

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

VICTOR MAURICIO DELGADO PEÑA

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

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

VICTOR MAURICIO DELGADO PEÑA

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 SISTEMAS  
TUNJA  
2021

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

---

---

Firma del presidente del Jurado

---

Firma del Jurado

---

Firma del Jurado

TUNJA, 29 de noviembre de 2021

## AGRADECIMIENTOS

Aprender autónomamente es un proceso que la Universidad Nacional Abierta y a Distancia Unad, nos enseñó, que, por medio de la investigación, el análisis y la perseverancia constante, finalizáramos una etapa muy importante en nuestras vidas, que es ser profesionales, pero nada sería exitoso, sin la compañía, de nuestros Tutores que con su orientación nos aportaron muchos conocimientos y nos ayudaron en esos momentos que no sabíamos que hacer, agradezco por su dedicación y acompañamiento en nuestro camino universitario, que aunque por dificultades presentadas en nuestra vida laboral, aun así, cumpliéramos con lo exigido, sus buenos valores y ética profesional nos refleja que no solo son nuestros facilitadores de conocimiento si no que podemos contar con personas amigables.

Muchas gracias por todo, y muchos éxitos en todo lo que hagan.

## CONTENIDO

AGRADECIMIENTOS.....	4
TABLA DE CONTENIDO .....	5
LISTA DE TABLAS .....	6
LISTA DE FIGURAS.....	8
GLOSARIO.....	13
RESUMEN.....	17
ABSTRACT. ....	18
INTRODUCCIÓN.....	19
DESARROLLO	
Escenario 1.....	20 - 37
Escenario 2.....	38 - 86
CONCLUSIONES .....	87
BIBLIOGRAFÍA.....	88

## LISTA DE TABLAS

Tabla 1. Dispositivos a utilizar.....	21
Tabla 2. Subredes.....	22
Tabla 3. Esquema de direccionamiento .....	23
Tabla 4. Configuración de las subredes.....	24
Tabla 5. Tabla de direccionamiento .....	24
Tabla 6. Configuración aspectos básicos R1 .....	25
Tabla 7. Configuración aspectos básicos S1.....	30
Tabla 8. PC_A Network Configuration .....	36
Tabla 9. PC_B Network Configuration .....	37
Tabla 10. Códigos de Inicializar dispositivos.....	39
Tabla 11. direccionamiento del servidor web.....	43
Tabla 12. configuración de R1 .....	44
Tabla 13. configuración de R2.....	45
Tabla 14. configuración de R3.....	47
Tabla 15. configuración de S1 .....	49
Tabla 16. configuración de S3.....	51
Tabla 17. ping para probar la conectividad entre los dispositivos .....	53
Tabla 18. Configurar la seguridad del switch S1 .....	54
Tabla 19. Configurar la seguridad del switch S3 .....	58
Tabla 20. Configurar la seguridad del Router R1 .....	61
Tabla 21. Configurar OSPF en el R1 .....	63

Tabla 22.: Configurar OSPF en el R2 .....	67
Tabla 23.: Configurar OSPFv3 en el R3.....	69
Tabla 24.: Verificar la información de OSPF .....	71
Tabla 25.: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23 .....	72
Tabla 26.: Configurar la NAT estática y dinámica en el R2 .....	74
Tabla 27.: Verificar el protocolo DHCP y la NAT estática.....	78
Tabla 28.: Configuración NTP .....	80
Tabla 29.: Restricción del acceso a las líneas VTY en el R2 .....	82
Tabla 30.: Restricción del acceso a las líneas VTY en el R2 .....	84

## LISTA DE FIGURAS

Figura 1: Topología escenario 1 .....	20
Figura 2: Red simulador.....	21
Figura 3: configuración del terminal, Desactivar las búsquedas DNS Cambio el nombre, nombre de dominio, asignando contraseñas para modo EXEC.....	26
Figura 4: Contraseña de acceso a la consola, longitud mínima para las contraseñas .....	27
Figura 5: Creación usuario Administrativo y configuración de inicio de sesión .....	27
Figura 6: Cifrado de las contraseñas de texto.....	28
Figura 7: Configuración banner motd.....	28
Figura 8: Configuración puerto G 0/0/0 .....	28
Figura 9: Configuración puerto G 0/0/1 .....	29
Figura 10: clave de cifrado RSA .....	29
Figura 11: Desactivar búsquedas DNS.....	31
Figura 12: Asignación de nombre al Switch.....	31
Figura 13: Asignación de nombre de dominio.....	32
Figura 14: Asignación contraseña EXEC en modo privilegiado .....	32
Figura 15: Creación de la contraseña de acceso a la consola .....	32
Figura 16: Creación usuario administrativo S1 .....	33
Figura 17: Configuración del inicio de sesión en las líneas VTY.....	33
Figura 18: Configuración VTY solo aceptando SSH .....	33
Figura 19: Cifrado de las contraseñas de texto.....	34
Figura 20: Configuración de MOTD Banner.....	34
Figura 21: Generar una clave de cifrado RSA.....	34
Figura 22: Configuración interface VLAN 1 .....	35
Figura 23: Configuración del Gateway predeterminado.....	35
Figura 24: Configuración de red PC_A .....	36

Figura 25: Configuración de red PC_B .....	37
Figura 26. Topología escenario 2 .....	38
Figura 27. Inicializar y volver a cargar R1 .....	39
Figura 28. Inicializar y volver a cargar R3.....	40
Figura 29. Inicializar y volver a cargar R3.....	40
Figura 30. Inicializar y volver a cargar S1 .....	41
Figura 31. Inicializar y volver a cargar S3.....	42
Figura 32. Verificar que la base de datos de VLAN no esté en la memoria flash en S3.....	42
Figura 33. Configuración de IP del servidor web .....	43
Figura 34. Configuración R1 .....	45
Figura 35. Configuración R2 .....	47
Figura 36. Configuración R3 .....	49
Figura 37. Configuración S1 .....	50
Figura 38. Configuración S3 .....	51
Figura 39. Ingreso a switches y routers con contraseñas .....	52
Figura 40. Ping R1 a R2, S0/0/0 .....	53
Figura41. Ping R2 a R3, S0/0/1 .....	53
Figura 42. Ping PC de Internet a Gateway predeterminado.....	53
Figura 43. base de datos de VLAN .....	54
Figura 44. Asignar la dirección IP de administración .....	55
Figura 45. Asignar el gateway predeterminado.....	55
Figura 46. Forzar el enlace troncal en la interfaz F0/5.....	55
Figura 47. Forzar el enlace troncal en la interfaz F0/3.....	56
Figura 48. Configurar el resto de los puertos como puertos de acceso .....	56
Figura 49. Asignar F0/6 a la VLAN 21 .....	57
Figura 50. Apagar todos los puertos sin usar.....	57

Figura 51. Crear la base de datos de VLAN en S3 .....	58
Figura52. Asignar la dirección IP de administración .....	58
Figura 53. Asignar el gateway predeterminado.....	59
Figura 54. Forzar el enlace troncal en la interfaz F0/3.....	59
Figura 55. Configurar el resto de los puertos como puertos de acceso .....	59
Figura 56. Asignar F0/18 a la VLAN 21 .....	60
Figura 57. Apagar todos los puertos sin usar.....	60
Figura 58. Configurar la subinterfaz 802.1Q .21 en G0/1 .....	61
Figura 59. Configurar la subinterfaz 802.1Q .23 en G0/1.....	61
Figura 60. Configurar la subinterfaz 802.1Q .99 en G0/1.....	62
Figura 61 Activar la interfaz G0/1 .....	62
Figura 62 Ping S1 a VLAN 99 de R1 .....	63
Figura 63 Ping S3 a VLAN 99 de R1 .....	63
Figura 64 Ping S1 a VLAN 21 de R1 .....	64
Figura 65 Ping S3 a VLAN 23 de R1 .....	64
Figura 66 Configuración OSPF área 0 R1 .....	65
Figura67 Anunciar las redes conectadas directamente .....	65
Figura68 Establecer todas las interfaces LAN como pasivas .....	66
Figura69 Desactivar la sumarización automática.....	66
Figura70 Configurar OSPF área 0 R2.....	67
Figura71 Anunciar las redes conectadas directamente a R2.....	67
Figura72 Establecer la interfaz LAN (loopback) como pasiva.....	68
Figura73 Desactivación de la sumarización automática .....	68
Figura74 Configurar OSPF área 0 R3.....	69
Figura75 Anunciar redes IPv4 conectadas directamente R3 .....	69
Figura76 Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas .....	70

Figura77 Desactive la sumarización automática. R3 .....	70
Figura78 ID del proceso OSPF e interfaces router .....	71
Figura79 comando muestra solo las rutas OSPF .....	71
Figura80 sección de OSPF de la configuración en ejecución .....	72
Figura81 primeras 20 direcciones IP en la VLAN 21 Reservadas.....	72
Figura82 primeras 20 direcciones IP en la VLAN 23 Reservadas.....	73
Figura83 Crear un pool de DHCP para la VLAN 21 .....	73
Figura84 Crear una base de datos local con una cuenta de usuario .....	74
Figura85 Crear una base de datos local con una cuenta de usuario .....	74
Figura86 Habilitar el servicio del servidor HTTP .....	75
Figura87 Habilitar el servicio del servidor HTTP .....	75
Figura88 Crear una NAT estática al servidor web .....	75
Figura89 Asignar la interfaz interna y externa para la NAT estática .....	76
Figura90 Configurar la NAT dinámica dentro de una ACL privada .....	77
Figura91 Defina el pool de direcciones IP públicas utilizables.....	77
Figura92 Definir la traducción de NAT dinámica.....	78
Figura93 Verificar que la PC-A haya adquirido información de IP del servidor de DHCP .....	78
Figura94 Verificar que la PC-C haya adquirido.....	79
Figura95 ping PC-A a PC-C.....	79
Figura96 acceder al servidor web (209.165.200.229.....	79
Figura97 Ajuste la fecha y hora en R2.....	80
Figura98 Configure R2 como un maestro NTP .....	80
Figura99 Configurar R1 como un cliente NTP .....	81
Figura100 R1 para actualizaciones de calendario periódicas con hora NTP .....	81
Figura101 Verifique la configuración de NTP en R1 .....	82
Figura102 R1 conexión Telnet con R2.....	82

Figura103 Aplicar la ACL con nombre a las líneas VTY .....	83
Figura104 Permitir acceso por Telnet a las líneas de VTY .....	83
Figura105 Verificar que la ACL funcione como se espera .....	83
Figura106 lista de acceso .....	84
Figura107 Restablecer los contadores de una lista de acceso .....	84
Figura108 mostrar qué ACL.....	85
Figura109 traducciones NAT .....	85
Figura110 eliminar las traducciones de NAT dinámicas .....	86

## GLOSARIO

**Cisco:** es una empresa dedicada a la interconexión de redes informáticas y de comunicaciones más grande del mundo. Es por tanto la que domina los sistemas y la que, prácticamente, ha creado un estándar propio para las redes de telecomunicaciones.

**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.

**Redes Internet:** Es la interconexión física o inalámbrica que vincula varios dispositivos informáticos (servidores, computadoras, teléfonos móviles, periféricos, entre otros) para que se comuniquen entre sí, con la finalidad de compartir datos y ofrecer servicios.

**IP:** «dirección del Protocolo de Internet» es un protocolo que se encarga de establecer las comunicaciones en la mayoría de nuestras redes y que para esto asigna una dirección única e irrepetible a cada dispositivo que trata de comunicarse en internet a esta dirección se le conoce como dirección ip la cual está conformada por cuatro bloques numéricos que van del 0 al 255 y está en cada uno separados por un punto.

**Router:** También conocido como encaminador o enrutador, es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.

**Switches:** son piezas de construcción clave para cualquier red. Conectan varios dispositivos, como computadoras, access points inalámbricos, impresoras y servidores; en la misma red dentro de un edificio o campus. Un switch permite a los dispositivos conectados compartir información y comunicarse entre sí.

**Cable directo:** Es el que cable que se usa para conectar, normalmente, dispositivos que no son iguales, como, por ejemplo, un equipo a un hub, o un equipo a un switch.

**Subnetting:** Es dividir una red IP física en subredes lógicas (redes más pequeñas) para que cada una de estas trabaje a nivel envío y recepción de paquetes como una red individual, aunque todas pertenezcan a la misma red física y al mismo dominio.

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

**CLI:** interfaz de línea de comando, **CISCO** usa una estructura jerárquica. Esta estructura requiere el ingreso a distintos modos para realizar tareas particulares. Por ejemplo, para configurar una interfaz del router, el usuario debe ingresar al modo de configuración de interfaces.

**Puertos de comunicación:** son aquellos donde se conectan los dispositivos externos al computador (también llamados periféricos) y por donde se recibe y/o envía información al computador desde el exterior.

**Red de Área Local (LAN) (Local Area Network)** Red de comunicación entre ordenadores situados en el mismo edificio o en edificios cercanos, de forma que permite a sus usuarios el intercambio de datos y la compartición de recursos.

**DNS:** corresponde a las siglas en inglés de "Domain Name System", es decir, "Sistema de nombres de dominio". Este sistema es básicamente la agenda telefónica de la Web que organiza e identifica dominios

**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.

**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.

**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. La conmutación permite la entrega de la señal desde el origen hasta el destino requerido.

**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. El enrutado en sentido estricto se refiere al enrutado IP y se opone al bridging.

**Vlan:** (red de área local virtual) es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.

**ACL:** (Lista de Control de Accesos), es una serie de instrucciones que controlan que en un router se permita el paso o se bloqueen los paquetes IP de datos, que maneja el equipo según la información que se encuentra en el encabezado de los mismos.

**VTP:**( Vlan Trunking Protocol) es un protocolo propietario de **Cisco** que propaga la definición de vlans entre los switchs que estén configurados en un mismo dominio. Se establece un switch con el rol de server y éste propaga las vlans que tenga configuradas a todos los switches que funcionen en el rol de cliente.

**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. El número de líneas **vty** que admite un router Cisco varía según el tipo de router y la versión de IOS.

**Troncal:** Es un enlace punto a punto, entre dos dispositivos de red, que transporta más de una VLAN. Un enlace **troncal** de VLAN le permite extender las VLAN a través de toda una red.

**DNS:** sistema de nombres de dominio, traduce los nombres de dominios aptos para lectura humana (por **ejemplo**, www.amazon.com) a direcciones IP aptas para lectura por parte de máquinas (por **ejemplo**, 192.0.2.44).

**Routing y Switching:** es lo que permite conectar dispositivos (switches y routers) para que los equipos y sus periféricos puedan conectarse entre sí y compartir determinada información o realizar acciones

**OSPF:** (Open Shortest Path First) es un protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes **IP** y basado en el algoritmo de primera vía más corta (SPF). ... **OSPF** puede recalcularse las rutas en muy poco tiempo cuando cambia la topología de la red.

## RESUMEN

Este documento final es una de las actividades evaluativas del Diplomado de profundización CISCO (diseño e implementación de soluciones integradas lan / wan), donde se identifica las capacidades y destreza que se adquirieron durante el desarrollo del diplomado, buscando la adquisición de conocimientos mediante la práctica y desarrollo de esta actividad.

En el **escenario 1**, se desarrolla la documentación de la solución a la configuración de cada dispositivo, describiendo el paso a paso de la solución de cada etapa realizada, siguiendo los parámetros que la guía ofrece para el entendimiento de esta actividad, verificando la conectividad mediante el uso de comandos **ping, ipconfig /all**, entre otros.

En el **escenario 2**, se configura y se realiza una topología de red pequeña donde admite conectividad IPV4 e IPV6, configurando los dispositivos de la siguiente manera, asignar seguridad en los switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

**Palabras Clave:** CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

## ABSTRACT

This final document is one of the evaluative activities of the CISCO in-depth Diploma (design and implementation of integrated solutions lan / wan), where the capacities and skills that were acquired during the development of the diploma are identified, seeking the acquisition of knowledge through practice and development of this activity.

In this **scenario 1**, the documentation of the solution to the configuration of each device is developed, describing the step-by-step solution of each stage carried out, following the parameters that the guide offers to understand this activity, verifying connectivity through the use of ping, traceroute, show ip route, among others.

In this **scenario 2**, a small network topology is configured and performed where it supports IPV4 and IPV6 connectivity, configuring the devices as follows, assign security in the switches, routing between VLANs, the dynamic routing protocol OSPF, the protocol of dynamic host configuration (DHCP), static and dynamic network address translation (NAT), access control lists (ACL), and server / client Network Time Protocol (NTP). During the evaluation, you will test and register your network using common CLI commands.

Keywords: CISCO, CCNA, Routing, Swicthing, Networking, Electronics.

## INTRODUCCIÓN

El Diplomado de Profundización diplomado de profundización cisco (diseño e implementación de soluciones integradas lan / wan), nos evalúa mediante las actividades de escenarios 1 y 2, donde tenemos que demostrar nuestras habilidades y conocimientos adquiridos en los laboratorios y evaluaciones desarrolladas durante las todas las etapas del curso.

En el escenario 1 se debe implementar la topología que la guía exige, donde se debe construir en el simulador Cisco Packet tracer utilizando dispositivos como Router, Switch, y PCs conectados con cables directos, luego se realiza el Subneteo para las subredes LAN 1 Y LAN 2 y sus dispositivos partiendo con la dirección Ip donde hay que completarla con los dos últimos números de la cedula de identificación.

Se debe configurar los ajustes básicos de seguridad en el Router y el Switch Configurando los hosts y verificar la conectividad entre los equipos mediante los comandos **ping, ipconfig /all** todo evidenciado con imágenes.

En el escenario 2 se debe implementar la topología que la guía exige, donde se debe construir en el simulador Cisco Packet tracer , Configurar los parámetros básicos de los dispositivos verificando la conectividad de la red mediante ping, configurar la seguridad vlan de switches y routers, Configurar la seguridad del switch, las VLAN y el routing entre VLAN, Configurar el protocolo de routing dinámico OSPF, Implementar DHCP y NAT para IPv4, Configurar NTP, Configurar y verificar las listas de control de acceso (ACL)

## DESARROLLO

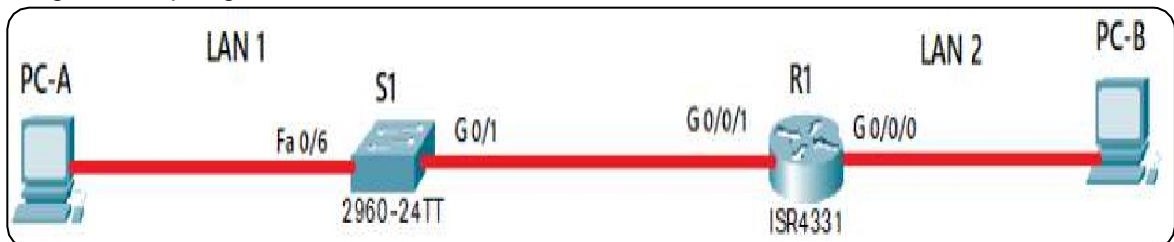
### 1. ESCENARIO 1

#### Aspectos básicos/situación

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

#### Topología

Figura 1: Topología escenario 1







Fuente: Realizado por Victor Mauricio Delgado Peña

#### Parte 1: Construya la Red

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

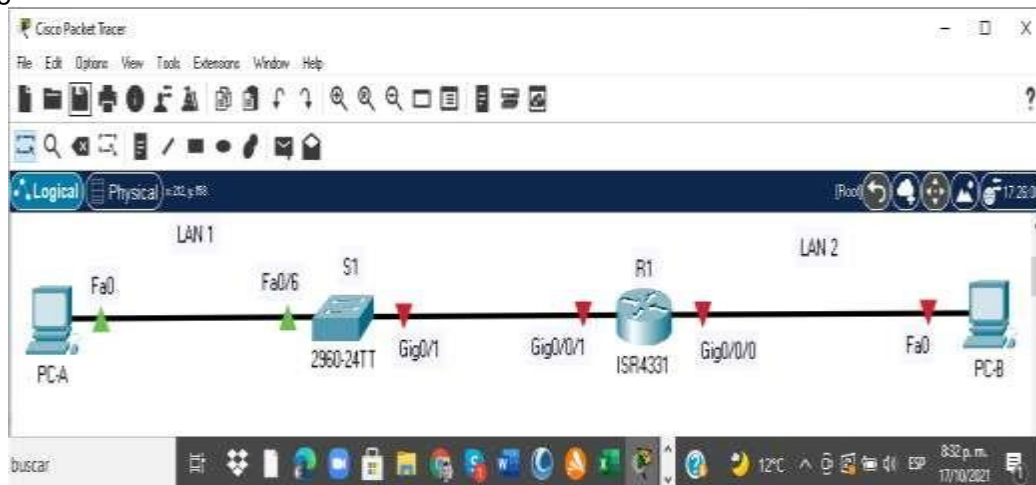
**Tabla 1. Dispositivos a utilizar**

# de Dispositivos	Tipo de Dispositivo	Dispositivo
2	2 PC-PT	 PC-A PC-B
3	Cable directo	
1	Switcho 2960 - 24TT	 S1
1	1 Router 4331	 R1

Fuente: Realizado por Victor Mauricio

La red empieza con la **PC-A** conectada en la **FastEthernet0** con el **cable directo** hasta la **FastEthernet0/6** del **Switcho S1** se definirá como **LAN 1**, con otro **cable directo** se conecta al **GigabitsEthernet0/1** del mismo **Switcho S1** al **GigabitsEthernet0/0/1** del **Router R1**, en el mismo **Router R1** conectado al **GigabitsEthernet0/0/0** con otro **cable directo** se conecta en la **FastEthernet0** del final de la red que es la **PC-B** el cual se definirá como **LAN 2**

Figura 2: Red simulador



Fuente: Realizado por Victor Mauricio Delgado Peña

## Parte 2: Desarrolle el esquema de direccionamiento IP

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

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

**Cedula:** 1.053.608.689

**Dirección IP:** 192.168.89.0

Se realiza el Subneteo, partiendo desde la dirección IP obtenida **192.168.89.0** el cual pertenece a la de clase C, vamos a subdividirla en pequeñas redes de manera que obtengamos dos redes **LAN 1** con la cantidad de 100 hosts y **LAN 2** con la cantidad de 50 hosts.

### LAN 1

Lo primordial es escribir la dirección de red con su mascara de subred en notación binaria

**192.168.89.0/24= 11000000. 10101000. 01011001 .00000000**

**255.255.255.0= 11111111.11111111.11111111.00000000**

De acuerdo a la información anterior necesitamos crear dos (2) subredes, buscamos en la tabla el número 2 elevado con algún número nos genere dos redes.

**Tabla 2. Subredes**

$2^0$	$2^1$	$2^2$	$2^3$	$2^4$	$2^5$	$2^6$	$2^7$
1	2	4	8	16	34	64	128

*Fuente: Realizado por Victor Mauricio Delgado Peña*

Para este caso usaremos  $2^1$  donde esta es igual a 2 el cual es la cantidad de subredes que necesitamos. Sabiendo que es la cantidad de bits que robaremos a

la dirección de red para la máscara y así obtener la máscara de red para las subredes.

**11000000 . 10101000 . 01011001 . 00000000**  
**11111111 . 11111111 . 11111111 . 10000000**  
**255 . 255 . 255 . 128 / 25**

Ya ocupado el bit encendido me queda 7 bits apagados y miramos que  $2^7 : 128$  lo cual nos confirma que el salto que tenemos 128 direcciones y solo se podrá utilizar 126.

## LAN 2

Ahora hallaremos la red LAN 2 el cual nos dice que son de 50 hosts entonces miramos la Tabla 2 e encontramos que la que nos sirve es  $2^6$  es igual a 64. Local en los bits del hosts dejamos 6 bits apagados disponibles para el host y encendemos 2 bits para cumplir con lo que exige en esta red 50hosts.

**11111111 . 11111111 . 11111111 . 00000000**  
**11111111 . 11111111 . 11111111 . 11000000**  
**255 . 255 . 255 . 192 / 26**

Tenemos 64 direcciones y 62 útiles

**Tabla 3. Esquema de direccionamiento**

# Sub	Dirección IP	Mask	1 <sup>ra</sup> Dirección válida	Última Valida	Broadcast	Host
1	192.168.89.0	/25	192.168.89.1	192.168.89.126	192.168.89.127	100
2	192.168.89.128	/26	192.168.89.129	192.168.89.190	192.168.89.191	50

*Fuente: Realizado por Victor Mauricio Delgado Peña*

**Tabla 4. Configuración de las subredes**

<b>PC-A</b>	192.168.89.2
<b>LAN 1</b>	100 hosts
<b>S1 SVI</b>	192.168.89.1
<b>R1 G 0/0/1</b>	192.168.89.1
<b>R1 G 0/0/0</b>	192.168.89.129
<b>LAN 2</b>	50 hosts
<b>PC_B</b>	192.168.89.130

*Fuente: Realizado por Victor Mauricio Delgado*

**Tabla 5. Tabla de direccionamiento**

<b>Item</b>	<b>Requerimiento</b>
Dirección de Red	192.168.X.0 donde X corresponde a los últimos dos dígitos de mi cédula el cual es <b>89</b> , quedaría 192.168. <b>89</b> .0.
Requerimiento de host Subred LAN1	100 hosts
Requerimiento de host Subred LAN2	50 hosts
R1 G0/0/1	192.168.89.1
R1 G0/0/0	192.168.89.129
S1 SVI	192.168.89.1
PC-A	192.168.89.2
PC-B	192.168.89.130

*Fuente: Realizado por Victor Mauricio Delgado*

### **Parte 3: Configure aspectos básicos**

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

#### **Paso 1: configurar los ajustes básicos**

Las tareas de configuración para R1 incluyen las siguientes:

**Tabla 6. Configuración aspectos básicos R1**

<b>Tarea</b>	<b>Especificación</b>
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 las contraseñas	10 caracteres
Crear un usuario administrativo en la base de datos local	<b>Nombre de usuario:</b> 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

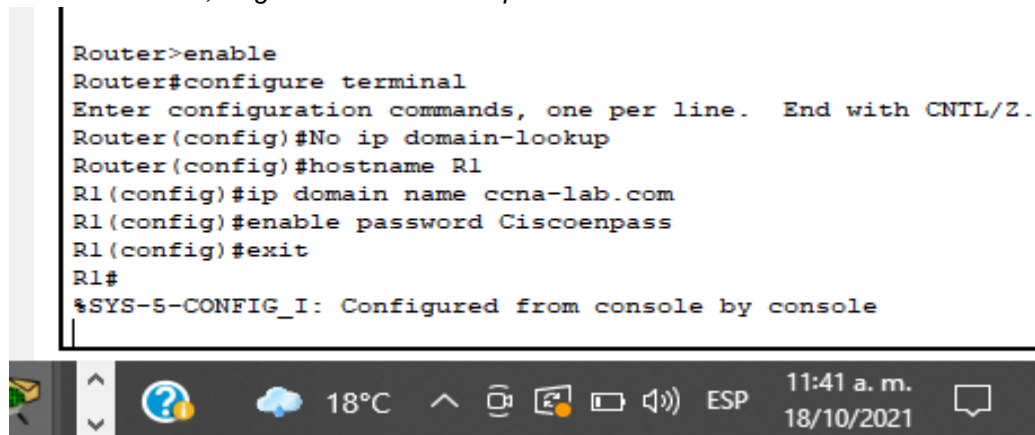
*Fuente: Realizado por Victor Mauricio Delgado Peña*

A él podemos acceder a la línea de comandos dándole clic a CLI y esperamos a que se descomprima la imagen del arranque del router R1 inmediatamente en un router nuevo nos pregunta si queremos de una vez hacer una configuración básica ayudados por un guía en este caso nosotros vamos decir que no porque vamos a hacer nuestra propia configuración de manera manual siguiendo nuestro propio orden.

Aquí ingresamos como usuarios privilegiados con el siguiente código, entrando a la configuración del terminal, Desactivar las búsquedas DNS y cambiando el nombre del Router a R1, configuramos el nombre de dominio, asignando contraseñas para modo EXEC privilegiado.

Figura 3: configuración del terminal, Desactivar las búsquedas DNS Cambio el nombre, nombre de dominio, asignando contraseñas para modo EXEC

```
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)#ip domain name ccna-lab.com
R1(config)#enable password Ciscoenpass
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```



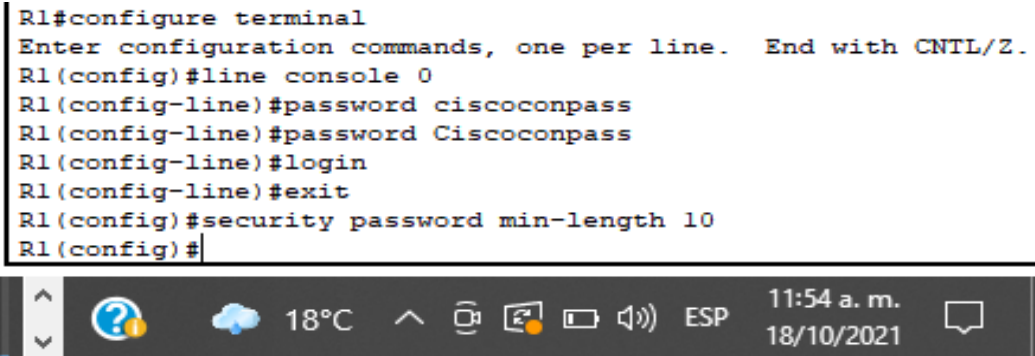
Fuente: Realizado por Victor Mauricio Delgado Peña

## Código R1

```
Router>enable..... abrir modo usuario privilegiado
Router#configure terminal ..... ingreso a la configuración del
terminal
Router(config)#No ip domain-lookup ..... Desactivar las búsquedas DNS
Router(config)#hostname R1..... Cambio de
nombre
R1(config)#ip domain name ccna-lab.com ..... asignar nombre de
dominio
R1(config)#enable password ciscoconpass..... contraseñas para modo
EXEC
```

Figura 4: Contraseña de acceso a la consola, longitud mínima para las contraseñas.

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#password Ciscoconpass
R1(config-line)#login
R1(config-line)#exit
R1(config)#security password min-length 10
R1(config)#
```



Fuente: Realizado por Victor Mauricio Delgado Peña

R1(config)#line console 0..... configuración interfaz de consola  
R1(config-line)#password Ciscoconpass ..... Contraseña de acceso a la consola  
R1(config-line)#login  
R1(config-line)#exit

Figura 5: Creación usuario Administrativo y configuración de inicio de sesión

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



Fuente: Realizado por Victor Mauricio Delgado Peña

R1(config)#username admin password admin1pass ..... crear usuario administrativo en la base de datos  
localR1(config)#line vty 0 4 ..... Configuramos inicio de sesión en las líneas vty para uso de BD local  
R1(config-line)#login

Figura 6: Cifrado de las contraseñas de texto

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

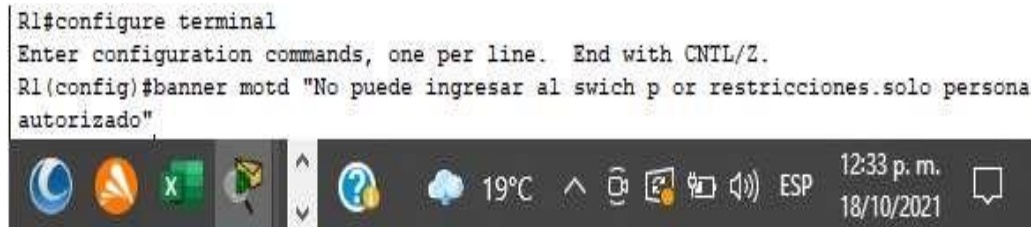


Fuente: Realizado por Victor Mauricio Delgado Peña

R1(config)#service password-encryption  
Código para cifrar las contraseñas de texto

Figura 7: Configuración banner motd

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1 (config) #banner motd "No puede ingresar al switch p or restricciones.solo personal
autorizado"
```



Fuente: Realizado por Victor Mauricio Delgado Peña

R1(config)#banner motd "No puede ingresar al switch por restricciones. Solo personal autorizado".....*Esto es un mensaje de aviso*

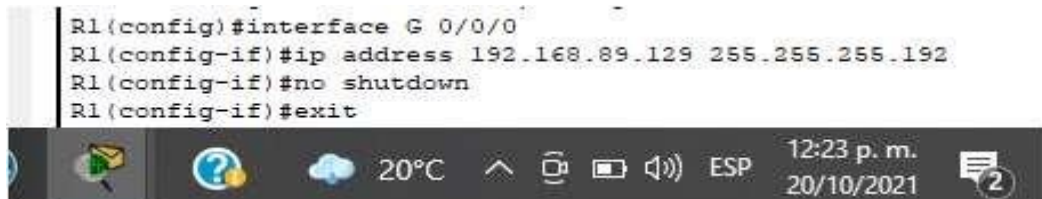
## Configuración de interfaces

**G0/0/0:** 192.168.89.129

Mask: 255.255.255.192

Figura 8: Configuración puerto G 0/0/0

```
R1 (config) #interface G 0/0/0
R1 (config-if) #ip address 192.168.89.129 255.255.255.192
R1 (config-if) #no shutdown
R1 (config-if) #exit
```



Fuente: Realizado por Victor Mauricio Delgado Peña

*Entramos a la interfaz del puerto*

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

*Configuramos la direccion IP con su mascara*

```
R1(config-if)#ip address 192.168.89.129 255.255.255.192
```

*habilitamos la interfaz*

```
R1(config-if)#no shutdown
```

**G 0/0/1: 192.168.89.1**

**Mask: 255.255.255.128**

*Figura 9: Configuración puerto G 0/0/1*

```
R1(config)#interface G 0/0/1
R1(config-if)#ip address 192.168.89.1 255.255.255.128
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#exit
```



*Fuente: Realizado por Victor Mauricio Delgado Peña*

*Entramos a la interfaz del puerto*

```
R1(config)#interface G 0/0/1
```

*Configuramos la direccion IP con su mascara*

```
R1(config-if)#ip address 192.168.89.1 255.255.255.128
```

*habilitamos la interfaz*

```
R1(config-if)#no shutdown
```

*Figura 10: clave de cifrado RSA*

```
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]
```



*Fuente: Realizado por Victor Mauricio Delgado Peña*

*Generamos una clave de cifrado*

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

### Configuración RSA

R1(config)#crypto key generate rsa

The name for the keys will be: R1.ccna-lab.com

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Las tareas de configuración del S1 incluyen:

**Tabla 7. 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	<b>Nombre de usuario:</b> 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: Realizado por Victor Mauricio Delgado Peña

### 1. desactivar búsqueda DNS

#### Código:

```
Switch(config)#No ip domain-lookup
```

Figura 11: Desactivar búsquedas DNS

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#No ip domain-lookup
Switch(config)#
```

Fuente: Realizado por Victor Mauricio Delgado Peña

### 2. Asignación de nombre al Switch

#### Código:

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

Figura 12: Asignación de nombre al Switch

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

Fuente: Realizado por Victor Mauricio Delgado Peña

### 3. Asignación de nombre de dominio

**Código:**

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

*Figura 13: Asignación de nombre de dominio*



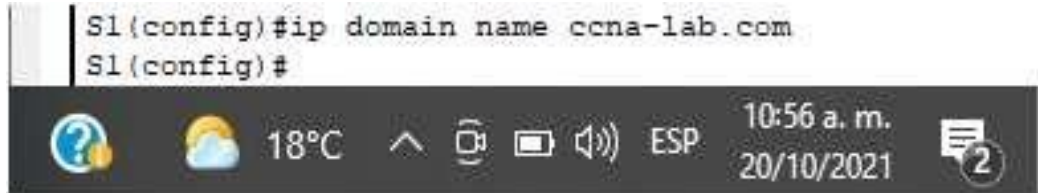
*Fuente: Realizado por Víctor Mauricio Delgado Peña*

**4. Asignación contraseña EXEC en modo privilegiado**

**Código:**

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

*Figura 14: Asignación contraseña EXEC en modo privilegiado*



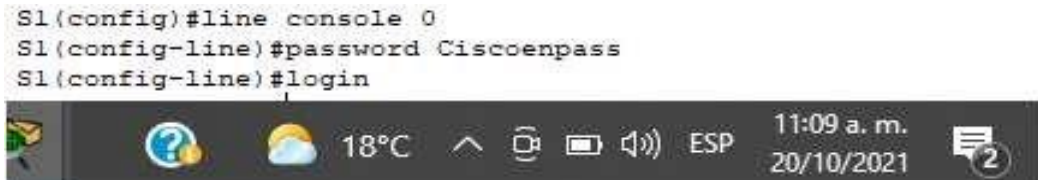
*Fuente: Realizado por Víctor Mauricio Delgado Peña*

**5. Creación de la contraseña de acceso a la consola**

**Código:**

```
S1(config)# line console 0  
S1(config-line)# password ciscoenpass  
S1(config-line)# login
```

*Figura 15: Creación de la contraseña de acceso a la consola*



*Fuente: Realizado por Víctor Mauricio Delgado Peña*

**6. Creación de usuario administrativo en la base de datos local**

**Código:**

S1(config)#username admin password admin1pass

Figura 16: Creación usuario administrativo S1

```
S1(config)#username admin password admin1pass
S1(config)#
```



Fuente: Realizado por Victor Mauricio Delgado Peña

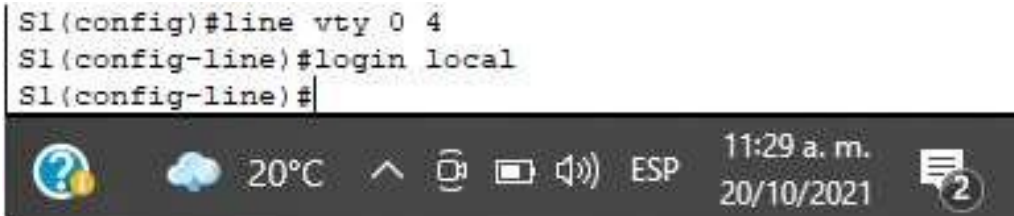
## 7. Configuración del inicio de sesión en las líneas VTY para que use la base de datos local

### Código:

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

Figura 17: Configuración del inicio de sesión en las líneas VTY

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



Fuente: Realizado por Victor Mauricio Delgado Peña

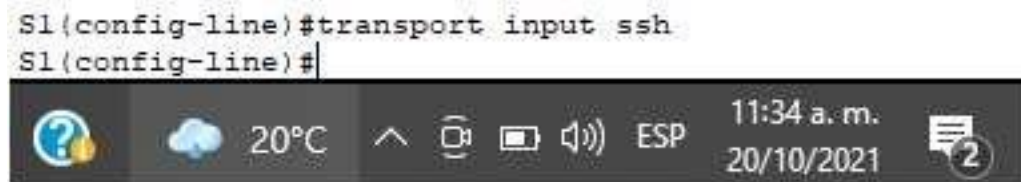
## 8. Configuración VTY solo aceptando SSH

### Código:

```
S1(config-line)#transport input ssh
```

Figura 18: Configuración VTY solo aceptando SSH

```
S1(config-line)#transport input ssh
S1(config-line)#
```



Fuente: Realizado por Victor Mauricio Delgado Peña

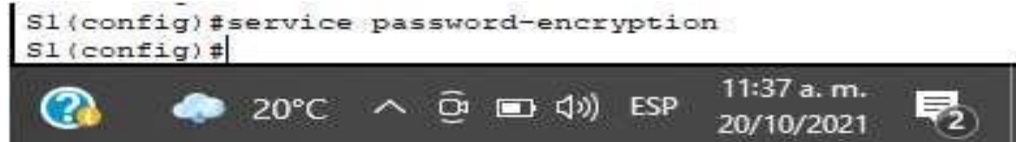
## 9. Cifrado de las contraseñas de texto

### Código:

S1(config)# service password-encryption

Figura 19: Cifrado de las contraseñas de texto

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



Fuente: Realizado por Víctor Mauricio Delgado Peña

## 10. Configuración de MOTD Banner

### Código:

S1(config)#banner motd "No puede ingresar al Router por restricciones. Solo personal autorizado"

Figura 20: Configuración de MOTD Banner

```
S1(config)#banner motd "No puede ingresar al Router por restricciones. Solo personal
autorizado"
S1(config)#
```



Fuente: Realizado por Víctor Mauricio Delgado Peña

## 11. Generar una clave de cifrado RSA

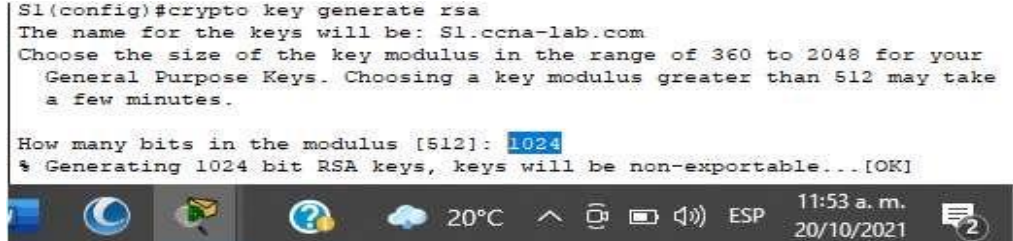
### Código:

S1(config)#crypto key generate rsa

Figura 21: Generar una clave de cifrado RSA

```
S1(config)#crypto key generate rsa
The name for the keys will be: S1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

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



Fuente: Realizado por Víctor Mauricio Delgado Peña

## 12. Configuración interface VLAN 1

### Código:


```
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.89.1 255.255.255.192
S1(config-if)#no shutdown
```

Figura 22: Configuración interface VLAN 1

```
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.89.1 255.255.255.192
S1(config-if)#no shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```



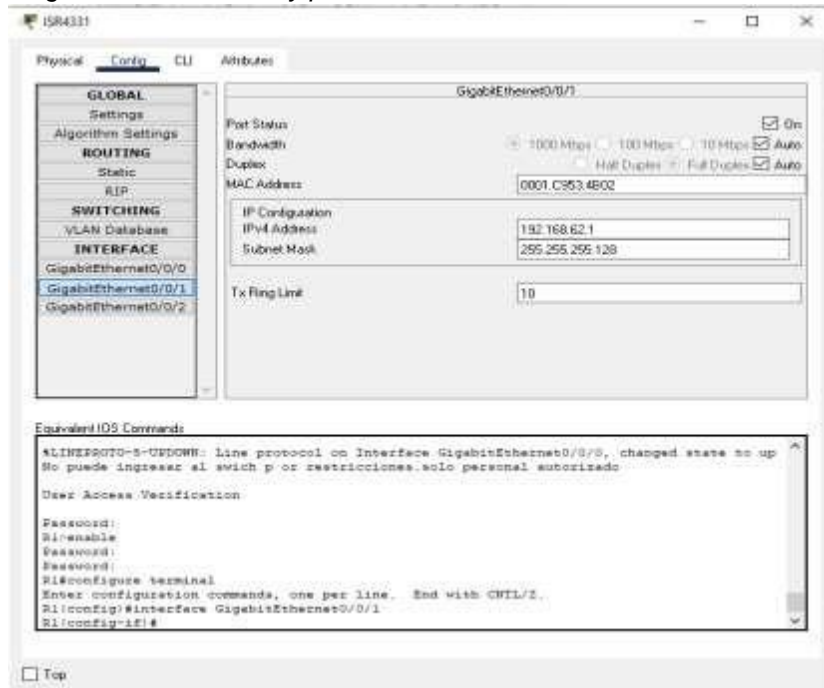
Fuente: Realizado por Víctor Mauricio Delgado Peña

## 12. Configuración del Gateway predeterminado

### Código:

```
S1(config)# interface G 0/1
S1(config-if)# ip address 192.168.89.1 255.255.255.192
S1(config-if)# no shutdown
```

Figura 23: Configuración del Gateway predeterminado



Fuente: Realizado por Victor Mauricio Delgado Peña

## Paso 2: Configurar los equipos

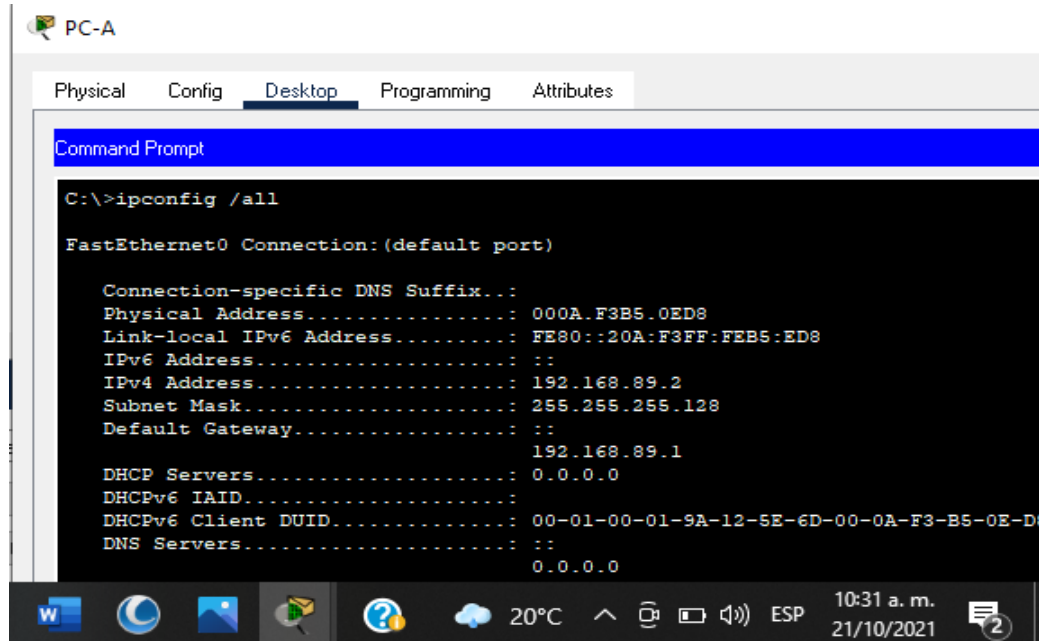
Configure los equipos host PC\_A y PC\_B conforme a la tabla de direccionamiento, registre las configuraciones de red de los hosts con el comando **ipconfig / all**

**Tabla 8. PC A Network Configuration**

PC_A Network Configuration	
Descripción	FastEthernet0 connection: (default port)
Dirección física	000A.F3B5.0ED8
Dirección IP	192.168.89.2
Mascara de subred	255.255.255.128
Gateway predeterminado	192.168.62.1

Fuente: Realizado por Victor Mauricio Delgado Peña

Figura 24: Configuración de red PC\_A



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Physical Address. . . . .: 000A.F3B5.0ED8
Link-local IPv6 Address . . . . .: FE80::20A:F3FF:FEB5:ED8
IPv6 Address. . . . .: ::
IPv4 Address. . . . .: 192.168.89.2
Subnet Mask . . . . .: 255.255.255.128
Default Gateway . . . . .: ::
                            192.168.89.1
DHCP Servers. . . . .: 0.0.0.0
DHCPv6 IAID. . . . .:
DHCPv6 Client DUID. . . . .: 00-01-00-01-9A-12-5E-6D-00-0A-F3-B5-0E-D8
DNS Servers. . . . .: ::
                            0.0.0.0
```

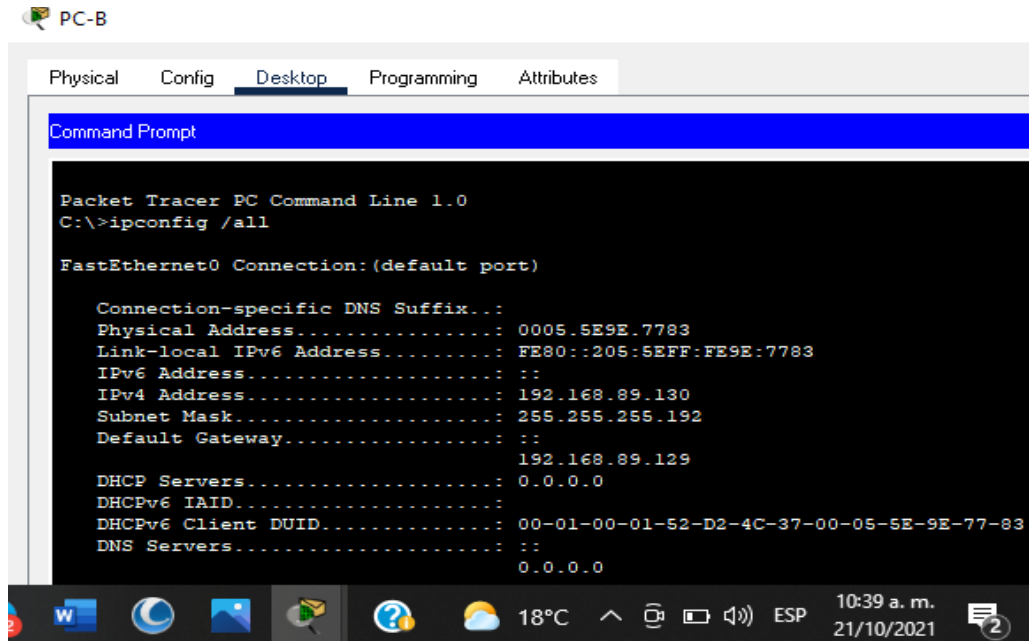
Fuente: Realizado por Victor Mauricio Delgado Peña

**Tabla 9. PC B Network Configuration**

PC_B Network Configuration	
Descripción	FastEthernet0 connection: (default port)
Dirección física	0005.5E9E.7783
Dirección IP	192.168.89.130
Mascara de subred	255.255.255.192
Gateway predeterminado	192.168.89.129

Fuente: Realizado por Victor Mauricio Delgado Peña

Figura 25: Configuración de red PC\_B

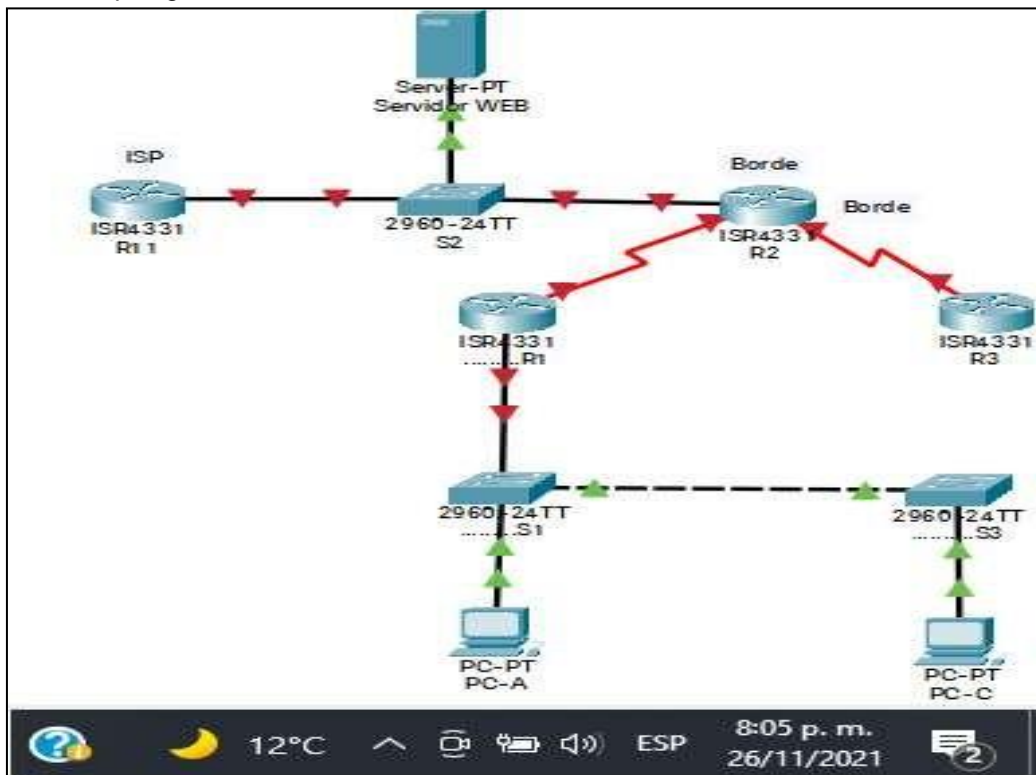


Fuente: Realizado por Victor Mauricio Delgado Peña

## Escenario 2

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

Figura 26. Topología escenario 2



Fuente: Raul Bareño Gutierrez (Tutor), archivo base propuesta topología Packet Tracer modificado e implementado por Victor Mauricio Delgado Peña

### Parte 1: Inicializar dispositivos

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

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

**Tabla 10. Códigos de Inicializar dispositivos**

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

Fuente: Realizado por Victor Mauricio Delgado Peña

## Router R1

*Figura 27. Inicializar y volver a cargar R1*

```

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

Press RETURN to get started!

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(3r), RELEASE SOFTWARE
Copyright (c) 1994-2016 by Cisco Systems, Inc.

Current image running: Boot ROM0

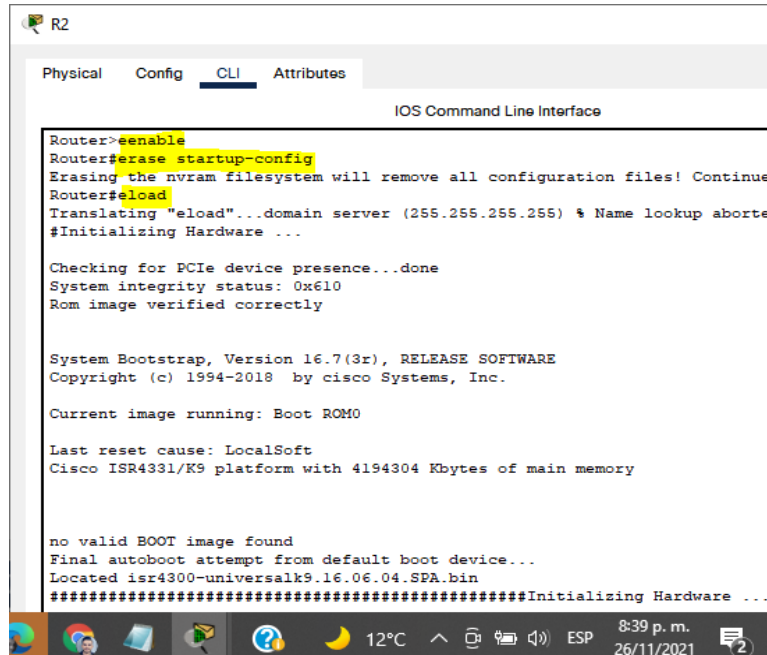
Last reset cause: LocalSoft
Cisco ISR4331/K5 platform with 4194304 Kbytes of main memory

no valid BOOT image found
Final autoboot attempt from default boot device...
Located 1sr4330-universalk5.16.06.04.SPA.bin
#####
  
```

Fuente: Realizado por Victor Mauricio Delgado Peña

## Router R2

Figura 28. Inicializar y volver a cargar R3



```
R2
Physical Config CLI Attributes
IOS Command Line Interface

Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
Router#reload
Translating "reload"...domain server (255.255.255.255) % Name lookup aborted
#Initializing Hardware ...

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

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

Current image running: Boot ROM0

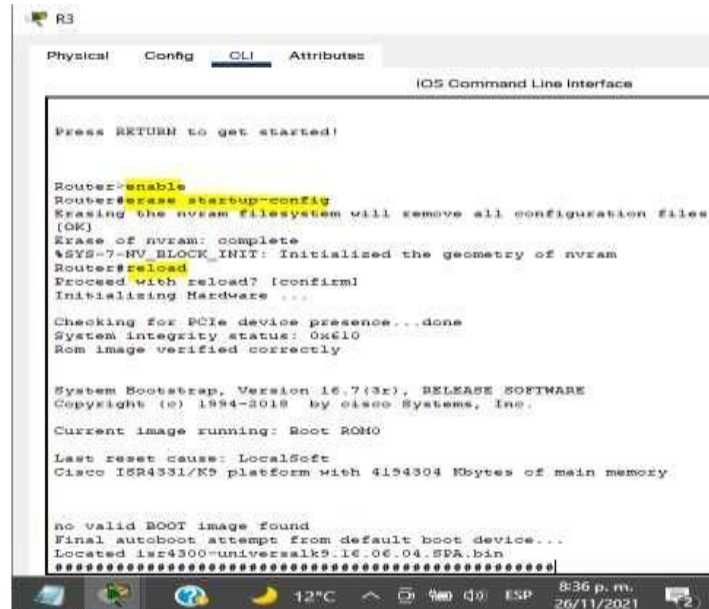
Last reset cause: LocalSoft
Cisco ISR4331/K9 platform with 4194304 Kbytes of main memory

no valid BOOT image found
Final autoboot attempt from default boot device...
Located isr4300-universalk9.16.06.04.SPA.bin
#####Initializing Hardware ...
```

Fuente: Realizado por Victor Mauricio Delgado Peña

## Router R3

Figura 29. Inicializar y volver a cargar R3



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

Press RETURN to get started!

Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
[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(3r), 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
#####
```

Fuente: Realizado por Victor Mauricio Delgado Peña

## Switch S1

Figura 30. Inicializar y volver a cargar S1



```
Switch>enable
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [OK]
Erase of nvram: complete
*SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of
2960-24TT starting...
Base ethernet MAC Address: 0002.4A41.75D0
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-ms.150-2.SE4.bin"
=====
```

Fuente: Realizado por Victor Mauricio Delgado Peña

Figura 31. Verificar que la base de datos de VLAN no esté en la memoria flash en S1



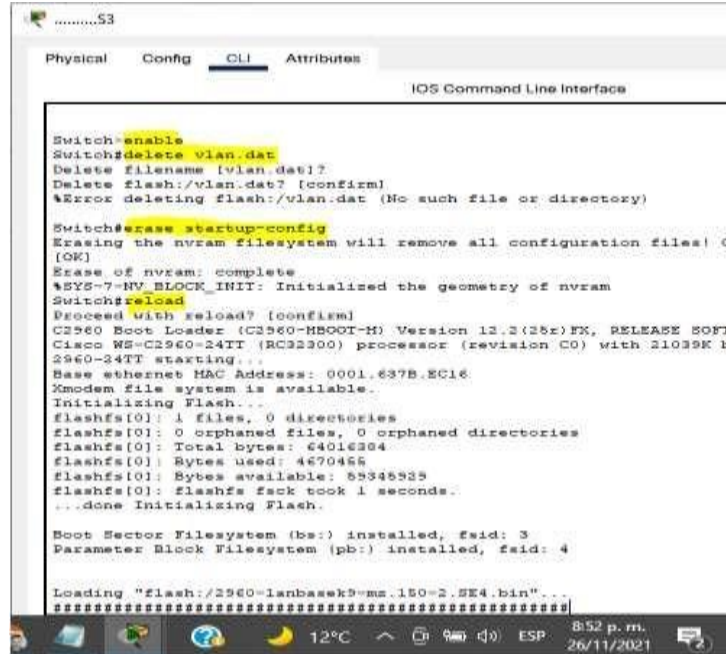
```
Switch>enable
Switch#show flash
Directory of flash:/

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

Fuente: Realizado por Victor Mauricio Delgado Peña

## Switch S3

Figura 31. Inicializar y volver a cargar S3



```
Switch>enable
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-MBOOT-M) Version 12.2(28z)FX, RELEASE SOFTWARE
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K b
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"...
*****
```

Fuente: Realizado por Victor Mauricio Delgado Peña

Figura 32. Verificar que la base de datos de VLAN no esté en la memoria flash en S3



```
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)
```

Fuente: Realizado por Victor Mauricio Delgado Peña

## 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):

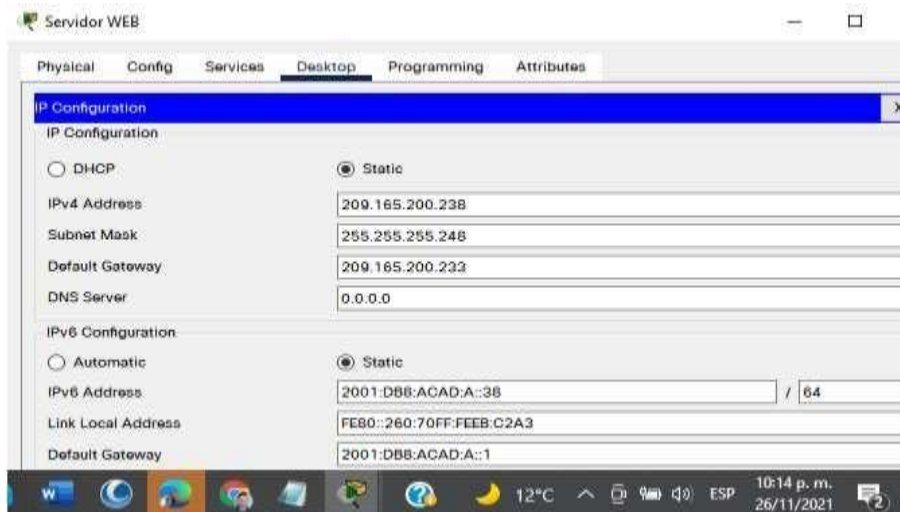
**Tabla 11. direccionamiento del servidor web**

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

Fuente: Realizado por Victor Mauricio Delgado Peña

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

Figura 33. Configuración de IP del servidor web



Fuente: Realizado por Victor Mauricio Delgado Peña

## Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

**Tabla 12. configuración de R1**

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config-line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd "Se prohíbe el acceso no autorizado"
Interfaz S0/0/0	R1(config)#interface serial0/2/0 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
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

*Fuente: Realizado por Victor Mauricio Delgado Peña*

**Nota:** Todavía no configure G0/1.

Figura 34. Configuración R1

```

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

Router>enable
Router#
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#service password-encryption
R1(config)#banner motd "Se prohbe el acceso no autorizado"
R1(config)#
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

R1(config-if)#
%LINK-S-CHANGED: Interface Serial0/2/0, changed state to up

R1(config-if)#
%LINEPROTO-S-UPDOWN: Line protocol on Interface Serial0/2/0, chang

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)#

```

Fuente: Realizado por Víctor Mauricio Delgado Peña

### Paso 3: Configurar R2

Las tareas de configuración para R1 incluyen las siguientes:

**Tabla 13. configuración de R2**

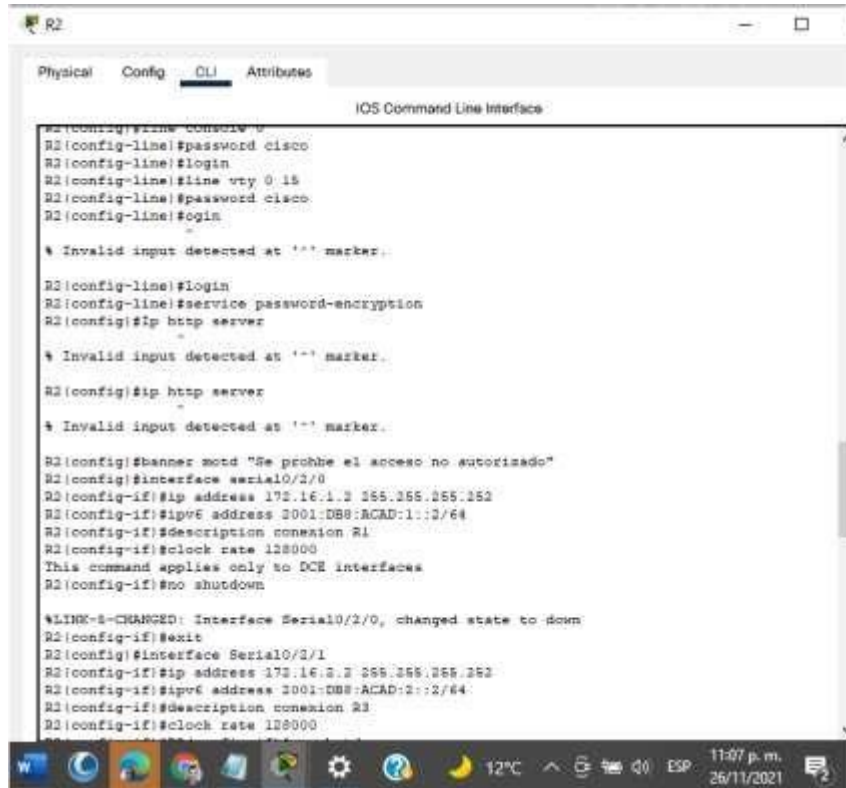
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login

Contraseña de acceso Telnet	R2(config-line)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	Ip http server
Mensaje MOTD	R2(config)#banner motd "Se prohíbe el acceso no autorizado"
Interfaz S0/2/0	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
Interfaz S0/2/1	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 R2(config-if)#exit
Interfaz G0/0 (simulación de Internet)	R2(config)#interface gigabitEthernet0/0 R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#description conexion servidor R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config)#interface 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.
Ruta predeterminada	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
--	---

Fuente: Realizado por Victor Mauricio Delgado Peña

Figura 35. Configuración R2



Fuente: Realizado por Victor Mauricio Delgado Peña

#### Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

**Tabla 14. configuración de R3**

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3

Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd "Se prohíbe el acceso no autorizado"
Interfaz S0/0/1	R3(config)#interface serial0/2/1 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#description conexion R2 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#description loopback 4 R3(config-if)#exit
Interfaz loopback 5	R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#description loopback 5 R3(config-if)#exit
Interfaz loopback 6	R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#description loopback 6 R3(config-if)#exit
Interfaz loopback 7	R3(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2 R3(config)# ipv6 route ::/0 2001:DB8:ACAD:2::2

Fuente: Realizado por Victor Mauricio Delgado Peña

Figura 36. Configuración R3

```

R3
Physical Config CLI Attributes
IOS Command Line Interface
R3(config-if)#ipve address 2001.255.255.1/24
R3(config-if)#description conexion R2
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/2/1, changed state to up

R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/1, change

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

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

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

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

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
    
```

Fuente: Realizado por Victor Mauricio Delgado Peña

### Paso 5: Configurar S1

**Tabla 15. configuración de S1**

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login

Contraseña de acceso Telnet	S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd "Se prohíbe el acceso no autorizado".

Fuente: Realizado por Victor Mauricio Delgado Peña

La configuración del S1 incluye las siguientes tareas:

Figura 37. Configuración S1

```

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

```

Fuente: Realizado por Victor Mauricio Delgado Peña

### **Tabla 16. configuración de S3**

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

Fuente: Realizado por Victor Mauricio Delgado Peña

Figura 38. Configuración S3

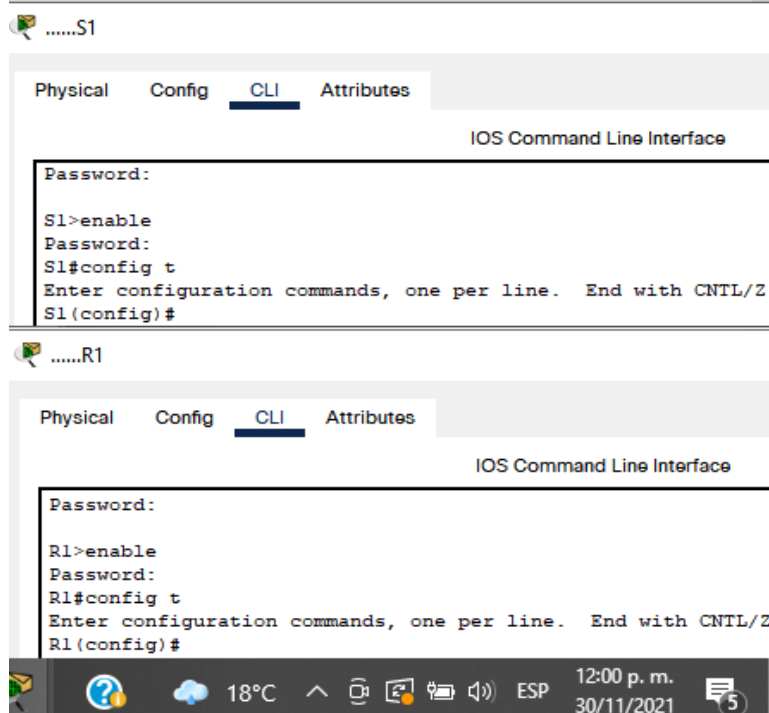
```

Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#service password-encryption
S3(config)#banner motd "Se prohíbe el acceso no autorizado"

```

Fuente: Realizado por Victor Mauricio Delgado Peña

Figura 39. Ingreso a switches y routers con contraseñas



Fuente: Realizado por Victor Mauricio Delgado Peña



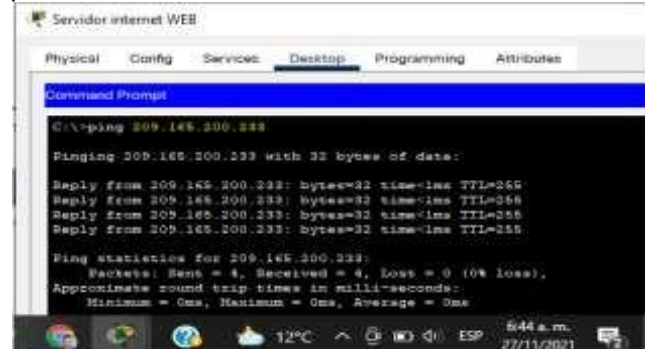
### Paso 7: Verificar la conectividad de la red

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 17. ping para probar la conectividad entre los dispositivos**

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	<p>Ping satisfactorio</p> <p><i>Figura 40. Ping R1 a R2, S0/0/0</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>
R2	R3, S0/0/1	172.16.2.1	<p>Ping satisfactorio</p> <p><b>Figura41.</b> Ping R2 a R3, S0/0/1</p>  <p><b>Fuente:</b> Realizado por Victor Mauricio Delgado Peña</p>
PC de Internet	Gateway predeterminado	209.165.200.233	<p>Ping satisfactorio</p> <p><i>Figura 42. Ping PC de Internet a Gateway predeterminado</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>

Fuente: Realizado por Victor Mauricio Delgado Peña


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

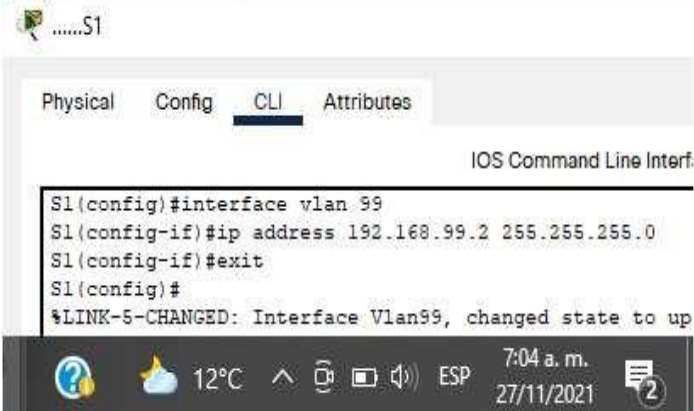
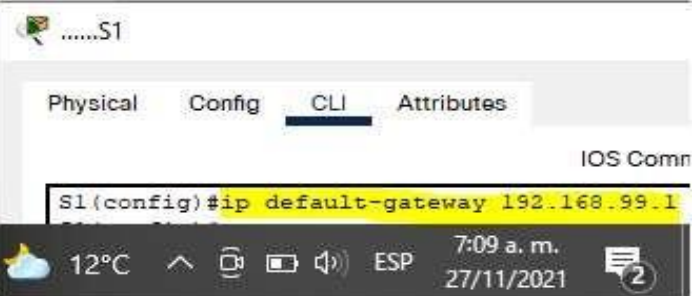
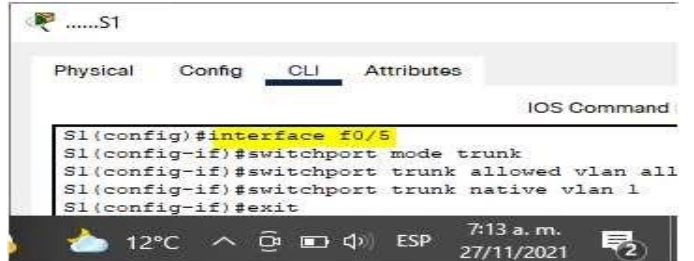
**Parte 3:** Configurar la seguridad del switch, las VLAN y el routing entre VLAN


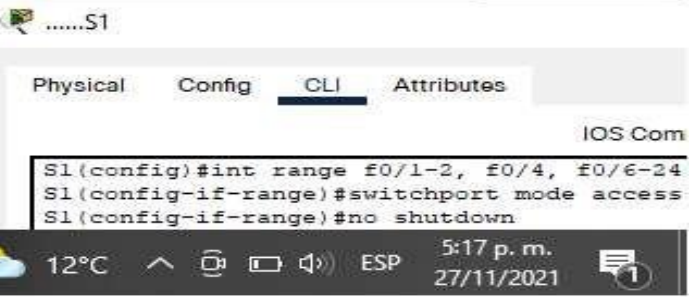
**Paso 1:** Configurar S1


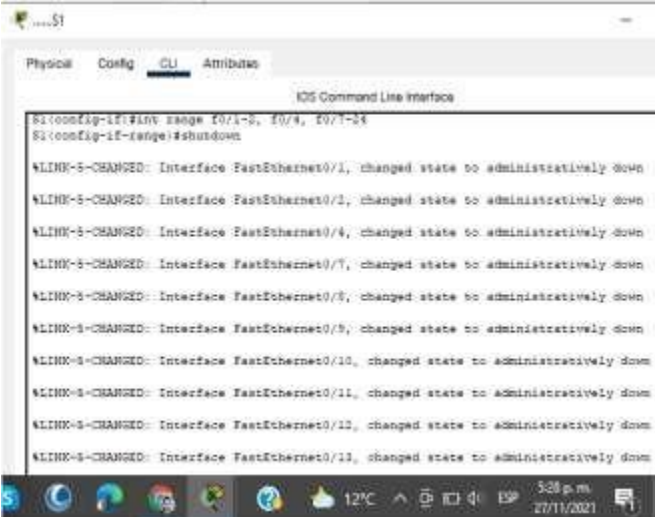
La configuración del S1 incluye las siguientes tareas:

**Tabla 18. : Configurar la seguridad del switch S1**

Elemento o tarea de configuración	Especificación
<p>Crear la base de datos de VLAN</p>	<pre>S1(config)#van 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>Figura 43. base de datos de VLAN</i></p>  <p>Fuente: Realizado por Victor Mauricio Delgado Peña</p>
<p>Asignar la dirección IP de administración</p>	<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>Figura 44. Asignar la dirección IP de administración</i></p>  <pre> .....S1  Physical  Config  CLI  Attributes  IOS Command Line Interf:  S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#exit S1(config)# %LINK-5-CHANGED: Interface Vlan99, changed state to up </pre> <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>
<p>Asignar el gateway predeterminado</p>	<p>S1(config)#ip default-gateway 192.168.99.1</p> <p><i>Figura 45. Asignar el gateway predeterminado</i></p>  <pre> .....S1  Physical  Config  CLI  Attributes  IOS Comn  S1(config)#ip default-gateway 192.168.99.1 </pre> <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></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>Figura 46. Forzar el enlace troncal en la interfaz F0/5</i></p>  <pre> .....S1  Physical  Config  CLI  Attributes  IOS Command  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>Fuente: Realizado por Victor Mauricio Delgado Peña</i></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>Figura 47. Forzar el enlace troncal en la interfaz F0/3</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></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>Figura 48. Configurar el resto de los puertos como puertos de acceso</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></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>Figura 49. Asignar F0/6 a la VLAN 21</i></p>

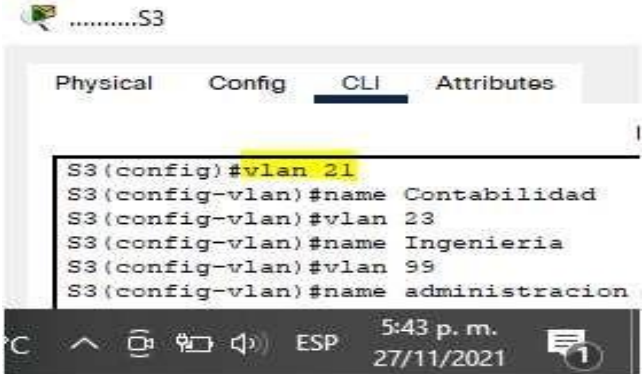

	 <p>.....S1</p> <p>Physical Config <b>CLI</b> Attributes</p> <p>IOS C</p> <pre>S1(config)#int f0/6 S1(config-if)#switchport access vlan 21</pre> <p>12°C ^ [network icons] ESP 5:24 p. m. 27/11/2021 [notification icon]</p> <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>
<p>Apagar todos los puertos sin usar</p>	<p>S1(config)#int range f0/1-2, f0/4, f0/7-24 S1(config-if-range)#shutdown</p> <p><i>Figura 50. Apagar todos los puertos sin usar</i></p>  <p>.....S1</p> <p>Physical Config <b>CLI</b> Attributes</p> <p>IOS Command Line Interface</p> <pre>S1(config-if-range)#int range f0/1-2, f0/4, f0/7-24 S1(config-if-range)#shutdown  %LINK-3-CHANGED: Interface FastEthernet0/1, changed state to administratively down %LINK-3-CHANGED: Interface FastEthernet0/2, changed state to administratively down %LINK-3-CHANGED: Interface FastEthernet0/4, changed state to administratively down %LINK-3-CHANGED: Interface FastEthernet0/7, changed state to administratively down %LINK-3-CHANGED: Interface FastEthernet0/8, changed state to administratively down %LINK-3-CHANGED: Interface FastEthernet0/9, changed state to administratively down %LINK-3-CHANGED: Interface FastEthernet0/10, changed state to administratively down %LINK-3-CHANGED: Interface FastEthernet0/11, changed state to administratively down %LINK-3-CHANGED: Interface FastEthernet0/12, changed state to administratively down %LINK-3-CHANGED: Interface FastEthernet0/13, changed state to administratively down</pre> <p>Windows taskbar: 12°C ^ [network icons] ESP 5:28 p. m. 27/11/2021 [notification icon]</p> <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>


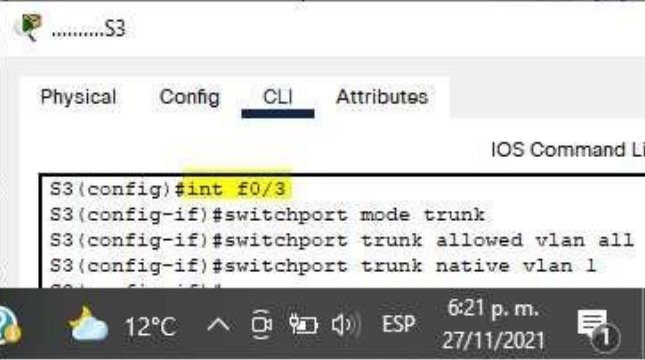
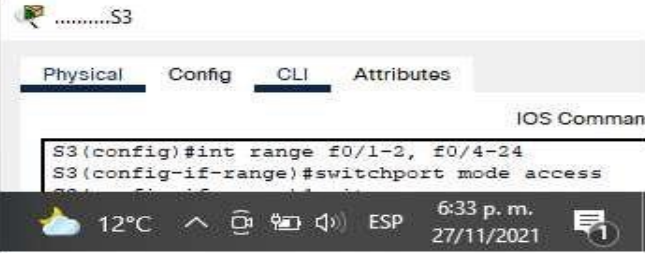
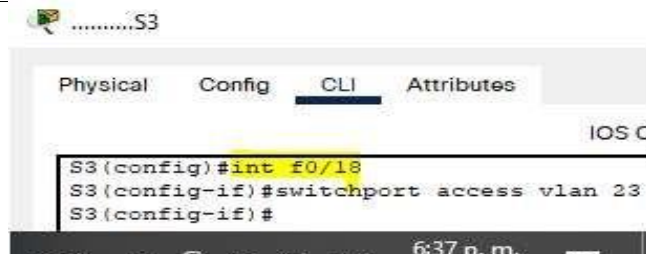
*Fuente: Realizado por Victor Mauricio Delgado Peña*

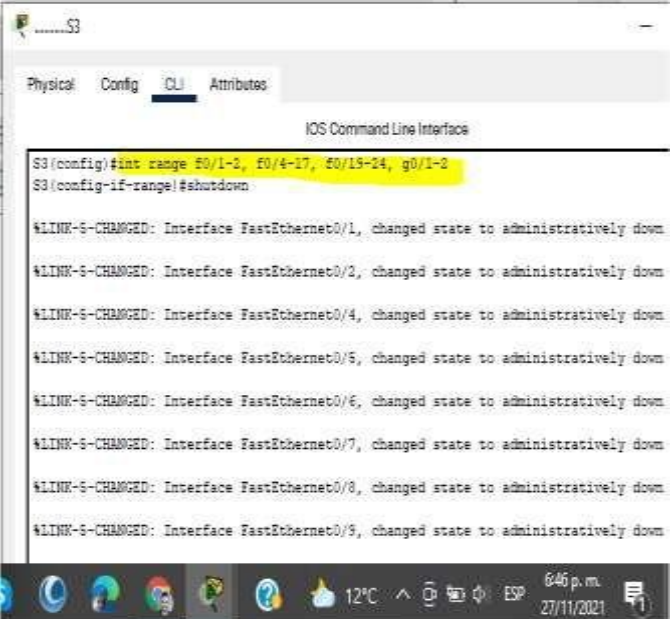
**Paso 2:** Configurar el S3

La configuración del S3 incluye las siguientes tareas:

**Tabla 19.: Configurar la seguridad del switch 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 23 S3(config-vlan)#name Ingenieria S3(config)#vlan 99 S3(config-vlan)#name administraci3n</pre> <p><i>Figura 51. Crear la base de datos de VLAN en S3</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>
<p>Asignar la direcci3n IP de administraci3n</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>Figura52. Asignar la direcci3n IP de administraci3n</i></p> 

<p>Asignar el gateway predeterminado</p>	<p>S3(config)#ip default-gateway 192.168.99.1</p> <p><i>Figura 53. Asignar el gateway predeterminado</i></p>  <p>Fuente: Realizado por Victor Mauricio Delgado Peña</p>
	<p>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</p> <p><i>Figura 54. Forzar el enlace troncal en la interfaz F0/3</i></p>  <p>Fuente: Realizado por Victor Mauricio Delgado Peña</p>
<p>Configurar el resto de los puertos como puertos de acceso</p>	<p>S3(config)#int range f0/1-2, f0/4-24  S3(config-if-range)#switchport mode access</p> <p><i>Figura 55. Configurar el resto de los puertos como puertos de acceso</i></p>  <p>Fuente: Realizado por Victor Mauricio Delgado Peña</p>
<p>Asignar F0/18 a la VLAN 21</p>	<p>S3(config)#int f0/18  S3(config-if)#switchport access vlan 23</p> <p><i>Figura 56. Asignar F0/18 a la VLAN 21.</i></p> 


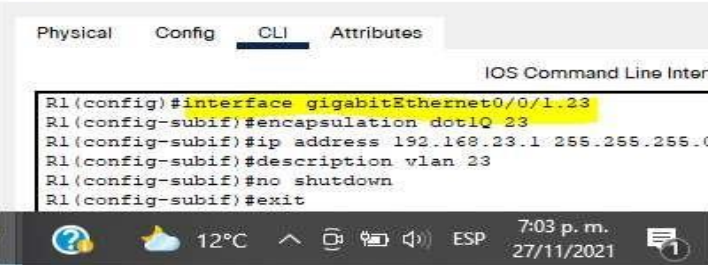
	<p>Fuente: Realizado por Victor Mauricio Delgado</p>
<p><i>Apagar todos los puertos sin usar</i></p>	<pre>S3(config)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown</pre> <p><i>Figura 57. Apagar todos los puertos sin usar</i></p>  <p>Fuente: Realizado por Victor Mauricio Delgado</p>


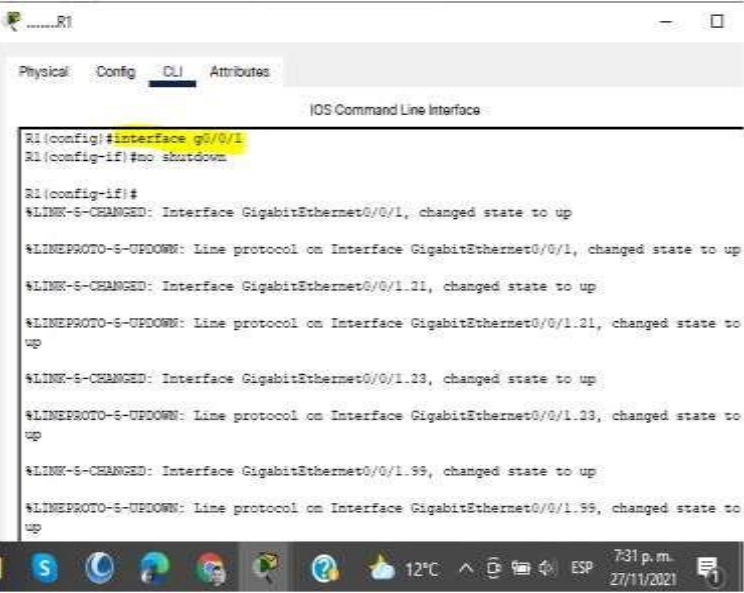
Fuente: Realizado por Victor Mauricio Delgado Peña

### Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

#### **Tabla 20.: Configurar la seguridad del Router R1**

Elemento o tarea de configuración	Especificación
<p>Configurar la subinterfaz 802.1Q .21 en G0/1</p>	<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>Figura 58. Configurar la subinterfaz 802.1Q .21 en G0/1</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado</i></p>
<p>Configurar la subinterfaz 802.1Q .23 en G0/1</p>	<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>Figura 59. Configurar la subinterfaz 802.1Q .23 en G0/1</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado</i></p>

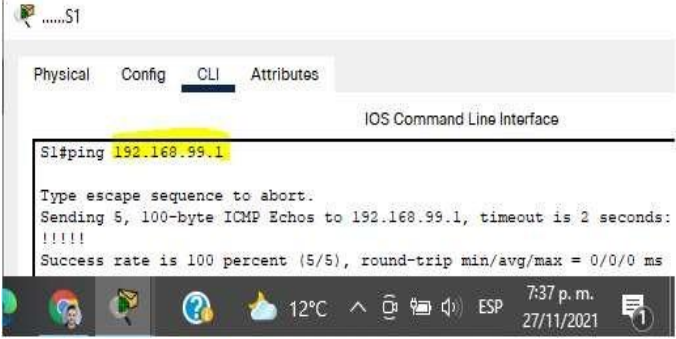
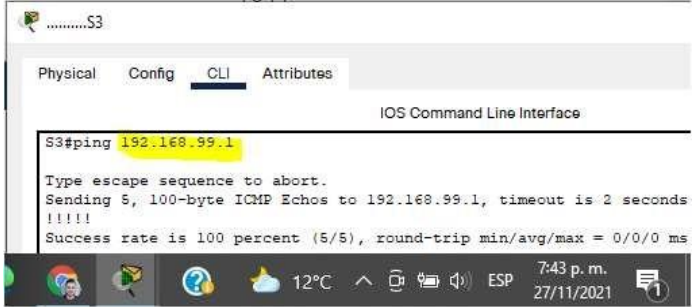
<p>Configurar la subinterfaz 802.1Q .99 en G0/1</p>	<pre>R1(config)#interface g0/0/1.99 R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#description vlan 99 R1(config-subif)#no shutdown R1(config-subif)#exit</pre> <p><i>Figura 60. Configurar la subinterfaz 802.1Q .99 en G0/1</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>
<p>Activar la interfaz G0/1</p>	<pre>R1(config)#interface g0/0/1 R1(config-if)#no shutdown</pre> <p><i>Figura 61 Activar la interfaz G0/1</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>

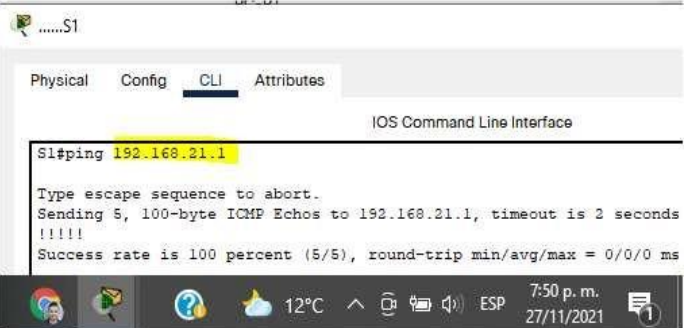
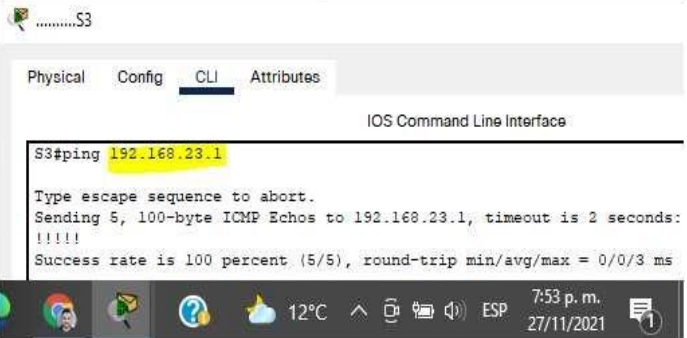
*Fuente: Realizado por Victor Mauricio Delgado Peña*

#### 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 21.: Verificación de la conectividad de la red**

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	<p>Ping satisfactorio</p> <p><i>Figura 62 Ping S1 a VLAN 99 de R1</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>
S3	R1, dirección VLAN 99	192.168.99.1	<p>Ping satisfactorio</p> <p><i>Figura 63 Ping S3 a VLAN 99 de R1</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>
S1	R1, dirección VLAN 21	192.168.21.1	<p>Ping satisfactorio</p>

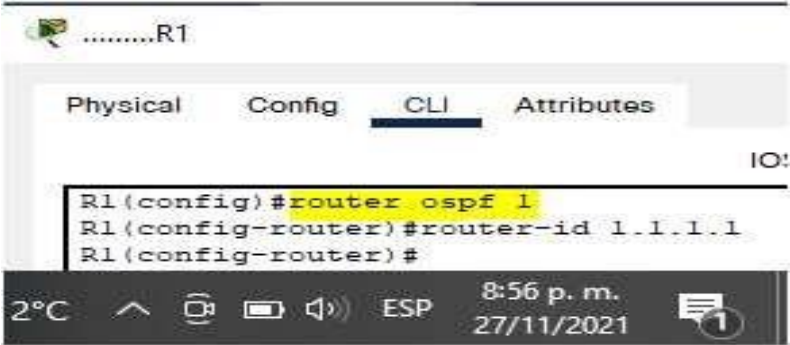
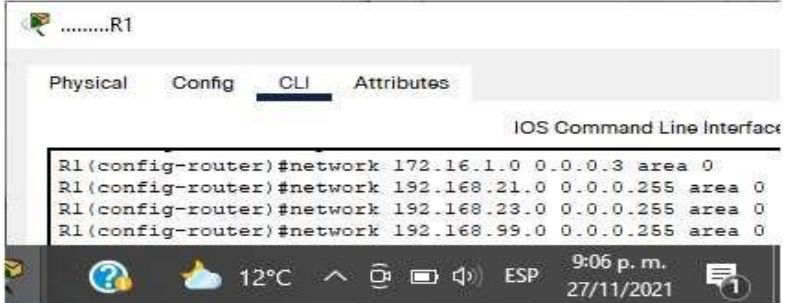
			<p><b>Figura 64 Ping S1 a VLAN 21 de R1</b></p>  <p>Fuente: Realizado por Victor Mauricio Delgado Peña</p>
S3	R1, dirección VLAN 23	192.168.23.1	<p><b>Ping satisfactorio</b></p> <p><b>Figura 65 Ping S3 a VLAN 23 de R1</b></p>  <p>Fuente: Realizado por Victor Mauricio Delgado Peña</p>

## 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 21.: Configurar OSPF en el R1**

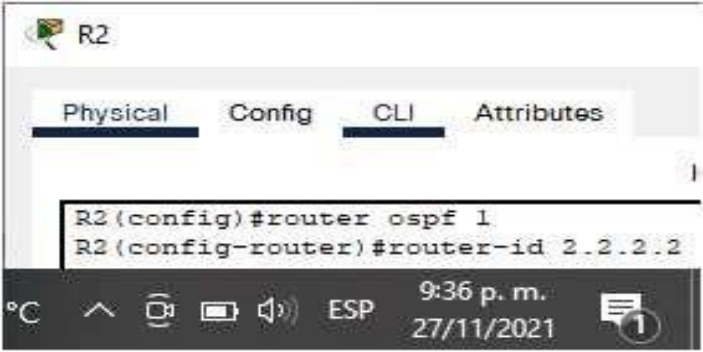
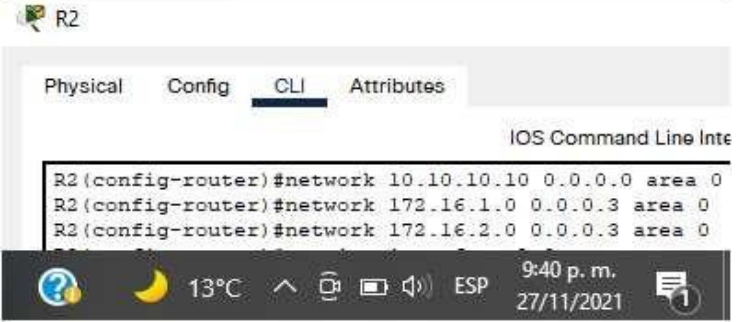
Elemento o tarea de configuración	Especificación
<p>Configurar OSPF área 0</p>	<p>R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1</p> <p><i>Figura 66 Configuración OSPF área 0 R1</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>
<p>Anunciar las redes conectadas directamente</p>	<p>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</p> <p><i>Figura67 Anunciar las redes conectadas directamente</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>
<p>Establecer todas las interfaces LAN como pasivas</p>	<p>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</p>

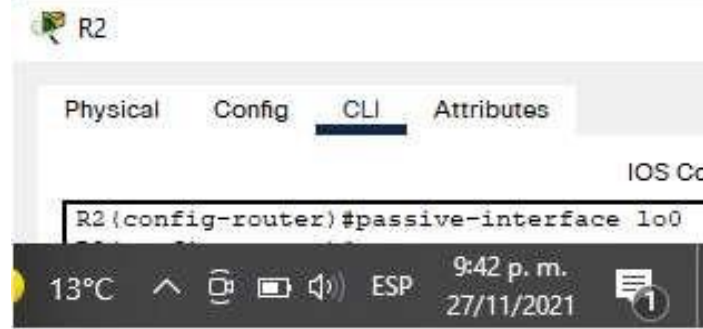
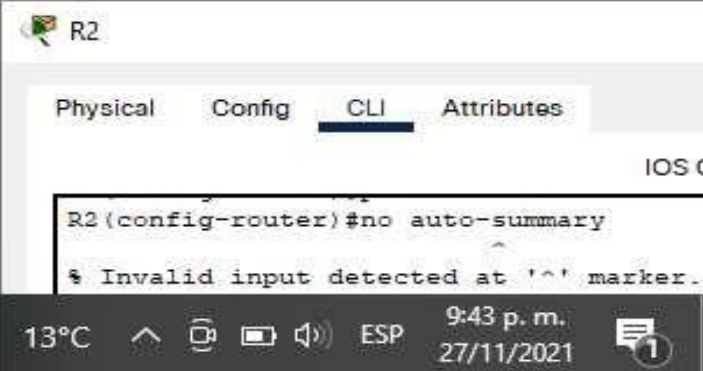
	<p><i>Figura68 Establecer todas las interfaces LAN como pasivas</i></p>  <p>The screenshot shows the CLI interface for router R1. The 'CLI' tab is selected. The command history shows the following commands being entered: <code>passive-interface g0/0/1.21</code>, <code>passive-interface g0/0/1.23</code>, and <code>passive-interface g0/0/1.99</code>. The prompt is <code>R1(config-router)#</code>. The system tray at the bottom shows a temperature of 12°C and the date 27/11/2021 at 9:12 p.m.</p> <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>
<p>Desactive la sumarización automática</p>	<p>R1(config-router)#no auto-summary</p> <p><i>Figura69 Desactivar la sumarización automática</i></p>  <p>The screenshot shows the CLI interface for router R1. The 'CLI' tab is selected. The command history shows the command <code>no auto-summary</code> being entered. The prompt is <code>R1(config-router)#</code>. Below the command, an error message is displayed: <code>% Invalid input detected at '^' marker.</code>. The system tray at the bottom shows a temperature of 13°C and the date 27/11/2021 at 9:23 p.m.</p> <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>

## Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

**Tabla 22.: Configurar OSPF en el R2**

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	<p>R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2</p> <p><i>Figura70 Configurar OSPF área 0 R2</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>
Anunciar las redes conectadas directamente	<p>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</p> <p><i>Figura71 Anunciar las redes conectadas directamente a R2</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>
Establecer la interfaz LAN (loopback) como pasiva	<p>R2(config-router)#passive-interface lo0</p>


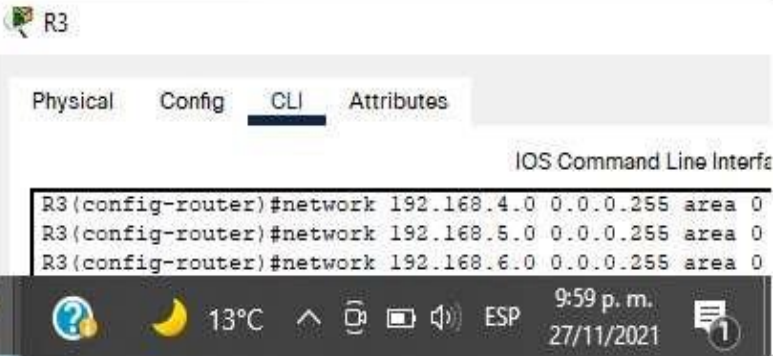
	<p><i>Figura72 Establecer la interfaz LAN (loopback) como pasiva</i></p>  <p>Fuente: Realizado por Victor Mauricio Delgado Peña</p>
<p>Desactive la sumarización automática</p>	<p>R1(config-router)#no auto-summary</p> <p><i>Figura73 Desactivación de la sumarización automática</i></p>  <p>Fuente: Realizado por Victor Mauricio Delgado Peña</p>

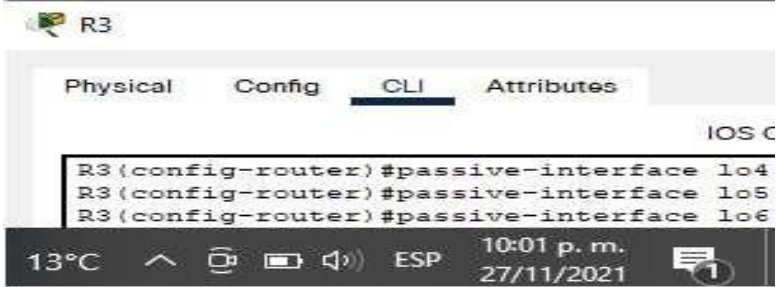
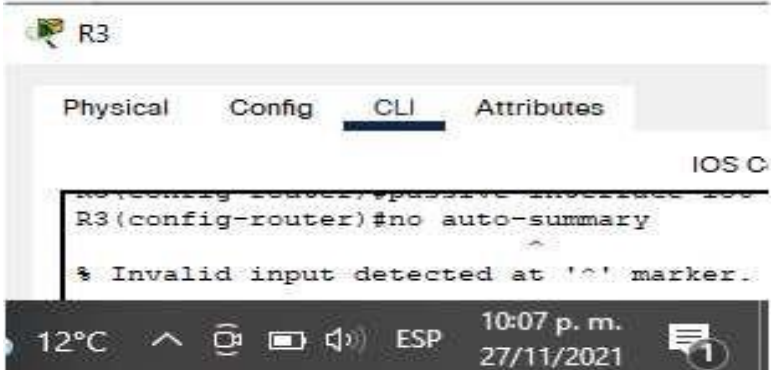
Fuente: Realizado por Victor Mauricio Delgado Peña

### Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

**Tabla 23.: Configurar OSPFv3 en el R3**

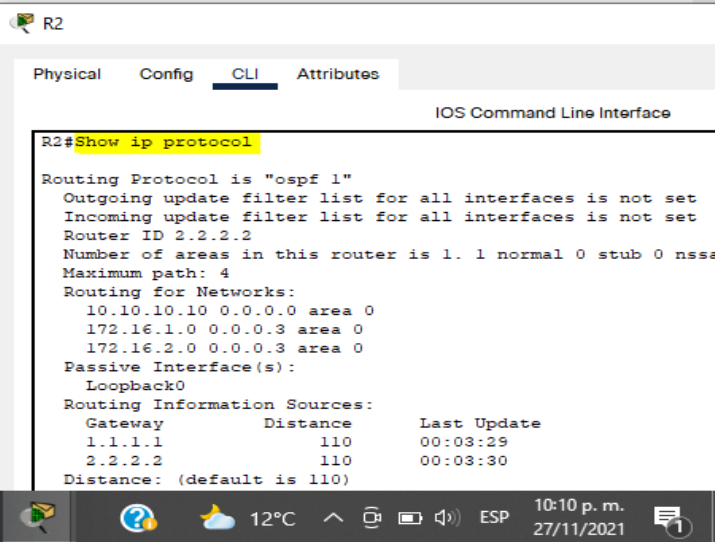

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	<p>R3(config)#router ospf 1 R3(config-router)#router-id 3.3.3.3</p> <p><i>Figura74 Configurar OSPF área 0 R3</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>
Anunciar redes IPv4 conectadas directamente	<p>R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0</p> <p><b>Figura75</b> Anunciar redes IPv4 conectadas directamente R3</p>  <p><b>Fuente:</b> Realizado por Victor Mauricio Delgado Peña</p>
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	<p>R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6</p>

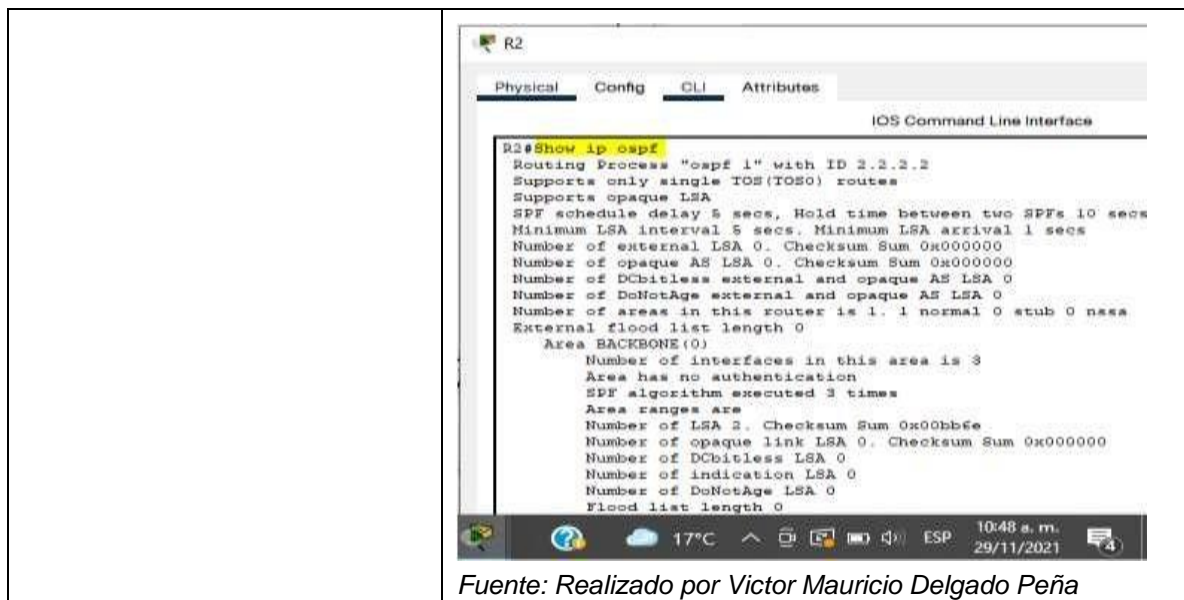
	<p><i>Figura76 Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas</i></p> <hr/>  <p>Fuente: Realizado por Victor Mauricio Delgado Peña</p>
<p>Desactive la sumarización automática.</p>	<p>R1(config-router)#no auto-summary</p> <p><i>Figura77 Desactive la sumarización automática.R3</i></p> <hr/>  <p>Fuente: Realizado por Victor Mauricio Delgado Peña</p>

#### **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 24.: Verificar la información de OSPF**

Pregunta	Respuesta
<p>¿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>	<p>Comando: <b>Show ip protocol</b></p> <p><i>Figura78 ID del proceso OSPF e interfaces router</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>
<p>¿Qué comando muestra solo las rutas OSPF?</p>	<p>Comando: Show ip route ospf</p> <p><i>Figura79 comando muestra solo las rutas OSPF</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>
<p>¿Qué comando muestra la sección de OSPF de la configuración en ejecución?</p>	<p>Show ip ospf</p> <p><i>Figura80 sección de OSPF de la configuración en ejecución</i></p>



Fuente: Realizado por Victor Mauricio Delgado Peña

## 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 25.: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23**

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	<p>R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20</p> <p><i>Figura81 primeras 20 direcciones IP en la VLAN 21 Reservadas</i></p> <p>R1</p> <p>Physical Config CLI Attributes</p> <p>IOS Command Line Interface</p> <pre>R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20</pre> <p>18°C 11:09 a.m. 29/11/2021</p> <p>Fuente: Realizado por Victor Mauricio Delgado Peña</p>

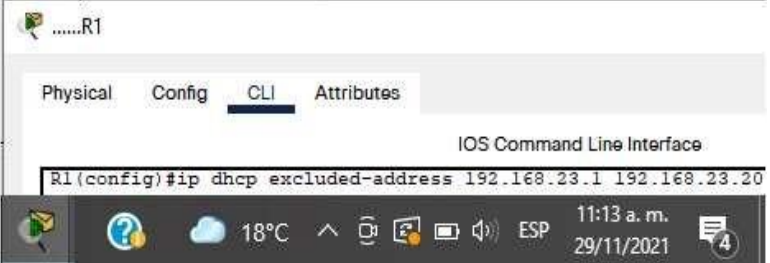
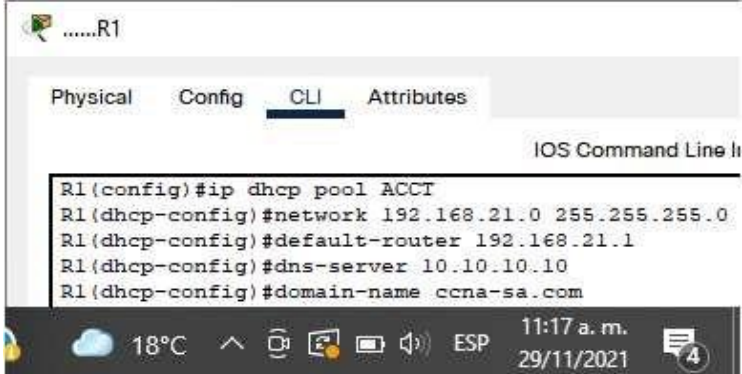
<p>Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas</p>	<pre>R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20</pre> <p><i>Figura82 primeras 20 direcciones IP en la VLAN 23 Reservadas</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>
<p>Crear un pool de DHCP para la VLAN 21.</p>	<pre>R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com</pre> <p><i>Figura83 Crear un pool de DHCP para la VLAN 21.</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>
<p>Crear un pool de DHCP para la VLAN 23</p>	<pre>R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com</pre>

Figura84 Crear un pool de DHCP para la VLAN 23




Fuente: Realizado por Victor Mauricio Delgado Peña

Fuente: Realizado por Victor Mauricio Delgado Peña

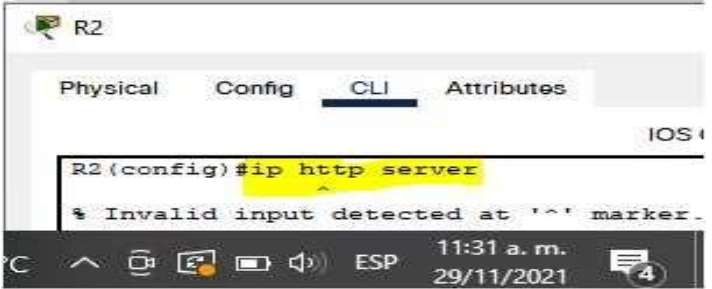
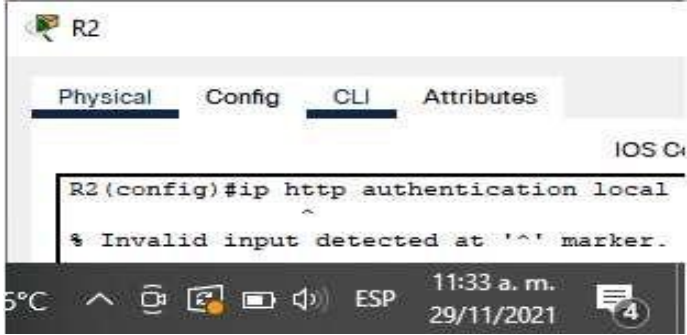

## Paso 2: Configurar la NAT estática y dinámica en el R2

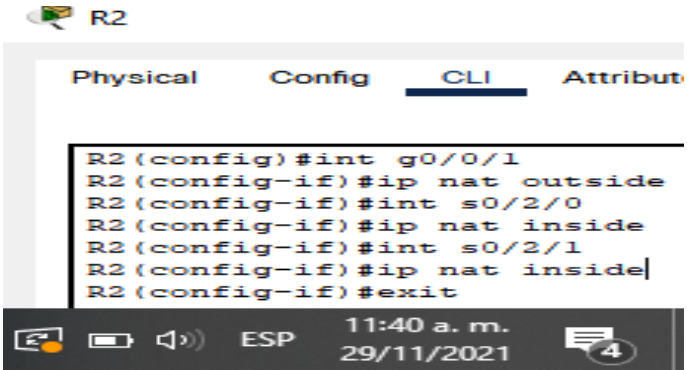
La configuración del R2 incluye las siguientes tareas:

**Tabla 26.: Configurar la NAT estática y dinámica en el R2**

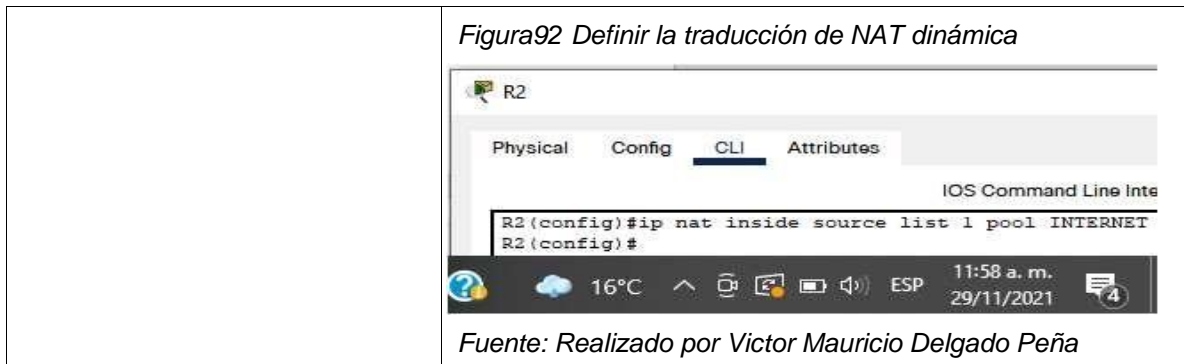
Elemento o tarea de configuración	Especificación
<p>Crear una base de datos local con una cuenta de usuario</p>	<p>Nombre de usuario: <b>webuser</b>                      Contraseña: <b>cisco12345</b>                      Nivel de privilegio: <b>15</b>                      Código:                      R2(config)#username webuser privilege 15 secret 5 cisco12345</p> <p><i>Figura85 Crear una base de datos local con una cuenta de usuario</i></p> 
<p>Habilitar el servicio del servidor HTTP</p>	<p><b>Código:</b> R2(config)#ip http server                      Comando no soportado</p>

Fuente: Realizado por Victor Mauricio Delgado Peña

	<p><i>Figura86 Habilitar el servicio del servidor HTTP</i></p>  <p>Fuente: Realizado por Victor Mauricio Delgado Peña</p>
<p>Configurar el servidor HTTP para utilizar la base de datos local para la autenticación</p>	<p><b>Codigo:</b>  R2(config)#ip http authentication local  Comando no soportado</p> <p><i>Figura87 Habilitar el servicio del servidor HTTP</i></p>  <p>Fuente: Realizado por Victor Mauricio Delgado Peña</p>
<p>Crear una NAT estática al servidor web.</p>	<p>Dirección global interna: <b>209.165.200.229</b>  R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229</p> <p><i>Figura88 Crear una NAT estática al servidor web</i></p>  <p>Fuente: Realizado por Victor Mauricio Delgado Peña</p>

<p>Asignar la interfaz interna y externa para la NAT estática</p>	<pre>R2(config)#int g0/0/1 R2(config-if)#ip nat outside R2(config-if)#int s0/2/0 R2(config-if)#ip nat inside R2(config-if)#int s0/2/1 R2(config-if)#ip nat inside R2(config-if)#exit</pre> <p><i>Figura89 Asignar la interfaz interna y externa para la NAT estática</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</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  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</pre>

	<p>R2(config)#access-list 1 permit 2001:DB8:ACAD:3::1 0.0.3.255</p> <p><i>Figura90 Configurar la NAT dinámica dentro de una ACL privada</i></p> <hr/>  <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>
<p>Defina el pool de direcciones IP públicas utilizables.</p>	<p>Nombre del conjunto: <b>INTERNET</b> El conjunto de direcciones incluye: <b>209.165.200.225 – 209.165.200.228</b></p> <p><b>Codigo:</b> R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.28</p> <p><i>Figura91 Defina el pool de direcciones IP públicas utilizables</i></p> <hr/>  <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>
<p>Definir la traducción de NAT dinámica</p>	<p>R2(config)#ip nat inside source list 1 pool INTERNET</p>

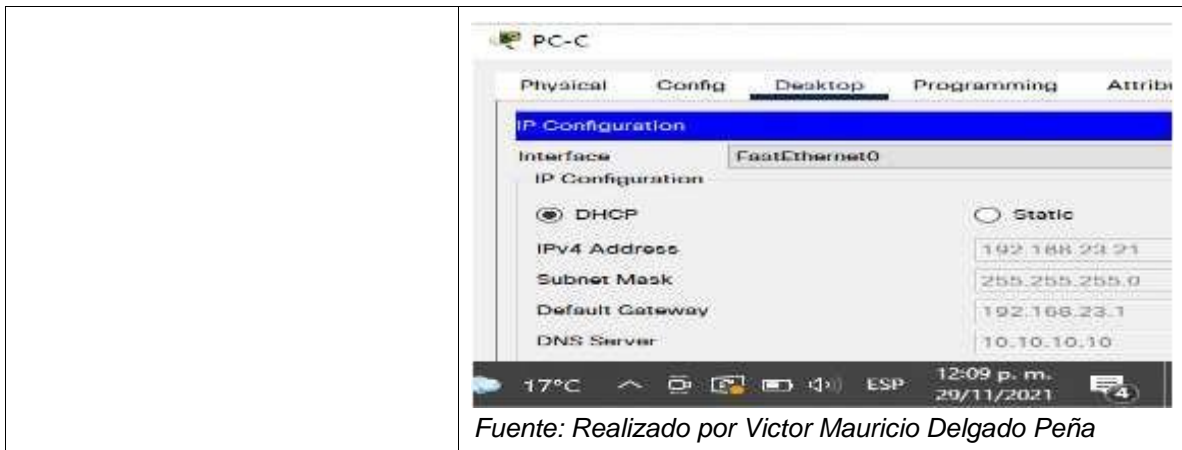


### Paso 3: Verificar el protocolo DHCP y la NAT estática

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 27.: Verificar el 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>Figura93 Verificar que la PC-A haya adquirido información de IP del servidor de DHCP</i></p> <p><i>Fuente: Realizado por Victor Mauricio Delgado Peña</i></p>
<p>Verificar que la PC-C haya adquirido información de IP del servidor de DHCP</p>	<p><i>Figura94 Verificar que la PC-C haya adquirido información de IP del servidor de DHCP</i></p>

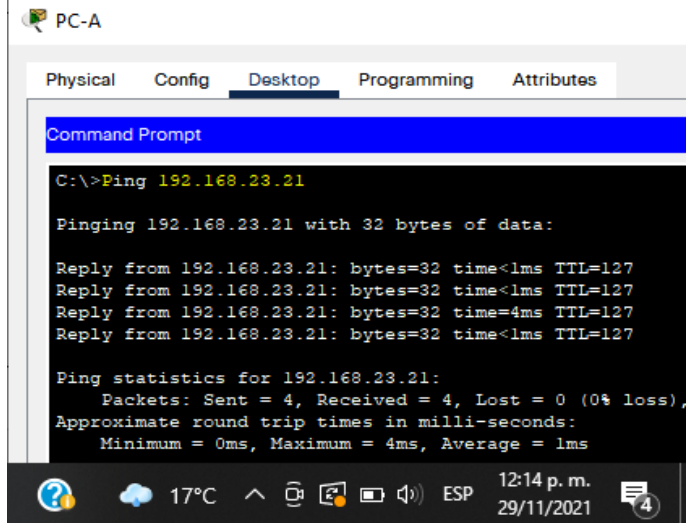


Fuente: Realizado por Victor Mauricio Delgado Peña

Verificar que la PC-A pueda hacer ping a la PC-C  
**Nota:** Quizá sea necesario deshabilitar el firewall de la PC.

Ping 192.168.23.21-Satisfactorio

Figura95 ping PC-A a PC-C



Fuente: Realizado por Victor Mauricio Delgado Peña

Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**

Figura96 acceder al servidor web (209.165.200.229)





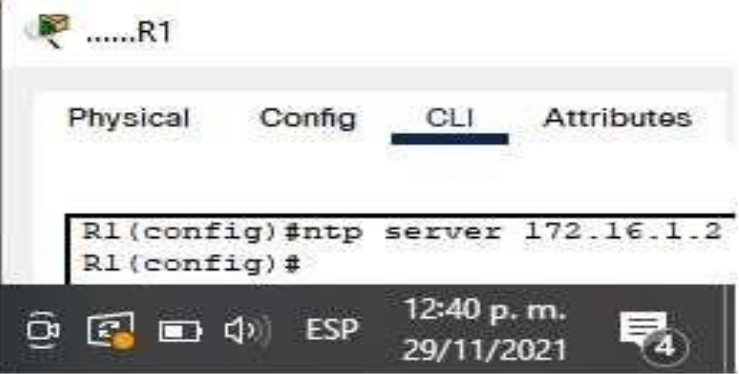
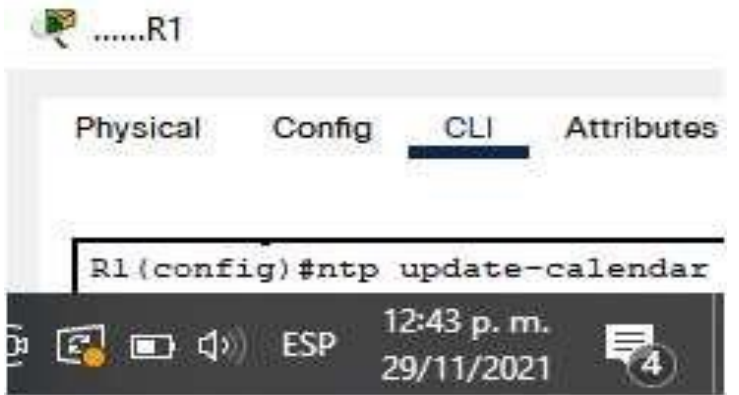
Fuente: Realizado por Victor Mauricio Delgado Peña

Fuente: Realizado por Victor Mauricio Delgado Peña

## Parte 6: Configurar NTP

**Tabla 28.: Configuración NTP**

Elemento o tarea de configuración	Especificación
<p>Ajuste la fecha y hora en R2.</p>	<p><b>5 de marzo de 2016, 9 a. m.</b></p> <p><b>Código:</b> R2#clock set 09:00:00 05 march 2016</p> <p><i>Figura97 Ajuste la fecha y hora en R2.</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado</i></p>
<p>Configure R2 como un maestro NTP.</p>	<p><b>Nivel de estrato: 5</b></p> <p><b>Código:</b> R2(config)#ntp master 5</p> <p><i>Figura98 Configure R2 como un maestro NTP.</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado</i></p>

<p>Configurar R1 como un cliente NTP.</p>	<p>Servidor: <b>R2</b></p> <p><b>Código:</b> R1(config)#ntp server 172.16.1.2</p> <p><i>Figura99 Configurar R1 como un cliente NTP.</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado</i></p>
<p>Configure R1 para actualizaciones de calendario periódicas con hora NTP.</p>	<p>R1(config)#ntp update-calendar</p> <p><i>Figura100 R1 para actualizaciones de calendario periódicas con hora NTP.</i></p>  <p><i>Fuente: Realizado por Victor Mauricio Delgado</i></p>
<p>Verifique la configuración de NTP en R1.</p>	<p>R1#show ntp associations</p> <p><i>Figura101 Verifique la configuración de NTP en R1.</i></p>



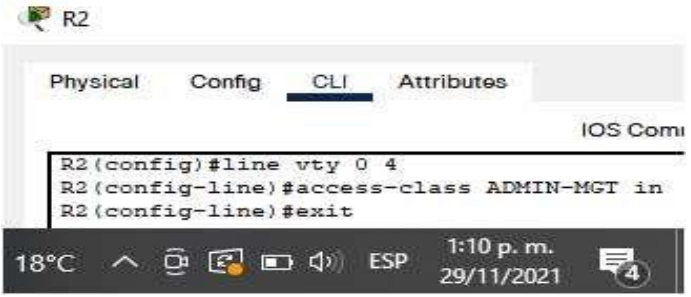

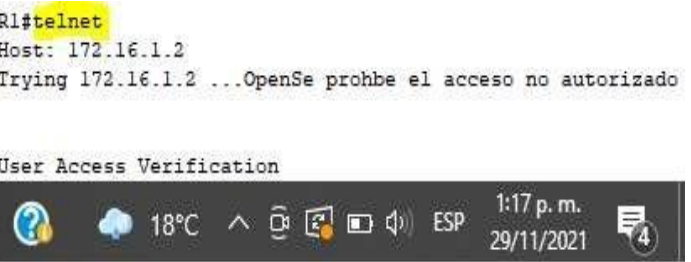
Fuente: Realizado por Victor Mauricio Delgado Peña

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

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

**Tabla 29.: Restricción del acceso a las líneas VTY en el R2**

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	<p>Nombre de la ACL: <b>ADMIN-MGT</b></p> <p>Código:</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>Figura102 R1 conexión Telnet con R2.</i></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>Fuente: Realizado por Víctor Mauricio Delgado</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 103 Aplicar la ACL con nombre a las líneas VTY</i></p>  <p>Fuente: Realizado por Víctor Mauricio Delgado</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 104 Permitir acceso por Telnet a las líneas de VTY</i></p>  <p>Fuente: Realizado por Víctor Mauricio Delgado</p>
<p>Verificar que la ACL funcione como se espera</p>	<pre>R1&gt;telnet Host: 172.16.1.2</pre> <p><i>Figura 105 Verificar que la ACL funcione como se espera</i></p>  <p>Fuente: Realizado por Víctor Mauricio Delgado</p>

Fuente: Realizado por Victor Mauricio Delgado Peña

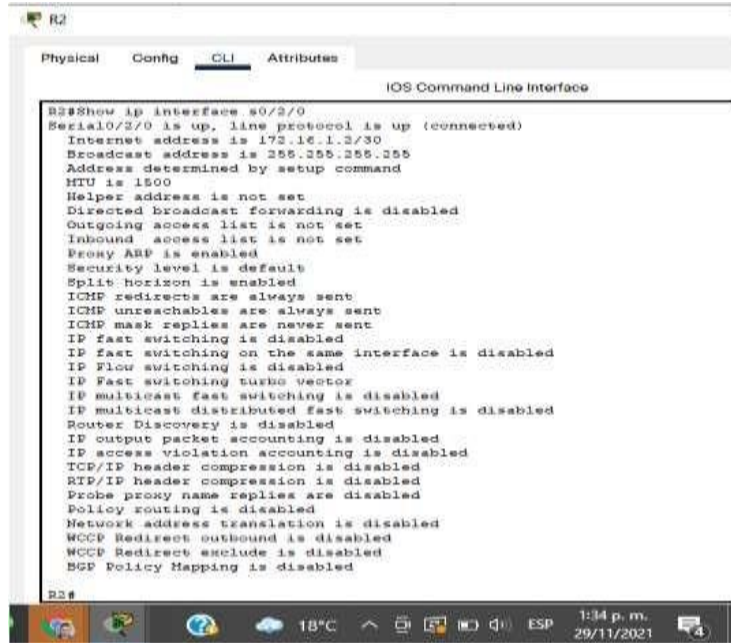
**Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente**

**Tabla 30.: Restricción del acceso a las líneas VTY en el R2**

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>R2#Show ip access-list</p> <p><i>Figura 106 lista de acceso</i></p>  <p>Fuente: Realizado por Víctor Mauricio Delgado</p>
<p>Restablecer los contadores de una lista de acceso</p>	<p>R2#Clear access-list counters</p> <p><i>Figura 107 Restablecer los contadores de una lista de acceso</i></p>  <p>Fuente: Realizado por Víctor Mauricio Delgado</p>
<p>¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la</p>	<p>R2#Show ip interface s0/2/0</p>

dirección en que se aplica?

Figura108 mostrar qué ACL



Fuente: Realizado por Víctor Mauricio Delgado

¿Con qué comando se muestran las traducciones NAT?

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

R2#Show ip nat translations

Figura109 traducciones NAT

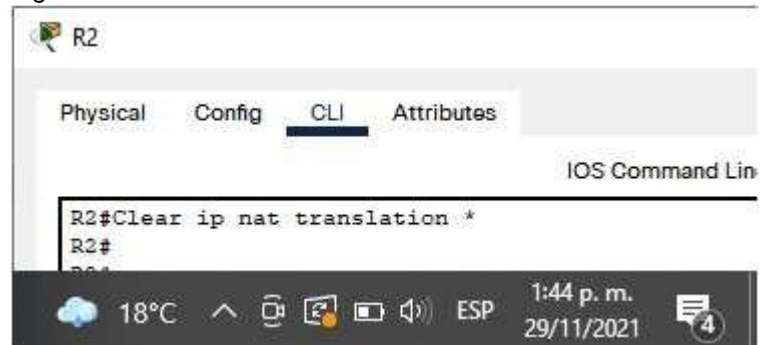


Fuente: Realizado por Víctor Mauricio Delgado

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

R2#Clear ip nat translation \*

Figura 110 eliminar las traducciones de NAT dinámicas



Fuente: Realizado por Víctor Mauricio Delgado

## CONCLUSIONES

El Subneteo o más conocido como Subnetting nos permite una mejor administración, y un mayor control del tráfico mejorando la seguridad al segmentar red en subredes, nos sirve para controlar el tamaño de las redes, en tamaño en cuanto a los hosts permitido dentro de la misma.

Si tenemos activo las búsquedas DNS en Router o Swich, provoca retrasos y esto puede resultar perjudicial para el usuario. Por ejemplo, si escribiera una URL incorrecta.

Las direcciones IP es la identificación de cada dispositivo el cual lo diferencia del uno al otro, es decir: es como el número de cedula de una persona que lo hace único e irrepetible

La máscara de subred o el prefijo se utilizan para determinar la porción de red de una dirección IP. Una vez implementada, una red IP debe ser probada para verificar su conectividad y rendimiento operativo.

el procesamiento de paquetes por parte de las ACL, Las entradas deny any implícitas rechazan cualquier paquete que no coincide con una ACE, los paquetes pueden rechazarse o reenviarse según lo indique la ACE con la que coincidan.

En la RAM se almacenan las direcciones MAC dinámicamente aprendidas cuando el aprendizaje persistente está habilitado con el comando `switchport port-security mac-address sticky`

Una diferencia entre usar Telnet o SSH para conectarse a un dispositivo de red con fines de administración, Telnet envía un nombre de usuario y una contraseña en texto sin formato, mientras que SSH cifra el nombre de usuario y la contraseña

El uso de Fast Ethernet full-duplex, El rendimiento se mejora con el flujo de datos bidireccional.

## BIBLIOGRAFÍA

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

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

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

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

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