elaborado por Omar Hernando Rojas García

CONCLUSIONES

Mediante la utilización de herramientas de simulación, se establecen escenarios LAN/WAN que permiten realizar un análisis sobre el comportamiento de diversos protocolos y rutas métricas de enrutamiento de redes informáticas.

Se identifican herramientas de supervisión y protocolos de administración de red disponibles en el IOS para resolver los problemas de redes de datos, evaluando el desempeño de routers y switches, mediante el uso de comandos especializados en gestión de redes.

Se configura de manera correcta, cada uno de los dispositivos de networking, que forman parte del primer escenario en el simulador de manera adecuada y funcional.

BIBLIOGRAFÍA

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

CISCO. (2019). 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>

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