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

GABRIELA SÁNCHEZ CASTILLO

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

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

GABRIELA SÁNCHEZ CASTILLO

Diplomado de opción de grado presentado para optar al título de INGENIERA DE SISTEMAS

DIRECTORA:
Mgtr. NANCY AMPARO GUACA

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

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Cali, 28 de noviembre de 2021

AGRADECIMIENTOS

Hoy que me encuentro a puertas de alcanzar una nueva meta en mi vida, la gloria es para Dios que me sostiene cada día y me permite hacer realidad este sueño.

Agradezco a mi familia, eje principal de mi vida y que merece compartir esta dosis de éxito que se aproxima en mi desarrollo profesional y con especial afecto hacia mi pequeño hijo Jacob Valero Sánchez.

A mi compañero de trabajo Williams Ávila Pardo, quien ha sido el promotor para la culminación de mi carrera.

A mis demás compañeros de la Contraloría General de la República, que con su experiencia me han guiado y compartido sus conocimientos en este proceso de formación, también para aquellos que en este año se adelantaron en el camino y hoy desde el cielo me acompañan.

Finalmente a los tutores de la Universidad Nacional Abierta y a Distancia – UNAD que han impartido sus conocimientos y son testigos de los triunfos que alcanzan sus estudiantes en pro de contribuir al desarrollo social de nuestro país.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

LAN: Es la abreviatura de Local Área Network. Denomina redes con extensión física limitada. La mayoría de las redes LAN se usan en hogares privados o en empresas, para instalar redes de hogar o de empresa. De este modo, distintos dispositivos pueden comunicarse entre ellos. De este modo, el intercambio de datos tiene lugar primero a nivel local.

IPV4: Es el nombre del protocolo de Internet utilizado actualmente para las direcciones IP de los dominios. Estas direcciones IP se asignan automáticamente cuando se registra un dominio.

IPV6: Es la última versión del protocolo de Internet (IP) desarrollada por el Internet Engineering Task Force (IETF). Esta versión sustituye la versión 4 (IPv4) que se usaba hasta ahora y establece un procedimiento estándar para transmitir paquetes de datos en redes de ordenadores.

HOST: Un host o anfitrión es un ordenador que funciona como el punto de inicio y final de las transferencias de datos. Más comúnmente descrito como el lugar donde reside un sitio web. Un host de Internet tiene una dirección de Internet única (dirección IP) y un nombre de dominio único o nombre de host.

ROUTER: Es el periférico que se encarga de llevar la conexión a los dispositivos. Es importante decir que un router no está conectado a Internet, sino que está conectado al módem. Un router per se no vale para nada si no hay un módem que le provea de la conexión a Internet. Es como tener un móvil sin batería: tienes el dispositivo pero no lo que le permite funcionar.

SWITCH: Es un dispositivo de interconexión utilizado para conectar equipos de red formando lo que se conoce como una red de área local (LAN) cuyas especificaciones técnicas siguen el estándar conocido como ethernet. Es importante tener claro que un switch NO proporciona por sí solo conectividad con otras redes, y obviamente tan poca conectividad con internet.

SERVIDOR: Es una máquina física integrada en una red informática en la que, además del sistema operativo, funcionan uno o varios servidores basados en

software. Una denominación alternativa para un servidor basado en hardware es "host" (término inglés para "anfitrión"). En principio, todo ordenador puede usarse como "host" con el correspondiente software para servidores.

SUBNETTING: Es la técnica de dividir una red grande en redes más pequeñas (subredes), para calcular qué máscara de subred necesitaremos utilizar en la nueva red, deberemos calcular diferentes parámetros.

VLAN: Las VLAN (redes de área local virtuales) pueden considerarse como dominios de difusión lógica. Una VLAN divide los grupos de usuarios de la red de una red física real en segmentos de redes lógicas

RESUMEN

El presente informe contiene la simulación de los escenarios propuestos para dos clases de topologías de red, con los cuales se busca fortalecer las habilidades y competencias que ofrece la Academia CISCO en todo lo relacionado a la implementación de infraestructura de redes empresariales LAN/WAN.

La solución de estos escenarios se desarrolla bajo las instrucciones brindadas en el documento denominado Prueba de Habilidades CCNA II-2021 y el acompañamiento del equipo de tutores de la UNAD para el Diplomado de Profundización Cisco (Diseño e Implementación de Soluciones Integradas LAN / WAN), quienes con su orientación contribuyen a la ejecución de este Proyecto.

Los ambientes de simulación son una herramienta de gran importancia, puesto que a través del uso de elementos interactivos proporcionan una experiencia de aprendizaje significativo, que ayudan a comprender el funcionamiento de una red tanto en la parte física como lógica.

El resultado obtenido en el desarrollo de los escenarios de la prueba de habilidades es el núcleo más importante del proceso de esta interacción, que con la ayuda de los programas de simulación y laboratorios remotos, constituyen un gran instrumento para el desempeño de competencias, debido a que invita al estudiante a explorar mediante la práctica un contexto cercano a la realidad.

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

ABSTRACT

This report contains the simulation of the proposed scenarios for two classes of network topologies, which seeks to strengthen the skills and competencies offered by the CISCO Academy in everything related to the implementation of LAN / WAN enterprise network infrastructure.

The solution of these scenarios is developed under the instructions provided in the document called CCNA II-2021 Skills Test and the accompaniment of the UNAD team of tutors for the Cisco Deepening Diploma (Design and Implementation of Integrated LAN / WAN Solutions), who with their guidance contribute to the execution of this Project.

Simulation environments are a tool of great importance, since through the use of interactive elements they provide a meaningful learning experience, which help to understand the functioning of a network both physically and logically.

The result obtained in the development of the skills test scenarios is the most important nucleus of the process of this interaction, which with the help of simulation programs and remote laboratories, constitutes a great instrument for the performance of skills, due to that invites the student to explore through practice a context close to reality.

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

INTRODUCCIÓN

En la actualidad se observa el alto impacto que tiene sobre la sociedad moderna la llamada transformación digital, de la cual hace parte la vertiginosa evolución que presenta las redes de datos, fundamentales para la gestión y operación de las tecnologías de la información y las comunicaciones.

La humanidad ha sido testigo en estos dos últimos años del auge que tiene la red global de internet que busca avanzar en un mundo cada vez más interconectado, con dispositivos inteligentes, la computación en la Nube y el internet de las cosas (IoT), todo ello precisamente por el avance de la tecnología en las redes de telecomunicaciones.

En el desarrollo de este informe partiremos de las operaciones básicas que tiene la interconexión de los diferentes dispositivos que conforman las topologías de red, que tratan de representar entornos casi reales para pequeñas y medianas empresas que buscan soluciones de infraestructuras ágiles, económicas, sólidas y seguras.

A continuación se presentan la configuración de dos escenarios con uno de los temas centrales del curso de profundización, como lo son los fundamentos de enrutamiento y conmutación, desplegando la configuración de los equipos para el diseño del esquema de direccionamiento IPv4 e IPv6 para las redes LAN planteadas, se establecerán comandos para la seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente.

DESARROLLO ESCENARIO 1

Escenario 1

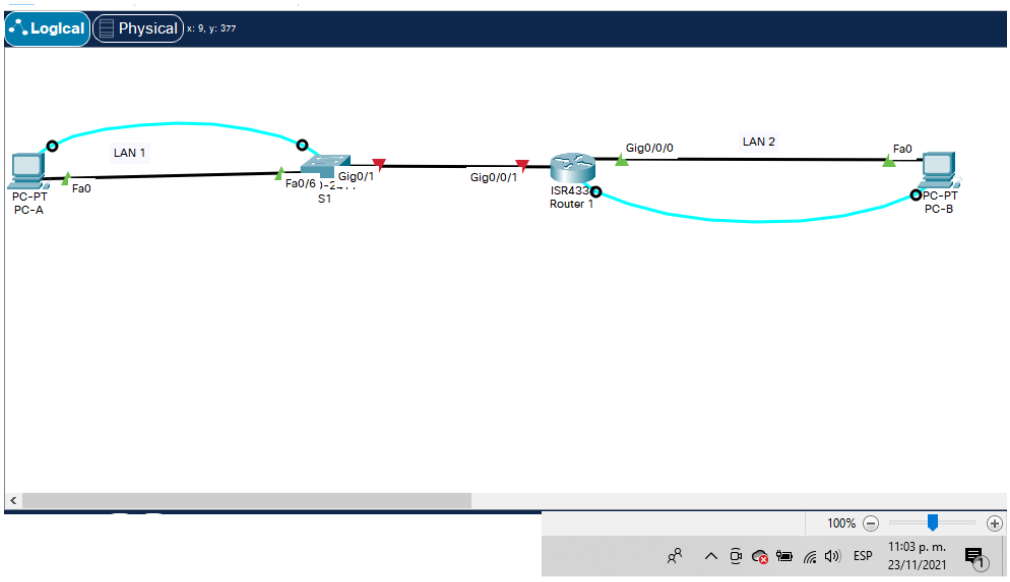
Figura 1. Topología Original Escenario 1

Fuente: Guía de Actividades

En el escenario propuesto se configurarán los dispositivos de una red pequeña. Se configurará un router 4331, un switch 2960 y equipos de cómputo que permitan tanto la conectividad con IPv4 como IPv6 para los hosts soportados.

Iniciamos Packet Tracer versión 8.0.1 se crea la topología de red utilizando para ello 1 Router Cisco 43331, 2 Switches Cisco 3560, 2 PCS con los respectivos cables de cobre directos para establecer la conexión.

Figura 2. Simulación Escenario 1 en Packet Tracer



Fuente: Autoría propia

Paso 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

Paso 2: Desarrolle el esquema de direccionamiento IP

Cada estudiante tomará el direccionamiento 192.168.**13**.0 donde X corresponde a los últimos dos dígitos de su cédula.

A continuación se procede a diseñar el Subnetting de la Topología de Red propuesta en la Figura 1, con el fin de modificar la máscara de red y conseguir mejor desempeño entre las subredes:

En el primer paso establecemos en la LAN 1 la dirección 192.168.**13**.0/24 para 100 hosts Se toma las posiciones que satisfagan los 100. Equivale a $2^7 = 128$

11111111.11111111.11111111.10000000/25 ⟶ (nueva máscara)

↓

$2^1 = 2$ subredes

Ahora la convertimos en decimal punteada: 255.255.255.128

SALTO: 128

Continuamos con la LAN 2 192.168.**13**.128

11111111.11111111.11111111.11000000/26 ⟶ (nueva máscara)

↓

$2^2 = 4$ subredes

Ahora la convertimos en decimal punteada: 255.255.255.192

Tabla 1. Subredes

Subred	Hosts	Dirección de Red	Máscara	Primera IP Válida	Última IP Válida	Broadcast
LAN 1	100	192.168.13.0	255.255.255.128	192.168.13.1	192.168.13.126	192.168.13.127
LAN 2	50	192.169.13.128	255.255.255.192	192.169.13.129	192.168.13.190	192.168.13.191

Fuente: Autoría propia

Tabla 2. Tabla de Direccionamiento

Ítem	Requerimiento
Dirección de Red	192.168.13.0
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	192.168.13.1/25
R1 G0/0/0	192.168.13.129/26
S1 SVI	192.168.13.2/25
PC-A	192.168.13.126/25
PC-B	192.168.13.190/26

Fuente: Autoría propia

Paso 3: Configure aspectos básicos:

Los dispositivos de red (S1 y R1) se configuran mediante conexión de consola. Las tareas de configuración para **R1** incluyen las siguientes:

Tabla 3. Configuración para R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config-line)#password ciscoconpass
Establecer la longitud mínima para las contraseñas	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1(config-line)#security password min-length 10: Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config-line)# line vty 0 4 R1(config-line)#password cisco R1(config-line)#login local
Configurar VTY solo aceptando SSH	R1(config-line)# transport input SSH
Cifrar las contraseñas de texto no cifrado	R1(config)# service password-encryption
Configure un MOTD Banner	R1(config)#banner motd #este es el router de la UNAD, cualquier intrusión tendrá efectos judiciales#
Configurar interfaz G0/0/0	R1(config)# int g0/0/0 R1(config -if)# ip address 192.168.13.129 255.255.255.192 R1(config -if)#description esta es la interfaz de la LAN 2 R1(config -if)#no sh

Configurar interfaz G0/0/1	R1(config)# int g0/0/1 R1(config -if)# ip address 192.168.13.1 255.255.255.128 R1(config -if)#description esta es la interfaz de la LAN 1 R1(config -if)#no sh
Generar una clave de cifrado RSA	R1(config)# ip domain-name ccna-lab.com Luego se genera la encripción a 1024 bits R1(config)# crypto key generate rsa Módulo de 1024 bits

Fuente: Autoría Propia

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 4.Configuración switch 1

Tarea	**Especificación**
Desactivar la búsqueda DNS.	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config-line)#password ciscoconpass
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config-line)# line vty 0 15 S1(config-line)#password cisco S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)# transport input SSH
Cifrar las contraseñas de texto no cifrado	S1(config)# service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd #este es el Switch de la UNAD, por favor no entrar aqui#
Generar una clave de cifrado RSA	S1(config)# crypto key generate rsa Módulo de 1024 bits
Configurar la interfaz de administración (SVI)	S1(config)# int vlan 1 S1(config)# ip address 192.168.13.2 255.255.255.128
Configuración del gateway predeterminado	S1(config)# ip default gateway 192.168.13.1

Fuente: Autoría Propia

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**.

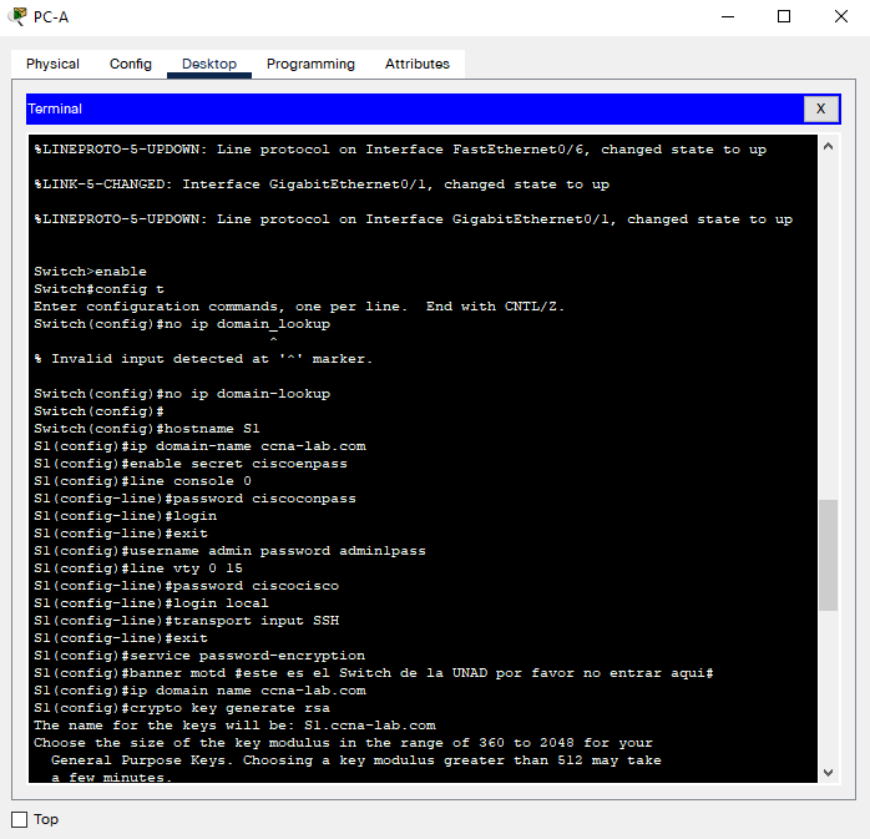
Tabla 5. Configuración de red del PC-A

PC-A Network Configuration	
Descripción	Este es el PC-A
Dirección física	002.4A3C.C3B0

Dirección IP	192.168.13.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.13.1

Fuente: Autoría Propia

Figura 3. Configuración PC-A



Fuente: Autoría Propia

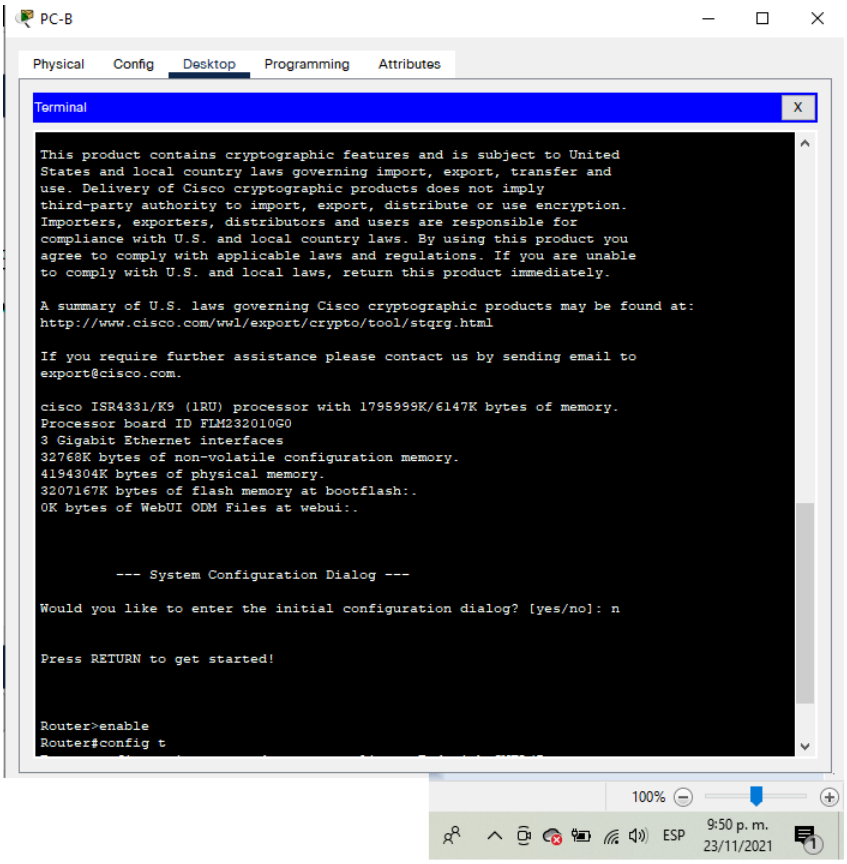
Tabla 6. Configuración de red del PC-B

PC-B Network Configuration	
Descripción	Este es el PC-B
Dirección física	0002.1799.6715
Dirección IP	192.168.13.190
Máscara de subred	255.255.255.128

Gateway predeterminado	192.168.13.129

Fuente: Autoría Propia

Figura 4. Configuración PC-B



Fuente: Autoría Propia

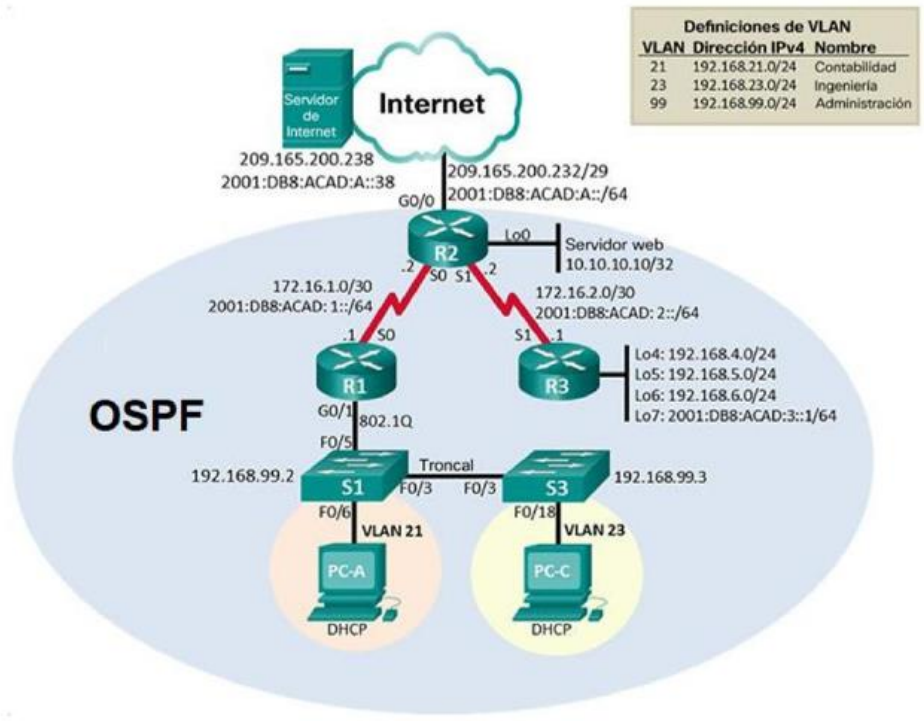
DESARROLLO ESCENARIO 2

Escenario 2

En este escenario nos presentan otra topología de una pequeña red que está diseñada para enlazar la conectividad IPv4 e IPv6, seguridad de switches, protocolo de configuración de hosts dinámicos (DHCP), routing entre VLAN, protocolo de routing dinámico OSPF, traducción de direcciones de red dinámicas y estáticas (NAT), configuración de listas de control de acceso (ACL) y finalmente el protocolo de tiempo de red (NTP) entre servidor/cliente.

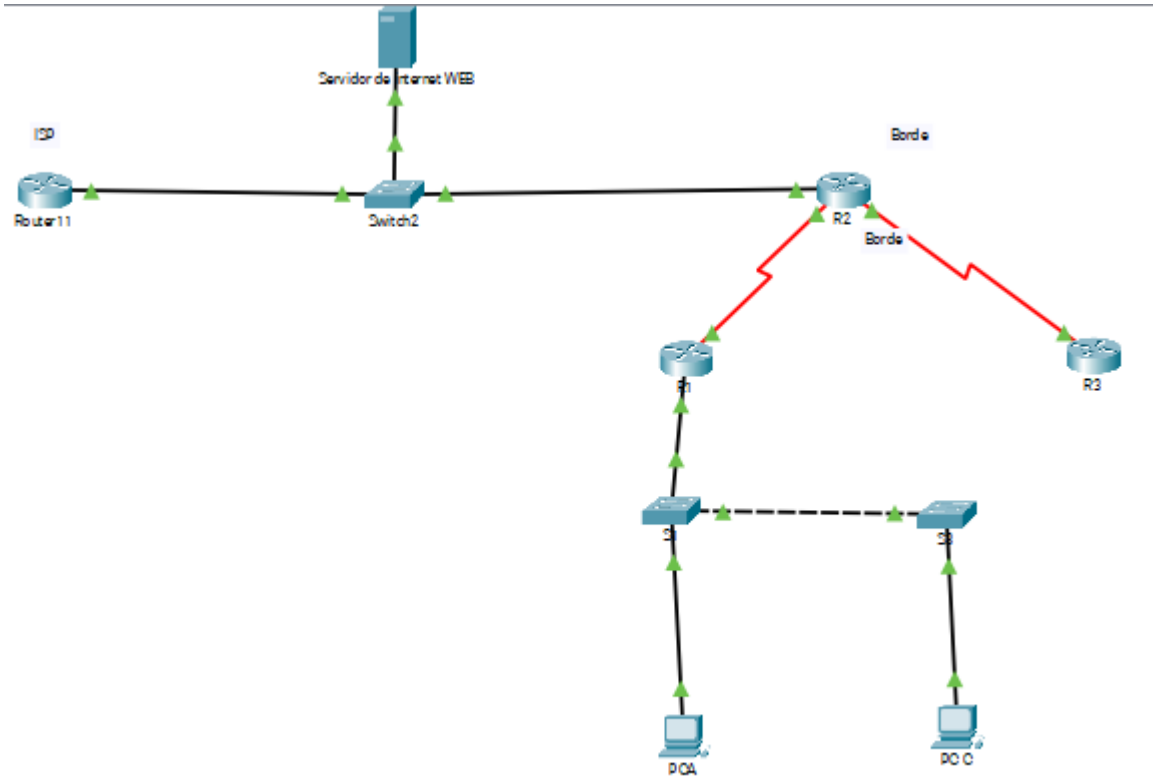
Los diferentes entornos de cada dispositivo, como Consola, Desktop, CLI, entre otros; serán nuestra principal herramienta durante la configuración y verificación del funcionamiento direccionados por las líneas de comando, que hemos aprendido y practicado en los talleres propuestos en el curso

Figura 5. Topología Original Escenario 2



Fuente: Guía de Actividades

Figura 6. Simulación Escenario 2 en Packet Tracer



Fuente: Topología Propuesta por el Tutor Raúl Bareño Gutiérrez

Parte 1: Inicializar dispositivos

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

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

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

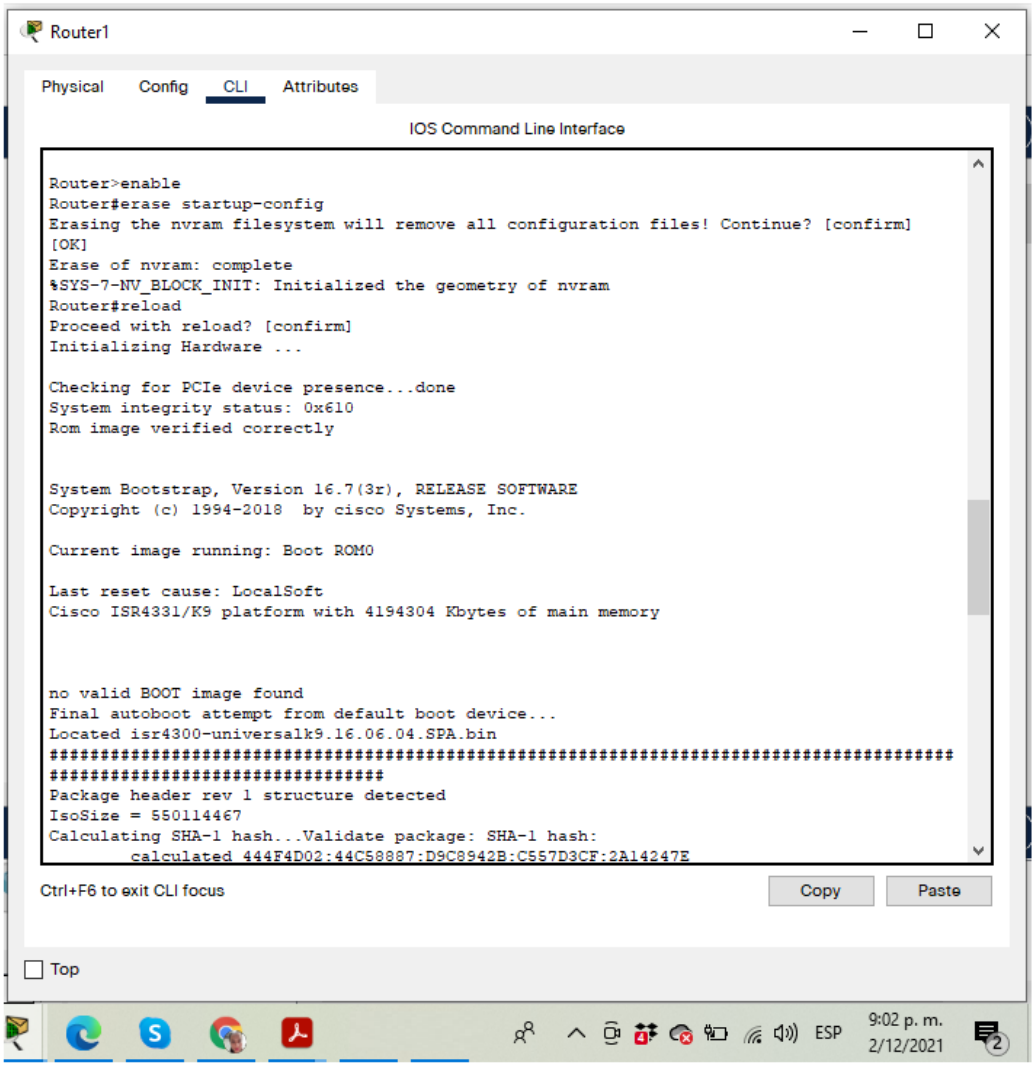
Tabla 7. Eliminar las configuraciones de inicio de los Router y Switchs

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config

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

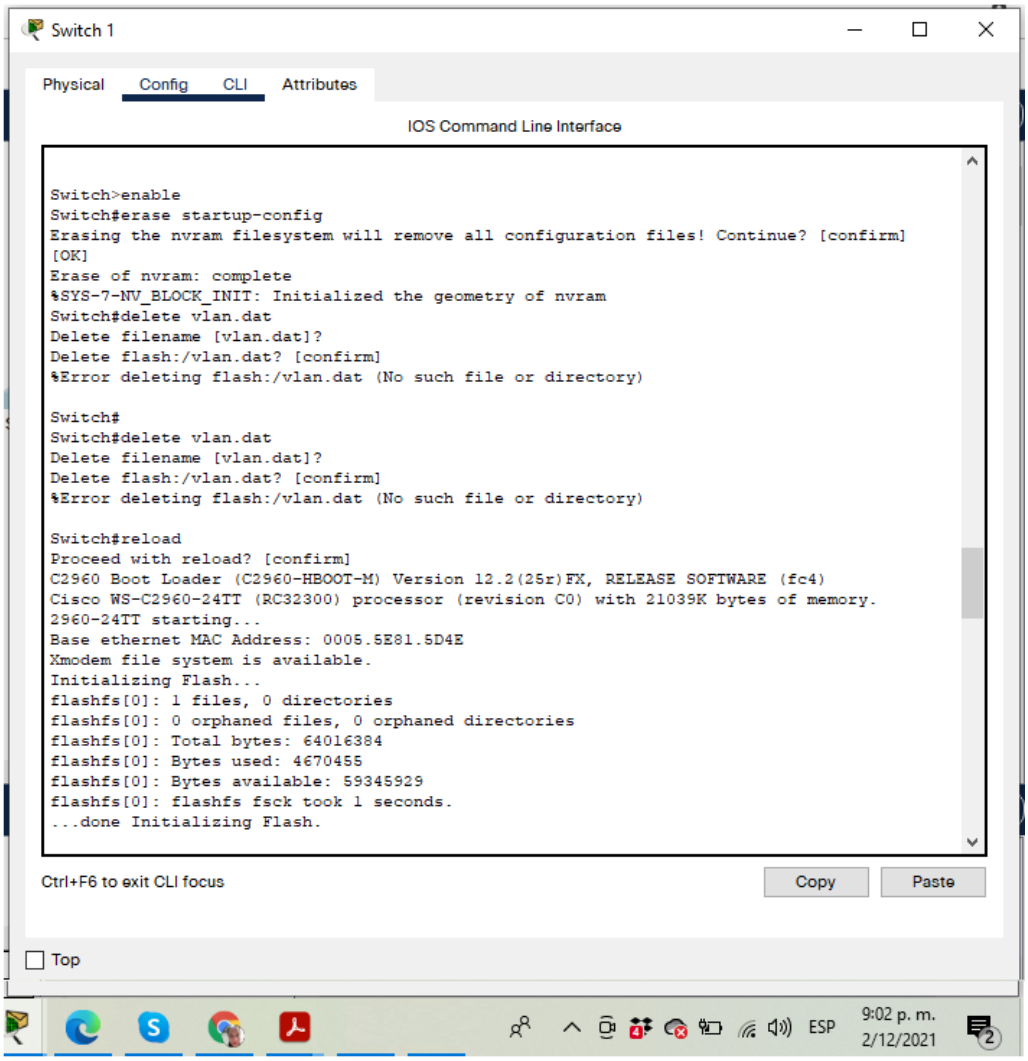
Fuente: Autoría Propia

Figura 7. Eliminación de la configuración del Router 1



Fuente: Autoría Propia

Figura 8. Eliminación de la configuración del Switch 1



Fuente: Autoría Propia

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

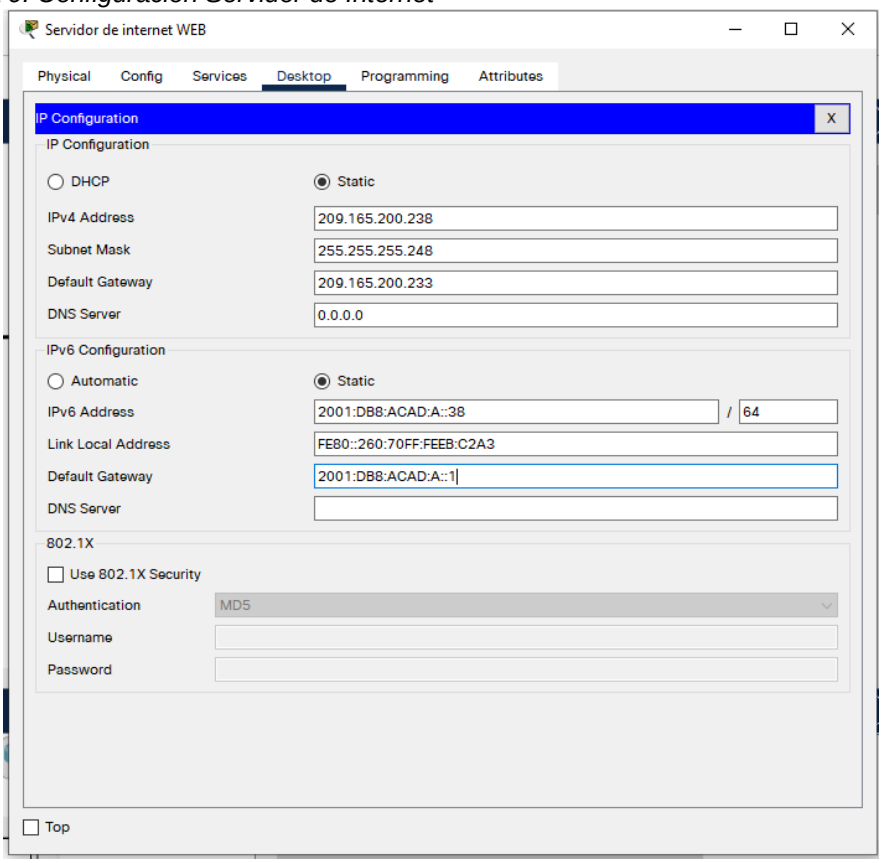
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 8. Configuración Servidor de Internet.

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	IPv6 2001:DB8: ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Fuente: Autoría Propia

Figura 9. Configuración Servidor de Internet



Fuente: Autoría Propia

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

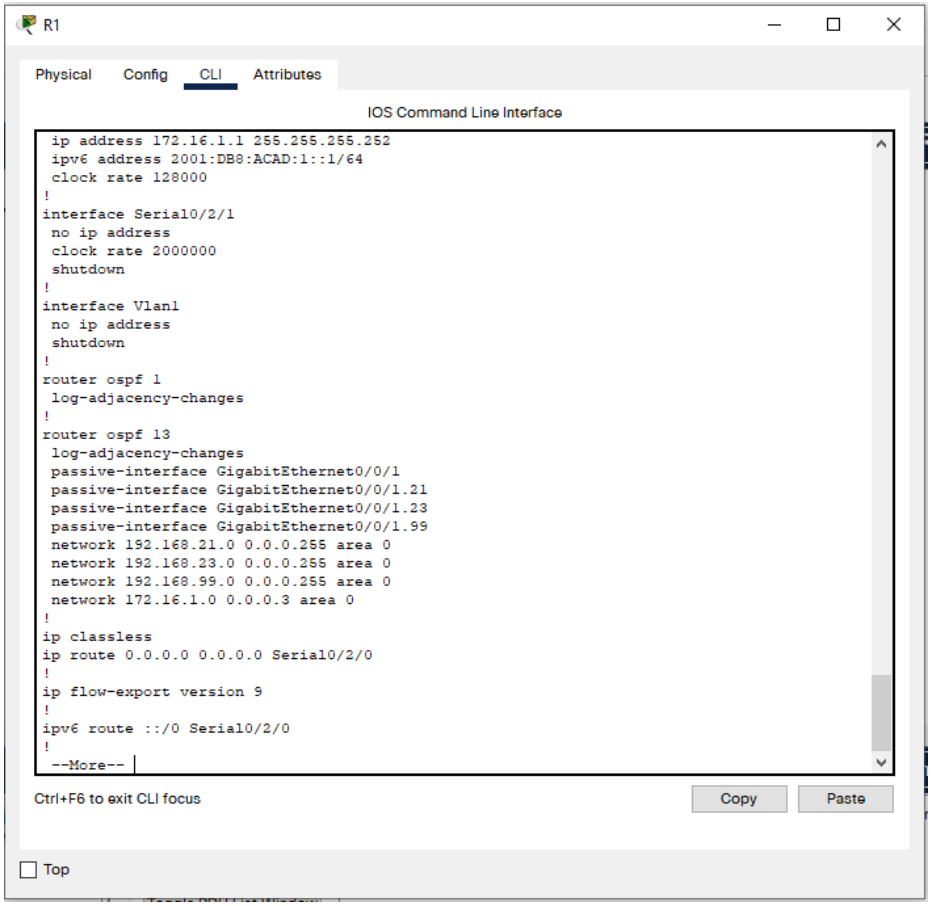
Tabla 9. Configuración Router 1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class R1
Contraseña de acceso a la consola	R1(config-line)#password cisco
Contraseña de acceso Telnet	R1(config-line)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd #Se prohíbe el acceso no autorizado#

Interfaz S0/2/0	R1(config)#int s0/2/0 R1(config-if)#des R1(config-if)#description interface hacia el router R2 R1(config-if)#exit R1(config)#ipv6 uni R1(config)#ipv6 unicast-routing R1(config)#int s0/2/0 R1(config-if)#ip a R1(config-if)#ip ad R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 add R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no sh
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 S0/2/0 R1(config)#ipv6 route ::/0 S0/2/0

Fuente: Autoría Propia

Figura 10. Configuración Router 1



Fuente: Autoría Propia

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 10. Configuración Router 2

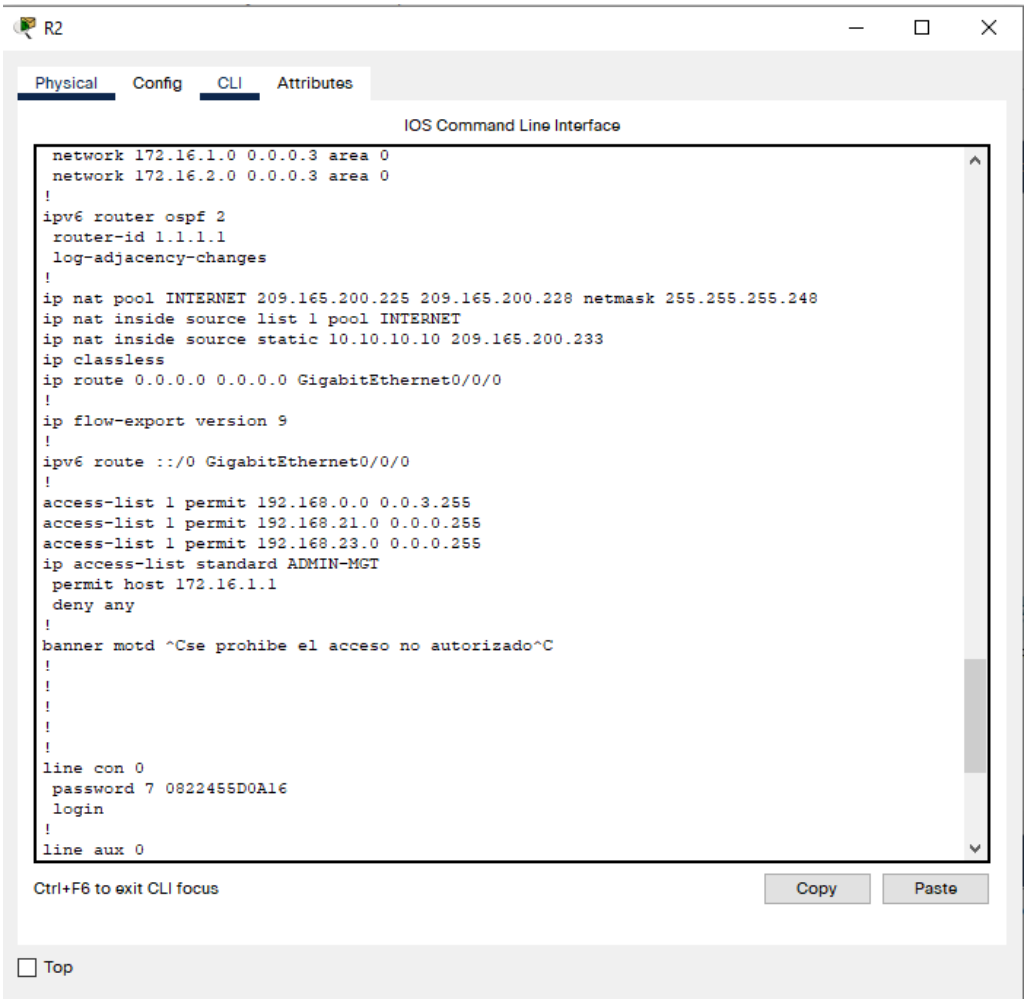
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2

Contraseña de exec privilegiado cifrada	R2(config)#enable secret class R2
Contraseña de acceso a la consola	R2(config-line)#password cisco
Contraseña de acceso Telnet	R2(config-line)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server, **Podemos observar que el mismo no es válido para ninguno de los routers de la versión 8.0.1 de Packet Tracer**
Mensaje MOTD	R1(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/2/0	R2(config)#int s0/2/0 R2(config-if)#description conexión R2 a R1 R2(config-if)#ip add R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 add R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown
Interfaz S0/2/1	R2(config-if)#interface s0/0/1 R2(config-if)#description conexión R2 a R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown

Interfaz G0/0 (simulación de Internet)	R2(config-if)#interface g0/0 R2(config-if)#description Conexion a Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config)#int loopback 0 R2(config-if)# %LINK-5-CHANGED: Interface Loopback0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up R2(config-if)#des R2(config-if)#description servidor WEB R2(config-if)#ip add R2(config-if)#ip address 10.10.10.10 255.255.255.255
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 R2(config)#ipv6 route ::/0 g0/0

Fuente: Autoría Propia

Figura 11. Configuración Router 2



Fuente: Autoría Propia

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

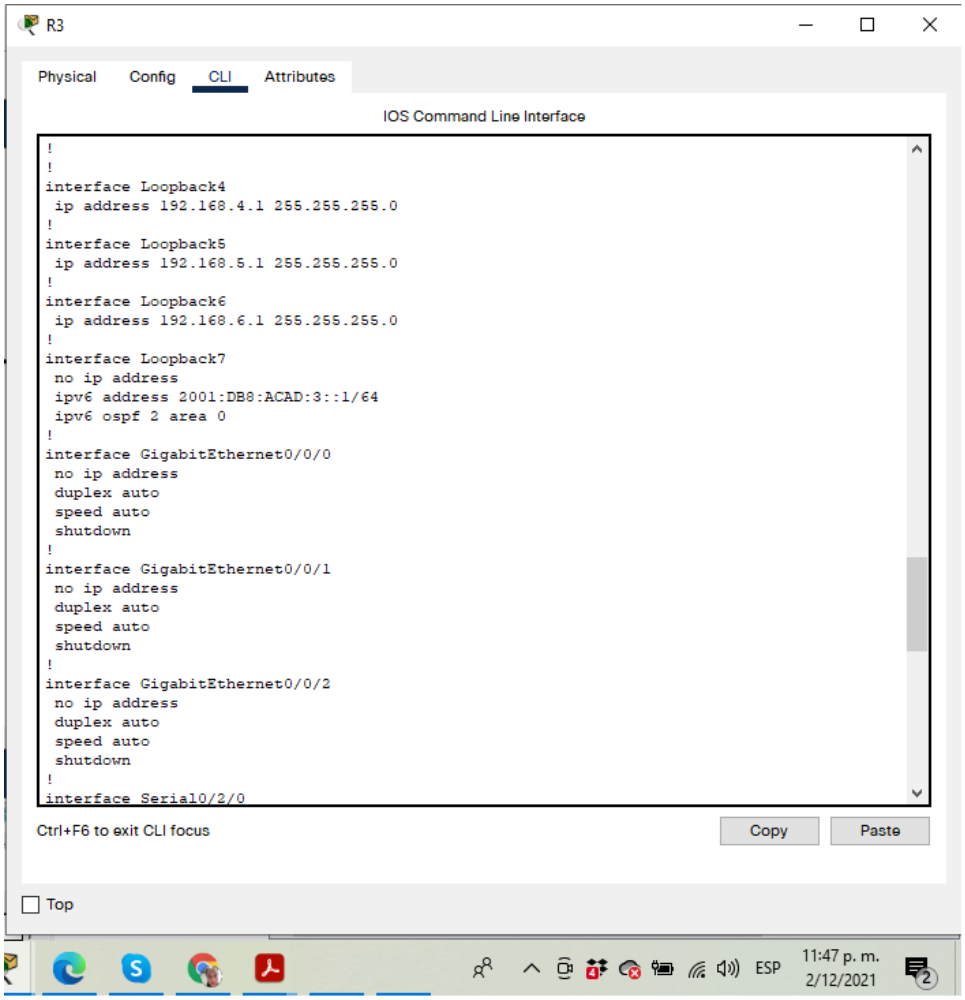
Tabla 11. Configuración Router 3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	(R3config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)# service password-encryption
Mensaje MOTD	R3(config)#banner motd "#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/0/1	R3(config)#int s0/2/1 R3(config-if)#description Conexion a R2 R3(config-if)#exit R3(config)#ipv6 unic R3(config)#ipv6 unicast-routing R3(config)#int s0/2/1 R3(config-if)#ip add R3(config-if)#ip address 172.16.2.2 255.255.255.252 R3(config-if)#ipv6 add R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown

Interfaz loopback 4	R3(config-if)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config-if)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config-if)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config-if)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
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

Fuente: Autoría Propia

Figura. 12 Configuración Router 3



Fuente: Autoría Propia

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 12. Configuración Router Switch 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1

Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config-line) # service password encryption
Mensaje MOTD	S1(config)#banner motd #Se prohíbe el acceso no autorizado#

Fuente: Autoría Propia

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 13. Configuración Router Switch 1

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

Cifrar las contraseñas de texto no cifrado	S3(config-line)# service password-encryption
Mensaje MOTD	S3(config)#banner motd #Se prohíbe el acceso no autorizado#.

Fuente: Autoría Propia

Paso 7: Verificar la conectividad de la red

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

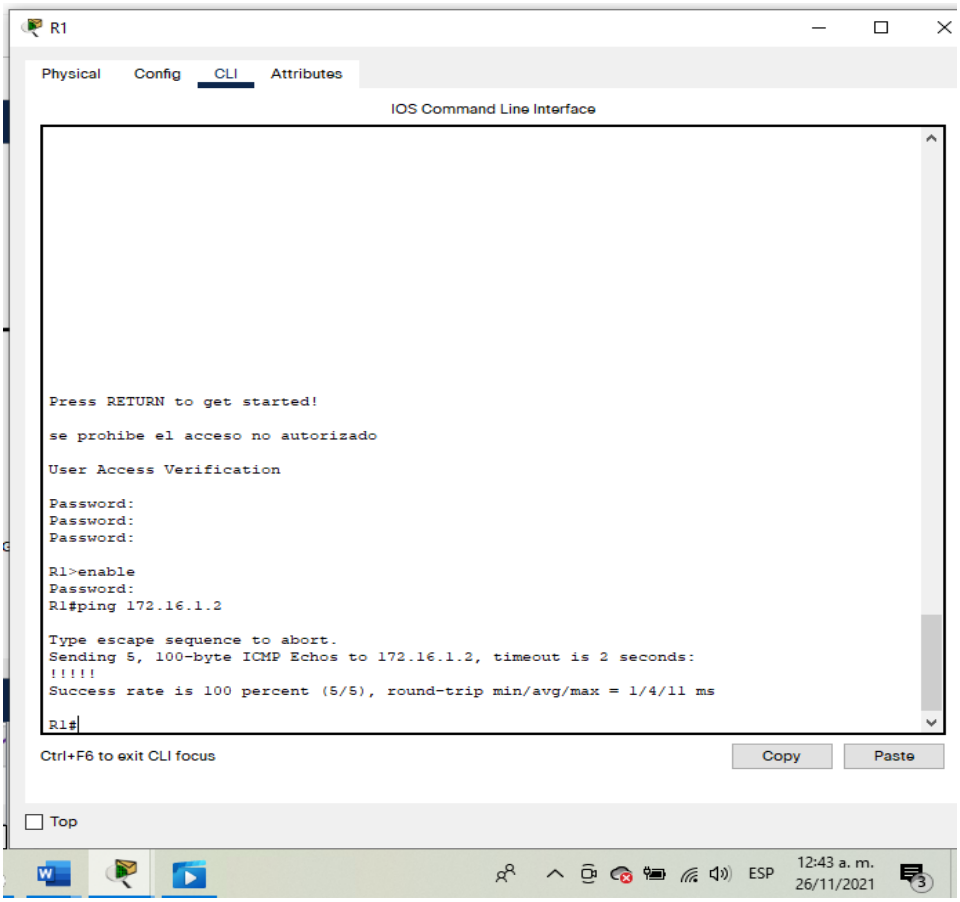
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 14. Verificación conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/2/0	172.16.1.2	Exitoso
R2	R3, S0/2/1	172.16.2.1	Exitoso
PC de Internet	Gateway predeterminado	209.165.200.233	Exitoso

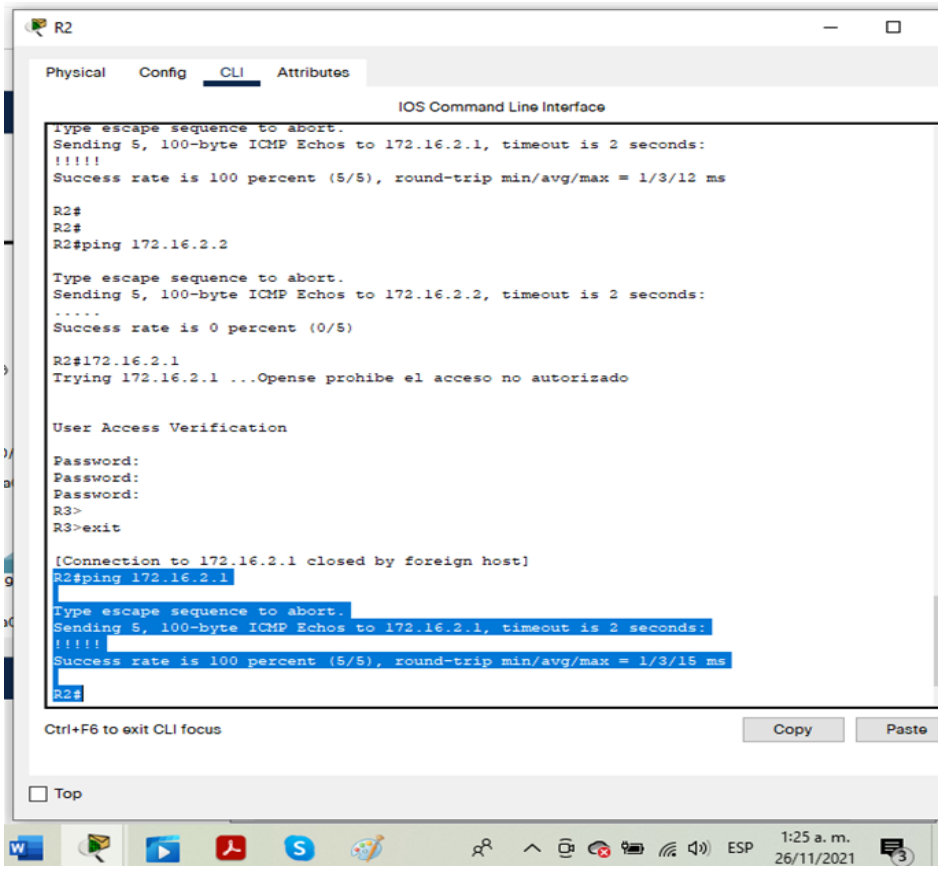
Fuente: Autoría Propia

Figura 13. Ping desde R1 a R2 a la S0/2/0



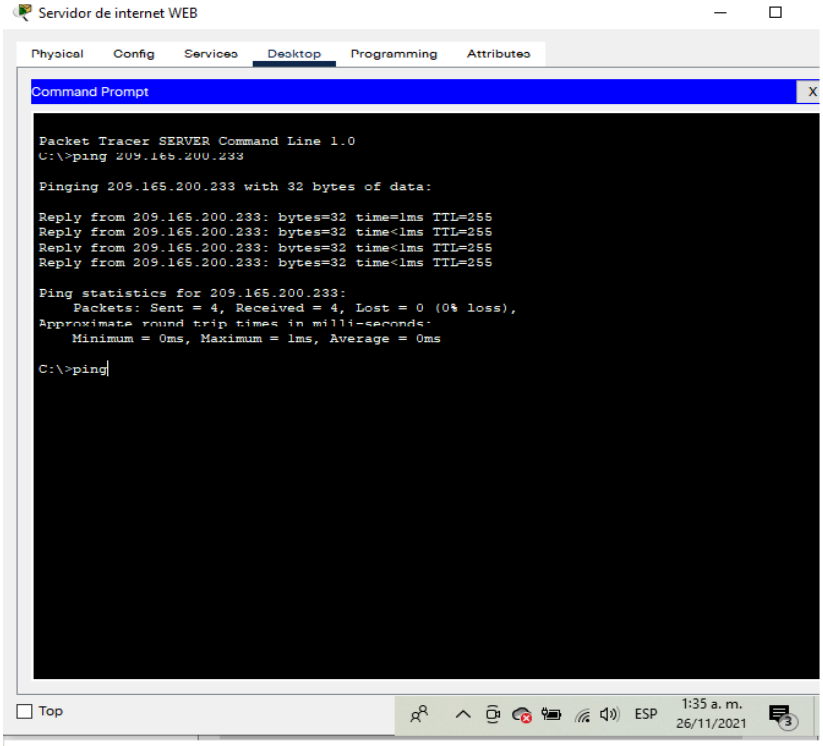
Fuente: Autoría Propia

Figura 14. Ping desde R2 a R3 a la S0/2/1



Fuente: Autoría Propia

Figura 15. Ping desde el servidor de internet a Gateway determinado



Fuente: Autoría 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:

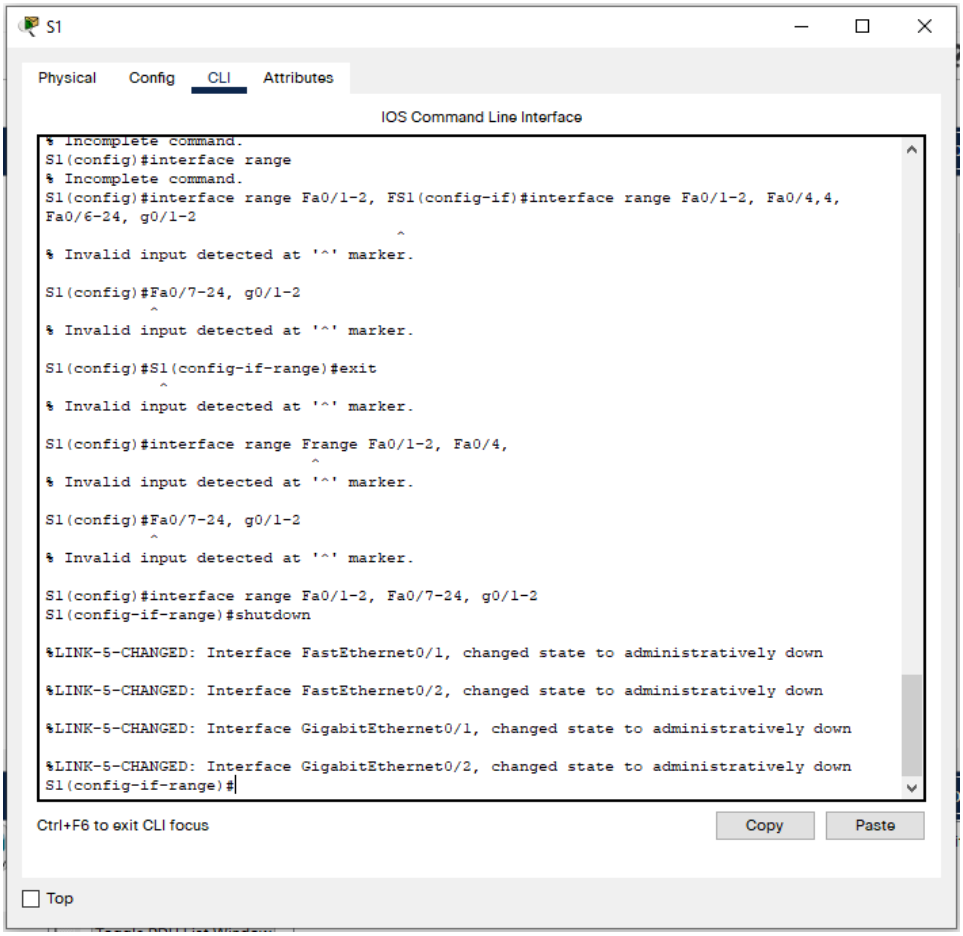
Tabla 15. Configuración seguridad del Switch 1 y routing entre Vlan

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1#configure terminal S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingeniería S1(config-vlan)#vlan 99 S1(config-vlan)#name Administración

Asignar la dirección IP de administración.	S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0
Asignar el Gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface Fa0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config)#interface Fa0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#interface range Fa0/1-2, Fa0/4, Fa0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if-range)#interface Fa0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#interface range Fa0/1-2, Fa0/4, Fa0/7-24, g0/1-2 S1(config-if-range)#shutdown

Fuente: Autoría Propia

Figura 16. Configuración seguridad del Switch 1 y routing entre Vlan



Fuente: Autoría Propia

Paso 2: Configurar el S3

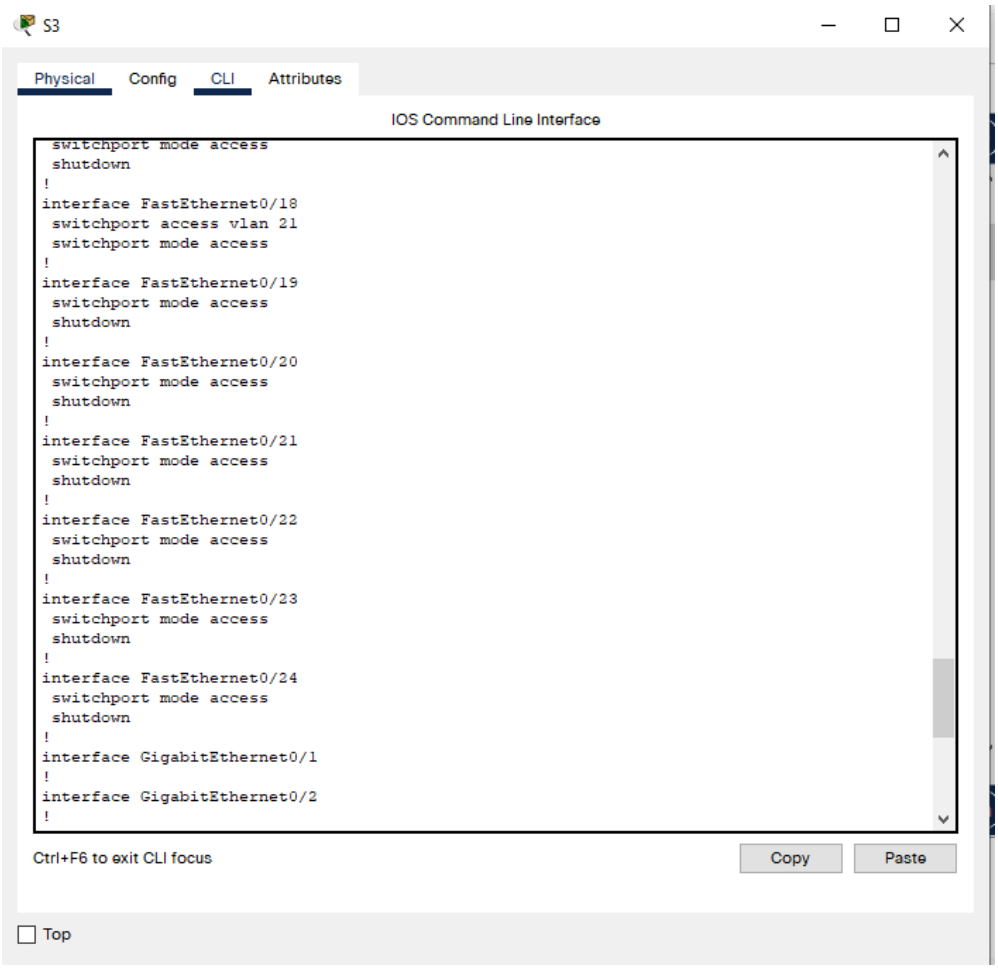
La configuración del S3 incluye las siguientes tareas:

Tabla 16. Configuración seguridad del Switch 3, routing entre Vlan

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	S3#configure terminal S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingeniería S3(config-vlan)#vlan 99 S3(config-vlan)#name Administración
Asignar la dirección IP de administración	S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#interface Fa0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#interface range Fa0/1-2, Fa0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 21	S3(config-if-range)#interface Fa0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#interface range Fa0/1-2, Fa0/4-17, Fa0/19-24, g0/1-2 S3(config-if-range)#shutdown

Fuente: Autoría Propia

Figura 17. Configuración seguridad del Switch 3, routing entre Vlan



Fuente: Autoría Propia

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17. Configuración Subinterfaz 802.1Q en el Router 1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#interface g0/1.21 R1(config-subif)#description Vlan 21 R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#interface g0/1.23 R1(config-subif)#description Vlan 23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config-subif)#interface g0/1.99 R1(config-subif)#description Vlan 99 R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)#interface g0/1 R1(config-if)#no shutdown

Fuente: Autoría 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:

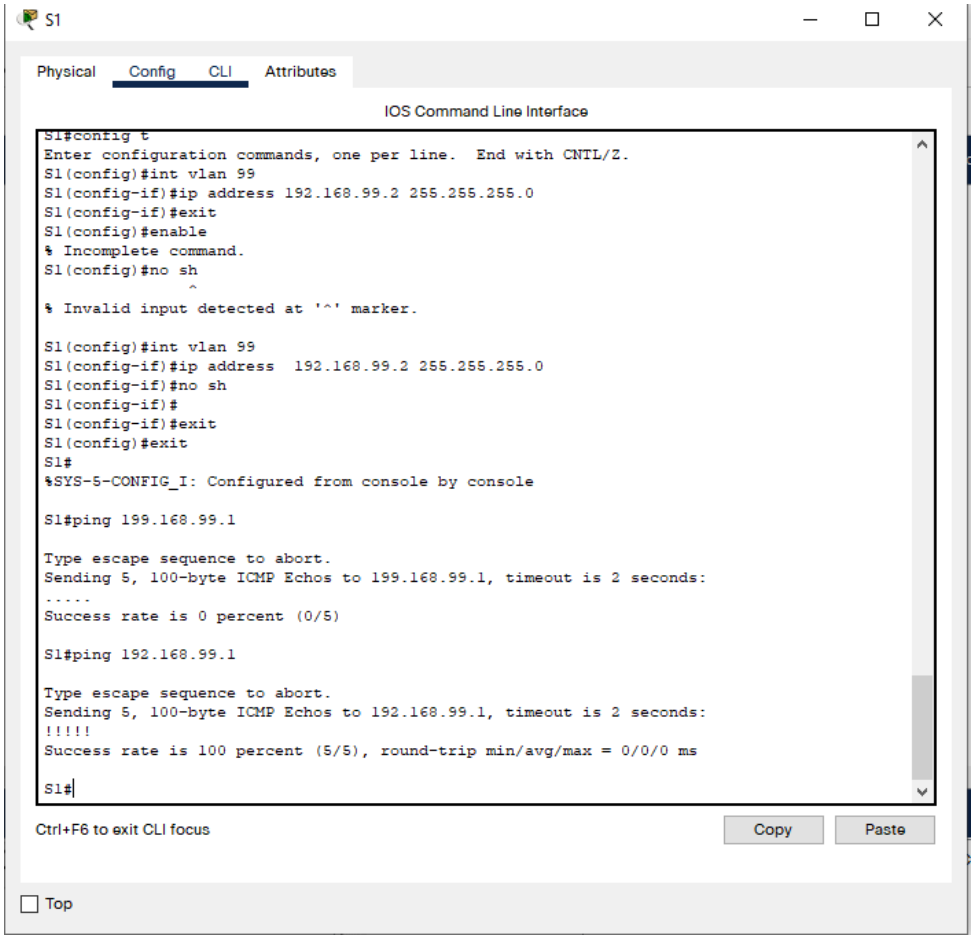
Tabla 18. Verificación de la conectividad en la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Exitoso

S3	R1, dirección VLAN 99	192.168.99.1	Exitoso
S1	R1, dirección VLAN 21	192.168.21.1	Exitoso
S3	R1, dirección VLAN 23	192.168.23.1	Exitoso

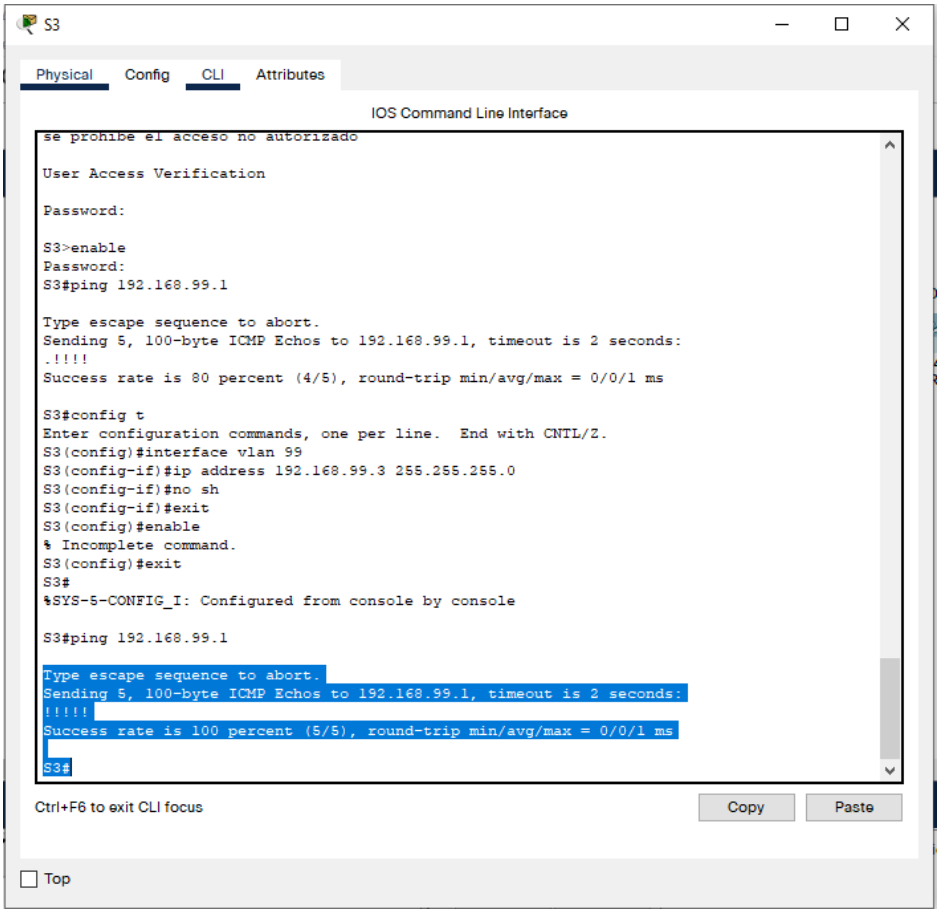
Fuente: Autoría Propia

Figura 18. Ping desde Switch 1 a la dirección VLAN 99



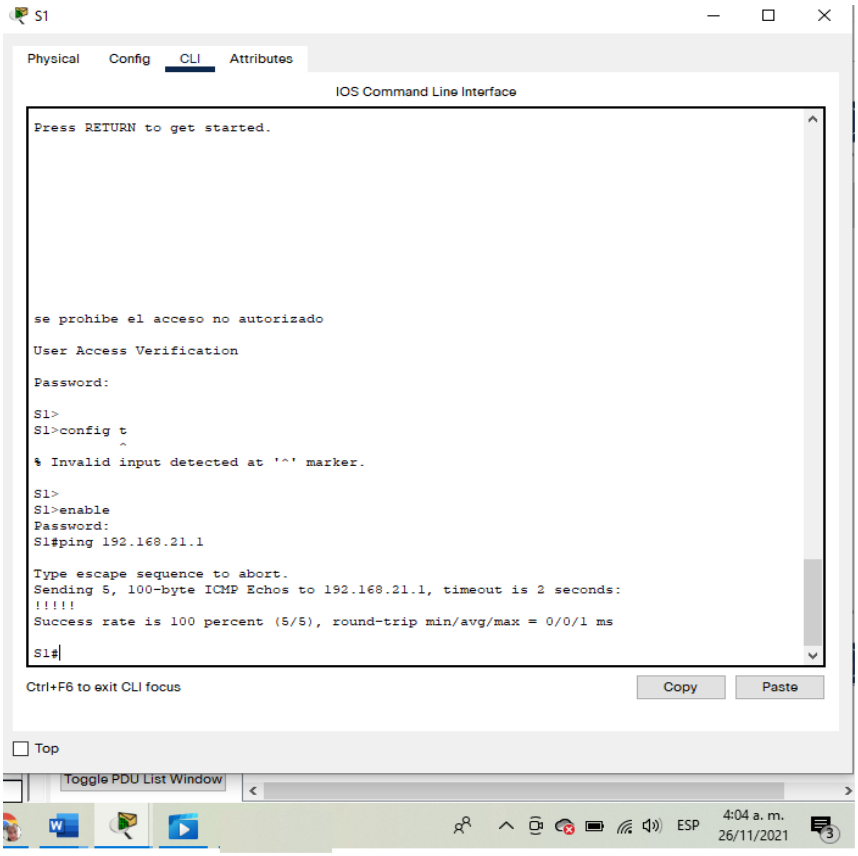
Fuente: Autoría Propia

Figura 19. Ping desde Switch 3 a la dirección VLAN 99



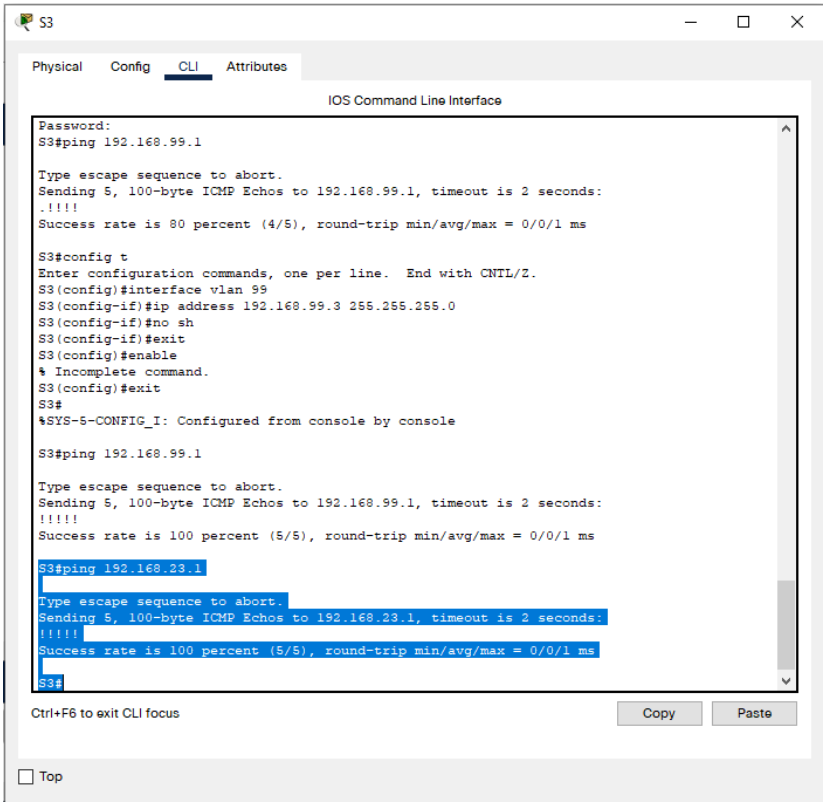
Fuente: Autoría Propia

Figura 20. Ping desde Switch 1 a la dirección VLAN 21



Fuente: Autoría Propia

Figura 21. Ping desde Switch 1 a la dirección VLAN 21



Fuente: Autoría 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:

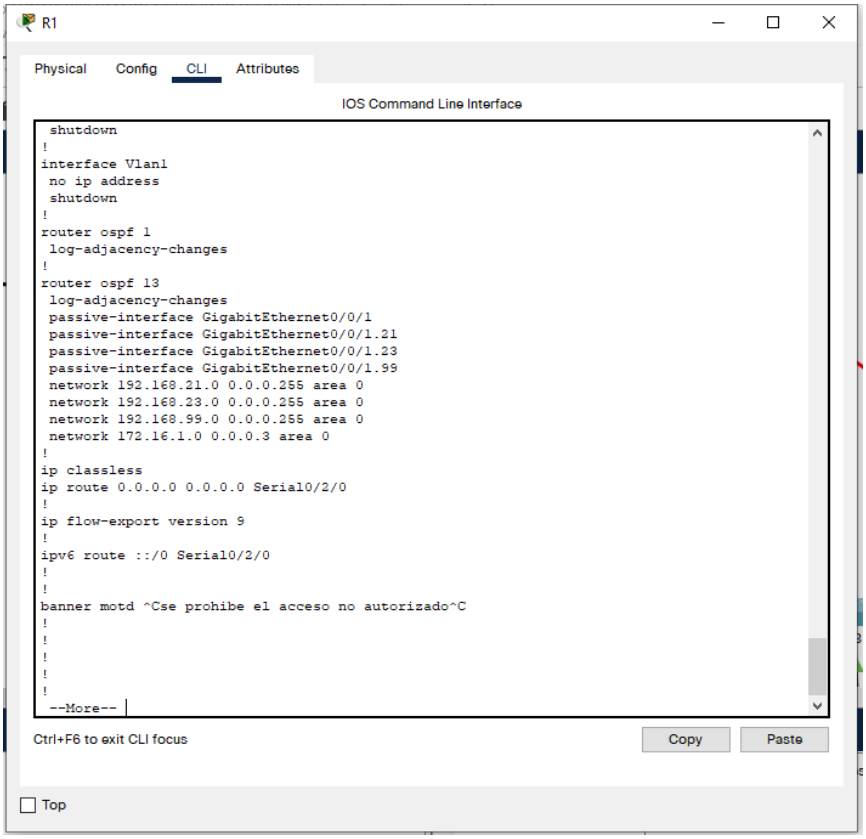
Tabla 19. Configuración del protocolo de routing dinámico OSPF en Router 1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 13

Anunciar las redes conectadas directamente	R1(config-router)# R1(config-router)#net 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)#net 172.16.1.0 0.0.0.3 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/0/1 R1(config-router)#passive-interface g0/0/1.21 R1(config-router)#passive-interface g0/0/1.23 R1(config-router)#passive-interface g0/0/1.99
Desactive la sumarización automática	**No se puede hacer en este sistema de enrutamiento, sólo se hace en rip y en EIGRP**

Fuente: Autoría Propia

Figura 22 Configuración del protocolo de routing dinámico OSPF en Router 1



Fuente: Autoría Propia

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

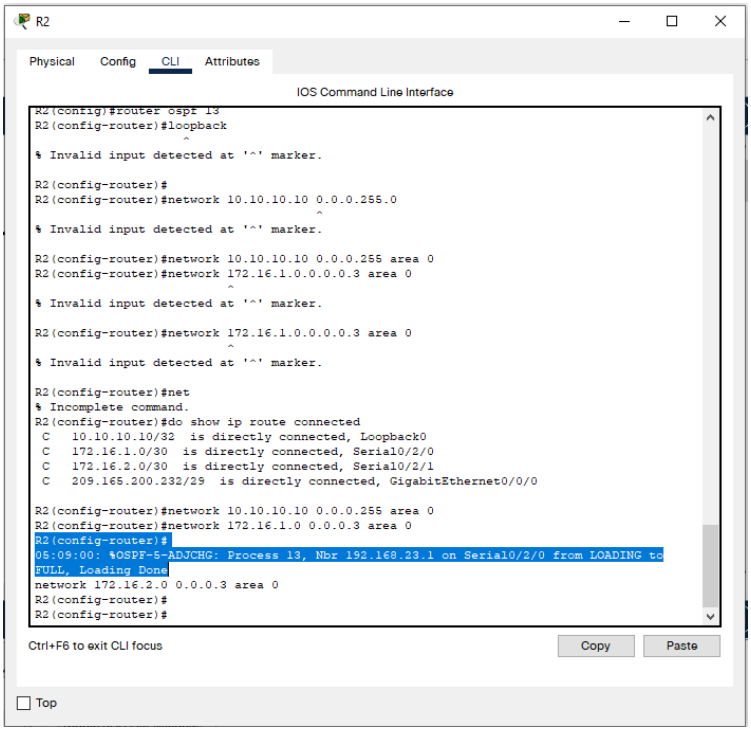
Tabla 20. Configuración del protocolo de routing dinámico OSPF en Router 2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2 (config)#router ospf 13 R2(config-router)#router-id 2.2.2.2

Anunciar las redes conectadas directamente	R2(config-router)#do show ip route connected R2(config-router)#network 10.10.10.10 0.0.0.255 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
Establecer todas las interfaces LAN como pasivas	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática	**No se puede hacer en este sistema de enrutamiento solo se hace en rip y en EIGRP**

Fuente: Autoría Propia

Figura 23 . Configuración del protocolo de routing dinámico OSPF en Router 2



Fuente: Autoría Propia

Paso 3: Configurar OSPFv3 en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 21. Configuración del protocolo de routing dinámico OSPF en Router 2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2 (config)#router ospf 13
Anunciar redes IPv4 conectadas directamente	**Error, esto debe ser para las redes bajo IPV6**
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	La loopback no tiene direcciones bajo IPV6
Desactive la sumarización automática.	En este protocolo eso no se realiza, en cambio se coloca la wildcard, en IPV6 no se hace.

Fuente: Autoría Propia

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 22. Configuración del protocolo de routing dinámico OSPF en Router 3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 13 R3(config-router)#router-id 2.2.2.2

Anunciar redes IPv4 conectadas directamente	R3(config-router)#do show ip route connected R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Fuente: Autoría Propia

Paso 4: Verificar la información de OSPF

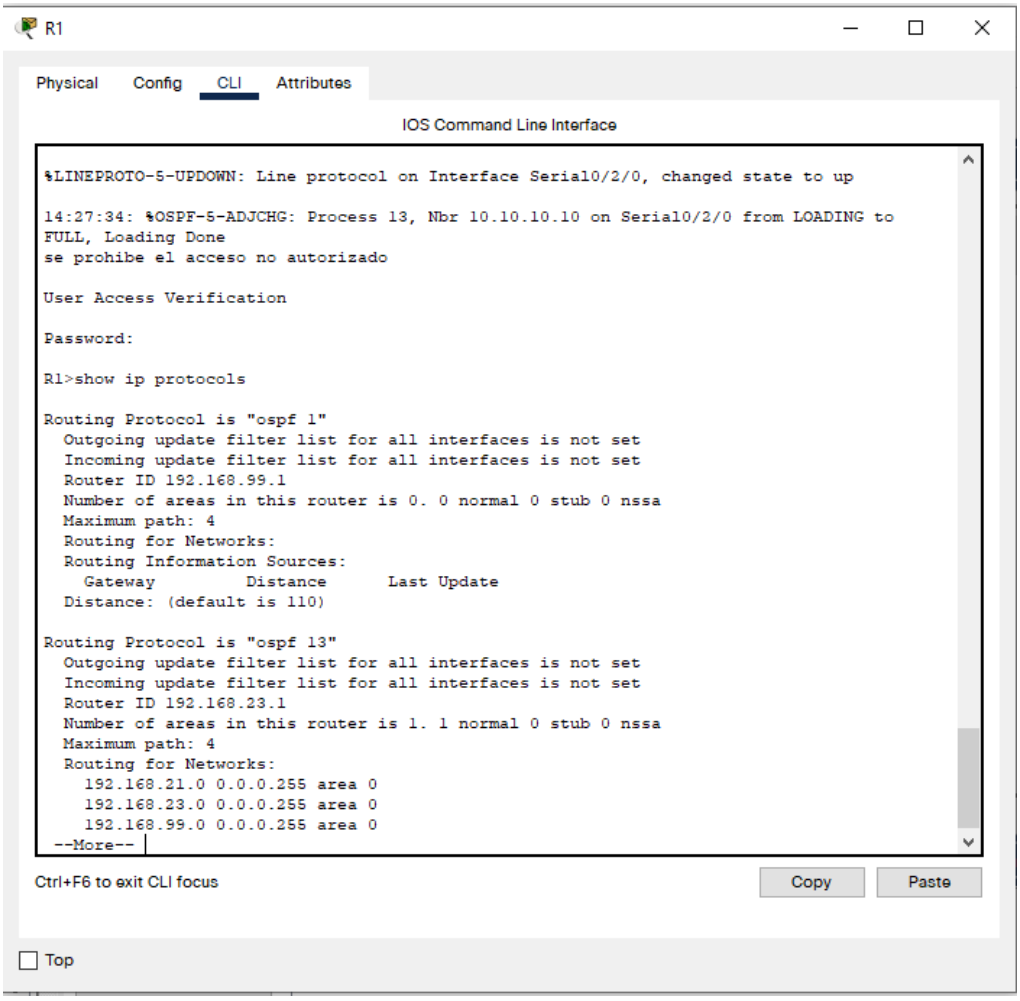
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 23. Verificación de la información del protocolo OSPF

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

Fuente: Autoría Propia

Figura 24 Verificar la información de OSPF



Fuente: Autoría Propia

Parte 5: Implementar DHCP y NAT para IPv4

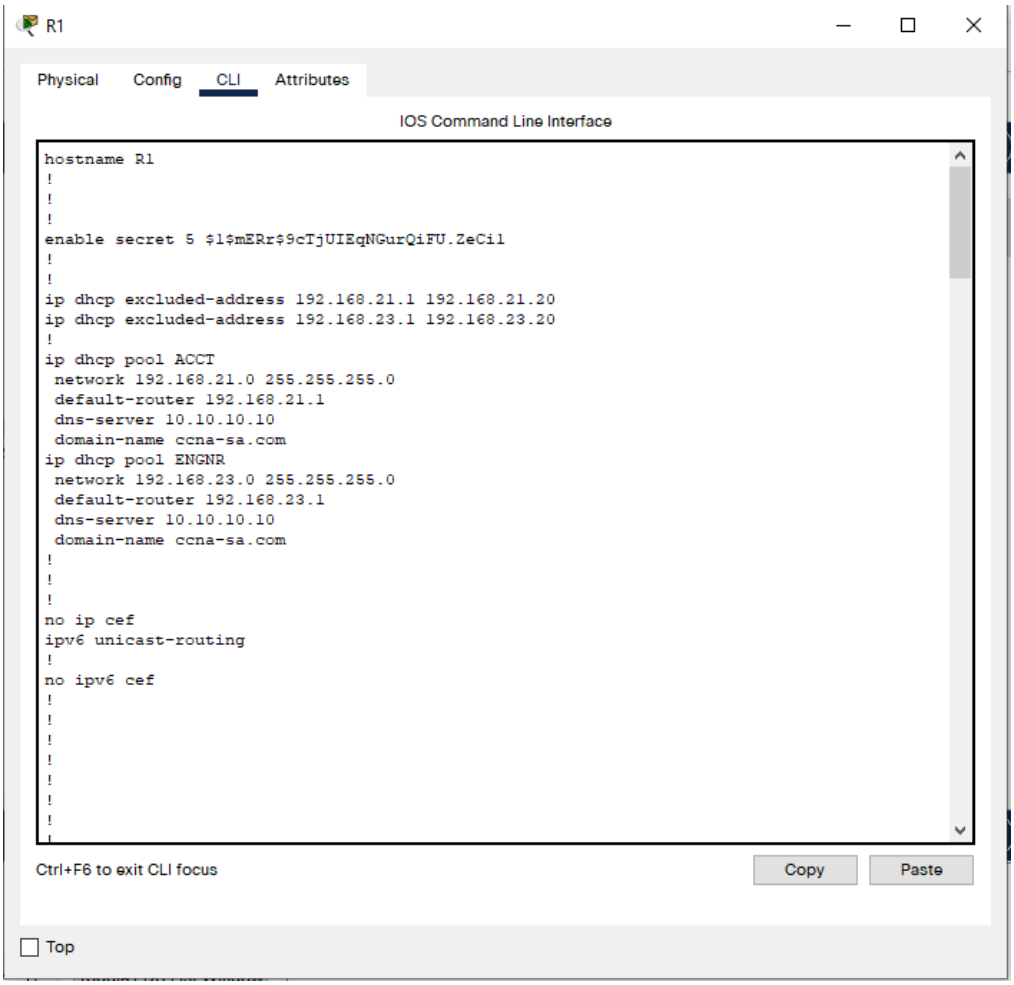
Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23 Las tareas de configuración para R1 incluyen las siguientes:

Tabla 24. Configuración del Router 1 como servidor DHCP

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23	R1(dhcp-config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1

Fuente: Autoría Propia

Figura. 25 Verificar la información de OSPF



Fuente: Autoría Propia

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

La configuración del R2 incluye las siguientes tareas:

Tabla 25. Configuración NAT estática y dinámica en Router 2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**	R2(config)#username webuser secret cisco12345 privilege 15
Habilitar el servicio del servidor HTTP	No Soportado en Packet Tracer
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	No soportado en Packet Tracer
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.233
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#interface s0/0/0 R2(config-if)#ip nat inside R2(config-if)#interface s0/0/1 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.0.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Fuente: Autoría Propia

Paso 3: Verificar el protocolo DHCP y la NAT estática

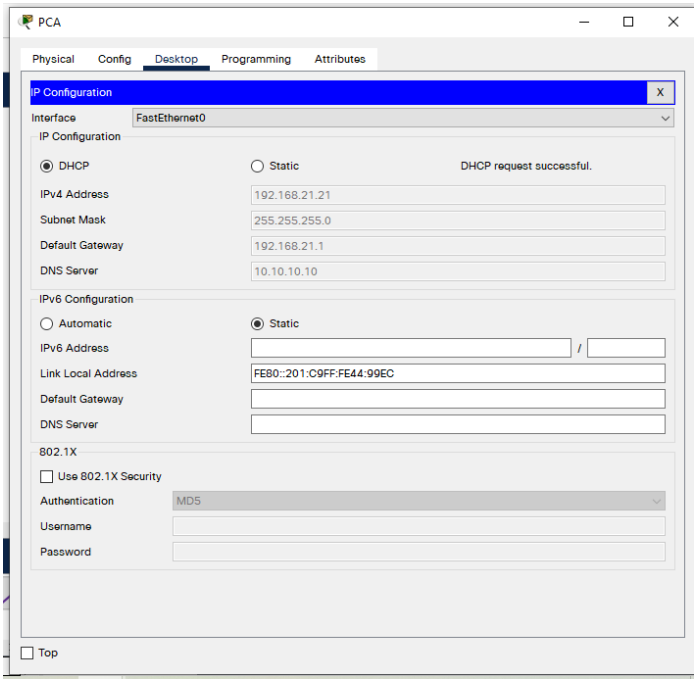
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 26. Verificación del protocolo DHCP y NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Si tiene información
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Si tiene información
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Si hay respuesta
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Si hay respuesta

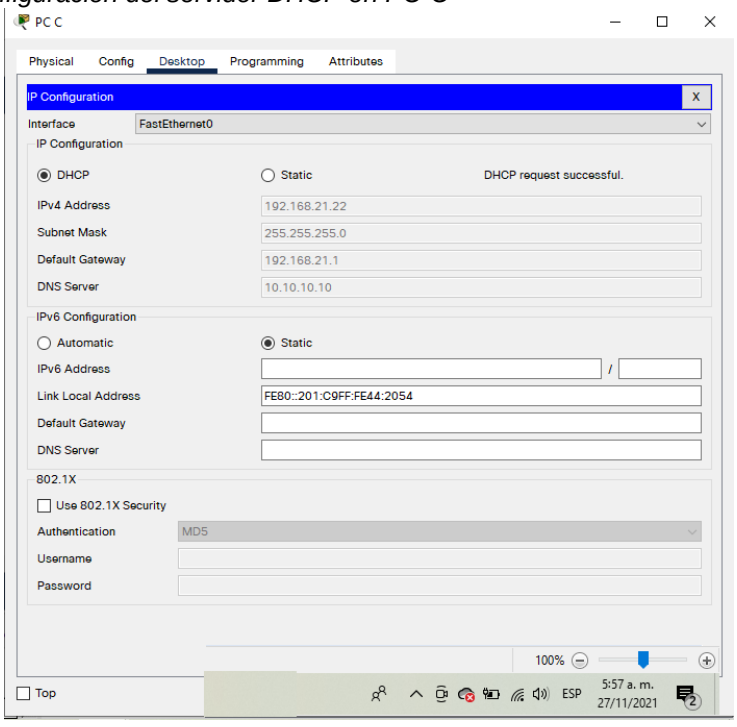
Fuente: Autoría Propia

Figura 26. Menú IP Configuración del servidor DHCP en PC-A



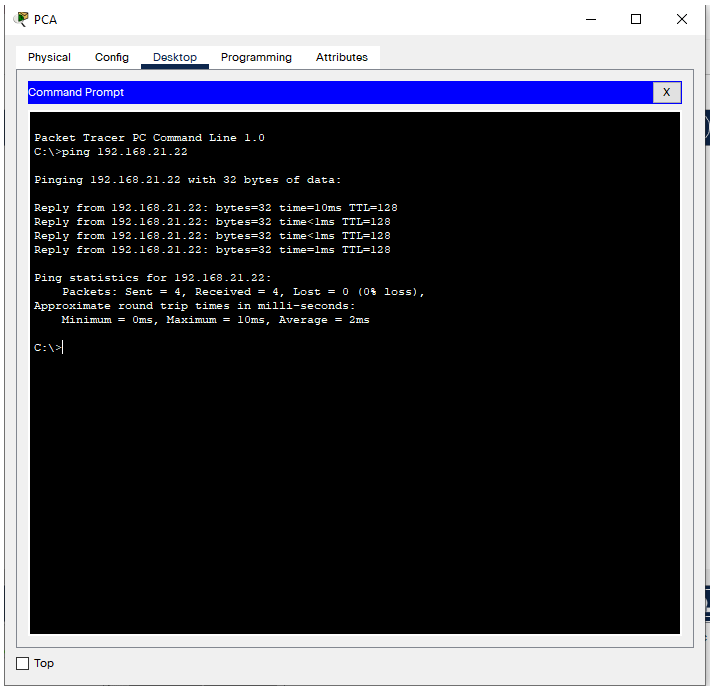
Fuente: Autoría Propia

Figura 27. Menú IP Configuración del servidor DHCP en PC-C



Fuente: Autoría Propia

Figura 28. Ping de la PC-A a la PC-C



Fuente: Autoría Propia

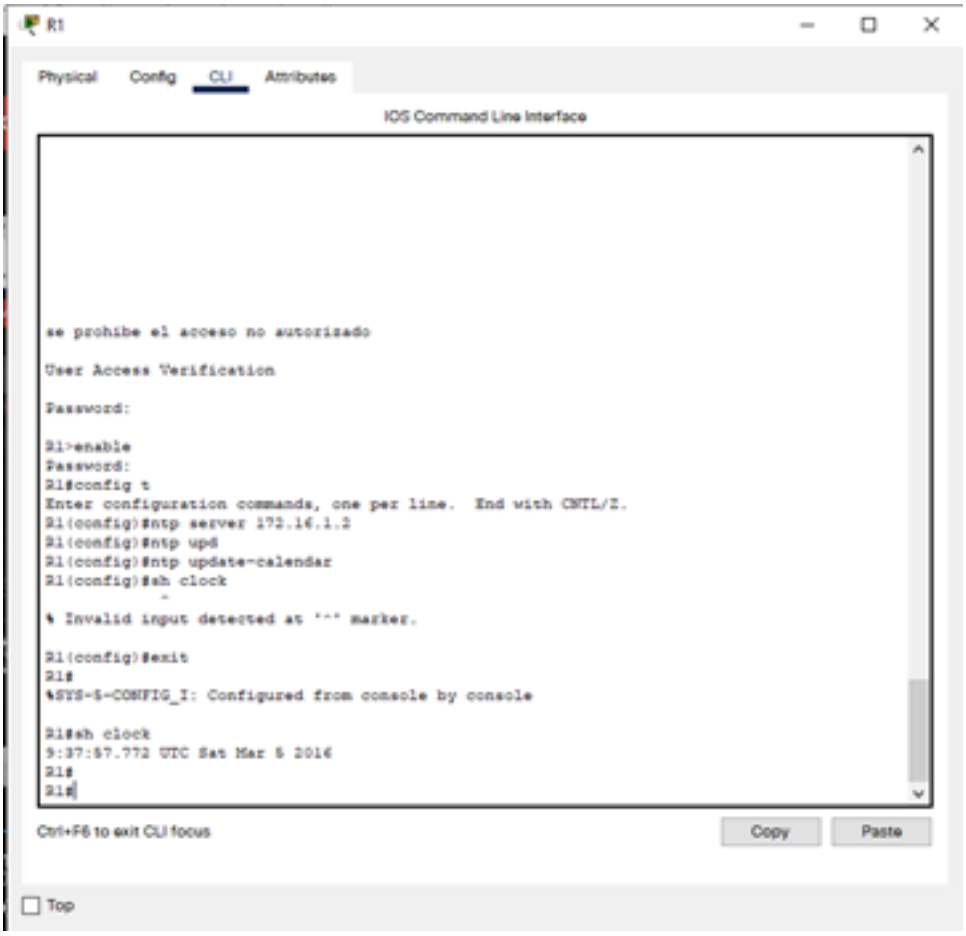
Parte 6: Configurar NTP

Tabla 27. Configuración NTP en Router 1.

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 05 March 2016
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	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: Autoría Propia

Figura 29. Configuración NTP en Router 1



Fuente: Autoría 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

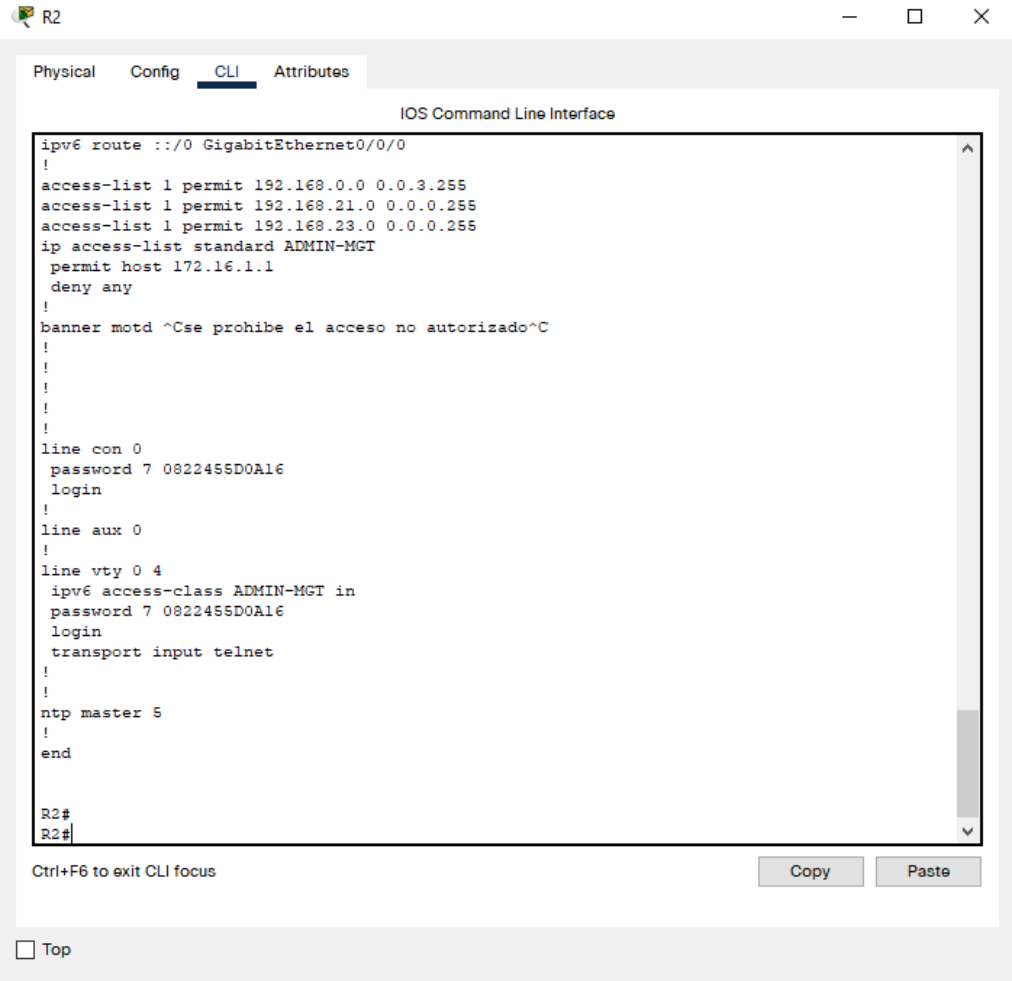
Tabla 28. Configuración NTP en Router 2.

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

Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2

Fuente: Autoría Propia

Figura 30. Restricción de acceso a líneas VTY en Router 2



Fuente: Autoría Propia

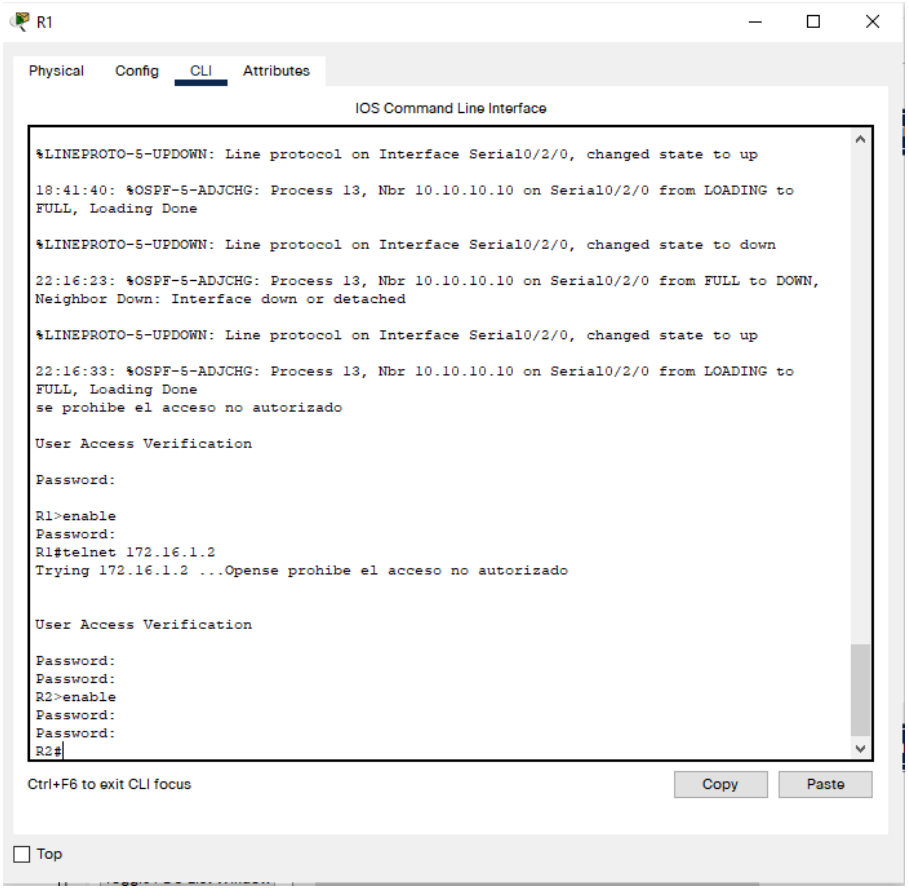
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 29. Verificación de configuración con comandos CLI

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list
Restablecer los contadores de una lista de acceso	R2#show access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation *

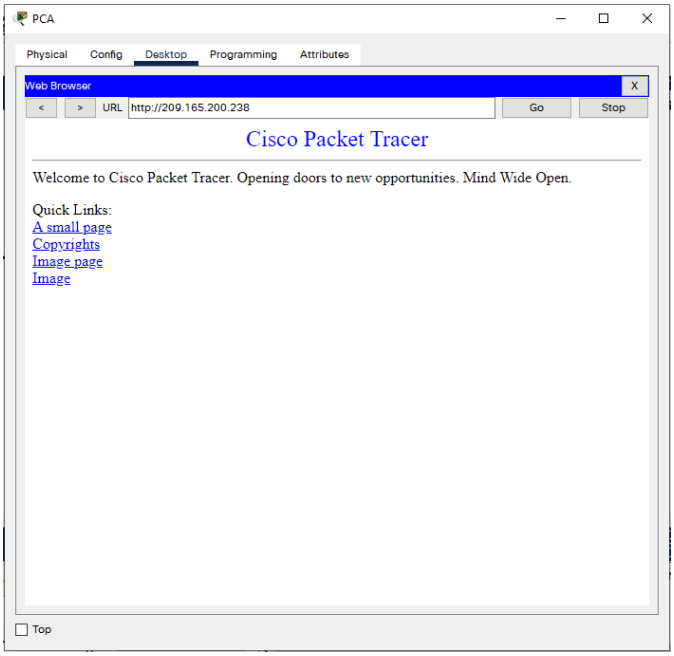
Fuente: Autoría Propia

Figura 31. Conexión remota de Router 1 a Router 2



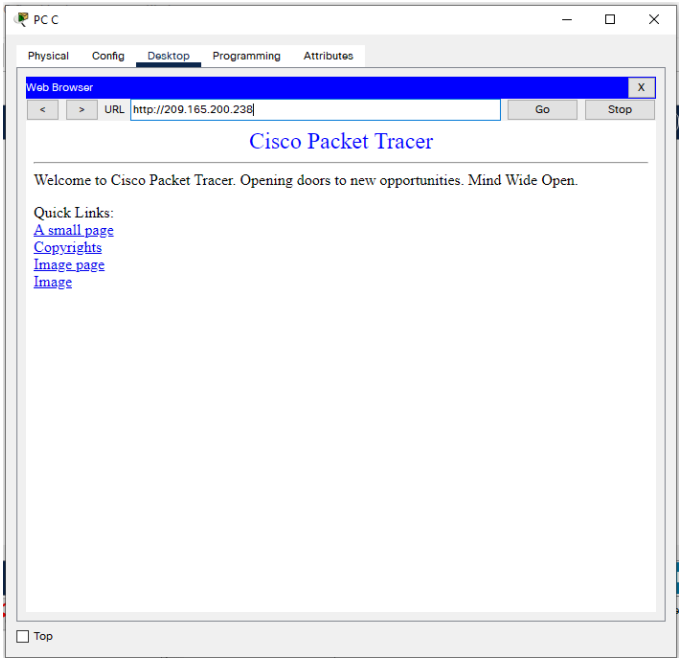
Fuente: Autoría Propia

Figura 32. Ping desde PC-A al servidor de Internet



Fuente: Autoría Propia

Figura 33. Desde PC-C Ping al servidor de Internet



Fuente: Autoría Propia

CONCLUSIONES

Sin lugar a dudas la expansión de la red global más grande conocida como “internet” ha proporcionado durante las últimas décadas los espacios de comunicación y acceso a la información a millones de personas, transformando su calidad de vida y la forma en que interactúan entre diferentes comunidades en las cuales las distancias geográficas son menos notables, gracias a la agilidad con la que los avances tecnológicos permiten llegar a más lugares.

El desarrollo del curso Diplomado de Profundización CISCO es un espacio de apoyo para profundizar las habilidades y competencias esenciales para diseñar y construir redes LAN/WAN, paralelamente a la configuración de los dispositivos que integran la infraestructura del direccionamiento IP.

Se alcanzó a desarrollar satisfactoriamente la configuración de los dos escenarios propuestos, en los cuales se logran identificar los protocolos de administración de red en el IOS; creando las respectivas VLANs, y verificando paralelamente la conectividad tanto en los dispositivos de enrutamiento y conmutación como en los Hosts que hacen parte de la topología.

A medida que se avanzaba en el entorno académico de la plataforma CISCO, se lograba simular un ambiente empresarial, en el que como futuros profesionales seremos capaces de tener las herramientas necesarias para el diseño, instalación y mantenimiento de redes pequeñas y con la experiencia que se adquiere poder transmitirlos a contextos de redes WAN.

BIBLIOGRAFÍA

CISCO. (2019). Acceso a la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4

CISCO. (2019). Capa de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

CISCO. (2019). Capa de transporte. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11

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

CISCO. (2019). Ethernet. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5

CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3