SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

OSCAR JAVIER JEREZ GONZÁLEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRÓNICA
FACATATIVÁ (CUND.)
2021

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

OSCAR JAVIER JEREZ GONZÁLEZ

DIPLOMADO DE PROFUNDIZACIÓN CISCO COMO OPCIÓN DE GRADO

PRESENTADO A:
ING. HÉCTOR MANUEL HERRERA HERRERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRÓNICA
FACATATIVÁ (CUNDINAMARCA)
2021

Nota de Aceptación

Aprobado por el comité y Director del Diplomando de Profundización CISCO. “Diseño e implementación de soluciones integradas LAN / WAN” Dando cumplimineto a los requisitos de opción de grado por la Universidad Nacional Abierta y a Distancia UNAD. CEAD Bogotá – Centro Jose´Acevedo y Gómez .

Ing. Nancy Amparo Guaca

Director de Curso

Ing. Héctor Manuel Herrera Herrera

Jurado

Jurado

Facatativá, 16 de Julio de 2021.

DEDICATORIA

Dedicaré este esfuerzo al Todopoderoso por guiarme y bríndame bendiciones, a mis padres, a mi amada esposa Luz Jaddy y mis queridos hijos, quienes son mi apoyo, mi energía y la motivación incondicional que hace parte fundamental de este proceso.

AGRADECIMIENTOS

En primera instancia, agradezco al Todopoderoso quien siempre está y estará en todos los momentos de mi vida y quien guía mis pensamientos hacia la perseverancia y el éxito.

Agradecer a mi amada esposa por su orientación y mis queridos hijos quienes me han brindado su apoyo y espacio para llevar a feliz término este proceso y han tenido la paciencia para brindarme los espacios de formación.

Agradecimiento especial a toda mi familia Unadista, tutores, Directivos, compañeros y a todos los que, con su paciencia, sapiencia y entrega me dieron los medios y la orientación en el desarrollo de este proceso de formación con el mejor ejercicio: **CONSTRUIR CONOCIMIENTO Y COMPARTIR EXPERIENCIAS**.

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

ACL: una lista de control de acceso (ACL) es una lista de filtros de tráfico de red y acciones correlacionadas utilizadas para mejorar la seguridad. Bloquea o permite a los usuarios acceder a recursos específicos. Una ACL contiene los hosts a los que se permite o se niega el acceso al dispositivo de red. Las ACL se pueden definir de una de dos maneras: por dirección IPv4 o por dirección IPv6.

Administración remota: la administración remota está manipulando los parámetros de un dispositivo de red desde una ubicación remota. Esto se suele hacer en dispositivos como ordenadores, switches, routers y muchos otros que tienen una dirección IP. Permite a los administradores de red responder rápidamente a las solicitudes o los retos, ya que no tienen que estar físicamente en el sitio. El acceso a los dispositivos en la administración remota es casi como hacerlo localmente, excepto que la dirección IP local del dispositivo se utiliza para acceder al dispositivo localmente, mientras que la IP de WAN del dispositivo se utiliza cuando se hace en un dispositivo remoto.

CISCO: Las certificaciones cisco son reconocidas a nivel mundial como un estándar de la industria para diseño y soporte de redes, garantizando altos niveles de conocimientos y confiabilidad. Su línea de cursos va desde la tecnología más básica de redes hasta áreas especializadas y tecnología avanzada tales como seguridad, redes inalámbricas y telefonía IP.

DHCP: Significa protocolo de configuración de host dinámico y es un protocolo de red utilizado en redes IP donde un servidor DHCP asigna automáticamente una dirección IP y otra información a cada host en la red para que puedan comunicarse de manera eficiente con otros puntos finales. Además de la dirección IP, DHCP también asigna la máscara de subred, la dirección de puerta de enlace predeterminada, la dirección del servidor de nombres de dominio (DNS) y otros parámetros de configuración pertinentes.

Fast Ethernet. Permite la agrupación lógica de varios enlaces físicos Ethernet, esta agrupación es tratada como un único enlace y permite sumar la velocidad nominal de cada puerto físico Ethernet usado y así obtener un enlace troncal de alta velocidad.

Gateway. Considerado como un dispositivo en red que actúa como un punto de entrada de una red a otras redes.Es el enlace que conecta dos ordenadores a Internet. La pasarela actúa como portal entre dos programas y como medio de comunicación entre los protocolos que les permite compartir datos en los mismos dispositivos informáticos o entre diferentes sistemas informáticos.

ISP: Son las siglas en inglés de Internet Service Provider –en español: Proveedor de servicios en Internet o PSI–, que es un término usado para referirse a empresas que proveen de conexión a Internet a sus clientes, tanto residenciales como corporativos. Muchos ISP ofrecen servicios relacionados, como son: correo electrónico, alojamiento de páginas web, registro de dominios, FTP, entre otros. El medio en que un ISP te conecta a Internet varía para cada proveedor.

IPv6: IPv6 es un sistema de direccionamiento de 128 bits utilizado para identificar un dispositivo en una red. Es el sucesor de IPv4 y la versión más reciente del sistema de direccionamiento utilizado en las redes informáticas. IPv6 se está implantando actualmente en todo el mundo. Una dirección IPv6 se representa en ocho campos de números hexadecimales, cada uno de los cuales contiene 16 bits. Una dirección IPv6 se divide en dos partes, cada una de las cuales consta de 64 bits. La primera parte es la dirección de red y la segunda parte la dirección de host.

VLAN: una red de área local virtual (VLAN) es una red conmutada segmentada lógicamente por función, área o aplicación, independientemente de las ubicaciones físicas de los usuarios. Las VLAN son un grupo de hosts o puertos que se pueden ubicar en cualquier lugar de una red pero que se comunican como si estuvieran en el mismo segmento físico.

VLAN basada en 802.1Q: la especificación IEEE 802.1Q establece un método estándar para etiquetar tramas Ethernet con información de pertenencia a VLAN, y define el funcionamiento de los puentes VLAN que permiten la definición, el funcionamiento y la administración de topologías VLAN dentro de una infraestructura LAN puenteada. El estándar 802.1Q está diseñado para abordar el problema de cómo dividir las redes grandes en partes más pequeñas, de modo que el tráfico de difusión y multidifusión no utilice más ancho de banda del necesario. El estándar también ayuda a proporcionar un mayor nivel de seguridad entre los segmentos de las redes internas.

OSPF: es probablemente el protocolo IGP más utilizado en redes grandes; IS-IS, otro protocolo de encaminamiento dinámico de enlace-estado, es más común en grandes proveedores de servicios. Como sucesor natural de RIP, acepta VLSM y CIDR desde su inicio.

1. INTRODUCCIÓN

Las redes de ordenadores actuales son una amalgama de dispositivos, técnicas y sistemas de comunicación que en su estudio promueven la investigación y el desarrollo tecnológico. Bajo esta premisa, para la transferencia de información de voz y datos está ligada a los sistemas de información que atienden peticiones recurrentes de los usuarios finales. Sin lugar a duda, las redes de computadores han sido uno de los grandes acontecimientos dentro del ámbito de las telecomunicaciones. Su crecimiento exponencial representa su gran éxito. Además, como resultado de su desarrollo, coadyuva al surgimiento de nuevas formas de comunicación. Por ejemplo, gracias a las redes de computadoras se creó la gran y bien conocida internet, de tal manera que ahora pueden realizarse operaciones (hoy en día comunes) como los envíos de correos electrónicos, acceso a sistemas de información, videoconferencias, VoIP, interoperabilidad, compartir recursos, conversaciones y transacciones en línea, tareas que optimizan el trabajo del ser humano.

En el presente informe se demostrará de forma práctica los conocimientos adquiridos durante el curso Diplomado de Profundización CCNA de CISCO aplicando las habilidades y competencias adquiridas a lo largo de este. Se configurarán los dispositivos en cada uno de los escenarios y al final se verificarán si fueron aplicadas apropiadamente las configuraciones implementadas y que las redes funcionen correctamente.

El simulador aplicado para el desarrollo de los dos escenarios es la aplicación propietaria de CISCO denominado Packet Tracer que permite las configuraciones básicas de switches y routers. Además, la configuración de interoperabilidad de protocolos IPv4 e IPv6, protocolos de enrutamiento, seguridad, aplicación de redes virtuales VLAN, direccionamiento dinámico, establecimiento de listas de control de acceso y traducción de direcciones de red NAT.

De esta manera, la consolidación de este trabajo nos permite organizar la adquisición de conocimientos, habilidades y destrezas en el diseño e implementación de redes informáticas que permiten el procesamiento, interoperabilidad, acceso seguro, comando y control y gestión de la información.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Rendir un informe de los requerimientos adelantados durante el Diplomando de Profundización CISCO aplicando las competencias y habilidades desarrolladas durante el proceso académico dando respuesta y solución a cada uno de los escenarios planteados.

2.2 OBJETIVOS ESPECÍFICOS

Conceptualizar las temáticas planteadas en los dos escenarios del Diplomado de profundización CCNA.

Implementar las topologías propuestas en un entorno de simulación evaluando los requerimientos y alternativas de solución.

Configurar los dispositivos: router, switch y equipos que admitan tanto la conectividad IPv4 como IPv6, protocolos de enrutamiento, creación de VLAN's, NAT, listas de control de acceso y seguridad con los comandos diseñados para tal fin.

Verificar el estado de conexiones y enrutamientos a través de las solicitudes de eco y trazabilidad en los diferentes enlaces de cada topología

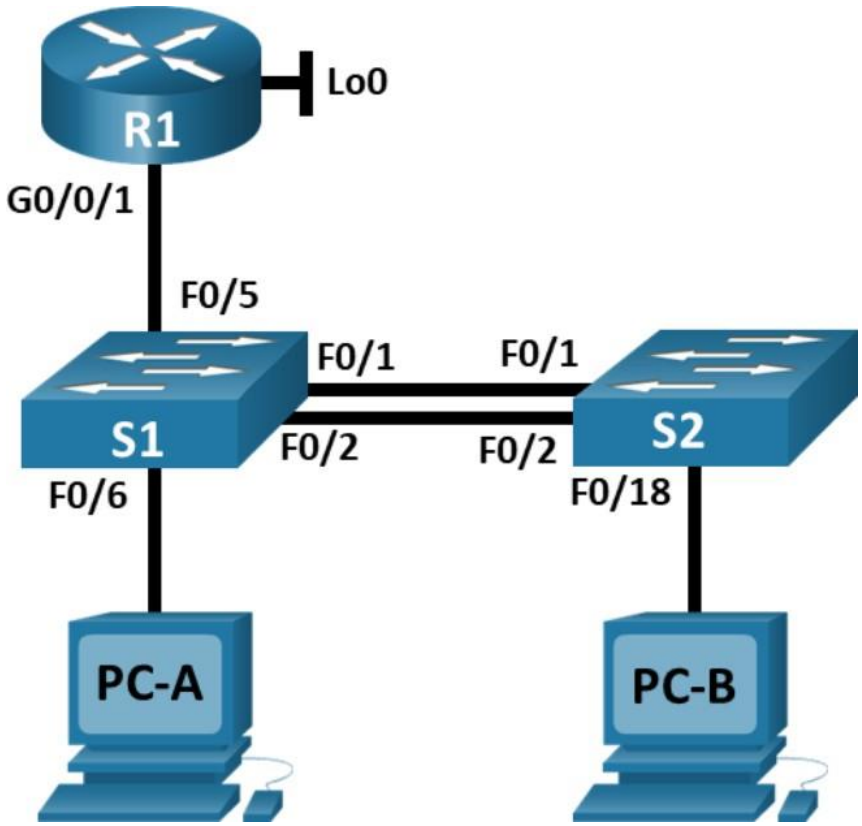
Adquirir habilidades para la administración y de gestión de redes orientadas a los entornos de producción corporativo. Además, necesarias para planificar, implementar, asegurar, diseñar, mantener y solucionar problemas de redes convergentes.

3. DESARROLLO DE ESCENARIOS

3.1 Escenario No. 1

Topología

Figura No. 1. Topología escenario No. 1.

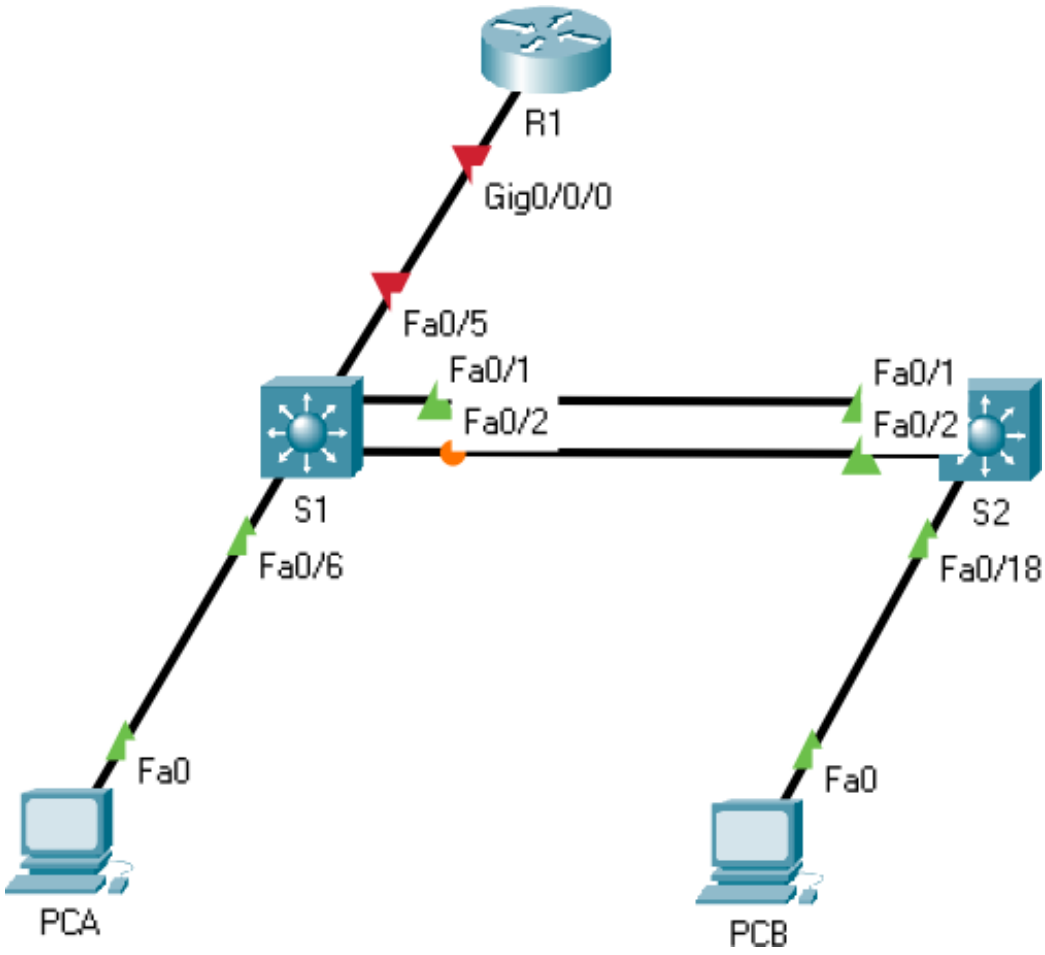


Fuente: Guía Prueba de habilidades prácticas CCNA.

"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."

Para el desarrollo de este escenario se instala el entorno de simulación de Packet Tracer versión 8.0. Se crea la topología de red con los siguientes dispositivos: **Router Cisco ISR4331** (01), **Switch Cisco WS-C3560-24PS** (02) y **Equipo de cómputo de escritorio** (02).

Figura No. 2. Topología escenario No. 1 Simulador Packet Tracert



Fuente: propia.

Tabla No. 1. Tabla de VLAN.

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

Fuente: Guía Prueba de habilidades prácticas CCNA.

Tabla No. 2. Tabla de asignación de direcciones.

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.21.5.1 /26	No corresponde
	2001:db5:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.21.5.65 /27	No corresponde
	2001:db5:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.21.5.97 /29	No corresponde
	2001:db5:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db5: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

Fuente: Guía Prueba de habilidades prácticas CCNA.

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

Instrucciones

3.1.1 Parte 1: Inicializar, recargar y configurar aspectos básicos de los dispositivos.

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

- Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos.
  Se ingresa al Router (R1) y Switches S1 y S2 a través de la interfaz de línea de comando (CLI) y en modo privilegiado se ejecuta los comandos: **erase startup-config** para eliminar el contenido de NVRAM, **delete flash:vlan.dat** para eliminar el contenido de la base de datos VLAN, **show startup-config** para visualizar la configuración y contenido de la NVRAM, que para este paso no presenta información y **reload** para reiniciar el dispositivo.

  Borrado y reinicio del **Router (R1)**:

```
Router>enable
Router#erase startup-config
Router#delete flash:vlan.dat
Delete filename [vlan.dat]?[Enter]
Delete flash:/vlan.dat? [confirm] [Enter]
Router#show startup-config
startup-config is not present
Router#reload
Proceed with reload? [confirm] [Enter]
Router#
```

  Borrado y reinicio del **Switch 1 (S1)**:

```
Switch>enable
Switch#erase startup-config
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?[Enter]
Delete flash:/vlan.dat? [confirm] [Enter]
Switch#show startup-config
startup-config is not present
Switch#reload
Proceed with reload? [confirm] [Enter]
Switch#
```

  Borrado y reinicio del **Switch 2 (S2)**:

```
Switch>enable
Switch#erase startup-config
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]? [Enter]
Delete flash:/vlan.dat? [confirm] [Enter]
Switch#show startup-config
```

```
startup-config is not present
Switch#
Switch#reload
Proceed with reload? [confirm] [Enter]
Switch#
```

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

  En este paso, se realizan las configuraciones en modo de configuración global en los Swiches S1 y S2 con la plantilla SDM (Switch Database Manager). Se aplica el comando **sdm prefer dual-ipv4-and-ipv6 default** que permite funciones equilibradas y se divide en enrutamiento y VLAN.

  Inicialmente, en modo privilegiado y con el comando **show sdm prefer** se visualiza el soporte únicamente para IPv4. Por esta razón, con la carga de la plantilla se obtiene la integración IPv4 e IPv6

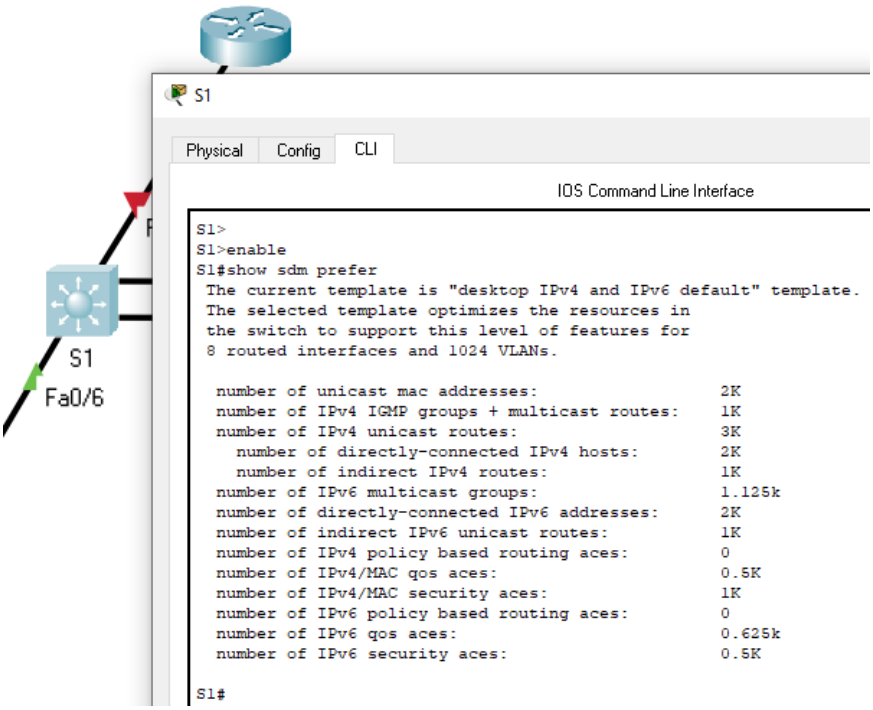
  Configuración Switch **S1**

  ```
  S1>
  S1>enable
  S1#configure terminal
  S1(config)#sdm prefer dual-ipv4-and-ipv6 default
  S1(config)#exit
  S1#reload
  System configuration has been modified. Save? [yes/no]:yes
  ```

  Configuración Switch **S2**

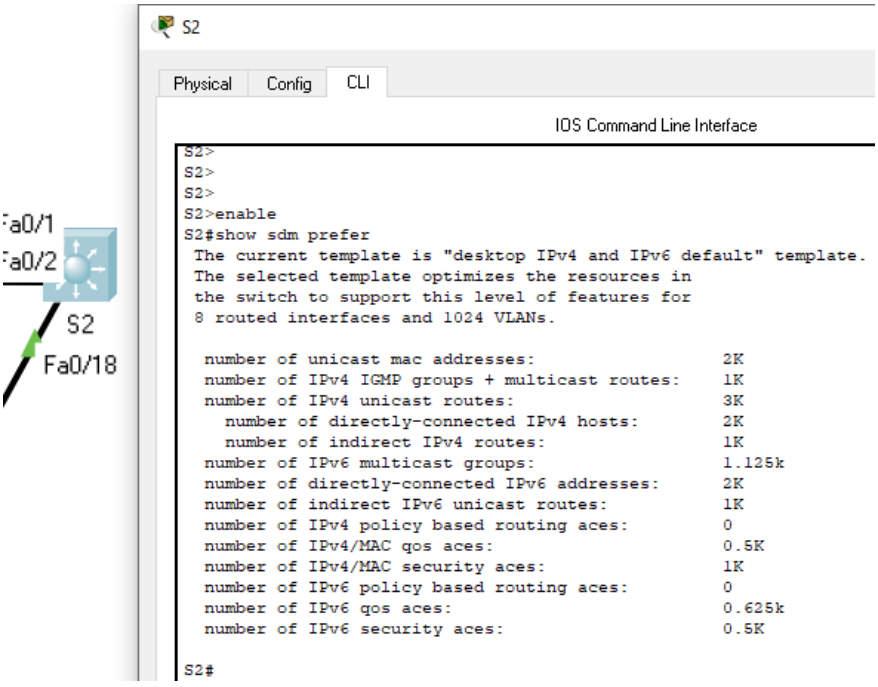
  ```
  S2>
  S2>enable
  S2#configure terminal
  S2(config)#sdm prefer dual-ipv4-and-ipv6 default
  S2(config)#exit
  S2#reload
  System configuration has been modified. Save? [yes/no]:yes
  ```

*Figura No. 3. Configuración plantilla **dual-ipv4-and-ipv6 default** en el **S1***



Fuente: propia

*Figura No. 4. Configuración plantilla **dual-ipv4-and-ipv6 default** en el **S1***



Fuente: propia.

Paso 2: Configurar Router R1.

Tabla No. 3. Configuración Router 1 (**R1**)

Tarea	Especificación
Desactivar la búsqueda DNS	Router> Router>**enable** Router# **configure terminal** Router(config)#**no ip domain-lookup** Router(config)#
Nombre del router	Router(config)#**hostname R1** R1(config)#
Nombre de dominio	R1(config)#**ip domain-name ccna-lab.com** R1(config)#
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#**enable secret ciscoenpass** R1(config)#
Contraseña de acceso a la consola	R1(config)#**line console 0** R1(config-line)#**password ciscoconpass** R1(config-line)#**login** R1(config-line)#**exit** R1(config)#
Establecer la longitud mínima para las contraseñas	R1(config)#**security passwords min-length 10** R1(config)#
Crear un usuario administrativo en la base de datos local	R1(config)#**username admin password admin1pass** R1(config)#
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#**line vty 0 15** R1(config-line)#**login local** R1(config-line)#**exit** R1(config)#
Configurar VTY solo aceptando SSH	R1(config)#**line vty 0 15** R1(config-line)#**transport input ssh** R1(config-line)#**login local** R1(config-line)#**exit** R1(config)#

Cifrar las contraseñas de texto no cifrado	R1(config)#**service password-encryption** R1(config)#
Configure un MOTD Banner	R1(config)#**banner motd # *** CCNA - Acceso restringido *** #** R1(config)#
Habilitar el routing IPv6	R1(config)#**ipv6 unicast-routing** R1(config)#
Configurar interfaz G0/0/1 y subinterfaces Establecer: · Descripción · Dirección IPv4. · Dirección local de enlace IPv6 como fe80: :1 · Dirección IPv6. · Activar la interfaz.	R1(config)#**interface gigabitEthernet 0/0/1.2** R1(config-subif)#**encapsulation dot1Q 2** R1(config-subif)#**description Vlan2 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)# R1(config)#**interface gigabitEthernet 0/0/1.3** R1(config-subif)#**encapsulation dot1Q 3** R1(config-subif)#**description Vlan3 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)# R1(config)#**interface gigabitEthernet 0/0/1.4** R1(config-subif)#**encapsulation dot1Q 4** R1(config-subif)#**description Vlan4 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)# R1(config)#**interface gigabitEthernet 0/0/1.6** R1(config-subif)#**encapsulation dot1Q 6** R1(config-subif)#**description Vlan6 Native** R1(config-subif)#**ipv6 address fe80::1 link-local** R1(config-subif)#**exit** R1(config)# R1(config)#**interface gigabitEthernet 0/0/1.6** R1(config-if)#**no shutdown** R1(config-if)#**exit** R1(config)#
Configure el Loopback0 interface	R1(config)# R1(config)#**interface loopback0** R1(config-if)#**ip address 209.165.201.1 255.255.255.224** R1(config-if)#**ipv6 address 2001:db8:acad:209::1/64** R1(config-if)#**ipv6 address fe80::1 link-local** R1(config-if)#**no shutdown** R1(config-if)#**exit** R1(config)#
Generar una clave de cifrado RSA Módulo de 1024 bits	R1(config)# R1(config)#**crypto key generate rsa 1024** R1(config)#**do wr** R1(config)#**exit** R1#

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

En la tabla No. 3 se realiza la configuración del Router atendiendo las tareas establecidas del escenario. Los ajustes se realizan en modo de configuración global aplicando los siguientes comandos:

no ip domain-lookup, desactivar la búsqueda DNS (solo para pruebas). Se desactiva cundo se hacen pruebas para que el router no intente buscar una entrada DNS.

hostname R1, asignación del nombre para el dispositivo.

ip domain-name ccna-lab.com, asignación de nombre de dominio.

enable secret ciscoenpass, asignación de contraseña para acceso en modo privilegiado

line console 0, password ciscoconpass, login, asignación de contraseña para el acceso a consola y activación con login.

security passwords min-length 10, asignación de la longitud para contraseña con un mínimo de 10 caracteres.

username admin password admin1pass, asignación de uno nombre de usuario administrador**.**

line vty 0 4, login local, configuración del inicio de sesión en las líneas VTY para que use la base de datos local

line vty 0 4, transport input ssh, login local, configuración VTY solo aceptando SSH.

service password-encryption, configuración el cifrado de las contraseñas de texto no cifrado

banner motd #CCNA - Acceso restringido#, configuración de un mensaje de inicio de sesión.

ipv6 unicast-routing, configuración para habilitar el router con el protocolo de red IPv6.

interface gigabitEthernet 0/0/1.2, configuración de la interfaz y subinterfaces. Al interior de la subinterface se aplica el comando **encapsulation dot1Q 2** para la asignación de la VLAN 2 (**Bikes**) a esta subinterface. Paso seguido, una descripción, direccionamiento IPv4 e IPv6 y el enlace local.

interface gigabitEthernet 0/0/1.3, configuración de la interfaz y subinterfaces. Al interior de la subinterface se aplica el comando **encapsulation dot1Q 3** para la asignación de la VLAN 3 (**Trikes**) a esta subinterface. Paso seguido, una descripción, direccionamiento IPv4 e IPv6 y el enlace local.

interface gigabitEthernet 0/0/1.4, configuración de la interfaz y subinterfaces. Al interior de la subinterface se aplica el comando **encapsulation dot1Q 4** para la asignación de la VLAN 4 (**Management**) a esta subinterface. Paso seguido, una descripción, direccionamiento IPv4 e IPv6 y el enlace local.

interface gigabitEthernet 0/0/1.6, configuración de la interfaz y subinterfaces. Al interior de la subinterface se aplica el comando **encapsulation dot1Q 4** para la asignación de la VLAN 6 (**Native**) a esta subinterface. Paso seguido, direccionamiento del enlace local.

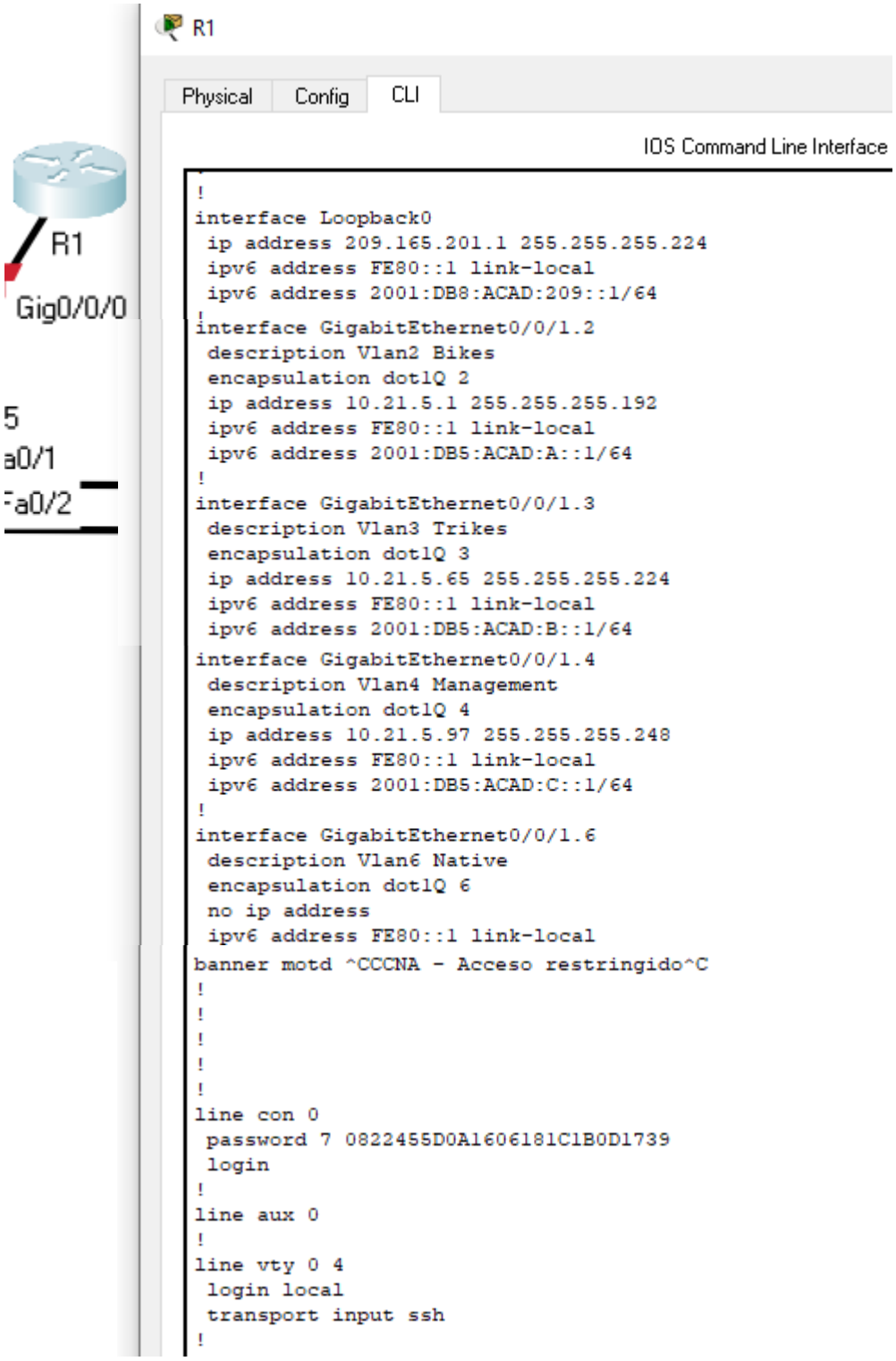
Después de credas las subinterfaces, su activa la interface física **gigabitEthernet 0/0/1** con el comando **no shutdown.**

interface loopback0, configuración de la interface loopback0 con la asignación de direccionamiento IPv4, IPv6 y enlace local. Seguido de **no shutdown** para subir la interface.

crypto key generate rsa general-keys modulus 1024, configuración para generar la clave de cifrado RSA con asignación de 2014 bits. Sin embargo, Para el simulador Packet Tracer **modulus** no está soportado y la línea programada es: **crypto key generate rsa 1024.**

En esta instancia, se pasa las líneas de configuración de la RAM a la NVRAM para ser almacenadas con el comando **do wr.**

*Figura No. 5. Configuración del Router **R1***



Fuente: propia.

Paso 3: Configurar Switches S1 y S2.

Tabla No. 4. Configuración Switch **S1.**

Tarea	Especificación
Desactivar la búsqueda DNS	Switch> Switch>**enable** Switch#**configure terminal** Switch(config)#**no ip domain lookup** Switch(config)#
Nombre del Switch	Switch(config)#**hostname S1** S1(config)#
Nombre de dominio	S1(config)#**ip domain-name ccna-lab.com** S1(config)#
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#**enable secret ciscoenpass** S1(config)#
Contraseña de acceso a la consola	S1(config)#**line console 0** S1(config-line)#**password ciscoconpass** S1(config-line)#**login** S1(config-line)#**exit** S1(config)#
Crear un usuario administrativo en la base de datos local	S1(config)#**username admin password admin1pass** S1(config)#
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#**line vty 0 15** S1(config-line)#**login local** S1(config-line)#**exit** S1(config)#
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)#**line vty 0 15** S1(config-line)#**transport input ssh** S1(config-line)#**login local** S1(config-line)#**exit** S1(config)#
Cifrar las contraseñas de texto no cifrado	S1(config)#**service password-encryption** S1(config)#
Configure un MOTD Banner	S1(config)#**banner motd # *** CCNA - Acceso restringido *** #** S1(config)#
Generar una clave de cifrado RSA Módulo de 1024 bits	S1(config)#**crypto key generate rsa 1024** S1(config)#
Configurar interfaz de administración (SVI)	S1(config)# S1(config)#**interface Vlan4**

Establecer: • Dirección IPv4 de capa 3. • Dirección local de enlace IPv6 como FE80::98 para S1 y FE80::99 para S2. • Dirección IPv6 en capa 3.	S1(config-if)#**ip address 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 Vlan4 Management** S1(config-if)#**no shutdown** S1(config-if)#**exit** S1(config)#
Configuración del Gateway predeterminado. Configure la puerta de enlace predeterminada como 10.21.5.97 para IPv4	S1(config)# S1(config)#**ip default-gateway 10.21.5.97** S1(config)#**do wr** Building configuration... [OK] S1(config)#

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Tabla No. 5. Configuración Switch **S2.**

Tarea	Especificación
Desactivar la búsqueda DNS	Switch> Switch>**enable** Switch#**configure terminal** Switch(config)#**no ip domain lookup** Switch(config)#
Nombre del Switch	Switch(config)#**hostname S2** S2(config)#
Nombre de dominio	S2(config)#**ip domain-name ccna-lab.com** S2(config)#
Contraseña cifrada para el modo EXEC privilegiado	S2(config)#**enable secret ciscoenpass** S2(config)#
Contraseña de acceso a la consola	S2(config)#**line console 0** S2(config-line)#**password ciscoconpass** S2(config-line)#**login** S2(config-line)#**exit** S2(config)#
Crear un usuario administrativo en la base de datos local	S2(config)#**username admin password admin1pass** S2(config)#
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#**line vty 0 15** S2(config-line)#**login local** S2(config-line)#**exit**

	S2(config)#
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config)#**line vty 0 15** S2(config-line)#**transport input ssh** S2(config-line)#**login local** S2(config-line)#**exit** S2(config)#
Cifrar las contraseñas de texto no cifrado	S2(config)#**service password-encryption** S2(config)#
Configure un MOTD Banner	S2(config)#**banner motd # *** CCNA - Acceso restringido *** #** S2(config)#
Generar una clave de cifrado RSA Módulo de 1024 bits	S2(config)#**crypto key generate rsa 1024** S2(config)#
Configurar interfaz de administración (SVI) Establecer: · Dirección IPv4 de capa 3. · Dirección local de enlace IPv6 como FE80::98 para S1 y FE80::99 para S2. · Dirección IPv6 en capa 3.	S2(config)# S2(config)#**interface Vlan4** S2(config-if)#**ip address 10.21.5.99 255.255.255.248** S2(config-if)#**ipv6 address 2001:db5:acad:c::99/64** S2(config-if)#**ipv6 address fe80::98 link-local** S2(config-if)#**description Vlan4 Management** S2(config-if)#**no shutdown** S2(config-if)#**exit** S2(config)#
Configuración del gateway predeterminado. Configure la puerta de enlace predeterminada como 10.21.5.97 para IPv4	S2(config)# S2(config)#**ip default-gateway 10.21.5.97** S2(config)#**do wr** Building configuration... [OK] S2(config)#

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

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

Paso 1: Configuración Switch S1.

Tabla No. 6. Configuración Switch **S1.**

Tarea	Especificación

Crear VLAN VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	S1(config)# S1(config)#**vlan 2** S1(config-vlan)#**name Bikes** S1(config-vlan)#**exit** S1(config)#**vlan 3** S1(config-vlan)#**name Trikes** S1(config-vlan)#**exit** S1(config)#**vlan 4** S1(config-vlan)#**name Management** S1(config-vlan)#**exit** S1(config)#**vlan 5** S1(config-vlan)#**name Parking** S1(config-vlan)#**exit** S1(config)#**vlan 6** S1(config-vlan)#**name Native** S1(config-vlan)#**exit** S1(config)#
Crear troncales 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1, F0/2 y F0/5	S1(config)# S1(config)#**interface fa0/5** S1(config-if)#**switchport trunk encapsulation dot1q** S1(config-if)#**switchport mode trunk** S1(config-if)#**switchport trunk native vlan 6** S1(config-if)#**switchport trunk allowed vlan 2,3,4,6** S1(config-if)#**exit** S1(config)# S1(config)#**interface range fastEthernet 0/1-2** S1(config-if-range)# **shutdown** S1(config-if-range)#**switchport trunk encapsulation dot1q** S1(config-if-range)#**switchport mode trun k** S1(config-if-range)#**switchport trunk native vlan 6** S1(config-if-range)#**switchport trunk allowed vlan 2,3,4,6** S1(config-if-range)#**exit** S1(config)#
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 Usar el protocolo LACP para la	S1(config)# S1(config)#**interface range fastEthernet 0/1-2** S1(config-if-range)#**channel-group 1 mode active**

negociación	S1(config-if-range)#**channel-protocol lacp** S1(config-if-range)#**interface Port-channel 1** S1(config-if)#**switchport trunk encapsulation dot1q** S1(config-if)#**switchport mode trun k** S1(config-if)#**switchport trunk native vlan 6** S1(config-if)#**exit** S1(config)#
Configurar el puerto de acceso de host para VLAN 2 en la Interface F0/6	S1(config)# S1(config)#**interface fastEthernet 0/6** S1(config-if)#**switchport mode access** S1(config-if)#**switchport access vlan 2** S1(config-if)#**exit** S1(config)#
Configurar la seguridad del puerto en los puertos de Acceso Permitir 3 direcciones MAC	S1(config)# S1(config)#**interface fastEthernet 0/6** S1(config-if)#**switchport port-security maximum 3** S1(config-if)#**exit** S1(config)#
Proteja todas las interfaces no utilizadas Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S1(config)# S1(config)#**interface range fa0/3-4, fa0/7-24, gig0/1-2** S1(config-if-range)#**switchport mode access** S1(config-if-range)#**switchport access vlan 5** S1(config-if-range)#**description *** Puertos sin utilizar ***** S1(config-if-range)#**shutdown** S1(config-if-range)#**exit** S1(config)#**do wr** Building configuration... [OK] S2(config)#

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 2: Configuración Switch S2.

Tabla No. 7. Configuración Switch **S2.**

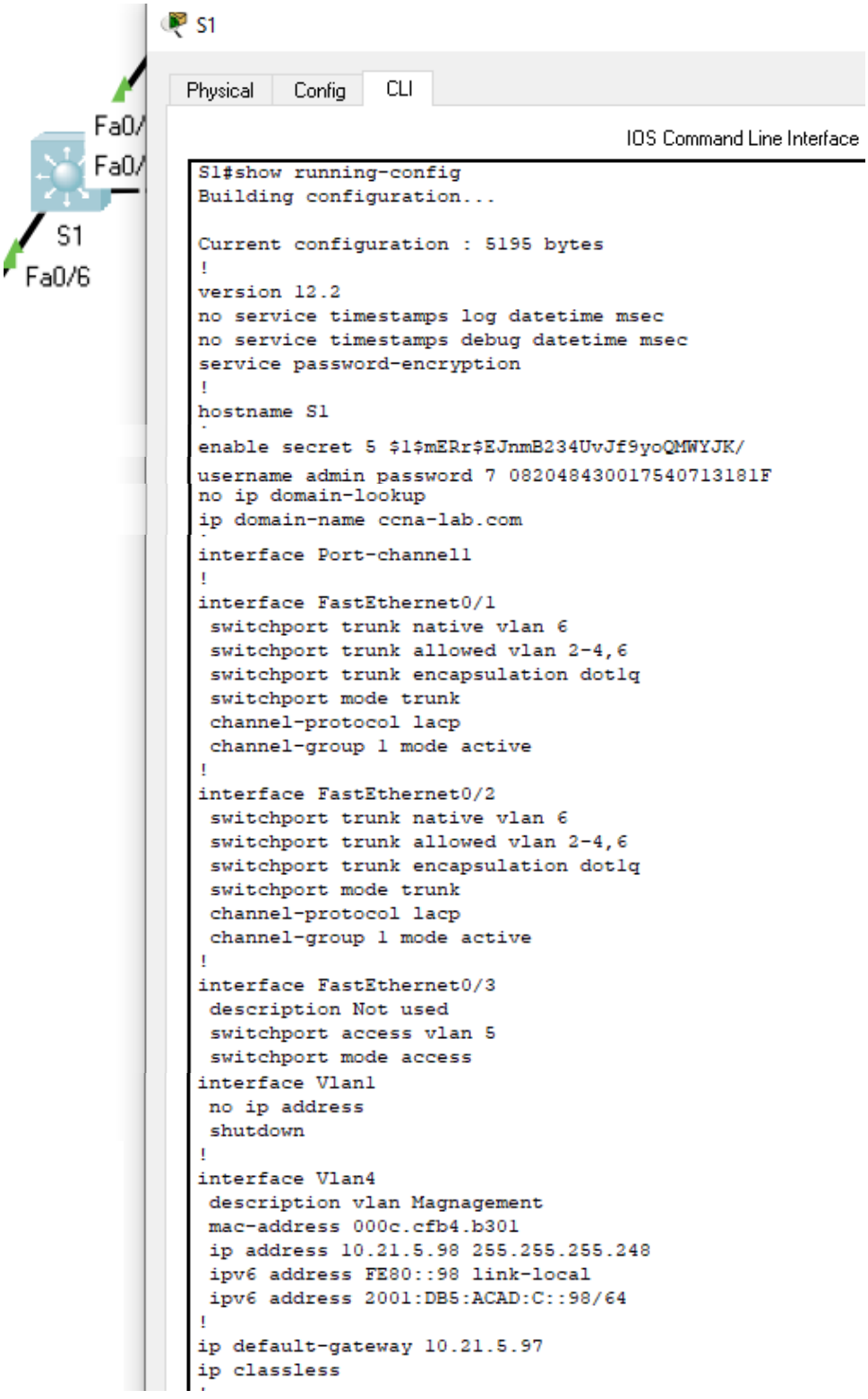
Tarea	Especificación
Crear VLAN VLAN 2, nombre Bikes	S2(config)# S2(config)#**vlan 2** S2(config-vlan)#**name Bikes**

VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	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)#**do wr** Building configuration... [OK] S2(config-vlan)#**exit** S2(config)#
Crear troncales 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1 y F0/2	S2(config)# S2(config)#**interface range fastEthernet 0/1-2** S2(config-if-range)# **shutdown** S2(config-if-range)#**switchport trunk encapsulation dot1q** S2(config-if-range)#**switchport mode trun k** S2(config-if-range)#**switchport trunk native vlan 6** S2(config-if-range)#**switchport trunk allowed vlan 2,3,4,6** S2(config-if-range)#**exit** S2(config)#
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 Usar el protocolo LACP para la negociación.	S2(config)# S2(config)#**interface range fastEthernet 0/1-2** S2(config-if-range)#**channel-group 1 mode active** S2(config-if-range)#**interface Port-channel 1** S2(config-if-range)#**channel-protocol lacp** S2(config-if)#**switchport trunk encapsulation dot1q** S2(config-if)#**switchport mode trunk** S2(config-if)#**switchport trunk native vlan 6** S2(config-if)#**exit** S2(config)#
Configurar el puerto de acceso de host para VLAN 3 en la Interface F0/18	S2(config)# S2(config)#**interface fastEthernet 0/18** S2(config-if)#**switchport mode access** S2(config-if)#**switchport access vlan 3** S2(config-if)#**exit**

	S2(config)#**do wr** Building configuration... [OK] S1(config)#
Configure port-security en los access ports Permitir 3 direcciones MAC	S2(config)# S2(config)#**interface fastEthernet 0/18** S2(config-if)#**switchport mode access** S2(config-if)#**switchport port-security maximum 3** S2(config-if)#**exit** S2(config)#
Proteja todas las interfaces no utilizadas Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S2(config)# S2(config)#**interface range fa0/3-17, fa0/19-24, gig0/1-2** S2(config-if-range)#**switchport mode access** S2(config-if-range)#**switchport access vlan 5** S2(config-if-range)# **switchport port-security** S2(config-if-range)# **switchport port-security violation shutdown** S2(config-if-range)#**description ***Puertos sin utilizar ***** S2(config-if-range)#**shutdown** S2(config-if)#**do wr** Building configuration... [OK] S2(config-if)#**exit** S2(config)#

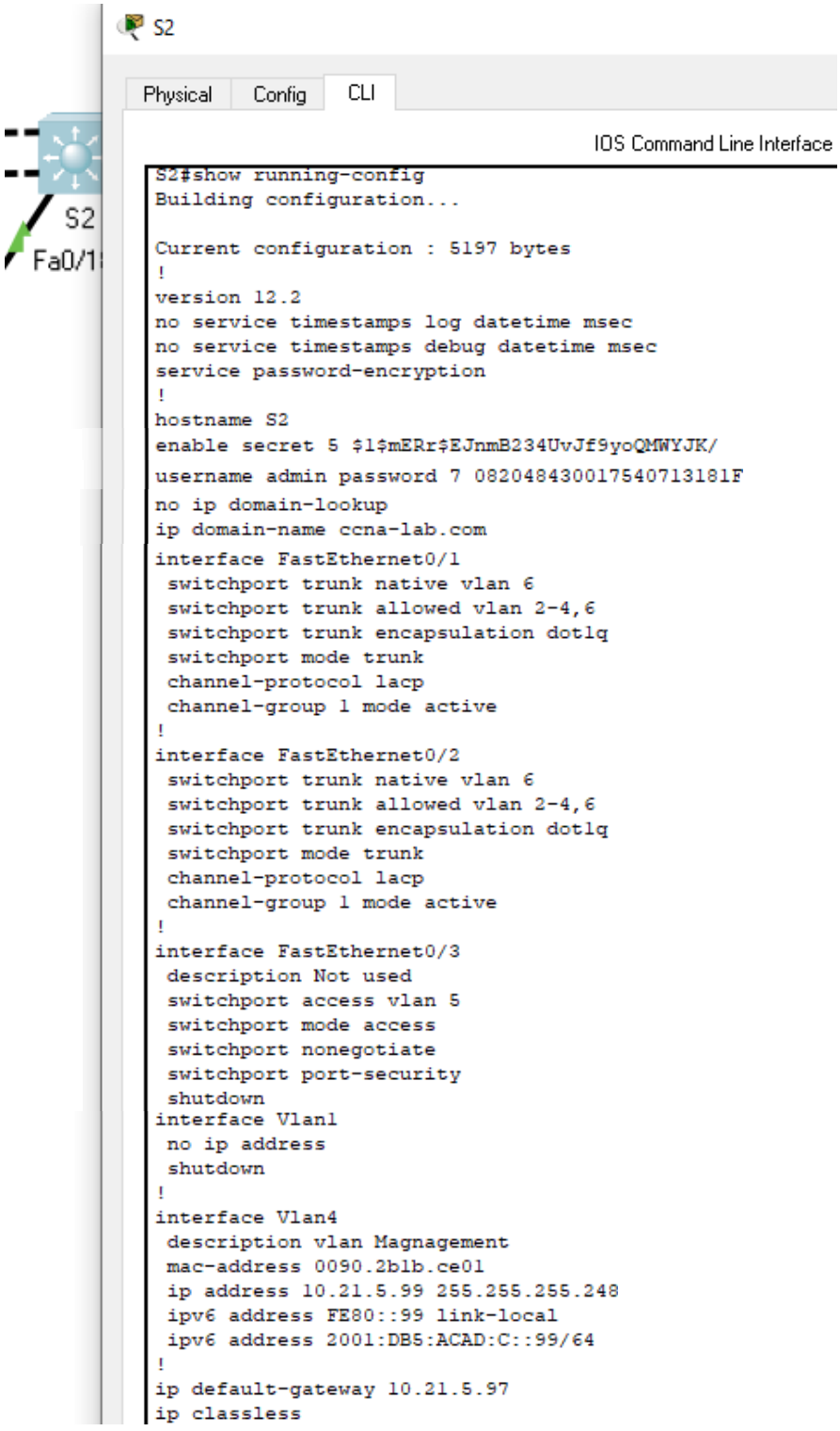
Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

*Figura No. 6. Configuración Switch **S1***



Fuente: propia.

*Figura No. 7. Configuración Switch **S2***



Fuente: propia.

3.1.3 Parte 3: Configurar soporte de Host.

Paso 1: Configuración Router R1.

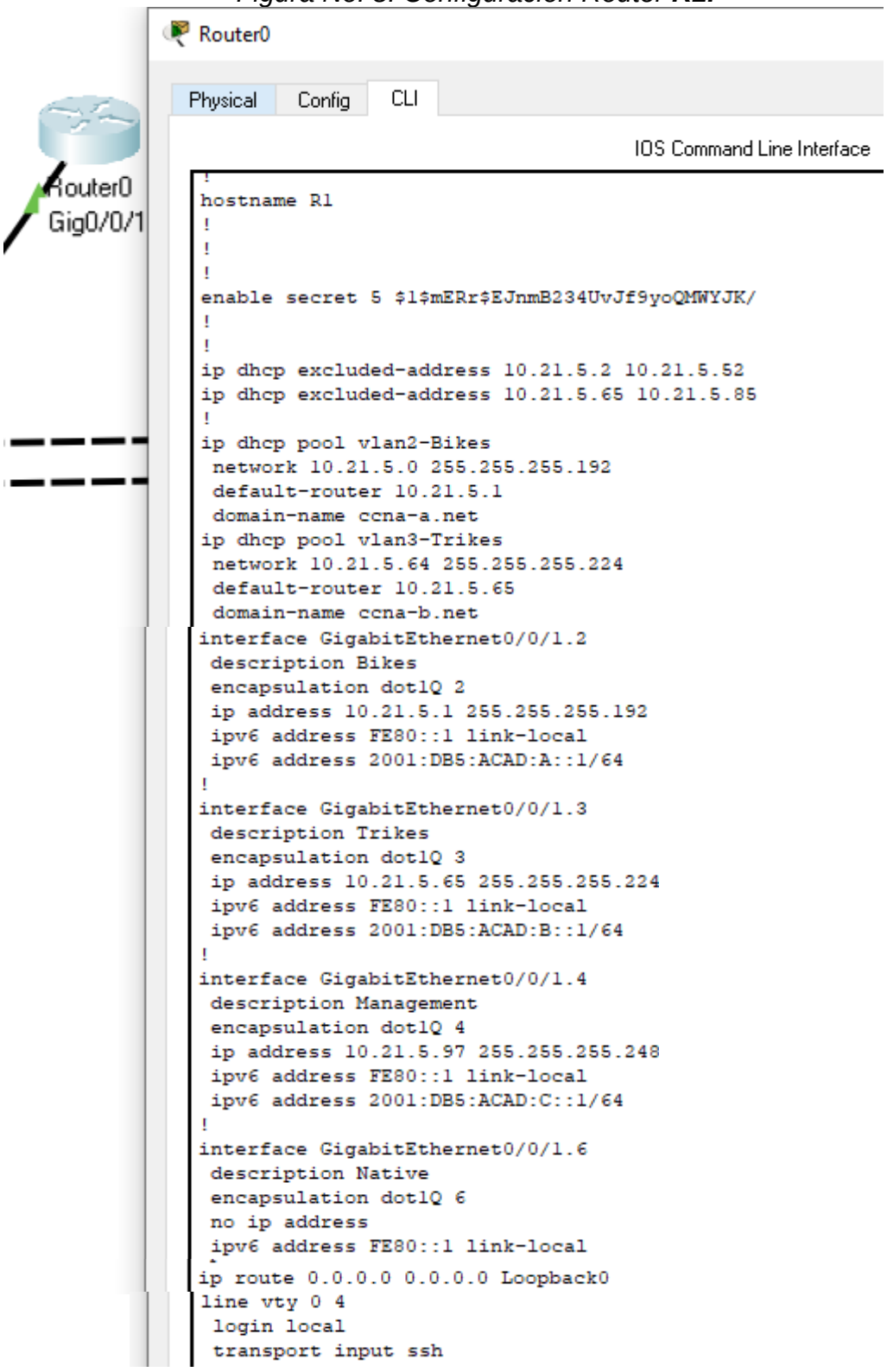
Las tareas de configuración para R1 incluyen las siguientes:

Tabla No. 8. Configuración de soporte Host en Router (**R1**)

Tarea	Especificación
Configure Default Routing Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0	R1>**enable** R1#**configure terminal** R1(config)# **ip route 0.0.0.0 0.0.0.0 loopback 0** R1(config)# **ipv6 route ::/0 loopback 0** R1(config)#**exit** R1#
Configurar IPv4 DHCP para VLAN 2 Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada	R1(config)# **ip dhcp excluded-address 10.21.5.2 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** R1(config)# R1#
Configurar DHCP IPv4 para VLAN 3 Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada.	R1(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** R1(config)#**do wr** R1(config)# R1#

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

*Figura No. 8. Configuración Router **R1.***



Fuente: propia.

Paso 2: Configurar los servidores.

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

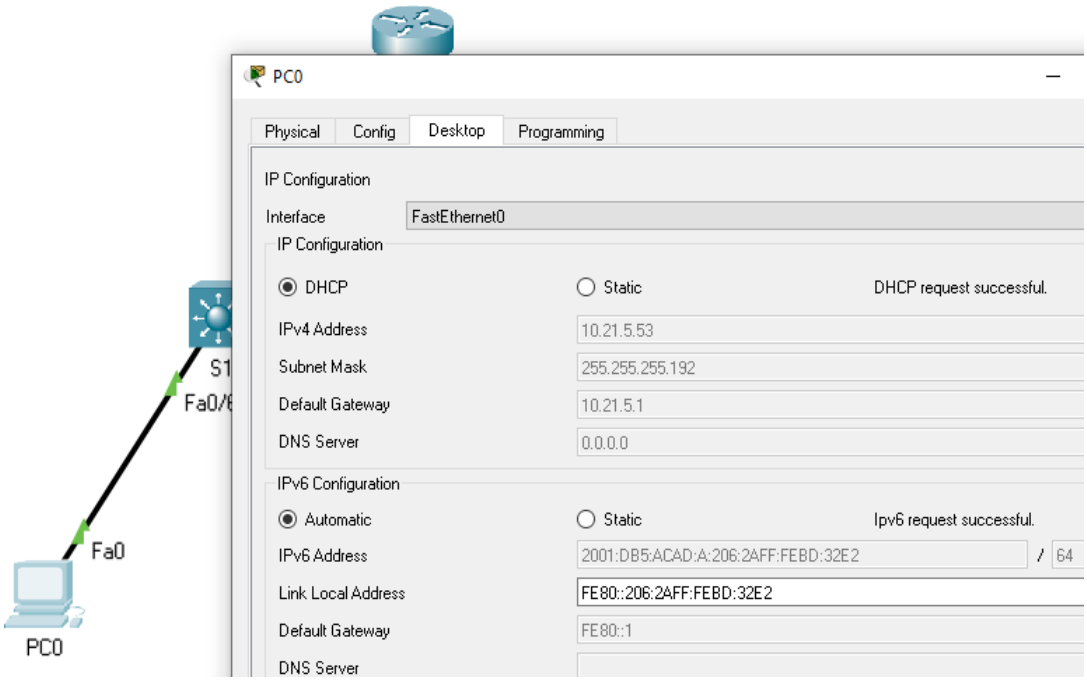
En las PC-A y B se activa el DHCP para IPv4 y configuración automática para IPv6.

Tabla No. 9. Configuración de red del PC-A

Configuración de red de PC-A	
Descripción	**PC-A**
Dirección física	**0006.2ABD.32E2**
Dirección IP	**10.21.5.53**
Máscara de subred	**255.255.255.192**
Gateway predeterminado	**10.21.5.1**
Gateway predeterminado IPv6	**FE80::1**

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

*Figura No. 9. Configuración **PC-A***



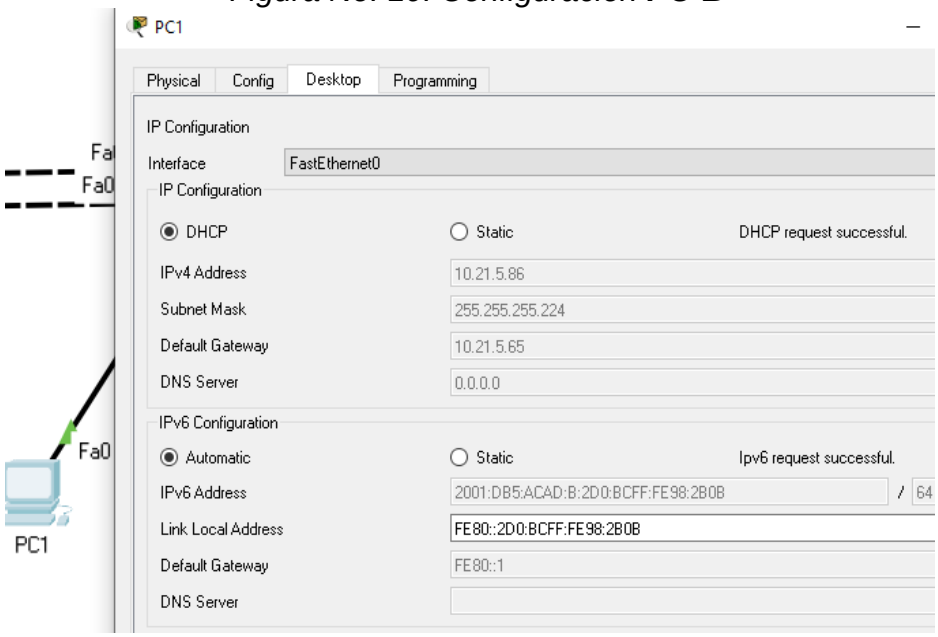
Fuente: propia.

Tabla No. 10. Configuración de red del PC-B

Configuración de red de PC-B	
Descripción	**PC-B**
Dirección física	**00D0.BC98.2B0B**
Dirección IP	**10.21.5.86**
Máscara de subred	**255.255.255.224**
Gateway predeterminado	**10.21.5.65**
Gateway predeterminado IPv6	**FE80::1**

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

*Figura No. 10. Configuración **PC-B***



Fuente: propia.

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

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

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

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

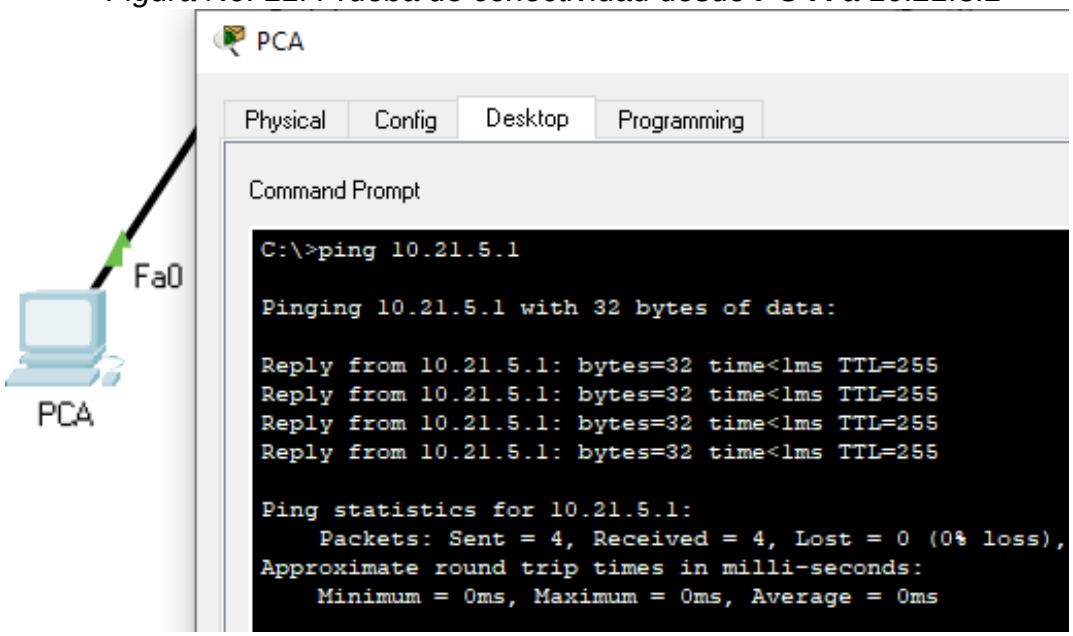
Tabla No. 11. Prueba de conectividad de red

Desde	A	de Internet	Dirección IP	Resultados de PING
PC-A	R1, G0/0/1.2	Dirección	10.21.5.1	✓
		IPv6	2001:db5:acad:a::1	✓
	R1, G0/0/1.3	Dirección	10.21.5.65	✓
		IPv6	2001:db5:acad:b::1	✓
	R1, G0/0/1.4	Dirección	10.21.5.97	✓
		IPv6	2001:db5:acad:c::1	✓
	S1, VLAN 4	Dirección	10.21.5.98	✓
		IPv6	2001:db5:acad:c::98	✓
	S2, VLAN 4	Dirección	10.21.5.99	✓
		IPv6	2001:db5:acad:c::99	✓
	PC-B	Dirección	10.21.5.86 (esta IP puede cambiar al momento de ejecutar la simulación por ser **DHCP**)	✓
		IPv6	2001:db5:acad:b::50	✓
	R1 Bucle 0	Dirección	209.165.201.1	✓
		IPv6	2001:db5:acad:209::1	✓
PC-B	R1 Bucle 0	Dirección	209.165.201.1	✓
		IPv6	2001:db5:acad:209::1	✓
	R1, G0/0/1.2	Dirección	10.21.5.1	✓
		IPv6	2001:db5:acad:a::1	✓
	R1, G0/0/1.3	Dirección	10.21.5.65	✓
		IPv6	2001:db5:acad:b::1	✓
	R1, G0/0/1.4	Dirección	10.21.5.97	✓
		IPv6	2001:db5:acad:c::1	✓
	S1, VLAN 4	Dirección	10.21.5.98	✓
		IPv6	2001:db5:acad:c::98	✓
	S2, VLAN 4	Dirección	10.21.5.99	✓
		IPv6	2001:db5:acad:c: :99	✓

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

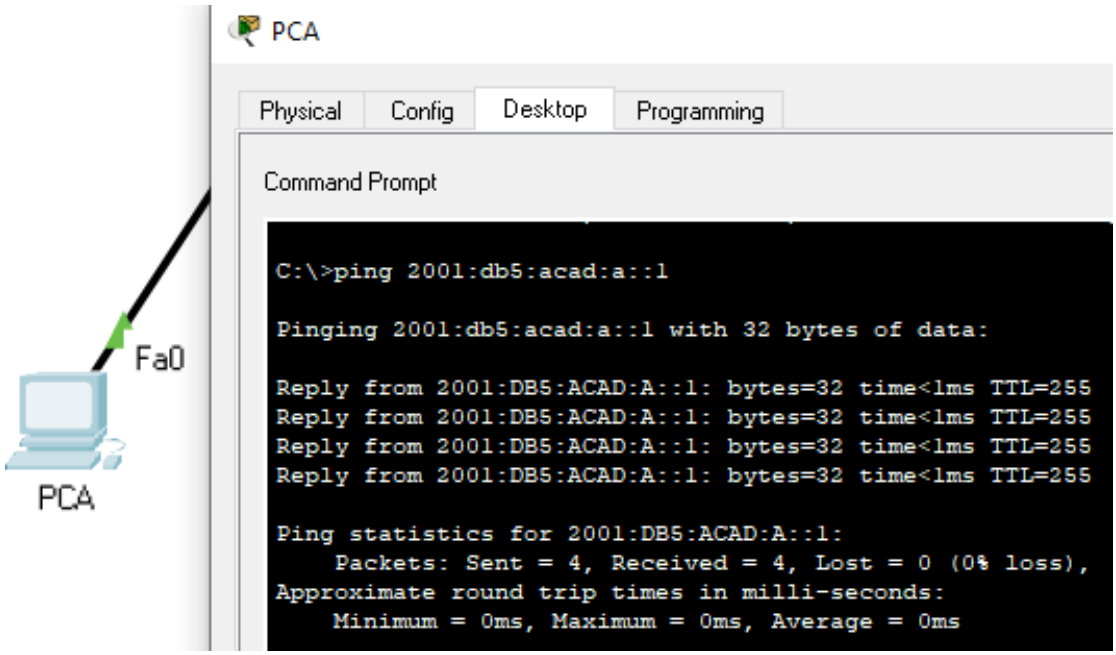
A continuación, se relacionan a través de imágenes el registro de conectividad a con la herramienta ping desde los PC's hacia las interfaces y subinterfaces de la topología.

*Figura No. 11. Prueba de conectividad desde **PC-A** a 10.21.5.1*



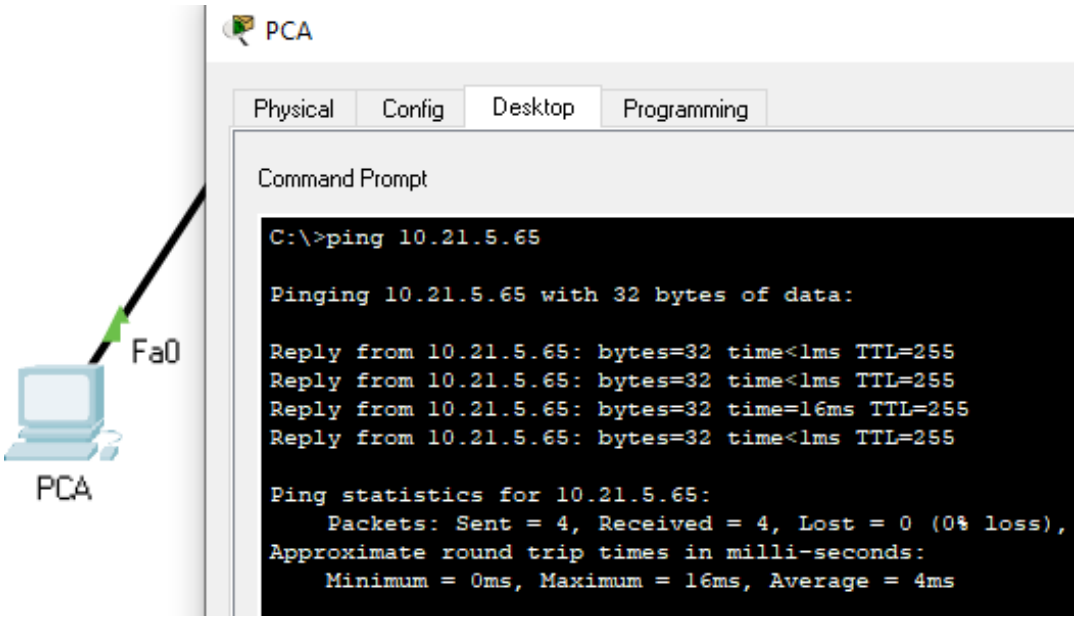
Fuente: propia.

*Figura No. 12. Prueba de conectividad desde **PC-A** a 2001:db5:acad:a::1*



Fuente: propia.

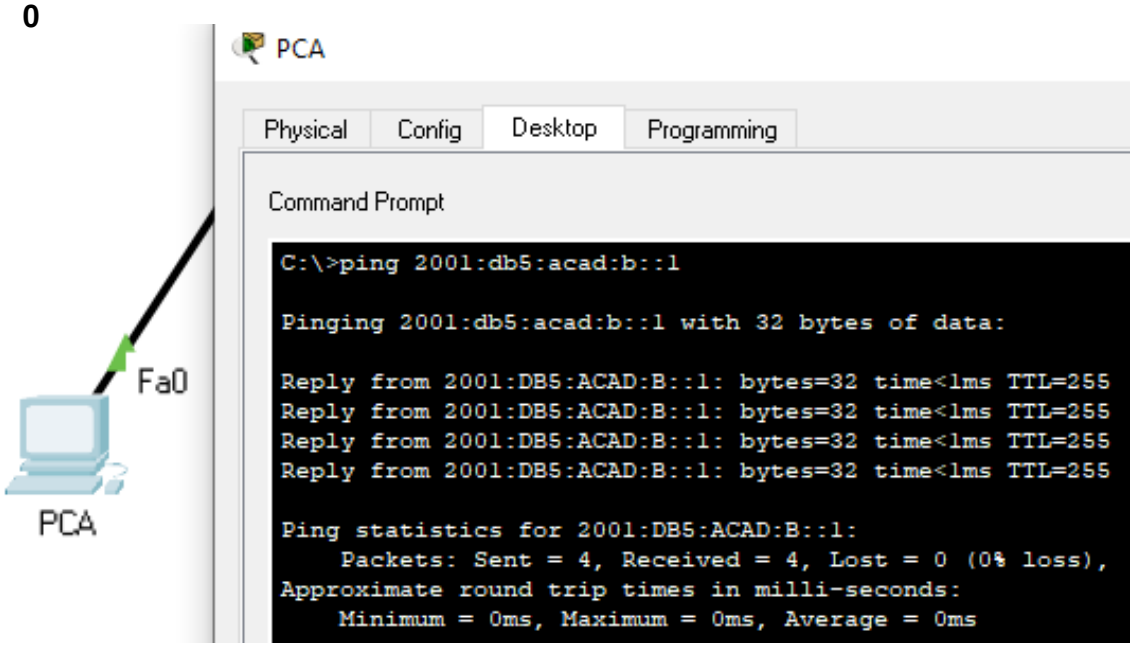
*Figura No. 13. Prueba de conectividad desde **PC-A** a 10.21.5.65*



Fuente: propia.

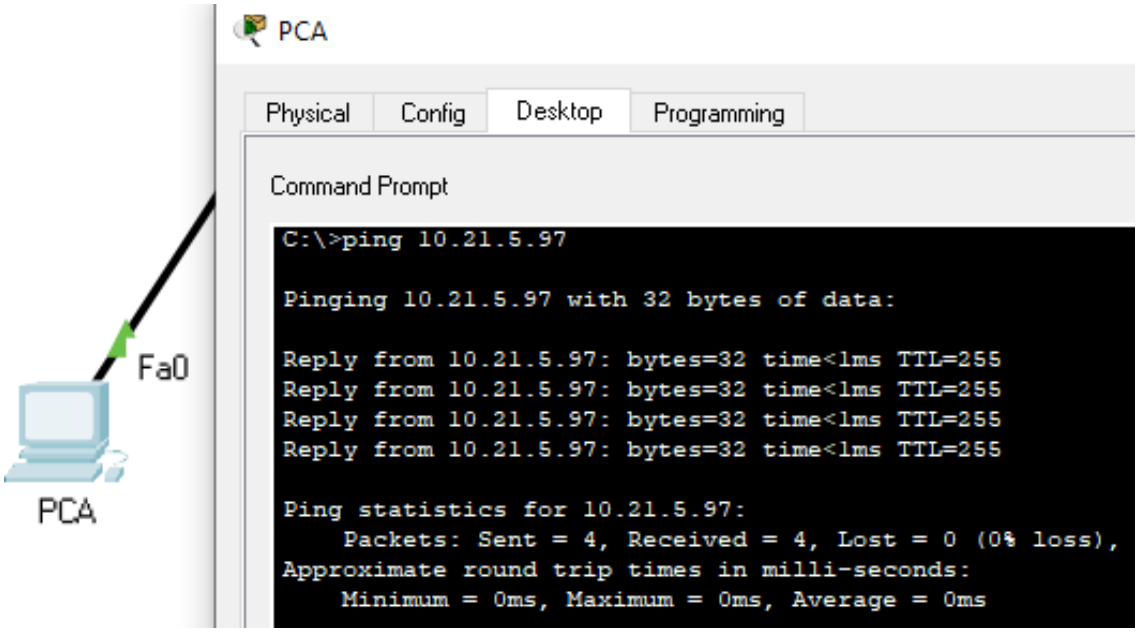
*Figura No. 14. Prueba de conectividad desde **PC-A** a 2001:db5:acad:b::1*

0



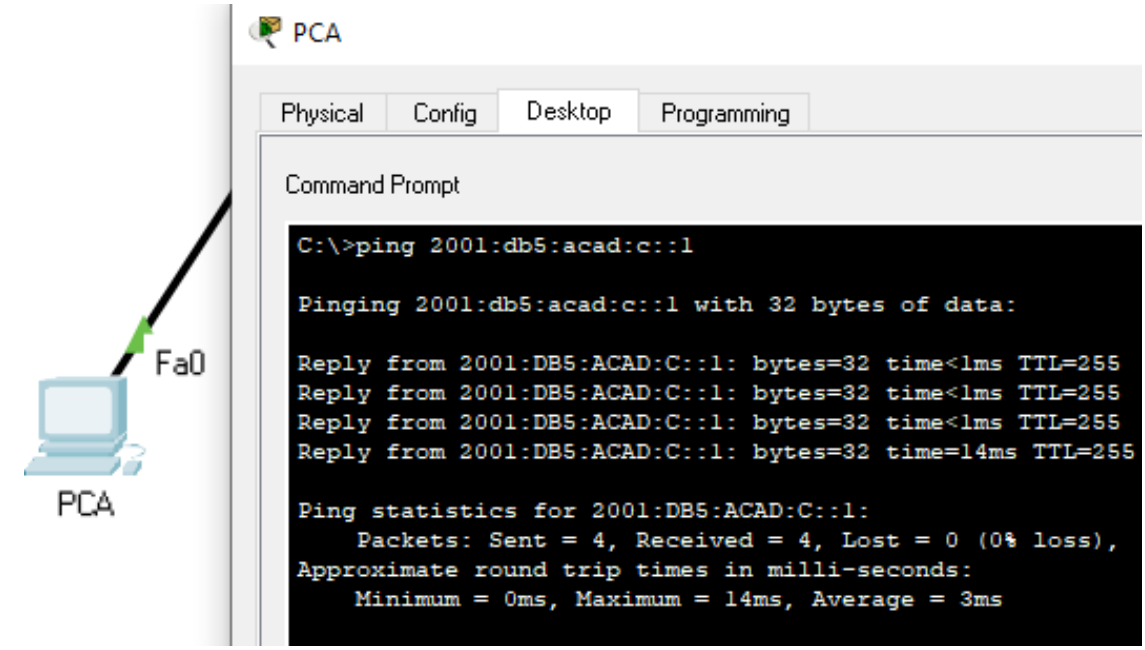
Fuente: propia.

*Figura No. 15. Prueba de conectividad desde **PC-A** a 10.21.5.97*



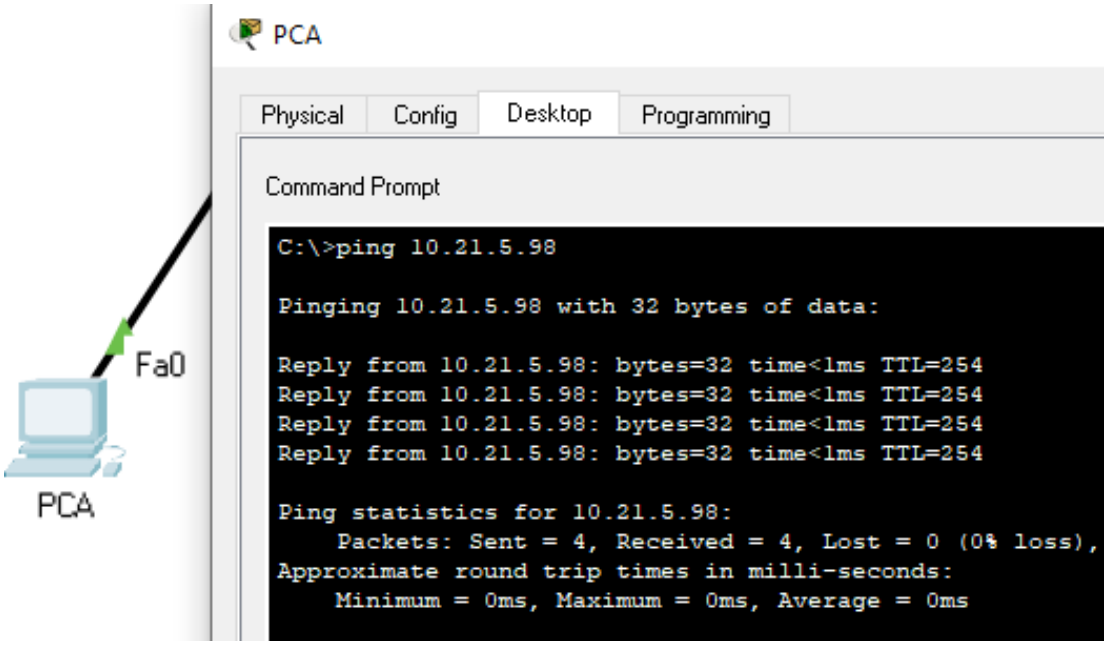
Fuente: propia.

*Figura No. 16. Prueba de conectividad desde **PC-A** a 2001:db5:acad:c: :1*



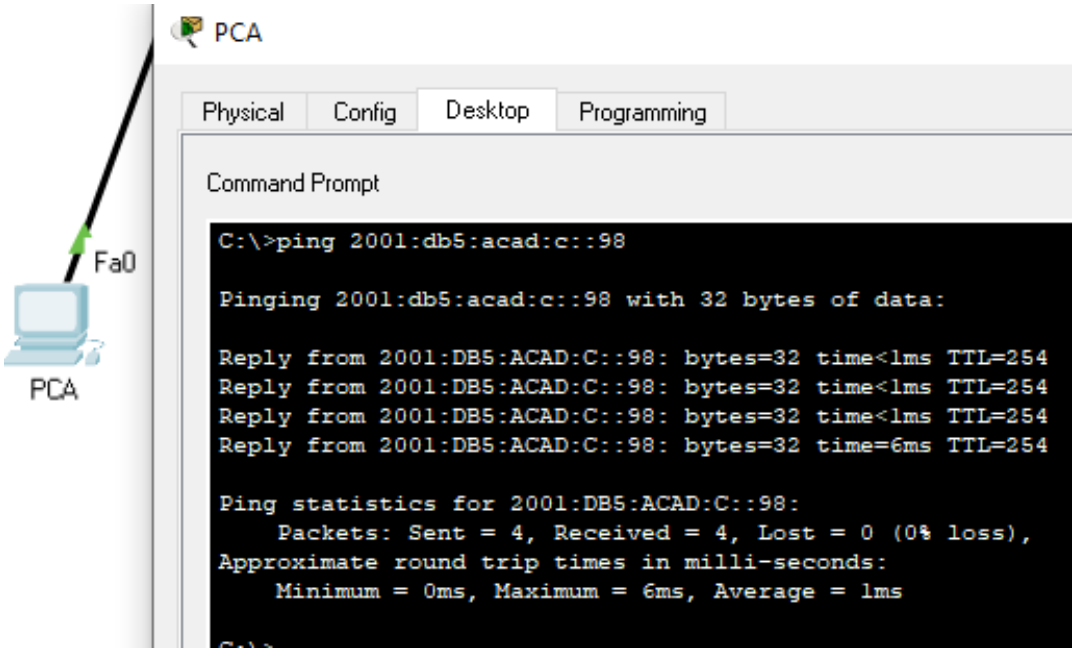
Fuente: propia.

*Figura No. 17. Prueba de conectividad desde **PC-A** a 10.21.5.98*



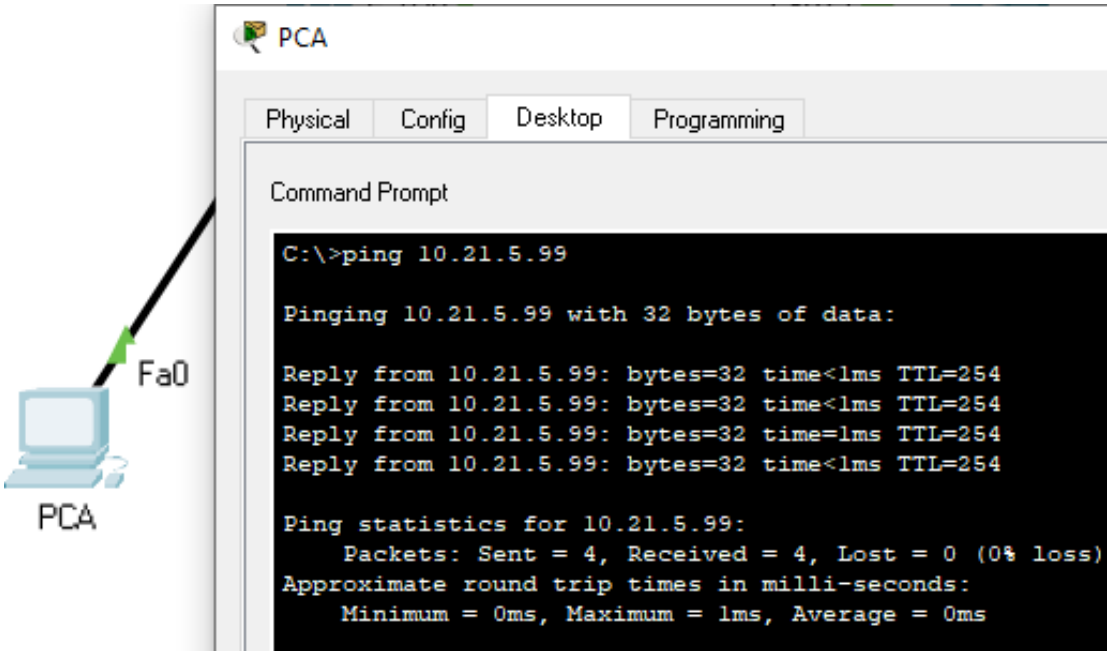
Fuente: propia.

*Figura No. 18. Prueba de conectividad desde **PC-A** a 2001:db5:acad:c::98*



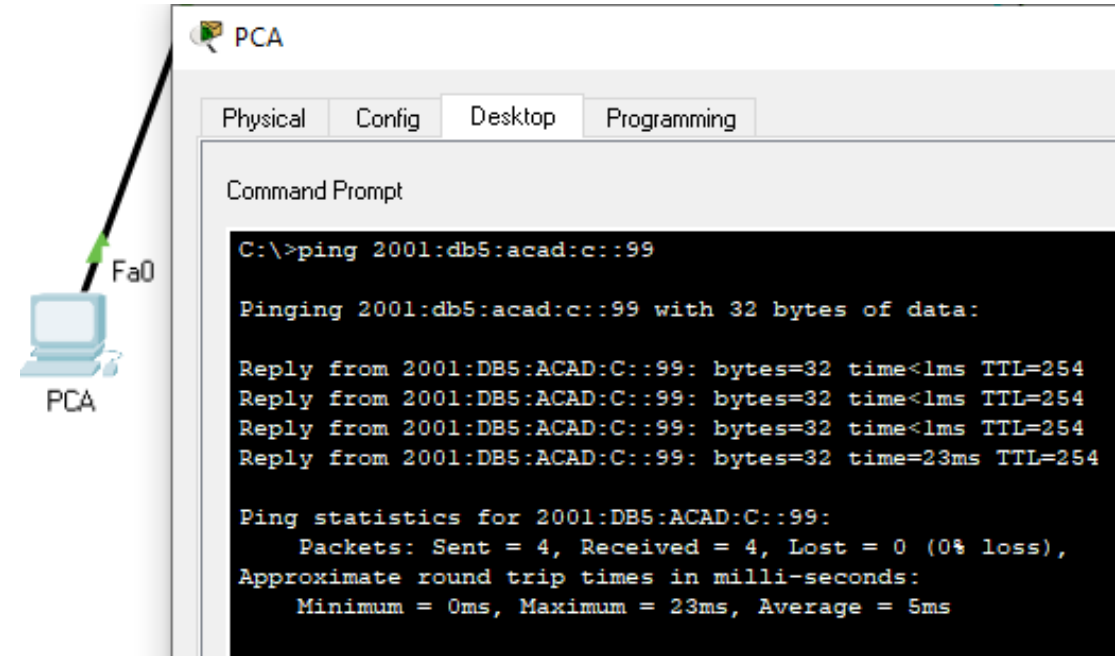
Fuente: propia.

*Figura No. 19. Prueba de conectividad desde **PC-A** a 10.21.5.99*



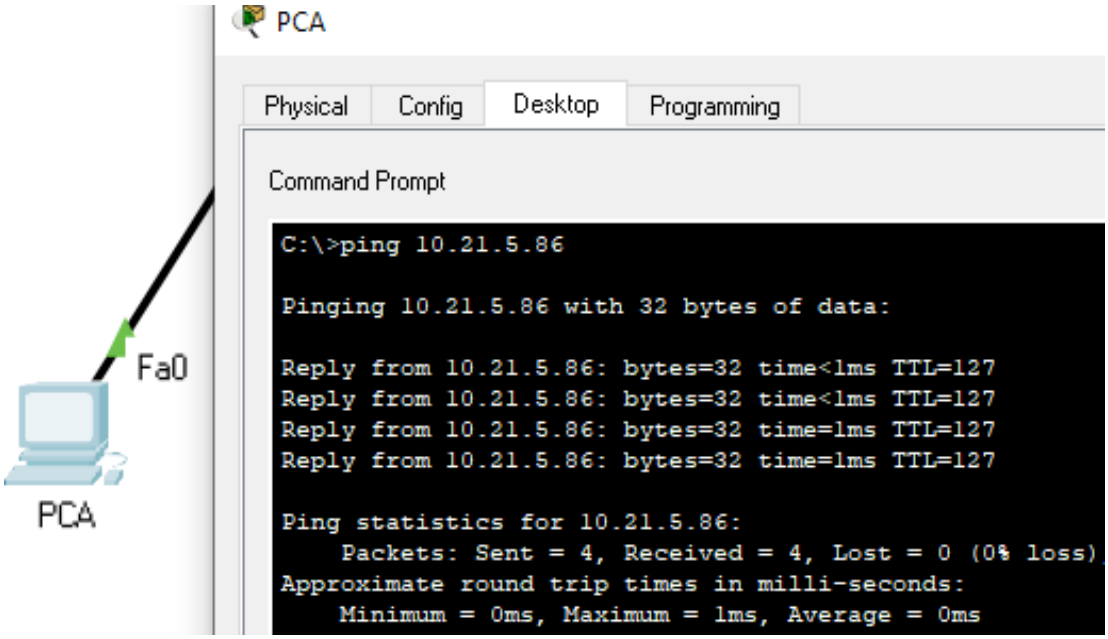
Fuente: propia.

*Figura No. 20. Prueba de conectividad desde **PC-A** a 2001:db5:acad:c::99*



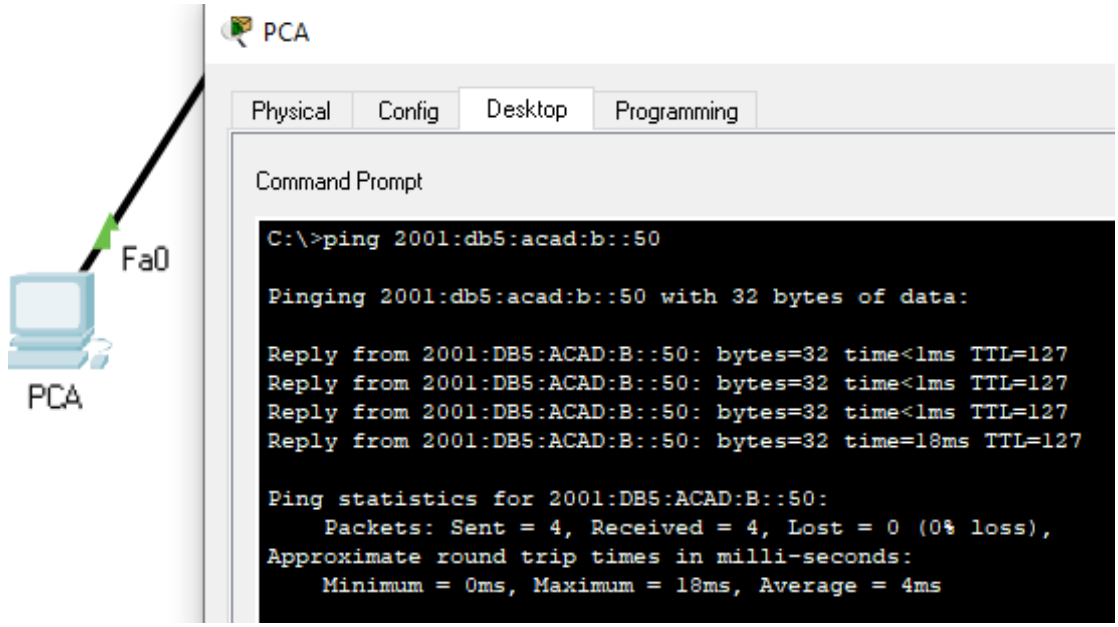
Fuente: propia.

*Figura No. 21. Prueba de conectividad desde **PC-A** a 10.21.5.86*



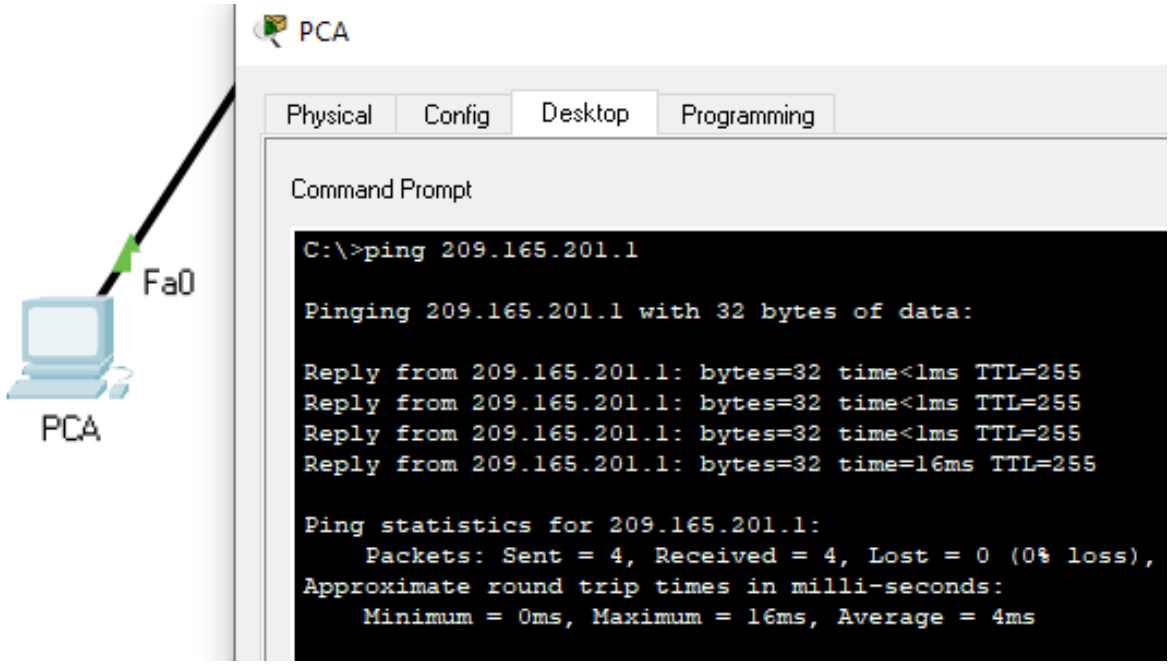
Fuente: propia.

*Figura No. 22. Prueba de conectividad desde **PC-A** a 2001:db5:acad:b::50*



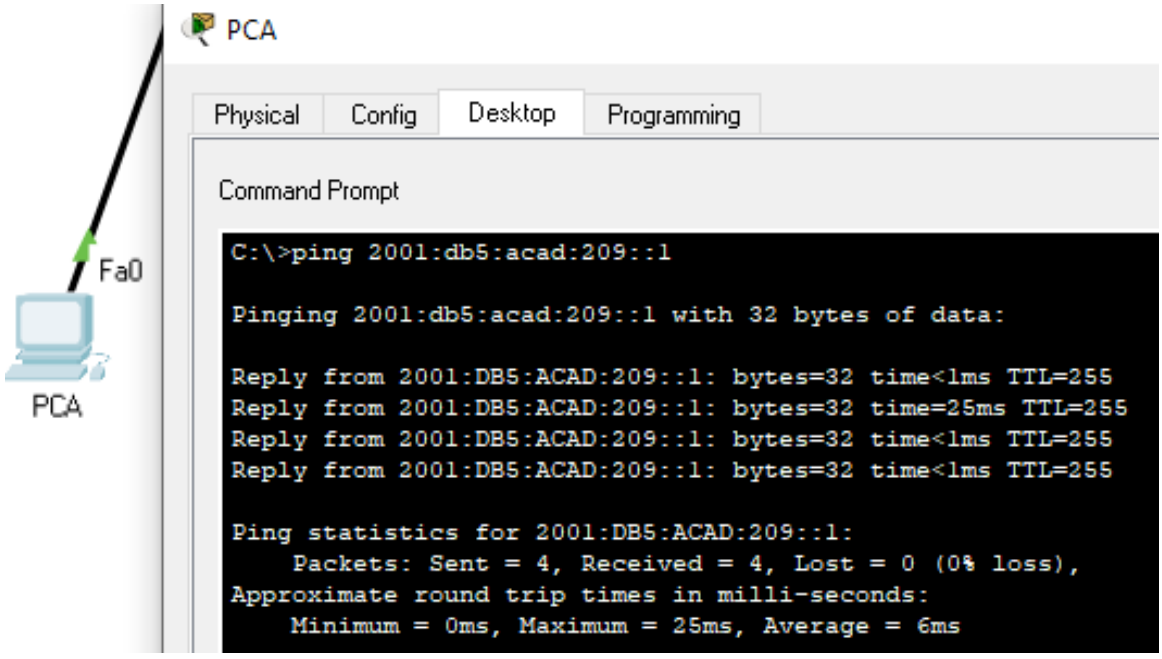
Fuente: propia.

*Figura No. 23. Prueba de conectividad desde **PC-A** a 209.165.201.1*



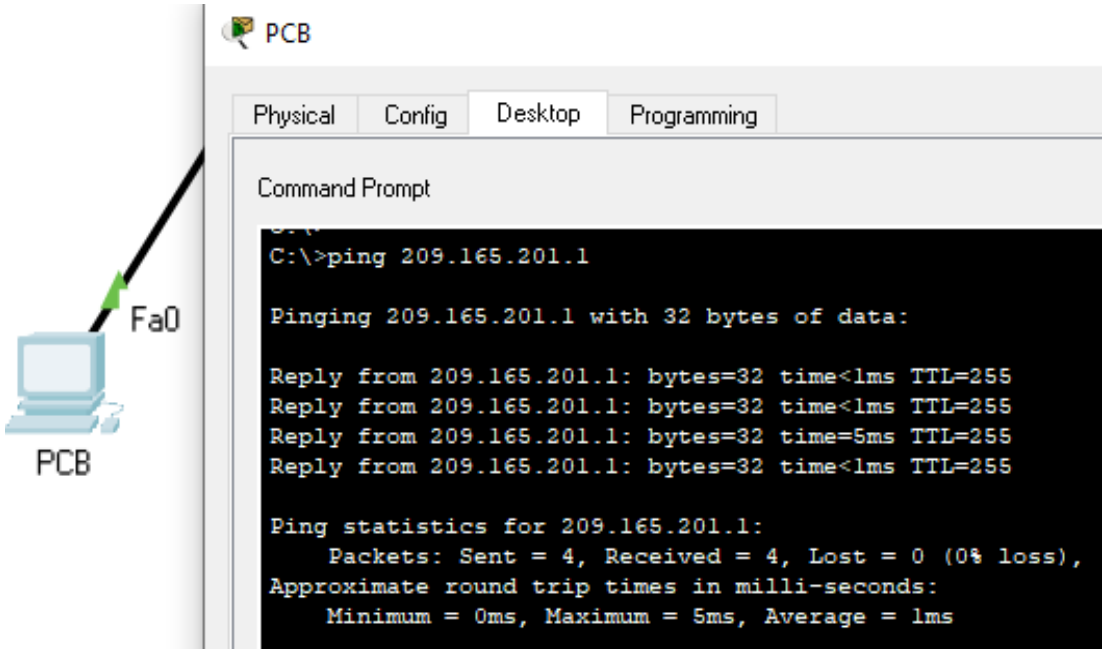
Fuente: propia.

*Figura No. 24. Prueba de conectividad desde **PC-A** a 2001:db5:acad:209::1*



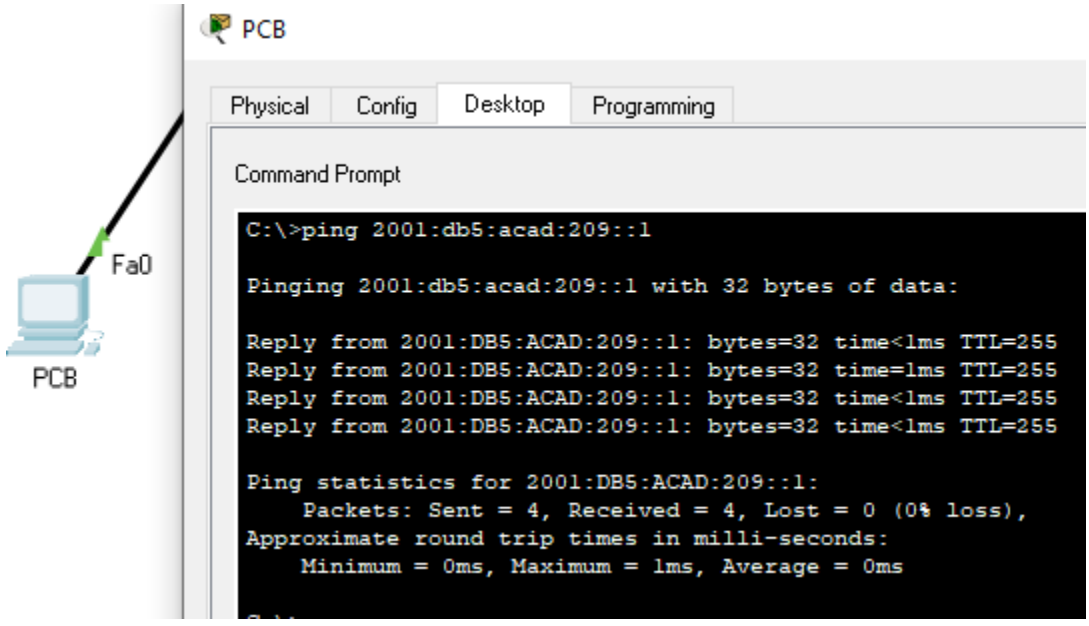
Fuente: propia.

*Figura No. 25. Prueba de conectividad desde **PC-B** a 209.165.201.1*



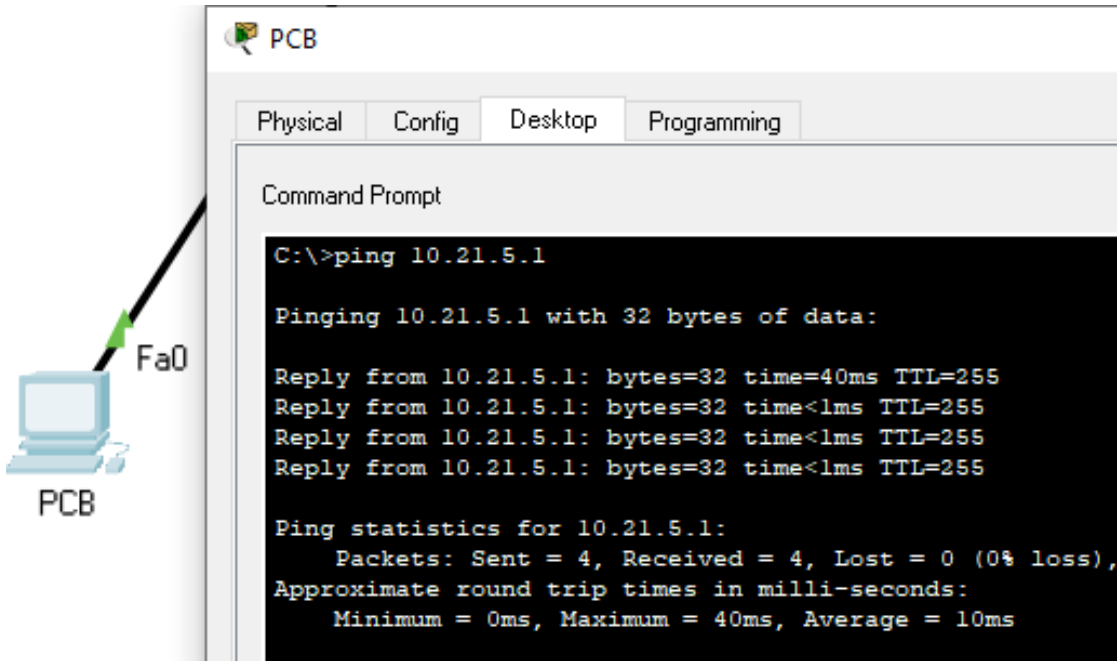
Fuente: propia.

*Figura No. 26. Prueba de conectividad desde **PC-B** a 2001:db5:acad:209::1*



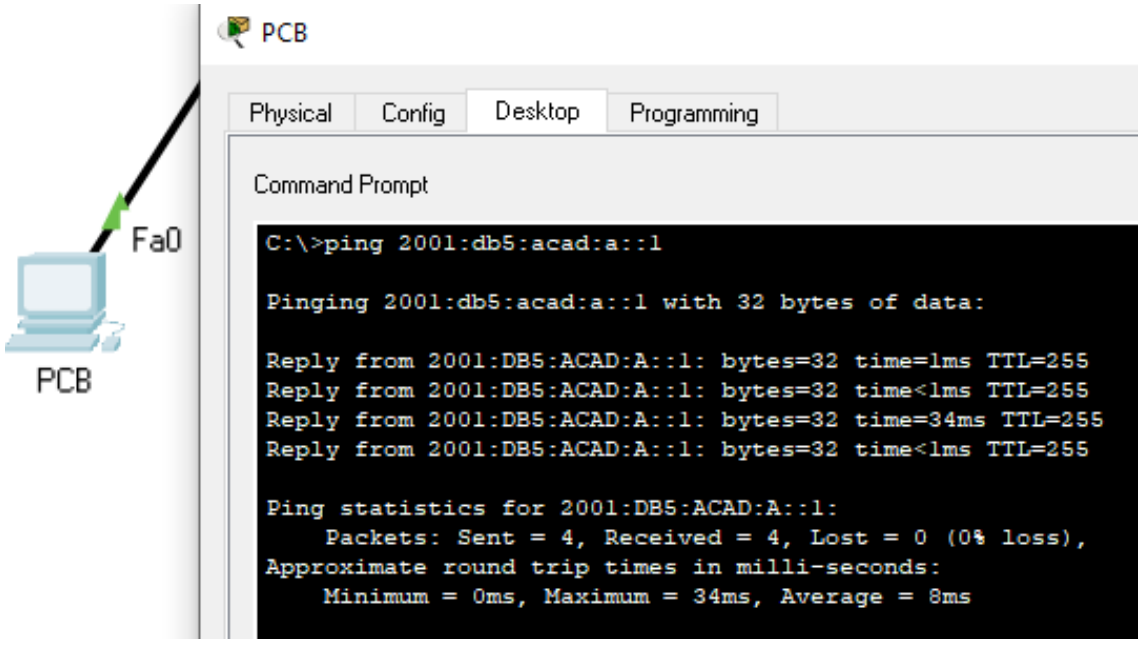
Fuente: propia.

*Figura No. 27. Prueba de conectividad desde **PC-B** a 10.21.5.1*



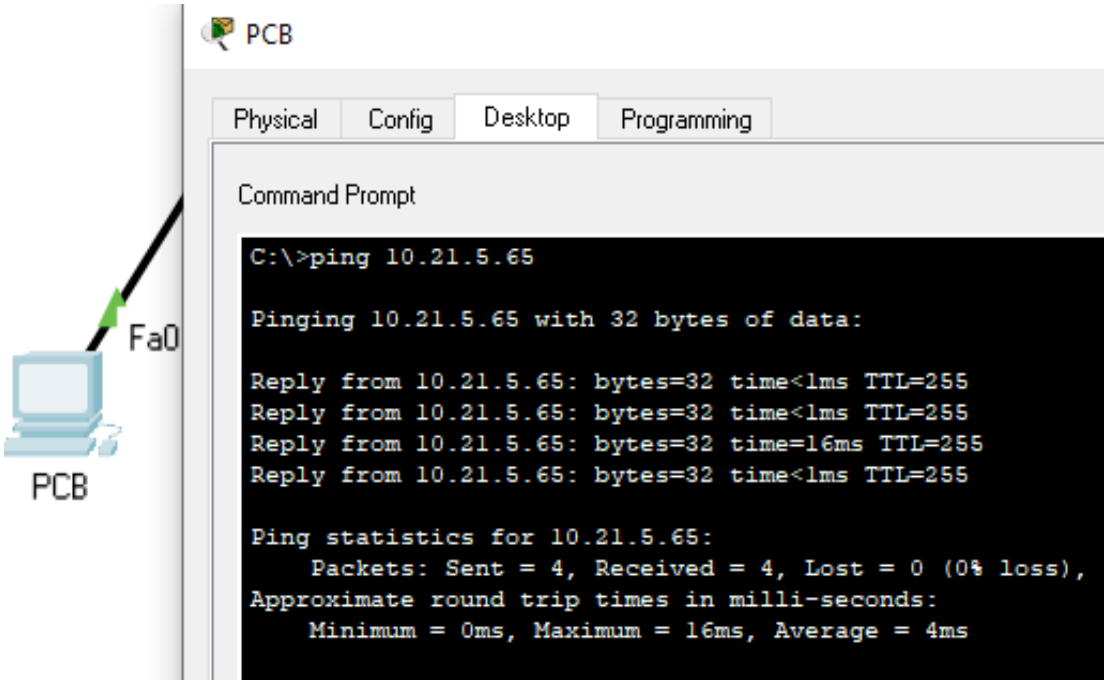
Fuente: propia.

*Figura No. 28. Prueba de conectividad desde **PC-B** a 2001:db5:acad:a::1*



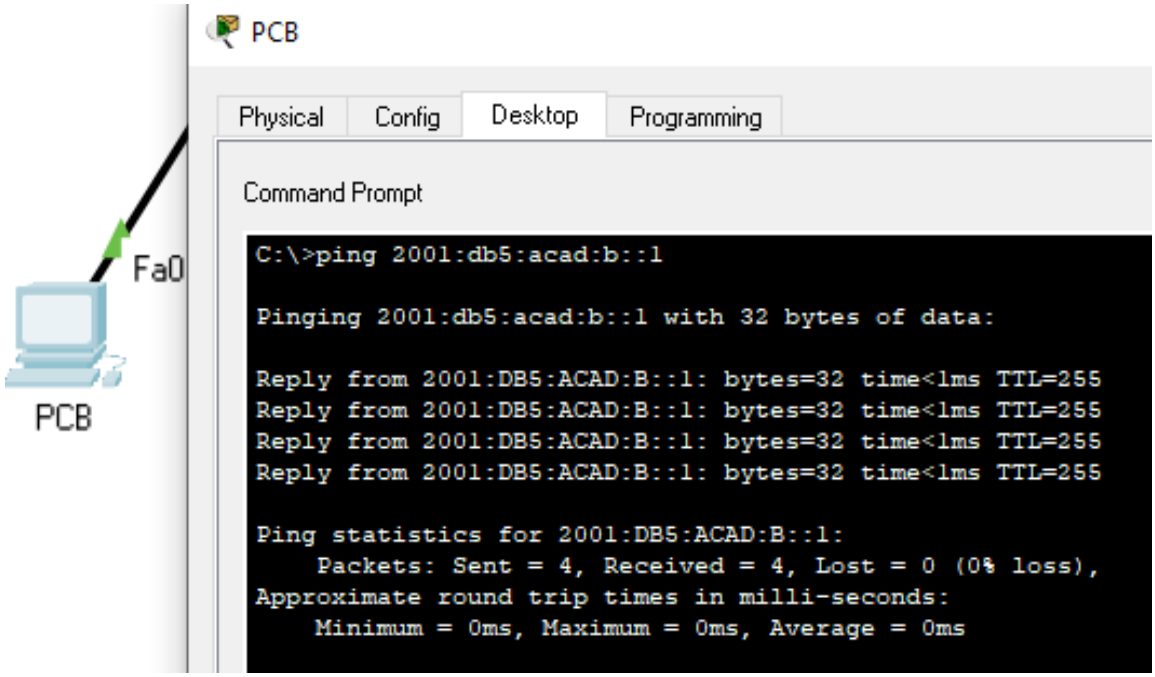
Fuente: propia.

*Figura No. 29. Prueba de conectividad desde **PC-B** a 10.21.5.65*



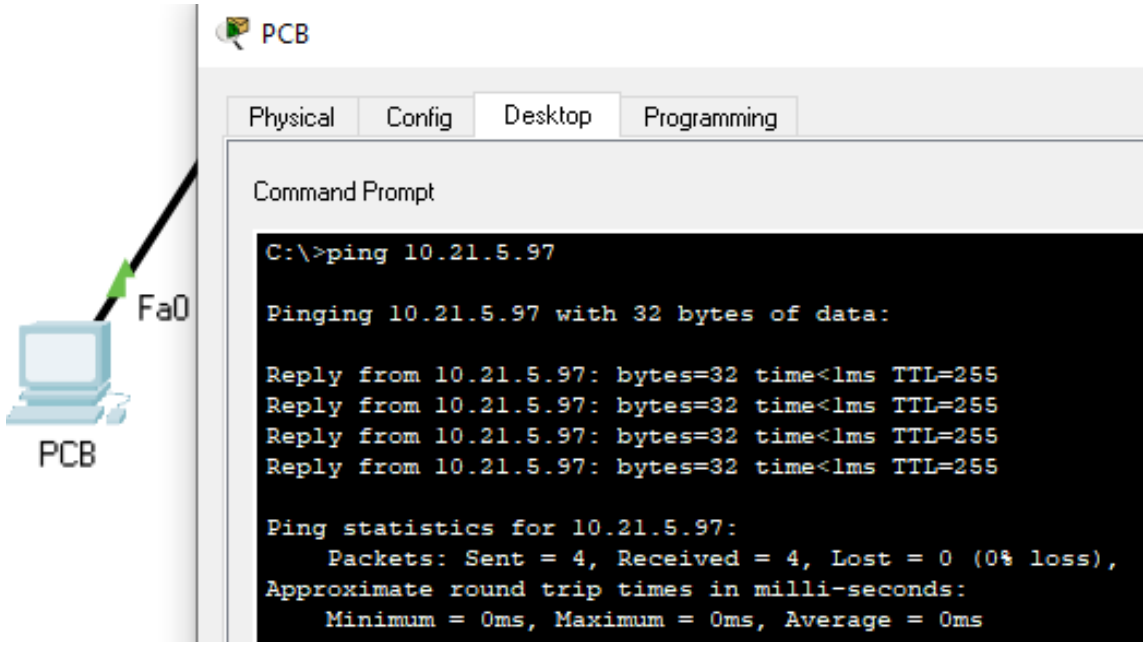
Fuente: propia.

*Figura No. 30. Prueba de conectividad desde **PC-B** a 2001:db5:acad:b::1*



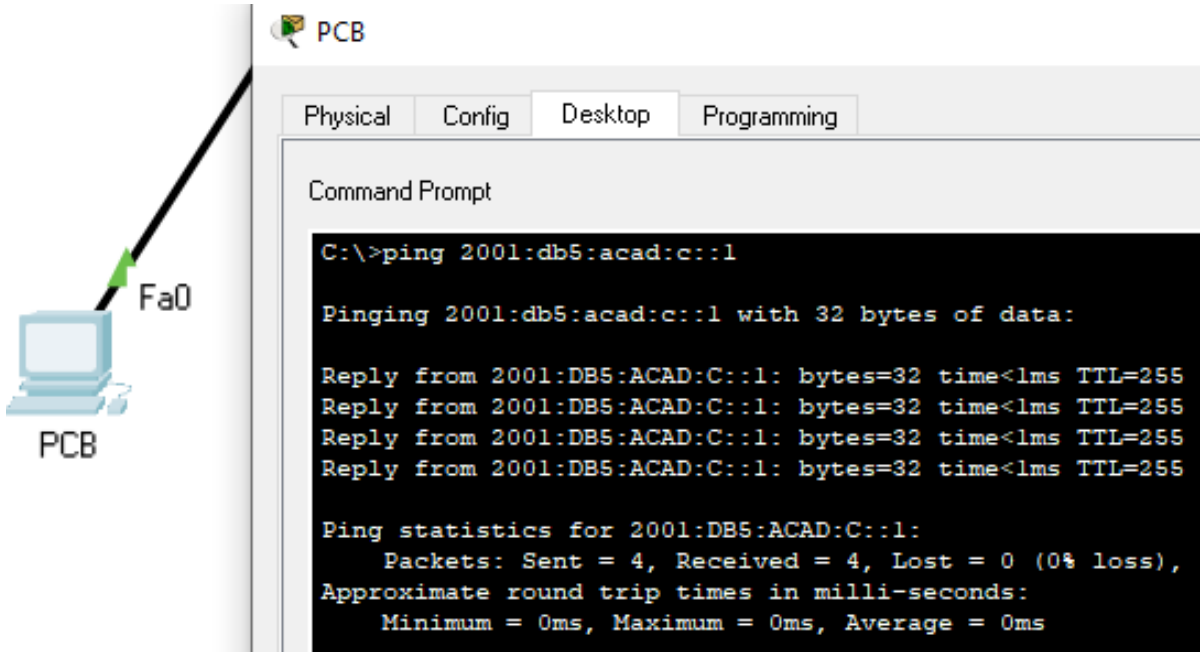
Fuente: propia.

*Figura No. 31. Prueba de conectividad desde **PC-B** a 10.21.5.97*



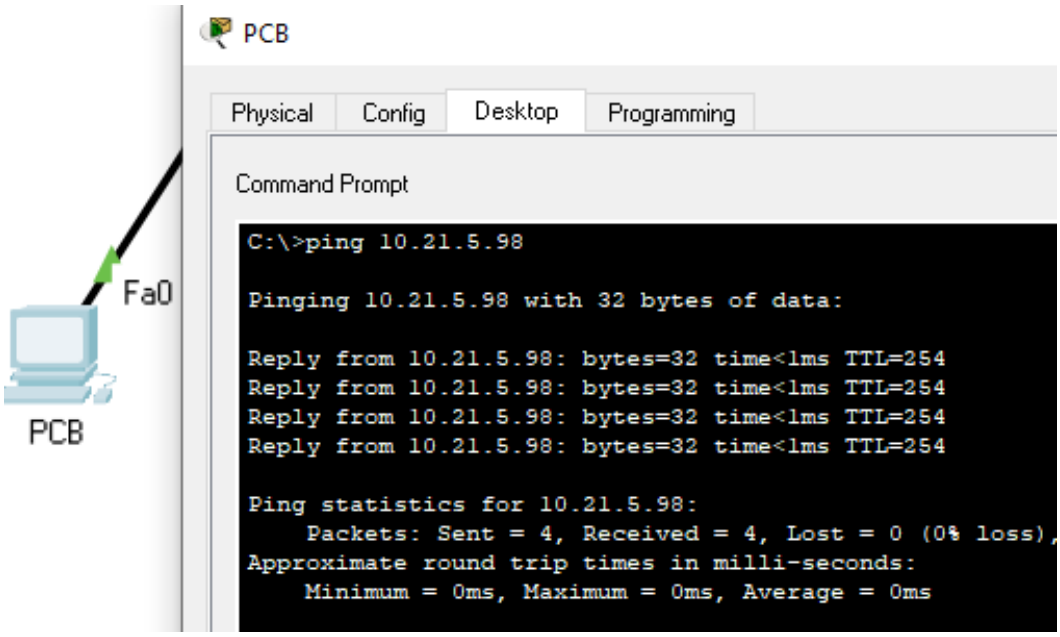
Fuente: propia.

*Figura No. 32. Prueba de conectividad desde **PC-B** a 2001:db5:acad:c::1*



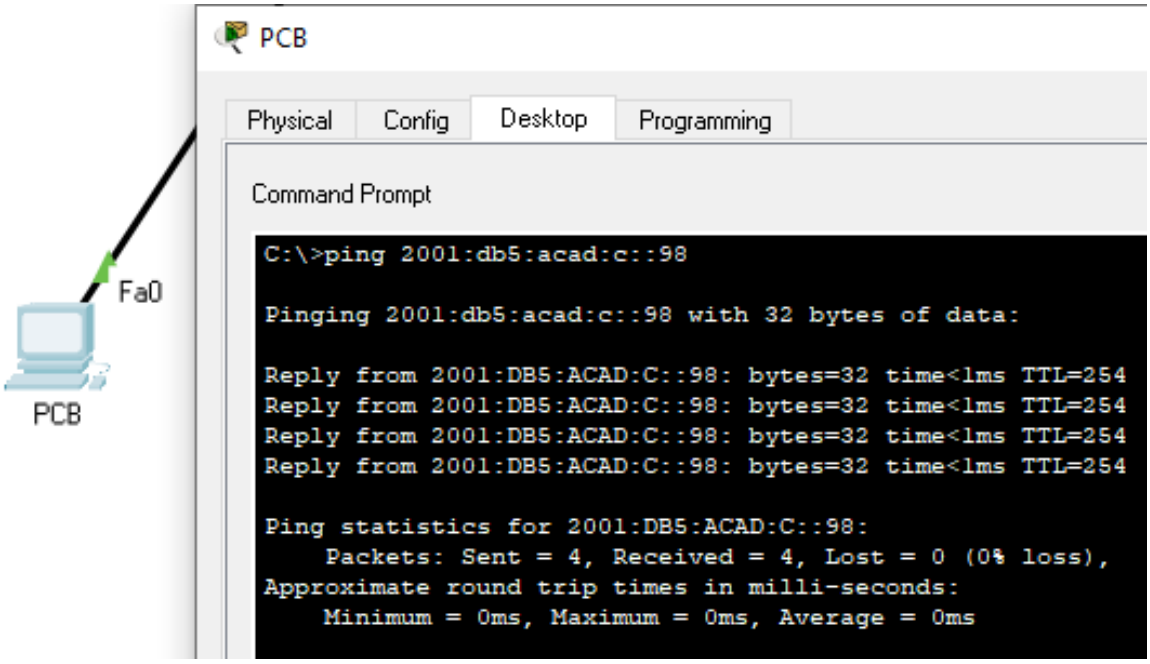
Fuente: propia.

*Figura No. 33. Prueba de conectividad desde **PC-B** a 10.21.5.98*



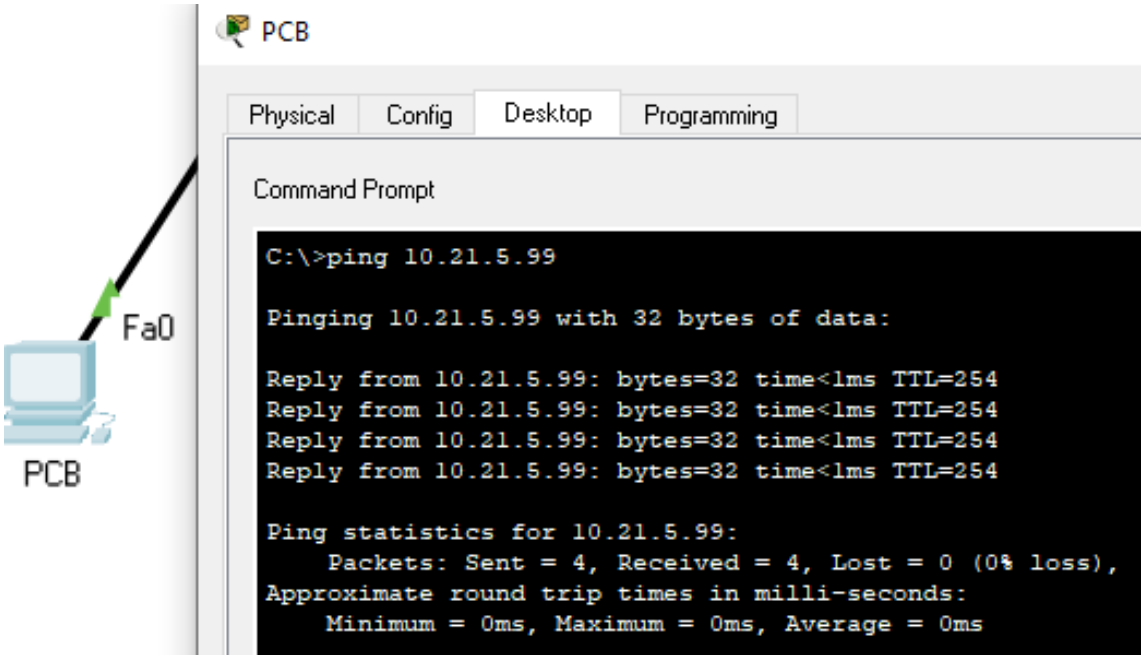
Fuente: propia.

*Figura No. 34. Prueba de conectividad desde **PC-B** a 2001:db5:acad:c::98*



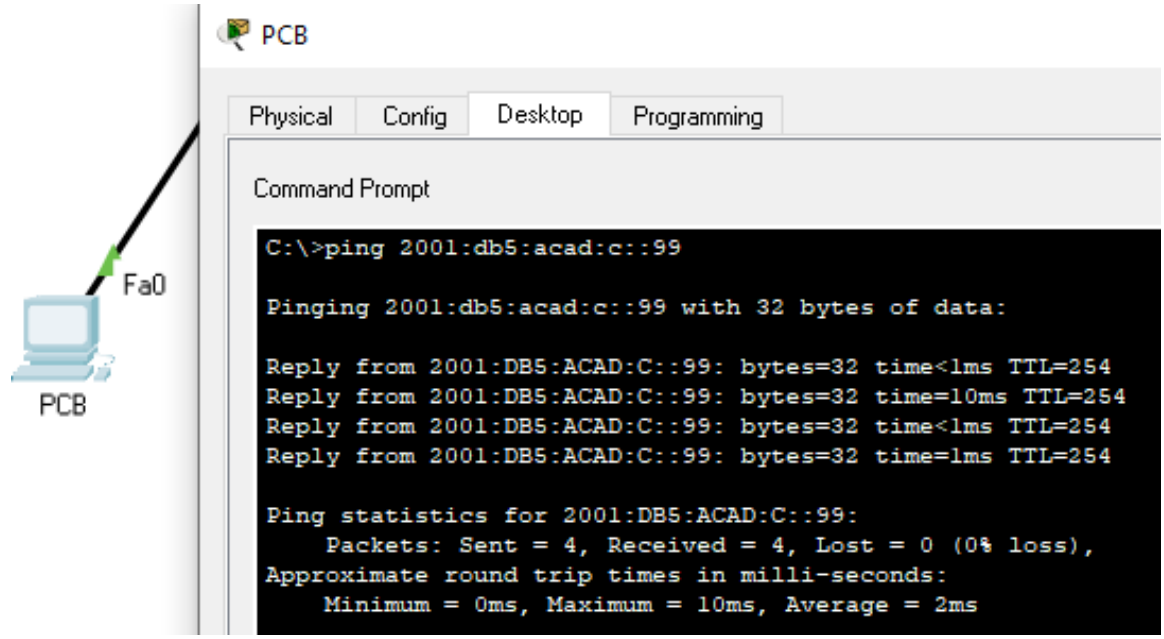
Fuente: propia.

*Figura No. 35. Prueba de conectividad desde **PC-B** a 10.21.5.99*



Fuente: propia.

*Figura No. 36. Prueba de conectividad desde **PC-B** a 2001:db5:acad:c::99*

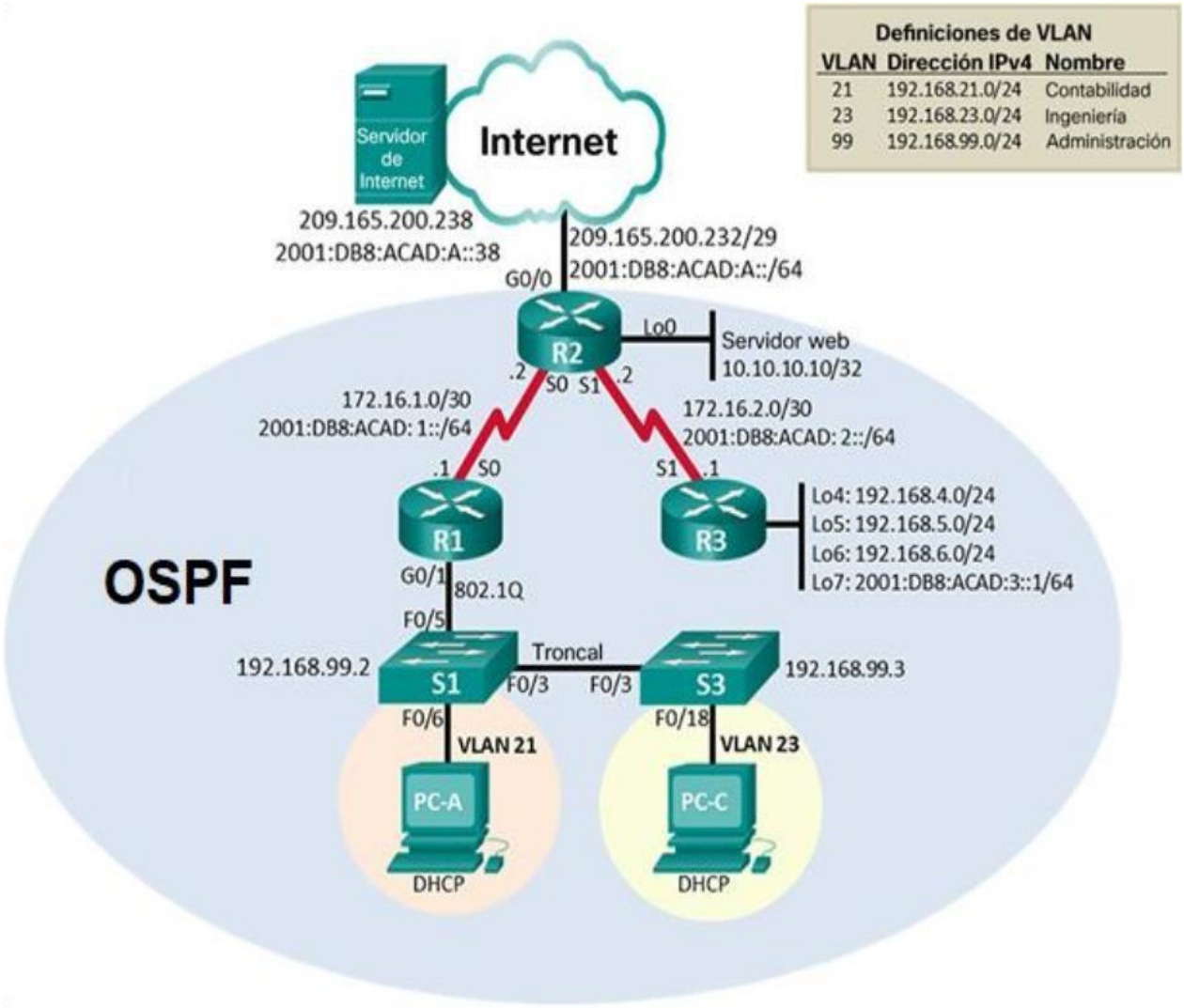


Fuente: propia.

3.2 Escenario No. 2

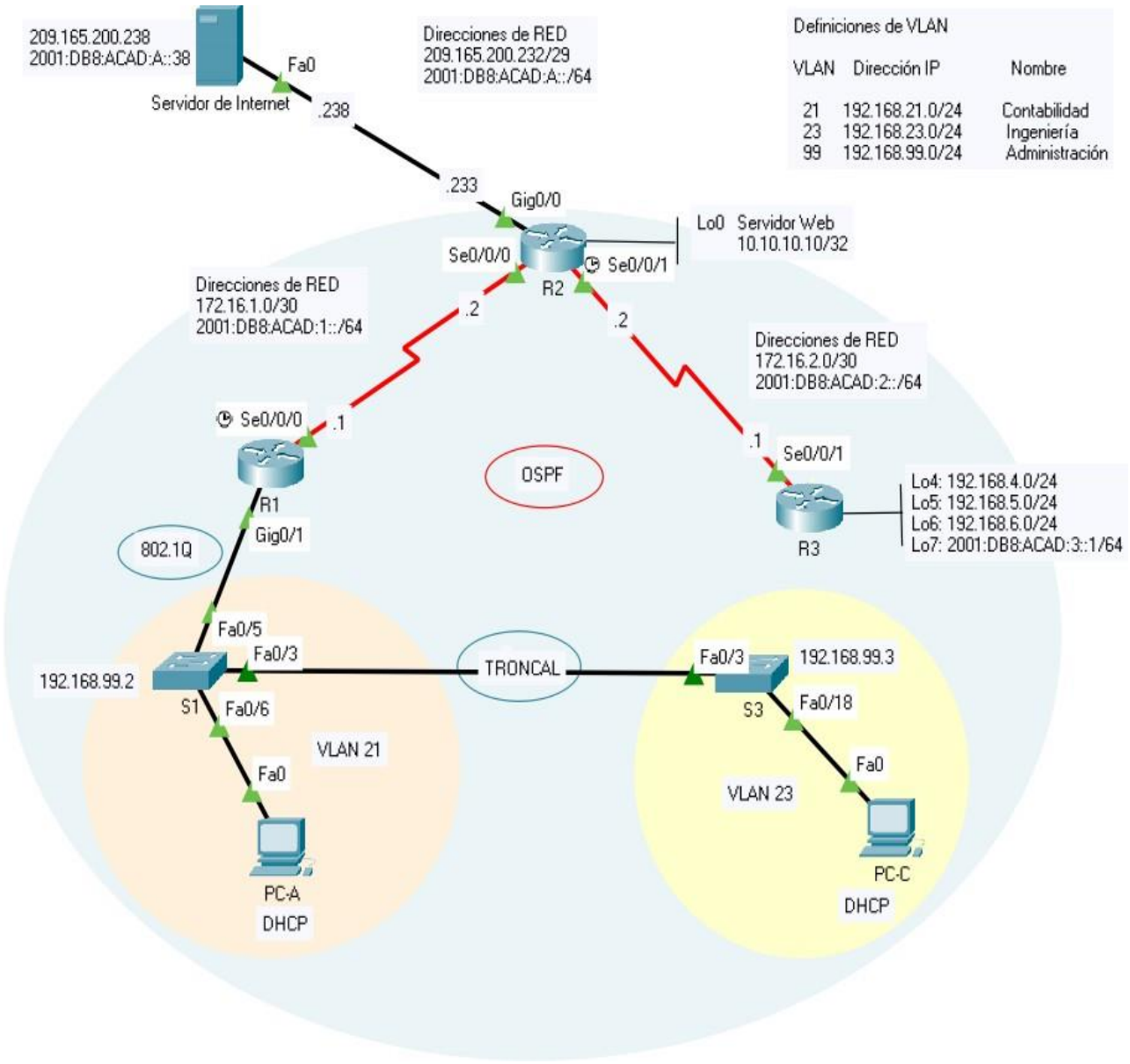
Topología

Figura No. 37. Topología escenario No. 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.

Figura No. 38. Topología en ambiente simulado escenario No. 2



Fuente: propia.

3.2.1 Parte 1: Inicializar dispositivos

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

Tabla No. 12. Inicialización y carga de routers y switches

Tarea	Comando de IOS
Eliminar el archivo **startup-config** de todos los routers	Configuración Routers **R1, R2 y R3** Router> Router>**enable** Router# **erase startup-config** Continue? [confirm] [**Enter**] [OK] Erase of nvram: complete Router#
Volver a cargar todos los routers	Configuración Routers **R1, R2 y R3** Router# **reload** Proceed with reload? [confirm] [**Enter**] Router>
Eliminar el archivo **startup-config** de todos los switches y eliminar la base de datos de VLAN anterior	Configuración Switches **S1 y S2** Switch# Switch#**erase startup-config** Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [Enter] [OK] Erase of nvram: complete Switch#
Volver a cargar ambos switches	Configuración Switches **S1 y S2** Switch# Switch# **reload** Proceed with reload? [confirm] [**Enter**] Switch>
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch# Switch#**show vlan brief** Switch#

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

En el requerimiento de la verificación de la base de datos de VLAN, se tiene la siguiente consideración:

Al aplicar el comando **delete flash:vlan.dat** aparece el siguiente mensaje: %Error deleting flash:/vlan.dat (No such file or directory) debido a que en el escenario simulado los routers y los switches no tienen archivos VLAN creados por ser dispositivos inicializados sin ningún tipo de configuración.

3.2.2 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 No. 13. Configurar la computadora 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 **"209.165.200.233"**	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6 **"2001:DB8:ACAD:A::1"**	2001:BD8:ACAD:A::1

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

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

Paso 2: Configurar R1.

Las tareas de configuración para **R1** incluyen las siguientes:

Tabla No. 14. Configuración **R1**.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>**enable** Router#**configure terminal** Router(config)#**no ip domain-lookup** Router(config)#
Nombre del router **"R1"**	Router>**enable** Router# **configure terminal** Router(config)#**hostname R1**

	R1(config)#
Contraseña de exec privilegiado cifrada **“class”**	R1>**enable** R1# **configure terminal** R1(config)# **enable secret class** R1(config)#**exit**
Contraseña de acceso a la consola **“cisco”**	R1>**enable** R1# **configure terminal** R1(config)# **line console 0** R1(config-line)# **password cisco** R1(config-line)# **login** R1(config-line)# **exit** R1(config)#**exit**
Contraseña de acceso Telnet **“cisco”**	R1#**configure terminal** R1(config)#**line vty 0 4** R1(config-line)#**password cisco** R1(config-line)# **login** R1(config-line)#**exit** R1(config)#
Cifrar las contraseñas de texto no cifrado	R1(config)#**service password-encryption** R1(config)#**exit**
Mensaje MOTD “Se prohíbe el acceso no autorizado.”	R1#**configure terminal** R1(config)# **banner motd # *** Se prohíbe el acceso no autorizado *** #** R1(config)# **exit** R1(config)#
Interfaz S0/0/0 • Establezca la descripción • Establecer la dirección **IPv4** (Consultar el diagrama de topología para conocer la información de direcciones) • Establecer la dirección **IPv6** (Consultar el diagrama de topología para conocer la información de direcciones) • Establecer **la frecuencia de reloj en 128000** • Activar la interfaz	R1#**config t** R1(config)#**interface serial 0/0/0** R1(config)#**description Conexion a R2** R1(config)#**ip address 172.16.1.1 255.255.255.252** R1(config)#**ipv6 address 2001:DB8:ACAD:1::1/64** R1(config)#**clock rate 128000** R1(config)#**no shutdown** R1(config)#**exit**
Rutas predeterminadas • Configurar una ruta **IPv4** predeterminada de S0/0/0	R1#**config t** R1(config)#**ip route 0.0.0.0 0.0.0.0 172.16.1.2** R1(config)#**ipv6 route ::/0 2001:DB8:ACAD:1::2** R1(config)#**exit**

• Configurar una ruta **IPv6** predeterminada de S0/0/0	

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2.

La configuración del **R2** incluye las siguientes tareas:

Tabla No. 15. Configuración **R2**.

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router>**enable** Router#**configure terminal** Router(config)#**no ip domain-lookup** Router(config)#
Nombre del router **"R2"**	Router>**enable** Router# **configure terminal** Router(config)#**hostname R2** R2(config)#**exit**
Contraseña de exec privilegiado cifrada **"class"**	R2>**enable** R2# **configure terminal** R2(config)# **enable secret class** R2(config)#**exit**
Contraseña de acceso a la consola **"cisco"**	R2>**enable** R2# **configure terminal** R2(config)# **line console 0** R2(config-line)# **password cisco** R2(config-line)# **login** R2(config-line)# **exit** R2(config)#
Contraseña de acceso Telnet **"cisco"**	R2#**configure terminal** R2(config)#**line vty 0 4** R2(config-line)#**password cisco** R2(config-line)# **login** R2(config-line)#**exit** R2(config)#
Cifrar las contraseñas de texto no cifrado	R1(config)#**service password-encryption** R1(config)#**exit**

Habilitar el **servidor HTTP**	**No aplica** (El escenario simulado en Packet Tracer no permite la inserción del protocolo HTTP). R2(config)# R2(config)#**ip http server** **^** **% Invalid input detected at '^' marker.** R2(config)#**exit** R2#
Mensaje MOTD **"Se prohíbe el acceso no autorizado."**	R2# configure terminal R2(config)# banner motd # *** Se prohibe el acceso no autorizado *** # R2(config)# exit
Interfaz S0/0/0 • Establezca la descripción • Establecer la dirección **IPv4** (Utilizar la siguiente dirección disponible en la subred) • Establecer la dirección **IPv6** (Consultar el diagrama de topología para conocer la información de direcciones) • Activar la interfaz	R2#**config t** R2(config)# **interface serial 0/0/0** R2(config)# **description Conexion a R1** R2(config)# **ip address 172.16.1.2 255.255.255.252** R2(config)# **ipv6 address 2001:DB8:ACAD:1::2/64** R2(config)# **no shutdown** R2(config)# **exit** R2#
Interfaz S0/0/1 • Establezca la descripción • Establecer la dirección **IPv4** (Utilizar la primera dirección disponible en la subred) • Establecer la dirección **IPv6** (Consultar el diagrama de topología para conocer la información de direcciones). • Establecer la **frecuencia de reloj en 128000** • Activar la interfaz	R2#**config t** R2(config)# **interface serial 0/0/1** R2(config)# **description Conexion a R3** R2(config)# **ip address 172.16.2.2 255.255.255.252** R2(config)# **ipv6 address 2001:DB8:ACAD:2::2/64** R2(config)# **clock rate 128000** R2(config)# **no shutdown** R2(config)# **exit** R2#

Interfaz G0/0 (simulación de Internet) • Establezca la descripción • Establecer la dirección **IPv4** (Utilizar la primera dirección disponible en la subred) • Establecer la dirección **IPv6** (Utilizar la primera dirección disponible en la subred) • Activar la interfaz	R2#**config t** R2(config)# **interface gigabitEthernet 0/0** R2(config)# **description Conexion Servidor** R2(config)# **ip address 209.165.200.233 255.255.255.248** R2(config)# **ipv6 address 2001:DB8:ACAD:A::1/64** R2(config)# **no shutdown** R2(config)# **exit** R2#
Interfaz loopback 0 (servidor web simulado) • Establezca la descripción. • Establecer la dirección **IPv4**	R2#**config t** R2(config)# **interface loopback 0** R2(config)# **description Conexion Servidor Web simulado** R2(config)# **ip address 10.10.10.10 255.255.255.255** R2(config)# **exit** R2#
Ruta predeterminada • Configure la ruta **IPv4** predeterminada de G0/0. • Configure la ruta **IPv6** predeterminada de G0/0.	R2#**config t** R2(config)# **ip route 0.0.0.0 0.0.0.0 172.16.1.1** R2(config)# **ipv6 route ::/0 2001:DB8:ACAD:1::1** R2(config)# **ip route 0.0.0.0 0.0.0.0 172.16.2.1** R2(config)# **ipv6 route ::/0 2001:DB8:ACAD:2::1** R2(config)# **ip route 0.0.0.0 0.0.0.0 209.165.200.238** R2(config)# **ipv6 route ::/0 2001:BD8:ACAD:A::38** R2(config)# **exit** R2#

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 4: Configurar R3.

La configuración del **R3** incluye las siguientes tareas:

Tabla No. 16. Configuración **R3**.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>**enable** Router#**configure terminal** Router(config)#**no ip domain-lookup** Router(config)#
Nombre del router **“R3”**	Router>**enable** Router# **configure terminal** Router(config)#**hostname R3** R3(config)#**exit**
Contraseña de exec privilegiado cifrada **“class”**	R3>**enable** R3# **configure terminal** R3(config)# **enable secret class** R3(config)#**exit**
Contraseña de acceso a la consola **“cisco”**	R3>**enable** R3# **configure terminal** R3(config)# **line console 0** R3(config-line)# **password cisco** R3(config-line)# **login** R3(config-line)# **exit** R3(config)#
Contraseña de acceso Telnet **“cisco”**	R3#**configure terminal** R3(config)#**line vty 0 4** R3(config-line)#**password cisco** R3(config-line)# **login** R3(config-line)#**exit** R3(config)#
Cifrar las contraseñas de texto no cifrado	R3(config)#**service password-encryption** R3(config)#**exit**
Mensaje MOTD **“Se prohíbe el acceso no autorizado.”**	R3# configure terminal R3(config)# banner motd # *** Se prohibe el acceso no autorizado *** # R3(config)# exit R3#
Interfaz S0/0/1 • Establezca la descripción • Establecer la dirección **IPv4** (Utilizar la siguiente dirección disponible en la subred) • Establecer la dirección **IPv6** (Consultar el diagrama de	R3#**config t** R3(config)# **interface serial 0/0/1** R3(config)# **description Conexion a R2** R3(config)# **ip address 172.16.2.1 255.255.255.252** R3(config)# **ipv6 address 2001:DB8:ACAD:2::1/64** R3(config)# **no shutdown**

topología para conocer la información de direcciones) • Activar la interfaz	R3(config)# **exit** R3#
Interfaz loopback 4 • Establecer la dirección **IPv4** (Utilizar la primera dirección disponible en la subred)	R3#**config t** R3(config)#**interface loopback 4** R3(config)#**description Interfaz virtual (para pruebas, en este caso el 4)** R3(config)# **ip address 192.168.4.1 255.255.255.0** R3(config)# **exit** R3#
Interfaz loopback 5 • Establecer la dirección **IPv4** (Utilizar la primera dirección disponible en la subred)	R3#**config t** R3(config)# **interface loopback 5** R3(config)# **description Interfaz virtual (para pruebas, en este caso el 5)** R3(config)# **ip address 192.168.5.1 255.255.255.0** R3(config)#**exit** R3#
Interfaz loopback 6 • Establecer la dirección **IPv4** (Utilizar la primera dirección disponible en la subred)	R3#**config t** R3(config)#**interface loopback 6** R3(config)#**description Interfaz virtual (para pruebas, en este caso el 6)** R3(config)#**ip address 192.168.6.1 255.255.255.0** R3(config)#**exit** R3#
Interfaz loopback 7 • Establecer la dirección **IPv6** (Consultar el diagrama de topología para conocer la información de direcciones)	R3#**config t** R3(config)#**interface loopback 7** R3(config)#**description Interfaz virtual (para pruebas, en este caso el 7)** R3(config)#**ip address 2001:db8:acad:3::1/64** R3(config)#**exit** R3#
Rutas predeterminadas	R3#**config t** R3(config)#**ip route 0.0.0.0 0.0.0.0 172.16.2.2** R3(config)#**ipv6 route ::/0 2001:DB8:ACAD:2::2** R3(config)#**exit** R3#

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 5: Configurar S1.

La configuración del **S1** incluye las siguientes tareas:

Tabla No. 17. Configuración **S1.**

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>**enable** Switch#**configure terminal** Switch(config)#**no ip domain-lookup** Switch(config)#**exit** Switch#
Nombre del switch **"S1"**	switch# **configure terminal** switch(config)#**hostname S1** S1(config)#**exit** S1#
Contraseña de exec privilegiado cifrada **"class"**	S1#**configure terminal** S1(config)# **enable secret class** S1(config)#**exit** S1#
Contraseña de acceso a la consola **"cisco"**	S1#**configure terminal** S1(config)# **line console 0** S1(config-line)# **password cisco** S1(config-line)# **login** S1(config-line)# **exit** S1(config)#**exit** S1#
Contraseña de acceso Telnet **"cisco"**	S1#**configure terminal** S1(config)#**line vty 0 4** S1(config-line)#**password cisco** S1(config-line)# **login** S1(config-line)#**exit** S1(config)#**exit** S1#
Cifrar las contraseñas de texto no cifrado	S1(config)#**service password-encryption** S1(config)#**exit** S1#
Mensaje MOTD **"Se prohíbe el acceso no**	S1#**configure terminal** S1(config)#**banner motd # *** Se prohibe el acceso no autorizado *** #**

autorizado.”	S1(config)#**exit** S1#

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 6: Configurar S3.

La configuración del **S3** incluye las siguientes tareas:

Tabla No. 18. Configuración **S3.**

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>**enable** Switch#**configure terminal** Switch(config)#**no ip domain-lookup** Switch(config)#**exit** Switch#
Nombre del switch **“S3”**	switch# **configure terminal** switch(config)#**hostname S3** S3(config)#**exit** S3#
Contraseña de exec privilegiado cifrada **“class”**	S3# **configure terminal** S3(config)# **enable secret class** S3(config)#**exit** S3#
Contraseña de acceso a la consola **“cisco”**	S3#**configure terminal** S3(config)# **line console 0** S3(config-line)# **password cisco** S3(config-line)# **login** S3(config-line)# **exit** S3(config)#**exit** S3#
Contraseña de acceso Telnet **“cisco”**	S3#**configure terminal** S3(config)#**line vty 0 4** S3(config-line)#**password cisco** S3(config-line)# **login** S3(config-line)#**exit** S3(config)#**exit** S3#
Cifrar las contraseñas de texto no cifrado	S3(config)#**service password-encryption** S3(config)#**exit** S3#
Mensaje MOTD	S3#**configure terminal**

“Se prohíbe el acceso no autorizado.”	S3(config)#**banner motd # *** Se prohibe el acceso no autorizado *** #** S3(config)#**exit** S3#

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

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:

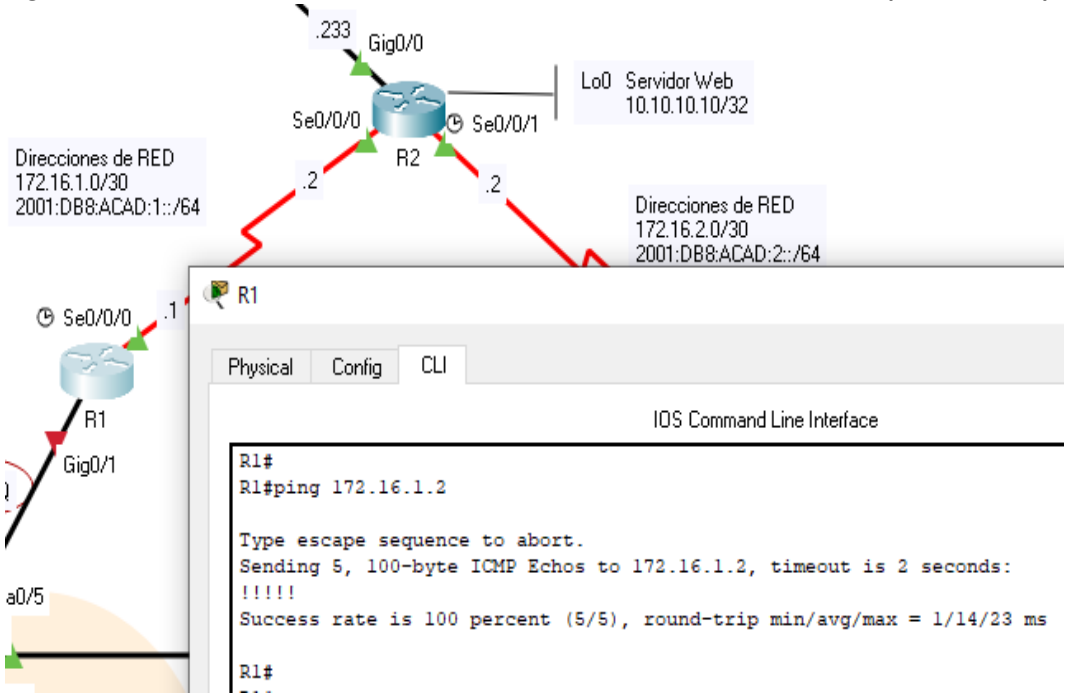
Tabla No. 19. Verificación de conectividad para Router y PC.

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

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

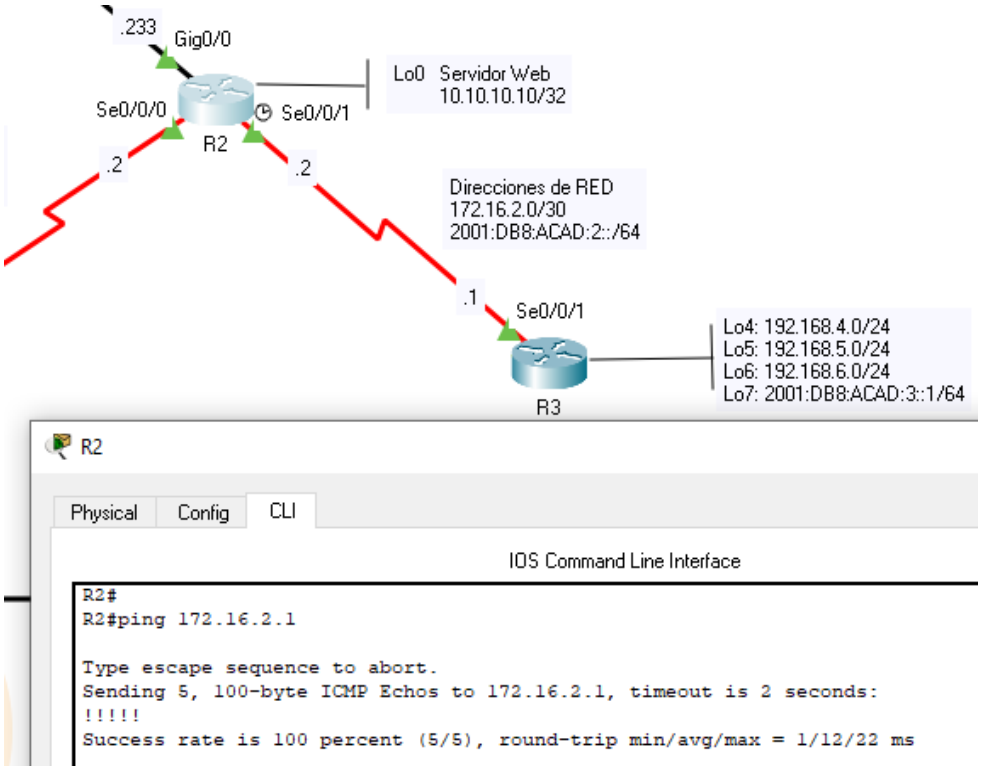
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

*Figura No. 39. Prueba de conectividad desde **R1** a **R2,** S0/0/0 (172.16.1.2)*



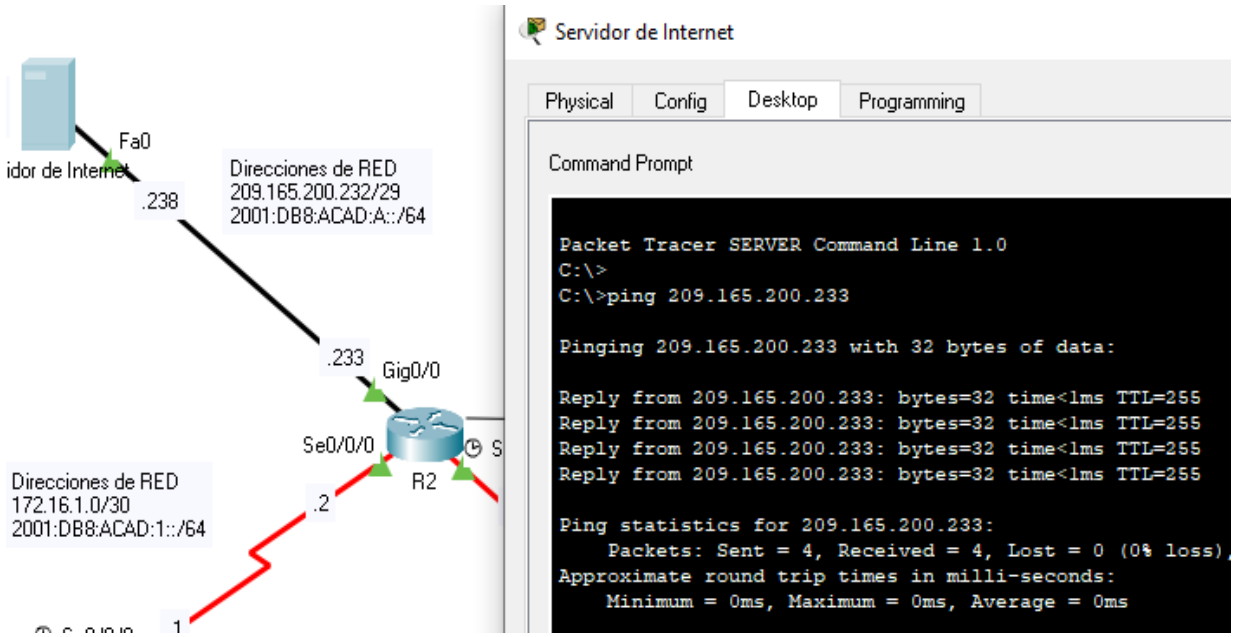
Fuente: propia.

*Figura No. 40. Prueba de conectividad desde **R2** a **R3,** S0/0/1 (172.16.2.1)*



Fuente: propia.

*Figura No. 41. Prueba de conectividad desde **R2** a **R3,** S0/0/1 (172.16.2.1)*



Fuente: propia.

3.2.3 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 No. 20. Configuración Switch **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#**config t** S1(config)#**vlan 21** S1(config)#**name Contabilidad** S1(config)#**vlan 23** S1(config)#**name Ingenieria** S1(config)#**vlan 99** S1(config)#**name Administracion** S1(config)#**exit** S1#
Asignar la dirección IP de administración.	S1#**config t** S1(config)#**interface Vlan 99** S1(config)#**ip address 192.168.99.2**

• Asigne la dirección IPv4 a la VLAN de administración. • Utilizar la dirección IP asignada al **S1** en el diagrama de topología	**255.255.255.0** S1(config)#**exit** S1#
Asignar el Gateway predeterminado • Asigne la primera dirección IPv4 de la subred como el Gateway predeterminado.	S1#**config t** S1(config)#**ip default-gateway 192.168.99.1** S1(config)#**exit** S1#
Forzar el enlace troncal en la interfaz **F0/3** • Utilizar la red VLAN 1 como VLAN nativa	S1#**config t** S1(config)#**interface fastEthernet 0/3** S1(config)#**switchport mode trunk** S1(config)#**switchport trunk native vlan 1** S1(config)#**exit** S1#
Forzar el enlace troncal en la interfaz **F0/5** • Utilizar la red VLAN 1 como VLAN nativa	S1#**config t** S1(config)#**interface fastEthernet 0/5** S1(config)#**switchport mode trunk** S1(config)#**switchport trunk native vlan 1** S1(config)#**exit** S1#
Configurar el resto de los puertos como puertos de acceso • Utilizar el comando interface range	S1#**config t** S1(config)#**interface range fastEthernet 0/1-2, f0/4, f0/6-24, g0/1-2** S1(config)#**switchport mode access** S1(config)#**exit** S1#
Asignar F0/6 a la VLAN 21	S1#**config t** S1(config)#**interface fastEthernet 0/6** S1(config)#**switchport access vlan 21** S1(config)#**exit** S1#
Apagar todos los puertos sin usar	S1#**config t** S1(config)#**interface range fastEthernet 0/1-2, f0/4, f0/7-24, g0/1-2** S1(config)#**shutdown** S1(config)#**exit** S1#

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 2: Configurar S3.

La configuración del **S3** incluye las siguientes tareas:

Tabla No. 21. Configuración Switch **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 y nombrar cada una de las VLAN que se indican	S3#**config t** S3(config)#**vlan 21** S3(config)#**name Contabilidad** S3(config)#**vlan 23** S3(config)#**name Ingenieria** S3(config)#**vlan 99** S3(config)#**name Administracion** S3(config)#**exit** S3#
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 t** S3(config)#**interface Vlan 99** S3(config)#**ip address 192.168.99.3 255.255.255.0** S3(config)#**exit** S3#
Asignar el Gateway predeterminado • Asigne la primera dirección IPv4 de la subred como el Gateway predeterminado.	S3#**config t** S3(config)#**ip default-gateway 192.168.99.1** S3(config)#**exit** S3#
Forzar el enlace troncal en la interfaz **F0/3** • Utilizar la red VLAN 1 como VLAN nativa	S3#**config t** S3(config)#**interface fastEthernet 0/3** S3(config)#**switchport mode trunk** S3(config)#**switchport trunk native vlan 1** S3(config)#**exit** S3#
Configurar el resto de los puertos como puertos de	S3#**config t** S3(config)#**interface range fastEthernet 0/1-**

acceso • Utilizar el comando interface range	**2, f0/4-24, g0/1-2** S3(config)#**switchport mode access** S3(config)#**exit** S3#
Asignar F0/18 a la VLAN 23	S3#**config t** S3(config)#**interface fastEthernet 0/18** S3(config)#**switchport access vlan 23** S3(config)#**exit** S3#
Apagar todos los puertos sin usar	S3#**config t** S3(config)#**interface range fastEthernet 0/1-2, f0/4-17, f0/19-24, g0/1-2** S3(config)#**shutdown** S3(config)#**exit**

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas.

Paso 3: Configurar R1.

Las tareas de configuración para R1 incluyen las siguientes:

Tabla No. 22. Configuración Router **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 t** R1(config)#**interface gigabitEthernet 0/1.21** R1(config)#**encapsulation dot1Q 21** R1(config)#**ip address 192.168.21.1 255.255.255.0** R1(config)#**description LAN de contabilidad VLAN 21** R1(config)#**no shutdown** R1(config)#**exit** R1#
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 t** R1(config)#**interface gigabitEthernet 0/1.23** R1(config)#**encapsulation dot1Q 23** R1(config)#**ip address 192.168.23.1 255.255.255.0** R1(config)#**description LAN de Ingenierai VLAN 23** R1(config)#**no shutdown**

	R1(config)#**exit** R1#
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 t** R1(config)#**interface gigabitEthernet 0/1.99** **encapsulation dot1Q 99** R1(config)#**ip address 192.168.99.1** **255.255.255.0** R1(config)#**description LAN de** **Administracion VLAN 99** R1(config)#**no shutdown** R1(config)#**exit** R1#
Activar la interfaz G0/1	R1#**config t** R1(config)#**interface gigabitEthernet 0/1** R1(config)#**no shutdown** R1(config)#**exit** R1#

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 4: Verificar la conectividad de la red.

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

✓ Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.

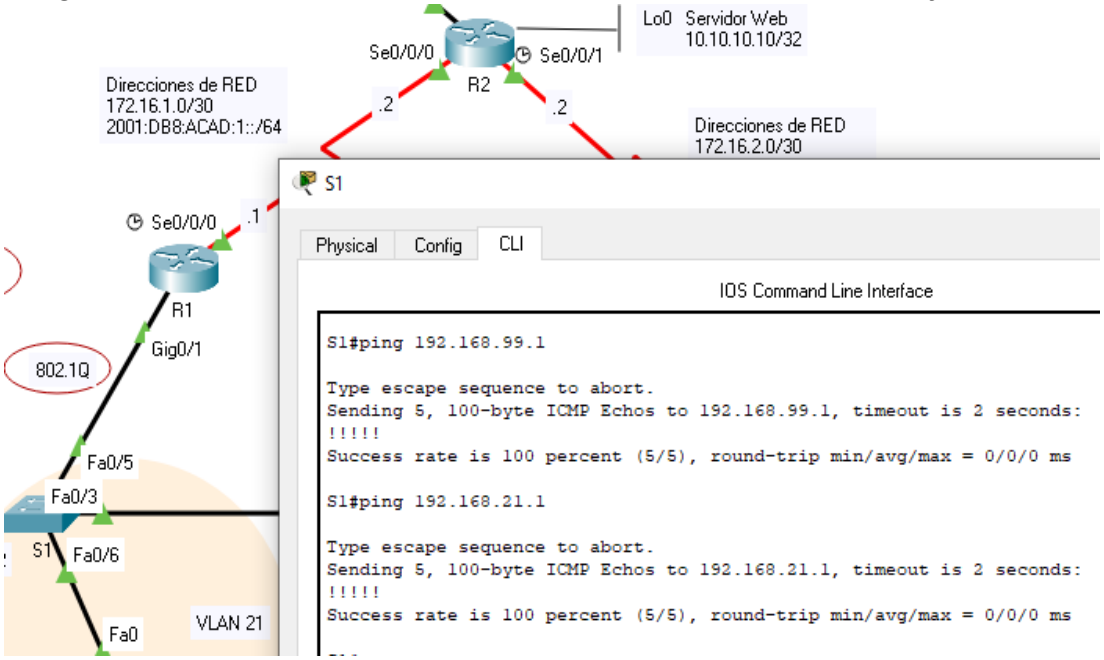
✓ Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla No. 23. Verificación de conectividad para switches y Router R1.

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

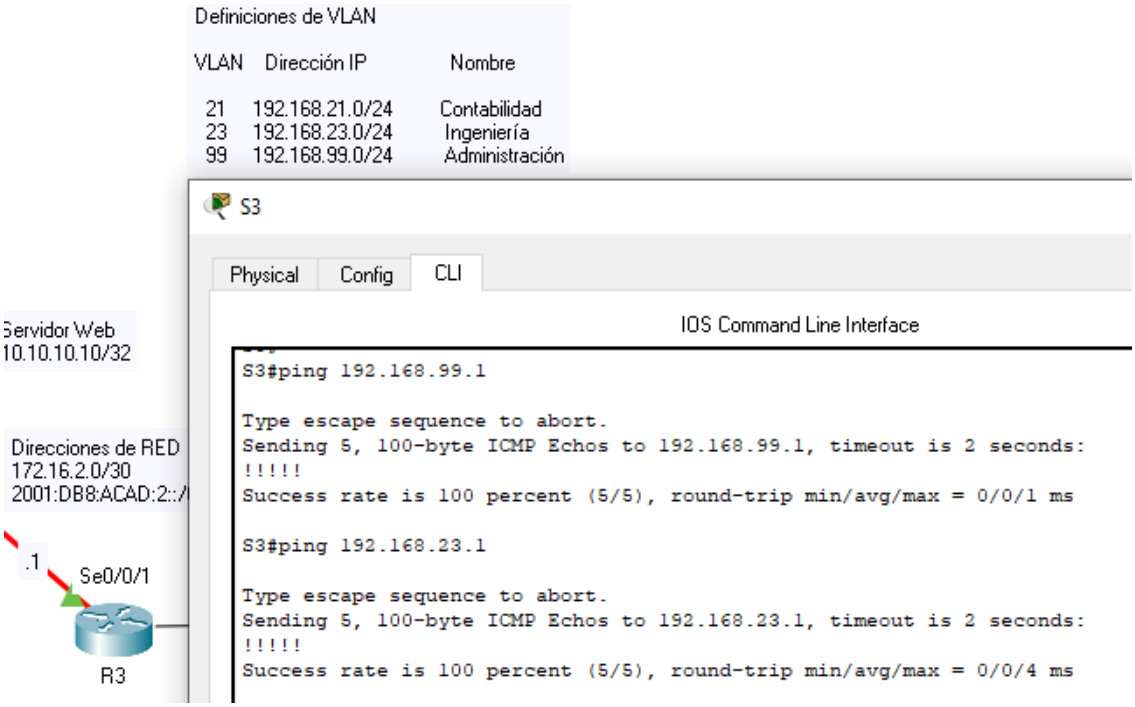
Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

*Figura No. 42. Prueba de conectividad desde **S1** a **R1,** Vlan 99 y Vlan 21.*



Fuente: propia.

*Figura No. 43. Prueba de conectividad desde **S3** a **R1,** Vlan 23 y Vlan 99.*



Fuente: propia.

Paso 5: Habilitar el envío de tráfico IPv6 en R1, R2 y R3.

Por defecto, IPv6 está desactivado en un dispositivo Cisco.

Tabla No. 24. Habilitación tráfico IPv6 en R1, R2 y R3**.**

Elemento o tarea de configuración	Especificación
Habilitar el routing de unidifusión IPv6 en R1, R2 y R3. (El comando de configuración global **ipv6 unicast-routing** debe configurarse para que habilite al router el reenvío de paquetes IPv6) (Permite enrutar paquetes IPv6 entre las distintas interfaces del router)	R1#**config t** R1(config)#**ipv6 unicast-routing** R1(config)#**exit** R1# R2#**config t** R2(config)#**ipv6 unicast-routing** R2(config)#**exit** R2# R3#**config t** R3(config)#**ipv6 unicast-routing** R3(config)#**exit** R1#

Fuente: Propia.

3.2.4 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 No. 25. Configuración protocolo de enrutamiento OSPF en el **R1.**

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

	area 0
Establecer todas las interfaces LAN como pasivas	R1(config)#**passive-interface gigabitEthernet 0/1.21** R1(config)#**passive-interface gigabitEthernet 0/1.23** R1(config)#**passive-interface gigabitEthernet 0/1.99** R1(config)#**exit** R1#
Desactive la sumarización automática	**No aplica** (El escenario simulado en Packet Tracer no permite la inserción del comando no auto-summary). R1#**config t** R1(config)#**router ospf 1** R1(config-router)#**no auto-summary** **^** **% Invalid input detected at '^' marker.** R1(config-router)#**exit** R1#

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 2: Configurar OSPF en el R2.

La configuración del R2 incluye las siguientes tareas:

Tabla No. 26. Configuración protocolo de enrutamiento OSPF en el **R2.**

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2#**config t** R2(config)#**router ospf 1** R2(config)#**router-id 2.2.2.2**
Anunciar las redes conectadas directamente • **Nota:** Omitir la red G0/0.	R2(config)#**network 10.10.10.10 0.0.0.0 area 0** R2(config)#**network 172.16.1.0 0.0.0.3 area 0** R2(config)#**network 172.16.2.0 0.0.0.3 area 0**
Establecer la interfaz LAN (loopback) como pasiva	R2(config)#**passive-interface loopback 0** R2(config)#**exit** R2#
Desactive la sumarización automática	**No aplica** (El escenario simulado en Packet Tracer no permite la inserción del comando no auto-

	summary). R2#**config t** R2(config)#**router ospf 1** R2(config-router)#**no auto-summary** **^** **% Invalid input detected at '^' marker.** R2(config-router)#**exit** R2#

Fuente: Guía Prueba de habilidades prácticas CCNA.

Paso 3: Configurar OSPFv3 en el R2.

Tabla No. 27. Configuración protocolo de enrutamiento OSPFv3 en el **R2.**

Elemento o tarea de configuración	Especificación
Configurar OSPFv3 área 0	R2#**config t** R2(config)#**ipv6 router ospf 1** R2(config-rtr)#**router-id 4.4.4.4** R2(config-rtr)#**exit** R2(config)#**interface gigabitEthernet 0/0** R2(config-if)#**ipv6 ospf 1 area 0** R2(config-if)#**exit** R2(config)#**interface serial 0/0/0** R2(config-if)#**ipv6 ospf 1 area 0** R2(config-if)#**exit** R2(config)#**interface serial 0/0/1** R2(config-if)#**ipv6 ospf 1 area 0** R2(config-if)#**exit** R2(config)#**exit** R2#

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

La configuración del R3 incluye las siguientes tareas:

Tabla No. 28. Configuración protocolo de enrutamiento en el **R3.**

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3#**config t** R3(config)#**router ospf 1**

	R3(config)#**router-id 3.3.3.3** R3(config)#
Anunciar las redes IPv4 conectadas directamente	R3(config)#**network 172.16.2.0 0.0.0.3 area 0** R3(config)#**network 192.168.4.0 0.0.0.255 area 0** R3(config)#**network 192.168.5.0 0.0.0.255 area 0** R3(config)#**network 192.168.6.0 0.0.0.255 area 0**
Establecer todas las interfaces de LAN IPv4 (loopback) como pasivas	R3(config)#**passive-interface loopback 4** R3(config)#**passive-interface loopback 5** R3(config)#**passive-interface loopback 6** R3(config)#**passive-interface loopback 7** R3(config)#**exit** R3#
Desactive la sumarización automática	**No aplica** (El escenario simulado en Packet Tracer no permite la inserción del comando no auto-summary). R3#**config t** R3(config)#**router ospf 1** R3(config-router)#**no auto-summary** **^** **% Invalid input detected at '^' marker.** R3(config-router)#**exit** R3#

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

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:

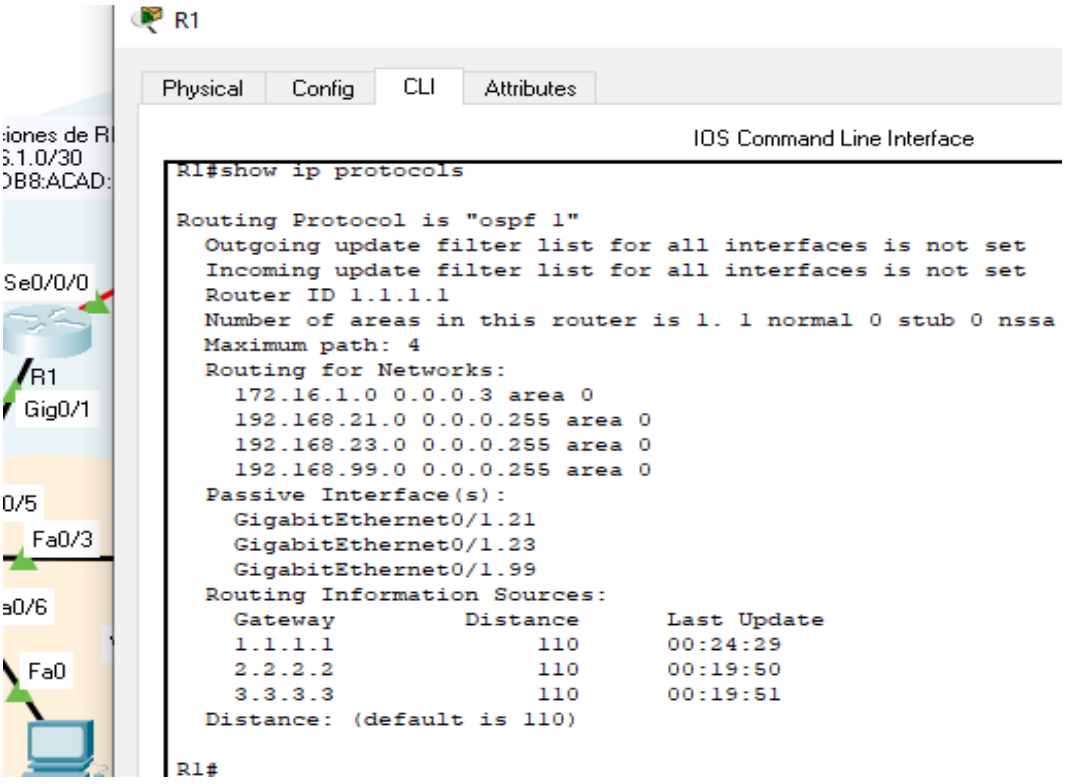
Tabla No. 29. Verificación información OSPF.

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso	Desde el modo de usuario y en R1, R2 y R3 se aplica el siguiente comando:

OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	R1#**show ip protocols**
¿Qué comando muestra solo las rutas OSPF?	Desde el modo de usuario y en R1, R2 y R3 se aplica el siguiente comando: R2#**show ip route ospf**
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Desde el modo de usuario y en R1, R2 y R3 se aplica el siguiente comando: R3#**show running-config | section router ospf**

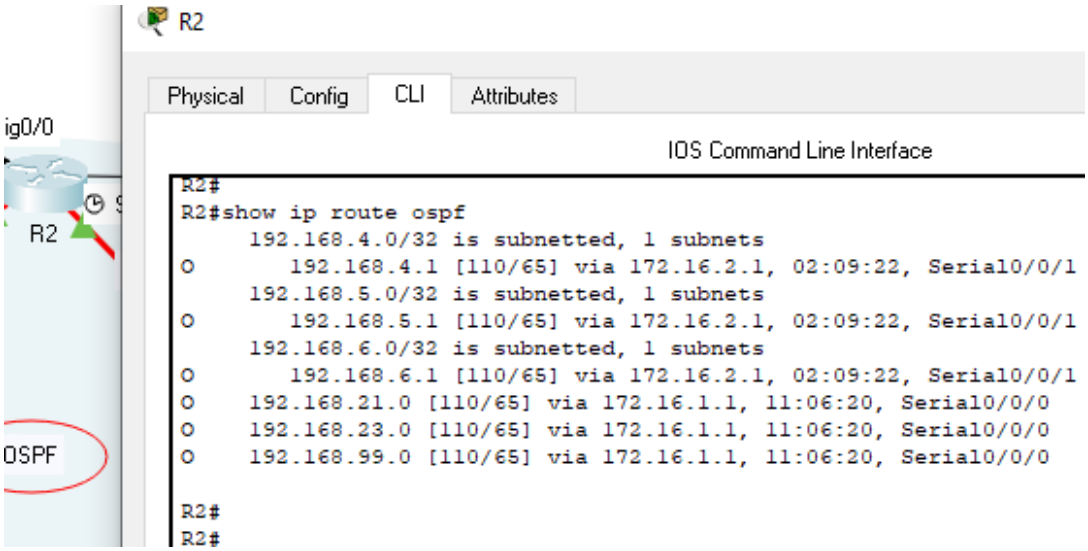
Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

*Figura No. 44. Comando Show Ip Protocols desde **R1.***



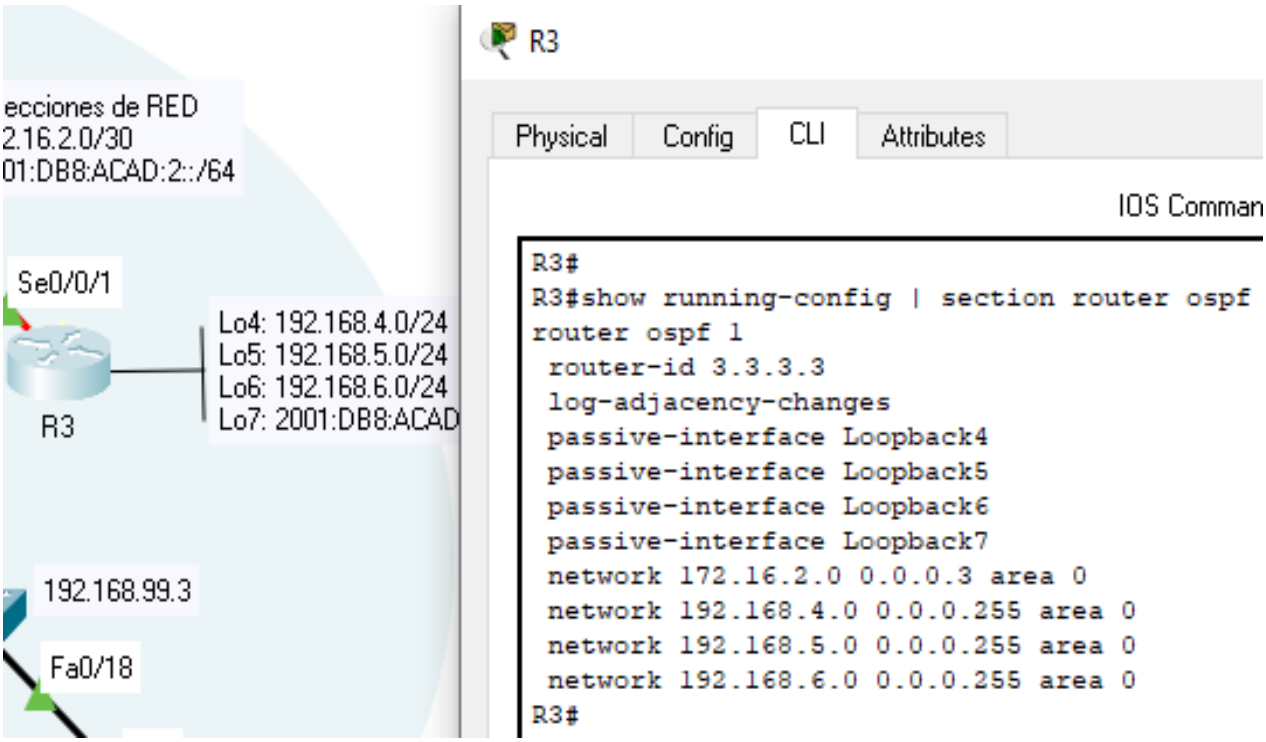
Fuente: propia.

*Figura No. 45. Comando Show Ip route Ospf desde **R2.***



Fuente: propia.

*Figura No. 46. Comando show running-config | section router ospf desde **R3.***



Fuente: propia.

3.2.5 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 No. 30. Configuración e implementación DHCP y NAT para IPv4.

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

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

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

La configuración del R2 incluye las siguientes tareas:

Tabla No. 31. Configuración de 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 t** R2(config)#**username webuser privilege 15** R2(config)#**password cisco12345** R2(config)#**exit** R2#
Habilitar el servicio del servidor HTTP	**No aplica** (El escenario simulado en Packet Tracer no permite la inserción del protocolo HTTP). R2(config)# R2(config)#**ip http server** ^ **% Invalid input detected at '^' marker.** R2(config)#**exit** R2#
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	**No aplica** (El escenario simulado en Packet Tracer no permite la inserción del protocolo HTTP). R2(config)# R2(config)#**ip http authentication local** ^ **% Invalid input detected at '^' marker.** R2(config)#**exit** R2#
Crear una NAT estática al servidor web. • Dirección global interna: 209.165.200.229	R2#**config t** R2(config)#**ip nat inside source static 10.10.10.10 209.165.200.229** R2(config)#**exit** R2#

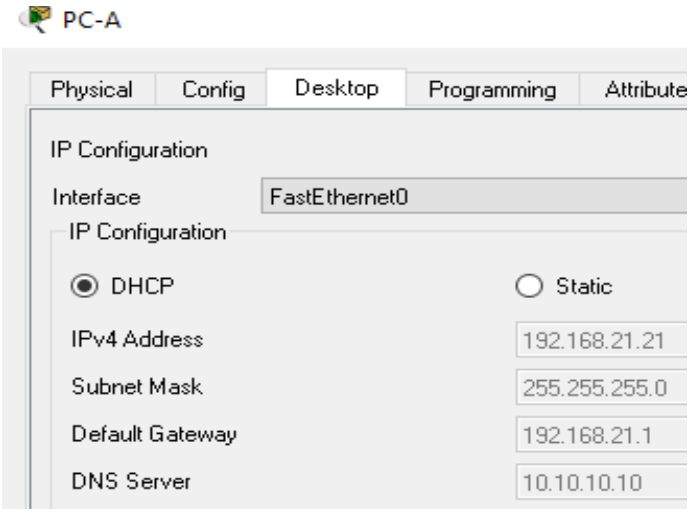
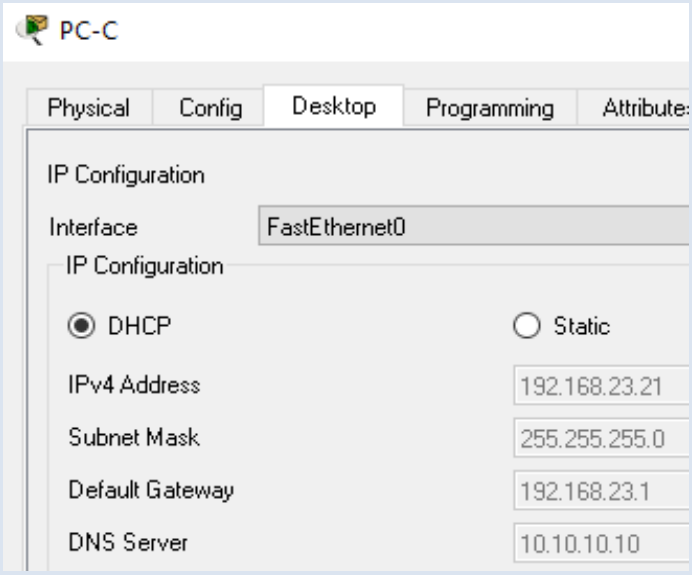
Asignar la interfaz interna y externa para la NAT estática	R2#**config t** R2(config)#**interface gigabitEthernet 0/0** R2(config)#**ip nat outside** R2(config)#**exit** R2(config)#**interface loopback 0** R2(config)#**ip nat inside** R2(config)#**exit** R2#
Configurar la NAT dinámica dentro de una ACL 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 t** 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 0.0.0.255** R2(config)#**access-list 1 permit 192.168.5.0 0.0.0.255** R2(config)#**access-list 1 permit 192.168.6.0 0.0.0.255** R2(config)#**exit** R2#
Defina el pool de direcciones IP públicas utilizables. • Nombre del conjunto: INTERNET • El conjun to de direcciones incluye: 209.165.200.225 – 209.165.200.228	R2#**config t** R2(config)#**ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248** R2(config)#**exit** R2#
Definir la traducción de NAT dinámica	R2#**config t** R2(config)#**ip nat inside source list 1 pool INTERNET** R2(config)#**exit** R2#

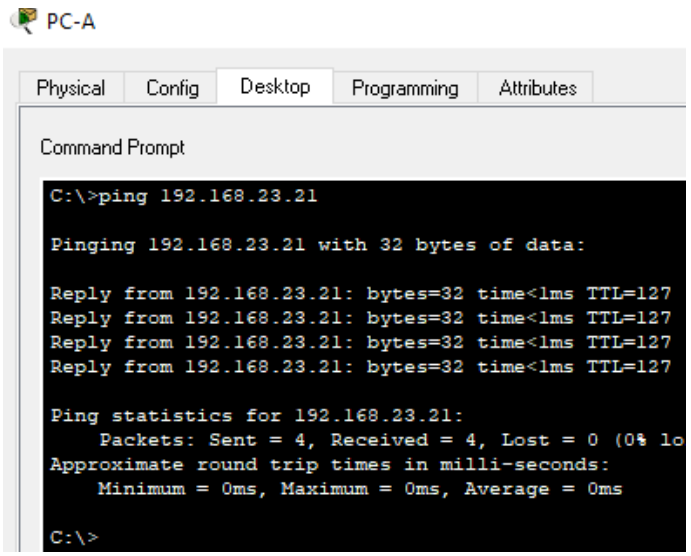
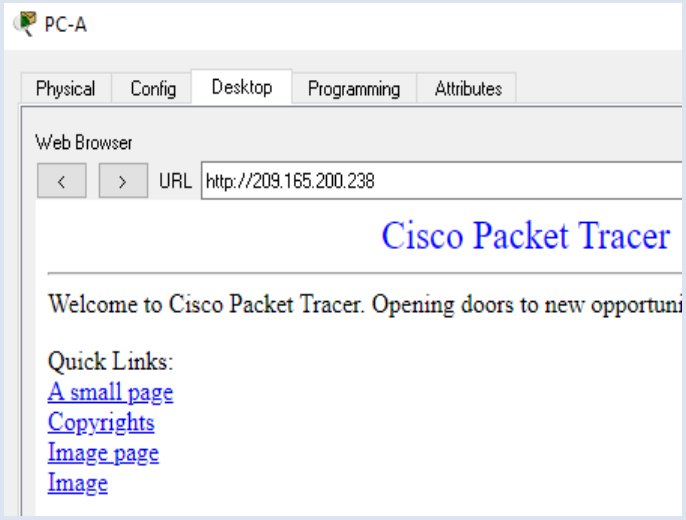
Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

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 No. 32. Verificación de protocolo DHCP y NAT estática.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	*Figura No. 47. Verificación de asignación IP por DHCP en PC-A.*  *Fuente: propia.*
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	*Figura No. 48. Verificación de asignación IP por DHCP en PC-C.*  *Fuente: propia.*

Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	*Figura No. 49. Verificación de conectividad de PC-A a PC-C.*  *Fuente: propia.*
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	*Figura No. 50. Verificación de acceso al Servidor.*  *Fuente: propia.* Para este caso, al insertar la IP 209.165.200.229 no tiene acceso ya que en el ambiente de simulación el router no permite la habilitación del protocolo HTTP.

	Sin embargo, se aplica en el navegador la IP configurada en el servidor que es: 209.165.200.238 y se visualiza la información configurada en el archivo **index.html** del servidor.

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

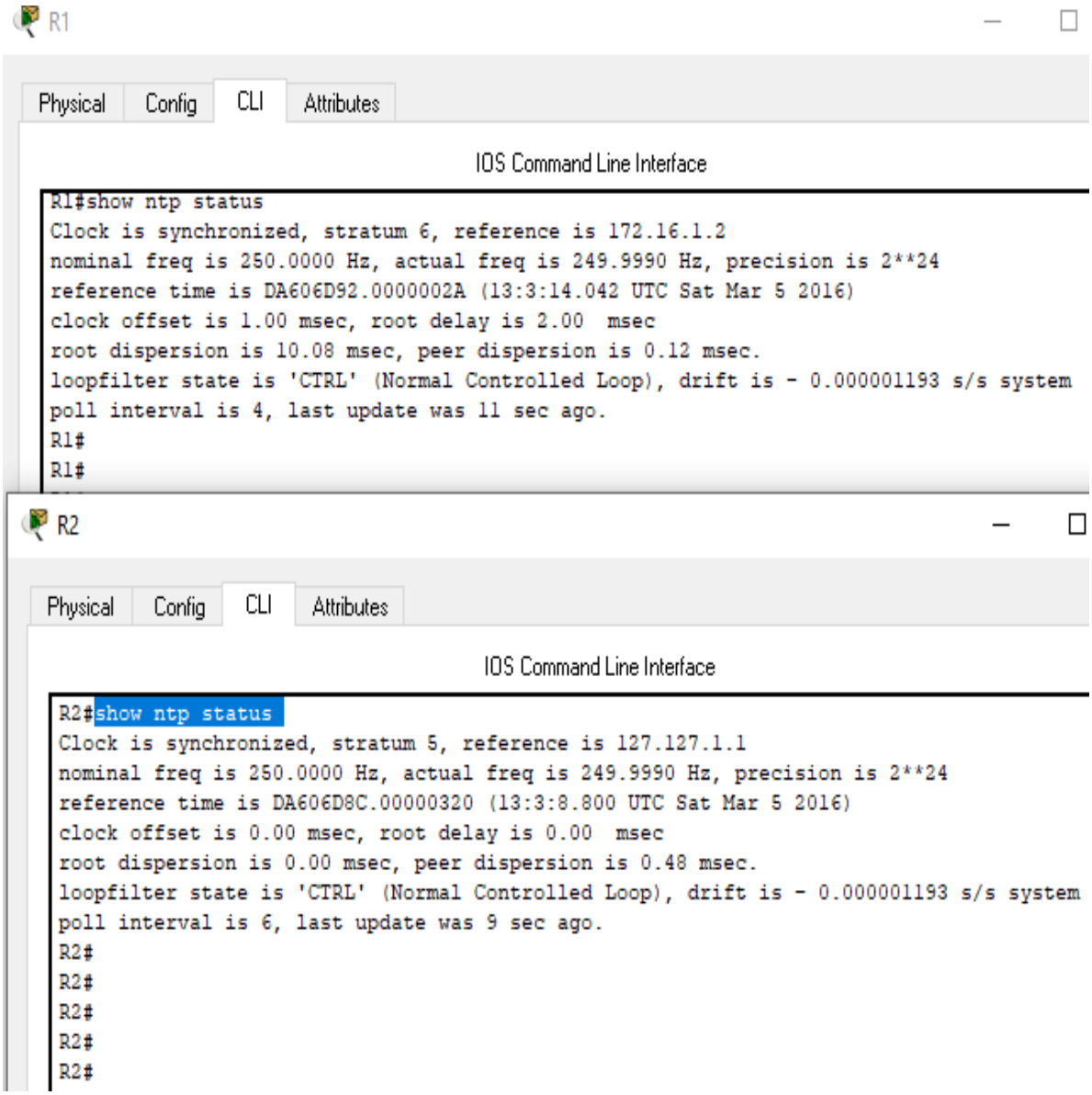
3.2.6 Parte 6: Configurar NTP.

Tabla No. 33. Configuración NTP.

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 t** R2(config)#**ntp master 5** R2(config)#**exit** R2#
Configure R1 como un cliente NTP. • Servidor: **R2**	R1#**config t** R1(config)#**ntp server 172.16.1.2** R1(config)#**exit** R1#
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1#**config t** R1(config)#**ntp update-calendar** R1(config)#**exit** R1#
Verifique la configuración de NTP en R1	Se aplica el comando **show ntp status** en R1 y R2.

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Figura No. 51. Visualización de configuración NTP en R1 y R2.



Fuente: propia.

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

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

Tabla No. 34. 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 t** R2(config)#**ip access-list standard ADMIN-MGT** R2(config)#**permit host 172.16.1.1** R2(config)#**exit** R2#
Aplicar la ACL con nombre a las líneas VTY	R2#**config t** R2(config)#**line vty 0 4** R2(config)#**access-class ADMIN-MGT in** R2(config)#**exit** R2#
Permitir acceso por Telnet a las líneas de VTY	R2#**config t** R2(config)#**line vty 0 4** R2(config)#**transport input telnet** R2(config)#**exit** R2#
Verificar que la ACL funcione como se espera	*Figura No. 52. Verificación y conexión Telnet desde R1 a R2*  *Fuente: propia.*

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

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

Tabla No. 35. Líneas de comando aplicadas a listas de acceso.

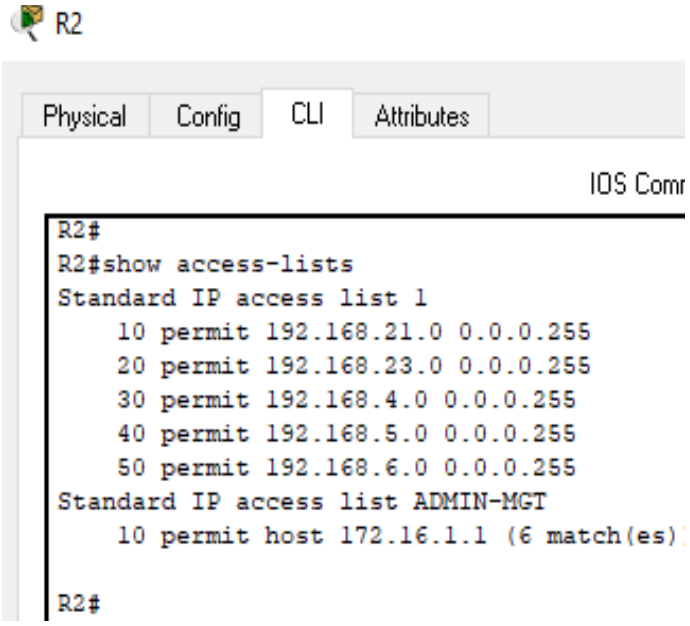
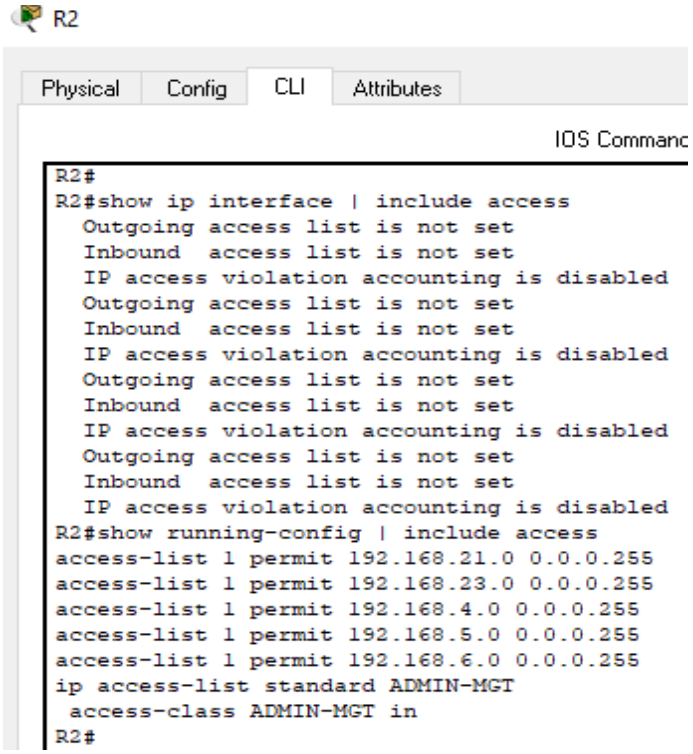
Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció.	R2#**show access-lists** R2# *Figura No. 53. Verificación lista de acceso.*  *Fuente: propia.*
Restablecer los contadores de una lista de acceso.	R2# R2#**clear access-list counters** R2#
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#**show ip interface | include access** R2#**show running-config | include access** R2#

Figura No. 54. Visualización lista de acceso.



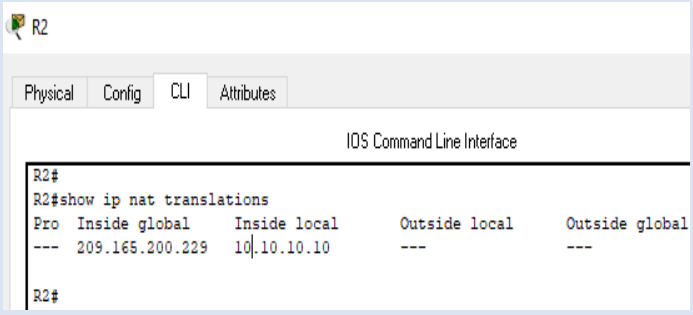
Fuente: propia.

¿Con qué comando se muestran las traducciones NAT?

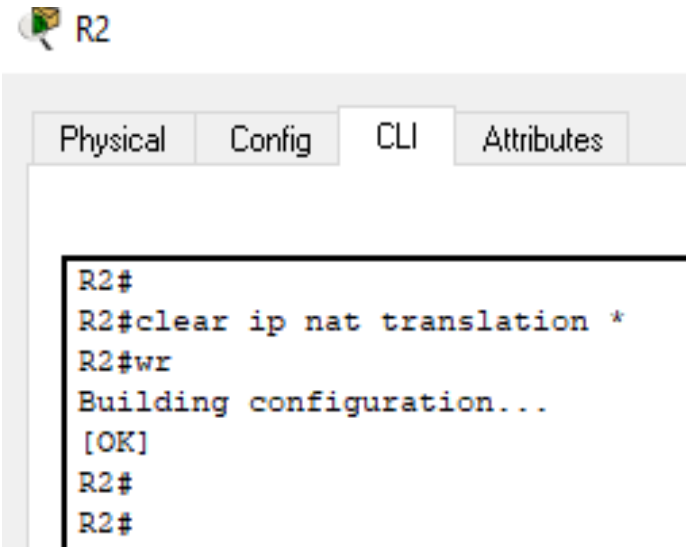
- Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.

R2#**show ip nat translations**

Figura No. 55. Visualización traducciones NAT.



Fuente: propia.

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#**clear ip nat translation** *Figura No. 56. Eliminación traducciones NAT.*  *Fuente: propia.*

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

4. CONCLUSIONES

Es de resaltar, que el desarrollo de los dos escenarios son una práctica exigente que permite atender diferentes temáticas y focaliza su estudio hacia el análisis, investigación y desarrollo que genera habilidades y destrezas en el diseño e implementación de una red. Dentro de las temáticas, se hizo necesario profundizar sobre EtherChannel, protocolo LACP, OSPF, NAT y ACL.

Se toma como referencias los dispositivos de tecnología CISCO que permiten la implementación de redes ajustados a conectividad, seguridad, control de acceso, interoperabilidad de protocolos IPv4 e IPv6, protocolos de enrutamiento, aplicación de redes virtuales VLAN, administración. direccionamiento dinámico, comando y control, establecimiento de listas de control de acceso y traducción de direcciones de red NAT.

La plataforma de CISCO Network Academy permite abordar las temáticas de CCNA1 y CCNA2 a través de módulos, simulaciones, pruebas y prácticas de laboratorio con información puntual y detallada que conlleva a un aprendizaje con efectividad y a preparar a los profesionales en campos relacionados directamente con las TIC's.

En el desarrollo de la actividad, se contrastaron diferentes comandos desde la interfaz de líneas de comandos en el ambiente simulado y con ello analizar, diagnosticar y corregir problemas a nivel de red y configuración de los dispositivos.

Las evidencias de los resultados exponen la construcción de redes WAN y LAN a través de los protocolos de enrutamiento estático y dinámico que permiten mayor eficiencia en la arquitectura de una red.

Los ambientes de simulación se acercan a la realidad frente a la configuración de los dispositivos familiarizando al profesional de redes en el empleo de comandos a través de la interfaz de línea de comandos y de esta manera planificar una adecuada programación del dispositivo de acuerdo con los requerimientos establecidos en una topología. El ambiente simulado de Packet Tracer permite conocer más a fondo las configuraciones, maneras y formas en las que se realiza un diseño e implementación de una red y posteriormente aplicar dichos conocimientos en un entorno de producción.

A través del ambiente simulado de las topologías se aprecia las diferentes configuraciones en el diseño e implementación de una red aplicados a los dispositivos activos como los son los switches y los routers.

Con la temática de IPV6, se identifica la capacidad, segmentación, direccionamiento e implementación siendo la evolución de IPv4. Además, aporta a la solución de los problemas de crecimientos de Internet, disminuye la congestión en las redes y reduce considerablemente el uso de NAT’s en redes.

5. BIBLIOGRAFÍA

CCNA1 Routing and Switching: Introducción a las redes (Introduction to Networks) (en línea) (20 de Junio de 2021) Disponible en: https://lms.netacad.com/course/view.php?id=470729

CCNA 2 Routing y switching de CCNA: Principios básicos de routing y switching (en línea) (01 de Julio de 2021) Disponible en: https://lms.netacad.com/course/view.php?id=542274

Bitacora Byte. DHCP en router CISCO. (en línea) (28 de Junio de 2021), Disponible en: https://bitacorabyte.wordpress.com/2017/07/18/configurar-dhcp-en-router-cisco/

Lobato, G. CURSO 7-1 Explicación de protocolo OSPF (Archivo de Vídeo) (en línea) (01 de Julio de 2021) Disponible en: https://www.youtube.com/watch?v=dwT5du44t_8

CISCO Networking Academy: Escalamiento de redes (en línea) (25 de Junio de 2021) Disponible en: https://www.itesa.edu.mx/netacad/scaling/index.html

CISCO Networking Academy: Principios básicos de routing y switching (en línea) (25 de Junio de 2021) Disponible en: https://www.itesa.edu.mx/netacad/switching/index.html

CISCO Networking Academy: Conexión de redes (en línea) (27 de Junio de 2021) Disponible en: https://www.itesa.edu.mx/netacad/networks/index.html

CISCO Networking Academy: Introducción a redes (en línea) (23 de Junio de 2021) Disponible en: https://www.itesa.edu.mx/netacad/introduccion/index.html

Redes CISCO. Guía de estudio para la certificación CCNA Security. Grupo Editorial RA-MA. (27 de Junio de 2021) Disponible en: https://books.google.es/books?hl=es&lr=&id=kI2fDwAAQBAJ&oi=fnd&pg=PP1&dq=libros+curso+cisco+ccna&ots=Jq1Ua8IxFk&sig=HSoG_fK_Z78G7lmNRI5cSLy0jv4#v=onepage&q=libros%20curso%20cisco%20ccna&f=false

UGALDE NAVA, EDUARDO Configuración de router CISCO con DHCP (Archivo de Vídeo) (en línea) (01 de Julio de 2021) Disponible en: https://www.youtube.com/watch?v=FIYGOzwjUqM

UGALDE NAVA, EDUARDO Cisco router ipv6 (Archivo de Vídeo) (en línea) (01 de Julio de 2021) Disponible en: https://www.youtube.com/watch?v=IKhrLNPD6uE

UGALDE NAVA, EDUARDO Configurar NAT con cisco router (Archivo de Vídeo) (en línea) (01 de Julio de 2021) Disponible en: https://www.youtube.com/watch?v=d18q-xYJuUU

Syllabus del curso Diplomado de profundización CISCO CCNA (2021). Disponible en: https://campus129.unad.edu.co/ecbti90/mod/folder/view.php?id=3858

Diseño e implementación de solucciones integradas LAN/WAN

"Solución de estudios de caso bajo el uso de la tecnología CISCO"

Oscar Javier Jerez González
ojjerezg@unadvirtual.edu.co
*Universidad Nacional Abierta y a Distancia **UNAD***
Escuela de Ciencias Básicas e Ingeniería **ECTBI**
Diplomando de Profundización CISCO CCNA

***Resumen* — Este entregable permite la familiarización con la implementación de redes LAN/WAN. En el informe demostrará de forma práctica los conocimientos adquiridos durante el curso Diplomado de Profundización CCNA de CISCO aplicando las habilidades y competencias adquiridas a lo largo de este. Se configurarán los dispositivos en cada uno de los escenarios y al final se verificarán si fueron aplicadas apropiadamente las configuraciones implementadas y que las redes funcionen correctamente. El simulador aplicado para el desarrollo de los dos escenarios es la aplicación propietaria de CISCO denominado Packet Tracer que permite las configuraciones básicas de switches y routers. Además, la configuración de interoperabilidad de protocolos IPv4 e IPv6, protocolos de enrutamiento, seguridad, aplicación de redes virtuales VLAN, direccionamiento dinámico, establecimiento de listas de control de acceso y traducción de direcciones de red NAT.**

***Abstract* — This deliverable allows familiarization with the implementation of LAN / WAN networks. The report will demonstrate in a practical way the knowledge acquired during the CISCO CCNA Deepening Diploma course, applying the skills and competencies acquired throughout it. The devices will be configured in each of the scenarios and at the end it will be verified if the implemented configurations were properly applied and that the networks are working correctly. The simulator applied for the development of the two scenarios is CISCO's proprietary application called Packet Tracer that allows the basic configurations of switches and routers. In addition, the interoperability configuration of IPv4 and IPv6 protocols, routing protocols, security, application of VLAN virtual networks, dynamic addressing, establishment of access control lists and NAT network address translation.**

Palabras clave: VPN, IOS, Protocolo, IPV4, IPV6, DHCP, topología, NAT, ACL, interfaz, gateway, seguridad, control de acceso, conectividad.

I. INTRODUCCIÓN

En este artículo se describe la implementación en un entorno de simulación del escenario No. 1. En esta instancia se identifica la topología, los dispositivos activos a emplear, las aplicaciones de software de simulación, un visón general a los requerimientos y una revisión previa a las literaturas relacionadas con las temáticas de la guía.

Es de resaltar la configuración de los switches y el router donde se validan: los protocolos de autenticación para el acceso, creación de enlaces a través de las interfaces, interoperabilidad de protocolos IPv4 e IPV6, creación de VLAN's, establecimiento de listas de control de acceso, traducción de direcciones NAT y los equipos de cómputo realizan configuración del protocolo DHCP.

Con el desarrollo e implementación de la topología, busca desarrollar un pensamiento crítico y habilidades para resolver problemas mediante equipamientos reales y entornos de simulación. Además, se desplegará un conocimiento práctico de esquemas de direccionamiento IP y la seguridad de la red fundacional, y podrá realizar configuraciones básicas para routers y switches.

En la adquisición conceptos básicos de manera lógica, clara y sencilla en un mundo dominado por los medios electrónicos y la tecnología de la información, resulta imprescindible conocer cómo funcionan las redes. Por ello, las temáticas tratadas en el tránsito del Diplomado conllevan a identificar que los aspectos más importantes de las redes no

son los dispositivos ni los medios, sino los protocolos que especifican la manera en que se envían los mensajes, cómo se direccionan a través de la red y como se interpretan en los dispositivos de destino.

II. OBJETIVOS

A. Objetivo General

Desarrollar los requerimientos de la guía "Prueba dde habilidades"

B. Objetivos específicos

- Aprehensión de conceptos relacionados con redes teleinformáticas.
- Implementar las topologías propuestas en un entorno de simulación evaluando los requerimientos y alternativas de solución.
- Configurar los dispositivos: router, switch y equipos que admitan tanto la conectividad IPv4 como IPv6, protocolos de enrutamiento, creación de VLAN's, NAT, listas de control de acceso y seguridad con los comandos diseñados para tal fin.
- Verificar el estado de conexiones y enrutamientos a través de las solicitudes de eco y trazabilidad en los diferentes enlaces de cada topología.

III. TEMÁTICAS PARA DESARROLLAR

Todas las temáticas vistas a lo largo del Diplomado de profundización CISCO CCNA. Tales como:

- Conectividad
- Seguridad.
- Control de acceso.
- Interoperabilidad de protocolos IPV4 e IPv6.
- protocolos de enrutamiento.
- Aplicación de redes virtuales VLAN.
- direccionamiento dinámico.
- Administración.
- Establecimiento de listas de control de acceso
- traducción de direcciones de red NAT.

IV. ACTIVIDADES PARA DESARROLLAR

Implementar la topología del escenario uno propuesto en la guía de "Prueba de habilidades prácticas CCNA"

V. METODOLOGÍA DE IMPLEMENTACIÓN Y DESARROLLO

Con base a las indicaciones y requerimientos de la guía del Diplomando se desarrolla la simulación del escenario No. 1

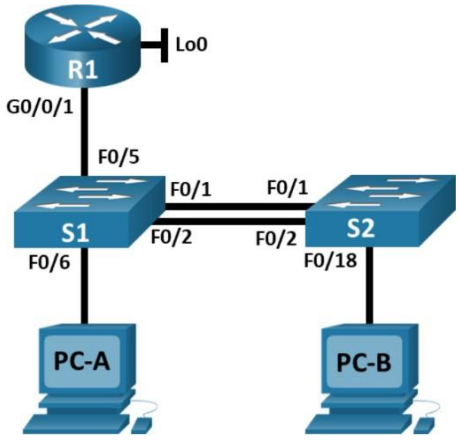


Figura No. 1. Topología escenario No. 1. Fuente: Guía Prueba de habilidades prácticas CCNA.

"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."

Para el desarrollo de este escenario se instala el entorno de simulación de Packet Tracer versión 8.0. Se crea la topología de red con los siguientes dispositivos: **Router Cisco ISR4331** (01), **Switch Cisco WS-C3560-24PS** (02) y **Equipo de cómputo de escritorio** (02).

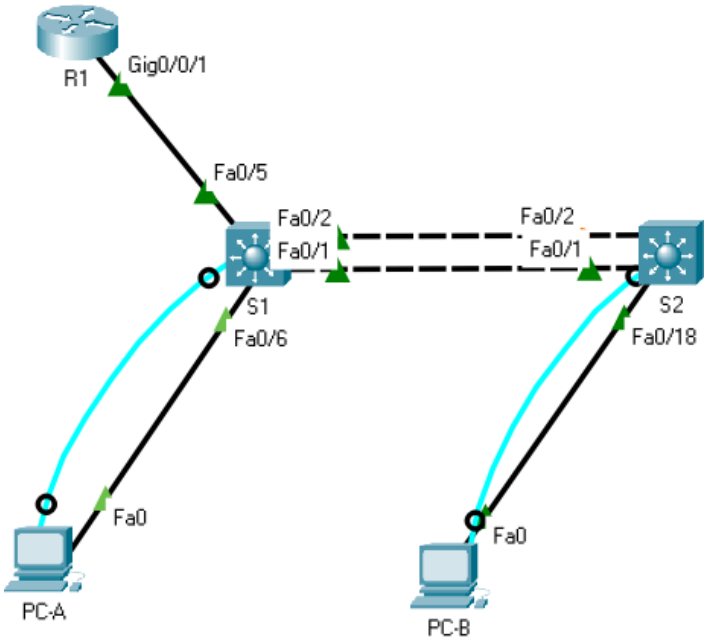


Figura No. 2. Topología escenario No. 1 Simulador Packet Tracer. Fuente: propia.

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

Tabla No. 1. Tabla de VLAN. Fuente: Propia, tomando como referencia Guía Prueba de habilidades prácticas CCNA.

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:db5: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

Tabla No. 2. Tabla de asignación de direcciones. Fuente: Propia, tomando como referencia Guía Prueba de habilidades prácticas CCNA.

VI. INSTRUCCIONES

Parte 1: Inicializar, recargar y configurar aspectos básicos de los dispositivos.

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

Parte 3: Configurar soporte de Host.

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

VII. DESARROLLO

Parte 1: Inicializar, recargar y configurar aspectos básicos de los dispositivos.

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

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

En este paso, se realizan las configuraciones en modo de configuración global en los Swiches S1 y S2 con la plantilla SDM (Switch Database Manager). Se aplica el comando sdm prefer dual-ipv4-and-ipv6 default que permite funciones equilibradas y se divide en enrutamiento y VLAN. Además, con la incorporación de la plantilla se garantiza la interoperabilidad entre IPV4 e IPV6.

Paso 2: Configurar Router R1.

Tarea	Especificación
Desactivar la búsqueda DNS	Router> Router> **enable** Router# **configure terminal** Router(config)# **no ip domain-lookup** Router(config)#
Nombre del router	Router(config)# **hostname R1** R1(config)#
Nombre de dominio	R1(config)# **ip domain-name ccna-lab.com** R1(config)#
Contraseña cifrada para el modo Ex EC privilegiado	R1(config)# **enable secret ciscoenpass** R1(config)#
Contraseña de acceso a la consola	R1(config)# **line console 0** R1(config-line)# **password ciscoconpass** R1(config-line)# **login** R1(config-line)# **exit** R1(config)#
Establecer la longitud mínima para las contraseñas	R1(config)# **security passwords min-length 10** R1(config)#
Crear un usuario administrativo en la base de datos local	R1(config)# **username admin password admin1pass** R1(config)#
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)# **line vty 0 15** R1(config-line)# **login local** R1(config-line)# **exit** R1(config)#
Configurar VTY solo aceptando SSH	R1(config)# **line vty 0 15** R1(config-line)# **transport input ssh** R1(config-line)# **login local** R1(config-line)# **exit** R1(config)#
Cifrar las contraseñas de texto no cifrado	R1(config)# **service password-encryption** R1(config)#
Configure un MOTD Banner	R1(config)# **banner motd # ⋯ CCNA - Acceso restringido ⋯ #** R1(config)#
Habilitar el routing IPv6	R1(config)# **ipv6 unicast-routing** R1(config)#
Configurar interfaz G0/0/1 y subinterfaces Establecer: · Descripción · Dirección IPv4. · Dirección local de enlace IPv6 como fe80: :1 · Dirección IPv6. · Activar la interfaz.	R1(config)# **interface gigabitEthernet 0/0/1.2** R1(config-subif)# **encapsulation dot1Q 2** R1(config-subif)# **description Vlan2 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)# R1(config)# **interface gigabitEthernet 0/0/1.3** R1(config-subif)# **encapsulation dot1Q 3** R1(config-subif)# **description Vlan3 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)# R1(config)# **interface gigabitEthernet 0/0/1.4** R1(config-subif)# **encapsulation dot1Q 4** R1(config-subif)# **description Vlan4 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)# R1(config)# **interface gigabitEthernet 0/0/1.6** R1(config-subif)# **encapsulation dot1Q 6** R1(config-subif)# **description Vlan6 Native** R1(config-subif)# **ipv6 address fe80::1 link-local** R1(config-subif)# **exit** R1(config)#
	R1(config)# **interface gigabitEthernet 0/0/1.6** R1(config-if)# **no shutdown** R1(config-if)# **exit** R1(config)#
Configure el Loopback0 interface	R1(config)# R1(config)# **interface loopback 0** R1(config-if)# **ip address 209.165.201.1 255.255.255.224** R1(config-if)# **ipv6 address 2001:db8:acad:209::1/64** R1(config-if)# **ipv6 address fe80::1 link-local** R1(config-if)# **no shutdown** R1(config-if)# **exit** R1(config)#
Generar una clave de cifrado RSA Módulo de 1024 bits	R1(config)# R1(config)# **crypto key generate rsa 1024** R1(config)# **do wr** R1(config)# **exit** R1#

Tabla No. 3. Configuración Router 1 (R1). Fuente: Propia, tomando como referencia Guía Prueba de habilidades prácticas CCNA.

Paso 3: Configurar Switches S1 y S2.

Tarea	Especificación
Desactivar la búsqueda DNS	Switch> Switch> **enable** Switch# **configure terminal** Switch(config)# **no ip domain lookup** Switch(config)#
Nombre del Switch	Switch(config)# **hostname S1** S1(config)#
Nombre de dominio	S1(config)# **ip domain-name ccna-lab.com** S1(config)#
Contraseña cifrada para el modo Ex EC privilegiado	S1(config)# **enable secret ciscoenpass** S1(config)#
Contraseña de acceso a la consola	S1(config)# **line console 0** S1(config-line)# **password ciscoconpass** S1(config-line)# **login** S1(config-line)# **exit** S1(config)#
Crear un usuario administrativo en la base de datos local	S1(config)# **username admin password admin1pass** S1(config)#
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)# **line vty 0 15** S1(config-line)# **login local** S1(config-line)# **exit** S1(config)#
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)# **line vty 0 15** S1(config-line)# **transport input ssh** S1(config-line)# **login local** S1(config-line)# **exit** S1(config)#
Cifrar las contraseñas de texto no cifrado	S1(config)# **service password-encryption** S1(config)#
Configure un MOTD Banner	S1(config)# **banner motd # ··· CCNA - Acceso restringido ··· #** S1(config)#
Generar una clave de cifrado RSA Módulo de 1024 bits	S1(config)# **crypto key ey generate rsa 1024** S1(config)#
Configurar interfaz de administración (SVI)	S1(config)# S1(config)# **interface Vlan4**
Establecer: · Dirección IPv4 de capa 3. · Dirección local de enlace IPv6 como FE80::98 para S1 y FE80::99 para S2. · Dirección IPv6 en capa 3.	S1(config-if)# **ip address 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 Vlan4 Management** S1(config-if)# **no shutdown** S1(config-if)# **exit** S1(config)#

Configuración del Gateway predeterminado. Configure la puerta de enlace predeterminada como 10.21.5.97 para IPv4	S1(config)# S1(config)# **ip default-gateway 10.21.5.97** S1(config)# **do wr** Building configuration... [OK] S1(config)#

Tabla No. 4. Configuración Switch 1 (S1). Fuente: Propia, tomando como referencia Guía Prueba de habilidades prácticas CCNA.

Tarea	Especificación
Desactivar la búsqueda DNS	Switch> Switch> **enable** Switch# **configure terminal** Switch(config)# **no ip domain lookup** Switch(config)#
Nombre del Switch	Switch(config)# **hostname S2** S2(config)#
Nombre de dominio	S2(config)# **ip domain-name ccna-lab.com** S2(config)#
Contraseña cifrada para el modo Ex EC privilegiado	S2(config)# **enable secret ciscoenpass** S2(config)#
Contraseña de acceso a la consola	S2(config)# **line console 0** S2(config-line)# **password ciscoconpass** S2(config-line)# **login** S2(config-line)# **exit** S2(config)#
Crear un usuario administrativo en la base de datos local	S2(config)# **username admin password admin1pass** S2(config)#
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)# **line vty 0 15** S2(config-line)# **login local** S2(config-line)# **exit** S2(config)#
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config)# **line vty 0 15** S2(config-line)# **transport input ssh** S2(config-line)# **login local** S2(config-line)# **exit** S2(config)#
Cifrar las contraseñas de texto no cifrado	S2(config)# **service password-encryption** S2(config)#
Configure un MOTD Banner	S2(config)# **banner motd # ··· CCNA - Acceso restringido ··· #** S2(config)#
Generar una clave de cifrado RSA Módulo de 1024 bits	S2(config)# **crypto key ey generate rsa 1024** S2(config)#
Configurar interfaz de administración (SVI) Establecer: · Dirección IPv4 de capa 3. · Dirección local de enlace IPv6 como FE80::98 para S1 y FE80::99 para S2. · Dirección IPv6 en capa 3.	S2(config)# S2(config)# **interface Vlan4** S2(config-if)# **ip address 10.21.5.99 255.255.255.248** S2(config-if)# **ipv6 address 2001:db5:acad:c::99/64** S2(config-if)# **ipv6 address fe80::99 link-local** S2(config-if)# **description Vlan4 Management** S2(config-if)# **no shutdown** S2(config-if)# **exit** S2(config)#
Configuración del gateway predeterminado. Configure la puerta de enlace predeterminada como 10.21.5.97 para IPv4	S2(config)# S2(config)# **ip default-gateway 10.21.5.97** S2(config)# **do wr** Building configuration... [OK] S2(config)#

Tabla No. 5. Configuración Switch 2 (S2). Fuente: Propia, tomando como referencia Guía Prueba de habilidades prácticas CCNA.

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

Paso 1: Configuración Switch S1.

Tarea	Especificación
Crear VLAN	S1(config)# S1(config)#**vlan 2** S1(config-vlan)#**name Bikes**
VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	S1(config-vlan)#**name Trikes** S1(config-vlan)#**exit** S1(config)#**vlan 4** S1(config-vlan)#**name Management** S1(config-vlan)#**exit** S1(config)#**vlan 5** S1(config-vlan)#**name Parking** S1(config-vlan)#**exit** S1(config)#**vlan 6** S1(config-vlan)#**name Native** S1(config-vlan)#**exit** S1(config)#
Crear troncales 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1, F0/2 y F0/5	S1(config)# S1(config)#**interface fa0/5** S1(config-if)#**switchport trunk encapsulation dot1q** S1(config-if)#**switchport mode trunk** S1(config-if)#**switchport trunk native vlan 6** S1(config-if)#**switchport trunk allowed vlan 2,3,4,6** S1(config-if)#**exit** S1(config)# S1(config)#**interface range fastEthernet 0/1-2** S1(config-if-range)# **shutdown** S1(config-if-range)#**switchport trunk encapsulation dot1q** S1(config-if-range)#**switchport mode trun k** S1(config-if-range)#**switchport trunk native vlan 6** S1(config-if-range)#**switchport trunk allowed vlan 2,3,4,6** S1(config-if-range)#**exit** S1(config)#
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 Usar el protocolo LACP para la negociación	S1(config)# S1(config)#**interface range fastEthernet 0/1-2** S1(config-if-range)#**channel-group 1 mode active** S1(config-if-range)#**channel-protocol lacp** S1(config-if-range)#**interface Port-channel 1**
	S1(config-if)#**switchport trunk encapsulation dot1q** S1(config-if)#**switchport mode trun k** S1(config-if)#**switchport trunk native vlan 6** S1(config-if)#**exit** S1(config)#
Configurar el puerto de acceso de host para VLAN 2 en la Interface F0/6	S1(config)# S1(config)#**interface fastEthernet 0/6** S1(config-if)#**switchport mode access** S1(config-if)#**switchport access vlan 2** S1(config-if)#**exit** S1(config)#
Configurar la seguridad del puerto en los puertos de Acceso Permitir 3 direcciones MAC	S1(config)# S1(config)#**interface fastEthernet 0/6** S1(config-if)#**switchport port-security maximum 3** S1(config-if)#**exit** S1(config)#
Proteja todas las interfaces no utilizadas Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S1(config)# S1(config)#**interface range fa0/3-4, fa0/7-24, gig0/1-2** S1(config-if-range)#**switchport mode access** S1(config-if-range)#**switchport access vlan 5** S1(config-if-range)#**description *** Puertos sin utilizar ***** S1(config-if-range)#**shutdown** S1(config-if-range)#**exit** S1(config)#**do wr** Building configuration... [OK] S2(config)#

Tabla No. 6. Configuración Switch 1 (S1). Fuente: Propia, tomando como referencia Guía Prueba de habilidades prácticas CCNA.

Tarea	Especificación
Crear VLAN VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	S2(config)# 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)#**do wr** Building configuration... [OK] S2(config-vlan)#**exit** S2(config)#
Crear troncales 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1 y F0/2	S2(config)# S2(config)#**interface range fastEthernet 0/1-2** S2(config-if-range)# **shutdown** S2(config-if-range)#**switchport trunk encapsulation dot1q** S2(config-if-range)#**switchport mode trun k** S2(config-if-range)#**switchport trunk native vlan 6** S2(config-if-range)#**switchport trunk allowed vlan 2,3,4,6** S2(config-if-range)#**exit** S2(config)#
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 Usar el protocolo LACP para la negociación.	S2(config)# S2(config)#**interface range fastEthernet 0/1-2** S2(config-if-range)#**channel-group 1 mode active** S2(config-if-range)#**interface Port-channel 1** S2(config-if-range)#**channel-protocol lacp** S2(config-if)#**switchport trunk encapsulation dot1q** S2(config-if)#**switchport mode trunk** S2(config-if)#**switchport trunk native vlan 6** S2(config-if)#**exit** S2(config)#
Configurar el puerto de acceso de host para VLAN 3 en la Interface F0/18	S2(config)# S2(config)#**interface fastEthernet 0/18** S2(config-if)#**switchport mode access** S2(config-if)#**switchport access vlan 3** S2(config-if)#**exit** S2(config)#**do wr** Building configuration... [OK] S1(config)#
Configure port-security en los access ports Permitir 3 direcciones MAC	S2(config)# S2(config)#**interface fastEthernet 0/18** S2(config-if)#**switchport mode access** S2(config-if)#**switchport port-security maximum 3** S2(config-if)#**exit** S2(config)#
Proteja todas las interfaces no utilizadas Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S2(config)# S2(config)#**interface range fa0/3-17, fa0/19-24, gig0/1-2** S2(config-if-range)#**switchport mode access** S2(config-if-range)#**switchport access vlan 5** S2(config-if-range)# **switchport port-security** S2(config-if-range)# **switchport port-security violation shutdown** S2(config-if-range)#**description ***Puertos sin utilizar ***** S2(config-if-range)#**shutdown** S2(config-if)#**do wr** Building configuration... [OK] S2(config-if)#**exit** S2(config)#

Tabla No. 7. Configuración Switch 2 (S2). Fuente: Propia, tomando como referencia Guía Prueba de habilidades prácticas CCNA.

Parte 3: Configurar soporte de Host.

Paso 1: Configuración Router R1.

Tarea	Especificación
Configure Default Routing Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0	R1> R1>**enable** R1#**configure terminal** R1(config)# **ip route 0.0.0.0 0.0.0.0 loopback 0** R1(config)# **ipv6 route ::/0 loopback 0** R1(config)#**exit** R1#
Configurar IPv4 DHCP para VLAN 2 Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada	R1(config)# **ip dhcp excluded-address 10.21.5.2 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** R1(config)# R1#
Configurar DHCP IPv4 para VLAN 3 Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada.	R1(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** R1(config)#**do wr** R1(config)# R1#

Tabla No. 8. Configuración Router 1 (R1). Fuente: Propia, tomando como referencia Guía Prueba de habilidades prácticas CCNA.

Paso 2: Configurar los servidores.

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

En las PC-A y B se activa el DHCP para IPv4 y configuración automática para
IPv6

Configuración de red de PC-A	
Descripción	**PC-A**
Dirección física	**0006.2ABD.32E2**
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 No. 9. Configuración de red del PC-A. Fuente: Propia, tomando como referencia Guía Prueba de habilidades prácticas CCNA.

Configuración de red de PC-B	
Descripción	**PC-B**
Dirección física	**00D0.BC98.2B0B**
Dirección IP	**10.21.5.86**
Máscara de subred	**255.255.255.224**
Gateway predeterminado	**10.21.5.65**
Gateway predeterminado IPv6	**FE80::1**

Tabla No. 10. Configuración de red del PC-B. Fuente: Propia, tomando como referencia Guía Prueba de habilidades prácticas CCNA.

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

Desde	A	de Internet	Dirección IP	Resultados de PING
PC-A	R1, G0/0/1.2	Dirección	10.21.5.1	✓
		IPv6	2001:db5:acad:a::1	✓
	R1, G0/0/1.3	Dirección	10.21.5.65	✓
		IPv6	2001:db5:acad:b::1	✓
	R1, G0/0/1.4	Dirección	10.21.5.97	✓
		IPv6	2001:db5:acad:c::1	✓
	S1, VLAN 4	Dirección	10.21.5.98	✓
		IPv6	2001:db5:acad:c::98	✓
	S2, VLAN 4	Dirección	10.21.5.99	✓
		IPv6	2001:db5:acad:c::99	✓
	PC-B	Dirección	10.21.5.86 (esta IP puede cambiar al momento de ejecutar la simulación por ser **DHCP**)	✓
		IPv6	2001:db5:acad:b::50	✓
	R1 Bucle 0	Dirección	209.165.201.1	✓
		IPv6	2001:db5:acad:209::1	✓
PC-B	R1 Bucle 0	Dirección	209.165.201.1	✓
		IPv6	2001:db5:acad:209::1	✓
	R1, G0/0/1.2	Dirección	10.21.5.1	✓
		IPv6	2001:db5:acad:a::1	✓
	R1, G0/0/1.3	Dirección	10.21.5.65	✓
		IPv6	2001:db5:acad:b::1	✓
	R1, G0/0/1.4	Dirección	10.21.5.97	✓
		IPv6	2001:db5:acad:c::1	✓
	S1, VLAN 4	Dirección	10.21.5.98	✓
		IPv6	2001:db5:acad:c::98	✓
	S2, VLAN 4	Dirección	10.21.5.99	✓
		IPv6	2001:db5:acad:c: :99	✓

Tabla No. 11. Configuración de red del PC-B. Fuente: Propia, tomando como referencia Guía Prueba de habilidades prácticas CCNA.

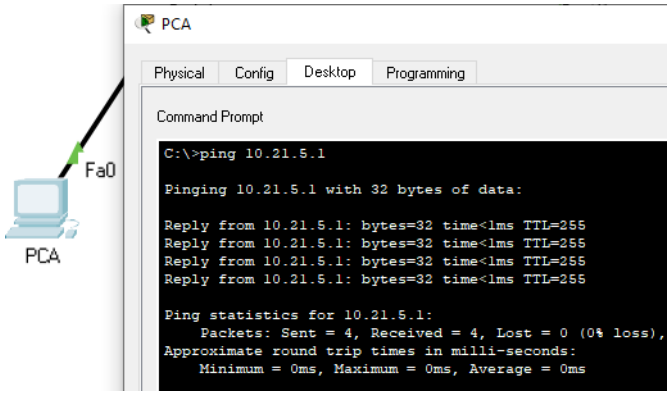


Figura No. 3. Prueba de conectividad desde PC-A a 10.21.5.1. Fuente: propia.

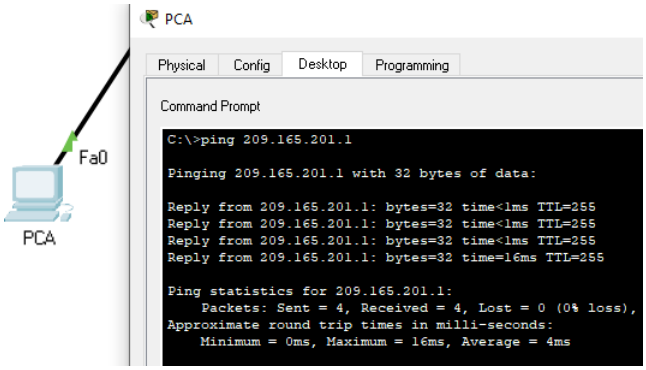


Figura No. 6. Prueba de conectividad desde PC-A a 209.165.201.1. Fuente: propia.

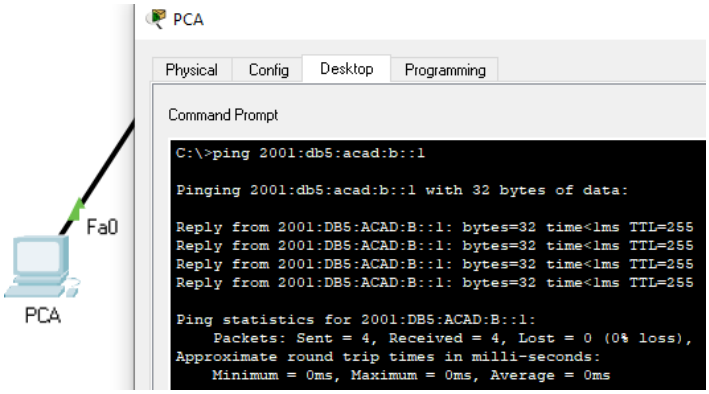


Figura No. 4. Prueba de conectividad desde PC-A a 2001:db5:acad:b::1. Fuente: propia.

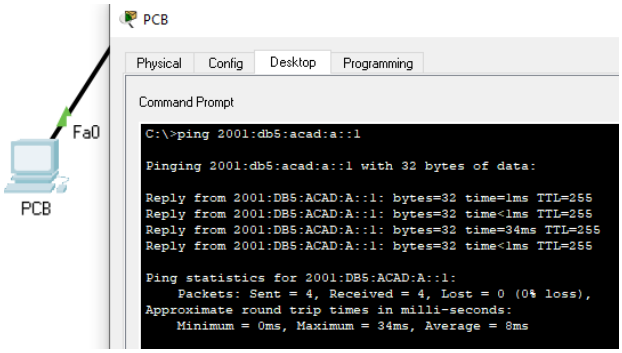


Figura No. 7. Prueba de conectividad desde PC-B a 2001:db5:acad:a::1. Fuente: propia.

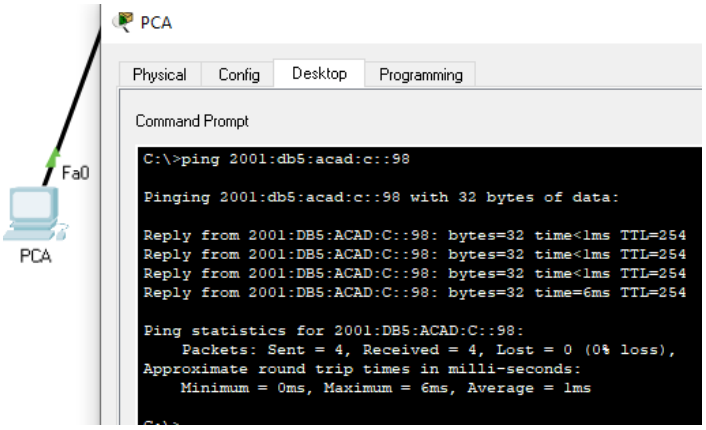


Figura No. 5. Prueba de conectividad desde PC-A a 2001:db5:acad:c::98. Fuente: propia.

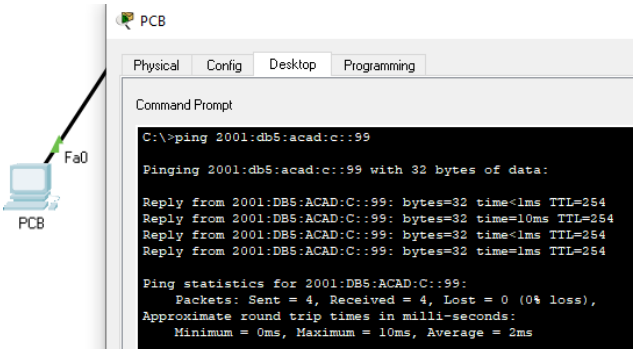


Figura No. 8. Prueba de conectividad desde PC-B a 2001:db5:acad:c::99. . Fuente: propia.

VIII. RESULTADOS DEL DESARROLLO E IMPLEMENTACIÓN DE LA TOPOLOGÍA DEL ESCENARIO NO. 1.

- Atendiendo los requerimientos de la guía, la orientación de las webs conferencias y encuentros CIPAS, se desarrolla e implementa la topología del escenario No. 1 en el entorno de simulación de Packet Tracer.

- A través de la interfaz de línea de comandos de switches y routers se realizan las configuraciones de seguridad, control de acceso, direccionamiento IPv4 e IPv6, NAT, VLAN's, ACL, DHCP y protocolos de enrutamiento.

- Se aplican las configuraciones básicas de switches y routers para el control de acceso a través de consola y líneas VTY y la encriptación de estas.

- El ambiente de simulación con Packet Tracer permite: la visualización global de una topología, realizar ajustes de configuración, reforzar conceptos teóricos, conocimiento de los dispositivos, y más importante detectar y corregir errores o fallas de funcionamiento en la red. Enfrentar

- Por último, con la configuración en cada dispositivo se realizan la verificación y pruebas de conectividad a través de la herramienta ping. De esta manera, se genera un diagnóstico de resultados.

IX. CONCLUSIONES

Es de resaltar, que el desarrollo de los dos escenarios son una práctica exigente que permite atender diferentes temáticas y focaliza su estudio hacia el análisis, investigación y desarrollo que genera habilidades y destrezas en el diseño e implementación de una red. Dentro de las temáticas, se hizo necesario profundizar sobre EtherChannel, protocolo LACP, OSPF, NAT y ACL.

Se toma como referencias los dispositivos de tecnología CISCO que permiten la implementación de redes ajustados a conectividad, seguridad, control de acceso, interoperabilidad de protocolos IPv4 e IPv6, protocolos de enrutamiento, aplicación de redes virtuales VLAN, direccionamiento dinámico, comando y control, establecimiento de listas de control de acceso y traducción de direcciones de red NAT.

La plataforma de CISCO Network Academy permite abordar las temáticas de CCNA1 y CCNA2 a través de módulos, simulaciones, pruebas y prácticas de laboratorio con información puntual y detallada que conlleva a un aprendizaje con efectividad y a preparar a los profesionales en campos relacionados directamente con las TIC's

En el desarrollo de la actividad, se contrastaron diferentes comandos desde la interfaz de líneas de comandos en el ambiente simulado y con ello analizar, diagnosticar y corregir problemas a nivel de red y configuración de los dispositivos.

Los ambientes de simulación se acercan a la realidad frente a la configuración de los dispositivos familiarizando al profesional de redes en el empleo de comandos a través de la interfaz de línea de comandos y de esta manera planificar una adecuada programación del dispositivo de acuerdo con los requerimientos establecidos en una topología. El ambiente simulado de Packet Tracer permite conocer más a fondo las configuraciones, maneras y formas en las que se realiza un diseño e implementación de una red y posteriormente aplicar dichos conocimientos en un entorno de producción.

En los entornos de producción y gracias a la tecnología de Cisco, es posible el acceso generalizado y seguro a la información desde diferentes dispositivos y en diversos lugares, con una mejora considerable de la productividad y la implementación de nuevos servicios.

X. REFERENCIAS BIBLIOGRÁFICAS

[1] CCNA1 Routing and Switching: Introducción a las redes (Introduction to Networks) Disponible en: https://lms.netacad.com/course/view.php?id=470729 [Ultimo acceso 20 de Junio de 2021]

[2] OpenWebinars. (2019, 26 abril). Cisco: Configuración de SDM Templates [Vídeo]. YouTube.com. https://www.youtube.com/watch?v=L4bwV5M6hkk.

[3] Ariganello, E. (2013). Redes CISCO. Guía de estudio para la certificación CCNA Security. Grupo Editorial RA-MA.

[4] SSH. (s. f.). SSH (Secure Shell). ssh.com. Recuperado 9 de noviembre de 2020, de https://www.ssh.com/ssh/

[5] CISCO. (s. f.-b). Configurar el enlace del EtherChannel y del 802.1Q. Recuperado 29 de junio de 2021, de https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-4000-series-switches/23408-140.html.

[6] Redes CISCO. Guía de estudio para la certificación CCNA Security. Grupo Editorial RA-MA. Disponible en: https://bit.ly/3e5ziTz [Ultimo acceso 27 de Junio de 2021]

[7] CCNA1 Routing and Switching: Introducción a las redes (Introduction to Networks) (en línea) Disponible en: https://lms.netacad.com/course/view.php?id=470729 [Ultimo acceso 20 de Junio de 2021]

[8] CCNA 2 Routing y switching de CCNA: Principios básicos de routing y switching (en línea) Disponible en:

https://lms.netacad.com/course/view.php?id=542274
[Ultimo acceso (01 de Julio de 2021)]

[9] Syllabus del curso Diplomado de profundización CISCO CCNA (2021). Disponible en: https://campus129.unad.edu.co/ecbti90/mod/folder/view.php?id=3858

[10] CISCO Networking Academy: Escalamiento de redes (en línea) Disponible en: https://www.itesa.edu.mx/netacad/scaling/index.html
[Ultimo acceso 25 de Junio de 2021]

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