SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

WALTER ALEXANDER LEON ORTIZ

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

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

WALTER ALEXANDER LEON ORTIZ

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR EL TÍTULO DE INGENIERO DE SISTEMAS

DIEGO EDINSON RAMIREZ
INGENIERO ELECTRÓNICO

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Pitalito Huila, octubre 20 de 2020

AGRADECIMIENTOS

En este informe, lo dedico con todo mi corazón a Dios por darme la capacidad intelectual y física de afrontar mis sueños y mi estudio, llenando mi vida de bendiciones. A mi Mamá, por traerme a este mundo maravilloso, sin ella yo no estaría aquí presente, a mi Papá, por darme energía emocional para impulsar mis sueños. Y a mi hermanita que han estado a mi lado concediéndome el apoyo necesario para continuar adelante. Y muy especialmente a todas las personas que han creído en mí.

Agradecer al Ingeniero Diego Edinson Ramírez, tutor del diplomado CISCO por su total, comprensión, así como su total entrega para transmitir sus conocimientos y experiencias en aras de una excelente formación de cada uno de los educandos bajo su tutoría personal y servicios necesarios para lograr un aprendizaje autónomo y excelente.

Dios colme y llene sus vidas de bendiciones

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

ACL (Access control list): Es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

DHCP (Dynamic Host Configuration Protocol): “Protocolo de Configuración Dinámica de Servidor. Se trata de un protocolo cliente-servidor que permite que una o más máquinas obtengan su configuración de red de manera totalmente automática.” (Pastor, 2009)

CCNA (Cisco Certified Network Associate): Es un plan de capacitación en tecnología de redes informáticas que la empresa Cisco ofrece.

EIGRP (Enhanced Interior Gateway Routing Protocol): Es utilizado en redes TCP/IP y de Interconexión de Sistemas Abierto (OSI) como un protocolo de enrutamiento del tipo vector distancia avanzado, propiedad de Cisco, que ofrece las mejores características de los algoritmos vector distancia y de estado de enlace.

LAN: Son las siglas de "Local Area Network", es decir, Red de área local. Una Red LAN conecta diferentes ordenadores en un área pequeña, como un edificio o una habitación, lo que permite a los usuarios enviar, compartir y recibir archivos
.

NAT (Network Address Translation): Es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

OSPF (Open Shortest Path First): Abrir el camino más corto primero en español, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

PACKET TRACERT: Herramienta de aprendizaje y simulación de redes interactiva para los instructores y alumnos de Cisco CCNA. Esta herramienta les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales.

ROUTER: Dispositivo de hardware que permite la interconexión de ordenadores en red. Este dispositivo es el encargado de distribuir la conexión a Internet a distintos computadores vinculados a una misma red local actuando como un puente entre nuestros dispositivos y la internet.

ROUTING: Proceso de determinar el mejor camino para realizar el encaminamiento. En otras palabras, routing es el proceso que se realiza para determinar las tablas de encaminamiento.

Topología física: disposición de cada uno de los dispositivos o hardware dentro de una red. Se refiere a la forma en que una red transfiere tramas de un nodo al siguiente. Esta disposición consta de conexiones virtuales entre los nodos de una red. Los protocolos de capa de enlace de datos definen estas rutas de señales lógicas.

Topología lógica: es la forma que utilizan los hosts para comunicarse a través de una red. Se refiere a la forma en que una red transfiere tramas de un nodo al siguiente. Esta disposición consta de conexiones virtuales entre los nodos de una red.

VLAN: procedimiento para establecer redes lógicas de una forma independiente dentro de una misma red física. Es el acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias **VLAN** pueden coexistir en un único conmutador físico o en una única red física.

RESUMEN

Como estudiante de Ingeniería de Sistemas y en medio de la era de la Información se hace necesario tener grandes conocimientos en redes de datos. Estos conocimientos nos permiten adaptarnos a un creciente mercado mundial que demanda a diario profesionales competitivos y con la capacidad para entender, diseñar e implementar redes de datos.
Además, se hace necesario poder diagnosticar y dar solución a los problemas específicos sobre redes.

En este informe vamos a observar “pruebas de Habilidades Prácticas”, donde nosotros como estudiante debemos configurar los dispositivos de una red pequeña, un Router, un switch y equipos que admitan la conectividad IPV4 como IPV6, donde la intención es incrementar su seguridad, añadiendo contraseñas de clave de cifrado RSA, con modulos de 1024 bits, ya finalizando, veremos cómo establecer dirección ipv6 de capa 3 y configurar Switchs, PC, creación de puertos EtherChannel de capa 2 y como hacer PING para un PC-A, hasta a un PC-B.

Afortunadamente Cisco, Líder mundial en la fabricación y comercialización de componentes de comunicación, ofrece la oportunidad de certificarse realizando los cursos CCNA. Según CISCO la certificación CCNA “Es una de las certificaciones más importantes dentro de la industria de la Tecnología de la Información.

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

ABSTRACT

As a Systems Engineering student and in the midst of the Information Age, it is necessary to have great knowledge in data networks. This knowledge allows us to adapt to a growing world market that demands competitive professionals on a daily basis and with the ability to understand, design and implement data networks.
In addition, it is necessary to be able to diagnose and solve specific problems on networks.

In this report we are going to observe "Practical Skills tests", where we as a student must configure the devices of a small network, a Router, a switch and equipment that support IPV4 and IPV6 connectivity, where the intention is to increase its security, adding RSA encryption key passwords, with 1024-bit modules, already finishing, we will see how to establish layer 3 ipv6 address and configure Switches, PCs, creation of layer 2 EtherChannel ports and how to PING for a PC-A, up to a PC-B.

Fortunately, Cisco, a world leader in the manufacture and marketing of communication components, offers the opportunity to become certified by taking the CCNA courses. According to CISCO, the CCNA certification “It is one of the most important certifications within the Information Technology industry.

Keywords: CISCO, CCNA, Conmutación, Enrutamiento, Redes, Electrónica.

INTRODUCCIÓN

Les presento “Prueba de Habilidades Practicas Escenario 1”, donde consiste en configurar una red pequeña, que contiene Un router 4331 y dos switch 3560, y dos Pc, donde el docente desea que apliquemos configuraciones especiales para demostrar nuestras capacidades y técnicas aprendidas en el transcurso de este Diplomado.

La evaluación del Diplomado de Profundización CCNA, busca identificar el grado de desarrollo de competencias y habilidades, donde debemos resolver los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Para esta actividad, como estudiante de la Universidad Nacional, Abierta y a Distancia, debemos explorar el escenario 1, lo cual es realizada por medio de una simulación de red, llamada Packet Tracer Version 7.3.1 del año 2020, el cual nos permite crear una red simulada, para lograr experimentar y desarrollar la topología física y analizar el comportamiento de toda la red del escenario uno.

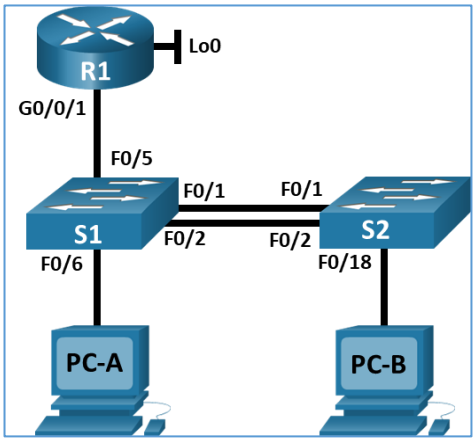
Vamos a registrar la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

1. Descripción de Escenarios propuestos para la prueba de habilidades

Escenario 1

Topología

Figura 1. Escenario 1



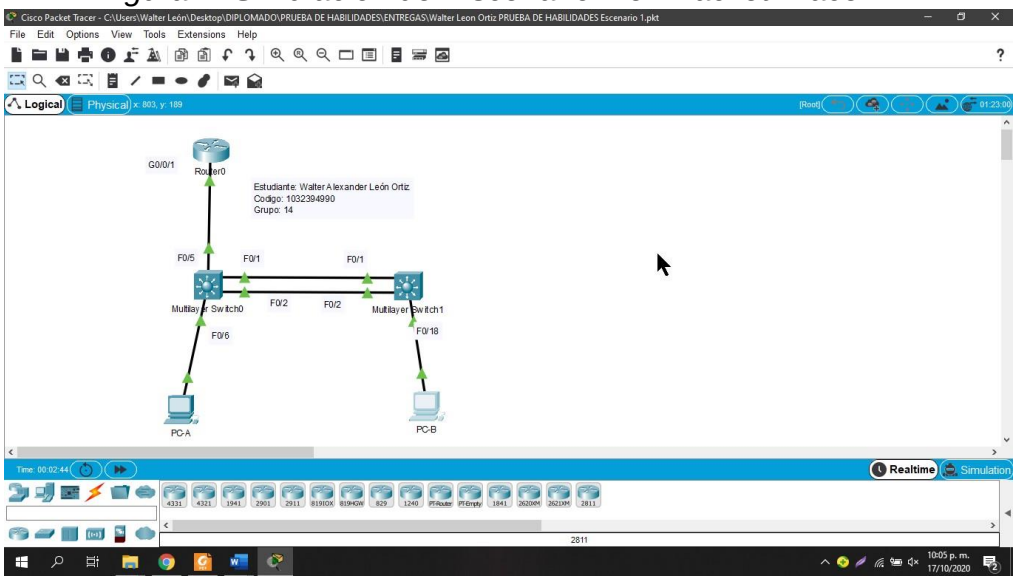
Se aprecia la Topologia “modelo” en Packet Tracer

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.

Ahora vamos a visualizar, la topología ya realizada en el Packet Tracer, lo cual es una herramienta de simulación de redes interactiva para los instructores y alumnos de Cisco CCNA. Esta herramienta les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales.

Figura 2. Simulación del 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

En esta tabla, observamos los nombres que se deben asignar en el modo privilegiado “Comandos”. Esto se hace desde la pestaña “CLI”.
Esto con el fin de que las direcciones Ipv6 e Ipv4 deben ser incorporadas al router y también a los switchs con la segmentación necesaria para que interactúen con el tráfico de paquetes en la red.

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

Es importante tomar en cuenta, que, en esta tabla, observamos la Asignacion de direcciones IPV6, que se deben asignar en el modo privilegiado “Comandos” eso se debe aplicar en el Router 1, Switchs 1 y 2 y tambien en la PC-A.

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

Instrucciones:

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

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.

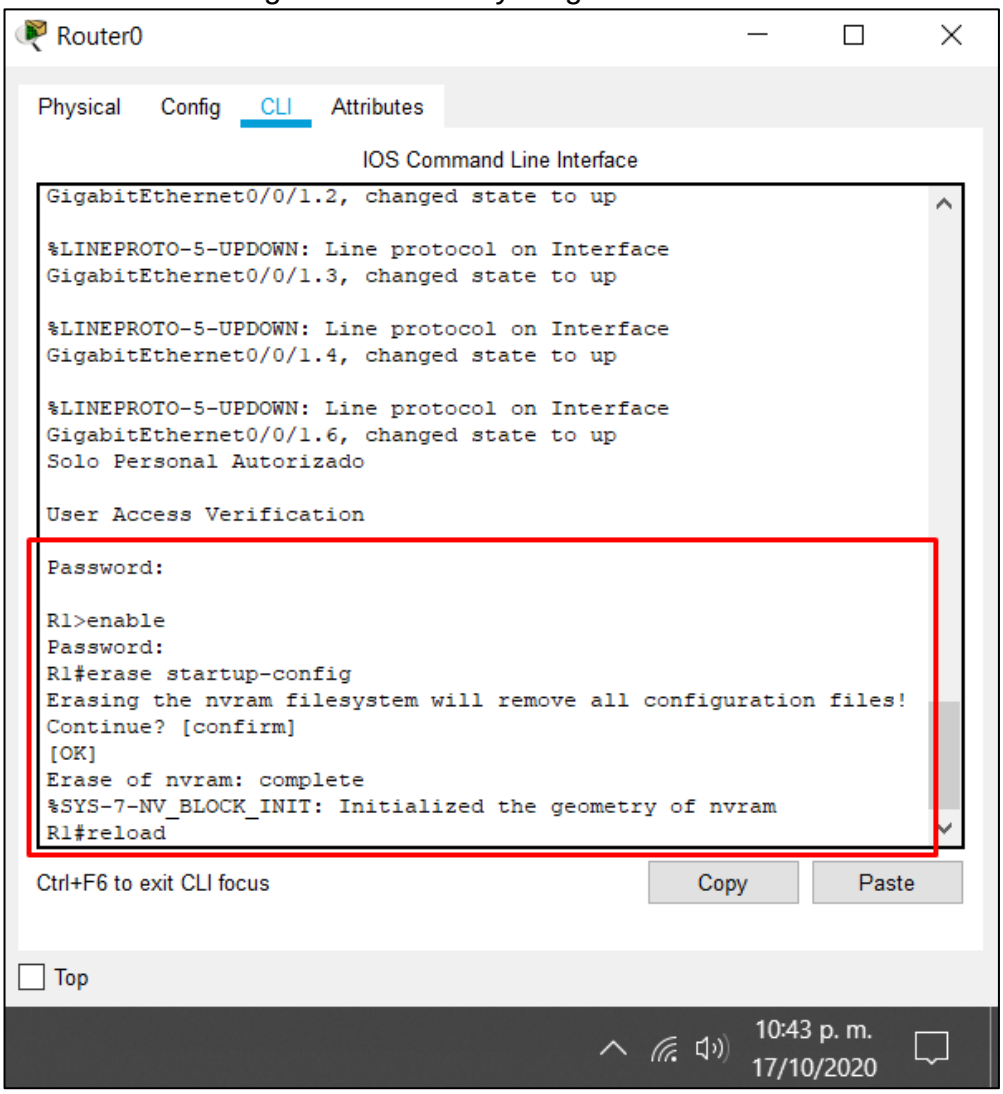
Debo acceder al Router 1 a través de la consola en modo privilegiado para borrar cualquier configuración de inicio con el comando *erase startup-config* el cual borra el contenido de la NVRAM, posteriormente se reinicia el Router con el comando *reload*, quedando esté listo para su configuración inicial.

Tabla 3: Borrado y Carga del Router Escenario 1

Inicialización y carga del Router: Borrado configuraciones Escenario 1	
Tarea	**Especificación**
Accedemos 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	**Router>enable** ***Router#erase startup-config*** **Router#reload** *Proceed with reload? [confirm]* *Initializing Hardware ...*

En esta sección, se realiza la inserción de esta línea de comandos para eliminar las configuraciones y la base de datos de VLAN del switch. En el laboratorio de simulación, lo único importante es que el switch también sea compatible con la VLAN. La única manera de crear VLAN es utilizando switches gestionables. La VLAN, a la que el punto de acceso y otros dispositivos de infraestructura, como el switch, se conectan, se denomina "VLAN”

Figura 3: Borrado y carga del Router:



Fuente: Autor

Se accede al Switch 1 con la consola en modo privilegiado para escribir el comando *erase startup-config* este comando borra el contenido de la NVRAM. El comando *delete vlan.dat* ayuda a eliminar la base de datos de la vlan. El procedimiento es igual para todos los Switch.

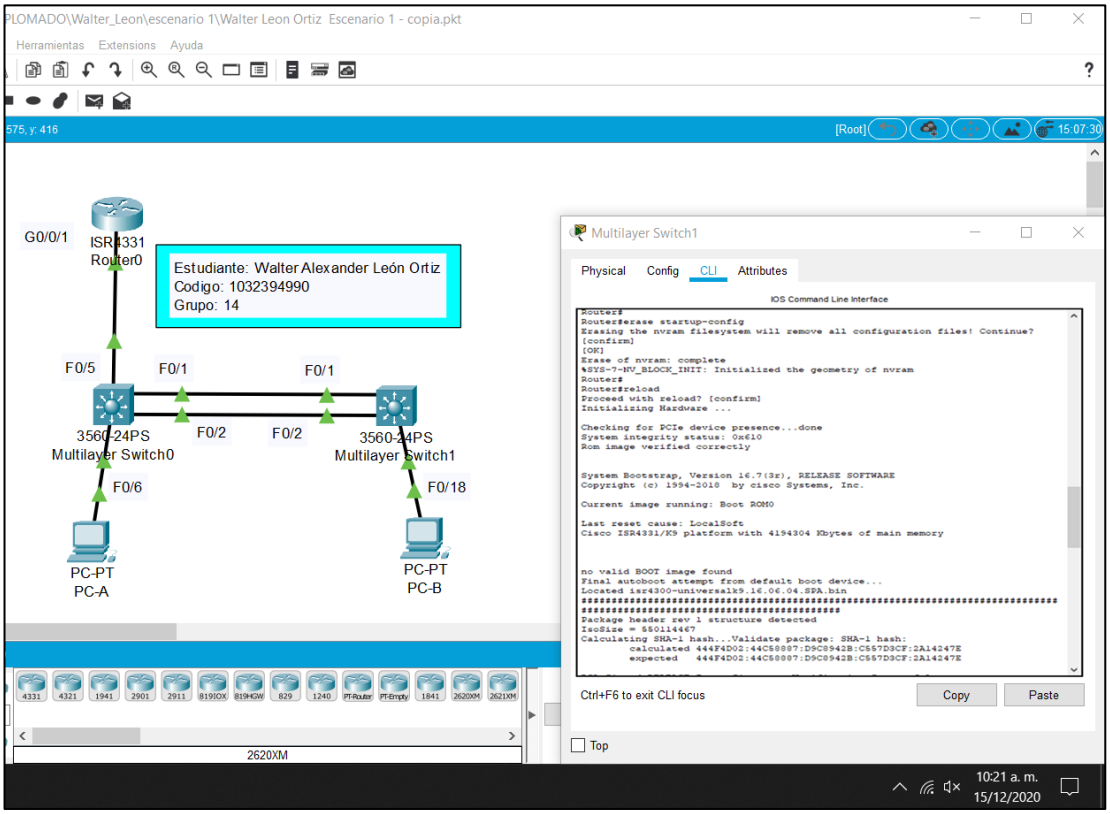
En este proceso permite restaurar el switch y borrar cualquier configuración de inicio, posteriormente se reinicia con el comando *reload*, quedando esté listo para su configuración inicial. Usaremos el Switch 1, para conectar equipos, como la PC-B, y Pc-A, cuyo objetivo puede conectarse a muchos dispositivos para formar una red, que puede ser pequeña o grande, (LAN, WAN).

Tabla 4. Reinicio de Switches 0 y 1

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	Switch#reload
	Proceed with reload? [confirm] Initializing Hardware ...
Para verificar que la base de datos, no está en la memoria Flash, se debe escribir el comando “show vlan brief”	Switch>enable Switch#show vlan brief

Nuestro objetivo es eliminar el vlan.dat, que contiene la base de datos y de configuración, empezamos desde la consola en modo privilegiado, con el fin de borrar todo, lo haremos con el comando *erase startup-config* el cual borra el contenido de la NVRAM

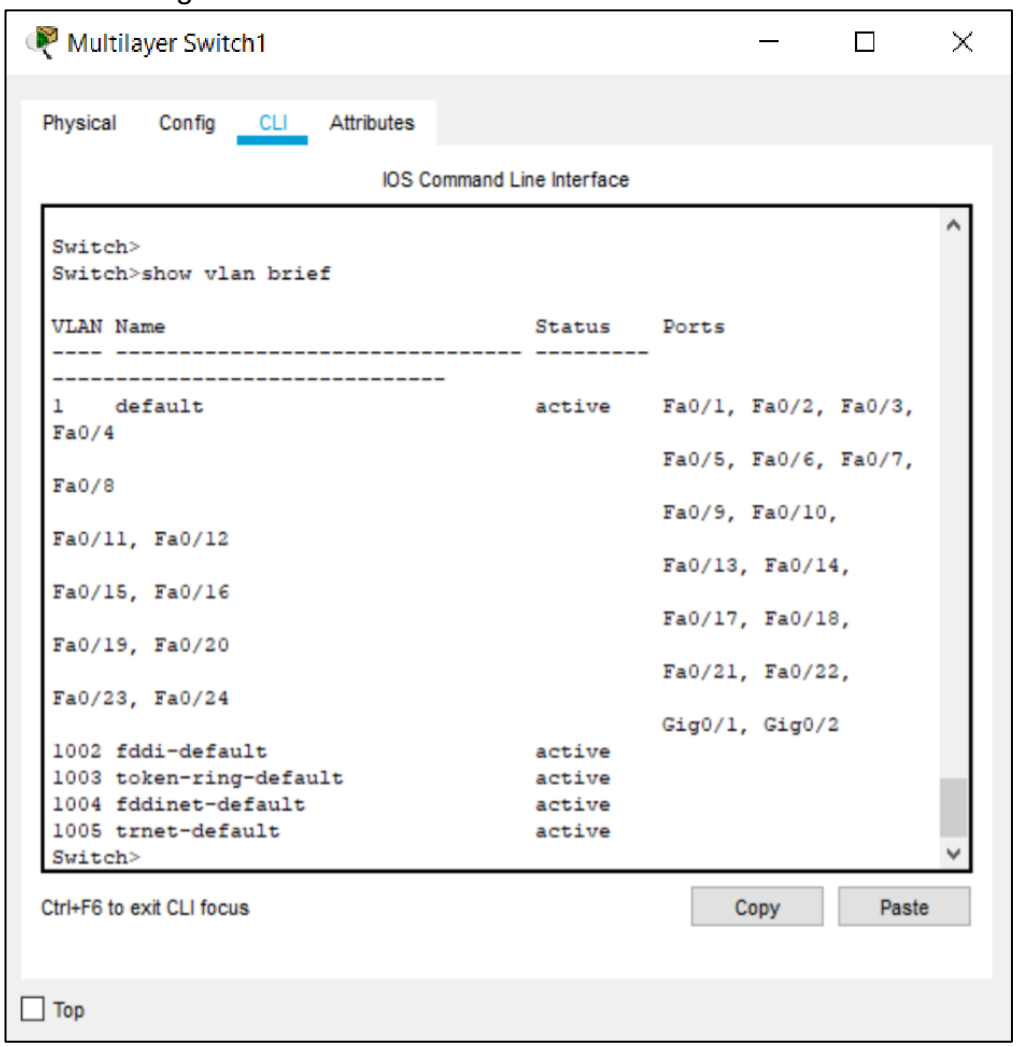
Figura 4: Reiniciando el Switch 1



Fuente: Autor

Se realiza el comando “**reload**” para reiniciar las configuraciones del router R1.

Figura 5: Verificar borrado de vlan.dat del Switch 1



Fuente: Autor

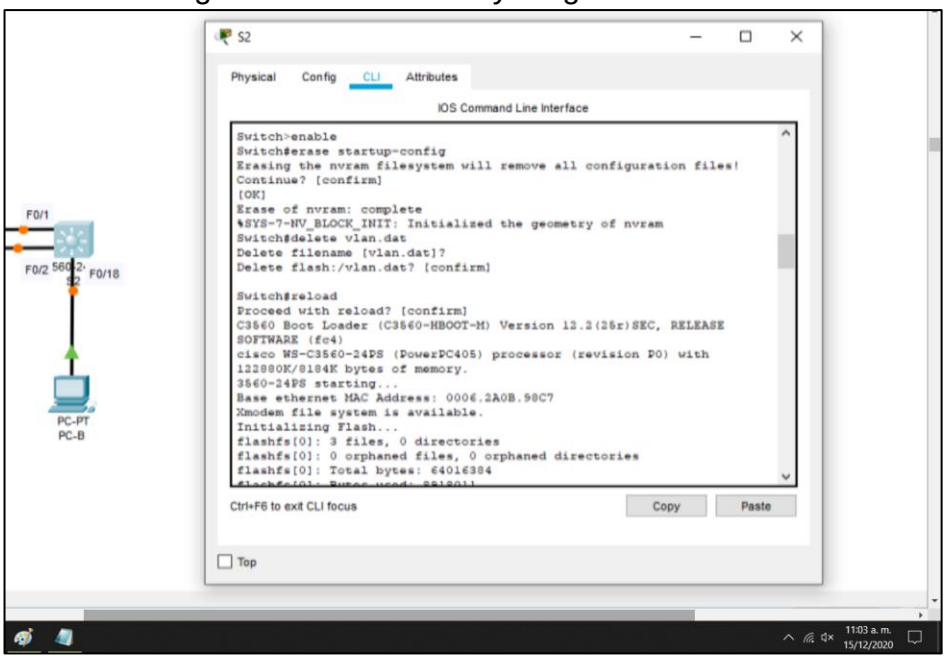
Usamos el comando “Show vlan brief”, para la verificación del borrado del archivo vlan.dat del s1. De lo contrario seguirá aoareciendo archivos vlan.dat

El comando show vlan brief muestra el tipo de asignación y pertenencia de VLAN para todos los puertos de switch. Este comando “show vlan brief”, Sirve para mostrar la información de VLAN.

Se realiza la inserción del comando “reload” para recargar o reiniciar las configuraciones del Switch S1 siendo exitoso.

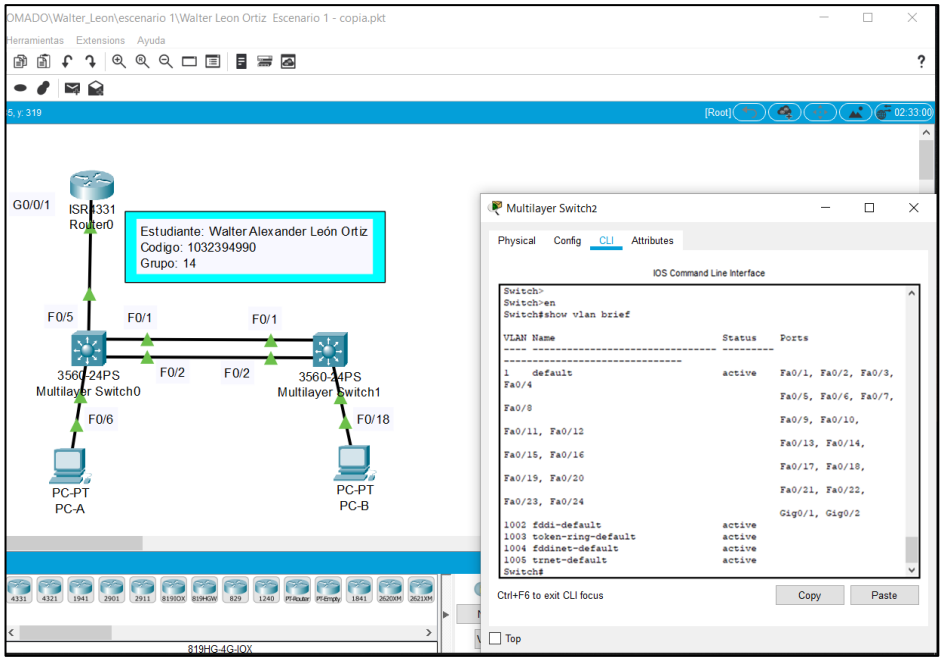
Nota: El comando show vlan brief muestra el tipo de asignación y pertenencia de VLAN para todos los puertos de switch. Cada VLAN debe corresponder a una subred IP única. Utilice el comando show vlan para verificar si el puerto pertenece a la VLAN esperada.

Figura 6. Inicialización y carga del Switch 2



Fuente: Autor

Figura 7: Verificar borrado de vlan.dat del Switch 2



Fuente: Autor

Se cambia los nombres de cada switch, se personaliza la Topologia, y usamos el mismo comando que vimos en el switch 1 “s1”, lo cual es, “**Show vlan brief**”.

1.2. Configuración plantilla SDM para que admita IPv6

✓ Ahora que ya reiniciamos el switch, configuraremos la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.

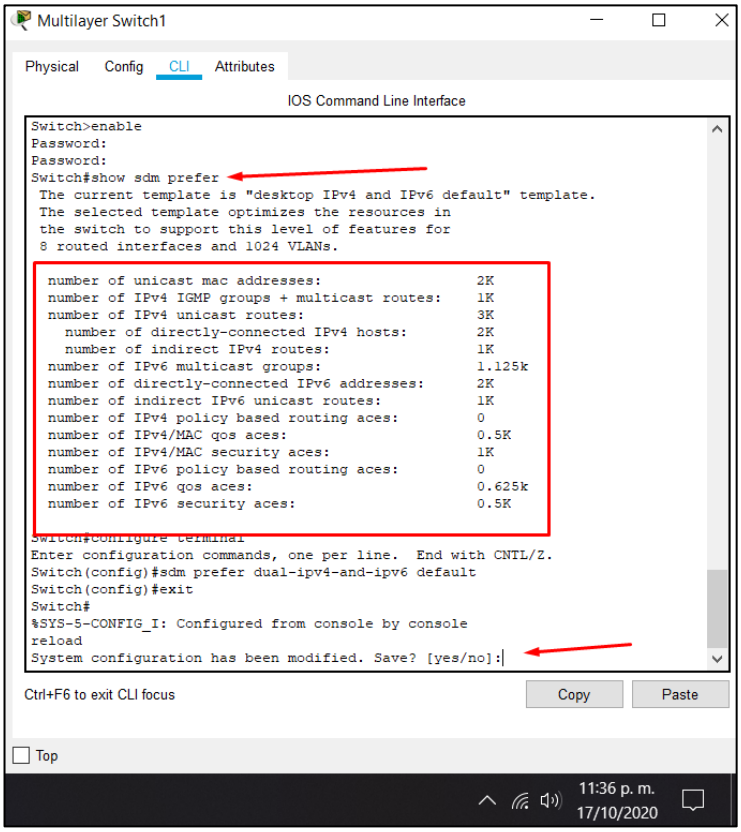
Teniendo en cuenta que el Switch Cisco 3560 no soporta capacidades IPv6 se debe configurar la plantilla SDM para que pueda admitir IPv6 junto con IPv4, se verifica desde modo privilegiado la configuración con el comando *show sdm prefer*, donde se muestra que solo soporta configuración IPv4, para activar 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.

Tabla 5. Configurando Plantilla SDM para admitir IPV6

Configuración de plantilla SDM en Switch 1 y 2:	
Tareas	**Especificación**
Verificamos y seleccionamos la plantilla. Este comando ayuda a habilitar el modo privilegiado, y a la vez habilitar comandos.	Switch>enable
Ver plantillas SMD. Este comando me ayuda a mostrar, lo que puede soportar este Switch, y hasta ahora, solo soporta configuración IPv4	Switch#show sdm prefer Switch#configure terminal Switch(config)#sdm prefer ?
Modificar la plantilla SMD.	Switch#configure terminal Switch(config)#sdm prefer dual-ipv4-and-ipv6 ? Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Volver a cargar switch. Se realiza la inserción de esta línea de comandos para recargar las configuraciones del switch	Switch(config)#exit Switch#reload
El comando “show sdm prefer” sirve para verificar los cambios efectuados switch.	Switch>en Switch#show sdm prefer
	Switch#reload

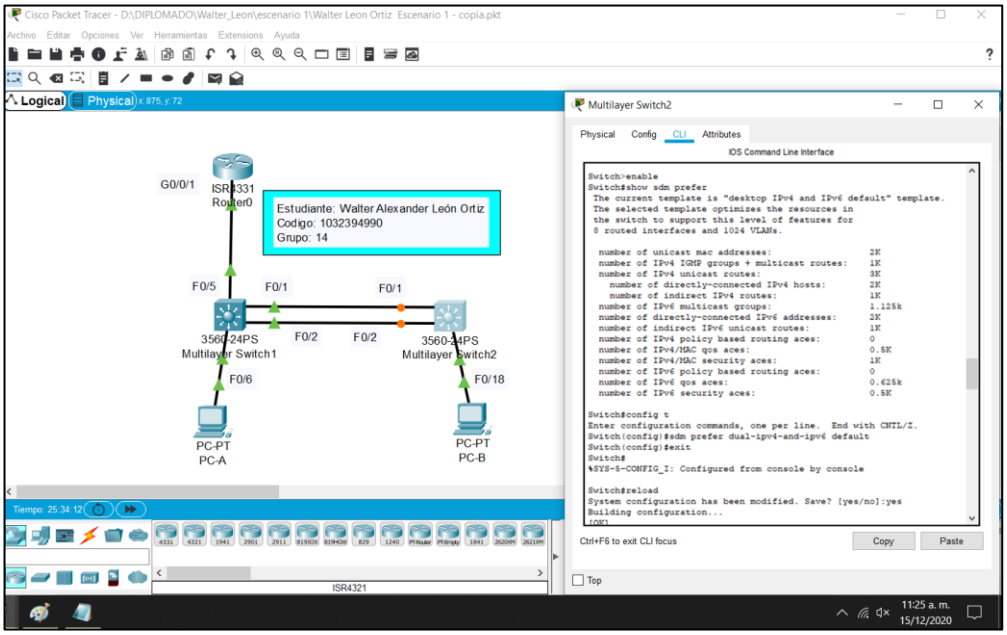
Para esta práctica, el Switch Cisco 3560 no soporta capacidades IPv6 se debe configurar la plantilla SDM para que pueda admitir IPv6 junto con IPv4. para activar la configuración IPv6 se procede a ejecutar el comando sdm prefer dual-ipv4-andipv6 default, inmediatamente se reinicia con el comando reload para que la nueva plantilla sea cargada.

Figura 8: Plantilla SDM en Switch 1



Fuente: Autor

Figura 9. Plantilla DSM en Switch 2



Fuente: Autor

Paso 2: Configurar R1

✓ Las tareas de configuración para R1 incluyen las siguientes:

Tabla 6. Configuración del Router

Tarea	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain lookup
Nombre del router (R1)	Router(config)#hostname R1
Nombre de dominio (ccnalab.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
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 linklocal.
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-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 linklocal 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 linklocal 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

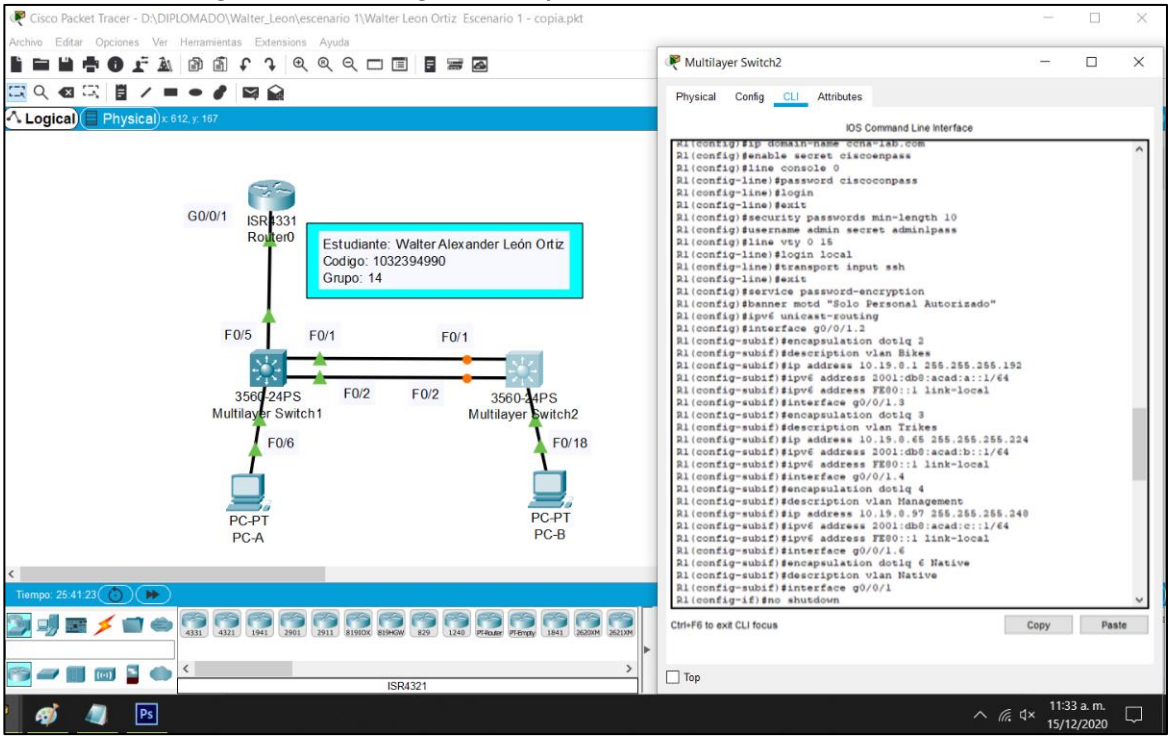
Debemos realizar la configuración inicial del Router, desde la consola modo privilegiado se procede a ejecutar el comando *no ip domain lookup* que permite desactivar la búsqueda DNS para indicar que, si hemos cometido un error en el scrip de configuración, nos muestra un aviso indicando el error, se configura el nombre del dispositivo con el comando "**hostnam**e" y nombre de dominio del mismo junto con la contraseña cifrada para ingresar al modo privilegiado a través del comando *enable secret*.

Configuracion contraseña en R1:

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*.

Entonces, configura el mensaje del día en el *banner, con el comando "MOTD"* dejando un aviso para acceso no autorizado, se activa el enrutamiento IPv6 con *ipv6 unicast-routing*.

Figura 10. Configuración parámetros básicos del Router

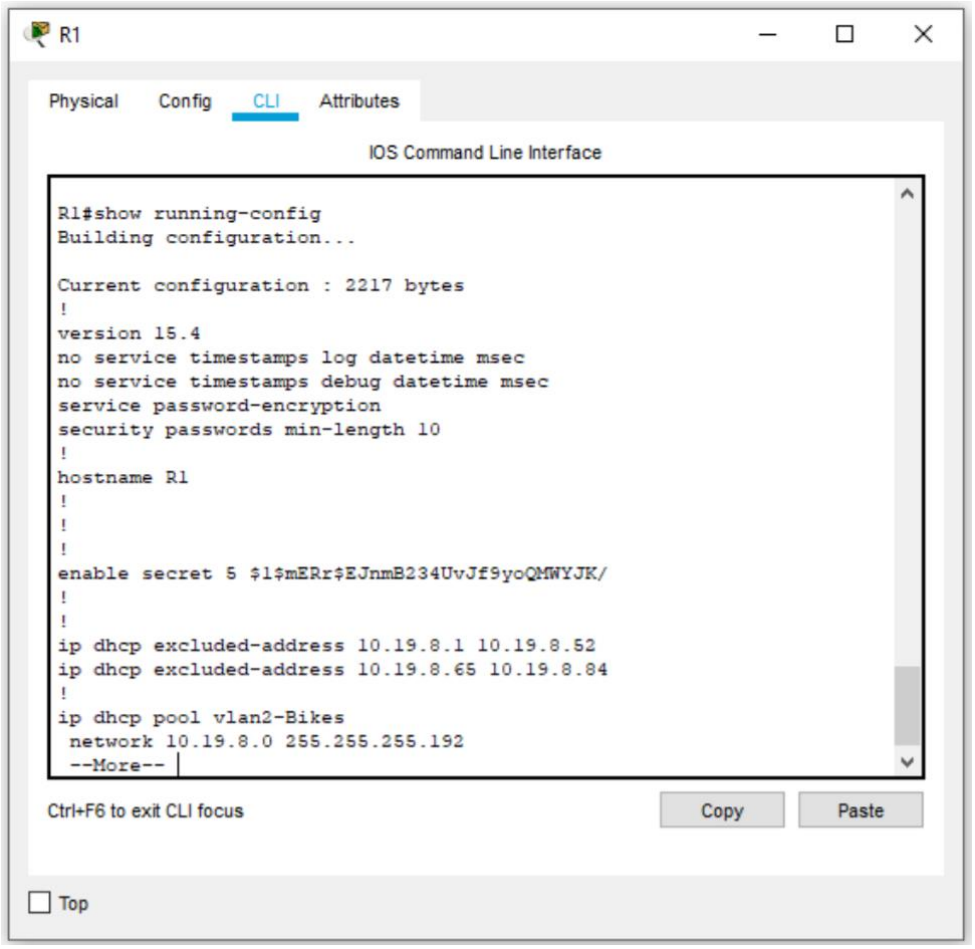


Fuente: Autor

Configurar la interfaz G0/0/1

Es aquí donde entramos a configurar 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, finalmente se crea una llave de encriptación RSA con el comando *crypto key generate rsa* asignándole una longitud de 1024 bits.

Figura 11. Verificacion del Router



Fuente: Autor

Aquí, finalmente se crea una llave de encriptación RSA con el comando crypto key generate rsa asignándole una longitud de 1024 bits.

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 (ccnalab.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 linklocal 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

Configuración para Switch 1:

Se realiza la 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. Ahora se configura el nombre del dispositivo con el comando “hostname” y nombre de dominio del mismo, junto con la contraseña cifrada para ingresar al modo privilegiado a través del comando *enable secret*.

Procedemos a crear y configurar 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*.

Aquí 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*, entonces, 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*.

Luego, en esta sección se configura el mensaje del día en el *banner, con el comando “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.

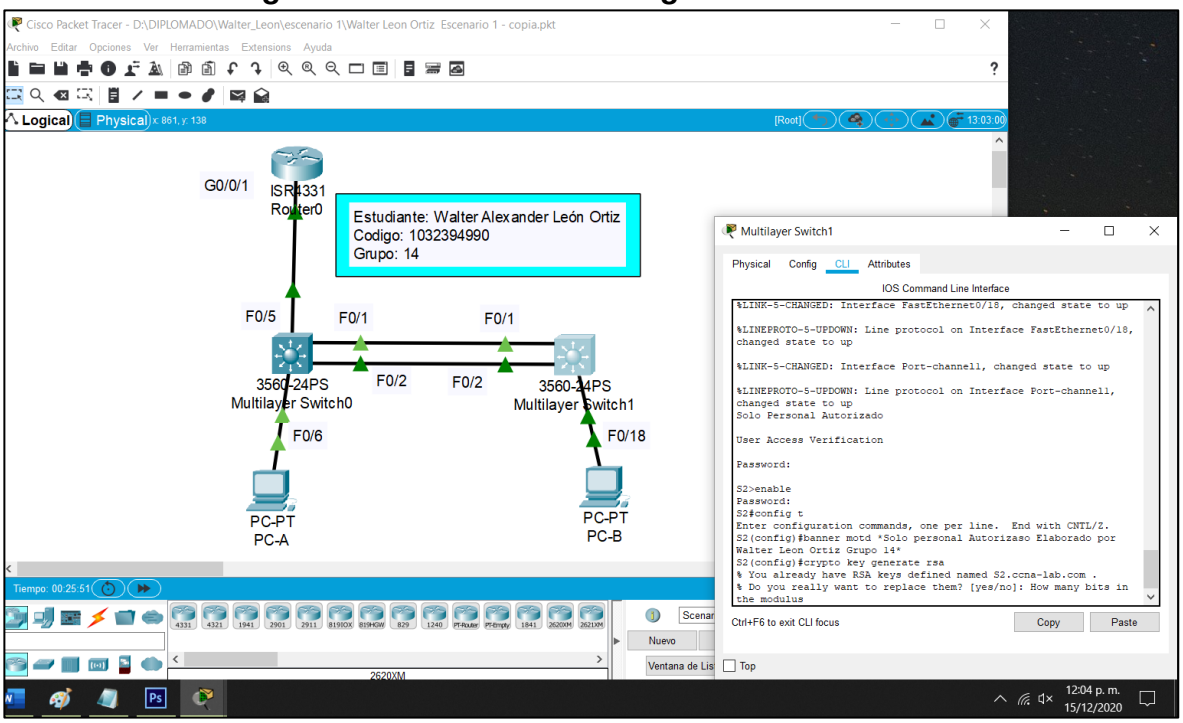
Una vez creada la llave deencriptacion RSA, se configura la Interfaz administrativa (SVI) correspondiente a la vlan 4 Management asignándole la IPv4 10.19.8.98 y mascara de red 255.255.255.248, con su dirección IPv6 2001:db8:acad:c::98 prefijo /64 y puerta de enlace local fe80::98. Ahora realizamos una descripción y se activa con el comando *no shutdown*.

Finalmente se configura la puerta de enlace predeterminada lo cual es: 10.19.8.97 para IPv4, no se configura puerta de enlace, en IPv6 si, porque se asigna de manera automática.

Figura 12. Configuración del Switch 1

Fuente: Autor

Figura 13. 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 (ccnalab.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

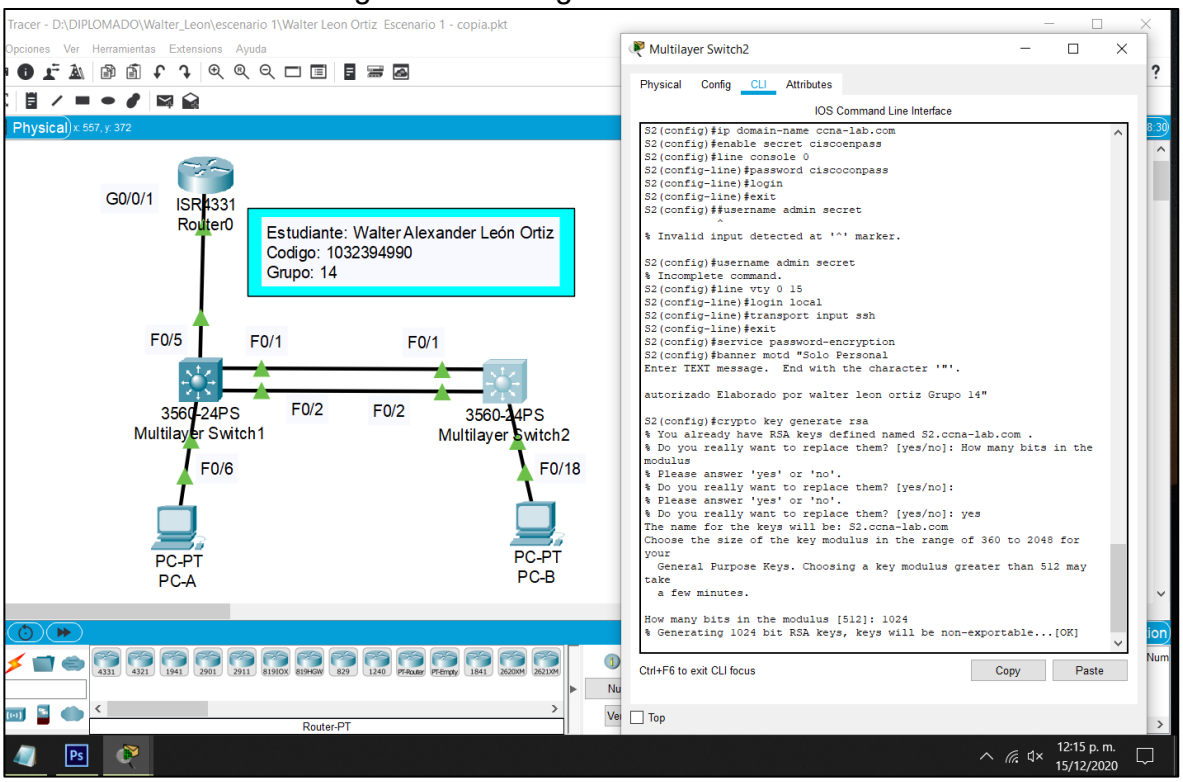
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 15 S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config-line)#transport input ssh S2(config-line)#exit
Cifrar las contraseñas de texto no 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
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 linklocal 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

Consola "Privilegiado" en switch 2:

Empezamos abrir el switch 2 para acceder a la consola modo privilegiado, donde se procede a ejecutar el comando *no ip domain lookup* que permite desactivar la búsqueda DNS, (pasos muy similares al switch 1), 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*, Luego, se configura la contraseña para ingresar a la consola con el comando *password* y activándola con *login,* estableciendo en una longitud mínima de 10 caracteres para las contraseñas con el comando *security passwords min-length 10*.

Vamos a crear 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 configura el mensaje del día en el *banner con el comando* ***"MOTD"*** dejando un aviso para acceso no autorizado.

Figura 14. Configurando El Switch 2



Fuente: Autor

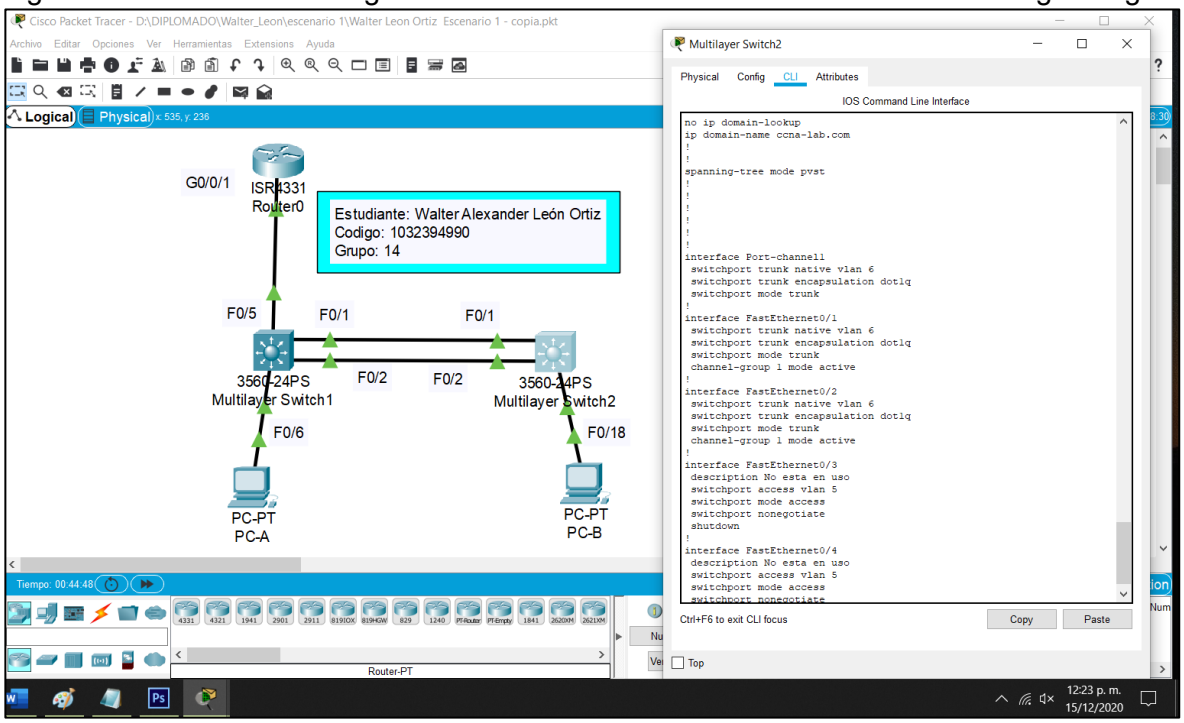
Posteriormente se debe crear una llave de encriptación RSA, con el comando *crypto key generate rsa* asignándole una longitud de 1024 bits, se configura la Interfaz administrativa (SVI) correspondiente a la vlan 4 Management asignándole la IPv4 10.19.8.98 y mascara de red 255.255.255.248, con su dirección IPv6 2001:db8:acad:c::99 prefijo /64 y puerta de enlace local fe80::99.

Luego se realiza una descripción y se activa con el comando *no shutdown*.

Finalmente se configura la puerta de enlace predeterminada 10.19.8.97

Nota: para IPv4, no se configura puerta de enlace, en IPv6 si, porque se asigna de manera automática.

Figura 15. Verificación configuración Switch 2 usando el comando “show running-config”



Fuente: Autor

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

Paso 4: Configurar S1

EN este paso, vamos a crear una red VLAN, Trunking, EtherChannel, todo esto en el Switch 1

Nota: Es un enlace que se configura en uno o más puertos de un switch para permitir el paso del tráfico de las distintas VLANs que hemos configurado. Este enlace puede funcionar en una conexión de switch a otro switch o bien, de un switch a un router.

Para corroborar la creación de nuestro VLAN puedes utilizar el siguiente comando: Show lan

✓ 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	Password: S1>enable Password: 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 fa0/724 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

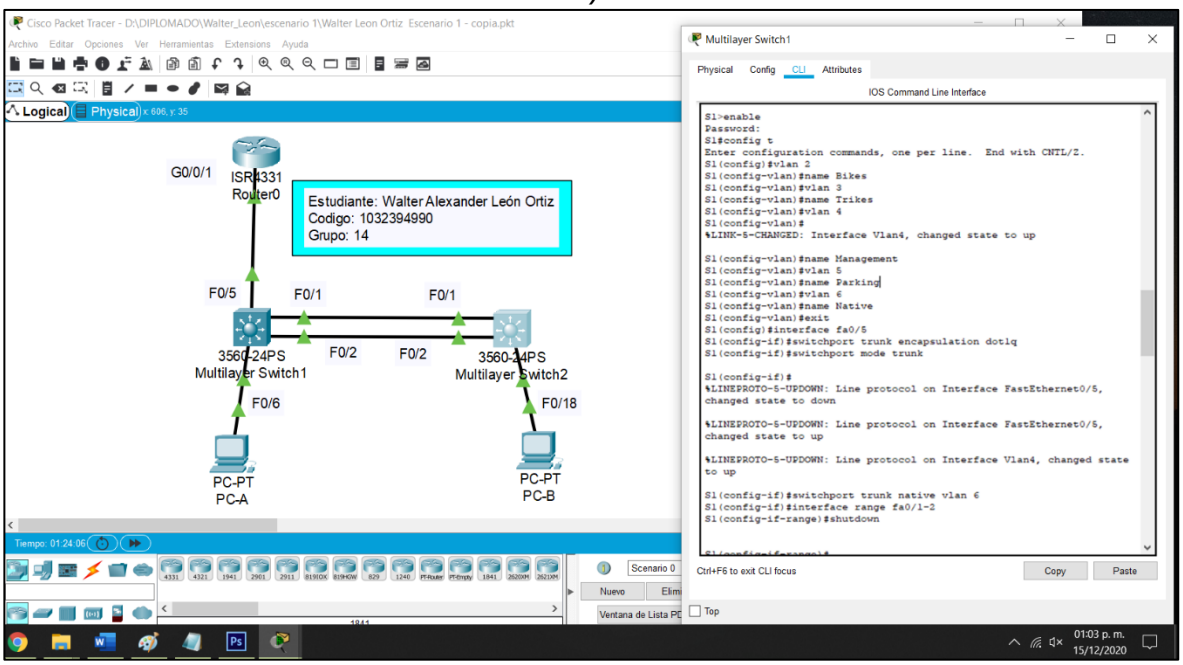
Desde la consola, modo privilegiado, configuración global se crean las vlan 2Bikes, vlan 3-Trikes, vlan 4-Management, vlan 5-Parking y vlan 6-Native, se crean las trocales 802.1Q que usen la vlan nativa interfaces fa0/1, fa0/2 y fa0/5, inicialmente

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.

Vamos a configurar 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*, entonces, 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.

Posteriormente, se configura un puerto de acceso para la vlan 2- Bikes, que pueda usar la fa0/2 con el comando *switchport acces vlan 2*, configuración de seguridad en los puertos de aceso que permita 3 direcciones MAC, luego, activamos la seguridad en la interfaz estableciendo máximo 3 direcciones MAC con *switchport port-security maximum 3*.

Figura 16. Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) en Switch 1



Fuente: Autor

Entonces, 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*.

Para configurar la VLAN de acceso cuando la interfaz está en modo de acceso, use el comando switchport access vlan. En el mundo de Cisco, los enlaces a otros conmutadores se conocen como puertos "troncales" y los enlaces a dispositivos finales como PC se conocen como puertos de " acceso ". En un puerto, que es un puerto de acceso, la VLAN sin etiquetar se denomina VLAN de acceso. En un puerto, que es un puerto troncal, la VLAN sin etiquetar se denomina VLAN nativa

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

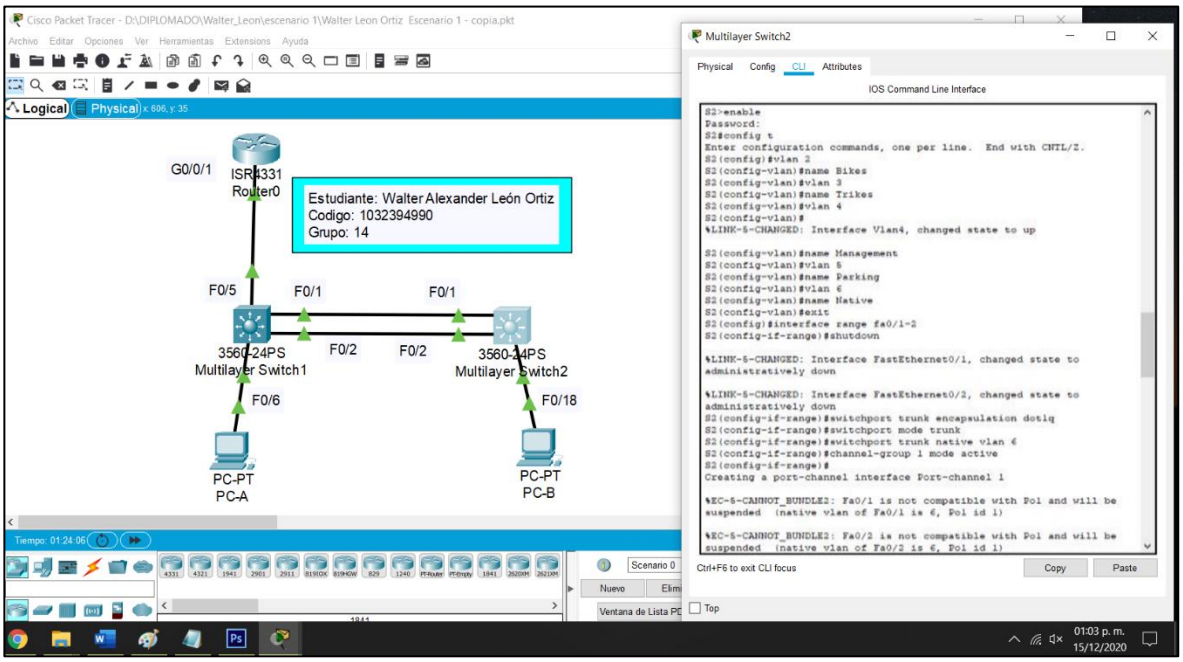
Los puertos trunk -trunk-Mode están diseñados para los enlaces de switch a switch. Los puertos troncales pueden recibir tanto paquetes etiquetados como no etiquetados. Los paquetes etiquetados recibidos en un puerto troncal se reenvían en la VLAN que se encuentra en la etiqueta si el puerto troncal es un miembro de la VLAN. Los paquetes no etiquetados recibidos en un puerto troncal se reenvían en la VLAN nativa.

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*.

Luego 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*.

Figura 17. Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) en Switch 2



Fuente: Autor

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*.

La 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*.

Parte 3: Configurar soporte de host

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11. Configuración de soporte de host en Router

Tarea	Especificación
Activar el rango fa0/1-2 en switch 1	Activar el rango fa0/1-2 en switch 1
S1(config)#interface range fa0/1-2	S1(config)#interface range fa0/1-2
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 que debe estar configurada.	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 este 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.

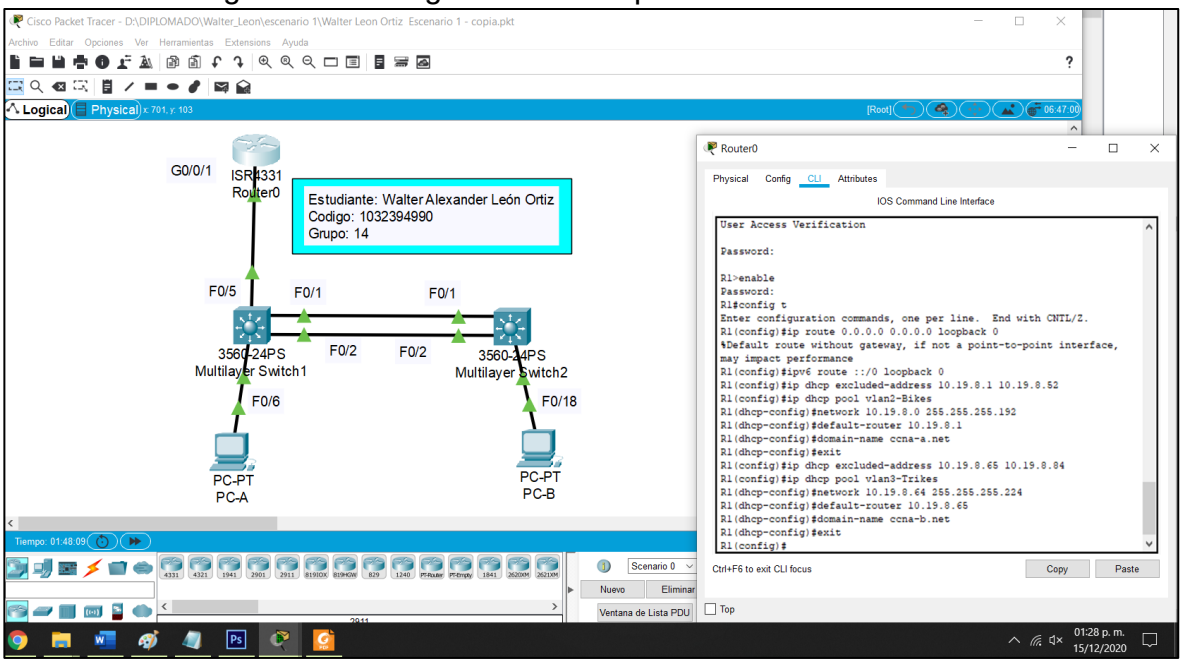
Para ello se aplicó para excluir estas 10 direcciones el comando *ip dhcp excluded-address 10.19.8.1 10.19.8.52*, y para el pool de DHCP *ip dhcp pool vlan2-Bikes*, red y mascara de red *network 10.19.8.0 255.255.255.192.*

El comando para la puerta de enlace predeterminada, es *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.

En esta sección, 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, luego, vamos a 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*, donde la puerta de enlace predeterminada, es *default-router 10.19.8.65*, nombre de dominio *domain-name ccna-b.net*.

Figura 18. Configuración de soporte de host en Router



Fuente: Autor

Paso 2: Configurar los servidores

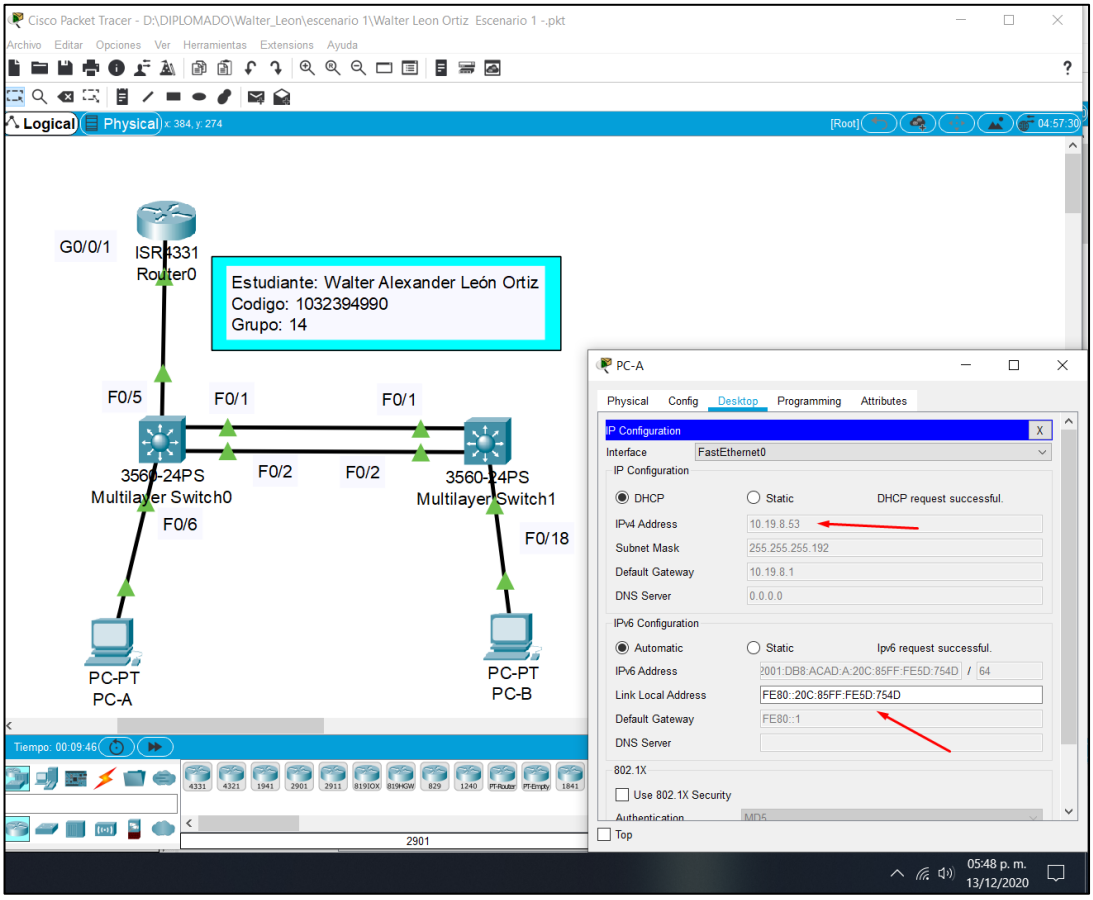
✓ Configuraremos los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, registre las configuraciones de red del host con el comando ipconfig /all.

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

Tabla 12. Configuración de red del PC-A

Configuración de red de PC-A	
Descripción	**Puerto**
Dirección física	FE80::20C:85FF:FE5D:754D
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 19. Configuracion de red PC-A



Fuente: Autor

Se realiza el procedimiento de Configuración del direccionamiento de red de PC-A utilizando las direcciones propuestas de acuerdo a Datos tomados por DHCP mostrados en (Tabla 10. Configuración de red de PC-A) siendo exitoso su configuración.

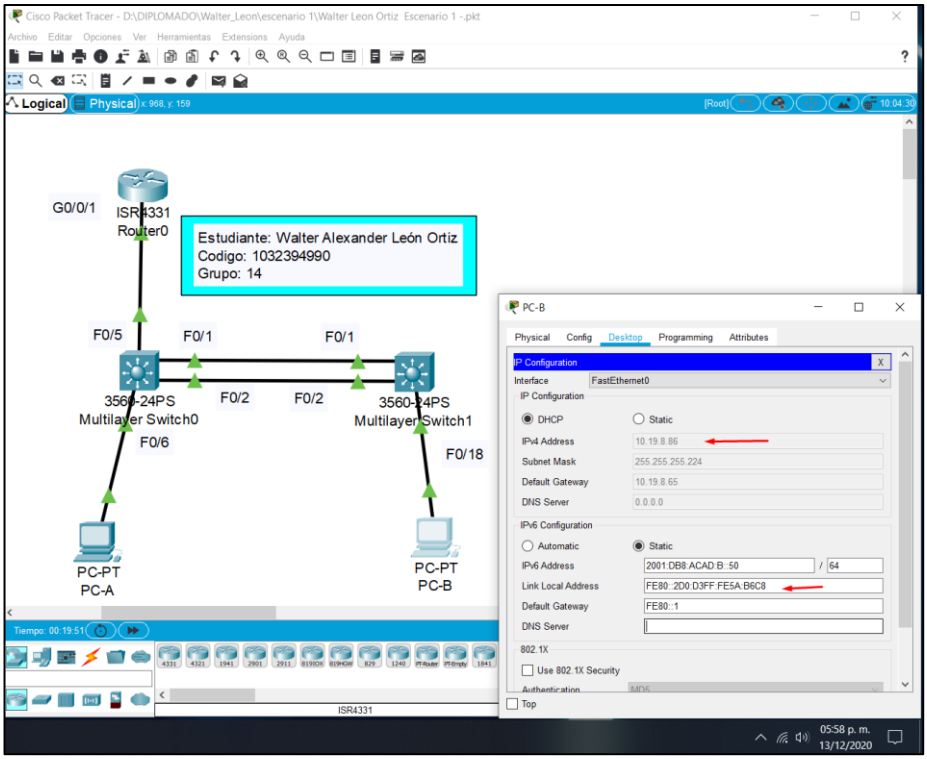
El protocolo DHCP funciona sobre un servidor central (servidor, estación de trabajo o incluso un PC) el cual asigna direcciones IP a otras máquinas de la red. Este protocolo puede entregar información IP en una LAN o entre varias VLAN. Esta tecnología reduce el trabajo de un administrador, que de otra manera tendría que visitar todos los ordenadores o estaciones de trabajo uno por uno. Para introducir la configuración IP consistente en IP, máscara, gateway, DNS, etc.

Realizando las Configuracines de los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y Después de configurar cada servidor, registre las configuraciones de red del host con el comando ipconfig /all.

Tabla 13. Configuración de red del PC-B

Configuración de red de PC-B	
Descripción	**Puerto**
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 20. Configuracion de red de Pc-B



Fuente: Autor

En la figura 20, se observa el resultado de Configuración del direccionamiento de red de PC-B utilizando las direcciones propuestas de acuerdo a Datos tomados por DHCP. Es importante que en la PC-B la casilla DHCP, debe estar marcada.

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. Ahora vamos a realizar las medidas correctivas para establecer la conectividad si alguna de las pruebas falla: Observemos la tabla 14.

Tabla 14. Verificación de los dispositivos de red PC-A

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

Tabla 15. Verificación de los dispositivos de red PC-B

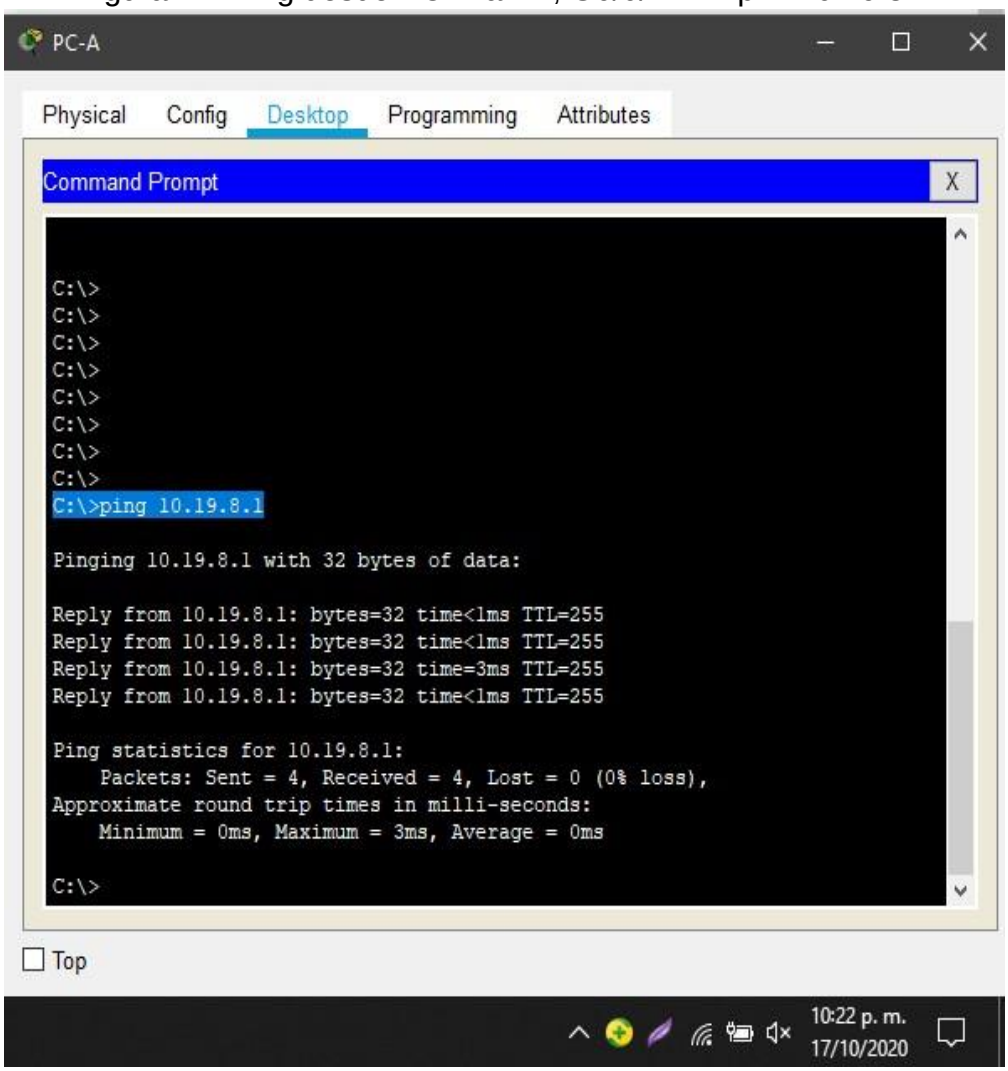
Desde	A	De INTERNET	Direccion IP	Resultados de Ping
	PC-B	Dirección	10.19.8.85	Si hay respuesta
		IPv6	2001:db8:acad:b::50	Se asigna IPv6 estática, prefijo 64 y puerta de enlace fe80::1 Si hay respuesta
	R1 Bucle 0	Dirección	209.165.201.1	Si hay respuesta
		IPv6	2001:db8:acad:209::1	Si hay respuesta
PC-B	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
	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

Realizamos las medidas correctivas para establecer la conectividad si alguna de las pruebas falla. Aunque depende de la configuración, quizás pueda fallar, o de lo contrario, podemos proceder al siguiente dispositivo.

Para realizar cada ping entre dispositivo se debe tener en cuenta el tipo de dirección a la cual se quiere hacer el procedimiento identificando si estas es IPv4 o IPv6 puesto que la estructura de dirección tiene diferente sintaxis.

Se debe realizar pin desde la PC_A hacia R1, G0/0/1.2 enviando los paquetes a su dirección IPv4 utilizando el comando ping 10.19.8.1 logrando realizar el pin con éxito del mismo modo se realiza pin desde la PC_A hacia R1, G0/0/1.2 enviando los paquetes a su dirección IPv6 utilizando el comando ping 2001:db8:acad:a::1 logrando realizar el pin también con éxito

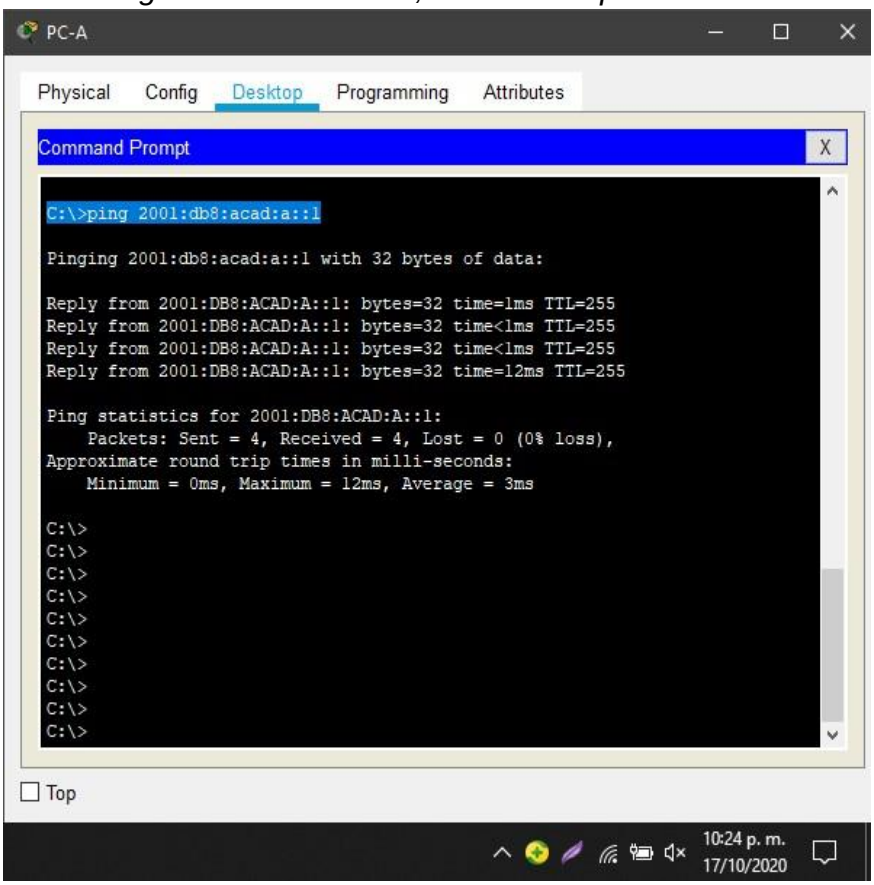
Figura 21. Ping desde PC-A a R1, G0/0/1.2 – Ipv4 10.19.8.1



Fuente: Autor

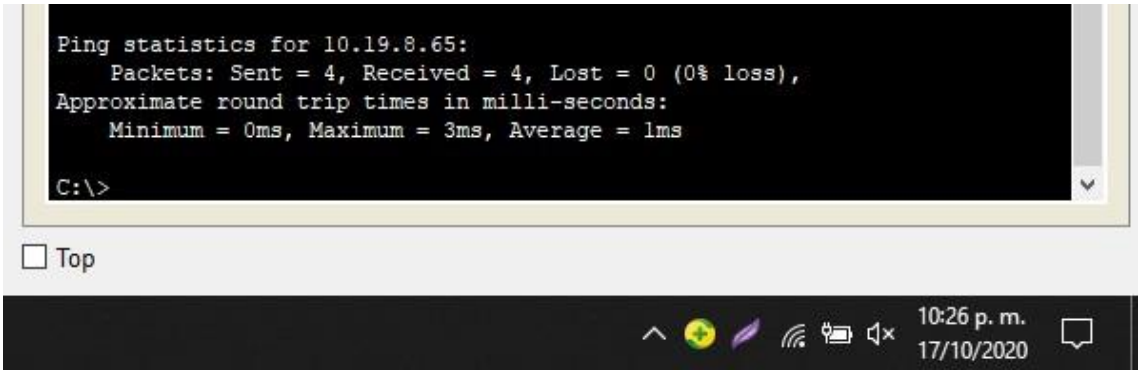
En la figura 21, se evidencia que el Pc-a si tiene ping a R1, G0/0/1.2 – Ipv4 10.19.8.1. Ahora seguimos estas mismas pruebas con todas las interfaces configuradas, incluyendo PC-B.

Figura 22. Ping desde PC-A a R1, G0/0/1.2 – Ipv6 2001:db8:acad:a::1



Fuente: Autor

Figura 23. Ping desde PC-A a R1, G0/0/1.3 – Ipv4 10.19.8.65

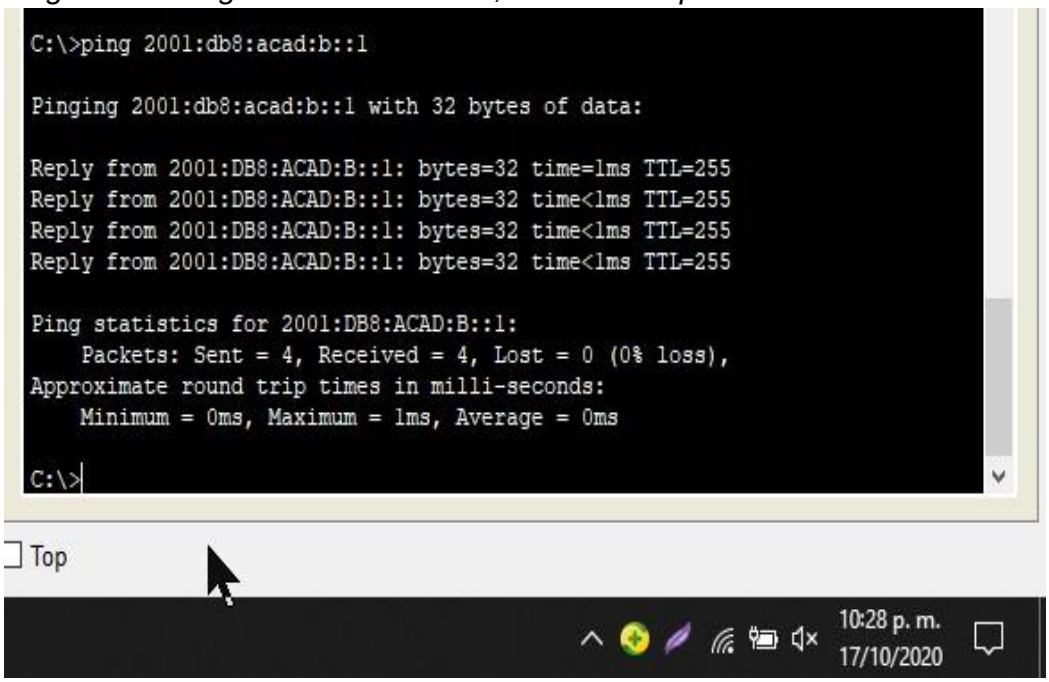


Fuente: Autor

Se realiza pin desde la PC_A hacia R1, G0/0/1.3 enviando los paquetes a su dirección IPv4 utilizando el comando ping 10.19.8.65 logrando realizar el pin con

éxito del mismo modo se realiza pin desde la PC_A hacia R1. Para esta sección, No debe fallar los pings en las computadoras host.

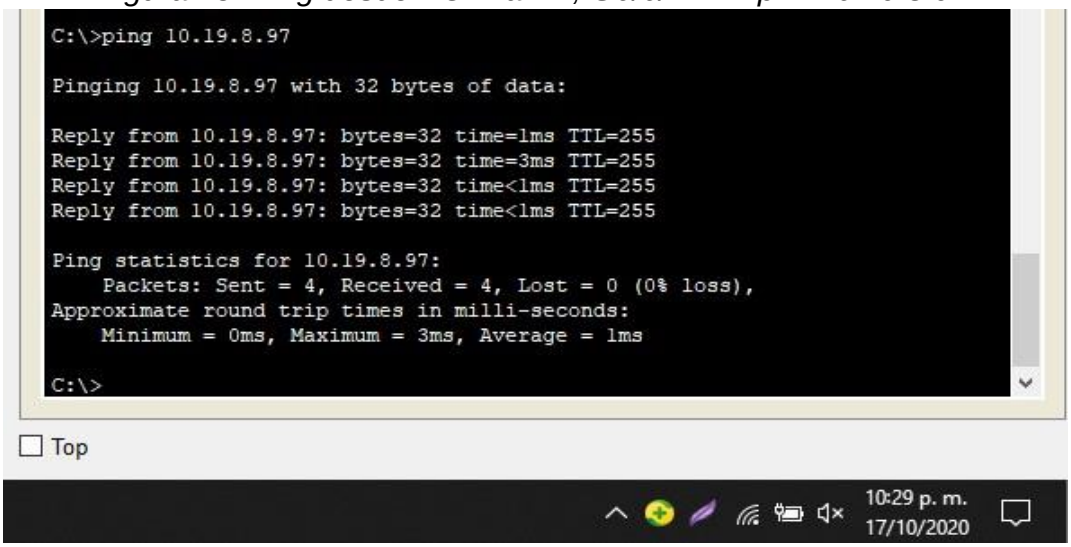
Figura 24. Ping desde PC-A a R1, G0/0/1.3 – Ipv6 2001:db8:acad:b::1



Fuente: Autor

Si fallan los pings en las computadoras host, si falla el ping, revisa el comando y vuelva a realizar la prueba.

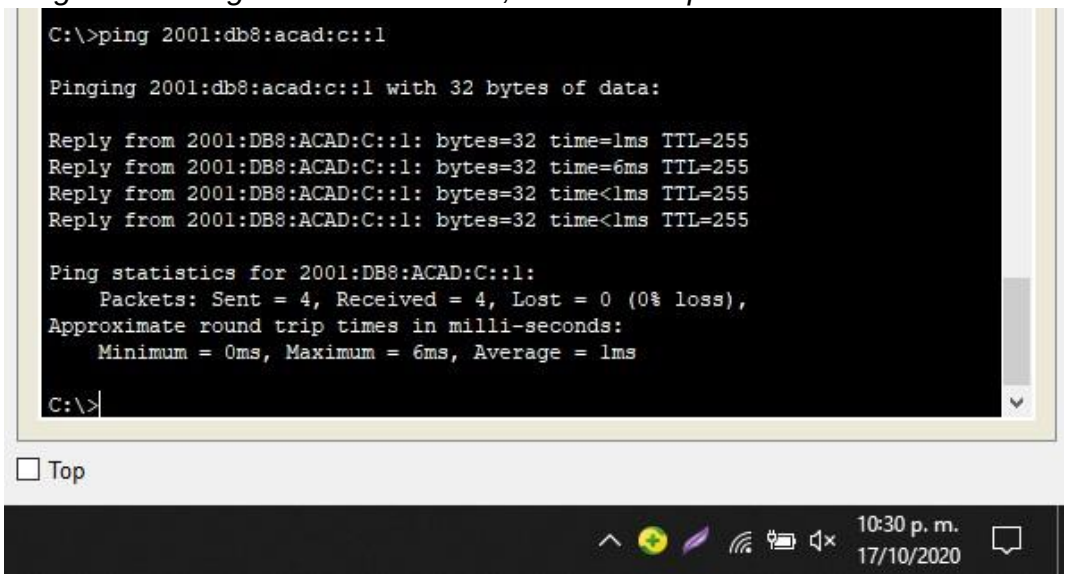
Figura 25. Ping desde PC-A a R1, G0/0/1.4 – Ipv4 10.19.8.97



Fuente: Autor

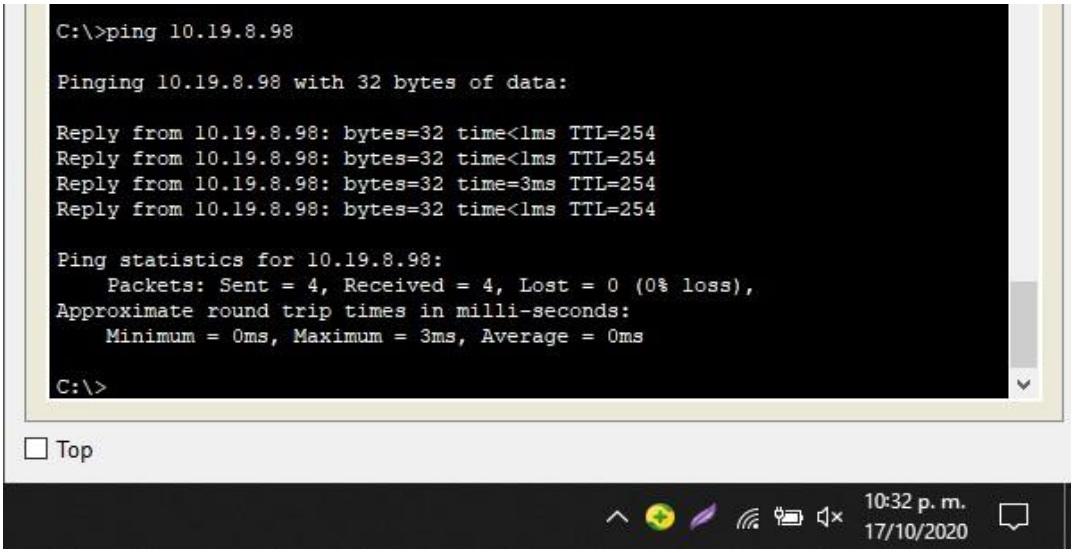
Se realiza pin desde la PC_A hacia R1, G0/0/1.4 enviando los paquetes a su dirección IPv4 utilizando el comando ping 10.19.8.97 logrando realizar el pin con éxito del mismo modo se realiza pin desde la PC_A hacia R1.

Figura 26. Ping desde PC-A a R1, G0/0/1.4 – Ipv6 2001:db8:acad:c::1



Fuente: Autor

Figura 27. Ping desde PC-A a S1 VLAN4 – Ipv4 10.19.8.98

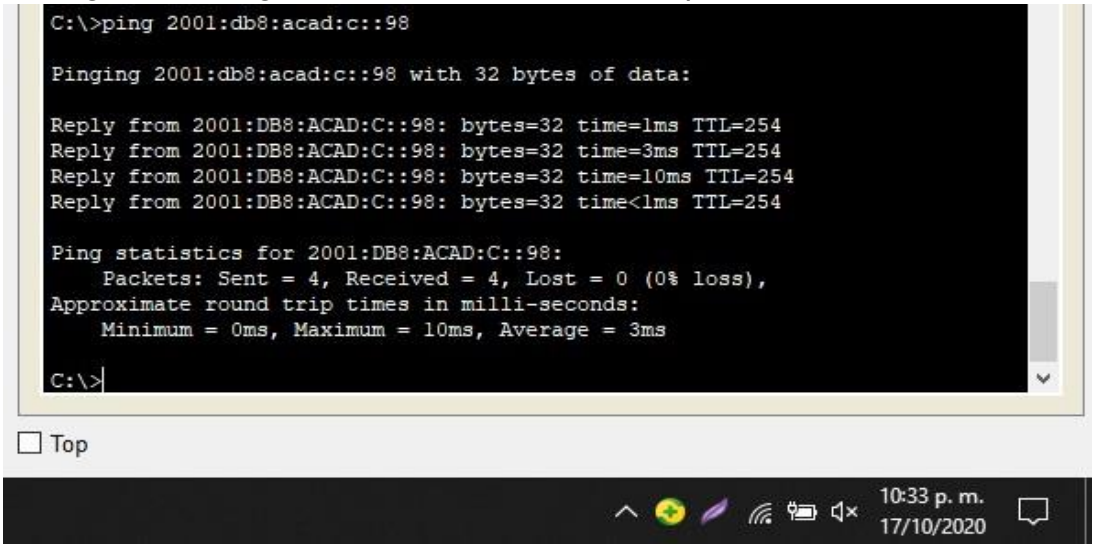


Fuente: Autor

Se realiza pin desde la PC_A hacia S1, VLAN 4 enviando los paquetes a su dirección IPv4 utilizando el comando ping 10.19.8.98 logrando realizar el pin conéxito del mismo modo se realiza pin desde la PC_A hacia S1. Si fallan los pings

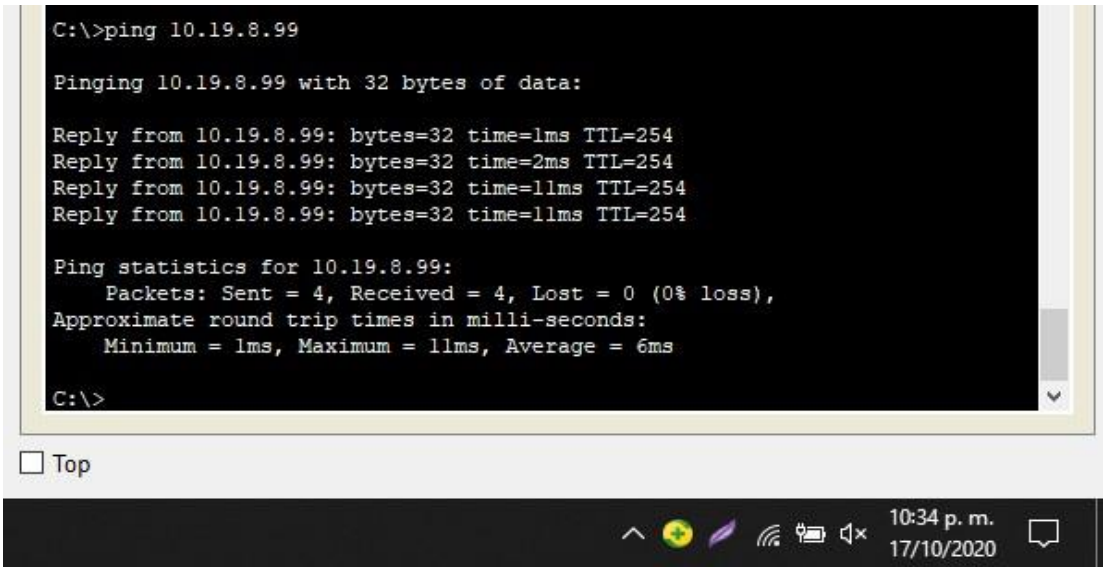
en las computadoras host, recomiendo que, revisa el comando y vuelva a realizar la prueba.

Figura 28. Ping desde PC-A a S1 VLAN4 – Ipv6 2001:db8:acad:c::98



Fuente: Autor

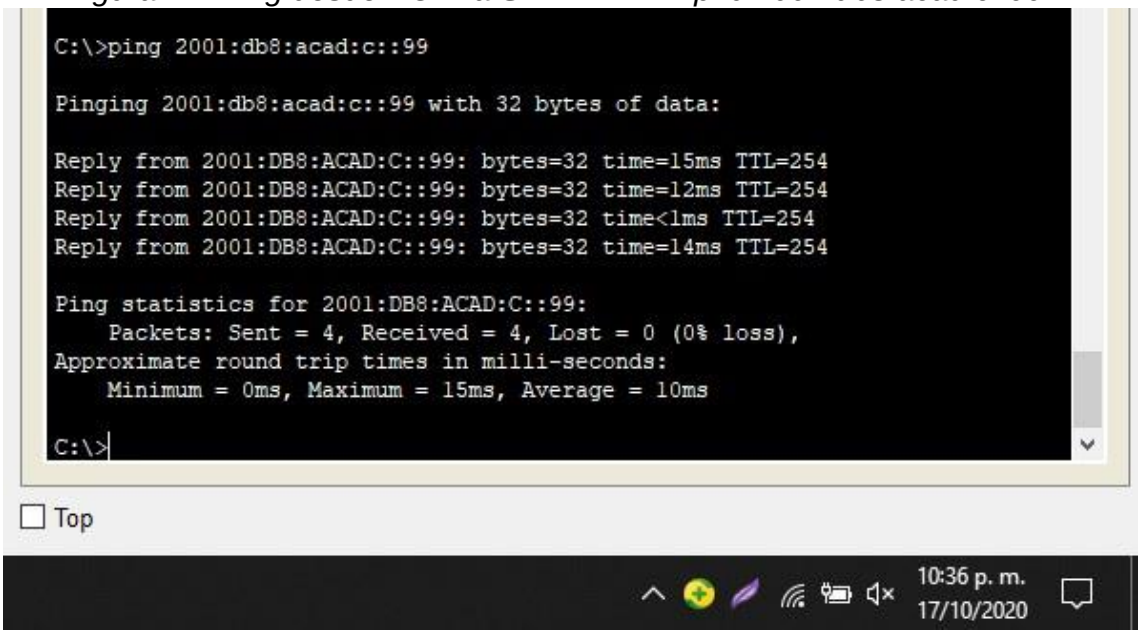
Figura 13. Ping desde PC-A a S2 VLAN4 – Ipv4 10.19.8.99



Fuente: Autor

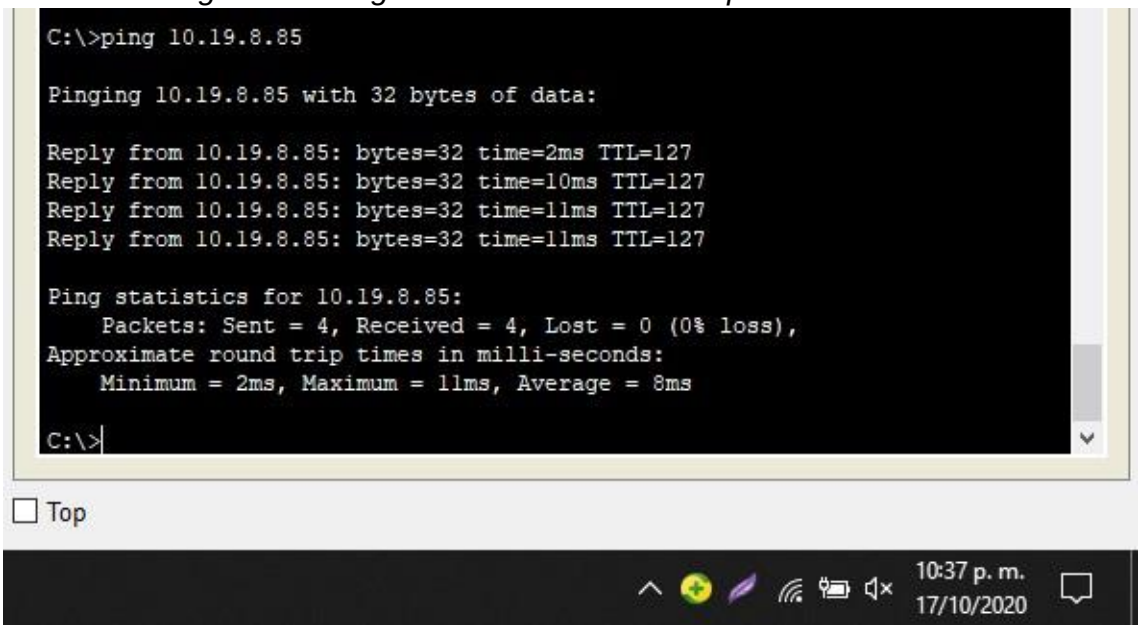
Hacemos pin desde la PC_A hacia S2, VLAN 4 enviando los paquetes a su dirección IPv4 utilizando el comando ping 10.19.8.99 logrando realizar el pin con éxito del mismo modo se realiza pin desde la PC_A hacia S2

Figura 14. Ping desde PC-A a S2 VLAN4 – Ipv6 2001:db8:acad:c::99



Fuente: Autor

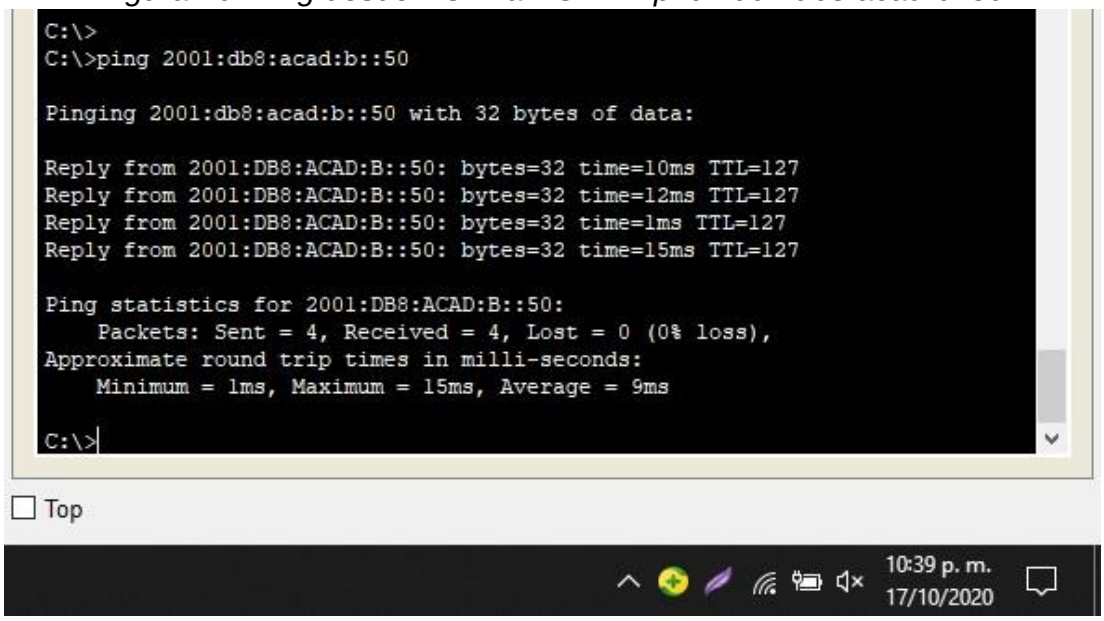
Figura 15. Ping desde PC-A a PC-B – Ipv4 10.19.8.85



Fuente: Autor

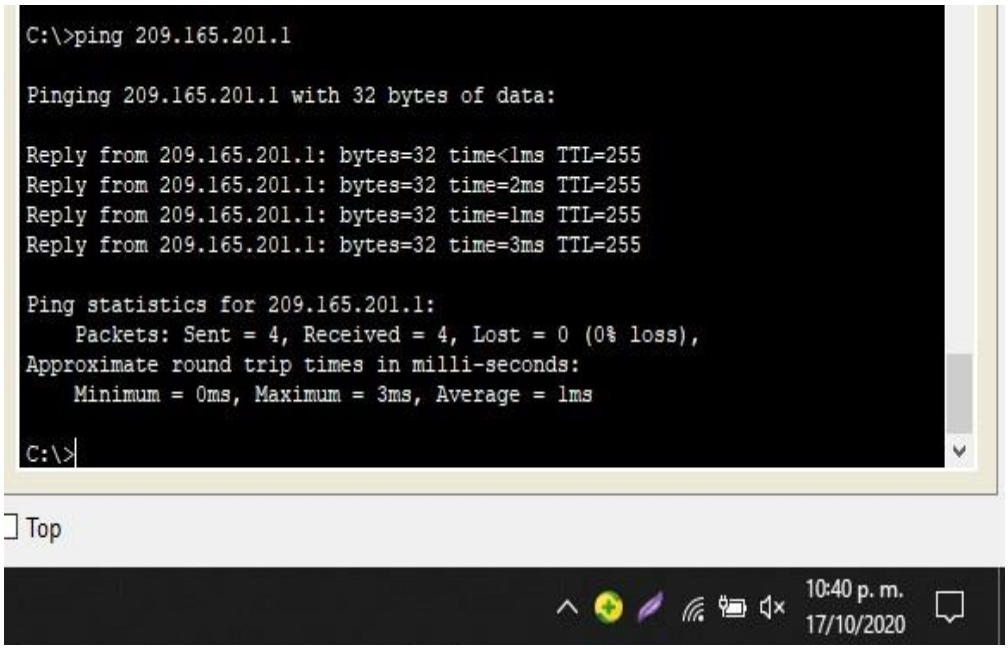
Realizo pin desde la PC_A hacia PC-B enviando los paquetes a su dirección IPv4 utilizando el comando ping 10.19.8.85 logrando realizar el pin con éxito del mismo modo se realiza pin desde la PC_A hacia PC-B.

Figura 16. Ping desde PC-A a PC-B – Ipv6 2001:db8:acad:b::50



Fuente: Autor

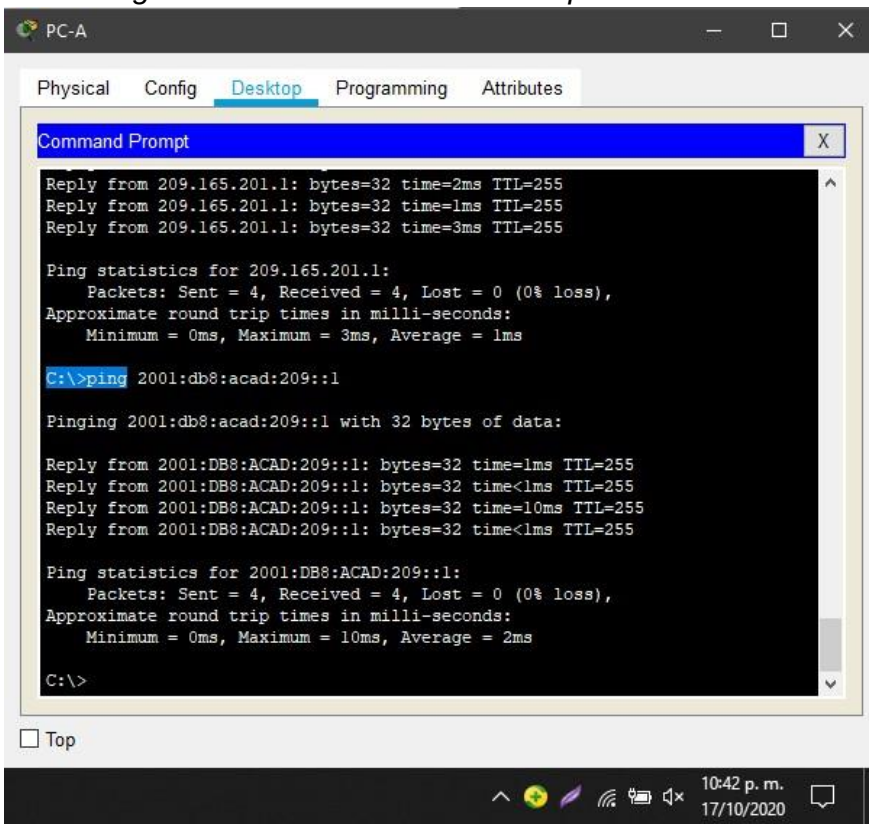
Figura 17. Ping desde PC-A a R1 Bucle 0 – IPv4 209.165.201.1



Fuente: Autor

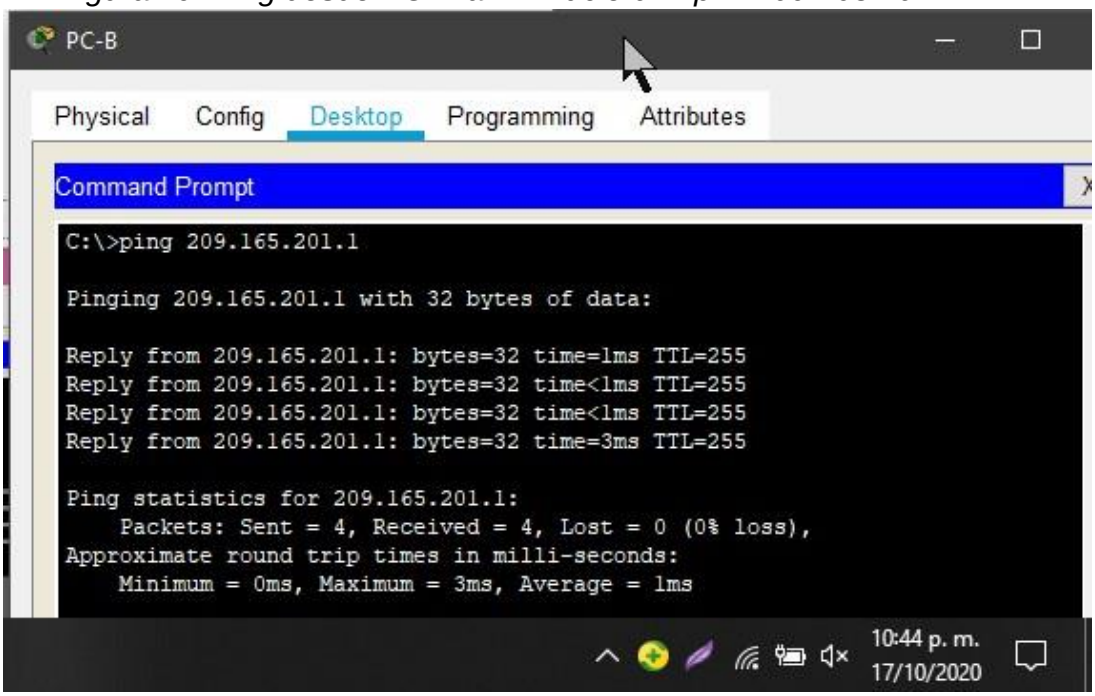
realizamos el pin con éxito del mismo modo se realiza pin desde la PC_A hacia R1, Bucle 0 enviando los paquetes a su dirección IPv6, también con éxito.

Figura 18. Ping desde PC-A a R1 Bucle 0 – Ipv6 2001:db8:acad:209::1



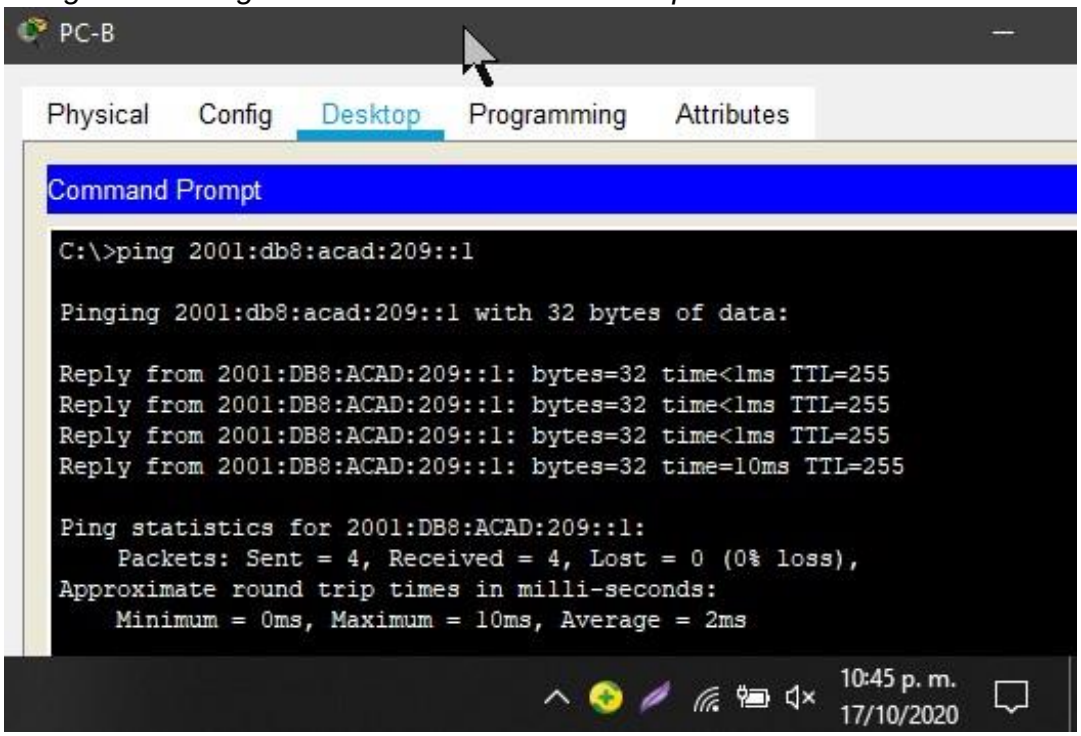
Fuente: Autor

Figura 19. Ping desde PC-B a R1 Bucle 0 – Ipv4 209.165.201.1



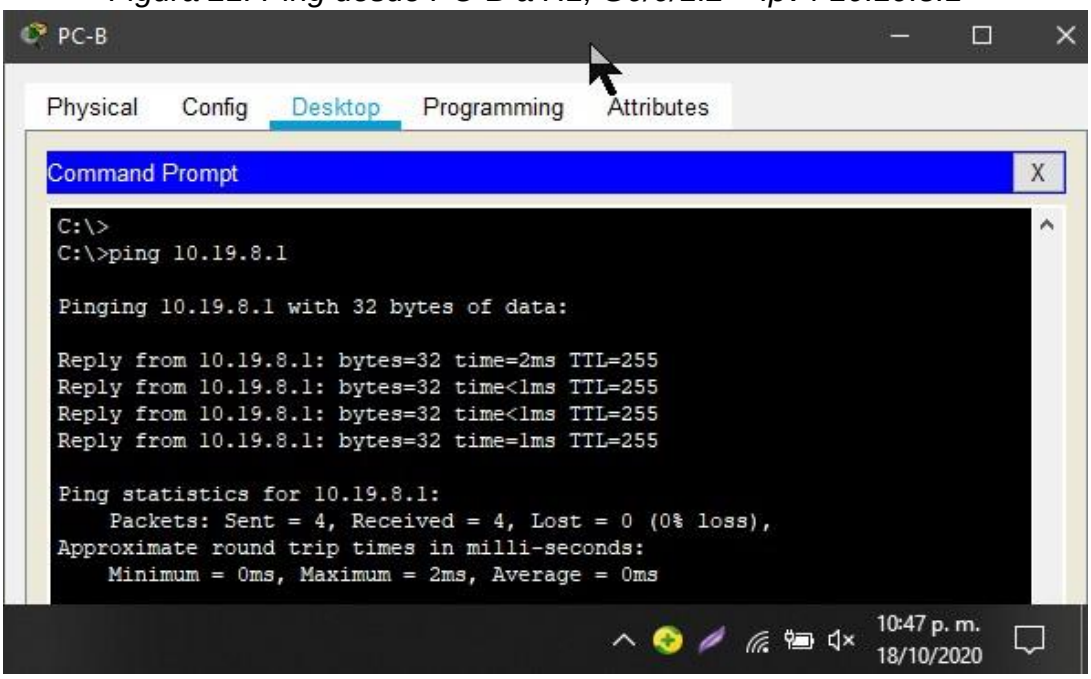
Fuente: Autor

Figura 20. Ping desde PC-B a R1 Bucle 0 – Ipv6 2001:db8:acad:209::1



Fuente: Autor

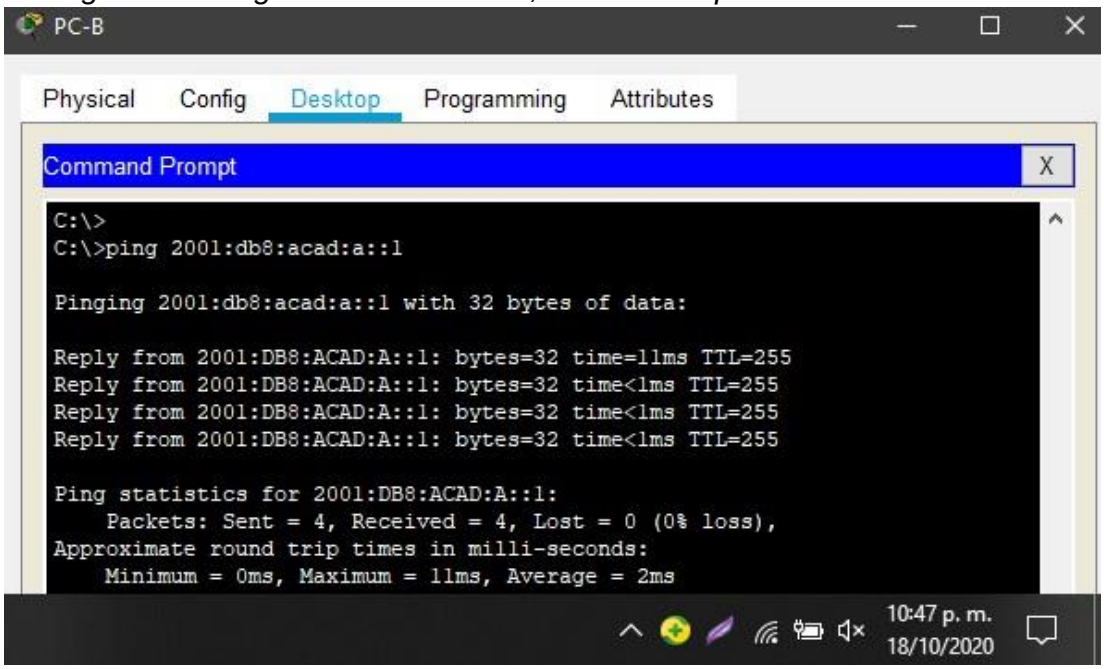
Figura 21. Ping desde PC-B a R1, G0/0/1.2 – Ipv4 10.19.8.1



Fuente: Autor

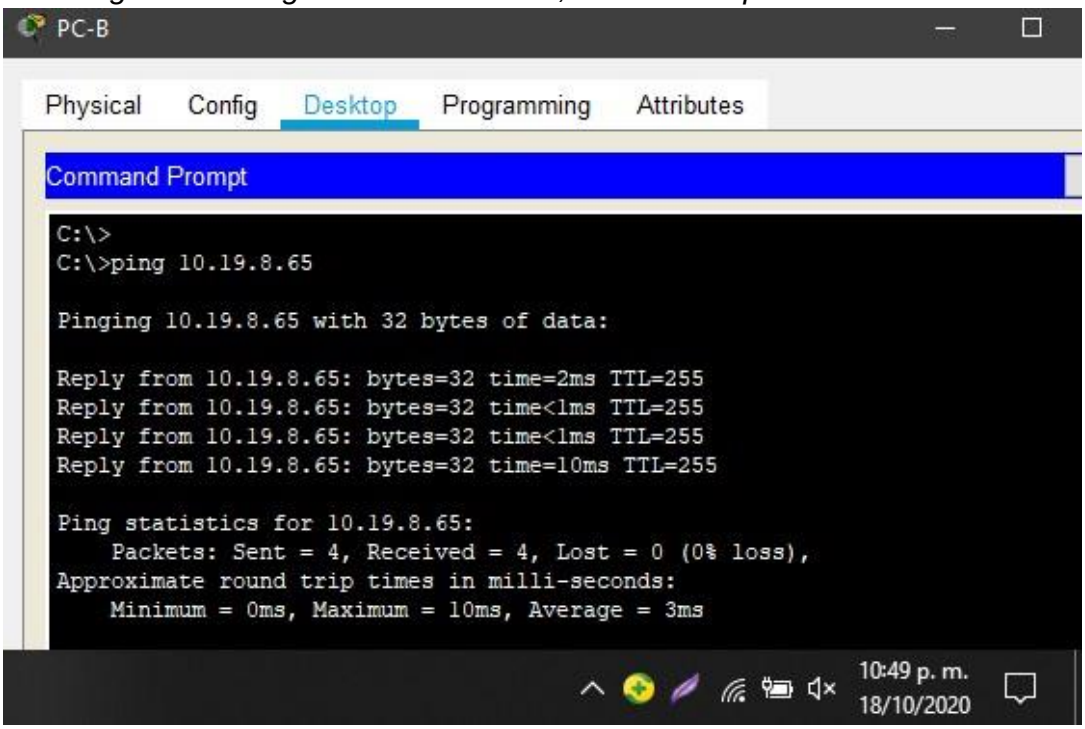
Se realiza pin desde la PC_B hacia R1, G0/0/1.2 enviando los paquetes a su dirección IPv4 utilizando el comando ping 10.19.8.1 logrando realizar el pin con éxito

Figura 22. Ping desde PC-B a R1, G0/0/1.2 – Ipv6 2001:db8:acad:a::1



Fuente: Autor

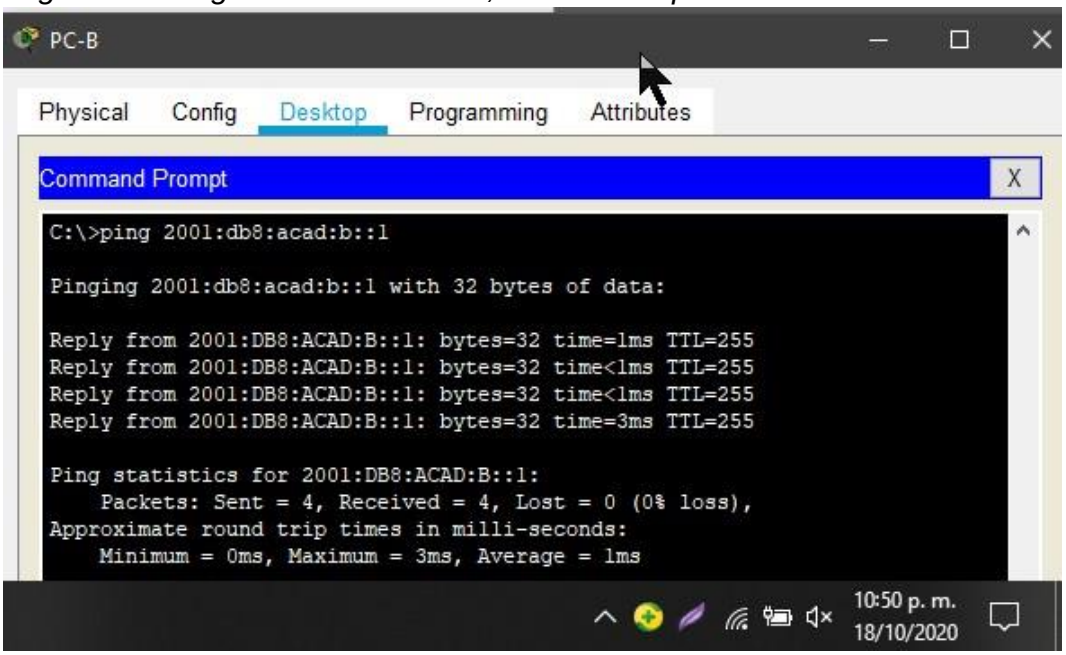
Figura 23. Ping desde PC-B a R1, G0/0/1.3 – Ipv4 10.19.8.65



Fuente: Autor

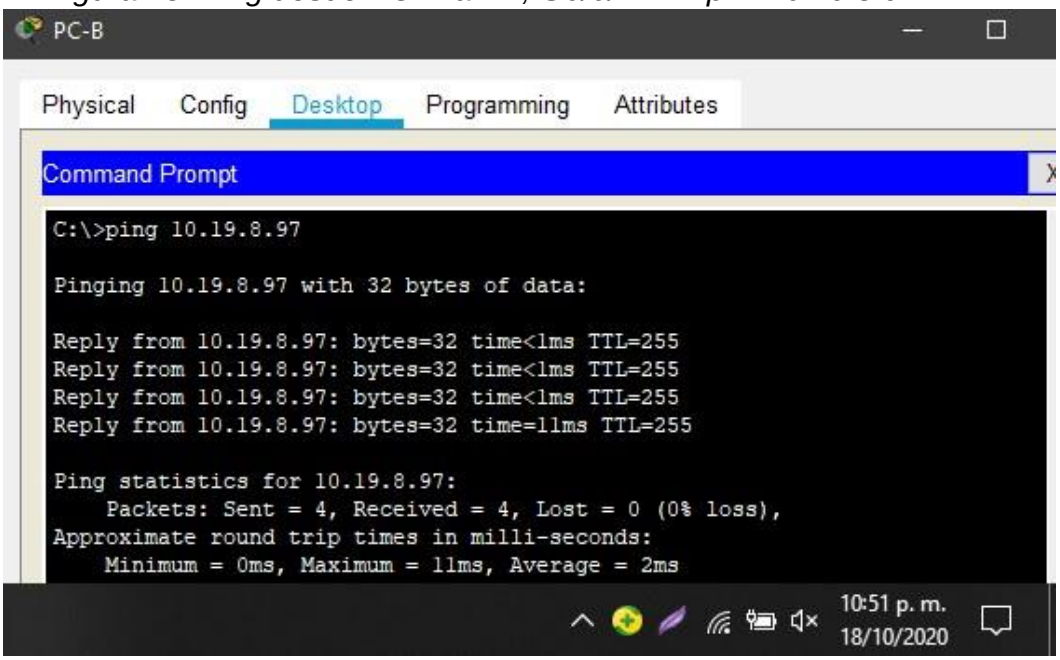
Se realiza pin desde la PC_B hacia R1, G0/0/1.3 enviando los paquetes a su dirección IPv6

Figura 24. Ping desde PC-B a R1, G0/0/1.3 – Ipv6 2001:db8:acad:b::1



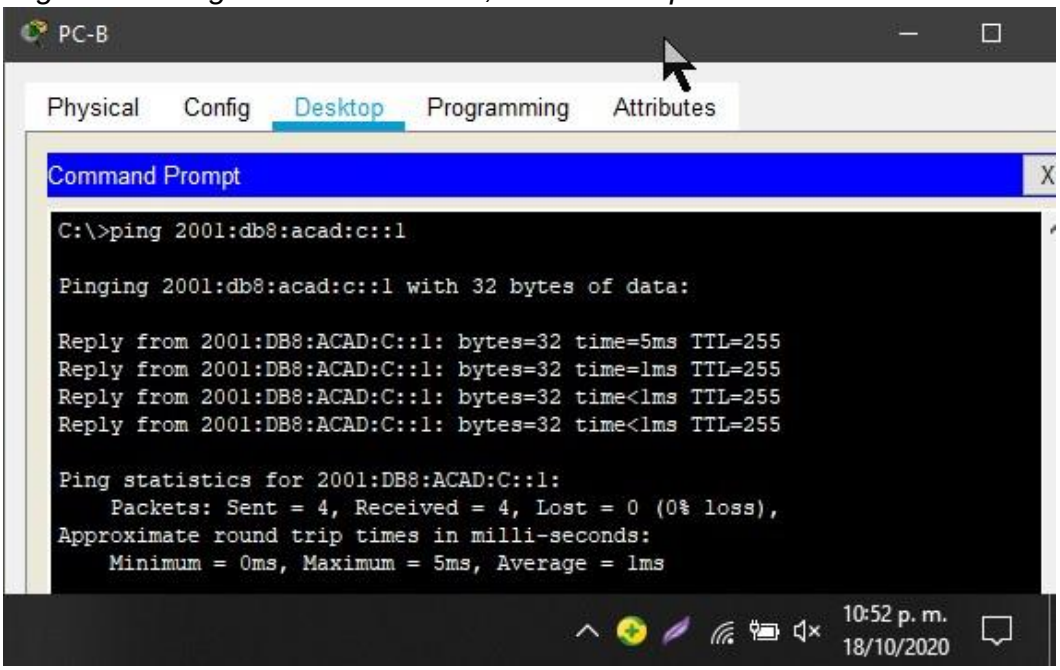
Fuente: Autor

Figura 25. Ping desde PC-B a R1, G0/0/1.4 – Ipv4 10.19.8.97



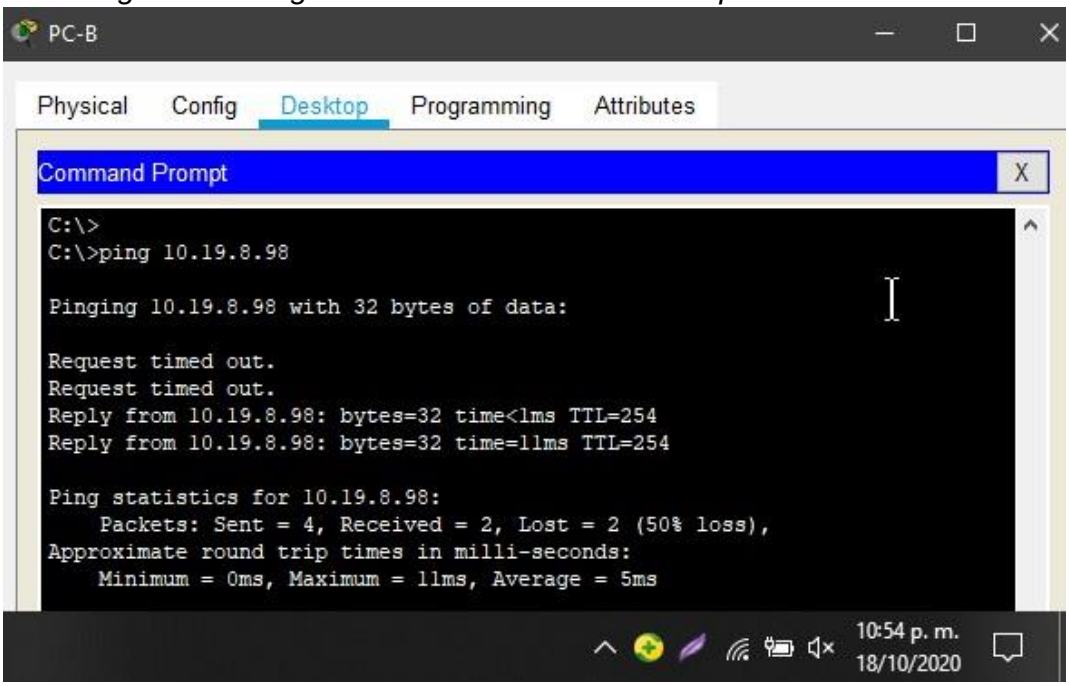
Fuente: Autor

Figura 26. Ping desde PC-B a R1, G0/0/1.4 – Ipv6 2001:db8:acad:c::1



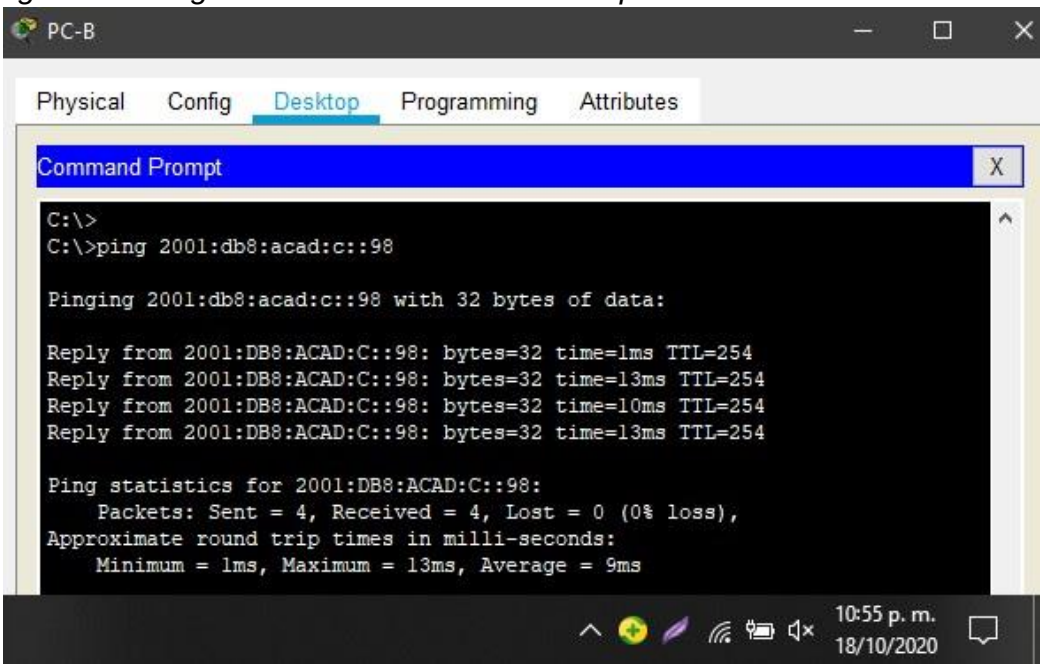
Fuente: Autor

Figura 27. Ping desde PC-B a S1 VLAN4 – Ipv4 10.19.8.98



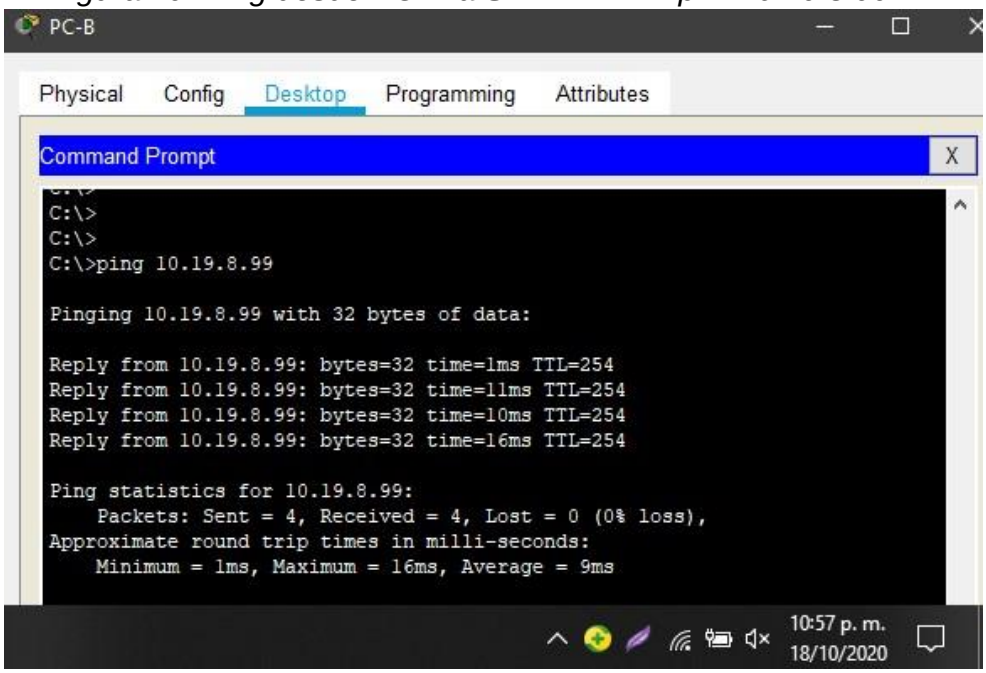
Fuente: Autor

Figura 28. Ping desde PC-B a S1 VLAN4 – Ipv6 2001:db8:acad:c::98



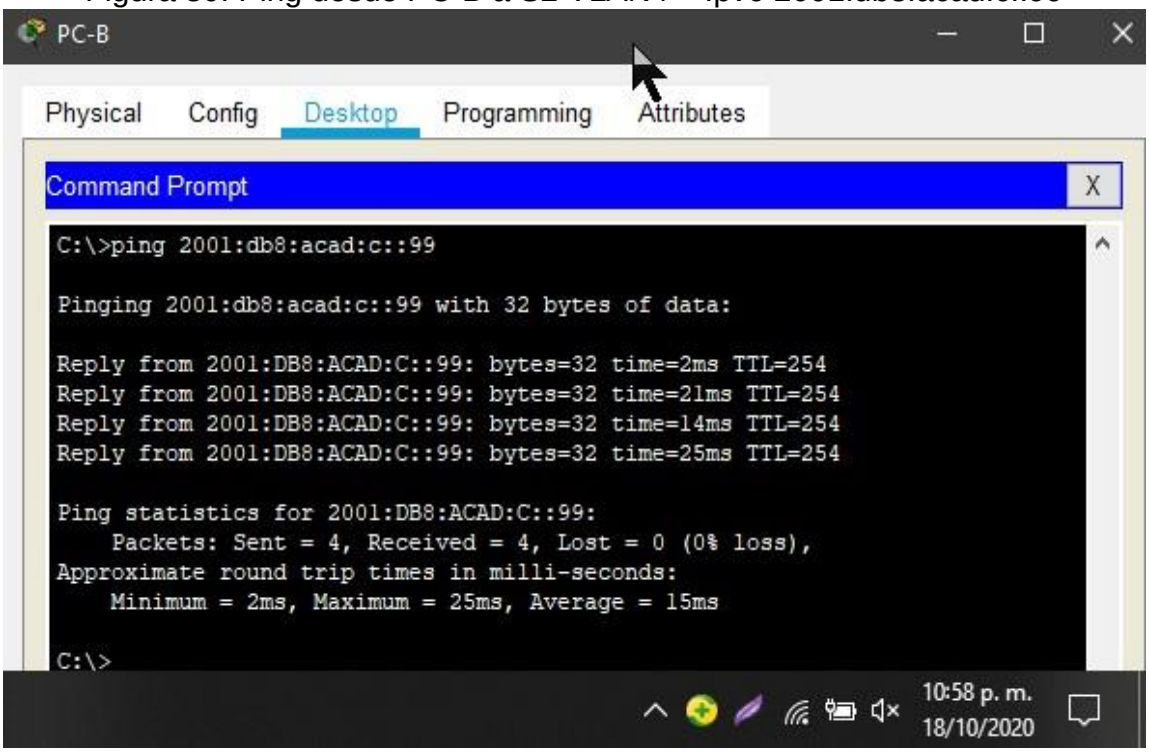
Fuente: Autor

Figura 29. Ping desde PC-B a S2 VLAN4 – Ipv4 10.19.8.99



Fuente: Autor

Figura 30. Ping desde PC-B a S2 VLAN4 – Ipv6 2001:db8:acad:c::99



Fuente: Autor

Se realiza pin desde la PC_B hacia S2, VLAN 4 enviando los paquetes a su dirección IPv6. Se realiza pin desde la PC_B hacia S2, VLAN 4 enviando los paquetes a su dirección IPv4 utilizando el comando ping 10.19.8.99

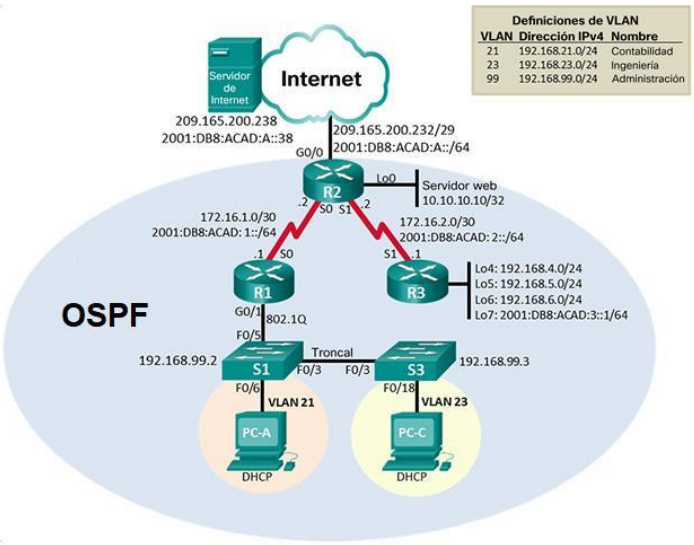
Nota: Ping es un comando o una herramienta de diagnóstico que permite hacer una verificación del estado de una determinada conexión o host local.

Ping es un comando o una herramienta de diagnóstico que permite hacer una verificación del estado de una determinada conexión de un host local con al menos un equipo remoto contemplado en una red de tipo TCP/IP.

Sirve para determinar si una dirección IP específica o host es accesible desde la red o no.

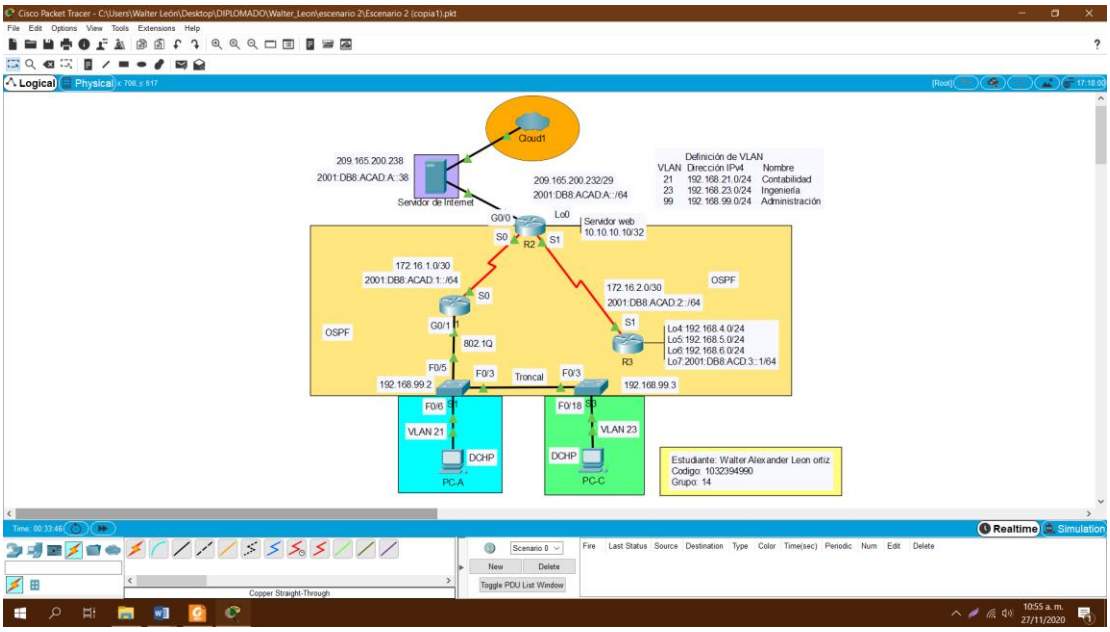
- **Escenario 2**

Figura 31. Topología de red del escenario 2



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

Figura 32. Simulación Escenario 2 en Packet Tracer



Fuente: *Autor*

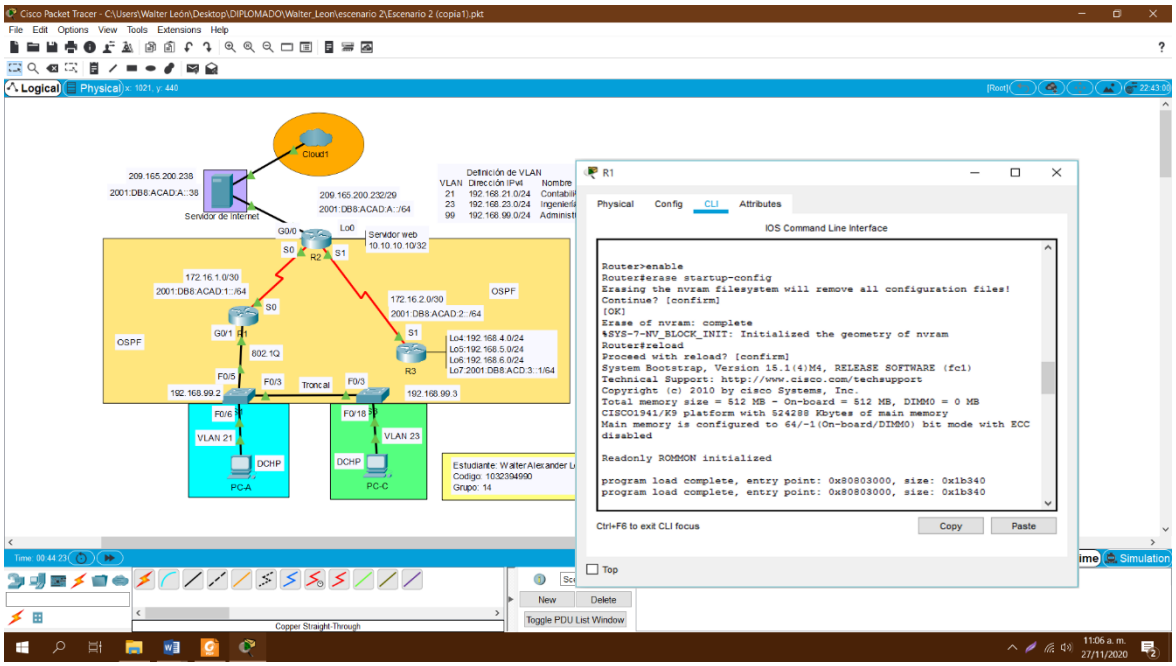
Parte 1: Inicializar dispositivos

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

✓ Elimine las configuraciones de inicio de los Routers y vuelva a cargarlos.

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 33. Eliminación configuración inicial y cargue de los Routers

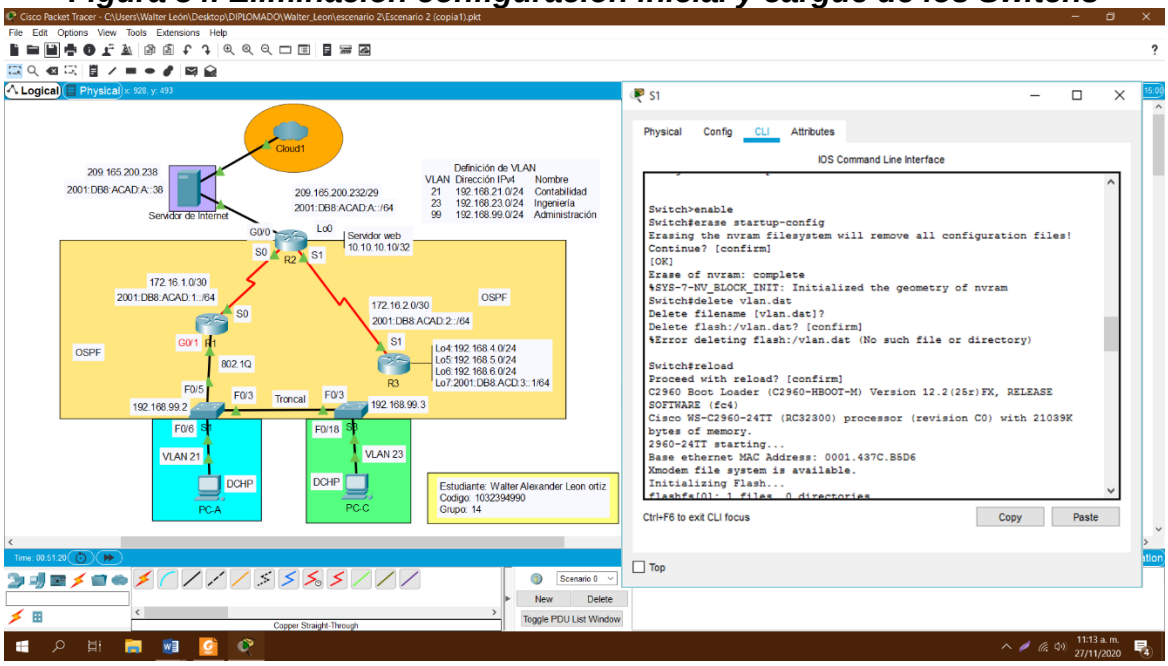


Fuente: Autor

✓ Elimine las configuraciones de inicio de los Switchs y vuelva a cargarlos.

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 34. Eliminación configuración inicial y cargue de los Switchs



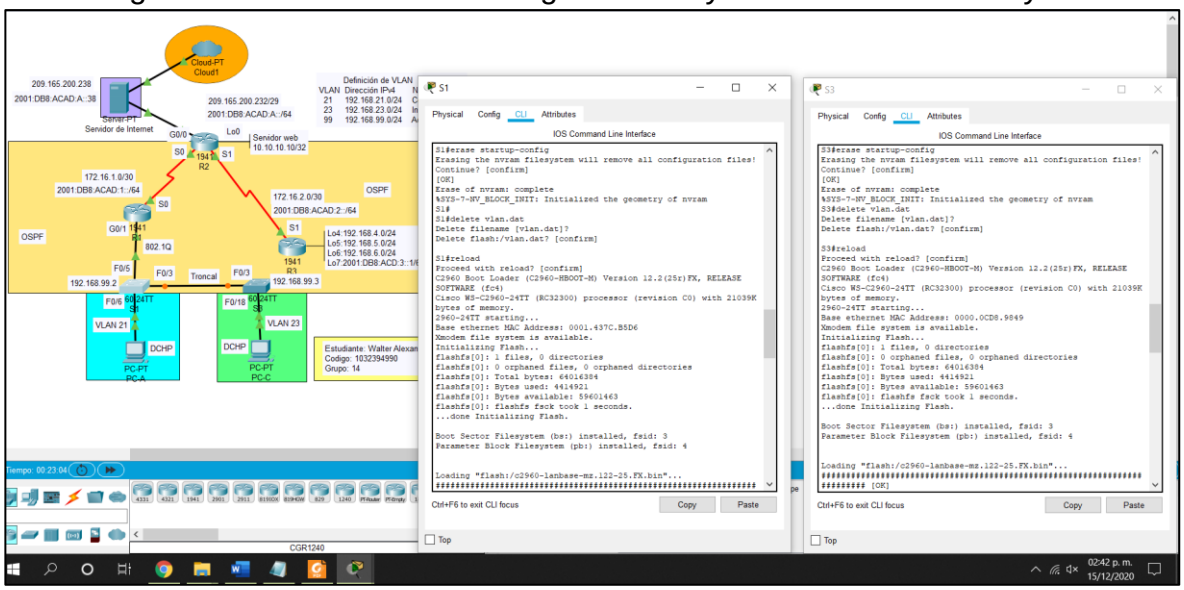
Fuente: Autor

Aquí es donde vamos a solicitar al docente que, si podemos continuar con la inicialización de los router o switchs.

Tabla 16. Inicializar y volver a cargar los routers y los switches

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

Figura 35. Eliminación de configuraciónes y reinicio del Router 2 y 3



Fuente: Autor

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1. Configurar la computadora de Internet

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

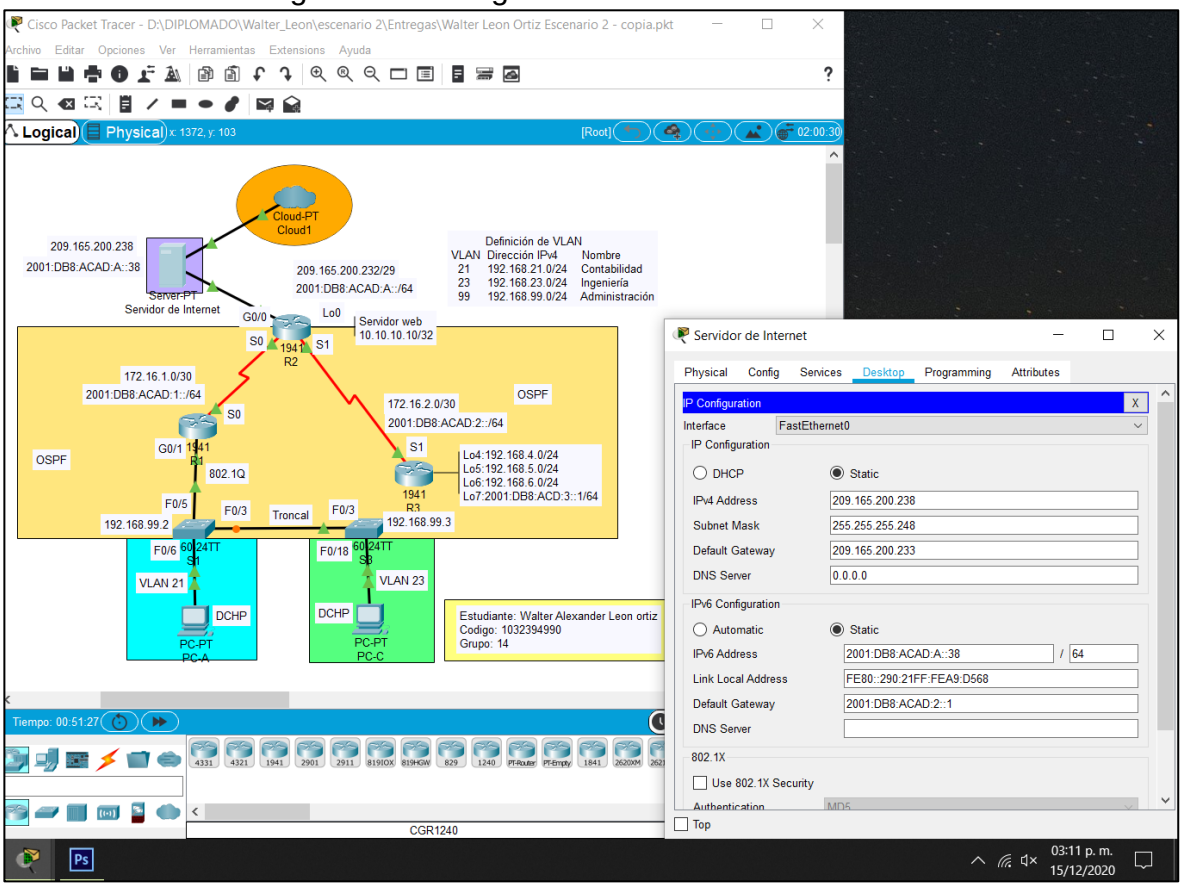
Tabla 17. Configuración Servidor de Internet.

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.

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

Figura 36. Configuración Servidor de Internet



Fuente: Autor

Paso 2. Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18. 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 password-encryption
Mensaje MOTD, Se prohíbe el acceso no autorizado.	R1(config)#banner motd "Se prohibe el acceso no autorizado"
Interfaz S0/0/0 Establezca la descripción Establecer la dirección IPv4 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

Bueno, aquí es donde empieza a crear las piezas de este escenario dos, vamos a ejecutar la configuración inicial en Router 1, entonces entro a la consola modo privilegiado →luego: ejecutar el comando ***no ip domain lookup*** esto me ayuda a desactivar la búsqueda DNS, me ayuda a descartar si hemos cometido un error en el scrip si eso es cierto, entonces, que muestre un aviso indicando el error.

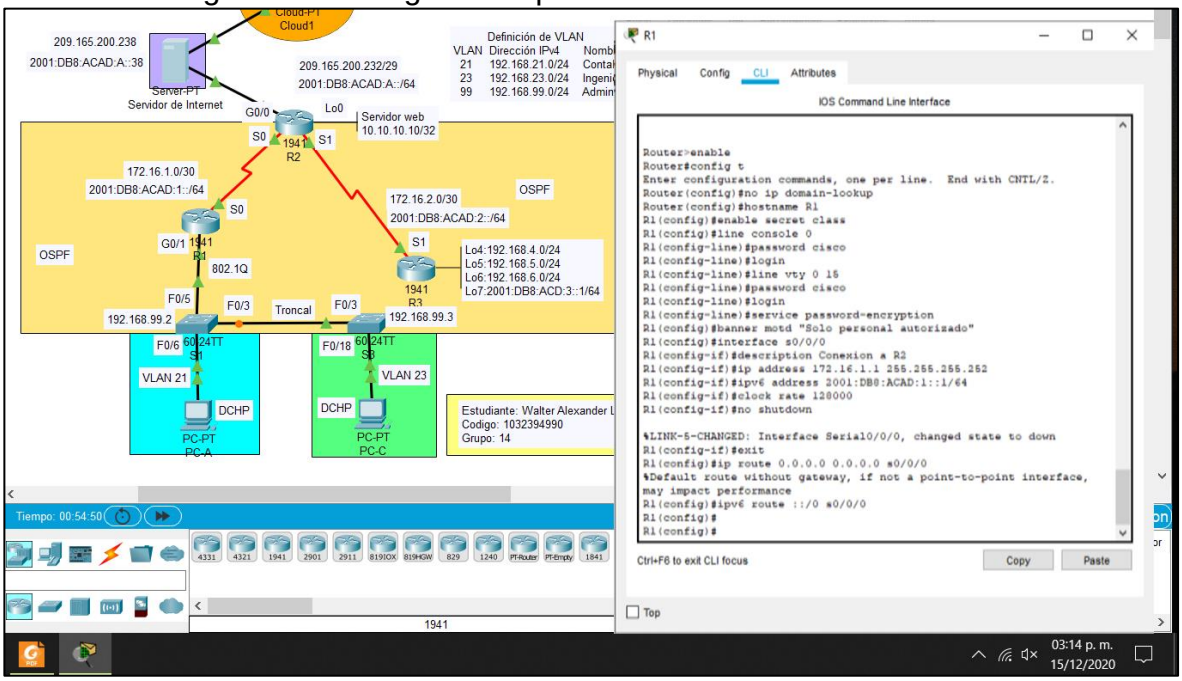
Procedo a configurar el nombre del dispositivo junto con la contraseña cifrada. Ingreso al modo privilegiado a través del comando **enable secret,** de igual manera se configura la contraseña para ingresar a la consola, y para ingresar a la consola es con el comando **password** y se activa con el comando **login,** se configuran el modo de línea de terminal virtual **vty 0 15** (Telnet) asignándole una contraseña

para el acceso. Entonces, para aumentar seguridad, se adiciona el comando **service password-encryption** que ayuda a cifrar las contraseñas de texto no cifrado. Por último, insertaremos 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 37. Configuracion parámetros básicos en Router 1



Fuente: Autor

Paso 3. Configurar R2

La configuración del R2 incluye las siguientes tareas:

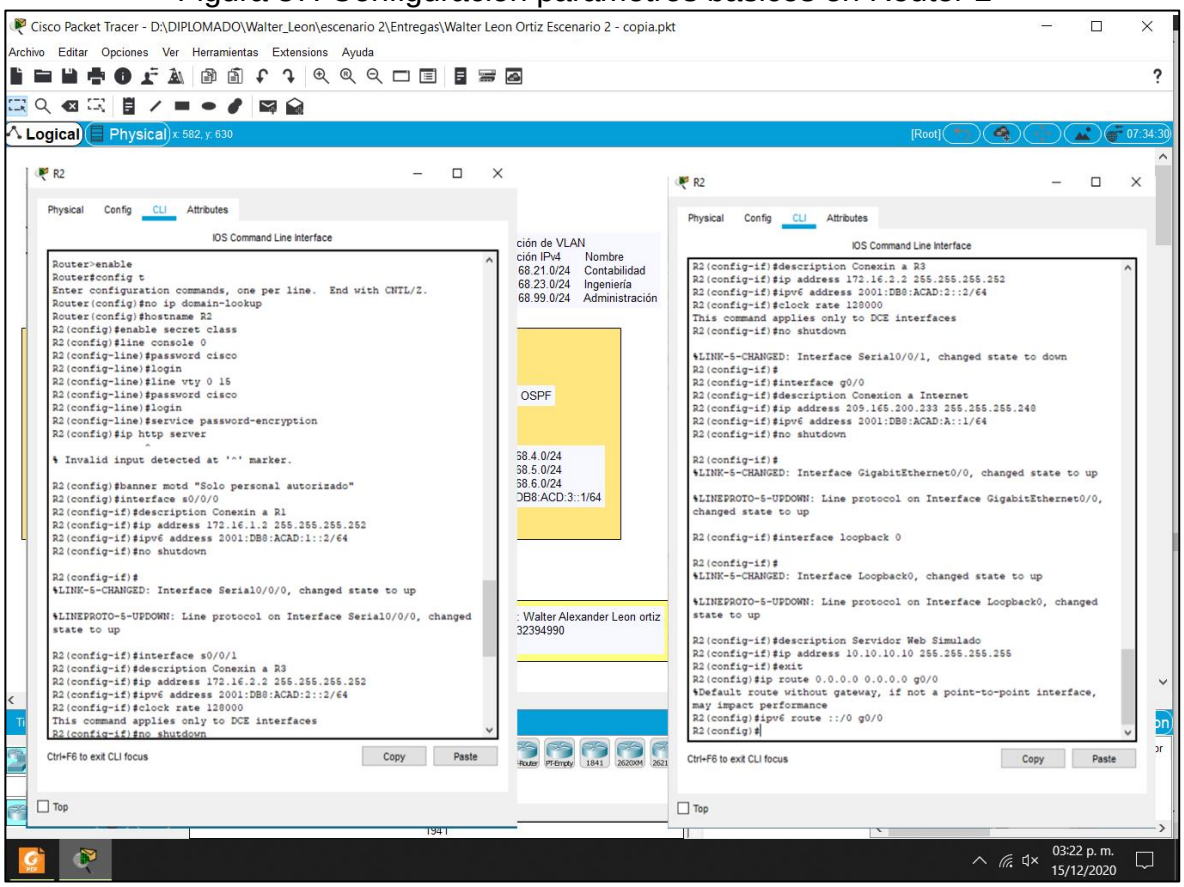
Tabla 19. Configuración Router 2 y 3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router, 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 password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server
Mensaje MOTD, Se prohíbe el acceso no autorizado.	R2(config)#banner motd " Se prohíbe el acceso no 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

Figura 37. Configuracion parámetros básicos en Router 2



Fuente: Autor

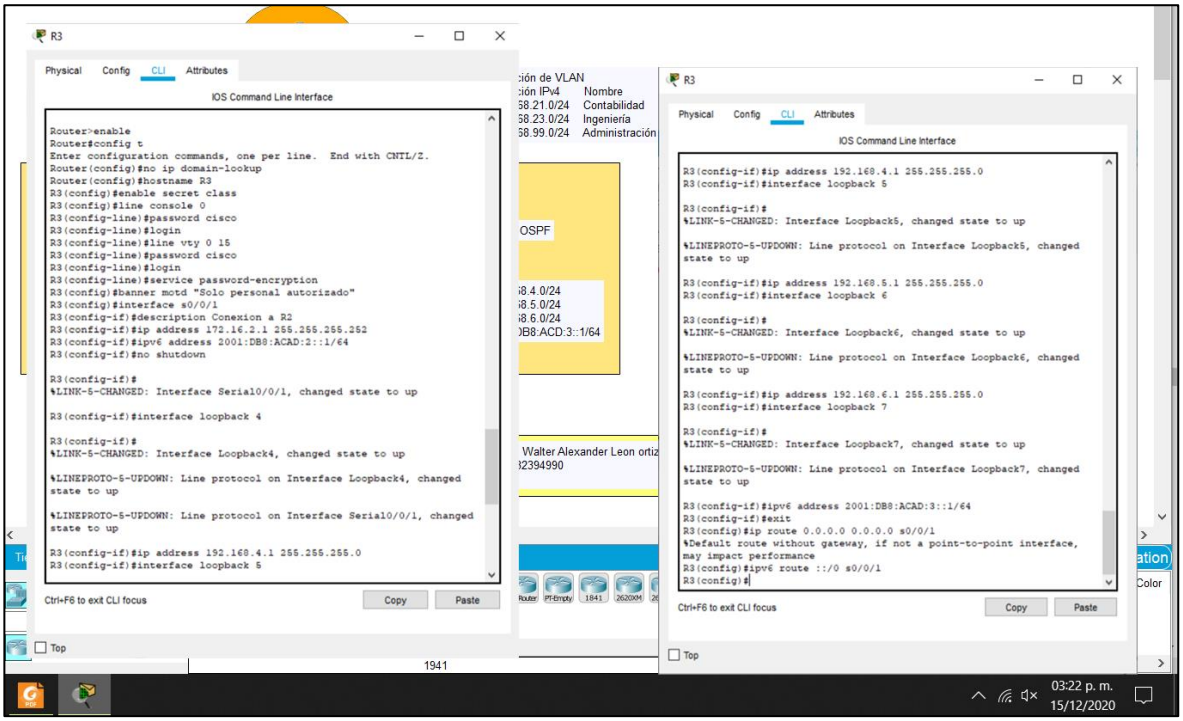
Paso 4. Se realiza configuración inicial del Router 2 y el mismo caso para R3.

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.

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.

Figura 37. Configuracion parámetros básicos en Router 3



Fuente: Autor

Recordemos que este paso es igual para el R2 y R3:
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.

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 20. 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 password-encryption
Mensaje MOTD, Se prohíbe el acceso no autorizado.	S1(config)#banner motd " Se prohíbe el acceso no 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 esta 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 por ultimo, debemos adicionar el mensaje del día para usuarios no autorizados en el motd. Esto con el fin de aumentar seguridad en el switch 1.
Nota: password-encryption, sirve para cifrar las contraseñas de texto no cifrado y se debe adicionar el mensaje del día para usuarios no autorizados en el motd.

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

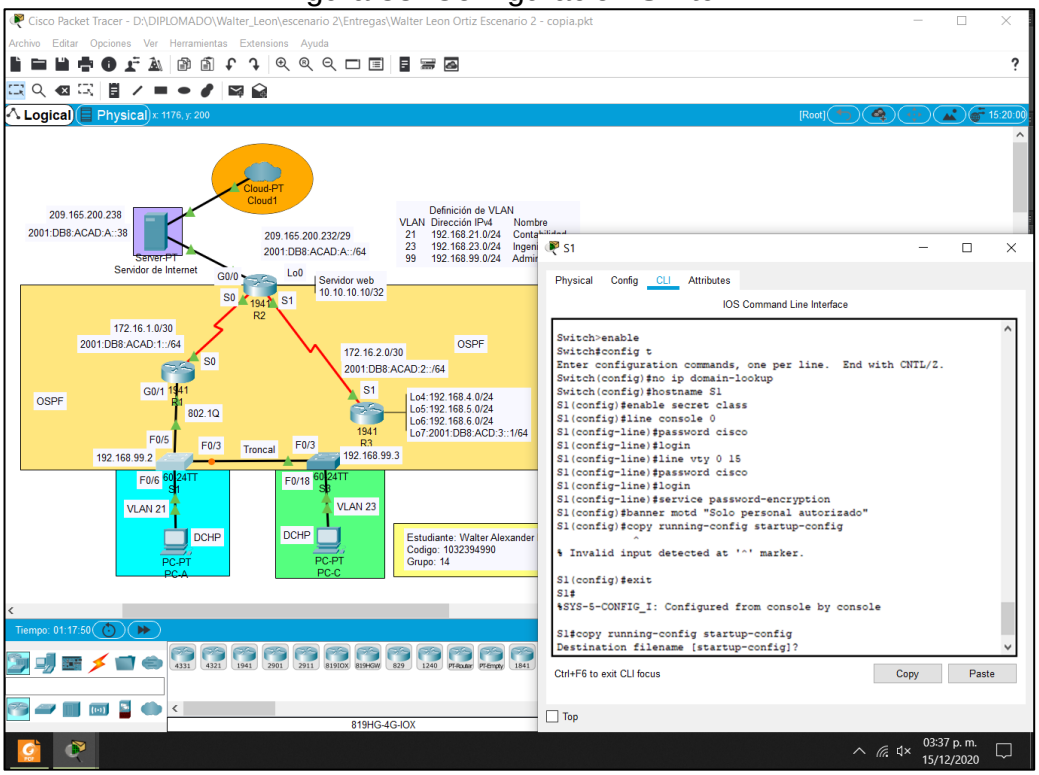
Tabla 21. Configuración Switch 3

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 " Se prohíbe el acceso no 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.

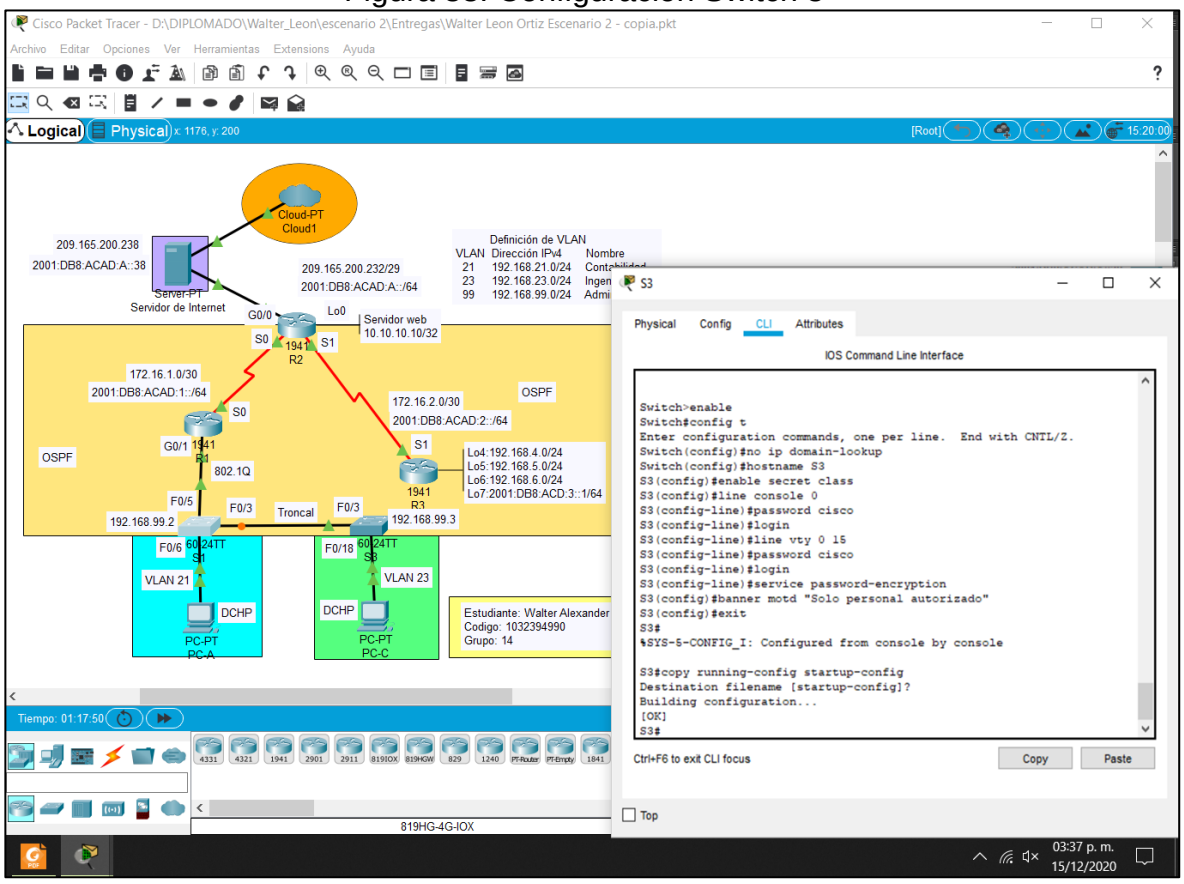
Figura 38. Configuracion Switch 1



Fuente: Autor

Por lo tanto, se configura el modo de línea de terminal virtual vty 0 15 (Telnet) asignándole una contraseña para el acceso,

Figura 38. Configuracion Switch 3



Fuente: Autor

Paso 7: Verificar la conectividad de la red

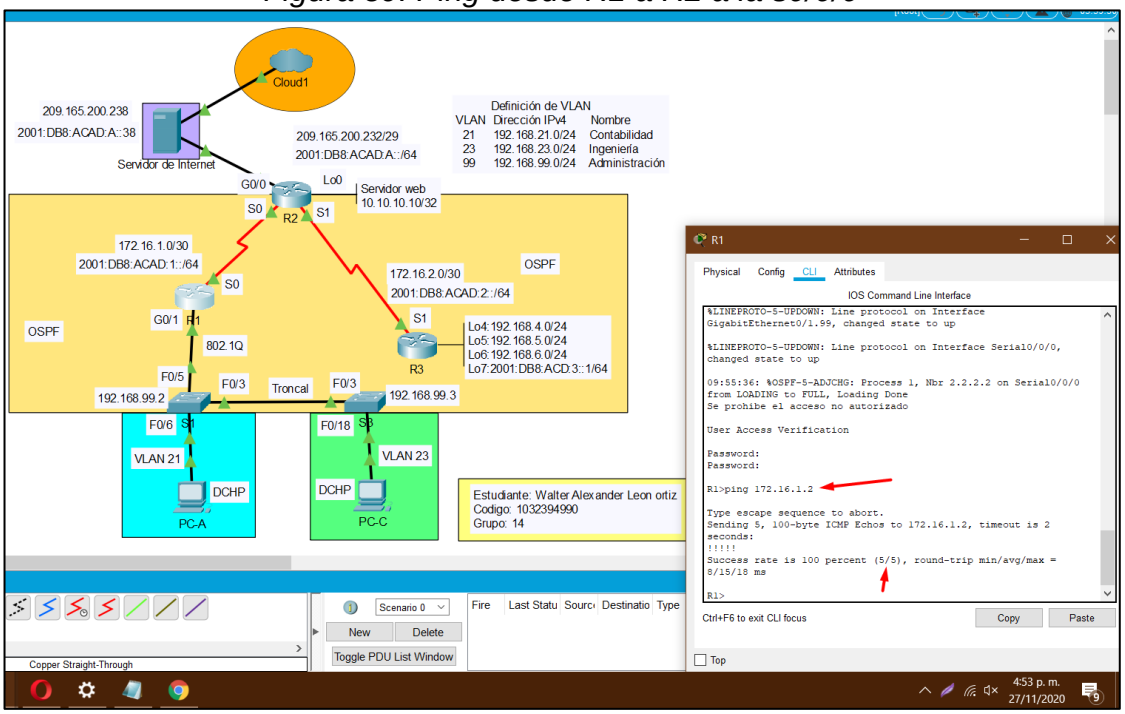
Utilice el comando ping para probar la conectividad entre los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 22. 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

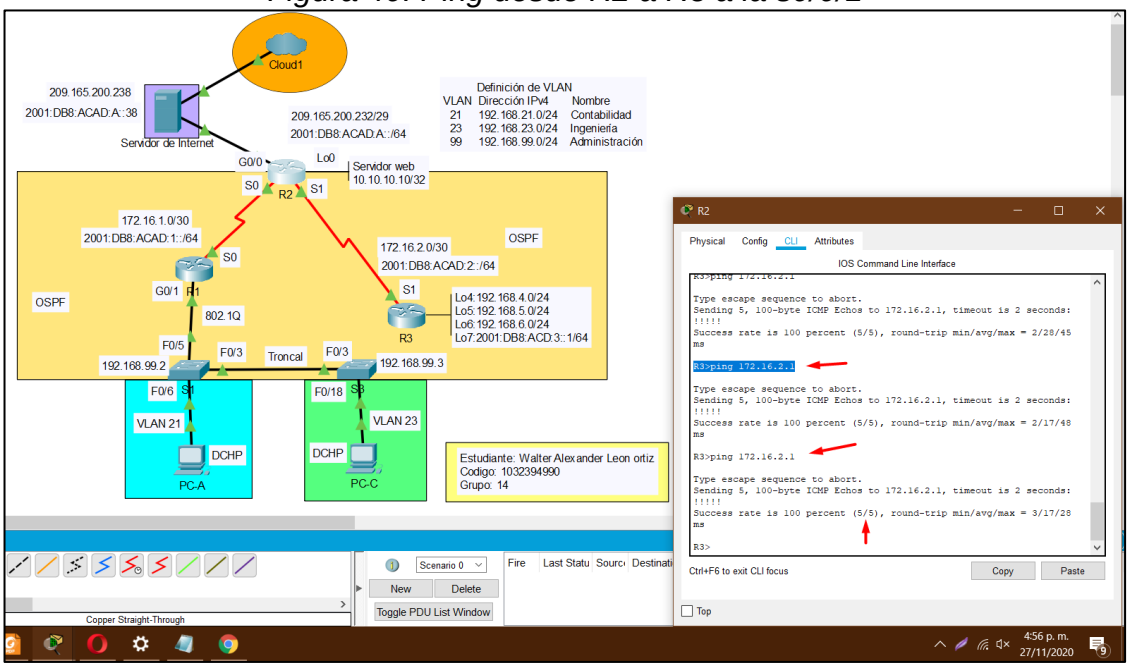
Se realizan pruebas de conexión para verificar el correcto funcionamiento de la red, ejecutando el comando ping entre routers y desde el pc de internet a la puerta de enlace prederminada.
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Figura 39. Ping desde R1 a R2 a la s0/0/0



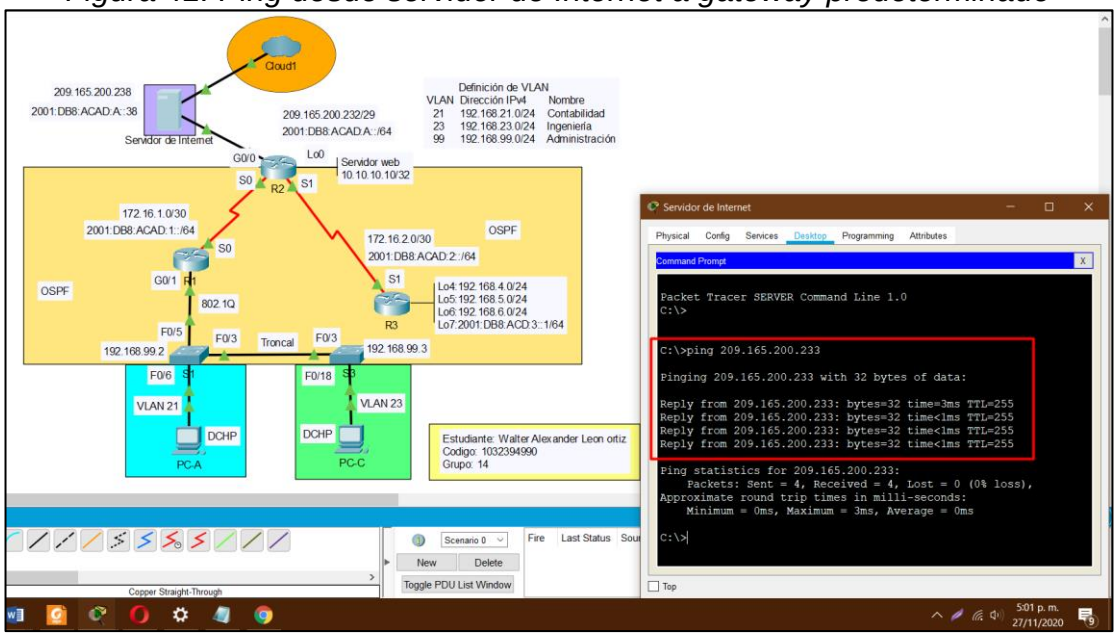
Fuente: Autor

Figura 40. Ping desde R2 a R3 a la s0/0/1



Fuente: Autor

Figura 41. Ping desde servidor de Internet a gateway predeterminado



Fuente: Autor

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

Paso 1. Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 23. 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 42. Configuración seguridad del switch 1, las VLAN y el routing entre VLAN.

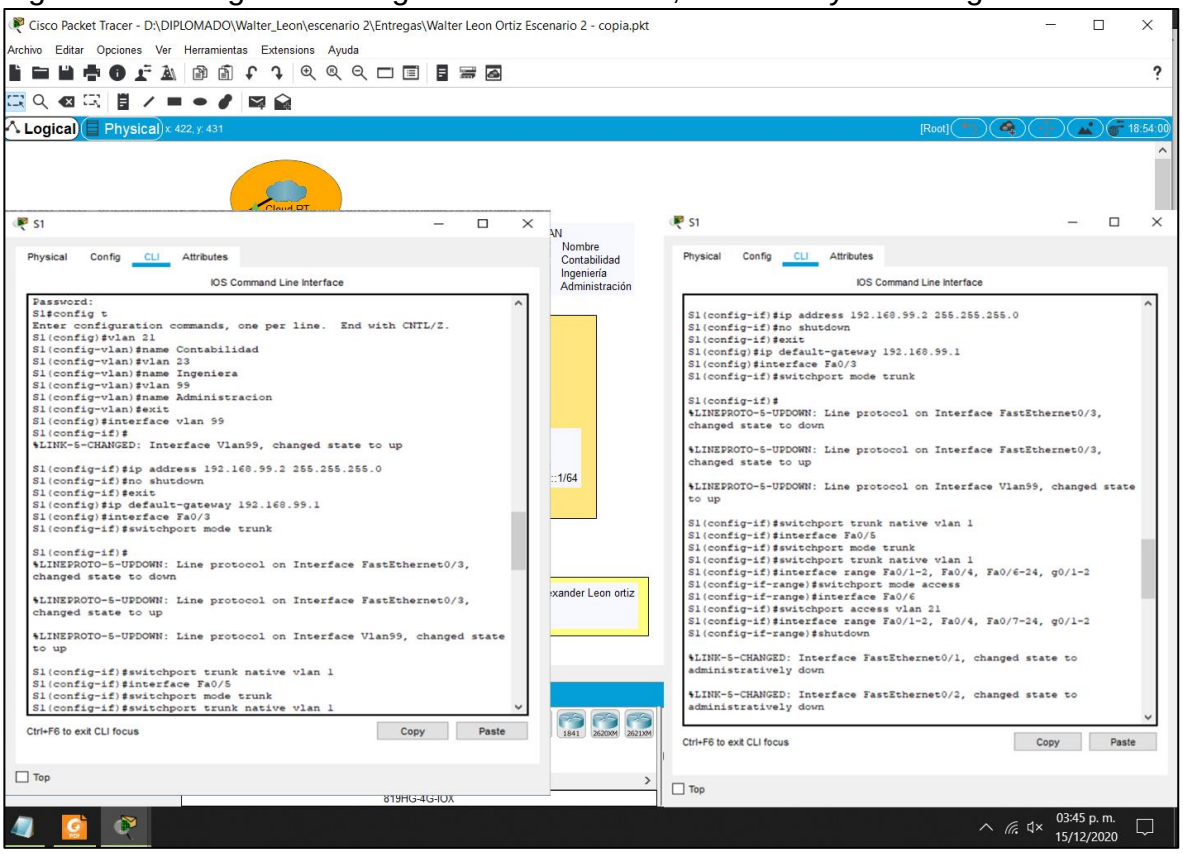
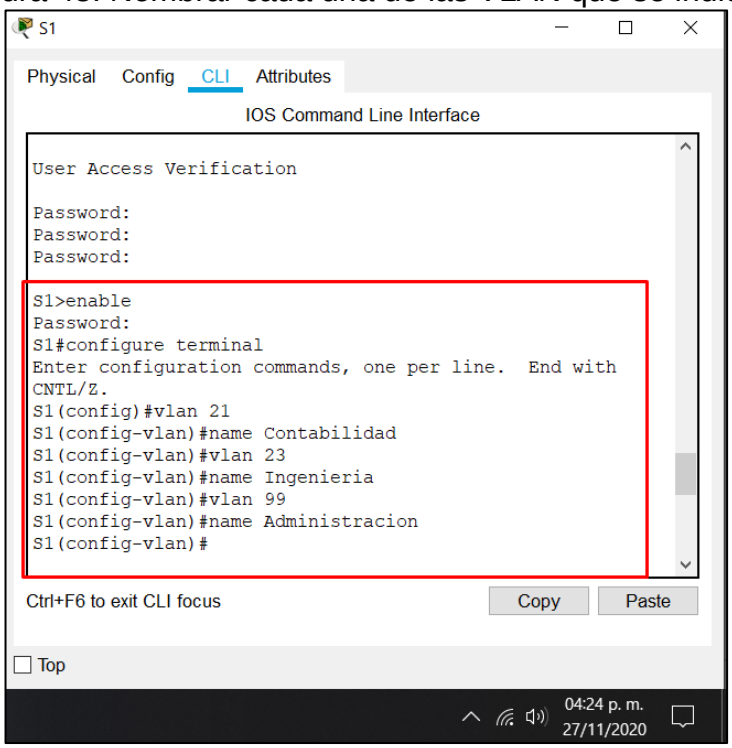


Figura 43: Nombrar cada una de las VLAN que se indican



Fuente: Autor

En esta figura 7, observamos que se introduce las contraseñas de privilegios para poder crear nombres a las vlan 21, como contabilidad, vlan 23, como Ingenieria, aunque la vlan 99 se llama Administracion, podemos colocar cualquier número de vlan, pero eso si respetando los objetivos de la practica.

Paso 2: Configurar el S3

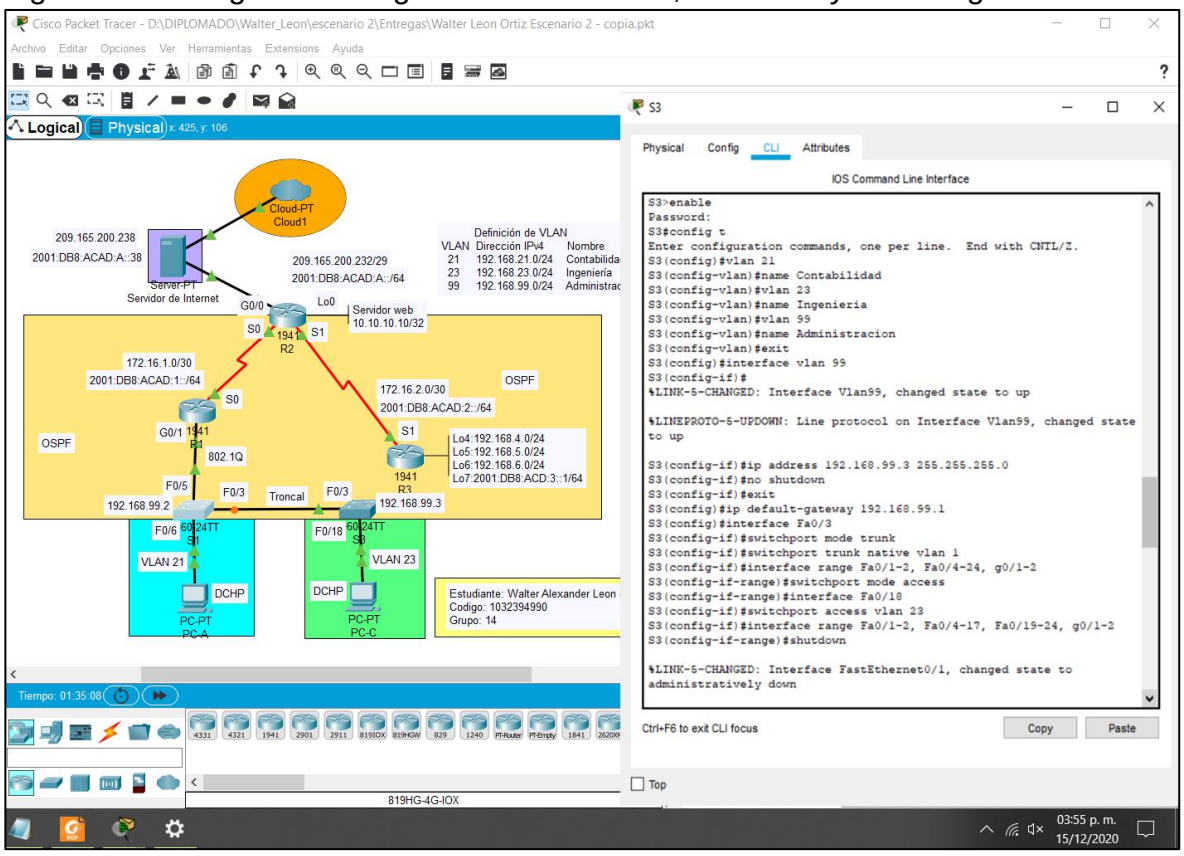
La configuración del S3 incluye las siguientes tareas:

Tabla 24. Configuración seguridad del Switch 3, Vlan y routing entre Vlan

Elemento 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 44. Configuración seguridad del switch 3, las VLAN y el routing entre VLAN.



Fuente: Autor

Paso 3: Configurar R1

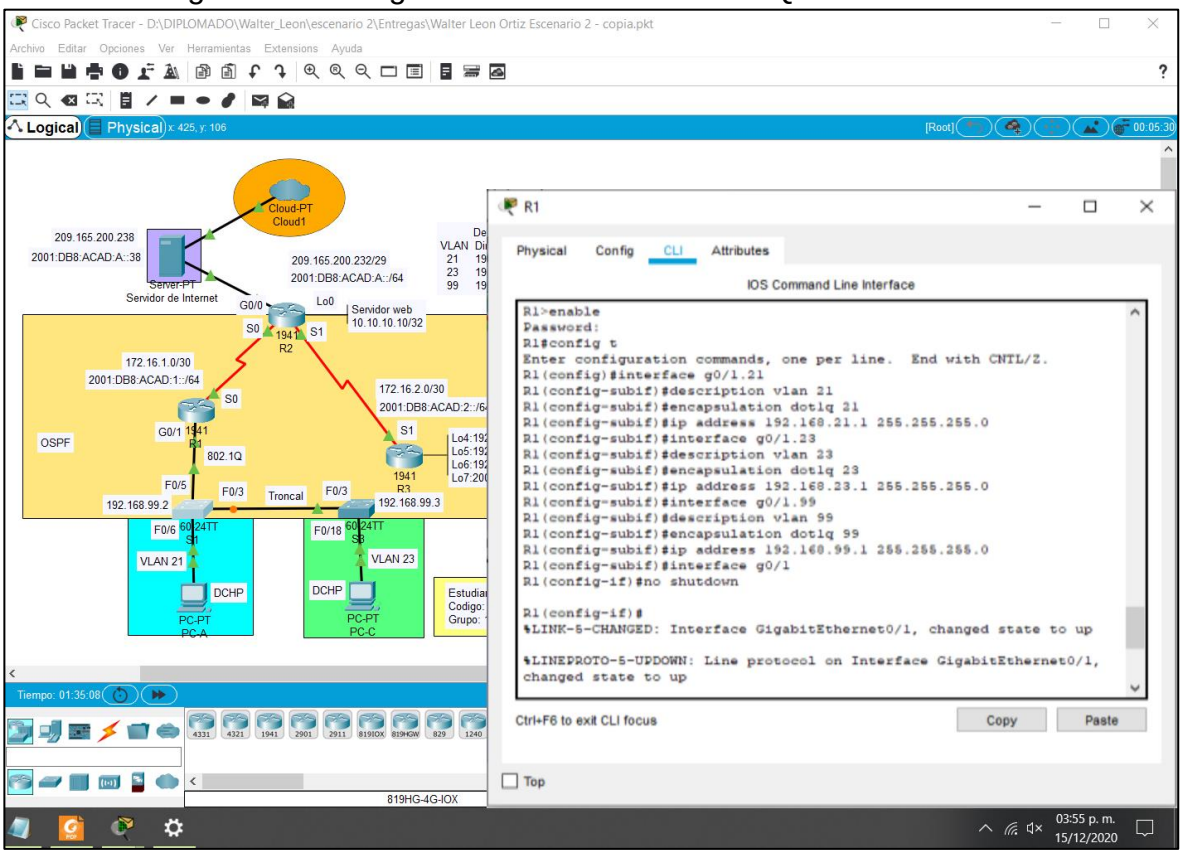
Las tareas de configuración para R1 incluyen las siguientes:
Tabla 25. Configuración Subinterfaz 802.1Q en el Router 1

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.

La 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 45. Configuración Subinterfaz 802.1Q en el Router 1



Paso 4: Verificar la conectividad de la red

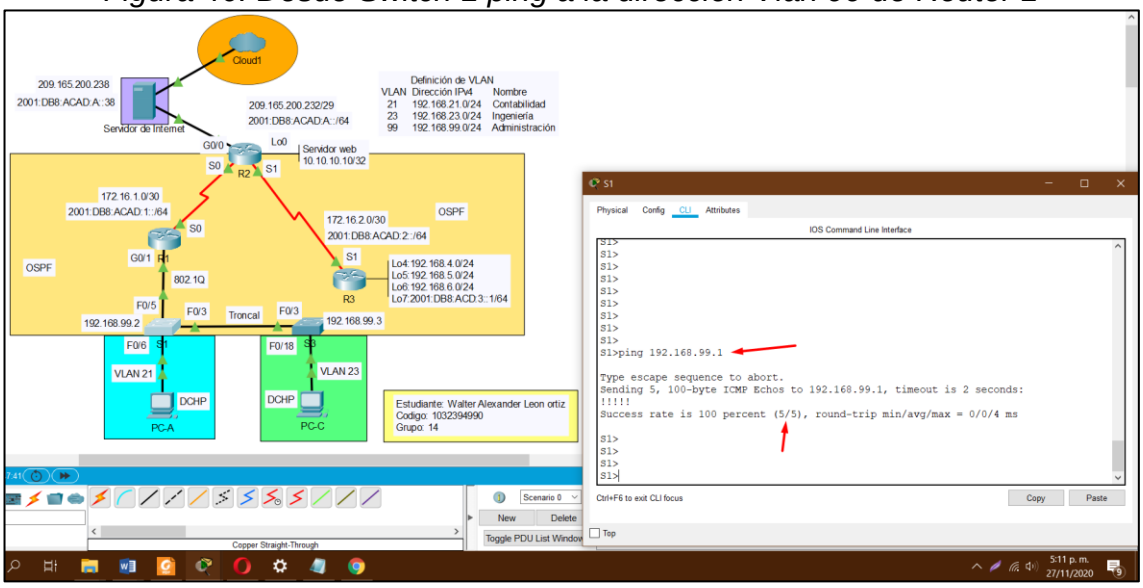
Utilice el comando ping para probar la conectividad entre los switches y el R1. Como estudiante, debes Utilizar la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 26. 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.

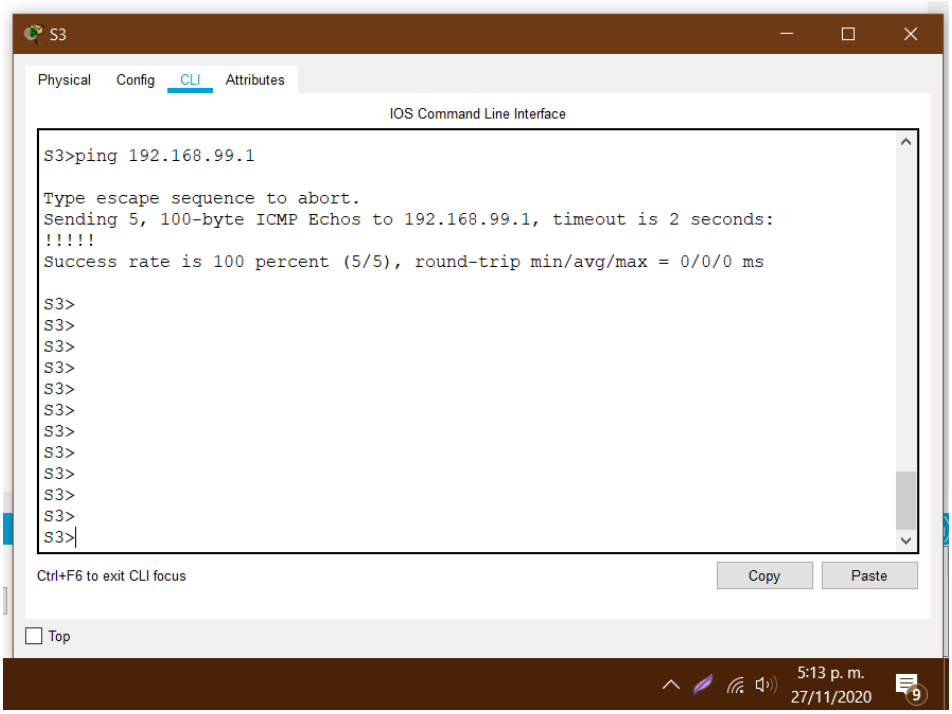
Figura 46. Desde Switch 1 ping a la dirección Vlan 99 de Router 1



Fuente: Autor

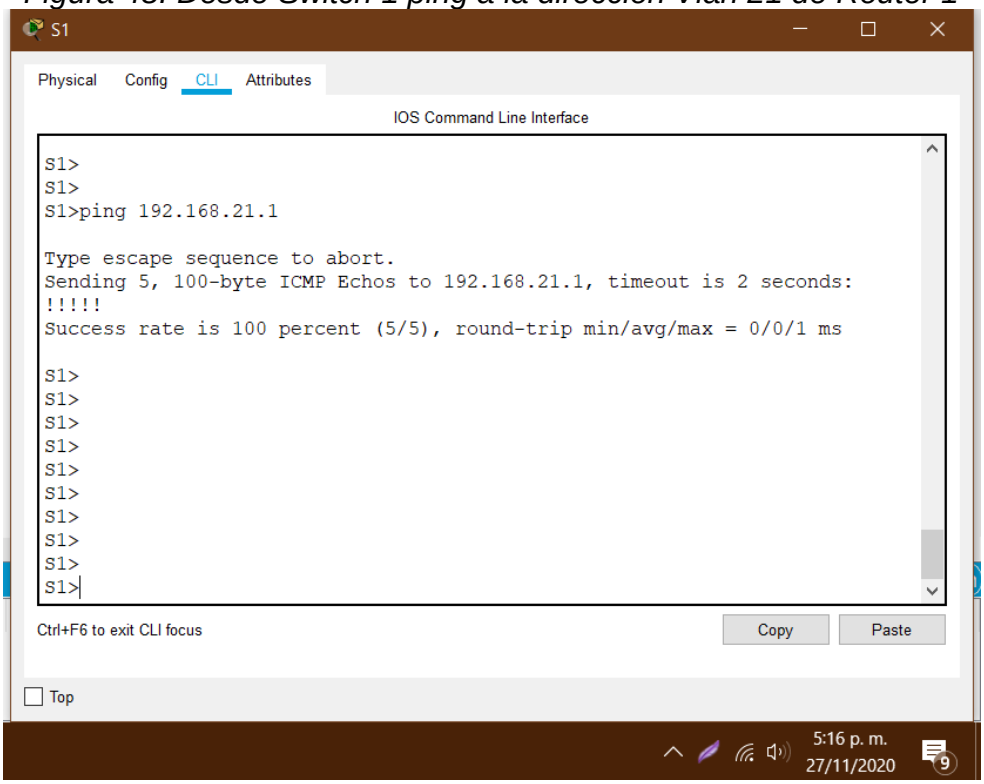
Aquí realizamos las comprobaciones entre diferentes dispositivos de la red para verificar el correcto funcionamiento de esta. Y es aquí, que, observamos que si hay ping 5 de 5, por lo tanto los avances son correctos hasta ahora.

Figura 47. Desde Switch 3 ping a la dirección Vlan 99 de Router 1



Fuente: Autor

Figura 48. Desde Switch 1 ping a la dirección Vlan 21 de Router 1



Fuente: Autor

Observamos que si hay ping 5 de 5.

Nota: Es importante mencionar que Ping es una utilidad de administración de red que se utiliza para probar la posibilidad de conexión de un dispositivo en una red IP. Esta utilidad también mide el tiempo de ida y vuelta para los mensajes que se envían desde el host de origen hasta una PC de destino.

El comando ping para mi, sirve para descartar problemas en la red y posiblemente detectar la razón del problema.

El comando ping prueba la conectividad enviando paquetes a una dirección IP, esperando que los paquetes vuelvan desde esa dirección de vuelta.

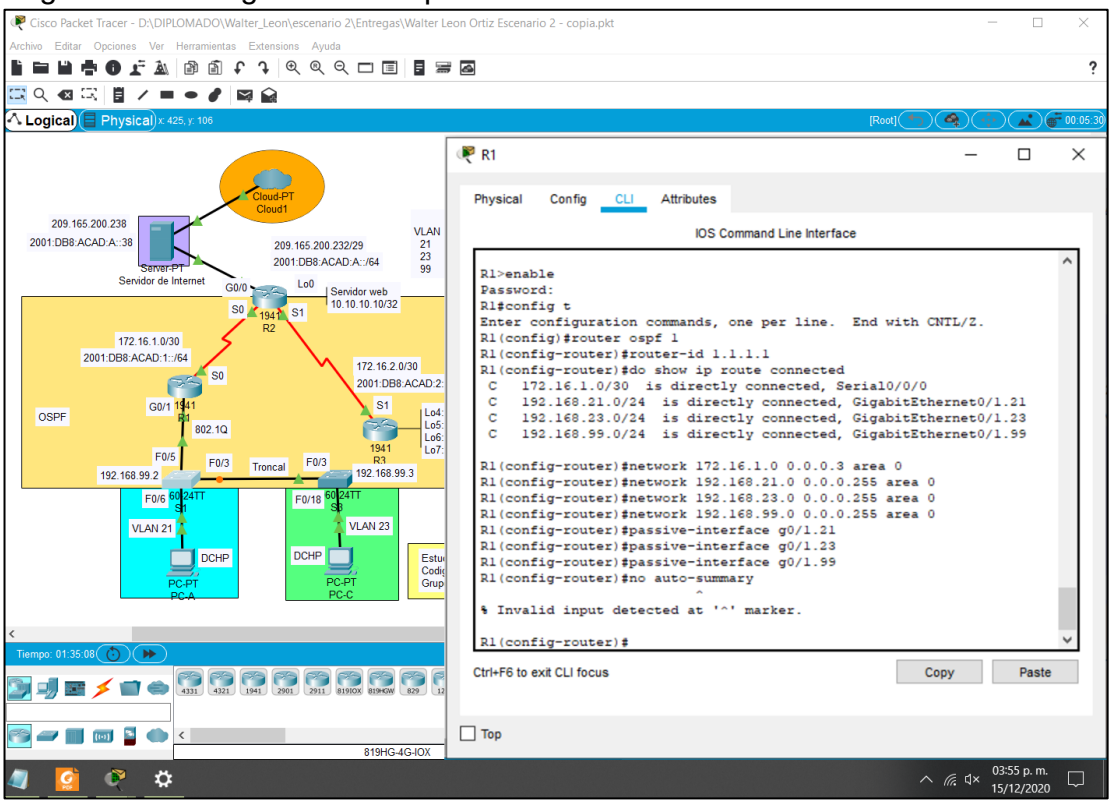
El comando envía paquetes que significan “si recibe este paquete, y está dirigido a ti, envía una respuesta”.

Cada vez que el comando ping envía uno de estos paquetes y recibe el mensaje enviado por el otro host (el destino), el comando ping sabe que un paquete se generó desde el host de origen al de destino y viceversa.

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Figura 49. Configuración del protocolo de routin dinámico OSPF en Router 1



Fuente: Autor

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 2. 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

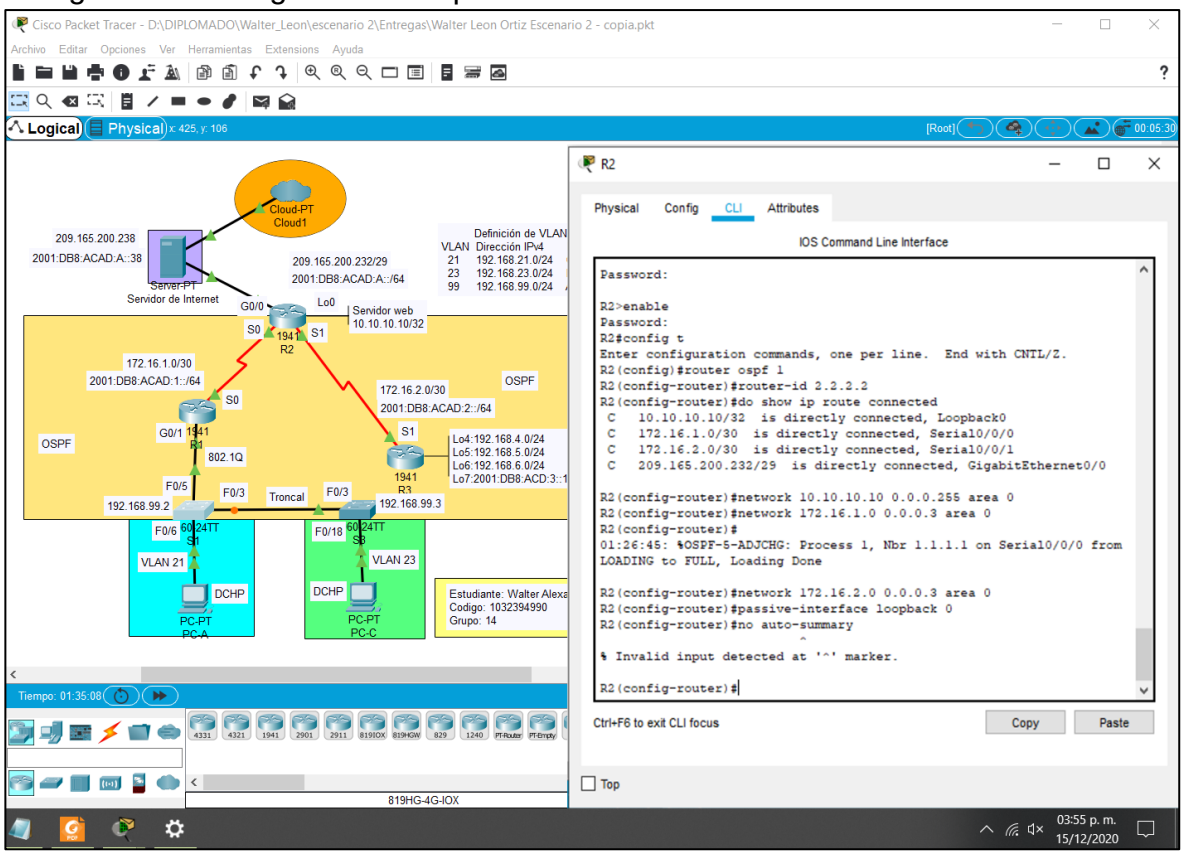
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

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.

Nota: 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.

Paso 2: Configurar OSPF en el R2

Figura 50. Configuración del protocolo de routin dinámico OSPF en Router 2



Fuente: Autor

La configuración del R2 incluye las siguientes tareas:

Tabla 3. 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

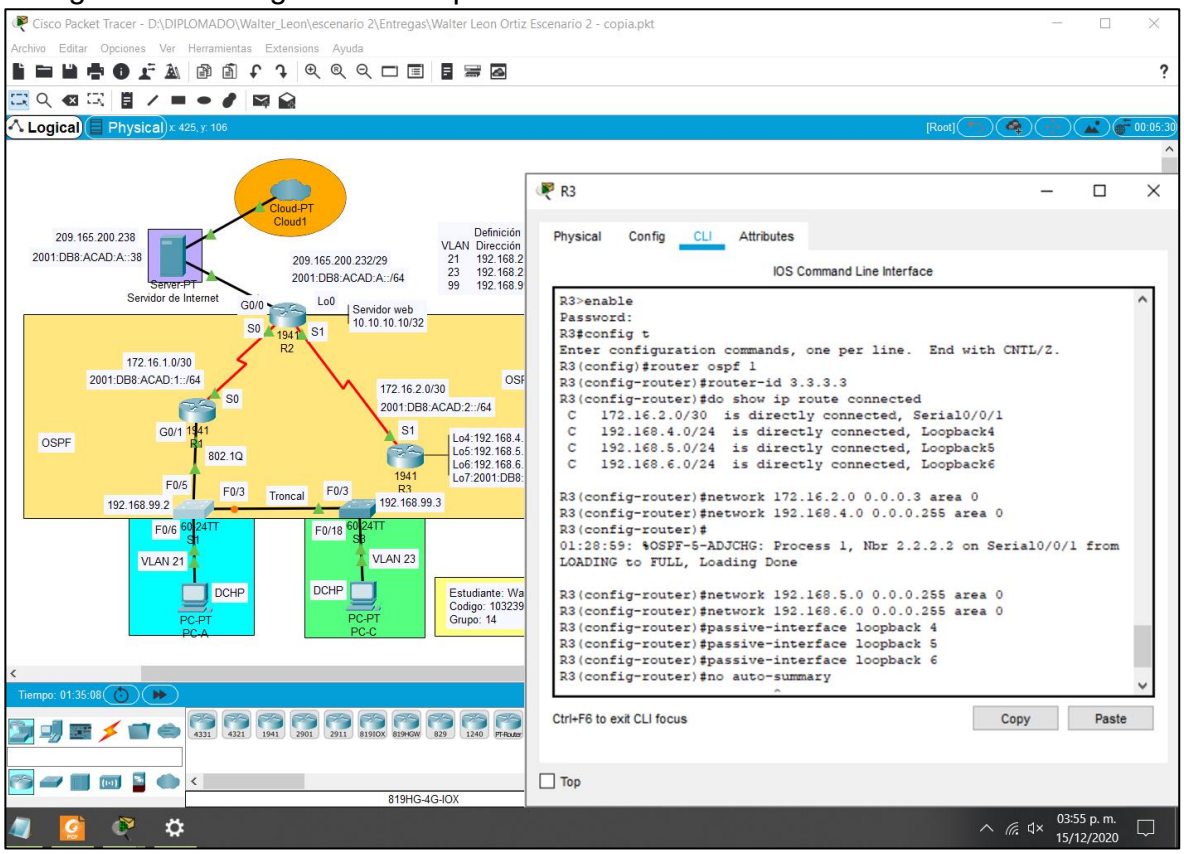
Se configura el protocolo OSPF en el Router 2 con el comando Router ospf 1, para verificar las redes conectadas se ejecuta el comando show ip route connected, con la verificación se procede asignar las redes al área 0 con el comando network asignándole la IP correspondiente.
Debemos comprender, que la 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.

El protocolo OSPF definido en RFC 1583, permite que redes de proveedores múltiples se comuniquen mediante la familia de protocolos TCP/IP. Algunas de las ventajas de OSPF son: convergencia rápida, VLSM, autenticación, segmentación jerárquica, resumen de ruta y agregación que son necesarias para gestionar redes complicadas y de gran tamaño.

Nota: *El protocolo OSPF "Open Shortest Path First" (OSPF), Abrir el camino más corto primero, en español, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.*
Paso 3: Configurar OSPF en el R3

La configuración del R3 incluye las siguientes tareas:

Figura 51. Configuración del protocolo de routin dinámico OSPF en Router 3



Fuente: Autor

Tabla 29. Configuración del protocolo de routin dinámico OSPF 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 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, 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.

Nota: *El dispositivo de red loopback es una interfaz de red virtual. Las direcciones del rango '127.0.0.0/8' son direcciones de loopback, de las cuales se utiliza, de forma mayoritaria, la '127.0.0.1' por ser la primera de dicho rango, añadiendo '::1' para el caso de IPv6 ('127.0.0.1::1').*

Las direcciones de loopback pueden ser redefinidas en los dispositivos, incluso con direcciones IP públicas, una práctica común en los routers. y son usualmente utilizadas para probar la capacidad de la tarjeta interna si se están enviando datos BGP.

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 30. 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.

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

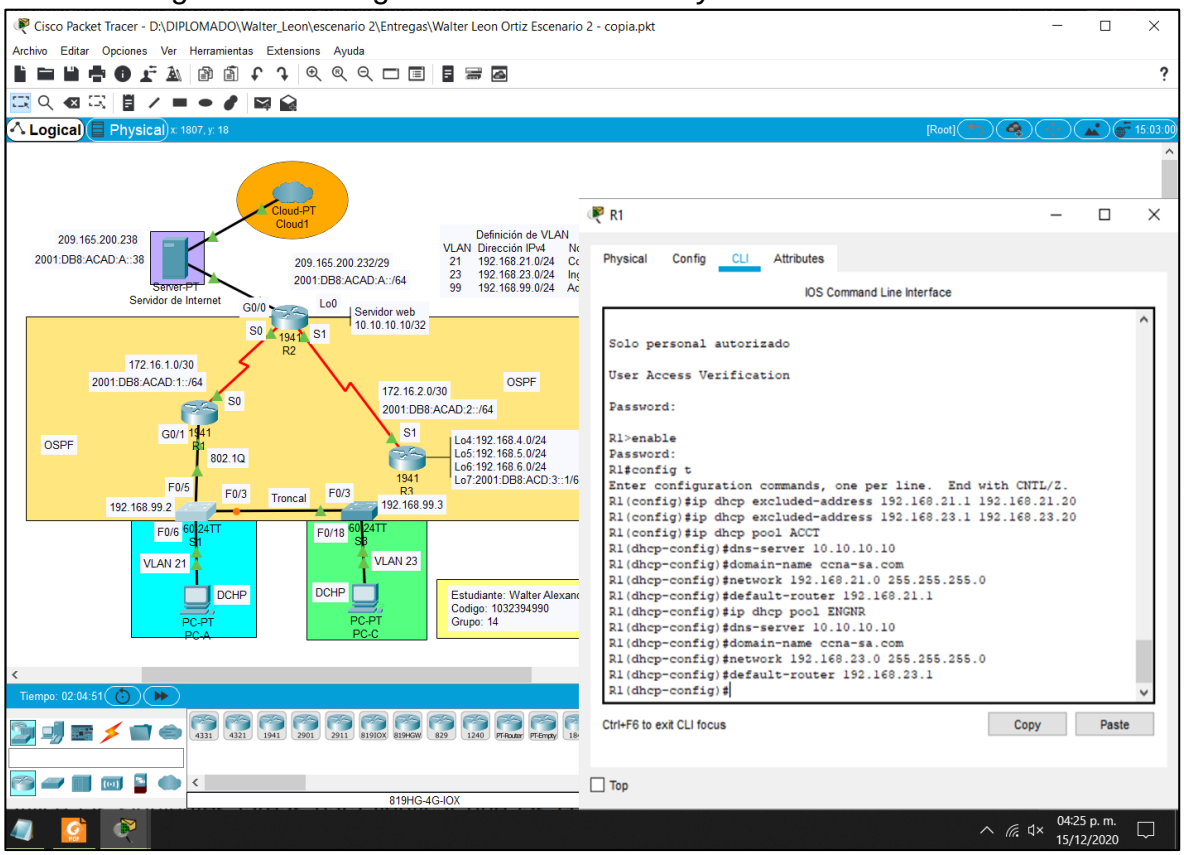
Tabla 314. Configuración del Router 1 como servidor DHCP para Vlan 21 y 23

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.

Entonces, 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 52. Configuración NAT estática y dinámica en Router 1



Fuente: Autor

Nota: El servidor DHCP, es un servidor de Red el cual permite una asignación automática de direcciones IP, getaways predeterminadas, así como otros parámetros de red que necesiten los clientes.

Dentro de sus beneficios también se encuentra una mejor administración de los servicios de red. Llegando al punto de interconectar los equipos, acceso a programas exclusivos de la empresa, entre otros.

La idea es crear 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 lo es el, ENGNR para la VLAN 23.

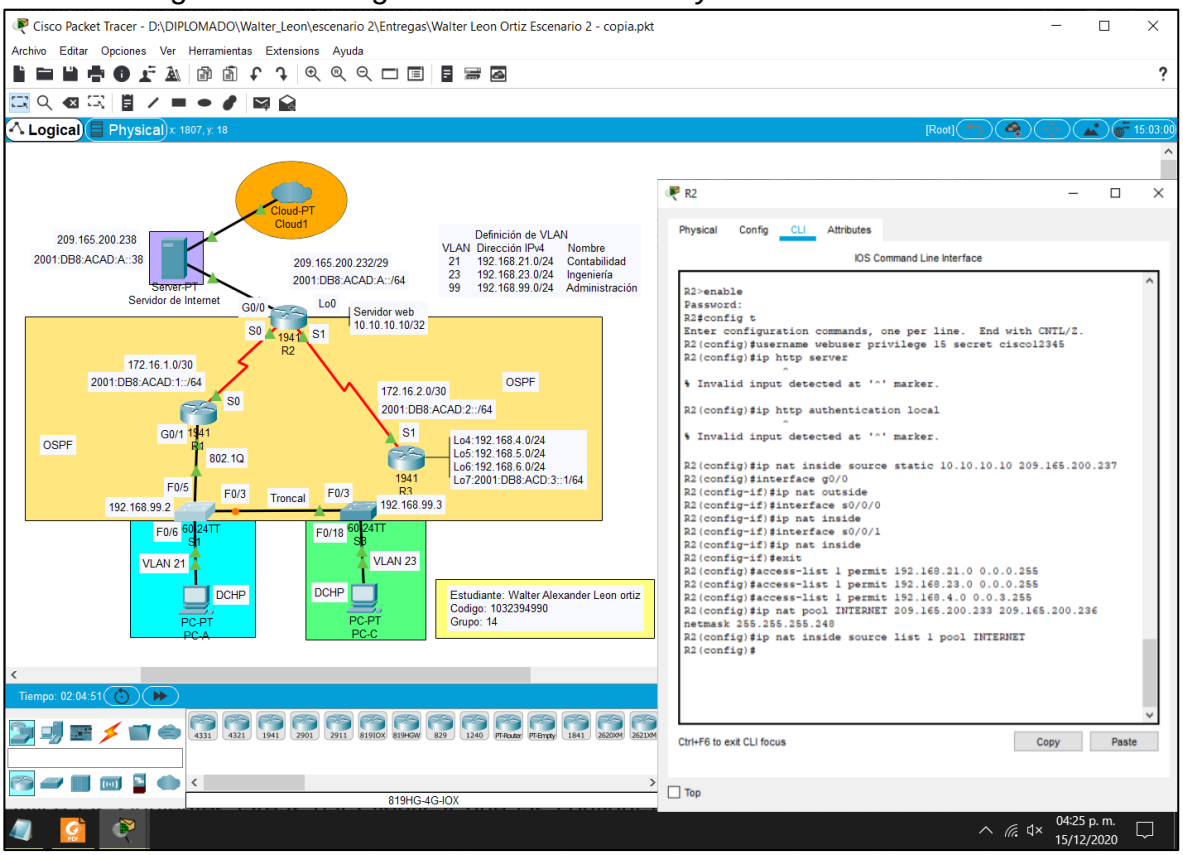
Paso 2: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 32. 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: **209.165.200.229**	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#interface 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: **209.165.200.225** – **209.165.200.228**	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Figura 53. Configuración NAT estática y dinámica en Router 2



Fuente: Autor

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 base 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 el 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.

NAT dinámica es el tipo de NAT que se utiliza con más frecuencia. Cambia la dirección IP de origen de una conexión saliente a la dirección IP pública del Firebox. ... NAT dinámica ofrece más seguridad para host internos que usan Internet porque oculta las direcciones IP de host en su red.

Paso 3: Verificar el protocolo DHCP y la NAT estática

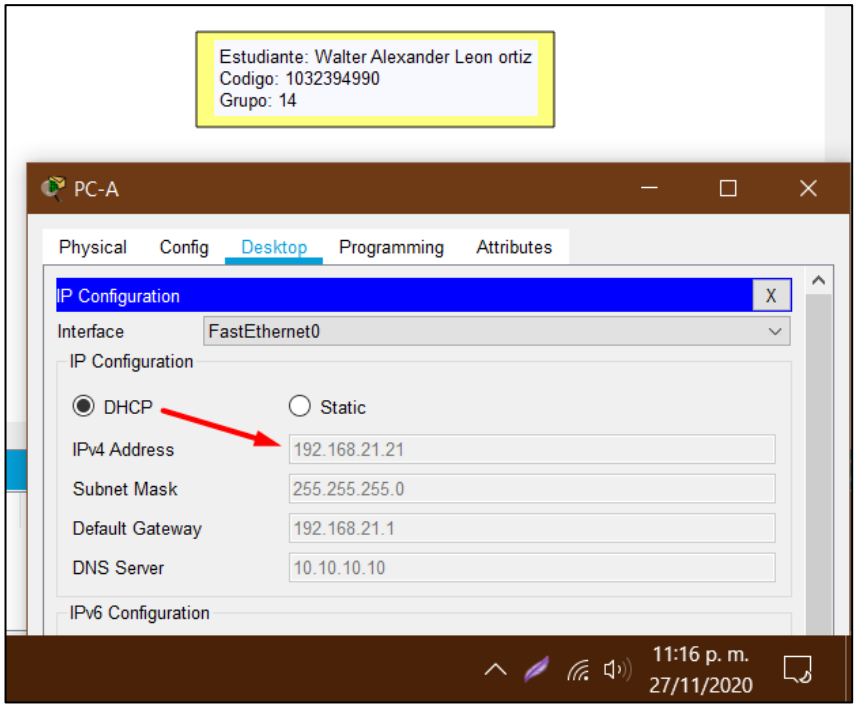
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 33. 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 respuesta
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Sí hay respuesta
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 (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	No hay respuesta

Descripcion: 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.

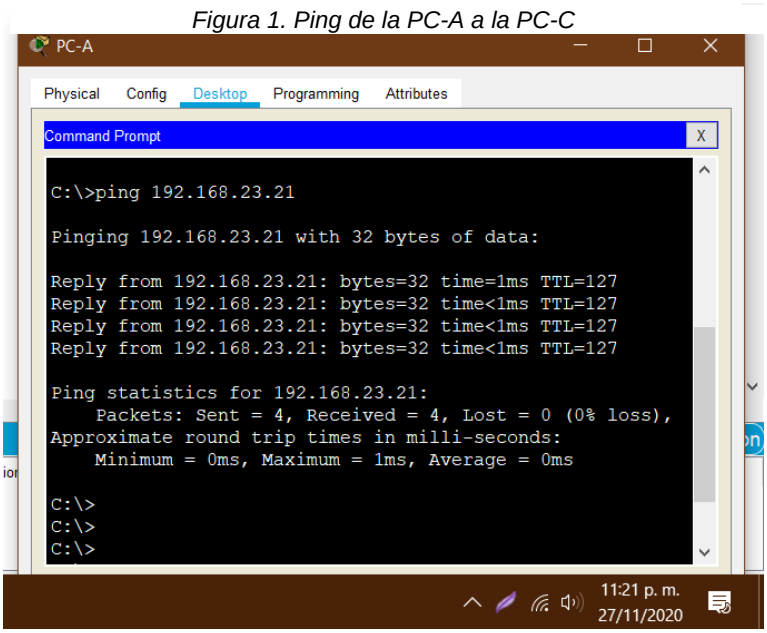
Figura 53. información de IP del servidor DHCP en PC-A



Fuente: Autor

Se verifica el funcionamiento del protocolo DHCP, para realizarlo, se verifica que la PC-A y PC-B hayan asignado la información en DHCP y es aquí donde estamos apreciando la figura 10

Figura 1. Ping de la PC-A a la PC-C



Fuente: Autor

Se verifica el funcionamiento del protocolo DHCP, para realizarlo, se verifica que la PC-A y PC-B hayan asignado la información en DHCP y es aquí donde estamos apreciando la figura 11.

El DHCP se desarrolló como solución para redes de gran envergadura y ordenadores portátiles y por ello complementa a BOOTP, entre otras cosas, por su capacidad para asignar automáticamente direcciones de red reutilizables y por la existencia de posibilidades de configuración adicionales.

La asignación de direcciones con DHCP se basa en un modelo cliente-servidor: el terminal que quiere conectarse solicita la configuración IP a un servidor DHCP que, por su parte, recurre a una base de datos que contiene los parámetros de red asignables.

Parte 6: Configurar NTP

Tabla 5. 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 update-calendar
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.

(NTP) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable.

Finalmente se verifica la configuración de NTP en R1 con el comando show ntp associations. Un método seguro para proporcionar sincronización a la red es que

los administradores implementen sus propios relojes maestros de red privada, sincronizados en UTC, mediante satélite o radio.

Además, la sincronización de relojes es fundamental para la interpretación correcta de los eventos dentro de los archivos de datos syslog, así como para los certificados digitales.

Nota: Es importante tener la hora correcta dentro de las redes. Se requieren marcas de tiempo correctas para hacer un seguimiento preciso de los eventos de red, como las violaciones de seguridad.

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

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

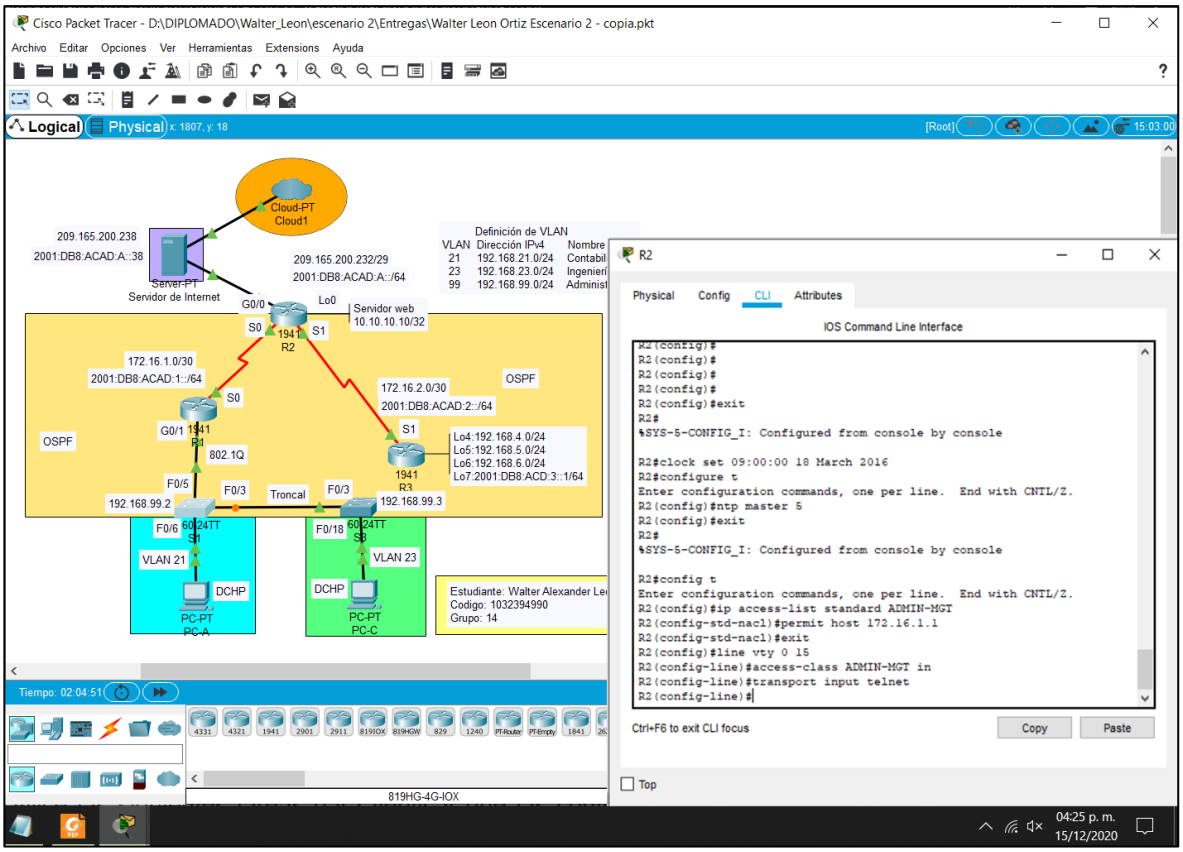
Tabla 6. Restricción de acceso a líneas VTY en Router 2

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

Aquí vamos a configurar 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.

Ambas computadoras deben poder hacer ping al Router, pero solo la computadora PC debería poder acceder al Router mediante Telnet.

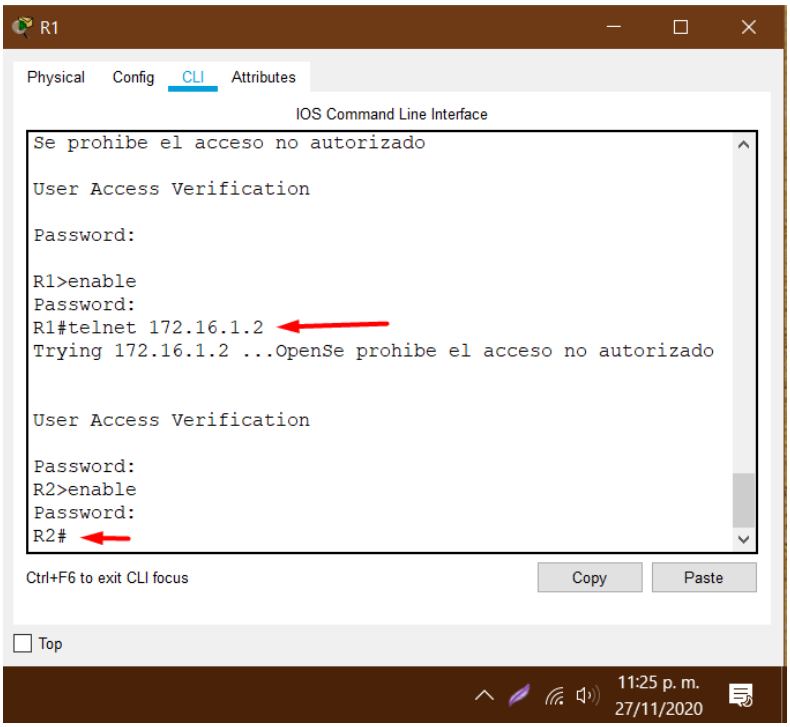
Figura 55. Restricción de acceso a líneas VTY en Router 2



Fuente: Autor

Entonces, la idea es mejorar la seguridad de las líneas administrativas mediante la restricción del acceso a VTY. Como administrador de red, la restricción del acceso a VTY es una técnica que permite definir las direcciones IP a las que se les permite acceder remotamente al proceso de EXEC del router. Puede controlar qué direcciones IP pueden acceder remotamente as router mediante la configuración de una ACL y una instrucción access-class en las líneas VTY.

Figura 2. Conexión remota de Router 1 a Router 2



Fuente: Autor

Se verifica la conexión por medio del comando “telnet” seguido de la dirección ip del Router 2, esto se hace si hay conexión, flujo de datos de Router 1 a Router 2.

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

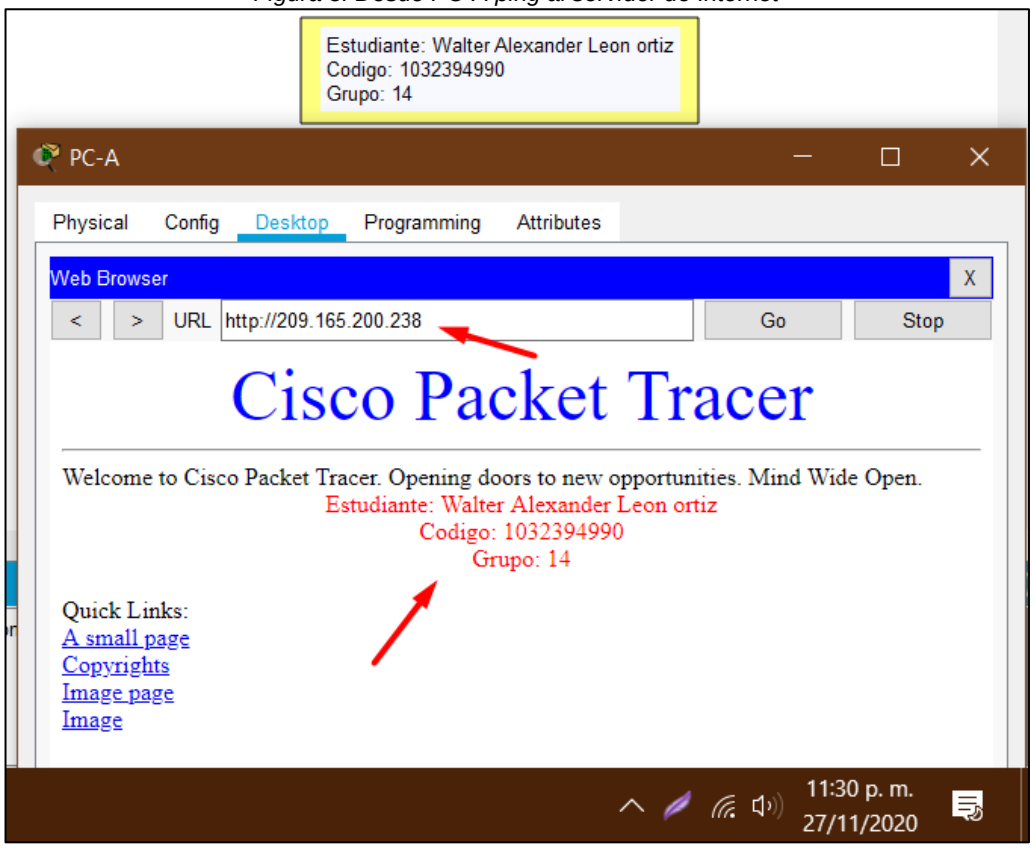
Tabla 36. Verificación de configuración con comandos CLI

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.

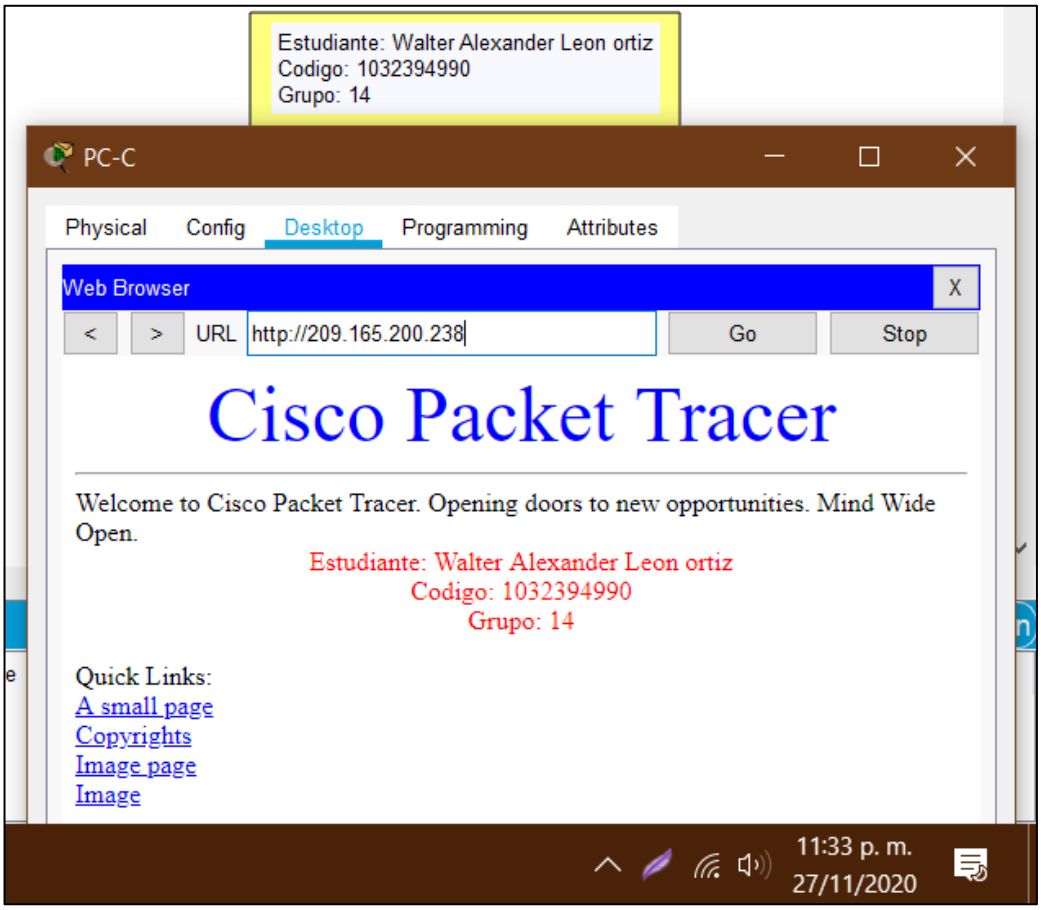
Figura 3. Desde PC-A ping al servidor de Internet



Fuente: Autor

Aquí apreciamos que si hay acceso a la dirección https://209.165.200.238, además, he modificado el archivo index.html de manera que agregué mis datos personales, para que se evidencie mi autoría.

Figura 4. Desde PC-C ping al Servidor de Internet usando: http://209.165.200.238



Fuente: Autor

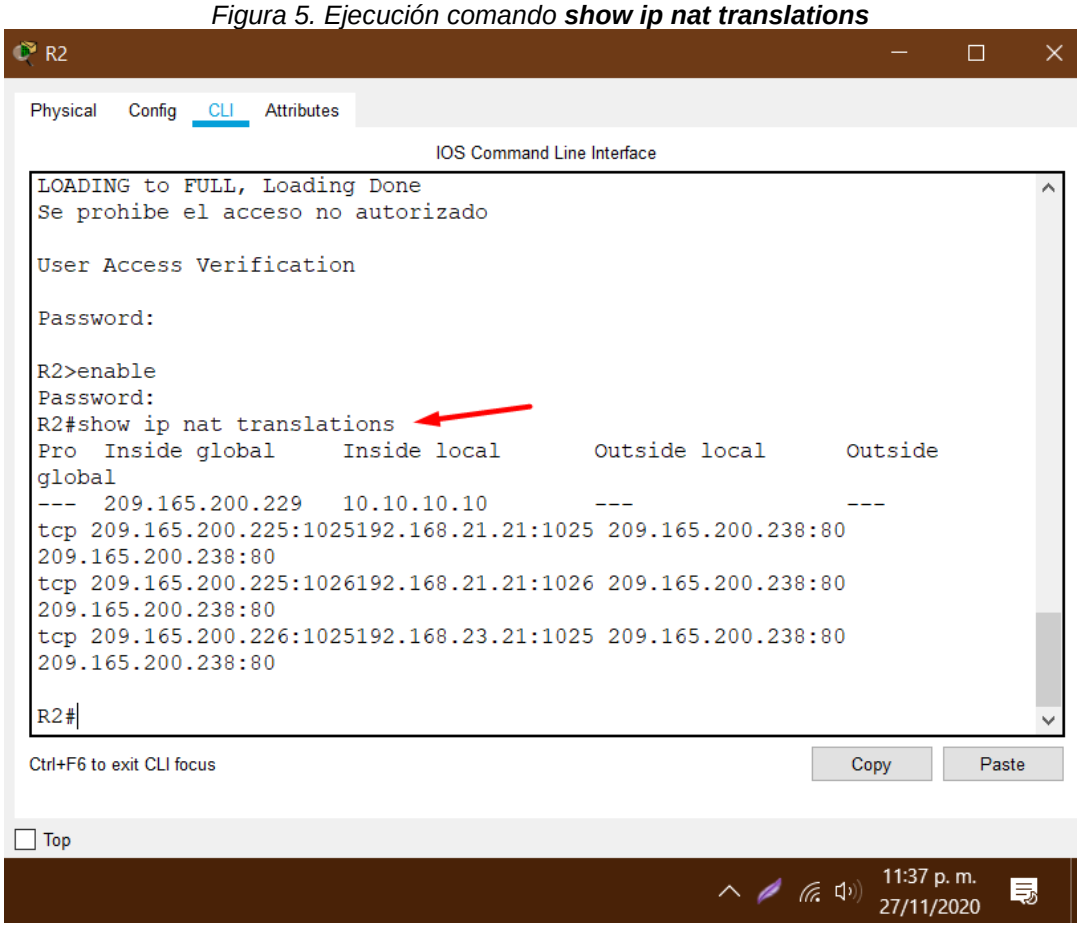
Aquí apreciamos que si hay acceso usando el protocolo http:// si hay conexión con la dirección http://209.165.200.238, además, he modificado el archivo index.html de manera que agregué mis datos personales, para que se evidencie mi autoría.

Los servidores actuales, operan a través de una arquitectura cliente-servidor. Los servidores son programas de computadora en ejecución que atienden las peticiones de otros programas: los clientes.

Nota: el servidor realiza otras tareas para beneficio de los clientes; les ofrece la posibilidad de compartir datos, información y recursos de hardware y software.

Los clientes usualmente se conectan al servidor a través de la red, pero también pueden acceder a él a través de la computadora donde está funcionando.

*Figura 5. Ejecución comando **show ip nat translations***



Fuente: Autor

Aquí realizamos la Ejecución del comando show ip nat translations.

El comando muestra todas las traducciones estáticas que se configuraron y todas las traducciones dinámicas que se crearon a causa del tráfico.

Si se agrega la palabra clave verbose, se muestra información adicional acerca de cada traducción, incluido el tiempo transcurrido desde que se creó y se utilizó la entrada.

Nota: con el comando show ip nat translations, podemos Verificar que las traducciones de la tabla son correctas.

CONCLUSIONES

En este escenario 1 y 2, se presentó Cisco IOS. Pude analizar la estructura básica de comandos en modo privilegiado, que se utiliza para configurar switch, router, y otros. También pude comprender la configuración inicial de los dispositivos de switch Cisco IOS, que incluye la configuración de un nombre, la limitación del acceso a la configuración de dispositivos, la configuración de mensajes de aviso y el guardado de la configuración.

En el escenario 2, logramos entender su principal tarea de OSPF, lo cual, es un protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta (SPF). Además, logre entender, que el protocolo OSPF, ayuda a calcular la ruta más corta entre dos nodos.

Aprendí, que los dispositivos Cisco IOS, se puede utilizar el comando **show version** para verificar y resolver problemas de algunos de los componentes básicos de hardware y software que se utilizan durante el proceso de arranque.

Lo más importante es que aprendí a configurar diversos dispositivos cisco, tanto Router como Switch, también como servidores web, y dns. Insertar comandos, es importante aprenderlas de manera básica, porque CISCO IOS, maneja diversos comandos, tanto http, como también https, y es importante resaltar que la mayoría de comandos es exclusiva para cisco, todo esto, es para que toda configuración que realicemos, es con el fin de mejorar la interacción con el software cisco packet tracer.

Sin los servidores, gran parte de las comunicaciones desaparece y no habría mucho campo laboral, sin los servidores y todo CISCO, no sería posible distinguir los servicios tales como, internet, telefonía y televisión.

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-course-assets.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-protocol-rip/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-mode-atm/permanent-virtual-circuits-pvc-switched-virtual-circuits-svc/6337-atmloopback.html

ANEXOS

Anexo A. Link de descarga Escenario 1, archivo ptk
https://drive.google.com/file/d/15pElHbwp6e6XqoJww1hy0wr178IhO0n3/view?usp=sharing

Anexo B. Link de descarga Escenario 2, archivo ptk

https://drive.google.com/file/d/1zYR_PYVgACLN9YT9w8FzpUY05LqnOiR2/view?usp=sharing

Anexo C. Link de descarga Artículo científico

https://drive.google.com/file/d/1YFlf84Fnr6xawp8j8PWqR_2Mg28Q_TBR/view?usp=sharing

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

Walter Alexander León Ortiz
Universidad Nacional Abierta y a Distancia UNAD, walterleonunad@gmail.com

Resumen

En este artículo, vamos a demostrar, la importancia y el impacto, que se logra obtener, desde una topología de red, en donde analizaremos sus tecnologías que está compuesta por varios tipos de dispositivos, como Router, Switch, host y los medios de transmisión (como cables) que, en conjunto, permite el envío de paquetes de información entre varios dispositivos a la vez. Hoy en dia, los dispositivos se pueden configurar con los protocolos adecuados usando el entorno de simulación Packet Tracer, que, con ella, nos permite enrutar, conmutar, recibir y enviar datos mediante el modelo de referencia OSI.

La configuración de los routers y Switch CISCO están diseñados para trabajar en Ipv4, que es el protocolo más usada al nivel mundial, pero las tecnologías cambian, mejoran tanto que, hoy día se está cambiando por el Ipv6 como protocolo estándar. En el escenario 1 y 2 vamos a ser testigos, de un acoplamiento de las dos IP en función de una misma red. La administración de las redes LAN y WAN en la actualidad ha permitido a las empresas e instituciones optimizar el uso de los recursos mediante una red centralizada permitiendo disponer la información de forma segura y rápida.

Palabras clave: Protocolo, topología, Vlan, Interfaces, Enrutador, LAN, WAN, Infraestructura, Comunicación, Red.

Abstract

In this article, we are going to demonstrate the importance and impact that can be obtained from a network topology, where we will analyze its technologies that are composed of several types of devices, such as Router, Switch, host and the transmission media (such as cables) that, together, allow the sending of information packets between several devices at the same time. Today, devices can be configured with the appropriate protocols using the Packet Tracer simulation environment, which, with it, allows us to route, switch, receive and send data using the OSI reference model.

The configuration of the CISCO routers and switches are designed to work in IPv4, which is the most used protocol worldwide, but technologies change, they improve so much that today it is being changed to IPv6 as the standard protocol. In scenarios 1 and 2 we are going to witness a coupling of the two IPs based on the same network. The administration of LAN and WAN networks today has allowed companies and institutions to optimize the use of resources through a centralized network, allowing information to be available safely and quickly.

Keywords: Protocol, topology, Vlan, Interfaces, Router, LAN, WAN, Infrastructure, Communication, Network.

I. INTRODUCCIÓN

En este artículo, vamos a estudiar el escenario uno, que tiene una topología muy específica que trae dos switch de capa 3 referencia 3560, un router con referencia 1142 CISCO y dos hosts. Vamos a entender sus comandos para cambiar nombres al Router 0, además vamos a entender como implementar la seguridad con contraseña, posteriormente encriptar las claves a los dispositivos de red como Switch y otros, por medios de comandos y modo privilegiado.

[1] Los modelos de switch Catalyst 3560, 3750, las Catalyst 4500/4000 Series con el Sup II+ o posteriores, o bien las Catalyst 6500/6000 Series, estos switchs, soportan funciones básicas del ruteo InterVLAN en todas sus versiones de software CISCO IOS. El switch 3560 utiliza la versión IOS 12.2(37) SE1, permitiendo el ruteo de InterVLAN y activación de Ipv6. [2] Una vez identificado los dispositivos que cumplieran con los requisitos necesarios para formar la topología de la red LAN, se ejecutan comandos para borrar el contenido de la NVRAM en los puntos de conexión.[3] El switch 3560 debe ser configurada, para que la plantilla SDM esté activada.

[4] Una vez organizados en el Packet Tracer, se configuran los nodos (Switch y router) con los protocolos necesarios para poder interactuar con el Modelo OSI.

[5] Debemos aprender que, el router como el switch, manejan comandos de configuraciónes, ya que pertenecen a la misma marca o empresa CISCO.

[6] De forma predeterminada, hay tres niveles de comando en el router: Nivel de privilegio 0: incluye los comandos disable, enable, exit, help y logout. La configuración de los accesos del administrador de la red LAN, establecen contraseñas para el modo usuario y modo privilegiado con la encriptación correspondiente.

[7] El protocolo SSH utiliza encriptación para asegurar la conexión entre un cliente y un servidor; esta configuración de protocolo permite encriptar las contraseñas de administradores para evitar que terceras personas identifiquen el password, esto ayuda aumentar la seguridad en la Red LAN.

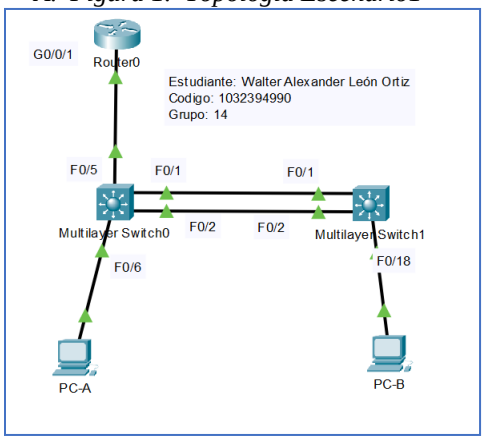
[8] La configuración de Ipv4 e Ipv6 en los conmutadores con las correspondientes máscaras. [9] La creación de Vlan como enlaces lógicos son determinantes en la creación de troncos 802.1Q que utilicen la VLAN nativa para la conexión de la red LAN. [10] El DHCP nos permite asignar automáticamente direcciones IP reutilizables a clientes DHCP. [11] Etherchannel ayuda aumentar el ancho de banda y el port-security en algunos casos ayuda bloquear los puertos como medidas de prevención y seguridad.

II. METODOLOGÍA DE IMPLEMENTACION Y ADMINISTRACION DE UNA RED LAN PEQUEÑA

Vamos a trabajar en base del escenario uno, porque es una investigación de tipo aplicada ya que se busca encontrar una solución para que se pueda transmitir paquetes de información en la red LAN entre Ipv4 e Ipv6 en los hosts.
[12] La Investigación Aplicada tiene el objetivo de resolver un determinado problema específico.

Para esta Red pequeña es necesario utilizar una cantidad determinada de equipos y los cuales juntos son conocidos como Topología de Red y la cual se muestran en la ilustración siguiente Figura 1.

A. *Figura 1. Topología Escenario1*



[13] La investigación aplicada también se le denomina activa o dinámica, ya que depende de sus descubrimientos y aportes teóricos; los enrutadores como los conmutadores CISCO están en constante desarrollo y actualización; desde las versiones de las IOS que permiten utilizar ciertas características que puedan adaptarse al modelo OSI como las plantillas SDM que habilitan la Ipv6 en los Switch 3560 de capa 3, hasta los comandos ipv6 unicast-routing que los habilita en el Router 1142.

III. PASOS DE IMPLEMENTACION DE LA TOPOLOGÍA

Para lograr implementar la topología presentada en la Figura

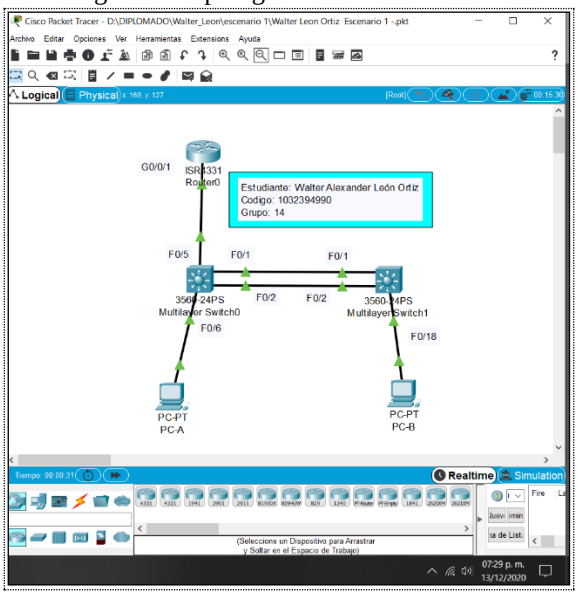
1. se realiza la creación de la topología necesaria en el software Packet Tracer empleando los siguientes equipos de este aplicativo.

- 01 Router 4331 para R1
- 01 Switch 3560 para S1
- 01 Switch 3560 para S2
- 01 PC para PC-A
- 01 PC para PC-B

A. *Creación de Topología*

Utilizando los diferentes equipos simulados mediante el Software Packet Tracer se elabora la topología necesaria para realizar ciertos parámetros de configuración en cada equipo y los cuales se pueden observar en la siguiente ilustración Figura 2.

Figura 2. Topología creada Escenario 1



También el método experimental es utilizado para obtener los resultados en la solución de la conexión de los dispositivos del escenario uno. [14] De manera general, al aplicarla a la Ingeniería de Sistemas (IS), la experimentación nos ayuda a identificar y comprender distintos aspectos, así como errores de conexiones, problemas de seguridad y mantenimiento, etc.

B. Borrado de configuraciones en router y switch

El primer paso paraantes de introducir nuevas configuraciones, debemos realizar la eliminación de la configuración de inicio de cada dispositivo y paso posterior volver a cargar estos dispositivos, con el fin de establecer borrado y carga los cuales podemos trabajar desde cero sin configuraciones que ya viene prestablecidas por el fabricante CISCO. La idea es trabajar sin registros, todo desde cero.

TABLA 1.
BORRADO ROUTER Y SWITCHES ESCENARIO 1

Borrado Router y Switches Escenario 1	
Tarea	**Especificación**
Eliminar el archivo startup-config de todos los routers	**Router>enable** **Router#erase startup-config**
Volver a cargar todos los routers	**Router#reload**
Eliminar el archivo	**Switch>enable**
startup-config de todos los switch y eliminar la base de datos de VLAN	**Switch#erase startup-config** **Switch#delete vlan.dat**
Volver a cargar ambos switch	**Switch#reload**
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	**Switch>enable** **Switch#show vlan brief**

C. Configuración plantilla SDM para que admita IPv6

Los switchs, no admiten ipv6, por lo tanto, vamos a crear una plantilla SDM, que este ayudará al switch, admitir protocolos IPV6. Vamos a utilizar los comandos establecidos en la tabla 2, la configuración en cualquiera de los Switch es igual, debemos, configurar VTY solo aceptando SSH.

TABLA 2. CONFIGURAR PLANTILLA SDM PARA QUE ADMITA IPV6

Configurar plantilla SDM para que admita IPv6	
Tarea	**Especificación**
Verificar y seleccionar plantilla	**Switch>enable** **Switch#show sdm prefer**
Ver plantilla SMD	**Switch#configure terminal** **Switch(config)#sdm prefer ?**
Modificar la plantilla SMD	**Switch(config)#sdm prefer dual-ipv4-and-ipv6 ?** **Switch(config)#sdm prefer dual-ipv4-and-ipv6 default**
Volver a cargar switch	**Switch(config)#exit** **Switch#reload**
Verificar que los cambios efectuados	**Switch>en** **Switch#show sdm prefer**

[15] Para adecuar los dispositivos se los adapto con algunos protocolos de capa 5,6 y 7 de aplicación, sesión y presentación como equivalentes, utilizando protocolos TCP/IP como NFS, NIS, DNS, LDAP, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP y otros.

D. Configurar el Router R1.

Una vez borradas las configuraciones y eliminadas los archivos vlan.dat, en cada Router y Switch, posteriormente se realizará el procedimiento de configuración teniendo en cuenta cada uno de los aspectos y requerimientos solicitados para esta red en base a esto nos apoyaremos en la lista de direccionamiento IP sobre la topología de red a trabajar.

Debemos crear un usuario administrativo en la base de datos local, configurar el inicio de sesión en las líneas VTY para que use la base de datos local, configurar VTY solo aceptando SSH, Cifrar las contraseñas de texto no cifrado, generar un mensaje MOTD que permita mostrar una alerta si la contraseña ingresada es diferente a la permitida,

Habilitar el routing IPv6, Configurar interfaz G0/0/1 y subinterfaces, configurar el Loopback0 interface generar una clave de cifrado RSA.

Para esta tarea se usaron diferentes comandos mostrados o contenidos en la Tabla 3.

TABLA 3. CONFIGURACIÓN R1

Configuración router 1	
Tarea	**Especificación**
Desactivar la búsqueda DNS	**Router>enable** **Router# (config)#no ip domainlookup**
Nombre del router	**Router# (config)#hostname R1**
Nombre de dominio	**R1(config)# ip domain name ccna-lab.com**
Contraseña cifrada para el modo EXEC privilegiado	**R1(config)#enable password ciscoenpass R1(config)#exit** **R1#en** **R1#config t** **R1#en** **R1#config t** **R1(config)#service passwordencryption** **R1(config)#exit**
Contraseña de acceso a la consola	**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	**R1#config t** **R1(config)#security passwords min-length 10** **R1(config)#enable password ciscoenpass**
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** **R1#config t** **R1(config)#username admin password admin1pass**

TABLA 4

ASIGNACIÓN DE DIRECCIONES DE LOS DISPOSITIVOS

Dispositivo	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

IV. RESULTADOS

A partir de la topología de red escenario uno, se plantean una serie de configuraciones de los dispositivos CISCO de la red LAN que, son implementadas en un entorno de simulación Packet Tracer para hacer las pruebas de funcionalidad y respuesta a las configuraciones planteadas.

En la Figura 1 se muestra la Topología red LAN del escenario 1, donde se observa Multilayer switch 0 y 1, con sus otros componentes que lo acompañan, como la PC-A y la PC-B, seguido del Router 0.

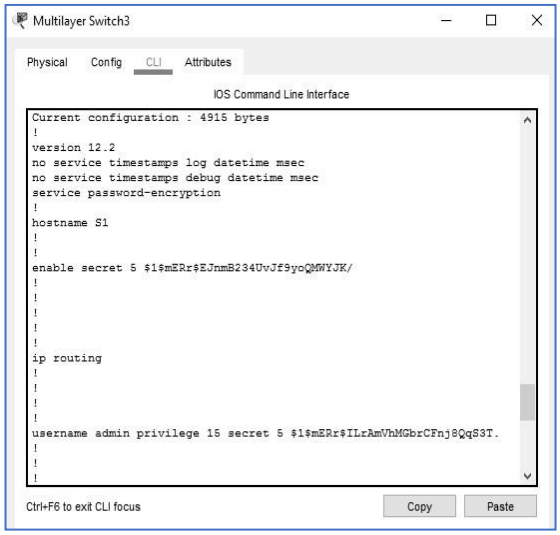
Para las pruebas de laboratorio, se brinda una serie de datos que identificaran los enlaces virtuales y físicos de las interfaces para el envio de paquetes. Información como el nombre de las VLAN y las direcciones de los switchs y routers en Ipv4 e Ipv6 que establezcan conexión de datos.

TABLA 2

NOMBRE DE VLAN

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

Para la administración de los dispositivos de la topología de red, se configura los enrutadores y conmutador el ingreso a los dispositivos con contraseñas en modo usuario y modo privilegiado; También algunas características que le permitan ser identificados en la red como el nombre, es con el comando **"hostname"**, el acceso, se realiza remotamente mediante Telnet o SSH y con encriptación de contraseñas que brinden seguridad en la administración de la red.



Las direcciones Ipv6 e Ipv4 son incorporadas al router y switchs con le segmentación necesaria para que interactúen con el tráfico de paquetes en la red.

A. Figura 3. Configuración Ipv4 e Ipv6

```
!
interface Vlan4
 mac-address 0009.7c3d.b701
 ip address 10.19.8.98 255.255.255.248
 ipv6 address FE80::98 link-local
 ipv6 address 2001:DB8:ACAD:C::98/64
!
interface Vlan5
 mac-address 0009.7c3d.b702
```

Las Vlans como enlaces lógicos dentro de la interface son creadas en los dispositivos de red, debidamente renombradas para que puedan tener acceso al tráfico de paquetes de información entre host. Los accesos se habilitan en los puertos físicos FastEternet, GigabitEternet y subinterfaces con las condiciones necesaria para que el transporte de paquetes sea direccionado mediante una Vlan Nativa. La configuración de troncos 802.1Q o encapsulamiento admite que se utilice un solo medio físico por donde transitan diferentes redes (VLAN) como protocolo que se adapte am modelo OSI de redes.

Una VLAN (virtual LAN) es, conceptualmente, una red de área local formada a nivel lógico. Una VLAN puede formarse también a partir de múltiples segmentos de LAN. Esto permiten que estaciones de trabajo ubicadas físicamente en lugares diferentes pueden trabajar en la misma red lógica (es decir, con el mismo direccionamiento de red), como si estuvieran conectadas al mismo switch. Si no se hace buen empleo de comandos privilegiados, no se podrá concluir las configuraciones.

B. Figura 4. Creación de VLANS

```
--------------------------------
1    default                          active    Po2, Fa0/10, Gig0/1,
Gig0/2
2    Bikes                            active    Fa0/6
3    Trikes                           active
4    Management                       active
5    Parking                          active    Fa0/3, Fa0/4, Fa0/7,
Fa0/8
                                                Fa0/9, Fa0/11,
Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15,
Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19,
Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23,
Fa0/24
6    Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode
Trans1 Trans2
```

En esta figura 4, se puede apreciar la creación de los nombres de VLANS mencionado en la Tabla 2

La topología de red LAN del escenario uno proporciona una configuración de EtherChannel entre el Swich uno y dos, por donde transitan los enlaces lógicos de las Vlan bikes, trikes, Management y Parkin en las interfaces lógicas FastEternet 1

y 2. EtherChannel garantiza el ancho de banda entre dispositivos, garantizando la tolerancia de fallos, la garantía de proporcionar una señal estable con dos enlaces físicos de conexión FastEternet 1 y 2 y distribución de envió de paquetes por dos enlaces equilibrando cargas.

Nota: EtherChannel se adapta a los estándares CISCO 802.3 fullduplex.

Figura 5. Configuración EtherChannel

```
Password:
S2#sho
S2#show ter
S2#show eth
S2#show etherchannel summ
S2#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------
+-----------------------------------------------

2      Po2(SD)           LACP   Fa0/1(I) Fa0/2(I)
S2#
```

Para garantizar la configuración establecida en los puntos de conexión de la red LAN, se realizan las pruebas mediante latencia (ping), que se envía de extremo a extremo mediante los hosts, con las respuestas positivas en donde refleja el tiempo de medición en milisegundos la subida y bajada de conexión. Las pruebas son realizadas con el router y los switchs desde los terminales, en donde se evidencia que los hosts han adquirido una ip dinámica ya que el router fue configurado con el protocolo DHCP cliente/servidor.

C. Figura 6. Ping IP 10.19.8.1 PC1

```
Packet Tracer PC Command Line 1.0
C:\>ping 10.19.8.1

Pinging 10.19.8.1 with 32 bytes of data:

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

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

D. Figura 7. Ping IP 10.19.8.65 PC1

```
C:\>ping 10.19.8.65

Pinging 10.19.8.65 with 32 bytes of data:

Reply from 10.19.8.65: bytes=32 time=1ms TTL=255
Reply from 10.19.8.65: bytes=32 time<1ms TTL=255
Reply from 10.19.8.65: bytes=32 time<1ms TTL=255
Reply from 10.19.8.65: bytes=32 time<1ms TTL=255

Ping statistics for 10.19.8.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Apoyado en la topología de la red se realizó la configuración del Switch 1 y 2 utilizando cada uno de los parámetros básicos establecidos para la red como son desactivar la búsqueda DNS.

E. Figura 8. Ping a IPV6 2001:db8:acad:b: :50PC1

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

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

Reply from 2001:DB8:ACAD:B::50: bytes=32 time=11ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=1ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127

Ping statistics for 2001:DB8:ACAD:B::50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 3ms
```

F. Figura 9. Ping a IPv6 2001:db8:acad:b::50 PC 2

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

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

Reply from 2001:DB8:ACAD:B::50: bytes=32 time=4ms TTL=128
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=4ms TTL=128
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=1ms TTL=128
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=4ms TTL=128

Ping statistics for 2001:DB8:ACAD:B::50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 3ms
```

G. Figura10. Ping a IPv6 2001:db8:acad:209::1 PC 2

```
C:\>ping 2001:db8:acad:209::1

Pinging 2001:db8:acad:209::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:209::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time=1ms TTL=255

Ping statistics for 2001:DB8:ACAD:209::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

V. Conclusión

Las prácticas de laboratorio de simulación de dos escenarios o topologías de red LAN, permiten el aprendizaje del funcionamiento de una red desde el conocimiento de los diferentes terminales, conexión de cables con puertos, configuración de los dispositivos mediante protocolos modelo OSI, administración de redes y seguridad de puntos

de conexión de red.

Los dispositivos como el router y switch CISCO están diseñados para enlazarse a través de protocolos de redes de host, que se adaptan al modelo OSI (Open Systems Interconnection), para garantizar la transmisión de paquetes enlazados con las capas 2 y capa 3 de las redes LAN y WAN.

Los ejercicios relacionados a las dos topologías de red, resaltan las configuraciones básicas de los enrutadores y conmutadores para las buenas prácticas en la administración de una red. Reseteo de dispositivos, configuración de password de seguridad a modo usuario y privilegiado, configuración de administradores locales y remotos mediante SSH o telnet, encriptación de contraseñas, descripciones, mensajes de seguridad (BANNER). El desarrollo de los escenarios permite la aplicación de enunciados con direcciones loopback para verificar el funcionamiento y programación con los parámetros establecidos para los ejercicios planteados.

VI. Referencias

[1] CISCO. (s. f.). Configurar routing interVLAN en switches de capa 3. CISCO.COM. Recuperado 22 de noviembre de 2020, de https://www.cisco.com/c/es_mx/support/docs/lanswitching/inter-vlan-routing/41860-howto-L3intervlanrouting.html

[2] Problemas causados por el acceso simultáneo a la NVRAM del enrutador. (s. f.). CISCO.COM. Recuperado 14 de noviembre de 2020, de https://www.cisco.com/c/en/us/support/docs/ios-nx-ossoftware/ios-software-releases-124-mainline/46942nvram.html#req

[3] OpenWebinars. (2019, 26 abril). Cisco: Configuración de SDM Templates [Vídeo]. YouTube.com. https://www.youtube.com/watch?v=L4bwV5M6hkk

[4] Asmoday S.A. (2016, 17 febrero). Cómo se utiliza el programa Packet Tracer (cisco). Asmodaysa.com. https://asmodaysacom.wordpress.com/2016/02/17/como-se-utiliza-el-programa-packet-tracer-cisco/

[5] Cabrera, C. C. (2020, 23 marzo). Configuración básica de routers/switches cisco: CCNAv7 ITN mod2. Cesarcabrera.inf. https://cesarcabrera.info/configuracion-basica-derouters-switches-cisco-ccnav7-itn-mod2/

[6] CISCO. (s. f.-b). Los niveles de privilegio de IOS no pueden ver la configuración completa en ejecución. Cisco.com. Recuperado 10 de noviembre de 2020, de https://www.cisco.com/c/es_mx/support/docs/securityvpn/terminal-access-controller-access-control-systemtacacs-/23383-showrun.html

[7] SSH. (s. f.). SSH (Secure Shell). ssh.com. Recuperado 9 de noviembre de 2020, de https://www.ssh.com/ssh/

[8] Guerreros de la Red Michely Lopez. (2019, 7 enero). Packet Tracer - Configurar Tunel IPV6 a IPV4 en Router cisco | Routing OSPF RIPV6 [Vídeo]. YouTube.com. https://www.youtube.com/watch?v=5mWMjAIPA8o

[9] CISCO. (s. f.-b). Enlace ISL y 802.1Q entre switches de configuración fija Catalyst Layer 2 y ejemplo de configuración de switches CatOS. cisco.com. Recuperado 3 de noviembre de 2020, de https://www.cisco.com/c/en/us/support/docs/lanswitching/8021q/8758-43.html

CISCO. (s. f.-a). Configuración dinámica de opciones del servidor DHCP. Cisco.com. Recuperado 1 de noviembre de 2020, de https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/22920-dhcp-ser.html

[10] CISCO. (s. f.-b). Configurar el enlace del EtherChannel y del 802.1Q entre los switches de configuración fija del Catalyst L2 y los switches de Catalyst que ejecutan CatOS. Cisco.com. Recuperado 29 de octubre de 2020, de https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-4000-series-switches/23408-140.html

[11] Duoc UC Bibliotecas. (s. f.). Definición y propósito de la investigación aplicada. Definición y Propósito de la investigación aplicada. Recuperado 17 de noviembre de 2020, de http://www.duoc.cl/biblioteca/crai/definiciony-proposito-de-la-investigacion-aplicada.

[12] Hernández, R. Fernández, C. y Baptista, P. (2014). Metodología de la Investigación. Venezuela. McGrawHill Education.

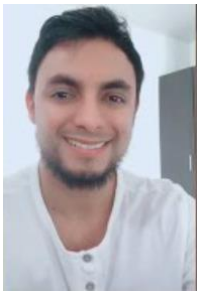
[13] Gómez, Omar S.& Aguilar Vera, Raul & Ucán Pech, Juan. (2018). Experimentación de Ingeniería de Software.

[14] Introducción al conjunto de protocolos TCP/IP. (s. f.). docs.oracle.com. Recuperado 21 de noviembre de 2020,

Obtenido de: https://docs.oracle.com/cd/E19957-01/8202981/6nei0r0r9/index.html

[15] Introducción al conjunto de protocolos TCP/IP. (s. f.). docs.oracle.com. Recuperado 21 de noviembre de 2020, de https://docs.oracle.com/cd/E19957-01/820-2981/6nei0r0r9/index.html.

VII. BIOGRAFÍA



Walter Alexander León Ortiz: nació en Neiva Huila, actualmente vive en Neiva, tiene 33 años, está cursando el décimo semestre de Ingeniería de Sistemas en la Universidad Nacional Abierta y a Distancia UNAD. Vive con su Papá Luis Leon Rubiano, actualmente trabaja a nivel virtual con la empresa de seguros "POSITIVA". Le gusta la lectura, matemáticas y las tecnologías.