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

JHOSER QUINTANA PULIDO

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

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

JHOSER QUINTANA PULIDO

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

TUTOR:

EDIGO EDISON RAMIREZ CLAROS

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

NOTA DE ACEPTACION

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Neiva, 30 de noviembre del 2020

AGRADECIMIENTOS

Agradecerle a DIOS por la oportunidad de adquirir conocimientos y mantenerme con salud, a mis tutores de la línea de electrónica por el apoyo brindado y la motivación dada, a cada uno de las personas que fueron mis compañeros en este proceso por apoyo y la confianza que otorgaron en cada una de las responsabilidades de la educación a distancias.

Quiero agradecerle especialmente a mi madre por estar apoyándome, por todo el esfuerzo y la dedicación que ha tenido para mí y mis hermanas.

También a mi esposa por estar hay en mis momentos más difíciles y complicados por entender y darme alientos en cada momento. Gracias por estar siempre a mi lado apoyándome.

Muchas gracias.

ATT:

Jhoser Quintana Pulido.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ENRUTAMIENTO: se define como la función que realiza la búsqueda de un camino adecuado entre múltiples posibilidades de conexión en una red

UDP: Es el protocolo de datagramas de usuario que es utilizado para el intercambio de datagramas entre usuarios. En el modelo OSI es se encuentra entre el protocolo de transporte.

ETHERCHANNEL: Es una tecnología que permite la agrupación lógica de múltiples enlaces ethernet físicos, con el fin de tener un enlace troncal de alta velocidad. Está basada en el estándar IEEE 802.3

IPV6: Es la versión 6 del protocolo de internet, el cual se diseñó para realizar la sustitución de IPv4 por agotamiento de dirección.

TRUNKING: Es una función utilizada para conectar dos dispositivos, tales como switch o router en paralelo. Lo que permite un aumento exponencial en el ancho de banda para comunicación entre ellos.

RESUMEN

En este documento se realiza el análisis del conocimiento adquirido, el cual es puesto aprueba por medio de escenarios de situaciones reales que nos ofrece Cisco en su curso en CCNA. Se aplican dos escenarios donde por medio de redes LAN/Wan con topología diferente para cada caso y utilizando tecnología de enrutamiento con la aplicación de sus diversos protocolos en cada dispositivo.

Se adquirieren habilidades importantes para el desarrollo de redes por medio del aprendizaje brindado en diplomado de profundización en CCNA, Lo cual permite la solución adecuada de la prueba de habilidades prácticas, donde se tiene como objetivo la solución de problemas de networking para cada caso planteado. aquí se encuentran topologías, configuraciones, conmutación entre dispositivos y redes. Para esta solución se aplican múltiples comandos de consola que permiten la verificación de la conectividad entre los equipos, y la correcta aplicación de trunkig, etherchannel y creación de vlan las cuales corresponden a solo algunas de las soluciones planteadas para casa caso.

Una de las partes de más importancia de una red es la de seguridad, pues esta solución al problema no es ajena a esto pues se implementan protocolos de seguridad y se utilizan comandos que nos permiten realizar, restricción de accesos, la asignación y encriptación de contraseñas, creación de mensaje de advertencias. Para cada escenario desarrollado se documenta, comprueba y se verifica cada uno de los pasos realizados, para dar una correcta solución a la prueba de habilidades.

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

ABSTRACT

In this document the analysis of the acquired knowledge is carried out, which is approved through scenarios of real situations that Cisco offers us in its course at CCNA. Two scenarios are applied where through LAN / Wan networks with different topology for each case and using routing technology with the application of its various protocols in each device.

Important skills are acquired for the development of networks through the learning provided in the deepening diploma in CCNA, which allows the adequate solution of the practical skills test, where the objective is to solve networking problems for each case raised. here are topologies, configurations, switching between devices and networks. For this solution, multiple console commands are applied that allow the verification of the connectivity between the computers, and the correct application of trunkig, etherchannel and creation of vlan, which correspond to only some of the solutions proposed for each case.

One of the most important parts of a network is security, since this solution to the problem is not alien to this, since security protocols are implemented and commands are used that allow us to carry out access restriction, the assignment and encryption of passwords, warning message creation. For each scenario developed, each of the steps performed is documented, checked and verified, to give a correct solution to the skills test.

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

INTRODUCCIÓN

Este documento presenta la solución del escenario 1 de la prueba de habilidades la cual hace parte de la evaluación final del diplomado de profundización CISCO CCNA, esta actividad está basada en la metodología de solución a problemas reales, mediante la implementación de software de simulación.

Para la solución del escenario 1, se utiliza el software de simulación Packet tracer desarrollado por Cisco Systems. En este entorno se simula la topología proporciona y se realiza las configuraciones básicas de cada equipo, se aplican los protocolos necesarios para establecer comunicaciones entre los dispositivos y se verifica cado uno de los pasos descritos para la solución del problema.

También se realiza la descripción detalla del código de comandos implementados y pantallazos de su ejecución, evidenciando la solución al problema.

DESARROLLO

ESCENARIO 1

Figura 1:Topologia 1.

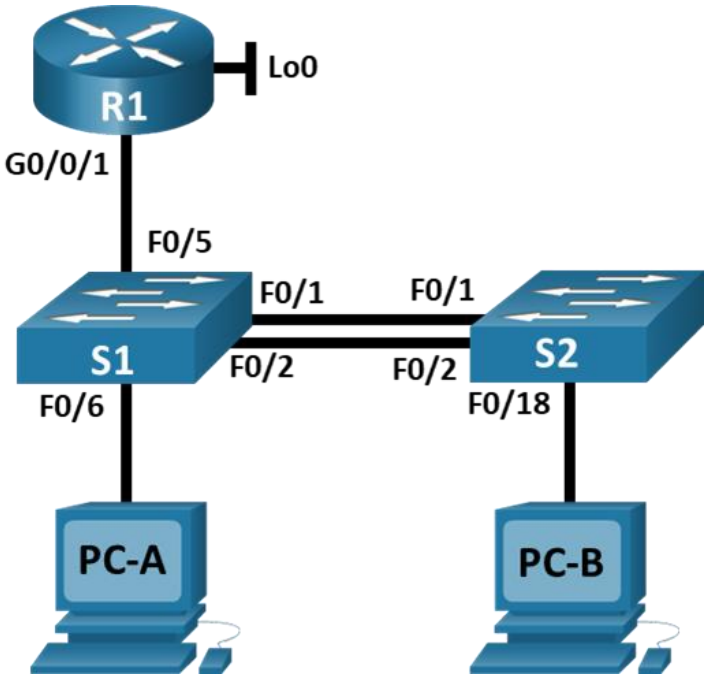


Tabla 1: Vlan

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

Tabla 2: ASIGNACION DE IP

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

La topología y las tablas anteriormente vistas son parte del requisito para el desarrollo de la esta actividad.

1.1. Inicializar y Recargar y Configurar aspectos básicos de los dispositivos

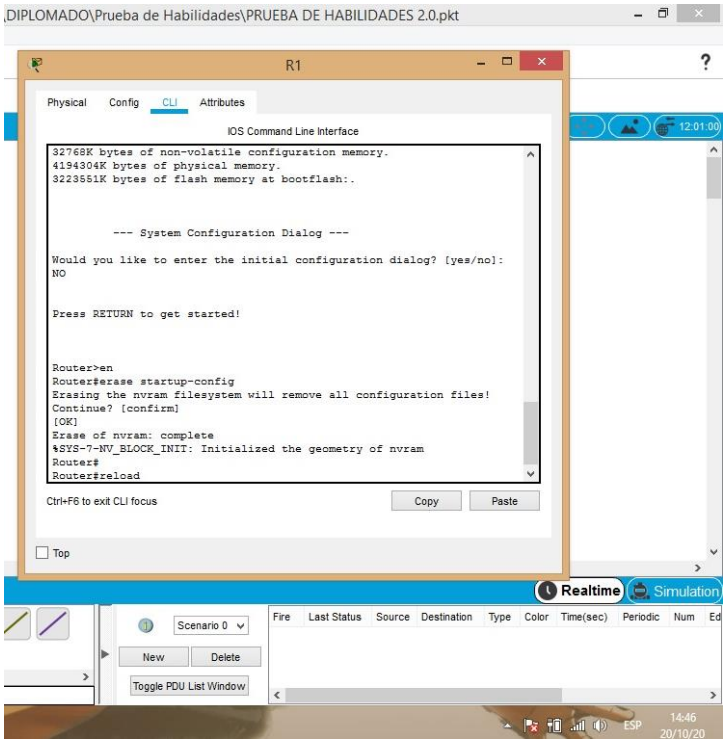
1.1.1. Inicializar y volver a cargar el router y el switch

Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos.

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

BORRADO Y RECARGA DEL ROUTER

Figura 2. Reset Router



Fuente: Autor.

Tabla 3.Codigo para Borrado y Recargue del Router

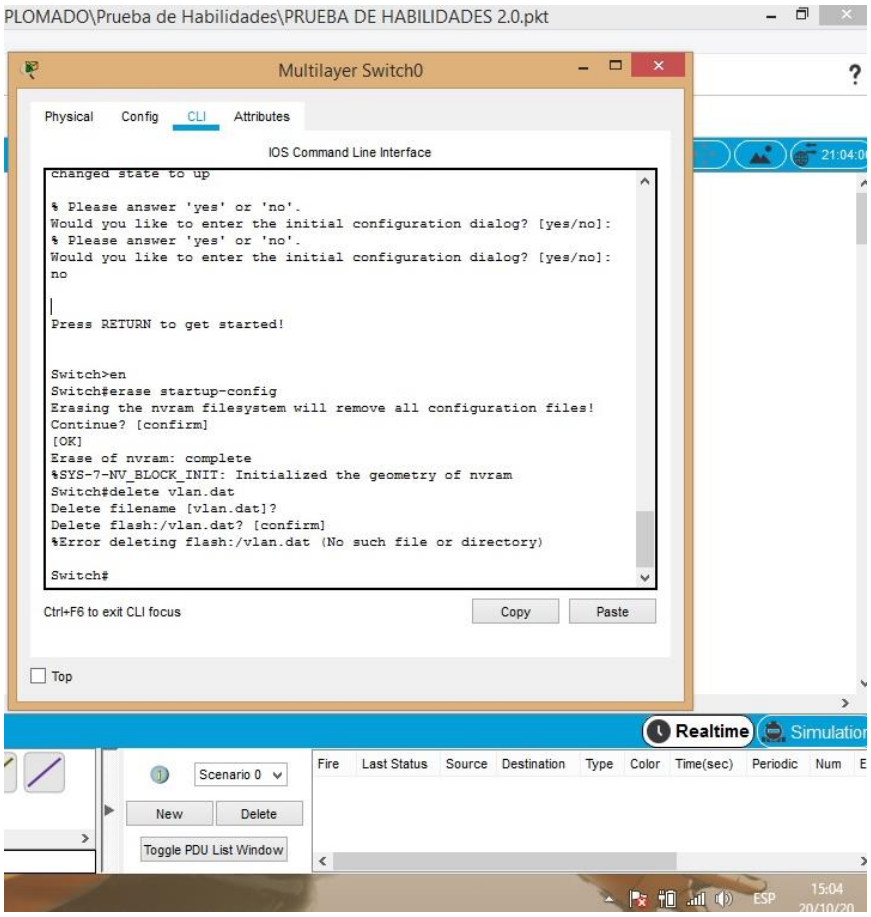
Código	**Descripción**
Router>en	línea de ingreso al modo exec
Router#erase startup-config línea para borrar la configuración inicial Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK]	se confirma con un enter
Router#	modo exec

Router#reload	reiniciar el router
Proceed with reload? [confirm]	confirmación de reinicio
Initializing Hardware ...	iniciando el dispositivo
Would you like to enter the initial configuration dialog? [yes/no]:	Esta línea indica que el Router no tiene configuración guardada.
No	respondemos

En la tabla 3 podemos observar el borrado y recargue del Router y la descripción de cada comando.

BORRADO Y RECARGA DE LOS SWITCH 1 y 2.

Figura 3. Reset switch



Fuente: Autor.

Tabla 4. Código para Reset del switch

Código	Descripción
Switch>en	línea de ingreso al modo exec
Switch#erase startup-config	línea para borrar la configuración inicial
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK]	se confirma con un enter
Switch#delete vlan.dat	
Delete filename [vlan.dat]? línea para preguntar si desea hacerlo	Comando para borrar el archivo vlan
Delete flash:/vlan.dat? [confirm]	enter para confirmar
%Error deleting flash:/vlan.dat (No such file or directory)	No hay archivo
Switch#reload	reiniciar el router
Proceed with reload? [confirm]	confirmar reinicio enter
Would you like to enter the initial configuration dialog? [yes/no]:	esta línea indica que el Router no tiene configuración guardada.
No	respondemos

En la tabla 4 podemos observar el borrado y recargue del Switch y la descripción de cada comando.

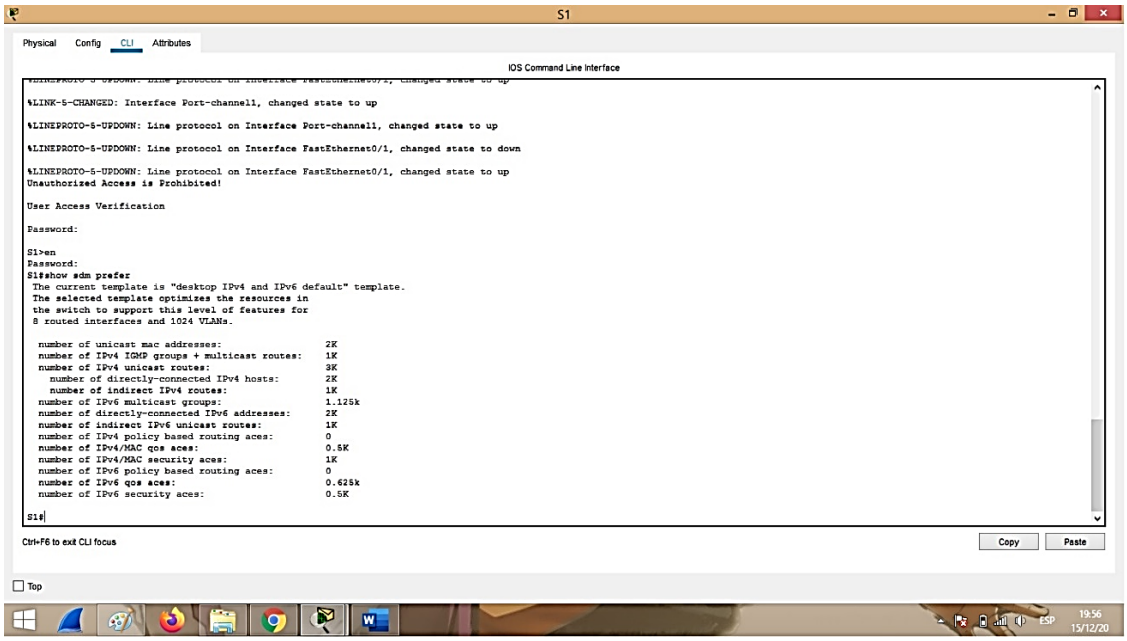
Las líneas de código anteriormente observadas y documentadas nos muestran el borrado del archivo de configuración de inicio, el borrado del archivo de configuración de vlan y el reinicio del switch. Respecto a la plantilla SDM en el tipo de switch que utilizamos (switch 3560) para este laboratorio no fue necesario activar la plantilla ya que switch capa 3 y soportan IPv6. Las siguientes líneas de código evidencian y respaldan lo anteriormente dicho.

Tabla 5. Código para verificación soporte IPV6

Código	Descripción
Switch#show sdm prefer	nos permite verificar si soporta IPV6

En la tabla 5. Se puede observar la ejecución del comando para verificar si el swicth soporta Ipv6.

Figura 4. Comprobación show sdm prefer

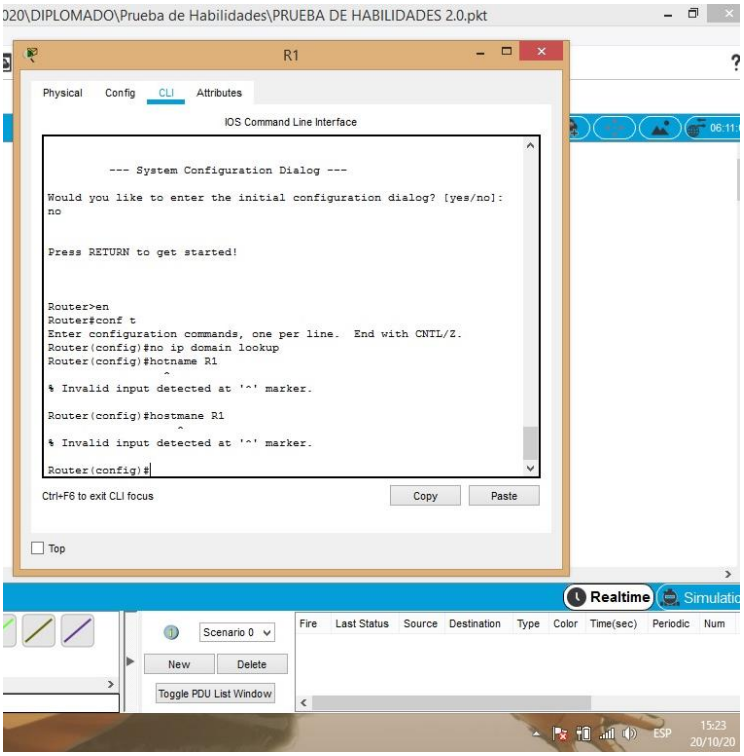


Fuente: Autor.

En la figura anterior observamos la comprobación del comando Show sdm prefer. El cual nos permite observa lasi la plantilla sdm esta activa para las dos versiones del direccionamiento IPv4 y IPv6, o si el switch soporta la versión 6 del direccionamiento.

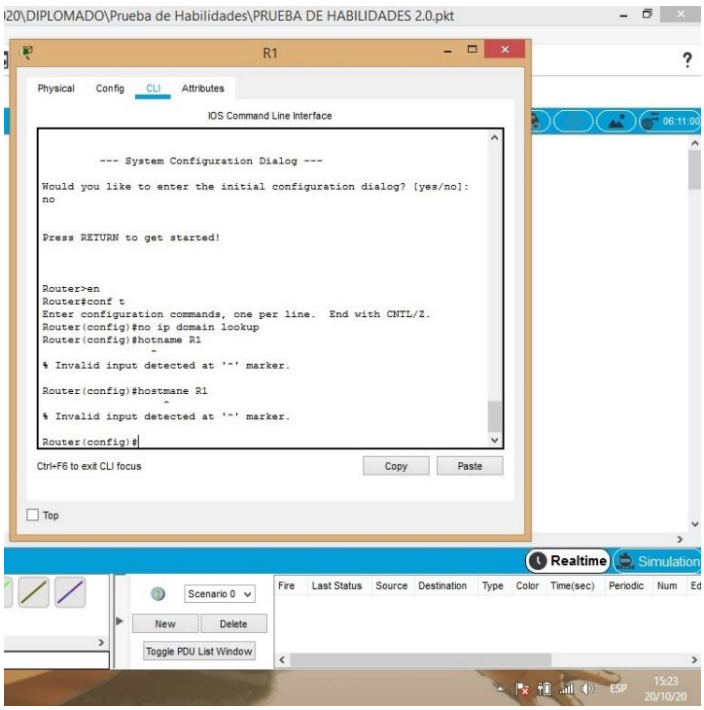
1.1.2 CONFIGURAR R1

Figura 5.Configuración 1 R1



Fuente: Autor.

Figura 6.Configuración 2 R1



Fuente: Autor.

En las figuras 5-6 podemos Observar la ejecución de los comandos que permiten la realización de las configuraciones iniciales.

Tabla 6. Código Configuración de R1

Código	Descripción
Router>en	ingreso modo exec
Router#conf t Enter configuration commands, one per line. End with CNTL/Z.	ingreso al modo de configuración
Router(config)#no ip domain lookup	se desactiva la búsqueda de DNS
Router(config)#hostname R1	Asignacion de nombre al router
R1(config)# ip domain-name ccna-lab.com	Asignacion de nombre de dominio
R1(config)#enable secret ciscoenpass	contraseña privilegiada exec
R1(config)#line console 0	línea de ingreso al modo consola
R1(config-line)#password ciscoconpass	Asignacion de contraseña de consola
R1(config-line)# login	permite establecer la contraseña
R1(config)#security passwords min-length 10	limitación de caracteres mínimos de contraseñas
R1(config)#username admin secret admin1pass	creación de usuario en base local
R1(config)# line vty 0	establecer login en base de datos local
R1(config-line)# login local	permite establecer la contraseña
R1(config-line)#transport input ssh	configuración de entrada ssh
R1(config)#service password-encryption	encriptación de contraseñas
R1(config)# banner motd #ACCESO ESTA PROHIBIDO#	configuración de mensaje
R1(config)#IPV6 unicast-routing	activación de IPV6
R1(config)# int g0/0/1.2	ingreso a la subinterfaz
R1(config-subif)#encapsulation dot1q 2	encapsulación de la vlan 2
R1(config-subif)#description Bikes	descripción
R1(config-subif)#ip address 10.19.8.1 255.255.255.192	asignación de ipv4
R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64	asignación de ipv6

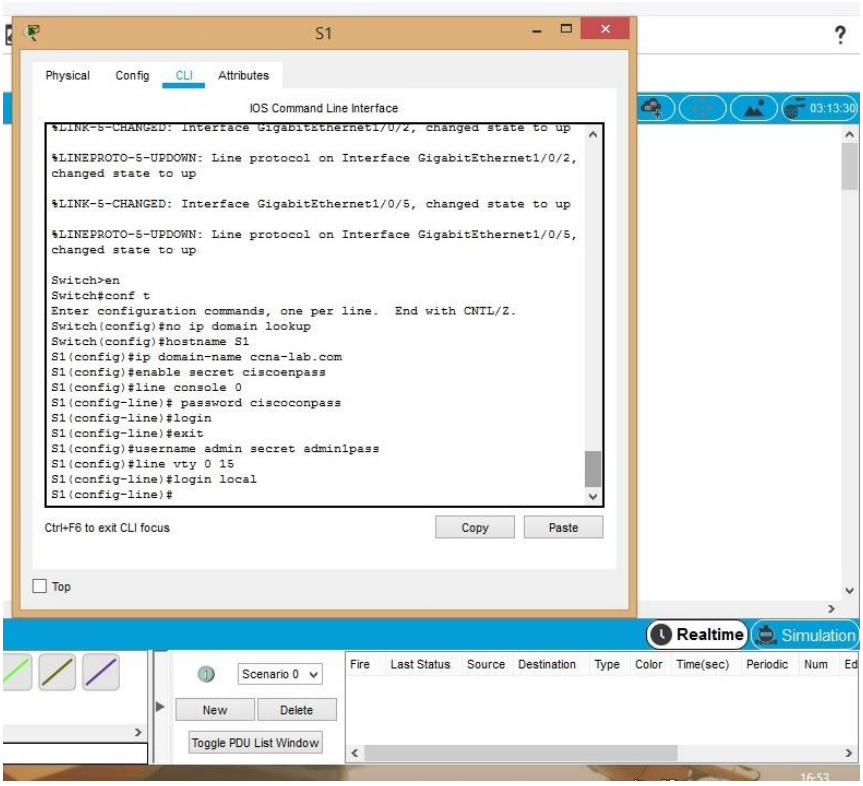
R1(config-subif)#ipv6 address fe80::1 link-local	asignación de la link-local
R1(config-subif)#	
R1(config-subif)# int g0/0/1.3	ingreso a la subinterfaz
R1(config-subif)#encapsulation dot1q 3	encapsulación de la vlan 3
R1(config-subif)#description Trikes	descripción
R1(config-subif)#ip address 10.19.8.65 255.255.255.224	asignación de ipv4
R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64	asignación de ipv6
R1(config-subif)#ipv6 address fe80::1 link-local	asignación de la link-local
R1(config-subif)#	
R1(config-subif)# int g0/0/1.4	ingreso a la subinterfaz
R1(config-subif)#encapsulation dot1q 4	encapsulación de la vlan 4
R1(config-subif)#description Management	descripción
R1(config-subif)#ip address 10.19.8.97 255.255.255.248	asignación de ipv4
R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64	asignación de ipv6
R1(config-subif)#ipv6 address fe80::1 link-local	asignación de la link-local
R1(config-subif)# int g0/0/1.6	ingreso a la subinterfaz
R1(config-subif)#encapsulation dot1q 6 native	encapsulación de la vlan 6
R1(config-subif)#description Native	descripción
R1(config-subif)# int g0/0/1	ingresamos a la interface
R1(config-if)# no shutdown	realizamos la activación
R1(config)#int loopback 0	ingreso interface red virtual
R1(config-if)# ip address 209.165.201.1 255.255.255.224	Asignacion de ipv4
R1(config-if)#ipv6 address 2001:db8:acad:209::1/64	Asignacion de ipv6
R1(config-if)#ipv6 address fe80::1 link-local	asignación de la link-local
R1(config-if)# R1(config)#crypto key generate rsa	Generar clave rsa
The name for the keys will be: R1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.	

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

En la tabla 6. Se puede observar la configuracion completa de R1 con la descripción de cada uno de los comandos ejecutados en la simulación de Packet tracer.

1.1.3 CONFIGURACION DE S1-S2

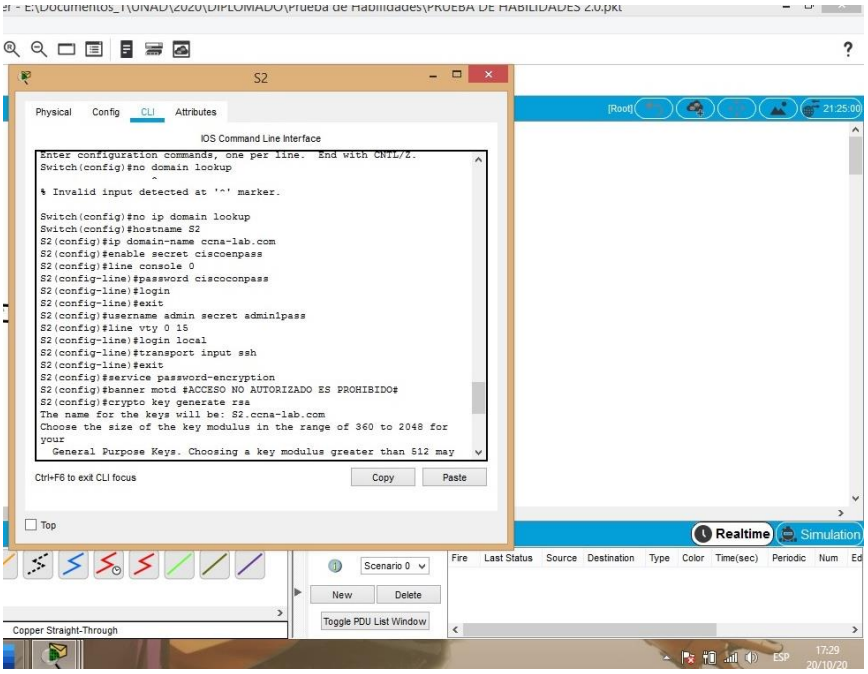
Figura 7. Configuración de S1



Fuente: Autor.

En la Figura 7 Podemos observar la ejecución de los comandos que nos permiten la configuracion del switch S1. Lagunas de ellas son la asignación de nombre, desactivación de la búsqueda de DNS, configuracion de seguridad, encriptación de contraseñas entre otras configuraciones básicas aplicadas al switch.

Figura 8.Configuración de S2



Fuente: Autor.

En la figura 7. Se observa la ejecución de los comandos para la configuracion básica del switch.

Tabla 7. Código de Configuración S1

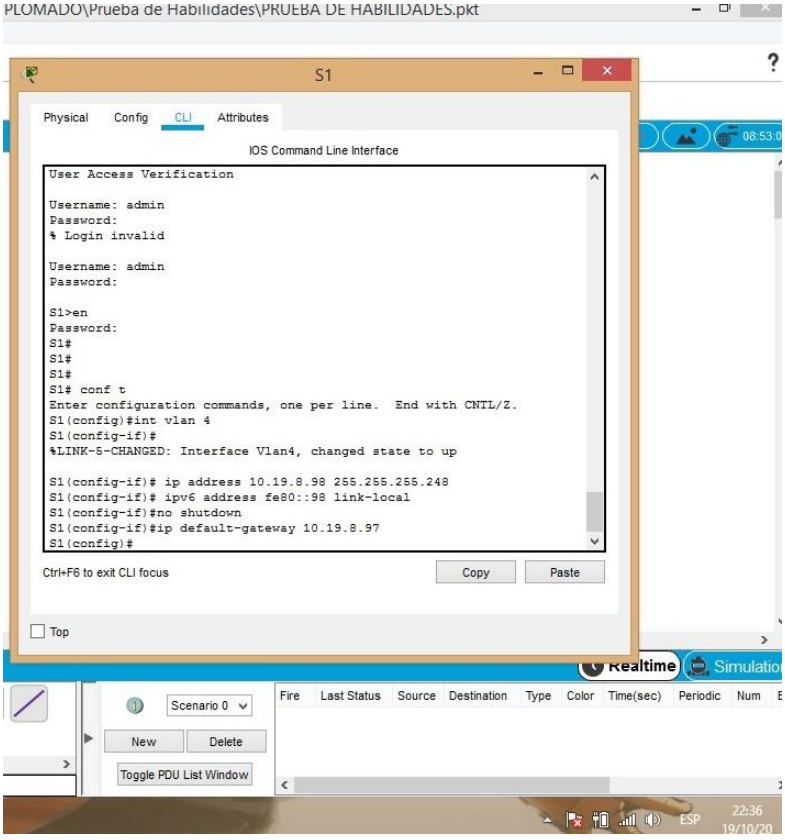
Código	Descripción
Switch>en	ingreso modo exec
Switch #conf t Enter configuration commands, one per line. End with CNTL/Z.	ingreso al modo de configuración
Switch (config)#no ip domain lookup	se desactiva la búsqueda de DNS
Switch(config)#hostname S1	Asignacion de nombre al router
S1(config)# ip domain-name ccna-lab.com	Asignacion de nombre de dominio
S1(config)#enable secret ciscoenpass	contraseña privilegiada exec
S1(config)#line console 0	línea de ingreso al modo consola
S1(config-line)#password ciscoconpass	Asignacion de contraseña de consola
S1(config-line)# login	permite establecer la contraseña
S1(config)#username admin secret admin1pass	creación de usuario en base local

S1(config)# line vty 0	establecer login en base de datos local
S1(config-line)# login local	permite establecer la contraseña
S1(config-line)#transport input ssh	configuración de entrada ssh
S1(config)#service password-encryption	encriptación de contraseñas
S1(config)# banner motd #ACCESO NO AUTORIZADO ES PROHIBIDO#	configuración de mensaje.

La configuración básica descrita en el código anterior es totalmente aplicable a cualquiera de los dos switch a utilizar. Por tal motivo solo se agrega el código de S1.

CONFIGURACION DE INTERFAZ DE ADMINISTRACIÓN (SVI) PARA S1

Figura 9. Configuración vlan4 S1



Fuente: Autor

En la Figura 8 Se puede observar la ejecución de los comandos para la creación de la vlan 4 en el switch 1.

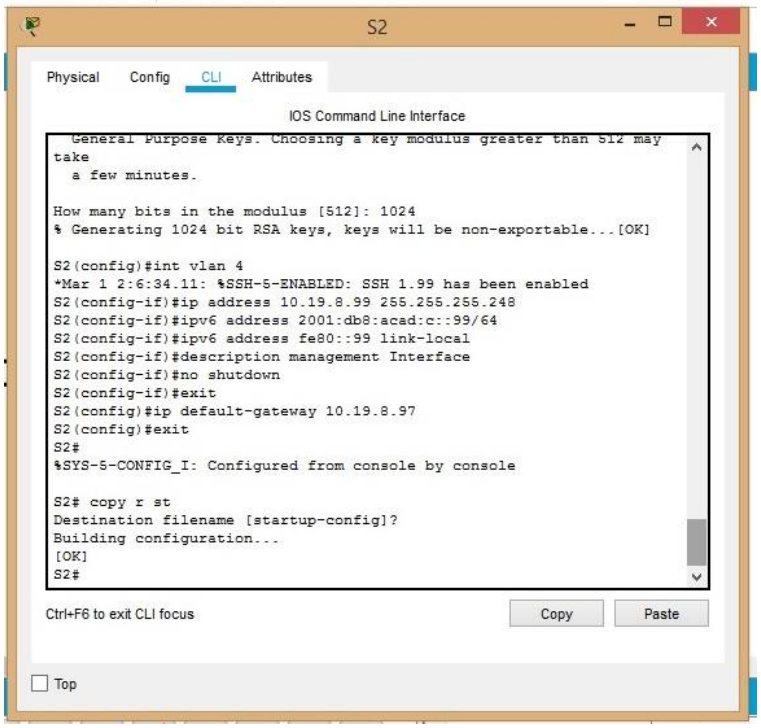
Tabla 8.Codigo Configuración de vlan4 S1

Código	Descripción
S1(config)#int vlan 4 *Mar 1 1:53:35.226: %SSH-5-ENABLED: SSH 1.99 has been enabled	Ingresamos a la Interfaz de vlan 4
S1(config-if)#ip address 10.19.8.98 255.255.255.248	Asignacion IPv4
S1(config-if)#ipv6 address 2001:db8:acad:c::98/64	Asignacion IPv6
S1(config-if)#ipv6 address fe80::98 link-local	Asignacion link-local
S1(config-if)#no shutdown	activamos la vlan 4
S1(config-if)# exit	salimos
S1(config)#ip default-gateway 10.19.8.97	configuramos la Puerta de enlace

En la tabla 8 Observamos los comandos con su respectiva descripción de la creación de la vlan 4.

CONFIGURACION DE INTERFAZ DE ADMINISTRACIÓN (SVI) PARA S2

Figura 10.Configuración de vlan 4 S2



Fuente: Autor.

En la figura 9 Se puede observar la ejecución de los comandos para la configuracion de la vlan 4.

Tabla 9.Código Configuración de vlan4 S2

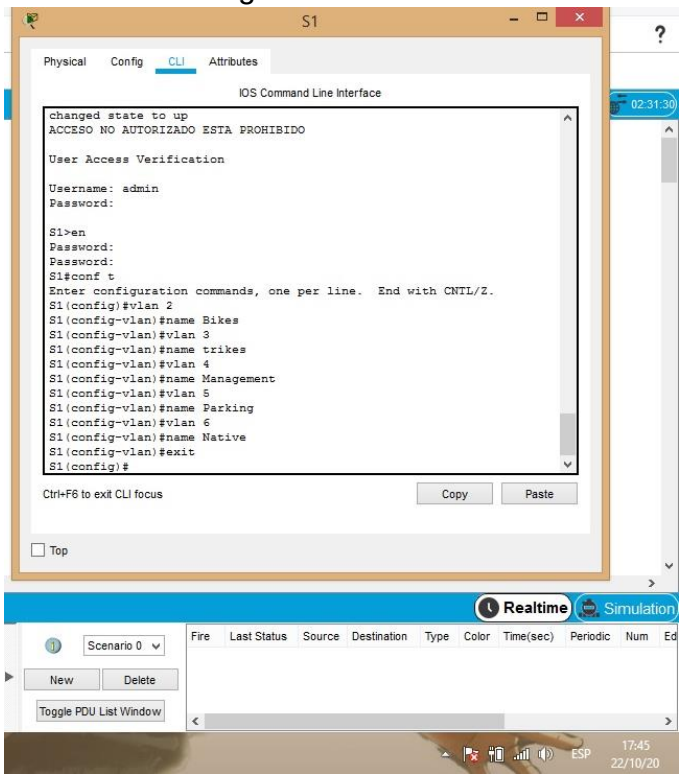
Código	Descripción
S2(config)#int vlan 4 *Mar 1 1:53:35.226: %SSH-5-ENABLED: SSH 1.99 has been enabled	Ingresamos a la Interfaz de vlan 4
S2(config-if)#ip address 10.19.8.99 255.255.255.248	Asignacion IPv4
S2(config-if)#ipv6 address 2001:db8:acad:c::99/64	Asignacion IPv6
S2(config-if)#ipv6 address fe80::99 link-local	Asignacion link-local
S2(config-if)#description Management interface	Descripción
S2(config-if)#no shutdown	Activamos la vlan 4
S2(config-if)# exit	Salimos
S2(config)#ip default-gateway 10.19.8.97	Configuramos la Puerta de enlace

En la tabla 9 se puede observar los comandos para realizar la asignación de las direcciones de IPv4 y IPv6, se agrega una descripción, y también de agrega el Gateway predeterminado, y de la link local para el direccionamiento IPv6 y sus respectivas descripciones para la configuracion de la vlan 4 en el switch 2.

1.2. CONFIGURACIÓN DE LA INFRAESTRUCTURA DE RED (VLAN, TRUNKING, ETHERCHANNEL)

1.2.1 CONFIGURACION VLANS TRUNKING, ETHERTCHANNEL EN S1

Figura 11. vlan S1



Fuente: Autor.

En la figura anterior se ingresa a las vlans y se les asigna un nombre. Esto se realiza para cada una de las vlan de la 1 hasta la 6.

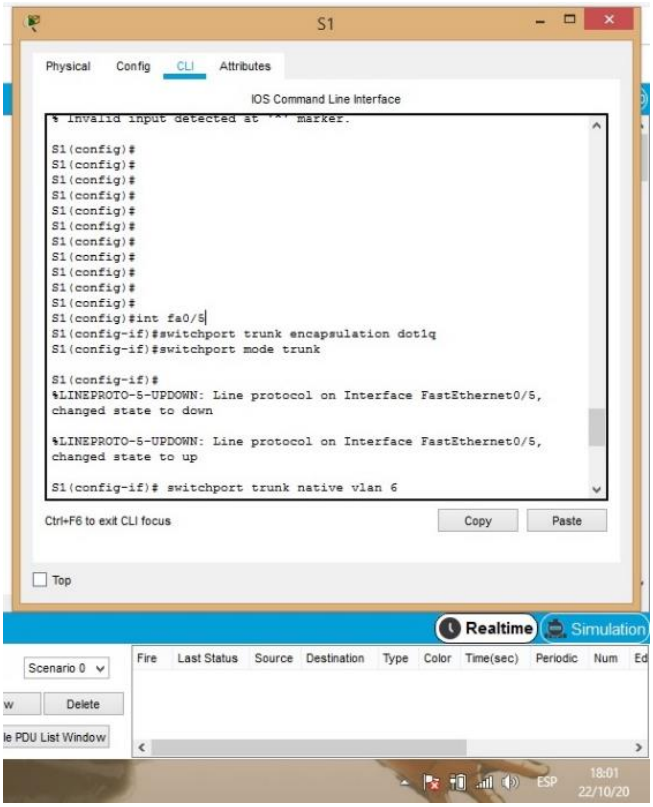
Tabla 10.Codigo Vlan S1.

Código	Descripción
S1#conf t Enter configuration commands, one per line. End with CNTL/Z.	Ingreso al modo de configuración global
S1(config)#vlan 2	Se ingresa a la vlan
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	Se le asigna nombre a la vlan
S1(config-vlan)#exit	Salir

En la tabla 10. Se crea las vlan, se ingresa a ellas y se les asigna un nombre. Esto se realiza para cada una de las vlan de la 1 hasta la 6.

CREAR TRONCALES 802.1Q QUE UTILICEN LA VLAN 6 NATIVA PARA S1

Figura 12. interface fa0/5



Fuente: Autor.

En la figura anterior se procede a configurar el puerto como troncal y se asigna a una vlan especifica.

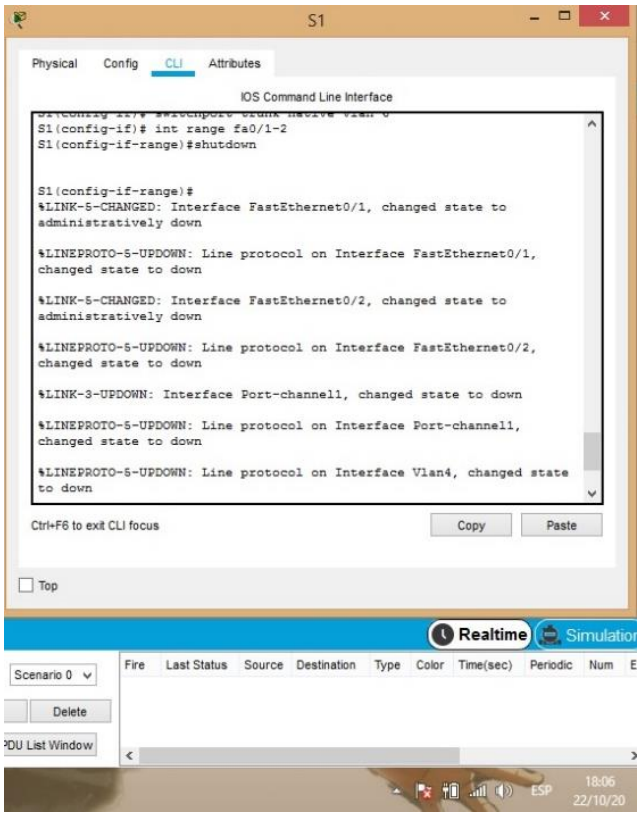
Tabla 11.Codigo Configuración Fa0/5

Código	Descripción
S1(config)# int fa0/5	ingreso a la interfaz
S1(config-if)#switchport trunk encapsulation dot1q	Se configura las troncales
S1(config-if)#switchport mode trunk %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up	Se pasa el Puerto a modo enlace troncal

S1(config-if)#switchport trunk native vlan 6	se asignan a la vlan 6

En la tabla 11. se puede observar los comandos y las descripciones de cada uno de ellos.

Figura 13.Interface fa0/1-2



Fuente: Autor.

E la figura anterior se procede apagar las interfaces y asignar a configurar en modo troncal, se asigna a una vlan especifica.

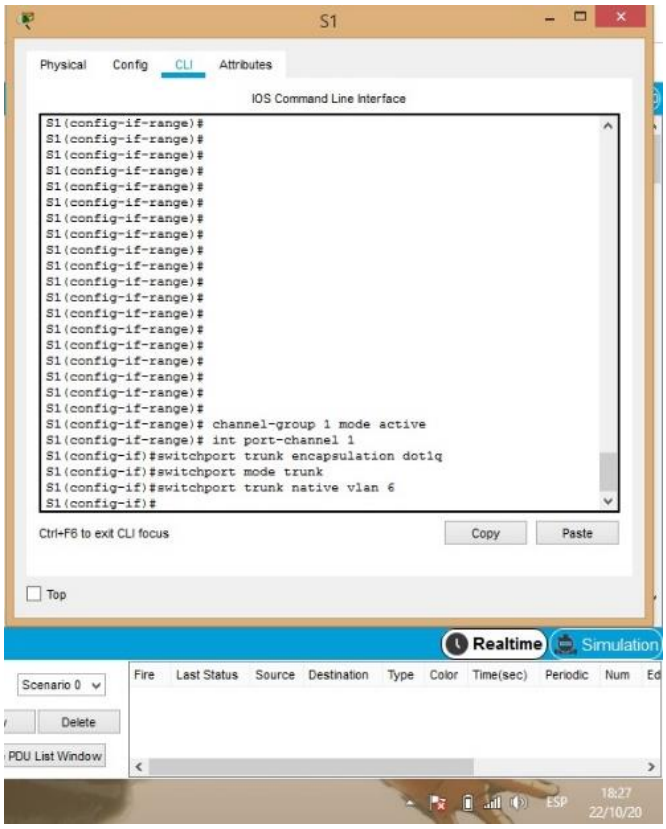
Tabla 12.Código Interface 1-2

Código	Descripción
S1(config-if)# int range fa0/1-2	se utiliza un rango para facilitar la configuración
S1(config-if-range)# shutdown	se apaga la interfaces
S1(config-if-range)#switchport mode trunk	se llama el modo troncal
S1(config-if-range)#switchport trunk native vlan 6	se asigna a la vlan 6

Tabla 12. Se observa los comandos para configuracion de las interfaces 1 y 2 con su respectiva descripción.

CREACIÓN UN GRUPO DE PUERTOS ETHERCHANNEL DE CAPA 2 QUE USE INTERFACES F0/1 Y F0/2

Figura 14.Puertos etherchannel



Fuente: Autor.

En la figura 14**.** observar la ejecución comandos de la configuracion de EtherChannel.

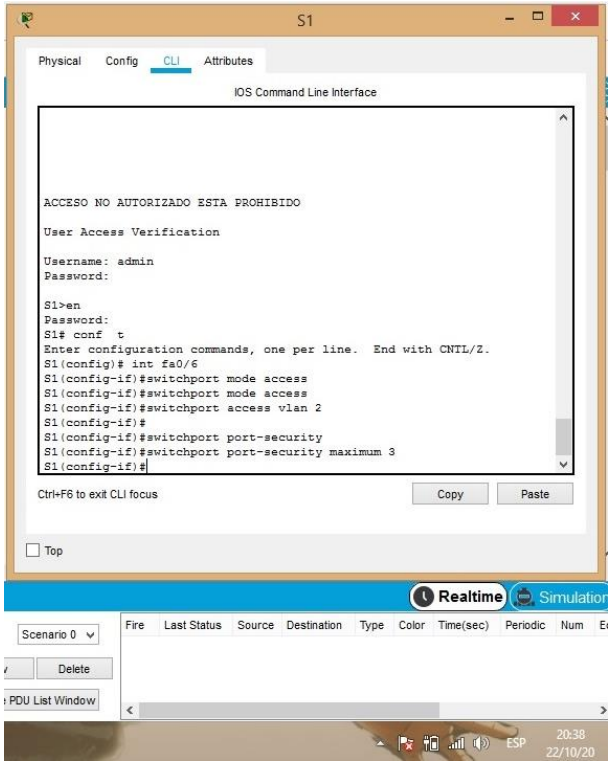
Tabla 13.Codigo Configuración EtherChannel

Código	Descripción
S1(config-if-range)#channel-group 1 mode active	Si agregran las interfaces al grupo de canales de LACP 1
S1(config-if-range)#int port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q	asignamos el canal 1
S1(config-if)#switchport mode trunk	se llama el modo troncal
S1(config-if)#switchport trunk native vlan 6	se asigna a la vlan 6

En la tabla 13 se puede observar los comandos y sus respectivas descripciones de la configuracion de EtherChannel.

CONFIGURAR EL PUERTO DE ACCESO DE HOST PARA VLAN 2

Figura 15.Configuracion de Vlan 2 S1



Fuente: Autor.

En la figura anterior podemos observar la ejecución de los comandos para la seguridad de puertos y se establece un límite maximo de MAC.

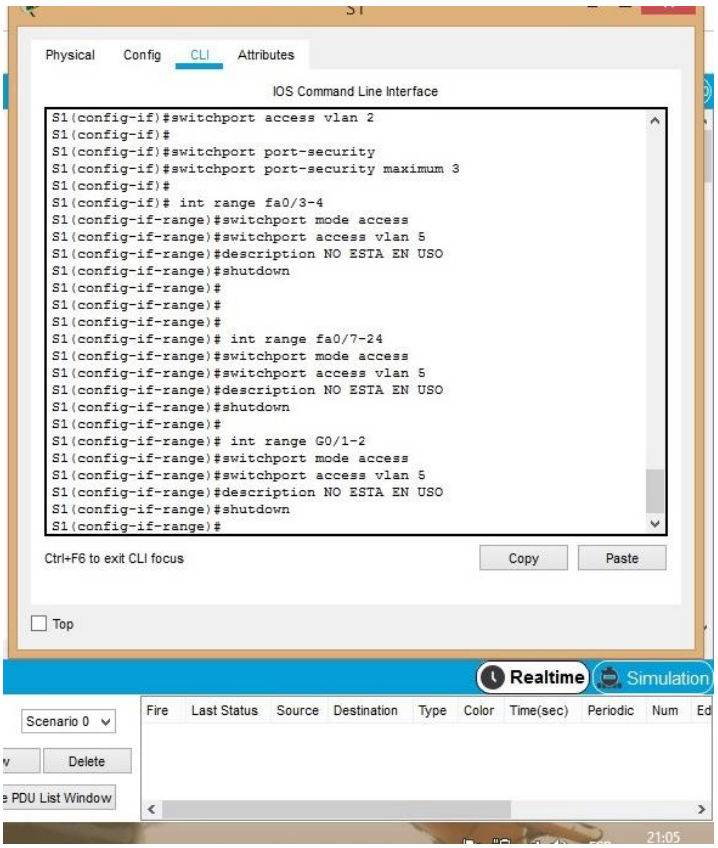
Tabla 14.Código Configuración Vlan 2 S1

Código	Descripción
S1(config)# int fa0/6	ingreso a la interfaz
S1(config-if)#switchport mode access	configuración como Puerto de acceso
S1(config-if)#switchport access vlan 2	Se agrega a la vlan
S1(config-if)#switchport port-security	Se habilita la seguridad del puerto
S1(config-if)#switchport port-security maximum 3	Se establece maximo de MAC

En el código anteriormente descrito se habilita el puerto de acceso y se asigna la vlan 2, luego se habilita la seguridad del puerto y se establece un maximo de 3 direcciones MAC.

PROTEJA TODAS LAS INTERFACES NO UTILIZADAS

Figura 16. Interfaces no utilizadas



Fuente: Autor.

En la figura anterior podemos observar cómo se procese apagar las interfaces no utilizadas.

Tabla 15.Código Interfaces no utilizadas.

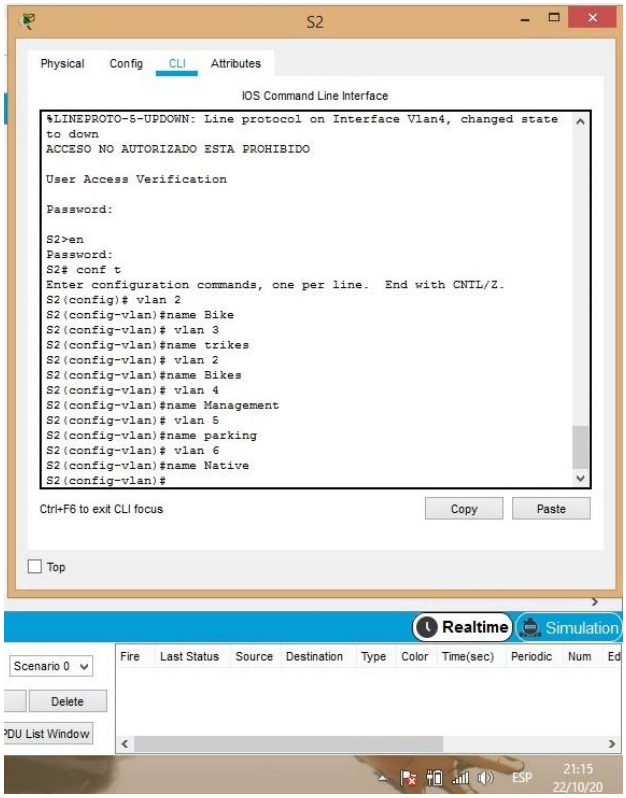
Código	Descripción
S1(config-if)# int range fa0/3-4	Se establece el rango de interfaces a trabajar
S1(config-if-range)#switchport mode acces	Configuración como Puerto de acceso
S1(config-if-range)#switchport access vlan 5	Se asigna a la vlan
S1(config-if-range)#description NO ESTA EN USO	Se introduce descripción
S1(config-if-range)#shutdown	Se apaga las interfaces
S1(config-if-range)# int range fa0/7-24	Se establece el rango de interfaces a trabajar
S1(config-if-range)#switchport mode access	Configuración como Puerto de acceso

S1(config-if-range)#switchport access vlan 5	Se asigna a la vlan
S1(config-if-range)#description NO ESTA EN USO	Se introduce descripción
S1(config-if-range)#shutdown	Se apaga la interfaces
S1(config-if-range)# int range G0/1-2	Se establece el rango de interfaces a trabajar
S1(config-if-range)#switchport mode access	Configuración como Puerto de acceso
S1(config-if-range)#switchport access vlan 5	Se asigna a la vlan
S1(config-if-range)#description NO ESTA EN USO	Se introduce descripción
S1(config-if-range)#shutdown	se apaga la interfaces

En el código anteriormente descrito se Procede a proteger las interfaces no utilizadas y a agregar una descripción para tal fin.

1.2.2 CONFIGURACION VLANS TRUNKING, ETHERTCHANNEL EN S2

Figura 17. VLAN S2



Fuente: Autor.

En la figura 17 observamos la creación de las vlan en S2 y su asignación de nombres.

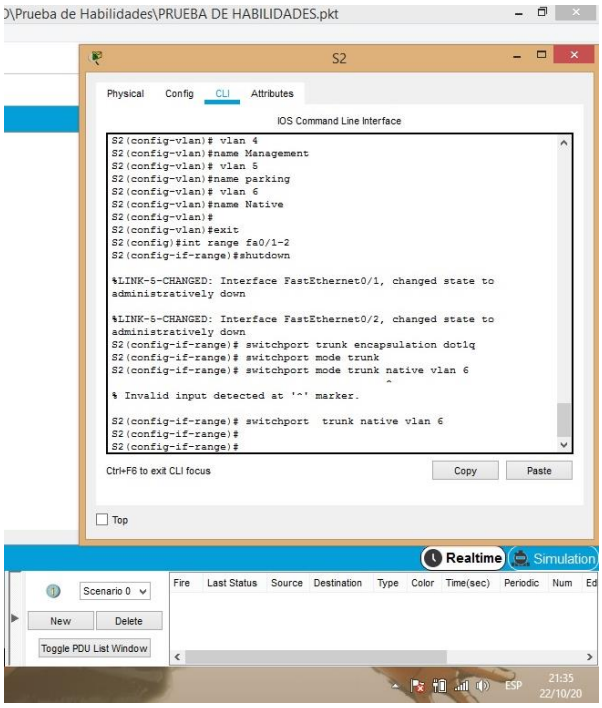
Tabla 16.Código Configuración de Vlan S2

Código	Descripción
S2#conf t Enter configuration commands, one per line. End with CNTL/Z.	Ingreso al modo de configuración global
S2(config)#vlan 2	Se ingresa a la vlan
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 Nativ	Se le asigna nombre a la vlan
S2(config-vlan)#exit	Salir

Se crea las vlan, se ingresa a ellas y se les asigna un nombre. Esto se realiza para cada una de las vlan de la 1 hasta la 6.

CREAR TRONCALES 802.1Q QUE UTILICEN LA VLAN 6 NATIVA PARA S2

Figura 18.Interfaces fa0/1-2



Fuente: Autor.

En la figura anterior se procede apagar las interfaces y la configurar como troncales, se asigna una vlan especifica.

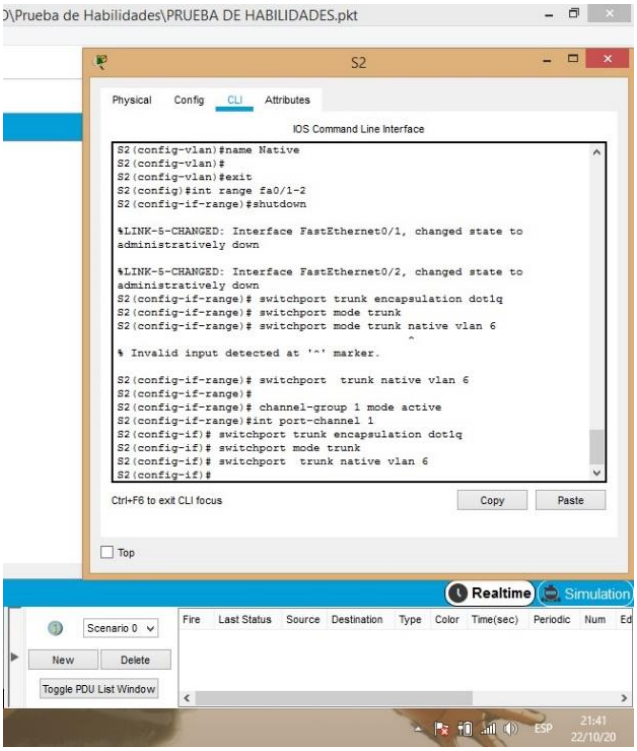
Tabla 17. Código Interface fa0/1-2 S2

Código	Descripción
S2(config-if)# int range fa0/1-2	se utiliza un rango para facilitar la configuración
S2(config-if-range)#	shutdown se apaga la interfaces
S2(config-if-range)#switchport mode trunk	se llama el modo troncal
S2(config-if-range)#switchport trunk native vlan 6	se asigna a la vlan 6

En la tabla 17. se observa los comandos y la descripción de las interfaces y la configurar como troncales, se asigna una vlan especifica.

CREACIÓN UN GRUPO DE PUERTOS ETHERCHANNEL DE CAPA 2 QUE USE INTERFACES F0/1 Y F0/2

Figura 19. puertos EtherChannel S2



En la figura 19. Se ejecuta los comandos la asignación y configuracion de los puertos EtherChannel para switch 2.

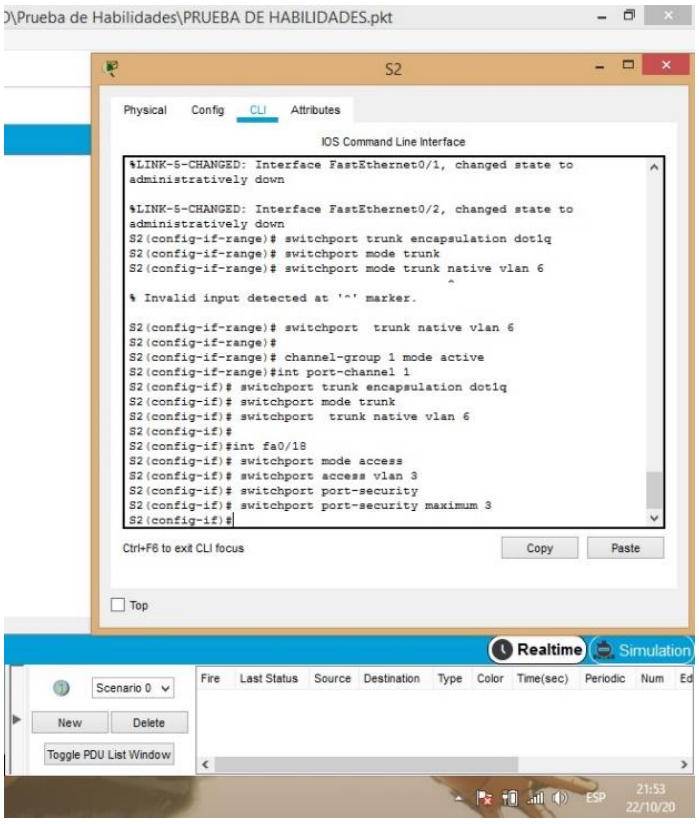
Tabla 18. Puertos EtherChannel S2

Código	Descripción
S2(config-if-range)#channel-group 1 mode active	si agregran las interfaces algrupo de canales de LACP 1
S2(config-if-range)#int port-channel 1	asignamos el canal 1
S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk	se llama el modo troncal
S2(config-if)#switchport trunk native vlan 6	se asigna a la vlan 6

En la tabla 18. Se observa los comandos y la descripción de la asignación y configuracion de los puertos EtherChannel para switch 2.

CONFIGURAR EL PUERTO DE ACCESO DEL HOST PARA LA VLAN 3 Y CONFIGURE PORT-SECURITY EN LOS ACCESS PORTS S2

Figura 20. Configuración Vlan3



Fuente: Autor.

En la figura anterior se procede a configurar el puerto del host y se establece la seguridad y un límite maximo de MAC.

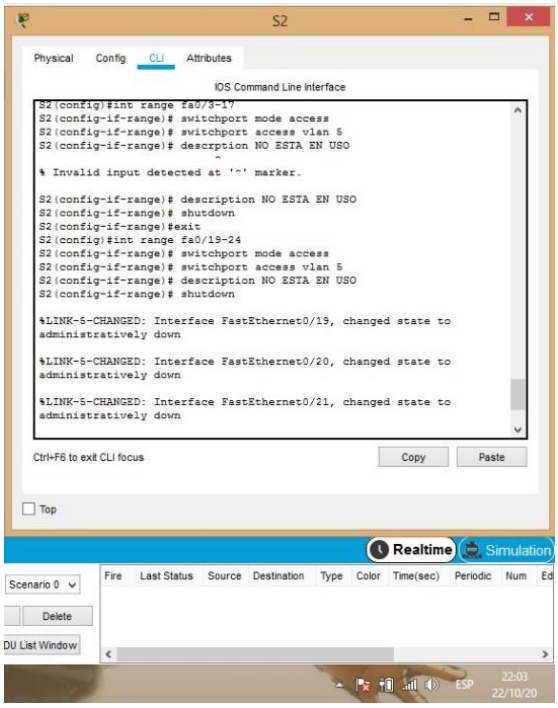
Tabla 19. Código Configuración de vlan 3 S2

Código	Descripción
S2(config)# int fa0/18	ingreso a la interfaz
S2(config-if)#switchport mode access	configuración como Puerto de acceso
S2(config-if)#switchport access vlan 3	se agrega a la vlan
S2(config-if)#switchport port-security	se habilita la seguridad del puerto
S2(config-if)#switchport port-security maximum 3	se establece maximo de MAC

En el código anteriormente descrito se habilita el puerto de acceso y se asigna la vlan 3, luego se habilita la seguridad del puerto y se establece un maximo de 3 direcciones MAC.

PROTEJA TODAS LAS INTERFACES NO UTILIZADAS

Figura 21. Interfases no utilizadas en S2.



En la figura 21 se procede a apagar las interfaces no utilizadas en el switch 2.

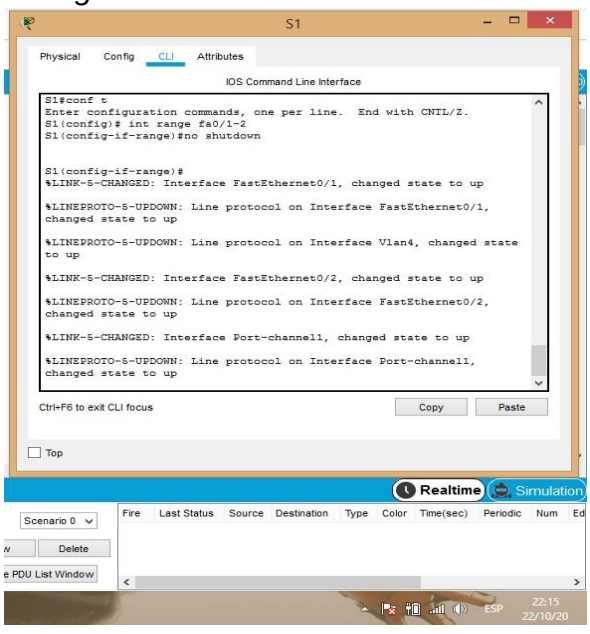
Tabla 20. Código interfaces no Utilizadas S2

Código	Descripción
S2(config-if)# int range fa0/3-17	Se establece el rango de interfaces a trabajar
S2(config-if-range)#switchport mode acces	Configuración como Puerto de acceso

S2(config-if-range)#switchport access vlan 5	Se asigna a la vlan
S2(config-if-range)#description NO ESTA EN USO	Se introduce descripción
S2(config-if-range)#shutdown	Se apaga las interfaces
S2(config-if-range)# int range fa0/19-24	Se establece el rango de interfaces a trabajar
S2(config-if-range)#switchport mode access	Configuración como Puerto de acceso
S2(config-if-range)#switchport access vlan 5	Se asigna a la vlan
S2(config-if-range)#description NO ESTA EN USO	Se introduce descripción
S2(config-if-range)#shutdown	Se apaga la interfaces
S2(config-if-range)# int range G0/1-2	Se establece el rango de interfaces a trabajar
S2(config-if-range)#switchport mode access	Configuración como Puerto de acceso
S2(config-if-range)#switchport access vlan 5	Se asigna a la vlan
S2(config-if-range)#description NO ESTA EN USO	Se introduce descripción
S2(config-if-range)#shutdown	Se apaga la interfaces

Ahora después de haber creado las troncales y tener el etherchannel listo, se procede a encender las interfaces fa0/1-2 en S1 Y S2 mediante en comando "**no shutdown**".

Figura 22.Encendido de fa0/1-2 S1



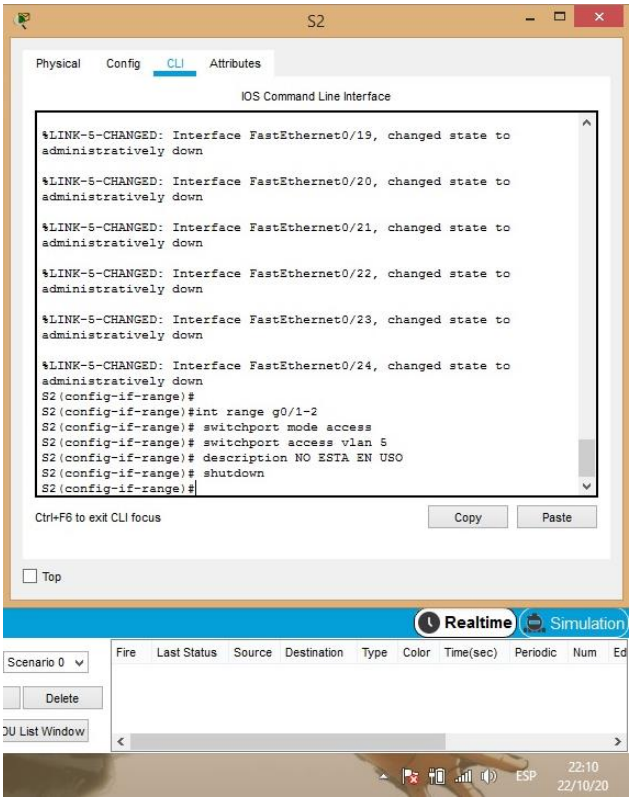
Fuente: Autor.

Tabla 21. Encendido de fa0/1-2 S1

Código	Descripción
S1>en	Ingreso al modo exec privilegiado
Password:	Ingrese contraseña para exec
S1#conf t Enter configuration commands, one per line. End with CNTL/Z.	Configuración global
S1(config)# int range fa0/1-2	Ingreso al rango de las interfaces a trabajar
S1(config-if-range)#no shutdown	Encendido de interfaces

En la figura 21 y en la tabla 21. Podemos observar la ejecución de los comandos y descripción de cada uno de ellos. Los cuales se utilizan para realizar el encendido de las interfaces.

Figura 23.Encendido de fa0/1-2 S2



Fuente: Autor.

En la figura 23. Podemos observar la ejecución de los comandos los cuales se utilizan para realizar el encendido de las interfaces.

Tabla 22.Encendido de fa0/1-2 S2

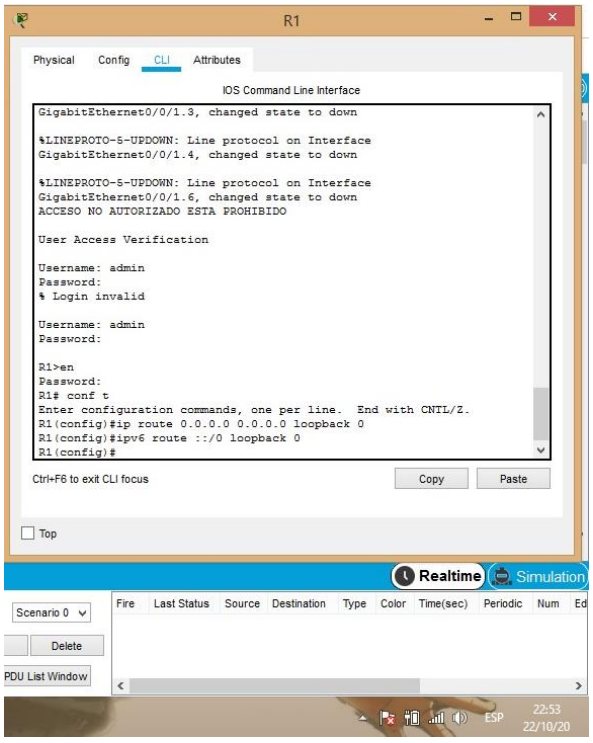
Código	Descripción
S1>en	Ingreso al modo exec privilegiado
Password:	Ingrese contraseña para exec
S1#conf t Enter configuration commands, one per line. End with CNTL/Z.	configuración global
S1(config)# int range fa0/1-2	Ingreso al rango de las interfaces a trabajar
S1(config-if-range)#no shutdown	Encendido de interfaces

En la tabla 22. Podemos observar la ejecución de los comandos y descripción de cada uno de ellos. Los cuales se utilizan para realizar el encendido de las interfaces.

1.2.3 CONFIGURACION DE R1

CREAR RUTAS PREDETERMINADAS PARA IPV4 E IPV6 QUE DIRIJAN EL TRÁFICO A LA INTERFAZ LOOPBACK 0

Figura 24.Rutas predeterminadas en R1.



Fuente: Autor.

En la Figura 24. Se observan la ejecución los comandos para la creación de las rutas en R1.

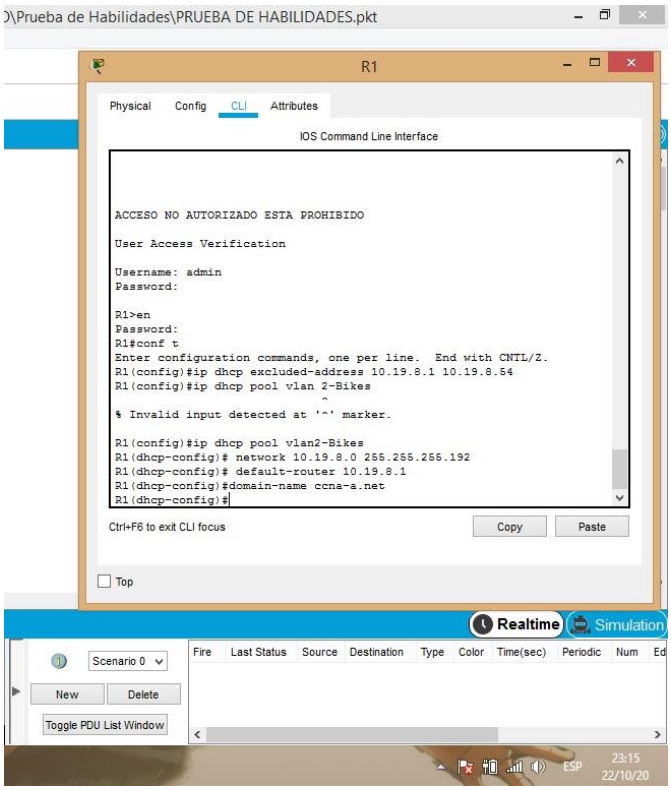
Tabla 23. Código Configuración de rutas Predeterminadas.

Código	Descripción
R1>en	Ingreso al modo exec privilegiado
Password:	contraseña del modo privilegiado
R1# conf t Enter configuration commands, one per line. End with CNTL/Z.	Ingreso a la configuración global
R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0	ruta ipv4 interfaces virtual
R1(config)#ipv6 route ::/0 loopback 0	ruta ipv6 interfaces virtual

En la tabla 23. Se observan la ejecución los comandos y la descripción para la creación de las rutas predeterminadas en R1.

CONFIGURAR IPV4 DHCP PARA VLAN 2

Figura 25. DHCP IPv4 Vlan 2



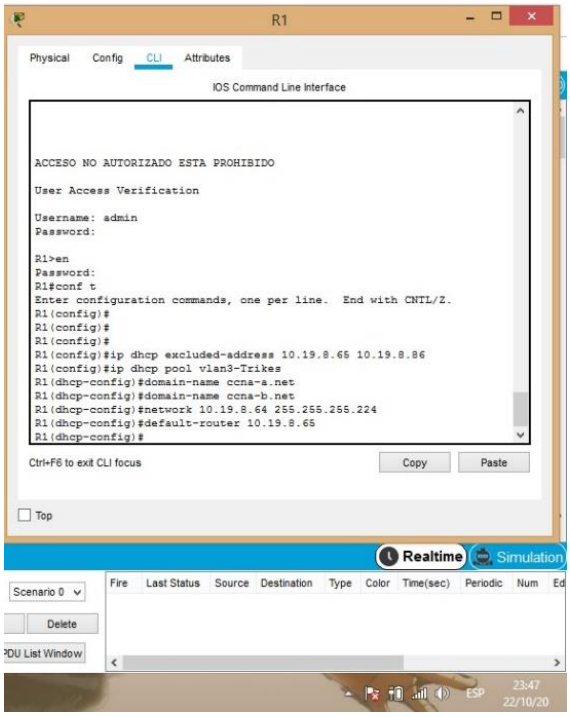
En la imagen 25. Podemos observar la creación de del pool DHCP en la vlan 2 para el direccionamiento de IPv4.

Tabla 24.Codigo DHCP IPv4 Vlan 2 R1

Código	Descripción
R1>en	Ingreso al modo exec privilegiado
Password:	Contraseña del modo privilegiado
R1# conf t Enter configuration commands, one per line. End with CNTL/Z.	Ingreso a la configuración global
R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.54	Excluimos este rango de ip
R1(config)#ip dhcp pool vlan2-Bikes	Creamos el pool de DHCP
R1(dhcp-config)# network 10.19.8.0 255.255.255.192	Agregamos la red a trabajar
R1(dhcp-config)# default-router 10.19.8.1	Definimos la puerta de enlace
R1(dhcp-config)#domain-name ccna-a.net	Asignamos el nombre del dominio

Describiendo un poco el código anterior podemos decir que al excluir una rango de red y agregar una red con mascara subred 26, nos daría más o menos unas 10 direcciones en las que puede trabajar el pool de dhcp.

Figura 26.DHCP Vlan 3 R1



Fuente: Autor.

En la figura 26. Podemos observar la ejecución de los comandos que permiten crear un Pool DHCP y la exclusión de un rango de direcciones IP.

Tabla 25.Código DHCP Vlan 3 R1

Código	Descripción
R1>en	Ingreso al modo exec privilegiado
Password:	contraseña del modo privilegiado
R1# conf t Enter configuration commands, one per line. End with CNTL/Z.	ingreso a la configuración global
R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.86	Excluimos este rango de ip
R1(config)#ip dhcp pool vlan3-Trikes	Creamos el pool de DHCP
R1(dhcp-config)# network 10.19.8.64 255.255.255.224	Agregamos la red a trabajar
R1(dhcp-config)# default-router 10.19.8.65	Definimos la puerta de enlace
R1(dhcp-config)#domain-name ccna-b.net	Asignamos el nombre del dominio

Describiendo un poco el código anterior podemos decir que al excluir un rango de red y agregar una red con mascara subred 27, nos daría más o menos unas 10 direcciones en las que puede trabajar el pool de dhcp.

1.2.4 Configurar los servidores

Configure los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, registre las configuraciones de red del host con el comando **ipconfig /all.**

Tabla 26.Configuración PC-A

Configuración de red de PC-A	
Dirección física	*00D0.5891.2D22*
Dirección IP	*10.19.8.53*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	*FE80::1*

Tabla 27.Configuracion PC-B

Configuración de red de PC-B	
Dirección física	*0001.43AB.1BA6*
Dirección IP	*10.19.8.86*
Máscara de subred	*255.255.255.224*
Gateway predeterminado	*10.19.8.65*

Configuración de red de PC-B	
Gateway predeterminado IPv6	*FE80::1*

1.3 PROBAR Y VERIFICAR LA CONECTIVIDAD DE EXTREMO A EXTREMO

Tabla 28. Verificación de ping

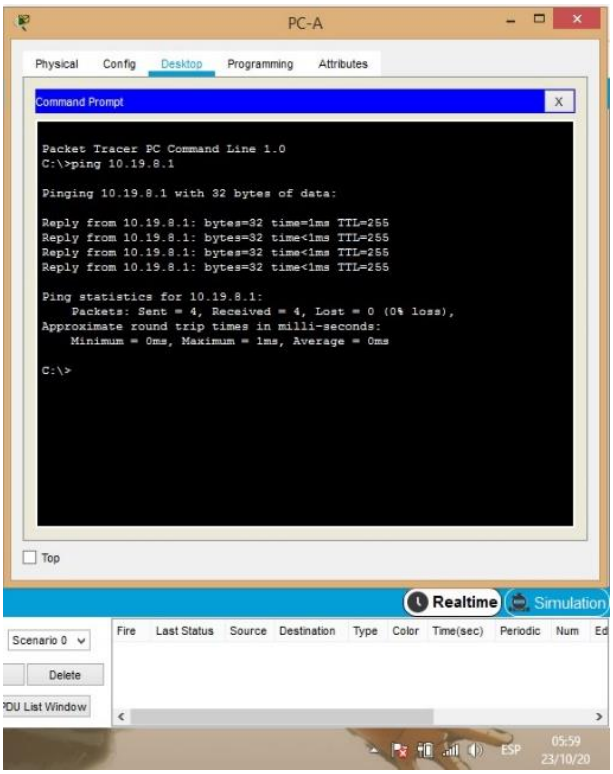
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	*OK*
		IPv6	2001:db8:acad:a: :1	*OK*
	R1, G0/0/1.3	Dirección	10.19.8.65	*OK*
		IPv6	2001:db8:acad:b: :1	*OK*
	R1, G0/0/1.4	Dirección	10.19.8.97	*OK*
		IPv6	2001:db8:acad:c: :1	*OK*
	S1, VLAN 4	Dirección	10.19.8.98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

Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:b: :1	*OK*
	R1, G0/0/1.4	Dirección	10.19.8.97	*OK*
		IPv6	2001:db8:acad:c: :1	*OK*
	S1, VLAN 4	Dirección	10.19.8.98	*OK*
		IPv6	2001:db8:acad:c: :98	*OK*
	S2, VLAN 4	Dirección	10.19.8.99.	*OK*
		IPv6	2001:db8:acad:c: :99	*OK*

EVIDENCIA DE LOS RESULTADOS IPV4 DESDE LA PC-A

PING DESDE LA PC-A A LA IP 10.19.8.1

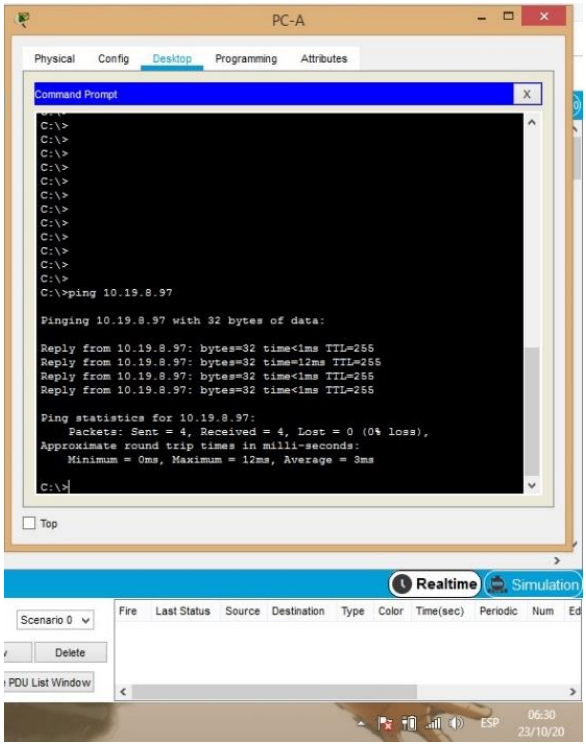
Figura 27.ping a 10.19.8.1



Fuente: Autor.

PING DESDE LA PC-A A LA IP 10.19.8.97

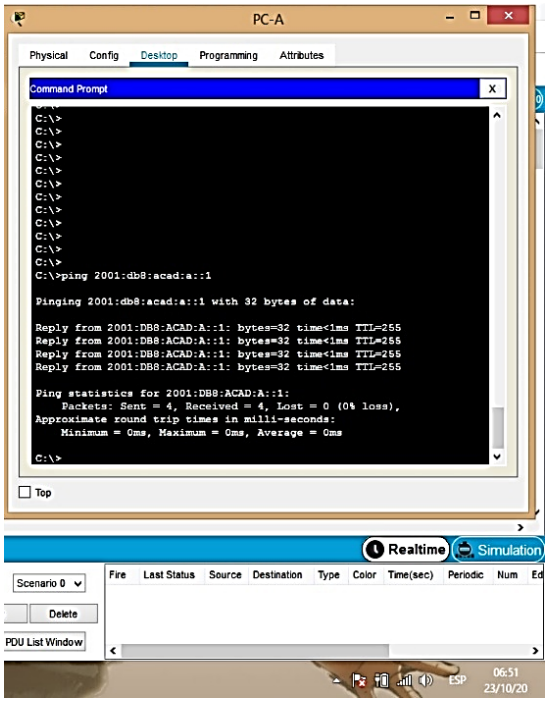
Figura 28.Ping a 10.19.8.97



Fuente: Autor.

PING DESDE LA PC-A A LA IPV6 2001:db8:acad:a: :1

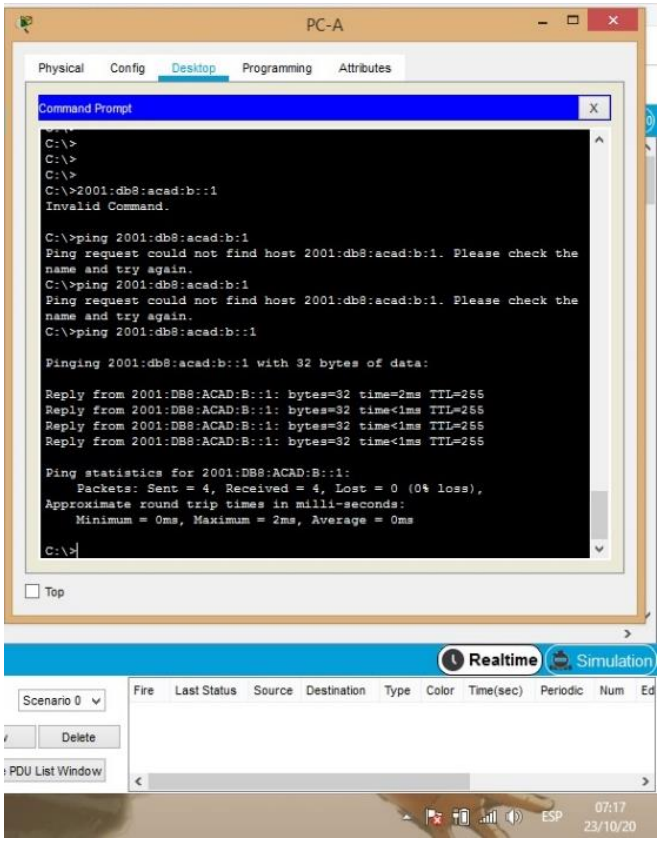
Figura 29.Ping a ipv6 2001:db8:acad:a::1



Fuente: Autor.

PING DESDE LA PC-A A LA IPV6 2001:db8:acad:b: :1

Figura 30.Ping a 2001:db8:acad:b: :1

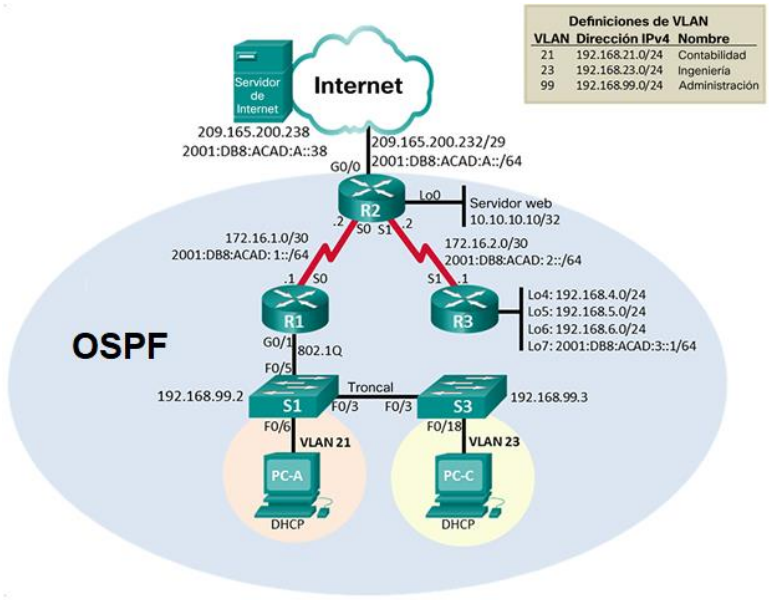


Fuente: Autor.

Como se observa en la tabla de verificación de ping y en las imágenes la simulación de Packet tracer del escenario 1 queda resulta al 100%.

ESCENARIO 2

Topología



Parte 1: Inicializar dispositivos

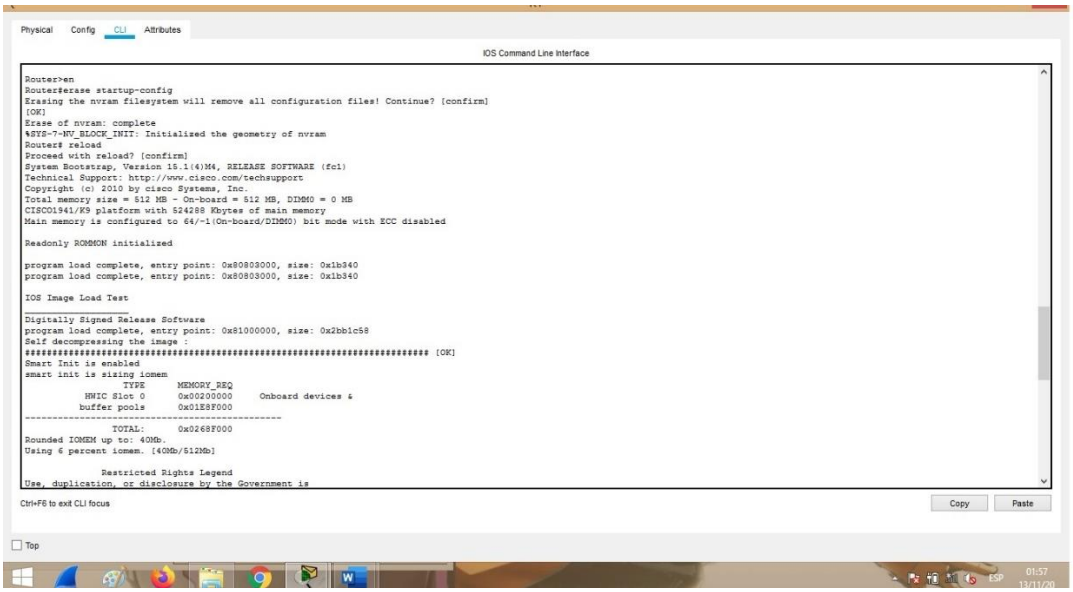
Paso 1: Inicializar y volver a cargar los routers y los switches.

Tabla 29. Inicialización de Dispositivos.

Descripción	Código
Eliminar el archivo startup-config de todos los routers	Router>en Router#erase startup-config
Volver a cargar todos los routers	Router# reload Proceed with reload? [confirm]
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch> Switch>en Switch# erase startup-config
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> en Switch# show flash

En la tabla 29. Podemos observar los comandos que se ejecutaron en la inicialización de los router y switch. Estos comandos son perfectamente ejecutables en los dos tipos de dispositivos.

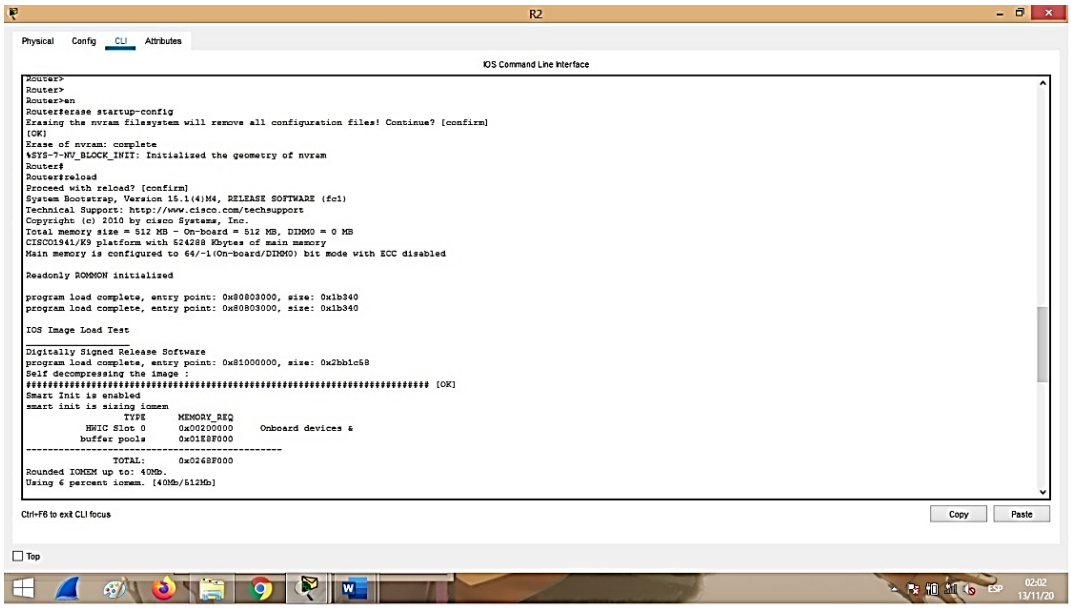
Figura 31. Inicialización R1.



Fuente: Autor.

En figura 43. Observamos los comandos de inicialización del router R1.

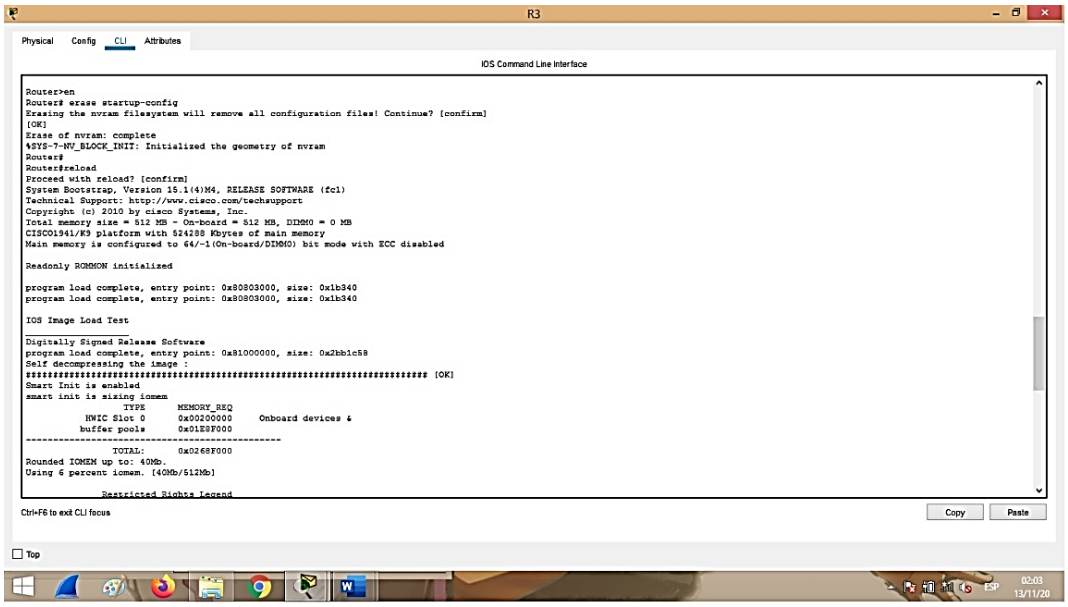
Figura 32. Inicialización R2



Fuente: Autor.

En figura 44. Observamos los comandos de inicialización del router R2.

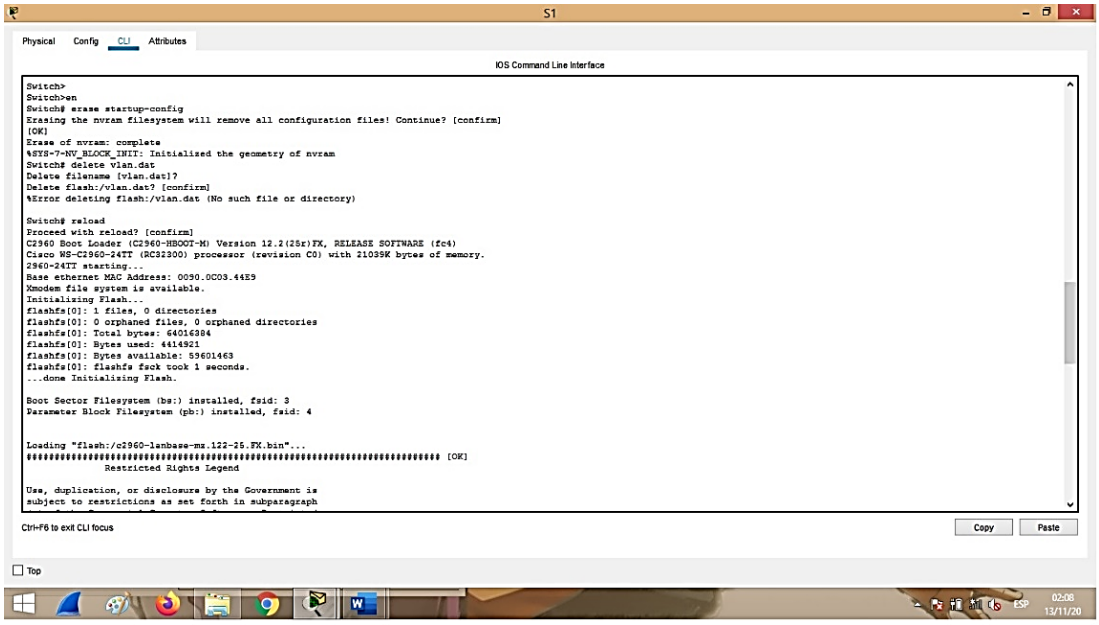
Figura 33. Inicialización R3



Fuente: Autor.

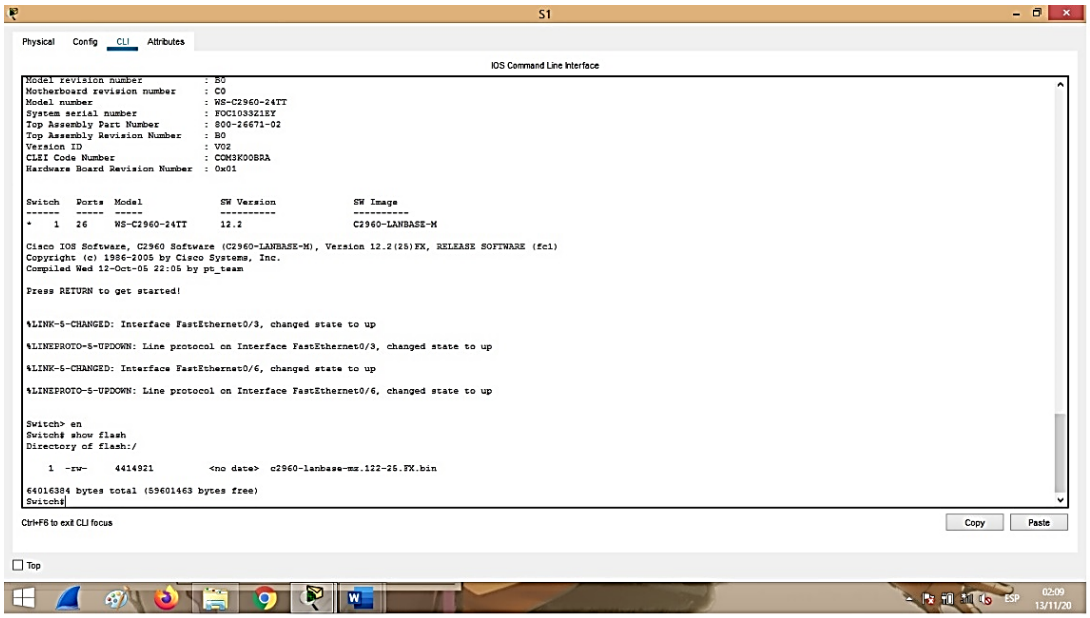
En figura 45. Observamos los comandos de inicialización del router R2.

Figura 34. Inicialización de S1-S2.



Fuente: Autor.

Figura 35. Inicialización 2. S1-S2



Fuente: Autor.

En las Figuras 46- 47 se muestran los comandos utilizados para la inicialización y el borrado de las configuraciones iniciales de los Switch S1-S2.

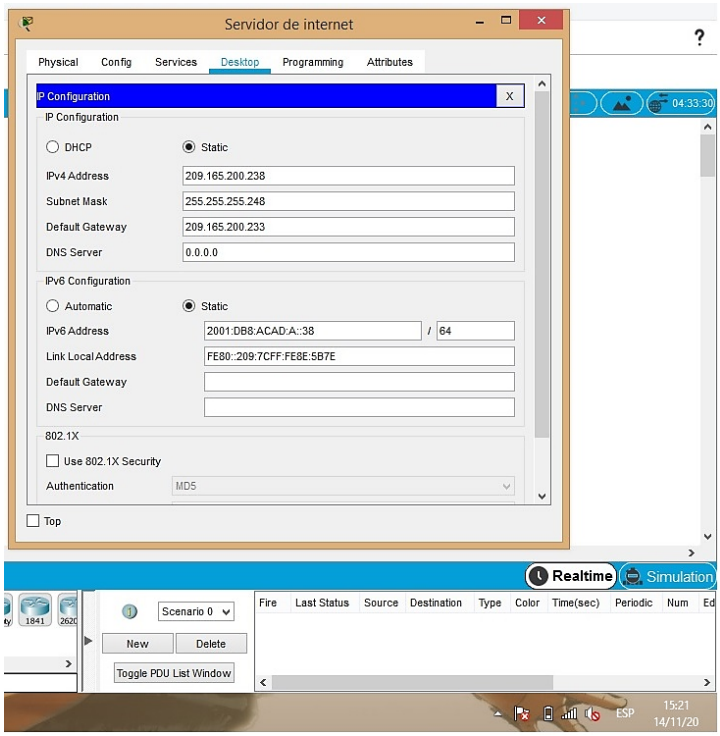
Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Tabla 30. Configuración del server

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.2555.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Figura 36. Configuración del Servidor



Fuente: Autor.

En la figura 48 se puede observar la configuración de los direccionamientos IPv4 y IPv6 para el servidor.

Paso 2: Configurar R1

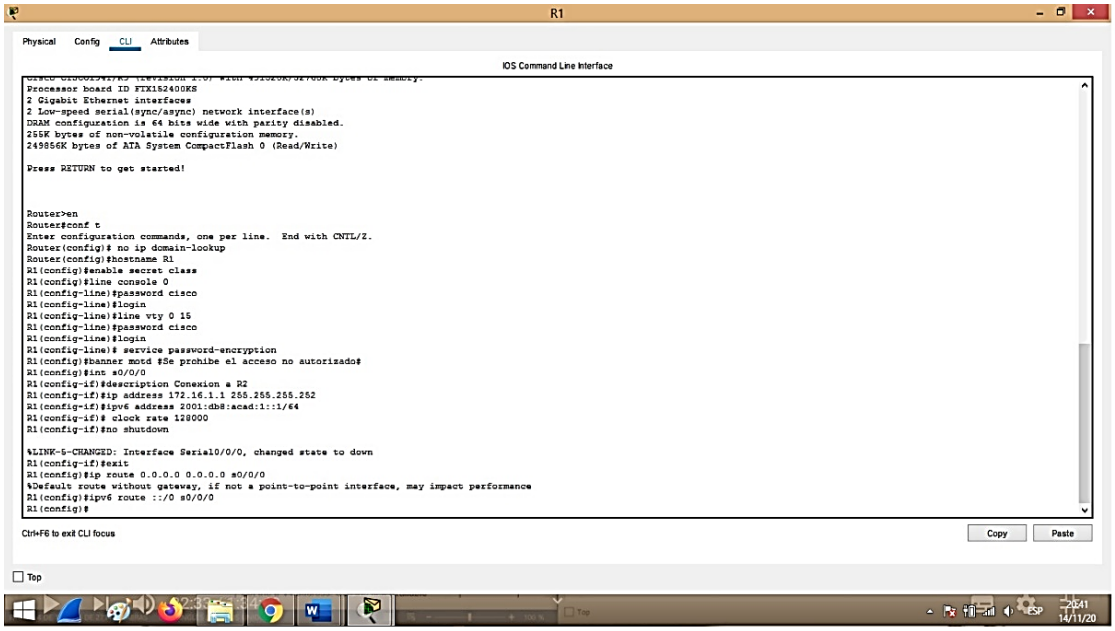
Tabla 31.Codigo Configuración R1 Escenario 2

Descripción	**Código**
Desactivar la búsqueda DNS	Router>en Router#conf t Router(config)# no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config-line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login

Cifrar las contraseñas de texto no cifrado	R1(config-line)#service password-encryption
Mensaje MOTD	R1(config)#banner motd #Se prohibe el acceso no autorizado#
Interfaz S0/0/0	Establezca la descripción R1(config)# int s0/0/0 R1(config-if)#description conexion a R2 Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones. R1(config-if)# ip address 172.16.1.1 255.255.255.252 Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones R1(config-if)# ipv6 address 2001:db8:acad:1::1/64 Establecer la frecuencia de reloj en 128000 R1(config-if)# clock rate 128000 Activar la interfaz R1(config-if)# no shutdown
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0 R1(config-if)# ip route 0.0.0.0 0.0.0.0 s0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0. R1(config-if)# ipv6 route ::/0 s0/0/0

En la tabla 31 Podemos observar los comandos y la descripción utilizados para la configuracion inicial de R1

Figura 37. Configuración de R1 Escenario 2



En la figura 49 podemos ver la configuración básica del router R1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

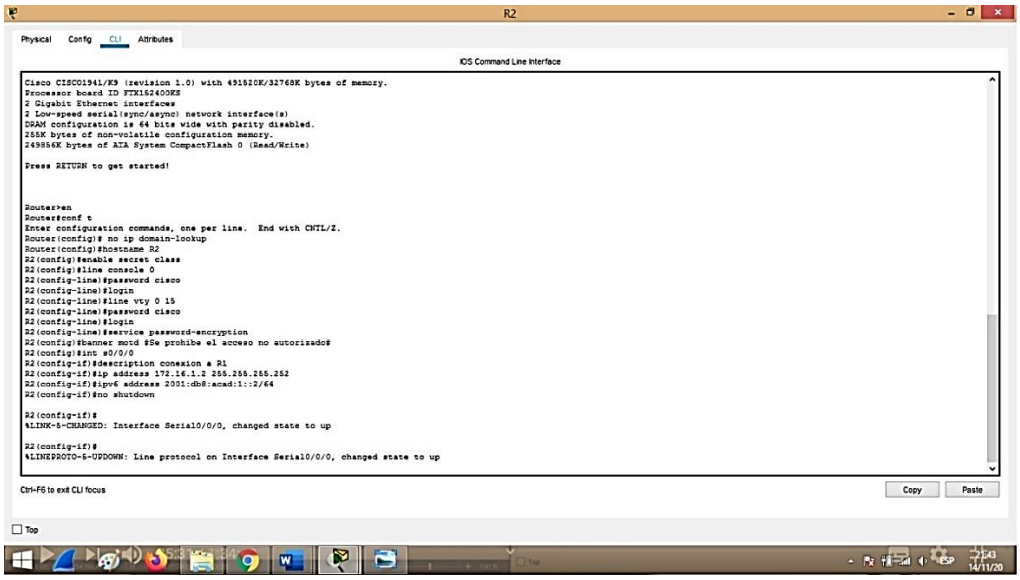
Tabla 32. Configuración en R2 escenario 2

Descripción	Código
Desactivar la búsqueda DNS	Router>en Router#conf t Router(config)# no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login

Contraseña de acceso Telnet	R2(config-line)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config-line)#service password-encryption
Habilitar el servidor HTTP	No se habilita el comando por que no es soportado en Packet tracer.
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción R2(config)# int s0/0/0 R2(config-if)#description conexion a R1 Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones. R2(config-if)# ip address 172.16.1.2 255.255.255.252 Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones R2(config-if)# ipv6 address 2001:db8:acad:1::2/64 Activar la interfaz R2(config-if)# no shutdown
Interfaz S0/0/1	Establecer la descripción R2(config)# int s0/0/1 R2(config-if)#description conexion a R3 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R2(config-if)# ip address 172.16.2.2 255.255.255.252 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.

	R2(config-if)# ipv6 address 2001:db8:acad:2::2/64 Establecer la frecuencia de reloj en 128000. R2(config-if)# clock rate 128000 Activar la interfaz R2(config-if)# no shutdown
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. R2(config-if)# description Conexion a internet Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R2(config-if)#ip address 209.165.200.233 255.255.255.248 Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 Activar la interfaz R2(config-if)# no shutdown
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. R2(config)#int loopback 0 R2(config-if)# description Simulacion de servidor web Establezca la dirección IPv4. R2(config-if)#ip address 10.10.10.10 255.255.255.255
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. R2(config)# ip route 0.0.0.0 0.0.0.0 g0/0 Configure una ruta IPv6 predeterminada de G0/0. R2(config)# ipv6 route ::/0 g0/0

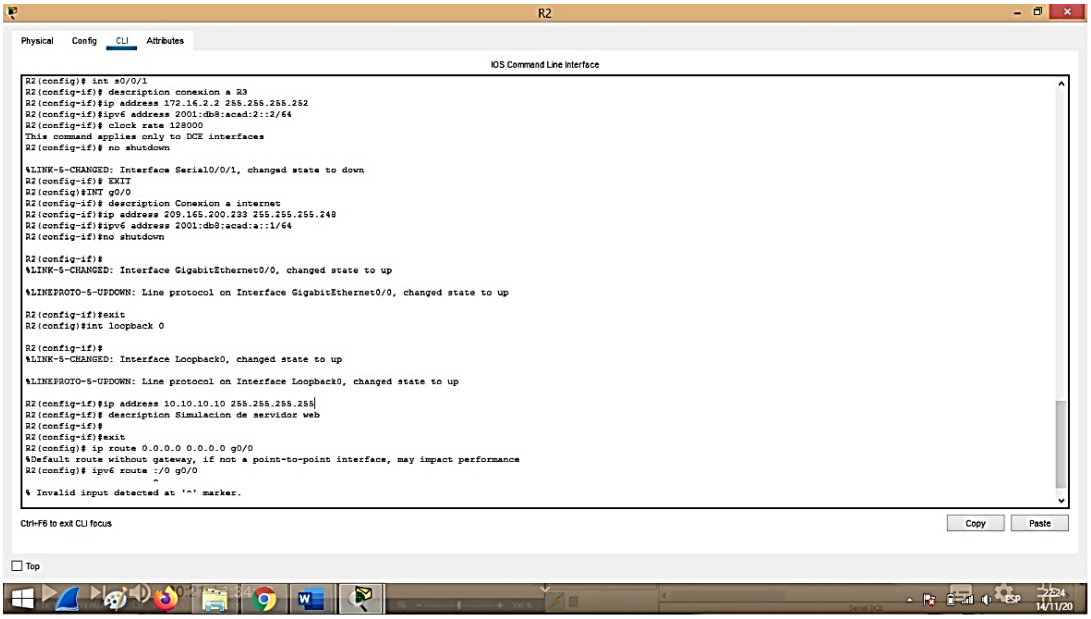
Figura 38. Configuración R2 Escenario 2



Fuente: Autor.

En la figura 50. Podemos observar los comandos ejecutados para la configuracion de R2.

Figura 39. Configuración 2 de R2 Escenario 2



Fuente: Autor.

Como se observa en las figuras 56 y 57 se realiza la configuración de R2 con las especificaciones dadas.

Paso 4: Configurar R3

Tabla 33.Configuración en R3 escenario 2

Descripción	Código
Desactivar la búsqueda DNS	Router(config)# no ip domain-lookup
Nombre del router	Router(config)# hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)# line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #Se prohibe el acceso no autorizado#
Interfaz S0/0/1	Establecer la descripción R3(config)# int s0/0/1 R3(config-if)#description Conexion a R2 Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. R3(config-if)#ip address 172.16.2.1 255.255.255.252 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config-if)#ipv6 address 2001:bd8:acad:2::1/64 Activar la interfaz R3(config-if)# no shutdown
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)# int loopback 4 R3(config-if)# ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)# int loopback 5 R3(config-if)# ip address 192.168.5.1 255.255.255.0

Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)# int loopback 6 R3(config-if)# ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config)# int loopback 7 R3(config-if)# ipv6 address 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

En la tabla 33. Podemos observar los comandos con sus respectivas descripciones de la configuracion del router R3.

Paso 5: Configurar S1

Tabla 34. Configuración en S1 escenario *2*

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

En la tabla 34. Podemos observar los comandos con sus respectivas descripciones de la configuracion del switch S1.

Paso 6: Configurar el S3

Tabla 35. Configuración en S3 escenario 2

Descripción	Código
Desactivar la búsqueda DNS	Switch>en Switch#conf t Switch(config)# no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)# enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	S3(config)#line vty 0 15 S3(config-line)# password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config-line)#service password-encryption
Mensaje MOTD	S3(config)#banner motd #Se prohibe el acceso no autorizado#

En la tabla 35. Podemos observar los comandos con sus respectivas descripciones de la configuracion del switch S3.

Paso 7: Verificar la conectividad de la red

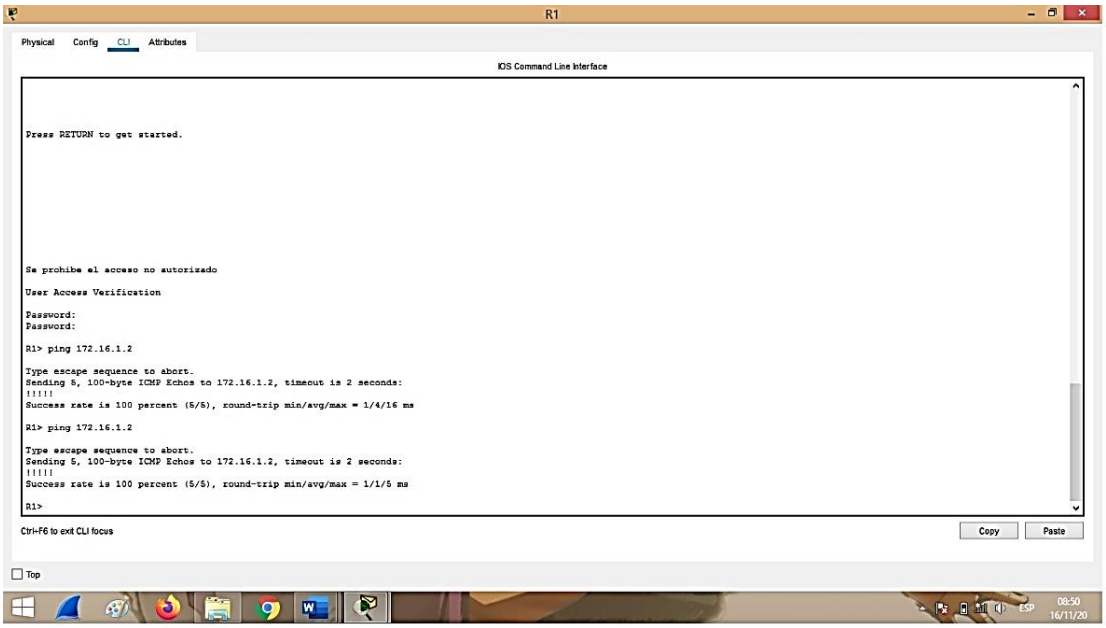
Utilice el comando ping para probar la conectividad entre los dispositivos de red.

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

Tabla 36. Verificación de Conectividad 1 escenario 2

Desde	**A**	**Dirección IP**	**Resultados de ping**
R1	R2, S0/0/0	172.16.1.2	Ok
R2	R3, S0/0/1	172.16.2.1	Ok
PC de Internet	Gateway predeterminado	209.165.200.233	Ok

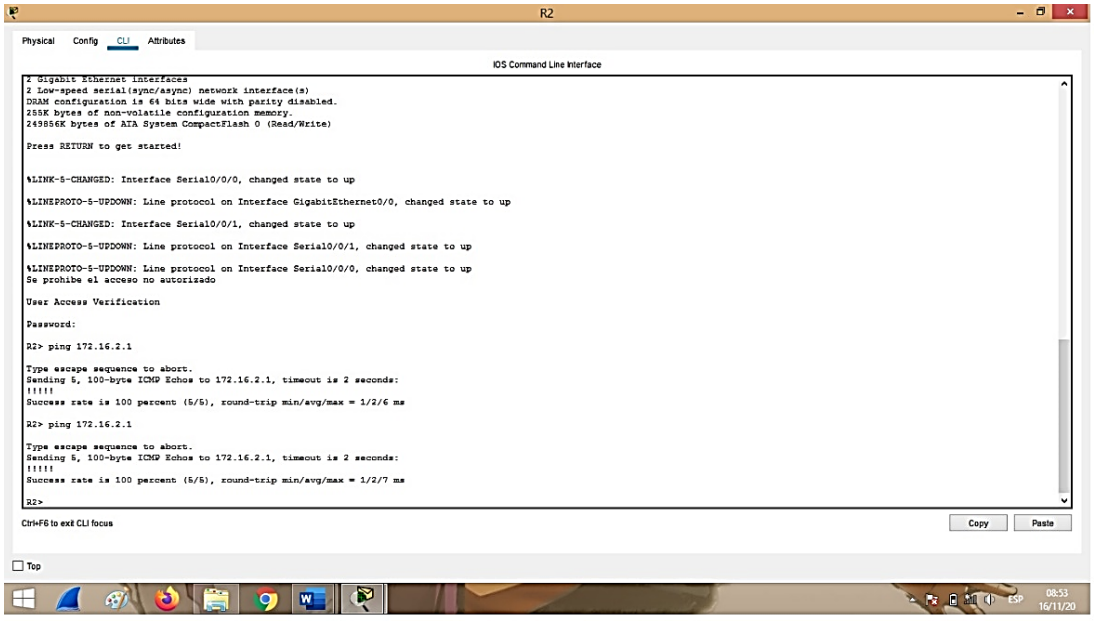
Figura 40. Verificación de Ping a R2 desde R1



Fuente: Autor.

En la figura 52. Podemos observar la realización de un Ping desde el router R1 a R2.

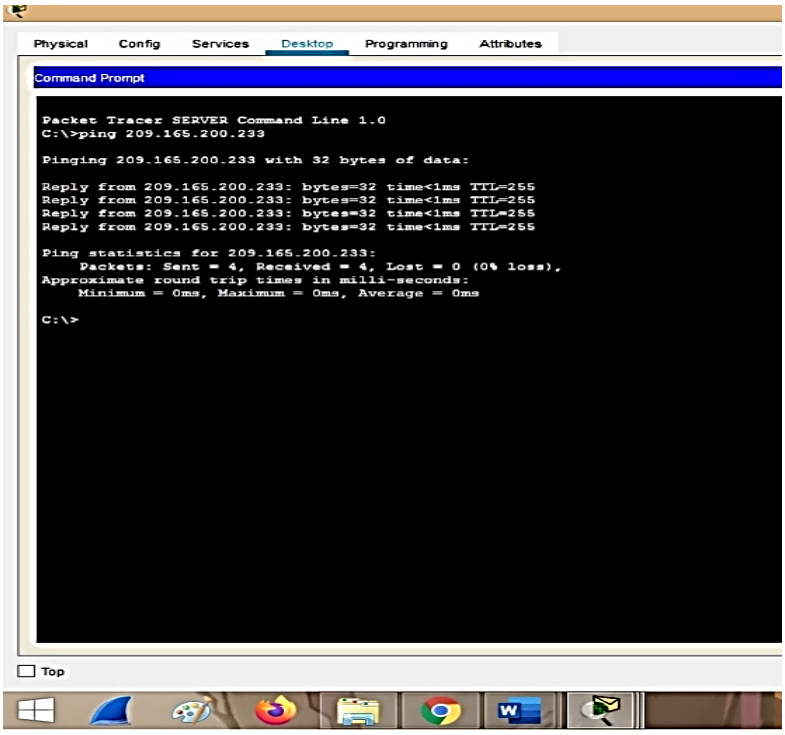
Figura 41. Verificación de ping a R3 desde R2



Fuente: Autor.

En la figura 53. Podemos observar la realización de un Ping desde el router R3 a R2.

Figura 42. Ping desde el sever al Gateway



Fuente: Autor.

En la figura 54 podemos observar un ping realizado desde el servidor a la puerta de enlace predeterminada.

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

Paso 1: Configurar S1

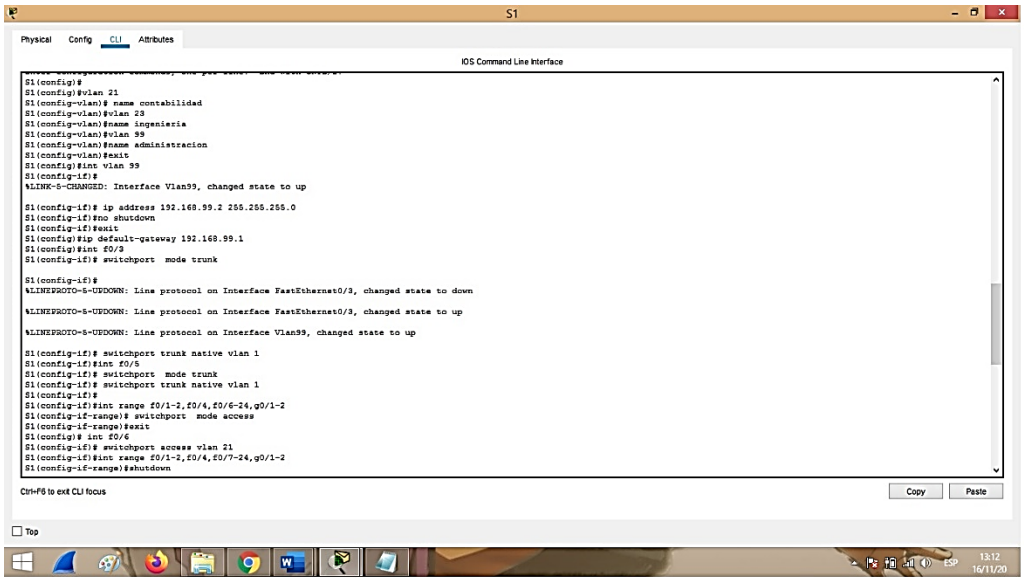
Tabla 37. Código configuración S1 vlan, routing Escenario 2

Descripción	Código
Crear la base de datos de VLAN	Se: Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar las VLAN: S1(config)# S1(config)#vlan 21 S1(config-vlan)# name contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name administracion

Asignar la dirección IP de administración.	Se asigna la dirección IPv4 a la VLAN de administración: 1(config)#int vlan 99 S1(config-if)# ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Asignar el gateway predeterminado	Se asigna el gateway predeterminado: S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Se utiliza 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
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa: S1(config-if)#int f0/5 S1(config-if)# switchport mode trunk S1(config-if)# switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Se utiliza el comando interface range : S1(config-if)#int range f0/1-2,f0/4,f0/6-24,g0/1-2 S1(config-if-range)# switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if)# switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#int range f0/1-2,f0/4,f0/7-24,g0/1-2 S1(config-if-range)#shutdown

En la tabla 37. Podemos observar los comandos y la descripción de la configuracion de las vlan, las troncales y el routing en el Switch S1.

Figura 43. Configuración de las vlan y las troncales en S1.



Fuente: Autor.

En la figura 55, se observa los comandos de configuración para la creación de las vlan y la asignación de puertos, también los puertos que se designan como troncales.

Paso 2: Configurar el S3

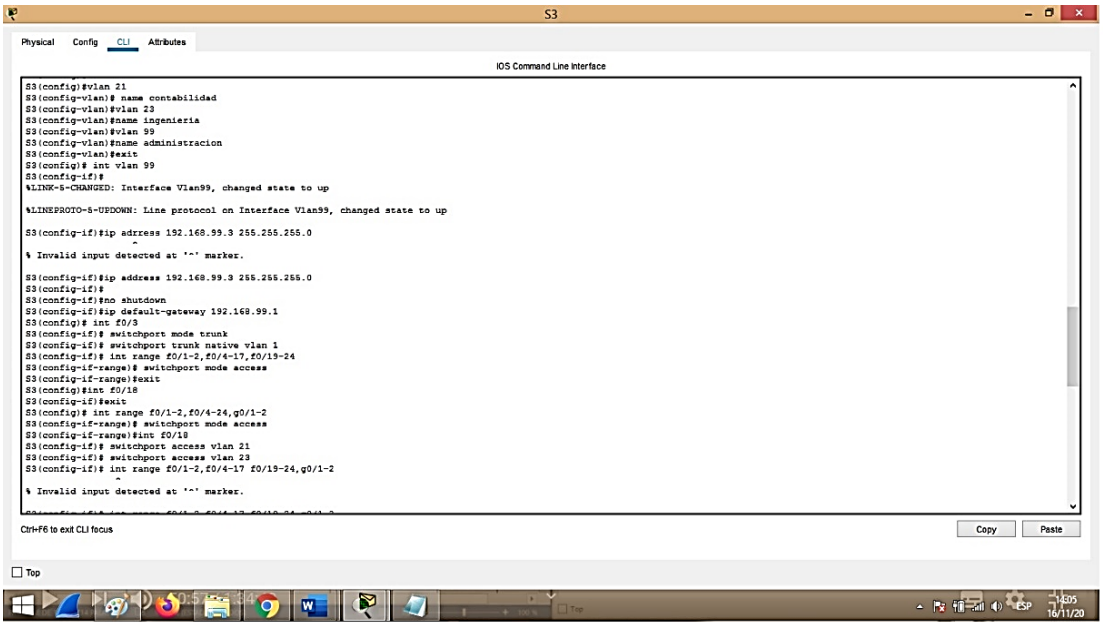
Tabla 38.Código configuración S3 vlan, routing Escenario 2

Descripción	**Código**
Crear la base de datos de VLAN	Se utiliza la tabla de equivalencias para crear cada una de las VLAN con sus respectivos nombres: S3(config)# S3(config)#vlan 21 S3(config-vlan)# name contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name administracion
Asignar la dirección IP de administración	Se asigna la dirección IPv4 a la VLAN de administración: S3(config)# int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
Asignar el gateway predeterminado.	Asigna la primera dirección IP como gateway predeterminado: S3(config-if)#ip default-gateway 192.168.99.1

Forzar el enlace troncal en la interfaz F0/3	Se utiliza la red VLAN 1 como VLAN nativa 3(config)# int f0/3 S3(config-if)# switchport mode trunk S3(config-if)# switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Se utiliza el comando interface range: S3(config)# int range f0/1-2,f0/4-24,g0/1-2 S3(config-if-range)# switchport mode access
Asignar F0/18 a la VLAN 23	S3(config-if-range)#int f0/18 S3(config-if)# switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)# int range f0/1-2,f0/4-17,f0/19-24,g0/1-2 S3(config-if-range)# shutdown

En la tabla 38. Podemos observar los comandos y la descripción de los mismos, los cuales periten la configuracion de las vlan, troncales, realización de routing, apagado de interfaces, configuracion de puertos entre otras varias acciones las cuales permiten la configuracion del switch S3.

Figura 44. Configuración de vlans y troncales en S3



Fuente: Autor.

En la figura 56 se puede observar la configuración del swicth S3, creación de la vlan y la asignación de puertos.

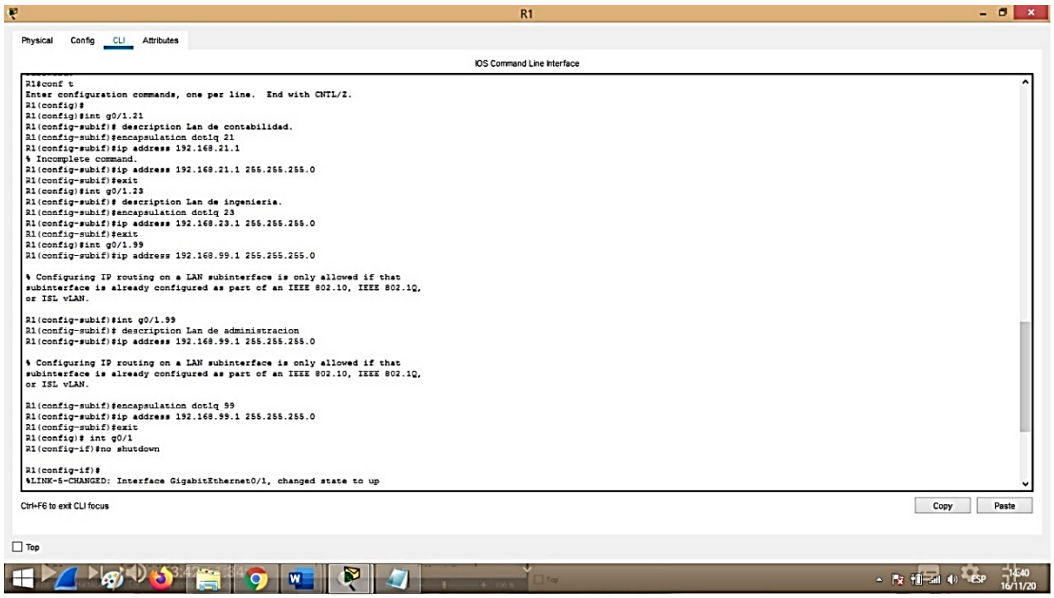
Paso 3: Configurar R1

Tabla 39. Código configuración de Subinterfaces en R1 Escenario 2

Descripción	**Código**
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad R1(config)#int g0/1.21 R1(config-subif)# description Lan de contabilidad. Se asigna la VLAN 21: R1(config-subif)#encapsulation dot1q 21 Se asigna la primera dirección disponible: R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería R1(config)#int g0/1.23 R1(config-subif)# description Lan de ingenieria. Se asigna la VLAN 23: R1(config-subif)#encapsulation dot1q 23 Se asigna la primera dirección disponible: R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración. R1(config)#int g0/1.99 R1(config-subif)# description Lan de administracion Se asigna la VLAN 99: R1(config-subif)#encapsulation dot1q 99 Se asigna la primera dirección disponible: R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	Se activa la interfaz G0/1: R1(config-if)#no shutdown.

En la tabla 39. Podemos observar la configuracion de las subinterfaces 21,23,99 y la activación de la interfaz G0/1. Con sus respectivos comandos y descripción

Figura 45. Configuración de interfaces en R1.



Fuente: Autor.

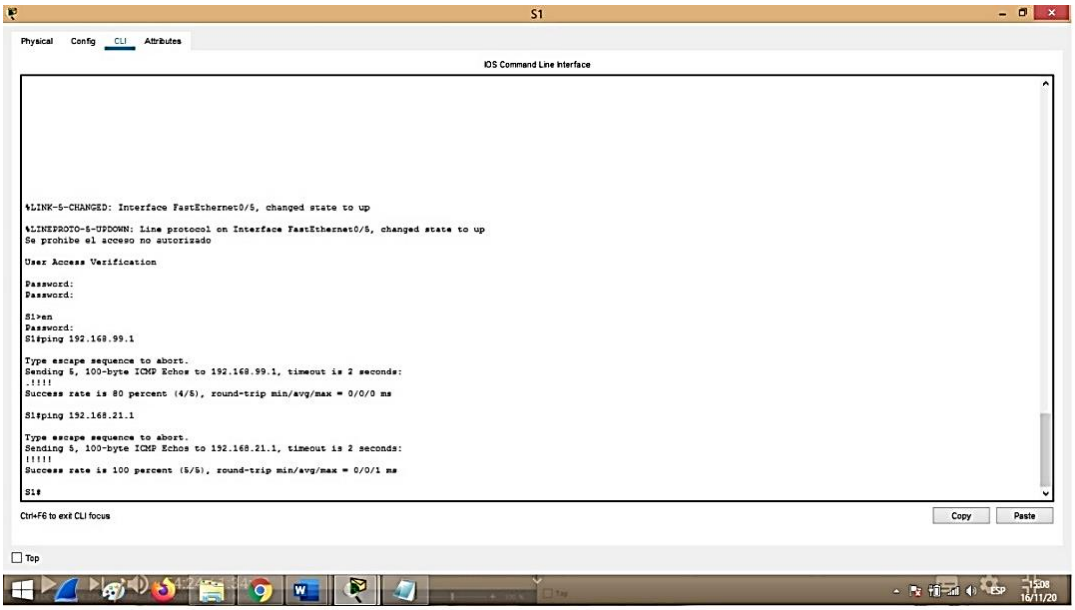
En la figura 57, podemos observar la ejecución de los comandos para la configuración de las subinterfaces en la g0/1 en el R1.

Paso 4: Verificar la conectividad de la red

Tabla 40. Verificación de conectividad 2 Escenario 2

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

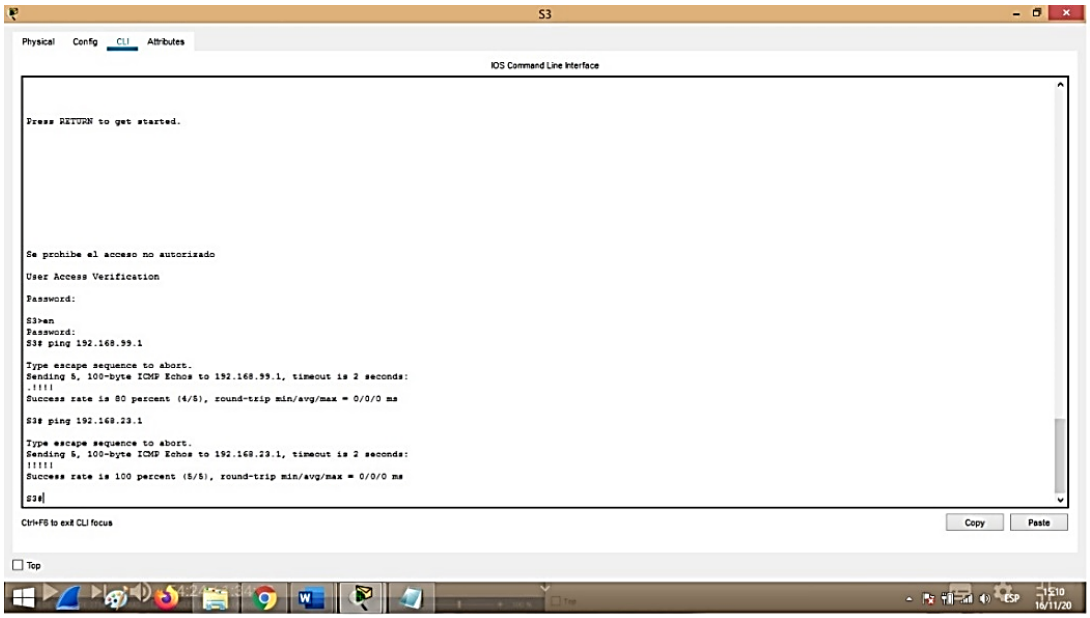
Figura 46. Verificación de Pines desde S1 a R1



Fuente: Autor.

En la figura 58. Podemos observar la realización de un Ping a R1 desde el switch S1.

Figura 47. Verificación de Pines de S3 a R1



Fuente: Autor.

En Figura 66-67. Se puede observar ejecución de los pines a las subredes de las vlan 21,23,99 desde los switch S1-S3.

Parte 4: Configurar el protocolo de routing dinámico OSPF

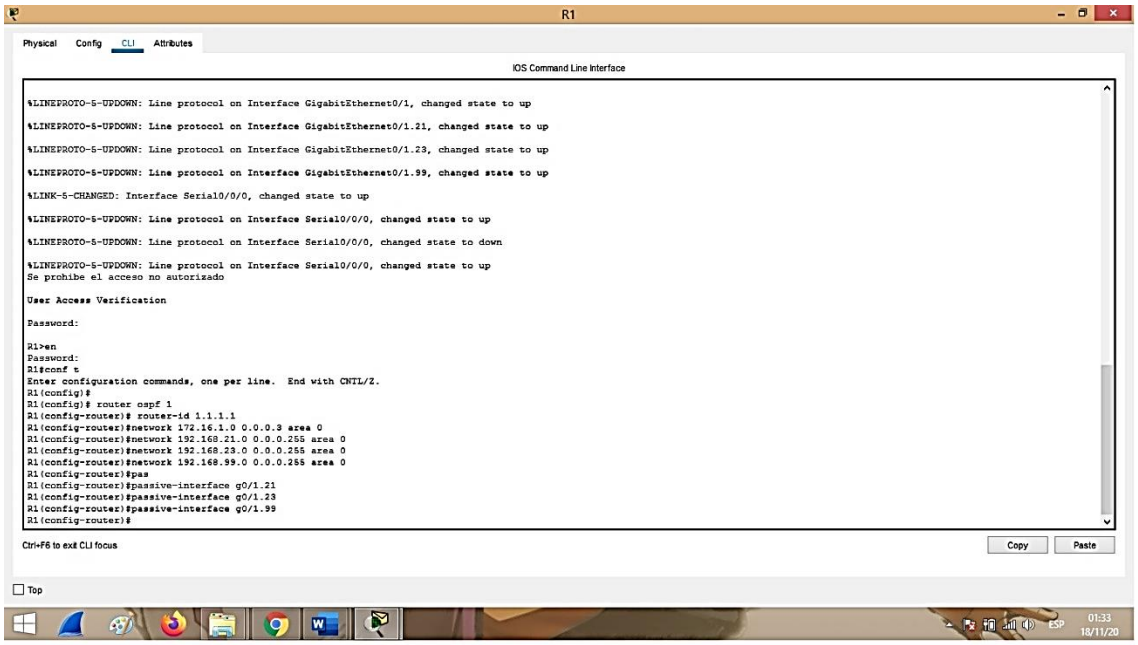
Paso 1: Configurar OSPF en el R1

Tabla 41. OSPF en R1 Escenario 2

Descripción	Código
Configurar OSPF área 0	R1(config)# R1(config)# router ospf 1 R1(config-router)# router-id 1.1.1.1
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
Desactive la sumarización automática	No es necesario deshabilitarla ya que OSPF NO REALIZA resumen automático.

En la tabla 41. Podemos observar los comandos y la descripción ejecutados para la configuracion de OSPF en el Router R1.

Figura 48. OSPF en R1



Fuente: Autor.

Como se observa en la figura 60 se configura OSPF en R1 siguiendo los parámetros descritos en el ítem.

Paso 2: Configurar OSPF en el R2

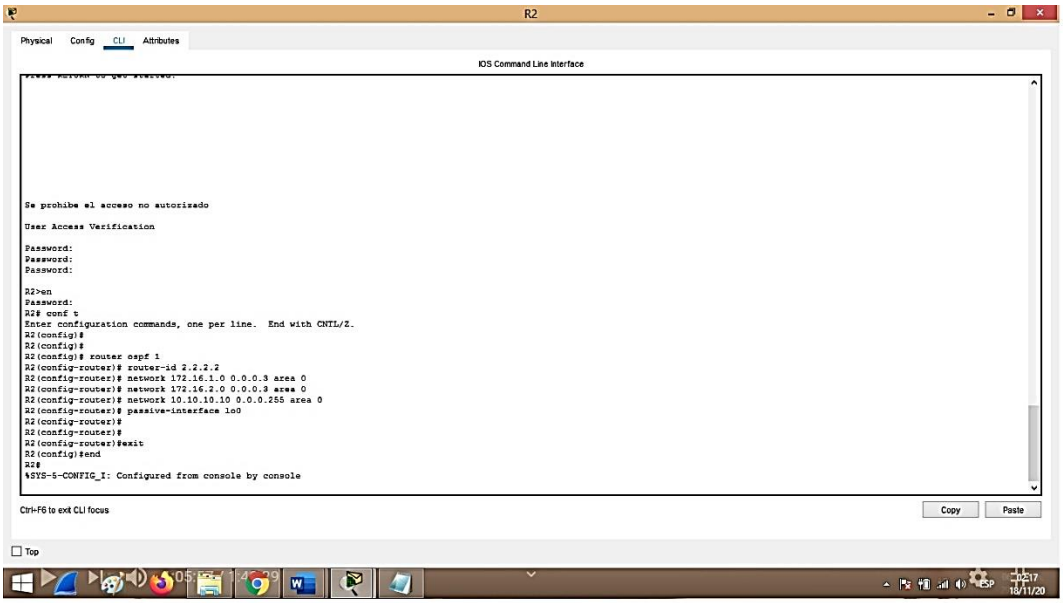
Tabla 42.OSPF en R2 Escenario 2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)# router ospf 1 R2(config-router)# router-id 2.2.2.2 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 R2(config-router)# network 10.10.10.10 0.0.0.255 area 0 **Nota:** Se omite la red G0/0. De la configuración de OSPF
Anunciar las redes conectadas directamente	
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)# passive-interface lo0

Desactive la sumarización automática.	No es necesario deshabilitarla ya que OSPF NO REALIZA resumen automático.

En la tabla 42. Podemos observar los comando y la descripción de la configuracion de OSPF en el Router R2.

Figura 49. OSPF en R2



Fuente: Autor.

Como se observa en la figura 61 se configura OSPF en R1 siguiendo los parámetros descritos en el ítem.

Paso 3: Configurar OSPFv3 en el R3

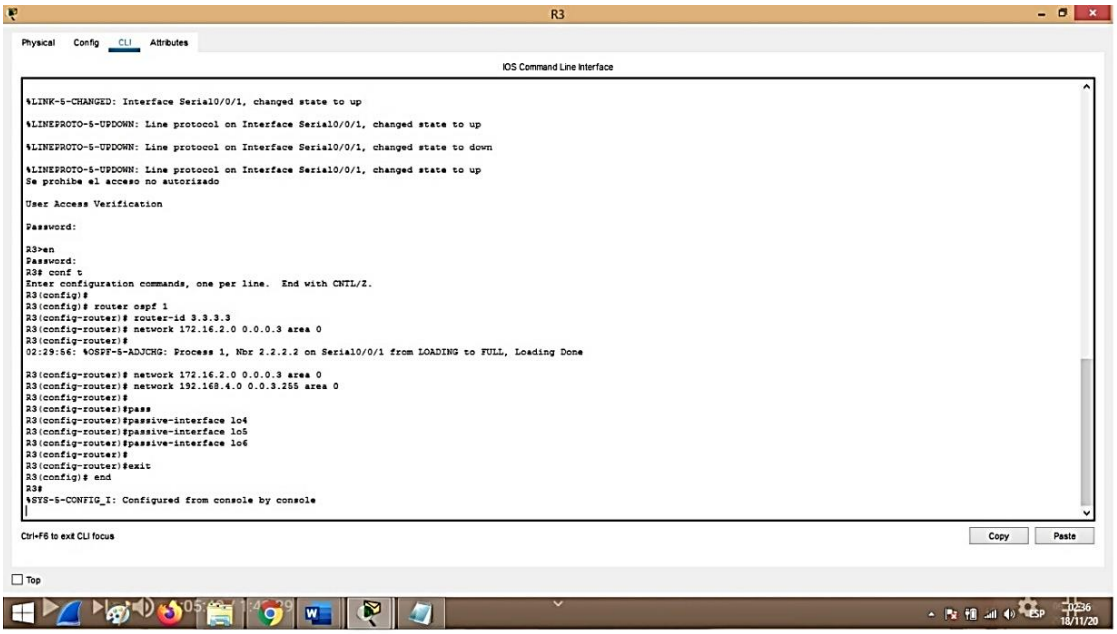
Tabla 43.OSPF en R3 Escenario 2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)# router ospf 1 R3(config-router)# router-id 3.3.3.3 R3(config-router)# network 172.16.2.0 0.0.0.3 area 0 R3(config-router)# network 192.168.4.0 0.0.3.255 area 0
Anunciar redes IPv4 conectadas directamente	

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
Desactive la sumarización automática.	No es necesario deshabilitarla ya que OSPF NO REALIZA resumen automático.

En la tabla 43. Podemos observar los comandos y la descripción de la configuracion de OSPF en R3.

Figura 50.OSPF en R3



Fuente: Autor.

Como se observa en la figura 62 se configura OSPF en R1 siguiendo los parámetros descritos en el ítem. En la asignacion de directa de las direcciones en la parte de asignacion de las loopback se realiza una sumariazacion de forma manual.

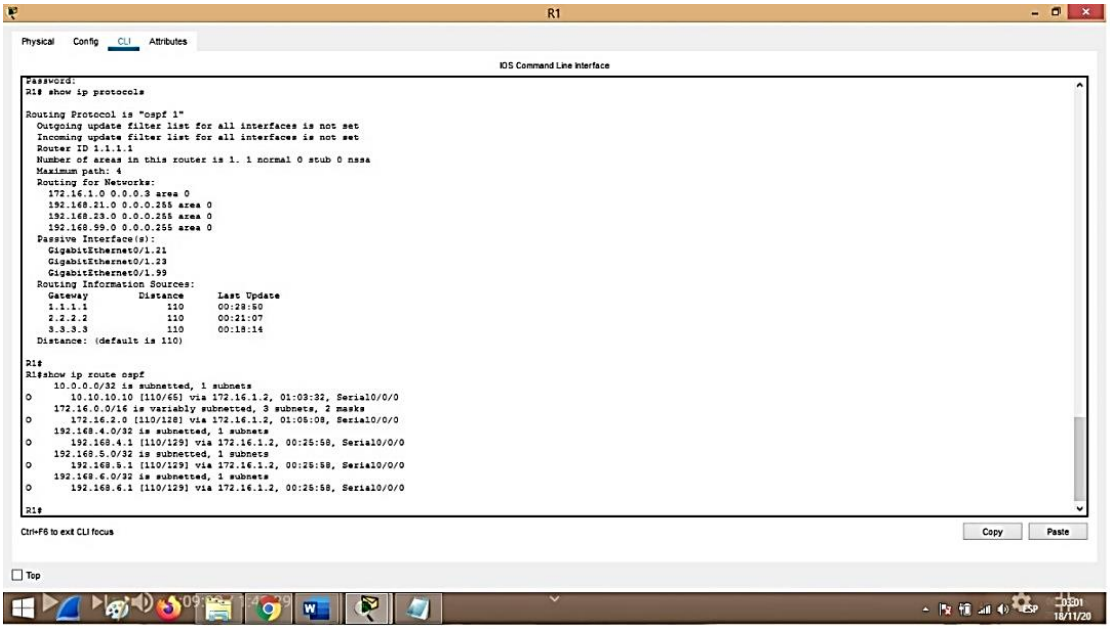
Paso 4: Verificar la información de OSPF

Tabla 44. Verificación 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
¿Qué comando muestra solo las rutas OSPF?	R1#show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R1# show run

En la tabla 44. Se observa la respuesta a preguntas relacionadas con los comandos de Configuracion de OSPF.

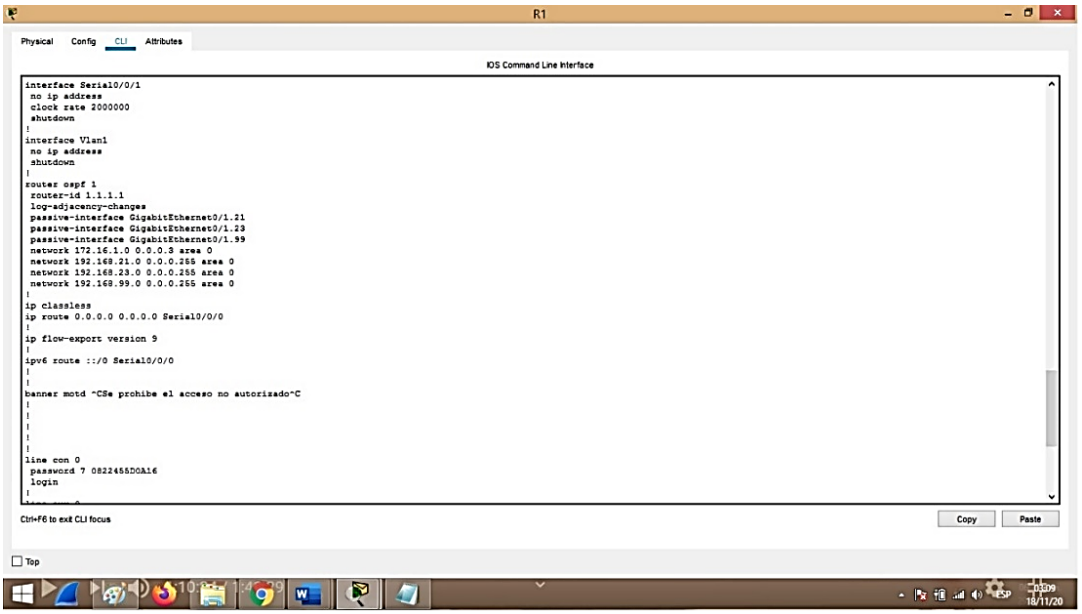
Figura 51. Verificación de comandos



Fuente: Autor.

Como se observa en la figura 63. El comando ejecutado “show ip protocols” nos permite observar el ID del proceso OSPF, ID del router, las interfaces pasivas configuradas anteriormente, en este caso el comando lo ejecutamos en el router 1 o R1, pero es de la misma manera para los otros 2 dispositivos ubicados en nuestra red. También podemos observar la ejecución del comando “show ip router ospf”, el cual nos permite observar las rutas OSPF configuradas previamente en el Router R1.

Figura 52. Verificación de comandos 2



Fuente: Autor.

En la figura 64 podemos observar la ejecución del comando “Show Run” el Cual nos permite observar la configuración general del router, donde también se observa la configuración de OSPF.

Parte 5: Implementar DHCP y NAT para IPv4

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

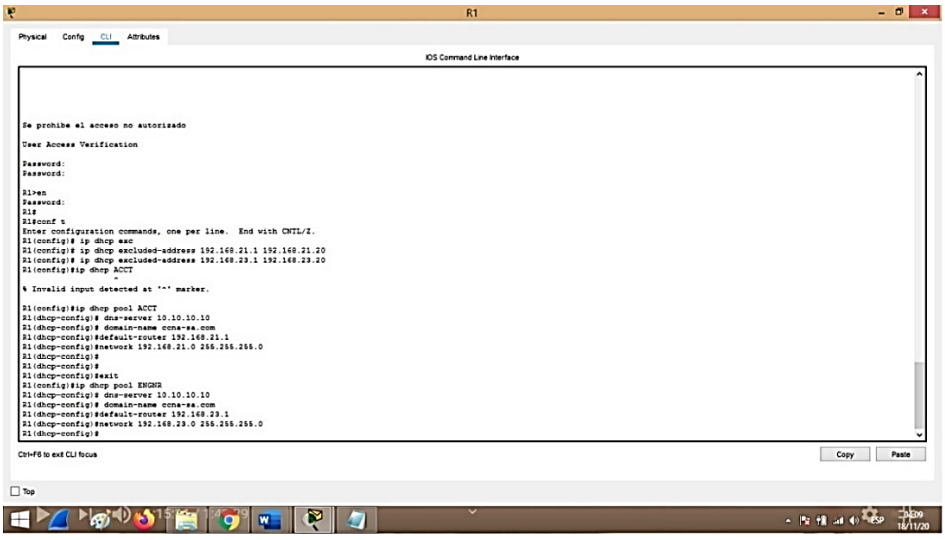
Tabla 45. Código Configuración Servidor DHCP

Descripción	**Código**
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.	Se crea y se agrega un nombre al pool R1(config)#ip dhcp pool ACCT Se configura el servidor DNS: R1(dhcp-config)# dns-server 10.10.10.10 Se agrega nombre de dominio: R1(dhcp-config)# domain-name ccna-sa.com Es establece el gateway predeterminado: R1(dhcp-config)#default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23	Se crea y se agrega un nombre al pool R1(config)#ip dhcp pool ENGNR Se configura el servidor DNS: R1(dhcp-config)# dns-server 10.10.10.10 Se agrega nombre de dominio: R1(dhcp-config)# domain-name ccna-sa.com Es establece el gateway predeterminado: R1(dhcp-config)#default-router 192.168.23.1

En la tabla 45. Podemos observar los comandos y su descripción para la creación del Pool DHCP. En las diferentes vlan creadas en el router R1.

Figura 53.Creación y configuración de Pool DHCP



Fuente: Autor.

Como se observa en la figura 65. Se procede a crear y configurar los pools DHCP para las vlan 21 y 23.

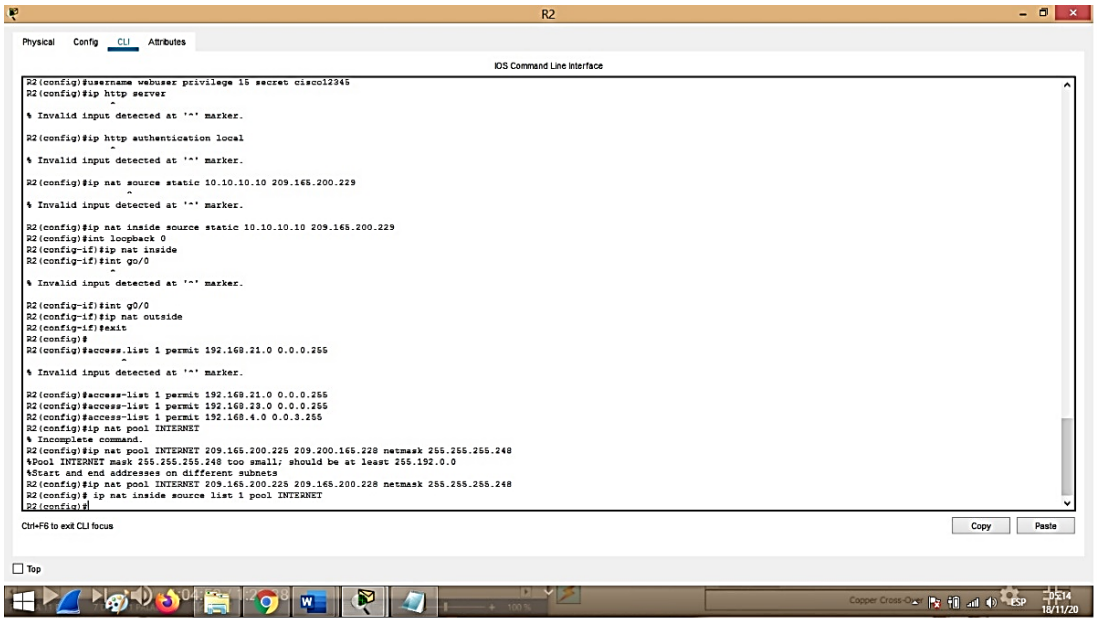
Paso 2: Configurar la NAT estática y dinámica en el R2

Tabla 46.Codigo Configuración NAT en R2 Escenario 2

Descripción	Código
Crear una base de datos local con una cuenta de usuario	Se configura nombre de usuario, contraseña, y nivel de privilegio: R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	Este es el comando para esta tarea, pero no es soportado por packet tracer: R2(config)#ip http server.
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	Este es el comando para esta tarea, pero no es soportado por Packet tracer: R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	Se asigna 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-if)#ip nat inside R2(config-if)#int g0/0 R2(config-if)#ip nat outside
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 y Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1: 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 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	Se define nombre y el conjunto de direcciones para el pool: 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

Tabla 46. Se observa la configuracion y creación de la NAT estática y dinámica en el router R2.

Figura 54. Configuración NAT en R2



Fuente: Autor.

En la figura 66. podemos observar la configuración de las NAT estáticas y dinámicas, definición de la NAT dinámica interna y externa, configuración de NAT dinámica dentro de una lista ACL privada, definición del pool de direcciones públicas que son utilizables. Entre otros parámetros que se describen a detalla en cada uno de los pasos del ítem anterior.

Paso 3: Verificar el protocolo DHCP y la NAT estática

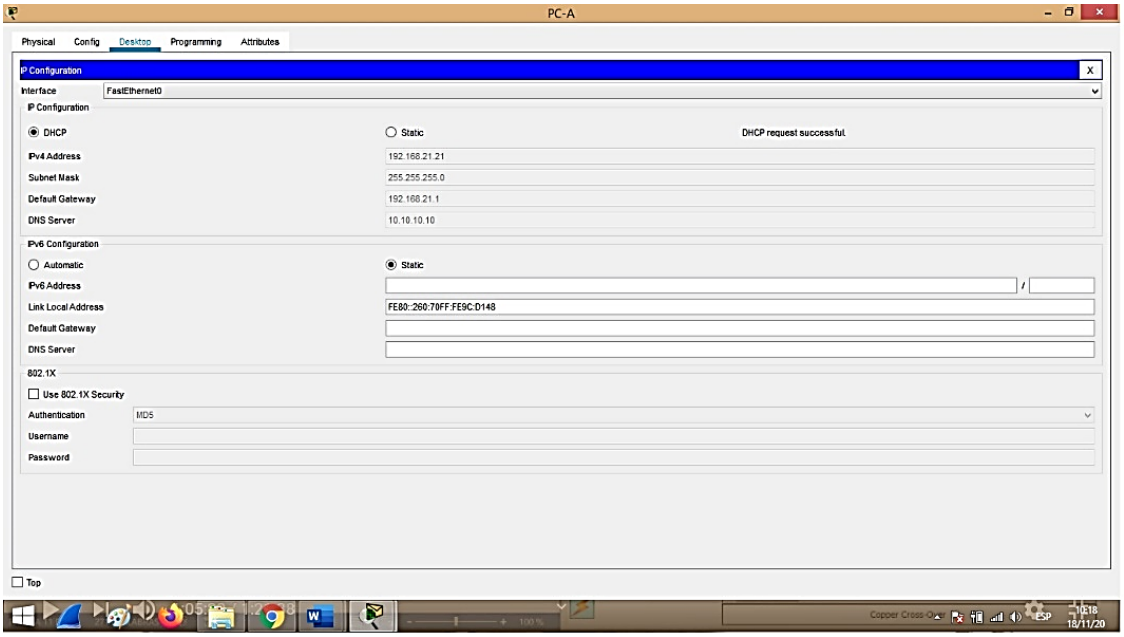
Tabla 47.Verificar el protocolo DHCP y la NAT

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Se verifica y está en estado Ok
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Se verifica y está en estado Ok

Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Se realiza ping a la dirección IP de la PC-C 192.168.33.21 el cual resulta correcto. Ok
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Packet tracer no soporta esta operación pero se realiza un ping desde el servidor a la dirección IP descrita el cual resulta satisfactorio. OK

En la tabla 46. Se observa o se da respuesta a los interrogantes propuestos en la misma sobre la configuracion de DHCP y NAT.

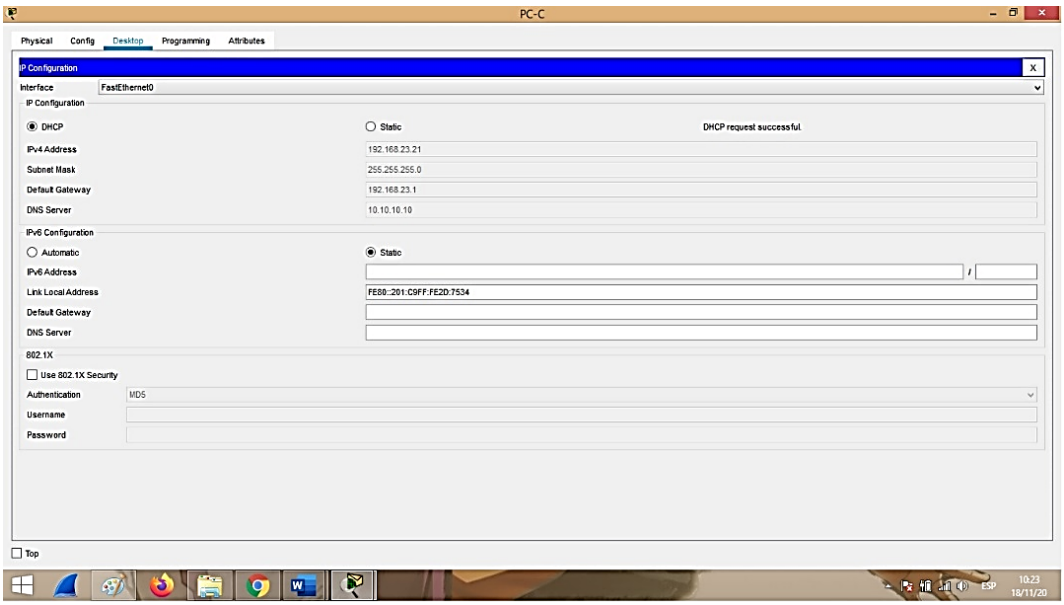
Figura 55. Verificación de DHCP en la PC-A



Fuente: Autor.

En la figura 67. Se observa la verificación del DHCP en la PC-A, el cual se configuro de forma correcta.

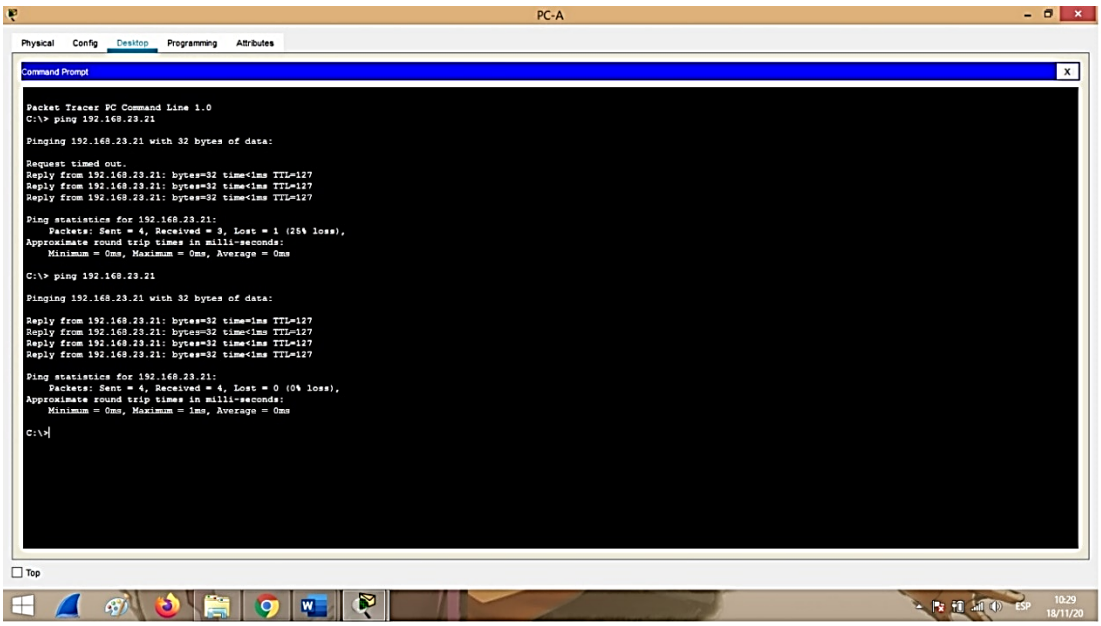
Figura 56.Verificación de DHCP en la PC-C



Fuente: Autor.

En la figura 68. Se observa la verificación del DHCP en la PC-C, el cual se configuro de forma correcta.

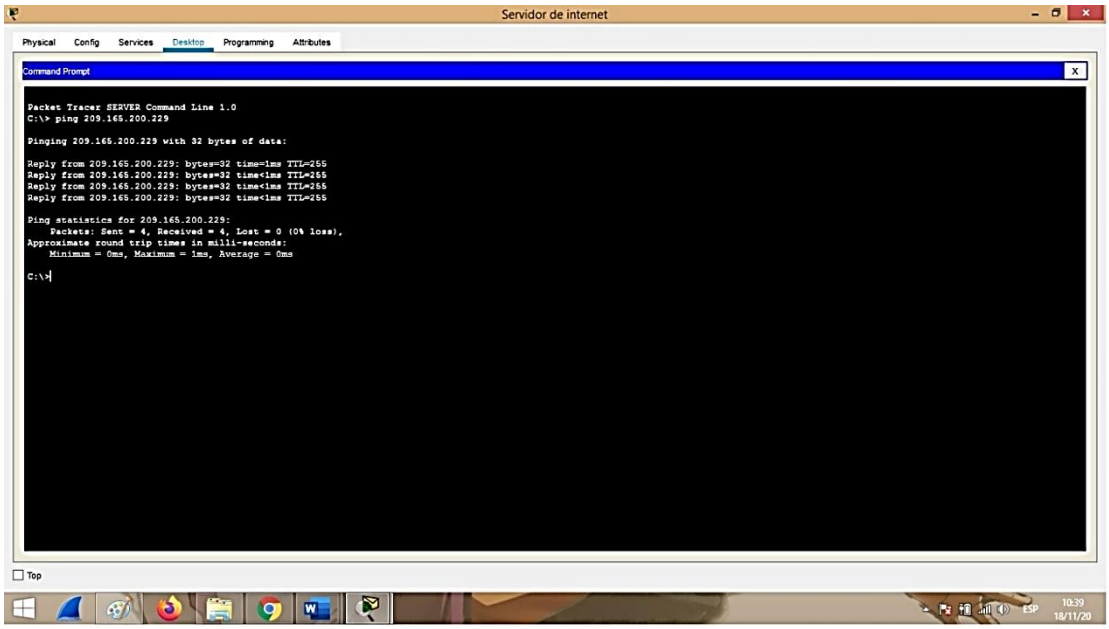
Figura 57. Verificación de Ping Desde PC-A a PC-C



Fuente: Autor.

En la figura 69. Se observa la realización de un Ping desde la PC-A a la PC-C el cual resulta satisfactorio.

Figura 58. Ping desde el servidor.



Fuente: Autor.

En la figura 70. Se observa la realización de un Ping desde el servidor a la dirección IP 209.165.200.229 resulta satisfactorio Ok, este se realiza ya que Packet tracer no soporta la realiza con de la verificación por medio del navegador web del servidor.

Parte 6: Configurar NTP

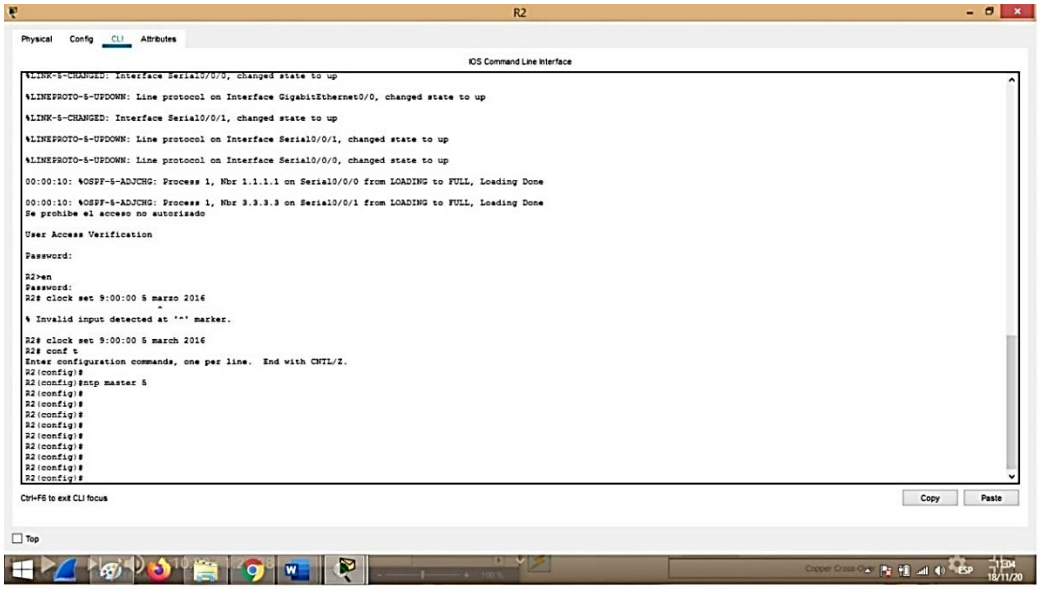
Tabla 48.Codigo Configuración NTP en R1 y R2

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**Se configura la fecha y hora en R2 :** R2# clock set 9:00:00 5 march 2016
Configure R2 como un maestro NTP.	Se establece como maestro nivel 5: R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Se establece R2 como servidor NTP: 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 ntp associations

En la tabla 48. Podemos observar los comandos y la descripción de la configuracion del reloj del router R1 y R2. la configuracion de NTP en ambos Routers.

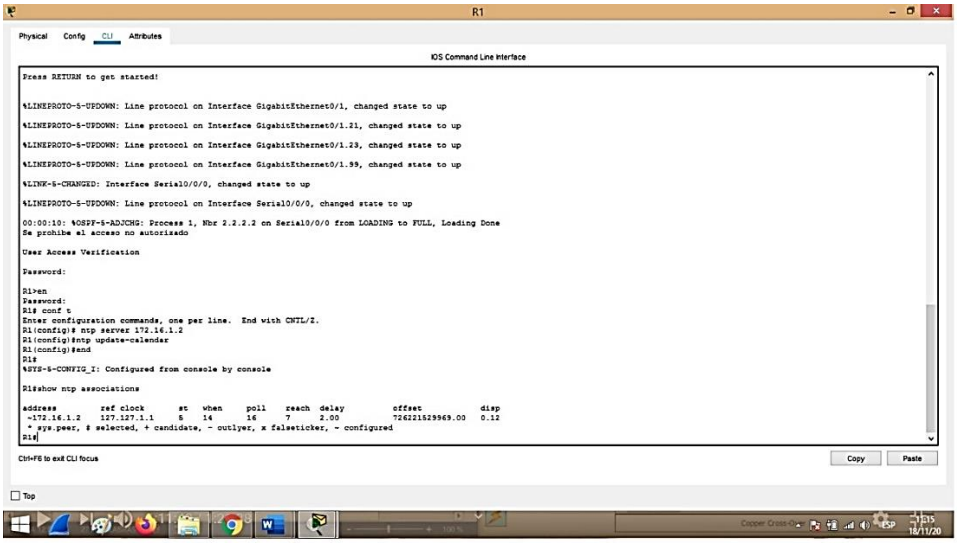
Figura 59.Configuración NTP R2.



Fuente: Autor.

Se configura la hora y fecha según lo establece el ítem anterior, R2 tambien se configura como maestro NTP con un estrato nivel 5.

Figura 60.Configuración NTP en R1



Fuente: Autor.

En la figura 72. Se observa cómo se establece la configuración de NTP en R1 donde se deja como servidor a R2 y se activa la actualización de calendario, también se realiza la verificación de la configuración NTP en R1 por medio del comando “show tnp associations”.

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

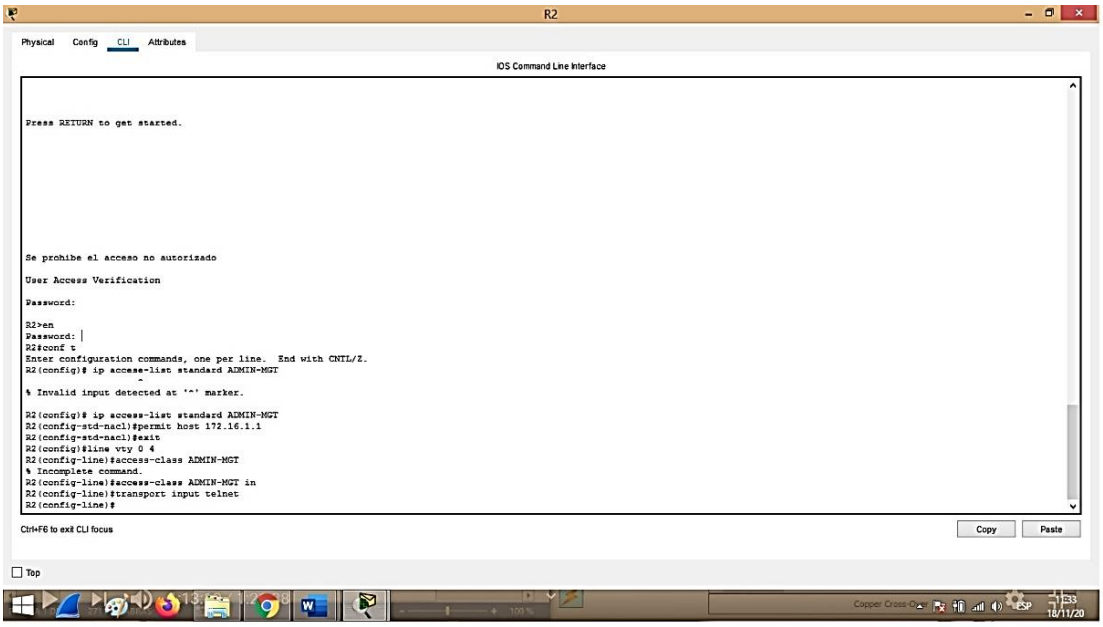
Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 49.Restricción de líneas VTY en R2

Descripción	Código
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(config)# ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	Desde R1 se verifica el acceso: R1# telnet 172.16.1.2 Trying 172.16.1.2 ...OpenSe prohibe el acceso no autorizado User Access Verification Password: R2>en

En la tabla 49. Podemos observar los comandos y la descripción de la configuracion de restricción de las líneas VTY al acceder por medio de telnet y la verificación del funcionamiento de ACL.

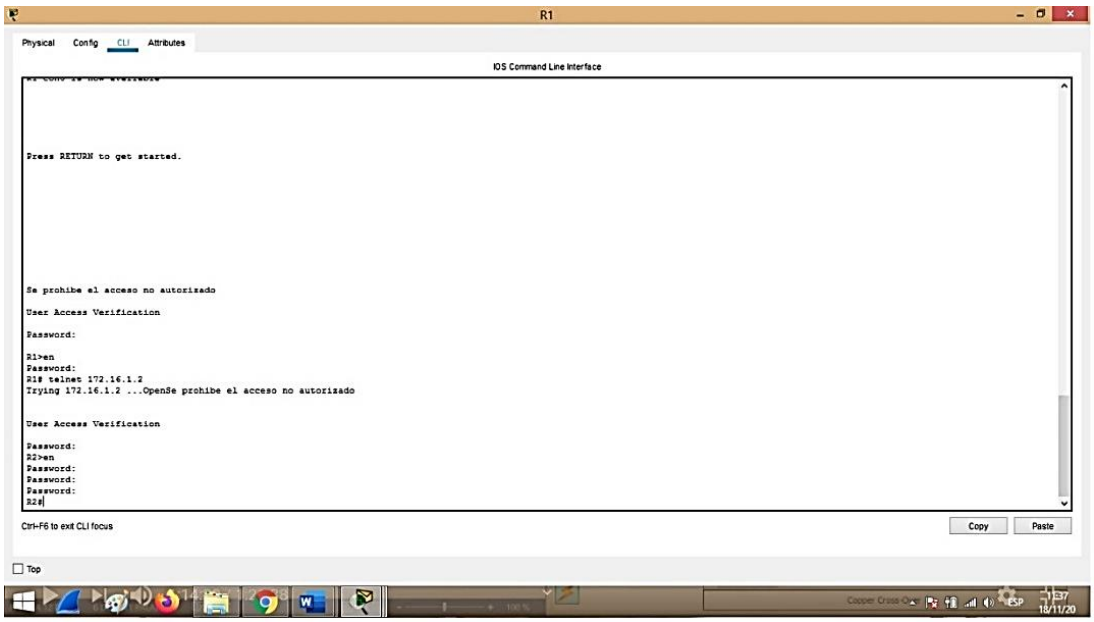
Figura 61. Configuración de acceso a R2.



Fuente: Autor.

En la figura 73. Se observa cómo se establece la configuración de la conexión telnet entre R1 y R2, También se configura las líneas VTY y se ingresa con nombre la ACL. Todo esto permite que solo R1 tenga acceso a R2.

Figura 62. Verificación de acceso a R2 desde R1.



Fuente: Autor.

Se verifica el correcto funcionamiento de la ACL, pues podemos acceder a R2 desde R1 sin ningún inconveniente.

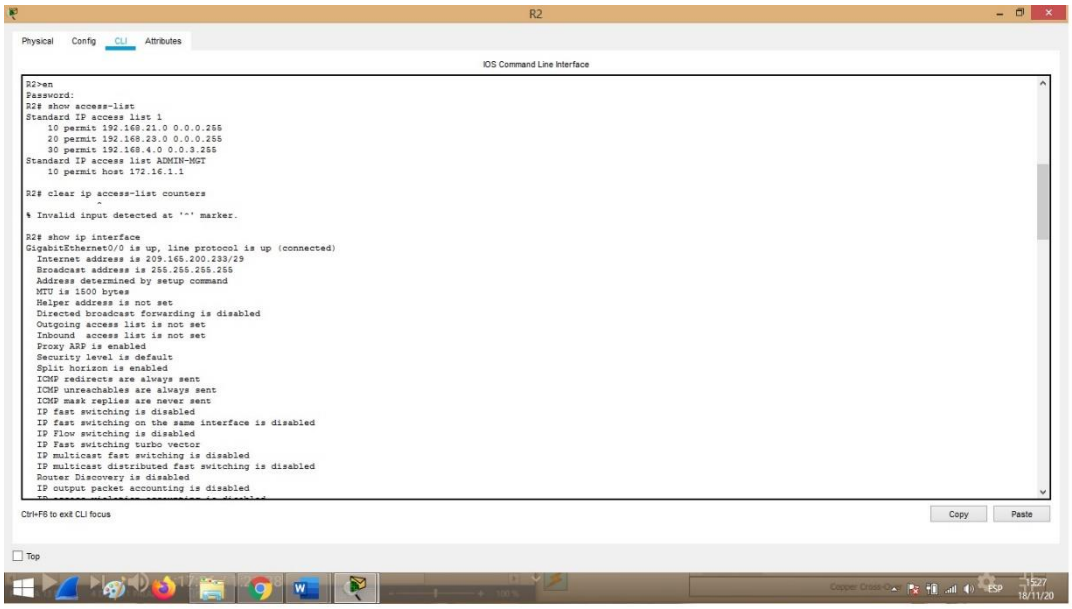
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 50. Verificación de comandos

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Me diente este comando podemos observar las coincidencias recibidas por la lista de acceso: R2# show access-list
Restablecer los contadores de una lista de acceso	R2# clear ip access-list counters. Este es comando que permite realizar dicha función, pero Packet traer no lo soporta.
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Este es el comando que permite realizar esta labor: R2# show ip interface
¿Con qué comando se muestran las traducciones NAT?	Se configuran las interfaces S0/0/0 y S0/0/1 en R2 como NAT inside y se procede a realizar pung desde la PC-A. luego se muestran las traducciones.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2# clear ip nat translation *

En la tabla 50. Podemos observar la respuesta los interrogantes planteados indicando que comandos son los adecuados para cad requerimiento de la tabla.

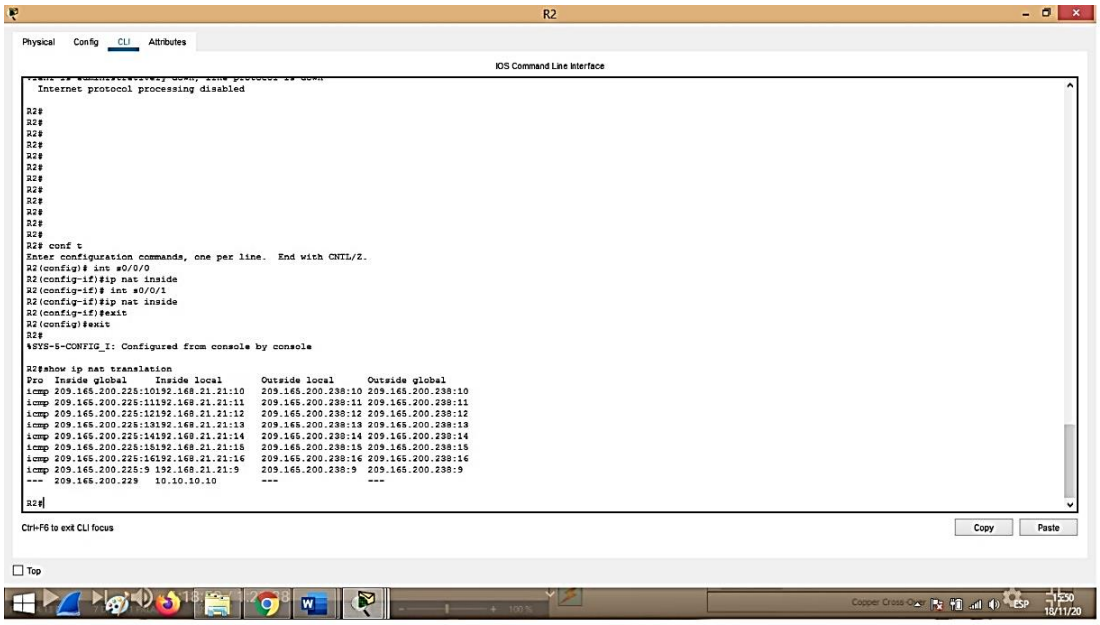
Figura 63. Verificación de comandos



Fuente: Autor.

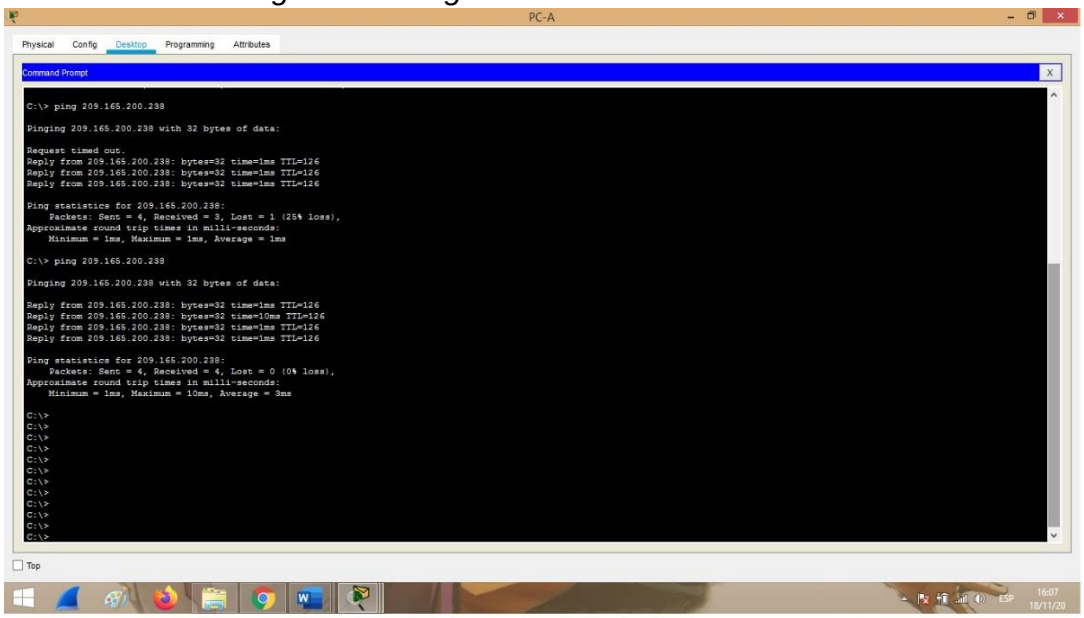
En la figura 75. Se puede apreciar los comandos ejecutados las el reset de contadores de la lista, coincidencias recibidas por la lista de acceso.

Figura 64. Verificación de traducciones en R2.



Fuente: Autor.

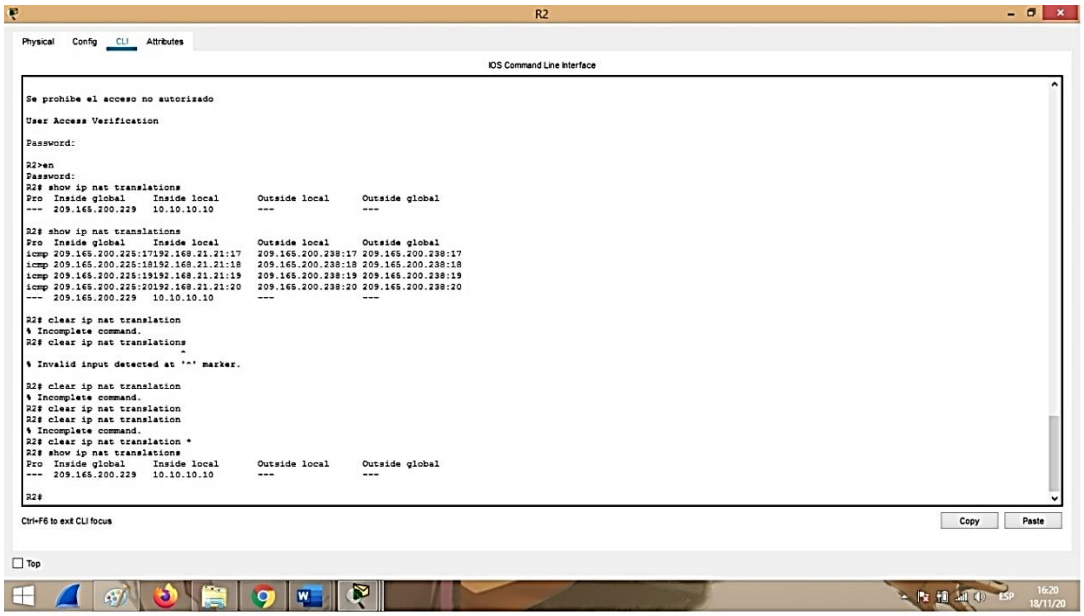
Figura 65. Ping al servidor desde la PC-A.



Fuente: Autor.

En las figuras 76-77. Podemos observar la configuración de las interfaces seriales S0/0/0 y S0/0/1 como NAT inside en R2, para poder realizar un ping desde la PC-A hasta el servidor y que las traslaciones se observen en R2 de forma correcta.

Figura 66. Comando para eliminar traslaciones



Fuente: Autor.

En esta figura podemos observar la ejecución del comando que permite eliminar las traslaciones de la lista.

CONCLUSIONES

El desarrollo de problemas de aplicación basados en situaciones reales son un en foque muy acertado a la hora de desarrollar habilidades y adquirir conocimiento en telecomunicación. Para este caso específico el aprendizaje e implementación de las redes lan/wan y sus diferentes tipos de desarrollo de una red. permiten tener un punto de vista más general. Lo que implica posibles soluciones más acertadas a los interrogantes presentados durante la implementación de una red.

En este caso la solución de los dos escenarios planteados a lo largo de este documento ha permitido desarrollar habilidades en la implementación de diferentes protocolos y configuraciones tales como; en la creación de vlan, interfaces, troncales, creación y configuracion de DHCP, aplicación de OSPF, NAT, NTP, ACL. Permitiendo tener gran varia de opciones y abriendo un mundo de posibles soluciones a futuros retos en la solución de implementación de redes.

Para dar solución al escenario 1 fue gran importancia la aplicación y configuracion trunking, el cual permitió conectar los dos switch de capa 3 y por medio de estos poder realizar la administración de las vlan, permitiendo dar una correcta solución a la red y la implementación del EtherChannel.

La solución del escenario 2 fue un éxito gracias a la correcta configuracion del protocolo OSPF, que al ser de código abierto permite la utilización de distintas marcas, teniendo variedad de dispositivos a utilizar. Este protocolo en sus distintas versiones permite la utilización e implementación del direccionamiento IP en su versión 4 y 6.

BIBLIOGRAFIA

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

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

CISCO. (2019). Routing Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#3

CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

UNAD (2017). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9

CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10

ANEXOS

ANEXO 1
Escenario 1 simulado en Packet tracer, Archivo.
https://drive.google.com/drive/folders/1FesLQq0dxMUrfoap9VRlxhjT9NCGp-4I?usp=sharing

ANEXO 2
Escenario 2 simulado en Packet tracer, Archivo
https://drive.google.com/drive/folders/1ngsCpuPWxk7iXgh-9NwY6eTOUkaBDTnk?usp=sharing

ANEXO 3
ARTICULO CIENTIFICO: IEEE.Jhoser_Quintana.
https://drive.google.com/drive/folders/1BTTcNbuHIdWQ2qsQDhLZ_JHVHbPtwHeS?usp=sharing

SOLUCIÓN DE DOS REDES PRESENTE EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

Jhoser Quintana Pulido
Universidad Abierta y A Distancia UNAD, jquinteropu@unadvirtual.edu.co

Resumen

En este escenario se realiza el análisis de una red planteada que tiene una influencia o aplicación en entornos corporativos, para lo cual se desarrolla bajo la tecnología de cisco. En la solución se implementa los conocimientos en soluciones a problemas networking en donde se pueden evidenciar, topologías de red, configuraciones, verificación de conectividad entre equipos, conmutación entre host o equipos y redes, realización de enrutamiento, trunkig, EtherChannel y creación de vlans, las cuales corresponde a una parte de la solución utilizada en dicha red.
Una parte de gran importancia en una red es la configuración de seguridad utilizada, este caso no es la excepción, pues se aplican restricciones de accesos, asignación, encriptación de contraseñas, mensajes de advertencias. Para cada paso realizado en este documento se comprueba, verifica que todo lo realizado cumpla y se desarrolle de la mejor forma posible.

Palabras clave: Conmutación, Enrutamiento, Redes.

Abstract:
In this scenario, the analysis of a proposed network that has an influence or application in corporate environments is carried out, for which it is developed under Cisco technology. In the solution, knowledge in solutions to networking problems is implemented where network topologies, configurations, verification of connectivity between equipment, switching between host or equipment and networks, conducting routing, trunkig, EtherChannel and creation of vlans can be demonstrated, which correspond to a part of the solution used in said network.
A very important part of a network is the security configuration used, this case is not the exception, as access restrictions, assignment, password encryption, warning messages are applied. For each step carried out in this document, it is verified, verifies that everything carried out complies and is developed in the best possible way.

Keywords: Switching, Routing, Networks.

I. INTRODUCCIÓN

Este documento presenta la solución al planteamiento de una topología de red en donde se evidencia la implementación de tecnología cisco. utilizando la metodología de solución de problemas reales, se desarrolla paso a paso por medio de elementos de apoyo como los softwares de simulación de redes, en este caso puntual y por el requerimiento de ser tecnología Cisco, se utiliza Packet tracer. Ya que este permite tener todo un ambiente de simulación de equipos. La topología anteriormente mencionada esta distribuida de la siguiente manera: cuenta con un router cisco 4321 el cual tiene uno de sus puertos conectado la interfase virtual loopback que nos permite simular una conexión a internet, dos switch cisco 3560 con una versión de IOS 12.2, se trabaja con esta referencia ya que se requiere direccionamiento ipv6, estos switch al ser capa 3 permite trabajar correctamente con IPv6, sin necesidad de activar la plantilla SDM, dos host o PC como dispositivos finales de red.
Teniendo los dispositivos simulados en Packet tracer de cisco, es necesario realizar las configuraciones iniciales como; Borrado de las configuraciones anteriores de la NVRAM, borrado de las vlan y guardar el nuevo estado de los equipos, para posteriormente realizar las configuraciones básicas como; asignación de nombre, desactivación de las búsquedas de DNS, Asignacion de nombre de dominio, asignación de las contraseñas de seguridad en los diferentes entornos como lo son el modo privilegiado exec, consola, y paralas líneas vty que nos permiten la comunicación por medio de telnet.
Se configuran las sub interfaces, se cran las vlan, se activa el direccionamiento ipv6 en los switch, se asigna direccionamiento ipv4 y 6 en los dispositivos con sus respectivas máscaras de red, se crean troncales 802.1Q, se crea y se aplica EtherChannel, DHCP.
En este entorno se desarrolla la topología proporcionada, se realiza las configuraciones básicas y especificas cada dispositivo y se verifican cada una de las pautas para dar solución de la forma más adecuada.

II. METODOLOGIA

El desarrollo del escenario 1, se basa en el método experimental, pues es utilizado para realizar los diferentes pasos del escenario. Donde controlando algunas variables se procede a observar un resultado. Para este escenario se aplican configuraciones en los dispositivos y estos en respuesta permiten la conexión entre ellos, como resultado se puede realizar el envió y recibo de información "Paquetes".
El meto experimental permite conocer a fondo los aspectos que involucra la topología de red que se está desarrollando, permitiendo validar o refutar las distintas creencias que existen en la configuración de las redes cisco, todo esto con hechos reales y de forma práctica.

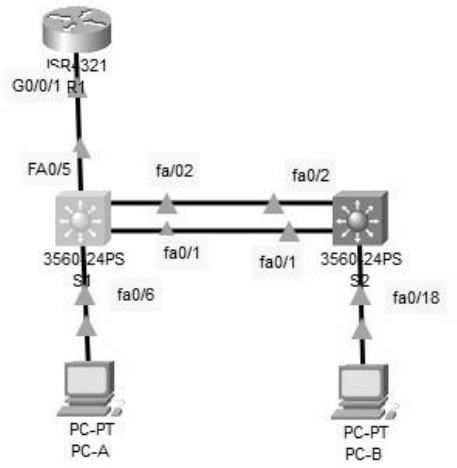
Dejando claro el método utilizado en el desarrollo del escenario, enunciamos que la Metodología utilizada para el planteamiento del escenario es la investigación de tipo aplicada. [1] La investigación aplicada es el tipo de investigación en la cual el problema está establecido y es conocido por el investigador, por lo que utiliza la investigación para dar respuesta a preguntas específicas.
Para este escenario se propone una topología de red de tipo LAN en la cual se expresa las necesidades como criterios para el desarrollo de la solución. La utilización de tecnología Cisco en la implementación de una respuesta para este escenario brinda una ventaja, pues una de las mas completas del mercado. Su constante evolución de sus sistemas operativos "IOS" permite encontrar solución a diferentes inconvenientes y estar la vanguardia de las actualizaciones de los diferentes protocolos de interconexión tales como el modelo OSI. [2] Es un estándar que tiene por objetivo conseguir interconectar sistemas de procedencia distinta para que estos pudieran intercambiar información sin ningún tipo de impedimentos debido a los protocolos con los que estos operaban de forma propia según su fabricante.

Los resultados generados en el desarrollo del escenario por medio de la implementación de la metodología anteriormente mencionada dan como resultado la solución final y comprensión de cada una de los pasos realizados, permitiendo encontrar una solución eficaz y acertada a la incógnita planteada.

III. RESULTADOS

Se basa en la topología de red diseñada e implementada para dar solución o respuesta al interrogante, donde se realiza la implementación de la red en el software de simulación de redes Packet tracer, se configurar de los diferentes disposivos que se indican a lo largo de dicha topología, permitiendo evaluar las respuestas a las configuraciones realizadas.

Figura 1. Topología



En el desarrollo practico de la actividad y para realizar las configuraciones a cada dispositivo se utilizan algunos datos que permiten realizar el direccionamiento tanto en IPV4 como en IPV6.

Tabla 1. Direccionamiento IP

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

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
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

Teniendo los datos requeridos para el direccionamiento IP se procede a obtener los datos que nos permite la creación de las redes virtuales LAN o más conocidas como Vlan.

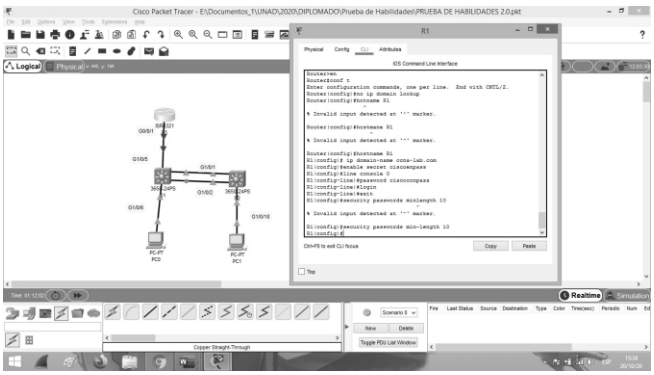
Tabla 2. VLAN

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

Teniendo en cuenta la tabla anterior se procedió a realizar la creación y asignación de nombre de las vlan las cuales al ser redes lógicas permiten funcionar dentro de una red física sin inconvenientes.

Continuando la realización de los resultados se procede a realizar el borrado del router, switch y cada dispositivo Cisco en la distribución de la red, para luego realizar las configuraciones iniciales de tal manera que no se presenten inconvenientes en la red por generalidades mal manejadas.

Figura 2. Borrado y reinicio de equipos.



Fuente: Autor.

Se realizan la configuración inicial esto incluye, asignación de nombre, desactivación de la búsqueda de Dns, configuración de la seguridad para los entornos privilegiados, consola y las líneas vty, se configura la entra ssh o secury Shell, se encriptan las contraseñas y creación de un mensaje de advertencia para cada dispositivo.

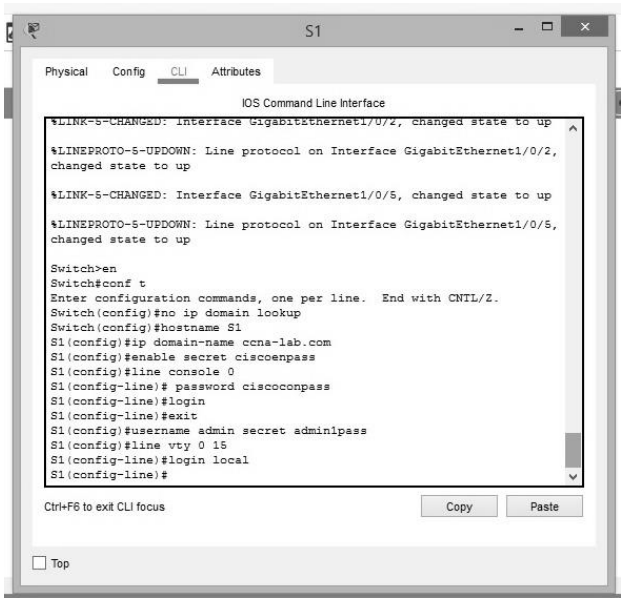
También se configura la interfaz de administración a la cual se le agrega el direccionamiento IPv4-6, la link-local, el gateway predeterminado y se activa la interfaz. A pesar se realizar la activación la interfaz en queda activa hasta que se creen las vlan. Esto se realiza en cada switch de la red.

Tabla 3. Configuracion R1.

Código	Descripción
Router>en	ingreso modo exec
Router#conf t Enter configuration commands, one per line. End with CNTL/Z.	ingreso al modo de configuración
Router(config)#no ip domain lookup	se desactiva la búsqueda de DNS
Router(config)#hostname R1	Asignacion de nombre al router
R1(config)# ip domain-name ccna-lab.com	Asignacion de nombre de dominio
R1(config)#enable secret ciscoenpass	contraseña privilegiada exec
R1(config)#line console 0	línea de ingreso al modo consola
R1(config-line)#password ciscoconpass	Asignacion de contraseña de consola
R1(config-line)# login	permite establecer la contraseña

R1(config)#security passwords min-length 10	limitación de caracteres mínimos de contraseñas
R1(config)#username admin secret admin1pass	creación de usuario en base local
R1(config)# line vty 0	establecer login en base de datos local
R1(config-line)# login local	permite establecer la contraseña
R1(config-line)#transport input ssh	configuración de entrada ssh
R1(config)#service password-encryption	encriptación de contraseñas
R1(config)# banner motd #ACCESO ESTA PROHIBIDO#	configuración de mensaje
R1(config)#IPV6 unicast-routing	activación de IPV6
R1(config)# int g0/0/1.2	ingreso a la subinterfaz
R1(config-subif)#encapsulation dot1q 2	encapsulación de la vlan 2
R1(config-subif)#description Bikes	descripción
R1(config-subif)#ip address 10.19.8.1 255.255.255.192	asignación de ipv4
R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64	asignación de ipv6
R1(config-subif)#ipv6 address fe80::1 link-local	asignación de la link-local
R1(config-subif)#	
R1(config-subif)# int g0/0/1.3	ingreso a la subinterfaz
R1(config-subif)#encapsulation dot1q 3	encapsulación de la vlan 3
R1(config-subif)#description Trikes	descripción
R1(config-subif)#ip address 10.19.8.65 255.255.255.224	asignación de ipv4
R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64	asignación de ipv6
R1(config-subif)#ipv6 address fe80::1 link-local	asignación de la link-local
R1(config-subif)#	
R1(config-subif)# int g0/0/1.4	ingreso a la subinterfaz

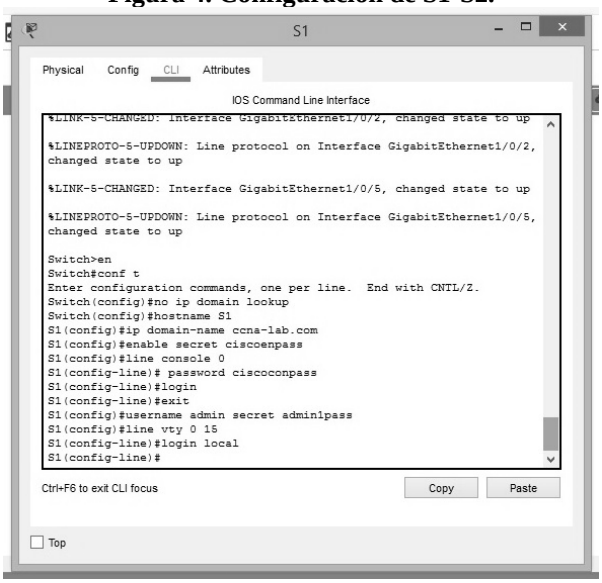
Figura 3. Comprobación de configuracion de R1



Fuente: Autor.

En la figura anterior podemos observar la comprobación de los comandos que se describen en la tabla 3. Llevando el paso a paso descrito para tener una correcta configuracion del router.

Figura 4. Configuracion de S1-S2.



Fuente: Autor.

Podemos observar la ejecución de los comandos que nos permiten la configuracion del switch S1-S2. Donde inicialmente se realiza la asignación de nombre, desactivación de la búsqueda de DNS, configuracion de seguridad, encriptación de contraseñas, se crea el usuario para la configuracion de base de datos local y se asigno un banner motd o un mensaje de advertencia. También se realiza la configuracion de la vlan 4 en los dos switches, con los direccionamientos Ipv4 y Ipv6. Y la respectiva

asignación de la puerta de enlace predeterminada o Gateway.

Tabla 4. Configuracion de S1-S2.

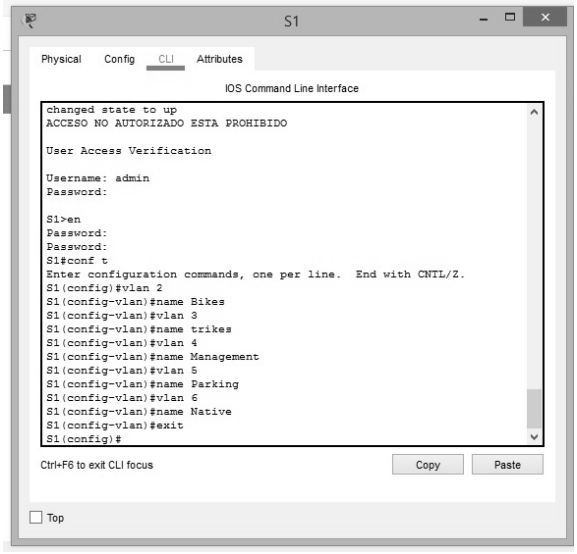
Código	Descripción
Switch>en	ingreso modo exec
Switch #conf t Enter configuration commands, one per line. End with CNTL/Z.	ingreso al modo de configuración
Switch (config)#no ip domain lookup	se desactiva la búsqueda de DNS
Switch(config)#hostname S1	Asignacion de nombre al router
S1(config)# ip domain-name ccna-lab.com	Asignacion de nombre de dominio
S1(config)#enable secret ciscoenpass	contraseña privilegiada exec
S1(config)#line console 0	línea de ingreso al modo consola
S1(config-line)#password ciscoconpass	Asignacion de contraseña de consola
S1(config-line)# login	permite establecer la contraseña
S1(config)#username admin secret admin1pass	creación de usuario en base local
S1(config)# line vty 0	establecer login en base de datos local
S1(config-line)# login local	permite establecer la contraseña
S1(config-line)#transport input ssh	configuración de entrada ssh
S1(config)#service password-encryption	encriptación de contraseñas
S1(config)# banner motd #ACCESO NO AUTORIZADO ES PROHIBIDO#	configuración de mensaje.

En la siguiente tabla podemos observar la configuracion de la vlan 4, los comandos utilizados son perfectamente aplicables tanto a S1 como a S2.

Tabla 5. Configuracion de vlan 4.

Código	Descripción
S1(config)#int vlan 4 *Mar 1 1:53:35.226: %SSH-5-ENABLED: SSH 1.99 has been enabled	Ingresamos a la Interfaz de vlan 4
S1(config-if)#ip address 10.19.8.98 255.255.255.248	Asignacion IPv4
S1(config-if)#ipv6 address 2001:db8:acad:c::98/64	Asignacion IPv6
S1(config-if)#ipv6 address fe80::98 link-local	Asignacion link-local
S1(config-if)#no shutdown	activamos la vlan 4
S1(config-if)# exit	salimos
S1(config)#ip default-gateway 10.19.8.97	configuramos la Puerta de enlace

Figura 5. Creación de las Vlan.



Fuente: Autor.

La creación de troncales 802.1Q en dispositivos Cisco es un método muy utilizado ya que estos enlaces punto a punto permiten una extensión de las vlan atreves de toda la red. En este caso se crea la troncal y se pasan las interfases a modo troncal, y se asignan a la vlan nativa. Estas configuraciones se realizan sobre los switch distribuidos en la red.

Se configura EtherChannel; el cual lo que permite agrupar de forma lógica dos o más enlaces que existen de forma física, estos enlaces son tratados como uno solo. Estos se realizan con el fin de sumar velocidad a los puertos involucrados y tener un enlace de alta velocidad. En este caso los dispositivos

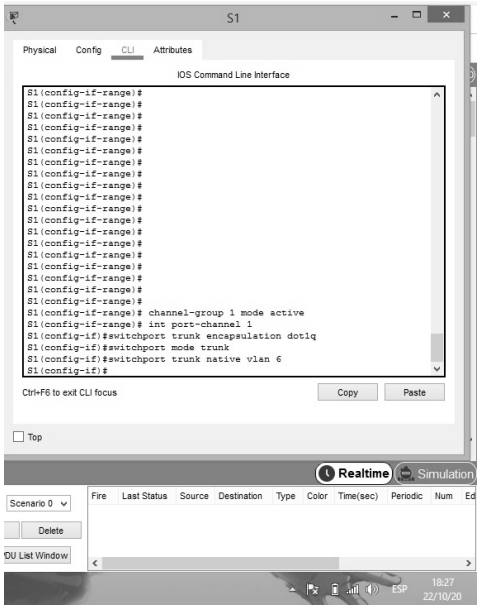
involucrados y que se les aplica dicha configuración son los switch previamente nombrados como S1 y S2.

Se procede a realizar la creación de las distintas vlan como se observa en la figura 4 y se le asigna un nombre a cada una de ellas, esto aplica en los switch S1-S2.

Tabla 6. Creación de Vlan en S1-S2.

Código	Descripción
S1#conf t Enter configuration commands, one per line. End with CNTL/Z.	Ingreso al modo de configuración global
S1(config)#vlan 2	Se ingresa a la vlan
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	Se le asigna nombre a la vlan
S1(config-vlan)#exit	Salir

Figura 6. Configuración de EtherChannel



Fuente: Autor.

Se realiza configuración de los puertos de acceso para cada host. Donde se indica cada puerto por donde se conectará el host al switch, y se habilita la seguridad de los puertos, la cual permite limitar el numero de direcciones MAC a conectar.

También se realiza protección de puertos o interfaces no utilizados en donde se asignan a una vlan especifica y se procede a apagar cada uno de los puertos, dejando configurado un mensaje de advertencia, se proecede a asignar a un vlan en este caso especifico es a la vlan 6.

Tabla 7. Configuracion de EthetChannel.

Código	Descripción
S1(config-if-range)#channel-group 1 mode active	Si agregran las interfaces al grupo de canales de LACP 1
S1(config-if-range)#int port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q	asignamos el canal 1
S1(config-if)#switchport mode trunk	se llama el modo troncal
S1(config-if)#switchport trunk native vlan 6	se asigna a la vlan 6

Figura 7. Puerto de acceso

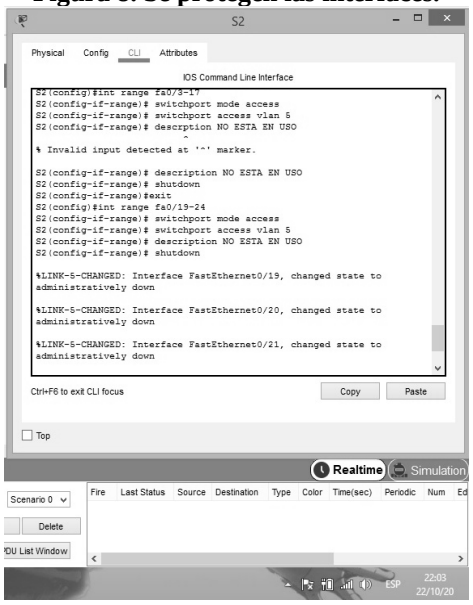
Fuente: Autor.

Se procede configurar los puertos de acceso, como primera medida se ingresa al puerto o interfaz fa0/6 en el caso del switch S1, se establece como un puerto de acceso, se procede a agragar una vlan especifica en este caso a la vlan 2, se habilita la seguridad de puerto y se establece un maximo de 3 direcciones MAC.

Tabla 8. Configuracion de puerto de acceso.

Código	Descripción
S1(config)# int fa0/6	ingreso a la interfaz
S1(config-if)#switchport mode access	configuración como Puerto de acceso
S1(config-if)#switchport access vlan 2	Se agrega a la vlan
S1(config-if)#switchport port-security	Se habilita la seguridad del puerto
S1(config-if)#switchport port-security maximum 3	Se establece maximo de MAC

Figura 8. Se protegen las interfaces.



Fuente: Autor.

Se procede a realizar protección de las interfaces no utilizadas en los switch S1-S2. De la siguiente manera se establece el rango de interfaces a trabajar siempre dejando excluida las interfaces en uso, Se estableen como puerto de acceso, se asignan a una vlan en este caso se utilizó la vlan 5, se asigna una descripción y se procede a realizar el apagado de las interfaces.

Tabla 9. Configuracion interfaces no utilizadas.

Código	Descripción
S1(config-if)# int range fa0/3-4	Se establece el rango de interfaces a trabajar
S1(config-if-range)#switchport mode acces	Configuración como Puerto de acceso
S1(config-if-range)#switchport access vlan 5	Se asigna a la vlan
S1(config-if-range)#description NO ESTA EN USO	Se introduce descripción
S1(config-if-range)#shutdown	Se apaga las interfaces
S1(config-if-range)# int range fa0/7-24	Se establece el rango de interfaces a trabajar
S1(config-if-range)#switchport mode access	Configuración como Puerto de acceso
S1(config-if-range)#switchport access vlan 5	Se asigna a la vlan
S1(config-if-range)#description NO ESTA EN USO	Se introduce descripción
S1(config-if-range)#shutdown	Se apaga la interfaces
S1(config-if-range)# int range G0/1-2	Se establece el rango de interfaces a trabajar
S1(config-if-range)#switchport mode access	Configuración como Puerto de acceso
S1(config-if-range)#switchport access vlan 5	Se asigna a la vlan
S1(config-if-range)#description NO ESTA EN USO	Se introduce descripción
S1(config-if-range)#shutdown	se apaga la interfaces

Figura 9. DHCP

Fuente: Autor.

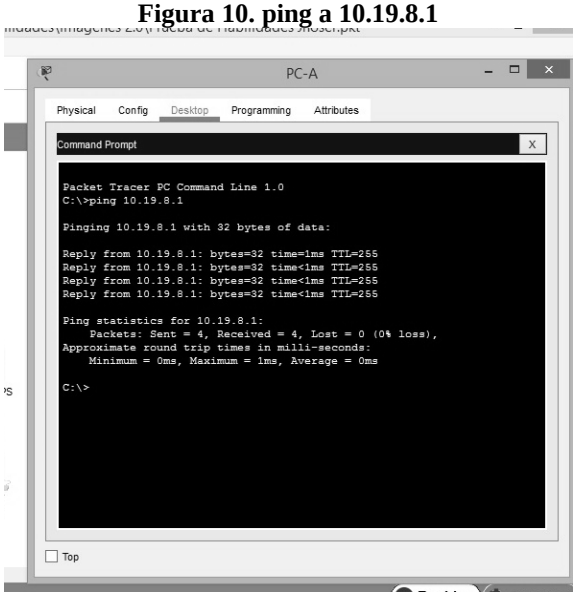
Para la configuracion de DHCP en cada uno de los switch se procede a realizar la creación de un grupo de canales LACP 1, se asigna al canal 1, se procede a llamar el modo troncal, y por ultimo se asigna a una vlan en este caso es a la vlan 6.

Tabla 10. Configuracion de DHCP

Código	Descripción
S2(config-if-range)#channel-group 1 mode active	si agregran las interfaces al grupo de canales de LACP 1
S2(config-if-range)#int port-channel 1	asignamos el canal 1
S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk	se llama el modo troncal
S2(config-if)#switchport trunk native vlan 6	se asigna a la vlan 6

Para la verificación de cada una de las configuraciones realizadas en los diferentes dispositivos Cisco, se realiza un Ping (Es una utilidad de diagnóstico; [2]Mediante esta utilidad puede diagnosticarse el estado, velocidad y calidad de una red determinada).

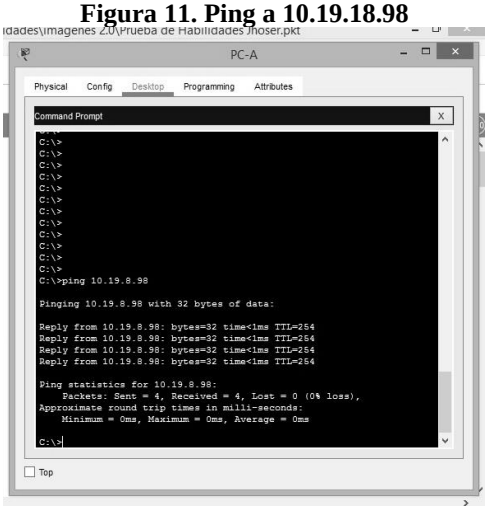
Figura 10. ping a 10.19.8.1



Fuente: Autor.
Se realiza Ping desde la PC-A a 10.19.8.1

Fuente: Autor.
Se realiza Ping desde la PC-A a 10.19.8.65

Figura 11. Ping a 10.19.18.98

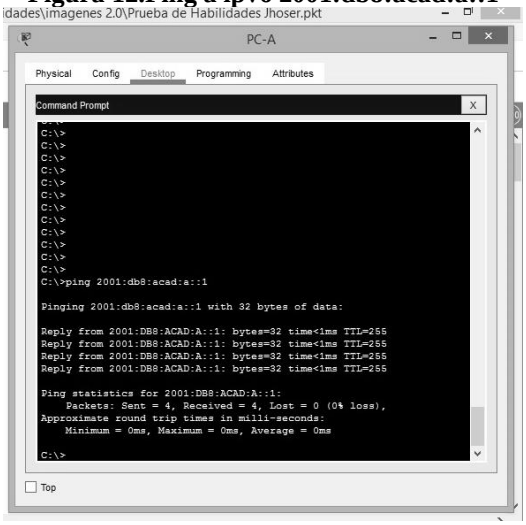


Fuente: Autor.
Se realiza Ping desde la PC-A a 10.19.8.98

Los Ping anteriores son la comprobación del resultado de las configuraciones realizadas a los dispositivos Cisco. Se ejecutan desde la PC-A que se observa en la topología de red. Los cuales tienen un resultado 100% satisfactorio.

Se procede a realizar ping desde la PC-A pero con el direccionamiento IPv6, para verificar su correcto funcionamiento.

Figura 12.Ping a ipv6 2001:db8:acad:a::1



Fuente: Autor.
Se realiza Ping desde la PC-A en IPv6 a 2001:db8:acad:a::1

De los anteriores pines Podemos definir que el funcionamiento de los direccionamientos IPv4 – IPv6 están funcionando de forma correcta y todos los pines fueron satisfactorios.
También se puede decir que el desarrollo y la configuracion de los equipos se realizo de manera adecuada, implementando de manera correcta los protocolos de DHCP,vlan, trunking, configuracion de interfaces, asignación de puertos, encriptación

de claves, seguridad en los puertos, restricción de accesos, configuracion de descripciones, configuracion de avisos de advertencias, entre otras configuraciones no tan relevantes pero si importantes en el desarrollo del escenario trabajo.

IV. Referencias

Las referencias son muy importantes, y se debe seguir el siguiente formato. El tamaño de letra es de 10 puntos:

[1] Rodríguez, D. (s. f.). Investigación aplicada: características, definición, ejemplos. Lifeder.com. Recuperado el 17 de noviembre del 2020. https://www.lifeder.com/investigacion-aplicada/

[2] Kozierok, Charles M. (9 de noviembre de 2004). TCP/IP Communication Verification Utility ping/ping6. The TCP/IP Guide. Recuperado el 19 de noviembre del 2020, de https://web.archive.org/web/20041109161927/http://www.tcpipguide.com/free/t_TCPIPCommunicationVerificationUtilitypingping6-2.htm

[3] Cisco (s. f). Configuring EtherChannel and 802.1Q Trunking Between Catalyst L2 Fixed Configuration Switches and a Router (InterVLAN Routing). Cisco.com. Recuperado el 21de noviembre del 2020. de: https://www.cisco.com/c/en/us/support/docs/switches/catalyst-2950-series-switches/24042-158.html

[4] Cisco (s. f). VLANs and Trunking. Cisco.com. Recuperado el 21de noviembre del 2020. de: https://www.ciscopress.com/articles/article.asp?p=29803&seqNum=3

[5] Tommaso, L.(15 de julio de 2009). configuración básica de un router. Mikroways.net. Recuperado el 15 de noviembre del 2020. de: https://www.mikroways.net/2009/07/15/configuracion-basica-de-un-router/

[6] ¿Qué es y para qué sirve el protocolo SSH?.(s. f). Linube.com. Recuperado el 23 de noviembre del 2020. de: https://linube.com/blog/que-es-protocolo-ssh/

[7] Bitacora Byte. (18 de Julio del 2017). Configurar DHCP en router CISCO. BitacoraByte.wordpress.com. Recuperado el 23 de noviembre del 2020. de: https://bitacorabyte.wordpress.com/2017/07/18/configurar-dhcp-en-router-cisco/

[8] Cisco (10 de Agosto de 2016). IP Addressing and Subnetting for New Users. Cisco.com. Recuperado el 24 de noviembre del 2020. de: https://www.cisco.com/c/es_mx/support/docs/ip/routing-information-protocol-rip/13788-3.html

[9] Tommaso, L.(26 de noviembre de 2009). seguridad de puerto en switches cisco. Mikroways.net. Recuperado el 15 de noviembre del 2020. de: https://www.mikroways.net/2009/07/15/configuracion-basica-de-un-router/

[10] Eclassvirtual. (s. f).el modelo osi para el ccna.eClassVirtual.com. Recuperado el 24 de noviembre del 2020. de: https://eclassvirtual.com/el-modelo-osi-para-el-ccna/

[11] Configurar SVI (29 septiembre de 2018). Recuperado el 24 de noviembre del 2020. de: https://todopacketracer.com/2017/10/13/configurar-svi/

[12] Gerometta, O.(12 de noviembre de 2020). Puertos e interfaces en un switch multilayer. librosnetworking.blogspot.com.). Recuperado el 24 de noviembre del 2020. de:

[13] Networklessons.(s. f). Trunking on Cisco IOS Switch. networklessons.com. Recuperado el 25 de noviembre del 2020. de: https://networklessons.com/switching/how-to-configure-trunk-on-cisco-catalyst-switch

[14] CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

[15] Todo lo que debes saber de Cisco Packet Tracer. (18 de febrero, 2020).ambit-bst.com. Recuperado el 23 de noviembre del 2020. de: https://www.ambit-bst.com/blog/todo-lo-que-debes-saber-de-cisco-packet-tracer#

Biografía

Jhoser Quintana Pulido. nació en Florencia (Caqueta), el 17 de enero de 1993. Se graduó del Colegio Jose Hilario Lopez, en Campoalegre, estudio en el Sena Industrial y Universidad Nacional abierta y a distancia Unad.
Su experiencia profesional incluye la Union temporal Merani-bt, la empresa Incer.sa.s, empresa Bethell.net. Sus áreas de interés incluyen, la electrónica de potencia y las telecomunicaciones.