SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

JOSE ANGEL GUERRERO MONTAÑEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
PROGRAMA INGENIERÍA DE SISTEMAS
BOGOTA
2020

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

JOSE ANGEL GUERRERO MONTAÑEZ

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR EL TÍTULO DE INGENIERO DE SISTEMAS

DIEGO EDINSON RAMIREZ
INGENIERO ELECTRÓNICO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
PROGRAMA INGENIERÍA DE SISTEMAS
BOGOTA
2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Ciudad y Fecha (día, mes, año) (Fecha de entrega)

AGRADECIMIENTOS

Agradezco en primera medida a Dios por brindarme la vida y permitirme la oportunidad de crecer como persona íntegra así como profesionalmente, a mi esposa, hijos, madre, hermanos y demás familiares por el apoyo, paciencia y amor incondicional que me han brindado durante toda la etapa académica que inicie años atrás, a cada uno de los tutores de la UNAD por estar pendiente de todo nuestro proceso formativo en su totalidad impulsando nuestro conocimiento con su apoyo y con sus experiencias vividas en los diferentes aspectos académicos, personales y sociales, al Ingeniero Diego Edinson Ramírez tutor del diplomado CISCO por su total comprensión, así como su total entrega para transmitir sus conocimientos y experiencias en aras de una excelente formación de cada uno de los educandos bajo su tutoría, logrando fortalecer los aspectos y competencias formativas así como personales y sociales de cada uno de nosotros mediante sus valiosas apreciaciones e indicaciones en temas académicos logrando establecernos como personas con calidad humana e idoneidad en nuestras carreras universitarias escogidas, a cada uno de los compañeros con los cuales compartí en los diferentes cursos realizados a lo largo del programa académico cursado, y en los cuales se obtuvieron no solo logros académicos sino también experiencias personales y académicas fomentando en mi un alto grado de empatía para con mis demás congéneres, a la Universidad Nacional Abierta y a Distancia UNAD y del mismo modo al CEAD Gacheta por brindarme todos los elementos como instalaciones, equipo, personal y servicios necesarios para lograr un aprendizaje autónomo y excelente.

Dios colme y llene sus vidas de bendiciones.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

CONMUTACIÓN: Se considera como la acción de establecer una vía, un camino, de extremo a extremo entre dos puntos, un emisor (Tx) y un receptor (Rx) a través de nodos o equipos de transmisión. La conmutación permite la entrega de la señal desde el origen hasta el destino requerido.

DIRECCIÓN IP: Es un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en la red (elemento de comunicación/conexión) de un dispositivo (computadora, laptop, teléfono inteligente) que utilice el protocolo (Internet Protocol) o que corresponde al nivel de red del modelo TCP/IP.

ENCAPSULACIÓN: Es un método de diseño modular de protocolos de comunicación en el cual las funciones lógicas de una red son abstraídas ocultando información a las capas de nivel superior. La encapsulación es una característica en la mayoría de modelos de redes, incluyendo el modelo OSI y la familia de protocolos TCP/IP.

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

ROUTER: También conocido como encaminador, es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función: se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.

ROUTING: Capacidad de mover paquetes a través de las redes, también conocido como encaminamiento, 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.

RESUMEN

Con el desarrollo de este trabajo se busca presentar la solución de las prácticas en el escenario 1 de pruebas de habilidades de las unidades presentadas a lo largo del curso, donde se tratan las temáticas como enrutamiento “routing” configuración de Router, Switches dispositivos como computadores, tables, Smartphones, configuración estática y dinámica de NAT entre otros que componen estas temáticas abordadas, logrando definir conceptos básicos y fundamentales los cuales son aplicables y muy relevantes en el campo de estudio de la Ingeniería de Sistemas y ciencias afines y las cuales se cursan en el momento de igual forma con el desarrollo de este escenario se pretende demostrar cada una de las capacidades que se lograron adquirir de forma práctica a través de cada temática abordada y presentada en el Software de Simulación de redes Packet Tracer generando con cada practica la adquisición de nuevos conocimientos que son importantes en nuestra área de aprendizaje y laboral en los diferentes contextos aplicados a la vida cotidiana.

Palabras Clave: CISCO, CCNA, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

With the development of this work it is sought to present the solution of the practices in scenario 1 of skills tests of the units presented throughout the course, where the topics such as routing "routing" configuration of Routers, Switches, devices such as computers are discussed , tables, Smartphones, static and dynamic NAT configuration among others that make up these topics addressed, managing to define basic and fundamental concepts which are applicable and very relevant in the field of study of Systems Engineering and related sciences and which are studied At the same time, with the development of this scenario, it is intended to demonstrate each of the capabilities that were achieved in a practical way through each topic addressed and presented in the Packet Tracer Network Simulation Software, generating the acquisition with each practice. of new knowledge that is important in our area of learning and work in the different contexts applied to everyday life.

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

INTRODUCCION

En esta actividad realizada en el software Packet Tracer, se utilizarán varios comandos para poder configurar los parámetros básicos del router, de igual forma se proporcionará un acceso seguro a la CLI y al puerto de consola mediante contraseñas encriptadas y contraseñas de texto no cifrado router y por ende se configurará mensajes para los usuarios que inicien sesión en el router, mostrando a los usuarios no autorizados que intenten ingresar que el acceso está prohibido así mismo se verificará y guardará la configuración en ejecución.

El siguiente trabajo tiene como finalidad el desarrollado de las temáticas de las unidades presentadas en el curso, se observará como se realizan diferentes procedimientos de configuración de direccionamiento IPv6 en router servidores y equipos de cómputo además de la verificación en el direccionamiento IPv6 mediante el proceso de envío de ping de igual forma se realizarán las pruebas correspondientes.

ESCENARIO 1.

Topología

Figura 1. Topología Escenario 1

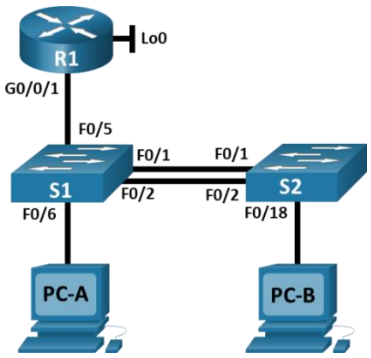
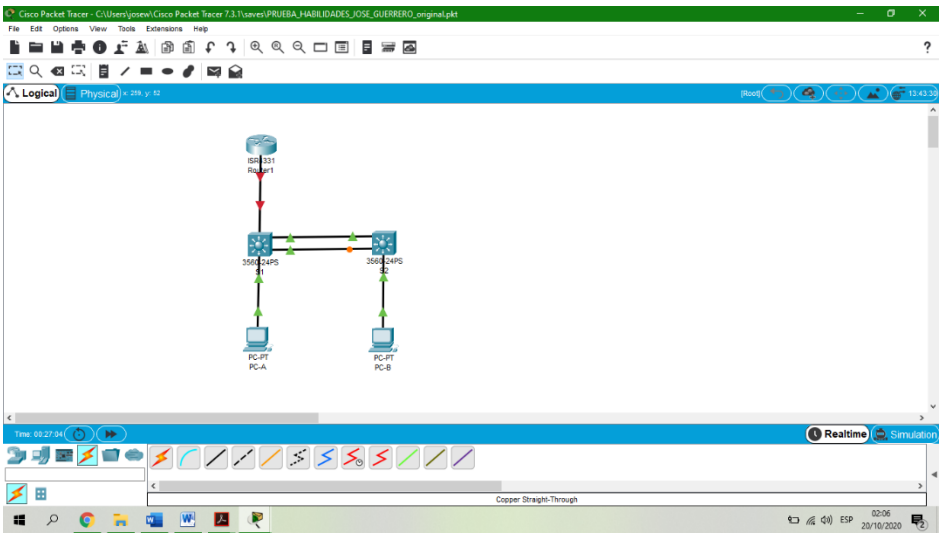


Figura 2. Topología creada Escenario 1



Fuente: Autor

Para el escenario 1 se realiza la creación de la topología necesaria en el software Packet Tracer empleando los siguientes equipos de este aplicativo.

- 01 Router 4331 para R1
- 01 Switch 3560 para S1
- 01 Switch 3560 para S2
- 01 PC para PC-A

- 01 PC para PC-B

Tabla 1. Tabla de VLAN

VLAN	Nombre de la VLAN
2	Bikes
3	Trikes
4	Management
5	Parking
6	Native

Tabla 2. Tabla de asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

Nota: No hay ninguna interfaz en el router que admita VLAN 5.

1. Parte 1: Inicializar, Recargar y Configurar aspectos básicos de los dispositivos

1.1. Paso 1: Inicializar y volver a cargar el router y el switch

La primera medida que se debe tomar antes de introducir cualquier configuración a los router y los switches en este paso, es realizar la eliminación de la configuración de inicio de cada dispositivo y paso posterior volver a cargar estos dispositivos, para esta tarea se realizara el uso de diferentes comandos con el fin de establecer borrado y carga los cuales se encontraran mostrados o contenidos en la (Tabla 3, Tabla 4, Tabla 5,) por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 3, podemos asegurar que cada uno de los dispositivos de red no tengan almacenados datos en memoria y en los cuales se pueden encontrar, la base de datos de VLAN además de otras configuraciones que vienen por defecto o ya preestablecidas.

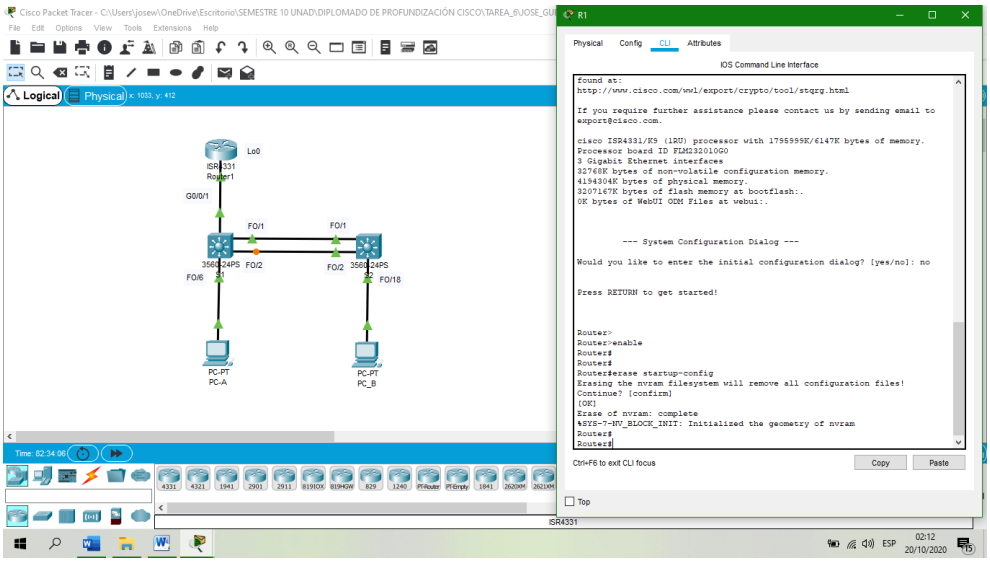
1.1.1 Borrado configuraciones Router

Los siguientes son los comandos utilizados con su respuesta respectiva en el router 1 para el procedimiento de borrado de las configuraciones predeterminadas, de este router.

Tabla 3. Borrado configuraciones Router Escenario 1

Borrado configuraciones Router Escenario 1	
Tarea	**Especificación**
Eliminar el archivo startup-config de todos los routers	Se realiza la inserción de esta línea de comandos para eliminar configuraciones del router. **Router>enable** **Router#erase startup-config**

Figura 3.Borrado configuraciones Router Escenario 1



Fuente: Autor

Mediante el comando erase startup-config se realiza el borrado de la base de datos preconfigurado en la memoria flash del R1 siendo exitoso.

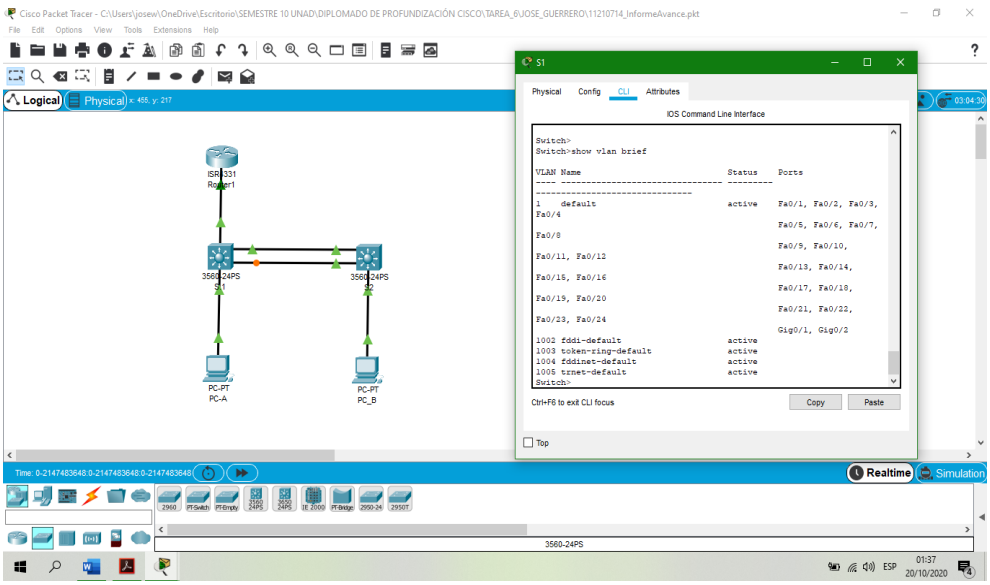
1.1.2 Borrado configuraciones y base datos VLAN Switch

Los siguientes son los comandos utilizados con su respuesta respectiva en el Switch 1 para el procedimiento de borrado de las configuraciones predeterminadas, así como el borrado de la base de datos de VLAN del Switch el procedimiento es igual en todos los Switch.

Tabla 4. Borrado configuraciones Switches Escenario 1

Borrado configuraciones Switches Escenario 1	
Tarea	**Especificación**
Eliminar el archivo startup-config de todos los switch y eliminar la base de datos de VLAN	Se realiza la inserción de esta línea de comandos para eliminar las configuraciones y la base de datos de VLAN del switch **Switch>enable** **Switch#erase startup-config** **Switch#delete vlan.dat**
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Se realiza la inserción de esta línea de comandos para verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches **Switch>enable** **Switch#show vlan brief**

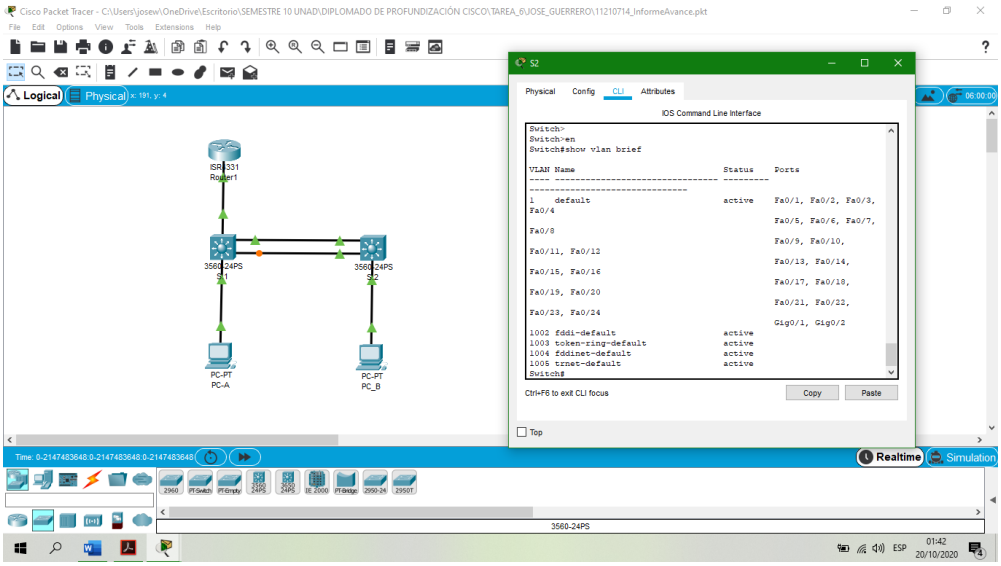
Figura 4. Verificar borrado de base de datos de VLAN en la memoria flash de S1



Fuente: Autor

Mediante el comando show vlan brief se realiza la verificación del borrado de la base de datos de VLAN en la memoria flash de S1 siendo exitoso.

Figura 5. Verificar borrado de base de datos de VLAN en la memoria flash de S2



Fuente: Autor

Mediante el comando show vlan brief se realiza la verificación de borrado de la base de datos de VLAN en la memoria flash de S2 siendo exitoso

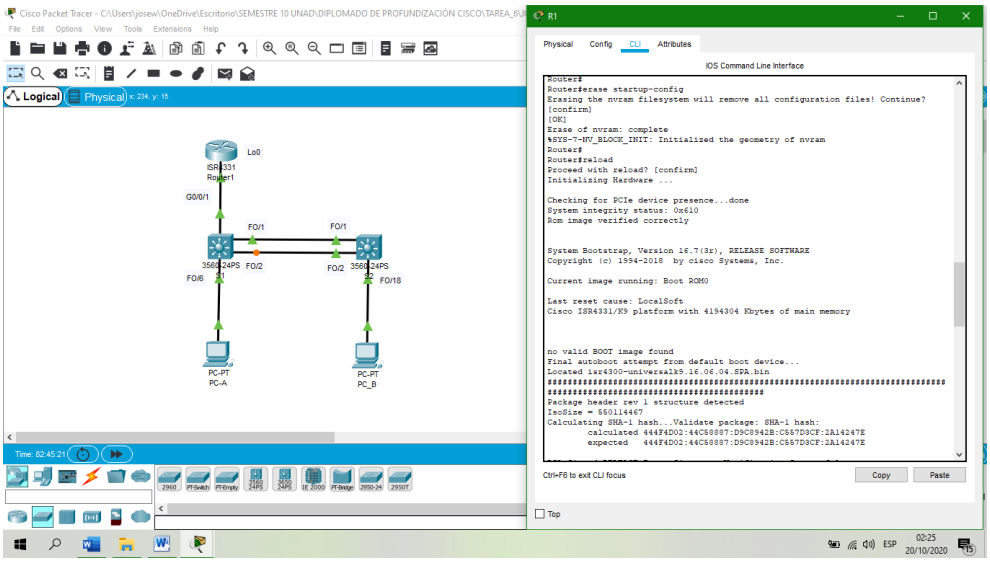
1.1.3 Reinicio de Router y Switches Escenario 1

Los siguientes son los comandos utilizados en el Router y los Switches para el procedimiento de reinicio de los equipos después de borrar sus configuraciones, el procedimiento es igual en todos los Switch y el router

Tabla 5. Reinicio de Router y Switches

Reinicio de Router y Switches Escenario 1	
Tarea	**Especificación**
Volver a cargar todos los routers	Se realiza la inserción de esta línea de comandos para recargar o reiniciar las configuraciones del router **Router#reload**
Volver a cargar ambos switch	Se realiza la inserción de esta línea de comandos para recargar o reiniciar las configuraciones del switch **Switch#reload**

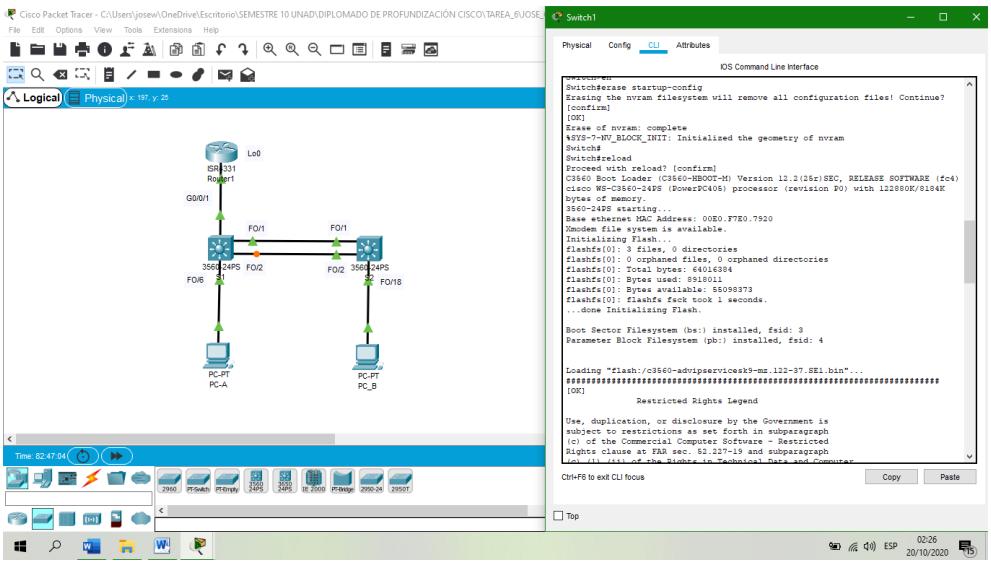
Figura 6. Reinicio de Router Escenario 1



Fuente: Autor

Se realiza la inserción del comando reload para recargar o reiniciar las configuraciones del router R1 siendo exitoso

Figura 7. Reinicio de Switches Escenario 1



Fuente: Autor

Se realiza la inserción del comando reload para recargar o reiniciar las configuraciones del Switch S1 siendo exitoso

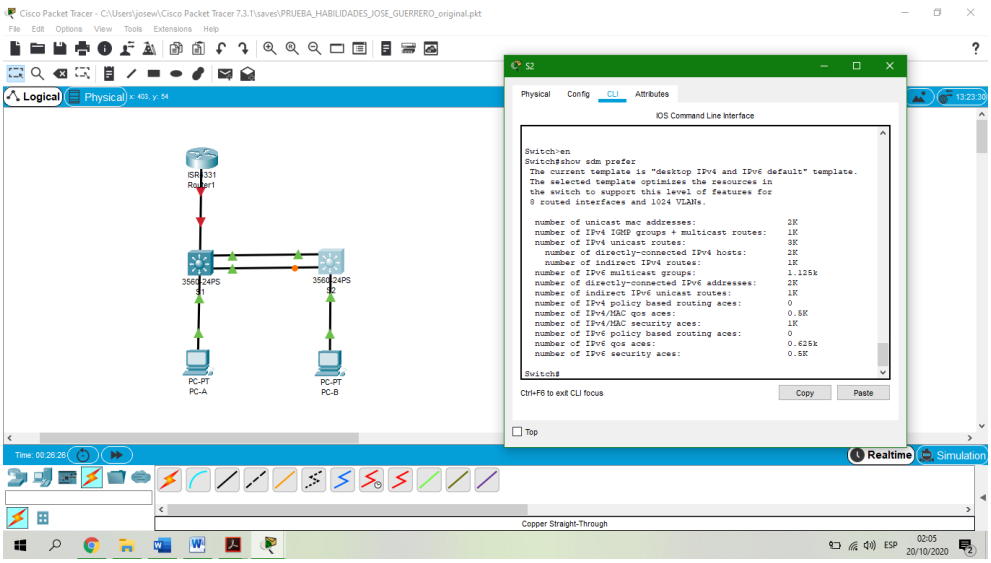
1.1.4 Configuración plantilla SDM para que admita IPv6

Para realizar la configuración de la plantilla SDM para que admita IPv6 según sea necesario y volver a cargar el switch se utilizaron los comandos establecidos en la siguiente tabla (Tabla 6. Configurar plantilla SDM para que admita IPv6)

Tabla 6. Configurar plantilla SDM para que admita IPv6

Configurar plantilla SDM para que admita IPv6	
Tarea	**Especificación**
Verificar y seleccionar plantilla	Se realiza la inserción de esta línea de comandos para verificar y seleccionar plantilla del switch **Switch>enable** **Switch#show sdm prefer**
Ver plantilla SMD	Se realiza la inserción de esta línea de comandos para ver plantilla SMD del switch **Switch#configure terminal** **Switch(config)#sdm prefer ?**
Modificar la plantilla SMD	Se realiza la inserción de esta línea de comandos para modificar la plantilla SMD del switch **Switch(config)#sdm prefer dual-ipv4-and-ipv6 ?** **Switch(config)#sdm prefer dual-ipv4-and-ipv6 default**
Volver a cargar switch	Se realiza la inserción de esta línea de comandos para recargar las configuraciones del switch **Switch(config)#exit** **Switch#reload**
Verificar que los cambios efectuados	Se realiza la inserción de esta línea de comandos para verificar los cambios efectuados switch **Switch>en** **Switch#show sdm prefer**

Figura 8. Prueba verificación configuración plantilla SDM que admita IPv6



Fuente: Autor

Se configura la plantilla SDM para que admita IPv6 y se verifican los cambios realizados mediante los comandos anteriormente descritos.

1.2. Paso 2: Configurar R1

Realizado el paso de borrar las diferentes configuraciones en cada Router y Switch y con el fin de garantizar que estos no posean datos en su memoria, posteriormente se realizara el procedimiento de configuración teniendo en cuenta cada uno de los aspectos y requerimientos solicitados en este escenario 1 para esto nos apoyaremos en la lista de direccionamiento IP sobre la topología de red a trabajar la cual se puede observar en la (Figura 2. Topología creada) mediante esta se realizarán las configuraciones empleando los siguientes equipos.

- 01 Router 4331 para R1
- 01 Switch 3560 para S1
- 01 Switch 3560 para S2
- 01 PC para PC-A
- 01 PC para PC-B

Apoyado en la topología de la red se realizará la configuración del router R1 utilizando cada uno de los parámetros básicos establecidos en este escenario 1 como son desactivar la búsqueda DNS, generar un nombre para el router, asignar un nombre de dominio, establecer una contraseña cifrada para el modo EXEC

privilegiado, configurar el acceso a la consola, realizar establecimiento de la longitud mínima para las contraseñas, crear un usuario administrativo en la base de datos local, 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, generar un mensaje MOTD que permita mostrar una alerta si la contraseña ingresada es diferente a la permitida, Habilitar el routing IPv6, Configurar interfaz G0/0/1 y subinterfaces, configurar el Loopback0 interface generar una clave de cifrado RSA.

Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 7. Configuración R1) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 7, podemos asegurar que el Router R1 quede configurado de la manera correcta.

Tabla 7. Configuración R1

Configuración router 1	
Tarea	**Especificación**
Desactivar la búsqueda DNS	Se realiza la inserción de esta línea de comandos para desactivar la búsqueda DNS en el router 1 **Router>enable** **Router# (config)#no ip domain-lookup**
Nombre del router	Se realiza la inserción de esta línea de comandos para asignar un nombre en el router 1 **Router# (config)#hostname R1**
Nombre de dominio	Se realiza la inserción de esta línea de comandos para asignar un nombre de dominio en el router 1 **R1(config)# ip domain name ccna-lab.com**
Contraseña cifrada para el modo EXEC privilegiado	Se realiza la inserción de estas líneas de comandos para asignar una Contraseña cifrada para el modo EXEC privilegiado en el router 1 **R1(config)#enable password ciscoenpass** **R1(config)#exit** **R1#en** **R1#config t** **R1#en** **R1#config t** **R1(config)#service password-encryption** **R1(config)#exit**

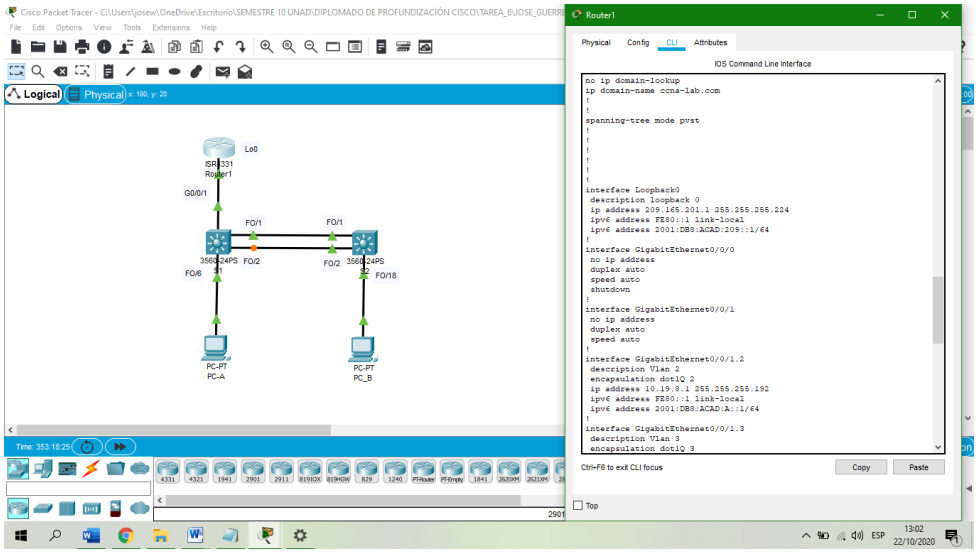
Contraseña de acceso a la consola	Se realiza la inserción de estas líneas de comandos para asignar una Contraseña de acceso a la consola en el router 1 **R1(config)#line console 0** **R1(config-line)#password ciscoconpass** **R1(config-line)#login** **R1(config-line)#exit**
Establecer la longitud mínima para las contraseñas	Se realiza la inserción de estas líneas de comandos para establecer la longitud mínima para las contraseñas en el router 1 **R1#config t** **R1(config)#security passwords min-length 10** **R1(config)#enable password ciscoenpass**
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** Se realiza la inserción de estas líneas de comandos para Crear un usuario administrativo en la base de datos local en el router 1 **R1#config t** **R1(config)#username admin password admin1pass** **R1(config)#line console 0** **R1(config-line)#login local**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Se realiza la inserción de estas líneas de comandos para Configurar el inicio de sesión en las líneas VTY para que use la base de datos local en el router 1 **R1(config)#line vty 0 4** **R1(config-line)#login local** **R1(config-line)#exit**
Configurar VTY solo aceptando SSH	Se realiza la inserción de estas líneas de comandos para Configurar VTY solo aceptando SSH en el router 1 **R1(config)#hostname R1** **R1(config)#ip domain name ccna-lab.com** **R1(config)#crypto key generate rsa** **How many bits in the modulus [512]: 1024** **R1(config)#ip ssh version 2** **R1(config)#line vty 0 15** **R1(config-line)#login local**

	R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	Se realiza la inserción de estas líneas de comandos para Cifrar las contraseñas de texto no cifrado en el router 1 **R1(config)#service password-encryption**
Configure un MOTD Banner	Se realiza la inserción de estas líneas de comandos para Configure un MOTD Banner en el router 1 **R1(config)#banner motd $Esta prohbido el acceso no autorizado.$**
Habilitar el routing IPv6	Se realiza la inserción de estas líneas de comandos para Habilitar el routing IPv6 en el router 1 **R1(config)#ipv6 unicast-routing**
Configurar interfaz G0/0/1 y subinterfaces	Se realiza la inserción de estas líneas de comandos para Configurar interfaz G0/0/1 y subinterfaces en el router 1 **Descripción interfaz G0/0/1** R1(config)#interface g0/0/1 R1(config-if)#no shutdown **Descripción interfaz G0/0/1.2** R1(config-if)#interface g0/0/1.2 R1(config-if)#description Vlan 2 R1(config-subif)#encapsulation dot1q 2 **Establece la dirección IPv4.** R1(config-if)#ip address 10.19.8.1 255.255.255.192 **Establezca la dirección local de enlace IPv6 como fe80: :1** R1(config-if)#ipv6 address fe80::1 link-local **Establece la dirección IPv6.** R1(config-if)#ipv6 address 2001:db8:acad:a::1/64 **Activar la interfaz.** R1(config-subif)#no shutdown **Descripción interfaz G0/0/1.3** R1(config-if)#interface g0/0/1.3

	R1(config-if)#description Vlan 3 R1(config-subif)#encapsulation dot1q 3 **Establece la dirección IPv4.** R1(config-if)#ip address 10.19.8.65 255.255.255.224 **Establezca la dirección local de enlace IPv6 como fe80: :1** R1(config-if)#ipv6 address fe80::1 link-local **Establece la dirección IPv6.** R1(config-if)#ipv6 address 2001:db8:acad:b::1/64 **Activar la interfaz.** R1(config-subif)#no shutdown **Descripción interfaz G0/0/1.4** R1(config-if)#interface g0/0/1.4 R1(config-if)#description Vlan 4 R1(config-subif)#encapsulation dot1q 4 **Establece la dirección IPv4.** R1(config-if)#ip address 10.19.8.97 255.255.255.248 **Establezca la dirección local de enlace IPv6 como fe80: :1** R1(config-if)#ipv6 address fe80::1 link-local **Establece la dirección IPv6.** R1(config-if)#ipv6 address 2001:db8:acad:c::1/64 **Activar la interfaz.** R1(config-subif)#no shutdown
Configure el Loopback0 interface	Se realiza la inserción de estas líneas de comandos para Configurar el Loopback0 interface en el router 1 **Descripción interfaz G0/0/1.4** R1(config-if)#in loopback 0 R1(config-if)#description loopback 0 **Establece la dirección IPv4.** R1(config-if)#ip address 209.165.201.1 255.255.255.224

	Establezca la dirección local de enlace IPv6 como fe80: :1 R1(config-if)#ipv6 address fe80::1 link-local **Establece la dirección IPv6.** R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 **Activar la interfaz.** R1(config-if)#no shutdown
Generar una clave de cifrado RSA	**Módulo de 1024 bits** Se realiza la inserción de estas líneas de comandos para Generar una clave de cifrado RSA en el router 1 **R1(config)#crypto key generate rsa general-keys modulus 1024**

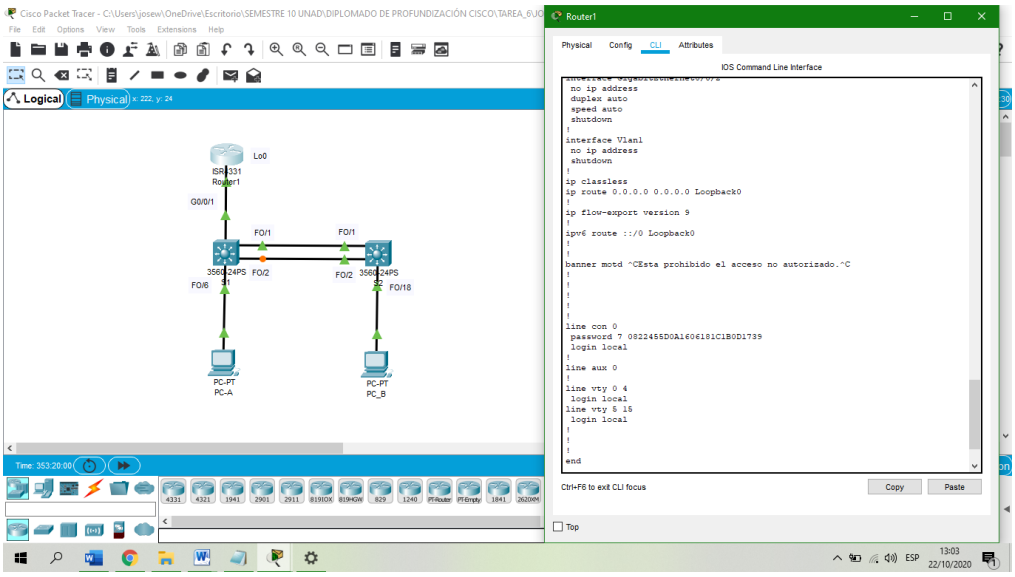
Figura 9. Verificación comando show running-config en router 1 (1)



Fuente: Autor

Se realiza la Verificación de la configuración de interfaces y dominio del Router 1 (R1) mediante el comando **R1#show running-config** saliendo exitosa la configuración.

Figura 10. Verificación comando show running-config en router 1 (2)



Fuente: Autor

Se realiza la Verificación de la configuración de contraseñas, cifrado y MOTD Banner del Router 1 (R1) mediante el comando **R1#show running-config** saliendo exitosa la configuración.

1.3. Paso 3: Configure S1 y S2.

1.3.1 Configuración Switch S1

Apoyado en la topología de la red se realizará la configuración del Switch 1 utilizando cada uno de los parámetros básicos establecidos en este escenario 1 como son desactivar la búsqueda DNS, generar un nombre para el Switch, asignar un nombre de dominio, establecer una contraseña cifrada para el modo EXEC privilegiado, configurar el acceso a la consola, crear un usuario administrativo en la base de datos local, 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, generar un mensaje MOTD que permita mostrar una alerta si la contraseña ingresada es diferente a la permitida, generar una clave de cifrado RSA.

Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 8. Configuración S1) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 8, podemos asegurar que el Switch S1 quede configurado de la manera correcta.

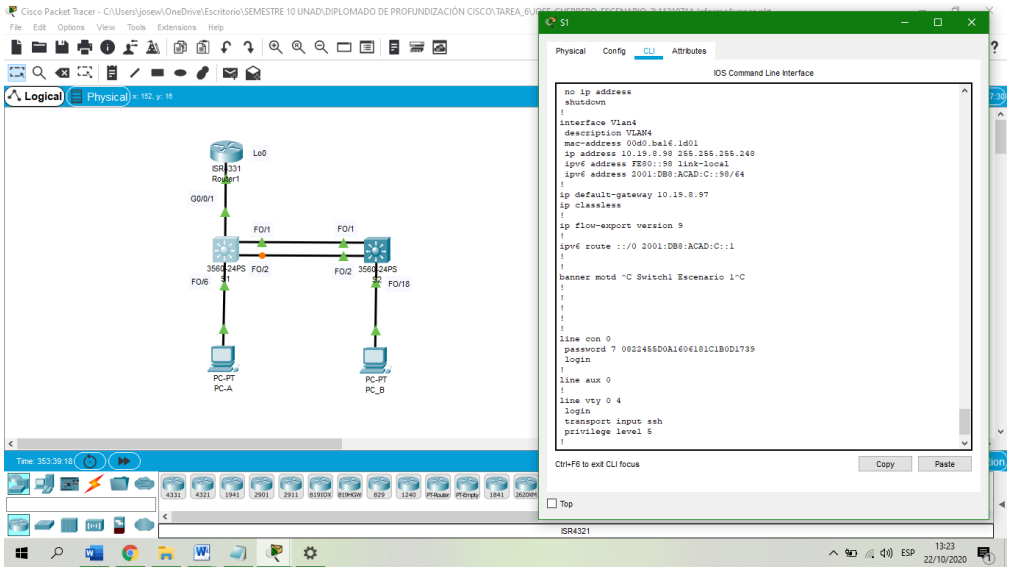
Tabla 8. Configuración S1

Configuración Switch 1	
Tarea	**Especificación**
Desactivar la búsqueda DNS	Se realiza la inserción de estas líneas de comandos para Desactivar la búsqueda DNS en el Switch 1 **Switch >enable** **Switch(config)#no ip domain-lookup**
Nombre del Switch	**S1 o S2, según proceda** Se realiza la inserción de estas líneas de comandos para asignar Nombre del Switch 1 **Switch(config)#hostname S1**
Nombre de dominio	**ccna-lab.com** Se realiza la inserción de estas líneas de comandos para asignar Nombre de dominio en el Switch 1 **S1(config)#ip domain name ccna-lab.com**
Contraseña cifrada para el modo EXEC privilegiado	**Ciscoenpass** Se realiza la inserción de estas líneas de comandos para asignar Contraseña cifrada para el modo EXEC privilegiado en el Switch 1 **S1(config)#enable secret ciscoenpass** **S1(config)#line console 0**
Contraseña de acceso a la consola	**Ciscoconpass** Se realiza la inserción de estas líneas de comandos para asignar Contraseña de acceso a la consola en el Switch 1 **S1(config)#line console 0** **S1(config-line)#password ciscoconpass** **S1(config-line)#login**
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**

	Se realiza la inserción de estas líneas de comandos para Crear un usuario administrativo en la base de datos local en el Switch 1 **S1#config t** **S1(config-line)#username admin password admin1pass**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Se realiza la inserción de estas líneas de comandos para Desactivar la búsqueda DNS en el Switch 1 **S1(config)#line vty 0 4**
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Se realiza la inserción de esta línea de comandos para Configurar el inicio de sesión en las líneas VTY para que use la base de datos local en el Switch 1 **S1(config-line)#privilege level 5** **S1(config-line)#transport input ssh**
Cifrar las contraseñas de texto no cifrado	Se realiza la inserción de estas líneas de comandos para Cifrar las contraseñas de texto no cifrado en el Switch 1 **S1(config-line)#service password-encryption**
Configure un MOTD Banner	Se realiza la inserción de estas líneas de comandos para Configure un MOTD Banner en el Switch 1 **S1(config)#banner motd # Switch1 Escenario 1#**
Generar una clave de cifrado RSA	**Módulo de 1024 bits** Se realiza la inserción de estas líneas de comandos para Generar una clave de cifrado RSA en el Switch 1 **S1(config)#crypto key generate rsa general-keys modulus 1024**
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como **FE80: :98 para S1 y FE80: :99 para S2** Establecer la dirección IPv6 de capa 3 Se realiza la inserción de estas líneas de comandos para Configurar la interfaz de administración (SVI) en el Switch 1

	Descripción interfaz vlan 4 S1(config)#int vlan 4 S1(config-if)#description VLAN4 **Establece la dirección IPv4.** S1(config-if)#ip address 10.19.8.98 255.255.255.248 **Establezca la dirección local de enlace IPv6 como fe80: :1** S1(config-if)#ipv6 address fe80::98 link-local **Establece la dirección IPv6.** S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 **Activar la interfaz.** R1(config-subif)#no shutdown copy running-config startup-config
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4 Se realiza la inserción de estas líneas de comandos para Configuración del gateway predeterminado en el Switch 1 **S1(config-if)#ip default-gateway 10.19.8.97**

Figura 11. Verificación Configuración comando show running-config en S1



Fuente: Autor

Se realiza la Verificación de la configuración de interfaces puerta enlace, contraseñas, cifrado y MOTD Banner del Switch1 mediante el comando **S1#show running-config** saliendo exitosa la configuración.

1.3.2 Configuración Switch S2

Apoyado en la topología de la red se realizará la configuración del Switch 2 utilizando cada uno de los parámetros básicos establecidos en este escenario 1 como son desactivar la búsqueda DNS, generar un nombre para el Switch, asignar un nombre de dominio, establecer una contraseña cifrada para el modo EXEC privilegiado, configurar el acceso a la consola, crear un usuario administrativo en la base de datos local, 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, generar un mensaje MOTD que permita mostrar una alerta si la contraseña ingresada es diferente a la permitida, generar una clave de cifrado RSA.

Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 9. Configuración S2) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 9, podemos asegurar que el Switch S1 quede configurado de la manera correcta.

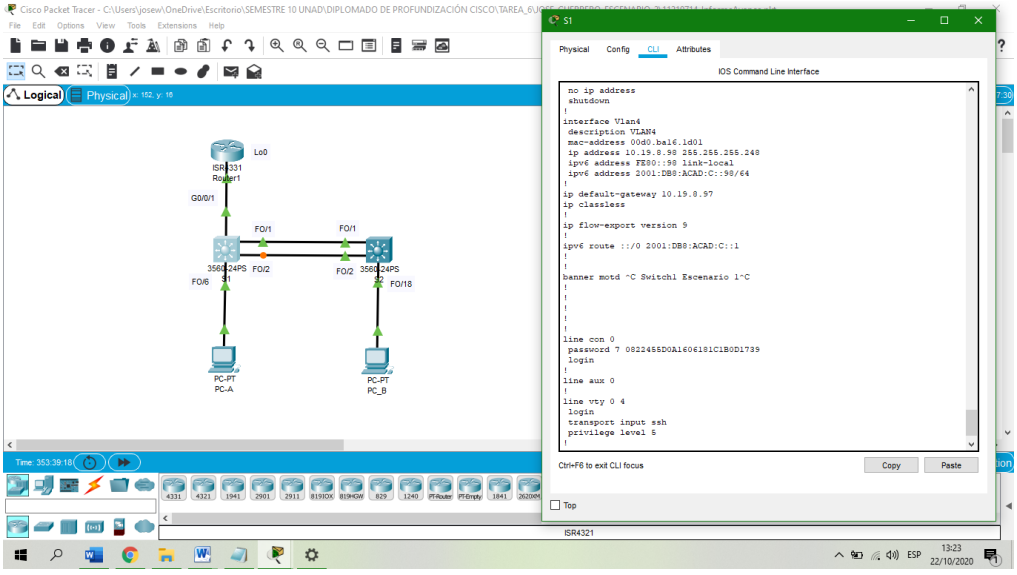
Tabla 9. Configuración S2

Configuración Switch 2	
Tarea	**Especificación**
Desactivar la búsqueda DNS	Se realiza la inserción de estas líneas de comandos para Desactivar la búsqueda DNS en el Switch 2 **Switch >enable** **Switch(config)#no ip domain-lookup**
Nombre del Switch	**S1 o S2, según proceda** Se realiza la inserción de estas líneas de comandos para asignar Nombre del Switch 2 **Switch(config)#hostname S2**
Nombre de dominio	**ccna-lab.com** Se realiza la inserción de estas líneas de comandos para asignar Nombre de dominio en el Switch 2 **S2(config)#ip domain name ccna-lab.com**
Contraseña cifrada para el modo EXEC privilegiado	**Ciscoenpass** Se realiza la inserción de estas líneas de comandos para asignar Contraseña cifrada para el modo EXEC privilegiado en el Switch 2 **S2(config)#enable secret ciscoenpass** **S2(config)#line console 0**
Contraseña de acceso a la consola	**Ciscoconpass** Se realiza la inserción de estas líneas de comandos para asignar Contraseña de acceso a la consola en el Switch 2 **S2(config)#line console 0** **S2(config-line)#password ciscoconpass** **S2(config-line)#login**
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**

	Se realiza la inserción de estas líneas de comandos para Crear un usuario administrativo en la base de datos local en el Switch 2 **S2#config t** **S2(config-line)#username admin password admin1pass**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Se realiza la inserción de estas líneas de comandos para Desactivar la búsqueda DNS en el Switch 2 **S2(config)#line vty 0 4**
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Se realiza inserción de estas líneas de comandos para Configurar el inicio de sesión en las líneas VTY para que use la base de datos local en el Switch 2 **S2(config-line)#privilege level 5** **S2(config-line)#transport input ssh**
Cifrar las contraseñas de texto no cifrado	Se realiza la inserción de estas líneas de comandos para Cifrar las contraseñas de texto no cifrado en el Switch 2 **S2(config-line)#service password-encryption**
Configure un MOTD Banner	Se realiza la inserción de estas líneas de comandos para Configure un MOTD Banner en el Switch 2 **S2(config)#banner motd # Switch1 Escenario 1#**
Generar una clave de cifrado RSA	**Módulo de 1024 bits** Se realiza la inserción de estas líneas de comandos para Generar una clave de cifrado RSA en el Switch 1 **S2(config)#crypto key generate rsa general-keys modulus 1024**
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como **FE80: :98 para S1 y FE80: :99 para S2** Establecer la dirección IPv6 de capa 3 **Descripción interfaz vlan 4** S2(config)#int vlan 4 S2(config-if)#description VLAN4

	Establece la dirección IPv4. S2(config-if)#ip address 10.19.8.99 255.255.255.248 **Establezca la dirección local de enlace IPv6 como fe80: :1** S2(config-if)# ipv6 address fe80::99 link-local **Establece la dirección IPv6.** S2(config-if)# ipv6 address 2001:db8:acad:c::99/64 **Activar la interfaz.** R1(config-subif)#no shutdown copy running-config startup-config
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4 Se realiza la inserción de estas líneas de comandos para Configuración del gateway predeterminado en el Switch 2 **S2(config-if)#ip default-gateway 10.19.8.97**

Figura 12. Verificación Configuración comando show running-config en S2



Fuente: Autor

Se realiza la Verificación de la configuración de interfaces puerta enlace, contraseñas, cifrado y MOTD Banner del Switch 2 mediante el comando **S2#show running-config** saliendo exitosa la configuración.

2. Parte 2: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

2.1. Paso 1: Configurar S1

Apoyado en la topología de la red se realizará la configuración de la infraestructura de red (VLAN, Trunking, EtherChannel del Switch S1 utilizando cada uno de los parámetros básicos establecidos en este escenario 1 como son creación de VLAN, Creación de troncos 802.1Q que utilicen la VLAN 6 nativa, Creación de un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 realizar configuración puertos de acceso de host para VLAN 2 y VLAN 3, así como la seguridad en los puertos de acceso protegiendo las interfaces que no se utilizaran

Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 10. Configuración Switch 1 Vlans) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 10, podemos asegurar que el Switch S1 quede configurado de la manera correcta.

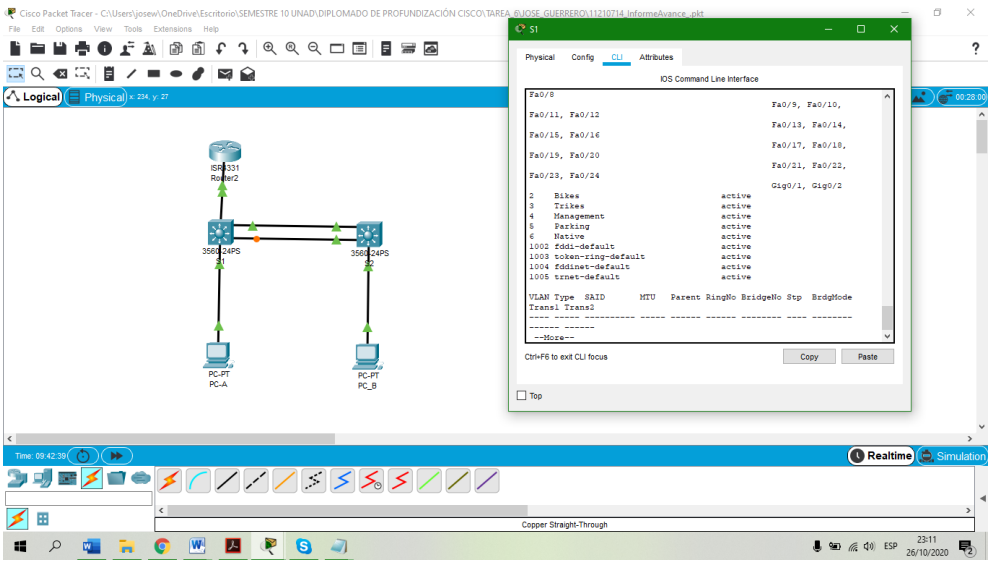
Tabla 10. Configuración Switch 1 Vlans

Configuración (VLAN, Trunking, EtherChannel) de Switch 1	
Tarea	**Especificación**
Crear VLAN	Se realiza la inserción de estas líneas de comandos para Crear VLAN en el Switch 1 S1# config t **VLAN 2, nombre Bikes** S1(config)#Vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#exit **VLAN 3, nombre Trikes** S1(config)#Vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#exit VLAN 4, name Management **S1(config)#Vlan 4** S1(config-vlan)# name Management S1(config-vlan)#exit

	VLAN 5, nombre Parking S1(config)#Vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#exit **VLAN 6, nombre Native** S1(config)#Vlan 6 S1(config-vlan)#name Native S1(config-vlan)#exit S1(config)#exit S1#show vlan
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5 Se realiza la inserción de estas líneas de comandos para Crear troncos 802.1Q que utilicen la VLAN 6 nativa en el Switch 1 **S1(config)#interface range fa0/1, fa0/2, fa0/5** **S1(config-if-range)#no shutdown** **S1(config-if-range)#switchport mode access** **S1(config-if-range)#switchport mode trunk** **S1(config-if-range)#switchport trunk native vlan 6** **S1(config-if-range)#switchport trunk encapsulation dot1q**
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación Se realiza la inserción de estas líneas de comandos para Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 en el Switch 1 **S1(config)#interface range fa0/1,fa0/2** **S1(config-if-range)#channel-group 2 mode active**
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6 Se realiza la inserción de estas líneas de comandos para Configurar el puerto de acceso de host para VLAN 2 en el Switch 1 **S1(config)#int fa 0/6** **S1(config-if)#no shutdown** **S1(config-if)#switchport mode access** **S1(config-if)#switchport access vlan 4** **S1(config-if)#switchport access vlan 2**
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC Se realiza la inserción de estas líneas de comandos para Configurar la seguridad del puerto en los puertos de acceso en el Switch 1

	S1(config)#int fa0/6 **S1(config-if)#switchport port-security** **S1(config-if)#switchport port-security maximum 3** **S1(config)#show port-security**
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar Se realiza la inserción de estas líneas de comandos para Proteger todas las interfaces no utilizadas en el Switch 1 **S1#** **S1#config t** **Enter configuration commands, one per line.** **End with CNTL/Z.** **S1(config)#int range fa 0/3-4, fa 0/7-24, G 0/1-2** **S1(config-if-range)#shutdown** **S1(config-if-range)#switchport mode access** **S1(config-if-range)#switchport access vlan 5** **S1(config-if-range)#description puertos sin usa** **S1(config-if-range)#exit** **S1(config)#**

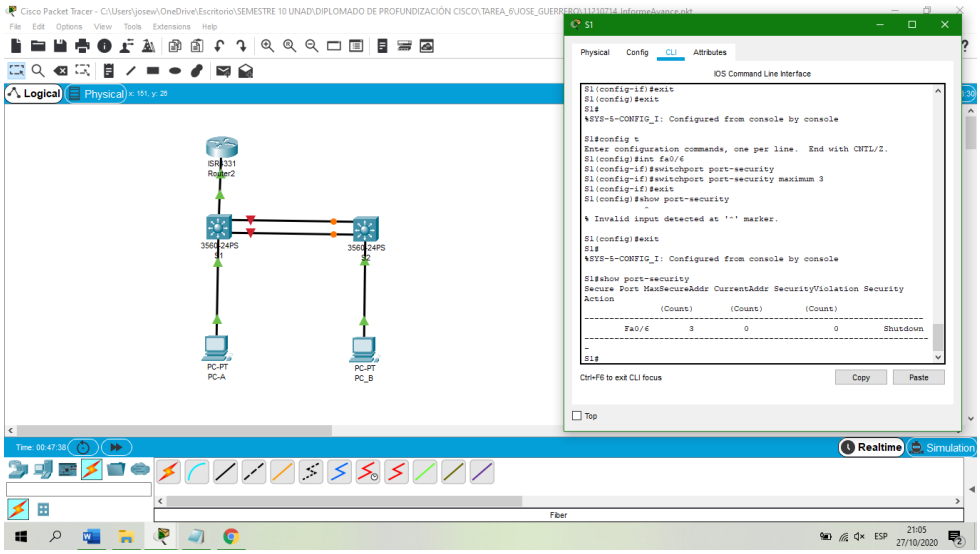
Figura 13. Configuración Switch 1 Vlans



Fuente: Autor

Se realizan las configuraciones de las VLAN en el Swicht 1 presentando su creación de forma exacta cumpliendo los parámetros solicitados.

Figura 14. Permitir 3 direcciones MAC



Fuente: Autor

Se utiliza el comando show port-security para verificar la Configurar la seguridad del puerto en los puertos de acceso Permitir 3 direcciones MAC

2.2. Paso 2: Configure el S2.

Apoyado en la topología de la red se realizará la configuración de la infraestructura de red (VLAN, Trunking, EtherChannel del Switch S2 utilizando cada uno de los parámetros básicos establecidos en este escenario 1 como son creación de VLAN, Creación de troncos 802.1Q que utilicen la VLAN 6 nativa, Creación de un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 realizar configuración puertos de acceso de host para VLAN 2 y VLAN 3, así como la seguridad en los puertos de acceso protegiendo las interfaces que no se utilizaran

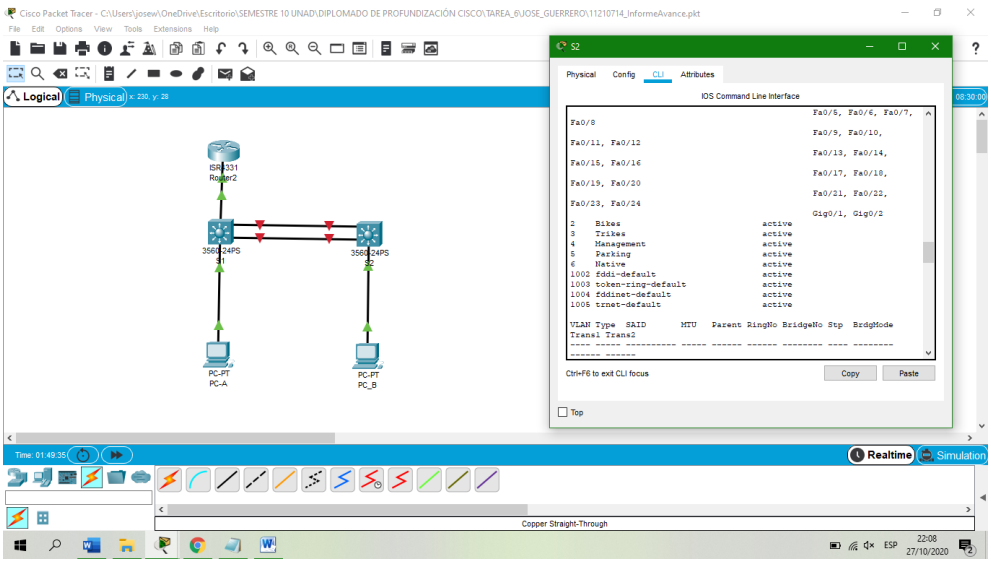
Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 11. Configuración Switch 2 Vlans) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 11, podemos asegurar que el Switch S2 quede configurado de la manera correcta.

Tabla 11. Configuración Switch 2 Vlans

Configuración (VLAN, Trunking, EtherChannel) Switch 2	
Tarea	**Especificación**
Crear VLAN	Se realiza la inserción de estas líneas de comandos para Crear VLAN en el Switch 2 S2# config t **VLAN 2, nombre Bikes** S2(config)#Vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#exit **VLAN 3, nombre Trikes** S2(config)#Vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#exit VLAN 4, name Management S2(config)#Vlan 4 S2(config-vlan)# name Management S2(config-vlan)#exit **VLAN 5, nombre Parking** S2(config)#Vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#exit **VLAN 6, nombre Native** S2(config)#Vlan 6 S2(config-vlan)#name Native S2(config-vlan)#exit S2(config)#exit S2#show vlan
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5 Se realiza la inserción de estas líneas de comandos para Crear troncos 802.1Q que utilicen la VLAN 6 nativa en el Switch 2 **S2(config)#interface range fa0/1, fa0/2, fa0/5** **S2(config-if-range)#no shutdown** **S2(config-if-range)#switchport mode access** **S2(config-if-range)#switchport mode trunk** **S2(config-if-range)#switchport trunk native vlan 6** **S2(config-if-range)#switchport trunk encapsulation dot1q**

Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación Se realiza la inserción de estas líneas de comandos para Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 en el Switch 2 **S2(config)#interface range fa0/1,fa0/2** **S2(config-if-range)#channel-group 2 mode passive**
Configurar el puerto de acceso de host para VLAN 3	Interface F0/18 Se realiza la inserción de estas líneas de comandos para Configurar el puerto de acceso de host para VLAN 3 en el Switch 2 **S2(config)#int fa 0/18** **S2(config-if)#no shutdown** **S2(config-if)#switchport mode access** **S2(config-if)#switchport access vlan 3**
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC Se realiza la inserción de estas líneas de comandos para Configurar la seguridad del puerto en los puertos de acceso en el Switch 1 **S2(config)#int fa0/18** **S2(config-if)#switchport port-security** **S2(config-if)#switchport port-security maximum 3** **S2(config)#show port-security**
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar Se realiza la inserción de estas líneas de comandos para Protejer todas las interfaces no utilizadas en el Switch 1 **S2#** **S2#config t** **Enter configuration commands, one per line. End with CNTL/Z.** **S2(config)#int range fa 0/3-17, fa 0/19-24, G 0/1-2** **S2(config-if-range)#no shutdown** **S2(config-if-range)#switchport mode access** **S2(config-if-range)#switchport access vlan 5** **S2(config-if-range)#description puertos sin usa** **S2(config-if-range)#exit** **S2(config)#**

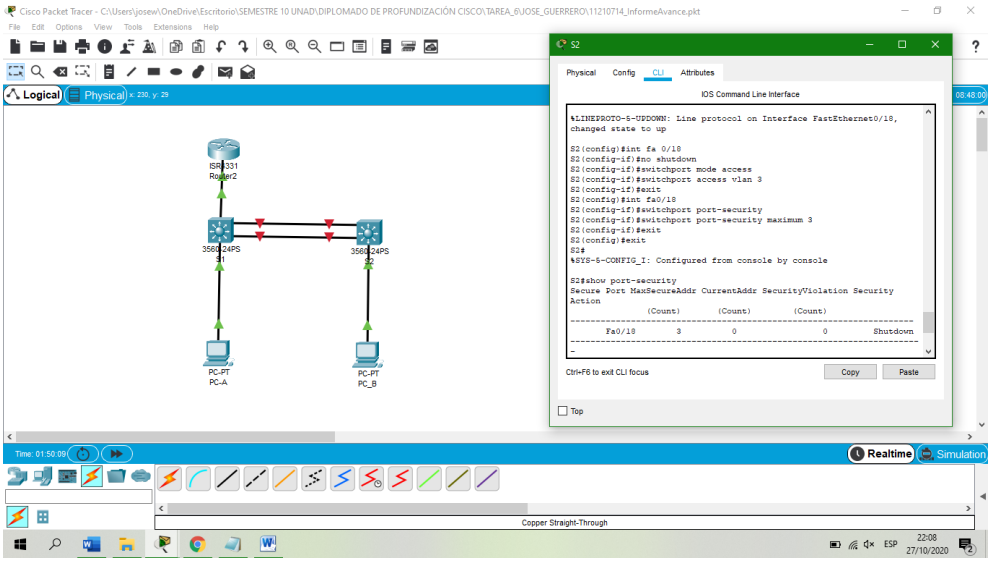
Figura 15. Configuración Switch 2 Vlans



Fuente: Autor

Se realizan las configuraciones de las VLAN en el Swicht 2 presentando su creación de forma exacta cumpliendo los parámetros solicitados.

Figura 16. Permitir 3 direcciones MAC



Fuente: Autor

Se utiliza el comando show port-security para verificar la Configurar la seguridad del puerto en los puertos de acceso Permitir 3 direcciones MAC

3. Parte 3: Configurar soporte de host

3.1. Paso 1: Configure R1

Apoyado en la topología de la red se realizará la configuración del soporte de host del Router R1 utilizando cada uno de los parámetros básicos establecidos en este escenario 1 como son Configuración Default Routing, IPv4 DHCP para VLAN 2 y la configuración de DHCP IPv4 para VLAN 3

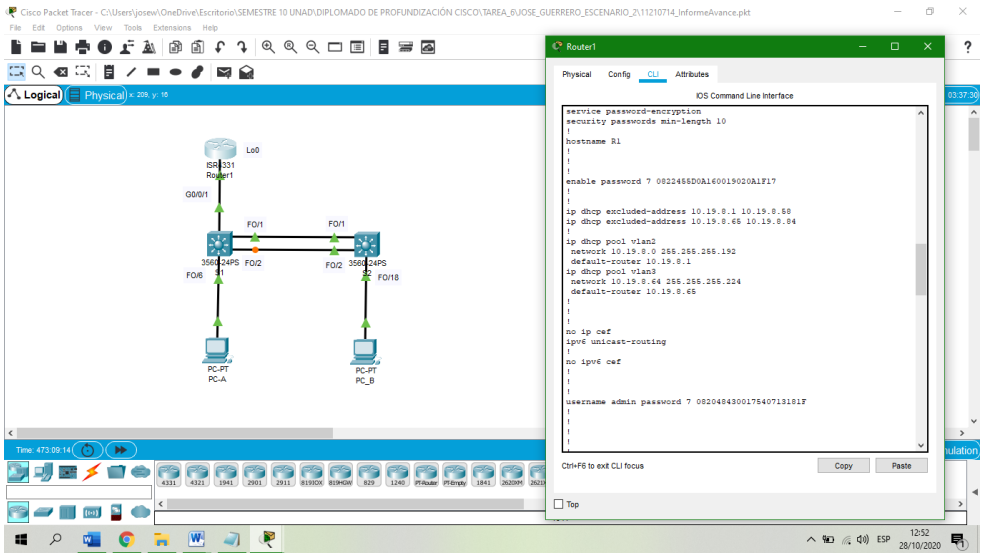
Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 12. Configuración Router 1 - R1) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración mostradas en la Tabla 12, podemos asegurar que el Router R1 quede configurado de la manera correcta.

Tabla 12. Configuración Router 1 - R1

Configuración Router 1 - R1	
Tarea	**Especificación**
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0 Se realiza la inserción de estas líneas de comandos para Configurar Default Routing en el Router 1 **R1(config)#ip route 0.0.0.0 0.0.0.0 Loopback0** **R1(config)#ipv6 route ::/0 Loopback0**
Configurar IPv4 DHCP para VLAN 2	Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada Se realiza la inserción de estas líneas de comandos para Configurar IPv4 DHCP para VLAN 2 en el Router 1 **R1(config)#ip dhcp pool vlan2** **R1(dhcp-config)#network 10.19.8.0 255.255.255.192** **R1(dhcp-config)#default-router 10.19.8.1** **R1(dhcp-config)#domain-name ccna-a.net** **R1(dhcp-config)#exit**

	R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.58
Configurar DHCP IPv4 para VLAN 3	Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada Se realiza la inserción de estas líneas de comandos para Configurar DHCP IPv4 para VLAN en el Router 1 **R1(config)#ip dhcp pool vlan3** **R1(dhcp-config)#network 10.19.8.64 255.255.255.224** **R1(dhcp-config)#default-router 10.19.8.65** **R1(dhcp-config)#domain-name ccna-b.net** **R1(dhcp-config)#exit** **R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84**

Figura 17. Prueba configuración IPv4 DHCP para VLAN 2 y VLAN 3



Fuente: Autor

Se realiza la verificación sobre Configuración Default Routing, IPv4 DHCP para VLAN 2 y la configuración de DHCP IPv4 para VLAN 3 en la configuración general de R1 siendo exitoso este procedimiento.

3.2. Paso 2: Configurar los servidores

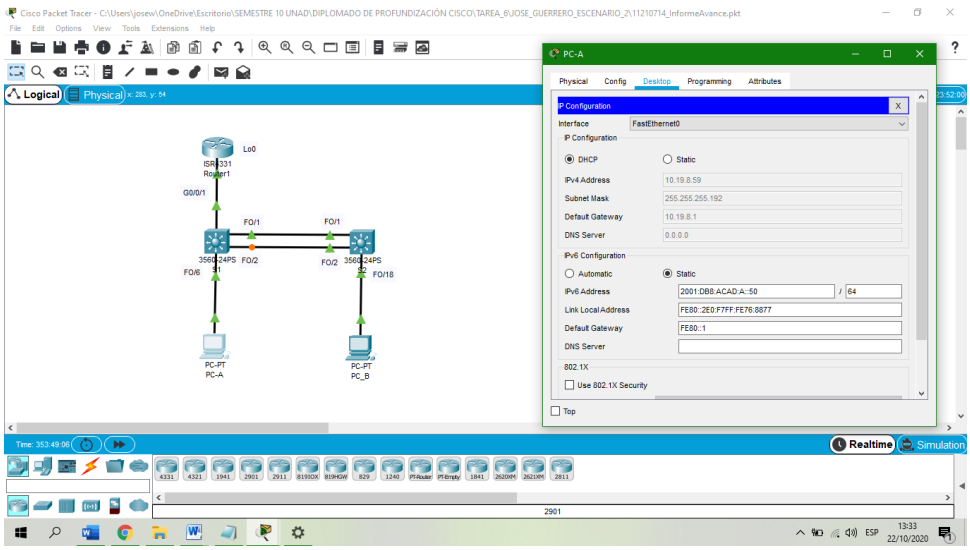
Apoyado en la topología de la red se realizará la configuración del equipo PC-A y PC-B utilizando cada uno de los parámetros básicos establecidos en este escenario 1 como son direccionamiento IPv4, la máscara de subred para IPv4, la puerta de enlace predeterminada (gateway predeterminado), la dirección IPv6/subred, la puerta de enlace predeterminada IPv6 (gateway predeterminado IPv6), para esta tarea se realizará el uso de diferentes direcciones IP las cuales permitirán el correcto direccionamiento.

Para realizar la configuración de los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asignar estáticamente las direcciones IPv6 GUA y Link Local se utilizarán las direcciones establecidas en las siguientes tablas (Tabla 13. Configuración de red de PC-A) y (Tabla 14. Configuración de red de PC-B) por tal motivo con cada una las tareas de configuración de direcciones, mostradas en las Tabla 13 y 14, podemos asegurar que cada uno de los dispositivos de red queden configurados de forma correcta.

Tabla 13. Configuración de red de PC-A

Configuración de red de PC-A	
Tarea	**Especificación**
Descripción	Datos tomados por DHCP
Dirección física	FE80::2E0:F7FF:FE76:8877
Dirección IP	10.19.8.59
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

Figura 18. Configuración de red de PC-A



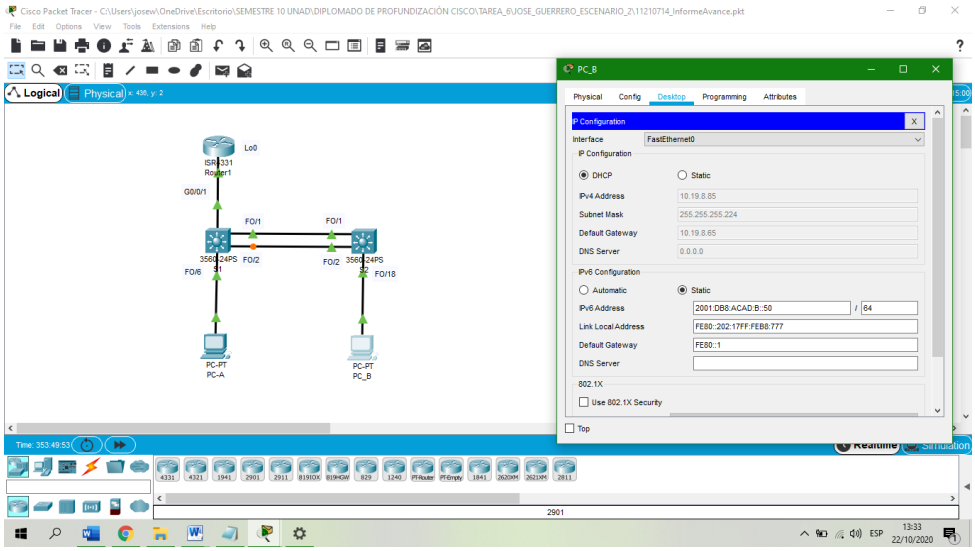
Fuente: Autor

Se realiza el procedimiento de Configuración del direccionamiento de red de PC-A utilizando las direcciones propuestas de acuerdo a Datos tomados por DHCP mostrados en (Tabla 11. Configuración de red de PC-A) siendo exitoso su configuración.

Tabla 14. Configuración de red de PC-B

Configuración de red de PC-B	
Tarea	**Especificación**
Descripción	Datos tomados por DHCP
Dirección física	0002.17B8.0777
Dirección IP	10.19.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::1

Figura 19. Configuración de red de PC-B



Fuente: Autor

Se realiza el procedimiento de Configuración del direccionamiento de red de PC-B utilizando las direcciones propuestas de acuerdo a Datos tomados por DHCP mostrados en (Tabla 12. Configuración de red de PC-B) siendo exitoso su configuración.

4. Parte 4: Probar y verificar la conectividad de extremo a extremo

Para realizar la prueba de pines entre dispositivos se utilizarán las direcciones establecidas en las siguientes tablas (Tabla 15. Verificación de pines entre equipos de escenario 1)

Tabla 15. Verificación de pines entre equipos de escenario 1

Verificación de pines entre equipos de escenario 1				
Desde	**A**	**de Internet**	**Dirección IP**	**Resultados de ping**
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	El ping IPv4 Si fue realizado con éxito
		IPv6	2001:db8:acad:a::1	El ping IPv6 Si fue realizado con éxito

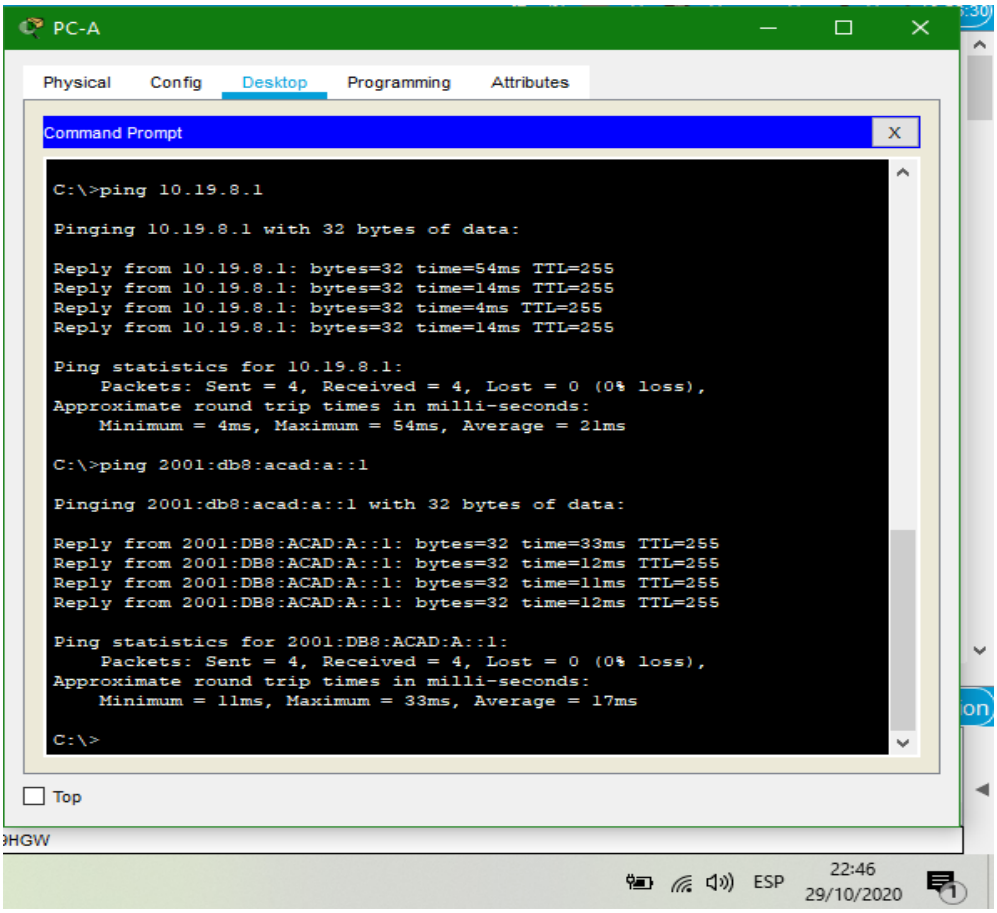
	R1, G0/0/1.3	Dirección	10.19.8.65	El ping IPv4 Si fue realizado con éxito
		IPv6	2001:db8:acad:b::1	El ping IPv6 Si fue realizado con éxito
	R1, G0/0/1.4	Dirección	10.19.8.97	El ping IPv4 Si fue realizado con éxito
		IPv6	2001:db8:acad:c::1	El ping IPv6 Si fue realizado con éxito
	S1, VLAN 4	Dirección	10.19.8.98	El ping IPv4 Si fue realizado con éxito
		IPv6	2001:db8:acad:c::98	El ping IPv6 Si fue realizado con éxito
	S2, VLAN 4	Dirección	10.19.8.99.	El ping IPv4 Si fue realizado con éxito
		IPv6	2001:db8:acad:c::99	El ping IPv6 Si fue realizado con éxito
	PC-B	Dirección	IP address will vary. 10.19.8.85	El ping IPv4 Si fue realizado con éxito
		IPv6	2001:db8:acad:b: :50	El ping IPv6 Si fue realizado con éxito
	R1 Bucle 0	Dirección	209.165.201.1	El ping IPv4 Si fue realizado con éxito
		IPv6	2001:db8:acad:209::1	El ping IPv6 Si fue realizado con éxito
PC-B	R1 Bucle 0	Dirección	209.165.201.1	El ping IPv4 Si fue realizado con éxito
		IPv6	2001:db8:acad:209: :1	El ping IPv6 Si fue realizado con éxito
	R1, G0/0/1.2	Dirección	10.19.8.1	El ping IPv4 Si fue realizado con éxito
		IPv6	2001:db8:acad:a::1	El ping IPv6 Si fue realizado con éxito
	R1, G0/0/1.3	Dirección	10.19.8.65	El ping IPv4 Si fue realizado con éxito
		IPv6	2001:db8:acad:b::1	El ping IPv6 Si fue realizado con éxito
	R1, G0/0/1.4	Dirección	10.19.8.97	El ping IPv4 Si fue realizado con éxito
		IPv6	2001:db8:acad:c::1	El ping IPv6 Si fue realizado con éxito
	S1, VLAN 4	Dirección	10.19.8.98	El ping IPv4 Si fue realizado con éxito

		IPv6	2001:db8:acad:c: :98	El ping IPv6 Si fue realizado con éxito
	S2, VLAN 4	Dirección	10.19.8.99.	El ping IPv4 Si fue realizado con éxito
		IPv6	2001:db8:acad:c: :99	El ping IPv6 Si fue realizado con éxito

4.1. Verificación mediante pines desde la PC- A hacia otras direcciones

Para realizar cada ping entre dispositivo se debe tener en cuenta el tipo de dirección a la cual se quiere hacer el procedimiento identificando si estas es IPv4 o IPv6 puesto que la estructura de dirección tiene diferente sintaxis.

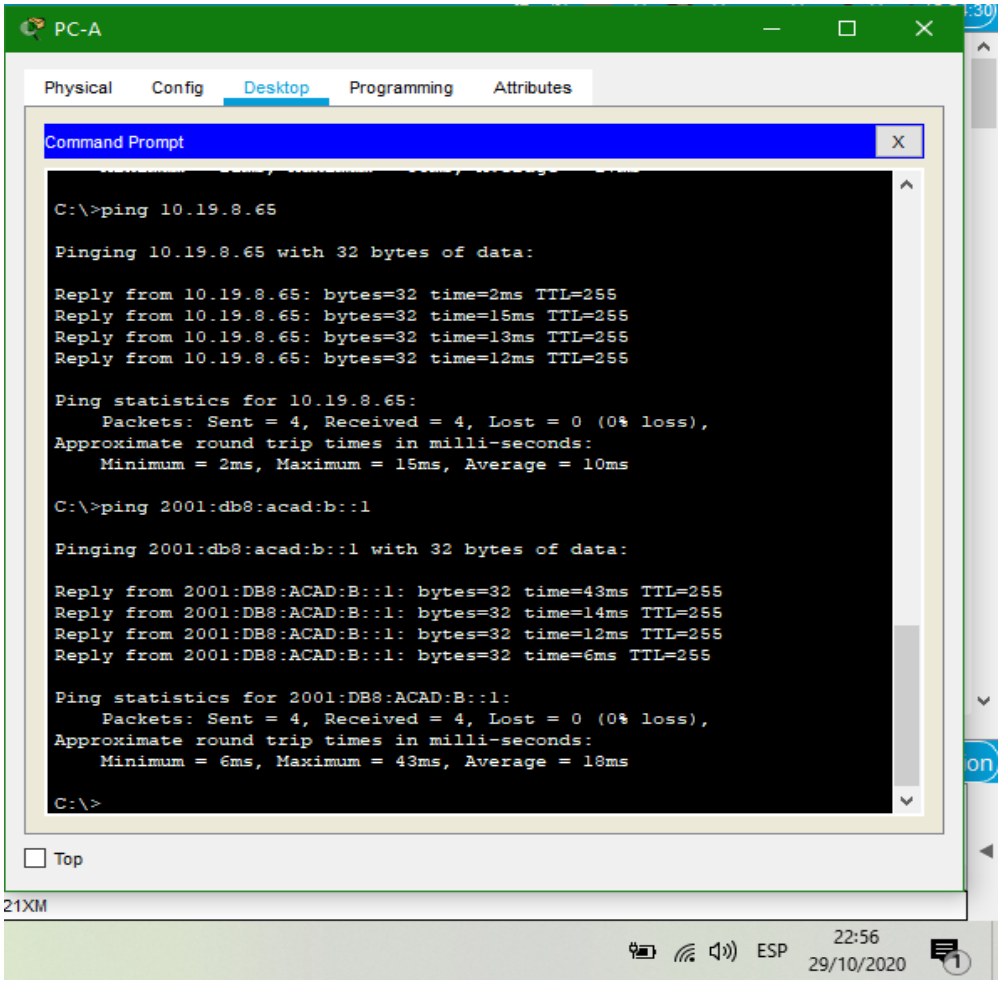
Figura 20. Pin desde la PC_A hacia R1, G0/0/1.2 en IPv4 e IPv6



Fuente: Autor

Se realiza pin desde la **PC_A** hacia **R1, G0/0/1.2** enviando los paquetes a su dirección **IPv4** utilizando el comando **ping 10.19.8.1** logrando realizar el pin con éxito del mismo modo se realiza pin desde la **PC_A** hacia **R1, G0/0/1.2** enviando los paquetes a su dirección **IPv6** utilizando el comando **ping 2001:db8:acad:a::1** logrando realizar el pin también con éxito

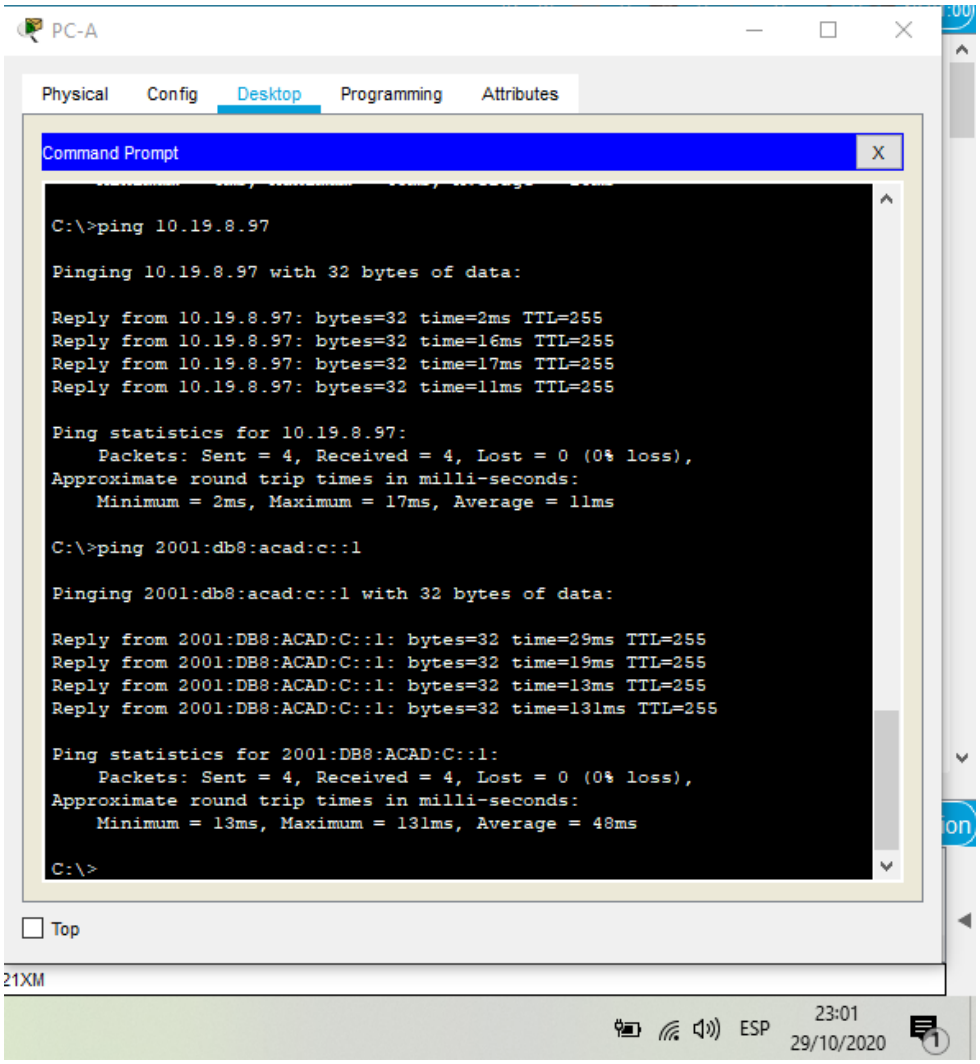
Figura 21. Pin desde la PC_A hacia R1, G0/0/1.3 en IPv4 e IPv6



Fuente: Autor

Se realiza pin desde la **PC_A** hacia **R1, G0/0/1.3** enviando los paquetes a su dirección **IPv4** utilizando el comando **ping 10.19.8.65** logrando realizar el pin con éxito del mismo modo se realiza pin desde la **PC_A** hacia **R1, G0/0/1.3** enviando los paquetes a su dirección **IPv6** utilizando el comando **ping 2001:db8:acad:b::1** logrando realizar el pin también con éxito

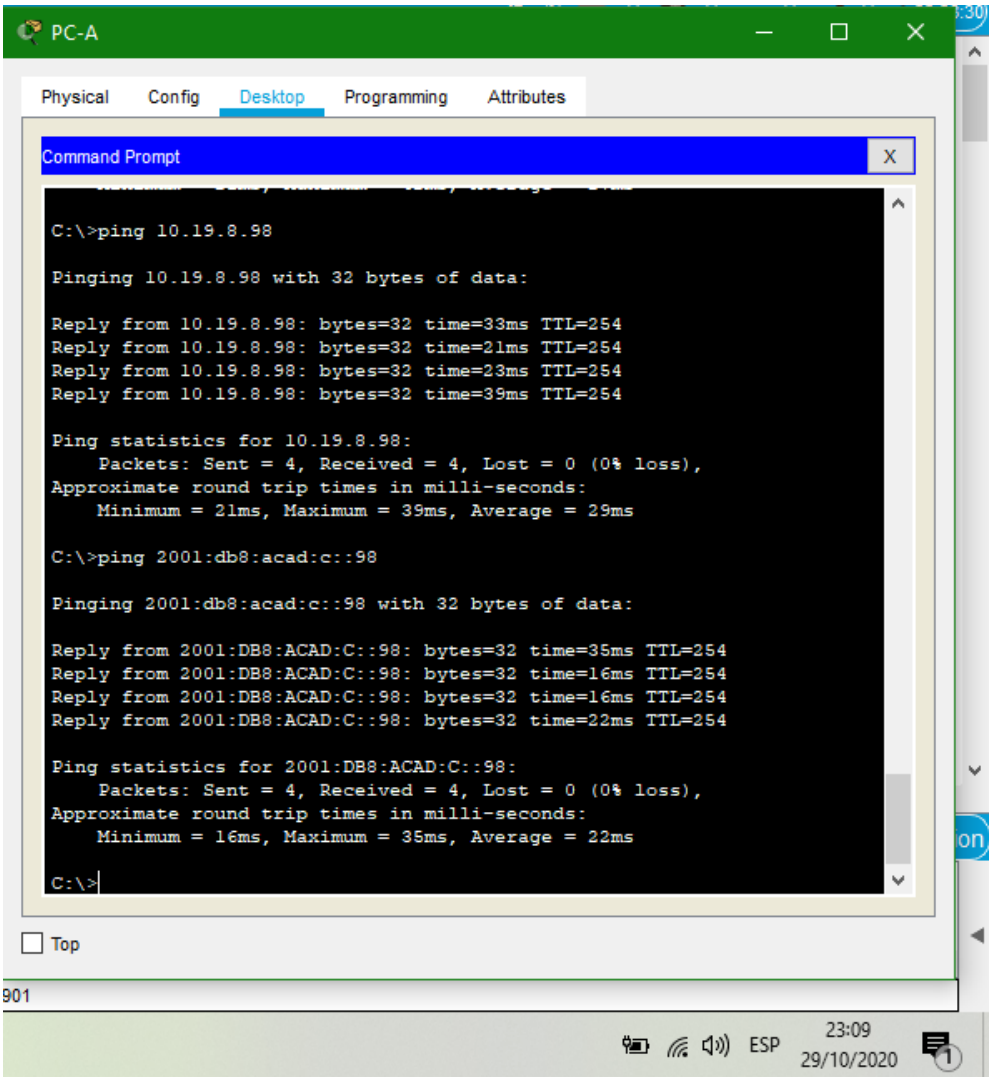
Figura 22. Pin desde la PC_A hacia R1, G0/0/1.4 en IPv4 e IPv6



Fuente: Autor

Se realiza pin desde la **PC_A** hacia **R1, G0/0/1.4** enviando los paquetes a su dirección **IPv4** utilizando el comando **ping 10.19.8.97** logrando realizar el pin con éxito del mismo modo se realiza pin desde la **PC_A** hacia **R1, G0/0/1.4** enviando los paquetes a su dirección **IPv6** utilizando el comando **ping 2001:db8:acad:c::1** logrando realizar el pin también con éxito

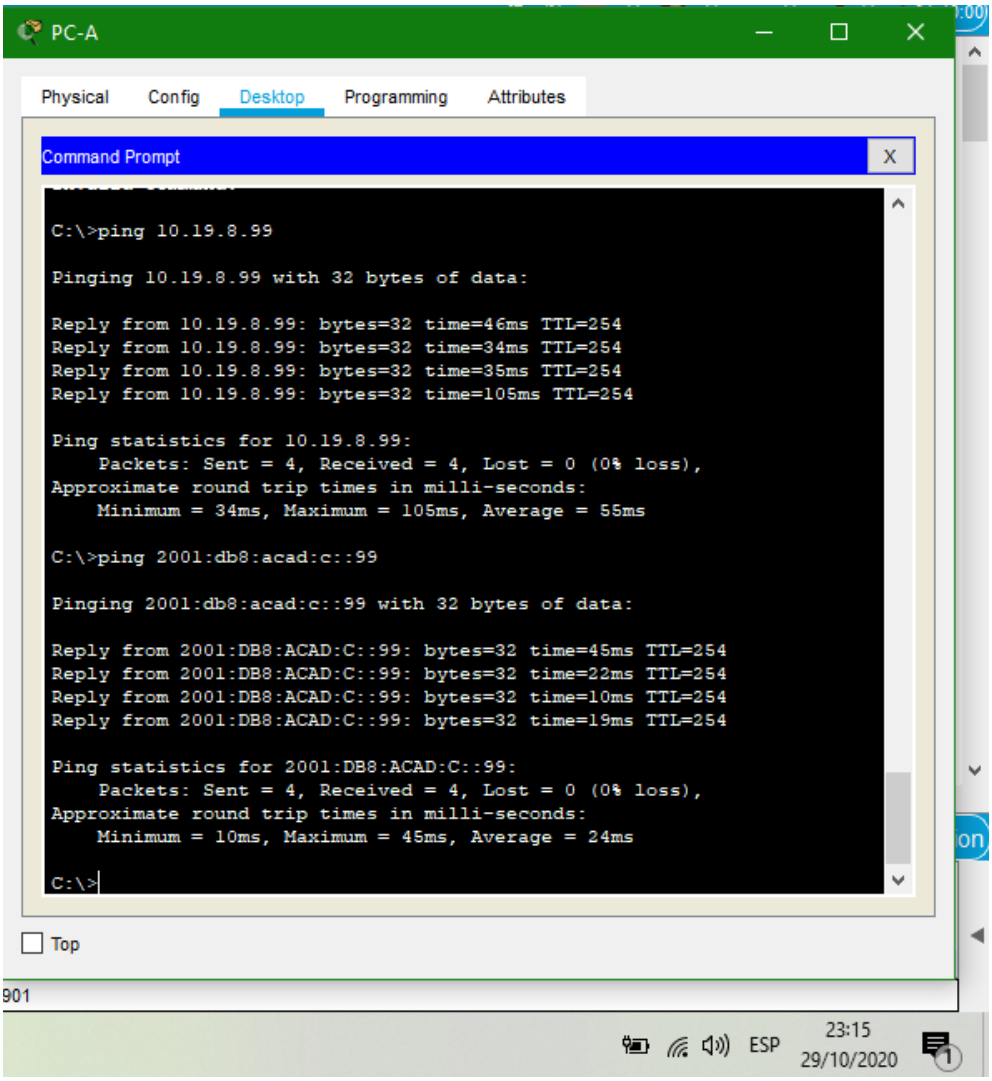
Figura 23. Pin desde la PC_A hacia S1, VLAN 4 en IPv4 e IPv6



Fuente: Autor

Se realiza pin desde la **PC_A** hacia **S1, VLAN 4** enviando los paquetes a su dirección **IPv4** utilizando el comando **ping 10.19.8.98** logrando realizar el pin con éxito del mismo modo se realiza pin desde la **PC_A** hacia **S1, VLAN 4** enviando los paquetes a su dirección **IPv6** utilizando el comando **ping 2001:db8:acad:c::98** logrando realizar el pin también con éxito

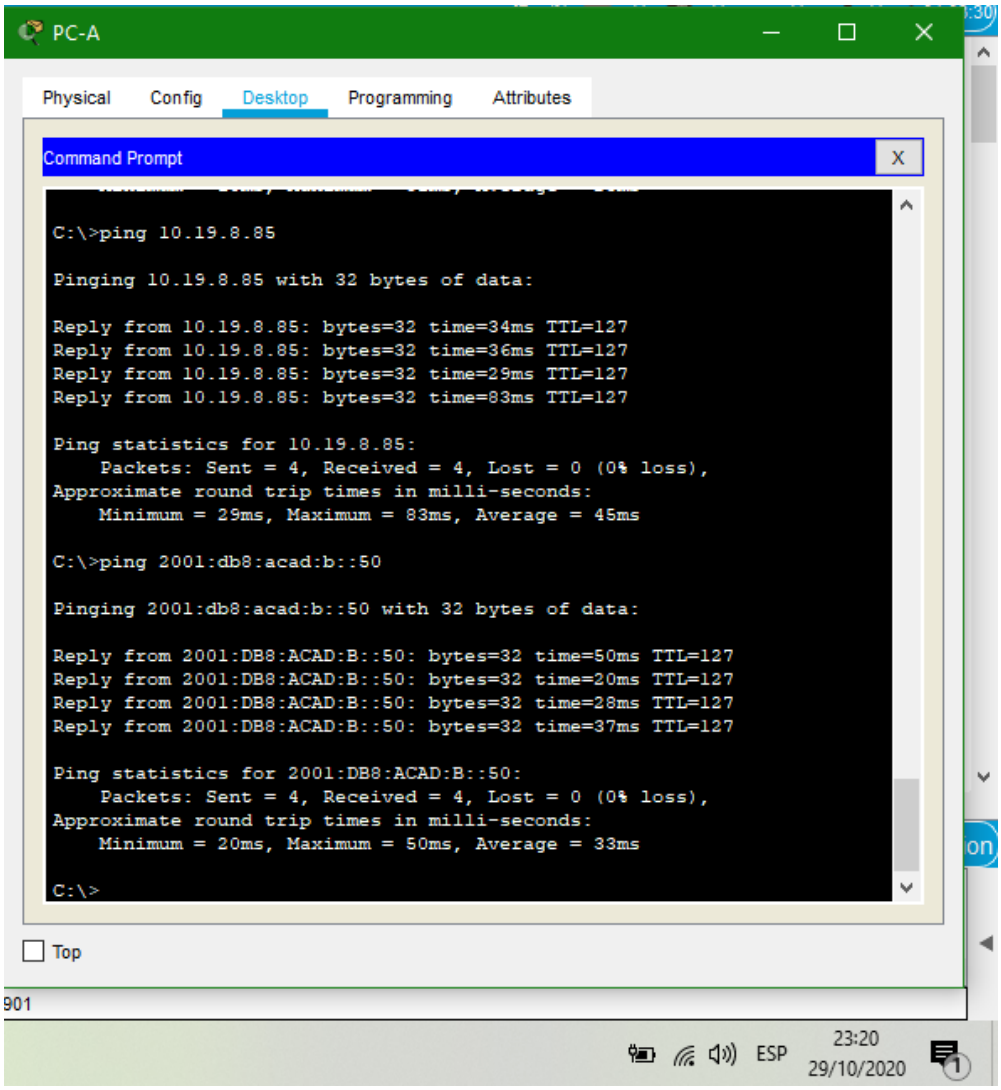
Figura 24. Pin desde la PC_A hacia S2, VLAN 4 en IPv4 e IPv6



Fuente: Autor

Se realiza pin desde la **PC_A** hacia **S2, VLAN 4** enviando los paquetes a su dirección **IPv4** utilizando el comando **ping 10.19.8.99** logrando realizar el pin con éxito del mismo modo se realiza pin desde la **PC_A** hacia **S2, VLAN 4** enviando los paquetes a su dirección **IPv6** utilizando el comando **ping 2001:db8:acad:c::99** logrando realizar el pin también con éxito

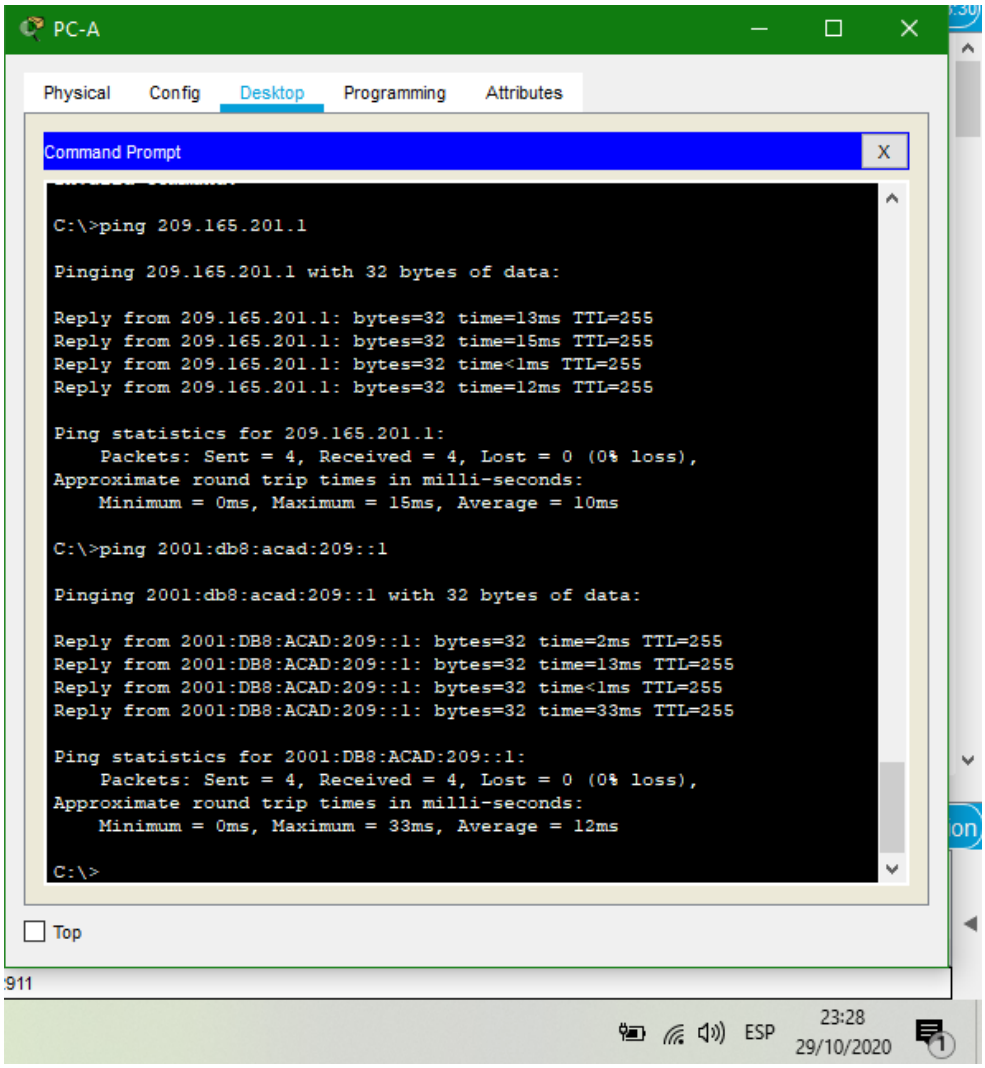
Figura 25. Pin desde la PC_A hacia PC-B en IPv4 e IPv6



Fuente: Autor

Se realiza pin desde la **PC_A** hacia **PC-B** enviando los paquetes a su dirección **IPv4** utilizando el comando **ping 10.19.8.85** logrando realizar el pin con éxito del mismo modo se realiza pin desde la **PC_A** hacia **PC-B** enviando los paquetes a su dirección **IPv6** utilizando el comando **ping 2001:db8:acad:b: :50** logrando realizar el pin también con éxito

Figura 26. Pin desde la PC_A hacia R1, Bucle 0 en IPv4 e IPv6

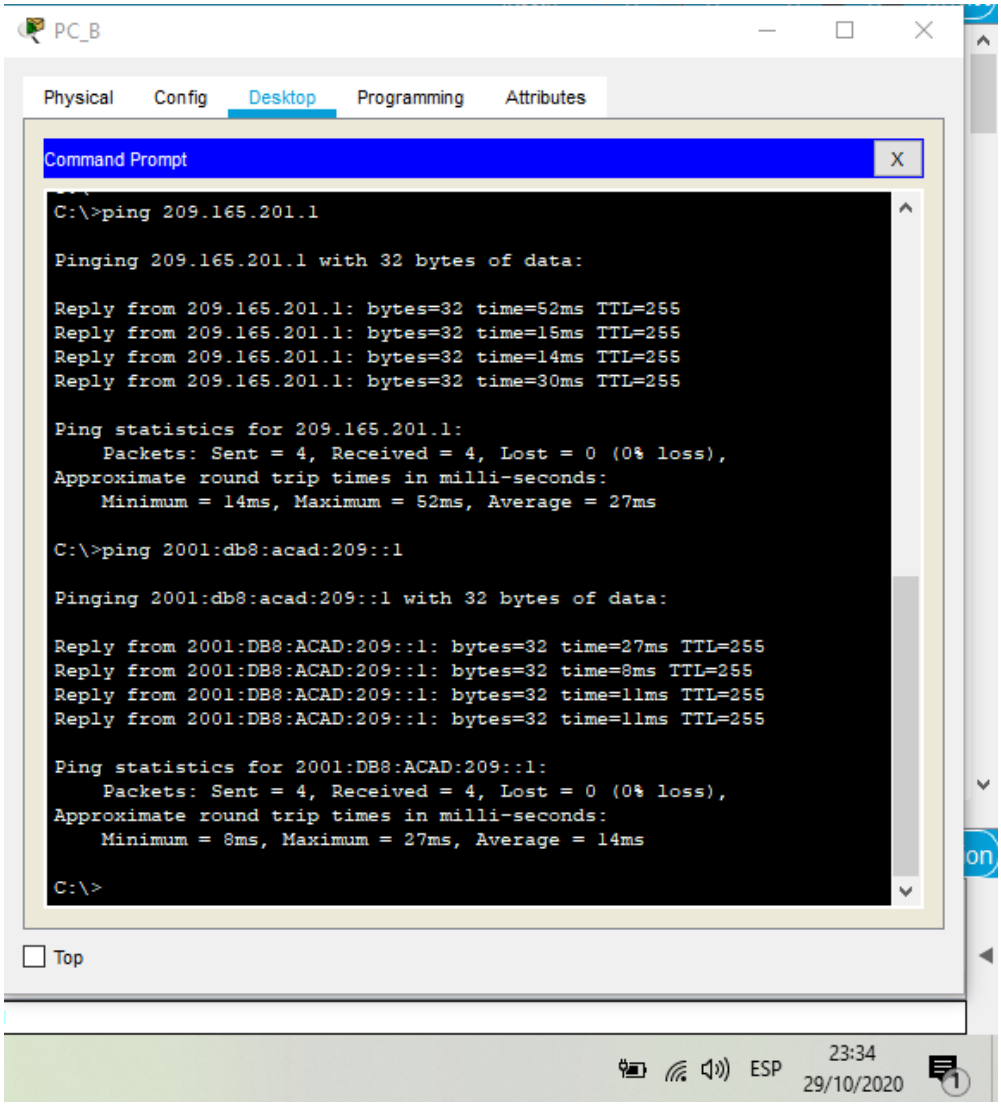


Fuente: Autor

Se realiza pin desde la **PC_A** hacia **R1, Bucle 0**enviando los paquetes a su dirección **IPv4** utilizando el comando **ping 209.165.201.1** logrando realizar el pin con éxito del mismo modo se realiza pin desde la **PC_A** hacia **R1, Bucle 0** enviando los paquetes a su dirección **IPv6** utilizando el comando **ping 2001:db8:acad:209::1** logrando realizar el pin también con éxito

4.2. Verificación mediante pines desde la PC- B hacia otras direcciones

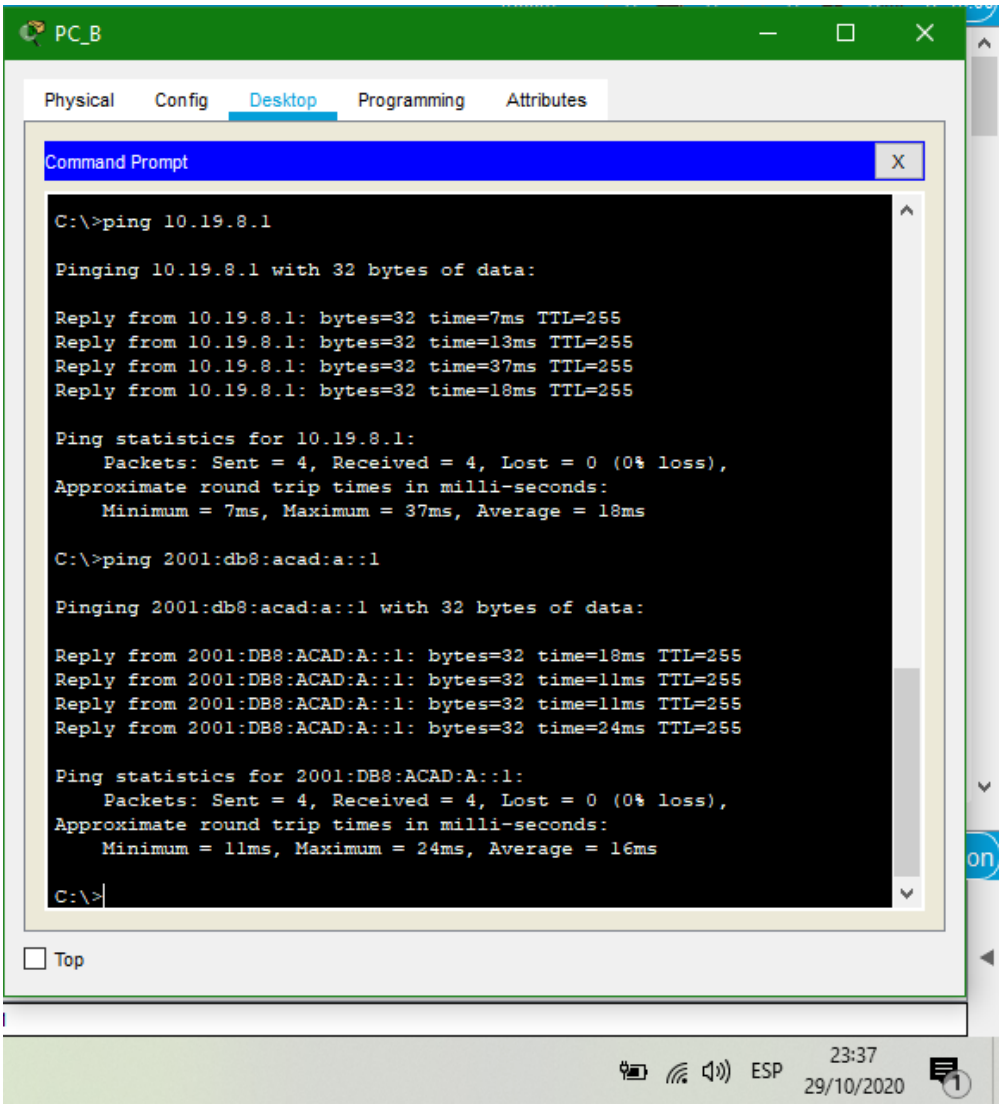
Figura 27. Pin desde la PC_A hacia R1, G0/0/1.2 en IPv4 e IPv6



Fuente: Autor

Se realiza pin desde la **PC_B** hacia **R1, Bucle 0** enviando los paquetes a su dirección **IPv4** utilizando el comando **ping 209.165.201.1** logrando realizar el pin con éxito del mismo modo se realiza pin desde la **PC_A** hacia **R1, Bucle 0** enviando los paquetes a su dirección **IPv6** utilizando el comando **ping 2001:db8:acad:209::1** logrando realizar el pin también con éxito

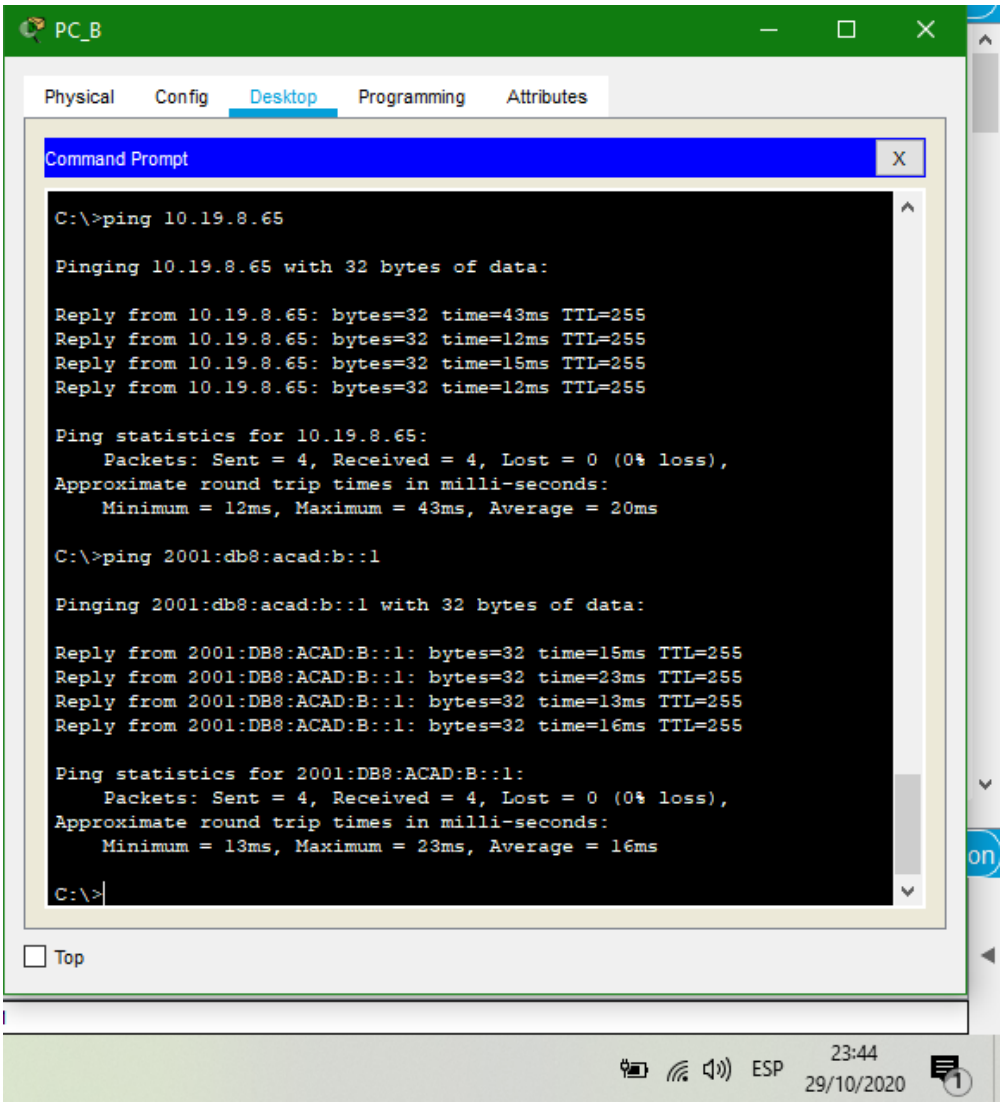
Figura 28. Pin desde la PC_B hacia R1, G0/0/1.2 en IPv4 e IPv6



Fuente: Autor

Se realiza pin desde la **PC_B** hacia **R1, G0/0/1.2** enviando los paquetes a su dirección **IPv4** utilizando el comando **ping 10.19.8.1** logrando realizar el pin con éxito del mismo modo se realiza pin desde la **PC_B** hacia **R1, G0/0/1.2** enviando los paquetes a su dirección **IPv6** utilizando el comando **ping 2001:db8:acad:a::1** logrando realizar el pin también con éxito

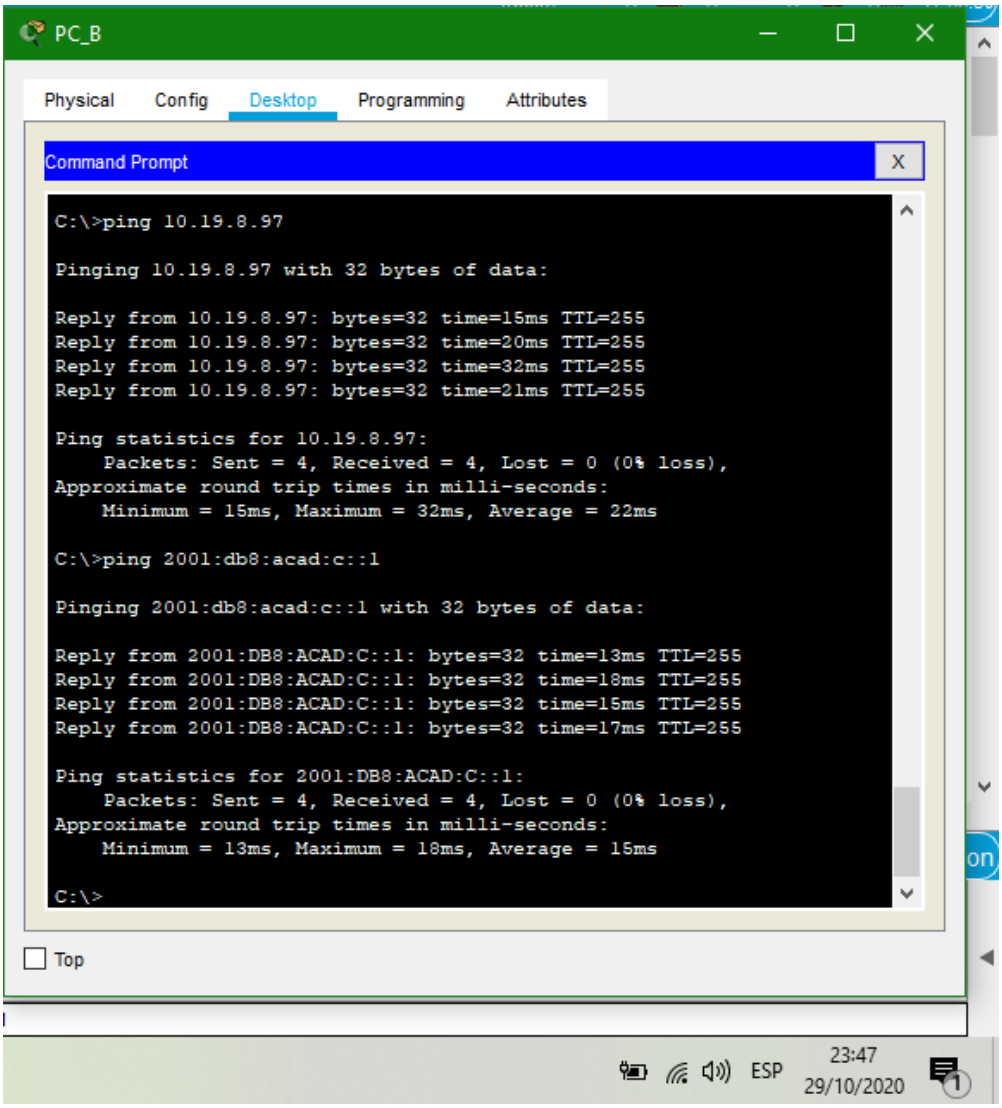
Figura 29. Pin desde la PC_B hacia R1, G0/0/1.3 en IPv4 e IPv6



Fuente: Autor

Se realiza pin desde la **PC_B** hacia **R1, G0/0/1.3** enviando los paquetes a su dirección **IPv4** utilizando el comando **ping 10.19.8.65** logrando realizar el pin con éxito del mismo modo se realiza pin desde la **PC_B** hacia **R1, G0/0/1.3** enviando los paquetes a su dirección **IPv6** utilizando el comando **ping 2001:db8:acad:b::1** logrando realizar el pin también con éxito

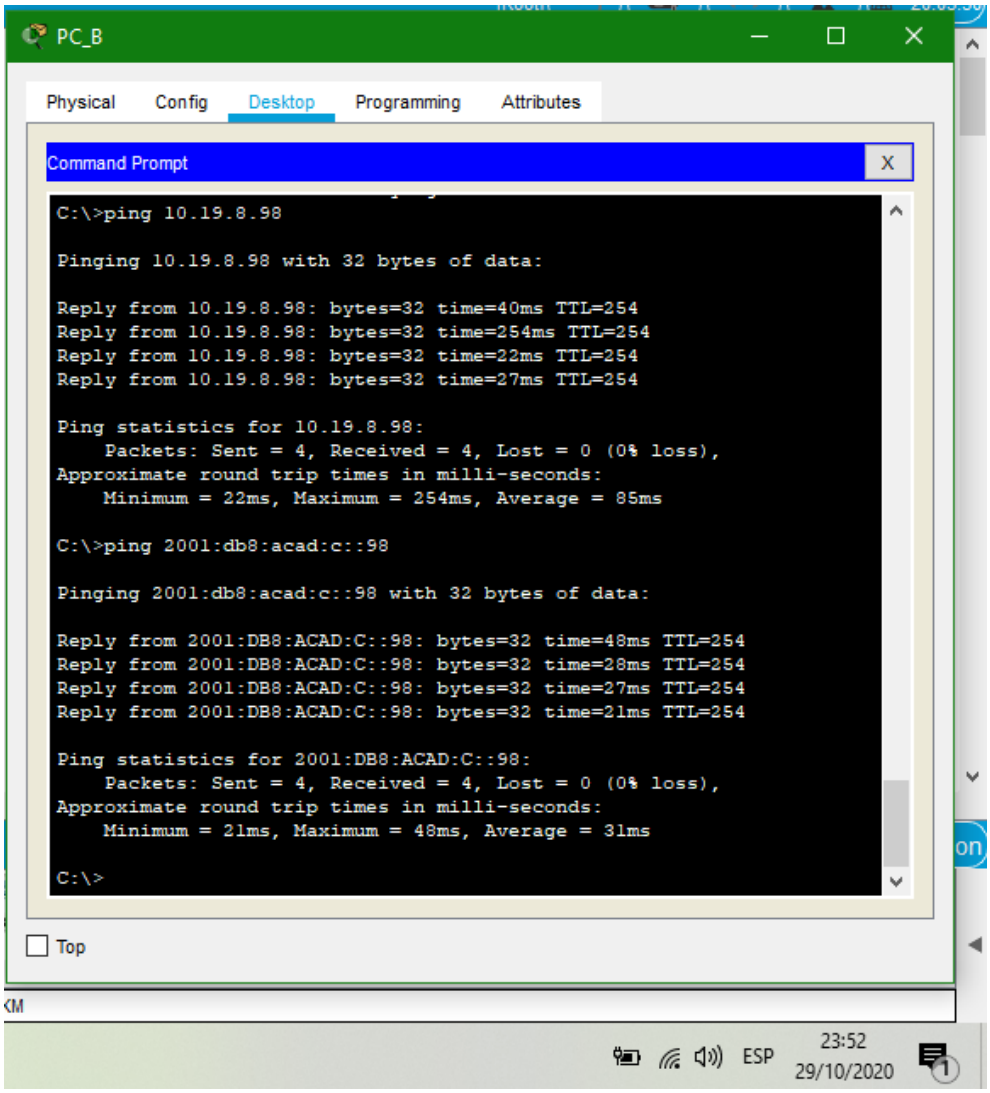
Figura 30. Pin desde la PC_B hacia R1, G0/0/1.4 en IPv4 e IPv6



Fuente: Autor

Se realiza pin desde la **PC_B** hacia **R1, G0/0/1.4** enviando los paquetes a su dirección **IPv4** utilizando el comando **ping 10.19.8.97** logrando realizar el pin con éxito del mismo modo se realiza pin desde la **PC_B** hacia **R1, G0/0/1.4** enviando los paquetes a su dirección **IPv6** utilizando el comando **ping 2001:db8:acad:c::1** logrando realizar el pin también con éxito

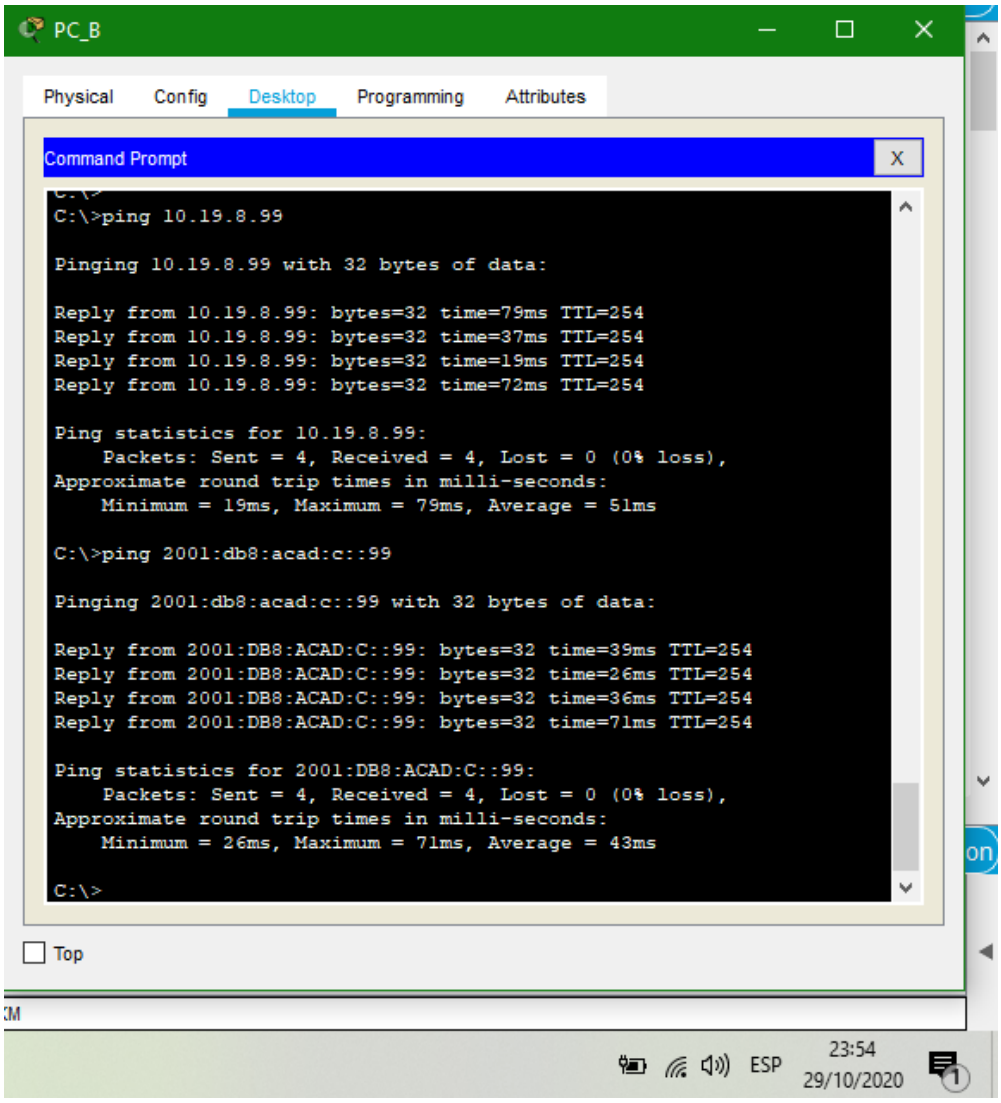
Figura 31. Pin desde la PC_B hacia S1, VLAN 4 en IPv4 e IPv6



Fuente: Autor

Se realiza pin desde la **PC_B** hacia **S1, VLAN 4** enviando los paquetes a su dirección **IPv4** utilizando el comando **ping 10.19.8.98** logrando realizar el pin con éxito del mismo modo se realiza pin desde la **PC_B** hacia **S1, VLAN 4** enviando los paquetes a su dirección **IPv6** utilizando el comando **ping 2001:db8:acad:c::98** logrando realizar el pin también con éxito

Figura 32. Pin desde la PC_B hacia S2, VLAN 4 en IPv4 e IPv6



Fuente: Autor

Se realiza pin desde la **PC_B** hacia **S2, VLAN 4** enviando los paquetes a su dirección **IPv4** utilizando el comando **ping 10.19.8.99** logrando realizar el pin con éxito del mismo modo se realiza pin desde la **PC_B** hacia **S2, VLAN 4** enviando los paquetes a su dirección **IPv6** utilizando el comando **ping 2001:db8:acad:c::99** logrando realizar el pin también con éxito

ESCENARIO 2.

Topología

Figura 33. Topología escenario 2

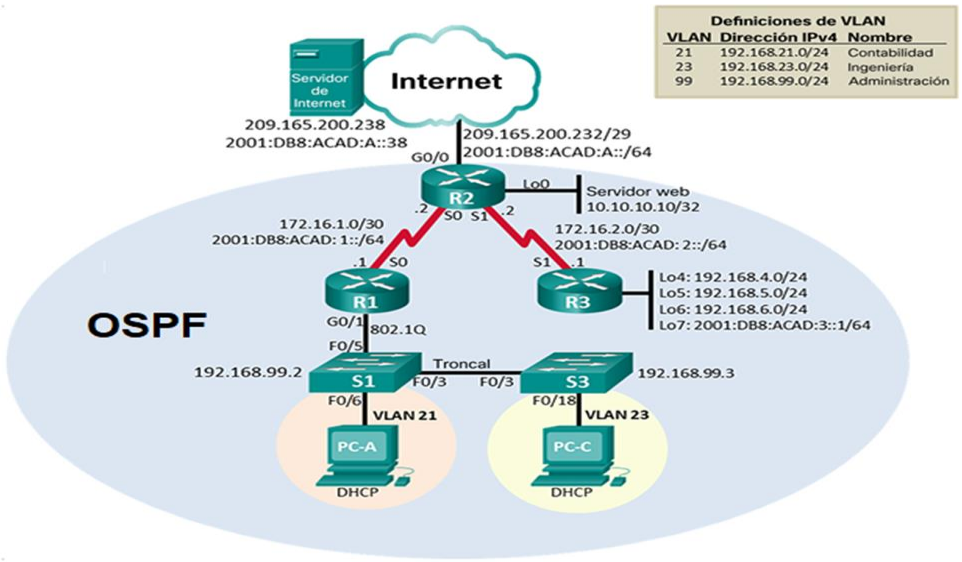
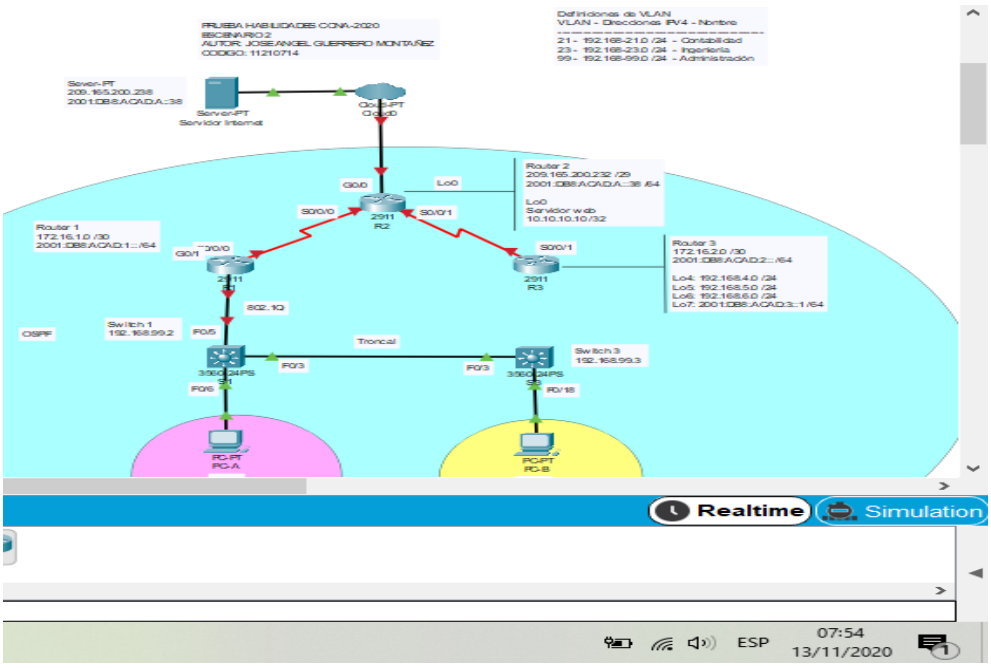


Figura 34. Topología creada Escenario 2



Fuente: Autor

Para el escenario 2 se realiza la creación de la topología necesaria en el software Packet Tracer empleando los siguientes equipos de este aplicativo.

- 01 servidor (Server-PT)
- 01 nube (Cloud-PT)
- 01 Router 2911 para R1
- 01 Router 2911 para R2
- 01 Router 2911 para R3
- 01 Switch 3560 para S1
- 01 Switch 3560 para S2
- 01 PC para PC-A
- 01 PC para PC-B

5. Parte 1: Inicializar dispositivos

5.1. Paso 1: Inicializar y volver a cargar los router y los switches

La primera medida que se debe tomar antes de introducir cualquier configuración a los router y los switches en este paso, es realizar la eliminación de la configuración de inicio de cada dispositivo y paso posterior volver a cargar estos dispositivos, para esta tarea se realizara el uso de diferentes comandos con el fin de establecer borrado y carga los cuales se encontraran mostrados o contenidos en la (Tabla 16. Borrado Router y Switches Escenario 2) por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 16, podemos asegurar que cada uno de los dispositivos de red no tengan almacenados datos en memoria y en los cuales se pueden encontrar, la base de datos de VLAN además de otras configuraciones que vienen por defecto o ya preestablecidas.

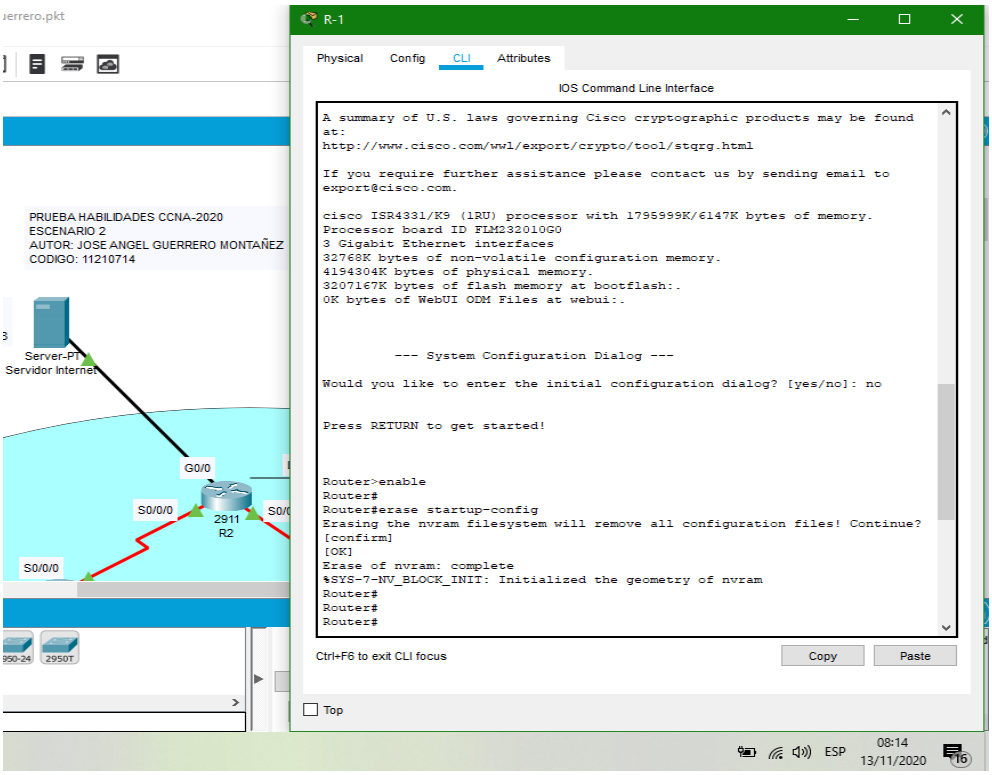
5.1.1 Borrado configuraciones Router

Los siguientes son los comandos utilizados con su respuesta respectiva en el router 1 para el procedimiento de borrado de las configuraciones predeterminadas, el procedimiento es igual en todos los router

Tabla 16. Borrado configuraciones Router Escenario 2

Borrado configuraciones Router Escenario 1	
Tarea	**Especificación**
Eliminar el archivo startup-config de todos los routers	Se realiza la inserción de esta línea de comandos para eliminar configuraciones del router. **Router>enable** **Router#erase startup-config**

Figura 35. Borrado configuraciones Router Escenario 2



Fuente: Autor

Mediante el comando erase startup-config se realiza el borrado de la base de datos preconfigurado en la memoria flash del R1 siendo exitoso.

5.1.2 Borrado configuraciones y base datos VLAN Switch

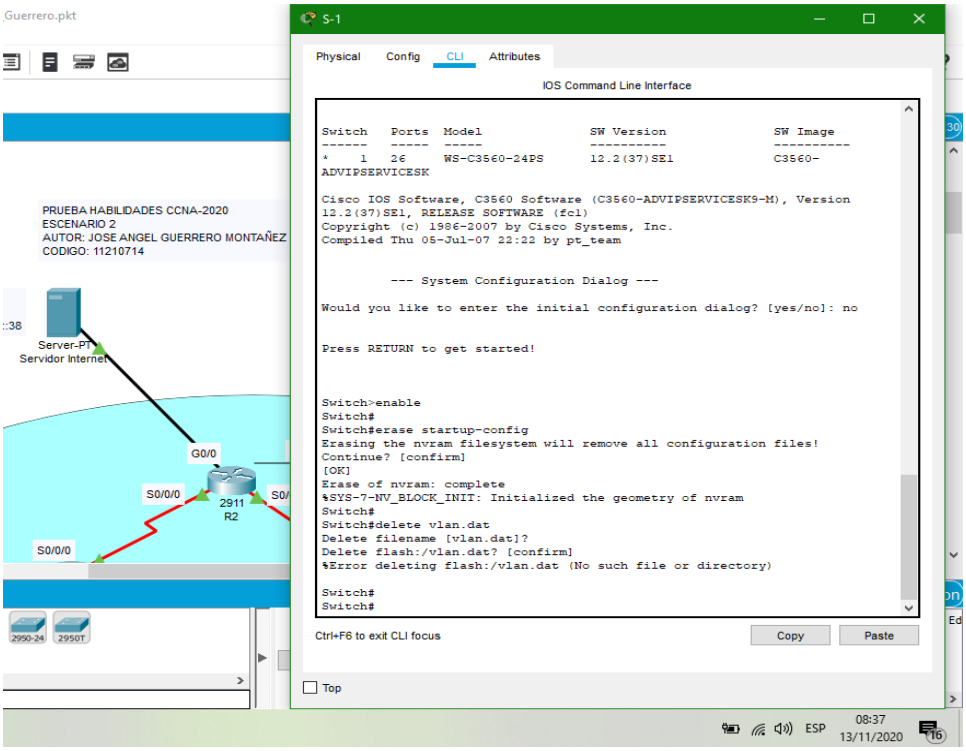
Los siguientes son los comandos utilizados con su respuesta respectiva en el Switch 1 para el procedimiento de borrado de las configuraciones predeterminadas, así como el borrado de la base de datos de VLAN del Switch el procedimiento es igual en todos los Switch.

Tabla 17. Borrado configuraciones Switches Escenario 2

Borrado configuraciones Switches Escenario 2	
Tarea	**Especificación**
Eliminar el archivo startup-config de todos los switch y eliminar la base de datos de VLAN	Se realiza la inserción de esta línea de comandos para eliminar las configuraciones y la base de datos de VLAN del switch **Switch>enable**

	Switch#erase startup-config **Switch#delete vlan.dat**
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Se realiza la inserción de esta línea de comandos para verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches **Switch>enable** **Switch#show vlan brief**

Figura 36. Borrado configuraciones iniciales y base de datos de VLAN en S1

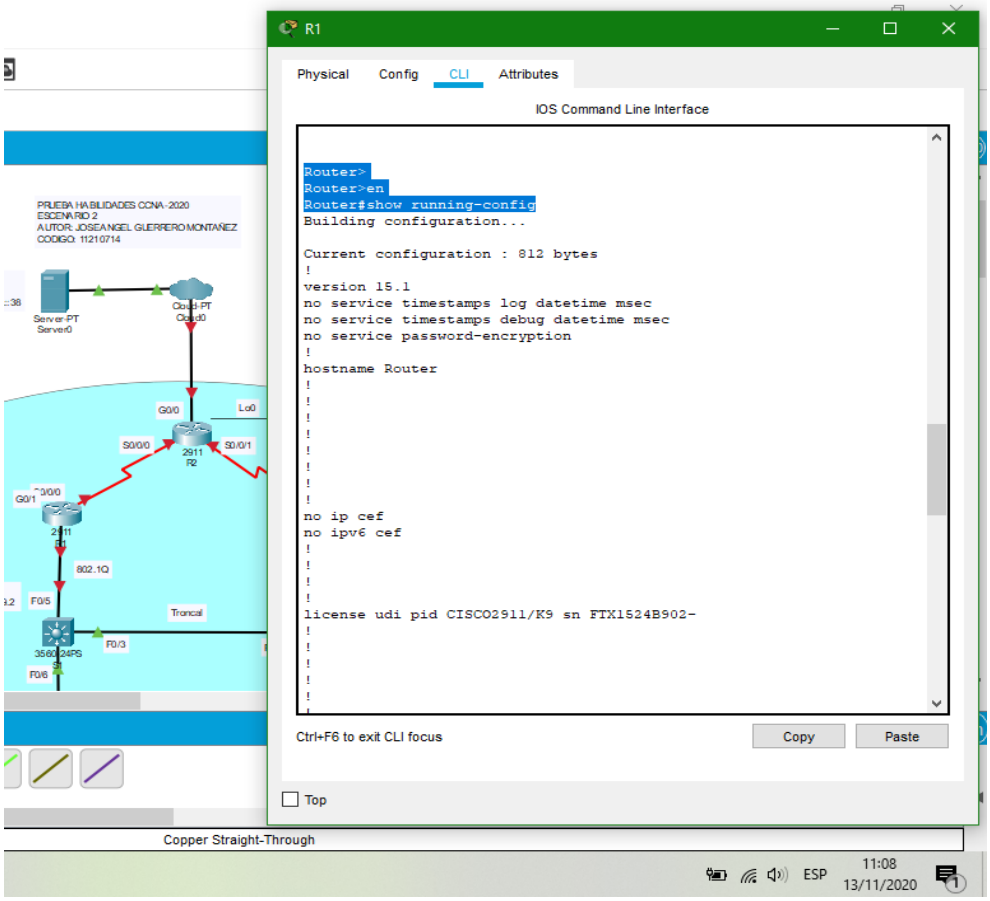


Fuente: Autor

Mediante los comandos de la tabla 17 se realiza Borrado configuraciones iniciales y base de datos de VLAN de S1 siendo exitoso su borrado el procedimiento es igual en los demás Switches.

5.1.3 Verificación borrado configuraciones Router R1, R2 y R3

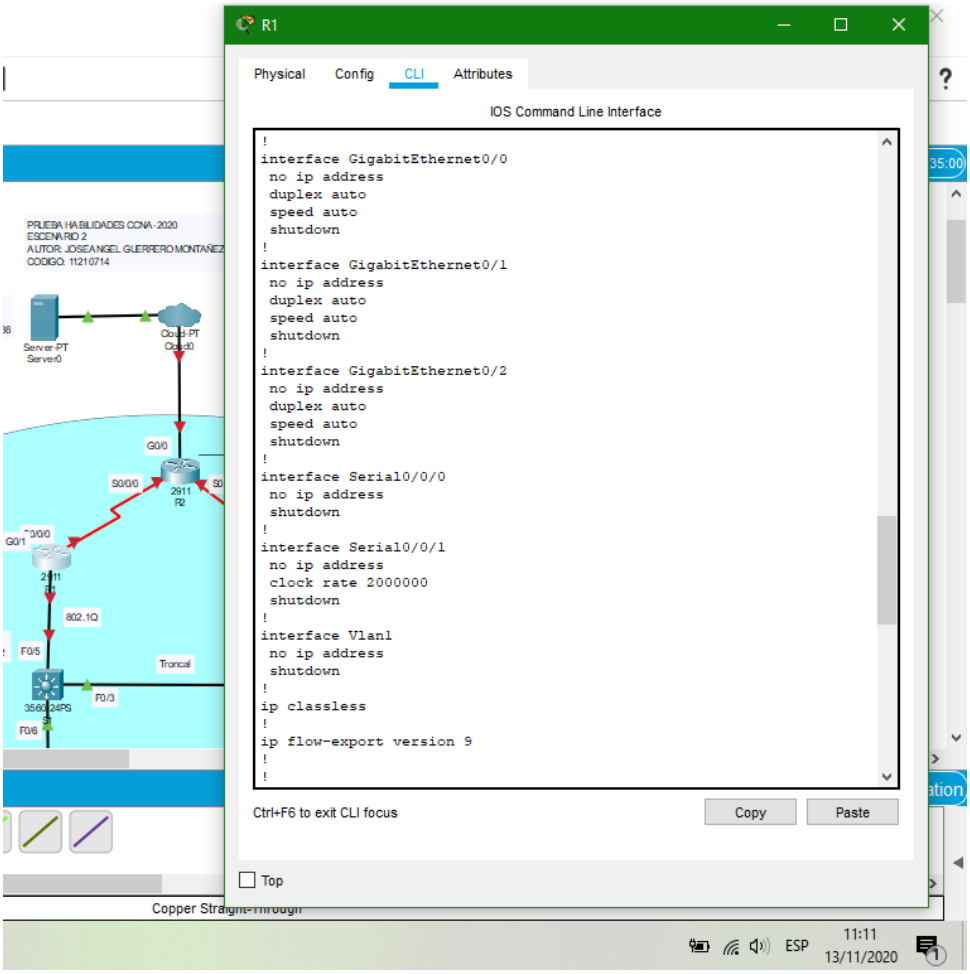
Figura 37. Verificar borrado de R1 (1)



Fuente: Autor

Se realiza la verificación del borrado de la configuración general de R1 siendo exitoso su borrado este procedimiento es el mismo en todos los router.

Figura 38. Verificar borrado de R1 (2)

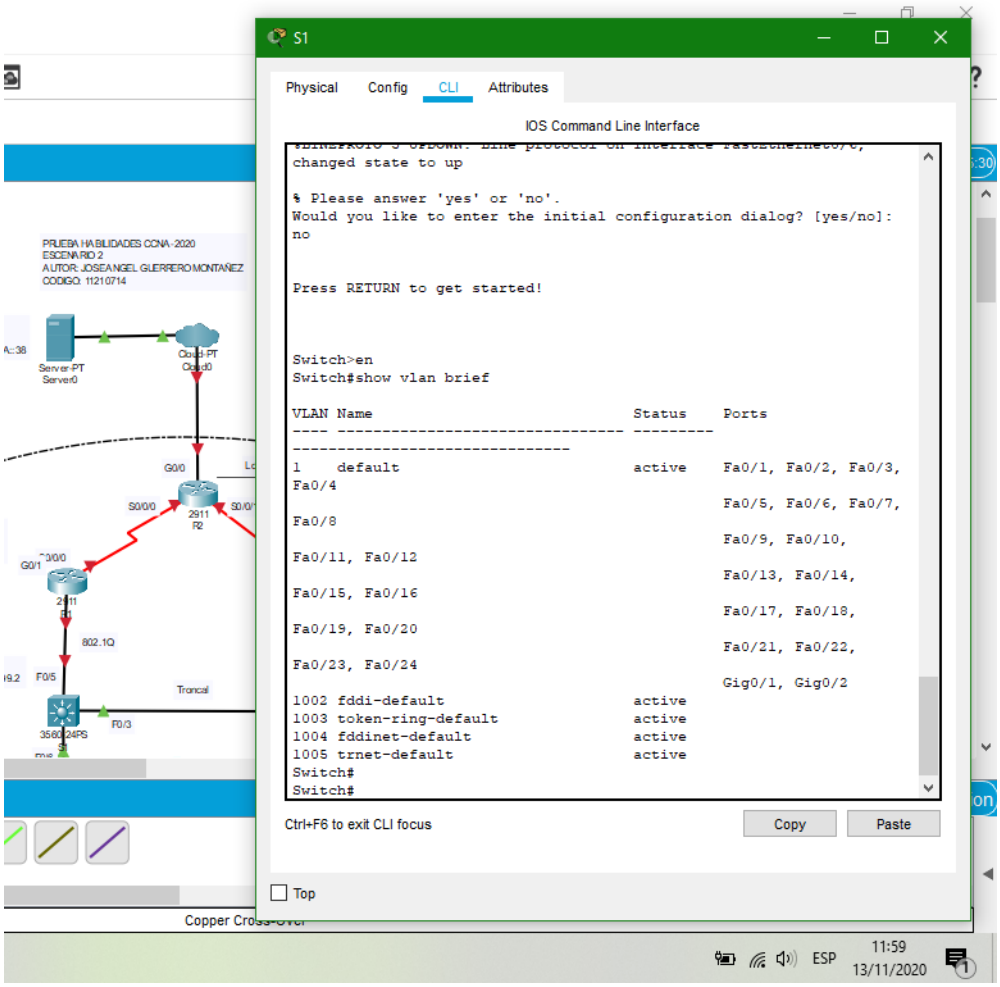


Fuente: Autor

Se realiza la verificación del borrado de la configuración general y direcciones IP de R1 siendo exitoso su borrado este procedimiento es el mismo en todos los router.

5.1.4 Verificación borrado configuraciones y base datos VLAN Switch

Figura 39. Verificar borrado base datos VLAN en la memoria flash de S1



Fuente: Autor

Se realiza la verificación del borrado de la base de datos de VLAN en la memoria flash de S1 siendo exitoso, este procedimiento es el mismo en todos los Switch.

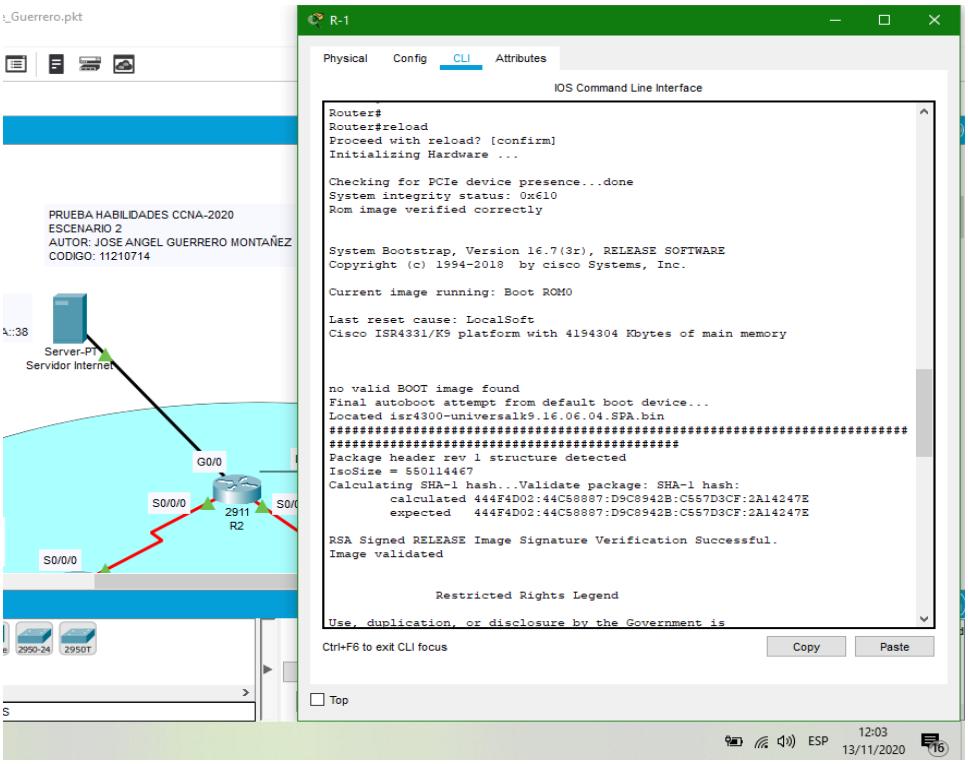
5.1.5 Reinicio de Router y Switches Escenario 2

Los siguientes son los comandos utilizados en el Router y los Switches para el procedimiento de reinicio de los equipos después de borrar sus configuraciones, el procedimiento es igual en todos los Switch y el router

Tabla 18. Reinicio de Router y Switches

Reinicio de Router y Switches Escenario 1	
Tarea	**Especificación**
Volver a cargar todos los routers	Se realiza la inserción de esta línea de comandos para recargar o reiniciar las configuraciones del router **Router#reload**
Volver a cargar ambos switch	Se realiza la inserción de esta línea de comandos para recargar o reiniciar las configuraciones del switch **Switch#reload**

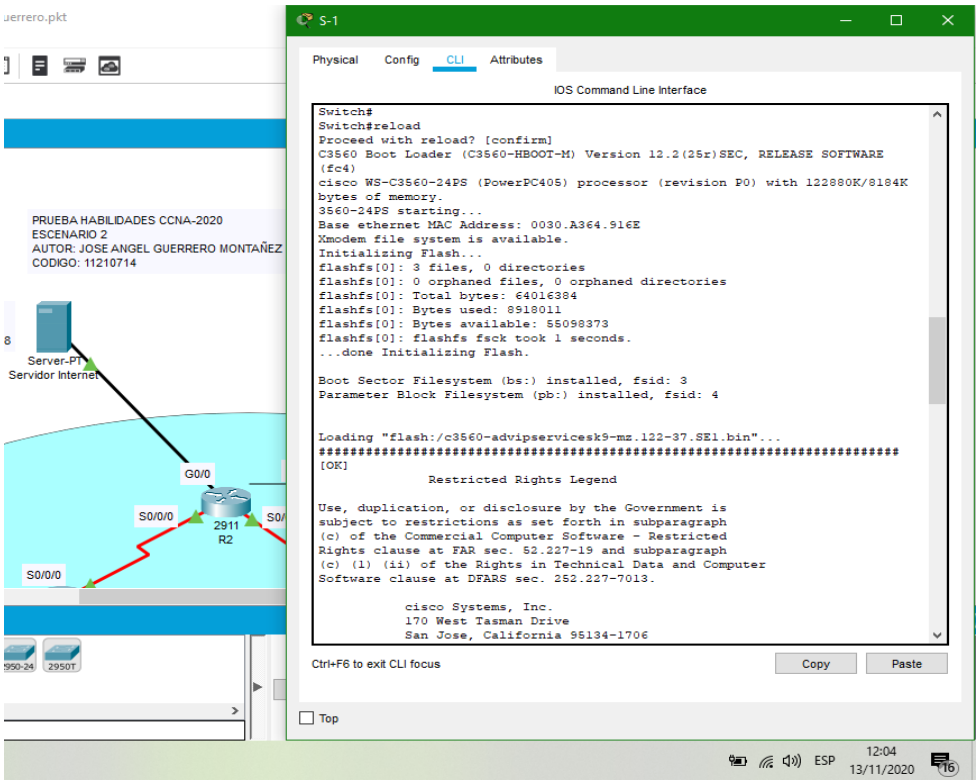
Figura 40. Reinicio de Router Escenario 2



Fuente: Autor

Se realiza la inserción del comando reload para recargar o reiniciar las configuraciones del router R1 siendo exitoso

Figura 41. Reinicio de Switches Escenario 2



Fuente: Autor

Se realiza la inserción del comando reload para recargar o reiniciar las configuraciones del Switch S1 siendo exitoso

6. Parte 2: Configurar los parámetros básicos de los dispositivos

Realizado el paso de borrar las diferentes configuraciones en cada Router y Switch y con el fin de garantizar que estos no posean datos en su memoria, posteriormente se realizara el procedimiento de configuración teniendo en cuenta cada uno de los aspectos y requerimientos solicitados en este escenario 2 para esto nos apoyaremos en la lista de direccionamiento IP sobre la topología de red a trabajar la cual se puede observar en la (Figura 23. Topología) mediante esta se realizarán las configuraciones empleando los siguientes equipos.

- 01 servidor (Server-PT)
- 01 nube (Cloud-PT)
- 01 Router 2911 para R1
- 01 Router 2911 para R2

- 01 Router 2911 para R3
- 01 Switch 3560 para S1
- 01 Switch 3560 para S2
- 01 PC para PC-A
- 01 PC para PC-B

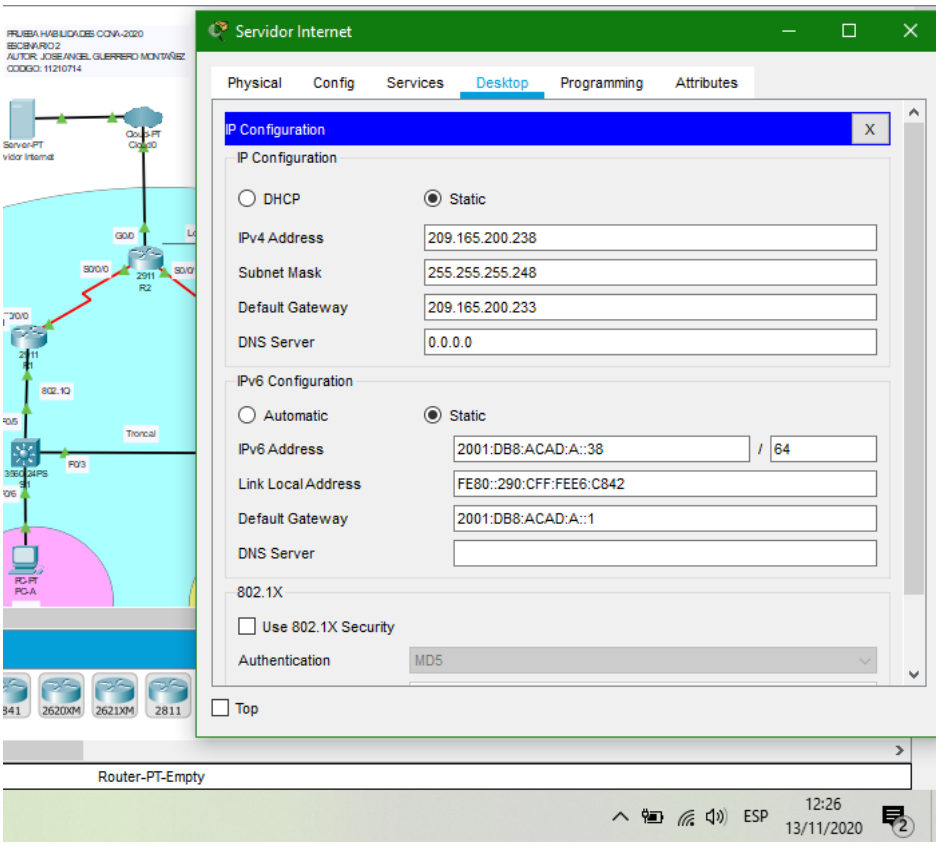
6.1. Paso 1: Configurar la computadora de Internet

Apoyado en la topología de la red se realizará la configuración del Servidor de internet utilizando cada uno de los parámetros básicos establecidos en este escenario como son direccionamiento IPv4, la máscara de subred para IPv4, la puerta de enlace predeterminada (gateway predeterminado), la dirección IPv6/subred, la puerta de enlace predeterminada IPv6 (gateway predeterminado IPv6), para esta tarea se realizará el uso de diferentes direcciones IP las cuales permitirán el correcto direccionamiento y las cuales están contenidas en la (Tabla 19. Direccionamiento Servidor de internet) por tal motivo con cada una las tareas de configuración de direcciones, mostradas en la Tabla 19, podemos asegurar que cada uno de los dispositivos de red queden configurados de forma correcta.

Tabla 19. Direccionamiento Servidor de internet

Servidor de internet configuración direccionamiento	
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

Figura 42. Configuración direccionamiento Servidor de internet



Fuente: Autor

Se realiza el procedimiento de Configuración del direccionamiento sobre el Servidor de internet utilizando las direcciones propuestas de acuerdo a la (Tabla 15. Direccionamiento Servidor de internet) siendo exitoso su configuración.

6.2. Paso 2: Configurar R1

Apoyado en la topología de la red se realizará la configuración del router R1 utilizando cada uno de los parámetros básicos establecidos en este escenario 2 como son desactivar la búsqueda DNS, generar un nombre para el router, establecer una contraseña, configurar el acceso a la consola, cifrar la contraseña de exec privilegiado, establecer la Contraseña de acceso Telnet, Cifrar las contraseñas de texto no cifrado, generar un mensaje MOTD que permita mostrar una alerta si la contraseña ingresada es diferente a la permitida, configuración de Interfaz S0/0/0, establecer una Ruta predeterminada y verificar configuraciones en los router.

Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 20. Configuración Router R1) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 20, podemos asegurar que el Rouer R1 quede configurado de la manera correcta

Tabla 20. Configuración Router R1

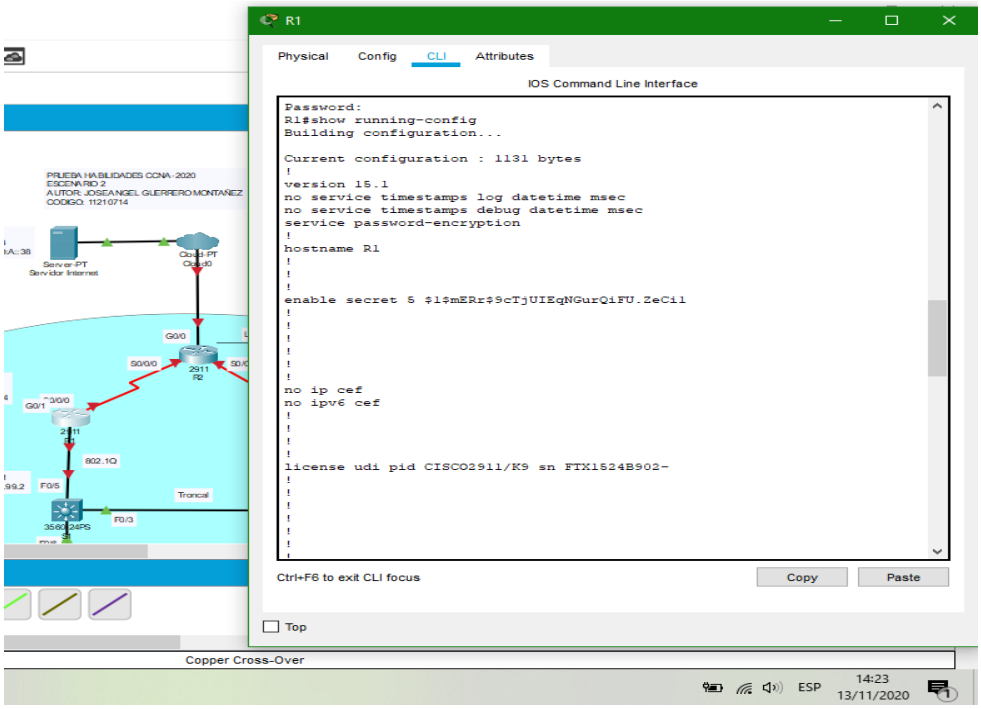
Configuración Router R1	
Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Se realiza la inserción de esta línea de comandos para desactivar la búsqueda DNS en el router 1 **Router>enable** **Router#config terminal** **Router# (config)#no ip domain-lookup**
Nombre del router	Se realiza la inserción de esta línea de comandos para asignar un nombre en el router 1 **Router# (config)#hostname R1**
Contraseña de exec privilegiado cifrada	Se realiza la inserción de estas líneas de comandos para asignar una Contraseña cifrada para el modo EXEC privilegiado en el router 1 **R1#config t** **R1(config)# enable secret class** **R1(config)#exit**
Contraseña de acceso a la consola	Se realiza la inserción de estas líneas de comandos para asignar una Contraseña de acceso a la consola en el router 1 **R1(config)#line console 0** **R1(config-line)#password cisco** **R1(config-line)#login** **R1(config-line)#exit**
Contraseña de acceso Telnet	Se realiza la inserción de estas líneas de comandos para Configurar el inicio de sesión en las líneas VTY para que use Contraseña de acceso Telnet en el router 1 **R1(config)#line vty 0 4** **R1(config-line)#password cisco** **R1(config-line)#login** **R1(config-line)#exit**

Cifrar las contraseñas de texto no cifrado	Se realiza la inserción de estas líneas de comandos para Cifrar las contraseñas de texto no cifrado en el router 1 **R1(config)#service password-encryption**
Mensaje MOTD	Se realiza la inserción de estas líneas de comandos para Configure un MOTD Banner en el router 2 **R1(config)#banner motd $Esta prohibido el acceso no autorizado$**
Interfaz S0/0/0	Se realiza la inserción de estas líneas de comandos para generar las diferentes configuraciones. Establezca la descripción **R1(config)#interface s0/0/0** **R1(config-if)# description Connection to R2** Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones **R1(config-if)#ip address 172.16.1.1 255.255.255.252** Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones **R1(config-if)#ipv6 address 2001:db8:acad:1::1/64** Establecer la frecuencia de reloj en 128000 **R1(config-if)#clock rate 128000** Activar la interfaz **R1(config-if)#no shutdown**
Ruta predeterminada	Configurar una ruta IPv4 predeterminada de S0/0/0 **R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0** Configurar una ruta IPv6 predeterminada de S0/0/0 **R1(config)#ipv6 route ::/0 s0/0/0**

Verificar que no hallan configuraciones en los router	Se realiza la inserción de esta línea de comandos para verificar que no hallan configuraciones en los router **R1>en** **R1#show running-config**

Nota: Todavía no configure G0/1.

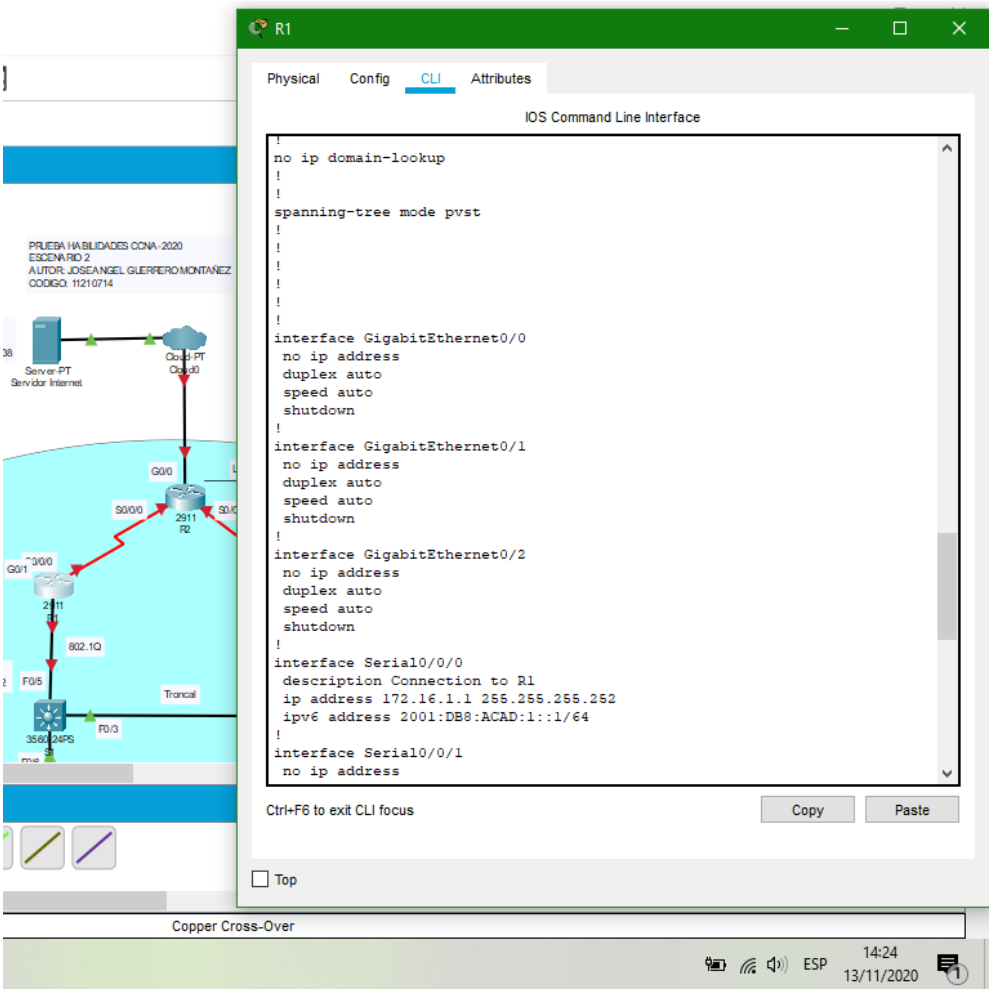
Figura 43. Configuración general Router 1



Fuente: Autor

Se realiza la verificación de la configuración general sobre creación o cambio de nombre el direccionamiento IPv4 e IPv6 así como creación de interfaces, así como los diferentes tipos de contraseñas que pueden asignarse en R1 siendo exitoso su creación este procedimiento es similar en todos los router..

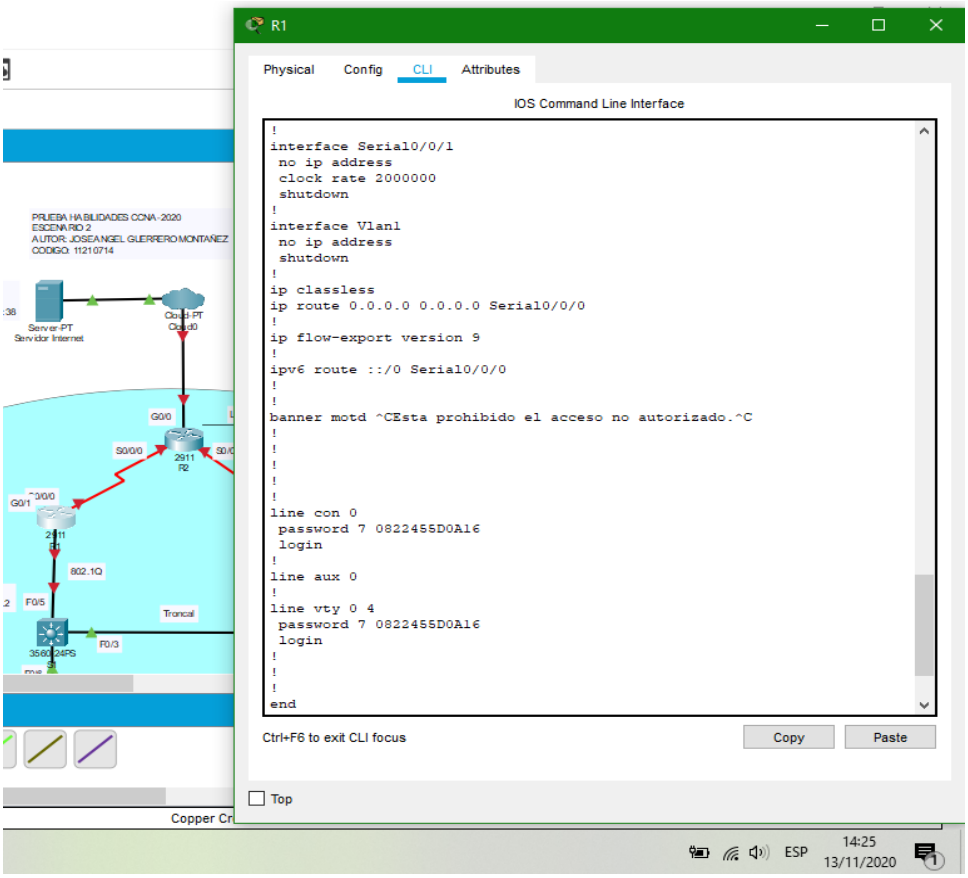
Figura 44. Configuración general Router 1 (1)



Fuente: Autor

Se realiza la verificación de la configuración general sobre creación o cambio de nombre el direccionamiento IPv4 e IPv6 así como creación de interfaces, así como los diferentes tipos de contraseñas que pueden asignarse de R2 siendo exitoso su creación este procedimiento es similar en todos los router.

Figura 45. Configuración general Router 1 (2)



Fuente: Autor

Se realiza la verificación de la configuración general sobre creación o cambio de nombre el direccionamiento IPv4 e IPv6 así como creación de interfaces, así como los diferentes tipos de contraseñas que pueden asignarse de R2 siendo exitoso su creación, este procedimiento es similar en todos los router aunque varían las direcciones que se asignaron.

6.3. Paso 3: Configurar R2

Apoyado en la topología de la red se realizará la configuración del router R2 utilizando cada uno de los parámetros básicos establecidos en este escenario 2 como son desactivar la búsqueda DNS, generar un nombre para el router, establecer una contraseña, configurar el acceso a la consola, cifrar la contraseña de exec privilegiado, establecer la Contraseña de acceso Telnet, Cifrar las contraseñas de texto no cifrado, realizar habilitación del servidor HTTP, generar un mensaje MOTD que permita mostrar una alerta si la contraseña ingresada es

diferente a la permitida, realizar configuración de Interfaz S0/0/0 y de Interfaz S0/0/1, así como Interfaz G0/0 (simulación de Internet) y la Interfaz loopback 0 (servidor web simulado), establecer una Ruta predeterminada y verificar configuraciones en los router.

Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 21. Configuración Router R2) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 21, podemos asegurar que el Router R2 quede configurado de la manera correcta.

Tabla 21. Configuración Router R2

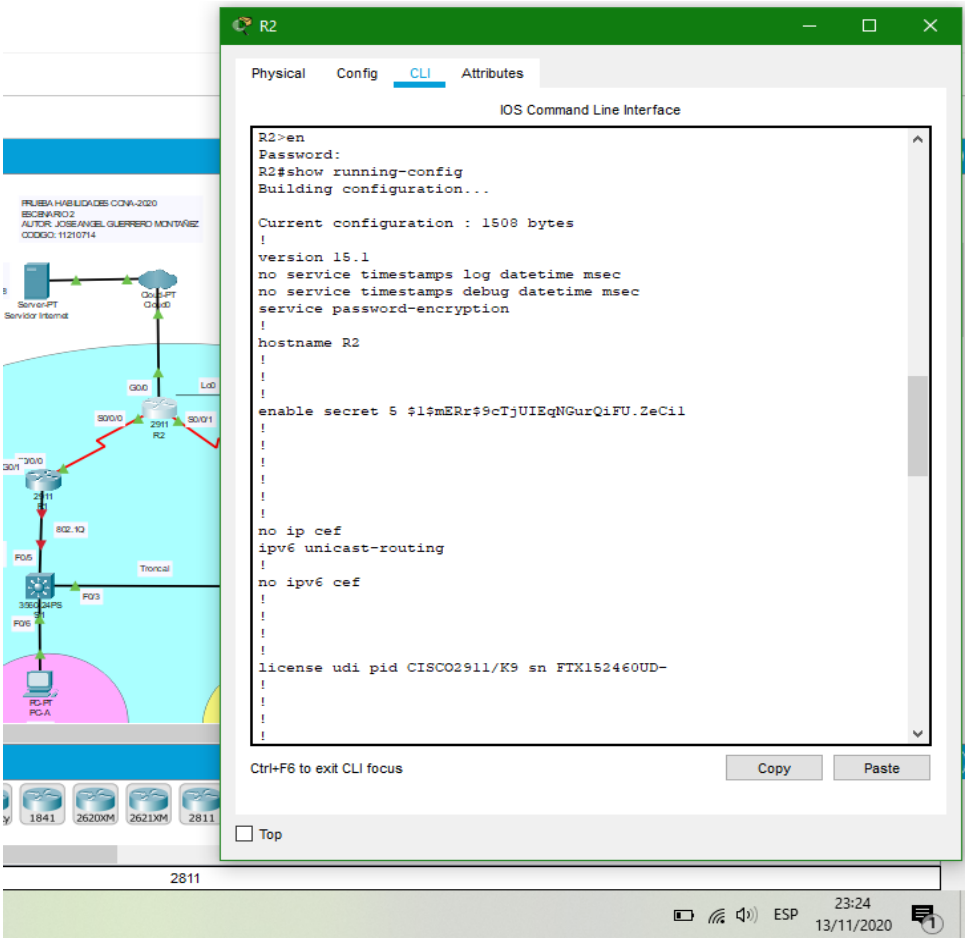
Configuración Router R2	
Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Se realiza la inserción de esta línea de comandos para desactivar la búsqueda DNS en el router 2 **Router>enable** **Router#config terminal** **Router# (config)#no ip domain-lookup**
Nombre del router	Se realiza la inserción de esta línea de comandos para asignar un nombre en el router 2 **Router# (config)#hostname R2**
Contraseña de exec privilegiado cifrada	Se realiza la inserción de estas líneas de comandos para asignar una Contraseña cifrada para el modo EXEC privilegiado en el router 2 **R2#config t** **R2(config)# enable secret class** **R2(config)#exit**
Contraseña de acceso a la consola	Se realiza la inserción de estas líneas de comandos para asignar una Contraseña de acceso a la consola en el router 2 **R2(config)#line console 0** **R2(config-line)#password cisco** **R2(config-line)#login** **R2(config-line)#exit**
Contraseña de acceso Telnet	cisco

	Se realiza la inserción de estas líneas de comandos para Configurar el inicio de sesión en las líneas VTY para que use Contraseña de acceso Telnet en el router 2 **R2(config)#line vty 0 4** **R2(config-line)#password cisco** **R2(config-line)#login** **R2(config-line)#exit**
Cifrar las contraseñas de texto no cifrado	Se realiza la inserción de estas líneas de comandos para Cifrar las contraseñas de texto no cifrado en el router 2 **R2(config)#service password-encryption**
Habilitar el servidor HTTP	Se realiza la inserción de estas líneas de comandos para Habilitar el servidor HTTP en el router 2 **R2(config)#Ip nat inside source static 10.10.10.10 209.165.200.229**
Mensaje MOTD	Se realiza la inserción de estas líneas de comandos para Configure un MOTD Banner en el router 2 **R2(config)#banner motd $Esta prohibido el acceso no autorizado$**
Interfaz S0/0/0	Se realiza la inserción de estas líneas de comandos para generar las diferentes configuraciones. Establezca la descripción **R2(config)#interface s0/0/0** **R2(config-if)# description Connection to R1** Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones **R2(config-if)# ip address 172.16.1.2 255.255.255.252** Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones **R2(config-if)#ipv6 address 2001:db8:acad:1::2/64**

	Activar la interfaz **R2(config-if)#no shutdown**
Interfaz S0/0/1	Se realiza la inserción de estas líneas de comandos para generar las diferentes configuraciones. Establecer la descripción **R2(config)#interface s0/0/1** **R2(config-if)# description Connection to R3** Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. **R2(config-if)# ip address 172.16.2.2 255.255.255.252** Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. **R2(config-if)# ipv6 address 2001:db8:acad:2::2/64** Establecer la frecuencia de reloj en 128000 **R2(config-if)#clock rate 128000** Activar la interfaz **R2(config-if)#no shutdown**
Interfaz G0/0 (simulación de Internet)	Se realiza la inserción de estas líneas de comandos para generar las diferentes configuraciones. Establecer la descripción. **R2(config)#interface G0/0** **R2(config-if)# description Salida Internet R2** Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. **R2(config-if)# ip address 209.165.200.233 255.255.255.248**

	Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. **R2(config-if)# ipv6 address 2001:db8:acad:A::1/64** Activar la interfaz **R2(config-if)#no shutdown**
Interfaz loopback 0 (servidor web simulado)	Se realiza la inserción de estas líneas de comandos para generar las diferentes configuraciones de Interfaz loopback 0 (servidor web simulado). Establecer la descripción. **R2(config-if)#int loopback 0** **R2(config-if)#description servidor web simulado** **R2(config-if)#exit** Establezca la dirección IPv4. **R2(config-if)#ip address 10.10.10.10 255.255.255.255** **R2(config-if)#exit**
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. **R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0** Configure una ruta IPv6 predeterminada de G0/0. **R2(config)#ipv6 route ::/0 g0/0** **R2(config)#**
Verificar configuraciones en los router	Se realiza la inserción de esta línea de comandos para verificar configuraciones en los router **R2>en** **R2#show running-config**

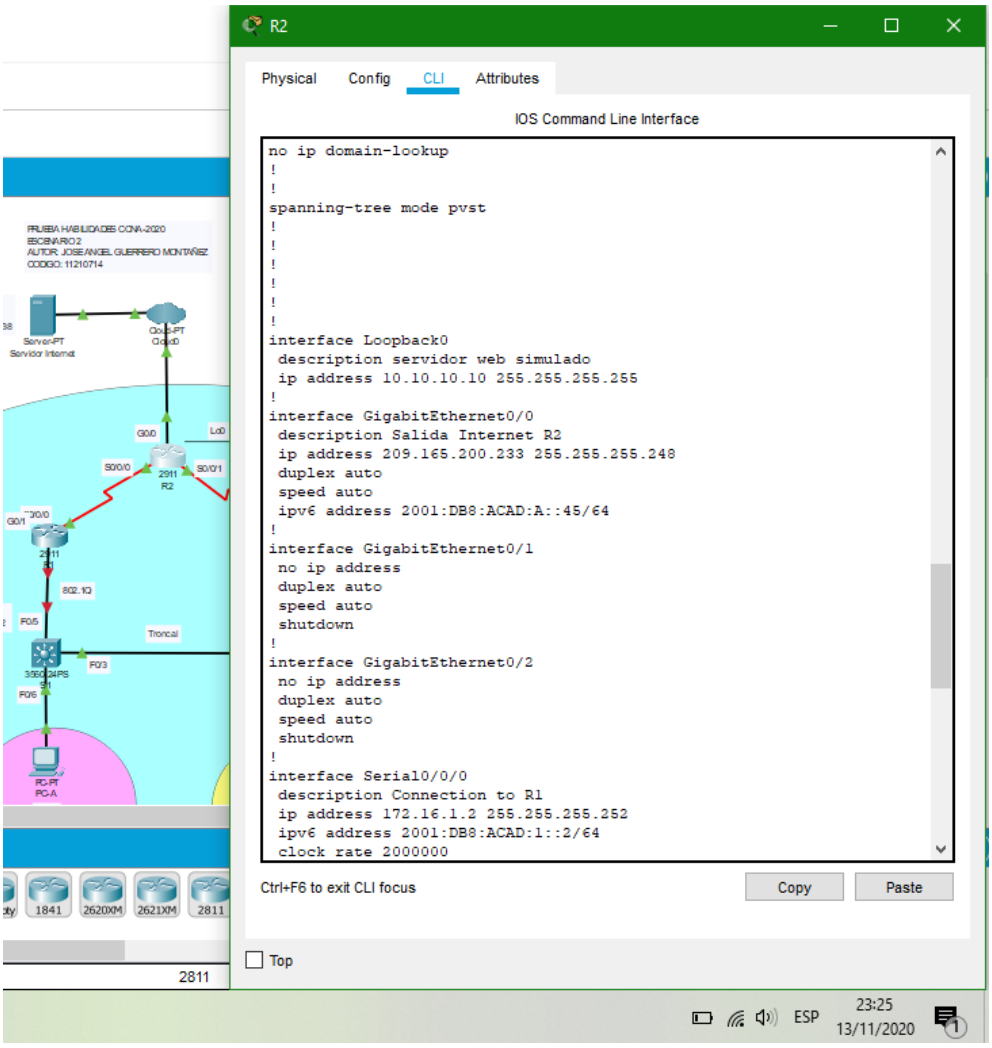
Figura 46. Configuración general Router 2



Fuente: Autor

Se realiza la verificación de la configuración general sobre creación o cambio de nombre el direccionamiento IPv4 e IPv6 así como creación de interfaces, así como los diferentes tipos de contraseñas que pueden asignarse de R2 siendo exitoso su creación, este procedimiento es similar en todos los router.

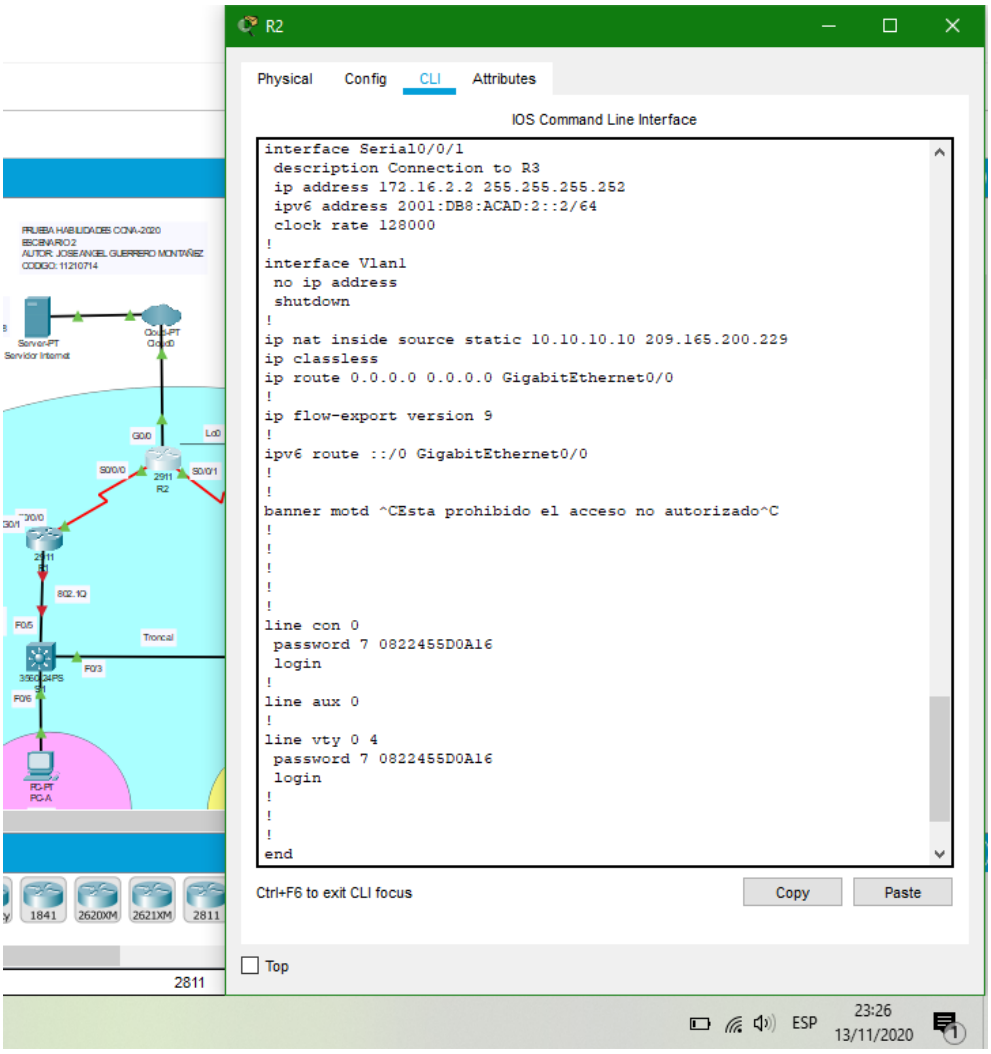
Figura 47. Configuración general Router 2 (1)



Fuente: Autor

Se realiza la verificación de la configuración general sobre creación o cambio de nombre el direccionamiento IPv4 e IPv6 así como creación de interfaces, así como los diferentes tipos de contraseñas que pueden asignarse de R2 siendo exitoso su creación, este procedimiento es similar en todos los router aunque varían las direcciones e interface que se asignaron.

Figura 48. Configuración general Router 2 (2)



Fuente: Autor

Se realiza la verificación de la configuración general sobre creación o cambio de nombre el direccionamiento IPv4 e IPv6 así como creación de interfaces, así como los diferentes tipos de contraseñas que pueden asignarse de R2 siendo exitoso su creación, este procedimiento es similar en todos los router aunque varían las direcciones e interface que se asignaron.

6.4. Paso 4: Configurar R3

Apoyado en la topología de la red se realizará la configuración del router R3 utilizando cada uno de los parámetros básicos establecidos en este escenario 2 como son desactivar la búsqueda DNS, generar un nombre para el router, establecer una contraseña, configurar el acceso a la consola, cifrar la contraseña de exec privilegiado, establecer la Contraseña de acceso Telnet, Cifrar las contraseñas de texto no cifrado, generar un mensaje MOTD que permita mostrar una alerta si la contraseña ingresada es diferente a la permitida.

Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 22. Configuración Router R3) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 22, podemos asegurar que el Router R3 quede configurado de la manera correcta.

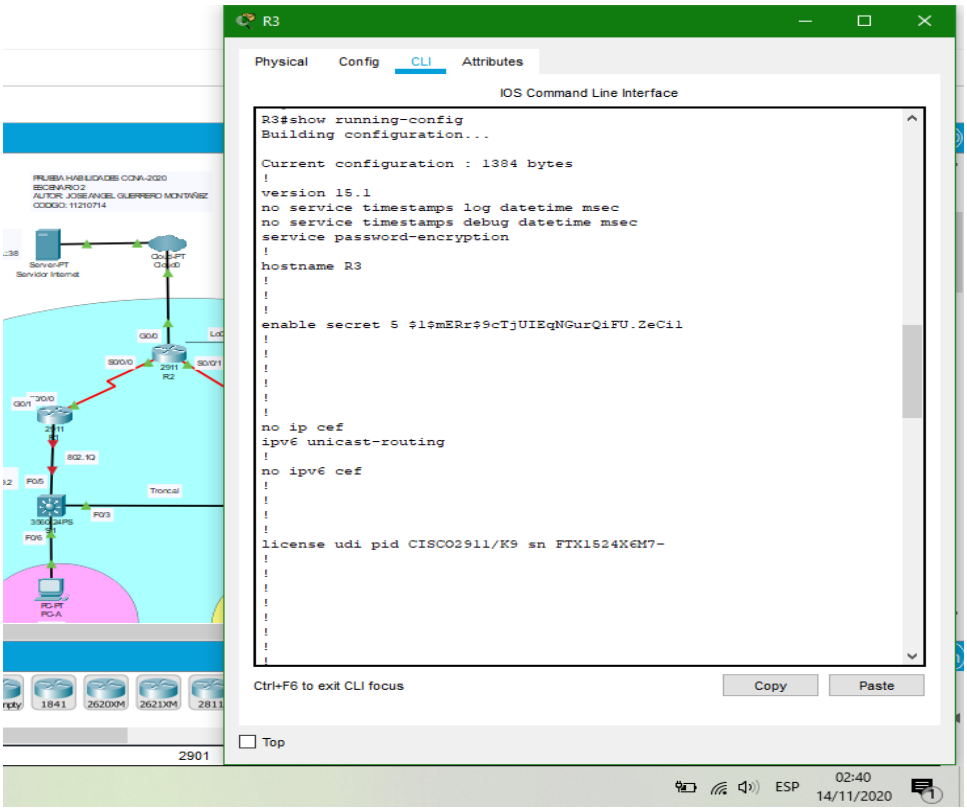
Tabla 22. Configuración Router R3

Configuración Router R3	
Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Se realiza la inserción de esta línea de comandos para desactivar la búsqueda DNS en el router 3 **Router>enable** **Router#config terminal** **Router# (config)#no ip domain-lookup**
Nombre del router	Se realiza la inserción de esta línea de comandos para asignar un nombre en el router 3 **Router# (config)#hostname R3**
Contraseña de exec privilegiado cifrada	Se realiza la inserción de estas líneas de comandos para asignar una Contraseña cifrada para el modo EXEC privilegiado en el router 3 **R3#config t** **R3(config)# enable secret class** **R3(config)#exit**
Contraseña de acceso a la consola	Se realiza la inserción de estas líneas de comandos para asignar una Contraseña de acceso a la consola en el router 3

	R3(config)#line console 0 **R3(config-line)#password cisco** **R3(config-line)#login** **R3(config-line)#exit**
Contraseña de acceso Telnet	Se realiza la inserción de estas líneas de comandos para Configurar el inicio de sesión en las líneas VTY para que se use Contraseña de acceso Telnet en el router 3 **R3(config)#line vty 0 4** **R3(config-line)#password cisco** **R3(config-line)#login** **R3(config-line)#exit**
Cifrar las contraseñas de texto no cifrado	Se realiza la inserción de estas líneas de comandos para Cifrar las contraseñas de texto no cifrado en el router 3 **R3(config)#service password-encryption**
Mensaje MOTD	Se realiza la inserción de estas líneas de comandos para Configure un MOTD Banner en el router 3 **R3(config)#banner motd $Esta prohibido el acceso no autorizado$**
Interfaz S0/0/1	Se realiza la inserción de estas líneas de comandos para generar las diferentes configuraciones. **R3(config)#ipv6 unicast-routing** Establecer la descripción **R3(config)#interface s0/0/1** **R3(config-if)# description Connection R3 to R2** Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. **R3(config-if)# ip address 172.16.2.1 255.255.255.252** Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz

	R3(config-if)# ipv6 address 2001:db8:acad:2::1/64 Activar la interfaz **R3(config-if)#no shutdown**
Interfaz loopback 4	Se realiza la inserción de estas líneas de comandos para Interfaz loopback 4 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. **R3(config-if)# int loopback 4** **R3(config-if)#ip address 192.168.4.1 255.255.255.0**
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. **R3(config-if)# int loopback 5** **R3(config-if)#ip address 192.168.5.1 255.255.255.0**
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. **R3(config-if)# int loopback 6** **R3(config-if)#ip address 192.168.6.1 255.255.255.0**
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. **R3(config-if)# int loopback 7** **R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64**
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/1 **R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1** Configurar una ruta IPv6 predeterminada de S0/0/1 **R3(config)#ipv6 route ::/0 s0/0/1**
Verificar configuraciones en los router	Se realiza la inserción de esta línea de comandos para verificar configuraciones en los router **R3>en** **R3#show running-config**

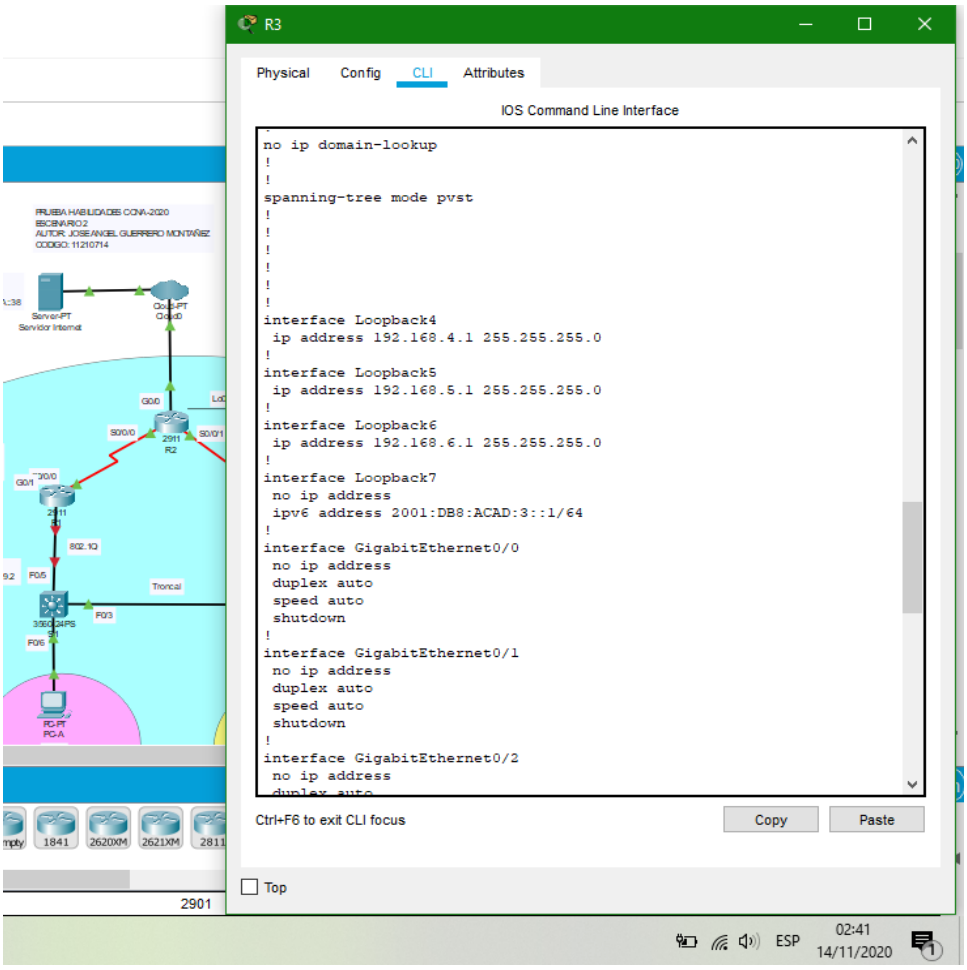
Figura 49. Configuración general Router 3



Fuente: Autor

Se realiza la verificación de la configuración general sobre creación o cambio de nombre el direccionamiento IPv4 e IPv6 así como creación de interfaces, así como los diferentes tipos de contraseñas que pueden asignarse de R2 siendo exitoso su creación, este procedimiento es similar en todos los router.

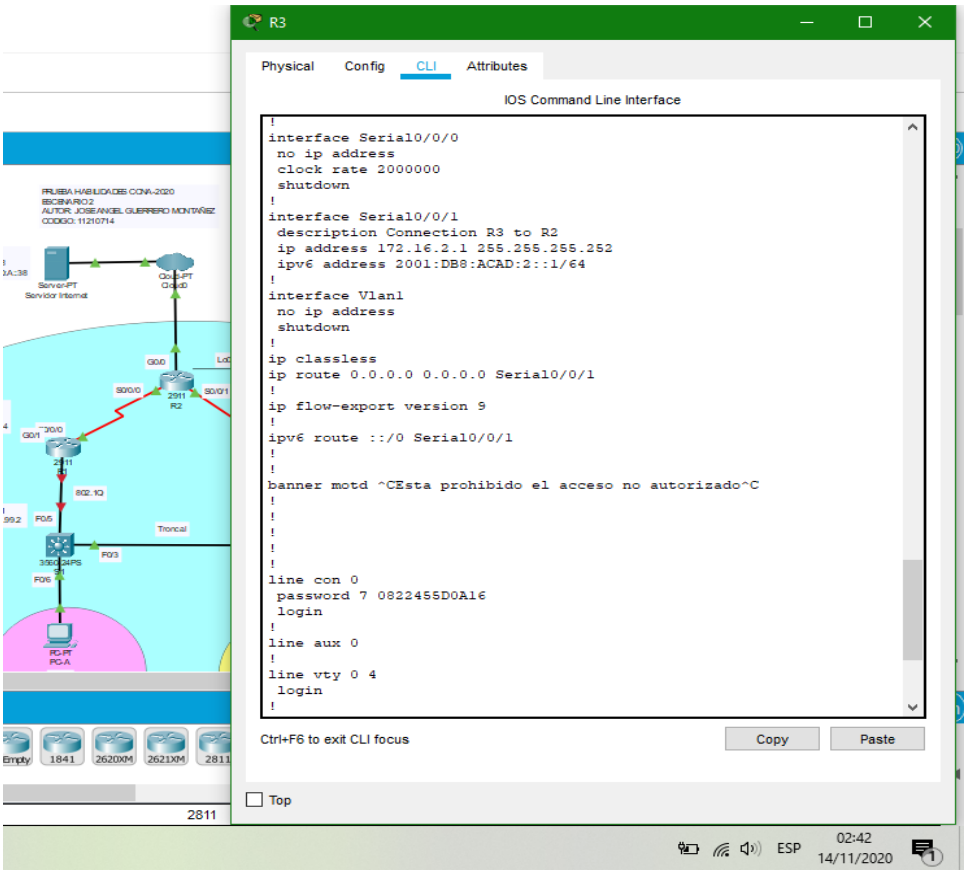
Figura 50. Configuración general Router 2 (1)



Fuente: Autor

Se realiza la verificación de la configuración general sobre creación o cambio de nombre el direccionamiento IPv4 e IPv6 así como creación de interfaces, así como los diferentes tipos de contraseñas que pueden asignarse de R2 siendo exitoso su creación, este procedimiento es similar en todos los router aunque varían las direcciones e interface que se asignaron.

Figura 51. Configuración general Router 2 (2)



Fuente: Autor

Se realiza la verificación de la configuración general sobre creación o cambio de nombre el direccionamiento IPv4 e IPv6 así como creación de interfaces, así como los diferentes tipos de contraseñas que pueden asignarse de R2 siendo exitoso su creación, este procedimiento es similar en todos los router aunque varían las direcciones e interface que se asignaron.

6.5. Paso 5: Configurar S1

Apoyado en la topología de la red se realizará la configuración del Switch 1 utilizando cada uno de los parámetros básicos establecidos en este escenario 2 como son desactivar la búsqueda DNS, generar un nombre para el Switch, establecer una contraseña, configurar el acceso a la consola, cifrar la contraseña de exec privilegiado, establecer la Contraseña de acceso Telnet, Cifrar las contraseñas de texto no cifrado, generar un mensaje MOTD que permita mostrar una alerta si la contraseña ingresada es diferente a la permitida.

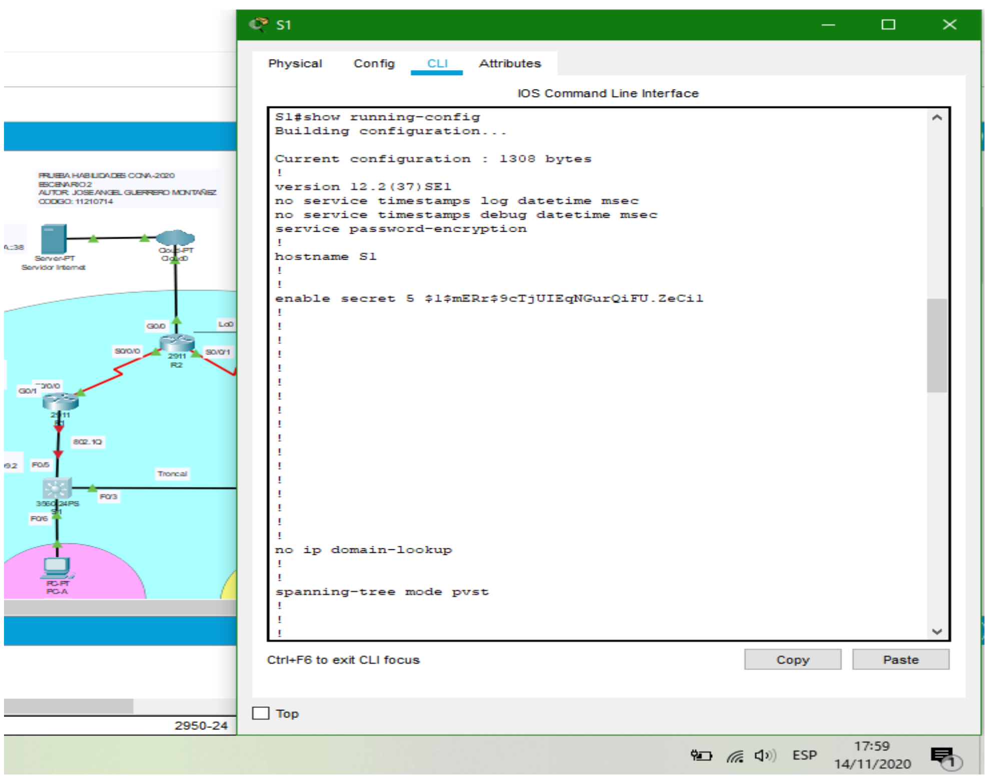
Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 23. Configuración Switch S1) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 23, podemos asegurar que el Switch S1 quede configurado de la manera correcta.

Tabla 23. Configuración Switch S1

Configuración Switch S1	
Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Se realiza la inserción de esta línea de comandos para desactivar la búsqueda DNS en el Switch 1 **Switch>enable** **Switch#config terminal** **Switch# (config)#no ip domain-lookup**
Nombre del switch	**S1 o S2, según proceda** Se realiza la inserción de estas líneas de comandos para asignar Nombre del Switch 1 **Switch(config)#hostname S1**
Contraseña de exec privilegiado cifrada	Se realiza la inserción de estas líneas de comandos para asignar una Contraseña cifrada para el modo EXEC privilegiado en el Switch 1 **S1#config t** **S1(config)# enable secret class** **S1(config)#exit**
Contraseña de acceso a la consola	Se realiza la inserción de estas líneas de comandos para asignar una Contraseña de acceso a la consola en el Switch 1 **S1(config)#line console 0** **S1(config-line)#password cisco** **S1(config-line)#login** **S1(config-line)#exit**
Contraseña de acceso Telnet	Se realiza la inserción de estas líneas de comandos para que use Contraseña de acceso Telnet en el Switch 1 **S1(config)#line vty 0 4** **S1(config-line)#password cisco** **S1(config-line)#login**

	S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	Se realiza la inserción de estas líneas de comandos para Cifrar las contraseñas de texto no cifrado en el Switch 1 **S1(config)#service password-encryption**
Mensaje MOTD	Se realiza la inserción de estas líneas de comandos para Configure un MOTD Banner en el Switch 1 **S1(config)#banner motd $Esta prohibido el acceso no autorizado$**
Guardar configuración del Switch	Se realiza la inserción de estas líneas de comandos para Guardar configuración del Switch **S1#copy running-config startup-config**
Verificar configuraciones en los Switch	Se realiza la inserción de esta línea de comandos para verificar configuraciones en los Switch **S1>en** **S1#show running-config**

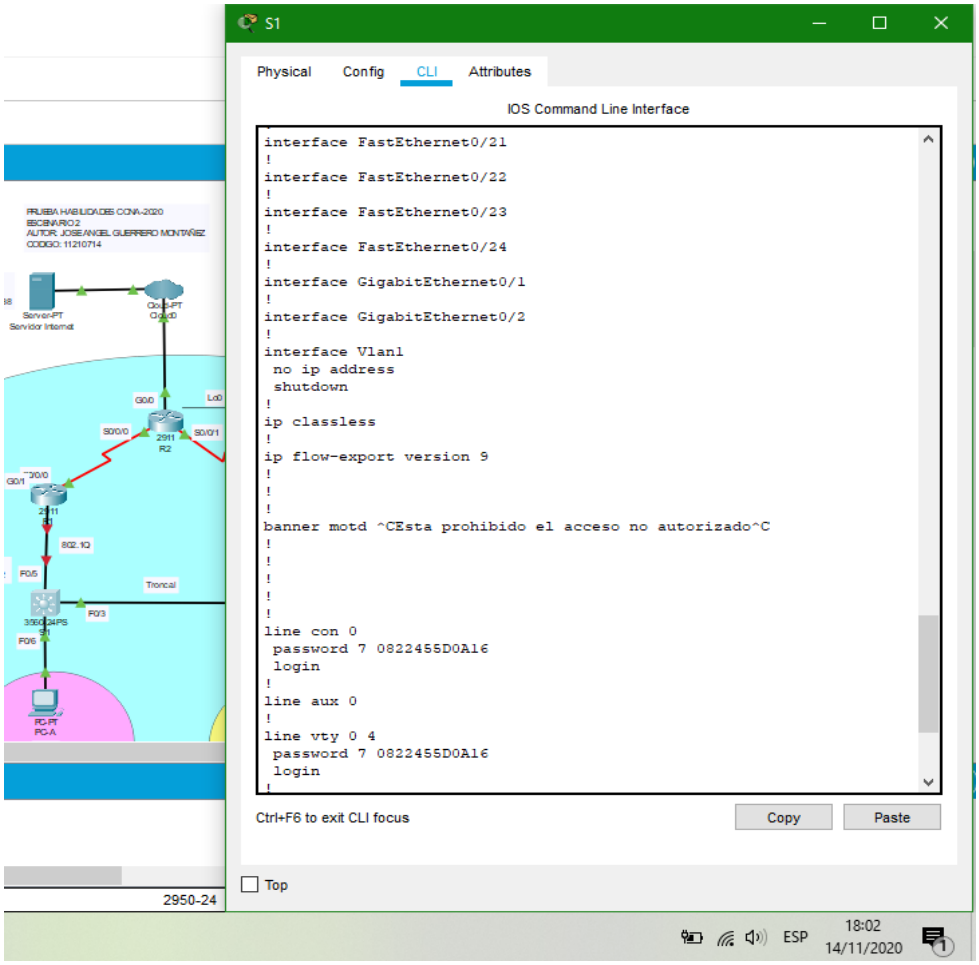
Figura 52. Configuración general Switch S1



Fuente: Autor

Se realiza la verificación de la configuración general sobre Desactivación la búsqueda DNS creación o cambio de nombre, así como los diferentes tipos de contraseñas que pueden asignarse en S1 siendo exitosa su creación este procedimiento es similar en todos los Switch

Figura 53. Configuración general Switch S1 (2)



Fuente: Autor

Se realiza la verificación de la configuración general sobre Desactivación la búsqueda DNS creación o cambio de nombre, así como los diferentes tipos de contraseñas que pueden asignarse en S1, creación de Mensaje MOTD y guardado de la configuración del Switch siendo exitosa su creación y guardado este procedimiento es similar en todos los Switch

6.6. Paso 6: Configurar el S3

Apoyado en la topología de la red se realizará la configuración del Switch 3 utilizando cada uno de los parámetros básicos establecidos en este escenario 2 como son desactivar la búsqueda DNS, generar un nombre para el Switch, establecer una contraseña, configurar el acceso a la consola, cifrar la contraseña de exec privilegiado, establecer la Contraseña de acceso Telnet, Cifrar las contraseñas de texto no cifrado, generar un mensaje MOTD que permita mostrar una alerta si la contraseña ingresada es diferente a la permitida.

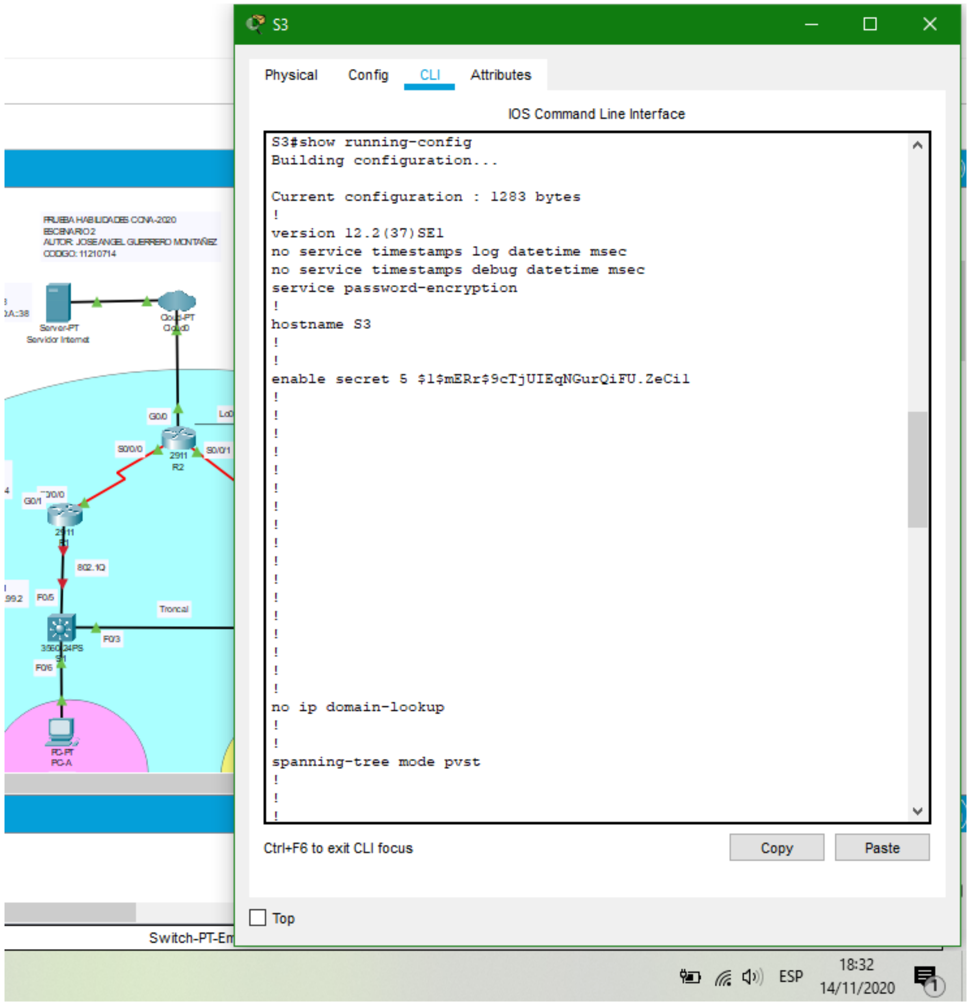
Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 24. Configuración Switch S3) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 24, podemos asegurar que el Switch S3 quede configurado de la manera correcta.

Tabla 24. Configuración Switch S3

Configuración Switch S3	
Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Se realiza la inserción de esta línea de comandos para desactivar la búsqueda DNS en el Switch 3 **Switch>enable** **Switch#config terminal** **Switch# (config)#no ip domain-lookup**
Nombre del switch	**S1 o S3, según proceda** Se realiza la inserción de estas líneas de comandos para asignar Nombre del Switch 3 **Switch(config)#hostname S3**
Contraseña de exec privilegiado cifrada	Se realiza la inserción de estas líneas de comandos para asignar una Contraseña cifrada para el modo EXEC privilegiado en el Switch 3 **S3#config t** **S3(config)# enable secret class** **S3(config)#exit**

Contraseña de acceso a la consola	Se realiza la inserción de estas líneas de comandos para asignar una Contraseña de acceso a la consola en el Switch 3 **S3(config)#line console 0** **S3(config-line)#password cisco** **S3(config-line)#login** **S3(config-line)#exit**
Contraseña de acceso Telnet	Se realiza la inserción de estas líneas de comandos para que use Contraseña de acceso Telnet en el Switch 3 **S3(config)#line vty 0 4** **S3(config-line)#password cisco** **S3(config-line)#login** **S3(config-line)#exit**
Cifrar las contraseñas de texto no cifrado	Se realiza la inserción de estas líneas de comandos para Cifrar las contraseñas de texto no cifrado en el Switch 3 **S3(config)#service password-encryption**
Mensaje MOTD	Se realiza la inserción de estas líneas de comandos para Configure un MOTD Banner en el Switch 3 **S3(config)#banner motd $Esta prohibido el acceso no autorizado$**
Guardar configuración del Switch	Se realiza la inserción de estas líneas de comandos para Guardar configuración del Switch 3 **S3#copy running-config startup-config**
Verificar configuraciones en los Switch	Se realiza la inserción de esta línea de comandos para verificar configuraciones en los Switch **S1>en** **S1#show running-config**

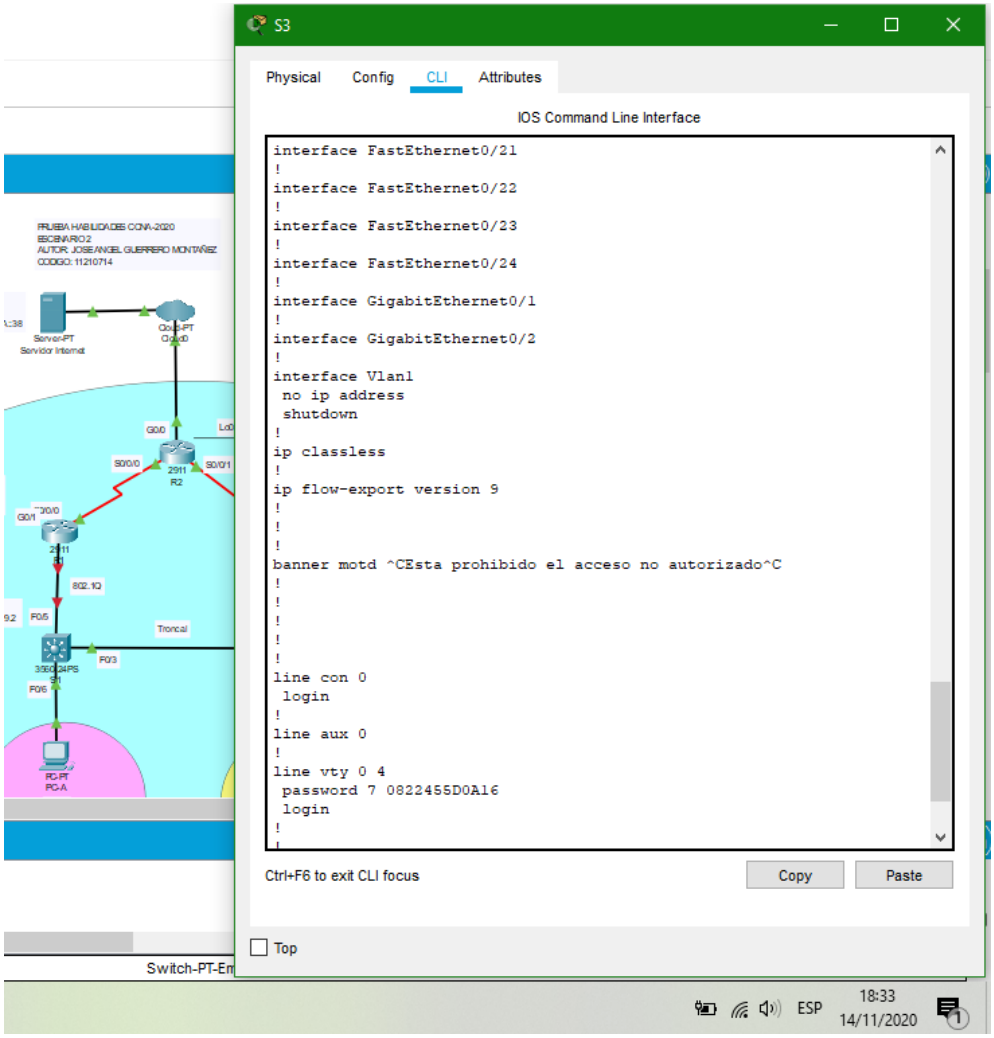
Figura 54. Configuración general Switch S3



Fuente: Autor

Se realiza la verificación de la configuración general sobre Desactivación la búsqueda DNS creación o cambio de nombre, así como los diferentes tipos de contraseñas que pueden asignarse en S3 siendo exitosa su creación este procedimiento es similar en todos los Switch

Figura 55. Configuración general Switch S3 (2)



Fuente: Autor

Se realiza la verificación de la configuración general sobre Desactivación la búsqueda DNS creación o cambio de nombre, así como los diferentes tipos de contraseñas que pueden asignarse en S3, creación de Mensaje MOTD y guardado de la configuración del Switch siendo exitosa su creación y guardado este procedimiento es similar en todos los Switch

6.7. Paso 7: Verificar la conectividad de la red

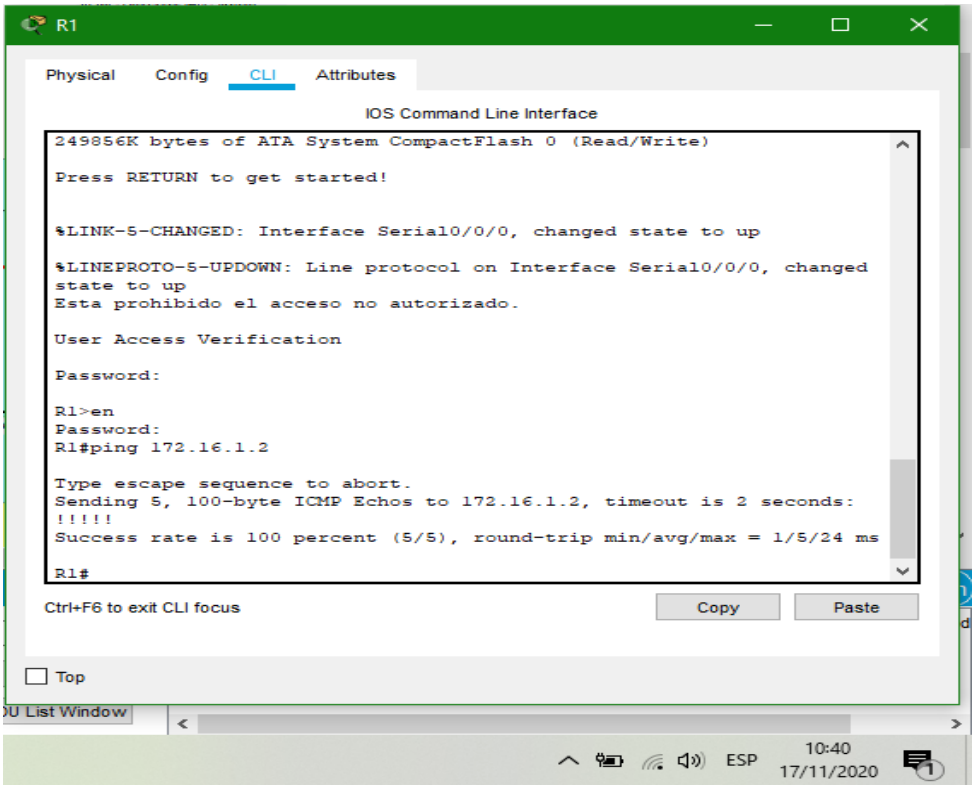
Para realizar la prueba de pines entre dispositivos se utilizarán las direcciones establecidas en las siguientes tablas (Tabla 21. Verificación de pines entre equipos de escenario 2)

Tabla 25. Verificación de pines entre equipos de escenario 2

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	El ping IPv4 Si fue realizado con éxito
R2	R3, S0/0/1	172.16.2.1	El ping IPv4 Si fue realizado con éxito
PC de Internet	Gateway predeterminado	209.165.200.233	El ping IPv4 Si fue realizado con éxito

Para realizar cada ping entre dispositivo se debe tener en cuenta el tipo de dirección a la cual se quiere hacer el procedimiento identificando si estas es IPv4 o IPv6 puesto que la estructura de dirección tiene diferente sintaxis.

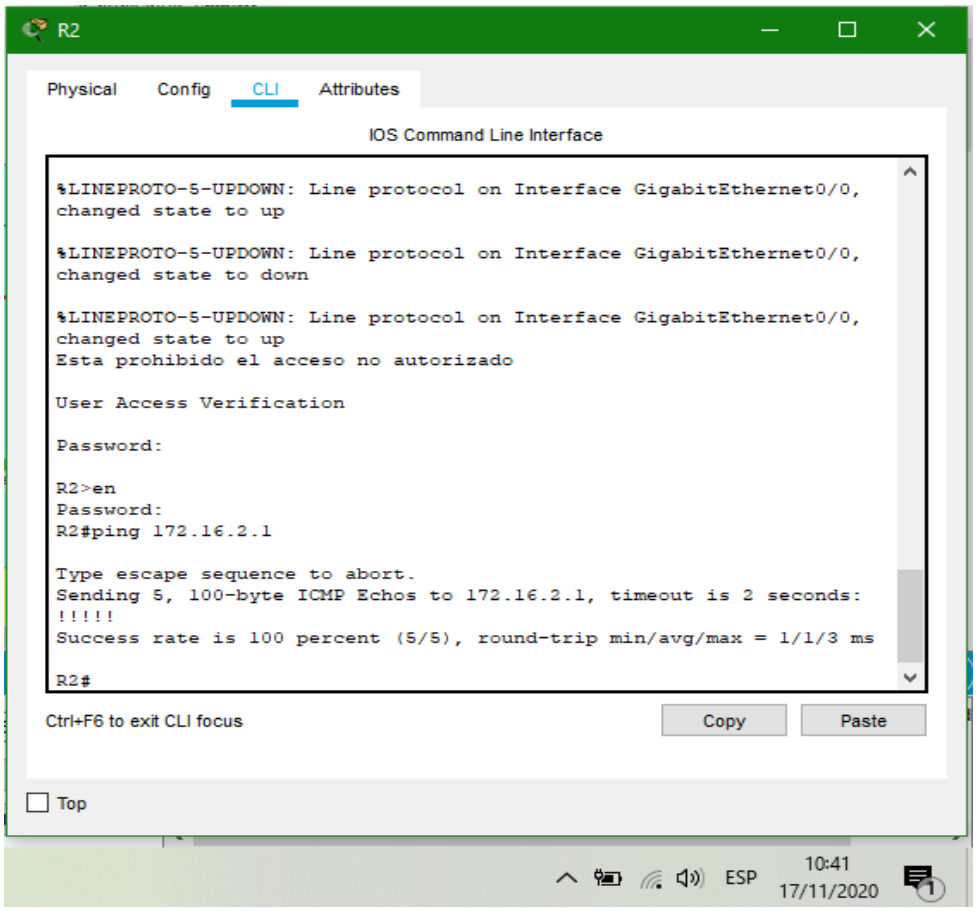
Figura 56. Pin desde el router R1 hacia R2, S0/0/0 IP 172.16.1.2



Fuente: Autor

Se realiza pin desde la **R1** hacia **R2, S0/0/0** enviando los paquetes a su dirección **IPv4** utilizando el comando **ping 172.16.1.2** logrando realizar el pin con éxito.

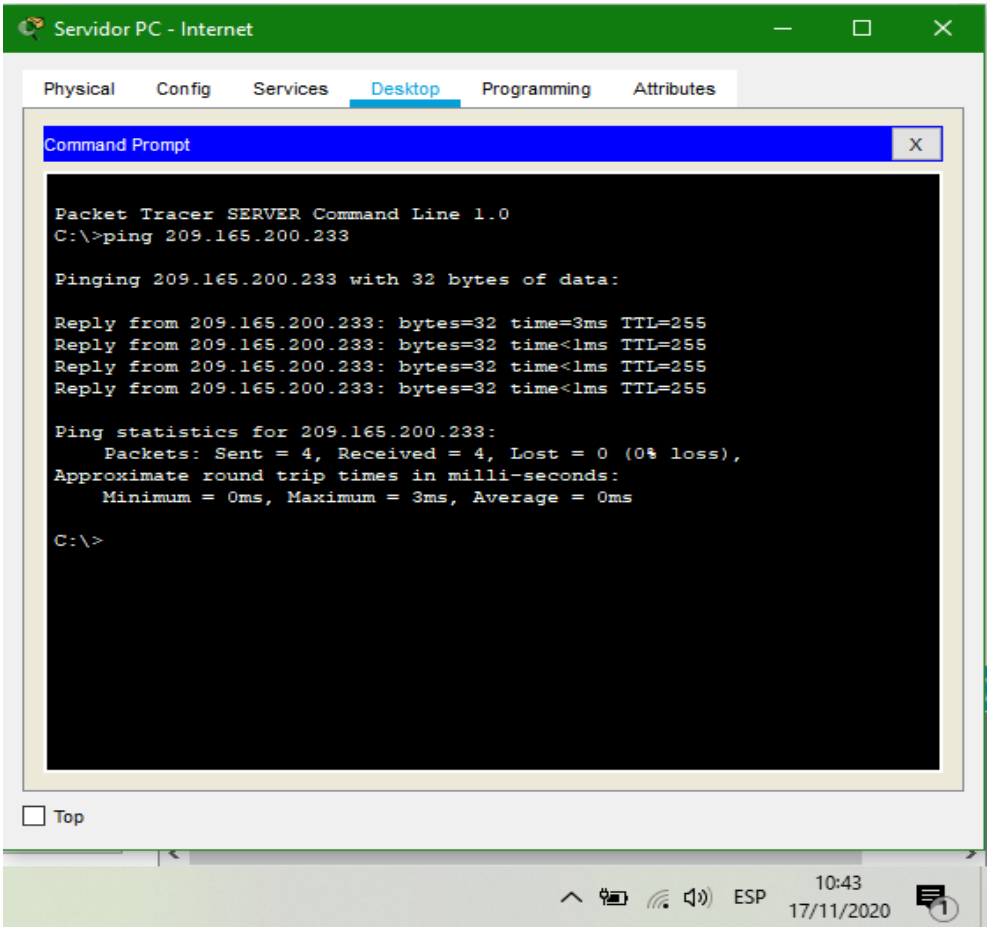
Figura 57. Pin desde el router R2 hacia R3, S0/0/1 IP 172.16.2.1



Fuente: Autor

Se realiza pin desde la **R2** hacia **R3, S0/0/1** enviando los paquetes a su dirección **IPv4** utilizando el comando **ping 172.16.2.1** logrando realizar el pin con éxito.

Figura 58. Pin desde PC de Internet R2 hacia Gateway predeterminado



Fuente: Autor

Se realiza pin desde la **PC de Internet** hacia **Gateway predeterminado** enviando los paquetes a su dirección **IPv4** utilizando el comando **ping 209.165.200.233** logrando realizar el pin con éxito.

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

7.1. Paso 1: Configurar S1

Apoyado en la topología de la red se realizará la configuración sobre la seguridad del switch, las VLAN y el routing entre VLAN del Switch S1 utilizando cada uno de los parámetros básicos establecidos en este escenario 2 como son creación de la base de datos de VLAN, realizar la asignación de su dirección IP de administración

así como el gateway predeterminado, realizar forzado de enlace troncal en las interfaces F0/3 y F0/5, generar configuración sobre el resto de los puertos como puertos de acceso, realizar signar la interface F0/6 a la VLAN 21 y realizar el apagado de todos los puertos sin usar en el Switch S1

Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 26. Configuración de seguridad, VLAN y routing entre VLAN del switch S1) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 26, podemos asegurar que el Switch S1 quede configurado de la manera correcta.

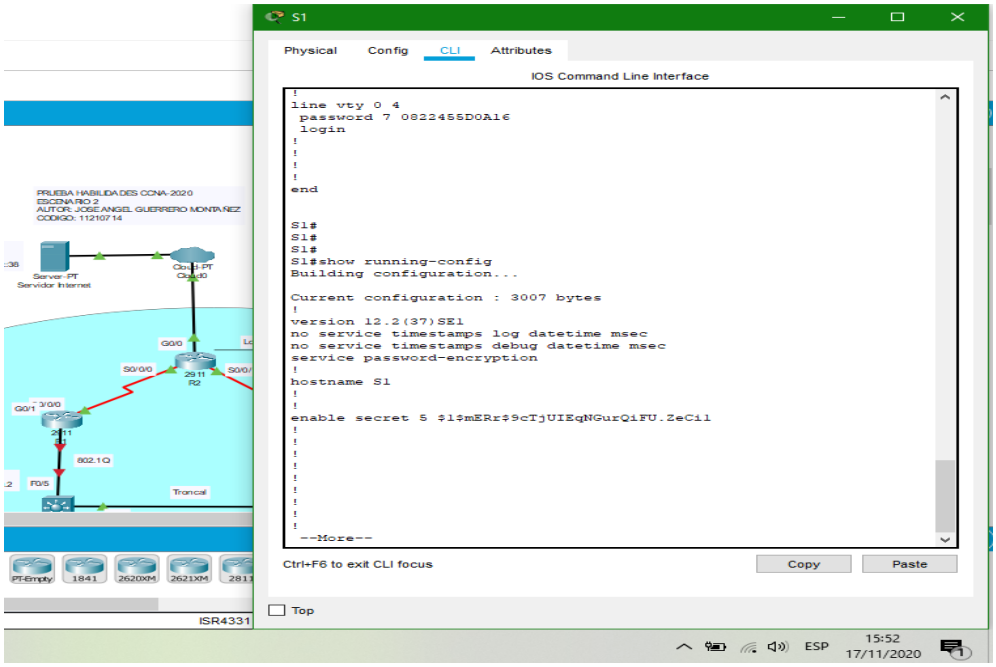
Tabla 26. Configuración de seguridad y routing entre VLAN del switch S1

Configuración Switch S1	
Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	Se realiza la inserción de esta línea de comandos para Crear la base de datos de VLAN en el Switch 1 **S1#config terminal** **S1(config)#vlan 21** **S1(config-vlan)#name Contabilidad** **S1(config-vlan)#exit** **S1(config)#vlan 23** **S1(config-vlan)#name Ingenieria** **S1(config-vlan)#exit** **S1(config)#vlan 99** **S1(config-vlan)#name Administracion** **S1(config-vlan)#exit**
Asignar la dirección IP de administración.	Se realiza la inserción de estas líneas de comandos para asignar dirección IP de administración en Switch 1 **S1(config)#int vlan 99** **S1(config-if)#ip address 192.168.99.2 255.255.255.0** **S1(config-if)#no shutdown**
Asignar el gateway predeterminado	Se realiza la inserción de estas líneas de comandos para asignar el gateway predeterminado en el Switch 1 **S1(config)#ip default-gateway 192.168.99.1**

Forzar el enlace troncal en la interfaz F0/3	Se realiza la inserción de estas líneas de comandos para Forzar el enlace troncal en la interfaz F0/3en el Switch 1 **S1(config)#int f0/3** **S1(config-if)#switchport mode access** **S1(config-if)#switchport mode trunk** **S1(config-if)#switchport trunk native vlan 1** **S1(config-if)#switchport trunk encapsulation dot1q** **S1(config-if)#no shutdown** **S1(config-if)#description Conexion a R1 S1(config-if)#exit**
Forzar el enlace troncal en la interfaz F0/5	Se realiza la inserción de estas líneas de comandos para Forzar el enlace troncal en la interfaz F0/5 en el Switch 1 **S1(config)#int f0/5** **S1(config-if)#switchport mode access** **S1(config-if)#switchport mode trunk** **S1(config-if)#switchport trunk native vlan 1** **S1(config-if)#switchport trunk encapsulation dot1q** **S1(config-if)#no shutdown** **S1(config-if)#description Conexion a R1**
Configurar el resto de los puertos como puertos de acceso	Se realiza la inserción de estas líneas de comandos para Configurar el resto de los puertos como puertos de acceso en el Switch 1 **S1(config)#int range f0/1-2, f0/4, f0/6-24, g0/1-2** **S1(config-if-range)#switch mode Access** **S1(config-if-range)#exit**
Asignar F0/6 a la VLAN 21	Se realiza la inserción de estas líneas de comandos para Asignar F0/6 a la VLAN 21 en el Switch 1 **S1(config-if)#interface f0/6** **S1(config-if)#switchport mode access** **S1(config-if)#switchport access vlan 21** **S1(config-if)#exit**
Apagar todos los puertos sin usar	Se realiza la inserción de estas líneas de comandos para Apagar todos los puertos sin usar en el Switch 1 **S1(config-if)#int range fa0/1-2, fa0/4, fa0/7-24, g0/1-2** **S1(config)#shutdown** **S1(config-if-range)#exit** **S1(config)#exit**

Verificar configuraciones en los Switch	Se realiza la inserción de esta línea de comandos para verificar configuraciones en los Switch **S1>en** **S1#show running-config**

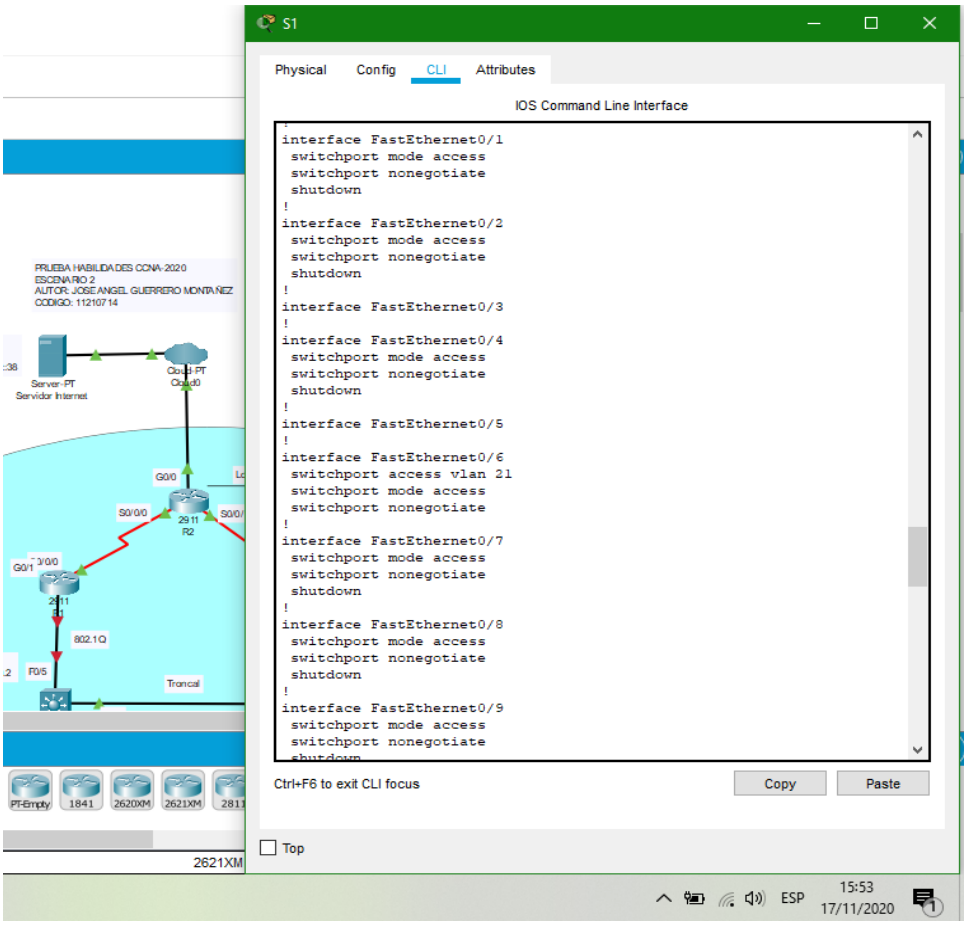
Figura 59. Configuración general VLANs en Switch S1



Fuente: Autor

Se realiza la verificación de la configuración general ingresada sobre la seguridad del switch S1, las VLAN y el routing entre VLAN en S1 siendo exitosa su creación este procedimiento es similar en todos los Switch

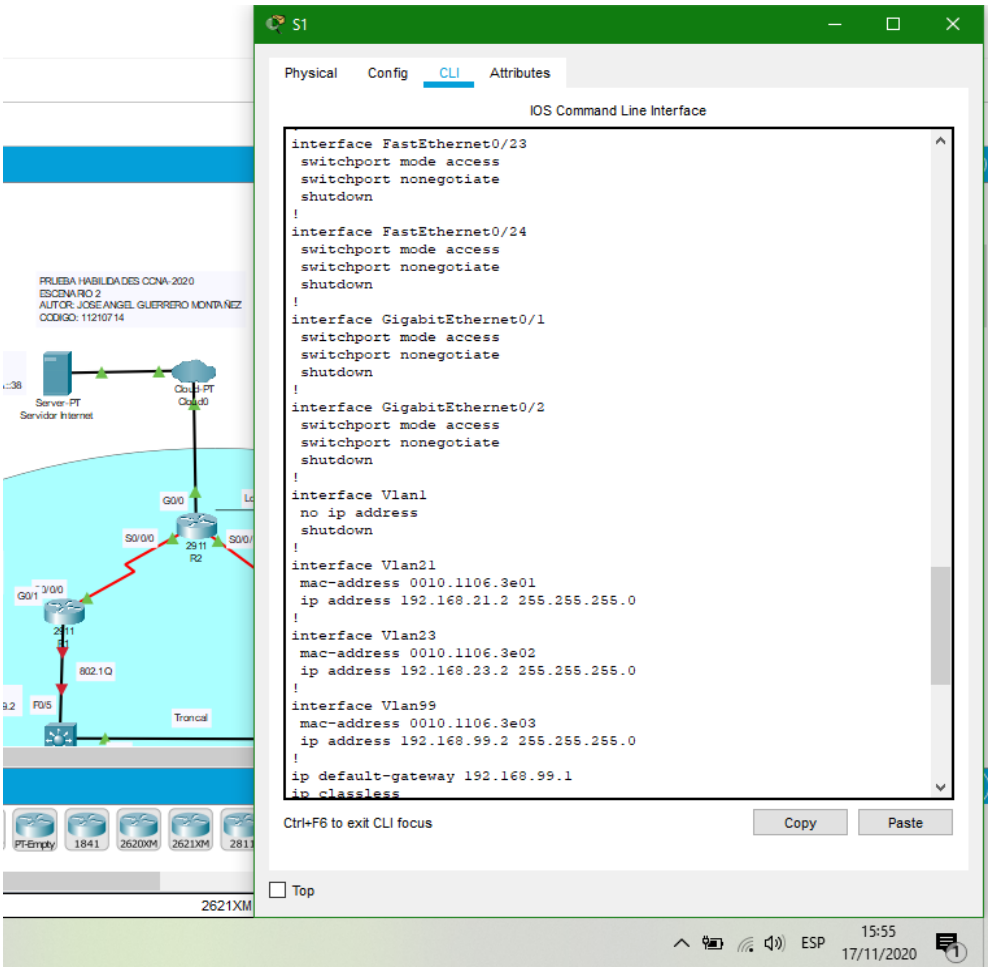
Figura 60. Configuración general VLANs en Switch S1 (2)



Fuente: Autor

Se realiza la verificación de la configuración general ingresada sobre la seguridad del switch S1, las VLAN y el routing entre VLAN en S1 siendo exitosa su creación este procedimiento es similar en todos los Switch

Figura 61. Configuración general VLANs en Switch S1 (3)



Fuente: Autor

Se realiza la verificación de la configuración general ingresada sobre la seguridad del switch S1, las VLAN y el routing entre VLAN en S1 siendo exitosa su creación este procedimiento es similar en todos los Switch

7.2. Paso 2: Configurar el S3

Apoyado en la topología de la red se realizará la configuración sobre la seguridad del switch, las VLAN y el routing entre VLAN del Switch S3 utilizando cada uno de los parámetros básicos establecidos en este escenario 2 como son creación de la base de datos de VLAN, realizar la asignación de su dirección IP de administración así como el gateway predeterminado, realizar forzado de enlace troncal en las interfaces F0/3, generar configuración sobre el resto de los puertos como puertos

de acceso, realizar signar la interface F0/18 a la VLAN 21 y realizar el apagado de todos los puertos sin usar en el Switch S3

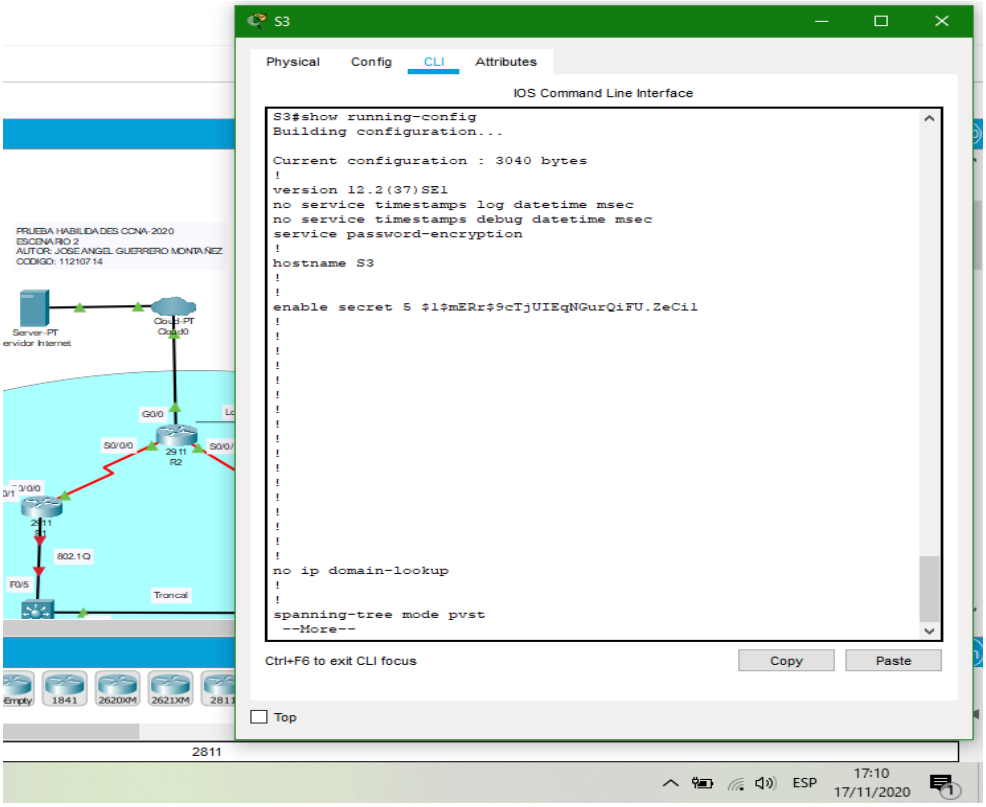
Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 27. Configuración de seguridad, VLAN y routing entre VLAN del switch S3) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 27, podemos asegurar que el Switch S3 quede configurado de la manera correcta.

Tabla 27. Configuración de seguridad y routing entre VLAN del switch S2

Configuración Switch S3	
Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	Se realiza la inserción de esta línea de comandos para Crear la base de datos de VLAN en el Switch 3 **S3#config terminal** **S3(config)#vlan 21** **S3(config-vlan)#name Contabilidad** **S3(config-vlan)#exit** **S3(config)#vlan 23** **S3(config-vlan)#name Ingenieria** **S3(config-vlan)#exit** **S3(config)#vlan 99** **S3(config-vlan)#name Administracion** **S3(config-vlan)#exit**
Asignar la dirección IP de administración.	Se realiza la inserción de estas líneas de comandos para asignar la dirección IP de administración en Switch 3 **S3(config)#int vlan 21** **S3(config-if)#ip address 192.168.21.3 255.255.255.0** **S3(config-if)#Description Vlan Contabilidad** **S3(config-if)#int vlan 23** **S3(config-if)#ip address 192.168.23.3 255.255.255.0** **S3(config-if)#description Vlan Ingenieria** **S3(config-if)#int vlan 99** **S3(config-if)#ip address 192.168.99.3 255.255.255.0** **S3(config-if)#description Vlan Ingenieria**
Asignar el gateway predeterminado	Se realiza la inserción de estas líneas de comandos para asignar el gateway predeterminado en Switch 3 **S3(config)#ip default-gateway 192.168.99.1**

Forzar el enlace troncal en la interfaz F0/3	Se realiza la inserción de estas líneas de comandos para Forzar el enlace troncal en la interfaz F0/3en el Switch 3 **S3(config)#int f0/3** **S3(config-if)#switchport mode access** **S3(config-if)#switchport mode trunk** **S3(config-if)#switchport trunk native vlan 1** **S3(config-if)#Switchport trunk encapsulation dot1q** **S3(config-if)#description Conexion a S1** **S3(config-if)#no shutdown** **S3(config-if)#exit**
Configurar el resto de los puertos como puertos de acceso	Se realiza la inserción de estas líneas de comandos para Configurar el resto de los puertos como puertos de acceso en el Switch 3 **S3(config)#int range fa0/1-2, fa0/4-24, g0/1-2** **S3(config-if-range)#switch mode Access** **S3(config-if-range)#exit**
Asignar F0/18 a la VLAN 21	Se realiza la inserción de estas líneas de comandos para Asignar F0/18 a la VLAN 21 en el Switch 3 **S3(config)#int f0/18** **S3(config-if)#switchport mode access** **S3(config-if)#switchport access vlan 23** **S3(config-if)#no shutdown** **S3(config-if)#exit**
Apagar todos los puertos sin usar	Se realiza la inserción de estas líneas de comandos para Apagar todos los puertos sin usar en el Switch 3 **S3(config)#interface range f0/1-2, f0/4-17, f0/19-24** **S3(config-if-range)#shutdown** **S3(config-if-range)#exit** **S3(config)#exit**
Verificar configuraciones en los Switch	Se realiza la inserción de esta línea de comandos para verificar configuraciones en los Switch **S3>en** **S3#show running-config**

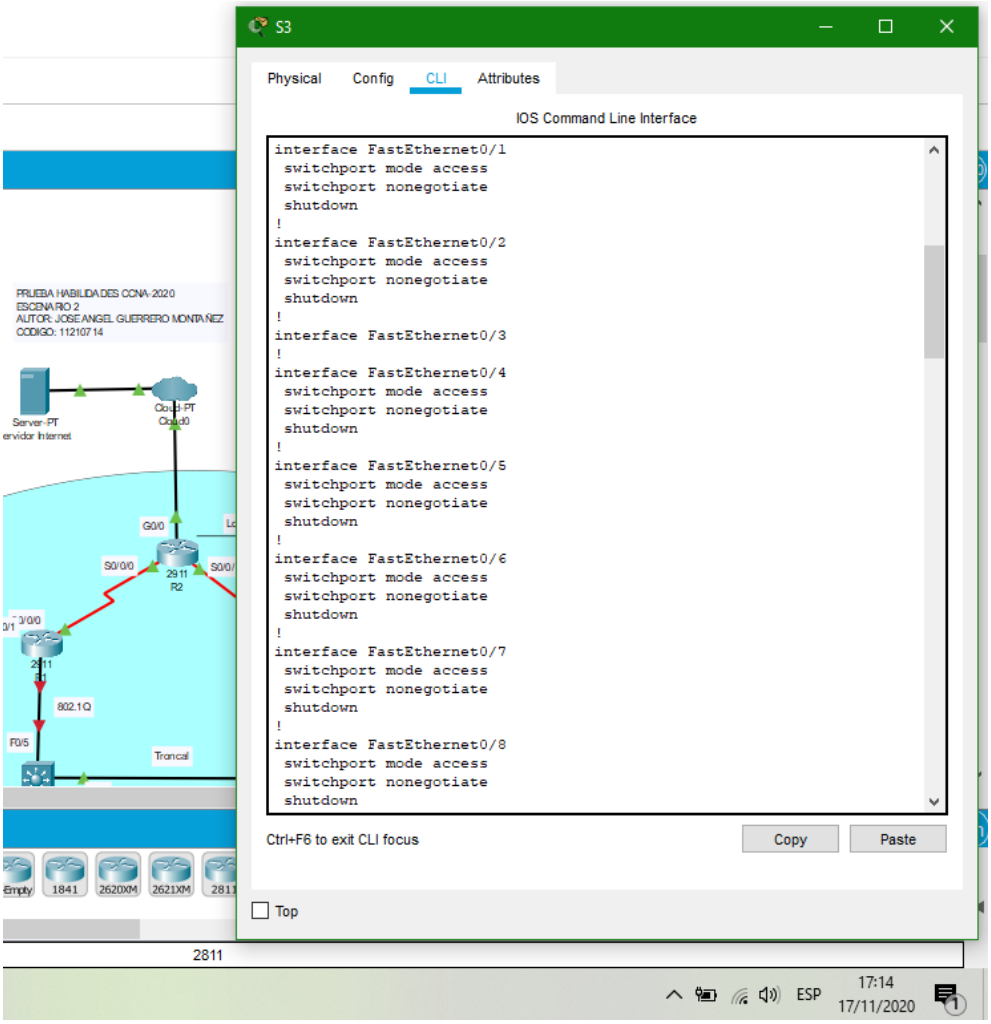
Figura 62. Configuración general VLANs en Switch S3



Fuente: Autor

Se realiza la verificación de la configuración general ingresada sobre la seguridad del switch S3, las VLAN y el routing entre VLAN en S3 siendo exitosa su creación este procedimiento es similar en todos los Switch

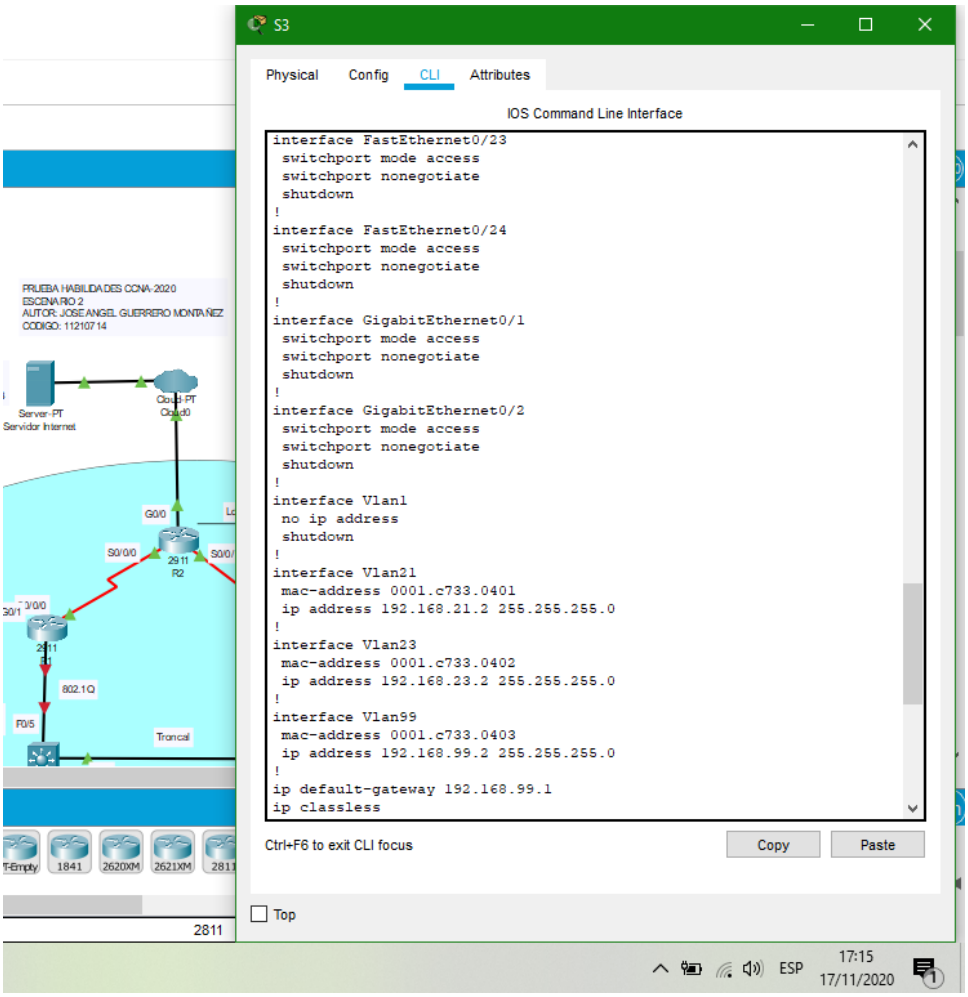
Figura 63. Configuración general VLANs en Switch S3 (2)



Fuente: Autor

Se realiza la verificación de la configuración general ingresada sobre la seguridad del switch S3, las VLAN y el routing entre VLAN en S3 siendo exitosa su creación este procedimiento es similar en todos los Switch

Figura 64. Configuración general VLANs en Switch S3 (3)



Fuente: Autor

Se realiza la verificación de la configuración general ingresada sobre la seguridad del switch S3, las VLAN y el routing entre VLAN en S3 siendo exitosa su creación este procedimiento es similar en todos los Switch

7.3. Paso 3: Configurar R1

Apoyado en la topología de la red se realizará la configuración del router R1 utilizando cada uno de los parámetros básicos establecidos en este escenario 2 como son Configurar la subinterfaz 802.1Q .21 en G0/1, subinterfaz 802.1Q .23 en G0/1, Configurar la subinterfaz 802.1Q .99 en G0/1, Activar la interfaz G0/1 y verificar configuraciones en los router.

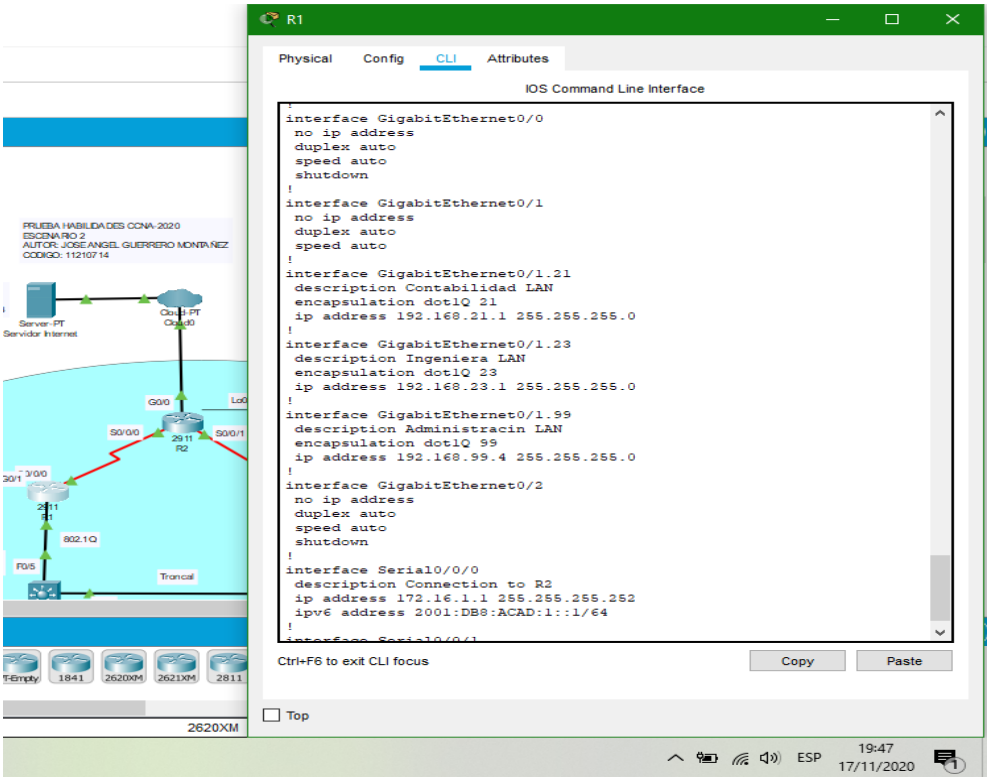
Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 28. Configuración subinterfaz 802.1Q en Router R1) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 28, podemos asegurar que el Router R1 quede configurado de la manera correcta

Tabla 28. Configuración subinterfaz 802.1Q en Router R1

Configuración Router R1	
Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	Se realiza la inserción de esta línea de comandos para Configurar la subinterfaz 802.1Q .21 en G0/1en el router 1 **R1(config)#int g0/1.1** **R1(config-subif)#description LAN de Contabilidad** **R1(config-subif)#encapsulation dot1q 21** **R1(config-subif)#ip address 192.168.21.4 255.255.255.0** **R1(config-subif)#exit**
Configurar la subinterfaz 802.1Q .23 en G0/1	Se realiza la inserción de esta línea de comandos para Configurar la subinterfaz 802.1Q .23 en G0/1en el router 1 **R1(config)#int g0/1.2** **R1(config-subif)#encapsulation dot1q 23** **R1(config-subif)#ip address 192.168.23.4 255.255.255.0** **R1(config-subif)#exit** **R1(config)#**
Configurar la subinterfaz 802.1Q .99 en G0/1	Se realiza la inserción de estas líneas de comandos para Configurar la subinterfaz 802.1Q .99 en G0/1en el router 1 **R1(config)#int g0/1.3** **R1(config-subif)#description LAN de Administracion** **R1(config-subif)#encapsulation dot1q 99** **R1(config-subif)#ip address 192.168.99.4 255.255.255.0** **R1(config-subif)#exit** **R1(config)#**

Activar la interfaz G0/1	Se realiza la inserción de estas líneas de comandos para asignar una Activar la interfaz G0/1en el router 1 **R1(config)#interface gigabitEthernet 0/1** **R1(config-if)#no shutdown** **R1(config-subif)#exit** **R1(config)#exit**
Verificar la configuración en el router	Se realiza la inserción de esta línea de comandos para verificar la configuración en el router **R1>en** **R1#show running-config**

Figura 65. Configuración subinterfaz 802.1Q en Router R1



Fuente: Autor

Se realiza la verificación de la configuración general sobre creación de interfaces o subinterfaz 802.1Q .21 en G0/1, subinterfaz 802.1Q .23 en G0/1, Configurar la subinterfaz 802.1Q .99 en G0/1, Activar la interfaz G0/1, así como la descripción que pueden asignarse en R1 siendo exitoso este procedimiento.

7.4. Paso 4: Verificar la conectividad de la red

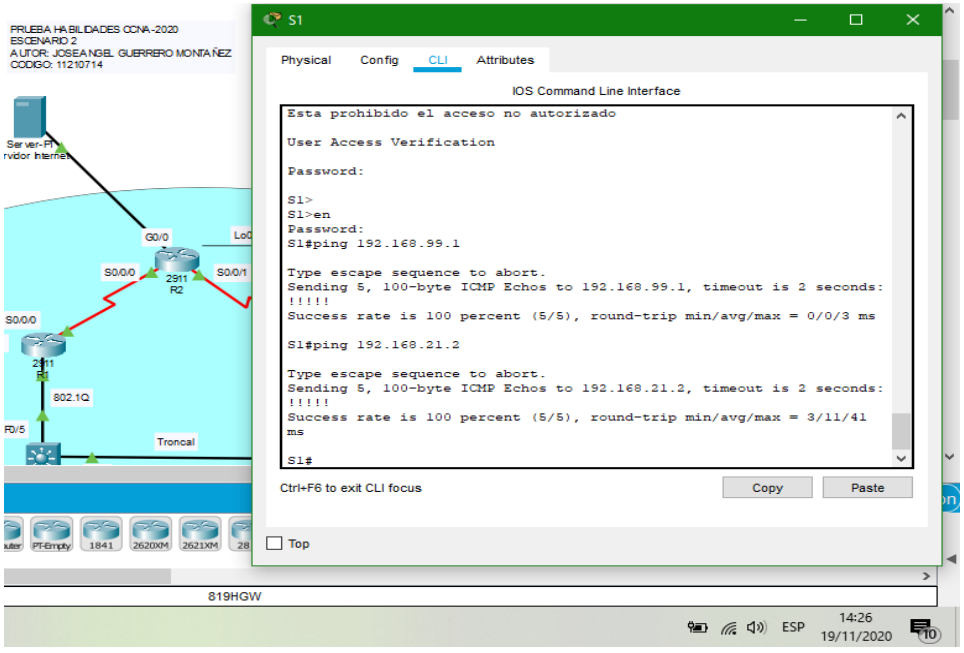
Para realizar la prueba de pines entre dispositivos se utilizarán las direcciones establecidas en las siguientes tablas (Tabla 29. Verificación de conectividad de la red) entre switches y el R1.

Tabla 29. Verificación de conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	El ping IPv4 Si fue realizado con éxito
S3	R1, dirección VLAN 99	192.168.99.1	El ping IPv4 Si fue realizado con éxito
S1	R1, dirección VLAN 21	192.168.21.2	El ping IPv4 Si fue realizado con éxito
S3	R1, dirección VLAN 23	192.168.23.2	El ping IPv4 Si fue realizado con éxito

Para realizar cada ping entre dispositivo se debe tener en cuenta el tipo de dirección a la cual se quiere hacer el procedimiento identificando si estas es IPv4 o IPv6 puesto que la estructura de dirección tiene diferente sintaxis.

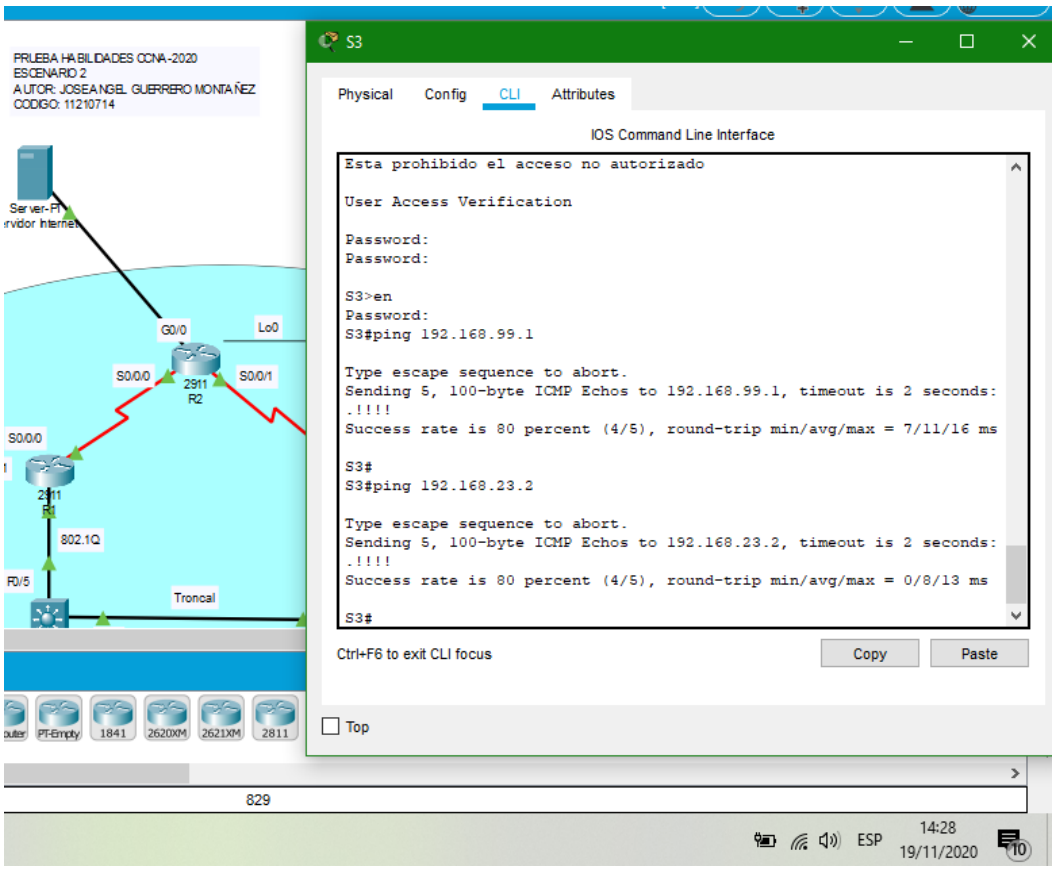
Figura 66. Ping desde Switch S1 hacia dirección de VLAN 99 y 21 en R1



Fuente: Autor

Se realiza Ping desde Switch S1 hacia cada dirección asignada a las VLAN 99 y 21 en R1 enviando los paquetes a sus dirección IPv4 utilizando el comando ping 192.168.99.1 para VLAN 99 y ping 192.168.21.2 para VLAN 21 logrando realizar el pin con éxito.

Figura 67. Ping desde Switch S3 hacia dirección de VLAN 99 y 23 en R1



Fuente: Autor

Se realiza Ping desde Switch S3 hacia cada dirección asignada a las VLAN 99 y 23 en R1 enviando los paquetes a su dirección IPv4 utilizando el comando ping 192.168.99.1 para VLAN 99 y ping 192.168.23.2 para VLAN 23 logrando realizar el pin con éxito.

8. Parte 4: Configurar el protocolo de routing dinámico OSPF

8.1. Paso 1: Configurar OSPF en el R1

Apoyado en la topología de la red se realizará la configuración del router R1 utilizando cada uno de los parámetros básicos establecidos en este escenario 2 como son realizar configuración OSPF área 0, anunciar las redes conectadas directamente, Estableciendo todas las interfaces LAN como pasivas, realizar la desactivación de la sumarización automática y verificar configuraciones en el router.

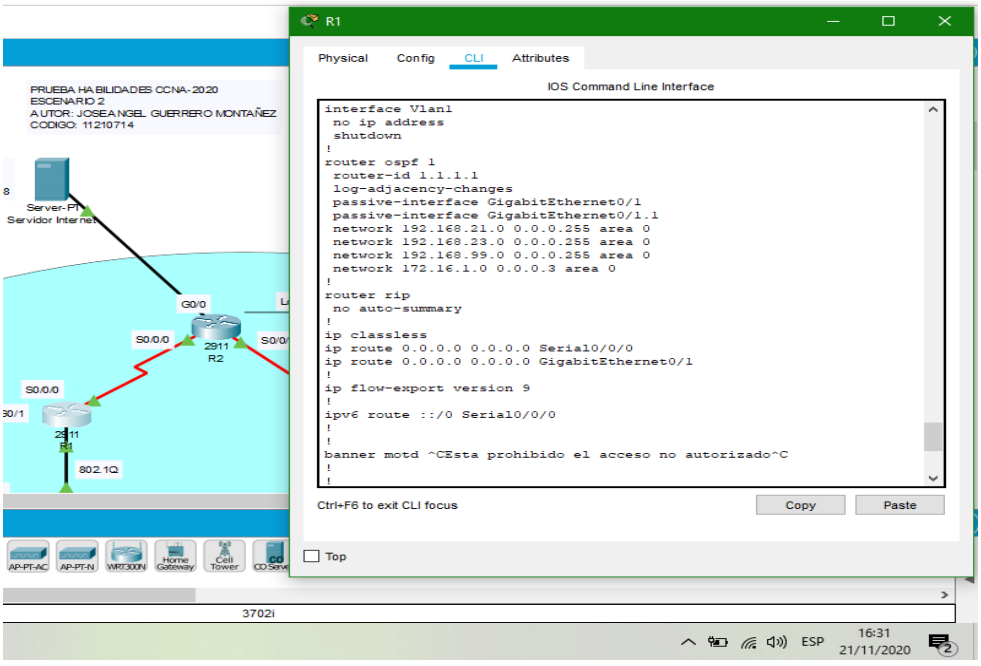
Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 30. Configuración OSPF en Router R1) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 30, podemos asegurar que el Router R1 quede configurado de la manera correcta

Tabla 30. Configuración OSPF en Router R1

Configuración OSPF en Router R1	
Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	Se realiza la inserción de esta línea de comandos para Configurar OSPF área 0 en el Router 1 **R1(config)#router ospf 1**
Anunciar las redes conectadas directamente	Se realiza la inserción de esta línea de comandos para Anunciar las redes conectadas directamente en el Router 1 **R1(config-router)#router-id 1.1.1.1** **R1(config-router)#network 192.168.21.0 0.0.0.255 area 0** **R1(config-router)#network 192.168.23.0 0.0.0.255 area 0** **R1(config-router)#network 192.168.99.0 0.0.0.255 area 0** **R1(config-router)#network 172.16.1.0 0.0.0.3 area 0** **R1#show running-config**
Establecer todas las interfaces LAN como pasivas	Se realiza la inserción de esta línea de comandos para Establecer todas las interfaces LAN como pasivas en el Router 1

	R1(config-router)#passive-interface g0/1.1 **R1(config-router)#passive-interface g0/1** **R1(config-router)#exit** **R1(config)#exit**
Desactive la sumarización automática	De forma predeterminada, RIP y EIGRP resumen las redes a sus límites con la clase por tal motivo el comando **no auto-summary** deshabilita esa función. Por otro lado OSPF como protocolo de enrutamiento de estado de enlace (se ocupa de LSA en lugar de rutas) no se resume automáticamente (no admite el "resumen automático"). En resumen de lo anterior en OSPF no se realiza un resumen automático, por lo que **R1(config-router)#no auto-summary** no es un comando necesario. Pero en RIP y EIGRP se usan los siguientes comandos. **R1(config-router)#router rip** **R1(config-router)#no auto** **R1(config-router)#no auto-summary** **R2#show running-config**

Figura 68. Configuración OSPF en Router R1



Fuente: Autor

Se realiza la verificación en el router R1 mediante el comando **show running-config** sobre la configuración OSPF área 0, anunciar las redes conectadas directamente, Estableciendo todas las interfaces LAN como pasivas, realizar la desactivación de la sumarización automática siendo exitoso este procedimiento.

8.2. Paso 2: Configurar OSPF en el R2

Apoyado en la topología de la red se realizará la configuración del router R2 utilizando cada uno de los parámetros básicos establecidos en este escenario 2 como son realizar configuración OSPF área 0, anunciar las redes conectadas directamente, Estableciendo todas las interfaces LAN como pasivas, realizar la desactivación de la sumarización automática y verificar configuraciones en el router.

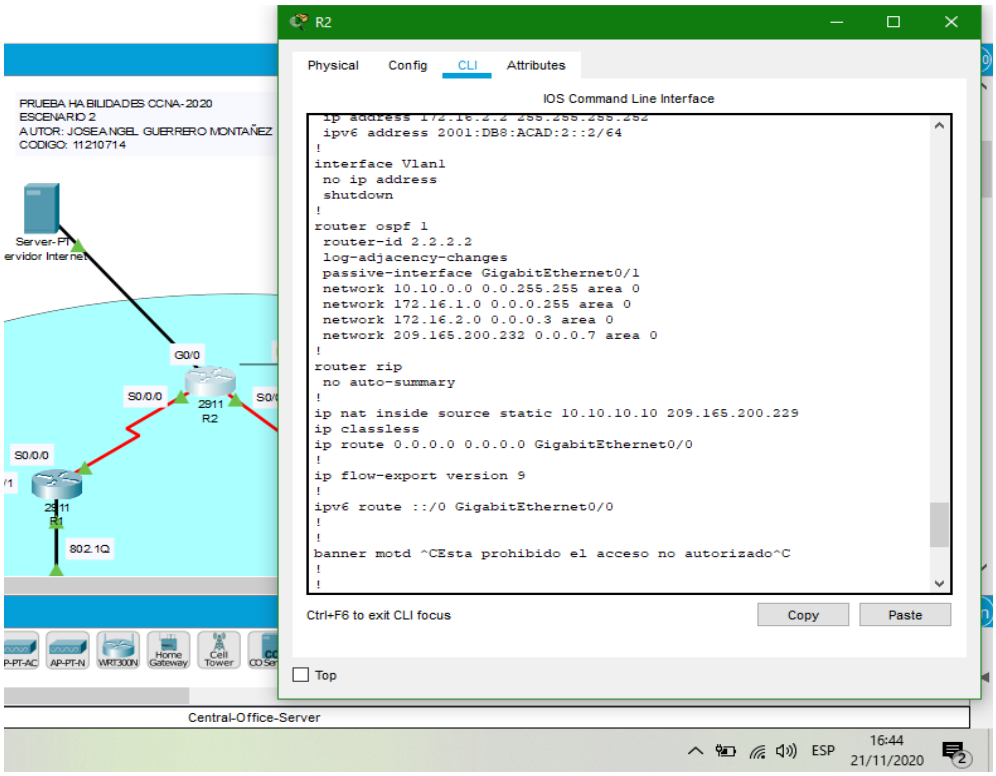
Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 31. Configuración OSPF en Router R2) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 31, podemos asegurar que el Router R1 quede configurado de la manera correcta

Tabla 31. Configuración OSPF en Router R2

Configuración Router R2	
Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	Se realiza la inserción de esta línea de comandos para Configurar OSPF área 0 en el Router 1 **R1(config)#router ospf 1**
Anunciar las redes conectadas directamente	Se realiza la inserción de esta línea de comandos para Anunciar las redes conectadas directamente en el Router 1 **R2(config-router)#router-id 2.2.2.2** **R2(config-router)#log-adjacency-changes** **R2(config-router)#passive-interface GigabitEthernet0/1** **R2(config-router)#network 10.10.0.0 0.0.255.255 area 0** **R2(config-router)#network 172.16.1.0 0.0.0.255 area 0**

	R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 **R2(config-router)#network 209.165.200.232 0.0.0.7 area 0**
Establecer todas las interfaces LAN como pasivas	Se realiza la inserción de esta línea de comandos para Establecer todas las interfaces LAN como pasivas en el Router 2 **R2(config-router)#passive-interface g0/1** **R2(config-router)#exit** **R2(config)#exit**
Desactive la sumarización automática	De forma predeterminada, RIP y EIGRP resumen las redes a sus límites con la clase por tal motivo el comando **no auto-summary** deshabilita esa función. Por otro lado OSPF como protocolo de enrutamiento de estado de enlace (se ocupa de LSA en lugar de rutas) no se resume automáticamente (no admite el "resumen automático"). En resumen de lo anterior en OSPF no se realiza un resumen automático, por lo que **R1(config-router)#no auto-summary** no es un comando necesario. Pero en RIP y EIGRP se usan los siguientes comandos. **R2(config-router)#router rip** **R2(config-router)#no auto** **R2(config-router)#no auto-summary** **R2#show running-config**

Figura 69. Configuración OSPF en Router R2



Fuente: Autor

Se realiza la verificación en el router R2 mediante **show running-config** sobre la configuración OSPF área 0, anunciar las redes conectadas directamente, Estableciendo todas las interfaces LAN como pasivas, realizar la desactivación de la sumarización automática siendo exitoso este procedimiento.

8.3. Paso 3: Configurar OSPFv3 en el R3

Apoyado en la topología de la red se realizará la configuración del router R3 utilizando cada uno de los parámetros básicos establecidos en este escenario 2 como son realizar configuración OSPF área 0, anunciar las redes conectadas directamente, Estableciendo todas las interfaces LAN como pasivas, realizar la desactivación de la sumarización automática y verificar configuraciones en el router.

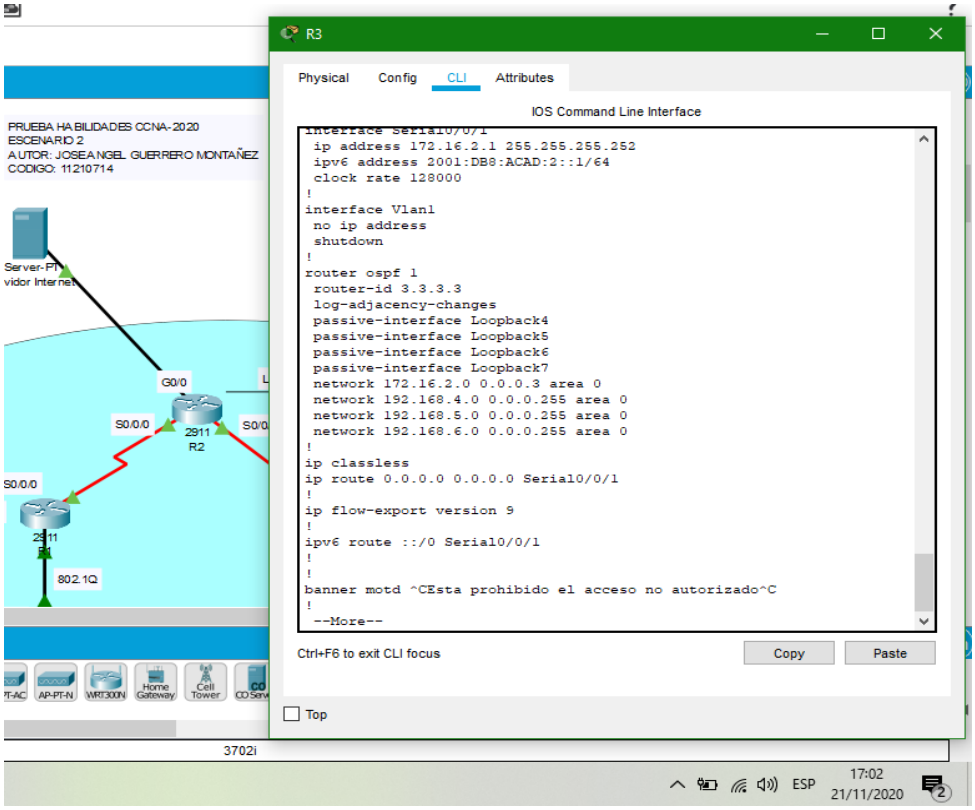
Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 32. Configuración OSPF en Router R3) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 32, podemos asegurar que el Router R1 quede configurado de la manera correcta

Tabla 32. Configuración OSPF en Router R3

Configuración OSPF Router R3	
Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	Se realiza la inserción de esta línea de comandos para Configurar OSPF área 0 en el Router 1 **R3(config)#router ospf 1** **R3(config-router)#router-id 3.3.3.3**
Anunciar las redes conectadas directamente	Se realiza la inserción de esta línea de comandos para Anunciar las redes conectadas directamente en el Router 1 **R3(config-router)#network 172.16.2.0 0.0.0.3 area 0** **R3(config-router)#network 192.168.4.0 0.0.0.255 area 0** **R3(config-router)#network 192.168.5.0 0.0.0.255 area 0** **R3(config-router)#network 192.168.6.0 0.0.0.255 area 0**
Establecer todas las interfaces LAN como pasivas	Se realiza la inserción de esta línea de comandos para Establecer todas las interfaces LAN como pasivas en el Router 2 **R3(config-router)#passive-interface loopback 4** **R3(config-router)#passive-interface loopback 5** **R3(config-router)#passive-interface loopback 6** **R3(config-router)#passive-interface loopback 7** **R3(config-router)#**
Desactive la sumarización automática	De forma predeterminada, RIP y EIGRP resumen las redes a sus límites con la clase por tal motivo el comando **no auto-summary** deshabilita esa función. Por otro lado OSPF como protocolo de enrutamiento de estado de enlace (se ocupa de LSA en lugar de rutas) no se resume automáticamente (no admite el "resumen automático"). En resumen de lo anterior en OSPF no se realiza un resumen automático, por lo que **R1(config-**

	router)#no auto-summary no es un comando necesario. Pero en RIP y EIGRP se usan los siguientes comandos. **R3(config-router)#router rip** **R3(config-router)#no auto** **R3(config-router)#no auto-summary** **R3#show running-config**

Figura 70. Configuración OSPF en Router R3



Fuente: Autor

Se realiza la verificación en el router R3 mediante **show running-config** sobre la configuración OSPF área 0, anunciar las redes conectadas directamente, Estableciendo todas las interfaces LAN como pasivas, realizar la desactivación de la sumarización automática siendo exitoso este procedimiento.

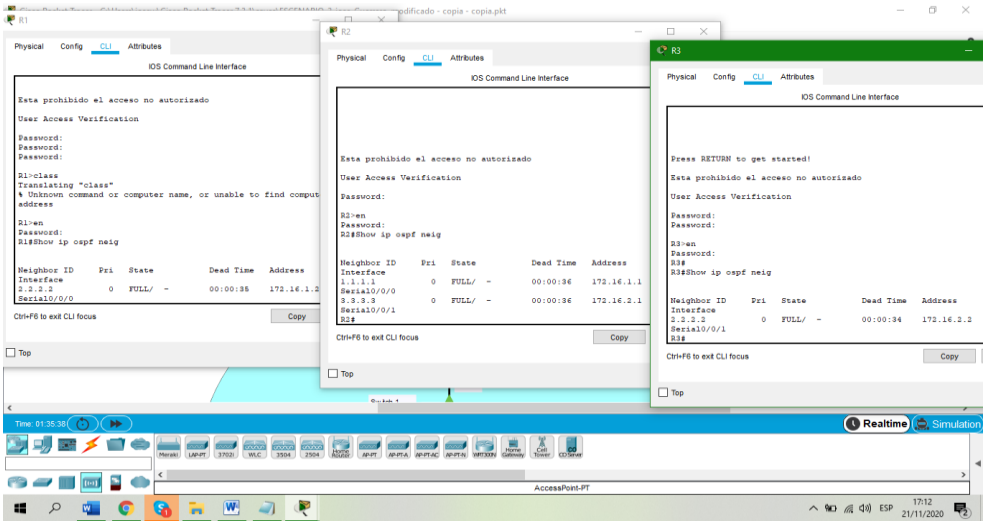
8.4. Paso 4: Verificar la información de OSPF

Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 27. Configuración OSPF en Router R3) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 27, podemos asegurar que el Router R1 quede configurado de la manera correcta

Tabla 33. Verificar configuración OSPF en Router R1, R2 y R3

Verificar configuración OSPF en Router R1, R2 y R3	
Elemento o tarea de configuración	**Especificación**
¿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?	Se realiza la inserción de esta línea de comandos para verificar con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en en el Router 1, 2 y3 **R3**# s**how ip ospf neig**
¿Qué comando muestra solo las rutas OSPF?	Se realiza la inserción de esta línea de comandos para verificar qué comando muestra solo las rutas OSPF en el Router 1, 2 y 3 **R3#show ip ospf interface**
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Se realiza la inserción de esta línea de comandos para verificar qué comando muestra la sección de OSPF de la configuración en ejecución en el Router 1, 2 y 3 **R3#show ip protocols**

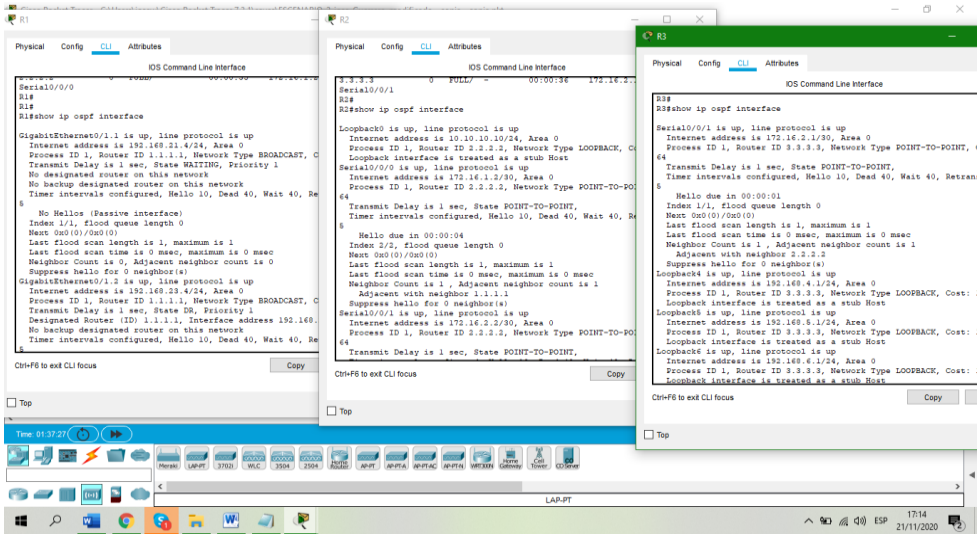
Figura 71. Verificar configuración OSPF en Router R1, R2 y R3 (1)



Fuente: Autor

Se realiza la verificación en el router R1, R2 y R3 sobre la configuración OSPF y con cual comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router siendo exitoso este procedimiento.

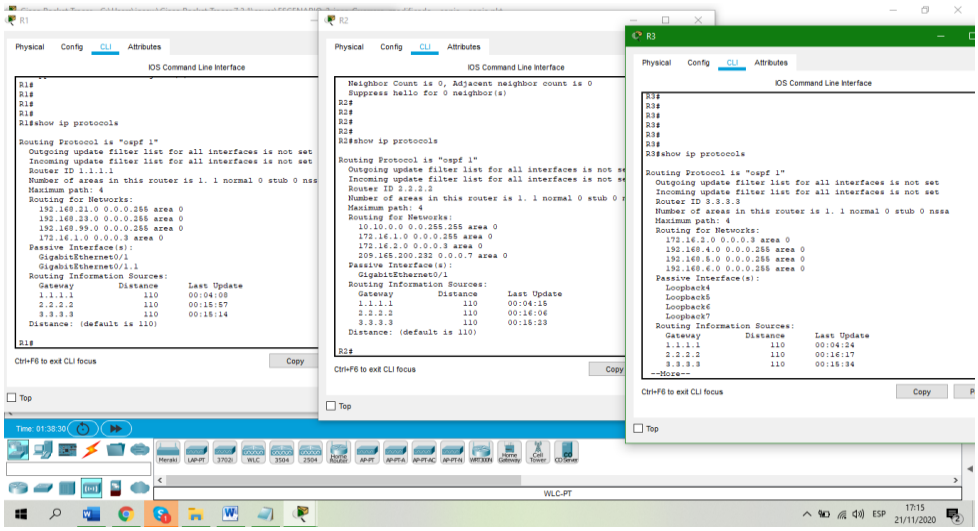
Figura 72. Verificar configuración OSPF en Router R1, R2 y R3 (2)



Fuente: Autor

Se realiza la verificación en el router R1, R2 y R3 sobre la configuración OSPF y con cual comando se muestran solo las rutas OSPF siendo exitoso este procedimiento.

Figura 73. Verificar configuración OSPF en Router R1, R2 y R3 (3)



Fuente: Autor

Se realiza la verificación en el router R1, R2 y R3 sobre la configuración OSPF y con cual comando se muestran la sección de OSPF de la configuración en ejecución en un router siendo exitoso este procedimiento.

9. Parte 5: Implementar DHCP y NAT para IPv4

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

Apoyado en la topología de la red se realizará la configuración del router R1 utilizando cada uno de los parámetros básicos establecidos en este escenario 2 como son reservar las primeras 20 direcciones IP en las VLAN 21 Y 23, así como crear un pool de DHCP para la VLAN 21 y otro para la VLAN 23 y verificar configuraciones en el router R1

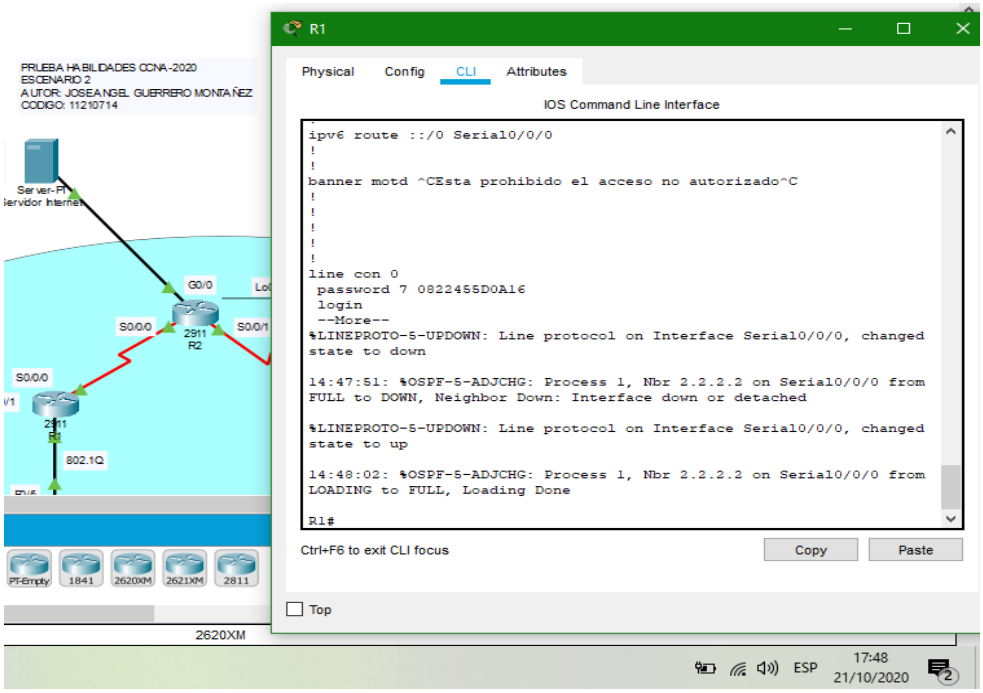
Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 36. Configuración DHCP y Pool en Router R1) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 34, podemos asegurar que el Router R1 quede configurado de la manera correcta.

Tabla 34. Configuración DHCP y Pool en Router R1

Configuración DHCP y Pool enRouter R1	
Elemento o tarea de configuración	**Especificación**
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	Se realiza la inserción de esta línea de comandos para Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas en el Router 1 **R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20**
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	Se realiza la inserción de esta línea de comandos para Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas en el Router 1 **R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20**
Crear un pool de DHCP para la VLAN 21.	Se realiza la inserción de esta línea de comandos para Crear un pool de DHCP para la VLAN 21 en el Router 1 Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el Gateway predeterminado **R1(config)#ip dhcp pool ACCT** **R1(dhcp-config)#dns-server 10.10.10.10** **R1(dhcp-config)#ip domain-name ccna-sa.com** **R1(dhcp-config)#default-router 192.168.21.1** **R1(dhcp-config)#network 192.168.21.0 255.255.255.0**
Crear un pool de DHCP para la VLAN 23	Se realiza la inserción de esta línea de comandos para Crear un pool de DHCP para la VLAN 23 en el Router 1 Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com

	Establecer el Gateway predeterminado **R1(config)#ip dhcp pool ENGNR** **R1(dhcp-config)#dns-server 10.10.10.10** **R1(dhcp-config)#default-router 192.168.23.1** **R1(dhcp-config)#ip domain-name ccna-sa.com** **R1(dhcp-config)#network 192.168.23.0** **255.255.255.0** **R1#show running-config**

Figura 74. Configuración DHCP y Pool en Router R1



Fuente: Autor

Se realiza la verificación de la configuración general ingresada sobre reservar las primeras 20 direcciones IP en las VLAN 21 Y 23, así como crear un pool de DHCP para la VLAN 21 y otro para la VLAN 23 mediante el comando **show running-config** en el R1

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

Apoyado en la topología de la red se realizará la configuración del router R1 utilizando cada uno de los parámetros básicos establecidos en este escenario 2

como son realizar la creación de una base de datos local con una cuenta de usuario, configurando el servidor HTTP utilizando la base de datos local para la autenticación, además realizar la creación de una NAT estática al servidor web agregando la interfaz interna y externa para esta misma en el router R2

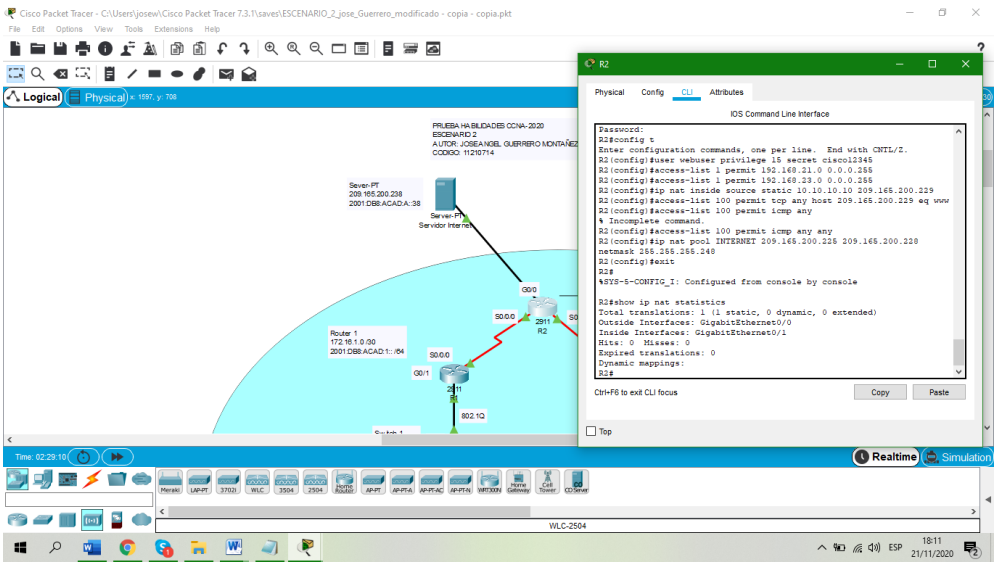
Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 35. Configuración NAT estática y dinámica en Router R2) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 35, podemos asegurar que el Router R1 quede configurado de la manera correcta.

Tabla 35. Configuración NAT estática y dinámica en Router R2

Configuración NAT estática y dinámica en Router R2	
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** Se realiza la inserción de esta línea de comandos para Crear una base de datos local con una cuenta de usuario en el Router 2 **R2(config)#user webuser privilege 15 secret cisco12345**
Habilitar el servicio del servidor HTTP	No Aplica equipos de simulación
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el Gateway predeterminado Se realiza la inserción de esta línea de comandos para Configurar el servidor HTTP para utilizar la base de datos local para la autenticación en el Router 1 **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 192.168.99.0 0.0.0.255**
Crear una NAT estática al servidor web.	Se realiza la inserción de esta línea de comandos para Crear una NAT estática al servidor web en el Router 2 **Dirección global interna: 209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	Se realiza la inserción de esta línea de comandos para Asignar la interfaz interna y externa para la NAT estática en el Router 2 **R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229**
Configurar la NAT dinámica dentro de una ACL privada	Se realiza la inserción de esta línea de comandos para Configurar la NAT dinámica dentro de una ACL privada en el Router 2 **R2(config)#access-list 100 permit tcp any host 209.165.200.229 eq www** **R2(config)#access-list 100 permit icmp any any**
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225 – 209.165.200.228** Se realiza la inserción de esta línea de comandos para Defina el pool de direcciones IP públicas utilizables en el Router 2 **R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248**
Definir la traducción de NAT dinámica	Se realiza la inserción de esta línea de comandos Definir la traducción de NAT dinámica en Router 2 **R2#show ip nat statistics**

Figura 75. Configuración NAT estática y dinámica en Router R2



Fuente: Autor

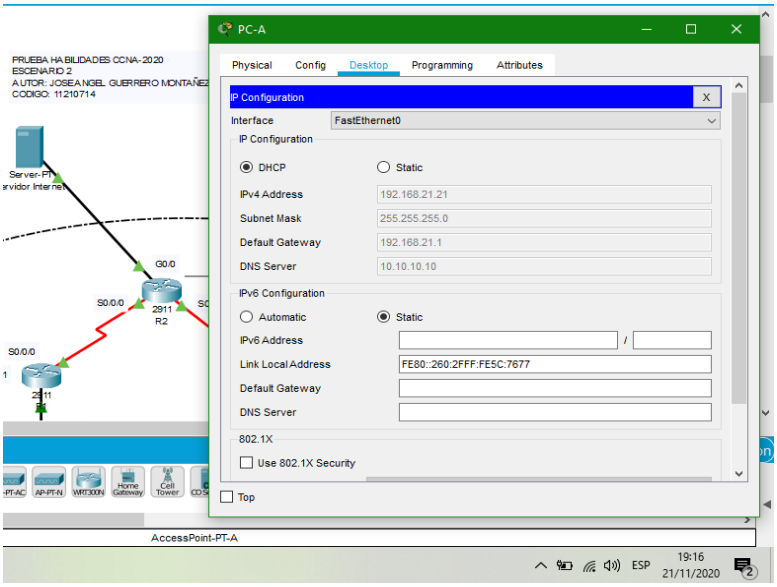
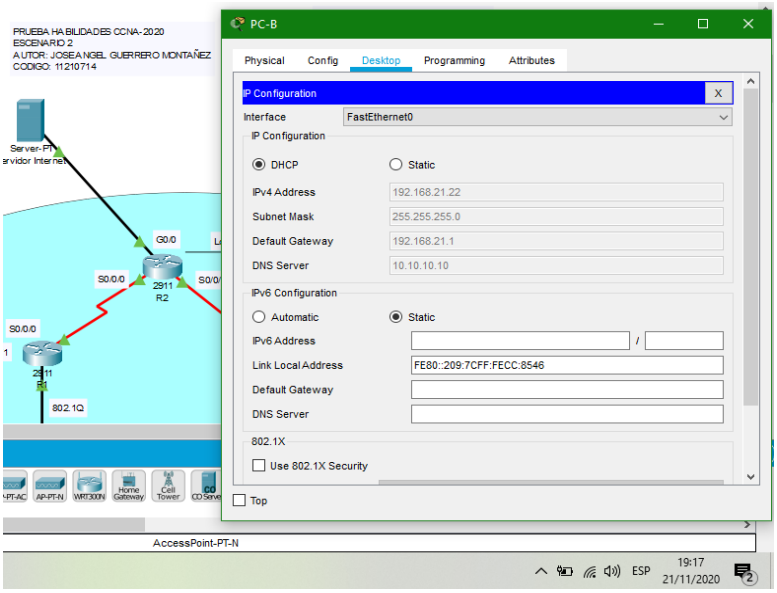
Se realiza la verificación de la configuración general ingresada sobre la creación de una base de datos local con una cuenta de usuario, configurando el servidor HTTP utilizando la base de datos local para la autenticación, además realizar la creación de una NAT mediante el comando **show ip nat statistics** en el R1

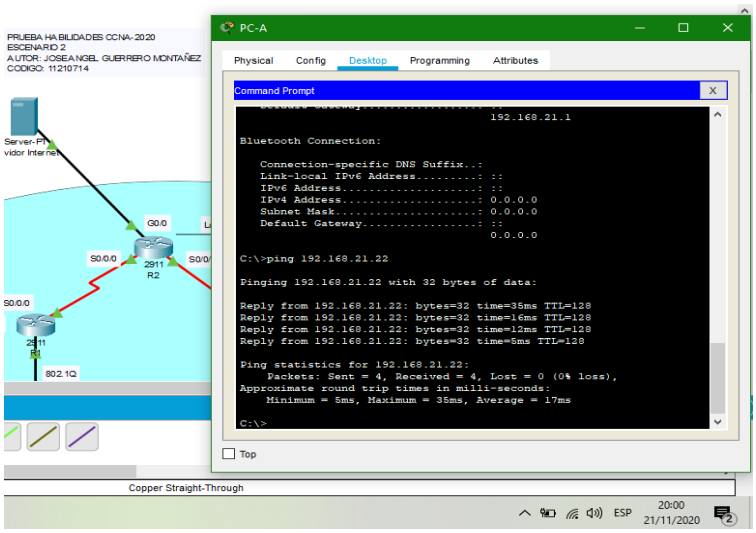
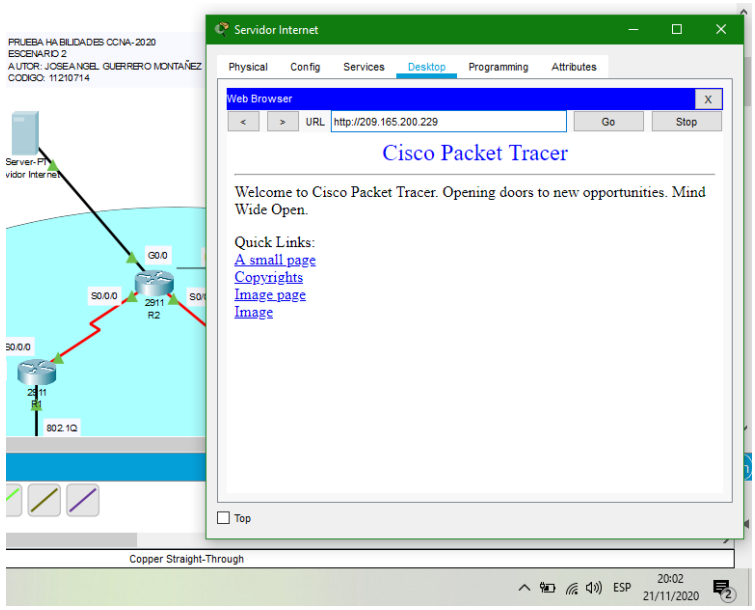
9.3. Paso 3: Verificar el protocolo DHCP y la NAT estática

Para esta tarea se realizará el uso de diferentes formas para verificar el protocolo DHCP y la NAT estática mediante el ingreso a las configuraciones de los diferentes dispositivos como Son el PC-A, PC-B y servidor web mostrados o contenidos en la (Tabla 36. Verificación del protocolo DHCP y la NAT estática) utilizando pines y configuración directa en los equipos observando que se han configurado de la manera correcta.

Tabla 36. Verificación del protocolo DHCP y la NAT estática

Verificación del protocolo DHCP y la NAT estática	
Elemento o tarea de configuración	**Especificación**

Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	*Figura 76. Verificación información de IP del servidor de DHCP*  Fuente: Autor
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	*Figura 77. Verificación información de IP del servidor de DHCP*  Fuente: Autor

Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	*Figura 78. Verificación Ping de PC-A a PC-B*  Fuente: Autor
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**	*Figura 79. Verificar el Inicio de sesión en Servidor*  Fuente: Autor

10. Parte 6: Configurar NTP

Apoyado en la topología de la red se realizará la configuración del router R1 y R2 utilizando cada uno de los parámetros básicos establecidos en este escenario 2 como son realizar la configuración y ajuste de la fecha y hora en R2 así como Configurar R2 como un maestro NTP y R1 como un cliente NTP y configurar las actualizaciones de calendario periódicas con hora NTP en R1 verificando la configuración NTP.

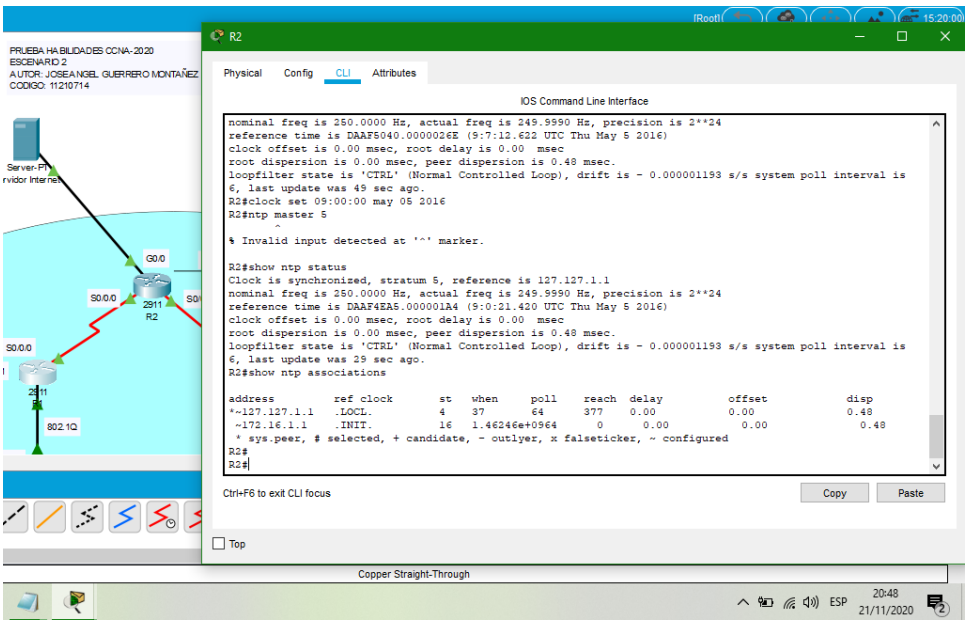
Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 37. Configuración NTP en Router R1 y R2) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 37, podemos asegurar que el Router R1 quede configurado de la manera correcta.

Tabla 37. Configuración NTP en Router R1 y R2

Configuración NTP en Router R1 y R2	
Elemento o tarea de configuración	**Especificación**
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** Se realiza la inserción de esta línea de comandos para Ajuste la fecha y hora en el Router 2 **R2#clock set 09:00:00 may 05 2016**
Configure R2 como un maestro NTP.	Nivel de estrato: **5** Se realiza la inserción de esta línea de comandos para Configure R2 como un maestro NTP en el Router 2 **R2(config)#ntp master 5**
Configurar R1 como un cliente NTP.	Servidor: **R2** Se realiza la inserción de esta línea de comandos para Configurar R1 como un cliente NTP **R2(config)#ntp server 172.16.1.1**

Configure R1 para actualizaciones de calendario periódicas con hora NTP.	Se realiza la inserción de esta línea de comandos para Configure R1 para actualizaciones de calendario periódicas con hora NTP. **R2(config)#ntp update-calendar** **R2(config)#end**
Verifique la configuración de NTP en R1.	Se realiza la inserción de esta línea de comandos para Configure R1 para actualizaciones de calendario periódicas con hora NTP. **R2#show ntp status** **R2#show ntp associations**

Figura 80. Configuración NTP en Router R1 y R2



Fuente: Autor

Se realiza la verificación de la configuración general ingresada sobre la creación y ajuste de la fecha y hora en R2 así como Configurar R2 como un maestro NTP y R1 como un cliente NTP y configurar las actualizaciones de calendario periódicas con hora NTP en R1 mediante el comando **show ntp status** y **show ntp associations** en el R1 y R2.

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

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

Apoyado en la topología de la red se realizará la configuración del router R1 y R2 utilizando cada uno de los parámetros básicos establecidos en este escenario 2 como son realizar la configuración de una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2, aplicando la ACL con nombre a las líneas VTY así como conceder permiso de acceso por Telnet a las líneas de VTY y su verificación.

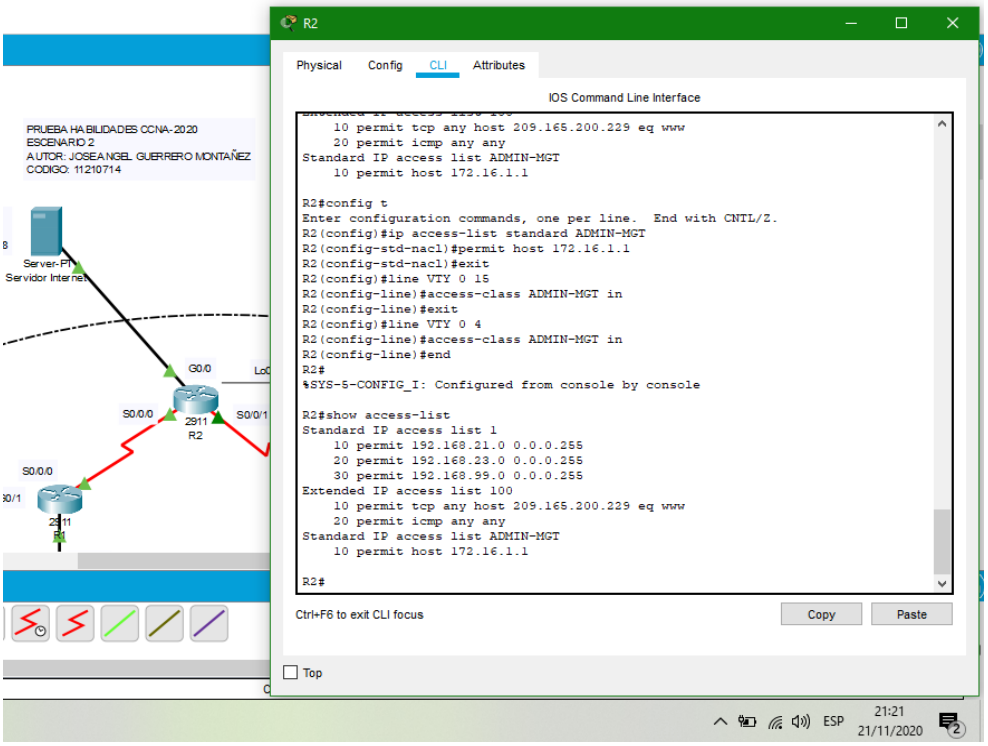
Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 38. Configuración NTP en Router R1 y R2) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 38, podemos asegurar que el Router R1 quede configurado de la manera correcta.

Tabla 38. Restricción de acceso a las líneas VTY en el R2

Restricción de 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.	Se realiza la inserción de esta línea de comandos para configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2.en el Router 2 **R2(config)#ip access-list standard ADMIN-MGT** **R2(config-std-nacl)#permit host 172.16.1.1** **R2(config-std-nacl)#exit**
Aplicar la ACL con nombre a las líneas VTY	Se realiza la inserción de esta línea de comandos para aplicar la ACL con nombre a las líneas VTY en el Router 2 **R2(config)#line VTY 0 15** **R2(config-line)#access-class ADMIN-MGT in** **R2(config-line)#exit**

Permitir acceso por Telnet a las líneas de VTY	Se realiza la inserción de esta línea de comandos para permitir acceso por Telnet a las líneas de VTY **R2(config)#line VTY 0 4** **R2(config-line)#access-class ADMIN-MGT in** **R2(config-line)#end**
Verificar que la ACL funcione como se espera	Se realiza la inserción de esta línea de comandos para verificar el funcionamiento de ACL. **R2# show access-list**

Figura 81. Restricción de acceso a las líneas VTY en el R2



Fuente: Autor

Se realiza la verificación de la configuración general ingresada sobre la creación la creación de una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2, aplicando la ACL con nombre a las líneas VTY así como conceder permiso de acceso por Telnet a las líneas de VTY mediante el comando **show access-list** el cual muestra que su creación fue exitosa

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

Apoyado en la topología de la red se realizará la introducción de los comandos necesarios de CLI que se necesitan para realizar las tareas como son mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció en cualquier router, realizar el restablecimiento de los contadores de una lista de acceso, además de mostrar cual comando es usado en ACL para aplicar a una interfaz y la dirección en que se aplica del mismo modo el comando que muestra las traducciones NAT y para eliminar las traducciones de NAT dinámicas?

Para esta tarea se realizará el uso de diferentes comandos mostrados o contenidos en la (Tabla 39. Configuración NTP en Router R1 y R2) con el fin de establecer las configuraciones anteriores por tal motivo con cada una las tareas de configuración, mostradas en la Tabla 39, podemos asegurar que el Router R1 quede configurado de la manera correcta.

Tabla 39. Comandos que muestran determinadas configuraciones en Router

Comandos que muestran determinadas configuraciones en R	
Descripción del comando	**Entrada del estudiante (comando)**
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Se realiza la inserción de esta línea de comandos para mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció en cualquier router **R1#show access-lists**
Restablecer los contadores de una lista de acceso	Se realiza la inserción de esta línea de comandos para restablecer los contadores de una lista de acceso en cualquier router **R1(config)#ip access-list standard 2** **R1(config-std-nacl)#18 permit 172.22.1.1** **R1(config-std-nacl)#exit**
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Se realiza la inserción de esta línea de comandos para saber qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica **R2#show ip nat translations**

¿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. Se realiza la inserción de esta línea de comandos para saber con qué comando se muestran las traducciones NAT **R2# show ip nat statistics**
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Se realiza la inserción de esta línea de comandos para saber qué comando se utiliza para eliminar las traducciones de NAT dinámicas. **R2#clear ip nat translation ***

12. CONCLUSIONES

Se concluye que mediante el desarrollo de este trabajo basado en la prueba de habilidades CCNA se establece el apropiamiento de cada concepto visto durante el curso del Diplomado de Profundización Cisco y con los cuales se lograron realizar configuraciones a dos redes en diferentes escenarios.

En conclusión, se establece que mediante la realización del escenario uno (1) y las diferentes configuraciones aplicadas a los equipos y en las cuales se permitió la conectividad mediante direccionamiento IPv4 e IPv6, realizando el proceso de configuración sobre temas de seguridad de switches, router, borrado de configuración inicial y de datos almacenados en memoria de estos dispositivos, así como la creación de VLAN y la verificación de cada comando insertado.

En conclusión, mediante la inserción de comandos se logran configurar interfaces y subinterfaces asignando direcciones y protocolos de seguridad, así como pruebas de seguimiento a los comandos insertados, validando la correcta configuración de los equipos mediante la generación de pines entre equipos y sus direcciones para comprobar él envió y recibido de paquetes de forma completa.

Se concluye mediante el escenario número dos (2) la importancia de conocer sobre protocolos de enrutamiento en este caso OSPF verificando que este quede bien configurado de igual forma proporcionarle configuración de rutas redistribuidas, encapsulamiento y autenticación cada router y switch así mismo se analiza y se genera la configuración de hosts dinámicos (DHCP), así como la traducción de direcciones establecidas en redes dinámicas y estáticas (NAT) utilizando (ACL) listas de control de acceso y de igual forma protocolo de tiempo de red (NTP) servidor/cliente.

En conclusión general se denota la correcta resolución de los escenarios propuesto siguiendo un manual de instrucciones para lograr la correcta la solución de estos ejercicios y en los cuales fue aplicado el uso de las diferentes estructuras como son armado de una topología simple usando cableado LAN Ethernet, accediendo a diferentes Router, switch, Servidores web y equipos PC Cisco para lograr su correcta configuración realizando borrado y reconfigurado básico en especial la asignación de las diferentes direcciones de los equipos en Versiones IPv4 e IPv6.y la asignación de estas mediante DHCP la cual permite evitar su asignación una por una y realizarlo de forma automática así mismo se logran afianzar los conocimientos adquiridos a través de algunas de las lecturas del curso y de esta manera se hace evidente la importancia de usar correctamente lo aprendido.

13. BIBLIOGRAFÍA

(86) Enrutamiento OSPF packet tracer comandos—YouTube. (s. f.). Recuperado 24 de noviembre de 2020, de https://www.youtube.com/watch?reload=9&v=iB6d3xmE1S0

⋆ Enrutamiento dinámico OSPF con Packet Tracer. (s. f.). Recuperado 24 de noviembre de 2020, de https://www.raulprietofernandez.net/blog/packet-tracer/enrutamiento-dinamico-ospf-con-packet-tracer

Altatec Seguridad. (2019a, octubre 1). Configurar Servidor DHCP en Packet Tracer (Paso a Paso) 2020. https://www.youtube.com/watch?v=JA1suf3o_Bw

Altatec Seguridad. (2019b, octubre 5). Como Configurar Servidor Web en Packet Tracer 2020. https://www.youtube.com/watch?v=xkLK7MWUIgQ

AquiHayDeTodo. (2017, marzo 27). Enrutamiento estatico (2 router) Packet Tracer. https://www.youtube.com/watch?v=IMwxIyqpbMU

AquiHayDeTodo. (2018, septiembre 20). Enrutamiento estatico (3 router) Packet Tracer. https://www.youtube.com/watch?v=ryf9oZy58Bo

Carlitos Tv Tutoriales. (2019, marzo 18). 1. CONFIGURACIÓN DE ROUTER Y SWITCH EN CISCO PACKET TRACER 2020. https://www.youtube.com/watch?v=gqDXPHAZ9gY

Configuración básica de un «router» Cisco. (s. f.). CCM. Recuperado 24 de noviembre de 2020, de https://es.ccm.net/faq/2759-configuracion-basica-de-un-router-cisco

Configuración básica de un Switch en Cisco. (s. f.). Solvetic. Recuperado 24 de noviembre de 2020, de https://www.solvetic.com/tutoriales/article/3711-configuracion-basica-switch-cisco/

Configuración de Servidores DNS y DHCP en Packet Tracer. (2020, mayo 3). eClassVirtual - Cursos Cisco en línea. https://eclassvirtual.com/configuracion-de-servidores-dns-y-dhcp-en-packet-tracer/

Configurar_dhcp_server_en_router.pdf. (s. f.). Recuperado 24 de noviembre

de 2020, de https://www.rafaelsantos.es/web/agora/apuntes/configurar_dhcp_server_en_router.pdf

CP CCNA2 II- 2020 16-04: Iniciar el capítulo 1. (s. f.). Recuperado 24 de noviembre de 2020, de https://lms.netacad.com/mod/lti/view.php?id=2417568

Franklin García. (2019, julio 16). Configuración de ROUTER en Packet Tracer | Switch | Interfaces | DHCP | 1/2 ✅. https://www.youtube.com/watch?v=VbRRWTMh1GA

Gabriel Marcano. (2017, julio 8). Direccionamiento IPv4 y Subredes (Explicado). https://www.youtube.com/watch?v=SHbBso63X38

InfoRed. (2017). Enrutamiento OSPF packet tracer comandos. https://www.youtube.com/watch?reload=9&v=iB6d3xmE1S0

Informática con Abaga Motu. (2020). CONFIGURACIÓN DE ENLACES TRONCALES ENTRE EN VLAN CON PACKET TRACER PASO A PASO| CÓMO CREAR VILANs. https://www.youtube.com/watch?v=k5qNn-usviY

Introducción a las redes. (s. f.). Recuperado 24 de noviembre de 2020, de https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7

mariontechacademy. (2013, noviembre 11). CS071 21.02 OSPF - Configuracion OSPF en Packet Tracer. https://www.youtube.com/watch?v=lw-IekHi9eY

MasterHeHeGar. (2013, noviembre 10). 11—VLAN (Red de Área Local Virtual) en Packet Tracer (CYERD). https://www.youtube.com/watch?v=cbN4iksKo2A

Salomon IPARRAGUIRRE RAMIREZ. (2016, noviembre 7). Configuración de los servicios WEB, DNS, DHCP, CORREO, FTP, TFTP. https://www.youtube.com/watch?v=K0lHcyV-Sdo

SEO - Blogger y Más. (2019, julio 20). Configurar Interfaces de Router en Packet Tracer. https://www.youtube.com/watch?v=BH25w-JOsl0

Un poco de todo. (2016, junio 10). CONFIGURACIÓN DE 3 ROUTERS , SERVIDORES DHCP, DNS Y WEB EN CISCO PACKET TRACER. https://www.youtube.com/watch?v=Q4ap_6yOdbg

Victor Simon Avalos Ortiz. (2012, marzo 8). VLAN - Configuración de una

Vlan—5/5. https://www.youtube.com/watch?v=_1QvnC4iEA8

VIDEOS INICIALES CISCO - OneDrive. (s. f.). Recuperado 24 de noviembre de 2020, de https://onedrive.live.com/?authkey=%21AJP1UK2X%2Dku08P0&id=483D35BEE8610962%21767&cid=483D35BEE8610962

Walton, A, ccnadesdecero . (s. f.). ▷ Cómo Configurar un Router Cisco » CCNA desde Cero. [sitio web]. (2017, noviembre 20). [Consultado 18 de septiembre de 2020]. Disponible en: https://ccnadesdecero.es/como-configurar-router-cisco/

Walton, A, ccnadesdecero . (s. f.). ▷ Guardar Configuraciones » CCNA desde Cero. CCNA desde Cero [sitio web]. (2017, juliom5). [Consultado 18 de septiembre de 2020]. Disponible en: https://ccnadesdecero.es/guardar-configuraciones/

Walton, A, ccnadesdecero . (s. f.). Configuración Inicial del Router. CCNA desde Cero. [sitio web]. (2017, noviembre 19). [Consultado 18 de septiembre de 2020]. Disponible en: https://ccnadesdecero.es/configuracion-inicial-del-router/

14. ANEXOS

Anexo A. Archivo Packet Tracer Escenario 1:
https://drive.google.com/drive/folders/1od18uchoavPQ7boLLkwyElQd3ab-Hvid?usp=sharing

Anexo B. Archivo Packet Tracer Escenario 2:
https://drive.google.com/drive/folders/1tE2B4Oal2N2-p6Cg5pv2JNJ3gt4PSYi_?usp=sharing

Anexo C. Archivo articulo Escenario 1:
https://drive.google.com/drive/folders/12cgCm4a0K5H3t32Qn2nW2Ajy4b9Fy6xD?usp=sharing