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

ROSA EMILIA PALACIOS PALACIOS

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

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

ROSA EMILIA PALACIOS PALACIOS

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

DIRECTOR Esp. JUAN CARLOS VESGA FERREIRA

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Chinú, Diciembre 13 de 2020

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

BANNER MOTD: Es un comando que especifica el mensaje que se muestra como Mensaje del día, el primer mensaje que se muestra en una conexión entrante. Este comando define solo el mensaje; el comando motd - banner habilita o deshabilita la visualización.

DHCP: Significa protocolo de configuración de host dinámico y es un protocolo de red utilizado en redes IP donde un servidor DHCP asigna automáticamente una dirección IP y otra información a cada host en la red para que puedan comunicarse de manera eficiente con otros puntos finales.

ETHERCHANNEL: Es una tecnología de agregación de enlaces de puertos desarrollada por Cisco, que proporciona enlaces de alta velocidad tolerantes a fallas entre conmutadores, enrutadores y servidores. La tecnología EtherChannel permite que varios enlaces Ethernet físicos (Fast Ethernet o Gigabit Ethernet) se combinen en un canal lógico.

GATEWAY: Un Gateway (puerta de enlace) es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

NVRAM: La NVRAM o “Non-Volatile Random Access Memory”, es una memoria de acceso aleatorio no volátil capaz de almacenar información y no perderla al retirar la alimentación eléctrica del componente.

PORT-SECURITY: Es una 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 entrada del switch. Si un dispositivo con otra dirección MAC intenta comunicarse a través de esa esa entrada, port-security deshabilitará el puerto.

TRUNKING: En telecomunicaciones, el enlace troncal es una forma de proporcionar acceso a la red a muchos clientes compartiendo un conjunto de líneas o frecuencias en lugar de proporcionarlas individualmente.

VLAN: Acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.1Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.

RESUMEN

Las necesidades, requerimientos y exigencias de las nuevas tecnologías de la información orientan indiscutiblemente a la adquisición y conmutación de un amplio conocimiento, habilidades, destrezas y capacidades para manejar y configurar redes de datos.

Es de suma importancia que el profesional de la ingeniería de sistemas sea altamente competitivo para que pueda enfrentarse a los nuevos retos e innovaciones que se presentan en el mercado de la tecnología, redes, informática y sistemas.

Los ingenieros de sistemas deben ser capaces de realizar un diagnóstico y una configuración de redes altamente certera y eficiente que le permita brindar soluciones y respuestas a los diversos problemas que las redes de información, electrónicas y de datos puedan presentar.

El diplomado de profundización CISCO contiene una prueba de habilidades prácticas que, considerando una serie de características para el aprendizaje y enrutamiento de diagnóstico, configuración y solución de problemas de redes, hacen parte intrínseca de los módulos educativos y permiten su revisión y valoración.

Considerando los dos escenarios que se presentan en la prueba de habilidades, se debe seleccionar uno de ellos para realizar el proceso de configuración de redes, utilizando “Packet Tracer” o “GNS3”.

La empresa líder en manufactura y distribución de componentes de comunicación CISCO brinda la posibilidad de realizar cursos de capacitación y certificarse. Esta certificación es una de las más importantes en las tecnologías de la información.

Palabras clave: Enlace troncal, Puerta de enlace, Puerto de switch, Red.

ABSTRACT

The needs, requirements and demands of the new information technologies unquestionably guide the acquisition and switching of extensive knowledge, skills, abilities and capacities to manage and configure data networks.

It's necessary and really important that the systems engineering professional is highly competitive so that they can face the new challenges and innovations that are presented in the technology, networks, computing and systems market.
Systems engineers must be able to perform a highly accurate and efficient network configuration and diagnosis that allows them to provide solutions and answers to the various problems that information, electronic and data networks may present.

The CISCO in-depth diplomat contains a practical skills test that, considering a series of characteristics for learning and routing diagnosis, configuration and solution of network problems, are an intrinsic part of the educational modules and allow their review and assessment.

Considering the two scenarios presented in the skills test, one of them must be selected to carry out the network configuration process, using "Packet Tracer" or "GNS3".

The leading company in the manufacture and distribution of communication components CISCO offers the possibility of taking training courses and getting certified. This certification is one of the most important in information technology nowadays.

Keywords: Trunking, Gateway, Switchport, Network.

INTRODUCCIÓN

Manejar correctamente la información es un factor fundamental, importante y necesario en la globalización del mundo moderno actual que estamos viviendo. Los ejecutivos y en general todo el recurso humano de las organizaciones requieren acceder a redes que les permitan una organización efectiva y eficiente de los datos, trabajando en equipo. Los ingenieros de sistemas son los encargados de trabajar en las redes de los programas, softwares o sitios de internet.

Las redes locales en las cuales se conectan varios ordenadores y periféricos son cada vez más utilizadas en los hogares y el trabajo, este tipo de redes reciben el nombre de “LAN” que es la abreviatura de “Local Área Network”, Red de Área Local. Estas redes abarcan un rango físico limitado al de una construcción o a un espacio que incluye pocos kilómetros. Su aplicación más amplia es la interconexión de ordenadores personales, espacios de trabajo, fábricas, oficinas, entre otros lugares, estas permiten a dos o más maquinas comunicarse entre sí.

El principal beneficio que nos brindan estas redes es permitirnos compartir los recursos disponibles entre los variados equipos con que contamos, ya sean bases de datos, periféricos o conexión a internet.

La Universidad Nacional Abierta y a Distancia (UNAD) dentro de los contenidos a desarrollar en el diplomado de profundización CISCO para optar el título de Ingeniero de sistemas, incluye el aprendizaje de configuración de redes donde se da aplicabilidad a todos los conceptos y temáticas estudiadas y aprendidas a lo largo del proceso de aprendizaje de la carrera, entre los cuales podemos mencionar: configuración de dispositivos intermedios y finales, CCNA, CCNP, interactuación entre varias redes e internet, comandos utilizados para la protección de acceso, conceptos aplicables para la configuración de redes mediante los protocolos y protocolos de seguridad entre otros.

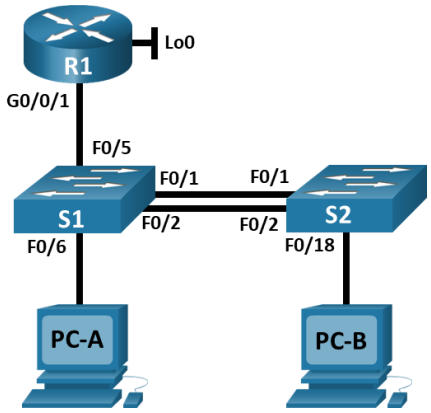
La realización de este trabajo de grado nos permite adquirir los conocimientos, habilidades y destrezas para desarrollar métodos, herramientas y modelos que permitan concebir, diseñar, implementar y operar tecnologías de información para el procesamiento y gestión de información, una de las características que integran el perfil del egresado de ingeniería de sistemas de la UNAD y que está intrínsecamente relacionada con las necesidades de las tecnologías de la información actuales.

1. Descripción de escenarios propuestos para la prueba de habilidades

1.1. Escenario 1

Topología

Figura 1. Topología escenario 1

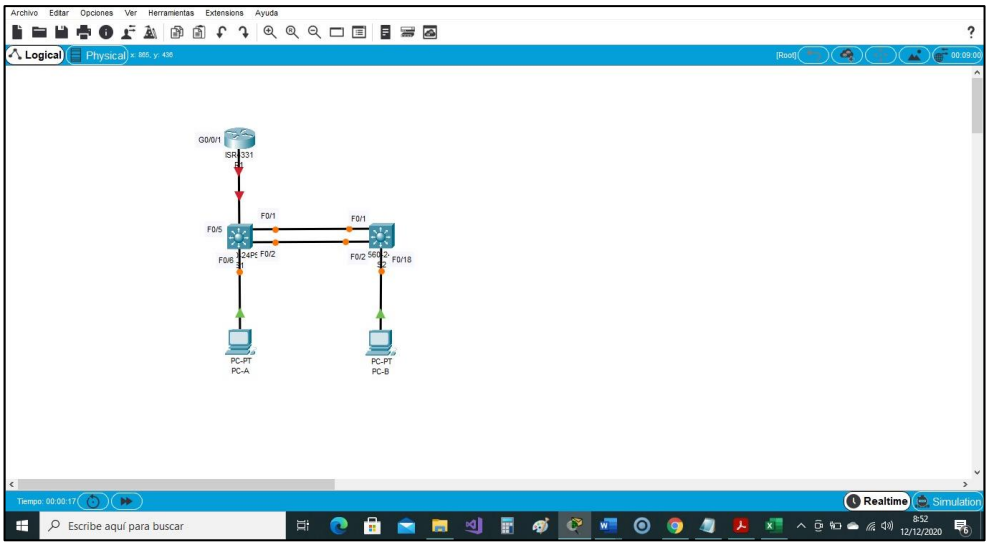


Fuente: Documento Cisco

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

Inicialmente en el simulador Packet Tracer versión 7.3.1 se crea la topología de red utilizando para ello 1 Router Cisco 43331, 2 Switchs Cisco 3560, 2 PCs. y cables de cobre directos para la respectiva conexión.

Figura 2. Simulación Escenario 1 en Packet Tracer



Fuente: Autor

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

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

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

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

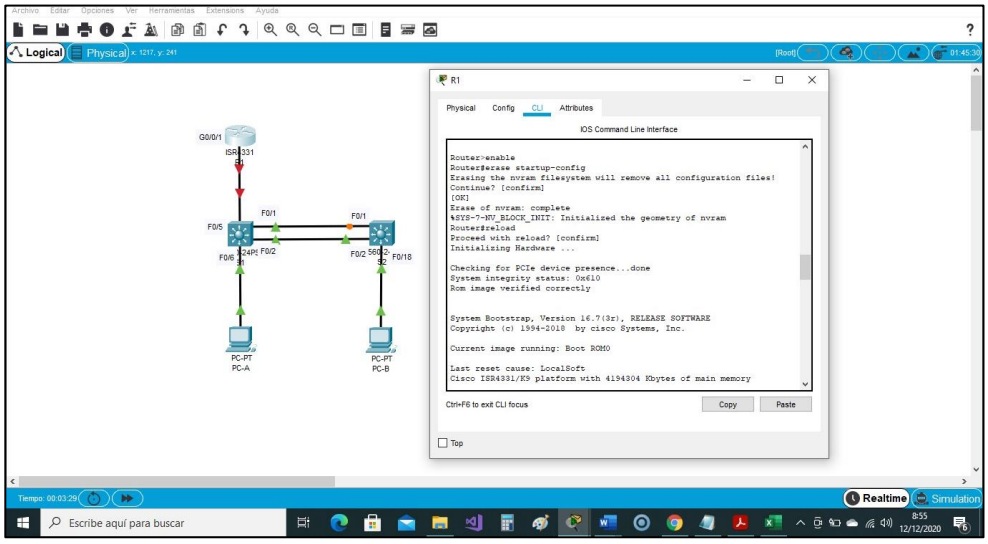
Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos.

Tabla 3. Inicialización y carga del Router

Tarea	Especificación
Ingresar al modo privilegiado	Router>enable
Restablecer valores predeterminados	Router#erase startup-config
Reiniciar el Router	Router#reload

Se accede al Router 1 a través de la consola en modo privilegiado para borrar cualquier configuración de inicio con el comando *erase startup-config* el cual borra el contenido de la NVRAM, posteriormente se reinicia el Router con el comando *reload*, quedando esté listo para su configuración inicial.

Figura 3. Inicialización y carga del Router



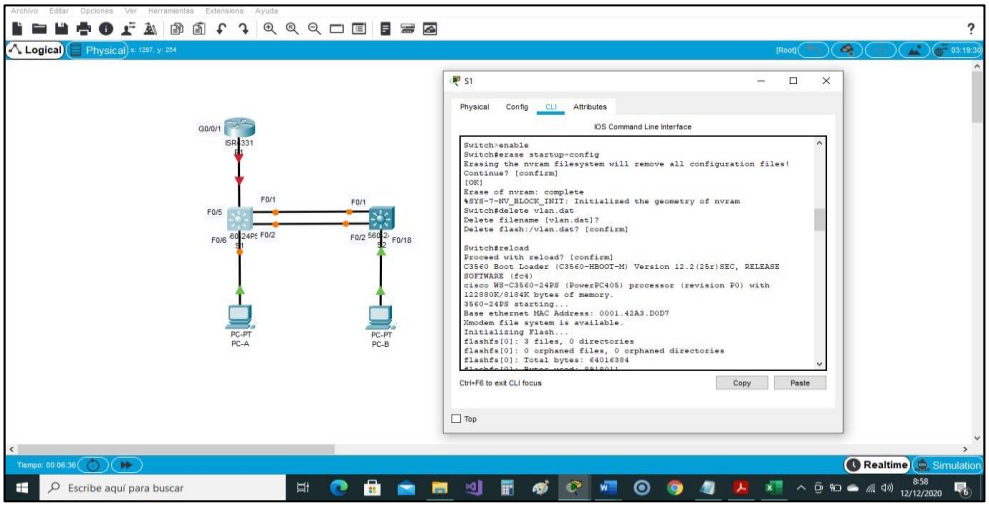
Fuente: Autor

Tabla 4. Inicialización y carga del Switch 1 y 2

Tarea	Especificación
Ingresar al modo privilegiado	Switch>enable
Restablecer valores predeterminados	Switch#erase startup-config
Eliminar Vlan	Switch#delete vlan.dat
Reiniciar el Switch	Switchr#reload

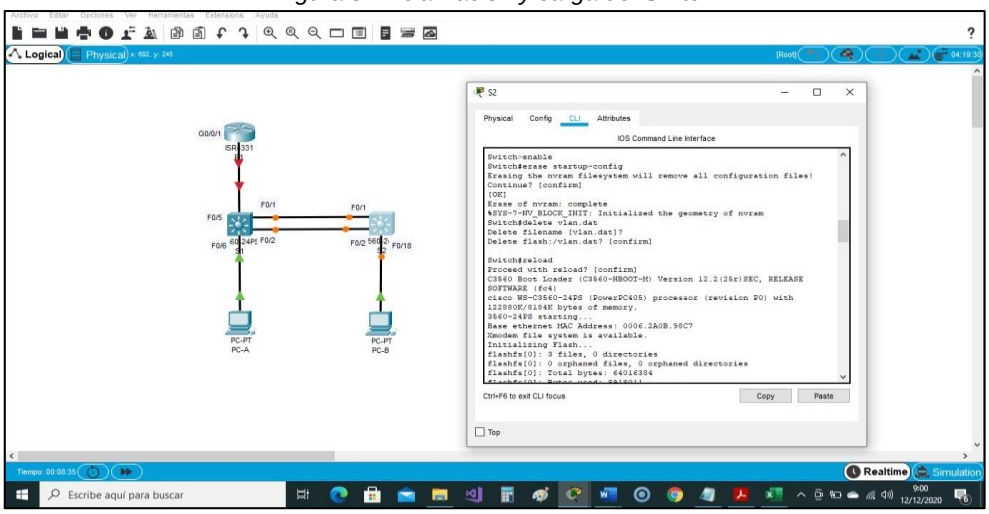
Se accede al Switch 1 y 2 a través de la consola en modo privilegiado para ejecutar el comando *erase startup-config* el cual borra el contenido de la NVRAM junto con el comando *delete vlan.dat* el cual elimina la base de datos de la vlan, este proceso permite restaurar el switch y borrar cualquier configuración de inicio, posteriormente se reinicia con el comando *reload*, quedando esté listo para su configuración inicial.

Figura 4. Inicialización y carga del Switch 1



Fuente: Autor

Figura 5. Inicialización y carga del Switch 2



Fuente: Autor

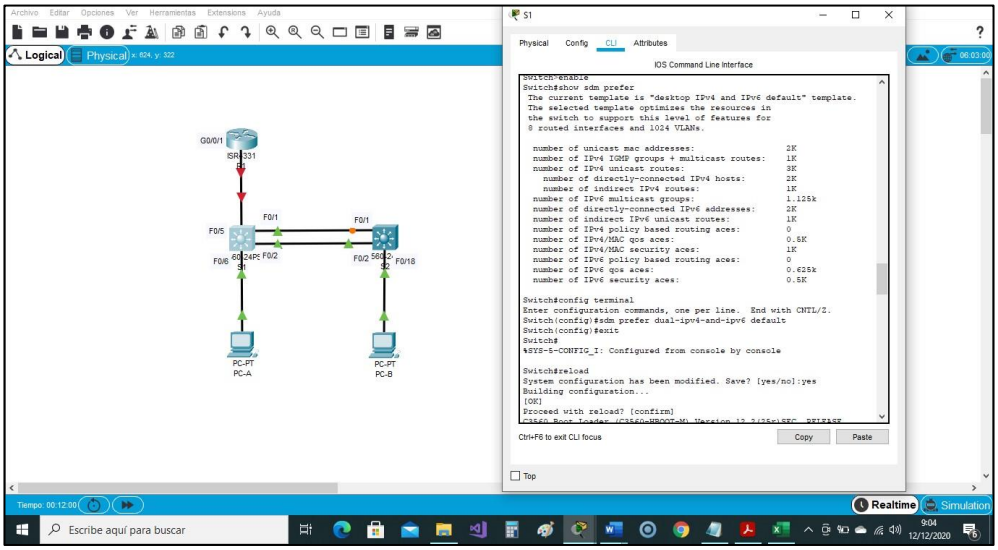
Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.

Tabla 5. Configuración de plantilla SDM en Switch 1 y 2

Tarea	Especificación
Ingresar al modo privilegiado	Switch>enable
Activar plantilla predeterminada	Switch#show sdm prefer
Habilitar plantilla SDM para IPv4 e IPv6	Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Reiniciar el Router	Switchr#reload

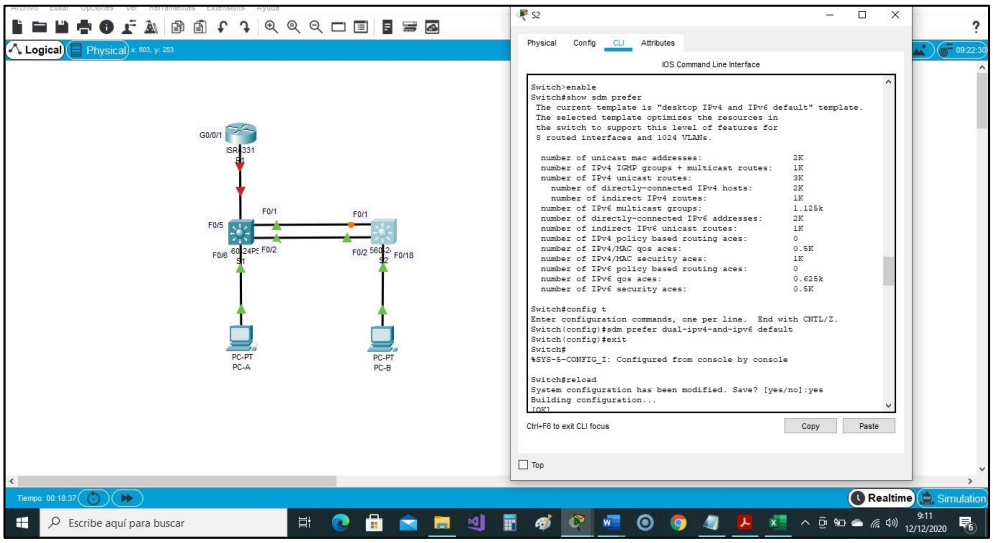
Teniendo en cuenta que el Switch Cisco 3560 no soporta capacidades IPv6 se debe configurar la plantilla SDM para que pueda admitir IPv6 junto con IPv4, se verifica desde modo privilegiado la configuración con el comando *show sdm prefer*, donde se muestra que solo soporta configuración IPv4, para activar la configuración IPv6 se procede a ejecutar el comando *sdm prefer dual-ipv4-andipv6 default*, inmediatamente se reinicia con el comando *reload* para que la nueva plantilla sea cargada y tenga el efecto esperado que es soportar IPv4 y IPv6.

Figura 6. Configuración de plantilla SDM en Switch 1



Fuente: Autor

Figura 7. Configuración de plantilla SDM en Switch 2



Fuente: Autor

1.2. Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 6. Configuración del Router

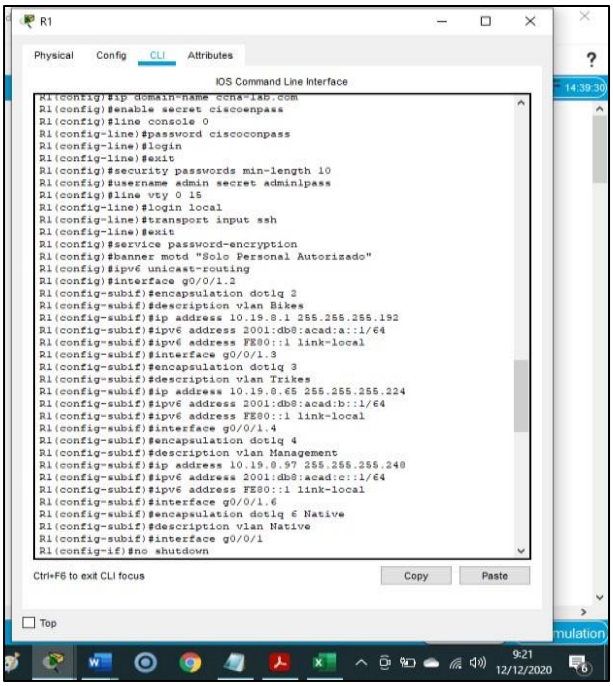
Desactivar la búsqueda DNS	Router(config)#no ip domain lookup
Nombre del router (R1)	Router(config)#hostname R1
Nombre de dominio (ccna-lab.com)	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado (ciscoenpass)	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola (ciscoconpass)	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas (10 caracteres)	R1(config)#security password s min-length 10
Crear 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 R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption

Tarea	Especificación
Configure un MOTD Banner	R1(config)#banner motd "Solo Personal Autorizado"
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como fe80: :1 Establece la dirección IPv6 Activar la interfaz.	R1(config)#interface g0/0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#descrition vlan Bikes R1(config-subif)#description vlan Bikes R1(config-subif)#ip address 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 address FE80::1 link-local R1(config-subif)# interface g0/0/1.3 R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#description vlan Trikes R1(config-subif)#ip address 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address FE80::1 link-local R1(config-subif)#interface g0/0/1.4 R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#description vlan Management R1(config-subif)#ip address 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 address FE80::1 link-local R1(config-subif)#interface g0/0/1.6 R1(config-subif)#encapsulation dot1q 6 Native R1(config-subif)#description vlan Native R1(config-subif)#interface g0/0/1 R1(config-if)#no shutdown
Configure el Loopback0 interface Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como fe80::1	R1(config-if)# interface loopback 0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address FE80::1 link-local R1(config-if)#description Internet R1(config-if)#exit
Generar una clave de cifrado RSA Módulo de 1024 bits	R1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024

Se realiza configuración inicial del Router, para ello desde la consola modo privilegiado se procede a ejecutar el comando *no ip domain lookup* que permite desactivar la búsqueda DNS para indicar que si hemos cometido un error en el scrip de configuración nos muestre un aviso indicando el error, se configura el nombre del dispositivo y nombre de dominio del mismo junto con la contraseña cifrada para ingresar al modo privilegiado a través del comando *enable secret*, de igual manera se configura la contraseña para ingresar a la consola con el comando *password* y activándola con *login,* estableciendo en modo de configuración global una longitud mínima de 10 caracteres para las contraseñas con el comando *security passwords min-length 10*, se crea un usuario administrativo con su usuario y contraseña y se configuran las líneas vty para

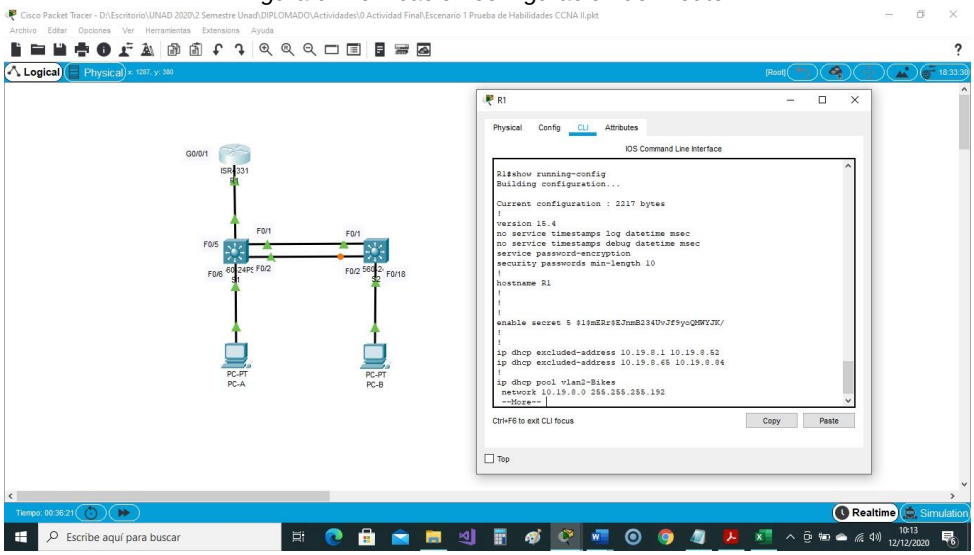
usar la base de datos local *line vty 0 15* y activándolas con *login local*, se configuran las líneas vty para admitir solo correcciones SSH con el comando *transport input ssh*, al salir de las líneas vty se configuran las contraseñas de texto no cifrado *service password-encryption*, se configura el mensaje del día en el *banner MOTD* dejando un aviso para acceso no autorizado, se activa el enrutamiento IPv6 con *ipv6 unicast-routing*, se configura la interfaz G0/0/1 y subinterfaces estableciendo la encapsulación a su respectiva vlan junto con la dirección IPv4, IPv6 y enlace local IPv6, estas son interface g0/0/1.2, interface g0/0/1.3, interface g0/0/1.4, interface g0/0/1.6, a esta última asignándole la vlan nativa y finalmente activando la interfaz G0/0/1con el comando *no shutdown*, se configura la interface Loopback0 (Internet) *interface loopback 0* asignándole una dirección IPv4, IPv6 y dirección local.

Figura 8. Configuración parámetros básicos del Router



Fuente: Autor

Figura 9. Verificación configuración del Router



Fuente: Autor

1.3. Paso 3: Configure S1 y S2.

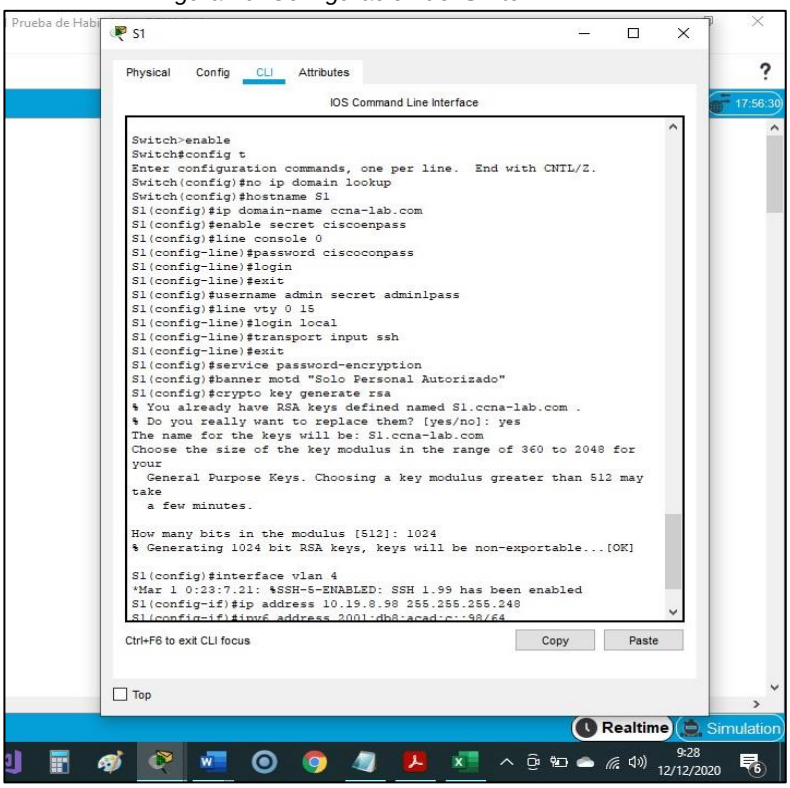
Las tareas de configuración incluyen lo siguiente:

Tabla 7. Configuración del Switch 1

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch(config)#no ip domain lookup
Nombre del switch S1	Switch(config)#hostname S1
Nombre de dominio (ccna-lab.com)	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado (ciscoenpass)	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola (ciscoconpass)	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit
Crear 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 S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd "Solo Acceso Autorizado"
Generar una clave de cifrado RSA (Módulo de 1024 bits)	S1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024
Configurar la interfaz de administración (SVI) Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2 Establecer la dirección IPv6 de capa 3	S1(config)#interface vlan 4 S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address FE80::98 link-local S1(config-if)#description vlan Management S1(config-if)#no shutdown S1(config-if)#exit
Configuración del gateway predeterminado Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4	S1(config)#ip default-gateway 10.19.8.97

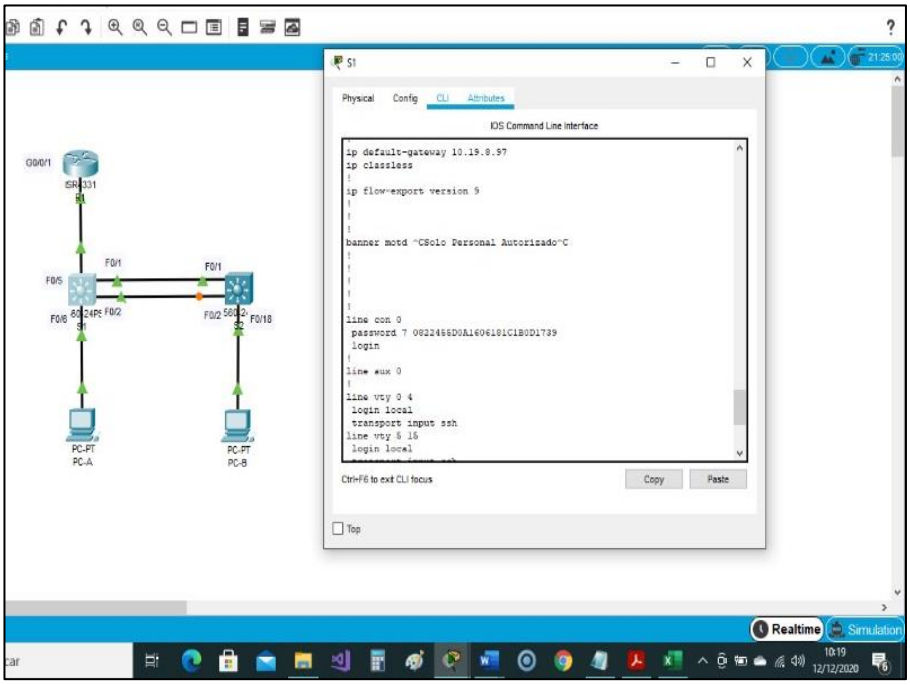
Se realiza configuración inicial del Switch 1, para ello desde la consola modo privilegiado se procede a ejecutar el comando *no ip domain lookup* que permite desactivar la búsqueda DNS para indicar que si hemos cometido un error en el scrip de configuración nos muestre un aviso indicando el error, se configura el nombre del dispositivo y nombre de dominio del mismo junto con la contraseña cifrada para ingresar al modo privilegiado a través del comando *enable secret*, de igual manera se configura la contraseña para ingresar a la consola con el comando *password* y activándola con *login,* estableciendo en modo de configuración global una longitud mínima de 10 caracteres para las contraseñas con el comando *security passwords min-length 10*, se crea un usuario administrativo con su usuario y contraseña y se configuran las líneas vty para usar la base de datos local *line vty 0 15* y activándolas con *login local*, se configuran las líneas vty para admitir solo correcciones SSH con el comando *transport input ssh*, al salir de las líneas vty se configuran las contraseñas de texto no cifrado *service password-encryption*, se configura el mensaje del día en el *banner MOTD* dejando un aviso para acceso no autorizado, se crea una llave de encriptación RSA con el comando *crypto key generate rsa* asignándole una longitud de 1024 bits, se configura la Interfaz administrativa (SVI) correspondiente a la vlan 4 Management asignándole la IPv4 10.19.8.98 y mascara de red 255.255.255.248, dirección IPv6 2001:db8:acad:c::98 prefijo /64 y puerta de enlace local fe80::98, se realiza un descripción y se activa con el comando *no shutdown*, finalmente se configura la puerta de enlace predeterminada 10.19.8.97 para IPv4, no se configura puerta de enlace en IPv6 porque se asigna de manera automática.

Figura 10. Configuración del Switch 1



Fuente: Autor

Figura 11. Verificación configuración Switch 1



Fuente: Autor

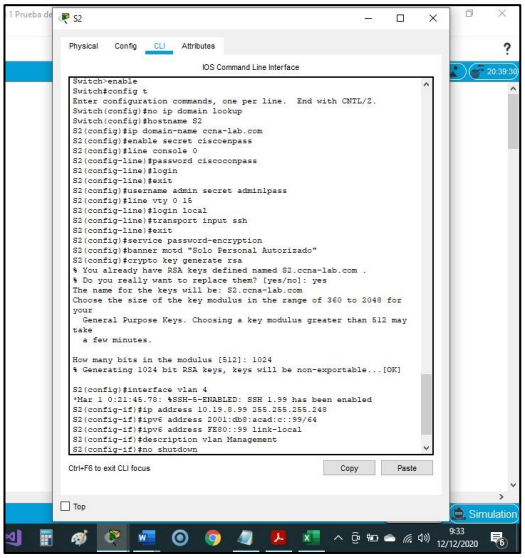
Tabla 8. Configuración Switch 2

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch(config)#no ip domain lookup
Nombre del switch S2	Switch(config)#hostname S2
Nombre de dominio (ccna-lab.com)	S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado (ciscoenpass)	S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola (ciscoconpass)	S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit
Crear un usuario administrativo en la base de datos local (Nombre de usuario: admin Password: admin1pass)	S2(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 15 S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config-line)#transport input ssh S2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption
Configurar un MOTD Banner	S2(config)#banner motd "Solo Personal Autorizado"
Generar una clave de cifrado RSA (Módulo de 1024 bits)	S2(config)#crypto key generate rsa How many bits in the modulus [512]: 1024

Tarea	Especificación
Configurar la interfaz de administración (SVI) Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2 Establecer la dirección IPv6 de capa 3	S2(config)#interface vlan 4 S2(config-if)#ip address 10.19.8.99 255.255.255.248 S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#ipv6 address FE80::99 link-local S2(config-if)#description vlan Management S2(config-if)#no shutdown S2(config-if)#exit
Configuración del gateway predeterminado Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4	S2(config)#ip default-gateway 10.19.8.97

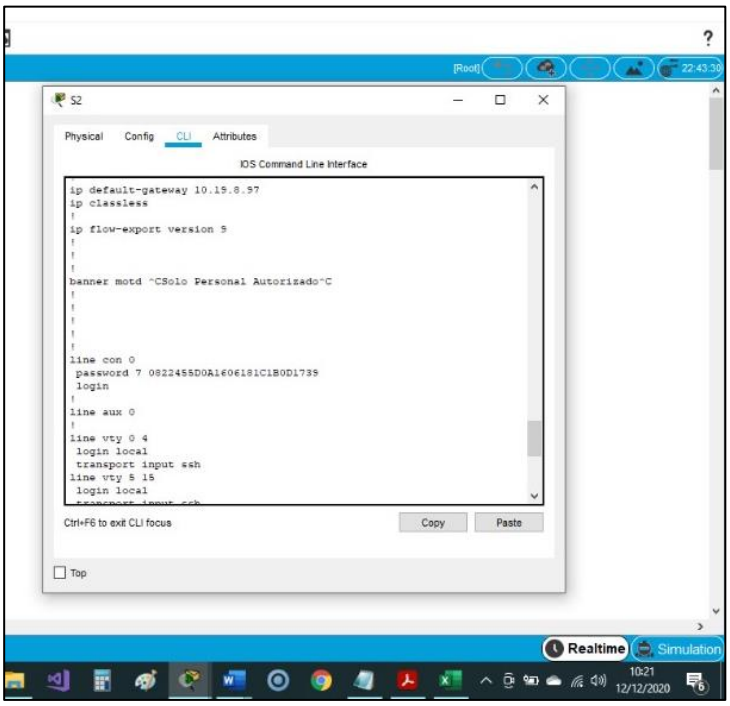
Se realiza configuración inicial del Switch 2, para ello desde la consola modo privilegiado se procede a ejecutar el comando *no ip domain lookup* que permite desactivar la búsqueda DNS para indicar que si hemos cometido un error en el scrip de configuración nos muestre un aviso indicando el error, se configura el nombre del dispositivo y nombre de dominio del mismo junto con la contraseña cifrada para ingresar al modo privilegiado a través del comando *enable secret*, de igual manera se configura la contraseña para ingresar a la consola con el comando *password* y activándola con *login,* estableciendo en modo de configuración global una longitud mínima de 10 caracteres para las contraseñas con el comando *security passwords min-length 10*, se crea un usuario administrativo con su usuario y contraseña y se configuran las líneas vty para usar la base de datos local *line vty 0 15* y activándolas con *login local*, se configuran las líneas vty para admitir solo correcciones SSH con el comando *transport input ssh*, al salir de las líneas vty se configuran las contraseñas de texto no cifrado *service password-encryption*, se configura el mensaje del día en el *banner MOTD* dejando un aviso para acceso no autorizado, se crea una llave de encriptación RSA con el comando *crypto key generate rsa* asignándole una longitud de 1024 bits, se configura la Interfaz administrativa (SVI) correspondiente a la vlan 4 Management asignándole la IPv4 10.19.8.98 y mascara de red 255.255.255.248, dirección IPv6 2001:db8:acad:c::99 prefijo /64 y puerta de enlace local fe80::99, se realiza un descripción y se activa con el comando *no shutdown*, finalmente se configura la puerta de enlace predeterminada 10.19.8.97 para IPv4, no se configura puerta de enlace en IPv6 porque se asigna de manera automática.

Figura 12. Configuración Switch 2



Fuente: Autor

Figura 13. Verificación configuración Switch 2



Fuente: Autor

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

2.1. Paso 4: Configurar S1

- La configuración del S1 incluye las siguientes tareas:

Tabla 9. Configuración de la infraestructura de red (VLAN, Trunking,

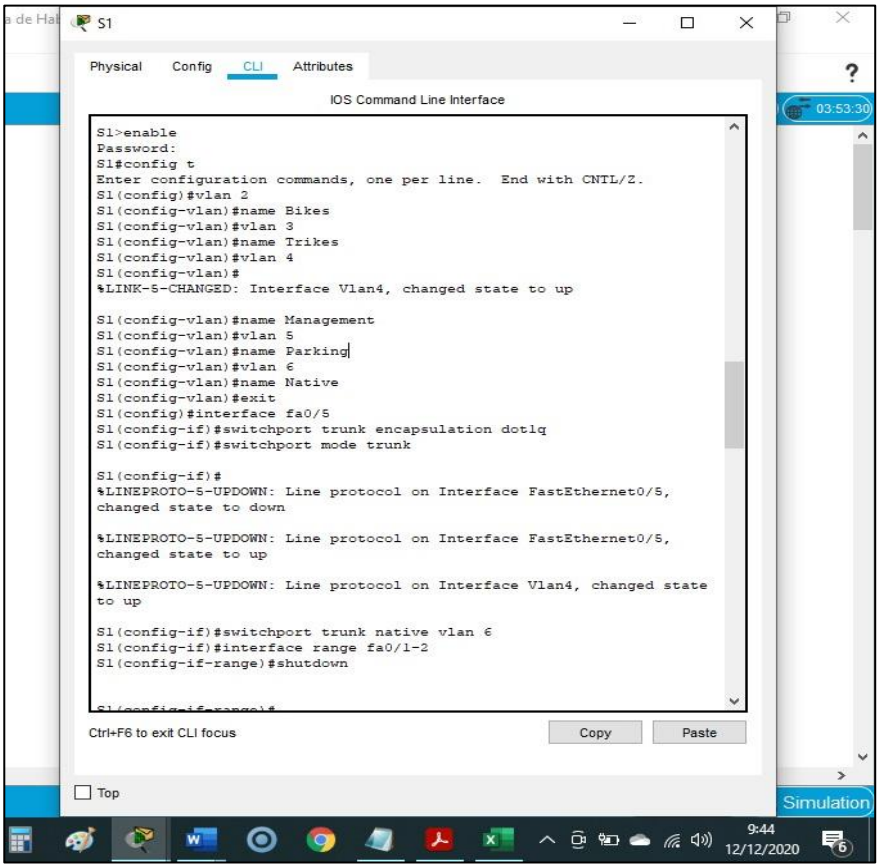
EtherChannel) en Switch 1

Tarea	Especificación
Crear VLAN VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	S1#configure terminal S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#vlan 4 S1(config-vlan)#name Management S1(config-vlan)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#vlan 6 S1(config-vlan)#name Native S1(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1, F0/2 y F0/5	S1(config)#interface fa0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#interface range fa0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6
Crear 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)#interface range fa0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)# S1(config-if-range)#interface Port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6
Configurar el puerto de acceso de host para VLAN 2 Interface F0/6	S1(config-if)#interface fa0/6 S1(config-if)#switchport mode acces S1(config-if)#switchport acces vlan 2
Configurar la seguridad del puerto en los puertos de acceso Permitir 3 direcciones MAC	S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S1(config-if-range)#interface range fa0/3-4 S1(config-if-range)#switchport acces vlan 5 S1(config-if-range)#description No esta en uso S1(config-if-range)#shutdown S1(config-if-range)#interface range fa0/7-24 S1(config-if-range)#switchport acces vlan 5 S1(config-if-range)#description No esta en uso S1(config-if-range)#shutdown S1(config-if-range)#interface range g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description No esta en uso S1(config-if-range)#shutdown

Desde la consola, modo privilegiado, configuración global se crean las vlan 2Bikes, vlan 3-Trikes, vlan 4-Management, vlan 5-Parking y vlan 6-Native, se crean las trocales 802.1Q que usen la vlan nativa interfaces fa0/1, fa0/2 y fa0/5, inicialmente se configura la interface fa0/5 utilizando solo en esta referencia de

Switch el comando de encapsulación *switchport trunk encapsulation dot1q*, y para implementar la interface con el código *switchport mode trunk* direccionándola a la vlan 6 nativa *switchport trunk native vlan 6*, para configurar las fa0/1 y fa0/2 se usa un rango *interface range fa0/1-2*, mientras se configura la EtherChannel se desactiva el rango anterior con *shutdown* para evitar conflictos, se configura la *interface range fa0/1-2* utilizando el comando de encapsulación *switchport trunk encapsulation dot1q*, y para implementar la interface con el código *switchport mode trunk* direccionándola a la vlan 6 nativa *switchport trunk native vlan 6*, se crea la EtherChannel que utilice el grupo de interfaces fa0/1-2 con el código *channel-group 1 mode active* y usar LACP creando el grupo 1, luego se entra a la interfaz de este con *interface Port-channel 1* y configurar las troncales, se configura un puerto de acceso para la vlan 2-Bikes que use la fa0/2 con el comando *switchport acces vlan 2*, configuración de seguridad en los puertos de aceso que permita 3 direcciones MAC, se activa la seguridad en la interfaz estableciendo máximo 3 direcciones MAC con *switchport port-security maximum 3*, se aseguran todas las interfaces sin usar asignándolas a la vlan 5-Parking e indicando que no están en uso y apagar *shutdown*, estas son fa0/3-4, fa0/7-24 y g0/1-2, finalmente se activa el rango de interfaz fa0/1-2 con *no shutdown*.

Figura 14. Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) en Switch 1



Fuente: Autor

2.2. Paso 5: Configure el S2.

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

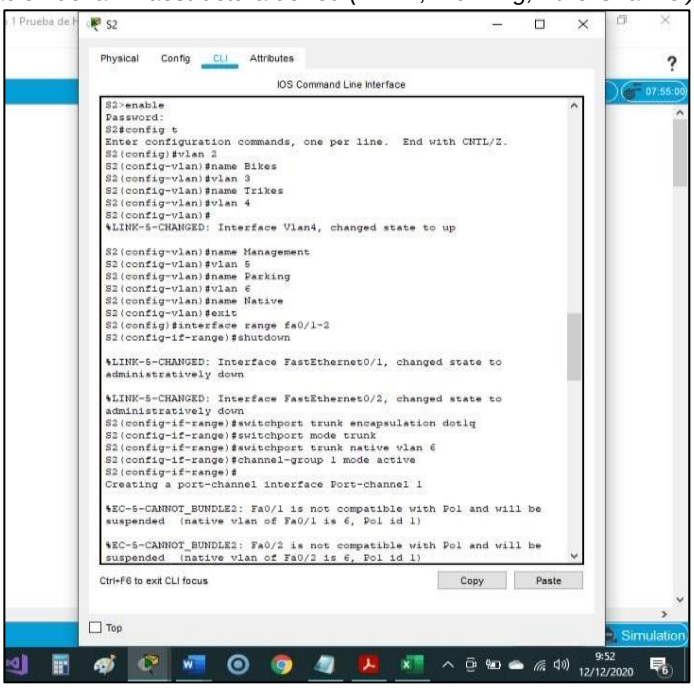
Tabla 10. Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) en Switch 2

Tarea	Especificación
Crear VLAN VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	S2>enable Password: S2#configure terminal S2(config)#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 S2(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1 y F0/2	S2(config)#interface range fa0/1-2 S2(config-if-range)#shutdown S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 6
Crear 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)#interface Port-channel 1 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6
Configurar el puerto de acceso del host para la VLAN 3 Interfaz F0/18	S2(config-if)# interface fa0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configure port-security en los access ports permite 3 MAC addresses	S2(config-if)#switchport port-security maximum 3
Asegure todas las interfaces no utilizadas. Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S2(config-if)#interface range fa0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description No esta en uso S2(config-if-range)#shutdown S2(config-if-range)#interface range fa0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description No esta en uso S2(config-if-range)#shutdown

Desde la consola, modo privilegiado, configuración global se crean las vlan 2Bikes, vlan 3-Trikes, vlan 4-Management, vlan 5-Parking y vlan 6-Native, se crean las trocales 802.1Q que usen la Vlan nativa interfaces fa0/1 y fa0/2,para configurar las fa0/1 y fa0/2 se usa un rango *interface range fa0/1-2*, mientras se

configura la EtherChannel se desactiva el rango anterior con *shutdown* para evitar conflictos, se configura la *interface range fa0/1-2* utilizando el comando de encapsulación *switchport trunk encapsulation dot1q*, y para implementar la interface con el código *switchport mode trunk* direccionándola a la vlan 6 nativa *switchport trunk native vlan 6*, se crea la EtherChannel que utilice el grupo de interfaces fa0/1-2 con el código *channel-group 1 mode active* y usar LACP creando el grupo 1, luego se entra a la interfaz de este con *interface Port-channel 1* y configurar las troncales, se configura un puerto de acceso para la vlan 3Trikes que use la fa0/18 con el comando *switchport acces vlan 3*, configuración de seguridad en los puertos de aceso que permita 3 direcciones MAC, se activa la seguridad en la interfaz estableciendo máximo 3 direcciones MAC con *switchport port-security maximum 3*, se aseguran todas las interfaces sin usar asignándolas a la vlan 5-Parking e indicando que no están en uso y apagar *shutdown*, estas son fa0/3-17, fa0/19-24 y g0/1-2, finalmente se activa el rango de interfaz fa0/1-2 con *no shutdown*.

Figura 15. Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) en Switch 2



Fuente: Autor

Tabla 11. Activación interface fa0/1-2 en s1 y S2

Tarea	Especificación
Activar el rango fa0/1-2 en switch 1	S1(config)#interface range fa0/1-2 S1(config-if-range)#interface range fa0/1-2 S1(config-if-range)#no shutdown
Activar el rango fa0/1-2 en switch 2	S2(config)#interface range fa0/1-2 S2(config-if-range)#interface range fa0/1-2 S2(config-if-range)#no shutdow

3. Parte 3: Configurar soporte de host

3.1. Paso 1: Configure R1

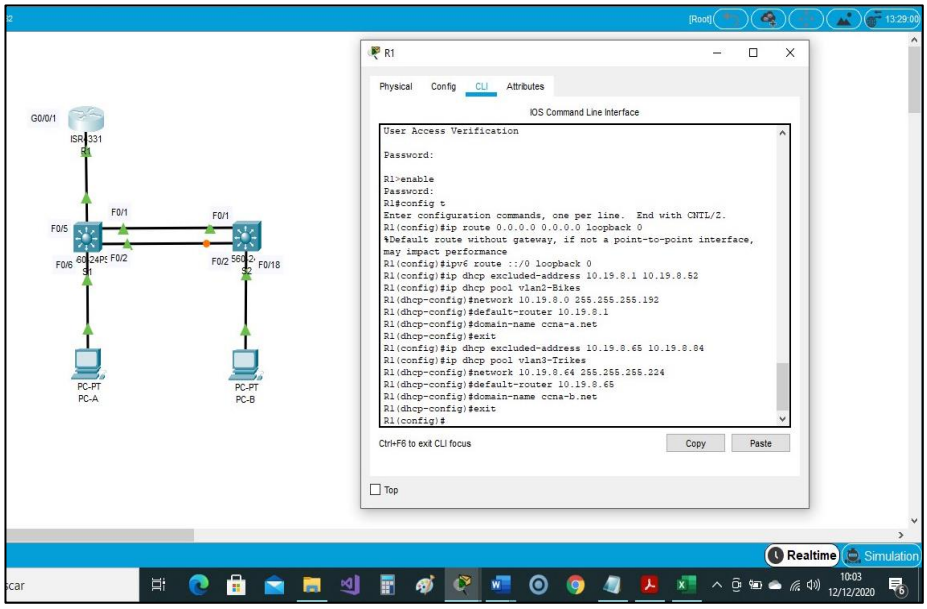
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 12. Configuración de soporte de host en Router

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 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 R1(dhcp-config)#exit
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 R1(dhcp-config)#exit

En el Router se asignan las rutas predeterminadas IPv4 *ip route 0.0.0.0 0.0.0.0 loopback 0* y IPv6 *ipv6 route ::/0 loopback 0*, las cuales direccionan el tráfico a la interfaz Loopback 0 (Lo0), estas son las rutas estáticas para conectar con Internet, se configura IPv4 DCHP para vlan 2-Bikes conformado solamente por las ultimas 10 direcciones de subred la cual está en el rango 10.19.8.1 – 10.19.8.52, para ello se aplicó para excluir estas 10 direcciones el comando *ip dhcp excluded-address 10.19.8.1 10.19.8.52*, y para el pool de DHCP *ip dhcp pool vlan2-Bikes*, red y mascara de red *network 10.19.8.0 255.255.255.192*, puerta de enlace predeterminada *default-router 10.19.8.1*, nombre de dominio *domain-name ccna-a.net*, finalmente se configura DHCP IPv4 para vlan 3-Trikes y grupo DHCP conformado por las ultimas 10 direcciones con sus respectivas especificaciones, se configura IPv4 DCHP para vlan 3-Trikes conformado solamente por las ultimas 10 direcciones de subred la cual está en el rango 10.19.8.65 – 10.19.8.84, para ello se aplicó para excluir estas 10 direcciones el comando *ip dhcp excluded-address 10.19.8.65 10.19.8.84*, y para el pool de DHCP *ip dhcp pool vlan3-Trikes*, red y mascara de red *network 10.19.8.64 255.255.255.224*, puerta de enlace predeterminada *default-router 10.19.8.65*, nombre de dominio *domain-name ccna-b.net*.

Figura 16. Configuración de soporte de host en Router



Fuente: Autor

3.2. Paso 2: Configurar los servidores

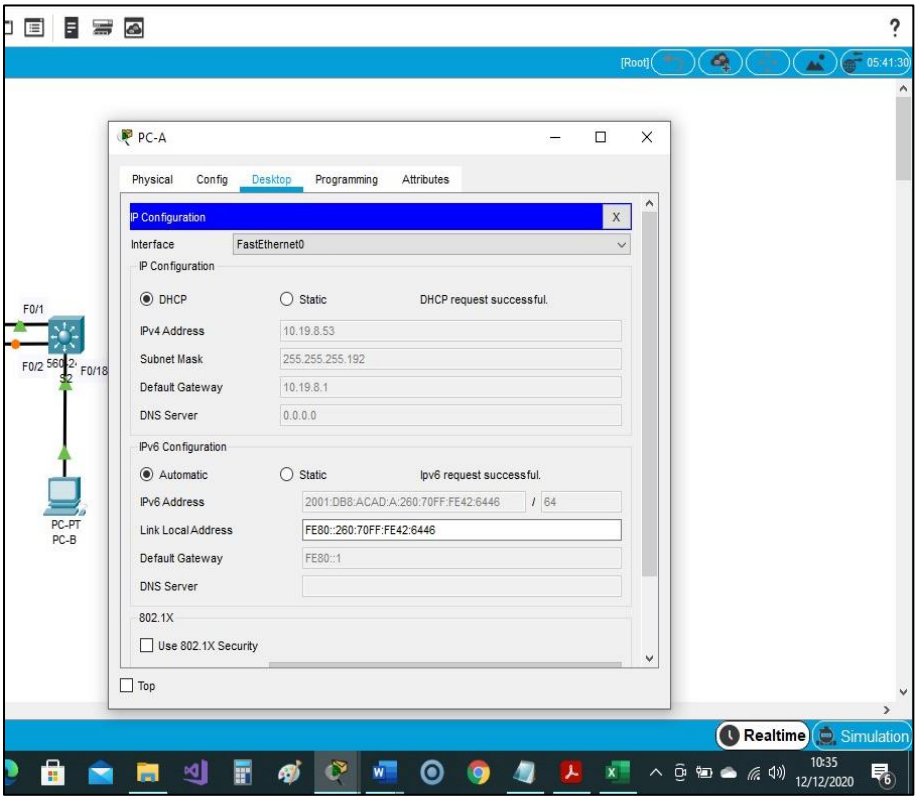
Configure los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, registre las configuraciones de red del host con el comando ipconfig /all.

En las PC-A y B se activa el DHCP para IPv4 y configuración automática para IPv6

Tabla 13. Configuración de red del PC-A

Configuración de red de PC-A	
Descripción	Datos por DHCP
Dirección física	0060.7042.6446
Dirección IP	10.19.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

Figura 17. Registro de configuraciones en PC-A

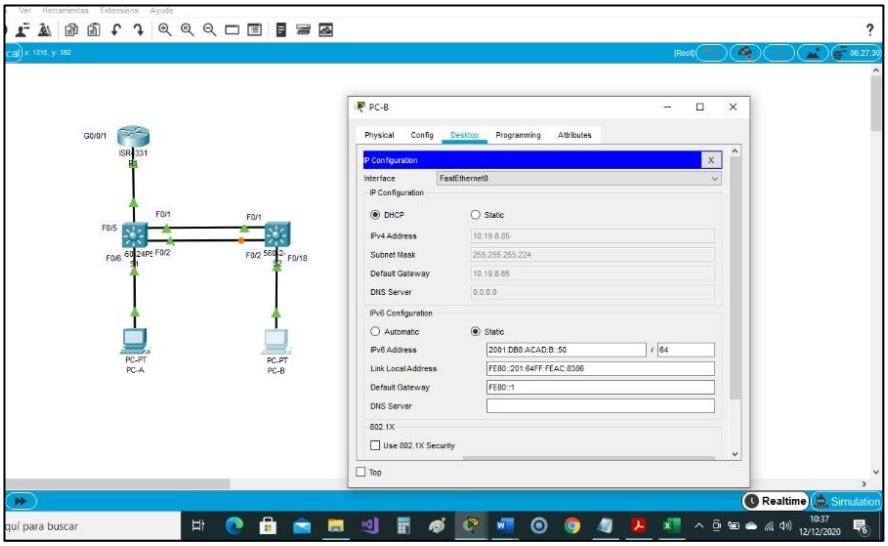


Fuente: Autor

Tabla 14. Configuración de red del PC-B

Configuración de red de PC-B	
Descripción	Datos por DHCP
Dirección física	0001.64AC.8386
Dirección IP	10.19.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::1

Figura 18. Registro de configuraciones en PC-B



Fuente: Autor

4. 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.

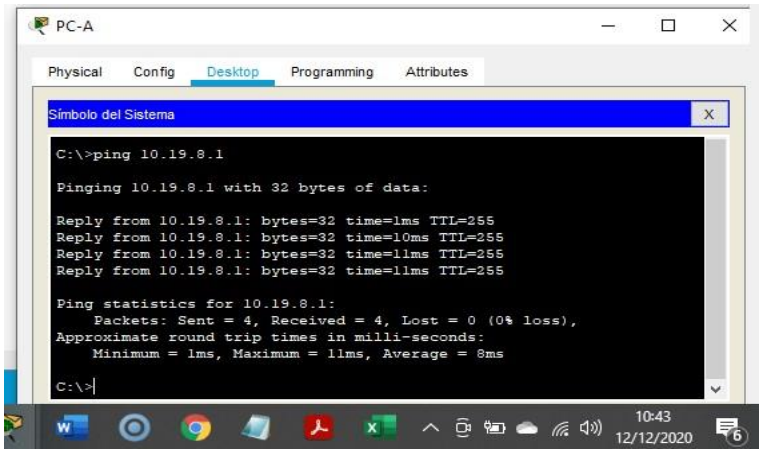
Nota: Si fallan los pings en las computadoras host, desactive temporalmente el firewall de la computadora y vuelva a realizar la prueba.
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 15. Verificación de los dispositivos de red

Desde	A	de Internet	Dirección IP	Resultados del ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	Si hay respuesta
		IPv6	2001:db8:acad:a: :1	Si hay respuesta
	R1, G0/0/1.3	Dirección	10.19.8.65	Si hay respuesta
		IPv6	2001:db8:acad:b: :1	Si hay respuesta
	R1, G0/0/1.4	Dirección	10.19.8.97	Si hay respuesta
		IPv6	2001:db8:acad:c: :1	Si hay respuesta
	S1, VLAN 4	Dirección	10.19.8.98	Si hay respuesta
		IPv6	2001:db8:acad:c: :98	Se configura puerta de enlace IPv6 route ::/0 2001:db8:acad:c::1 y Si hay respuesta
	S2, VLAN 4	Dirección	10.19.8.99	Si hay respuesta

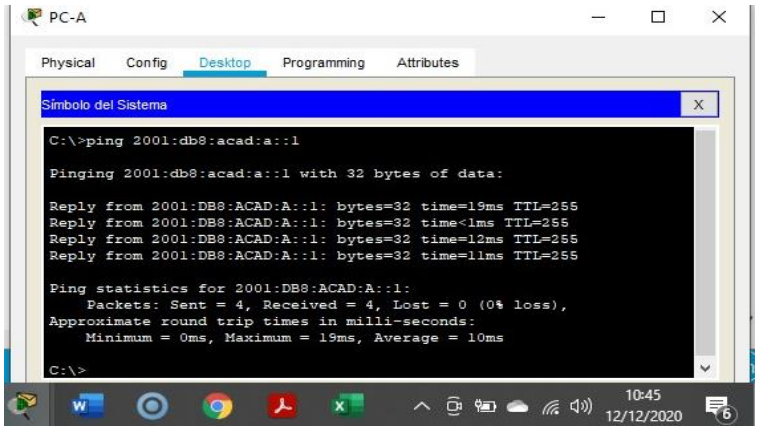
		IPv6	2001:db8:acad:c: :99	Se configura puerta de enlace IPv6 route ::/0 2001:db8:acad:c::1 y Si hay respuesta
	PC-B	Dirección	10.19.8.85	Si hay respuesta
		IPv6	2001:db8:acad:b: :50	Se asigna IPv6 estática, prefijo 64 y puerta de enlace fe80::1 Si hay respuesta
	R1 Bucle 0	Dirección	209.165.201.1	Si hay respuesta
		IPv6	2001:db8:acad:209: :1	Si hay respuesta
	R1 Bucle 0	Dirección	209.165.201.1	Si hay respuesta
		IPv6	2001:db8:acad:209: :1	Si hay respuesta
	R1, G0/0/1.2	Dirección	10.19.8.1	Si hay respuesta
		IPv6	2001:db8:acad:a: :1	Si hay respuesta
Desde	**A**	**de Internet**	**Dirección IP**	**Resultados del ping**
PC-B	R1, G0/0/1.3	Dirección	10.19.8.65	Si hay respuesta
		IPv6	2001:db8:acad:b: :1	Si hay respuesta
	R1, G0/0/1.4	Dirección	10.19.8.97	Si hay respuesta
		IPv6	2001:db8:acad:c: :1	Si hay respuesta
	S1, VLAN 4	Dirección	10.19.8.98	Si hay respuesta
		IPv6	2001:db8:acad:c: :98	Si hay respuesta
	S2, VLAN 4	Dirección	10.19.8.99.	Si hay respuesta
		IPv6	2001:db8:acad:c: :99	Si hay respuesta

Figura 19. Ping desde PC-A a R1, G0/0/1.2 – Ipv4 10.19.8.1



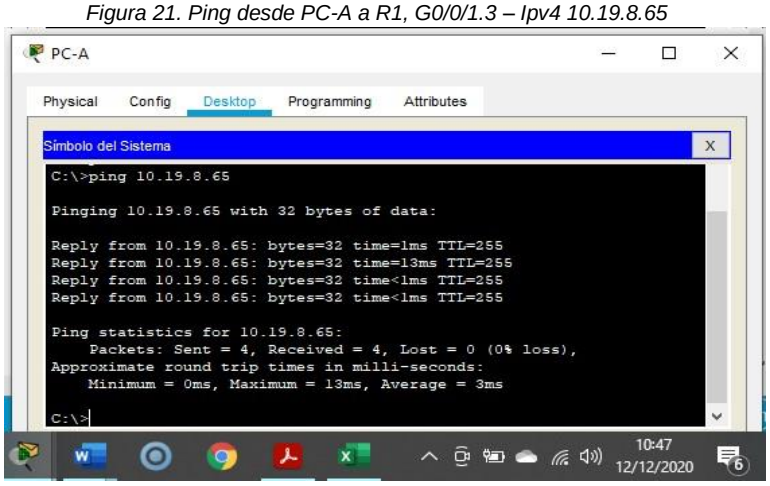
Fuente: Autor

Figura 20. Ping desde PC-A a R1, G0/0/1.2 – Ipv6 2001:db8:acad:a: :1



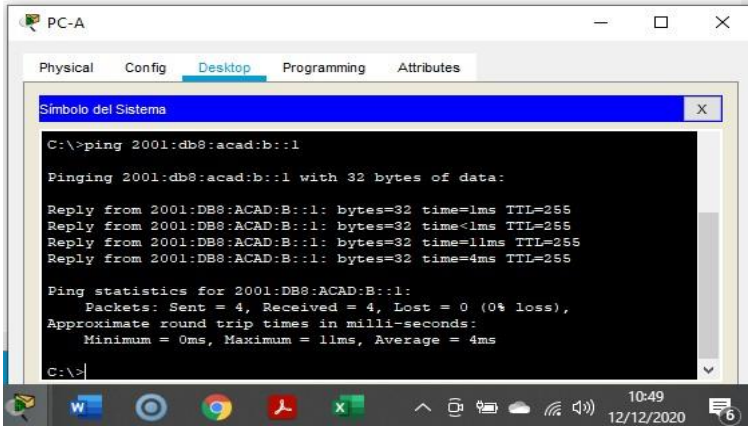
Fuente: Autor

Figura 21. Ping desde PC-A a R1, G0/0/1.3 – Ipv4 10.19.8.65



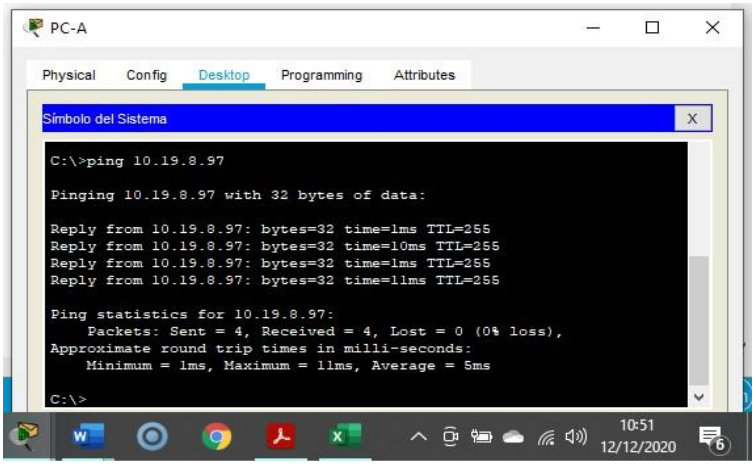
Fuente: Autor

Figura 22. Ping desde PC-A a R1, G0/0/1.3 – Ipv6 2001:db8:acad:b: :1



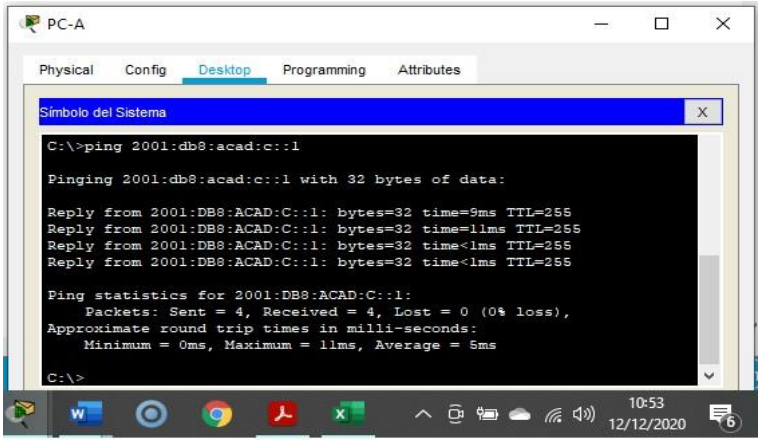
Fuente: Autor

Figura 23. Ping desde PC-A a R1, G0/0/1.4 – Ipv4 10.19.8.97



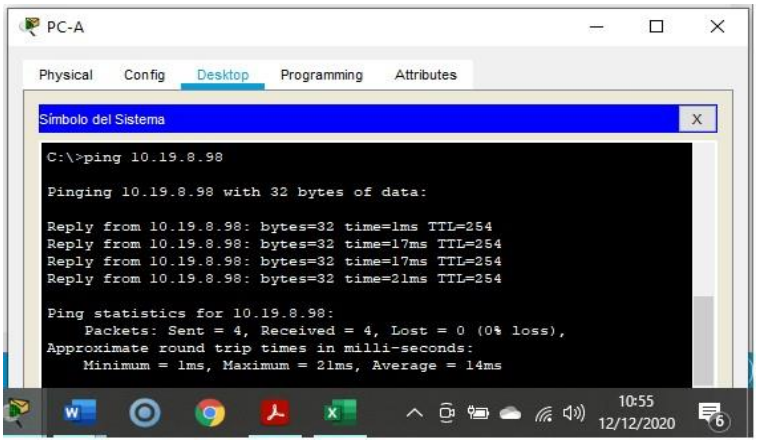
Fuente: Autor

Figura 24. Ping desde PC-A a R1, G0/0/1.4 – Ipv6 2001:db8:acad:c: :1



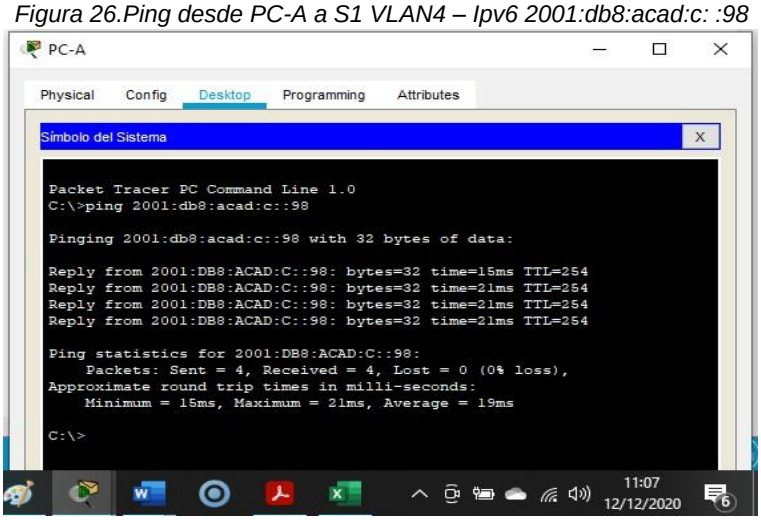
Fuente: Autor

Figura 25. Ping desde PC-A a S1 VLAN4 – Ipv4 10.19.8.98



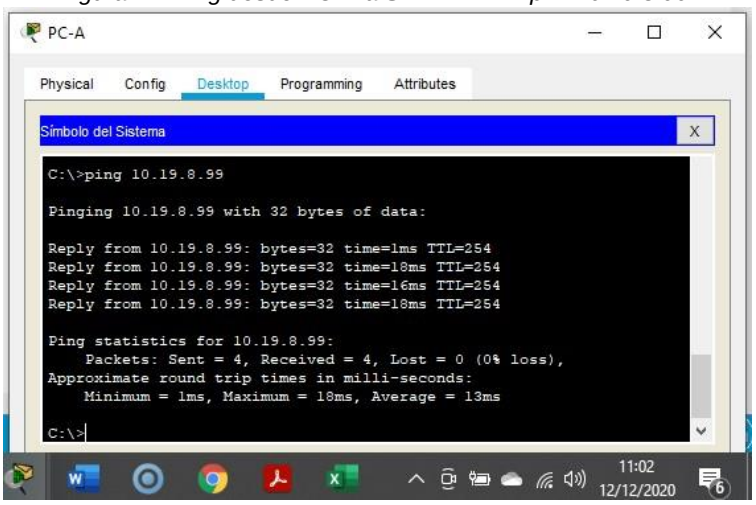
Fuente: Autor

Figura 26.Ping desde PC-A a S1 VLAN4 – Ipv6 2001:db8:acad:c: :98



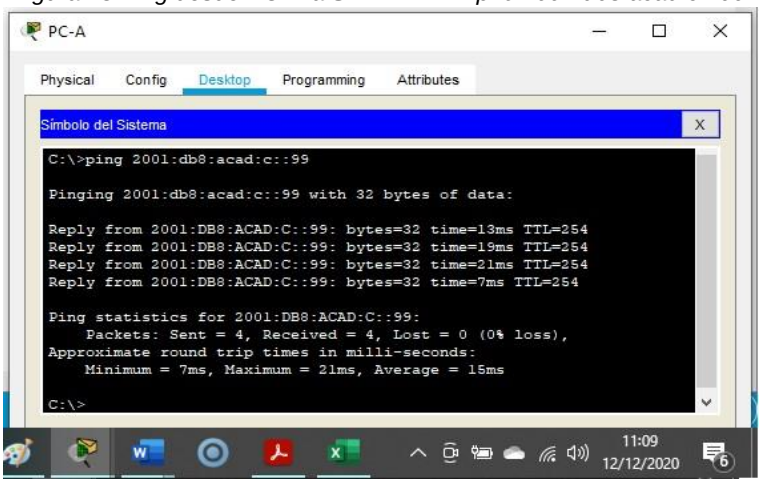
Fuente: Autor

Figura 27. Ping desde PC-A a S2 VLAN4 – Ipv4 10.19.8.99.



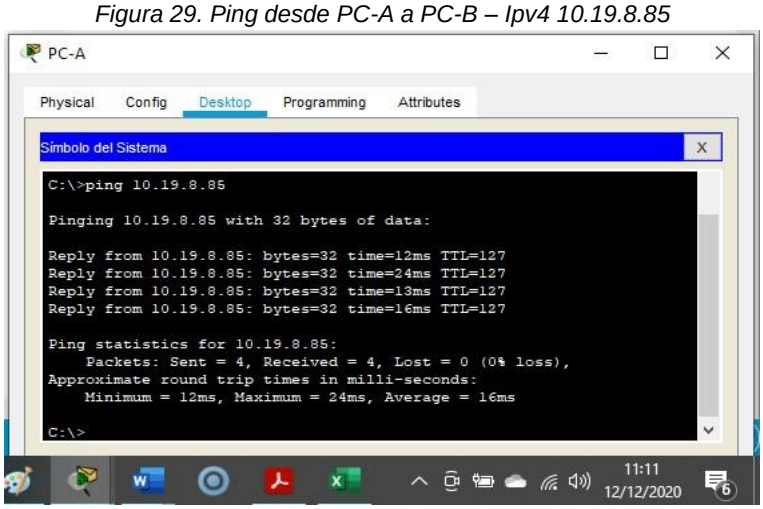
Fuente: Autor

Figura 28.Ping desde PC-A a S2 VLAN4 – Ipv6 2001:db8:acad:c: :99



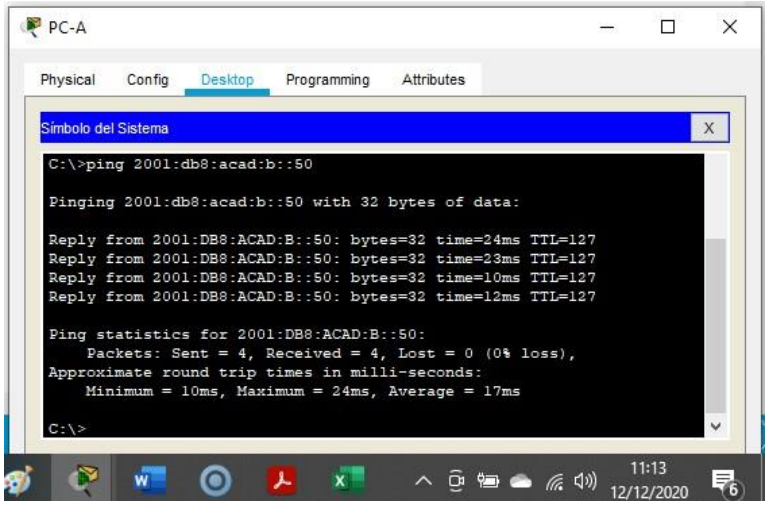
Fuente: Autor

Figura 29. Ping desde PC-A a PC-B – Ipv4 10.19.8.85



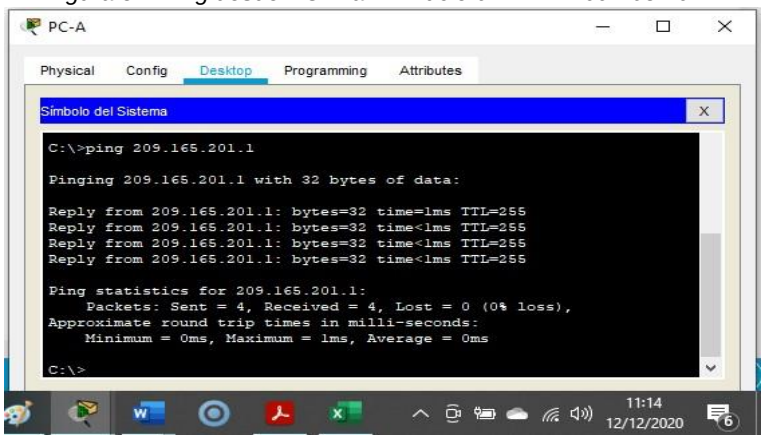
Fuente: Autor

Figura 30. Ping desde PC-A a PC-B – Ipv6 2001:db8:acad:b: :50



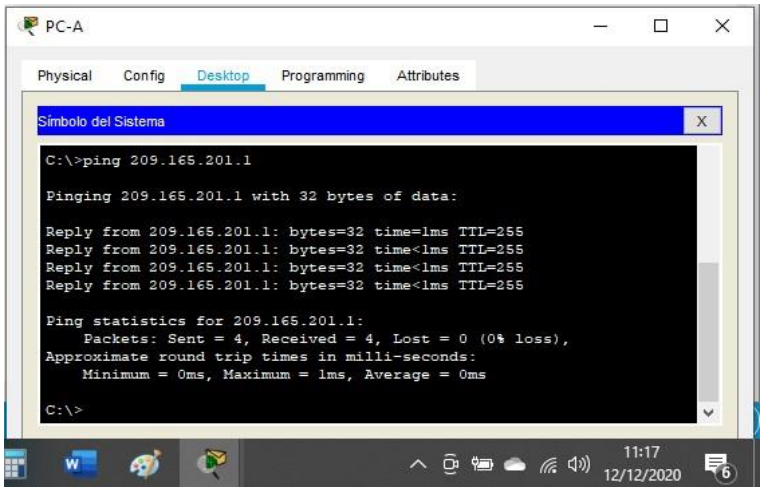
Fuente: Autor

Figura 31. Ping desde PC-A a R1 Bucle 0 – IPv4 209.165.201.1



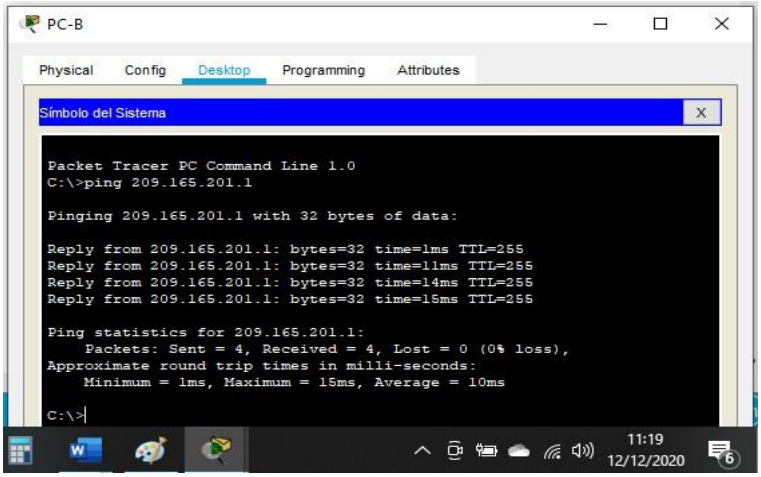
Fuente: Autor

Figura 32. Ping desde PC-A a R1 Bucle 0 – Ipv6 2001:db8:acad:209: :1



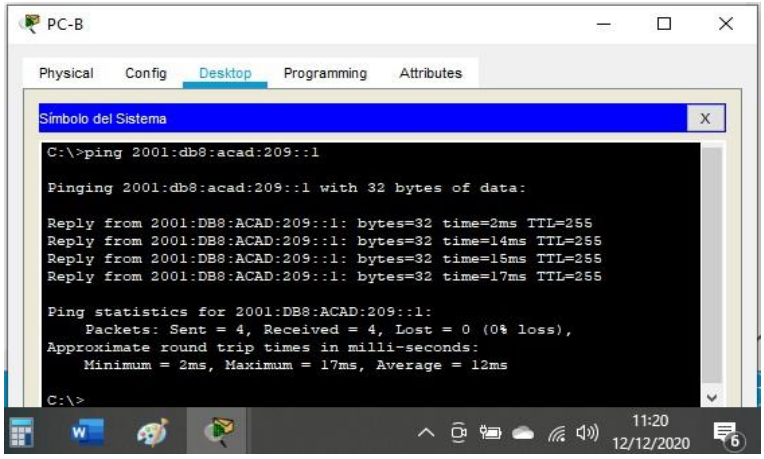
Fuente: Autor

Figura 33. Ping desde PC-B a R1 Bucle 0 – Ipv4 209.165.201.1



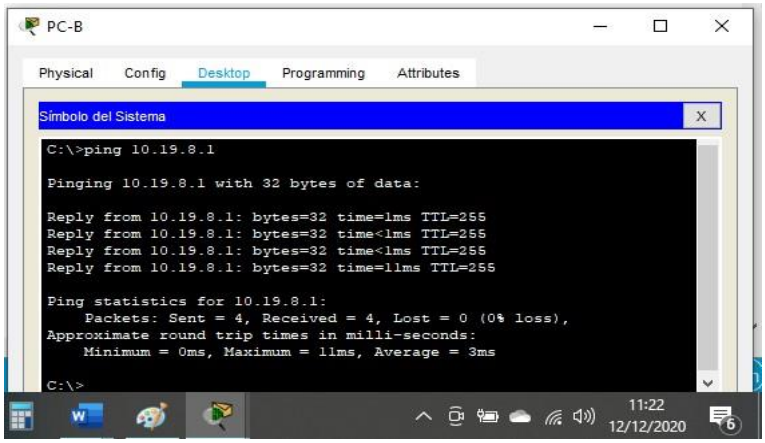
Fuente: Autor

Figura 34. Ping desde PC-B a R1 Bucle 0 – Ipv6 2001:db8:acad:209: :1



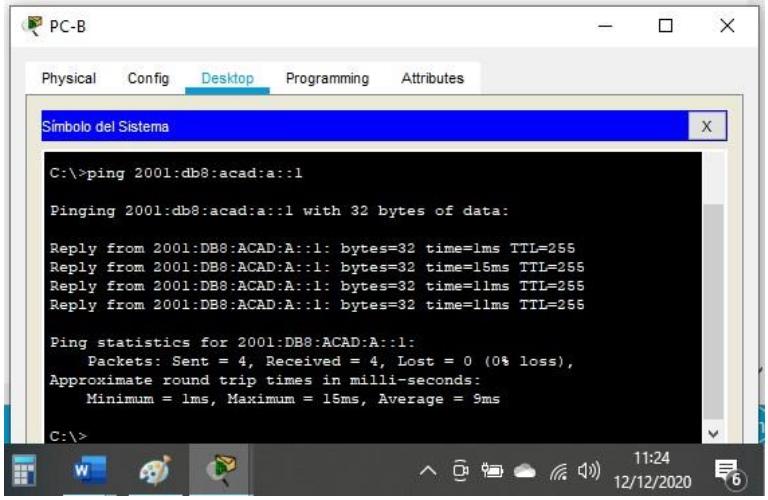
Fuente: Autor

Figura 35. Ping desde PC-B a R1, G0/0/1.2 – Ipv4 10.19.8.1



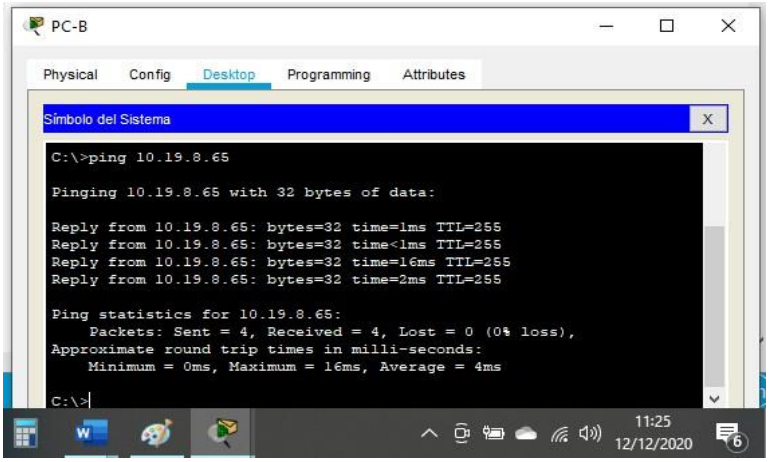
Fuente: Autor

Figura 36. Ping desde PC-B a R1, G0/0/1.2 – Ipv6 2001:db8:acad:a: :1



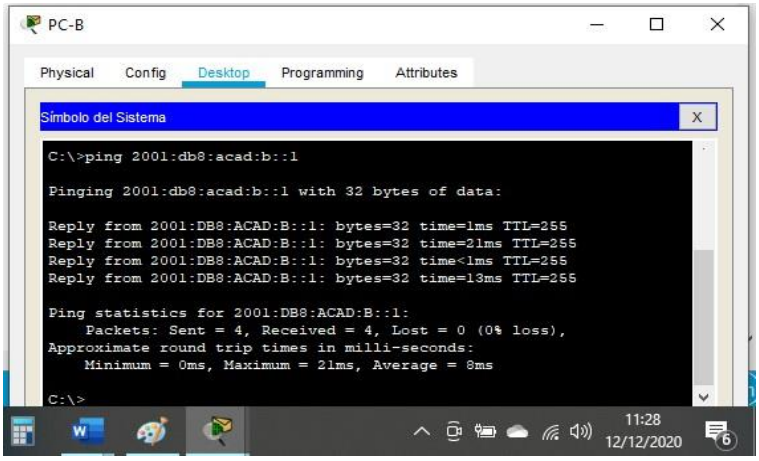
Fuente: Autor

Figura 37. Ping desde PC-B a R1, G0/0/1.3 – Ipv4 10.19.8.65



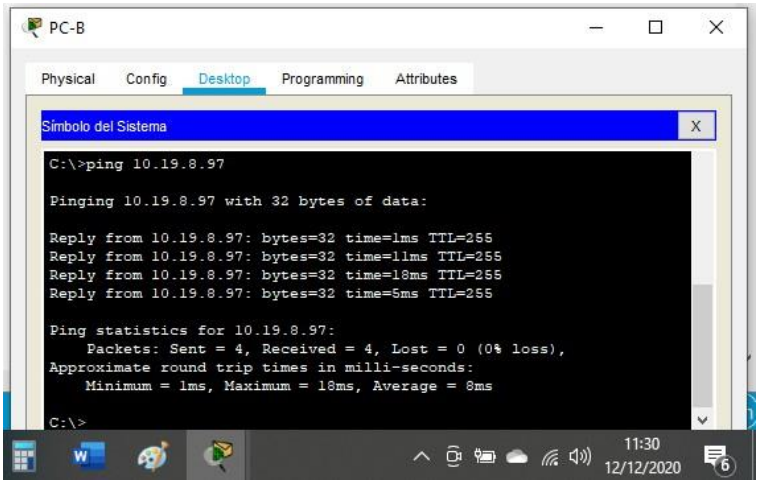
Fuente: Autor

Figura 38. Ping desde PC-B a R1, G0/0/1.3 – Ipv6 2001:db8:acad:b: :1



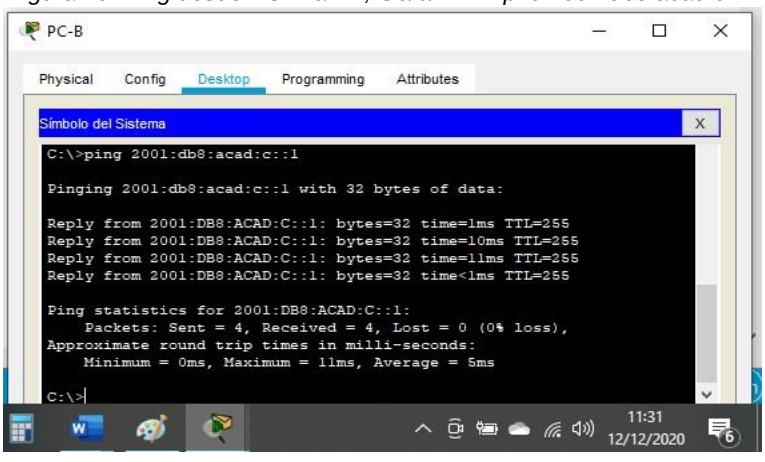
Fuente: Autor

Figura 39. Ping desde PC-B a R1, G0/0/1.4 – Ipv4 10.19.8.97



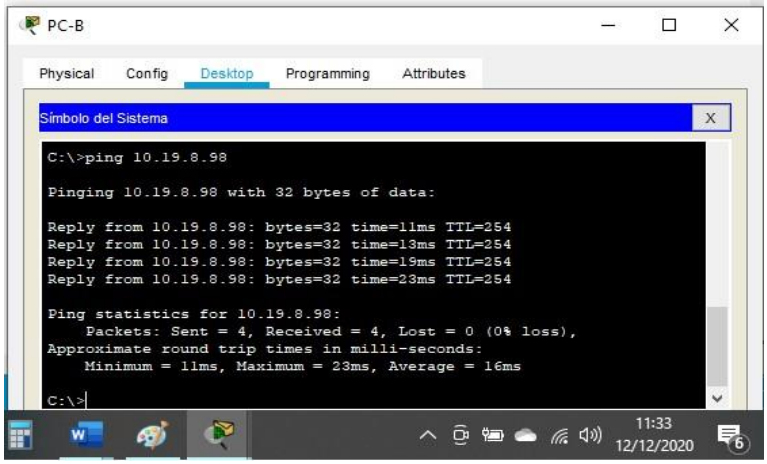
Fuente: Autor

Figura 40. Ping desde PC-B a R1, G0/0/1.4 – Ipv6 2001:db8:acad:c: :1



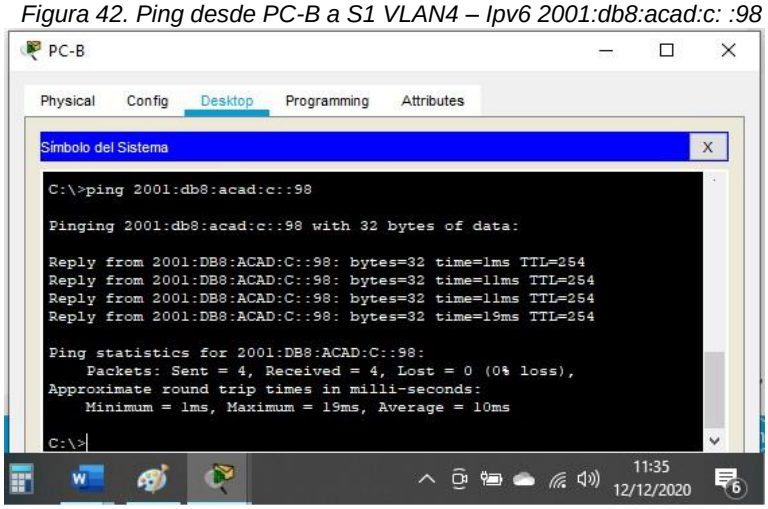
Fuente: Autor

Figura 41. Ping desde PC-B a S1 VLAN4 – Ipv4 10.19.8.98



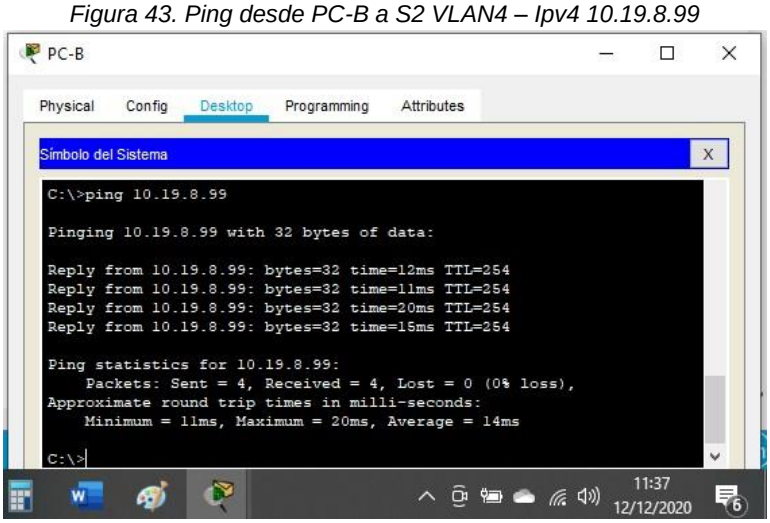
Fuente: Autor

Figura 42. Ping desde PC-B a S1 VLAN4 – Ipv6 2001:db8:acad:c: :98



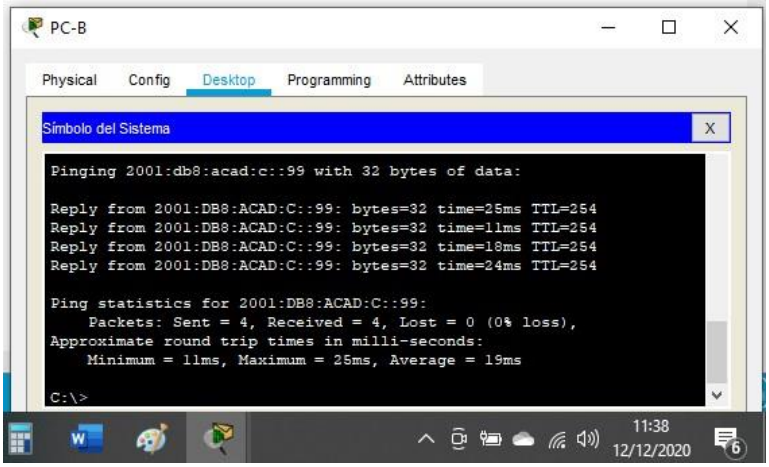
Fuente: Autor

Figura 43. Ping desde PC-B a S2 VLAN4 – Ipv4 10.19.8.99



Fuente: Autor

Figura 44. Ping desde PC-B a S2 VLAN4 – Ipv6 2001:db8:acad:c: :99



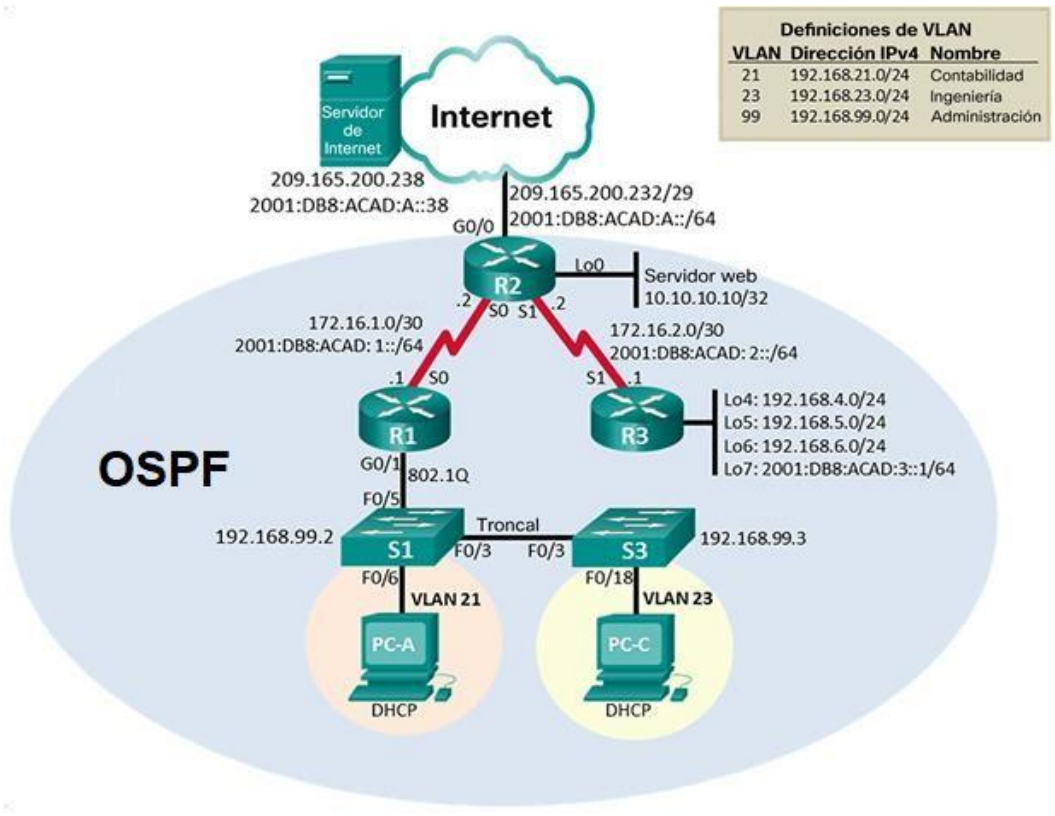
Fuente: Autor

5. 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.

Topología

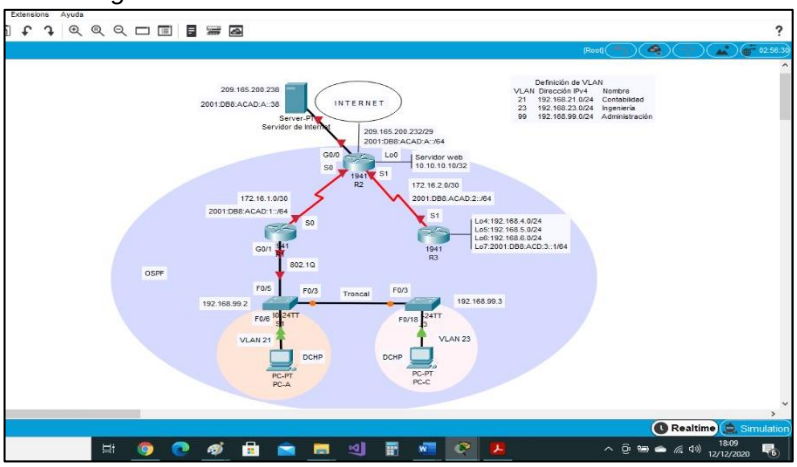
Figura 45. Topología escenario 2



Fuente: Documento Cisco

En el simulador Packet Tracer versión 7.3.1 se crea la topología de red utilizando para ello 3 Routers Cisco 1941, 2 Switchs Cisco 2960, 2 Computadoras, 1 Servidor y cables de cobre directos para la respectiva conexión.

Figura 46. Simulación Escenario 2 en Packet Tracer



Fuente: Autor

5.1. Parte 1: Inicializar dispositivos

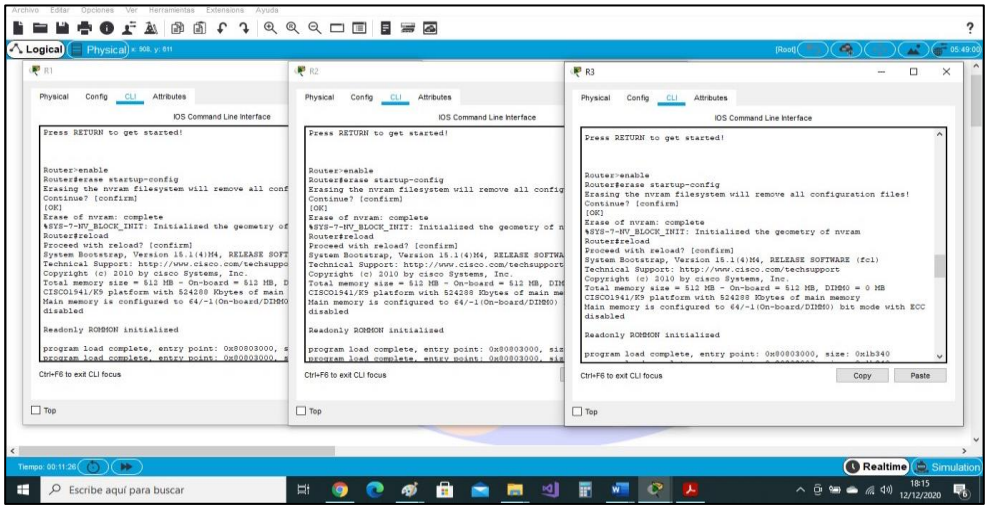
5.1.1. Paso 1. Inicializar y volver a cargar los routers y los switches

Tabla 16. Eliminar las configuraciones de inicio de los Routers y vuelva a cargarlos.

Tarea	Especificación
Ingresar al modo privilegiado	Router>enable
Restablecer valores predeterminados	Router#erase startup-config
Reiniciar el Router	Router#reload

Se accede al Router 1,2 y 3 a través de la consola en modo privilegiado para borrar cualquier configuración de inicio con el comando *erase startup-config* el cual borra el contenido de la NVRAM, posteriormente se reinicia el Router con el comando *reload*, quedando esté listo para su configuración inicial.

Figura 47. Eliminación de configuraciónes y reinicio de los routers



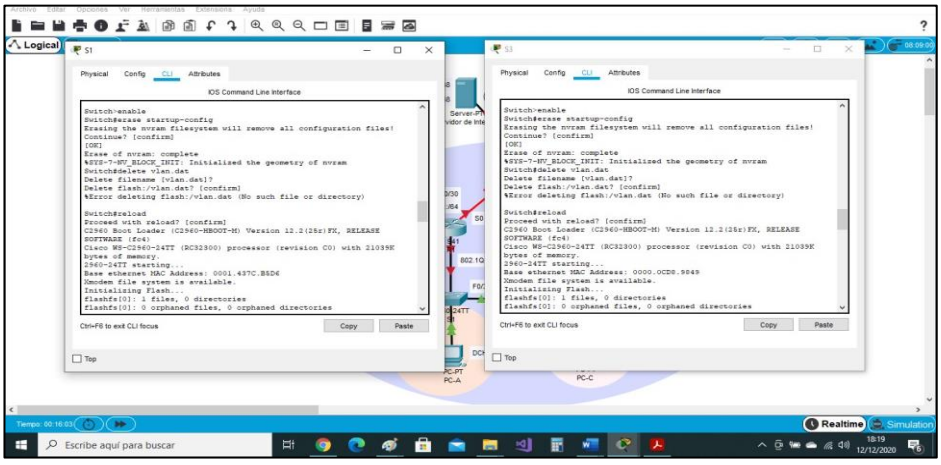
Fuente: Autor

Tabla 17. Eliminar las configuraciones de inicio de los Switchs y vuelva a cargarlos.

Tarea	Especificación
Ingresar al modo privilegiado	Switch>enable
Restablecer valores predeterminados	Switch#erase startup-config
Eliminar Vlan	Switch#delete vlan.dat
Reiniciar el Router	Switchr#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show flash

Se accede al Switch 1 y 2 a través de la consola en modo privilegiado para ejecutar el comando *erase startup-config* el cual borra el contenido de la NVRAM junto con el comando *delete vlan.dat* el cual elimina la base de datos de la vlan, este proceso permite restaurar el switch y borrar cualquier configuración de inicio, posteriormente se reinicia con el comando *reload*, quedando esté listo para su configuración inicial, con el comando show flash se verifica que la base de datos VLAN se halla borrado de la memoria flash.

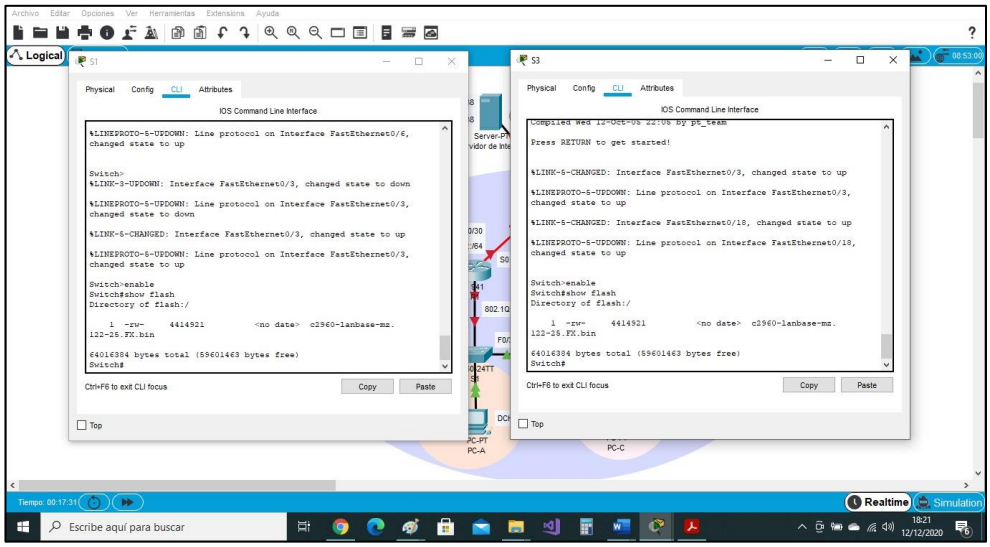
Figura 48. Eliminación configuraciones y reinicio de los Switchs



Fuente: Autor

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

Figura 49. Verificación eliminación base de datos en switches



Fuente: Autor

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

6.1. Paso 1. Configurar la computadora de Internet

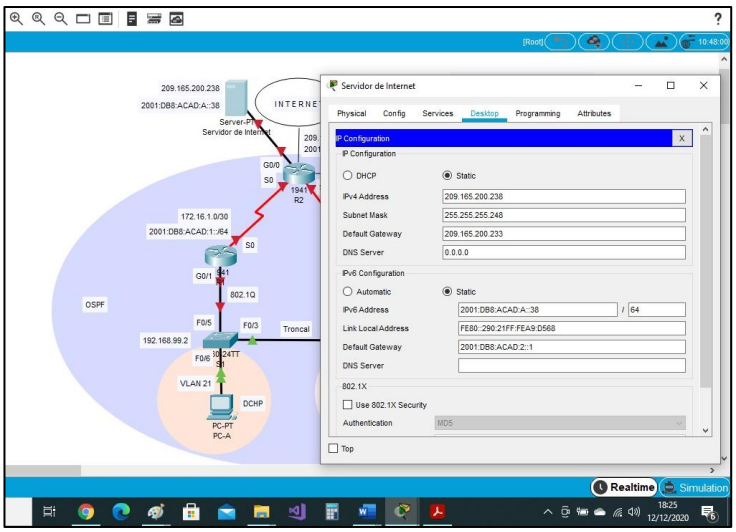
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 18. Configuración Servidor de Internet.

Elemento o tarea de configuración	**Especificación**
Dirección IPv4	209.165200.238
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:2::1

En el Servidor de Internet se asigna la IPv4 con su máscara de subred y Gateway predeterminado, del mismo modo se asigna la IPv6 con prefijo 64 y el Gateway predeterminado IPv6.

Figura 50. Configuración Servidor 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.

6.2. Paso 2. Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 19. Configuración Router 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal 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 passwordencryption
Mensaje MOTD, Se prohíbe el acceso no autorizado.	R1(config)#banner motd "Solo personal autorizado"

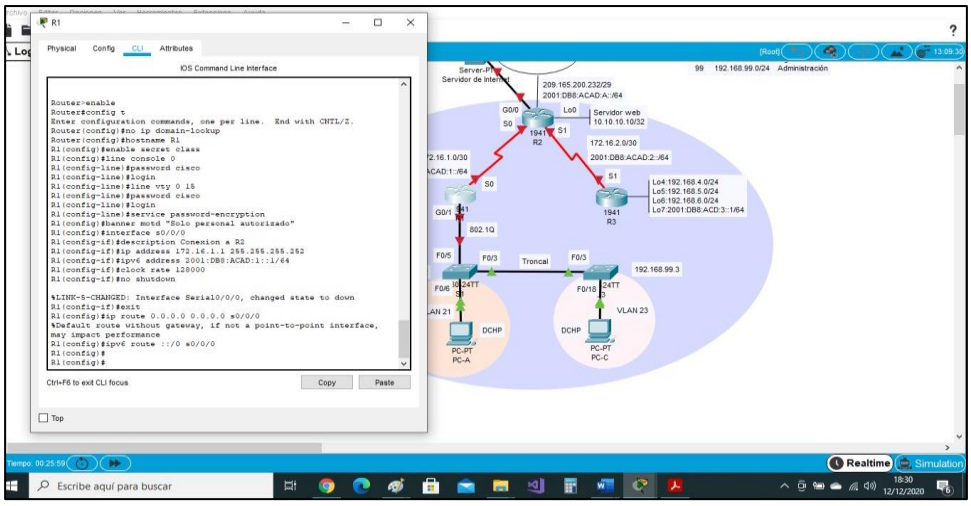
Interfaz S0/0/0 Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz	R1(config)#interface 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:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Rutas predeterminadas Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Se realiza configuración inicial del Router 1, para ello desde la consola modo privilegiado se procede a ejecutar el comando no ip domain lookup que permite desactivar la búsqueda DNS, esto para indicar que si hemos cometido un error en el scrip de configuración nos muestre un aviso indicando el error, se configura el nombre del dispositivo junto con la contraseña cifrada para ingresar al modo privilegiado a través del comando enable secret, de igual manera se configura la contraseña para ingresar a la consola con el comando password y se activa con el comando login, se configuran el modo de línea de terminal virtual vty 0 15 (Telnet) asignándole una contraseña para el acceso, para seguridad se adiciona el comando service password-encryption para cifrar las contraseñas de texto no cifrado y un mensaje para usuarios no autorizados.

Se establece la interfaz s0/0/0 para la conexión con R2 y se le asigna una dirección y IPv4 e IPv6 con una frecuencia de reloj de 128000 bits, se activa con el comando no shutdown, y se asignan las rutas predeterminadas IPv4 e IPv6.

Nota: Todavía no configure G0/1.

Figura 51. Configuración parámetros básicos en Router 1



Fuente: Autor

6.3. Paso 3. Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 20. Configuración Router 2

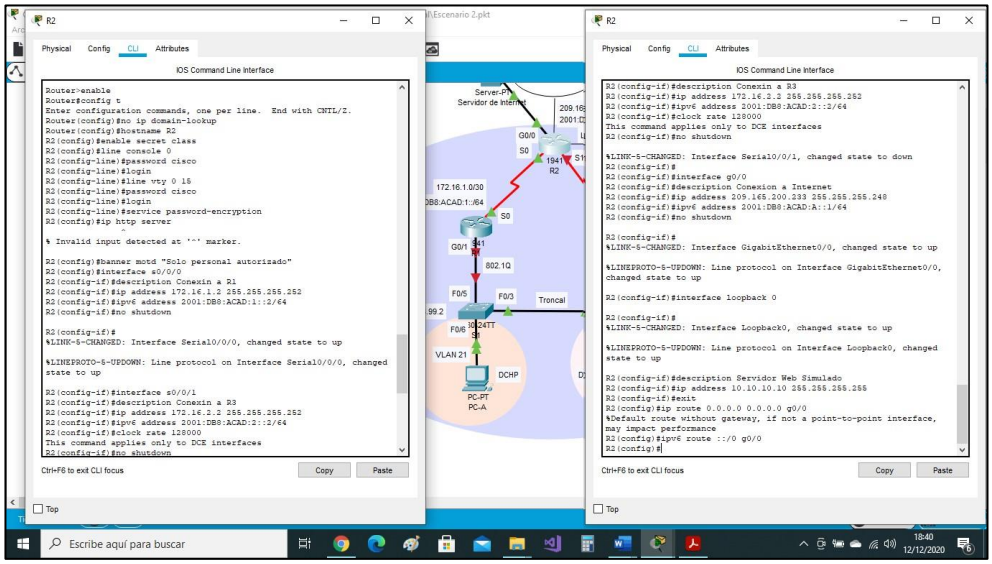
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router, R2	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada, class	R2(config)#enable secret class
Contraseña de acceso a 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 vty 0 15 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config-line)# service passwordencryption
Habilitar el servidor HTTP	R2(config)#ip http server
Mensaje MOTD, Se prohíbe el acceso no autorizado.	R2(config)#banner motd " Solo personal autorizado"
Interfaz S0/0/0 Establezca 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	R2(config)#interface s0/0/0 R2(config-if)#description Conexion a R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1 Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz	R2(config-if)#interface s0/0/1 R2(config-if)#description Conexion a R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet) Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz	R2(config-if)#interface g0/0 R2(config-if)#description Conexion a Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown

Interfaz loopback 0 (servidor web simulado) Establecer la descripción. Establezca la dirección IPv4.	R2(config-if)#interface loopback 0 R2(config-if)#description Servidor Web Simulado R2(config-if)#ip address 10.10.10.10 255.255.255.255
Ruta predeterminada Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.	 R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

Se realiza configuración inicial del Router 2, para ello desde la consola modo privilegiado se procede a ejecutar el comando no ip domain lookup que permite desactivar la búsqueda DNS, esto para indicar que si hemos cometido un error en el scrip de configuración nos muestre un aviso indicando el error, se configura el nombre del dispositivo junto con la contraseña cifrada para ingresar al modo privilegiado a través del comando enable secret, de igual manera se configura la contraseña para ingresar a la consola con el comando password y se activa con el comando login, se configura el modo de línea de terminal virtual vty 0 15 (Telnet) asignándole una contraseña para el acceso, para seguridad se adiciona el comando service password-encryption para cifrar las contraseñas de texto no cifrado, se habilita el servidor http con el comando ip http server y se adiciona el mensaje del día para usuarios no autorizados en el banner motd.

Se configura la interfaz s0/0/0 para la conexión con R1 asignándose una dirección IPv4 e IPv6, luego se procede con la configuración de la interfaz serial s0/0/01 para la conexión con R3 asignándosele una dirección IPv4 e IPv6 con una frecuencia de reloj de 128000 bits, se procede activar la interfaz g0/0 la cual representa la simulación de Internet asignándoseles la respectiva dirección IPv4 e IPv6, todas estas interfaces al configurarse se activaron con el comando no shutdown. Se configura la interfaz loopback 0 que corresponde al servidor web simulado, se le asigna una dirección Ipv4 y mascara de red para finalmente configurar las rutas predeterminadas IPv4 y IPv6 en la g0/0.

Figura 52. Configuración parámetros básicos en Router 2



Fuente: Autor

6.4. Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 21. Configuración Router 3

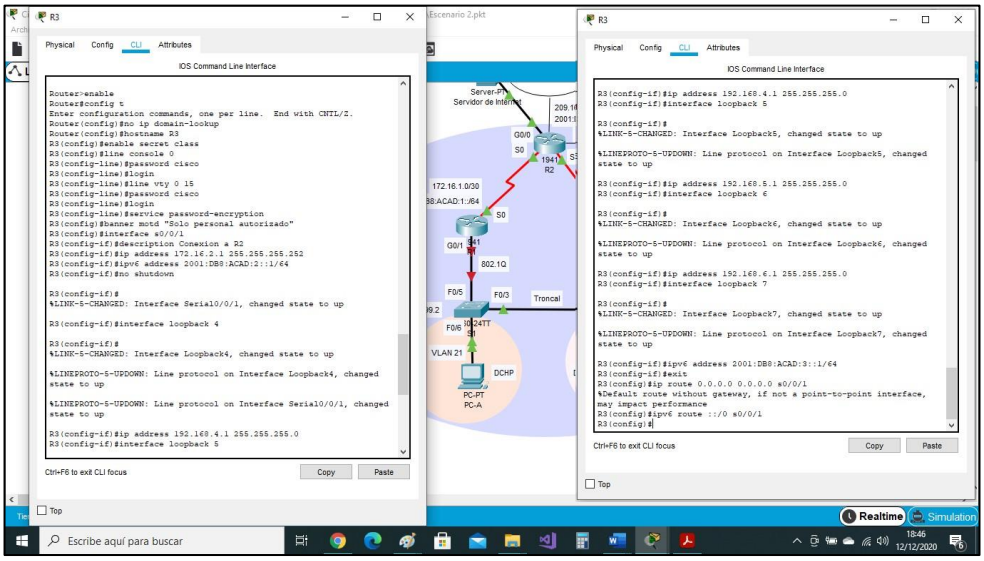
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router, R3	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada, class	R3(config)#enable secret class
Contraseña de acceso a 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 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 "Solo personal 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)#interface s0/0/1 R3(config-if)#description Conexion 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)#interface 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)#interface 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)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.	R3(config-if)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
Rutas prederminadas Configurar una ruta IPv4 predeterminada de S0/0/1 Configurar una ruta IPv6 predeterminada de S0/0/1	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Se realiza configuración inicial del Router 3, desde la consola EXEC privilegiado se procede a ejecutar el comando no ip domain lookup que permite desactivar la búsqueda DNS, se configura el nombre del dispositivo junto con la contraseña cifrada para ingresar al modo privilegiado a través del comando enable secret, de igual manera se configura la contraseña para ingresar a la consola con el comando password y se activa con el comando login, se configura el modo de línea de terminal virtual vty 0 15 (Telnet) asignándole una contraseña para el acceso, para seguridad se adiciona el comando service password-encryption para cifrar las contraseñas de texto no cifrado, se habilita el servidor http con el comando ip http server y se adiciona el mensaje del día para usuarios no autorizados en el banner motd.

Se configura la interfaz s0/0/1 para la conexión con R2 asignándose una dirección IPv4 e IPv6, y se activa, se configuran las interfaces loopback 4, 5 y 6 direccionandolas con IPv4 y la loopback 7 con IPv6, se establecen las rutas predeterminadas IPv4 e IPv6 en la s0/0/1.

Figura 53. Configuración parámetros básicos Router 3



Fuente: Autor

6.5. Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

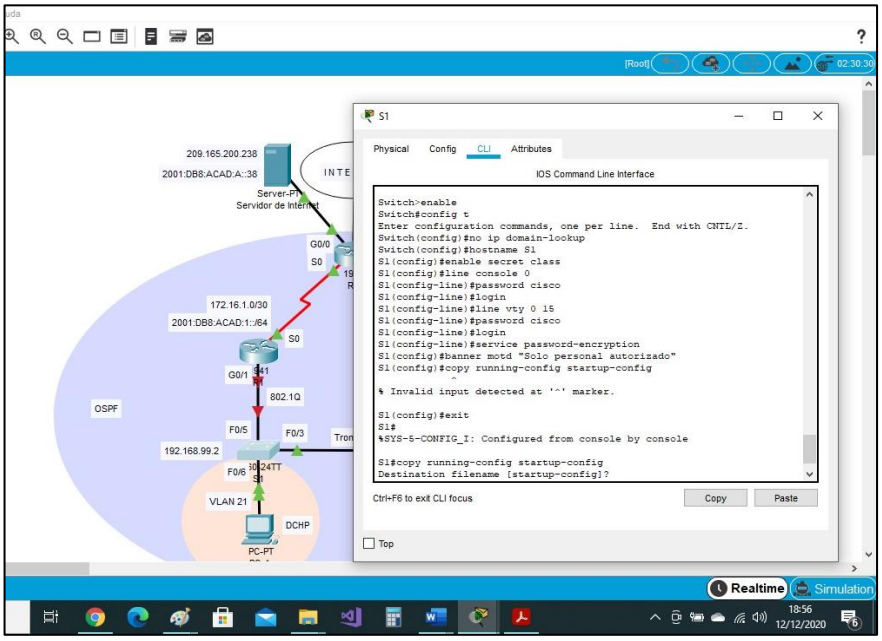
Tabla 22. Configuración Switch 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal 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 vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config-line)# service passwordencryption
Mensaje MOTD, Se prohíbe el acceso no autorizado.	S1(config)#banner motd " Solo personal autorizado "

Se realiza configuración inicial del Switch 1, desde la consola EXEC privilegiado se procede a ejecutar el comando no ip domain lookup que permite desactivar la búsqueda DNS, se configura el nombre del dispositivo junto con la contraseña cifrada para ingresar al modo privilegiado a través del comando enable secret, de igual manera se configura la contraseña para ingresar a la consola con el

comando password, activándose con el comando login, se configura el modo de línea de terminal virtual vty 0 15 (Telnet) asignándole una contraseña para el acceso, para seguridad se adiciona el comando service password-encryption para cifrar las contraseñas de texto no cifrado y se adiciona el mensaje del día para usuarios no autorizados en el motd.

Figura 54. Configuración Switch 1



Fuente: Autor

6.6. Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

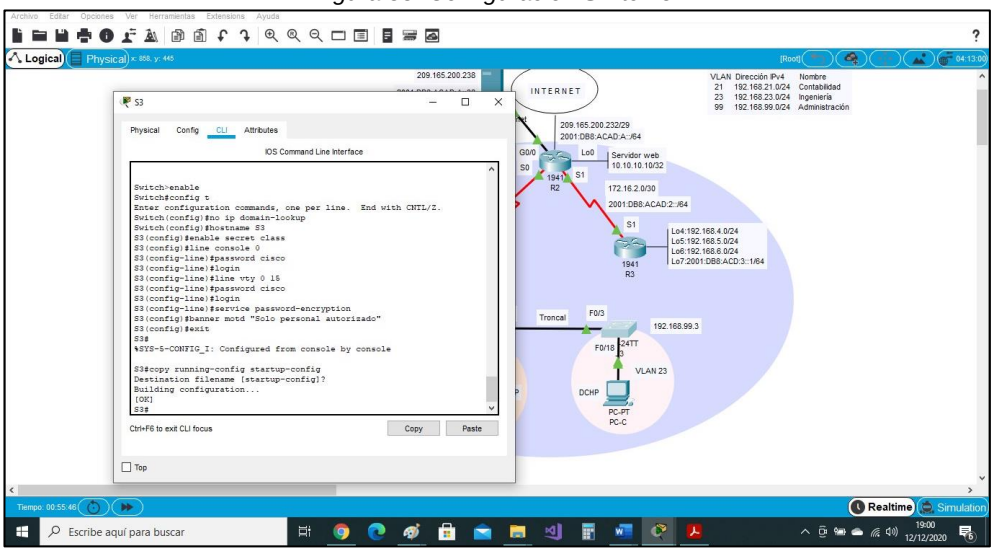
Tabla 23. Configuración Switch 3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch, S3	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada, class	S3(config)#enable secret class
Contraseña de acceso a la consola, cisco	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet, cisco	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config-line)# service password-encryption

Mensaje MOTD, Se prohíbe el acceso no autorizado.	S3(config)#banner motd " Solo personal autorizado "

Se realiza configuración básica del Switch 3, desde la consola EXEC privilegiado se procede a ejecutar el comando no ip domain lookup que permite desactivar la búsqueda DNS, se configura el nombre del dispositivo junto con la contraseña cifrada para ingresar al modo privilegiado a través del comando enable secret, de igual manera se configura la contraseña para ingresar a la consola con el comando password, activándose con el comando login, se configura el modo de línea de terminal virtual vty 0 15 (Telnet) asignándole una contraseña para el acceso, para seguridad se adiciona el comando service password-encryption para cifrar las contraseñas de texto no cifrado y se adiciona el mensaje del día para usuarios no autorizados en el motd.

Figura 55. Configuración Switch 3



Fuente: Autor

6.7. Paso 7: Verificar la conectividad de la red

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

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

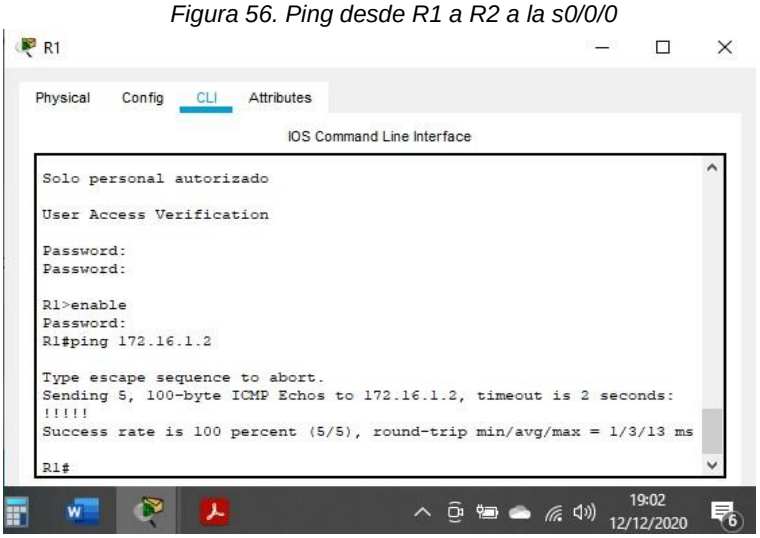
Tabla 24. Verificación conectividad de la red

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

Se realizan pruebas de conexión para verificar el correcto funcionamiento de la red, ejecutando el comando ping entre routers y desde el pc de internet a la puerta de enlace predeterminada.

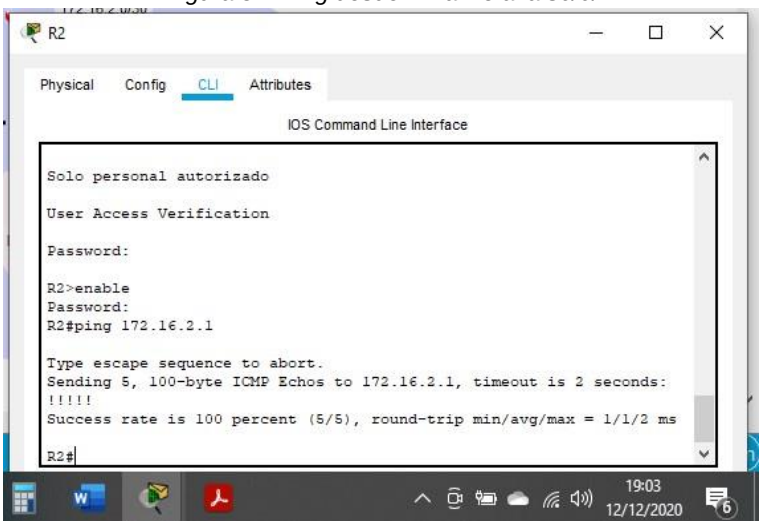
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Figura 56. Ping desde R1 a R2 a la s0/0/0



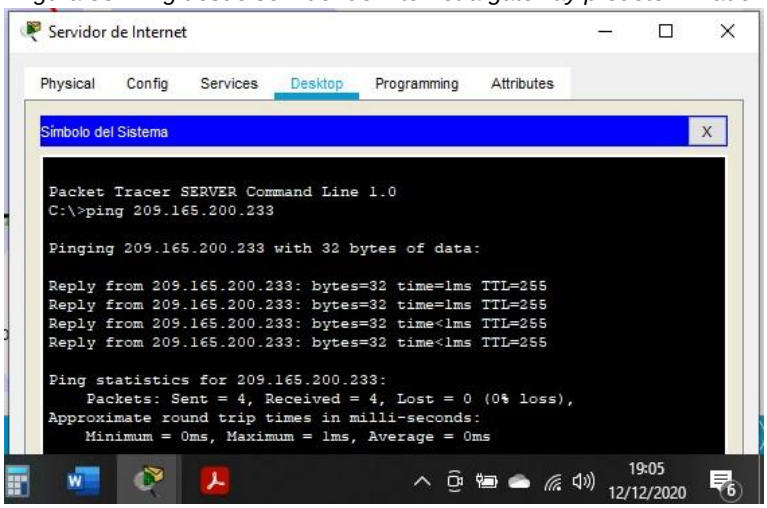
Fuente: Autor

Figura 57. Ping desde R2 a R3 a la s0/0/1



Fuente: Autor

Figura 58. Ping desde servidor de Internet a gateway predeterminado



Fuente: Autor

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

7.1. Paso 1. Configurar S1

La configuración del S1 incluye las siguientes tareas:

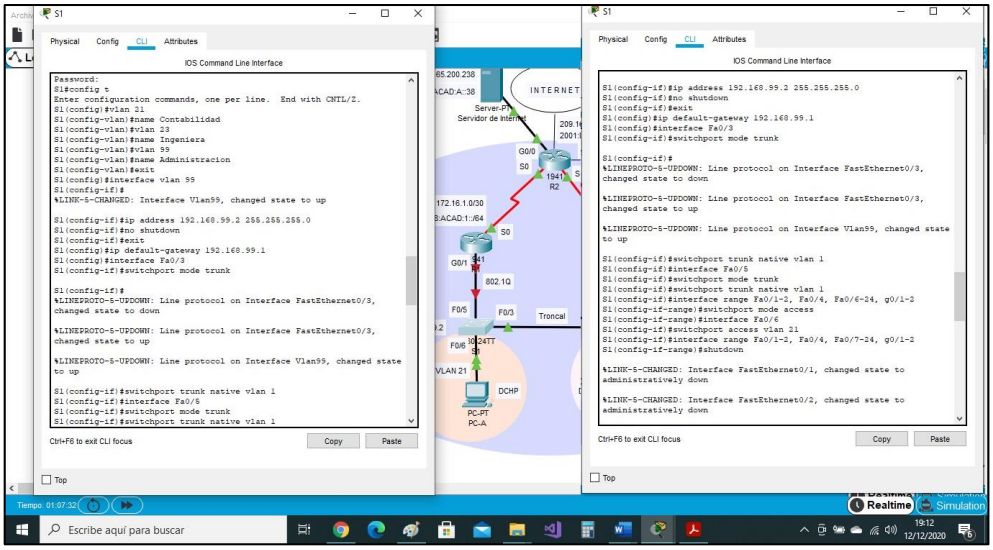
Tabla 25. Configuración seguridad del Switch 1, Vlan y routing entre Vlan

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#configure terminal S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingeniería 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)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.	S1(config)#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)#interface Fa0/3 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)#interface Fa0/5 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)#interface range Fa0/1-2, Fa0/4, Fa0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if-range)#interface Fa0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#interface range Fa0/1-2, Fa0/4, Fa0/7-24, g0/1-2 S1(config-if-range)#shutdown

En el switch 1 se crea la base de datos para las VLAN 21 (Contabilidad), VLAN 23 (Ingeniería) y VLAN 99 (Administración), a esta última se le asigna una dirección IPv4 con su máscara de red, se asigna una dirección IPv4 como Gateway predeterminado, la interfaz fa0/3 se establece como enlace troncal utilizando la VLAN 1 como VLAN nativa, se realiza el mismo proceso a la interfaz fa0/5, el resto de los puertos se configuran en rango como puertos de acceso, la interfaz fa0/6 se asigna a la VLAN 21, el resto de las interfaces utilizar se desactivan con el comando shutdown.

Figura 59. Configuración seguridad del switch 1, las VLAN y el routing entre VLAN.



Fuente: Autor

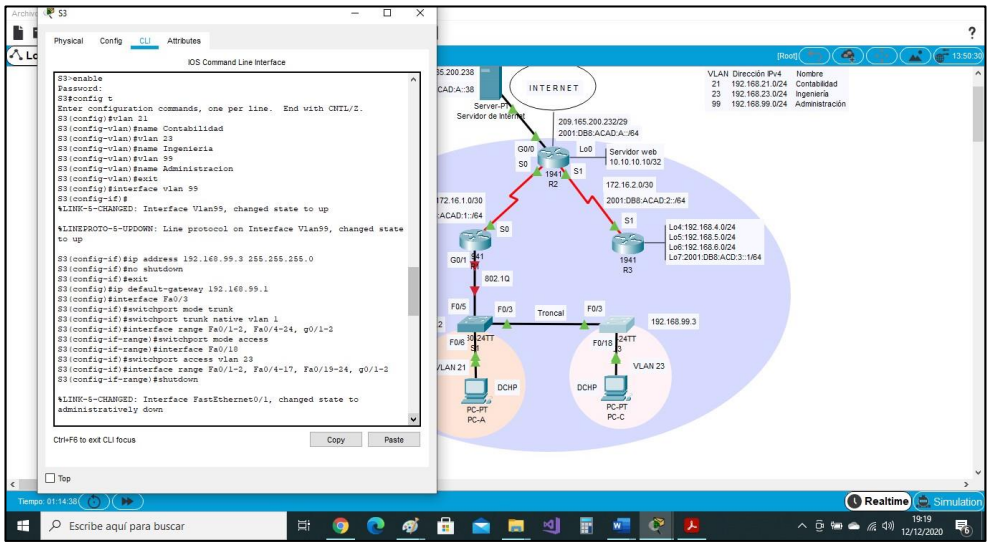
7.2. Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 26. Configuración seguridad del Switch 3, Vlan y routing entre Vlan

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#configure terminal S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingeniería 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)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado. Asignar la primera dirección IP en la subred como gateway predeterminado.	S3(config)#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)#interface Fa0/3 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)#interface range Fa0/1-2, Fa0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 23	S3(config-if-range)#interface Fa0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#interface range Fa0/1-2, Fa0/4-17, Fa0/19-24, g0/1-2 S3(config-if-range)#shutdown

Figura 60. Configuración seguridad del switch 3, las VLAN y el routing entre VLAN.



Fuente: Autor

7.3. Paso 3: Configurar R1

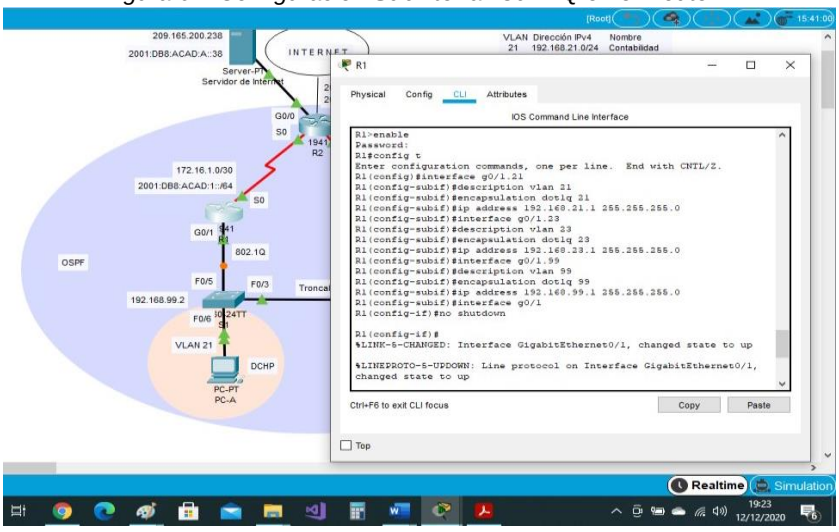
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 27. Configuración Subinterfaz 802.1Q en el Router 1

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

En la Interfaz g0/1 se configuran las Subinterfaces 802.1Q en el Router 1, se procede a configurar la subinterfaz g0/1.21, habilitándola con el comando ecapsulation dot1q asociándole la vlan 21 (Lan de Contabilidad) y asignándole la IPv4 correspondiente, se realiza el mismo procedimiento para activar la subinterfaz g0/1.23, Vlan 23 (Lan de Ingeniaría) y la subinterfaz g0/1.99, Vlan 99 (Lan de Administración) finalmente se activa la interfaz g0/1 con el comando no shutdown.

Figura 61. Configuración Subinterfaz 802.1Q en el Router 1



Fuente: Autor

7.4. Paso 4: Verificar la conectividad de la red

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

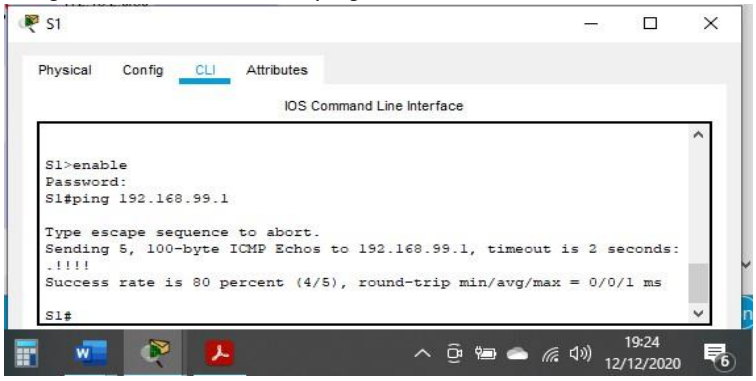
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 28. Verificación de la conectividad en la red

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

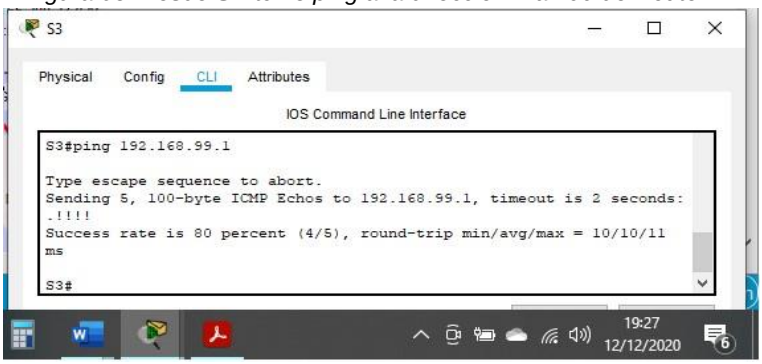
Se realizan comprobaciones entre diferentes dispositivos de la red para verificar el correcto funcionamiento de esta.

Figura 62. Desde Switch 1 ping a la dirección Vlan 99 de Router 1



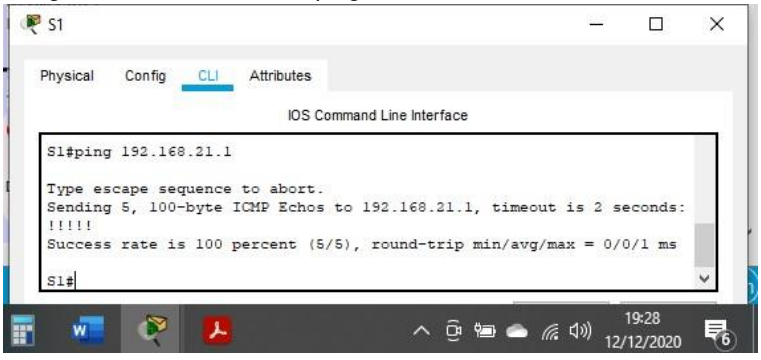
Fuente: Autor

Figura 63. Desde Switch 3 ping a la dirección Vlan 99 de Router 1



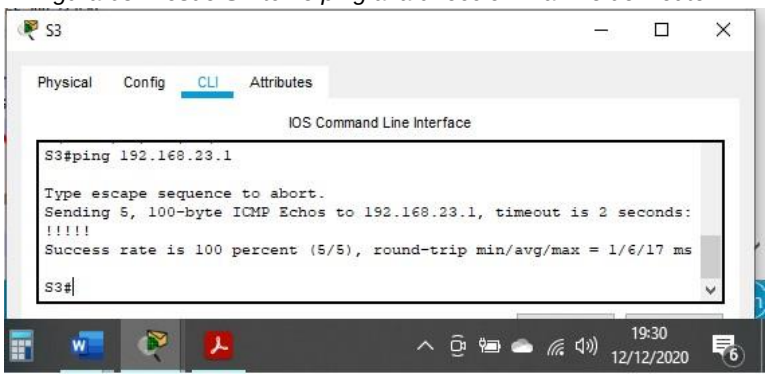
Fuente: Autor

Figura 64. Desde Switch 1 ping a la dirección Vlan 21 de Router 1



Fuente: Autor

Figura 65. Desde Switch 3 ping a la dirección Vlan 23 de Router 1



Fuente: Autor

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

8.1. Paso 1: Configurar OSPF en el R1

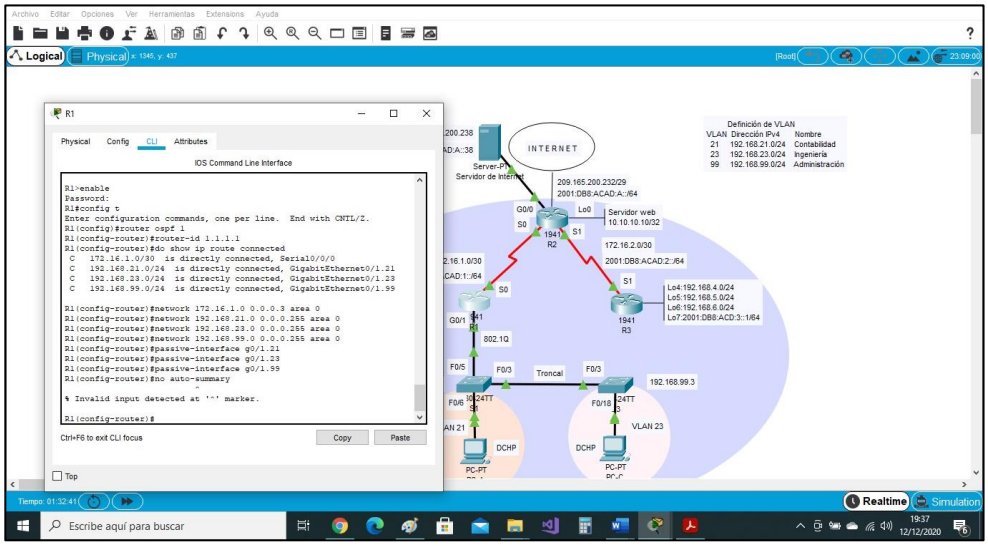
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 29. Configuración del protocolo de routin dinámico OSPF en Router 1

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1
Anunciar las redes conectadas directamente Asigne todas las redes conectadas directamente.	R1(config-router)#do show ip route connected R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

Se configura el protocolo OSPF en el Router 1 con el comando Router ospf 1, para verificar las redes conectadas se ejecuta el comando show ip route connected, con la verificación se procede asignar las redes al área 0 con el comando network asignándole la IP correspondiente, todas las subintefaces LAN (g0/1.21, g0/1.23, g0/199) se establecen como pasivas y se desactiva la sumarización automática con el comando no auto-summary.

Figura 66. Configuración del protocolo de routin dinámico OSPF en Router 1



Fuente: Autor

8.2. Paso 2: Configurar OSPF en el R2

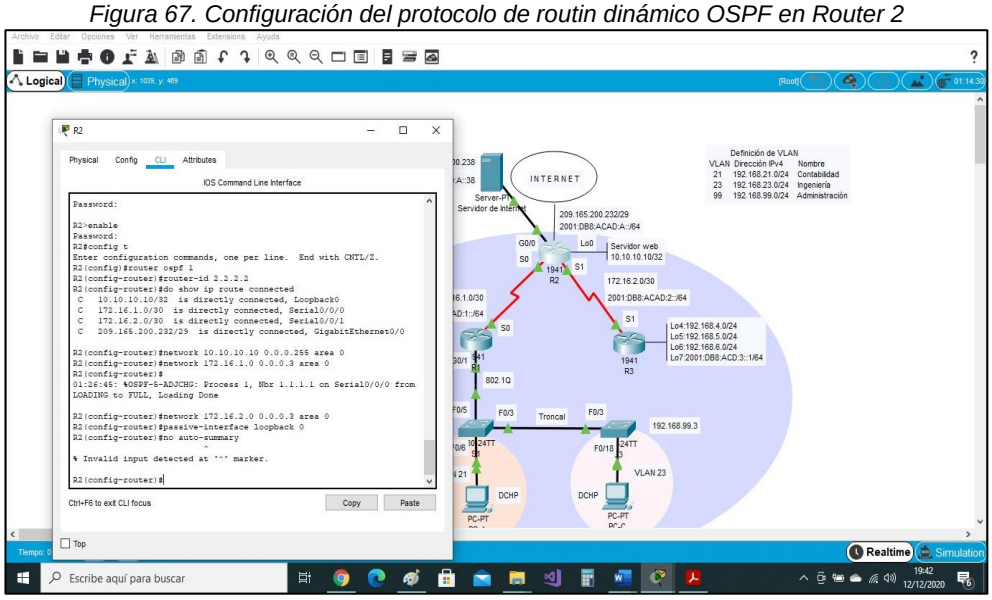
La configuración del R2 incluye las siguientes tareas:

Tabla 30. Configuración del protocolo de routin dinámico OSPF en Router 2

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2
Anunciar las redes conectadas directamente **Nota:** Omitir la red G0/0.	R2(config-router)#do show ip route connected R2(config-router)#network 10.10.10.10 0.0.0.255 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Se configura el protocolo OSPF en el Router 2 con el comando Router ospf 1, para verificar las redes conectadas se ejecuta el comando show ip route connected, con la verificación se procede asignar las redes al área 0 con el comando network asignándole la IP correspondiente, la interfaz de red g0/0 no se tiene en cuenta y por tanto no establece, se asigna la interfaz LAN loopback 0 como pasiva y se desactiva la sumarización automática con el comando no auto-summary.

Figura 67. Configuración del protocolo de routin dinámico OSPF en Router 2



Fuente: Autor

8.3. Paso 3: Configurar OSPFv3 en el R3

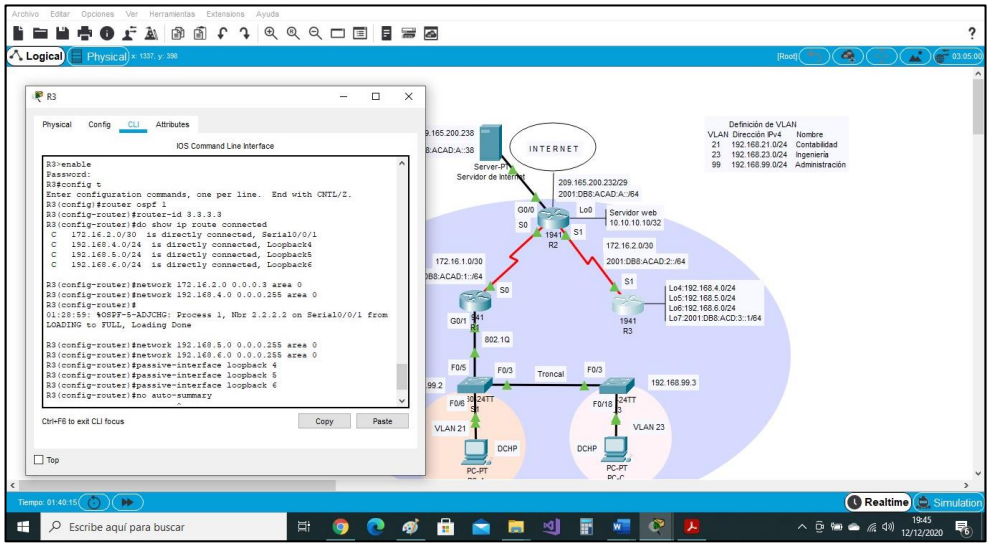
La configuración del R3 incluye las siguientes tareas:

Tabla 31. Configuración del protocolo de routin dinámico OSPFv3 en Router 3.

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)#do show ip route connected R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface 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

Se configura el protocolo OSPF en el Router 3 con el comando Router ospf 1, para verificar las redes conectadas se ejecuta el comando show ip route connected, con la verificación se procede asignar las redes al área 0 con el comando network asignándole la IP correspondiente, las interfaces de LAN IPv4 Loopback 4, 5 y 6 se establecen como pasivas y se desactiva la sumarización automática con el comando no auto-summary.

Figura 68. Configuración del protocolo de routin dinámico OSPFv3 en Router 3



Fuente: Autor

8.4. Paso 4: Verificar la información de OSPF

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

Tabla 32. Verificación de la información del protocolo OSPF

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

En el Router 3 se ingresan comandos CLI para verificar la configuración e información del protocolo OSPF.

9. Parte 5: Implementar DHCP y NAT para IPv4

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

Ahora veremos las tareas pendientes por hacer:

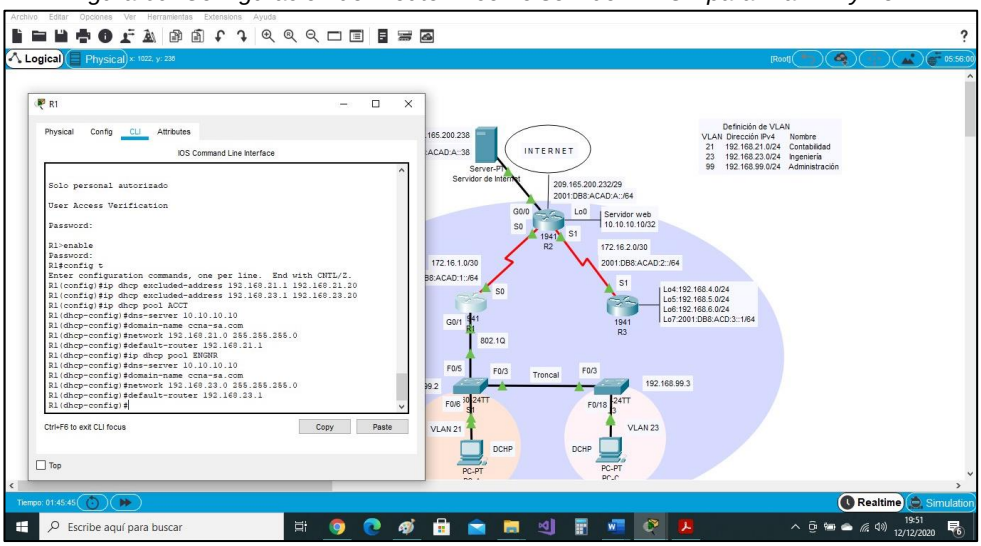
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 33. Configuración del Router 1 como servidor DHCP para 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)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23 Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado	R1(dhcp-config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1

El Router 1 se configura como servidor DHCP para las vlan 21 y 23, para ello se aplica el comando ip dhcp excluded-address acompañado del rango del numero de ip a reservar, para este caso se reservan las primeras 20 direcciones IP en la VLAN 21 y la VLAN 23 para configuraciones estáticas, se crea el pool de DCHP como ACCT para la VLAN 21, se le asigna un nombre de dominio y se establece el Gateway predeterminado con el comando defaul-router, de igual manera se crea el pool DHCP como ENGNR para la VLAN 23.

Figura 69. Configuración del Router 1 como servidor DHCP para Vlan 21 y 23



Fuente: Autor

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

La configuración del R2 incluye las siguientes tareas:

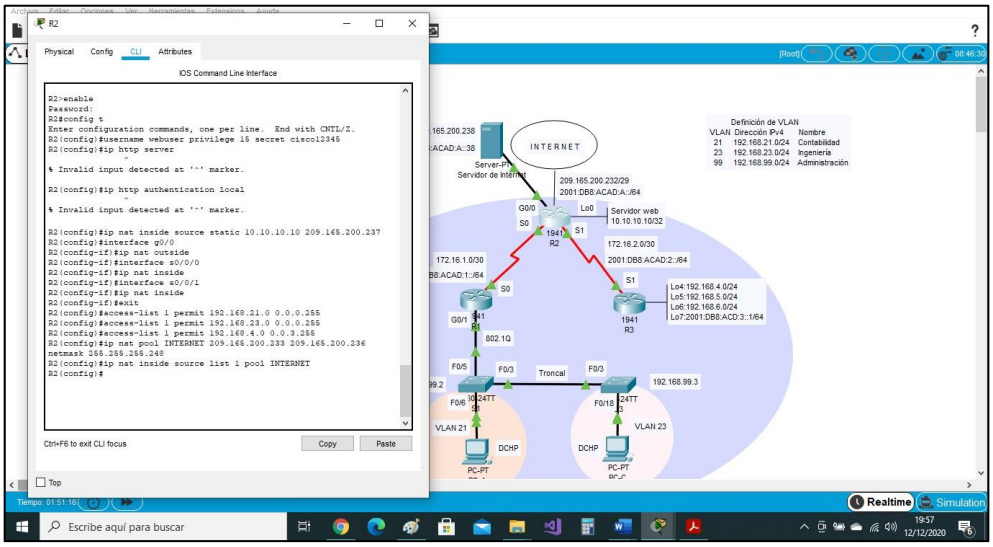
Tabla 34. Configuración NAT estática y dinámica en Router 2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**	R2(config)#username webuser secret cisco12345 privilege 15
Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local
Crear una NAT estática al servidor web. Dirección global interna: **209.165.200.237**	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#interface s0/0/0 R2(config-if)#ip nat inside R2(config-if)#interface s0/0/1 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables. Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.233** – **209.165.200.248**	R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

El Router 2 se establece como NAT estática y dinámica, se crea una base de datos local asignándole un nombre, una contraseña y nivel privilegiado, posteriormente se habilita el servicio del servidor HTTP con el comando ip http server y se configura para que poder utilizar la bases de datos local para la autenticación con el comando ip http autentication local, estas dos últimas configuraciones no surtieron efecto puesto que packet tracert no soporta estos

comandos, se crea la NAT estática al servidor Web con el comando ip nat inside source static, se asigna como interfaz externa la g0/0 e interfaz interna la serial s0/0/0 y s0/0/1, se habilita la lista de acceso 1 para permitir la traducción de las redes de contabilidad e ingeniería en el Router 1, se hace los mismo para las redes LAN loopback en el Router 3, se define el pool de direcciones ip publicas utilizables de Internet con el comando ip nat pool Internet asignando el conjunto de direcciones y la máscara de red, posteriormente se configura la traducción de la NAT dinámica con el comando ip nat inside source list 1 pool Internet.

Figura 70. Configuración NAT estática y dinámica en Router 2



Fuente: Autor

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

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

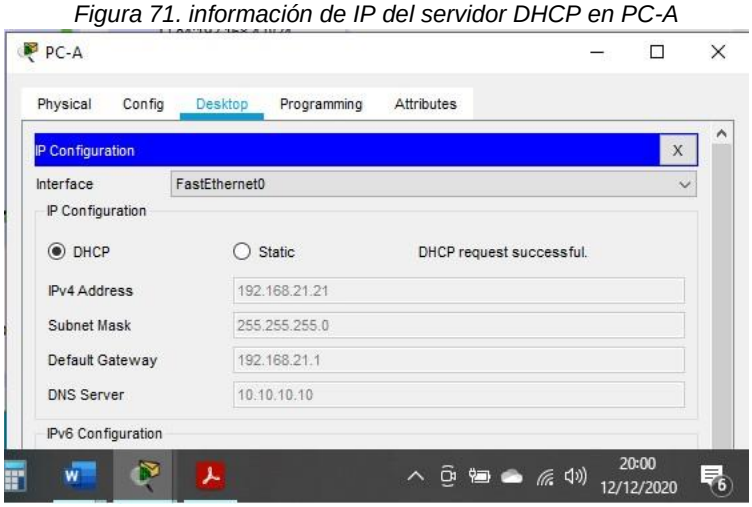
Tabla 35. Verificación del protocolo DHCP y NAT estática

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

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**	Si hay respuesta

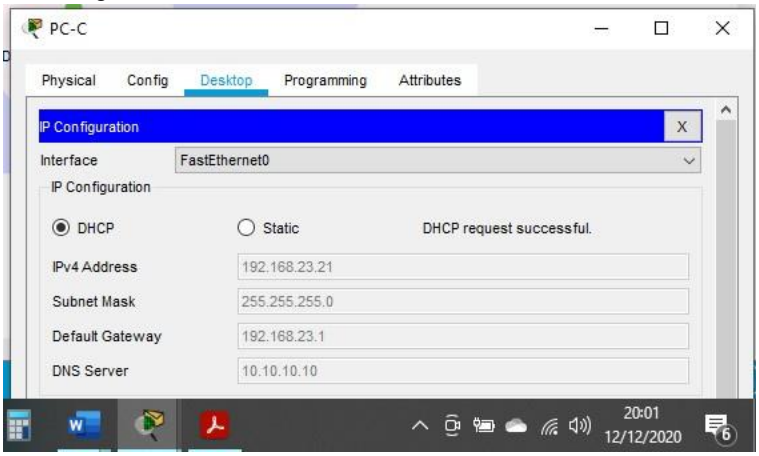
Se verifica el funcionamiento del protocolo DHCP y NAT estática, para ello se verifica que la PC-A y PC-B hayan asignado la información en DHCP, se hace un ping de la PC-A a la dirección IP del PC-C, este establece comunicación, desde el servidor de Internet utilizando el navegador web se intenta acceder al servidor web, pero este no responde.

Figura 71. información de IP del servidor DHCP en PC-A



Fuente: Autor

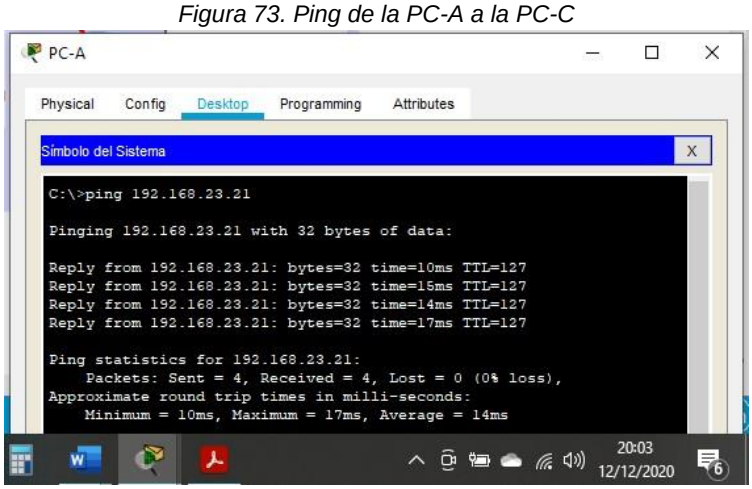
Figura 72. información de IP del servidor DHCP en PC-C



Fuente: Autor

Ahora vamos hacert ping desde la Pc-A a la Pc-C:

Figura 73. Ping de la PC-A a la PC-C



Fuente: Autor

10. Parte 6: Configurar NTP

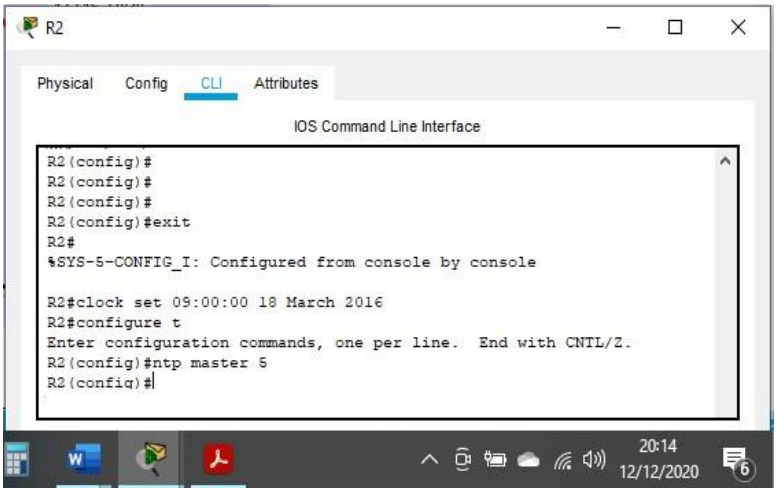
Tabla 36. Configuración NTP en Router 2.

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2. **5 de marzo de 2016, 9 a. m.**	R2#clock set 09:00:00 18 March 2016
Configure R2 como un maestro NTP. Nivel de estrato: **5**	R2(config)#ntp master 5
Configurar R1 como un cliente NTP. Servidor: **R2**	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp updatecalendar
Verifique la configuración de NTP en R1.	R1#show ntp associations

Se configura en el Router 2 el protocolo NTP, se inicia ajustando la hora y la fecha con el comando clock set y formato 09:00:00 18 march 2016, se asigna al R2 como maestro NTP vivel de estrato 5 con el comando ntp master 5, posteriormente al Router 1 se le asigna como cliente NTP el Router 2 con el comando ntp server y la ip del Router 2.

En R1 se configuran las actualizaciones de calendario periódicas con la hora NTP con el comando ntp update-calendar, finalmente se verifica la configuración de NTP en R1 con el comando show ntp associations.

Figura 74. Configuración NTP en Router 2



Fuente: Autor

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

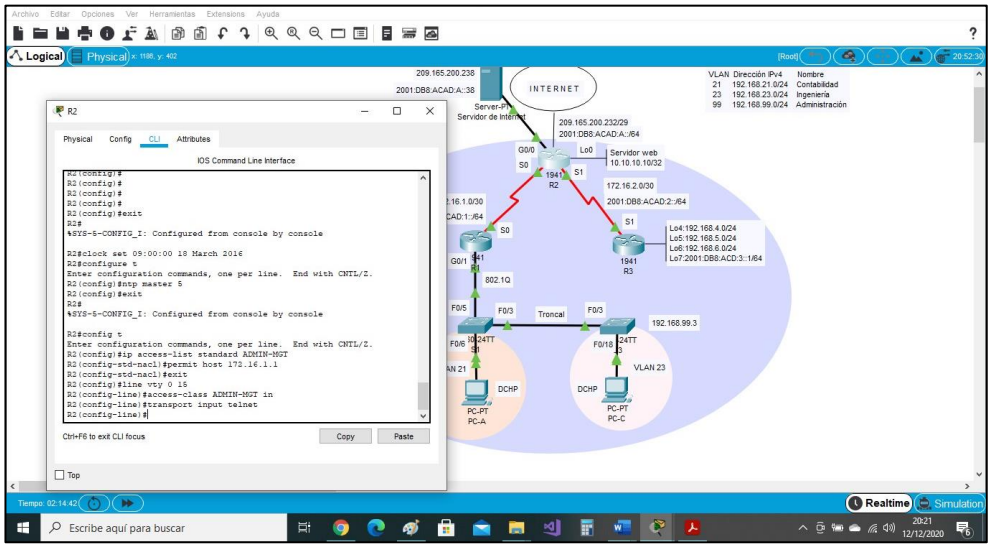
11.1. Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 37. Restricción de acceso a líneas VTY en Router 2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 Nombre de la ACL: **ADMIN-MGT**	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
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

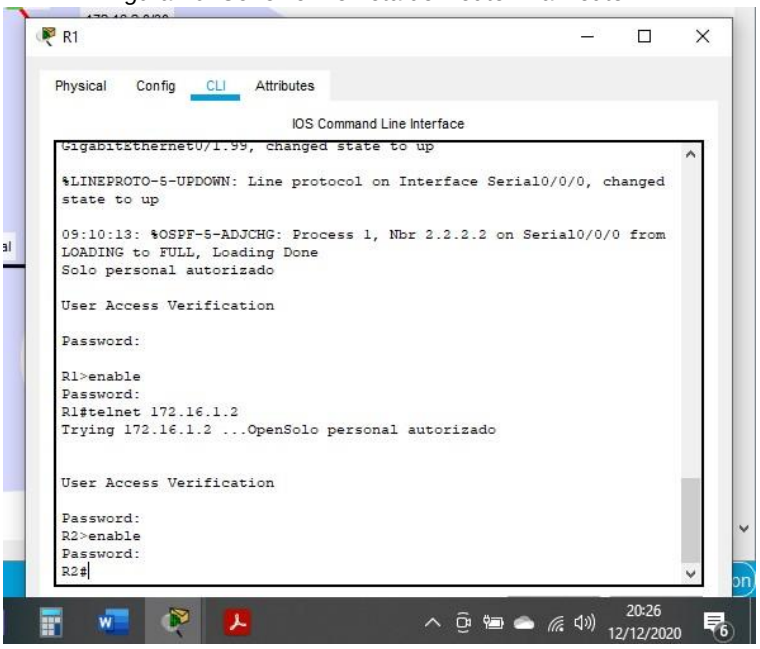
Se configura en el Router 2 la restricción de acceso a las líneas VTY, se configura lista de acceso ADMIN-MGT con el comando ip acces-list standard para conexión remota con R2, se establece la entrada a las líneas VTY con el comando Access-class y para que permita el acceso a esas líneas se ejecuta el comando transport input telnet, finalmente se realiza verificación de conexión de R1 a R2.

Figura 75. Restricción de acceso a líneas VTY en Router 2



Fuente: Autor

Figura 76. Conexión remota de Router 1 a Router 2



Fuente: Autor

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

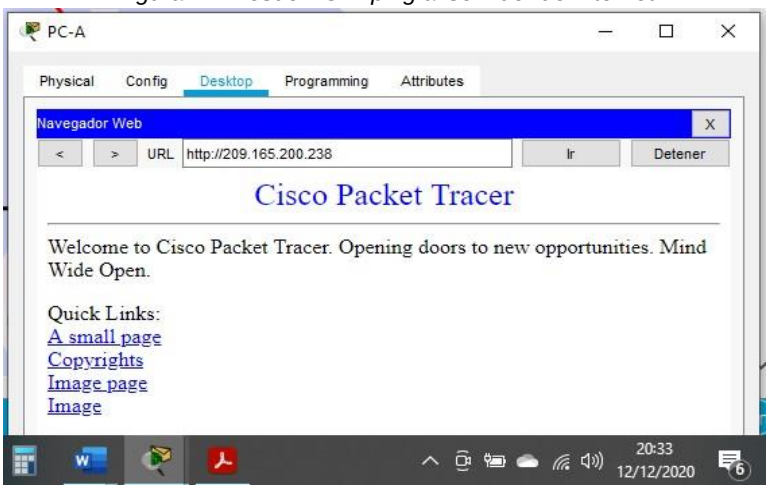
Tabla 38. Verificación de configuración con comandos CLI

Descripción del comando	**Entrada del estudiante (comando)**
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list
Restablecer los contadores de una lista de acceso	R2#show access-list counters

¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface
¿Con qué comando se muestran las traducciones NAT? **Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation *

En el Router 2 se ingresan comandos CLI para verificar que la configuración se halla asignado.

Figura 77. Desde PC-A ping al servidor de Internet



Fuente: Autor

Figura 78. Desde PC-C ping al Servidor de Internet

Fuente: Autor

CONCLUSIONES

Con la realización y presentación de este trabajo, podemos concluir que es fundamental y necesario para un profesional de la ingeniería de sistemas el conocimiento y manejo de habilidades, capacidades y destrezas para diagnosticar, configurar y brindar solución, a todo lo relacionado con el manejo de redes de datos para ser altamente competitivos y enfrentar la demanda y exigencias de este tipo de profesionales en el mundo moderno.

Al realizar esta topología de red en el escenario 1 para poner en práctica todas las habilidades, capacidades y destrezas, aprendidas previamente en las definiciones del curso se hizo énfasis en la aplicabilidad de procesos que cumplieran de manera satisfactoria con las exigencias del escenario, y se llevara a cabo la implementación de la topología diseñada para tal fin.

Las actividades inherentes al proceso que se sigue según las dos topologías de red priorizan los ajustes elementales de los conmutadores y enrutadores con el objetivo de lograr unos buenos ejercicios prácticos en la administración de una red.

Los dispositivos utilizados poseen su propio sistema operativo, acompañado del concepto que da viabilidad a la realización de la asignación del direccionamiento y sus posibles variables, llegando de igual forma a un verdadero dispositivo, cada uno de los procesos experimentales está soportado por Cisco.

La realización del proceso de experimentación utilizando dos contextos o topologías de red LAN nos permite ser capaces de aprender cómo funciona una determinada red atendiendo los conceptos aprendidos sobre los variados terminales que lo integran, administración de redes, conexión de cables con puertos, configuración de los dispositivos mediante protocolo OSPF y seguridad de puntos de conexión de red.

La configuración de servidores locales y remotos mediante SSH o telnet, configuración de protocolos e interfaces lógicas y físicas, configuración de passwords de seguridad a modo usuario y privilegiado, reinicio de dispositivos, contraseñas encriptadas, mensajes del día (banner-motd), entre otros procesos nos dan la seguridad del aprendizaje en este proceso.

BIBLIOGRAFÍA

Bitacora Byte. (18 de julio de 2017). Configurar DHCP en router CISCO. Recuperado el 18 de octubre de 2020, de Bitacora Byte: https://bitacorabyte.wordpress.com/2017/07/18/configurar-dhcp-en-router-cisco/

CISCO. (2019). División de redesIP en subredes. Fundamentos de Networking. Recuperado el 18 de octubre de 2020 de: https://static-courseassets.s3.amazonaws.com/ITN6/es/index.html#8

Cisco. (10 de agosto de 2005). Configuración de una puerta de enlace de último recurso mediante comandos IP. Recuperado el 18 de Octubre de 2020, de Cisco: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocolrip/16448-default.html

Cisco. (sf de sf de 2020). Guía de configuración del software del switch Catalyst 3750-X y 3560-X, versión 12.2 (55) SE. Recuperado el 18 de Octubre de 2020, de Cisco: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swsdm.html

Cisco. (21 de noviembre de 2007). Información sobre los modos de loopback en routers de Cisco. Recuperado el 18 de Octubre de 2020, de Cisco: https://www.cisco.com/c/es_mx/support/docs/asynchronous-transfer-modeatm/permanent-virtual-circuits-pvc-switched-virtual-circuits-svc/6337atmloopback.html

CISCO. (abril 21 de 200). Configurar el enrutamiento de InterVLAN en conmutadores de capa 3. Recuperado el 14 de noviembre 2020 de: https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlanrouting/41860-howto-L3-intervlanrouting.html

Lobato, G. (mayo 24 de 2014). CURSO 7-1 Explicación de protocolo OSPF [Archivo de Vídeo]. Recuperado el 14 de noviembre de 2020 de: https://www.youtube.com/watch?v=dwT5du44t_8

Salazar, P. (2020). CIPA 2 Prueba de Habilidades Diplomado Cisco (octubre 16 de 2020). Recuperado el 18 de octubre de 2020 de: https://drive.google.com/file/d/1XTTmvwmU_Z4SDMoRom6HeJSAJiqj_Q6/view

WF-Networking (2020). Configuración básica IPv6 Router Cisco. Recuperado el 19 de octubre de 2020 de https://www.w0lff4ng.org/configuracion-basica-ipv6router-cisco/

ANEXOS

Anexo B. Link de descarga Escenario 1, archivo ptk:
https://drive.google.com/file/d/1A__eNEW0YiMWRCIzfRUoe_vqwn0qBy8P/view?usp=sharing

Anexo C. Link de descarga Escenario 2, archivo ptk
https://drive.google.com/file/d/1jewvvWR_2Y8nvywiX8kYYSVzCy7KdfFt/view?usp=sharing

Anexo D. Link de descarga Artículo científico
https://drive.google.com/file/d/1j9_M8rxm1NsSRY_2NmPkjRQpKvVOT55H/view?usp=sharing