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

YECID FABIÁN ALVARADO GUIO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
INGENIERÍA ELECTRÓNICA
SOGAMOSO
2021

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

YECID FABIÁN ALVARADO GUIO

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR EL TITULO DE INGENIERO ELECTRÓNICO

DIRECTOR:
ING. HECTOR MANUEL HERRERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
INGENIERÍA ELECTRÓNICA
SOGAMOSO
2021

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

FIRMA DEL PRESIDENTE DEL JURADO

_____

FIRMA DEL JURADO

_____

FIRMA DEL JURADO

SOGAMOSO 13 DE JULIO 2021

TABLA DE CONTENIDO

LISTA DE TABLAS

Pag.

LISTA DE FIGURAS

Pag.

GLOSARIO

BANNER MOTD requiere el uso de delimitadores para identificar el contenido del mensaje de aviso. El comando banner motd va seguido de un espacio y un carácter delimitador. Luego, se ingresan una o más líneas de texto para representar el mensaje del aviso.

GATEWAY predeterminado se utiliza solo cuando el host desea enviar un paquete a un dispositivo en otra red. Por lo general, la dirección de gateway predeterminado es la dirección de la interfaz del router asociada a la red local del host.

PORT-SECURITY: Es una característica de los switches Cisco que les permite retener las direcciones MAC conectadas a cada puerto del dispositivo y permitir solamente a esas direcciones MAC comunicarse a través de esa entrada del switch. Si un dispositivo con otra dirección MAC intenta comunicarse a través de esa esa entrada, port-security deshabilitará el puerto.

ROUTER: Dispositivo hardware o software de interconexión de redes de computadores que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras.

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

MÁSCARA DE SUBRED: La máscara de subred es particularmente necesaria al momento de señalar la dirección de red correspondiente a cada subred, y que es la que se encuentra referenciada en la tabla de enrutamiento.

RESUMEN

El informe de avance del escenario 1 cisco ccnp, en la prueba de habilidades nos da un conocimiento amplio sobre la utilización de las herramientas de simulación junto con los laboratorios remotos con el fin de establecer escenarios LAN/WAN que nos permite analizar sobre el comportamiento de diversos protocolos y métricas de enrutamiento

Además, busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del curso. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

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

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

ABSTRACT

The progress report of scenario 1 cisco ccnp, in the skills test gives us extensive knowledge about the use of simulation tools together with remote laboratories in order to establish LAN / WAN scenarios that allow us to analyze the behavior of various routing protocols and metrics

It also seeks to identify the degree of development of skills and abilities that were acquired throughout the course. The essential thing is to test the levels of understanding and solving problems related to various aspects of Networking.

Electronic engineers must be able to perform a highly accurate and efficient diagnosis and configuration of networks that allows them to provide solutions and answers to the various problems that information, electronic and data networks may present.

Keywords: Cisco, CCNP, Switching, Routing, Networking, Electronics

INTRODUCCIÓN

Por medio del siguiente trabajo se utiliza herramientas de simulación con el fin de establecer escenarios LAN/WAN que permitan realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento. Junto a ello identificaremos las herramientas de supervisión y protocolos de administración de red disponibles en el IOS para resolver los problemas de las redes de datos, evaluando el desempeño de routers y switches, mediante el uso de comandos especializados en gestión de redes y compatibles con el protocolo SMNP, realizaremos y diseña políticas de enrutamiento estático y/o dinámico (RIP y OSPF), bajo un esquema de direccionamiento IP sin clase, para dar soluciones de red y conectividad escalables, mediante el uso de los principios de enrutamiento y conmutación de paquetes en ambientes LAN y WAN junto con configura esquemas de conmutación, mediante el uso de protocolos basados en STP y VLANs en escenarios corporativos y residenciales, con el fin de comprender el modo de operación de las VLAN y las bondades de administrardominios Y por último diseñaremos un esquema de direccionamiento IP para proporcionar conectividad; seguridad y acceso a la WAN mediante el uso del protocolo DHCP; listas de control de acceso y traducción de direcciones IP sobre NAT-PAT

2. DESARROLLO DEL PROYECTO

2.1.Escenario 1

Topología

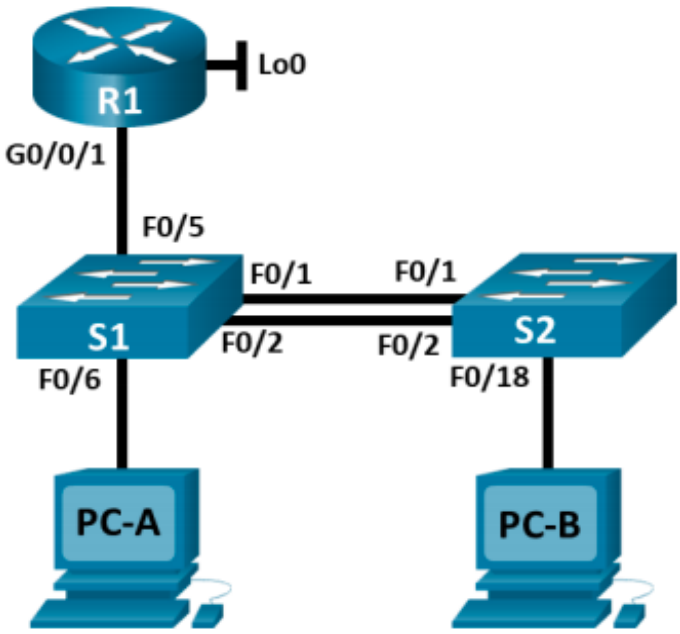

Figura 1 - fuente prueba de habilidades

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.

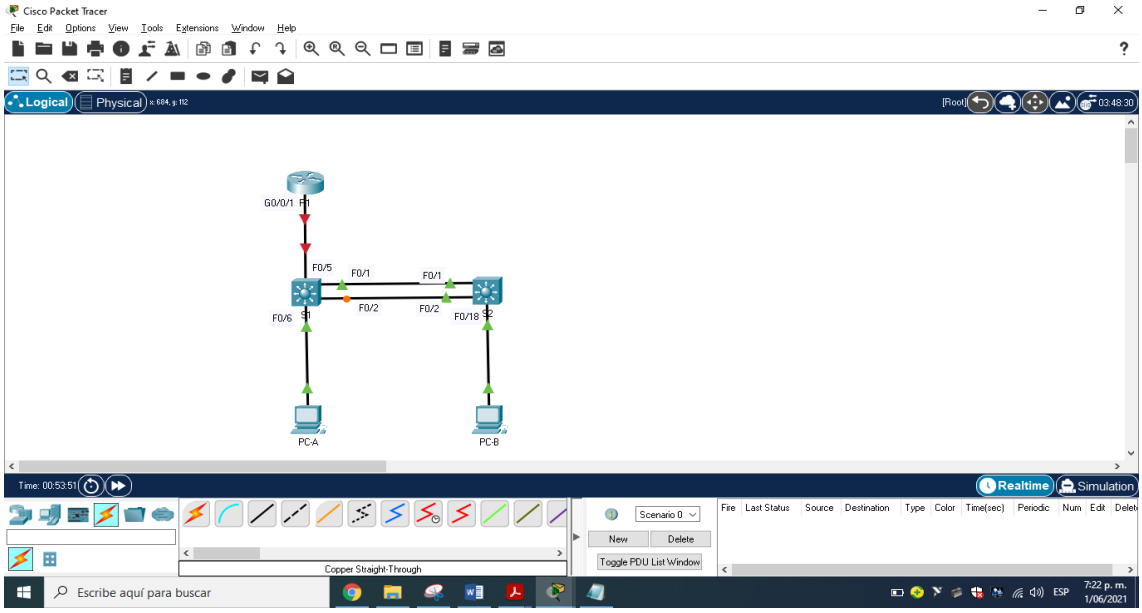

Figura 2. Simulación: fuente propia

EXPLICACIÓN

Creamos la topología en el simulador, empezamos a agregar en el simulador un (1) router 4331 dos (2) switchs 3560 porque necesitamos ipv6, dos (2) pc y cables para conectar los dispositivos

Tabla 1 de VLAN

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

Tabla 2 de asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.21.5.1 /26	No corresponde
	2001:db5:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.21.5.65 /27	No corresponde
	2001:db5:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.21.5.97 /29	No corresponde
	2001:db5: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	10.21.5.98 /29	10.21.5.97
	2001:db5:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.21.5.99 /29	10.21.5.97
	2001:db5: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:db5:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db5:acad:b: :50 /64	fe80::1

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

Instrucciones

2.1.1. Parte 1: Inicializar y Recargar y Configurar aspectos básicos de los dispositivos
2.1.1.1. Paso 1: Inicializar y volver a cargar el router y el switch

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

Desarrollo parte 1, paso 1

Ingresamos al modo privilegiado y escribimos: enable
Después estableceremos los valores predeterminados escribimos: erase startup-config

Posteriormente Reiniciamos el Router escribiremos: reload
Y así podremos ingresar nuestros valores

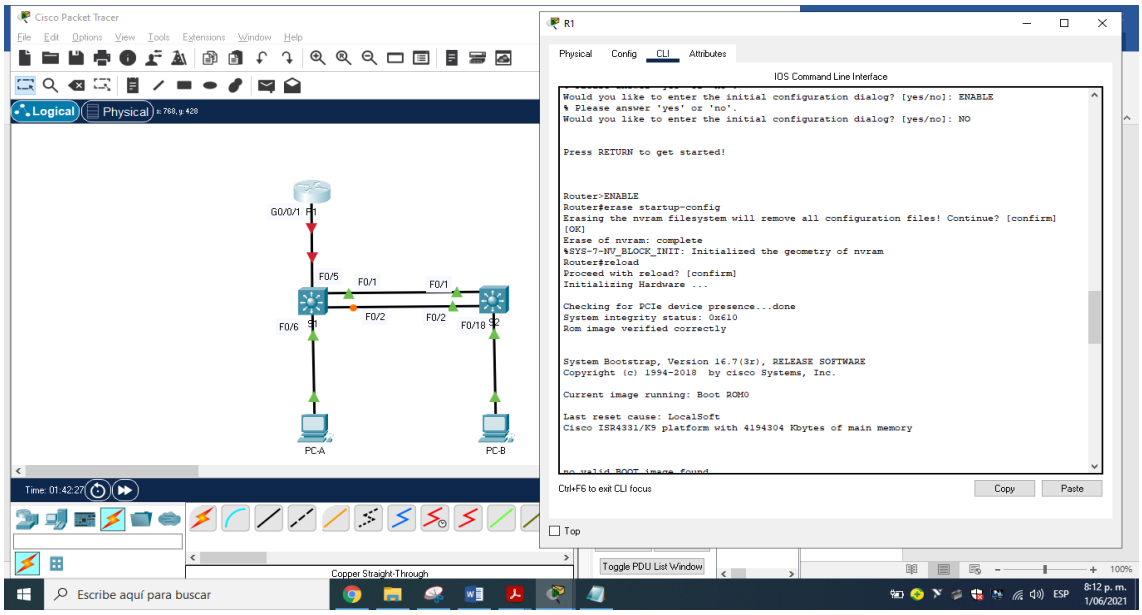

Figura 3. Carga e inicialización de R1: fuente propia

Posteriormente ingresamos a S 1 y S 2 en modo privilegiado e ingresamos comando erase startup-config este eliminara lo que posee la NVRAM igual que el comando delete vlan.dat el cual elimina los datos de la vlan.

Con este procedimiento restaurara el switch y elimina la configuración de inicio, luego reiniciaremos con reload, Y así podremos ingresar nuestros valores.

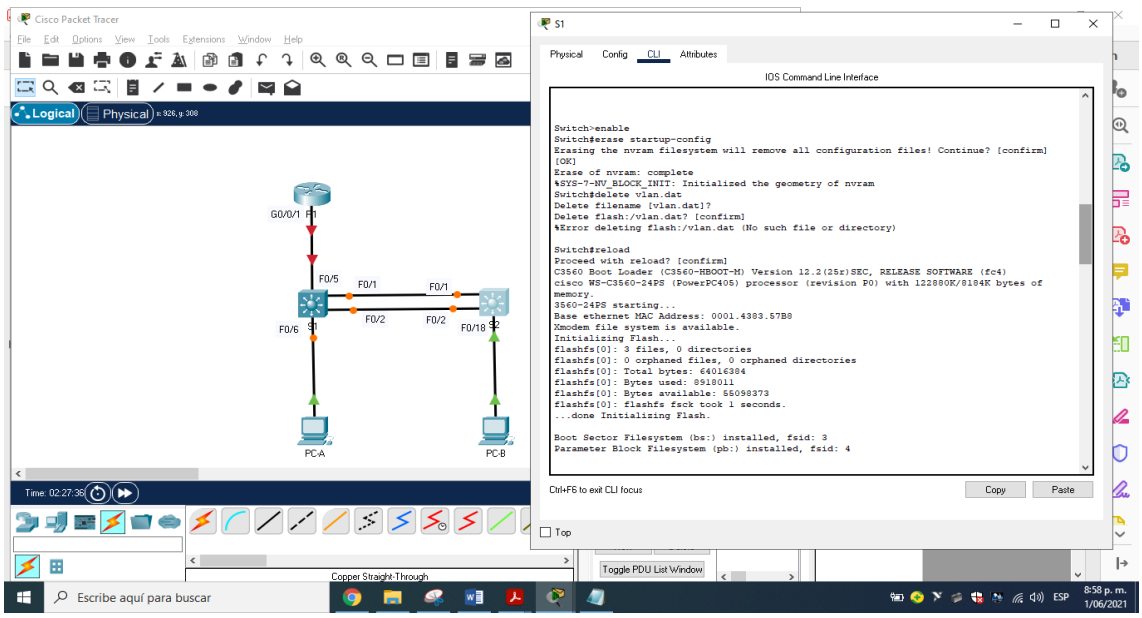

Figura 4. Carga e inicialización de S1: fuente propia

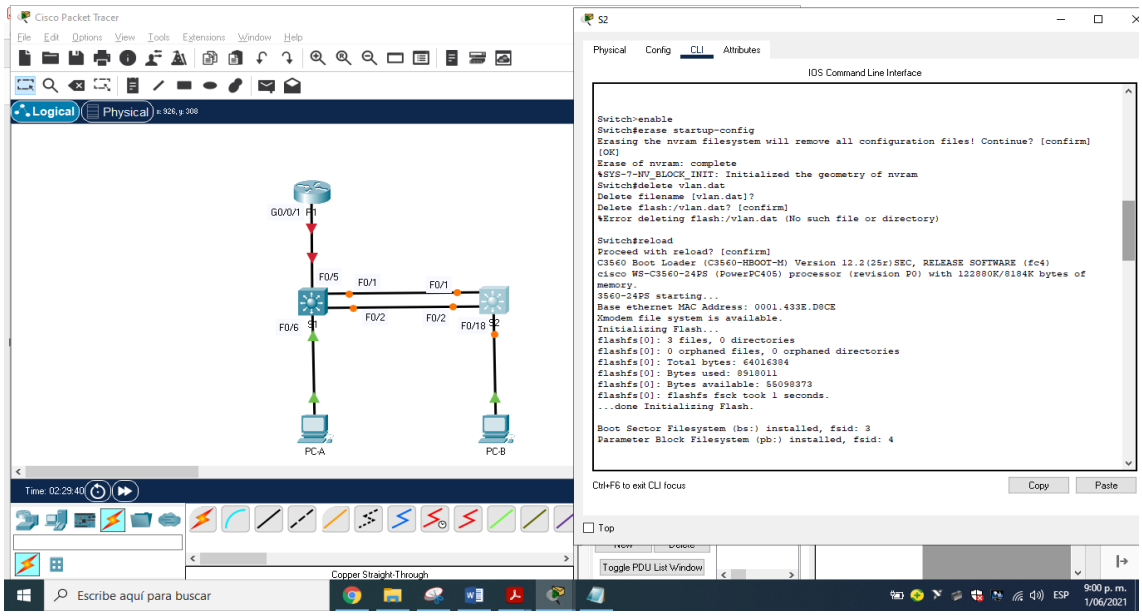

Figura 5. Carga e inicialización de S2: fuente propia

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

Como el Switch Cisco 3560 no soporta IPv6 configuraremos SDM para que admita IPv6 junto con IPv4, se confirma desde el modo privilegiado escribimos enable la configuración con el comando show sdm prefer, y nos damos cuenta que solo admite IPv4, por consiguiente, activaremos la configuración IPv6 realizamos el comando config terminal y luego sdm prefer dual-ipv4-and-ipv6 default, luego escribimos exit y reiniciamos con el comando reload para que soporte IPv4 y IPv6.

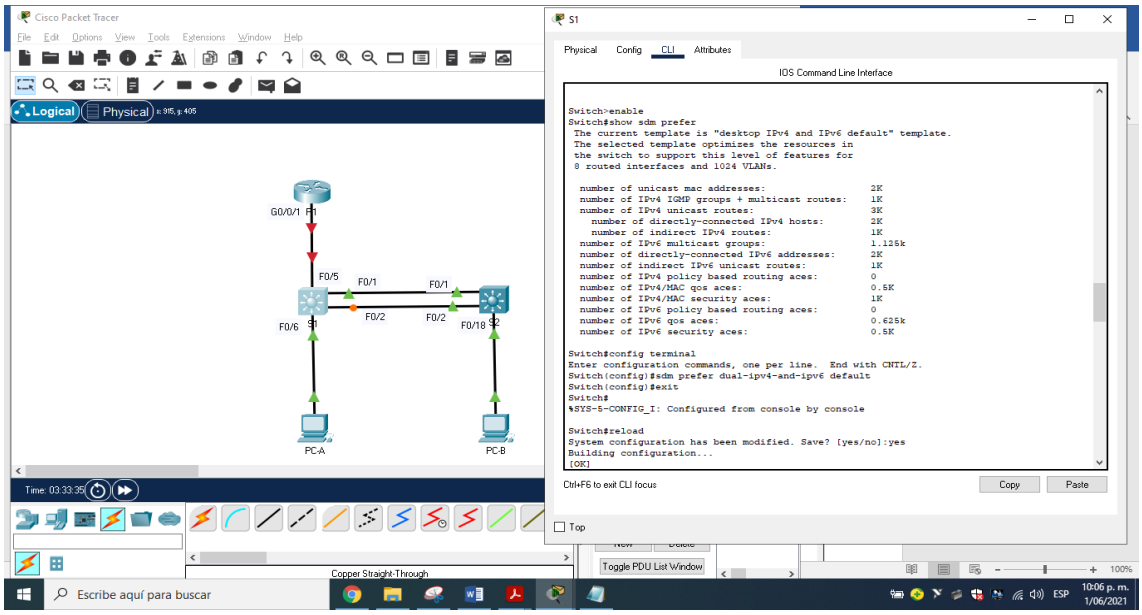

Figura 6. configuración IPv6 : fuente propia

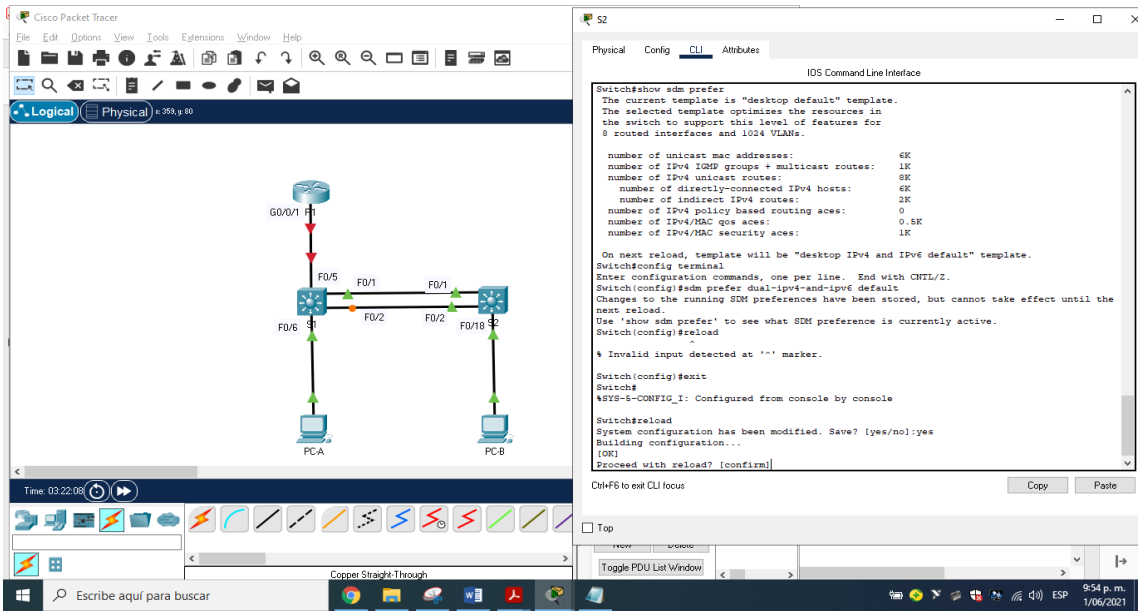

Figura 7. configuración IPv6 : fuente propia

2.2. Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3. Tareas de configuración para el Router R1

Tarea	Especificación	solución
Desactivar la búsqueda DNS		Router(config)#no ip domain lookup
Nombre del router	R1	Router(config)#hostname R1
Nombre de dominio	ccna-lab.com	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	ciscoconpass	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	10 caracteres	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin	R1(config)# username admin secret admin1pass

	Password: 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)#description vlan Bikes R1(config-subif)#ip address 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 address FE80::1 link-local R1(config-subif)# interface g0/0/1.3 R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#description vlan Trikes R1(config-subif)#ip address 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address FE80::1 link-local R1(config-subif)#interface g0/0/1.4 R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#description vlan Management R1(config-subif)#ip address 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 address FE80::1 link-local R1(config-subif)#interface g0/0/1.6

		R1(config-subif)#encapsulation dot1q 6 Native R1(config-subif)#description vlan Native R1(config-subif)#interface g0/0/1 R1(config-if)#no shutdown
Configure el Loopback0 interface	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como fe80::1	R1(config-if)# interface loopback 0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address FE80::1 link-local R1(config-if)#description Internet R1(config-if)#exit
Generar una clave de cifrado RSA	Módulo de 1024 bits	R1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024

Para este paso ingresamos modo privilegiado escribimos no ip domain lookup que desactivar la búsqueda DNS la cual nos comunicara si comentemos un error colocaremos el nombre del mecanismo y dominio con su contraseña cifrada para entrar al modo privilegiado por medio del comando enable secret, igualmente instalaremos la contraseña para entrar a la consola, por medio del comando password y encendiéndola con login, por otro lado estableceremos una longitud mínima de 10 caracteres para las contraseñas con el comando security passwords min-length 10, crearemos un usuario administrativo en la base de datos local. usuario y contraseña y Configuraremos el inicio de sesión en las líneas VTY para que use la base de datos local con line vty 0 15 y encendiéndolas con login local, Configurar las líneas VTY para que acepten únicamente las conexiones SSH escribiendo transport input ssh, posteriormente salimos de vty y configuraremos contraseñas de texto no cifrado escribiendo service password-encryption, si alguna persona extraña quiere manipular el sistema se mostrara en el banner MOTD solo acceso autorizado, Se realiza una llave de encriptación RSA con crypto key generate rsa colocando longitud de 1024 bits, se configura la Interfaz administrativa (SVI) correspondiente a la vlan 4 Management asignándole la IPv4 10.19.8.98 y mascara de red 255.255.255.248, dirección IPv6 2001:db8:acad:c::98 prefijo /64 y puerta de enlace local fe80::98, se coloca un descripción y se enciende con no shutdown, por último se configura la puerta de enlace predeterminada 10.19.8.97 para IPv4, no se configura puerta de enlace en IPv6 porque se asigna de manera automática. se encenderá el enrutamiento IPv6 escribiendo ipv6 unicast-routing, configuraremos la interfaz G0/0/1 y configuraremos las subinterfaces colocando la encapsulación con su vlan respectiva con la dirección IPv4, IPv6 y enlace local

IPv6, con las interface g0/0/1.2, g0/0/1.3, g0/0/1.4, g0/0/1.6, a la última interface se le asignará la vlan nativa y por último se enciende la interfaz G0/0/1 escribiendo no shutdown, se establece la interface Loopback0 (Internet) interface loopback y/o colocándole la dirección IPv4, IPv6 y local.

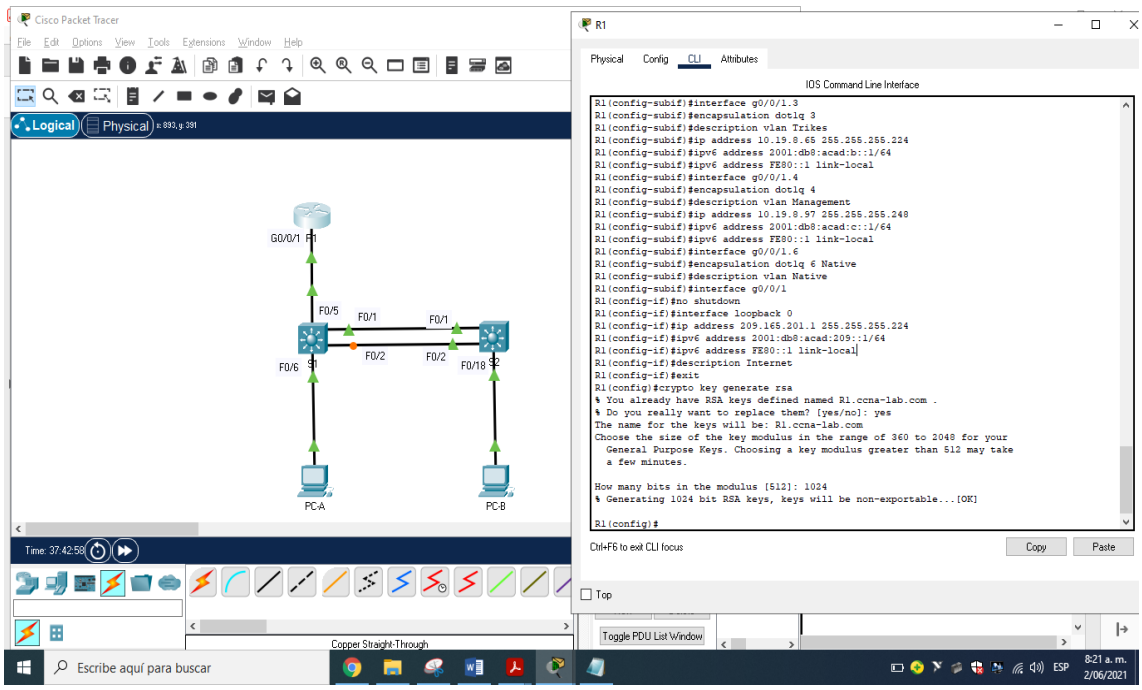

Figura 8. configuración parámetros R1 : fuente propia

Verificamos nuestros r1 con la siguiente función

R1#show running-config

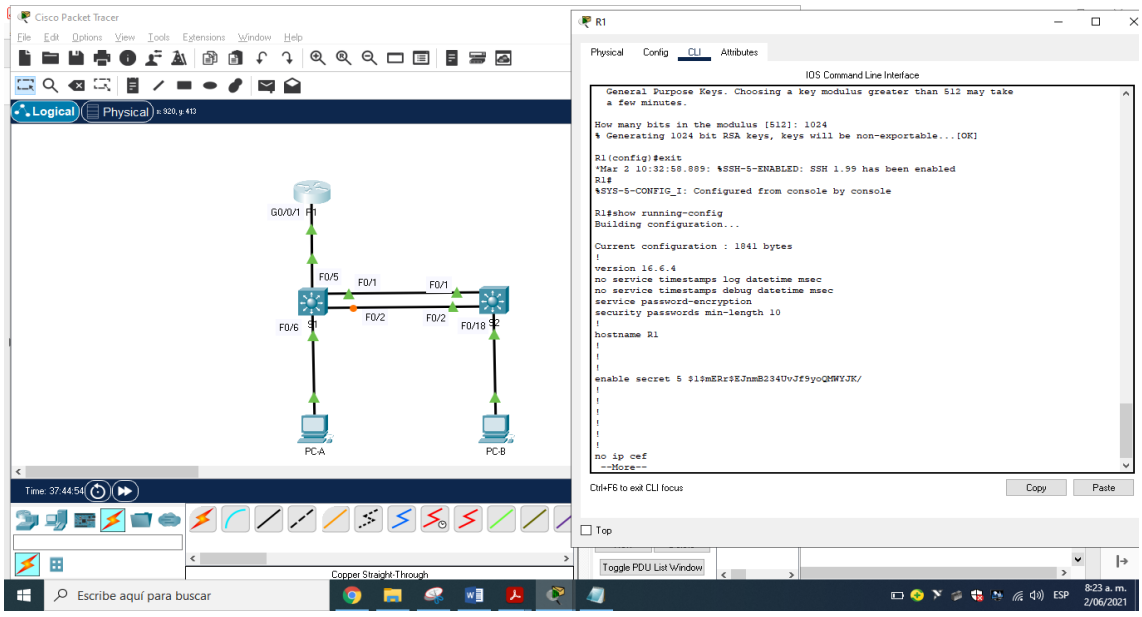

Figura 9. verificando R1 : fuente propia

2.3. Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Configurando s1

Tabla 4. Tareas de configuración para el Switch, S1

Tarea	Especificación	solución
Desactivar la búsqueda DNS		S1(config)#no ip domain lookup
Nombre del router	S1 o S2, según proceda	S1(config)#hostname S1
Nombre de dominio	ccna-lab.com	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	ciscoconpass	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass	S1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local		S1(config)#line vty 0 15 S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH		S1(config-line)#transport input ssh S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado		S1(config)#service password-encryption
Configurar un MOTD Banner		S1(config)#banner motd "Solo Acceso Autorizado"

Generar una clave de cifrado RSA	Módulo de 1024 bits	S1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2 Establecer la dirección IPv6 de capa 3	S1(config)#interface vlan 4 S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address FE80::98 link-local S1(config-if)#description vlan Management S1(config-if)#no shutdown S1(config-if)#exit
Configuración del gateway predeterminado	Configure la puerta de enlace predetermina da como 10.21.5.97 para IPv4	S1(config)#ip default-gateway 10.19.8.97

Para este paso ingresamos modo privilegiado escribimos no ip domain lookup que desactivar la búsqueda DNS la cual nos comunicara si comentemos un error colocaremos el nombre del mecanismo y dominio con su contraseña cifrada para entrar al modo privilegiado por medio del comando enable secret, igualmente instalaremos la contraseña para entrar a la consola, por medio del comando password y encendiéndola con login, por otro lado estableceremos una longitud mínima de 10 caracteres para las contraseñas con el comando security passwords min-length 10, crearemos un usuario administrativo en la base de datos local. usuario y contraseña y Configuraremos el inicio de sesión en las líneas VTY para que use la base de datos local con line vty 0 15 y encendiéndolas con login local, Configurar las líneas VTY para que acepten únicamente las conexiones SSH escribiendo transport input ssh, posteriormente salimos de vty y configuraremos contraseñas de texto no cifrado escribiendo service password-encryption, si alguna persona extraña quiere manipular el sistema se mostrara en el banner MOTD solo acceso autorizado, Se realiza una llave de encriptación RSA con crypto key generate rsa colocando longitud de 1024 bits, se configura la Interfaz administrativa (SVI) correspondiente a la vlan 4 Management asignándole la IPv4 10.19.8.98 y mascara de red 255.255.255.248, dirección IPv6 2001:db8:acad:c::98 prefijo /64 y puerta de enlace local fe80::98, se coloca un descripción y se enciende con no shutdown, por último se configura la puerta de enlace predeterminada 10.19.8.97 para IPv4, no se configura puerta de enlace en IPv6 porque se asigna de manera automática.

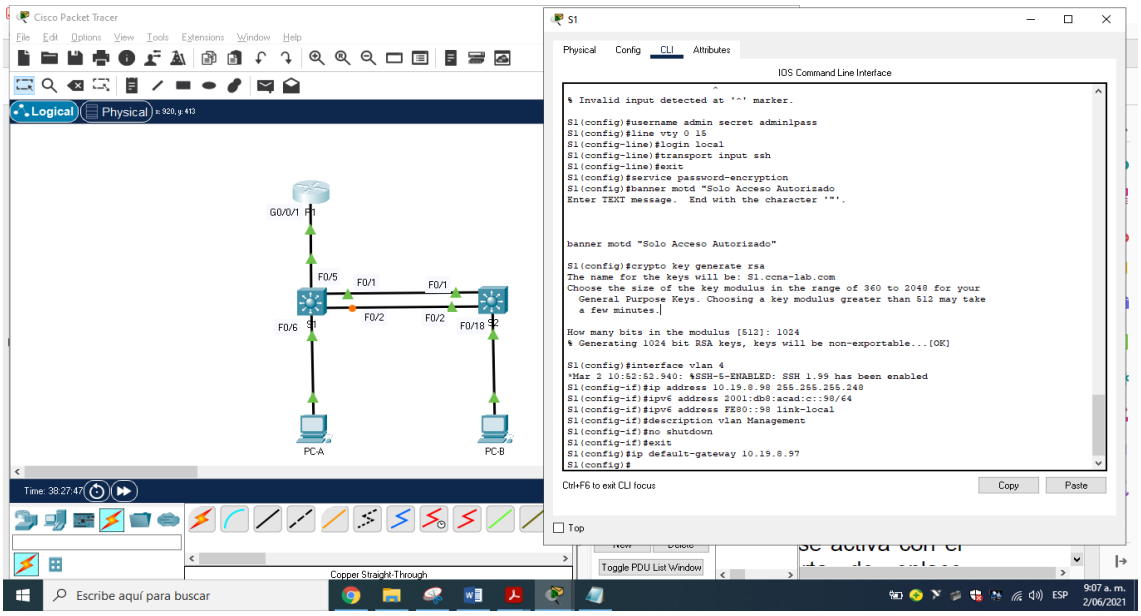

Figura 10. configuración parámetros S1 : fuente propia

Verificamos nuestros S1 con la siguiente función

s1#show running-config

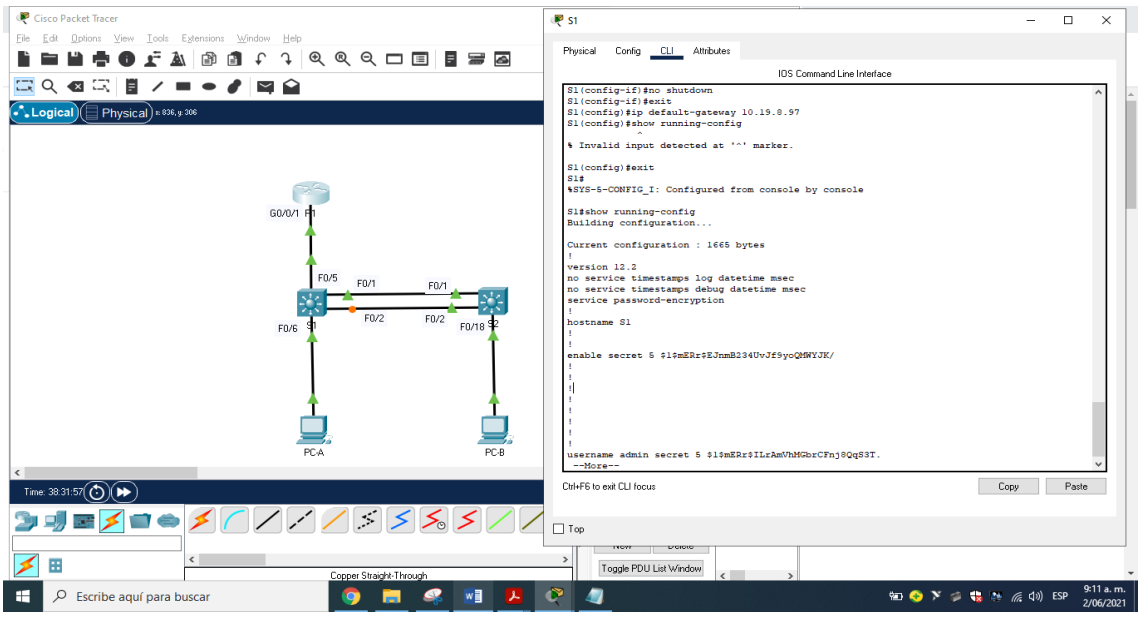

Figura 11. Verificando S1: fuente propia

Realizamos el mismo procedimiento anterior y con la misma tabla para el s2

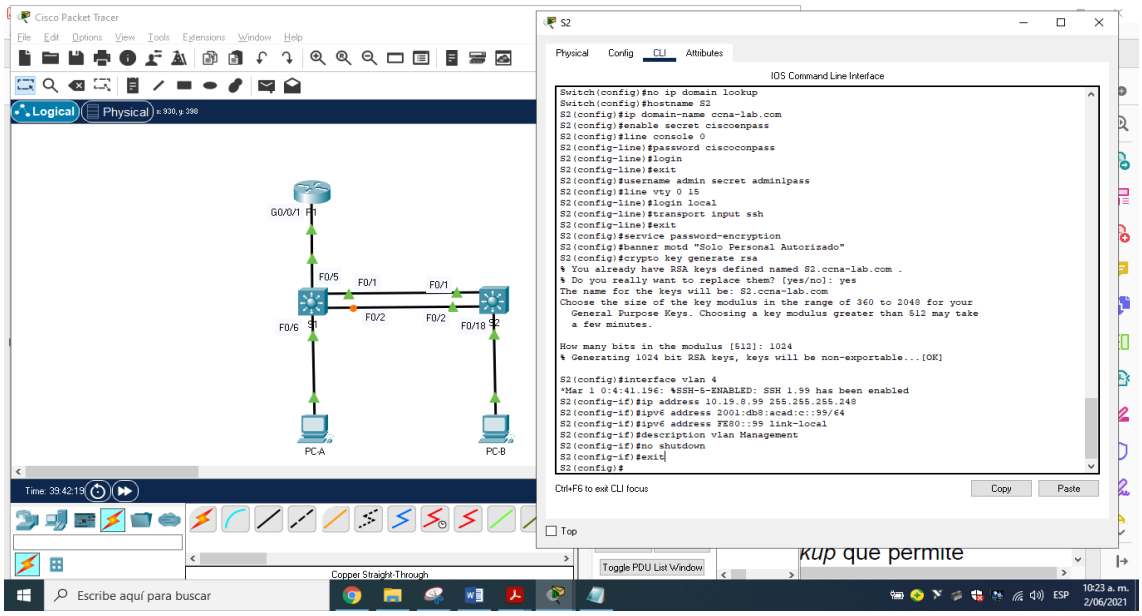

Figura 12. configuración parámetros S2: fuente propia

Verificamos nuestros S2 con la siguiente función

S2#show running-config

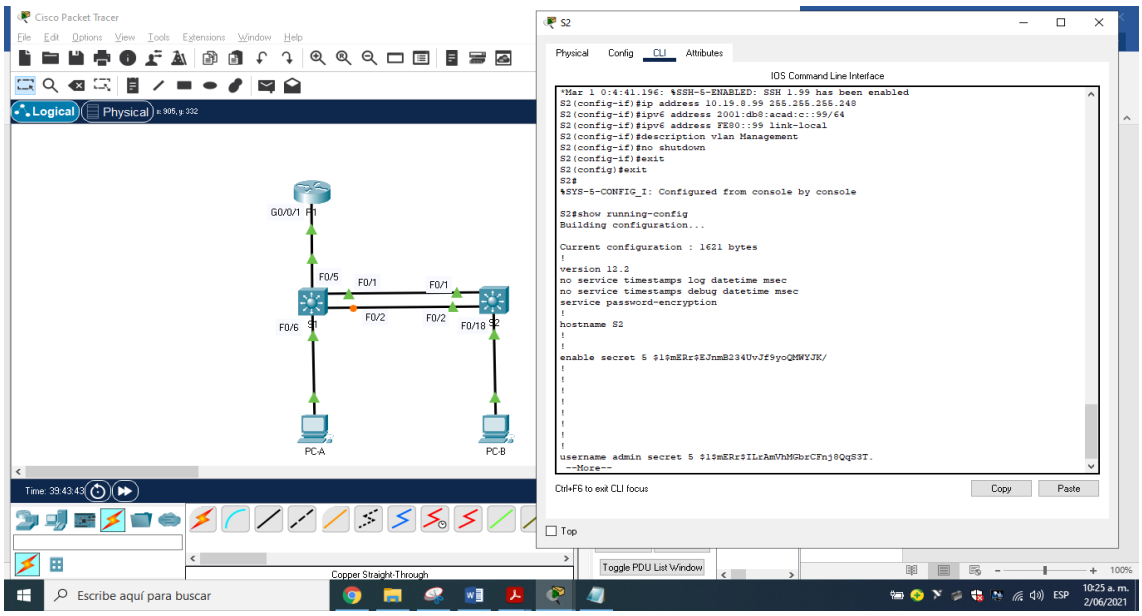

Figura 13. Verificando S2: fuente propia

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

2.1. Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 5. Tareas de configuración VLAN y troncales para el Switch S1

Tarea	Especificación	solucion
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	S1#configure terminal S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#vlan 4 S1(config-vlan)#name Management S1(config-vlan)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#vlan 6 S1(config-vlan)#name Native S1(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5	S1(config)#interface fa0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#interface range fa0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6

Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación	S1(config)#interface range fa0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)# S1(config-if-range)#interface Port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6	S1(config-if)#interface fa0/6 S1(config-if)#switchport mode acces S1(config-if)#switchport acces vlan 2
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC	S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S1(config-if-range)#interface range fa0/3-4 S1(config-if-range)#switchport acces vlan 5 S1(config-if-range)#description No esta en uso S1(config-if-range)#shutdown S1(config-if-range)#interface range fa0/7-24 S1(config-if-range)#switchport acces vlan 5 S1(config-if-range)#description No esta en uso S1(config-if-range)#shutdown S1(config-if-range)#interface range g0/1-2

		S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description No esta en uso S1(config-if-range)#shutdown

Para esta parte del escenario lo primero que debemos hacer es escribir enable damos enter, después escribimos configure terminal damos enter y creamos vlan 2, damos enter y escribimos name Bikes, enter y asi sucesivamente con los otros comandos vlan 3-Trikes, vlan 4-Management, vlan 5-Parking y vlan 6-Native, salimos con exit

Para la creación de troncos 802.1Q que utilicen la vlan 6 nativa interfaces fa0/1, fa0/2 y fa0/5, primero configuraremos la interface fa0/5 utilizando comando de encapsulación switchport trunk encapsulation dot1q, posteriormente realizaremos la interface con switchport mode trunk direccionándola a la vlan 6 nativa switchport trunk native vlan 6, luego configuraremos las fa0/1 y fa0/2 usando el rango interface range fa0/1-2, por tanto se configura la EtherChannel se apaga el rango anterior con shutdown para no tener problemas, se programa range fa0/1-2 con switchport trunk encapsulation dot1q, y luego utilizamos el código switchport mode trunk dirijiendo a vlan 6 nativa switchport trunk native vlan 6, después creamos EtherChannel escribiendo fa0/1-2 con channel-group 1 mode active y usar LACP creando el grupo 1, posteriormente entramos con interface Port-channel 1 y programamos los troncos, configuramos vlan 2- Bikes que utilice fa0/2 con switchport acces vlan 2, configuramos en los puertos de aceso que admita 3 direcciones MAC, se inicia la interfaz creando máximo 3 direcciones MAC con switchport port-security maximum 3, se afirman las interfaces sin utilizar determinandolas a vlan 5-Parking mostrando que no se usan y apagamos con shutdown, estas son fa0/3-4, fa0/7-24 y g0/1-2,por ultimo encendemos el fa0/1-2 con no shutdown.

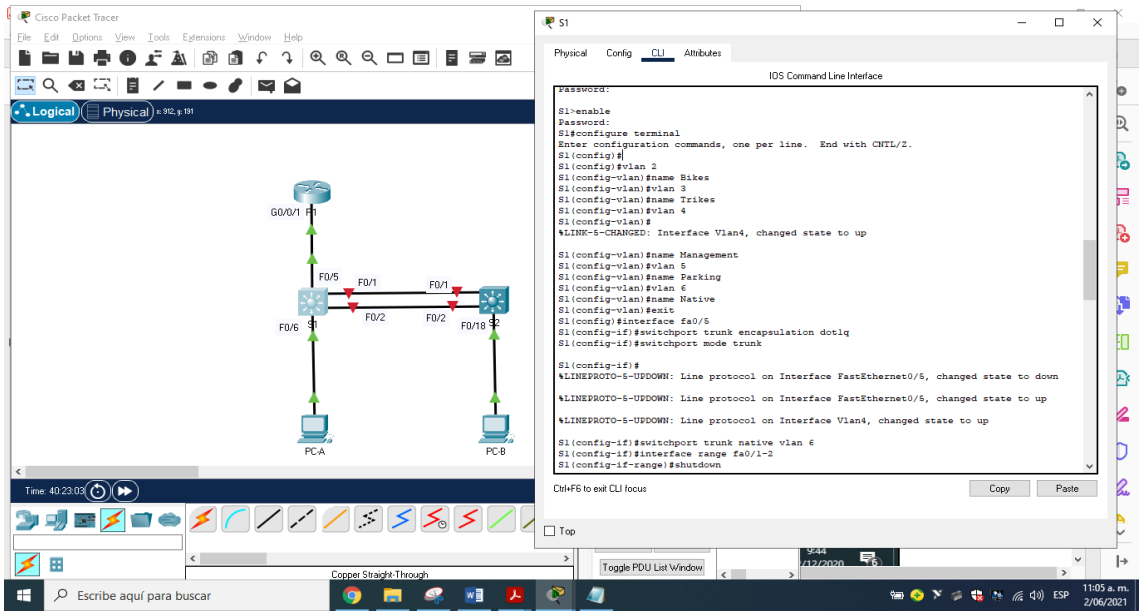

Figura 14. configuración de red S1: fuente propia

2.2. Paso 5: Configure el S2

Tabla 6. Tareas de configuración VLAN y troncales para el Switch S2

Tarea	Especificación	solucion
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	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 F0/1y 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 de host para VLAN 3	Interface F0/18	S2(config-if)# interface fa0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
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	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

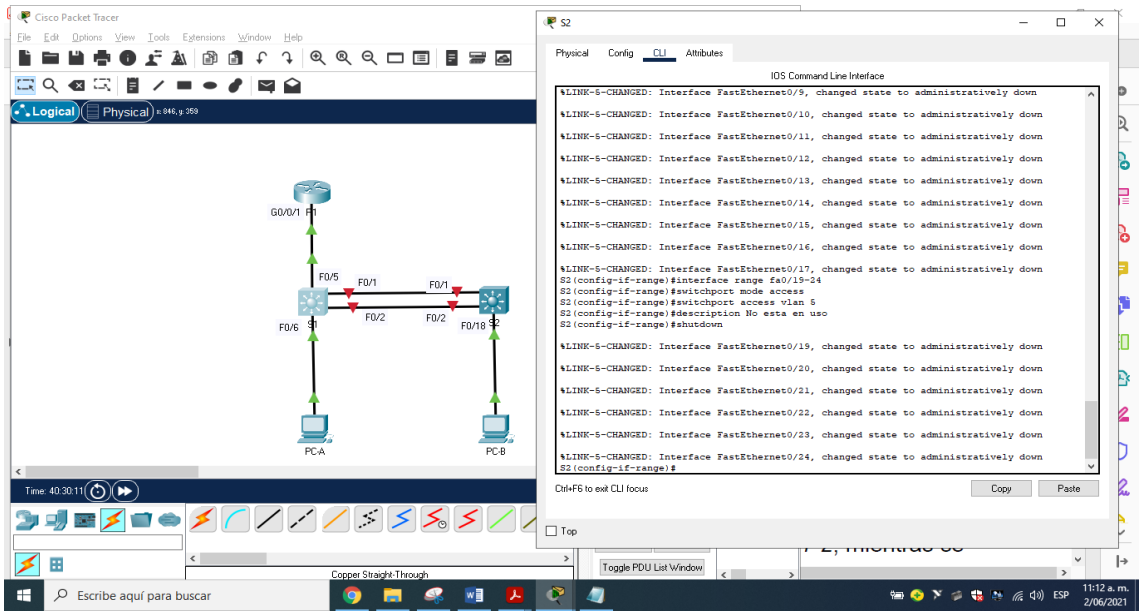

Figura 15. configuración de red S2: fuente propia

3. Parte 3: Configurar soporte de host

3.1. Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 7. Tareas de configuración DHCP Router R1

Tarea	Especificación	solucion
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.	R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84 R1(config)#ip dhcp pool vlan3-Trikes

	Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada	R1(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

Para esta parte del proceso al Router se programa con rutas predeterminadas IPv4 ip route 0.0.0.0 0.0.0.0 loopback 0 y IPv6 ipv6 route ::/0 loopback 0, y estas direccionan la interfaz Loopback 0 (Lo0), y ellas serian rutas estáticas para conectar el Internet, se progrma IPv4 DCHP para vlan 2-Bikes conformando por las ultimas 10 direcciones de subred las cuales están en los limites 10.19.8.1 – 10.19.8.52, para lo cual se aplica, para quitar 10 direcciones el comando ip dhcp excluded-address 10.19.8.1 10.19.8.52, y luego el pool de DHCP ip dhcp pool vlan2-Bikes, red y mascara de red network 10.19.8.0 255.255.255.192, puerta de enlace predeterminada default-router 10.19.8.1, nombre de dominio domain-name ccna-a.net, por ultimo se configura DHCP IPv4 para vlan 3-Trikes y grupo DHCP conformado por las ultimas 10 direcciones con sus respectivas especificaciones, se configura IPv4 DCHP para vlan 3-Trikes conformado solamente las ultimas 10 direcciones de subred la cual está en el rango 10.19.8.65 – 10.19.8.84, para ello se aplicara para quitar estas 10 direcciones el comando ip dhcp excluded-address 10.19.8.65 10.19.8.84, y para el pool de DHCP ip dhcp pool vlan3-Trikes, red y mascara de red network 10.19.8.64 255.255.255.224, puerta de enlace predeterminada default-router 10.19.8.65, nombre de dominio domain-name ccna-b.net.

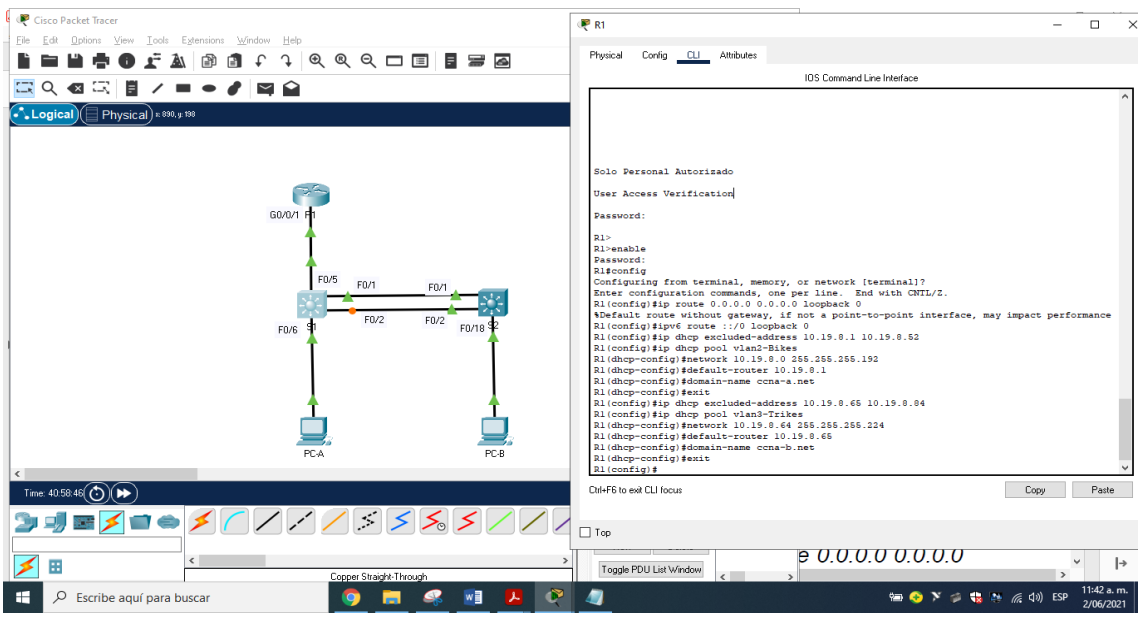

Figura 16. Configuración de soporte de host R1: fuente propia

3.2. Paso 2: Configurar los servidores

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

En las PC-A y PCB se enciende el DHCP para IPv4 y instrucción para IPv6

Tabla 8. Configuración PC-A DHCP

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

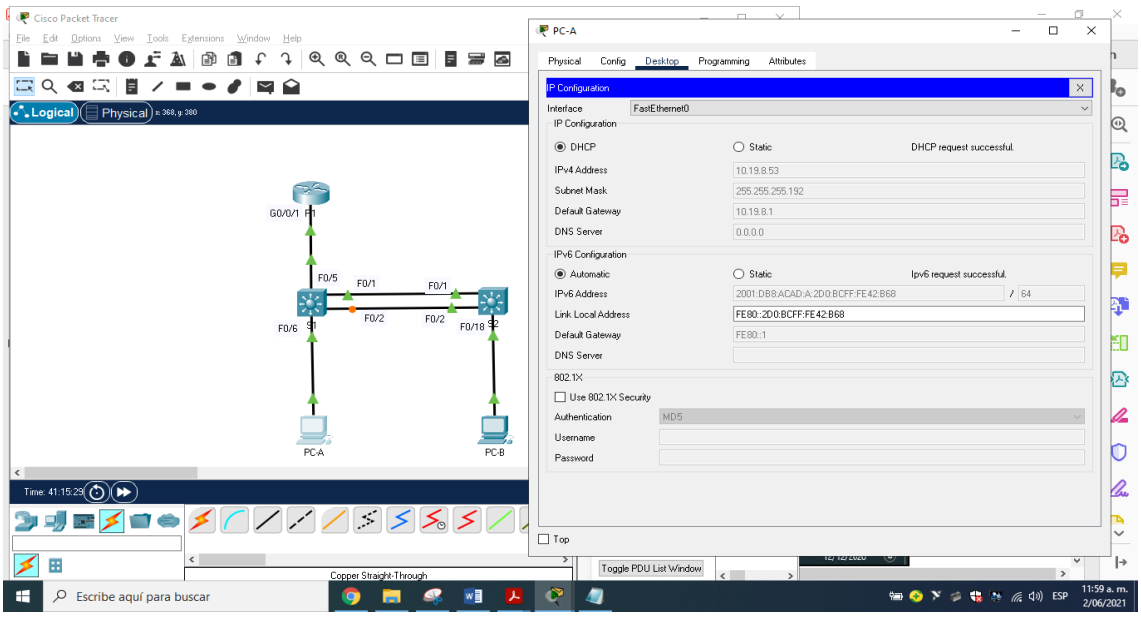

Figura 17. Configuración PC-A: fuente propia

Tabla 9. Configuración PC-A DHCP

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

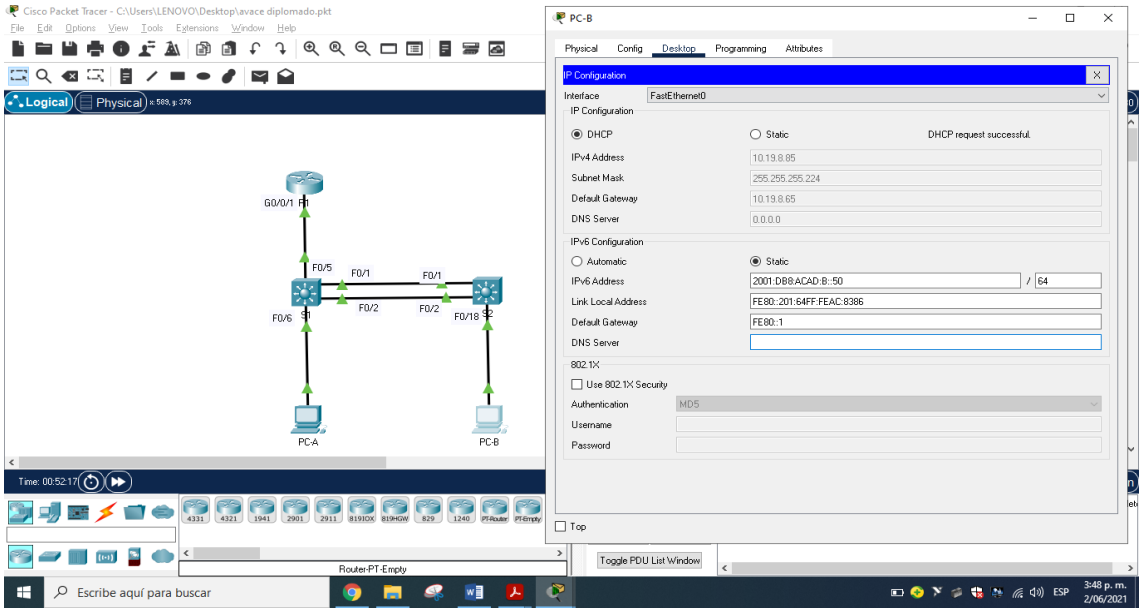

Figura 18. Configuración PC-B: fuente propia

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

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

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

Tabla 10. Verificación de las configuraciones y conectividad extremo a extremo

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

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

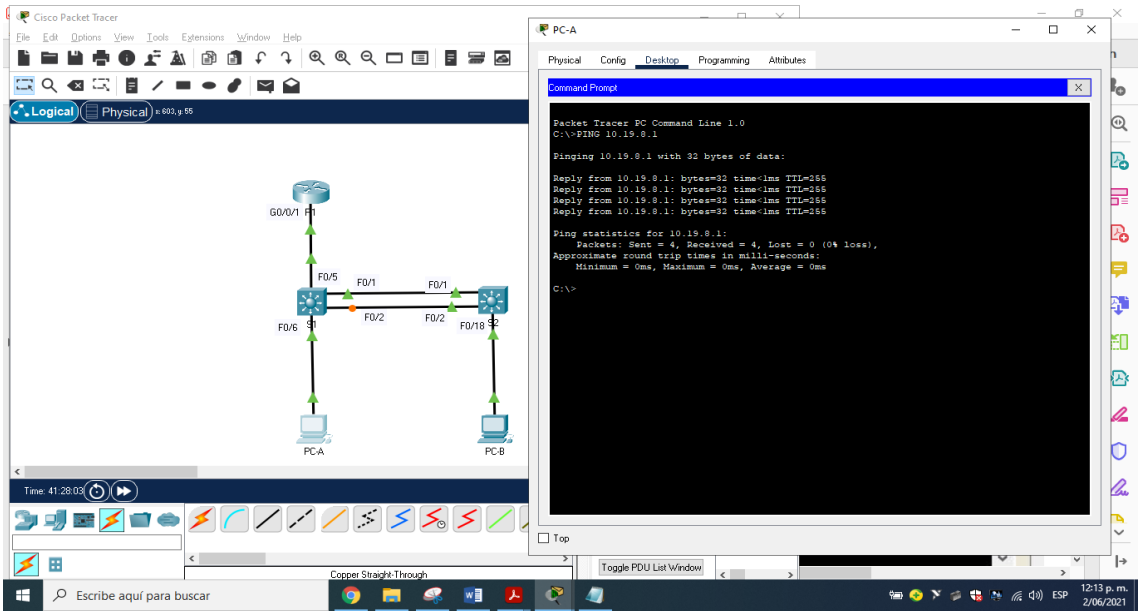

Figura 19. Ping desde PC-A a R1, G0/0/1.2 de internet Dirección a dirección ip 10.19.8.1 - fuente propia

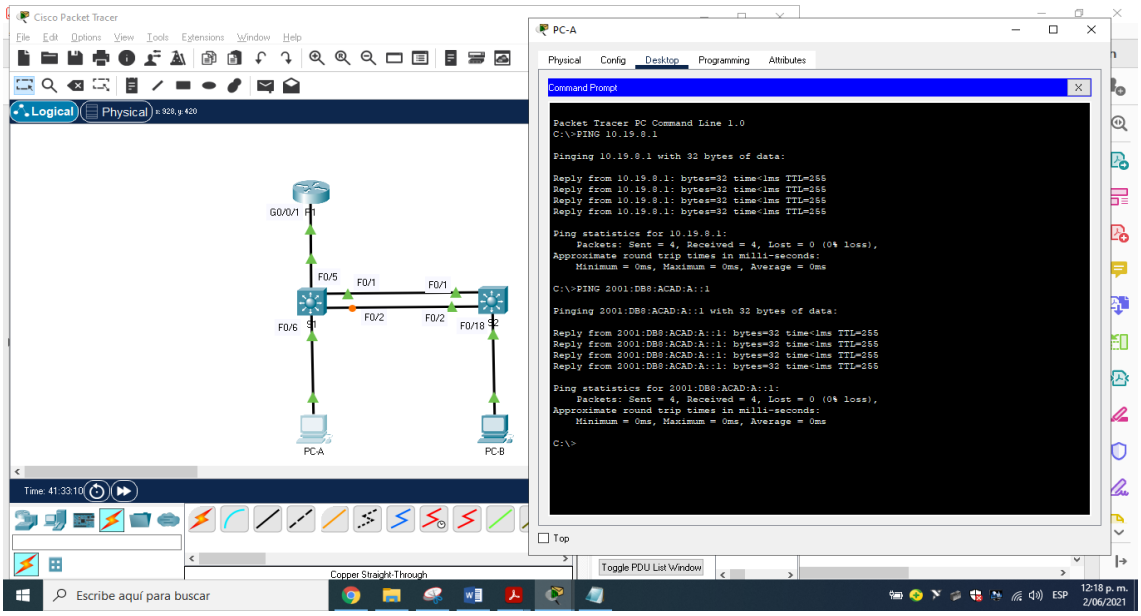

Figura 20. Ping desde PC-A a R1, G0/0/1.2 de internet Ipv6 a dirección ip 2001:db8:acad:a::1 - fuente propia.

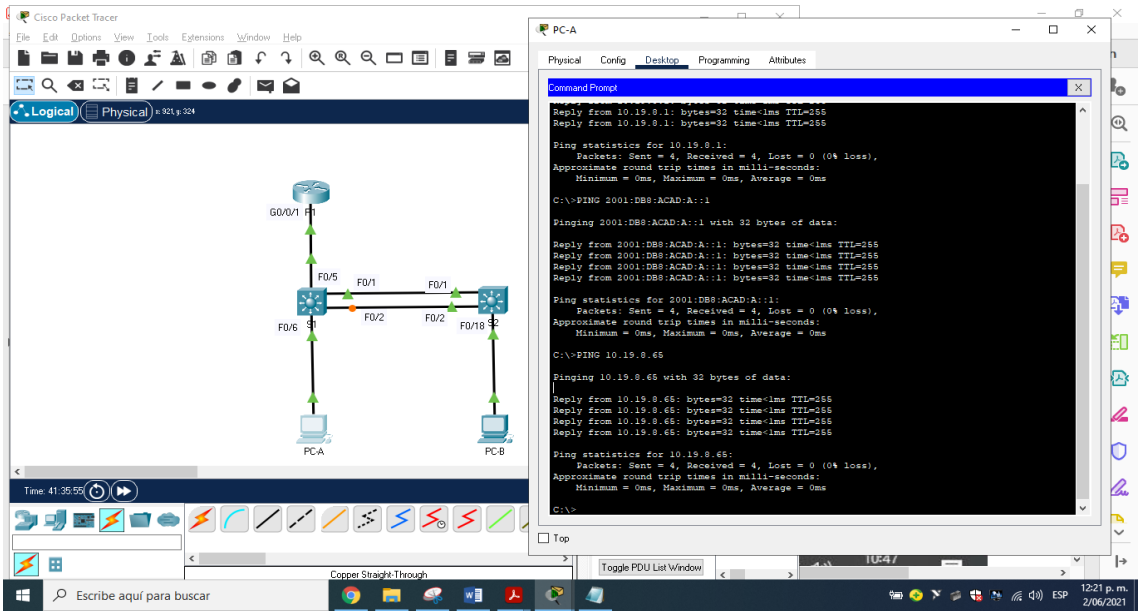

Figura 21. Ping desde PC-A a R1, G0/0/1.3 de internet Dirección a dirección ip 10.19.8.65 - fuente propia.

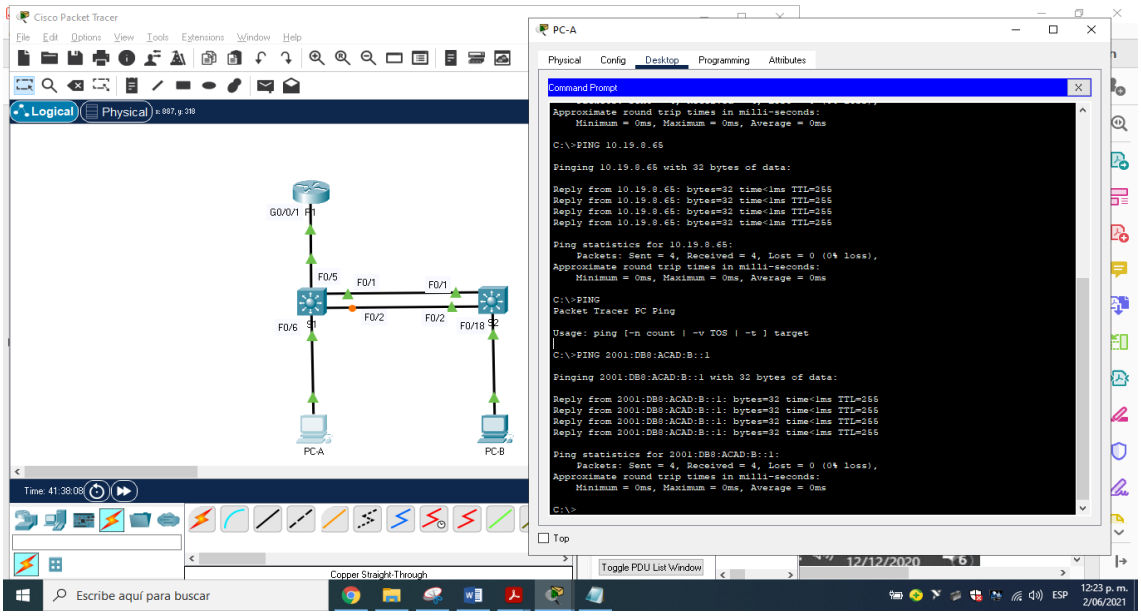

Figura 22. Ping desde PC-A a R1, G0/0/1.3 de internet Ipv6 a dirección ip 2001:db8:acad:b::1 - fuente propia.

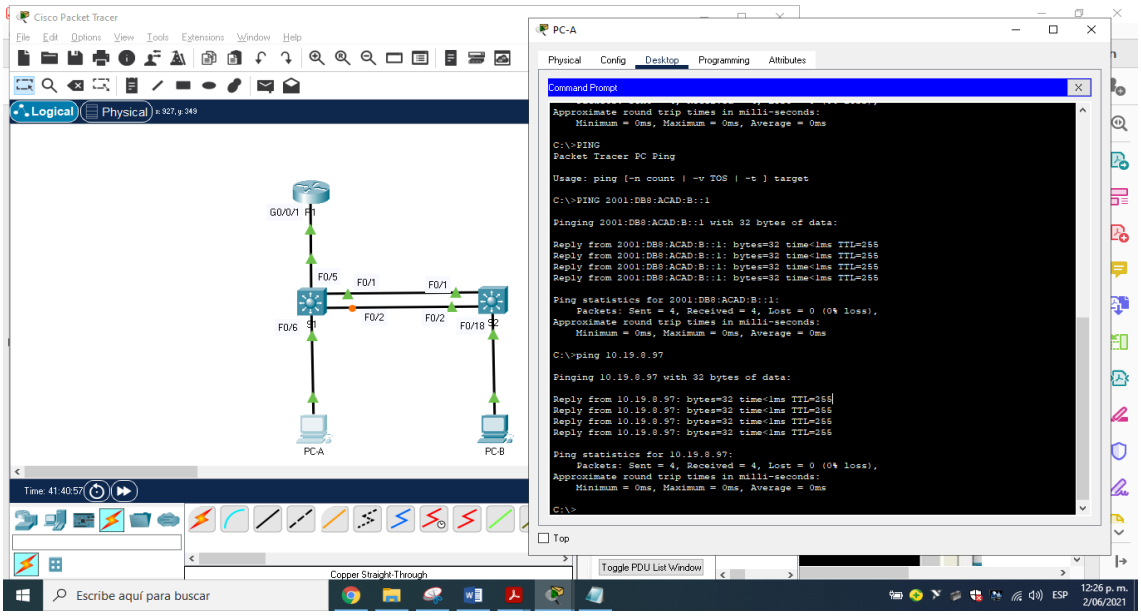

Figura 23. Ping desde PC-A a R1, G0/0/1.4 de internet Dirección a dirección ip 10.19.8.97 - fuente propia

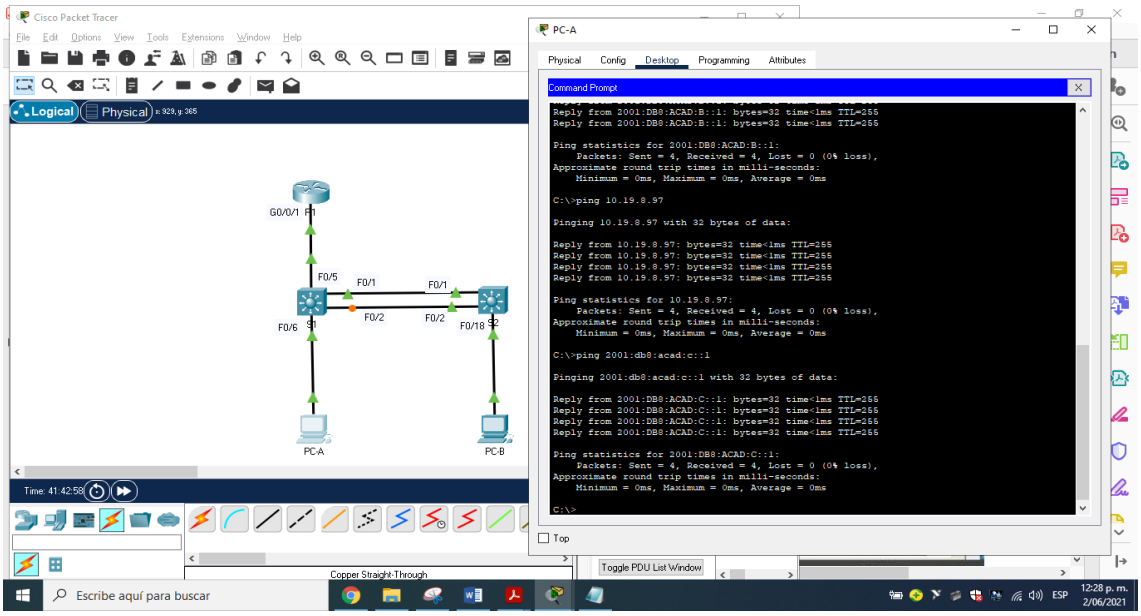

Figura 24. Ping desde PC-A a R1, G0/0/1.4 de internet Ipv6 de dirección ip 2001:db8:acad:c::1 – fuente propia

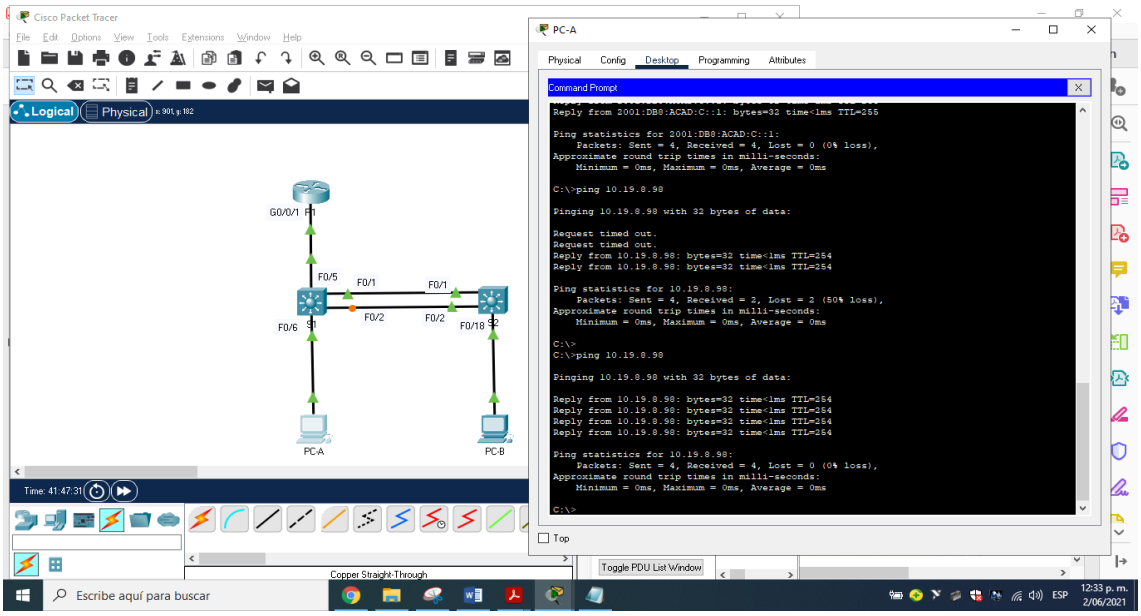

Figura 25. Ping desde PC-A a S1 VLAN4 de internet Dirección a dirección ip 10.19.8.98 - fuente propia

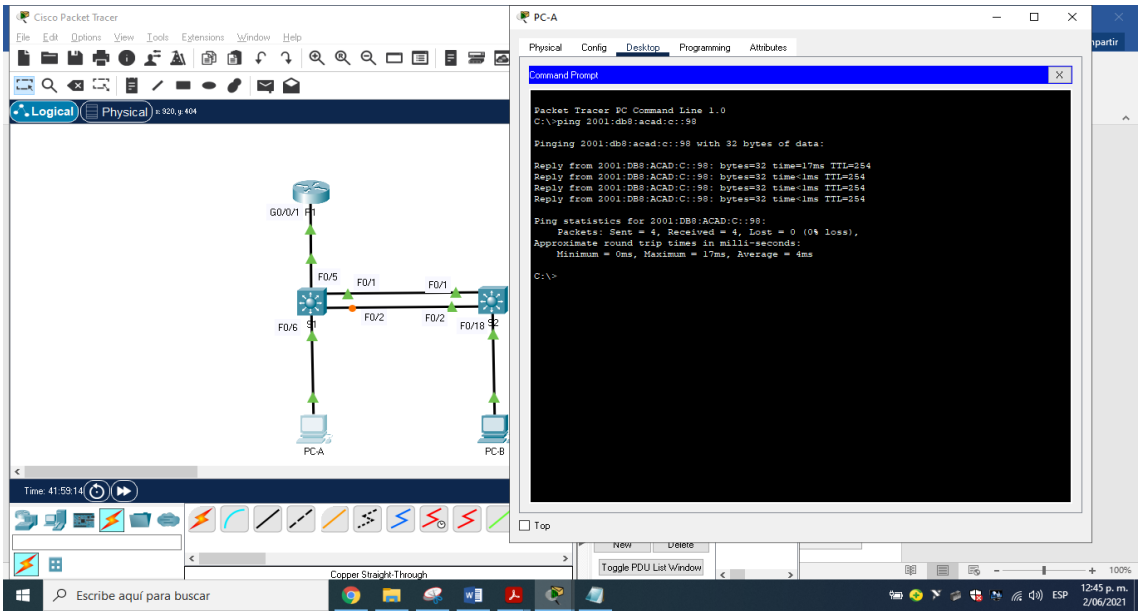

Figura 26. Ping PC-A a S1 VLAN4 de internet Ipv6 a dirección ip 2001:db8:acad:c::98 - fuente propia

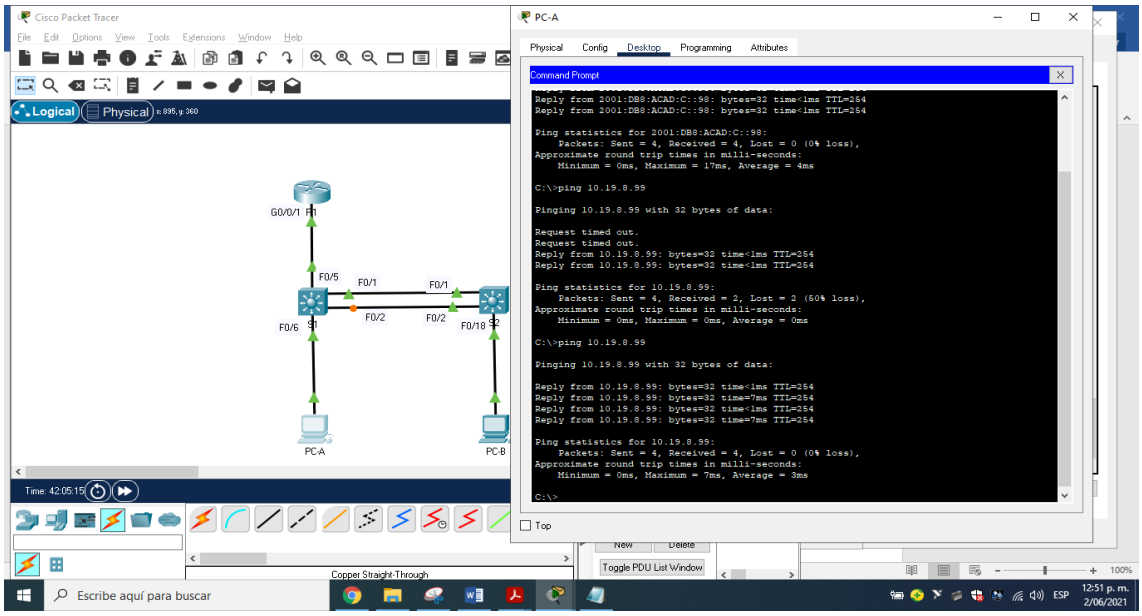

Figura 27. Ping desde PC-A a S2 VLAN4 de internet Dirección a dirección ip 10.19.8.99 - fuente propia

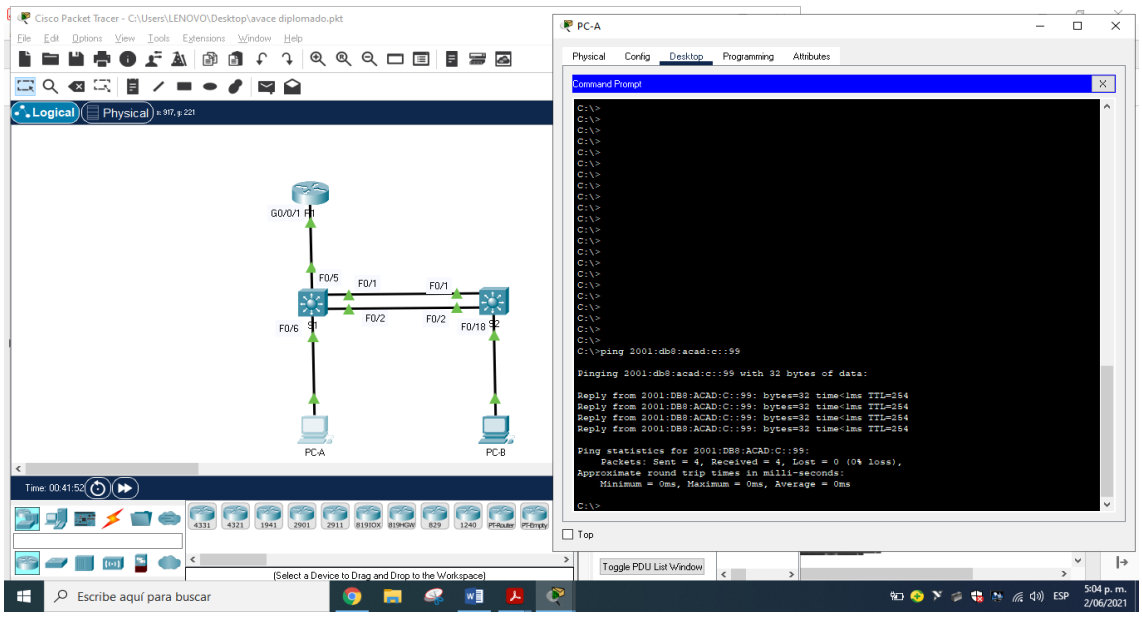

Figura 28. Ping desde PC-A a S2 VLAN4 de internet Ipv6 a dirección ip 2001:db8:acad:c: :99 - fuente propia

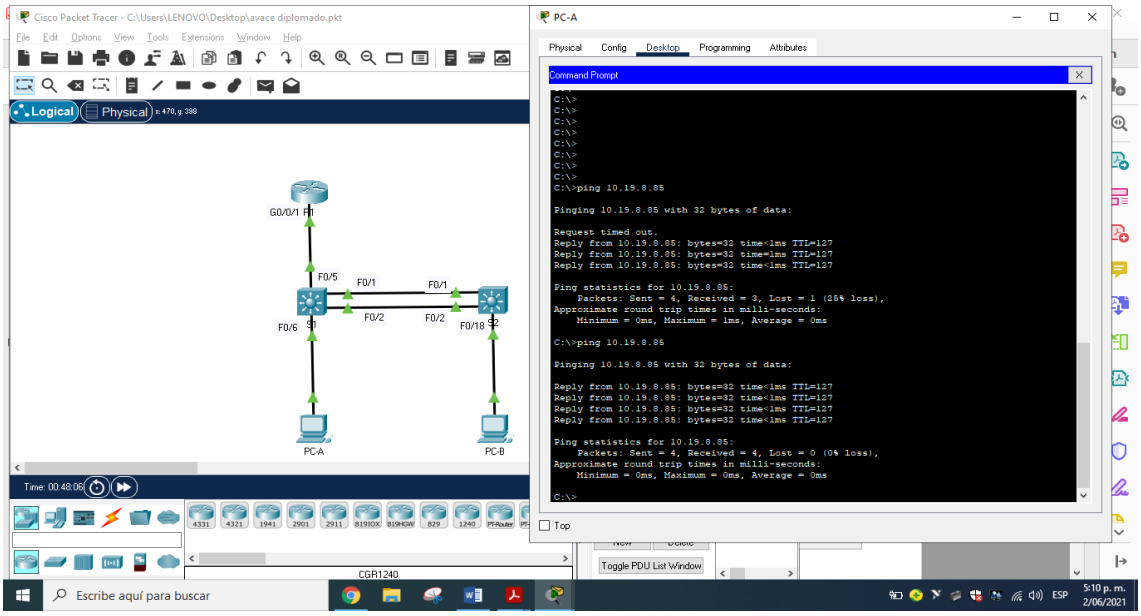

Figura 29. Ping desde PC-A a PC-B de internet Dirección a dirección ip 10.19.8.85 - fuente propia

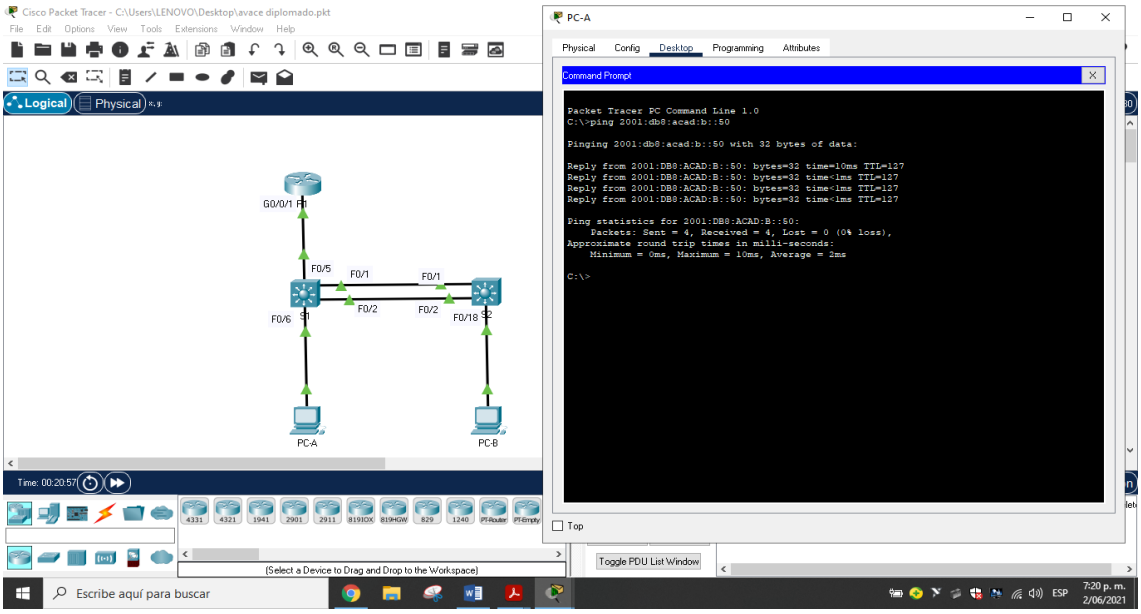

Figura 30. Ping desde PC-A a PC-B de internet Ipv6 a Dirección ip 2001:db8:acad:b::50 - fuente propia.

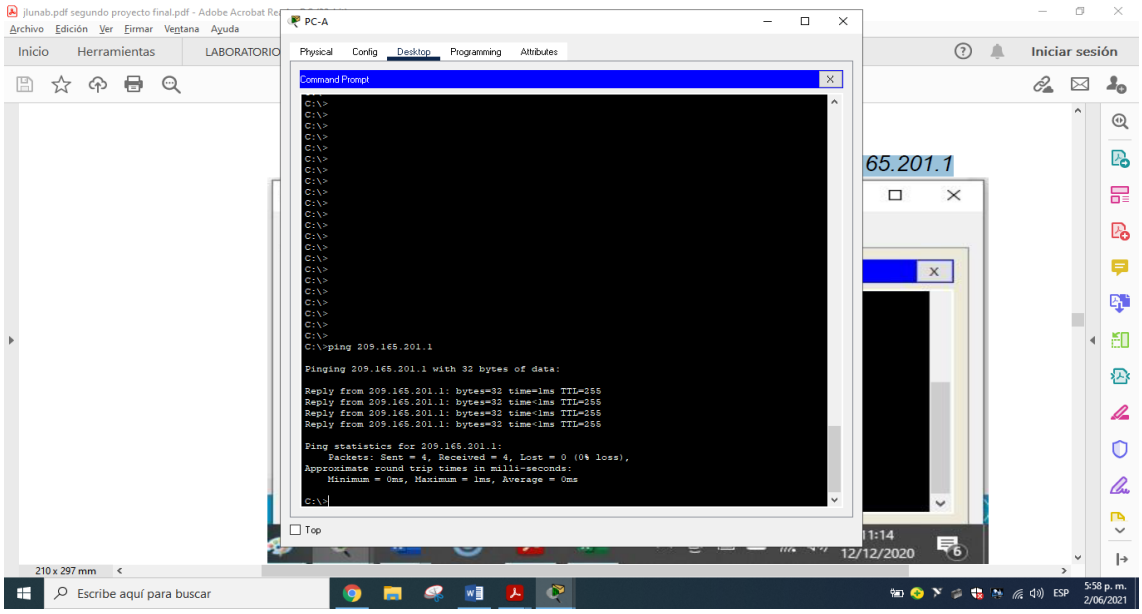

Figura 31. Ping desde PC-A a R1 Bucle 0 de internet Dirección a dirección ip 209.165.201.1 - fuente propia

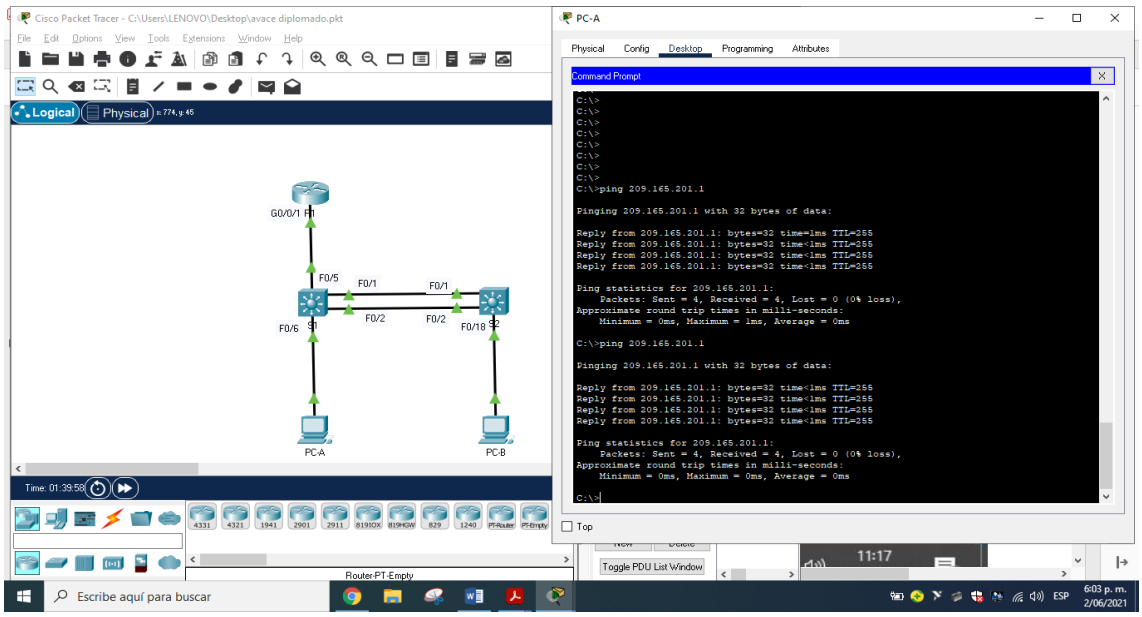

Figura 32. Ping desde PC-A a R1 Bucle 0 de internet Ipv6 a dirección ip 2001:db8:acad:209::1 - fuente propia

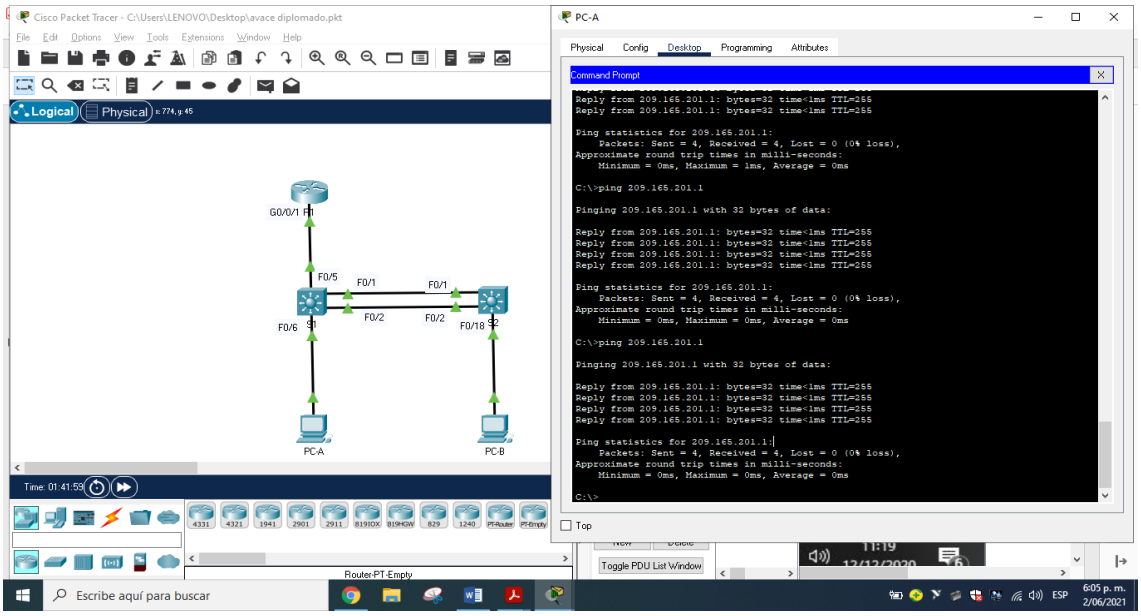

Figura 33 Ping desde PC-B a R1 Bucle 0 de internet Dirección a dirección ip 209.165.201.1 - fuente propia

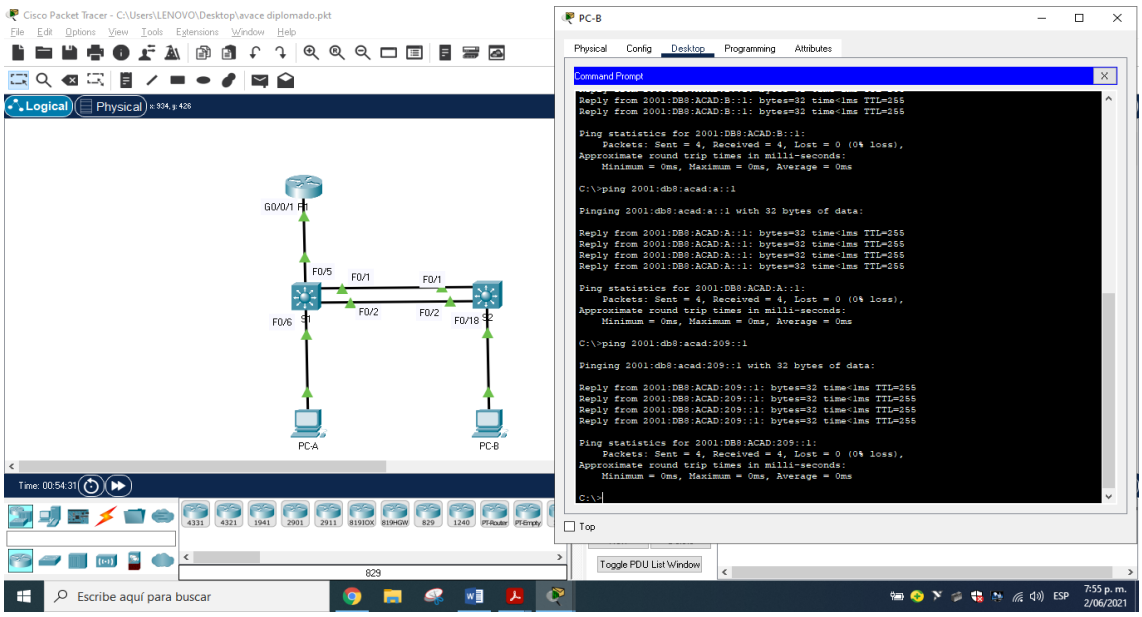

Figura 34. Ping desde PC-B a R1 Bucle 0 de internet Ipv6 a dirección ip 2001:db8:acad:209::1 - fuente propia

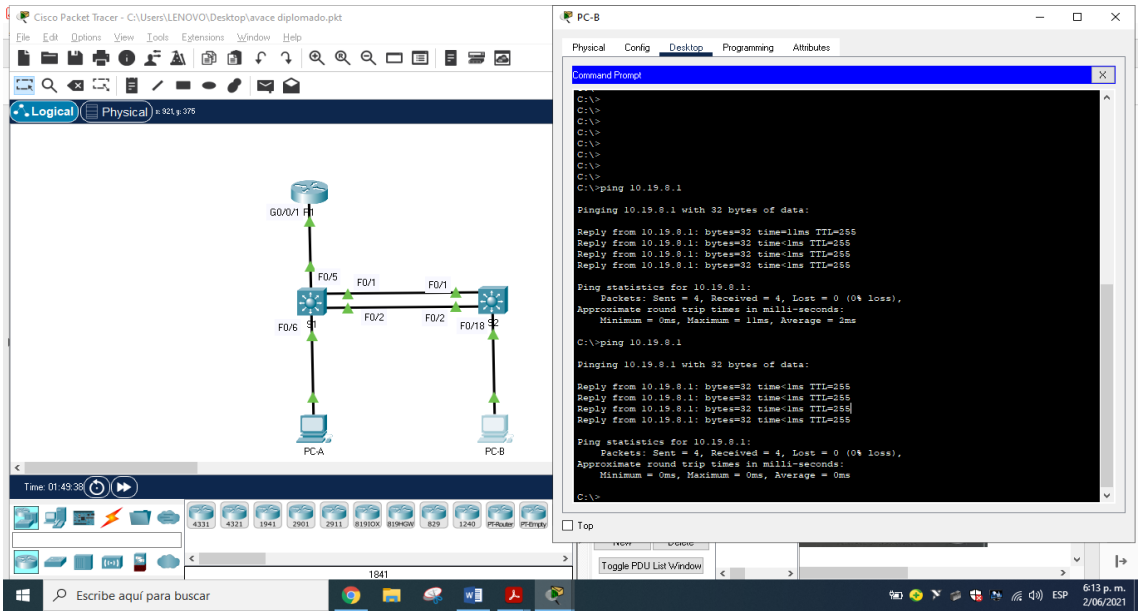

Figura 35. Ping desde PC-B a R1, G0/0/1.2 de internet Dirección a dirección ip 10.19.8.1 - fuente propia

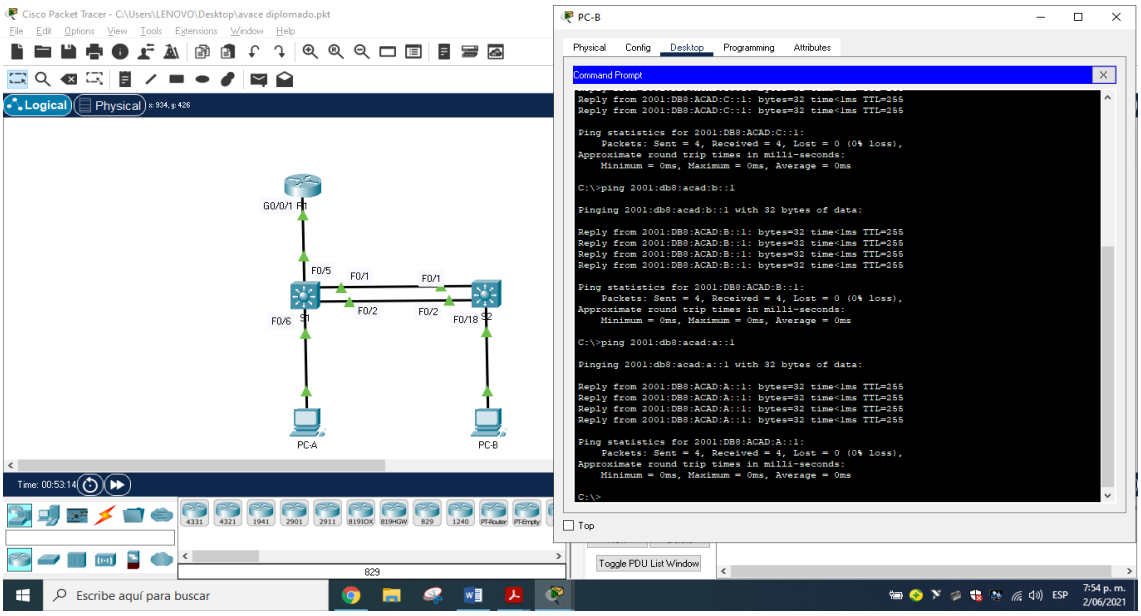

Figura 36. Ping desde PC-B a R1, G0/0/1.2 de internet Ipv6 a dirección ip 2001:db8:acad:a: :1 - fuente propia

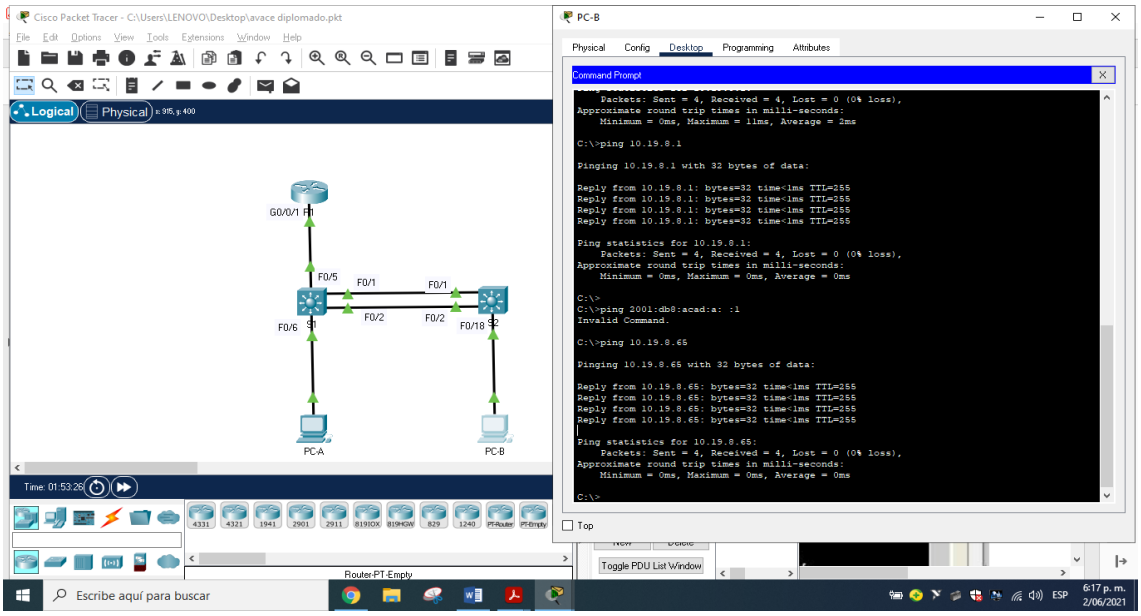

Figura 37. Ping desde PC-B a R1, G0/0/1.3 de internet Dirección a dirección ip 10.19.8.65 - fuente propia

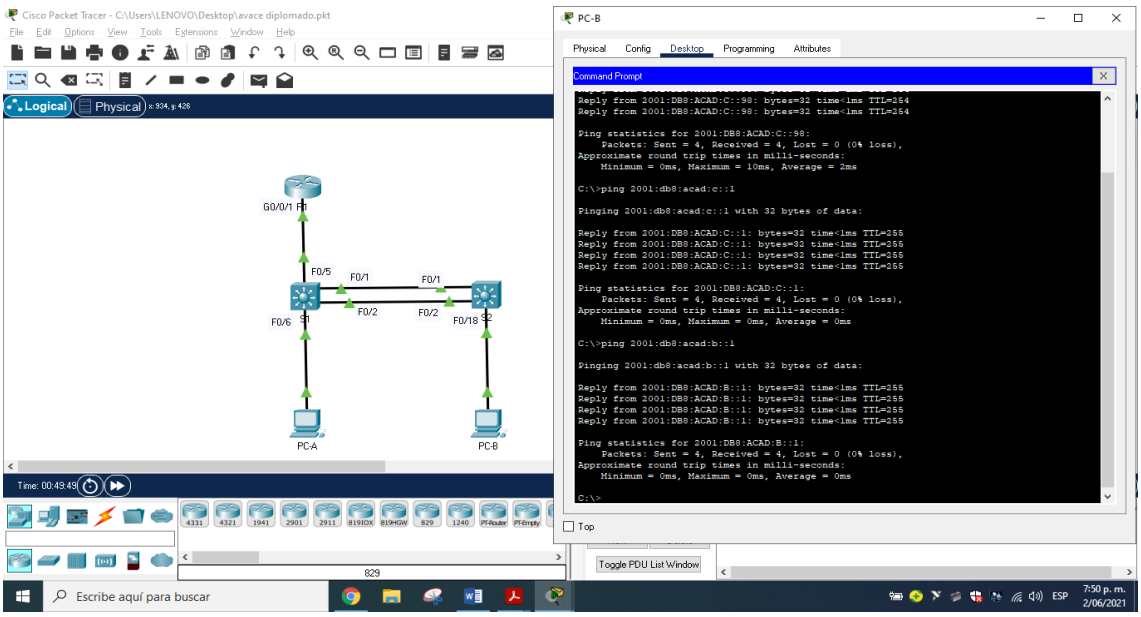

Figura 38. Ping desde PC-B a R1, G0/0/1.3 de internet Ipv6 a dirección ip 2001:db8:acad:b: :1 - fuente propia

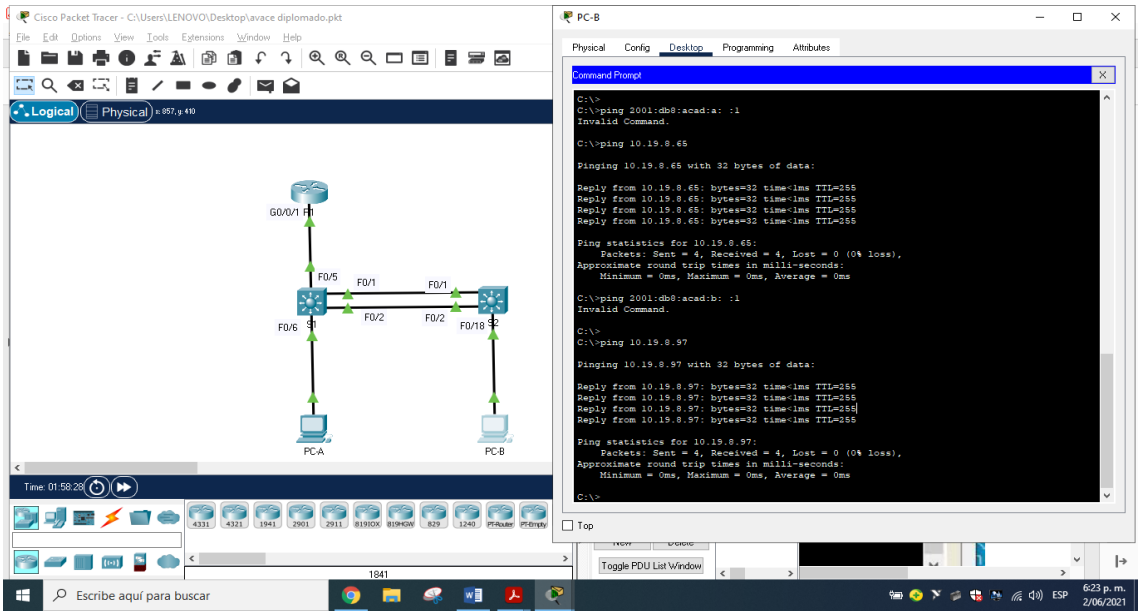

Figura 39. Ping desde PC-B a R1, G0/0/1.4 de internet Dirección a dirección ip 10.19.8.97 - fuente propia

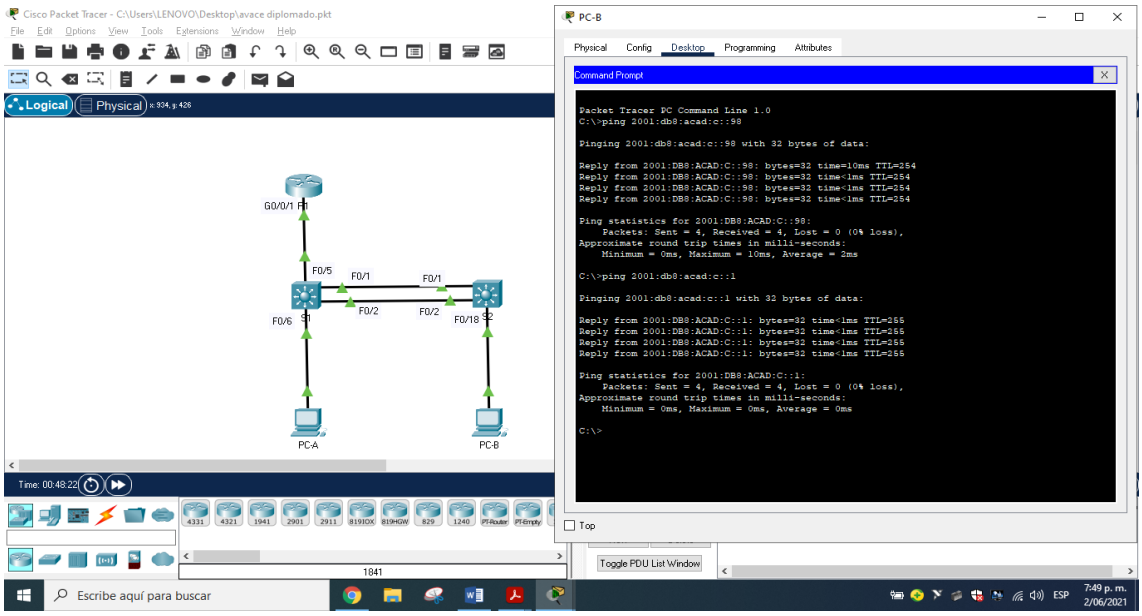

Figura 40. Ping desde PC-B a R1, G0/0/1.4 de internet Ipv6 a dirección ip 2001:db8:acad:c::1 - fuente propia

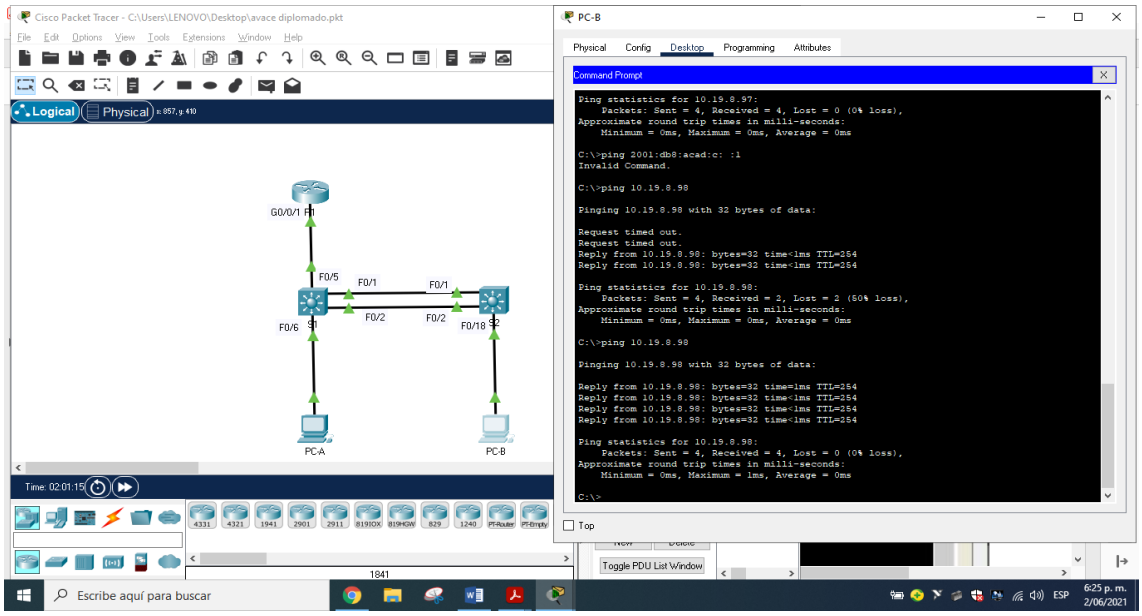

Figura 41. Ping desde PC-B a S1, VLAN4 de internet Dirección a dirección ip 10.19.8.98 - fuente propia

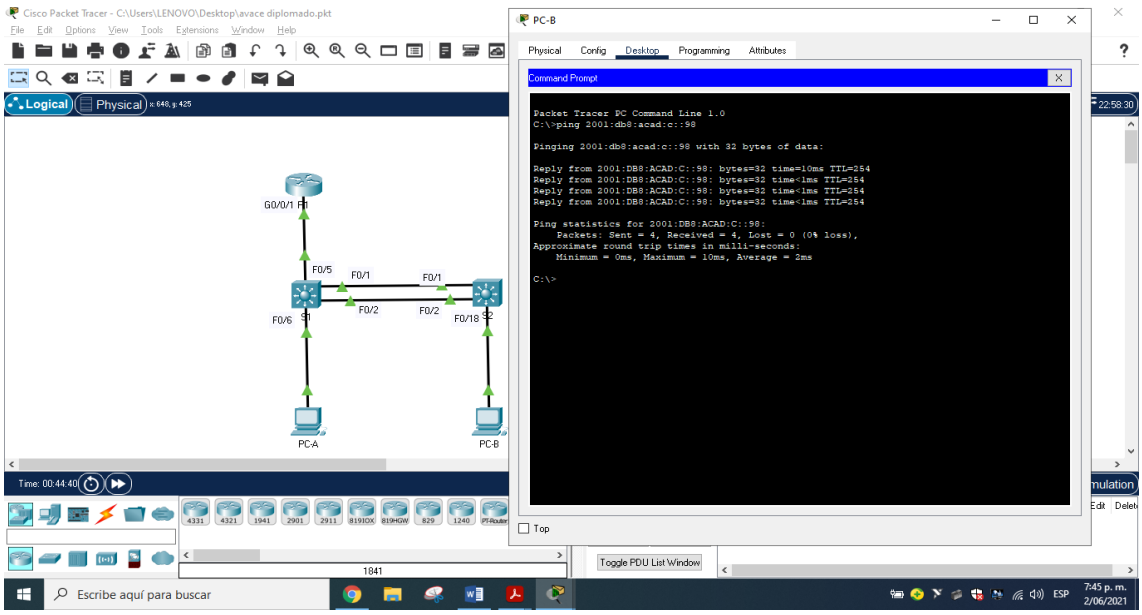

Figura 42. Ping desde PC-B a S1, VLAN4 de internet Ipv6 a dirección ip 2001:db8:acad:c::98 - fuente propia

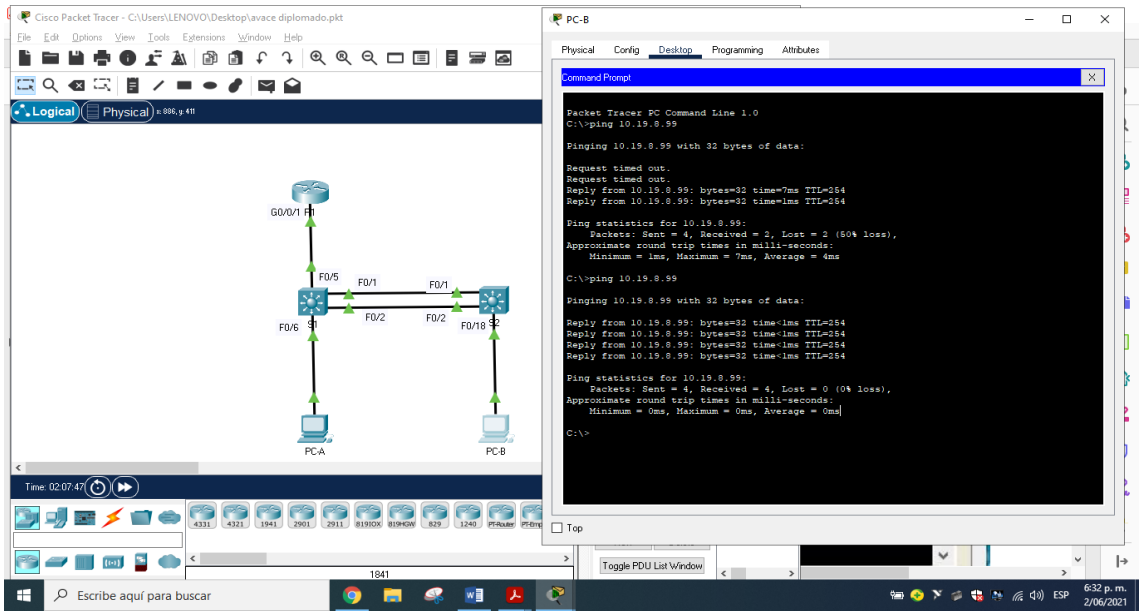

Figura 43. Ping desde PC-B a S2, VLAN4 de internet Dirección a dirección ip 10.19.8.99 - fuente propia

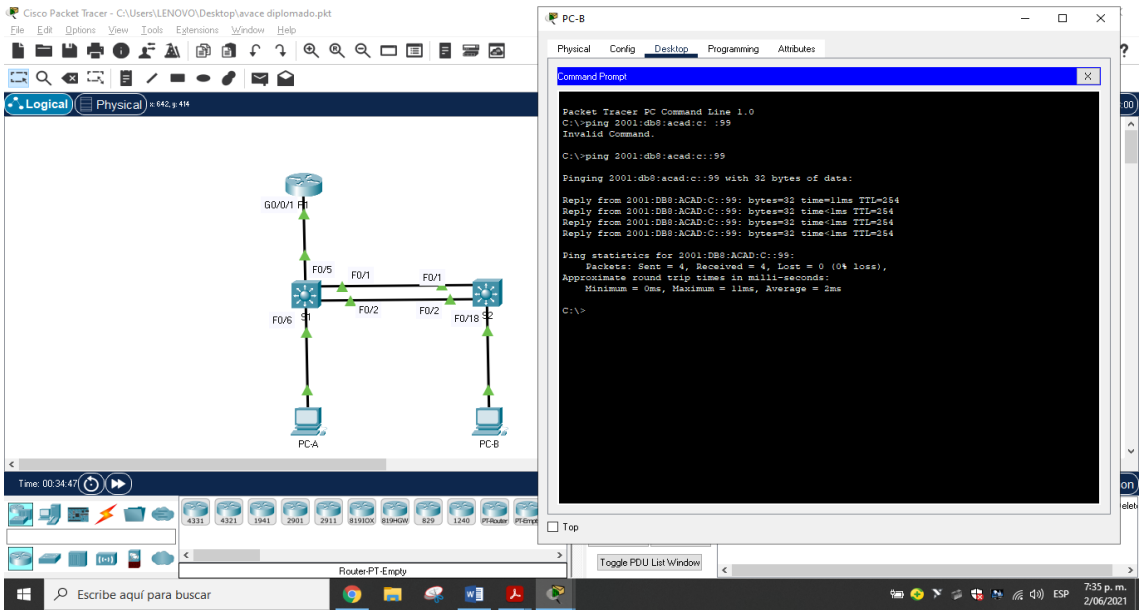

Figura 44. Ping desde PC-B a S2, VLAN4 de internet Ipv6 a dirección ip 2001:db8:acad:c: :99 - fuente propia

5. Escenario 2

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

Topología

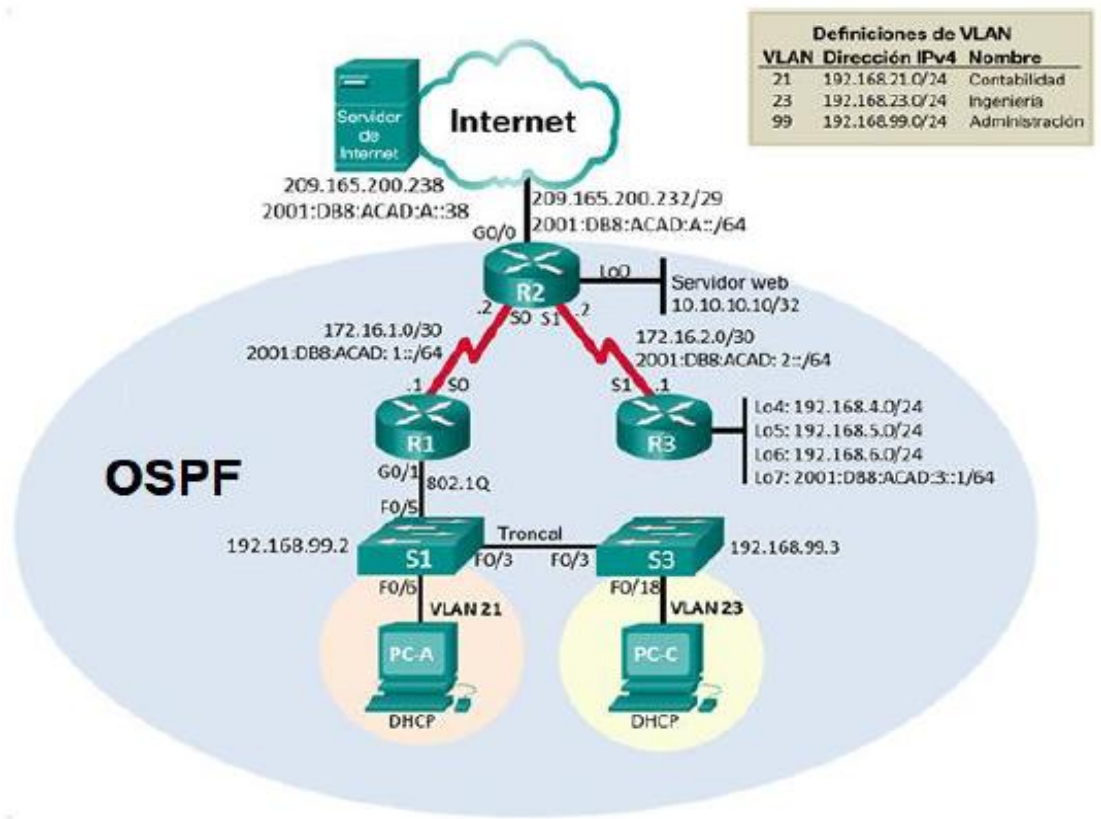

Figura 45 - fuente prueba de habilidades

Realizamos la topología de red utilizando para ello 3 Routers 1941, 2 Switchs 2960, 2 Computadoras, 1 Servidor y cables de cobre directos para la conexión.

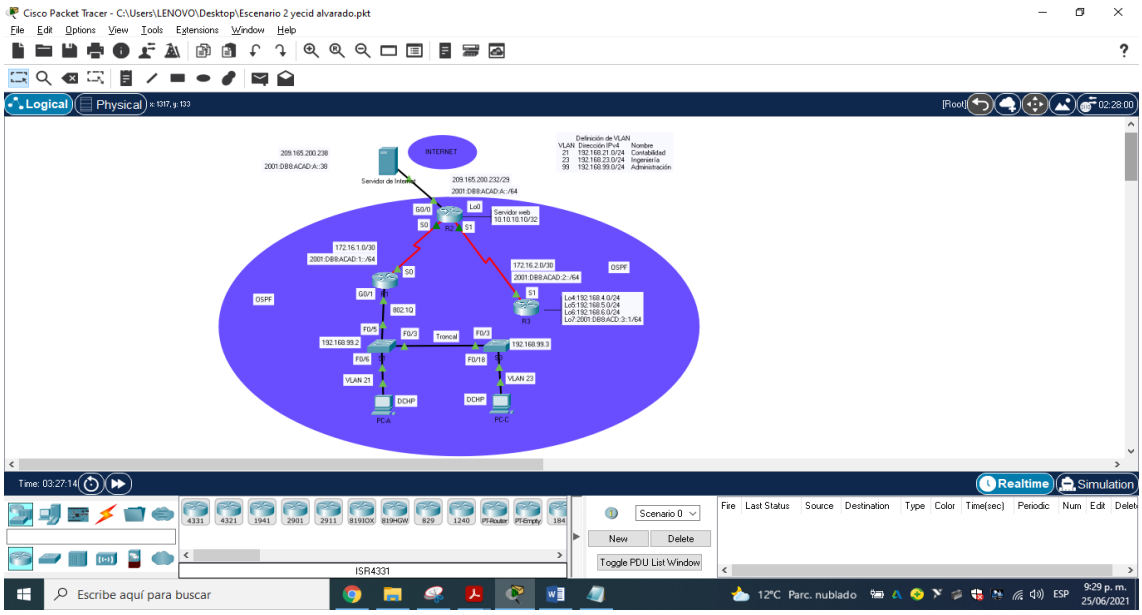

Figura 46. Simulación Escenario 2 - fuente propia

5.1. Parte 1: Inicializar dispositivos

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

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.
Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 11. Eliminar las configuraciones de inicio de los Routers y vuelva a cargarlos.

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

Se accede al Router 1,2 y 3 a través de la consola en modo privilegiado para borrar configuración de inicio con erase startup-config el cual borra lo que contiene NVRAM, después reiniciamos el Router con reload, quedando listo para la configuración de inicio.

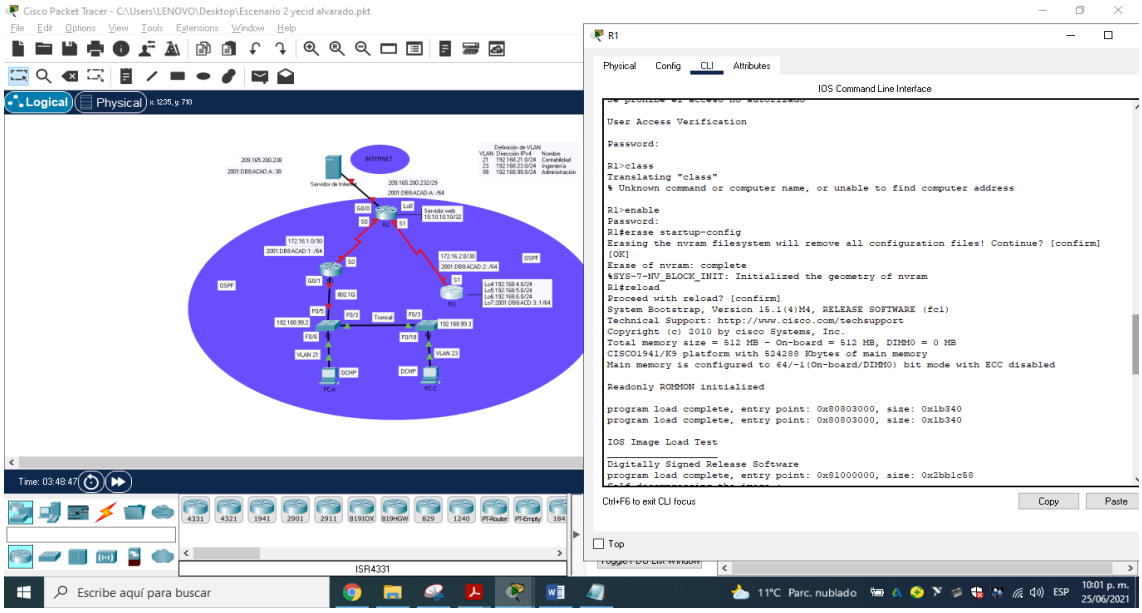

Figura 47. Eliminación de configuraciones y reinicio de los routers – fuente propia

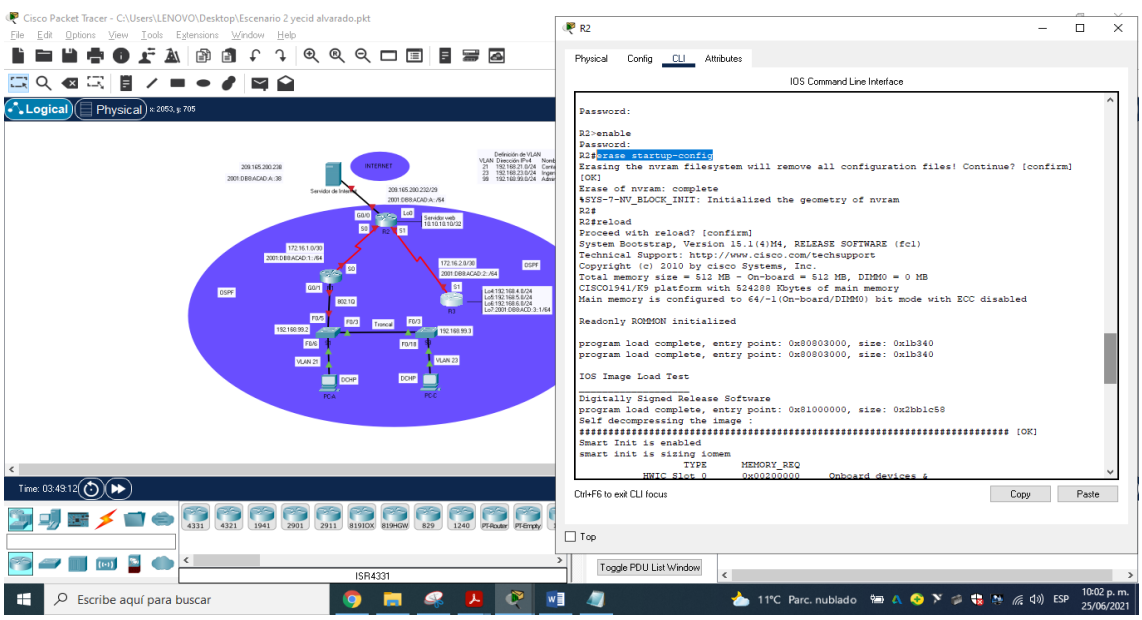

Figura 48. Eliminación de configuraciones y reinicio de los routers – fuente propia

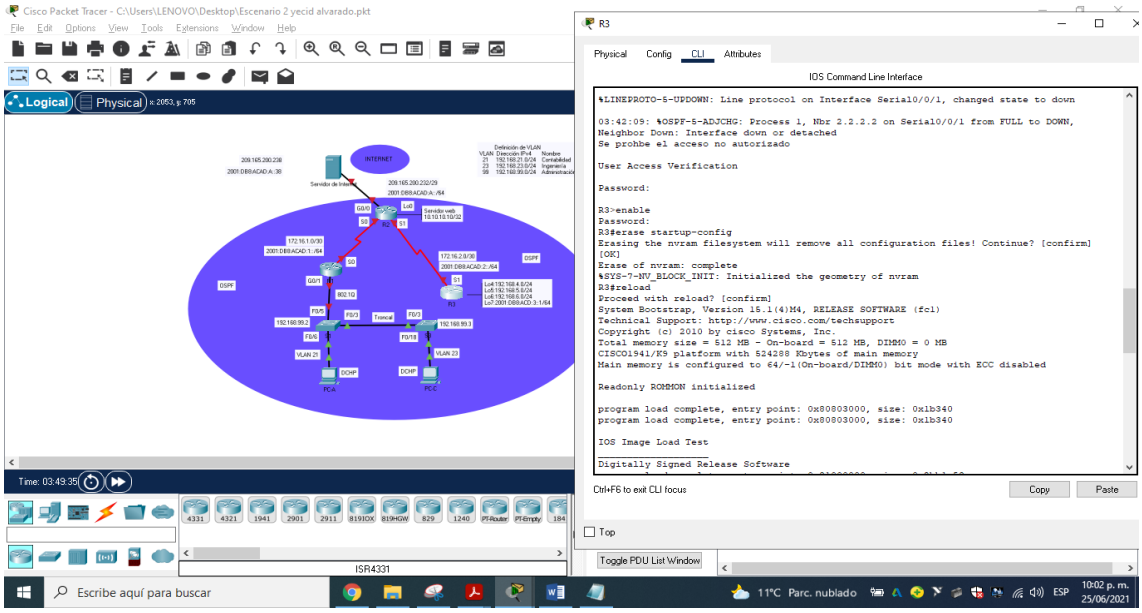

Figura 49. Eliminación de configuraciones y reinicio de los routers – fuente propia

Tabla 12. Eliminacion configuraciones de inicio de los Switchs y vuelver a cargarlos.

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

Ingresamos al Switch 1 y 2 a través del modo privilegiado erase startup-config el cual borra la NVRAM junto con delete vlan.dat este elimina la base de datos de la vlan, esto permite restaurar el switch y borrar la configuración de inicio, después se reinicia con reload, quedando listo para la configuración, y con show flash se verifica que los datos VLAN se halla borrado de la memoria flash.

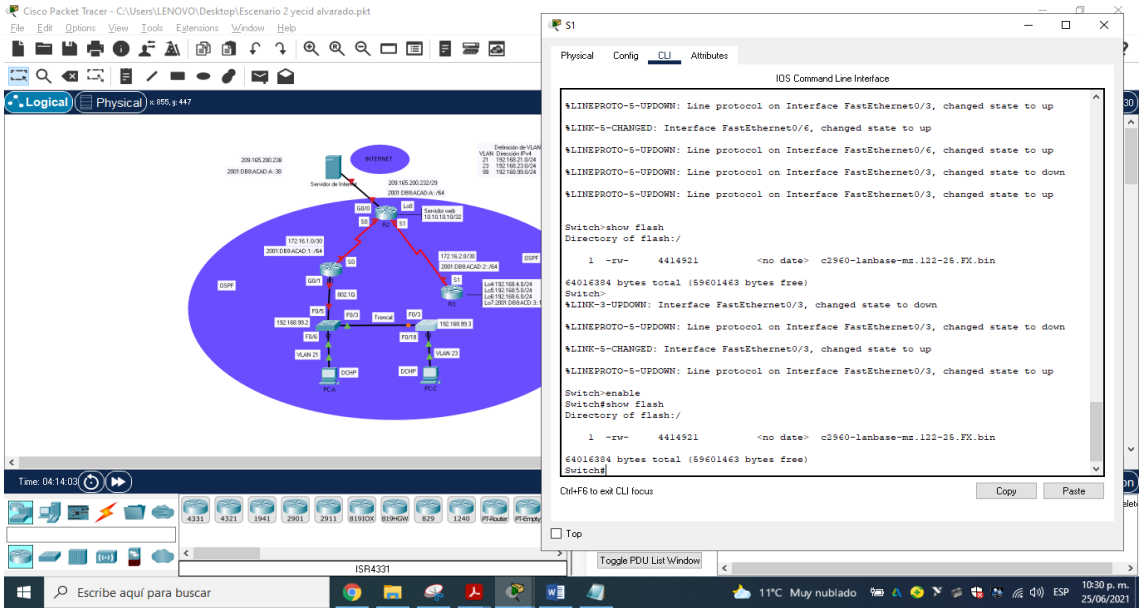

Figura 50. Eliminación configuraciones y reinicio de los Switchs – fuente propia

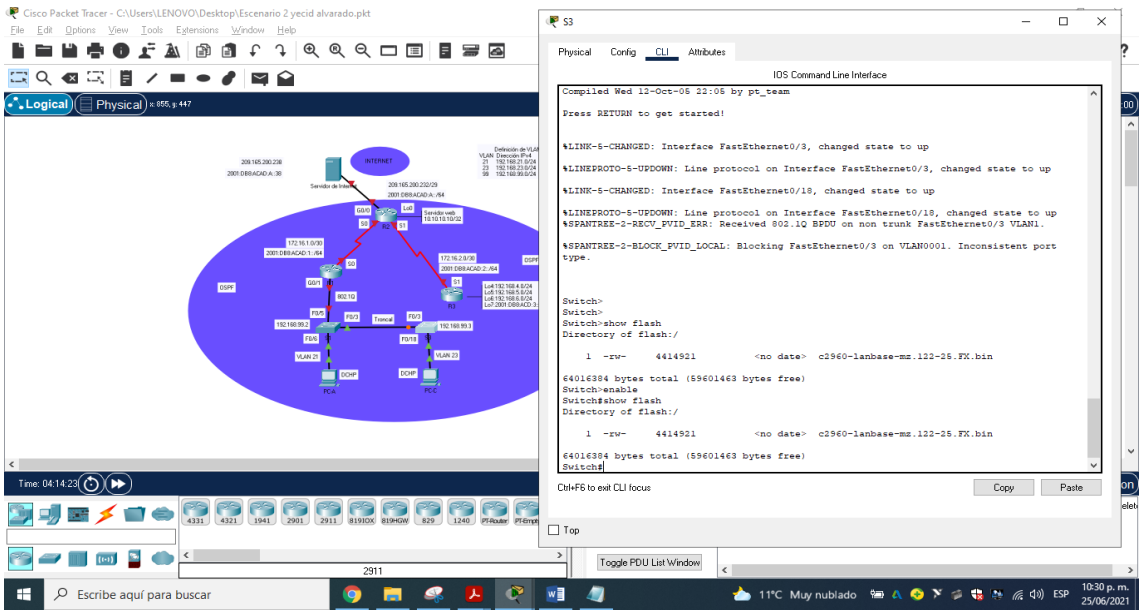

Figura 51. Eliminación configuraciones y reinicio de los Switchs – fuente propia

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

6.1. Paso 1. Configurar la computadora de Internet

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

Tabla 13. Configuración Servidor de Internet.

Elemento o tarea de configuración	Especificacion	Solucion
Dirección IPv4		209.165.200.238
Máscara de subred para IPv4		255.255.255.248
Gateway predeterminado	209.165.200.233	209.165.200.233
Dirección IPv6/subred		2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1	2001:DB8:ACAD:2::1

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

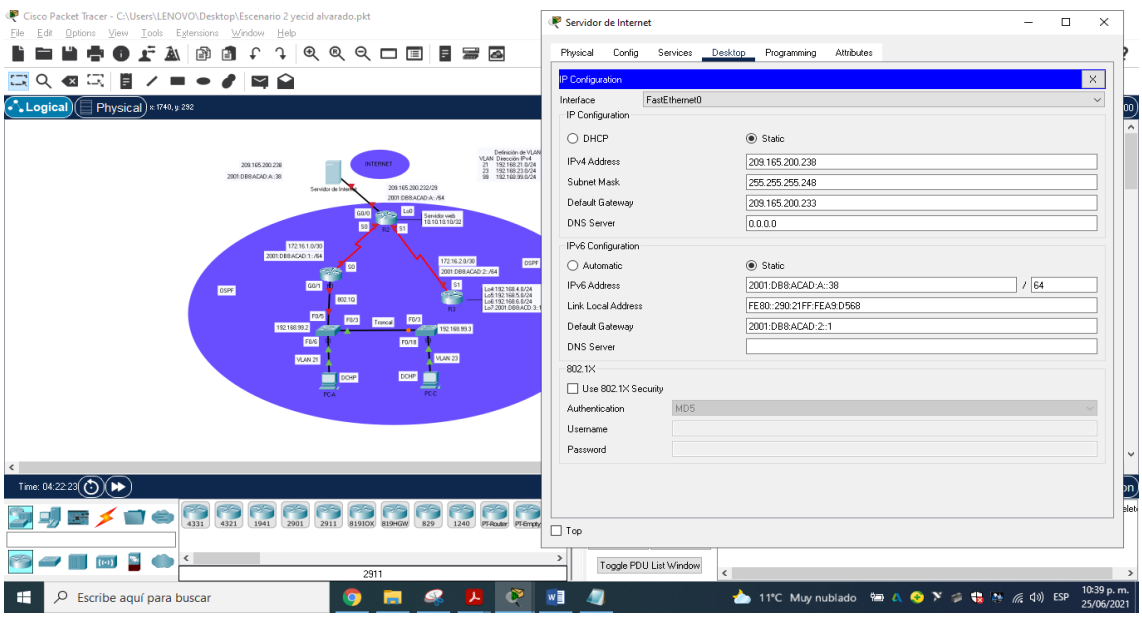

Figura 52. Configuración Servidor de Internet. – fuente propia

6.2. Paso 2. Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 14. Configuración R1

Elemento o tarea de configuración	**Especificacion**	**Solucion**
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 "Solo personal autorizado"
Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz	R1(config)#interface s0/0/0 R1(config-if)#description Conexion a R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config-if)#exit
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

Realizamos configuración inicial del R1, desde modo privilegiado se procede a realizar no ip domain lookup que desactivar la búsqueda DNS, esto para indicar que si hay un error en el scrip de configuración nos muestre un aviso de el error, configuraremos el nombre del dispositivo despues con la contraseña para ingresar al modo privilegiado por medio de enable secret, despues se configura la contraseña para ingresar a la consola con el comando password y se activa con el comando login, luego se configuran el modo de línea de terminal virtual vty 0 15 (Telnet) estableciendo una contraseña para el acceso, para seguridad se suma el comando service password-encryption para cifrar las contraseñas de texto no cifrado y un mensaje para usuarios no autorizados.
Se establece la interfaz s0/0/0 para la conexión con R2 y se le fija una dirección y IPv4 e IPv6 con una frecuencia de reloj de 128000 bits, se activa con el comando no shutdown, y se fijan las rutas predeterminadas IPv4 e IPv6.
Nota: Todavía no configure G0/1.

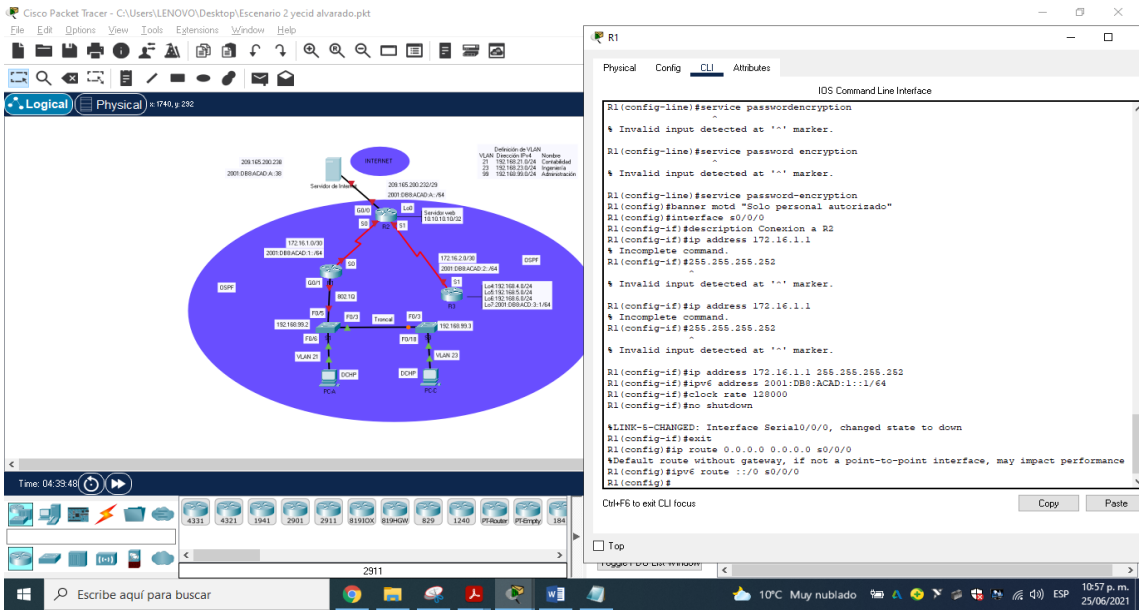

Figura 53. Configuración parámetros básicos en R1- fuente propia

6.3. Paso 3. Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 15. Configuración R2

Elemento o tarea de configuración	**Especificación**	**Solucion**
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 " Solo personal autorizado"
Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	R2(config)#interface s0/0/0 R2(config-if)#description Conexion a R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz	R2(config-if)#interface s0/0/1 R2(config-if)#description Conexion a R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4.	R2(config-if)#interface g0/0 R2(config-if)#description Conexion a Internet

	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)#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

Realizamos configuración inicial del R2, para ello desde modo privilegiado se procede a realizar el comando no ip domain lookup que desactiva la búsqueda DNS, para indicar que si hemos cometido un error nos muestre un aviso indicando el error, se coloca el nombre del dispositivo junto con la contraseña cifrada para ingresar al modo privilegiado por medio de enable secret, y se configura la contraseña para ingresar a la consola con el comando password y activamos con el comando login, se configura el modo de línea de terminal virtual vty 0 15 (Telnet) fijandole la 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 suma el mensaje del día para usuarios no autorizados en el banner motd.
Se configura la interfaz s0/0/0 para la conexión con R1 colocandole una dirección IPv4 e IPv6, luego se configura 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 activar la interfaz g0/0 la cual representa la simulación de Internet colocandoles la respectiva dirección IPv4 e IPv6, todas las interfaces al configurarse se activan con no shutdown. Se configura la interfaz loopback 0 que corresponde al servidor web simulado, se asigna una dirección Ipv4 y mascara de red para configurar las rutas predeterminadas IPv4 y IPv6 en la g0/0.

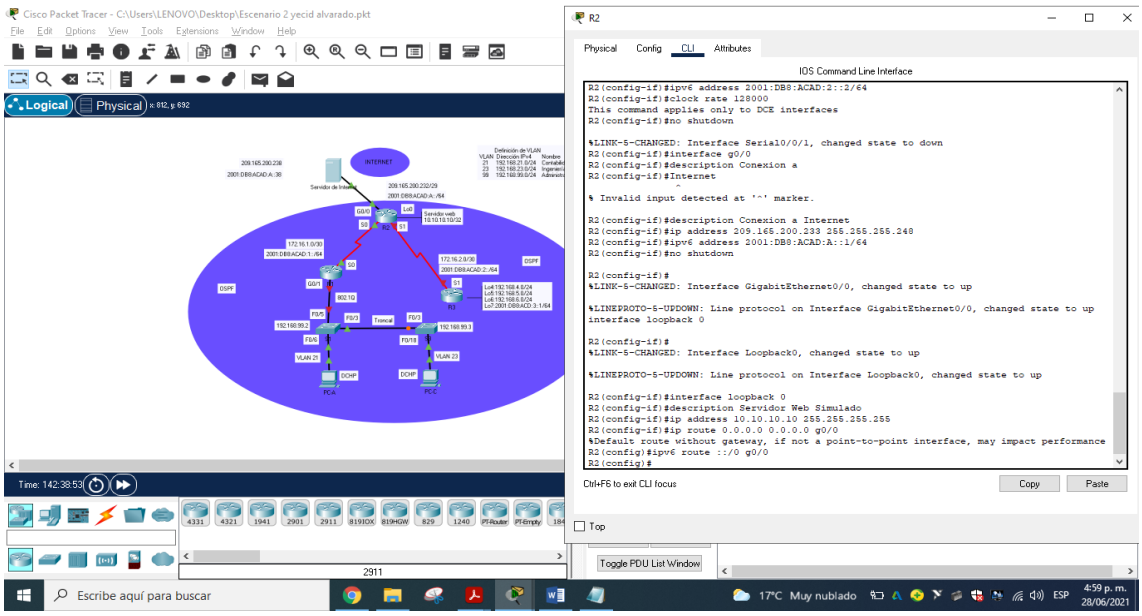

Figura 54. Configuración parámetros básicos en R2- fuente propia

6.4. Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 16. Configuración R3

Elemento o tarea de configuración	**Especificación**	**Solución**
Desactivar la búsqueda DNS		Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	R3	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	class	R3(config)#enable secret class
Contraseña de acceso a la consola, cisco	cisco	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	cisco	R3(config)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado		R3(config-line)# service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.	R3(config)#banner motd "Solo personal autorizado"
Interfaz S0/0/1	Establecer la descripción	R3(config)#interface s0/0/1

	Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	R3(config-if)#description Conexion a R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config-if)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config-if)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config-if)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.	R3(config-if)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
Rutas prederminadas	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Se configura R3, desde la consola EXEC privilegiado se procede a realizar no ip domain lookup que desactiva la búsqueda DNS, se fija el nombre del dispositivo junto con la contraseña cifrada para entrar al modo privilegiado a través de enable secret, de igual manera se fija la contraseña para ingresar a la consola con el comando password y se activa con el comando login, se fija el modo de línea de terminal virtual vty 0 15 (Telnet) se asigna una contraseña para el acceso, para seguridad se suma 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 suma el mensaje del día para usuarios no autorizados en el banner motd.
Se fija la interfaz s0/0/1 para la conexión con R2 fijandole una dirección IPv4 e IPv6, y se enciende, se configuran las interfaces loopback 4, 5 y 6 direccionandolas con IPv4 y la loopback 7 con IPv6, se establecen las rutas predeterminadas IPv4 e IPv6 en la s0/0/1.

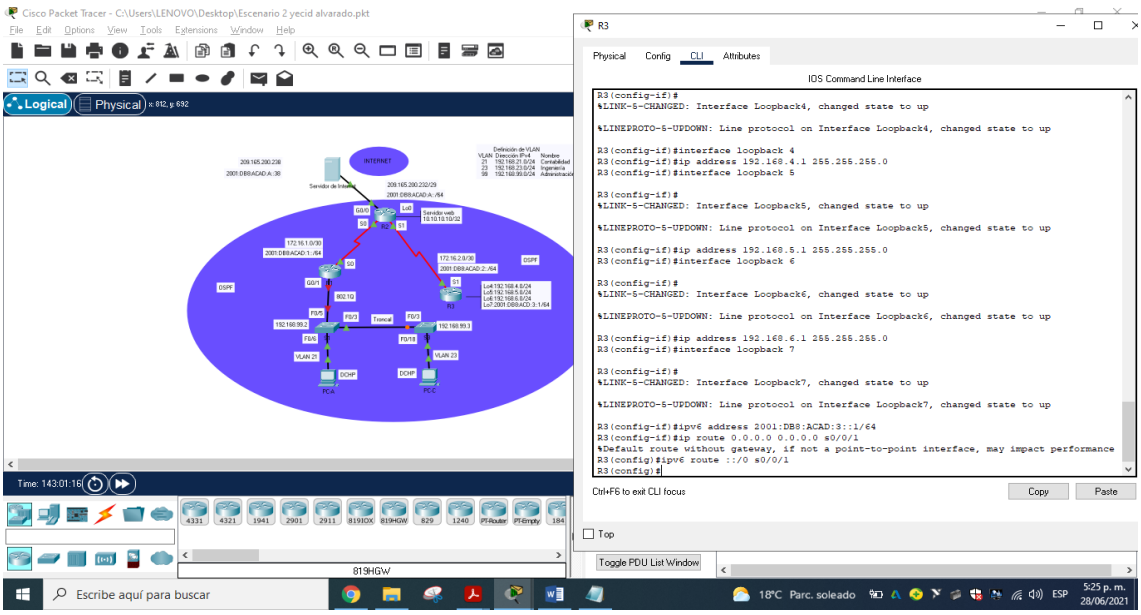

Figura 55. Configuración parámetros básicos en R2- fuente propia

6.5. Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 17. Configuración Switch 1

Elemento o tarea de configuración	**Especificación**	**Solucion**
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 " Solo personal autorizado "

Se Hace configuración inicial del S1, desde la consola EXEC privilegiado se procede a realizar el comando no ip domain lookup que desactivar la búsqueda DNS, se fija el nombre del dispositivo junto con la contraseña cifrada para ingresar al modo privilegiado a través de enable secret, de igual manera se fija la contraseña para ingresar a la consola con el comando password, activándose con el comando login, se fija el modo de línea de terminal virtual vty 0 15 (Telnet) asignándole una contraseña para el acceso, para seguridad se suma el comando service password-encryption para cifrar las contraseñas de texto no cifrado y se suma el mensaje del día para usuarios no autorizados en el motd.

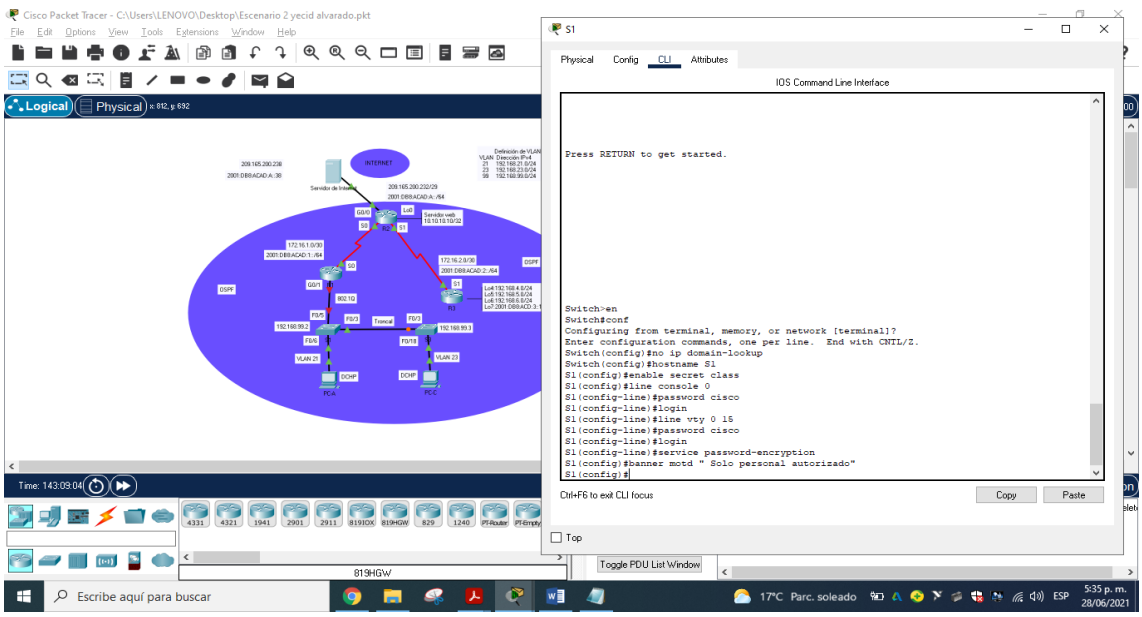

Figura 56. Configuración S1: fuente propia

6.6. Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 18. Configuración S3

Elemento o tarea de configuración		**Especificación realizada**
Desactivar la búsqueda DNS		Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch,	S3	Switch(config)#hostname S3

Contraseña de exec privilegiado cifrada,	class	S3(config)#enable secret class
Contraseña de acceso a la consola,	cisco	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet,	cisco	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado		S3(config-line)# service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.	S3(config)#banner motd " Solo personal autorizado "

Se hace configuración básica del S3, desde la consola EXEC privilegiado se procede a realizar el comando no ip domain lookup que desactiva la búsqueda DNS, se configura el nombre junto con la contraseña cifrada para ingresar al modo privilegiado escribiendo enable secret, de igual manera se configura la contraseña para entrar a la consola con el comando password, escribiendo con el comando login, se configura el modo de línea de terminal virtual vty 0 15 (Telnet) fijando una contraseña para el acceso, para seguridad se suma el comando service password-encryption para cifrar las contraseñas de texto no cifrado y se suma el mensaje del día para usuarios no autorizados en el motd.

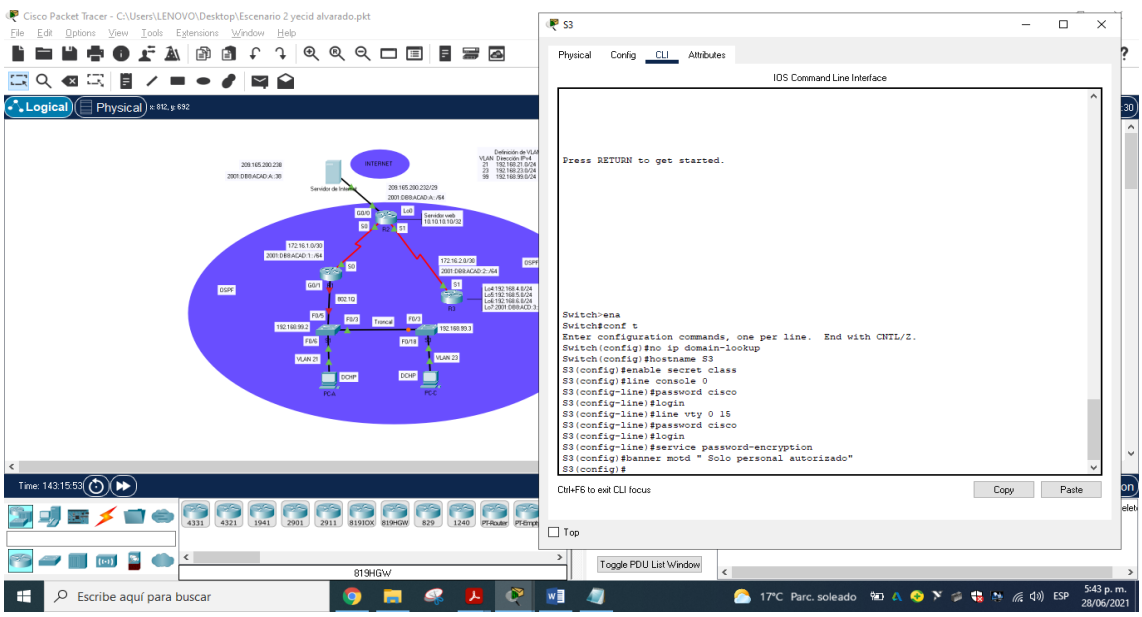

Figura 57. Configuración S3: fuente propia

6.7. Paso 7: Verificar la conectividad de la red

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

Tabla 19. 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 verificar el correcto funcionamiento de la red, ejecutando el comando ping entre routers y desde el pc de internet a la puerta de enlace predeterminada.

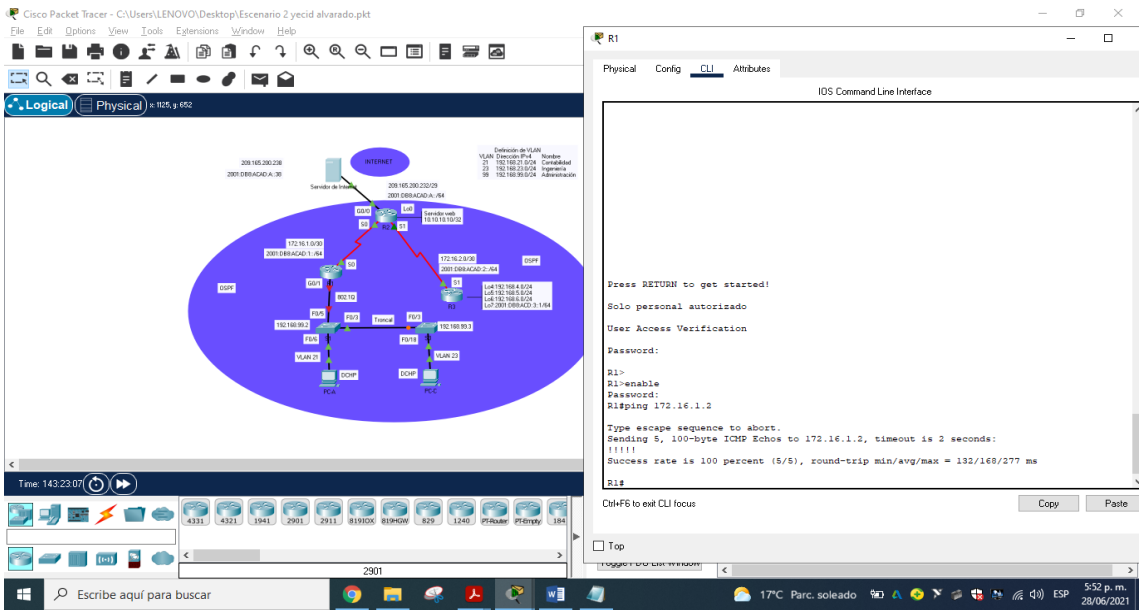

Figura 58. Ping desde R1 a R2 a s0/0/0 direccion ip 172.16.1.2: fuente propia

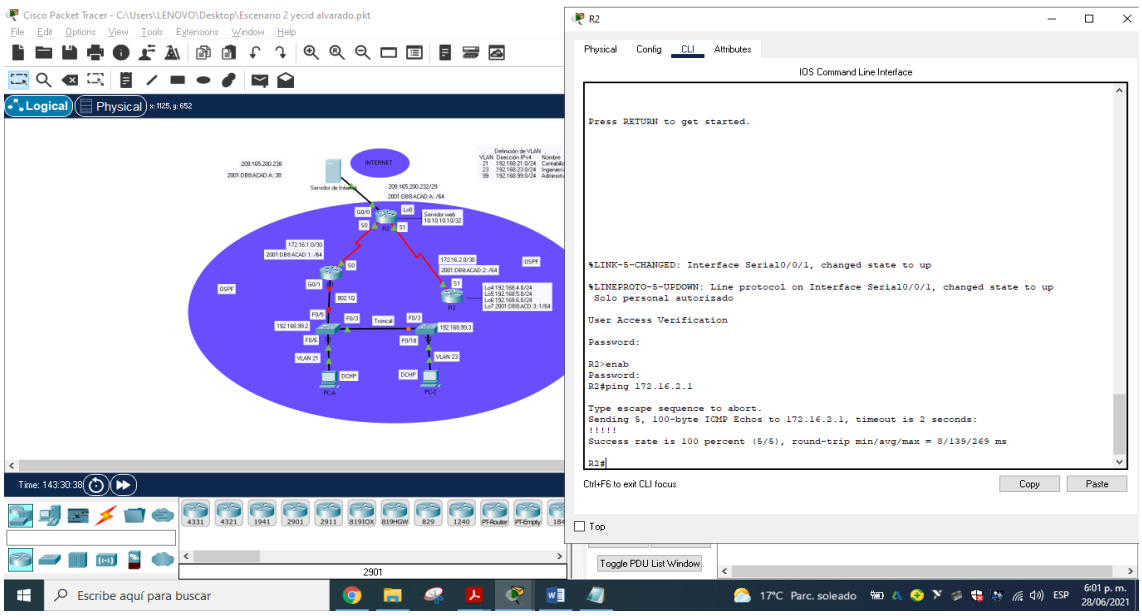

Figura 59. Ping desde R1 a R2 a s0/0/0 direccion ip 172.16.2.1: fuente propia

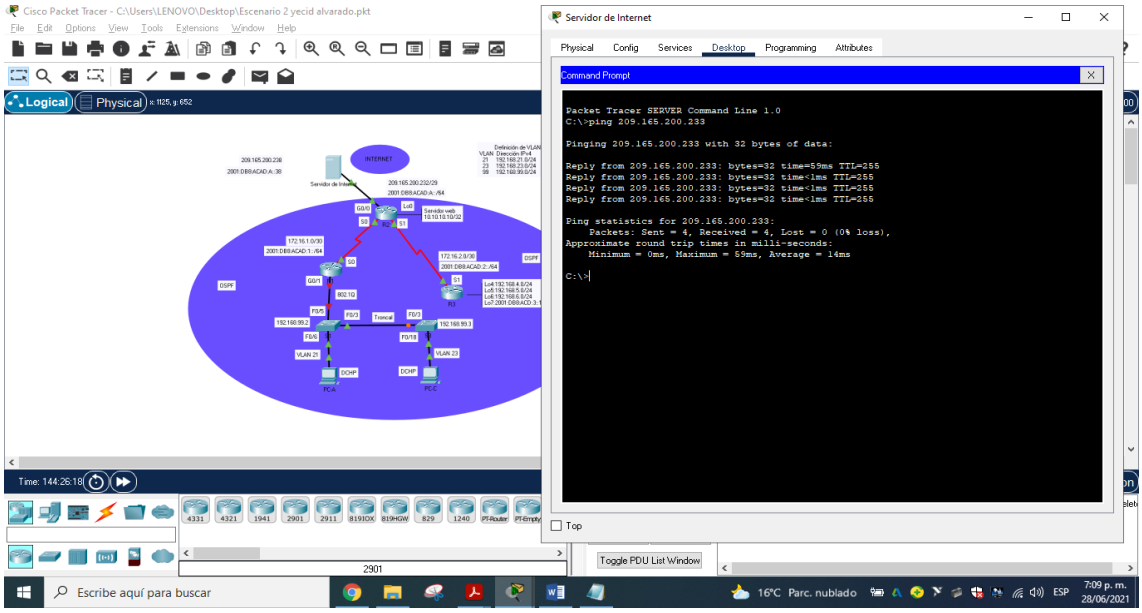

Figura 60. Ping desde servidor de Internet a gateway predeterminado: fuente propia

7.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 20. Configuración seguridad del S1, Vlan y routing entre Vlan

Elemento o tarea de configuración	**Especificación**	**Solucion**
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>enable 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 S1(config-vlan)exit
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 S1(config-if)exit

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 S1(config-if) exit
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	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 s1 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 hace los mismo con 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.

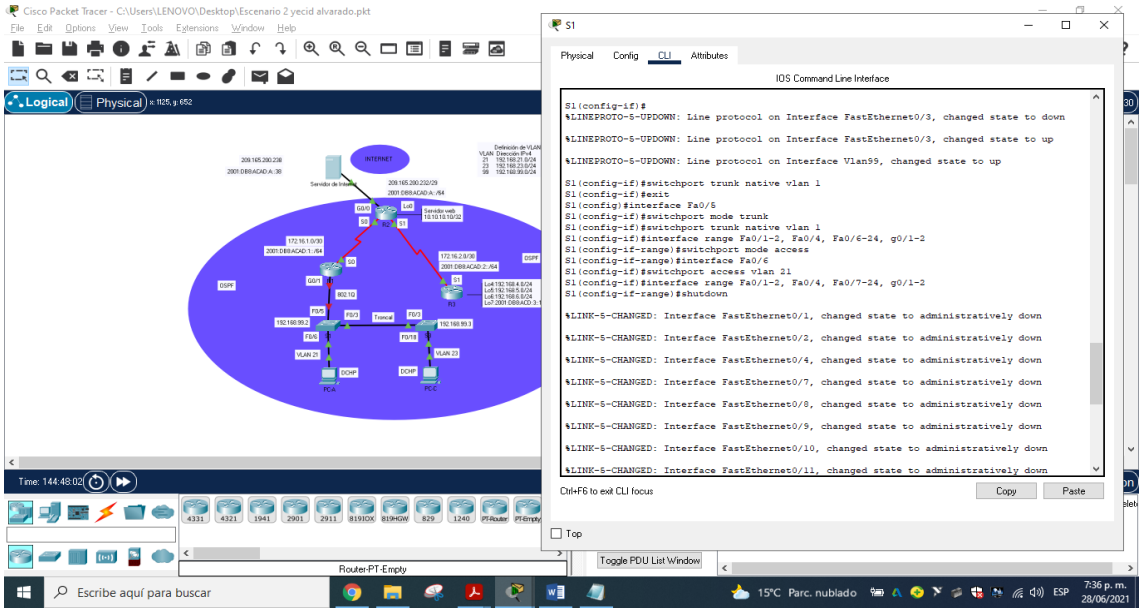

Figura 61. Configuración seguridad del s1, las VLAN y el routing entre VLAN: fuente propia

7.2. Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 21. Configuración seguridad del S3, Vlan y routing entre Vlan

Elemento o tarea de configuración	**Especificación**	**solucion**
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>enable 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 S3(config-vlan)exit
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	S3(config)#ip default-gateway 192.168.99.1

	como gateway predeterminado.	
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 21		S3(config-if-range)#interface Fa0/18 S3(config-if)#switchport access vlan 21
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

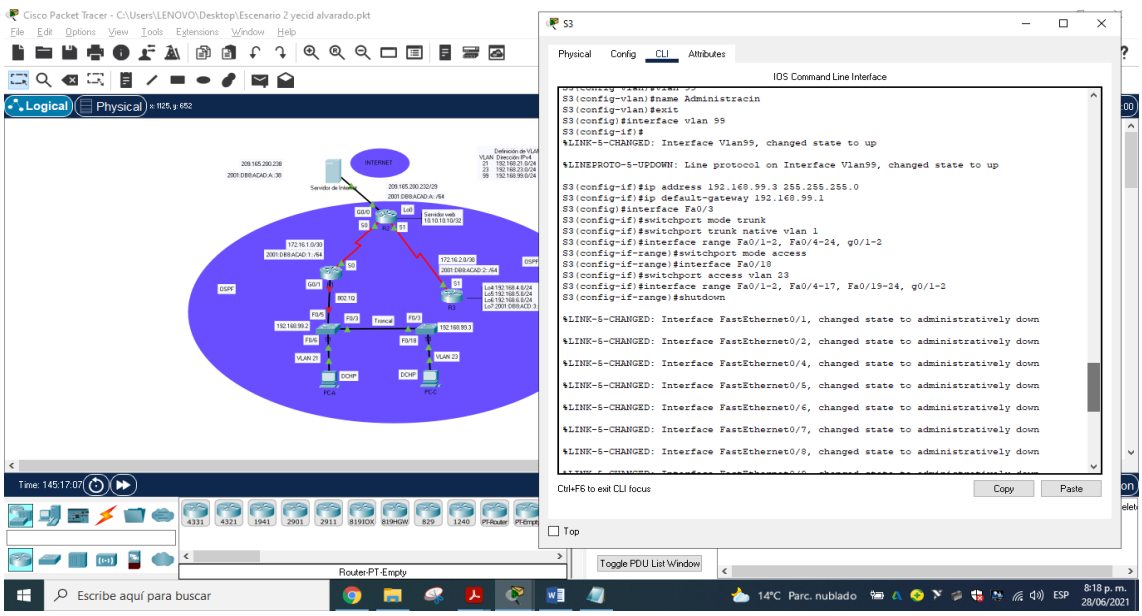

Figura 62. Configuración seguridad del s3, las VLAN y el routing entre VLAN: fuente propia.

7.3. Paso 3: Configurar R1
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22. Configuración Subinterfaz 802.1Q en el Router 1

Elemento o tarea de configuración	**Especificación**	**solucion**
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>enable R1#configure terminal 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

La Interfaz g0/1 se configuran las Subinterfaces 802.1Q en el R1, se procede a configurar la subinterfaz g0/1.21, habilitándola con el comando ecapsulation dot1q asociándole la vlan 21 (Lan de Contabilidad) y fija la IPv4 correspondiente, se realiza el mismo procedimiento para encender la subinterfaz g0/1.23, Vlan 23 (Lan de Ingeniaría) y la subinterfaz g0/1.99, Vlan 99 (Lan de Administración) finalmente se activa la interfaz g0/1 con el comando no shutdown.

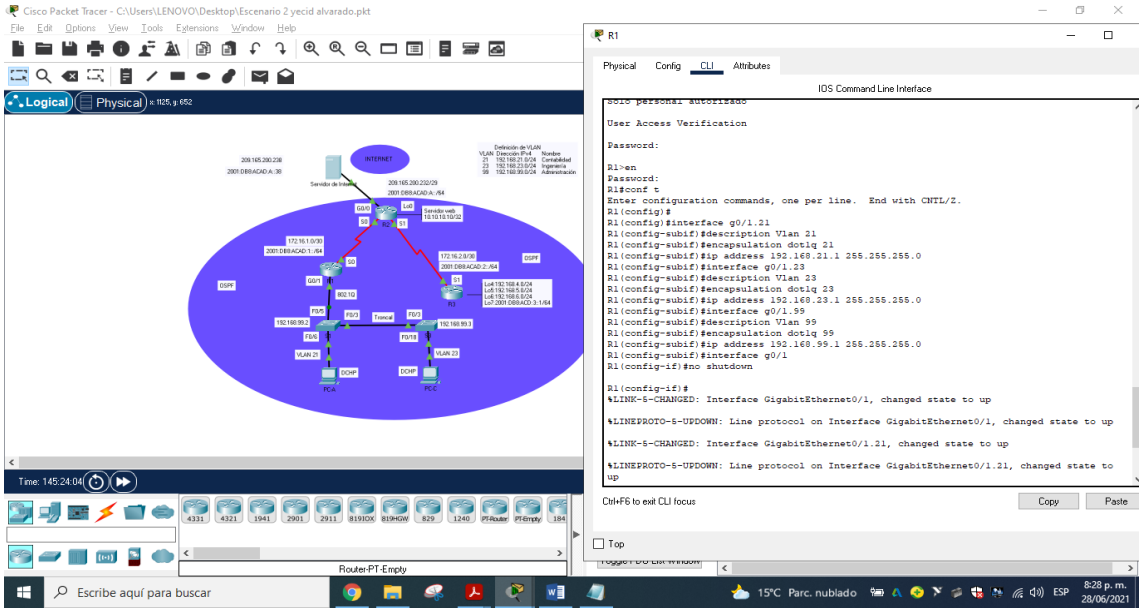

Figura 63. Configuración Subinterfaz 802.1Q en el R1: fuente propia.

7.4 Paso 4: Verificar la conectividad de la red

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

Tabla 23. 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 verificar el correcto funcionamiento de esta.

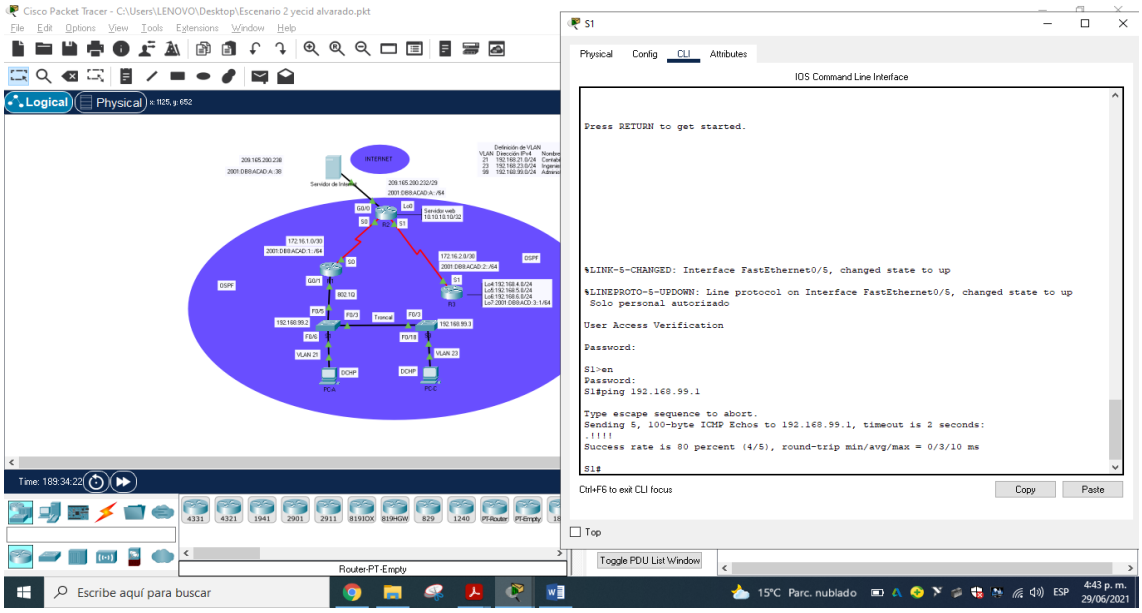

Figura 63. Desde S1 ping a R1 a dirección Vlan 99 Direccion ip 192.168.99.1: fuente propia.

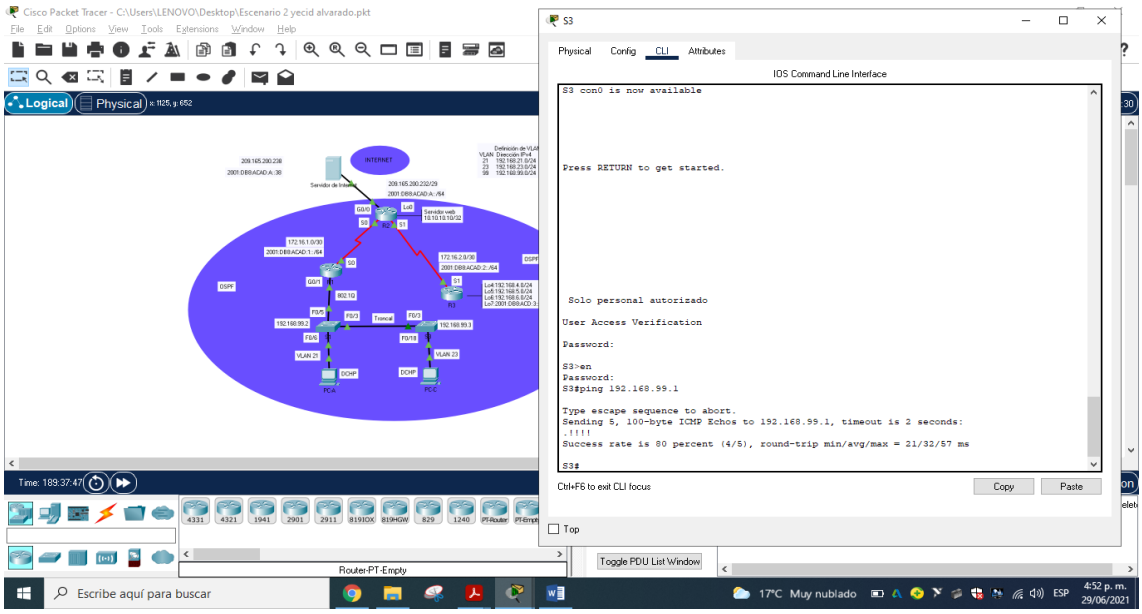

Figura 64. Desde S3 ping a R1 a dirección Vlan 99 Direccion ip 192.168.99.1: fuente propia.

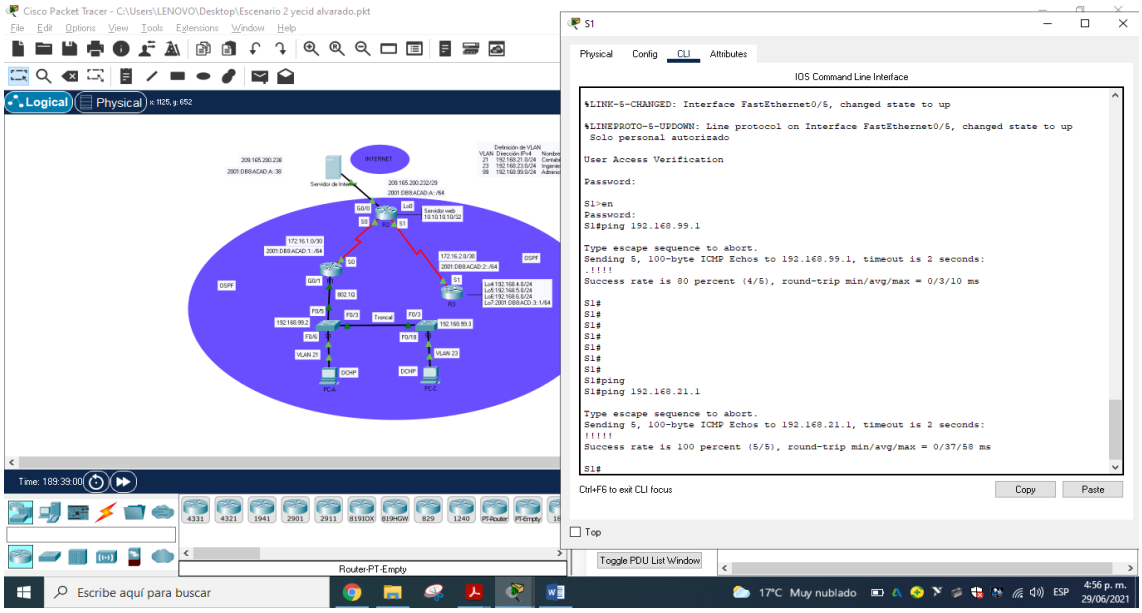

Figura 65. Desde S1 ping a R1 a dirección Vlan 21 Direccion ip 192.168.21.1: fuente propia.

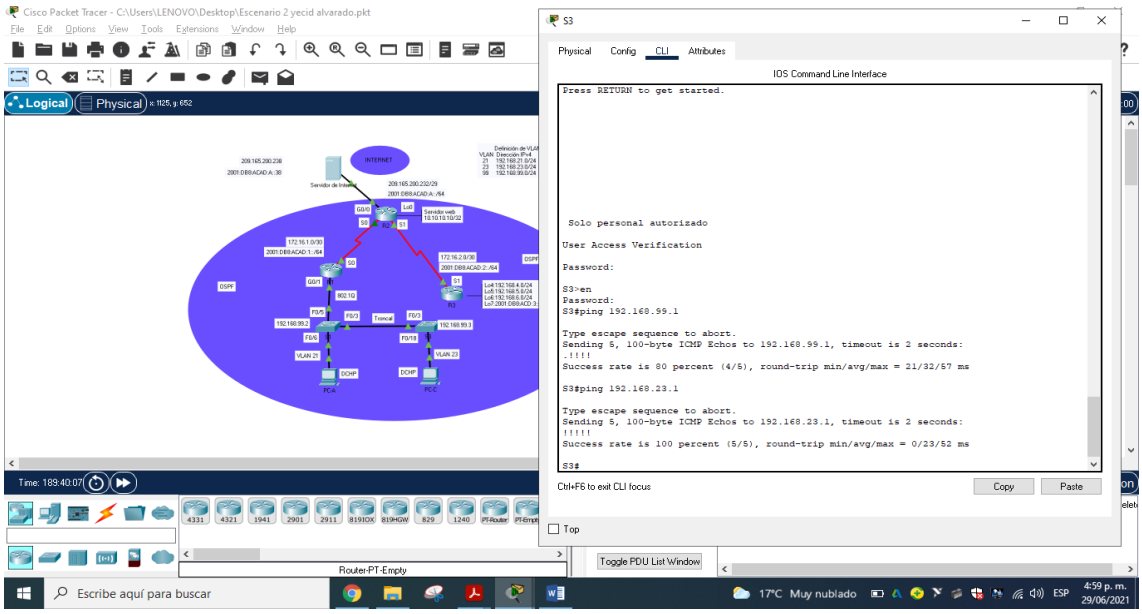

Figura 66. Desde S3 ping a R1 a dirección Vlan 23 Direccion ip 192.168.23.1: fuente propia.

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

8.1. Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 24. Configuración del protocolo de routin dinámico OSPF en Router 1.

Elemento o tarea de configuración	**Especificación**	**Solucion**
Configurar OSPF área 0		R1>enable R1#conf t 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

configuramos el protocolo OSPF en el R1 con Router ospf 1, para verificar las redes conectadas escrbiendo show ip route connected, con la verificación se procede asignar las redes al área 0 con el comando network asignándole la IP correspondiente, todas las subintefaces LAN (g0/1.21, g0/1.23, g0/199) se establecen como pasivas y se desactiva la sumarización automática con el comando no auto-summary.

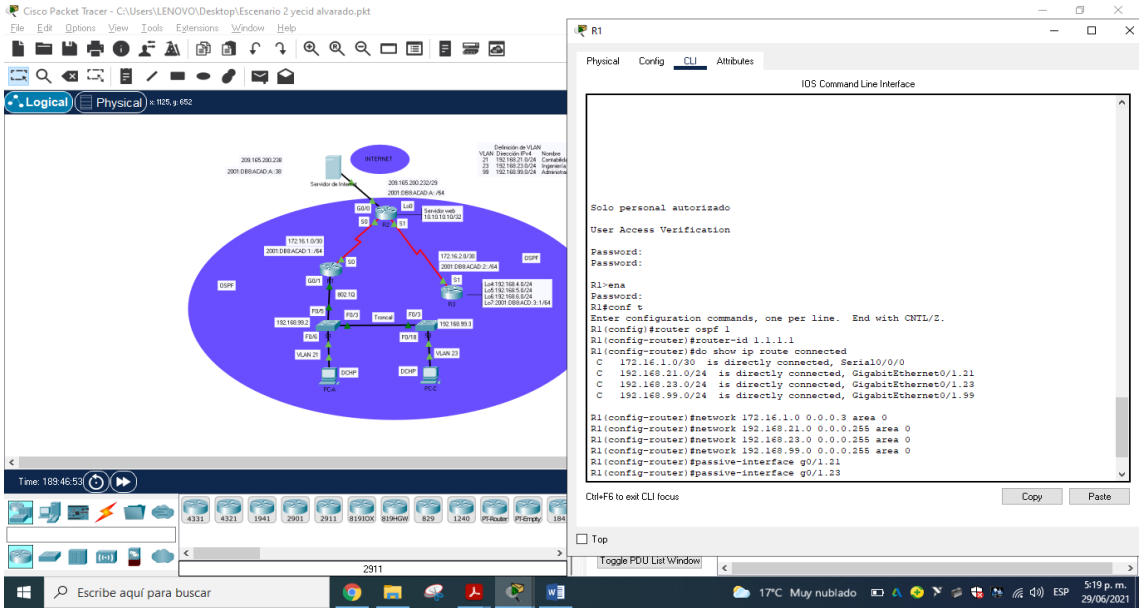

Figura 67. Configuración del protocolo de routin dinámico OSPF en R 1: fuente propia

8.2. Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 25. Configuración del protocolo de routin dinámico OSPF en R2

Elemento o tarea de configuración	**Especificación**	**Solución**
Configurar OSPF área 0		R2>enable R2 conf t 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

Configuramos el protocolo OSPF en el R2 con el comando Router ospf 1, para verificar las redes conectadas se trabaja el comando show ip route connected, con la verificación se asignar las redes al área 0 con el comando network asignándole la IP correspondiente, la interfaz de red g0/0 no se tiene en cuenta y por tanto no establece, se fija la interfaz LAN loopback 0 como pasiva y se desactiva la suma automática con el comando no auto-summary.

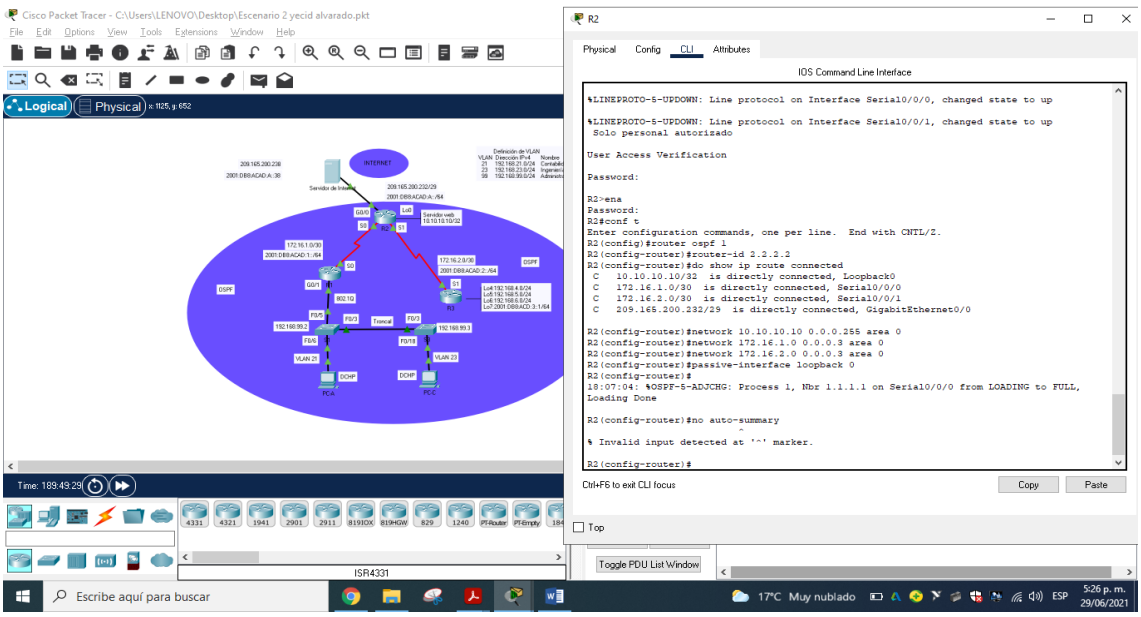

Figura 68. Configuracion protocolo de routin dinamico OSFP en R2: fuente propia

8.3. Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 26. Configuración del protocolo de routin dinámico OSPFv3 en R 3.

Elemento o tarea de configuración	**Especificación**	**solucion**
Configurar OSPF área 0		R3>enable R3 conf t 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

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

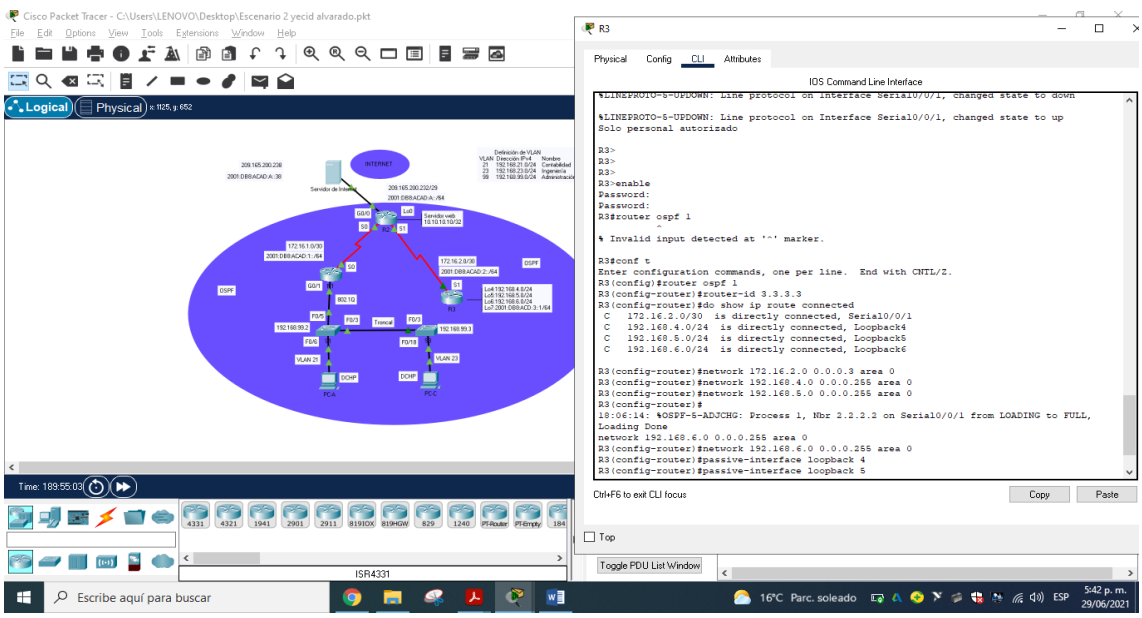

Figura 69. Configuración del protocolo de routin dinámico OSPFv3 en R3: fuente propia

8.4. Paso 4: Verificar la información de OSPF

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

Tabla 27. Verificación de la información del protocolo OSPF

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

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

9. Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 28. Configuración del R1 como servidor DHCP para Vlan 21 y 23

Elemento o tarea de configuración	Especificación	solucion
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas		R1>enable R1#conf t 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

R1 se configura como servidor DHCP para las vlan 21 y 23, para ello con ip dhcp excluded-address acompañado del rango del numero de ip a reservar, en este caso se reservan las primeras 20 direcciones IP en la VLAN 21 y la VLAN 23 para configuraciones estáticas, se crea el pool de DCHP como ACCT para la VLAN 21, se le asigna un nombre de dominio y se establece el Gateway predeterminado con el comando defaul-router, de igual manera se crea el pool DHCP como ENGNR para la VLAN 23.

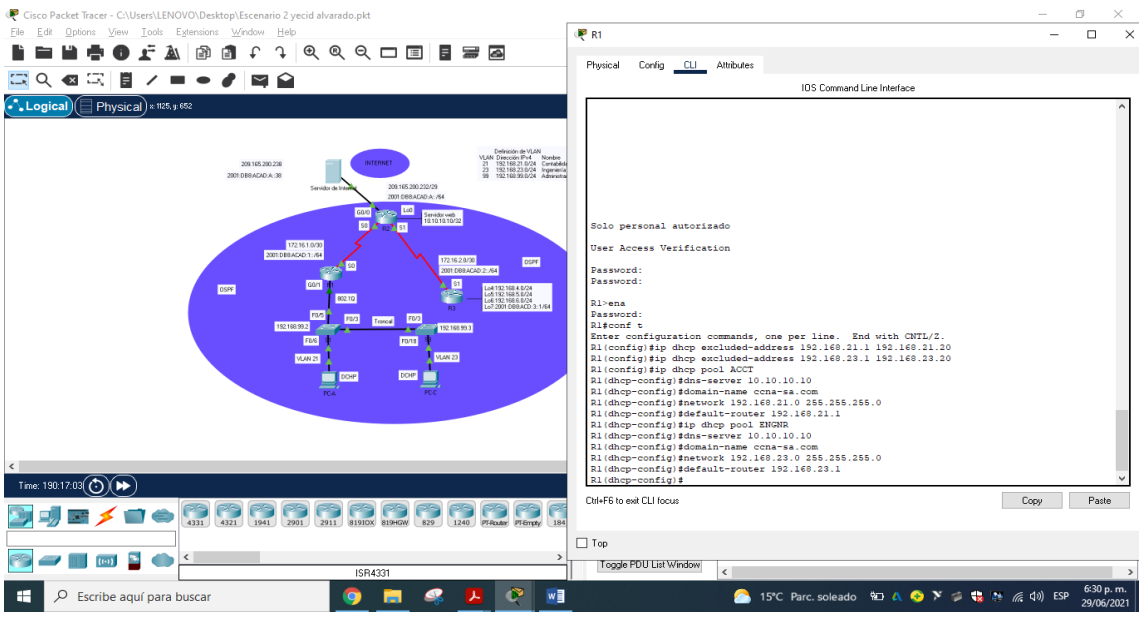

Figura 70. Configuración del Router 1 como servidor DHCP para Vlan 21 y 23 fuente propia

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

La configuración del R2 incluye las siguientes tareas:

Tabla 29. Configuración NAT estática y dinámica en R2

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

El R2 se fija como NAT estática y dinámica, se asignándole un nombre, una contraseña y nivel privilegiado, despues se habilita el servicio del servidor HTTP

con ip http server se configura para que poder utilizar la bases de datos local para la autenticación con ip http autentication local, estas dos últimas configuraciones no surtieron efecto puesto que packet tracert no soporta estos comandos, se crea la NAT estática al servidor Web con el comando ip nat inside source static, se asigna como interfaz externa la g0/0 e interfaz interna la serial s0/0/0 y s0/0/1, se habilita la lista de acceso 1 para permitir la traducción de las redes de contabilidad e ingeniería en el Router 1, se hace los mismo para las redes LAN loopback en el R3, 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, despues se configura la traducción de la NAT dinámica con el comando ip nat inside source list 1 pool Internet.

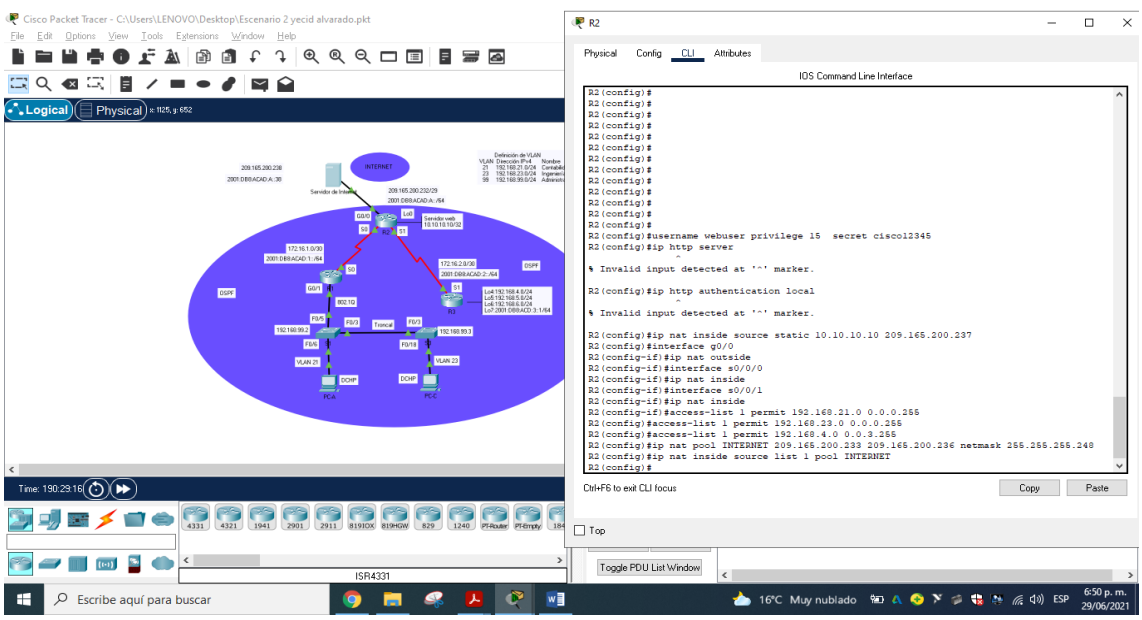

Figura 71. Configuración NAT estática y dinámica en Router 2: fuente propia

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

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

Tabla 30. Verificación del protocolo DHCP y NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Sí hay información
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Sí hay información

Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Sí hay respuesta
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	Si hay respuesta

Se verifica el 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.

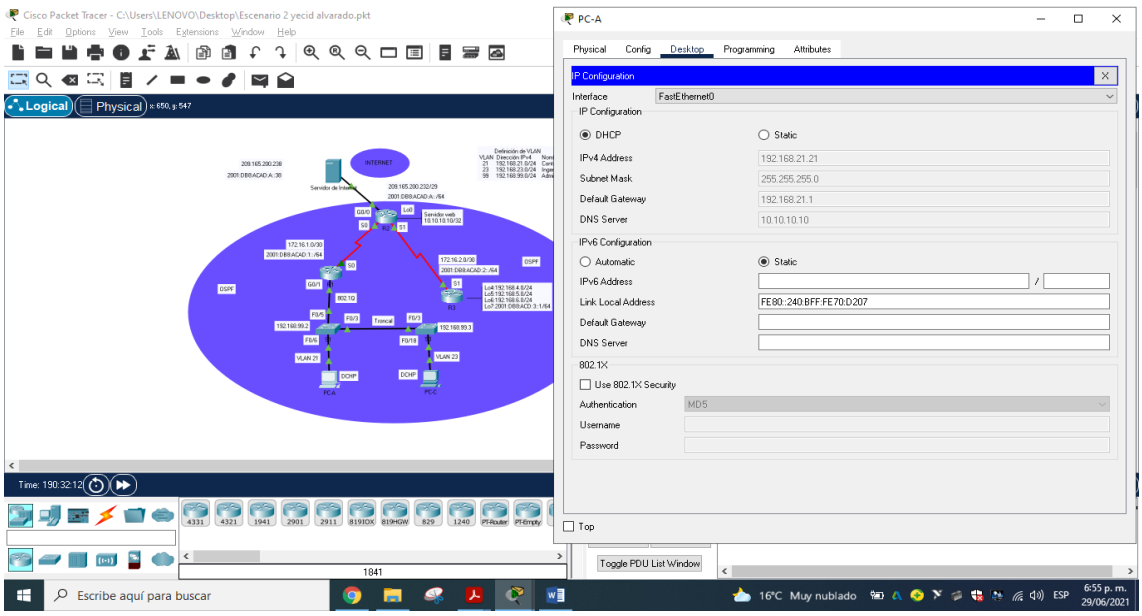

Figura 72. información de IP del servidor DHCP en PC-A: fuente propia

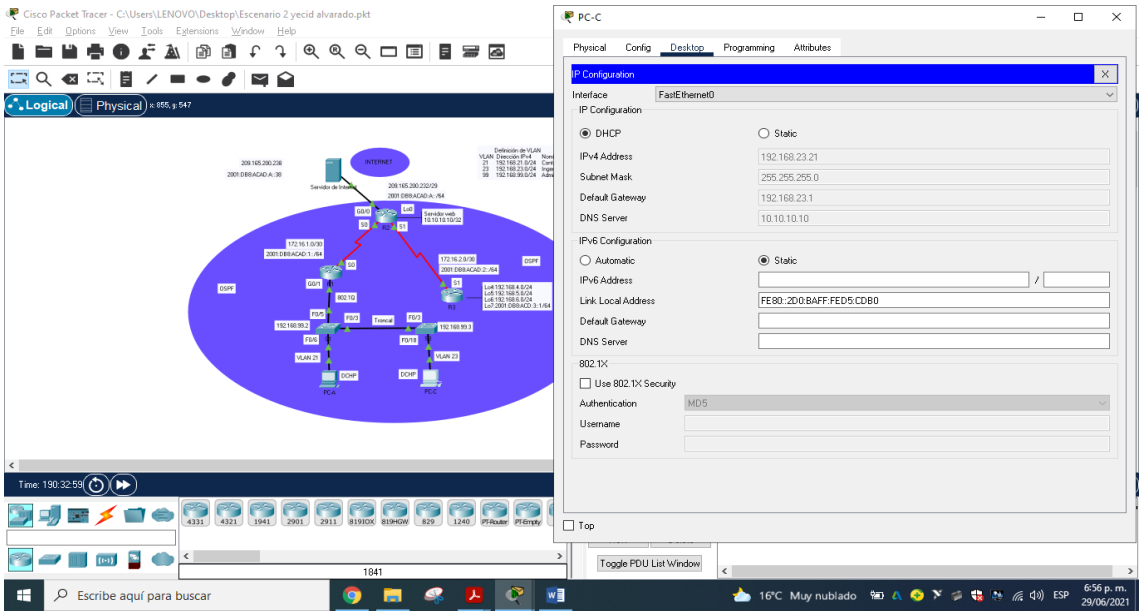

Figura 73. información de IP del servidor DHCP en PC-C: fuente propia

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

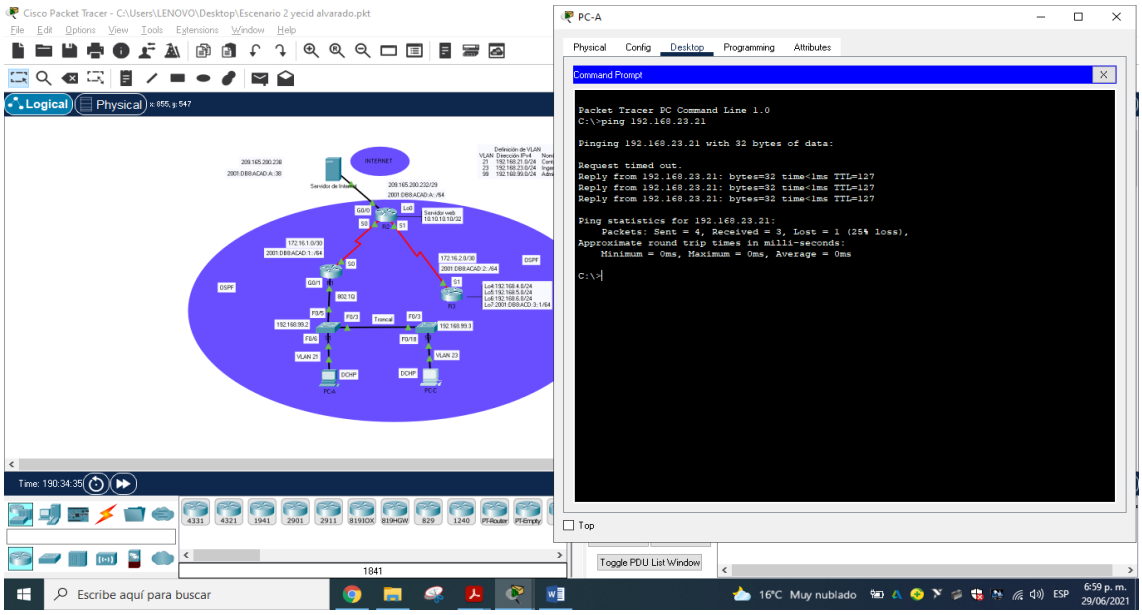

Figura 74. Ping de la PC-A a la PC-C: fuente propia

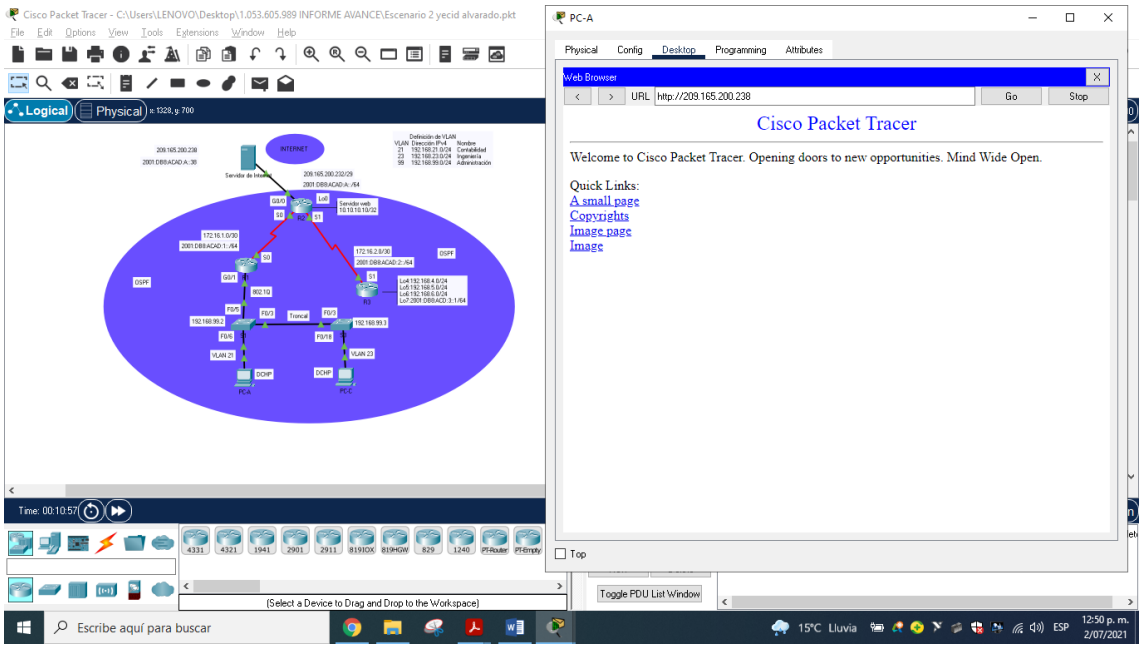

Figura75. navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229). fuente propia

10. Parte 6: Configurar NTP

Tabla 31. Configuración NTP en R2.

Elemento o tarea de configuración	**Especificación**	**Solucion**
Ajuste la fecha y hora en R2.	5 de marzo de 2016, 9 a. m.	R2>enable R2#clock set 09:00:00 5 March 2016 R2(config)
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 R1(config)exit
Verifique la configuración de NTP en R1.		R1#show ntp associations

Configuramos R2 el protocolo NTP, ajustamos la hora y la fecha con clock set y formato 09:00:00 5 march 2016, aplicamos al R2 como maestro NTP nivel de estrato 5 con ntp master 5, luego al R1 aplicamos como cliente NTP el R2 con ntp server y la ip del R2.

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

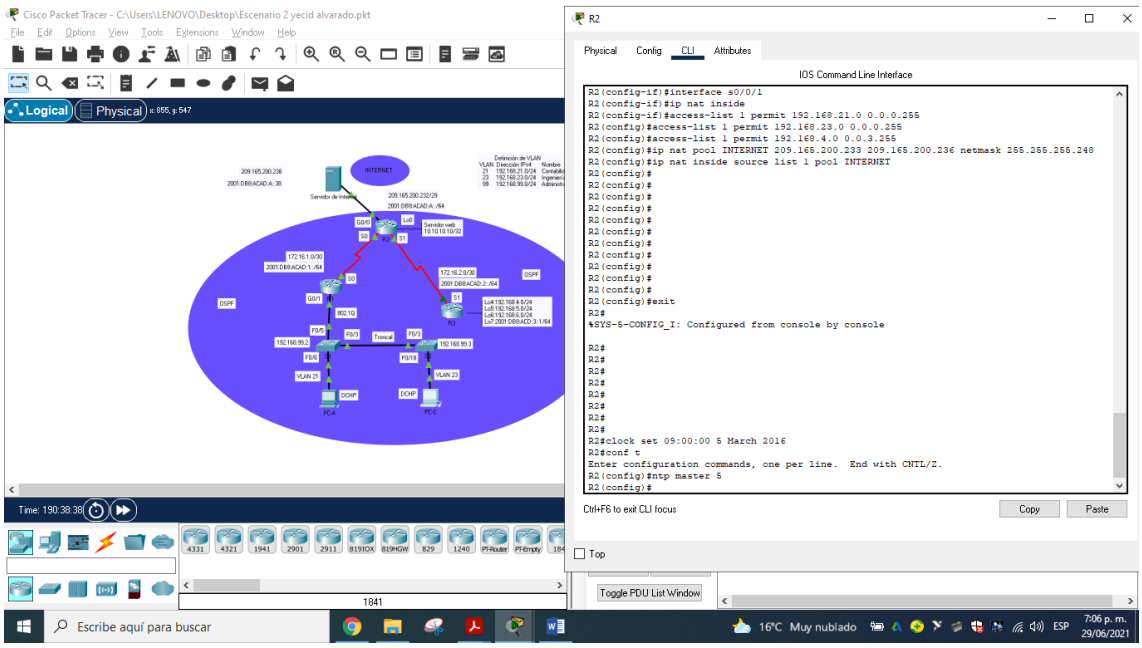

Figura 76. Configuración NTP en R2: fuente propia

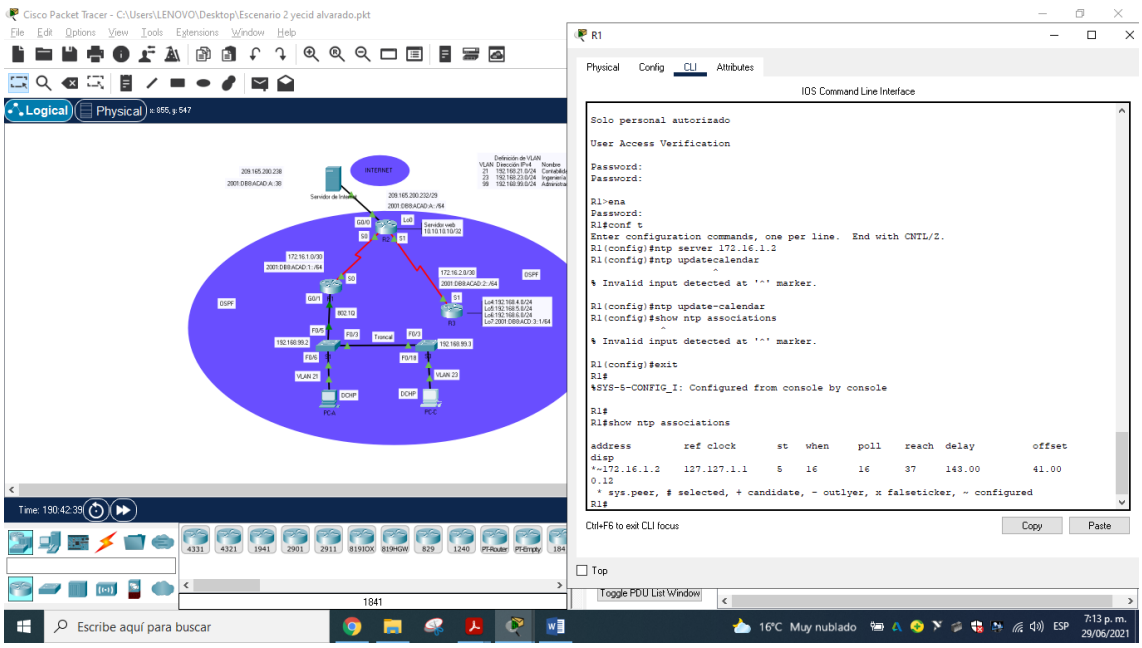

Figura 77. Configuración NTP en R1: fuente propia

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

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

Tabla 32. Restricción de acceso a líneas VTY en R2

Elemento o tarea de configuración	Especificación	solucion
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 R2(config-std-nacl)exit
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 R2(config-line)exit R2(config)exit
Verificar que la ACL funcione como se espera		R1#telnet 172.16.1.2

confuguramos R2 la restricción de acceso a las líneas VTY, se configura ADMIN-MGT con ip acces-list standard para conexión remota con R2, establecemos la entrada a las líneas VTY con Access-class y para que permita el acceso a esas líneas se ejecuta transport input telnet, por ultimo se verificación de conexión de R1 a R2.

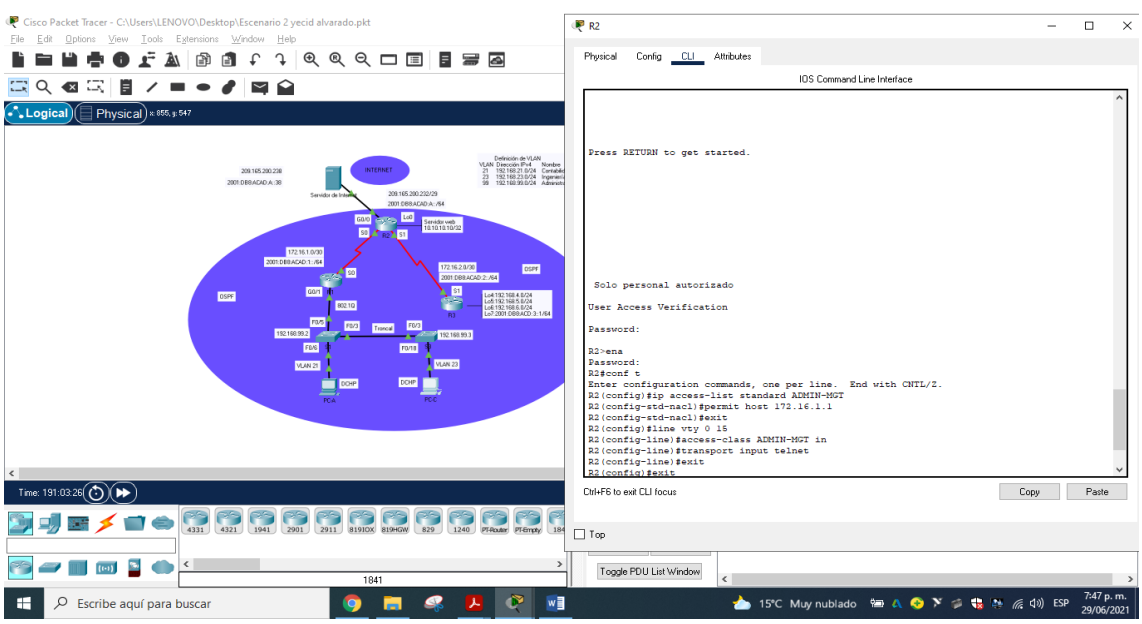

Figura 78. Restricción de acceso a líneas VTY en Router 2: fuente propia

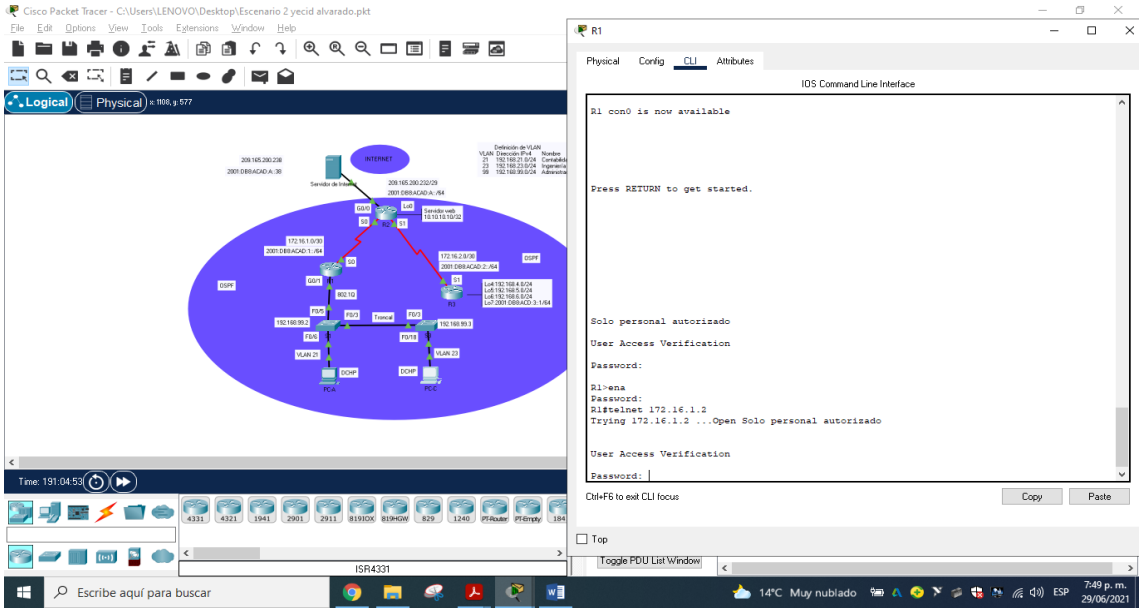

Figura 79. Conexión remota de R1 a R2: fuente propia

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

Tabla 33. Verificación de configuración con comandos CLI

Descripción del comando	Entrada del estudiante (comando)	Solución
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	R2#show ip nat translations

	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.	
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?		R2#clear ip nat translation

En R2 se ingresan comandos CLI para verificar que la configuración

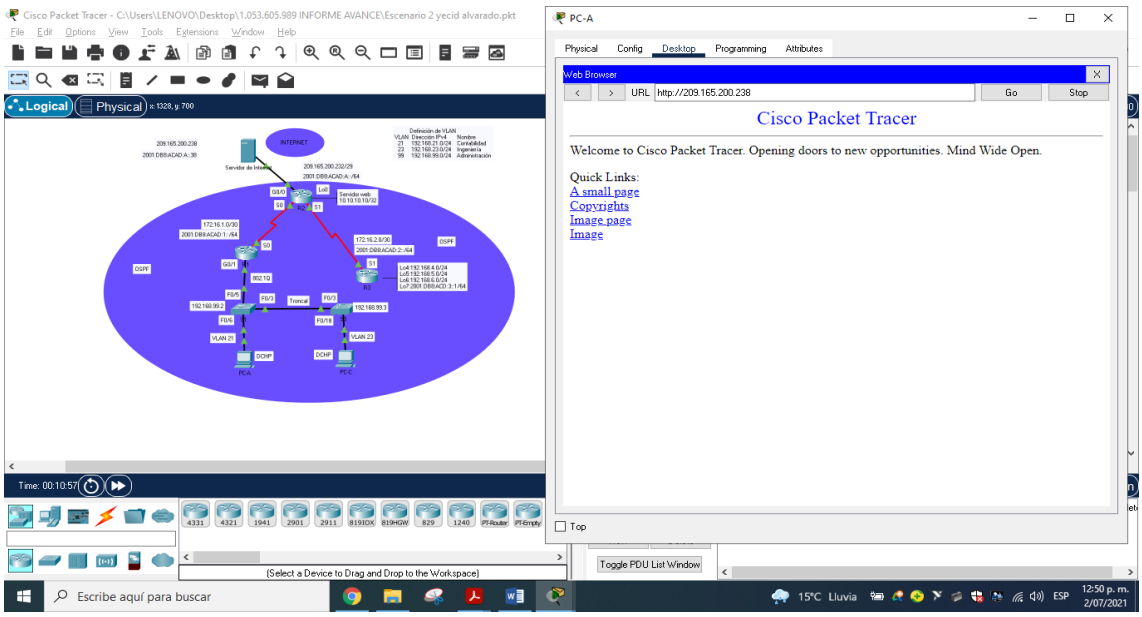

Figura 80. Desde PC-A ping al servidor de Internet: fuente propia

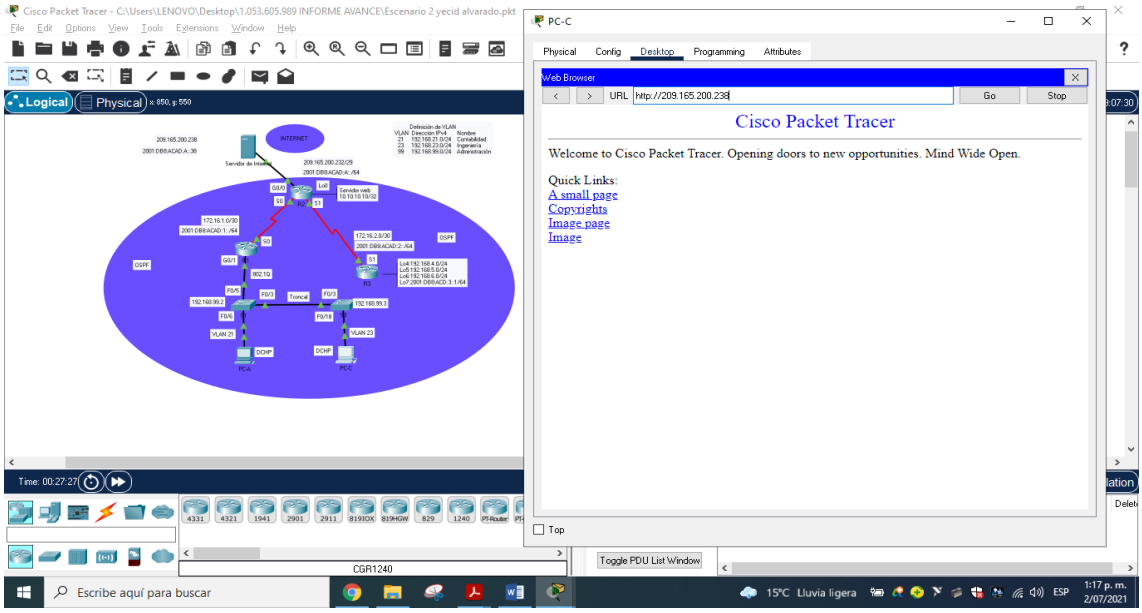

Figura 81. Desde PC-c ping al servidor de Internet: fuente propia

CONCLUSIONES

Por medio del siguiente trabajo se utilizase utilizo las herramientas de simulación con el fin de establecer escenarios LAN/WAN las cuales nos permitieron, realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento.

Por otra parte, con el siguiente trabajo individual identificamos las herramientas de supervisión y protocolos de administración de red disponibles en el IOS igualmente conocimos los problemas de las redes de datos, evaluando el desempeño de routers y switches, mediante el uso de comandos especializados en gestión de redes y compatibles con el protocolo SMNP.

En las practicas de las configuraciones realizadas nos permiten mirar que el protocolo ospf es un buen elemento ya que no es tan difícil de implementar si nosotros como futuros ingenieros electrónicos si realizamos una red física con este programa podemos darnos los parámetros y las herramientas que vamos a utilizar en la red física

BIBLIOGRÁFIA

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación.Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

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

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

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

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

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

Anexo 1. Artículo científico IEEE

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNA

Yecid Fabian Alvarado Guio
yfalvaradog@unadvirtual.edu.co
Escuela de Ciencias Básicas, Tecnología e Ingeniería
Universidad Nacional Abierta y a Distancia (UNAD)

Resumen

la prueba de habilidades nos da un conocimiento amplio sobre la utilización de las herramientas de simulación junto con los laboratorios remotos con el fin de establecer escenarios LAN/WAN que nos permite analizar sobre el comportamiento de diversos protocolos y métricas de enrutamiento

Además, busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del curso. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

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

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

ABSTRACT

The skills test gives us extensive knowledge about the use of simulation tools in conjunction with remote labs in order to establish LAN / WAN scenarios that allows us to analyze the behavior of various routing protocols and metrics

In addition, it seeks to identify the degree of development of skills and abilities that were acquired throughout the course. The essential thing is to test the levels of understanding and problem solving related to various aspects of Networking.

Electronic engineers must be able to perform a diagnosis and a highly accurate and efficient network configuration that allows them to provide solutions and answers to the various problems that information, electronic and data networks may present.

Keywords: CISCO, CCNP, Switching, Routing, Networks, Electronics.

INTRODUCCION

Por medio del siguiente trabajo se utiliza herramientas de simulación con el fin de establecer escenarios LAN/WAN que permitan realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento. Junto a ello identificaremos las herramientas de supervisión y protocolos de administración de red disponibles en el IOS para resolver los problemas de las redes de datos, evaluando el desempeño de routers y switches, mediante el uso de comandos especializados en gestión de redes y compatibles con el protocolo SMNP.

Prueba de habilidades está conformada por dos (2) escenarios, el estudiante deberá realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: Packet Tracer o GNS3. 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.

I. PROCEDIMIENTO PARA ADMINISTRAR UNA RED LAN USANDO OSPF

El procedimiento para llevar a cabo la configuración del protocolo OSPF (Open Shortest Path First) de la siguiente pequeña red, se realiza por medio de los siguientes pasos y estos son:

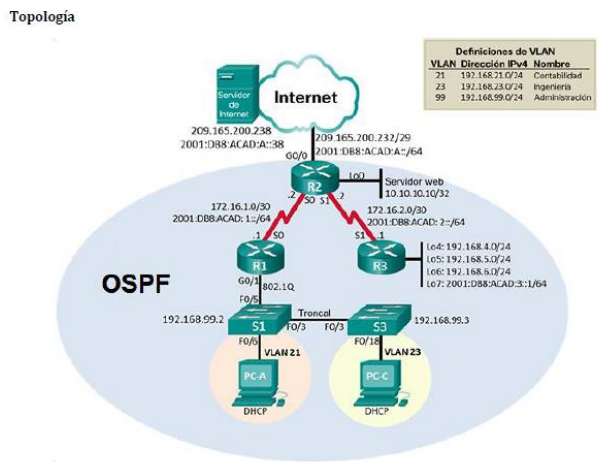

Figura 1. Topología de la red

Realizamos la topología de red utilizando para ello 3 Routers 1941, 2 Switchs 2960, 2 Computadoras, 1 Servidor y cables de cobre directos para la conexión

Inicializar dispositivos

Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.
Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 1. Eliminar las configuraciones de inicio de los Routers y vuelva a cargarlos.

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

Se accede al Router 1,2 y 3 a través de la consola en modo privilegiado para borrar configuración de inicio con erase startup-config el cual borra lo que contiene NVRAM, después reiniciamos el Router con reload, quedando listo para la configuración de inicio.

Tabla 2. Eliminacion configuraciones de inicio de los Switchs y vuelver a cargarlos.

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

Ingresamos al Switch 1 y 2 a través del modo privilegiado erase startup-config el cual borra la NVRAM junto con delete vlan.dat este elimina la base de datos de la vlan, esto permite restaurar el switch y borrar la configuración de inicio, después se reinicia con reload, quedando listo para la configuración, y con show flash se verifica que los datos VLAN se halla borrado de la memoria flash.

Tabla 3. Configuración de los parámetros básicos en los dispositivos R1

Elemento o tarea de configuración	Solucion
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada,	R1(config)#enable secret class
Contraseña de acceso a la consola,	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet,	R1(config-line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service password-encryption
Mensaje MOTD	R1(config)#banner motd "Solo personal autorizado"
Interfaz S0/0/0	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 R1(config-if)#exit
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Las tareas de configuración para R1, R2 y R3 incluyen las siguientes:

Tabla 4. Configuración R2

Elemento o tarea de configuración	Solucion
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router,	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada,	R2(config)#enable secret class
Contraseña de acceso a la consola,	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet,	R2(config)#line 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,	R2(config)#banner motd " Solo personal autorizado"
Interfaz S0/0/0	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	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)	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)	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	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

Después de realizar las configuraciones básicas en los dispositivos es importante por medio del comando ping probar la conectividad entre los dispositivos de red.

La configuración del S1 incluye las siguientes tareas:

Tabla 5 Configurar la seguridad del switch, las VLAN y el routing entre VLAN

Elemento o tarea de configuración	**Solucion**
Crear la base de datos de VLAN	S1>enable 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 S1(config-vlan)exit
Asignar la dirección IP de administración.	S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)exit
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface Fa0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if) exit
Forzar el enlace troncal en la interfaz F0/5	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

Una vez realizada la creación y configuración de las VLAN en S1 y S3, procedemos a configurar la interfaz G0/1. Las tareas de configuración para R1 incluyen las siguientes:

Tabla 6. Configuración Subinterfaz 802.1Q en el Router 1

Elemento o tarea de configuración	**solucion**
Configurar la subinterfaz 802.1Q .21 en G0/1	R1>enable R1#configure terminal 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	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	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

CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO OSPF

En esta sección se describen los comandos para realizar la configuración OSPF en la red. Las tareas de configuración para R1 son:

Tabla 7. Configurar OSPF

Elemento o tarea de configuración	**Solucion**
Configurar OSPF área 0	R1>enable R1#conf t R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1
Anunciar 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

Tabla 8. La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	**solucion**
Configurar OSPF área 0	R3>enable R3 conf t 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

VERIFICAR LA INFORMACIÓN DE OSPF

Después de realizar las configuraciones anteriores en los dispositivos verificamos que OSPF esté funcionando como se espera. Por medio de los siguientes comandos

Tabla 9. 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

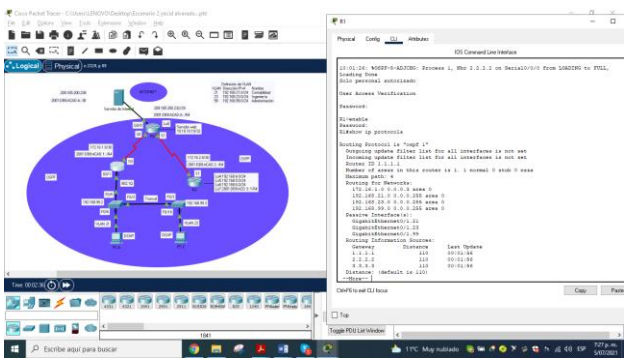

Figura 1. Comando para ver ID del proceso OSPF. Fuente propia

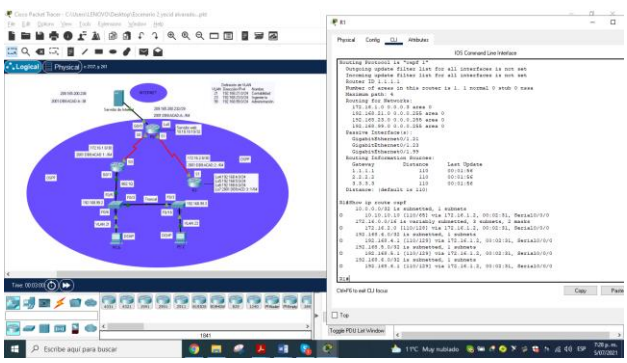

Figura 2. Comando para mostrar solo las rutas OSPF. Fuente propia

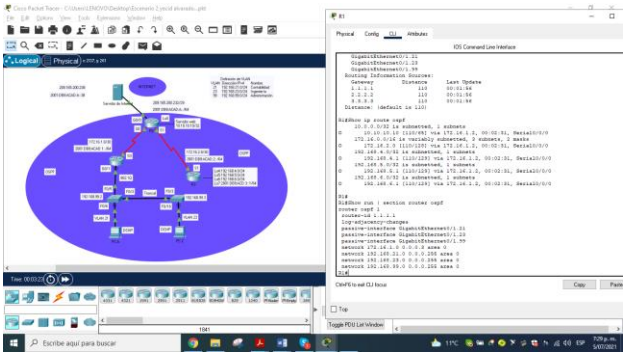

Figura 3. Muestra la sección de OSPF de la configuración en ejecución. Fuente propia

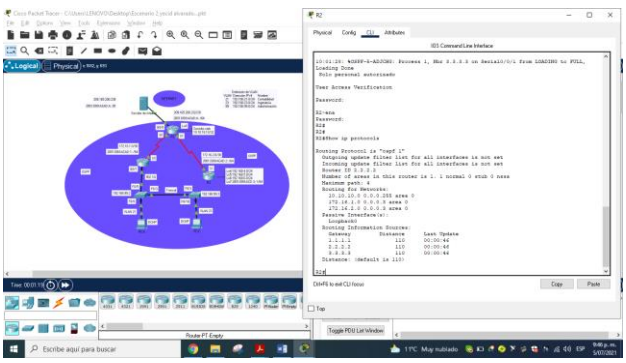

Figura 4. Comando para ver ID del proceso OSPF. Fuente propia

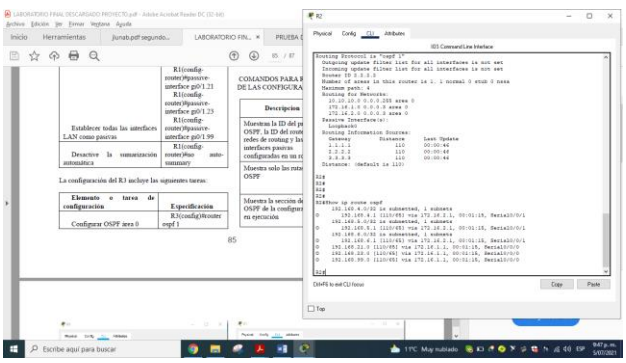

Figura 5. Comando para mostrar solo las rutas OSPF. Fuente propia

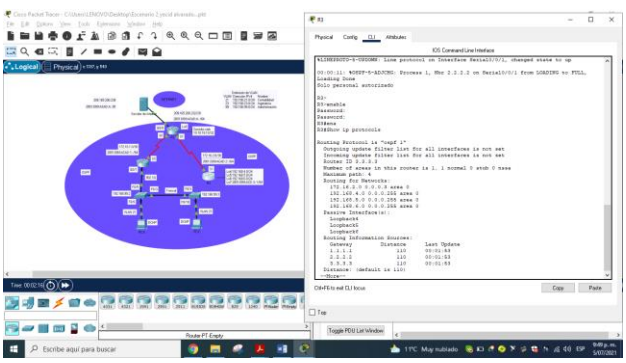

Figura 6. Comando para ver ID del proceso OSPF. Fuente propia.

CONCLUSIONES

En las parcticas de las configuraciones realizadas nos permiten mirar que el protocolo OSPF, es un buen elemento ya aque no es tan difícil de implementar si nosotros como futuros ingenieros electrónicos si realizamos una red física con este programa podemos darnos los parámetros y las herramientas que vamos a utilizar en la red física

Por otra parte, con el siguiente trabajo individual identificamos las herramientas de supervisión y protocolos de administración de red disponibles igualmente conocimos los problemas de las redes de datos, evaluando el desempeño de routers y switches, mediante el uso de comandos especializados en gestión de redes y compatibles.

BIBLIOGRAFÍA

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

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

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

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

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

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

CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

CISCO. (2017). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO. (2017). Soluciones de Red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

CISCO. (2017). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

UNAD (2017). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

BIBLIOGRAFIA

Yecid Fabian Alvarado Guio estiudiante de ingeniería electrónica me guta mucho todo lo relacionado con la electrónica y sus avances mis proyecciones de vida es ser cada dia mejor estudiar cada dia con las nuevas tecnologías y los avances de la actrovica y ser un excelente ser una mano tanto como en mi vida personal como laboral profesional