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

GABRIEL MANGONES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRONICA
COVEÑAS
2020

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

GABRIEL MANGONES TOSCANO

Diplomado de opción de grado presentado para optar el título de
INGENIERO ELECTRONICO

DIRECTOR:
DIEGO EDINSON RAMÍREZ CLAROS MASTER EN GERENCIA DE PROYECTO DE TELECOMUNICACIONES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRONICA
COVEÑAS
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Coveñas, 25 de noviembre 2020

AGRADECIMIENTOS

En primer lugar, quiero agradecer al ingeniero Wilson Arrubla, quien con mucha paciencia demostró un gran compromiso en su papel como tutor lo cual ha sido importante en mi proceso académico.

También quiero agradecer a la Universidad Nacional Abierta y a Distancia UNAD y todo su cuerpo docente que siempre han facilitado los medios necesarios para enriquecer las competencias de cada uno de nosotros los estudiantes.

Por último, agradecer a mi familia, en especial a mis padres que siempre me han apoyado en todo lo que me he propuesto.

Muchas gracias a todos.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

Pág.

GLOSARIO

D

DNS
Es la sigla que forman la denominación Domain Name System o Sistema de Nombres de Dominio y además de apuntar los dominios al servidor correspondiente, nos servirá para traducir la dirección real, que es una relación numérica denominada IP, en el nombre del dominio., 69

P

Packet Tracer
Es un programa de simulación de redes que permite a los estudiantes experimentar con el comportamiento de la red, 62

R

router
Dispositivo que permite interconectar computadoras que funcionan en el marco de una red., 63

S

SHH
Secure Shell, es un protocolo de administración remota que le permite a los usuarios controlar y modificar sus servidores remotos a través de Internet a través de un mecanismo de autenticación., 73
switch
Dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local., 67

RESUMEN

En este informe se encontrará con el desarrollo de las actividades evaluativas propuestas para la aprobación del diplomado CISCO CCNA; para este caso particular en este documento se presentan dos escenarios problemáticos relacionados con las ciencias de la electrónica y las telecomunicaciones, que tienen solución en las bases teórico-prácticas adquiridas en este diplomado.

El primer escenario que se desarrolla en este informe consiste en la interconexión de una pequeña red de datos conformada por un router, dos switchs y dos computadores, con los cuales se pretende obtener conectividad entre todos los equipos a través de los protocolos de comunicación IPV4 e IPV6 simultáneamente, soportados y administrados por interfaces virtuales de comunicación y acceso remoto a los switchs por validación de cuentas de usuarios.

Para el segundo escenario, el objetivo es configurar una segunda red de modo que tenga conectividad tanto por el direccionamiento IPv4 como el IPv6, se deben configurar seguridad basica de los switches, routing entre las VLAN, el protocolo OSPF, el protocolo DHCP, traducción de direcciones NAT, listas de control de acceso ACL y el protocolo de tiempo de red NTP.

Para el desarrollo de este ejercicio, se empleó la herramienta informática de simulación CISCO PACKET TRACER, la cual de forma muy sencilla y grafica emula un sin número de redes de datos con sus propiedades más importantes a la hora de configurarlas y ponerlas en marcha, lo cual resulta un medio muy práctico para el desarrollo de esta etapa evaluativa. Gracias a esta herramienta se pueden analizar los procesos que ocurren durante la conmutación o un enrutamiento de un mensaje transmitido a través de los dispositivos de red.

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

ABSTRACT

In this report you will find the development of the evaluation activities proposed for the approval of the CISCO CCNA diploma; For this particular case, this document presents two problematic scenarios related to the sciences of electronics and telecommunications, which have a solution in the theoretical-practical bases acquired in this diploma.

The first scenario that is developed in this report consists of the interconnection of a small data network made up of a router, two switches and two computers, with which it is intended to obtain connectivity between all the equipment through the IPV4 communication protocols and IPV6 simultaneously, supported and managed by virtual interfaces for communication and remote access to the switches by validation of user accounts.

For the second scenario, the objective is to configure a second network so that it has connectivity through both IPv4 and IPv6 addressing, basic security of the switches, routing between VLANs, the OSPF protocol, the DHCP protocol, translation of NAT addresses, ACL access control lists, and the NTP network time protocol.

For the development of this exercise, the computer simulation tool CISCO PACKET TRACER was used, which in a very simple and graphical way emulates a number of data networks with their most important properties when configuring and starting them up. which is a very practical means for the development of this evaluative stage. Thanks to this tool, it is possible to analyze the processes that occur during the switching or routing of a message transmitted through the network devices.

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

INTRODUCCIÓN

En presente informe tiene como objeto mostrar las evidencias del desarrollo y aprendizaje que el estudiante del Diplomado de Profundización CCNA ha tenido durante el curso. Para ello se han planteado dos escenarios que corresponden a la configuración de dispositivos de red y sus respectivas pruebas de conectividad mediante el uso de comandos especializados para los procesos de verificación.

Teniendo en cuenta la naturaleza de los ejercicios propuestos, se deben implementar como soporte de la actividad herramientas de simulación como Packet Tracer o GNS3 en este caso usaremos Packet Tracer.

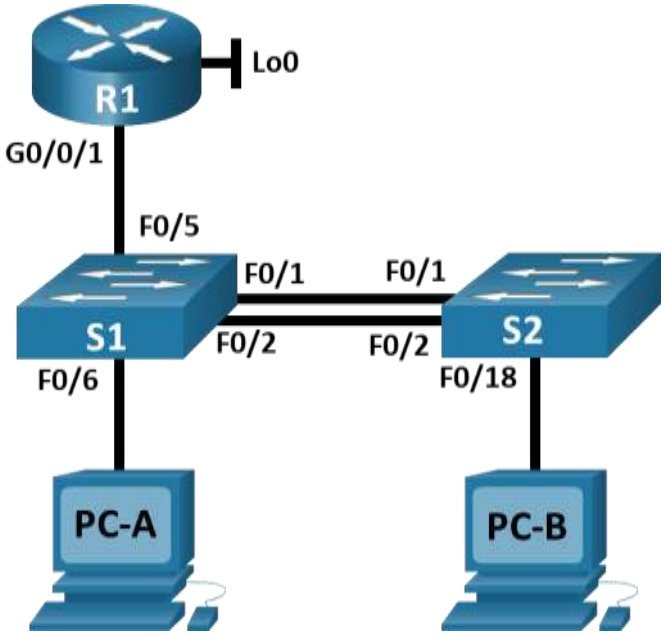
En este primer escenario se solicita al estudiante configurar una pequeña red que incluye un router, un switch que admitan tanto la conectividad IPv4 e IPv6 para los hosts soportados con la configuración de una administración segura tanto para el router como para el switch.

Para el segundo escenario también se debe configurar una red con conectividad IPv4 e IPv6 además de la seguridad de los switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo DHCP, la traducción de direcciones de red dinámicas y estáticas, listas de control de acceso y el protocolo de tiempo de red (NTP) servidor/cliente.
Veamos entonces el desarrollo de esta prueba.

DESARROLLO

1. ESCENARIO 1

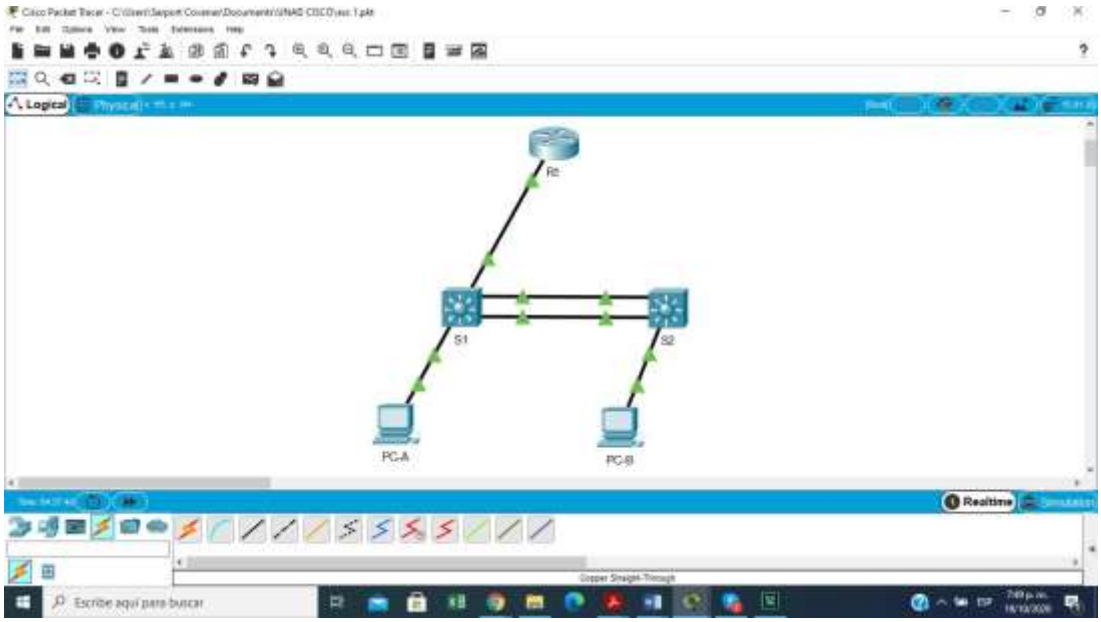
Figura 1. Escenario 1



Fuente: Autor

Para el escenario mostrado en la figura 1, se muestra la topologia de la red en la que se realizarán la configuracion de los dispositivos. Configuraremos un router, dos switchs y dos computadores que admitan conexion IPv4 como IPv6. El router los switchs se deben administrarse de forma remota segura, se configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Figura 2. Simulación de escenario 1



Fuente: Autor

Tabla 1. Listado de VLAN

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

Tabla 2. Asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
R1 G0/0/1.2	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
R1 G0/0/1.3	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
R1 G0/0/1.4	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
R1 Loopback0	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
VLAN S1 4	2001:db8:acad:c: :98 /64	No corresponde
S1 VLAN 4	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
S2 VLAN 4	2001:db8:acad:c: :99 /64	No corresponde
S2 VLAN 4	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-A NIC	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-B NIC	2001:db8:acad:b: :50 /64	fe80::1

La tabla anterior nos muestra el direccionamiento que se debe implementar en cada uno de los dispositivos de la red.

1.1 INICIALIZACIÓN, RECARGAR Y CONFIGURACIÓN BÁSICA DE LOS DISPOSITIVOS:

- Borrar las configuraciones de inicio y las VLAN del router y del switch y volver a cargar los dispositivos.

- Después de recargar el switch, configurar la plantilla SDM para que admita IPv6 según sea necesario y vuelver a cargar el switch.

Para la primera solicitud debemos ingresar al modo de configuración privilegiado para realizar tanto en el router como en los dos switchs la ejecución de los comandos para borrar las configuraciones previas, borrar el archivo vlan.dat, luego en el modo de configuracion global en los switchs configuraremos la plantilla SDM para dire ciones IPV4 e IPV6; seguidamente el comando para reiniciar el dispositivo, estos tres comandos se encuentran en las siguientes tablas:

Router:

Tabla 3. Comandos para reinicializar el router

Tarea	comando
Entrar el modo privilegiado	Router>enable
Borrar la configuracion de inicio	Router#erase startup-config
Borrar las VLANS anterriormente creadas	Router#delete vlan.dat
Reiniciar el Router	Router#reload

Con los comandos realizados el router queda libre de configuraciones previas y listo para realizar las configuraciones solicitadas en el escenario.

Tabla 4. Comandos para reinicializar los switchs y configurar la plantilla SDM para direccionamiento ipv6 e IPV4.

Tarea	comando
Entrar el modo privilegiado	Switch>enable
Borrar la configuracion de inicio	Switch#erase startup-config
Borrar las VLANS anterriormente creadas	Switch#delete vlan.dat
Entrar al modo de configuracion global	Switch#configure terminal
Configuracion de la plantilla SDM para que admita direccionamientoIPV4 e IPv6	Switch(config)#sdm prefer dual-ipv4-and-ipv6 default

Tarea	comando
Reiniciar el Switch	Switch#reload

La tabla numero 4, nos muestra los pasos realizados en la CLI de los siwtchs para borrar configuraciones previas y Vlans antes creadas, ademas nos muestra como se realizó la activacion de la plantilla SDM para admitir direccionamiento IPV4 e IPV6.

1.2 CONFIGURAR R1

En este paso se realizan en el router las configuraciones básicas como la desactivación de la búsqueda por DNS, el nombre del dispositivo, el dominio, mensajes del día y las contraseñas para el modo de ejecución y el modo privilegiado con el cifrado de las claves.

También se realiza la configuración de inicio de sesión en líneas VTY que solo acepten el protocolo de administración remota SSH, validadas por usuario y contraseña de mínimo 10 caracteres, ambos registrados en la base local del dispositivo.

Por último, se configurará la interface G0/0/1 dividida en 4 subinterfaces con conexión ipv4 e ipv6.

Para poder realizar los siguientes comandos, se requiere que al menos nos encontremos ubicados dentro del modo privilegiado, a partir del cual se generaran las demás configuraciones.

Tabla 5. Configuraciones iniciales para el router

Tarea	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router “R1”	Router(config)#hostname R1
Nombre de dominio “ccna-lab.com”	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado “ciscoenpass”	R1(config)#enable secret ciscoenpass

Tarea	Especificación
Contraseña de acceso a la consola “ciscoconpass”	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas “10 min”	R1(config)#security password min-length 10
Crear un usuario administrativo en la base de datos local “user:admid”, “Key: admin1pass”	R1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 15 R1(config-line)#login local
Configurar VTY solo aceptando protocolo “SSH”	R1(config-line)#transport input ssh R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner: “Pribibido el acceso al personal no autorizado”	R1(config)#banner motd #Pribibido el acceso al personal no autorizado#
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing

Tarea	Especificación
Configurar interfaz G0/0/1 Activar la interface física Configurar interfaz G0/0/1.2, G0/0/1.3, G0/0/1.4: Encapsular la vlan correspondiente, poner descripción de que la identifica, asignar direcciones ip e ipv6, poner fe80::1 como el link local, levantar la interface, salir de la subinterface. Configurar interfaz G0/0/1.6 Encapsular la vlan correspondiente, poner descripción de que la identifica, levantar la interface, salir de la subinterface.	R1(config)#int g0/0/1 R1(config-if)#no shut R1(config)#exit R1(config)#int g0/0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description vlan2 R1(config-subif)#ip address 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:DB8:ACAD:A::1/64 R1(config-subif)#ipv6 address FE80::1 link-local R1(config-subif)#no shut R1(config-subif)#exit R1(config)#int g0/0/1.3 R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#description vlan3 R1(config-subif)#ip address 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:DB8:ACAD:B::1/64 R1(config-subif)#ipv6 address FE80::1 link-local R1(config-subif)#no shut R1(config-subif)#exit R1(config-subif)#int g0/0/1.4 R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#description vlan4 R1(config-subif)#ip address 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:DB8:ACAD:C::1/64 R1(config-subif)#ipv6 address FE80::98 link-local R1(config-subif)#no shut R1(config-subif)#exit R1(config-subif)#int g0/0/1.6 R1(config-subif)#encapsulation dot1q 6 R1(config-subif)#description vlan6 R1(config-subif)#no shut R1(config-subif)#exit

Tarea	Especificación
Configure el Loopback0 interface: Entrar a la interface, asignar dirección de bucle ipv4 e ipv6, asignar fe80::1 como link local, salir de la interface.	R1(configf)#int Loopback0 R1(config-if)#ip route 0.0.0.0 0.0.0.0 Loopback0 R1(config)#ipv6 route 0:0:0:0:0:0:0:0/0 Loopback0 R1(config-if)#ipv6 add fe80::1 link-local R1(config-if)#exit
Generar una clave de cifrado RSA, escoger 1024 bits para el modulo.	R1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024

Con la ejecucion de los pasos de la tabla 5, hasta el momento tenemos en el router 1 configurado acceso protegido a la consola, lineas VTY y al modo de configuracion privilegiado con encryptacion de las claves y la comunicación SSH. Se ha subdividido la interface giga 0/0/1 en 4 subintterface ya configuradas con direccionamiento y Vlans asignadas. Se creó la interface loopback 0, se asigno R1 como nombre del host, se creó un nombre de dominio al dispositivo, se desactivo la busqueda por DNS, mensaje de bienvenida y se creó un usuario en la base local para el acceso remoto.

1.3 CONFIGURACIÓN DE S1 y S2

Los pasos para la configuración de los switchs son muy parecidos a los realizados en el router, se debe desactivar la búsqueda por DNS, nombrar el equipo, asignarle un nombre de dominio para hacer control de seguridad por medio SHH, se asignarán contraseñas para el modo de ejecución y el privilegiado, también se creará un usuario administrativo y su contraseña en la base local del switch para validación remota por las conexiones SSH que se habilitaran. Se encriptarán las contraseñas no cifradas y se creará una llave rsa para el acceso por las vty.

Tabla 6. Configuraciones iniciales para el Switch 1

Tarea Par S1	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch#conf t Switch(config)#no ip domain-lookup
Nombre del switch “S1”	Switch(config)#hostname S1
Nombre de dominio “ccna-lab.com”	S1(config)#ip domain-name ccna-lab.com

Tarea Par S1	Especificación
Contraseña cifrada para el modo EXEC privilegiado “ciscoenpass”	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola “ciscoconpass”	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login
Crear un usuario administrativo en la base de datos local “username: admin” “password: admin1pass”	S1(config-line)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Configurar un MOTD Banner “probibido el acceso al personal no autosrizado”	S1(config)#banner motd #probibido el acceso al personal no autosrizado#
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024
Configurar la interfaz de administración (SVI), asignar direcciones ip e ipv6, asignar a fe80::98 como link local, activar la interface.	S1(config)#int vlan 4 S1(config-if)#ip add 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 add 2001:db8:acad:c::98/64 S1(config-if)#ipv6 add fe80::98 link-local S1(config-if)#no shut
Configuración del gateway predeterminado a la interface Vlan 4 y salir de ella.	S1(config-if)#ip default-gateway 10.19.8.97 S1(config-if)#exit

Del uso de los comandos de la tabla 6, se han configurado en el switch 1, el nombre del host, el nombre de dominio, la desactivacion de la busqueda por DNS y el mensaje de bienvenida. Quedaron encriptadas las contraseñas creadas para los accesos a consola, modo privilegiado y lineas VTY. Se creo el m ismo usuario local creado en el router 1 y se configuró la interface administrativa en la VLAN 4.

Tabla 7. Configuraciones iniciales para el Switch 2

Tarea Para S2	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch#conf t Switch(config)#no ip domain-lookup
Nombre del switch “S2”	Switch(config)#hostname S2
Nombre de dominio “ccna-lab.com”	S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado “ciscoenpass”	S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola “ciscoconpass”	S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login
Crear un usuario administrativo en la base de datos local “username: admin” “password: admin1pass”	S2(config-line)#username admin password admi1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 15 S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S2(config-line)#service password-encryption
Configurar un MOTD Banner “probibido el acceso al personal no autosrizado”	S2(config)#banner motd #probibido el acceso al personal no autosrizado#
Generar una clave de cifrado RSA	S2(config)#crypto key generate rsa How many bits in the modulus [512]: 1024
Configurar la interfaz de administración (SVI), asignar direcciones ip e ipv6, asignar a fe80::98 como link local, activar la interface.	S2(config)#int vlan 4 S2(config-if)#ip add 10.19.8.99 255.255.255.248 S2(config-if)#ipv6 add 2001:db8:acad:c::99/64 S1(config-if)#ipv6 add fe80::99 link-local S1(config-if)#no shut
Configuración del gateway predeterminado a la interface Vlan 4 y salir de ella.	S1(config-if)#ip default-gateway 10.19.8.97

En el switch 2, se realizan configuraciones similares que en el switch 1, la diferencia radica en la interface administrativa para este switch, la cual debe tener un direccionamiento distinto al switch 1 como se puede notar en la tabla 7.

1.4 CONFIGURACIÓN DE LA INFRAESTRUCTURA DE RED (VLAN, TRUNKING, ETHERCHANNEL)

Comenzamos configurando a S1, en este paso crearemos 5 vlan cada uno con un nombre distintivos la cuales se conectarán a las respectivas subinterfaces creadas en el router. En este switch se deben configurar tres puertos como troncales, el f0/1, f0/2 y el f0/5 porque por ellos circularan información de varias vlans rumbo hacia el router. Como los puertos f0/1 y f0/2 están conectados en paralelo entre el mismo par de dispositivos, estos se configurarán como un canal único formando un EtherChannel, el cual mejora el ancho de banda entre los switchs y además brinda redundancia de soporte.

Se habilitará también el canal de acceso para el PC-A a través de la vlan 2 por el puerto f0/6 y se asignará seguridad al puerto protegiendo el acceso no autorizado a un máximo de 3 equipos diferentes. El resto de interface no utilizadas se agruparán en una vlan y se protegerá el acceso apagando esos puertos.

Tabla 8. Configuraciones puertos, troncales y Vlans en el Switch 1

Tarea	Especificación
Crear 5 VLAN y asignarles un nombre a cada una	S1(config-vlan)#vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#vlan 4 S1(config-vlan)#name management S1(config-vlan)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#vlan 6 S1(config-vlan)#name Native

Tarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 6 nativa en los puertos f0/1, f0/2 y f0/5	S1(config)#int r f0/1,f0/2,f0/5 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 6 S1(config-if-range)#switchport mode trunk
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 y utilicen el protocolo LACP	S1(config)#int r f0/1,f0/2 S1(config-if-range)#channel-protocol lacp S1(config-if-range)#channel-group 1 mode active
Configurar el puerto de acceso del host PC-A para VLAN 2 por el puerto f0/6	S1(config)#int f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 S1(config-if)#no shut
Configurar la seguridad del puerto f0/6 para permitir la conexión de máximo 3 dispositivos diferentes	S1(config)#int f0/6 S1(config-if)#switchport port-security maximum 3 S1(config-if)#end
Proteja todas las interfaces no utilizadas, agrupándolas en una vln, y apagando todos esos puertos.	S1(config)#int r f0/3-4,f0/7-24, g0/1-2 S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description APAGADAS S1(config-if-range)#shutdown

De la informacion suministrada en la tabla numero 8, podemos ver que en el switch 1 se han configurado las VLANS que segmentarán la red y se han asignado los puertos por los cuales se permitirá el acceso a dichas VLANS. Así mismo se han creado de acuerdo a la topologia inicial los puertos troncales y de acceso necesarios para el correcto funcionamiento de la red incluido la agrupacion del puerto F0/1 y f0/2 en un etherchannel. Se asignó al puerto de acceso fa0/6 seguridad de puerto por rebosamiento de 3 direcciones MAC maximo. Los puertos no utilizados se asignaron a la VLAN 5 y se apagaron.

Seguimos ahora con la configuración en el S2, crearemos las mismas vlan en este switch con los mismos nombres que en S1; también agruparemos los puertos f0/1 y f0/2 en el Etherchannel; a diferencia de S1 en este switch solo se configurará como troncal los puertos f0/1 y f0/2 porque en este caso el puerto f0/5 no se está utilizando. Otra diferencia es que el puerto de acceso al host PC-B se configura en el f0/18 pero si se configurará la seguridad del puerto a máximo tres dispositivos diferentes para conectar; el resto de las interfaces también serán agrupadas y apagadas para protegerlas.

Tabla 9. Configuraciones puertos, troncales y Vlans en el Switch 2

Tarea	Especificación
Crear 5 VLAN y se les asigna nombres a cada una de ellas.	S2(config-vlan)#vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#vlan 4 S2(config-vlan)#name management S2(config-vlan)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#vlan 6 S2(config-vlan)#name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa en los puertos f0/1 y f0/2	S2(config)#int r f0/1,f0/2 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 6 S2(config-if-range)#switchport mode trunk
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 para consolidar el canal en los dos extremos en cada switch.	S2(config)#int r f0/1,f0/2 S2(config-if-range)#channel-protocol lacp S2(config-if-range)#channel-group 1 mode passive
Configurar el puerto f0/18 de acceso de host para VLAN 3 y levantar la interface.	S2(config)#int f0/18 S(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#no shut
Configurar la seguridad del puerto en el puerto de acceso f0/18 a máximo 3 equipos diferentes que puedan conectarse.	S2(config)#int f0/18 S2(config-if)#switchport port-security maximum 3 S2(config-if)#end
Proteja todas las interfaces no utilizadas agrupándolas en una vlan no utilizada y apagar esas interfaces.	S2(config)#int r f0/3-17,f0/19-24, g0/1-2 S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description APAGADAS S2(config-if-range)#shutdown

En el paso anterior quedó configurado en el switch 2, las mismas VLANS creadas en el switch 1 con sus respectivos puertos asignados tanto los de acceso con su seguridad por rebosamiento de 3 direcciones MAC maximo, como los troncales en este caso el etherchannel. Igualmente se asignaron a la VLAN 5 los puertos no utilizados y se apagaron.

1.5 CONFIGURAR SOPORTE DE HOST

En esta parte se configurará una ruta de acceso a la interface de loopback con la versión ipv4 e ipv6; seguidamente se configurarán los servicios DHCP para la vlan 2 y la vlan 3, donde se excluyan todas las direcciones IP excepto las 10 últimas del segmento de red.

Para determinar las direcciones de red de las vlan 2 y 3 se realizó la operación and en los octetos binarios de la dirección IP y la máscara del estas vlan y del resultado se obtuvieron los nuevos octetos y se llevaron a notación decimal.

Tabla 10. Configuraciones para loopback0 y servicios DHCP

Tarea	Especificación
Configure Default Routing hacia el loopback	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route 0:0:0:0:0:0:0:0/0 loopback 0
Configurar DHCP IPv4 para VLAN 2, con nombre de dominio “ccna-a.net” establecemos la red de la vlan con su máscara, excluimos las direcciones IP desde la del Gateway hasta dejar disponible solo 10 direcciones.	R1(config)#ip dhcp pool ccna-a.net R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#exit R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#exit
Configurar DHCP IPv4 para VLAN 3, con nombre de dominio “ccna-b.net” establecemos la red de la vlan con su máscara, excluimos las direcciones IP desde la del Gateway hasta dejar disponible solo 10 direcciones	R1(config)#ip dhcp pool ccna-b.net R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(dhcp-config)#exit R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.85 R1(config)#exit

Hasta el momento queda configurado las rutas estaticas hacia el loopback 0, y queda activo el servicio DHCP para la red 10.19.8.0 de la VLAN 2 y para la red 10.19.8.64 de la VLAN 3, cada una queda configurada para excluir las primeras direcciones disponibles dejando solo las diez ultimas direcciones el servicio DHCP.

1.6 CONFIGURAR LOS SERVIDORES

Los equipos PC-A y PC-B serán configurados para usar DHCP para las direcciones IPv4 y se le asignará manualmente la dirección IPv6 y el Link Local. Después de configurar cada servidor, registre las configuraciones de red del host con el comando **ipconfig /all**.

Tabla 11. Configuración de red para el PC-A

Configuración de red de PC-B	
Descripción	*PC-B*
Dirección física	*0001.C989.74E0*
Dirección IP	*10.19.8.85*
Máscara de subred	*255.255.255.224*
Gateway predeterminado	*10.19.8.65*
Gateway predeterminado IPv6	*2001:DB8:ACAD:B::1*

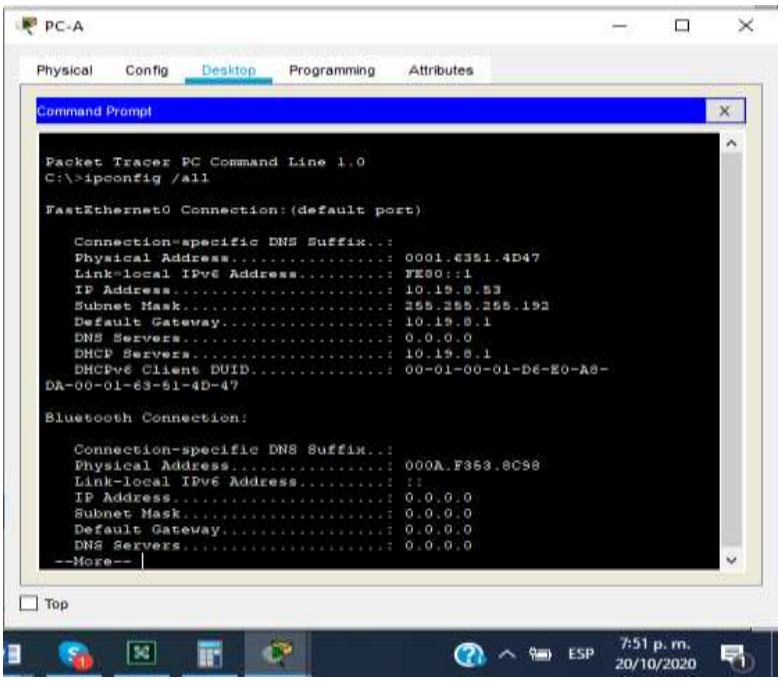
Hemos configurado el direccionamiento del PC-A para su respectivo acceso a la red.

Tabla 12. Configuración de red para el PC-B

PC-A Network Configuración	
Descripción	*PC-A*
Dirección física	*0001.6351.4D47*
Dirección IP	*10.19.8.53*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	*2001:DB8:ACAD:A::1*

Ahora se ha configurado el direccionamiento del PC-B para su permitirle el acceso a la red.

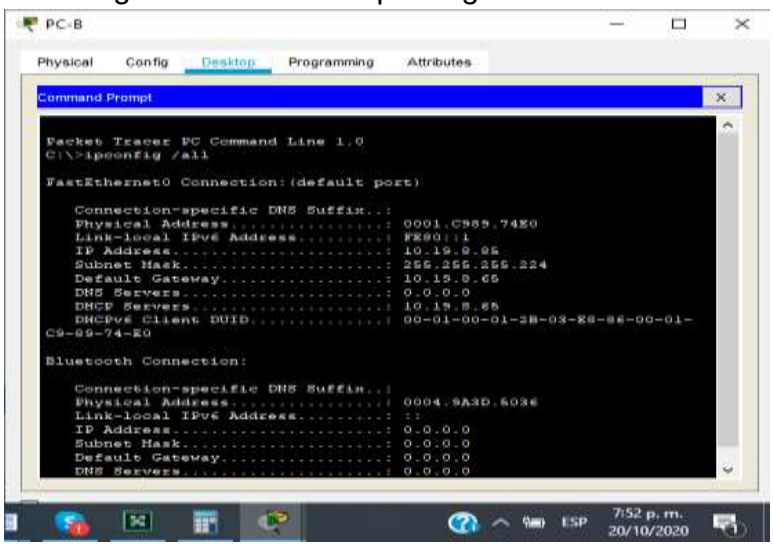
Figura 3. Comando ipconfig /all en el PC-A



Fuente: Autor

La imagen muestra la verificacion en la consola del PC-A de su direccionamiento

Figura 4. Comando ipconfig /all en el PC-B



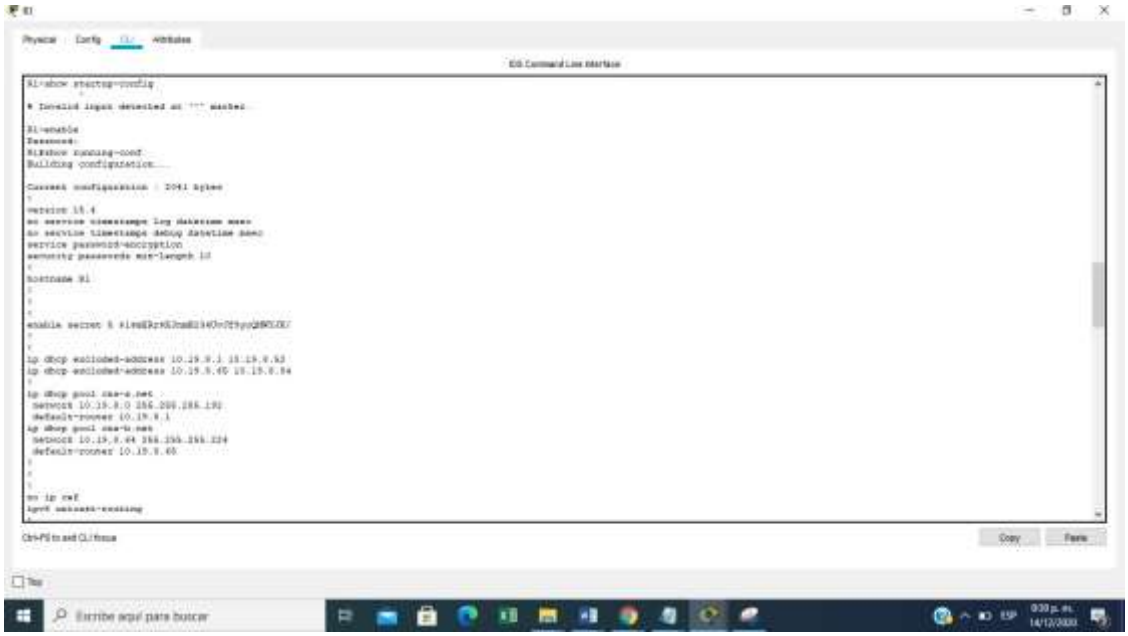
Fuente: Autor

La imagen 4 muestra la verificacion en la consola del PC-B de su direccionamiento

1.7 RESUMEN DE LAS CONFIGURACIONES DE TODOS LOS DISPOSITIVOS DEL ESCENARIO 1

En las siguienes imágenes veremos en aglomerado de comandos y configuraciones implementados en cada uno de los dispositivos de la red.

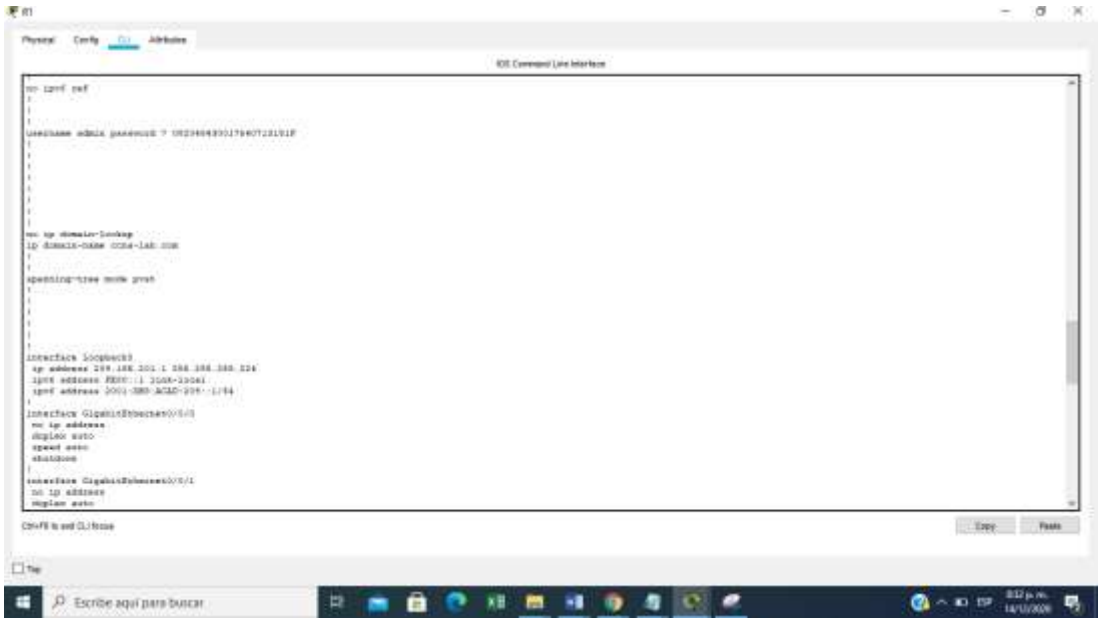
Figura 5. Configuraciones en R1 primera parte



Fuente: Autor

La figura 5 muestra la priemera de 4 imágenes de la configuracion del router 1

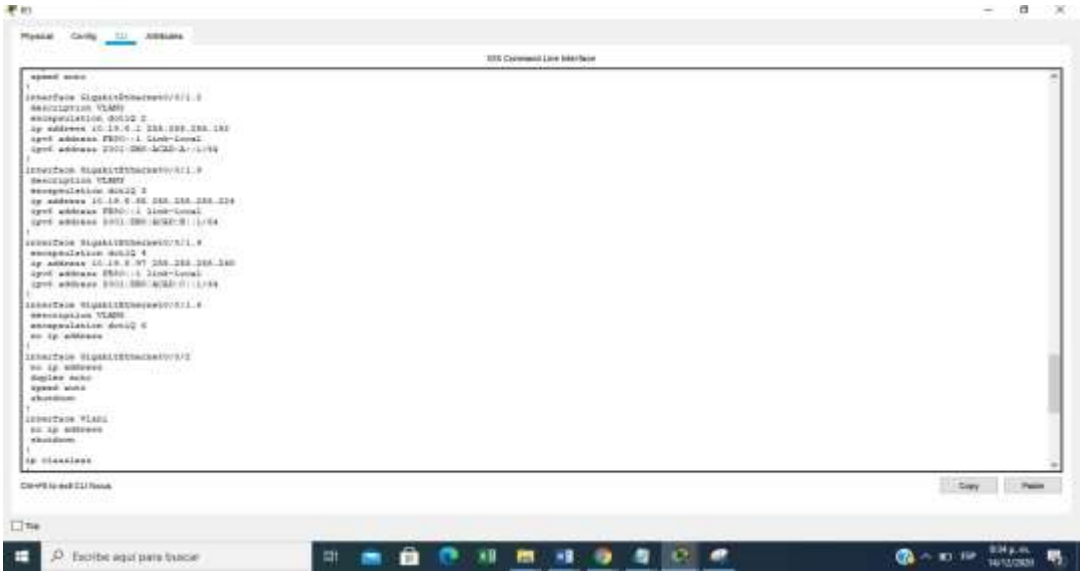
Figura 6. Configuracion en R1 segunda parte



Fuente: Autor

La figura 6 muestra la segunda de 4 imágenes de la configuracion del router 1

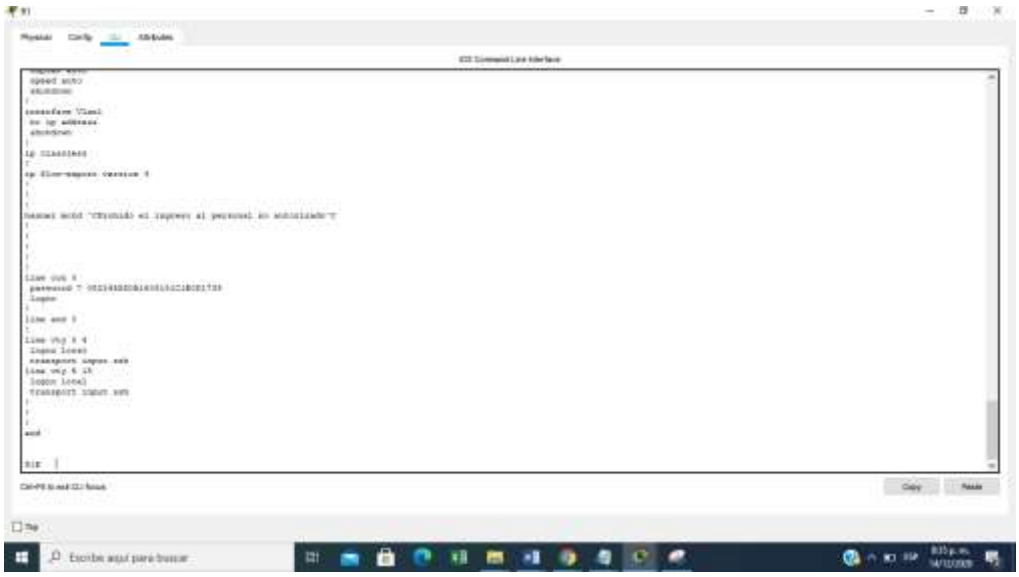
Figura 7. Configuracion en R1 tercera parte



Fuente: Autor

Se muestra la tercera de 4 imágenes de la configuracion del router 1

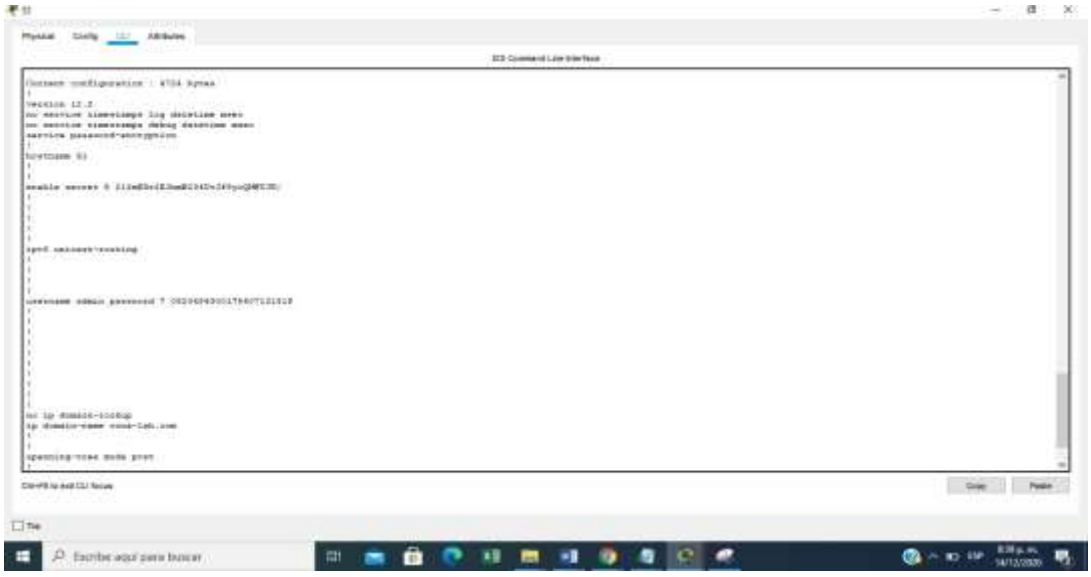
Figura 8. Configuracion en R1 cuarta parte



Fuente: Autor

Se muestra la cuarta de 4 imágenes de la configuracion del router 1

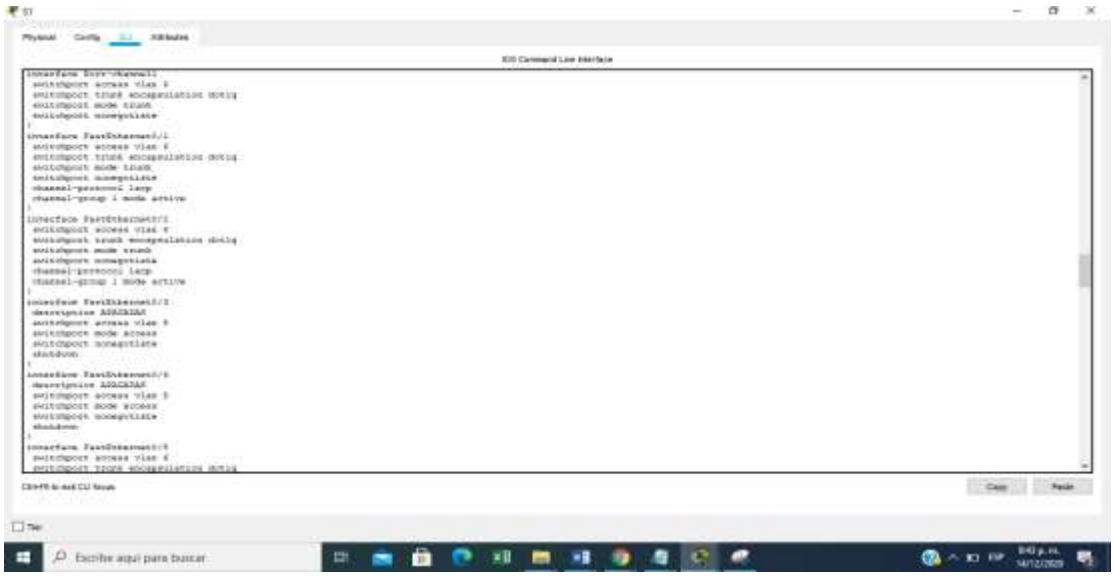
Figura 9. Configuracion de S1 Primera parte



Fuente: Autor

La figura muestra la primera de 8 imágenes de la configuracion en S1

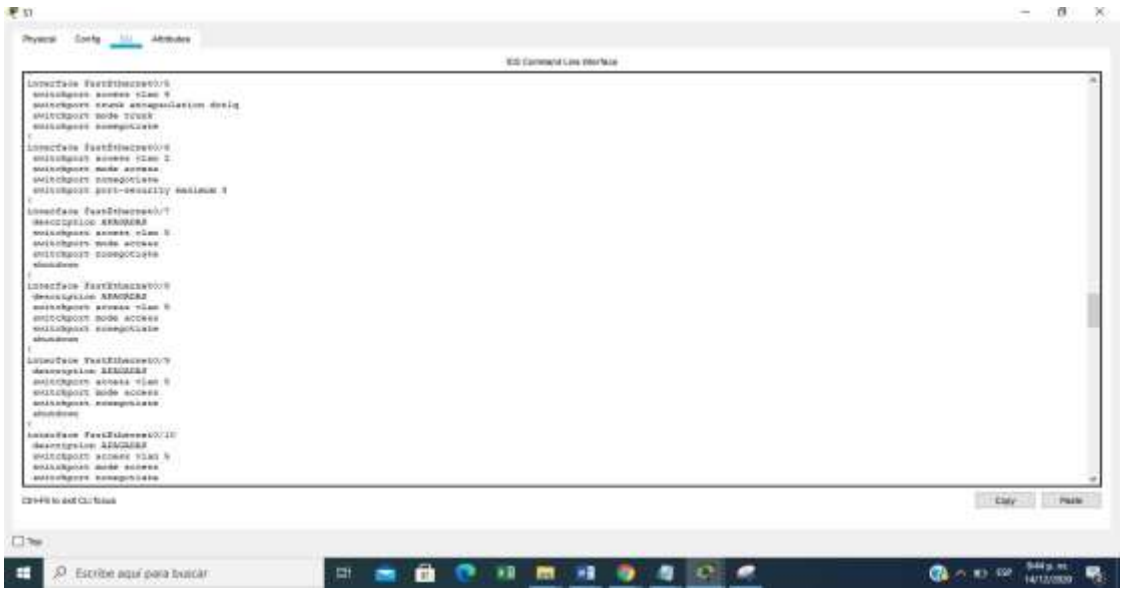
Figura 10. Configuracion de S1 segunda parte



Fuente: Autor

La figura muestra la segunda de 8 imágenes de la configuracion en S1

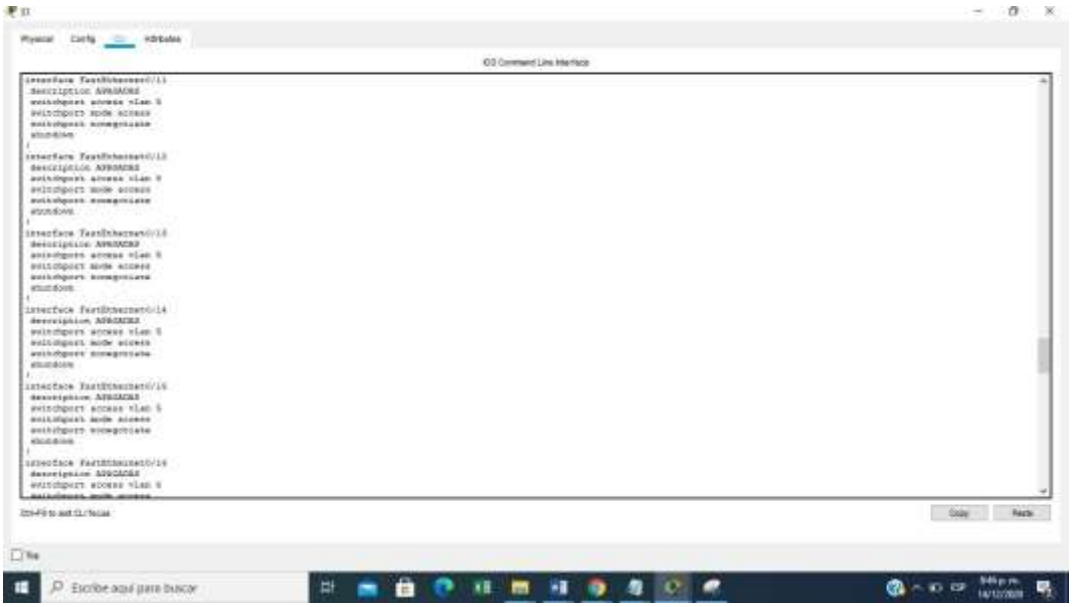
Figura 11. Configuracion de S1 tercera parte



Fuente: Autor

La figura muestra la tercera de 8 imágenes de la configuracion en S1

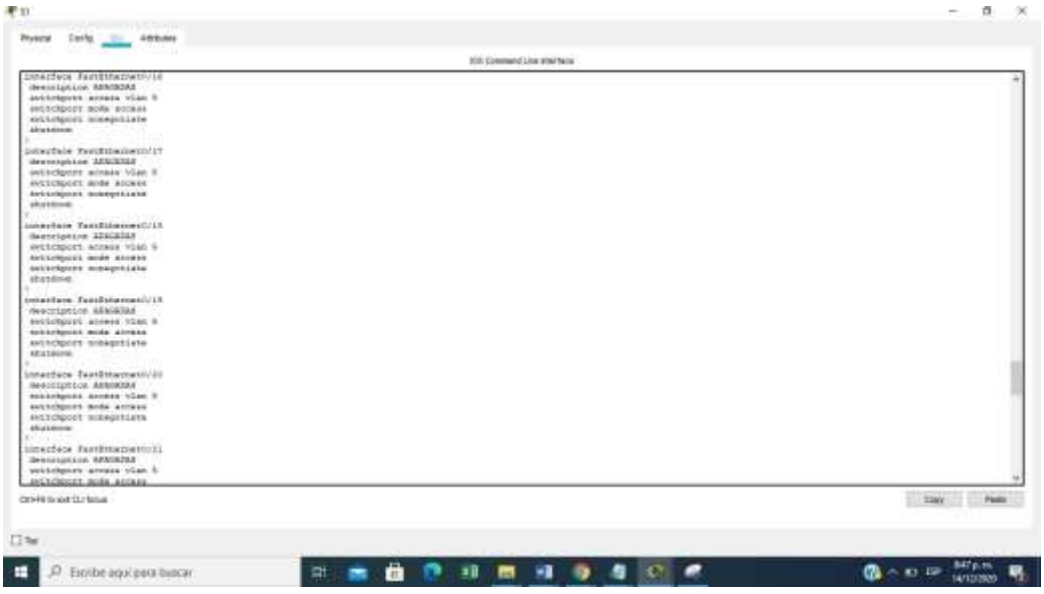
Figura 12. Configuracion de S1 cuarta parte



Fuente: Autor

La figura muestra la cuarta de 8 imágenes de la configuracion en S1

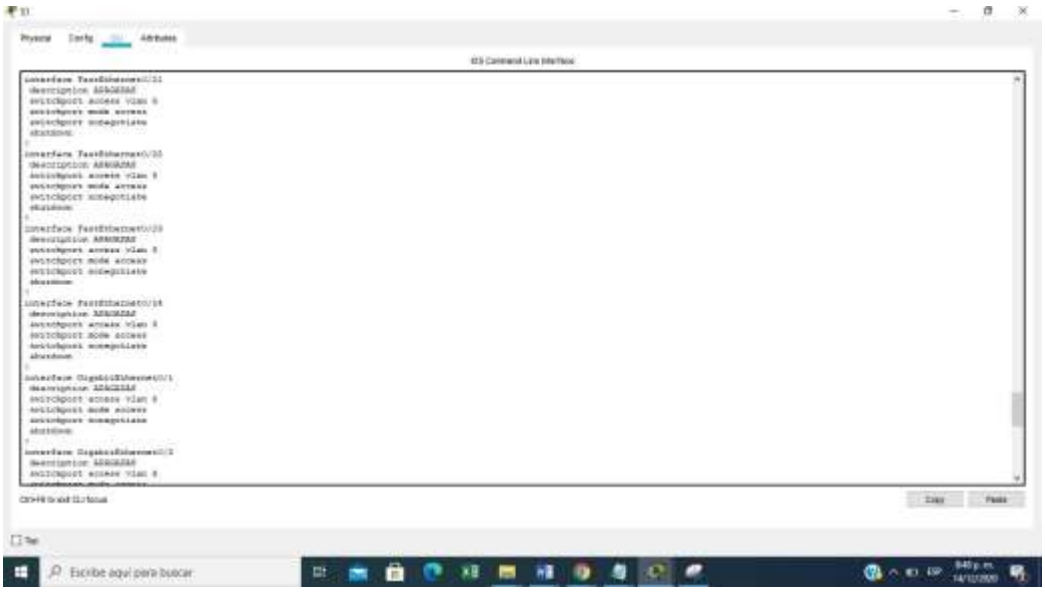
Figura 13. Configuracion de S1 quinta parte



Fuente: Autor

La figura muestra la quinta de 8 imágenes de la configuracion en S1

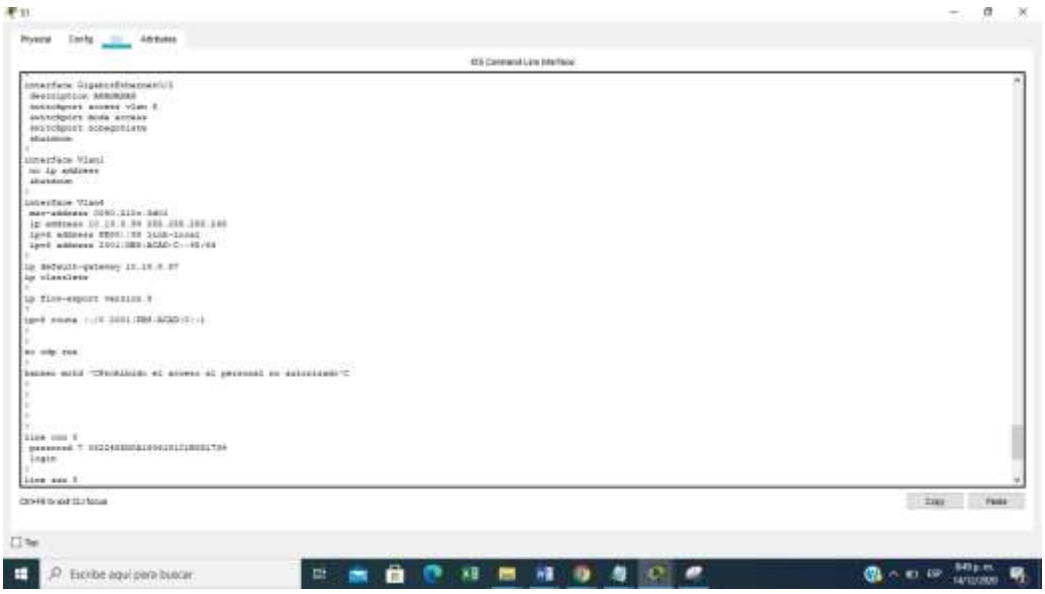
Figura 14. Configuracion de S1 sexta parte



Fuente: Autor

La figura muestra la sexta de 8 imágenes de la configuracion en S1

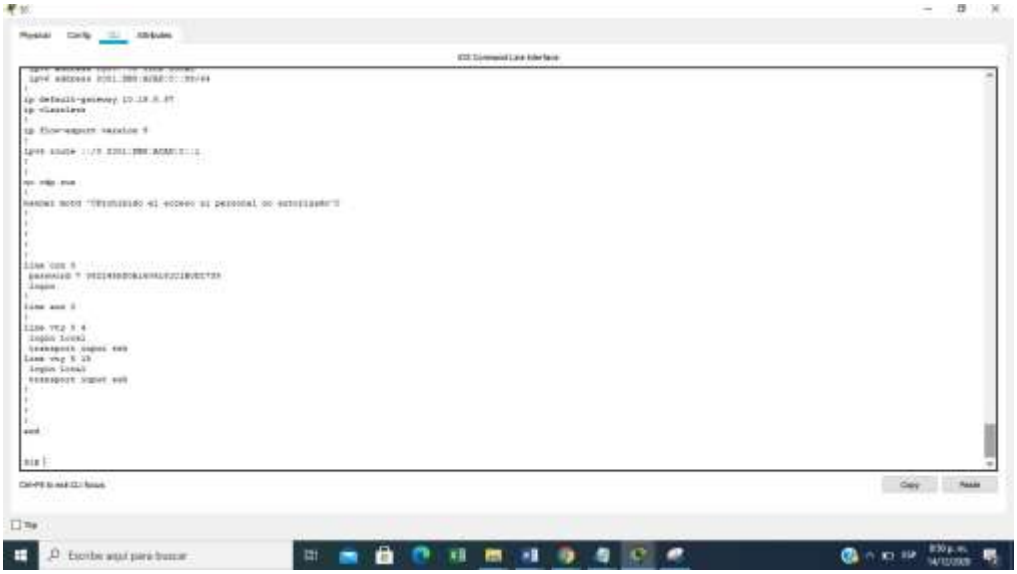
Figura 15. Configuracion de S1 septima parte



Fuente: Autor

La figura muestra la septima de 8 imágenes de la configuracion en S1

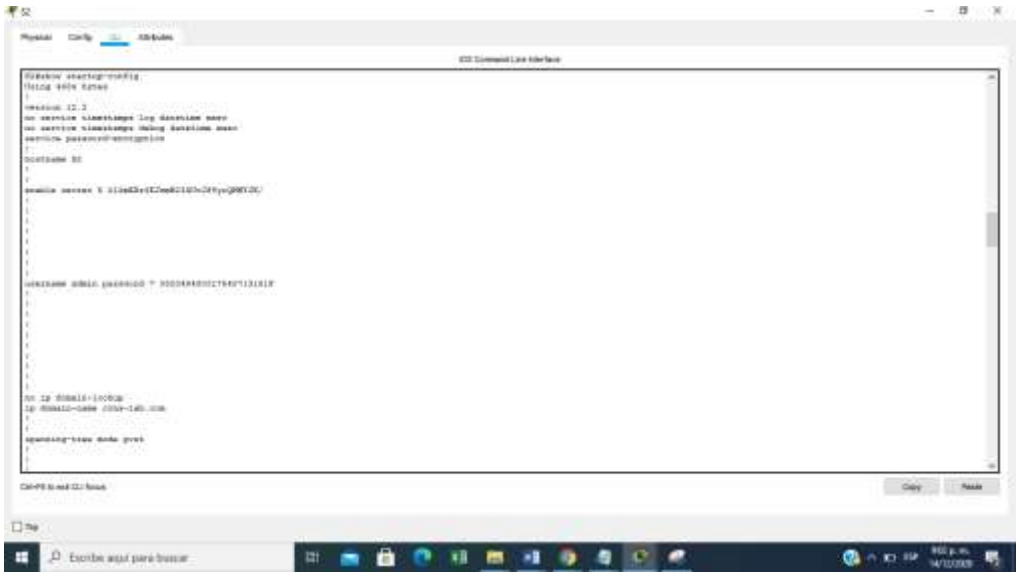
Figura 16. Configuracion de S1 octava parte



Fuente: Autor

La figura muestra la octava de 8 imágenes de la configuracion en S1

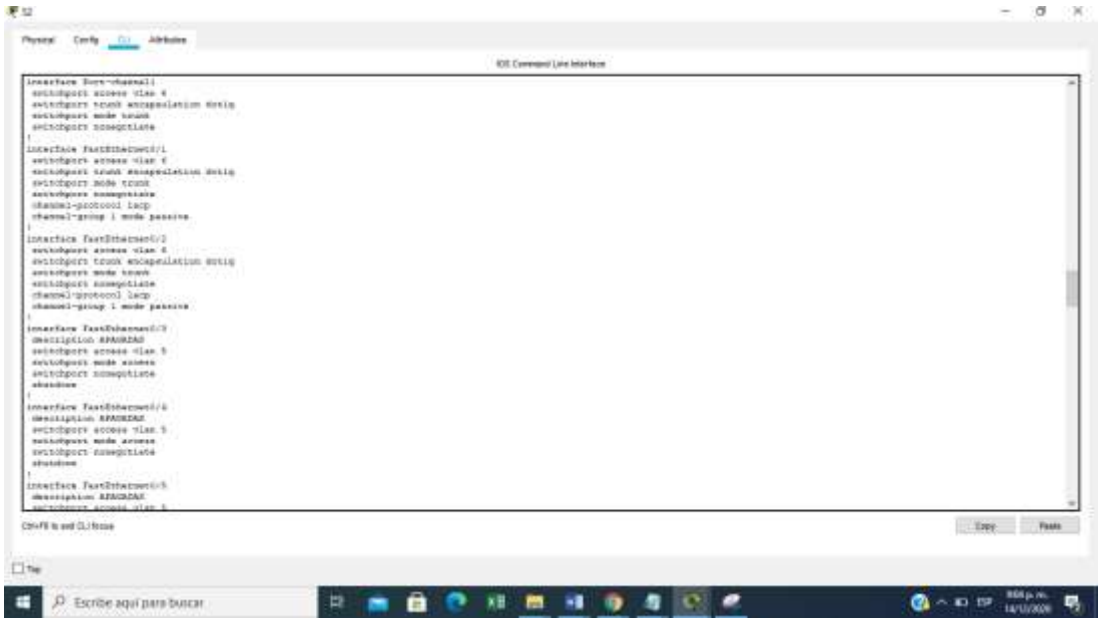
Figura 17. Configuracion de S2 Primera parte



Fuente: Autor

La figura muestra la primera de 8 imágenes de la configuracion de S2

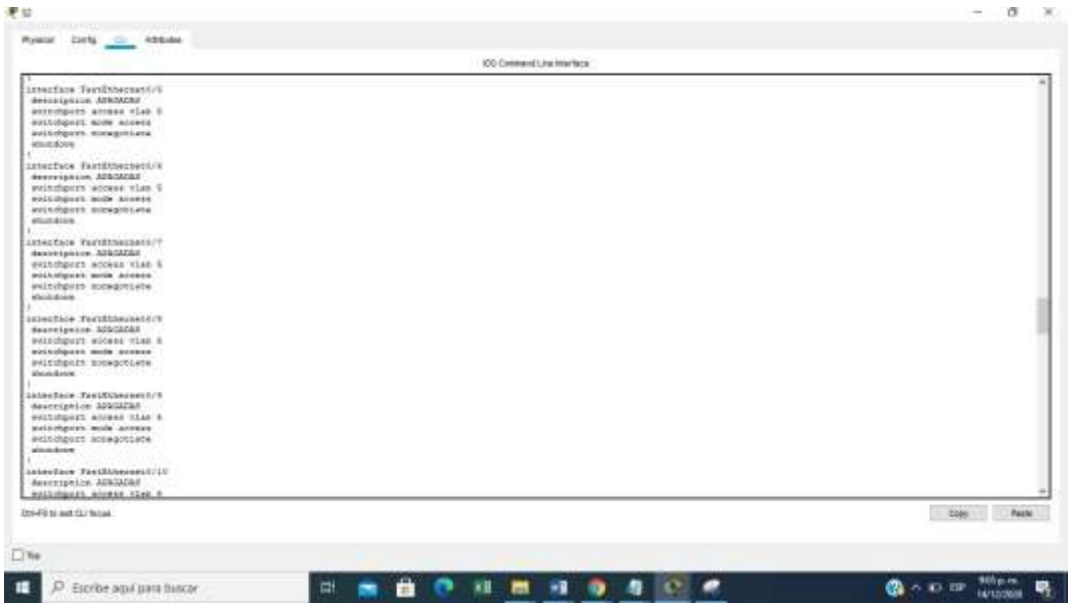
Figura 18. Configuracion de S2 segunda parte



Fuente: Autor

La figura muestra la segunda de 8 imágenes de la configuracion de S2

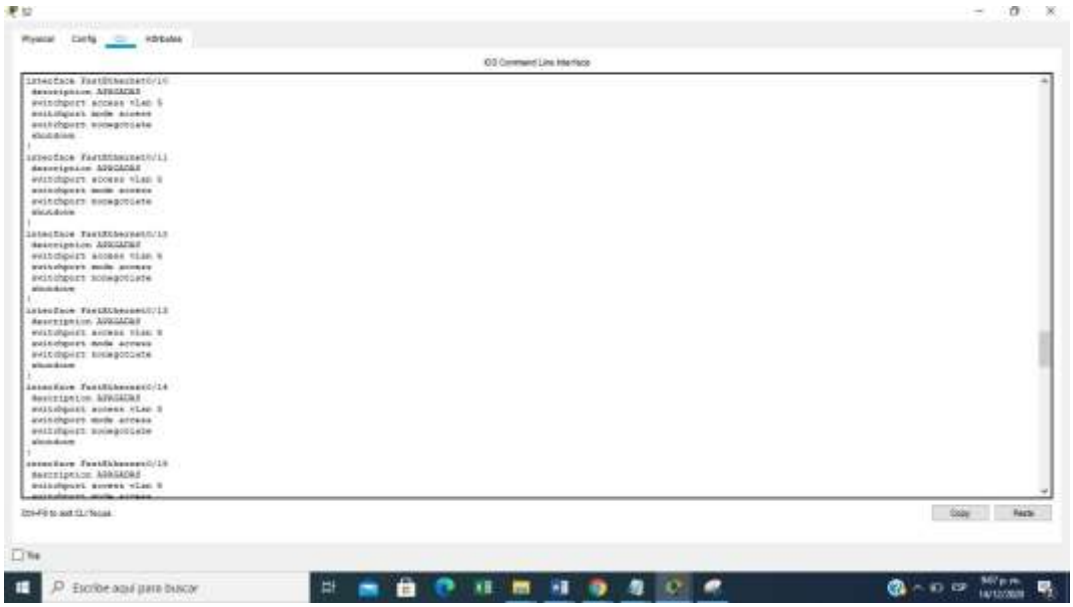
Figura 19. Configuracion de S2 tercera parte



Fuente: Autor

La figura muestra la tercera de 8 imágenes de la configuracion de S2

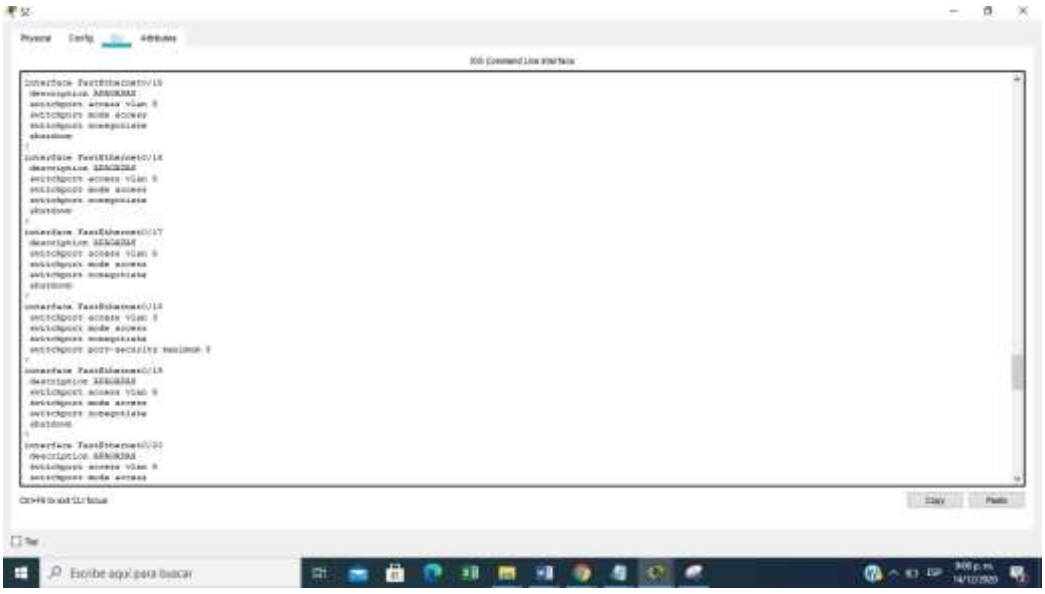
Figura 20. Configuracion de S2 cuarta parte



Fuente: Autor

La figura muestra la cuarta de 8 imágenes de la configuracion de S2

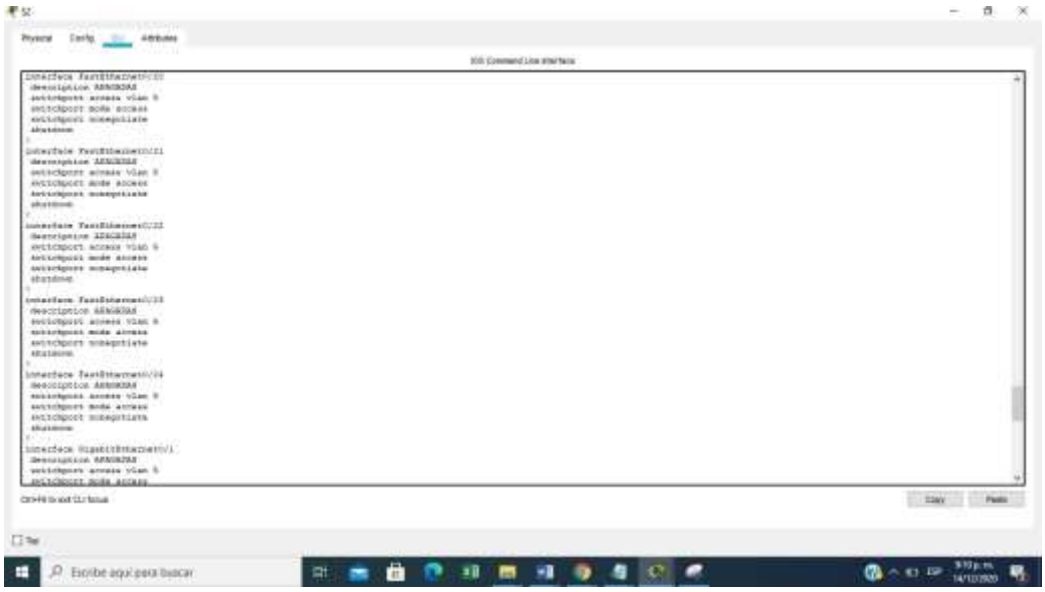
Figura 21. Configuracion de S2 quinta parte



Fuente: Autor

La figura muestra la quinta de 8 imágenes de la configuracion de S2

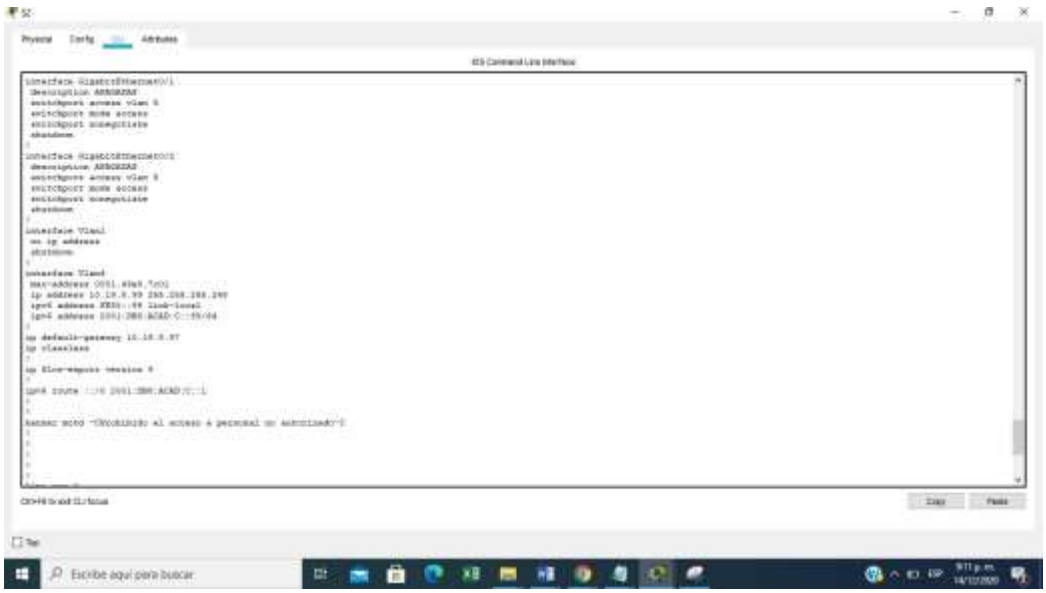
Figura 22. Configuracion de S2 sexta parte



Fuente: Autor

La figura muestra la sexta de 8 imágenes de la configuracion de S2

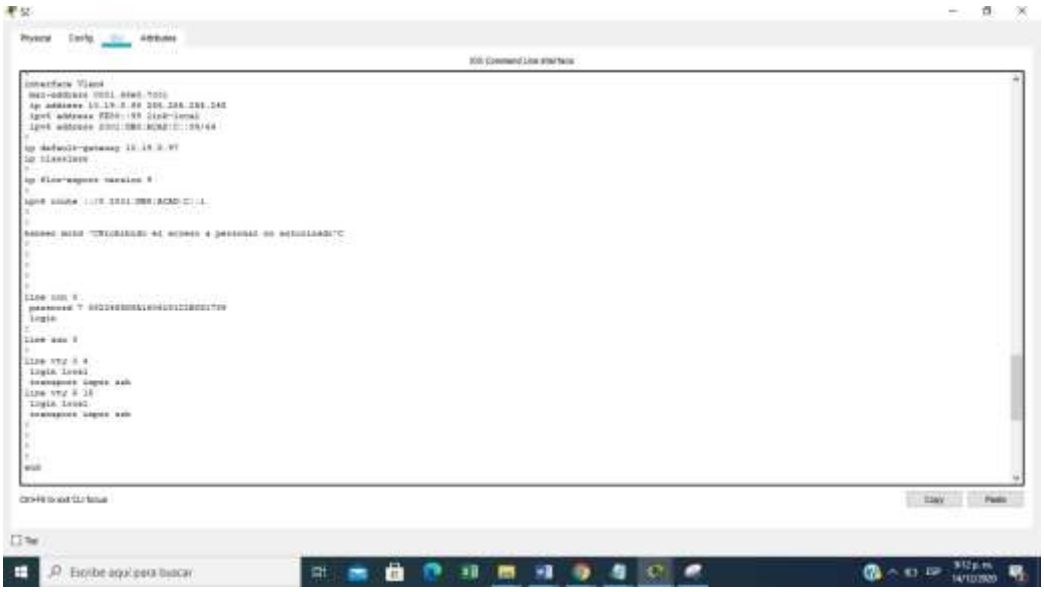
Figura 23. Configuracion de S2 septima parte



Fuente: Autor

La figura muestra la septima de 8 imágenes de la configuracion de S2

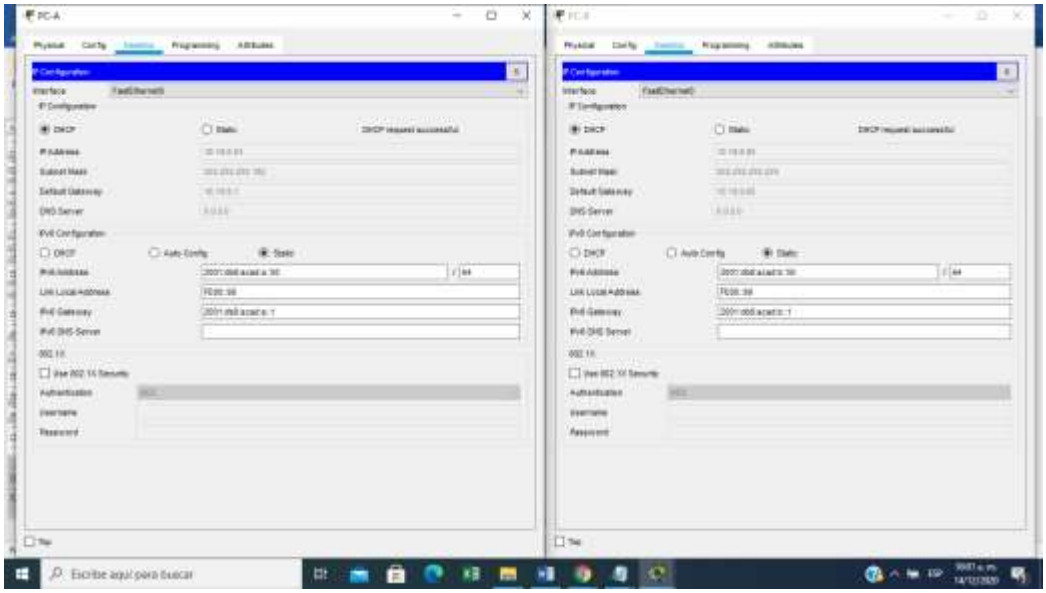
Figura 24. Configuracion de S2 octava parte



Fuente: Autor

La figura muestra la octava de 8 imágenes de la configuracion de S2

Figura 25. Configuracion de PC-A y PC-B



Fuente: Autor

La figura muestra la configuracion de las NIC de los PC-A y PC-B

1.8 PROBAR Y VERIFICAR LA CONECTIVIDAD DE EXTREMO A EXTREMO

A continuación, veremos el resultado de las configuraciones anteriores utilizando el comando ping en su versión ipv4 e ipv6 entre los equipos de la red.

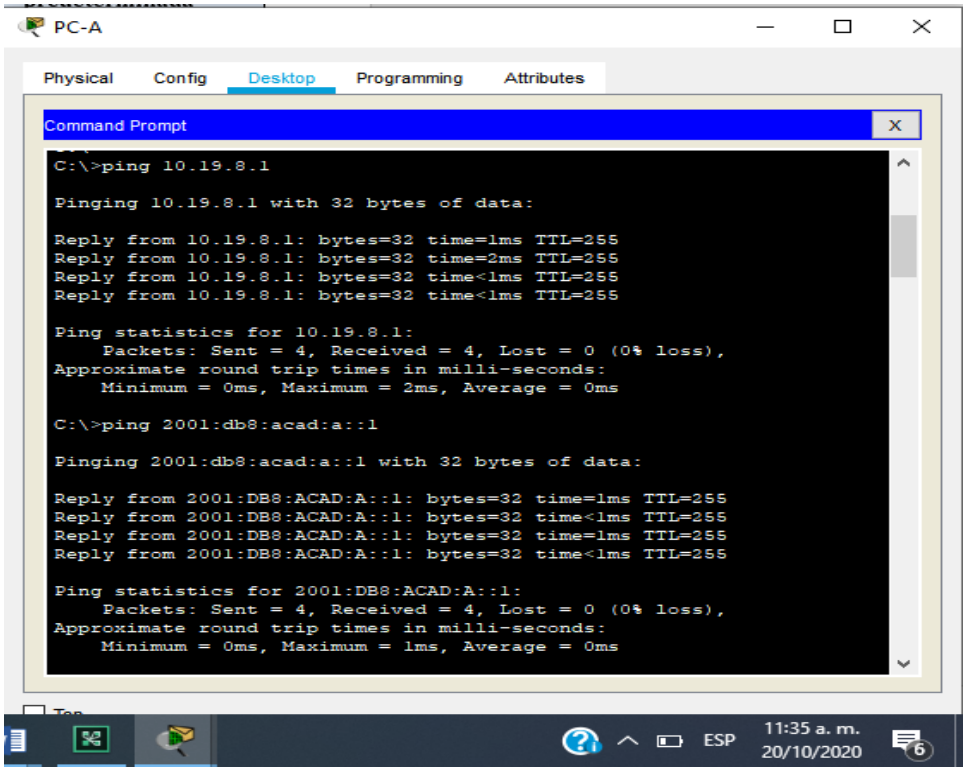
Tabla 13. Configuración de red para el PC-A

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	100%
PC-A	R1, G0/0/1.2	IPv6	2001:db8:acad:a::1	100%
PC-A	R1, G0/0/1.3	Dirección	10.19.8.65	100%
PC-A	R1, G0/0/1.3	IPv6	2001:db8:acad:b: :1	100%
PC-A	R1, G0/0/1.4	Dirección	10.19.8.97	100%
PC-A	R1, G0/0/1.4	IPv6	2001:db8:acad:c: :1	100%
PC-A	S1, VLAN 4	Dirección	10.19.8.98	100%
PC-A	S1, VLAN 4	IPv6	2001:db8:acad:c::98	0%
PC-A	S2, VLAN 4	Dirección	10.19.8.99.	100%
PC-A	S2, VLAN 4	IPv6	2001:db8:acad:c: :99	0%
PC-A	PC-B	Dirección	IP address will vary.	100%
PC-A	PC-B	IPv6	2001:db8:acad:b: :50	100%
PC-A	R1 Bucle 0	Dirección	209.165.201.1	100%
PC-A	R1 Bucle 0	IPv6	2001:db8:acad:209::1	100%
PC-B	R1 Bucle 0	Dirección	209.165.201.1	100%
PC-B	R1 Bucle 0	IPv6	2001:db8:acad:209::1	100%
PC-B	R1, G0/0/1.2	Dirección	10.19.8.1	100%
PC-B	R1, G0/0/1.2	IPv6	2001:db8:acad:a::1	100%
PC-B	R1, G0/0/1.3	Dirección	10.19.8.65	100%
	R1, G0/0/1.3	IPv6	2001:db8:acad:b: :1	100%
PC-B	R1, G0/0/1.4	Dirección	10.19.8.97	100%
PC-B	R1, G0/0/1.4	IPv6	2001:db8:acad:c: :1	100%

PC-B	S1, VLAN 4	Dirección	10.19.8.98	100%
PC-B	S1, VLAN 4	IPv6	2001:db8:acad:c: :98	0%
<PC-B	S2, VLAN 4	Dirección	10.19.8.99	100%
PC-B	S2, VLAN 4	IPv6	2001:db8:acad:c: :99	0%

La anterior tabla indica los pings necesarios para comprobar la conectividad de toda la red.

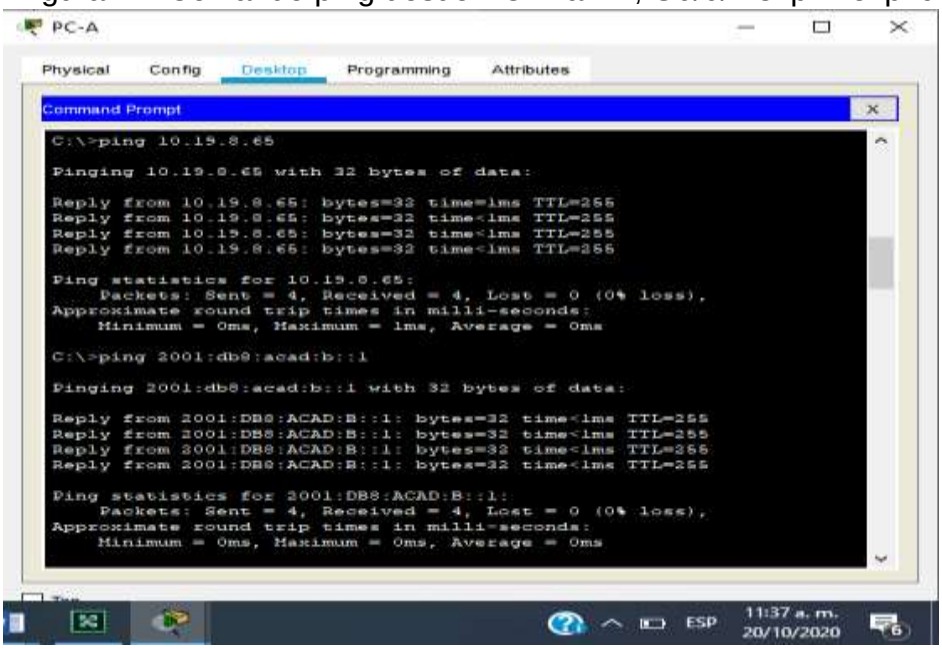
Figura 26. Comando ping desde PC-A a R1, G0/0/1.2 ipv4 e ipv6



Fuente: Autor

Se realiza exitosamente el comando desde el PC-A hacia la interface G0/0/1.2 con la direccion ip4 e ipv6.

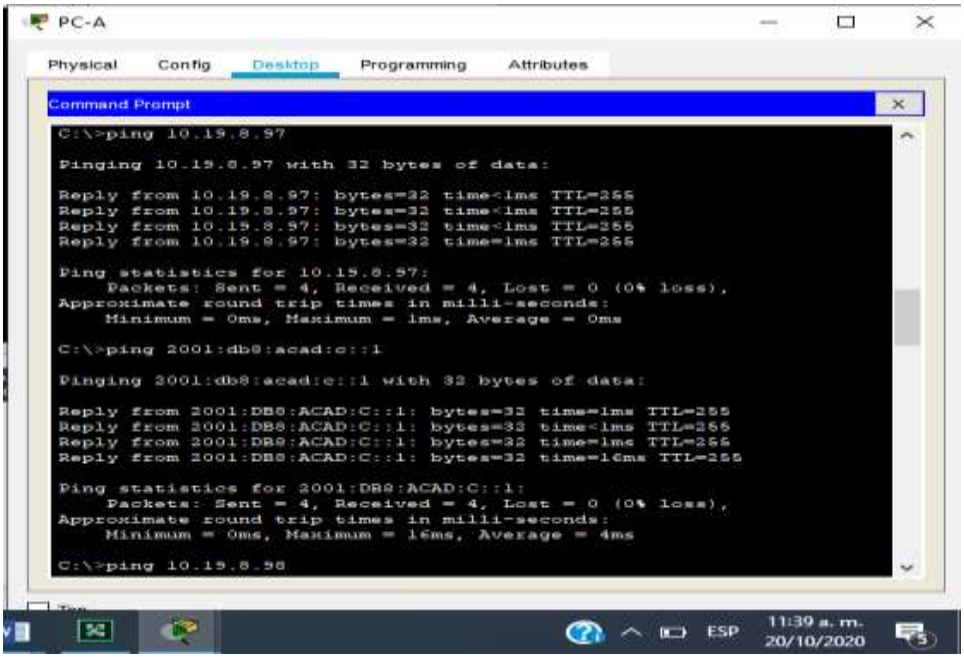
Figura 27. Comando ping desde PC-A a R1, G0/0/1.3 ipv4 e ipv6



Fuente: Autor

Se realiza exitosamente el comando desde el PC-A hacia la interface G0/0/1.3 con la direccion ip4 e ipv6.

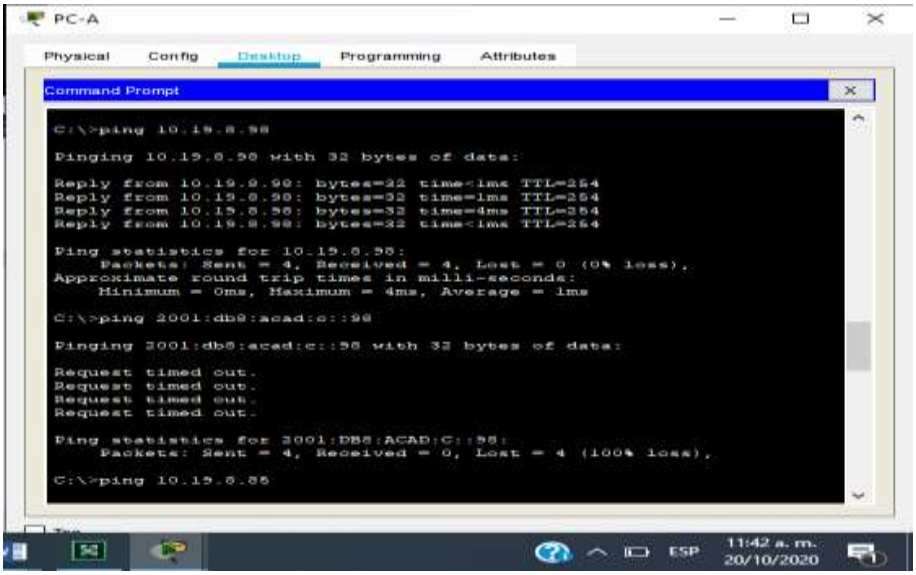
Figura 28. Comando ping desde PC-A a R1, G0/0/1.4 ipv4 e ipv6



Fuente: Autor

Se realiza exitosamente el comando desde el PC-A hacia la interface G0/0/1.4 con la direccion ip4 e ipv6.

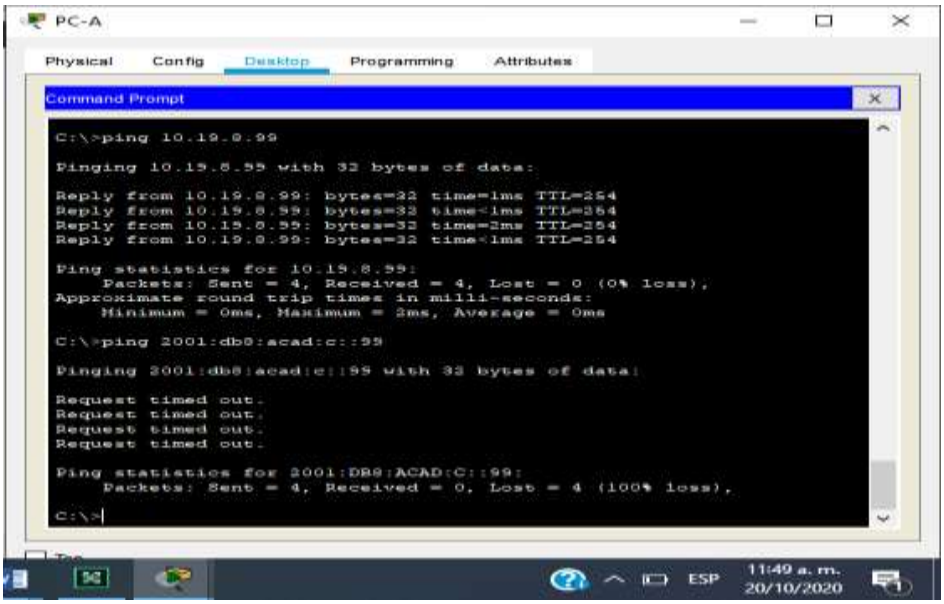
Figura 29. Comando ping desde PC-A a S1, VLAN 4 ipv4 e ipv6



Fuente: Autor

Se realiza exitosamente el comando desde el PC-A hacia la VLAN 4 de S1 con la direccion ip4 e ipv6.

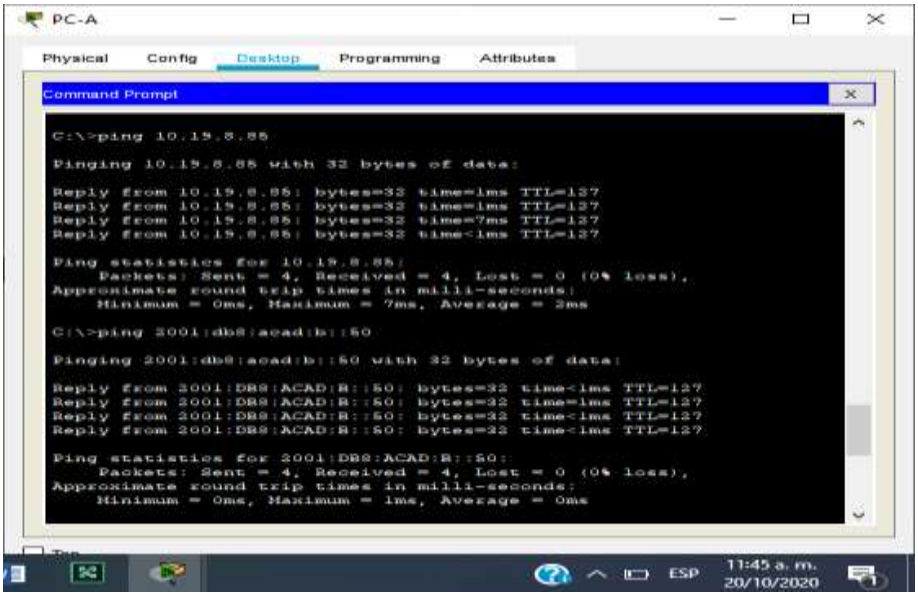
Figura 30. Comando ping desde PC-A a S2, VLAN 4 ipv4 e ipv6



Fuente: Autor

Se realiza exitosamente el comando desde el PC-A hacia la VLAN 4 de S2 con la direccion ip4 e ipv6.

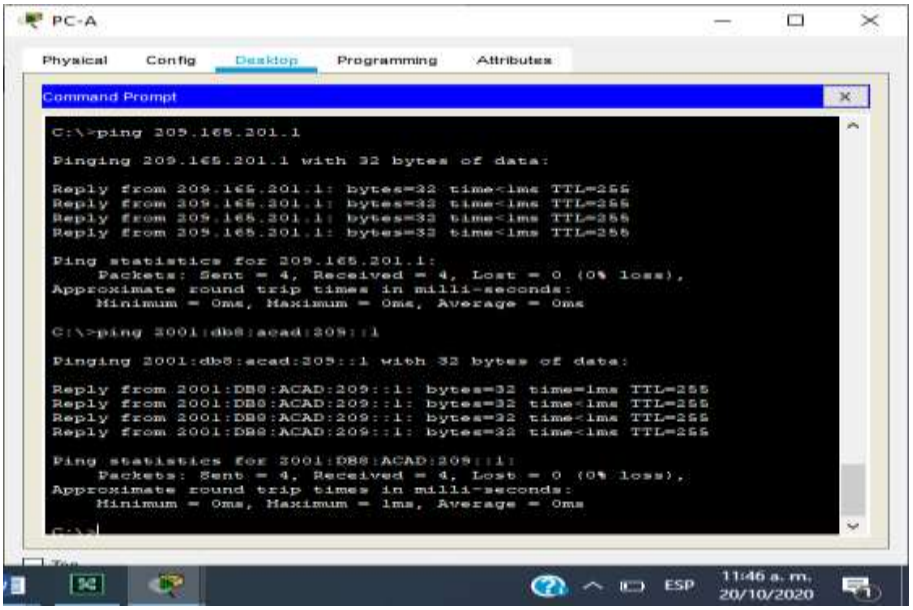
Figura 31. Comando ping desde PC-A a PC-B ipv4 e ipv6



Fuente: Autor

Se realiza exitosamente el comando desde el PC-A hacia el PC-B de S1 con la direccion ip4 e ipv6.

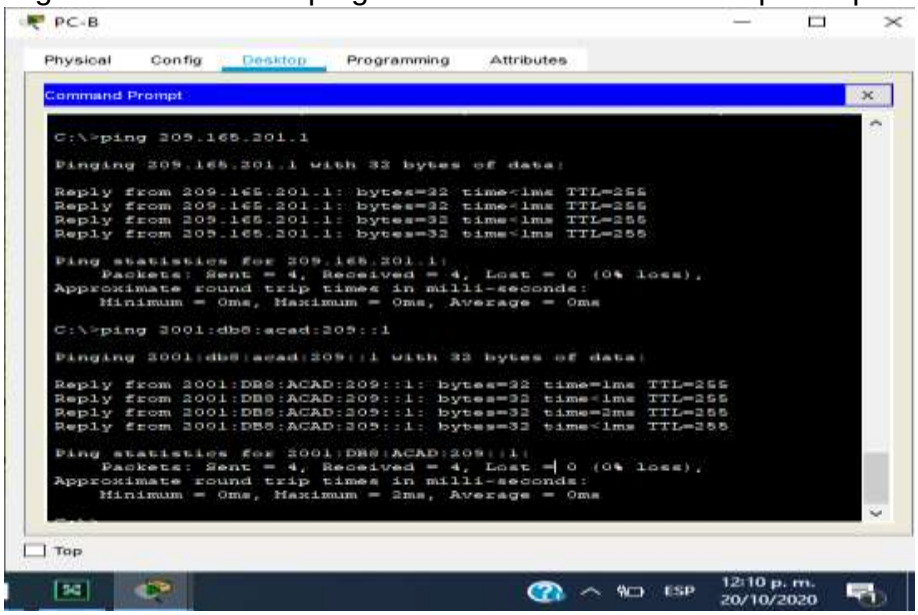
Figura 32. Comando ping desde PC-A a R1 Bucle 0 ipv4 e ipv6



Fuente: Autor

Se realiza exitosamente el comando desde el PC-A hacia el loopback 0 con la direccion ip4 e ipv6.

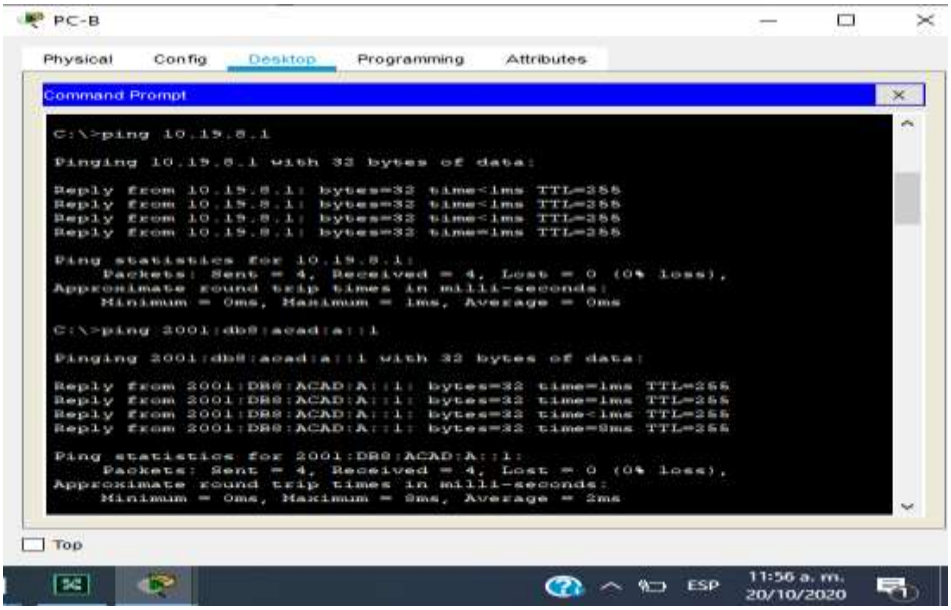
Figura 33. Comando ping desde PC-B a R1 Bucle 0 ipv4 e ipv6



Fuente: Autor

Se realiza exitosamente el comando desde el PC-B hacia el loopback 0 con la direccion ip4 e ipv6.

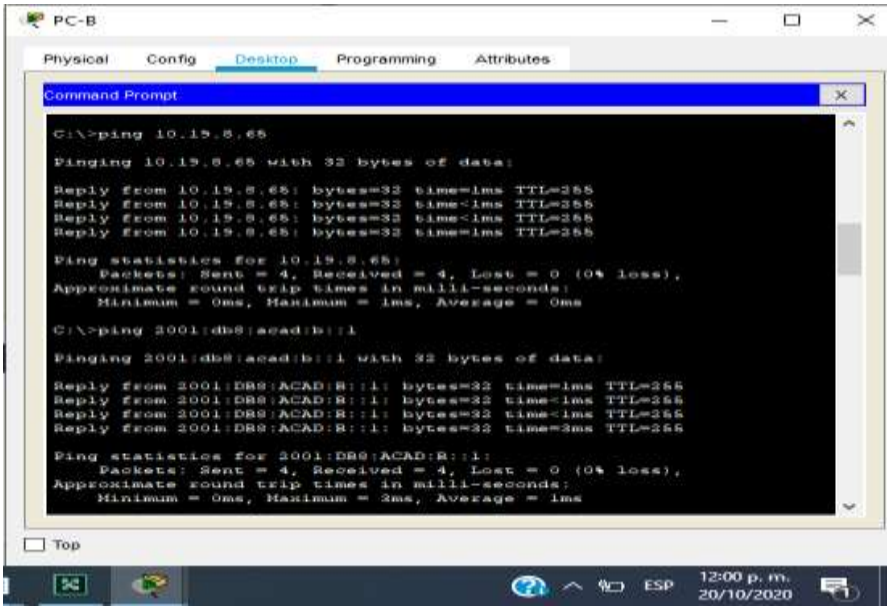
Figura 34. Comando ping desde PC-B R1, G0/0/1.2 Bucle 0 ipv4 e ipv6



Fuente: Autor

Se realiza exitosamente el comando desde el PC-B hacia la interface g0/0/1.2 con la direccion ip4 e ipv6

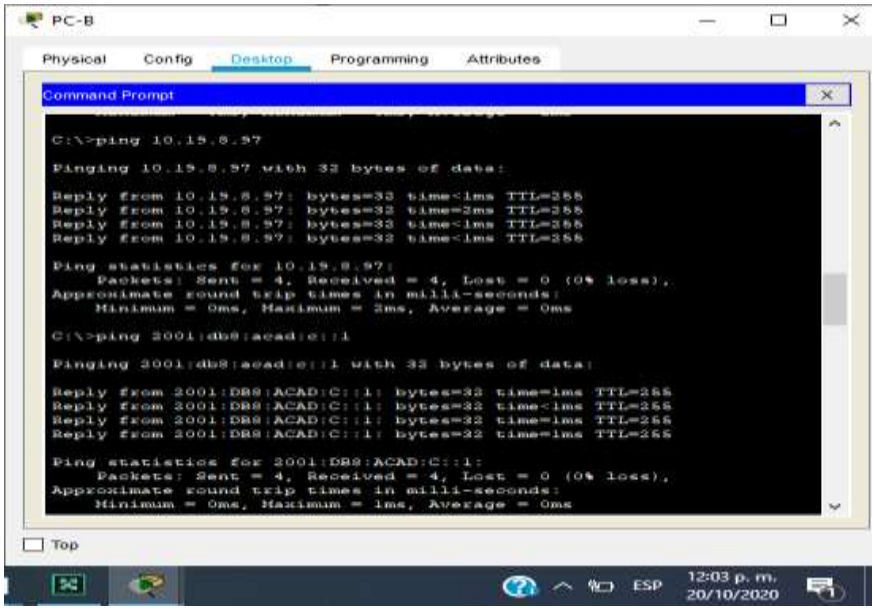
Figura 35. Comando ping desde *PC-B a R1, G0/0/1.3* ipv4 e ipv6



Fuente: Autor

Se realiza exitosamente el comando desde el PC-B hacia la interface g0/0/1.3 con la direccion ip4 e ipv6

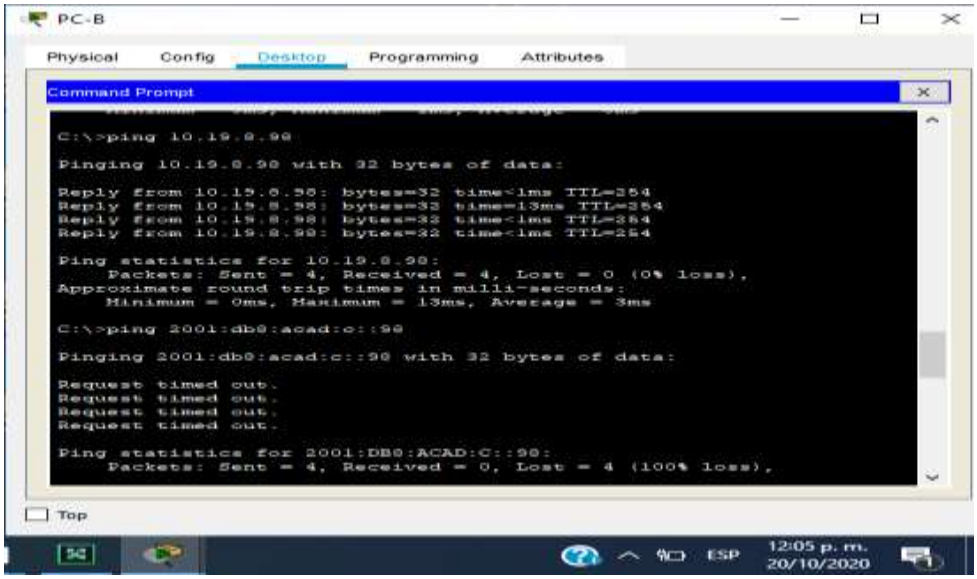
Figura 36. Comando ping desde PC-B a PCB a R1, G0/0/1.4 ipv4 e ipv6



Fuente: Autor

Se realiza exitosamente el comando desde el PC-B hacia la interface g0/0/1.4 con la direccion ip4 e ipv6

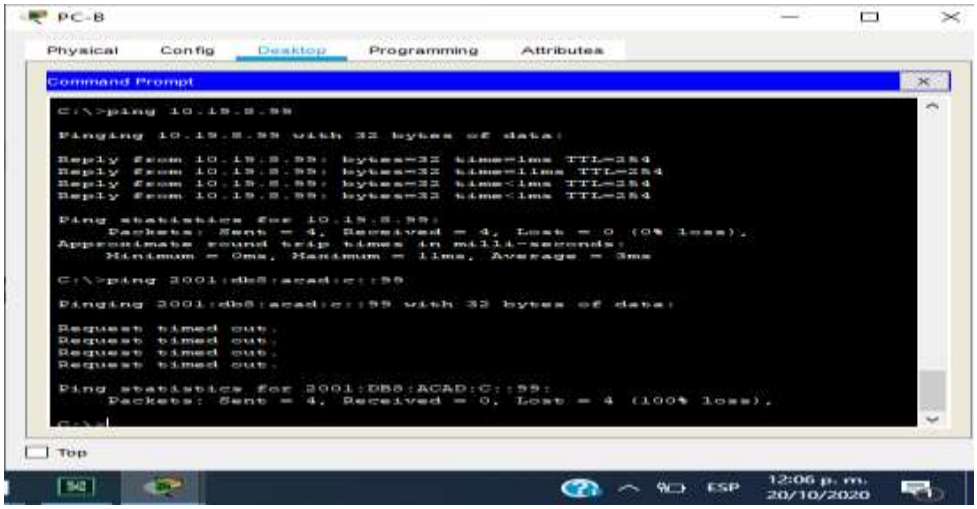
Figura 37. Comando ping desde PC-B a S1, VLAN 4 ipv4 e ipv6



Fuente: Autor

Se realiza exitosamente el comando desde el PC-B hacia la VLAN 4 de S2 con la direccion ip4 e ipv6

Figura 38. Comando ping desde PC-B a S2, VLAN 4 ipv4 e ipv6

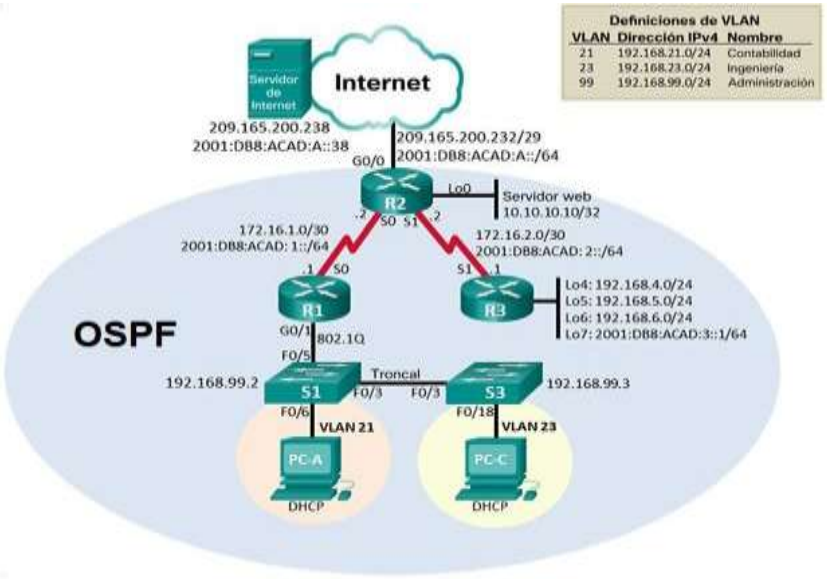


Fuente: Autor

Se realiza exitosamente el comando desde el PC-B hacia la VLAN 4 de S2 con la direccion ip4 e ipv6

2. ESCENARIO 2

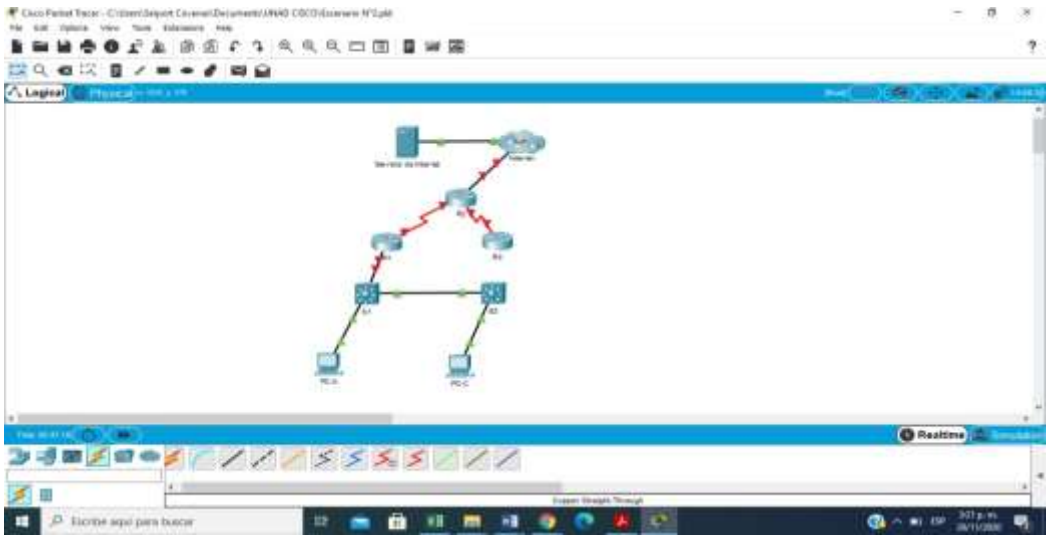
Figura 39. Escenario 2



Fuente: Autor

La imagen numero 28 corresponde a una red pequeña la cual se debe configurar los siguientes requerimientos: conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente.

Figura 40. Simulación del Escenario 2



Fuente: Autor

La imagen 29 muestra la representacion de la topologia de la imagen 28 en el entrono de packet tracer.

1.1 INICIALIZAR DISPOSITIVOS

Inicializamos todos los dispositivos borrando las configuraciones previas y los archivos Vlan.dat, luego volvemos a cargar tanto en los routers como en los switches:

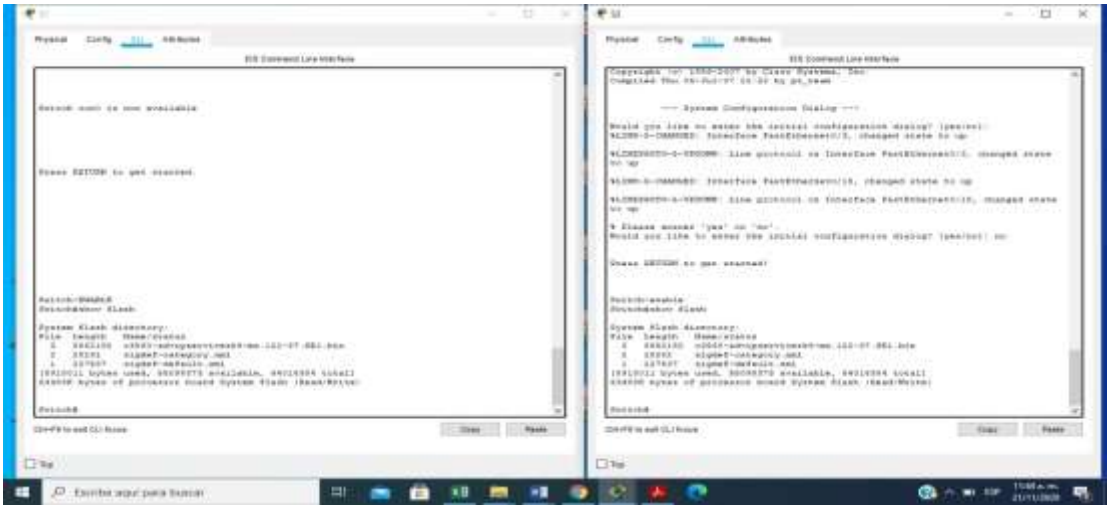
Tabla 14. Tareas de configuración inicial para los routers y switchs

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>enable Router#erase startup-config
Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm] Initializing Hardware ...
Eliminar el archivo startup-config de todos los switches y eliminar la	Switch>enable Switch#delete vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm]

base de datos de VLAN anterior	
Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm]
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>show flash

Despues de realizar los comandos de la tabla 14, tenemos todos los dispositivos libres de archivos de configuraciones previas y listos para una nueva configuracion.

Figura 41. Verificando la eliminación de los archivos VLAN.dat en S1 y S3



Fuente: Autor

Queda verificado con la imagen 20 que no existen archivos VLAN.dat ni en el switch 1 ni en el switch 2.

1.2 CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

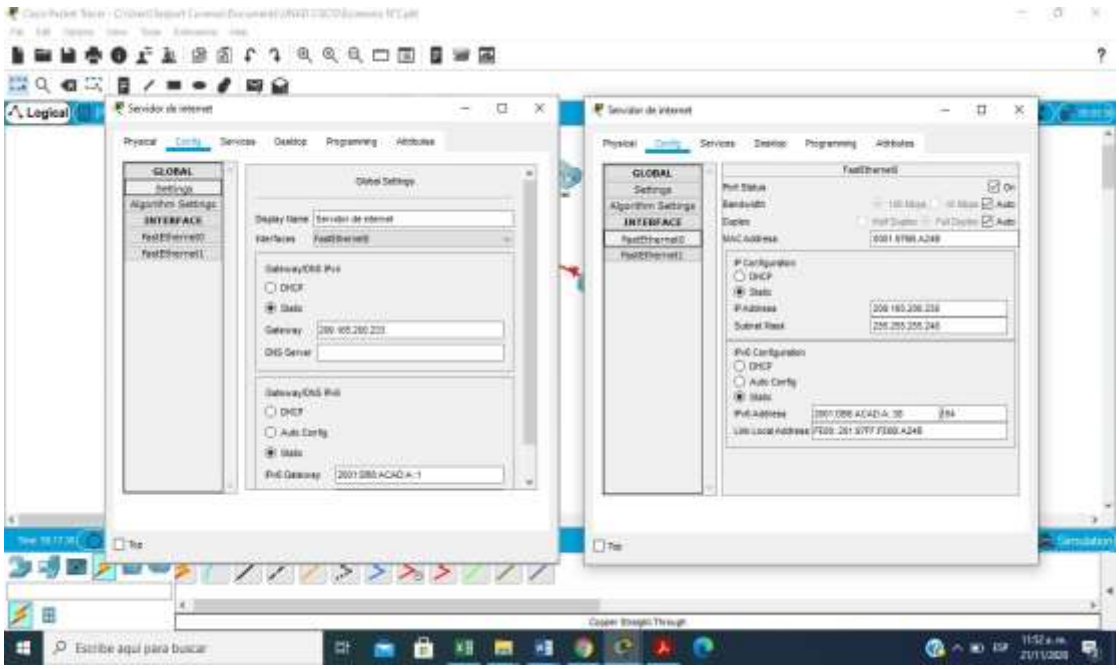
Configuraremos el servidor de Internet con los siguientes tareas y comandos:

Tabla 15. Direccionamiento del servidor de internet

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

Los pasos de la tabla anterior dejan configurado el direccionamiento del servidor de internet de la red para conectarse a la red una vez esta quede completamente configurada.

Figura 42. Configuración del servidor de internet



Fuente: Autor

Vemos en la imagen 31 la configuracion del direccionamiento del servidor de internet en el entorno de packet tracer.

Continuamos con la Configuración de R1, dichas tareas incluyen la siguientes:

Tabla 16. Configuraciones de acceso remoto de R1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router R1	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada "class”	R1(config)#enable secret class
Contraseña de acceso a la consola "cisco”	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet "cisco”	R1(config)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login R1(config)#line exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD "Se prohíbe el acceso no autorizado”	R1(config)#banner motd #Se prohibe el acceso no autorizado#
Interfaz S0/0/0 -Establezca la descripción -Establecer la dirección IPv4 -Establecer la dirección IPv6 -Establecer la frecuencia de reloj en 128000 -Activar la interfaz	R1(config)#int s0/0/0 R1(config-if)#description CONEXION A R2 R1(config-if)#ip add 172.16.1.2 255.255.255.252 R1(config-if)#ipv6 add 2001:DB8:ACAD:1::2/64 R1(config-if)#clock rate 128000 R1(config-if)#no shut
Rutas predeterminadas: Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Con los pasos realizados en la tabla 16, el router 1 quedó nombrado como R1, sin busqueda por DNS, con claves cifradas para consola, modo privilejiado y lineas VTY. Se configuró un mensaje preventivo de bienvenida, se configuró y se activó la interface serial s0/0/0 y se crearon las rutas estaticas para las redes externas conectadas a la interface s0/0/0.

Ahora Configuraremos a R2, para ello seguimos al pie de la letra los siguientes comandos:

Tabla 17. Configuraciones de acceso remoto de R2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router "R2"	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada "class"	R2(config)#enable secret class
Contraseña de acceso a la consola "cisco"	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet "cisco"	R2(config)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login R2(config)#line exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http sever
Mensaje MOTD "Se prohíbe el acceso no autorizado"	R2(config)#banner motd #Se prohibe el acceso no autorizado#
Interfaz S0/0/0: -Establezca la descripción -Establezca la dirección IPv4. -Establezca la dirección IPv6. -Activar la interfaz	R2(config)#int s0/0/0 R2(config-if)#description CONEXION A R1 R2(config-if)#ip add 172.16.1.1 255.255.255.252 R2(config-if)#ipv6 add 2001:DB8:ACAD:1::1/64 R2(config-if)#no shut

Interfaz S0/0/1: -Establecer la descripción -Establezca la dirección IPv4. -Establezca la dirección IPv6. -Establecer la frecuencia de reloj en 128000. -Activar la interfaz	R2(config)#int s0/0/1 R2(config-if)#description CONEXION A R3 R2(config-if)#ip add 172.16.2.1 255.255.255.252 R2(config-if)#ipv6 add 2001:DB8:ACAD:2::1/64 R2(config-if)#clock rate 128000 R2(config-if)#no shut
Interfaz G0/0 (simulación de Internet): -Establecer la descripción. -Establezca la dirección IPv4. -Establezca la dirección IPv6. -Activar la interfaz	R2(config)#int G0/0 R2(config-if)#description CONEXION A LA NUBE R2(config-if)#ip add 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 add 2001:DB8:ACAD:A::1/64 R2(config-if)#no shut
Interfaz loopback 0 (servidor web simulado) -Establecer la descripción. -Establezca la dirección IPv4.	R2(config)#int Lo0 R2(config-if)# description Servidor wed simulado R2(config-if)#ip add 10.10.10.10 255.255.255.255
Ruta predeterminada: -Configure una ruta IPv4 predeterminada de G0/0. -Configure una ruta IPv6 predeterminada de G0/0.	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

En la tabla 17, el router 2 quedó nombrado como R2, sin la busqueda por DNS, configuracion de claves cifradas para consola, modo privilejiado y lineas VTY. Se configuró un mensaje preventivo de bienvenida, se configuró y se activó la interface serial s0/0/0 para conecion al router 1, se configuró y activó la interface serial s0/0/1 para conexión al router 3, configuracion y activacion de la interface G0/0 para conexión a la nube, configuracion y activcion de la interface loopback 0, se crearon las rutas estaticas para las redes externas conectadas a la interface G0/0.

También debemos configurar en el router 3 sus interfaces y las lineas vty siguiendo los comandos acordes a la tarea solicitada:

Tabla 18. Configuraciones de acceso remoto de R3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router "R3"	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada "class"	R3(config)#enable secret class
Contraseña de acceso a la consola "cisco"	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Contraseña de acceso Telnet "cisco"	R3(config)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login R3(config)#exit
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD "Se prohíbe el acceso no autorizado".	R3(config)#banner motd #Se prohibe el acceso no autorizado#
Interfaz S0/0/1 -Establecer la descripción -Establezca la dirección IPv4. -Establezca la dirección IPv6. -Activar la interfaz	R3(config)#int s0/0/1 R3(config-if)#description CONEXION A R2 R3(config-if)#ip add 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 add 2001:DB8:ACAD:2::1/64 R3(config-if)#no shut
Interfaz loopback 4 -Establezca la dirección IPv4. -Utilizar la primera dirección disponible en la subred.	R3(config)#int Lo4 R3(config-if)# description Loop4 R3(config-if)#ip add 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)#int Lo5 R3(config-if)# description Loop5 R3(config-if)#ip add 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)#int Lo6 R3(config-if)# description Loop6 R3(config-if)#ip add 192.168.6.1 255.255.255.0
Interfaz loopback 7 -Establezca la dirección IPv6.	R3(config)#int Lo7 R3(config-if)# description Loop7 R3(config-if)#ipv6 add 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

La tabla anterior, muestra los cambios configurados en el router 3, el cual fué nombrado como R3, se le quitó la busqueda por DNS, se le configuró de claves cifradas para consola, modo privilejiado y lineas VTY. Se configuró su mensaje preventivo de bienvenida, se configuró y se activó la interface serial s0/0/1 para conecion al router 2, se configuraron y activcion 4 interfaces loopback y por ultimo se crearon las rutas estaticas para las redes externas conectadas a la interface s0/0/1.

En el siguiente paso vamos a configurar en S1 las lineas vty, acceso a consola, contraseñas entre otras:

Tabla 19. Configuraciones de acceso remoto de S1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch "S1"	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada "class"	S1(config)#enable secret class
Contraseña de acceso a la consola "cisco"	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Contraseña de acceso Telnet "cisco"	S1(config)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login S1(config)#line exit

Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD "Se prohíbe el acceso no autorizado"	S1(config)#banner motd #Se prohibe el acceso no autorizado#

Se ha configurado en el switch 1 su nombre de host y se ha desactivado la busqueda por DNS; Se establecen las claves de consola, VTY y acceso al modo privilegiado, se realiza la encriptacion de las claves y se deja configurado un mensaje de bienvenida.

Al igual que en el switch S1 en el S3 vamos a configurar en las lineas vty, acceso a consola, contraseñas y hostname:

Tabla 20. Configuraciones de acceso remoto de S3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch "S3"	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada "class"	S3(config)#enable secret class
Contraseña de acceso a la consola "cisco"	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Contraseña de acceso Telnet "cisco"	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login S3(config)#line exit
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD "Se prohíbe el acceso no autorizado"	S1(config)#banner motd #Se prohibe el acceso no autorizado#

Tal como se configuró en el switch 1, en el switch 3 se ha configurado el nombre de host, se ha desactivado la busqueda por DNS; Se establecen las claves de

consola, VTY y acceso al modo privilegiado, encriptacion de las claves y se deja configurado un mensaje de bienvenida.

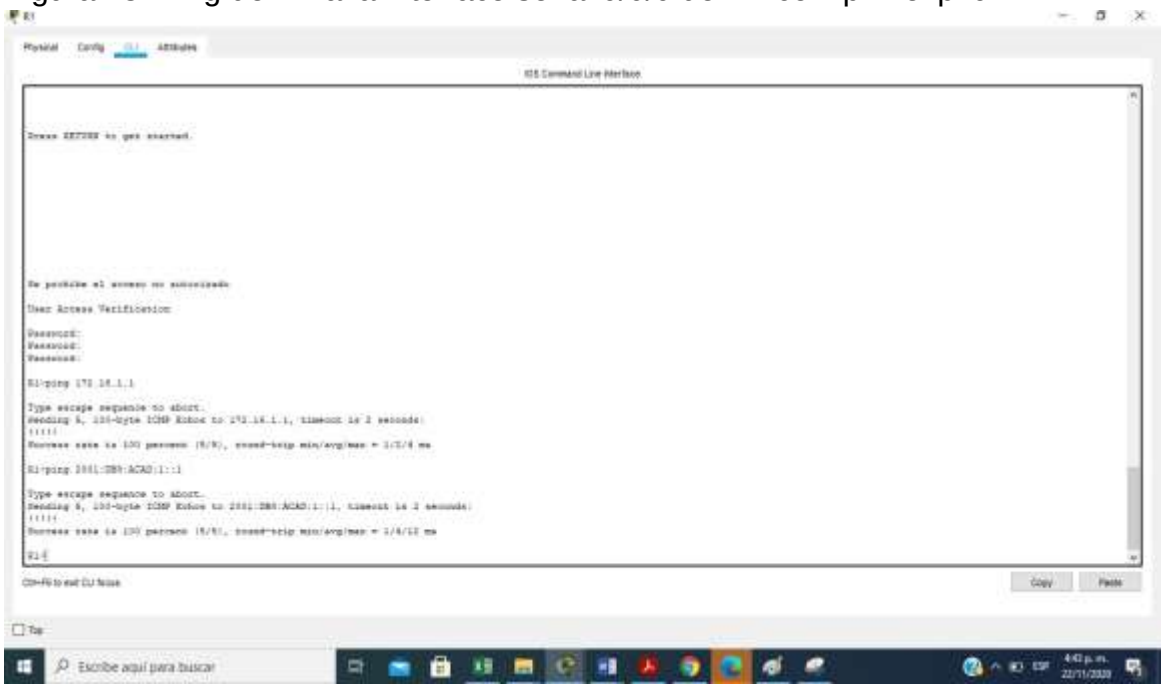
Por ultimo en este paso vamos a verificar la conectividad de la red con el comando ping usaremos la siguiente tabla para registrar los resultados obtenidos:

Tabla 21. Pruebas de conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.1 2001:DB8:ACAD:1::1	CORRECTO
R2	R3, S0/0/1	172.16.2.1 2001:DB8:ACAD:2::1	CORRECTO
PC de Internet	Gateway predeterminado	209.165.200.233 2001:DB8:ACAD:A::1	CORRECTO

La tabla 21 muestra los pings necesarios para verificar la conectividad entre routers.

Figura 43. Ping de R1 a la interface serial 0/0/0 de R2 con ipv4 e ipv6



Fuente: Autor

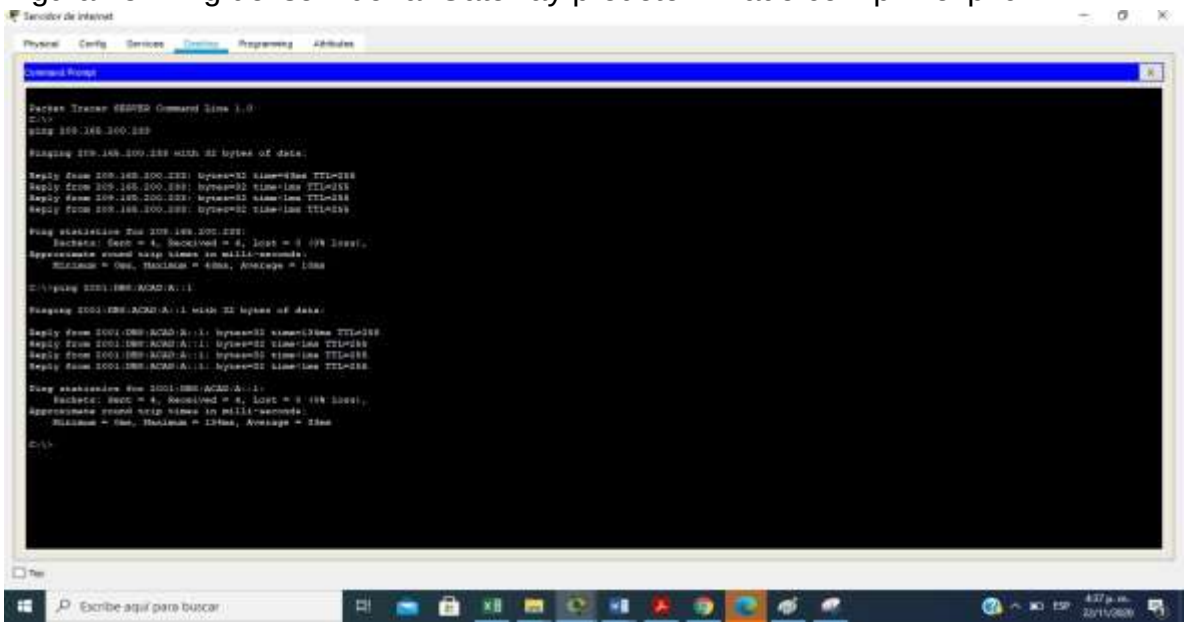
Se muestra el resultado de realizar el ping desde R1 a la direccion ipv4 e ipv6 de la interface s0/0/0 de R2.

Figura 44. Ping de R2 a la interface serial 0/0/1 de R3 con ipv4 e ipv6

Fuente: Autor

Se muestra el resultado de realizar el ping desde R2 a la direccion ipv4 e ipv6 de la interface s0/0/1 de R3.

Figura 45. Ping del servidor al Gateway predeterminado con ipv4 e ipv6



Fuente: Autor

Se muestra el resultado de realizar el ping desde el servidor de internet a la direccion ipv4 e ipv6 de su propio Gateway

2.3 CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN

La configuración del S1 incluye la creación de las VLAN 21, 23, 99; asignación de puertos troncales y de acceso, por último, el apagado de los puertos no utilizados.

Tabla 22. Configuración de las VLAN en S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN: Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican	S1(config)#vlan 21 S1(config)#name Contabilidad S1(config)#vlan 23 S1(config)#name Ingenieria S1(config)#vlan 99 S1(config)#name Administracion
Asignar la dirección IP de administración: -Asigne la dirección IPv4 a la VLAN de administración.	S1(config)#int vlan 99 S1(config-if)#ip add 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado: Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.	S1(config-if)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3: Utilizar la red VLAN 1 como VLAN nativa	S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#no shut
Forzar el enlace troncal en la interfaz F0/5: Utilizar la red VLAN 1 como VLAN nativa	S1(config)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#no shut
Configurar el resto de los puertos como puertos de acceso: Utilizar el comando interface range	S1(config)#int r f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config)#int f0/6 S1(config-if)#switchport access vlan 21

Apagar todos los puertos sin usar	S1(config)#int r f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if)#shutdown

En este paso se han creado las VLANs 21, 23 y 99. En la interface de la VLAN 99 se configuró el direccionamiento ip para usarla como VLAN de administracion. Se toma la VLAN 1 como nativa para el switch con los puertos f0/3 y f0/5 como troncales. El puerto f0/6 quedó como acceso a la VLAN 21 y el resto de los puertos fueron apagados.

A continuación, se configura en S3 las mismas VLANs configuradas en S1, así mismo se configuran los puertos de acceso y la troncal. Apagaremos también los puertos no utilizados.

Tabla 23. Configuración de las VLAN en S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN: Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.	S3(config)#vlan 21 S3(config)#name Contabilidad S3(config)#vlan 23 S3(config)#name Ingenieria S3(config)#vlan 99 S3(config)#name Administracion
Asignar la dirección IP de administración Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología	S3(config)#int vlan 99 S3(config-if)#ip add 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado Asignar la primera dirección IP en la subred como gateway predeterminado.	S3(config-if)#ip default-gateway 192.168.99.1

Forzar el enlace troncal en la interfaz F0/3 Utilizar la red VLAN 1 como VLAN nativa	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#no shut
Configurar el resto de los puertos como puertos de acceso Utilizar el comando interface range	S3(config)#int r f0/1-2, f0/4-24, g0/1-2 S3(config-if)#switchport mode access
Asignar F0/18 a la VLAN 21	S3(config)#int f0/18 S3(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S3(config)#int r f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if)#shutdown

Al igual que en el switch 1 en este switch se crearon las VLANs 21, 23 y 99. En la interface de la VLAN 99 se configuró el direccionamiento ip para usarla como VLAN de administracion. Se toma la VLAN 1 como nativa con el puerto f0/3 como troncal. El puerto f0/6 quedó como acceso a la VLAN 21 y el resto de los puertos se configuraron en modo acceso, pero fueron apagados por no estar utilizados.

Para completar las redes de las VLAN pasamos a configuras en R1 las subinterfaces con su respectivo encapsulamiento DOT1Q seguido de la activación de la interface g0/1:

Tabla 24. Configuración de las subinterfaces en R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1 Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz	R1(config)#int g0/1.21 R1(config-line)#encapsulation dot1q 21 R1(config-line)#description Contabilidad R1(config)#ip add 192.168.21.1 255.255.255.0

Configurar la subinterfaz 802.1Q .23 en G0/1 Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz	R1(config)#int g0/1.23 R1(config-line)#encapsulation dot1q 23 R1(config-line)#description Ingenieria R1(config)#ip add 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1 Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz	R1(config)#int g0/1.99 R1(config-line)#encapsulation dot1q 99 R1(config-line)#description Administracion R1(config)#ip add 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config)#int g0/1 R1(config-line)#no shut

Los pasos de la tabla 24 nos muestran como se configuraron las subinterfaces G0/1.21, G0/1.23 y G0/1.99 dividiendo la interface G0/1. Se les asigna una descripcion a cada una subinterface y su respectiva direccion ip.

Pasamos a verificar la conectividad de la red hasta este paso usando el comando ping; Nos valdremos de la siguiente tabla para hacer las pruebas de forma metódica:

Tabla 25. Verificación de conectividad entre VLANs

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Correcto
S3	R1, dirección VLAN 99	192.168.99.1	Correcto
S1	R1, dirección VLAN 21	192.168.21.1	Correcto
S3	R1, dirección VLAN 23	192.168.23.1	Correcto

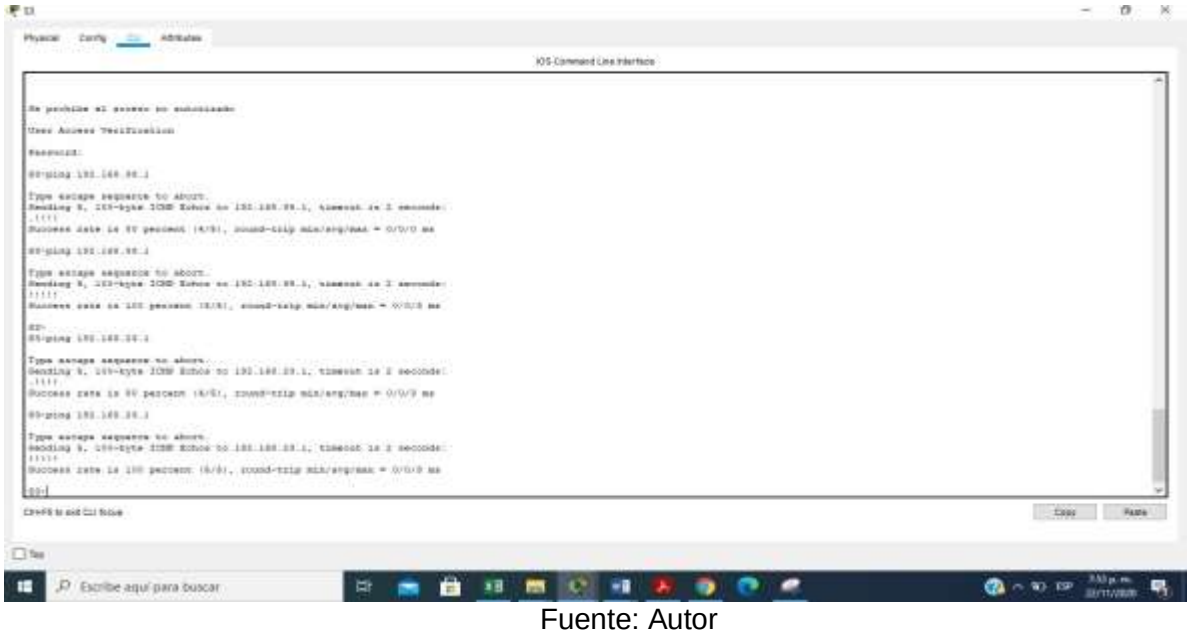
Esta tabla muestra los pings necesarios que realizaremos para verificar la conectividad entre las VLANS.

Figura 46. Ping desde S1 a VLAN 99 y a la VLAN 21 en R1

Fuente: Autor

Se observa desde el CLI de S1 que los pines a las VLAN 99 y 21 fueron exitosos indicando que si hay conexión entre S1 y R1

Figura 47. Ping desde S3 a VLAN 99 y la VLAN 23 en R1



Fuente: Autor

Se observa desde el CLI de S3 que los pines a las VLAN 99 y 23 fueron exitosos indicando que si hay conexión entre S3 y R1

2.4 CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO OSPF

Comenzamos esta parte configurando el OSPF en el R1, crearemos el área 0, asignaremos las redes conectadas directamente y haremos pasivas las redes LAN asociadas:

Tabla 26. Configuraciones del OSPF en R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#router-id 1.0.0.0
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99 R1(config-router)#end
Desactive la sumarización automática	No necesario.

Con los comandos de la tabla 26, hemos activado el protocolo OSPF, asignamos el ID al router 1 y le hemos creado al area 0 las redes conectadas directamente al router incluyendo las redes de las VLANs. Las subinterfaces del router 1 estan ubicadas en un puerto de acceso G0/1, por lo tanto, se configuraron con interfaces pasivas para omitir mensajes OSPF atravez de este puerto.

Seguimos con el router 2 con la misma área 0, asignando las redes conectadas y volviendo pasivas las redes LAN del router.

Tabla 27. Configuraciones del OSPF en R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config-router)#router-id 2.0.0.0
Anunciar las redes conectadas directamente **Nota:** Omitir la red G0/0.	R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
Establecer la interfaz LAN (loopback) como pasiva	R1(config-router)#passive-interface lo0 R1(config-router)#end
Desactive la sumarización automática.	No necesario.

En este paso activamos el protocolo OSPF al router 2 y le asignamos el ID y le asociamos al area 0 las redes conectadas directamente al router. La interface del loopback 0 no esta relacionada como un dispositivo de enrutamiento por lo tando se configura con interfaces pasiva.

La siguiente configuración del R3 incluye la creación nuevamente del área 0, anuncio de las redes LAN conectadas directamente y la configuración de las interfaces pasivas:

Tabla 28. Configuraciones del OSPF en R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 1 R3(config-router)#router-id 3.0.0.0
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0

Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6 R1(config-router)#end
Desactive la sumarización automática.	No necesario.

Ahora activamos el protocolo OSPF en el router 3, le asignamos el ID y le asociamos al area 0 las redes conectadas directamente al router. Las interfaces loopback no estan relacionadas como un dispositivo de enrutamiento por lo tando todas se configuran con interfaces pasivas.

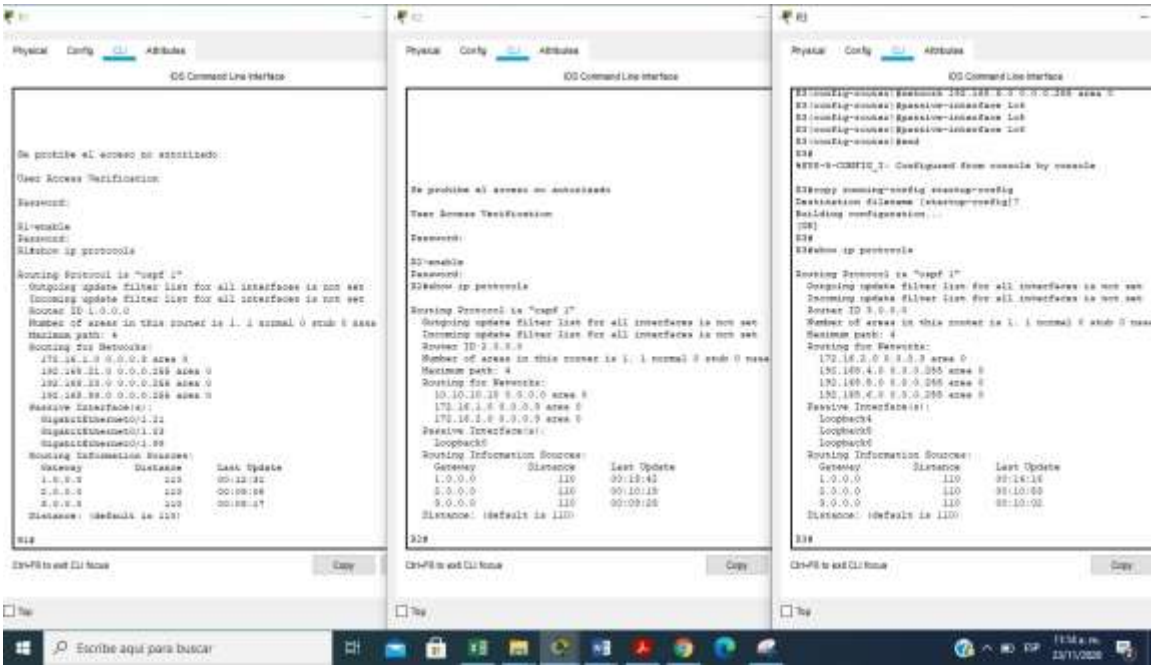
En este punto verificamos la información de OSPF valiéndonos de los siguientes comandos:

Tabla 29. Comandos de verificación de OSPF

Pregunta	**Respuesta**
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	R1#show ip protocols R2#show ip protocols R3#show ip protocols
¿Qué comando muestra solo las rutas OSPF?	R1#show ip route ospf R2#show ip route ospf R3#show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R1#show ip ospf neighbor R2#show ip ospf neighbor R3#show ip ospf neighbor

En la tabla anterior se exponen los comandos basicos para verivicar la implementacion del protocolo OSPF.

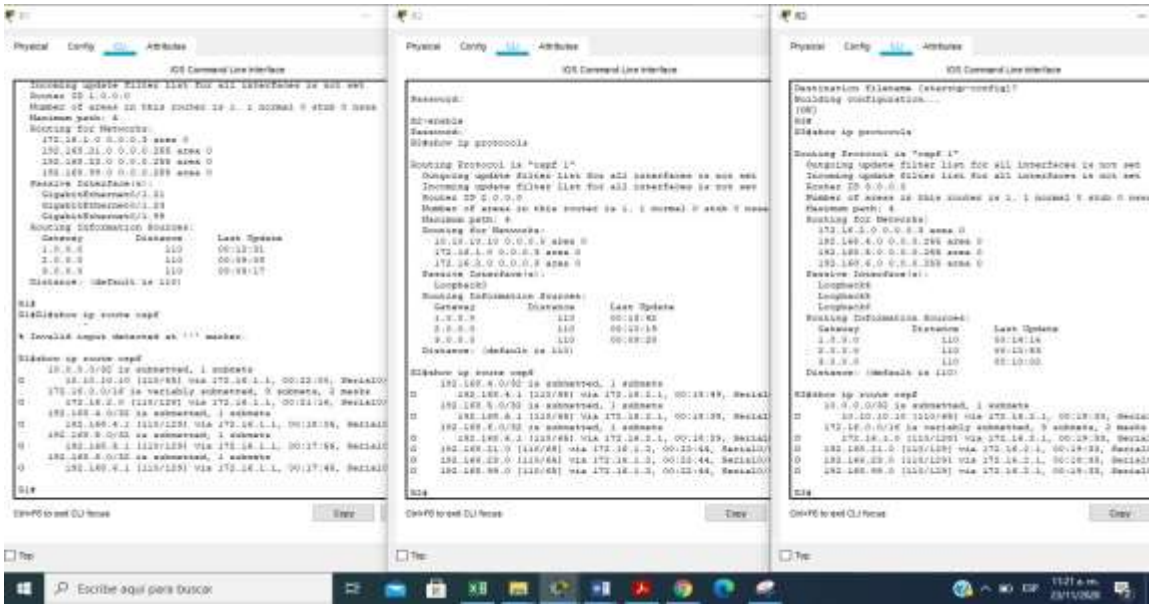
Figura 48. Comando show ip protocols en R1, R2 y R3



Fuente: Autor

En esta imagen se observa el resultado tanto en R1, R2 y R3 del comando show ip protocols, en donde se expone la configuracion OSPF de en cada router.

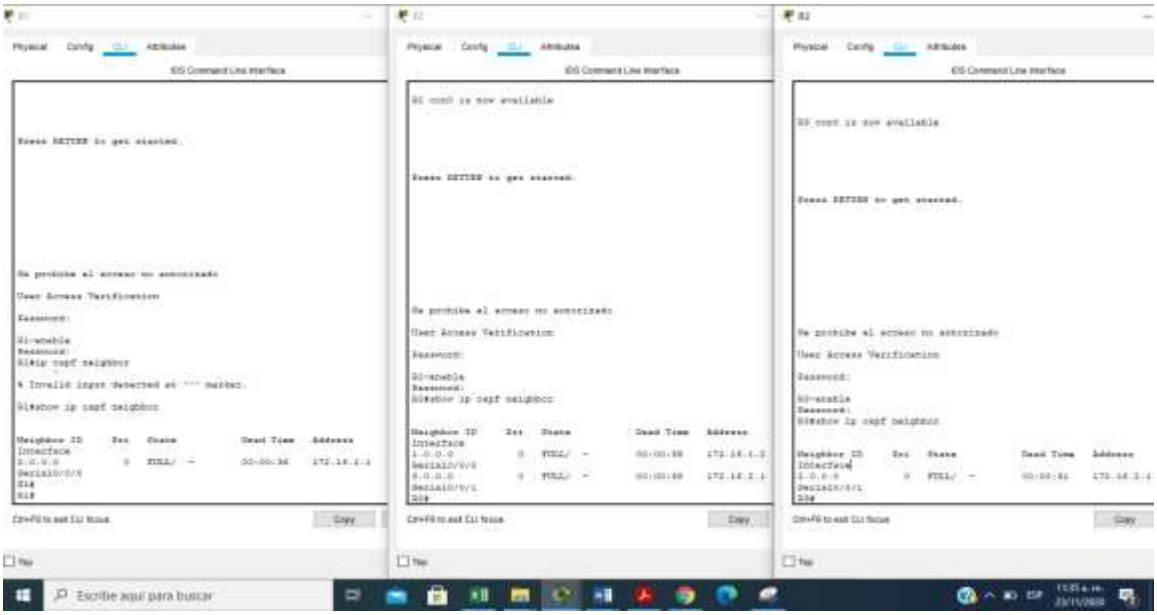
Figura 49. Comando show ip route ospf en R1, R2 y R3



Fuente: Autor

En la imagen 38 vemos las rutas OSPF almacenadas en los routers 1, 2 y 3

Figura 50. Comando show ip ospf neighbor en R1, R2 y R3



Fuente: Autor

Observamos del resultado del comando OSPF neighbor en todos los routers las redes de los routers conectados entre las interfaces de cada uno de ellos.

2.5 IMPLEMENTAR DHCP Y NAT PARA IPV4

Configuraremos a continuación en el R1 dos servidores DHCP para asignar direcciones ipv4 automáticamente a los dispositivos de las VLAN 21 y 23 según las respectivas redes indicadas en la topología del escenario 2. En cada red reservaremos las 20 primeras direcciones, indicaremos un Gateway y un DNS.

Tabla 30. Configuración del DHCP en R1

Elemento o tarea de configuración	**Especificación**
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20

Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21: 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(config-config)#network 192.168.21.0 255.255.255.0 R1(config-config)#dns-server 10.10.10.10 R1(config)#ip domain-name ccna-sa.com R1(config-config)#default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23 Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado	R1(config)#ip dhcp pool ENGNR R1(config)#ip network 192.168.23.0 255.255.255.0 R1(config)#dns-server 10.10.10.10 R1(config)#ip domain-name ccna-sa.com R1(config)#default-router 192.168.23.1

Los comandos ejecutados en la tabla anterior dejan configurado en el router 1 dos pools, uno con la red 192.168.21.0 y el otro con la red 192.168.23.0 los cuales entregan la primera ip disponible como la ip de gateway y en ambos pools se excluyen las primeras 20 direcciones.

Ahora repetiremos los pasamos al router 2 para configurarle la NAT estática y dinámica:

Tabla 31. Configuración de la NAT estática y dinámica de R2

Elemento o tarea de configuración	**Especificación**
Crear una base de datos local con una cuenta de usuario: Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**	R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local
Crear una NAT estática al servidor web. Dirección global interna: **209.165.200.229**	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229

Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#interface lo0 R2(config-if)#ip nat inside R2(config-if)#exit
Configurar la NAT dinámica dentro de una ACL privada Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.0.0 0.0.255.255
Defina el pool de direcciones IP públicas utilizables. Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225 – 209.165.200.228**	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

En la tabla 31 se muestran los comandos con los cuales se asignaron las interfaces g0/0 como externa y la interface Loopback 0 como interna; se permitío el nateo de las redes VLAN 21 y 23 junto con las redes de loopback de R3

Verificaremos ahora el protocolo DHCP y la NAT estática usando las tareas indicadas en la siguiente tabla:

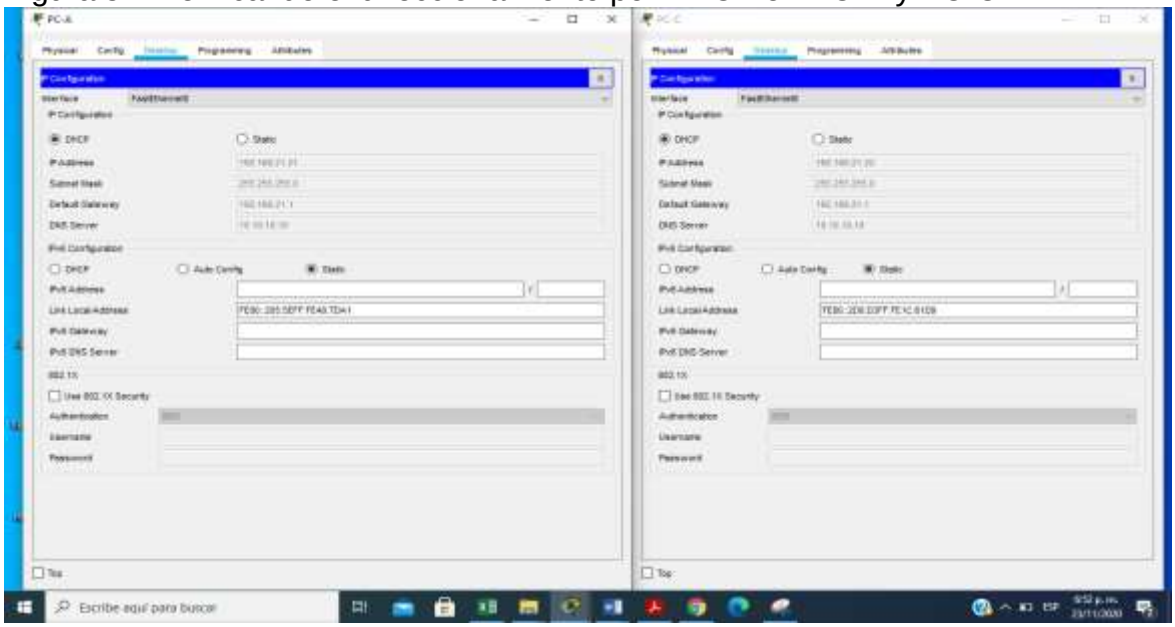
Tabla 32. Verificación de los protocolos DHCP y NAT implementados

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

Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.238)	CORRECTO

De acuerdo a los datos tabulados en la tabla 32, todas los pines y pruebas fueron exitosas; acontinuacion vemos las evidencias.

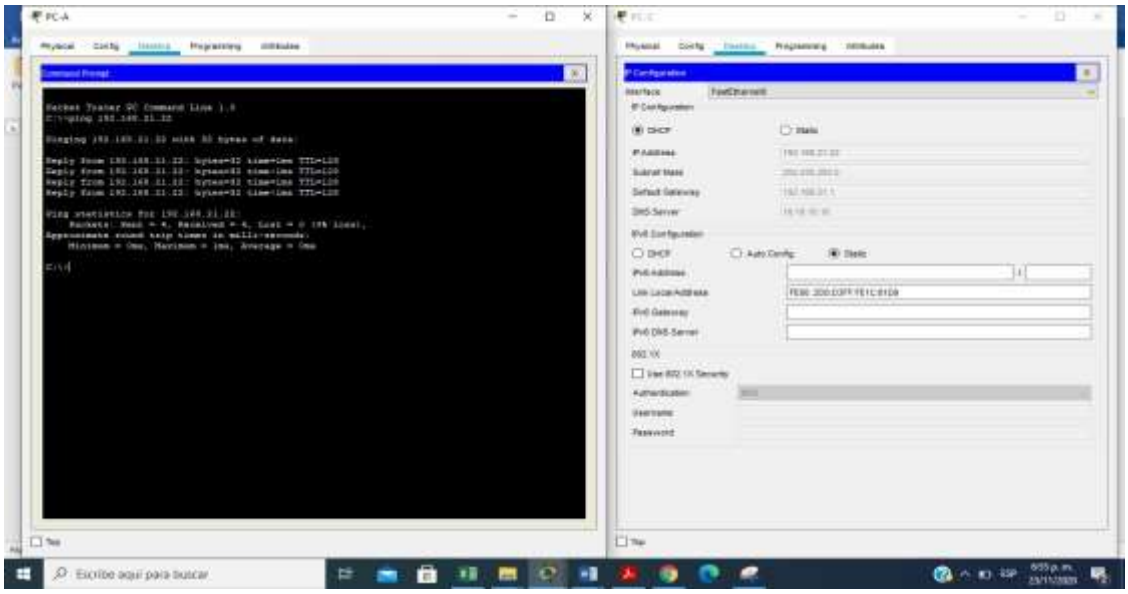
Figura 51. Verificando el direccionamiento por DHCP en PC-A y PC-C



Fuente: Autor

Despues de revisar los PC-A y PC-C, comprobamos la funcionalidad del servicio DHCP.

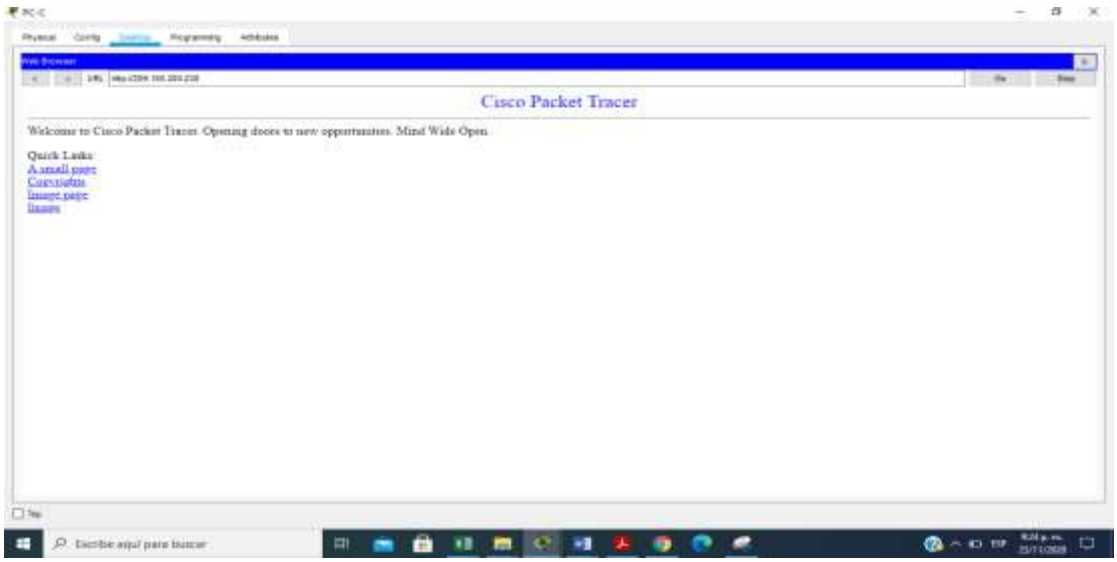
Figura 52. Ping desde PC-A a PC-C



Fuente: Autor

En la imagen observamos la configuracion ip del PC-C a la derecha y el comando ping desde el PC-A a la izquierda.

Figura 53. Accediendo a la interface del servidor wed



Fuente: Autor

La imagen 42 nos muestra la pagina wed del servidor de internet accedida desde el PC-C.

2.6 CONFIGURAR NTP

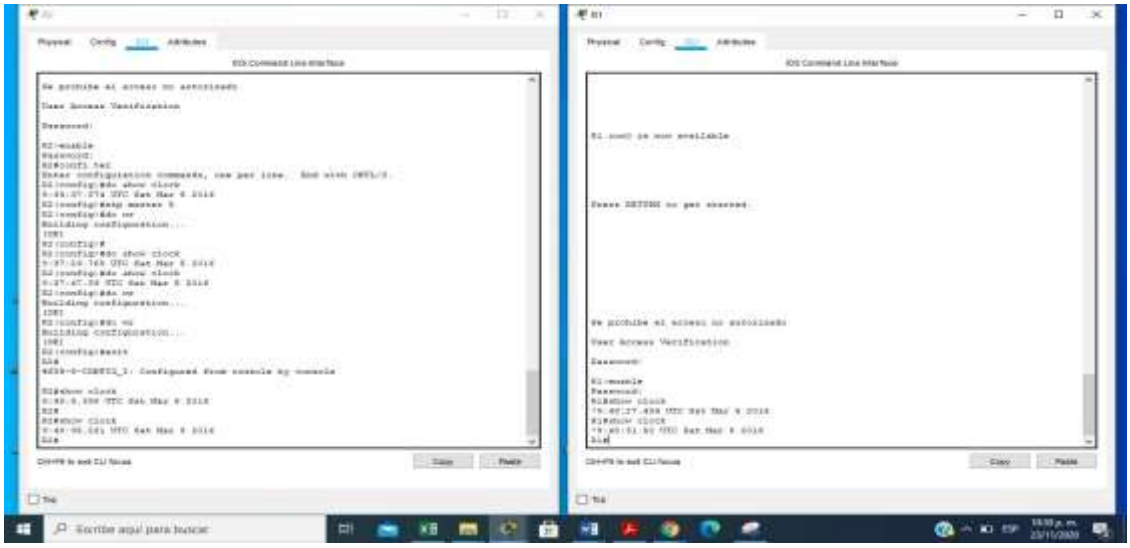
En este momento vamos a configurar los router R1 y R3 de tal forma que tengan sincronizadas la hora y la fecha de cada uno de ellos; para ello haremos a R2 como servidor NTP y a R1 como cliente de modo que ambos queden sincronizados:

Tabla 33. Configuración del servidor NTP

Elemento o tarea de configuración	**Especificación**
Ajuste la fecha y hora en R2. **5 de marzo de 2016, 9 a. m.**	R2#clock set 09:00:00 05 mar 2016
Configure R2 como un maestro NTP. Nivel de estrato: **5**	R2(config)#ntp master 5
Configurar R1 como un cliente NTP. Servidor: **R2**	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1# show clock R2# show clock

La tabla 33 muestra la hora y fecha que se configuró en el router 2, luego cuando se configura como servidor ntp master 5, seguidamente cuonfiguramos el roter 1 como cliente dl router 2.

Figura 54. Verificando la sincronización de la hora en R1 y R2



Fuente: Autor

La figura 43 muestra la hora y fecha en los routers 1 y 2 despues de realizar en ambos el comando show clock.

2.7 CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

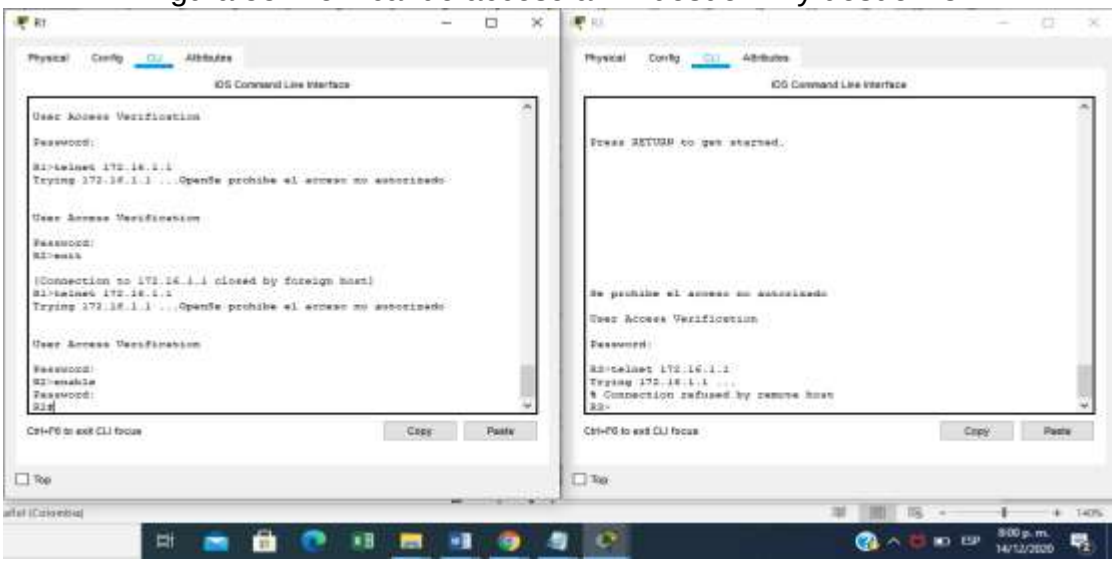
Ahora se configura la restricción para el acceso a las líneas VTY del R2, permitiendo que solo R1 pueda acceder al CLI de R2, luego veremos la verificación de los comandos realizados:

Tabla 34. Configuración de las líneas VTY en R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 Nombre de la ACL: **ADMIN-MGT**	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.2 R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in

Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet R2(config-line)#exit
Verificar que la ACL funcione como se espera	R1>telnet 172.16.1.1 R2>telnet 172.16.1.1

Figura 55. Verificando acceso a R2 desde R1 y desde R3



Fuente: Autor

De la figura 44 vemos que el router 1 pudo conectarse al CLI del router 2 pero para el router 3 el acceso fue denegado.

2.8 INTRODUCIR EL COMANDO DE CLI ADECUADO

A continuación, se resuelve la tabla siguiente investigando y registrando los comandos correspondientes a la respectiva descripción indicada en la tabla:

Tabla 35. Comandos de verificación usados en el escenario 2

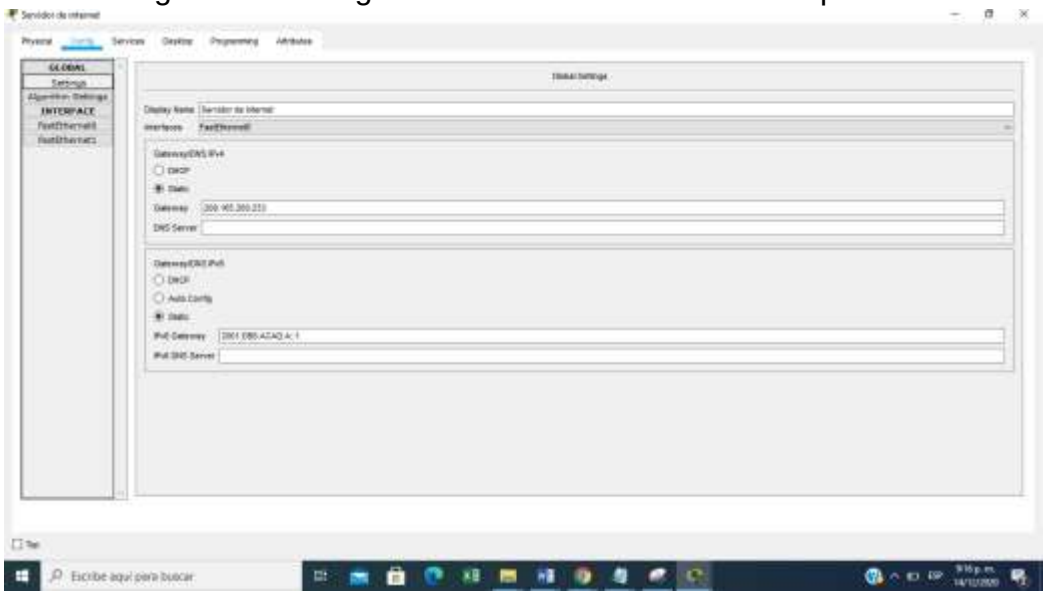
Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Router(config)#show access-list

Restablecer los contadores de una lista de acceso	Router(config)#clear access-list counters 1
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Router#show ip interfaces
¿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.	Router(config)#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Router(config)#clear ip nat translation

En la tabla 35 estan tabulados algunos comandos utilizados durante el desarrollo de los dos escenarios de la presente prueba de habilidades.

2.9 RESUMEN DE LAS CONFIGURACIONES DE TODOS LOS DISPOSITIVOS DEL ESCENARIO 2

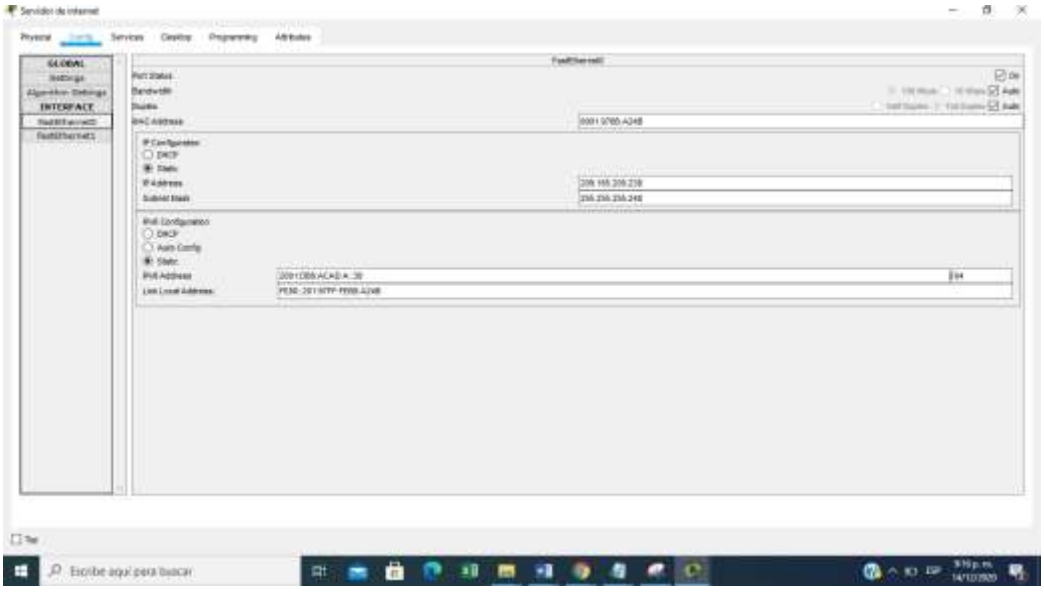
Figura 56. Configuracion del servidor de internet parte 1



Fuente: Autor

Se observa la configuracion del gateway del servidor en ipv4 e ipv6

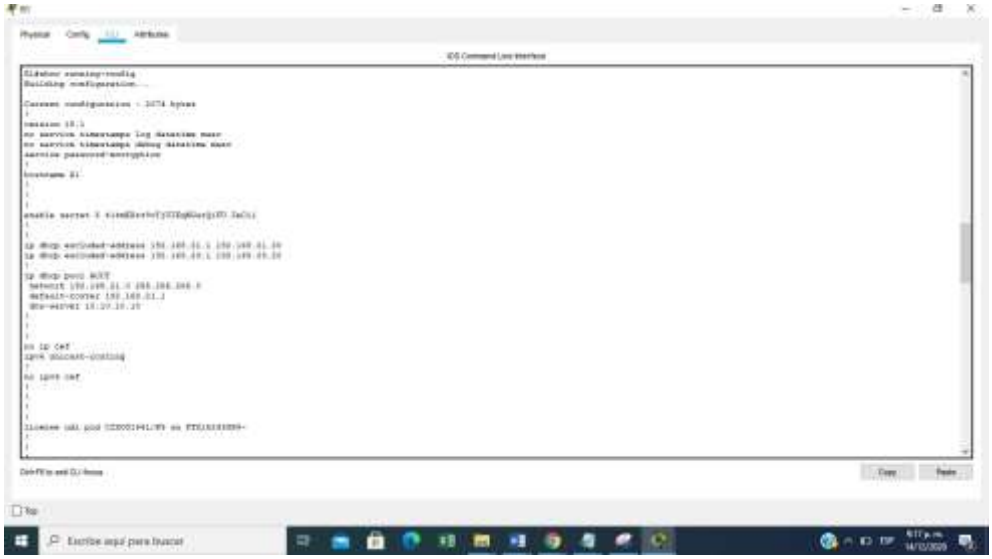
Figura 57. Configuracion del servidor de internet parte 2



Fuente: Autor

Configuracion del direccionamiento de la interface g0/0 en ipv4 e ipv6 del servidor

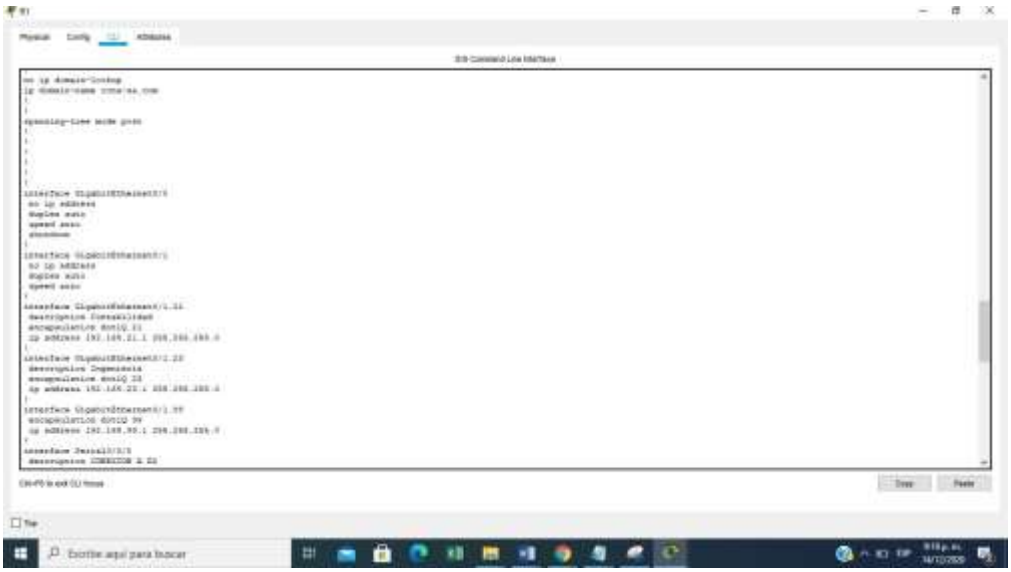
Figura 58. Configuracion del R1 parte 1



Fuente: Autor

La anterior imagen es la numero 1 de 4 imágenes de la configuracion de R1

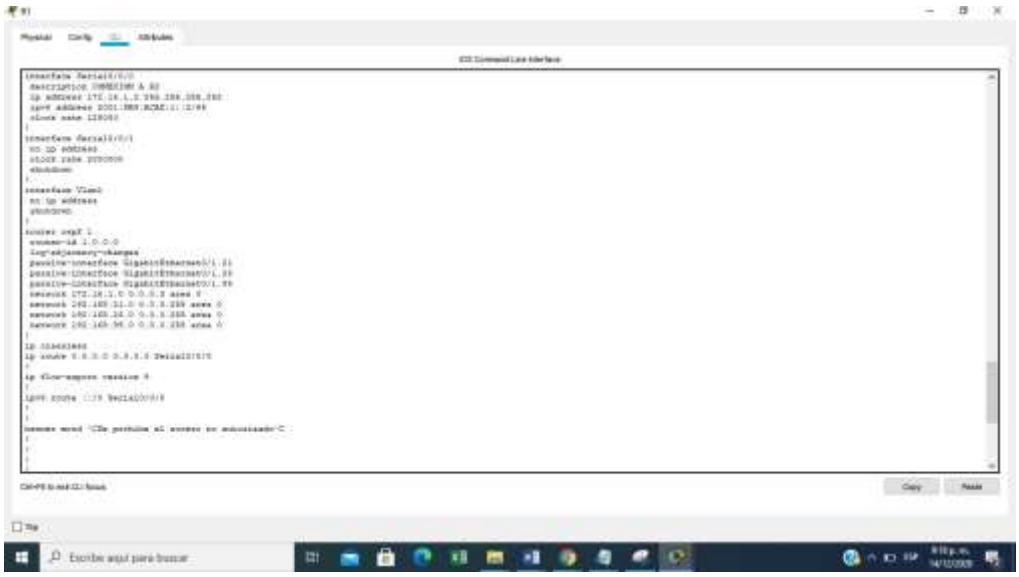
Figura 59. Configuracion del R1 parte 2



Fuente: Autor

La anterior imagen es la numero 2 de 4 imágenes de la configuracion de R1

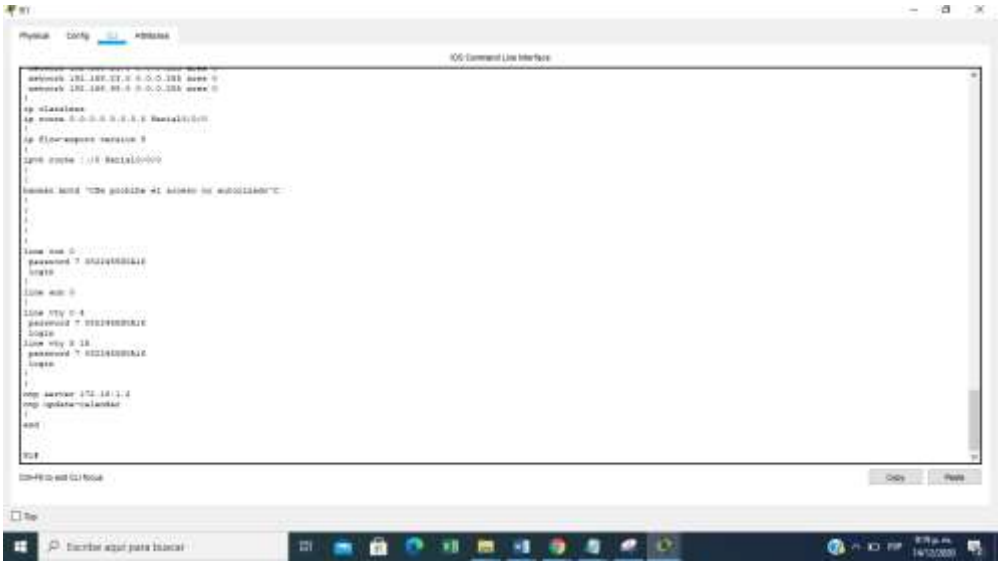
Figura 60. Configuracion del R1 parte 3



Fuente: Autor

La anterior imagen es la numero 3 de 4 imágenes de la configuracion de R1

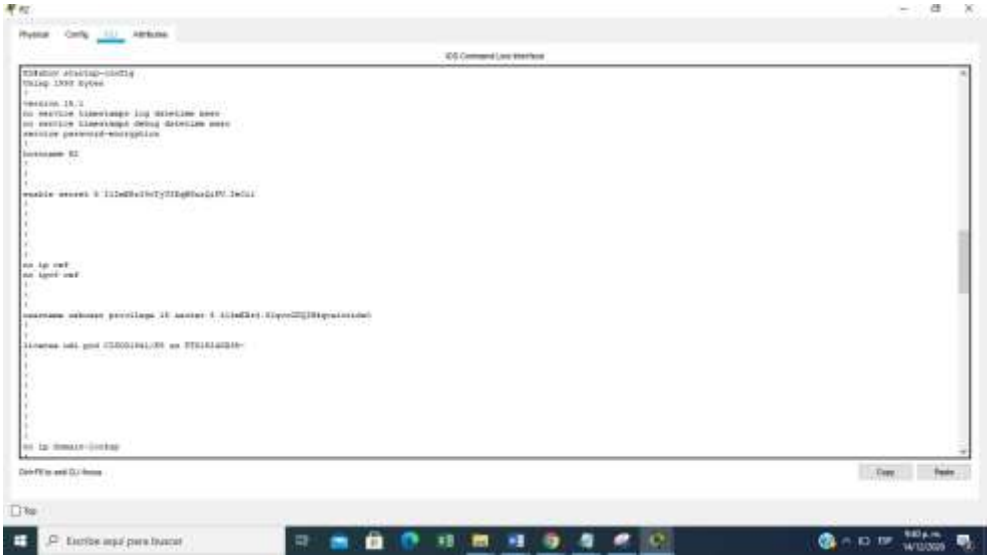
Figura 61. Configuracion del R1 parte 4



Fuente: Autor

La anterior imagen es la numero 4 de 4 imágenes de la configuracion de R1

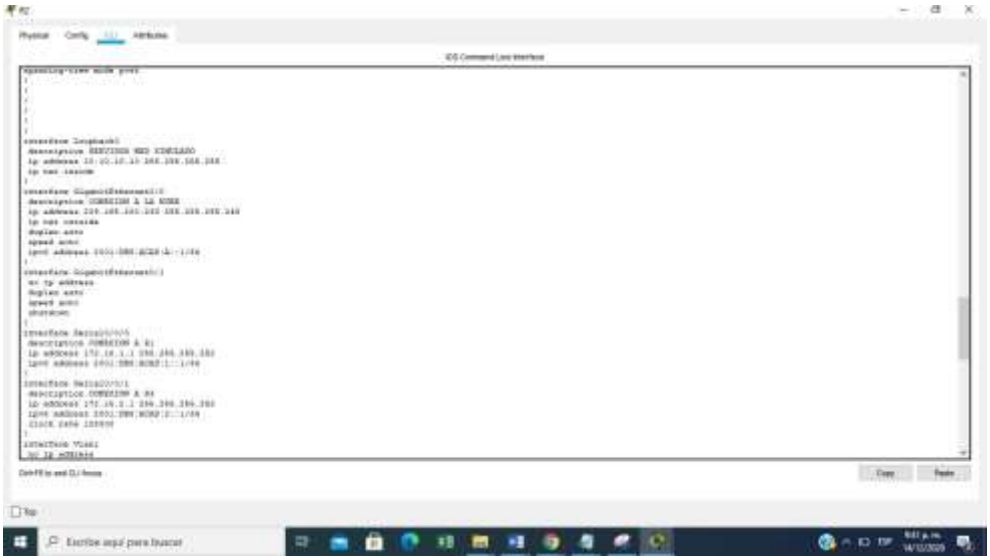
Figura 62. Configuracion del R2 parte 1



Fuente: Autor

La anterior imagen es la numero 1 de 4 imágenes de la configuracion de R2

Figura 63. Configuracion del R2 parte 2



Fuente: Autor

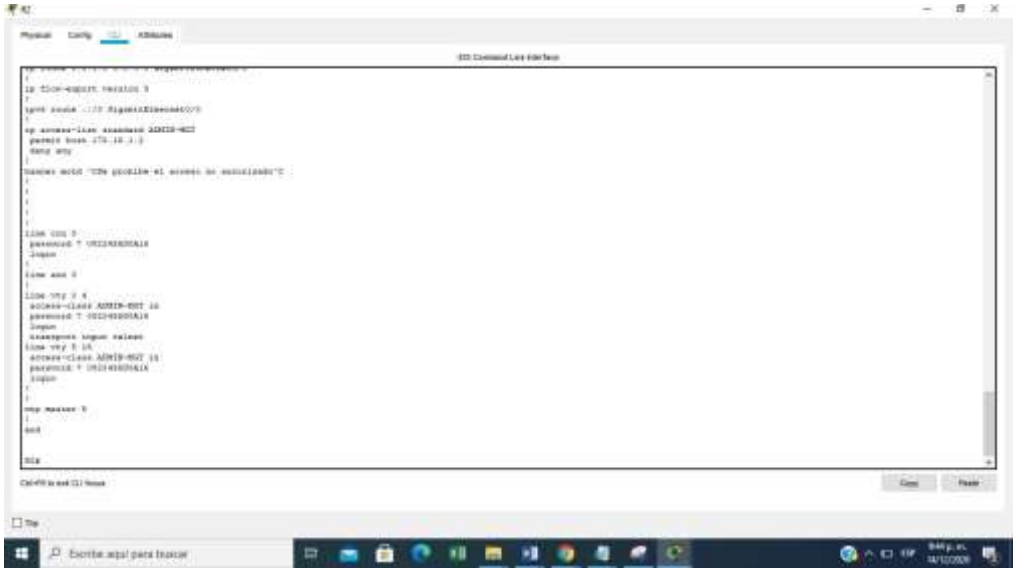
La anterior imagen es la numero 2 de 4 imágenes de la configuracion de R2

Figura 64. Configuracion del R2 parte 3

Fuente: Autor

La anterior imagen es la numero 3 de 4 imágenes de la configuracion de R2

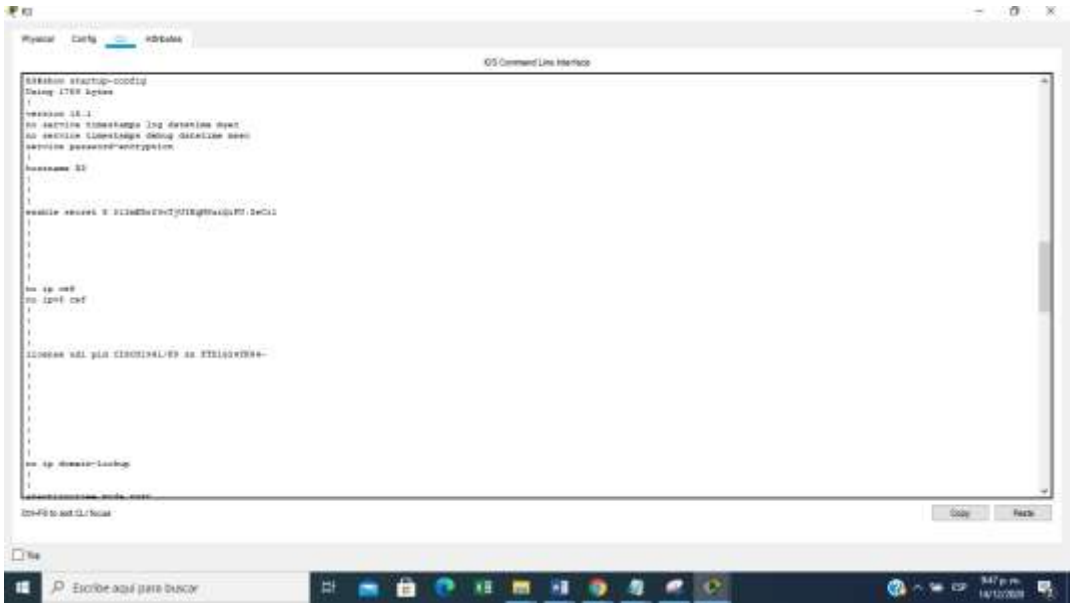
Figura 65. Configuracion del R2 parte 4



Fuente: Autor

La anterior imagen es la numero 4 de 4 imágenes de la configuracion de R2

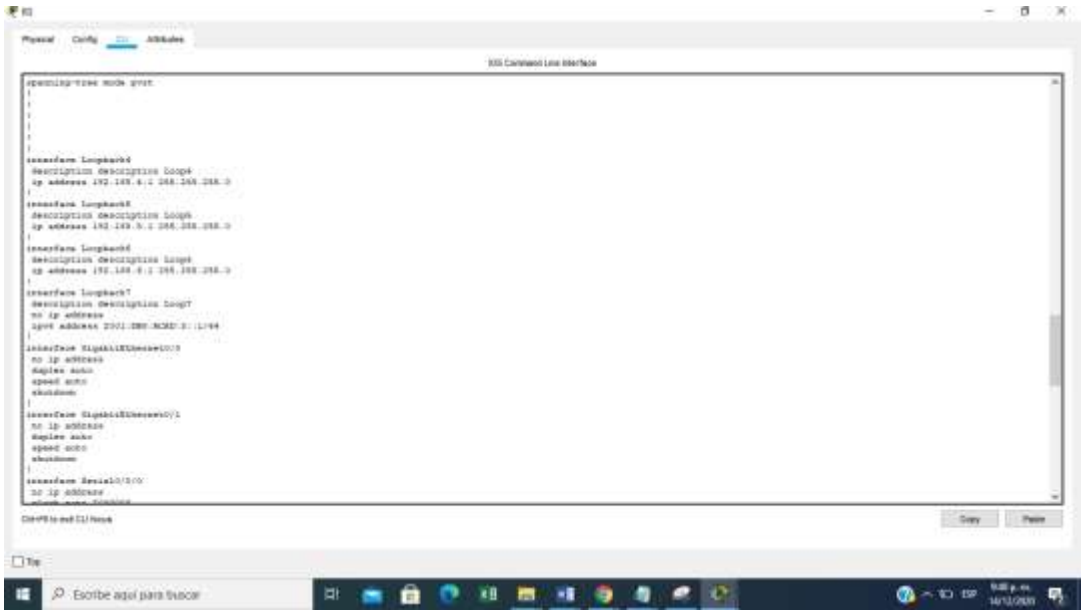
Figura 66. Configuracion del R3 parte 1



Fuente: Autor

La anterior imagen es la numero 1 de 4 imágenes de la configuracion de R3

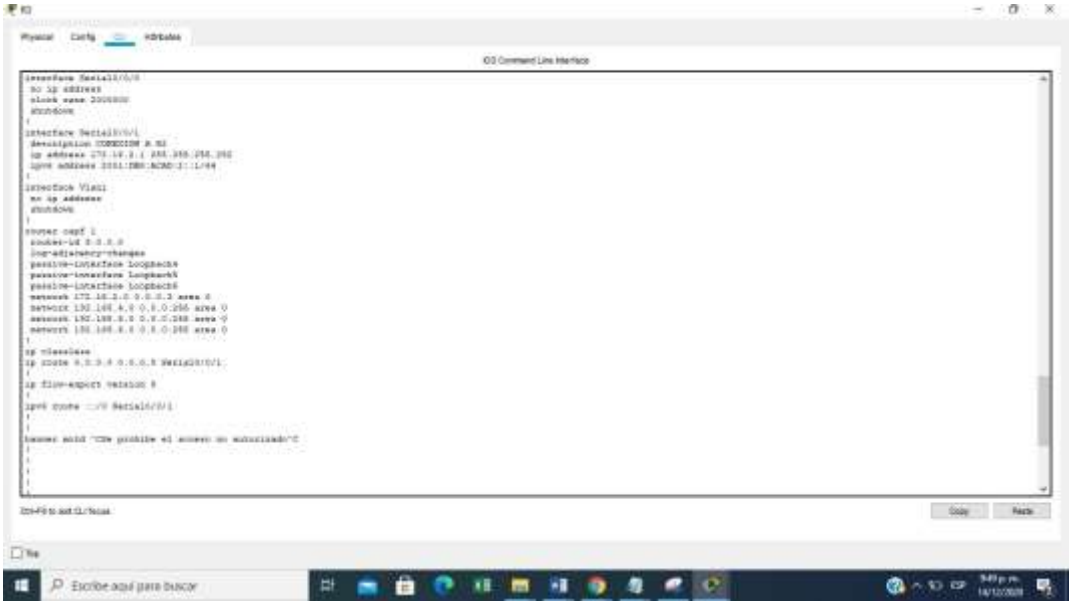
Figura 67. Configuracion del R3 parte 2



Fuente: Autor

La anterior imagen es la numero 2 de 4 imágenes de la configuracion de R3

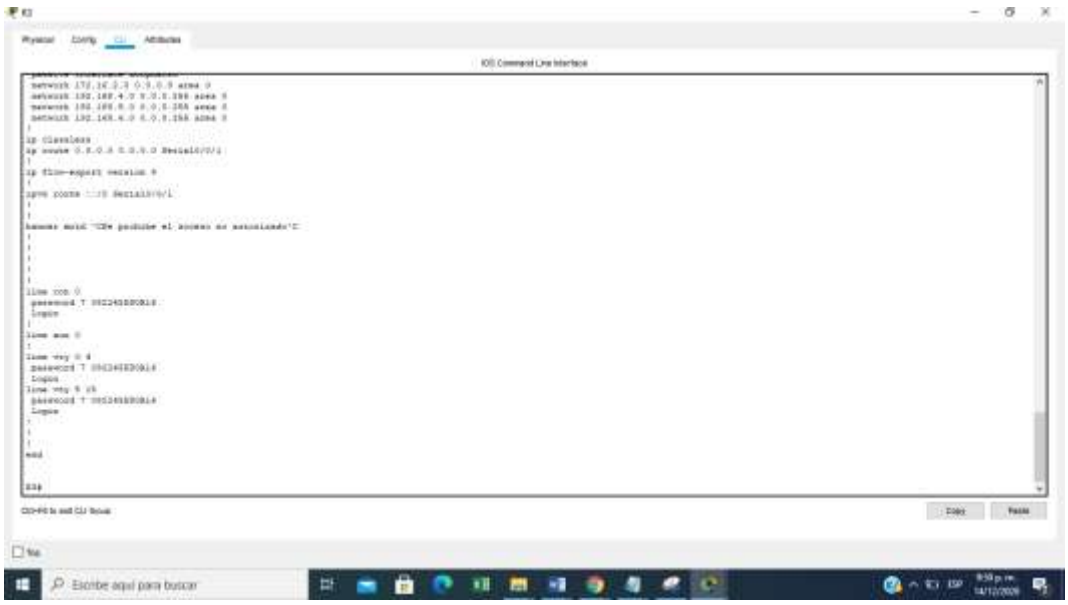
Figura 68. Configuracion del R3 parte 3



Fuente: Autor

La anterior imagen es la numero 3 de 4 imágenes de la configuracion de R3

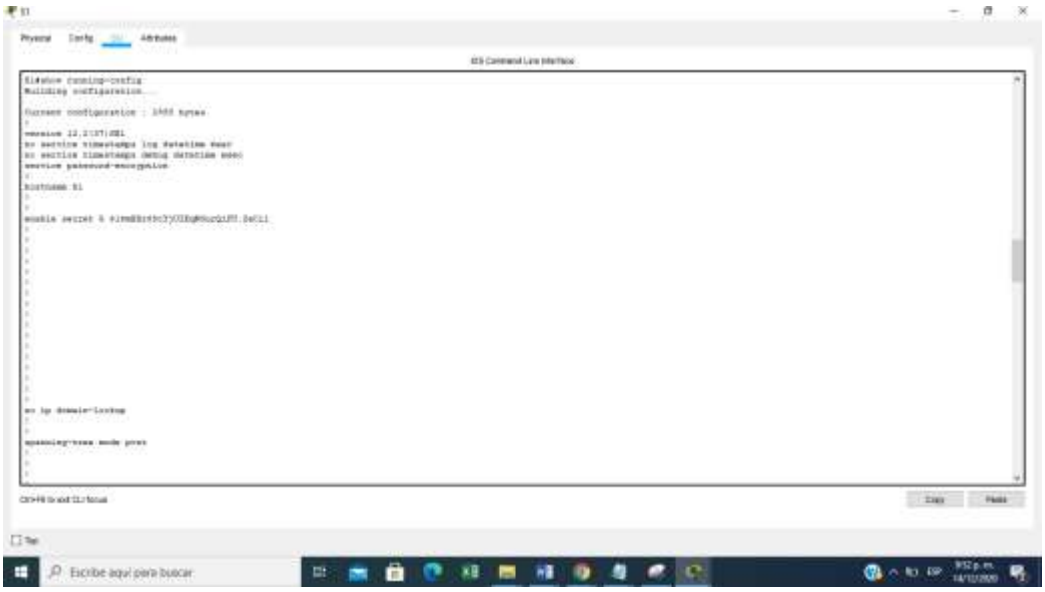
Figura 69. Configuracion del R3 parte 4



Fuente: Autor

La anterior imagen es la numero 4 de 4 imágenes de la configuracion de R3

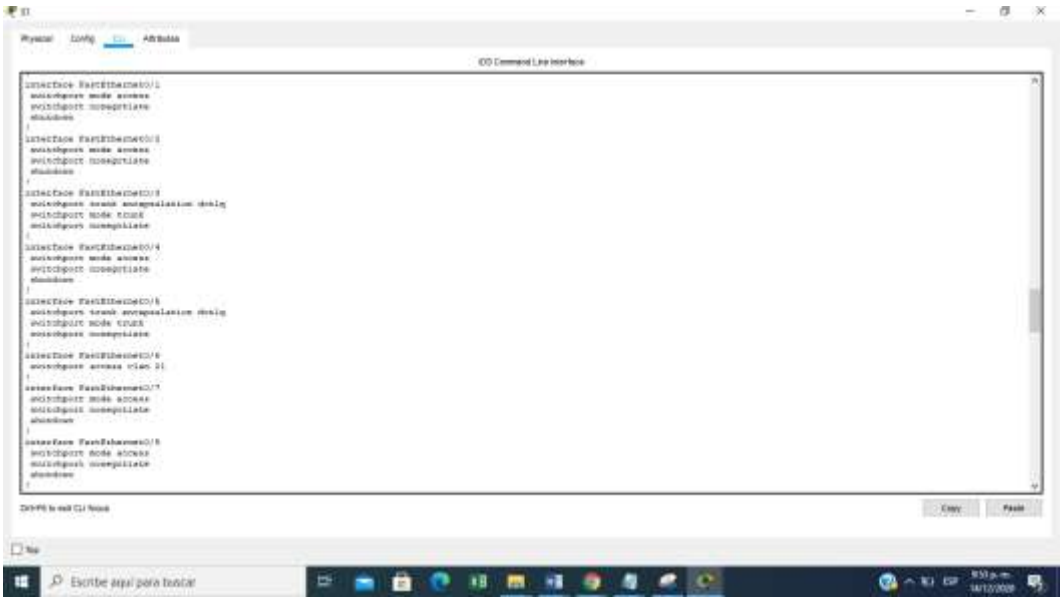
Figura 70. Configuracion del S1 parte 1



Fuente: Autor

La anterior imagen es la numero 1 de 6 imágenes de la configuracion de S1

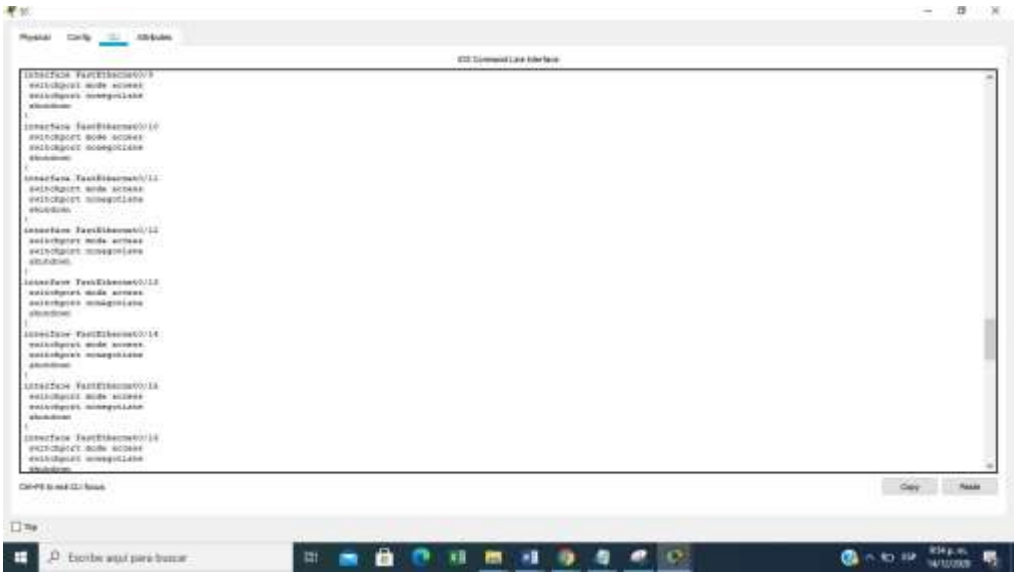
Figura 71. Configuracion del S1 parte 2



Fuente: Autor

La anterior imagen es la numero 2 de 6 imágenes de la configuracion de S1

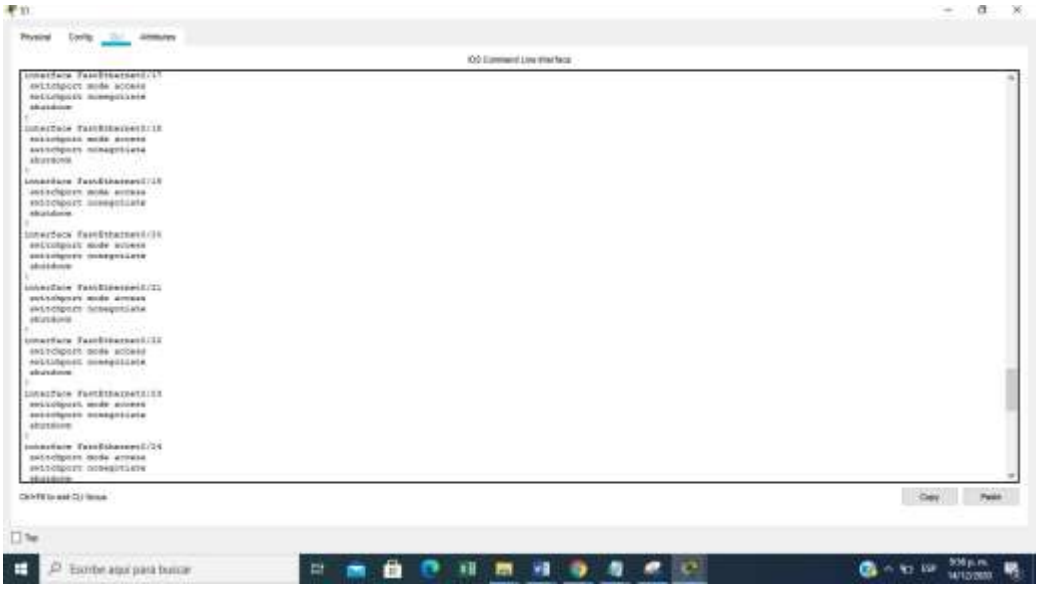
Figura 72. Configuracion del S1 parte 3



Fuente: Autor

La anterior imagen es la numero 3 de 6 imágenes de la configuracion de S1

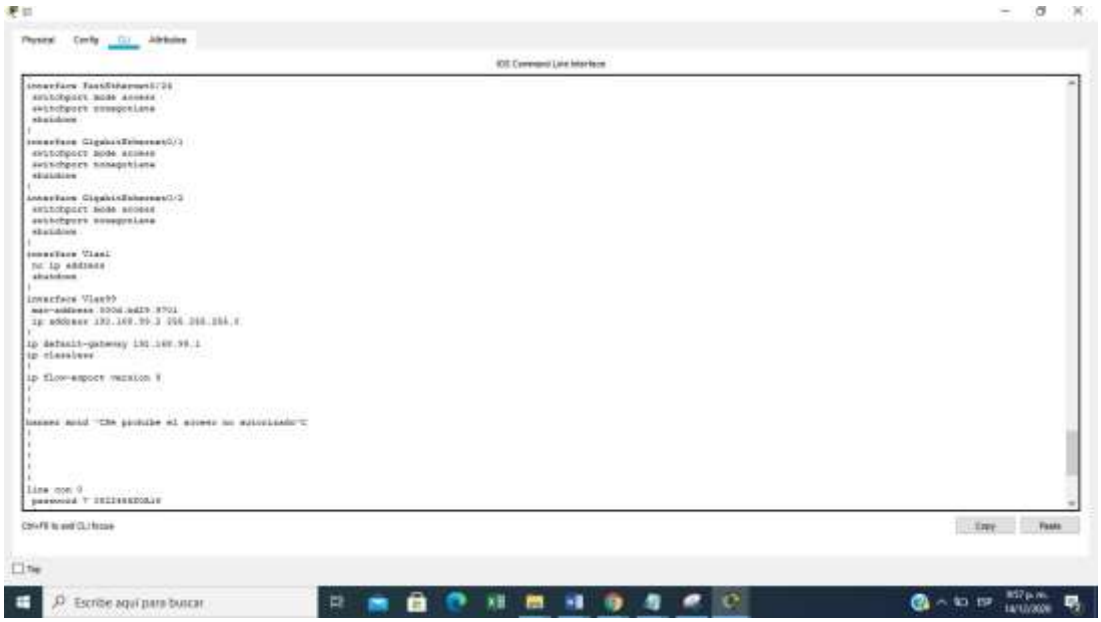
Figura 73. Configuracion del S1 parte 4



Fuente: Autor

La anterior imagen es la numero 4 de 6 imágenes de la configuracion de S1

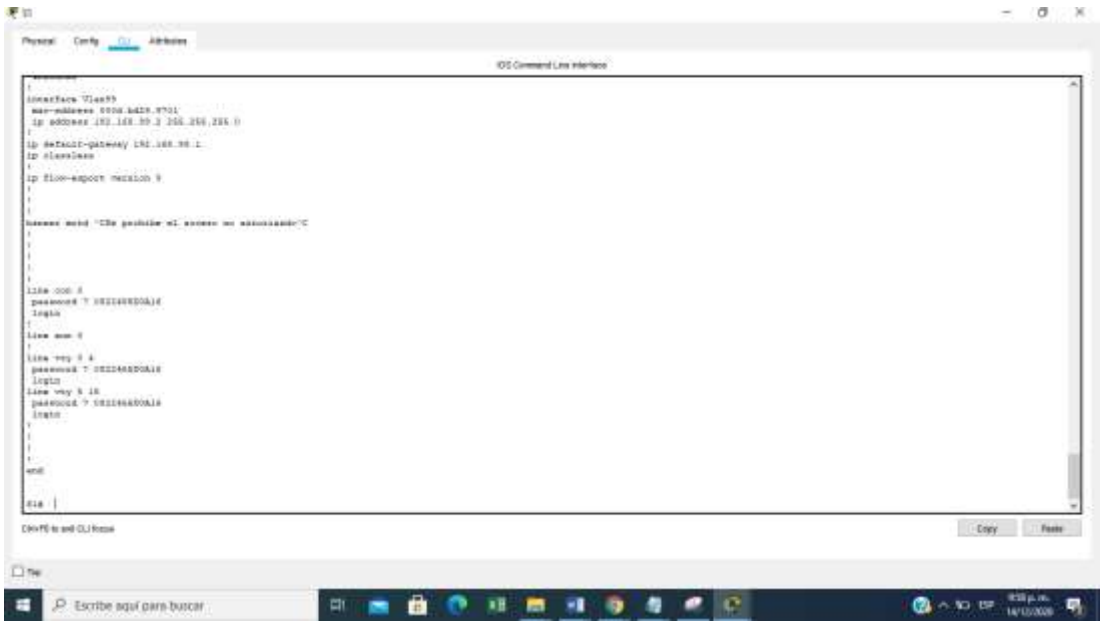
Figura 74. Configuracion del S1 parte 5



Fuente: Autor

La anterior imagen es la numero 5 de 6 imágenes de la configuracion de S1

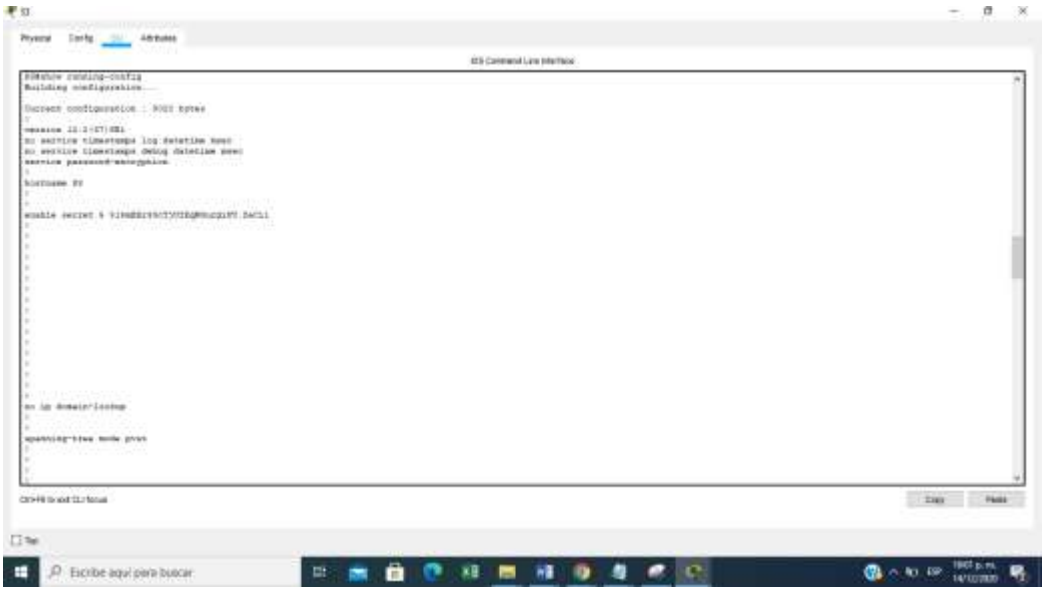
Figura 75. Configuracion del S1 parte 6



Fuente: Autor

La anterior imagen es la numero 6 de 6 imágenes de la configuracion de S1

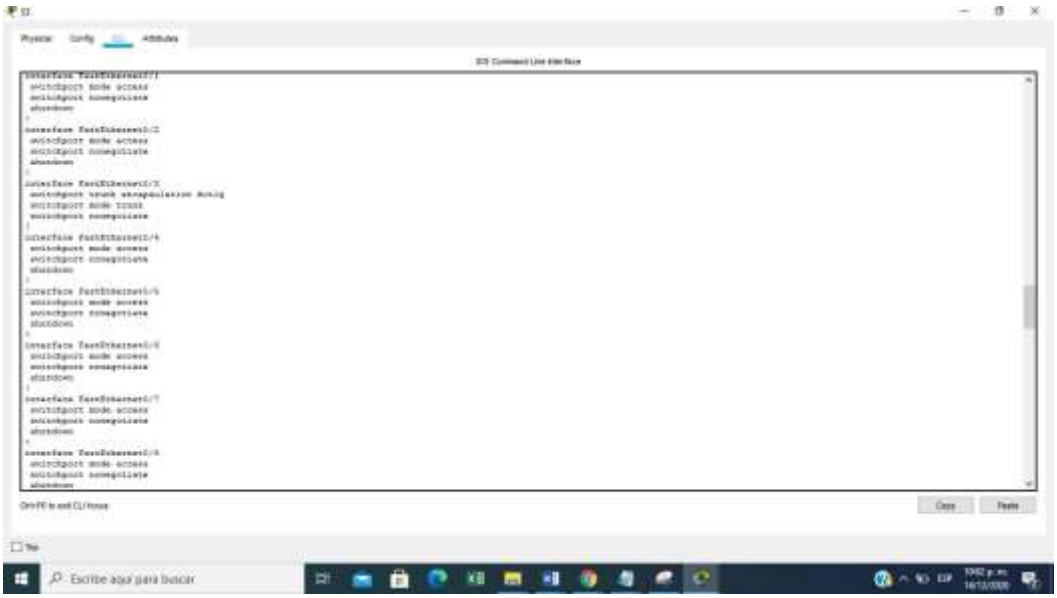
Figura 76. Configuracion del S3 parte 1



Fuente: Autor

La anterior imagen es la numero 1 de 6 imágenes de la configuracion de S3

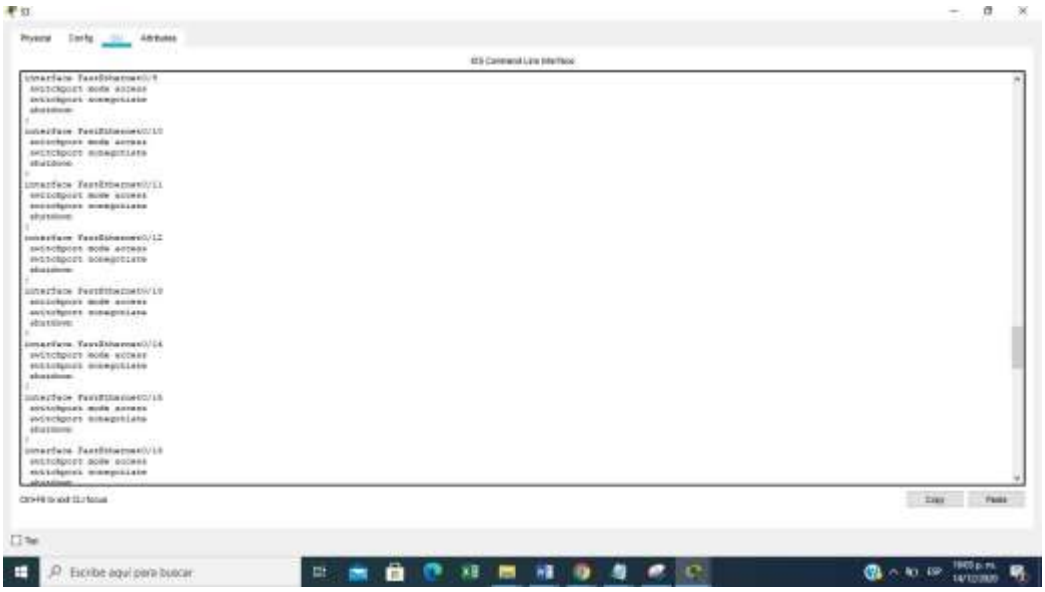
Figura 77. Configuracion del S3 parte 2



Fuente: Autor

La anterior imagen es la numero 2 de 6 imágenes de la configuracion de S3

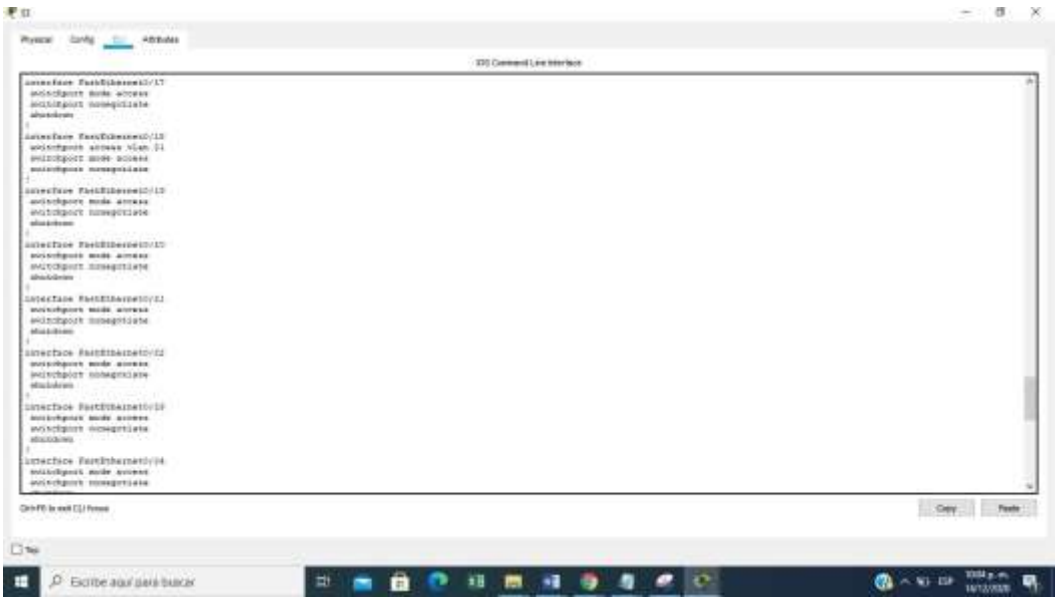
Figura 78. Configuracion del S3 parte 3



Fuente: Autor

La anterior imagen es la numero 3 de 6 imágenes de la configuracion de S3

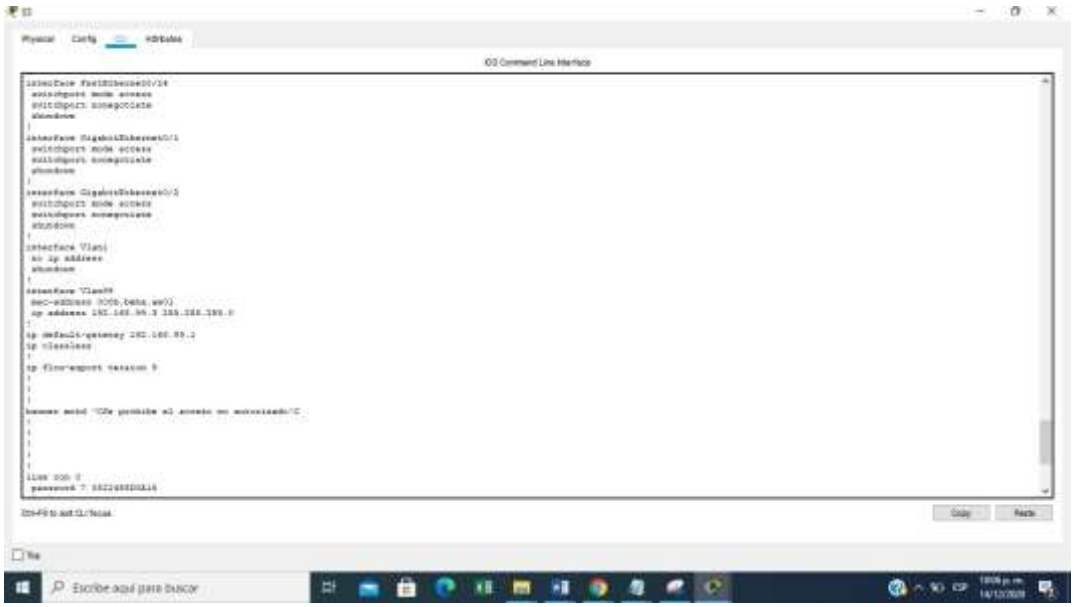
Figura 79. Configuracion del S3 parte 4



Fuente: Autor

La anterior imagen es la numero 4 de 6 imágenes de la configuracion de S3

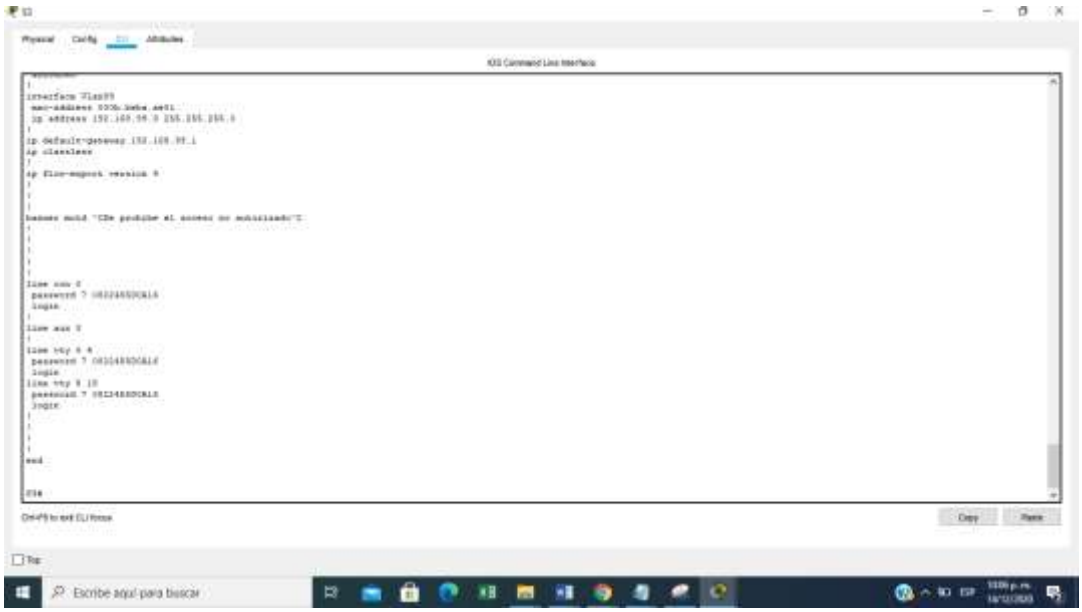
Figura 80. Configuracion del S3 parte 5



Fuente: Autor

La anterior imagen es la numero 5 de 6 imágenes de la configuracion de S3

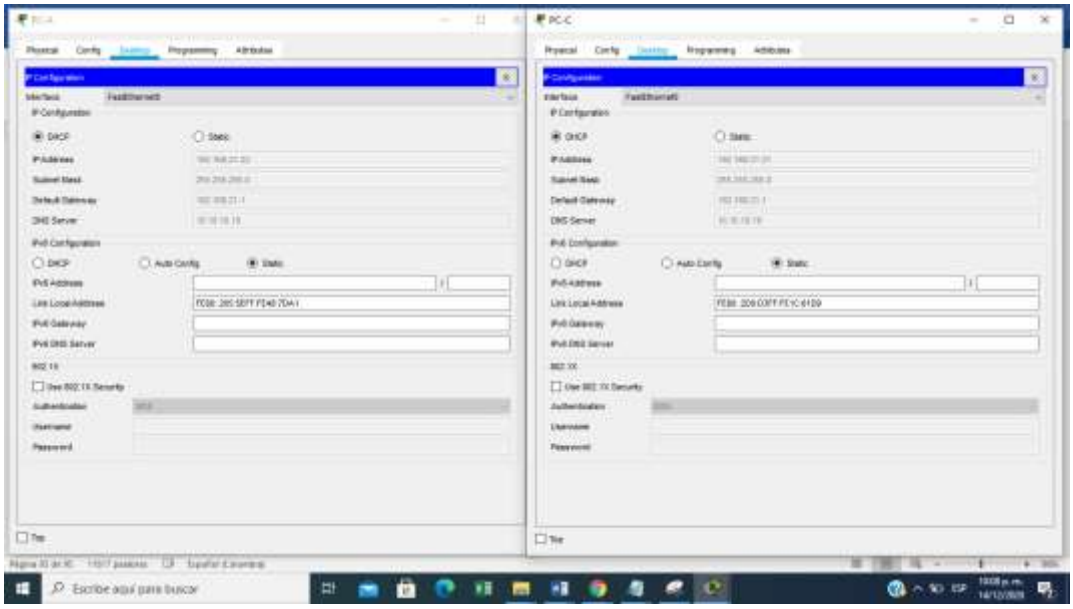
Figura 81. Configuracion del S3 parte 6



Fuente: Autor

La anterior imagen es la numero 6 de 6 imágenes de la configuracion de S3

Figura 82. Configuracion del S3 parte 6



Fuente: Autor

Direccionamiento DHCP del PC-A a la izquierda de la imagen y direccionamiento DHCP del PC-C a la derecha.

CONCLUSIONES

Del ejercicio de crear y probar la conectividad entre las VLANs acompañado por la configuracion de encapsulamiento Dot1Q, llegamos a concluir que el uso de estas dos tecnologias es un modo economico de implementar varias redes sobre la misma red fisica lo cual reduce gastos en cableado y otros equipos de red. Con lo aprendido tambien inferimos que el uso de las subinterfaces con sus respectivas VLANs encapsuladas, hacen mas facil la administracion y el mantenimiento de la red debido a la reduccion de la cantidad de equipos que ya mencionamos.

Un aspecto importante de este desarrollo ha sido la configuracion del Etherchannel en el escenario 1, este paso tiene importantes conclusiones entre esas vimos lo clave que resulta implementar un etherchannel en un enlace troncal que comunica dos switchs, teniendo en cuenta la agrupacion de las capacidades de cada una de las interfaces que comforman el canal, el trancito de informacion se ve beneficiado por un ancho de banda mayor comparado con sola interface, garantizando que halla un buen flujo de datos entre dispositivos que se encuentran conectados commutadores separados.

La configuracion del servicio DHCP en un router, resuelto tambien en este desarrollo, nos mostró que los equipos de computo se configuran automaticamente una vez esten conectados en la red tras haber configurado correctamente este servicio en el router; a pesar de que en el ejercicio son muy pocos los computadores conectados en la red, al escalar la red a una red muchisimo mas grande con una gran cantidad de dispositivos, podemos imaginar que la conexion manual de todos los diaspositivos a la red seria muy tediosa y sijeta a muchos errores humanos. De aquí podemos extaer la importancia del servicio DHCP, el cual nos dio la solucion de este planteamiento representado en la pequeña red del escenario 1.

Con la configuracion del protocolo de enrutamiento dinamico OSPF y las pruebas realizadas verificamos que con este protocolo se garantiza automaticamente las mejores rutas de conexión entre los router de una red incluyendo la mejor alternativa en el caso de que alguna ruta falle.

Finalmente concluimos sobre las listas de control de acceso ACLs; en estas aprendimos la forma como podemos bloquear o permitir el trafico de los usuarios a algunos recursos especificos, lo cual resulta en una mejora en la seguridad de la red, con estas podemos configurar en el routers estrategicos las reglas que protege la red de la circulacion de paquetes que son confidenciales para ciertos dispositivos.

BIBLIOGRAFIA

CISCO. (2019). Redes Conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4

CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5

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

ANEXOS

ANEXO1:

Enlace de descarga del archivo de simulación del escenario 1:
https://drive.google.com/file/d/12aPY76aiTAkbw_H0d0pHWSXfBPPI8419/view?usp=sharing

ANEXO2:

Enlace de descarga del archivo de simulación del escenario 2:
https://drive.google.com/file/d/1SLIBc8kRMy4OhqLuaGYvWoOdI6IfLfkM/view?usp=sharing

ANEXO3:

Enlace de descarga del artículo cientifico:
https://drive.google.com/file/d/1bKLKybqeJicwuHT-rNC9H29Y_CjpqG-_/view?usp=sharing

ANEXO4:

Enlace del video de sustentacion:
https://youtu.be/5tay4n5GQQI