

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

JAVIER ANDRES ACEVEDO CASTAÑEDA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERIA ELECTRONICA  
VILLAVICENCIO  
2021

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

JAVIER ANDRES ACEVEDO CASTAÑEDA

HECTOR MANUEL HERRERA HERRERA

TUTOR

GRUPO: 203092\_3

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

INGENIERIA ELECTRONICA

VILLAVICENCIO

2021

Nota de Aceptación

---

---

---

---

---

---

Presidente del Jurado

---

Jurado

---

Jurado

Villavicencio 09 de julio de 2021

## AGRADECIMIENTOS

Primeros a Dios por darme la vida y una hermosa familia que me apoya incondicionalmente, una esposa que me da aliento y me anima cuando estoy a punto de desistir, una hija que ve en mi un ejemplo y una persona a quien quiere imitar, a la universidad nacional abierta y a distancia, que me dio la oportunidad de ser profesional y no por ser último y menos importante a aquellas personas que han aportado su tiempo y dedicación en mi para colaborarme y hacer que mis sueños se hagan realidad.

## CONTENIDO

1. LISTA DE FIGURAS.....	3
2. LISTA DE TABLAS.....	6
3. INTRODUCCIÓN .....	8
4. RESUMEN .....	9
5. PRUEBA DE HABILIDADES CCNA I.....	10
4.1 ESCENARIO 1 .....	10
4.2 ESCENARIO 2.....	43
6. CONCLUSIONES.....	87
7. BIBLIOGRAFÍA .....	89
8. ANEXOS .....	91

## 1. LISTA DE FIGURAS

Figura 1 - Escenario 1 .....	10
Figura 2 - Simulación Packet Tracer Escenario 1 .....	13
Figura 3 – Configuración del Router 1 .....	14
Figura 4 - Configuración del Switch 1 .....	15
Figura 5 – Configuración para R1 .....	19
Figura 6 - Configuración para R1 .....	19
Figura 7 - Configuración para R1 .....	20
Figura 8 - Configuración S1 .....	22
Figura 9 - Configuración S1 .....	23
Figura 10 - Configuración S2 .....	25
Figura 11 - Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) para S1 .....	28
Figura 12 - Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) para S1 .....	28
Figura 13 - Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) para S2 .....	31
Figura 14 - Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) para S2 .....	31
Figura 15 - Configurar soporte de host para R1 .....	33
Figura 16 - Configuración PC-A .....	34
Figura 17 - Configuración PC-B .....	35
Figura 18 – Comando Ping desde PC-A a dirección 10.21.5.1 y 2001:db5:acad:a::1 .....	37
Figura 19 - Comando Ping desde PC-A a dirección 10.21.5.65 y 2001:db5:acad:b::1 .....	37
Figura 20 - Comando Ping desde PC-A a dirección 10.21.5.97 y 2001:db5:acad:c::1 .....	38

Figura 21 - Comando Ping desde PC-A a dirección 10.21.5.98 y 2001:db5:acad:c::98 .....	38
Figura 22 - Comando Ping desde PC-A a dirección 10.21.5.52 y 10.21.5.99 .....	39
Figura 23 - Comando Ping desde PC-A a dirección 2001:db8:acad:209::1 .....	39
Figura 24 - Comando Ping desde PC-A a dirección 2001:db5:acad:b::50 .....	40
Figura 25 - Comando Ping desde PC-B a dirección 10.21 5.1, 2001:db5:acad:a::1 y 10.21.5.65 .....	41
Figura 26 - Comando Ping desde PC-B a dirección 2001:db5:acad:b::1, 10.21.5.97 y 2001:db5:acad:c::1 .....	42
Figura 27 - Comando Ping desde PC-B a dirección 10.21.5.98, 2001:db5:acad:c::98 y 10.21.5.99 .....	42
Figura 28 - Escenario 2 .....	43
Figura 29 - Configuración de los 3 Routers .....	45
Figura 30 - Configuración en los 2 Switches .....	46
Figura 31 - Comando Show Flash .....	46
Figura 32 - Configuración en Router1 .....	49
Figura 33 - Configuración en Router1 .....	50
Figura 34 - Configuración en Router2 .....	53
Figura 35 - Configuración en Router2 .....	53
Figura 36 - Configuración en Router3 .....	56
Figura 37 - Configuración del S1 .....	57
Figura 38 - Configuración del S3 .....	59
Figura 39 - Verificación con comando ping de R1 a R2 .....	60
Figura 40 - Verificación con comando ping de R2 a R3 .....	61
Figura 41 - Verificación con comando ping de PC INTERNET a 209.165.200.23361	
Figura 42 - Configuración del S1 .....	64
Figura 43 - Configuración el S3 .....	66
Figura 44 - Configuración para R1 .....	67
Figura 45- Configuración del Switch 1 .....	70
Figura 46 - Configuración del Switch 3 .....	70

Figura 47 - Configuración del protocolo de routing dinámico OSPF para R1.....	72
Figura 48 - Configuración del protocolo de routing dinámico OSPF para R2.....	73
Figura 49 - Configuración del protocolo OSPFv3 en el R3 .....	74
Figura 50 - Verificación de la información de OSPF en R1 .....	75
Figura 51 - Comando de verificación show ip route OSPF en R1 .....	76
Figura 52 - Comando de verificación show ip route OSPF database en R1 .....	76
Figura 53 - Configuración para R1 con DHCP y NAT para IPv4.....	78
Figura 54 – Configuración de la NAT estática y dinámica en el R2 .....	79
Figura 55 - Configuración del NTP en R2 .....	82
Figura 56 - Configuración del NTP en R1 .....	82
Figura 57 - Verifique la configuración de NTP en R1 .....	83
Figura 58 – Verificación de ACL en R2.....	84
Figura 59 - Verificación de ACL en R3.....	85



## 2. LISTA DE TABLAS

Tabla 1 - Tabla de VLAN.....	10
Tabla 2 - Tabla de asignación de direcciones.....	11
Tabla 3 - Configuración para R1 .....	15
Tabla 4 - Configuración S1 .....	20
Tabla 5 - Configuración S2 .....	23
Tabla 6 - Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) para S1 .....	26
Tabla 7 - Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) para S2 .....	29
Tabla 8 - Configurar soporte de host para R1 .....	32
Tabla 9 – Configuración de red para PC-A .....	34
Tabla 10 - configuración de red para PC-B.....	34
Tabla 11 - Tabla de verificación .....	36
Tabla 12 - Tabla de verificación 2 .....	40
Tabla 13 - Configuración escenario 2 .....	44
Tabla 14 – Configuración de la computadora de Internet .....	47
Tabla 15 - Configuración para R1 .....	47
Tabla 16 - Configuración en Router2 .....	50
Tabla 17 - Configuración para R3.....	54
Tabla 18 - Configuración para el S1.....	56
Tabla 19 - Configuración del S3.....	58
Tabla 20 - Tabla de verificar .....	59
Tabla 21 - Configuración del S1.....	62
Tabla 22 - Configuración el S3.....	64
Tabla 23 - Configuración para R1 .....	66
Tabla 24 - Tabla de verificación .....	68
Tabla 25 – Configuración del protocolo de routing dinámico OSPF para R1 .....	71

Tabla 26 - Configuración del protocolo de routing dinámico OSPF para R2.....	72
Tabla 27 – Configuración del protocolo OSPFv3 en el R3.....	73
Tabla 28 – Tabla de verificación de la información de OSPF .....	75
Tabla 29 - Configuración para R1 .....	77
Tabla 30 - Configuración del R2 .....	78
Tabla 31 - Configuración del NTP en R1 y R2.....	81
Tabla 32 - Verificación las listas de control.....	83
Tabla 33 – Comando de configuración .....	85

### 3. INTRODUCCIÓN

En el siguiente informe encontrarán el desarrollo del escenario 1 y 2, donde se plasma la solución del caso propuesto como prueba de habilidades prácticas, con el fin de modelar cada uno de los temas desarrollados durante el primer periodo del año 2021, estos escenarios está compuesto por una topología de red pequeña, se configuraron un router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados, El router y el switch se administran de forma segura, con su debida configuración y enrutamiento entre VLAN, DHCP, Etherchannel y port-security, entre otros.

#### 4. RESUMEN

En el siguiente documento estar desarrollados los dos escenarios planteados como desarrollo de proyecto final del curso de Diplomado de profundización CISCO, con la finalidad de instituir la prueba de habilidades prácticas. Dichos escenarios se realizaron con ayuda del software Packet Tracer, herramienta que permitió simular y configurar cada escenario según lo estipula la guía de actividades

**PALABRAS CLAVE:** Red, IPv4, IPv6, Escenarios, Cisco, Packet Tracer, conectividad, Switch, Router, Vlans enrutamiento, VTP

#### ABSTRACT

In the following document, the two scenarios proposed as development of the final project of the CISCO in-depth Diploma course will be developed, in order to institute the practical skills test. These scenarios were carried out with the help of Packet Tracer software, a tool that allowed simulating and configuring each scenario as stipulated in the activity guide.

**KEYWORDS:** Network, IPv4, IPv6, Scenarios, Cisco, Packet Tracer, connectivity, Switch, Router, Vlans routing, VTP

## 5. PRUEBA DE HABILIDADES CCNA I

### 4.1 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. Configuraré el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Topología de red

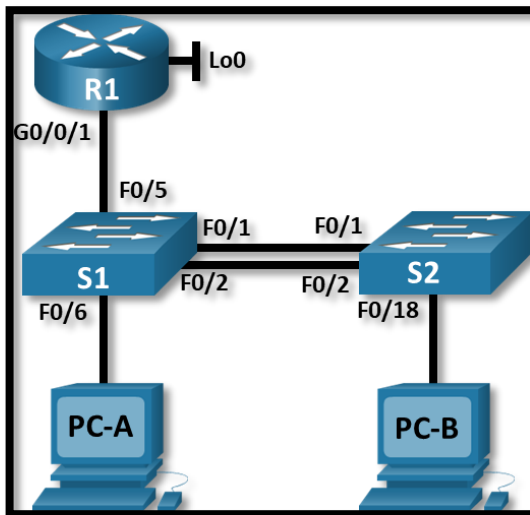


Figura 1 - Escenario 1

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	10.21.5.1 /26	No corresponde
	2001:db5:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.21.5.65 /27	No corresponde
	2001:db5:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.21.5.97 /29	No corresponde
	2001:db5:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.21.5.98 /29	10.21.5.97
	2001:db5:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.21.5.99 /29	10.21.5.97
	2001:db5:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4

	2001:db5:acad:a::50/64	fe80::1
PC-B NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db5:acad:b: :50 /64	fe80::1

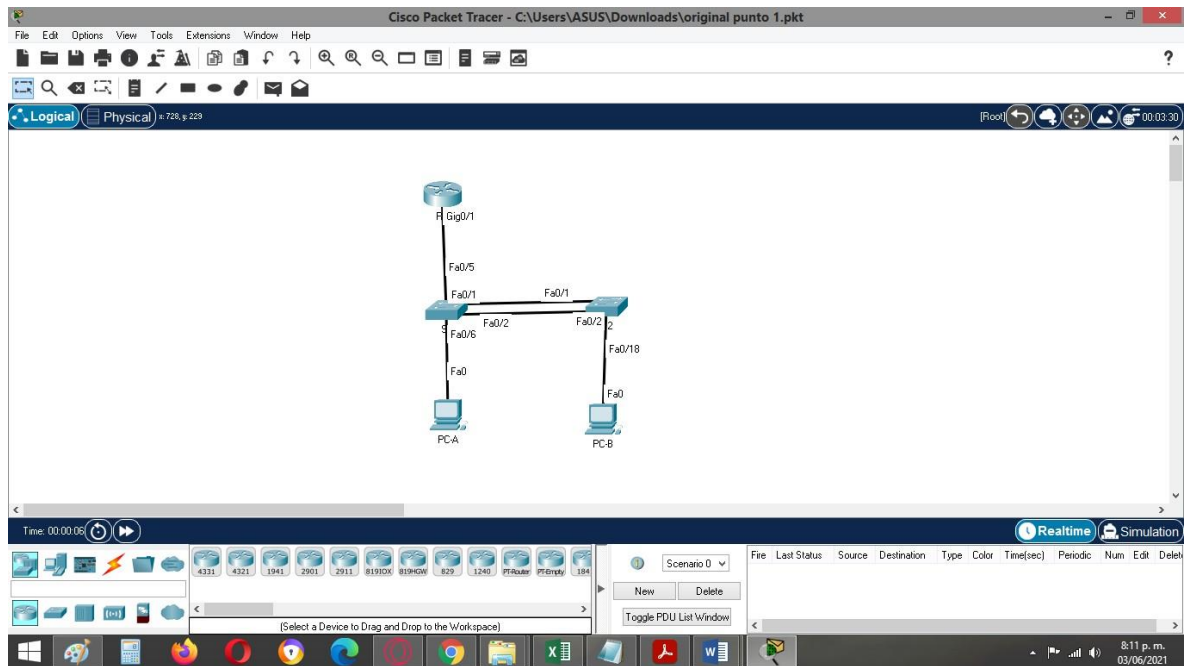
**Nota:** No hay ninguna interfaz en el router que admita VLAN 5.

Instrucciones

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

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

- Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos.
- Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.
- Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.



*Figura 2 - Simulación Packet Tracer Escenario 1*

## ROUTER 1

Router>enable

Router#erase st

Router#erase startup-config

Router#Delete flash:vllans.dat

Router#reload



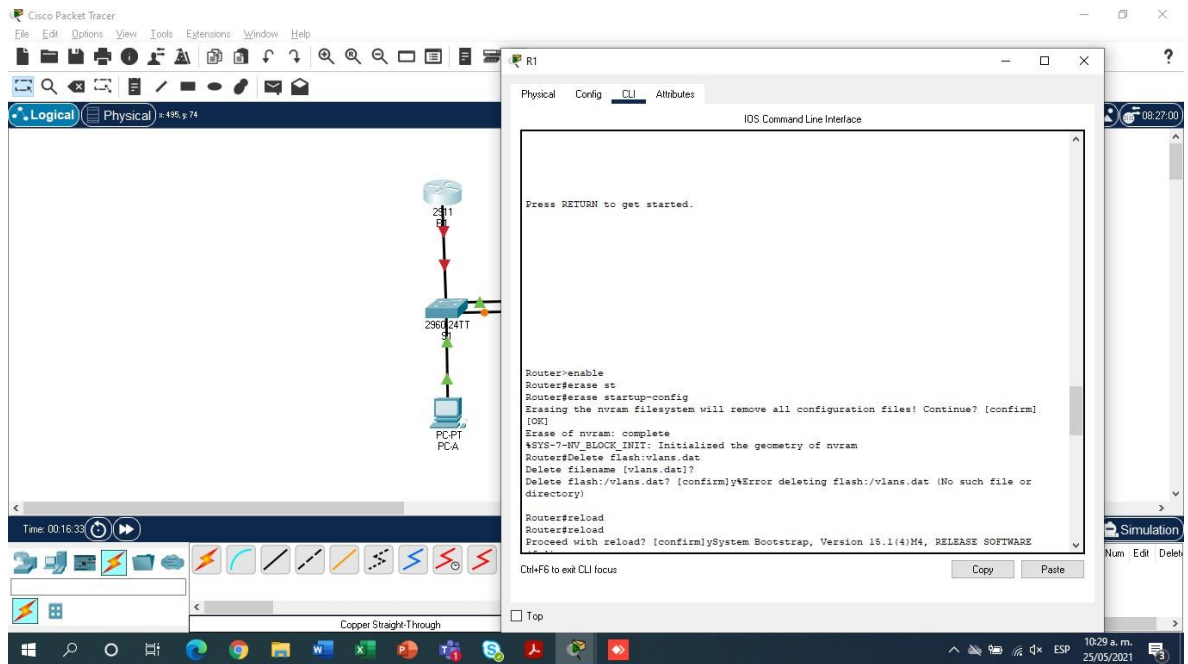


Figura 3 – Configuración del Router 1

## SWITCH 1 Y SWITCH 2

Switch>enab

Switch#erase star

Switch#erase startup-config

Switch#Delete flash:vlan.dat

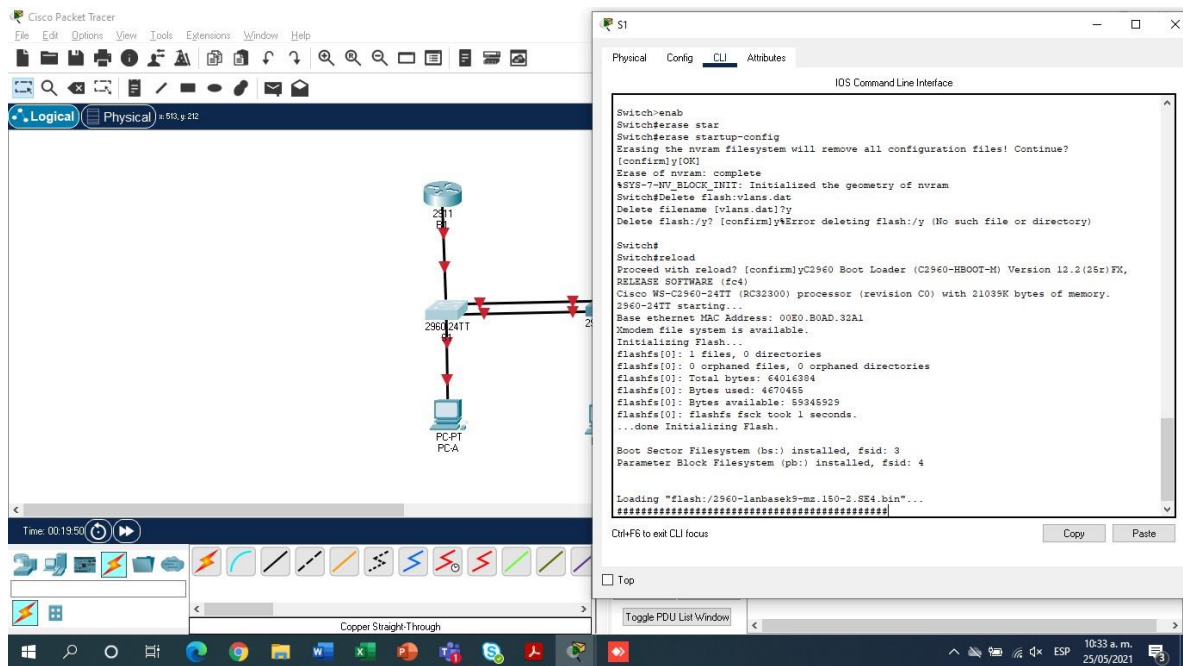


Figura 4 - Configuración del Switch 1

## Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3 - Configuración para R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1 R1(config)#
Nombre de dominio	R1(config)#ip domain-name ccna-lab.com

Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config)#line conso 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	R1(config)#security pass mi R1(config)#security pass min-length 10
Crear un usuario administrativo en la base de datos local	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	R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	R1(config)#line vty 0 4 R1(config-line)#transport input ssh R1(config-line)#login local R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd #Acceso a personal autorizado#
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
	R1(config)#interface g0/1.2 R1(config-subif)#encapsula do R1(config-subif)#encapsula dot1Q 2 R1(config-subif)#descrip LAN to VLAN2 R1(config-subif)#ip add 10.21.5.1 255.255.255.192

<p>Configurar interfaz G0/0/1 y subinterfaces</p>	<pre> R1(config-subif)#ipv6 add 2001:db5:acad:a::1/64 R1(config-subif)#ipv6 add fe80::1 link- local R1(config-subif)#no shutdown R1(config-subif)#exit  R1(config)#interfac g0/1.3 R1(config-subif)#encapsulation do R1(config-subif)#encapsulation dot1Q 3 R1(config-subif)#ip add 10.21.5.65 255.255.255.224 R1(config-subif)#ipv6 add 2001:db5:acad:b::1/64 R1(config-subif)#ipv6 add fe80::1 link- local R1(config-subif)#description LAN to VLAN3 R1(config-subif)#no shutdown R1(config-subif)#exit  R1(config)#interface g0/1.4 R1(config-subif)#encapsulation dot1Q 4 R1(config-subif)#ip add 10.21.5.97 255.255.255.248 R1(config-subif)#ipv6 add 2001:db5:acad:c::1/64 R1(config-subif)#ipv6 add fe80::1 link- local </pre>
---	---

	<pre> R1(config-subif)#description LAN to VLAN4 R1(config-subif)#no shutdow R1(config-subif)#exit  R1(config)#interfac g0/1.6 R1(config-subif)#encapsulation dot1Q 6 R1(config-subif)#exit R1(config)#interfac g0/1 R1(config-if)#no shutdo </pre>
Configure el Loopback0 interface	<pre> R1(config)#interfac lo0 R1(config-if)#description LAN to Loopback0 R1(config-if)#ip add 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 add 2001:db8:acad:209::1/64 R1(config-if)#ipv6 add fe80::1 link-local R1(config-if)#no shut R1(config-if)#exit </pre>
Generar una clave de cifrado RSA	<pre> R1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] </pre>

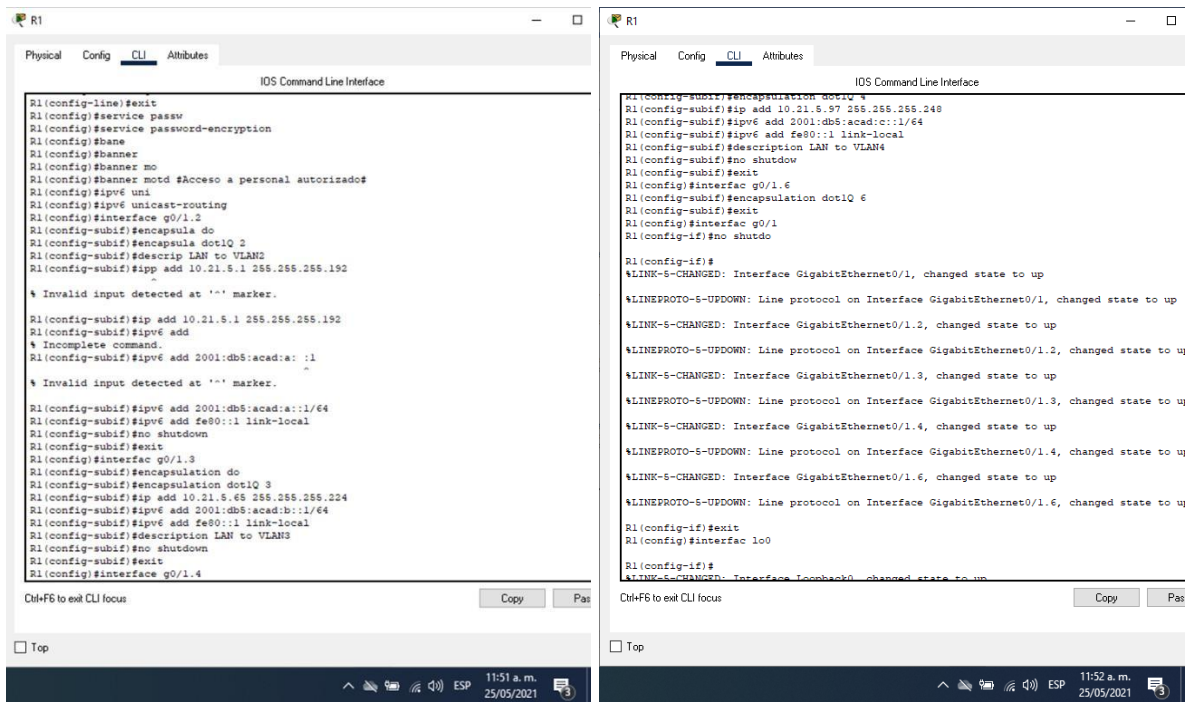


Figura 5 – Configuración para R1

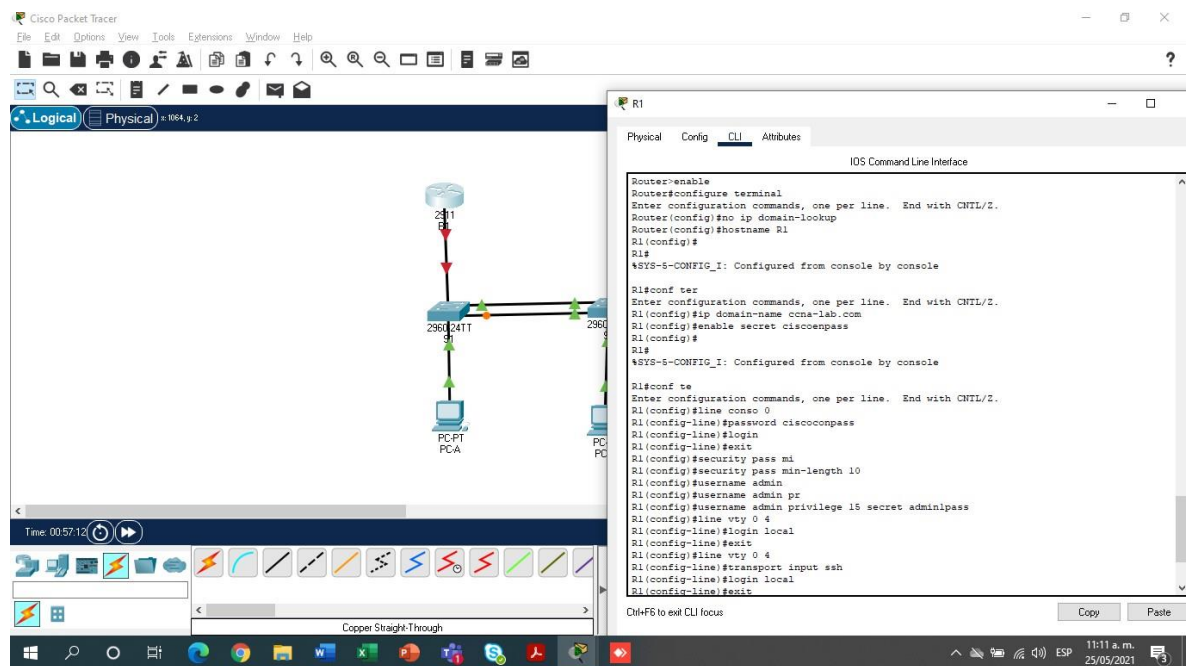


Figura 6 - Configuración para R1

```

R1
Physical Config CLI Attributes
IOS Command Line Interface

%LINK-5-CHANGED: Interface GigabitEthernet0/1.3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.3, changed state to u
%LINK-5-CHANGED: Interface GigabitEthernet0/1.4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.4, changed state to u
%LINK-5-CHANGED: Interface GigabitEthernet0/1.6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.6, changed state to u

R1(config-if)#exit
R1(config)#interfac lo0

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R1(config-if)#description LAN to Loopback0
R1(config-if)#ip add 209.165.201.1 255.255.255.224
R1(config-if)#ipv6 add 2001:db9:acad:209::1/64
R1(config-if)#ipv6 add fe80::1 link-local
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#crypto key gen
R1(config)#crypto key generate rsa
The name for the keys will be: R1.ccsa-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#
  
```

Figura 7 - Configuración para R1

### Parte 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tabla 4 - Configuración S1

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch#conf termin Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1

Nombre de dominio	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	S1(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local S1(config-line)#exit
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	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd #Acceso a personal autorizado#
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa  The name for the keys will be: S1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your



	<p>General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.</p> <p>How many bits in the modulus [512]: 1024</p> <p>% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]</p>
Configurar la interfaz de administración (SVI)	<pre>S1(config)#interface vlan 4 *Mar 1 1:46:9.676: %SSH-5-ENABLED: SSH 1.99 has been enabled S1(config-if)#ip add 10.21.5.98 255.255.255.248 S1(config)#inter vlan 4 S1(config-if)#ipv6 add 2001:db5:acad:c::98/64 S1(config-if)#ipv6 add fe80::98 link-local S1(config-if)#no shut S1(config-if)#exit</pre>
Configuración del gateway predeterminado	<pre>S1(config)#ip default-gateway 10.21.5.97</pre>

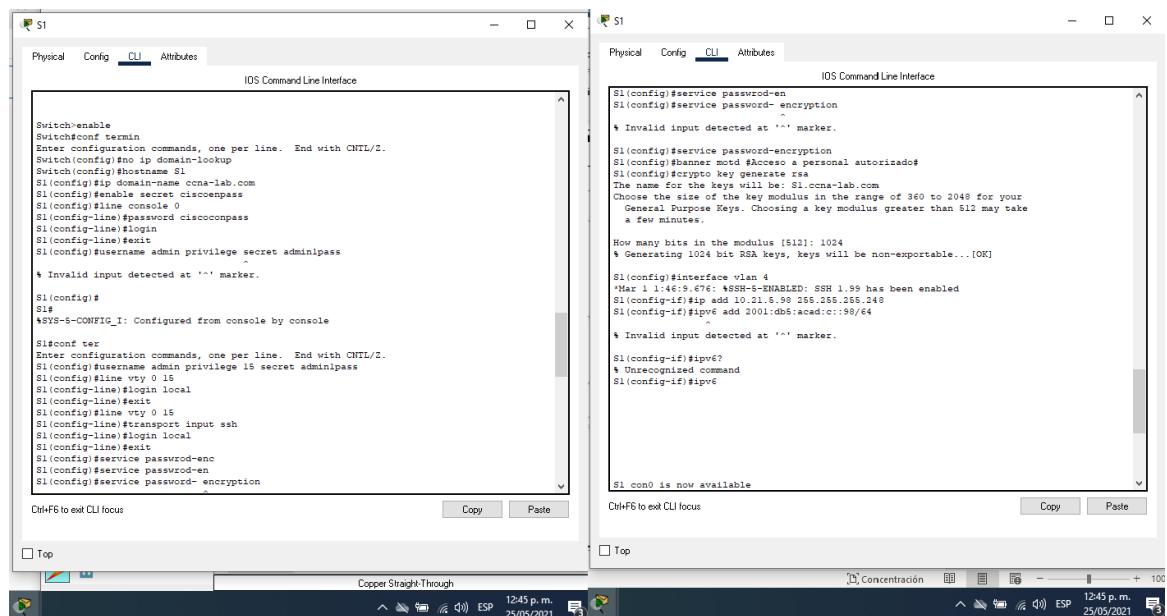


Figura 8 - Configuración S1

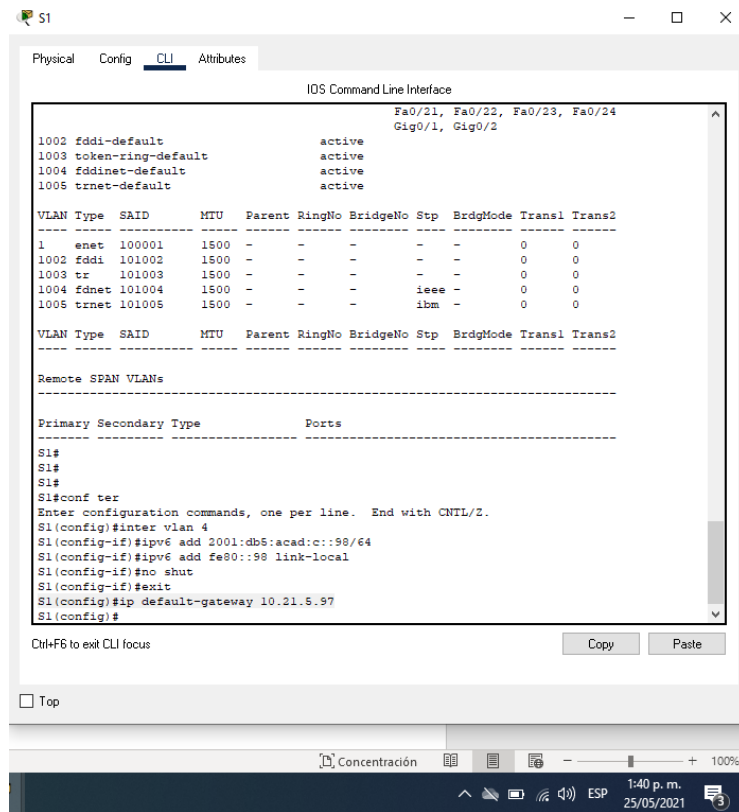


Figura 9 - Configuración S1

Tabla 5 - Configuración S2.

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch#conf termin Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S2
Nombre de dominio	S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo	S2(config)#enable secret ciscoenpass

EXEC privilegiado	
Contraseña de acceso a la consola	<pre>S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit</pre>
Crear un usuario administrativo en la base de datos local	<pre>S2(config)#username admin privilege 15 secret admin1pass</pre>
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	<pre>S2(config)#line vty 0 15 S2(config-line)#login local S2(config-line)#exit</pre>
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	<pre>S2(config)#line vty 0 15 S2(config-line)#transport input ssh S2(config-line)#login local S2(config-line)#exit</pre>
Cifrar las contraseñas de texto no cifrado	<pre>S2(config)#service password-encryption</pre>
Configurar un MOTD Banner	<pre>S2(config)#banner motd #Acceso a personal autorizado#</pre>
Generar una clave de cifrado RSA	<pre>S2(config)#crypto key generate rsa</pre> <p>The name for the keys will be: S2.ccna-lab.com</p> <p>Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.</p> <p>How many bits in the modulus [512]: 1024</p>

	% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Configurar la interfaz de administración (SVI)	<pre>S2(config)#inter vlan 4 *Mar 1 0:2:7.704: %SSH-5-ENABLED: SSH 1.99 has been enabled S2(config-if)#ip add 10.21.5.99 255.255.255.248 S2(config-if)#ipv6 add 2001:db5:acad:c::99/64 S2(config-if)#ipv6 add fe80::99 link-local S2(config-if)#no shutd S2(config-if)#exit</pre>
Configuración del gateway predeterminado	S2(config)#ip default-gateway 10.21.5.97

```

S2
-----
Physical  Config  CLI  Attributes
-----
IOS Command Line Interface

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S2
S2(config)#ip domain-name ccsa-lab.com
S2(config)#enable secret ciscoenpass
S2(config)#line console 0
S2(config-line)#password ciscocompass
S2(config-line)#login
S2(config-line)#exit
S2(config)#username admin privilege 15 secret adminipass
S2(config)#line vty 0 15
S2(config-line)#transport input ssh
S2(config-line)#login local
S2(config-line)#exit
S2(config)#service password-encryption
S2(config)#banner motd #Acceso a personal autorizado#
S2(config)#crypto key generate rsa
The name for the keys will be: S2.ccsa-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S2(config)#inter vlan 4
*Mar 1 0:2:7.704: %SSH-5-ENABLED: SSH 1.99 has been enabled
S2(config-if)#ip add 10.21.5.99 255.255.255.248
S2(config-if)#ipv6 add 2001:db5:acad:c::99/64
S2(config-if)#ipv6 add fe80::99 link-local
S2(config-if)#no shutd
S2(config-if)#exit
S2(config)#ip default-gateway 10.21.5.97
S2(config)#

```

Figura 10 - Configuración S2.

## 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 de la infraestructura de red (VLAN, Trunking, EtherChannel) para S1*

Tarea	Especificación
Crear VLAN	S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#vlan 4 S1(config-vlan)#name Management S1(config-vlan)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#vlan 6 S1(config-vlan)#name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S1(config)#int f0/1 S1(config-if)#switch S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6  S1(config)#int f0/2 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6  S1(config)#int f0/5

	<pre>S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6</pre>
<p>Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2</p>	<pre>S1(config)#interface range fa0/1-2 S1(config-if-range)#channel-group 2 mode active S1(config)#interface port-channel 2 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6</pre>
<p>Configurar el puerto de acceso de host para VLAN 2</p>	<pre>S1(config)#int f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 S1(config-if)#no shutd S1(config-if)#exit</pre>
<p>Configurar la seguridad del puerto en los puertos de acceso</p>	<pre>S1(config)#int f0/6 S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3</pre>
<p>Proteja todas las interfaces no utilizadas</p>	<pre>S1(config)#interface range fa0/3- 4, fa0/7-24, gi0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Puertos sin utilizar S1(config-if-range)#shutd</pre>

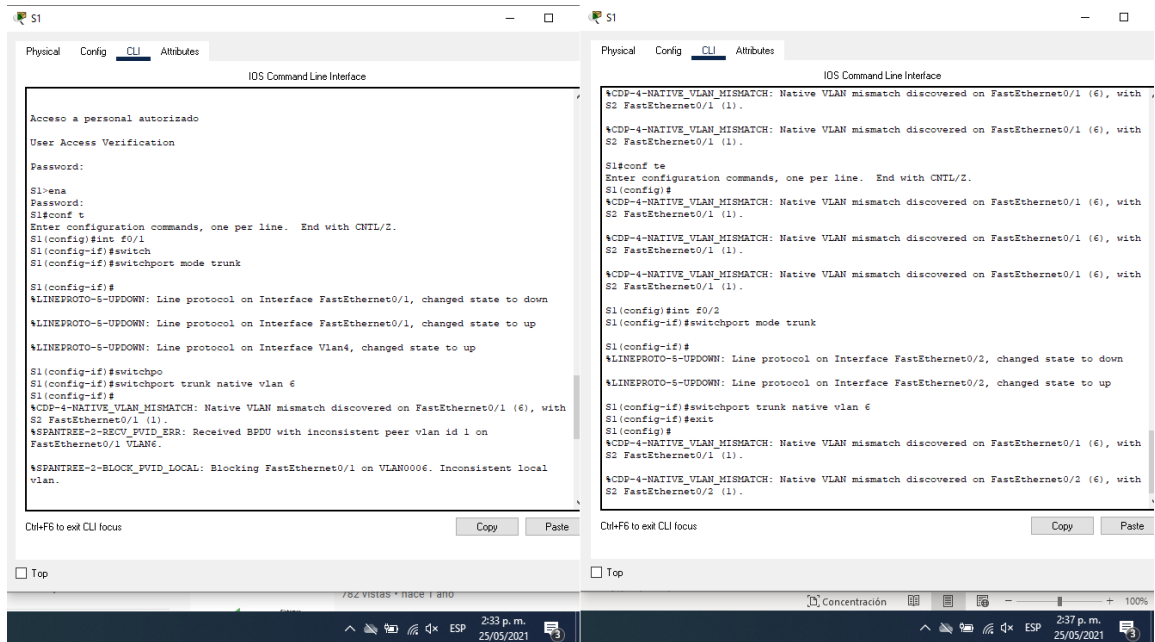


Figura 11 - Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) para S1

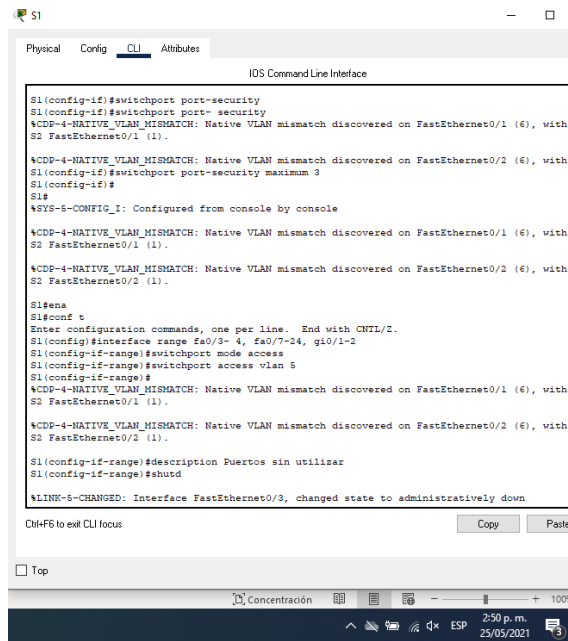


Figura 12 - Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) para S1

## Paso 5: Configurar S1

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

*Tabla 7 - Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) para S2*

Tarea	Especificación
Crear VLAN	S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#vlan 4 S2(config-vlan)#name Management S2(config-vlan)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#vlan 6 S2(config-vlan)#name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S2(config)#interface range fa0/1-2 S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S2(config)#interface port-channel 2 S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config-if)#exit S2(config)#interface range fa0/1-2 S2(config-if-range)#channel-group 2 mode passive
Configurar el puerto de acceso del host para la VLAN 3	S2(config)#interface fa0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3



	S2(config-if)#exit
Configure port-security en los access ports	<pre>S2(config)#interface fa0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#exit S2(config)#interface          fa0/18 S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3</pre>
Asegure todas las interfaces no utilizadas.	<pre>S2#conf t Enter configuration commands, one per line. End with CNTL/Z. S2(config)#interface range fa0/3-17, fa0/19-24, gi0/1-2 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Puertos no utilizados S2(config-if-range)#shutdown</pre>

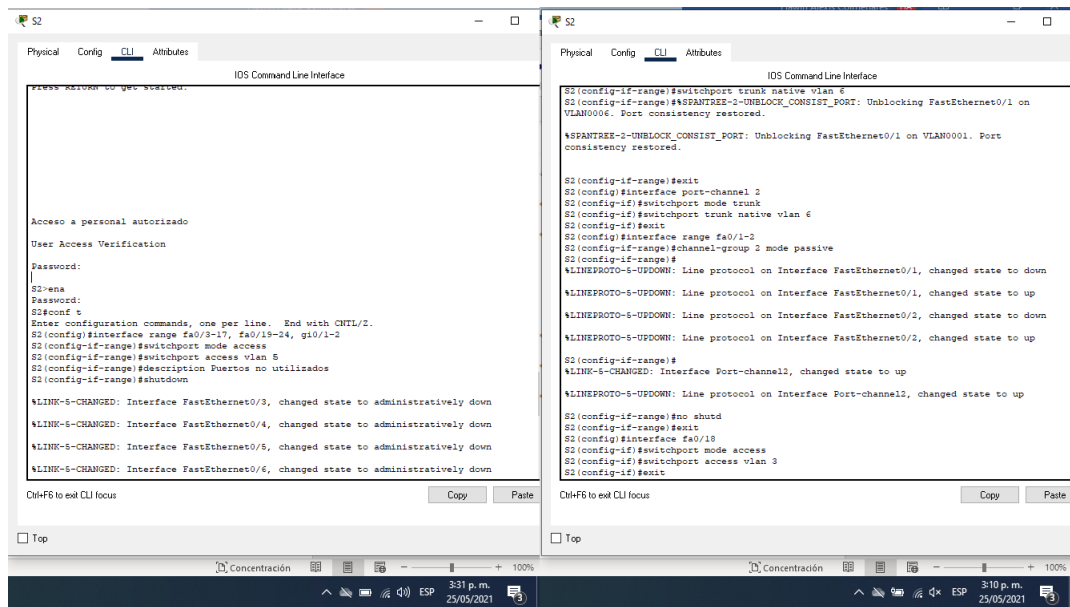


Figura 13 - Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) para S2

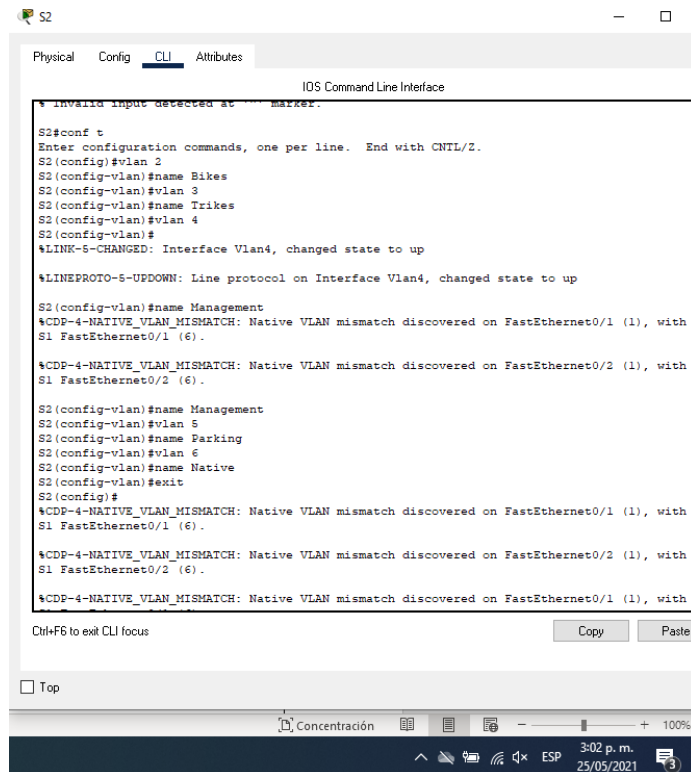


Figura 14 - Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) para S2

## Parte 2: Configurar soporte de host

### Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

*Tabla 8 - Configurar soporte de host para R1*

Tarea	Especificación
Configure Default Routing	ip route 0.0.0.0 0.0.0.0 lo0
Configurar IPv4 DHCP para VLAN 2	R1#conf t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ip dhcp pool vlan2 R1(dhcp-config)#network 10.21.5.0 255.255.255.192 R1(dhcp-config)#default R1(dhcp-config)#default-router 10.21.5.1 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#exit R1(config)#ip dhcp excluded-address 10.21.5.2 10.21.5.51 R1(config)#
Configurar IPv4 DHCP para VLAN 3	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)#ip dhcp excluded-address

	10.21.5.66 10.21.5.83
--	-----------------------

```

R1
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.6, changed state to up
Acceso a personal autorizado
User Access Verification
Password:
R1>ena
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route 0.0.0.0 0.0.0.0 100
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#
R1#
$SYS-5-CONFIG_I: Configured from console by console
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp pool vian3
R1(dhcp-config)#network 10.21.5.0 255.255.255.192
R1(dhcp-config)#default-router 10.21.5.1
R1(dhcp-config)#domain-name ccna-a.net
R1(dhcp-config)#exit
R1(config)#ip dhcp excluded-address 10.21.5.2 10.21.5.51
R1(config)#
R1(config)#ip dhcp pool vian3
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)#ip dhcp excluded-address 10.21.5.66 10.21.5.83
R1(config)#

```

Figura 15 - Configurar soporte de host para R1

## 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 de red para PC-A

PC-A Network Configuration	
Descripción	ccna-a.net
Dirección física	0006.2A30.40E2
Dirección IP	10.21.5.52
Máscara de subred	255.255.255.192
Gateway predeterminado	10.21.5.1
Gateway predeterminado IPv6	FE80::1

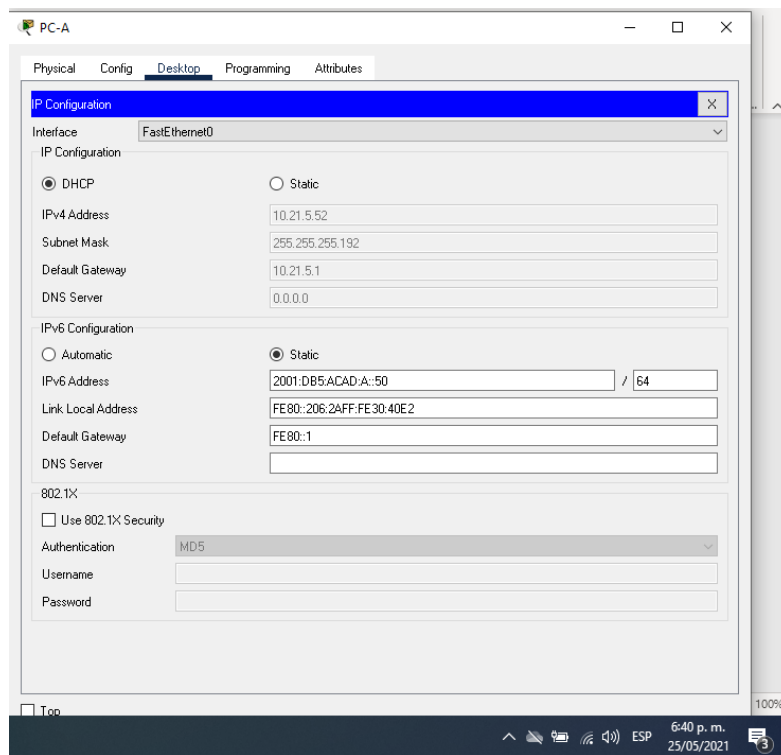


Figura 16 - Configuración PC-A

Tabla 10 - configuración de red para PC-B

Configuración de red de PC-B
------------------------------

Descripción	ccna-b.net
Dirección física	0040.0BB1.7818
Dirección IP	10.21.5.84
Máscara de subred	255.255.255.224
Gateway predeterminado	10.21.5.65
Gateway predeterminado IPv6	FE80::1

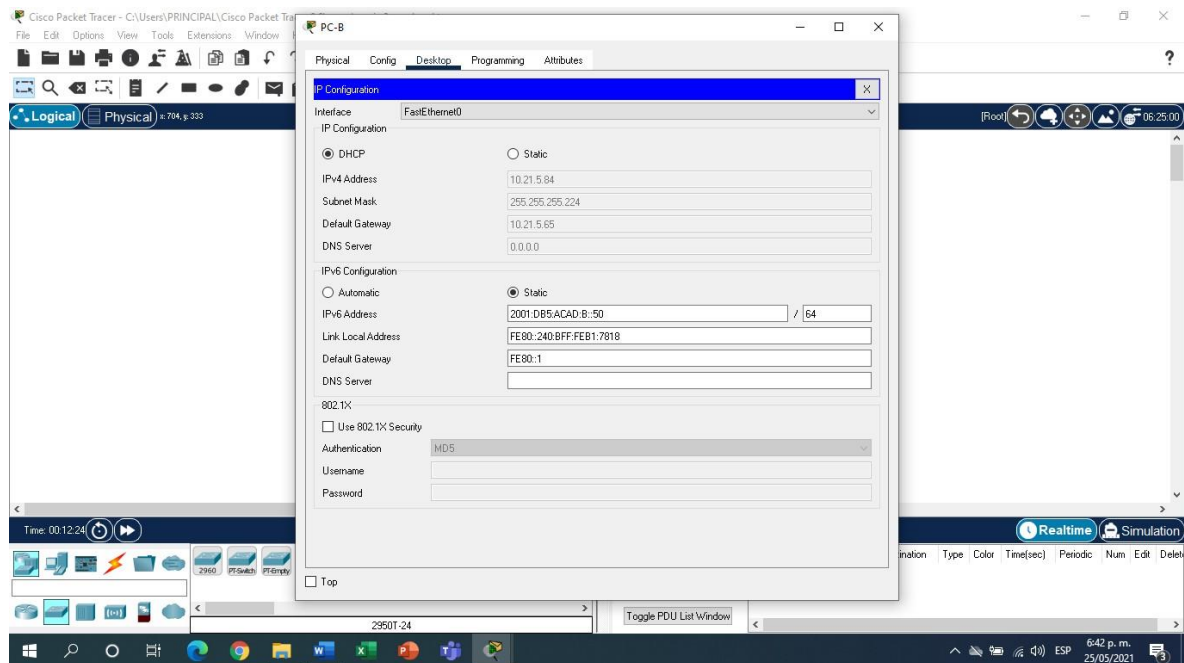


Figura 17 - Configuración PC-B

### 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 - Tabla de verificación*

<b>Desde</b>	<b>A</b>	<b>de Internet</b>	<b>Dirección IP</b>	<b>Resultados de ping</b>
PC-A	R1, G0/0/1.2	Dirección	10.21.5.1	Ping exitoso
		IPv6	2001:db5:acad:a::1	Ping exitoso
	R1, G0/0/1.3	Dirección	10.21.5.65	Ping exitoso
		IPv6	2001:db5:acad:b::1	Ping exitoso
	R1, G0/0/1.4	Dirección	10.21.5.97	Ping exitoso
		IPv6	2001:db5:acad:c::1	Ping exitoso
	S1, VLAN 4	Dirección	10.21.5.98	Ping exitoso
		IPv6	2001:db5:acad:c::98	Ping exitoso
	S2, VLAN 4	Dirección	10.21.5.99.	Ping exitoso
		IPv6	2001:db5:acad:c::99	Ping exitoso
	PC-B	Dirección	10.21.5.52	Ping exitoso
		IPv6	2001:db5:acad:b::50	Ping exitoso
	R1 Bucle 0	Dirección	209.165.201.1	Ping exitoso
		IPv6	2001:db8:acad:209::1	Ping exitoso
PC-B	R1 Bucle 0	Dirección	209.165.201.1	Ping exitoso
			2001:db8:acad:209::1	Ping exitoso

	IPv6	
--	------	--

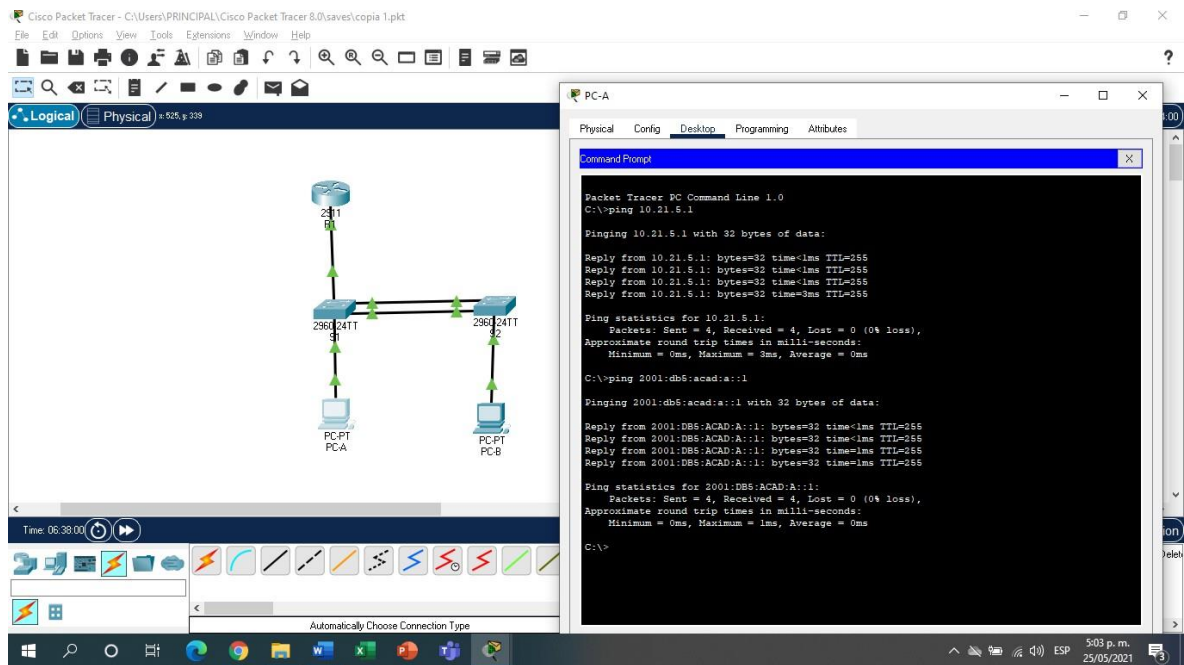


Figura 18 – Comando Ping desde PC-A a dirección 10.21.5.1 y 2001:db5:acad:a::1

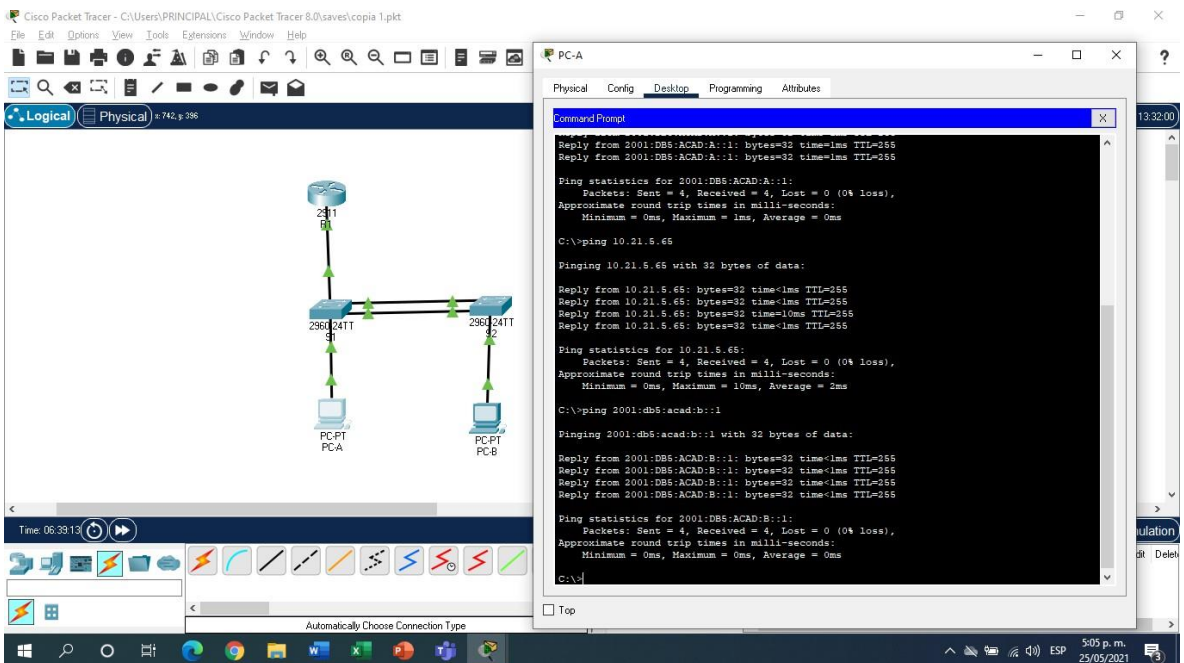


Figura 19 - Comando Ping desde PC-A a dirección 10.21.5.65 y 2001:db5:acad:b::1



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 2001:DB5:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:B::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB5:ACAD:B::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.21.5.97

Pinging 10.21.5.97 with 32 bytes of data:

Reply from 10.21.5.97: bytes=32 time<1ms TTL=255
Reply from 10.21.5.97: bytes=32 time<1ms TTL=255
Reply from 10.21.5.97: bytes=32 time<1ms TTL=255
Reply from 10.21.5.97: bytes=32 time<1ms TTL=255

Ping statistics for 10.21.5.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 2001:db5:acad:c::1

Pinging 2001:db5:acad:c::1 with 32 bytes of data:

Reply from 2001:DB5:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:C::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB5:ACAD:C::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figura 20 - Comando Ping desde PC-A a dirección 10.21.5.97 y 2001:db5:acad:c::1

```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 10.21.5.98: bytes=32 time<1ms TTL=254
Ping statistics for 10.21.5.98:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.21.5.98

Pinging 10.21.5.98 with 32 bytes of data:

Reply from 10.21.5.98: bytes=32 time<1ms TTL=254
Reply from 10.21.5.98: bytes=32 time<1ms TTL=254
Reply from 10.21.5.98: bytes=32 time<3ms TTL=254
Reply from 10.21.5.98: bytes=32 time<1ms TTL=254

Ping statistics for 10.21.5.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 3ms

C:\>ping 2001:db5:acad:c::98

Pinging 2001:db5:acad:c::98 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB5:ACAD:C::98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 2001:db5:acad:c::98

Pinging 2001:db5:acad:c::98 with 32 bytes of data:
```

Figura 21 - Comando Ping desde PC-A a dirección 10.21.5.98 y 2001:db5:acad:c::98

```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 2001:db5:acad:c::99
Pinging 2001:db5:acad:c::99 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB5:ACAD:C::99:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
C:\>ping 10.21.5.52
Pinging 10.21.5.52 with 32 bytes of data:
Reply from 10.21.5.52: bytes=32 time<1ms TTL=128
Reply from 10.21.5.52: bytes=32 time=10ms TTL=128
Reply from 10.21.5.52: bytes=32 time=6ms TTL=128
Reply from 10.21.5.52: bytes=32 time<1ms TTL=128

Ping statistics for 10.21.5.52:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 4ms

C:\>ping 10.21.5.99
Pinging 10.21.5.99 with 32 bytes of data:
Reply from 10.21.5.99: bytes=32 time<1ms TTL=254
Reply from 10.21.5.99: bytes=32 time=12ms TTL=254
Reply from 10.21.5.99: bytes=32 time=11ms TTL=254
Reply from 10.21.5.99: bytes=32 time<1ms TTL=254

Ping statistics for 10.21.5.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 6ms

C:\>
```

Figura 22 - Comando Ping desde PC-A a dirección 10.21.5.52 y 10.21.5.99

```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 209.165.201.1
Pinging 209.165.201.1 with 32 bytes of data:
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time=3ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\>ping 2001:db8:acad:209::1
Pinging 2001:db8:acad:209::1 with 32 bytes of data:
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.
Reply from 2001:DB8:ACAD:A::1: Destination host unreachable.

Ping statistics for 2001:DB8:ACAD:209::1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
```

Figura 23 - Comando Ping desde PC-A a dirección 2001:db8:acad:209::1

```

PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 10.21.5.52: bytes=32 time=10ms TTL=128
Reply from 10.21.5.52: bytes=32 time=9ms TTL=128
Ping statistics for 10.21.5.52:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 5ms
C:\>ping 2001:db5:acad:b::50
Finging 2001:db5:acad:b::50 with 32 bytes of data:
Reply from 2001:DB5:ACAD:B::50: bytes=32 time<1ms TTL=127
Reply from 2001:DB5:ACAD:B::50: bytes=32 time<1ms TTL=127
Reply from 2001:DB5:ACAD:B::50: bytes=32 time<1ms TTL=127
Reply from 2001:DB5:ACAD:B::50: bytes=32 time<1ms TTL=127
Ping statistics for 2001:DB5:ACAD:B::50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 2001:db5:acad:209::1
Finging 2001:db5:acad:209::1 with 32 bytes of data:
Reply from 2001:DB5:ACAD:209::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:209::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:209::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:209::1: bytes=32 time<1ms TTL=255
Ping statistics for 2001:DB5:ACAD:209::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>

```

Figura 24 - Comando Ping desde PC-A a dirección 2001:db5:acad:b::50

Tabla 12 - Tabla de verificación 2

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-B	R1, G0/0/1.2	Dirección	10.21.5.1	Ping exitoso
		IPv6	2001:db5:acad:a::1	Ping exitoso
	R1, G0/0/1.3	Dirección	10.21.5.65	Ping exitoso
		IPv6	2001:db5:acad:b::1	ping exitoso

R1, G0/0/1.4	Dirección	10.21.5.97	Ping exitoso
	IPv6	2001:db5:acad:c::1	Ping exitoso
S1, VLAN 4	Dirección	10.21.5.98	Ping exitoso
	IPv6	2001:db5:acad:c::98	Ping exitoso
S2, VLAN 4	Dirección	10.21.5.99	Ping exitoso
	IPv6	2001:db5:acad:c::99	Ping exitoso

```

PC-B
Physical Config Desktop Programming Attributes
Command Prompt

Pinging 10.21.5.1 with 32 bytes of data:
Reply from 10.21.5.1: bytes=32 time<1ms TTL=255
Reply from 10.21.5.1: bytes=32 time<1ms TTL=255
Reply from 10.21.5.1: bytes=32 time<1ms TTL=255
Reply from 10.21.5.1: bytes=32 time=16ms TTL=255

Ping statistics for 10.21.5.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 16ms, Average = 4ms

C:\>ping 2001:db5:acad:a::1

Pinging 2001:db5:acad:a::1 with 32 bytes of data:
Reply from 2001:DB5:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:A::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB5:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.21.5.65

Pinging 10.21.5.65 with 32 bytes of data:
Reply from 10.21.5.65: bytes=32 time<1ms TTL=255
Reply from 10.21.5.65: bytes=32 time<1ms TTL=255
Reply from 10.21.5.65: bytes=32 time<1ms TTL=255
Reply from 10.21.5.65: bytes=32 time=10ms TTL=255

Ping statistics for 10.21.5.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
  
```

Figura 25 - Comando Ping desde PC-B a dirección 10.21.5.1, 2001:db5:acad:a::1 y 10.21.5.65

```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 2001:db5:acad:b::1
Pinging 2001:db5:acad:b::1 with 32 bytes of data:
Reply from 2001:DB5:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:B::1: bytes=32 time<1ms TTL=255
Ping statistics for 2001:DB5:ACAD:B::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 10.21.5.97
Pinging 10.21.5.97 with 32 bytes of data:
Reply from 10.21.5.97: bytes=32 time<1ms TTL=255
Reply from 10.21.5.97: bytes=32 time<1ms TTL=255
Reply from 10.21.5.97: bytes=32 time<1ms TTL=255
Reply from 10.21.5.97: bytes=32 time<1ms TTL=255
Ping statistics for 10.21.5.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 2001:db5:acad:c::1
Pinging 2001:db5:acad:c::1 with 32 bytes of data:
Reply from 2001:DB5:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:C::1: bytes=32 time<1ms TTL=255
```

Figura 26 - Comando Ping desde PC-B a dirección 2001:db5:acad:b::1, 10.21.5.97 y 2001:db5:acad:c::1

```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.21.5.98
Pinging 10.21.5.98 with 32 bytes of data:
Reply from 10.21.5.98: bytes=32 time<1ms TTL=254
Reply from 10.21.5.98: bytes=32 time=12ms TTL=254
Reply from 10.21.5.98: bytes=32 time<1ms TTL=254
Reply from 10.21.5.98: bytes=32 time<1ms TTL=254
Ping statistics for 10.21.5.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 3ms
C:\>ping 2001:db5:acad:c::98
Pinging 2001:db5:acad:c::98 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 2001:DB5:ACAD:C::98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 10.21.5.99
Pinging 10.21.5.99 with 32 bytes of data:
Reply from 10.21.5.99: bytes=32 time<1ms TTL=254
Reply from 10.21.5.99: bytes=32 time=12ms TTL=254
Reply from 10.21.5.99: bytes=32 time=12ms TTL=254
Reply from 10.21.5.99: bytes=32 time<1ms TTL=254
Ping statistics for 10.21.5.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Figura 27 - Comando Ping desde PC-B a dirección 10.21.5.98, 2001:db5:acad:c::98 y 10.21.5.99

## 4.2 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.

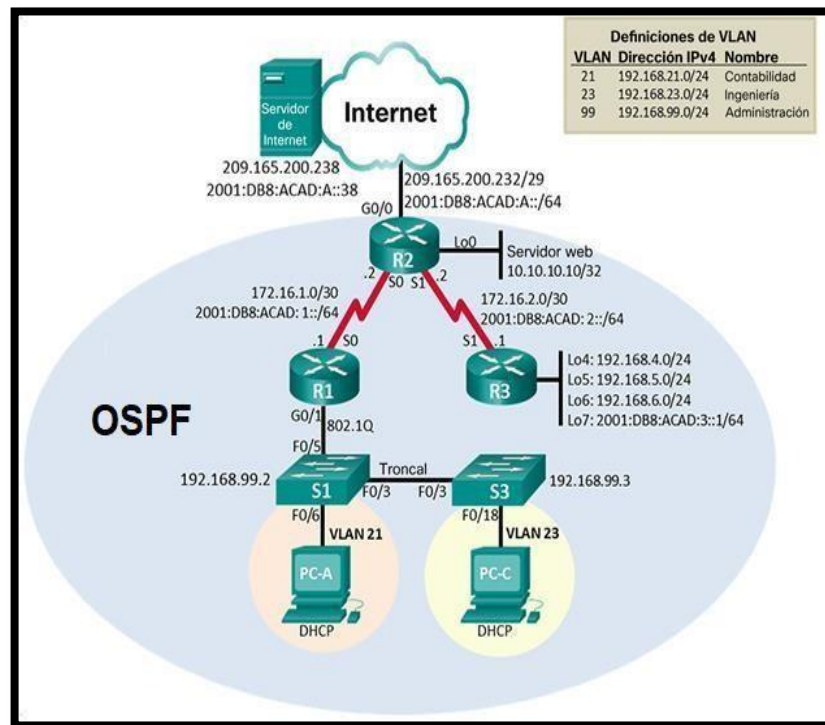


Figura 28 - Escenario 2

## Parte 1: Inicializar dispositivos

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

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

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

*Tabla 13 - Configuración escenario 2*

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>ENA Router#erase star Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]y[OK] Erase of nvram: complete
Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm]
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>ena Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]y[OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm]y

<p>Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches</p>	<pre>Switch&gt;ena Switch#show fla Switch#show flash: Directory of flash:/  1 -rw- 4670455 &lt;no date&gt; 2960-lanbasek9- mz.150-2.SE4.bin  64016384 bytes total (59345929 bytes free)</pre>
---	---

Se realiza el procedimiento con los 3 Routers

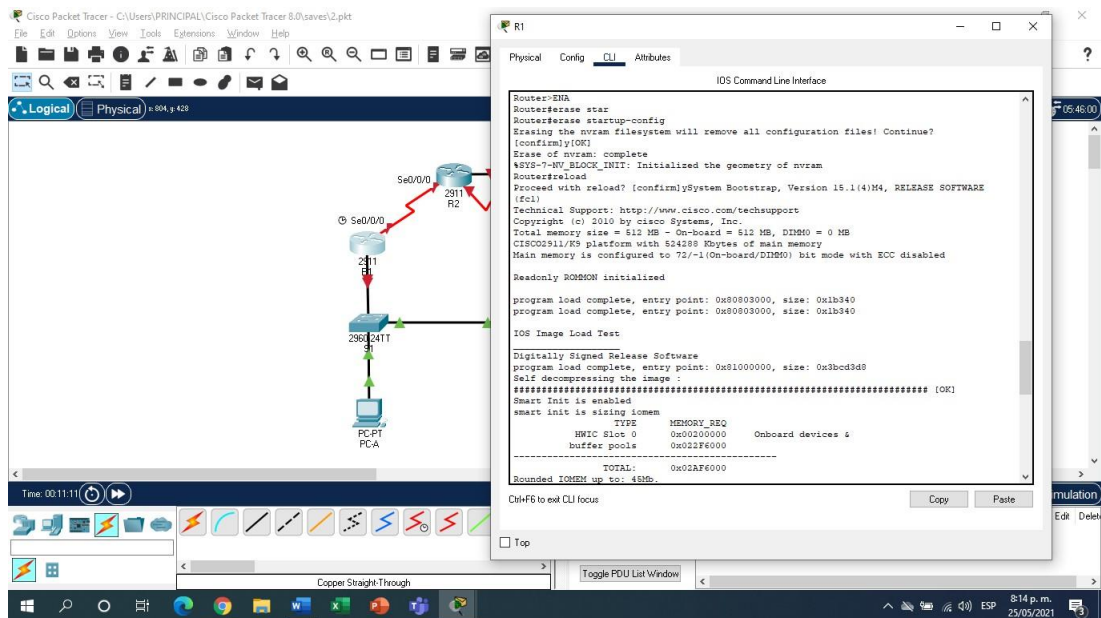


Figura 29 - Configuración de los 3 Routers

Se realiza el procedimiento con los 2 Switches



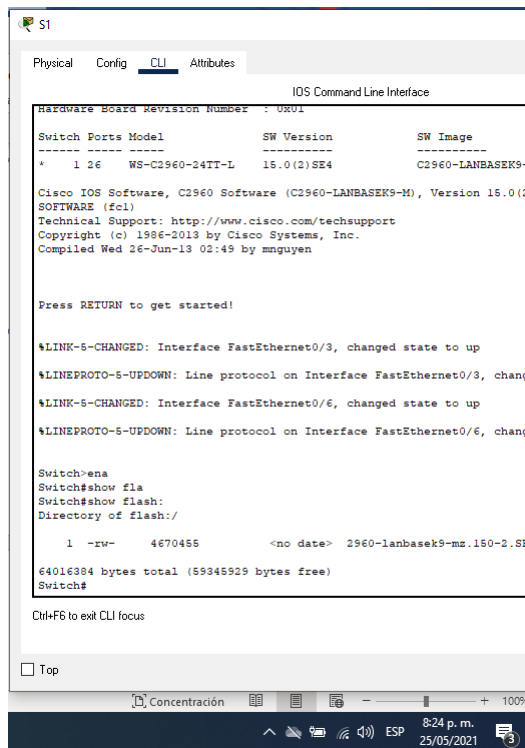


Figura 30 - Configuración en los 2 Switches

Show Flash:

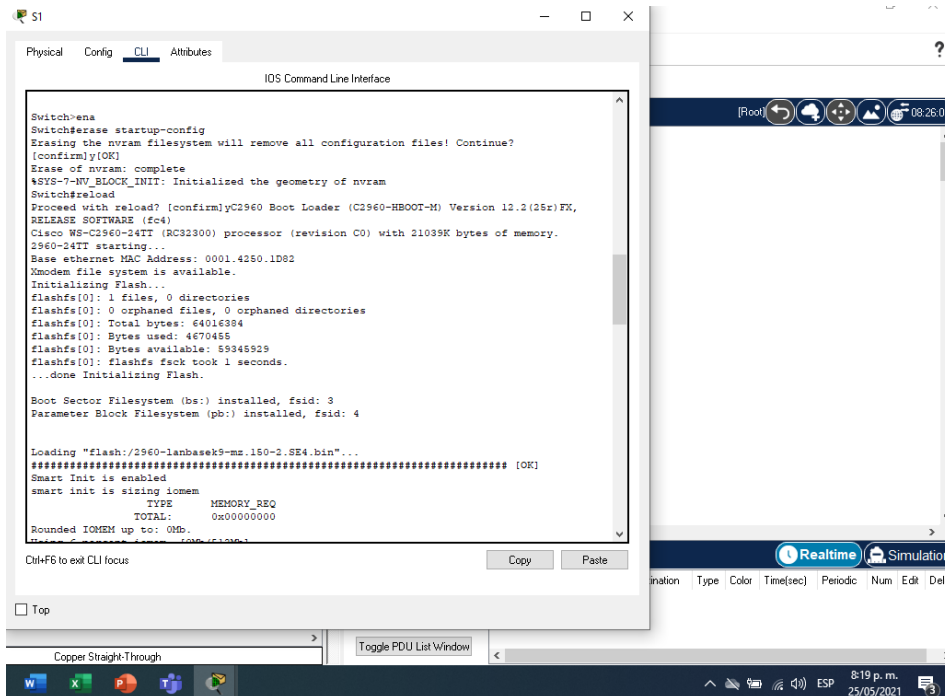


Figura 31 - Comando Show Flash

**Parte 2: Configurar los parámetros básicos de los dispositivos**

**Paso 1: Configurar la computadora de Internet**

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

*Tabla 14 – Configuración de la computadora de Internet*

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

**Paso 2: Configurar R1**

Las tareas de configuración para R1 incluyen las siguientes:

*Tabla 15 - Configuración para R1*

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
Desactivar la búsqueda DNS	Router>ena Router#conf ter Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class

Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/0/0	R1(config)#interface serial 0/0/0 R1(config-if)#description R1 a R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown %LINK-5-CHANGED: Interface Serial0/0/0, changed state to down R1(config-if)#exit
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 %Default route without gateway, if not a point-to-point interface, may impact performance R1(config)#ipv6 route ::/0 s0/0/0

	R1(config)#ipv6 unicast-routing R1(config)#exit
--	--

## Router1

```

Router>ena
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd #Se prohíbe el acceso no autorizado#
R1(config)#interface serial 0/0/0
R1(config-if)#description R1 a R2
R1(config-if)#ip address 172.16.1.1
% Incomplete command.
R1(config-if)#255.255.255.252
^
% Invalid input detected at '^' marker.

R1(config-if)#ip
R1(config-if)#ip
R1(config-if)#ip ad
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

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit

```

Figura 32 - Configuración en Router1

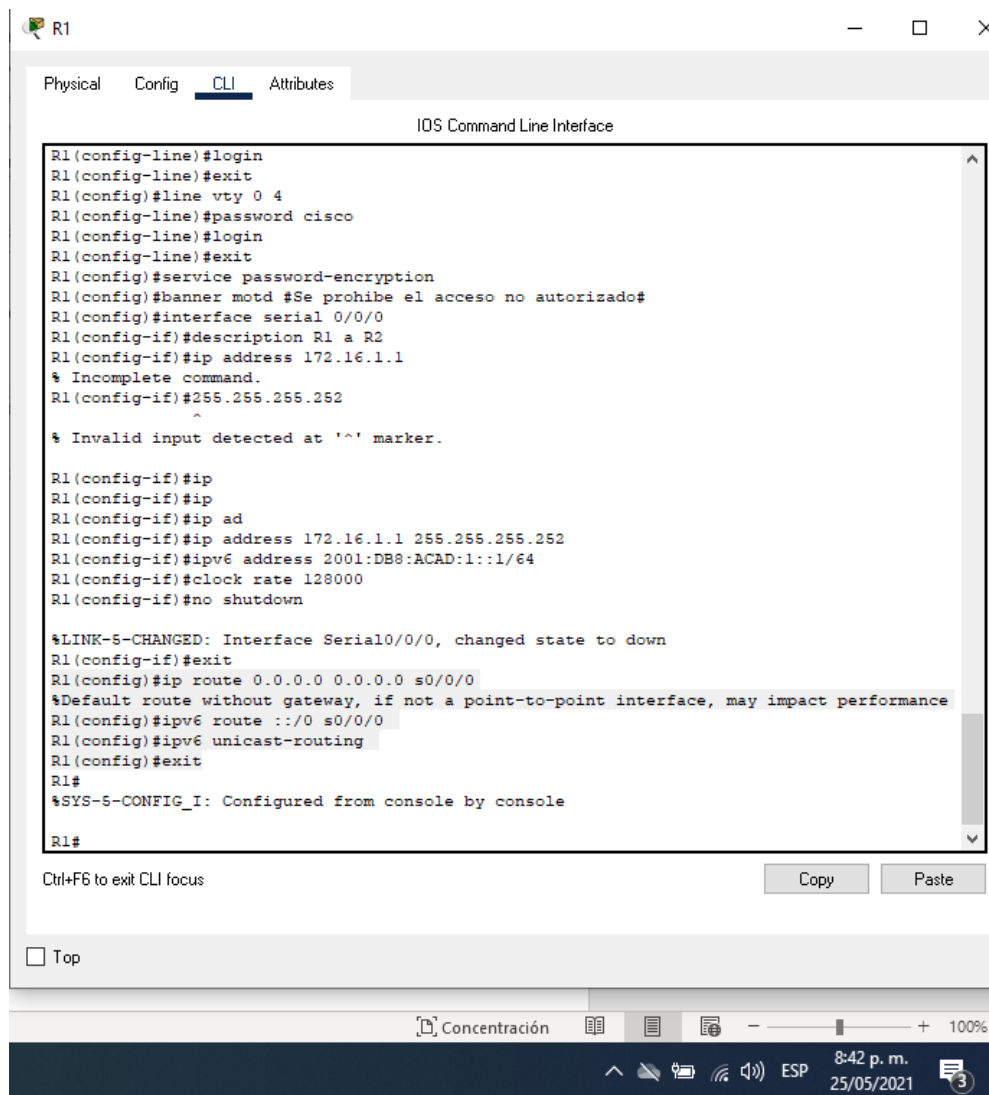


Figura 33 - Configuración en Router1

### Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 16 - Configuración en Router2

Elemento o tarea de configuración	Especificación
-----------------------------------	----------------

Desactivar la búsqueda DNS	Router>ena Router#conf term Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line con 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit R2(config)#
Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	
Mensaje MOTD	R2(config)#banner motd #Se prohibe el acceso no autorizado#
Interfaz S0/0/0	R2(config)#interface serial 0/0/0 R2(config-if)#description R1 a R2 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 shutd
Interfaz S0/0/1	R2(config-if)#exit R2(config)#interface serial 0/0/1 R2(config-if)#description R2 a R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutd
Interfaz G0/0 (simulación de Internet)	R2(config-if)#exit R2(config)#interface gigabitEthernet 0/0 R2(config-if)#description R2 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 shutd
Interfaz loopback 0 (servidor web simulado)	R2(config-if)#interface lo0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#exit
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/0 %Default route without gateway, if not a point-to-point interface, may impact performance R2(config)#ipv6 route ::/0 gigabitEthernet 0/0 R2(config)#

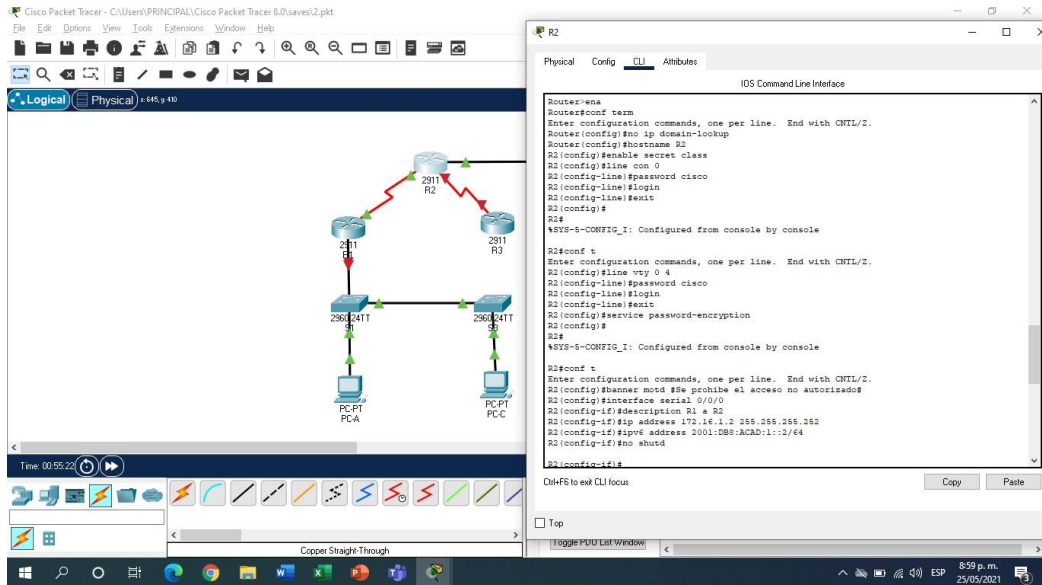


Figura 34 - Configuración en Router2

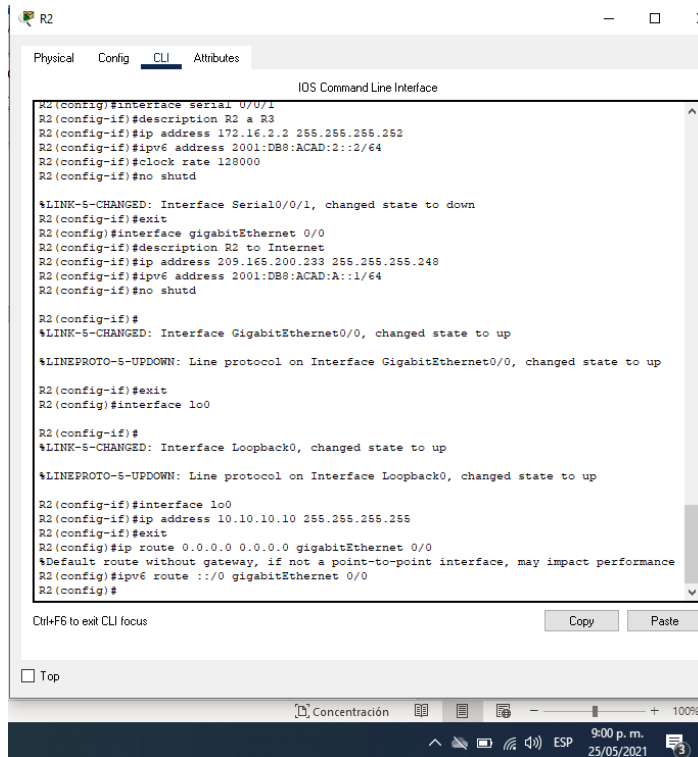


Figura 35 - Configuración en Router2



#### Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 17 - Configuración para R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enabl Router#conf ter Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line con 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Contraseña de acceso Telnet	R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #Se prohíbe el acceso no autorizado#
	R3(config)#interface serial 0/0/1 R3(config-if)#description R3 a R2

Interfaz S0/0/1	<pre>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 shutd</pre>
Interfaz loopback 4	<pre>R3(config-if)#interface lo4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#no shutd R3(config-if)#exit</pre>
Interfaz loopback 5	<pre>R3(config-if)#interface lo5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#no shut R3(config-if)#exit R3(config)#interface lo6</pre>
Interfaz loopback 6	<pre>R3(config-if)#interface lo6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#no shut R3(config-if)#exit</pre>
Interfaz loopback 7	<pre>R3(config-if)#interface lo7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#exit R3(config)#ipv6 unicast-routing R3(config)#</pre>
Rutas predeterminadas	<pre>R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1</pre>

%Default route without gateway, if not a point-to-point interface, may impact performance  
R3(config)#ipv6 route ::/0 s0/0/1

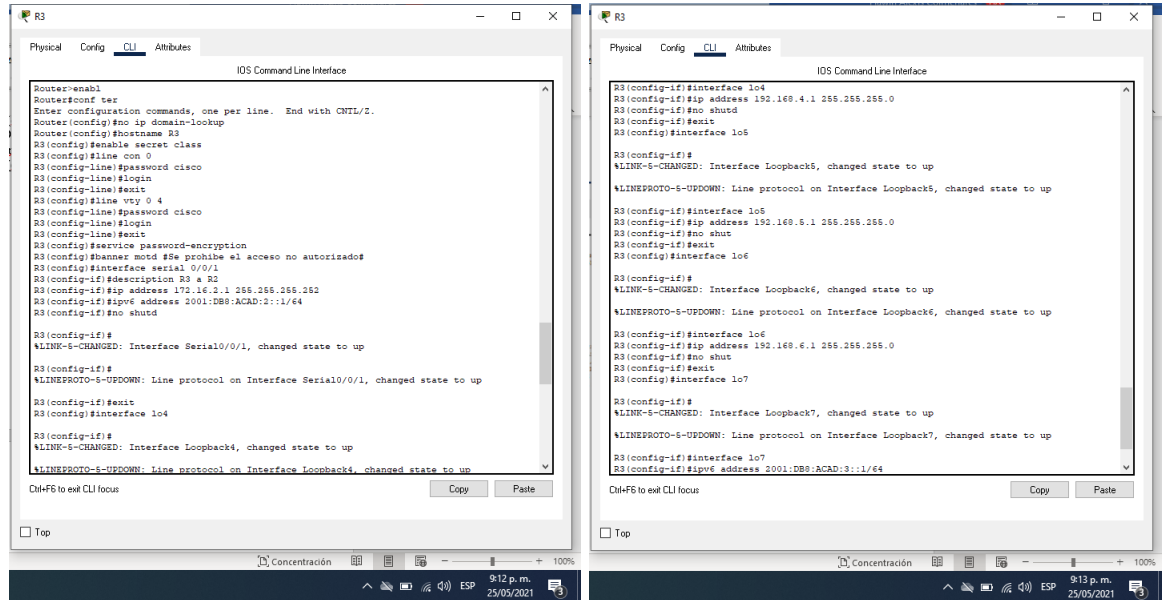


Figura 36 - Configuración en Router3

### Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 18 - Configuración para el S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#conf ter Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup

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

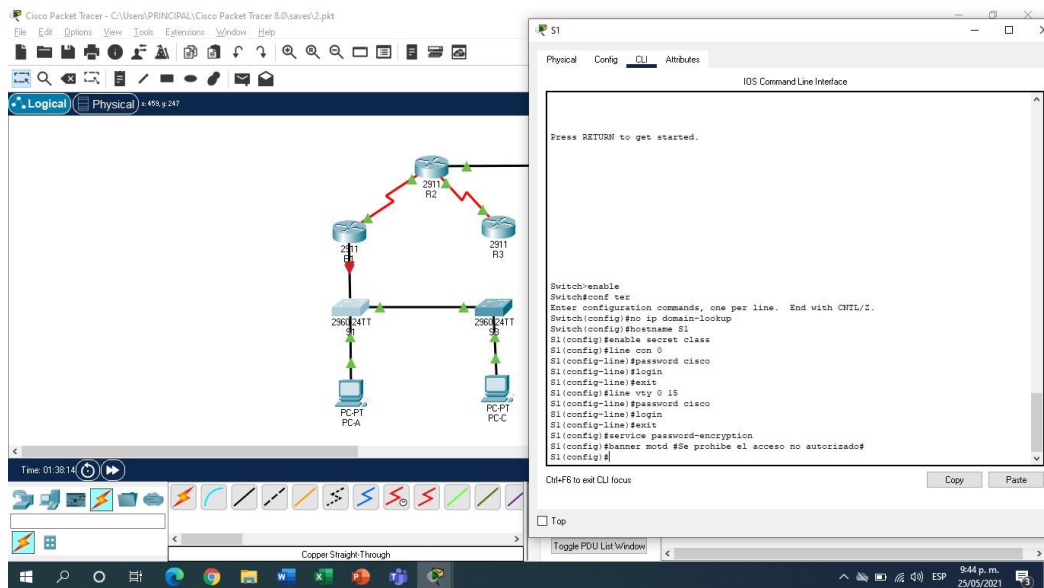


Figura 37 - Configuración del S1

## Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 19 - Configuración del S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#conf ter Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line con 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Contraseña de acceso Telnet	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd #Se prohíbe el acceso no autorizado#

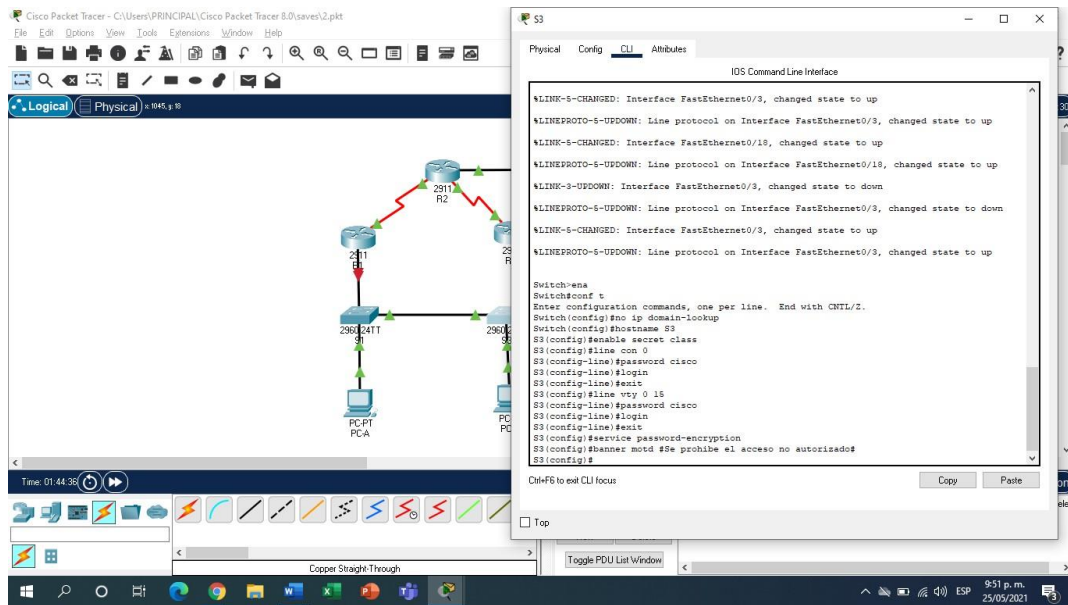


Figura 38 - Configuración del S3

### Paso 7: Verificar la conectividad de la red

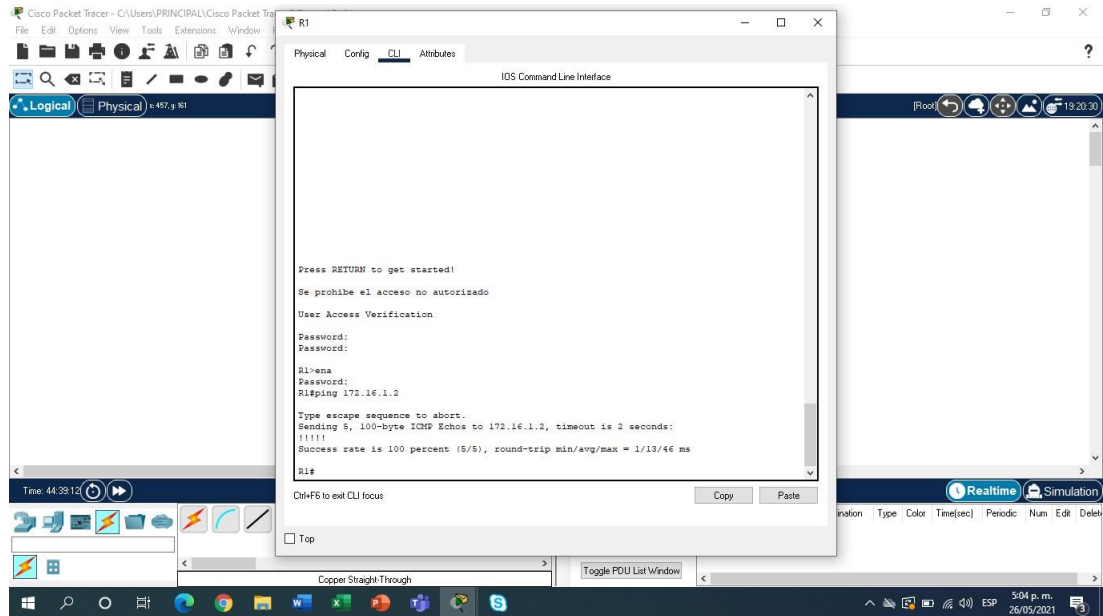
Utilice el comando ping para probar la conectividad entre los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 20 - Tabla de verificar

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/13/46 ms

R2	R3, S0/0/1	172.16.2.1	Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/7 ms
PC de Internet	Gateway predeterminado	209.165.200.233	Reply from 209.165.200.233: bytes=32 time<1ms TTL=255  Ping statistics for 209.165.200.233: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 38ms, Average = 9ms

## R1 a R2



*Figura 39 - Verificación con comando ping de R1 a R2*

R2 a R3

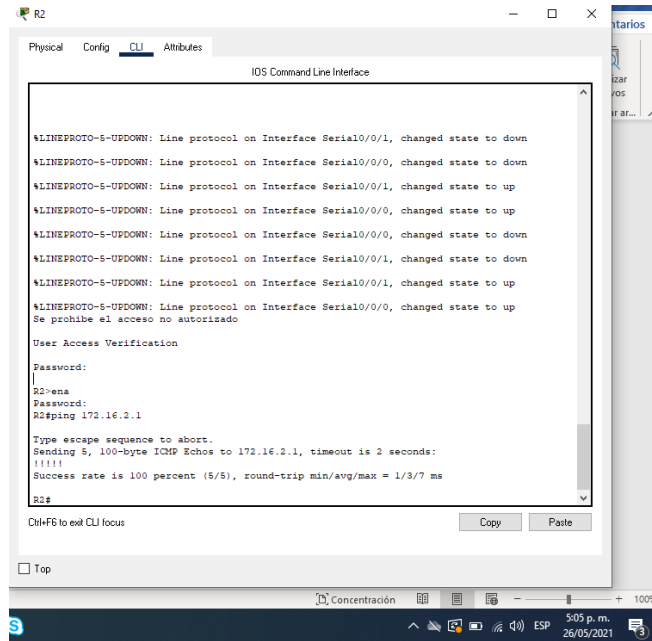


Figura 40 - Verificación con comando ping de R2 a R3

PC INTERNET a 209.165.200.233

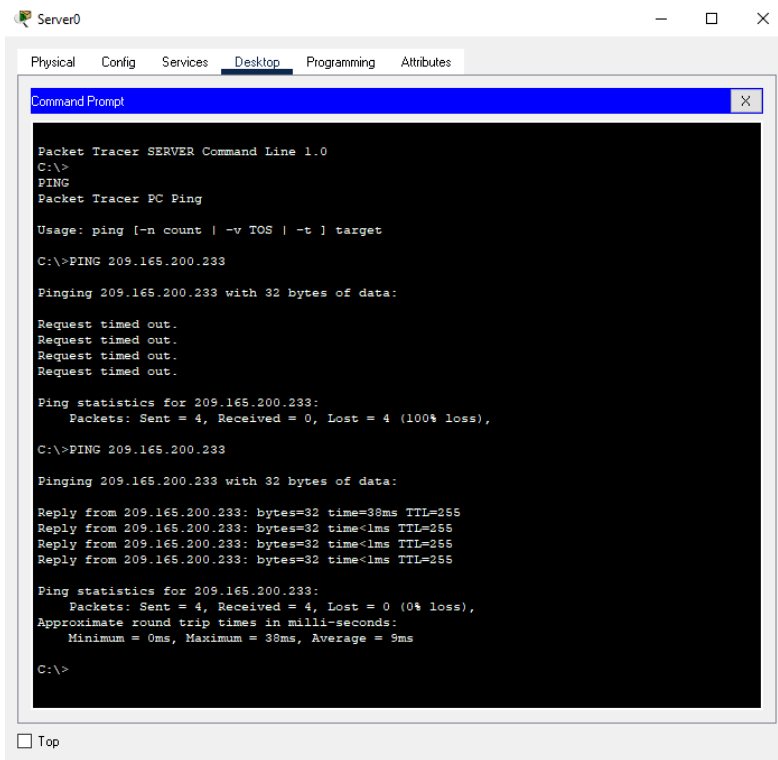


Figura 41 - Verificación con comando ping de PC INTERNET a 209.165.200.233



### 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 del S1*

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	<pre>S1&gt;ena Password: S1#conf t Enter configuration commands, one per line. End with CNTL/Z. 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</pre>
Asignar la dirección IP de administración.	<pre>S1(config)#interface vlan 99 S1(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up S1(config-if)#ip add 192.168.99.2 255.255.255.0 S1(config-if)#exit</pre>
Asignar el gateway predeterminado	<pre>S1(config)#ip default-gateway 192.168.99.1</pre>

Forzar el enlace troncal en la interfaz F0/3	S1(config)#interfa f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#exit S1(config)#interfa 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	S1(config)#interface range fa0/1-2, fa0/4, fa0/6-24 S1(config-if-range)#switchport mode access S1(config-if-range)#exit
Asignar F0/6 a la VLAN 21	S1(config)#interface range fa0/6 S1(config-if-range)#switchport access vlan 21 S1(config-if-range)#exit
Apagar todos los puertos sin usar	S1(config)#interface range fa0/1-2,fa0/4,fa0/7-24,gi0/1-2 S1(config-if-range)#shutdown

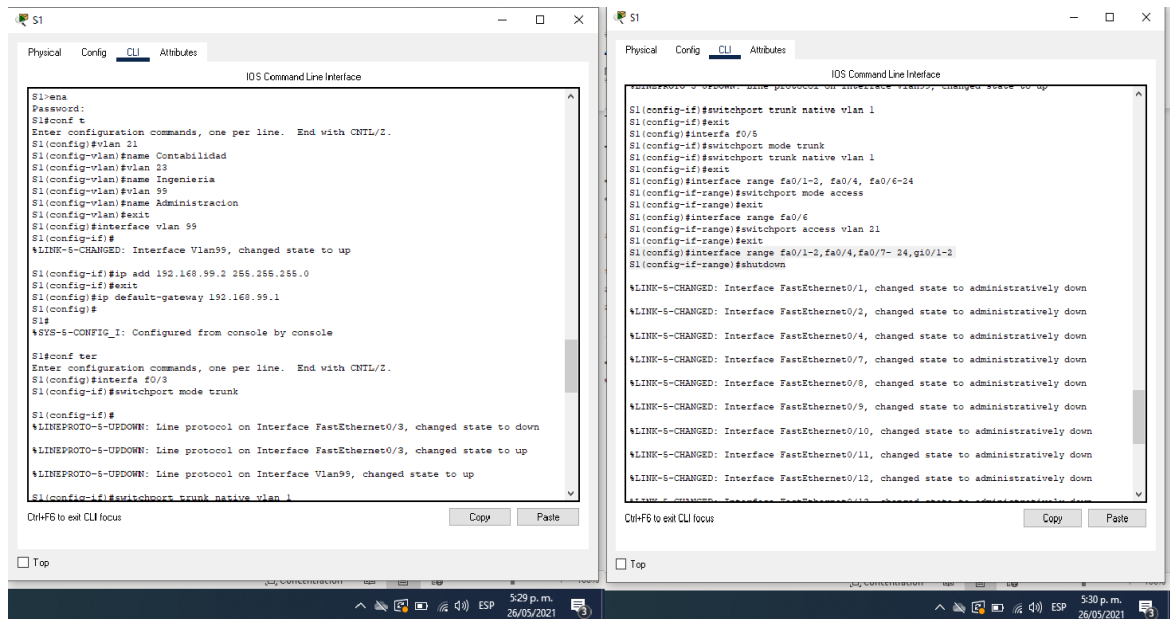


Figura 42 -Configuración del S1

## Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 22 - Configuración el S3

Elemento o tarea de configuración	Especificación
<p>Crear la base de datos de VLAN</p>	<pre>S3&gt;ena Password: S3#conf t Enter configuration commands, one per line. End with CNTL/Z. S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99</pre>

	S3(config-vlan)#name Administracion S3(config-vlan)#exit
Asignar la dirección IP de administración	S3(config)#interface vlan 99 S3(config-if)#ip add 192.168.99.3 255.255.255.0 S3(config-if)#exit
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#ip default-gateway 192.168.99.1 S3(config)#interface fastEthernet 0/3 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	S3(config)#interface range fa0/1-2,fa0/4-24,gi0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#exit
Asignar F0/18 a la VLAN 21	S3(config)#interface fastEthernet 0/18 S3(config-if)#switchport access vlan 21 S3(config-if)#exit
Apagar todos los puertos sin usar	S3(config)#interface range fa0/1-2,fa0/4-17,fa0/19-24,gi0/1-2 S3(config-if-range)#shutdown

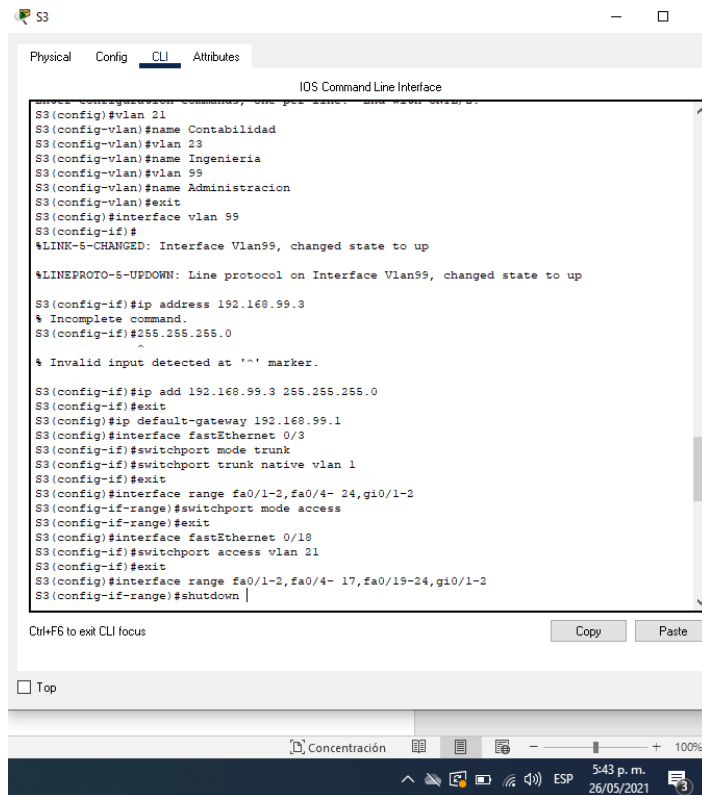


Figura 43 - Configuración el S3

### Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 23 - Configuración para R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	<pre> R1(config)#int g0/1.21 R1(config-subif)#description accounting LAN de Contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip add 192.168.21.1 255.255.255.0 R1(config-subif)#exit           </pre>

<p>Configurar la subinterfaz 802.1Q .23 en G0/1</p>	<pre>R1(config)#interface gigabitEthernet 0/1.23 R1(config-subif)#description accounting LAN de Ingenieria R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip add 192.168.23.1 255.255.255.0 R1(config-subif)#exit</pre>
<p>Configurar la subinterfaz 802.1Q .99 en G0/1</p>	<pre>R1(config)#interface gigabitEthernet 0/1.99 R1(config-subif)#description accounting LAN de Administracion R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip add 192.168.99.1 255.255.255.0 R1(config-subif)#exit</pre>
<p>Activar la interfaz G0/1</p>	<pre>R1(config)#int g0/1 R1(config-if)#no shut</pre>

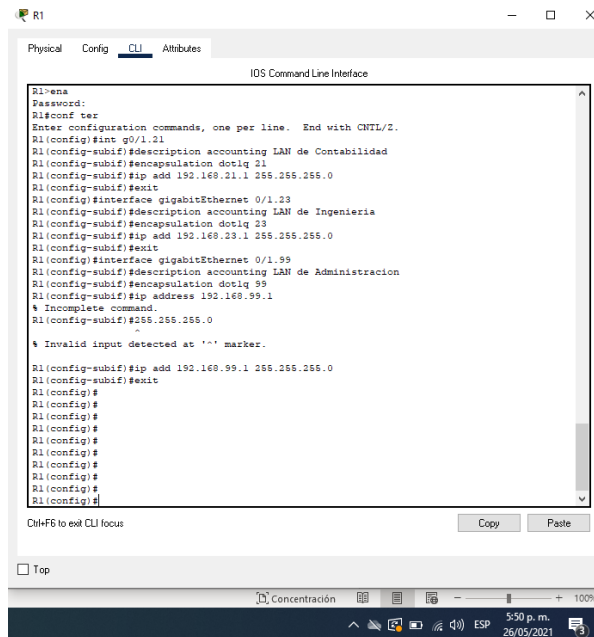


Figura 44 - Configuración para R1

#### 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 - Tabla de verificación

Desde	A	Dirección IP	Resultados de 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
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

			= 0/0/3 ms
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 = 0/0/0 ms
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 = 0/6/34 ms

Switch 1



```
S1
Physical Config CLI Attributes
IOS Command Line Interface

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
Se prohíbe el acceso no autorizado

User Access Verification

Password:
S1>ena
Password:
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 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

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

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 = 0/0/0 ms

S1#
```

Figura 45- Configuración del Switch 1

### Switch 3

```
S3
Physical Config CLI Attributes
IOS Command Line Interface

Se prohíbe el acceso no autorizado

User Access Verification

Password:
S3>ena
Password:
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 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

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 = 0/0/3 ms

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 = 0/6/34 ms

S3#
```

Figura 46 - Configuración del Switch 3

## 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 del protocolo de routing dinámico OSPF para R1*

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

```

R1
Physical Config CLI Attributes
IOS Command Line Interface
$LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Se prohíbe el acceso no autorizado

User Access Verification

Password:

R1>enab
Password:
R1#conf ter
Enter configuration commands, one per line. End with CNTRL/Z.
R1(config)#router ospf 1
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0
R1(config-router)#network 192.168.23.0 0.0.0.255 area
% Incomplete command.
R1(config-router)#0
^
% Invalid input detected at '^' marker.

R1(config-router)#network 192.168.23.0 0.0.0.255 area
% Incomplete command.
R1(config-router)#0
^
% Invalid input detected at '^' marker.

R1(config-router)#network 192.168.23.0 0.0.0.255 area 0
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
R1(config-router)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
R1(config-router)#no auto
R1(config-router)#no auto-suma
R1(config-router)#no auto-sum
R1(config-router)#no auto-summary
Ctrl+F6 to exit CLI focus
Copy Paste
 Top

```

Figura 47 - Configuración del protocolo de routing dinámico OSPF para R1

## Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 26 - Configuración del protocolo de routing dinámico OSPF para R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1
Anunciar las redes conectadas directamente	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 209.165.200.232 0.0.0.7 area 0

Establecer la interfaz LAN (loopback) como pasiva	passive-interface lo0
Desactive la sumarización automática	R1(config-router)#no auto-summary

```

R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2 (config)#router ospf 1
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 209.165.200.232 0.0.0.7 area 0
R2 (config-router)#passive-interface lo0
R2 (config-router)#no auto-summary
R2 (config-router)#

```

Figura 48 - Configuración del protocolo de routing dinámico OSPF para R2

### Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 27 – Configuración del protocolo OSPFv3 en el R3

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

Anunciar redes IPv4 conectadas directamente	<pre>R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0</pre>
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	<pre>R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6</pre>
Desactive la sumarización automática.	<pre>R3(config-router)#no auto-summary</pre>

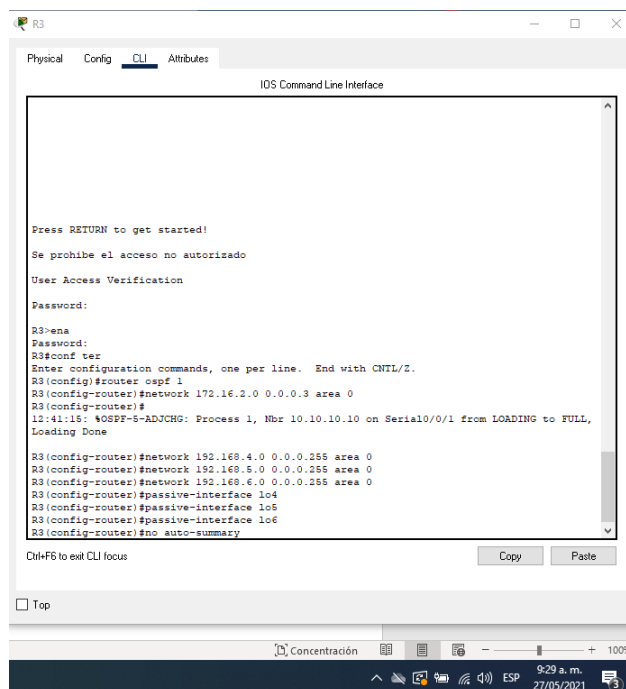


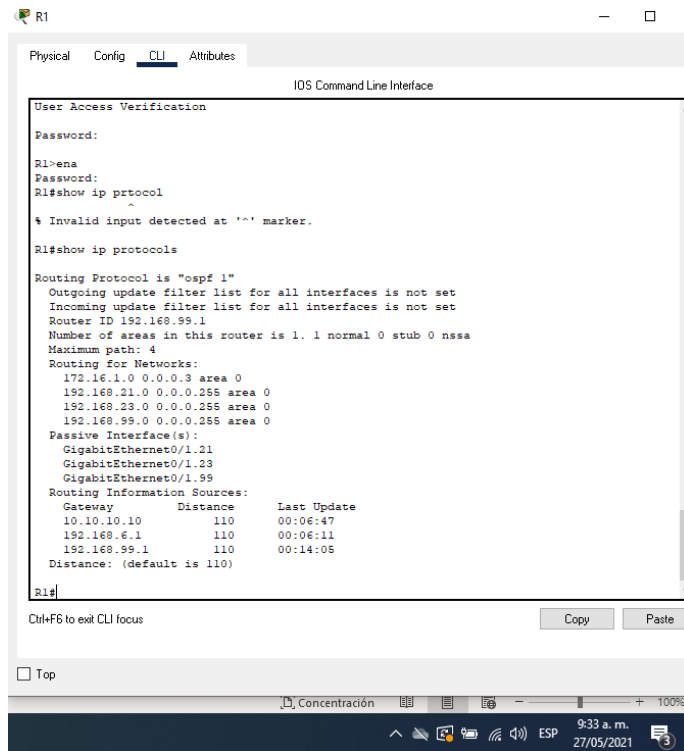
Figura 49 - Configuración del protocolo OSPFv3 en el R3

#### 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 – Tabla de verificación de la información de OSPF

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



```
R1
Physical Config CLI Attributes
IOS Command Line Interface
User Access Verification
Password:
R1>ena
Password:
R1#show ip protocol
% Invalid input detected at '^' marker.
R1#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.99.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.3 area 0
    192.168.21.0 0.0.0.255 area 0
    192.168.23.0 0.0.0.255 area 0
    192.168.99.0 0.0.0.255 area 0
  Passive Interface(s):
    GigabitEthernet0/1.21
    GigabitEthernet0/1.23
    GigabitEthernet0/1.99
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.10.10      110          00:06:47
    192.168.6.1      110          00:06:11
    192.168.99.1     110          00:14:05
  Distance: (default is 110)
R1#
```

Figura 50 - Verificación de la información de OSPF en R1

```

R1
Physical Config CLI Attributes
IOS Command Line Interface
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 192.168.99.1
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
 172.16.1.0 0.0.0.3 area 0
 192.168.21.0 0.0.0.255 area 0
 192.168.23.0 0.0.0.255 area 0
 192.168.99.0 0.0.0.255 area 0
Passive Interface(s):
 GigabitEthernet0/1.21
 GigabitEthernet0/1.23
 GigabitEthernet0/1.99
Routing Information Sources:
 Gateway Distance Last Update
 10.10.10.10 110 00:06:47
 192.168.6.1 110 00:06:11
 192.168.99.1 110 00:14:05
Distance: (default is 110)

R1#show ip route ospf
 172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O 172.16.2.0 [110/128] via 172.16.1.2, 00:16:09, Serial0/0/0
O 192.168.4.0/32 is subnetted, 1 subnets
O 192.168.4.1 [110/129] via 172.16.1.2, 00:09:19, Serial0/0/0
O 192.168.5.0/32 is subnetted, 1 subnets
O 192.168.5.1 [110/129] via 172.16.1.2, 00:08:59, Serial0/0/0
O 192.168.6.0/32 is subnetted, 1 subnets
O 192.168.6.1 [110/129] via 172.16.1.2, 00:08:49, Serial0/0/0
O 209.165.200.0/29 is subnetted, 1 subnets
O 209.165.200.232 [110/65] via 172.16.1.2, 00:15:27, Serial0/0/0

R1#
R1#
Ctrl+FB to exit CLI focus
Copy Paste
Top
Concentración 9:37 a. m.
27/05/2021

```

Figura 51 - Comando de verificación show ip route OSPF en R1

```

R1
Physical Config CLI Attributes
IOS Command Line Interface
192.168.99.0 0.0.0.255 area 0
Passive Interface(s):
 GigabitEthernet0/1.21
 GigabitEthernet0/1.23
 GigabitEthernet0/1.99
Routing Information Sources:
 Gateway Distance Last Update
 10.10.10.10 110 00:06:47
 192.168.6.1 110 00:06:11
 192.168.99.1 110 00:14:05
Distance: (default is 110)

R1#show ip route ospf
 172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O 172.16.2.0 [110/128] via 172.16.1.2, 00:16:09, Serial0/0/0
O 192.168.4.0/32 is subnetted, 1 subnets
O 192.168.4.1 [110/129] via 172.16.1.2, 00:09:19, Serial0/0/0
O 192.168.5.0/32 is subnetted, 1 subnets
O 192.168.5.1 [110/129] via 172.16.1.2, 00:08:59, Serial0/0/0
O 192.168.6.0/32 is subnetted, 1 subnets
O 192.168.6.1 [110/129] via 172.16.1.2, 00:08:49, Serial0/0/0
O 209.165.200.0/29 is subnetted, 1 subnets
O 209.165.200.232 [110/65] via 172.16.1.2, 00:15:27, Serial0/0/0

R1#
R1#show ip ospf database
OSPF Router with ID (192.168.99.1) (Process ID 1)

Router Link States (Area 0)

Link ID ADV Router Age Seq# Checksum Link count
192.168.99.1 192.168.99.1 1215 0x80000005 0x000cd3 5
10.10.10.10 10.10.10.10 777 0x80000005 0x001f4c 5
192.168.6.1 192.168.6.1 741 0x80000005 0x00c5f6 5

R1#
Ctrl+FB to exit CLI focus
Copy Paste
Top
9:40 a. m.
27/05/2021

```

Figura 52 - Comando de verificación show ip route OSPF database en R1

## 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 para R1*

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.30
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.30
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#exit
Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#exit



```

R1
Physical Config CLI Attributes
IOS Command Line Interface
O 192.168.4.1 [110/129] via 172.16.1.2, 00:09:19, Serial0/0/0
O 192.168.5.0/32 is subnetted, 1 subnets
O 192.168.5.1 [110/129] via 172.16.1.2, 00:08:59, Serial0/0/0
O 192.168.6.0/32 is subnetted, 1 subnets
O 192.168.6.1 [110/129] via 172.16.1.2, 00:08:49, Serial0/0/0
O 209.165.200.0/29 is subnetted, 1 subnets
O 209.165.200.232 [110/65] via 172.16.1.2, 00:15:27, Serial0/0/0

R1#
R1#Show ip ospf database
      OSPF Router with ID (192.168.99.1) (Process ID 1)

      Router Link States (Area 0)

Link ID        ADV Router    Age           Seq#           Checksum
192.168.99.1   192.168.99.1  1215          0x80000005    0x00b2d3
10.10.10.10    10.10.10.10   777           0x80000005    0x001f4c
192.168.6.1    192.168.6.1   741           0x80000005    0x00c5f6

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.30
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.30
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#exit
R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#exit
R1(config)#

```

Figura 53 - Configuración para R1 con DHCP y NAT para IPv4

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

La configuración del R2 incluye las siguientes tareas:

Tabla 30 - Configuración del R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	N/A
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	N/A

Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.238
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interfac g0/0 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.232 209.165.200.237 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

```

R2
-----
Physical  Config  CLI  Attributes
-----
IOS Command Line Interface

Se prohíbe el acceso no autorizado
User Access Verification
Password:
R2>ena
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#user webuser privilege 15 secret cisco12345
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.238
R2(config-if)#interfac g0/0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255
R2(config)#ip nat pool INTERNET 209.165.200.232 209.165.200.237 netmask
* Incomplete command.
R2(config)#255.255.248
* Invalid input detected at '^' marker.

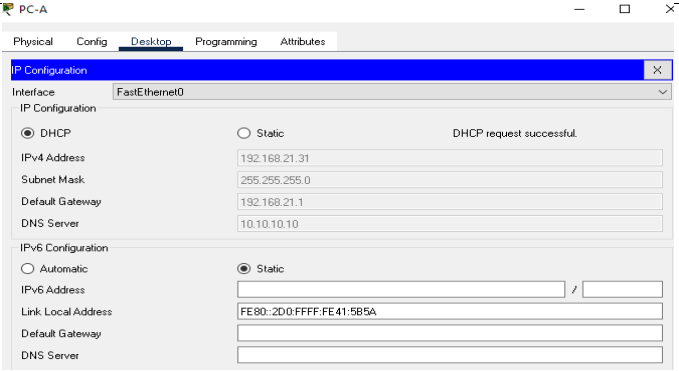
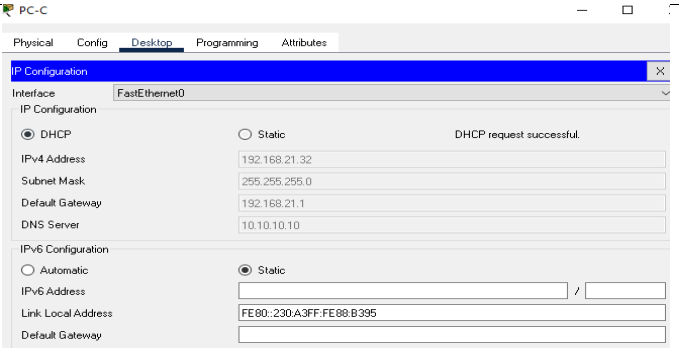
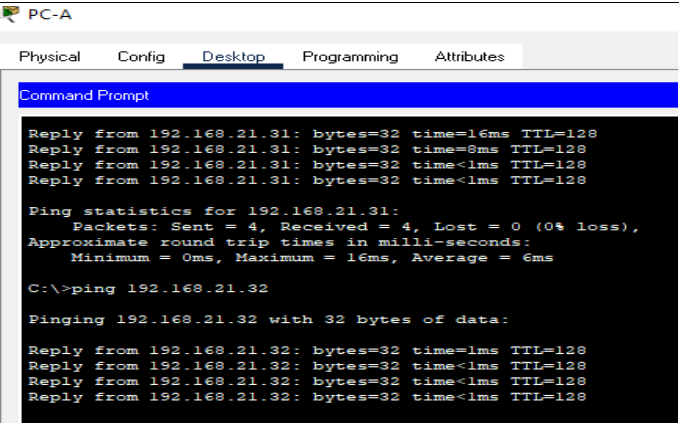
R2(config)#ip nat pool INTERNET 209.165.200.232 209.165.200.237 netmask 255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#

```

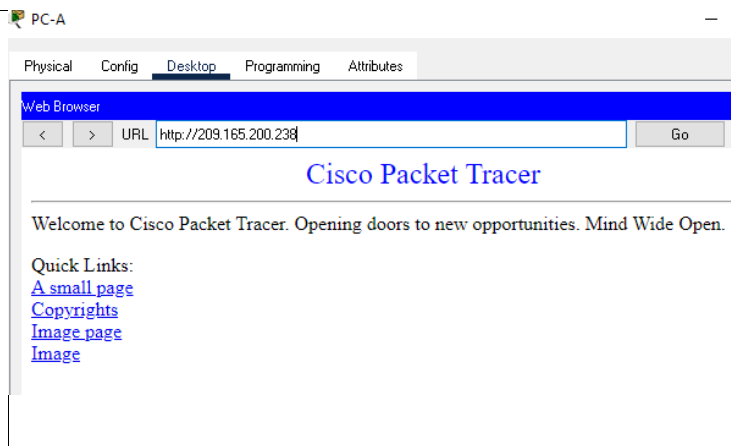
Figura 54 – Configuración de la NAT estática y dinámica en el R2

### 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.

Prueba	Resultados
<p>Verificar que la PC-A haya adquirido información de IP del servidor de DHCP</p>	
<p>Verificar que la PC-C haya adquirido información de IP del servidor de DHCP</p>	
<p>Verificar que la PC-A pueda hacer ping a la PC-C</p> <p><b>Nota:</b> Quizá sea necesario deshabilitar el firewall de la PC.</p>	 <pre> C:\&gt;ping 192.168.21.31  Reply from 192.168.21.31: bytes=32 time=16ms TTL=128 Reply from 192.168.21.31: bytes=32 time=8ms TTL=128 Reply from 192.168.21.31: bytes=32 time&lt;1ms TTL=128 Reply from 192.168.21.31: bytes=32 time&lt;1ms TTL=128  Ping statistics for 192.168.21.31:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 16ms, Average = 6ms  C:\&gt;ping 192.168.21.32  Pinging 192.168.21.32 with 32 bytes of data:  Reply from 192.168.21.32: bytes=32 time=1ms TTL=128 Reply from 192.168.21.32: bytes=32 time&lt;1ms TTL=128 Reply from 192.168.21.32: bytes=32 time&lt;1ms TTL=128 Reply from 192.168.21.32: bytes=32 time&lt;1ms TTL=128 </pre>

Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**



## Parte 6: Configurar NTP

Tabla 31 - Configuración del NTP en R1 y R2

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 11:40:50 13 May 2021
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1#show ntp status

R2

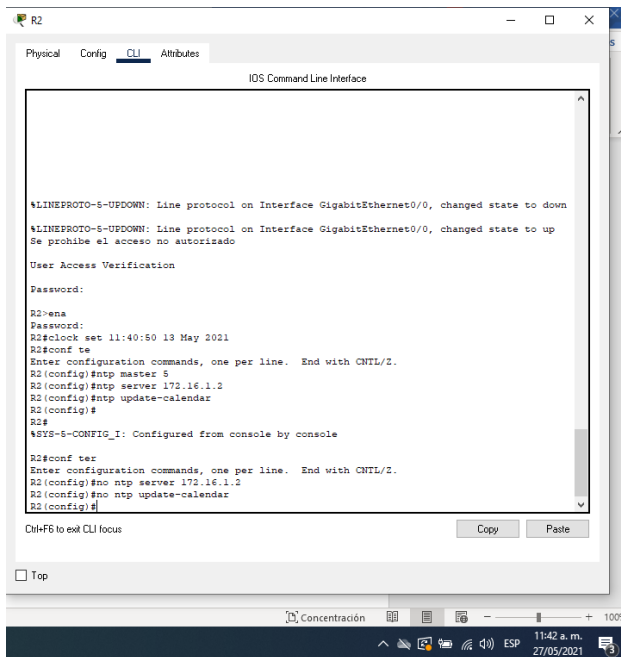


Figura 55 - Configuración del NTP en R2

R1

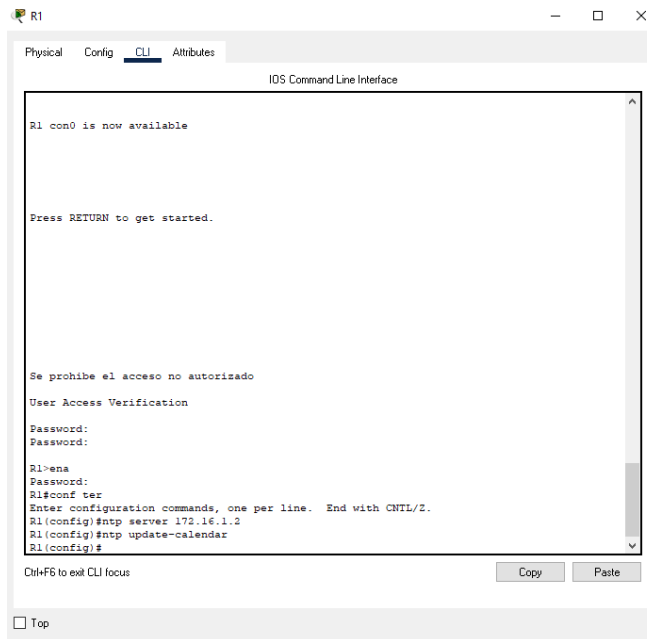


Figura 56 - Configuración del NTP en R1

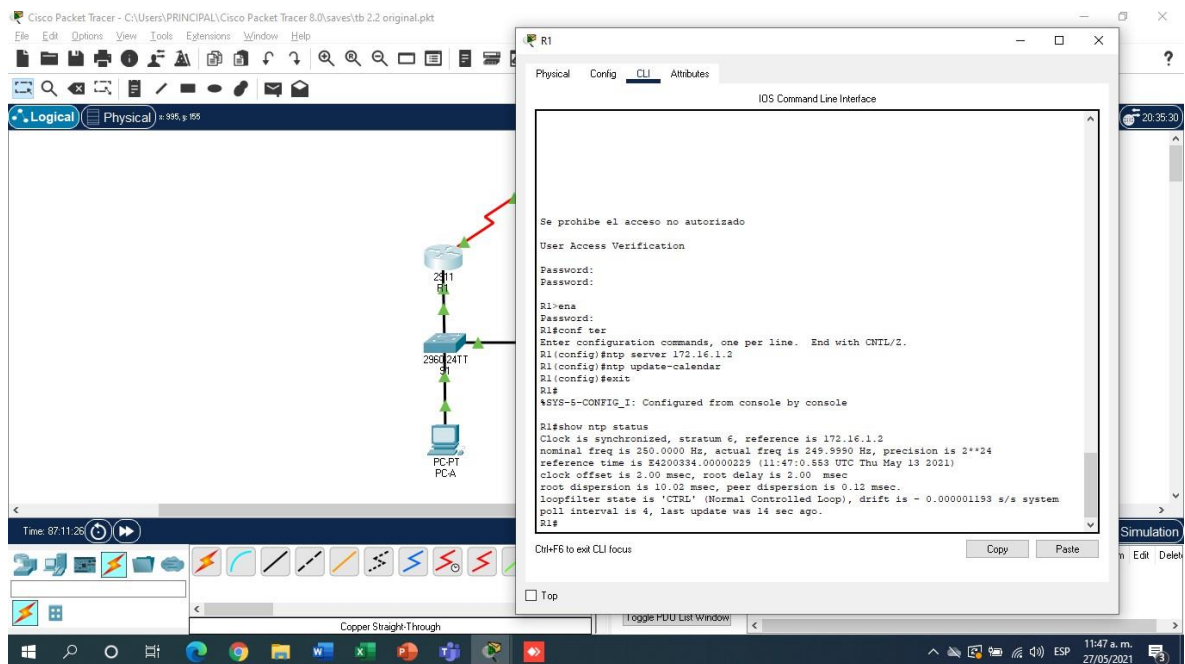


Figura 57 - Verifique la configuración de NTP en R1

## 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 32 - Verificación las listas de control

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

<p>Permitir acceso por Telnet a las líneas de VTY</p>	<pre>R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT % Incomplete command. R2(config-line)#access-class ADMIN-MGT in R2(config-line)#exit</pre>
<p>Verificar que la ACL funcione como se espera</p>	

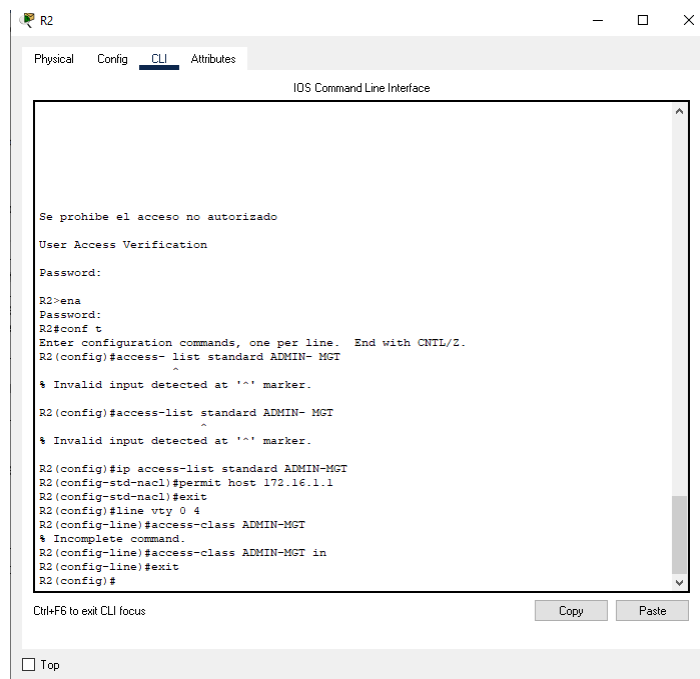


Figura 58 – Verificación de ACL en R2

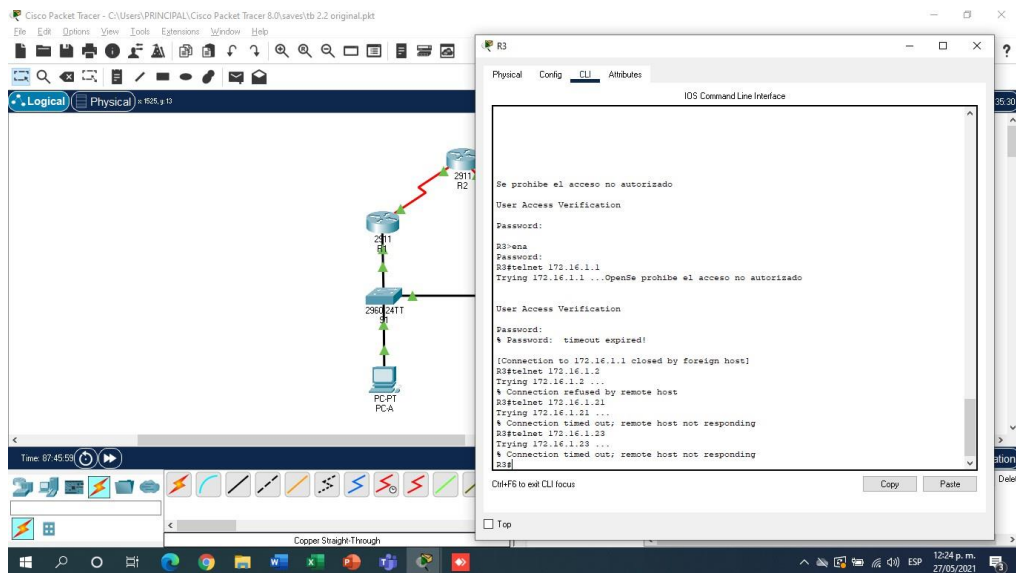


Figura 59 - Verificación de ACL en R3

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

Tabla 33 – Comando de configuración

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R1#show access-list
Restablecer los contadores de una lista de acceso	R1#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R1 (config)#interface Fa0/1 R1 (config-if)#ip access-group 1 out



<p>¿Con qué comando se muestran las traducciones NAT?</p>	<p>R1 (config)#show ip nat translations</p> <p>Las traducciones para la PC-A y la PC- C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.</p>
<p>¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?</p>	<p>R1(config)#clear ip nat translation</p>

## 6. CONCLUSIONES

Se logra realizar con éxito la topología de red solicitada para el caso de estudio, respetando la solicitud de la guía.

La programación de los routers se estableció de forma adecuada y funcionaron de manera correcta, asignación de nombre, contraseñas, banner, interfaces y demás. Logramos reunir información importante en cuanto a los principales componentes de nuestros equipos, sus modelos, fabricantes, como están constituidos, desarme y rearme de los mismos lo que nos ayuda a conocer mucho mejor su funcionamiento.

Se hizo la simulación en Packet tracer funcionando todos los dispositivos y además realizando las pruebas de conectividad.

La herramienta virtual Packet trace es de suma importancia para este tipo de proyectos, porque con la utilización y puesta en marcha de toda la estructura este programa podemos ver cómo funciona y como se programa este tipo de redes, facilitando tanto en diseño como en recursos económicos ya que no se tiene que empezar a realizar la red sin tener un datos virtuales de la misma

La realización de este tipo de proyectos hace que nos afiancemos más en el tema del módulo CCNA1 y CCNA2 porque realizando proyectos de esta envergadura podemos desarrollar más habilidades como estudiantes, para que cuando nos enfrentemos a la realidad se tengan los conceptos bien claros y definidos de cómo se diseña y fabrica este tipo de estructuras.

Para la configuración de una red no solo basta con configurar los dispositivos que controlar la fluidez de la información dentro de la red, sino que también tenemos

que resguardar su acceso por medio de protocolos, protegerlos con contraseñas y no dejarlos vulnerables a ataques que pueden dañar nuestra infraestructura de comunicación. Además no solo basta con conocer los diferentes modos de acceso, también debemos saber para qué utilizar cada uno de ellos.

Se comprendió todo el funcionamiento y programación que tenemos que distinguir y manejar con los protocolos para IPv6, los cuales son utilizados para poder realizar las comunicaciones, logrando una comunicación efectiva, también aprendimos a manejar y configurar el routing RIPv2 en todos los routers de la red, creando y verificando las tablas para su configuración, este tipo de prácticas logra que desarrollemos nuestras habilidades para los routers.

## 7. BIBLIOGRAFÍA

- Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1IlnWR0hoMxgBNv1CJ>
- Lammle, T. (2010). CISCO Press (Ed). Cisco Certified Network Associate Study Guide. Recuperado de <http://www.birminghamcharter.com/ourpages/auto/2012/3/22/41980164/C>
- Lucas, M. (2009). Cisco Routers for the Desperate: Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de <http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xw&AN=440032&lang=es&site=ehost-live>
- Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de <http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live>
- Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de <https://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf>
- Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). OSPF Implementation. Implementing Cisco IP Routing (ROUTE) Foundation

Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Basic Network and Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx>

## 8. ANEXOS

Link de los dos escenarios:

<https://drive.google.com/drive/folders/1dRH2uoOobytWsyMj3xVbmK8h6XGEwUzR?usp=sharing>