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

EDISON ARMANDO GARZON YARA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
IBAGUE-TOLIMA
2021

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

EDISON ARMANDO GARZON YARA

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

TUTOR: HECTOR MANUEL HERRERA HERRERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
IBAGUE-TOLIMA
2021

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Ibague, julio 19 de 2021

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

DHCP: El Protocolo de configuración dinámica de host (DHCP) es un protocolo de administración de red que se utiliza para automatizar el proceso de configuración de dispositivos en redes IP, lo que les permite utilizar servicios de red como DNS, NTP y cualquier protocolo de comunicación basado en UDP o TCP. Un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP. DHCP es una mejora de un protocolo anterior llamado BOOTP. DHCP es una parte importante de la solución DDI (DNS-DHCP-IPAM).

NAT: La **traducción de direcciones de red,** es un método para asignar un espacio de direcciones IP a otro mediante la modificación de la información de la dirección de red en el encabezado IP de los paquetes mientras se encuentran en tránsito a través de un dispositivo de enrutamiento de tráfico. La técnica se utilizó originalmente para evitar la necesidad de asignar una nueva dirección a cada host cuando se movía una red o cuando se reemplazaba el proveedor de servicios de Internet ascendente, pero no podía enrutar el espacio de direcciones de la red.

VLAN: Las LAN virtuales, son agrupaciones lógicas de dispositivos en el mismo dominio de transmisión. Las VLAN generalmente se configuran en conmutadores colocando algunas interfaces en un dominio de transmisión y algunas interfaces en otro. Cada VLAN actúa como un subgrupo de puertos de conmutador en una LAN Ethernet.

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

TRUNKING: En telecomunicaciones, el enlace troncal es una forma de proporcionar acceso a la red a muchos clientes compartiendo un conjunto de líneas o frecuencias en lugar de proporcionarlas individualmente.

OSPF: el protocolo OSPF (Open Shortest Path First) forma parte de una familia de protocolos de enrutamiento IP y es un protocolo de puerta de enlace interior (IGP) para Internet, que se utiliza para distribuir información de enrutamiento IP a través de un único sistema autónomo (AS) en una red IP.

RESUMEN

Las necesidades, requerimientos y exigencias de las nuevas tecnologías de la información, orientan indiscutiblemente al aprovechamiento de las herramientas que brindan un conocimiento, habilidades, destrezas y capacidades para manejar y configurar redes de datos.

El diplomado de profundización CISCO, permite desarrollar las habilidades practicas desde ambientes simulados, orientando el conocimiento a la solución de distintos escenarios que brindan las posibilidades de diagnosticar, configurar y solucionar problemas de redes, llevando finalmente a la realización de unas pruebas de habilidades que se desarrollan haciendo uso del simulador de redes “Packet Tracer” para este caso o GNS3 en otros.

En el desarrollo de los escenarios propuestos se plantea la configuración de diversos dispositivos que estructuran una red, desde configuraciones básicas esenciales, como procesos de encapsulamiento que otorgan garantías de seguridad a la información, creación de Vlan, redes locales y virtuales, protocolos DHCP y NAT, facilitando el uso de las direcciones IP dentro de rangos de direcciones establecidas previamente, así como la validación de conexiones que diagnostiquen el éxito de las configuraciones realizadas.

Palabras clave: Packet Tracer, GNS3, Vlan, DHCP, NAT, CISCO

ABSTRACT

The needs, requirements and demands of new information technologies undoubtedly guide the use of tools that provide knowledge, skills, abilities and capacities to manage and configure data networks.

The CISCO in-depth diploma allows to develop practical skills from simulated environments, directing knowledge to the solution of different scenarios that offer the possibilities of diagnosing, configuring and solving network problems, finally leading to the performance of skills tests that are developed using the network simulator "Packet Tracer" for this case or GNS3 in others.

In the development of the proposed scenarios, the configuration of various devices that structure a network is proposed, from essential basic configurations, such as encapsulation processes that provide security guarantees to the information, creation of Vlan, local and virtual networks, DHCP and NAT protocols. , facilitating the use of IP addresses within previously established ranges of addresses, as well as the validation of connections that diagnose the success of the configurations made.

Keywords: Packet Tracer, GNS3, Vlan, DHCP, NAT, CISCO

INTRODUCCIÓN

La realización de este trabajo brinda una gran oportunidad para adquirir conocimiento, habilidades y destrezas que permitan desarrollar las técnicas y los métodos para dar solución a problemas que puedan surgir al momento de la puesta en marcha de una red de informacion, con los dispositivos necesarios para modelar, diseñar, implementar y operar las herramientas tecnológicas que llevan a cabo el enrutamiento, tráfico y seguridad de la información para su procesamiento.

El manejo adecuado de esta información se ha convertido en un factor fundamental, que requiere de las garantías de seguridad e integridad de esos datos, mediante el recurso y talento humano, se lleva a cabo la construcción de las redes de información, conectando no solo equipos de cómputo u ordenadores, sino también diferentes dispositivos electrónicos que buscan su paso por las redes de información, destinados a finalmente transitar por la Internet. La simulación de redes ha estado evolucionando, en cuanto al uso de software para estas aplicaciones, la herramienta de simulación de Cisco Packet Tracer, nos permite crear topologías de red, con múltiples representaciones virtualmente muy cercanas a un entorno físico. Principalmente esta herramienta que nos permite crear topologías, configurar dispositivos, insertar, enviar, enrutar y seguir paquetes de datos, simula de forma muy didáctica el funcionamiento y uso de la red.

Este trabajo se realizó mediante un proceso paso a paso de las configuraciones requeridas, necesarias para poder implementar la simulación del escenario 1, aplicando la configuración inicial, y el enrutamiento para los Router, donde se le asigna nombre y protocolo de comunicación. Y por ende en esta primera simulación del escenario 1. Se realizo la configuración del Router y Switch 1 y 2 en este proceso se tuvo que tener en cuenta dos versiones tanto IPV4 y IPV6 para interconectar la PC -A y la PC- B, para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 y se puedan realizar las validaciones mediante el uso del comando “ping”, además también es una característica de suma importancia, poder garantizar la seguridad del router, a través de la creación de cuentas de usuarios y la asignación de contraseñas secretas para habilitar router, line de consola, línea terminal virtual. En el escenario 2 se realizará la configuración de OPSF, para lo cual básicamente se deben primero inicializar los routers y los switches, posteriormente proceder a la configuración de los Routers siguiendo el paso a paso. Finalmente, se configuran los

switches, realizando toda la conectividad del escenario en el simulador Packet Tracer. Se configurará la seguridad del switch, las VLAN y el routing entre VLAN de cada switch, así como también el protocolo de routing dinámico OSPF, se implementará DHCP y NAT para ipv4, mediante los comandos por el entorno de CLI adecuado y que se necesita para la práctica de cada unas de las instrucciones y soluciones a desarrollar.

1. Descripción de escenarios propuestos para la prueba dehabilidades

1.1 Escenario 1

Topología

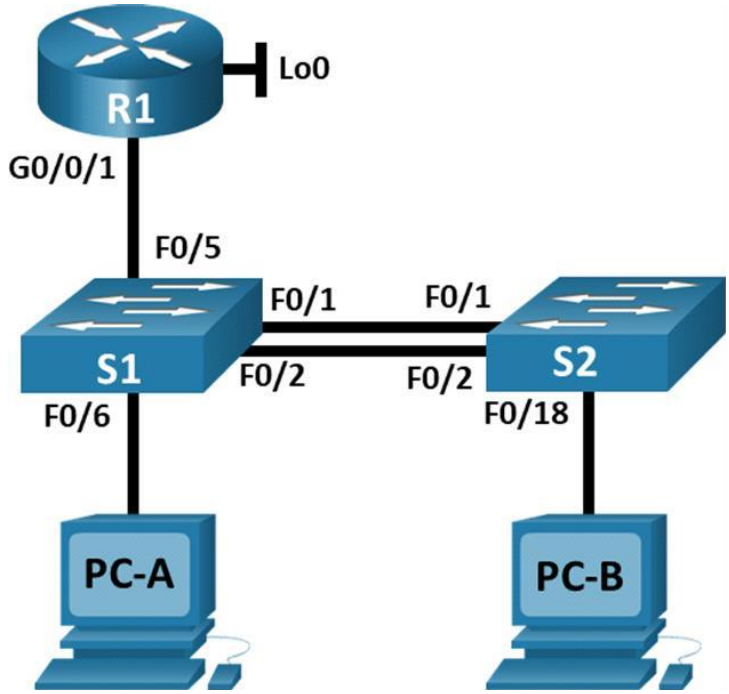

Figura 1. Topología escenario 1.
Fuente: Documento Cisco

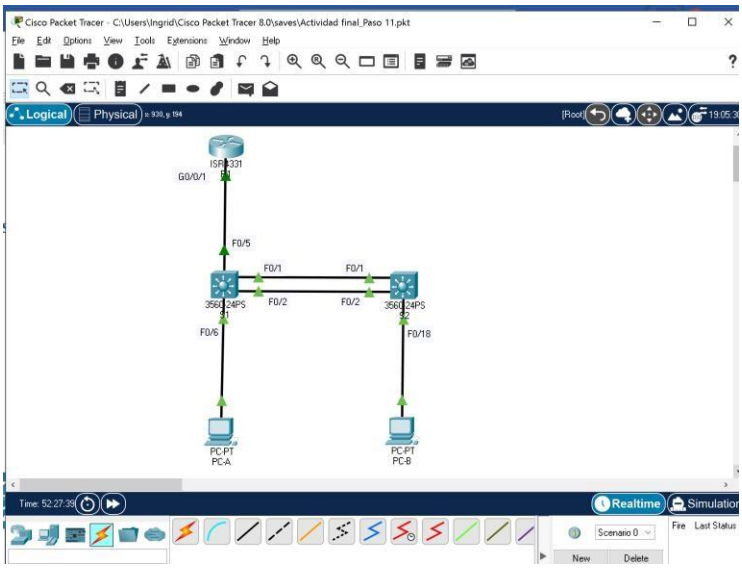

Figura 2. Simulación escenario 1 – Packet Tracer.
Fuente: Autor

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch también deben administrarse de forma segura. Configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Tabla 1. VLAN's

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

Tabla 2. Asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.21.5.1 /26	No corresponde
	2001:db5:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.21.5.65 /27	No corresponde
	2001:db5:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.21.5.97 /29	No corresponde
	2001:db5:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.21.5.98 /29	10.21.5.97
	2001:db5:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.21.5.99 /29	10.21.5.97
	2001:db5:acad:c: :99 /64	No corresponde

	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db5:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db5:acad:b: :50 /64	fe80::1

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

1.1.2 Parte 1: Inicializar y Recargar y Configurar aspectos básicos de los dispositivos

1.1.2.1 Paso 1: Inicializar y volver a cargar el router y el switch

- Borre las configuraciones de inicio y las VLAN del router y delswitch y vuelva a cargar losdispositivos.

Router>enable

Router#erase startup-config

Router#reload

Switch0>enable

Switch0#erase startup-config

Switch0# show vlan brief

Switch0#reload

Switch1>enable

Switch1#erase startup-config

Switch1#show vlan brief

Switch1#reload

Se verifica con el comando "**show vlan brief**" la existencia de vlan para eliminar si es el caso (No aplica).

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

Switch0#show sdm prefer

Switch0#config t

Switch0(config)#sdm prefer dual-ipv4-and-ipv6 routing

Switch0(config)#exit

Switch0#

Switch0#reload

Switch0#show sdm prefer

The current template is "desktop IPv4 and IPv6 routing" template.

The selected template optimizes the resources in

the switch to support this level of features for

8 routed interfaces and 1024 VLANs.

number of unicast mac addresses: 1.5K

number of IPv4 IGMP groups + multicast routes: 1K

number of IPv4 unicast routes: 2.75K

number of directly-connected IPv4 hosts: 1.5K

number of indirect IPv4 routes: 1.25K

number of IPv6 multicast groups: 1.125k

number of directly-connected IPv6 addresses: 1.5K

number of indirect IPv6 unicast routes: 1.25K

number of IPv4 policy based routing aces: 0.25K

number of IPv4/MAC qos aces: 0.5K

number of IPv4/MAC security aces: 0.5K

number of IPv6 policy based routing aces: 0.25K

number of IPv6 qos aces: 0.625k

number of IPv6 security aces: 0.5K

Switch1#show sdm prefer

Switch1#config t

Switch1(config)#sdm prefer dual-ipv4-and-ipv6 routing

Switch1(config)#exit

Switch1#

Switch1#reload

Switch1#show sdm prefer

The current template is "desktop IPv4 and IPv6 routing" template.

The selected template optimizes the resources in

the switch to support this level of features for

8 routed interfaces and 1024 VLANs.

number of unicast mac addresses: 1.5K

number of IPv4 IGMP groups + multicast routes: 1K

number of IPv4 unicast routes: 2.75K

number of directly-connected IPv4 hosts: 1.5K

number of indirect IPv4 routes: 1.25K

number of IPv6 multicast groups: 1.125k

number of directly-connected IPv6 addresses: 1.5K

number of indirect IPv6 unicast routes: 1.25K

number of IPv4 policy based routing aces: 0.25K

number of IPv4/MAC qos aces: 0.5K

number of IPv4/MAC security aces: 0.5K

number of IPv6 policy based routing aces: 0.25K

number of IPv6 qos aces: 0.625k

number of IPv6 security aces: 0.5K

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

1.1.2.2 Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3. Configuracion de R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure t 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 EXECprivilegiado	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config)#line con 0 R1(config-line)#password ciscoenpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base dedatos local	R1(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTYpara que use la base de	R1(config)#line vty 0 15 R1(config-line)#login local

datos local	
Configurar VTY solo aceptando SSH	R1(config-line)#transport input ssh R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd #*****ACCESO NO AUTORIZADO*****#
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	R1>enable Password: R1#config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#int g0/0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description vlan Bikes R1(config-subif)#ip address 10.21.5.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db5:acad:a::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#exit R1(config)#int g0/0/01.3 R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#description vlan Trikes R1(config-subif)#ip address 10.21.5.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db5:acad:b::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#exit R1(config)#int g0/0/01.4 R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#description vlan Management R1(config-subif)#ip address 10.21.5.97 255.255.255.248

	R1(config-subif)#ipv6 address 2001:db5:acad:c::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#exit R1(config)#int g0/0/01.6 R1(config-subif)#encapsulation dot1q 6 R1(config-subif)#description vlan Native R1(config-subif)#exit R1(config)#int g0/0/1 R1(config-if)#no shut
Configure el Loopback0 interface	R1(config-if)# R1(config-if)#int loopback 0 R1(config-if)# R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db5:acad:209::1/64 R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#description Internet R1(config-if)#exit
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024 R1(config)#

1.1.2.3 Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tabla 4. Configuración de S1

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch0#config t Switch0(config)#no ip domain lookup
Nombre del switch	Switch0>enable Switch0(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 console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	S1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para queuse la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local S1(config-line)#exit
Configurar las líneas VTY para que acepten únicamentelas conexiones SSH	S1(config)#line vty 0 15 S1(config-line)#transport input ssh S1(config-line)#login local S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd #*****ACCESO NO AUTORIZADO*****#
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024
Configurar la interfaz de administración (SVI)	S1(config)#int vlan 4 S1(config-if)#ip addres 10.21.5.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db5:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#description vlan Management S1(config-if)#no shut S1(config-if)#exit
Configuración del gateway predeterminado	S1(config)#ip default-gateway 10.21.5.97 S1(config)#

Tabla 5. Configuración de S2

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch1>enable Switch1#config t Switch1(config)#no ip domain lookup
Nombre del switch	Switch1>enable Switch1(config)#hostname S2
Nombre de dominio	S2(config)#ip domain-name CCNA-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit
Crear un usuario administrativo en la base de datos local	S2(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para queuse la base de datos local	S2(config)#line vty 0 15 S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamentelas conexiones SSH	S2(config-line)#transport input ssh S2(config-line)#login local S2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption
Configurar un MOTD Banner	S2(config)#banner motd #*****ACCESO NO AUTORIZADO*****#
Generar una clave de cifrado RSA	S2(config)#crypto key generate rsa How many bits in the modulus [512]: 1024
	S2(config)#int vlan 4 S2(config-if)#ip address 10.21.5.99 255.255.255.248 S2(config-if)#ipv6 address 2001:db5:acad:c::99/64

Configurar la interfaz de administración (SVI)	S2(config-if)#ipv6 addres fe80::99 link-local S2(config-if)#description vlan Management S2(config-if)#no shut S2(config-if)#exit
Configuración del gateway predeterminado	S2(config)#default-gateway 10.21.5.97 S1(config)#

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

1.1.3.1 Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 6. Configuración de infraestructura de red (VLAN, Trunking, EtherChannel) en S1

Tarea	Especificación
Crear VLAN	S1>enable Password: S1#config t Enter configuration commands, one per line. End with CNTL/Z. S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#vlan 4 S1(config-vlan)# S1(config-vlan)#name Management S1(config-vlan)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#vlan 6

	S1(config-vlan)#name Native S1(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S1(config)#interface fa0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config)#int range f0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)# S1(config-if-range)#int Port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1(config)#interface range fa0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#interface Port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6
Configurar el puerto de acceso de host para VLAN 2	S1(config-if)#int f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2
Configurar la seguridad del puerto en los puertos deacceso	S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas	S1(config-if)#int range f0/3-4 S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description No utilizada S1(config-if-range)#shut S1(config-if-range)#int range f0/7-24 S1(config-if-range)#switchport access vlan 5

	S1(config-if-range)#description No utilizada S1(config-if-range)#shut S1(config-if-range)#int range g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description No utilizada S1(config-if-range)#shut S1(config-if-range)#

1.1.3.2 Paso 2: Configure el S2.

Entre las tareas de configuración de S2 se incluyen las siguientes:

Tabla 7. Configuración de infraestructura de red (VLAN, Trunking, EtherChannel) en S2

Tarea	Especificación
Crear VLAN	S2>enable S2#configure terminal S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#vlan 4 S2(config-vlan)#name Management S2(config-vlan)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#vlan 6 S2(config-vlan)#name Native S2(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S2(config)#interface range fa0/1-2 S2(config-if-range)#shutdown S2(config-if-range)#switchport trunk encapsulation dot1q

	S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2que use interfaces F0/1 y F0/2	S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#interface Port-channel 1 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6
Configurar el puerto de acceso del host para la VLAN 3	S2(config-if)# interface fa0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configure port-security en los access ports	S2(config-if)#switchport port-security maximum 3
Asegure todas las interfaces no utilizadas.	S2(config-if)#interface range fa0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description No esta en uso S2(config-if-range)#shutdown S2(config-if-range)#interface range fa0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description No esta en uso S2(config-if-range)#shutdown

Tabla 8. Activación interfaces fa0/1-2 en s1 y S2

Tarea	Especificación
Activar el rango fa0/1-2 en switch 1	S1(config)#interface range fa0/1-2 S1(config-if-range)#interface range fa0/1-2 S1(config-if-range)#no shutdown

Activar el rango fa0/1-2 en switch 2	S2(config)#interface range fa0/1-2 S2(config-if-range)#interface range fa0/1-2 S2(config-if-range)#no shutdow

1.1.4 Parte 3: Configurar soporte de host

1.1.4.1 Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 9. Configuración de soporte de host en R1

Tarea	Especificacion
Configure Default Routing	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0
Configurar IPv4 DHCP para VLAN 2	R1(config)#ip dhcp excluded-address 10.21.5.1 10.21.5.52 R1(config)#ip dhcp pool vlan2-Bikes R1(dhcp-config)#network 10.21.5.0 255.255.255.192 R1(dhcp-config)#default-router 10.21.5.1 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#exit
Configurar DHCP IPv4 para VLAN 3	R1(config)#ip dhcp excluded-address 10.21.5.65 10.21.5.84 R1(config)#ip dhcp pool vlan3-Trikes R1(dhcp-config)#network 10.21.5.64 255.255.255.224 R1(dhcp-config)#default-router 10.21.5.65 R1(dhcp-config)#domain-name ccna-b.net

	R1(dhcp-config)#exit

1.1.4.2 Paso 2: Configurar los servidores

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

Tabla 10. Configuración del PC-A

PC-A Network Configuration	
Descripción	DHCP
Dirección física	0002.4A0C.2376
Dirección IP	10.21.5.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.21.5.1
Gateway predeterminado IPv6	FE80::1

Tabla 11. Configuración del PC-B

Configuración de red de PC-B	
Descripción	DHCP
Dirección física	0002.17E0.0C3C
Dirección IP	10.21.5.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.21.5.65
Gateway predeterminado IPv6	FE80::1

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

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

Nota: Si fallan los pings en las computadoras host, desactive temporalmente el firewall de lacomputadora y vuelva a realizarla prueba.

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

Tabla 12. Validacion de conexión dispositivos de red.

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.21.5.1	Exitoso
		IPv6	2001:db5:acad:a: :1	Exitoso
	R1, G0/0/1.3	Dirección	10.21.5.65	Exitoso
		IPv6	2001:db5:acad:b: :1	Exitoso
	R1, G0/0/1.4	Dirección	10.21.5.97	Exitoso
		IPv6	2001:db5:acad:c: :1	Exitoso
	S1, VLAN 4	Dirección	10.21.5.98	Exitoso
		IPv6	2001:db5:acad:c: :98	No se establece
	S2, VLAN 4	Dirección	10.21.5.99.	Exitoso
		IPv6	2001:db5:acad:c: :99	No se establece
	PC-B	Dirección	IP address will vary.	Exitoso
		IPv6	2001:db5:acad:b: :50	Exitoso
	R1 Bucle 0	Dirección	209.165.201.1	Exitoso

Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db5:acad:209: :1	Exitoso
PC-B	R1 Bucle 0	Dirección	209.165.201.1	Exitoso
		IPv6	2001:db5:acad:209: :1	Exitoso
	R1, G0/0/1.2	Dirección	10.21.5.1	Exitoso
		IPv6	2001:db5:acad:a: :1	Exitoso
	R1, G0/0/1.3	Dirección	10.21.5.65	Exitoso
		IPv6	2001:db5:acad:b: :1	Exitoso
	R1, G0/0/1.4	Dirección	10.21.5.97	Exitoso
		IPv6	2001:db5:acad:c: :1	Exitoso
	S1, VLAN 4	Dirección	10.21.5.98	Exitoso

		IPv6	2001:db5:acad:c: :98	No se establece
	S2, VLAN 4	Dirección	10.21.5.99.	Exitoso
		IPv6	2001:db5:acad:c: :99	No se establece

Pings desde PC-A

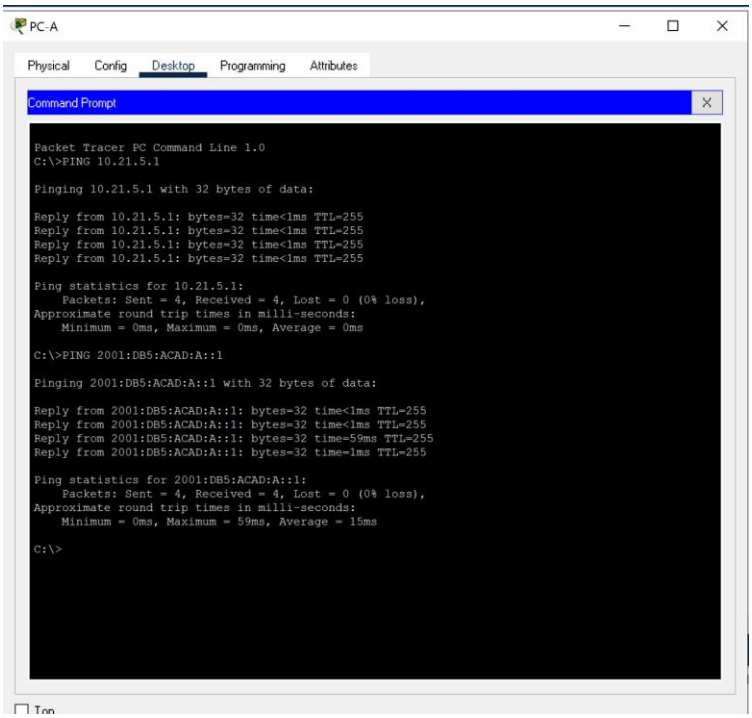

Figura 3. Ping de PC-A a R1, G0/0/1.2.
Fuente: Autor

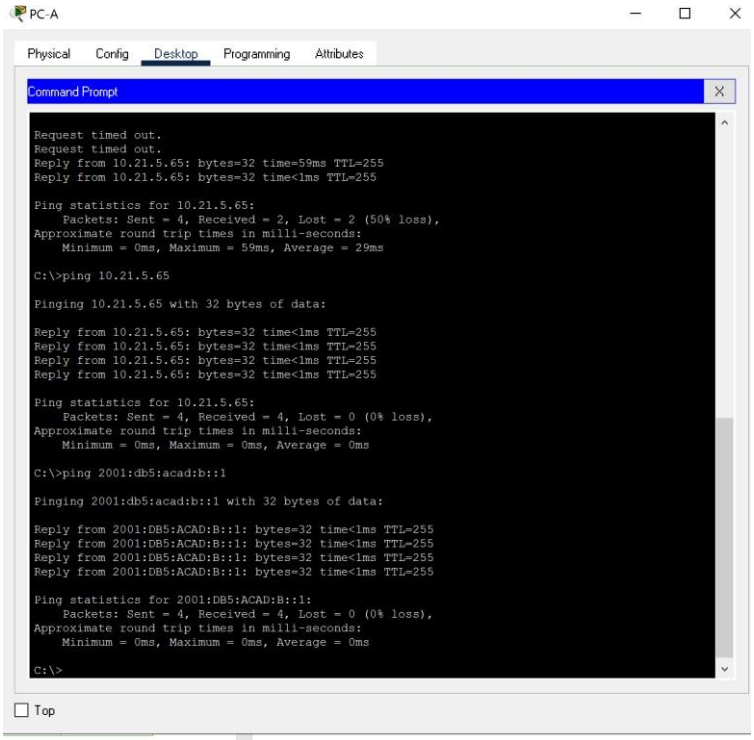

Figura 4. Ping de PC-A a R1, G0/0/1.3.
Fuente: Autor

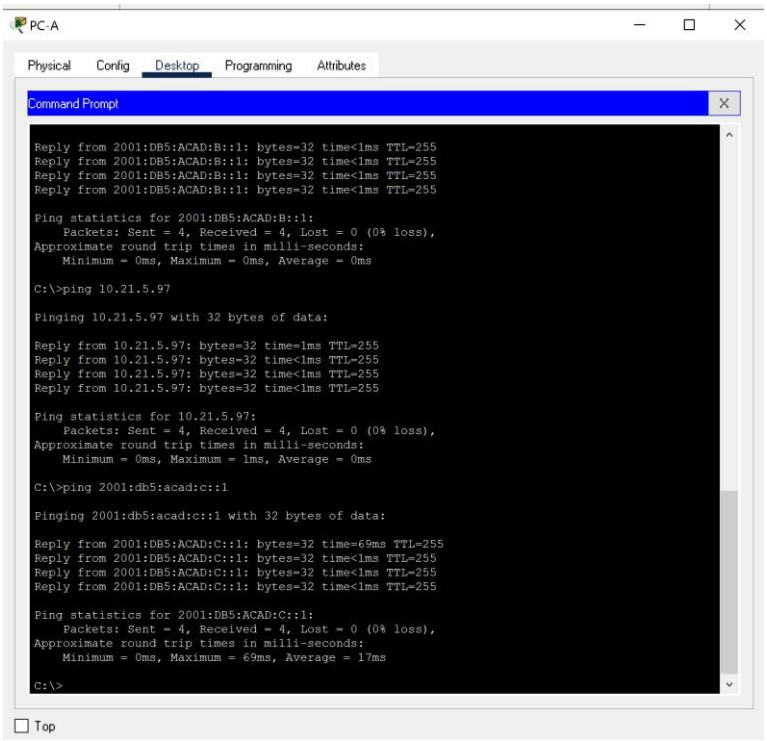

Figura 5. Ping de PC-A a R1, G0/0/1.4.
Fuente: Autor

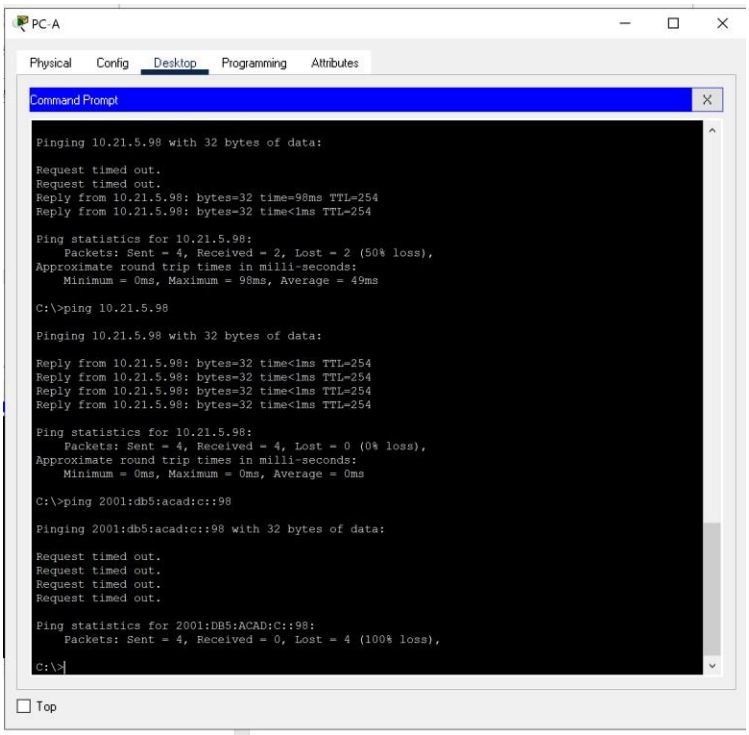

Figura 6. Ping de PC-A a S1, VLAN 4.
Fuente: Autor

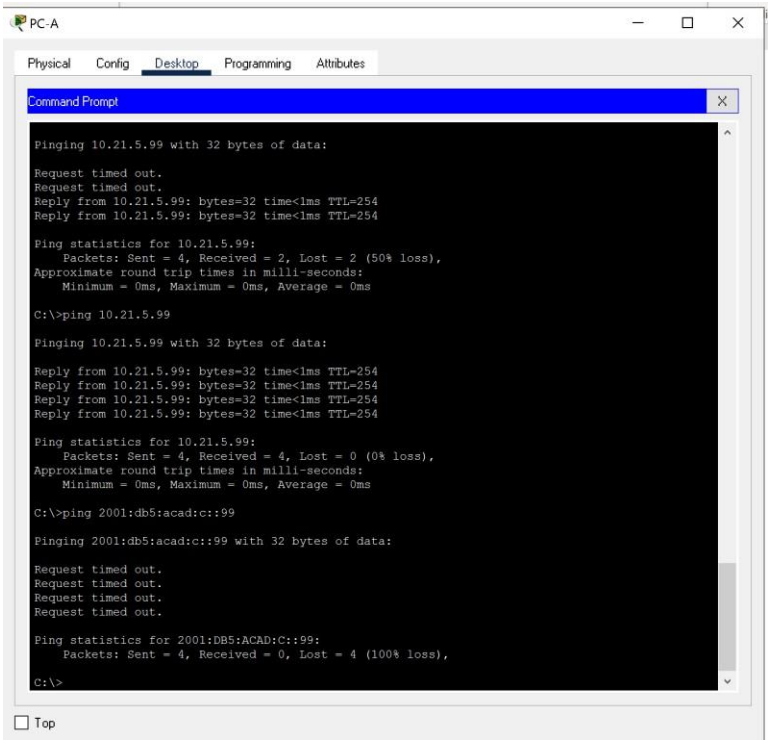

Figura 7. Ping de PC-A a S2, VLAN 4.
Fuente: Autor

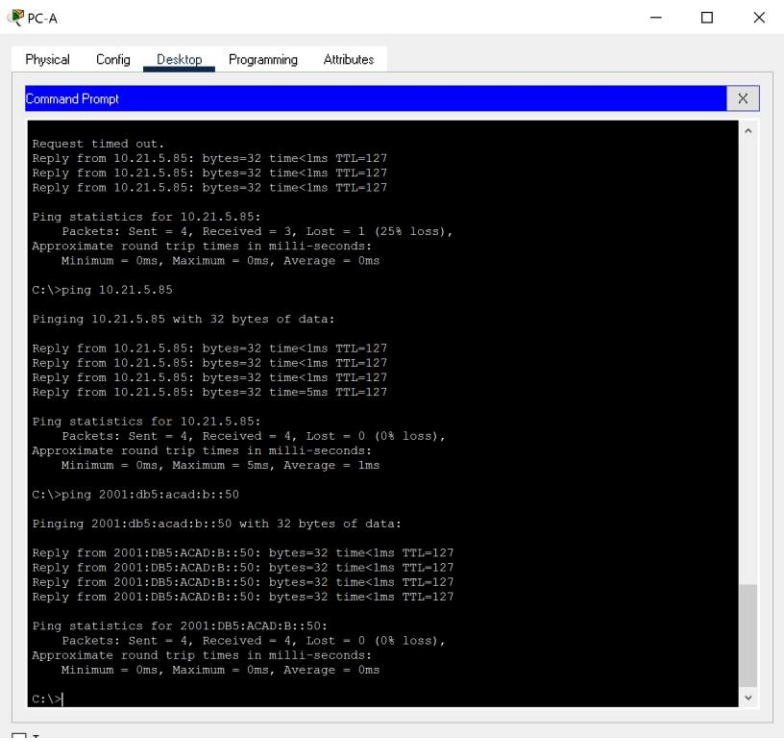

Figura 8. Ping de PC-A a PC-B.
Fuente: Autor

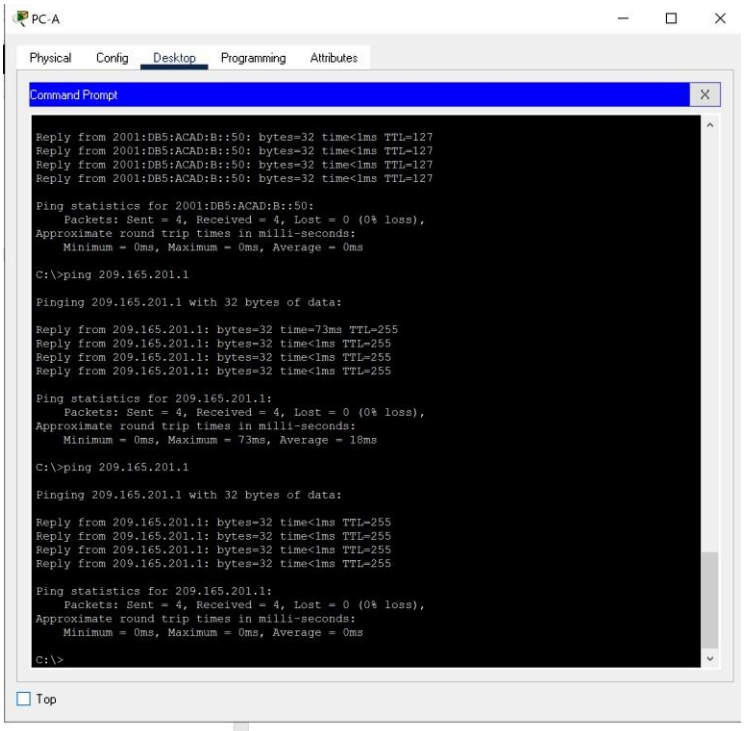

Figura 9. Ping de PC-A a R1 bucle 0.
Fuente: Autor

Pings desde PC-B

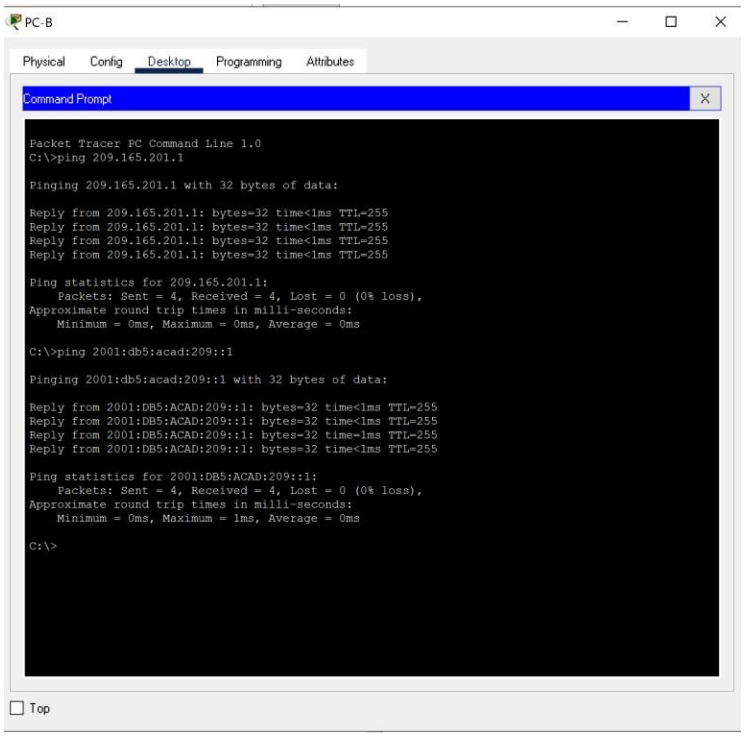

Figura 10. Ping de PC-B a R1 bucle 0.
Fuente: Autor

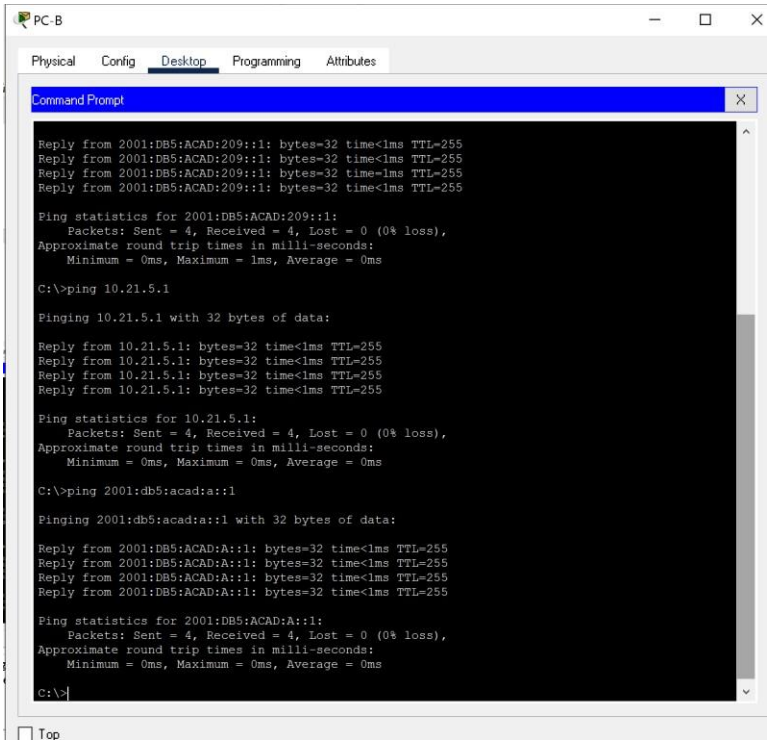

Figura 13. Ping de PC-B a R1, G0/0/1.4.
Fuente: Autor

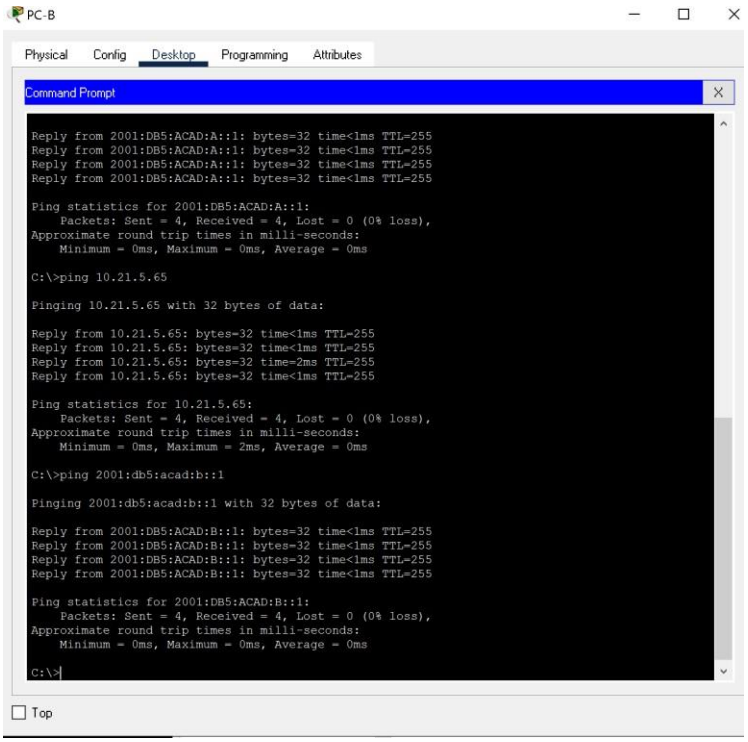

Figura 12. Ping de PC-B a R1, G0/0/1.3.
Fuente: Autor

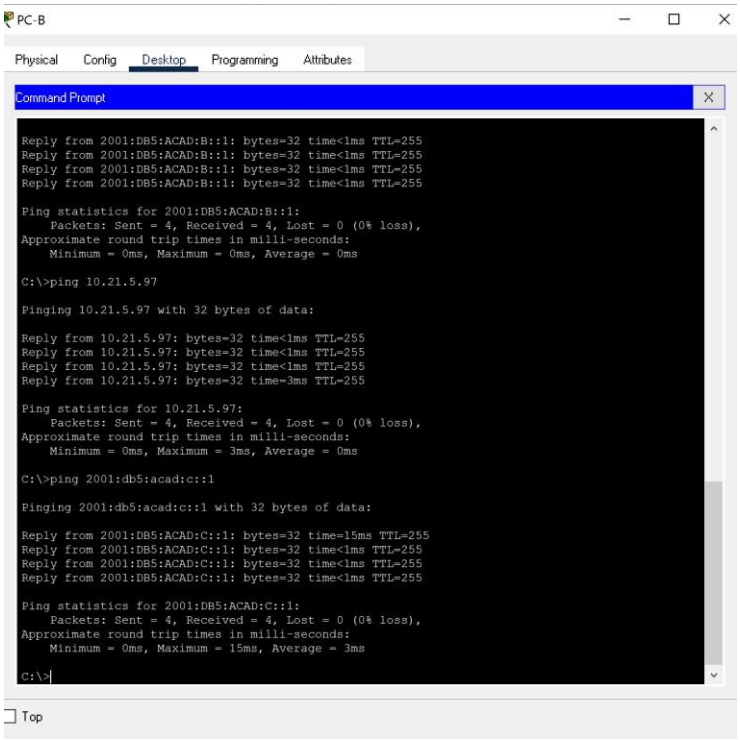

Figura 13. Ping de PC-B a R1, G0/0/1.4.
Fuente: Autor

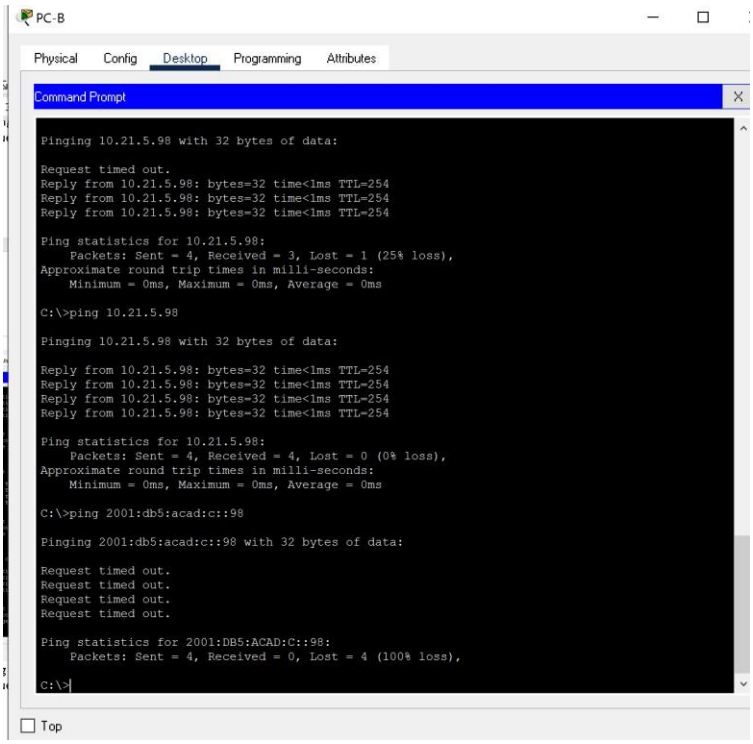

Figura 14. Ping de PC-B a S1, VLAN 4.
Fuente: Autor

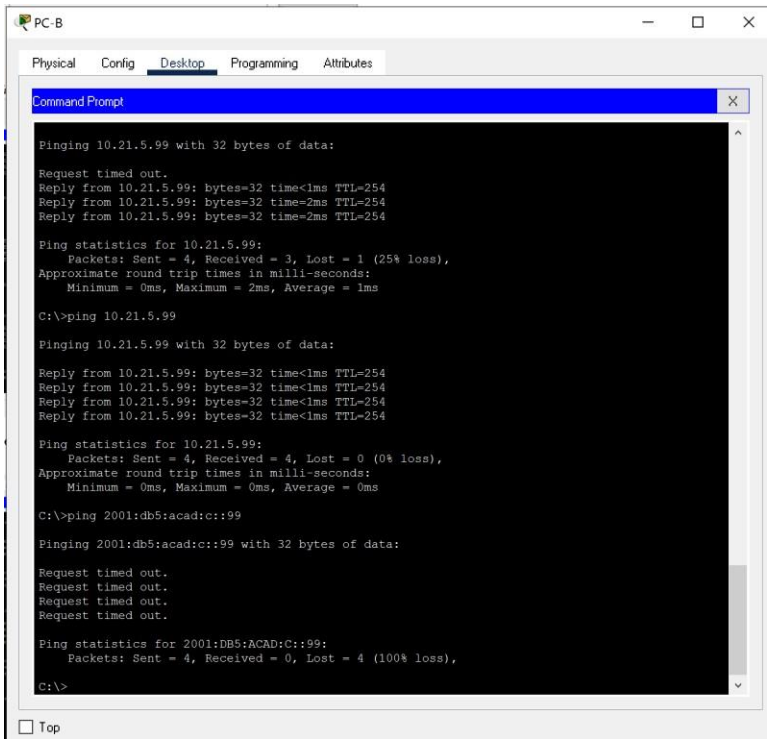

Figura 15. Ping de PC-B a S2, VLAN 4.

Fuente: Autor

1.2 Escenario 2

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

Topología

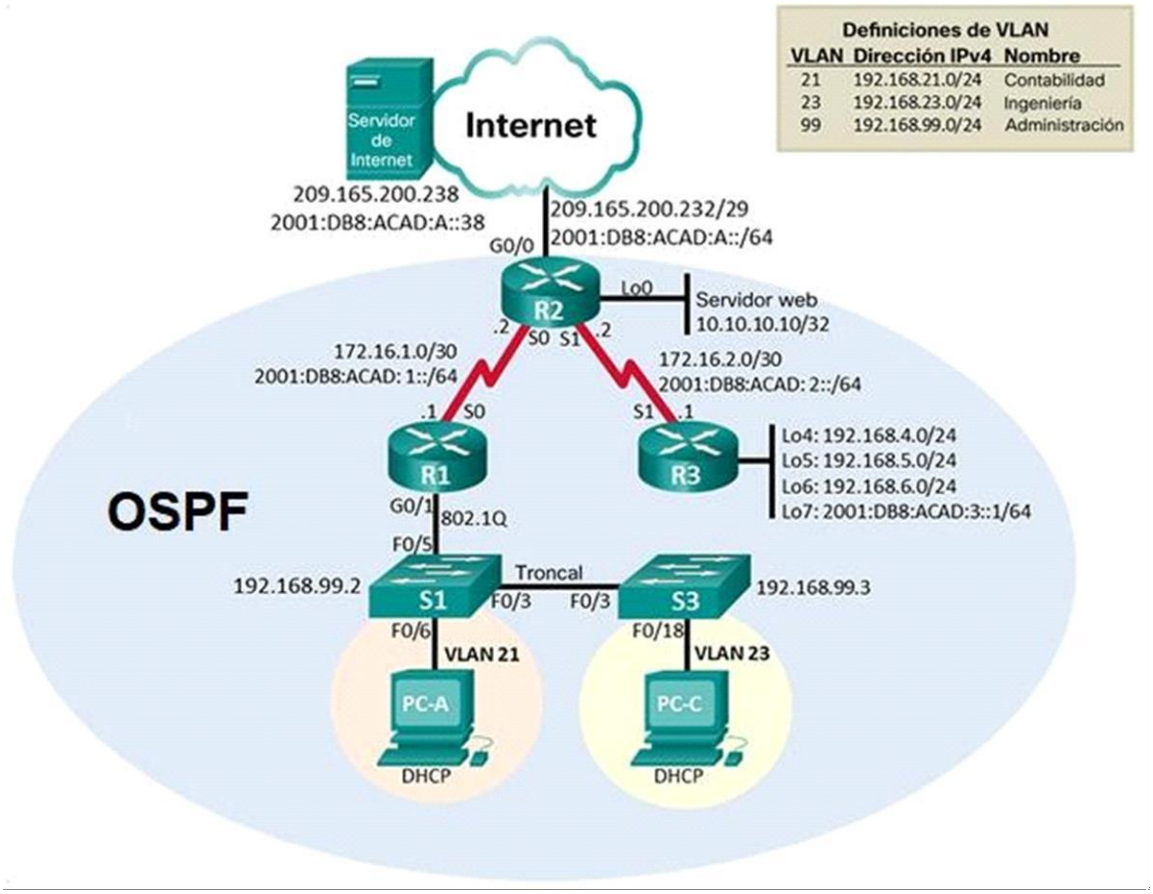

Figura 16. Topología escenario 2.
Fuente: Documento Cisco

1.2.1 Parte 1: Inicializar dispositivos

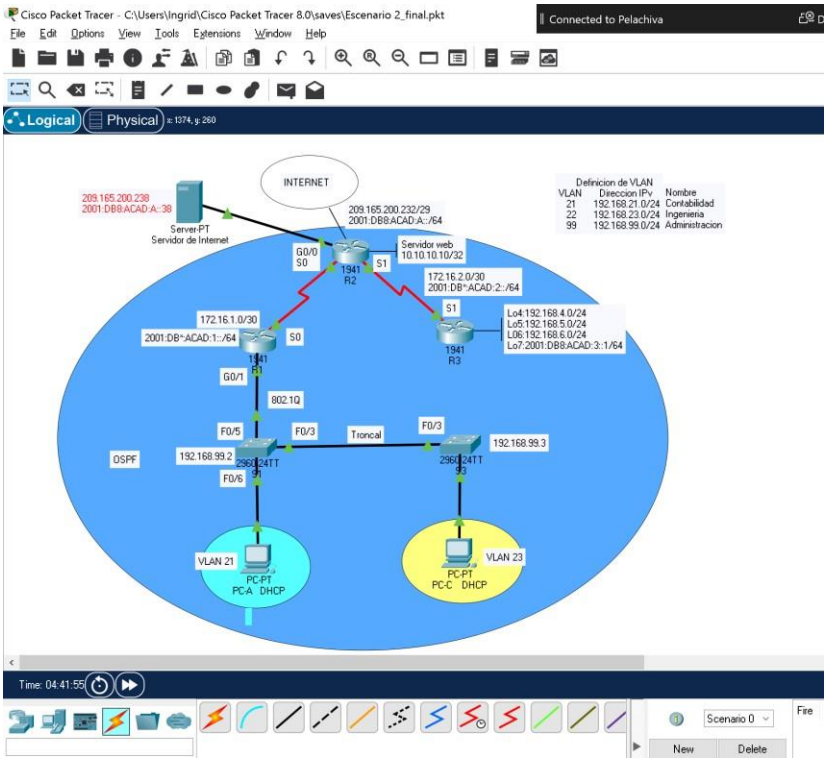

Figura 17. Simulación escenario 2 – Packet Tracer.
Fuente: Autor

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

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

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

Tabla 13. Inicialización y recarga de R1, R2 y R3.

Tarea	Comando del IOS (Para R1, R2 y R3)
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config
Volver a cargar todos los routers	Router#reload

Tabla 14. Inicialización y recarga de S1 y S3.

Tarea	Comando del IOS (Para S1 y S3)
Eliminar el archivo startup-config de todos los switches y eliminar la base dedatos de VLAN anterior	Switch#erase startup-config
Volver a cargar ambos switches	Switchr#reload

Verificar que la base de datos de VLAN noesté en la memoria flash en ambos switches	Switch#show flash

1.3.1 Parte 2: Configurar los parámetros básicos de los dispositivos

1.3.1.1 Paso 1: Configurar la computadora de Internet

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

Tabla 15. Configuración de Servidor de Internet.

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

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

1.3.1.2 Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16. Configuración de R1.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router R1	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada, Class	R1(config)#enable secret class
Contraseña de acceso a la consola, Cisco	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login

Contraseña de acceso Telnet,Cisco	R1(config-line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config-line)#servicepassword-encryption
Mensaje MOTD, Se prohíbe el acceso noautorizado.	R1(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/0/0	R1(config)#interface s0/0/0 R1(config-if)#description Conexion a R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Nota: Todavía no configure G0/1.

1.3.1.3 Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 17. Configuración de R2.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure t Router(config)#no ip domain-lookup
Nombre del router, R2	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada, class	R2(config)#enable secret class
Contraseña de acceso a la consola, cisco	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet, cisco	R2(config)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config-line)# service password-

	encryption
Habilitar el servidor HTTP	R2(config)#ip http server
Mensaje MOTD, Se prohíbe el acceso no autorizado.	R2(config)#banner motd " Se prohíbe el acceso no autorizado"
Interfaz S0/0/0 Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	R2(config)#interface s0/0/0 R2(config-if)#description Conexion a R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1 Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz	R2(config-if)#interface s0/0/1 R2(config-if)#description Conexion a R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado) Establecer la descripción. Establezca la dirección IPv4.	R2(config-if)#interface loopback 0 R2(config-if)#description Servidor WebSimulado R2(config-if)#ip address 10.10.10.10 255.255.255.255
Ruta predeterminada Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

1.3.1.4 Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 18. Configuración de R3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router, R3	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada,class	R3(config)#enable secret class
Contraseña de acceso a la consola, cisco	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet, cisco	R3(config)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)# service password-encryption
Mensaje MOTD, Se prohíbe el acceso no autorizado.	R3(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/0/1 Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	R3(config)#interface s0/0/1 R3(config-if)#description Conexion a R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config-if)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0

Interfaz loopback 5 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config-if)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config-if)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.	R3(config-if)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas Configurar una ruta IPv4 predeterminada deS0/0/1 Configurar una ruta IPv6 predeterminada deS0/0/1	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

1.3.1.5 Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 19. Configuración de S1.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch, S1	Switch(config)#hostname S1
Contraseña de ese privilegiado cifrada, class	S1(config)#enable secret class
Contraseña de acceso a la consola, cisco	S1(config)#line console 0 S1(config-line)#password ciscoS1(config-line)#login

Contraseña de acceso Telnet, cisco	S1(config)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config-line)# service password-encryption
Mensaje MOTD, Se prohíbe el acceso noautorizado.	S1(confit)#banner motd #Se prohíbe el acceso no autorizado#

1.3.1.6 Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 20. Configuración de S3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch, S3	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada, class	S3(config)#enable secret class
Contraseña de acceso a la consola, cisco	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet, cisco	S3(config)#line vty 0 15 S3(config- line)#password ciscoS3(config- line)#login
Cifrar las contraseñas de texto no cifrado	S3(config-line)# service password-encryption
Mensaje MOTD, Se prohíbe el acceso no autorizado.	S3(config)#banner motd #Se prohíbe el acceso no autorizado#

1.3.1.7 Paso 7: Verificar la conectividad de la red

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

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

Tabla 21. Verificación de la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Sí hay respuesta
R2	R3, S0/0/1	172.16.2.1	Sí hay respuesta
PC de Internet	Gateway predeterminado	209.165.200.225	Sí hay respuesta

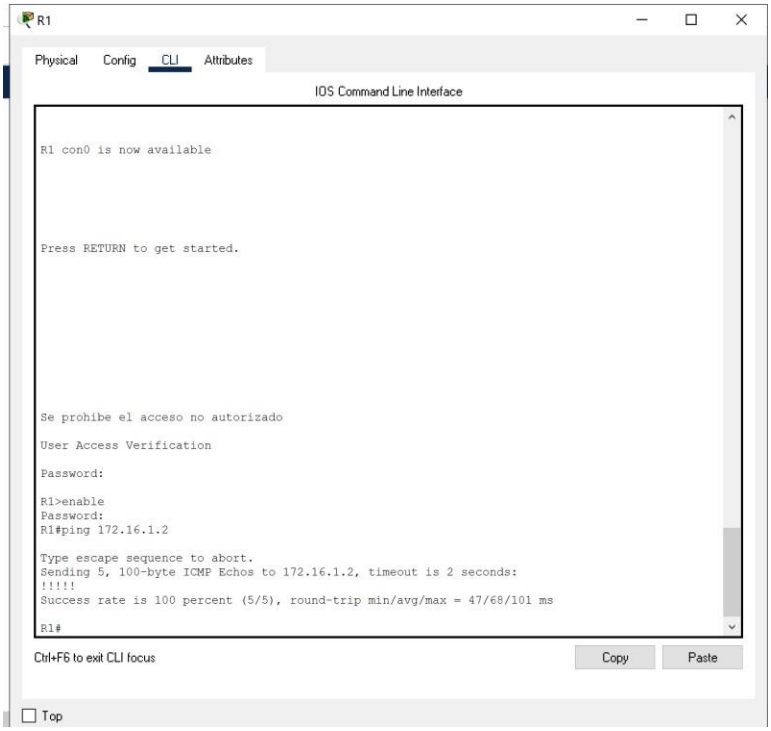

Figura 18. Ping de R1 a R2, S0/0/0.
Fuente: Autor

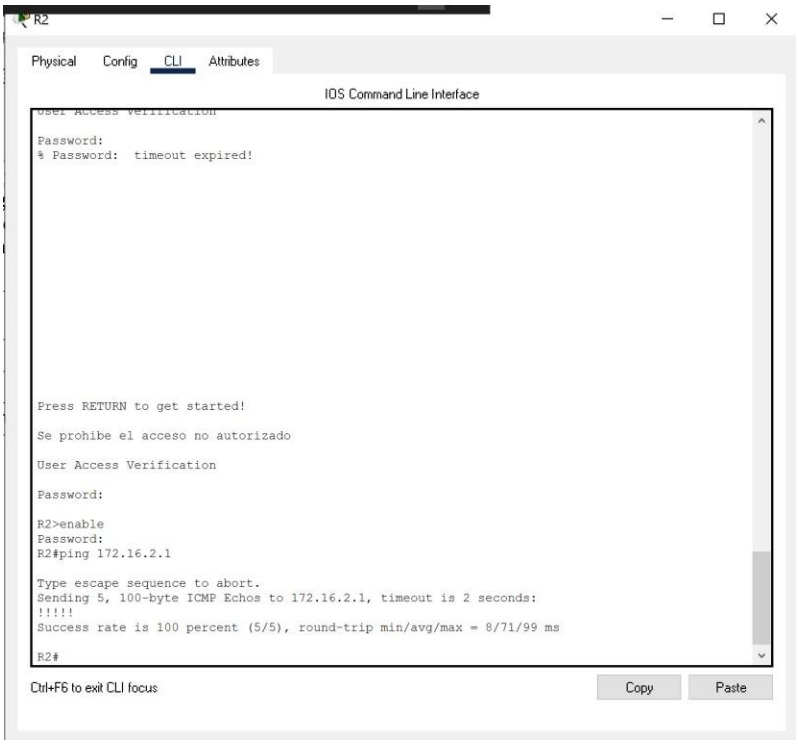

Figura 19. Ping de R2 a R3, S0/0/1.
Fuente: Autor

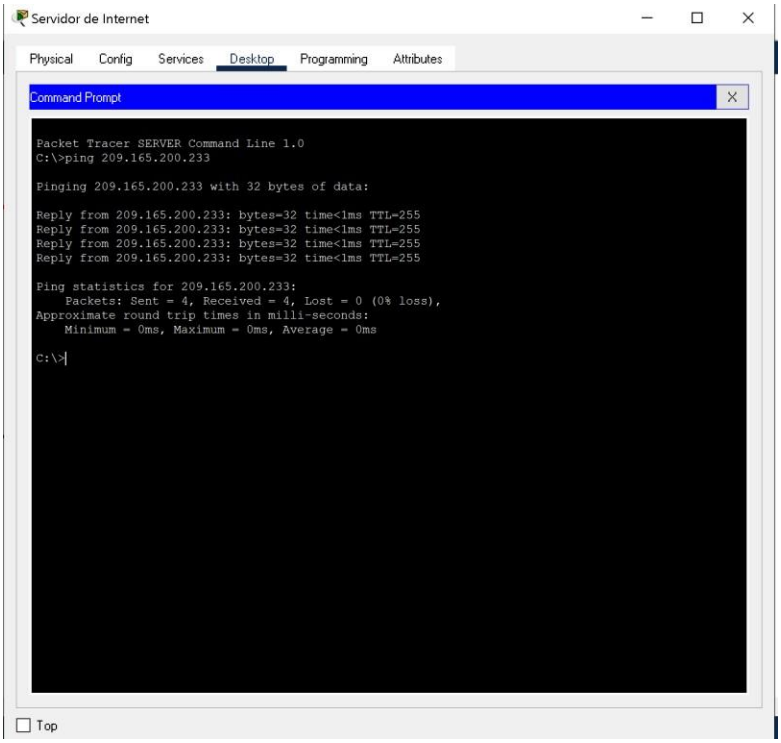

Figura 20. Ping de PC de Internet a Gateway predeterminado.
Fuente: Autor

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que lospings se realicencorrectamente.

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

1.4.1.1 Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 22. Configuración de seguridad S1, VLAN y routing S1.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican	S1#configure terminal S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingeniería S1(config-vlan)#vlan 99 S1(config-vlan)#name Administración
Asignar la dirección IP de administración. Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología	S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3 Utilizar la red VLAN 1 como VLAN nativa	S1(config)#interface Fa0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5 Utilizar la red VLAN 1 como VLAN nativa	S1(config)#interface Fa0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso Utilizar el comando interface range	S1(config-if)#interface range Fa0/1-2, Fa0/4, Fa0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if-range)#interface Fa0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#interface range Fa0/1-2, Fa0/4, Fa0/7-24, g0/1-2 S1(config-if-range)#shutdown

1.4.1.2 Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 23. Configuración de seguridad S1, VLAN y routing S3.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.	S3#configure terminal S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingeniería S3(config-vlan)#vlan 99 S3(config-vlan)#name Administración
Asignar la dirección IP de administración Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología	S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado. Asignar la primera dirección IP en la subredcomo gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3 Utilizar la red VLAN 1 como VLAN nativa	S3(config)#interface Fa0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso Utilizar el comando interface range	S3(config-if)#interface range Fa0/1-2, Fa0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 23	S3(config-if-range)#interface Fa0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#interface range Fa0/1-2, Fa0/4-17, Fa0/19-24, g0/1-2 S3(config-if-range)#shutdown

1.4.1.3 Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 24. Configuración de subinterfaz 802.1Q en R1.

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1 Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz	R1(config)#interface g0/1.21 R1(config-subif)#description Vlan 21 R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1 Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz	R1(config-subif)#interface g0/1.23 R1(config-subif)#description Vlan 23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1 Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz	R1(config-subif)#interface g0/1.99 R1(config-subif)#description Vlan 99 R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0

Activar la interfaz G0/1	R1(config-subif)#interface g0/1 R1(config-if)#no shutdown

1.4.1.4 Paso 4: Verificar la conectividad de la red

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

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

Tabla 25. Verificación de conectividad de la red.

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Sí hay respuesta
S3	R1, dirección VLAN 99	192.168.99.1	Sí hay respuesta
S1	R1, dirección VLAN 21	192.168.21.1	Sí hay respuesta
S3	R1, dirección VLAN 23	192.168.23.1	Sí hay respuesta

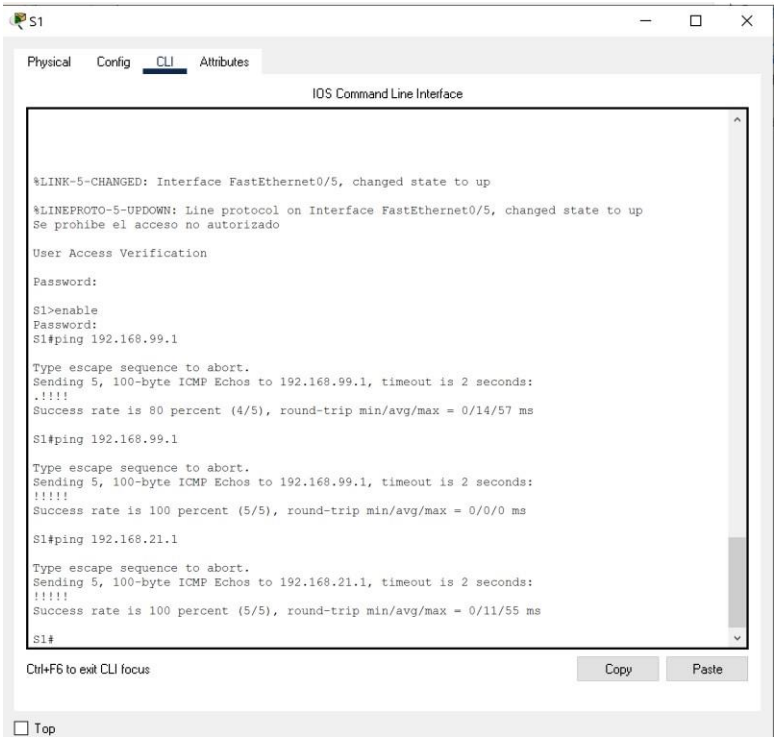

Figura 21. Ping de S1 a R1, VLAN 99 y VLAN 21.
Fuente: Autor

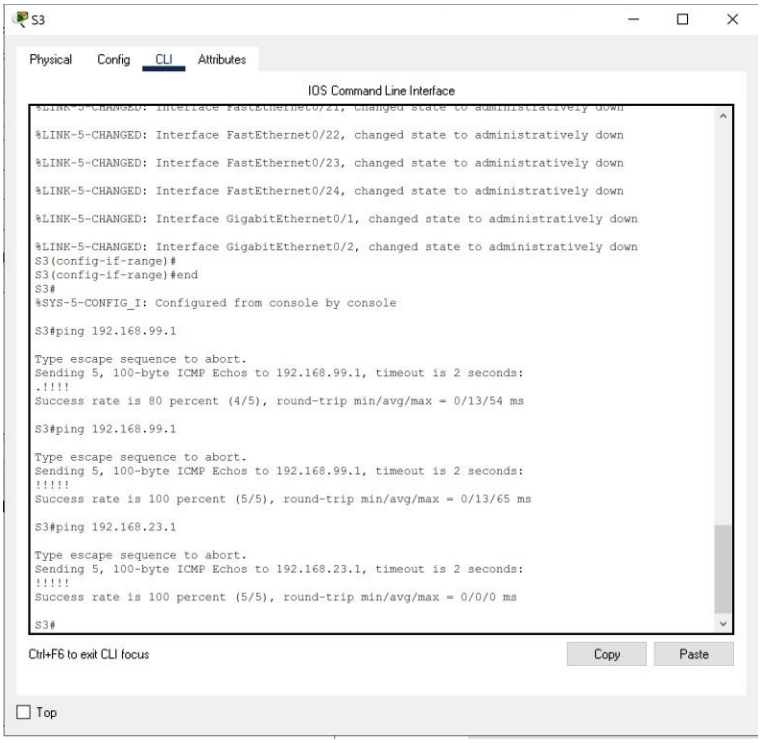

Figura 22. Ping de S3 a R1, VLAN 99 y VLAN 23.
Fuente: Autor

1.5.1 Parte 4: Configurar el protocolo de routing dinámico OSPF

1.5.1.1 Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 26. Configuración del protocolo de routing dinámico OSPF en R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1
Anunciar las redes conectadas directamente Asigne todas las redes conectadas directamente.	R1(config-router)#do show ip route connected R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0

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

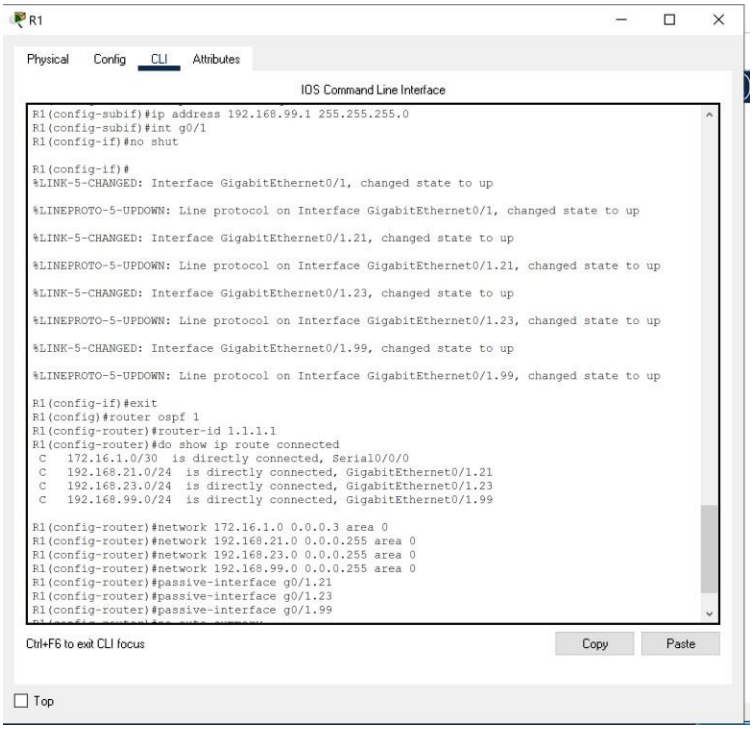

Figura 23. Configuración OSPF en el R1
Fuente: Autor

1.5.1.2 Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 27. Configuración del protocolo de routing dinámico OSPF en R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2

Anunciar las redes conectadas directamente **Nota:** Omitir la red G0/0.	R2(config-router)#do show ip route connected R2(config-router)#network 10.10.10.10 0.0.0.255 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

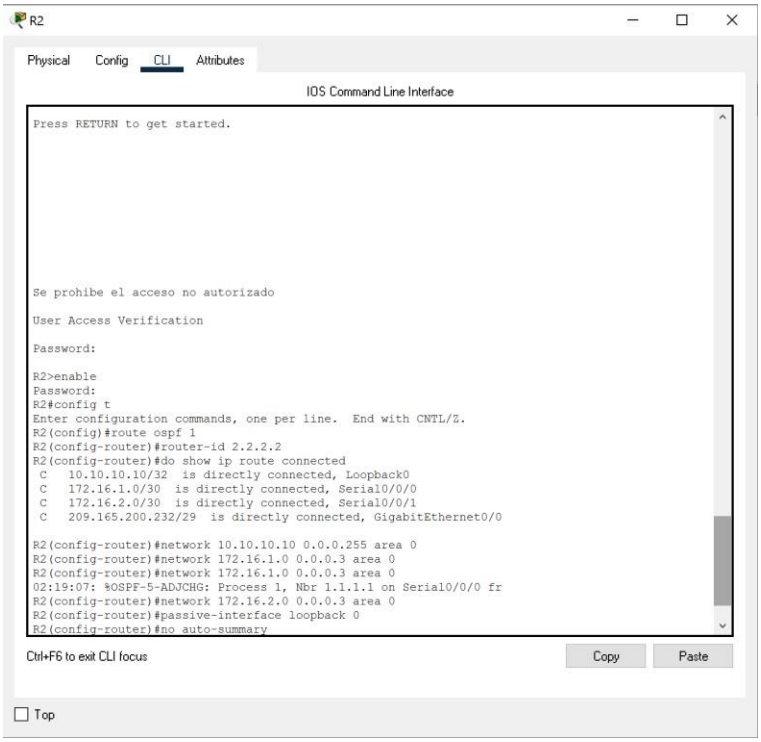

Figura 24. Configuración OSPF en el R2
Fuente: Autor

1.5.1.3 Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 28. Configuración del protocolo de routing dinámico OSPF en R3

Elemento o tarea de configuración	Especificación

Configurar OSPF área 0	R3(config)#router ospf 1 R3(config-router)#router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente	R3(config-router)#do show ip route connected R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

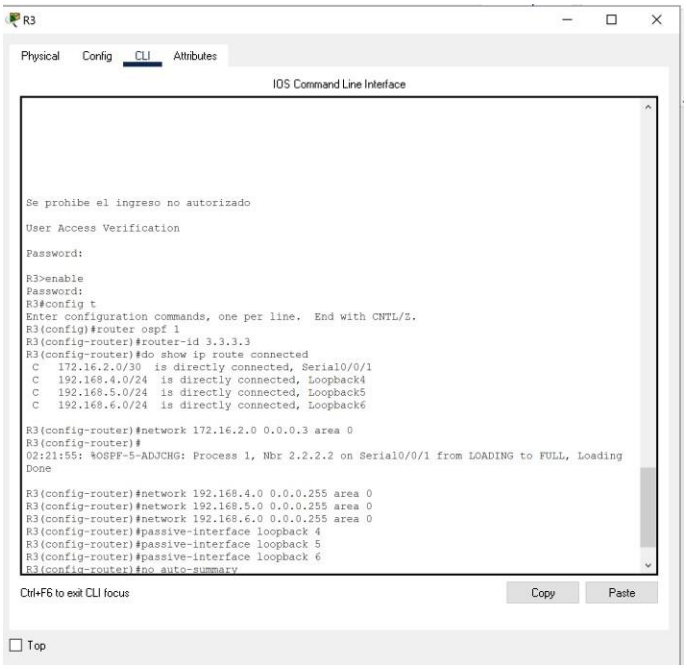

Figura 25. Configuración OSPFv3 en el R3
Fuente: Autor

1.5.1.4 Paso 4: Verificar la información de OSPF

Verifique que OSPF esté funcionando como se espera. Introduzca el comando deCLI adecuado paraobtener la siguiente información:

Tabla 29. Verificación de la información 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 run | section router ospf

1.6.1 Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 30. Configuración del R1 como servidor de DHCP para las VLAN 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP enla 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 enla VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21. Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23 Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado	R1(dhcp-config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.comR1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1

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

La configuración del R2 incluye las siguientes tareas:

Tabla 31. Configuración de la NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario Nombre de usuario: **webuser**Contraseña: **cisco12345** Nivel de privilegio: **15**	R2(config)#username webuser secret cisco12345 privilege 15
Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la basede datos local para la autenticación	R2(config)#ip http authentication local
Crear una NAT estática al servidor web. Dirección global interna: **209.165.200.229**	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#interface s0/0/0R2(config-if)#ip nat inside R2(config-if)#interface s0/0/1R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255

Defina el pool de direcciones IP públicas utilizables. Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228**	R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.225 netmask 255.255.255.228
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

1.6.1.3 Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Tabla 32. Verificación el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Sí hay información
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Sí hay información
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Sí hay respuesta
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Desde el servidor de Internet utilizando el navegador web se intenta acceder al servidor web, pero no responde, se prueba con los Pc's a la dirección del servidor.

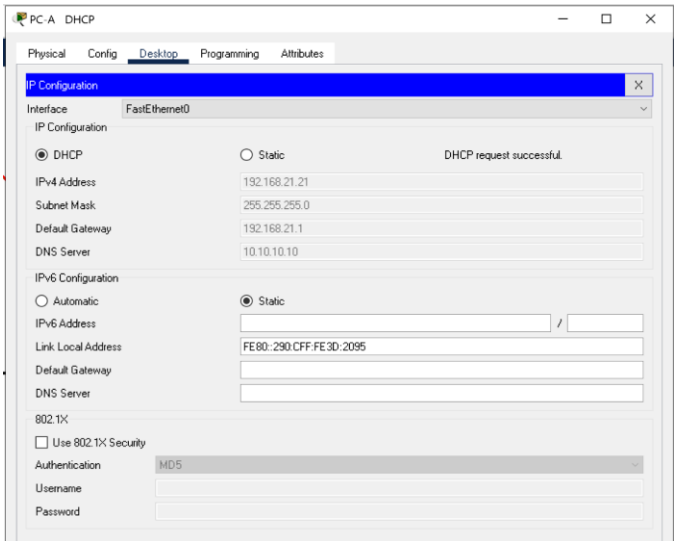

Figura 26. Información IP PC-A del servidor de DHCP.
Fuente: Autor

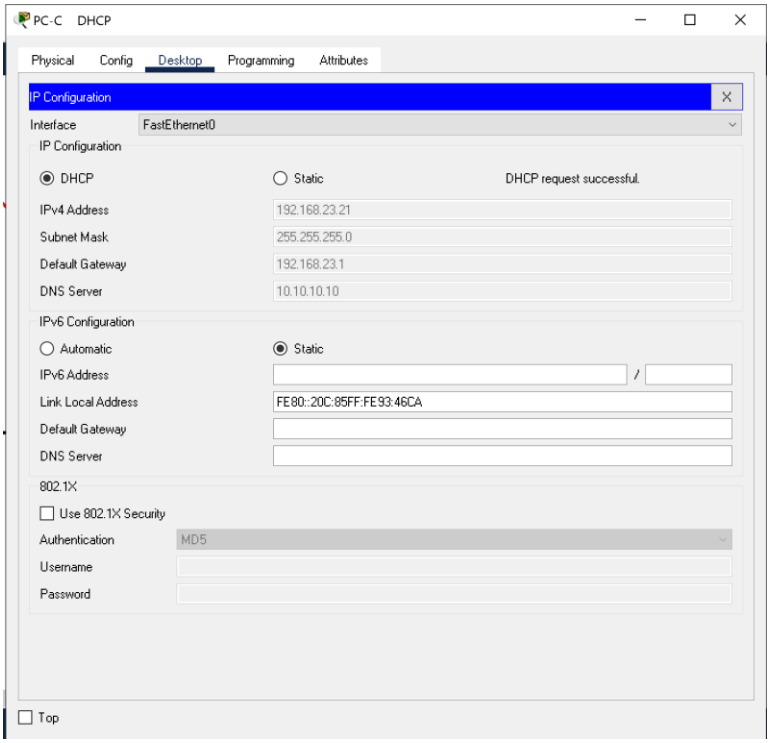

Figura 27. Información IP PC-C del servidor de DHCP.
Fuente: Autor

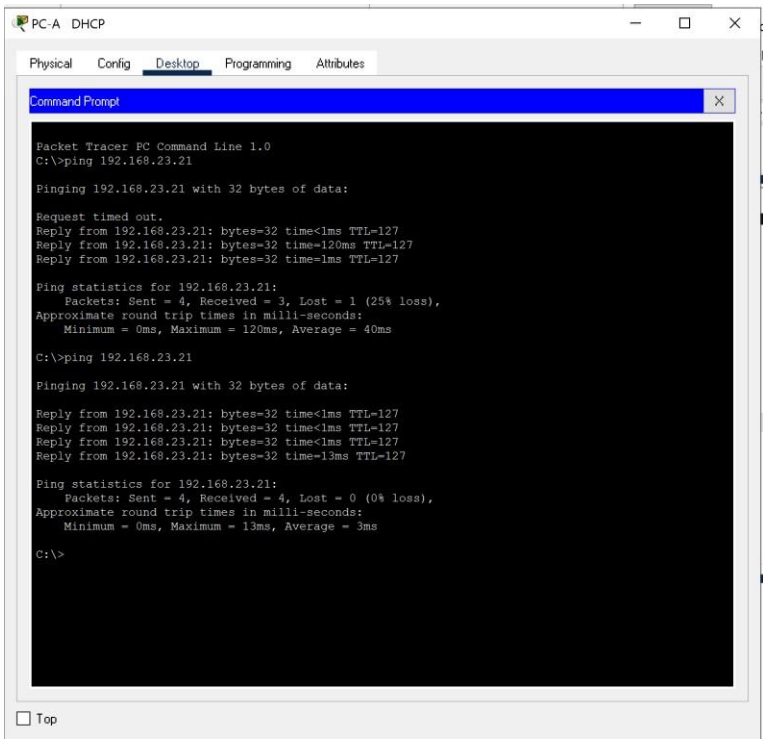

Figura 28. Ping de PC-A a PC-C.
Fuente: Autor

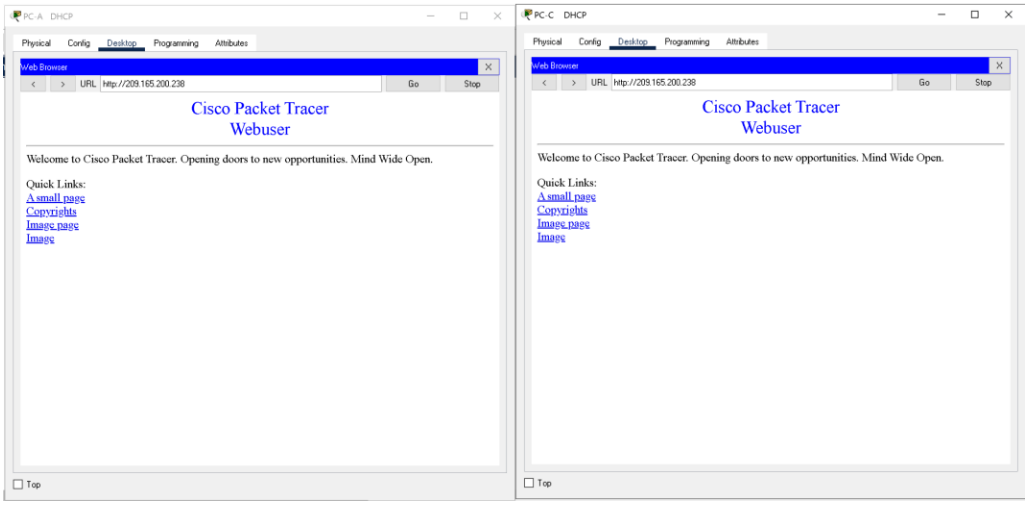

Figura 29. Verificación navegador web.
Fuente: Autor

1.7.1 Parte 6: Configurar NTP

Tabla 33. Configuración de NTP en R1

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2. **5 de marzo de 2016, 9 a. m.**	R2#clock set 09:00:00 05 March 2016
Configure R2 como un maestro NTP. Nivel de estrato: **5**	R2(config)#ntp master 5
Configurar R1 como un cliente NTP. Servidor: **R2**	R1(config)#ntp server172.16.1.2
Configure R1 para actualizaciones de calendario periódicascon hora NTP.	R1(config)#ntp updatecalendar
Verifique la configuración de NTP en R1.	R1#show ntp associations

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

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

Tabla 34. Configuración restricción de acceso a las líneas VTY en R2

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

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

Tabla 35. Verificación de configuración 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 aplicaa una interfaz y la dirección en que se aplica?	R2#show ip interface
¿Con qué comando se muestran las traducciones NAT? **Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internetintentó hacer ping a esos equipos en el paso 2. Si haceping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traduccionesde NAT dinámicas?	R2#clear ip nat translation *

CONCLUSIONES

- La realización del proceso desarrollado en el primer escenario nos permite comprender cómo funciona una determinada red atendiendo los conceptos aprendidos sobre los dispositivos terminales que lo integran, administración de redes, conexión de cables con puertos, configuración de los dispositivos y seguridad de puntos de conexión de red. La configuración de servidores locales y remotos mediante SSH o telnet, configuración de protocolos e interfaces lógicas y físicas, configuración de passwords de seguridad a modo usuario y privilegiado, reinicio de dispositivos, contraseñas encriptadas, mensajes del día (banner-motd), entre otros procesos nos dan la seguridad del aprendizaje en este proceso.

- El desarrollo del segundo escenario nos permite comprender que el servicio DHCP se puede encontrar activo en un servidor donde se centraliza la administración de las direcciones IP de la red, que los cambios en una parte de la red no tienen por qué afectar a toda ella, y buena parte del tráfico puede ser dividido en su área. - Las listas de control de acceso desempeñan un gran papel como medida de seguridad lógica, ya que su cometido siempre es controlar el acceso a los recursos o activos del sistema, para poder aplicar los conocimientos adquiridos a lo largo del curso de profundización Cisco y sobre todo relacionados con el protocolo de enrutamiento denominado OSPF, aplicando su configuración básica a los dispositivos de red, configurando una prioridad de routers, desactivando las actualizaciones de enrutamiento en las interfaces adecuadas y verificando la conectividad entre los dispositivos de la topología.

BIBLIOGRAFIA

- CISCO. (2019). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#1

- CISCO. (2019). Routing Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/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

- UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

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

- UNAD (2017). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

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

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

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

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

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

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