

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

IVAN FELIPE STEVENSON ZULETA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
VALLEDUPAR
2021

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

IVAN FELIPE STEVENSON ZULETA

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

DIRECTOR:

MSc. NANCY AMPARO GUACA

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

INGENIERÍA DE SISTEMAS

VALLEDUPAR

2021

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Valledupar, 10 de diciembre de 2021

AGRADECIMIENTOS

A mi familia que siempre estuvo apoyándome en este proceso académico, dando de su tiempo y comprensión para brindar la ayuda necesaria para que este trabajo saliera de la mejor forma.

Al tutor que con sus enseñanzas se pudieron lograr los objetivos trazados en este documento.

A todas aquellas personas que hicieron parte de este proceso académico, gracias a todos.

Sobre todo, a lo supremo, que va más allá de nuestra imaginación y que hizo de este trabajo algo llevadero y que se realizó con esfuerzo y dedicación

CONTENIDO

AGRADECIMIENTOS.....	4
LISTA DE TABLAS	6
LISTA DE FIGURAS	7
GLOSARIO	9
RESUMEN.....	10
ABSTRACT.....	10
INTRODUCCIÓN.....	11
DESARROLLO	12
ESCENARIO 1	12
Escenario 2.....	23
CONCLUSIONES	71
BIBLIOGRAFÍA.....	72

LISTA DE TABLAS

Tabla 1. Direccionamiento IP.....	14
Tabla 2. Configuración de PC-A.	19
Tabla 3. Configuración de PC-B.	20
Tabla 4. Configuraciones generales de los Router's y switches respectivos.	25
Tabla 5. Datos de direccionamiento de la computadora de internet.	28
Tabla 6. Pings exitosos resumen.....	44
Tabla 7. Pings exitosos resumen.....	53
Tabla 8. Comandos CLI.....	66

LISTA DE FIGURAS

Figura 1. Escenario 1	12
Figura 2. Construcción de escenario 1 en Packet tracer	12
Figura 2. Configuración inicial R1.	16
Figura 3. Configuración inicial S1.	18
Figura 4. Direccionamiento IP de PC-A.	20
Figura 5. Direccionamiento IP de PC-B.	21
Figura 6. Ping de PC-A a PC-B.....	22
Figura 7. Escenario 2.....	23
Figura 8. Topología propuesta	24
Figura 9. Preconfiguración inicial de R1.	26
Figura 10. Directorio Flash de S1.	27
Figura 11. Revisión memoria Flash S3.	28
Figura 12. Direccionamiento del servidor WEB.....	29
Figura 13. Configuración inicial R1.	31
Figura 14. Configuración inicial R2.	34
Figura 15. Configuración inicial R3.	36
Figura 16. Configuración inicial S1.	38
Figura 17. Configuración inicial S3.	40
Figura 18. Ping exitoso de R1 a R2 en s0/2/0.	41
Figura 19. Ping exitoso de R2 a R3 en s0/2/1.	42
Figura 20. Ping exitoso de pc internet a Gateway predeterminado.....	43
Figura 21. Configuración de S1.	46
Figura 22. Configuración S3.	48
Figura 23. Configuración de R1.	50
Figura 24. Ping exitoso de S1 a R1 en VLAN 99.	51
Figura 25. Ping exitoso de S3 a R1 en VLAN 99.	51
Figura 26. Ping exitoso de S1 a R1 en VLAN 21.	52
Figura 27. Ping exitoso de S3 a R1 en VLAN 23.	52
Figura 28. Configuración de OSPF en R1.	54
Figura 29. Configuración de OSPF en R2.	54

Figura 30. Configuración de OSPF en R3.	55
Figura 31. Protocolos de IP en R1.	56
Figura 32. Protocolos de IP en R3.	57
Figura 33. Protocolos de IP en R2.	58
Figura 34. Configuración en ejecución de OSPF en R1.	59
Figura 35. Configuración en ejecución de OSPF en R3.	60
Figura 36. Configuración en ejecución de OSPF en R2.	60
Figura 37. Configuración DHCP en R1.	62
Figura 38. Configuración NAT estática y dinámica en R2.....	63
Figura 39. Ping de PC-A a PC-C.	64
Figura 40. Configuración de NTP en R1.	65
Figura 41. Ingreso por telnet de R1 a R2.....	66
Figura 42. Listas de acceso en router R2.	67
Figura 43. Interfaz ip de router R2.	68
Figura 44. Interfaz ip de router R1.	69
Figura 45. NAT estáticas de servidor web en router 2.	70
Figura 46. Borrando entradas dinámicas.	70

GLOSARIO

DHCP: Este es un protocolo de configuración dinámica de host que asigna una dirección IP de manera dinámica y ajusta otros parámetros de red a cada dispositivo con el fin de comunicarse con otras redes IP.

Dirección IP: Es un conjunto de números que identifica de manera lógica, una interfaz en la red de este dispositivo mediante el protocolo TCP/IP o que pertenece a este nivel de red.

LAN: Es una red de área local o red de computadoras que abarca un área específica de la casa, conjunto residencial o apartamento. La topología de red define el andamiaje de una red.

NAT: Este es un mecanismo de los routers IP para intercambiar paquetes entre dos redes que se asignan direcciones incompatibles. Este método consiste en convertir, en tiempo real, las direcciones utilizadas por los paquetes transportados y permitir salir a la red con una IP pública específica.

OSPF: Este es un protocolo de direccionamiento IP, basado en el algoritmo de la primera vía más corta, este es un protocolo de red para encaminar de manera jerárquica de pasarela interior o interior Gateway Protocol, este protocolo usa el algoritmo de Dijkstra para determinar el camino más corto entre dos nodos.

RESUMEN

En este escrito se realiza el procedimiento de solución de dos redes compuesta cada una en escenarios de trabajo. Aplicando los conceptos de direccionamiento IP, entre otros conceptos importantes para la realización de este proyecto del diplomado de profundización Cisco CCNA, gracias a la electrónica de redes se pudo dar solución a varios de los problemas de conectividad entre dispositivos.

En el escenario 1 se construyeron 2 subredes y se realizó las configuraciones básicas del Router y el switch específico mediante una conexión de consola, mediante esto se realizó la configuración del direccionamiento y enrutamiento IP y las características de seguridad en los diferentes modos tanto en el switch como en el Router.

En el escenario se construyó una red en donde se aplicaron diferentes conceptos como el protocolo dinámico ospf, además se implementaron cuestiones de seguridad en VLANs y el ruteo entre estas, además con la ayuda de las subinterfaces se logró expandir la cantidad de hosts disponibles que pudiese tener una interfaz, aplicando DHCP y NAT se dio por finalizado la configuración del escenario 2

Palabras clave: Cisco, CCNA, Conmutación, Enrutamiento, Redes, Electrónica

ABSTRACT

In this writing, the solution procedure of two networks composed each one in work scenarios is carried out. Applying the concepts of IP addressing, among other important concepts for the realization of this project of the Cisco CCNA in-depth diploma, thanks to the electronics of networks, it was possible to solve several of the connectivity problems between devices.

In scenario 1, 2 subnets were built, and the basic configurations of the Router and the specific switch were carried out through a console connection, through this, the IP addressing and routing configuration and the security characteristics in the different modes were carried out in both the switch. as in the router.

In the scenario, a network was built where different concepts were applied such as the dynamic ospf protocol, in addition, security issues were implemented in VLANs and the routing between them, also with the help of the subinterfaces it was possible to expand the number of available hosts that could have an interface, applying DHCP and NAT, the configuration of scenario 2 was finished

Keywords: Cisco, CCNA, Switching, Routing, Networking, Electronics

INTRODUCCIÓN

El ingeniero de sistemas hoy día debe enfrentarse a retos importantes en lo que es la revolución de las redes, por lo que es muy importante el objetivo que busca el curso de diplomado de profundización en cisco CCNA.

Uno de estos objetivos principales que busca el curso es encaminar al estudiante a los retos que demarcan la ruta para el futuro, esto es las redes como eje central de la humanidad en donde es de vital importancia el manejo de este tipo de problemas eventuales y que pueden suceder en cualquier momento en la carrera de un ingeniero de sistemas.

Para el escenario 1 se trata de crear 2 subredes mediante las limitaciones del direccionamiento IP, teniendo en cuenta la cantidad de hosts requeridos y es cierto que este tipo de problemas o de restricciones se encuentran hoy en día en la era de las redes y telecomunicaciones, donde más y más dispositivos se empiezan a interconectar, por lo que se necesita la optimización y el buen uso de las direcciones IP'S.

En el escenario 2 se verá el uso de diferentes conceptos importantes como el routing dinámico, DHCP, NAT, NTP, ruteo entre VLANs entre otros.

DESARROLLO

ESCENARIO 1

Figura 1. Escenario 1

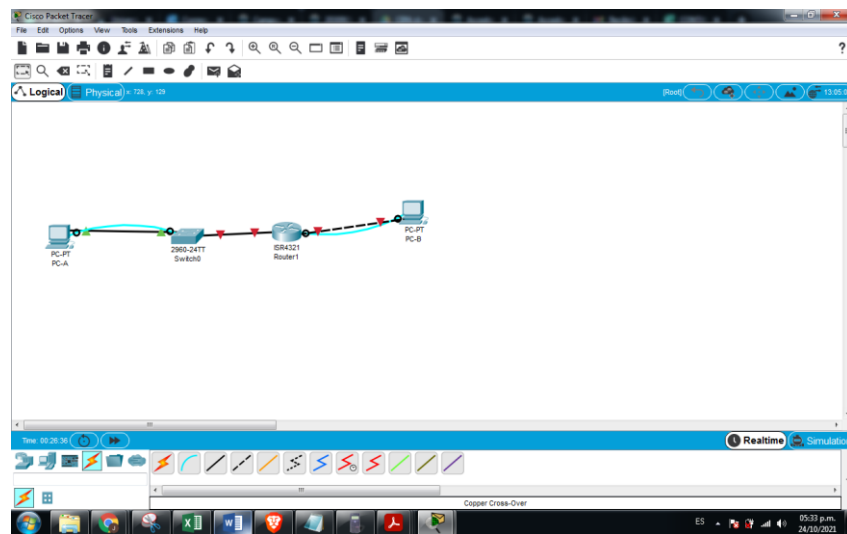


Fuente: Guía de actividades.

Parte 1: Construya la Red

En esta parte se construirá la red con la ayuda del software Packet tracer.

Figura 2. Construcción de escenario 1 en Packet tracer



Fuente: Autoría propia.

En la figura 2 se puede ver la construcción del escenario 1 con la ayuda del software Packet Tracer, este consta de dos LAN's una de 100 hosts y la otra de 50 hosts.

Parte 2: Desarrolle el esquema de direccionamiento IP

En esta parte se desarrollará el esquema de direccionamiento de la IP respectiva, se partirá de la siguiente dirección teniendo en cuenta los dos últimos dígitos del documento de identidad, la dirección respectiva es;

$$192.168.X.0$$

Donde;

$$X = 68$$

Por lo tanto, la dirección es;

$$192.168.68.0/24$$

Esta dirección teniendo en cuenta la máscara de subred da la posibilidad de trabajar hasta con;

$$256 \text{ hosts}$$

Para este requerimiento sumando los hosts de cada una de las LAN's a configurar son un total de;

$$150 \text{ hosts a utilizar}$$

Por lo tanto, la red dada es suficiente para el direccionamiento IP a estas dos subredes.

Tabla 1. Direccionamiento IP.

Ítem	Requerimiento
Dirección de red	192.168.68.0/24
Requerimiento de host subred LAN 1	100
Requerimiento de host subred LAN 2	50
R1 G0/0/1	192.168.68.1/25
R1 G0/0/0	192.168.68.129/26
S1 SV1	192.168.68.2/25
PC-A	192.168.68.126/25
PC-B	192.168.68.190/26

Fuente: Autoría propia.

Parte 3: Configure aspectos básicos

Paso 1: configurar los ajustes básicos

Configuración para R1:

Comandos

Router(config)#no ip domain-lookup	Desactiva la búsqueda DNS
Router(config)#hostname R1	Configuración de nombre.
R1(config)#ip domain-name ccna-lab.com	Dominio del Router
R1(config)#enable secret ciscoenpass privilegiado	Contraseña para modo privilegiado
R1(config-line)#password ciscoconpass el modo consola	Asignando contraseña para el modo consola
R1(config)#security passwords min-length 10 caracteres en contraseña	Restricción de 10 caracteres en contraseña
R1(config)#username admin password admin1pass contraseña	Asignación de usuario y contraseña

R1(config)#line vty 0 4	Configuración líneas vty 0 4
R1(config-line)#password ciscocisco	Asignación de contraseña
R1(config-line)#login local	Logeo con la base de datos
local.	
R1(config-line)#transport input ssh	Configurando para
aceptar solo SSH	
R1(config)#service password-encryption	Cifrando contraseñas
de texto no cifrado	
Configuración de advertencia	
R1(config)#banner motd #Este es un Router de la Unad, cualquier intrusión tendrá un efecto secundario#	
R1(config)#int g0/0/0	Entrando a interfaz G0/0/0
Configuración de dirección y descripción en interfaz g0/0/0.	
R1(config-if)#ip address 192.168.68.129 255.255.255.192	
R1(config-if)#description Esta es la interfaz de la LAN 2	
R1(config-if)#no shutdown	Activado de interfaz
R1(config)#int g0/0/1	Entrando a interfaz G0/0/1
Configuración de dirección y descripción en interfaz g0/0/1.	
R1(config-if)#ip address 192.168.68.1 255.255.255.128	
R1(config-if)#description Esta es la interfaz de la LAN 1	
R1(config-if)#no shutdown	Activado de interfaz
R1(config)#crypto key generate rsa	Generando clave de cifrado RSA

Configuración para S1:

Switch(config)#no ip domain-lookup	Desactiva la búsqueda DNS
Switch(config)#hostname S1	Nombre a Switch
S1(config)#ip domain-name ccna-lab.com	Dominio de Switch
S1(config)#enable secret ciscoenpass privilegiado	Contraseña de modo privilegiado
S1(config)#line console 0	Ingresando a modo consola
S1(config-line)#password ciscoconpass modo consola	Asignando contraseña a modo consola
S1(config-line)#login	Asignando logeo
S1(config-line)#exit	Saliendo de modo consola

Asignando usuario y contraseña

```
S1(config)#username admin password admin1pass
```

S1(config)#line vty 0 15	ingresando a lineas vty
S1(config-line)#password ciscocisco	Asignando contraseña
S1(config-line)#login local	Ingreso solo con la base de datos local
S1(config-line)#transport input ssh	Configurando para aceptar SSH
S1(config-line)#exit	Saliendo del comando de linea
S1(config)#service password encryption	Encriptado de las contraseñas

Configuración de advertencia

```
S1(config)#banner motd #Este es el Switch de la UNAD, POR FAVOR NO  
ENTRAR AQUI#
```

S1(config)#ip domain-name ccna-lab.com	Ingresando a dominio de
generación de cripto.	
S1(config)#crypto key generate rsa	Generando clave de cifrado RS
S1(config)#int vlan1	Ingresando a interface VLAN 1

Asignando dirección ip, mascara de subred y puerta de enlace predeterminada

```
S1(config-if)#ip address 192.168.68.2 255.255.255.128  
S1(config-if)#exit  
  
S1(config)#ip default-gateway 192.168.68.1
```

Figura 3. Configuración inicial S1.

```
S1#show run
Building configuration...

Current configuration : 1532 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1
!
enable secret 5 $l$mERr$EJnmB234UvJf9yoQMWYJK/
!
!
!
no ip domain-lookup
ip domain-name ccna-lab.com
!
username admin privilege 1 password 7 082048430017540713181F
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

30°C 1:01 p.m. 9/12/2021

Simulation

Fuente: Autoría propia.

Paso 2. Configurar los equipos

Configuración PC-A;

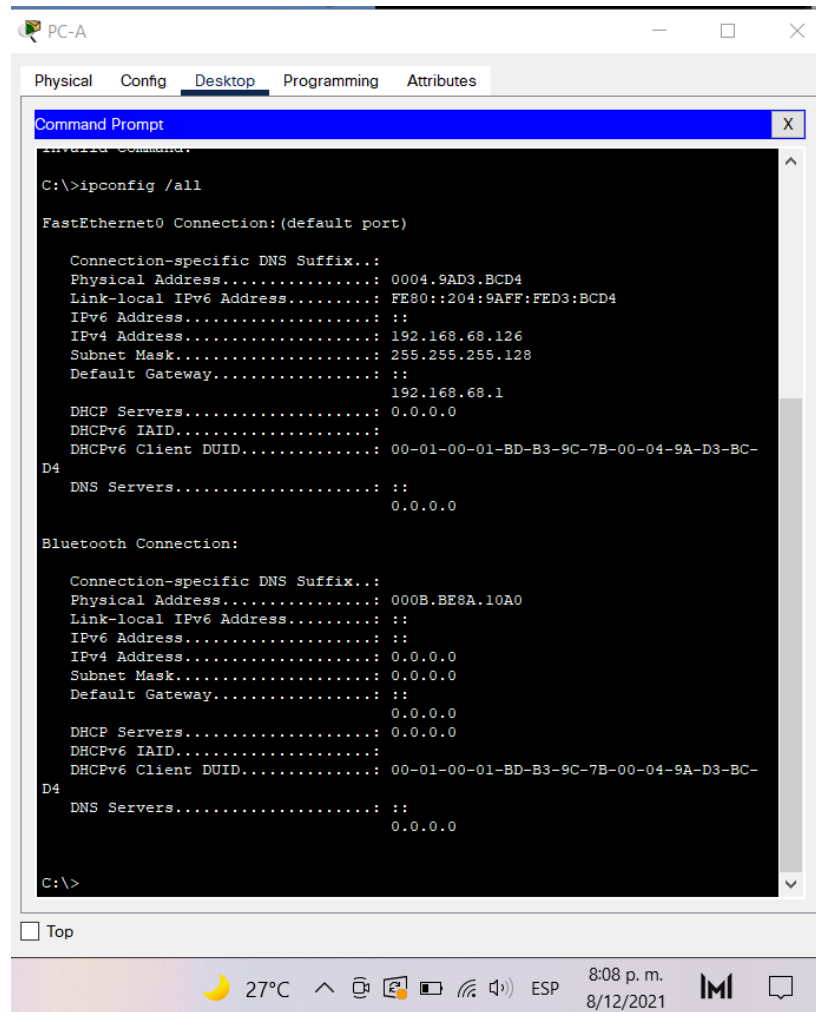
Tabla 2. Configuración de PC-A.

PC-A Network Configuration	
Descripción	Este es el PC-A
Dirección física	0004.9AD3.BCD4
Dirección IP	192.168.68.126
Mascara de subred	255.255.255.128
Gateway predeterminado	192.168.68.1

Fuente: Autoría propia.

Verificación de direccionamiento en PC-A.

Figura 4. Direccionamiento IP de PC-A.



Fuente: Autoría propia.

Configuración PC-B;

Tabla 3. Configuración de PC-B.

PC-B Network Configuration	
Descripción	Este es el PC-B
Dirección física	0001.42CE.D70D
Dirección IP	192.168.68.190
Mascara de subred	255.255.255.192
Gateway predeterminado	192.168.68.129

Fuente: Autoría propia.

Verificación de direccionamiento en PC-B.

Figura 5. Direccionamiento IP de PC-B.

```
Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Physical Address. ....: 0001.42CE.D70D
    Link-local IPv6 Address. ....: FE80::201:42FF:FECE:D70D
    IPv6 Address. ....: ::
    IPv4 Address. ....: 192.168.68.190
    Subnet Mask. ....: 255.255.255.192
    Default Gateway. ....: ::
                                192.168.68.129

    DHCP Servers. ....: 0.0.0.0
    DHCPv6 IAID. ....:
    DHCPv6 Client DUID. ....: 00-01-00-01-A3-3B-02-B7-00-01-42-CE-
D7-0D
    DNS Servers. ....: ::
                                0.0.0.0

Bluetooth Connection:

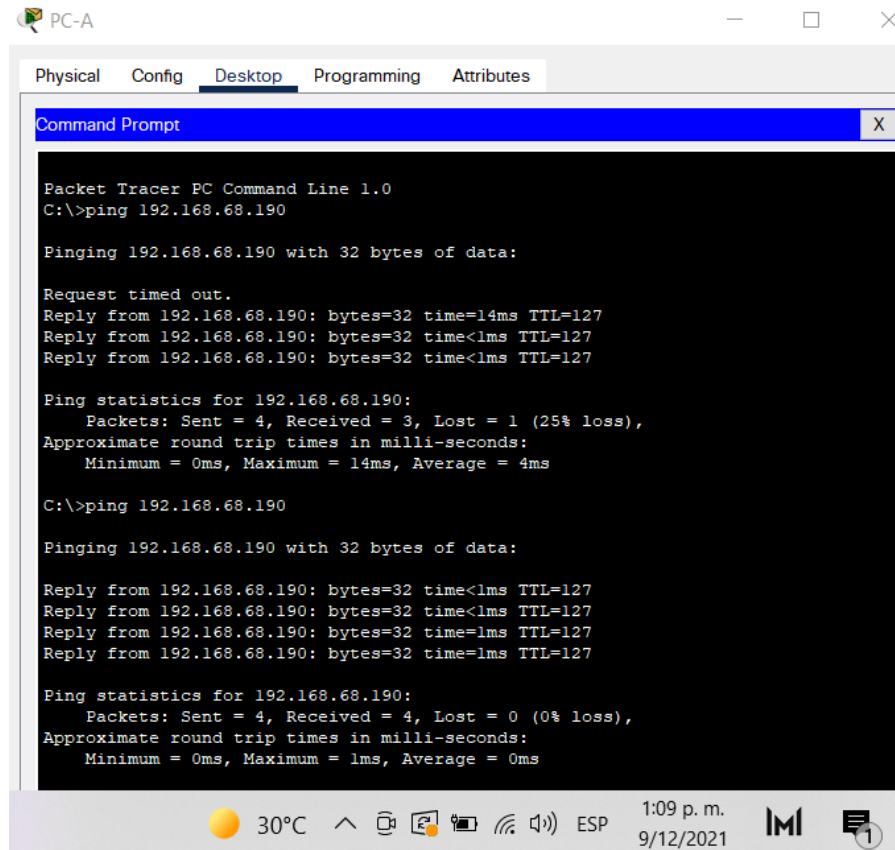
    Connection-specific DNS Suffix...:
    Physical Address. ....: 0002.179C.A980
    Link-local IPv6 Address. ....: ::
    IPv6 Address. ....: ::
    IPv4 Address. ....: 0.0.0.0
    Subnet Mask. ....: 0.0.0.0
    Default Gateway. ....: ::
                                0.0.0.0

    DHCP Servers. ....: 0.0.0.0
    DHCPv6 IAID. ....:
    DHCPv6 Client DUID. ....: 00-01-00-01-A3-3B-02-B7-00-01-42-CE-
D7-0D
    DNS Servers. ....: ::
                                0.0.0.0
```

Fuente: Autoría propia.

Prueba de conectividad entre PC-A y PC-B.

Figura 6. Ping de PC-A a PC-B.



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.68.190

Pinging 192.168.68.190 with 32 bytes of data:

Request timed out.
Reply from 192.168.68.190: bytes=32 time=14ms TTL=127
Reply from 192.168.68.190: bytes=32 time<1ms TTL=127
Reply from 192.168.68.190: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.68.190:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 4ms

C:\>ping 192.168.68.190

Pinging 192.168.68.190 with 32 bytes of data:

Reply from 192.168.68.190: bytes=32 time<1ms TTL=127
Reply from 192.168.68.190: bytes=32 time<1ms TTL=127
Reply from 192.168.68.190: bytes=32 time=1ms TTL=127
Reply from 192.168.68.190: bytes=32 time=1ms TTL=127

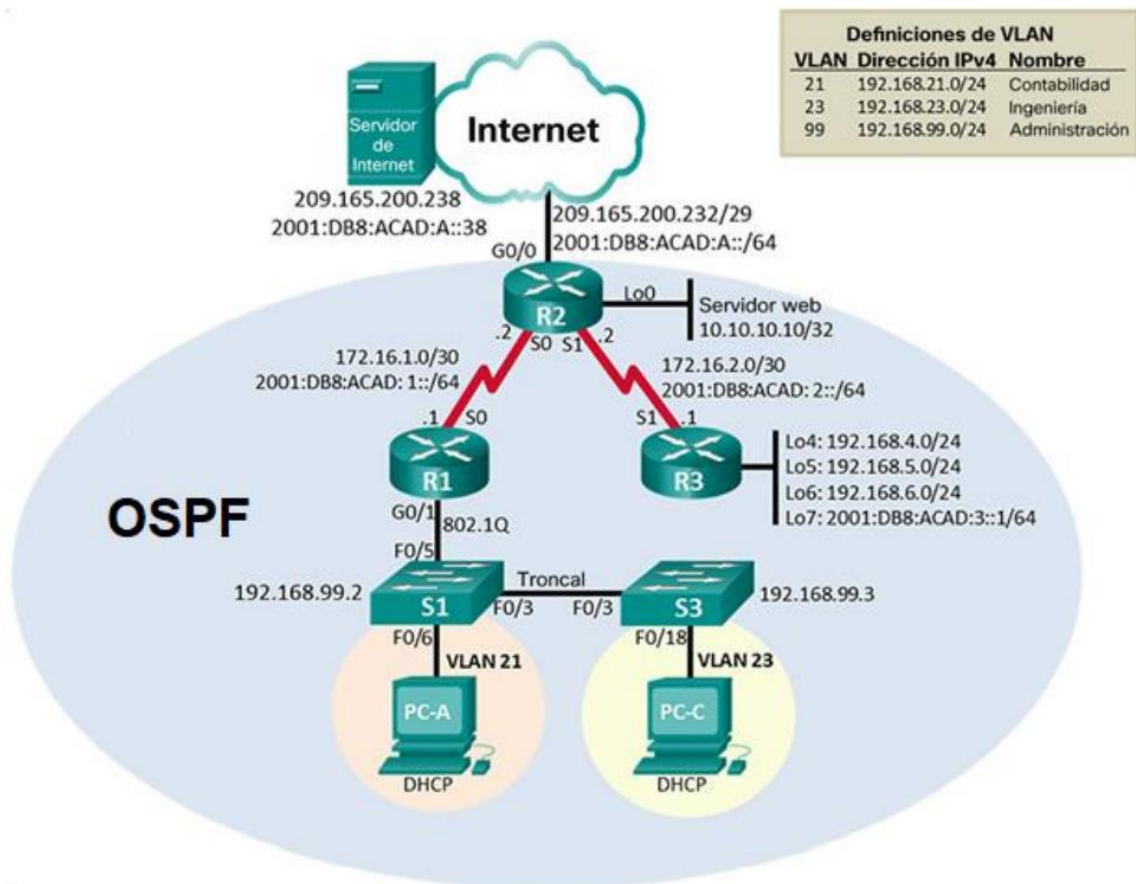
Ping statistics for 192.168.68.190:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Fuente: Autoría propia.

Escenario 2

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

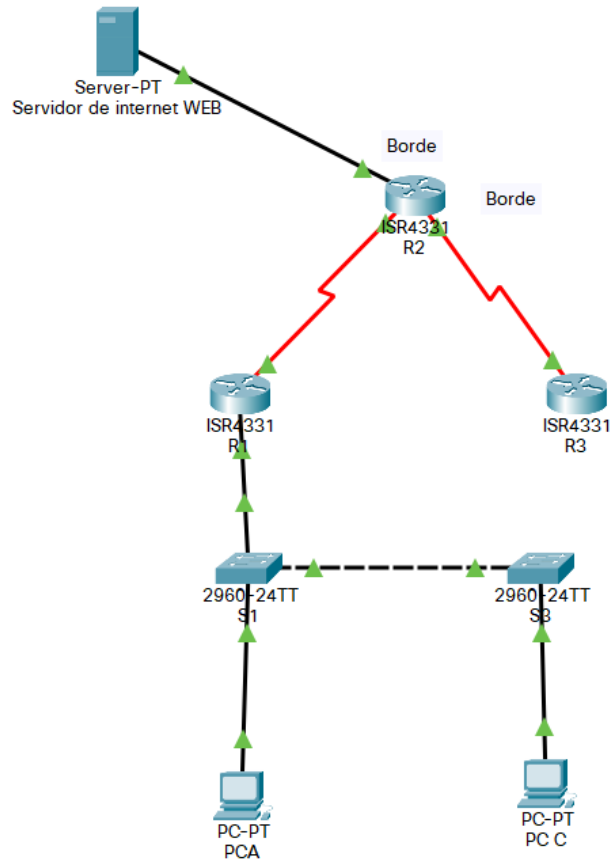
Figura 7. Escenario 2



Fuente: Guía de actividades.

En la figura 7 se puede apreciar la topología a implementar en este escenario 2 utilizando el protocolo de routing dinámico OSPF.

Figura 8. Topología propuesta



Fuente: Autoría propia.

Para la topología propuesta que aparece en la figura 8 se muestra, el montaje en el software Packet Tracer para realizar las conectividades respectivas mediante OSPF.

Parte 1: Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los Router's 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.

Las operaciones de este paso 1 se encuentran resumidas en la siguiente tabla;

Tabla 4. Configuraciones generales de los Router's y switches respectivos.

Tarea	Comando 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 este en la memoria flash en ambos switches	Switch#show flash

Fuente: Autoría propia.

Configuración general para todos los routers;

Comandos

Router>ena

ingresando al modo exec privilegiado

Router#erase startup-config

Eliminar archivo de configuración inicial

Router#reload

Reinicializar el sistema del Router

Figura 9. Preconfiguración inicial de R1.

```
Router>ena
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#reload
Proceed with reload? [confirm]
Initializing Hardware ...

Checking for PCIe device presence...done
System integrity status: 0x610
Rom image verified correctly

System Bootstrap, Version 16.7(3r), RELEASE SOFTWARE
Copyright (c) 1994-2018 by Cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft
Cisco ISR4331/K9 platform with 4194304 Kbytes of main memory

no valid BOOT image found
Final autoboot attempt from default boot device...
Located isr4300-universalk9.16.06.04.SPA.bin
#####
#####
Package header rev 1 structure detected
IsoSize = 550114467
Calculating SHA-1 hash...Validate package: SHA-1 hash:
  calculated 444F4D02:44C58887:D9C8942B:C557D3CF:2A14247E
  expected   444F4D02:44C58887:D9C8942B:C557D3CF:2A14247E

RSA Signed RELEASE Image Signature Verification Successful.
Image validated

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
```

Fuente: Autoría propia.

En la figura 9 se puede observar la pre-configuración inicial de los routers.

Configuración general para todos los switches;

Comandos

Switch>ena entrando al modo exec privilegiado

Switch#erase startup-config borrando archivo de configuración inicial

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]

Switch#show flash

Verificando el directorio de flash

Verificación de directorio en Switches.

Figura 10. Directorio Flash de S1.

```
S1>ena
Password:
S1#show flash
Directory of flash:/

 1  -rw-   4670455      <no date>  2960-lanbasek9-mz.150-2.SE4.bin
10  -rw-     796      <no date>  vlan.dat

64016384 bytes total (59345133 bytes free)
S1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

27°C 8:32 p. m. 8/12/2021

Fuente: Autoría propia.

Figura 11. Revisión memoria Flash S3.

```

S3>ena
Password:
S3#show flash
Directory of flash:/

   1  -rw-     4670455      <no date>  2960-lanbasek9-mz.150-2.SE4.bin
  10  -rw-         736      <no date>    vlan.dat

64016384 bytes total (59345193 bytes free)
S3#
    
```

Ctrl+F6 to exit CLI focus

Copy Paste

27°C 8:33 p. m. 8/12/2021

Fuente: Autoría propia.

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

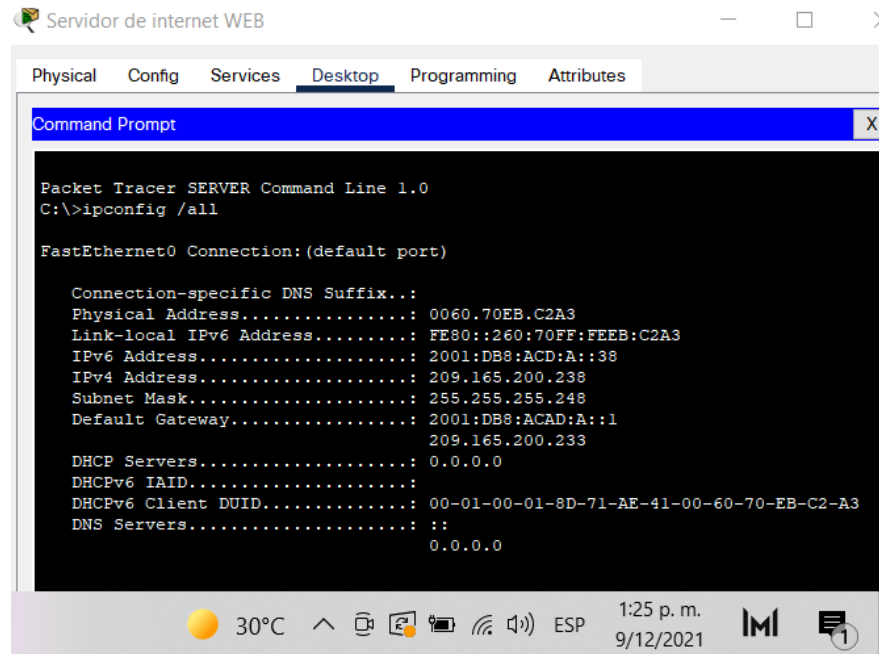
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 5. Datos de direccionamiento de la computadora de internet.

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Mascara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:db8:acad:a::38
Gateway predeterminado IPv6	2001:db8:acad:a::1/64

Fuente: Autoría propia.

Figura 12. Direccinamiento del servidor WEB.



Fuente: Autoría propia.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Desactivar la búsqueda DNS.

Router(config)#no ip domain-lookup

Asignar nombre al Router

Router(config)#hostname R1

Contraseña de exec privilegiado

R1(config)#enable secret class

Contraseña de línea de consola

R1(config)#line console 0

R1(config-line)#password cisco

R1(config-line)#login

Entrando a línea de consola
Asignando contraseña Cisco
comando login para ingresar

Contraseña de acceso Telnet

R1(config)#line vty 0 15

Configurando líneas VTY

R1(config-line)#password cisco	Ingresando contraseña
R1(config-line)#login	Ingreso por login
R1(config-line)#exit	Saliendo del comando

Cifrar las contraseñas de texto no cifrado

R1(config)#service password-encryption

Mensaje MOTD

R1(config)#banner motd %Se prohíbe el acceso no autorizado%

Interfaz S0/2/0

R1(config)#int s0/2/0	Ingresando a interfaz serial
R1(config-if)#description "Conexion a R2"	Describiendo interfaz
R1(config-if)#ip address 172.16.1.1 255.255.255.252	Asignando dirección ipv4
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64	Asignando dirección ipv6
R1(config-if)#clock rate 128000	Asignando frecuencia de reloj
R1(config-if)#no shutdown	Activando la interfaz

Rutas predeterminadas

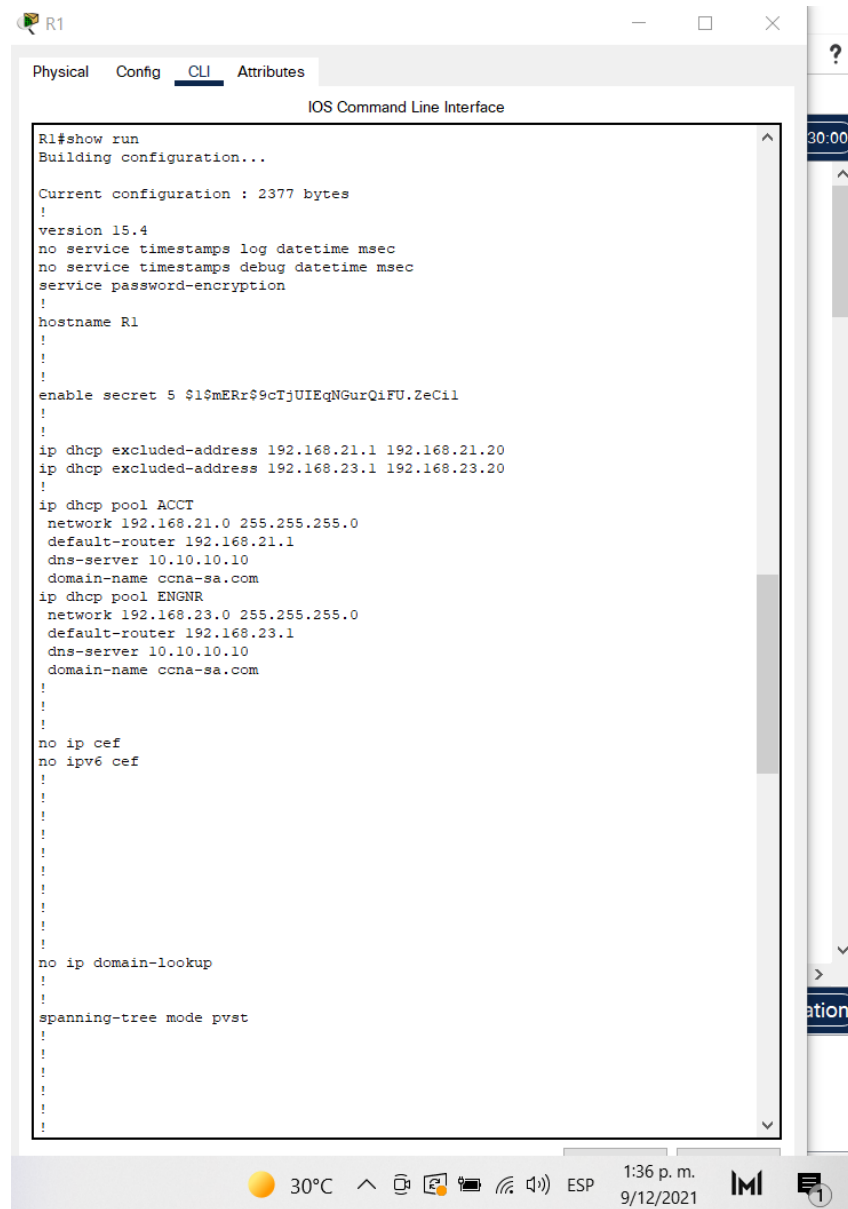
Ruta ipv4

R1(config)#ip route 0.0.0.0 0.0.0.0 s0/2/0 Asignando ruta estática ipv4.

Asignando rutas predeterminadas ipv6

R1(config)#ipv6 route 2001:db8:acad:a::/64 2001:db8:acad:1::2

Figura 13. Configuración inicial R1.



```
R1#show run
Building configuration...

Current configuration : 2377 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
ip dhcp excluded-address 192.168.21.1 192.168.21.20
ip dhcp excluded-address 192.168.23.1 192.168.23.20
!
ip dhcp pool ACCT
network 192.168.21.0 255.255.255.0
default-router 192.168.21.1
dns-server 10.10.10.10
domain-name ccna-sa.com
ip dhcp pool ENGR
network 192.168.23.0 255.255.255.0
default-router 192.168.23.1
dns-server 10.10.10.10
domain-name ccna-sa.com
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
!
!
!
!
```

Fuente: Autoría propia.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Desactivar la búsqueda DNS.

R2(config)#no ip domain-lookup

Asignar nombre al Router

```
R2(config)#hostname R2
```

Contraseña de exec privilegiado

```
R2(config)#enable secret class
```

Contraseña de línea de consola

```
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
```

Entrando a línea de consola
Asignando contraseña Cisco
Ingreso por login

Contraseña de acceso Telnet

```
R2(config)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
```

Configurando líneas VTY.
Asignando contraseña Cisco
Ingreso por login
Saliendo.

Cifrar las contraseñas de texto no cifrado

```
R2(config)#service password-encryption
```

Habilitar el servidor HTTP

```
R2(config)#ip http server
```

Comando anterior no soportado por Packet Tracer.

Mensaje MOTD

```
R2(config)#banner motd %Se prohíbe el acceso no autorizado%
```

Configurando interfaz serial 0/2/0.

```
R2(config)#int s0/2/0
R2(config-if)#description "Conexion a R1"
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:db8:acad:1::2/64
R2(config-if)#no shutdown
```

Configurando interfaz serial 0/2/1

```
R2(config)#int s0/2/1
R2(config-if)#description "Conexion a R3"
R2(config-if)#ip address 172.16.2.2 255.255.255.252
R2(config-if)#ipv6 address 2001:db8:acad:2::2/64
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown
```

Configuración de interfaz G0/0/0 (simulación de Internet).

```
R2(config)#int g0/0/0
R2(config-if)#description "Conexion a Internet"
R2(config-if)#ip address 209.165.200.233 255.255.255.240
R2(config-if)#ipv6 address 2001:db8:acad:a::1/64
```

Interfaz loopback 0 (servidor web simulado)

```
R2(config-if)#int lo0
R2(config-if)#description "Servidor web"
R2(config-if)#ip address 10.10.10.10 255.255.255.255
```

Rutas predeterminadas

```
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0/0
R2(config)#ipv6 route ::/0 g0/0/0
```

Figura 14. Configuración inicial R2.



```
!
!
!
interface Loopback0
description "Servidor web"
ip address 10.10.10.10 255.255.255.255
ip nat inside
!
interface GigabitEthernet0/0/0
description "Conexion a Internet"
ip address 209.165.200.233 255.255.255.240
duplex auto
speed auto
ipv6 address 2001:DB8:ACAD:A::1/64
ipv6 address 2011:DB8:ACAD:A::1/64
!
interface GigabitEthernet0/0/1
no ip address
ip nat outside
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/2/0
description "Conexion a R1"
ip address 172.16.1.2 255.255.255.252
ipv6 address 2001:DB8:ACAD:1::2/64
!
interface Serial0/2/1
description "Conexion a R3"
ip address 172.16.2.2 255.255.255.252
ipv6 address 2001:DB8:ACAD:2::2/64
clock rate 128000
!
interface Vlan1
no ip address
shutdown
```

Fuente: Autoría propia.

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Desactivar la búsqueda DNS.

R3(config)#no ip domain-lookup

Asignar nombre al Router

R3(config)#hostname R3

Contraseña de exec privilegiado

```
R3(config)#enable secret class
```

Contraseña de línea de consola

```
R3(config)#line console 0
```

```
R3(config-line)#password cisco
```

```
R3(config-line)#login
```

Contraseña de acceso Telnet

```
R3(config)#line vty 0 15
```

```
R3(config-line)#password cisco
```

```
R3(config-line)#login
```

```
R3(config-line)#exit
```

Configurando líneas VTY.
Asignando contraseña Cisco
Verificando ingreso por login
Saliendo

Cifrar las contraseñas de texto no cifrado

```
R3(config)#service password-encryption
```

Mensaje MOTD

```
R3(config)#banner motd %Se prohíbe el acceso no autorizado%
```

Configuración de interfaz serial 0/2/1

```
R3(config)#int s0/2/1
```

```
R3(config-if)#description "Conexion a R2"
```

```
R3(config-if)#ip address 172.16.2.1 255.255.255.252
```

```
R3(config-if)#ipv6 address 2001:db8:acad:2::1/64
```

```
R3(config-if)#no shutdown
```

Configuración de interfaz loopback 4

```
R3(config)#int lo4
```

```
R3(config-if)#ip address 192.168.4.1 255.255.255.0
```

```
R3(config-if)#exit
```

Configurando interfaz loopback 5

```
R3(config)#int lo5
```

```
R3(config-if)#ip address 192.168.5.1 255.255.255.0
```

```
R3(config-if)#exit
```

Configurando interfaz loopback 6

```
R3(config)#int lo6
```

```
R3(config-if)#ip address 192.168.6.1 255.255.255.0
```

```
R3(config-if)#exit
```

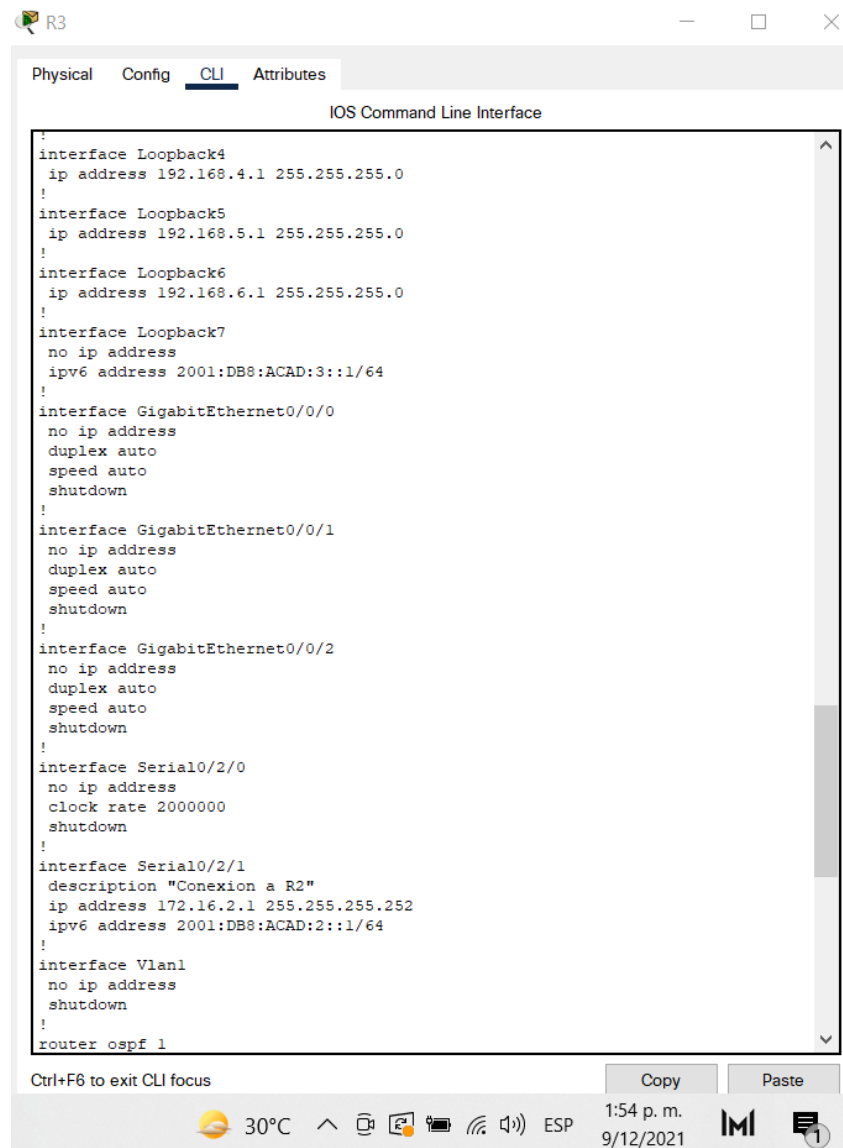
Configurando interfaz loopback 7

```
R3(config)#int lo7
R3(config-if)#ipv6 address 2001:db8:acad:3::1/64
R3(config-if)#exit
```

Rutas predeterminadas

```
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/2/1
R3(config)#ipv6 route ::/0 s0/2/1
```

Figura 15. Configuración inicial R3.



```
R3
Physical Config CLI Attributes
IOS Command Line Interface
:
interface Loopback4
 ip address 192.168.4.1 255.255.255.0
!
interface Loopback5
 ip address 192.168.5.1 255.255.255.0
!
interface Loopback6
 ip address 192.168.6.1 255.255.255.0
!
interface Loopback7
 no ip address
 ipv6 address 2001:DB8:ACAD:3::1/64
!
interface GigabitEthernet0/0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/2/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/2/1
 description "Conexion a R2"
 ip address 172.16.2.1 255.255.255.252
 ipv6 address 2001:DB8:ACAD:2::1/64
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
```

Fuente: Autoría propia.

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Desactivar la búsqueda DNS

```
Switch(config)#no ip domain-lookup
```

Nombre del switch

```
Switch(config)#hostname S1
```

Contraseña de exec privilegiado

```
S1(config)#enable secret class
```

Contraseña de línea de consola

```
S1(config)#line console 0
```

```
S1(config-line)#password cisco
```

```
S1(config-line)#login
```

Contraseña de acceso Telnet

```
S1(config)#line vty 0 15
```

```
S1(config-line)#password cisco
```

```
S1(config-line)#login
```

```
S1(config-line)#exit
```

Cifrar las contraseñas de texto no cifrado

```
S1(config)#service password-encryption
```

Mensaje MOTD

```
S1(config)#banner motd %Se prohíbe el acceso no autorizado%
```

Figura 16. Configuración inicial S1.



```
password:
S1#show run
Building configuration...

Current configuration : 2244 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
no ip domain-lookup
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport mode access
 shutdown
!
interface FastEthernet0/2
 switchport mode access
 shutdown
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport mode access
 shutdown
!
interface FastEthernet0/5
 switchport mode trunk
!
interface FastEthernet0/6
 switchport access vlan 21
 switchport mode access
!
interface FastEthernet0/7
 switchport mode access
 shutdown
!
interface FastEthernet0/8
 switchport mode access
```

Fuente: Autoría propia.

Paso 6: Configurar S3

La configuración del S3 incluye las siguientes tareas:

Desactivar la búsqueda DNS

Switch(config)#no ip domain-lookup

Switch(config)#hostname S3
Contraseña de exec privilegiado

S3(config)#enable secret class
Contraseña de línea de consola

S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login

Contraseña de acceso Telnet

S3(config)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit

Configurando líneas VTY.
Asignando contraseña
Verificando login
Saliendo

Cifrar las contraseñas de texto no cifrado

S3(config)#service password-encryption

Mensaje MOTD

S3(config)#banner motd %Se prohíbe el acceso no autorizado%

Figura 17. Configuración inicial S3.



```
IOS Command Line Interface
Password:
S3#show run
Building configuration...

Current configuration : 2255 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S3
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
!
no ip domain-lookup
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport mode access
 shutdown
!
interface FastEthernet0/2
 switchport mode access
 shutdown
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport mode access
 shutdown
!
interface FastEthernet0/5
 switchport mode access
 shutdown
!
interface FastEthernet0/6
 switchport mode access
 shutdown
!
interface FastEthernet0/7
 switchport mode access
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

31°C 2:35 p. m. 9/12/2021

Fuente: Autoría propia.

Paso 7: Verificar la conectividad de la red

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

R1 a R2 s0/2/0

Figura 18. Ping exitoso de R1 a R2 en s0/2/0.

```
R1#ping 172.16.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6 ms

R1#ping 2001:db8:acad:1::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:1::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6 ms

R1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

29°C Muy soleado 4:25 p. m. 5/12/2021

Fuente: Autoría propia.

R2 a R3 s0/2/1

Ping

Figura 19. Ping exitoso de R2 a R3 en s0/2/1.

```
R2#ping 172.16.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/5 ms

R2#ping 2001:db8:acad:2::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:2::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/13 ms

R2#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

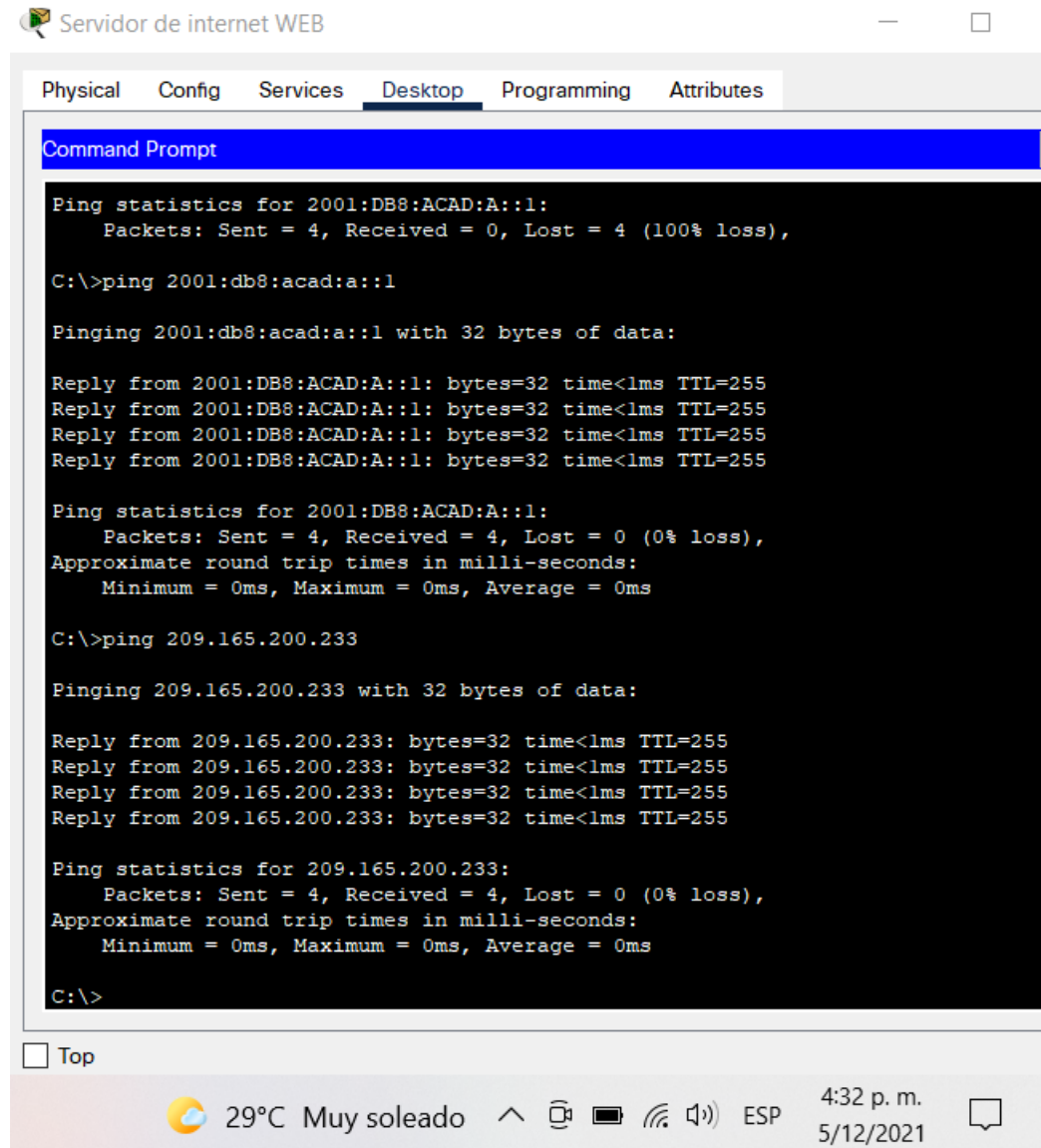
29°C Muy soleado ESP 4:27 p. m. 5/12/2021

Fuente: Autoría propia.

Pc de internet a Gateway predeterminado

Ping

Figura 20. Ping exitoso de pc internet a Gateway predeterminado.



Fuente: Autoría propia.

Tabla resumen de pings

Tabla 6. Pings exitosos resumen.

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/2/0	172.16.1.2	exitoso
R2	R3, S0/2/1	172.16.2.1	exitoso
PC de Internet	Gateway predeterminado	209.165.200.233	exitoso

Fuente: Autoría propia.

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:

Crear la base de datos de VLAN

```
S1(config)#vlan 21           Ingresando a VLAN 21
S1(config-vlan)#name Contabilidad Asignando nombre
S1(config-vlan)#vlan 23     Ingresando a VLAN 23
S1(config-vlan)#name Ingenieria Asignando nombre
S1(config-vlan)#vlan 99     Ingresando a VLAN 99
S1(config-vlan)#name Administración Asignando nombre
```

Asignar la dirección IP de administración

```
S1(config)#int vlan99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#exit
```

Asignar el gateway predeterminado

```
S1(config)#ip default-gateway 192.168.99.1
```

Forzar el enlace troncal en la interfaz F0/3

```
S1(config)#int fa0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1   Asignando VLAN 1 como troncal nativo.
S1(config-if)#exit
```

Forzar el enlace troncal en la interfaz F0/5

```
S1(config)#int fa0/5
```

```
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1    Asignando VLAN 1 como troncal
nativo.
```

Configurar el resto de los puertos como puertos de acceso

```
S1(config)#interface range fa0/1-2,fa0/4,fa0/6-24,gi0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#exit
```

Asignar F0/6 a la VLAN 21

```
S1(config)#int fa0/6
S1(config-if)#switchport access vlan 21
S1(config-if)#exit
```

Apagar todos los puertos sin usar

```
S1(config)#interface range fa0/1-2,fa0/4,fa0/7-24,gi0/1-2
S1(config-if-range)#shutdown
```

Figura 21. Configuración de S1.



```
!
interface FastEthernet0/1
 switchport mode access
 shutdown
!
interface FastEthernet0/2
 switchport mode access
 shutdown
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport mode access
 shutdown
!
interface FastEthernet0/5
 switchport mode trunk
!
interface FastEthernet0/6
 switchport access vlan 21
 switchport mode access
!
interface FastEthernet0/7
 switchport mode access
 shutdown
!
interface FastEthernet0/8
 switchport mode access
 shutdown
!
interface FastEthernet0/9
 switchport mode access
 shutdown
!
interface FastEthernet0/10
 switchport mode access
 shutdown
!
interface FastEthernet0/11
 switchport mode access
 shutdown
!
interface FastEthernet0/12
 switchport mode access
 shutdown
!
interface FastEthernet0/13
 switchport mode access
 shutdown
!
interface FastEthernet0/14
```

Fuente: Autoría propia.

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Crear la base de datos de VLAN

S3(config)#vlan 21

Ingresando a VLAN 21

```
S3(config-vlan)#name Contabilidad    Asignando nombre
S3(config-vlan)#vlan 23              ingresando a VLAN 23
S3(config-vlan)#name Ingenieria     Asignando nombre
S3(config-vlan)#vlan 99              Ingresando a VLAN 99
S3(config-vlan)#name Administración Asignando nombre
```

Asignar la dirección IP de administración – VLAN 99

```
S3(config)#int vlan99
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#exit
```

Asignar el gateway predeterminado

```
S3(config)#ip default-gateway 192.168.99.1
```

Forzar el enlace troncal en la interfaz F0/3

```
S3(config)#int fa0/3
S3(config-if)#switchport mode trunk    Forzando como enlace troncal
S3(config-if)#switchport trunk native vlan 1    Asignando VLAN 1 como troncal
nativo.
S3(config-if)#exit
```

Configurar el resto de los puertos como puertos de acceso

```
S3(config)#interface range fa0/1-2,fa0/4-24,gi0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#exit
```


Asignar F0/18 a la VLAN 21

```
S3(config)#int fa0/18                Ingresando a interfaz f0/18
S3(config-if)#switchport access vlan 21    Asignando f0/18 a VLAN 21
S3(config-if)#exit                    Saliendo de interfaz f0/18
```

Apagar todos los puertos sin usar

```
S3(config)#interface range fa0/1-2, fa0/4-17,fa0/19-24,gi0/1-2
S3(config-if-range)#shutdown
```

Figura 22. Configuración S3.



The screenshot shows a window titled 'S3' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The configuration commands are as follows:

```
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport mode access
 shutdown
!
interface FastEthernet0/2
 switchport mode access
 shutdown
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport mode access
 shutdown
!
interface FastEthernet0/5
 switchport mode access
 shutdown
!
interface FastEthernet0/6
 switchport mode access
 shutdown
!
interface FastEthernet0/7
 switchport mode access
 shutdown
!
interface FastEthernet0/8
 switchport mode access
 shutdown
!
interface FastEthernet0/9
 switchport mode access
 shutdown
!
interface FastEthernet0/10
 switchport mode access
 shutdown
!
interface FastEthernet0/11
 switchport mode access
 shutdown
!
interface FastEthernet0/12
 switchport mode access
 shutdown
!
```

At the bottom of the CLI window, there is a 'Ctrl+F6 to exit CLI focus' message and 'Copy' and 'Paste' buttons. Below the window, the Windows taskbar shows the system tray with a temperature of 31°C, the time 3:17 p.m., and the date 9/12/2021.

Fuente: Autoría propia.

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Configurar la subinterfaz 802.1Q .21 en G0/1

```
R1(config)#int g0/0/1.21
```

```
R1(config-subif)#description "LAN de Contabilidad" Asignando nombre de
subinterfaz
R1(config-subif)#encapsulation dot1Q 21 Habilitando protocolo para asignar a
VLAN 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0 Asignando dirección
ipv4 a subinterfaz
R1(config-subif)#exit
```

Configurar la subinterfaz 802.1Q .23 en G0/1

```
R1(config)#int g0/0/1.23
R1(config-subif)#description "LAN de Ingenieria" Asignando nombre de
subinterfaz
R1(config-subif)#encapsulation dot1Q 23 Habilitando protocolo para asignar a
la VLAN 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0 Asignando dirección
ipv4 a subinterfaz
R1(config-subif)#exit
```

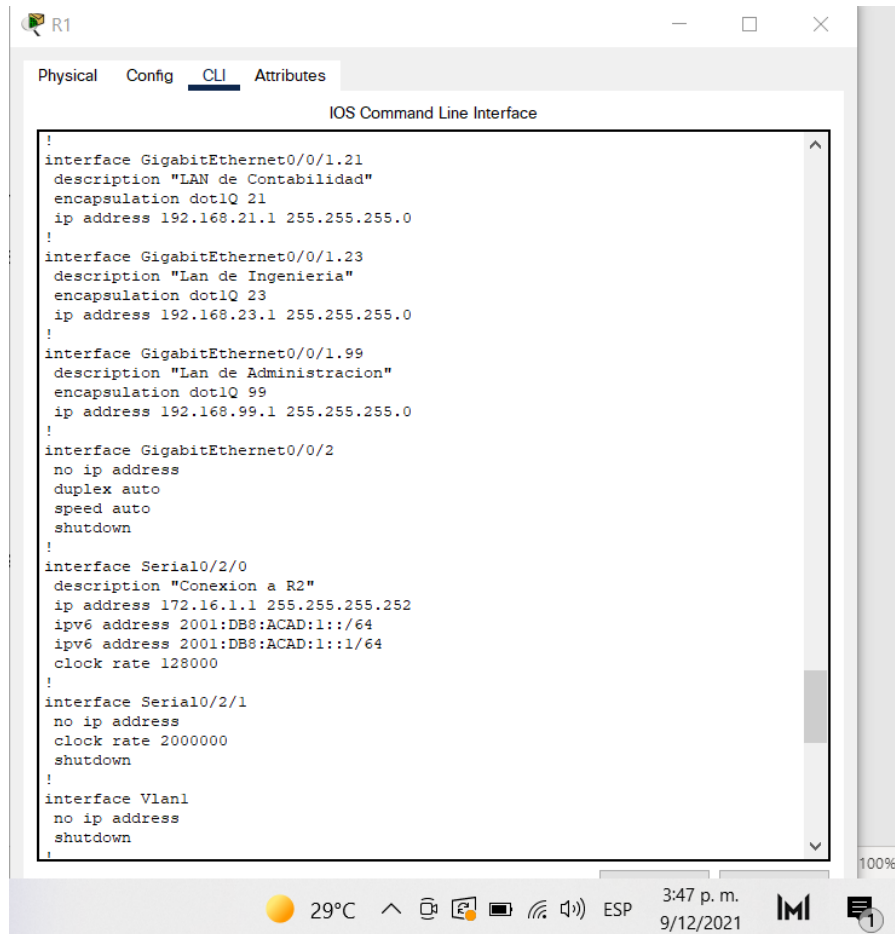
Configurar la subinterfaz 802.1Q .99 en G0/1

```
R1(config)#int g0/0/1.99
R1(config-subif)#description "LAN de Administracion" Asignando
nombre de subinterfaz
R1(config-subif)#encapsulation dot1Q 99 Habilitando protocolo para asignar
VLAN 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0 Asignando dirección
ipv4 a subinterfaz
R1(config-subif)#exit
```

Activar la interfaz G0/1

```
R1(config)#int g0/0/1
R1(config-if)#no shutdown
```

Figura 23. Configuración de R1.



```
!
interface GigabitEthernet0/0/1.21
description "LAN de Contabilidad"
encapsulation dot1Q 21
ip address 192.168.21.1 255.255.255.0
!
interface GigabitEthernet0/0/1.23
description "Lan de Ingenieria"
encapsulation dot1Q 23
ip address 192.168.23.1 255.255.255.0
!
interface GigabitEthernet0/0/1.99
description "Lan de Administracion"
encapsulation dot1Q 99
ip address 192.168.99.1 255.255.255.0
!
interface GigabitEthernet0/0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/2/0
description "Conexion a R2"
ip address 172.16.1.1 255.255.255.252
ipv6 address 2001:DB8:ACAD:1::/64
ipv6 address 2001:DB8:ACAD:1::1/64
clock rate 128000
!
interface Serial0/2/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
```

Fuente: Autoría propia.

Paso 4: Verificar la conectividad de la red

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

PING

S1 a R1 VLAN 99

Figura 24. Ping exitoso de S1 a R1 en VLAN 99.

```
S1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

S1#
```

Ctrl+F6 to exit CLI focus

Copy Pa

Top

28°C Bruma ESP 5:03 p. m. 5/12/2021

Fuente: Autoría propia.

S3 a R1 VLAN 99

Figura 25. Ping exitoso de S3 a R1 en VLAN 99.

```
password:
S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms

S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

S3#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

28°C Bruma ESP 5:06 p. m. 5/12/2021

Fuente: Autoría propia.

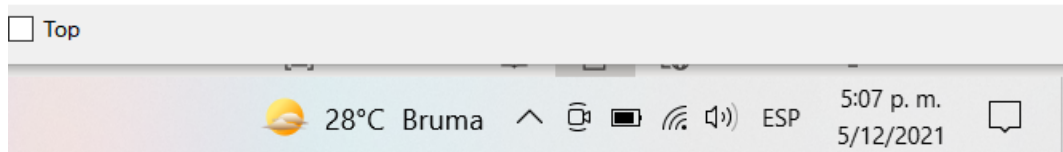
S1 a R1 VLAN 21

Figura 26. Ping exitoso de S1 a R1 en VLAN 21.

```
S1#ping 192.168.21.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S1#
```

Ctrl+F6 to exit CLI focus

Copy Paste



Fuente: Autoría propia.

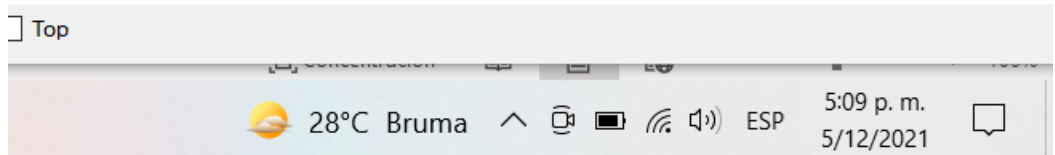
S3 a R1 VLAN 23

Figura 27. Ping exitoso de S3 a R1 en VLAN 23.

```
S3#ping 192.168.23.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S3#
```

Ctrl+F6 to exit CLI focus

Copy Paste



Fuente: Autoría propia.

Tabla resumen de pings

Tabla 7. Pings exitosos resumen.

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	192.168.21.1	exitoso
S3	R1, dirección VLAN 23	192.168.23.1	exitoso

Fuente: Autoría propia.

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:

Configurar OSPF área 0

```
R1(config)#router ospf 1
```

```
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
```

```
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0
```

```
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0
```

```
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
```

Configurando rutas directamente conectadas a router R1.

Establecer todas las interfaces LAN como pasivas

```
R1(config)#router ospf 1
```

```
R1(config-router)#passive-interface g0/0/1.21
```

```
R1(config-router)#passive-interface g0/0/1.23
```

```
R1(config-router)#passive-interface g0/0/1.99
```

Desactive la sumarización automática

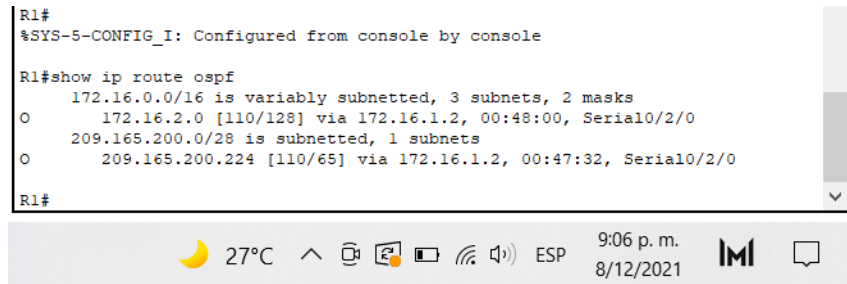
En Ospf no hay sumarización automática.

Figura 28. Configuración de OSPF en R1.

```
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ip route ospf
 172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O   172.16.2.0 [110/128] via 172.16.1.2, 00:48:00, Serial0/2/0
   209.165.200.0/28 is subnetted, 1 subnets
O   209.165.200.224 [110/65] via 172.16.1.2, 00:47:32, Serial0/2/0

R1#
```



Fuente: Autoría propia.

Paso 2: Configurar OSPF en el R2

Las tareas de configuración para R2 incluyen las siguientes:

Configurar OSPF área 0

```
R2(config)#router ospf 1
```

```
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0
```

```
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
```

```
R2(config-router)#network 209.165.200.232 0.0.0.255 area 0
```

Configurando rutas directamente conectadas a router R2.

Establecer la interfaz LAN (loopback) como pasiva

```
R2(config)#router ospf 1
```

```
R2(config-router)#passive-interface lo0
```

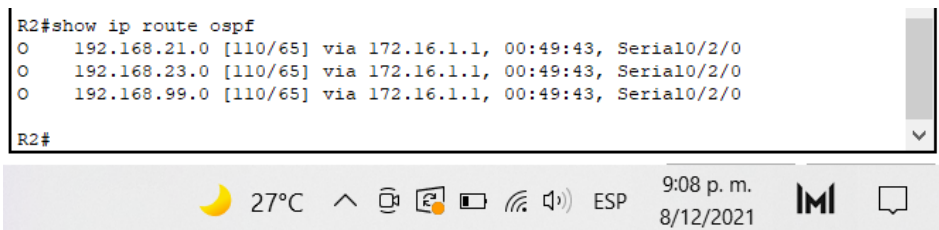
Desactive la sumarización automática

En Ospf no hay sumarización automática.

Figura 29. Configuración de OSPF en R2.

```
R2#show ip route ospf
O   192.168.21.0 [110/65] via 172.16.1.1, 00:49:43, Serial0/2/0
O   192.168.23.0 [110/65] via 172.16.1.1, 00:49:43, Serial0/2/0
O   192.168.99.0 [110/65] via 172.16.1.1, 00:49:43, Serial0/2/0

R2#
```



Fuente: Autoría propia.

Paso 3: Configurar OSPF en el R3

La configuración del R3 incluye las siguientes tareas:

Configurar OSPF área 0

```
R3(config)#router ospf 1
```

```
R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
```

Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas

```
R3(config-router)#passive-interface lo4
```

```
R3(config-router)#passive-interface lo5
```

```
R3(config-router)#passive-interface lo6
```

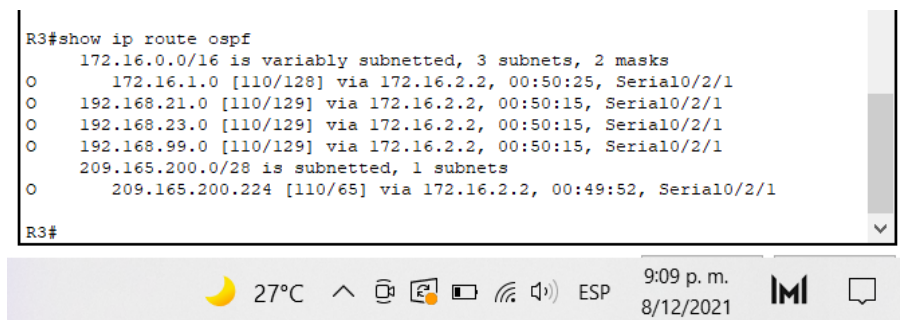
```
R3(config-router)#passive-interface lo7
```

Desactive la sumarización automática

En Ospf no hay sumarización automática.

Figura 30. Configuración de OSPF en R3.

```
R3#show ip route ospf
 172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O   172.16.1.0 [110/128] via 172.16.2.2, 00:50:25, Serial0/2/1
O   192.168.21.0 [110/129] via 172.16.2.2, 00:50:15, Serial0/2/1
O   192.168.23.0 [110/129] via 172.16.2.2, 00:50:15, Serial0/2/1
O   192.168.99.0 [110/129] via 172.16.2.2, 00:50:15, Serial0/2/1
 209.165.200.0/28 is subnetted, 1 subnets
O   209.165.200.224 [110/65] via 172.16.2.2, 00:49:52, Serial0/2/1
R3#
```



Fuente Autoría propia.

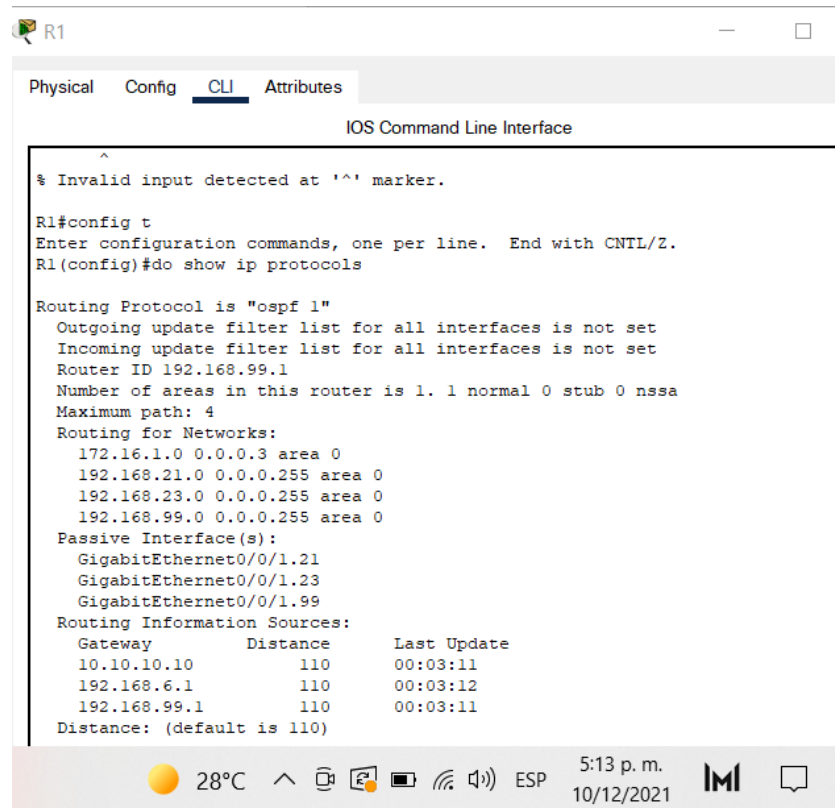
Paso 4: Verificar la información de OSPF

Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

¿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?

Con el comando do show ip protocols

Figura 31. Protocolos de IP en R1.

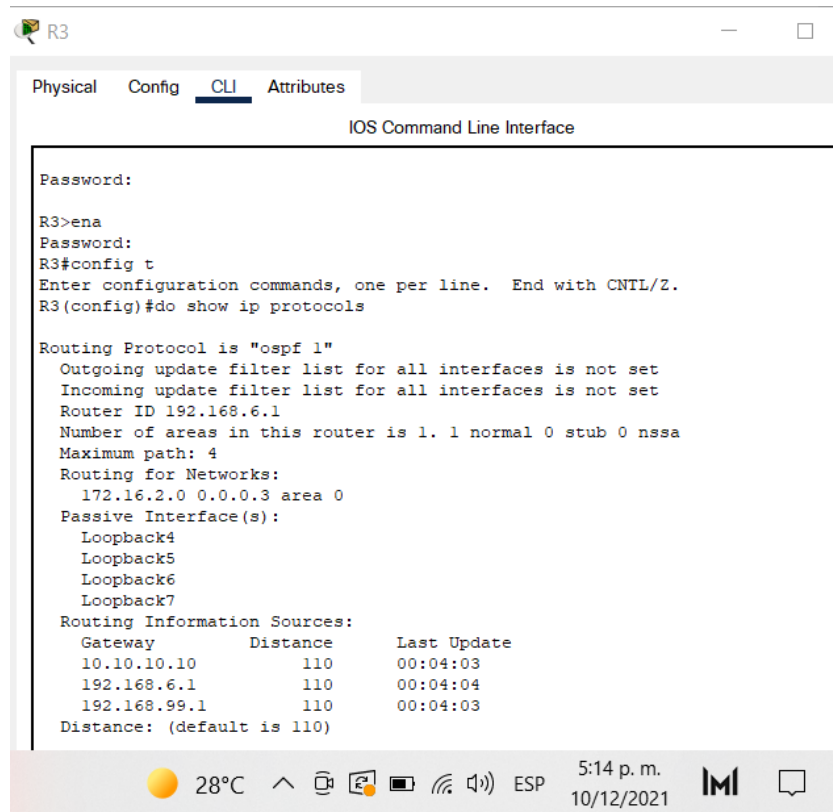


```
R1
Physical Config CLI Attributes
IOS Command Line Interface
^
% Invalid input detected at '^' marker.
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#do show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.99.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.3 area 0
    192.168.21.0 0.0.0.255 area 0
    192.168.23.0 0.0.0.255 area 0
    192.168.99.0 0.0.0.255 area 0
  Passive Interface(s):
    GigabitEthernet0/0/1.21
    GigabitEthernet0/0/1.23
    GigabitEthernet0/0/1.99
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.10.10      110          00:03:11
    192.168.6.1      110          00:03:12
    192.168.99.1     110          00:03:11
  Distance: (default is 110)
```

Fuente Autoría propia.

Figura 32. Protocolos de IP en R3.

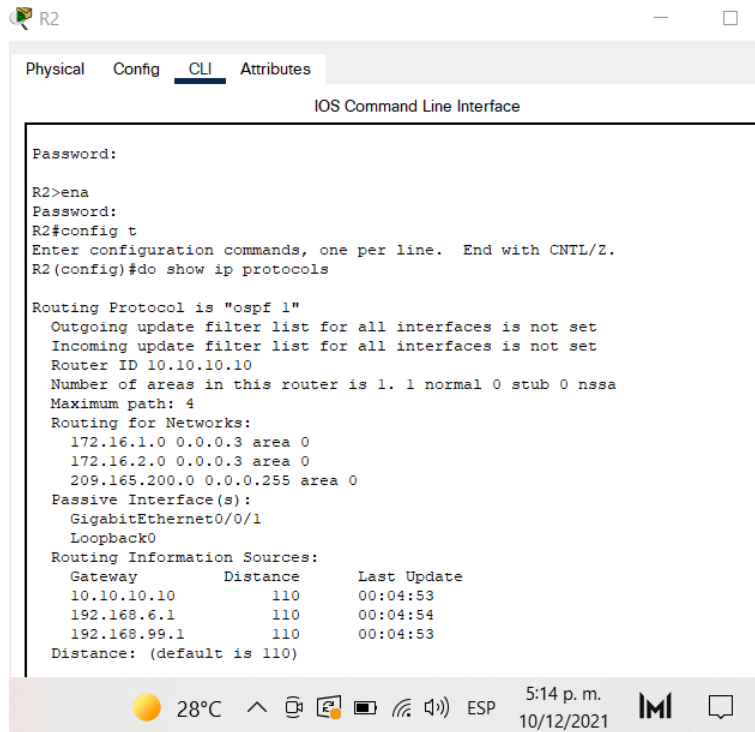


```
R3
Physical Config CLI Attributes
IOS Command Line Interface
Password:
R3>ena
Password:
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#do show ip protocols

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 0.0.0.3 area 0
  Passive Interface(s):
    Loopback4
    Loopback5
    Loopback6
    Loopback7
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.10.10      110          00:04:03
    192.168.6.1      110          00:04:04
    192.168.99.1     110          00:04:03
  Distance: (default is 110)
```

Fuente Autoría propia.

Figura 33. Protocolos de IP en R2.



```
R2
Physical Config CLI Attributes
IOS Command Line Interface
Password:
R2>ena
Password:
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#do 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 10.10.10.10
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.3 area 0
    172.16.2.0 0.0.0.3 area 0
    209.165.200.0 0.0.0.255 area 0
  Passive Interface(s):
    GigabitEthernet0/0/1
    Loopback0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.10.10      110          00:04:53
    192.168.6.1      110          00:04:54
    192.168.99.1     110          00:04:53
  Distance: (default is 110)
```

Fuente Autoría propia.

¿Qué comando muestra solo las rutas OSPF?

Con el comando `show ip route ospf` se muestran solo las rutas OSPF descubiertas por el Router.

Observar figuras 28, 29 y 30.

¿Qué comando muestra la sección de OSPF de la configuración en ejecución?

Con el comando `show ip ospf interface`, se puede ver una lista detallada de la configuración en ejecución del protocolo OSPF en el Router.

Figura 34. Configuración en ejecución de OSPF en R1.

```
R1#show ip ospf interface

GigabitEthernet0/0/1.21 is up, line protocol is up
  Internet address is 192.168.21.1/24, Area 0
  Process ID 1, Router ID 192.168.99.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.99.1, Interface address 192.168.21.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
GigabitEthernet0/0/1.23 is up, line protocol is up
  Internet address is 192.168.23.1/24, Area 0
  Process ID 1, Router ID 192.168.99.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.99.1, Interface address 192.168.23.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
GigabitEthernet0/0/1.99 is up, line protocol is up
  Internet address is 192.168.99.1/24, Area 0
  Process ID 1, Router ID 192.168.99.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.99.1, Interface address 192.168.99.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/2/0 is up, line protocol is up
  Internet address is 172.16.1.1/30, Area 0
  Process ID 1, Router ID 192.168.99.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:04
  Index 4/4, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

Fuente Autoría propia.

Figura 35. Configuración en ejecución de OSPF en R3.

```
R3# show ip ospf interface

Serial0/2/1 is up, line protocol is up
Internet address is 172.16.2.1/30, Area 0
Process ID 1, Router ID 192.168.6.1, Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:07
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
Adjacent with neighbor 10.10.10.10
Suppress hello for 0 neighbor(s)
R3#
```

Ctrl+F6 to exit CLI focus

Copy Paste

27°C 5:19 p.m. 10/12/2021

Fuente Autoría propia.

Figura 36. Configuración en ejecución de OSPF en R2.

```
R2# show ip ospf interface

Serial0/2/1 is up, line protocol is up
Internet address is 172.16.2.2/30, Area 0
Process ID 1, Router ID 10.10.10.10, Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:00
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
Adjacent with neighbor 192.168.6.1
Suppress hello for 0 neighbor(s)
Serial0/2/0 is up, line protocol is up
Internet address is 172.16.1.2/30, Area 0
Process ID 1, Router ID 10.10.10.10, Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:06
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
Adjacent with neighbor 192.168.99.1
Suppress hello for 0 neighbor(s)
R2#
```

Physical Config CLI Attributes

IOS Command Line Interface

27°C 5:20 p.m. 10/12/2021

Fuente Autoría propia.

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:

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.

```
R1(config)#ip dhcp pool ACCT          Asignando nombre a pool
R1(dhcp-config)#dns-server 10.10.10.10  Asignando dirección de servidor
dns.
```

```
R1(dhcp-config)#domain-name ccna-sa.com  Asignando nombre de dominio
R1(dhcp-config)#network 192.168.21.0 255.255.255.0  Asignando dirección
de network.
```

```
R1(dhcp-config)#default-router 192.168.21.1      Ingresando dirección de
puerta de enlace predeterminada.
```

Crear un pool de DHCP para la VLAN 23

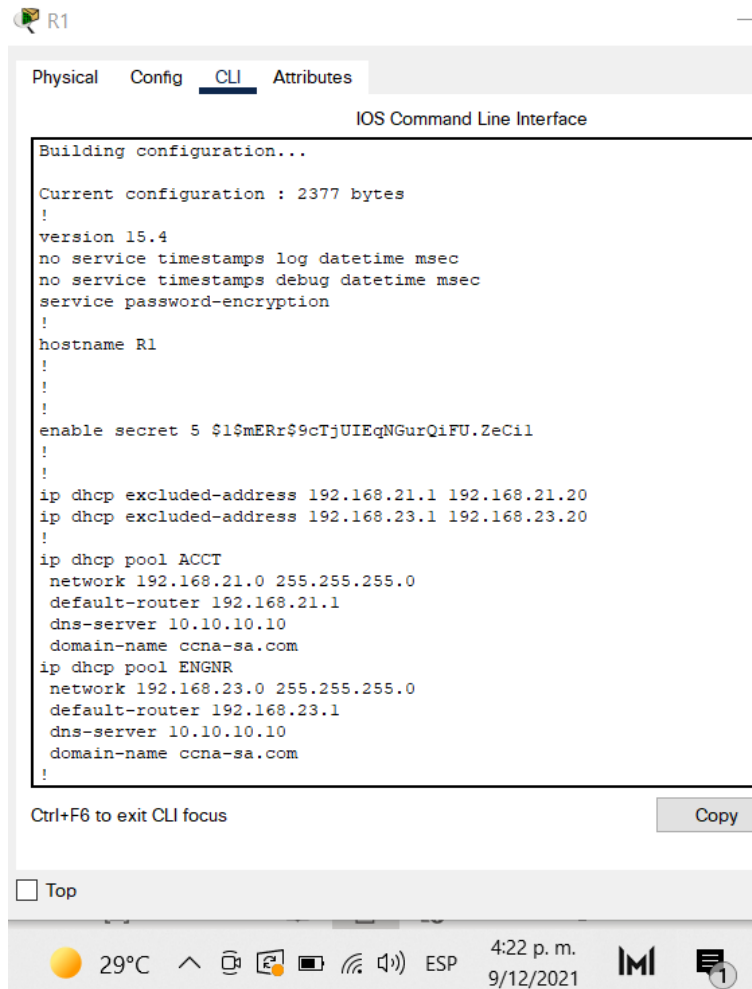
```
R1(config)#ip dhcp pool ENGNR          Asignando nombre a pool
R1(dhcp-config)#dns-server 10.10.10.10  Asignando dirección de servidor
dns.
```

```
R1(dhcp-config)#domain-name ccna-sa.com  Asignando nombre de dominio
R1(dhcp-config)#network 192.168.23.0 255.255.255.0  Asignando dirección
de network.
```

```
R1(dhcp-config)#default-router 192.168.23.1  Ingresando dirección de puerta de
enlace predeterminada.
```

```
R1(dhcp-config)#exit
```

Figura 37. Configuración DHCP en R1.



```
Building configuration...

Current configuration : 2377 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
!
ip dhcp excluded-address 192.168.21.1 192.168.21.20
ip dhcp excluded-address 192.168.23.1 192.168.23.20
!
ip dhcp pool ACCT
network 192.168.21.0 255.255.255.0
default-router 192.168.21.1
dns-server 10.10.10.10
domain-name ccna-sa.com
ip dhcp pool ENGNR
network 192.168.23.0 255.255.255.0
default-router 192.168.23.1
dns-server 10.10.10.10
domain-name ccna-sa.com
!
```

Fuente: Autoría propia.

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

La configuración del R2 incluye las siguientes tareas:

Crear una base de datos local con una cuenta de usuario

```
R2(config)#username webuser privilege 15 secret cisco12345
```

Crear una NAT estática al servidor web.

```
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
```

Asignando la interfaz interna y externa para la NAT estática

```
R2(config)#int g0/0/1
```

R2(config-if)#ip nat outside	Interfaz externa
R2(config)#int s0/2/0	
R2(config-if)#ip nat inside	Interfaz interna
R2(config-if)#int s0/2/1	
R2(config-if)#ip nat inside	Interfaz interna
R2(config-if)#exit	

Configurar la NAT dinámica dentro de una ACL privada

```
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
```

Defina el pool de direcciones IP públicas utilizables.

```
R2(config)#ip nat pool INTERNET 209.165.200.226 209.165.200.228
netmask 255.255.255.248
```

Definir la traducción de NAT dinámica

```
R2(config)#ip nat inside source list 1 pool INTERNET
```

Figura 38. Configuración NAT estática y dinámica en R2.

```

R2
Physical Config CLI Attributes
IOS Command Line Interface
!
ip nat pool INTERNET 209.165.200.226 209.165.200.228 netmask 255.255.255.248
ip nat inside source list 1 pool INTERNET
ip nat inside source static 10.10.10.10 209.165.200.229
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0/0
!
ip flow-export version 9
!
ipv6 route ::/0 GigabitEthernet0/0/0
!
ip access-list standard ADMIN-MGT
 permit host 172.16.1.1
access-list 1 permit 192.168.21.0 0.0.0.255
access-list 1 permit 192.168.23.0 0.0.0.255
access-list 1 permit 192.168.4.0 0.0.3.255
!
banner motd ^CSe prohíbe el acceso no autorizado^C
!
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
!
Ctrl+F6 to exit CLI focus
Copy Paste
29°C 4:36 p. m. 9/12/2021

```

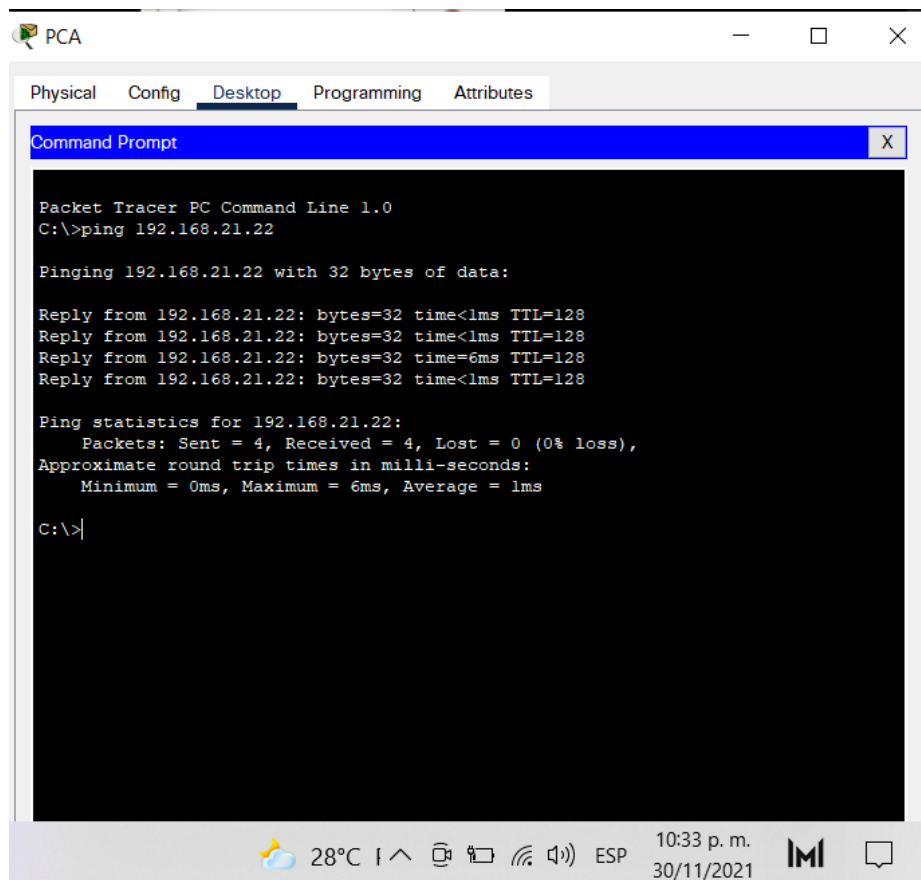
Fuente: Autoría propia.

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

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

Figura 39. Ping de PC-A a PC-C.



Fuente: Autoría propia.

Parte 6: Configurar NTP

Ajuste la fecha y hora en R2.

```
R2#clock set 9:00:00 march 5 2016
```

Configure R2 como un maestro NTP.

```
R2(config)#ntp master 5
```

Configurar R1 como un cliente NTP.

```
R1(config)#ntp server 172.16.1.2
```

Configure R1 para actualizaciones de calendario periódicas con hora NTP.

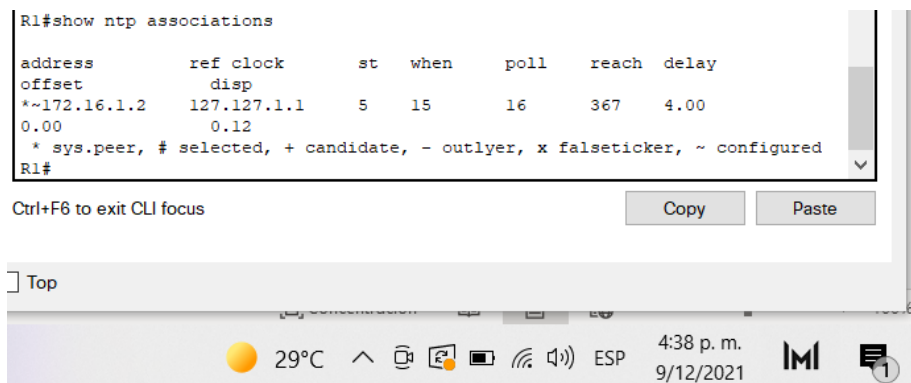
```
R1(config)#ntp update-calendar
```

```
R1(config)#exit
```

Verifique la configuración de NTP en R1.

```
R1#show ntp associations
```

Figura 40. Configuración de NTP en R1.



```
R1#show ntp associations
address      ref clock    st  when  poll  reach  delay
offset
*~172.16.1.2 127.127.1.1  5   15   16   367   4.00
0.00         0.12
* sys.peer, # selected, + candidate, - outlier, x falseticker, ~ configured
R1#
```

Fuente: Autoría propia.

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

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

Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2

```
R2(config)#ip access-list standard ADMIN-MGT
```

Asignando nombre de lista de acceso standard

```
R2(config-std-nacl)#permit host 172.16.1.1
```

Permitiendo conexión telnet para R1.

```
R2(config-std-nacl)#end
```

Aplicar la ACL con nombre a las líneas VTY

```
R2(config)#line vty 0 15
```

Ingresando a líneas vty 0 15

```
R2(config-line)#access-class ADMIN-MGT in
```

Aplicando ACL a líneas vty

Permitir acceso por Telnet a las líneas de VTY

R2(config-line)#transport input telnet
líneas vty.

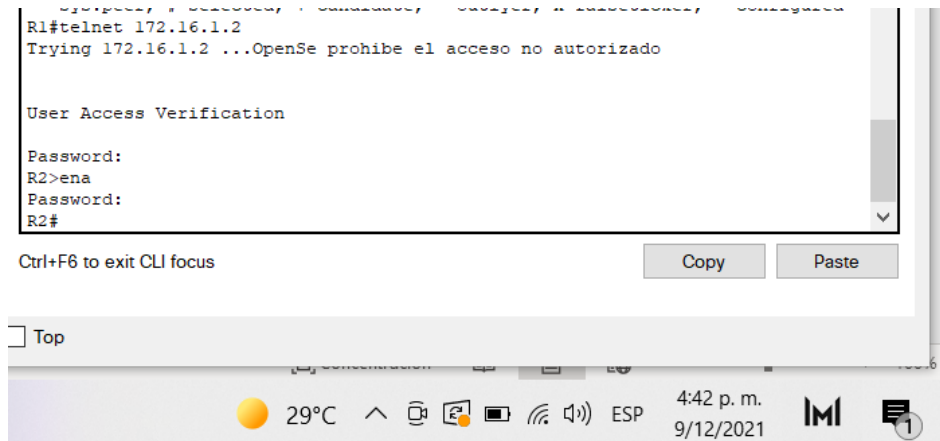
Permitiendo acceso por Telnet a las

Verificar que la ACL funcione como se espera

R1#telnet 172.16.1.2

Ingresando por telnet a R2.

Figura 41. Ingreso por telnet de R1 a R2..



Fuente: Autoría propia.

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

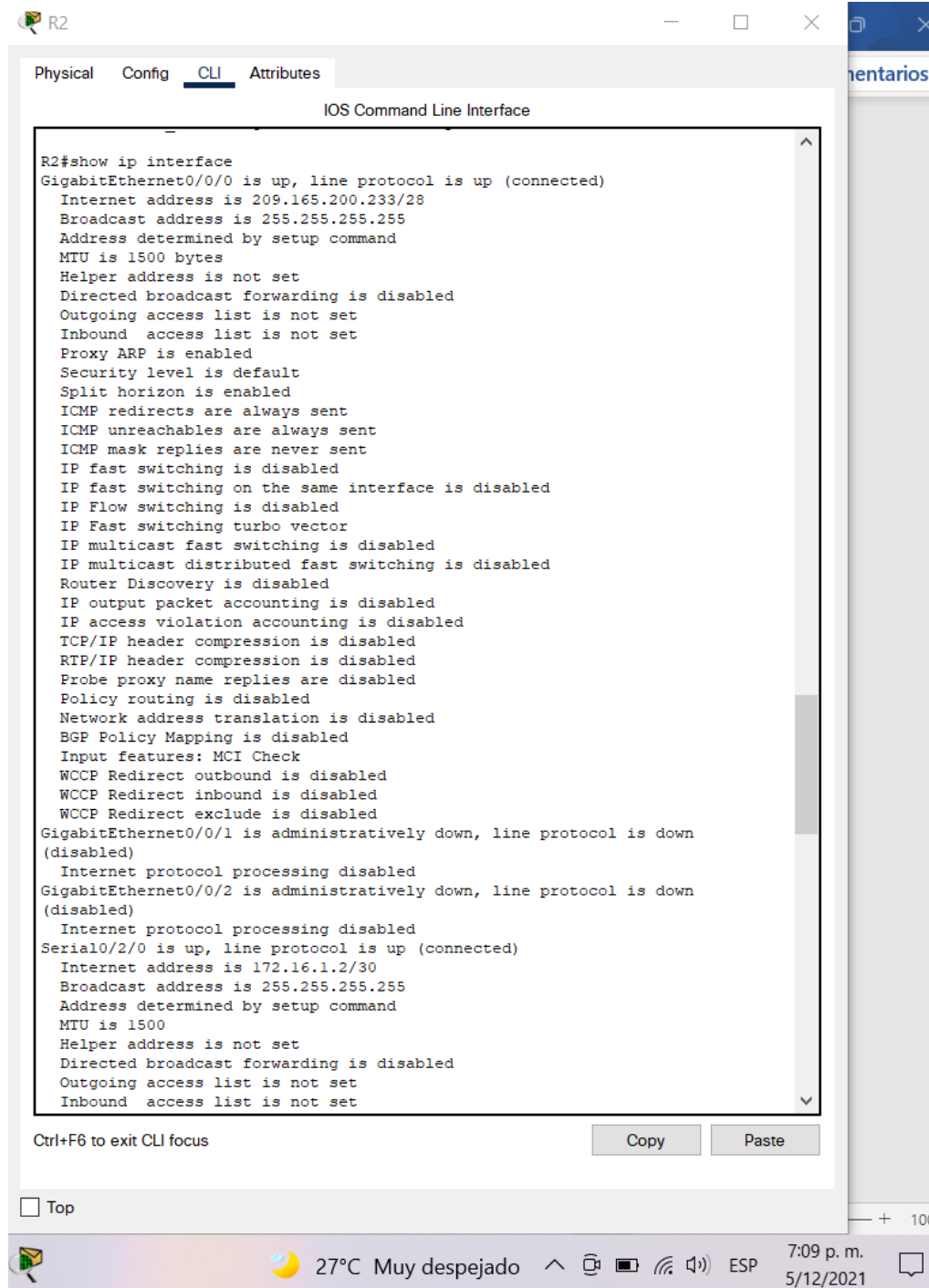
Tabla 8. Comandos CLI.

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Show access list
Restablecer los contadores de una lista de acceso	Clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Show ip interface
¿Con qué comando se muestran las traducciones NAT?	Show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Clear ip nat translation

Fuente: Autoría propia.

Show ip interface

Figura 43. Interfaz ip de router R2.



Fuente: Autoría propia.

Figura 44. Interfaz ip de router R1.

```
IOS Command Line Interface

Internet protocol processing disabled
GigabitEthernet0/0/1 is up, line protocol is up (connected)
Internet protocol processing disabled
GigabitEthernet0/0/1.21 is up, line protocol is up (connected)
Internet address is 192.168.21.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
GigabitEthernet0/0/1.23 is up, line protocol is up (connected)
Internet address is 192.168.23.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

27°C Muy despejado 7:12 p. m. 5/12/2021

Fuente: Autoría propia.

Figura 45. NAT estáticas de servidor web en router 2.

```
R2#show ip nat translations
Pro  Inside global    Inside local      Outside local     Outside global
---  209.165.200.229  10.10.10.10      ---              ---
R2#
```

Ctrl+F6 to exit CLI focus

Copy

Paste

Top

27°C Muy despejado ^ ☰ 🔋 📶 🔊 ESP 7:30 p. m. 5/12/2021

Fuente: Autoría propia.

Figura 46. Borrando entradas dinámicas.

```
R2#clear ip nat translation *
R2#
```

Ctrl+F6 to exit CLI focus

Copy

Paste

Top

27°C Muy despejado ^ ☰ 🔋 📶 🔊 ESP 7:26 p. m. 5/12/2021

Fuente: Autoría propia

CONCLUSIONES

En este trabajo se muestra la solución de los 2 escenarios, dando por cumplido los objetivos principales de cada uno de estos.

En el escenario 1 se logró la construcción y configuraciones principales del direccionamiento IP, para el Switch y el Router mediante una conexión por consola, se realizaron las configuraciones básicas de los dispositivos finales o PC'S.

En el escenario 2 se realizó una configuración de una red en donde inicialmente se realizó una configuración inicial a los routers y switches pertenecientes al esquema, después de esto se le implemente seguridad en cada uno de ellos, además de esto se estableció el routing entre VLANs.

En la segunda parte del escenario 2 se empleó el protocolo de routing dinámico OSPF, además de esto se empleó DHCP y NAT, en donde por último se configuro NTP para dar por terminado el escenario.

En cada uno de estos escenarios se logró el reconocimiento de los conceptos principales de las redes y telecomunicaciones, como así implementar esquemas de seguridad en dispositivos pertenecientes a esta red.

BIBLIOGRAFÍA

ARIGANELLO, Ernesto. Redes CISCO. Guía de estudio para la certificación CCNA Security. Grupo Editorial RA-MA, 2013.

BAREÑO Gutiérrez, R. (2013). Elaboración de un estado de arte sobre el protocolo IPV6; y su implementación sobre protocolos de enrutamiento dinámico como RIPNG, EIGRP y OSPF basado sobre la plataforma de equipos cisco.

BAREÑO Raúl, G., & Sevillano, A. M. L. (2017, October). Services cloud under HSTS, Strengths and weakness before an attack of man in the middle MITM. In *2017 Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI)* (pp. 1-5). IEEE.

BELTRÁN BRAVO, Jhoan Alexis, et al. Conectividad y configuración dinámica de direcciones NAT, ACL Y DHCP.

BORONAT SEGUI, Fernando. Configuración DHCP en routers CISCO. 2015.

DUMITRACHE, C. G., et al. Comparative study of RIP, OSPF and EIGRP protocols using Cisco Packet Tracer. En *2017 5th International Symposium on Electrical and Electronics Engineering (ISEEE)*. IEEE, 2017. p. 1-6.

GUTIERREZ, R. B., Núñez, W. N., Urrea, S. C., Osorio, H. S., & Acosta, N. D. (2016). Revisión de la seguridad en la implementación de servicios sobre IPv6. *Inge Cuc*, 12(1), 86-93.

GUTIERREZ, R. B., Urrea, S. C., Núñez, W. N., Sarmiento, H., Acosta, N. D., & Sánchez, G. G. V. (2015). Análisis de la seguridad en la implementación de servicios corporativos sobre el protocolo IPV. *Revista de Tecnología*, 14(1), 127-138.

KHEDR, Mohamed E.; ZAGHLOUL, Mohamed S.; EL-DESOUKY, Mohamed I. Wireless adhoc multi access networks optimization using ospf routing protocol based on cisco devices. *International Journal of Computer Networks & Communications*, 2015, vol. 7, no 2, p. 59.

MENDEZ SANJUAN, LICETH LORENA. CONFIGURACION Y RESOLUCION DE PROBLEMAS DE NAT EN IPV4 E IPV6, UTILIZANDO DISPOSITIVOS CISCO. 2018. Tesis Doctoral.

MUÑOZ MORENO, Lilia Alexandra, et al. Solución de dos estudios de caso bajo el uso de tecnología Cisco. 2014.

PRAYITNO, Ragiel Hadi; YAKTI, Bayu Kumoro. IMPLEMENTASI NAT IPv4 DENGAN NETWORK AUTOMATION PADA CISCO ROUTER. UG Journal, 2021, vol. 14, no 4.

RASHID, Nazre Abdul, et al. Cisco Packet Tracer Simulation as effective pedagogy in computer networking course. 2019.

SERRANO RECHE, Juan. Desarrollo de un entorno práctico sobre direccionamiento estático y dinámico basado en equipos Cisco. 2013. Tesis Doctoral. Universitat Politècnica de València.

STERLING MARTÍNEZ, Diego Andrés, et al. Desarrollo e implementación de red estructurada en simulador Cisco. 2018.