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

LUIS FERNANDO PALACIOS DIAZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

INGENIERÍA DE SISTEMAS

SOGAMOSO

2022

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

LUIS FERNANDO PALACIOS DIAZ

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

Director de curso:

Msc. HÉCTOR JULIAN PARRA MOGOLLÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

INGENIERÍA DE SISTEMAS

SOGAMOSO

2022

Nota de Aceptación

Firma del presidente del Jurado

Firma del Jurado

Firma de Jurado

Sogamoso, 14 de junio de 2022

AGRADECIMIENTOS

Mi agradecimiento está dirigido a todos aquellos profesores de la UNAD que a lo largo de los años han hecho posible que yo haya podido estudiar a pesar de la distancia, en especial al equipo docente del CEAD Sogamoso. Mi especial reconocimiento a las ingenieras Ana Milena Corregidor Castro y Yenny Stella Núñez Álvarez por todo su apoyo técnico.

CONTENIDO

Pág.

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

DHCP (Dynamic Host Configuration Protocol). DHCP es un protocolo de configuración que asigna de forma dinámica direcciones IP para clientes. Funciona en versión DHCPv4 y DHCPv6 .(Lammle (2013, p. 98).

DIRECCIÓN IPv4. La estructura de notación decimal punteada, que tiene la forma X.X.X.X, donde cada x representa un número decimal entre 0 y 255. “Las direcciones IPv4 son números asignados a los dispositivos individuales conectados a una red (Cisco, s.f., ap. 2.6.1) “.

INTERFAZ. “Puertos especializados en un dispositivo de red que se conecta a redes individuales. Debido a que los routers conectan redes, los puertos en un router se denominan interfaces de red (Cisco, s.f.)”.

LAN. Una LAN (*Local Area Network*) es una infraestructura de la red cuyo alcance se restringe a un área geográfica pequeña, como una oficina, un edificio, un hotel o un campus universitario.

MÁSCARA DE SUBRED IPv4. “Una máscara de subred IPv4 es un valor de 32 bits que separa la porción de red de la dirección de la porción de host. Junto con la dirección IPv4, la máscara de subred determina a qué subred pertenece el dispositivo (Cisco, s.f., ap. 2.6.1)“.

NAT (Network Address Translation) La Traducción de Direcciones de Red se utiliza para “Traducir las direcciones IPv4 de una red privada en direcciones IPv4 públicas globalmente únicas (Cisco, s.f., ap. 3.3.4)”.

NTP (Network Time Protocol). Protocolo que se utiliza para sincronizar los relojes de los sistemas informáticos a través de redes de datos de latencia variable conmutadas por paquetes (Lammle, 2013, p. 293),.

OSPF (Open Shortest Path First). Es un protocolo de enrutamiento de estándar abierto, de tipo pasarela interior (IGP), que permite encontrar el camino más corto entre dos hosts. OSPF es compatible con IPV4 e IPv6, minimiza el tráfico de routing, es altamente flexible, versátil, escalable y soporta VLSM (Lammle, 2013, p. 386).

TOPOLOGÍA FÍSICA. “Los diagramas de topología física ilustran la ubicación física de los dispositivos intermedios y la instalación del cable (Cisco, s.f., ap. 1.3.1)”.

TOPOLOGÍA LÓGICA. “Los diagramas de topología lógica ilustran los dispositivos, los puertos y el esquema de direccionamiento de la red (Cisco, s.f., ap. 1.3.1)”.

VLAN. Una Interfaz virtual de red (Switch virtual Interface, SVI) es una representación lógica de una interface de capa 3 en un switch. “La interfaz virtual le permite administrar de forma remota un switch a través de una red utilizando IPv4 e IPv6 (Cisco, s.f., ap. 2.6.2)”.”.

RESUMEN

En este documento se ponen a prueba las habilidades prácticas obtenidas por el estudiante en el Diplomado de profundización Cisco (Diseño e implementación de soluciones integradas LAN / WAN) mediante el desarrollo de dos ejercicios prácticos denominados *Escenario 1* y *Escenario 2, ambos construidos en el simulador Cisco Packet Tracer*. En el *escenario 1* se construye una topología de red compuesta por dos LAN unidas a un router: la primera LAN tiene 50 host y un switch, y la segunda LAN tiene 50 hosts. El ejercicio consiste en crear la tabla de direccionamiento IPv4 para cada una de esas LAN aplicando VLSM, configurar los equipos intermedios con medidas de seguridad y comprobar que hay conectividad entre todos los dispositivos. En el Escenario 2 se configura una red corporativa que contiene tres routers, dos switches, acceso a servidores de internet y varias VLAN. Las configuraciones incluyen: medidas de seguridad básicas, direccionamiento estático en IPV4 e IPv6, direccionamiento dinámico con OSPF, servidor DHCP, listas de acceso ACL, sincronización NTP y traducción de direcciones NAT.

PALABRAS CLAVE: Configuración de redes LAN, Conmutación y enrutamiento, Protocolos de red, Cisco.

ABSTRACT

In this document, the practical skills obtained by the student in the Cisco Deepening Diploma (Design and implementation of integrated LAN / WAN solutions) are tested through the development of two practical exercises called *Scenario 1* and *Scenario 2*, both built in the Cisco Packet Tracer simulator. In *scenario 1*, a network topology is built consisting of two LANs joined to a router: the first LAN has 50 hosts and a switch, and the second LAN has 50 hosts. The exercise consists of creating the IPv4 address table for each of these LANs by applying VLSM, configuring the intermediate equipment with security measures and checking that there is connectivity between all the devices. In *Scenario 2*, a corporate network is configured. It contains three routers, two switches, access to Internet servers, and several VLANs. Configurations include basic security measures, static addressing in IPV4 and IPv6, dynamic addressing with OSPF, DHCP server, ACL access lists, NTP synchronization, and NAT address translation.

KEYWORDS: LAN network configuration, Switching and Routing, Network protocols, Cisco

1. INTRODUCCIÓN

El ser humano se distingue de otras especies, entre otros aspectos, por su alta capacidad comunicativa. La necesidad de recopilar, gestionar y transmitir información de forma ágil y efectiva, cubriendo distancias cada vez mayores, ha sido uno de los grandes pilares del desarrollo tecnológico de nuestra especie.

Poco a poco, siglo a siglo, cada sociedad ha ido efectuando mejoras en los sistemas de comunicación para que estos sean más fiables, más económicos, más efectivos y, sobre todo, más rápidos. Desde el uso de aves mensajeras y estafetas personales hasta el despliegue de las sofisticadas redes de telecomunicaciones actuales, compuesta de protocolos, entramados de cables, computadores, frecuencias electromagnéticas y satélites artificiales.

En este contexto se comprende la importancia que tiene para los estudiantes universitarios de ingeniería de sistemas adquirir las habilidades técnicas necesarias para diseñar y administrar redes, que son como sistemas vivos que evolucionan constantemente, porque de ellas depende en gran medida el estilo de vida actual, todos los sistemas críticos de control y abastecimiento de los servicios públicos, la economía y la banca, el transporte y la navegación, el entretenimiento, la defensa nacional y hasta la guerra híbrida.

En el presente documento se presentan los ejercicios prácticos denominados Escenario 1 y Escenario 2, del Diplomado de profundización cisco (Diseño e implementación de soluciones integradas LAN / WAN), con los cuales el estudiante deja constancia de sus habilidades en administración de redes. Los escenarios se desarrollan en equipos virtuales usando en simulador Packet Tracer de CISCO.

El uso de simuladores permite al estudiante acceder de forma virtual a una gran cantidad de equipos y componentes que funcionan en gran medida como los equipos reales, pero con un costo económico y logístico que tiende a cero; si bien es verdad que se echa en falta la experiencia pedagógica que aporta la manipulación física de los equipos.

El *switching and routing* realizado en estos escenarios se asemejan a los requisitos y necesidades generales que podría demandar una empresa pequeña y se corresponde con las habilidades técnicas requeridas para la certificación CCNA de Cisco.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Desarrollar los ejercicios prácticos propuestos en la Guía de Trabajo denominada “Prueba de habilidades CCNA 2022”, según los requerimientos de la “Guía de actividades - Unidad 5 - Paso 6 - Entrega Avance Documento Final”.

2.2. OBJETIVOS ESPECÍFICOS

Desarrollar el Escenario 1 propuesto de forma tal que la red sea completamente operativa en el simulador de Cisco Packet Tracer.

Desarrollar, usando el simulador de Cisco Packet Tracer, el Escenario 2 propuesto de forma tal que se cumplan con todos los requerimientos de configuración solicitados.

Presentar evidencia del correcto funcionamiento de los equipos, según las configuraciones realizadas.

3. DESARROLLO DE LA ACTIVIDAD

3.1. ESCENARIO 1

3.1.1. Parte 1. “Topología del escenario 1”

De acuerdo con el documento “1. Prueba de habilidades CCNA 2022”, en el primer escenario se debe construir una topología de red similar a la que se muestra en la Figura 1 y configurarla para que funcione en IPv4.

Figura 1. Topología “escenario 1”

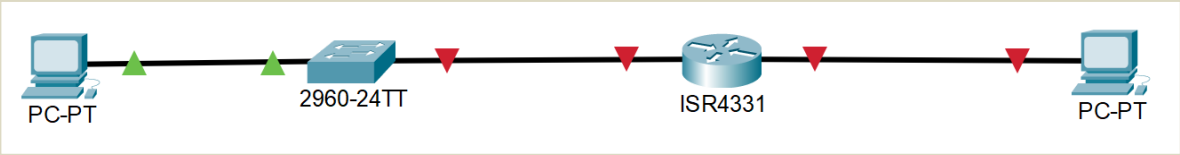
Fuente. Documento “Prueba de habilidades CCNA 2022”.

Siguiendo al documento citado arriba, el desarrollo del escenario se compone de las siguientes partes:

- Parte 1. Construir la topología física de red en el simulador Packet Tracer.
- Parte 2. Desarrollar un esquema de direccionamiento IPv4 para las subredes LAN1 y LAN2, en donde LAN1 se compone de 100 hosts y LAN2 se compone de 50 hosts.
- Parte 3. Configurar los dispositivos intermedios con ajustes básicos de seguridad y según el esquema de direccionamiento del paso anterior.
- Parte 4. Configurar los hosts PC-A y PC-B y verificar que hay concectividad entre los equipos.

En el simulador Cisco Packet Tracer se construye la topología física que se muestra en la Figura 2, usando los siguientes equipos: dos PC modelo PC-PT, un switch modelo 2960-24TT y un router modelo ISR4331. Las conexiones se hacen con cable de cobre directo porque se están conectando equipos de diferente tipo.

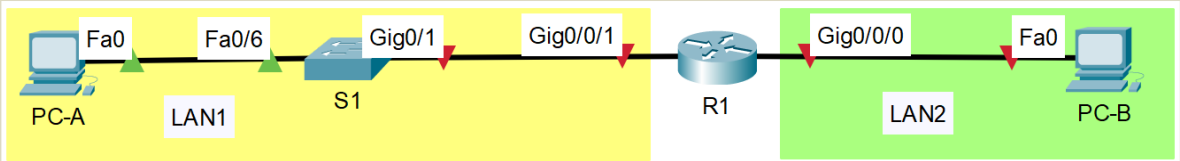
Figura 2. Componentes físicos Topología Escenario 1.



Fuente. Elaboración propia.

En la Figura 3 se muestran los nombres asignados a los equipos, las interfaces utilizadas y las dos LAN que requiere el escenario.

Figura 3. Redes LAN conectadas a R1.



Fuente. Elaboración propia.

3.1.2. Parte 2. Esquema de direccionamiento IP

La Tabla 1 muestra el esquema general de direccionamiento IPv4 desarrollado para dar cobertura a las necesidades actuales de la topología. Se aplica *máscara de subred de longitud variable* (VLSM) para optimizar la distribución de las direcciones IPv4.

Tabla 1. Escenario 1. Creación de subredes mediante VLSM

TABLA DE DIRECCIONAMIENTO PARA LA RED: 192.168.17.0/24					
	Hosts	Rango de host por red			Subnet mask
RED		Network	First	Last	
LAN1	100	192.168.17.0/25	192.168.17.1	192.168.17.126	/25
LAN2	50	92.168.17.128/26	192.168.17.129	192.168.17.190	/26
Sin usar	0	192.168.17.192/26	192.168.17.193	192.168.17.254	/26

Fuente. Elaboración propia.

3.1.2.1 Descripción del esquema de direccionamiento.

Se crea la red 192.168.17.0/24, en donde 17 se corresponde con los dos últimos dígitos del documento de identidad del autor de este documento.

La red 192.168.17.0/24 se divide en dos subredes /25, que tienen 126 direcciones IPv4 disponibles cada una, más la dirección reservada para de red y para el broadcast. Debido a que LAN1 sólo tiene 100 host, aún quedan 26 hosts libres para futuras expansiones. Se asigna la dirección 192.168.17.0/25 a la LAN1.

La subred 192.168.17.128/25 se subdivide en dos obteniéndose dos subredes /26, cada una con 64 hosts (62 libres). Se asigna la subred 192.168.17.128/26 a la LAN2, que solo requiere 50 direcciones IPv4. Pensando en futuros requerimientos de escalabilidad se deja disponible la subred 192.168.17.192/26.

3.1.2.2 Tabla de direccionamiento IPv4.

La tabla 2 describe los requerimientos técnicos que se solicitan para el escenario de red LAN.

Tabla 2. Escenario 1. Requerimientos del modelo.

Item	**Requerimiento**
Dirección de red	192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula.
Requerimiento de host LAN1	110
Requerimiento de host LAN2	50
R1 G0/0/1	Primera dirección de host de la subred LAN1
R1 G0/0/0	Primera dirección de host de la subred LAN2
S1 SVI	Segunda dirección de host de la subred LAN1
PC-A	Última dirección de host de la subred LAN1
PC-B	Última dirección de host de la subred LAN2

Fuente. Elaboración propia.

En la Tabla 3 se especifica la asignación de direcciones IPv4 solicitados en la Tabla 2. Estas son las direcciones y máscaras de subred que se van a configurar en cada uno de los dispositivos que componen la LAN1 y la LAN2 teniendo en cuenta las necesidades de número de host en cada una de las secciones de la topología.

Tabla 3. Escenario 1. Esquema de direcciones para LAN1 y LAN2.

Item	**Requerimiento**	
	Dirección	Máscara de subred
Dirección de red	192.168.17.0/24	255.255.255.0
R1 G0/0/1	192.168.17.1	255.255.255.128
R1 G0/0/0	192.168.17.129	255.255.255.192
S1 SVI	192.168.17.2	255.255.255.128
PC-A	192.168.17.126	255.255.255.128
PC-B	192.168.17.190	255.255.255.192

Fuente. Elaboración propia.

3.1.3. Parte 3. Configurar aspectos básicos

3.1.2.3 Configuración del router R1.

Las configuraciones de terminal que se que se muestran a continuación se realizan en el modo EXEC privilegiado, al cual se accede desde el modo EXEC usuario con la siguiente secuencia de comandos:

```
R1>enable
R1#configure terminal
```

A continuación se muestra el código necesario para configurar cada uno de los elementos solicitados:

Nombre del router: *R1*.

```
Router(config)#hostname R1
```

Desactivación de la búsqueda DNS.

```
R1(config)#no ip domain-lookup
```

Contraseña cifrada para el modo EXEC privilegiado: *ciscoenpass.*

```
R1(config)#enable secret ciscoenpass
```

Contraseña de acceso a la consola: *ciscoconpass:* Se entra a la línea de consola, se asigna la contraseña, se activa su uso al inicio de sesión.

```
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
```

Longitud mínima para las contraseñas: 10 caracteres.

```
R1(config)#security passwords min-length 10
```

Cifrado de contraseñas de texto no cifrado.

```
R1(config)#service password-encryption
```

Mensaje MOTD de advertencia.

```
R1(config)#banner motd #Acceso prohibido sin
autorizacion!#
```

Desconexión de la consola por inactividad: 5 minutos

```
R1(config-line)#exec-timeout 5
R1(config-line)#exit
```

Se asigna un nombre de dominio: *ccna-lab.com*.

```
R1(config)#ip domain-name ccna-lab.com
```

Generación de una clave de cifrado RSA, con módulo de 1024 bits

```
R1(config)#crypto key generate rsa
<…texto omitido …>
How many bits in the modulus [512]: 1024
<…texto omitido …>
R1(config)#
```

Configuración de la línea VTY con uso de la base de datos local

```
R1(config)#line vty 0 4
R1(config-line)#login local
```

Solo se acepta tráfico SSH.

```
R1(config-line)#transport input SSH
```

Tiempo de inactividad permitido.

```
R1(config-line)#exec-timeout 5
R1(config-line)#exit
```

Creación de un usuario administrativo en la base de datos local: nombre *admin*, contraseña *admin1pass*.

```
R1(config)#username admin secret admin1pass
```

Prevención de ataques DoS con *login block-for.* Se configura para que bloquee el proceso de autenticación SSH o Telnet durante 180 segundos para un usuario que ha fallado 4 veces en 120 segundos

```
R1(config)#login block-for 180 attempts 4 within 120
```

Configuración de la interfaz *gigabitEthernet 0/0/1*, que conecta con LAN1. Incluye descripción de la interfaz, asignación de dirección IPv4, máscara de red y activación de la interfaz.

```
R1(config)#interface g0/0/1
```

```
R1(config-if)#description CONECTA CON LAN1
R1(config-if)#ip address 192.168.17.1 255.255.255.128
R1(config-if)#no shutdown
R1(config-if)#exit
```

Configuración de la interfaz *gigabitEthernet 0/0/0*, que conecta con la LAN2. Incluye descripción de la interfaz, asignación de dirección IPv4 y activación de la interfaz.

```
R1(config)#interface g0/0/0
R1(config-if)#description CONECTA CON LAN2
R1(config-if)#ip address 192.168.17.129 255.255.255.192
R1(config-if)#no shutdown
R1(config-if)#exit
```

Una vez terminada la configuración solicitada, se guardan los cambios en la NVRAM:

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Para comprobar el estado actual de las interfaces del router se usa el comando *`show ip interface brief`*. Su ejecución muestra cómo las interfaces g0/0/0 y g0/0/1 tienen asignadas direcciones IPv4 requeridas y están activas, tal como se observa en la Figura 4.

Figura 4. Estado de las interfaces g0/0/0 y g0/0/1

```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0/0   192.168.17.129  YES manual up                    up
GigabitEthernet0/0/1   192.168.17.1    YES manual up                    up
GigabitEthernet0/0/2   unassigned      YES NVRAM  administratively down down
Vlan1                  unassigned      YES NVRAM  administratively down down
R1#
```

Fuente. Elaboración propia.

3.1.2.4 Configuración del switch S1.

Una vez finalizada la configuración del router se procede a configurar el switch S1 desde el CLI, en concreto.

Nombre del switch, que cambia a S1:

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname S1
```

Desactivación de la búsqueda DNS:

```
S1(config)#no ip domain-lookup
```

Se asigna un 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
```

Cifrado de contraseñas de texto no cifrado:

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

Mensaje MOTD de advertencia:

```
S1(config)#banner motd #Acceso prohibido sin
autorizacion!#
```

Creación de un usuario administrativo en la base de datos local: nombre *admin*, contraseña *admin1pass*:

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

Configuración de la línea VTY con uso de la base de datos local:

```
S1(config)#line vty 0 4
```

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

Configuración del tráfico SSH en la línea VTY:

```
S1(config-line)#transport input SSH
S1(config-line)#exit
```

Clave de cifrado RSA, con módulo de 1024 bits:

```
S1(config)#crypto key generate rsa
< … texto omitido… >
How many bits in the modulus [512]: 1024
< … texto omitido… >
```

Configuración de la interfaz virtual VLAN 1. Se incluye una descripción de la interfaz, su dirección IPv4 y máscara de red (se corresponde con la segunda dirección IPv4 disponible en la red LAN1) y se da de alta:

```
S1(config)#interface vlan 1
S1(config-if)#description VLAN del switch S1
S1(config-if)#ip address 192.168.17.2 255.255.255.128
S1(config-if)#no shutdown
S1(config-if)#exit
```

Configuración del Gateway predeterminado. Se usa la dirección de la interfaz g0/0/1 del router R1:

```
S1(config)#ip default-gateway 192.168.17.1
```

Se guarda la configuración en la NVRAM

```
S1#copy running-config startup-config
```

Para terminar, se comprueba el estado de la interfaz VLAN 1 con el comando *`show ip interfaz vlan 1`*, tal como se observa en la Figuras 5:

Figura 5. Estado de la interfaz virtual en S1

```
S1#show ip interface vlan 1
Vlan1 is up, line protocol is up
  Internet address is 192.168.17.2/25
```

Fuente. Elaboración propia.

3.1.2.5 Configurar los hosts PC-A y PC-B.

La Tabla 4 se muestran la configuración del PC-A, que se obtiene con el comando `ipconfig /all`, en el Command prompt de PC-A:

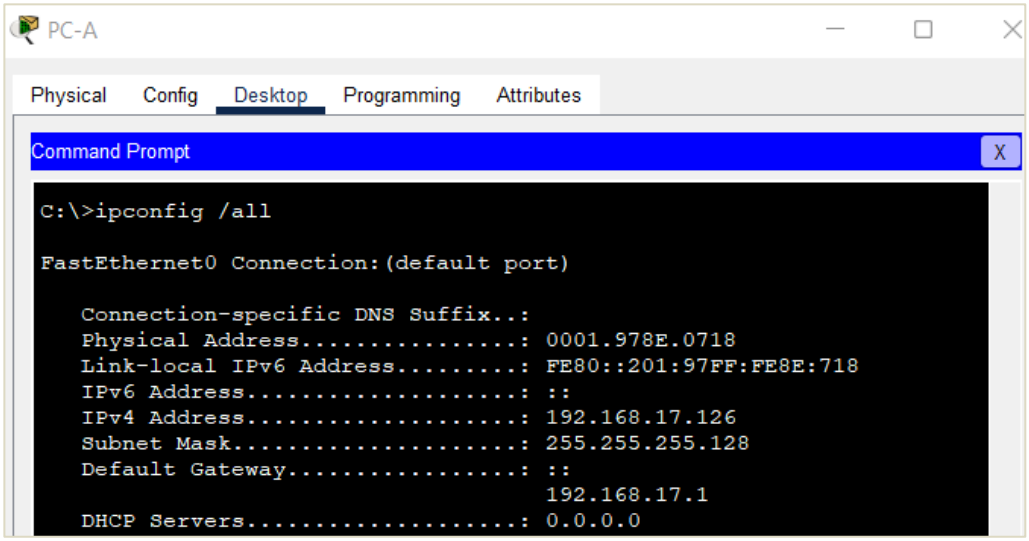
Tabla 4. Configuración del PC-A con IPv4 estática.

PC-A Network Configuration	
Descripción	PC-A
Dirección física	0001.978E.0718
Dirección IP	192.168.17.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.17.1

Fuente. Elaboración propia.

En la Figura 6 se observa el uso del comando `ipconfig /all` para obtener la información de la Tabla 4:

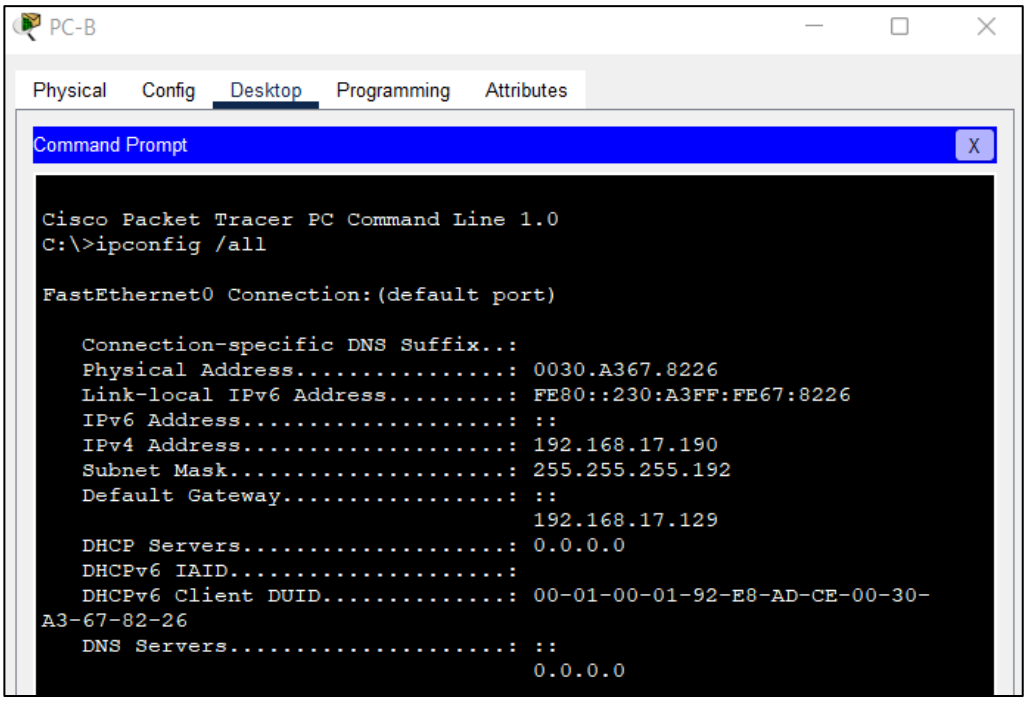
Figura 6. Comando ipconfig / all, en PC-A.



Fuente. Elaboración propia.

La Figura 7 y la Tabla 5 muestran la configuración de red PC-B, extraída con el comando `ipconfig /all`, en el Command prompt de PC-B:

Figura 7. Comando ipconfig / all, en PC-B.



Fuente. Elaboración propia.

Tabla 5. Escenario 1. Configuración del PC-B con IPv4 estática

PC-B Network Configuration	
Descripción	PC-B
Dirección física	0030.A367.8226
Dirección IP	192.168.17.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.17.129

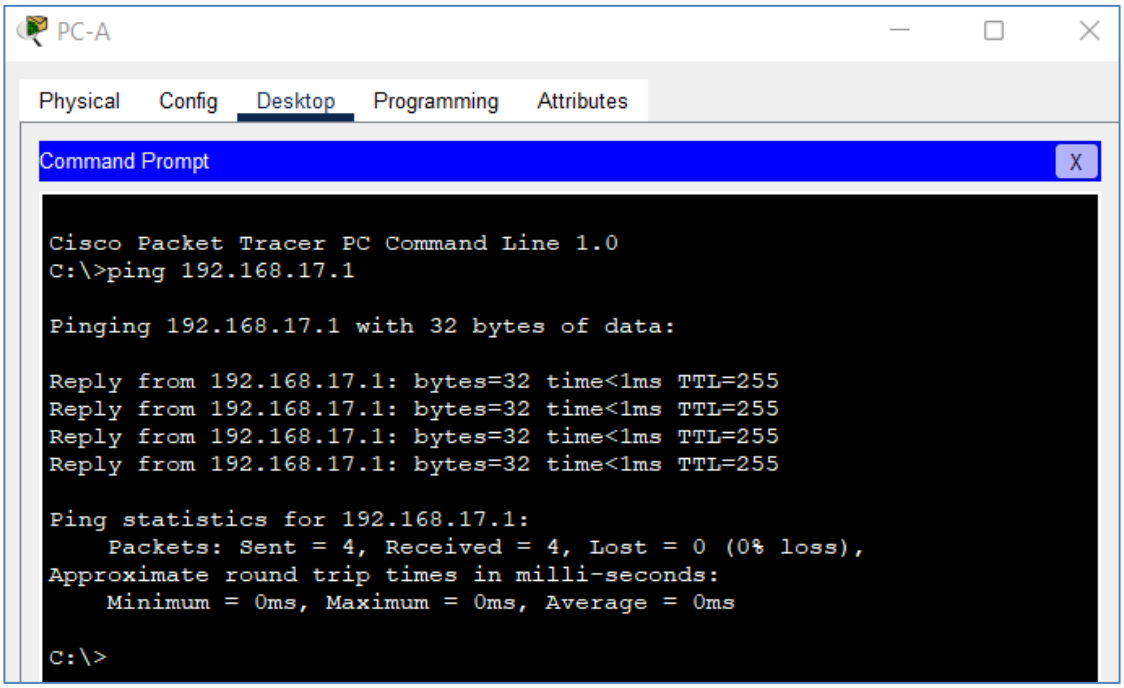
Fuente. Elaboración propia.

3.1.4. Parte 4. Comprobar la conexión.

3.1.2.6 Conexión con las puertas de enlace predeterminadas.

En la figura 8 se muestra la prueba de conexión entre PA-A y su puerta de enlace predeterminada, la interfaz g0/0/1 del router.

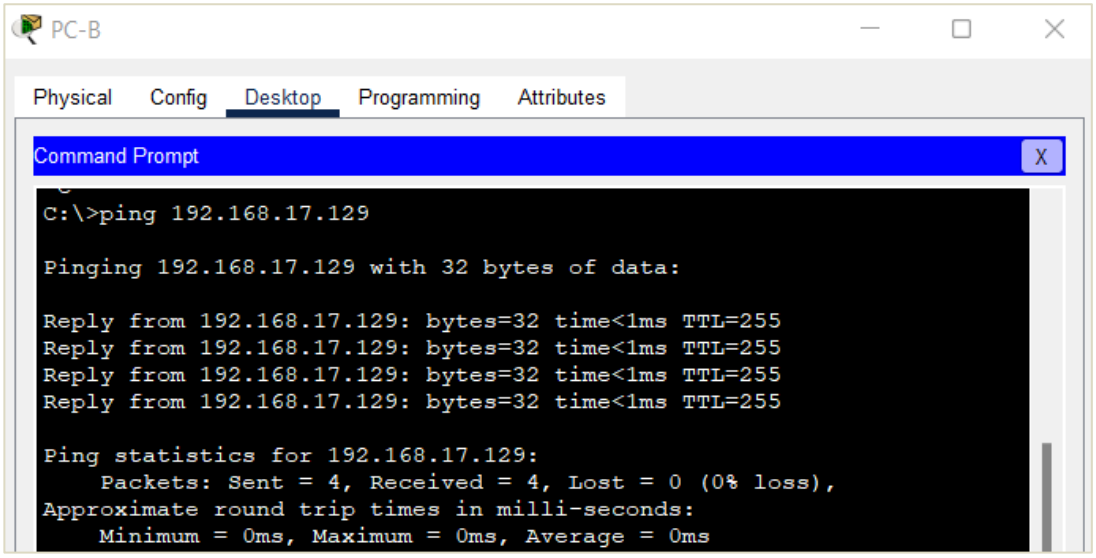
Figura 8. Conexión de PC-A con el router.



Fuente. Elaboración propia.

En la figura 9 se muestra la prueba de conexión entre PA-B y su puerta de enlace predeterminada, la interfaz g0/0/0 del router.

Figura 9. Conexión de PC-B con el router.

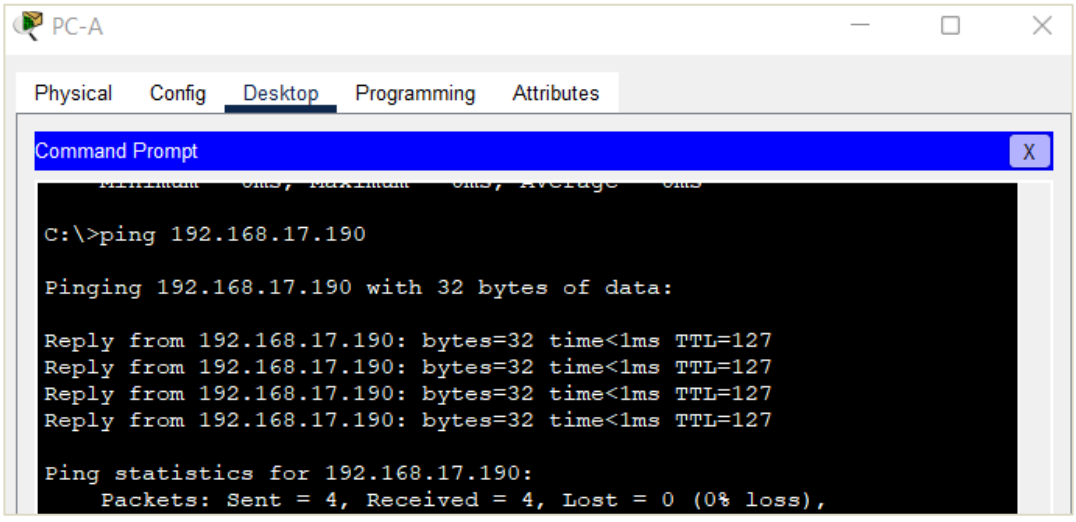


Fuente. Elaboración propia.

3.1.2.7 Conexión de extremo a extremo.

La Figura 10 muestra cómo se hace un Ping exitoso desde PC-A hasta PC-B.

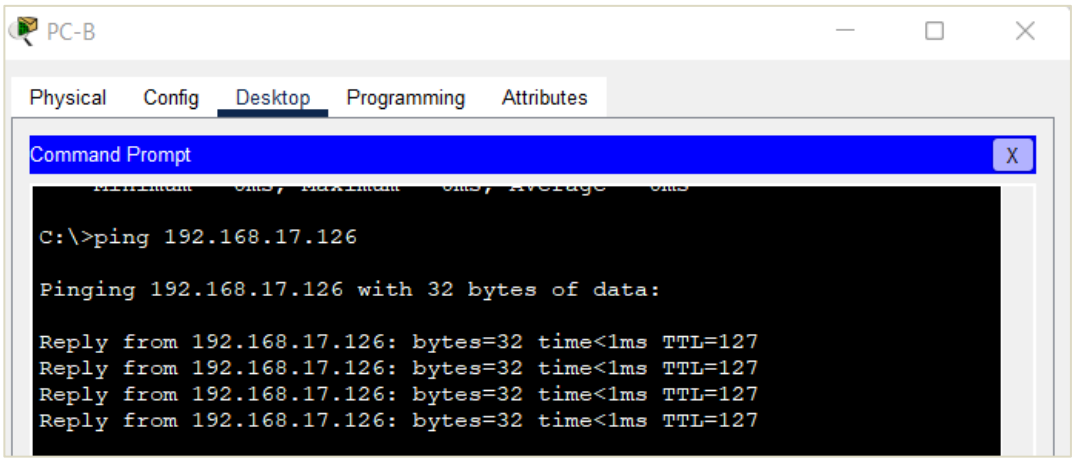
Figura 10. Prueba de conexión entre PC-A y PC-B.



Fuente. Elaboración propia.

La Figura 11 muestra cómo se hace un Ping exitoso desde PC-B hasta PC-A:

Figura 11. Prueba de conexión entre PC-B y PC-A.

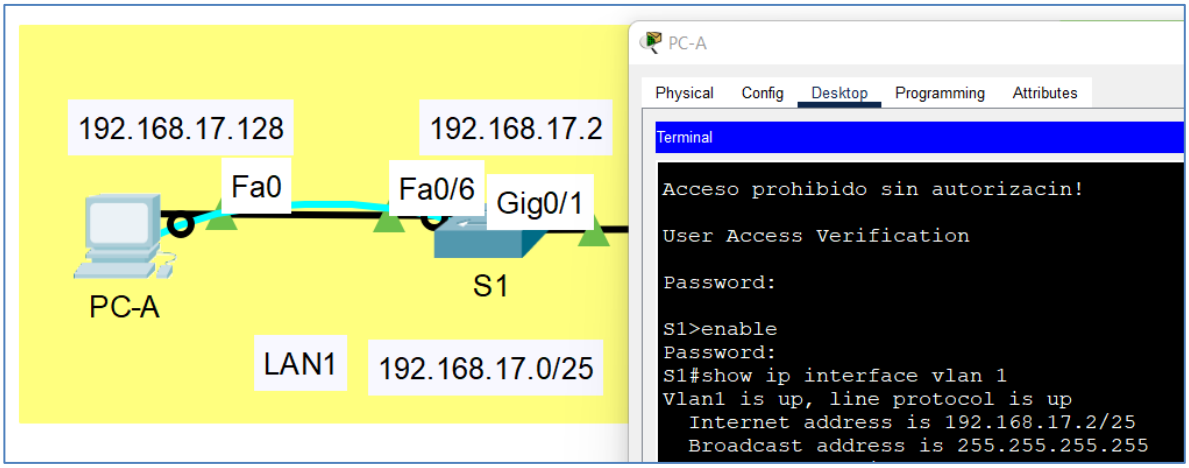


Fuente. Elaboración propia.

3.1.2.8 Conexión SSH a la interfaz VLAN 1 del switch S1.

Se conecta el switch S1 con el PC-A mediante el puerto de consola para comprobar el acceso SSH. En la parte izquierda de la Figura 12 se observa la conexión entre el PC-A y S1 usando el cable de consola, en color azul.

Figura 12. Conexión SSH en el switch S1.

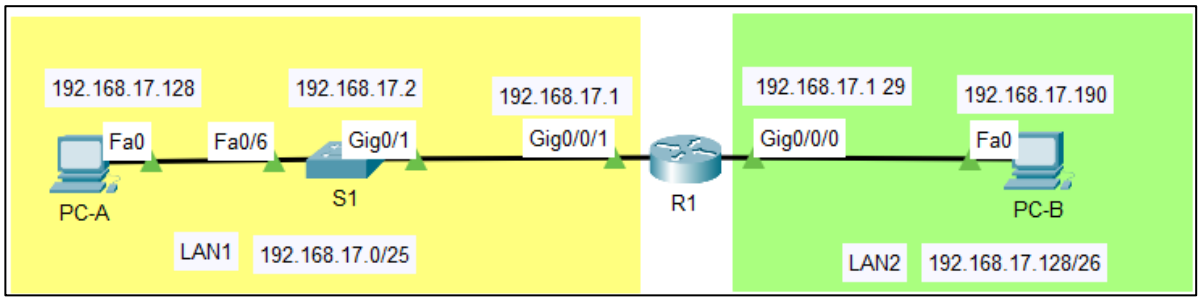


Fuente. Elaboración propia.

En el lado derecho de la Figura se observa la Terminal de PC-A durante el acceso durante el proceso de login: se evidencian el MOTD configurado y la solicitud de contraseñas de acceso a la consola y al modo EXEC privilegiado. Una vez logados se ejecuta un comando que permite ver el estado de la VLAN 1.

La Figura 13 muestra la topología lógica de la red, una vez comprobada su conectividad.

Figura 13. Topología lógica de la red.



Fuente. Elaboración propia.

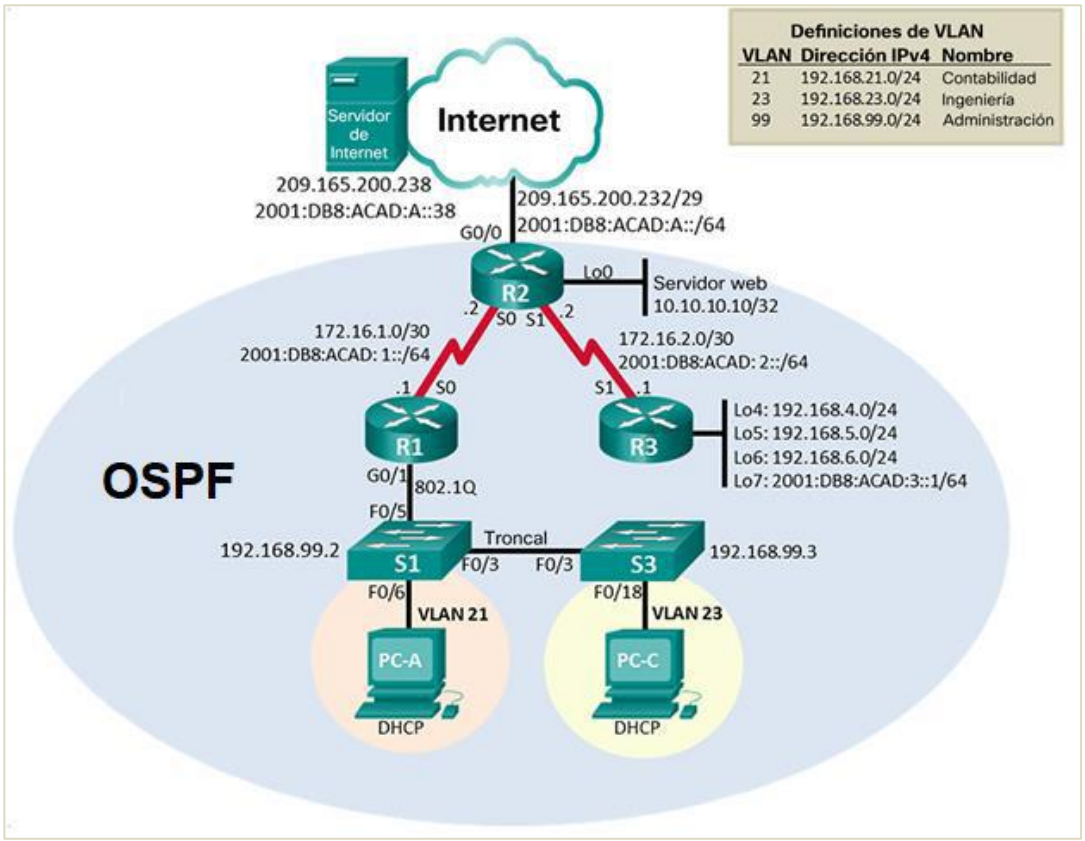
3.2. ESCENARIO 2

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.

3.2.1. Topología del “Escenario 2”

La Figura 14 muestra la topología de referencia del enunciado del problema.

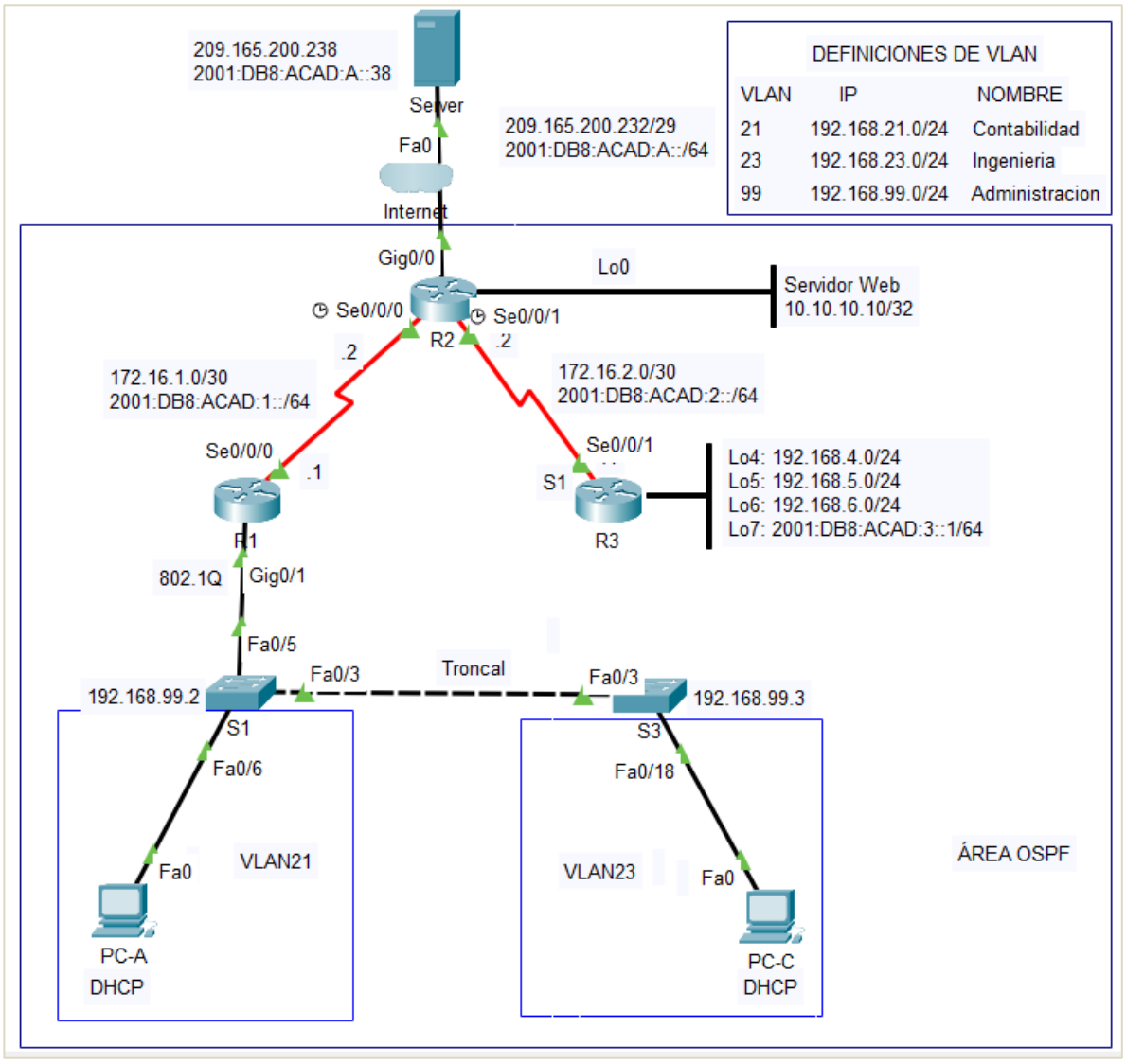
Figura 14. Topología del Escenario 2.



Fuente. Elaboración propia.

La Figura 15 muestra la misma topología, pero desarrollada en *Packet Tracer* con el fin de realizar las tareas solicitadas en el escenario.

Figura 15. Topología del Escenario 2 en Packet Tracer.



Fuente. Elaboración propia.

En la Tabla 6 se muestra el esquema de direccionamiento de toda la topología del escenario 2.

Tabla 6. Escenario 2. Tabla de enrutamiento.

Equipo	Interfaz	Dirección
Server		209.165.200.238/29
		2001:DB8:ACAD:A::38/64
	Gateway	2001:DB8:ACAD:A::1
R1	S0/0/0 (a R2)	172.16.1.1/30
		2001:DB8:ACAD:1::1/64
R2	S0/0/0 (a R1)	172.16.1.2/30
		2001:DB8:ACAD:1::2/64
	S0/0/1 (a R3)	172.16.2.2/30
		2001:DB8:ACAD:2::2/64
	G0/0 (a Server)	209.165.200.233/29
		2001:DB8:ACAD:A::1/64
	Lo0 (a Serv. Web)	10.10.10.10/32
R3	S0/0/1 (a R2)	172.16.2.1/30
		2001:DB8:ACAD:2::1/64
	Lo4	192.168.4.1/24
	Lo5	192.168.5.1/24
	Lo6	192.168.6.1/24
	Lo7	192.168.7.1/24
		Lo7: 2001:DB8:ACAD:3::1/64
S1	VLAN 99	192.168.99.2
	VLAN 21	192.168.21.0/24
S3	VLAN 99	192.168.99.3
	VLAN 23	192.168.23.0/24
PC-A	Fa0/0	DHCP
PC-C	Fa0/0	DHCP

Fuente. Elaboración propia.

3.2.2. Parte 1: Inicializar dispositivos

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

Acceder a los routers y eliminar sus archivos startup-config:

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

Volver a cargar todos los routers.

```
Router#reload
```

Para eliminar el archivo startup-config de los switches y eliminar la base de datos de VLAN que puedan tener se usa el siguiente comando:

```
Switch#erase startup-config
Switch#delete vlan.dat
```

Luego, para reiniciar los switches con su configuración por defecto:

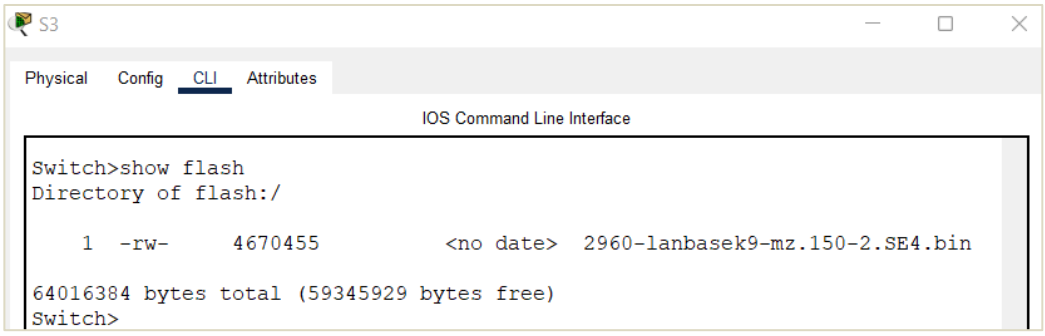
```
Switch#reload
```

Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches.

```
Switch>show flash, o bien, Switch>show dir flash
```

Tal como se observa en la Figura 16, al ejecutar el comando `show flash` sólo existe el archivo binario preconfigurado por el fabricante.

Figura 16. Contenido inicial de la menoria flash de un switch



Fuente. Elaboración propia.

3.2.3. Parte 2: Configurar los parámetros básicos de los dispositivos

3.2.3.1. Paso 1: Configurar la computadora de Internet.

Las tareas de configuración del servidor de Internet incluyen la información de la tabla 7. La red IPv4 209.165.200.232/29 tiene el siguiente rango de direcciones: 209.165.200.233 - 209.165.200.239.

Tabla 7. Configuración del servidor de internet.

Elemento o tarea de configuración	Especificación
Dirección IPv4 del servidor Server	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Broadcast	209.165.200.239
Dirección IPv6/subred	201:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Fuente. Elaboración propia.

En la Figura 17, que se muestra en la siguiente página, se observa la configuración del Servidor de internet.

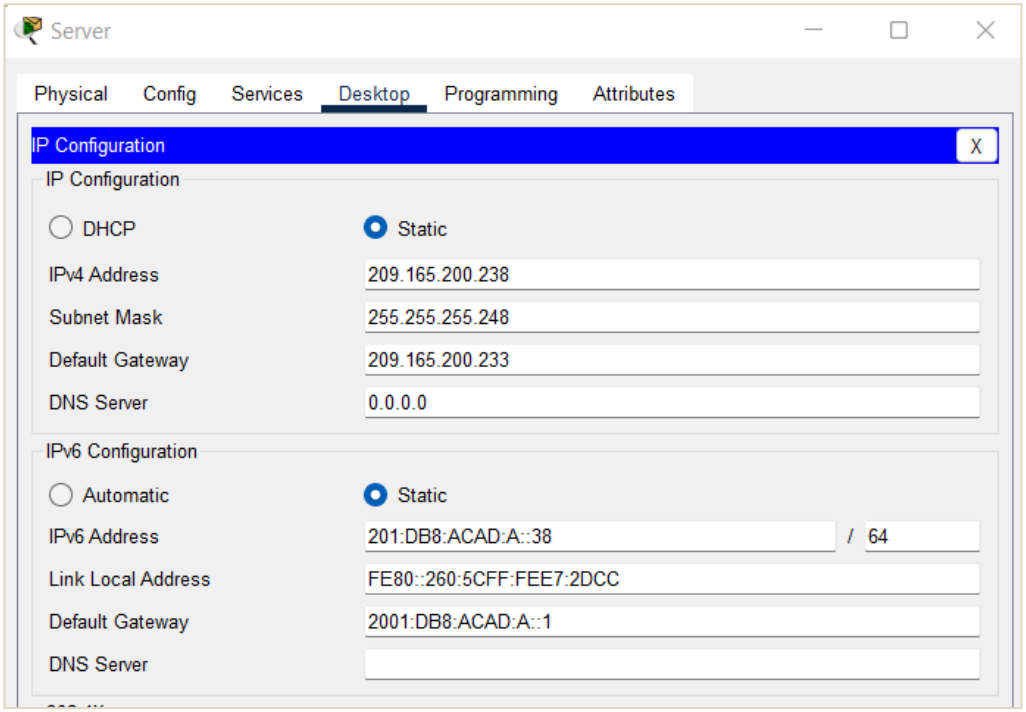
3.2.3.2. Paso 2: Configurar las interfaces.

a) Interfaz s0/0/0 en R1.

Desactivar la búsqueda DNS:

```
Router#config terminal
Router(config)#no ip domain-lookup
```

Figura 17. Configuración del servidor de internet.



Fuente. Elaboración propia.

Nombrar el router como *R1*

```
Router(config)#hostname R1
```

Contraseña de exec privilegiado cifrada: *class*

```
R1(config)#enable secret class
```

Contraseña de acceso a la consola: *cisco*

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
```

Contraseña de acceso Telnet y SSH: *cisco*

```
R1(config)#line vty 0 15
R1(config-line)#password cisco
```

```
R1(config-line)#login
R1(config-line)#exit
```

Cifrar las contraseñas de texto no cifrado

```
R1(config)#service password-encryption
```

Mensaje MOTD: "*Se prohíbe el acceso no autorizado*".

```
R1(config)#banner motd #Se prohibe el acceso no
autorizado.#
```

b) Configuración de la Interfaz S0/0/0.

Establecer una descripción

```
R1(config)#interface s0/0/0
R1(config-if)#description CONNECTION TO R2
```

Establecer la dirección IPv4

```
R1(config-if)#ip address 172.16.1.1 255.255.255.252
```

Establecer la dirección IPv6

```
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
```

Establecer la frecuencia de reloj en 128000. Packet Tracer rechaza este comando debido a que cuando se tendió el cable serial se conectó primero en R1 y luego en R2. La configuración se podrá aplicar en R2. En todo caso, el comando es:

```
R1(config-if)#clock rate 128000
```

Activar la interfaz

```
R1(config-if)#no shutdown
```

c) Configurar en S0/0/0 las rutas predeterminadas.

Ruta IPv4 predeterminada

```
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
```

Ruta IPv6 predeterminada

```
R1(config)#ipv6 route ::/0 s0/0/0
```

3.2.3.3. Paso 3: Configurar R2.

La configuración del R2 incluye las siguientes tareas:

Desactivar la búsqueda DNS

```
Router>enable
Router#config terminal
Router(config)#no ip domain-lookup
```

Nombrar el router como R2

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

Contraseña de exec privilegiado cifrada: *class*

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

Contraseña de acceso a la consola: *cisco*

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

Contraseña de acceso Telnet y SSH: *cisco*

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

Habilitar el servidor HTTP *

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

* Nota: Este comando no es compatible en la versión 8.1 de Packet Tracer.

Mensaje MOTD: “*Se prohíbe el acceso no autorizado*”.

```
R2(config)#banner motd #Se prohibe el acceso no
autorizado.#
```

a) Interfaz S0/0/0.

Establecer una descripción

```
R2(config)#interface s0/0/0
R2(config-if)#description CONNECTION TO R1
```

Establecer la dirección IPv4

```
R2(config-if)#ip address 172.16.1.2 255.255.255.252
```

Establecer la dirección IPv6

```
R2(config-if)#ipv6 address 2001:db8:acad:1::2/64
```

Establecer la frecuencia de reloj en 128000

```
R2(config-if)#clock rate 128000
```

Activar la interfaz

```
R2(config-if)#no shutdown
```

b) Interfaz S0/0/1.

Establecer la descripción

```
R2(config)#interface s0/0/1
R2(config-if)#description CONNECTION TO R3
```

Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

```
R2(config-if)#ip address 172.16.2.2 255.255.255.252
```

Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.

```
R2(config-if)#ipv6 address 2001:db8:acad:2::2/64
```

Establecer la frecuencia de reloj en 128000.

```
R2(config-if)#clock rate 128000
```

Activar la interfaz

```
R2(config-if)#no shutdown
```

c) Interfaz G0/0 (simulación de Internet).

Establecer la descripción.

```
R2(config)#interface g0/0
R2(config-if)#description CONNECTION TO INTERNET
```

Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

```
R2(config-if)#ip address 209.165.200.233 255.255.255.248
```

Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred.

```
R2(config-if)#ipv6 address 2001:db8:acad:a::1/64
```

Activar la interfaz

```
R2(config-if)#no shutdown
```

d) Interfaz loopback 0 (servidor web simulado).

Establecer la descripción.

```
R2(config)#interface Loopback0
R2(config-if)#description CONNECTION TO LOOPBACK 0
```

Establecer la dirección IPv4.

```
R2(config-if)#ip address 10.10.10.10 255.255.255.255
```

e) Ruta predeterminada.

Configure una ruta IPv4 predeterminada de G0/0.

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

Configure una ruta IPv6 predeterminada de G0/0.

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

3.2.3.4. Paso 4: Configurar R3.

La configuración del R3 incluye las siguientes tareas:

Desactivar la búsqueda DNS

```
Router>enable
Router#configure terminal
Router(config)#no ip domain-lookup
```

Nombre del router: *R3*

```
Router(config)#hostname R3
```

Contraseña de exec privilegiado cifrada: *class*

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

Contraseña de acceso a la consola: *cisco*

```
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
```

Contraseña de acceso Telnet y SSH: *cisco*

```
R3(config)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
```

Mensaje MOTD: "*Se prohíbe el acceso no autorizado*".

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

Cifrar las contraseñas de texto no cifrado

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

a) Interfaz S0/0/1.

Establecer la descripción

```
R3(config)#interface s0/0/1
R3(config-if)#description CONNECTION TO R2
```

Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

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

Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.

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

Activar la interfaz

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

b) Interfaz loopback 4.

Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

```
R3(config)#interface loopback4
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#exit
```

c) Interfaz loopback 5.

Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

```
R3(config)#interface loopback5
R3(config-if)#ip address 192.168.5.1 255.255.255.0
```

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

d) Interfaz loopback 6.

Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

```
R3(config)#interface loopback6
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#exit
```

e) Interfaz loopback 7.

Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.

```
R3(config)#interface loopback6
R3(config-if)# ipv6 address 2001:DB8:ACAD:3::1/64
R3(config-if)#exit
```

f) Ruta predeterminada

Configure una ruta IPv4 predeterminada de S0/0/1.

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

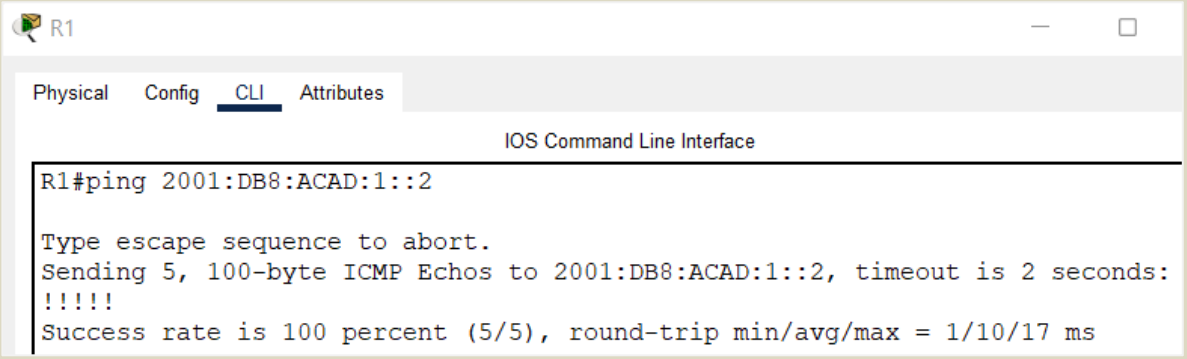
Configure una ruta IPv6 predeterminada de S0/0/1.

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

3.2.3.5. Paso 5: Comprobar la conectividad en IPv6

La Figura 18 muestra el resultado de un ping desde el router R1 a la interfaz s/0/0/0 del router R2 usando la dirección IPv6.

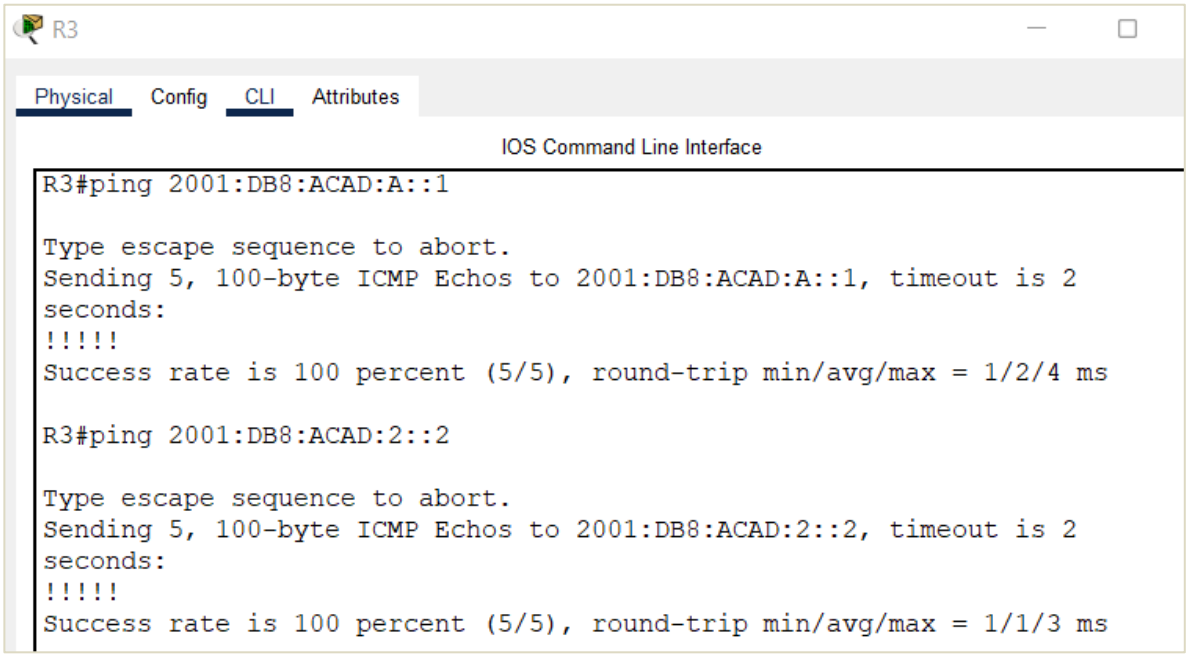
Figura 18. Conexión IPv6 entre R1 y R2



Fuente. Elaboración propia.

La Figura 19 muestra las pruebas de conectividad desde el router R3 a las intefaces G0/0 y S0/0/1, de R2.

Figura 19. Conexión IPv6 entre R3 y R2



Fuente. Elaboración propia.

3.2.3.6. Paso 6: Configurar S1.

La configuración del S1 incluye las siguientes tareas:

Desactivar la búsqueda DNS

```
Switch>enable
Switch#configure terminal
Switch(config)#no ip domain-lookup
```

Nombre del switch: *S1*

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

Contraseña de exec privilegiado cifrada: *class*

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

Contraseña de acceso a la consola: *cisco*

```
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
```

Contraseña de acceso Telnet y SSH: *cisco*

```
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: "*Se prohíbe el acceso no autorizado*.".

```
S1(config)#banner motd #Se prohibe el acceso no
autorizado.#
```

3.2.3.7. Paso 7: Configurar S3.

La configuración del S3 incluye las siguientes tareas:

Desactivar la búsqueda DNS

```
Switch>enable
Switch#configure terminal
Switch(config)#no ip domain-lookup
```

Nombre del switch: *S3*

```
Switch(config)#hostname S3
```

Contraseña de exec privilegiado cifrada: *class*

```
S3(config)#enable secret class
```

Contraseña de acceso a la consola: *cisco*

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

Contraseña de acceso Telnet y SSH: *cisco*

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

Cifrar las contraseñas de texto no cifrado

```
S3(config)#service password-encryption
```

Mensaje MOTD: "*Se prohíbe el acceso no autorizado*.".

```
S3(config)#banner motd #Se prohibe el acceso no
autorizado.#
```

3.2.3.8. Paso 8: Verificar la conectividad de la red

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

La Tabla 8 verifica metódicamente la conectividad con cada dispositivo de red.

Tabla 8. Verificación de la conectividad.

Desde	**A**	**Dirección IP**	**Resultados de ping**
R1	R2, S0/0/0	172.16.1.2	Correcto 5/5
R2	R3, S0/0/1	172.16.2.1	Correcto 5/5
PC de Internet	Gateway predeterminado	209.165.200.233	Correcto 5/5

Fuente. Elaboración propia.

En las Figuras 20, 21 y 22 se observan las imágenes de la consola CLI al realizar las comprobaciones descritas en la Tabla 7.

Figura 20. Ping entre el Router R1 y el Router R2.

```
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 = 1/8/20 ms
```

Fuente. Elaboración propia.

Figura 21. Ping entre el Router R2 y el Router R3.

```
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 = 1/12/18 ms
```

Fuente. Elaboración propia.

Figura 22. Ping entre el PC-A y el Gateway predeterminado.

```
C:\>ping 209.165.200.233

Pinging 209.165.200.233 with 32 bytes of data:

Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
```

Fuente. Elaboración propia.

3.2.4. Parte 3: Seguridad del switch, las VLAN y el routing entre VLAN.

3.2.4.1. Paso 1: Configurar S1.

La configuración del S1 incluye las siguientes tareas:

Crear la base de datos de VLAN. Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican.

```
S#configure terminal
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
```

```
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administracion
```

Asignar la dirección IP de administración. Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología.

```
S1(config-vlan)#vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
```

Asignar el gateway predeterminado. Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.

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

Forzar el enlace troncal en la interfaz F0/3. Utilizar la red VLAN 1 como VLAN nativa

```
S1(config)#interface f0/3
S1(config-if)#switchport mode trunk
<… texto omitido…>
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
```

Forzar el enlace troncal en la interfaz F0/5. Utilizar la red VLAN 1 como VLAN nativa.

```
S1(config)#interface f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
```

Configurar el resto de los puertos como puertos de acceso. Utilizar el comando *interface range*.

```
S1(config-if)#interface range f0/1-2 , f0/4 , f0/6-24 ,
g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#exit
```

Asignar F0/6 a la VLAN 21

```
S1(config)#interface f0/6
S1(config-if)#switchport access
```

```
S1(config-if)#switchport access vlan 21
```

Apagar todos los puertos sin usar.

```
S1(config-if)#interface range f0/1-2 , f0/4 , f0/7 - 24 ,
g0/1-2
S1(config-if-range)#shutdown
```

3.2.4.2. Paso 2: Configurar S3

La configuración del S3 incluye las siguientes tareas:

Crear la base de datos de VLAN. Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican.

```
S3(config)#enable
S3#configure terminal
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
```

Asignar la dirección IP de administración. Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología

```
S3(config)#interface vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
```

Asignar el gateway predeterminado. Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.

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

Forzar el enlace troncal en la interfaz F0/3 y utilizar la red VLAN 1 como VLAN nativa.

```
S3(config)#interface f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
```

Configurar el resto de los puertos como puertos de acceso. Utilizar el comando *interface range*.

```
S3(config)#interface f0/3
S3(config-if)#interface range f0/1-2, f0/4-24, fa0/6-24, g0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#exit
```

Asignar F0/18 a la VLAN 23

```
S3(config)#interface fa0/18
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 23
```

Apagar todos los puertos sin usar

```
S3(config-if)#interface range fa0/1-2, fa0/4-17, fa0/19-24, g0/1-2
S3(config-if-range)#shutdown
S3(config-if-range)#exit
```

3.2.4.3. Paso 3: Configurar R1.

Las tareas de configuración para R1 incluyen las siguientes:

Configurar la subinterfaz 802.1Q .21 en G0/1: Descripción: “LAN de Contabilidad”, asignar la VLAN 21 y asignar la primera dirección disponible a esta interfaz.

```
R1(config)#configure terminal
```

```
R1(config)#interface g0/1.21
R1(config-subif)#description LAN DE CONTABILIDAD
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#exit
```

Configurar la subinterfaz 802.1Q .23 en G0/1: Descripción: “LAN de Ingeniería”, asignar la VLAN 23 y asignar la primera dirección disponible a esta interfaz.

```
R1(config)#interface g0/1.23
R1(config-subif)#description LAN DE INGENIERIA
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#exit
```

Configurar la subinterfaz 802.1Q .99 en G0/1: Descripción: “LAN de Administración”, asignar la VLAN 99 y asignar la primera dirección disponible a esta interfaz.

```
R1(config)#interface g0/1.99
R1(config-subif)#description LAN DE ADMINISTRACION
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#exit
```

Activar la interfaz G0/1

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

3.2.4.4. Paso 4: Verificar la conectividad de la red.

La Tabla 9 muestra la verificación metódicamente la conectividad con cada dispositivo de red usando el comando ping entre los switches y R1.

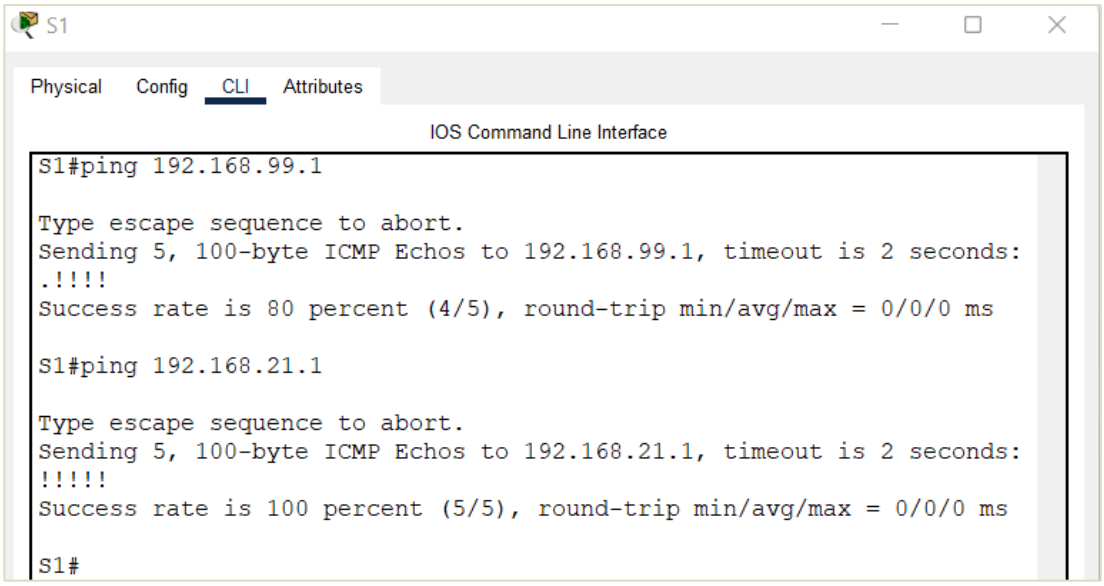
Tabla 9. Conectividad entre las VLAN.

Desde	Hasta	Dirección IP	Resultado de ping
S1	R1, dirección VLAN 99	192.168.99.1	Exitoso 5/5
S3	R1, dirección VLAN 99	192.168.99.1	Exitoso 5/5
S1	R1, dirección VLAN 21	192.168.21.1	Exitoso 5/5
S3	R1, dirección VLAN 23	192.168.23.1	Exitoso 5/5

Fuente. Elaboración propia.

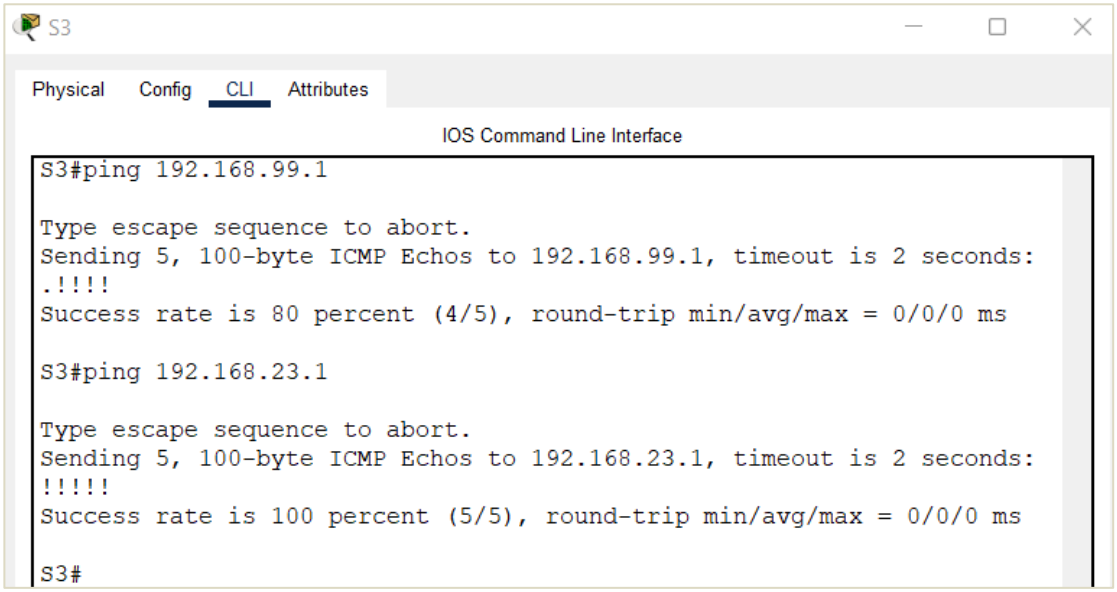
En las Figuras 23 y 24 se muestra la pantalla CLI durante la ejecución de los ping.

Figura 23. Conectividad entre S1 y R1, VLAN 99 y VLAN 21.



Fuente. Elaboración propia.

Figura 24. Conectividad entre S3 y R1, VLAN 99 y VLAN 23.



Fuente. Elaboración propia.

3.2.5. Parte 4: Configurar el protocolo de routing dinámico OSPF.

3.2.5.1. Paso 1: Configurar OSPF en el R1.

Según Cisco (2022), activar OSPF en el enrutador implica los siguientes dos pasos en el modo de configuración:

1. Habilitar OSPF mediante el comando `router ospf <process-id>`
2. Asignar áreas a las interfaces con el comando `network <network or IP address> <mask> <area-id>.`

Las tareas de configuración para R1 incluyen las siguientes:

Configurar la ID del OSPF área 0

```
R1>enable
R1#configure terminal
R1(config)#router ospf 1
```

Anunciar las redes conectadas directamente. Asignar todas las redes conectadas directamente.

> Para la máscara se usan bits comodines (wild cards) donde 0 es una coincidencia y 1 es un bit “no importa el contenido”. Por ejemplo, para la máscara de la VLAN 21, 255.255.255.0, se traduce como 0.0.0.255, indicando la coincidencia de los tres primeros bytes de tal red (Cisco, 2022).

```
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
```

Establecer todas las interfaces LAN como pasivas

```
R1(config-router)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
```

Desactivar la *sumarización* automática.

```
R1#configure terminal
R1(config)#router rip
R1(config-router)#no auto-summary
```

3.2.5.2. Paso 2: Configurar OSPF en el R2.

Configurar OSPF área 0

```
R2>enable
R2#configure terminal
R2(config)#router ospf 1
```

Anunciar las redes conectadas directamente (NOTA: omitir la red G0/0)

```
R2(config-router)#network 10.10.10.10 0.0.0.0 area 0
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
```

Establecer la interfaz LAN (loopback) como pasiva.

```
R2(config-router)#passive-interface loopback 0
```

Desactive la sumarización automática.

```
R2#configure terminal
R2(config)#router rip
R2(config-router)#no auto-summary
```

3.2.5.3. Paso 3: Configurar OSPFv3 en el R2.

La configuración del R3 incluye las siguientes tareas:

Configurar OSPF área 0

```
R3>enable
R3#configure terminal
R3(config)#router ospf 1
```

Anunciar redes IPv4 conectadas directamente

```
R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
R3(config-router)#network 192.168.4.0 0.0.0.255 area 0
R3(config-router)#network 192.168.5.0 0.0.0.255 area 0
R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
```

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

```
R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
```

Desactivar la *sumarización* automática.

```
R3#configure terminal
R3(config)#router rip
R3(config-router)#no auto-summary
```

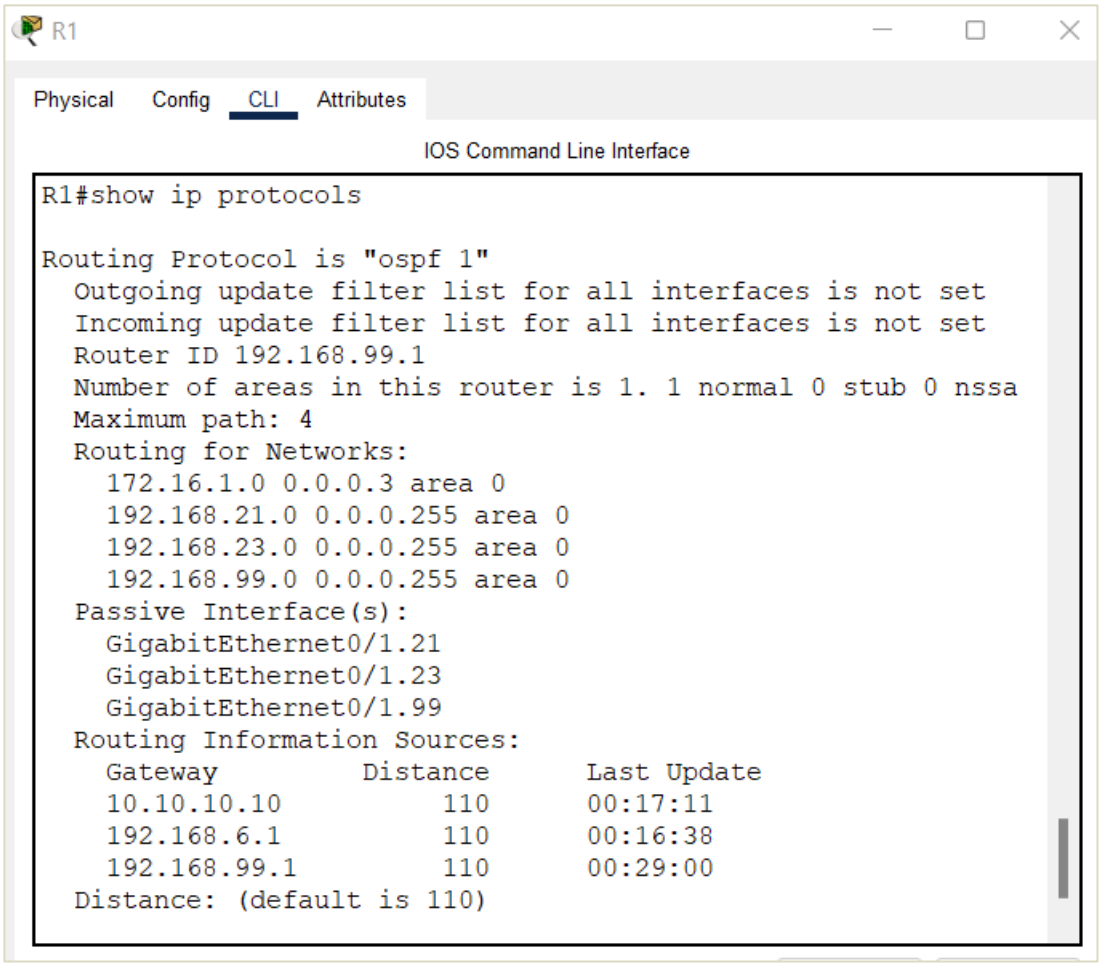
3.2.5.4. Paso 4: Verificar la información de OSPF.

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

a) ¿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?

Respuesta: Con el comando `show ip protocols`. En la Figura 25 se muestra como ejemplo, el router R1:

Figura 25. El comando show ip protocols en OSPF.

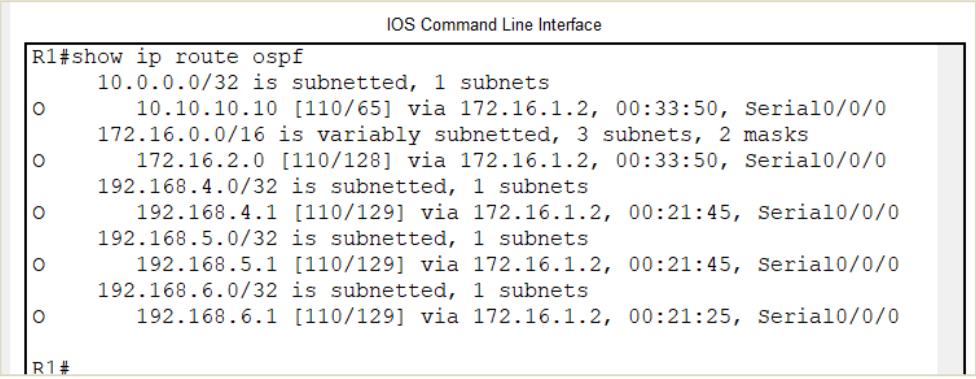


Fuente. Elaboración propia.

b) ¿Qué comando muestra solo las rutas OSPF?

Respuesta: El comando `show ip route ospf`. En la Figura 26 se puede ver el resultado de este comando en el CLI del router R1:

Figura 26. El comando show ip route ospf.

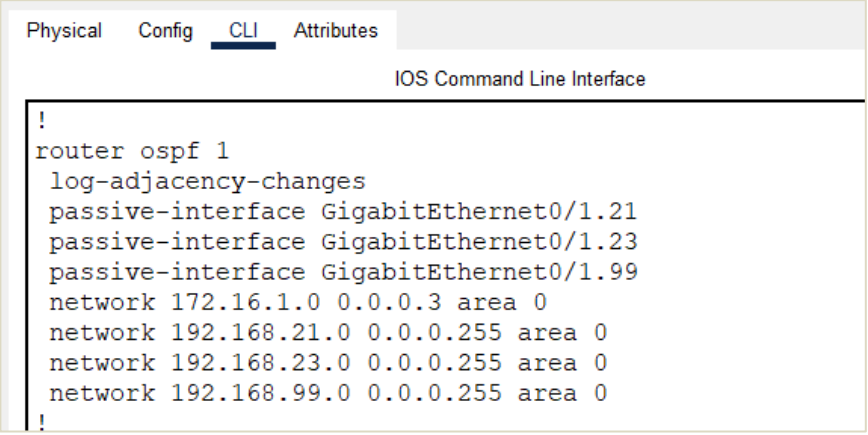


Fuente. Elaboración propia.

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

Respuesta. Esta información es accesible con el comando `show running-config`. La Figura 27 muestra el resultado en Router R1:

Figura 27. El comando comando show running-config en OSPF.



Fuente. Elaboración propia.

Por otra parte, el comando `show run | begin ospf`, también devuelve la misma información, como se muestra en la Figura 28.

Figura 28. El comando show run | begin ospf.

```
R1#Sh run | begin ospf
router ospf 1
 log-adjacency-changes
 passive-interface GigabitEthernet0/1.21
 passive-interface GigabitEthernet0/1.23
 passive-interface GigabitEthernet0/1.99
 network 172.16.1.0 0.0.0.3 area 0
 network 192.168.21.0 0.0.0.255 area 0
 network 192.168.23.0 0.0.0.255 area 0
 network 192.168.99.0 0.0.0.255 area 0
!
```

Fuente. Elaboración propia.

3.2.6. Parte 5: Implementar DHCP y NAT para IPv4.

3.2.6.1. Paso 1: Configurar R1 como servidor DHCP para las VLAN 21 y 23.

Para configurar el router R1 como servidor DHCP para las VLAN 21 y VLAN23 en primer lugar se debe reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas.

```
R1>enable

R1#configure terminal

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#configure terminal

R1(config)#ip dhcp excluded-address 192.168.23.1
192.168.23.20
```

Crear un pool de DHCP para la VLAN 21 con las siguientes especificaciones: Nombre: *ACCT*, servidor DNS: *10.10.10.10*, nombre de dominio: *ccna-sa.com* y establecer el gateway predeterminado.

```
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#ip domain-name ccna-sa.com
```

Crear un pool de DHCP para la VLAN 23 con las siguientes especificaciones: Nombre: *ENGNR*, servidor DNS: *10.10.10.10*, nombre de dominio: *ccna-sa.com* y establecer el gateway predeterminado.

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

3.2.6.2. 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 con la siguiente información: a) Nombre de usuario: *webuser*, b) contraseña: *cisco12345,* y c) nivel de privilegio: *15*.

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

Habilitar el servicio del servidor HTTP *

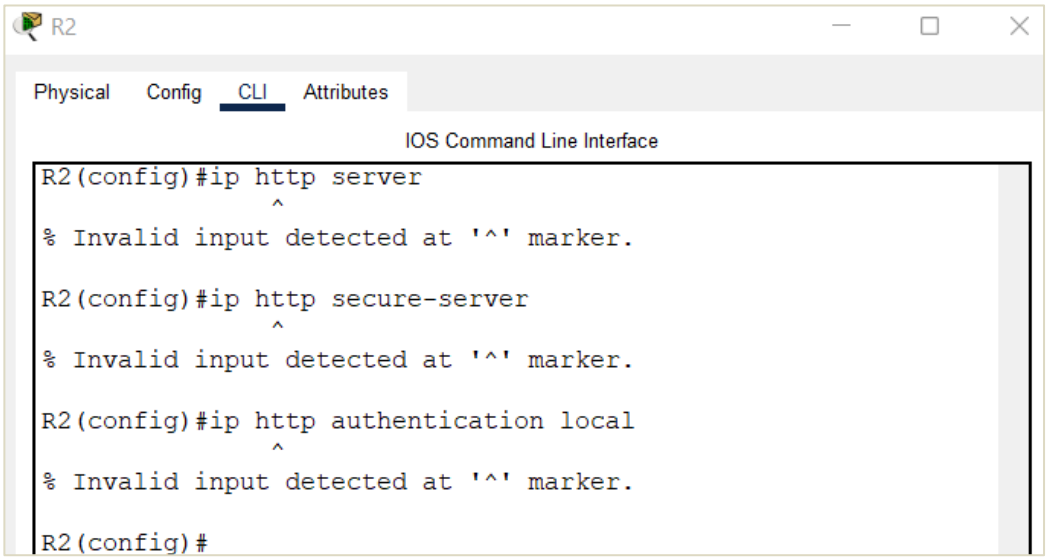
```
R2(config)#ip http server
R2(config)#ip http secure-server
```

Configurar el servidor HTTP para utilizar la base de datos local para la autenticación.*

```
R2(config)#ip http authentication local
```

* NOTA. Los comandos `ip http server`, `ip http secure-server` e `ip http authentication local` no son compatibles con la versión 8.1 de Packet Tracer, tal como se muestra en la Figura 29.

Figura 29. Comandos no soportados en PT 8.1.



Fuente. Elaboración propia.

Crear una NAT estática al servidor web con la dirección global interna: 209.165.200.229.

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

Asignar la interfaz interna y externa para la NAT estática.

```
R2(config)#interface GigabitEthernet 0/0
R2(config-if)#ip nat outside
R2(config)#interface GigabitEthernet 0/1
R2(config-if)#ip nat inside
```

Configurar la NAT dinámica dentro de una ACL privada con las siguientes especificaciones: a) Lista de acceso: *1*, b) permitir la traducción de las redes de

Contabilidad y de *Ingeniería* en el R1, y c) permitir la traducción de un resumen de las redes LAN (loopback) en el R3.

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

Defina el pool de direcciones IP públicas utilizables con las siguientes especificaciones: a) Nombre del conjunto: *INTERNET*, b) el conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228.

```
R2(config)#ip nat pool INTERNET 209.165.200.225
209.165.200.228 netmask 255.255.255.248
```

Definir la traducción de NAT dinámica

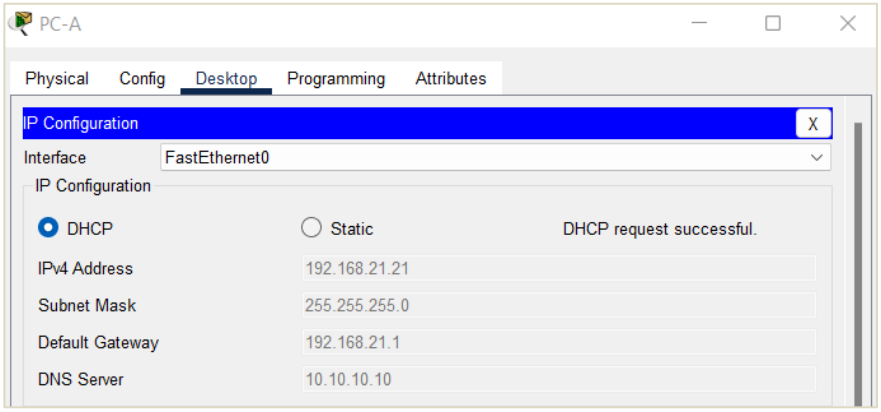
```
R2(config)#ip nat inside source list 1 pool INTERNET
```

3.2.6.3. 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.

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

Figura 30. Direccionamiento IPv4 por DHCP en la VLAN 21.



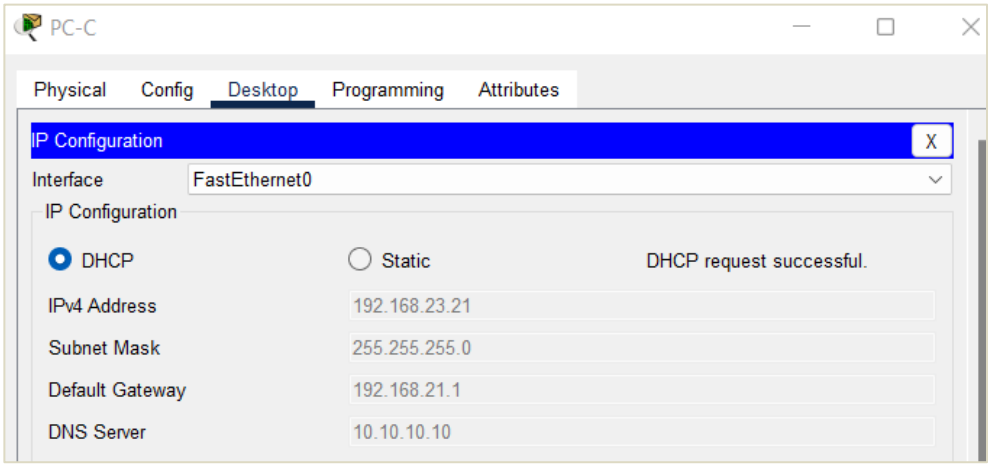
Fuente. Elaboración propia.

La Figura 30, ubicada en la siguiente página, muestra cómo el PC-A de la VLAN 21 adquiere de forma dinámica una dirección IPv4.

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

La Figura 31 muestra cómo el PC-C de la VLAN 23 adquiere de forma dinámica una dirección IPv4 desde el servidor DHCP.

Figura 31. Direccionamiento IPv4 por DHCP en la VLAN 23

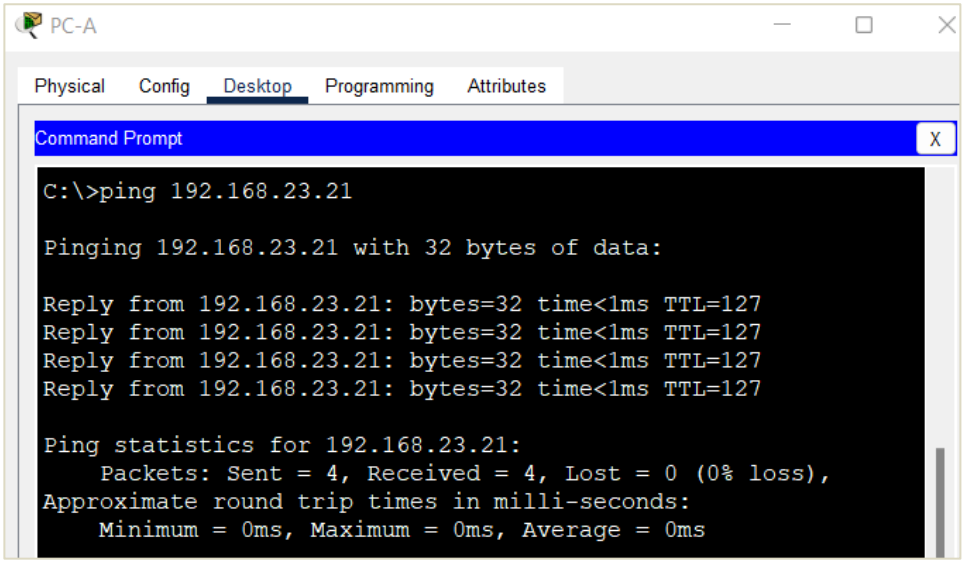


Fuente. Elaboración propia.

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

La Figura 32 muestra cómo el PC-A de la VLAN 21 es capaz de establecer comunicación con el PC-C de la VLAN 23.

Figura 32. Comunicación entre dos VLAN.

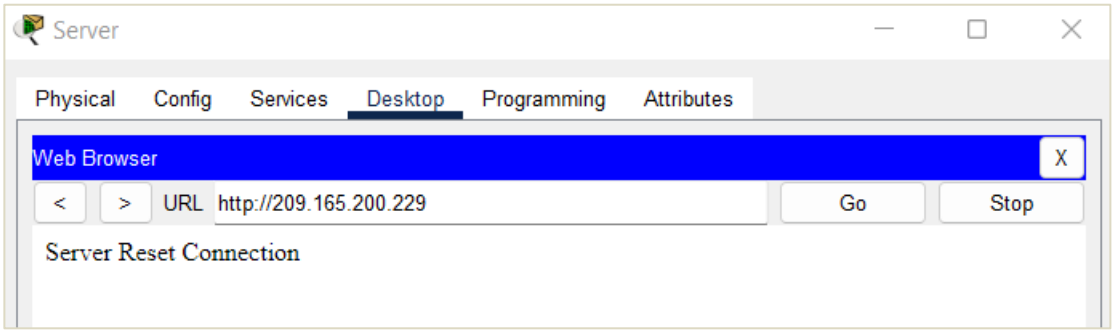


Fuente. Elaboración propia.

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

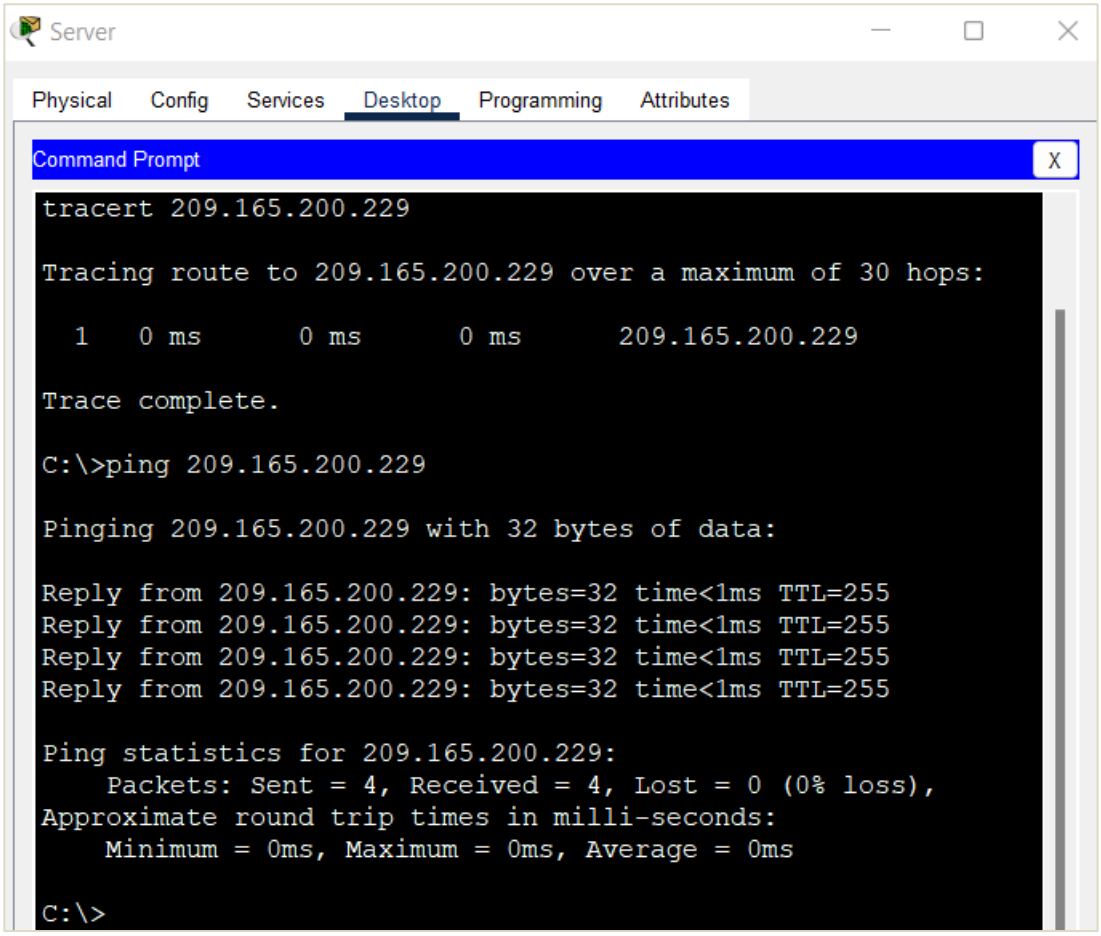
La Figura 33 muestra que existe comunicación con el servidor web. Si bien no se carga el archivo index.html la conexión es efectiva, tal como se muestra en la Figura 34 al utilizar los comandos `tracert` y `ping`.

Figura 33. Acceso al servidor web.



Fuente. Elaboración propia.

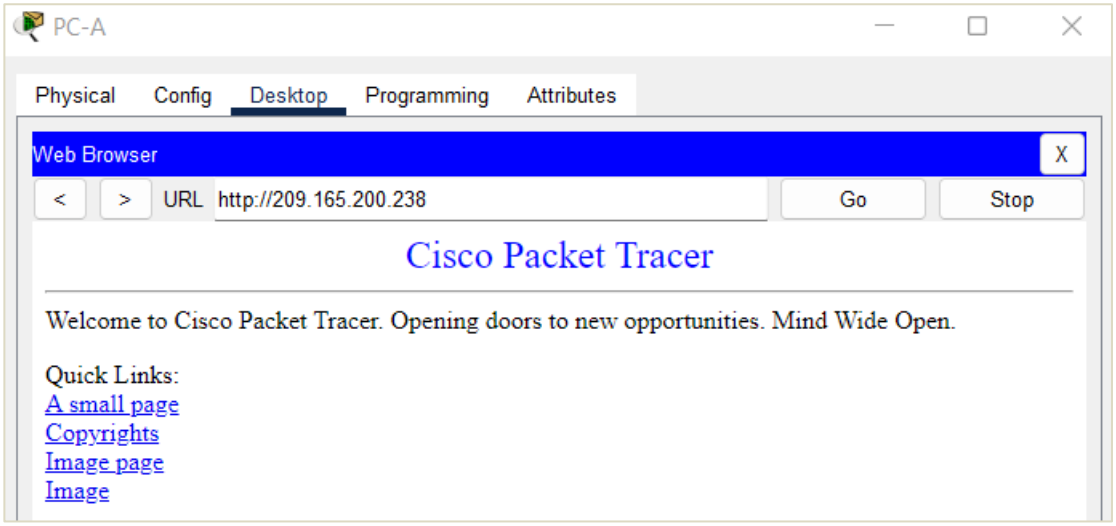
Figura 34. Uso de tracert y ping con el servidor web.



Fuente. Elaboración propia.

En la Figura 35 se muestra cómo el PC-A de la VLAN 21 tiene acceso al servidor ubicado en Internet, más allá del área local.

Figura 35. Acceso al servidor remoto desde un PC.



Fuente. Elaboración propia.

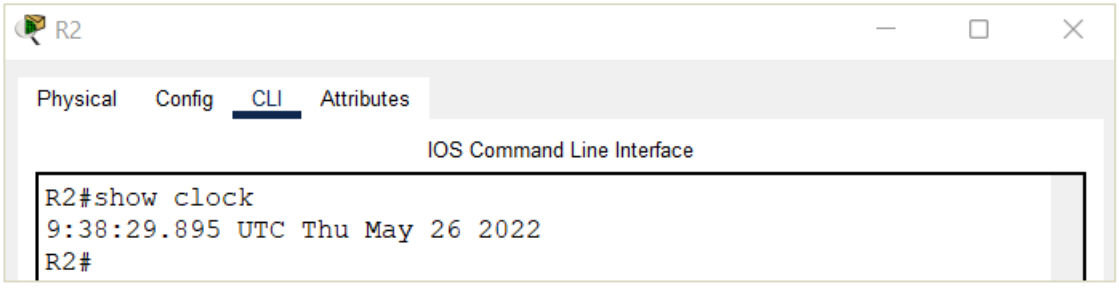
3.2.7. Parte 6: Configurar NTP.

Ajuste la fecha y hora en R2. *24 de mayo de 2022, 9 a. m.*

```
R2>enable
R2#clock set 09:38:00 26 May 2022
```

La Figura 36 muestra la hora configurada en el router R2.

Figura 36. Configuración de la hora y fecha en NTP.



Fuente. Elaboración propia.

Configure R2 como un maestro NTP. Nivel de estrato: *5*

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

Configurar R1 como un cliente NTP. Servidor: *R2*

```
R1>enable
R1#configure terminal
R1(config)#ntp server 172.16.1.2
```

Configure R1 para actualizaciones de calendario periódicas con hora NTP.

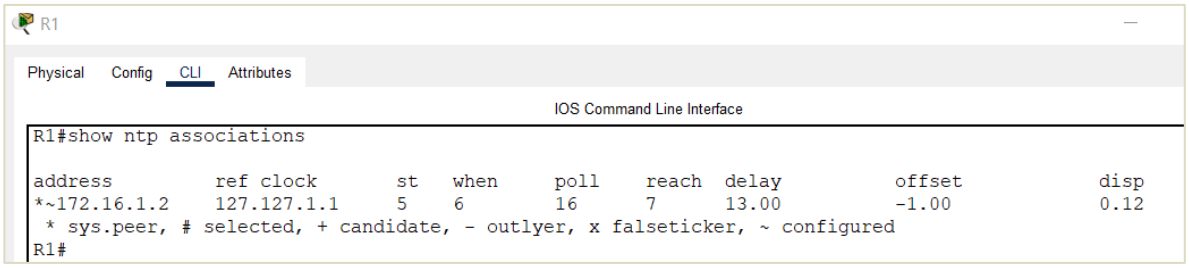
```
R1#configure terminal
R1(config)#ntp update-calendar
```

Verifique la configuración de NTP en R1.

```
R1#show ntp associations
```

La Figura 37 muestra la configuración de Network Time Protocol (NTP) a la que accede el router R1. Tal como se puede observar, el router se sincroniza de forma automática con el router R2.

Figura 37. Configuración de NTP en R1



Fuente. Elaboración propia.

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

A continuación se crean y comprueban las lista de acceso ACL.

3.2.8.1. 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. Nombre de la ACL: *ADMIN-MGT*

```
R2#configure terminal
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 15
R2(config-line)#access-class ADMIN-MGT in
```

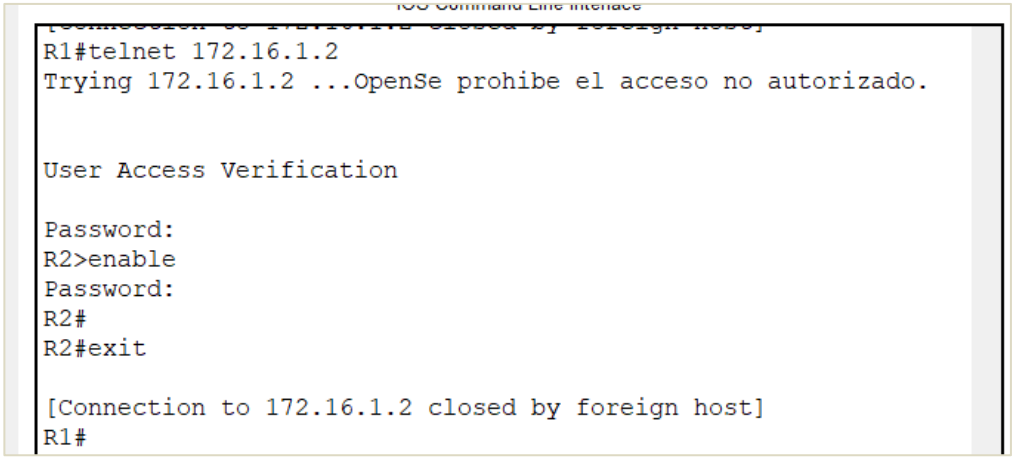
Permitir acceso por Telnet a las líneas de VTY.

```
R2(config-line)#transport input telnet
```

Verificar que la ACL funcione como se espera.

Conexión desde R1. La Figura 38 muestra cómo el acceso vía Telnet a R2 es posible. El proceso de verificación es total y se puede acceder al nivel EXEC privilegiado de forma remota.

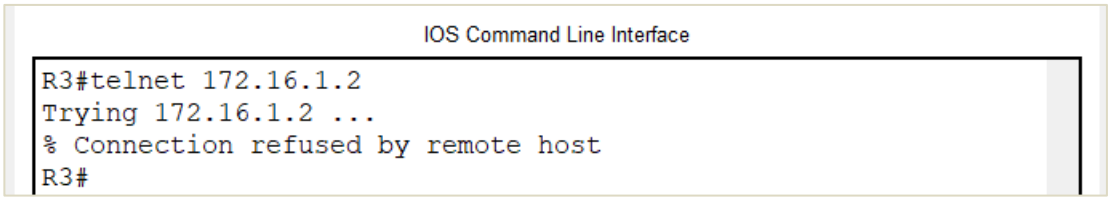
Figura 38. ACL en Router R1.



Fuente. Elaboración propia.

Desde R3. La Figura 39 muestra cómo el router R2 bloquea el acceso vía Telnet a los paquetes provenientes del router R3. Esto se debe a que no está conectado en la interfaz s0/0/0, que es la que tiene la dirección 172.16.1.1 definida en la ACL *ADMIN-MGT.*

Figura 39. ACL en Router R3.



Fuente. Elaboración propia.

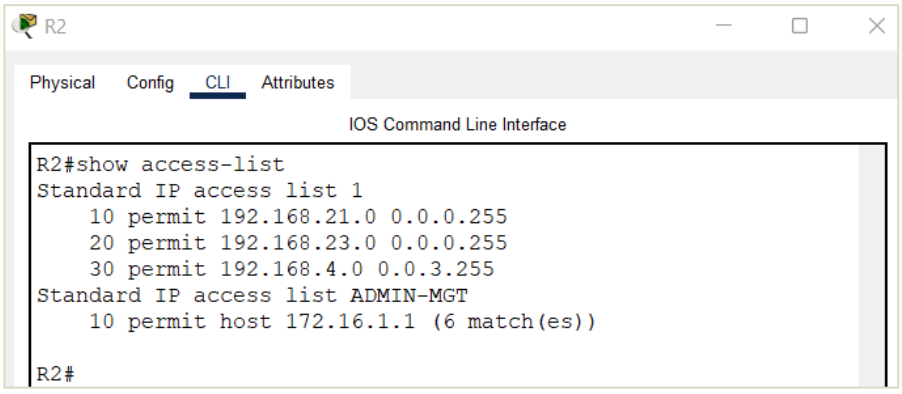
3.2.8.2. Paso 2: Uso de comandos para gestionar ACL

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

a) Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció.

```
R2#show access-list
```

Figura 40. ACL. Comando show access-list en R2.



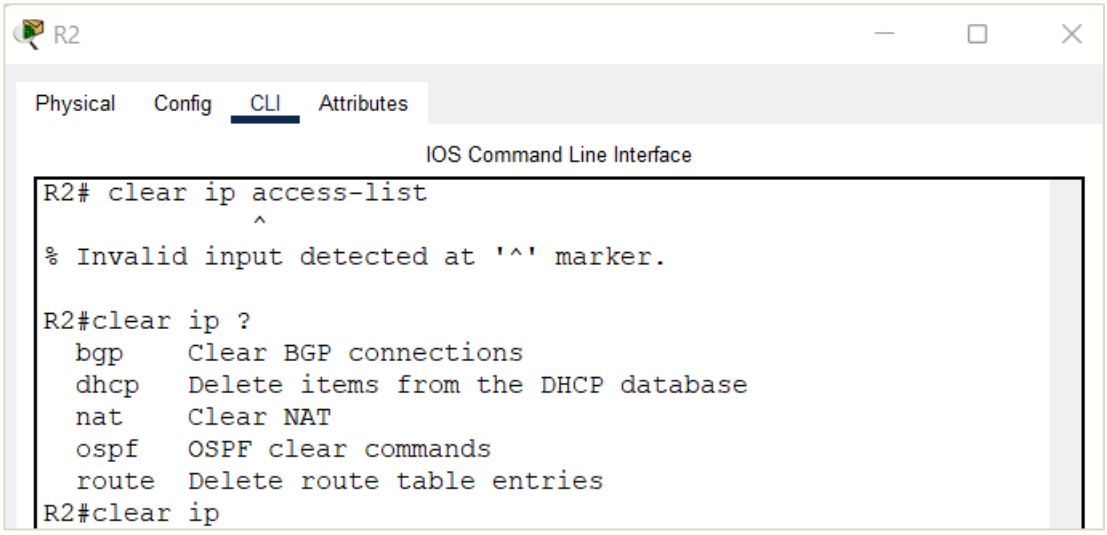
Fuente. Elaboración propia.

La Figura 40 muestra el resultado obtenido al utilizar este comando.

b) Restablecer los contadores de una lista de acceso.*

> * NOTA. De acuerdo con la documentación de Cisco (Cisco, 2021) el comando es `clear ip access-list counters`, que se ejecuta en modo EXEC privilegiado, sin embargo, tal como se muestra en la Figura en Packet Tracer 8.1 no es posible usarlo tal como se muestra en la Figura 41.

Figura 41. El comando clear ip access-list counters en Packet Tracer.



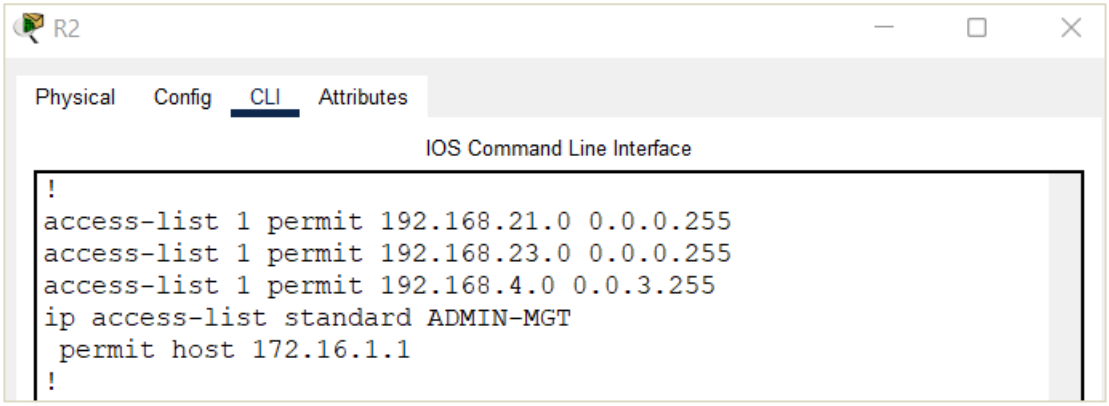
Fuente. Elaboración propia.

c) ¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?

```
R2#show running-config
```

La Figura 42 muestra las listas ACL configuradas en el router R2.

Figura 42. ACL. Comando show running-config en R2.



Fuente. Elaboración propia.

d) ¿Con qué comando se muestran las traducciones NAT?

```
R2#show ip nat translations
```

La Figura 43 muestra la pantalla de CLI con el comando `show ip nat translations` antes de hacer ping desde PC-A y PC-C al servidor de internet 209.165.200.238:

Figura 43. NAT. Uso del comando show ip nat translations.

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

R2#
```

Fuente. Elaboración propia.

La Figura 44 muestra de nuevo el uso del comando `show ip nat translations` después de hacer ping desde PC-A y PC-C al servidor de internet 209.165.200.238. En seguida se llena la tabla y la utilidad del comando se hace evidente.

Figura 44. NAT. El comando ip nat translations con actividad en la red.

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

R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.225:1 192.168.21.21:1    209.165.200.238:1  209.165.200.238:1
icmp 209.165.200.225:2 192.168.21.21:2    209.165.200.238:2  209.165.200.238:2
icmp 209.165.200.225:3 192.168.21.21:3    209.165.200.238:3  209.165.200.238:3
icmp 209.165.200.225:4 192.168.21.21:4    209.165.200.238:4  209.165.200.238:4
icmp 209.165.200.226:1 192.168.21.22:1    209.165.200.238:1  209.165.200.238:1
icmp 209.165.200.226:2 192.168.21.22:2    209.165.200.238:2  209.165.200.238:2
icmp 209.165.200.226:3 192.168.21.22:3    209.165.200.238:3  209.165.200.238:3
icmp 209.165.200.226:4 192.168.21.22:4    209.165.200.238:4  209.165.200.238:4
---  209.165.200.229   10.10.10.10        ---                ---

R2#
```

Fuente. Elaboración propia.

e. ¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?

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

La Figura 45 muestra cómo el comando `ip nat translation *` borra el contenido de la tabla de traducciones NAT dinámicas que se generó al hacer ping en el paso anterior.

*Figura 45. Borrado de las traducciones NAT con ip nat translation *.*

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

R2#
```

Fuente. Elaboración propia.

4. CONCLUSIONES

Se realiza la configuración de la topología del escenario 1, la cual permite identificar aspectos de configuración básica de enrutamiento y gestión de la seguridad en dispositivos de red Cisco. En particular, por una parte, se configuran las interfaces de red de acuerdo con el esquema VLSM diseñado acorde al tamaño de cada una de las subredes LAN; por otra parte, se configuran el acceso seguro a la línea de consola y a las líneas VTY, la conexión SSH, el encriptado simple y por RSA, los temporizadores de cierre de sesión por inactividad y el filtrado ante ataques de fuerza bruta.

Se realiza la configuración de la topología del escenario 2, la cual permite identificar los aspectos básicos de configuración de acceso seguro en las líneas de consola y VTY, direccionamiento en los protocolos IPv4 e IPv6, redes VLAN, enrutamiento estático y OSPF, servidor DHCP, listas de acceso ACL, traducción de direcciones NAT y sincronización NTP.

El conjunto de las configuraciones realizadas en los escenarios 1 y 2 en la herramienta de simulación *Packet Tracer* se ajusta a los requerimientos básicos de acceso LAN/WAN que pueden tener muchas empresas pequeñas en cuanto a explotación de las direcciones disponibles, escalabilidad, políticas de enrutamiento, y seguridad en los dispositivos intermedios y da respuesta a las especificaciones teóricas planteadas en los enunciados de cada escenario.

BIBLIOGRAFÍA

Cisco (s.f.) *Introduction to Networks v7.0 (ITN).* https://lms.netacad.com/course/view.php?id=1189231

Cisco (2021) *clear ip access-list counters*. Cisco. https://www.cisco.com/en/US/docs/ios/security/command/reference/sec_c2.pdf

Cisco (2022, mar. 16) *OSPF Design Guide. Document ID:7039*. OSPF Design Guide - Cisco

Lammle, T. (2013) CCNA. Routing and Switching Study Guide. https://www.academia.edu/22906018/CCNA_Routing_and_Switching_Study_Guide_Todd_Lammle

Odom, W. (2016) *CCENT/CCNA ICND1 100-105 Official Cert Guide. CISCO*. https://usermanual.wiki/Document/CiscoICND1CCENTCCNAICND1100105OfficialCertGuide100105.1378544952/view

UNAD (s.f.) *Diplomado Paso 6 – 10* [archivo comprimido]. UNAD. https://campus129.unad.edu.co/ecbti105/pluginfile.php/2086/mod_folder/content/0/Diplomado%20Paso%206%20-%2010.rar?forcedownload=1

UNAD (s.f.) *Guía de actividades - Unidad 5 - Paso 6 - Entrega Avance Documento Final*. UNAD. 203092A_1142: Guía de actividades y rúbrica de evaluación - Unidad 5 - Paso 6 - Entrega Avance Documento Final (unad.edu.co)