

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

**PRESENTADO POR:
YOHAN SEBASTIAN FORERO ZABALA**

**TUTOR:
DIEGO EDINSON RAMIREZ**

**UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERIA
INGENIERIA DE SISTEMAS
FACATATIVÁ
2020**

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

**PRESENTADO POR:
YOHAN SEBASTIAN FORERO ZABALA**

**Trabajo de grado bajo la opción de diplomado
presentado como requisito para obtener el título de ingeniero de sistemas.**

**TUTOR:
DIEGO EDINSON RAMIREZ**

**UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERIA
INGENIERIA DE SISTEMAS
FACATATIVÁ
2020**

Nota de aceptación

Presidente del jurado

Jurado

Jurado

Facatativá, ___ de ___ del año _____

AGRADECIMIENTOS

En primer lugar, quiero agradecer a mi familia y amigos que me apoyó a lo largo de mi proceso académico, a cada uno de los docentes que me brindaron su ayuda en mi formación profesional, a mi director Diego Fernando Medina quien me brindo acompañamiento en mis inicios en la universidad, a mi alma mater por aceptarme dentro de su campus para obtener mi título profesional.

TABLA DE CONTENIDO

1. INTRODUCCIÓN	13
2. OBJETIVOS	14
2.1 OBJETIVOS GENERALES.....	14
2.2 OBJETIVOS ESPECIFICOS.....	14
3. DESARROLLO.....	15
DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES.....	15
ESCENARIO 1	15
1. Instrucciones	17
Parte 1: Inicializar y Recargar y Configurar aspectos básicos de los dispositivos	17
Paso 1. Inicializar y volver a cargar el router y el switch	17
Paso 2: Configurar R1	18
Paso 3: Configure S1 y S2.	21
Parte 2: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel).....	24
Paso 1: Configurar S1	24
Paso 2. Configure el S2.....	27
Parte 3. Configurar soporte de host.....	29
Paso 1. Configure R1	29
Paso 2. Configurar los servidores.....	31
Parte 4. Probar y verificar la conectividad de extremo a extremo.....	35
ESCENARIO 2	44
1. Instrucciones	45
Parte 1: inicializar dispositivos	45
Paso 1: Inicializar y volver a cargar los routers y los switches	45
Parte 2: Configurar los parámetros básicos de los dispositivos.....	45
Paso 1: Configurar la computadora de Internet	45
Paso 2: Configurar R1	47
Paso 3: configurar R2.....	49
Paso 4: configurar R3.....	52

Paso 5: Configurar S1	54
Paso 6: Configurar S3:	56
Paso 7: Verificar la conectividad de la red.....	57
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN	60
Paso 1: Configurar S1	60
Paso 2: Configurar el S3.....	62
Paso 3: Configurar R1	63
Paso 4: Verificar la conectividad de la red.....	65
Parte 4: Configurar el protocolo de routing dinámico OSPF	68
Paso 1: Configurar OSPF en el R1	68
Paso 2: Configurar OSPF en el R2.....	69
Paso 3: Configurar OSPFv3 en el R2.....	70
Paso 4: Verificar la información de OSPF	71
Parte 5: Implementar DHCP y NAT para IPv4	73
Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23	73
Paso 2: Configurar la NAT estática y dinámica en el R2	74
Paso 3: Verificar el protocolo DHCP y la NAT estática.....	76
Parte 6: Configurar NTP	79
Parte 7: Configurar y verificar las listas de control de acceso (ACL)	81
Paso 1: Restringir el acceso a las líneas VTY en el R2.....	81
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente	83
4. CONCLUSIONES.....	87
5. BIBLIOGRAFÍA	88
ANEXOS.....	89

LISTA DE FIGURAS

Figura 1. Topología del Primer Escenario.....	15
Figura 2. Evidencia de Paso 1: Inicializar y volver a cargar el router.....	18
Figura 3. Ejecución comando Show run R1	21
Figura 4. Ejecución comando show run S1.....	23
Figura 5. Ejecución comando show run S1.....	24
Figura 6. Ejecución comando show vlan en S1	26
Figura 7. Ejecución comando Show vlan en S2.....	29
Figura 8. Evidencia configuración DHCP en R1	31
Figura 9. Evidencia de configuración IPV4 tomada automáticamente por DHCP e IPV6 asignada manualmente en PC-A.	32
Figura 10. Ejecución del comando ipconfig /all en PC-A que muestra la toda la configuración IP del ordenador	33
Figura 11. Evidencia de configuración IPV4 tomada automáticamente por DHCP e IPV6 asignada manualmente en PC-B	34
Figura 12. Ejecución del comando ipconfig /all en PC-B que muestra la toda la configuración IP del ordenador.	34
Figura 13. Ping desde PCA a R1, G0/0/1.2 en IPV4 e IPV6	37
Figura 14. Ping desde PCA a R1, G0/0/1.3 en IPV4 e IPV6	37
Figura 15. Ping desde PCA a R1, G0/0/1.4 en IPV4 e IPV6	38
Figura 16. Ping desde PCA a S1, VLAN4 en IPV4 e IPV6	38
Figura 17. Ping desde PCA a S2, VLAN4 en IPV4 e IPV6	39
Figura 18. Ping desde PC-A a PC-B en IPV4.....	39
Figura 19. Ping desde PC-A a R1 Bucle 0 en IPV4 e IPV6	40
Figura 20. Ping desde PC-B a R1 Bucle 0 en IPV4 e IPV6	40
Figura 21. Ping desde PC-B a R1, G0/0/1.2 en IPV4 e IPV6.....	41
Figura 22. Ping desde PC-B a R1, G0/0/1.3 en IPV4 e IPV6.....	41
Figura 23. Ping desde PC-B a R1, G0/0/1.4 en IPV4 e IPV6.....	42
Figura 24. Ping desde PC-B a S1, VLAN 4 en IPV4 e IPV6	42
Figura 25. Ping desde PC-B a S2, VLAN 4 en IPV4 e IPV6	43
Figura 26. Topología del segundo escenario	44
Figura 27. Paso 1: Configurar la computadora de Internet	46
Figura 28. Ejecución comando Show run en R1	49
Figura 29. Ejecución comando show run en R2.....	52
Figura 30. Ejecución comando show run en R3.....	54
Figura 31. Ejecución comando show run en S1.....	55
Figura 32. Ejecución comando show run en S3.....	57
Figura 33. Ping desde R1 a R2 S0/0/0	58
Figura 34. Ping desde R2 a R3 S0/0/1	59
Figura 35. Ping desde Servidor de internet a Gateway predeterminado.....	59

Figura 36. Ejecución comando Show vlan en S1	61
Figura 37. Ejecución comando Show vlan en S3.....	63
Figura 38. Verificación de subinterfaces en R1	65
Figura 39. Ping desde S1 a R1, dirección VLAN 99.	66
Figura 40. Ping desde S3 a R1, dirección VLAN 99	67
Figura 41. Ping desde S1 a R1, dirección VLAN 21	67
Figura 42. Ping desde S3 a R1, dirección VLAN 23	68
Figura 43. Ejecución comando R3#show ip protocols	71
Figura 44. Ejecución de comando R3#show ip route OSPF	72
Figura 45. Ejecución del comando R3#show run.....	73
Figura 46. configuración DHCP de PC-A.....	77
Figura 47. configuracion DHCP de PC-C.....	78
Figura 48. Ping realizado desde PC-A a PC-C correcto.	78
Figura 49. Ingreso a servidor web desde servidor.	79
Figura 50. Verificación de la configuración NAT en R1.....	80
Figura 51. Ingreso por telnet desde R1 a R2.	82
Figura 52. Coincidencias recibidas lista de acceso.....	83
Figura 53. Comando clear ip access-list counters ejecutado.....	84
Figura 54. Comando show ip interface ejecutado.	84
Figura 55. Comando show ip nat translations ejecutado.	85
Figura 56. Comando clear ip nat translation ejecutado.....	86

LISTA DE TABLAS

Tabla 1. VLAN de red propuesta.....	16
Tabla 2. Direccionamiento de interfaces	16
Tabla 3. Paso 1. Inicializar y volver a cargar el router y el switch.....	17
Tabla 4. Evidencia del Paso 2: Configurar R1	19
Tabla 5. Paso 3: Configure S1 y S2.....	21
Tabla 6. Parte 2: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel).....	25
Tabla 7. Paso 2. Configure el S2	27
Tabla 8. Parte 3. Configurar soporte de host.	30
Tabla 9. Parte 3. Configurar soporte de host (continuación).....	32
Tabla 10. Parte 4. Probar y verificar la conectividad de extremo a extremo	35
Tabla 11 Paso 1 Inicializar y volver a cargar los routers y los switches.....	45
Tabla 12. Configurar la computadora de Internet.....	46
Tabla 13. Paso 2: Configurar R1.....	47
Tabla 14. Paso 3: configurar R2	50
Tabla 15. Paso 4: configurar R3.	52
Tabla 16. Paso 5: Configurar S1	55
Tabla 17. Paso 6: Configurar S3.....	56
Tabla 18. Paso 7: Verificar la conectividad de la red	57
Tabla 19. Paso 1: Configurar S1.....	60
Tabla 20. Paso 2: Configurar el S3.	62
Tabla 21. Paso 3: Configurar R1.....	64
Tabla 22. Paso 4: Verificar la conectividad de la red	65
Tabla 23. Paso 1: Configurar OSPF en el R1	68
Tabla 24. Paso 2: Configurar OSPF en el R2	69
Tabla 25. Paso 3: Configurar OSPFv3 en el R2	70
Tabla 26. Paso 4: Verificar la información de OSPF	71
Tabla 27. Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23	73
Tabla 28. Paso 2: Configurar la NAT estática y dinámica en el R2.....	75
Tabla 29. Paso 3: Verificar el protocolo DHCP y la NAT estática.	77
Tabla 30. Parte 6: Configurar NTP.....	80
Tabla 31. Paso 1: Restringir el acceso a las líneas VTY en el R2	81
Tabla 32. Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente.....	83

GLOSARIO

RED: Es un conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (acceso a internet, e-mail, chat, juegos), etc.

PROTOCOLO: Son lenguajes o códigos de comunicación entre sistemas informáticos, definidos en base a una sintaxis, una semántica y una sincronización, así como de métodos de recuperación de errores.

ENRUTAMIENTO: Es el proceso de reenviar paquetes entre redes, siempre buscando la mejor ruta (la más corta).

VLAN: Es un segmento lógico más pequeño dentro de una gran red física cableada.

DHCP: Es una extensión del protocolo Bootstrap (BOOTP) desarrollado en 1985 para conectar dispositivos como terminales y estaciones de trabajo sin disco duro con un Bootserver, del cual reciben su sistema operativo.

ETHERCHANNEL: Es una tecnología de Cisco construida con los estándares 802.3 Full-Duplex y Fast Ethernet; permite la agrupación lógica de varios enlaces físicos Ethernet.

PORT-SECURITY: Es un feature o característica de los switches Cisco que les permite retener las direcciones MAC conectadas a cada puerto del dispositivo y permitir solamente a esas direcciones MAC comunicarse a través de esa boca del switch.

RESUMEN

Por medio del desarrollo del siguiente trabajo demostraré todos los conocimientos adquiridos a lo largo del diplomado de profundización donde por medio de la realización de dos escenarios propuestas evidenciaré cada una de las configuraciones que se requieren para poder conectar redes pequeñas y grandes de empresas, implementando métodos de seguridad y protocolos de conexión que actualmente se implementan en las empresas a nivel global.

El proceso de montaje y configuración se llevará a cabo en el emulador Packet Tracer otorgado por la empresa Cisco que sin duda alguna es una herramienta útil para todos los ingenieros de telecomunicaciones ya que permite realizar una simulación perfecta de una red con todos sus funciones y características.

Palabras clave: *Red, Protocolos, enrutamiento, VLAN, DHCP, EtherChannel y Port-security.*

ABSTRACT

Through the development of the following work I will demonstrate all the knowledge acquired throughout the in-depth diploma where, through the realization of two proposed scenarios, I will demonstrate each of the configurations that are required to connect small and large networks of companies, implementing methods security and connection protocols that are currently implemented in companies globally.

The assembly and configuration process will be carried out in the Packet Tracer emulator granted by the Cisco company, which is undoubtedly a useful tool for all telecommunications engineers since it allows a perfect simulation of a network with all its functions and characteristics.

Keywords: Network, protocols, routing, VLAN, DHCP, EtherChannel and Port-security.

1. INTRODUCCIÓN

Actualmente, las empresas han tenido que acoplarse al termino de transmodernización, donde cada una de ellas debe implementar sistemas de Comunicaciones para crear relaciones con el resto del mundo, hoy por hoy, las operaciones empresariales se realizan con Europa, Asia, Arica, América del Norte, y no solamente con clientes locales, lo que ha obligado a las empresas a mejorar la calidad de sus ordenadores, redes y su personal, generando un Sistema eficiente y accesible desde cualquier parte del mundo.

Por tal motivo, es necesario que haya personal capacitado para el diseño, desarrollo de infraestructura de redes, así mismo, la Universidad nacional abierta y a distancia ha dispuesto dentro de su formación académica un diplomado de profundización en CISCO, dirigido a profesionales en ingeniería de sistemas, abarcando temas como: RIPv2, OSPFv2, OSPFv3, DHCPv4 y DHCPv6 en switches y routers, diseñar e implementar NAT dinámicas y estáticas, listas de acceso bajo los protocolos IPv4 y IPv6, entre otros temas de gran importancia para afianzar nuestros conocimientos en redes. A través de herramientas de simulación en los escenarios propuestos, herramientas de protocolos de administración de redes para la solución de problemas, evaluación de desempeños de routers y switches, además, de instruir al profesional en el diseño de políticas de enrutamiento estático y/o dinámico bajo un esquema de direccionamiento IP, entre otras cosas. De esta manera, se desarrolló un Proyecto aplicado a ejecutar dos escenarios propuestos por el tutor, mostrando el paso a paso con su respectiva evidencia, además, de la simulación en el software Packet Tracer. Las evidencias se basaron en describir cada etapa, configurar de manera correcta cada uno de los dispositivos de networking en el simulador antes mencionado y evidenciarlo en el trabajo final.

2. OBJETIVOS

2.1 OBJETIVOS GENERALES

Desarrollar dos escenarios con base en la prueba de habilidades propuestos por el diplomado de profundización cisco (Diseño e implementación de soluciones integradas LAN/WAN).

2.2 OBJETIVOS ESPECIFICOS

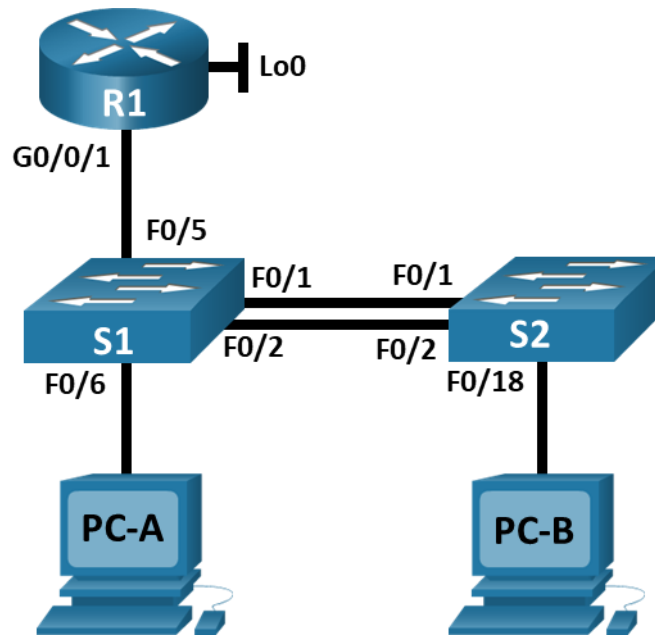
- ✓ Realizar el montaje de cada escenario en el simulador Packet Tracer.
- ✓ Ejecutar los comandos adecuados para llevar a cabo la correcta configuración de cada dispositivo usado en los 2 escenarios.
- ✓ Identificar los requerimientos establecidos por la guía e implementarlos adecuadamente para un buen funcionamiento.
- ✓ Evidenciar por medio de pantallazos el correcto funcionamiento de cada uno de los dispositivos configurados en la red.

3. DESARROLLO

DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

ESCENARIO 1

Figura 1. Topología del Primer Escenario



Fuente: CISCO

Mediante el desarrollo del primer escenario se configurarán los dispositivos de una red pequeña. Realizar el proceso de configuración de un Router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. Tanto el Router como el switch deben administrarse de forma segura. Por último, se Configuraré el enrutamiento entre VLAN, DHCP, EtherChannel y port-security.

Tabla 1. VLAN de red propuesta

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

Tabla 2. Direccionamiento de interfaces

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

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
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

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

1. Instrucciones

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

Se realiza el montaje de la red con Switches 3650 debido a que en Packet Tracer son compatibles con IPV6, los switches 2960 también son compatibles con ipv6 en vida real, El Router usado para el ejercicio corresponde al 1741 y por último 2 PC, se realiza las conexiones como lo muestra la topología para comenzar con el desarrollo del ejercicio.

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.

Para llevar a cabo el proceso de inicializar los dispositivos ingreso a la consola de cada dispositivo e introduzco los siguientes comandos con su función específica como se evidencia en la tabla 3.

Tabla 3.Paso 1. Inicializar y volver a cargar el router y el switch

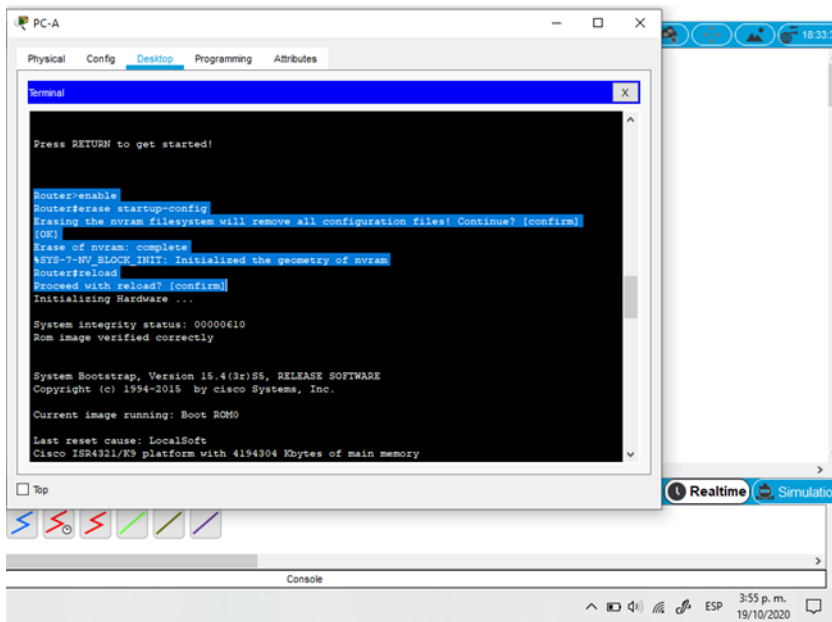
Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config
Volver a cargar todos los routers	Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar	Switch#erase startup-config Switch#delete vlan.dat

la base de datos de VLAN anterior	
Volver a cargar ambos switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show flash

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

El Switch 3650 admite IPV6 por defecto en Packet Tracer como lo muestra la imagen con el comando show sdm prefer.

Figura 2. Evidencia de Paso 1: Inicializar y volver a cargar el router.



Fuente: Autor

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

Paso 2: Configurar R1

Para comenzar con el desarrollo del ejercicio comienzo con la configuración inicial de administración en el Router1 que tiene como objetivo configurar los siguientes parámetros:

Desactivar la búsqueda DNS para evitar que el Router busque soluciones por DNS a comandos que ejecutaremos más adelante esto podría generar retrasos y demoras en el proceso de la configuración, nombre del Router para llevar un registro organizado, nombre del dominio para la administración de la red, protocolos de seguridad como lo son la clave de cifrado para el modo EXEC privilegiado y para la consola con esto evito que alguien acceda remotamente a la configuración del Router y a su administración.

Creación del usuario y contraseña para la base de datos local del Router para la seguridad de inicio de sesión remotamente en el Router, activación del protocolo SSH para permitir la conexión de acceso remoto, y el proceso de habilitación de routing en el protocolo IPV6 que vamos a usar en el ejercicio.

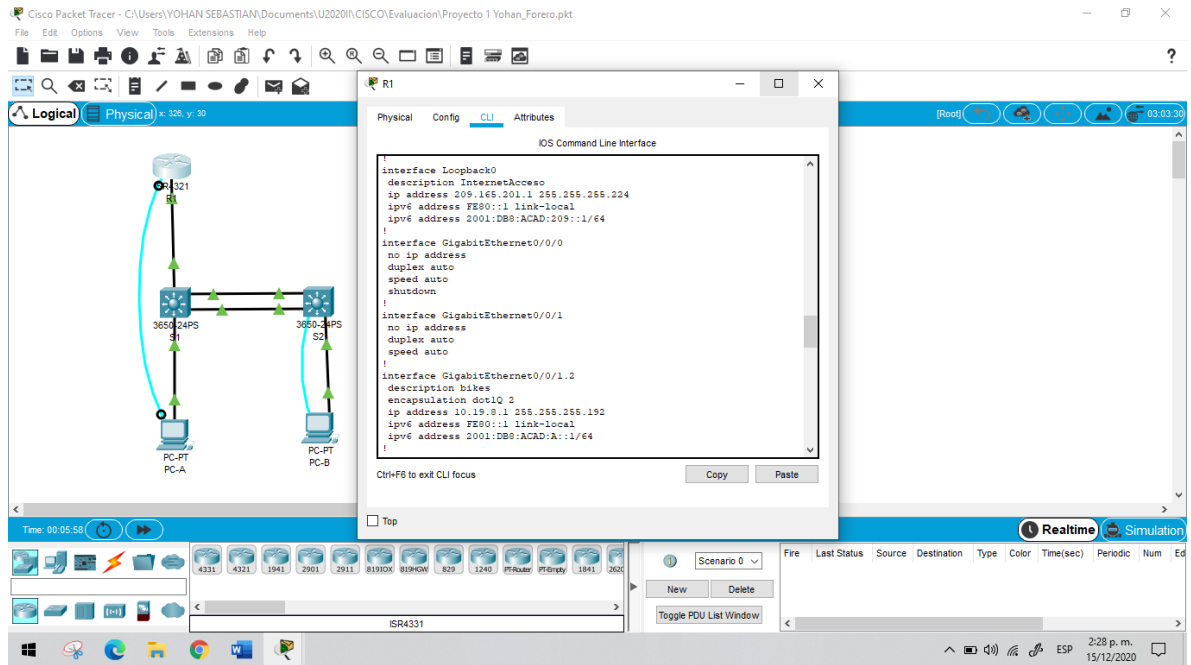
Por último, configuro los interfaces que serán usadas en el ejercicio con su respectivo direccionamiento ip, descripciones y proceso de activación. Evidencia de configuración tabla 4.

Tabla 4. Evidencia del Paso 2: Configurar R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain lookup
Nombre del Router: R1	Router(config)#hostname R1
Nombre de dominio: ccna-lab.com	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado: ciscoenpass	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola: ciscoconpass	R1(config)#line console 0 R1(config-line) #password ciscoconpass
Establecer la longitud mínima para las contraseñas de 10 caracteres	R1(config)#security passwords min-length 10
Creación de un usuario administrativo en la base de datos local Nombre de usuario: admin Password: admin1pass	R1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 15 R1(config-line)#login local
Configurar VTY solo aceptando SSH	R1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption

Tarea	Especificación
Configure un MOTD Banner	R1(config)#banner motd %ACCESO DENEGADO%
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
<p>Configurar interfaz G0/0/1 y subinterfaces Establezca la descripción</p> <p>Establece la dirección IPv4.</p> <p>Establezca la dirección local de enlace IPv6 como fe80::1</p> <p>Establece la dirección IPv6.</p> <p>Activar la interfaz.</p>	<p>R1(config)#int g0/0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description bikes</p> <p>R1(config-subif)#ip address 10.19.8.1 255.255.255.192</p> <p>R1(config-subif)#ipv6 address fe80::1 link-local</p> <p>R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64</p> <p>R1(config-subif)#no shutdown</p>
<p>Configure el Loopback0 interface Establezca la descripción</p> <p>Establece la dirección IPv4.</p> <p>Establece la dirección IPv6.</p> <p>Establezca la dirección local de enlace IPv6 como fe80::1</p>	<p>R1(config-if)#int loopback 0 R1(config-if)#description InternetAcceso</p> <p>R1(config-if)#ip address 209.165.201.1 255.255.255.224</p> <p>R1(config-if)#ipv6 address 2001:db8:acad:209::1/64</p> <p>R1(config-if)#ipv6 address fe80::1 link-local</p>
Generar una clave de cifrado RSA Módulo de 1024 bits	R1(config)#crypto key generate rsa 1024

Figura 3. Ejecución comando Show run R1



Fuente: Autor

Paso 3: Configure S1 y S2.

El proceso de configuración inicial de los Switches es similar al del Router mencionado en el paso anterior debido a que es importante que cada dispositivo en la red tenga seguridad ya que esto nos garantiza un perfecto y confiable funcionamiento de la red.

En ambos Switches realizo la configuración de la interfaz de administración SVI con la correcta configuración IP y el Gateway predeterminado que nos permitirá la comunicación correcta entre todos los dispositivos de la red. Proceso e configuración en la tabla 5.

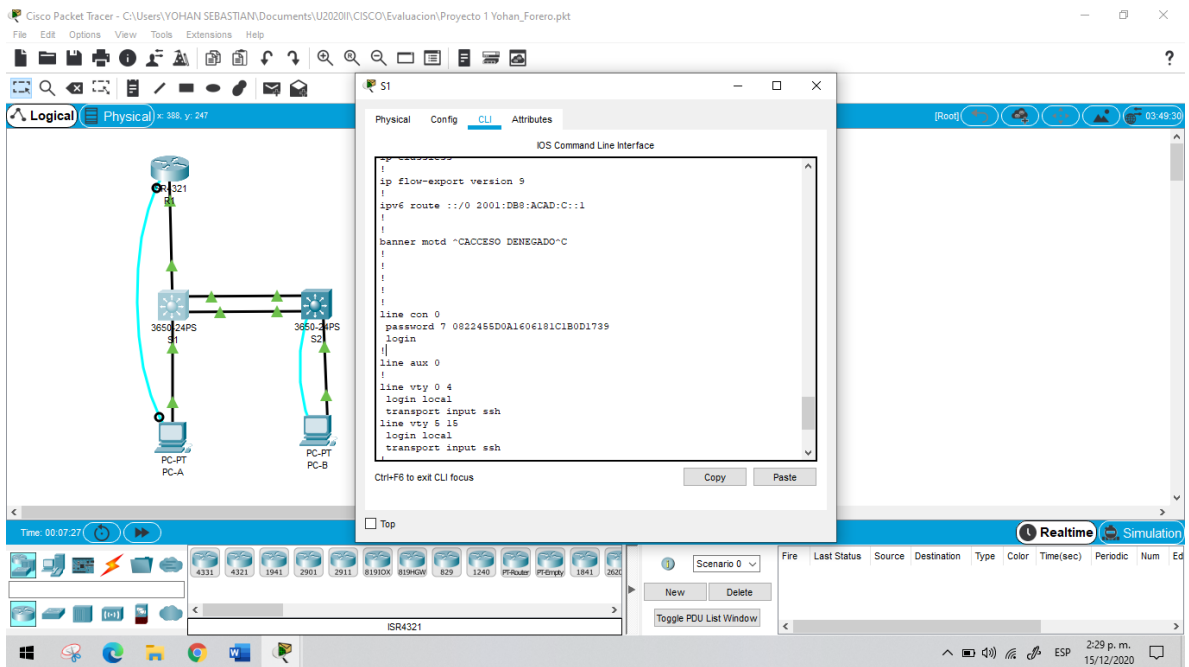
Tabla 5. Paso 3: Configure S1 y S2.

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch(config)#no ip domain lookup
Asignación nombre del switch	S1 o S2, según proceda Switch(config)#hostname S1

Tarea	Especificación
Asignación nombre de dominio: ccna-lab.com	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado: Ciscoenpass	S1(config)#enable secret ciscoenpass
Configuración de contraseña de acceso a la consola: Ciscoconpass	S1(config)#line console 0 S1(config-line)#password ciscoconpass
Creación de un usuario administrativo en la base de datos local Nombre de usuario: admin Password: admin1pass	S1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd "ACCESO DENEGADO"
Generar una clave de cifrado RSA	Módulo de 1024 bits S1(config)#crypto key generate rsa 1024
Configuración de la interfaz de administración (SVI) Establecimiento de la dirección local de enlace IPv6 como FE80::98 para S1 y FE80::99 para S2 Establecer la dirección IPv6 de capa 3	S1(config)#int vlan 4 S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S2(config)#int vlan 4 S2(config-if)#ip address 10.19.8.99 255.255.255.248 S2(config-if)#ipv6 address fe80::99 link-local S2(config-if)#ipv6 address 2001:db8:acad:c::99/64

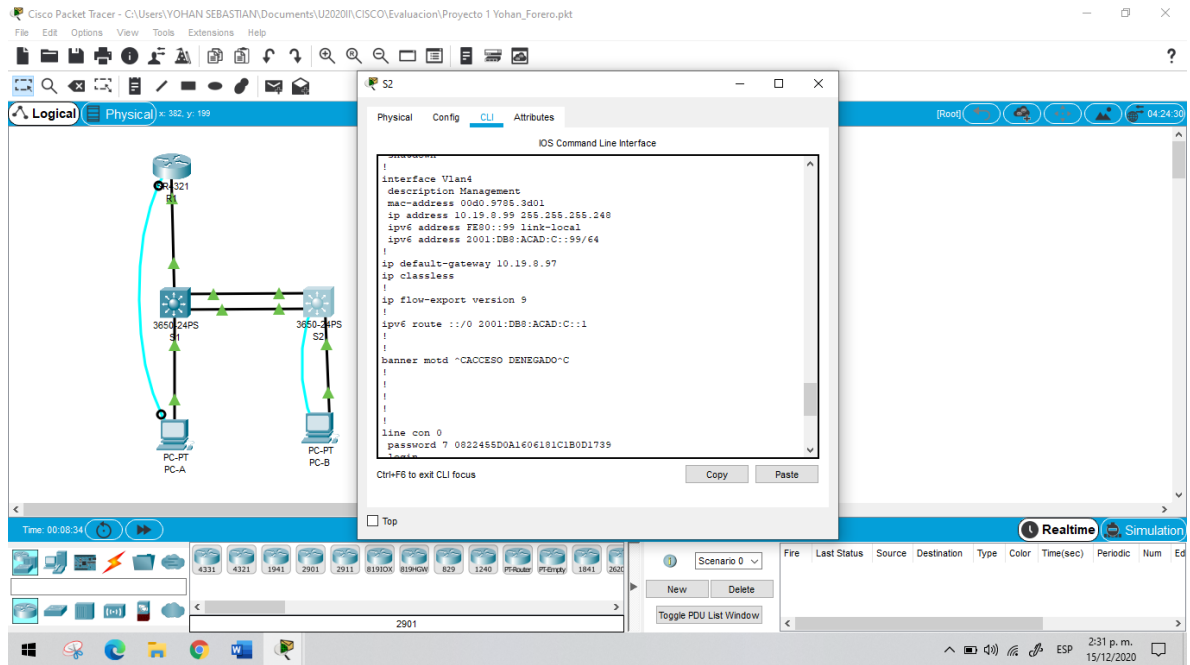
Tarea	Especificación
Configuración del Gateway predeterminado Se configuró la puerta de enlace predeterminada como 10.19.8.97 para IPv4 según la tabla de direcciones.	S1(config)#ip default-gateway 10.19.8.97

Figura 4. Ejecución comando show run S1



Fuente: Autor

Figura 5. Ejecución comando show run S1



Fuente: Autor

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

Paso 1: Configurar S1

Para el proceso de configuración en el S1 comienzo con la creación de las VLAN con su respectiva descripción ya que este nos permitirá trabajar de forma organizada para poder identificarlos en la red, seguidamente creo los troncos 802.1Q que serán los encargados de los enlaces troncales a la VLAN 6 nativa, creo el grupo de puertos de EtherChannel donde irán configuradas nuestras VLAN.

Una vez creado el grupo de puerto de EtherChannel asignamos la VLAN 6 como puerto de acceso para la comunicación entre los dispositivos que se encuentran en la misma red, ahora asigno el puerto G1/0/6 a la VLAN 2 que es donde está conectada la PC-A, luego creo los parámetros de seguridad en los puertos para que solo permita un máximo de 3 direcciones conectadas.

Por último, desactivo las interfaces que no se usaran en el Switch en este caso el Switch 1 está usando las interfaces g1/0/1-2 y g1/0/5-6 por lo que se procederá a

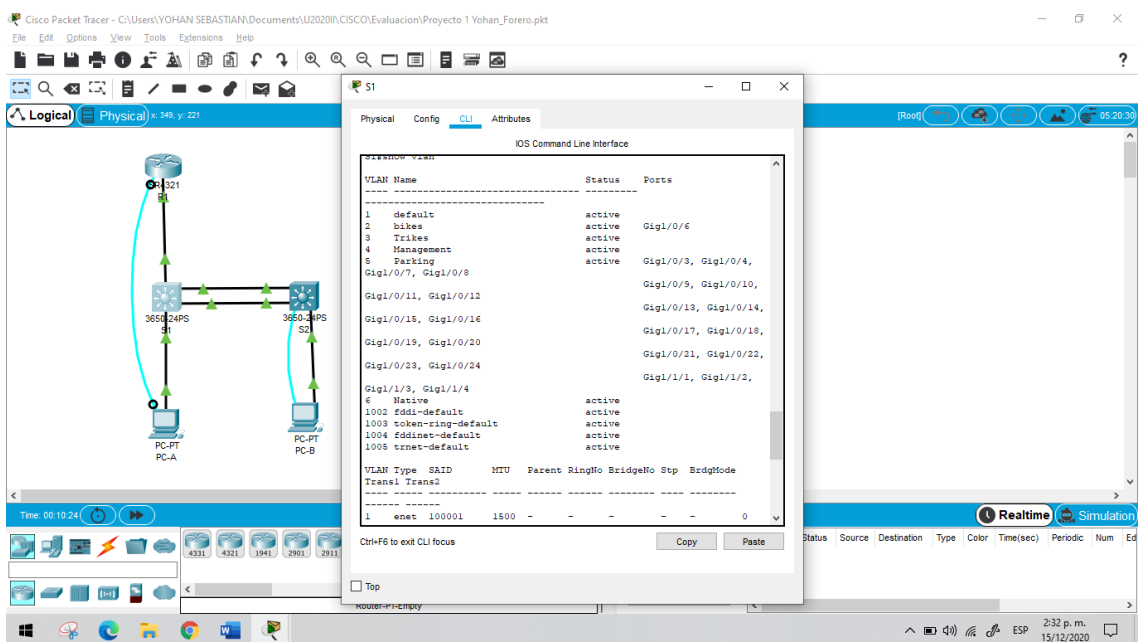
desactivar el siguiente rango de interfaces g1/0/3-4 y g1/0/7-24 con su respectiva descripción que están deshabilitadas. Evidencia tabla 6.

Tabla 6. Parte 2: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel).

Tarea	Especificación
<p>Creación de las VLAN con su respectiva descripción.</p> <p>VLAN 2, nombre Bikes</p> <p>VLAN 3, nombre Trikes</p> <p>VLAN 4, name Management</p> <p>VLAN 5, nombre Parking</p> <p>VLAN 6, nombre Native</p>	<p>S1(config-vlan)#vlan 2</p> <p>S1(config-vlan)#name bikes</p> <p>S1(config-vlan)#vlan 3</p> <p>S1(config-vlan)#name Trikes</p> <p>S1(config-vlan)#vlan 4</p> <p>S1(config-vlan)#name Management</p> <p>S1(config-vlan)#vlan 5</p> <p>S1(config-vlan)#name Parking</p> <p>S1(config-vlan)#vlan 6</p> <p>S1(config-vlan)#name Native</p>
<p>Creación de los troncos 802.1Q que utilizaran la VLAN 6 nativa</p>	<p>S1(config)#int g1/0/5</p> <p>S1(config-if)#switchport mode trunk</p> <p>S1(config-if)# switchport trunk native vlan 6</p>
<p>Creación de un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2</p> <p>Usar el protocolo LACP para la negociación</p>	<p>S1(config-if)#int range g1/0/1-2</p> <p>S1(config-if-range)#channel-group 1 mode active</p> <p>S1(config-if-range)#int port-channel 1</p> <p>S1(config-if)#switchport mode trunk</p> <p>S1(config-if)#switchport trunk native vlan 6</p>

Tarea	Especificación
Configuración del puerto de acceso de host para VLAN 2 Interface F0/6	S1(config-if)#int g1/0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2
Configuración de la seguridad del puerto en los puertos de acceso Permitir 3 direcciones MAC	S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas, es el mismo procedimiento para todas las interfaces que se establecen en el siguiente rango: g1/0/3-4 y g1/0/7-24 Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S1(config-if)#int range g1/0/3-4 S1(config-if-range)#switchport mode Access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Not In Use S1(config-if-range)#shutdown

Figura 6. Ejecución comando show vlan en S1



Fuente: Autor

Paso 2. Configure el S2.

Para el proceso de configuración en el S12 comienzo con la creación de las VLAN con su respectiva descripción ya que este nos permitirá trabajar de forma organizada para poder identificarlos en la red, seguidamente creo los troncos 802.1Q que serán los encargados de los enlaces troncales a la VLAN 6 nativa, creo el grupo de puertos de EtherChannel donde irán configuradas nuestras VLAN.

Una vez creado el grupo de puerto de EtherChannel asignamos la VLAN 6 como puerto de acceso para la comunicación entre los dispositivos que se encuentran en la misma red, ahora asigno el puerto G1/0/18 a la VLAN 3 que es donde está conectada la PC-C, luego creo los parámetros de seguridad en los puertos para que solo permita un máximo de 3 direcciones conectadas.

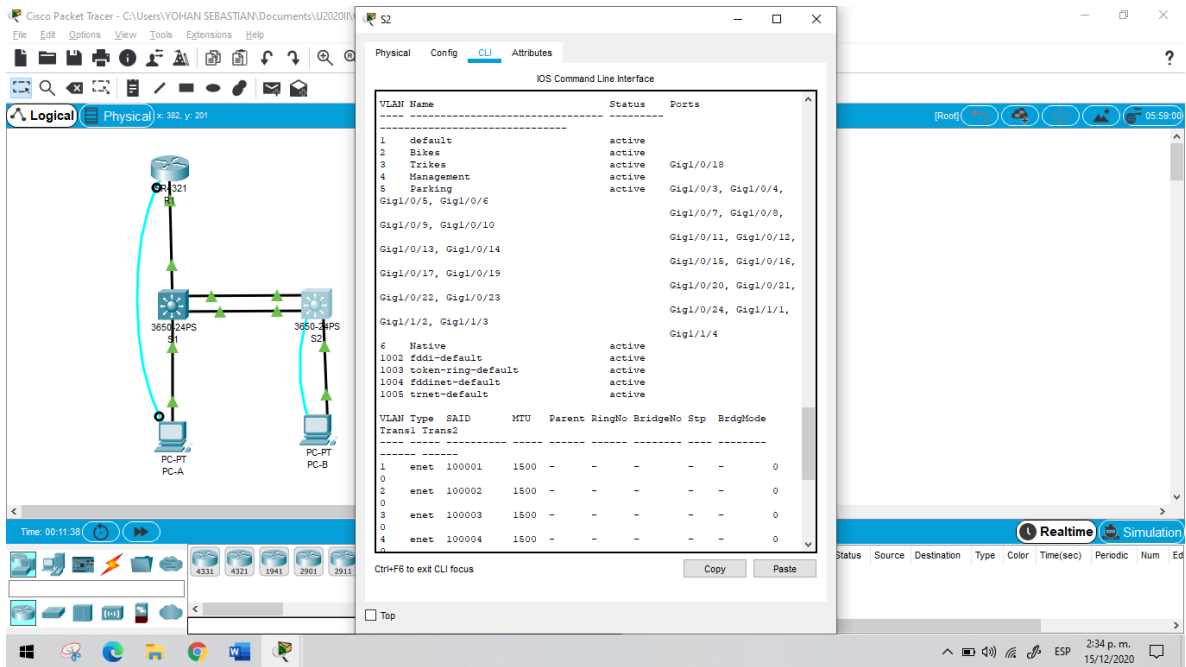
Por último, desactivo las interfaces que no se usaran en el Switch en este caso el Switch 1 está usando las interfaces g1/0/1-2 por lo que se procede a desactivar el siguiente rango de interfaces g1/0/3-4 y g1/0/7-24 con su respectiva descripción que están deshabilitadas. Proceso de configuración tabla 7.

Tabla 7. Paso 2. Configure el S2

Tarea	Especificación
Creación de VLAN con su respectiva descripción VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	S2(config-vlan)#vlan 2 S2(config-vlan)#name bikes S2(config-vlan)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#vlan 4 S2(config-vlan)#name Management S2(config-vlan)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#vlan 6 S2(config-vlan)#name Native

Tarea	Especificación
<p>Creación de troncos 802.1Q que utilicen la VLAN 6 nativa</p> <p>Interfaces F0/1 y F0/2</p>	<pre>S2(config)#int range g1/0/1-2 S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 6</pre>
<p>Creación de un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2</p> <p>Usar el protocolo LACP para la negociación</p>	<pre>S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#int port-channel 1 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6</pre>
<p>Configuro el puerto de acceso del host para la VLAN 3</p> <p>Interfaz F0/18</p>	<pre>S2(config-if)#int g1/0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3</pre>
<p>Configuro port-security en los access ports permite 3 MAC addresses</p>	<pre>S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3</pre>
<p>Asegure todas las interfaces no utilizadas. Es el mismo procedimiento para todas las interfaces que se establecen en el siguiente rango: g1/0/3-17 y g1/0/19-24</p> <p>Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar</p>	<pre>S2(config-if)#int range g1/0/3-17 S2(config-if-range)#switchport mode Access S2(config-if-range)#description Not In Use S2(config-if-range)#shutdown</pre>

Figura 7. Ejecución comando Show vlan en S2



Fuente: Autor

Parte 3. Configurar soporte de host

Paso 1. Configure R1

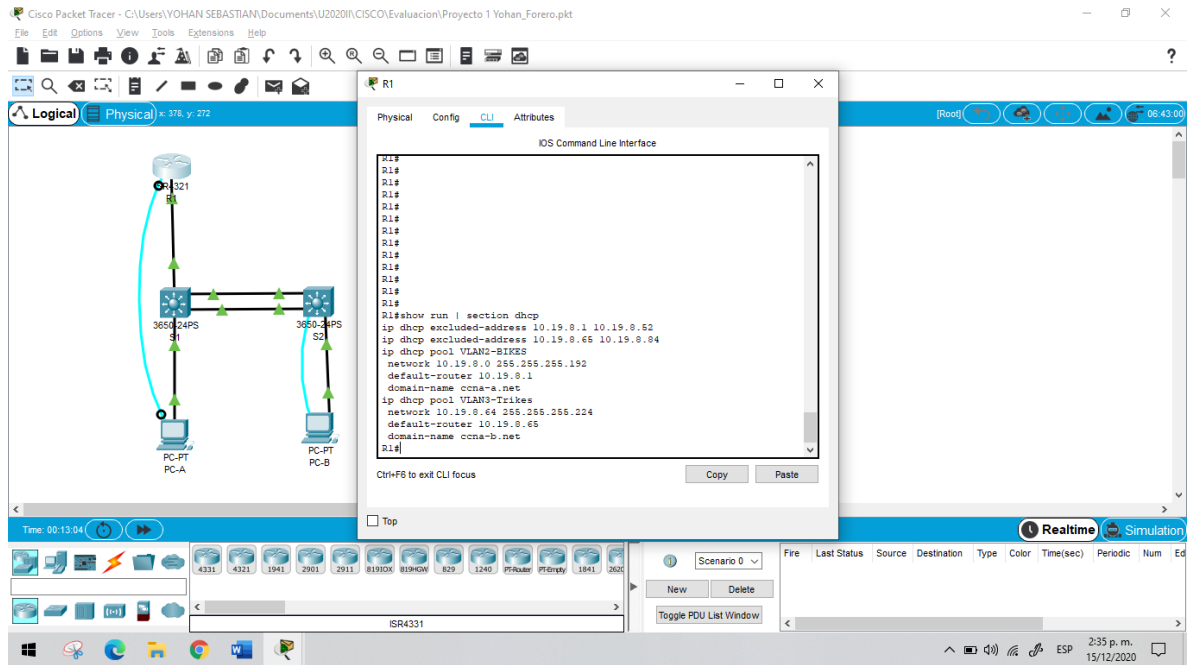
Como primera medida para la configuración de R1 es indispensable asignar las direcciones predeterminadas loopback que nos ayudara a que los protocolos configurados en los dispositivos funcionen de la manera correcta esto quiere decir que el tráfico de red ira dirigido a las direcciones predeterminadas.

Ahora configuro el DHCP en IPV4 para la VLAN 2 para que solo use las ultimas 10 direcciones disponibles es la estructura quedaría de la siguiente forma: se desactiva el siguiente rango de direcciones IP: 10.19.8.1 a 10.19.8.52 por lo que al momento de conectar los hosts deberían usar únicamente las direcciones 10.19.8.52 a la 10.19.8.62. en el caso de la VLAN 3 se procede a desactivar el rango de direcciones 10.19.8.65 al 10.19.8.84 por lo que las direcciones que usarán los hosts conectados serán del siguiente rango: 10.19.8.85 al 10.19.8.95. evidencia de configuración tabla 8.

Tabla 8. Parte 3. Configurar soporte de host.

Tarea	Especificación
<p>Configure Default Routing Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0</p>	<pre>R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0</pre>
<p>Configurar IPv4 DHCP para VLAN 2 Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada</p>	<pre>R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#ip dhcp pool R1(config)#ip dhcp pool VLAN2-BIKES 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</pre>
<p>Configurar DHCP IPv4 para VLAN 3 Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada</p>	<pre>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-b.net</pre>

Figura 8. Evidencia configuración DHCP en R1



Fuente: Autor

Paso 2. Configurar los servidores

Para el desarrollo de las configuraciones de los hosts ingreso al escritorio en el menú de configuración IP y lo configuro de la siguiente forma: para el protocolo IPV4 asigno DHCP es decir que tome la IP automáticamente de la VLAN donde está conectado, las IP del PC-A quedo como 10.19.8.53 y para el PC-B 10.19.8.85 es decir que la regla que añadimos anteriormente en el R1 ha funcionado y cada host está utilizando la primera de las ultimas 10 direcciones disponibles.

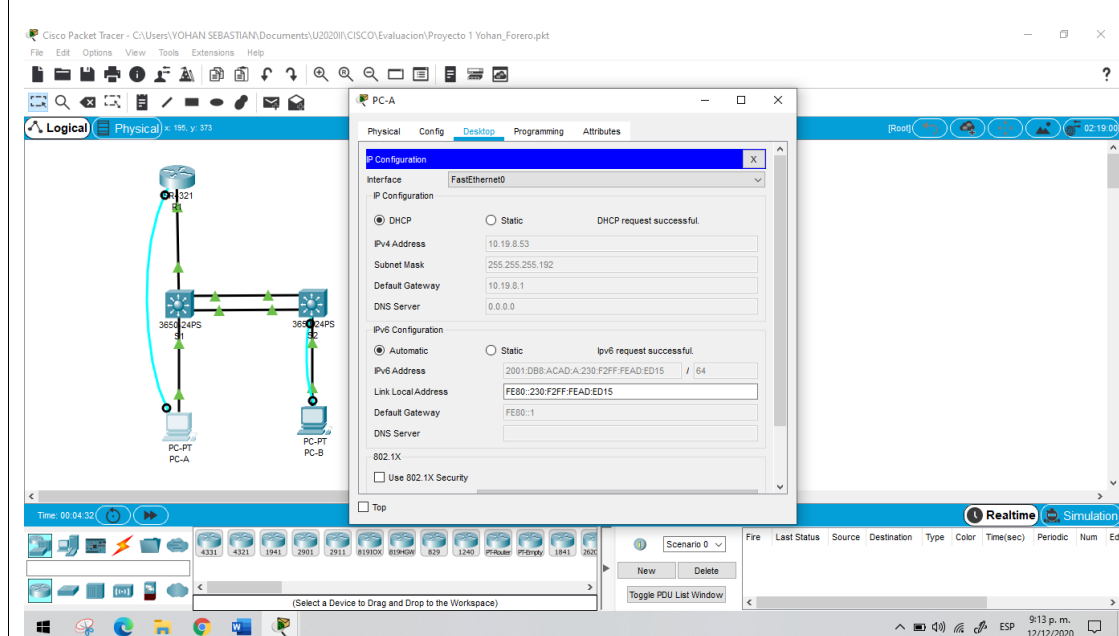
Para el protocolo IPV6 asigno a cada host manualmente la dirección IP según la tabla de direccionamiento.

Por último, para verificar la configuración de la red en cada host me dirijo a la consola y ejecuto el comando ipconfig /all que me proporcionara toda la configuración de red del host donde evidencio: el nombre del dominio que asignamos anteriormente, la dirección física, dirección IP, mascara de red, Gateway predeterminado, servidor DNS y servidor DHCP. Esto para los protocolos IPV4 E IPV6 Y demás protocolos que contenga el equipo. Evidencias tabla 9.

Tabla 9. Parte 3. Configurar soporte de host (continuación)

PC-A Network Configuration	
Descripción	ccna-a.net
Dirección física	0030.F2AD.ED15
Dirección IP	0.19.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

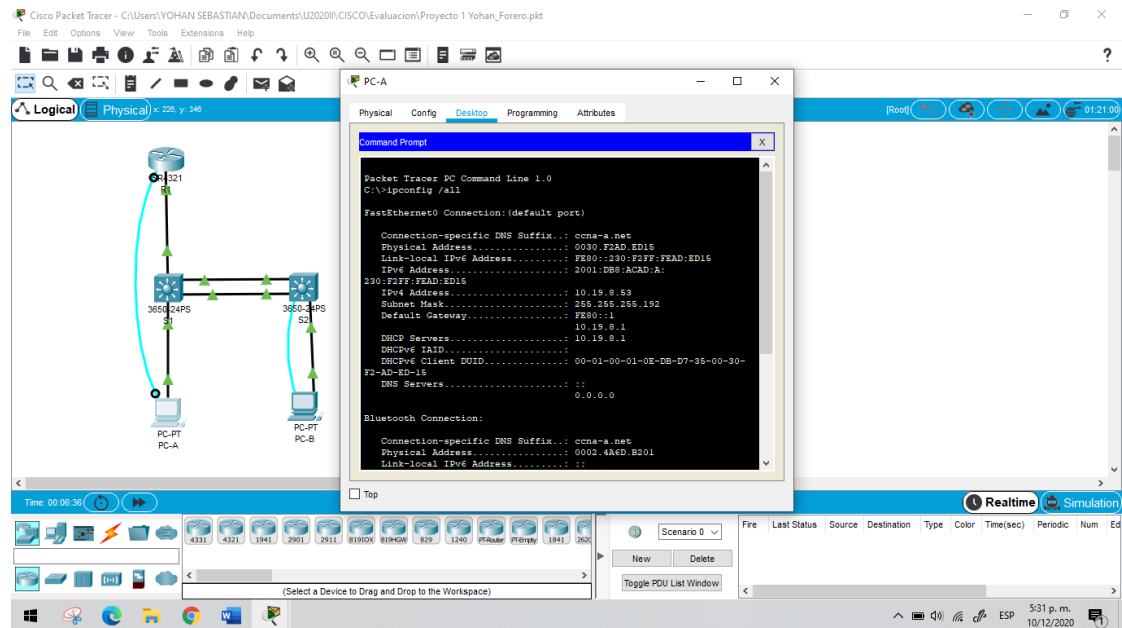
Figura 9. Evidencia de configuración IPV4 tomada automáticamente por DHCP e IPV6 asignada manualmente en PC-A.



Fuente: Autor

PC-A Network Configuration

Figura 10. Ejecución del comando `ipconfig /all` en PC-A que muestra toda la configuración IP del ordenador



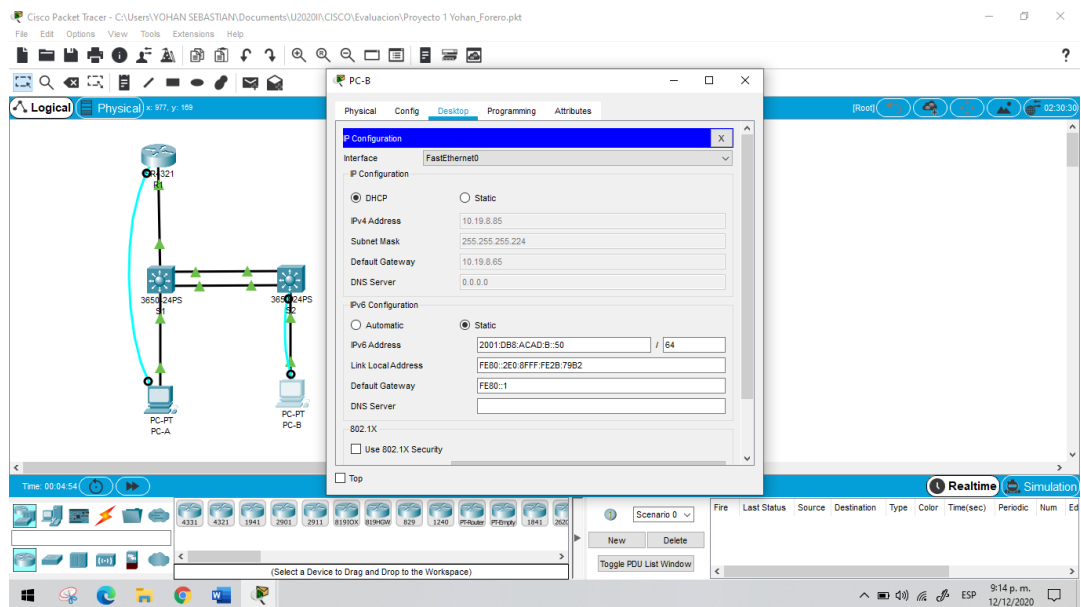
Fuente: Autor

Configuración de red de PC-B

Descripción	ccna-b.net
Dirección física	00E0.8F2B.79B2
Dirección IP	10.19.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::1

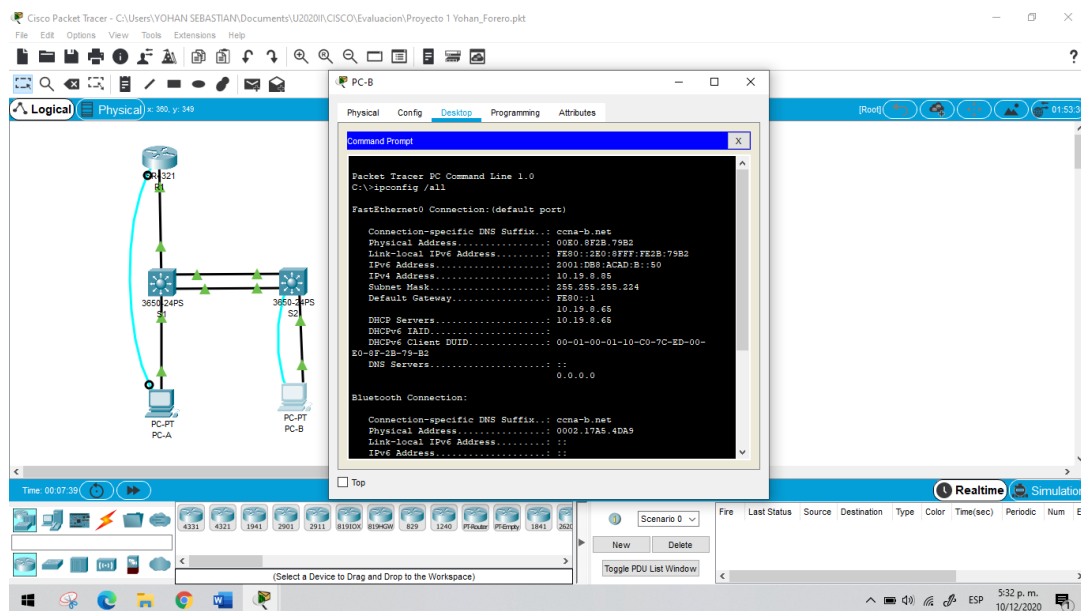
PC-A Network Configuration

Figura 11. Evidencia de configuración IPv4 tomada automáticamente por DHCP e IPv6 asignada manualmente en PC-B



Fuente: Autor

Figura 12. Ejecución del comando ipconfig /all en PC-B que muestra toda la configuración IP del ordenador.



Fuente: Autor

Parte 4. 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 10. Parte 4. Probar y verificar la conectividad de extremo a extremo

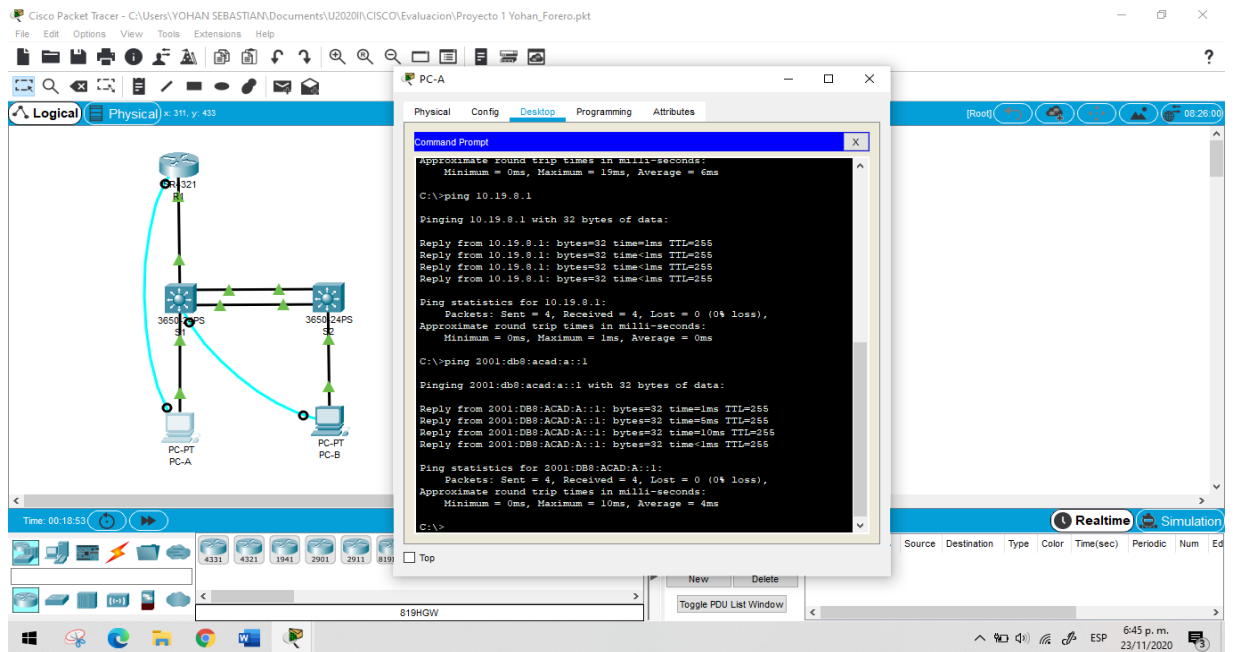
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	CORRECTO
PC-A	R1, G0/0/1.2	IPv6	2001:db8:acad:a :1	CORRECTO
PC-A	R1, G0/0/1.3	Dirección	10.19.8.65	CORRECTO
PC-A	R1, G0/0/1.3	IPv6	2001:db8:acad:b: :1	CORRECTO
PC-A	R1, G0/0/1.4	Dirección	10.19.8.97	CORRECTO
PC-A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

Desde	A	de Internet	Dirección IP	Resultados de ping
<i>PC-B</i>	<i>R1 Bucle 0</i>	IPv6	2001:db8:acad:209: :1	CORRECTO
<i>PC-B</i>	<i>R1, G0/0/1.2</i>	Dirección	10.19.8.1	CORRECTO
<i>PC-B</i>	<i>R1, G0/0/1.2</i>	IPv6	2001:db8:acad:a: :1	CORRECTO
<i>PC-B</i>	<i>R1, G0/0/1.3</i>	Dirección	10.19.8.65	CORRECTO
<i>PC-B</i>	<i>R1, G0/0/1.3</i>	IPv6	2001:db8:acad:b: :1	CORRECTO
<i>PC-B</i>	<i>R1, G0/0/1.4</i>	Dirección	10.19.8.97	CORRECTO
<i>PC-B</i>	<i>R1, G0/0/1.4</i>	IPv6	2001:db8:acad:c: :1	CORRECTO
<i>PC-B</i>	<i>S1, VLAN 4</i>	Dirección	10.19.8.98	CORRECTO
<i>PC-B</i>	<i>S1, VLAN 4</i>	IPv6	2001:db8:acad:c: :98	CORRECTO
<i>PC-B</i>	<i>S2, VLAN 4</i>	Dirección	10.19.8.99.	CORRECTO
<i>PC-B</i>	<i>S2, VLAN 4</i>	IPv6	2001:db8:acad:c: :99	CORRECTO

Capturas de pantalla de pings realizados

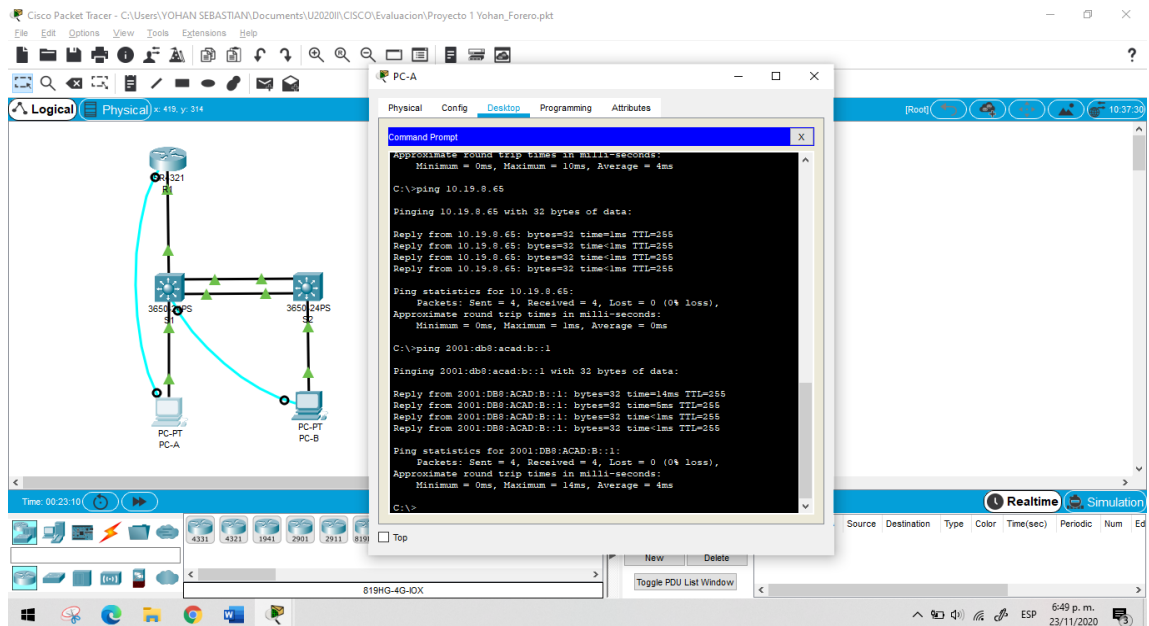
Para proceder a probar la conectividad de todos los dispositivos de la red se ejecuta el comando ping en los dispositivos, este comando se encarga de enviar paquetes a una dirección de destino y recibirlos de nuevo, por medio de las siguientes figuras evidenciare el correcto funcionamiento y conectividad de toda la red como esta establecido en la tabla 10.

Figura 13. Ping desde PCA a R1, G0/0/1.2 en IPV4 e IPV6



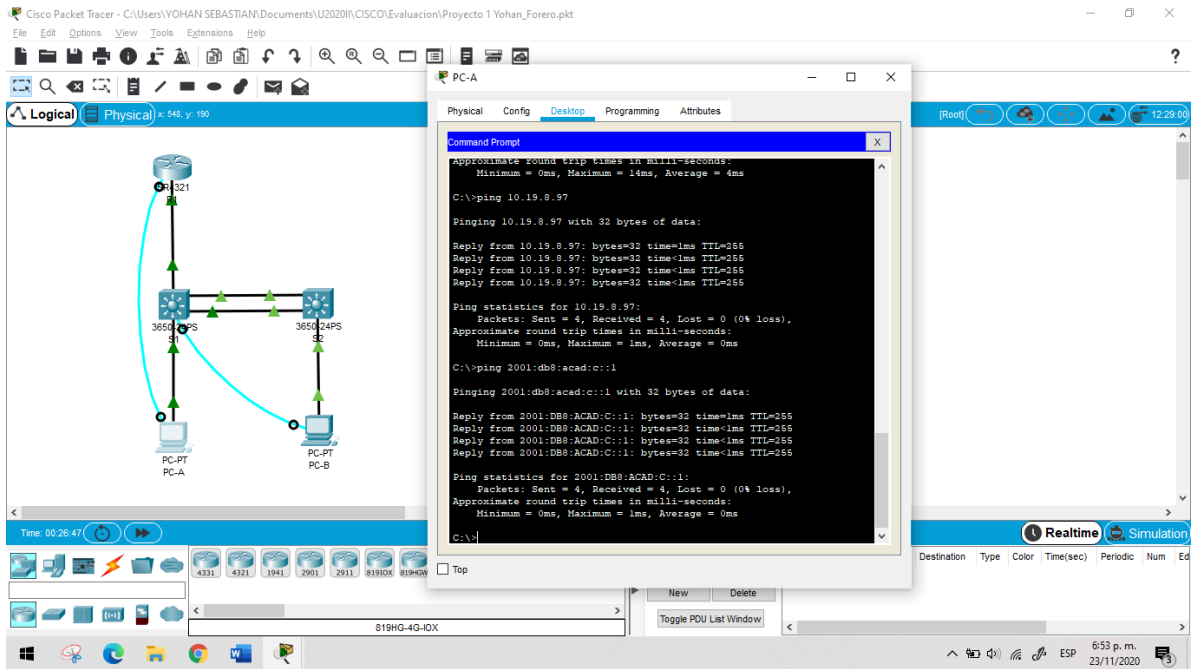
Fuente: Autor

Figura 14. Ping desde PCA a R1, G0/0/1.3 en IPV4 e IPV6



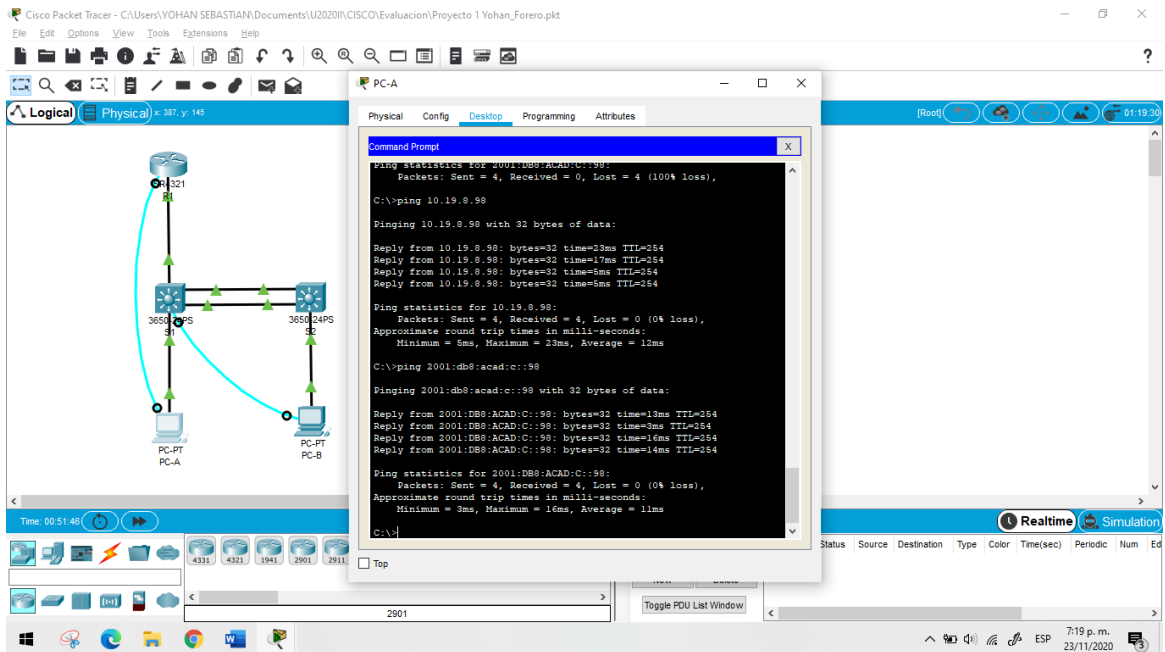
Fuente: Autor

Figura 15. Ping desde PCA a R1, G0/0/1.4 en IPV4 e IPV6



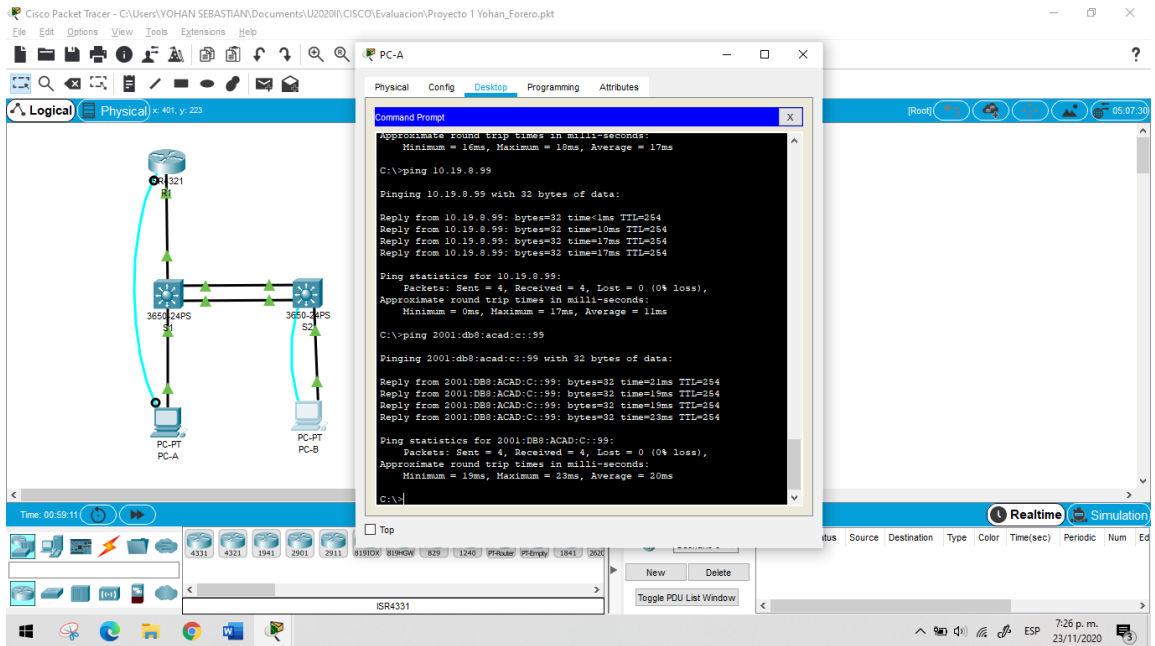
Fuente: Autor

Figura 16. Ping desde PCA a S1, VLAN4 en IPV4 e IPV6



Fuente: Autor

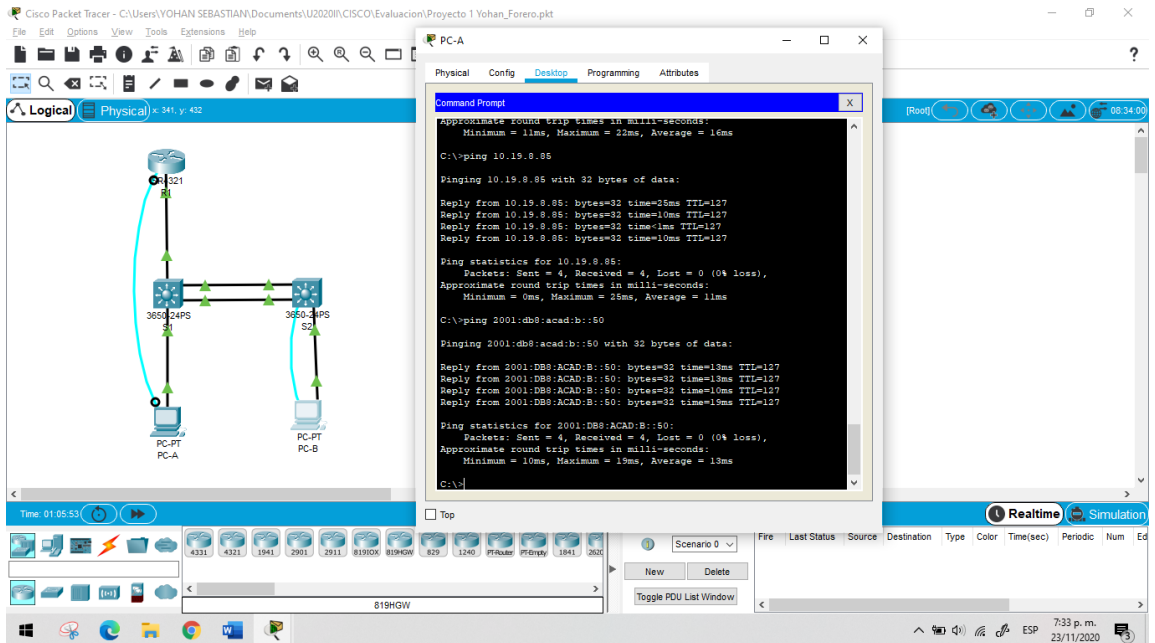
Figura 17. Ping desde PCA a S2, VLAN4 en IPV4 e IPv6



Fuente: Autor

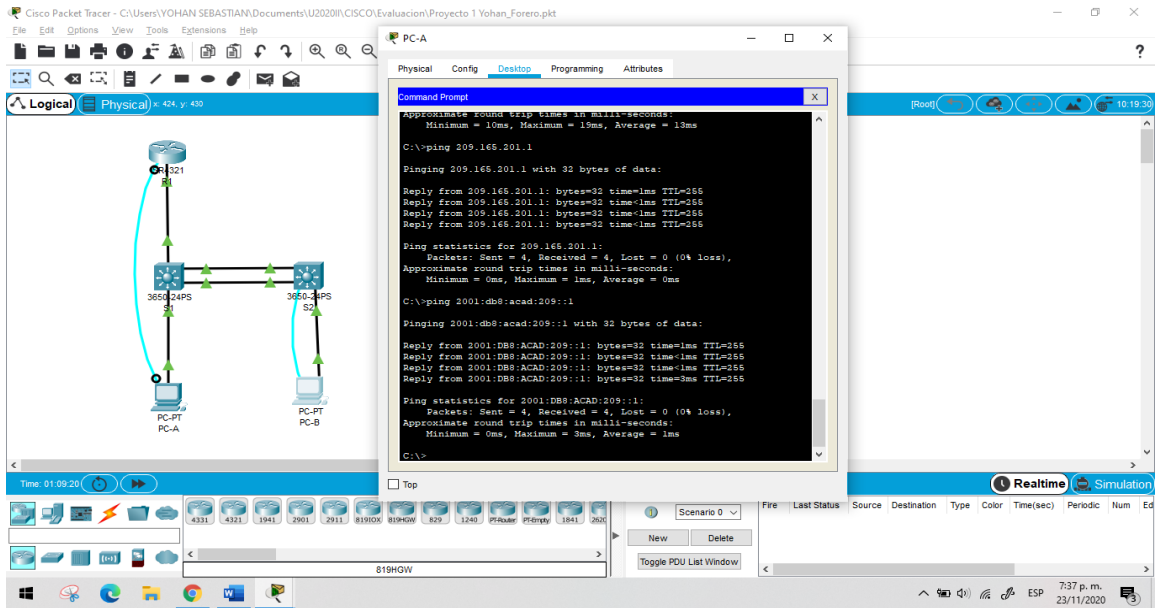
Figura 18. Ping desde PC-A a PC-B en IPv4

En este caso corresponde a la IP 10.19.8.85 y a la dirección IPv6 asignada manualmente 2001:db8:acad:b: :50.



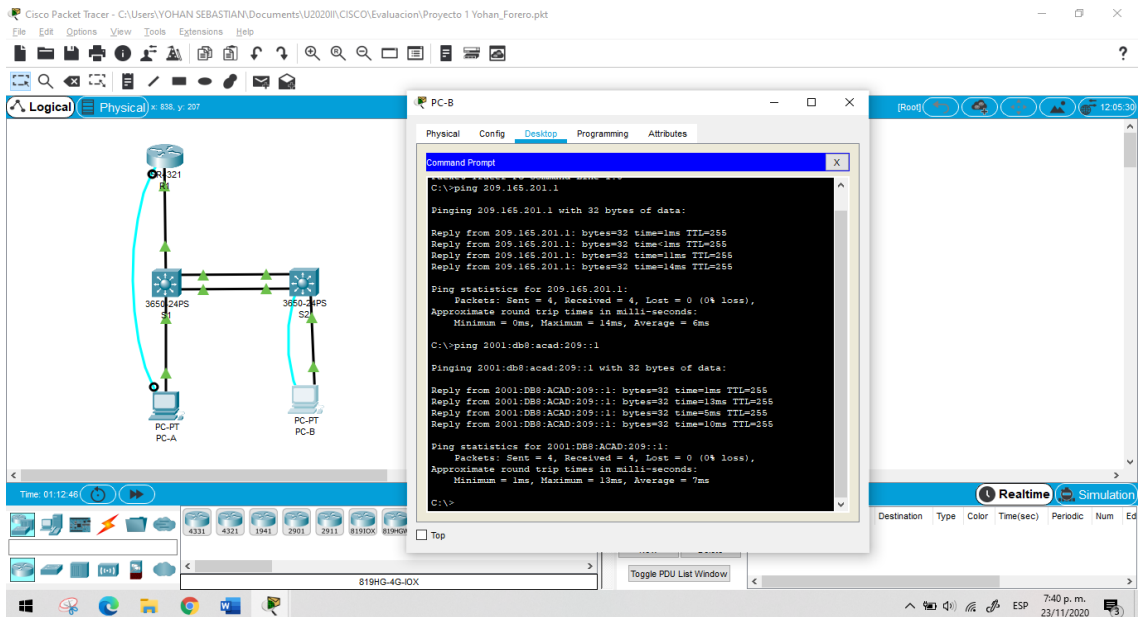
Fuente: Autor

Figura 19. Ping desde PC-A a R1 Bucle 0 en IPV4 e IPV6



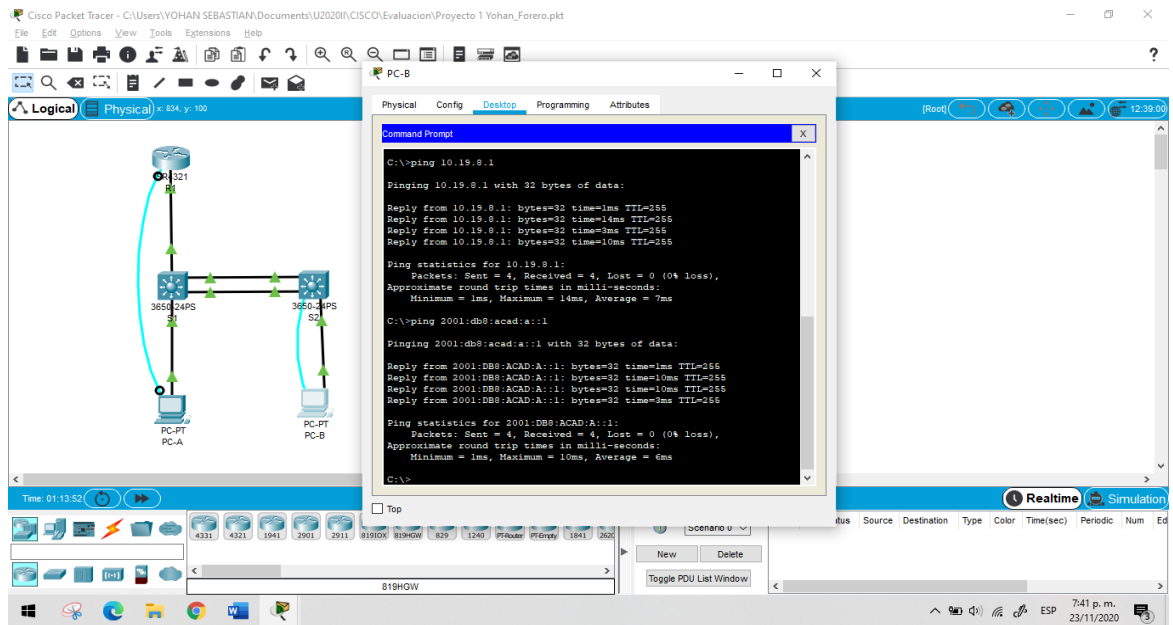
Fuente: Autor

Figura 20. Ping desde PC-B a R1 Bucle 0 en IPV4 e IPV6



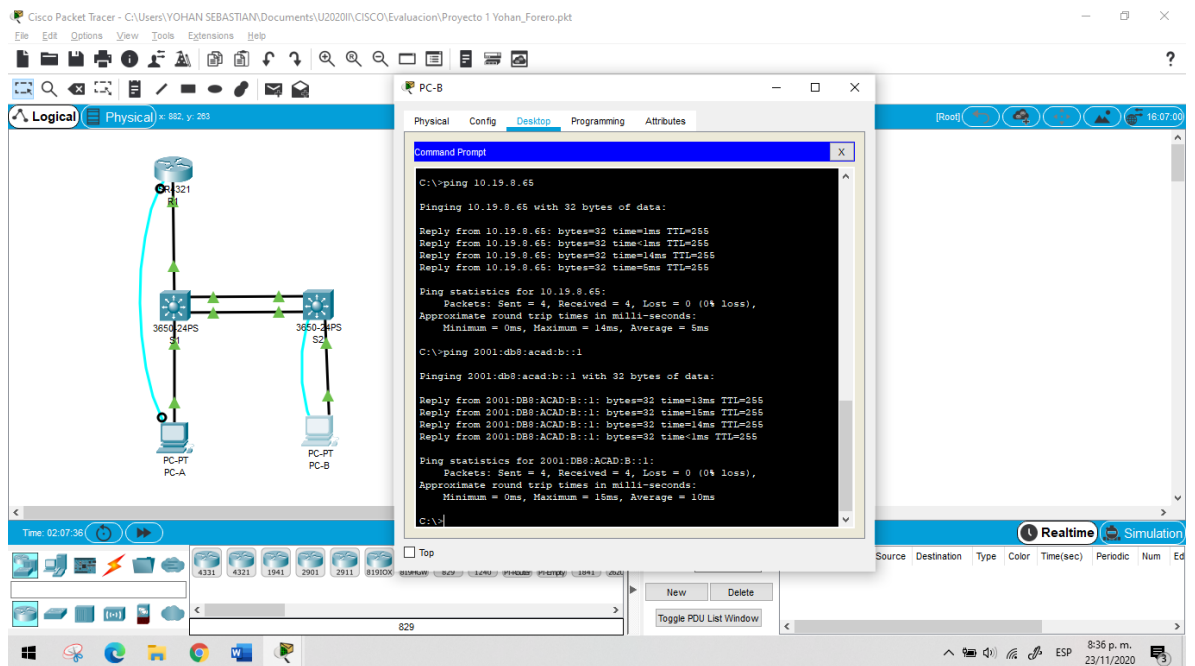
Fuente. Autor

Figura 21. Ping desde PC-B a R1, G0/0/1.2 en IPV4 e IPV6



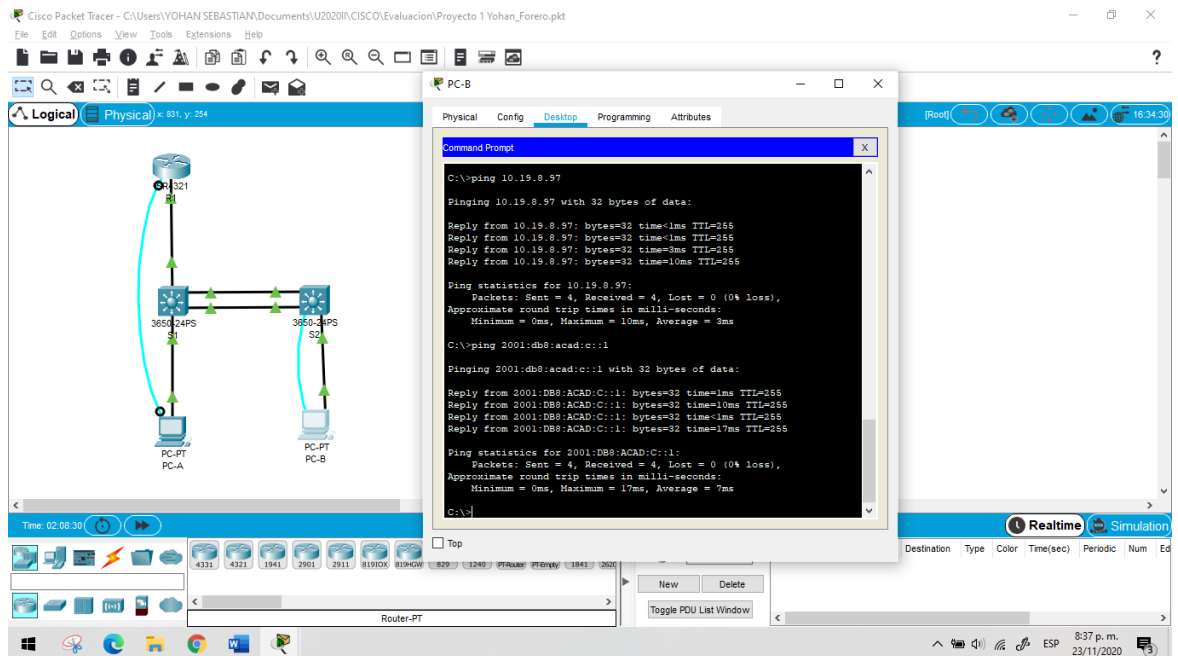
Fuente: Autor

Figura 22. Ping desde PC-B a R1, G0/0/1.3 en IPV4 e IPV6



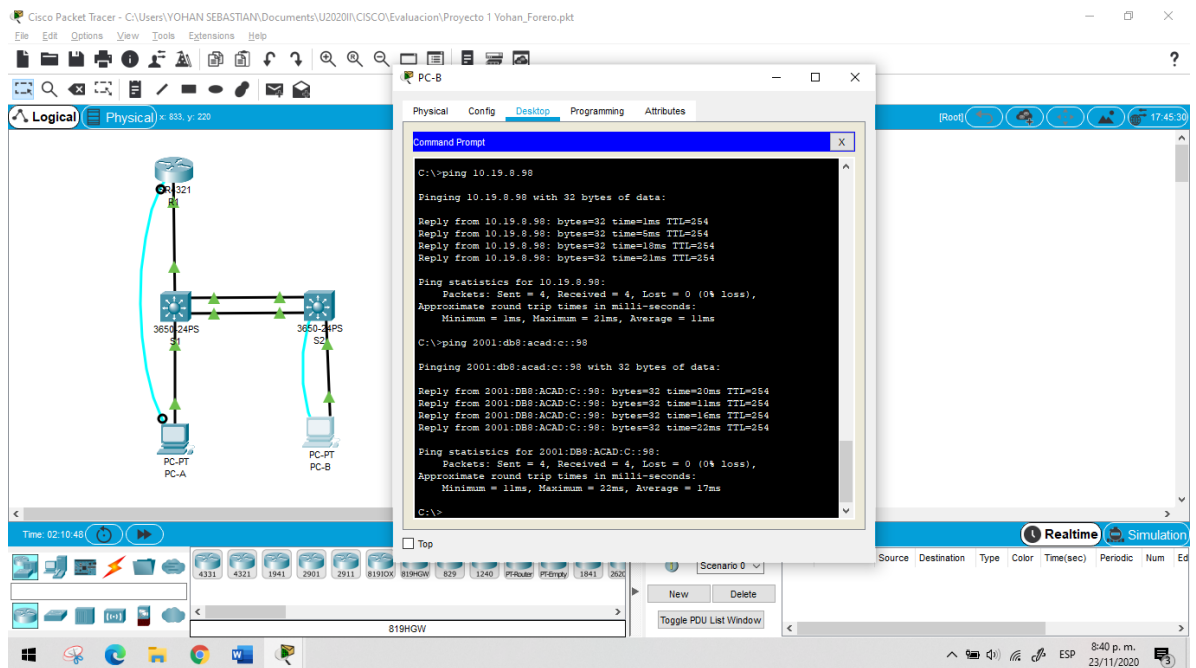
Fuente: Autor

Figura 23. Ping desde PC-B a R1, G0/0/1.4 en IPV4 e IPV6



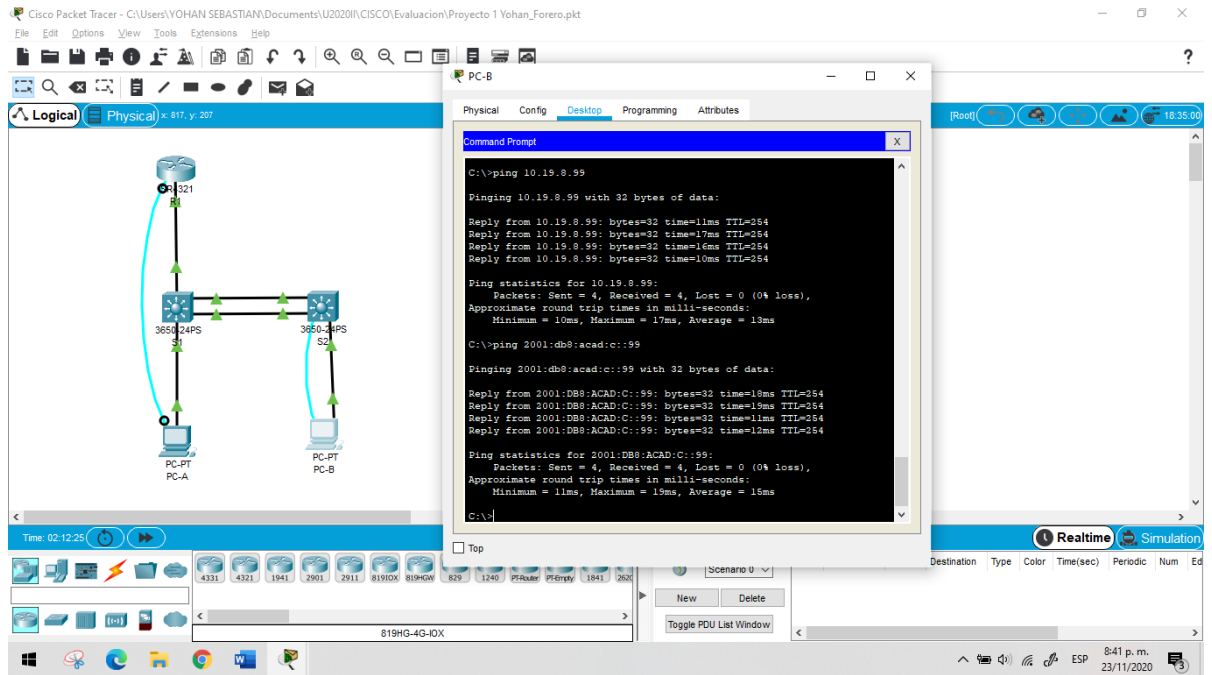
Fuente: Autor

Figura 24. Ping desde PC-B a S1, VLAN 4 en IPV4 e IPV6



Fuente: Autor

Figura 25. Ping desde PC-B a S2, VLAN 4 en IPV4 e IPV6

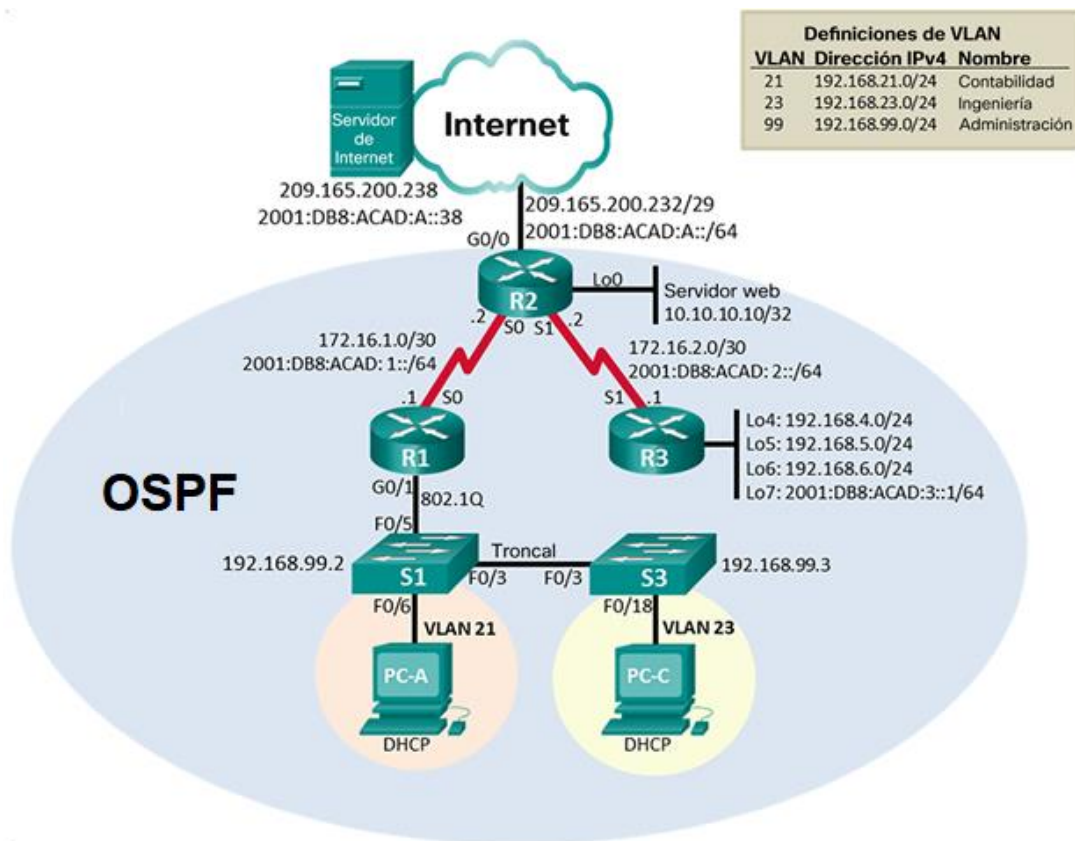


Fuente: Autor

ESCENARIO 2

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

Figura 26. Topología del segundo escenario



Fuente: CISCO

1. Instrucciones

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

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

Parte 2: Configurar los parámetros básicos de los dispositivos

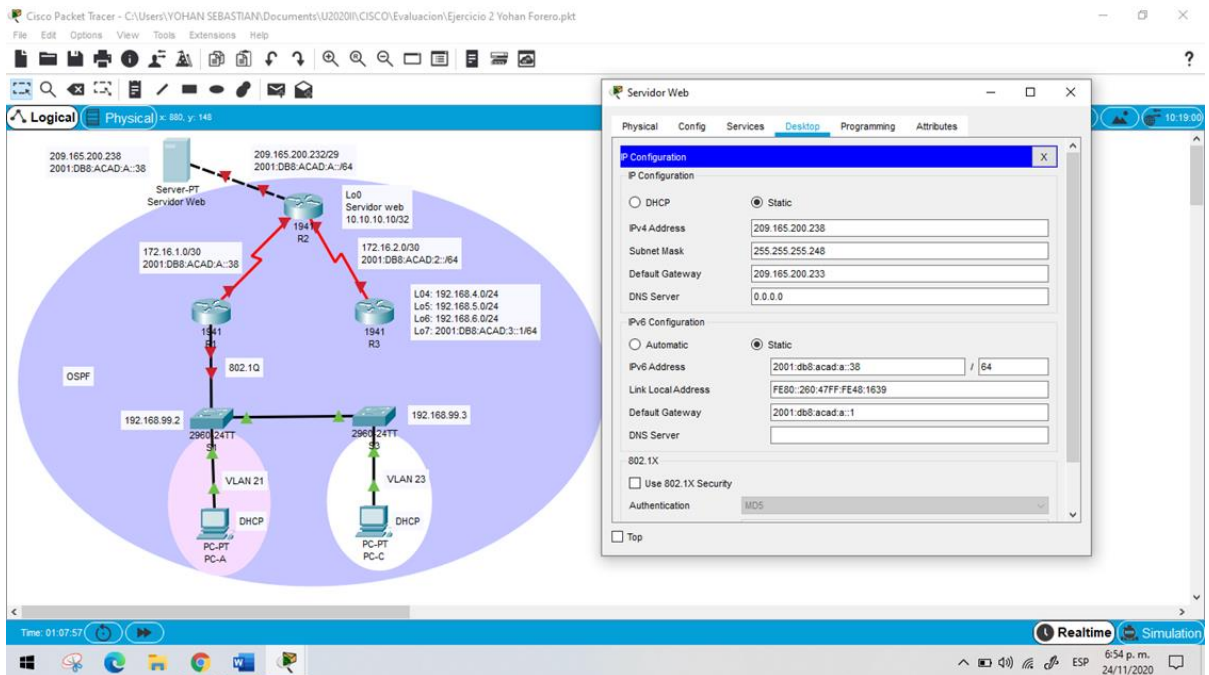
Paso 1: Configurar la computadora de Internet

Para el proceso de configuración del servidor procedo a realizarlo de forma manual en el escritorio en el menú de configuración IP donde realizo la asignación de: dirección IPV4, mascara de red IPV4, Gateway predeterminado IPV4, dirección IPV6 Y Gateway predeterminado IPV6. Las direcciones fueron tomadas de la tabla de direccionamiento. Configuración tabla 12.

Tabla 12. Configurar la 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

Figura 27. Paso 1: Configurar la computadora de Internet



Fuente: Autor

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.

Paso 2: Configurar R1

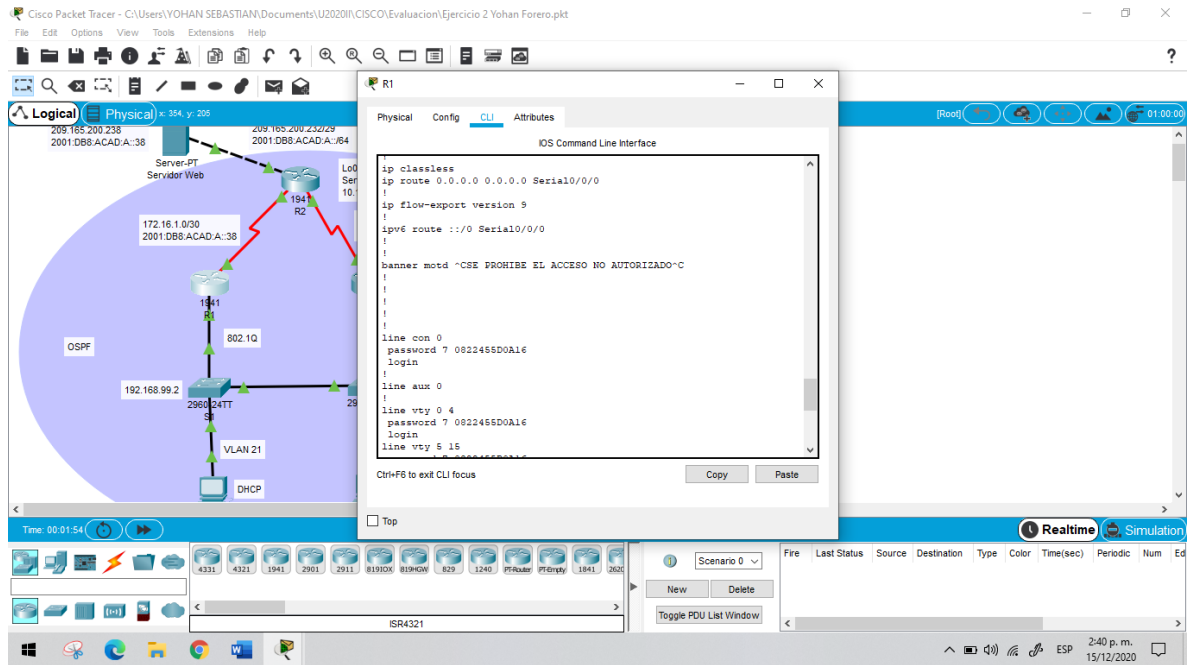
Para el proceso de configuración de R1 comienzo con los siguientes parámetros: desactivo la búsqueda DNS para evitar que el Router busque soluciones por DNS a comandos que ejecutaremos más adelante esto podría generar retrasos en el proceso de configuración, asigno un nombre al Router para poder llevar a cabo una administración más organizada, protocolos de seguridad como lo son la clave de cifrado para el modo EXEC privilegiado y para la consola con esto evito que alguien acceda remotamente a la configuración del Router y a su administración. Evidencia de configuración tabla 13.

Tabla 13. Paso 2: Configurar R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del Router: R1	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada: Class	R1(config)#enable secret class
Contraseña de acceso a la consola: cisco	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet: cisco	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: Se prohíbe el acceso no autorizado.	R1(config)#banner motd %SE PROHIBE EL ACCESO NO AUTORIZADO%

<p>Interfaz S0/0/0</p> <p>Establezca la descripción</p> <p>Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones</p> <p>Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones</p> <p>Establecer la frecuencia de reloj en 128000</p> <p>Activar la interfaz</p>	<pre>R1(config)#int s0/0/0 R1(config-if)#description conexion a R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:a::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown</pre>
<p>Rutas predeterminadas</p> <p>Configurar una ruta IPv4 predeterminada de S0/0/0</p> <p>Configurar una ruta IPv6 predeterminada de S0/0/0</p>	<pre>R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0</pre>

Figura 28. Ejecución comando Show run en R1



Fuente: Autor

Nota: Todavía no se configura G0/1.

Paso 3: configurar R2

Para la configuración de R2 realizo la configuración inicial como en R1 que comprende los parámetros de: desactivar búsqueda DNS, nombre del Router, Contraseña de exec privilegiado y contraseña de acceso a la consola.

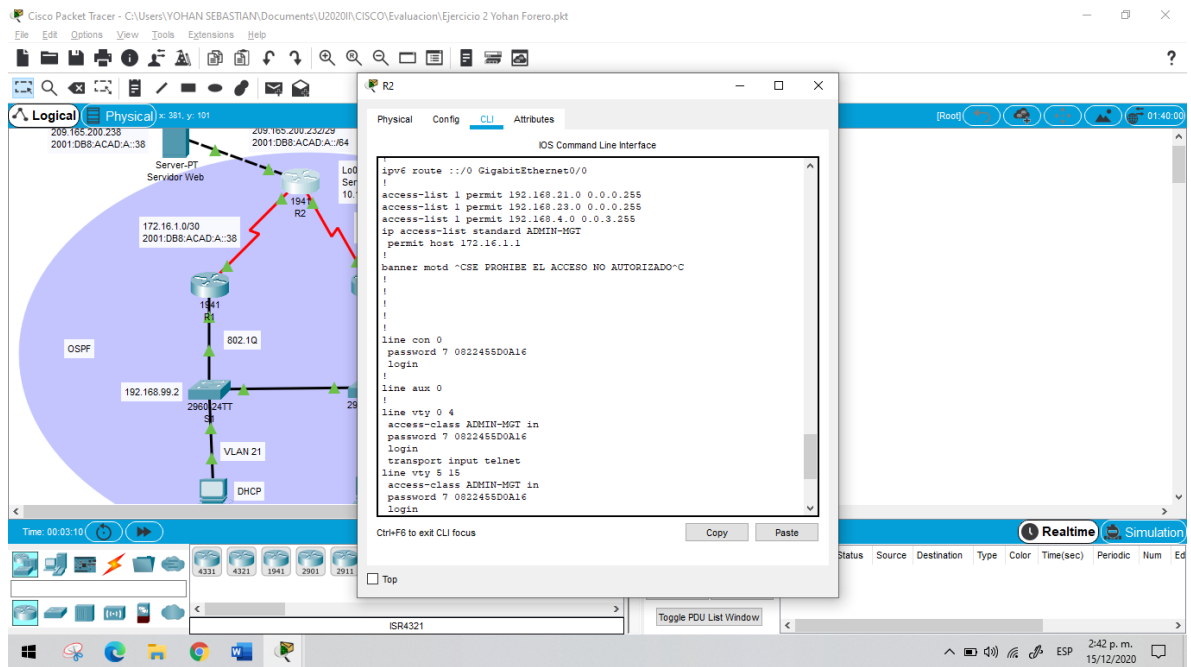
Se habilita el servidor HTTP en el Router, y proceso a realizar la configuración de las interfaces S0/0/0, S0/0/1, G0/0 interfaz de simulación de internet, loopback 0 servidor web simulado con su respectiva asignación de IP según la tabla de direccionamiento, se activan las interfaces configuradas y se establece las rutas predeterminadas IPV4 e IPV6 en la interfaz G0/0. Las configuraciones se encuentran en la tabla 14.

Tabla 14. Paso 3: configurar R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del Router: R2	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada: class	R2(config)#enable secret class
Contraseña de acceso a la consola: cisco	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet: cisco	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	R2(config)#ip http server
Mensaje MOTD: Se prohíbe el acceso no autorizado.	R2(config)#banner motd %SE PROHIBE EL ACCESO NO AUTORIZADO%
<p>Interfaz S0/0/0</p> <p>Establezca la descripción</p> <p>Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.</p> <p>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.</p> <p>Activar la interfaz</p>	<p>R2(config)#int s0/0/0</p> <p>R2(config-if)#description conexion a R1</p> <p>R2(config-if)#ip address 172.16.1.2 255.255.255.252</p> <p>R2(config-if)#ipv6 address 2001:db8:acad:1::2/64</p> <p>R2(config-if)#no shutdown</p>

<p>Interfaz S0/0/1</p> <p>Establecer la descripción</p> <p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <p>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.</p> <p>Establecer la frecuencia de reloj en 128000.</p> <p>Activar la interfaz</p>	<p>R2(config-if)#int s0/0/1</p> <p>R2(config-if)#description conexion a R3</p> <p>R2(config-if)#ip address 172.16.2.2 255.255.255.252</p> <p>R2(config-if)#ipv6 address 2001:db8:acad:2::2/64</p> <p>R2(config-if)#clock rate 128000</p> <p>R2(config-if)#no shutdown</p>
<p>Interfaz G0/0 (simulación de Internet) Establecer la descripción.</p> <p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <p>Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred.</p> <p>Activar la interfaz</p>	<p>R2(config-if)#int g0/0</p> <p>R2(config-if)#description conexión a internet</p> <p>R2(config-if)#ip address 209.165.200.233 255.255.255.248</p> <p>R2(config-if)#ipv6 address 2001:db8:acad:a::1/64</p> <p>R2(config-if)#no shutdown</p>
<p>Interfaz loopback 0 descripción : servidor web simulado Establecer la descripción. Establezca la dirección IPv4.</p>	<p>R2(config-if)#int loopback 0</p> <p>R2(config-if)#description simulador del servidor web</p> <p>R2(config-if)#ip address 10.10.10.10 255.255.255.255</p>
<p>Ruta predeterminada Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.</p>	<p>R2(config)# ip route 0.0.0.0 0.0.0.0 g0/0</p> <p>R2(config)#ipv6 route ::/0 g0/0</p>

Figura 29. Ejecución comando show run en R2



Fuente: Autor

Paso 4: configurar R3

Para la configuración de R2 realizo la configuración inicial como en R1 que comprende los parámetros de: desactivar búsqueda DNS, nombre del Router, Contraseña de exec privilegiado y contraseña de acceso a la consola.

Proceso a realizar la configuración de la interfaz S0/0/1 con los siguientes parámetros: añado la descripción, establezco la dirección IPV4 e IPV6 y activo la interfaz. Para las interfaces Loopback 4 – 6 establezco que usen la primera dirección IP de la subred en la que se ubican, para Loopback 7 se establezco dirección IPV6. Proceso de configuración tabla 15.

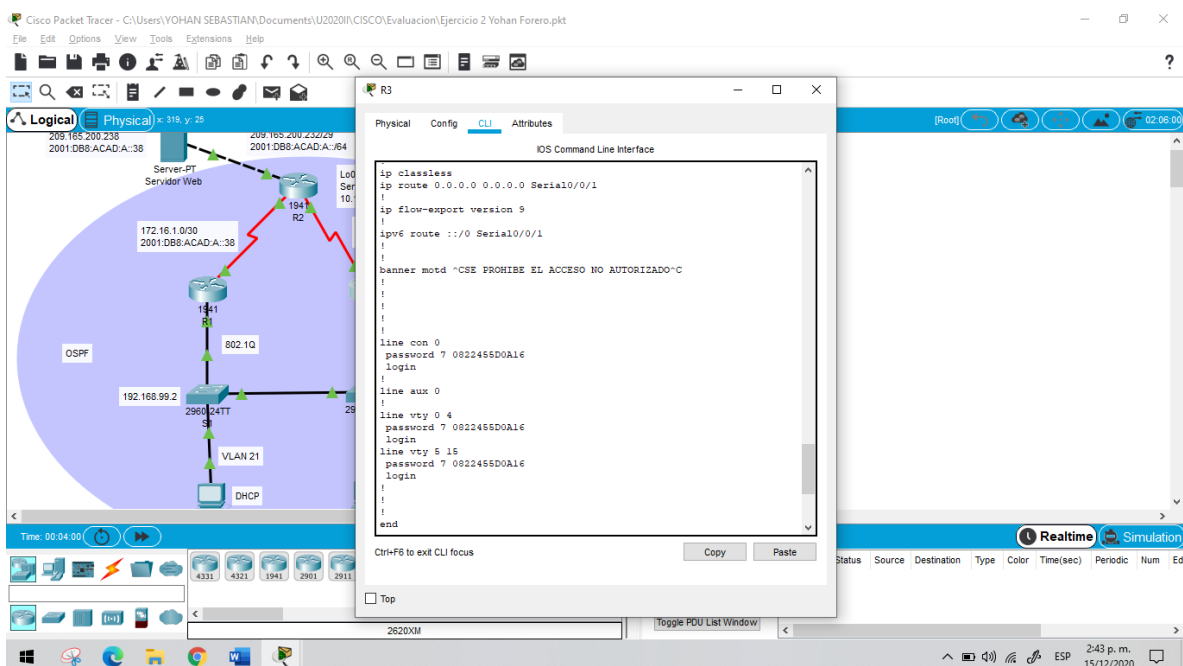
Tabla 15. Paso 4: configurar R3.

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

Contraseña de exec privilegiado cifrada: class	R3(config)#enable secret class
Contraseña de acceso a la consola: cisco	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet: cisco	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: Se prohíbe el acceso no autorizado.	R3(config)#banner motd %SE PROHIBE EL ACCESO NO AUTORIZADO%
Interfaz S0/0/1 Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	R3(config)#int s0/0/1 R3(config-if)#description conexión a R2 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 shutdown
Interfaz loopback 4 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred	R3(config-if)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred	R3(config-if)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred	R3(config-if)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0

<p>Interfaz loopback 7 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.</p>	<p>R3(config-if)#int loopback 7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64</p>
<p>Rutas predeterminadas para IPV4 e IPV6. Interfaz S0/0/1</p>	<p>R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1</p>

Figura 30. Ejecución comando show run en R3



Fuente: Autor

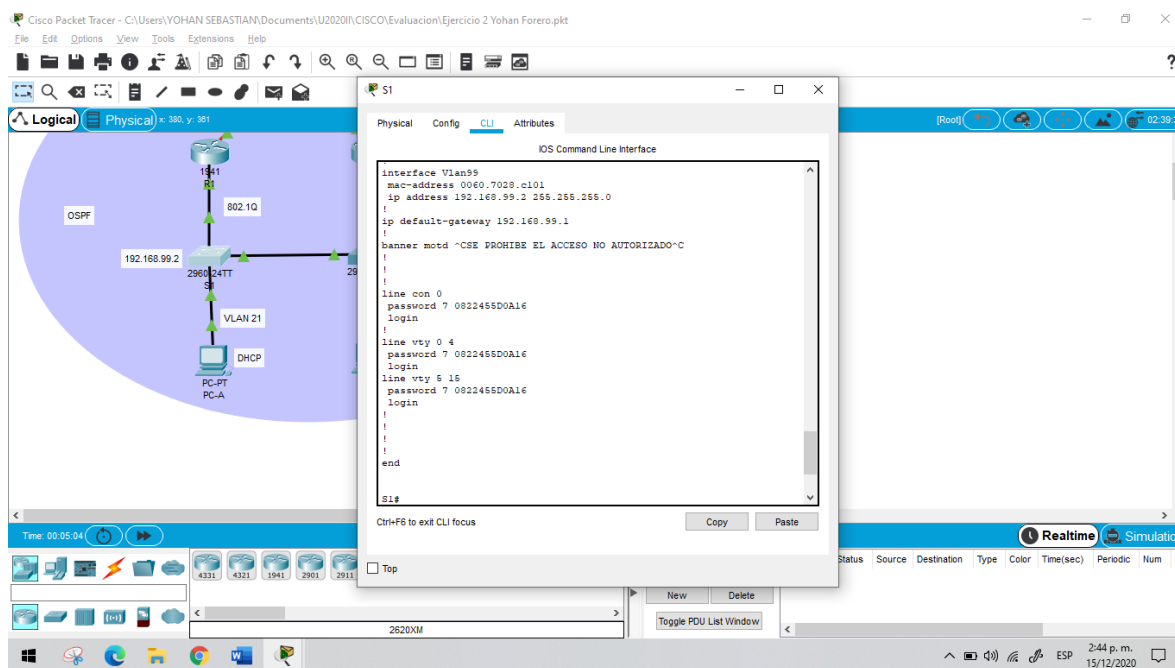
Paso 5: Configurar S1

Para la configuración de S2 realizo la configuración inicial como en R1 que comprende los parámetros de: desactivar búsqueda DNS, nombre del Router, Contraseña de exec privilegiado y contraseña de acceso a la consola, cifrado de las contraseñas de texto no cifrado y mensaje de Motd Banner. Configuración tabla 16.

Tabla 16. Paso 5: Configurar S1

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

Figura 31. Ejecución comando show run en S1



Fuente: Autor

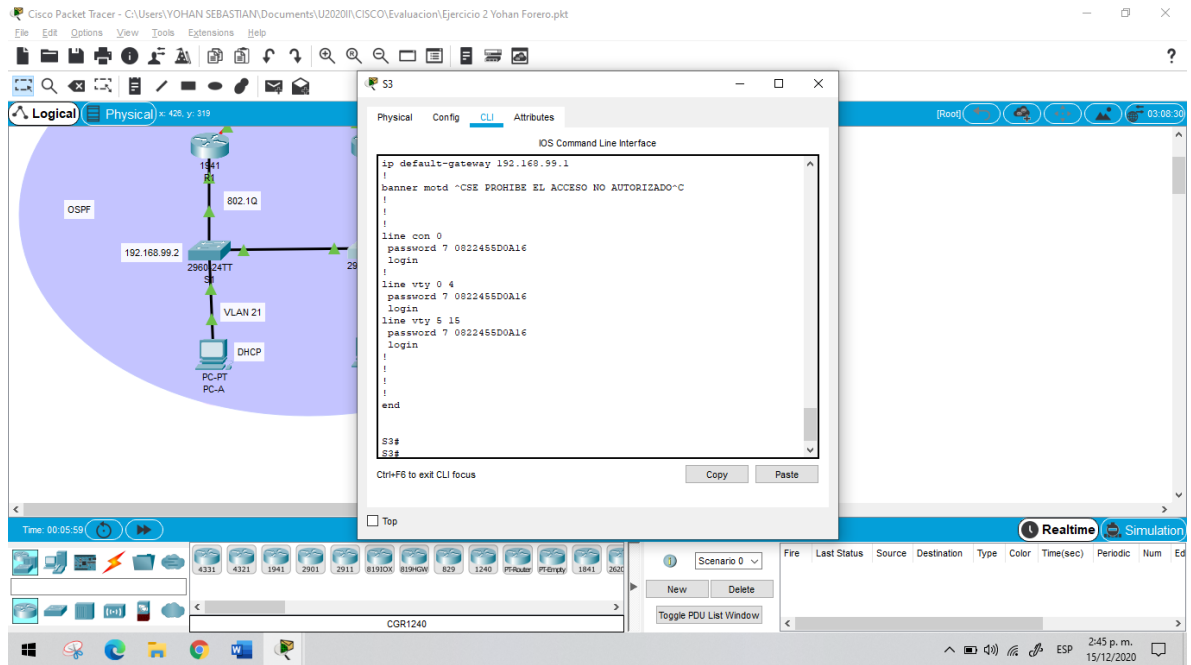
Paso 6: Configurar S3:

Para la configuración de S3 realizo la configuración inicial como en R1 que comprende los parámetros de: desactivar búsqueda DNS, nombre del Router, Contraseña de exec privilegiado y contraseña de acceso a la consola, cifrado de las contraseñas de texto no cifrado y mensaje de Motd Banner. Configuración tabla 17.

Tabla 17. Paso 6: Configurar S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch: S2	Switch(config)#hostname S2
Contraseña de exec privilegiado cifrada: class	S2(config)#enable secret class
Contraseña de acceso a la consola: cisco	S2(config)#line console 0 S2(config-line)#password cisco S2(config-line)#login
Contraseña de acceso Telnet: cisco	S2(config-line)#line vty 0 15 S2(config-line)#password cisco S2(config-line)#login
Cifrar las contraseñas de texto no cifrado	S2(config-line)#service password-encryption
Mensaje MOTD: Se prohíbe el acceso no autorizado.	S2(config)#banner motd %SE PROHIBE EL ACCESO NO AUTORIZADO%

Figura 32. Ejecución comando show run en S3



Fuente: Autor

Paso 7: Verificar la conectividad de la red

Para el proceso de verificación de conectividad usare el comando Ping entre los Routers y servidor mencionados en la siguiente tabla. Si la configuración se ha realizado de manera correcta todos los pings deberán ser correctos.

Tabla 18. Paso 7: Verificar la conectividad de la red

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

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

Capturas de pantalla de pings realizados

Las figuras 18,19 y 20 tienen como evidencia los pings realizados en la tabla 18, donde podemos visualizar la conexión establecido de manera correcta.

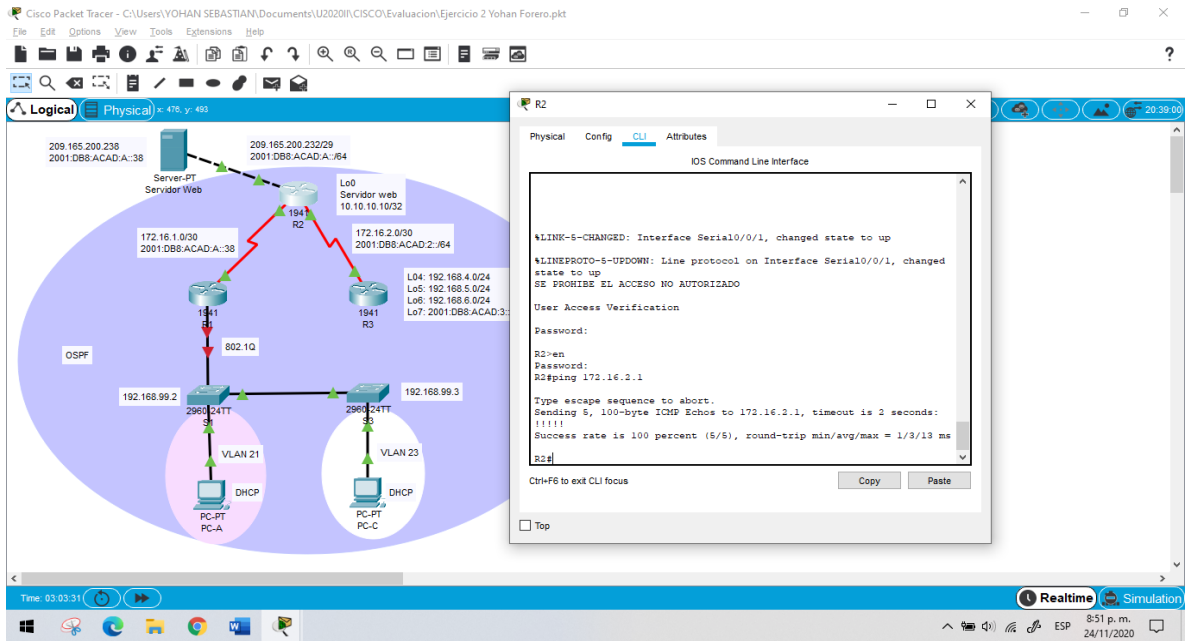
Figura 33. Ping desde R1 a R2 S0/0/0

The screenshot shows the Cisco Packet Tracer interface. On the left, a network diagram is visible with several routers (R1, R2, R3) and servers. R1 is connected to R2, and R2 is connected to R3. R1 is also connected to a switch (S1) which is connected to PC-A. R2 is connected to a switch (S2) which is connected to PC-C. The diagram includes labels for IP addresses and interface configurations. On the right, a CLI window for R1 is open, showing the output of a ping command. The output indicates that the ping was successful with a 100% success rate and a round-trip time of 1/4/18 ms.

```
SE PROHIBE EL ACCESO NO AUTORIZADO
User Access Verification
Password:
Password:
R1>en
R1#ping 172.16.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/18 ms
R1#
```

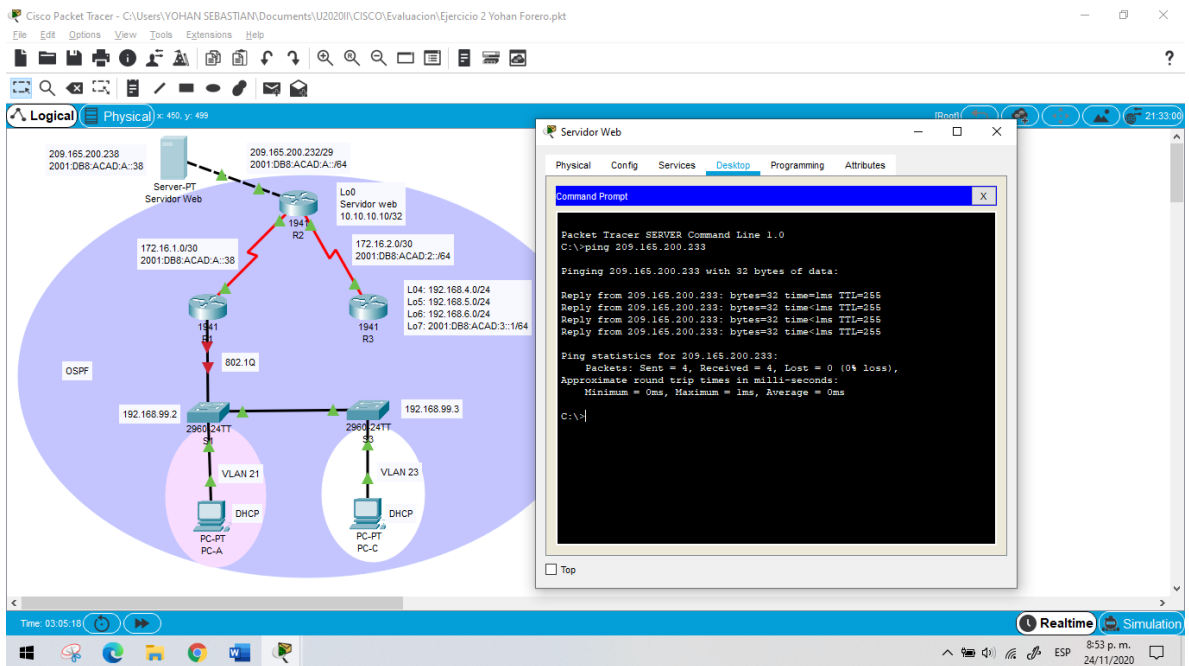
Fuente: Autor

Figura 34. Ping desde R2 a R3 S0/0/1



Fuente: Autor

Figura 35. Ping desde Servidor de internet a Gateway predeterminado



Fuente: Autor

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

Paso 1: Configurar S1

Realizo la creación de la base de datos de VLAN que se usaran de la siguiente forma: VLAN 21 corresponde a Contabilidad, VLAN 23 corresponde a ingeniería y VLAN 99 corresponde a Administración. Continuo con la asignación de la dirección IP a VLAN de administración y su respectivo Gateway predeterminado en este caso va a ser la primera dirección IP.

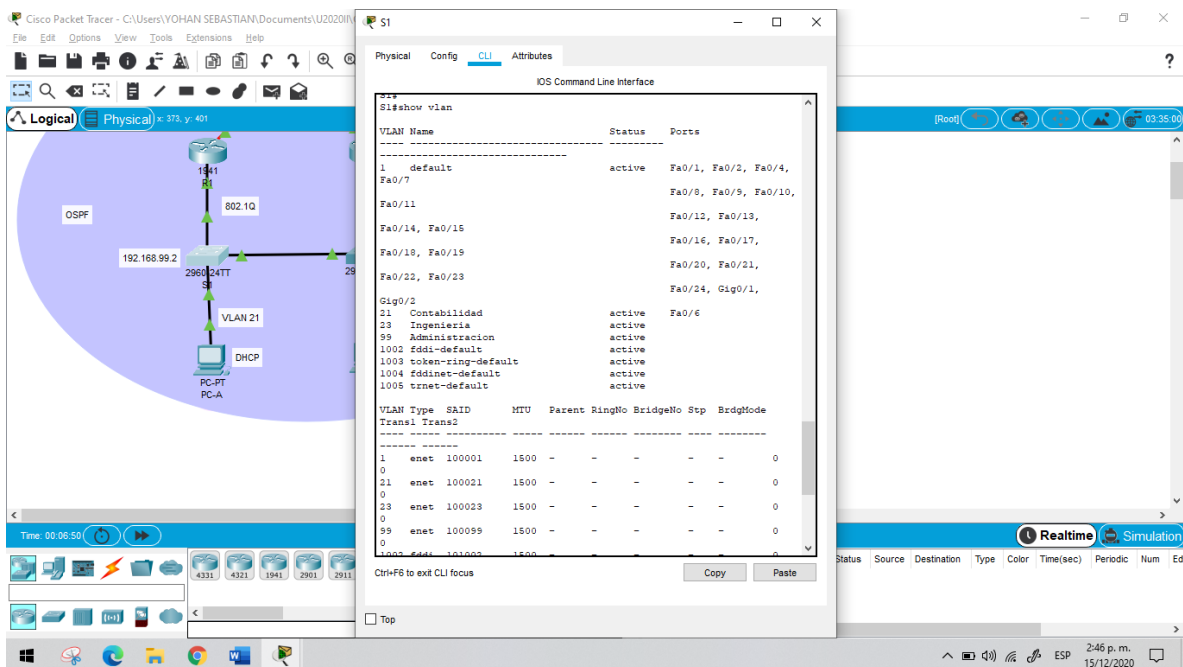
Asigno a las interfaces F0/3 y F0/5 el enlace troncal para que use la VLAN 1 como nativa, el resto de los puertos los configuro como puertos de acceso usando el comando interface range. Asigno la interfaz F0/6 puerto de acceso a la VLAN 21 y se procede a apagar las interfaces sin usar. Las anteriores configuraciones se evidencian en la tabla 19.

Tabla 19. Paso 1: Configurar S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN. Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican.	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administración
Asignar la dirección IP de administración. Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología	S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Asignar el gateway predeterminado Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.	S1(config)#ip default-gateway 192.168.99.1

Forzar el enlace troncal en la interfaz F0/3 Utilizar la red VLAN 1 como VLAN nativa	S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
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 Utilizar 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-range)#int f0/6 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

Figura 36. Ejecución comando Show vlan en S1



Fuente: Autor

Paso 2: Configurar el S3

Realizo la creación de la base de datos de VLAN que se usaran de la siguiente forma: VLAN 21 corresponde a Contabilidad, VLAN 23 corresponde a ingeniería y VLAN 99 corresponde a Administración. Continuo con la asignación de la dirección IP a VLAN de administración y su respectivo Gateway predeterminado en este caso va a ser la primera dirección IP.

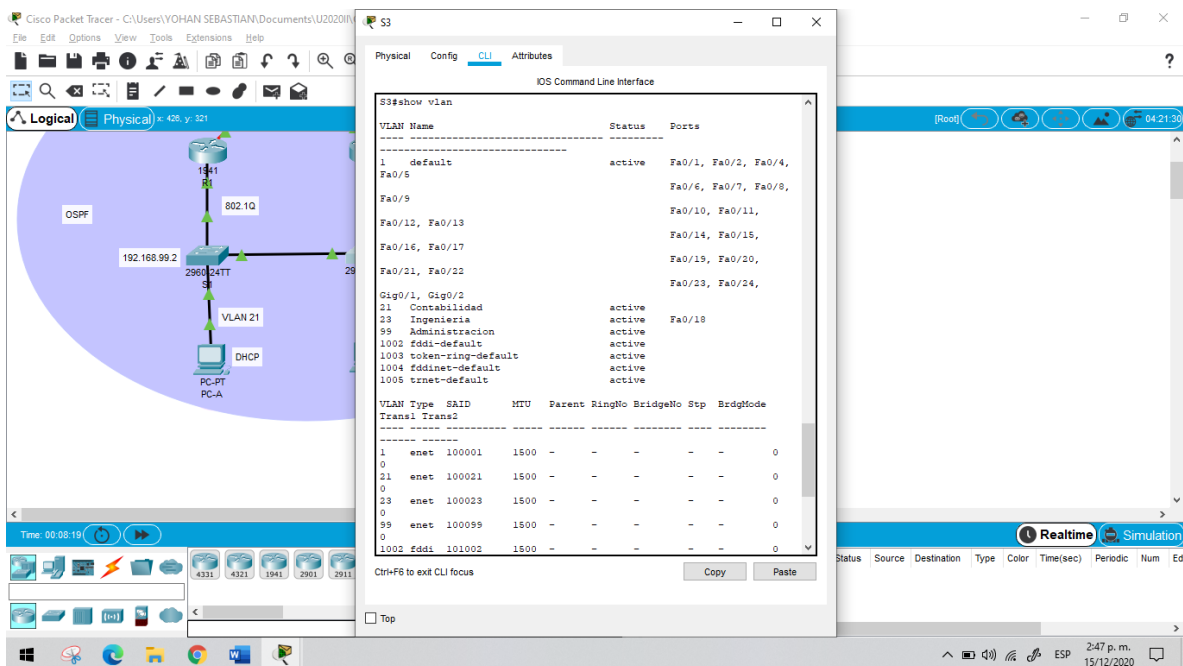
Asigno a las interfaces F0/3 el enlace troncal para que use la VLAN 1 como nativa, el resto de los puertos los configuro como puertos de acceso usando el comando interface range. Asigno la interfaz F0/18 puerto de acceso a la VLAN 23 y se procede a apagar las interfaces sin usar. Las anteriores configuraciones se evidencian en la tabla 20.

Tabla 20. Paso 2: Configurar el S3.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#Vlan 23 S3(config-vlan)#Name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administración
Asignar la dirección IP de administración Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología	S3(config)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
Asignar el gateway predeterminado. Asignar la primera dirección IP en la subred como gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3 Utilizar la red VLAN 1 como VLAN nativa	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso Utilizar el comando interface range	S3(config-if)#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

Figura 37. Ejecución comando Show vlan en S3



Fuente: Autor

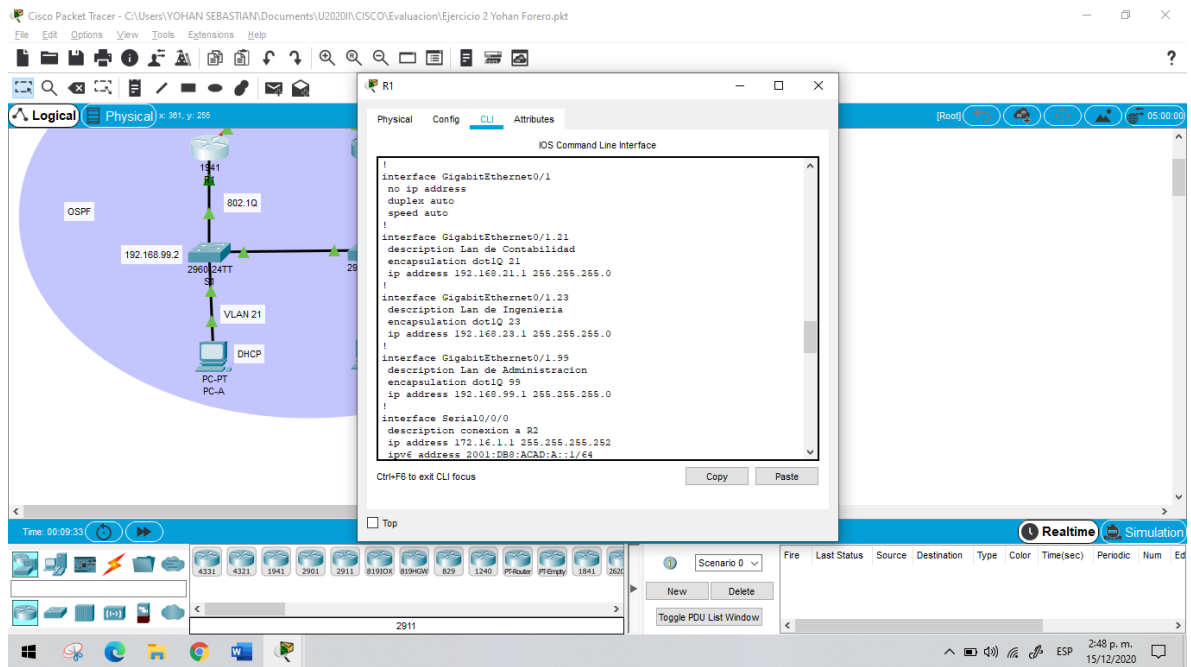
Paso 3: Configurar R1

En este paso realizo el procedimiento de configuración y troncales de las subinterfaces en el puerto G0/1, el encapsulamiento queda de la siguiente forma: g0/1.21 para contabilidad, g0/1.23 para ingeniería y g0/1.99 para administración. Cada interfaz se configuró con la primera dirección IP disponible de la interfaz. Por último, proceso a activar la interfaz G0/1. Evidencia de configuración tabla 21.

Tabla 21. Paso 3: Configurar R1

Elemento o tarea de configuración	Especificación
<p>Configurar la subinterfaz 802.1Q .21 en G0/1</p> <p>Descripción: LAN de Contabilidad</p> <p>Asignar la VLAN 21</p> <p>Asignar la primera dirección disponible a esta interfaz</p>	<p>R1(config)#int g0/1.21</p> <p>R1(config-subif)#description Lan de Contabilidad</p> <p>R1(config-subif)#encapsulation dot1q 21</p> <p>R1(config-subif)#ip address 192.168.21.1 255.255.255.0</p>
<p>Configurar la subinterfaz 802.1Q .23 en G0/1</p> <p>Descripción: LAN de Ingeniería</p> <p>Asignar la VLAN 23</p> <p>Asignar la primera dirección disponible a esta interfaz</p>	<p>R1(config-subif)#int g0/1.23</p> <p>R1(config-subif)#description Lan de Ingeniería</p> <p>R1(config-subif)#encapsulation dot1q 23</p> <p>R1(config-subif)#ip address 192.168.23.1 255.255.255.0</p>
<p>Configurar la subinterfaz 802.1Q .99 en G0/1</p> <p>Descripción: LAN de Administración</p> <p>Asignar la VLAN 99</p> <p>Asignar la primera dirección disponible a esta interfaz</p>	<p>R1(config-subif)#int g0/1.99</p> <p>R1(config-subif)#description Lan de Administración</p> <p>R1(config-subif)#encapsulation dot1q 99</p> <p>R1(config-subif)#ip address 192.168.99.1 255.255.255.0</p>
<p>Activar la interfaz G0/1</p>	<p>R1(config-subif)#int g0/1</p> <p>R1(config-if)#no shutdown</p>

Figura 38. Verificación de subinterfaces en R1



Fuente: Autor

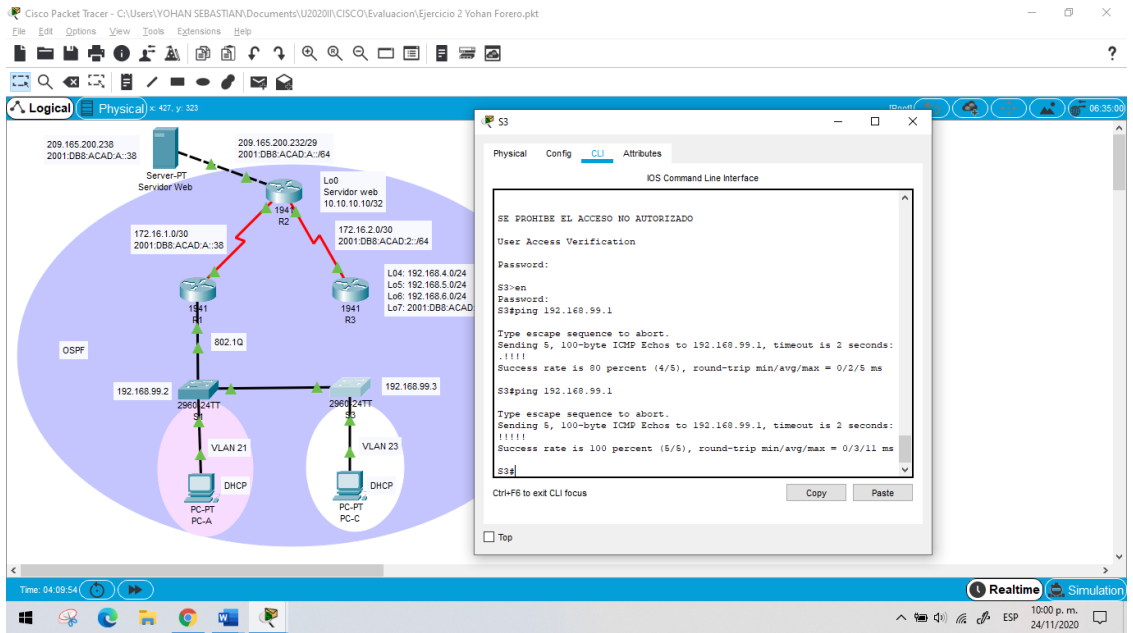
Paso 4: Verificar la conectividad de la red

Para el proceso de verificación de conectividad usare el comando Ping entre los Switches y Routers mencionados en la siguiente tabla. Si la configuración se ha realizado de manera correcta todos los pings deberán ser correctos.

Tabla 22. Paso 4: Verificar la conectividad de la red

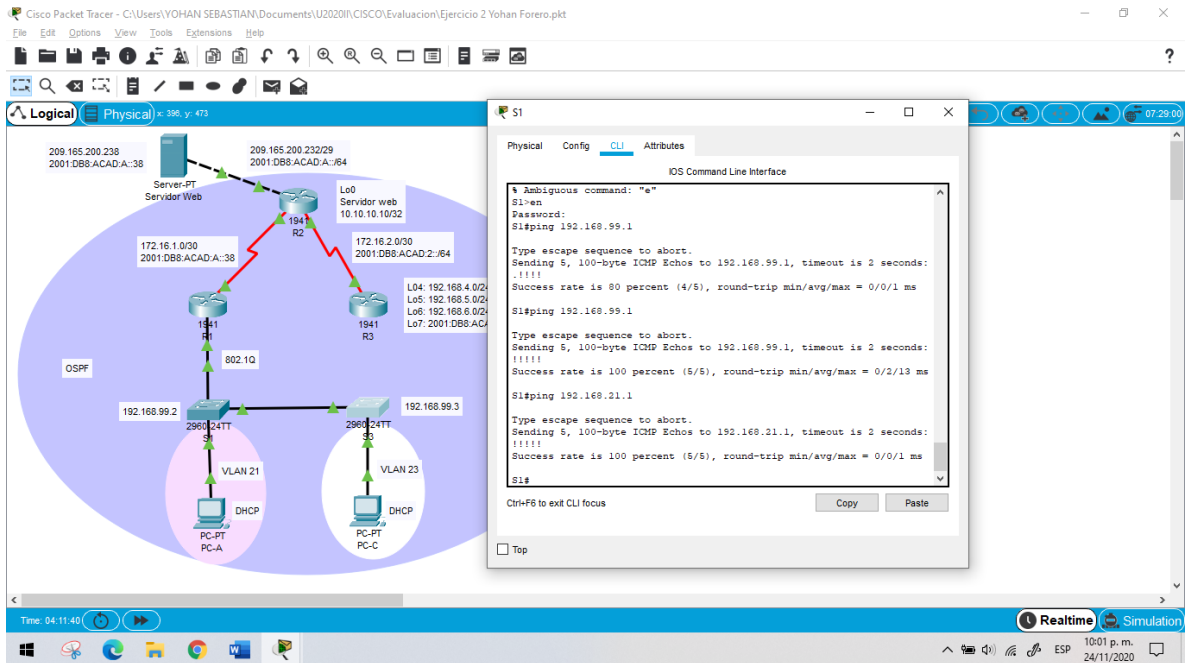
Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Correcto
S3	R1, dirección VLAN 99	192.168.99.1	Correcto
S1	R1, dirección VLAN 21	192.168.21.1	Correcto
S3	R1, dirección VLAN 23	192.168.23.1	Correcto

Figura 40. Ping desde S3 a R1, dirección VLAN 99



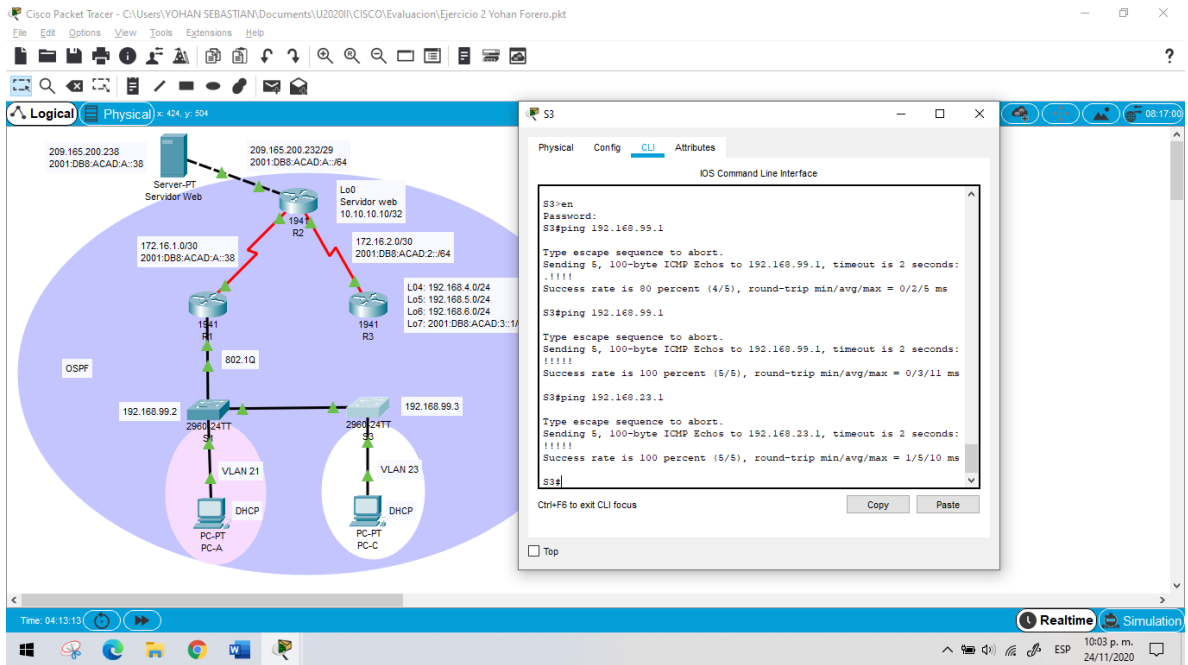
Fuente: Autor

Figura 41. Ping desde S1 a R1, dirección VLAN 21



Fuente: Autor

Figura 42. Ping desde S3 a R1, dirección VLAN 23



Fuente: Autor

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Procedo a configurar el protocolo OSPF en el Router con su respectivo id que nos ayudara a la gestión de red, asigno y anuncio las redes conectadas directamente al área 0. Para verificar las redes conectadas podemos hacerlo por medio del comando: #do show ip route connected, por último, establezco todas las interfaces como pasivas y se desactiva la somatización automática.

Tabla 23. Paso 1: Configurar OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1 R2(config-router)#router-id 1.1.1.1

Anunciar las redes conectadas directamente Asigne todas 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 área 0 R1(config-router)#network 192.168.99.0 0.0.0.255 área 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

Paso 2: Configurar OSPF en el R2

Procedo a configurar el protocolo OSPF en el Router con su respectivo id que nos ayudara a la gestión de red, asigno y anuncio las redes conectadas directamente al área 0 omitiendo la red G0/0. Para verificar las redes conectadas podemos hacerlo por medio del comando: #do show ip route connected, por último, establezco todas las interfaces Loopback como pasiva y se desactiva la sumarización automática.

Tabla 24. Paso 2: Configurar OSPF en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2
Anunciar las redes conectadas directamente. Omitir la red G0/0.	R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 área 0 R2(config-router)#network 172.16.1.0 0.0.0.3 área 0 R2(config-router)#network 172.16.2.0 0.0.0.3 área 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0

Desactive la sumarización automática.	R2(config-router)#no auto-summary
---------------------------------------	-----------------------------------

Paso 3: Configurar OSPFv3 en el R2

Procedo a configurar el protocolo OSPF en el Router con su respectivo id que nos ayudara a la gestión de red, asigno y anuncio las redes conectadas directamente al área 0. Para verificar las redes conectadas podemos hacerlo por medio del comando: #do show ip route connected, por último, establezco todas las interfaces de Loopback como pasivas y se desactiva la sumarización automática.

Tabla 25. Paso 3: Configurar OSPFv3 en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 1 R3(config-router)#router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 área 0 R3(config-router)#network 192.168.5.0 0.0.0.255 área 0 R3(config-router)#network 192.168.6.0 0.0.0.255 área 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

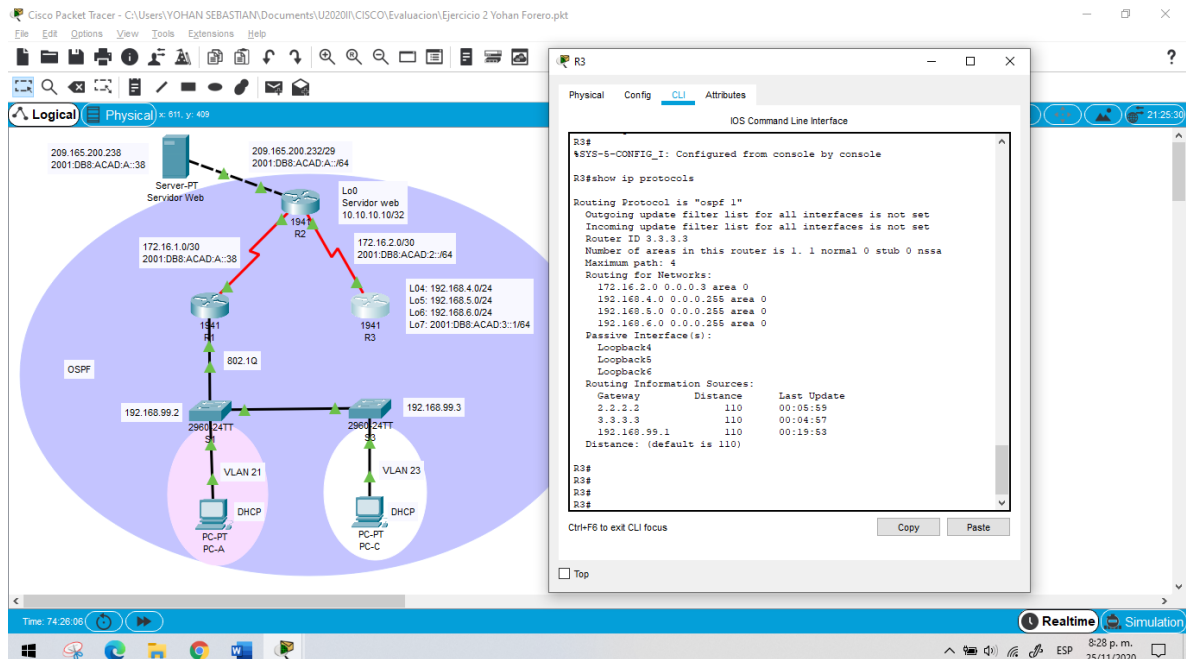
Paso 4: Verificar la información de OSPF

Para el proceso de verificación de la información de los Routers usaremos los siguientes comandos que nos servirán para visualizar configuraciones, protocolos, interfaces, rutas, etc. que hayamos realizado en cada Router.

Tabla 26. Paso 4: Verificar la información de OSPF

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

Figura 43. Ejecución comando R3#show ip protocols



Fuente: Autor

Figura 44. Ejecución de comando R3#show ip route OSPF

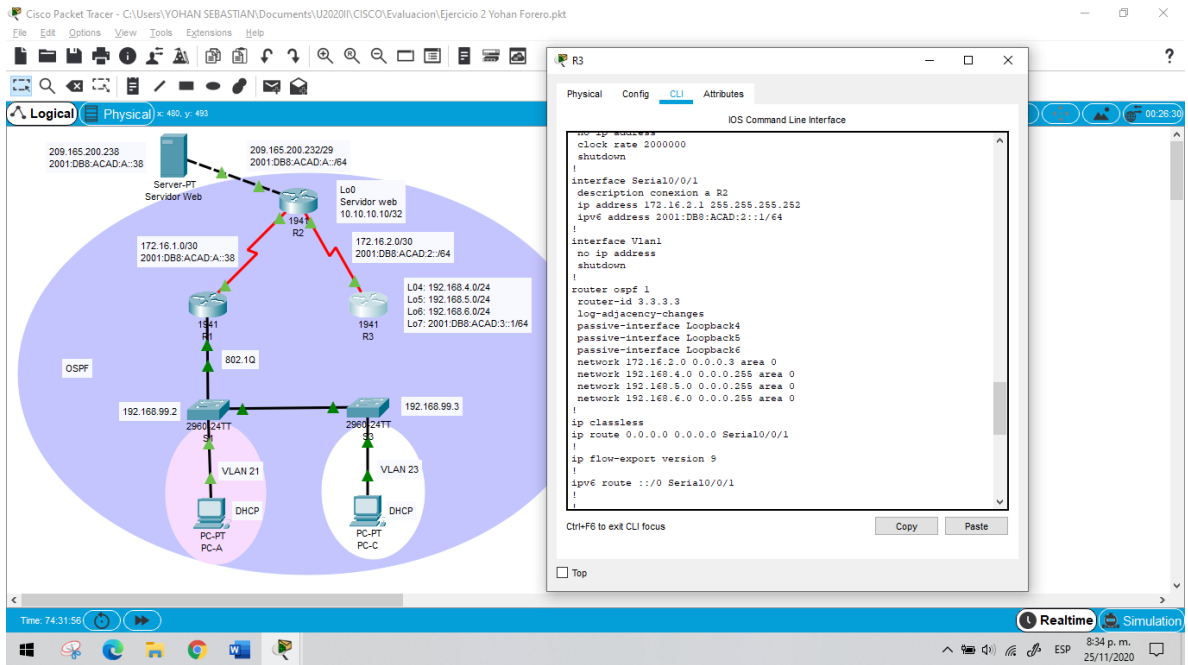
The screenshot shows a Cisco Packet Tracer environment with a network diagram and a CLI window for router R3. The network diagram includes several routers (R1, R2, R3), servers (Server-PT, Server Web), and PCs (PC-A, PC-C) connected via VLANs and DHCP. The CLI window displays the output of the command 'show ip route ospf' on router R3.

```

R3#
R3#
R3#
R3#show ip route ospf
  10.0.0.0/32 is subnetted, 1 subnets
O    10.10.10.10 [110/65] via 172.16.2.2, 00:07:11, Serial0/0/1
O   172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O   172.16.1.0 [110/128] via 172.16.2.2, 00:07:11, Serial0/0/1
O  192.168.21.0 [110/128] via 172.16.2.2, 00:07:11, Serial0/0/1
O  192.168.23.0 [110/128] via 172.16.2.2, 00:07:11, Serial0/0/1
O  192.168.99.0 [110/128] via 172.16.2.2, 00:07:11, Serial0/0/1
R3#
  
```

Fuente: Autor

Figura 45. Ejecución del comando R3#show run.



Fuente: Autor

Parte 5: Implementar DHCP y NAT para IPv4

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

Para el proceso de configuración de R1 como servidor DHCP para las VLAN 21 Y 23 proceso a realizar las siguientes configuraciones: reservo las primeras 20 direcciones IP en ambas VLAN que se usaran para configuraciones estáticas, realizo la creación del Pool DHCP que es el encargado de asignar las direcciones, configuro la dirección IP del servidor DNS, asigno nombre del dominio y establezco el Gateway predeterminado, las configuraciones se evidencian en la tabla 27.

Tabla 27. Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

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

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

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

Para el proceso de implementación del servicio NAT que es el encargado de realizar la traducción de las direcciones IP para hacer que las conexiones se realicen ejecutare los siguientes pasos: creo una base de datos local con el respectivo usuario y contraseña, habilito el servicio HTTP y lo configuro para que use la base de datos local de autenticación al momento del acceso, creamos el servicio de NAT estática al servidor con la IP 209.165.200.237, asigno las interfaces internas y externas para el servicio de NAT estática, configuro el servicio de NAT dinámico dentro del ACL privado para permitir la traducción de las redes de Contabilidad y de Ingeniería en el R3 y defino el pool o segmento de direcciones IP públicas que usara el servicio. Las configuraciones se evidencian en la tabla 28.

Tabla 28. Paso 2: Configurar la NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
<p>Crear una base de datos local con una cuenta de usuario Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15</p>	<p>R2(config)#username webuser privilege 15 secret cisco12345</p>
<p>Habilitar el servicio del servidor HTTP</p>	<p>R2(config)#ip http server</p>
<p>Configurar el servidor HTTP para utilizar la base de datos local para la autenticación</p>	<p>R2(config)#ip http authentication local</p>
<p>Crear una NAT estática al servidor web. Dirección global interna: 209.165.200.237</p>	<p>R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237</p>
<p>Asignar la interfaz interna y externa para la NAT estática</p>	<p>R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside</p>
<p>Configurar la NAT dinámica dentro de una ACL privada Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3</p>	<p>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</p>

Defina el pool de direcciones IP públicas utilizables. Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.236	<pre>R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248</pre>
Definir la traducción de NAT dinámica	<pre>R2(config)#ip nat inside source list 1 pool INTERNET</pre>

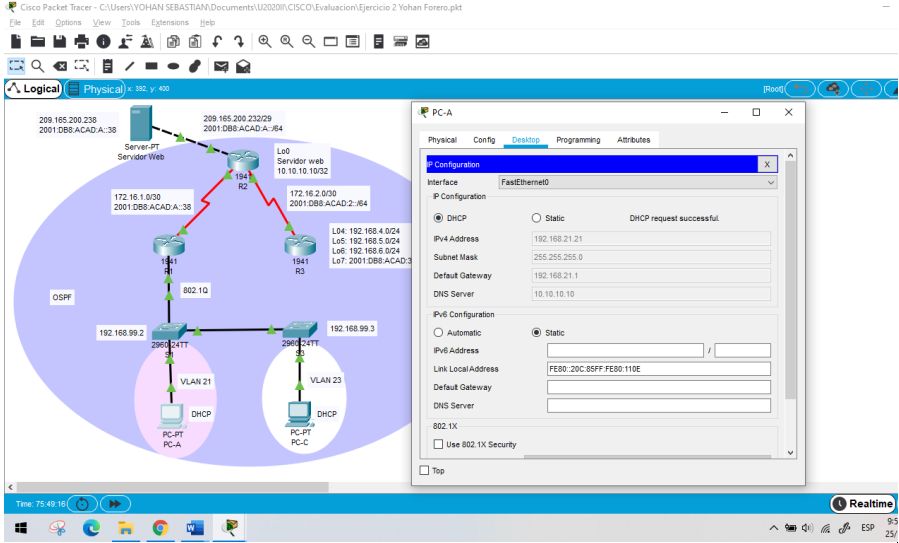
Paso 3: Verificar el protocolo DHCP y la NAT estática

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.

Procedo a ingresar a la PC-A y a la PC-C vamos a escritorio y en el menú de configuración IP vemos que se ha asignado automáticamente por el servicio DHCP la IP asignada al PC-A es: 192.168.21.21 y para PC-C 192.168.23.21, ambos tienen el mismo Gateway predeterminado correspondiente a: 192.168.21.1 correspondiente a la configuración realizada.

Realizo una prueba de conectividad entre ambos PC para que puedan hacerse ping el uno al otro, por último, desde el servidor web ingresamos al servidor 209.165.200.23 con el usuario webuser y la contraseña cisco12345 para acceder. Evidencia en la tabla 29.

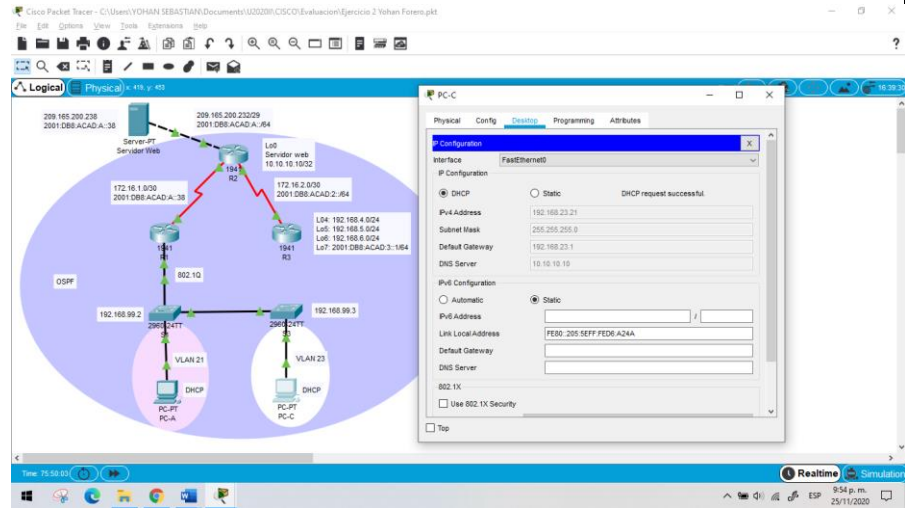
Tabla 29. Paso 3: Verificar el protocolo DHCP y la NAT estática.

Prueba	Resultados
<p>Verificar que la PC-A haya adquirido información de IP del servidor de DHCP</p>	<p>Evidencia de la configuración DHCP de PC-A donde recibió automáticamente y correctamente la configuración suministrada anteriormente.</p> <p style="text-align: center;"><i>Figura 46. configuración DHCP de PC-A</i></p>  <p>Fuente: Autor</p>

Evidencia de la configuración DHCP de PC-C donde recibió automáticamente y correctamente la configuración suministrada anteriormente.

Figura 47. configuración DHCP de PC-C

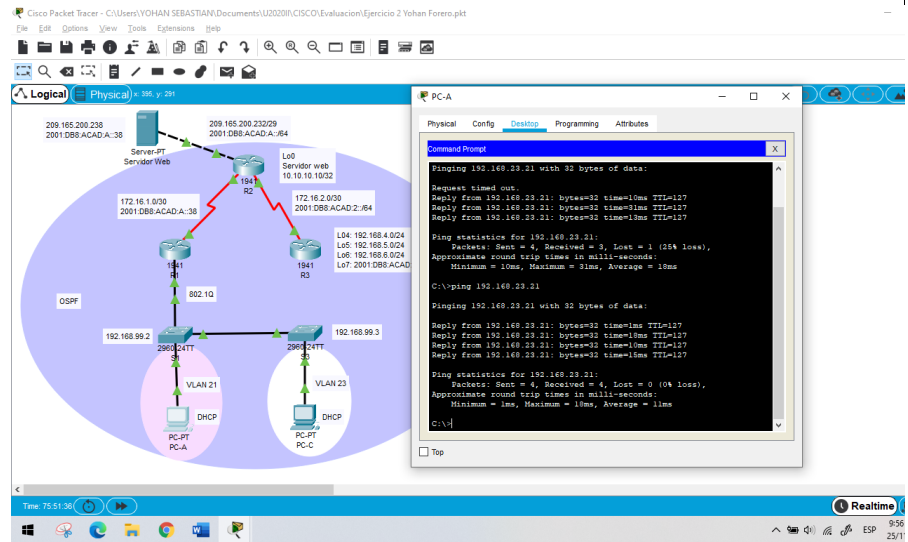
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP



Fuente: Autor

Figura 48. Ping realizado desde PC-A a PC-C correcto.

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

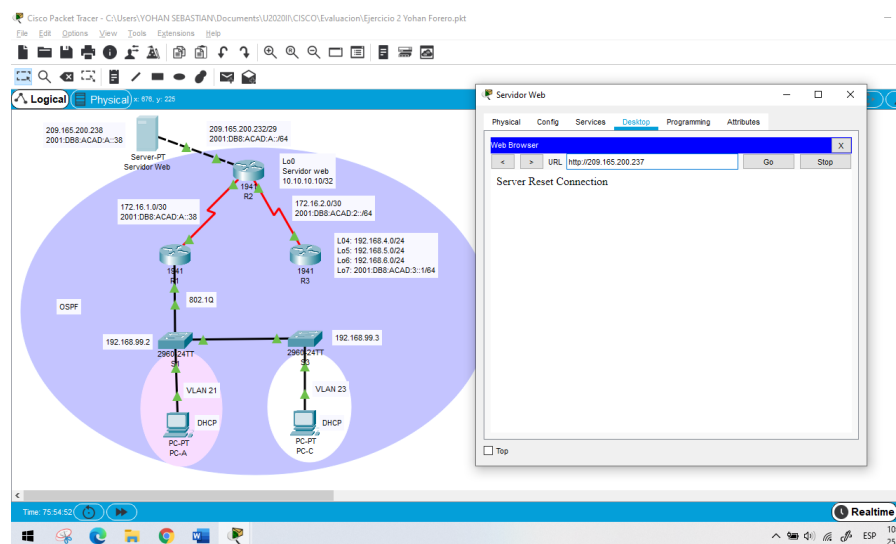


Fuente: Autor

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 este comando y tampoco soporto el comando al momento de crear el Servidor, en una red real si funcionara y con el proceso de logeo sin ningun problema. Evidencia figura 35.

Figura 49. Ingreso a servidor web desde servidor.



Fuente: Autor

Parte 6: Configurar NTP

Procedo a configurar el protocolo NTP que será el encargado de sincronizar varios relojes de red, ajusto la fecha del Router con la estructura 09:00:00 25 march 2016, configuro a R2 como maestro NTP de estrato 5, configuro a R1 como cliente NTP, realizo la configuración de actualización periódica de calendario y verifico el funcionamiento del protocolo con el comando `show ntp associations`. Configuración tabla 30.

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

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

Realizo la configuración de la lista de acceso con nombre y de esta forma permitir que solo R1 pueda acceder por medio de Telnet a R2, aplico ACL para las líneas VTY y se permite el acceso. Por último, verifico el funcionamiento ingresando a R1 y ejecuto el comando telnet 172.16.1.2 que es la ip de R2 automáticamente solicitara las claves de acceso de las líneas VTY las colocas y podremos ingresar a R2. Evidencia configuración tabla 31.

Tabla 31. Paso 1: Restringir el acceso a las líneas VTY en el R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 Nombre de la ACL: ADMIN-MGT	R2(config)#ip access-list standard ADMIN-MGT
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 Trying 172.16.1.2 ...Open SE PROHIBE EL ACCESO NO AUTORIZADO User Access Verification Password: R2>

Figura 51. Ingreso por telnet desde R1 a R2.

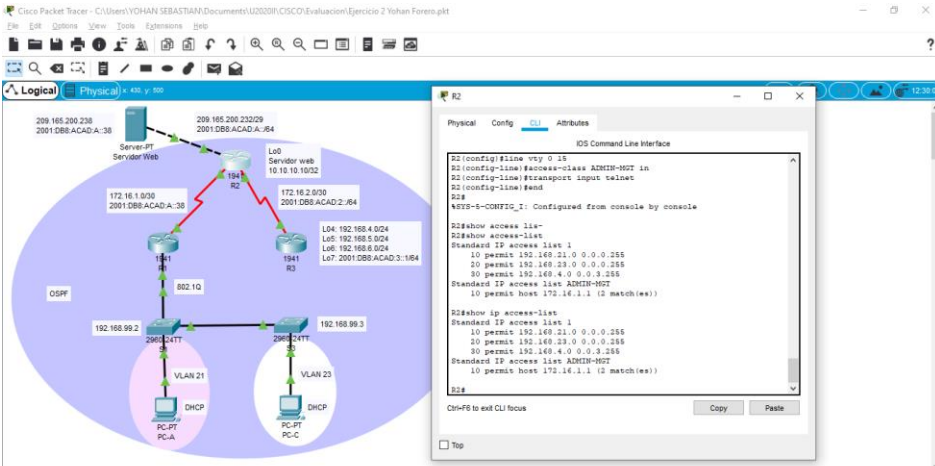
The screenshot displays the Cisco Packet Tracer interface. On the left, a network diagram shows a central router R1 (1941) connected to R2 (1942) and R3 (1943). R1 is also connected to a switch (2960) which has two VLANs: VLAN 21 (with PC-A) and VLAN 23 (with PC-C). R2 is connected to a server (209.165.200.232/29) and a web server (10.10.10.10/32). R3 is connected to a web server (172.16.2.0/30). The network is running OSPF. On the right, the CLI window for R1 shows the following commands and output:

```
R1#  
R1#  
R1#  
R1#  
R1#  
R1#show ntp associations  
address      ref clock    st  when  poll  reach  delay  
offset      disp  
~172.16.1.2  127.127.1.1  5   7     16    7     3.00  
727680949186.00  0.12  
! * sys.peer, # selected, + candidate, - outlyer, x falseticker, -  
configured  
R1#telnet 172.16.1.2  
Trying 172.16.1.2 ...OpenSE PROHIBE EL ACCESO NO AUTORIZADO  
User Access Verification  
Password:  
R2>  
R2>  
R2>  
R1#
```

Fuente: Autor

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

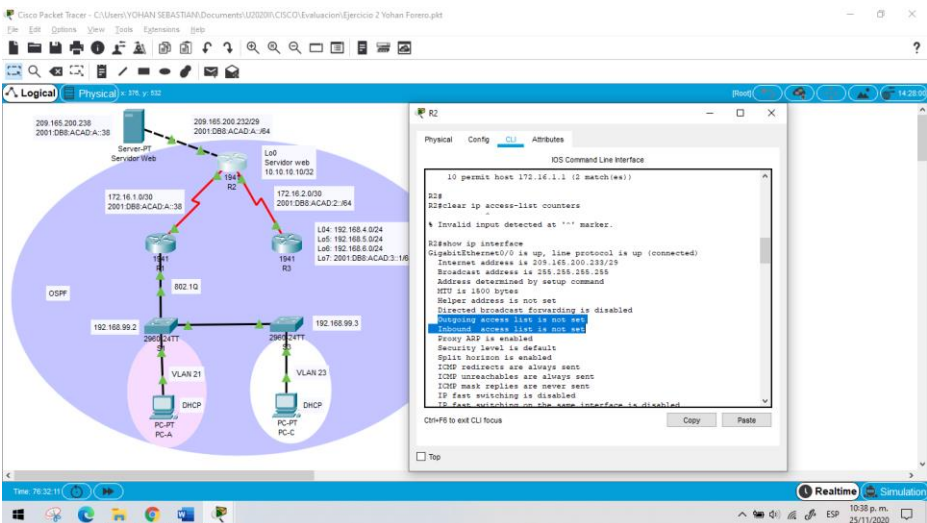
Tabla 32. Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Descripción del comando	Entrada del estudiante (comando)
<p>Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció</p>	<p>R2#show access-list R2#show ip access-list Ejecución en la figura 38.</p> <p style="text-align: center;"><i>Figura 52. Coincidencias recibidas lista de acceso.</i></p>  <p>Fuente: Autor</p>

Restablecer los contadores de una lista de acceso

R2#clear ip access-list counters
Ejecución en la figura 39.

Figura 53. Comando clear ip access-list counters ejecutado.



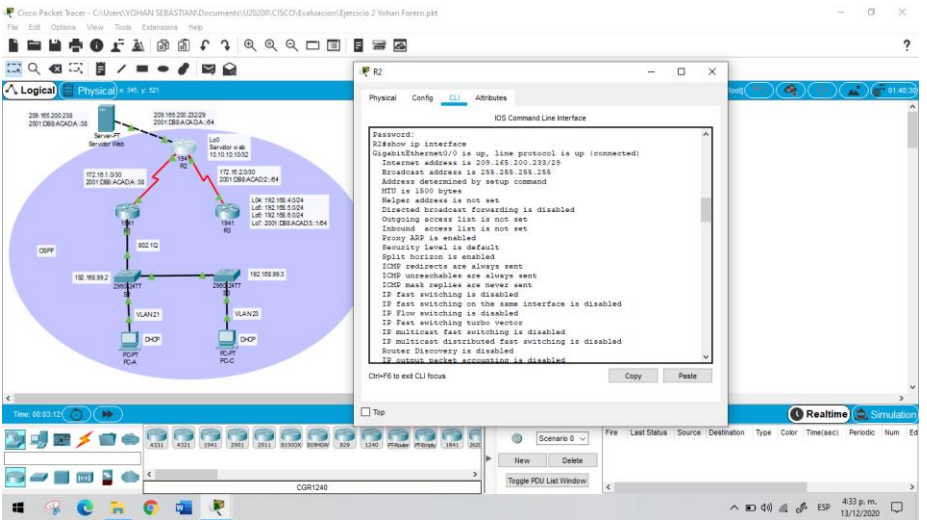
Fuente: Autor

El comando no es soportado en el programa Packet Tracer.

¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?

R2#show ip interface
Ejecución en la figura 40.

Figura 54. Comando show ip interface ejecutado.



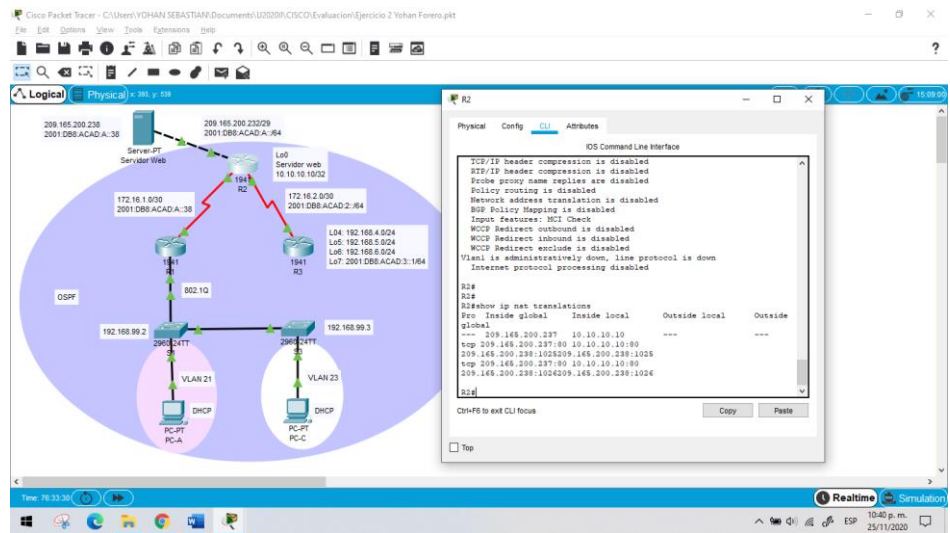
Fuente: Autor

¿Con qué comando se muestran las traducciones NAT?

R2#show ip nat translations
Ejecución en la figura 41

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.

Figura 55. Comando show ip nat translations ejecutado.

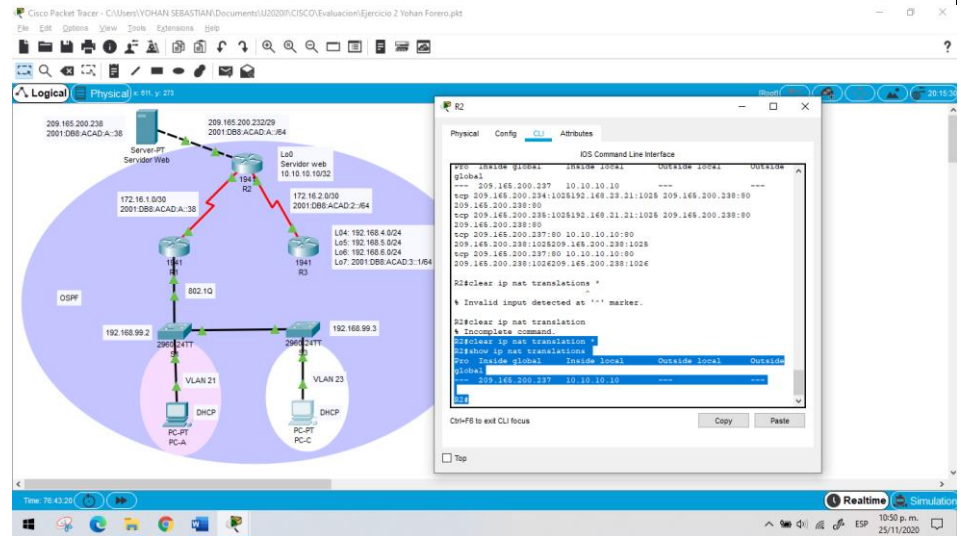


Fuente: Autor

R2#clear ip nat translation *
Ejecución en la figura 42

Figura 56. Comando clear ip nat translation ejecutado.

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



Fuente: Autor

4. CONCLUSIONES

En el desarrollo del escenario numero 1 puedo concluir que es de vital importancia conocer en totalidad la topología de la red y como esta ira configurada ya que al momento de configurar las VLAN con sus respectivos cálculos en los dispositivos no podemos confundir las direcciones de lo contrario la red no funcionara adecuadamente generando inconsistencias en las conexiones.

En el escenario número 2 se evidencio la consideración de una buena administración en las redes con implementación de seguridad a la hora de realizar el montaje de un servidor http y acceso remoto por medio de telnet a otros dispositivos permitiéndonos esa gran facilidad de administrar remotamente además de la importancia de la monitorización de los dispositivos para verificar las conexiones, llevar un adecuado control de acceso y las traducciones ip sobre NAT-PAT que se han llevado a cabo, en el funcionamiento de la red este servicio de traducción sirve para evitar que se acabe el espacio que existe para las IP publicas globales y de este modo ocultar la configuración establecida en la red.

Reconozco la importancia del servicio dhcp en los dispositivos ya que brinda la facilidad de que los dispositivos que se conecten a la red puedan obtener la configuración automática en su dirección ip, puerta de enlace, mascara de red y DNS.

Adicionalmente, en relación con uso del software de emulación Packet Tracer ha sido de gran ayuda, debido a la facilidad de emular los dos escenarios eficientemente con todas las funciones requeridas por la guía cumpliendo su objetivo principal y servir de apoyo para el desarrollo de las actividades propuestas por el diplomado y requerimientos reales que se presenten a lo largo del ámbito laboral.

5. BIBLIOGRAFÍA

- 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). Redes Conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4>
- CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5>
- CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6>
- 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>
- CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8>
- 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 correspondiente al artículo científico y archivos de simulación.

<https://drive.google.com/drive/folders/1QNlId2K0ckjwNdf2U760Nmt4JL7YKEGt?usp=sharing>

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

Yohan Sebastian Forero Zabala
Universidad Nacional Abierta y a Distancia ysforeroz@unadvirtual.edu.co

Resumen

Durante la simulación del primer escenario propuesto se llevo a cabo la configuración de los dispositivos de una red pequeña está conformado por un Router y dos Switch además de dos ordenadores que admitan los protocolos IPv4 e IPv6, el Router y el Swicht serán administrados de forma segura con sus respectivas configuraciones como Logins con contraseña con su respectivo proceso de encriptación, finalmente se procederá con el enrutamiento entre VLAN, DHCP, EtherChannel y Port-security.

Palabras clave: Red, Protocolos, enrutamiento, VLAN, DHCP, EtherChannel y Port-security.

Abstract:

During the simulation of the first proposed scenario, the configuration of the devices of a small network was carried out, it is made up of a Router and two Switches in addition to two computers that support the IPv4 and IPv6 protocols, the Router and the Swicht will be managed safely with their respective configurations such as Logins with password with their respective encryption process, finally the routing between VLAN, DHCP, EtherChannel and Port-security will proceed.

Keywords: Network, protocols, routing, VLAN, DHCP, EtherChannel and Port-security

I. INTRODUCCIÓN

Actualmente, las empresas han tenido que acoplarse al termino de transmodernización, donde cada una de ellas debe implementar sistemas de Comunicaciones para crear relaciones con el resto del mundo, hoy por hoy, las operaciones empresariales se realizan con Europa, Asia, Arica, América del Norte, y no solamente con clientes locales, lo que ha obligado a las empresas a mejorar la calidad de sus ordenadores, redes y su personal, generando un Sistema eficiente y accesible desde cualquier parte del mundo.

Por tal motivo, es necesario que haya personal capacitado para el diseño, desarrollo de infraestructura de redes, así mismo, la Universidad nacional abierta y a distancia ha dispuesto dentro de su formación académica un diplomado de profundización en CISCO, dirigido a profesionales en

ingeniería de sistemas, abarcando temas como: RIPv2, OSPFv2, OSPFv3, DHCPv4 y DHCPv6 en suiches y routers, diseñar e implementar NAT dinámicas y estáticas, listas de acceso bajo los protocolos IPv4 y IPv6, entre otros temas de gran importancia para afianzar nuestros conocimientos en redes. A través de herramientas de simulación en los escenarios propuestos, herramientas de protocolos de administración de redes para la solución de problemas, evaluación de desempeños de routers y switches, además, de instruir al profesional en el diseño de políticas de enrutamiento estático y/o dinámico bajo un esquema de direccionamiento IP, entre otras cosas. De esta manera, se desarrolló un Proyecto aplicado a ejecutar dos escenarios propuestos por el tutor, mostrando el paso a paso con su respectiva evidencia, además, de la simulación en el software Packet Tracer. Las evidencias se basaron en describir cada etapa, configurar de manera correcta cada uno de los dispositivos de networking en el simulador antes mencionado y evidenciarlo en el trabajo final.

II. METODOLOGIA

Para el desarrollo de la simulación se aplicó la investigación de tipo cuantitativa, a través de técnicas basada en el análisis de contenidos de material suministrado por CISCO, basada en la ejecución de una propuesta de un montaje de una red pequeña bajo unos lineamientos técnicos. El software de simulación en Packet Tracer, una aplicación gratuita ofrecida por CISCO, en la cual dispone de una interfaz intuitiva que facilita su utilización a la hora de añadir los distintos elementos que componen la red, pudiendo conectarse unos con otros y realizar las configuraciones necesarias de red en apenas unos clics¹, basado en la aplicación de técnicas procedentes de la ingeniería de telecomunicaciones.

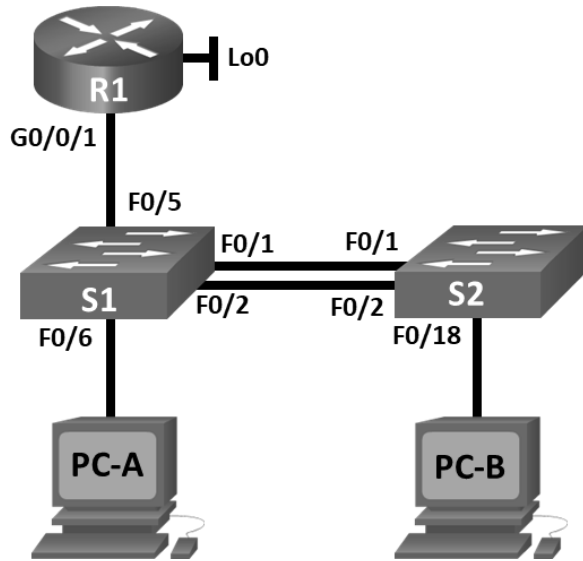
III. DESARROLLO

Para la simulación del escenario 1 se configura los dispositivos (router, switch y equipos u ordenadores) de una red pequeña por medio de una conectividad IPv4 e IPv6 y finalmente enrutarlos entre VLAN, DHCP, EtherChannel y port-security, como se muestra en la Figura 1 suministrado por CISCO. La simulación consta de 4 partes necesarias

¹ AMBIT, Todo lo que debes saber de Cisco Packet Tracer,020

para el desarrollo del escenario respectivo, cada una determinada por una serie de pasos para explicar el proceso ejecutado.

Figura 1. Topología del Escenario 1.



Como toda organización necesita vincular una serie de ordenadores a través de una red, en esta simulación pequeña se requiere una red privada para brindar seguridad a los datos que se están trasladando entre ordenadores, en la tabla 1 se muestran las VLAN que se usarán para el desarrollo de este ejercicio, sin embargo, para realizar el correcto proceso de enrutamiento y configuración de las direcciones IP en los diferentes dispositivos de la red en la tabla 2 encontraremos los direccionamientos para cada dispositivo que debemos tener presentes para el desarrollo de todo el ejercicio.

TABLA 1. ASIGNACIÓN DE VLAN

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

TABLA 2. ASIGNACIÓN DE DIRECCIONES

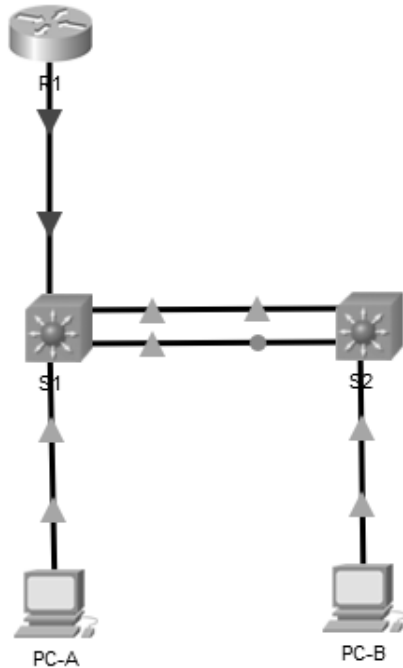
Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
R1 G0/0/1.2	2001:db8: acad: a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
R1 G0/0/1.3	2001:db8: acad: b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde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

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

Se realiza el montaje de la red con Switches 3650 debido a que en Packet Tracer son compatibles con IPV6, los switches 2960 también son compatibles con ipv6 en vida real, El Router usado para el ejercicio corresponde al 1941 y

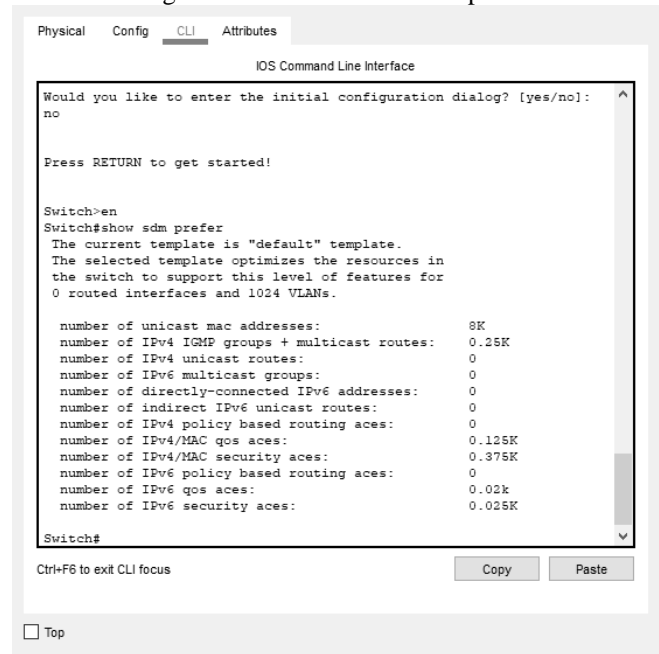
por último 2 PC, se realiza las conexiones como lo muestra la topología para comenzar con el desarrollo del ejercicio., así como se muestra en la figura 2.

Figura 2. Montaje en Packet Tracer.



como lo muestra la siguiente imagen.

Figura 3. Comando show sdm prefer



Paso 2: Configurar R1

Para comenzar con el desarrollo del ejercicio comienzo con la configuración inicial de administración en el Router1 que tiene como objetivo configurar los siguientes parámetros:

Desactivar la búsqueda DNS para evitar que el Router busque soluciones por DNS a comandos que ejecutaremos más adelante esto podría generar retrasos y demoras en el proceso de la configuración, nombre del Router para llevar un registro organizado, nombre del dominio para la administración de la red, protocolos de seguridad como lo son la clave de cifrado para el modo EXEC privilegiado y para la consola con esto evito que alguien acceda remotamente a la configuración del Router y a su administración..

Seguidamente, se procede con la configuración de la red donde se habilita el routing IPV6 en el Router, ingreso a las VLAN que vamos a usar. en este caso seria las VLAN g0/0/1.2, g0/0/1.3, g0/0/1.4, g0/0/1.6, una vez realizada, procedo a configurarlas. Por ejemplo, usando el g0/0/1.2: A partir del ingreso a la VLAN con el comando: R1(config)#int g0/0/1.2, luego de añadir el nombre de la descripción con el comando: R1(config-subif)#description bikes, inmediatamente se realiza el encapsulamiento que permite usar la interfaz como puerto troncal con el comando R1(config-subif)#encapsulation dot1q 2, ahora se realiza la asignación de las direcciones IPV4 e IPV6 según la tabla de direccionamiento con los comandos: R1(config-subif)#ip address 10.19.8.1 255.255.255.192 para IPV4 y R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 para IPV6, finalmente se incluye la dirección local de enlace con el

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

- En primer lugar, se suprimieron las configuraciones de inicio y las VLAN del router y del switch y se volvió a cargar los dispositivos.

Por medio del acceso desde la PC-A a R1 por terminal se ingresó a la configuración de R1, así mismo se accedió al modo de configuración con el comando *enable* y ejecutamos el comando: Router#erase startup-config este comando borrara todas las configuraciones del Router por último con el comando Router#reload se procedió a reiniciar el Router. Para inicializar los Switchs se ejecuta los comandos en modo de configuración: Switch#erase startup-config que borrara las configuraciones del Switch, a continuación, se ejecuta el comando Switch#delete VLAN.dat que borrara todas las configuraciones de VLAN en el Switch, por último, se reinicia con el comando Switch#reload.

- Después de recargar el switch, configuré la plantilla SDM para que admita IPV6 dada la necesidad y se procede a cargar el switch.

El Switch 3650 admite IPV6 por defecto en Packet Tracer en la vida real el Switch 2960 admite el protocolo ipv6 también, por medio del comando Switch#show sdm prefer podemos verificar que el switch es compatible con IPV6, así

comando: R1(config-subif)#ipv6 address fe80::1 link-local.
Este procedimiento se realiza con todas las VLAN que vamos a configurar en el ejercicio y también en la interfaz loopback 0. Evidencia de configuración Tabla 3.

Tabla 3.
Configuración R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain lookup
Nombre del Router: R1	Router(config)#hostname R1
Nombre de dominio: ccna-lab.com	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado: ciscoenpass	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola: ciscoconpass	R1(config)#line console 0 R1(config-line)#password ciscoconpass
Establecer la longitud mínima para las contraseñas de 10 caracteres	R1(config)#security passwords min-length 10
Creación de un usuario administrativo en la base de datos local Nombre de usuario: admin Password: admin1pass	R1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 15 R1(config-line)#login local
Configurar VTY solo aceptando SSH	R1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd %ACCESO DENEGADO%
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing

Tarea	Especificación
Configurar interfaz G0/0/1 y subinterfaces	R1(config)#int g0/0/1.2
Establezca la descripción	R1(config-subif)#encapsulation dot1q 2
Establece la dirección IPv4.	R1(config-subif)#description bikes
Establezca la dirección local de enlace IPv6 como fe80::1	R1(config-subif)#ip address 10.19.8.1 255.255.255.192
Establece la dirección IPv6.	R1(config-subif)#ipv6 address fe80::1 link-local
Activar la interfaz.	R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#no shutdown
Configure el Loopback0 interface	R1(config-if)#int loopback 0
Establezca la descripción	R1(config-if)#description InternetAcceso
Establece la dirección IPv4	R1(config-if)#ip address 209.165.201.1 255.255.255.224
Establece la dirección IPv6.	R1(config-if)#ipv6 address 2001:db8:acad:209::1/64
Establezca la dirección local de enlace IPv6 como fe80::1	R1(config-if)#ipv6 address fe80::1 link-local
Generar una clave de cifrado RSA Módulo de 1024 bits	R1(config)#crypto key generate rsa 1024

Paso 3: Configure S1 y S2.

La configuración inicial de los switches contiene: desactivar la búsqueda DNS, asignar el nombre del Router, la asignación del nombre del dominio, en este caso es ccna-lab.com, generación de contraseñas para el modo exec privilegiado y acceso a la consola, cifrar las contraseñas de texto y añadir un mensaje al Motd Banner y crear usuario en la base de datos local.

Luego de esto ingreso a la VLAN 4 que será la interfaz de administración de SVI del Switch y asigno el direccionamiento IPV4 e IPV6 según la tabla de direcciones, además, de asignar la dirección local de enlace para generar la comunicación en la red local, se incluye a la descripción de la VLAN y se procede a configurar el Gateway predeterminado. Evidencia en la tabla 4.

Tabla 4.
Configuración S1 y S2

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch(config)#no ip domain lookup
Asignación nombre del switch	S1 o S2, según proceda Switch(config)#hostname S1
Asignación nombre de dominio: ccna-lab.com	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado: Ciscoenpass	S1(config)#enable secret ciscoenpass
Configuración de contraseña de acceso a la consola: Ciscoconpass	S1(config)#line console 0 S1(config-line)#password ciscoconpass
Creación de un usuario administrativo en la base de datos local Nombre de usuario: admin Password: admin1pass	S1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd "ACCESO DENEGADO"
Generar una clave de cifrado RSA	Módulo de 1024 bits S1(config)#crypto key generate rsa 1024

Tarea	Especificación
Configuración de la interfaz de administración (SVI)	S1(config)#int vlan 4 S1(config-if)#ip address 10.19.8.98 255.255.255.248
Establecimiento de la dirección local de enlace IPv6 como FE80::98 para S1 y FE80::99 para S2	S1(config-if)#ipv6 address fe80::98 link-local S2(config-if)#ipv6 address fe80::99 link-local S1(config-if)#ipv6 address 2001:db8:acad:c::98/64
Establecer la dirección IPv6 de capa 3	
Configuración del Gateway predeterminado	S1(config)#ip default-gateway 10.19.8.97
Se configuró la puerta de enlace predeterminada como 10.19.8.97 para IPv4 según la tabla de direcciones.	

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

Paso 1: Configurar S1

Para el proceso de configuración en el S1 comienzo con la creación de las VLAN con su respectiva descripción ya que este nos permitirá trabajar de forma organizada para poder identificarlos en la red, contiene la siguiente estructura:

```
S1(config-vlan)#vlan 2
S1(config-vlan)#name bikes
```

Seguidamente creo los troncos 802.1Q que serán los encargados de los enlaces troncales a la VLAN 6 nativa, se procede a crear el grupo de puertos de EtherChannel donde irán configuradas nuestras VLAN, una vez creado el grupo de puerto de EtherChannel asignamos la VLAN 6 como puerto de acceso para la comunicación entre los dispositivos que se encuentran en la misma red, ahora asigno el puerto G1/0/6 a la VLAN 2 que es donde está conectada la PC-A, luego asigno los parámetros de seguridad en los puertos para que solo permita un máximo de 3 direcciones conectadas.

Por último, desactivo las interfaces que no se usaran en el Switch en este caso el Switch 1 está usando las interfaces g1/0/1-2 y g1/0/5-6 por lo que se procederá a desactivar el siguiente rango de interfaces g1/0/3-4 y g1/0/7-24 con su respectiva descripción que están deshabilitadas. Configuraciones en tabla 5.

Tabla 5.
Configuración S1

Tarea	Especificación
Creación de los troncos 802.1Q que utilizaran la VLAN 6 nativa	S1(config)#int g1/0/5 S1(config-if)#switchport mode trunk S1(config-if)# switchport trunk native vlan 6
Creación de un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 Usar el protocolo LACP para la negociación	S1(config-if)#int range g1/0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#int port-channel 1 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6
Configuración del puerto de acceso de host para VLAN 2 Interface F0/6	S1(config-if)#int g1/0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2
Configuración de la seguridad del puerto en los puertos de acceso Permitir 3 direcciones MAC	S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas, es el mismo procedimiento para todas las interfaces que se establecen en el siguiente rango: g1/0/3-4 y g1/0/7-24 Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S1(config-if)#int range g1/0/3-4 S1(config-if-range)#switchport mode Access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Not In Use S1(config-if-range)#shutdown

Paso 2. Configure el S2.

Para el proceso de configuración en el S12 comienzo con la creación de las VLAN con su respectiva descripción ya que este nos permitirá trabajar de forma organizada para poder identificarlos en la red, seguidamente creo los troncos 802.1Q que serán los encargados de los enlaces troncales a

la VLAN 6 nativa, creo el grupo de puertos de EtherChannel donde irán configuradas nuestras VLAN.

Una vez creado el grupo de puerto de EtherChannel asignamos la VLAN 6 como puerto de acceso para la comunicación entre los dispositivos que se encuentran en la misma red, ahora asigno el puerto G1/0/18 a la VLAN 3 que es donde está conectada la PC-C, luego creo los parámetros de seguridad en los puertos para que solo permita un máximo de 3 direcciones conectadas.

Por último, desactivo las interfaces que no se usaran en el Switch en este caso el Switch 1 está usando las interfaces g1/0/1-2 por lo que se procede a desactivar el siguiente rango de interfaces g1/0/3-4 y g1/0/7-24 con su respectiva descripción que están deshabilitadas. Evidencia de configuración tabla 6.

Tabla 6.
Configuración S2

Tarea	Especificación
Creación de VLAN con su respectiva descripción VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	S2(config-vlan)#vlan 2 S2(config-vlan)#name bikes S2(config-vlan)#vlan 3 S2(config-vlan)#name Trikes El mismo procedimiento para todas las vlan.
Creación de troncos 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1 y F0/2	S2(config)#int range g1/0/1-2 S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 6
Creación de un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 Usar el protocolo LACP para la negociación	S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#int port-channel 1 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6

Tarea	Especificación
Configuro el puerto de acceso del host para la VLAN 3 Interfaz F0/18	S2(config-if)#int g1/0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configuro port-security en los access ports permite 3 MAC addresses	S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3
Asegure todas las interfaces no utilizadas. Es el mismo procedimiento para todas las interfaces que se establecen en el siguiente rango: g1/0/3-17 y g1/0/19-24 Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S2(config-if)#int range g1/0/3-17 S2(config-if-range)#switchport mode Access S2(config-if-range)#description Not In Use S2(config-if-range)#shutdown

Parte 3. Configurar soporte de host

Paso 1. Configure R1

Como primera medida para la configuración de R1 es indispensable asignar las direcciones predeterminadas loopback que nos ayudara a que los protocolos configurados en los dispositivos funcionen de la manera correcta esto quiere decir que el tráfico de red ira dirigido a las direcciones predeterminadas.

Ahora configuro el DHCP en IPV4 para la VLAN 2 para que solo use las ultimas 10 direcciones disponibles es la estructura quedaria de la siguiente forma: se desactiva el siguiente rango de direcciones IP: 10.19.8.1 a 10.19.8.52 por lo que al momento de conectar los hosts deberían usar únicamente las direcciones 10.19.8.53 a la 10.19.8.62. en el caso de la VLAN 3 se procede a desactivar el rango de direcciones 10.19.8.65 al 10.19.8.84 por lo que las direcciones que usarán los hosts conectados serán del siguiente rango: 10.19.8.85 al 10.19.8.94. configuraciones realizadas en tabla7.

Tabla 7.
Configuración DHCP R1

Tarea	Especificación
Configure Default Routing Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 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 ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada	R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#ip dhcp pool R1(config)#ip dhcp pool VLAN2-BIKES 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
Configurar DHCP IPv4 para VLAN 3 Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada	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-b.net

Paso 2. Configurar los servidores

Para el desarrollo de las configuraciones de los hosts ingreso al escritorio en el menú de configuración IP y lo configuro de la siguiente forma: para el protocolo IPV4 asigno DHCP es decir que tome la IP automáticamente de la VLAN donde está conectado, las IP del PC-A quedo como 10.19.8.53 y para el PC-B 10.19.8.85 es decir que la regla que añadimos anteriormente en el R1 ha funcionado y cada host está utilizando la primera de las ultimas 10 direcciones disponibles.

Para el protocolo IPV6 asigno a cada host manualmente la dirección IP según la tabla de direccionamiento.

A continuación, anexo evidencia de la configuración IPV4 asignada por dhcp en ambos PC y la configuración

IPV6 asignada manualmente en ambos PC.

Figura 4. Evidencia configuración PC-A

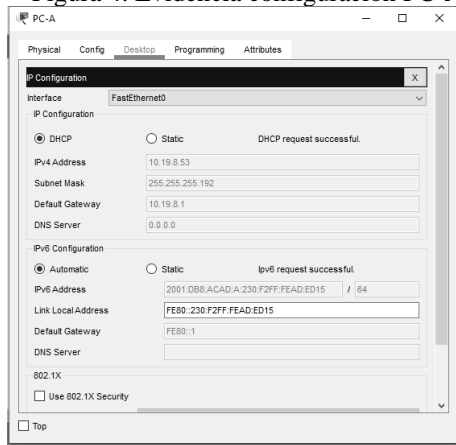


Figura 5. Evidencia configuracion PC-B

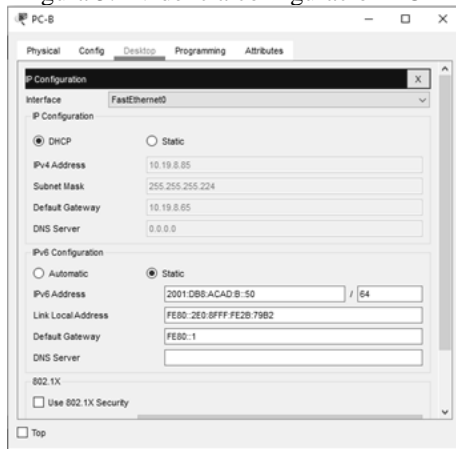


Figura 6. Configuración final PC-A

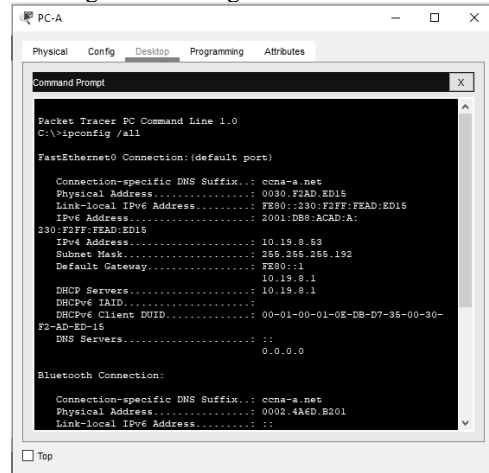
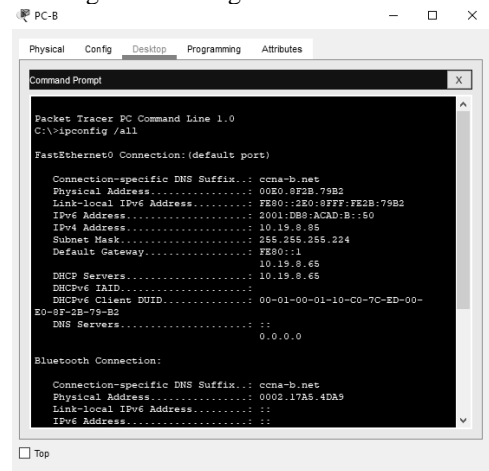


Figura 7. Configuración final PC-B



Por último, para verificar la configuración de la red en cada host me dirijo a la consola y ejecuto el comando ipconfig /all que me proporcionara toda la configuración de red del host donde evidencio: el nombre del dominio que asignamos anteriormente, la dirección física, dirección IP, mascara de red, Gateway predeterminado, servidor DNS y servidor DHCP. Esto para los protocolos IPV4 E IPV6 Y demás protocolos que contenga el equipo.

A continuación, anexo pantallazo de la configuración de final de los host PC-A y PC-B.

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

La mejor forma de comprobar el funcionamiento de una red es realizando Pings entre todos los dispositivos esto quiere decir que si todos los Ping funcionan la red esta adecuadamente configurada con los parametros exactos y protocolos funcionando, por ende para finalizar el ejercicio se desarrolla ping entro todos los dispositivos para verificar el correcto funcionamiento de la red.

Añado los ping mas importantes en la red como evidencia.

Figura 8. Ping desde PCA a R1, G0/0/1.2 en IPV4 e IPV6

```

Command Prompt
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 15ms, Average = 6ms

C:\>ping 10.19.8.1

Pinging 10.19.8.1 with 32 bytes of data:

Reply from 10.19.8.1: bytes=32 time=1ms TTL=255
Reply from 10.19.8.1: bytes=32 time=1ms TTL=255
Reply from 10.19.8.1: bytes=32 time=1ms TTL=255
Reply from 10.19.8.1: bytes=32 time=1ms TTL=255

Ping statistics for 10.19.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
      Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 2001:db8:acad:a::1

Pinging 2001:db8:acad:a::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=5ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=10ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255

Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
      Minimum = 0ms, Maximum = 10ms, Average = 4ms

C:\>
    
```

Figura 9. Ping desde PCA a PC-B en IPV4 e IPV6

```

Command Prompt
Approximate round trip times in milli-seconds:
  Minimum = 11ms, Maximum = 22ms, Average = 16ms

C:\>ping 10.19.8.85

Pinging 10.19.8.85 with 32 bytes of data:

Reply from 10.19.8.85: bytes=32 time=25ms TTL=127
Reply from 10.19.8.85: bytes=32 time=10ms TTL=127
Reply from 10.19.8.85: bytes=32 time=1ms TTL=127
Reply from 10.19.8.85: bytes=32 time=10ms TTL=127

Ping statistics for 10.19.8.85:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
      Minimum = 0ms, Maximum = 25ms, Average = 15ms

C:\>ping 2001:db8:acad:b::50

Pinging 2001:db8:acad:b::50 with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::50: bytes=32 time=13ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=13ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=10ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=13ms TTL=127

Ping statistics for 2001:DB8:ACAD:B::50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
      Minimum = 10ms, Maximum = 19ms, Average = 13ms

C:\>
    
```

IV. CONCLUSION

Reconozco la importancia del servicio dhcp en los dispositivos ya que brinda la facilidad de que los dispositivos que se conecten a la red puedan obtener la configuración automática en su dirección ip, puerta de enlace, mascara de red y DNS.

El proceso de configuración de las Vlan en una manera efectiva de segmentación de red por lo que mediante su implementación nos permite agrupar los dispositivos de una red de forma organizada incrementando el rendimiento en la red y disminuyendo la difusión de broadcast innecesario.

V. REFERENCIAS

[1] AMBIT. (2020). Todo lo que debes saber de Cisco Packet Tracer. Recuperado de: <https://www.ambitbst.com/blog/todo-lo-que-debes-saber-de-cisco-packet-tracer#>

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

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

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

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

[6] 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>

[7] CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8>

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

[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#10biografia>

VI. BIOGRAFÍA



Yohan Forero Zabala (1996) nació en Facatativá, Cundinamarca, el día 30 de mayo de 1996, sus estudios en instituciones como el Colegio Emilio Cifuentes y el Servicio Nacional de Aprendizaje, Técnico en Sistemas, con experiencia en empresas tales como: Carvajal, Americas Bussiness, como director técnico de procesos electorales nacionales y departamentales.