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

MIGUEL ARMANDO YELA QUENGUAN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE SISTEMAS
PROVIDENCIA – NARIÑO
2021

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

MIGUEL ARMANDO YELA QUENGUAN

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

DIRECTORA: Esp. NANCY AMPARO GUACA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
PROVIDENCIA - NARIÑO
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Providencia, 20 de octubre del 2021

AGRADECIMIENTOS

En el presente trabajo quiero agradecer primeramente a Dios por ser mi guía y acompañarme en el transcurso y logro de esta importante meta, brindándome su bendición, paciencia, fuerza y sabiduría para culminar con éxito mi carrera profesional.

A mis padres, Jesús Álvaro Yela y Mercedes Dolores Quenguán, que han sabido darme su ejemplo de trabajo e inspirar valores que me permiten ser una gran persona. Además, por ser un pilar fundamental y apoyarme incondicionalmente para lograr cumplir todas mis metas.

A la Universidad Nacional Abierta y Distancia, que con su gran equipo de tutores estuvieron guiándome académicamente con su experiencia y profesionalismo para concluir esta importante etapa de mi vida formándome como una gran persona y profesional en Ingeniería de Sistemas.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

SWITCH: También conocido como conmutador, es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se llama red de área local (LAN).

ROUTER: Dispositivo de hardware, el cual gestiona el tráfico de información entre los equipos y dispositivos que están conectados a una red. Este determina las rutas por las que pasarán los paquetes de datos y permite la interconexión de redes.

GATEWAY: También llamado puerta de enlace, es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación ya que se encuentra dentro de la misma. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

DHCP: Protocolo de configuración de host dinámico, utilizado en redes IP, el cual asigna automáticamente una dirección IP a cada host en la red para que puedan comunicarse de manera eficiente con otros puntos finales.

DIRECCIÓN IP: Dirección que se utiliza para identificar un equipo o dispositivo en una red.

DIRECCIÓN IP DINÁMICA: Dirección IP temporal que asigna un servidor DHCP.

DIRECCIÓN IP ESTÁTICA: Dirección IP fija que se asigna de manera manual a un equipo o dispositivo conectado a una red

IPV4: Sistema direccional de 32 bits, que se usa para identificar un dispositivo en una red.

IPV6: Sistema direccional de 128 bits, que se usa para identificar un dispositivo en una red. Este sistema es una actualización al IPv4, la mayoría de la versión reciente del sistema direccional usado en las redes informáticas. Una de sus principales características es que cuenta con mayor capacidad de direcciones IP.

MÁSCARA DE SUBRED: Código que define un rango de Direcciones IP disponible dentro de una red.

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

RESUMEN

El diplomado de profundización CCNA permite adquirir conocimientos para implementar y administrar redes soportadas con tecnología CISCO, se centra en explicar de forma detallada y práctica los fundamentos de las redes informáticas, los protocolos de red y gestionar de forma segura los routers y switches que forman parte de una infraestructura de red.

Este documento destaca el conocimiento, las habilidades y la resolución de problemas adquiridos a lo largo del curso. En el primer escenario, se construye una pequeña red, donde se desarrolla un esquema de direccionamiento IPV4 para LAN1 y LAN2, se configuran los dispositivos, se administran de manera segura y finalmente se prueba la conectividad entre las computadoras. En el siguiente escenario, se configura una pequeña red que debe soportar conectividad IPv4 e IPv6, garantizar la seguridad del equipo VLAN, el protocolo de enrutamiento dinámico OSPF, el protocolo de configuración dinámica de host (DHCP), la traducción de direcciones de red (dinámica y estática). NAT), listas de control de acceso (ACL) y servidor / cliente de protocolo de tiempo de red (NTP), al final se prueba la conectividad y se registra la red mediante comandos CLI comunes.

Palabras clave: Puerta de enlace, dirección IP, máscara de subred, conmutador, router, host.

ABSTRACT

The CCNA in-depth diploma allows you to acquire knowledge to implement and manage networks supported with CISCO technology, it is mainly focused on explaining in a detailed and practical way the fundamentals of computer networks, network protocols and securely managing routers and switches, which they are part of a network infrastructure.

This document highlights the knowledge, skills, and problem solving acquired throughout the course. In the first scenario, a small network is built, where an IPV4 addressing scheme is developed for LAN1 and LAN2, the devices are configured, managed safely and finally the connectivity between the computers is tested. In the following scenario, a small network is configured that must support IPv4 and IPv6 connectivity, guarantee the security of the VLAN equipment, the dynamic routing protocol OSPF, the dynamic host configuration protocol (DHCP), the translation of network addresses (Dynamic and static NAT), Access Control Lists (ACLs) and Network Time Protocol (NTP) server / client, at the end connectivity is tested and the network is registered using common CLI commands.

Keywords: Gateway, IP address, subnet mask, switch, router, host.

INTRODUCCIÓN

El diplomado de profundización de CNNA es de gran importancia para el desarrollo de nuestra carrera, con su sello de calidad y prestigio se fundamenta en el enriquecimiento de nuestro conocimiento como futuros ingenieros, permitiendo el desarrollo intelectual, brindando oportunidades para adquirir habilidades y la experiencia práctica para, analizar, diseñar, instalar, operar y mantener redes empresariales de tamaño pequeño y mediano, así como también en los entornos empresariales y de proveedores de servicios.

Se implementa el primer escenario donde se construye una red pequeña y de acuerdo con el requerimiento de la misma para LAN1 y LAN 2 se desarrollando un esquema de direccionamiento IPV4 con mascara de subred longitud variable VLSM, posteriormente se configurarán y se administran los dispositivos de forma segura, por último, se comprueba conectividad entre equipos obteniendo los resultados esperados.

El siguiente escenario permite administrar de forma correcta una red pequeña con conectividad IPv4 e IPv6. Además, garantiza seguridad de equipos, configurar distintos protocolos como OSPF, (DHCP), (NTP). Al finalizar se obtiene los resultados esperados mediante la conectividad entre equipos y pruebas con comandos, de igual forma se observa la lista comandos utilizados y cada pantallazo que se le tomó como evidencia en la simulación y configuración de cada dispositivo intermedio y hosts.

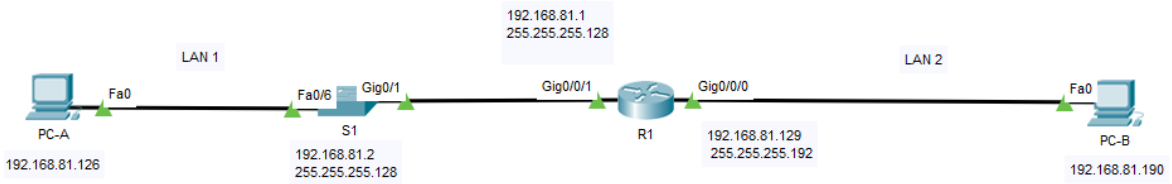
DESARROLLO

1. ESCENARIO 1

Figura 1. Escenario propuesto

Fuente: Prueba de habilidades CISCO CCNA II

Figura 2. Simulación del escenario 1



Fuente: Elaboración propia

1.1 Desarrollo del esquema de direccionamiento IP.

Para la dirección IPv4 se creó las dos subredes con la cantidad requerida de hosts. Se asigno las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento.

Para el direccionamiento se toma como base la IP 192.168.X.0 donde X corresponde a los últimos dos dígitos del número de cedula 1.085.899.481 perteneciente a Miguel Armando Yela Quenguán.

Dirección IP base con su mascara de subred = 192.168.81.0 255.255.255.0

Requerimiento de Red

LAN 1 = 100 hosts

LAN 2 = 50 hosts

Para el requerimiento, se aplicó mascara de subred de longitud variable VLSM

LAN 1 Para 100 host 2^7= 128

Mascara x defecto	11111111	11111111	11111111	00000000	/24
Nueva máscara	11111111	11111111	11111111	10000000	/25
Notación Decimal	255	255	255	128	

Salto de 128 direcciones

LAN 2 Para 50 host 2^6= 64

Mascara x defecto	11111111	11111111	11111111	00000000	/24
Nueva máscara	11111111	11111111	11111111	11000000	/26
Notación Decimal	255	255	255	192	

Salto de 64 direcciones

Tabla 1. Subnetting

Subred	**Dirección**	**1 IP válida**	**ultima IP válida**	**Broadcast**	**N° host**
LAN 1	192.168.81.0/25	192.168.81.1	192.168.81.126	192.168.81.127	126
LAN 2	192.168.81.128/26	192.168.81.129	192.168.81.190	192.168.81.191	62

Fuente: Elaboración propia

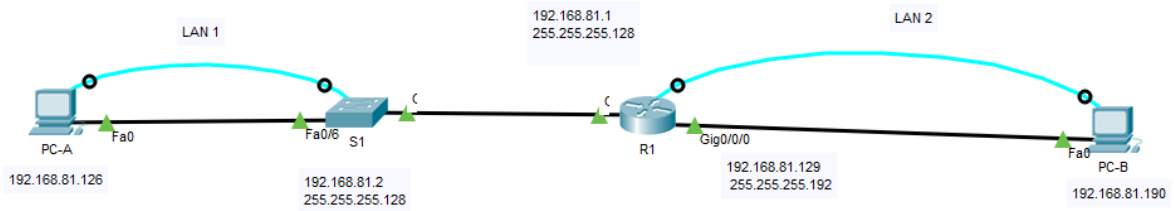
Tabla 2. Direccionamiento

Ítem	Requerimiento
Dirección de Red	192.168.81.0
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	Primera dirección de host de la subred LAN1 192.168.81.1
R1 G0/0/0	Primera dirección de host de la subred LAN2 192.168.81.129
S1 SVI	Segunda dirección de host de la subred LAN1 192.168.81.2
PC-A	Última dirección de host de la subred LAN1 192.168.81.126
PC-B	Última dirección de host de la subred LAN2 192.168.81.190

Fuente: Elaboración propia

Los dispositivos de red (S1 y R1) se configuraron mediante conexión de consola.

Figura 3. Simulación escenario 1, configuración por consola



Fuente: Elaboración propia

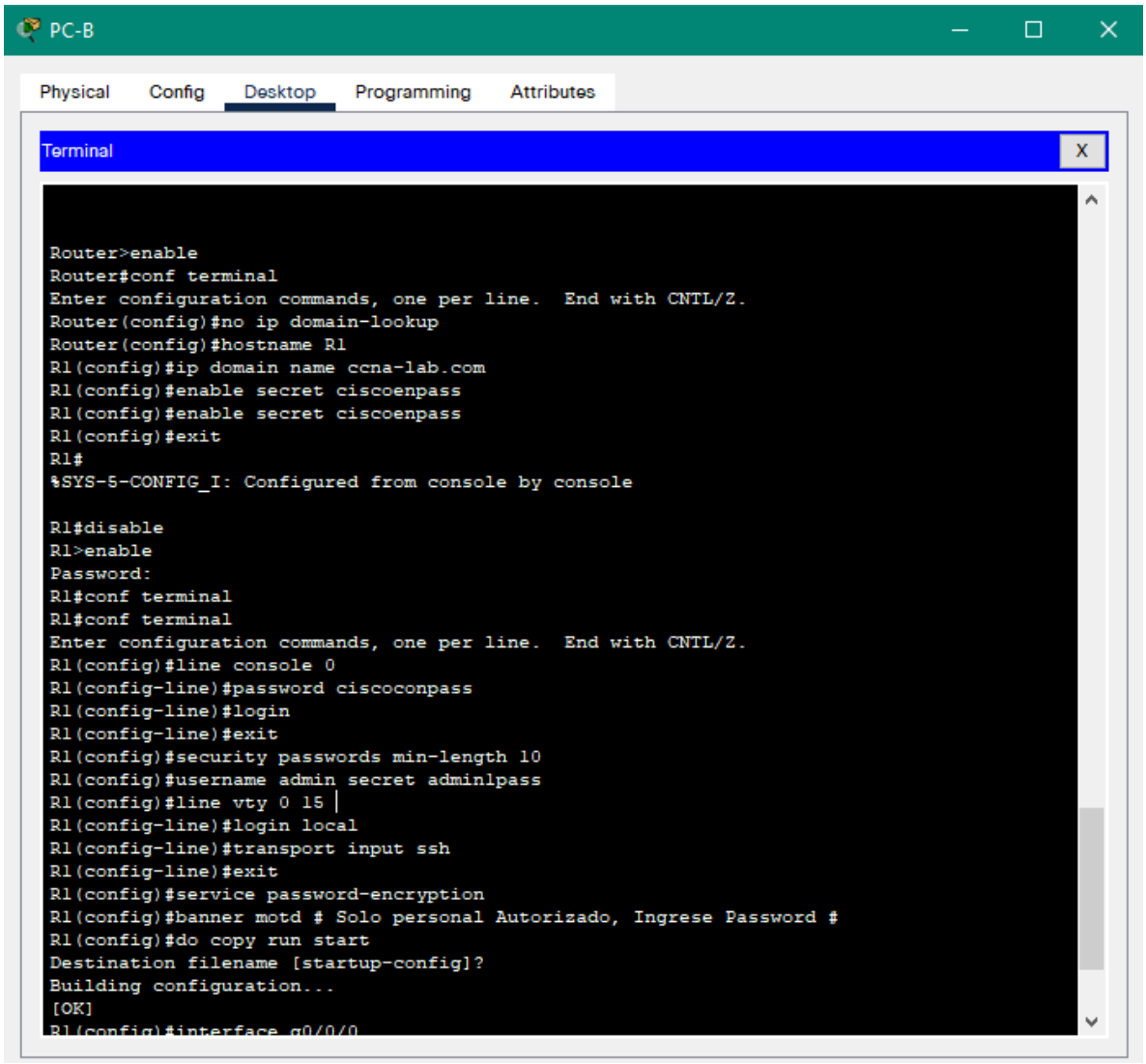
Se adjunta código y pantallazos con veracidad del código.

1.2 Configuración para R1

```
Router>enable                                   Ingreso a modo privilegiado
Router#conf terminal                            Ingreso a modo de configuración
Router(config)#no ip domain-lookup              Desactivo la búsqueda DNS
Router(config)#hostname R1                      Asigno nombre al router
R1(config)#ip domain name ccna-lab.com          Asigno nombre de dominio a router
R1(config)#enable secret ciscoenpass            Asigno contraseña cifrada para
modo EXEC privilegiado
R1(config)#exit                                 Salgo del modo configuración
R1#disable                                      Salgo del modo privilegiado
R1>enable                                       Ingreso a modo privilegiado
Password:                                       Ingreso contraseña cifrada
R1#conf terminal                                Ingreso a modo de configuración
R1(config)#line console 0                       Ingreso a configuración de consola
R1(config-line)#password ciscoconpass           Asigno clave de acceso a consola
R1(config-line)#login                           Habilito la clave ingresada
R1(config-line)#exit                            Salgo de configuración de consola
R1(config)#security passwords min-length 10     Asigno longitud mínima para
contraseñas
R1(config)#username admin secret admin1pass     Creo usuario administrativo
en la base de datos local
R1(config)#line vty 0 15                        Configuro el inicio de sesión en VTY
R1(config-line)#login local                     Configuración a base de datos local
R1(config-line)#transport input ssh             Configuro VTY solo para SSH
R1(config-line)#exit                            Salgo de configuración VTY
R1(config)#service password-encryption          Asigno contraseñas de texto no
cifrado
R1(config)#banner motd # Solo personal Autorizado, Ingrese Password # Configuro
un MOTD Banner al inicio del router
R1(config)#do copy run start                    Guardo la configuración del router
R1(config)#interface g0/0/0                     Configuro interfaz g0/0/0
R1(config-if)#description Conexion LAN 2 -PC-B      Agrego descripción
R1(config-if)#ip address 192.168.81.129 255.255.255.192   Asigno IP y mascara
R1(config-if)#no shutdown                           Habilito la interfaz
R1(config-if)#exit                              Salgo de configuración de interfaz
R1(config)#interface g0/0/1                     Configuro interfaz g0/0/1
R1(config-if)#description Conexion a LAN 1 -PC-A    Agrego descripción
R1(config-if)#ip address 192.168.81.1 255.255.255.128   Asigno IP y mascara
R1(config-if)#no shutdown                           Habilito la interfaz
R1(config-if)#do show ip interface brief        Verifico interfaces del router
R1(config-if)#exit                              Salgo de configuración de interfaz
```

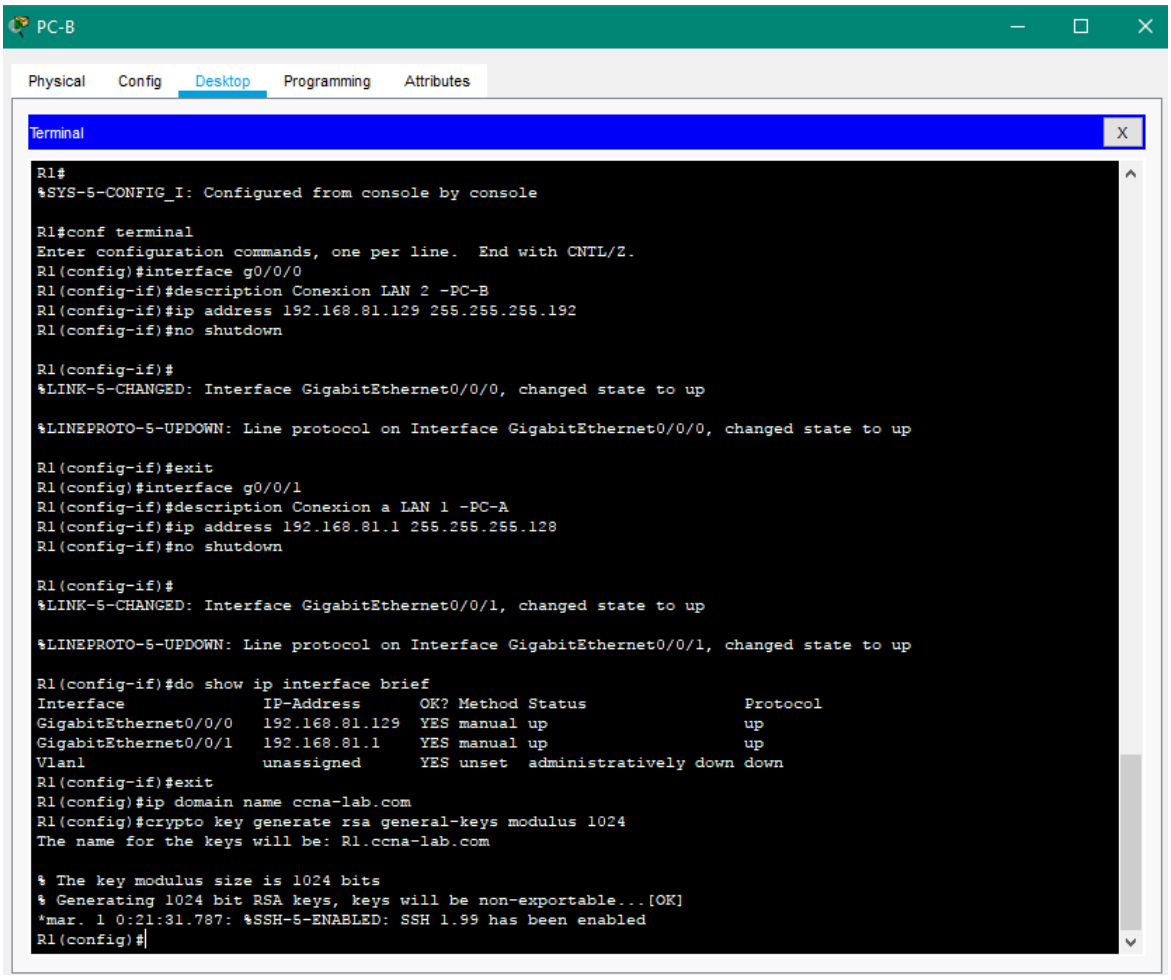
R1(config)#ip domain name ccna-lab.com Creo dominio para generar clave de cifrado RSA
R1(config)#crypto key generate rsa general-keys modulus 1024 Genero la Clave
R1(config-if)#exit Salgo de modo configuración

Figura 4. Configuración inicial R1



Fuente: Elaboración propia

Figura 5. Configuración de interfaces R1



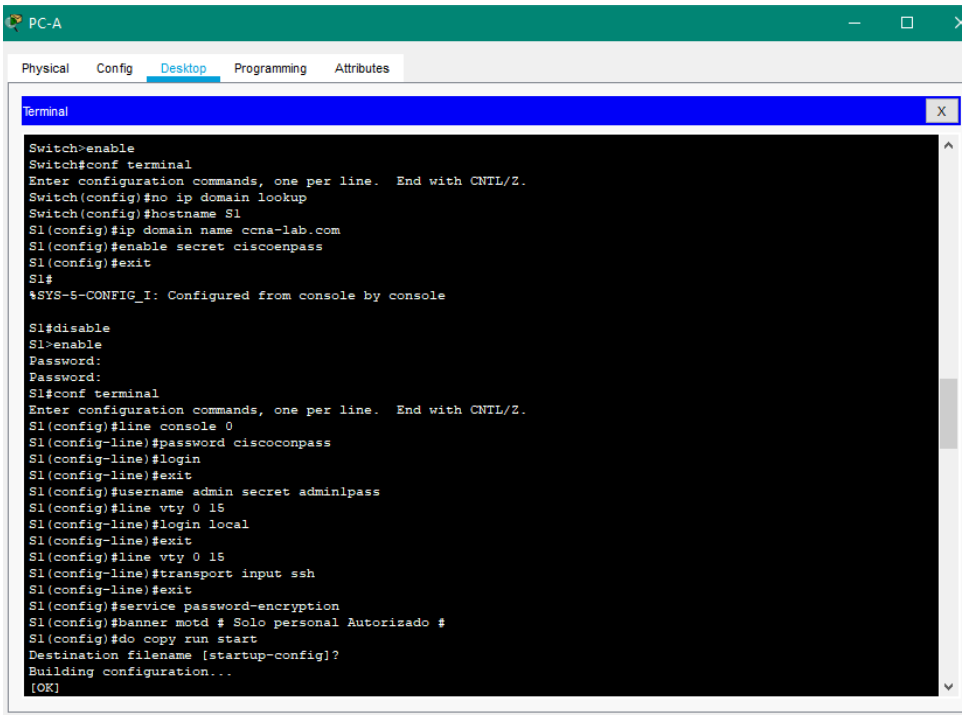
Fuente: Elaboración propia

1.3 Configuración para S1

Switch>enable	Ingreso a modo privilegiado
Switch#conf terminal	Ingreso a modo de configuración
Switch(config)#no ip domain lookup	Desactivo la búsqueda DNS
Switch(config)#hostname S1	Asigno nombre al switch
S1(config)#ip domain name ccna-lab.com	Asigno nombre de dominio al switch
S1(config)#enable secret ciscoenpass	Asigno contraseña cifrada para modo EXEC privilegiado
S1(config)#exit	Salgo del modo configuración

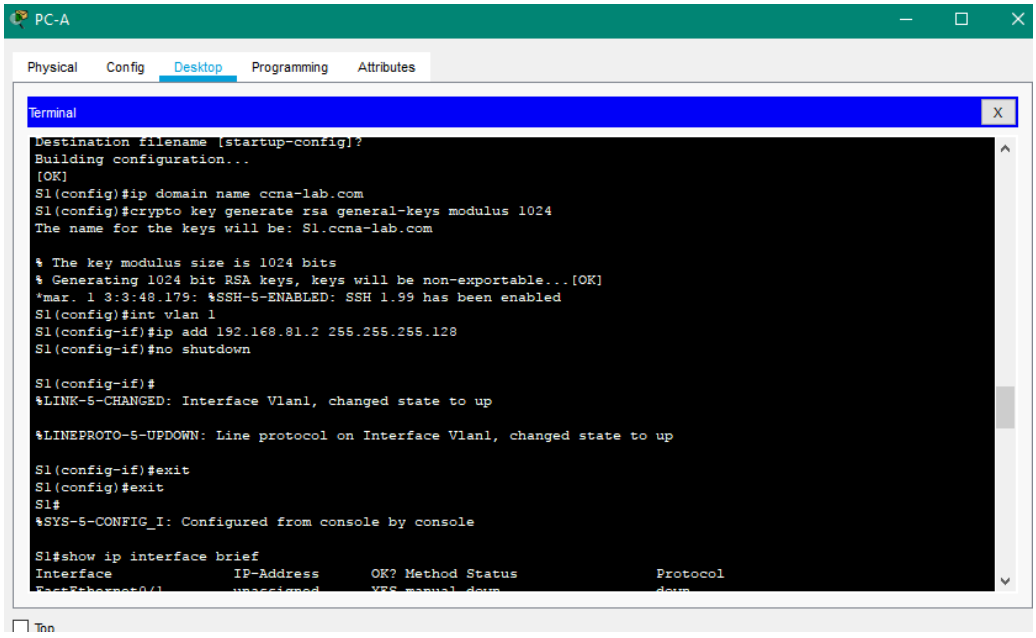
S1#disable Salgo del modo privilegiado
S1>enable Ingreso a modo privilegiado
Password: Ingreso contraseña cifrada
S1#conf terminal Ingreso a modo de configuración
S1(config)#line console 0 Ingreso a configuración de consola
S1(config-line)#password ciscoconpass Asigno clave de acceso a consola
S1(config-line)#login Habilito la clave ingresada
S1(config-line)#exit Salgo de configuración de consola
S1(config)#username admin secret admin1pass Creo usuario administrativo en la base de datos local
S1(config)#line vty 0 15 Configuro el inicio de sesión en VTY
S1(config-line)#login local Configuración a base de datos local
S1(config-line)#exit Salgo de configuración VTY
S1(config)#line vty 0 15 Configuro el inicio de sesión en VTY
S1(config-line)#transport input ssh Configuro VTY solo para SSH
S1(config-line)#exit Salgo de configuración VTY
S1(config)#service password-encryption Asigno contraseñas de texto no cifrado
S1(config)#banner motd # Solo personal Autorizado # Configuro un MOTD Banner al inicio del switch
S1(config)#do copy run start Guardo la configuración del switch
S1(config)#ip domain name ccna-lab.com Creo dominio para generar clave de cifrado RSA
S1(config)#crypto key generate rsa general-keys modulus 1024 Genero la Clave
S1(config)#int vlan 1 configuro interfaz de administración
S1(config-if)#ip add 192.168.81.2 255.255.255.128 Asigno IP y máscara
S1(config-if)#no shutdown Habilito la interfaz
S1(config-if)#exit Salgo de Interfaz
S1#conf terminal
S1(config)#ip default-gateway 192.168.81.1 Configuración del gateway predeterminado
S1(config)#do copy running-config startup-config Guardo configuración
S1(config)#

Figura 6. Configuración inicial S1



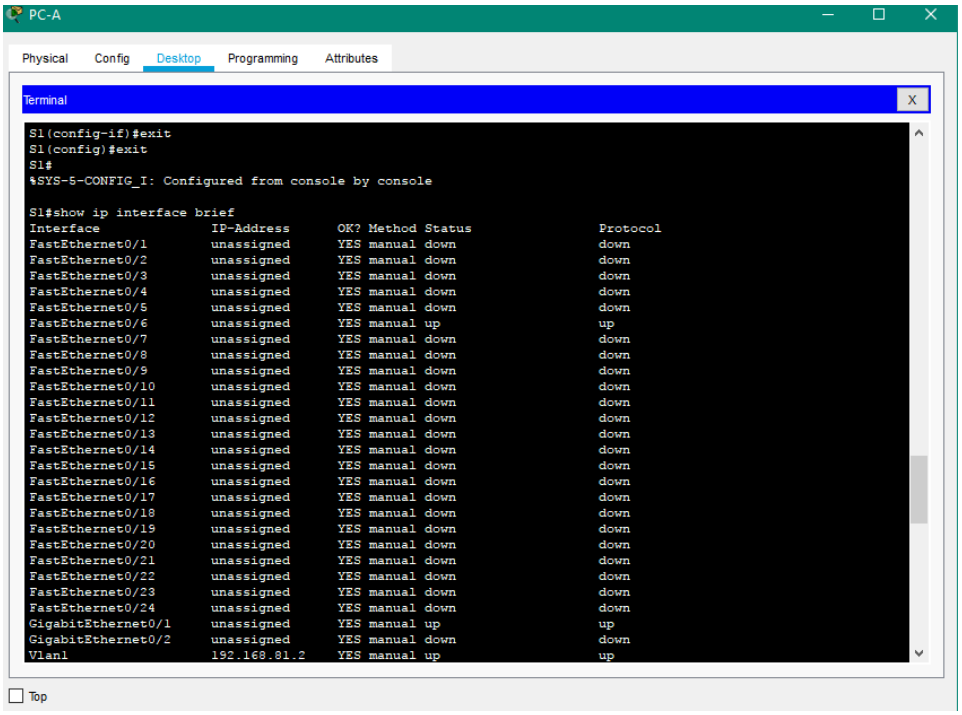
Fuente: Elaboración propia

Figura 7. Configuración de interfaz S1



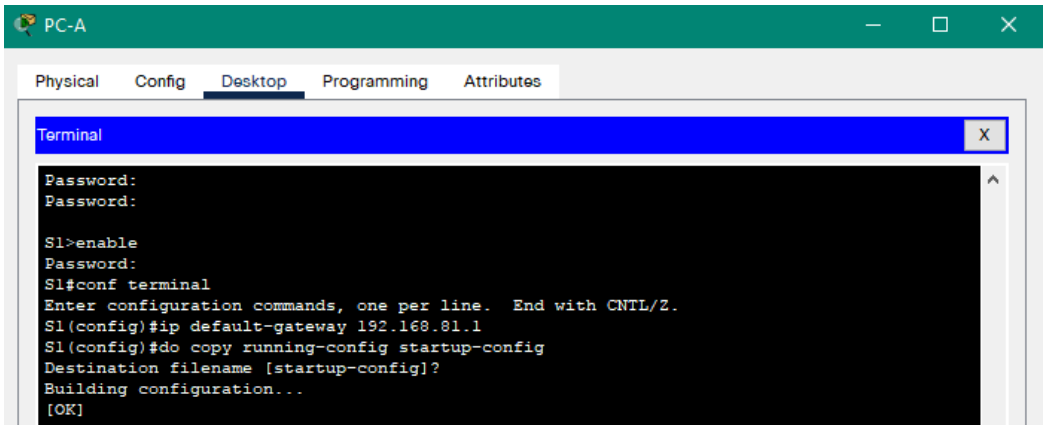
Fuente: Elaboración propia

Figura 8. Verificación de configuración de interfaz S1



Fuente: Elaboración propia

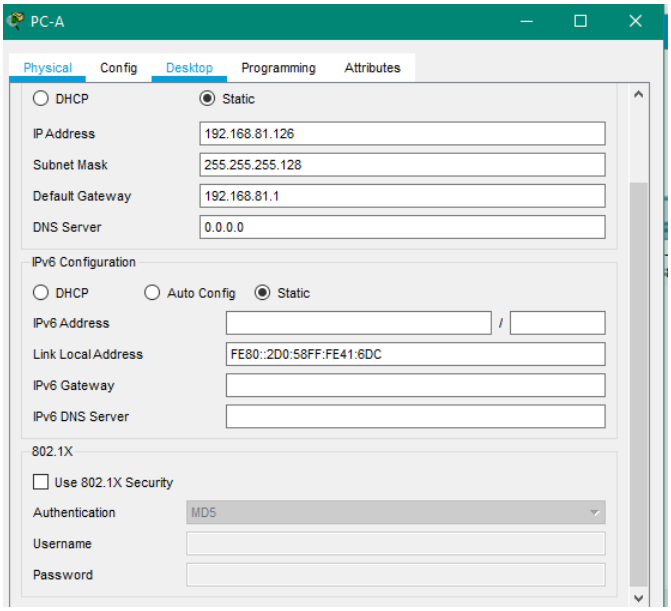
Figura 9. Configuración Gateway predeterminado S1



Fuente: Elaboración propia

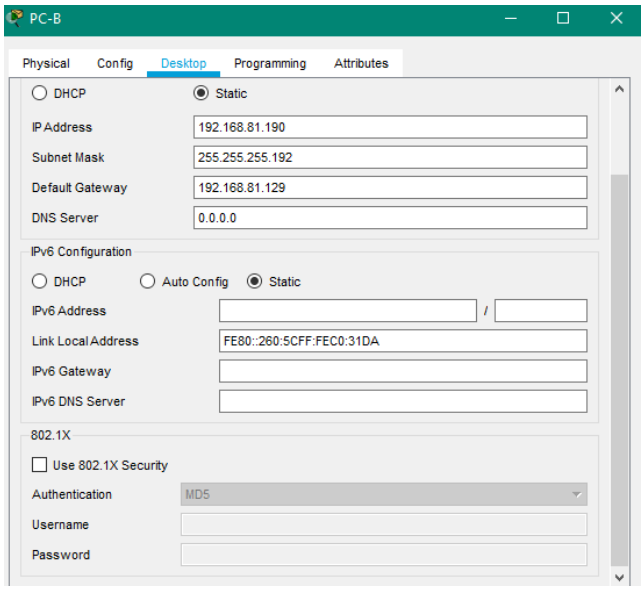
1.4 Configuración de los equipos host PC-A y PC-B conforme a la tabla de direccionamiento.

Figura 10. Configuración host PC-A



Fuente: Elaboración propia

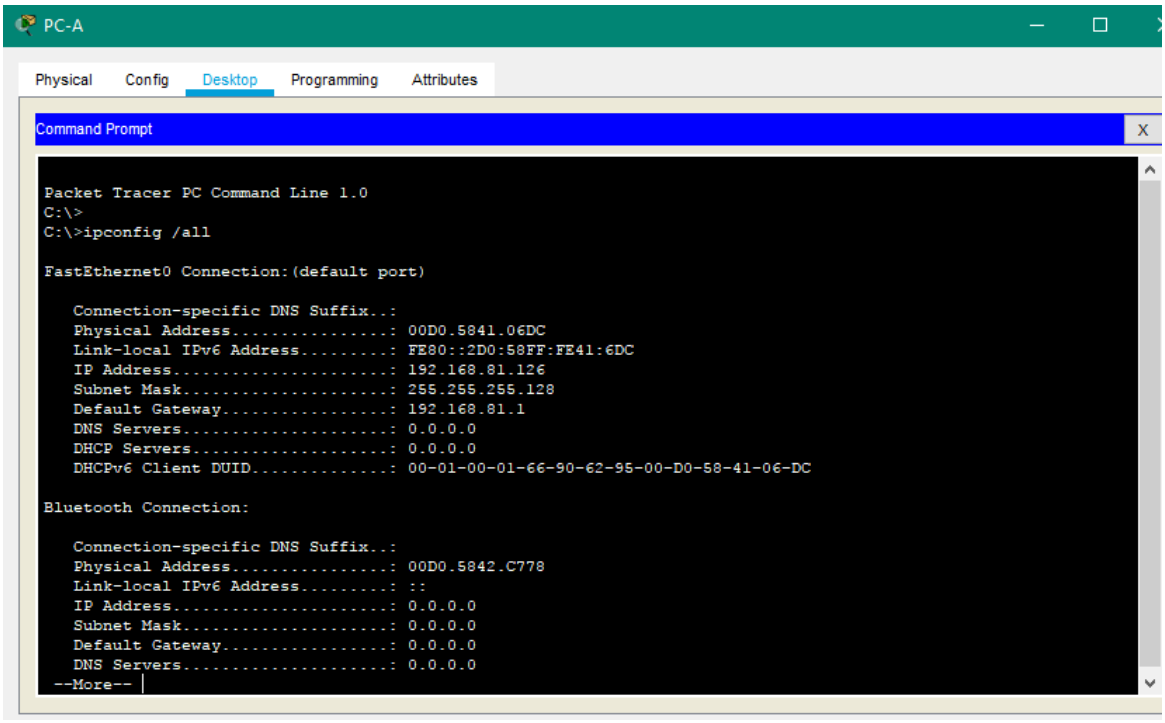
Figura 11.Configuración host PC-B



Fuente: Elaboración propia

1.5 Registro de las configuraciones de red del host con el comando ipconfig /all.

Figura 12. Comando ipconfig /all host PC-A



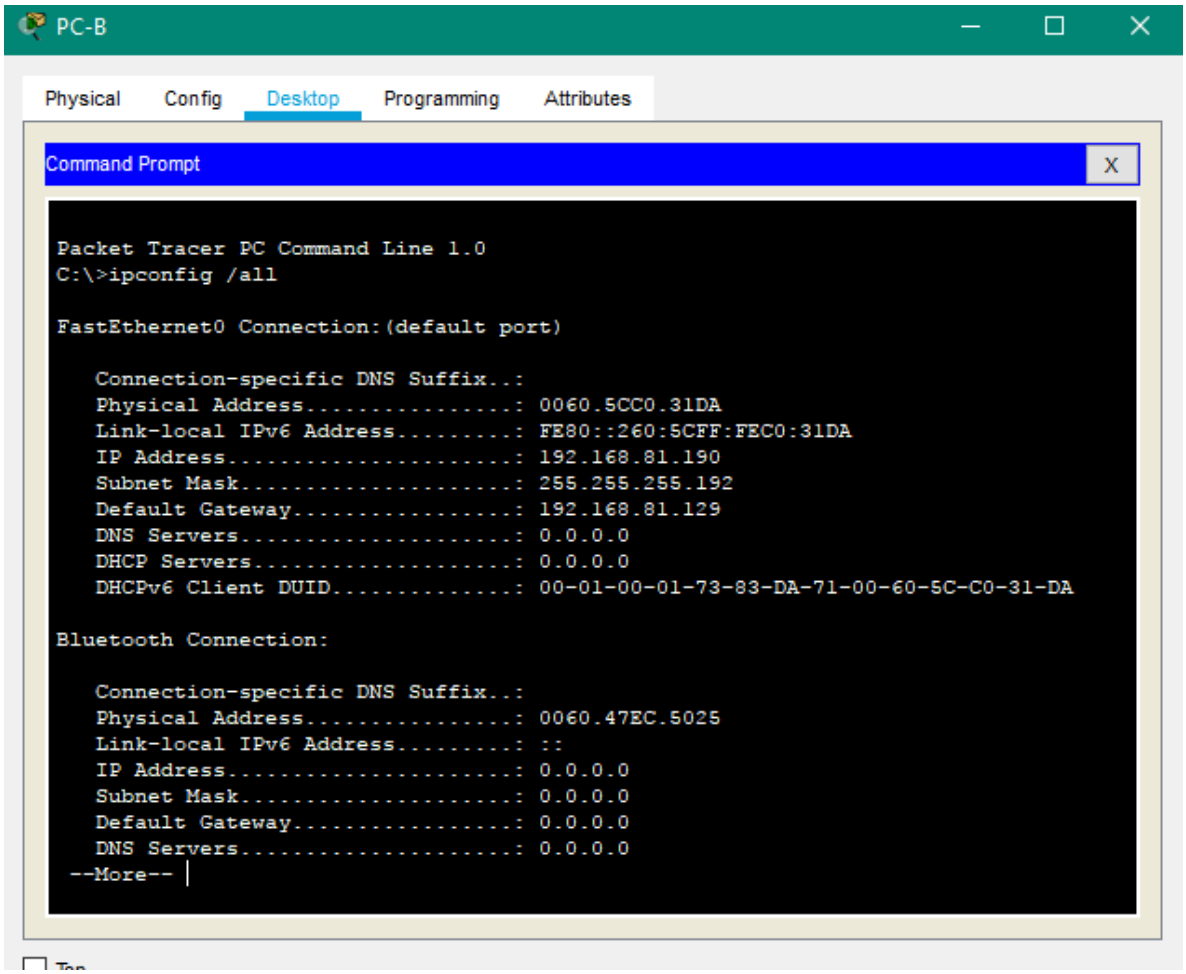
Fuente: Elaboración propia

Tabla 3. Configuración host PC-A – LAN 1

Descripción	**PC-A- LAN 1**
Dirección física	00D0.5841.06DC
Dirección IP	192.168.81.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.81.1

Fuente: Elaboración propia

Figura 13. Comando ipconfig /all host PC-B



Fuente: Elaboración propia

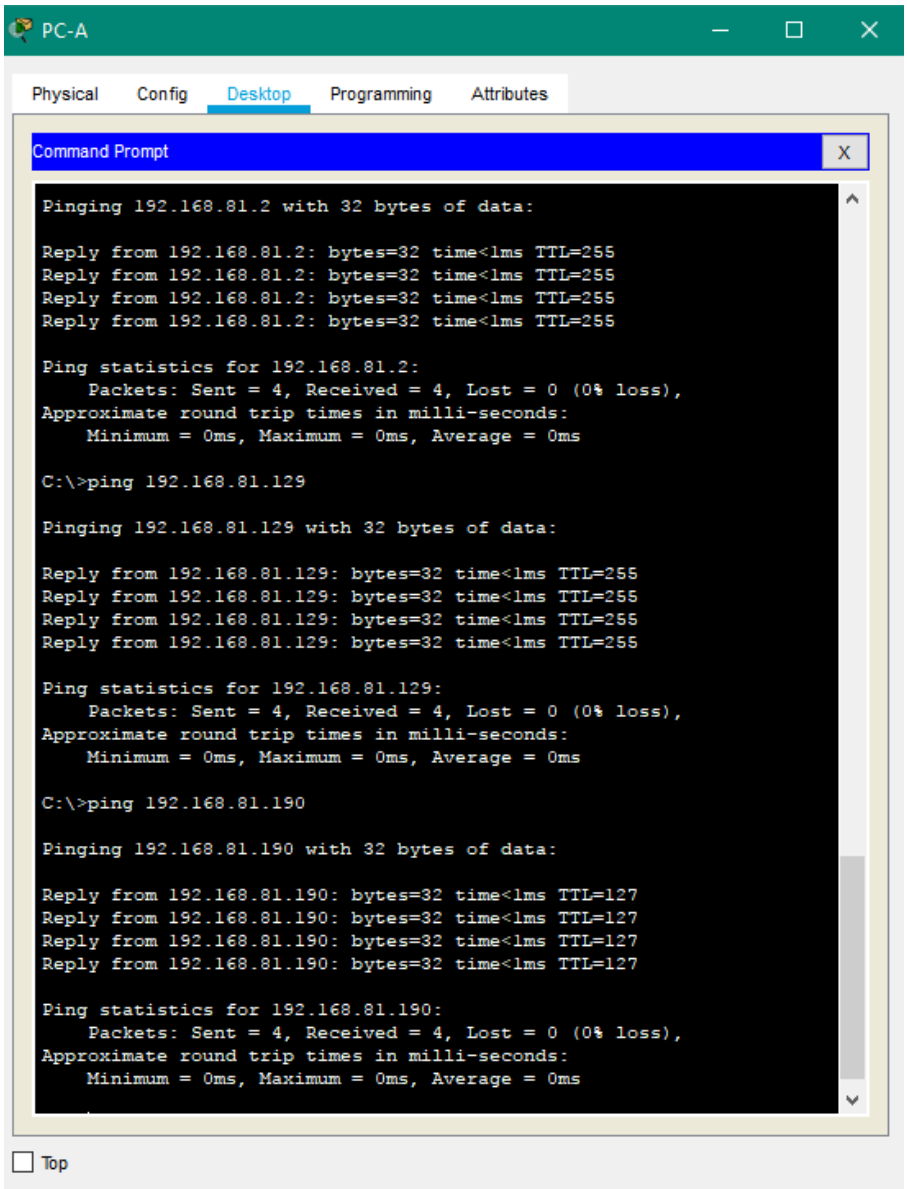
Tabla 4. Configuración host PC-B – LAN 2

Descripción	**PC-B LAN 2**
Dirección física	0060.5CC0.31DA
Dirección IP	192.168.81.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.81.128

Fuente: Elaboración propia

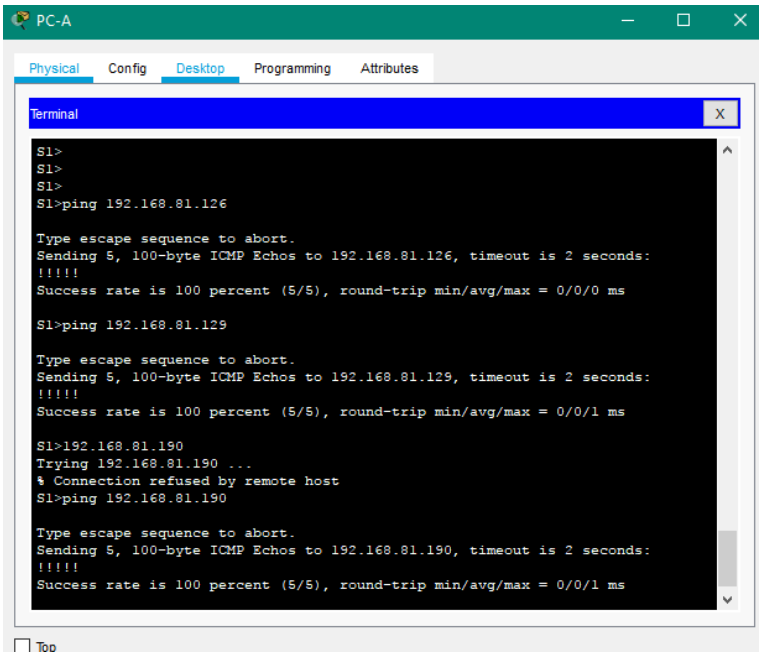
1.6 Pruebas de conectividad

Figura 14. Prueba de conectividad desde LAN 1- PC-A a todos los equipos



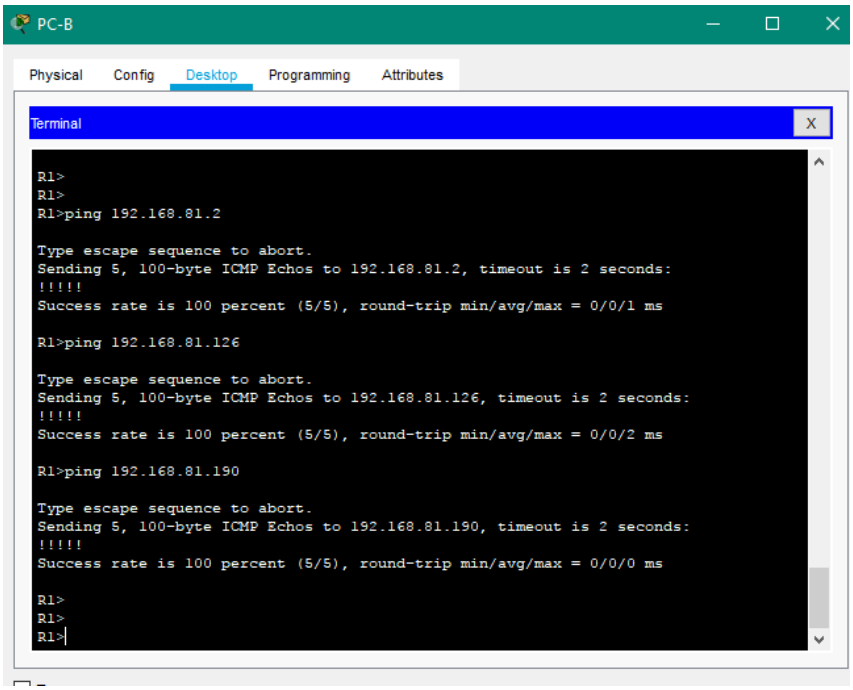
Fuente: Elaboración propia

Figura 15. Prueba de conectividad desde LAN 1- S1 a todos los equipos



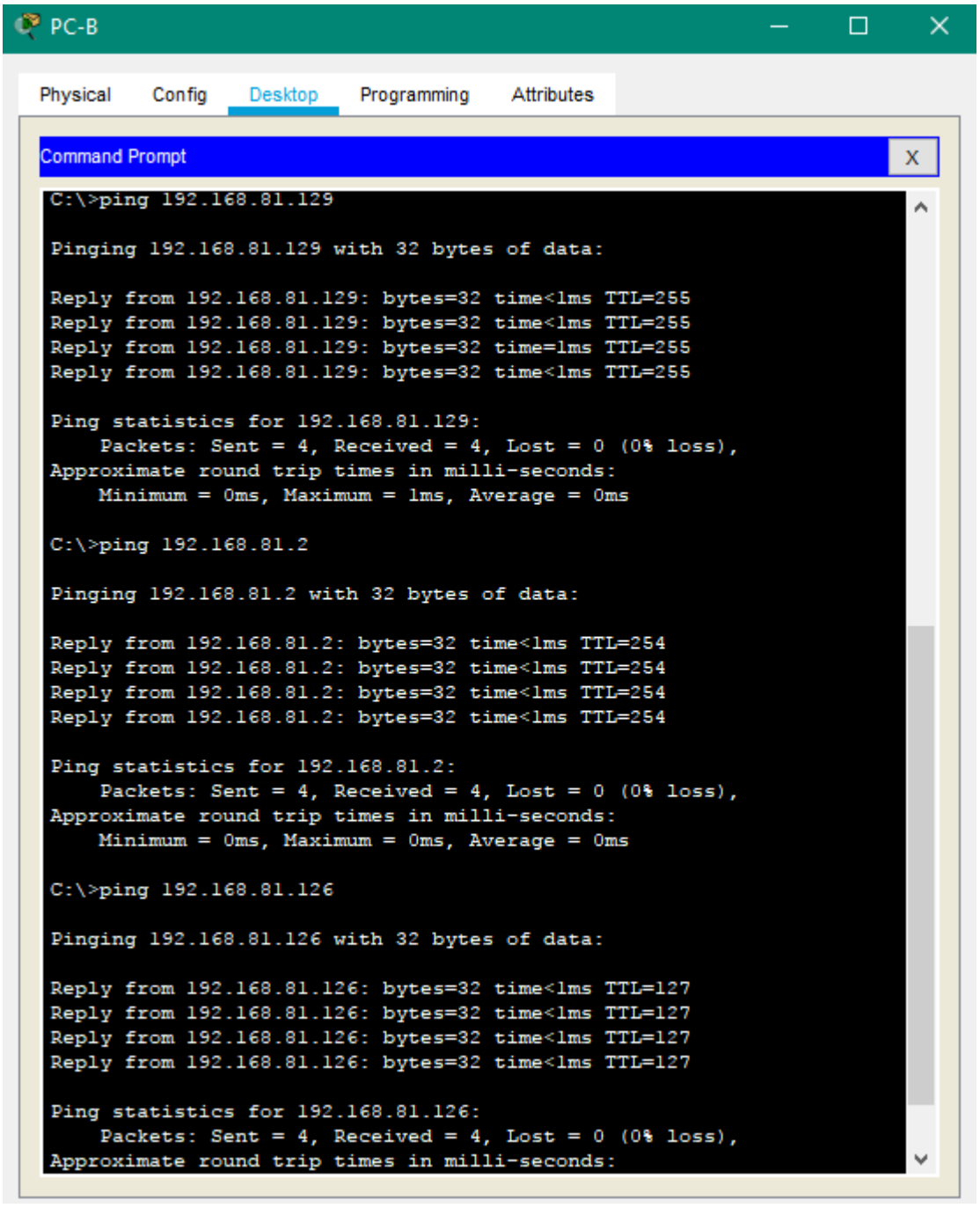
Fuente: Elaboración propia

Figura 16. Prueba de conectividad desde LAN 2- R1 a todos los equipos



Fuente: Elaboración propia

Figura 17. Prueba de conectividad desde LAN 2- PC-B a todos los equipos

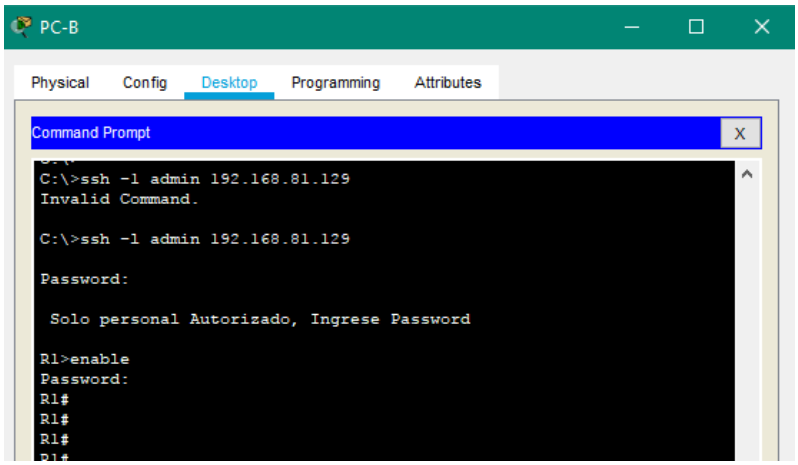


Fuente: Elaboración propia

1.7 Pruebas de acceso con SSH – Entrada de configuración por acceso remoto

Se realizó entrada de acceso remoto SSH desde el PC-B a configuración privilegiada del R1, la entrada será satisfactoria si las configuraciones anteriores al R1 se realizaron de forma correcta

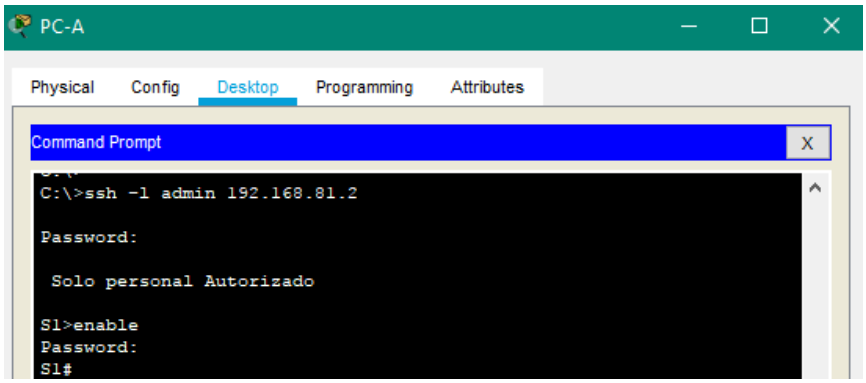
Figura 18. Verificación de entrada de acceso remoto desde PC-B a R1



Fuente: Elaboración propia

Se realizó entrada de acceso remoto SSH desde el PC-A a configuración privilegiada del S1, la entrada será satisfactoria si las configuraciones anteriores al S1 se realizaron de forma correcta

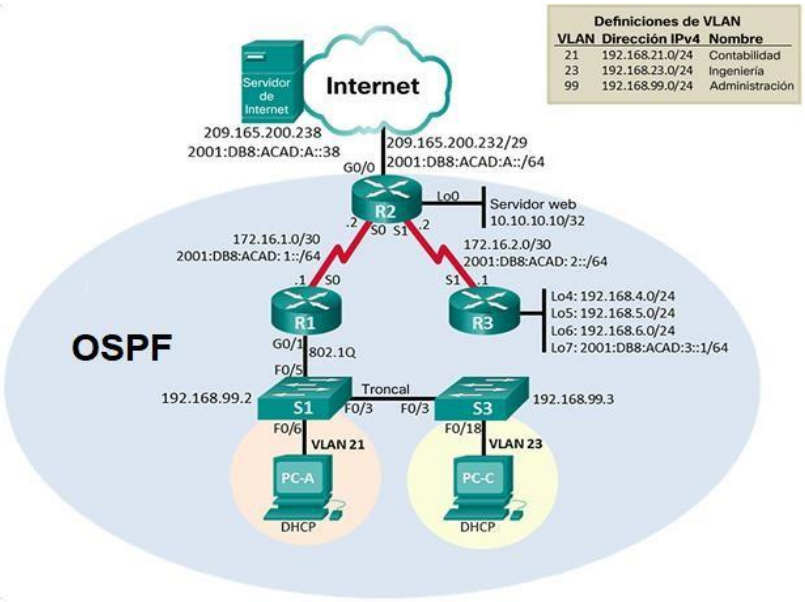
Figura 19. Verificación de entrada de acceso remoto desde PC-A a S1



Fuente: Elaboración propia

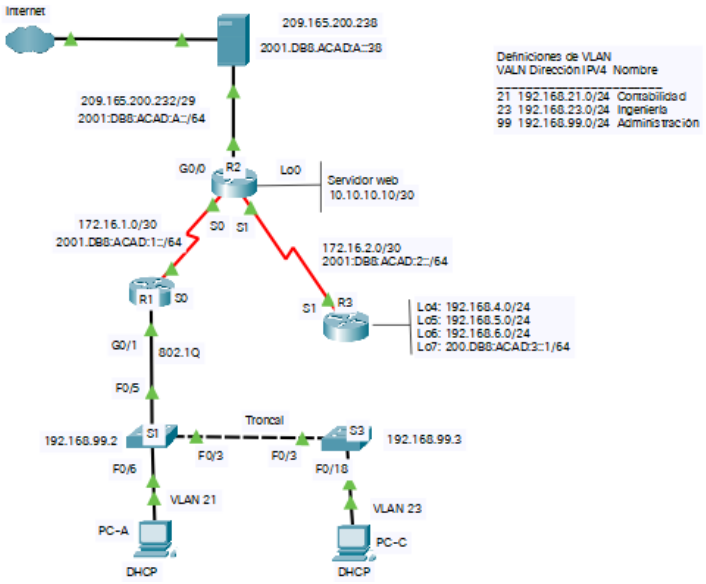
2. ESCENARIO 2

Figura 20. Escenario Propuesto 2



Fuente: Prueba de habilidades CISCO CCNA II

Figura 21. Simulación Escenario 2



Fuente: Elaboración propia

Parte 1: Inicializar dispositivos

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

Se eliminan las configuraciones de inicio y se vuelven a cargar los dispositivos.

2.1.1 Inicialización dispositivos R1 - R2- R3

Router >enable	Ingreso a modo privilegiado
Router#erase startup-config	borra el archivo de configuración de la NVRAM
Router#reload	vuelve a carga el dispositivo

2.1.2 Inicialización dispositivos S1 - S2.

Switch>enable	Ingreso a modo privilegiado
Switch#erase startup-config	borra el archivo de configuración de la NVRAM
Switch#delete vlan.dat	borra la información de Vlan
Router#reload	vuelve a carga el dispositivo

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

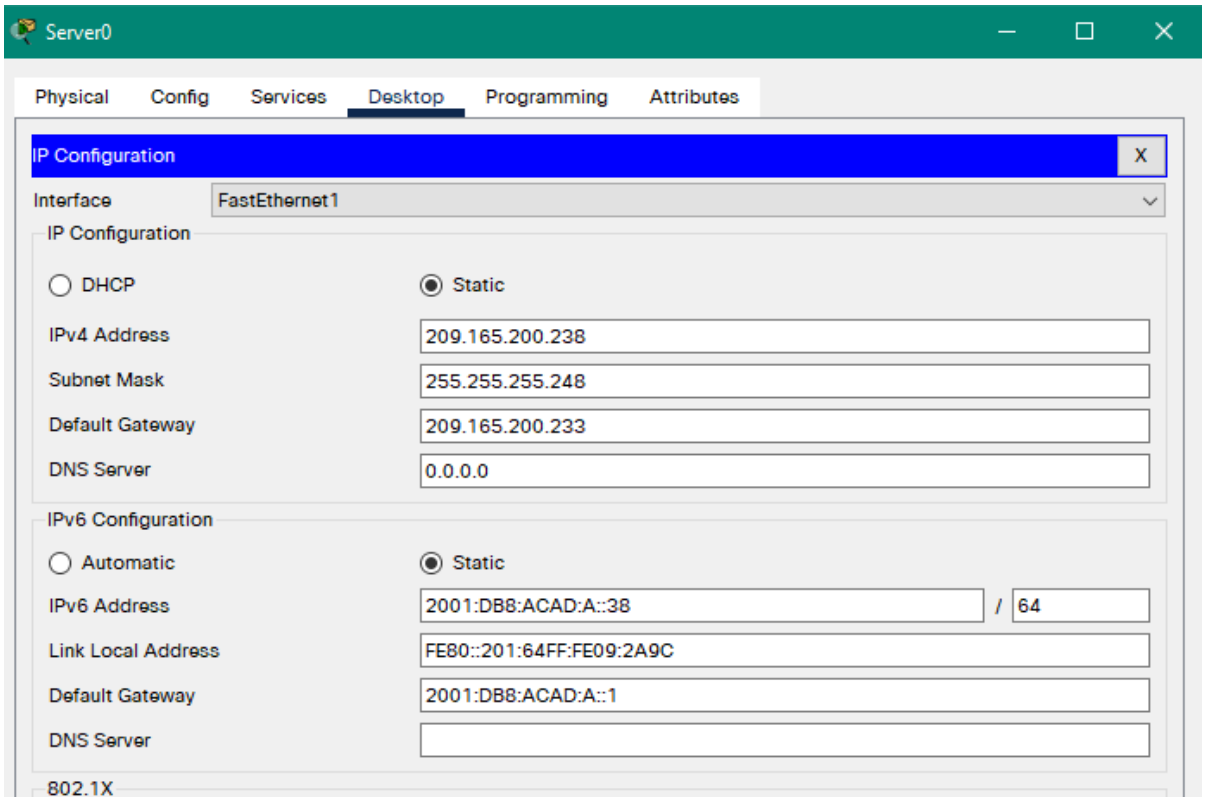
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, se consulta la topología):

Tabla 5. Configuración del Servidor

Elemento o tarea de configuración	**Especificación**
Dirección IPv4	209.165.200.238/29
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1/64

Fuente: Elaboración propia

Figura 22. Configuración del servidor



Fuente: Elaboración propia

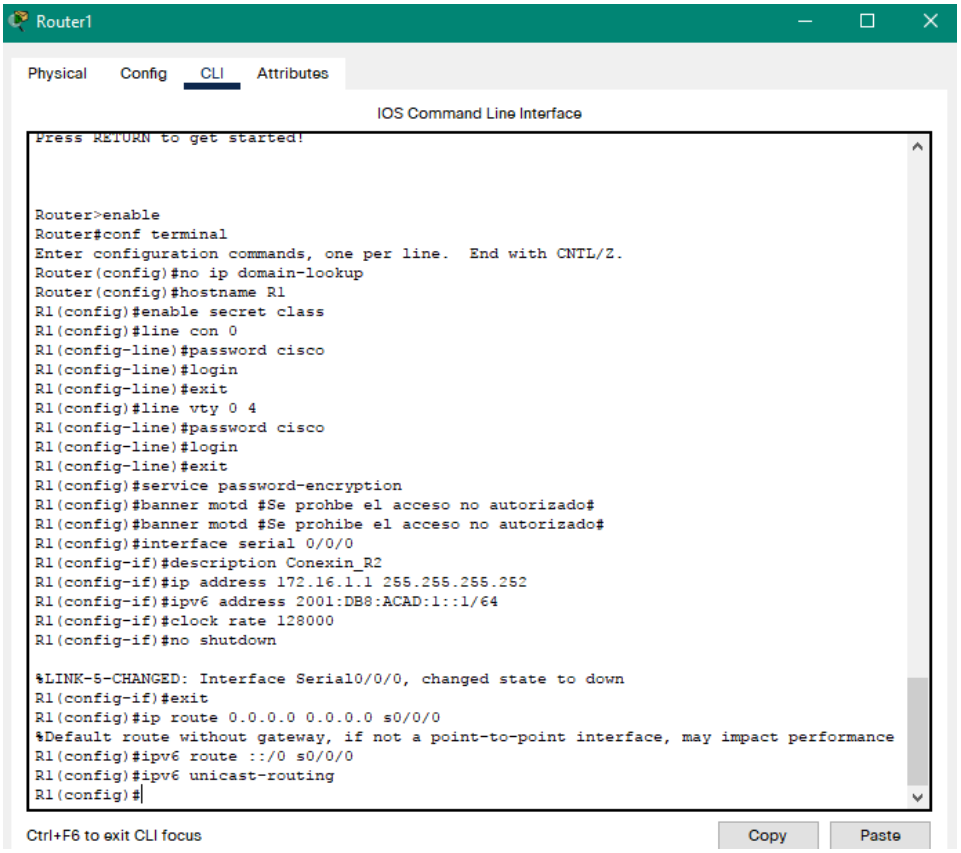
Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Router>enable	Ingreso a modo privilegiado
Router#conf terminal	Ingreso a modo de configuración
Router(config)#no ip domain-lookup	Desactivo la búsqueda DNS
Router(config)#hostname R1	Asigno nombre al router
R1(config)#enable secret class	Asigno contraseña cifrada para modo EXEC privilegiado
R1(config)#line con 0	Ingreso a configuración de la línea de consola
R1(config-line)#password cisco	Asigno contraseña en consola
R1(config-line)#login	Autenticación al iniciar la sesión
R1(config-line)#exit	Salgo del modo configuración de consola
R1(config)#line vty 0 4	Ingreso a configuración Telnet L4

R1(config-line)#password cisco	Asigno contraseña al Telnet
R1(config-line)#login	Autenticación al iniciar la sesión
R1(config-line)#exit	Salgo del modo configuración de line
R1(config)#service password-encryption	Cifrado a contraseñas
R1(config)#banner motd #Se prohibe el acceso no autorizado#	Mensaje al ingreso del dispositivo
R1(config)#interface serial 0/0/0	Ingreso a configuración de interfaz
R1(config-if)#description Conexión_R2	Descripción de la Subinterfaz
R1(config-if)#ip address 172.16.1.1 255.255.255.252	Asigno dirección ipv4/30
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64	Asigno dirección Ipv6/64
R1(config-if)#clock rate 128000	Establece frecuencia de reloj en 128000
R1(config-if)#no shutdown	Activa la Interfaz
R1(config-if)#exit	Sale de modo configuración interfaz
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0	Asigno ruta IPv4 predeterminada
R1(config)#ipv6 route ::/0 s0/0/0	Asigno ruta IPv6 predeterminada
R1(config)#ipv6 unicast-routing	Habilita router para IPv6

Figura 23. Configuración inicial R1



Fuente: Elaboración propia

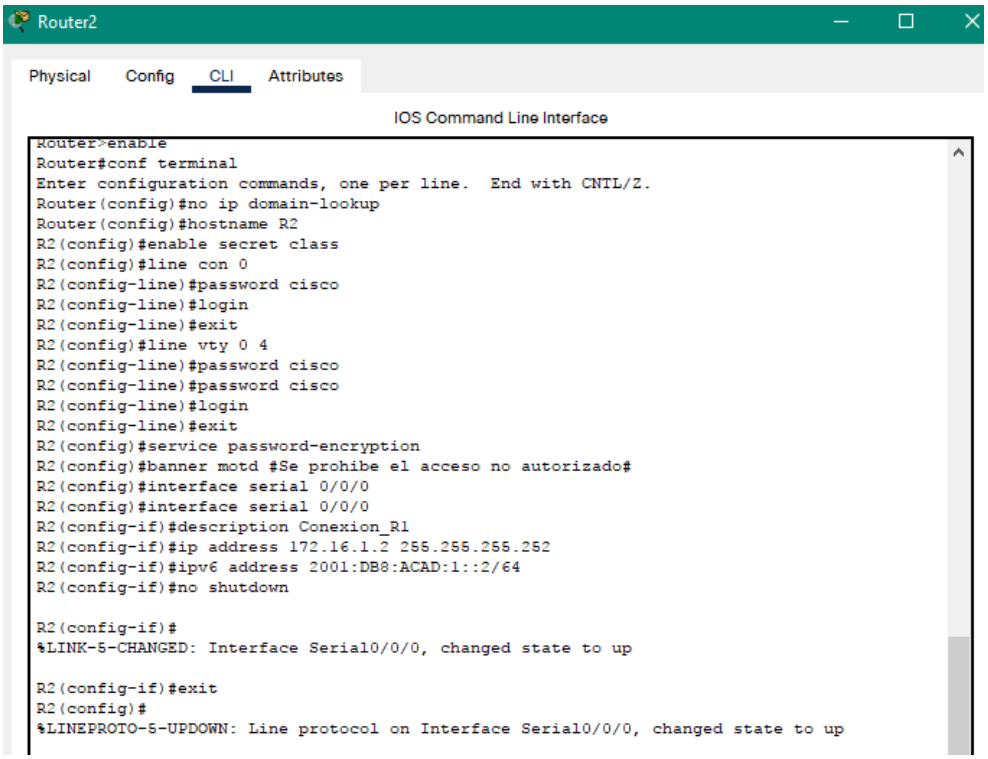
Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Router>enable	Ingreso a modo privilegiado
Router#conf terminal	Ingreso a modo de configuración
Router(config)#no ip domain-lookup	Desactivo la búsqueda DNS
Router(config)#hostname R2	Asigno nombre al router
R2(config)#enable secret class	Asigno contraseña cifrada para modo EXEC privilegiado
R2(config)#line con 0	Ingreso a configuración de la línea de consola
R2(config-line)#password cisco	Asigno contraseña en consola
R2(config-line)#login	Autenticación al iniciar la sesión
R2(config-line)#exit	Salgo del modo configuración de consola
R2(config)#line vty 0 4	Ingreso a configuración Telnet L14
R2(config-line)#password cisco	Asigno contraseña al Telnet
R2(config-line)#login	Autenticación al iniciar la sesión
R2(config-line)#exit	Salgo del modo configuración de line
R2(config)#service password-encryption	Cifrado a contraseñas
R2(config)#ip http server	servicio HTTP no soportado en simuladores
R2(config)#banner motd #Se prohibe el acceso no autorizado#	Mensaje al ingreso del dispositivo
R2(config)#interface serial 0/0/0	Ingreso a configuración de interfaz
R2(config-if)#description Conexion_R1	Descripción de la Subinterfaz
R2(config-if)#ip address 172.16.1.2 255.255.255.252	Asigno dirección ipv4/30
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64	Asigno dirección Ipv6/64
R2(config-if)#no shutdown	Activo la Interfaz
R2(config-if)#exit	Sale de modo configuración interfaz
R2(config)#interface serial 0/0/1	Ingreso interfaz a configurar
R2(config-if)#description Conexion_R3	Asigno descripción
R2(config-if)#ip address 172.16.2.2 255.255.255.252	Asigno dirección ipv4/30
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64	Asigno dirección Ipv6/64
R2(config-if)#clock rate 128000	Establezco frecuencia del reloj
R2(config-if)#no shutdown	Activo la Interfaz
R2(config-if)#exit	Sale de modo configuración interfaz
R2(config)#interface gigabitEthernet 0/0	Ingreso interfaz a configurar
R2(config-if)#description ConexiónS_Internet	Asigno descripción
R2(config-if)#ip address 209.165.200.233 255.255.255.248	Asigno dirección ipv4/29
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64	Asigno dirección Ipv6/64
R2(config-if)#no shutdown	Activo la Interfaz

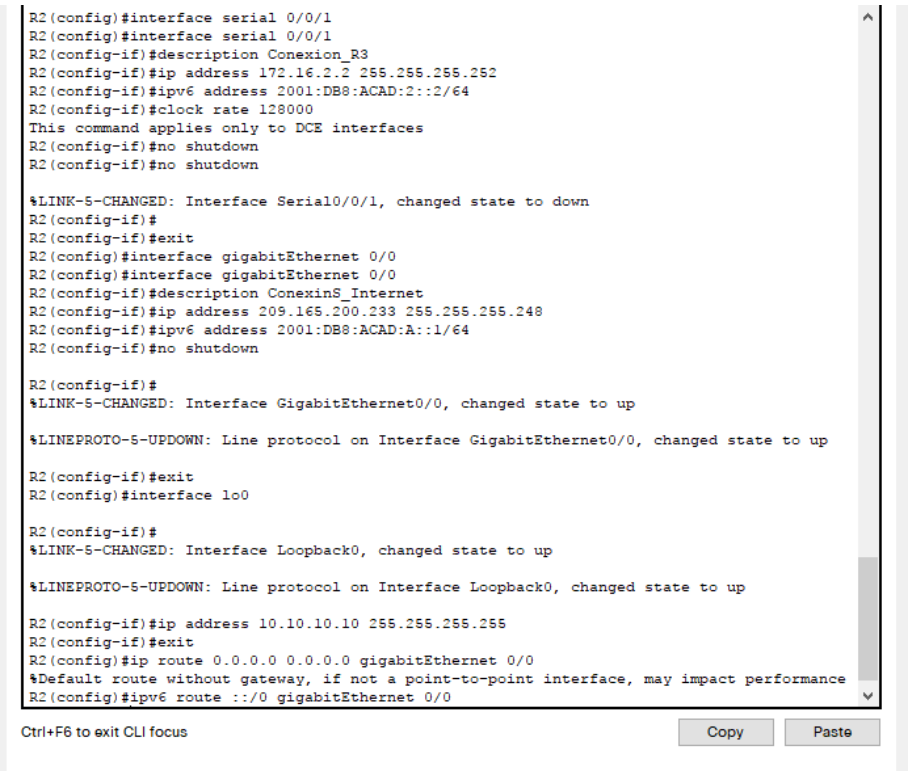
R2(config-if)#exit Sale de modo configuración interfaz
R2(config)#interface lo0 Ingreso a Interfaz loopback 0
R2(config-if)#ip address 10.10.10.10 255.255.255.255 Asigno dirección ipv4/32
R2(config-if)#exit Sale de modo configuración interfaz
R2(config)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/0 Asigno ruta predeterminada IPV4
R2(config)#ipv6 route ::/0 gigabitEthernet 0/0 Asigno ruta predeterminada IPV6

Figura 24. Configuración inicial R2



Fuente: Elaboración propia

Figura 25. Continuación de Configuración inicial R2



Fuente: Elaboración propia

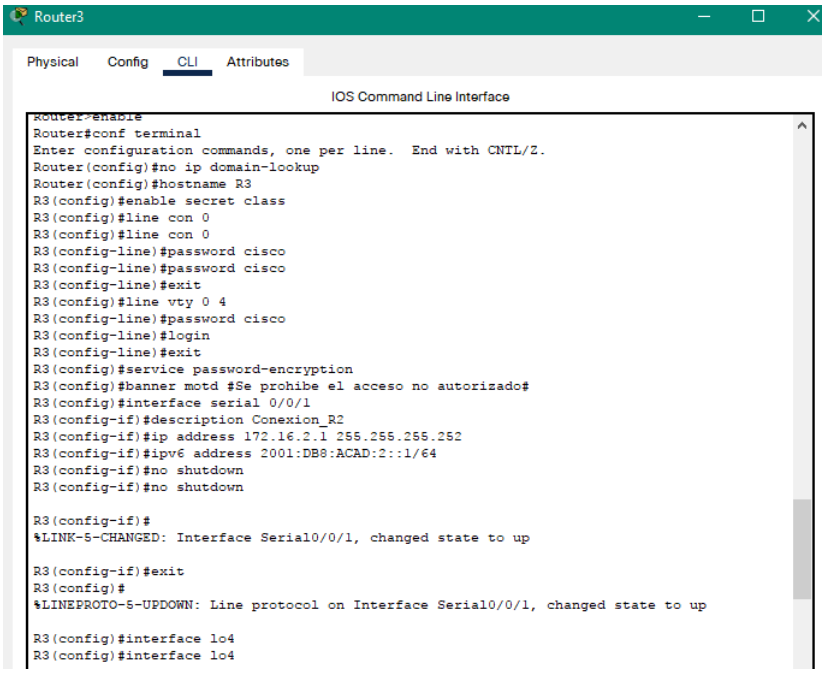
Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Router>enable	Ingreso a modo privilegiado
Router#conf terminal	Ingreso a modo de configuración
Router(config)#no ip domain-lookup	Desactivo la búsqueda DNS
Router(config)#hostname R3	Asigno nombre al router
R3(config)#enable secret class	Asigno contraseña cifrada para modo EXEC privilegiado
R3(config)#line con 0	Ingreso a configuración de la línea de consola
R3(config-line)#password cisco	Asigno contraseña en consola
R3(config-line)#login	Autenticación al iniciar la sesión
R3(config-line)#exit	Salgo del modo configuración de consola
R3(config)#line vty 0 4	Ingreso a configuración Telnet L4
R3(config-line)#password cisco	Asigno contraseña al Telnet
R3(config-line)#login	Autenticación al iniciar la sesión

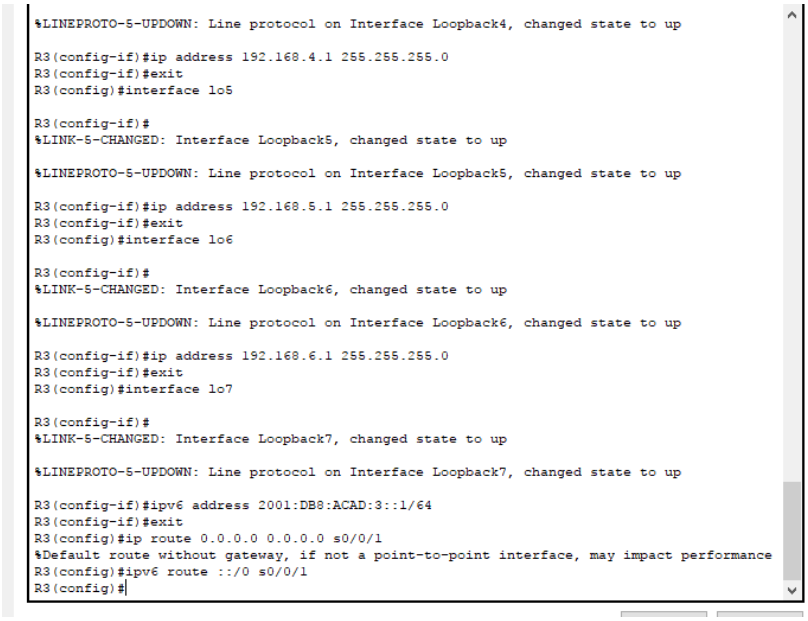
R3(config-line)#exit Salgo del modo configuración de line
R3(config)#service password-encryption Cifrado a contraseñas
R3(config)#banner motd #Se prohibe el acceso no autorizado# Mensaje al ingreso del dispositivo
R3(config)#interface serial 0/0/1 Ingreso a configuración de interfaz
R3(config-if)#description Conexion_R2 Descripción de la Subinterfaz
R3(config-if)#ip address 172.16.2.1 255.255.255.252 Asigno dirección ipv4/30
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 Asigno dirección Ipv6/64
R3(config-if)#no shutdown Activo la Interfaz
R3(config-if)#exit Sale de modo configuración interfaz
R3(config)#interface lo4 Ingreso a Interfaz loopback 4
R3(config-if)#ip address 192.168.4.1 255.255.255.0 Asigno dirección ipv4/24
R3(config-if)#exit Sale de modo configuración interfaz
R3(config)#interface lo5 Ingreso a Interfaz loopback 5
R3(config-if)#ip address 192.168.5.1 255.255.255.0 Asigno dirección ipv4/24
R3(config-if)#exit Sale de modo configuración interfaz
R3(config)#interface lo6 Ingreso a Interfaz loopback 6
R3(config-if)#ip address 192.168.6.1 255.255.255.0 Asigno dirección ipv4/24
R3(config-if)#exit Sale de modo configuración interfaz
R3(config)#interface lo7 Ingreso a Interfaz loopback 7
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 Asigno dirección ipv6/64
R3(config-if)#exit Sale de modo configuración interfaz
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 Asigno ruta predeterminada IPV4
R3(config)#ipv6 route ::/0 s0/0/1 Asigno ruta predeterminada IPV6

Figura 26. Configuración inicial R3



Fuente: Elaboración propia

Figura 27. Continuación configuración inicial R3



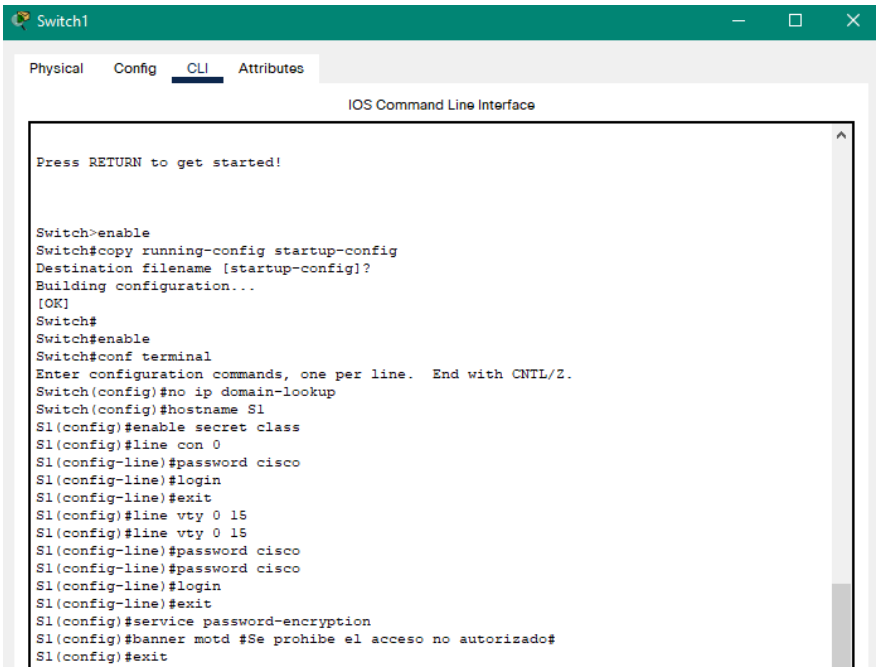
Fuente: Elaboración propia

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Switch>enable	Ingreso a modo privilegiado
Switch#conf terminal	Ingreso a modo de configuración
Switch(config)#no ip domain-lookup	Desactivo la búsqueda DNS
Switch(config)#hostname S1	Asigno nombre al router
S1(config)#enable secret class	Asigno contraseña cifrada para modo EXEC privilegiado
S1(config)#line con 0	Ingreso a configuración de la línea de consola
S1(config-line)#password cisco	Asigno contraseña en consola
S1(config-line)#login	Autenticación al iniciar la sesión
S1(config-line)#exit	Salgo del modo configuración de consola
S1(config)#line vty 0 15	Ingreso a configuración Telnet L15
S1(config-line)#password cisco	Asigno contraseña a Telnet
S1(config-line)#login	Autenticación al iniciar la sesión
S1(config-line)#exit	Salgo del modo configuración de line
S1(config)#service password-encryption	Cifrado a contraseñas
S1(config)#banner motd #Se prohibe el acceso no autorizado#	Mensaje al ingreso del dispositivo

Figura 28. Configuración inicial S1



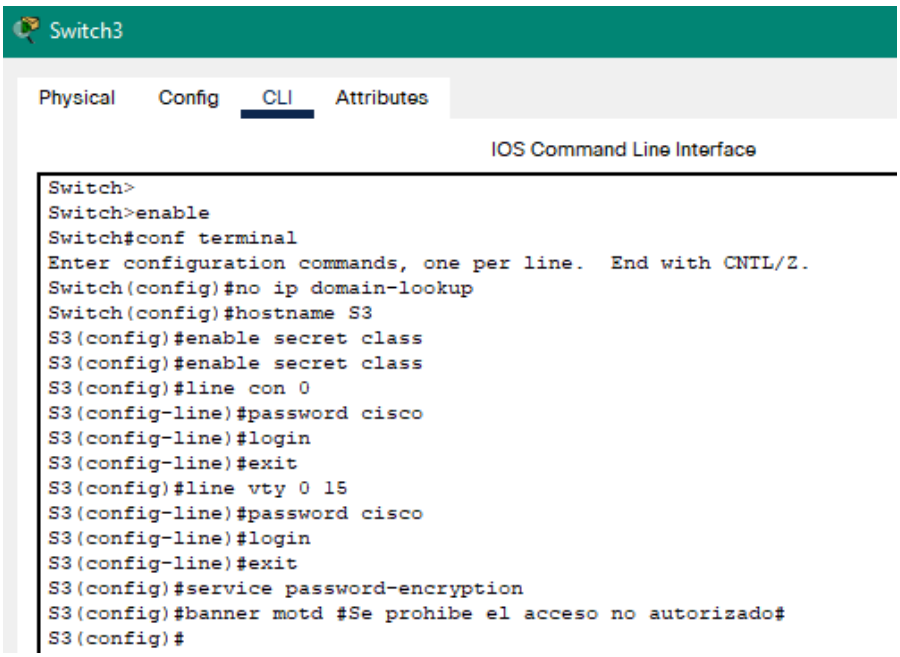
Fuente: Elaboración propia

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Switch>enable	Ingreso a modo privilegiado
Switch#conf terminal	Ingreso a modo de configuración
Switch(config)#no ip domain-lookup	Desactivo la búsqueda DNS
Switch(config)#hostname S3	Asigno nombre al router
S3(config)#enable secret class	Asigno contraseña cifrada para modo EXEC privilegiado
S3(config)#line con 0	Ingreso a configuración de la línea de consola
S3(config-line)#password cisco	Asigno contraseña en consola
S3(config-line)#login	Autenticación al iniciar la sesión
S3(config-line)#exit	Salgo del modo configuración de consola
S3(config)#line vty 0 15	Ingreso a configuración Telnet L15
S3(config-line)#password cisco	Asigno contraseña a Telnet
S3(config-line)#login	Autenticación al iniciar la sesión
S3(config-line)#exit	Salgo del modo configuración de line
S3(config)#service password-encryption	Cifrado a contraseñas
S3(config)#banner motd #Se prohibe el acceso no autorizado#	Mensaje al ingreso del dispositivo

Figura 29. Configuración inicial S3



Fuente: Elaboración propia

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.

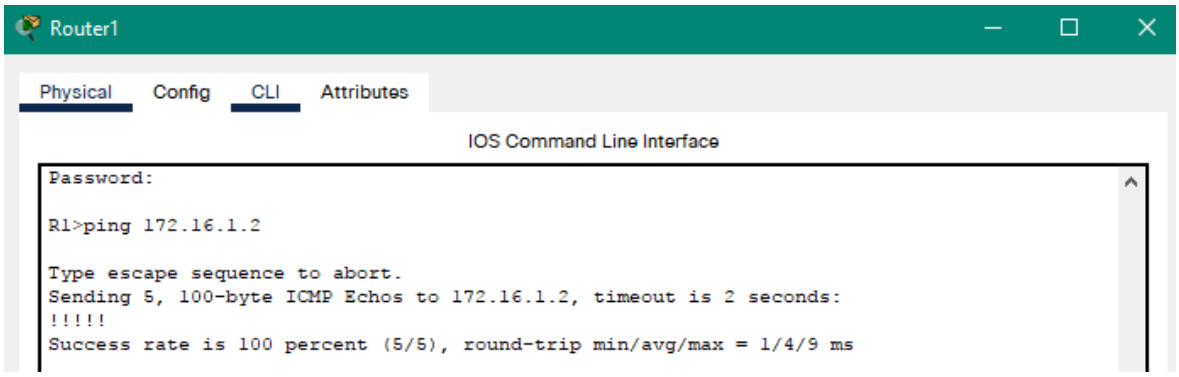
Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 6. Verificación de conectividad con cada dispositivo

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

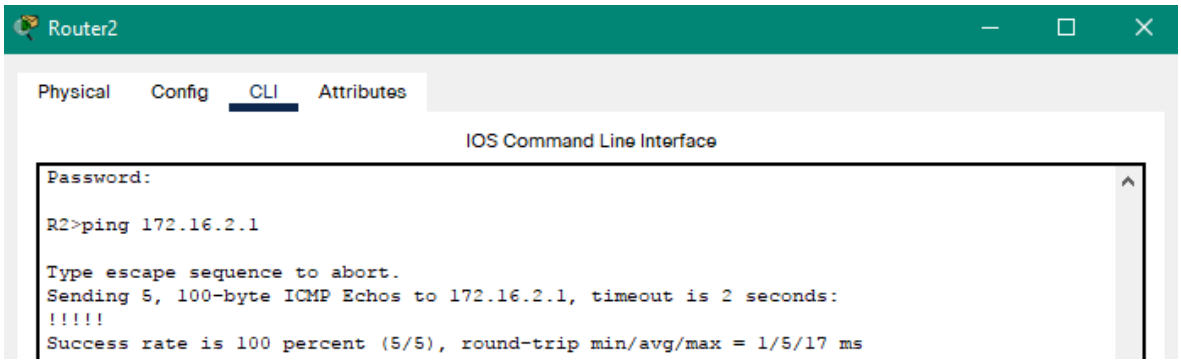
Fuente: Elaboración propia

Figura 30. Conectividad R1 a R2



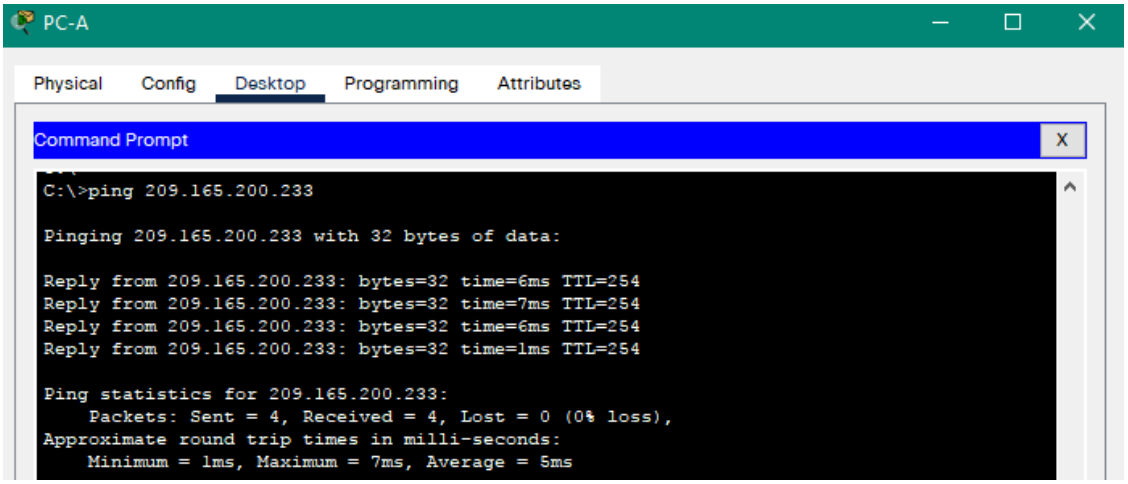
Fuente: Elaboración propia

Figura 31. Conectividad R2 a R3



Fuente: Elaboración propia

Figura 32. Conectividad PC a Gateway predeterminado



Fuente: Elaboración propia

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

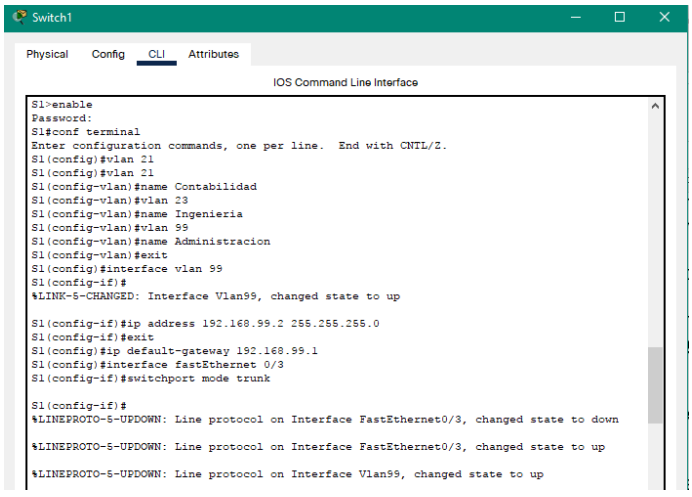
Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

S1#conf terminal	Ingreso a modo de configuración
S1(config)#vlan 21	Ingreso a vlan 21
S1(config-vlan)#name Contabilidad	Asigno nombre a vlan 21
S1(config-vlan)#vlan 23	Ingreso a vlan 23
S1(config-vlan)#name Ingenieria	Asigno nombre a vlan 23
S1(config-vlan)#vlan 99	Ingreso a vlan 21

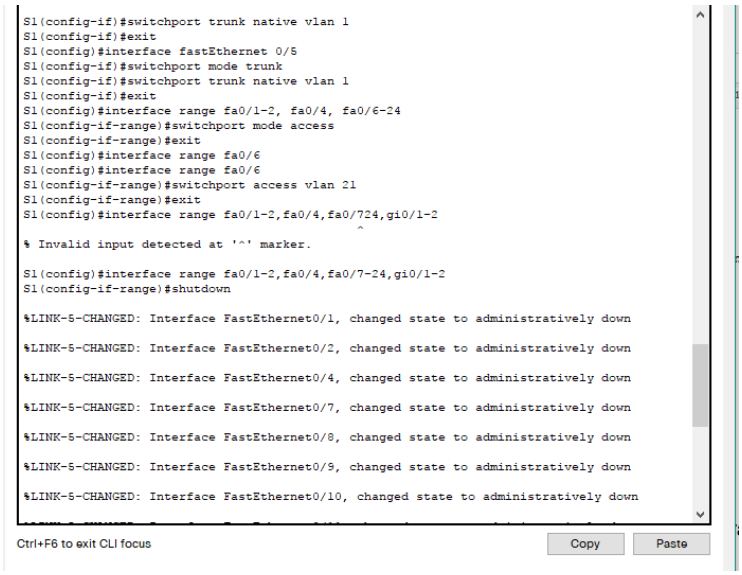
S1(config-vlan)#name Administracion	Asigno nombre a vlan 23
S1(config-vlan)#exit	Salgo de configuración vlans
S1(config)#interface vlan 99	ingreso a configuración interfaz
S1(config-if)#ip address 192.168.99.2 255.255.255.0	Asigno IPV4/24
S1(config-if)#exit	Sale de modo configuración interfaz
S1(config)#ip default-gateway 192.168.99.1	Asigno gateway predeterminado
S1(config)#interface fastEthernet 0/3	Ingreso a configuración interfaz
S1(config-if)#switchport mode trunk	Forza el enlace troncal en la interfaz
S1(config-if)#switchport trunk native vlan 1	Especifica vlan nativa
S1(config-if)#exit	Sale de modo configuración interfaz
S1(config)#interface fastEthernet 0/5	Ingreso a configuración interfaz
S1(config-if)#switchport mode trunk	Forza el enlace troncal en la interfaz
S1(config-if)#switchport trunk native vlan 1	Especifica vlan nativa
S1(config-if)#exit	Sale de modo configuración interfaz
S1(config)#interface range fa0/1-2, fa0/4, fa0/6-24	Ingreso a interface de configuración especificando el rango
S1(config-if-range)#switchport mode access	Establezco interfaces como puertos de acceso
S1(config-if-range)#exit	Sale de modo configuración interfaz
S1(config)#interface range fa0/6	Ingreso a interface de configuración
S1(config-if-range)#switchport access vlan 21	Asigno F0/6 a la VLAN 21
S1(config-if-range)#exit	
S1(config)#interface range fa0/1-2,fa0/4,fa0/7-24,gi0/1-2	Ingreso a interface de configuración especificando el rango
S1(config-if-range)#shutdown	Apago los puertos sin usar
S1(config-if-range)#exit	Salgo de modo configuración de interfaz

Figura 33. Configuración S1 de seguridad, las VLAN y el routing entre VLAN



Fuente: Elaboración propia

Figura 34. C. configuración S1 de seguridad, las VLAN y el routing entre VLAN



Fuente: Elaboración propia

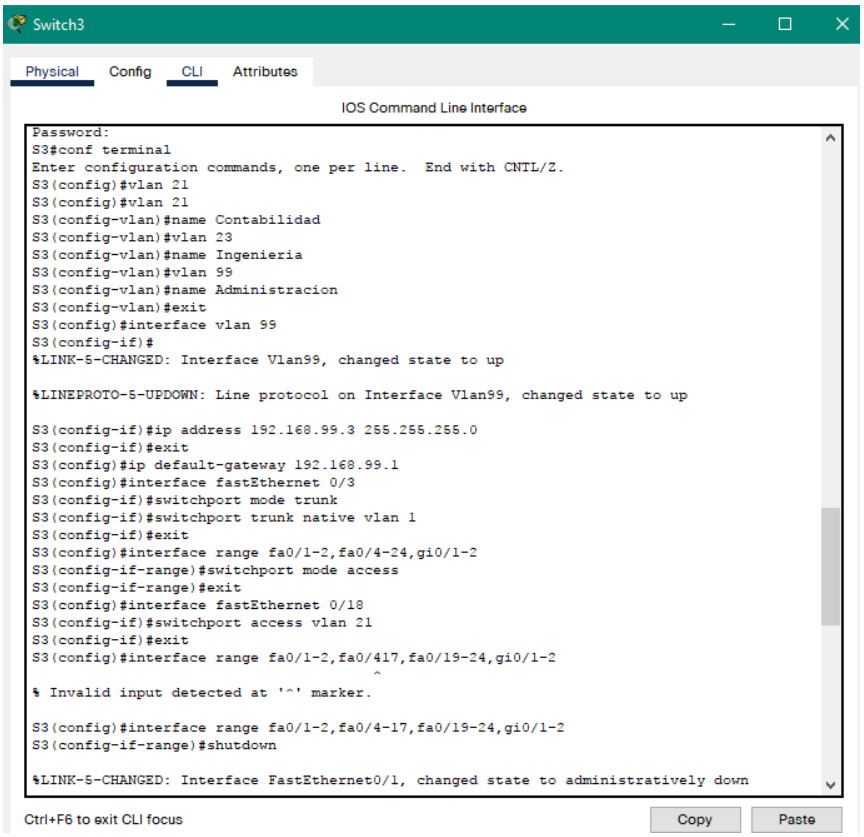
Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

S3#conf terminal	Ingreso a modo de configuración
S3(config)#vlan 21	Ingreso a vlan 21
S3(config-vlan)#name Contabilidad	Asigno nombre a vlan 21
S3(config-vlan)#vlan 23	Ingreso a vlan 23
S3(config-vlan)#name Ingenieria	Asigno nombre a vlan 23
S3(config-vlan)#vlan 99	Ingreso a vlan 21
S3(config-vlan)#name Administracion	Asigno nombre a vlan 23
S3(config-vlan)#exit	Salgo de configuración vlans
S3(config)#interface vlan 99	ingreso a configuración interfaz
S3(config-if)#ip address 192.168.99.3 255.255.255.0	Asigno IPV4/24
S3(config-if)#exit	Sale de modo configuración interfaz
S3(config)#ip default-gateway 192.168.99.1	Asigno gateway predeterminado
S3(config)#interface fastEthernet 0/3	Ingreso a configuración interfaz
S3(config-if)#switchport mode trunk	Forza el enlace troncal en la interfaz
S3(config-if)#switchport trunk native vlan 1	Especifica vlan nativa
S3(config-if)#exit	Sale de modo configuración interfaz
S3(config)#interface range fa0/1-2,fa0/4-24,gi0/1-2	Ingreso a interface de configuración especificando el rango
S3(config-if-range)#switchport mode access	Establezco interfaces como puertos de acceso

S3(config-if-range)#exit Sale de modo configuración interfaz
S3(config)#interface fastEthernet 0/18 Ingreso a interface de configuración
S3(config-if-range)#switchport access vlan 21 Asigno F0/18 a la VLAN 21
S3(config-if-range)#exit
S3(config)#interface range fa0/1-2,fa0/4-17,fa0/19-24,gi0/1-2 Ingreso a interface de configuración especificando el rango
S3(config-if-range)#shutdown Apago los puertos sin usar
S3(config-if-range)#exit Salgo de modo configuración de interfaz

Figura 35. Configuración S3 de seguridad, las VLAN y el routing entre VLAN



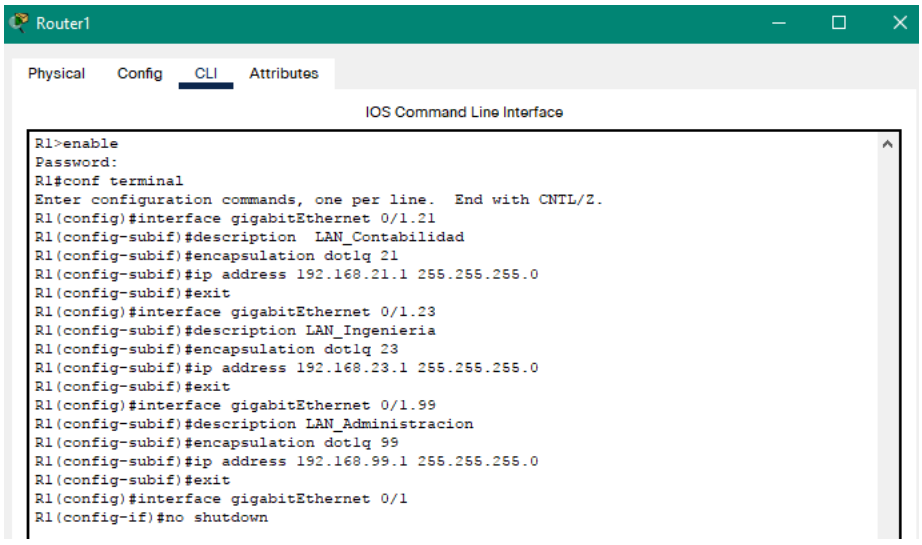
Fuente: Elaboración propia

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

R1(config)#interface gigabitEthernet 0/1.21 Ingreso subinterfaz a configurar
R1(config-subif)#description LAN_Contabilidad Asigno descripción
R1(config-subif)#encapsulation dot1q 21 habilitar 802.1Q Permite enlace troncal
R1(config-subif)#ip address 192.168.21.1 255.255.255.0 Asignar la primera dirección IPV4/24 disponible a esta interfaz
R1(config-subif)#exit sale de modo configuración
R1(config)#interface gigabitEthernet 0/1.23 Ingreso subinterfaz a configurar
R1(config-subif)#description LAN_Ingenieria Asigno descripción
R1(config-subif)#encapsulation dot1q 23 habilitar interfaz 802.1Q Permite enlace troncal
R1(config-subif)#ip address 192.168.23.1 255.255.255.0 Asignar la primera dirección IPV4/24 disponible a esta interfaz
R1(config-subif)#exit Sale de modo configuración
R1(config)#interface gigabitEthernet 0/1.99 Ingreso subinterfaz a configurar
R1(config-subif)#description LAN_Administracion Asigno descripción
R1(config-subif)#encapsulation dot1q 99 habilitar interfaz 802.1Q Permite enlace troncal
R1(config-subif)#ip address 192.168.99.1 255.255.255.0 Asignar la primera dirección IPV4/24 disponible a esta interfaz
R1(config-subif)#exit Sale de modo configuración
R1(config)#interface gigabitEthernet 0/1 Ingreso a interfaz a configurar
R1(config-if)#no shutdown Activo la Interfaz
R1(config-if)#exit Salgo de modo configuración

Figura 36. Configuración R1 de seguridad, las VLAN y el routing entre VLAN



Fuente: Elaboración propia

Paso 4: Verificar la conectividad de la red

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

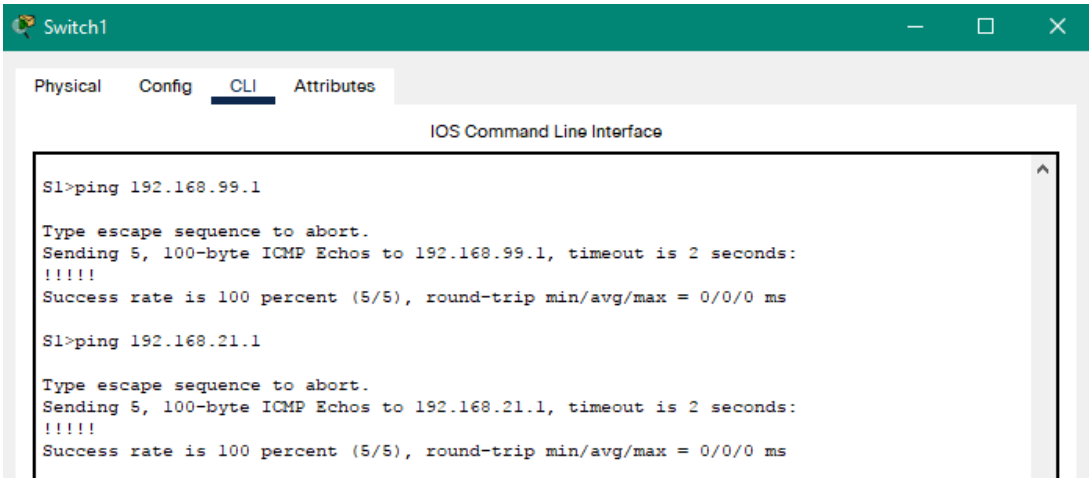
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 7. Verificación de conectividad con cada dispositivo

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

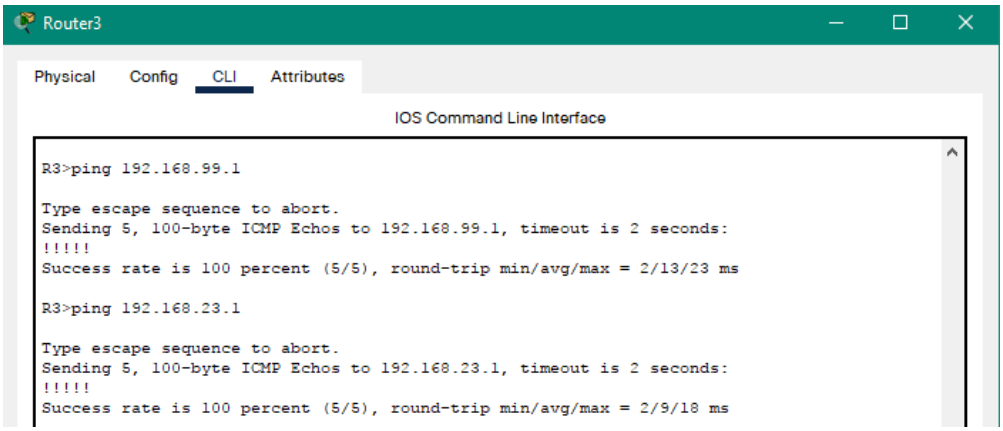
Fuente: Elaboración propia

Figura 37. Prueba de Conectividad de S1 a R1 y de S1 a R1



Fuente: Elaboración propia

Figura 38. Prueba de Conectividad de S3 a R1 y de S3 a R1



Fuente: Elaboración propia

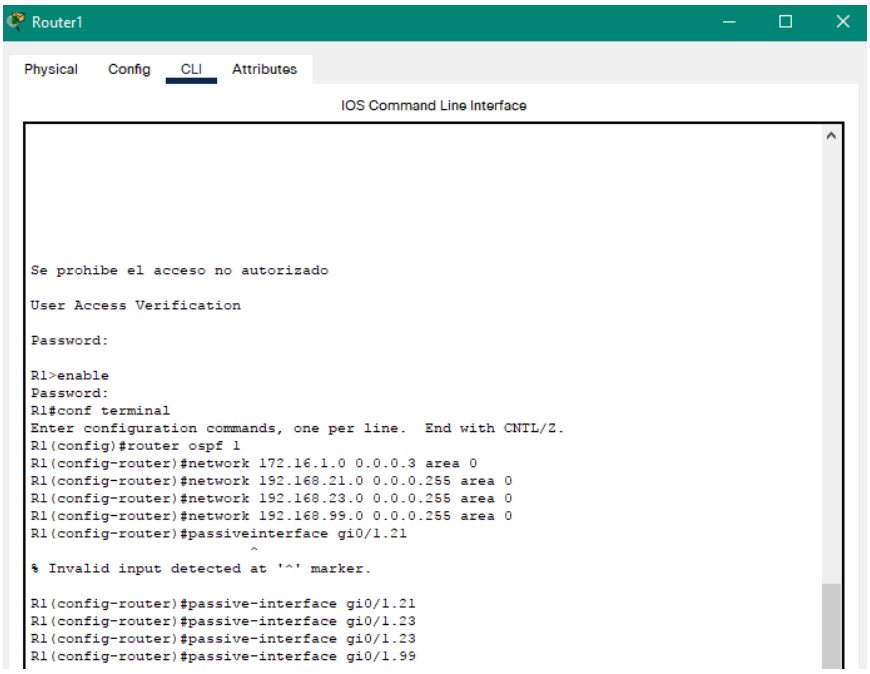
Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

R1#conf terminal	Ingreso a modo configuración
R1(config)#router ospf 1	Configurar OSPF área 0
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0	Anuncio red conectada directamente al área 0
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0	Anuncio red conectada directamente al área 0
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0	Anuncio red conectada directamente al área 0
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0	Anuncio red conectada directamente al área 0
R1(config-router)#passive-interface gi0/1.21	Establece interfaz LAN como pasiva
R1(config-router)#passive-interface gi0/1.23	Establece interfaz LAN como pasiva
R1(config-router)#passive-interface gi0/1.99	Establece interfaz LAN como pasiva
R2(config-router)#no auto-summary	Desactivo la sumarización automática, no aplica en OSPF

Figura 39. Configuración OSPF en el R1



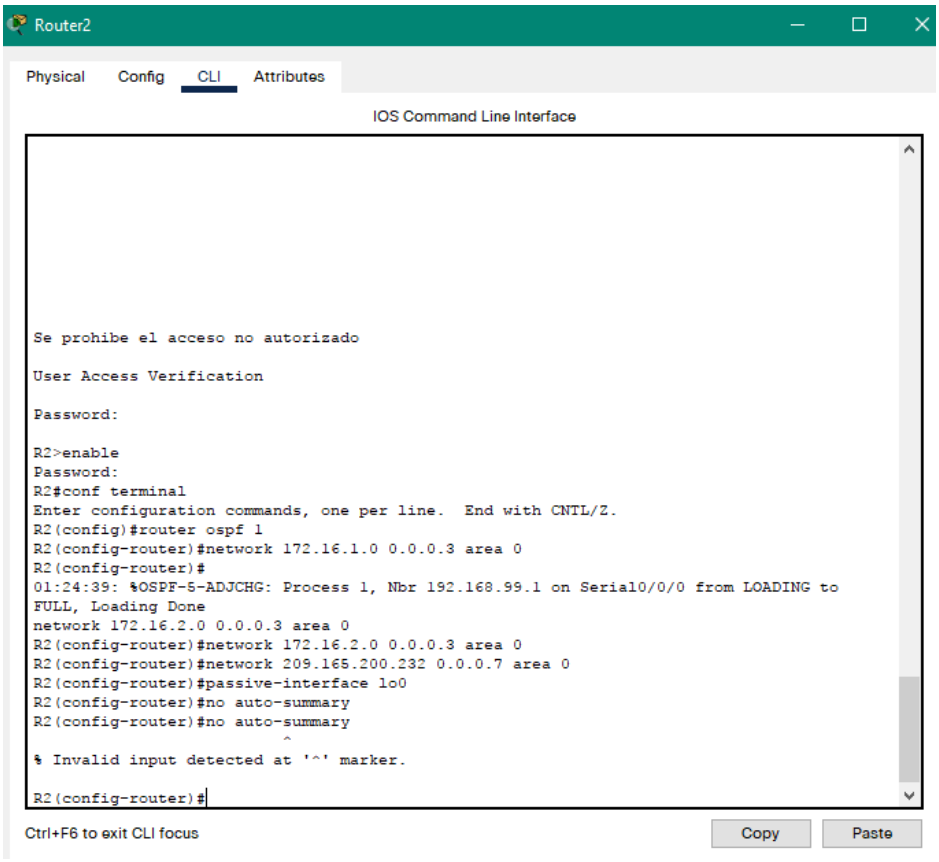
Fuente: Elaboración propia

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

R2#conf terminal	Ingreso a modo configuración
R2(config)#router ospf 1	Configurar OSPF área 0
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0	Anuncio red conectada directamente al área 0
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0	Anuncio red conectada directamente al área 0
R2(config-router)#network 209.165.200.232 0.0.0.7 area 0	Anuncio red conectada directamente al área 0
R2(config-router)#passive-interface lo0	Establecer la interfaz LAN (loopback) como pasiva
R2(config-router)#no auto-summary	Desactivo la sumarización automática, no aplica en OSPF

Figura 40. Configuración OSPF en el R2



Fuente: Elaboración propia

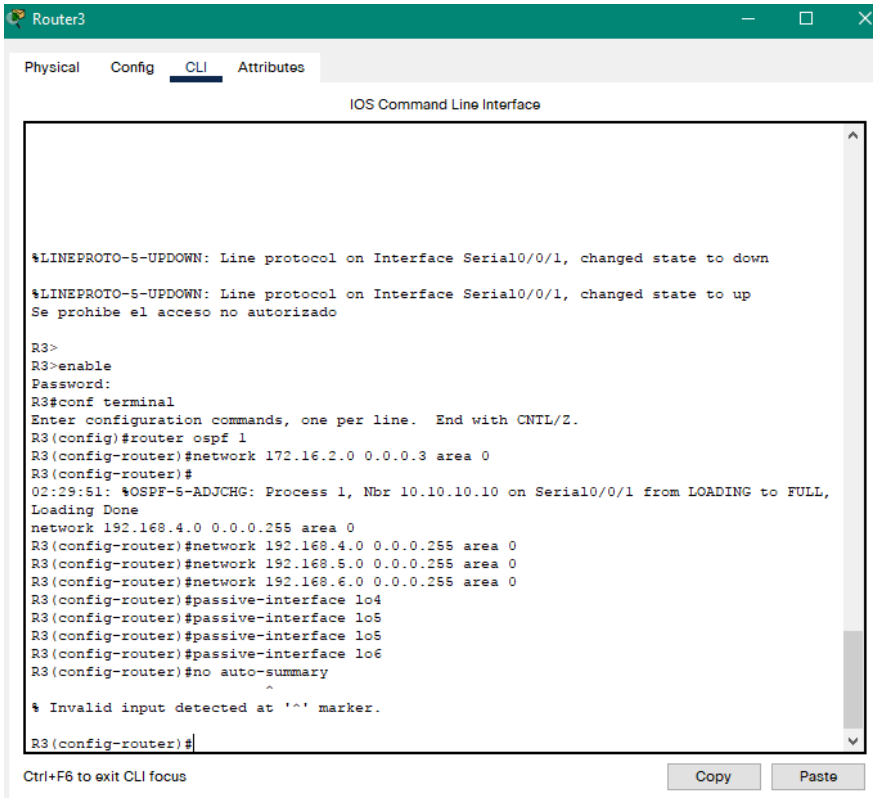
Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

R3#conf terminal Ingreso a modo configuración
R3(config)#router ospf 1 Configurar OSPF área 0
R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 Anuncio red conectada directamente al área 0
R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 Anuncio red conectada directamente al área 0
R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 Anuncio red conectada directamente al área 0
R3(config-router)#network 192.168.6.0 0.0.0.255 area 0 Anuncio red conectada directamente al área 0

R3(config-router)#passive-interface lo4 Establece la interfaz de LAN IPv4 (Loopback) como pasiva
R3(config-router)#passive-interface lo5 Establece la interfaz de LAN IPv4 (Loopback) como pasiva
R3(config-router)#passive-interface lo6 Establece la interfaz de LAN IPv4 (Loopback) como pasiva
R2(config-router)#no auto-summary Desactivo la sumarización automática, no aplica en OSPF

Figura 41. Configuración OSPFv3 en el R3



Fuente: Elaboración propia

Paso 4: Verificar la información de OSPF

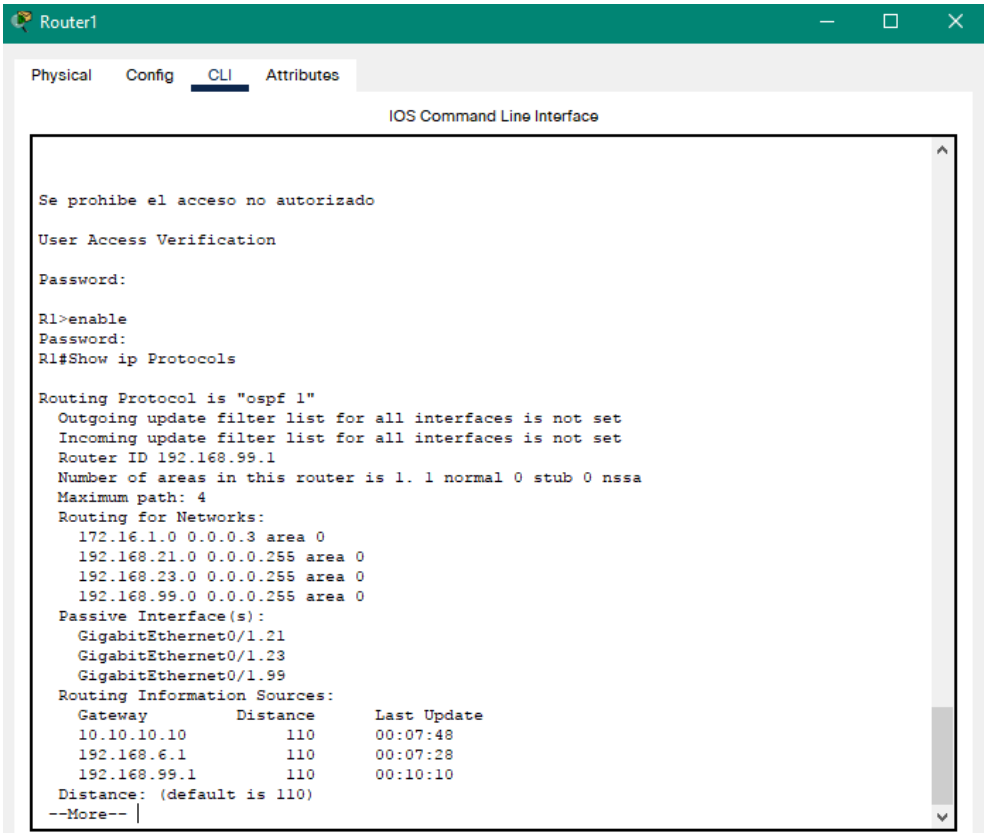
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 8. Verificación funcionamiento correcto de OSPF

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	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 ip ospf database

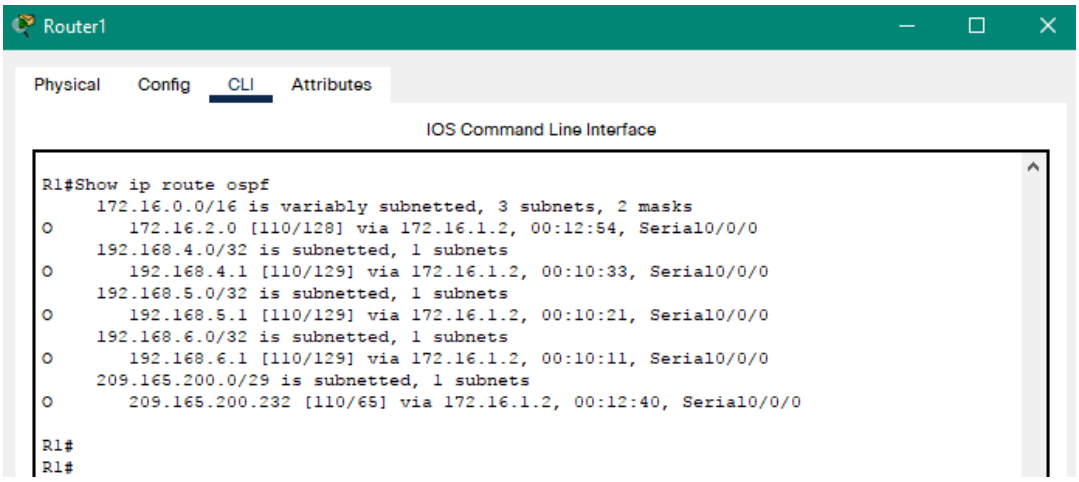
Fuente: Elaboración propia

Figura 42. Verificación de la información de OSPF R1



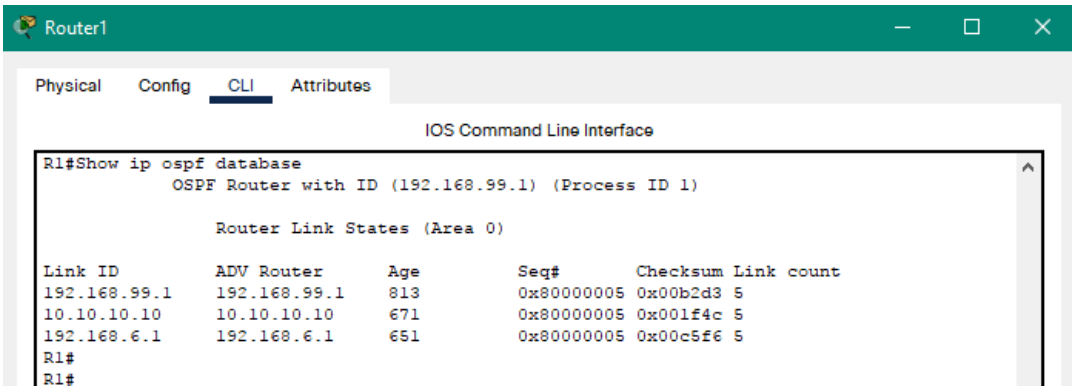
Fuente: Elaboración propia

Figura 43. Rutas OSPF



Fuente: Elaboración propia

Figura 44. Sección de OSPF de la configuración en ejecución



Fuente: Elaboración propia

Parte 5: Implementar DHCP y NAT para IPv4

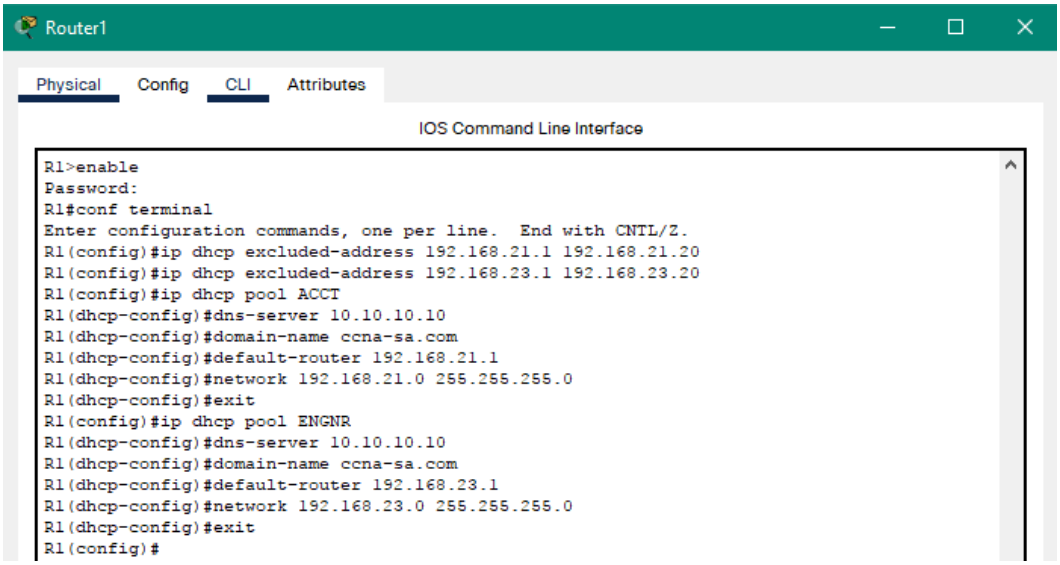
Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

R1#configure terminal Ingreso a modo configuración
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20 Reserva las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas

R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20 Reserva las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas
R1(config)#ip dhcp pool ACCT Crear un pool de DHCP para la VLAN 21
R1(dhcp-config)#dns-server 10.10.10.10 Asigno Servidor DNS
R1(dhcp-config)#domain-name ccna-sa.com Asigno nombre de dominio
R1(dhcp-config)#default-router 192.168.21.1 Establezco el Gateway predeterminado
R1(dhcp-config)#network 192.168.21.0 255.255.255.0 Asigno IPV4 en dhcp
R1(dhcp-config)#exit Salgo de modo configuración dhcp pool
R1(config)#ip dhcp pool ENGNR Crear un pool de DHCP para la VLAN 23 Asigno Servidor DNS
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com Asigno nombre de dominio
R1(dhcp-config)#default-router 192.168.23.1 Establezco el Gateway predeterminado
R1(dhcp-config)#network 192.168.23.0 255.255.255.0 Asigno IPV4 en dhcp
R1(dhcp-config)#exit Salgo de modo configuración dhcp pool

Figura 45. Configuración R1 como servidor de DHCP para las VLAN 21 y 23



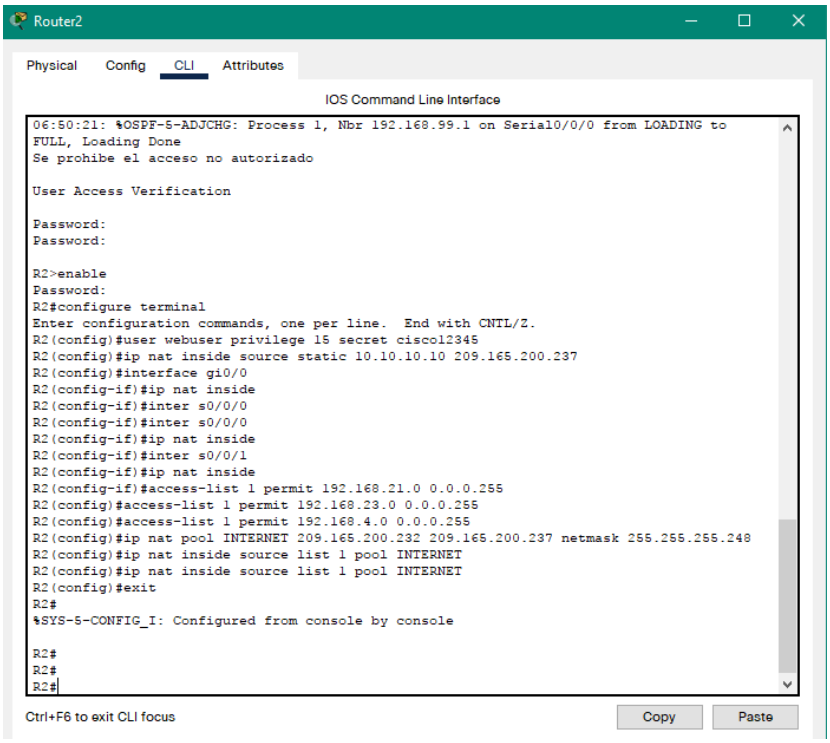
Fuente: Elaboración propia

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

La configuración del R2 incluye las siguientes tareas:

R2#configure terminal Ingreso a modo configuración
R2(config)#user webuser privilege 15 secret cisco12345 Crea una base de datos local con una cuenta de usuario
R2(config)#ip http server HTTP no soportado
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237 Crea una NAT estática al servidor web con la dirección global interna
R2(config)#interface gi0/0 Asigna la interfaz externa para la NAT estática
R2(config-if)#ip nat inside Asigna la interfaz interna para la NAT estática
R2(config-if)#inter s0/0/0 Asigna la interfaz externa para la NAT estática
R2(config-if)#ip nat inside Asigna la interfaz interna para la NAT estática
R2(config-if)#inter s0/0/1 Asigna la interfaz externa para la NAT estática
R2(config-if)#ip nat inside Asigna la interfaz interna para la NAT estática
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 Lista acceso 1
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 Lista acceso 1
R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255 Lista acceso 1
R2(config)#ip nat pool INTERNET 209.165.200.232 209.165.200.237 netmask 255.255.255.248 Define pool de direcciones IP públicas utilizables
R2(config)#ip nat inside source list 1 pool INTERNET Define la traducción de NAT dinámica

Figura 46. Configuración NAT estática y dinámica en el R2



Fuente: Elaboración propia

Paso 3: Verificar el protocolo DHCP y la NAT estática

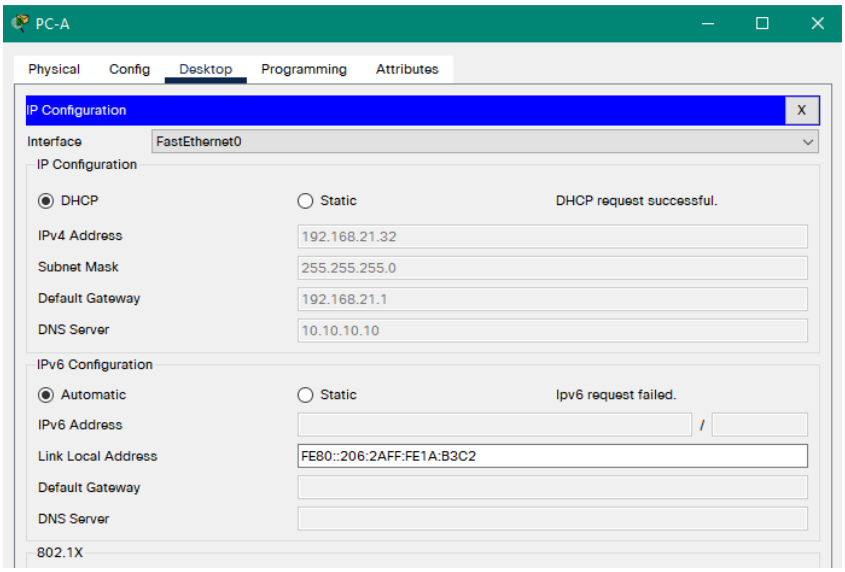
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 9. Verificación del protocolo DHCP y la NAT estática

Prueba
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.238) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**

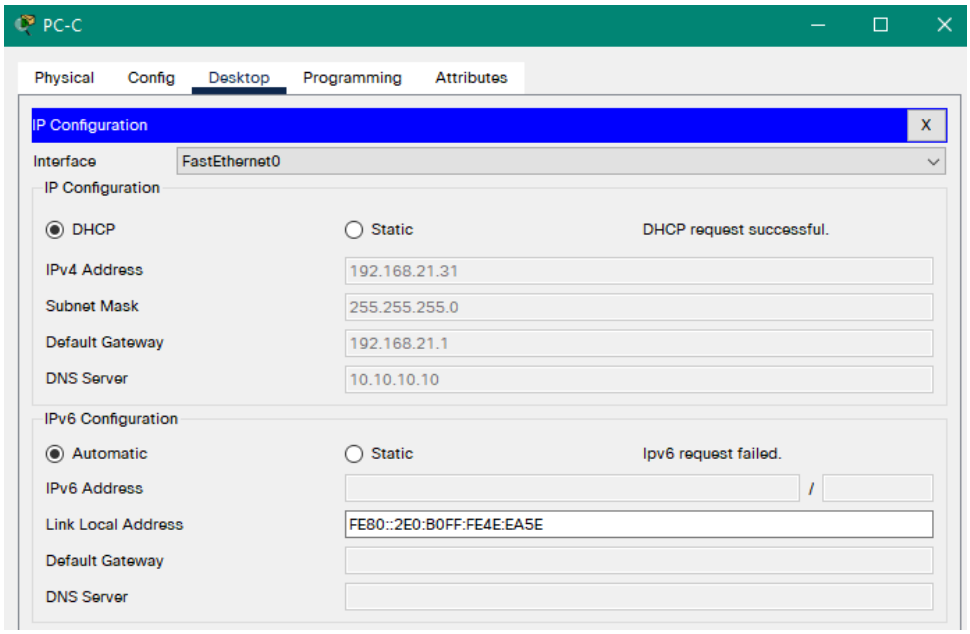
Fuente: Elaboración propia

Figura 47. Verificación PC-A adquirió información de IP del servidor de DHCP



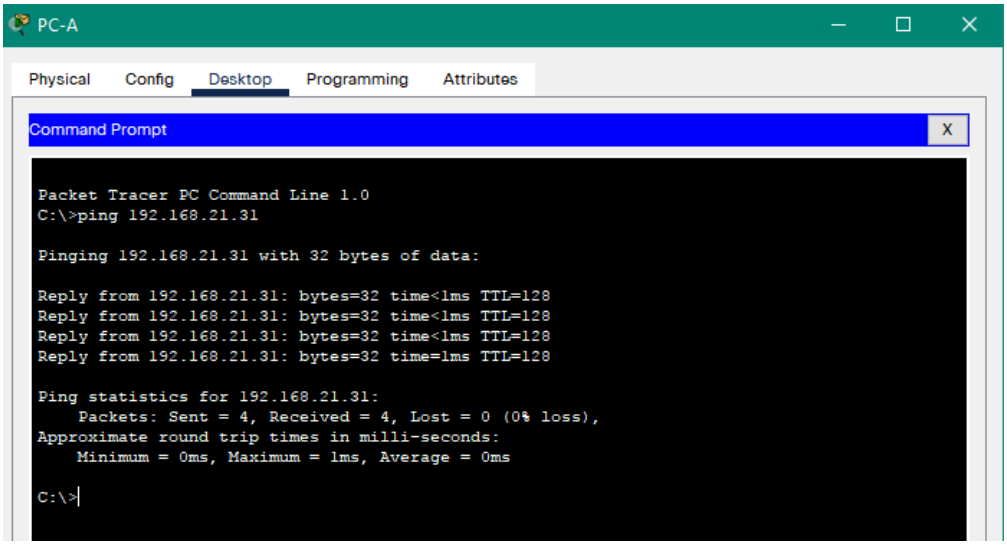
Fuente: Elaboración propia

Figura 48. Verificación PC-A adquirió información de IP del servidor de DHCP



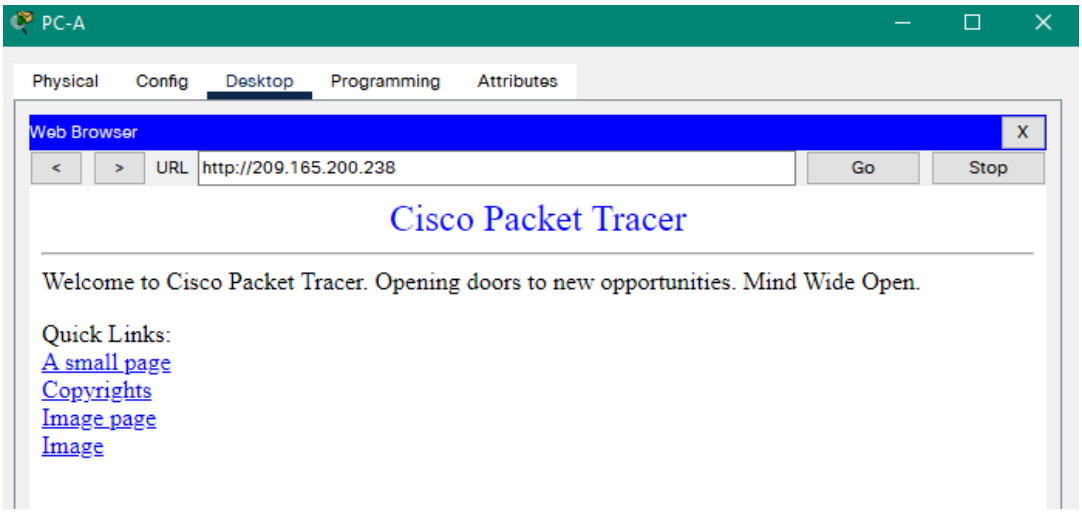
Fuente: Elaboración propia

Figura 49. Verificación PC-A puede hacer ping con la PC-C



Fuente: Elaboración propia

Figura 50. Prueba de acceso al servidor web



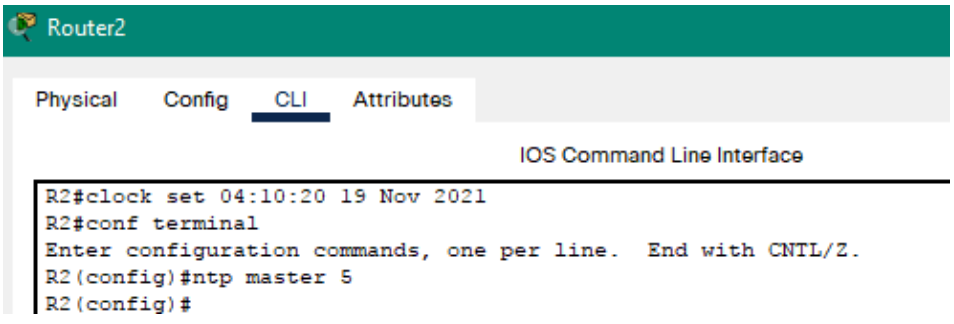
Fuente: Elaboración propia

Parte 6: Configurar NTP

Ajuste la fecha y hora en R2., Configure R2 como un maestro NTP.

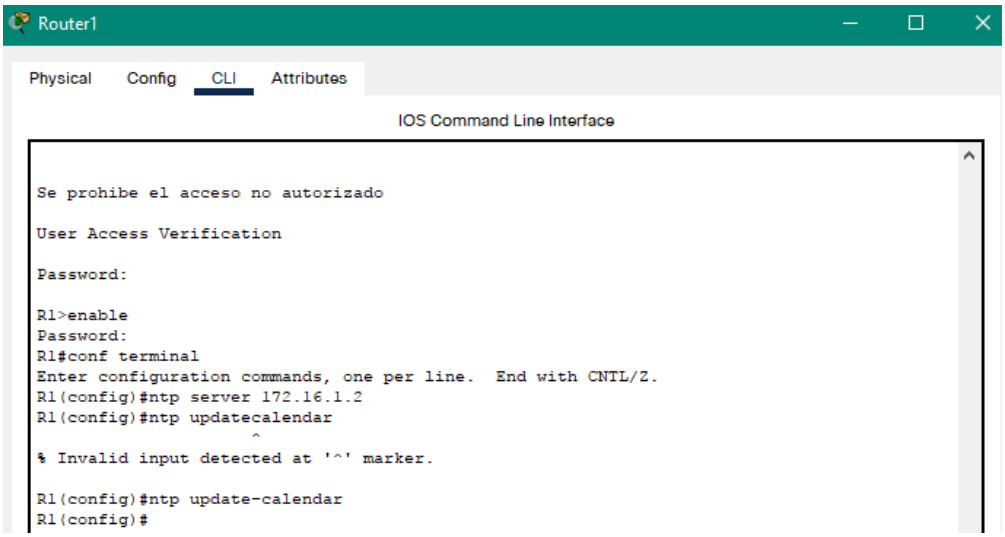
R2#clock set 04:10:20 19 Nov 2021	Ajusto fecha y hora
R2(config)#ntp master 5	Configuro nivel estrato
R1(config)#ntp server 172.16.1.2	Configuró R1- cliente NTP
R1(config)#ntp update-calendar	Configuró R1 para actualizaciones de calendario periódicas con hora NTP

Figura 51. Configuración NTP R2



Fuente: Elaboración propia

Figura 52. Configuración NTP R1

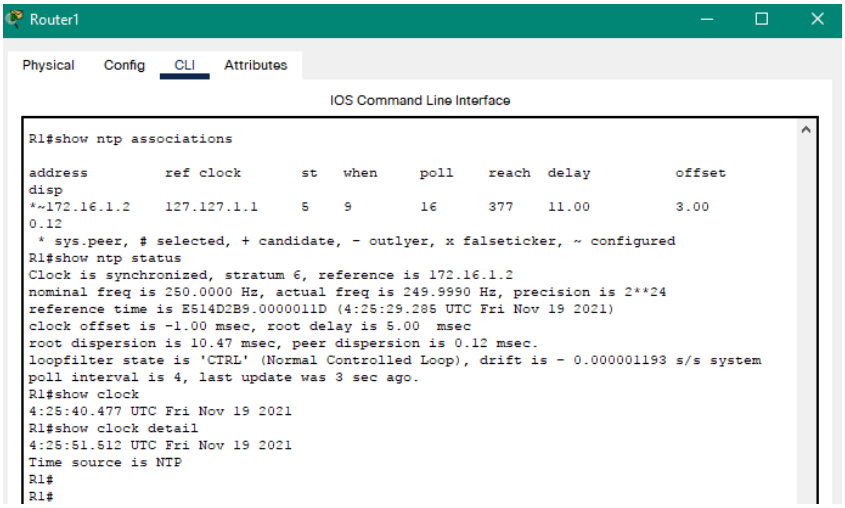


Fuente: Elaboración propia

Verifique la configuración de NTP en R1.

R1#show ntp associations	Verifica funcino y comunicación de NTP
R1#show ntp status	Verifica la configuración NTP
R1#show clock	Muestra la hora fijada en el router

Figura 53. Verificación de la configuración de NTP en R1.



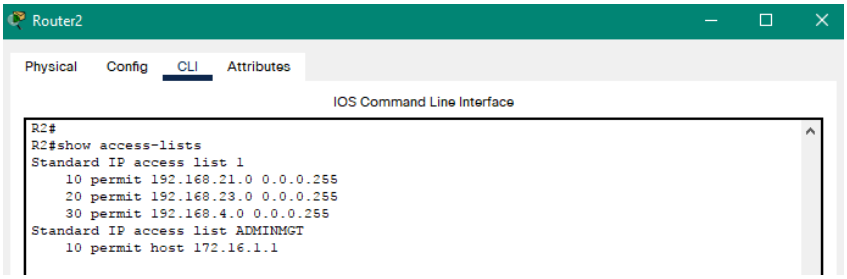
Fuente: Elaboración propia

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

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

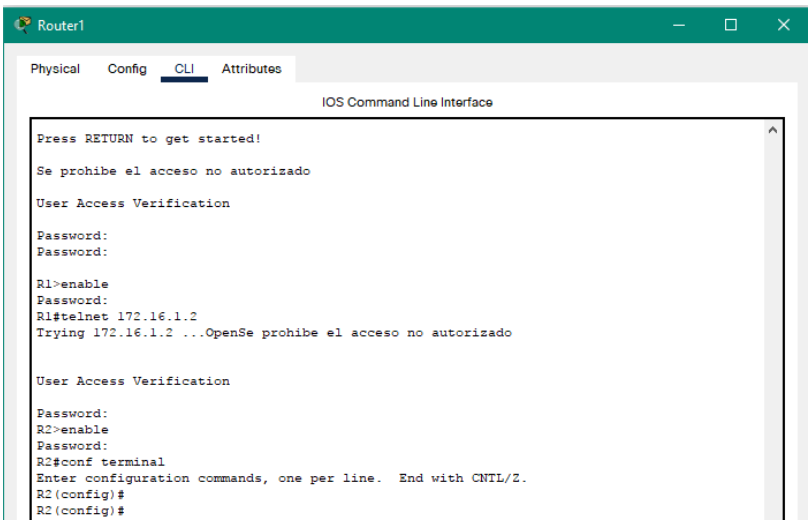
R2(config)#ip access-list standard ADMINMGT	Asigno nombre ACL tipo estándar
R2(config-std-nacl)#permit host 172.16.1.1	Asigno dirección del host permitido
R2(config-std-nacl)#exit	Saldo de configuración
R2(config)#line vty 0 4	Ingreso a la línea vty
R2(config-line)#access-class ADMINMGT in	Asigno permiso con nombre ACL
R2(config-line)#exit	Salgo de configuración
R2#show access-lists	Permite ver la lista de acceso

Figura 54. Verificación de ACL funcionando correctamente



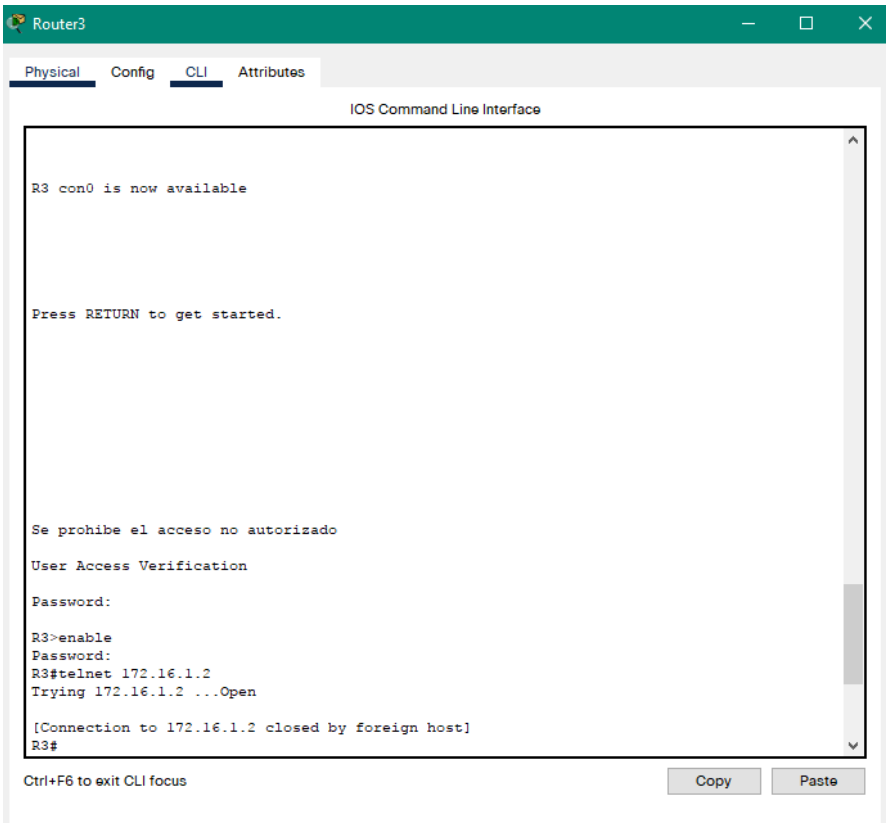
Fuente: Elaboración propia

Figura 55. Verificación desde R1 A R2 mediante conexión SSH



Fuente: Elaboración propia

Figura 56. Verificación R3 A R2 mediante conexión SSH



Fuente: Elaboración propia

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

R1(config)#show access-list Muestra las coincidencias recibidas por una lista de acceso desde la última vez que se restableció

R1(config)#clear access-list counters Restablece los contadores de una lista de acceso

R1 (config)#interface Fa0/1 Muestra qué ACL se aplica a una interfaz

R1 (config-if)#ip access-group 1 out Muestra qué ACL se aplica a una dirección

R1 (config)#show ip nat translations Muestran las traducciones NAT

R1(config)#clear ip nat translation Elimina las traducciones de NAT dinámicas

CONCLUSIONES

Se logra desarrollar habilidades que permiten resolver problemas mediante un requerimiento de red ya sea para pequeñas o grandes empresas, todo esto a través de análisis y conocimiento adquirido en el diplomado, el cual permitió aprender de forma teórica y práctica con equipamiento de tecnología Cisco, la cual tiene prestigio, experiencia y calidad para implementar o administrar redes de forma segura.

Se logra verificar las distintas configuraciones que se realizan a los equipos tanto en conectividad, tipos de acceso y seguridad, de este modo comprobar la realización de un trabajo correcto y sobre todo enriquecer el conocimiento propio.

Con el apoyo de los tutores se realiza de forma correcta los ejercicios que se presentaron durante este diplomado, se explicó los conceptos, tecnologías, protocolos y configuraciones realizadas, así obteniendo un buen desarrollo en todas las actividades a lo largo de este, que sin duda alguna son para el desarrollo de nuestra carrera como ingenieros de sistemas y al mismo tiempo reconocer la importancia de la tecnología en el mundo y que evoluciona cada día. Además, con todo el conocimiento y la experiencia que se adquiere tanto profesional y como persona facilita oportunidades al mundo laboral.

BIBLIOGRÁFIA

Barreño Gutiérrez, R. (2013). Elaboración de un estado de arte sobre el protocolo IPV6; y su implementación sobre protocolos de enrutamiento dinámico como RIPNG, EIGRP y OSPF basado sobre la plataforma de equipos cisco. Disponible en: https://repository.upb.edu.co/handle/20.500.11912/1259?show=full

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

CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

Cobo, A. "Direccionamiento IP-Subredes. (2009). Disponible en: https://archivos.csif.es/archivos/andalucia/ensenanza/revistas/csicsif/revista/pdf/Numero_23/ANGEL_COBO_2.pdf

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

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. Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9

Echegaray Yépez, M. A. (2021). Direccionamiento IPv4 e IPv6. Disponible en: https://repositorio.continental.edu.pe/handle/20.500.12394/9061

Gutiérrez, R. B., Núñez, W. N., Urrea, S. C., Osorio, H. S., & Acosta, N. D. (2016). Revisión de la seguridad en la implementación de servicios sobre IPv6. Inge Cuc, 12(1), 86-93. Disponible en: https://revistascientificas.cuc.edu.co/ingecuc/article/view/720/pdf_17

Vesga, J. (2017). Ping y Tracer como estrategia en los procesos de Networking [OVA]. Disponible en https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

ANEXOS

Archivo de simulación en Packet Tracer Escenario 1 https://drive.google.com/file/d/1OWljjXl9BM5ftUunVmsiyhW5AH-1EVo_/view?usp=sharing

Archivo de simulación en Packet Tracer Escenario 2 https://drive.google.com/file/d/1hSSrkAcRjZ71wKyPQ3nxQpaiHHMBfu0f/view?usp=sharing