

Diplomado De Profundización Cisco (Diseño E Implementación De Soluciones
Integradas Lan / Wan)

Luis Carlos Aponza Varon

Universidad Nacional Abierta Y A Distancia UNAD
Escuela De Ciencias Básicas Tecnología E Ingeniería
Programa Ingeniería De Sistemas
Bogotá D.C.
Noviembre de 2020

Diplomado De Profundización Cisco (Diseño E Implementación De Soluciones
Integradas Lan / Wan)

Luis Carlos Aponza Varon

Trabajo escrito para optar por el título de: Ingeniería De Sistemas

Tutor

Ing. Jose Ignacio Cardona

Universidad Nacional Abierta Y A Distancia UNAD
Escuela De Ciencias Básicas Tecnología E Ingeniería
Programa Ingeniería De Sistemas
Bogotá D.C.
Noviembre de 2020

Dedicatoria

Mi trabajo final lo dedico primero a Dios que guía todos mis pasos para nunca me ha abandonado ni en los momentos más difíciles es mi guía eterna.

Segundo a mis padres y mi abuela que desde el cielo guían mis pasos y sé que están muy orgullosos de ver a su hijo convertido en un profesional.

Tercero a mi esposa e hija que han luchado a mi lado por ver mi sueño de ser profesional realizado...

Tabla De Contenido

Lista de Tablas	1
Lista de Figuras.....	2
Glosario	3
Resumen	4
Introducción	5
Objetivo General	6
Objetivos específicos	7
Descripción Del Escenario 1	8
Inicializar y Recargar y Configurar aspectos básicos de los dispositivos	9
Inicializar y volver a cargar el router y el switch	10
Configurar R1	11
Configure S1 y S2	12
Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)....	13
Configurar soporte de host	14
Configurar los servidores PC-A y PC-B PC-A.....	15
Probar y verificar la conectividad de extremo a extrem	16
Descripción Del Escenario 2.....	17
Inicializar y volver a cargar los routers y los switches	18
Configurar los parámetros básicos de los dispositivos.....	19
Configurar la seguridad del switch, las VLAN y el routing entre VLAN	20
Implementar DHCP y NAT para IPv4	21
Configurar NTP	22
Configurar y verificar las listas de control de acceso (ACL).....	23

Lista de Tablas

Escenario 1

Tabla 1 configurar r1.....	13
Tabla 2 configure s1 y s2.....	15
Tabla 3. Configurar s1.....	15
Tabla 4. Configurar s2.....	16
Tabla 5. Parte 2: configurar soporte de host.....	16
Tabla 6. Parte 3: probar y verificar la conectividad de extremo a extremo	18

Escenario 2

Tabla 7. paso 1: inicializar y volver a cargar los routers y los switches.....	37
Tabla 8. paso 1: configurar la computadora de internet.....	40
Tabla 9.configurar r1.....	42
Tabla 10.configurar r2.....	45
Tabla 11.configurar r3.....	48
Tabla 12.configurar s1.....	50
Tabla 13.configurar s3.....	51
Tabla 14.verificacion conectividad de la red configurar s3.....	52
Tabla 15 seguridad del switch, las vlan y el routing entre vlan s1.....	52
Tabla 16 seguridad del switch, las vlan y el routing entre vlan s3.....	56
tabla17 seguridad del switch, las vlan y el routing entre vlan s3.....	58
Tabla 18. Verificar la conectividad de la red en switches y r1.....	59
Tabla 19. Configurar el protocolo de routing dinámico ospf r1.....	61
Tabla 20. Paso 2.configurar ospf en el r2.....	62
Tabla 21. Configurar ospfv3 en el r2.....	63
Tabla 22. Verificar la información de ospf	63
Tabla 23. implementar dhcp y nat para ipv4.....	65
Tabla 24. Configurar la nat estática y dinámica en el r2.....	67
Tabla 25. Verificar el protocolo dhcp y la nat estática.....	68
Tabla 26. Configurar ntp.....	70
Tabla 27. Configurar y verificar las listas de control de acceso (acl).....	71

Lista de Figuras

Topología de red.....	13
Figura 2. Inicialización y carga de R1.....	20
Figura 3. Inicialización y carga de S1.....	20
Figura 4. Inicialización y carga de S2.....	20
Figura 5. Configuración del SDM.....	21
Figura 6. Configuración R1.....	22
Figura 7. Configuración S1.....	23
Figura 8. Configuración S2.....	24
Figura 9. Configuración S1 Configuración de la infraestructura de red.....	27
Figura 10. Configuración S1 Configuración VLAN, Trunking, therChannel.....	29
Figura 11. Configurar soporte de host Configure R1.....	30
Figura 12 Configuración PC-A.....	31
Figura 13 Configuración PC-B	32
Figura 14. Probar y verificar la con ectividad de extremo a extremo.....	35
Figura 15. Topología escenario 2	36
Figura 16. Configuración Routers 1.....	36
Figura 17. Configuración Routers 2.....	37
Figura 18. Configuración Routers 3.....	38
Figura 19. Configuración S1.....	38
Figura 20. Configurar la computadora de Internet.....	40
Tabla 21. Configurar R1.....	47
Tabla 22. Configurar R2.....	47
Figura 23. Configurar R3.....	49
Figura 24. Configurar S1.....	50
Figura 25. Configurar S3.....	50
Figura 26. Verificación conectividad de la Red.....	51
Figura 27. Seguridad del switch, las VLAN y el routing entre VLAN S1.....	51
Figura 28. Seguridad del switch, las VLAN y el routing entre VLAN S3.....	51
Figura 29. Seguridad del switch, las VLAN y el routing entre VLAN R1.....	51
Figura 30. Verificar la conectividad de la red en switches y R1.....	60
Figura 31. Configurar el protocolo de routing dinámico OSPF R1.....	61
Figura 32. Configurar OSPF en el R2.....	63
Figura 33. Configurar OSPFv3 en el R2.....	63
Figura 34. Verificar la información de OSPF.....	65
Figura 35. Implementar DHCP y NAT para IPv4	65
Figura 36. Configurar la NAT estática y dinámica en el R2.....	67
Figura 37. Tabla 25. Verificar el protocolo DHCP y la NAT estática.....	68
Figura 38. Configurar NTP.....	70
Figuras 39. Configurar y verificar las listas de control de acceso (ACL).....	71

Glosario

Conectividad: es la capacidad de un dispositivo de conectarse con otro dispositivo de una forma autónoma.

Dirección IP: es un direccionamiento utilizado para identificar un dispositivo en la red.

DNS: (sistema de nombres de dominio) es la nomenclatura utilizada para asociar información de dominio y la dirección IP de cada uno de los dispositivos que conforman o acceden a una red.

DHCP: (Protocolo de configuración dinámica de host) de tipo cliente/servidor en el que un servidor cuenta con un listado de direcciones IP dinámicas y las asigna a los clientes en el momento en el que se encuentran disponibles.

Encapsulamiento: es el proceso en el que los datos que se encuentran dispuestos para ser enviados a través de una red se ubican en paquetes con la capacidad de ser administrados y rastreados por el administrador de la red

NAT. protocolo con el cual se intercambian o transportan paquetes entre dos redes normalmente incompatibles.

OSPF: protocolo de enrutamiento desarrollado para redes IP, de tipo enlace-estado.

Ping: comando utilizado para realizar un diagnóstico de estado de comunicación entre dos o más equipos en el cual se puede determinar la velocidad, calidad y estado de red.

Protocolos de enrutamiento: conjunto de reglas que permiten determinar la mejor ruta para enviar paquetes de datos entre routers.

Puertos troncales: enlace punto a punto para enviar y recibir el tráfico entre routers o switches.

Topología física: disposición de cada uno de los dispositivos o hardware dentro de una red.

Topología lógica: es la forma que utilizan los hosts para comunicarse a través de una red.

VLAN: procedimiento para establecer redes lógicas de una forma independiente dentro de una misma red física.

Resumen

En el presente trabajo se desarrollan dos escenarios los cuales mediante un arduo análisis se logró establecer el desarrollo y puesta en funcionamiento de los dos proyectos, así mismo se realizó su descripción detallada, la implementación de su topología física, las configuraciones de cada uno de los dispositivos y la verificación de la conectividad de cada uno de ellos por medio de la simulación del escenario en el software Packet Tracer 6.1.1.0001

Introducción

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Para esta actividad, se desarrollaran dos (2) escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

(Prueba de habilidades-2020)

Objetivo General

Dar solución a los escenarios propuesto como trabajo final del diplomado de profundización CCNA, utilizando los conocimientos adquiridos sobre la implementación y diseño de las actividades propuestas.

Objetivos específicos

- Analizar la arquitectura propuesta y dar solución a los escenarios propuestos en este trabajo.
- Realizar la Configuración adecuada en los escenarios para un adecuado funcionamiento de la red propuesta en esta actividad
- Documentar y registrar cada uno de los procedimientos realizados para la configuración de los dispositivos y realizar la verificación de la conectividad entre cada uno de ellos.

1. Descripción Del Escenario 1

1.1. Escenario: 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

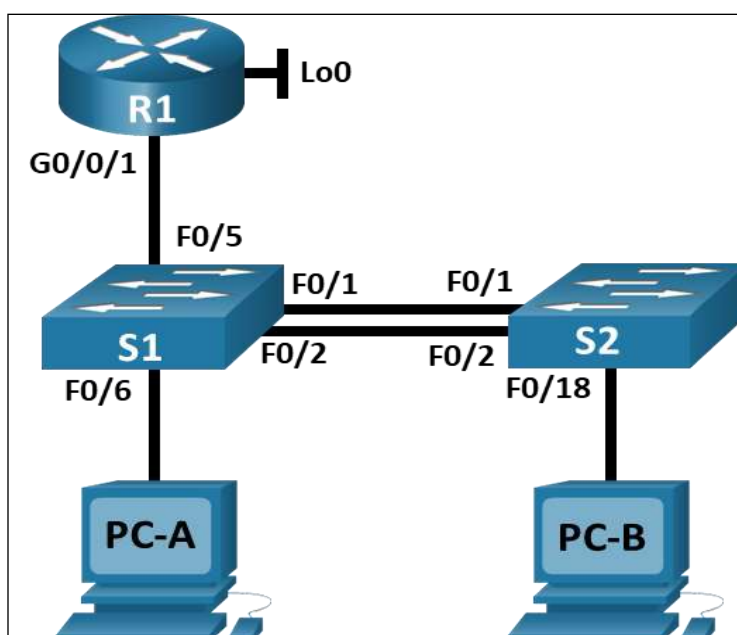


Figura 1. Topología de red propuesta

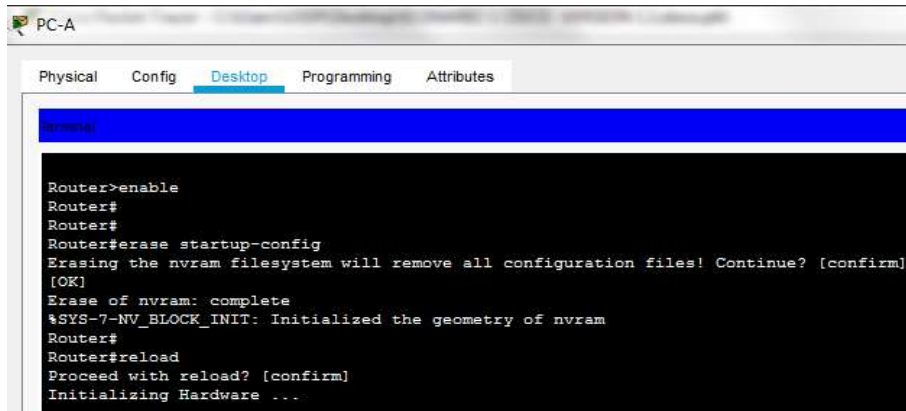
1.2. Requerimientos para el desarrollo del escenario propuesto para la prueba de habilidades

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.

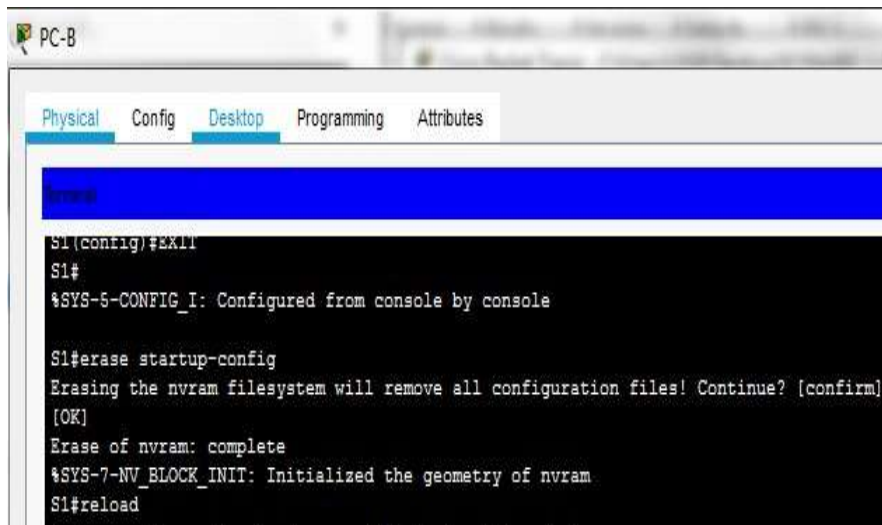
```
Router >enable
Router#erase startup-config
Router #reload
```



```
PC-A
Physical Config Desktop Programming Attributes
Router>enable
Router#
Router#
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
Router#reload
Proceed with reload? [confirm]
Initializing Hardware ...
```

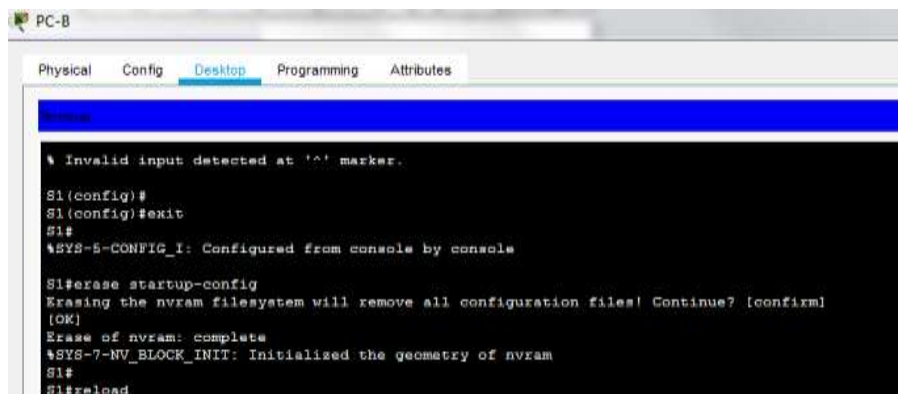
Figura 2. Inicialización y carga de R1

S1 Y S2
switch >enable
switch #erase startup-config
switch #reload



```
PC-B
Physical Config Desktop Programming Attributes
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
S1#reload
```

Figura 3. Inicialización y carga de S1



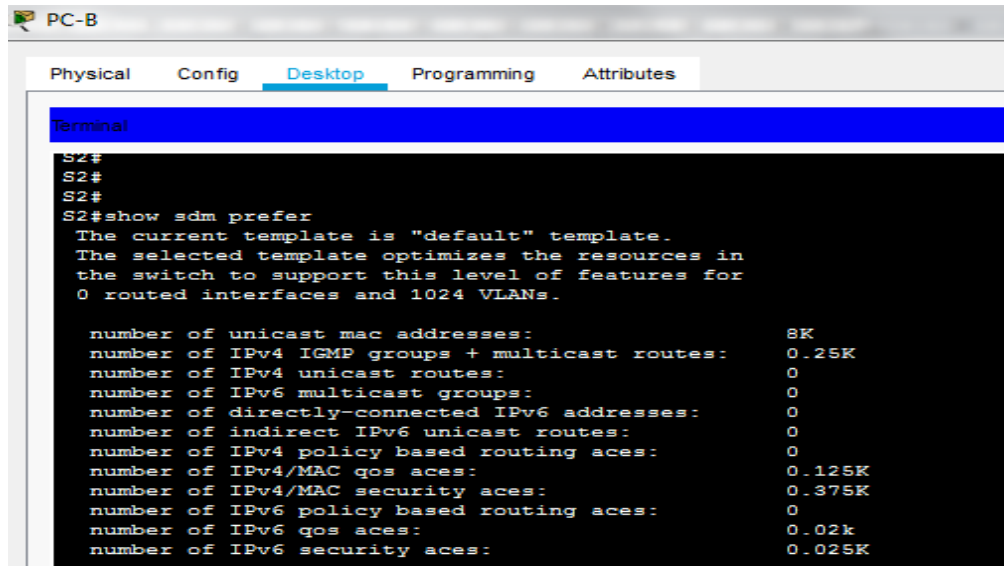
```
PC-B
Physical Config Desktop Programming Attributes
% Invalid input detected at '^' marker.
S1(config)#
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
S1#
S1#reload
```

Figura 4. Inicialización y carga de S2

Análisis: con la inicialización y recarga de los dispositivos podemos prevenir un mal funcionamiento de estos en la ejecución de la actividad.

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

```
S2(config)# sdm prefer dual-ipv4-and-ipv6 default
S2(config)# exit
S2# reload
Proceed with reload? [confirm]
```



En este caso si hay compatibilidad con ipv6
Figura 5. Configuración del SDM

Análisis: con este procedimiento podremos asegurar que los switch acepten el protocolo IPV6

Paso 1: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config 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

Tarea	Especificación
Contraseña cifrada para el modo EXEC privilegiado	Ciscoenpass R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	Ciscoconpass R1(config)#line console 0 R1(config-line)#password ciscoconpass 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 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 15 R1(config-line)#login local
Configurar VTY solo aceptando SSH	R1(config-line)#transport input ssh R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd #Unauthorized Access is Prohibited#
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing

Tarea	Especificación
<p>Configurar interfaz G0/0/1 y subinterfaces</p>	<p>Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como fe80: :1 Establece la dirección IPv6. Activar la interfaz.</p> <pre>R1(config)#interface g0/0/1.2 R1(config-subif)#encapsulation dot1Q 2 R1(config-subif)#description Bikes R1(config-subif)#ip address 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#interface g0/0/1.3 R1(config-subif)#encapsulation dot1Q 3 R1(config-subif)#description Trikes R1(config-subif)#ip address 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#interface g0/0/1.4 R1(config-subif)#encapsulation dot1Q 4 R1(config-subif)#description Management R1(config-subif)#ip address 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#interface g0/0/1.6 R1(config-subif)#encapsulation dot1Q 6 R1(config-subif)#description Native R1(config)#interface g0/0/1 R1(config-if)#no shutdown</pre>

Tarea	Especificación
Configure el Loopback0 interface	<p>Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como fe80::1</p> <pre>R1(config-subif)#interface Loopback 0 R1(config-subif)#description Loopback R1(config-subif)#ip address 209.165.201.1 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:209::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#description Native R1(config-subif)#exit</pre>
Generar una clave de cifrado RSA	<p>Módulo de 1024 bits</p> <pre>R1(config)#crypto key generate rsa 1024</pre>

Tabla 1. Configuración R1

```

PC-A
Physical Config Desktop Programming Attributes
Terminal
R1(config-if)#
R1(config-if)#
R1(config-if)#
R1(config-if)#int Loopback 0

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)#ip 209.165.201.1 255.255.255.224
^
% Invalid input detected at '^' marker.

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 Internet
R1(config-if)#
R1(config-if)#
R1(config-if)#exit
R1(config)#
R1(config)#crypto key generate rsa
The name for the keys will be: R1.ccna-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)#
*mar 1 1:23:6.248: %SSH-5-ENABLED: SSH 1.99 has been enabled

```

```
PC-A
Physical Config Desktop Programming Attributes
Terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#no ip domain lookup
Router(config)#hostname R1
R1(config)#ccna-lab.com
^
% Invalid input detected at '^' marker.
R1(config)#ip domain-name ccna-lab.com
R1(config)#enable secret ciscoenpass
R1(config)#line console 0
^
% Invalid input detected at '^' marker.
R1(config)#line console 0
R1(config-line)#password ciscoenpass
R1(config-line)#login
R1(config-line)#exit
R1(config)#security passwords min-length 10
R1(config)#username admin secret adminpass
R1(config)#line vty 0 15
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd %unauthorized access is prohibited!%
R1(config)#ipv6 unicast-routing
R1(config)#
R1(config)#
R1(config)#int g0/0/1.2
R1(config-subif)#encapsulation dot1q 2
R1(config-subif)#description bikes
R1(config-subif)#description Bikes
R1(config-subif)#ip address 10.19.8.1 255.255.255.192
R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64
^
% Invalid input detected at '^' marker.
R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#
R1(config-subif)#
R1(config-subif)#int g0/0/1.3
R1(config-subif)#encapsulation dot1q 3
R1(config-subif)#description Trikes
R1(config-subif)#ip address 10.19.8.65 255.255.255.224
R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#
R1(config-subif)#int g0/0/1.4
R1(config-subif)#encapsulation dot1q 4
R1(config-subif)#description Management
R1(config-subif)#ip address 10.19.8.97 255.255.255.248
R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#
R1(config-subif)#int g0/0/1.6
R1(config-subif)#encapsulation dot1q 6 native
R1(config-subif)#description Native
R1(config-subif)#
R1(config-subif)#int g0/0/1
R1(config-if)#no shutdown
```

Figura 6. Configuración R1

Paso 2: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente: S1

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch1>enable Switch1#config terminal Switch1(config)#no ip domain lookup
Nombre del switch	S1 o S2, según proceda Switch1(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	Ciscoconpass 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	Nombre de usuario: admin Password: admin1pass S1(config)#username admin 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
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#login local S1(config-line)#transport input ssh S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd #Unauthorized Access is Prohibited!#
Generar una clave de cifrado RSA	Módulo de 1024 bits S1(config)#crypto key generate rsa 1024

Tarea	Especificación
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 y FE80: :99 para S2 Establecer la dirección IPv6 de capa 3 S1(config)#interface vlan 4 S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#description Management Interface S1(config-if)#no shutdown S1(config-if)#exit
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4 S1(config)#ip default-gateway 10.19.8.97

Las tareas de configuración incluyen lo siguiente: S2

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch2>enable Switch2#config terminal Switch1(config)#no ip domain lookup
Nombre del switch	S1 o S2, según proceda Switch2(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	Ciscoconpass S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit

Tarea	Especificación
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass S2(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 15
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config-line)#login local S2(config-line)#transport input ssh S2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption
Configurar un MOTD Banner	S2(config)#banner motd #Unauthorized Access is Prohibited!#
Generar una clave de cifrado RSA	Módulo de 1024 bits S2(config)#crypto key generate rsa 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 y FE80: :99 para S2 Establecer la dirección IPv6 de capa 3 S2(config)#interface vlan 4 S2(config-if)#ip address 10.19.8.99 255.255.255.248 S2(config-if)#ipv6 address address 2001:db8:acad:c::99/64 S2(config-if)#ipv6 address fe80::99 link-local S2(config-if)#description Management Interface S2(config-if)#no shutdown S2(config-if)#exit
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4 S1(config)#ip default-gateway 10.19.8.97

Tabla 2. Topología de red propuesta

```
PC-B
Physical Config Desktop Programming Attributes

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet1/0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to up
S1>
S1>
S1>
S1>en
S1#
S1#
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#
S1(config)#
S1(config)#
S1(config)#no ip domain lookup
S1(config)#ip domain-name ccna-lab.com
S1(config)#enable secret ciscoenpass
S1(config)#line console 0
S1(config-line)#password ciscoenpass
S1(config-line)#login
S1(config-line)#exit
S1(config)#username admin secret adminpass
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd Unauthorized Access is Prohibited!
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
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]
S1(config)#
*mar 1 0:16:34.701: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#
S1(config)#
S1(config)#
S1(config)#int vlan 4
S1(config-if)#
S1(config-if)#ip address 10.19.8.99 255.255.255.248
S1(config-if)#ipv6 address 2001:db8:acad:e::99/64
S1(config-if)#ipv6 address fe80::39 link-local
S1(config-if)#description Management Interface
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#ip default-gateway 10.19.8.97
S1(config)#
```

Figura 7. Configuración S1

```
PC-B
Physical Config Desktop Programming Attributes

S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#ip domain-name ccna-lab.com
S2(config)#crypto key generate rsa
The name for the keys will be: S2.ccna-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)#int vlan 4
*mar 1 0:54:42.402: %SSH-5-ENABLED: SSH 1.99 has been enabled
S2(config-if)#ip address 10.19.8.99 255.255.255.248
S2(config-if)#ipv6 address 2001:db8:acad:e::99/64
S2(config-if)#ipv6 address fe80::39 link-local
S2(config-if)#description Management Interface
S2(config-if)#no shutdown
S2(config-if)#exit
S2(config)#ip default-gateway 10.19.8.97
```

```
PC-B
Physical Config Desktop Programming Attributes
Terminal
S2>
S2>en
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#
S2(config)#
S2(config)#no ip domain lookup
S2(config)#ip domain-name ccna-lab.com
S2(config)#enable secret ciscoenpass
S2(config)#line console 0
S2(config-line)#password ciscoconpass
S2(config-line)#login
S2(config-line)#exit
S2(config)#username admin secret adminlpass
S2(config)#line vty 0 15
S2(config-line)#login local
S2(config-line)#transport input ssh
S2(config-line)#exit
S2(config)#service password-encryption
S2(config)#banner motd &unauthorized Access is Prohibited!&
S2(config)#crypto key generate rsa
% Please define a domain-name first.
S2(config)#
S2(config)#crypto key generate rsa
% Please define a domain-name first.
S2(config)#crypto key generate rsa
% Please define a domain-name first.
S2(config)#1024
^
% Invalid input detected at '^' marker.

S2(config)#crypto key generate rsa modulus 1024
^
% Invalid input detected at '^' marker.

S2(config)#crypto key generate rsa
% Please define a domain-name first.
S2(config)#
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#
S2(config)#
S2(config)#crypto key generate rsa
% Please define a domain-name first.
S2(config)#
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#ip domain-name ccna-lab.com
S2(config)#
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#ip domain-name ccna-lab.com
```

Figura 8. Configuración S2

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

Paso 3: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tarea	Especificación
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native S1(config)#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

Tarea	Especificación
<p>Crear troncos 802.1Q que utilicen la VLAN 6 nativa</p>	<p>Interfaces F0/1, F0/2 y F0/5</p> <pre>S1(config)#interface range f0/1-2 S1(config-if-range)#switchport trunk encapsulation dot1q 1 S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6 S1(config-if-range)#switchport trunk allowed vlan 2 3 4 5 6 S1(config-if-range)#exit S1(config)#interface f0/5 S1(config-if)#switchport trunk encapsulation dot1q 5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#switchport trunk allowed vlan 2 3 4 5 6 S1(config-if)#exit</pre>
<p>Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2</p>	<p>Usar el protocolo LACP para la negociación</p> <pre>S1(config)#interface range f0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#exit</pre>
<p>Configurar el puerto de acceso de host para VLAN 2</p>	<p>Interface F0/6</p> <pre>S1(config)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2</pre>
<p>Configurar la seguridad del puerto en los puertos de acceso</p>	<p>Permitir 3 direcciones MAC</p> <pre>S1(config-if)#switchport port-security maximum 3</pre>

Tarea	Especificación
<p>Proteja todas las interfaces no utilizadas</p>	<p>Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar</p> <pre> S1(config)#interface range f0/3-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Unused Interfaces S1(config-if-range)#shutdown S1(config)#interface range f0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Unused Interfaces S1(config-if-range)#shutdown S1(config)#interface range g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Unused Interfaces S1(config-if-range)#shutdown </pre>

Tabla 3. Configurar s1

```
PC-B
Physical Config Desktop Programming Attributes
Terminal
Password:
Password:

S1>enable
Password:
S1#
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#
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)#
%LINK-5-CHANGED: Interface Vlan4, changed state to up

S1(config-vlan)#name Management
S1(config-vlan)#vlan 5
S1(config-vlan)#name Parking
S1(config-vlan)#vlan 6
S1(config-vlan)#name Native
S1(config-vlan)#
S1(config-vlan)#exit
S1(config)#
S1(config)#int g1/0/5
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan4, changed state to up

S1(config-if)#switchport trunk native vlan 6
S1(config-if)#int range g1/0/1-2
S1(config-if-range)#shutdown

S1(config-if-range)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0/1, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to down

%LINK-5-CHANGED: Interface GigabitEthernet1/0/2, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to down

S1(config-if-range)#switchport trunk encapsulation dot1q
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 6
S1(config-if-range)#channel-group 1 active
^
% Invalid input detected at '^' marker.
```

```
PC-B
Physical Config Desktop Programming Attributes
Terminal
S1(config-if-range)#channel-group 1 mode active
S1(config-if-range)#
Creating a port-channel interface Port-channel 1

%EC-5-CANNOT_BUNDLE2: Gig1/0/1 is not compatible with Po1 and will be suspended (native vlan of Gig1/0/1 is 6, Po1 id 1)

%EC-5-CANNOT_BUNDLE2: Gig1/0/2 is not compatible with Po1 and will be suspended (native vlan of Gig1/0/2 is 6, Po1 id 1)

S1(config-if-range)#int Port-channel 1
S1(config-if)#
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int range g1/0/1-2
S1(config-if-range)#
S1(config-if-range)#int Port-channel 1
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#int g1/0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 3
S1(config-if)#int range g1/0/3-4
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description Not In Use
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface GigabitEthernet1/0/3, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/4, changed state to administratively down
S1(config-if-range)#
S1(config-if-range)#int range g1/0/7-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description Not In Use
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface GigabitEthernet1/0/7, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/8, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/9, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/10, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/11, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/12, changed state to administratively down
```

PC-B

Physical Config Desktop Programming Attributes

Terminal

```
%LINK-5-CHANGED: Interface GigabitEthernet1/0/11, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/12, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/13, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/14, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/15, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/16, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/17, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/18, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/19, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/20, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/21, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/22, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/23, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/24, changed state to administratively down
S1(config-if-range)#
S1(config-if-range)#int range g1/1/1-4
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description Not In Use
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface GigabitEthernet1/1/1, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/1/2, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/1/3, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/1/4, changed state to administratively down
```

Figura 9. Configuración S1 Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

Paso 4: Configure el S2.

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

Tarea	Especificación
Crear VLAN	VLAN 2, name Bikes VLAN 3, name 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)#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	Interfaces F0/1 y F0/2 S2(config)#interface range f0/1-2 S2(config-if-range)#switchport trunk encapsulation dot1q 1 S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 6 S2(config-if-range)#switchport trunk allowed vlan 2 3 4 5 6 S2(config-if-range)#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)#interface range f0/1-2 S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#exit

Tarea	Especificación
Configurar el puerto de acceso del host para la VLAN 3	<p>Interfaz F0/18</p> <pre>S2(config)#interface f0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3</pre>
Configure port-security en los access ports	<p>permite 3 MAC addresses</p> <pre>S2(config-if)#switchport port-security maximum 3</pre>
Asegure todas las interfaces no utilizadas.	<p>Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar</p> <pre>S2(config)#interface range f0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Unused Interfaces S2(config-if-range)#shutdown S2(config)#interface range f0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Unused Interfaces S2(config-if-range)#shutdown S2(config)#interface range g0/1-2 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Unused Interfaces S2(config-if-range)#shutdown</pre>

Tabla 4. Configurar s2

```
PC-B
Physical Config Desktop Programming Attributes
Terminal
S2>enable
Password:
S2#
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#
S2(config)#
S2(config)#vlan 2
S2(config-vlan)#name Bikes
S2(config-vlan)#vlan 3
S2(config-vlan)#name Trikes
S2(config-vlan)#vlan 4
S2(config-vlan)#
%LINK-5-CHANGED: Interface Vlan4, changed state to up

S2(config-vlan)#name Management
S2(config-vlan)#vlan 5
S2(config-vlan)#name Parking
S2(config-vlan)#vlan 6
S2(config-vlan)#name Native
S2(config-vlan)#exit
S2(config)#
S2(config)#int range g1/0/1-2
S2(config-if-range)#shutdown

%LINK-5-CHANGED: Interface GigabitEthernet1/0/1, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet1/0/2, changed state to administratively down
S2(config-if-range)#
S2(config-if-range)#switchport trunk encapsulation dot1q
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 6
S2(config-if-range)#channel-group 1 mode active
S2(config-if-range)#
Creating a port-channel interface Port-channel 1

%EC-5-CANNOT_BUNDLE2: Gig1/0/1 is not compatible with Po1 and will be suspended (native vlan of Gig1/0/1 is
6, Po1 id 1)

%EC-5-CANNOT_BUNDLE2: Gig1/0/2 is not compatible with Po1 and will be suspended (native vlan of Gig1/0/2 is
6, Po1 id 1)

S2(config-if-range)#int 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)#int g1/0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 3
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 3
S2(config-if)#int range g1/0/3-17
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#description Not In Use
S2(config-if-range)#shutdown
```



```

PC-B
Physical Config Desktop Programming Attributes

S2 (config-if-range)#shutdown
%LINK-5-CHANGED: Interface GigabitEthernet1/0/3, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/4, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/5, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/6, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/7, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/8, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/9, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/10, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/11, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/12, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/13, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/14, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/15, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/16, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/17, changed state to administratively down
S2 (config-if-range)#
S2 (config-if-range)#
S2 (config-if-range)#int range g1/0/19-24
S2 (config-if-range)#switchport mode access
S2 (config-if-range)#switchport access vlan 5
S2 (config-if-range)#description Not In Use
S2 (config-if-range)#shutdown
%LINK-5-CHANGED: Interface GigabitEthernet1/0/19, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/20, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/21, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/22, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/23, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/24, changed state to administratively down
S2 (config-if-range)#int range g1/1/1-4
S2 (config-if-range)#switchport mode access
S2 (config-if-range)#switchport access vlan 5
S2 (config-if-range)#description Not In Use
S2 (config-if-range)#shutdown
%LINK-5-CHANGED: Interface GigabitEthernet1/1/1, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/1/2, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/1/3, changed state to administratively down

```

```

PC-B
Physical Config Desktop Programming Attributes

%LINK-5-CHANGED: Interface GigabitEthernet1/1/3, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/1/4, changed state to administratively down
S2 (config-if-range)#
S2 (config-if-range)#int range g1/0/1-2
S2 (config-if-range)#no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet1/0/1, changed state to down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/2, changed state to down
S2 (config-if-range)#
S2 (config-if-range)#
S2#
%SYS-5-CONFIG_I: Configured from console by console
%LINK-5-CHANGED: Interface GigabitEthernet1/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan4, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet1/0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to up
S2#

```

Figura 10. Configuración S1 Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

La anterior configuración sirvió para proporcionar velocidades ampliadas entre las vlan a través de la implementación de puertos múltiples

Parte 2: Configurar soporte de host

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Configure Default Routing	<p>Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0</p> <pre>R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0</pre>
Configurar IPv4 DHCP para VLAN 2	<p>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</p> <pre>R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#ip dhcp pool VLAN2-Bikes R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#exit</pre>
Configurar DHCP IPv4 para VLAN 3	<p>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</p> <pre>R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84 R1(config)#ip dhcp pool VLAN3-Trikes R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(dhcp-config)#domain-name ccna-b.net</pre>

Tabla 5. Parte 2: configurar soporte de host

```

PC-A
-----
Physical  Config  Desktop  Programming  Attributes
-----
Terminal
-----
Press RETURN to get started!

unauthorized access is prohibited!

User Access Verification

Password:
Password:

R1>enable
Password:
R1#
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
^
% Invalid input detected at '^' marker.

R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#ipv6 route ::/0 loopback 0
R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52
R1(config)#ip dhcp pool VLAN2-Bikes
R1(dhcp-config)#network 10.19.8.0 255.255.255.192
R1(dhcp-config)#default-router 10.19.8.1
R1(dhcp-config)#domain-name ccna-a.net
R1(dhcp-config)#
R1(dhcp-config)#exit
R1(config)#
R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84
R1(config)#ip dhcp pool VLAN3-Trikes
R1(dhcp-config)#network 10.19.8.64 255.255.255.224
R1(dhcp-config)#default-router 10.19.8.65
R1(dhcp-config)#domain-name ccna-b.net
R1(dhcp-config)#exit

```

Figura 11. Configurar soporte de host Configure R1

Con la implementación y soporte de los host se puede analizar una de sus funciones como lo es que si se presenta una falla en algún servidor otro más suplirá sus funciones asiéndose cargo del trabajo asignado al primero.

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**.

PC-A Network Configuration	
Descripción	
Dirección física	0000.0C28.146E
Dirección IP	10.19.8.53
Máscara de subred	255.255.255.192

PC-A Network Configuration	
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

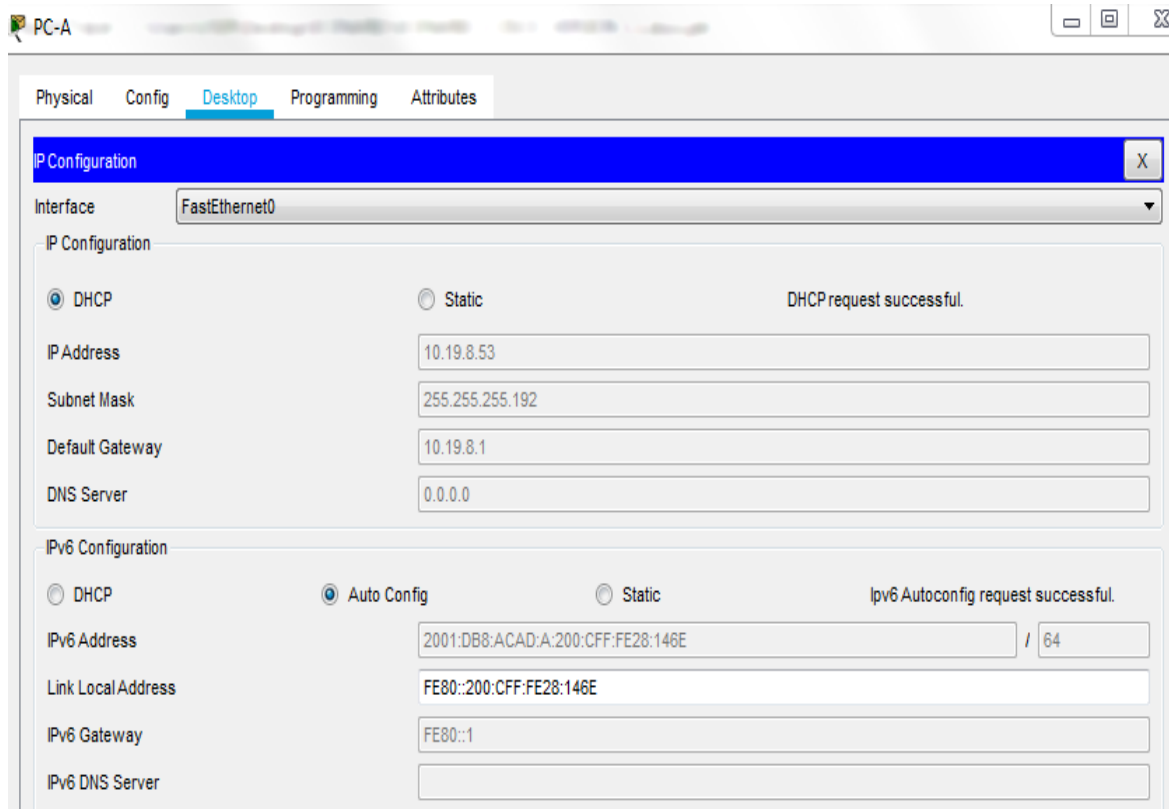


Figura 12 configuraciones pc-a.

PC-B Network Configuration	
Descripción	
Dirección física	00E0.8F79.DAB7
Dirección IP	10.19.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::1

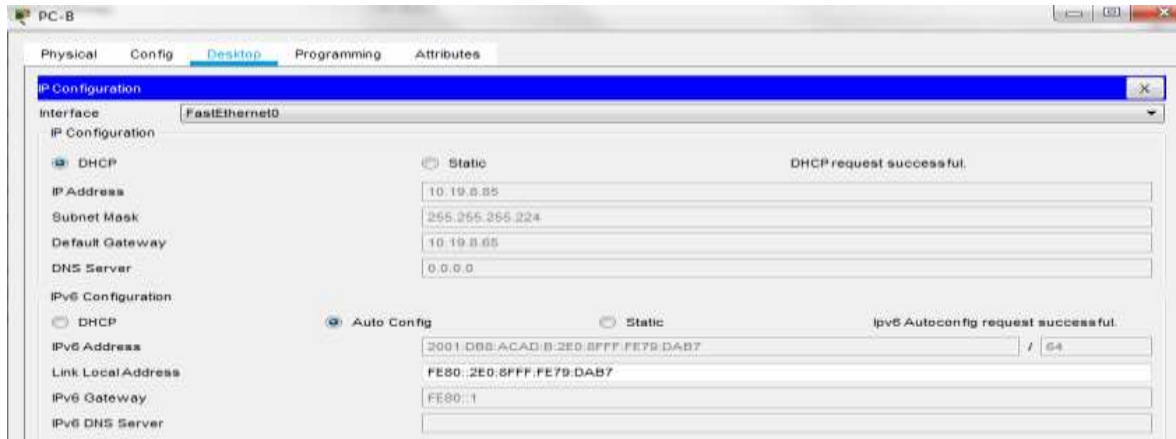


Figura 13 CONFIGURACIÓN PC-B

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:

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	exitoso
		IPv6	2001:db8:acad:a :1	exitoso
	R1, G0/0/1.3	Dirección	10.19.8.65	exitoso
		IPv6	2001:db8:acad:b :1	exitoso
	R1, G0/0/1.4	Dirección	10.19.8.97	exitoso
		IPv6	2001:db8:acad:c :1	exitoso
	S1, VLAN 4	Dirección	10.19.8.98	exitoso
		IPv6	2001:db8:acad:c :98	exitoso
S2, VLAN 4	Dirección	10.19.8.99.	exitoso	
	IPv6	2001:db8:acad:c :99	exitoso	
	PC-B	Dirección	IP address will vary.	exitoso
		IPv6	2001:db8:acad:b :50	exitoso
	R1 Bucle 0	Dirección	209.165.201.1	exitoso
		IPv6	2001:db8:acad:209: :1	exitoso
PC-B	R1 Bucle 0	Dirección	209.165.201.1	exitoso
		IPv6	2001:db8:acad:209: :1	exitoso
	R1, G0/0/1.2	Dirección	10.19.8.1	exitoso

Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:a: :1	exitoso
	R1, G0/0/1.3	Dirección	10.19.8.65	exitoso
		IPv6	2001:db8:acad:b: :1	exitoso
	R1, G0/0/1.4	Dirección	10.19.8.97	exitoso
		IPv6	2001:db8:acad:c: :1	exitoso
	S1, VLAN 4	Dirección	10.19.8.98	Received 3
		IPv6	2001:db8:acad:c: :98	Received 0
	S2, VLAN 4	Dirección	10.19.8.99.	Received 3
		IPv6	2001:db8:acad:c: :99	Received 0

Tabla 6. Parte 3: probar y verificar la conectividad de extremo a extremo


```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.19.8.1

Pinging 10.19.8.1 with 32 bytes of data:

Reply from 10.19.8.1: bytes=32 time=1ms TTL=255
Reply from 10.19.8.1: bytes=32 time<1ms TTL=255
Reply from 10.19.8.1: bytes=32 time<1ms TTL=255
Reply from 10.19.8.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.19.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 2001:db8:acad:a::1

Pinging 2001:db8:acad:a::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: bytes=32 time=10ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=4ms TTL=255

Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>ping 10.19.8.65

Pinging 10.19.8.65 with 32 bytes of data:

Reply from 10.19.8.65: bytes=32 time=1ms TTL=255
Reply from 10.19.8.65: bytes=32 time<1ms TTL=255
Reply from 10.19.8.65: bytes=32 time<1ms TTL=255
Reply from 10.19.8.65: bytes=32 time<1ms TTL=255

Ping statistics for 10.19.8.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 2001:db8:acad:b::1

Pinging 2001:db8:acad:b::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::1: bytes=32 time=13ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:B::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 3ms

C:\>ping 10.19.8.97

Pinging 10.19.8.97 with 32 bytes of data:

Reply from 10.19.8.97: bytes=32 time=1ms TTL=255
Reply from 10.19.8.97: bytes=32 time<1ms TTL=255
Reply from 10.19.8.97: bytes=32 time<1ms TTL=255
Reply from 10.19.8.97: bytes=32 time<1ms TTL=255
```

```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Ping statistics for 10.19.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 2001:db8:acad:c::1

Pinging 2001:db8:acad:c::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8: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:\>ping 10.19.8.98

Pinging 10.19.8.98 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.19.8.98: bytes=32 time<1ms TTL=254
Reply from 10.19.8.98: bytes=32 time<1ms TTL=254

Ping statistics for 10.19.8.98:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 2001:db8:acad:c::98

Pinging 2001:db8:acad:c::98 with 32 bytes of data:

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

Ping statistics for 2001:DB8:ACAD:C::98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.19.8.99

Pinging 10.19.8.99 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.19.8.99: bytes=32 time<1ms TTL=254
Reply from 10.19.8.99: bytes=32 time<1ms TTL=254

Ping statistics for 10.19.8.99:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 2001:db8:acad:c::99
Invalid Command.
```

```
PC-B
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=12ms 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
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 = 12ms, Average = 3ms

C:\>ping 2001:db8:acad:209::1

Pinging 2001:db8:acad:209::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:209::1: bytes=32 time=14ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:209::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 3ms

C:\>ping 10.19.8.1

Pinging 10.19.8.1 with 32 bytes of data:

Reply from 10.19.8.1: bytes=32 time=1ms TTL=255
Reply from 10.19.8.1: bytes=32 time=1ms TTL=255
Reply from 10.19.8.1: bytes=32 time<1ms TTL=255
Reply from 10.19.8.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.19.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 2001:db8:acad:a::1

Pinging 2001:db8:acad:a::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:A::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 10.19.8.65

Pinging 10.19.8.65 with 32 bytes of data:

Reply from 10.19.8.65: bytes=32 time=1ms TTL=255
Reply from 10.19.8.65: bytes=32 time<1ms TTL=255
```

```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 10.19.8.65: bytes=32 time<1ms TTL=255
Reply from 10.19.8.65: bytes=32 time<1ms TTL=255
Reply from 10.19.8.65: bytes=32 time<1ms TTL=255

Ping statistics for 10.19.8.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 2001:db8:acad:b::1

Pinging 2001:db8:acad:b::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::1: bytes=32 time=14ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:B::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 3ms

C:\>ping 10.19.8.97

Pinging 10.19.8.97 with 32 bytes of data:

Reply from 10.19.8.97: bytes=32 time=2ms TTL=255
Reply from 10.19.8.97: bytes=32 time=1ms TTL=255
Reply from 10.19.8.97: bytes=32 time=1ms TTL=255
Reply from 10.19.8.97: bytes=32 time=4ms TTL=255

Ping statistics for 10.19.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms

C:\>ping 2001:db8:acad:c::1

Pinging 2001:db8:acad:c::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:C::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 10.19.8.98

Pinging 10.19.8.98 with 32 bytes of data:

Request timed out.
Reply from 10.19.8.98: bytes=32 time<1ms TTL=254
Reply from 10.19.8.98: bytes=32 time<1ms TTL=254
Reply from 10.19.8.98: bytes=32 time<1ms TTL=254

Ping statistics for 10.19.8.98:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
```

Figura 14. Probar y verificar la conectividad de extremo a extremo

Desarrollo Del Escenario 2 Propuesto Para La Prueba De Habilidades Prácticas

Descripción

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

Topología

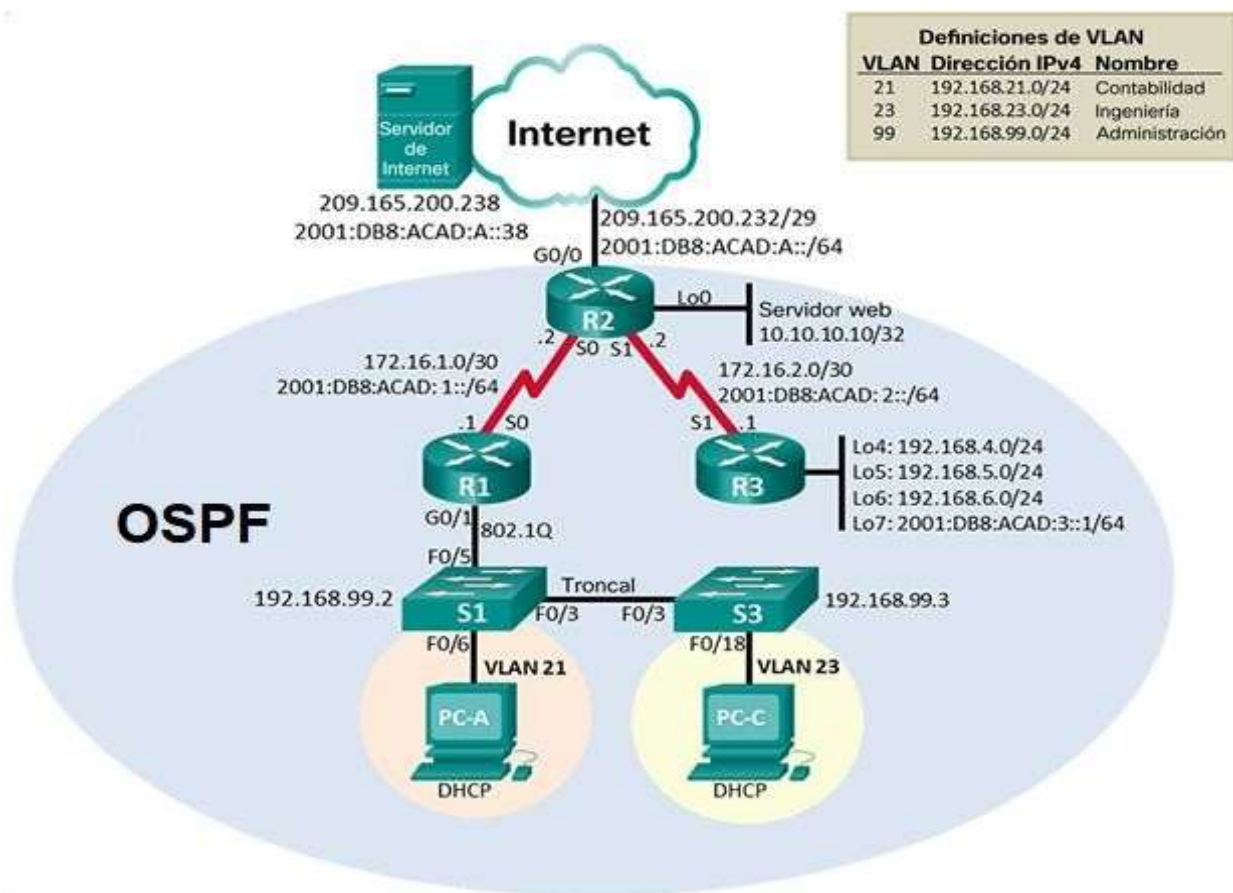


Figura 15. Topología escenario 2

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.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config
Volver a cargar todos los routers	Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#erase startup-config Switch#delete flash: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 vlan

Tabla 7. Paso 1: inicializar y volver a cargar los routers y los switches

Esta recarga y inicialización de los dispositivos nos permite prevenir errores al momento de iniciar la configuración inicial de los dispositivos.

Routers 1

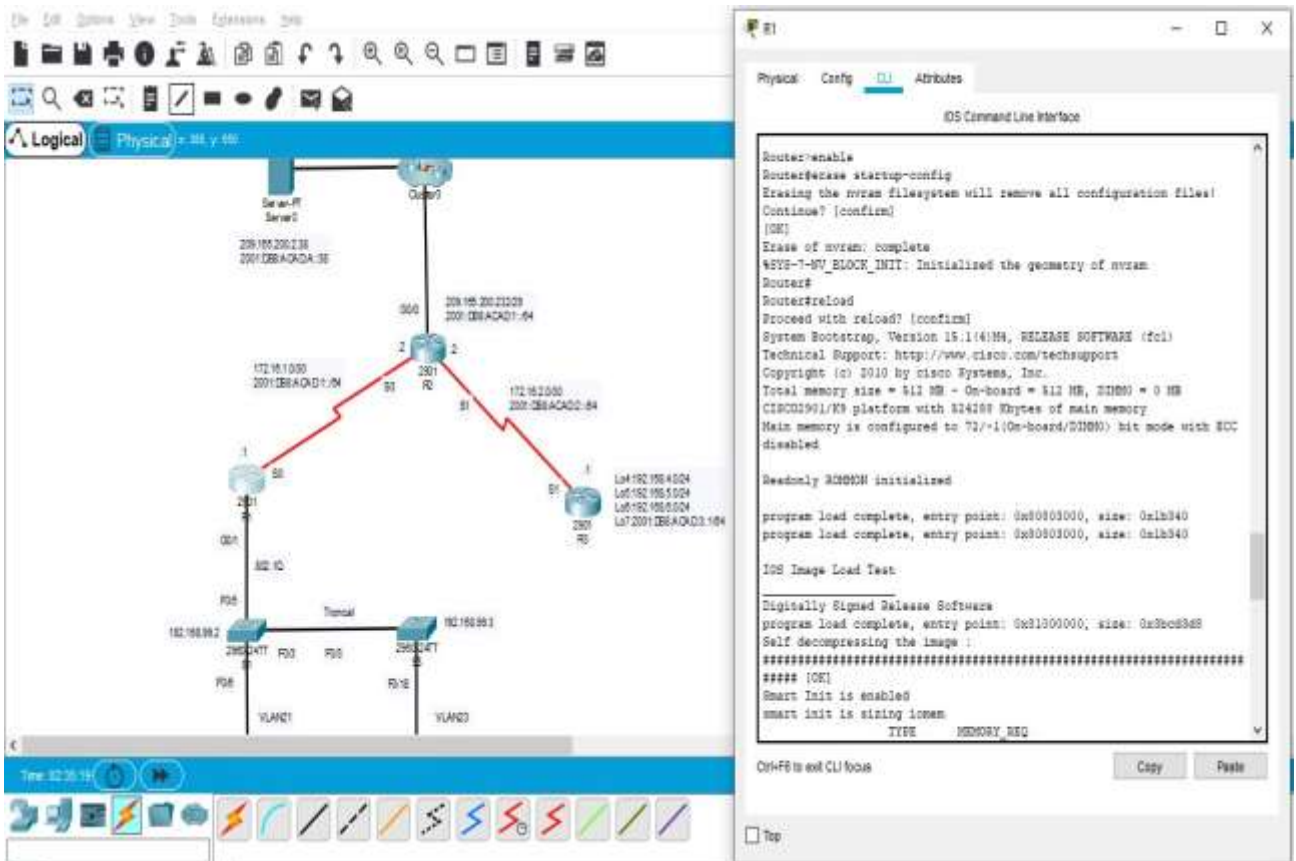


Figura 16. Configuración Routers 1

Routers 2

The screenshot shows the configuration of Router 2 in Cisco Packet Tracer. The network diagram on the left shows Router 2 (2901) connected to a Server (2901) and two other routers (2901 and 2901). The right pane shows the IOS Command Line Interface with the following configuration and boot logs:

```

Router>
Router>enable
Router#
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
MIPS-7-0U_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2015 by Cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO02/01/K9 platform with 524288 Bytes of main memory
Main memory is configured to 72"/"1.0n-board/DIMM0) bit mode with ECC
disabled

Readonly ROMMON initialized

program load complete, entry point: 0x00000000, size: 0x1b340
program load complete, entry point: 0x00000000, size: 0x1b340

IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x01000000, size: 0x0bc03d5
Self decompressing the image :
#####
##### IOS!
Smart Init is enabled
Smart Init is sizing L2mem:
          TYPE      MEMORY_REQ
HWIC Slot 0      0x00200000   Onboard devices 4
buffer pools    0x0224F000
          TOTAL:      0x0344F000

Routed ROMMON up to: 489.
  
```

Figura 17. Configuración Routers 2

Routers 3

The screenshot shows the configuration of Router 3 in Cisco Packet Tracer. The network diagram on the left shows Router 3 (2901) connected to a Server (2901) and two other routers (2901 and 2901). The right pane shows the IOS Command Line Interface with the following configuration and boot logs:

```

Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
MIPS-7-0U_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2015 by Cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO02/01/K9 platform with 524288 Bytes of main memory
Main memory is configured to 72"/"1.0n-board/DIMM0) bit mode with ECC
disabled

Readonly ROMMON initialized

program load complete, entry point: 0x00000000, size: 0x1b340
program load complete, entry point: 0x00000000, size: 0x1b340

IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x01000000, size: 0x0bc03d5
Self decompressing the image :
#####
##### IOS!
Smart Init is enabled
Smart Init is sizing L2mem:
          TYPE      MEMORY_REQ
HWIC Slot 0      0x00200000   Onboard devices 4
buffer pools    0x0224F000
          TOTAL:      0x0344F000

Routed ROMMON up to: 489.
  
```

Figura 18. Configuración Routers 3

S1

```
Switch#enable
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
$VFS-FS_MOUNT_INIT: Initialized the geometry of nvram
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash://vlan.dat? [confirm]
%Error deleting flash://vlan.dat (No such file or directory)

Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.3(26)FX, RELEASE
SOFTWARE (fo4)
Class WS-C2960-24TT (RC32300) processor (revision C0) with 210384
bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 0000.1234.5678
Nvram file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64014944
flashfs[0]: Bytes used: 4414921
flashfs[0]: Bytes available: 59601463
flashfs[0]: flashfs took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 0
Parameter Block Filesystem (pb:) installed, fsid: 4

Loading "flash://c2960-lanbase-sw.123-25.FX.bin"...
#####
##### [OK]

Ctrl-F to exit CLI from
```

Figura 19. Configuración S1

S3

```
Switch#enable
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
$VFS-FS_MOUNT_INIT: Initialized the geometry of nvram
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash://vlan.dat? [confirm]
%Error deleting flash://vlan.dat (No such file or directory)

Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.3(26)FX, RELEASE
SOFTWARE (fo4)
Class WS-C2960-24TT (RC32300) processor (revision C0) with 210384
bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 0000.1234.5678
Nvram file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64014944
flashfs[0]: Bytes used: 4414921
flashfs[0]: Bytes available: 59601463
flashfs[0]: flashfs took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 0
Parameter Block Filesystem (pb:) installed, fsid: 4

Loading "flash://c2960-lanbase-sw.123-25.FX.bin"...
#####
##### [OK]

Ctrl-F to exit CLI from
```

Figura 19. Configuración S1

```

S1
Physical Config CLI Attributes
IOS Command Line Interface

Switch>enable
Switch#show vlan

VLAN Name                                Status      Ports
-----
1    default                                active      Fa0/1, Fa0/2, Fa0/3,
Fa0/4, Fa0/5, Fa0/6, Fa0/7,
Fa0/8, Fa0/9, Fa0/10,
Fa0/11, Fa0/12,
Fa0/13, Fa0/14,
Fa0/15, Fa0/16,
Fa0/17, Fa0/18,
Fa0/19, Fa0/20,
Fa0/21, Fa0/22,
Fa0/23, Fa0/24
1002 fddi-default                          active
1003 token-ring-default                    active
1004 fddinet-default                       active
1005 trnet-default                         active

VLAN Type SAID      MTU   Parent  RingNo BridgeNo  Stp   BrdgMode
Trans1 Trans2
-----
1    enet  100001  1500  -      -      -      -      -      0
0
1002 fddi  101002  1500  -      -      -      -      -      0
0
1003 tr   101003  1500  -      -      -      -      -      0
0
1004 fdnet 101004  1500  -      -      -      ieee  -      0
0
1005 trnet 101005  1500  -      -      -      ibm   -      0
0

```

```

S3
Physical Config CLI Attributes
IOS Command Line Interface

Switch>enable
Switch#show vlan

VLAN Name                                Status      Ports
-----
1    default                                active      Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/11, Fa0/12
Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/17, Fa0/18, Fa0/19, Fa0/20
Fa0/21, Fa0/22, Fa0/23, Fa0/24
Gig0/1, Gig0/2
1002 fddi-default                          active
1003 token-ring-default                    active
1004 fddinet-default                       active
1005 trnet-default                         active

VLAN Type SAID      MTU   Parent  RingNo BridgeNo  Stp   BrdgMode  Trans1 Trans2
-----
1    enet  100001  1500  -      -      -      -      -      0      0
1002 fddi  101002  1500  -      -      -      -      -      0      0
1003 tr   101003  1500  -      -      -      -      -      0      0
1004 fdnet 101004  1500  -      -      -      ieee  -      0      0
1005 trnet 101005  1500  -      -      -      ibm   -      0      0

VLAN Type SAID      MTU   Parent  RingNo BridgeNo  Stp   BrdgMode  Trans1 Trans2
-----

Remote SPAN VLANs
-----

Primary Secondary Type          Ports
-----

```

Figura 19. Configuración S1 y S3

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):

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

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.

Tabla 8. Paso 1: Configurar la computadora de Internet

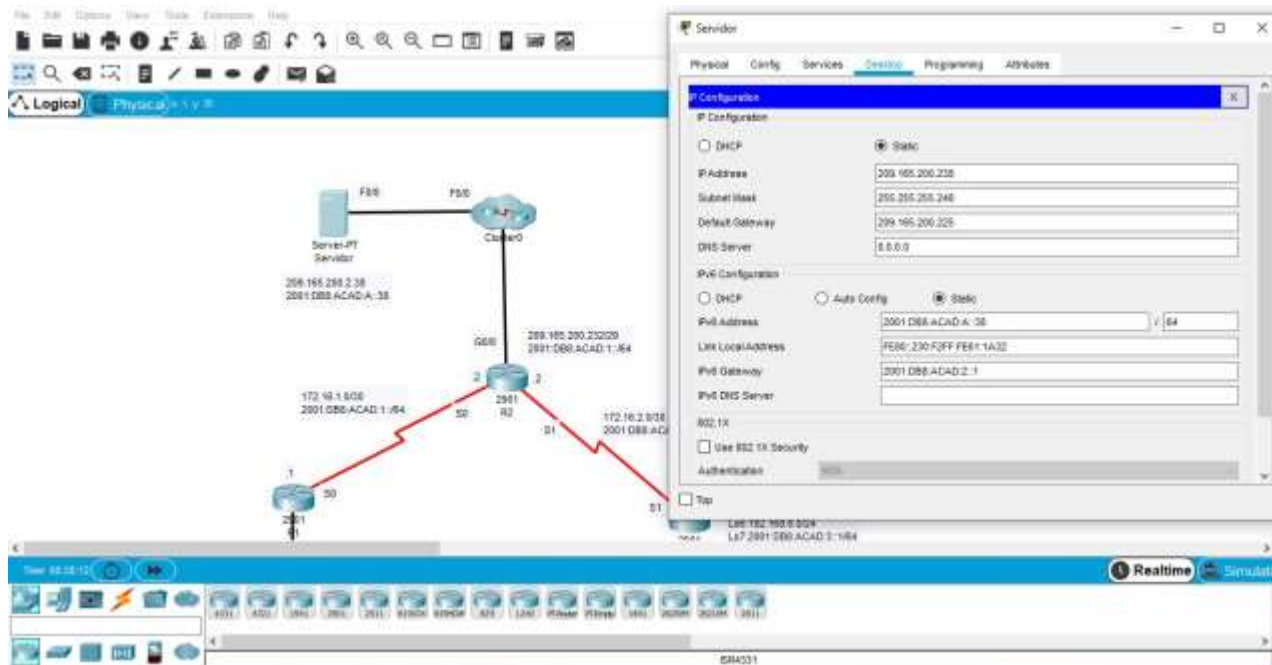


Figura 20. Configurar la computadora de Internet

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

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

Nombre del router	hostname R1 R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	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 pass R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd #Se prohíbe el acceso no autorizado!# Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción R1(config)#interface s0/0/0 R1(config-if)#description R1-R2 Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones R1(config-if)#ip address 172.16.1.1 255.255.255.252 Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones R1(config-if)#ipv6 address 2001:DB8:ACAD:1::/64 Establecer la frecuencia de reloj en 128000 Activar la interfaz R1(config-if)#clock rate 128000 R1(config-if)#no shutdown

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

Nota: Todavía no configure G0/1.

Tabla 9. Configurar R1

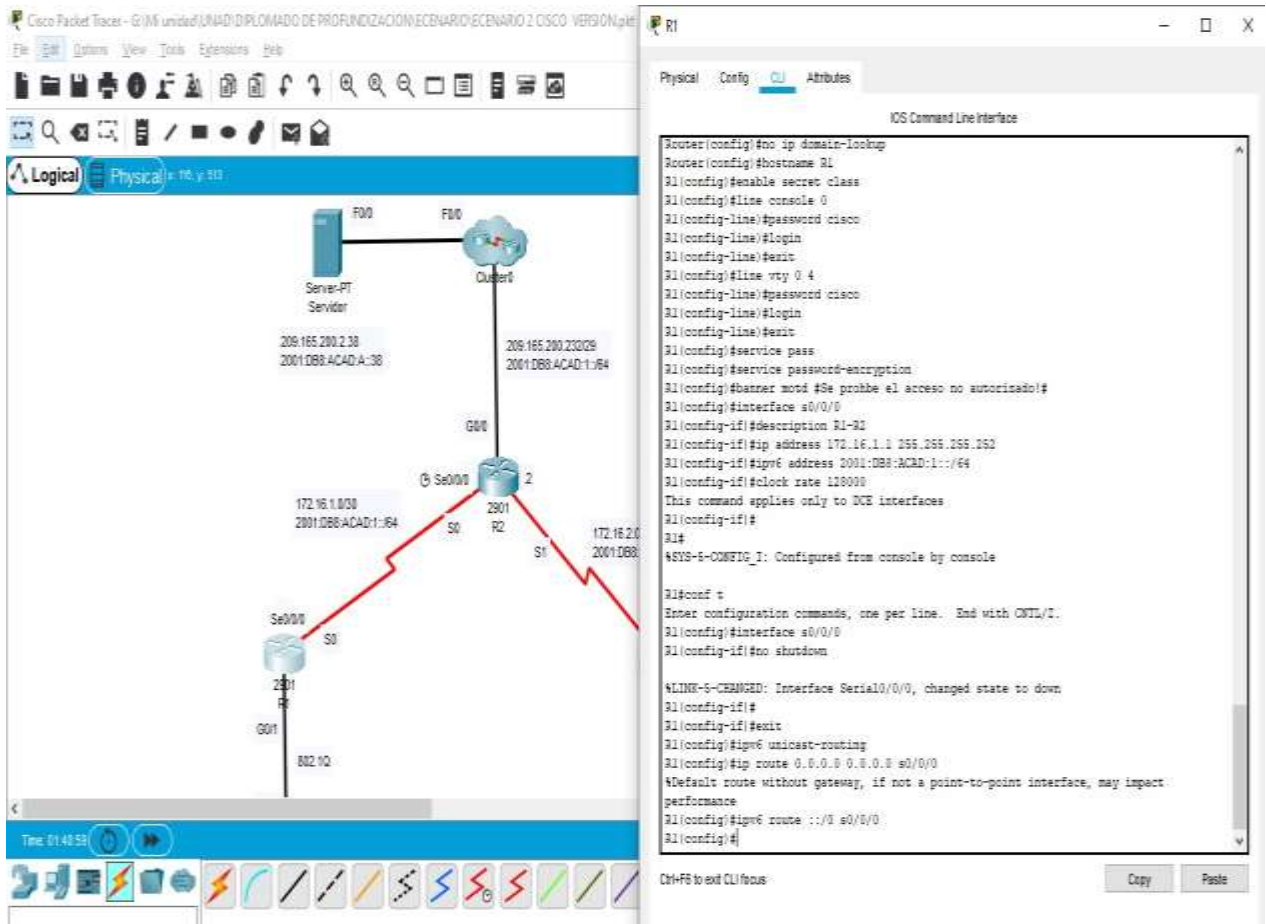


Figura 21. Configurar R1

Paso 3: Configurar R2

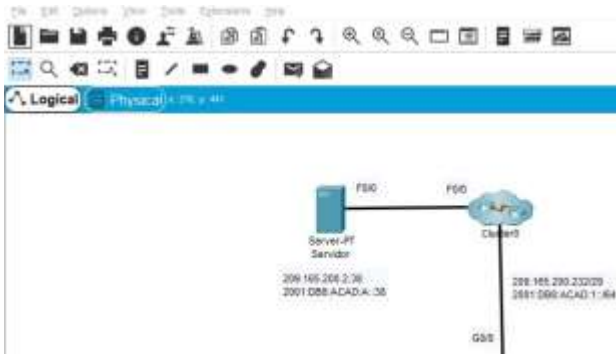
La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	hostname R2 R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	R2(config)#enable secret class R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit R2(config)#service pass R2(config)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server
Mensaje MOTD	R2(config)#banner motd #Se prohíbe el acceso no autorizado!# Se prohíbe el acceso no autorizado.

<p>Interfaz S0/0/0</p>	<p>Establezca la descripción</p> <pre>R2(config)#interface s0/0/0 R2(config-if)#description R2-R1</pre> <p>Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.</p> <pre>R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#no shutdown</pre> <p>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.</p> <p>Activar la interfaz</p> <pre>R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown</pre>
<p>Interfaz S0/0/1</p>	<p>Establecer la descripción</p> <pre>R2(config)#interface s0/0/1 R2(config-if)#description R2-R3</pre> <p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <pre>R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown</pre> <p>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.</p> <p>Establecer la frecuencia de reloj en 128000.</p> <p>Activar la interfaz</p> <pre>R2(config)#interface s0/0/1 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown</pre>

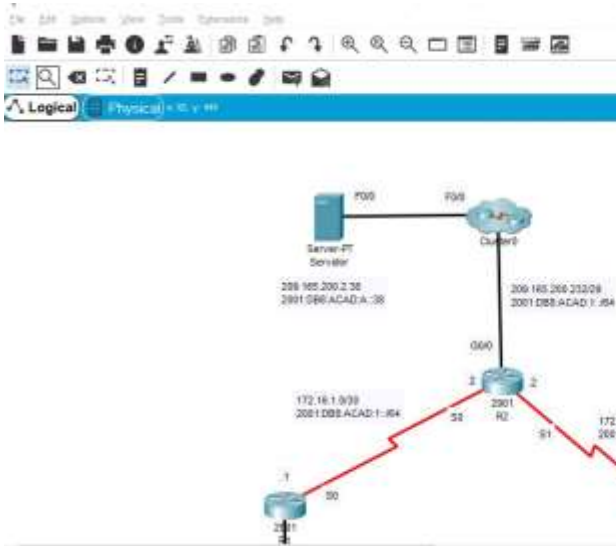
<p>Interfaz G0/0 (simulación de Internet)</p>	<p>Establecer la descripción.</p> <pre>R2(config)#interface g0/0 R2(config-if)#description R2-Internet</pre> <p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <pre>R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#no shutdown</pre> <p>Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred.</p> <p>Activar la interfaz</p> <pre>R2(config)#interface g0/0 R2(config-if)#description R2-Internet R2(config-if)#ipv6 address 2001:DB8:ACAD:A::2/64 R2(config-if)#no shutdown</pre>
<p>Interfaz loopback 0 (servidor web simulado)</p>	<p>Establecer la descripción.</p> <p>Establezca la dirección IPv4.</p> <pre>R2(config-if)#description SIMULADOR SERVIDOR WEB</pre> <pre>R2(config-if)#ip address 10.10.10.10 255.255.255.0 R2(config-if)#no shutdown</pre>
<p>Ruta predeterminada</p>	<p>Configure una ruta IPv4 predeterminada de G0/0.</p> <pre>R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0</pre> <p>Configure una ruta IPv6 predeterminada de G0/0.</p> <pre>R2(config)#ipv6 route ::/0 g0/0</pre>

Tabla 10. Configurar R2



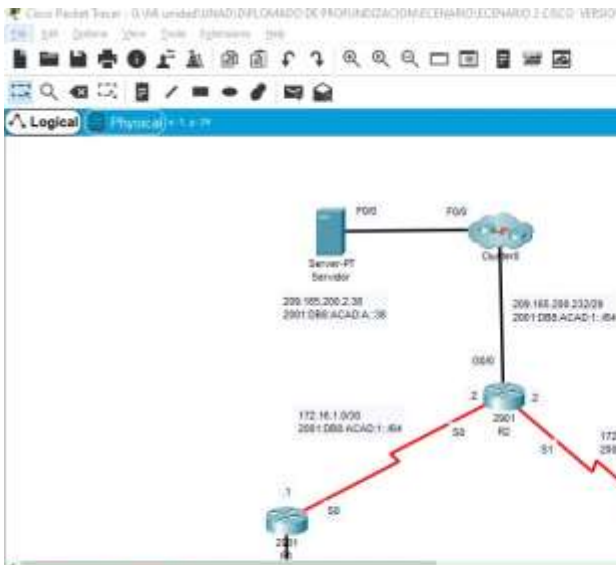
```

R2:
Physical Config CLI Attributes
IOS Command Line Interface
Router>
Router>en
Router>conf t
Enter configuration commands, one per line. End with CTRL/Z.
Router(config)#
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password class
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password class
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#ip http server
  
```



```

R2:
Physical Config CLI Attributes
IOS Command Line Interface
R1(config)#banner motd $!$ probe el access no autorizado!$
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#interface e0/0/0
R1(config-if)#description R2-R1
R1(config-if)#ip address 172.16.1.2 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#
LINE-1-CHANGED: Interface Serial0/0/0, changed state to up
R1(config-if)#
LINEPROTO-0-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to up
R1(config-if)#ipV6 address 2001:D85:ACAD:1::1/64
R1(config-if)#no shutdown
R1(config-if)#clock rate 120000
R1(config-if)#no shutdown
R1(config-if)#
R1(config-if)#
R1(config-if)#
Ctrl-F to exit CLI mode
  
```



```

R2:
Physical Config CLI Attributes
IOS Command Line Interface
R1(config)#banner motd $!$ probe el acceso no autorizado!$
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#interface e0/0/0
R1(config-if)#description R2-R1
R1(config-if)#ip address 172.16.1.2 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#
LINE-1-CHANGED: Interface Serial0/0/0, changed state to up
R1(config-if)#
LINEPROTO-0-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to up
R1(config-if)#ipV6 address 2001:D85:ACAD:1::2/64
R1(config-if)#no shutdown
R1(config-if)#clock rate 120000
R1(config-if)#no shutdown
R1(config-if)#
R1(config-if)#
R1(config-if)#
R1(config-if)#interface e0/0/1
R1(config-if)#description R2-R3
R1(config-if)#ip address 172.16.2.2 255.255.255.252
R1(config-if)#clock rate 120000
This command applies only to DCE interfaces.
R1(config-if)#no shutdown
LINE-1-CHANGED: Interface Serial0/0/1, changed state to down
R1(config-if)#
R1(config-if)#
R1(config-if)#
R1(config-if)#interface e0/0/3
R1(config-if)#description 2001:D85:ACAD:1::1/64
R1(config-if)#ipV6 address 2001:D85:ACAD:1::1/64
R1(config-if)#clock rate 120000
This command applies only to DCE interfaces.
Ctrl-F to exit CLI mode
  
```

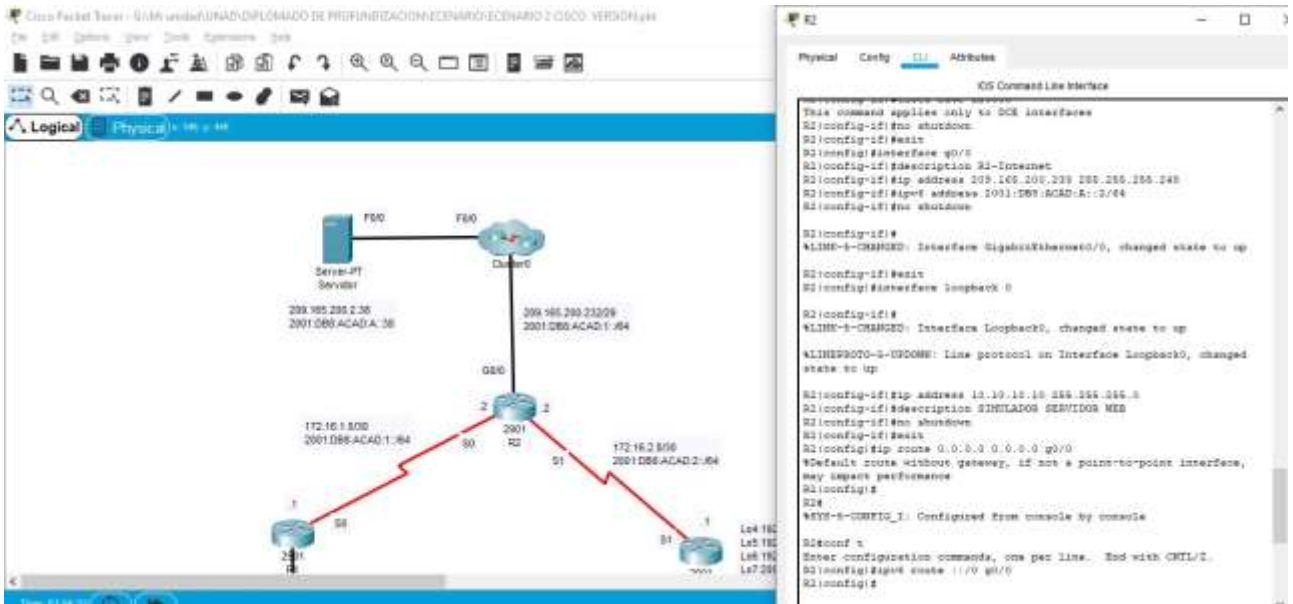


Figura 22. Configurar R2

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	hostname R3 R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	R3(config)#enable secret class R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit R3(config)#service pass R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #Se prohíbe el acceso no autorizado!# Se prohíbe el acceso no autorizado.

<p>Interfaz S0/0/1</p>	<p>Establecer la descripción R3(config)#interface s0/0/1 R3(config-if)#description R3-R2</p> <p>Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.</p> <p>R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#no shutdown</p> <p>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz</p> <p>R3(config)#interface s0/0/1 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R3(config-if)#no shutdown</p>
<p>Interfaz loopback 4</p>	<p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <p>R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0</p>
<p>Interfaz loopback 5</p>	<p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <p>R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0</p>
<p>Interfaz loopback 6</p>	<p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <p>R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0</p>
<p>Interfaz loopback 7</p>	<p>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.</p> <p>R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64</p>
<p>Rutas predeterminadas</p>	<p>R3(config)#interface s0/0/1 R3(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/1</p> <p>R3(config)#interface s0/0/1 R3(config-if)#ipv6 route ::/0 s0/0/1</p>

Tabla 11. Configurar R3

The figure consists of three screenshots from Cisco Packet Tracer, each showing a network diagram and a terminal window for configuring R3. The network diagram in all three shows a central R3 connected to two other routers (R1 and R2) and a server. The terminal windows show the following configuration steps:

First Screenshot: The terminal shows the configuration of the console interface and the first serial interface (S0/0/0).

```

R3>configure terminal
R3>enable
R3>conf t
R3>interface console 0
R3>ip address 10.10.10.1 255.255.255.0
R3>line 0
R3>password cisco
R3>login
R3>exit
R3>interface serial 0/0/0
R3>ip address 172.16.2.2 255.255.255.0
R3>no shutdown
R3>exit

```

Second Screenshot: The terminal shows the configuration of the second serial interface (S0/0/1).

```

R3>interface serial 0/0/1
R3>ip address 172.16.1.1 255.255.255.0
R3>no shutdown
R3>exit

```

Third Screenshot: The terminal shows the configuration of the loopback interface (L0).

```

R3>interface loopback 0
R3>ip address 10.10.10.1 255.255.255.0
R3>no shutdown
R3>exit

```

Figura 23. Configurar R3

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

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

Tabla 12. Configurar S1

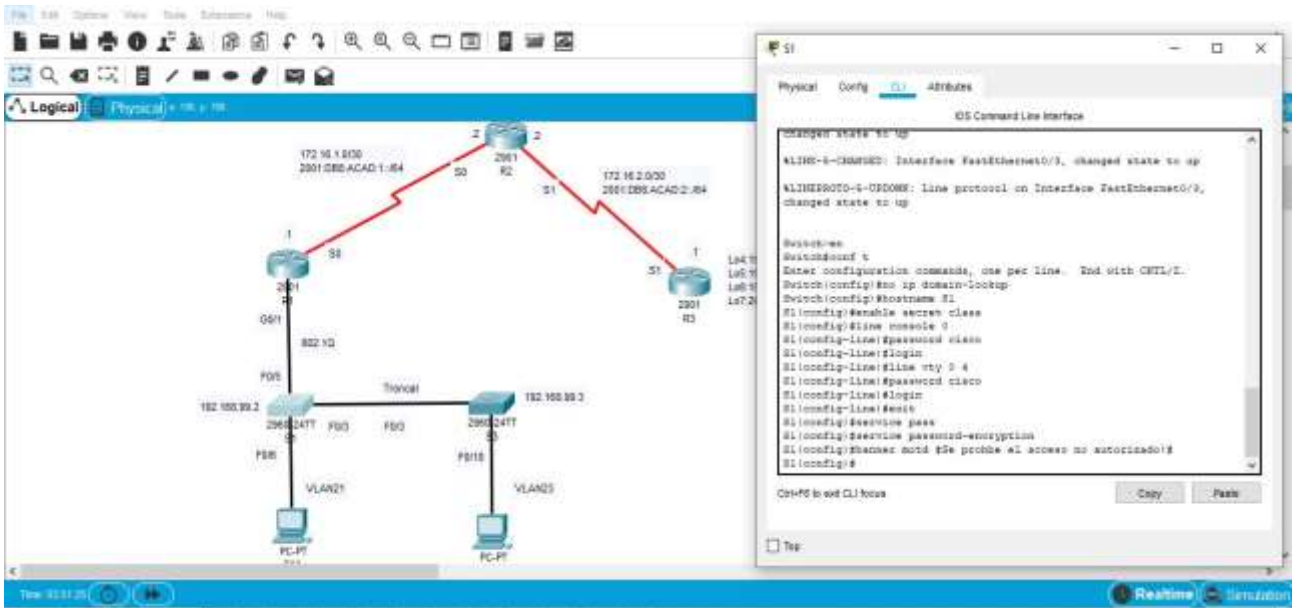


Figura 24. Configurar S1

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

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

Mensaje MOTD

Se prohíbe el acceso no autorizado.

S3(config)#banner motd #Se prohbe el acceso no autorizado!#

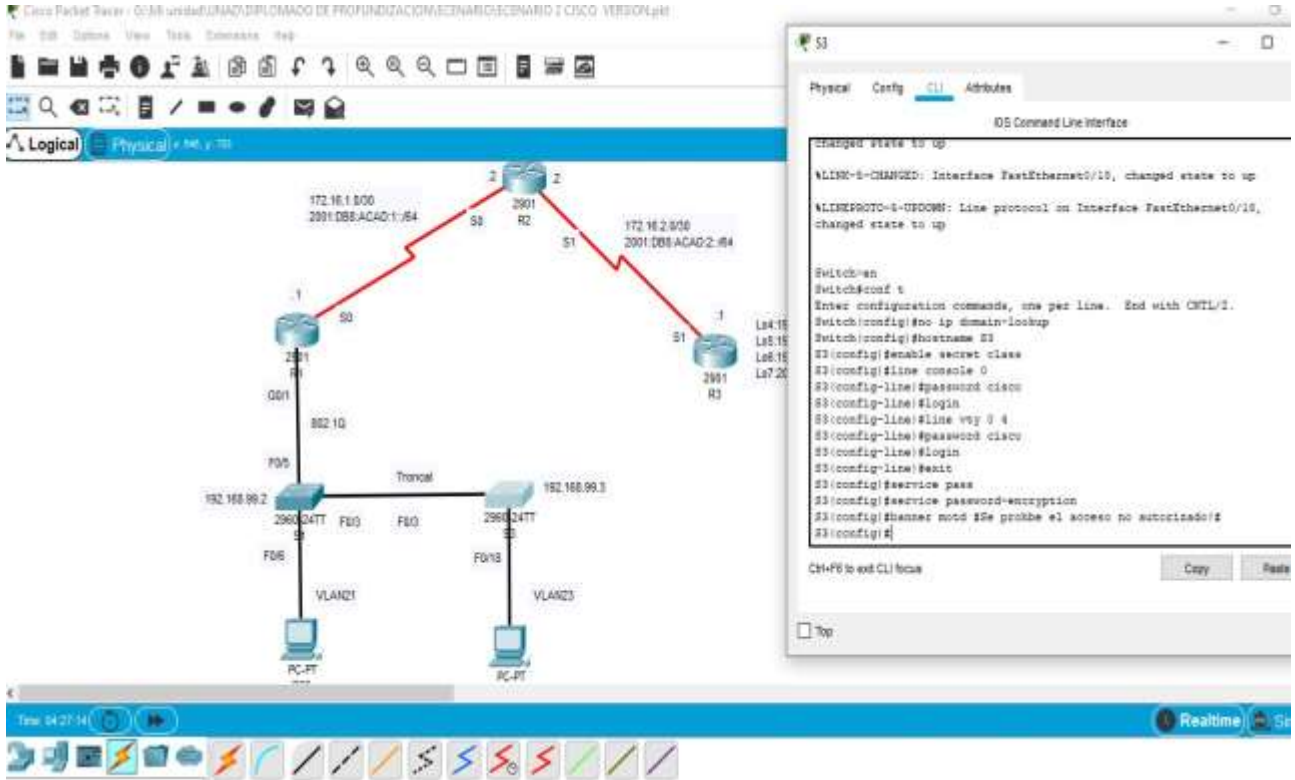


Figura 25. Configurar S3

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:

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

Tabla 14.verificacion conectividad de la Red

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



Figura 26. verificación conectividad de la Red

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:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	<p>Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican</p> <pre> S1(config)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#exit </pre>

Asignar la dirección IP de administración.	<p>Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología</p> <pre>S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#exit</pre>
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	<p>Utilizar la red VLAN 1 como VLAN nativa</p> <pre>S1(config)#interface f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit</pre>
Forzar el enlace troncal en la interfaz F0/5	<p>Utilizar la red VLAN 1 como VLAN nativa</p> <pre>S1(config)#interface f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit</pre>
Configurar el resto de los puertos como puertos de acceso	<p>Utilizar el comando interface range</p> <pre>S1(config-if)#interface range f0/1, f0/2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown</pre>
Asignar F0/6 a la VLAN 21	<pre>S1(config)#int fa0/6 S1(config-if)#switchport access vlan 21 S1(config-if)#exit</pre>
Apagar todos los puertos sin usar	<pre>S1(config)#int range fa0/1-2,fa0/4,f0/7-24,g0/1-2 S1(config-if-range)#shutdown</pre>

Tabla 15 Configurar la seguridad del switch, las VLAN y el routing entre VLAN S1

The figure consists of three screenshots from Cisco Packet Tracer, illustrating the configuration of a network topology for security, VLANs, and routing.

Top Screenshot (Physical Topology): Shows a network with three switches (S0, S1, S2) and two PCs (PC-PT). S0 and S1 are connected to S2. S0 and S1 are also connected to each other. S0 and S1 are connected to PC-PT. S0 and S1 are connected to S2. S0 and S1 are connected to S2. S0 and S1 are connected to S2.

Middle Screenshot (VLAN Configuration): Shows the configuration of VLANs on the switches. The configuration for S0 is as follows:

```

Switch S0 configuration:
Switch S0 configuration commands, one per line. End with CTRL-Z.
Switch S0
vlan 10
vlan 20
vlan 30
vlan 40
vlan 50
vlan 60
vlan 70
vlan 80
vlan 90
vlan 100
vlan 110
vlan 120
vlan 130
vlan 140
vlan 150
vlan 160
vlan 170
vlan 180
vlan 190
vlan 200
vlan 210
vlan 220
vlan 230
vlan 240
vlan 250
vlan 260
vlan 270
vlan 280
vlan 290
vlan 300
vlan 310
vlan 320
vlan 330
vlan 340
vlan 350
vlan 360
vlan 370
vlan 380
vlan 390
vlan 400
vlan 410
vlan 420
vlan 430
vlan 440
vlan 450
vlan 460
vlan 470
vlan 480
vlan 490
vlan 500
vlan 510
vlan 520
vlan 530
vlan 540
vlan 550
vlan 560
vlan 570
vlan 580
vlan 590
vlan 600
vlan 610
vlan 620
vlan 630
vlan 640
vlan 650
vlan 660
vlan 670
vlan 680
vlan 690
vlan 700
vlan 710
vlan 720
vlan 730
vlan 740
vlan 750
vlan 760
vlan 770
vlan 780
vlan 790
vlan 800
vlan 810
vlan 820
vlan 830
vlan 840
vlan 850
vlan 860
vlan 870
vlan 880
vlan 890
vlan 900
vlan 910
vlan 920
vlan 930
vlan 940
vlan 950
vlan 960
vlan 970
vlan 980
vlan 990
vlan 1000

```

Bottom Screenshot (Routing Configuration): Shows the configuration of inter-VLAN routing on the switches. The configuration for S0 is as follows:

```

Switch S0 configuration:
Switch S0 configuration commands, one per line. End with CTRL-Z.
Switch S0
vlan 10
vlan 20
vlan 30
vlan 40
vlan 50
vlan 60
vlan 70
vlan 80
vlan 90
vlan 100
vlan 110
vlan 120
vlan 130
vlan 140
vlan 150
vlan 160
vlan 170
vlan 180
vlan 190
vlan 200
vlan 210
vlan 220
vlan 230
vlan 240
vlan 250
vlan 260
vlan 270
vlan 280
vlan 290
vlan 300
vlan 310
vlan 320
vlan 330
vlan 340
vlan 350
vlan 360
vlan 370
vlan 380
vlan 390
vlan 400
vlan 410
vlan 420
vlan 430
vlan 440
vlan 450
vlan 460
vlan 470
vlan 480
vlan 490
vlan 500
vlan 510
vlan 520
vlan 530
vlan 540
vlan 550
vlan 560
vlan 570
vlan 580
vlan 590
vlan 600
vlan 610
vlan 620
vlan 630
vlan 640
vlan 650
vlan 660
vlan 670
vlan 680
vlan 690
vlan 700
vlan 710
vlan 720
vlan 730
vlan 740
vlan 750
vlan 760
vlan 770
vlan 780
vlan 790
vlan 800
vlan 810
vlan 820
vlan 830
vlan 840
vlan 850
vlan 860
vlan 870
vlan 880
vlan 890
vlan 900
vlan 910
vlan 920
vlan 930
vlan 940
vlan 950
vlan 960
vlan 970
vlan 980
vlan 990
vlan 1000

```

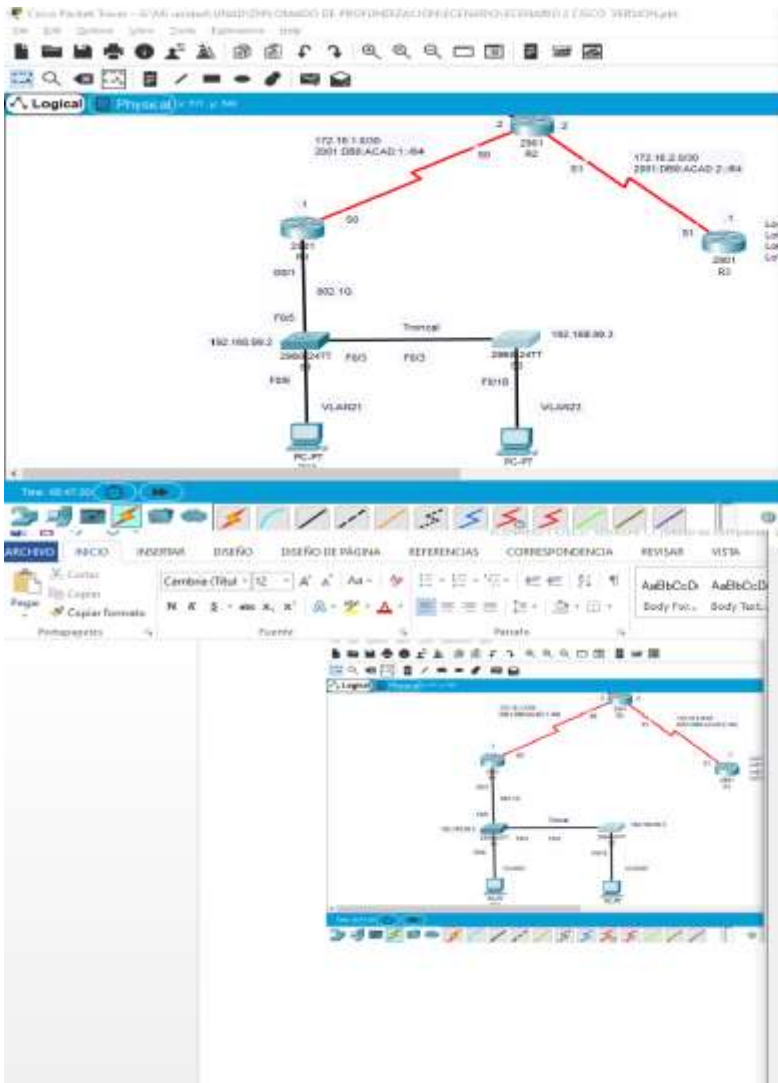
Figura 27. Configurar la seguridad del switch, las VLAN y el routing entre VLAN S1

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	<p>Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.</p> <pre>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</pre>
Asignar la dirección IP de administración	<p>Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología</p> <pre>S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown</pre>
Asignar el gateway predeterminado.	<p>Asignar la primera dirección IP en la subred como gateway predeterminado.</p>
Forzar el enlace troncal en la interfaz F0/3	<p>Utilizar la red VLAN 1 como VLAN nativa</p> <pre>S3(config)#interface f0/3 S3(config-if)#swi S3(config-if)#switchport mode trunk S3(config-if)#swi S3(config-if)#switchport trunk native vlan 1</pre>
Configurar el resto de los puertos como puertos de acceso	<p>Utilizar el comando interface range</p> <pre>S3(config)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#swi S3(config-if-range)#switchport mode access S3(config-if-range)#shutdown</pre>
Asignar F0/18 a la VLAN 21	<pre>S3(config)#int fa0/6 S3(config-if)#switchport access vlan 21 S3(config-if)#exit</pre>
Apagar todos los puertos sin usar	

Tabla 16 Configurar la seguridad del switch, las VLAN y el routing entre VLAN S3



```

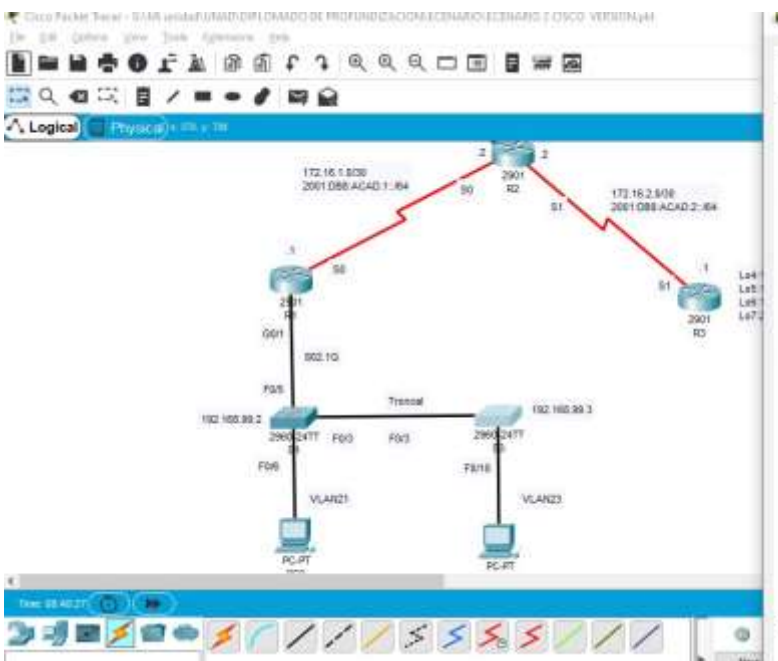
IOS Command Line Interface

R3>en
R3>conf t
Enter configuration commands, one per line. End with CNTL-Z.
R3(config)#
R3(config)#vlan 21
R3(config-vlan)#name Conectividad
R3(config-vlan)#exit
R3(config)#vlan 23
R3(config-vlan)#name Inspecta
R3(config-vlan)#exit
R3(config)#vlan 99
R3(config-vlan)#name Administration
R3(config-vlan)#exit
R3(config)#
R3(config)#interface FastEthernet 0/24
R3(config-if)#
R3(config-if)#shutdown
%LINK-3-CHANGED: Interface FastEthernet0/24, changed state to up
%LINKS-3-DCOORN- Line personal on Interface Vlan21, changed state to up
R3(config-if)#ip address 192.168.90.9 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface FastEthernet 0/0
R3(config-if)#shutdown
R3(config-if)#
R3(config-if)#interface range FastEthernet 0/24-27, 0/28-29, 0/30-31
R3(config-if-range)#shutdown
R3(config-if-range)#exit
R3(config)#
R3(config)#interface FastEthernet0/2
R3(config-if)#
R3(config-if)#shutdown
%LINK-3-CHANGED: Interface FastEthernet0/2, changed state to administratively down
R3(config-if)#
R3(config)#interface FastEthernet0/3
R3(config-if)#
R3(config-if)#shutdown
%LINK-3-CHANGED: Interface FastEthernet0/3, changed state to administratively down
R3(config-if)#
R3(config)#
R3>
  
```

```

IOS Command Line Interface

administratively down
%LINK-3-CHANGED: Interface FastEthernet0/2, changed state to administratively down
%LINK-3-CHANGED: Interface FastEthernet0/4, changed state to administratively down
%LINK-3-CHANGED: Interface FastEthernet0/6, changed state to administratively down
%LINK-3-CHANGED: Interface FastEthernet0/8, changed state to administratively down
%LINK-3-CHANGED: Interface FastEthernet0/7, changed state to administratively down
%LINK-3-CHANGED: Interface FastEthernet0/9, changed state to administratively down
%LINK-3-CHANGED: Interface FastEthernet0/10, changed state to administratively down
%LINK-3-CHANGED: Interface FastEthernet0/11, changed state to administratively down
%LINK-3-CHANGED: Interface FastEthernet0/11, changed state to administratively down
%LINK-3-CHANGED: Interface FastEthernet0/12, changed state to administratively down
%LINK-3-CHANGED: Interface FastEthernet0/13, changed state to administratively down
%LINK-3-CHANGED: Interface FastEthernet0/14, changed state to administratively down
R3>
  
```



```

IOS Command Line Interface

administratively down
%LINK-3-CHANGED: Interface FastEthernet0/18, changed state to administratively down
%LINK-3-CHANGED: Interface FastEthernet0/17, changed state to administratively down
%LINK-3-CHANGED: Interface FastEthernet0/15, changed state to administratively down
%LINK-3-CHANGED: Interface FastEthernet0/20, changed state to administratively down
%LINK-3-CHANGED: Interface FastEthernet0/21, changed state to administratively down
%LINK-3-CHANGED: Interface FastEthernet0/22, changed state to administratively down
%LINK-3-CHANGED: Interface FastEthernet0/23, changed state to administratively down
%LINK-3-CHANGED: Interface FastEthernet0/24, changed state to administratively down
%LINK-3-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
%LINK-3-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
R3(config-if-range)#
R3(config-if-range)#exit
R3(config-if-range)#
R3(config)#interface FastEthernet 0/18
R3(config-if)#switchport access vlan 21
R3(config-if)#exit
R3(config-if)#
R3>
  
```

Figura 28. Configurar la seguridad del switch, las VLAN y el routing entre VLAN S3

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	<p>Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz</p> <pre>R1(config)#interface g0/1.21 R1(config-subif)#description LAN_Contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.2 255.255.255.0 R1(config-subif)#exit</pre>
Configurar la subinterfaz 802.1Q .23 en G0/1	<p>Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz</p> <pre>R1(config)#interface g0/1.23 R1(config-subif)#description LAN_Ingenieria R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.2 255.255.255.0 R1(config-subif)#exit</pre>
Configurar la subinterfaz 802.1Q .99 en G0/1	<p>Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz</p> <pre>R1(config)#interface g0/1.99 R1(config-subif)#description LAN_Administracion R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#exit</pre>
Activar la interfaz G0/1	<pre>R1(config)#interface g0/1 R1(config-if)#no shutdown R1(config-if)#exit</pre>

Tabla 17 Configurar la seguridad del switch, las VLAN y el routing entre VLAN R1

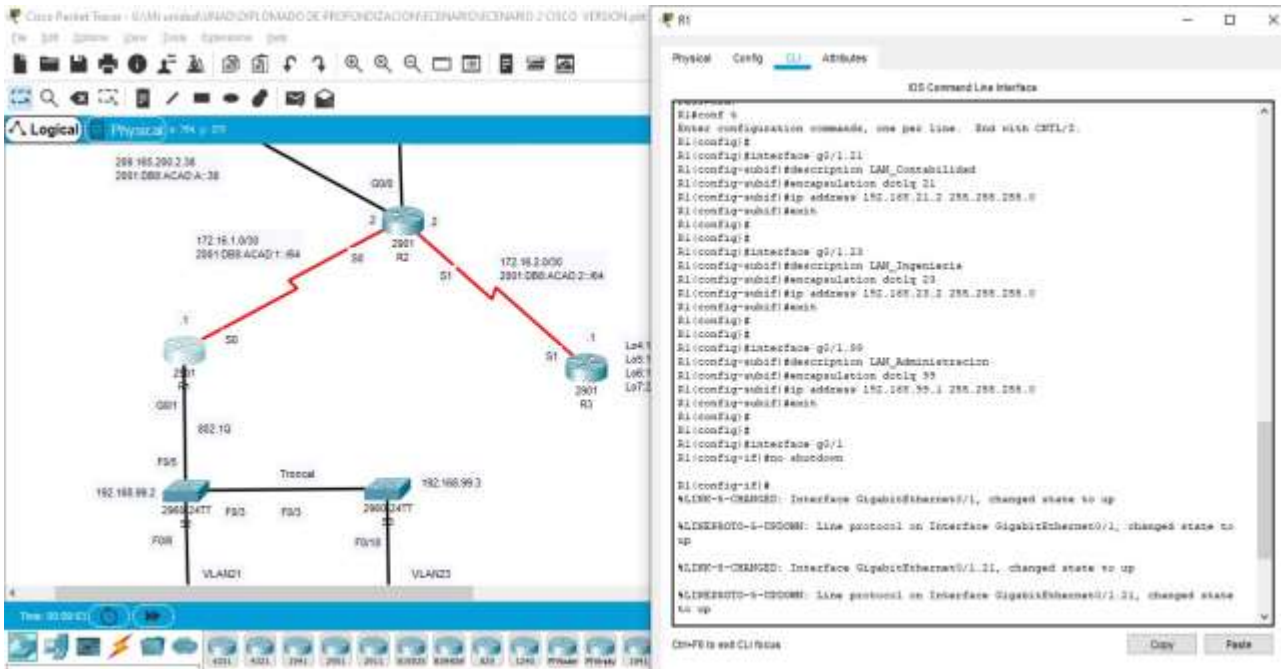


Figura 29. Configurar la seguridad del switch, las VLAN y el routing entre VLAN R1

La seguridad en estos dispositivos es comúnmente utilizada para restringir accesos no permitidos a una red con el fin de evitar pérdida de información y propagación de usuarios no autorizados

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:

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	exitoso
S3	R1, dirección VLAN 99	192.168.99.1	exitoso
S1	R1, dirección VLAN 21	192.168.21.2	exitoso
S3	R1, dirección VLAN 23	192.168.23.2	exitoso

Tabla 18. Verificar la conectividad de la red en switches y R1

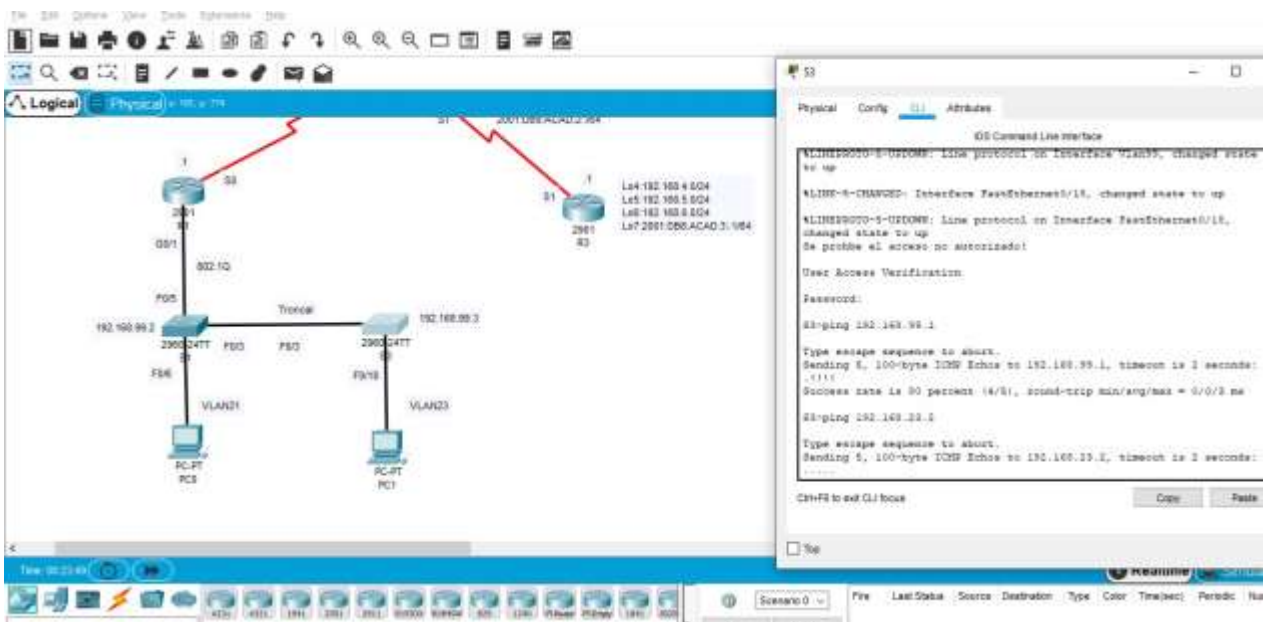
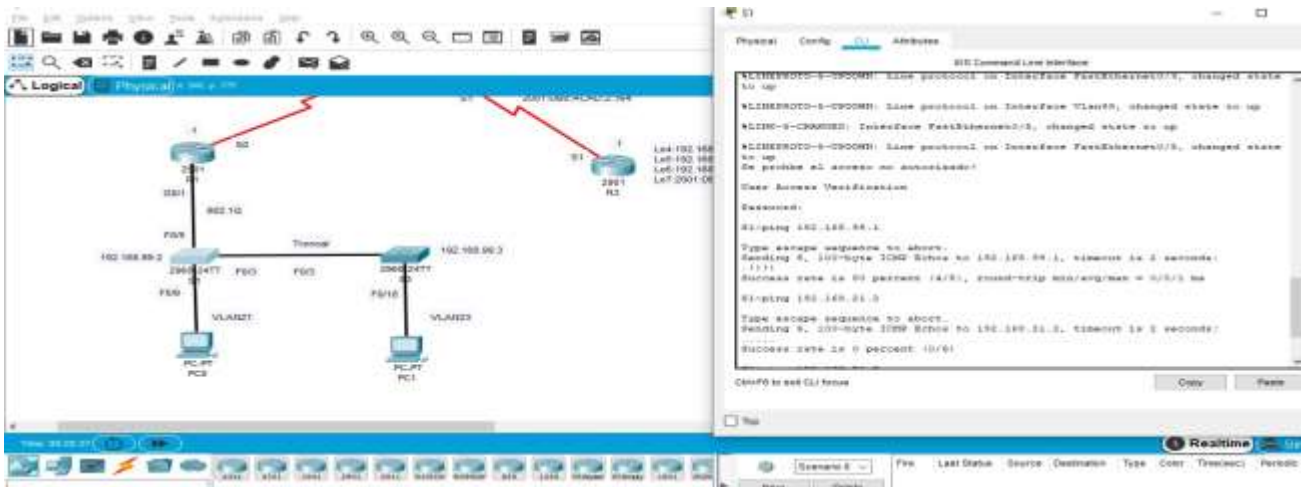


Figura 30. Verificar la conectividad de la red en switches y R1

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:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1

<p>Anunciar las redes conectadas directamente</p>	<p>Asigne todas las redes conectadas directamente.</p> <pre>R1(config-router)#network 172.16.1.0 255.255.255.252 area 0 R1(config-router)#network 172.16.1.8 255.255.255.252 area 0 R1(config-router)#network 192.168.21.0 255.255.255.0 area 0 R1(config-router)#network 192.168.23.0 255.255.255.0 area 0 R1(config-router)#network 192.168.99.0 255.255.255.0 area 0</pre>
<p>Establecer todas las interfaces LAN como pasivas</p>	<pre>R1(config)#router ospf 1 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)#passive-interface s0/0/0</pre>
<p>Desactive la sumarización automática</p>	<pre>R1(config-router)#no auto-summary</pre>

Table 19. Configurar el protocolo de routing dinámico OSPF R1

The image shows a network simulator interface with a network diagram on the left and a configuration window for router R1 on the right.

Network Diagram: The diagram shows a central router R2 (2901) connected to three other routers: R1 (2901) on the left, R3 (2901) on the right, and a switch (2960) at the bottom. R2 is connected to R1 via S0/S1 and to R3 via S1/S0. R2 is also connected to the switch via G0/0/24. The switch has two VLANs: VLAN21 (192.168.99.0/24) and VLAN23 (192.168.99.0/24). The switch is connected to two PCs (2960) via F0/24 and F0/18. The PCs are connected to the switch via F36 and F0/24. The network is divided into three areas: Area 0 (172.16.1.0/24), Area 1 (172.16.2.0/24), and Area 2 (192.168.21.0/24).

Configuration Window (R1): The window shows the configuration for router R1. The configuration is as follows:

```
R1(config)#interface serial0/0/0
R1(config-if)#
R1(config-if)#exit
R1(config)#interface Serial0/0/1
R1(config-if)#
R1(config-if)#exit
R1(config)#interface Serial0/0/0
R1(config-if)#
R1(config-if)#exit
R1(config)#
R1(config)#router ospf 1
R1(config-router)#network 172.16.1.0 255.255.255.252 area 0
R1(config-router)#network 172.16.2.0 255.255.255.252 area 0
R1(config-router)#network 192.168.21.0 255.255.255.0 area 0
R1(config-router)#network 192.168.23.0 255.255.255.0 area 0
R1(config-router)#network 192.168.99.0 255.255.255.0 area 0
R1(config-router)#exit
R1(config)#
```

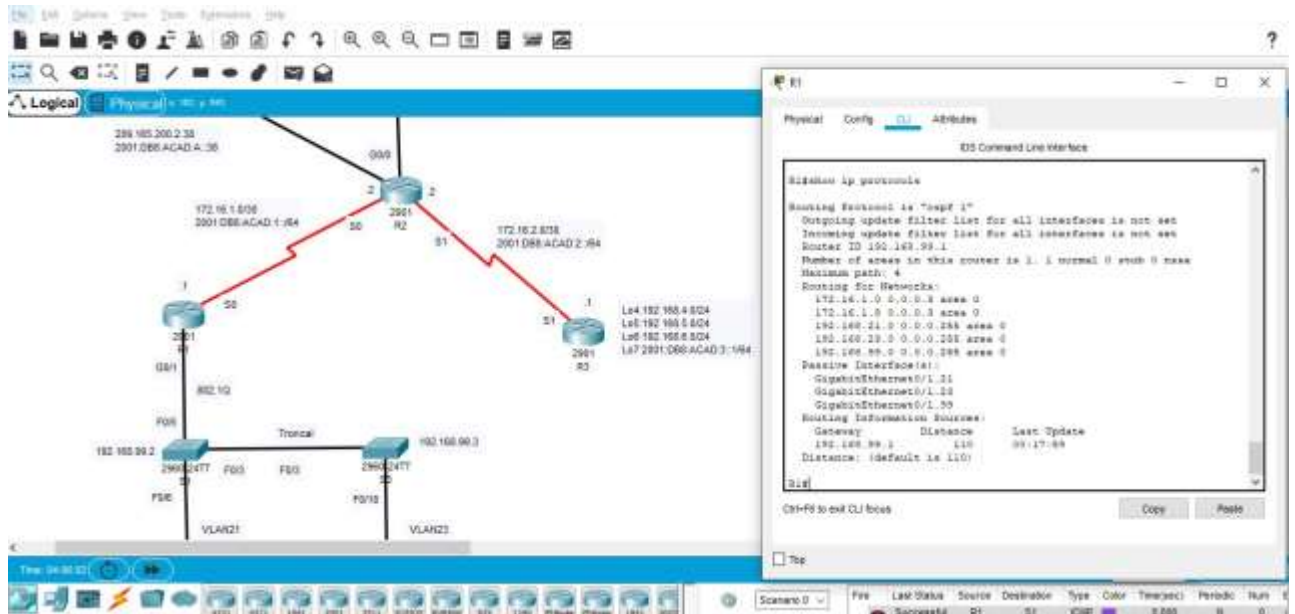


Figura 31. Configurar el protocolo de routing dinámico OSPF R1

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1
Anunciar las redes conectadas directamente	Nota: Omitir la red G0/0. R2(config-router)#network 10.10.10.0 255.255.255.0 area 0 R2(config-router)#network 172.16.1.0 255.255.255.252 area 0 R2(config-router)#network 172.16.2.0 255.255.255.252 area 0 R2(config-router)#exit
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Table 20. Paso 2. Configurar OSPF en el R2

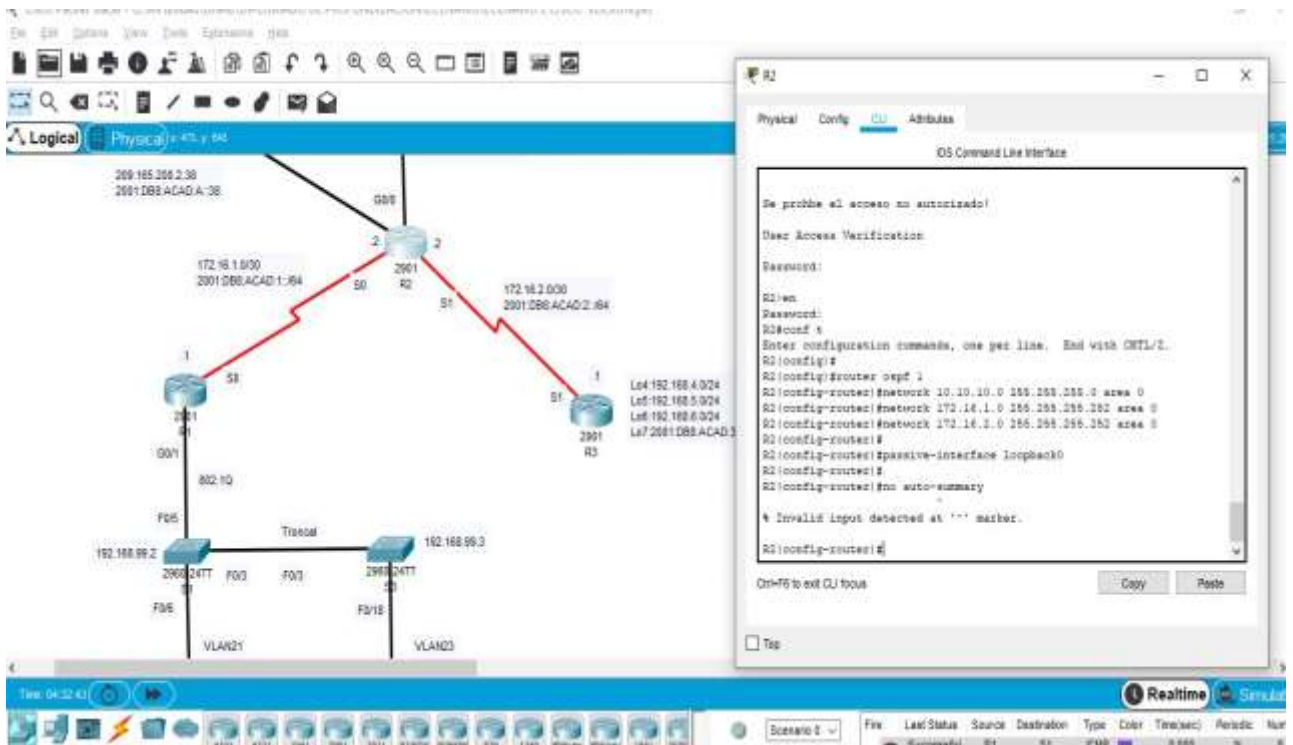


Figura 32. Configurar OSPF en el R2

Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 1
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 255.255.255.252 area 0 R3(config-router)#network 192.168.4.0 255.255.255.0 area 0 R3(config-router)#network 192.168.5.0 255.255.255.0 area 0 R3(config-router)#network 192.168.6.0 255.255.255.0 area 0 R3(config-router)#exit
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback4 R3(config-router)#passive-interface loopback5 R3(config-router)#passive-interface loopback6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Tabla 21. Configurar OSPFv3 en el R2

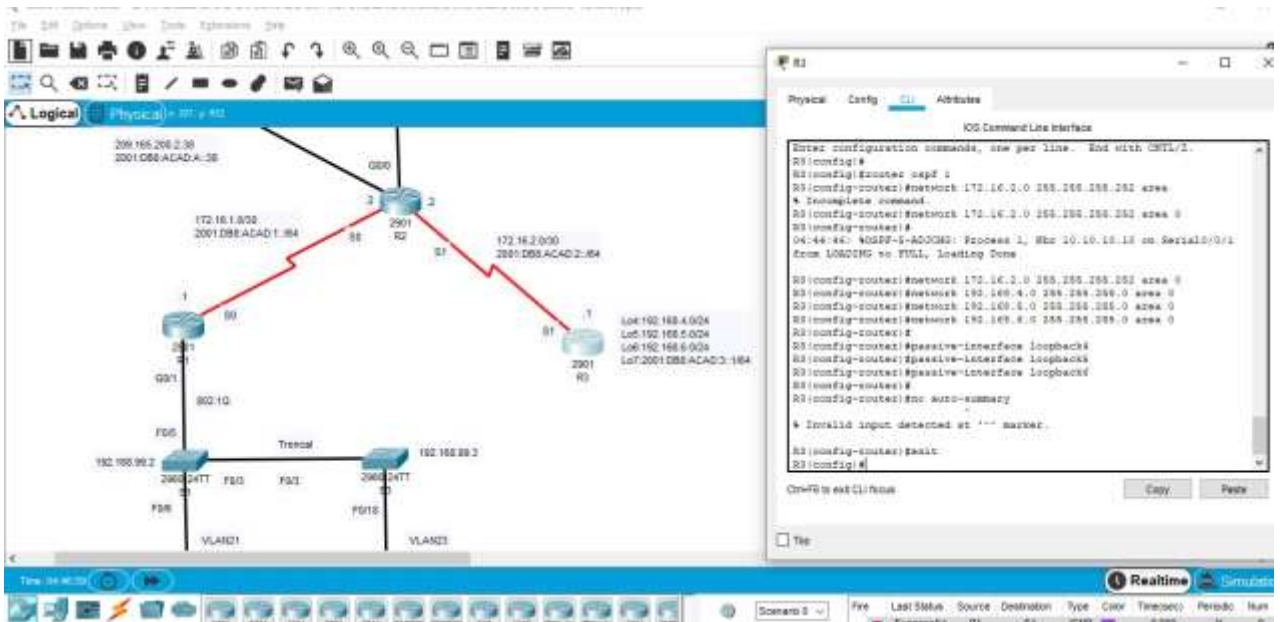


Figura 33. Configurar OSPFv3 en el R2

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:

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#debug ip rip
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R1#show ip route

Tabla 22. Verificar la información de OSPF

The screenshot shows a network diagram in Cisco Packet Tracer. The network consists of several routers and switches. Router R3 is highlighted, and its CLI is open, showing the following configuration and output:

```

R3#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 192.168.6.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.2.0 0.0.0.0 area 0
    192.168.4.0 0.0.0.255 area 2
    192.168.5.0 0.0.0.255 area 2
    192.168.6.0 0.0.0.255 area 2
  Passive Interface(s):
    Loopback4
    Loopback5
    Loopback6
  Routing Information Sources:
    Gateway         Distance      Last Update
  10.10.10.10       110           00:04:18
  192.168.5.1       110           00:05:20
  Distance: (Default is 110)

R3#
  
```

Below the CLI, a table shows the OSPF routing table:

Pre	Last Status	Source	Destination	Type	Cost	Time(s)	Period	Num
●	Successful	R1	S1	ICMP	1000	0	0	1
●	Successful	R1	R2	ICMP	1000	0	0	1

The screenshot shows the same network diagram as above. The CLI of Router R3 is open, displaying the OSPF routing table:

```

R3#show ip route
Codes: L - local, C - connected, S - static, B - BGP, H - mobile, W - WSP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

10.0.0.0/32 is subnetted, 1 subnets
  10.10.10.10/32 [110/0] via 172.16.2.2, 00:10:00, Serial0/0/1
172.16.0.0/24 is variably subnetted, 3 subnets, 2 masks
  172.16.2.0/30 [110/0] via 172.16.2.2, 00:10:00, Serial0/0/1
  172.16.2.0/30 is directly connected, Serial0/0/1
192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
  C 192.168.4.0/24 is directly connected, Loopback4
  S 192.168.4.1/32 is directly connected, Loopback4
192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
  C 192.168.5.0/24 is directly connected, Loopback5
  L 192.168.5.1/32 is directly connected, Loopback5
192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
  C 192.168.6.0/24 is directly connected, Loopback6
  S 192.168.6.1/32 is directly connected, Loopback6
O* 0.0.0.0/0 is directly connected, Serial0/0/1

R3#
  
```

Figura 34. Verificar la información de OSPF

Se evidencia la ejecución de este protocolo el cual busca una identificación del camino mas corto en la red utilizando un encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP).

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:

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

Tabla 23. Implementar DHCP y NAT para IPv4

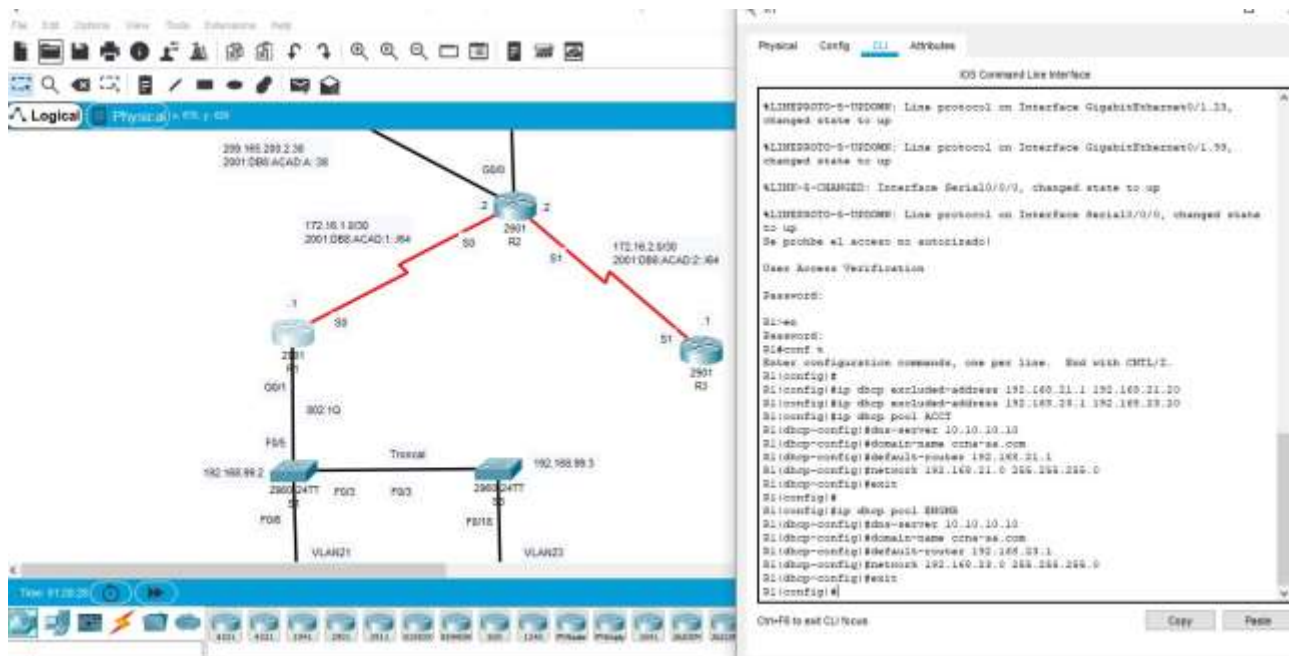


Figura 35. Implementar DHCP y NAT para IPv4

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

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15 R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server (no soportado)
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local (no soportado)
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229 R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#interface g0/0 R2(config-if)#ip nat inside R2(config-if)#exit

<p>Configurar la NAT dinámica dentro de una ACL privada</p>	<p>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</p> <pre>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 192.168.4.1 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.1 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.1 0.0.0.255</pre>
<p>Defina el pool de direcciones IP públicas utilizables.</p>	<p>Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228</p> <pre>R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248 R2(config)#ip nat inside source list 1 pool INTERNET</pre>
<p>Definir la traducción de NAT dinámica</p>	

Tabla 24. Configurar la NAT estática y dinámica en el R2

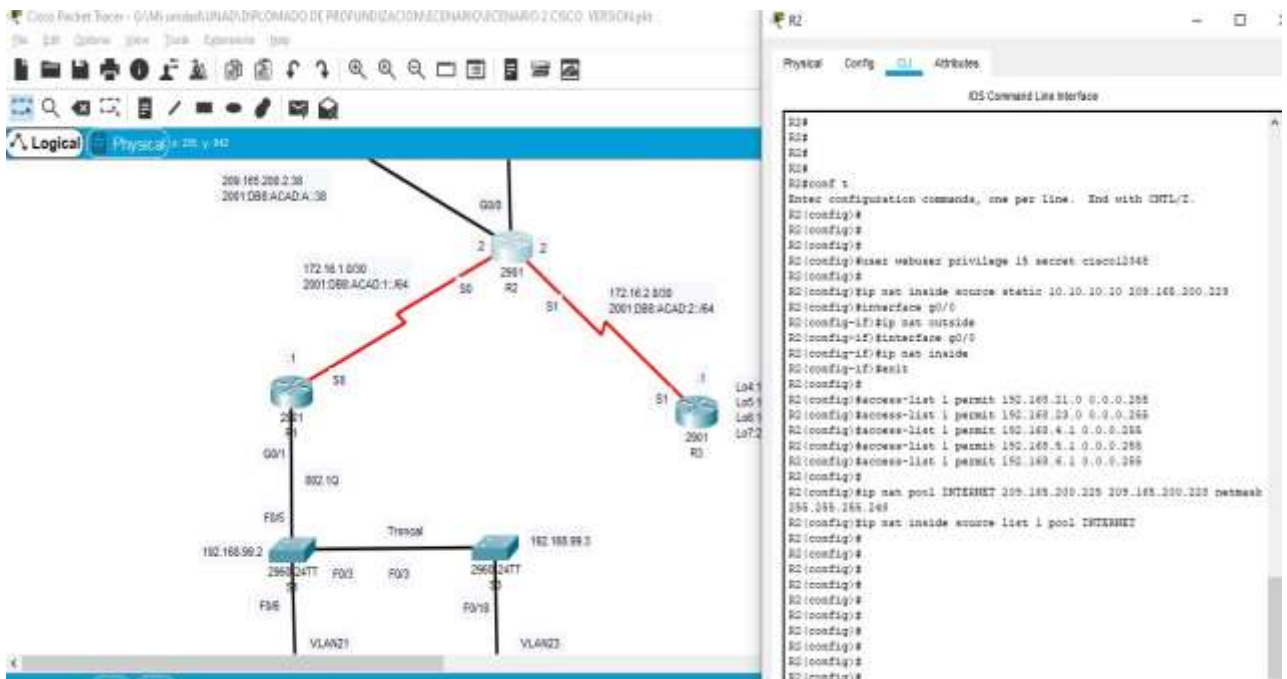


Figura 36. Configurar la NAT estática y dinámica en el R2

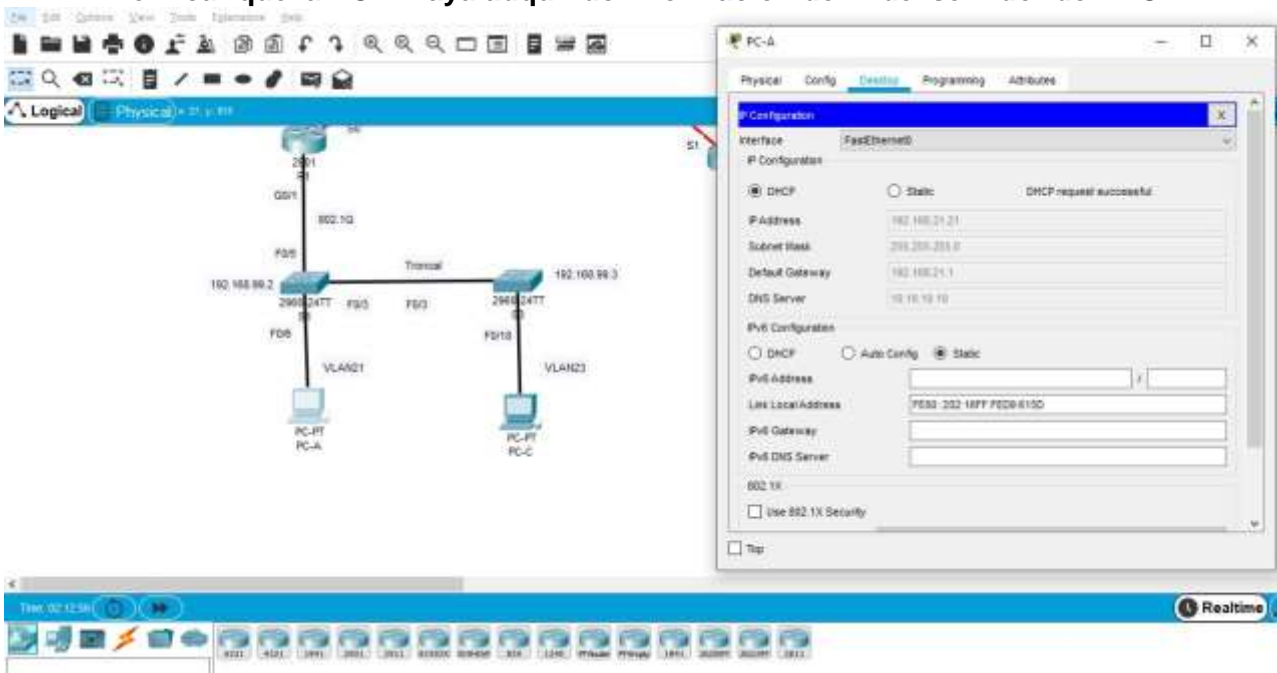
Paso 3: Verificar el protocolo DHCP y la NAT estática

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.

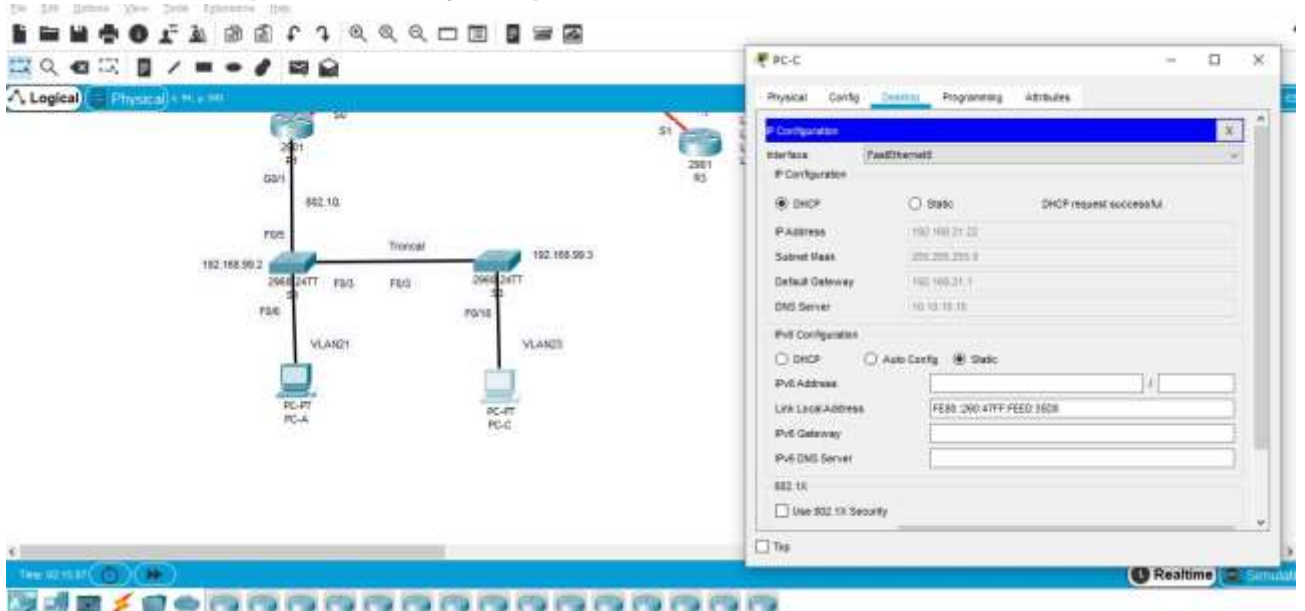
Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Ping 192.168.23.21 exitoso
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	

Tabla 25. Verificar el protocolo DHCP y la NAT estática

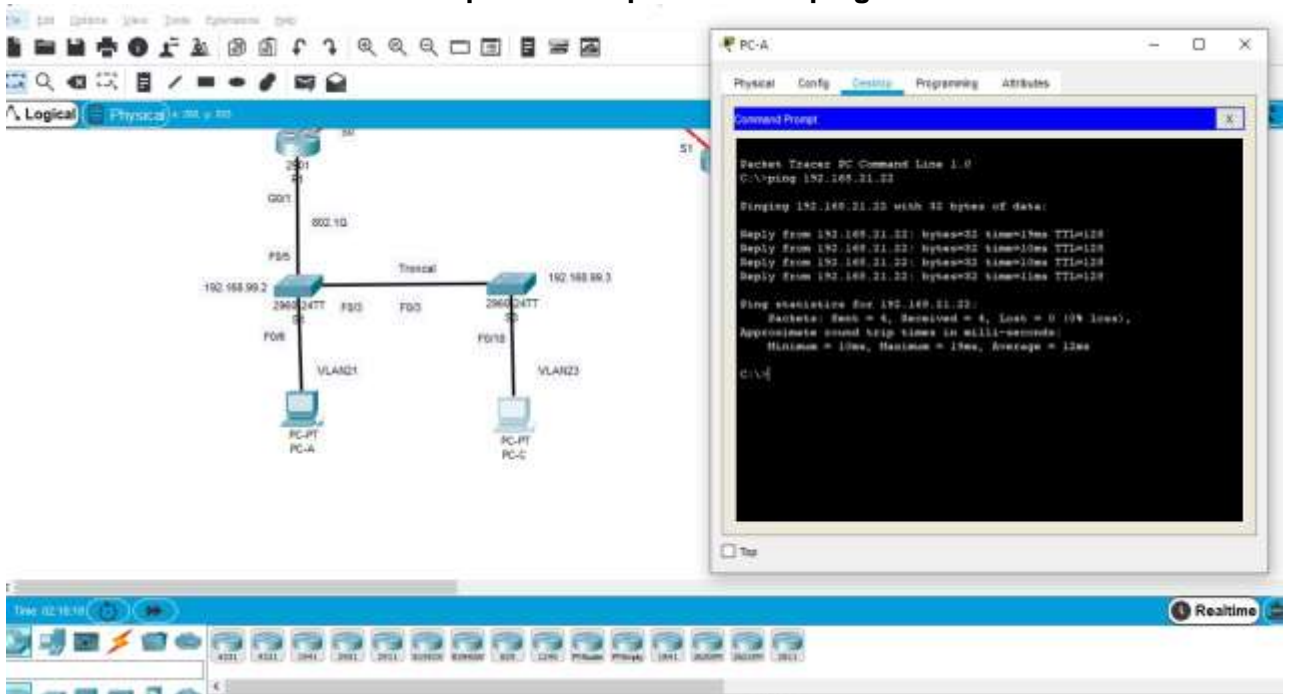
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP



Verificar que la PC-C haya adquirido información de IP del servidor de DHCP



Verificar que la PC-A pueda hacer ping a la PC-C



Figuras 37. Tabla 25. Verificar el protocolo DHCP y la NAT estática

Parte 6: Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	5 de marzo de 2016, 9 a. m. R2#clock set 9:00:00 March 5 2016
Configure R2 como un maestro NTP.	Nivel de estrato: 5 R2(config)#ntp master Stratum 5 (no soportado por cisco)
Configure R1 como un cliente NTP.	Servidor: R2 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(config)#do show ntp status

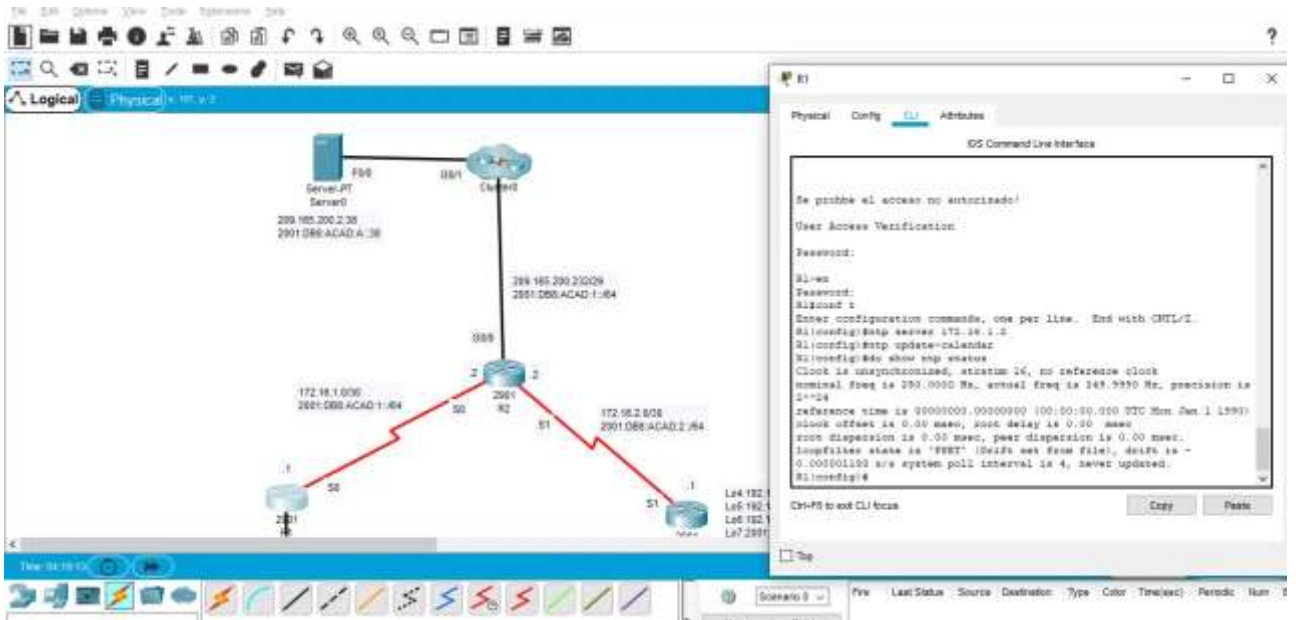
Tabla 26. Configurar NTP

```

R2#
R2#clock set 9:00:00 March 5 2016
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp master Stratum 5
^
% Invalid input detected at '^' marker.
R2(config)#
    
```

Ctrl+F6 to exit CLI focus

Copy Paste



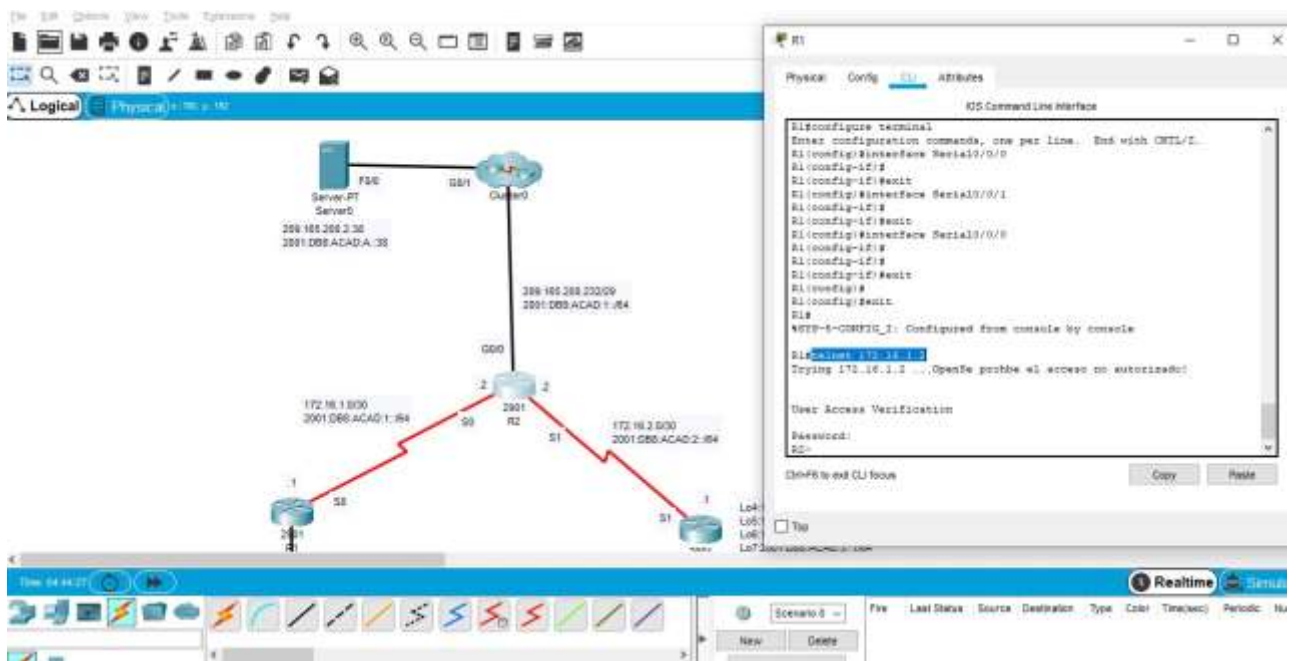
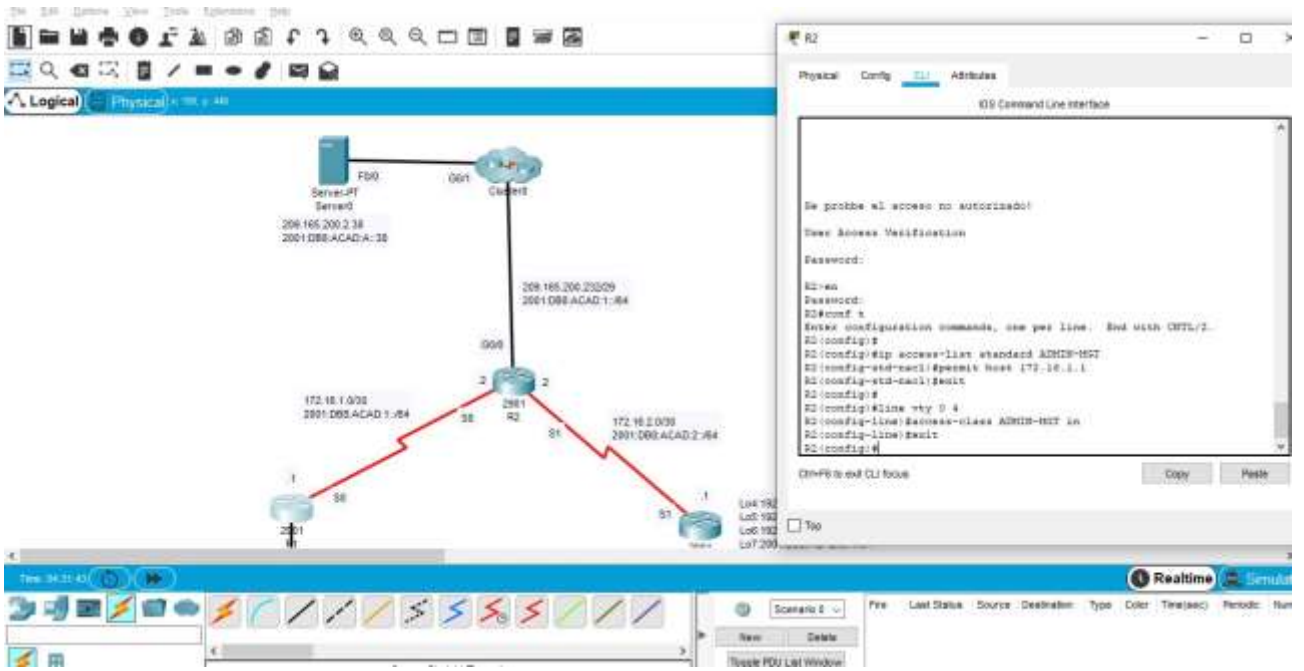
Figuras 38. Configurar NTP

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

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

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: ADMIN-MGT R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#access-class ADMIN-MGT in R2(config-line)#exit
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2

Tabla 27. Configurar y verificar las listas de control de acceso (ACL)



Figuras 39. Configurar y verificar las listas de control de acceso (ACL)

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

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Router(config)#show access-list
Restablecer los contadores de una lista de acceso	Router(config)#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Router(config)#interface Fa0/1 Router(config-if)#ip access-group 1 out R2#sh ip int s0/0/1
¿Con qué comando se muestran las traducciones NAT?	Router(config)#show ip nat translations Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Router(config)#clear ip nat translation

Tabla 28. Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

The image shows a network simulation environment. On the left, a network diagram displays a central router (R2) connected to a Server-PT (Server) and two other routers (R1 and R3). The Server-PT has IP 209.165.209.138 and is connected to R2 via interface G0/0. R2 has interfaces S0/0/1 and S0/0/2 connected to R1 and R3 respectively. On the right, a CLI window for R2 shows the following commands and output:

```

R2#
R2#
R2#show access-list
Standard IP access list 1
 10 permit 192.168.21.0 0.0.0.255
 20 permit 192.168.22.0 0.0.0.255
 30 permit 192.168.4.0 0.0.0.255
 40 permit 192.168.5.0 0.0.0.255
 50 permit 192.168.6.0 0.0.0.255
Standard IP access list ADMIN-HOST
 10 permit host 172.16.1.1 (3 matches)
R2#clear access-list counters
R2#
R2#show access-list
Standard IP access list 1
 10 permit 192.168.21.0 0.0.0.255
 20 permit 192.168.22.0 0.0.0.255
 30 permit 192.168.4.0 0.0.0.255
 40 permit 192.168.5.0 0.0.0.255
 50 permit 192.168.6.0 0.0.0.255
Standard IP access list ADMIN-HOST
 10 permit host 172.16.1.1
R2#
  
```

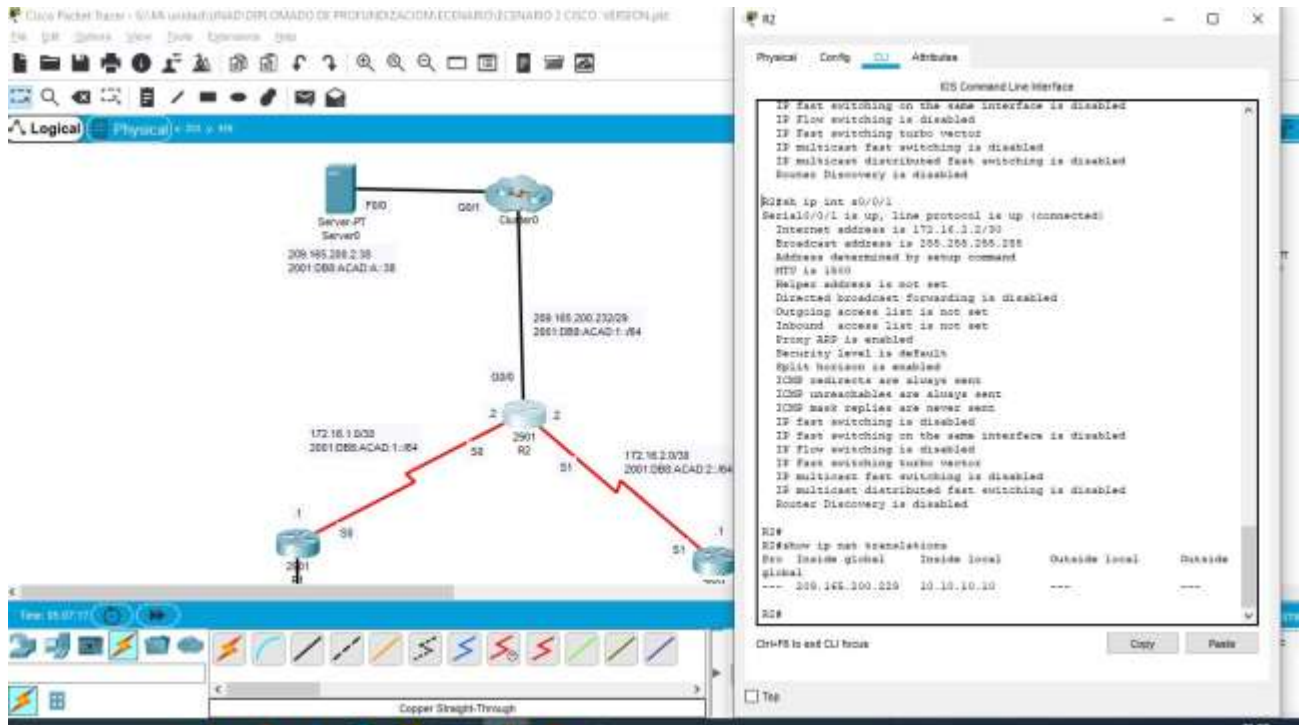



Figura 40. Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Link Archivos De Simulación En Packet Tracer y artículo científico

https://drive.google.com/drive/folders/1Jyk7d8Wbh6qU82vTpETi3Z_bhxqs2cUL?usp=sharing

Conclusiones

Mediante la elaboración, implementación y puesta en marcha de los dos escenarios se logró afianzar y fortalecer los conocimientos aprendidos durante el desarrollo del Diplomado de Profundización Cisco (Diseño E Implementación De Soluciones Integradas Lan / Wan), es un acierto emprender esta nueva etapa como ingenieros de sistemas con conocimientos en esta área los cuales en la actualidad están ofreciendo el punto de partida en el desarrollo tecnológico nacional y mundial, es por esto que este nuevo conocimiento adquirido marca un plus frente a la competencia sana en la obtención de oportunidades laborales.

Referencias Bibliográficas

CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking.

Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1>

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de

Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1>

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación.

Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1>

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación.

Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1>

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación.

Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación.

Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1>