DIPLOMADO DE PROFUNDIZACION CISCO

PRUEBA DE HABILIDADES CCNA I-2021

ANDRES YAIR OSPINA CALVO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA –ECBTI

INGENIERIA ELECTRONICA

PEREIRA

2021

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES CCNA I-2021

ANDRES YAIR OSPINA CALVO

Diplomado de opción de grado presentado para optar el título de
INGENIERO ELECTRONICO

DIRECTOR
HECTOR MANUEL HERRERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA –ECBTI
INGENIERIA ELECTRONICA
PEREIRA
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Pereira Risaralda, 06 de julio de 2021

AGRADECIMIENTOS

Agradecimientos primeramente a Dios por permitirme llegar hasta donde estoy, gracias a mi familia por apoyarme en cada decisión y proyecto con amor y palabras de aliento, gracias a cada uno de los profesores por su entrega y excelente labor en el transcurso de mi formación profesional.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

CISCO: es una empresa de origen estadounidense fabricante de dispositivos para redes locales y externa, también presta el servicio de soluciones de red, su objetivo es conectar a todos y demostrar las cosas asombrosas que se pueden lograr con una visión clara del futuro.

ROUTER: es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función es la de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.

SWITCH: es un dispositivo que permite que la conexión de computadoras y periféricos a la red, puedan comunicarse entre sí y con otras redes**.**

RED DE COMPUTADORAS: es un conjunto de equipos nodos y software conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

VLAN: es un método para crear redes lógicas independientes dentro de una misma red física, también conocida como red de área local virtual.

DHCP: El protocolo de configuración dinámica de host (DHCP) es un protocolo cliente/servidor que proporciona automáticamente un host de protocolo de Internet (IP) con su dirección IP y otra información de configuración relacionada, como la máscara de subred y la puerta de enlace predeterminada.

PROTOCOLO DE ENRUTAMIENTO: Son el conjunto de reglas utilizadas por un router cuando se comunica con otros routers con el fin de compartir información de enrutamiento, Ejemplo de este tipo de enrutamiento esta en los protocolos RIP, IGRP, EIGRP y OSPF.

RESUMEN

En este trabajo se procederá a realizar las configuraciones básicas, seguridad conectividad ipv4-ipv6, enrutamiento de las vlan, DHCP de los router, protocolo de routing dinámico OSPF, 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, switches y host del escenario 1 y 2, con la finalidad de tener respuestas remotas en la red local y un envió perfecto de paquetes.

Palabras claves: vlan, DHCP, router, switch, host,OSPF.

ABSTRACT

In this work, we will proceed to carry out the basic configurations, ipv4-ipv6 connectivity security, vlan routing, router DHCP, OSPF dynamic routing protocol, dynamic and static network address translation (NAT), control lists of access (ACL) and network time protocol (NTP) server / client, switches and hosts of scenarios 1 and 2, in order to have remote responses in the local network and a perfect sending of packets.

Keywords: vlan, DHCP, router, switch, host, OSPF.

INTRODUCCION

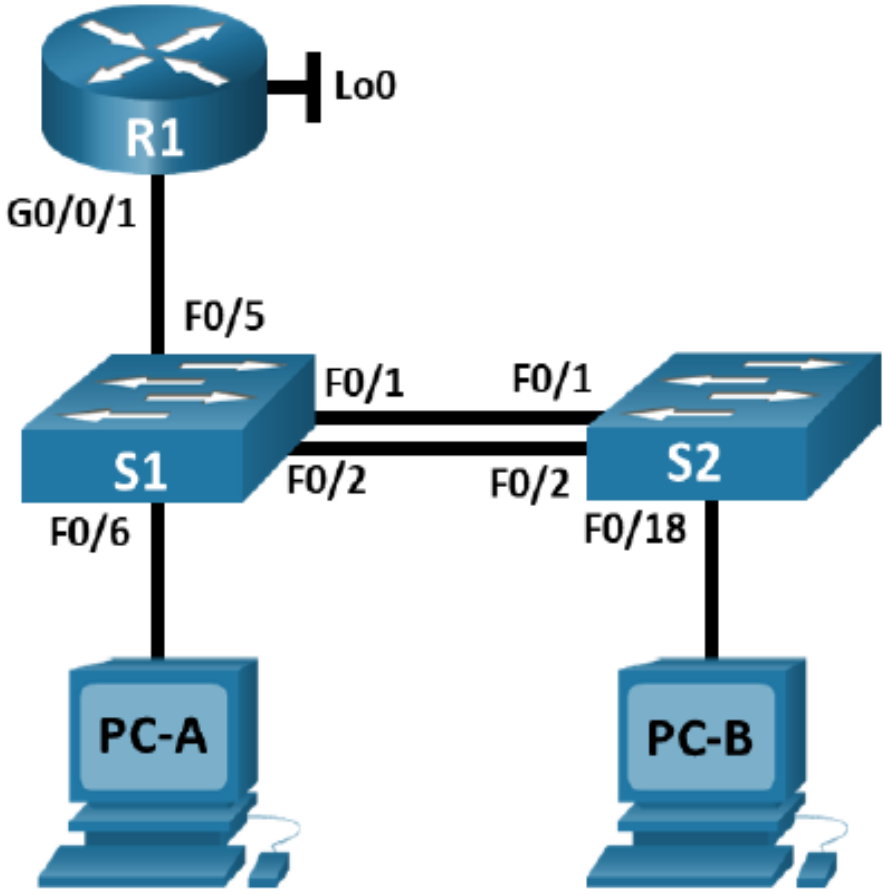
La finalidad del diplomado de profundización CISCO es capacitar y enseñar a los estudiantes a planificar, verificar, implementar y dar solución a problemas en redes LAN y WAN en un entorno virtual mediante un software de aprendizaje como packet tracer, el cual tiene las herramientas necesarias para que los estudiantes se familiaricen con los dispositivos informáticos y sus correspondientes configuraciones y de esta manera llevar sus conocimientos a un entorno real sea doméstico o empresarial.

En el desarrollo de las pruebas de habilidades prácticas CISCO nos vamos a centrar en el escenario 1 y 2 los cuales son redes locales pequeñas que constan de dispositivos básicos de redes (hosts, routers, switches, servidores, etc.), con los cuales se procederá a realizar las configuraciones básicas, seguridad, conectividad ipv4-ipv6, enrutamiento de las vlan y DHCP, protocolo de routing dinámico OSPF, 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 de los dispositivos antes mencionados.

DESARROLLO

1. escenario 1

Figura 1. Topología Escenario 1



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

Tabla 1. Tabla de vlan

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

Tabla 2. Tabla de asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8: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:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

Instrucciones

Parte 1: Inicializar,Recargar y Configurar aspectos basicos 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.

Router R1

Router>enable

Router#erase startup-config

Router#reload

Switch S1

switch>enable

switch#erase startup-config

switch#reload

Switch S2

switch>enable

switch#erase startup-config

switch#reload

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

Switch 1

Switch#configure terminal

Switch(config)#sdm prefer dual-ipv4-and-ipv6 default

Switch#reload

Switch 2

Switch#configure terminal

Switch(config)#sdm prefer dual-ipv4-and-ipv6 default

Switch#reload

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3. Configuración router R1

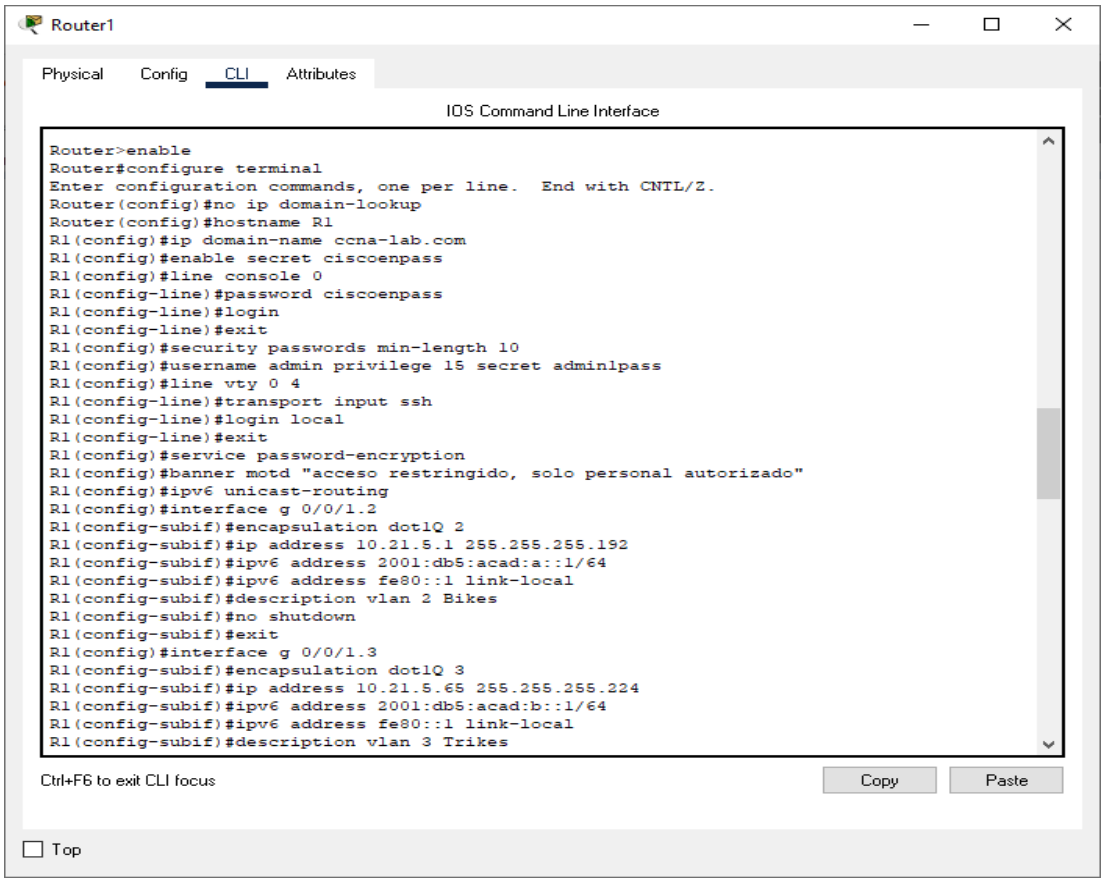
Tarea	Especificación	Solución
Desactivar la búsqueda DNS	N/A	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	R1	Router(config)#hostname R1
Nombre de dominio	ccna-lab.com	R1(config)#ip domain-name ccna-lab.com

Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	ciscoenpass	R1(config)#line console 0 R1(config-line)#password ciscoenpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	10 caracteres	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**	R1(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	N/A	R1(config)#line vty 0 4
Configurar VTY solo aceptando SSH	N/A	R1(config-line)#transport input ssh R1(config-line)#login local R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	N/A	R1(config)#service password-encryption
Configure un MOTD Banner	N/A	R1(config)#banner motd "acceso restringido, solo personal autorizado"
Habilitar el routing IPv6	N/A	R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como **fe80: :1** Establece la dirección IPv6. Activar la interfaz.	R1(config)#interface g 0/0/1.2 R1(config-subif)#encapsulation dot1Q 2 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)#description vlan 2 Bikes

		R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface g 0/0/1.3 R1(config-subif)#encapsulation dot1Q 3 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)#description vlan 3 Trikes R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface g 0/0/1.4 R1(config-subif)#encapsulation dot1Q 4 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)#description vlan 4 Management R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface g 0/0/1.6 R1(config-subif)#encapsulation dot1Q 6 Native R1(config-subif)#description vlan 6 native R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface g 0/0/1 R1(config-if)#no shutdown R1(config-if)#exit
Configure el Loopback0 interface	Establezca la descripción	R1(config)#interface lo0

	Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como **fe80::1**	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)#description loopback 0 R1(config-if)#exit
Generar una clave de cifrado RSA	Módulo de 1024 bits	R1(config)#crypto key generate rsa general-key modulus 1024

Figura 2. Configuración router R1 packet tracer



Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tabla4. Configuración Switch S1

Tarea	Especificación	Solución
Desactivar la búsqueda DNS.	N/A	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch	S1	Switch(config)#hostname S1
Nombre de dominio	ccna-lab.com	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	ciscoenpass	S1(config)#line console 0 S1(config-line)#password ciscoenpass S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass	S1(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	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
Cifrar las contraseñas de texto no cifrado	N/A	S1(config)#service password-encryption
Configurar un MOTD Banner	N/A	S1(config)#banner motd "acceso restringido, solo personal autorizado"

Generar una clave de cifrado RSA	Módulo de 1024 bits	S1(config)#crypto key generate rsa general-key modulus 1024
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 Establecer la dirección IPv6 de capa 3	S1(config)#interface vlan4 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
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.21.5.97 para IPv4	S1(config-if)#ip default-gateway 10.21.5.97 ipv6 route ::/0 2001:db5:acad:c::1

Figura 3. Configuración switch S1 packet tracer

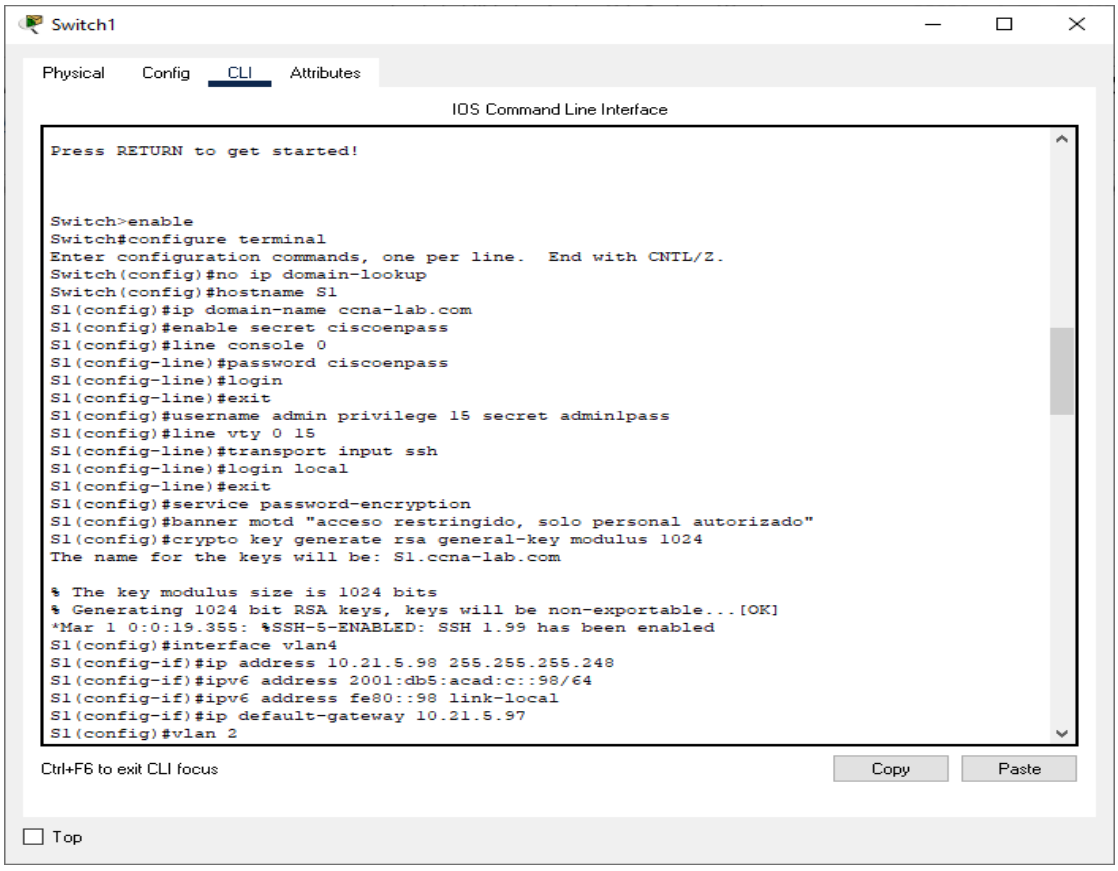
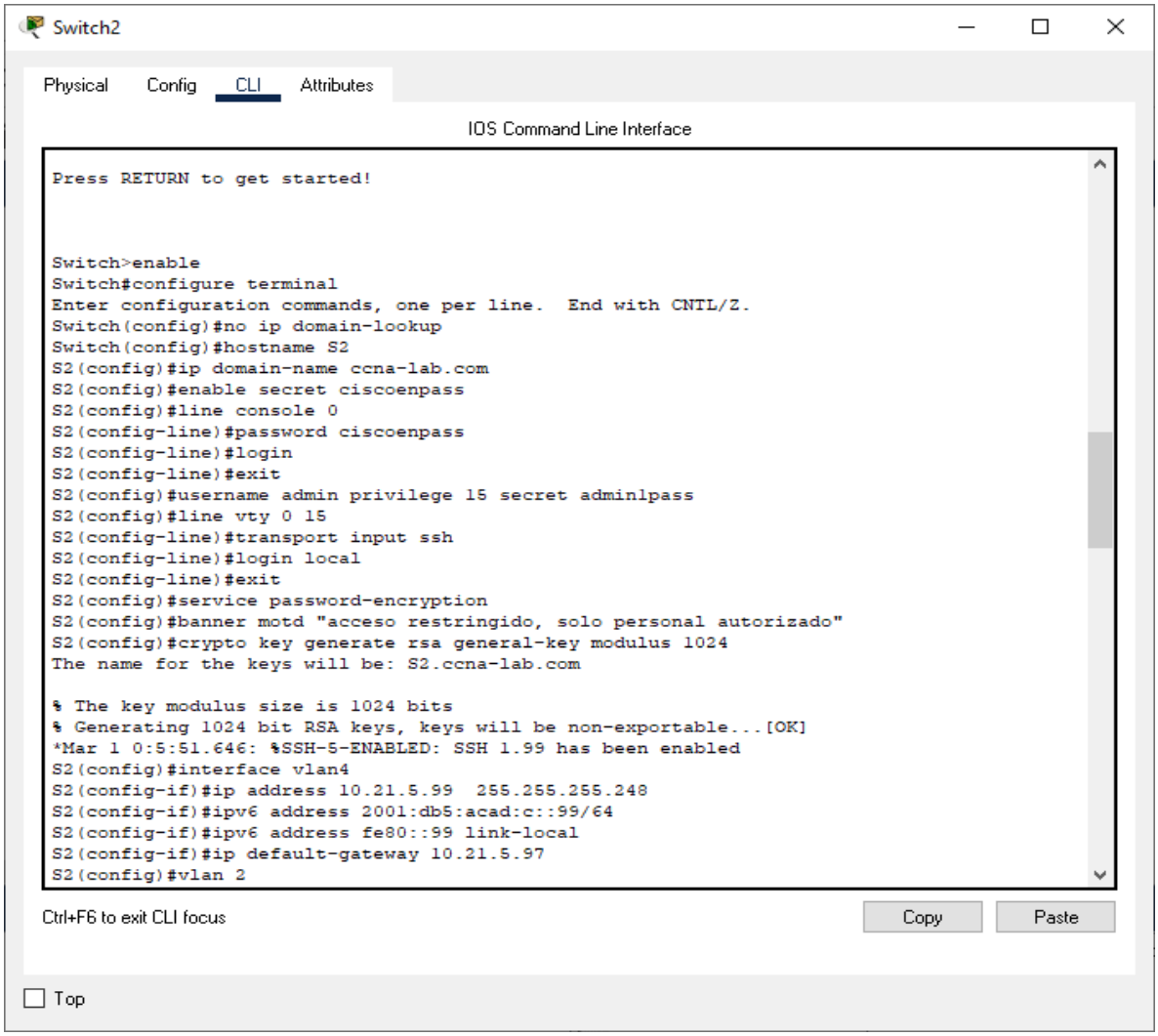


Tabla5. Configuración Switch S2

Tarea	Especificación	Solución
Desactivar la búsqueda DNS.	N/A	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch	S2	Switch(config)#hostname S2
Nombre de dominio	ccna-lab.com	S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass	S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	ciscoenpass	S2(config)#line console 0 S2(config-line)#password ciscoenpass S2(config-line)#login S2(config-line)#exit
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass	S2(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	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
Cifrar las contraseñas de texto no cifrado	N/A	S2(config)#service password-encryption
Configurar un MOTD Banner	N/A	S2(config)#banner motd "acceso restringido, solo personal autorizado"
Generar una clave de cifrado RSA	Módulo de 1024 bits	S2(config)#crypto key generate rsa general-key modulus 1024
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :99 para S2	S2(config)#interface vlan4 S2(config-if)#ip address 10.21.5.99 255.255.255.248

	Establecer la dirección IPv6 de capa 3	S2(config-if)#ipv6 address 2001:db5:acad:c::99/64 S2(config-if)#ipv6 address fe80::99 link-local
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.21.5.97 para IPv4	S2(config-if)#ip default-gateway 10.21.5.97 ipv6 route ::/0 2001:db5:acad:c::1

Figura 4. Configuración switch S2 packet tracer



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

Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 6. Configuración estructura de red Switch S1

Tarea	Especificación	Solución
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	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
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5	S1(config)#interface f 0/1 switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#exit S1(config)#interface f 0/2 switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#exit

		S1(config)#interface f 0/5 switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#exit
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)#int range f0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#interface port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk Native vlan 6 S1(config-if)#exit
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6	S1(config)#interface f 0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 S1(config-if)#exit
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC	S1(config)#interface f0/6 S1(config-if)#switchport port-security S1(config-if)#switchport port-security Maximum 3 S1(config-if)#exit
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S1(config)#int range g0/1-2,f0/3-4,f0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#switchport port-security

		S1(config-if-range)#switchport port-security violation shutdown S1(config-if-range)#description no usar S1(config-if-range)#shutdown

Figura 5. Configuración estructura de red Switch S1 packet tracer

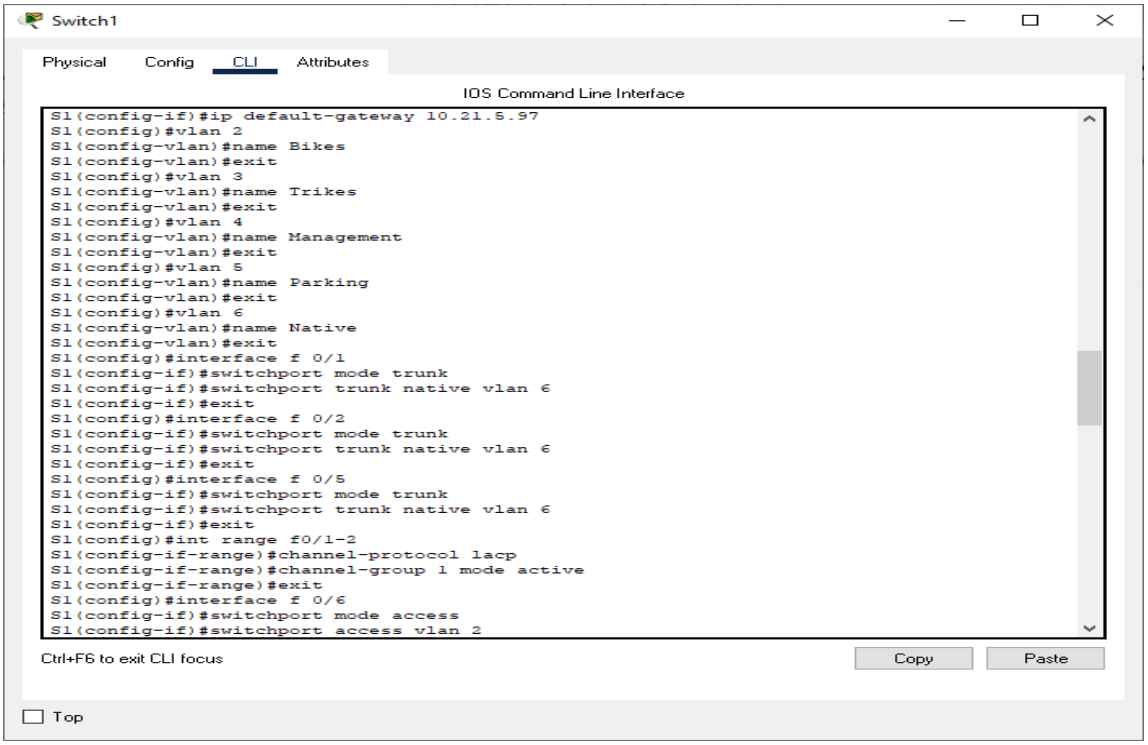


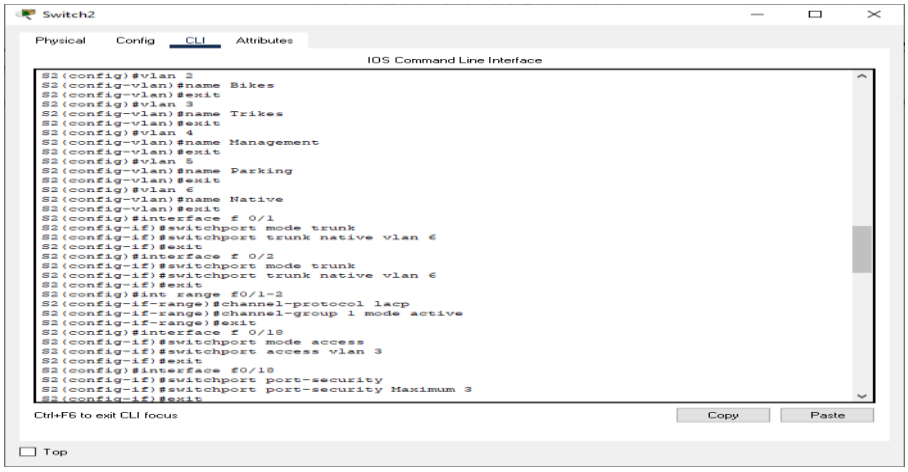
Tabla 7. Configuración estructura de red Switch S2

Tarea	Especificación	Solución
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management	S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#exit S2(config)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#exit S2(config)#vlan 4

	VLAN 5, nombre Parking VLAN 6, nombre Native	S2(config-vlan)#name Management S2(config-vlan)#exit S2(config)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#exit S2(config)#vlan 6 S2(config-vlan)#name Native S2(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2	S2(config)#interface f 0/1 switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config-if)#exit S2(config)#interface f 0/2 switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config-if)#exit
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)#int range f0/1-2 S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#interface port-channel 1 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk Native vlan 6 S2(config-if)#exit
Configurar el puerto de acceso de host para VLAN 3	Interface F0/18	S2(config)#interface f 0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3

		S2(config-if)#exit
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC	S2(config)#interface f0/18 S2(config-if)#switchport port-security S2(config-if)#switchport port-security Maximum 3 S2(config-if)#exit
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S2(config)#int range g0/1-2,f0/3-17,f0/19-24 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 no usar S2(config-if-range)#shutdown

Figura 6. Configuración estructura de red Switch S2 packet tracer



Parte 2: Configurar soporte de host

Paso 1: Configure R1

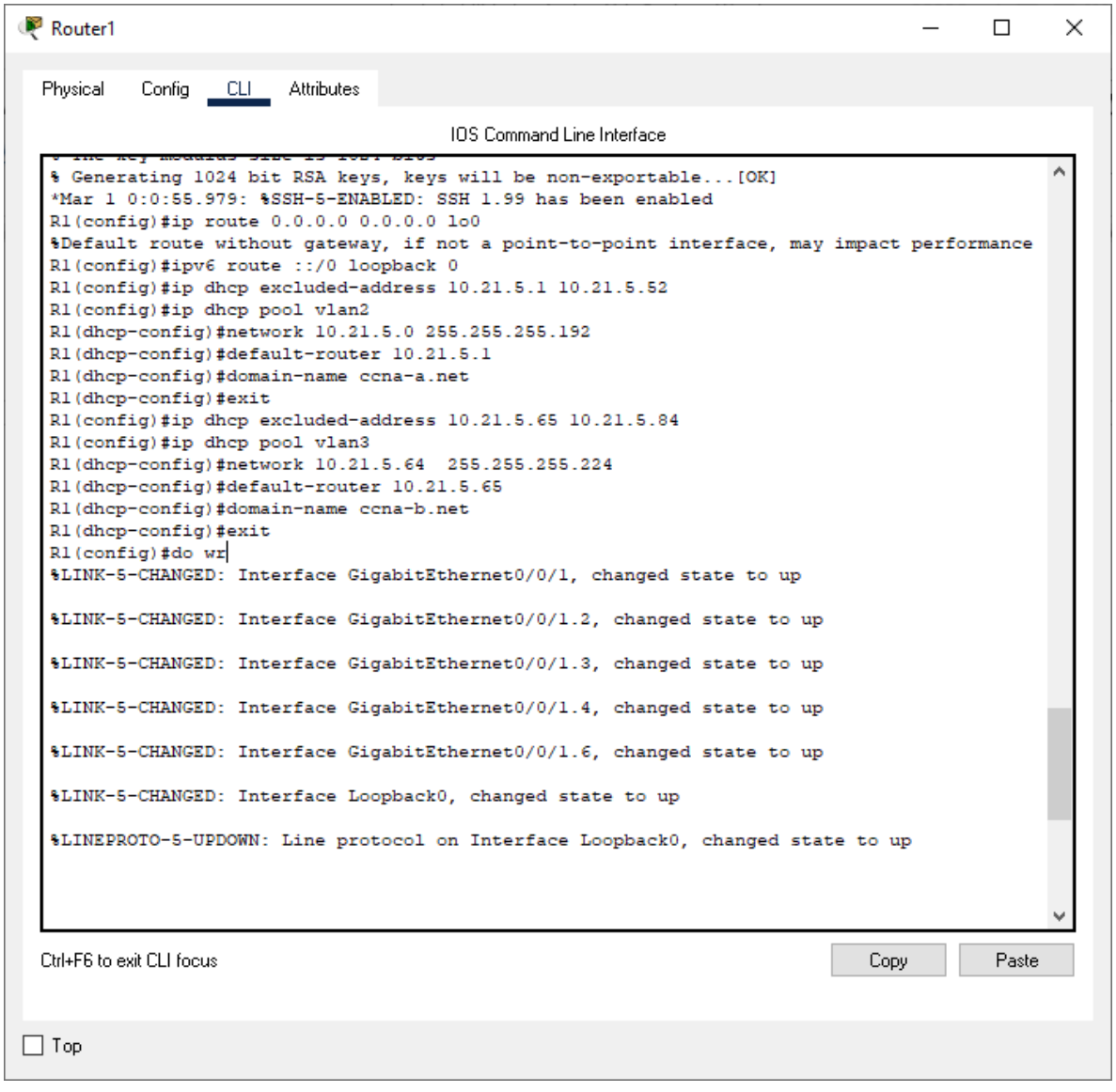
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 8. Configuración soporte del Host

Tarea	Especificación	Solución
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0	R1(config)#ip route 0.0.0.0 0.0.0.0 lo0 R1(config)#ipv6 route ::/0 loopback 0
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 10.21.5.1 10.21.5.52 R1(config)#ip dhcp pool vlan2 R1(dhcp-config)#network 10.21.5.0 255.255.255.192 R1(dhcp-config)#default-router 10.21.5.1 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#exit
Configurar DHCP IPv4 para VLAN 3	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 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

Figura 7. Configuración soporte del host packet tracer



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**.

Tabla 9. Configuración PC-A

Configuración de red de PC-A	
Descripción	PC-A
Dirección física	0001.966C.E899
Dirección IP	10.21.5.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.21.5.1
Gateway predeterminado IPv6	FE80::1

Figura 8.ipconfig all /all PC-A

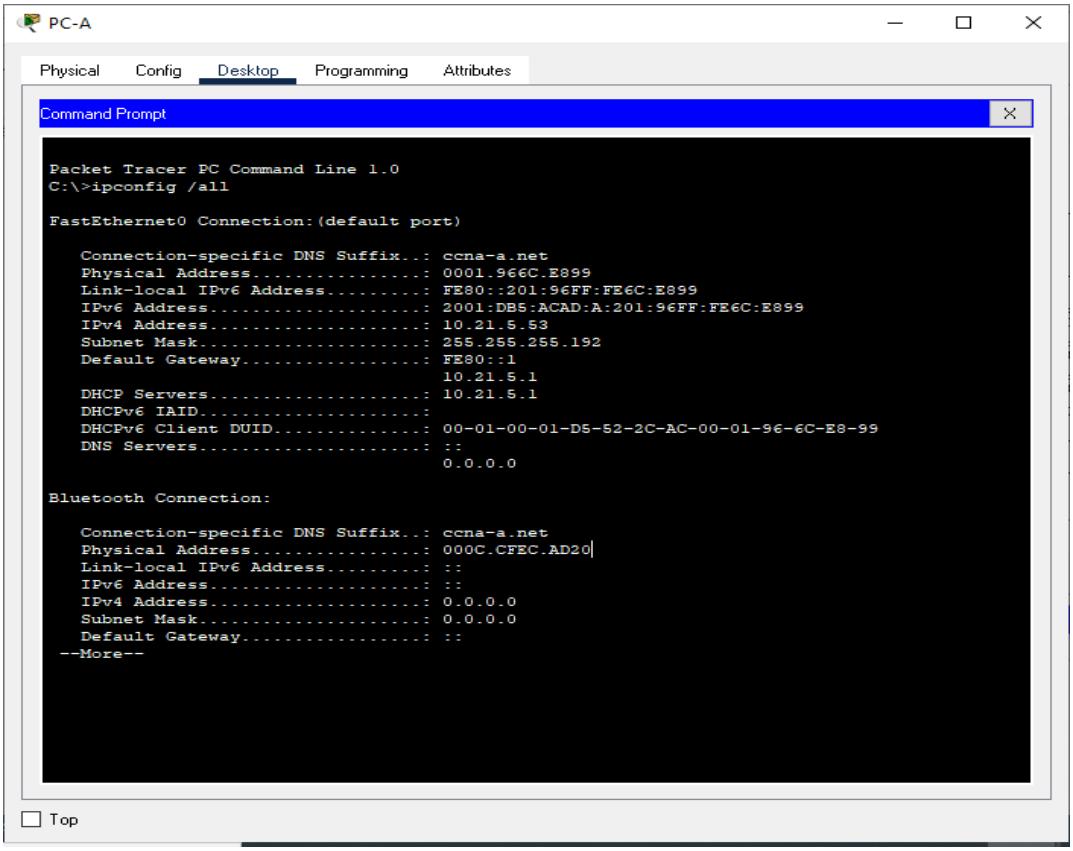


Figura 9. Configuración PC-A packet tracer

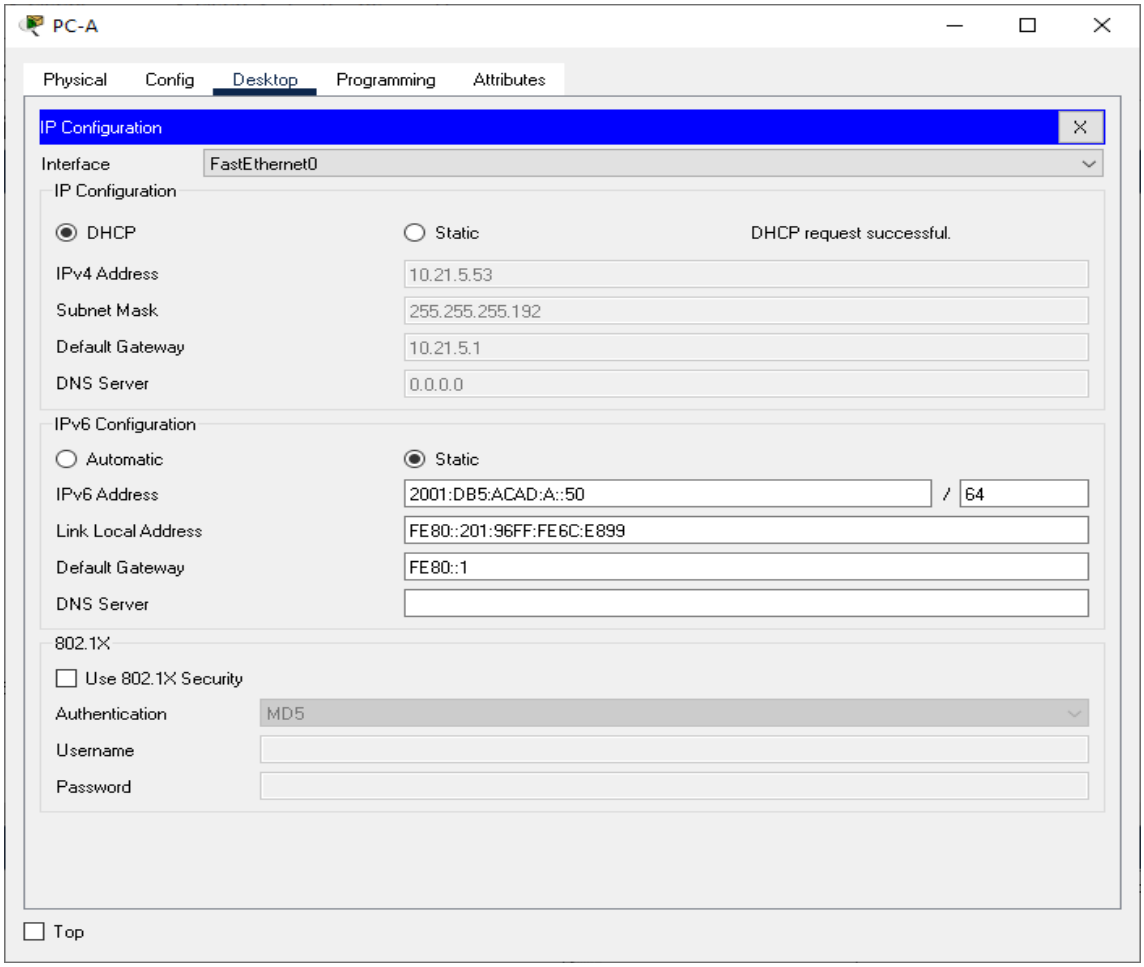


Tabla 10. Configuración PC-B

Configuración de red de PC-B	
Descripción	PC-B
Dirección física	000D.BD2C.3BCC
Dirección IP	10.21.5.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.21.5.65
Gateway predeterminado IPv6	FE80::1

Figura 10.ipconfig all /all PC-B

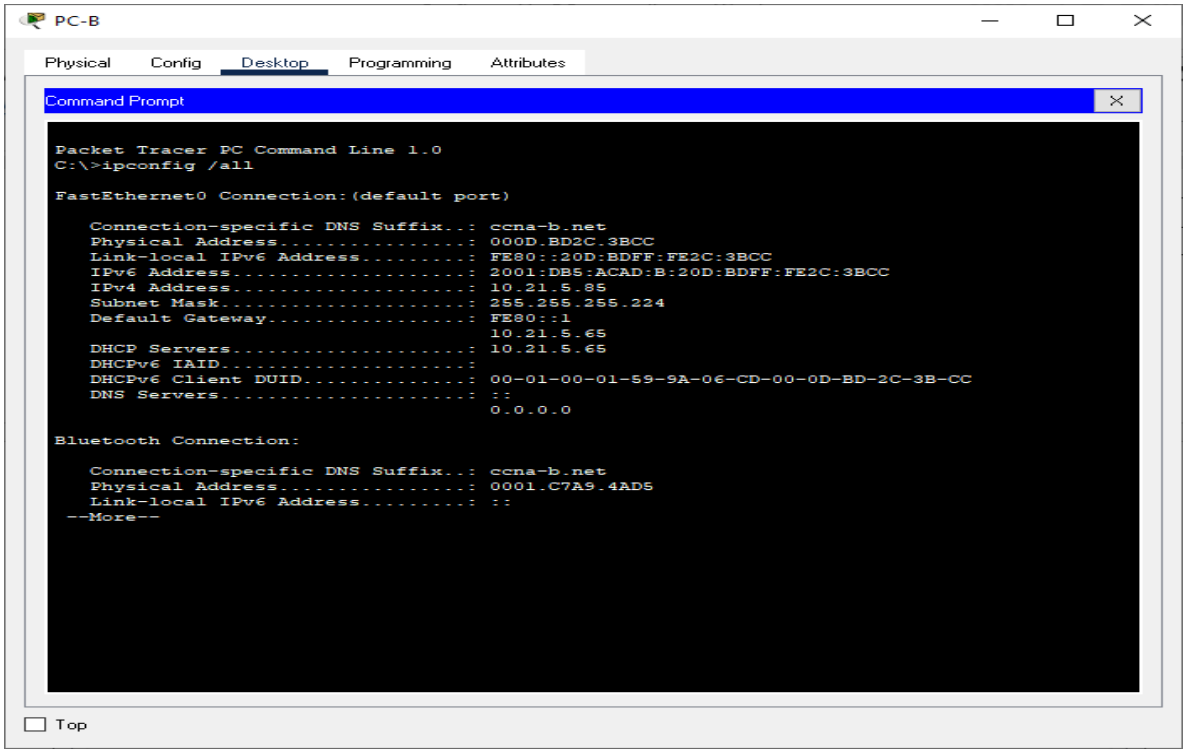


Figura 11. Configuración PC-B packet tracer

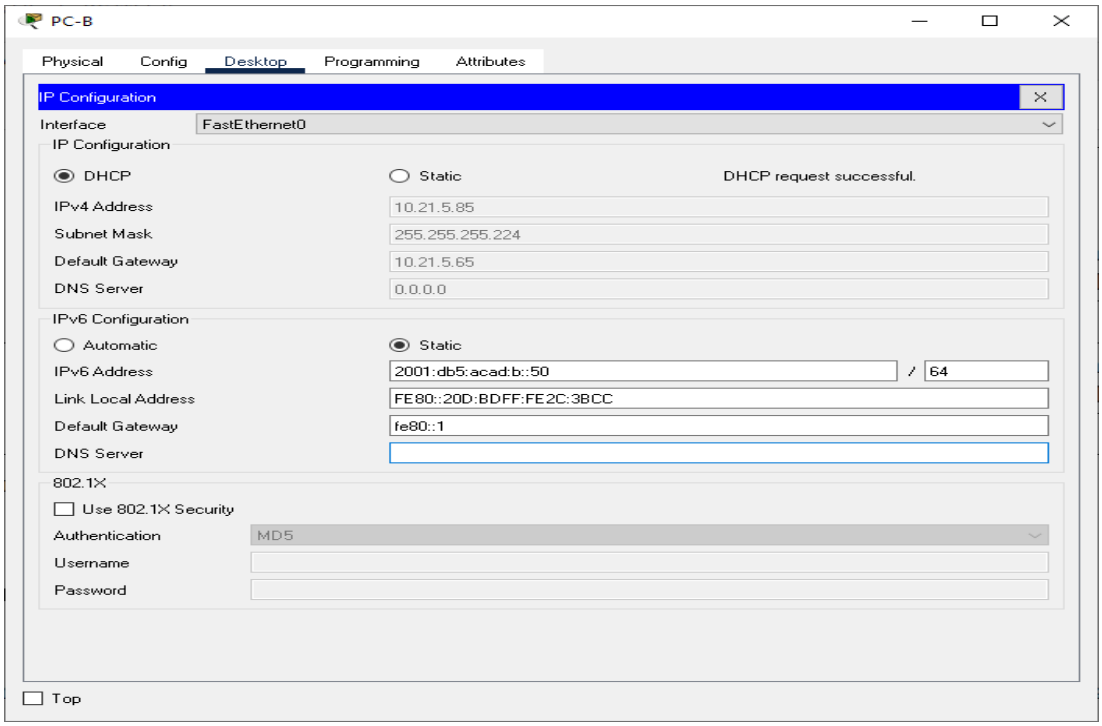
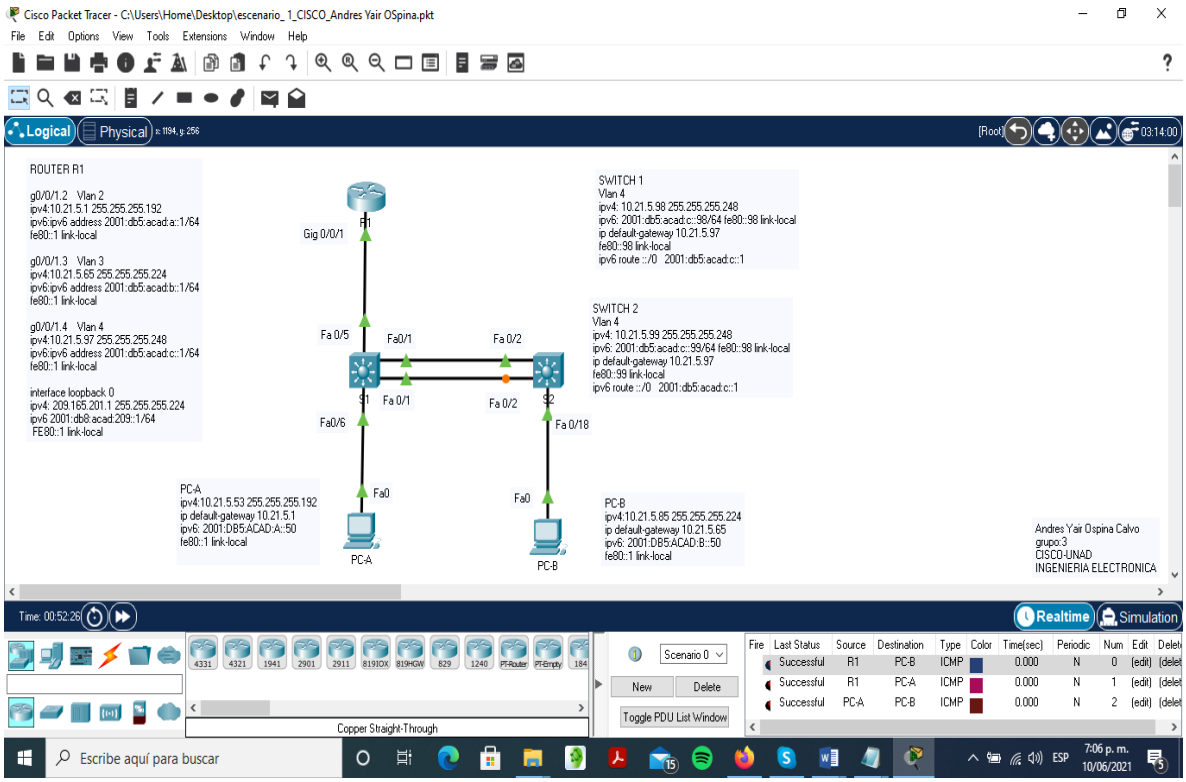


Figura 12. Simulación escenario 1 packet tracer



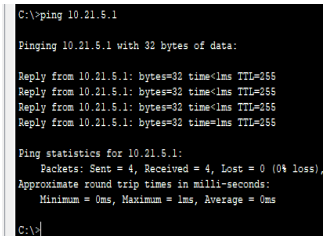
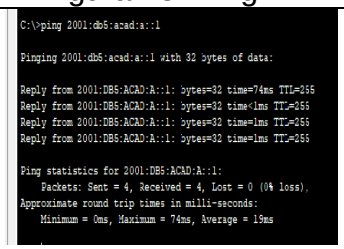
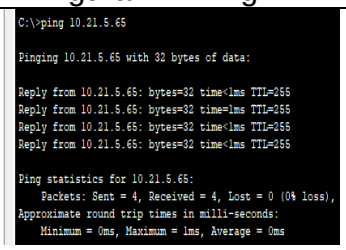
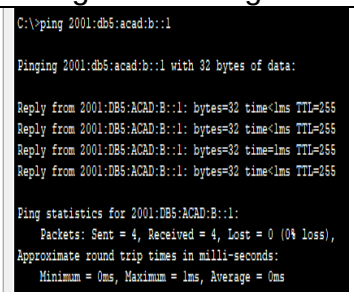
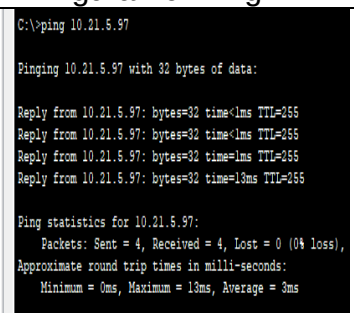
Parte 3: Probar y verificar la conectividad de extremo a extremo

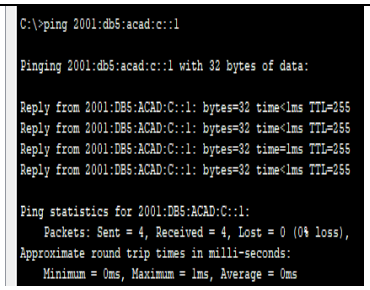
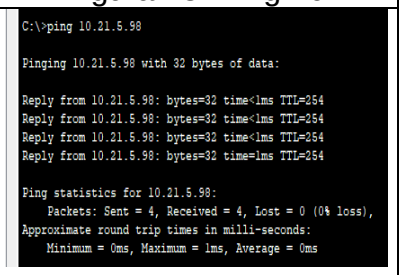
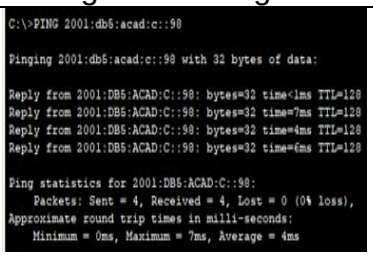
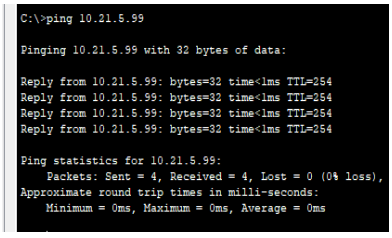
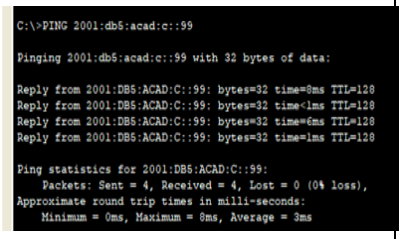
Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

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 11. Prueba de conectividad de extremo a extremo PC-A

desde	A	Internet	Dirección ip	Resultado de ping
PC-A	R1,G0/0/1.2	Dirección	10.21.5.1	 Figura 13. Ping #1
		IPV6	2001:db5:acad:a::1	 Figura 14. Ping #2
	R1, G0/0/1.3	Dirección	10.21.5.65	 Figura 15. Ping #3
		IPV6	2001:db5:acad:b::1	 Figura 16. Ping #4
	R1, G0/0/1.4	Dirección	10.21.5.97	 Figura 17. Ping #5

		IPV6	2001:db5:acad:c::1	 Figura 18. Ping #6
	S1, VLAN 4	Dirección	10.21.5.98	 Figura 19. Ping #7
		IPV6	2001:db5:acad:c::98	 Figura 20. Ping #8
	S2, VLAN 4	Dirección	10.21.5.99	 Figura 21. Ping #9
		IPV6	2001:db5:acad:c::99	 Figura 22. Ping #10

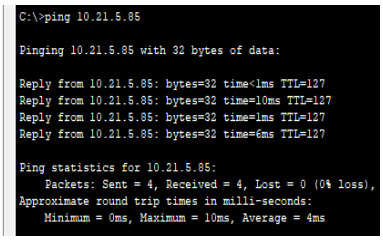
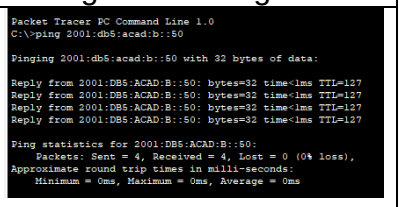
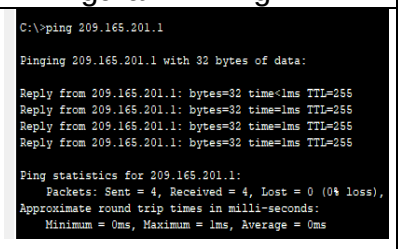
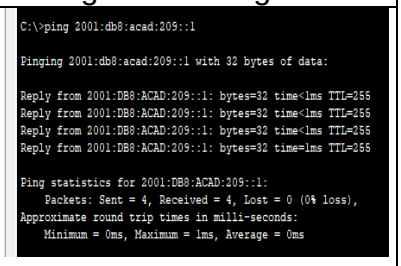
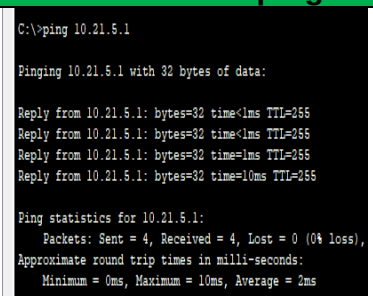
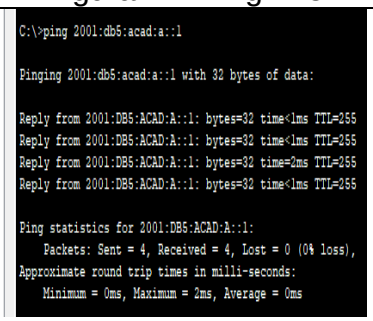
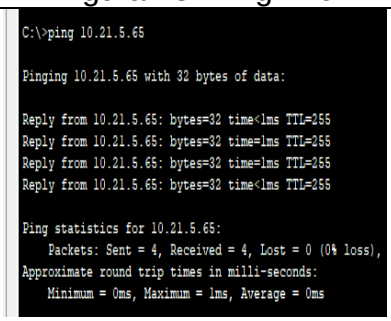
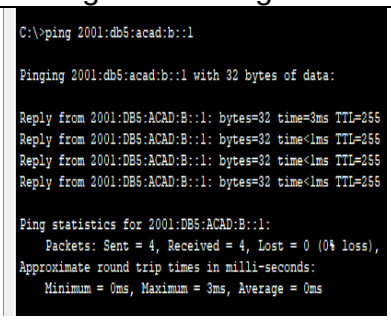
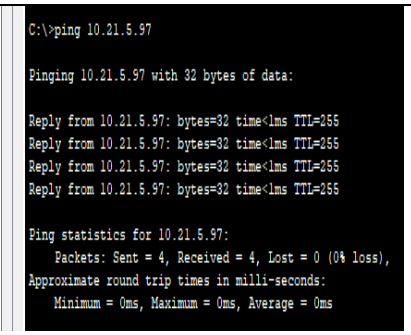
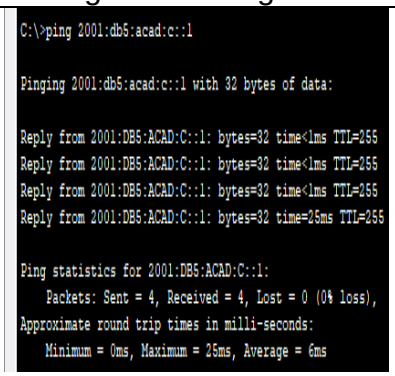
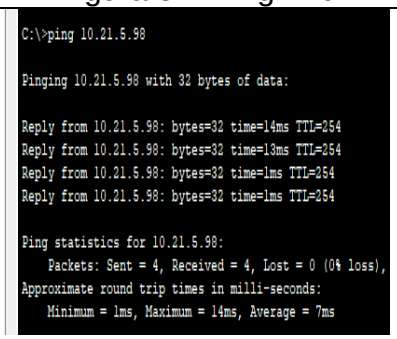
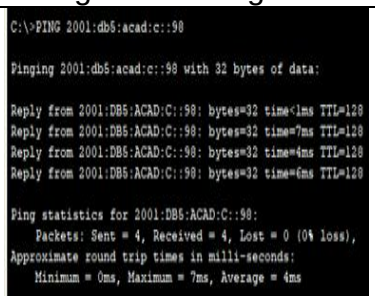
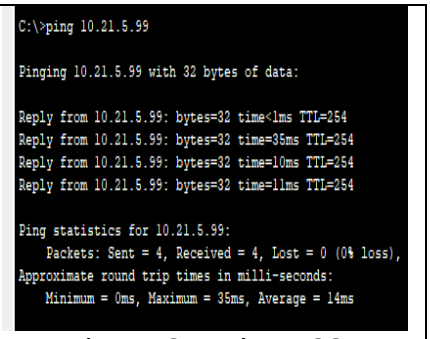
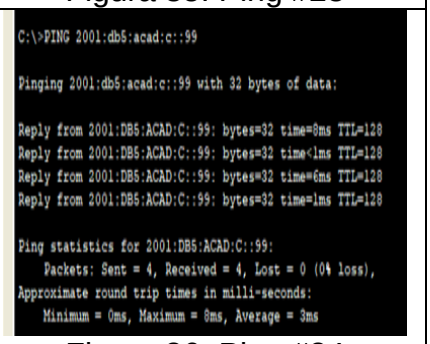
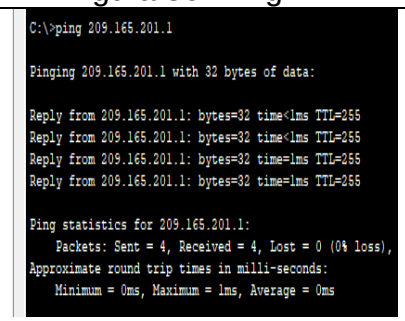
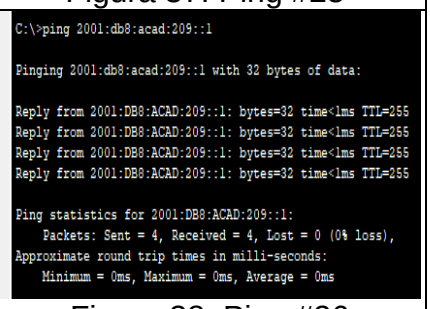
	PC-B	Dirección	10.21.5.85	 Figura 23. Ping #11
		IPV6	2001:db5:acad:b::50	 Figura 24. Ping #12
	R1 Bucle 0	Dirección	209.165.201.1	 Figura 25. Ping #13
		IPV6	2001:db8:acad:209: :1	 Figura 26. Ping #14

Tabla 12. Prueba de conectividad de extremo a extremo PC-B

desde	A	Internet	Dirección ip	Resultado de ping
PC-B	R1, G0/0/1.2	Dirección	10.21.5.1	 Figura 27. Ping #15
		IPV6	2001:db5:acad:a::1	 Figura 28. Ping #16
	R1, G0/0/1.3	Dirección	10.21.5.65	 Figura 29. Ping #17
		IPV6	2001:db5:acad:b::1	 Figura 30. Ping #18

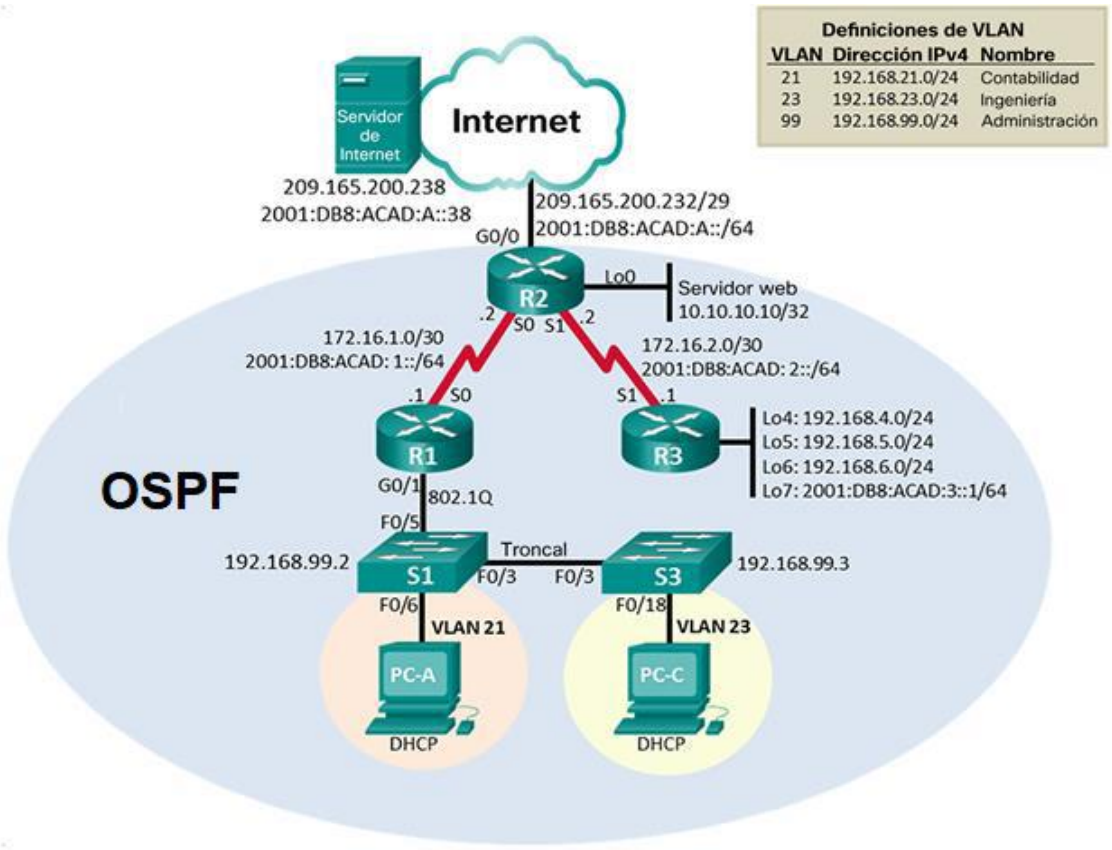
	R1, G0/0/1.4	Dirección	10.21.5.97	 Figura 31. Ping #19
		IPV6	2001:db5:acad:c::1	 Figura 32. Ping #20
	S1, VLAN 4	Dirección	10.21.5.98	 Figura 33. Ping #21
		IPV6	2001:db5:acad:c::98	 Figura 34. Ping #22

	S2, VLAN 4	Dirección	10.21.5.99	 Figura 35. Ping #23
		IPV6	2001:db5:acad:c::99	 Figura 36. Ping #24
	R1 Bucle 0	Dirección	209.165.201.1	 Figura 37. Ping #25
		IPV6	2001:db8:acad:209: :1	 Figura 38. Ping #26

2. escenario 2

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

Figura 39. Topología escenario 2



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

Parte 1: Inicializar dispositivos

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos. Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 13. Inicialización de los dispositivos

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

Paso 1: Configurar la computadora de Internet

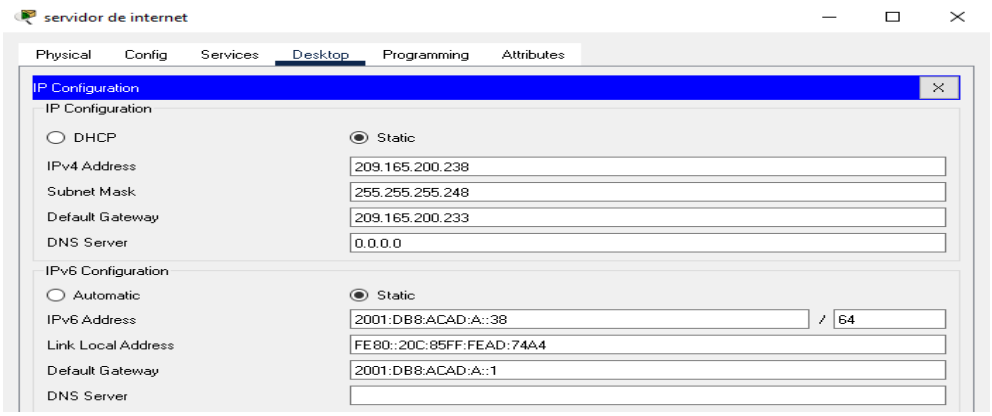
Parte 2: Configurar los parámetros básicos de los dispositivos

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

Tabla 14. Configuración de 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
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Figura 40. Configuración de la computadora de internet packet tracer



Paso 2: Configurar R1

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.

Las tareas de configuración para R1 incluyen las siguientes:

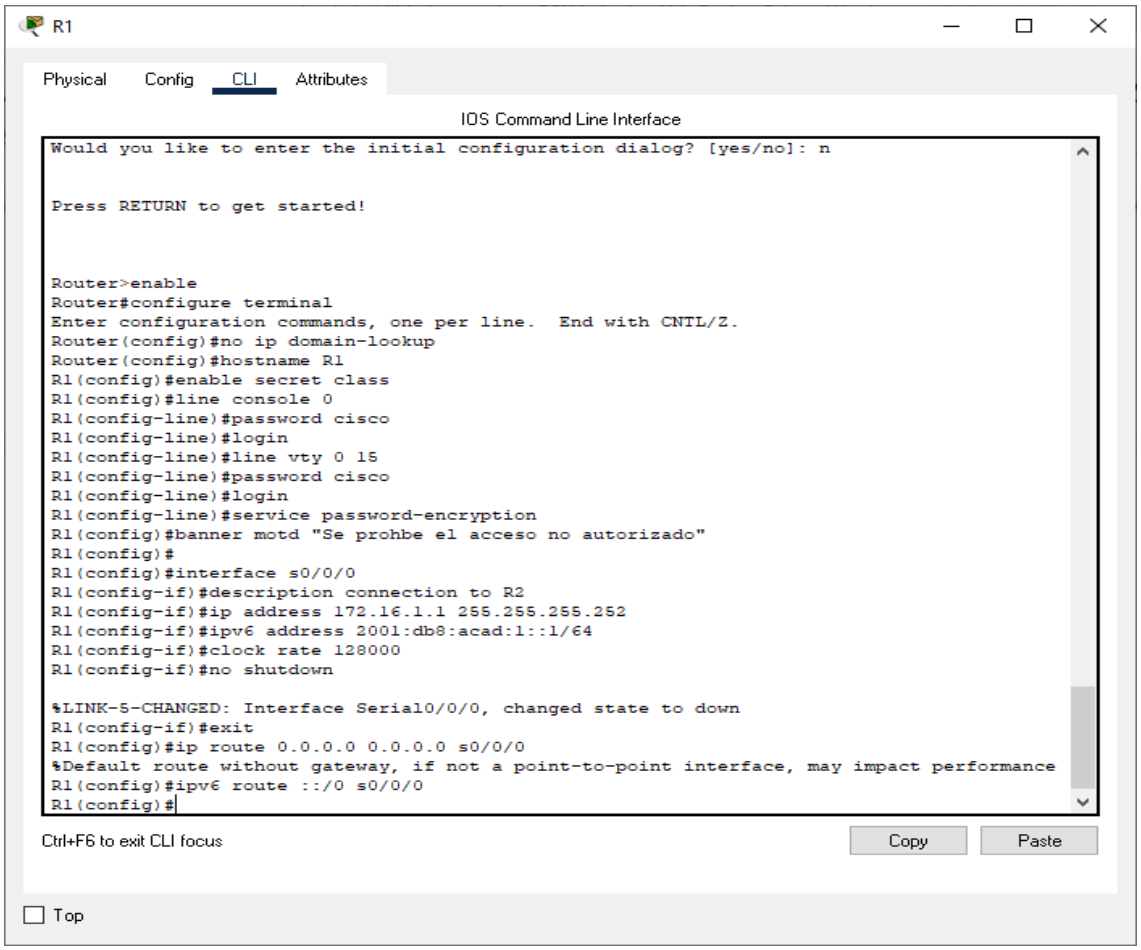
Tabla 15. Configuración router R1 escenario 2

Tarea	Especificación	Solución
Desactivar la búsqueda DNS	N/A	router#enable router#configure terminal router(config)#no ip domain-lookup
Nombre del router	R1	R1(config)#hostname R1
Contraseña de exec privilegiado cifrada	class	R1(config)#enable secret class
Contraseña de acceso a la consola	cisco	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	cisco	R1(config-line)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	N/A	R1(config-line)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.	R1(config)#banner motd "Se prohibe el acceso no autorizado"
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)#interface s0/0/0 R1(config-if)#description connection to R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config-if)#exit

Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Nota: Todavía no configure G0/1.

Figura 41. Configuración router R1 escenario 2 packet tracer



Paso 3: Configurar R2

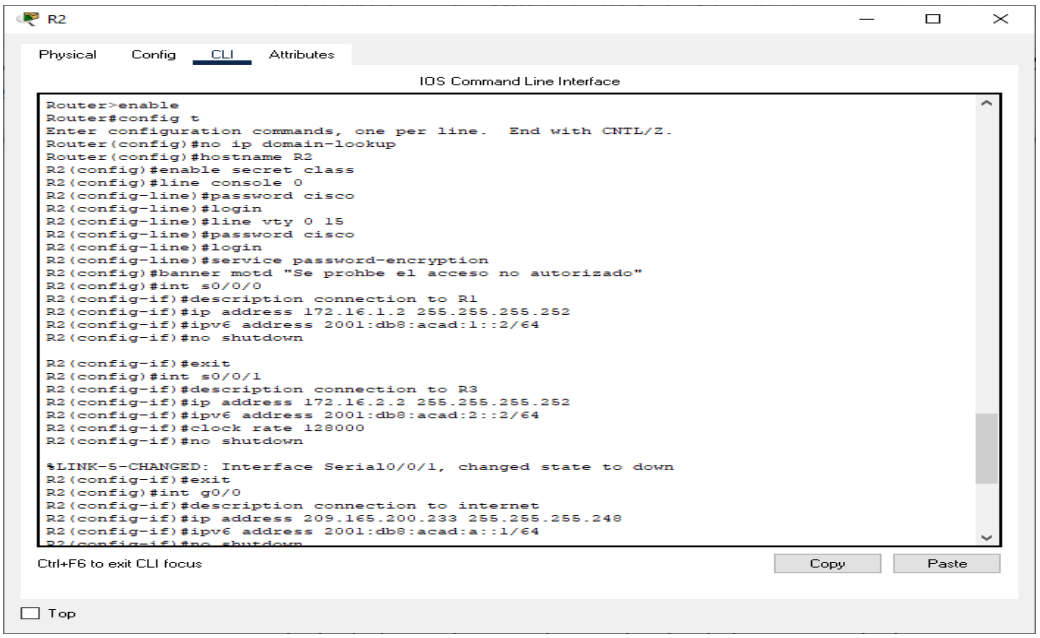
La configuración del R2 incluye las siguientes tareas:

Tabla 16. Configuración router R2 escenario 2

Tarea	Especificación	Solución
Desactivar la búsqueda DNS	N/A	router#enable router#configure terminal router(config)#no ip domain-lookup
Nombre del router	R2	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	class	R2(config)#enable secret class
Contraseña de acceso a la consola	cisco	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	cisco	R2(config-line)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	N/A	R2(config-line)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.	R2(config)#banner motd "Se prohibe el acceso no autorizado"
Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	R2(config)#int s0/0/0 R2(config-if)#description connection to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.	R2(config-if)#exit R2(config)#int s0/0/1 R2(config-if)#description connection to R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown

	Establecer la frecuencia de reloj en 128000. Activar la interfaz	
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz	R2(config)#int g0/0 R2(config-if)#description connection to internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.	R2(config)#int loopback 0 R2(config-if)#description simulated web server R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#exit
Rutas predeterminadas	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

Figura 42. Configuración router R2 escenario 2 packet tracer



Paso 4: Configurar R3

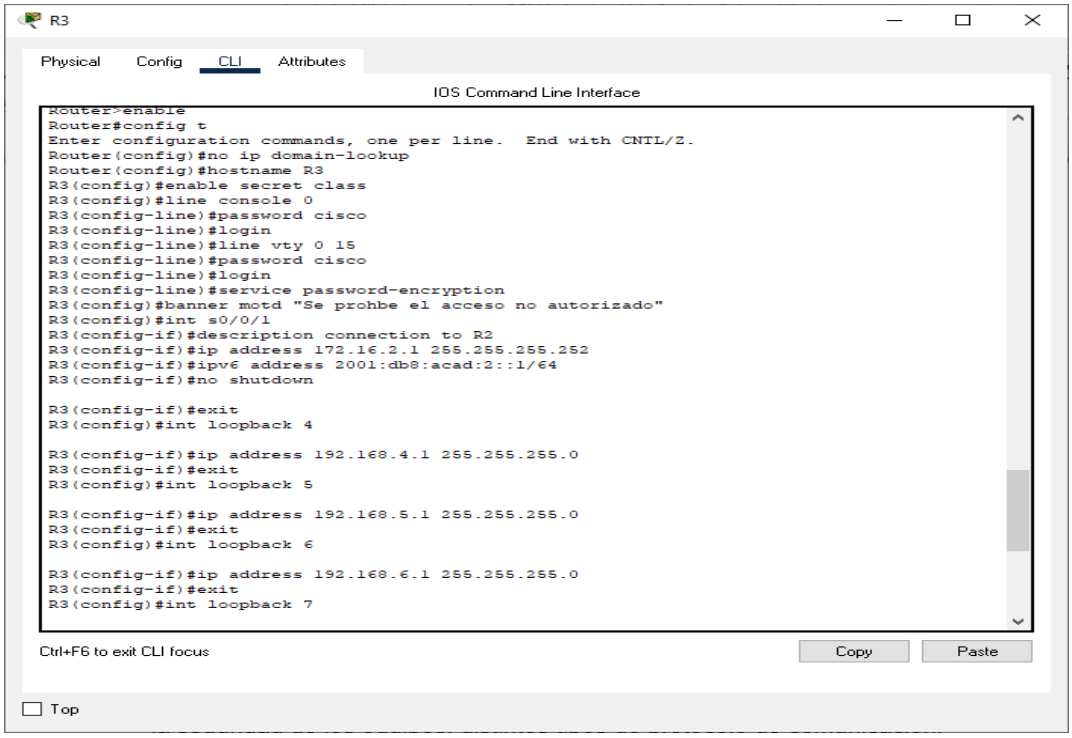
La configuración del R3 incluye las siguientes tareas:

Tabla 17. Configuración router R3 escenario 2

Tarea	Especificación	Solución
Desactivar la búsqueda DNS	N/A	router#enable router#configure terminal router(config)#no ip domain-lookup
Nombre del router	R3	R3(config)#hostname R1
Contraseña de exec privilegiado cifrada	class	R3(config)#enable secret class
Contraseña de acceso a la consola	cisco	R3(config)#line console 0 R3(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	cisco	R3(config-line)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	N/A	R3(config-line)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.	R3(config)#banner motd "Se prohibe el acceso no autorizado"
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	R3(config)#int s0/0/1 R3(config-if)#description connection to R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera	R3(config)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0

	dirección disponible en la subred.	
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.	R3(config)#int loopback 7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64 R3(config-if)#exit
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/1 Configurar una ruta IPv6 predeterminada de S0/0/1	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Figura 43. Configuración router R3 escenario 2 packet tracer



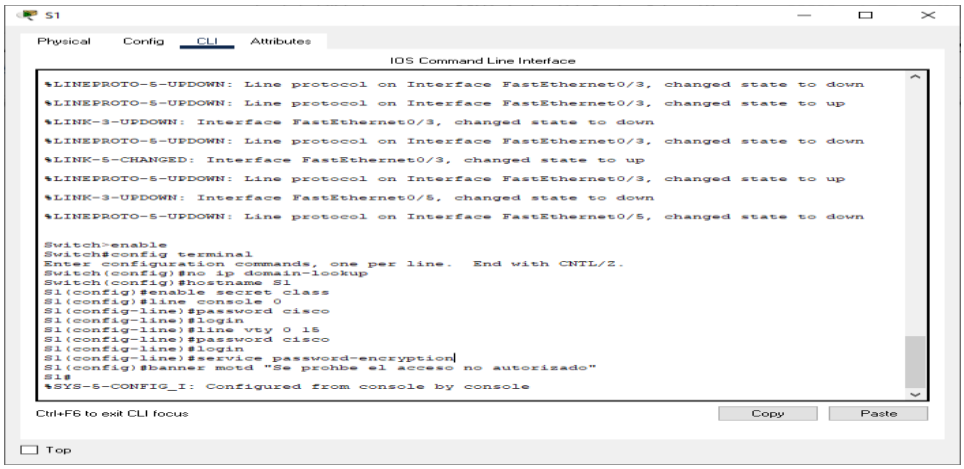
Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 18. Configuración switch S1 escenario 2

Tarea	Especificación	Solución
Desactivar la búsqueda DNS	N/A	Switch>enable Switch#config terminal Switch(config)#no ip domain-lookup
Nombre del router	S1	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	class	S1(config)#enable secret class
Contraseña de acceso a la consola	cisco	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	cisco	S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	N/A	S1(config-line)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.	S1(config)#banner motd "Se prohbe el acceso no autorizado"

Figura 44. Configuracion switch S1 escenario 2 packet tracer



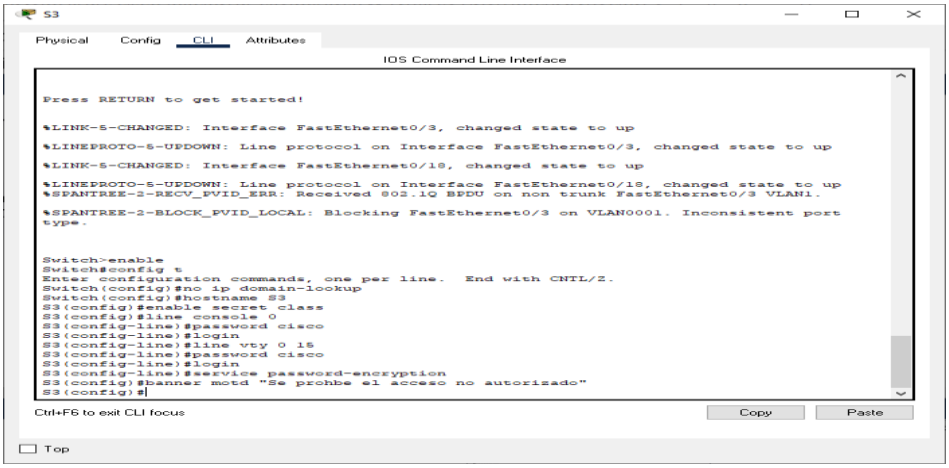
Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 19. Configuración switch S3 escenario 2

Tarea	Especificación	Solución
Desactivar la búsqueda DNS	N/A	Switch>enable Switch#config terminal Switch(config)#no ip domain-lookup
Nombre del router	S3	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	class	S3(config)#enable secret class
Contraseña de acceso a la consola	cisco	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	cisco	S3(config-line)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	N/A	S3(config-line)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.	S3(config)#banner motd "Se prohbe el acceso no autorizado"

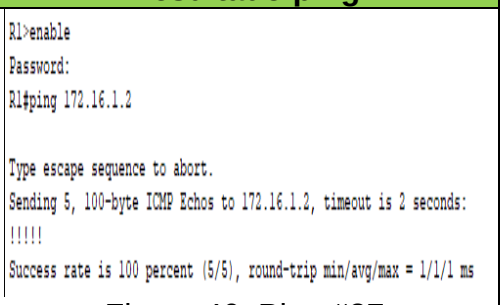
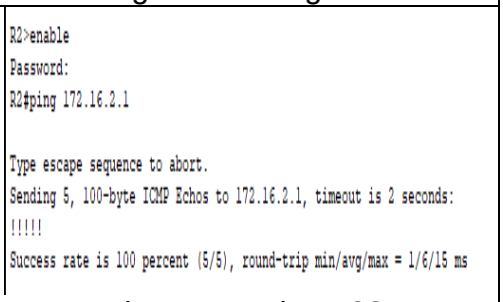
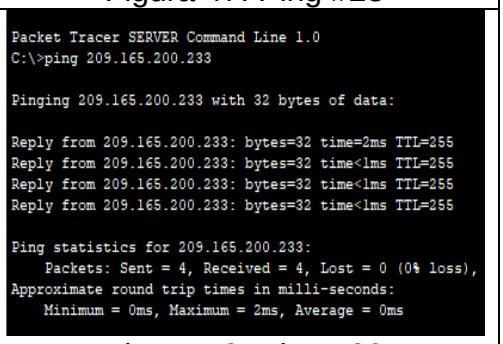
Figura 45. Configuracion switch S3 escenario 2 packet tracer



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 20. Verificación de conectividad #1

Desde	A	Dirección IP	Resultado ping
R1	R2, S0/0/0	172.16.1.2	 Figura 46. Ping #27
R2	R3, S0/0/1	172.16.2.1	 Figura 47. Ping #28
Pc de internet	Gateway predeterminado	209.165.200.233	 Figura 48. Ping #29

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

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

Paso 1: Configurar S1

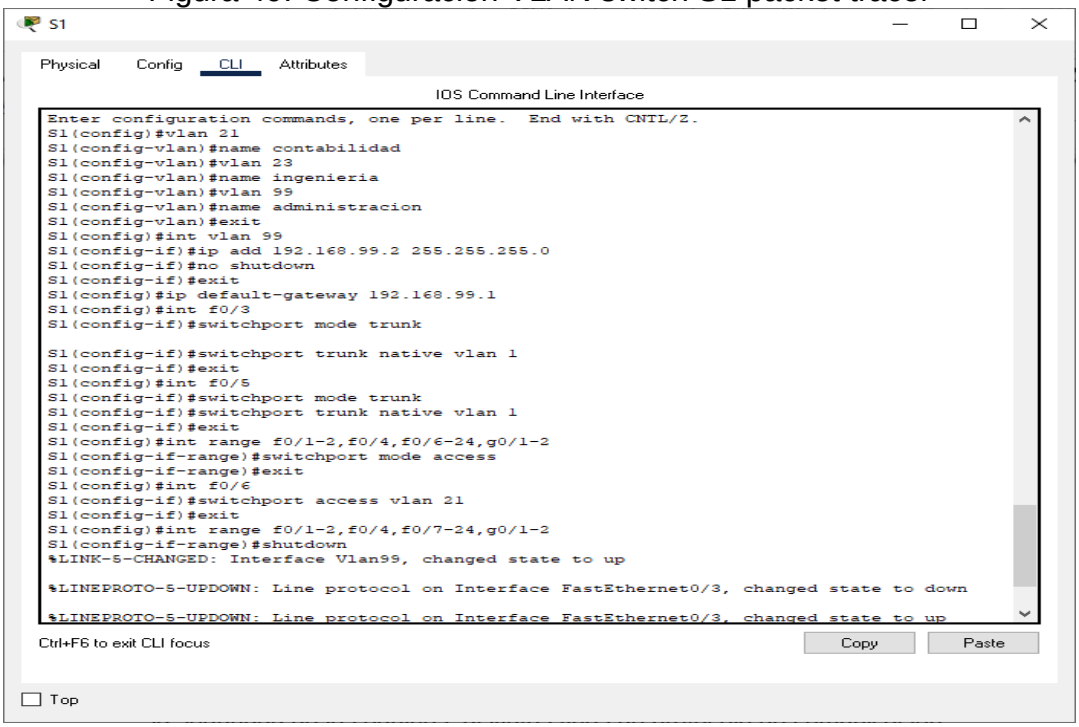
La configuración del S1 incluye las siguientes tareas:

Tabla 21. Configuración VLAN switch S1

Elemento o tarea de configuración	Descripción	Solución
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican	S1(config)#vlan 21 S1(config-vlan)#name contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name administracion S1(config-vlan)#exit S1(config)#int vlan 99
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología	S1(config-if)#ip add 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#exit
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa	S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa	S1(config)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit

Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range.	S1(config)#int range f0/1-2,f0/4,f0/6-24,g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#exit
Asignar F0/6 a la VLAN 21	N/A	S1(config)#int f0/6 S1(config-if)#switchport access vlan 21 S1(config-if)#exit
Apagar todos los puertos sin usar	N/A	S1(config)#int range f0/1-2,f0/4,f0/7-24,g0/1-2 S1(config-if-range)#shutdown

Figura 49. Configuracion VLAN switch S1 packet tracer



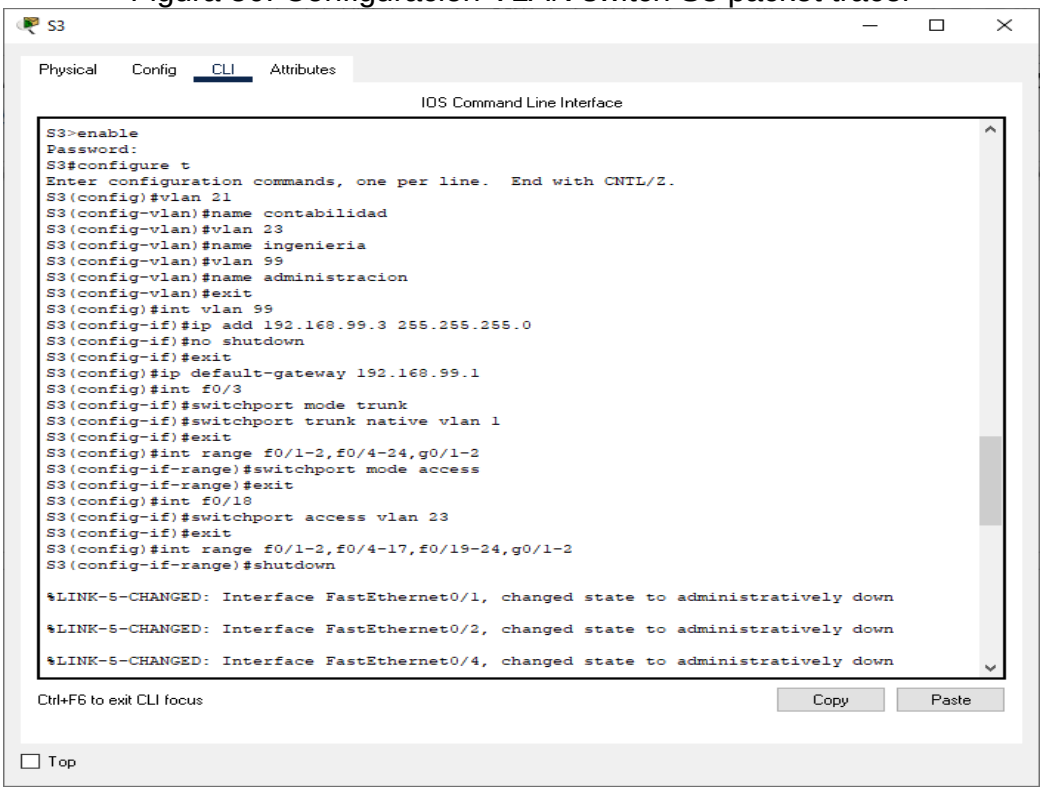
Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 22. Configuración VLAN switch S3

Elemento o tarea de configuración	Descripción	Solución
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican	S3(config)#vlan 21 S3(config-vlan)#name contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name administracion S3(config-vlan)#exit S3(config)#int vlan 99
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S2 en el diagrama de topología	S3(config-if)#ip add 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#exit
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range	S3(config)#int range f0/1-2,f0/4-24,g0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#exit
Asignar F0/18 a la VLAN 23	N/A	S3(config)#int f0/18 S3(config-if)#switchport access vlan 23 S3(config-if)#exit
Apagar todos los puertos sin usar	N/A	S3(config)#int range f0/1-2,f0/4-17,f0/19-24,g0/1-2 S3(config-if-range)#shutdown

Figura 50. Configuracion VLAN switch S3 packet tracer



Paso 3: Configurar R1

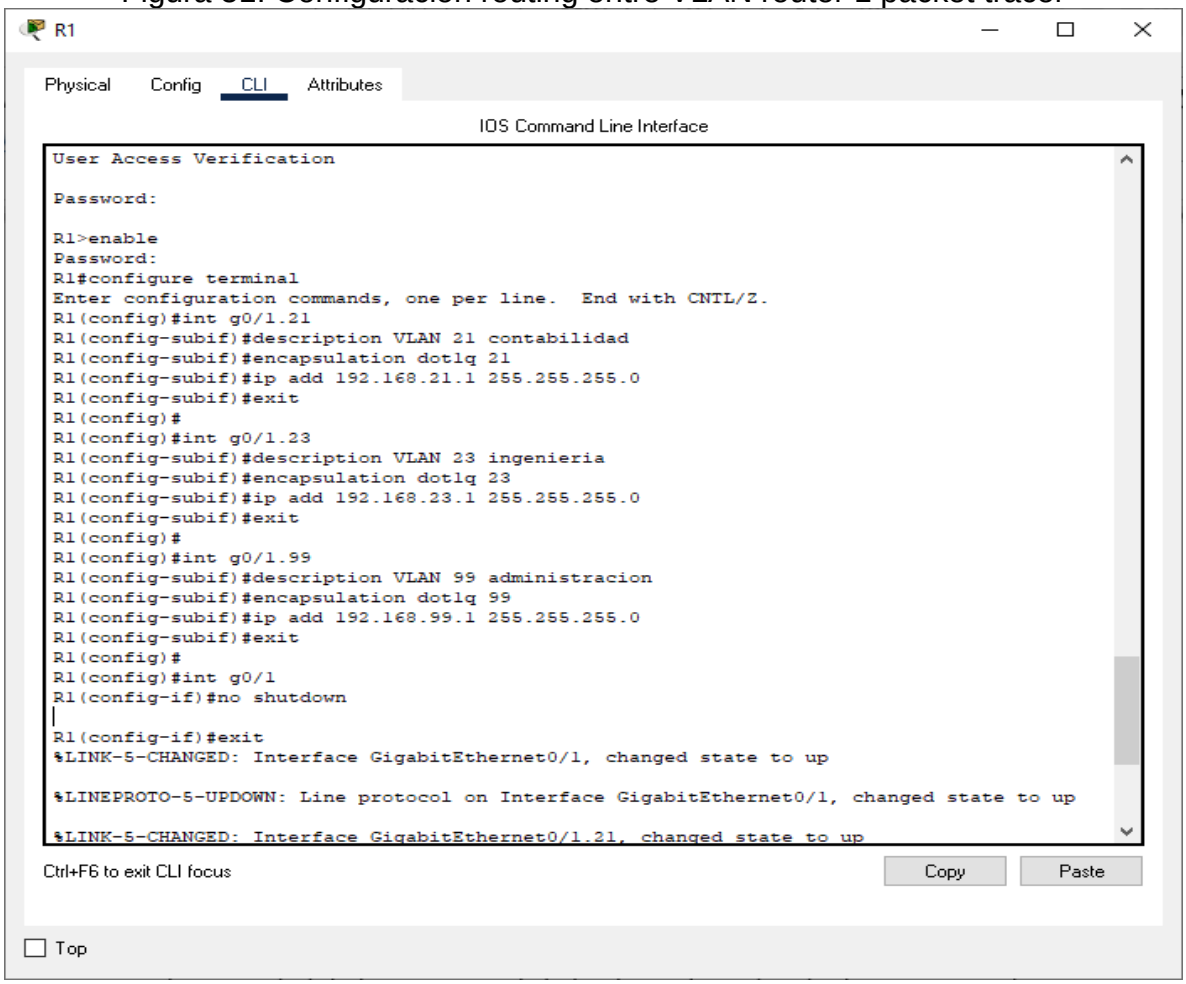
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 23. Configuración routing entre VLAN router R1

Elemento o tarea de configuración	Especificacion	Solucion
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz	R1(config)#int g0/1.21 R1(config-subif)#description VLAN 21 contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip add 192.168.21.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23	R1(config)#int g0/1.23 R1(config-subif)#description VLAN 23 ingenieria R1(config-subif)#encapsulation dot1q 23

	Asignar la primera dirección disponible a esta interfaz	R1(config-subif)#ip add 192.168.23.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz	R1(config)#int g0/1.99 R1(config-subif)#description VLAN 99 administracion R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip add 192.168.99.1 255.255.255.0 R1(config-subif)#exit
Activar la interfaz G0/1	N/A	R1(config)#int g0/1 R1(config-if)#no shutdown

Figura 51. Configuracion routing entre VLAN router 1 packet tracer



Paso 4: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los switches y el R1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 24. Verificación de conectividad #2

Desde	A	Dirección IP	Resultado ping
S1	R1, dirección VLAN 99	192.168.99.1	S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms Figura 52. Ping#30
S3	R1, dirección VLAN 99	192.168.99.1	S3#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms Figura 53. Ping#31
S1	R1, dirección VLAN 21	192.168.21.1	S1#ping 192.168.21.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms Figura 54. Ping#32
S3	R1, dirección VLAN 23	192.168.23.1	S3#ping 192.168.23.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms Figura 55. Ping#33

Parte 4: Configurar el protocolo de routing dinámico OSPF

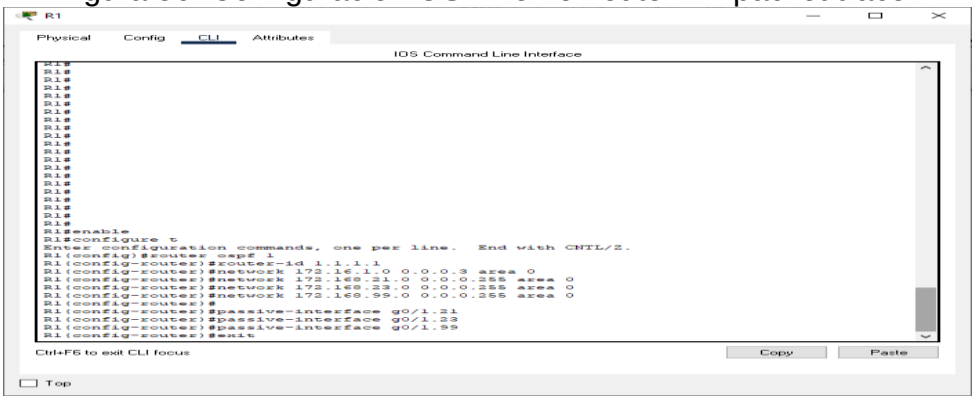
Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 25. Configuración OSPF en el router R1

Elemento o tarea de configuración	descripción	solución
Configurar OSPF área 0	N/A	R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.	R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 172.168.21.0 0.0.0.255 area 0 R1(config-router)#network 172.168.23.0 0.0.0.255 area 0 R1(config-router)#network 172.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	N/A	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99 R1(config-router)#exit
Desactive la sumarización automática	N/A	R1(config)#no auto-summary

Figura 56. Configuración OSPF en el router R1 packet tracer



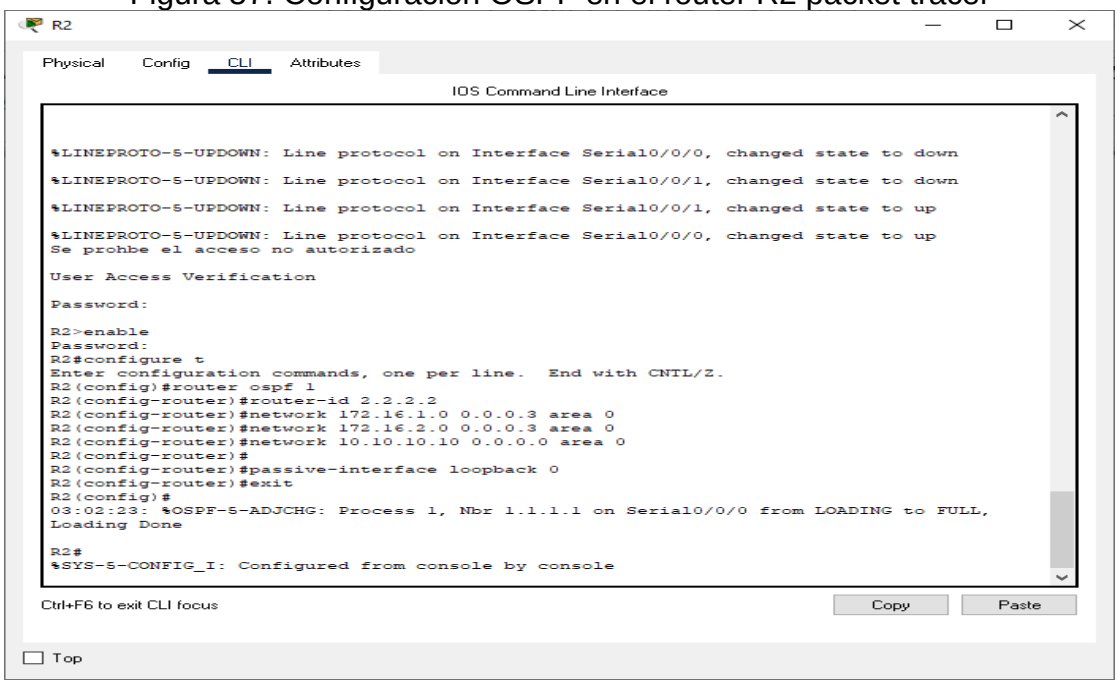
Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 26. Configuración OSPF en el router R2

Elemento o tarea de configuración	descripción	solución
Configurar OSPF área 0	N/A	R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.	R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 10.10.10.10 0.0.0.0 area 0
Establecer todas las interfaces LAN como pasivas	N/A	R2(config-router)#passive-interface loopback 0 R2(config-router)#exit
Desactive la sumarización automática	N/A	R2(config)#no auto-summary

Figura 57. Configuración OSPF en el router R2 packet tracer



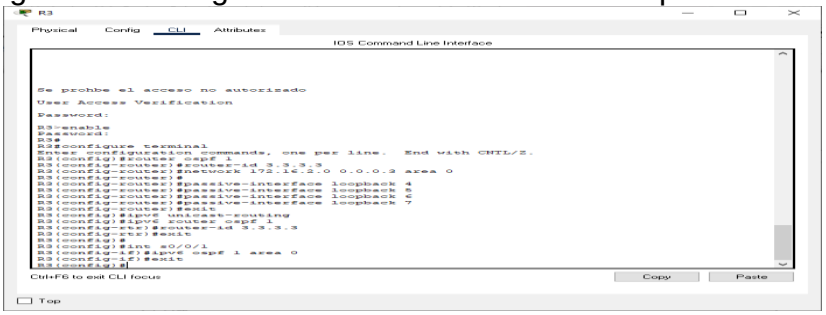
Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 27. Configuración OSPF en el router R3

Elemento o tarea de configuración	descripción	solución
Configurar OSPF área 0	N/A	R3(config)#router ospf 1 R3(config-router)#router-id 3.3.3.3
Anunciar las redes IPV4 conectadas directamente	N/A	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config)#ipv6 unicast-routing R3(config)#ipv6 router ospf 1 R3(config-rtr)#router-id 3.3.3.3 R3(config-rtr)#exit R3(config)#int s0/0/1 R3(config-if)#ipv6 ospf 1 area 0 R3(config-if)#exit
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	N/A	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6 R3(config-router)#passive-interface loopback 7
Desactive la sumarización automática	N/A	R2(config)#no auto-summary

Figura 58. Configuración OSPF en el router R3 packet tracer



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 28. Comandos OSPF

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	R1#show ip protocols
¿Qué comando muestra solo las rutas OSPF?	R1#show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R1#show ip ospf interface

Parte 5: Implementar DHCP y NAT para IPv4

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

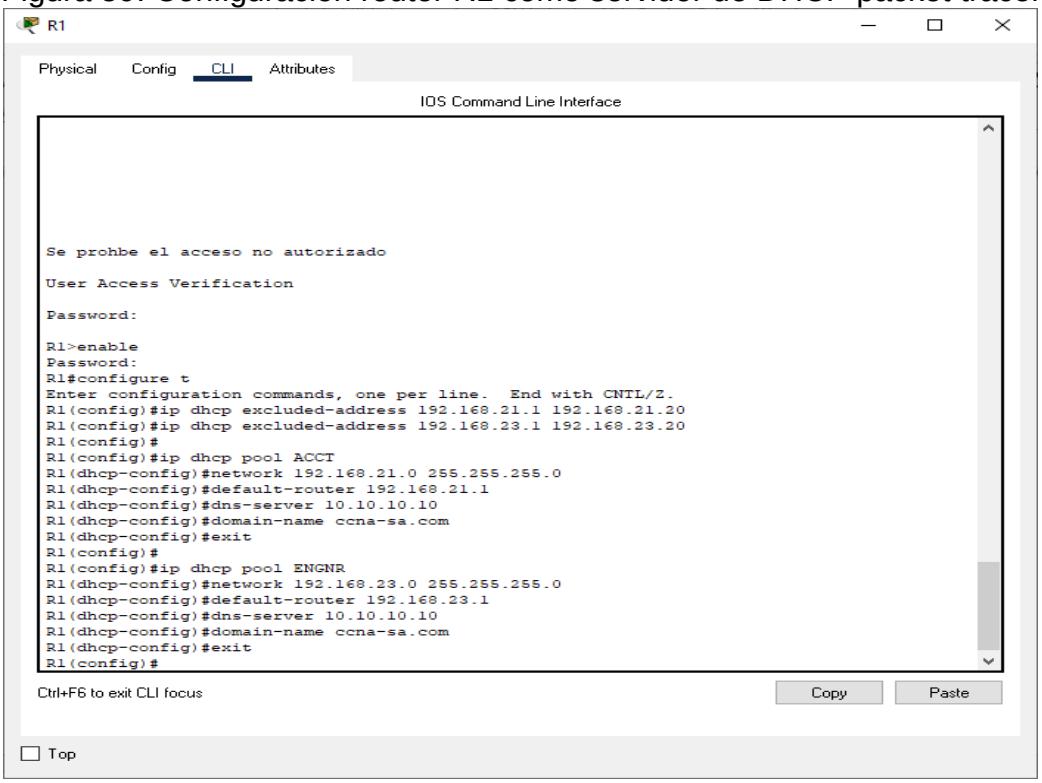
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 29. Configuración router R1 como servidor de DHCP

Elemento o tarea de configuración	Especificación	Solución
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	N/A	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	N/A	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10

		R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#exit
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)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#exit

Figura 59. Configuración router R1 como servidor de DHCP packet tracer



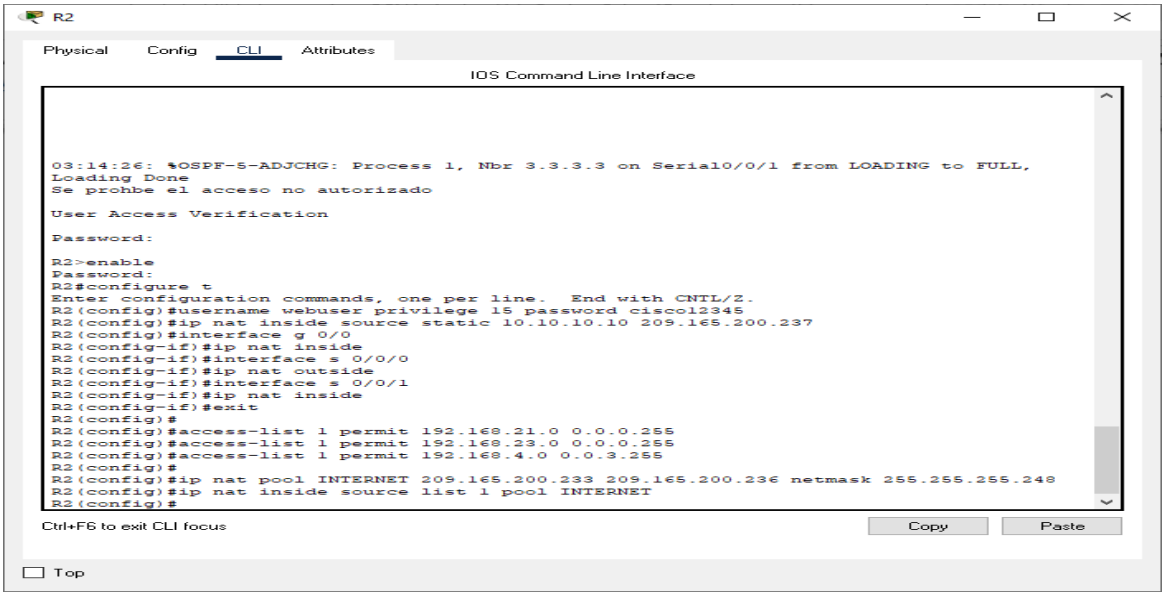
Paso 2: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 30. Configuración NAT estática y dinámica en router R2

Elemento o tarea de configuración	Especificación	Solución
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: 15	R2(config)#username webuser privilege 15 password cisco12345
Habilitar el servicio del servidor HTTP	N/A	Packet tracer no compatible con comandos HTTP
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	N/A	Packet tracer no compatible con comandos HTTP
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	N/A	R2(config)#interface g 0/0 R2(config-if)#ip nat inside R2(config-if)#interface s 0/0/0 R2(config-if)#ip nat outside R2(config-if)#interface s 0/0/1 R2(config-if)#ip nat inside R2(config-if)#exit
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228**	R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.24
Definir la traducción de NAT dinámica	N/A	R2(config)#ip nat inside source list 1 pool INTERNET

Figura 60. Configuración NAT estatica y dinámica en router R2 packet tracer



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 31. Verificación protocolo DHCP

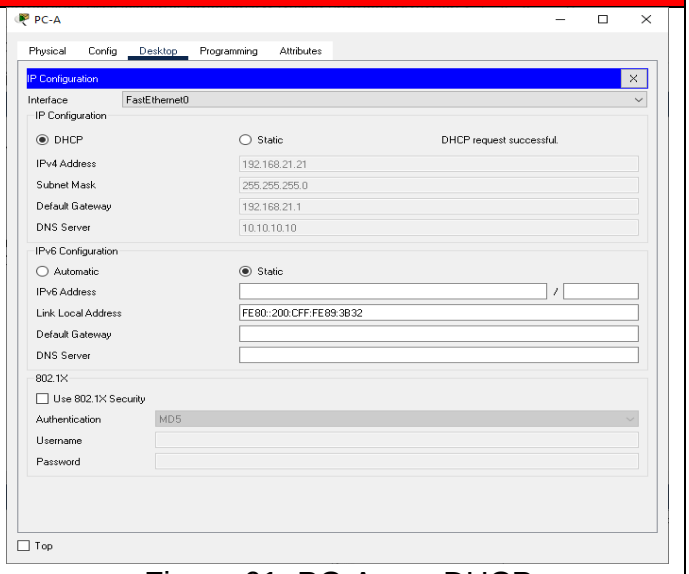
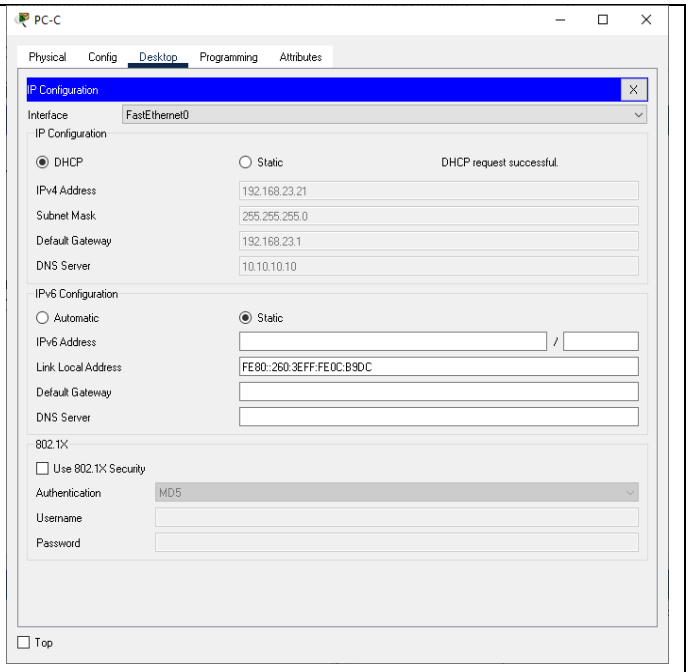
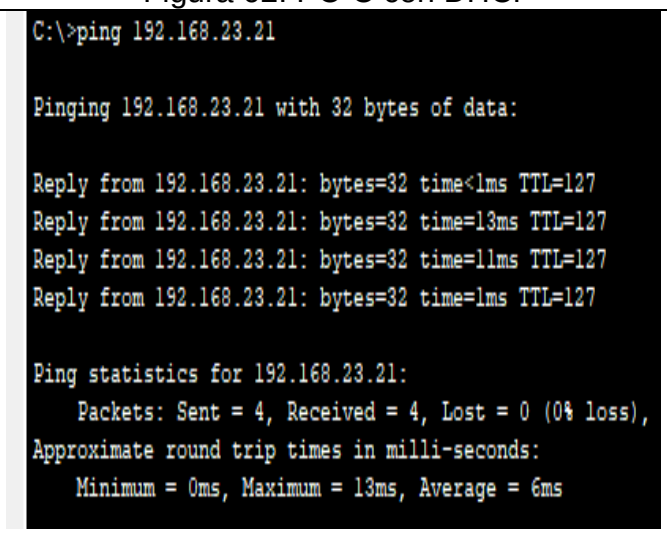
Prueba	Resultado
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	

Figura 61. PC-A con DHCP

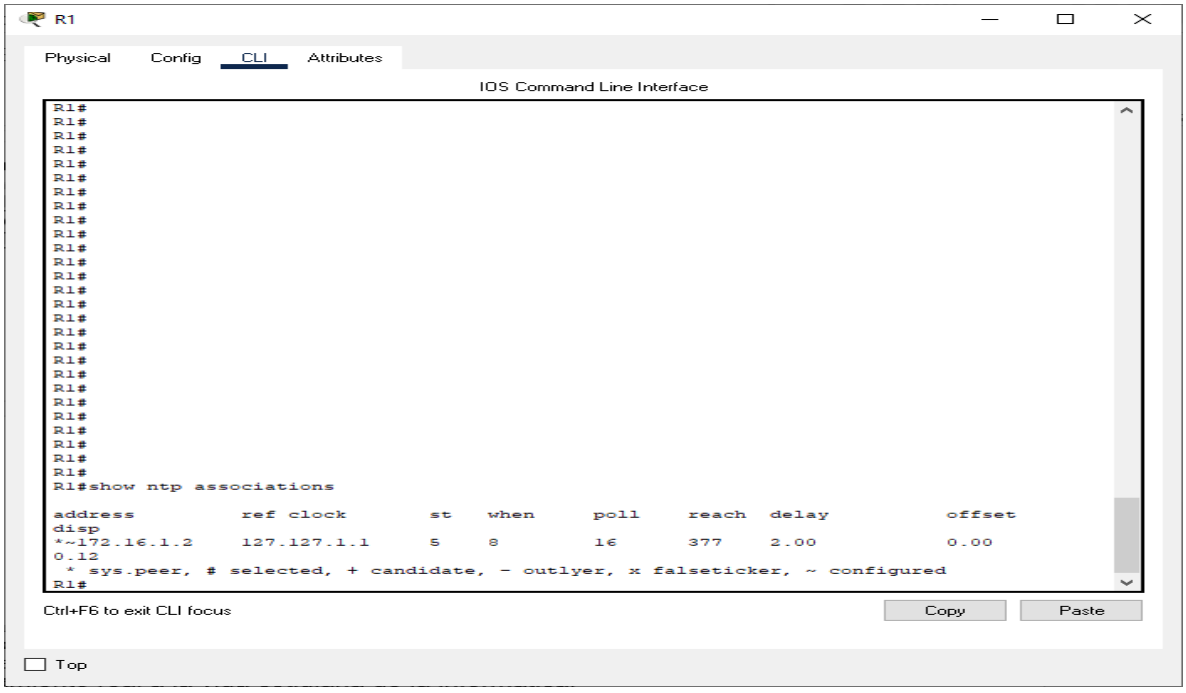
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	 Figura 62. PC-C con DHCP
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	 Figura 63. Ping de PC-A a PC-C
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	(como el comando correspondiente al HTTP no es compatible con packet tracer no es posible hacer esta comprobación).

Parte 6: Configurar NTP

Tabla 32. Configuración NTP

Elemento o tarea de configuración	Especificación	Solución
Ajuste la fecha y hora en R2.	**5 de julio de 2021, 15.34**	R2#clock set 11:05:00 3 july 2021 R2#show clock 11:5:7.656 UTC Sat Jul 3 2021
Configure R2 como un maestro NTP.	Nivel de estrato: 5	R2#configure terminal R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Servidor: R2	R1#configure terminal R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	N/A	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	N/A	R1#show ntp associations

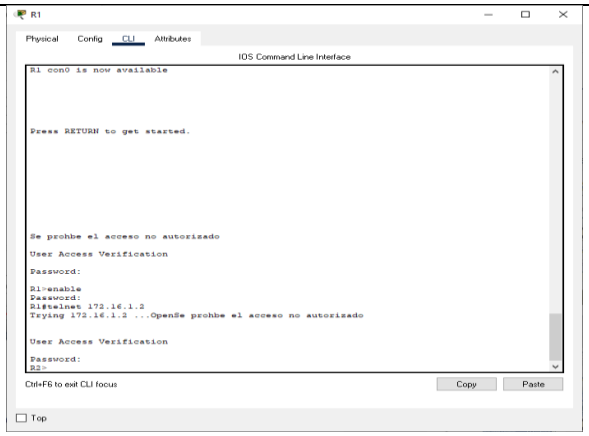
Figura 64. Verificación configuración NTP R1 packet tracer



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

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

Tabla 33. Restricción acceso a líneas VTY en router R2

Elemento o tarea de configuración	Especificación	Solución
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT**	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY		R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY		R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera		 Figura.65 telnet permitido de R1 a R2

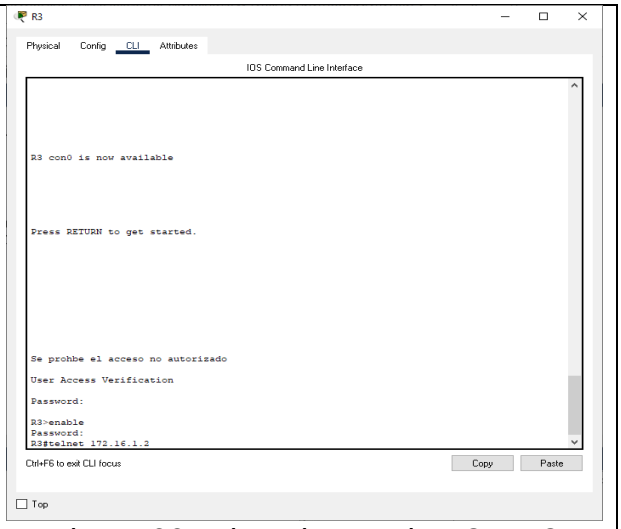


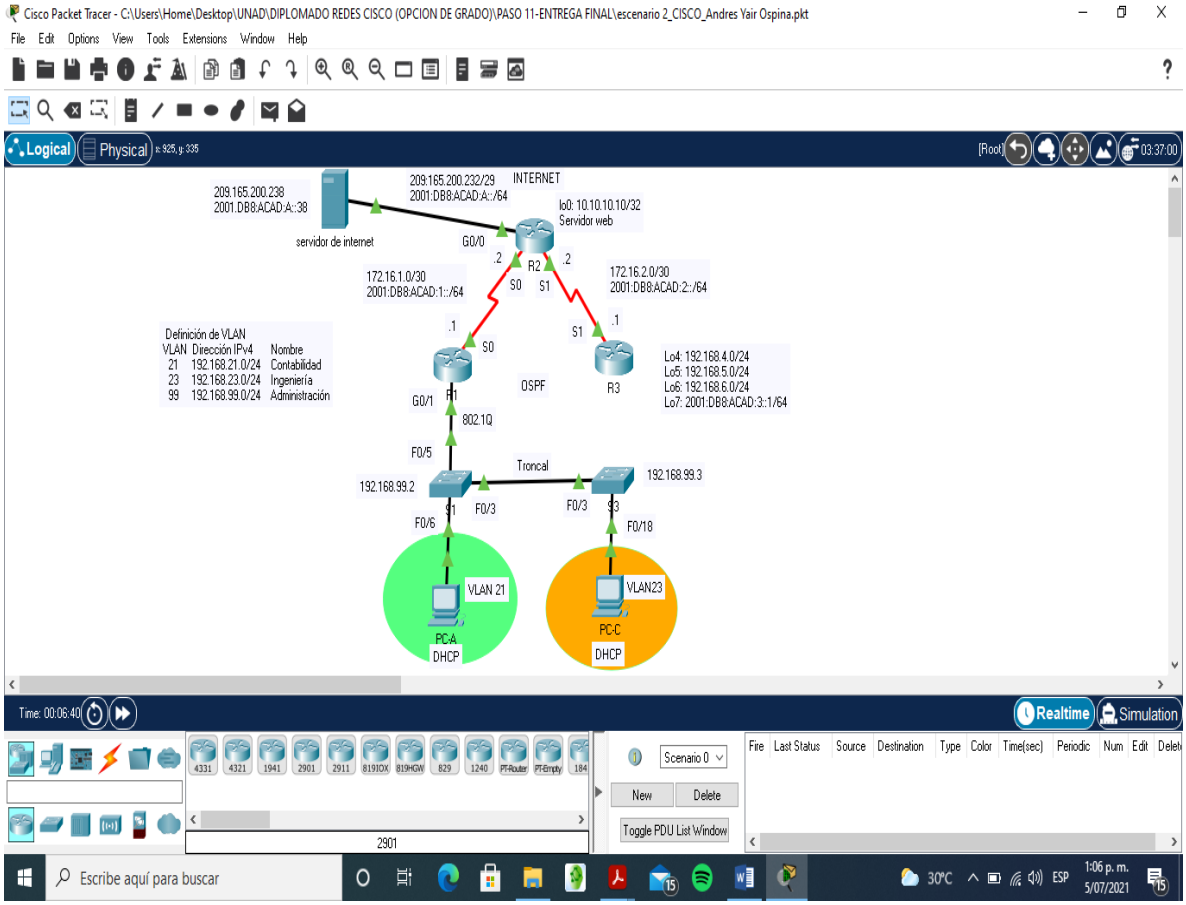
Figura 66. telnet denegado R3 a R2

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

Tabla 34. Comando CLI parte 7

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 20 permit 192.168.23.0 0.0.0.255 30 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 (6 match(es))
Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translations

Figura 67. Simulación escenario 2 packet tracer



CONCLUSIONES

Con la elaboración de esta actividad se colocaron en práctica los conocimientos obtenidos durante el diplomado de CISCO (diseño e implementación soluciones integradas LAN/WAN) mediante escenarios de simulación para lograr un acercamiento real a la vida cotidiana de la informática.

Por medio de este trabajo se aprendieron configuraciones de distintos equipos (routers, switchs, host, etc.) de redes desde las más básicas hasta las complejas con una excelente dinámica de aprendizaje, abordando temas importantes como la seguridad de los equipos, distintos tipos de protocolo de comunicación, interfaces virtuales, protocolos de enrutamiento, listas de control de acceso, la traducción de direcciones de red dinámicas y estáticas, entre otras.

Para nosotros como futuros ingenieros es muy importante esta actividad ya que nos capacitan para enfrentarnos a nuestra realidad en la vida laboral, llegando a distintos tipos de soluciones de problemas los cuales van hacer rutina cuando estemos ejerciendo la profesión.

BIBLIOGRAFIA

- CISCO. (2019). Exploración de la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1

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

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

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

- Vesga, J. (2017). Ping y Tracer como estrategia en los procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1lhgTCtKY-7F5KIRC3

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

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

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

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

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

- CISCO. (2019). Capa de aplicación. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10

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

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

- CISCO. (2019). Routing Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2

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

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

- CISCO. (2019). Redes Conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4

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

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

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

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

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

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

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

ESCENARIO 1: PRUEBA DE HABILIDADES CCNA-I

Ospina Calvo, Andres Yair
Universidad nacional abierta y a distancia
Dosquebradas, Risaralda
andresospiina@hotmail.com

resumen- En este trabajo se procederá a realizar las configuraciones básicas, seguridad conectividad ipv4-ipv6,enrutamiento de las vlan y DHCP de los routers, switches y host del escenario 1, con la finalidad de tener respuestas remotas en la red local y un envió perfecto de paquetes.

Palabras claves: vlan, DHCP, router, switch, host.

I. INTRODUCCION

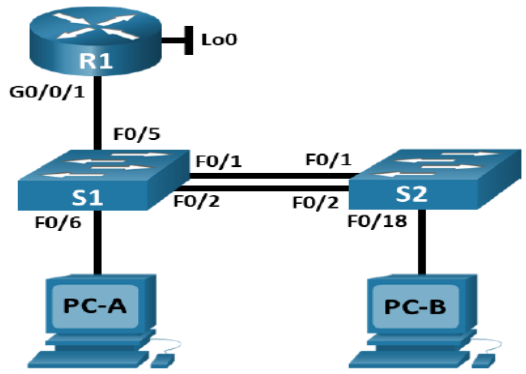
La finalidad del diplomado de profundización CISCO es capacitar y enseñar a los estudiantes a planificar, verificar, implementar y dar solución a problemas en redes LAN y WAN en un entorno virtual mediante un software de aprendizaje como packet tracer, el cual tiene las herramientas necesarias para que los estudiantes se familiaricen con los dispositivos informáticos y sus correspondientes configuraciones y de esta manera llevar sus conocimientos a un entorno real sea doméstico o empresarial.

En el desarrollo de las pruebas de habilidades prácticas CISCO nos vamos a centrar en el escenario 1 el cual es una red local pequeña que consta de un router, 2 swtich y 2 computadores y se procederá a realizar las configuraciones básicas, seguridad, conectividad ipv4-ipv6, enrutamiento de las vlan y DHCP de los dispositivos de antes mencionados.

II. DESARROLLO

Actividades a desarrollar

Figura 1. Topología Escenario 1



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

Tabla 1. Tabla de vlan

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

Tabla 2. Tabla de asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predetermina da
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8: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:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

Instrucciones

Parte 1: Inicializar y Recargar y Configurar aspectos basicos 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.

Router R1

Router>enable

Router#erase startup-config

Router#reload

Switch S1

switch>enable

switch#erase startup-config

switch#reload

Switch S2

switch>enable

switch#erase startup-config

switch#reload

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

Switch 1

Switch#configure terminal

Switch(config)#sdm prefer dual-ipv4-and-ipv6 default

Switch#reload

Switch 2

Switch#configure terminal

Switch(config)#sdm prefer dual-ipv4-and-ipv6 default

Switch#reload

Paso 2: Configurar R1

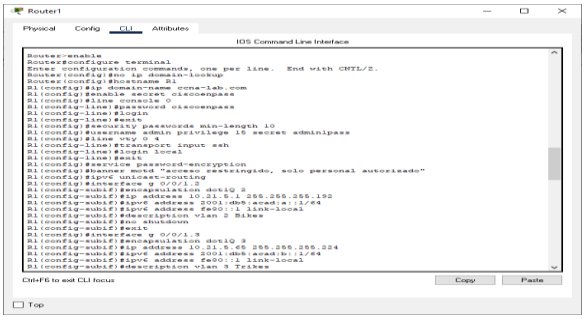
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3. Configuración router R1

Tarea	Especificación	Solución
Desactivar la búsqueda DNS	N/A	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	R1	Router(config)#hostname R1
Nombre de dominio	ccna-lab.com	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	ciscoenpass	R1(config)#line console 0 R1(config-line)#password ciscoenpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	10 caracteres	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**	R1(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	N/A	R1(config)#line vty 0 4
Configurar VTY solo aceptando SSH	N/A	R1(config-line)#transport input ssh R1(config-line)#login local R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	N/A	R1(config)#service password-encryption
Configure un MOTD Banner	N/A	R1(config)#banner motd "acceso restringido, solo personal autorizado"
Habilitar el routing IPv6	N/A	R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como **fe80: :1** Establece la dirección IPv6. Activar la interfaz.	R1(config)#interface g 0/0/1.2 R1(config-subif)#encapsulation dot1Q 2 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)#description vlan 2 Bikes R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface g 0/0/1.3 R1(config-subif)#encapsulation dot1Q 3 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)#description vlan 3 Trikes R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface g 0/0/1.4 R1(config-subif)#encapsulation dot1Q 4 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)#description vlan 4 Management R1(config-subif)#no shutdown R1(config-subif)#exit

		R1(config)#interface g 0/0/1.6 R1(config-subif)#encapsulation dot1Q 6 Native R1(config-subif)#description vlan 6 native R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface g 0/0/1 R1(config-if)#no shutdown R1(config-if)#exit
Configure el Loopback0 interface	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como fe80::1	R1(config)#interface lo0 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)#description loopback 0 R1(config-if)#exit
Generar una clave de cifrado RSA	Módulo de 1024 bits	R1(config)#crypto key generate rsa general-key modulus 1024

Figura 2. Configuración router R1 packet tracer



Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tabla4. Configuración Switch S1

Tarea	Especificación	Solución
Desactivar la búsqueda DNS.	N/A	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch	S1	Switch(config)#hostname S1
Nombre de dominio	ccna-lab.com	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	ciscoenpass	S1(config)#line console 0 S1(config-line)#password ciscoenpass S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass	S1(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	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
Cifrar las contraseñas de texto no cifrado	N/A	S1(config)#service password-encryption
Configurar un MOTD Banner	N/A	S1(config)#banner motd "acceso restringido, solo personal autorizado"
Generar una clave de cifrado RSA	Módulo de 1024 bits	S1(config)#crypto key generate rsa general-key modulus 1024
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1	S1(config)#interface vlan4 S1(config-if)#ip address 10.21.5.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db5:acad:c::98/64
	Establecer la dirección IPv6 de capa 3	S1(config-if)#ipv6 address fe80::98 link-local
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.21.5.97 para IPv4	S1(config-if)#ip default-gateway 10.21.5.97 ipv6 route ::/0 2001:db5:acad:c::1

Figura 3. Configuración switch S1 packet tracer

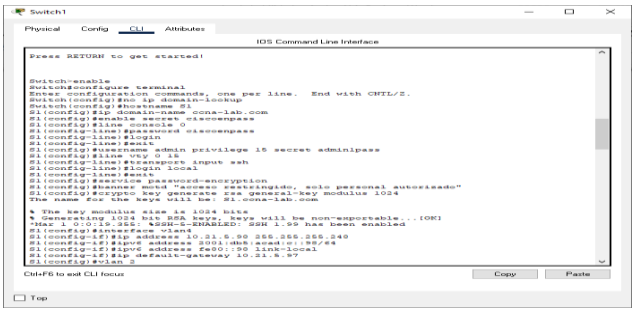
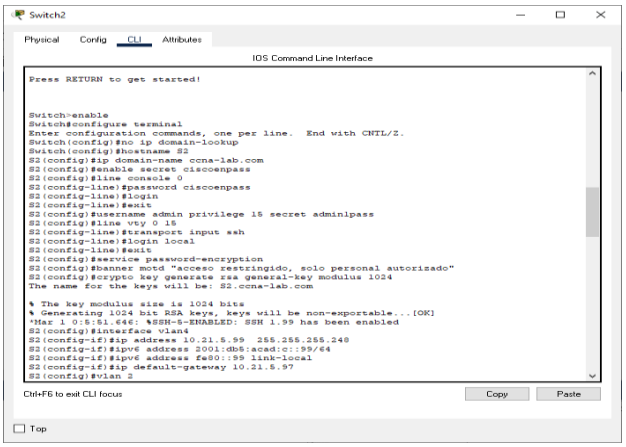


Tabla5. Configuración Switch S2

Tarea	Especificación	Solución
Desactivar la búsqueda DNS.	N/A	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch	S2	Switch(config)#hostname S2
Nombre de dominio	ccna-lab.com	S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass	S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	ciscoenpass	S2(config)#line console 0 S2(config-line)#password ciscoenpass S2(config-line)#login S2(config-line)#exit
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass	S2(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	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
Cifrar las contraseñas de texto no cifrado	N/A	S2(config)#service password-encryption
Configurar un MOTD Banner	N/A	S2(config)#banner motd "acceso restringido, solo personal autorizado"
Generar una clave de cifrado RSA	Módulo de 1024 bits	S2(config)#crypto key generate rsa general-key modulus 1024
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :99 para S2	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
	Establecer la dirección IPv6 de capa 3	S2(config-if)#ipv6 address fe80::99 link-local
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.21.5.97 para IPv4	S2(config-if)#ip default-gateway 10.21.5.97 ipv6 route ::/0 2001:db5:acad:c::1

Figura 4. Configuración switch S2 packet tracer



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

Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 6. Configuración estructura de red Switch S1

Tarea	Especificación	Solución
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	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
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5	S1(config)#interface f 0/1 switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#exit S1(config)#interface f 0/2 switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#exit S1(config)#interface f 0/5 switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#exit
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)#int range f0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#interface port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk Native vlan 6 S1(config-if)#exit
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6	S1(config)#interface f 0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 S1(config-if)#exit
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC	S1(config)#interface f0/6 S1(config-if)#switchport port-security S1(config-if)#switchport port-security Maximum 3 S1(config-if)#exit
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S1(config)#int range g0/1-2,f0/3-4,f0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#switchport port-security S1(config-if-range)#switchport port-security violation shutdown S1(config-if-range)#description no usar S1(config-if-range)#shutdown

Figura 5. Configuración estructura de red Switch S1 packet tracer

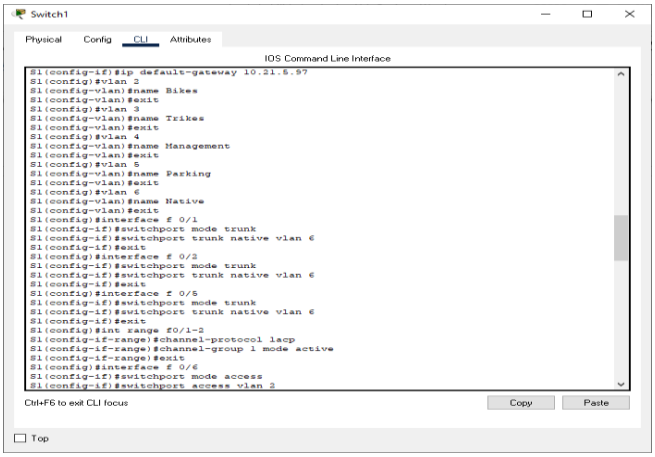
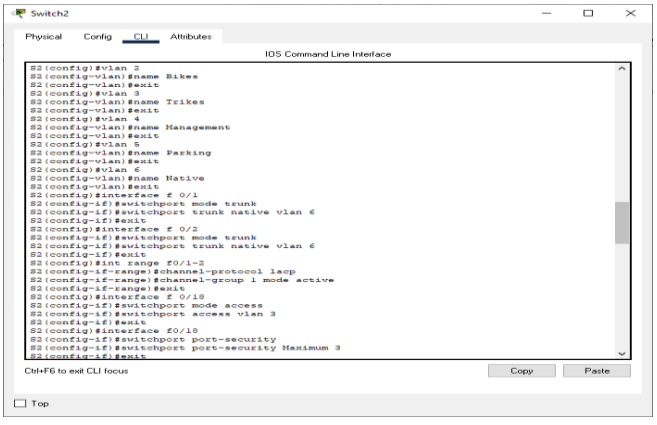


Tabla 7. Configuración estructura de red Switch S2

Tarea	Especificación	Solución
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#exit S2(config)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#exit S2(config)#vlan 4 S2(config-vlan)#name Management S2(config-vlan)#exit S2(config)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#exit S2(config)#vlan 6 S2(config-vlan)#name Native S2(config-vlan)#exit

Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2	S2(config)#interface f 0/1 switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config-if)#exit S2(config)#interface f 0/2 switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config-if)#exit
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)#int range f0/1-2 S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#interface port-channel 1 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk Native vlan 6 S2(config-if)#exit
Configurar el puerto de acceso de host para VLAN 3	Interface F0/18	S2(config)#interface f 0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#exit
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC	S2(config)#interface f0/18 S2(config-if)#switchport port-security S2(config-if)#switchport port-security Maximum 3 S2(config-if)#exit
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S2(config)#int range g0/1-2,f0/3-17,f0/19-24 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 no usar S2(config-if-range)#shutdown

Figura 6. Configuración estructura de red Switch S2 packet tracer



Parte 2: **Configurar soporte de host**

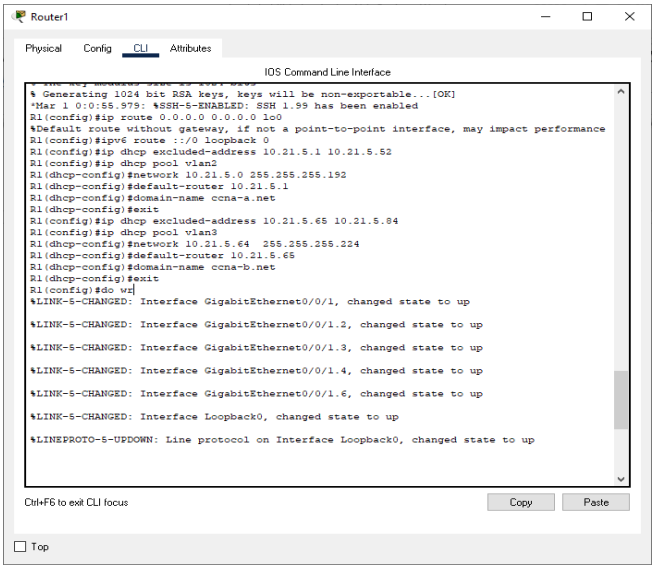
Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 8. Configuración soporte del Host

Tarea	Especificación	Solución
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0	R1(config)#ip route 0.0.0.0 0.0.0.0 lo0 R1(config)#ipv6 route ::/0 loopback 0
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 10.21.5.1 10.21.5.52 R1(config)#ip dhcp pool vlan2 R1(dhcp-config)#network 10.21.5.0 255.255.255.192 R1(dhcp-config)#default-router 10.21.5.1 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#exit
Configurar DHCP IPv4 para VLAN 3	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 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

Figura 7. Configuración soporte del host packet tracer



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**.

Tabla 9. Configuración PC-A

Configuración de red de PC-A	
Descripción	PC-A
Dirección física	0001.966C.E899
Dirección IP	10.21.5.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.21.5.1
Gateway predeterminado IPv6	FE80::1

Figura 8.ipconfig all /all PC-A

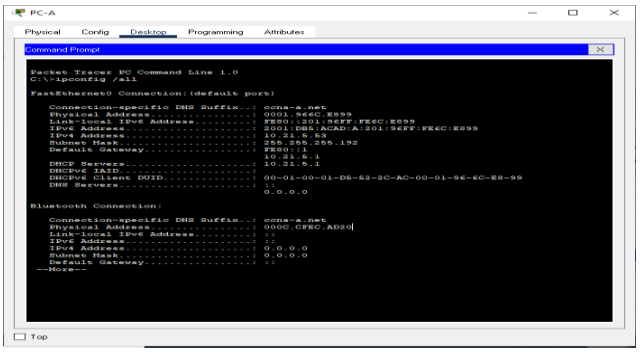


Figura 9. Configuración PC-A packet tracer

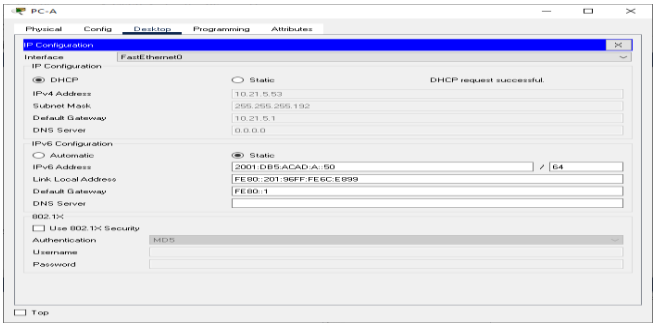


Tabla 10. Configuración PC-B

Configuración de red de PC-B	
Descripción	PC-B
Dirección física	000D.BD2C.3BCC
Dirección IP	10.21.5.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.21.5.65
Gateway predeterminado IPv6	FE80::1

Figura 10.ipconfig all /all PC-B

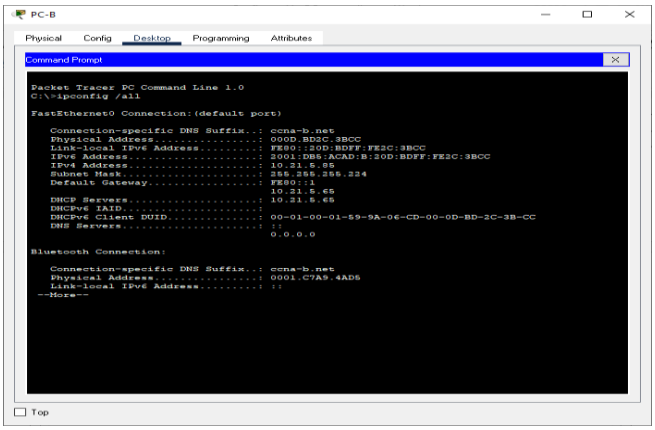


Figura 11. Configuración PC-B packet tracer

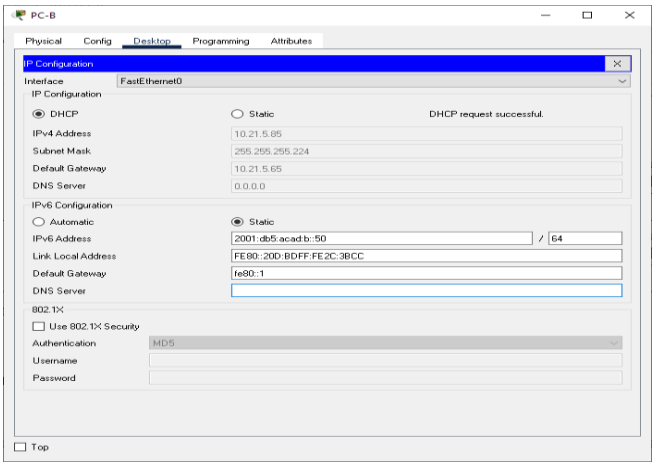
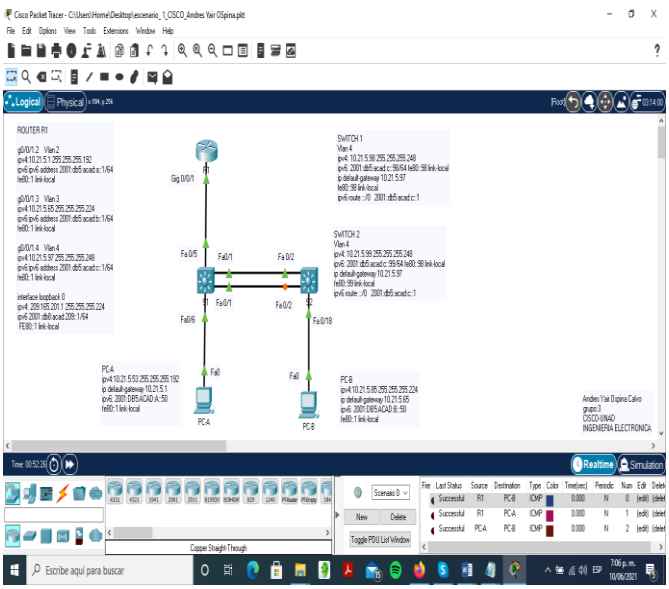


Figura 12. Simulación escenario 1 packet tracer



Parte 3: 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 11. Prueba de conectividad de extremo a extremo PC-A

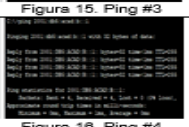
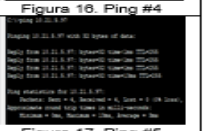
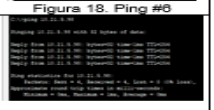
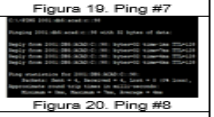
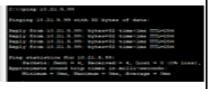
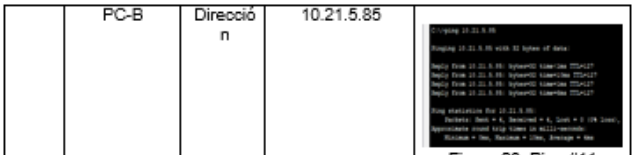
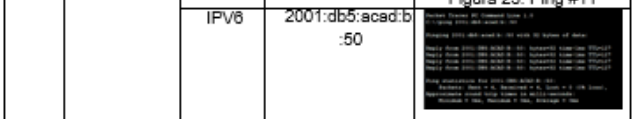
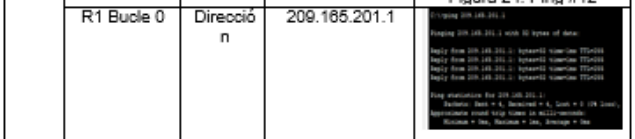
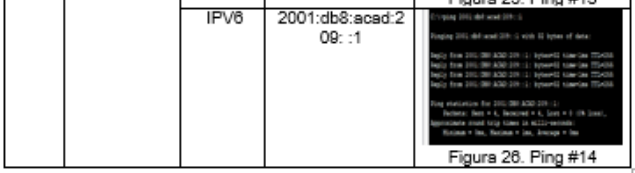
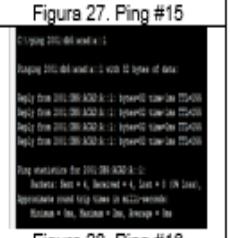
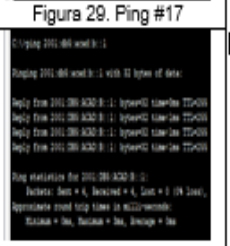
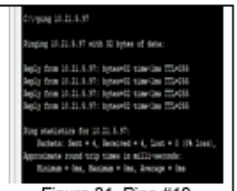
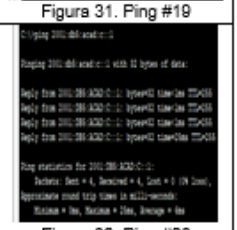
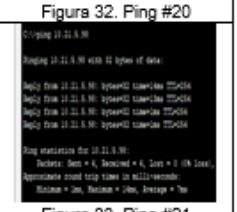
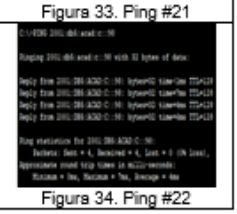
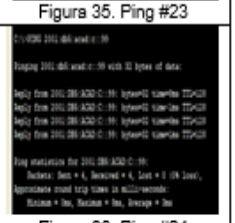
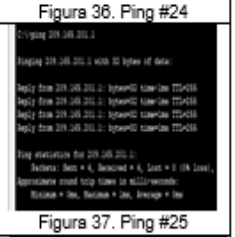
desde	A	Internet	Dirección ip	Resultado de ping
PC-A	R1,G0/0/1.2	Dirección	10.21.5.1	 Figura 13. Ping #1
		IPV6	2001:db5:acad:a::1	 Figura 14. Ping #2
	R1, G0/0/1.3	Dirección	10.21.5.65	 Figura 15. Ping #3
		IPV6	2001:db5:acad:b::1	 Figura 16. Ping #4
	R1, G0/0/1.4	Dirección	10.21.5.97	 Figura 17. Ping #5
		IPV6	2001:db5:acad:c::1	 Figura 18. Ping #6
	S1, VLAN 4	Dirección	10.21.5.98	 Figura 19. Ping #7
		IPV6	2001:db5:acad:c::98	 Figura 20. Ping #8
	S2, VLAN 4	Dirección	10.21.5.99	 Figura 21. Ping #9
		IPV6	2001:db5:acad:c::99	 Figura 22. Ping #10
	PC-B	Dirección	10.21.5.85	 Figura 23. Ping #11
		IPV6	2001:db5:acad:b::50	 Figura 24. Ping #12
	R1 Bucle 0	Dirección	209.165.201.1	 Figura 25. Ping #13
		IPV6	2001:db8:acad:209::1	 Figura 26. Ping #14

Tabla 12. Prueba de conectividad de extremo a extremo PC-B

desde	A	Internet	Dirección ip	Resultado de ping
PC-B	R1, G0/0/1.2	Dirección	10.21.5.1	 Figura 27. Ping #15
		IPV6	2001:db5:acad:a::1	 Figura 28. Ping #16
	R1, G0/0/1.3	Dirección	10.21.5.65	 Figura 29. Ping #17
		IPV6	2001:db5:acad:b::1	 Figura 30. Ping #18

	R1, G0/0/1.4	Dirección	10.21.5.97	 Figura 31. Ping #19
		IPV6	2001:db5:acad:c::1	 Figura 32. Ping #20
	S1, VLAN 4	Dirección	10.21.5.98	 Figura 33. Ping #21
		IPV6	2001:db5:acad:c::98	 Figura 34. Ping #22

	S2, VLAN 4	Dirección	10.21.5.99	 Figura 35. Ping #23
		IPV6	2001:db5:acad:c::99	 Figura 36. Ping #24
	R1 Bucle 0	Dirección	209.165.201.1	 Figura 37. Ping #25
		IPV6	2001:db8:acad:209::1	 Figura 38. Ping #26

III. CONCLUSIONES

[1] Con la elaboración de esta actividad se colocaron en práctica los conocimientos obtenidos durante el diplomado de CISCO (diseño e implementación soluciones integradas LAN/WAN) mediante escenarios de simulación para lograr un acercamiento real a la vida cotidiana de la informática.

[2] Por medio de este trabajo se aprendieron configuraciones de distintos equipos (routers, switchs, host, etc.) de redes desde las más básicas hasta las complejas con una excelente dinámica de aprendizaje, abordando temas importantes como la seguridad de los equipos, distintos tipos de protocolo de comunicación, interfaces virtuales entre otras.

[3] Para nosotros como futuros ingenieros es muy importante esta actividad ya que nos capacitan para enfrentarnos a nuestra realidad en la vida laboral, llegando a distintos tipos de soluciones de problemas los cuales van hacer rutina cuando estemos ejerciendo la profesión.

IV. BIBLIOGRAFIA

[1] CISCO. (2019). Exploración de la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1

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

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

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

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

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

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

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

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

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

[11] CISCO. (2019). Capa de aplicación. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10

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

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

[14]CISCO. (2019). Routing Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2

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

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

[17]CISCO. (2019). Redes Conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4

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

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

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

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

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

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

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