

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

ANYENSON JEFFERSON MACIAS BERMUDEZ

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

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

ANYENSON JEFFERSON MACIAS BERMUDEZ

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

DIRECTOR:
DIEGO EDINSON RAMIREZ CLAROS

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

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma de Jurado

Firma de Jurado

Ibagué, 27 de Noviembre de 2020

AGRADECIMIENTOS

Agradezco primeramente a Dios por haberme guiado en este proceso y a su vez darme la sabiduría para afrontar los retos que a lo largo de este proceso de formación tuve.

A mis padres, esposa e hijos, por siempre estar a mi lado brindándome sus consejos, apoyo y confianza para escalar un peldaño mas y lograr una meta mas en mi vida.

A mis profesores que con mucha paciencia siempre estuvieron prestos para ayudarme en mi formación profesional, con un consejo acertado y oportuno los cuales contribuyeron en gran manera para lograr mis objetivos y culminar mi carrera universitaria

CONTENIDO

AGRADECIMIENTOS.....	4
CONTENIDO	5
LISTA DE TABLAS	6
LISTA DE FIGURAS	7
GLOSARIO	9
RESUMEN.....	11
ABSTRACT.....	11
INTRODUCCIÓN	12
DESARROLLO	13
1. ESCENARIO 1	13
2. ESCENARIO 2	40
CONCLUSIONES	83
BIBLIOGRAFIA.....	84
ANEXOS.....	85
ANEXO 1.....	85
ANEXO 2.....	85

LISTA DE TABLAS

Tabla 1. Tabla de VLAN.....	14
Tabla 2. Tabla de asignación de direccionamiento	15
Tabla 3. Configuración inicial	16
Tabla 4. Proceso de Configuración R1	17
Tabla 5. Proceso de Configuración S1	20
Tabla 6. Proceso de Configuración S2	22
Tabla 7. Proceso de Configuración y Creación de Vlan S1	24
Tabla 8. Proceso de Configuración y Creación de Vlan S2	27
Tabla 9. Creación de rutas y DHCP para Vlan 2 y 3.....	30
Tabla 10. Proceso Configuración y Creación de rutas y DHCP para Vlan 2 y 3....	31
Tabla 11. Configuración de red equipo PC-A	33
Tabla 12. Configuración de red equipo PC-B	33
Tabla 13. Direccionamiento para verificar conectividad de extremo a extremo	34
Tabla 14. Pasos Configuración inicial Escenario 2	41
Tabla 15. Configuración computadora de Internet.....	41
Tabla 16. Proceso de Configuración R1	43
Tabla 17. Proceso de Configuración R2	45
Tabla 18. Proceso de Configuración R3	47
Tabla 19. Proceso de Configuración S1	49
Tabla 20. Proceso de Configuración S3	50
Tabla 21. Proceso de Configuración S1	53
Tabla 22. Proceso de Configuración S3	55
Tabla 23. Proceso de Configuración R1	57
Tabla 24. Verificación de conectividad.....	59
Tabla 25. Proceso de Configuración OSPFv2 R1	62
Tabla 26. Proceso de Configuración OSPFv2 R2.....	64
Tabla 27. Proceso de Configuración OSPFv2 R3.....	65
Tabla 28. Proceso de Configuración OSPFv3 R3.....	66
Tabla 29. Comandos para verificar OSPF	67
Tabla 30. Proceso de configuración R1 como servidor de DHCP.....	69
Tabla 31. Proceso de configuración R2 con NAT estática y dinámica.....	71
Tabla 32. Verificación de protocolo DHCP y NAT estática	73
Tabla 33. Configuración NTP en R1 y R2.....	76
Tabla 34. Proceso de configuración NTP en R1 y R2.....	76
Tabla 35. Proceso de configuración acceso líneas VTY en R2	77
Tabla 36. Comandos CLI	78

LISTA DE FIGURAS

Figura 1. Escenario 1	13
Figura 2. simulación de escenario 1	14
Figura 3. Proceso de Configuración R1	17
Figura 4. Proceso de Configuración S1	20
Figura 5. Proceso de Configuración S2	22
Figura 6. Proceso de Configuración y Creación de Vlan S1	24
Figura 7. Proceso de Configuración y Creación de Vlan S2	27
Figura 8. Proceso Configuración y Creación de rutas y DHCP para Vlan 2 y 3	31
Figura 9. Ping de PC-A a R1, G0/0/1.2 Ipv4 e Ipv6	35
Figura 10. Ping de PC-A a R1, G0/0/1.3 Ipv4 e Ipv6	36
Figura 11. Ping de PC-A a R1, G0/0/1.4 Ipv4 e Ipv6	36
Figura 12. Ping de PC-A a PC-B Ipv4 e Ipv6	37
Figura 13. Ping de PC-A a R1 Loopback 0, Ipv4 e Ipv6	37
Figura 14. Ping de PC-B a R1 Loopback 0, Ipv4 e Ipv6	38
Figura 15. Ping de PC-B a R1, G0/0/1.2 Ipv4 e Ipv6	38
Figura 16. Ping de PC-B a R1, G0/0/1.3 Ipv4 e Ipv6	39
Figura 17. Ping de PC-B a R1, G0/0/1.4 Ipv4 e Ipv6	39
Figura 18. Escenario 2	40
Figura 19. Configuración computadora de Internet	42
Figura 20. Proceso de Configuración R1	43
Figura 21. Proceso de Configuración R2	45
Figura 22. Proceso de Configuración R3	47
Figura 23. Ping de R1 a R2	51
Figura 24. Ping de R2 a R3	52
Figura 25. Ping de PC de internet a gateway	52
Figura 26. Proceso de Configuración S1	53
Figura 27. Proceso de Configuración S3	55
Figura 28. Proceso de Configuración R1	57
Figura 29. Ping S1 a VLAN 99 en R1	59
Figura 30. Ping S3 a VLAN 99 en R1	60
Figura 31. Ping S1 a VLAN 21 en R1	60
Figura 32. Ping S3 a VLAN 23 en R1	61
Figura 33. Proceso de Configuración OSPFv2 OSPFv3 R1	62
Figura 34. Proceso de Configuración OSPFv2 OSPFv3 R2	64
Figura 35. Proceso de Configuración OSPFv2 OSPFv3 R3	65
Figura 36. Comando show Ip protocols	67
Figura 37. Comando show ip route ospf	68

Figura 38. Comando show run	68
Figura 39. Proceso de configuración R1 como servidor de DHCP	69
Figura 40. Proceso de configuración R2 con NAT estática y dinámica	71
Figura 41. Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	74
Figura 42. Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	74
Figura 43. Verificar que la PC-A pueda hacer ping a la PC-C	75
Figura 44. Servicio web desde computadora de internet	75
Figura 45. Acceso telnet a R2 desde R1	77
Figura 46. Acceso telnet desde R3 a R2	78
Figura 47. Comando Show access-list 1	79
Figura 48. Comando clear ip access-list counters	80
Figura 49. Comando show ip interface	80
Figura 50. ping PC-A y PC-C para traducción NAT	81
Figura 51. Comando Show ip nat translations	81
Figura 52. Comando clear ip nat translation *	82

GLOSARIO

- **DHCP:** Es un protocolo de red que es utilizado en redes IP que mediante un servidor automáticamente asigna las direcciones IP a los diferentes equipos de la red para que logren comunicarse eficientemente con otros equipos, y su significado es protocolo dinámico de configuración de host (DHCP).
- **Enrutamiento:** Es conocido por el nombre de enrutamiento el proceso que posibilita que los paquetes enviados de un equipo origen lleguen al equipo destino de forma correcta, cuando un equipo envía datos a otro, lo primero que hace es verificar si la Ip de este se encuentre en su tabla ARP, en caso de no ser así este enviara una petición que responderá el equipo destino con su dirección física, de esta forma completara los datos para transmitir las tramas, a esto se le llama routing directo.
- **EXEC:** Es el modo de privilegio para acceder a todos los comandos de un router, este modo se puede configurar para que al ingresar el comando enable solicite una autenticación de usuario mediante una contraseña, esto con el único fin de generar una mayor protección y poder garantizar que solo personal autorizado pueda ingresar y manipular la configuración del router.
- **Ping:** Se considera una herramienta o un comando que diagnostica y nos permite verificar el estado de una conexión determinada de un equipo local con por lo menos un equipo remoto visto en una red de tipo TCP/IP.
- **VLAN:** acrónimo derivado de virtual LAN (red de área local virtual), método que se utiliza para crear una red lógica que sea independiente dentro de la red física, de esta forma se puede afirmar que una VLAN describe una red de área local.
- **OSPF:** es un protocolo de enrutamiento de fuente abierta (open source), es por eso que puede ser utilizado por equipos de diferentes marcas a cisco, este protocolo se puede configurar para ipv4 con su versión ospfv2 y para ipv6 con su versión ospfv3.

- **NAT**: siglas en inglés Network Address Translator y en español traductor de direcciones de red, como su nombre lo indica es la encargada de traducir las direcciones para que se pueda establecer las conexiones.
- **http** siglas que se traducen del inglés (HyperText Transfer Protocol) o en español (Protocolo de Transferencia de Hiper Textos). se puede decir que es el código que establece entre el computador que contiene la información y el computador solicitante para que se puedan comunicar en un mismo idioma al transmitir la información de la red.

RESUMEN

Este documento contiene los escenarios desarrollados con un paso a paso de como fue el proceso, donde se explica detalladamente las acciones tomadas para lograr dar una solución viable y efectiva, aplicando los conocimientos en redes y enrutamiento que nos permitieron dar conectividad a los escenarios propuestos, configurando con éxito los Router y los Switch de estas redes.

Podemos evidenciar que en los escenarios se logra establecer una conmutación efectiva entre los diferentes equipos configurados, logrando satisfacer los requerimientos solicitados para su desarrollo.

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

ABSTRACT

This document contains the scenarios developed with a step by step of how the process was, where the actions taken to achieve a viable and effective solution are explained in detail, applying the knowledge in networks and routing that allowed us to give connectivity to the proposed scenarios. successfully configuring the routers and switches of these networks.

We can show that in the scenarios it is possible to establish an effective commutation between the different configured equipment, managing to satisfy the requirements requested for its development.

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

INTRODUCCIÓN

Con el desarrollo de estos dos escenarios logramos afianzar los conocimientos en el área de redes y sus diferentes funciones, los cuales nos dan las habilidades para dar una solución efectiva, haciendo uso de simulaciones por medio de la herramienta CISCO Packet Tracer, que se asemejan a los equipos reales con los cuales nos podemos encontrar en nuestro ámbito laboral.

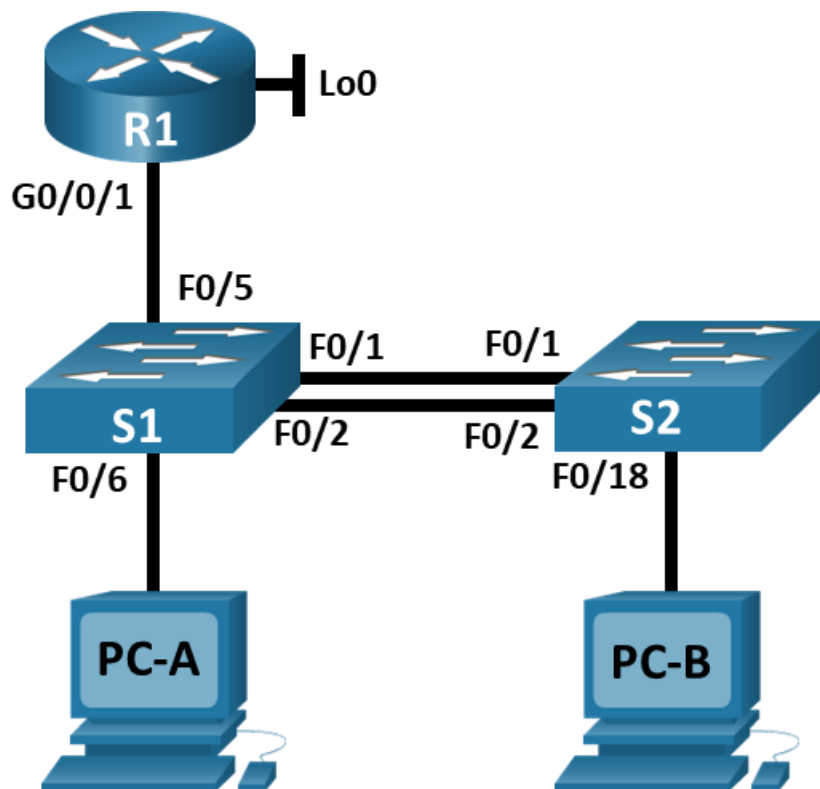
El diplomado tiene como objetivo principal, que desarrollemos nuestras habilidades en el área de las redes y telecomunicaciones, lo cual se logra por medio de la practica realizada en el desarrollo de los 2 escenarios, dándonos con esto la oportunidad de convertirnos en profesionales altamente competitivos, ya que el diplomado cuenta con un esquema de aprendizaje teórico practico, que nos ayuda a cimentar un pensamiento crítico y desarrollar habilidades que pondremos en práctica como futuros ingenieros.

Con el desarrollo de los escenarios propuestos, se logra conocer parte de los diferentes comandos que se utilizan en equipos reales para efectos de configuración, pero que en el simulador de packet tracer no funcionan de la manera adecuada ya que el servicio que nos presta el programa no soporta dichas funciones, enriqueciendo de esta forma nuestros conocimientos tanto en el manejo de equipos reales como de simulación.

DESARROLLO

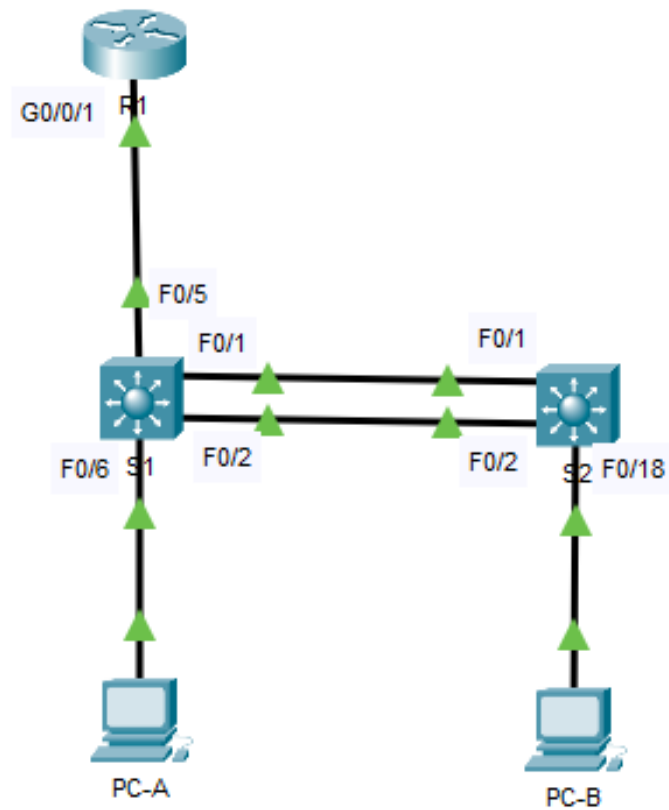
1. ESCENARIO 1

Figura 1. Escenario 1



En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch también deben administrarse de forma segura. Configuraré el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Figura 2. simulación de escenario 1



Fuente: Autor

Tabla 1. Tabla de VLAN

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

Tabla 2. Tabla de asignación de direccionamiento

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 2001:db8:acad:a: :50 /64	DHCP para puerta de enlace predeterminada IPv4 fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

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

Instrucciones

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

Paso 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.

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

En esta parte se realiza la configuración básica de los switch y el router que consiste en borrar la configuración que viene por defecto en los equipos con la finalidad de realizar una configuración de cero.

Tabla 3. Configuración inicial

Router>enable Router#erase startup-config Router#reload	ingreso a modo privilegiado eliminar configuración de inicio recargar el equipo
Switch>enable Switch#erase startup-config Switch#delete vlan.dat Switch#reload	ingreso a modo privilegiado eliminar configuración de inicio eliminar el archivo vlan recargar el equipo
Switch>enable Switch#config t Switch(config)#sdm prefer dual- ipv4-and-ipv6 default Switch(config)#exit Switch#reload	ingreso a modo privilegiado ingreso a modo de configuración configuración para que nuestro switch admita ipv4 e ipv6 salir recargar el equipo para que funcione la configuración sdm

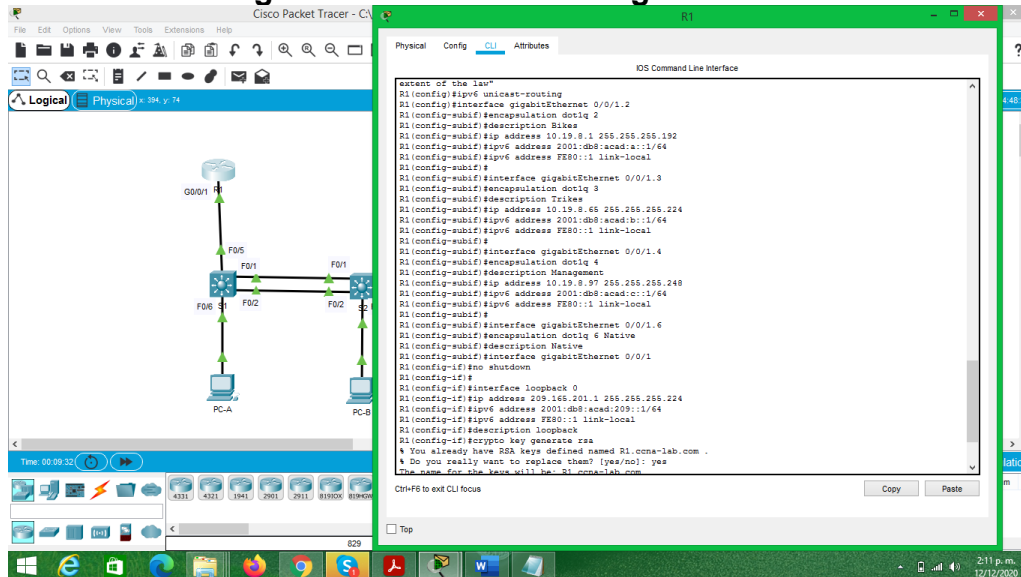
Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

En este paso se realiza la configuración del R1, donde iniciamos desactivando el servicio de DNS, luego realizamos la configuración de su nombre y la seguridad para ingreso a consola y modo de configuración, donde se le pone una longitud mínima de 10 caracteres para las contraseñas, y luego se cifran para garantizar la seguridad, además se crea un usuario para la administración de la base de datos local, también se configuro un banner con un mensaje de restricción.

De igual forma se establecieron las subinterfaces y sus direcciones tanto para Ipv4 como para Ipv6, así mismo se configuro la interface para loopback 0.

Figura 3. Proceso de Configuración R1



Fuente: Autor

En esta imagen podemos evidenciar el desarrollo de la configuración más importante de R1, donde se establecen las subinterfaces y sus direcciones IP, el cual se explica más detalladamente en la siguiente tabla

Tabla 4. Proceso de Configuración R1

Router>enable	ingreso a modo privilegiado
Router#config t	ingreso a modo de configuración
Router(config)#no ip domain lookup	Desactivar la búsqueda DNS
Router(config)#hostname R1	asignar el nombre al router
R1(config)#ip domain-name ccna-lab.com	asignar nombre de dominio

R1(config)#enable secret ciscoenpass	asignar contraseña cifrada para modo privilegiado
R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit	ingreso al modo de configuración de línea de consola asignar contraseña acceso consola activa la autenticación inicio sesión salir
R1(config)#security password min-length 10	Instaurar los caracteres mínimos que debe tener las contraseñas
R1(config)#username admin secret admin1pass R1(config)#line vty 0 15 R1(config-line)#login local	asignar un nombre de usuario y contraseña para para el ingreso a la base de datos local ingreso a configuración de telnet activar la autenticación de inicio a la base de datos local
R1(config-line)#transport input ssh R1(config-line)#exit	configura solo acceso remoto salir
R1(config)#service password-encryption	cifrado para las contraseñas
R1(config)#banner motd "Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law"	configura un mensaje de inicio de sesión
R1(config)#ipv6 unicast-routing	activa interface ipv6 en el router
R1(config)#interface gigabitEthernet 0/0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description Bikes R1(config-subif)#ip address 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 address FE80::1 link-local R1(config-subif)#exit R1(config)#interface gigabitEthernet 0/0/1.3 R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#description Trikes	configura subinterface encapsula tráfico de la subinterface descripción o nombre de la vlan 2 asigna dirección ipv4 a subinterface de la vlan 2 asigna dirección ipv6 a subinterfaz de la vlan 2 asigna dirección local ipv6 a subinterfaz de la vlan 2 salir configura subinterface encapsula tráfico de la subinterface descripción o nombre de la vlan

<pre> R1(config-subif)#ip address 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address FE80::1 link-local R1(config-subif)#exit R1(config)#interface gigabitEthernet 0/0/1.4 R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#description Management R1(config-subif)#ip address 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 address FE80::1 link-local R1(config-subif)#exit R1(config)#interface gigabitEthernet 0/0/1.6 R1(config-subif)#encapsulation dot1q 6 Native R1(config-subif)#description Native R1(config-subif)#interface gigabitEthernet 0/0/1 R1(config-if)#no shutdown </pre>	<p>asigna dirección ipv4 a subinterface de la vlan 3</p> <p>asigna dirección ipv6 a subinterfaz de la vlan 3</p> <p>asigna dirección local ipv6 a subinterface de la vlan 3</p> <p>salir</p> <p>configura subinterface</p> <p>encapsula tráfico de la subinterface descripción o nombre de la vlan</p> <p>asigna dirección ipv4 a subinterface de la vlan 4</p> <p>asigna dirección ipv6 a subinterfaz de la vlan 4</p> <p>asigna dirección local ipv6 a subinterface de la vlan 4</p> <p>salir</p> <p>configura subinterface</p> <p>encapsula tráfico de la subinterface descripción o nombre de la vlan 6</p> <p>ingresa a interface principal enciende la interface</p>
<pre> R1(config-if)#interface loopback 0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address FE80::1 link- local R1(config-if)#description loopback R1(config-if)#exit </pre>	<p>configura interfase de prueba</p> <p>asigna dirección ipv4 a interface de prueba</p> <p>asigna dirección ipv6 a interface de prueba</p> <p>asigna dirección ipv6 local a interface de prueba</p> <p>descripción o nombre de la interface</p> <p>salir</p>
<pre> R1(config)#crypto key generate rsa How many bits in the modulus [512]:1024 R1(config)#exit R1#copy r st </pre>	<p>genera clave de cifrado</p> <p>tamaño del módulo en bits</p> <p>salir</p> <p>guardar configuración realizada</p>

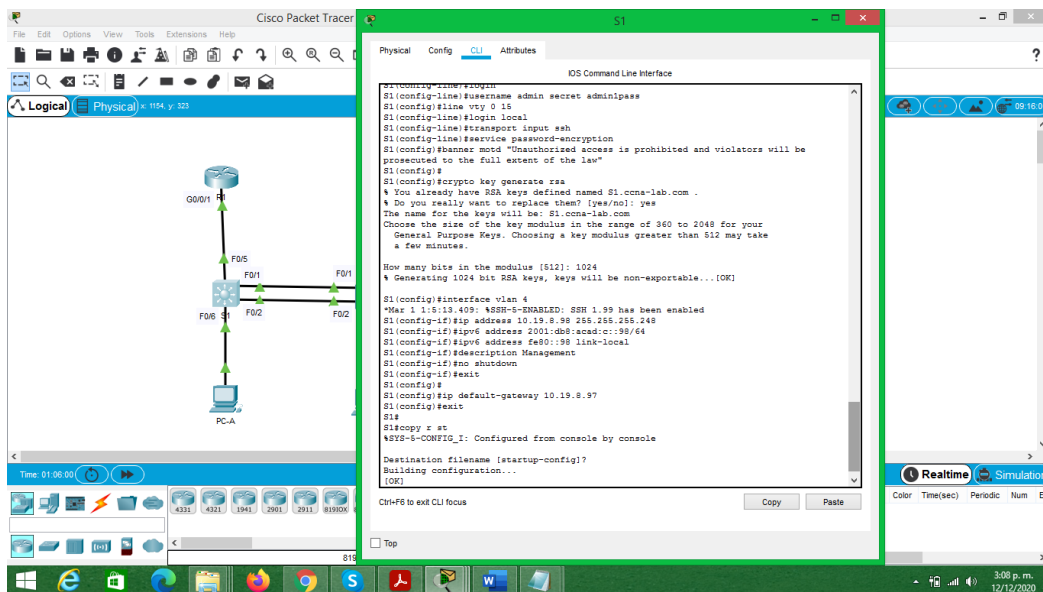
Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

En este paso se realiza la configuración del S1 y S2, donde se inicia desactivando el servicio de DNS, luego realizamos la configuración de su nombre y la seguridad para ingreso a consola y modo de configuración, y luego se cifran para garantizar la seguridad, además se crea un usuario para la administración de la base de datos local, también se configuro un banner con un mensaje de restricción.

De igual forma se configuro la interface para la Vlan 4 en los 2 dispositivos, donde se establecieron sus respectivas direcciones tanto para Ipv4 como para Ipv6, así mismo se configuro el Gateway predeterminado.

Figura 4. Proceso de Configuración S1



Fuente: Autor

En esta imagen podemos evidenciar el desarrollo de la configuración mas importante de S1, donde se configuro la interface para Vlan 4 y se establecieron sus direcciones ip, así mismo se configuro el Gateway predeterminado, el proceso se ve mas detalladamente en la siguiente tabla

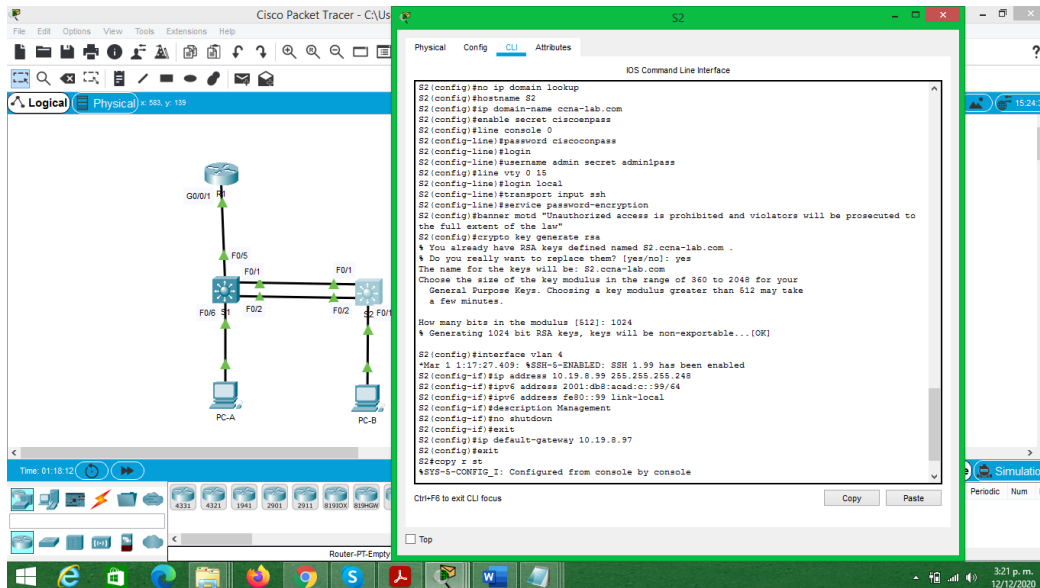
Configuración S1

Tabla 5. Proceso de Configuración S1

Switch>enable	ingreso a modo privilegiado
Switch#config t	ingreso a modo de configuración
Switch(config)#no ip domain lookup	Desactivar la búsqueda DNS
Switch(config)#hostname S1	asignar el nombre al switch

S1(config)#ip domain-name ccna-lab.com	asignar nombre de dominio
S1(config)#enable secret ciscoenpass	asignar contraseña cifrada para modo privilegiado
S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit	ingreso al modo de configuración de línea de consola asignar contraseña para acceso a consola activa la autenticación de inicio de sesión salir
S1(config)#username admin secret admin1pass	asignar un nombre de usuario y contraseña para para el ingreso a la base de datos local
S1(config)#line vty 0 15 S1(config-line)#login local	ingreso a configuración telnet activar la autenticación de inicio a la base de datos local
S1(config-line)#transport input ssh S1(config-line)#exit	configura solo acceso remoto salir
S1(config)#service password-encryption	cifrado para las contraseñas
S1(config)#banner motd "Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law"	configura un mensaje de inicio de sesión
S1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024	genera clave de cifrado tamaño del módulo de clave en bits
S1(config)#interface vlan 4 S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address FE80::98 link-local S1(config-if)#description Management S1(config-if)#no shutdown S1(config-if)#exit	configura interfase vlan 4 asigna dirección ipv4 a vlan 4 asigna dirección ipv6 a vlan 4 asigna dirección ipv6 local a vlan 4 descripción o nombre de la vlan 4 enciende la interface salir
S1(config)#ip default-Gateway 10.19.8.97 S1(config)#exit S1#copy r st	configura puerta de enlace para ipv4 salir guardar configuración realizada

Figura 5. Proceso de Configuración S2



Fuente: Autor

En esta imagen podemos evidenciar el desarrollo de la configuración mas importante de S2, donde se configuro la interface para Vlan 4 y se establecieron sus direcciones ip, así mismo se configuro el Gateway predeterminado, el proceso se ve mas detalladamente en la siguiente tabla

Configuración S2

Tabla 6. Proceso de Configuración S2

Switch>enable	ingreso a modo privilegiado
Switch#config t	ingreso a modo de configuración
Switch(config)#no ip domain lookup	Desactivar la búsqueda DNS
Switch(config)#hostname S1	asignar el nombre al switch
S2(config)#ip domain-name ccna-lab.com	asignar nombre de dominio
S2(config)#enable secret ciscoenpass	asignar contraseña cifrada para modo privilegiado
S2(config)#line console 0	ingreso al modo de configuración de línea de consola
S2(config-line)#password ciscoconpass	asignar contraseña para acceso a consola
S2(config-line)#login	activa la autenticación de inicio de sesión

S2(config-line)#exit	salir
S2(config)#username admin secret admin1pass	asignar un nombre de usuario y contraseña para para el ingreso a la base de datos local
S2(config)#line vty 0 15 S2(config-line)#login local	ingreso a configuración telnet activar la autenticación de inicio a la base de datos local
S2(config-line)#transport input ssh S2(config-line)#exit	configura solo acceso remoto salir
S2(config)#service password-encryption	cifrado para las contraseñas
S2(config)#banner motd "Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law"	configura un mensaje de inicio de sesión
S2(config)#crypto key generate rsa How many bits in the modulus [512]: 1024	genera clave de cifrado tamaño del módulo de clave en bits
S2(config)#interface vlan 4 S2(config-if)#ip address 10.19.8.99 255.255.255.248 S2(config-if)#ipv6 address 2001:db8:acad:c::98/64 S2(config-if)#ipv6 address FE80::98 link-local S2(config-if)#description Management S2(config-if)#no shutdown S2(config-if)#exit	configura interfase vlan 4 asigna dirección ipv4 a vlan 4 asigna dirección ipv6 a vlan 4 asigna dirección ipv6 local a vlan 4 descripción o nombre de la vlan 4 enciende la interface salir
S1(config)#ip default-Gateway 10.19.8.97 S1(config)#exit S1#copy r st	configura puerta de enlace para ipv4 salir guardar configuración realizada

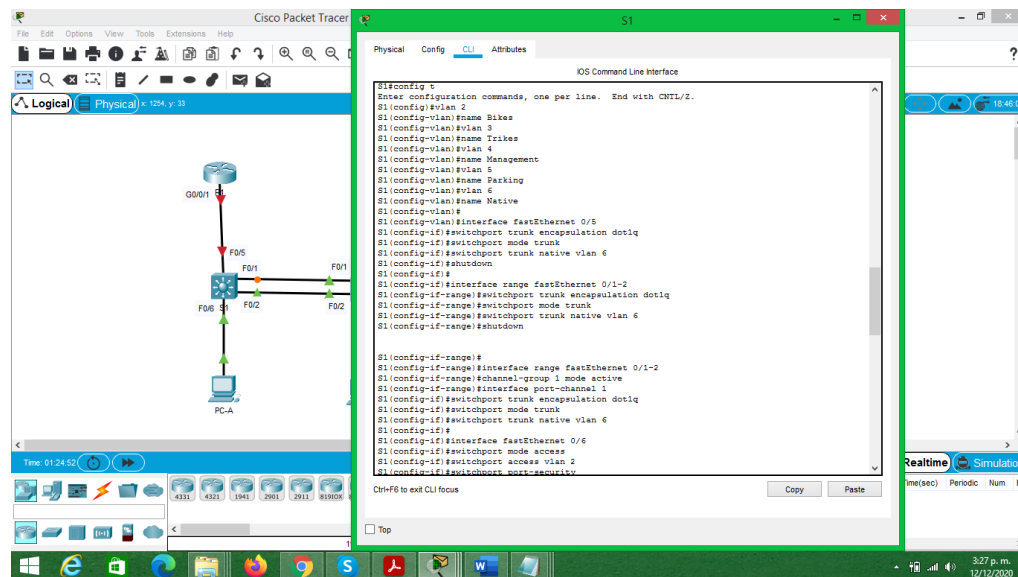
Parte 2: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

En este paso se realiza la configuración del S1 donde realizamos la creación de las Vlan 2, 3, 4, 5 y 6, luego se creó las troncales en los puertos F0/1, F0/2 y F0/5 para que utilicen la Vlan 6 nativa y se configuro un grupo de conexión con el protocolo LACP para la negociación, así mismo se configuro el modo acceso en la interface 6. De igual se configuraron en modo acceso las interfaces que no se utilizan y se le asignaron a la Vlan 5 para luego apagarlas.

Figura 6. Proceso de Configuración y Creación de Vlan S1



Fuente: Autor

En esta imagen podemos evidenciar el desarrollo de la configuración y creación de Vlan en S1, a si mismo se configuraron en modo acceso las interfaces que no se utilizan y se le asignaron a la Vlan 5 para luego apagarlas, el proceso se ve mas detalladamente en la siguiente tabla

Configuración S1

Tabla 7. Proceso de Configuración y Creación de Vlan S1

S1>enable	ingreso a modo privilegiado
Password:	
S1#config t	ingreso a modo de configuración
S1(config)#vlan 2	crea vlan 2
S1(config-vlan)#name Bikes	dar nombre a la vlan creada

<p>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 S1(config-vlan)#exit</p>	<p>crea vlan 3 dar nombre a la vlan creada crea vlan 4 dar nombre a la vlan creada crea vlan 5 dar nombre a la vlan creada crea vlan 6 dar nombre a la vlan creada salir</p>
<p>S1#config t S1(config)#interface fastEthernet 0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native</p> <p>S1(config-if)#no shutdown S1(config-if)#exit S1#config t S1(config)#interface range fastEthernet 0/1-2</p> <p>S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6</p>	<p>ingreso a modo de configuración ingreso a interface encapsula el tráfico de la troncal</p> <p>crea el modo trocal en la interface vlan 6 crea el modo troncal en la interface para que utilice la vlan 6 nativa enciende interface salir</p> <p>ingreso a modo de configuración ingresa al rango de interfaces seleccionadas para darles una configuración encapsula el tráfico de la troncal</p> <p>crea el modo trocal en la interface</p> <p>crea el modo troncal en la interface para que utilice la vlan 6 nativa</p>
<p>S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#interface port- channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if-range)#shutdown S1(config-if-range)#exit</p>	<p>agrupa las interfaces 1 y 2 para crear un solo canal y permitir la negociación ingresa a la interface creada</p> <p>encapsula el tráfico de la troncal</p> <p>crea el modo trocal en la interface crea el modo troncal en la interface para que utilice la vlan 6 nativa enciende la interface salir</p>
<p>S1(config)#interface fastEthernet 0/6 S1(config-if)#switchport mode access</p>	<p>ingresa a la interface modifica en modo del puerto para acceso</p>

S1(config-if)#switchport access vlan 2	configura el acceso por el puerto a la vlan 2
S1(config-if)#switchport port-security	configura la seguridad para el acceso al puerto
S1(config-if)#switchport port-security maximum 3	configura el puerto para que solo solo admita 3 direcciones MAC
S1(config-if)#interface range fastethernet 0/3-4	ingresa al rango de interfaces seleccionadas para darles una configuración
S1(config-if-range)#switchport mode access	modifica en modo del puerto para acceso
S1(config-if-range)#switchport access vlan 5	configura el acceso por el puerto a la vlan 5
S1(config-if-range)#description no están en uso	descripción del estado del puerto
S1(config-if-range)#shutdown	apaga la interface
S1(config-if-range)#exit	salir
S1(config)#interface range fastethernet 0/7-24	ingresa al rango de interfaces seleccionadas para darles una configuración
S1(config-if-range)#switchport mode access	modifica en modo del puerto para acceso
S1(config-if-range)#switchport access vlan 5	configura el acceso por el puerto a la vlan 5
S1(config-if-range)#description no están en uso	descripción del estado del puerto
S1(config-if-range)#shutdown	apaga la interface
S1(config-if-range)#exit	salir
S1(config)#interface range gigabitethernet 0/1-2	ingresa al rango de interfaces seleccionadas para darles una configuración
S1(config-if-range)#switchport mode access	modifica en modo del puerto para acceso
S1(config-if-range)#switchport access vlan 5	configura el acceso por el puerto a la vlan 5
S1(config-if-range)#description no están en uso	descripción del estado del puerto
S1(config-if-range)#shutdown	apaga la interface
S1(config-if-range)#exit	salir
S1(config)#interface range fastEthernet0/1-2	ingresa al rango de interfaces seleccionadas para darles una configuración
S1(config-if-range)#no shutdown	enciende la interface
S1(config-if-range)#exit	salir

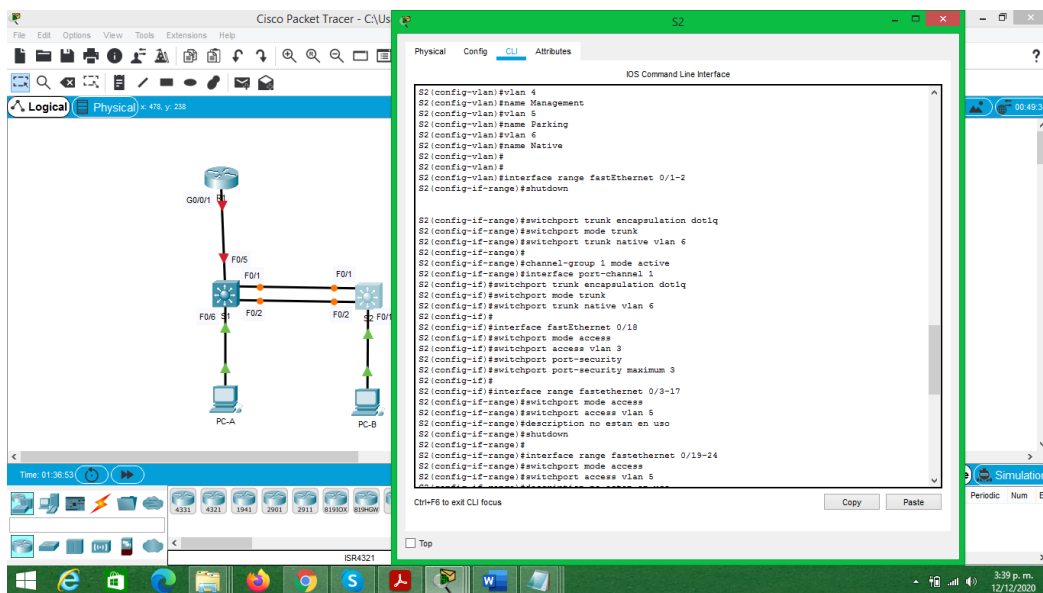
Paso 5: Configure el S2.

Entre las tareas de configuración de S2 se incluyen las siguientes:

En este paso se realiza la configuración del S1 donde realizamos la creación de las Vlan 2, 3, 4, 5 y 6, luego se creó las troncales en los puertos F0/1, F0/2 para que utilicen la Vlan 6 nativa y se configuro un grupo de conexión con el protocolo LACP para la negociación, así mismo se configuro el modo acceso en la interface 18

De igual se configuraron en modo acceso las interfaces que no se utilizan y se le asignaron a la Vlan 5 para luego apagarlas.

Figura 7. Proceso de Configuración y Creación de Vlan S2



Fuente: Autor

En esta imagen podemos evidenciar el desarrollo de la configuración y creación de Vlan en S1, a si mismo se configuraron en modo acceso las interfaces que no se utilizan y se le asignaron a la Vlan 5 para luego apagarlas, el proceso se ve mas detalladamente en la siguiente tabla

Configuración S2

Tabla 8. Proceso de Configuración y Creación de Vlan S2

S2>enable	ingreso a modo privilegiado
S2#config t	ingreso a modo de configuración
S2(config)#vlan 2	crea vlan 2
S2(config-vlan)#name Bikes	dar nombre a la vlan creada
S2(config-vlan)#vlan 3	crea vlan 3

<p>S2(config-vlan)#name Trikes S2(config-vlan)#vlan 4 S2(config-vlan)#name Management S2(config-vlan)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#vlan 6 S2(config-vlan)#name Native S2(config-vlan)#exit</p>	<p>dar nombre a la vlan creada crea vlan 4 dar nombre a la vlan creada crea vlan 5 dar nombre a la vlan creada crea vlan 6 dar nombre a la vlan creada salir</p>
<p>S2#config t S2(config)#interface range fastEthernet 0/1-2 S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 6 S2(config-if)#exit</p>	<p>ingreso a modo de configuración ingresa al rango de interfaces seleccionadas para darles una configuración encapsula el tráfico de la troncal crea el modo trocal en la interface crea el modo troncal en la interface para que utilice la vlan 6 nativa salir</p>
<p>S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#interface port-channel 1 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config-if-range)#shutdown S2(config-if-range)#exit</p>	<p>agrupa las interfaces 1 y 2 para crear un solo canal y permitir la negociación ingresa a la interface creada encapsula el tráfico de la troncal crea el modo trocal en la interface crea el modo troncal en la interface para que utilice la vlan 6 nativa enciende interface salir</p>
<p>S2(config)#interface fastEthernet 0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#switchport port-security</p>	<p>ingresa a la interface modifica en modo del puerto para acceso configura el acceso por el puerto a la vlan 3 configura la seguridad para el acceso al puerto</p>
<p>S2(config-if)#switchport port-security maximum 3</p>	<p>configura el puerto para que solo solo admita 3 direcciones MAC</p>

S2(config-if)#interface range fastethernet 0/3-17	ingresa al rango de interfaces seleccionadas para darles una configuración
S2(config-if-range)#switchport mode access	modifica en modo del puerto para acceso
S2(config-if-range)#switchport access vlan 5	configura el acceso por el puerto a la vlan 5
S2(config-if-range)#description no están en uso	descripción del estado del puerto
S2(config-if-range)#shutdown	apaga la interface
S2(config-if-range)#exit	salir
S2(config)#interface range fastethernet 0/19-24	ingresa al rango de interfaz seleccionada para darles configuración
S2(config-if-range)#switchport mode access	modifica en modo del puerto para acceso
S2(config-if-range)#switchport access vlan 5	configura el acceso por el puerto a la vlan 5
S2(config-if-range)#description no están en uso	descripción del estado del puerto
S2(config-if-range)#shutdown	apaga la interface
S2(config-if-range)#exit	salir
S2(config)#interface range gigabitethernet 0/1-2	ingresa al rango de interfaces seleccionadas para darles una configuración
S2(config-if-range)#switchport mode access	modifica en modo del puerto para acceso
S2(config-if-range)#switchport access vlan 5	configura el acceso por el puerto a la vlan 5
S2(config-if-range)#description no están en uso	descripción del estado del puerto
S2(config-if-range)#shutdown	apaga la interface
S2(config-if-range)#exit	salir
S2(config)#interface range fastEthernet0/1-2	ingresa al rango de interfaces seleccionadas para darles una configuración
S2(config-if-range)#no shutdown	enciende la interface
S2(config-if-range)#exit	salir
S2#copy r st	guardar configuración realizada

Parte 2: Configurar soporte de host

Paso 1: Configure R1

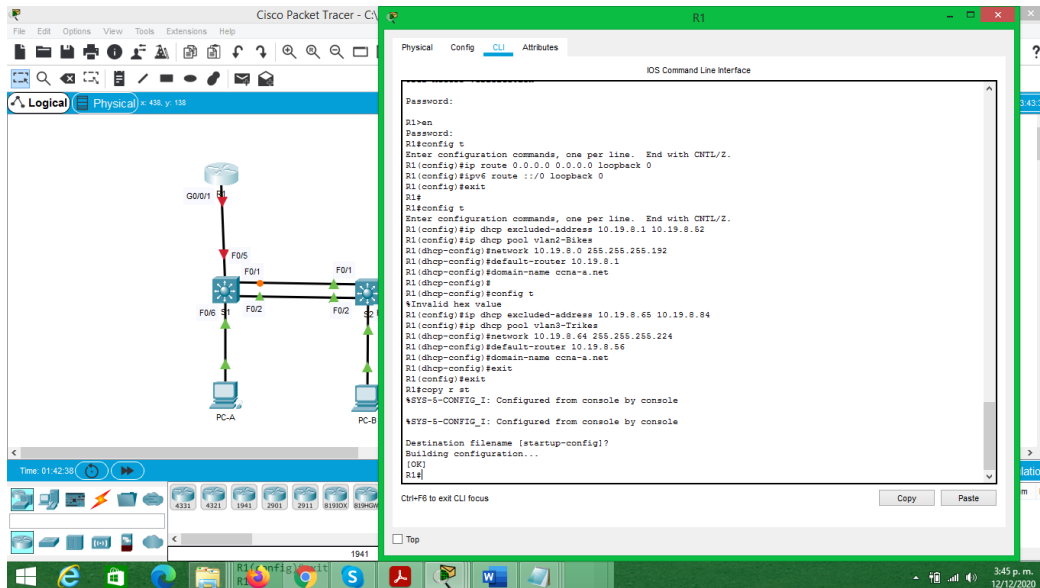
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 9. Creación de rutas y DHCP para Vlan 2 y 3

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0
Configurar IPv4 DHCP para VLAN 2	Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio cca-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada
Configurar DHCP IPv4 para VLAN 3	Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio cca-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada

En este paso se realiza la configuración del R1, donde creamos las rutas para Ipv4 e Ipv6 para que guíen el tráfico a la Loopback 0, también creamos un pool DHCP con las últimas 10 direcciones de la subred tanto para la Vlan 2 como para la Vlan 3, donde le asignamos un nombre de dominio y le asignamos la dirección predeterminada como puerta de enlace

Figura 8. Proceso Configuración y Creación de rutas y DHCP para Vlan 2 y 3



Fuente: Autor

En esta imagen podemos evidenciar el desarrollo de la configuración y creación de rutas y DHCP para Vlan 2 y 3 en R1, donde creamos las rutas para Ipv4 e Ipv6 para que guíen el tráfico a la Loopback 0, también creamos un pool DHCP con las ultimas 10 direcciones de la subred tanto para la Vlan 2 como para la Vlan 3, el proceso se ve mas detalladamente en la siguiente tabla

Configuración R1

Tabla 10. Proceso Configuración y Creación de rutas y DHCP para Vlan 2 y 3

<pre>R1#config t R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0 R1(config)#exit</pre>	<p>ingreso a modo de configuración crea ruta establecida Ipv4 para enviar el tráfico a la interface loopback 0 crea ruta establecida Ipv4 para enviar el tráfico a la interface loopback 0 salir</p>
<pre>R1#config t R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#ip dhcp pool vlan2-Bikes</pre>	<p>ingreso a modo de configuración se excluye las direcciones desde la .1 a la .52 para que no se asignen por dhcp se crea el pool de direcciones para la vlan 2 con las 10 direcciones</p>

<pre>R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#domain-name ccna- a.net R1(dhcp-config)#exit R1(config)#exit</pre>	<p>sobrantes de la subred. Que va de la .53 a la .62 se asigna la dirección de red a la vlan2</p> <p>se asigna la dirección predeterminada para la puerta de enlace de la subred fija nombre de dominio a la interface</p> <p>salir salir</p>
<pre>R1#config t R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84 R1(config)#ip dhcp pool vlan3-Trikes R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(dhcp-config)#domain-name ccna- a.net R1(dhcp-config)#exit R1(config)#exit R1#copy r st</pre>	<p>ingreso a modo de configuración se excluye las direcciones desde la .65 a la .84 para que no se asignen por dhcp</p> <p>se crea el pool de direcciones para la vlan 3 con las 10 direcciones sobrantes de la subred. Que va de la .85 a la .94</p> <p>se asigna la dirección de red a la vlan3</p> <p>se asigna la dirección predeterminada para la puerta de enlace de la subred fija nombre de dominio a la interface</p> <p>salir salir guardar configuración realizada</p>

Paso 2: 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 11. Configuración de red equipo PC-A

Configuración de red de PC-A	
Descripción	FastEthernet0 Connection
Dirección física	0090.0CC4.7332
Dirección IP	Ipv6 2001:DB8:ACAD:A::50 Ipv4 10.19.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

Tabla 12. Configuración de red equipo PC-B

Configuración de red de PC-B	
Descripción	FastEthernet0 Connection
Dirección física	0030.F249.5D17
Dirección IP	Ipv6 2001:DB8:ACAD:B::50 Ipv4 10.19.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	FE80::1
Gateway predeterminado IPv6	10.19.8.65

Parte 3: Probar y verificar la conectividad de extremo a extremo

Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

Nota: Si fallan los pings en las computadoras host, desactive temporalmente el firewall de la computadora y vuelva a realizar la prueba.

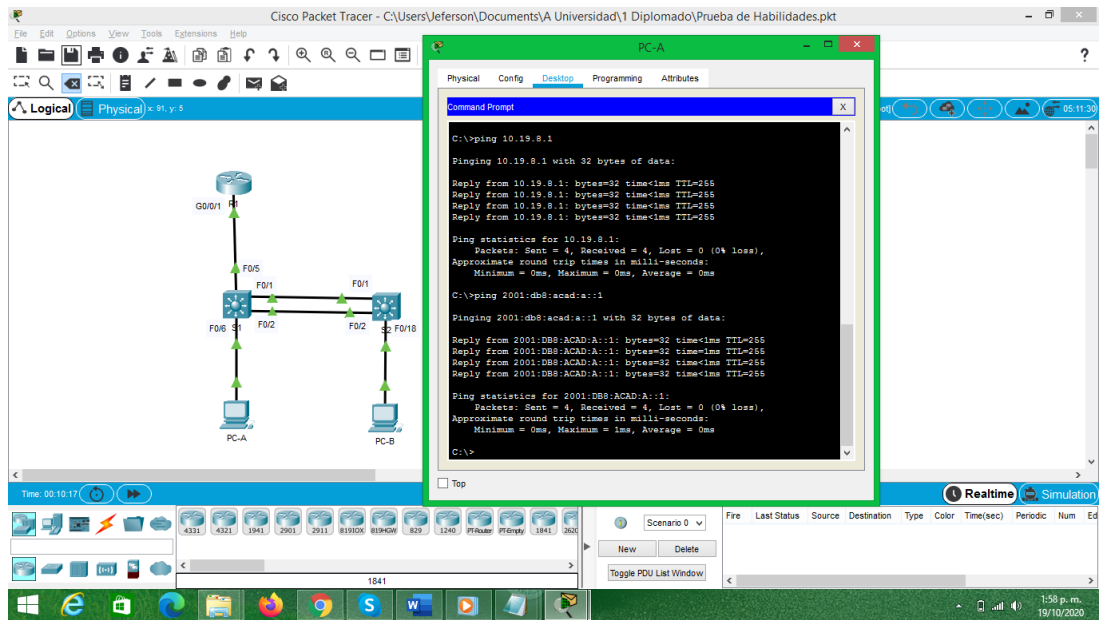
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 13. Direccionamiento para verificar conectividad de extremo a extremo

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	
		IPv6	2001:db8:acad:b :1	OK	

Desde	A	de Internet	Dirección IP	Resultados de ping
	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

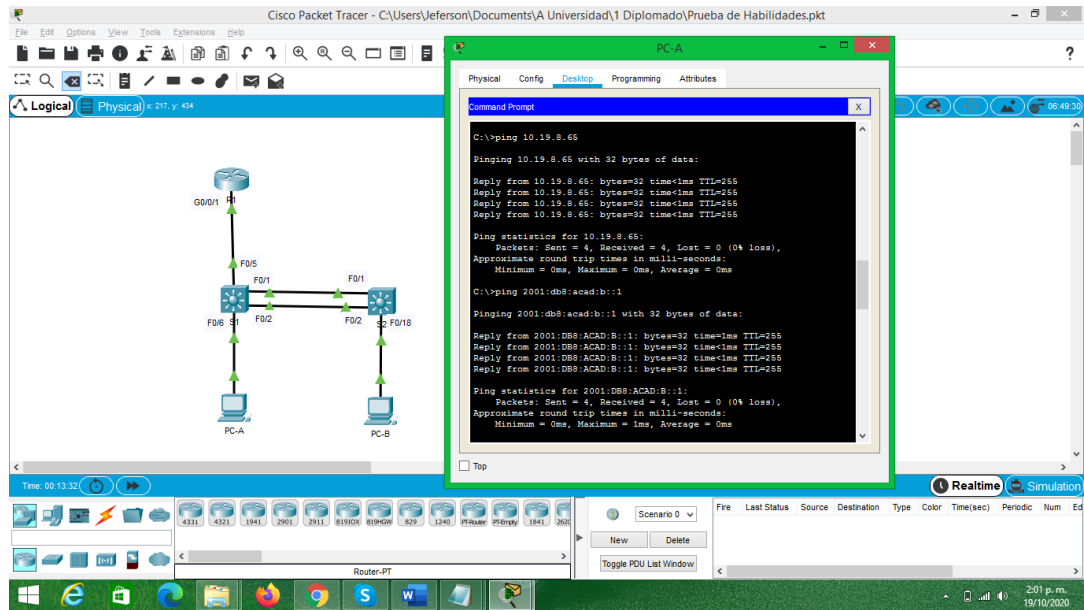
Figura 9. Ping de PC-A a R1, G0/0/1.2 Ipv4 e Ipv6



Fuente: Autor

Se realiza ping desde PC-A a dirección Ipv4 e Ipv6 con éxito

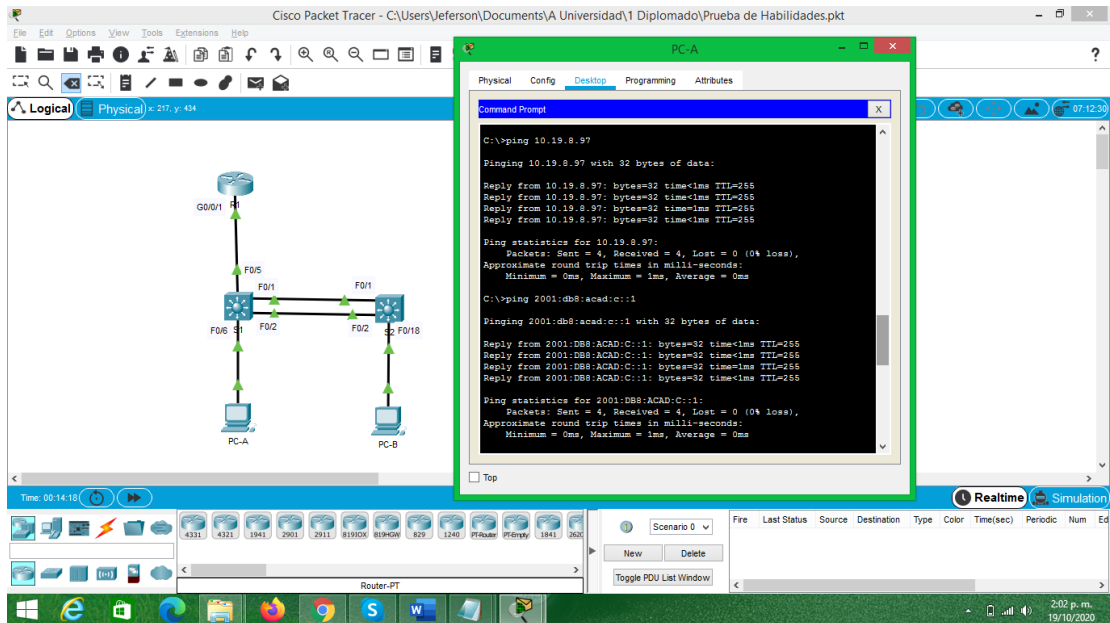
Figura 10. Ping de PC-A a R1, G0/0/1.3 Ipv4 e Ipv6



Fuente: Autor

Se realiza ping desde PC-A a dirección Ipv4 e Ipv6 con éxito

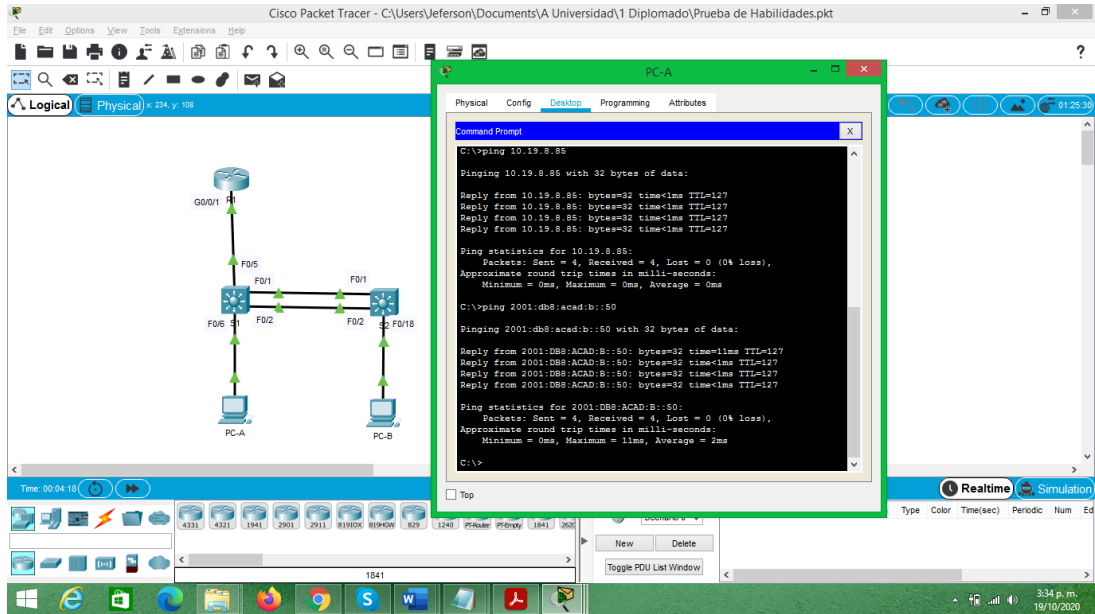
Figura 11. Ping de PC-A a R1, G0/0/1.4 Ipv4 e Ipv6



Fuente: Autor

Se realiza ping desde PC-A a dirección Ipv4 e Ipv6 con éxito

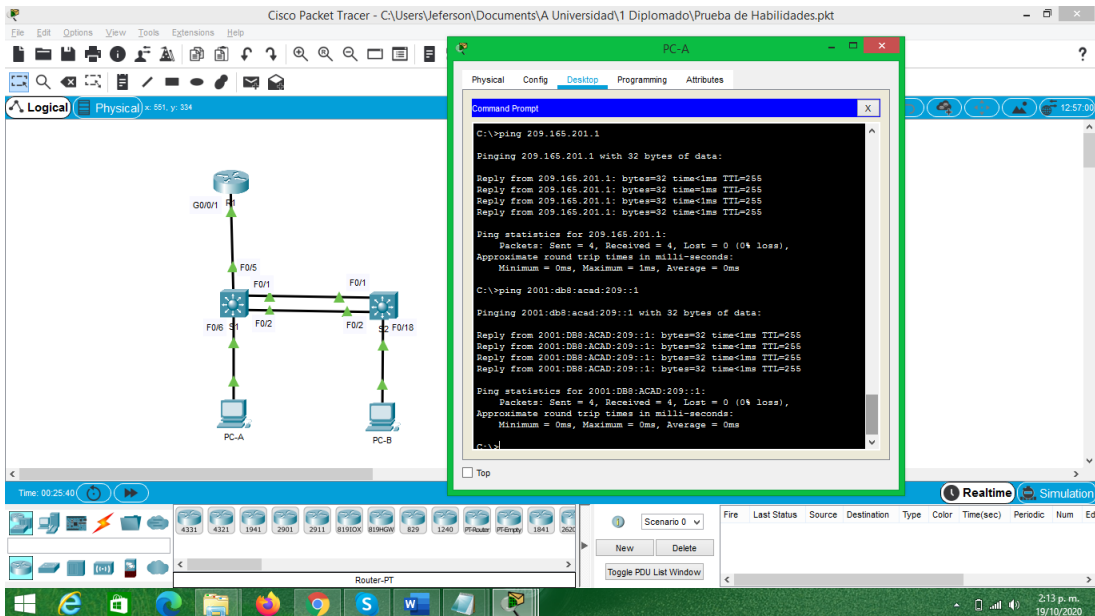
Figura 12. Ping de PC-A a PC-B Ipv4 e Ipv6



Fuente: Autor

Se realiza ping desde PC-A a PC-B a dirección Ipv4 e Ipv6 con éxito, en el caso de los pings Ipv4 de PC-A a PC-B se debe verificar primero la dirección asignada por DHCP, en este caso la dirección Ipv4 asignada por el DHCP al PC-B fue 10.19.8.85

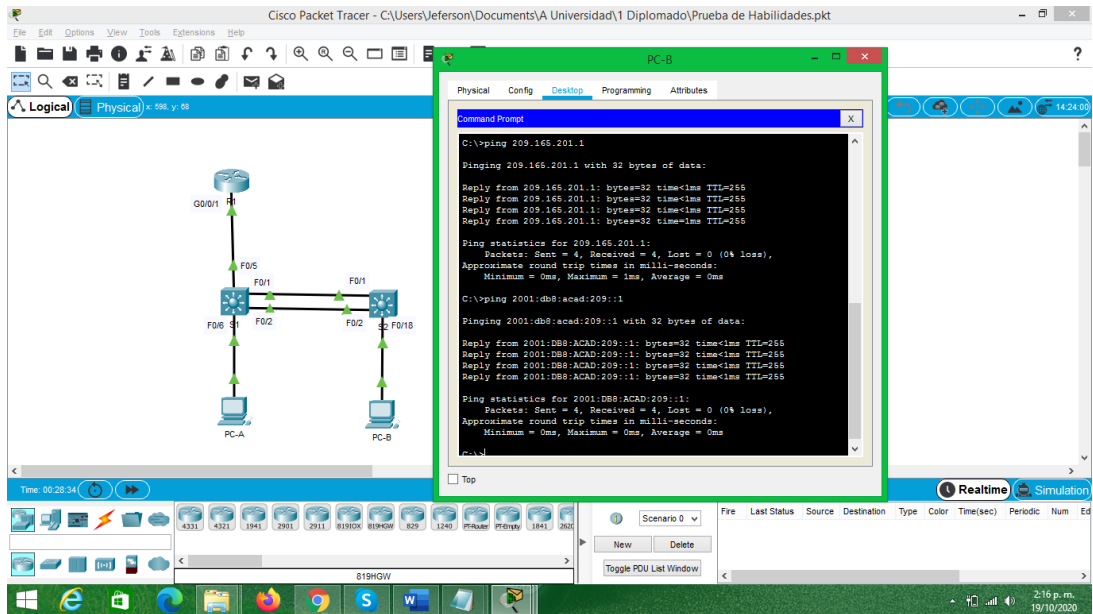
Figura 13. Ping de PC-A a R1 Loopback 0, Ipv4 e Ipv6



Fuente: Autor

Se realiza ping desde PC-A a R1 Loopback 0, dirección Ipv4 e Ipv6 con éxito

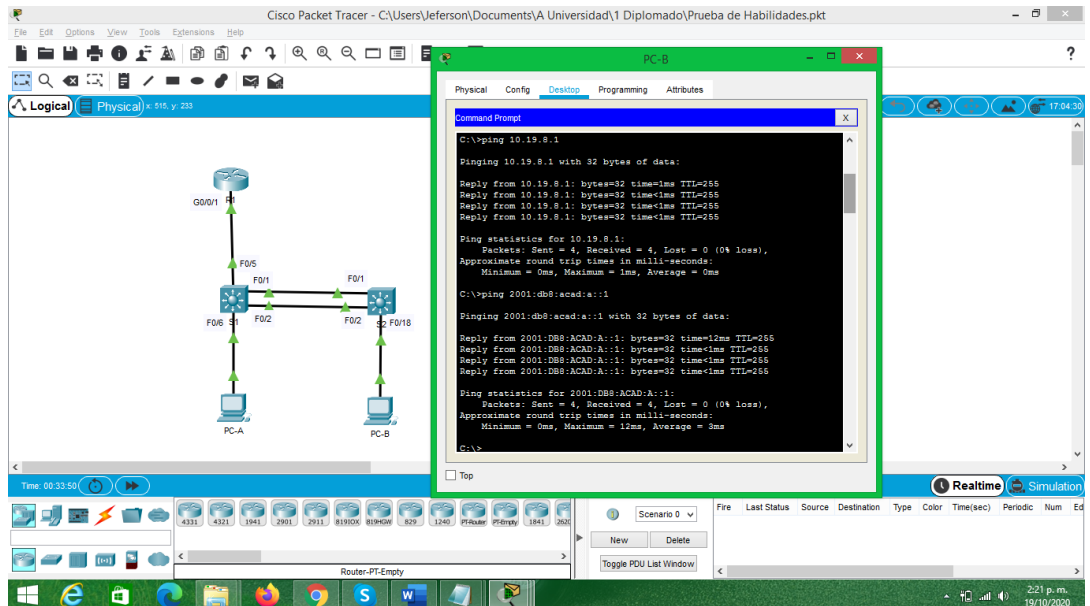
Figura 14. Ping de PC-B a R1 Loopback 0, Ipv4 e Ipv6



Fuente: Autor

Se realiza ping desde PC-B a dirección Ipv4 e Ipv6 con éxito

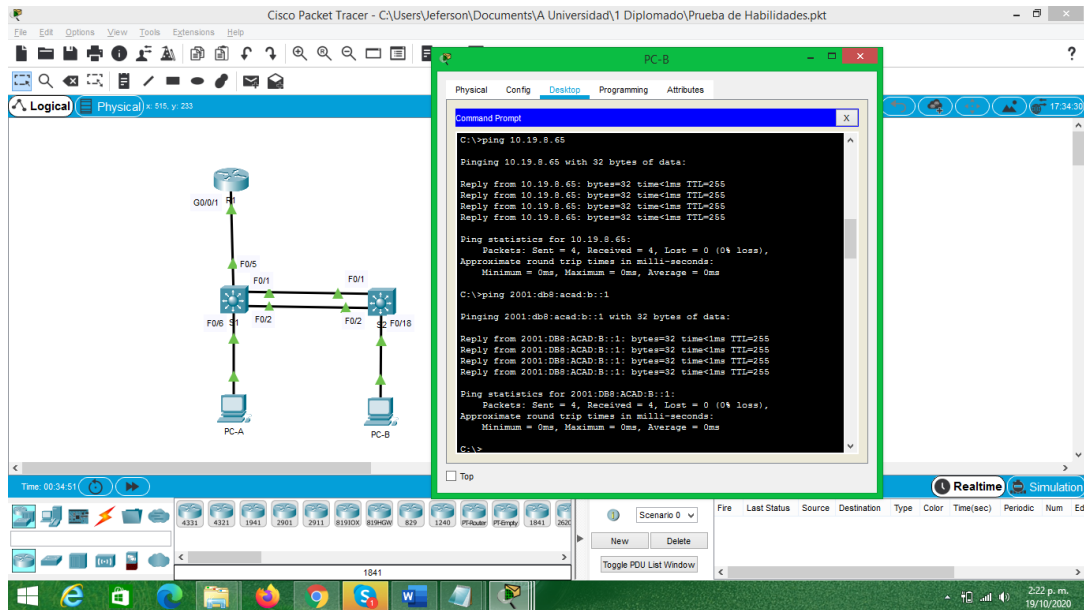
Figura 15. Ping de PC-B a R1, G0/0/1.2 Ipv4 e Ipv6



Fuente: Autor

Se realiza ping desde PC-B a dirección Ipv4 e Ipv6 con éxito

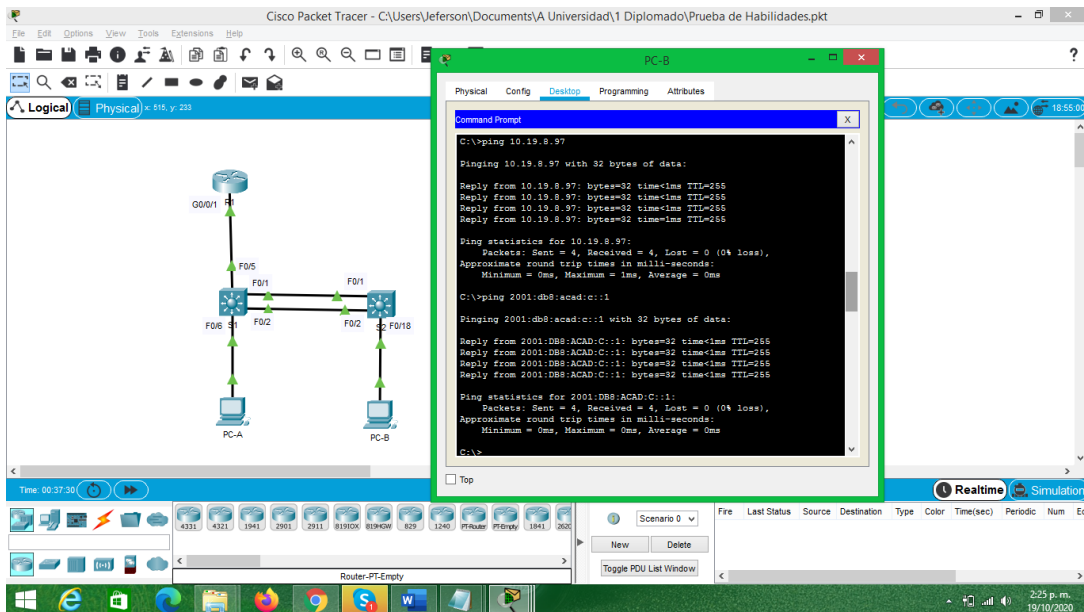
Figura 16. Ping de PC-B a R1, G0/0/1.3 Ipv4 e Ipv6



Fuente: Autor

Se realiza ping desde PC-B a dirección Ipv4 e Ipv6 con éxito

Figura 17. Ping de PC-B a R1, G0/0/1.4 Ipv4 e Ipv6

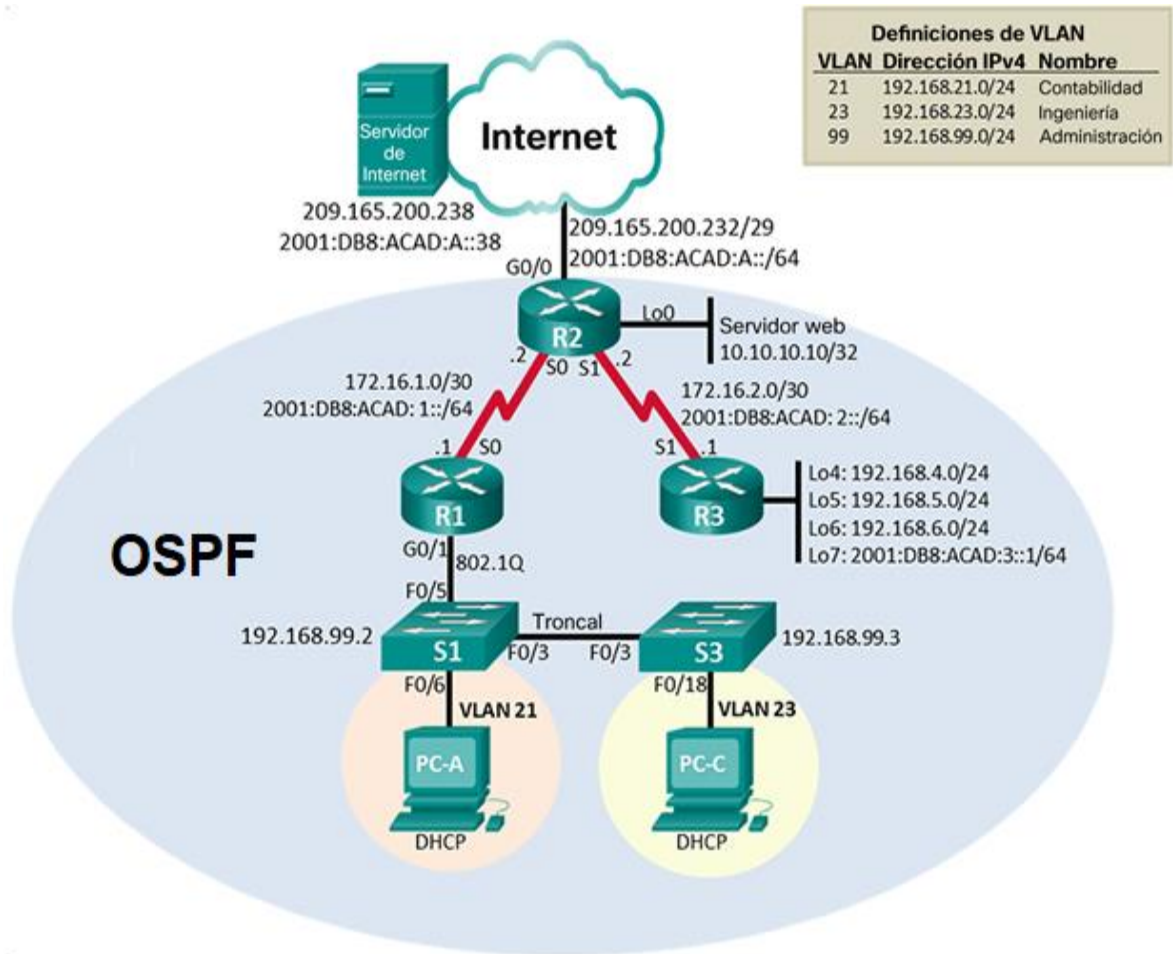


Fuente: Autor

Se realiza ping desde PC-B a dirección Ipv4 e Ipv6 con éxito

2. ESCENARIO 2

Figura 18. Escenario 2



Parte 1: Inicializar dispositivos

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

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

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

Tabla 14. Pasos Configuración inicial Escenario 2

Router>enable	ingreso a modo privilegiado
Router#erase startup-config	eliminar configuración de inicio
Router#reload	recargar el equipo
Switch>enable	ingreso a modo privilegiado
Switch#erase startup-config	eliminar configuración de inicio
Switch#delete vlan.dat	eliminar el archivo vlan
Switch#reload	recargar el equipo
Switch# show vlan brief	Verifica que se eliminó con éxito las bases de datos de los swich

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

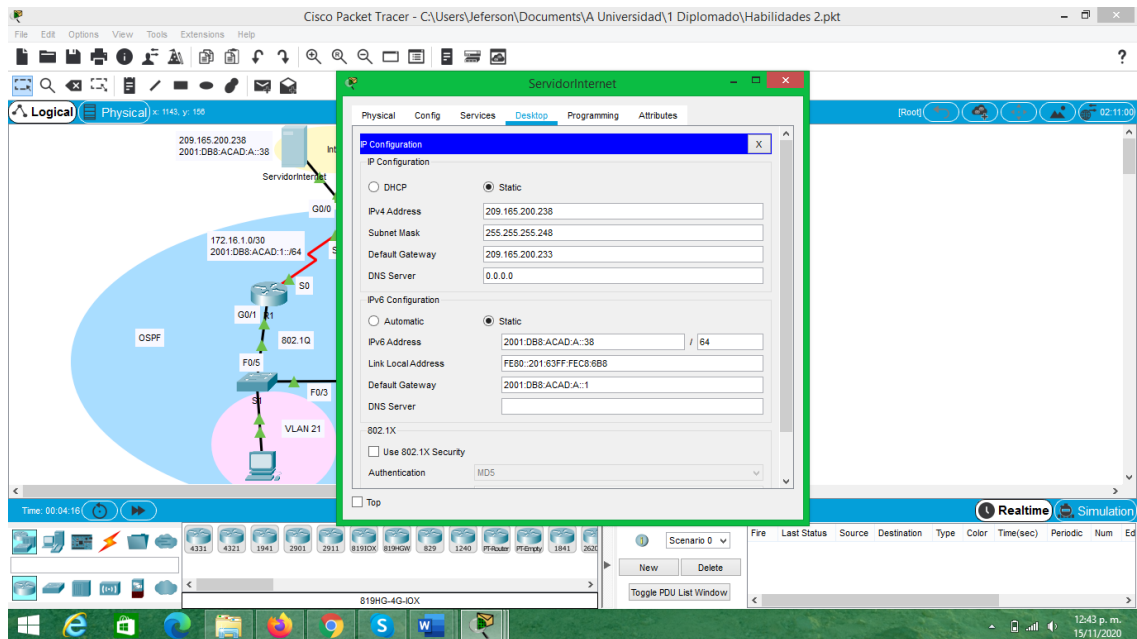
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 15. Configuración computadora de Internet

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

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

Figura 19. Configuración computadora de Internet



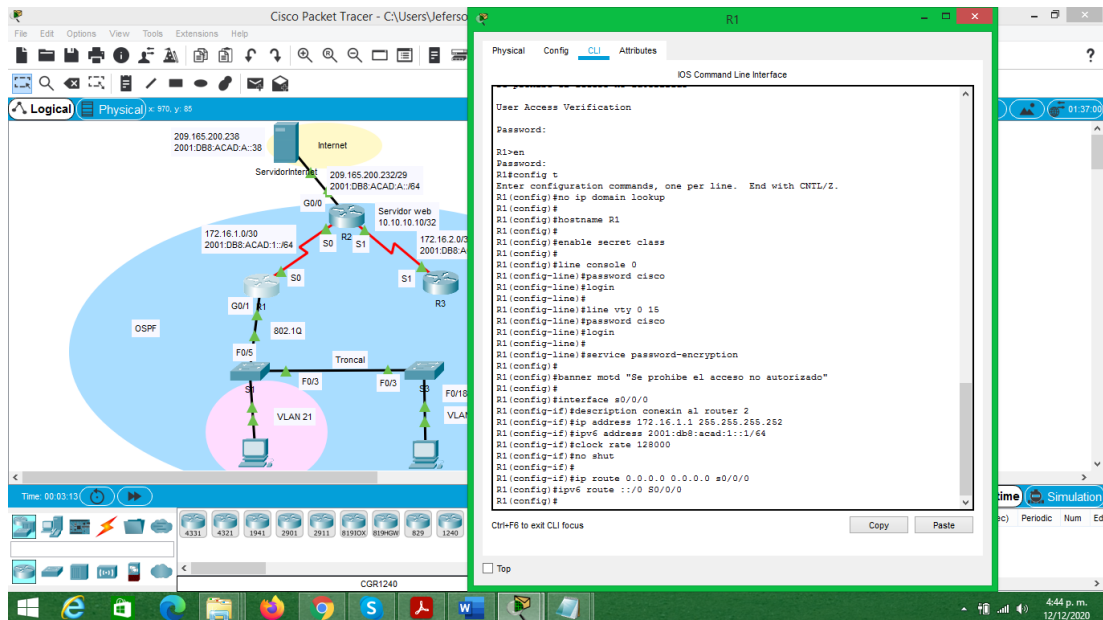
Fuente: Autor

Se realiza la configuración de la computadora de internet de acuerdo al direccionamiento dado en la topología

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Figura 20. Proceso de Configuración R1



Fuente: Autor

En esta imagen podemos evidenciar el desarrollo de la configuración mas importante en R1, donde asignamos las direcciones ip correspondientes a cada interface según la topología, así mismo creamos una ruta predeterminada para ipv4 e ipv6, el proceso se ve mas detalladamente en la siguiente tabla

Tabla 16. Proceso de Configuración R1

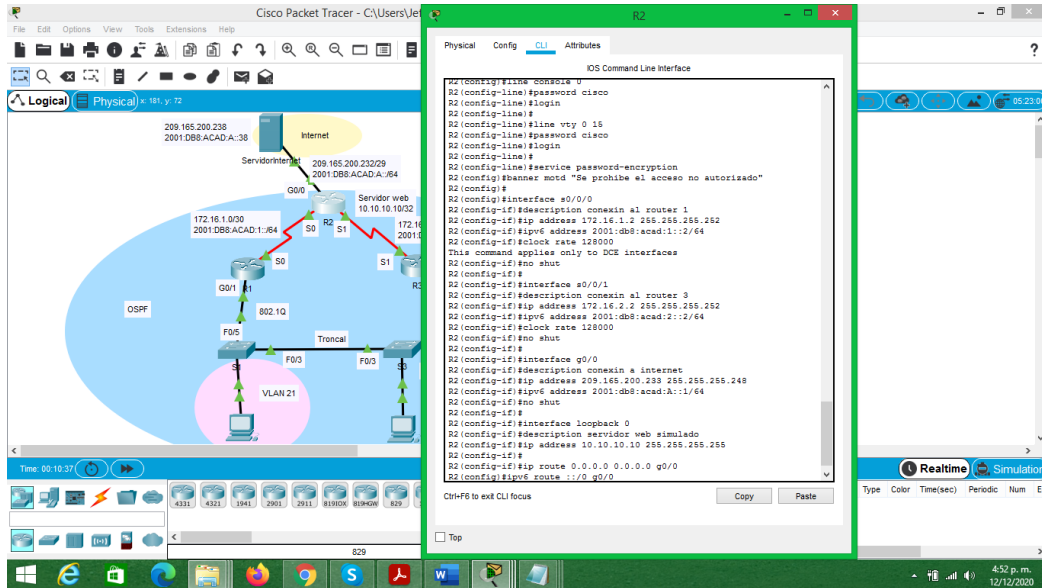
Router>enable	ingreso a modo privilegiado
Router#config t	ingreso a modo de configuración
Router(config)#no ip domain lookup	Desactivar la búsqueda DNS
Router(config)#hostname R1	asignar el nombre al router
R1(config)#enable secret class	asignar contraseña cifrada para modo privilegiado
R1(config)#line console 0	ingreso al modo de configuración de línea de consola
R1(config-line)#password cisco	asignar contraseña acceso consola

R1(config-line)#login	activa la autenticación de inicio de sesión
R1(config-line)#exit	salir
R1(config)#line vty 0 15	ingreso a configuración de telnet
R1(config-line)#password cisco	asigna contraseña de acceso
R1(config-line)#login	activar la autenticación de inicio
R1(config)#service password-encryption	cifrado para las contraseñas
R1(config)#banner motd " Se prohíbe el acceso no autorizado"	configura un mensaje de inicio de sesión
R1(config)#interface s0/0/0	Ingresa a la interface
R1(config-if)#description conexin al router 2	descripción o nombre de la interface
R1(config-if)#ip address 172.16.1.1 255.255.255.252	asigna dirección ipv4 a interface
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64	asigna dirección ipv6 a interface
R1(config-if)#clock rate 128000	establece la frecuencia de reloj
R1(config-if)#no shut	enciende la interface
R1(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/0	Configura ruta IPv4 predeterminada
R1(config)#ipv6 route ::/0 S0/0/0	Configura ruta IPv6 predeterminada

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Figura 21. Proceso de Configuración R2



Fuente: Autor

En esta imagen podemos evidenciar el desarrollo de la configuración mas importante en R2, donde asignamos las direcciones ip correspondientes a cada interface según la topología, así mismo creamos una ruta predeterminada para ipv4 e ipv6, el proceso se ve mas detalladamente en la siguiente tabla

Tabla 17. Proceso de Configuración R2

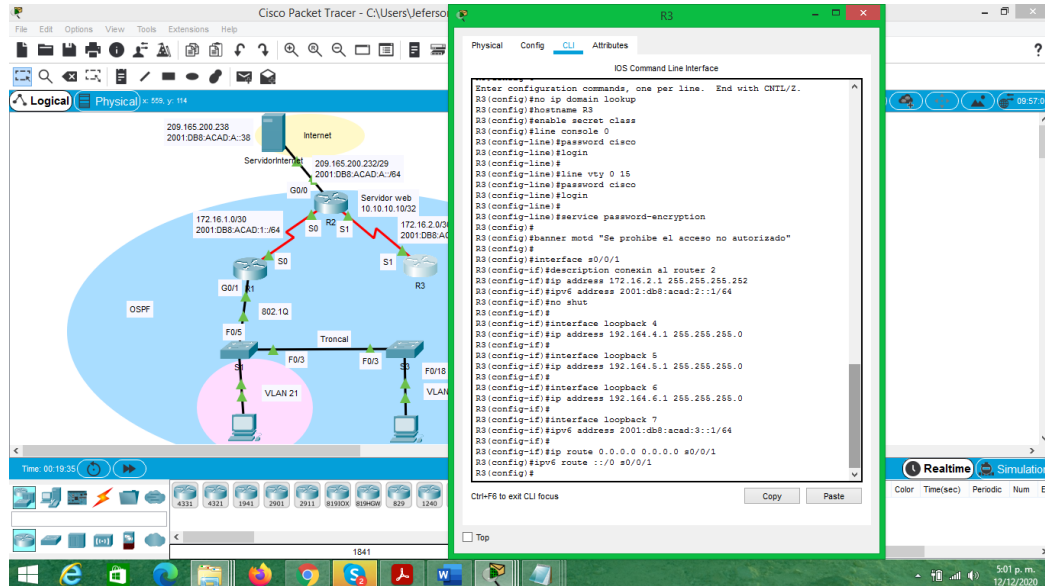
Router>enable	ingreso a modo privilegiado
Router#config t	ingreso a modo de configuración
Router(config)#no ip domain lookup	Desactivar la búsqueda DNS
Router(config)#hostname R1	asignar el nombre al router
R2(config)#enable secret class	asignar contraseña cifrada para modo privilegiado
R2(config)#line console 0	ingreso al modo de configuración de línea de consola
R2(config-line)#password cisco	asignar contraseña para acceso a consola
R2(config-line)#login	activa autenticación inicio de sesión
R2(config-line)#exit	salir

R2(config)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login	ingreso a configuración de telnet asigna contraseña de acceso activar la autenticación de inicio
R2(config)#service password-encryption	cifrado para las contraseñas
R2(config)#ip http server	Packet tracer no soporta el comando
R2(config)#banner motd " Se prohíbe el acceso no autorizado"	configura un mensaje de inicio de sesión
R2(config)#interface s0/0/0 R2(config-if)#description conexin router 1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shut	Ingresa a la interface descripción o nombre de la interface asigna dirección ipv4 a interface asigna dirección ipv6 a interface enciende la interface
R2(config-if)#interface s0/0/1 R2(config-if)#description conexin router 3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shut	Ingresa a la interface descripción o nombre de la interface asigna dirección ipv4 a interface asigna dirección ipv6 a interface establece la frecuencia de reloj enciende la interface
R2(config-if)#interface g0/0 R2(config-if)#description conexin internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:A::1/64 R2(config-if)#no shut	Ingresa a la interface descripción o nombre de la interface asigna dirección ipv4 a interface asigna dirección ipv6 a interface enciende la interface
R2(config-if)#interface loopback 0 R2(config-if)#description servidor web simulado R2(config-if)#ip address 10.10.10.10 255.255.255.255	Crea e Ingresa a la interface descripción o nombre de la interface asigna dirección ipv4 a interface
R2(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R2(config)#ipv6 route ::/0 S0/0/0	Configura ruta IPv4 predeterminada Configura ruta IPv6 predeterminada

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Figura 22. Proceso de Configuración R3



Fuente: Autor

En esta imagen podemos evidenciar el desarrollo de la configuración mas importante en R3, donde asignamos las direcciones ip correspondientes a cada interface según la topología, así mismo creamos una ruta predeterminada para ipv4 e ipv6, el proceso se ve mas detalladamente en la siguiente tabla

Tabla 18. Proceso de Configuración R3

Router>enable	ingreso a modo privilegiado
Router#config t	ingreso a modo de configuración
Router(config)#no ip domain lookup	Desactivar la búsqueda DNS
Router(config)#hostname R1	asignar el nombre al router
R3(config)#enable secret class	asignar contraseña cifrada para modo privilegiado
R3(config)#line console 0	ingreso al modo de configuración de línea de consola
R3(config-line)#password cisco	asignar contraseña acceso consola
R3(config-line)#login	activa la autenticación de inicio de sesión
R3(config-line)#exit	salir

R3(config)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login	ingreso a configuración de telnet asigna contraseña de acceso activar la autenticación de inicio
R3(config)#service password-encryption	cifrado para las contraseñas
R3(config)#ip http server	Packet tracer no soporta el comando
R3(config)#banner motd " Se prohíbe el acceso no autorizado"	configura un mensaje de inicio de sesión
R3(config)#interface s0/0/1 R3(config-if)#description conexin al router 1 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#no shut	Ingresa a la interface descripción o nombre de la interface asigna dirección ipv4 a interface asigna dirección ipv6 a interface enciende la interface
R3(config-if)#interface loopback 4 R3(config-if)#description servidor web simulado R3(config-if)#ip address 192.164.4.1 255.255.255.0	Crea e Ingresa a la interface descripción o nombre de la interface asigna dirección ipv4 a interface
R3(config-if)#interface loopback 5 R3(config-if)#description servidor web simulado R3(config-if)#ip address 192.164.5.1 255.255.255.0	Crea e Ingresa a la interface descripción o nombre de la interface asigna dirección ipv4 a interface
R3(config-if)#interface loopback 6 R3(config-if)#description servidor web simulado R3(config-if)#ip address 192.164.6.1 255.255.255.0	Crea e Ingresa a la interface descripción o nombre de la interface asigna dirección ipv4 a interface
R3(config-if)#interface loopback 7 R3(config-if)#description servidor web simulado R3(config-if)#ipv6 address 2001:db8:acad:3::1/64	Crea e Ingresa a la interface descripción o nombre de la interface asigna dirección ipv6 a interface
R3(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 S0/0/0	Configura ruta IPv4 predeterminada Configura ruta IPv6 predeterminada

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 19. Proceso de Configuración S1

Switch>enable	ingreso a modo privilegiado
Switch#config t	ingreso a modo de configuración
Switch(config)#no ip domain lookup	Desactivar la búsqueda DNS
Switch(config)#hostname S1	asignar el nombre al swich
S1(config)#enable secret class	asignar contraseña cifrada para modo privilegiado
S1(config)#line console 0	ingreso al modo de configuración de línea de consola
S1(config-line)#password cisco	asignar contraseña para acceso a consola
S1(config-line)#login	activa la autenticación de inicio de sesión
S1(config-line)#exit	salir
S1(config)#line vty 0 15	ingreso a configuración telnet
S1(config-line)#password cisco	asigna contraseña de acceso
S1(config-line)#login local	activar la autenticación de inicio
S1(config)#service password-encryption	cifrado para las contraseñas
S1(config)#banner motd "Se prohíbe el acceso no autorizado"	configura un mensaje de inicio de sesión

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 20. Proceso de Configuración S3

Switch>enable	ingreso a modo privilegiado
Switch#config t	ingreso a modo de configuración
Switch(config)#no ip domain lookup	Desactivar la búsqueda DNS
Switch(config)#hostname S1	asignar el nombre al swich
S3(config)#enable secret class	asignar contraseña cifrada para modo privilegiado
S3(config)#line console 0	ingreso al modo de configuración de línea de consola
S3(config-line)#password cisco	asignar contraseña para acceso a consola
S3(config-line)#login	activa la autenticación de inicio de sesión
S3(config-line)#exit	salir
S3(config)#line vty 0 15	ingreso a configuración telnet
S3(config-line)#password cisco	asigna contraseña de acceso
S3(config-line)#login local	activar la autenticación de inicio
S3(config)#service password-encryption	cifrado para las contraseñas
S3(config)#banner motd "Se prohíbe el acceso no autorizado"	configura un mensaje de inicio de sesión

Paso 7: Verificar la conectividad de la red

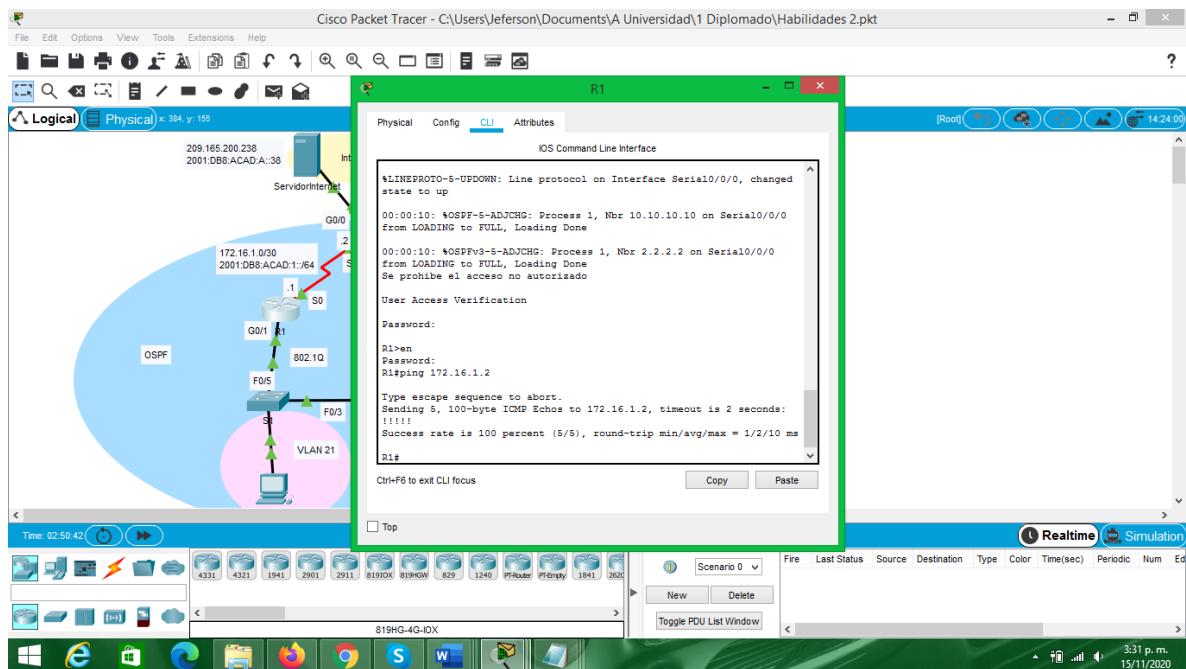
Utilice el comando ping para probar la conectividad entre los dispositivos de red.

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:

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

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

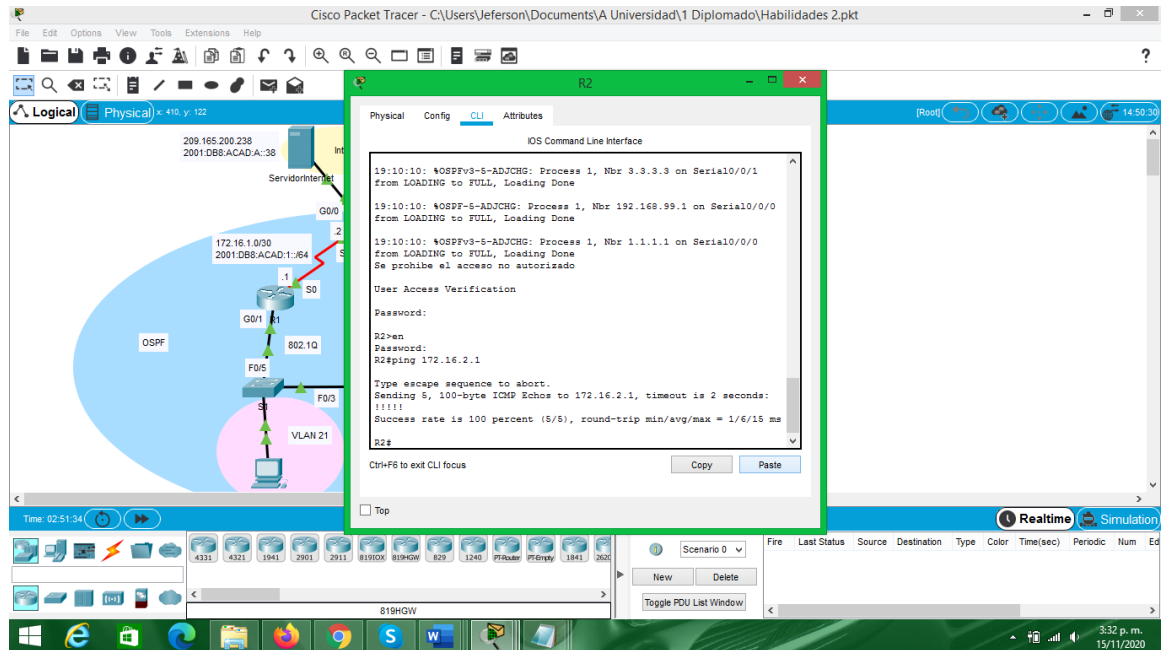
Figura 23. Ping de R1 a R2



Fuente: Autor

Se realiza ping desde R1 a R2 a la dirección IPv4 con éxito

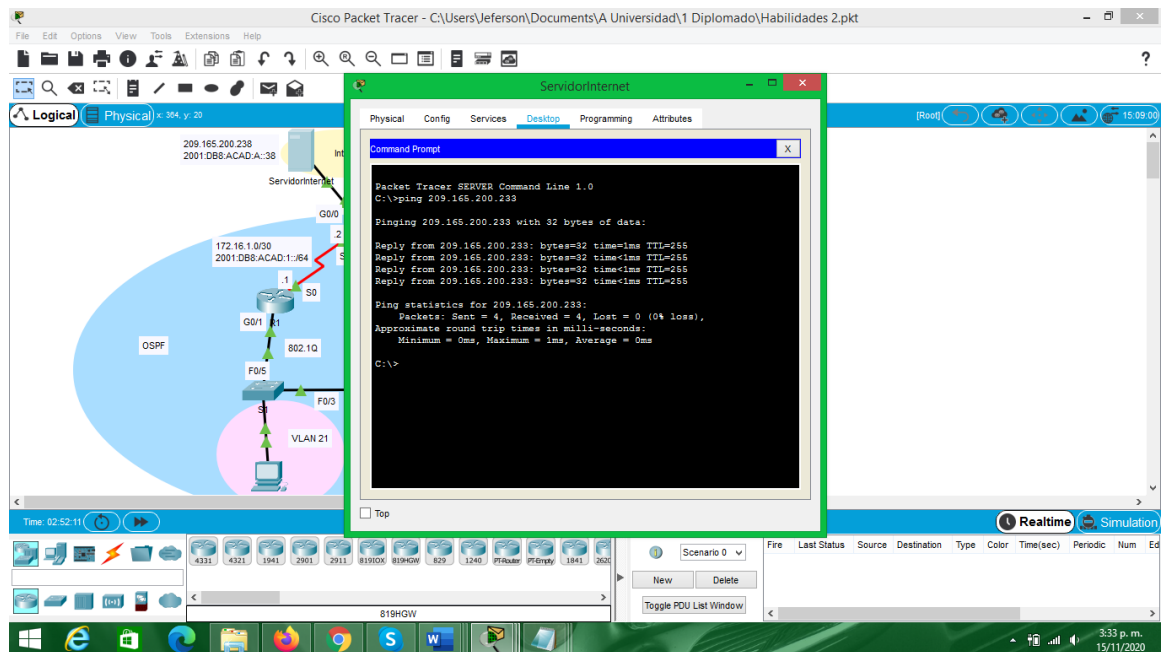
Figura 24. Ping de R2 a R3



Fuente: Autor

Se realiza ping desde R2 a R3 a la dirección IPv4 con éxito

Figura 25. Ping de PC de internet a gateway



Fuente: Autor

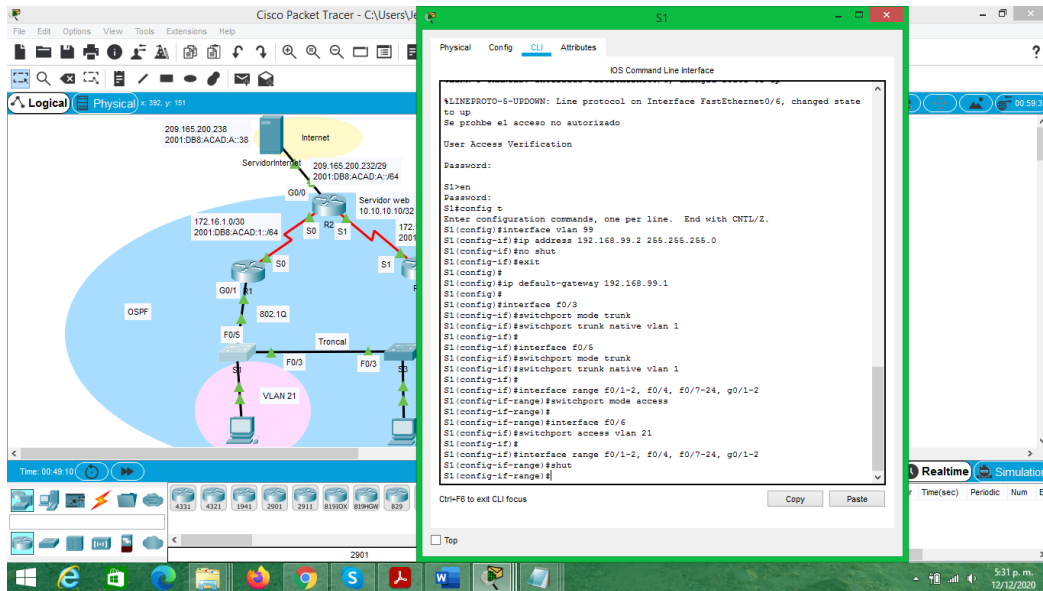
Se realiza ping desde PC de internet a gateway predeterminado

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Figura 26. Proceso de Configuración S1



Fuente: Autor

En esta imagen podemos evidenciar el desarrollo de la configuración mas importante en S1, donde se configurar la seguridad del switch, las VLAN y el routing entre VLAN, el proceso se ve mas detalladamente en la siguiente tabla

Tabla 21. Proceso de Configuración S1

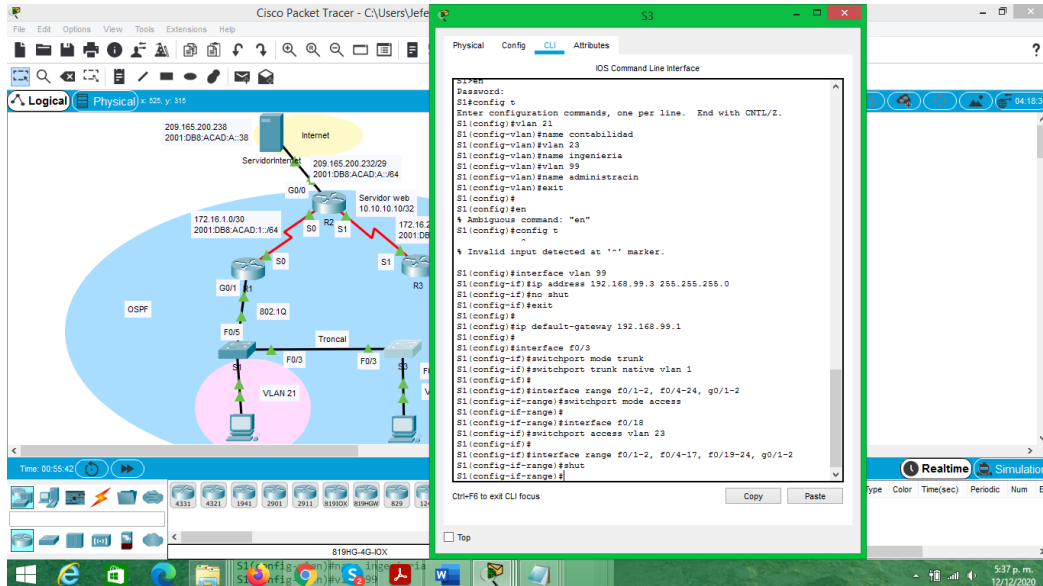
S1>en	ingreso a modo privilegiado
S1#config t	ingreso a modo de configuración
S1(config)#vlan 21	crea vlan 21
S1(config-vlan)#name contabilidad	dar nombre a la vlan creada
S1(config-vlan)#vlan 23	crea vlan 23
S1(config-vlan)#name ingenieria	dar nombre a la vlan creada
S1(config-vlan)#vlan 99	crea vlan 99
S1(config-vlan)#name administracin	dar nombre a la vlan creada

S1(config-vlan)#exit	salir
S1(config-if)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shut S1(config-if)#exit	configura interfase vlan 99 asigna dirección ipv4 a vlan 99 enciende la interface salir
S1(config)#ip default-gateway 192.168.99.1	configura puerta de enlace para ipv4
S1(config)#interface f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1	ingreso a interface crea el modo trocal en la interface crea el modo troncal en la interface para que utilice la vlan 1 como nativa
S1(config-if)#interface f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1	ingreso a interface crea el modo trocal en la interface crea el modo troncal en la interface para que utilice la vlan 1 como nativa
S1(config-if)#interface range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#switchport mode Access	ingresa al rango de interfaces señaladas y darles una configuración modifica en modo del puerto para acceso
S1(config-if-range)#interface f0/6 S1(config-if)#switchport access vlan 21	ingresa a la interface configura el acceso por el puerto a la vlan 21
S1(config-if)#interface range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shut S1(config-if-range)#exit S1#copy r st	ingresa al rango de interfaces seleccionadas para darles una configuración apaga la interface salir guarda la configuración realizada

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Figura 27. Proceso de Configuración S3



Fuente: Autor

En esta imagen podemos evidenciar el desarrollo de la configuración mas importante en S3, donde se configurar la seguridad del switch, las VLAN y el routing entre VLAN, el proceso se ve mas detalladamente en la siguiente tabla

Tabla 22. Proceso de Configuración S3

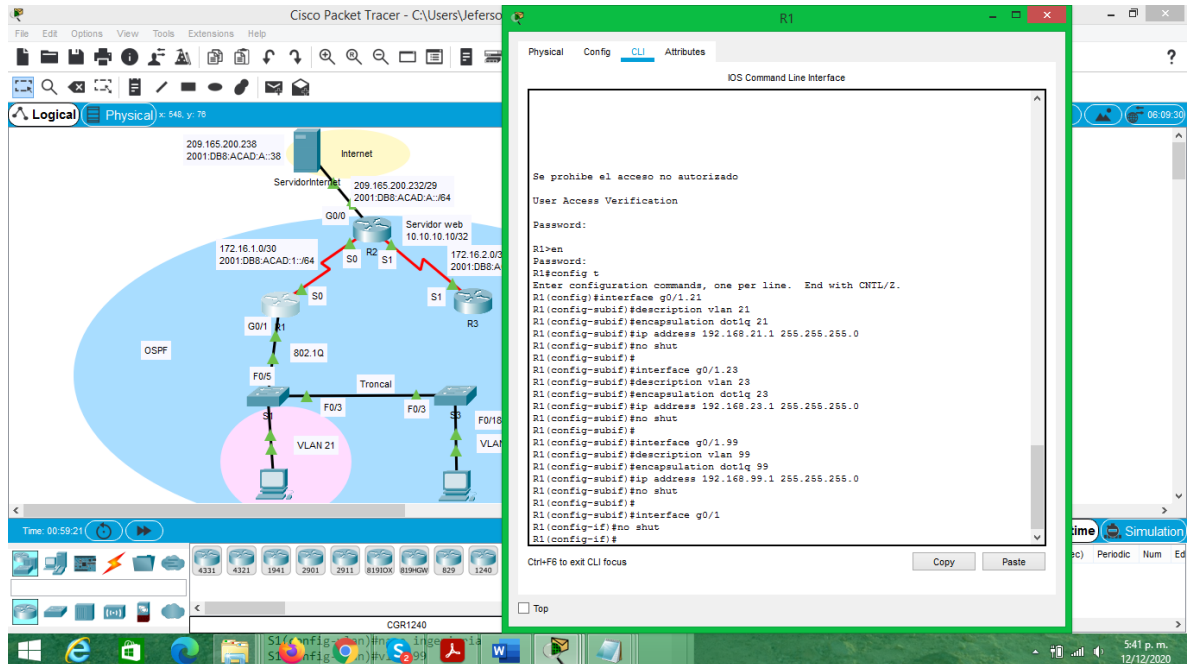
S3>en	ingreso a modo privilegiado
Password:	
S3#config t	ingreso a modo de configuración
S3(config)#vlan 21	crea vlan 21
S3(config-vlan)#name contabilidad	dar nombre a la vlan creada
S3(config-vlan)#vlan 23	crea vlan 23
S3(config-vlan)#name ingenieria	dar nombre a la vlan creada
S3(config-vlan)#vlan 99	crea vlan 99
S3(config-vlan)#name administracin	dar nombre a la vlan creada

S3(config-vlan)#exit	salir
S3(config-if)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shut S3(config-if)#exit	configura interfase vlan 99 asigna dirección ipv4 a vlan 99 enciende la interface salir
S3(config)#ip default-gateway 192.168.99.1	configura puerta de enlace para ipv4
S3(config)#interface f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1	ingreso a interface crea el modo trocal en la interface crea el modo troncal en la interface para que utilice la vlan 1 como nativa
S3(config-if)#interface range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode Access	ingresa al rango de interfaces seleccionadas para darles una configuración modifica en modo del puerto para acceso
S3(config-if-range)#interface f0/18 S3(config-if)#switchport access vlan 23	ingresa a la interface configura el acceso por el puerto a la vlan 23
S3(config-if)#interface range f0/1-2, f0/4-f0/17, f0/19-24 g0/1-2 S3(config-if-range)#shut S3(config-if-range)#exit S3(config)#exit S3#copy r st	ingresa al rango de interfaces seleccionadas para darles una configuración apaga la interface salir salir guarda la configuración realizada

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Figura 28. Proceso de Configuración R1



Fuente: Autor

En esta imagen podemos evidenciar el desarrollo de la configuración mas importante en R1, donde se configuran las subinterfaces para la Vlan 21, 23 y 99, el proceso se ve mas detalladamente en la siguiente tabla

Tabla 23. Proceso de Configuración R1

R1#en	ingreso a modo privilegiado
R1#config t	ingreso a modo de configuración
R1(config)#interface g0/1.21	configura subinterface
R1(config-subif)#description vlan 21	descripción o nombre de la vlan 21
R1(config-subif)#encapsulation dot1q 21	encapsula el tráfico de la subinterface

R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#no shut	asigna dirección ipv4 a subinterface de la vlan 21 enciende la interface
R1(config-subif)#interface g0/1.23 R1(config-subif)#description vlan 23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#no shut	configura subinterface descripción o nombre de la vlan 23 encapsula el tráfico de la subinterface asigna dirección ipv4 a subinterface de la vlan 23 enciende la interface
R1(config-subif)#interface g0/1.99 R1(config-subif)#description vlan 99 R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#no shut	configura subinterface descripción o nombre de la vlan 99 encapsula el tráfico de la subinterface asigna dirección ipv4 a subinterface de la vlan 99 enciende la interface
R1(config-subif)#interface g0/1 R1(config-if)#no shut	ingreso a interface enciende la interface

Paso 4: Verificar la conectividad de la red

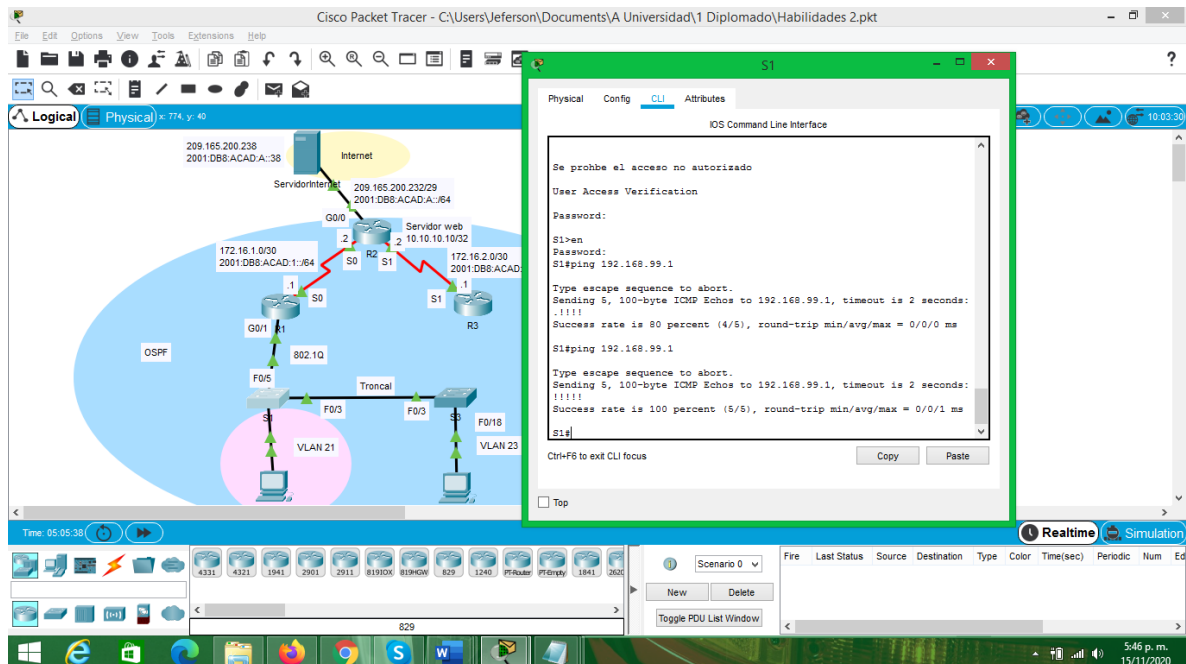
Utilice el comando ping para probar la conectividad entre los switches y el R1.

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

Tabla 24. Verificación de conectividad

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

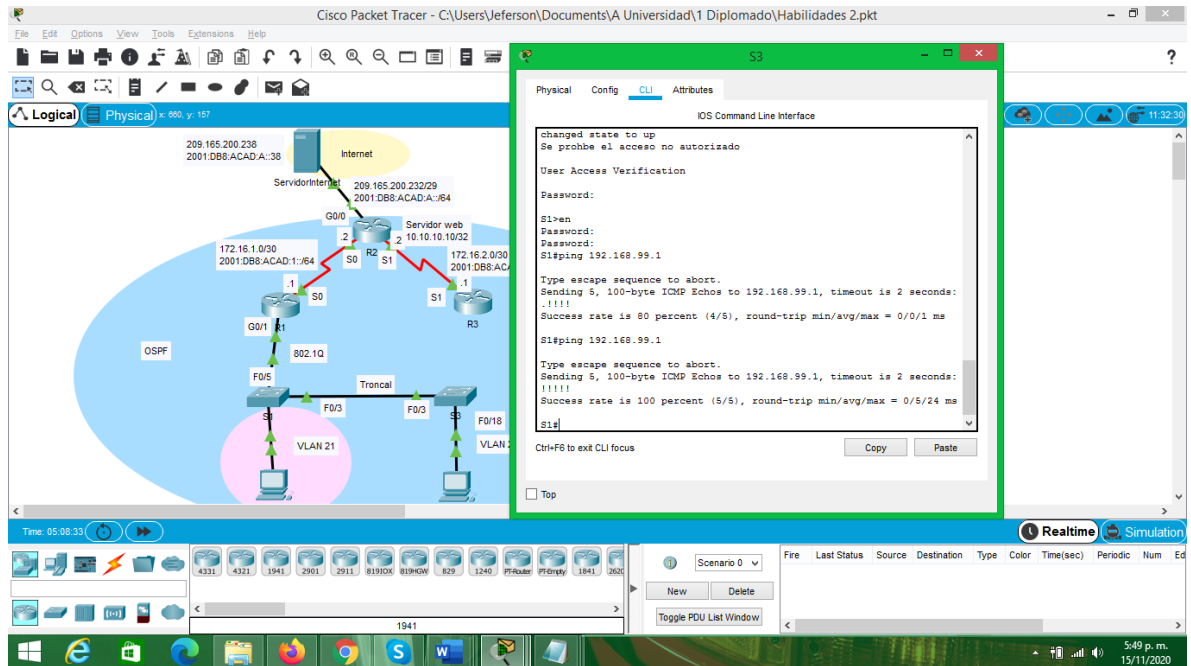
Figura 29. Ping S1 a VLAN 99 en R1



Fuente: Autor

Se realiza ping desde S1 a VLAN 99 en R1 con éxito

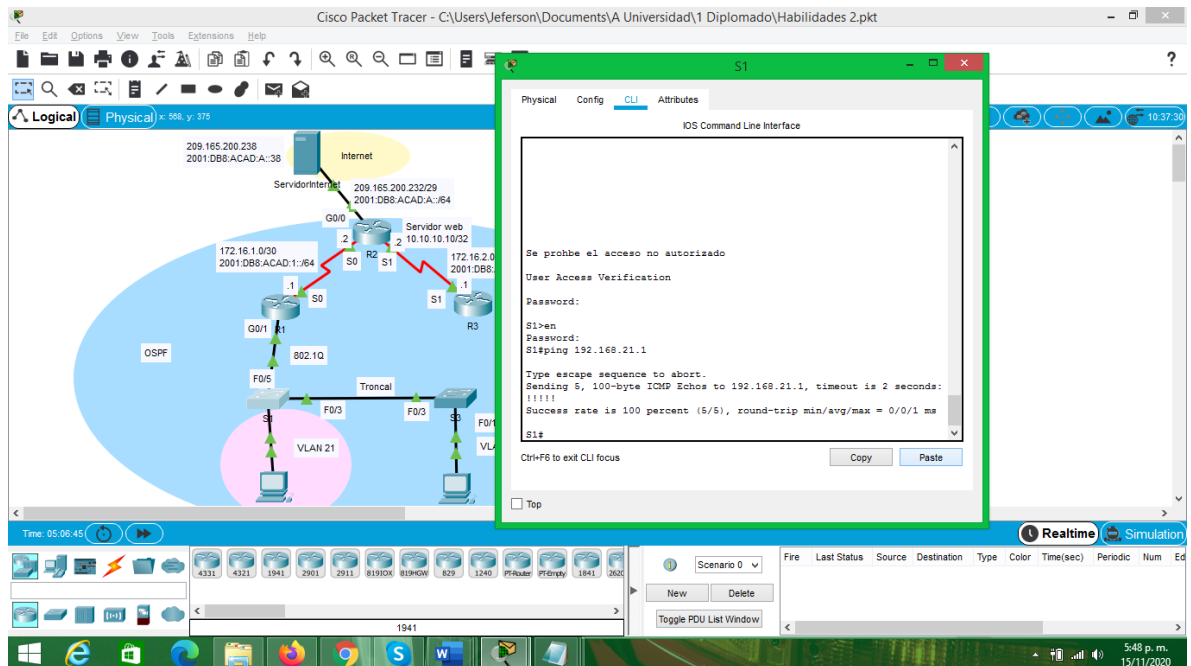
Figura 30. Ping S3 a VLAN 99 en R1



Fuente: Autor

Se realiza ping desde S3 a VLAN 99 en R1 con éxito

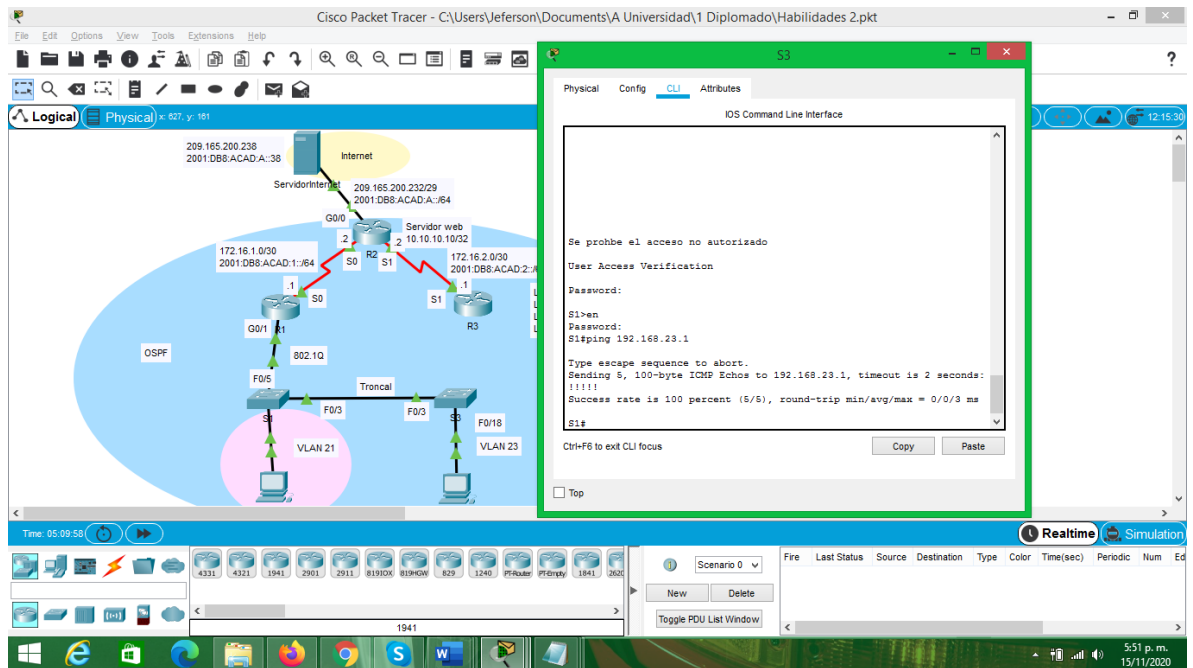
Figura 31. Ping S1 a VLAN 21 en R1



Fuente: Autor

Se realiza ping desde S1 a VLAN 21 en R1 con éxito

Figura 32. Ping S3 a VLAN 23 en R1



Fuente: Autor

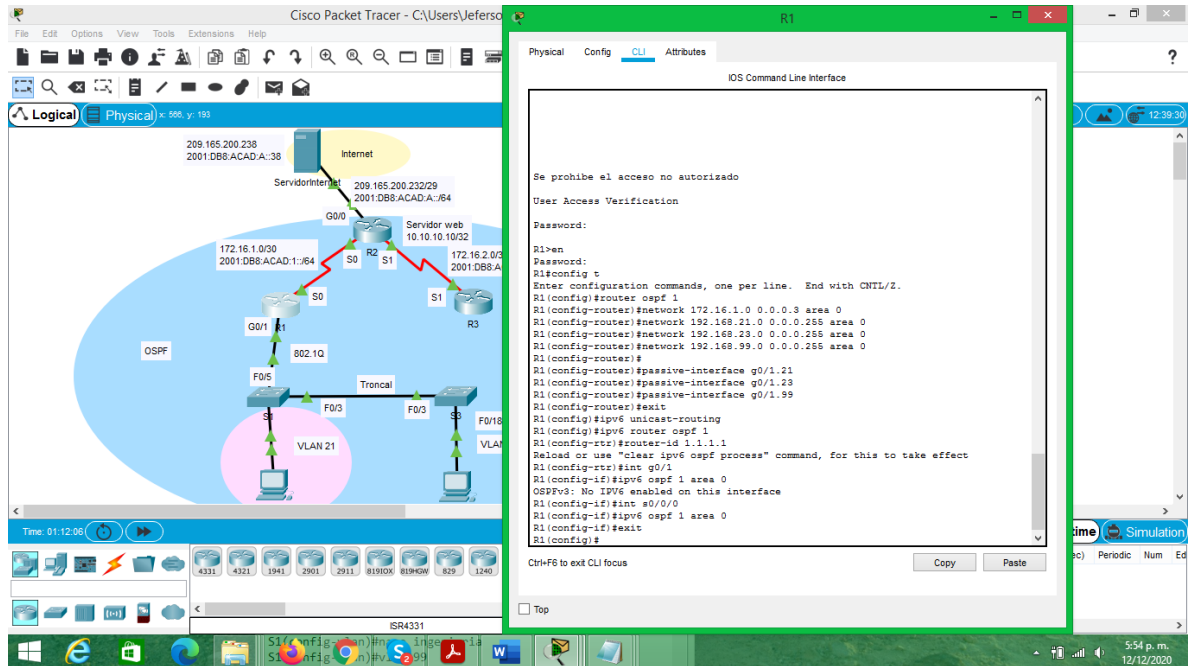
Se realiza ping desde S3 a VLAN 23 en R1 con éxito

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Figura 33. Proceso de Configuración OSPFv2 OSPFv3 R1



Fuente: Autor

En esta imagen podemos evidenciar el desarrollo de la configuración mas importante en R1, donde se Configura el protocolo de routing dinámico OSPFv2 y OSPFv3, el proceso se ve mas detalladamente en la siguiente tabla

Tabla 25. Proceso de Configuración OSPFv2 R1

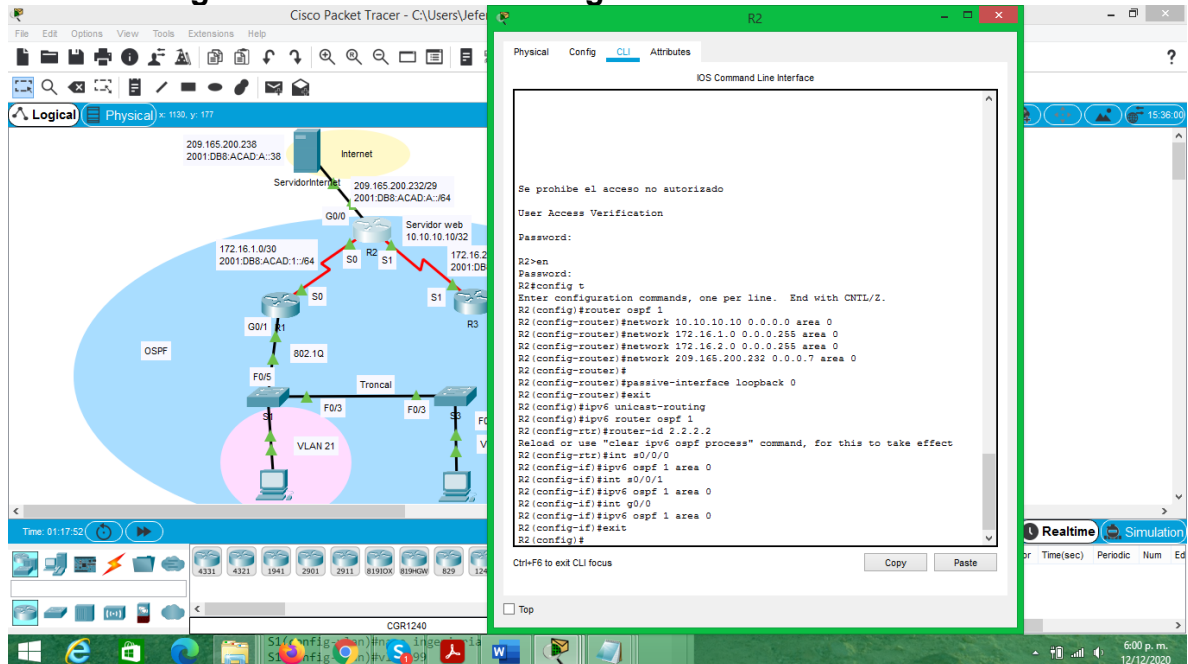
R1>en	ingreso a modo privilegiado
R1#config t	ingreso a modo de configuración
R1(config)#router ospf 1	ingresa al modo de configuración ospf

<pre>R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0 R1(config-router)#exit</pre>	<p>anuncia las redes directamente conectadas y configura el área 0</p> <p>anuncia las redes directamente conectadas y configura el área 0</p> <p>anuncia las redes directamente conectadas y configura el área 0</p> <p>anuncia las redes directamente conectadas y configura el área 0</p> <p>salir</p>
<pre>R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99 R1(config-router)#exit R1(config)#exit</pre>	<p>Establece como pasiva la interfaz LAN</p> <p>Establece como pasiva la interfaz LAN</p> <p>Establece como pasiva la interfaz LAN</p> <p>Salir</p> <p>Salir</p>
<pre>R1(config)#no auto-summary</pre>	<p>no lo admite el protocolo ospf</p>

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Figura 34. Proceso de Configuración OSPFv2 OSPFv3 R2



Fuente: Autor

En esta imagen podemos evidenciar el desarrollo de la configuración mas importante en R2, donde se Configura el protocolo de routing dinámico OSPFv2 y OSPFv3, el proceso se ve mas detalladamente en la siguiente tabla

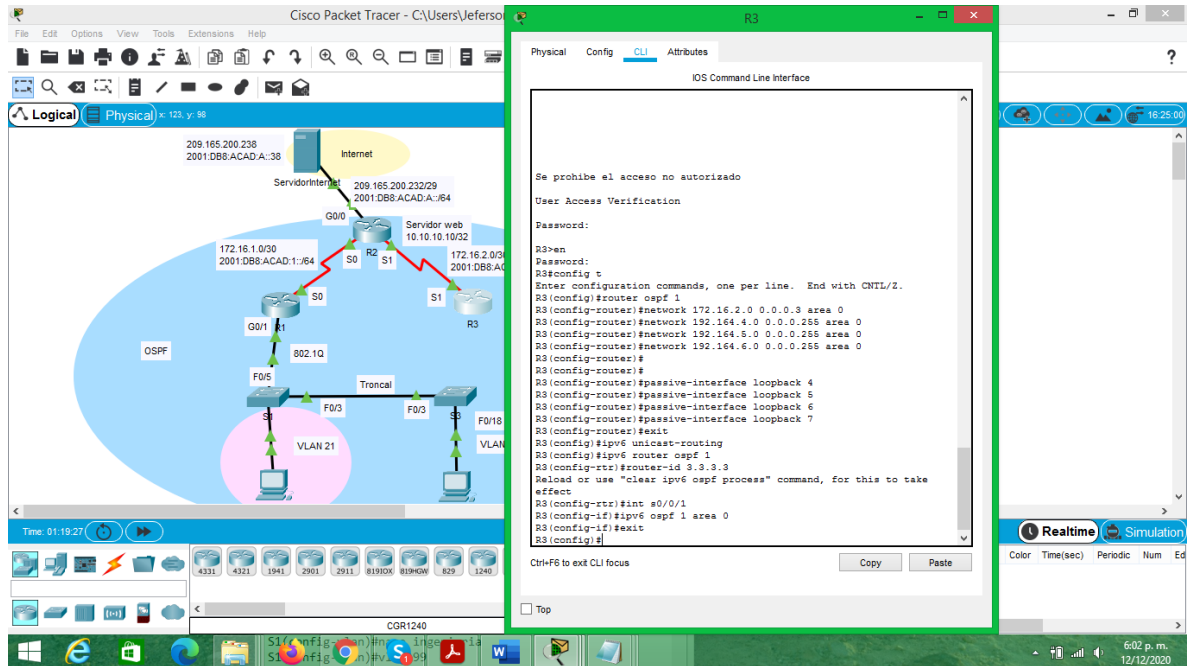
Tabla 26. Proceso de Configuración OSPFv2 R2

R2>en	ingreso a modo privilegiado
R2#config t	ingreso a modo de configuración
R2(config)#router ospf 1	ingresa al modo de configuración ospf
R2(config-router)# network 10.10.10.10 0.0.0.0 area 0	anuncia las redes directamente conectadas y configura el área 0
R2(config-router)# network 172.16.1.0 0.0.0.255 area 0	anuncia las redes directamente conectadas y configura el área 0
R2(config-router)# network 172.16.2.0 0.0.0.255 area 0	anuncia las redes directamente conectadas y configura el área 0
R2(config-router)#exit	salir
R2(config-router)# passive-interface loopback 0	Establece como pasiva la interfaz LAN
R2(config)#no auto-summary	no lo admite el protocolo ospf

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Figura 35. Proceso de Configuración OSPFv2 OSPFv3 R3



Fuente: Autor

En esta imagen podemos evidenciar el desarrollo de la configuración mas importante en R3, donde se Configura el protocolo de routing dinámico OSPFv2 y OSPFv3, el proceso se ve mas detalladamente en la siguiente tabla

Tabla 27. Proceso de Configuración OSPFv2 R3

R3>en	ingreso a modo privilegiado
R3#config t	ingreso a modo de configuración
R3(config)#router ospf 1	ingresa al modo de configuración ospf
R3(config-router)# network 172.16.2.0 0.0.0.3 area 0	anuncia las redes directamente conectadas y configura el área 0
R3(config-router)# network 192.164.4.0 0.0.0.255 area 0	anuncia las redes directamente conectadas y configura el área 0

R3(config-router)# network 192.164.5.0 0.0.0.255 area 0	anuncia las redes directamente conectadas y configura el área 0
R3(config-router)# network 192.164.6.0 0.0.0.255 area 0	anuncia las redes directamente conectadas y configura el área 0
R3(config-router)#exit	salir
R3(config-router)# passive-interface loopback 4	Establece como pasiva la interfaz LAN
R3(config-router)# passive-interface loopback 5	Establece como pasiva la interfaz LAN
R3(config-router)# passive-interface loopback 6	Establece como pasiva la interfaz LAN
R3(config-router)# passive-interface loopback 7	Establece como pasiva la interfaz LAN
R3(config)#no auto-summary	no lo admite el protocolo ospf

Tabla 28. Proceso de Configuración OSPFv3 R3

R3>en R3#config t Router(config)#int s0/0/1 Router(config-if)#ipv6 ospf 1 area 0 Router(config-if)#exit Router(config)#exit	ingreso a modo privilegiado ingreso a modo de configuración ingreso a interface ingresa al modo ospf ipv6 y crea área0 salir salir
R3>en R3#config t R3(config)#ipv6 unicast-routing R3(config)#ipv6 router ospf 1 Router(config-rtr)#router-id 3.3.3.3 Router(config-rtr)#exit Router(config)#exit	ingreso a modo privilegiado ingreso a modo de configuración activa interface ipv6 en el router ingresa al modo de configuración ospf ipv6 para para anunciar cada interface asigna la ID del router para ospfv3 salir salir
R3(config)#no auto-summary	no lo admite el protocolo ospf

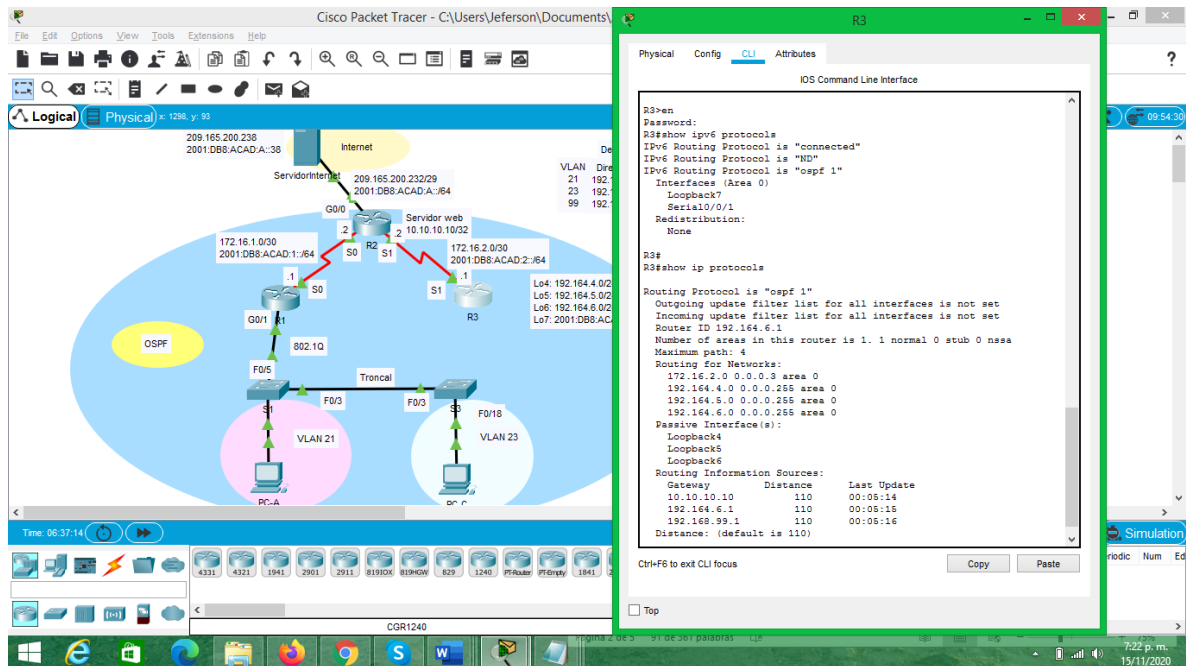
Paso 4: Verificar la información de OSPF

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

Tabla 29. Comandos para verificar 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?	show ipv6 protocols show ip protocols
¿Qué comando muestra solo las rutas OSPF?	show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R1#show run section route ospf R1#show run

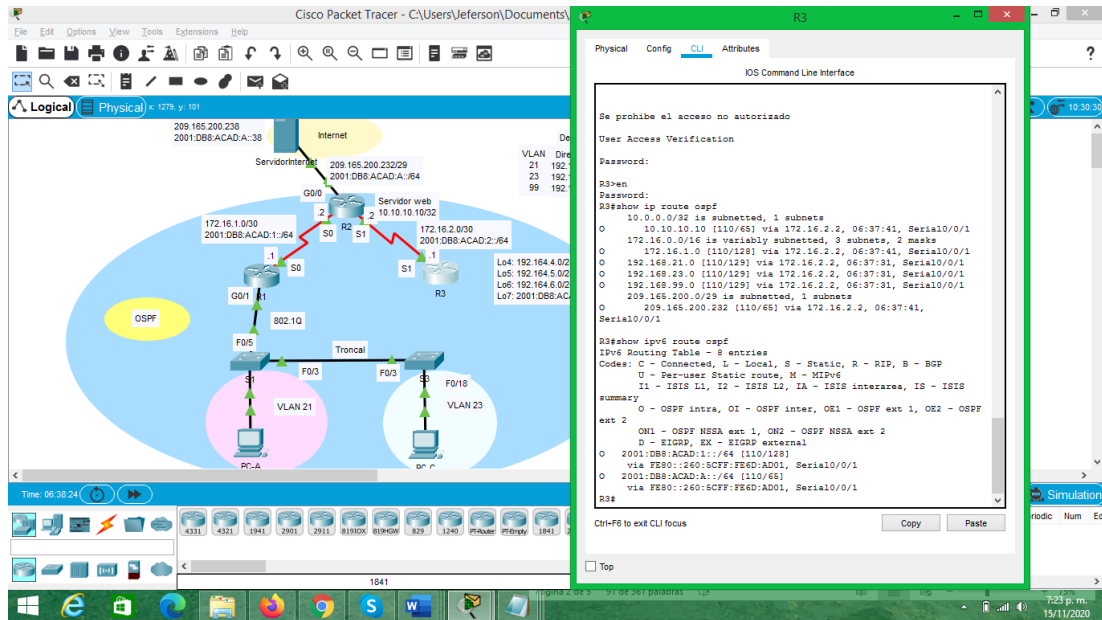
Figura 36. Comando show Ip protocols



Fuente: Autor

Con el comando show ip protocols se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en el router?

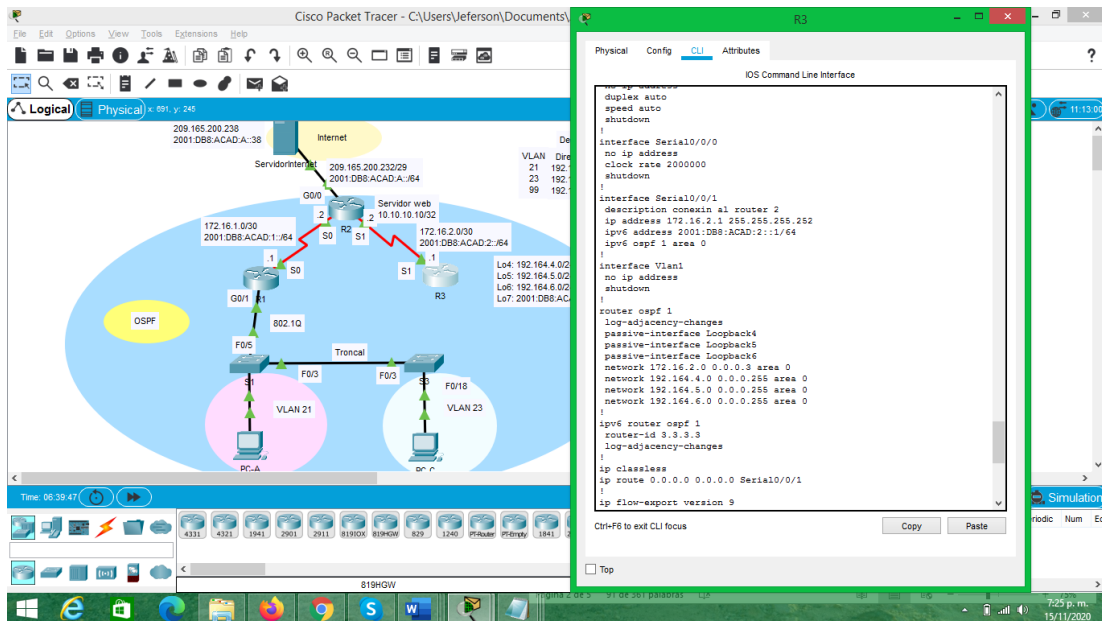
Figura 37. Comando show ip route ospf



Fuente: Autor

Con el comando show ip route ospf se muestra solo las rutas OSPF

Figura 38. Comando show run



Fuente: Autor

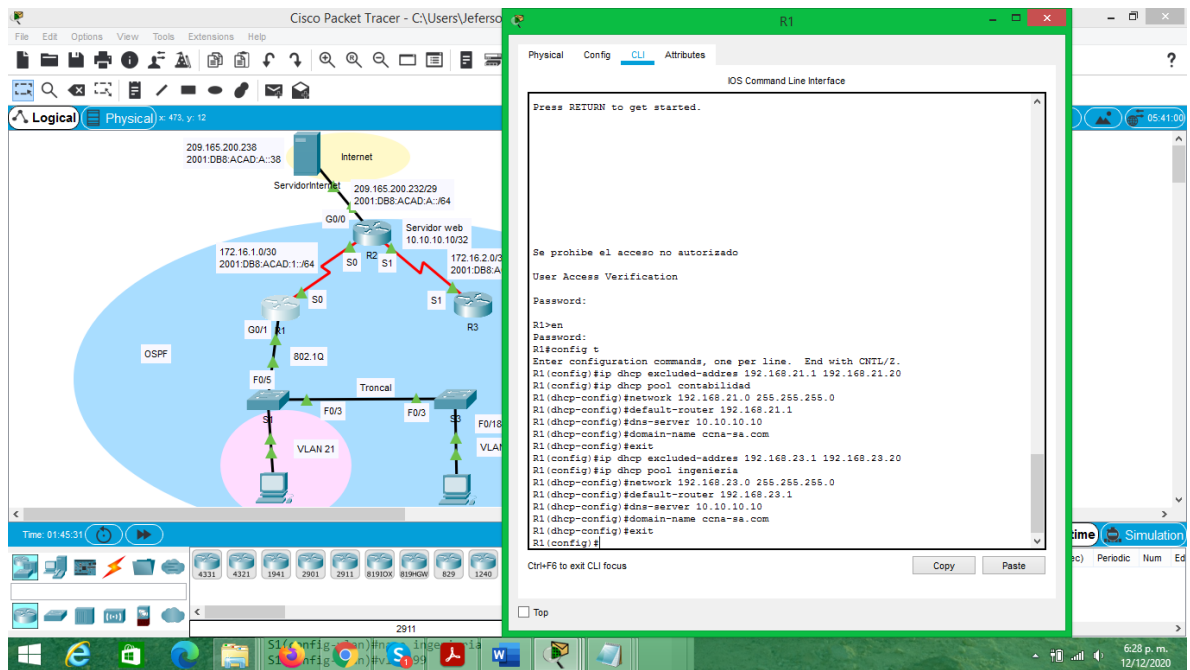
Con el comando show run | section route ospf se muestra la sección de OSPF de la configuración en ejecución, pero packet tracer no soporta el comando se debe utilizar el comando show run

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Figura 39. Proceso de configuración R1 como servidor de DHCP



Fuente: Autor

En esta imagen podemos evidenciar el desarrollo de la configuración mas importante en R1, donde se Configura el R1 como servidor de DHCP para las VLAN 21 y 23, el proceso se ve mas detalladamente en la siguiente tabla

Tabla 30. Proceso de configuración R1 como servidor de DHCP

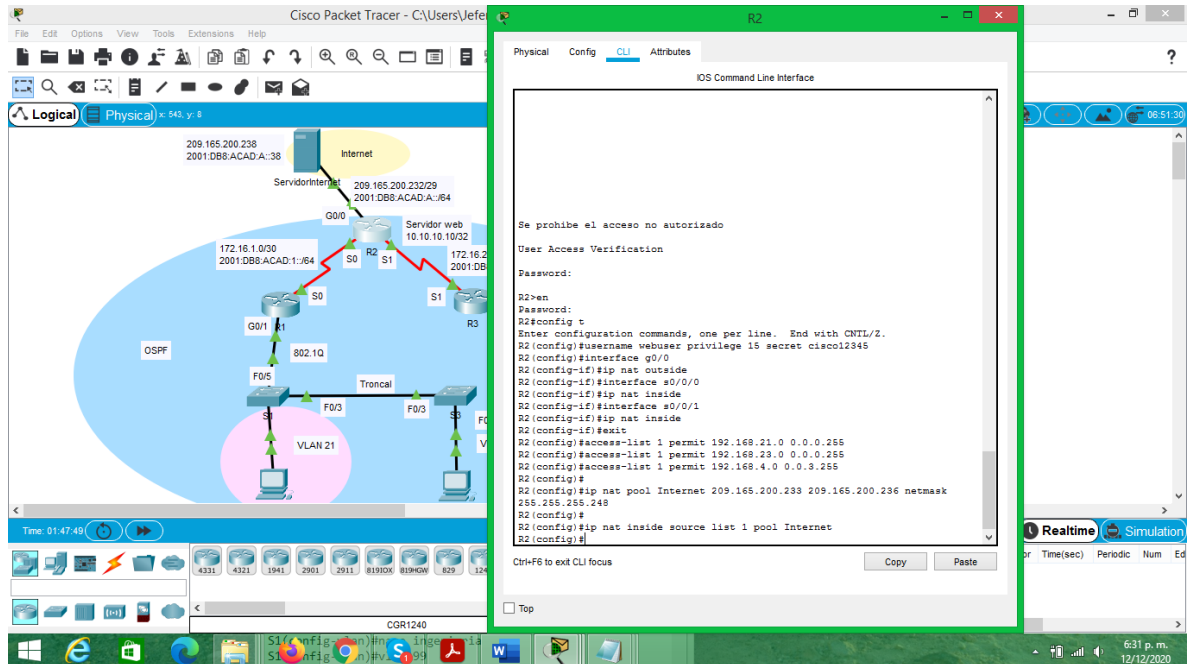
R1>en	ingreso a modo privilegiado
R1#config t	ingreso a modo de configuración
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20	reserva las primeras 20 direcciones ip
R1>en	ingreso a modo privilegiado

R1#config t R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20	ingreso a modo de configuración reserva las primeras 20 direcciones ip
R1(config)#ip dhcp pool contabilidad R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna- sa.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#exit R1(config)#exit	Crea dhcp para vlan 21 Asigna la red al dhcp pool Indica la ip del servidor Crea nombre del dominio Asigna la puerta de enlace Salir Salir
R1(config)#ip dhcp pool ingeniería R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna- sa.com R1(dhcp-config)#exit R1(config)#exit	Crea dhcp para vlan 23 Asigna la red al dhcp pool Indica la ip del servidor Crea nombre del dominio Asigna la puerta de enlace Salir Salir

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

La configuración del R2 incluye las siguientes tareas:

Figura 40. Proceso de configuración R2 con NAT estática y dinámica



Fuente: Autor

En esta imagen podemos evidenciar el desarrollo de la configuración mas importante en R1, donde se configurar la NAT estática y dinámica en el R2, el proceso se ve mas detalladamente en la siguiente tabla

Tabla 31. Proceso de configuración R2 con NAT estática y dinámica

R2>en	ingreso a modo privilegiado
R2#config t	ingreso a modo de configuración
R2(config)#username webuser privilege 15 secret cisco12345	crea la base de datos local con usuario y contraseña
R2(config)#ip http server	Habilita servicio HTTP, pero Packet Tracer no lo soporta

R2(config)#ip http authentication local	Configura el servidor HTTP, pero Packet Tracer no lo soporta
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237	Crea una NAT estática al servidor web
R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#interface s0/0/0 R2(config-if)#ip nat inside R2(config-if)#interface s0/0/1 R2(config-if)#ip nat inside R2(config-if)#exit	Ingresa a la interface Asigna la interface externa para la NAT Ingresa a la interface Asigna la interface interna para la NAT Ingresa a la interface Asigna la interface interna para la NAT salir
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255	Configura lista de acceso que permite la traducción de las redes asignadas Configura lista de acceso que permite la traducción de las redes asignadas Configura lista de acceso que permite la traducción de un resumen de las redes LAN (loopback) de R3
R2(config)#ip nat pool Internet 209.165.200.233 209.165.200.236 netmask 255.255.255.248	Define el pool de direcciones publicas utilizables
R2(config)#ip nat inside source list 1 pool Internet R2(config)#	Define la traducción de la NAT dinámica

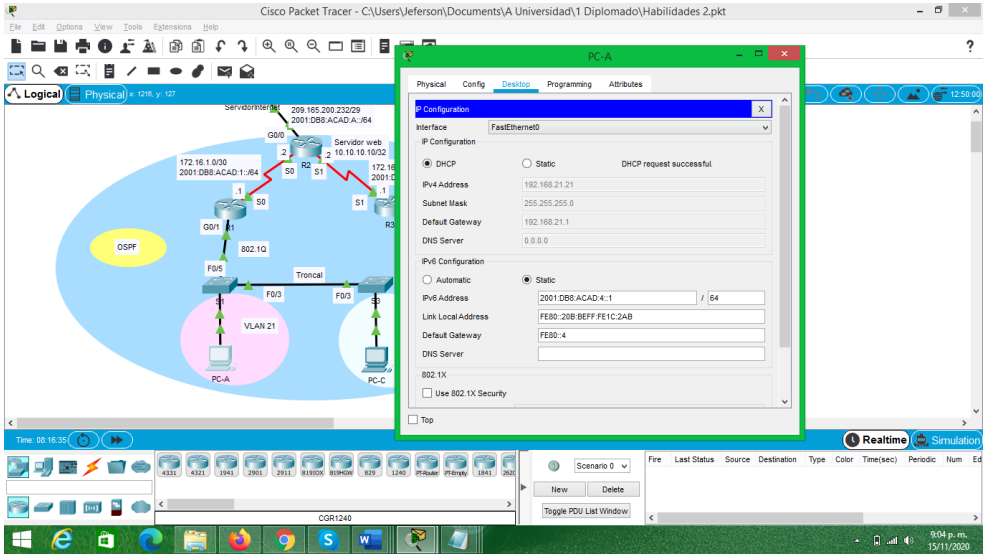
Paso 3: Verificar el protocolo DHCP y la NAT estática

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 32. Verificación de protocolo DHCP y NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Ok
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Ok
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Ok
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	Packet Tracer no soporta el servidor web

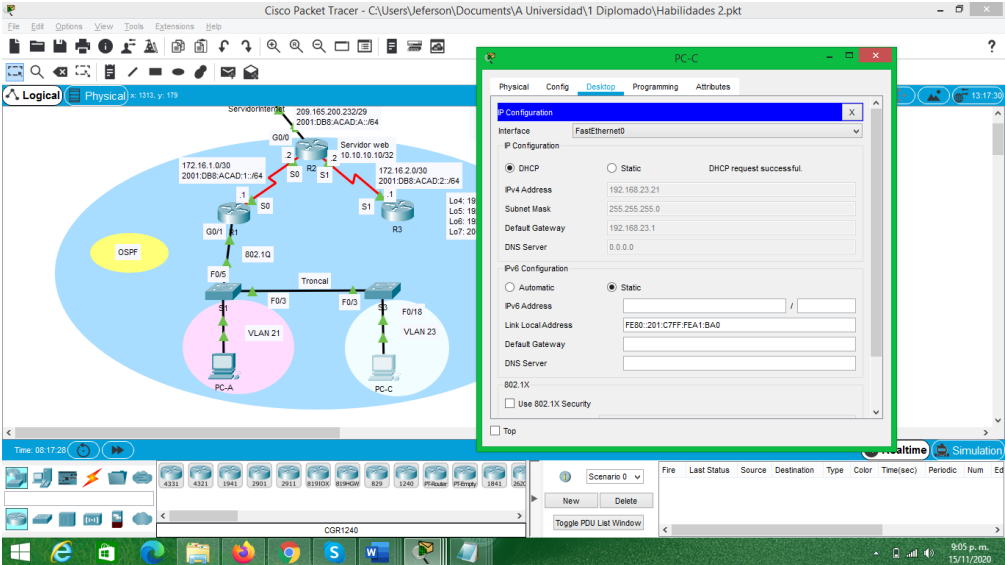
Figura 41. Verificar que la PC-A haya adquirido información de IP del servidor de DHCP



Fuente: Autor

Se verifica que el router este entregando dirección por DHCP al PC-A

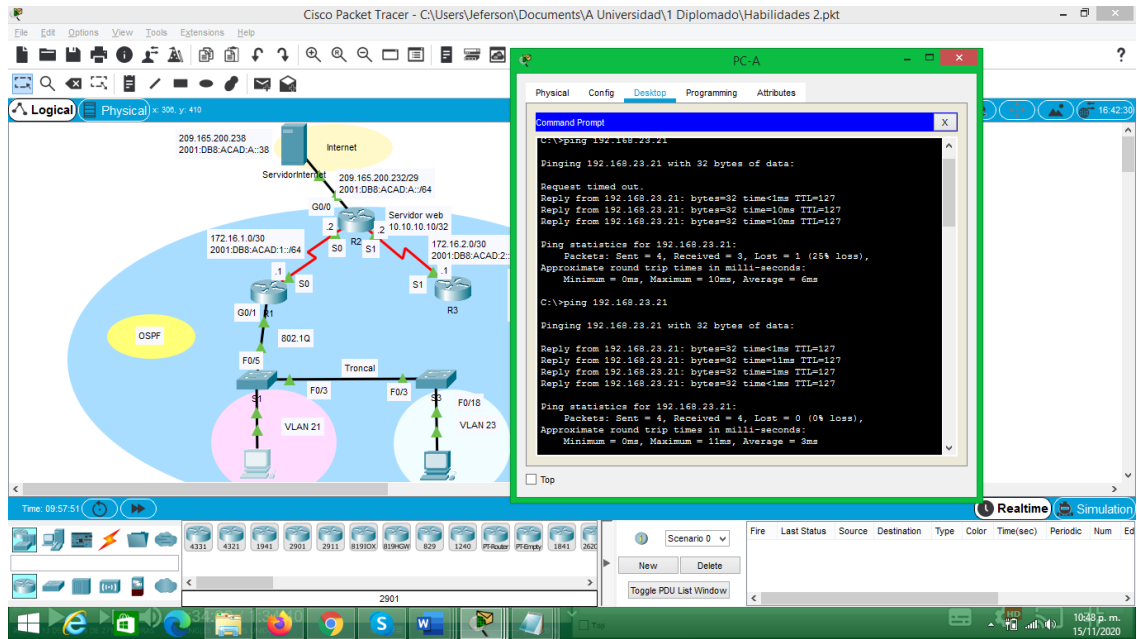
Figura 42. Verificar que la PC-C haya adquirido información de IP del servidor de DHCP



Fuente: Autor

Se verifica que el router este entregando dirección por DHCP al PC-C

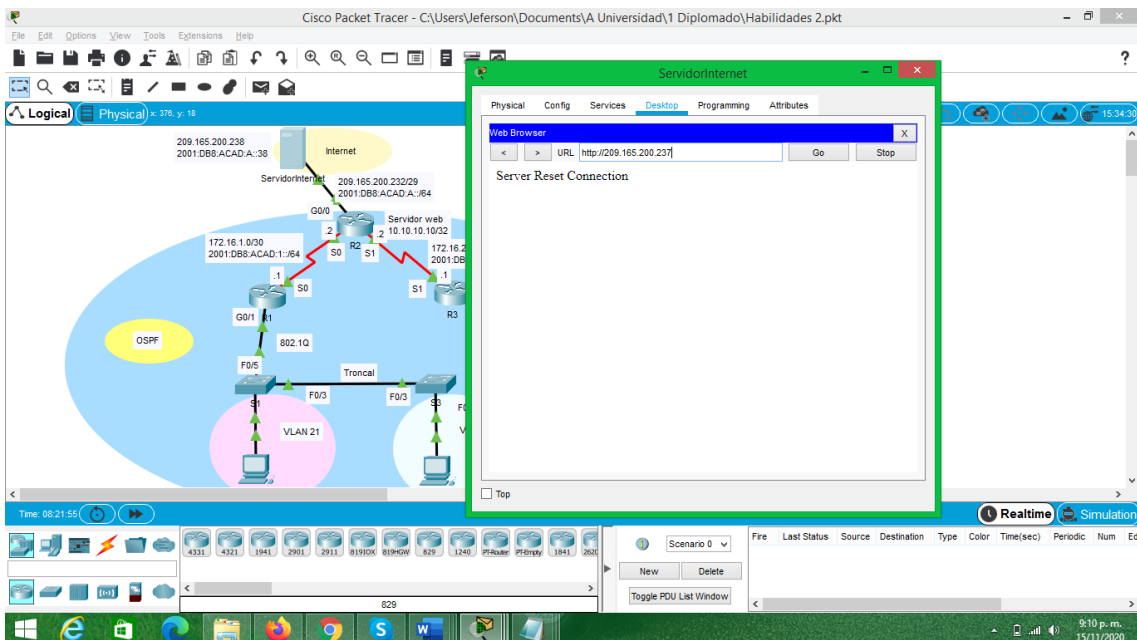
Figura 43. Verificar que la PC-A pueda hacer ping a la PC-C



Fuente: Autor

Se realiza ping de PC-A a PC-C para verificar que tengan comunicación

Figura 44. Servicio web desde computadora de internet



Fuente: Autor

Se verifica el acceso al servidor web (209.165.200.237), el cual resulta fallido dado que packet tracer no soporta los comandos de configuración para el servidor web

Parte 6: Configurar NTP

Tabla 33. Configuración NTP en R1 y R2

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	5 de marzo de 2016, 9 a. m.
Configure R2 como un maestro NTP.	Nivel de estrato: 5
Configurar R1 como un cliente NTP.	Servidor: R2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	Actualiza calendario R1
Verifique la configuración de NTP en R1.	R1 ntp

Tabla 34. Proceso de configuración NTP en R1 y R2

R2>en R2#clock set 19:10:00 14 noviembre 2020	ingreso a modo de configuración se ajusta hora y fecha
R2#config t R2(config)# ntp master 5	ingreso a modo de configuración no soporta packet tracer
R1>en Password: R1#config t R1(config)#ntp server 172.16.1.2	ingreso a modo privilegiado ingreso a modo de configuración configura cliente servidor NTP
R1(config)#ntp update-calendar	Actualiza calendario con hora NTP
R1#show ntp associations	Packet Tracer no soporta el comando, pero debe mostrar la conexión al servidor NTP en R2

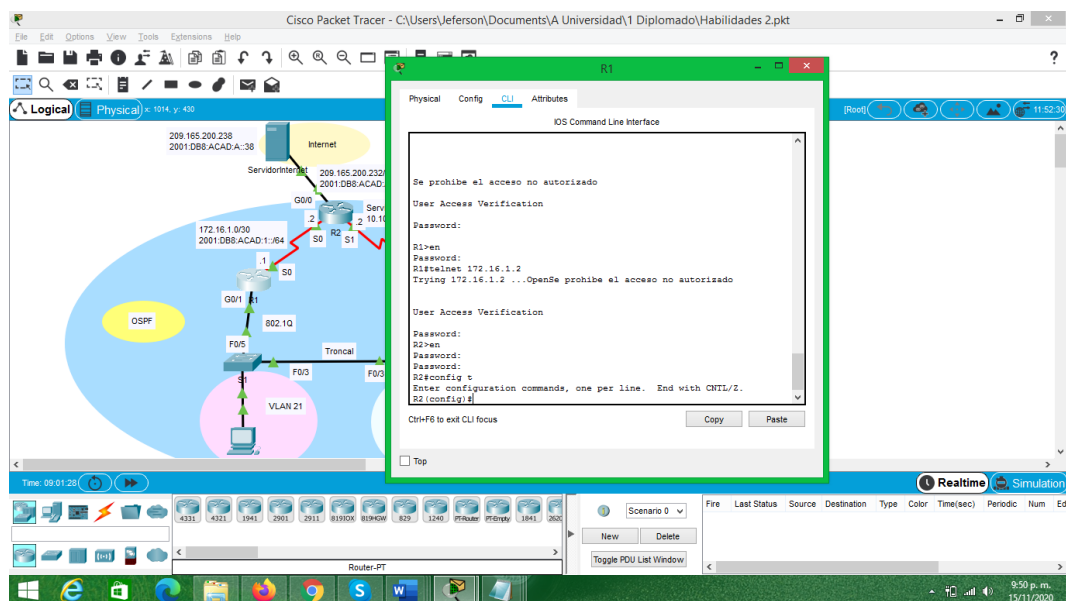
Parte 7: Configurar y verificar las listas de control de acceso (ACL)

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

Tabla 35. Proceso de configuración acceso líneas VTY en R2

<pre>R2>en R2#config t R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit</pre>	<p>ingreso a modo privilegiado ingreso a modo de configuración configura lista de acceso</p> <p>permite conexión telnet solo al host mencionado salir</p>
<pre>R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MTG in</pre>	<p>ingreso a configuración de telnet asigna nombre a líneas vty</p>
<pre>R2(config-line)#transport input telnet R2(config-line)#exit</pre>	<p>Permite acceso por telnet a líneas vty</p>
<p>Verificar que la ACL funcione como se espera</p>	<p>En los pantallazos a continuación, se verifica el funcionamiento</p>

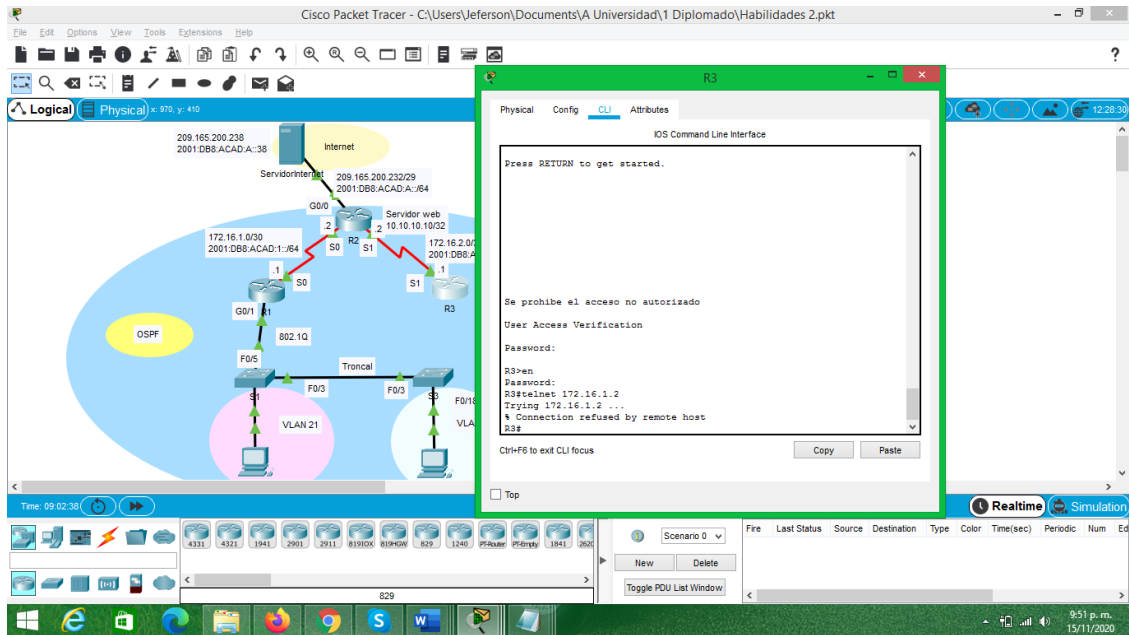
Figura 45. Acceso telnet a R2 desde R1



Fuente: Autor

Se verifica que R1 pueda conectar por telnet a R2, dando una conexión exitosa

Figura 46. Acceso telnet desde R3 a R2



Fuente: Autor

Se verifica que R3 pueda conectar por telnet a R2, dando una conexión fallida teniendo en cuenta que solo se configure para que R1 tuviera acceso

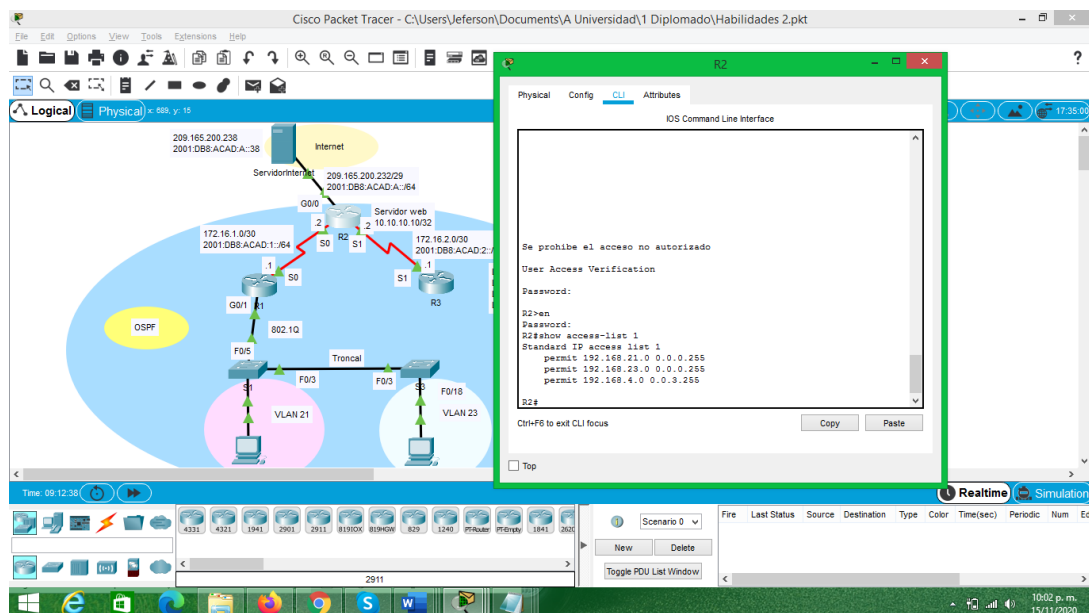
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 36. Comandos CLI

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2 Show access-list 1
Restablecer los contadores de una lista de acceso	Clear ip access-list counters no soporta
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	show ip interface

<p>¿Con qué comando se muestran las traducciones NAT?</p>	<p>Show ip nat translations</p> <p>Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.</p> <p>Se realiza ping a 209.165.200.233</p>
<p>¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?</p>	<p>clear ip nat translation *</p>

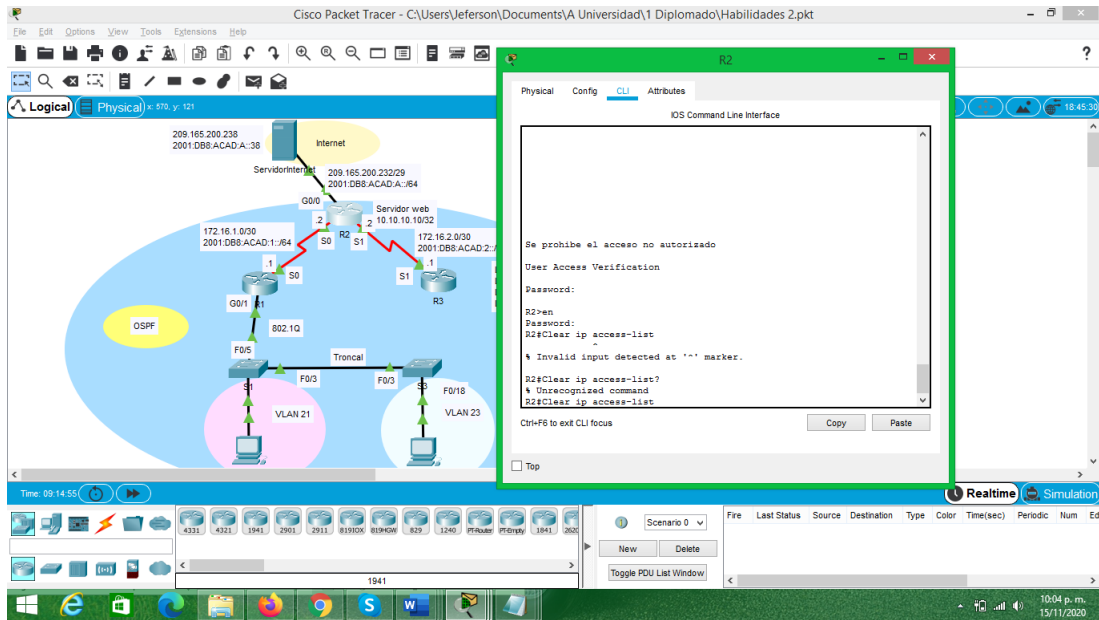
Figura 47. Comando Show access-list 1



Fuente: Autor

Se utiliza el comando CLI Show access-list 1 para mostrar coincidencias recibidas por lista de acceso desde la última vez que se restableció.

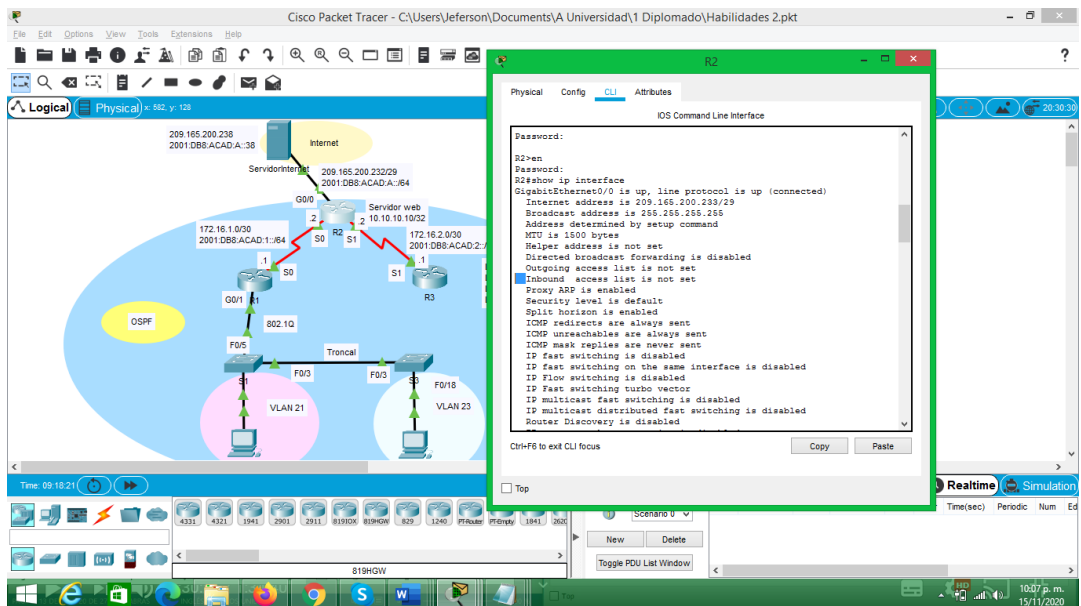
Figura 48. Comando clear ip access-list counters



Fuente: Autor

Con el comando clear ip access-list counters se puede restablecer los contadores de una lista de acceso, esto en equipos reales por que packet tracer no lo soporta

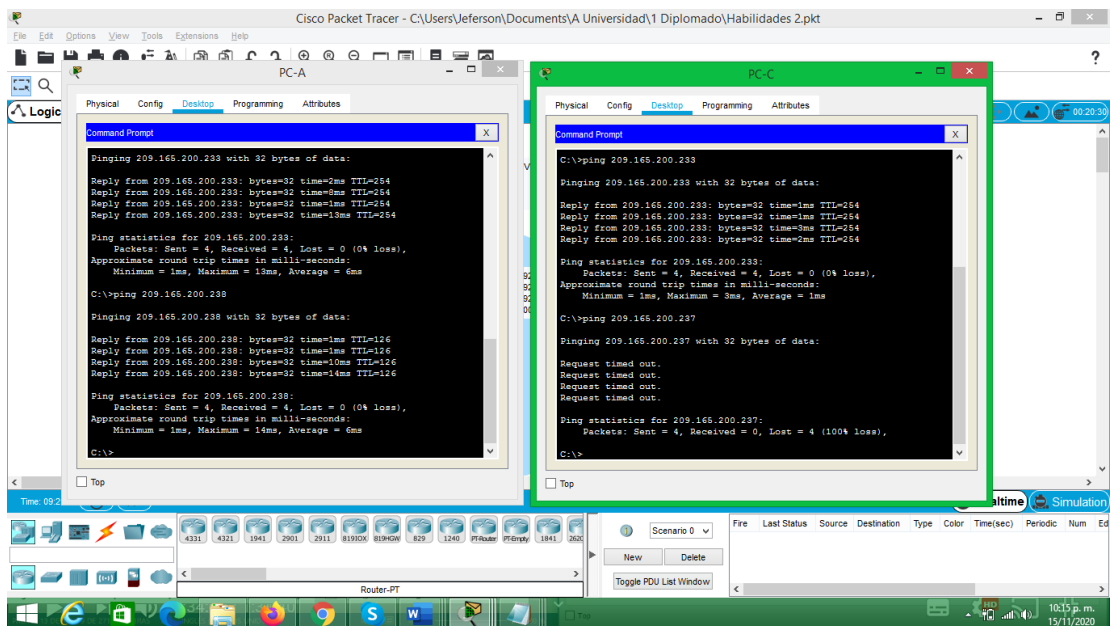
Figura 49. Comando show ip interface



Fuente: Autor

Con el comando show ip interface se muestra qué ACL se aplica a una interfaz y la dirección en que se aplica

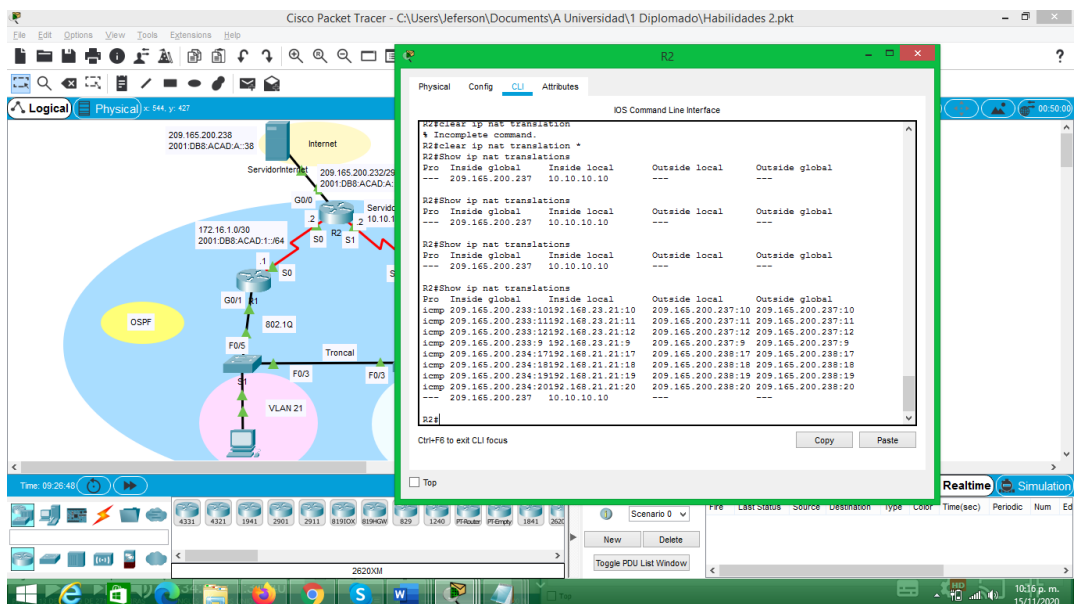
Figura 50. ping PC-A y PC-C para traducción NAT



Fuente: Autor

Se realiza Ping PC-A y PC-C para poder aplicar el comando show ip nat translations y se muestre las traducciones NAT

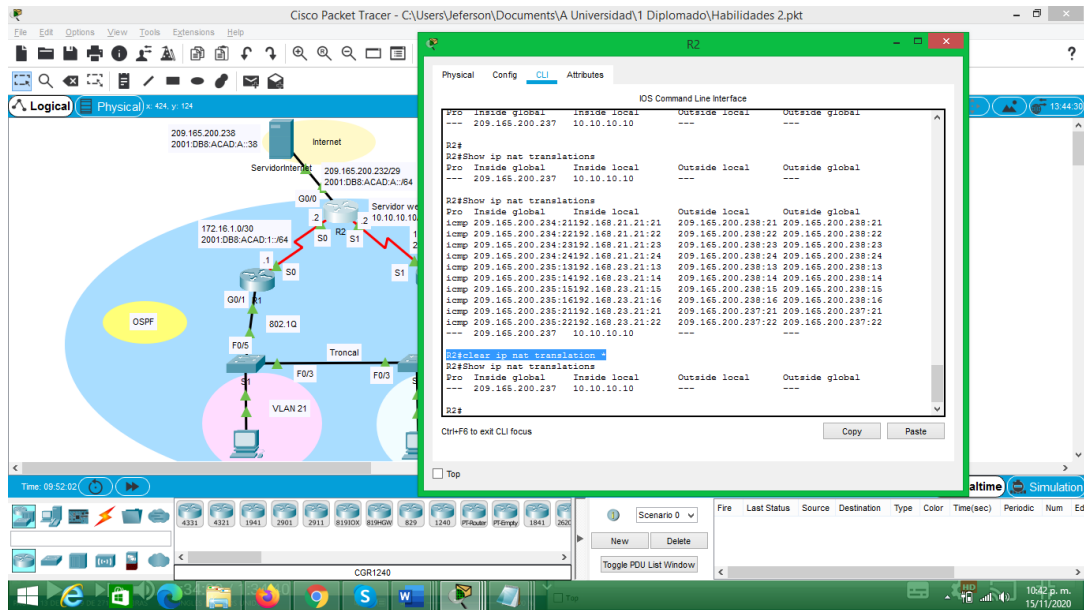
Figura 51. Comando Show ip nat translations



Fuente: Autor

Se utiliza el comando Show ip nat translations para que se muestre las traducciones NAT

Figura 52. Comando clear ip nat translation *



Fuente: Autor

Se utiliza el comando clear ip nat translations para eliminar los registros de las traducciones NAT

CONCLUSIONES

Como resultado del desarrollo de este trabajo obtuvimos la configuración exitosa de los dos escenarios los cuales cuentan con los estándares establecidos por la academia CISCO, donde se realizó los enrutamientos necesarios y configuraciones de red, que nos permitieron tener una comunicación fluida en nuestra red, por medio del uso y configuración de las subredes y sus respectivas Vlan.

También se realizó de forma adecuada las configuraciones necesarias en los diferentes equipos utilizados para mitigar los ataques malintencionados o la manipulación inadecuada de personal inexperto o de terceros.

En conclusión, general aprendimos la importancia que representa la configuración adecuada de una red, tanto en su parte de seguridad física como lógica, ya que en la parte física se deben deshabilitar los puertos que no se encuentren en actividad para mitigar de un posible robo de información o sabotaje a nuestra red lógica.

Para poder lograr la configuración exitosa de la red del escenario 1 se tuvo que hacer uso de swich capa 3 o multicapa, dado que estos soportan la interacción entre los protocolos Ipv4 e Ipv6, ya que el swich capa 3 es capas de ejecutar enrutamiento estático y enrutamiento dinámico considerando las direcciones ip tanto IPv6 como IPv4.

Para el desarrollo exitoso del escenario 2 se utilizo como parte de su configuración el protocolo de enrutamiento OSPF, el cual es de fuente abierta o (open source), que nos brinda la opción de poderlo utilizar en equipos que no sean de la marca cisco, este protocolo nos da la opción de configurar tanto su versión para IPv4 como la versión para IPv6.

BIBLIOGRAFIA

RAMIREZ, C. D. E. (19/09/2020). Obtenido de Cipas.

RAMIREZ, C. D. E. (24/09/2020). Obtenido de Cipas.

RAMIREZ, C. D. E. (06/10/2020). Obtenido de Cipas.

SALAZAR, P. (08/10/2020). Obtenido de Cipas

SALAZAR, P. (16/10/2020). Obtenido de Cipas

SALAZAR, P. (19/10/2020). Obtenido de Cipas

ANEXOS

ANEXO 1

Archivos PKT

https://unadvirtualedu-my.sharepoint.com/:f:/g/personal/ajmaciasb_unadvirtual_edu_co/EhXr93qH8hhAhiA2nGqx09QBmaG1z-7UYGoXCRaSGMy49g?e=9ctXLj

ANEXO 2

Articulo

https://unadvirtualedu-my.sharepoint.com/:f:/g/personal/ajmaciasb_unadvirtual_edu_co/EmcqhnN9n-5Ok-1nx6eTJgcB5MjINJg7CcD7D2-GWRCR6g?e=0zVtgd