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

LEIDY SOLANDY GÓMEZ GONZALEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERIA-ECBTI.
INGENIERÍA DE SISTEMAS.
MADRID
2021

LEIDY SOLANDY GÓMEZ GONZALEZ

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

MSc. JAVIER RICARDO VASQUEZ ROJAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA-ECBTI.
INGENIERÍA DE SISTEMAS.
MADRID
2021

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Madrid, 26 de noviembre de 2021.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ROUTER: Un router es un dispositivo de hardware que permite la interconexión de ordenadores en red.

IP: IP es la sigla de Internet Protocol o, en nuestro idioma, Protocolo de Internet. Se trata de un estándar que se emplea para el envío y recepción de información mediante una red que reúne paquetes conmutados.

SUBRED: Son un método para maximizar el espacio de direcciones IPv4 de 32 bits y reducir el tamaño de las tablas de enrutamiento en una interred mayor.

ETHERNET: Es una tecnología que conecta redes de área local (LAN) cableadas y permite que el dispositivo se comunique entre sí a través de un protocolo que es el lenguaje de red común.

RESUMEN

El presente trabajo aborda temáticas relacionadas con las redes y el mundo de las telecomunicaciones donde es posible aplicar conocimientos y adquirir habilidades para solucionar problemáticas que se presenten en dichos entornos, teniendo en cuenta un análisis estructurado de los requerimientos de los clientes generando así productos y servicios de calidad.

Se aplica configuraciones de dispositivos de Red LAN, estableciendo direccionamiento IPV4 y seguridad en los distintos modos de acceso a los equipos, garantizando un acceso restringido y protección en el sistema, estableciendo enlace en la red y conectividad entre los dispositivos.

PALABRAS CLAVE: CISCO, CCNA, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

This paper addresses issues related to networks and the world of telecommunications where it is possible to apply knowledge and acquire skills to solve problems that arise in these environments, taking into account a structured analysis of customer requirements, thus generating products and services quality.

Network LAN device configurations are applied, establishing IPV4 addressing and security in the different modes of access to the equipment, guaranteeing restricted access and protection in the system, establishing link in the network and connectivity between the devices.

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

INTRODUCCIÓN

En esta actividad se lleva a cabo el desarrollo de una Red en la cual se establece un esquema de direccionamiento IPV4, para ello se configura los dispositivos que la componen, aplicando los diferentes comandos en la terminal de cada equipo garantizando de esta manera la seguridad en el acceso y la conectividad en los dispositivos.

Se implementa comunicación entre dispositivos por medio de las VLAN y protocolo OSPF permitiendo que haya interacción entre las diferentes redes LAN y se obtenga conectividad a la red WAN.

Se lleva a cabo configuraciones de subinterfaces en las interfaces primarias generando tráfico a través de los medios para la comunicación de las diferentes VLAN creadas, permitiendo así que los Router establezcan una ruta determinada de los paquetes recibidos, de igual manera se aplica NAT protocolo que traduce una red local en una red pública para la conexión a internet.

Se implementa enrutamiento estático y dinámico, se aplica listas de acceso para permitir o denegar tráfico de un dispositivo, logrando así el diseño de una red que cumple con los estándares de velocidad, calidad, escalabilidad y seguridad.

Es importante tener en cuenta la seguridad de los dispositivos en una Red, evitando así accesos no deseados en el sistema que pondría en peligro la información y los datos personales de los usuarios, es así como este curso está enfocado en dar a conocer las formas de incorporar seguridad, rendimiento y calidad.

En el curso es posible adquirir conocimientos y habilidades que permitan la construcción de redes según los requerimientos de los clientes logrando abarcar en soluciones avanzadas y eficientes de seguridad para el funcionamiento optimo del sistema.

OBJETIVOS

OBJETIVO GENERAL

Desarrollar escenarios de redes estableciendo parámetros básicos de configuración, seguridad y conectividad.

OBJETIVOS ESPECÍFICOS

Construir esquema físico y lógico de la red, adaptando el cálculo de subnetting de subredes.

Configurar dispositivos intermediarios y terminales aplicando ajustes seguridad y parámetros de funcionalidad.

Configurar una red que permita conectividad IPV4 e IPV6.

Aplicar seguridad entre dispositivos, mediante la creación de VLAN.

Implementar protocolos OSPF, DHCP, NAT y NTP para la interacción en la red.

Activar listas ACL para la seguridad de acceso a la información de los hosts.

DESARROLLO.

1. Escenario 1.

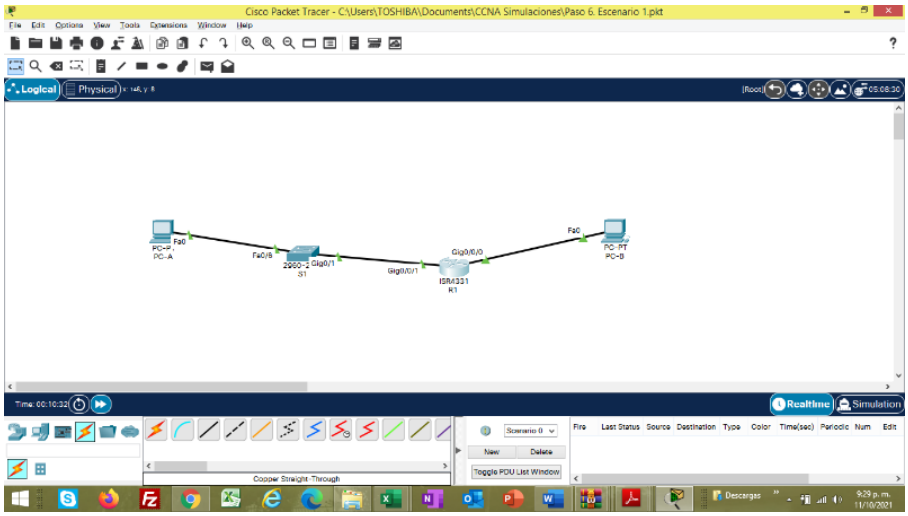
Figura 1. Topología Escenario propuesto.

Fuente: Vesga Juan Carlos. Evaluación – Prueba de habilidades Practicas CCNA.

1.1. Parte 1. Construya la Red.

En el simulador construya la red de acuerdo con la topología lógica que se plantea en la figura 1, cablee conforme se indica en la topología, y conecte los equipos de cómputo.

Figura 2. Simulación Red.



Fuente: Propia. Topología Escenario 1 en PT.

1.2. Parte 2. Desarrolle el esquema de direccionamiento IP.

Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento.

Cada estudiante tomará el direccionamiento 192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula.

Cedula: 10698528***06***

Dirección de Red: 192.168.06.0
Mascara de Subred: 255.255.255.0

Subred LAN1:

Mascara de Subred binaria: 11111111.11111111.11111111.00000000

Se utiliza la formula $2^7 = 128$ para abarcar el requerimiento de 100 host, y se tendrían 7 bits para la porcion de host.

Nueva Mascara de Subred binaria: 11111111.11111111.11111111.10000000
Notación decimal: 255.255.255.128
Prefijo: /25
Saltos = $2^7 = 128 - 2 = 126$
Rango: 192.168.06.1 – 192.168.06.126
Broadcast = 192.168.06.127/25

Subred LAN2:

Dirección de Red: 192.168.06.128
Mascara de Subred binaria: 11111111.11111111.11111111.10000000

Se utiliza la formula $2^6 = 64$ para abarcar el requerimiento de 50 host, por lo que se tendría 6 bits para la porción de host.

Nueva Mascara de Subred binaria: 11111111.1111111.11111111.11000000
Notación decimal: 255.255.255.192
Prefijo: /26
Saltos = $2^6 = 64 - 2 = 62$
Rango: 192.168.06.129 – 192.168.06.190
Broadcast = 192.168.06.191/26

Tabla 1. Direccionamiento.

Ítem	Requerimiento
Dirección de Red	192.168.06.0
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	192.168.06.1/25
R1 G0/0/0	192.168.06.129/26
S1 SVI	192.168.06.2/25
PC-A	192.168.06.126/25
PC-B	192.168.06.190/26

Fuente: Propia. Esquema de direccionamiento.

1.3. Parte 3. Configure aspectos básicos.

1.3.1. Paso 1. Configurar los aspectos básicos.

Tabla 2. Configuración R1.

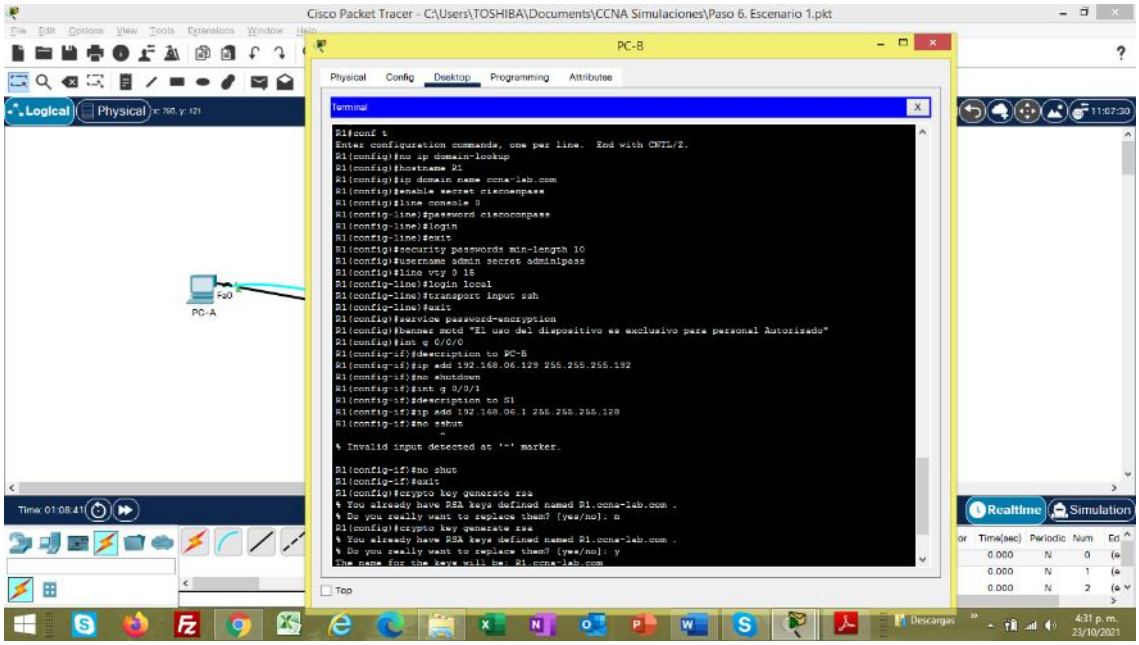
Tarea	Especificación	*Comandos*
Desactivar la búsqueda DNS		*Router>enable* *Router#configure terminal* *Router(config)#no ip domain-lookup* *R1(config)#*
Nombre del router	R1	*Router>enable* *Router#configure terminal* *Router(config)#hostname R1* *R1(config)#*
Nombre de dominio	ccna-lab.com	*R1>enable* *R1#configure terminal* *R1(config)# ip domain name ccna-lab.com* *R1(config)#*
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass	*R1>enable* *R1#configure terminal* *R1(config)#enable secret ciscoenpass* *R1(config)#*
Contraseña de acceso a la consola	ciscoconpass	*R1>enable* *R1#configure terminal* *R1(config)#line console 0* *R1(config-line)#password ciscoconnpass* *R1(config-line)#login* *R1(config-line)#exit* *R1(config)#*
Establecer la longitud mínima para las contraseñas	10 caracteres	*R1>enable* *R1#configure terminal* *R1(config)#security passwords min-length 10* *R1(config)#*

Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**	*R1>enable* *R1#configure terminal* *R1(config)# username admin secret admin1pass* *R1(config)#*
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local		*R1>* *R1>enable* *R1#configure terminal* *R1(config)# line vty 0 15* *R1(config-line)#login local* *R1(config-line)#*
Configurar VTY solo aceptando SSH		*R1>* *R1>enable* *R1#configure terminal* *R1(config)# line vty 0 15* *R1(config-line)#login local* *R1(config-line)# transport input ssh* *R1(config-line)#*
Cifrar las contraseñas de texto no cifrado		*R1>* *R1>enable* *R1#configure terminal* *R1(config)# service password-encryption* *R1(config)#*
Configure un MOTD Banner		*R1>* *R1>enable* *R1#configure terminal* *R1(config)#banner motd "El uso del dispositivo es exclusivo para personal Autorizado"* *R1(config)#*
Configurar interfaz G0/0/0	Establezca la descripción Establece la dirección IPv4. Activar la interfaz.	*R1>* *R1>enable* *R1#configure terminal* *R1(config)#int g 0/0/0* *R1(config-if)#description to PC-B* *R1(config-if)#ip address 192.168.06.129 255.255.255.192* *R1(config-if)#no shutdown* *R1(config-if)#exit* *R1(config)#*

Configurar interfaz G0/0/1	Establezca la descripción Establece la dirección IPv4. Activar la interfaz.	*R1>enable* *R1#configure terminal* *R1(config)#int g 0/0/1* *R1(config-if)#description to S1* *R1(config-if)#ip address 192.168.06.1 255.255.255.128* *R1(config-if)#no shutdown* *R1(config-if)#exit* *R1(config)#*
Generar una clave de cifrado RSA	Módulo de 1024 bits	*R1(config)#crypto key generate rsa* *The name for the keys will be: R1.ccna-lab.com* *Choose the size of the key modulus in the range of 360 to 2048 for your* *General Purpose Keys.* *Choosing a key modulus greater than 512 may take* *a few minutes.* *How many bits in the modulus [512]:* ***1024*** *% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]* *R1(config)#*

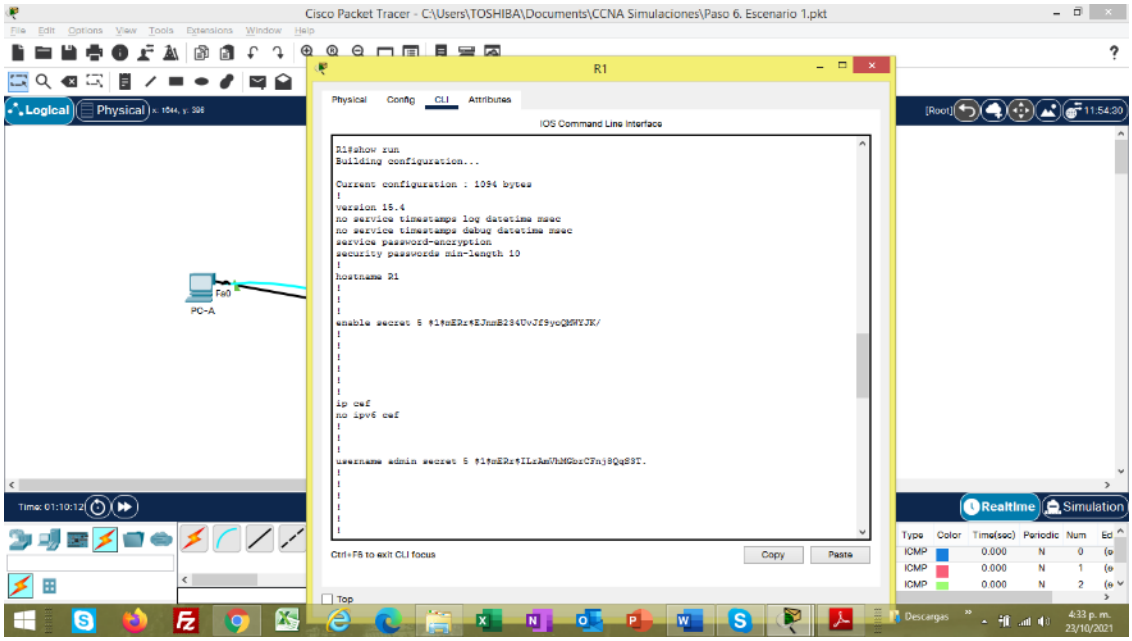
Fuente: Propia. Configuración básica de R1.

Figura 3. Configuración Consola R1.



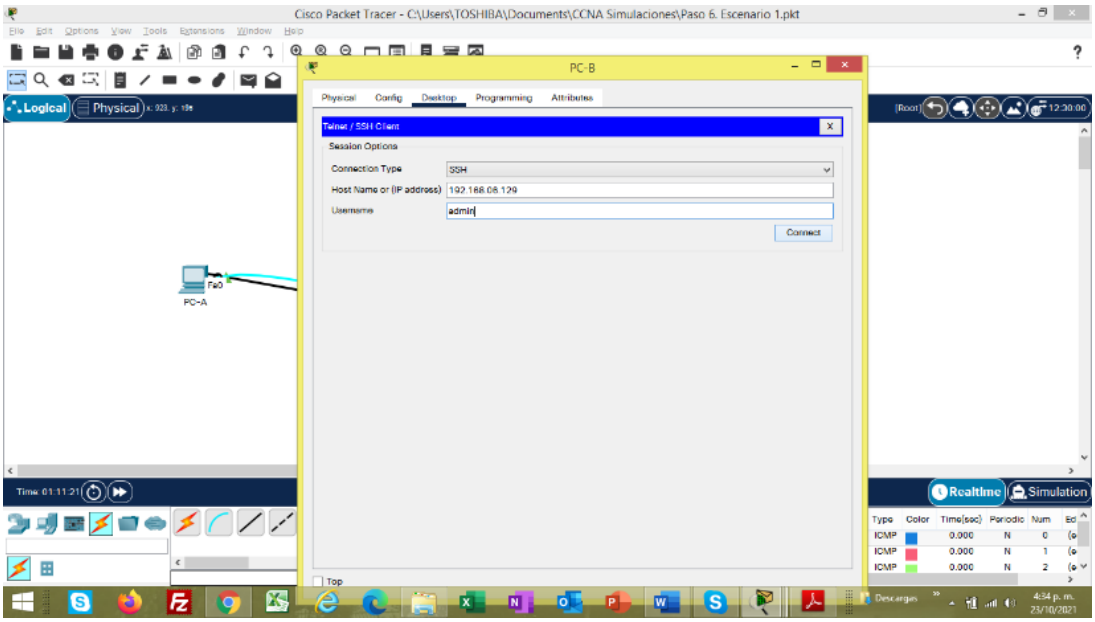
Fuente: Propia. Configuración por terminal en PC-B.

Figura 4. Contenido de configuración en R1.



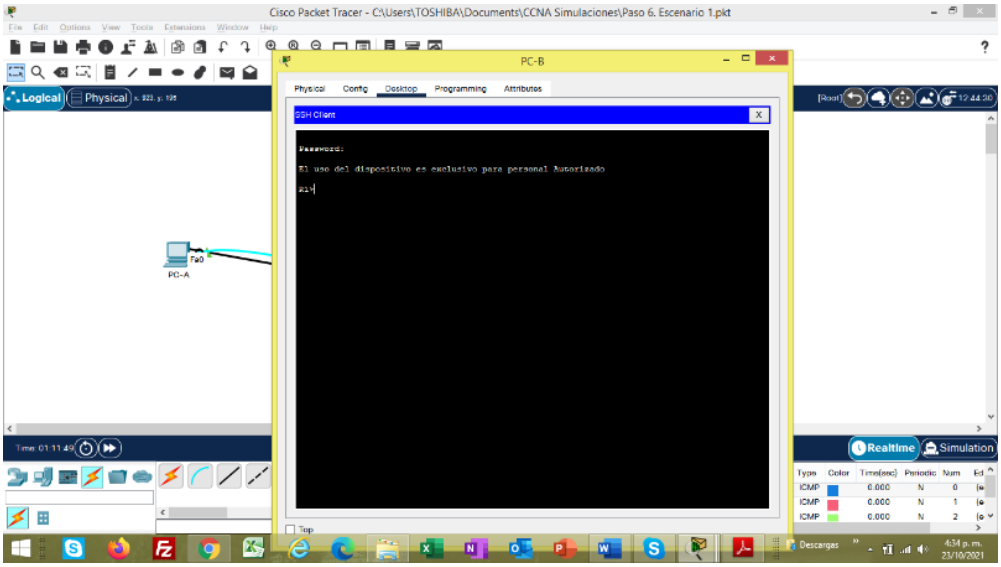
Fuente: Propia. Comando Show Run.

Figura 5. Acceso a Protocolo SSH desde PC-B.



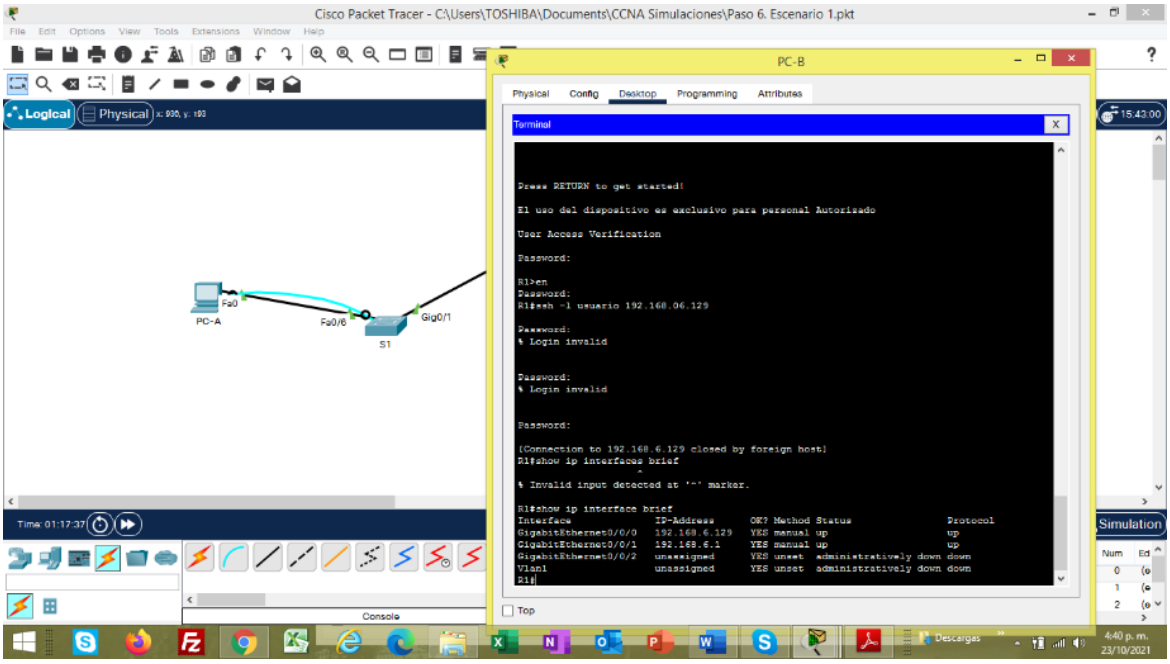
Fuente: Propia. Verificación de conectividad por SSH.

Figura 6. Conexión a R1 desde SSH en PC-B.



Fuente: Propia. Ingreso a R1 por SSH.

Figura 7. Acceso R1 desde Consola por SSH en PC-B.



Fuente: Propia. Acceso por Terminal a R1.

Configuración completa R1.

R1#show run
Building configuration...

Current configuration : 1094 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 10
!
hostname R1
!
!
!
enable secret 5 1mERr$EJnmB234UvJf9yoQMWYJK/

!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
username admin secret 5 1mERr$ILrAmVhMGbrCFnj8QqS3T.
!
!
!
!
!
!
!
!
no ip domain-lookup
ip domain-name ccna-lab.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0/0
description to PC-B
ip address 192.168.6.129 255.255.255.192
duplex auto
speed auto
!
interface GigabitEthernet0/0/1
description to S1
ip address 192.168.6.1 255.255.255.128
duplex auto
speed auto
!
interface GigabitEthernet0/0/2
no ip address

duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^CEl uso del dispositivo es exclusivo para personal Autorizado^C
!
!
!
!
!
line con 0
password 7 0822455D0A1606181C1B0D1739
login
!
line aux 0
!
line vty 0 4
login local
transport input ssh
line vty 5 15
login local
transport input ssh
!
!
!
End

Tabla 3. Configuración S1.

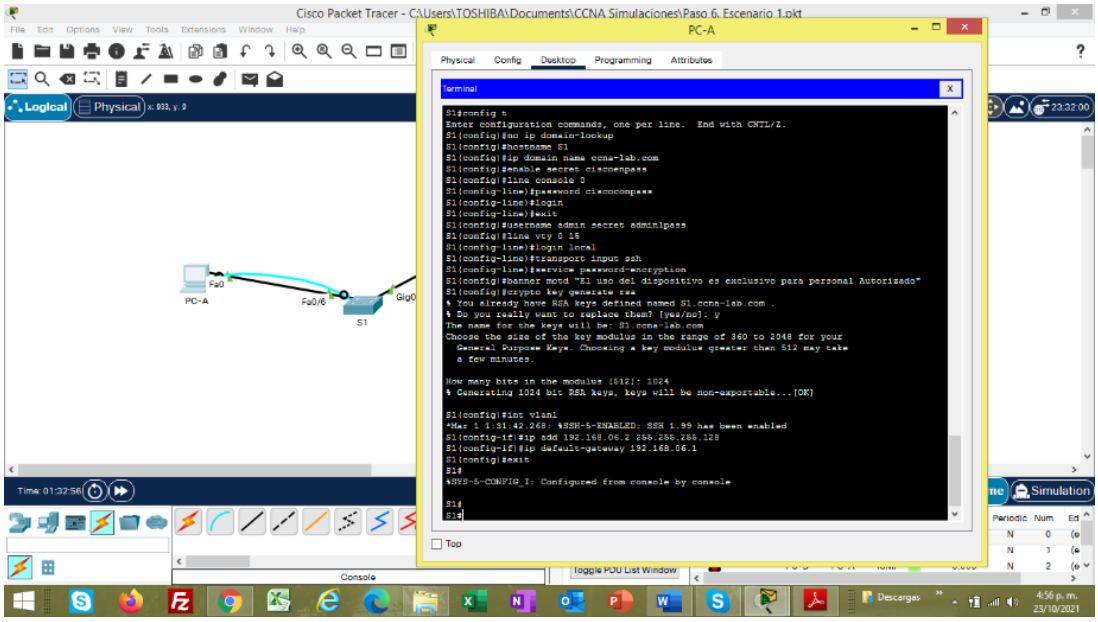
Tarea	Especificación	*Comandos*
Desactivar la búsqueda DNS		*Switch> Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup Switch(config)#*
Nombre del Switch	S1	*Switch> Switch>enable Switch#configure terminal Switch(config)#hostname S1 S1(config)#*
Nombre de dominio	ccna-lab.com	*S1> S1>enable S1#configure terminal S1(config)# ip domain name ccna-lab.com S1(config)#*
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass	*S1> S1>enable S1#configure terminal S1(config)#enable secret ciscoenpass S1(config)#*
Contraseña de acceso a la consola	ciscoconpass	*S1> S1>enable S1#configure terminal S1(config)#line console 0 S1(config-line)# S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit S1(config)#*
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**	*S1> S1>enable S1#configure terminal S1(config)# username admin secret admin1pass S1(config)#*
Configurar el inicio de sesión en las líneas VTY		*S1> S1>enable*

para que use la base de datos local		*S1#configure terminal* *S1(config)# line vty 0 15* *S1(config-line)#login local* *S1(config-line)#*
Configurar VTY solo aceptando SSH		*S1>* *S1>enable* *S1#configure terminal* *S1(config)# line vty 0 15* *S1(config-line)#login local* *S1(config-line)#transport input ssh* *S1(config-line)#*
Cifrar las contraseñas de texto no cifrado		*S1>* *S1>enable* *S1#configure terminal* *S1(config)# service password-encryption* *S1(config)#*
Configure un MOTD Banner		*S1>* *S1>enable* *S1#configure terminal* *S1(config)#banner motd "El uso del dispositivo es exclusivo para personal Autorizado"* *S1(config)#*
Generar una clave de cifrado RSA	Módulo de 1024 bits	*S1>* *S1>enable* *S1#configure terminal* *S1(config)#crypto key generate rsa* *The name for the keys will be: S1.ccna-lab.com* *Choose the size of the key modulus in the range of 360 to 2048 for your* *General Purpose Keys.* *Choosing a key modulus greater than 512 may take* *a few minutes.* *How many bits in the modulus [512]: 1024*

		% Generating 1024 bit RSA keys, keys will be non-exportable...[OK] *S1(config)#*
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento	*S1(config)#interface vlan 1* *S1(config-if)#ip address 192.168.06.2 255.255.255.128* *S1(config-if)#*
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento.	*S1>* *S1>enable* *S1#configure terminal* *S1(config-if)#ip default-gateway 192.168.06.1* *S1(config-if)#*

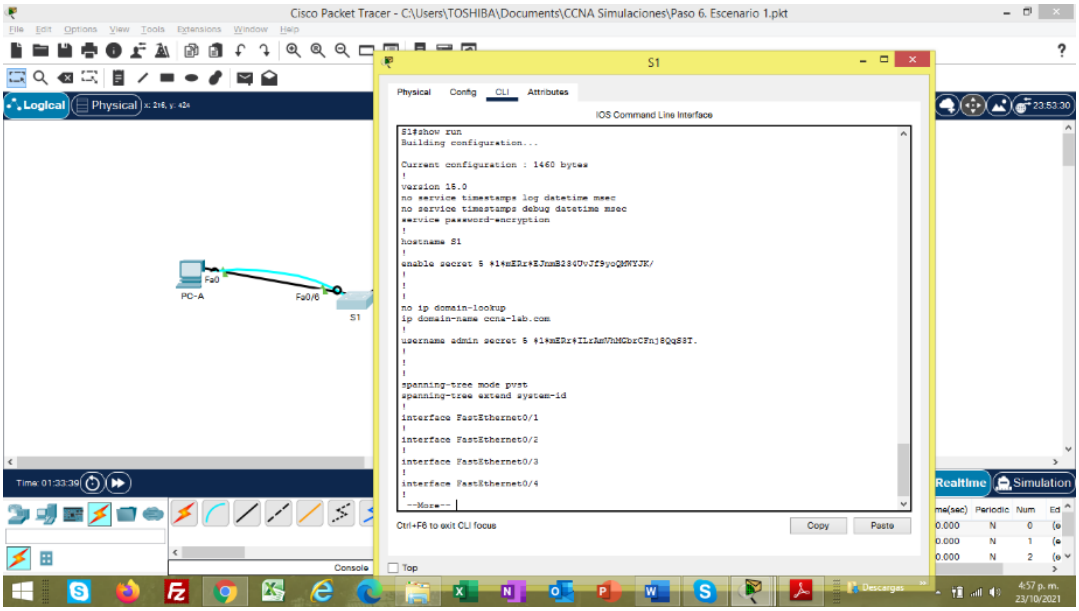
Fuente: Propia. Configuración básica en S1.

Figura 8. Configuración Consola S1.



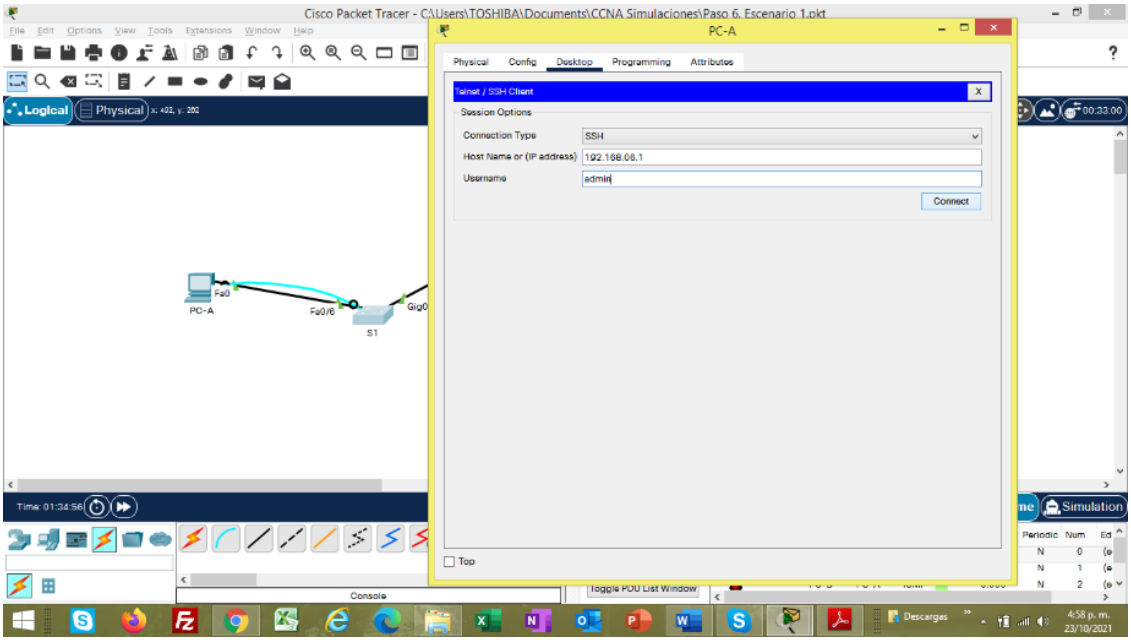
Fuente: Propia. Ingreso a terminal PC-A.

Figura 9. Contenido de configuración en S1.



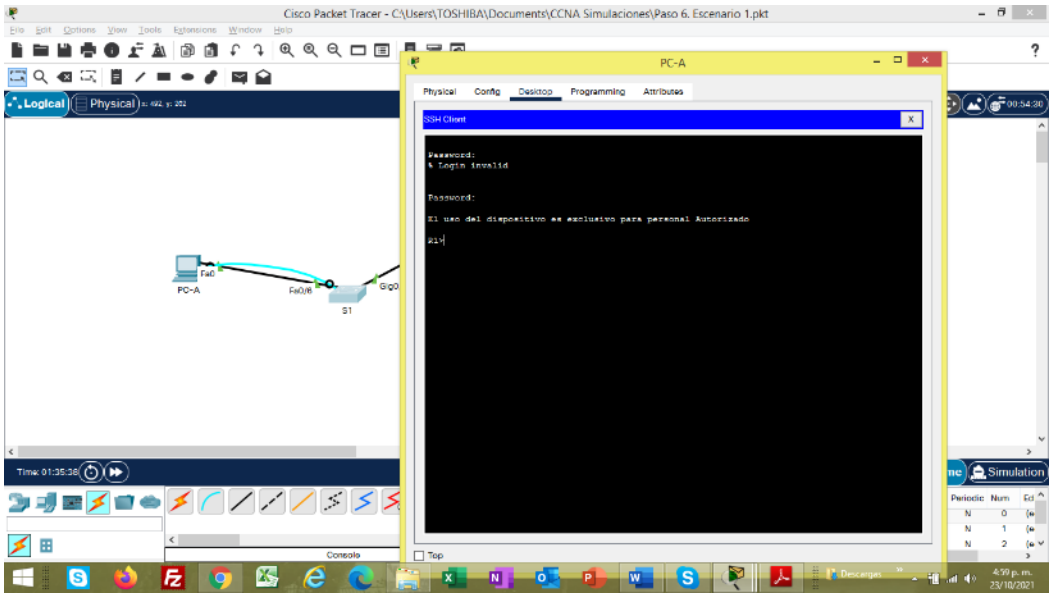
Fuente: Propia. Comando Show Run en S1.

Figura 10. Acceso a Protocolo SSH.



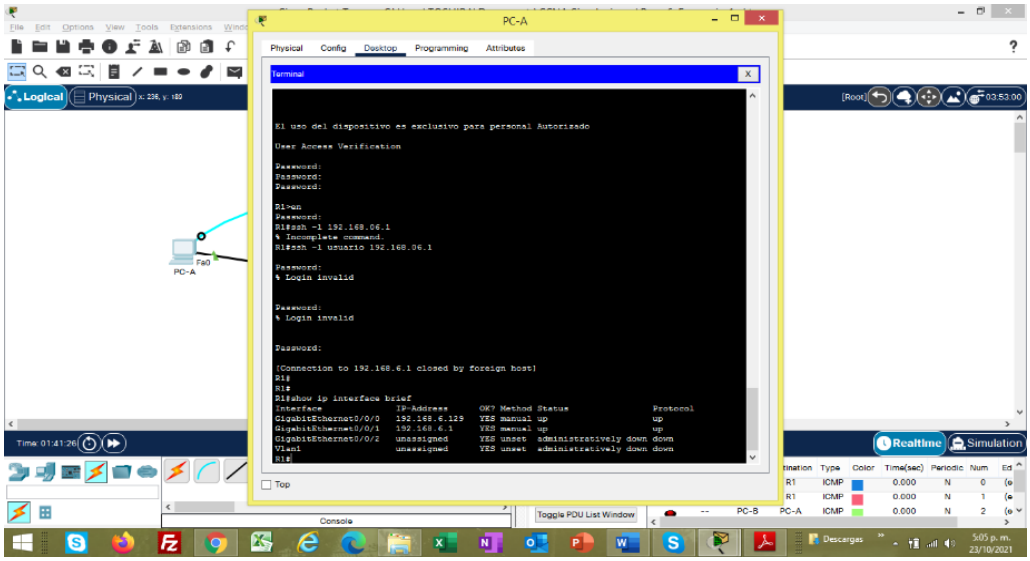
Fuente: Propia. Conexión por SSH desde PC-A.

Figura 11. Conexión a R1 desde SSH en PC-A.



Fuente: Propia. Acceso SSH.

Figura 12. Acceso R1 desde Consola por SSH en PC-A.



Fuente: Propia. Acceso a R1 por Terminal.

Configuración Completa S1.

```
S1#show run
Building configuration...

Current configuration : 1460 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$EJnmB234UvJf9yoQMWYJK/
!
!
!
no ip domain-lookup
ip domain-name ccna-lab.com
!
username admin secret 5 $1$mERr$ILrAmVhMGbrCFnj8QqS3T.
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
```

interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 192.168.6.2 255.255.255.128
shutdown
!
ip default-gateway 192.168.6.1
!
banner motd ^CEl uso del dispositivo es exclusivo para personal Autorizado^C
!
!

!
line con 0
password 7 0822455D0A1606181C1B0D1739
login
!
line vty 0 4
login local
transport input ssh
line vty 5 15
login local
transport input ssh
!
!
!
!
end

1.3.2. Paso 2. Configurar los equipos

Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all**.

Tabla 4. Configuración Host PC-A.

PC-A Network Configuration	
Descripción	LAN 1 PC-A
Dirección Física	0001.9675.7E08
Dirección IP	192.168.06.126
Mascara de Subred	255.255.255.128
Gateway Predeterminado	192.168.06.1

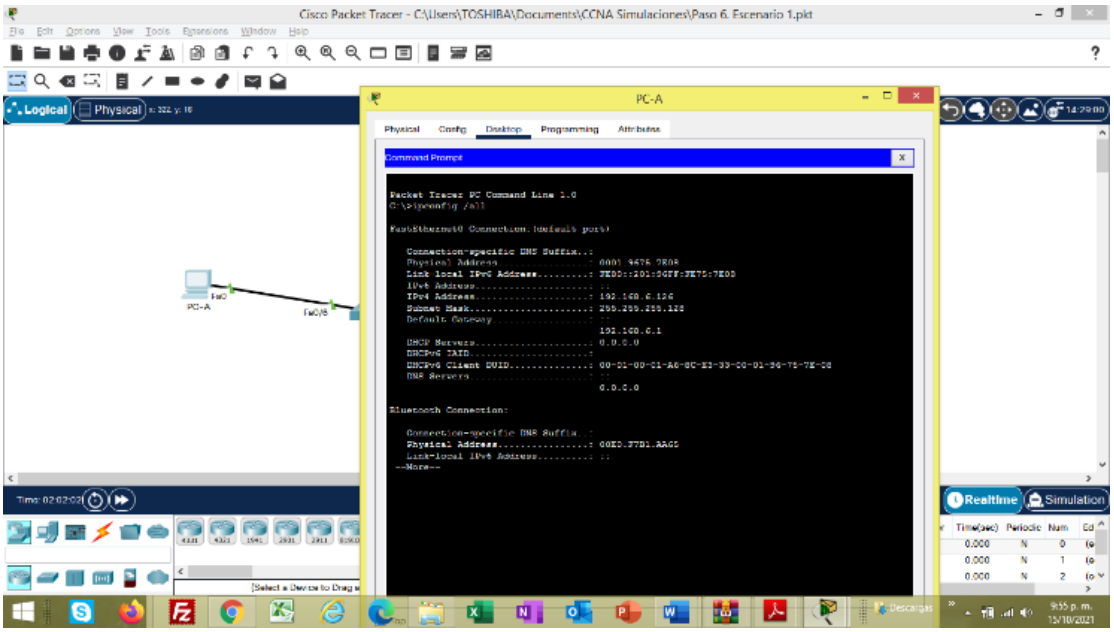
Fuente: Propia. Direccionamiento en Host.

Tabla 5. Configuración Host PC-B.

PC-B Network Configuration	
Descripción	LAN 2 PC-B
Dirección Física	0001.C775.6592
Dirección IP	192.168.06.190
Mascara de Subred	255.255.255.128
Gateway Predeterminado	192.168.06.129

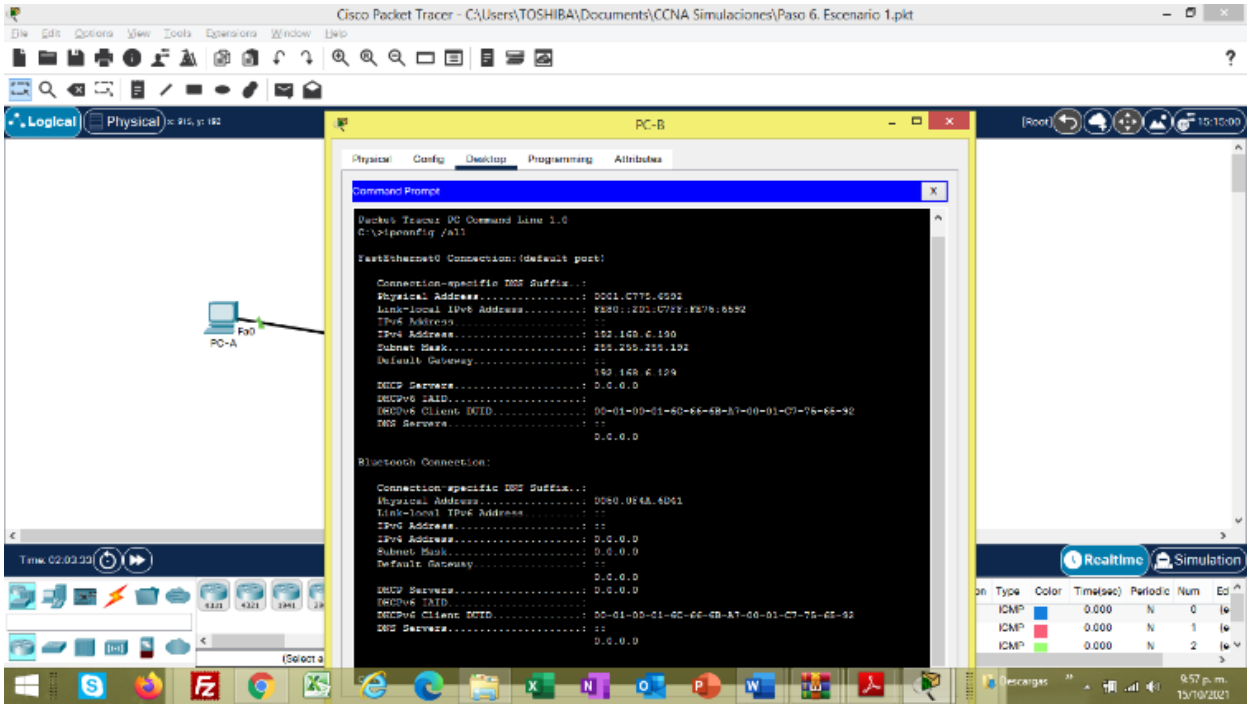
Fuente: Propia. Configuración de PC-B.

Figura 13. Información PC-A.



Fuente: Propia. Información de configuración en PC-A.

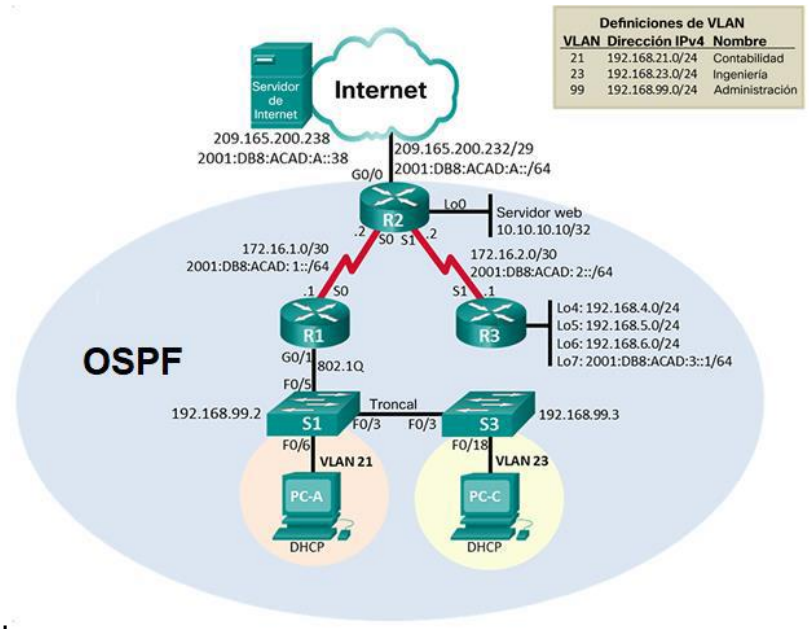
Figura 14. Información PC-B.



Fuente: Propia. Información de configuración PC-B.

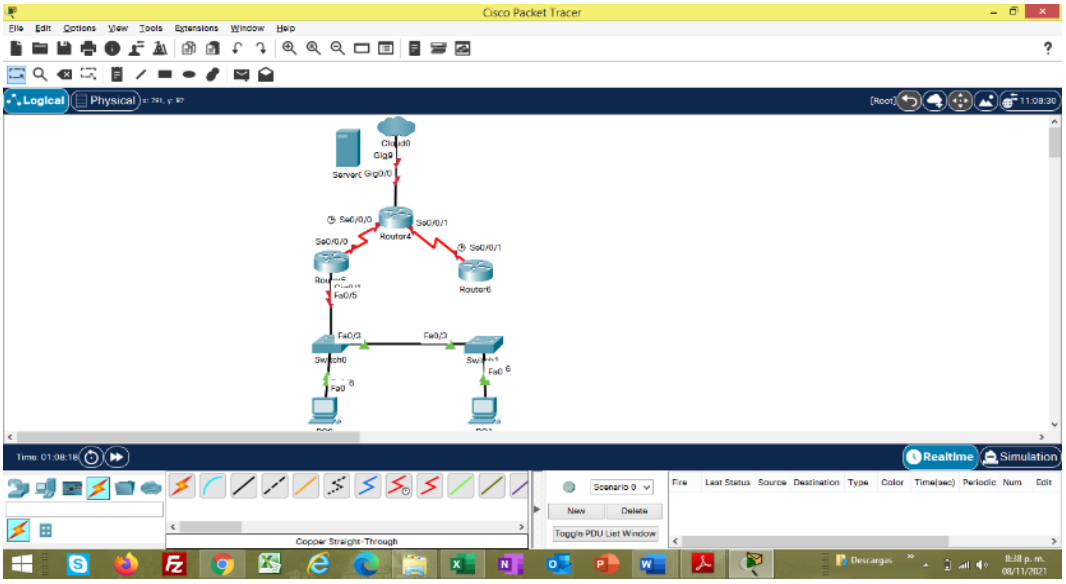
2. ESCENARIO 2.

Figura 15. Topología de la Red Escenario 2.



Fuente: Vesga Juan Carlos. Evaluación – Prueba de habilidades Practicas CCNA.

Figura 16. Simulación Red escenario 2.



Fuente: Propia. Topología Escenario 2.

2.1. Parte 1: Inicializar dispositivos

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

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

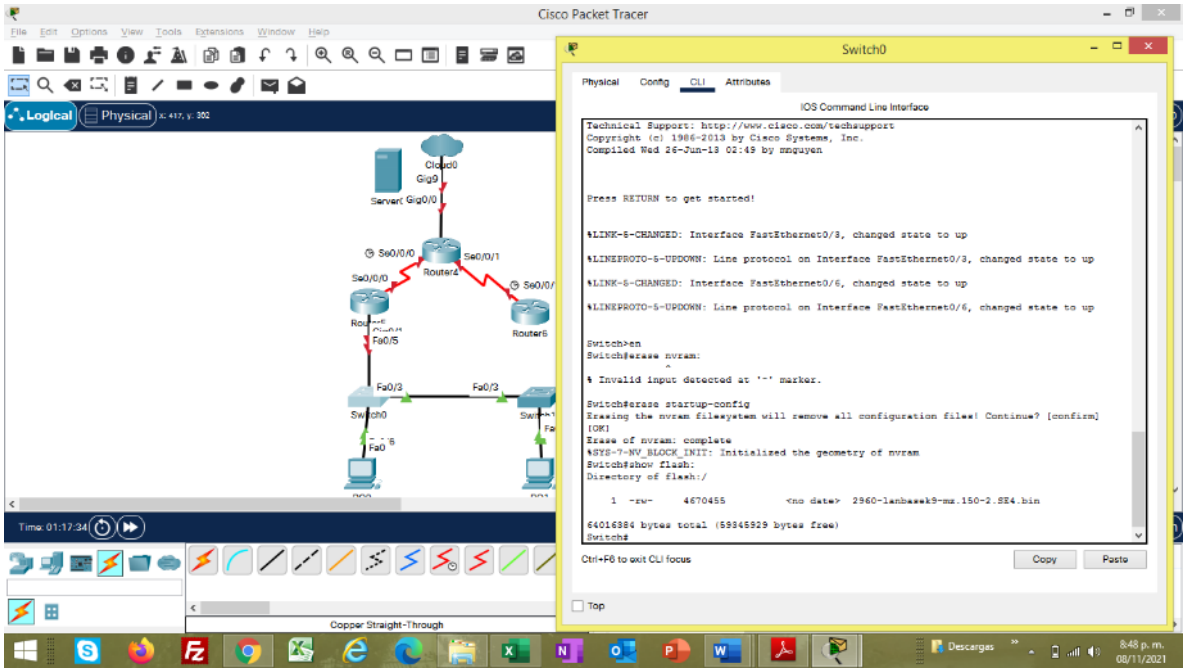
Tabla 6. Inicialización de dispositivos.

Tarea	*Comandos de IOS*
Eliminar el archivo startup-config de todos los routers	*Router>en* *Router#erase startup-config* *Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]y[OK]* *Erase of nvram: complete* *%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram* *Router#*
Volver a cargar todos los routers	*Router#reload* *Proceed with reload? [confirm]*
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior.	*Switch#erase startup-config* *Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]* *[OK]* *Erase of nvram: complete* *%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram* *Switch#* *Verificar si existe el archivo vlan.dat en la flash:* *Switch#show flash:* *Si existe se elimina con el comando:* *Switch#delete vlan.dat* *Y se confirma la ejecución.*
Volver a cargar ambos switches	*Switch#reload* *Proceed with reload? [confirm]*
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches.	*Switch#show flash:*

Fuente: Propia. Inicialización y cargue de Switch.

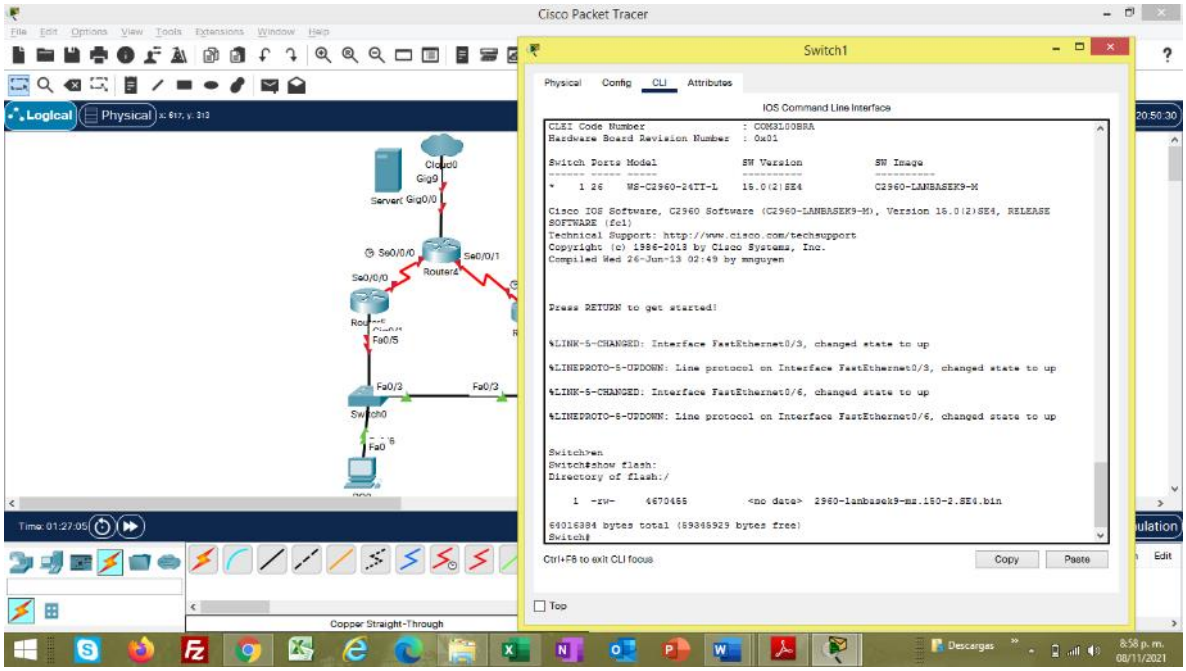
Se inicializan los Router y Switch de la red, aplicando los comandos anteriores, se procede a verificar el archivo vlan.dat en los Switch:

Figura 17. Información Flash Switch0 o S1.



Fuente: Propia. Verificación de archivo Vlan.data.

Figura 18. Información Flash Switch 1 o S2.



Fuente: Propia. Información Vlan.data en S1 y S2.

2.2. Parte 2 Configurar los parámetros básicos de los dispositivos.

2.2.1. Paso 1: Configurar la computadora de Internet.

En la topología creada se procede a ingresar en el servidor de Internet para configurar los datos de acuerdo con el diagrama de la Red.

Teniendo en cuenta los rangos de la red en la topología del escenario se aplica el Gateway predeterminado IPV4 209.165.200.233 y IPV6 2001:DB8:ACAD:A::1

Tabla 7. Configuración Computadora de Internet.

Elemento o tarea de Configuración	Especificación
Dirección IPV4	209.165.200.238
Mascara de subred para IPV4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPV6 / subred	2001:DB8:ACAD:A::38
Gateway predeterminada IPV6	2001:DB8:ACAD:A::1

Fuente: Propia. Configuración de servidor de Internet.

2.2.2. Paso 2. Configurar R1.

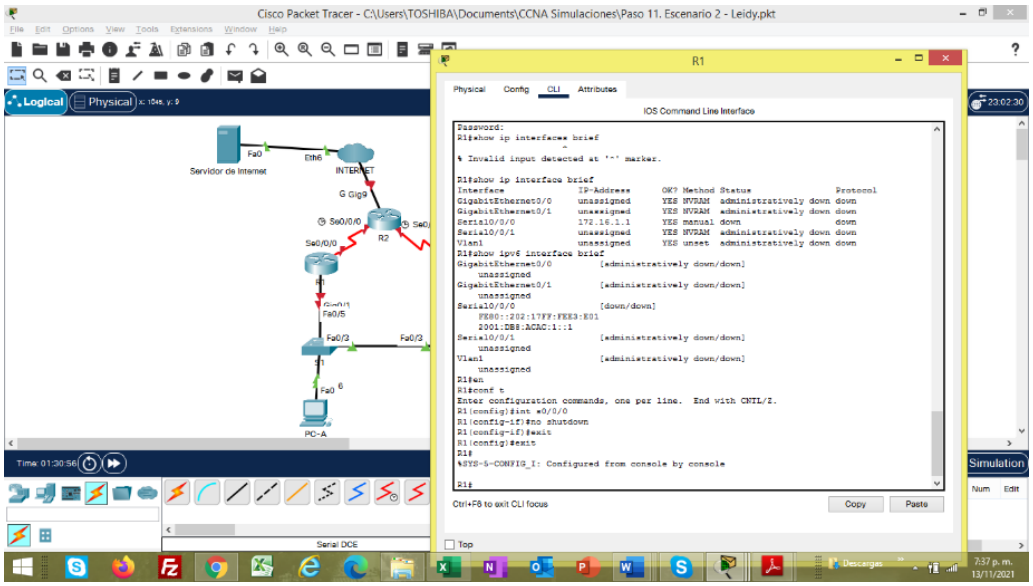
Tabla 8. Configuración básica R1.

Tarea	Especificación	*Comandos*
Desactivar la búsqueda DNS		*Router>enable* *Router#configure terminal* *Router(config)#no ip domain-lookup* *Router(config)#*
Nombre del router	R1	*Router>enable* *Router#configure terminal* *Router(config)#hostname R1* *R1(config)#*
Contraseña de exec privilegiado	class	*R1>enable* *R1#configure terminal* *R1(config)#enable secret class* *R1(config)#*
Contraseña de acceso a la consola	cisco	*R1>enable* *R1#configure terminal* *R1(config)#line console 0* *R1(config-line)#password cisco* *R1(config-line)#login* *R1(config-line)#exit* *R1(config)#*
Contraseña de acceso Telnet	cisco	*R1>enable* *R1#configure terminal* *R1(config-line)#line vt 0 4* *R1(config-line)#password cisco* *R1(config-line)#login*

		R1(config-line)#exit *R1(config)#*
Cifrar las contraseñas de texto no cifrado		*R1>* *R1>enable* *R1#configure terminal* *R1(config)# service password-encryption* *R1(config)#*
Mensaje MOTD	Se prohíbe el acceso no autorizado	*R1>* *R1>enable* *R1#configure terminal* *R1(config)#banner motd #Se 40rohíbe el acceso no autorizado#* *R1(config)#*
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)#int s0/0/0* *R1(config-if)#description Conectado a R2* *R1(config-if)#ip address 172.16.1.1 255.255.255.252* *R1(config-if)#ipv6 address 2001:DB8:ACAC:1::1/64* *R1(config-if)#clock rate 128000* *R1(config-if)#no shut* *R1(config-if)#ipv6 unicast-routing* *R1(config)#*
Rutas predeterminadas		*R1>* *R1>enable* *R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2* *R1(config)#ipv6 route ::/0 s0/0/0* *R1(config)#*

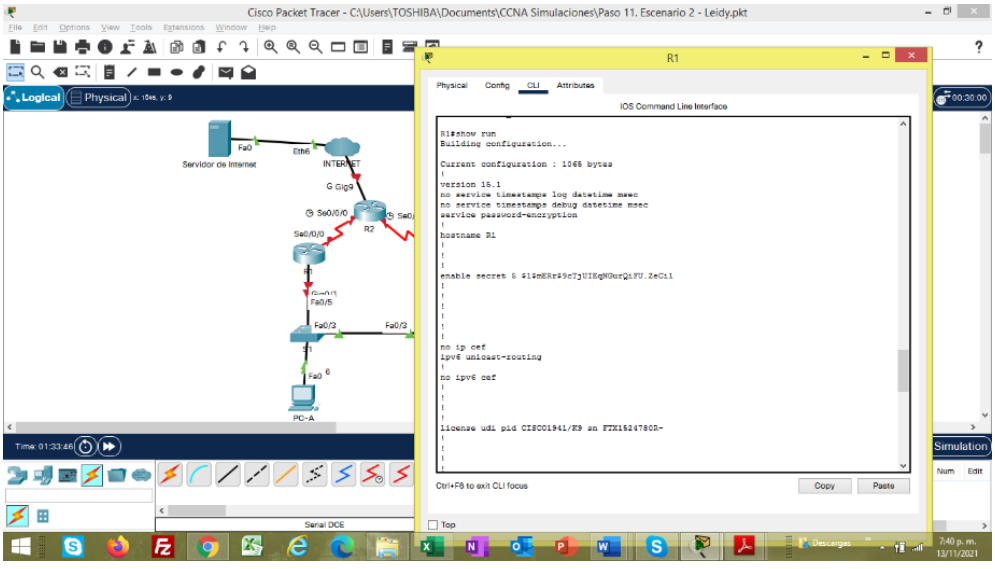
Fuente: Propia.

Figura 19. Verificación de las interfaces configuradas en R1.



Fuente: Propia. Comando Show ip interface brief.

Figura 20. Verificación de la configuración en ejecución.



Fuente: Propia. Comando Show Run en R1.

2.2.3. Paso 3 Configurar R2.

Tabla 9. Configuración básica R2.

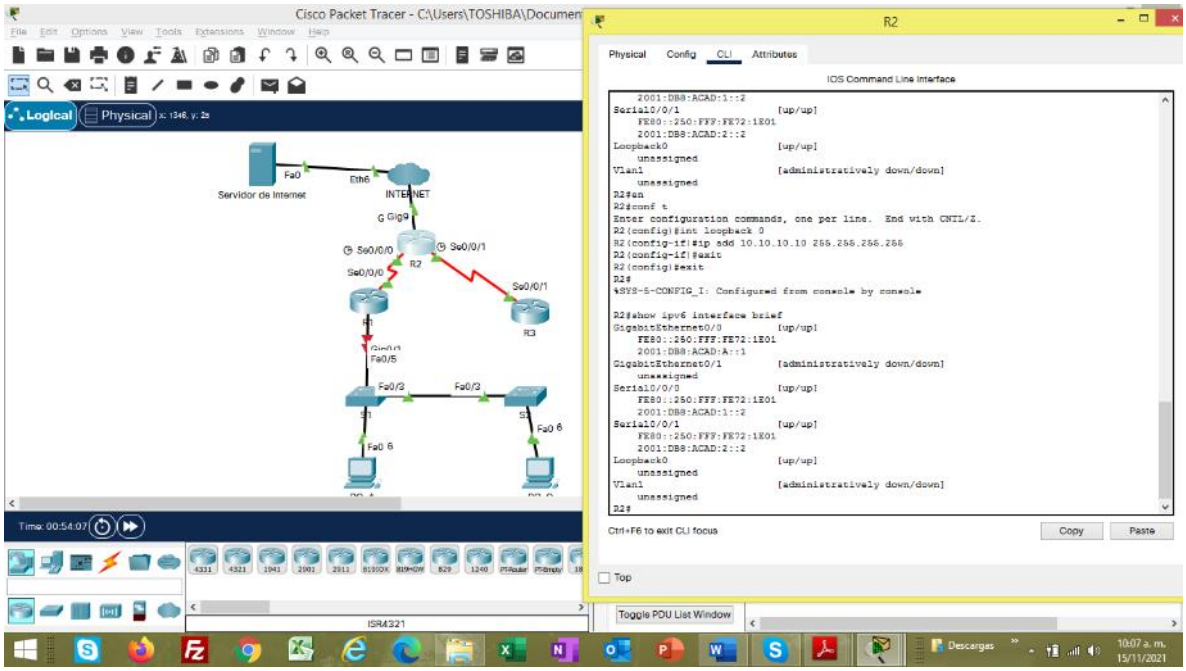
Tarea	Especificación	*Comandos*
Desactivar la búsqueda DNS		*Router>enable* *Router#configure terminal* *Router(config)#no ip domain-lookup* *Router(config)#*
Nombre del router	R2	*Router>enable* *Router#configure terminal* *Router(config)#hostname R2* *R2(config)#*
Contraseña de exec privilegiado	class	*R2>enable* *R2#configure terminal* *R2(config)#enable secret class* *R2(config)#*
Contraseña de acceso a la consola	cisco	*R2>enable* *R2#configure terminal* *R2(config)#line console 0* *R2(config-line)#password cisco* *R2(config-line)#login* *R2(config-line)#exit* *R2(config)#*
Contraseña de acceso Telnet	cisco	*R2>enable* *R2#configure terminal* *R2(config-line)#line vt 0 4* *R2(config-line)#password cisco* *R2(config-line)#login* *R2(config-line)#exit* *R2(config)#*
Cifrar las contraseñas de texto no cifrado		*R2>* *R2>enable* *R2#configure terminal* *R2(config)# service password-encryption* *R2(config)#*
Habilitar el servidor HTTP		*R2(config)#ip http secure-server*
Mensaje MOTD	Se prohíbe el acceso no autorizado	*R2>* *R2>enable*

		R2#configure terminal *R2(config)#banner motd #Se prohibe el acceso no autorizado#* *R2(config)#*
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	*R2(config)#ipv6 unicast-routing* *R2(config)#int s0/0/0* *R2(config-if)#description Conectado a R1* *R2(config-if)#ip add 172.16.1.2 255.255.255.252* *R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64* *R2(config-if)#no shutdown* *R2(config-if)#CLOCK RATE 128000* *R2(config-if=#ipv6 unicast-routing*
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)#int s0/0/1* *R2(config-if)#description Conectado 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* *R2*
Interfaz G0/0	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz	*R2(config-if)#int g0/0* *R2(config-if)#description Conectado a Servidor de Internet* *R2(config-if)#ip address 209.165.200.232 255.255.255.0* *R2(config)#int g0/0* *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)#int loopback 0* *R2(config-if)#ip add 10.10.10.10 255.255.255.255*

		R2(config-if)#description Servidor web *R2(config-if)#exit*
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*

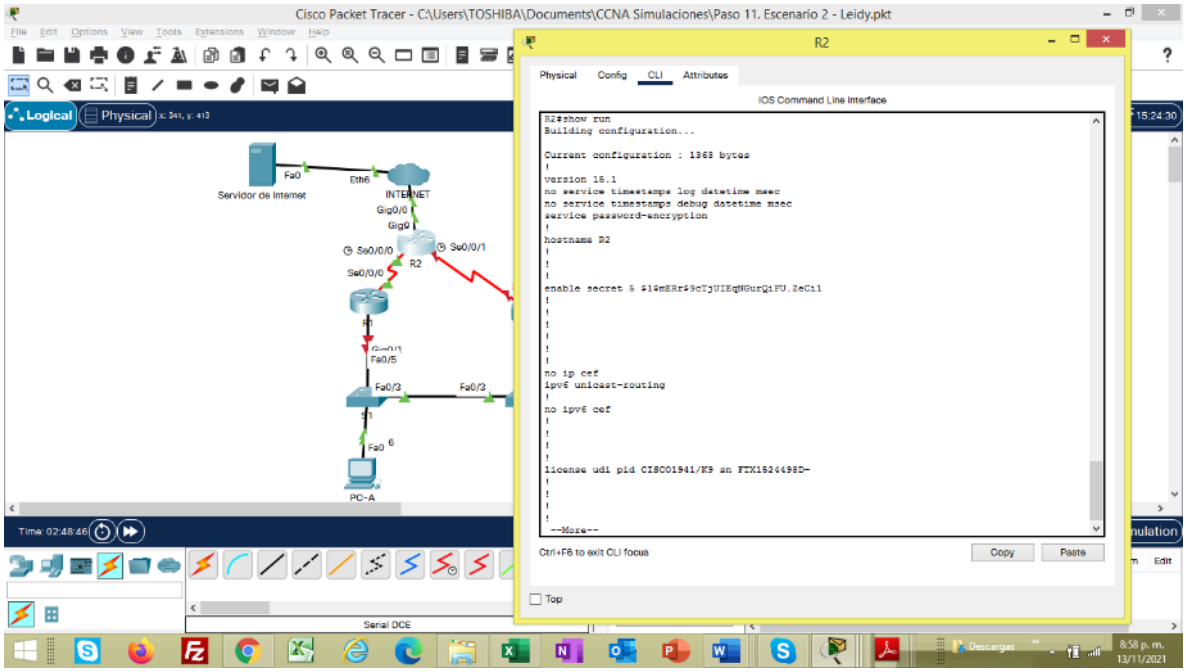
Fuente: Propia.

Figura 21. Verificación de interfaces en R2.



Fuente: Propia. Comando Show ip interface brief.

Figura 22. Verificación de configuración en Ejecución R2.



Fuente: Propia. Comando Show run en R2.

2.2.4. Paso 4. Configurar R3.

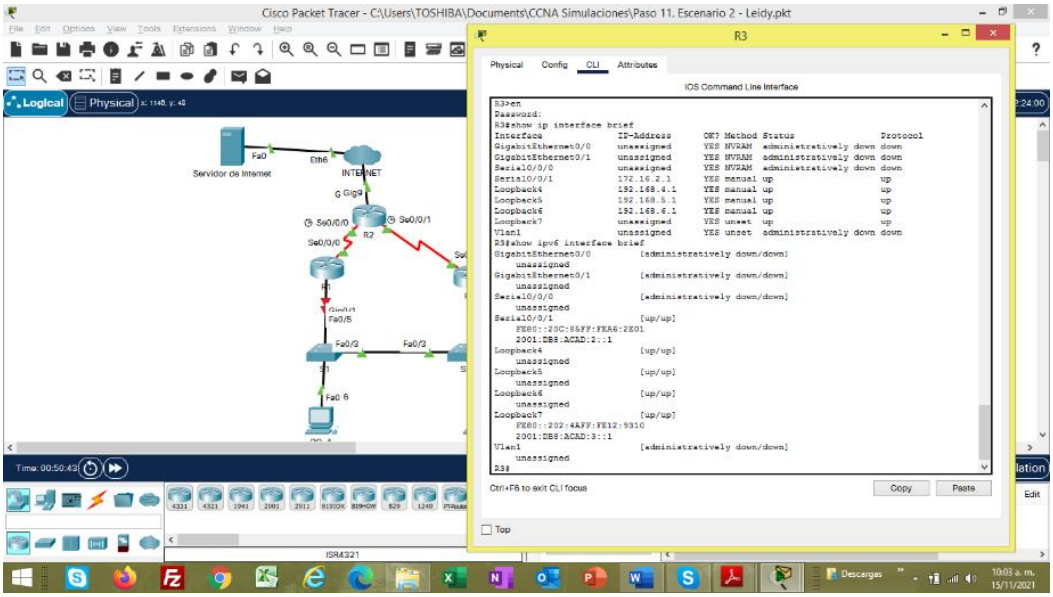
Tabla 10. Configuración Básica en R3.

Tarea	Especificación	*Comandos*
Desactivar la búsqueda DNS		*Router>enable* *Router#configure terminal* *Router(config)#no ip domain-lookup* *Router(config)#*
Nombre del router	R3	*Router>enable* *Router#configure terminal* *Router(config)#hostname R3* *R3(config)#*
Contraseña de exec privilegiado	class	*R3>enable* *R3#configure terminal* *R3config)#enable secret class* *R3(config)#*
Contraseña de acceso a la consola	cisco	*R3>enable* *R3#configure terminal* *R3(config)#line console 0* *R3(config-line)#password cisco* *R3(config-line)#login* *R3(config-line)#exit* *R3(config)#*
Contraseña de acceso Telnet	cisco	*R3>enable* *R3#configure terminal* *R3(config-line)#line vt 0 4* *R3(config-line)#password cisco* *R3(config-line)#login* *R3(config-line)#exit* *R3(config)#*
Cifrar las contraseñas de texto no cifrado		*R3>* *R3>enable* *R3#configure terminal* *R3(config)# service password-encryption* *R3(config)#*
Mensaje MOTD	Se prohíbe el acceso no autorizado	*R3>* *R3>enable* *R3#configure terminal* *R3(config)#banner motd #Se prohibe el acceso no autorizado#* *R3(config)#*

Interfaz S0/0/0	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	*R3(config)#int s0/0/1* *R3(config-if)#description Conectado a R2* *R3(config-if)#ip add 172.16.2.1 255.255.255.252* *R3(config-if)#ipv6 unicast-routing* *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)#int loopback4* *R3(config-if)#ip address 192.168.4.1 255.255.255.0*
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	*R3(config-if)#int loopback 5* *R3(config-if)#ip add 192.168.5.1 255.255.255.0*
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	*R3(config-if)#int loopback 6* *R3(config-if)#ipv6 unicast-routing* *R3(config-if)#ip add 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)#ipv6 unicast-routing* *R3(config)#int loopback 7* *R3(config-if)#ipv6 add 2001:DB8:ACAD:3::1/64* *R3(config-if)#exit*
Rutas predeterminadas		*R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1* *R3(config)#ipv6 route ::/0 s0/0/1* *R3(config)#exit*

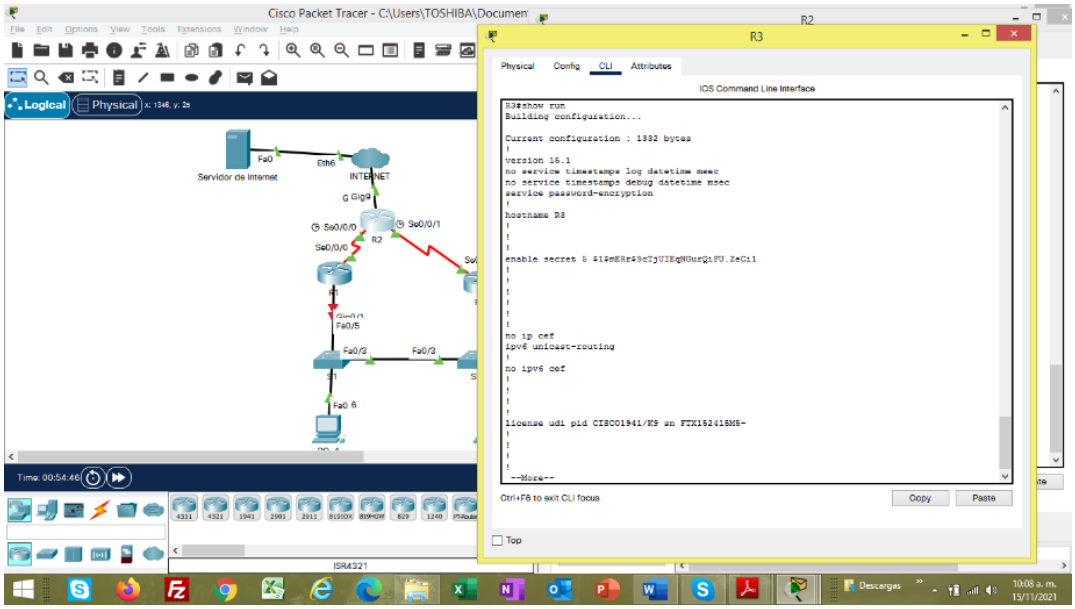
Fuente: Propia.

Figura 23. Verificación interfaces en R3.



Fuente: Propia. Comando Show ip interface brief.

Figura 24. Verificación de configuración en ejecución en R3.



Fuente: Propia. Comando Show run en R3.

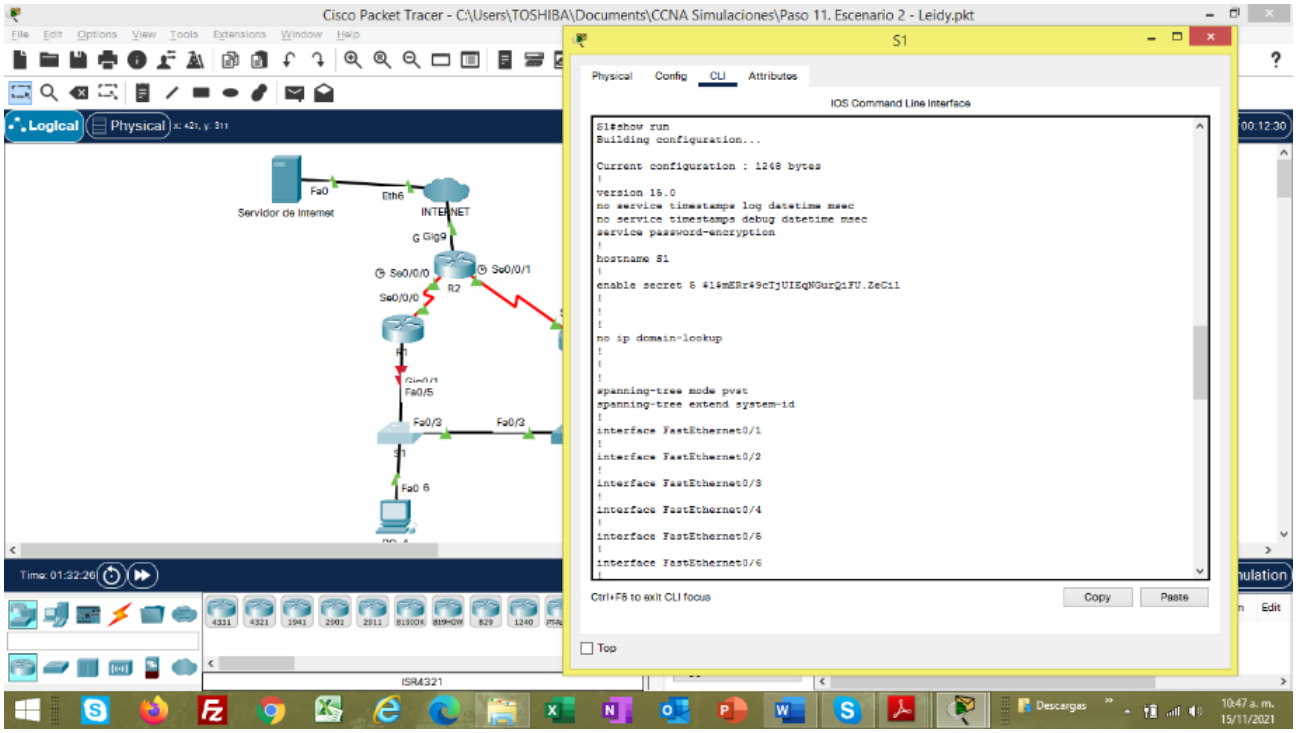
2.2.5. Paso 5 Configurar S1.

Tabla 11. Configuración básica en S1.

Tarea	Especificación	*Comandos*
Desactivar la búsqueda DNS		*Switch>en* *Switch#conf t* *Switch(config)#no ip domain-lookup*
Nombre del Switch	R3	*Switch(config)#hostname S1* *S1(config)#*
Contraseña de exec privilegiado	class	*S1(config)#enable secret class*
Contraseña de acceso a la consola	cisco	*S1(config)#line console 0* *S1(config-line)#password cisco* *S1(config-line)#login*
Contraseña de acceso Telnet	cisco	*S1(config-line)#line vty 0 4* *S1(config-line)#password cisco* *S1(config-line)#login* *S1(config-line)#exit*
Cifrar las contraseñas de texto no cifrado		*S1(config)#service password-encryption*
Mensaje MOTD	Se prohíbe el acceso no autorizado	*S1(config)#banner motd #Se prohibe el acceso no autorizado#* *S1(config)#*

Fuente: Propia.

Figura 25. Verificación de configuración en ejecución en S1.



Fuente: Propia. Comando Show Run en S1.

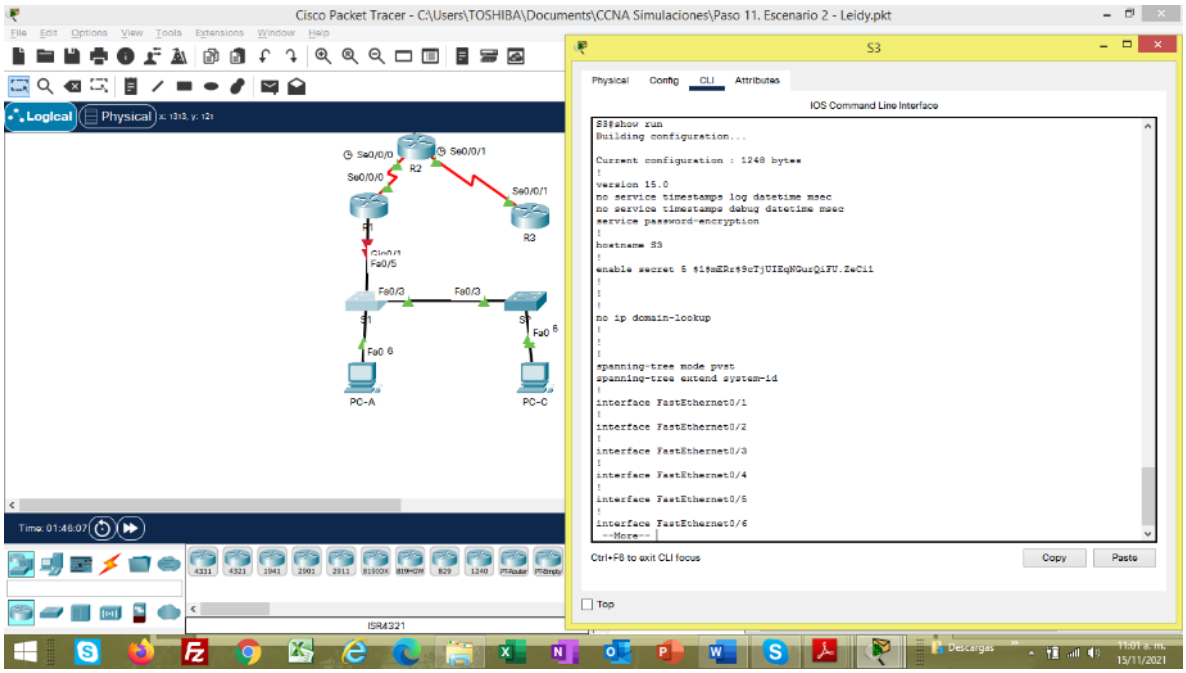
2.2.6. Paso 6 Configurar S3.

Tabla 12. Configuración básica en S3.

Tarea	Especificación	*Comandos*
Desactivar la búsqueda DNS		*Switch>en* *Switch#conf t* *Switch(config)#no ip domain-lookup*
Nombre del Switch	R3	*Switch(config)#hostname S3* *S3(config)#*
Contraseña de exec privilegiado	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)#line vty 0 4* *S3(config-line)#password cisco* *S3(config-line)#login* *S3(config-line)#exit*
Cifrar las contraseñas de texto no cifrado		*S3(config)#service password-encryption*
Mensaje MOTD	Se prohíbe el acceso no autorizado	*S3(config)#banner motd #Se prohibe el acceso no autorizado#* *S3(config)#*

Fuente: Propia.

Figura 26. Verificación configuración en ejecución de S3.



Fuente: Propia. Comando Show Run en S3.

2.2.7. Paso 7. Verificar la conectividad de la Red.

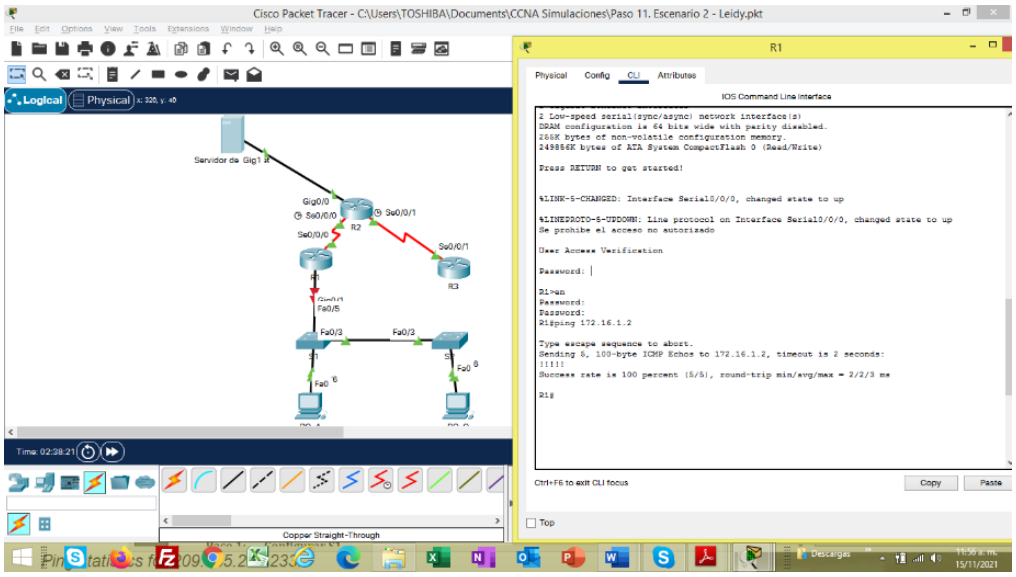
Se utiliza el comando Ping para comprobar la conexión entre los equipos Router de la Red.

Tabla 13. Resultados de conectividad.

Desde	A	DIRECCION IP	RESULTADOS
R1	R2, S0/0/0	172.16.1.2	OK
R2	R3, S0/0/1	172.16.2.1	OK
PC de internet	Gateway predeterminado	209.165.200.233	OK

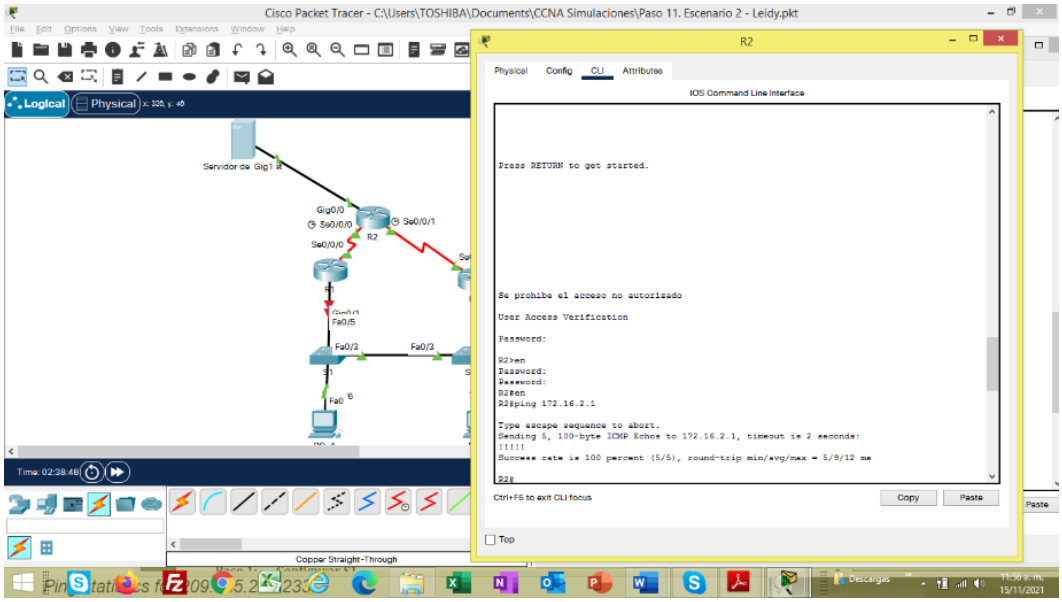
Fuente: Propia. Resultados de conexión entre las LAN de la red.

Figura 27. Ping R1 a R2.



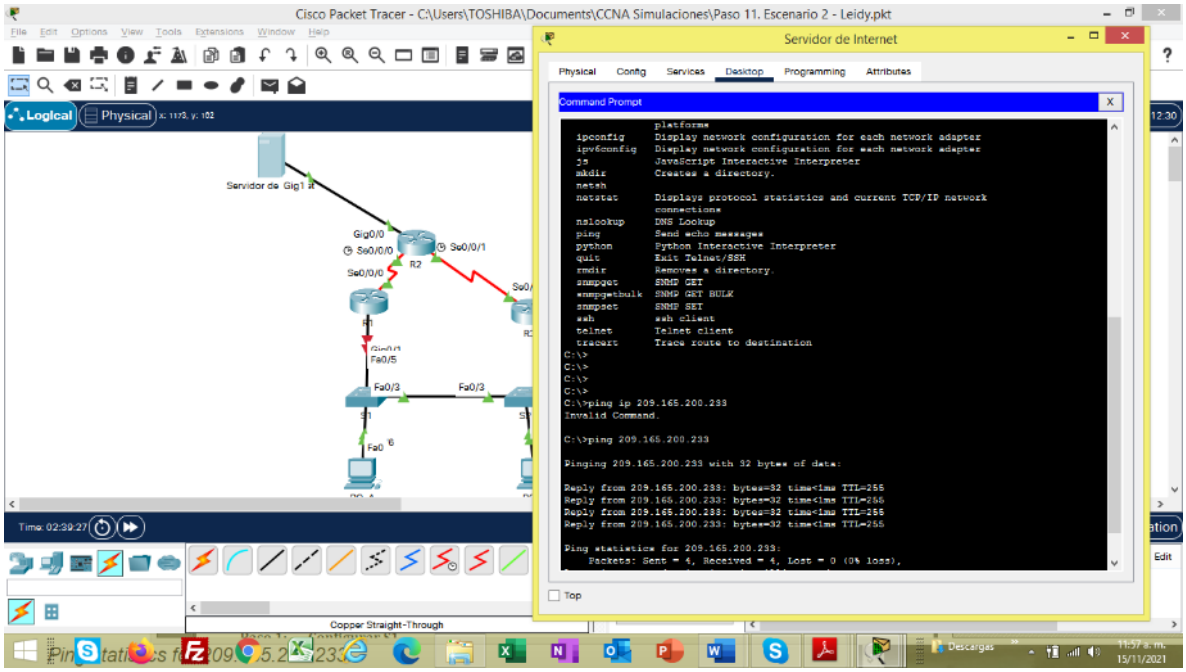
Fuente: Propia. Verificación conectividad R1 y R2.

Figura 28. Ping R2 a R3.



Fuente: Propia. Verificación conectividad entre R2 y R3.

Figura 29. Ping Computadora de Internet a Gateway.



Fuente: Propia. Verificación conectividad entre servidor y R2.

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

2.3.1. Paso 1. Configurar S1.

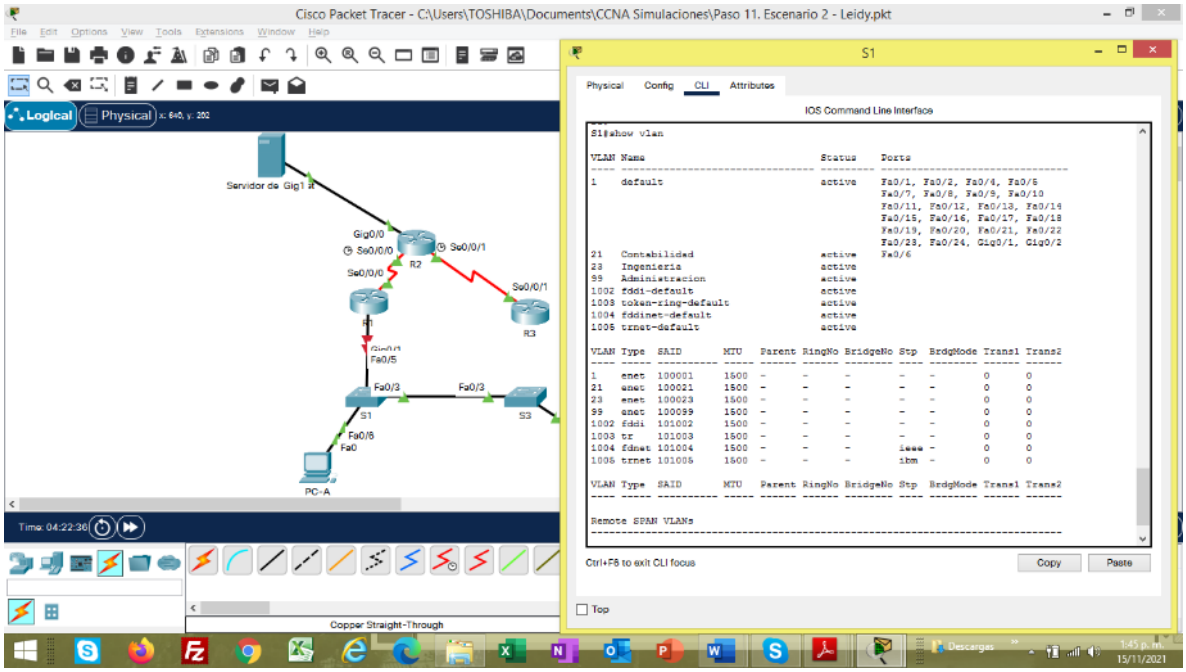
Tabla 14. Configuración S1.

Elemento o tarea de configuración.	Especificación	*Comandos*
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican	*S1(config)#vlan 21* *S1(config-vlan)#name Contabilidad* *S1(config-vlan)#vlan 23* *S1(config-vlan)# name Ingenieria* *S1(config-vlan)#vlan 99* *S1(config-vlan)#name Administracion* *S1(config-vlan)#*
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología	*S1(config)#int vlan 99* *S1(config-if)#ip add 192.168.99.2 255.255.255.0* *S1(config-if)#no shut* *S1(config-if)#*
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.	*S1(config)#ip default-gateway 192.168.99.1*
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa	*S1(config)#int f0/3* *S1(config-if)#switchport mode trunk* *S1(config-if)#switchport trunk native vlan 1* *S1(config-if)#*
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa	*S1(config)#int f0/5* *S1(config-if)#switchport mode trunk* *S1(config-if)#switchport trunk native vlan 1* *S1(config-if)#*
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range	*S1(config)#int range f0/1-2, f0/4, f0/6-24, g0/1-2* *S1(config-if-range)#switchport mode access* *S1(config-if-range)#*
Asignar F0/6 a la VLAN 21		*S1(config)#int f0/6*

		S1(config-if)#switchport access vlan 21 *S1(config-if)#*
Apagar todos los puertos sin usar		*S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2* *S1(config-if-range)#no shutdown* *S1(config-if-range)#*

Fuente: Propia.

Figura 30. Verificación configuración de VLAN en S1.



Fuente: Propia. Comando Show Vlan para verificar configuración.

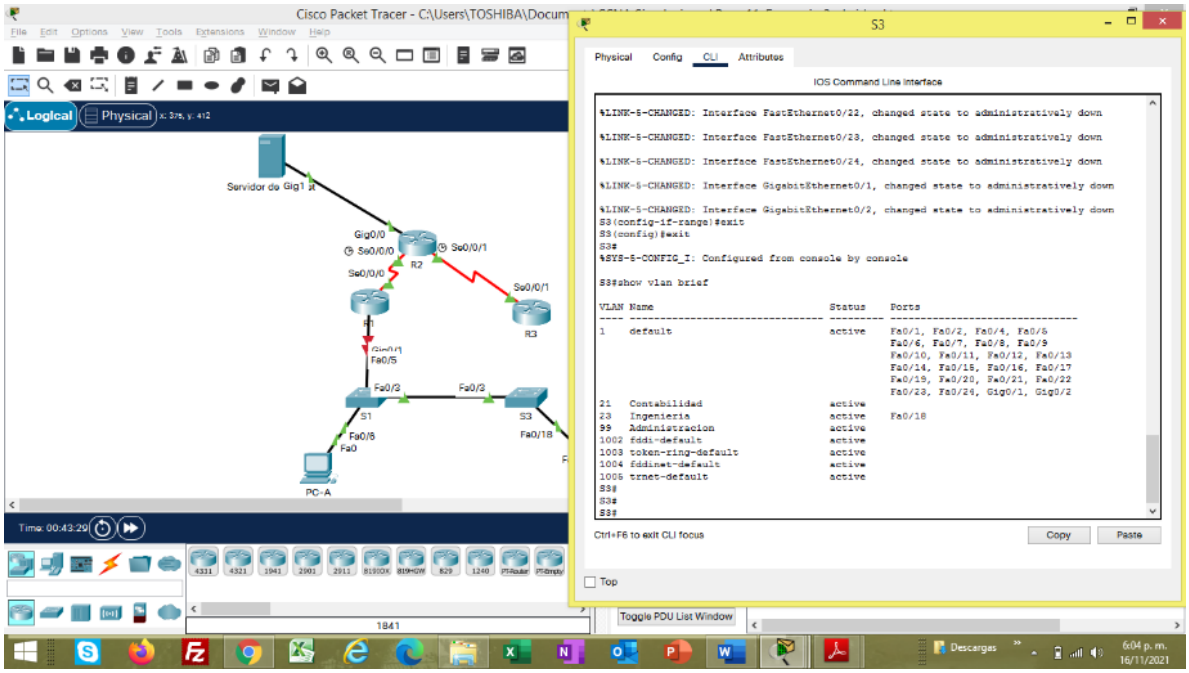
2.3.2. Paso 2. Configurar S3.

Tabla 15. Configuración en S3.

Elemento o tarea de configuración.	Especificación	*Comandos*
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	*S3 (config)#vlan 21* *S3(config-vlan)#name Contabilidad* *S3(config-vlan)#vlan 23* *S3(config-vlan)# name Ingenieria* *S3(config-vlan)#vlan 99* *S3(config-vlan)#name Administracion* *S3(config-vlan)#*
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	*S3(config)#int vlan 99* *S3(config-if)#ip add 192.168.99.3 255.255.255.0* *S3(config-if)#no shut* *S3(config-if)#*
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.	*S3(config)#ip default-gateway 192.168.99.1*
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa	*S3(config)#int f0/3* *S3(config-if)#switchport mode trunk* *S3(config-if)#switchport trunk native vlan 1* *S3(config-if)#*
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range	*S3(config)#int range f0/1-2,f0/4-24,g0/1-2* *S3(config-if-range)#sw mode Access* *S3(config-if-range)#*
Asignar F0/18 a la VLAN 21		*S3(config-if-range)#int f0/18* *S3(config-if)#switchport access vlan 23* *S3(config)#*
Apagar todos los puertos sin usar		*S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2* *S3(config-if-range)#shutdown*

Fuente: Propia.

Figura 31. Verificación configuración VLAN en S3.



Fuente: Propia. Verificación de Vlan en S3.

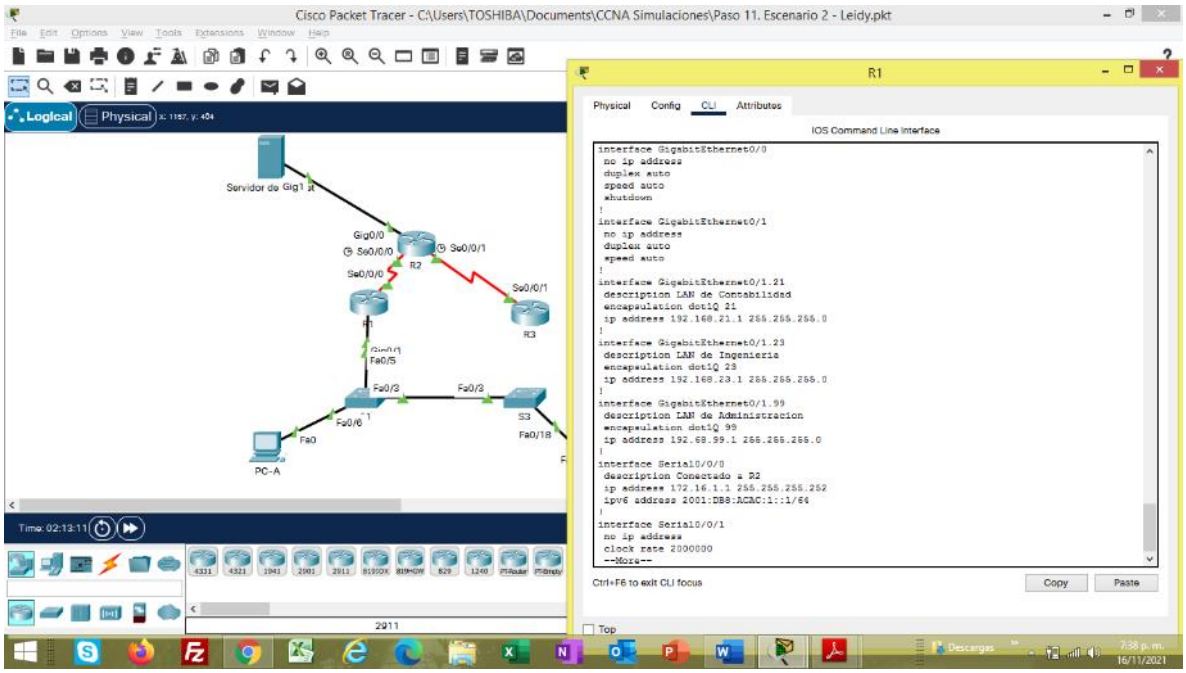
2.3.3. Paso 3. Configurar R1.

Tabla 16. Configuración de R1.

Tarea	Especificación	*Comandos*
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz	*R1(config)#int g0/1.21* *R1(config-subif)#* *R1(config-subif)#description LAN de Contabilidad* *R1(config-subif)#encapsulation dot1q 21* *R1(config-subif)#ip address 192.168.21.1 255.255.255.0* *R1(config-subif)#exit*
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)#int g0/1.23* *R1(config-subif)#* *R1(config-subif)#description LAN de Ingenieria* *R1(config-subif)#encapsulation dot1q 23* *R1(config-subif)#ip add 192.168.23.1 255.255.255.0* *R1(config-subif)#exit*
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)#int g0/1.99* *R1(config-subif)#* *R1(config-subif)#description LAN de Administracion* *R1(config-subif)#encapsulation dot1q 99* *R1(config-subif)#ip add 192.168.99.1 255.255.255.0* *R1(config-subif)#exit*
Activar la interfaz G0/1		*R1(config)#int g0/1* *R1(config-if)#no shutdown*

Fuente: Propia. Configurar subinterfaces en R1.

Figura 32. Verificación de configuración en ejecución de R1.



Fuente: Propia. Comando show Run.

2.3.4. Paso 4. Verificar la conectividad de la red.

Tabla 17. Verificación de Conectividad.

Desde	A	DIRECCION IP	RESULTADOS
S1	R1, dirección VLAN 99	192.168.99.1	Ok
S3	R1, dirección VLAN 99	192.168.99.1	Ok
S1	R1, dirección VLAN 21	192.168.21.1	Ok
S3	R1, dirección VLAN 23	192.168.23.1	Ok

Fuente: Propia. Validación de conexión entre dispositivos de la red.

S1#ping 192.168.99.1

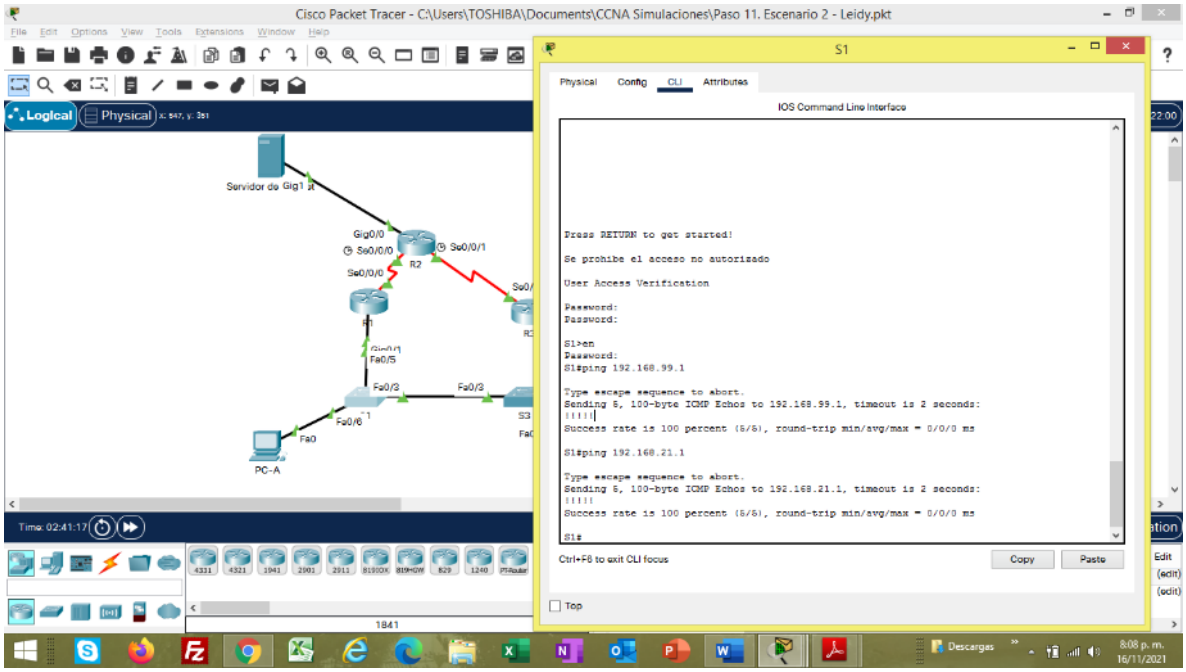
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

S1#ping 192.168.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

S1#

Figura 33. Ping S1 a R1.



Fuente: Propia. Verificación de Conexión entre S1 y R1.

S3#ping 192.168.99.1

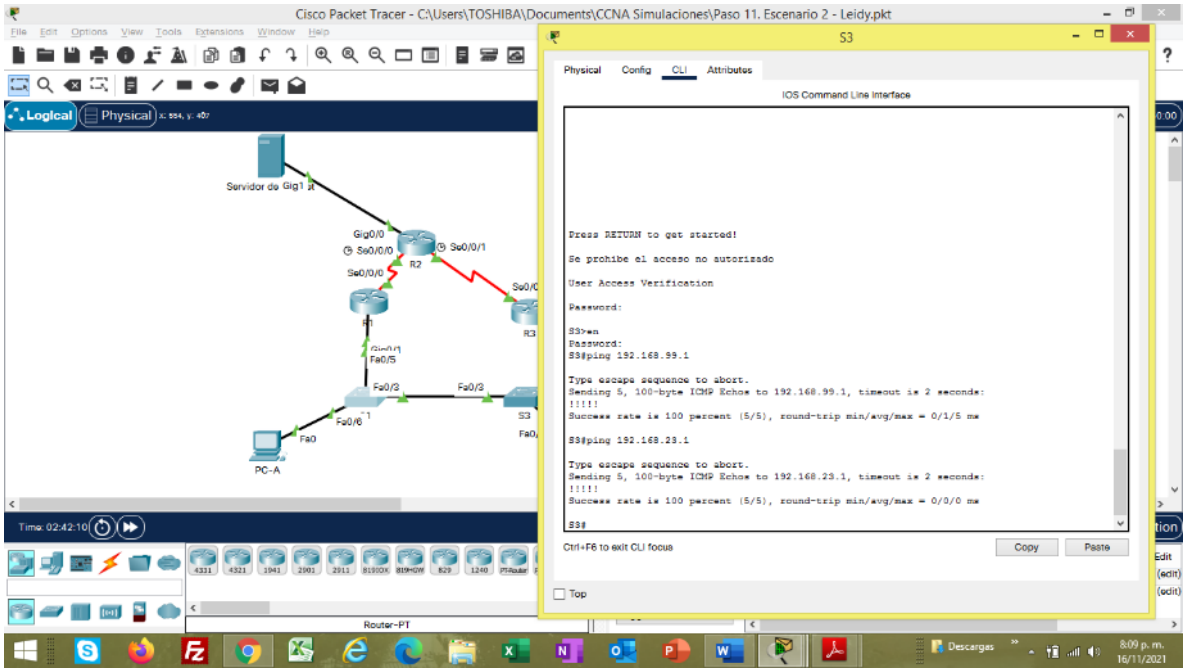
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/5 ms

S3#ping 192.168.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

S3#

Figura 34. Ping S3 a R1.



Fuente: Propia. Validación de conexión entre S3 y R1.

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

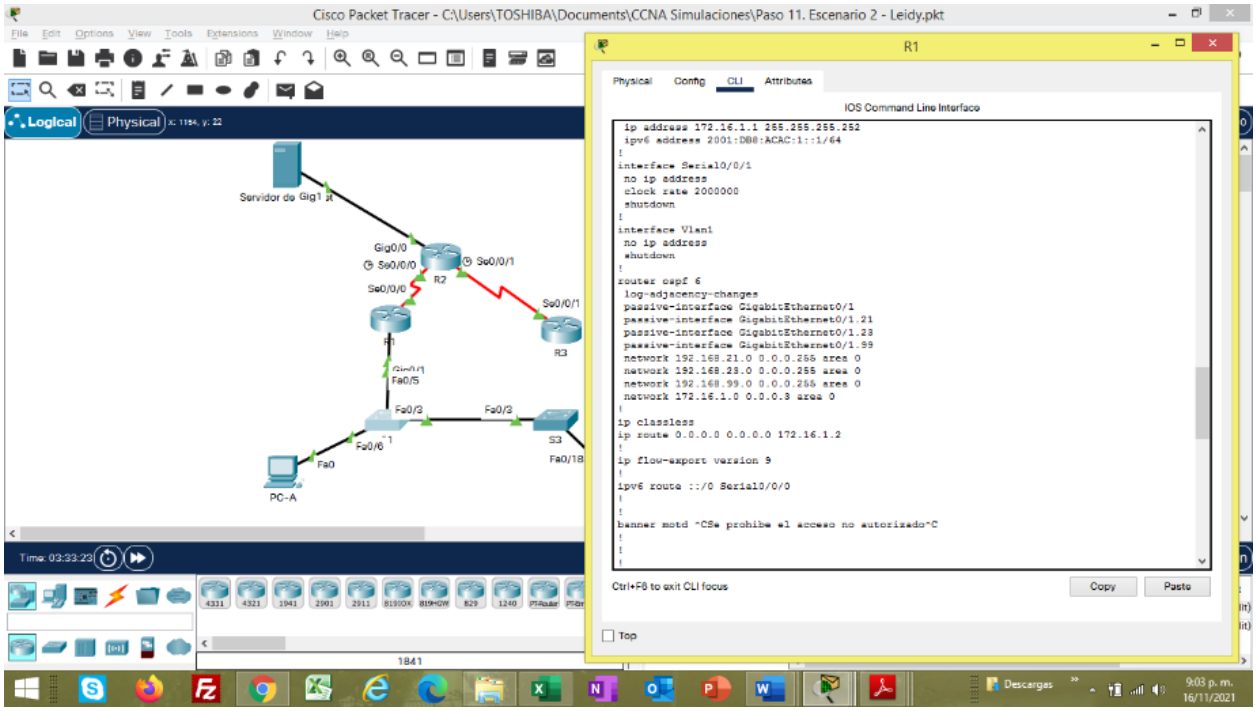
2.4.1. Paso 1: Configurar OSPF en el R1.

Tabla 18. Configuración de OSPF en R1.

Elemento o tarea de configuración	Especificación	*Comandos*
Configurar OSPF área 0		*R1(config)#router ospf 06*
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.	*R1(config-router)#network 192.168.21.0 0.0.0.255 area 0* *R1(config-router)#network 192.168.23.0 0.0.0.255 area 0* *R1(config-router)#network 192.168.99.0 0.0.0.255 area 0* *R1(config-router)#network 172.16.1.0 0.0.0.3 area 0* *R1(config-router)#*
Establecer todas las interfaces LAN como pasivas		*R1(config-router)#passive-interface g0/1* *R1(config-router)#passive-interface g0/1.21* *R1(config-router)#passive-interface g0/1.23* *R1(config-router)#passive-interface g0/1.99* *R1(config-router)#*
Desactive la sumariación automática		*OSPF no realiza la sumarización de rutas de manera predeterminada.*

Fuente: Propia. Configuración Protocolo OSPF.

Figura 35. Verificación configuración en ejecución R1.



Fuente: Propia. Comando Show Run en R1.

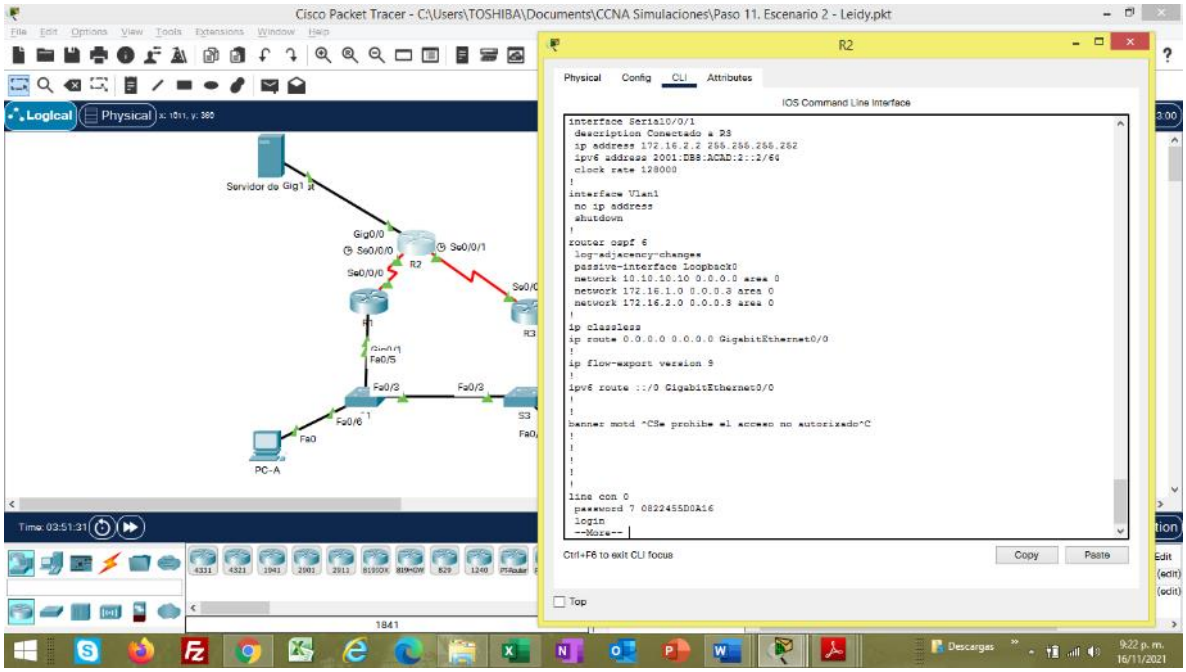
2.4.2. Paso 2: Configurar OSPF en el R2.

Tabla 19. Configuración Protocolo OSPF en R2.

Elemento o tarea de configuración	Especificación	*Comandos*
Configurar OSPF área 0		*R2(config)#router ospf 6*
Anunciar las redes conectadas directamente		*R2(config-router)#net 10.10.10.10 0.0.0.0 area 0* *R2(config-router)#net 172.16.1.0 0.0.0.3 area 0* *R2(config-router)#net 172.16.2.0 0.0.0.3 area 0*
Establecer la interfaz LAN (loopback) como pasiva		*R2(config-router)#passive-interface loopback 0* *R2(config-router)#*
Desactive la sumarización automatica		*OSPF no realiza la sumarización de rutas de manera predeterminada.*

Fuente: Propia. Protocolo OSPF.

Figura 36. Verificación de configuración en Ejecución R2.



Fuente: Propia. Comando Show Run.

2.4.3. Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

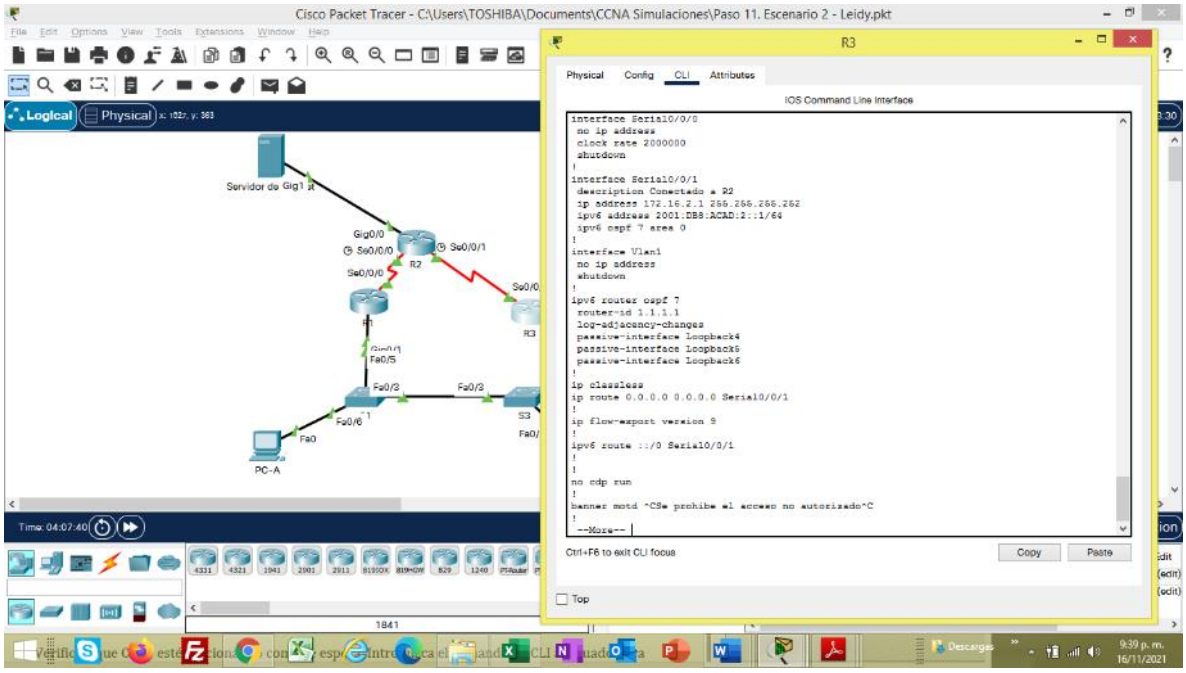
Teniendo en cuenta que el equipo R2 ya se configuro y que el mismo no posee interfaces IPV6 se procede a configurar el Router R3.

Tabla 20. Configuración Protocolo OSPFv3 en R3.

Elemento o tarea de configuración	Especificación	*Comandos*
Configurar OSPF área 0		*R3(config)#ipv6 router ospf 7* *R3(config-rtr)#router-id 1.1.1.1* *R3(config-rtr)#*
Anunciar redes IPv4 conectadas directamente		*R3(config)#int s0/0/1* *R3(config-if)#ipv6 ospf 7 area 0* *R3(config)#int loopback 7* *R3(config-if)#ipv6 ospf 7 area 0* *R3(config-if)#exit*
Establecer todas las interfaces de LAN Ipv4 (Loopback) como pasivas		*R3(config)#ipv6 router ospf 7* *R3(config-rtr)#passive-interface loopback 4* *R3(config-rtr)#passive-interface loopback 5* *R3(config-rtr)#passive-interface loopback 6* *R3(config-rtr)#exit*
Desactive la sumariación automatica		*OSPF no realiza la sumarización de rutas de manera predeterminada.*

Fuente: Propia. Protocolo OSPF.

Figura 37. Verificación de configuración en ejecución R3.



Fuente: Propia. Comando Show run en R3.

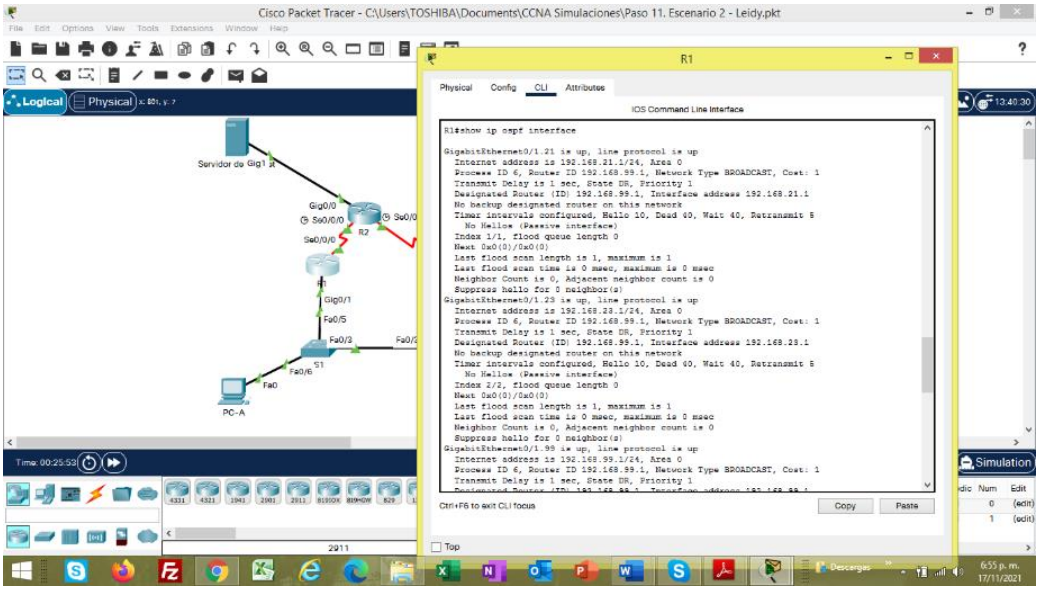
2.4.4. Paso 4: Verificar la información de OSPF

Tabla 21. Verificación de información 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 ospf interface
¿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 ospf

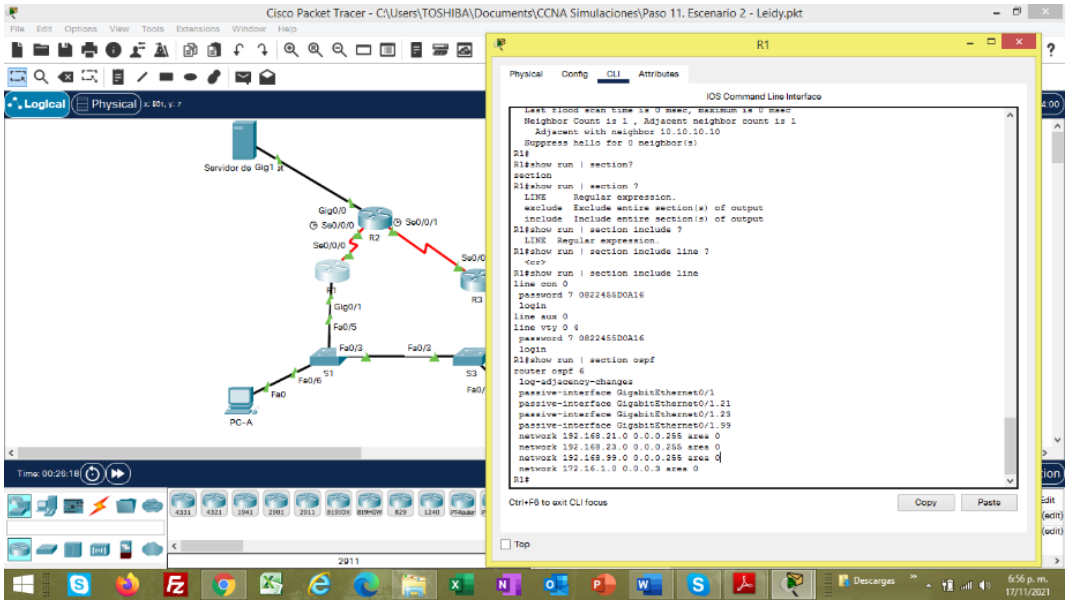
Fuente: Propia. Validación de OSPF.

Figura 38. Verificación protocolo OSPF en interfaces.



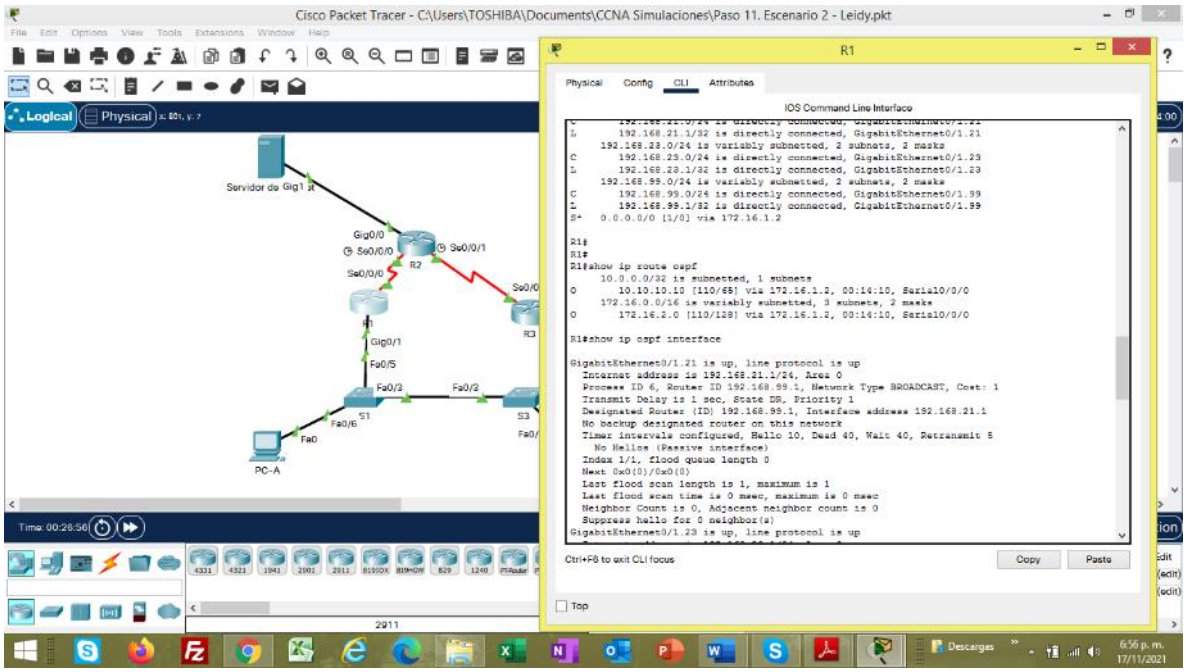
Fuente: Propia. Comando Show ip ospf interface.

Figura 39. Verificación línea OSPF de configuración en ejecución.



Fuente: Propia. Comando de Show run sección OSPF.

Figura 40. Rutas OSPF configuradas.



Fuente: Propia. Comando show ip route ospf.

2.5. Parte 5. Implementar DHCP y NAT para IPv4

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

Tabla 22. Configuración R1 DHCP.

Elemento o tarea de configuración	Especificación	*Comandos*
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas.		*R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20* *R1(config)#*
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* *R1(config)#*
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado	*R1(config)#ip dhcp pool ACCT* *R1(dhcp-config)#network 192.168.21.0 255.255.255.0* *R1(dhcp-config)#default-router 192.168.21.1* *R1(dhcp-config)#dns-server 10.10.10.10* *R1(dhcp-config)#domain-name ccna-sa.com*
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)#network 192.168.23.0 255.255.255.0* *R1(dhcp-config)#default-router 192.168.23.1* *R1(dhcp-config)#dns-server 10.10.10.10* *R1(dhcp-config)#domain-name ccna-sa.com*

Fuente: Propia. Configuración DHCP.

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

Tabla 23. Configuración NAT en R2.

Elemento o tarea de configuración	**Especificación**	***Comandos***
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: 15	*R2(config)#username webuser privilege 15 secret cisco12345* *R2(config)#*
Habilitar el servicio del servidor HTTP	En packet tracer se observa error al configurar el protocolo HTTP.	*R2(config)#ip http server* *^* *% Invalid input detected at '^' marker.* *R2(config)#*
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	En packet tracer se observa error al configurar el protocolo HTTP	*R2(config)#ip http authentication local* *^* *% Invalid input detected at '^' marker.* *R2(config)#*
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**	*R2(config)#ip nat inside source static 10.10.10.10 209.165.200.233* *R2(config)#*
Asignar la interfaz interna y externa para la NAT estática		*R2(config)#int g0/0* *R2(config-if)#ip nat outside* *R2(config-if)#int s0/0/0* *R2(config-if)#ip nat inside* *R2(config-if)#int s0/0/1* *R2(config-if)#ip nat inside* *R2(config-if)#int lo 0* *R2(config-if)#ip nat inside* *R2(config-if)#*
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1	*R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255*

	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 192.168.23.0 0.0.0.255* *R2(config)#access-list 1 permit 192.168.0.0 0.0.3.255* *R2(config)#*
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228**	*R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248* *R2(config)#*
Definir la traducción de NAT dinámica		*R2(config)#ip nat inside source list 1 pool INTERNET* *R2(config)#*

Fuente: Propia. Configuración de NAT (Traducción de direcciones de Red).

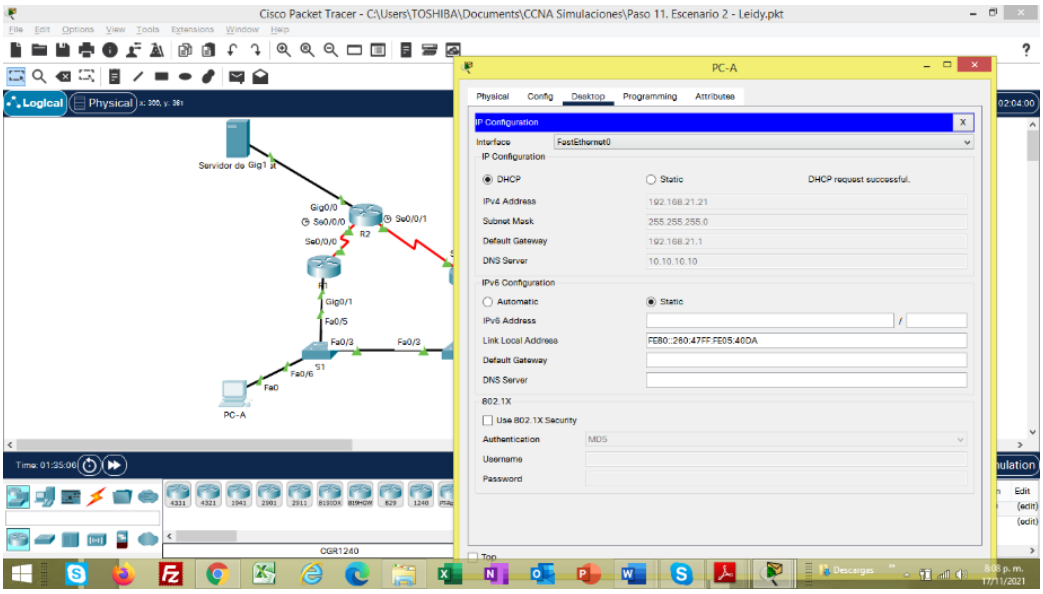
2.5.3. Paso 3: Verificar el protocolo DHCP y la NAT estática.

Tabla 24. Verificación DHCP y NAT.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	OK
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	OK
Verificar que la PC-A pueda hacer ping a la PC-C	OK
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	No es exitoso ya que no fue posible configurar los comandos para el servidor HTTP por lo que no solicita login de la base de datos local.

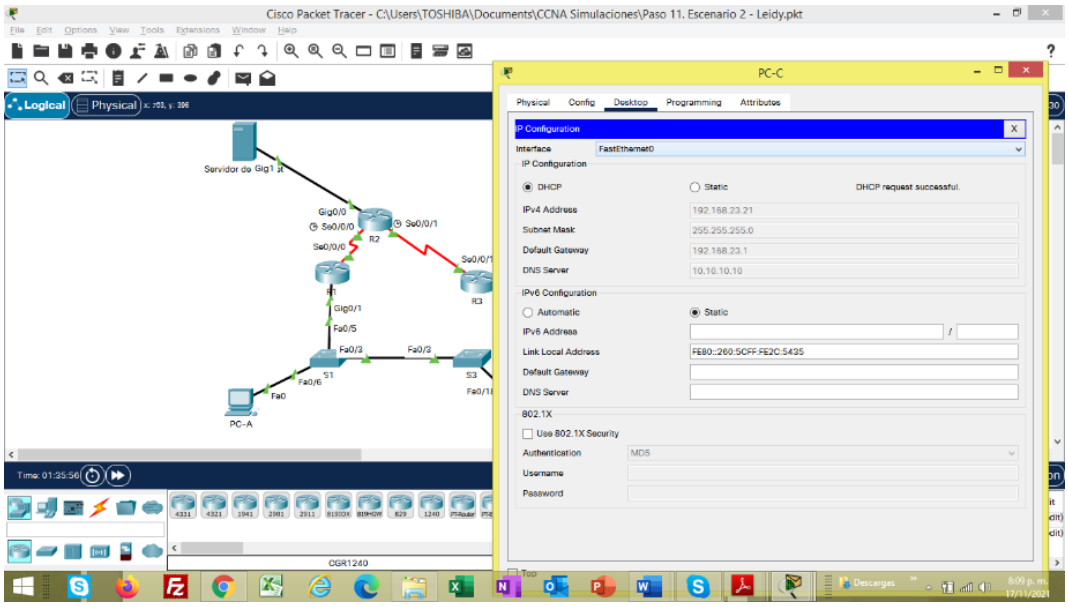
Fuente: Propia. Validación de configuración DHCP.

Figura 41. DHCP en PCA.



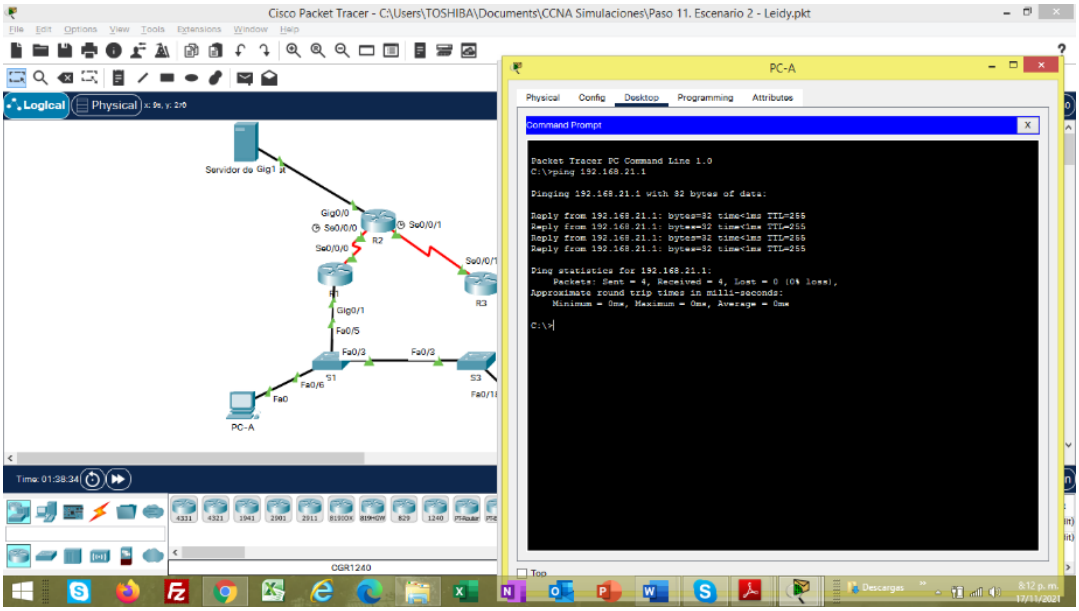
Fuente: Propia. Habilitación de direccionamiento dinámico en PC-A.

Figura 42. DHCP en PCC.



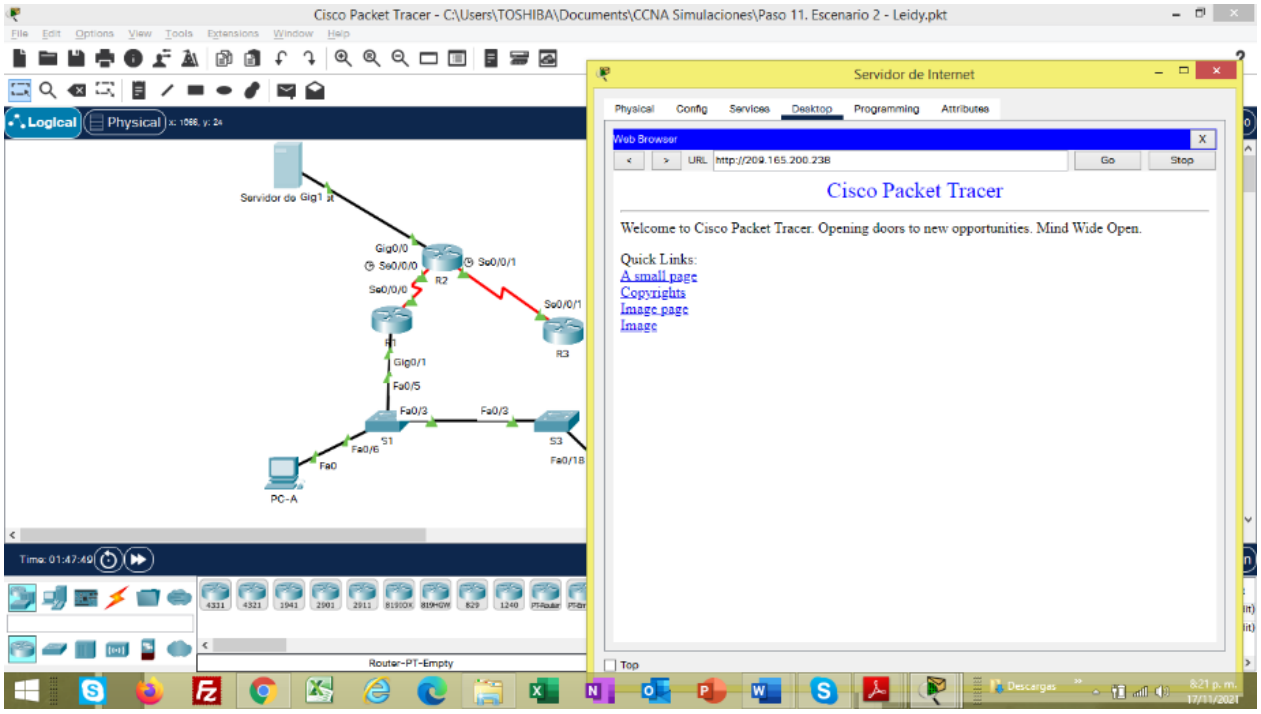
Fuente: Propia. Habilitación DHCP en PC-C.

Figura 43. Ping PCA a PCC.



Fuente: Propia. Validación de PC-A a PC-C.

Figura 44. Conexión HTTP desde computadora de Internet.



Fuente: Propia. Acceso a Servidor de Internet.

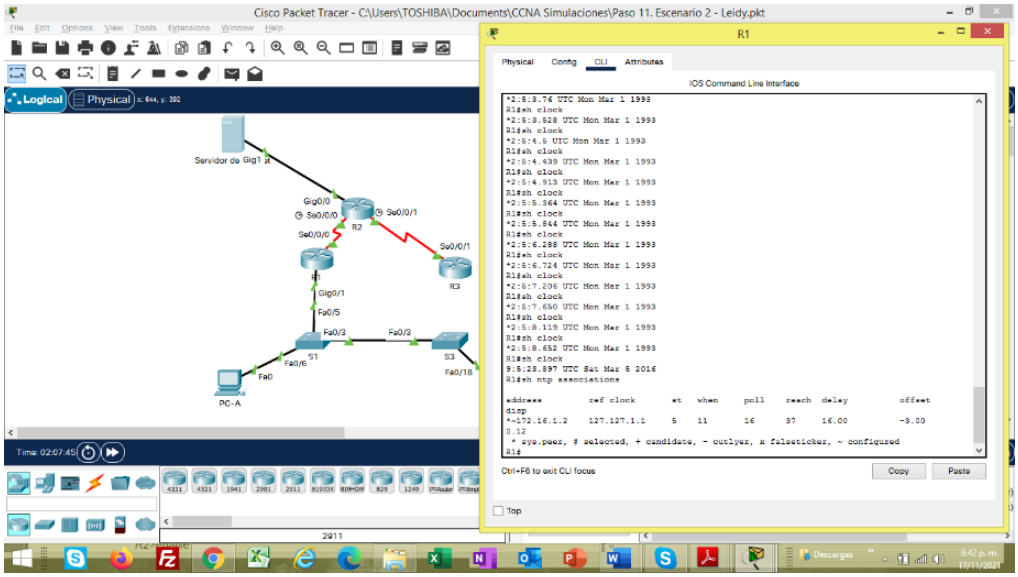
2.6. Parte 6. Configurar NTP.

Tabla 25. Configuración NTP.

Elemento o tarea de configuración	Especificación	*Comandos*
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.**	*R2#clock set 09:00:00 05 march 2016*
Configure R2 como un maestro NTP.	Nivel de estrato: 5	*R2(config)#ntp master 5*
Configurar R1 como un cliente NTP.	Servidor: R2	*R1#config t R1(config)#ntp server 172.16.1.2*
Configure R1 para actualizaciones de calendario periódicas con hora NTP.		*R1(config)#ntp updatecalendar*
Verifique la configuración de NTP en R1.		*R1#show ntp associations*

Fuente: Propia. Configuración de protocolo de sincronización de reloj.

Figura 45. Verificación de NTP en R1.



Fuente: Propia. Validación de NTP comando show ntp associations.

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

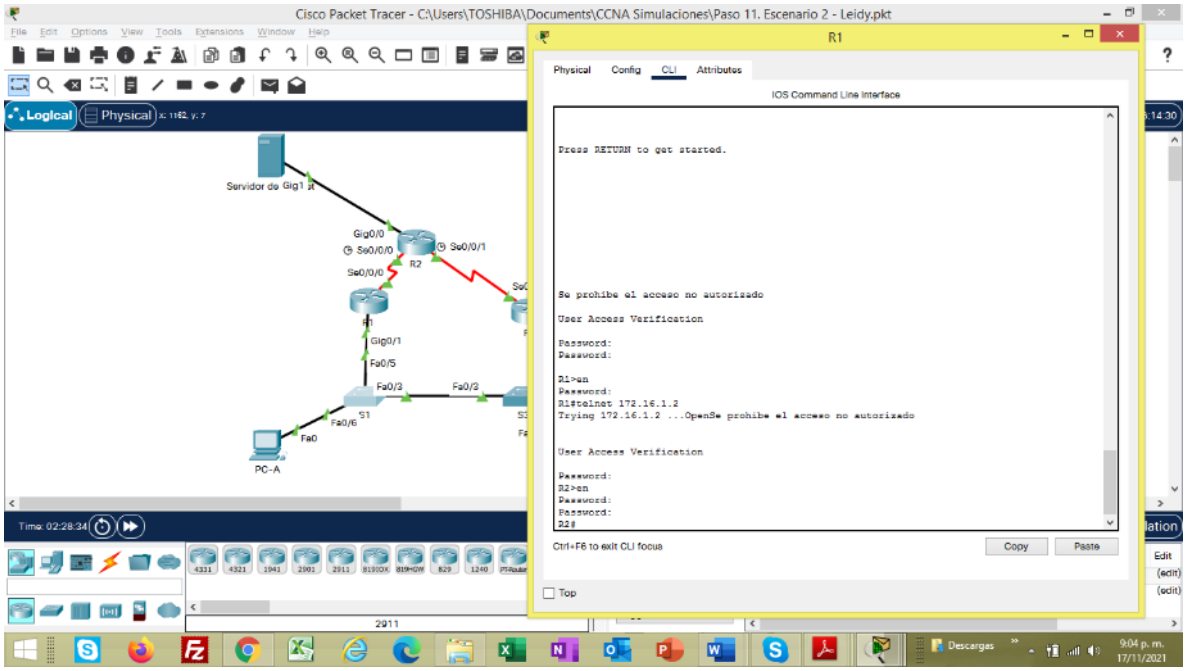
2.7.1. Paso 1: Restringir el acceso a las líneas VTY en el R2.

Tabla 26. Configuración Listas ACL.

Elemento o tarea de configuración	**Especificación**	***Comandos***
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)#deny any*
Aplicar la ACL con nombre a las líneas VTY		*R2(config)#line vty 0 4* *R2(config-line)#access-class ADMIN-MGT in* *R2(config-line)#*
Permitir acceso por Telnet a las líneas de VTY		*R2(config-line)#transport input telnet*
Verificar que la ACL funcione como se espera		*R1>en* *Password:* *R1#telnet 172.16.1.2* *Trying 172.16.1.2 ...OpenSe prohibe el acceso no autorizado* *User Access Verification* *Password:* *R2>en* *Password:*

Fuente: Propia. Configuración de Listas de acceso.

Figura 46. Acceso Telnet R1 a R2.



Fuente: Propia. Verificación de acceso Telnet.

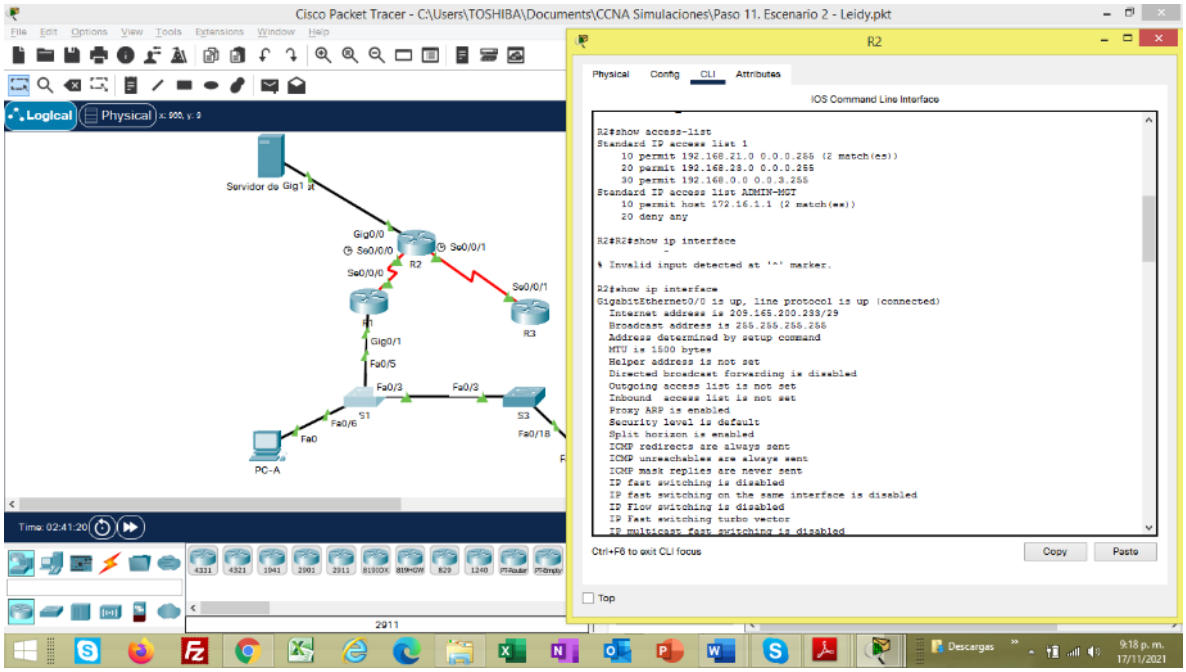
2.7.2. Paso 2. Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente.

Tabla 27. Verificación de listas de Acceso.

Descripción del comando	*Entrada del estudiante (comando)*
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	*R2#show access-list* *Standard IP access list 1* *10 permit 192.168.21.0 0.0.0.255 (2 match(es))* *20 permit 192.168.23.0 0.0.0.255* *30 permit 192.168.0.0 0.0.3.255* *Standard IP access list ADMIN-MGT* *10 permit host 172.16.1.1 (2 match(es))* *20 deny any*
Restablecer los contadores de una lista de acceso	*R2#clear ip 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?	*R2#show ip nat translations* ***Nota:*** *Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.*
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	*R2#clear ip nat translation*

Fuente: Propia. Comando para validar ACL, NAT y NTP.

Figura 47. Verificación de Configuración Listas de acceso.



Fuente: Propia. Verificación de ACL.

CONCLUSIONES

El simulador de redes permite creación y esquematización de una topología, ofreciendo opciones de configuración de diferentes dispositivos como Router, Switch, PC o Accespoint generando un espacio de practica donde se adquieren habilidades y destrezas para interactuar con redes.

La seguridad en las redes es de vital importancia para las organizaciones y redes domesticas originando protección ante intrusos o programas mal intencionados que requieren la información y los datos del sistema, por lo tanto, se aplica configuraciones de acceso a consola, a modo privilegiado y en SSH.

BIBLIOGRAFÍA

BEMBIBRE, Victoria. Definición de Router. {En línea}. {22 de octubre de 2021}. Disponible en https://www.definicionabc.com/tecnologia/router.php

PEREZ, Julian. Definición de IP. {En línea}. {22 de octubre de 2021}. Disponible en https://definicion.de/ip/

Oracle, Corporation. ¿Qué son las Subredes?. {En línea}. {22 de octubre de 2021}. Disponible en https://docs.oracle.com/cd/E19957-01/820-2981/ipconfig-31/index.html

CISCO. (2019). Direccionamiento IP. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7

CISCO. (2019). División de redesIP en subredes. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8