DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNA

ESTEFANIA ISABEL MONTENEGRO ROLON

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNA

ESTEFANIA ISABEL MONTENEGRO ROLON

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

ASESOR:
ING. JAVIER RICARDO VASQUEZ ROJAS

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

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

SANTA MARTA, 24 de noviembre de 2021

AGRADECIMIENTOS

Primero que todo dar gracias a Dios, porque sin él nada hubiese sido posible, gracias a él por darme la oportunidad de llegar a este punto, gracias por esas hermosas personas que me han sido leal y me han guiado en este gran camino de la vida, esas personas que han sido un gran apoyo para subir este escalón, a mi madre por su apoyo incondicional, a mi hijo por ser el mayor motivo para salir adelante, a mi esposo por su comprensión y apoyo total, a mi padre que siempre ha sido esa voz de aliento para “*romper paradigmas*”, a cada una de mis hermanas, y a la Universidad Nacional Abierta y a Distancia, que por su excelente servicio y su gran organización han sido participe en mi crecimiento personal y profesional.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

GLOSARIO

BROADCAST: Método por el cual se envía un paquete de un host a todos los hosts de la red. Existe un direccionamiento particular cuando los bits de la dirección de host están todos en una llamada a la dirección de broadcast, o de difusión.

DIRECCIONAMIENTO: Permite identificar a cada ordenador de forma única en toda la red por ejemplo un número de teléfono en formato internacional permite identificar a ese teléfono de forma única en todo el mundo

LAN: Una red de área local o LAN (Local Area Network) es una red limitada a un área geográfica limitada, no muy grande (una casa, un aula, un edificio, etc.).
Los elementos de esta red pueden estar interconectados por cableado o sin cables (wireless) por medio de ondas electromagnéticas, como ocurre en las redes WIFI.

ROUTERS: Son los dispositivos de interconexión que permiten que cada paquete enviado llegue a su destino siguiendo el camino o la ruta más factible.

TOPOLOGÍA: Hace referencia al aspecto físico y lógico de la red. La topología física depende de la distribución y conducción física de los elementos de la red.
La topología lógica depende de cómo circular la información por la red.

VLAN - Virtual Local Area Network o Red de Área Local Virtual, organiza a los miembros de una LAN que tienen características comunes (su propia subred IP, acceso a determinados sitios, etc).
Lo que hace es segmentar los dominios del broadcast como si se tratara de un switches diferentes.

SWITCH (conmutador): Este dispositivo de interconexión es capaz de identificar los equipos alcanzables a través de cada uno de sus puertos.
Esto permite que la información dirigida a un equipo se dirija únicamente desde el puerto origen al puerto que permite alcanzar el equipo destino.
Es el dispositivo usual para unir equipos en una red LAN.

GATEWAY - PUERTA DE ENLACE: La puerta de enlace es la dirección IP del equipo por el que se sale de la LAN hacia otra red (normalmente a Internet).
Suele ser la dirección IP de un router.
Dicha dirección debe pertenecer a la misma subred del equipo

COMANDO PING: Sirve para enviar mensajes, llamados paquetes, a una dirección concreta.
Ping se utiliza para comprobar que dos equipos se pueden comunicar por la LAN.
Si el destinatario contesta podemos asegurar que hay comunicación con él.

RESUMEN

El diplomado de profundización CISCO (diseño e implementación de soluciones integradas LAN / WAN), aborda diferentes temáticas, en los que presentan conceptos básicos de redes, presentan diversos laboratorios que ayudaron el desarrollo de laboratorio práctico por intermedio de la herramienta Packet Tracer.
Cada una de las unidades abordadas en el diplomado de profundización CISCO CCNA1, ayudaron al desarrollo de los dos escenarios, donde se construyeron redes LAN simples, configuraciones básicas y de seguridad para routers y switches, configurar los hosts y verificar la conectividad entre los equipos.

Palabras claves: CISCO, LAN, Redes, Packet Tracer, Routers, Switches.

ABSTRACT

The CISCO in-depth diploma (design and implementation of integrated LAN / WAN solutions), addresses different topics, in which they present basic concepts of networks, present various laboratories that helped the development of a practical laboratory through the Packet Tracer tool.
Each of the units addressed in the CISCO CCNA1 in-depth diploma, helped the development of the two scenarios, where simple LAN networks, basic and security configurations for routers and switches, were built, hosts were configured, and connectivity between equipment was verified.

Keywords: CISCO, LAN, Networks, Packet Tracer, Routers, Switches.Keywords: CISCO, LAN, Networks, Packet Tracer, Routers, Switches.

INTRODUCCION

El diplomado de profundización Cisco, ha sido muy importante y ayuda significativamente al crecimiento profesional ingeniero de sistemas, ya que gracias a este es posible poner práctica los conocimientos adquiridos a lo largo de carrera, con cada uno de los laboratorios propuestos se presentaron desafíos muy parecidos al entorno real.

Gracias al desarrollo de los módulos Network Fundamentals (CCNA1 R&S) y Routing and Switching Fundamentals (CCNA2 R&S) , fue posible el desarrollo de la prueba de habilidades prácticas, la cual consiste en el desarrollo de dos escenarios, en un primer escenario se configuran los dispositivos de una red pequeña, lo que incluye un router, un switch y dos PC, se diseña el esquema de direccionamiento IPv4 para 2 redes LAN, una que consta de 100 host y otra de 50 host, tanto al router como al switch se aplica la configuración de aspectos básicos y se configura su seguridad, teniendo encuentra que deben administrarse de forma segura.

En un segundo escenario se configura una red también pequeña que comprende tres routers, dos switches , dos PC's y un servidor, se maneja 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.

En este documento de PRUEBA DE HABILIDADES PRÁCTICAS se conocerán los diferentes comandos utilizados, tanto para la configuración como para la verificación del funcionamiento de la red.

DESARROLLO

ESCENARIO 1

Figura 1. Topología propuesta

Fuente: Prueba de habilidades CISCO CCNAII

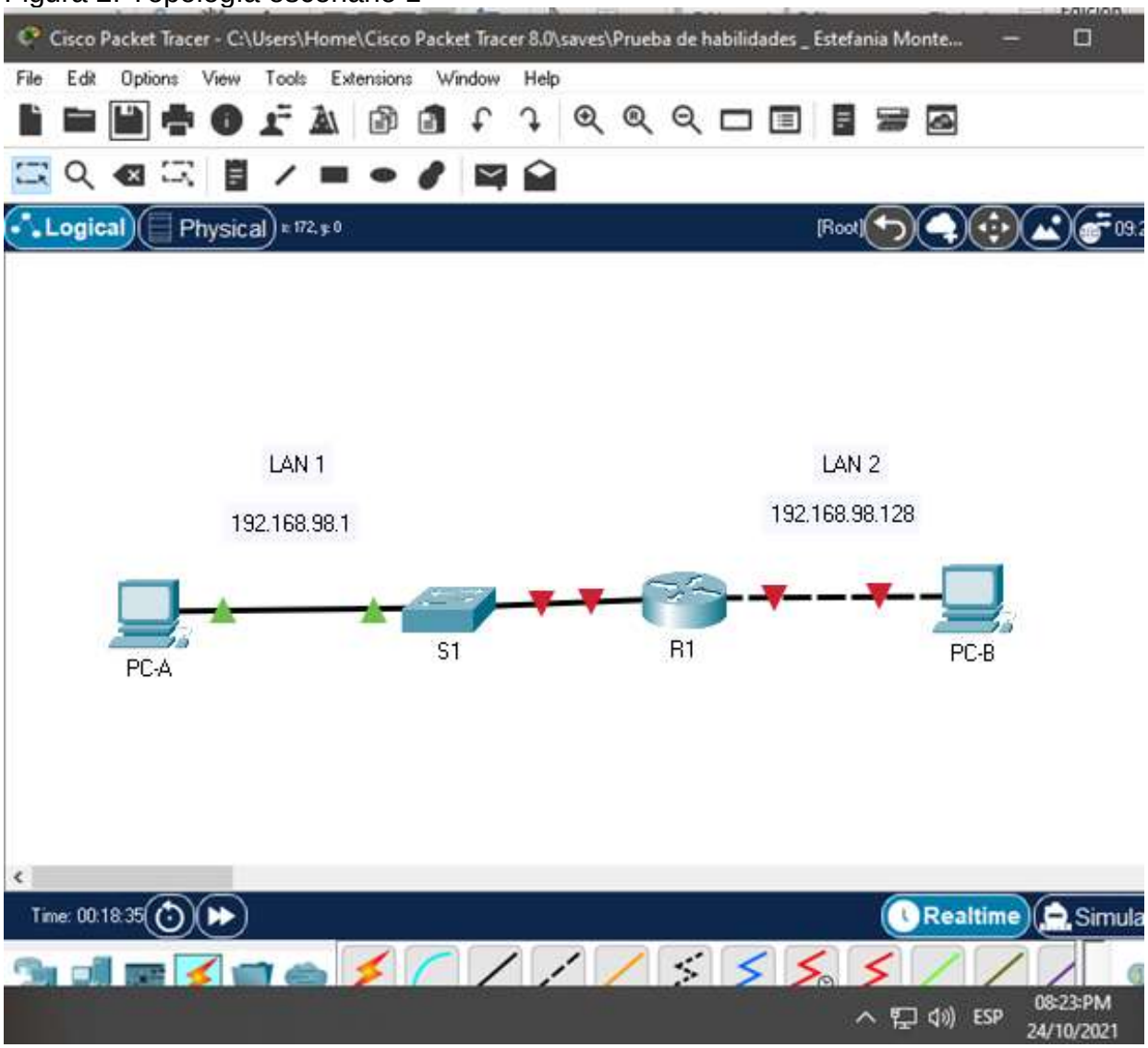
En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos, diseñar el esquema de direccionamiento IPv4 para las LAN propuestas. El router y el switch también deben administrarse de forma segura.

Objetivos
Parte 1: Construir en el simulador la Red
Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2
Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta.
Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1
Parte 5: Configurar los hosts y verificar la conectividad entre los equipos

Aspectos básicos/situación:
En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el swich S1, y los PCs.
Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

Parte 1: construya la red
En el simulador construya la red de acuerdo con la topología lógica que se plantea en la figura 1, cablee conforme se indica en la topología, y conecte los equipos de cómputo.

Figura 2. Topología escenario 1



Fuente: Propia.

Parte 2: El esquema de direccionamiento IP

Desarrolle el esquema de direccionamiento IP.

Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento.

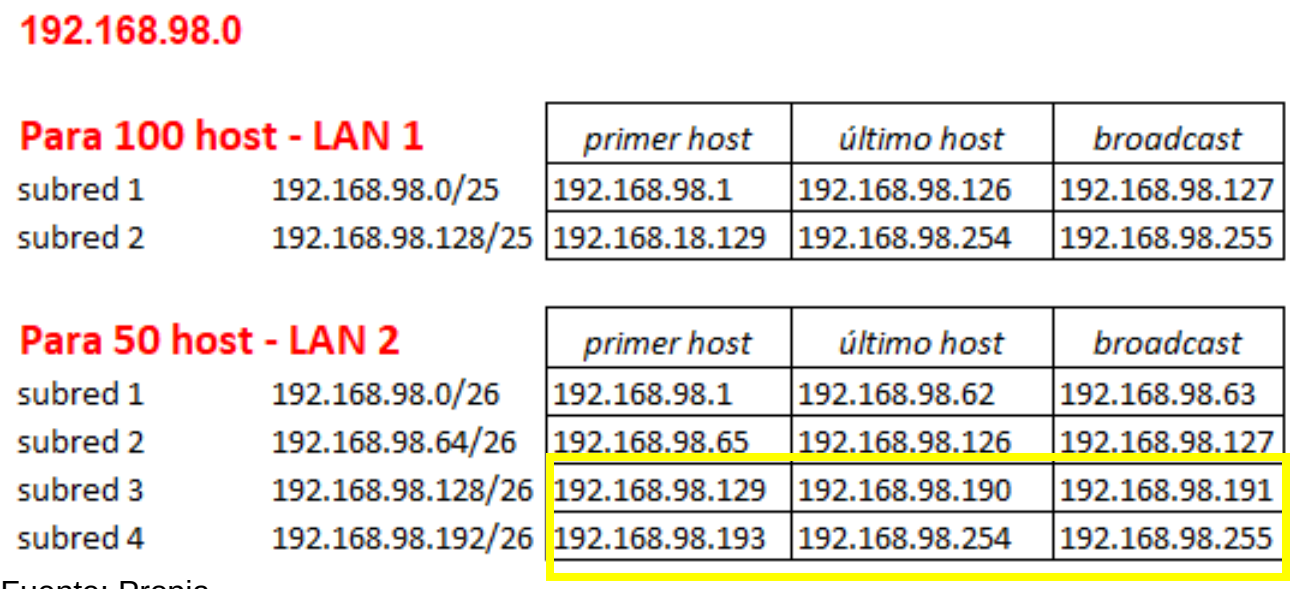
Cada estudiante tomará el direccionamiento 192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula.

Tabla 1. Requerimiento de escenario 1

Item	Requerimiento
Dirección de Red	192.168.98.0
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN 2	50
R1 G0/0/1	192.168.98.1
R1 G0/0/0	192.168.98.129
S1 SVI	192.168.98.2
PC-A	192.168.98.126
PC-B	192.168.98.190

Fuente: Propia.

Figura 3. Subnetting LAN 1 Y LAN 2



Fuente: Propia.

Parte 3: Configuración de aspectos básicos

Los dispositivos de red (S1 y R1) se configuran mediante conexión de consola.

Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 2. Configuración R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router>**enable** Router# **configure terminal** Router(config)#**no ip domain-lookup**
Nombre del router	Router(config)#**hostname R1**
Nombre de dominio	R1(config)#**ip domain-name ccna-lab.com**
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#**enable secret cisco**
Contraseña de acceso a la consola	R1(config)#**line console 0** R1(config-line)#**password cisco** R1(config-line)#**login** R1(config-line)#**exit**
Establecer la longitud mínima para las contraseñas	R1(config)#**security passwords min-length 10**
Crear un usuario administrativo en la base de datos local	R1(config)#aaa new-model R1(config)#aaa authentication login default local R1(config)#username admin privilege 10 password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#**line vty 0 15** R1(config-line)#**login local** R1(config-line)#**exit**
Configurar VTY solo aceptando SSH	R1(config)#**line vty 0 15** R1(config-line)#**transport input ssh** R1(config-line)#**login local** R1(config-line)#**exit**
Cifrar las contraseñas de texto no cifrado	R1(config)#**service password-encryption**
Configure un MOTD Banner	R1(config)#**banner motd # Acceso restringido #**
Configurar interfaz G0/0/1	R1(config)#**interface G0/0/1** R1(config-if)#**ip address 192.168.98.1 255.255.255.128** R1(config-if)#**no shutdown** R1(config-if)#**exit**
Configurar interfaz G0/0/0	R1(config)#**interface G0/0/0** R1(config-subif)#**ip address** 192.168.98.129 **255.255.255.192** R1(config-if)#**no shutdown** R1(config-if)#**exit**

Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa
	The name for the keys will be: R1.ccna-lab.com
	Choose the size of the key modulus in the range of 360 to 2048 for your
	  General Purpose Keys. Choosing a key modulus greater than 512 may take
	  a few minutes.
	
	How many bits in the modulus [512]: 1024
	% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
	R1(config)#**do wr**
	R1(config)#**exit**

Fuente: Propia.

Las tareas de configuración de **S1** incluyen lo siguiente:

Tabla 3. Configuración de **S1**

Tarea	Especificación
Desactivar la búsqueda DNS.	**Switch>** **Switch>enable** **Switch#configure terminal** **Switch(config)#no ip domain lookup**
Nombre del switch	Switch(config)#**hostname S1**
Nombre de dominio	S1(config)#**ip domain-name ccna-lab.com**
Contraseña cifrada para el modo EXEC privilegiado	**S1(config)#enable secret cisco**
Contraseña de acceso a la consola	S1(config)#**line console 0** S1(config-line)#**password cisco** S1(config-line)#**login** S1(config-line)#**exit**
Crear un usuario administrativo en la base de datos local	S1#conf t S1(config)#aaa new-model S1(config)#aaa authentication login default local S1(config)#username **admin** privilege 10 password **admin1pass** **Otra forma seria:** S1(config)#username admin privilege 10 password admin1pass

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	**S1(config)#line vty 0 15** **S1(config-line)#login local** **S1(config-line)#exit**
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	**Switch#configure terminal** **S1(config)#line vty 0 15** **S1(config-line)#login local** **S1(config-line)#exit**
Cifrar las contraseñas de texto no cifrado	S1(config)#**service password-encryption**
Configurar un MOTD Banner	**Switch#configure terminal** **S1(config)#banner motd # Acceso restringido #**
Generar una clave de cifrado RSA	**Switch#configure terminal** S1(config)#crypto key generate rsa The name for the keys will be: S1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] S1(config)#do wr *Mar 1 3:30:33.882: %SSH-5-ENABLED: SSH 1.99 has been enabled Building configuration... [OK]
Configurar la interfaz de administración (SVI)	S1(config)#**interface Vlan4**
Configuración del Gateway predeterminado	**Switch#configure terminal** S1(config)#**ip default-gateway** 192.168.98.2 S1(config)#**do wr** Building configuration... [OK]

Fuente: Propia.

Paso 2. Configurar los equipos.

Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all.**

Tabla 4. Configuración PC-A

PC-A Network Configuration	
Descripción	PC-A
Dirección física	0001.C9C9.8429
Dirección IP	192.168.98.126
Máscara de subred	255.255.255.128
Gateway determinado	192.168.98.1

Fuente: Propia.

Tabla 5. Configuración PC-B

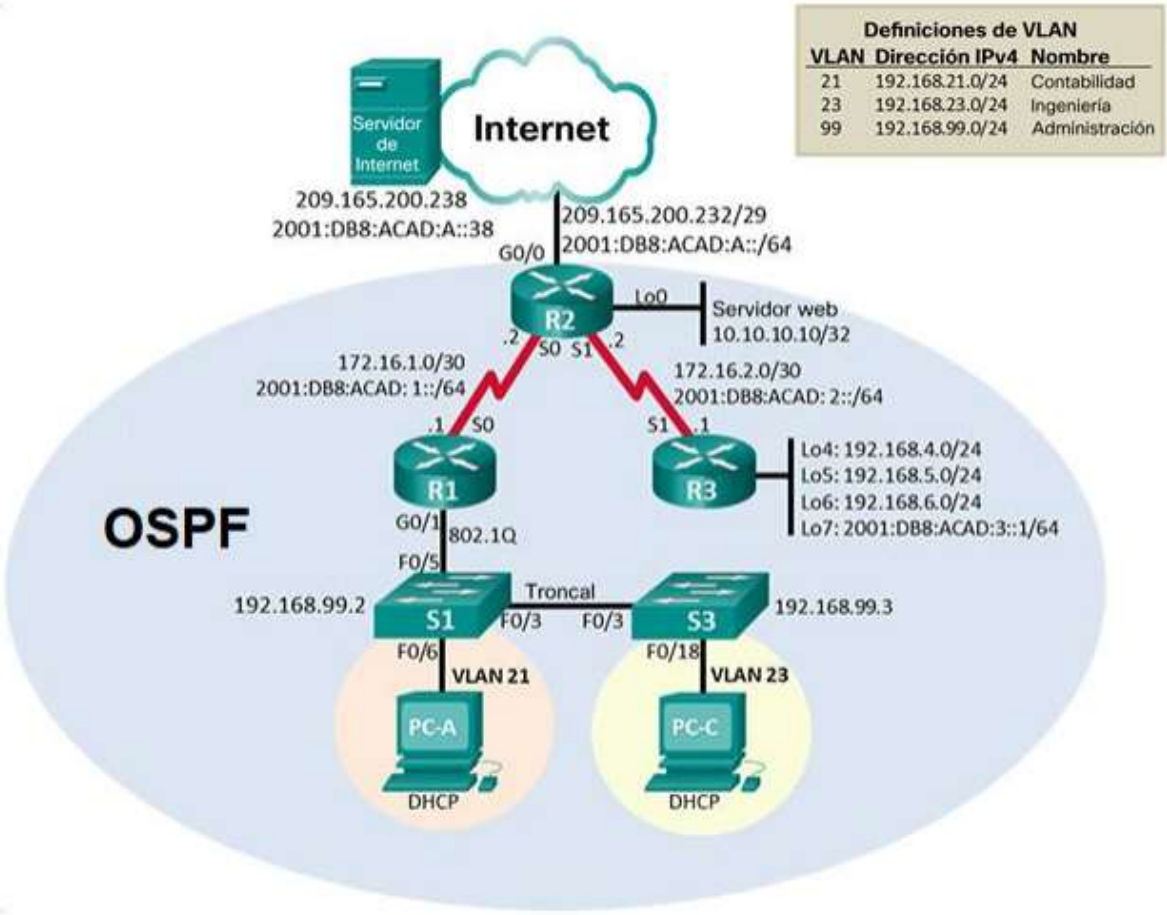
PC-B Network Configuration	
Descripción	PC-B
Dirección física	0001.C70B.AEA1
Dirección IP	192.168.98.198
Máscara de subred	255.255.255.192
Gateway determinado	192.168.98.129

Fuente: Propia.

ESCENARIO 2

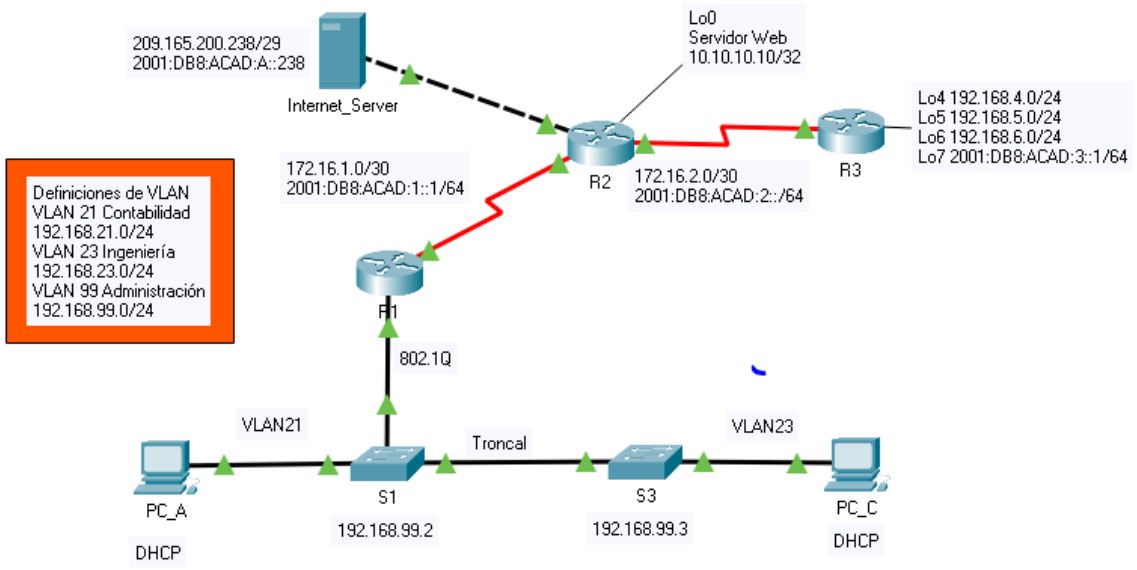
Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de 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.

Figura 4. Topología propuesta



Fuente: Prueba de habilidades CCNA II

Figura 5. Topología escenario 1



Fuente: Propia.

Parte 1: inicializar dispositivos.

Paso 1: Inicializar y volver a cargar los routers y los switches.
Elimine las configuraciones de inicio y vuelva a cargar los dispositivos. Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

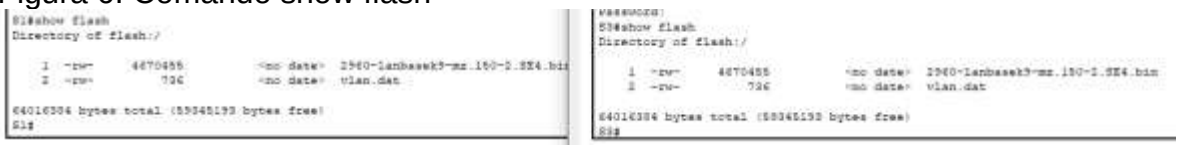
Tabla 6. Inicializar y volver a cargar los routers y switches

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Comando ejecutado en **R1, R2 y R3** Router>enable 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
Volver a cargar todos los routers	Comando ejecutado en **R1, R2 y R3** Router# **reload** Proceed with reload? [confirm] [**Enter**]

Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Comando ejecutado en **S1 y S3** Switch#**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
Volver a cargar ambos switches	Comando ejecutado en **S1 y S3** Switch# **reload** Proceed with reload? [confirm] [**Enter**]
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Comando ejecutado en **S1 y S3** Switch#**show flash**

Fuente: Propia.

Figura 6. Comando show flash



Fuente: 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 7. Configuración del servidor de Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::238/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Fuente: Propia.

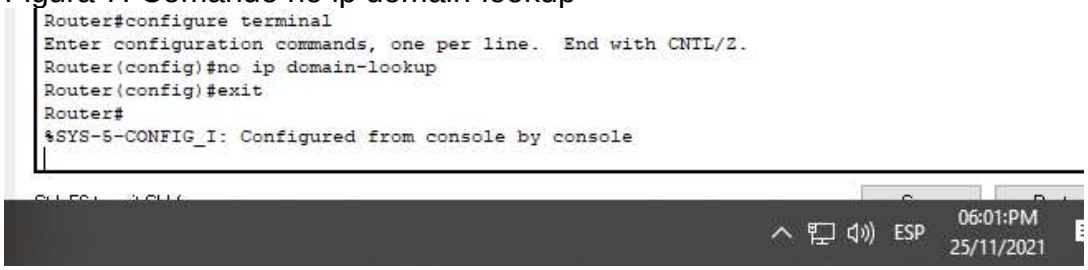
Paso 2: Configurar R1
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 8. Configuración R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>**enable** Router#**configure terminal** Router(config)#**no ip domain-lookup**
Nombre del router	Router(config)#**hostname R1**
Contraseña de exec privilegiado cifrada	R1(config)# **enable secret class**
Contraseña de acceso a la consola	R1(config)# **line console 0** R1(config-line)# **password cisco** R1(config-line)# **login**
Contraseña de acceso Telnet	R1(config)#**line vty 0 4** R1(config-line)#**password cisco** R1(config-line)# **login**
Cifrar las contraseñas de texto no cifrado	R1(config)#**service password-encryption** R1(config)#**exit**
Mensaje MOTD	R1(config)# **banner motd** # *** Prohibido el acceso no autorizado *** #
Interfaz S0/0/0	R1(config)#**interface serial 0/0/0** R1(config)#**description** Conexion a R2 R1(config)#**ip address** 172.16.1.1 255.255.255.252 R1(config)#**ipv6 address** 2001:DB8:ACAD:1::1/64 R1(config)#**clock rate** 128000 R1(config)#**no shutdown** R1(config)#**exit**
Rutas predeterminadas	R1(config)# **ip route** 0.0.0.0 0.0.0.0 serial 0/0/0 R1(config)#**ipv6 route** ::/0 serial 0/0/0 R1(config)#**exit**

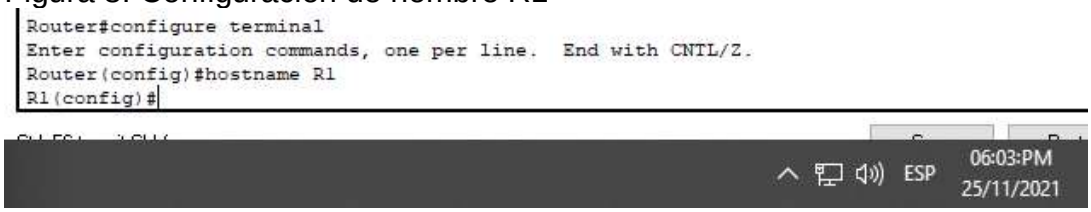
Fuente: Propia.

Figura 7. Comando no ip domain-lookup



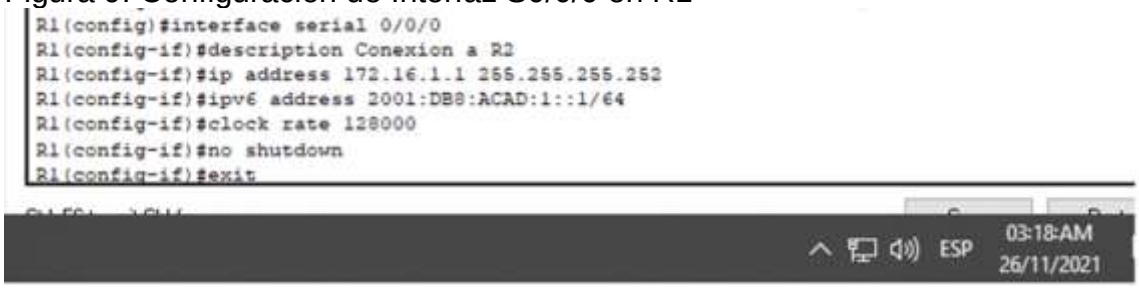
Fuente: Propia.

Figura 8. Configuración de nombre R1



Fuente: Propia.

Figura 9. Configuración de Interfaz S0/0/0 en R1



Fuente: Propia.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 9. Configuración de R2.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>**enable** Router#**configure terminal** Router(config)#**no ip domain-lookup**
Nombre del router	Router(config)#**hostname R2**

Contraseña de exec privilegiado cifrada	R2(config)# **enable secret class**
Contraseña de acceso a la consola	R2(config)# **line console 0** R2(config-line)# **password cisco** R2(config-line)# **login** R2(config-line)# **exit**
Contraseña de acceso Telnet	R2(config)#**line vty 0 4** R2(config-line)#**password cisco** R2(config-line)# **login** R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#**service password-encryption**
Habilitar el servidor HTTP	**No aplica** *(El escenario simulado en Packet Tracer no permite la inserción del protocolo HTTP).* R2(config)#**ip http server** ^ % Invalid input detected at '^' marker.
Mensaje MOTD	R2(config)# **banner motd #** *** Se prohíbe el acceso no autorizado *** # R2(config)# exit
Interfaz S0/0/0	R2(config)# **interface serial 0/0/0** R2(config)# **description** Conexion a R1 R2(config)# **ip address** 172.16.1.2 255.255.255.252 R2(config)# **ipv6 address** 2001:DB8:ACAD:1::2/64 R2(config)# **no shutdown**
Interfaz S0/0/1	R2(config)#**interface serial 0/0/1** 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** R2(config-if)#exit

Interfaz G0/0 (simulación de Internet)	R2(config)#**interface gigabitEthernet 0/0** R2(config-if)#**description** Conexion Servidor R2(config-if)#**ip address** 209.165.200.233 255.255.255.248 R2(config-if)#**ipv6 address** 2001:DB8:ACAD:A::1/64 R2(config-if)#**no shutdown**
Interfaz loopback 0 (servidor web simulado)	R2(config)# **interface loopback 0** R2(config)# **description** Conexion Servidor Web simulado R2(config)# **ip address** 10.10.10.10 255.255.255.255
Ruta predeterminada	R2(config)# **ip route** 0.0.0.0 0.0.0.0 G0/0 R2(config)# **ipv6 route** ::/0 G0/0

Fuente: Propia.

Figura 10. Configuración de seguridad en R2

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip http server
                ^
% Invalid input detected at '^' marker.

R2(config)#banner motd # *** Se prohbe el acceso no autorizado *** #
R2(config)#
```

Fuente: Propia.

Figura 11. Configuración S0/0/0 en R2

```
R2(config)#interface serial 0/0/0
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
```

Fuente: Propia.

Figura 12. Configuración S0/0/0 en R2

```
R2(config)#interface serial 0/0/1
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
R2(config-if)#exit
R2(config)#
```

Fuente: Propia.

Figura 13. Configuración G 0/0 en R2

```
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#description Conexion Servidor
R2(config-if)#ip address 209.165.200.233 255.255.255.248
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to
```

Fuente: Propia.

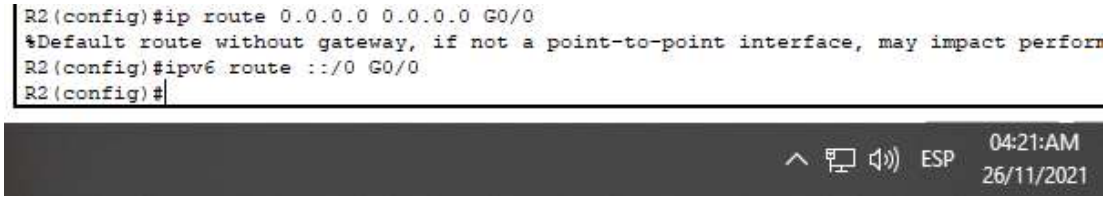
Figura 14. Configuración de loopback 0 en R2

```
R2(config)#interface loopback 0

R2(config-if)#description Conexion Servidor Web simulado
R2(config-if)#ip address 10.10.10.10 255.255.255.255
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
```

Fuente: Propia.



Fuente: Propia.

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 10. Configuración R3

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

Interfaz S0/0/1	R3(config)# **interface serial 0/0/1** R3(config)# **description Conexion a R2** R3(config)# **ip address 172.16.2.1 255.255.255.252** R3(config)# **ipv6 address 2001:DB8:ACAD:2::1/64** R3(config)# **no shutdown**
Interfaz loopback 4	R3(config)#**interface loopback 4** R3(config)#**description Interfaz virtual 4** R3(config)# **ip address 192.168.4.1 255.255.255.0**
Interfaz loopback 5	R3(config)# **interface loopback 5** R3(config)# **description Interfaz virtual 5** R3(config)# **ip address 192.168.5.1 255.255.255.0**
Interfaz loopback 6	R3(config)#**interface loopback 6** R3(config)#**description Interfaz virtual 6** R3(config)#**ip address 192.168.6.1 255.255.255.0**
Interfaz loopback 7	R3(config)#**interface** loopback 7 R3(config-if)#**description** Interfaz virtual 7 R3(config-if)#**ipv6 address** 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	R3(config)#**ip route 0.0.0.0 0.0.0.0 s0/0/1** R3(config)#**ipv6 route ::/0 s0/0/1** R3(config)#**exit**

Fuente: Propia.

Figura 15. Configuración de seguridad en R3

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd # *** Prohibido el acceso no autorizado *** #
```

Fuente: Propia.

Figura 16. Configuración S0/0/1 en R3

```
R3(config)#interface serial 0/0/1
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

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
```

Fuente: Propia.

Figura 17. Configuración de loopback 4 en R3

```
R3(config)#interface loopback 4
R3(config-if)#description Interfaz virtual 4
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#
```

Fuente: Propia.

Figura 18. Configuración de loopback 5 en R3

```
R3(config-if)#description Interfaz virtual 5
R3(config-if)#ip address 192.168.5.1 255.255.255.0
%LINK-5-CHANGED: Interface Loopback5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up
```

Fuente: Propia.

Figura 19. Configuración de loopback 6 en R3

```
R3(config)#interface loopback 6

R3(config-if)#description Interfaz virtual 6
R3(config-if)#ip address 192.168.6.1 255.255.255.0
%LINK-5-CHANGED: Interface Loopback6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up
```

Fuente: Propia.

Figura 20. Configuración de loopback 7 en R3

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface loopback 7
R3(config-if)#description Interfaz virtual 7
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
R3(config-if)#
```

Fuente: Propia.

Figura 21. Configuración de Rutas predeterminadas en R3

```
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
%Default route without gateway, if not a point-to-point interface,
R3(config)#ipv6 route ::/0 s0/0/1
R3(config)#
```

Fuente: Propia.

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

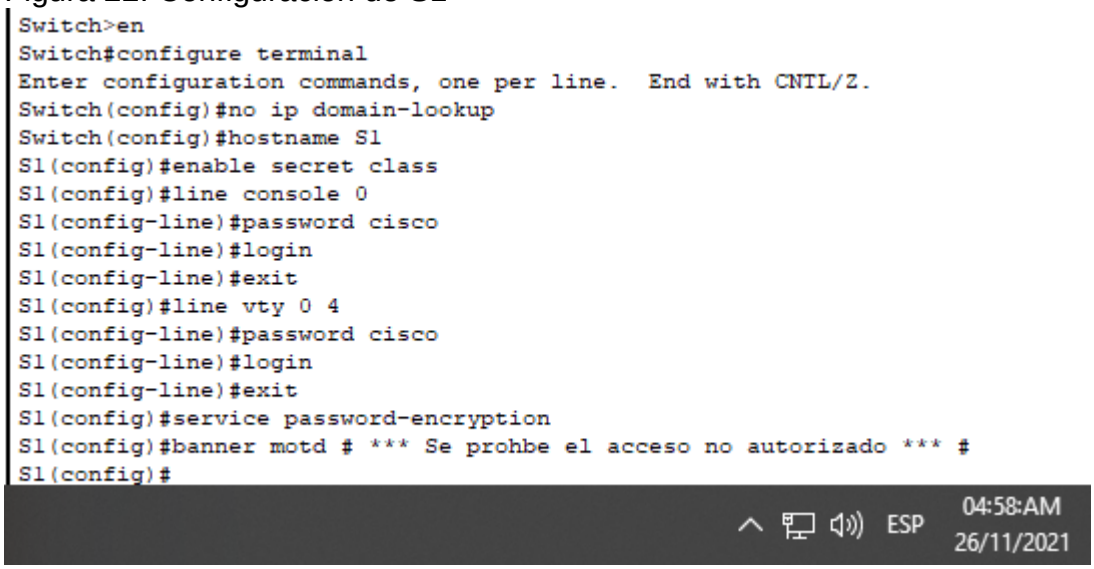
Tabla 11. Configuración de S1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch(config)#**no ip domain-lookup**
Nombre del switch	switch(config)#**hostname S1**
Contraseña de exec privilegiado cifrada	S1(config)# **enable secret class**
Contraseña de acceso a la consola	S1(config)# **line console 0** S1(config-line)# **password cisco** S1(config-line)# **login** S1(config-line)# **exit**
Contraseña de acceso Telnet	S1#**configure terminal** S1(config)#**line vty 0 4** 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 prohbe el acceso no autorizado *** #**

Fuente: Propia.

Figura 22. Configuración de S1



Fuente: Propia.

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

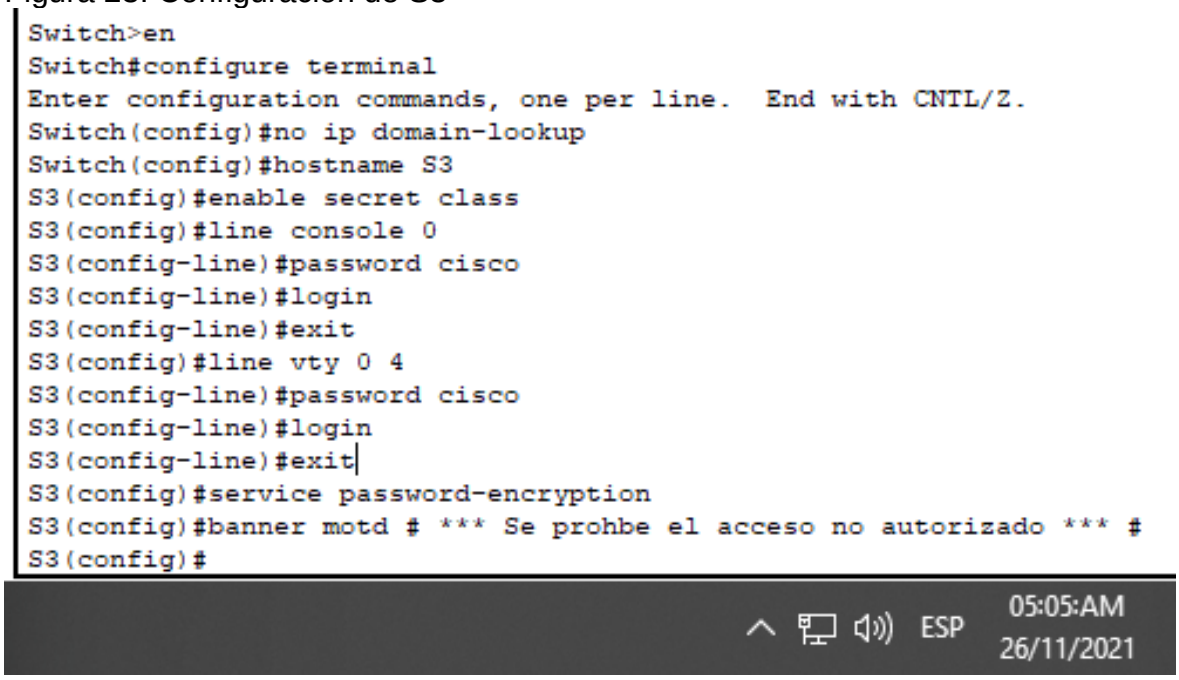
Tabla 12. Configuración de S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>**enable** Switch#**configure terminal** Switch(config)#**no ip domain-lookup**
Nombre del switch	switch(config)#**hostname S3**
Contraseña de exec privilegiado cifrada	S3(config)# **enable secret class**
Contraseña de acceso a la consola	S3(config)# **line console 0** S3(config-line)# **password cisco** S3(config-line)# **login** S3(config-line)# **exit**

Contraseña de acceso Telnet	S3(config)#**line vty 0 4** S3(config-line)#**password cisco** S3(config-line)# **login** S3(config-line)#**exit**
Cifrar las contraseñas de texto no cifrado	S3(config)#**service password-encryption**
Mensaje MOTD	S3(config)#**banner motd # *** Se prohbe el acceso no autorizado *** #**

Fuente: Propia.

Figura 23. Configuración de S3



Fuente: Propia.

Paso 7: Verificar la conectividad de la red

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

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.

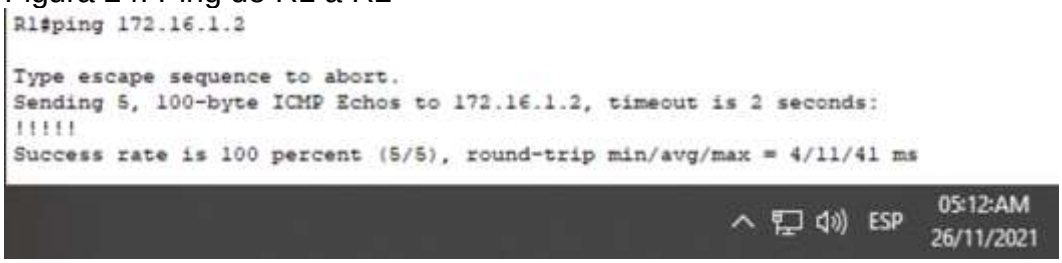
Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 13. Verificar la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2	172.16.1.2	Success rate is 100 percent (5/5)
R2	R3	172.16.2.1	Success rate is 100 percent (5/5)
PC de Internet	Gateway predeterminado	209.165.200.233	Packets: Sent = 4, Received = 4

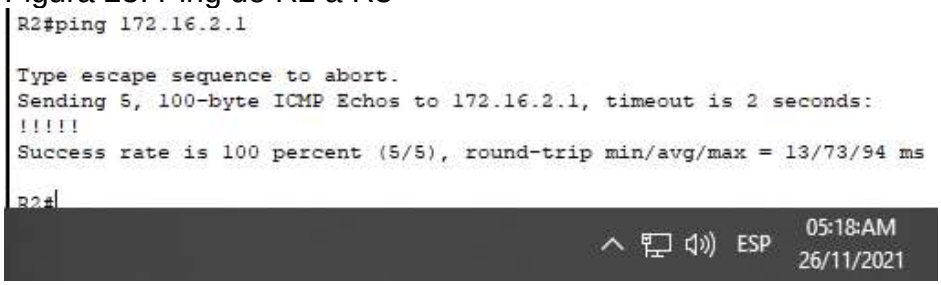
Fuente: Propia.

Figura 24. Ping de R1 a R2



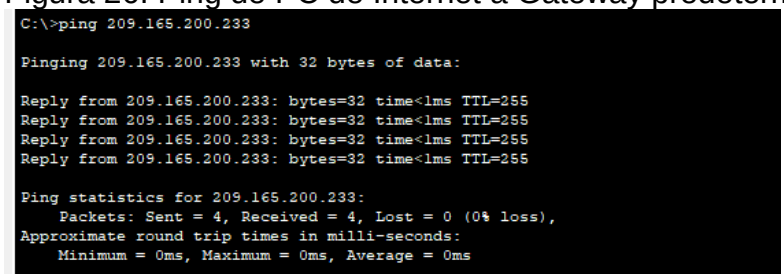
Fuente: Propia.

Figura 25. Ping de R2 a R3



Fuente: Propia.

Figura 26. Ping de PC de Internet a Gateway predeterminado



Fuente: 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:

Tabla 14. Configuración de la seguridad de S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1# **configure terminal** S1(config)#**vlan 21** S1(config)#**name** Contabilidad S1(config)#**vlan 23** S1(config)#**name** Ingenieria S1(config)#**vlan 99** S1(config)#**name** Administracion S1(config)#**exit**
Asignar la dirección IP de administración.	S1(config)#**interface** Vlan 99 S1(config)#**ip address** 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado	S1(config)#**ip default-gateway** 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#**interface** fastEthernet 0/3 S1(config)#**switchport mode trunk** S1(config)#**switchport trunk native vlan 1**
Forzar el enlace troncal en la interfaz F0/5	S1(config)#**interface** fastEthernet 0/5 S1(config)#**switchport mode trunk** S1(config)#**switchport trunk native vlan 1**
Configurar el resto de los puertos como puertos de acceso	S1(config)#**interface range** fastEthernet 0/1- 2, f0/4, f0/6-24, g0/1-2 S1(config)#**switchport mode access**
Asignar F0/6 a la VLAN 21	S1(config)#**interface** fastEthernet 0/6 S1(config)#**switchport access vlan 21**

Apagar todos los puertos sin usar	S1(config)#**interface range** fastEthernet 0/1- 2, f0/4, f0/7-24, g0/1-2 S1(config)#**shutdown**

Fuente: Propia.

Figura 27. Creación base de datos de VLAN

```
S1>en
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administracion
S1(config-vlan)#exit
S1(config)#
```

Fuente: Propia.

Figura 28. Asignar dirección IP de administración.

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface Vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#ip default-gateway 192.168.99.1
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config)#interface fastEthernet 0/3
```

Fuente: Propia.

Figura 29. Forzar el enlace troncal en la interfaz F0/3

```
S1(config)#interface fastEthernet 0/3
S1(config-if)#switchport mode trunk

S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed stat

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed stat

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S1(config)#interface fastEthernet 0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
S1(config)#interface range fastEthernet 0/1- 2, f0/4, f0/6-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#exit
```

Fuente: Propia.

Figura 30. Asignar F0/6 a la VLAN 21

```
S1(config)#interface fastEthernet 0/6
S1(config-if)#switchport access vlan 21
S1(config-if)#exit
```

Fuente: Propia.

Figura 31. Configurar el resto de los puertos como puertos de acceso

```
S1(config)#interface range fastEthernet 0/1- 2, f0/4, f0/7-24, g0/1-2
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively
```

Fuente: Propia.

Paso 2: Configurar el S3
La configuración del S3 incluye las siguientes tareas:

Tabla 15. Configuración de la seguridad de S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3# **configure terminal** S3(config)#**vlan 21** S3(config)#**name** Contabilidad S3(config)#**vlan 23** S3(config)#**name** Ingenieria S3(config)#**vlan 99** S3(config)#**name** Administracion S3(config)#**exit**
Asignar la dirección IP de administración	S3(config)#**interface** Vlan 99 S3(config)#**ip address** 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado.	S3(config)#**ip default-gateway** 192.168.99.1 S3(config)#**exit**
Forzar el enlace troncal en la interfaz F0/3	S3(config)#**interface fastEthernet 0/3** S3(config)#**switchport mode trunk** S3(config)#**switchport trunk native vlan 1** S3(config)#**exit**
Configurar el resto de los puertos como puertos de acceso	S3(config)#**interface range fastEthernet 0/1- 2, f0/4-24, g0/1-2** S3(config)#**switchport mode access** S3(config)#**exit**
Asignar F0/18 a la VLAN 21	S3(config)#**interface fastEthernet 0/18** S3(config)#**switchport access vlan 21** S3(config)#**exit**
Apagar todos los puertos sin usar	S3(config)#**interface range fastEthernet 0/1- 2, f0/4-17, f0/19-24, g0/1-2** S3(config)#**shutdown** S3(config)#**exit**

Fuente: Propia.

Figura 32. Configuración de la seguridad de S3

```
S3>en
Password:
S3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#vlan 21
S3(config-vlan)#name Contabilidad
S3(config-vlan)#vlan 23
S3(config-vlan)#name Ingenieria
S3(config-vlan)#vlan 99
S3(config-vlan)#name Administracion
S3(config-vlan)#exit
S3(config)#interface Vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#ip default-gateway 192.168.99.1
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S3(config)#interface fastEthernet 0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#exit
S3(config)#interface range fastEthernet 0/1- 2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#exit
S3(config)#interface fastEthernet 0/18
S3(config-if)#switchport access vlan 21
S3(config-if)#exit
S3(config)#interface range fastEthernet 0/1- 2, f0/4-17, f0/19-24, g0/1-2
S3(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
```

Fuente: Propia.

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

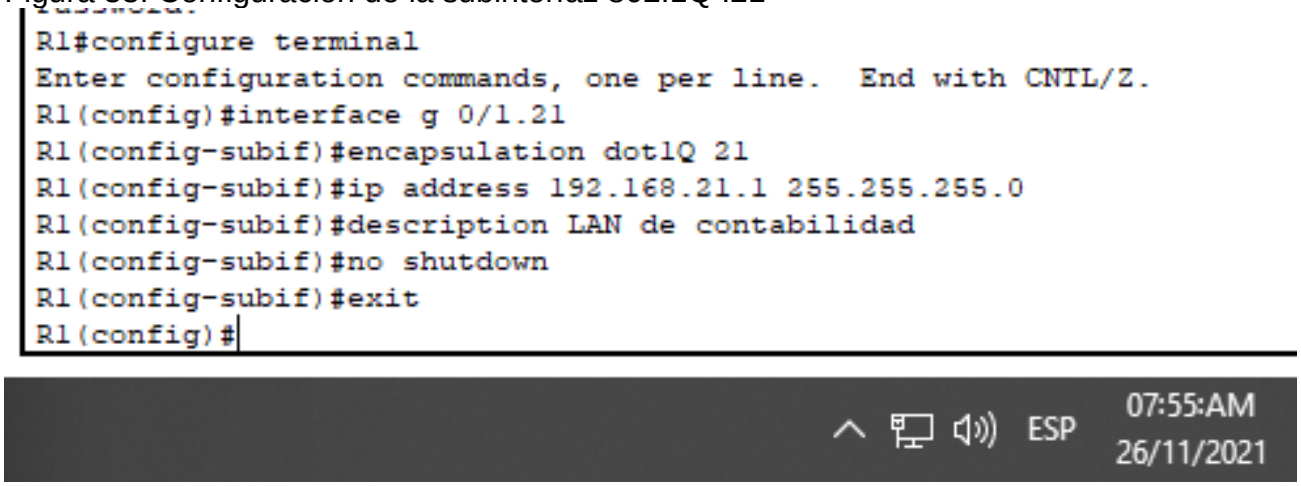
Tabla 16. configuración para R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1# **configure terminal** R1(config)#**interface g 0/1.21** R1(config)#**encapsulation dot1Q 21** R1(config)#**ip address** 192.168.21.1 255.255.255.0 R1(config)#**description** LAN de contabilidad

	R1(config)#**no shutdown** R1(config)#**exit**
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)#**interface g 0/1.23** R1(config)#**encapsulation dot1Q 23** R1(config)#**ip address** 192.168.23.1 255.255.255.0 R1(config)#**description** LAN de Ingenieria R1(config)#**no shutdown** R1(config)#**exit**
Configurar la subinterfaz 802.1Q .99 en G0/1	R1# **configure terminal** R1(config)#**interface g 0/1.99** R1(config)#**encapsulation dot1Q 99** R1(config)#**ip address** 192.168.99.1 255.255.255.0 R1(config)#**description** LAN de Administracion R1(config)#**no shutdown** R1(config)#**exit**
Activar la interfaz G0/1	R1# **configure terminal** R1(config)#**interface g 0/1** R1(config)#**no shutdown** R1(config)#**exit**

Fuente: Propia.

Figura 33. Configuración de la subinterfaz 802.1Q .21



Fuente: Propia.

Figura 34. Configuración de la subinterfaz 802.1Q .23

```
R1(config)#interface g 0/1.23
R1(config-subif)#encapsulation dot1Q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#description LAN de Ingenieria
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#
```

Fuente: Propia.

Figura 35. Configuración de la subinterfaz 802.1Q .99

```
R1(config)#interface g 0/1.99
R1(config-subif)#encapsulation dot1Q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#description LAN de Administracion
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#
```

Fuente: Propia.

Paso 4: Verificar la conectividad de la red

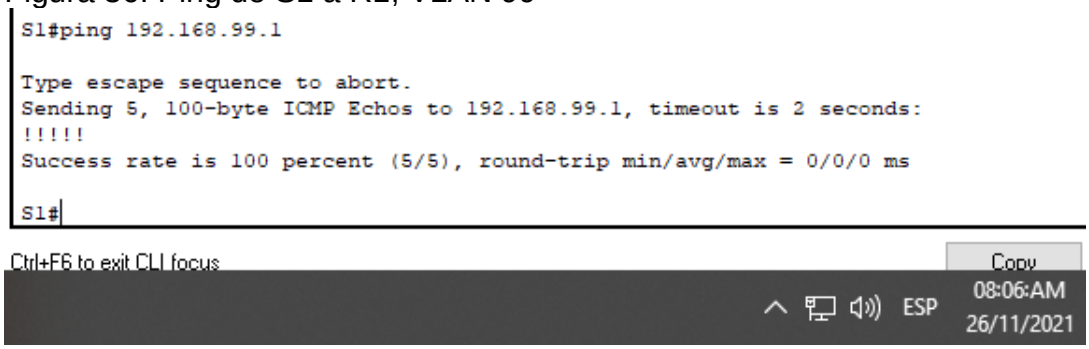
Utilice el comando **ping** para probar la conectividad entre los switches y el R1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 17. Verificar la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	*Success rate is 100 percent (5/5)*
S3	R1, dirección VLAN 99	192.168.99.1	*Success rate is 100 percent (5/5)*
S1	R1, dirección VLAN 21	192.168.21.1	*Success rate is 100 percent (5/5)*

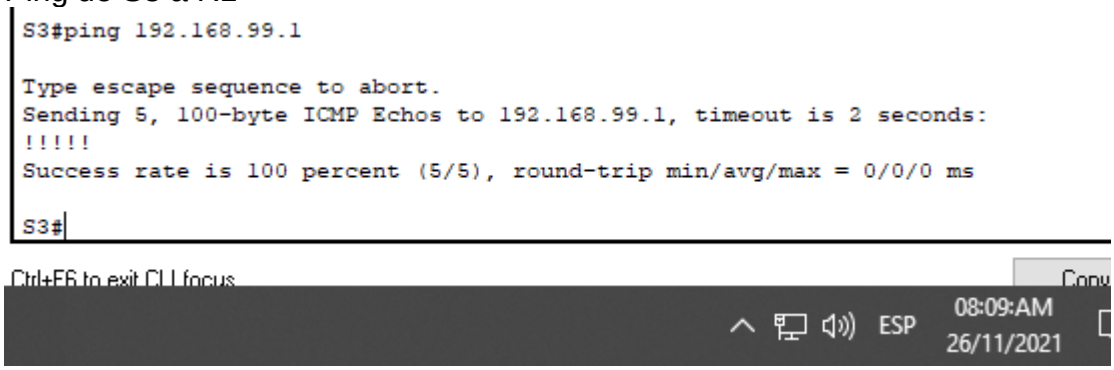
Fuente: Propia.

Figura 36. Ping de S1 a R1, VLAN 99



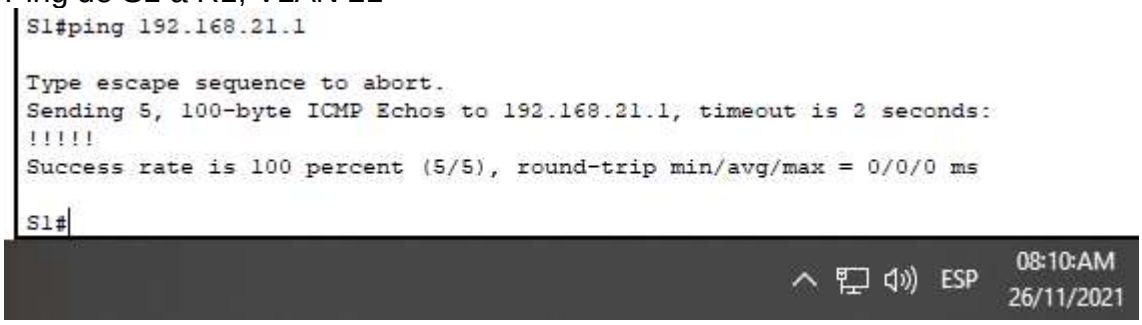
Fuente: Propia.

Ping de S3 a R1



Fuente: Propia.

Ping de S1 a R1, VLAN 21



Fuente: 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:

Tabla 18. Configurar OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1#**configure terminal** R1(config)#**router ospf 10** R1(config)#**router-id 1.1.1.1**
Anunciar las redes conectadas directamente	R1#**configure terminal** R1(config)#**network** 172.16.1.0 0.0.0.3 area 0 R1(config)#**network** 192.168.21.0 0.0.0.255 area 0 R1(config)#**network** 192.168.23.0 0.0.0.255 area 0 R1(config)#**network** 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1#**configure terminal** R1(config)#**passive-interface** gigabitEthernet 0/1.21 R1(config)#**passive-interface** gigabitEthernet 0/1.23 R1(config)#**passive-interface** gigabitEthernet 0/1.99 R1(config)#**exit**
Desactive la sumarización automática	**No aplica**

Fuente: Propia.

Figura 37. Error OSPF con IPv6

Fuente: Propia.

Figura 38. Configuración OSPF

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 10
R1(config-router)#router-id 1.1.1.1
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
R1(config-router)#passive-interface gigabitEthernet 0/1.21
R1(config-router)#passive-interface gigabitEthernet 0/1.23
R1(config-router)#passive-interface gigabitEthernet 0/1.99
R1(config-router)#
```

Fuente: Propia.

Figura 39. Verificación de OSPF

```
R1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.99.1
  Number of areas in this router is 0. 0 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 110)

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.3 area 0
    192.168.21.0 0.0.0.255 area 0
    192.168.23.0 0.0.0.255 area 0
    192.168.99.0 0.0.0.255 area 0
  Passive Interface(s):
    GigabitEthernet0/1.21
    GigabitEthernet0/1.23
    GigabitEthernet0/1.99
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:02:09
  Distance: (default is 110)
```

Fuente: Propia.

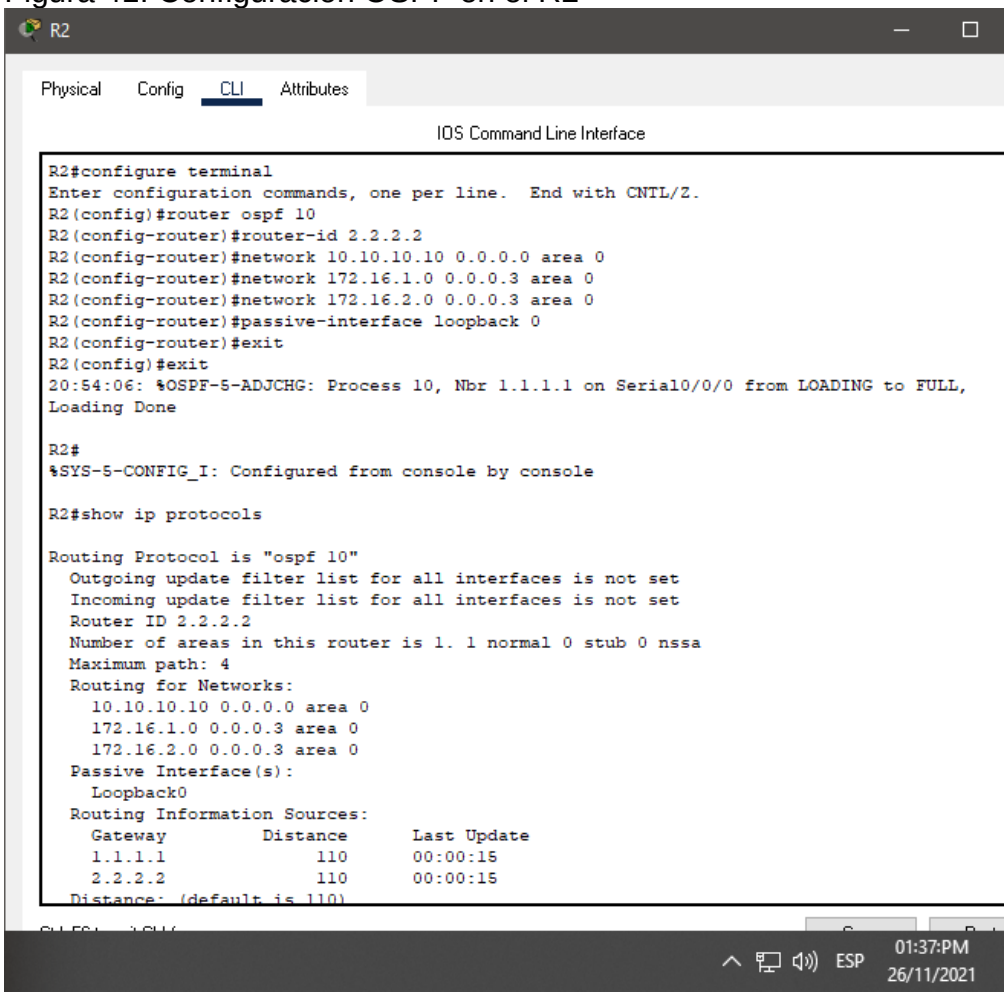
Paso 2: Configurar OSPF en el R2
La configuración del R2 incluye las siguientes tareas:

Figura 40. Configuración OSPF en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2# **configure terminal** R2(config)#**router ospf 10** R2(config)#**router-id 2.2.2.2**
Anunciar las redes conectadas directamente	R2(config)#**network** 10.10.10.10 0.0.0.0 area 0 R2(config)#**network** 172.16.1.0 0.0.0.3 area 0 R2(config)#**network** 172.16.2.0 0.0.0.3 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config)#**passive-interface loopback 0** R2(config)#**exit**
Desactive la sumarización automática.	**No aplica**

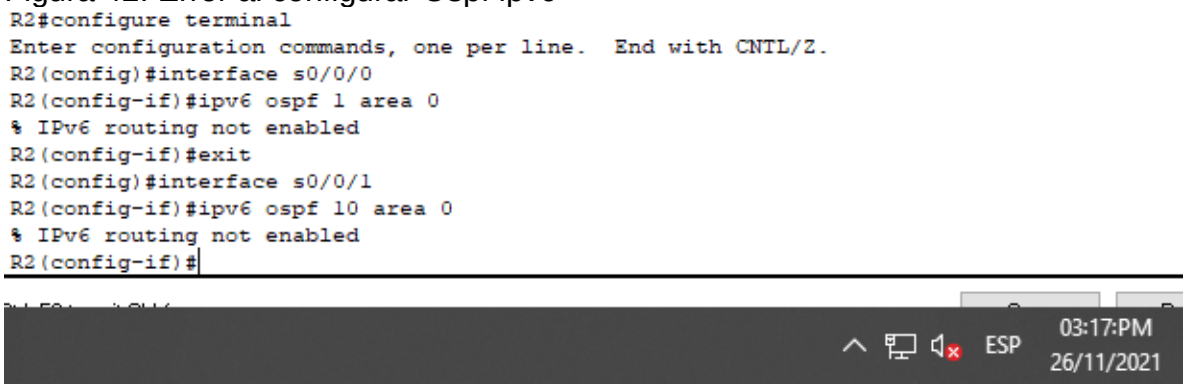
Fuente: Propia.

Figura 41. Configuración OSPF en el R2



Fuente: Propia.

Figura 42. Error al configurar Ospf ipv6



Fuente: Propia.

Paso 3: Configurar OSPF en el R3

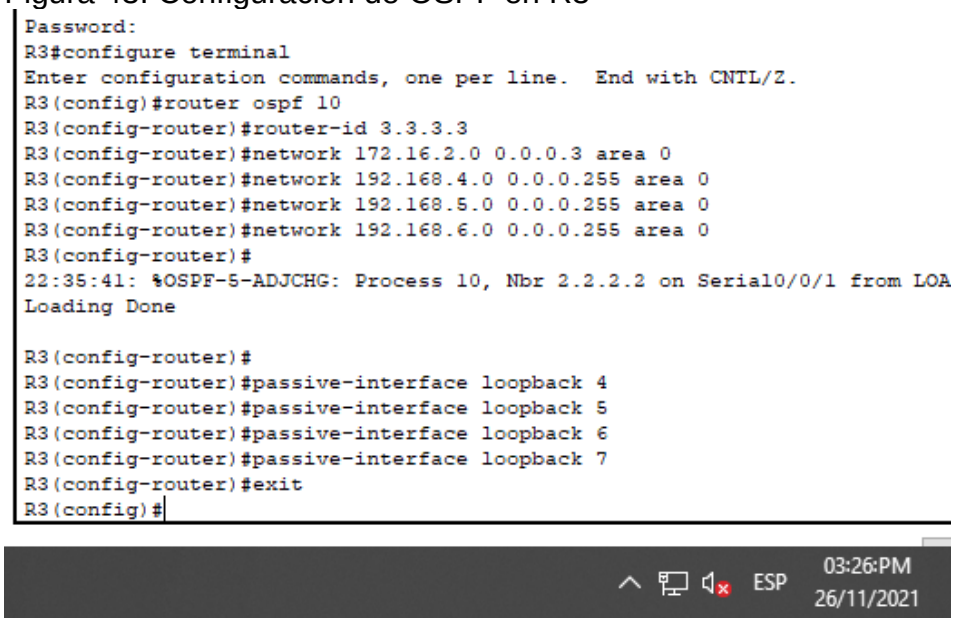
La configuración del R3 incluye las siguientes tareas:

Tabla 19. Configuración de OSPF en R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3#**configure terminal** R3(config)#**router ospf 10** R3(config)#**router-id 3.3.3.3**
Anunciar redes IPv4 conectadas directamente	R3(config)#**network** 172.16.2.0 0.0.0.3 area 0 R3(config)#**network** 192.168.4.0 0.0.0.255 area 0 R3(config)#**network** 192.168.5.0 0.0.0.255 area 0 R3(config)#**network** 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config)#**passive-interface loopback 4** R3(config)#**passive-interface loopback 5** R3(config)#**passive-interface loopback 6** R3(config)#**exit**
Desactive la sumarización automática.	**No aplica**

Fuente: Propia.

Figura 43. Configuración de OSPF en R3



Fuente: Propia.

Figura 44. Verificación de OSPF en R3

```
R3#show ip protocols

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  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
    192.168.4.0 0.0.0.255 area 0
    192.168.5.0 0.0.0.255 area 0
    192.168.6.0 0.0.0.255 area 0
  Passive Interface(s):
    Loopback4
    Loopback5
    Loopback6
    Loopback7
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:16:09
    2.2.2.2              110      00:04:21
    3.3.3.3              110      00:04:21
  Distance: (default is 110)
```

Fuente: 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:

Tabla 20. Comandos para Verificación de OSPF

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Con el comando: **show ip protocols**
¿Qué comando muestra solo las rutas OSPF?	El comando **show ip route ospf**
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Los comandos: **show running-config | section router ospf** **show ip protocols**

Fuente: Propia.

Figura 45. Comando show ip protocols

```
R3#show ip protocols

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  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
    192.168.4.0 0.0.0.255 area 0
    192.168.5.0 0.0.0.255 area 0
    192.168.6.0 0.0.0.255 area 0
  Passive Interface(s):
    Loopback4
    Loopback5
    Loopback6
    Loopback7
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:04:13
    2.2.2.2              110      00:22:26
    3.3.3.3              110      00:22:26
  Distance: (default is 110)
```

Fuente: Propia.

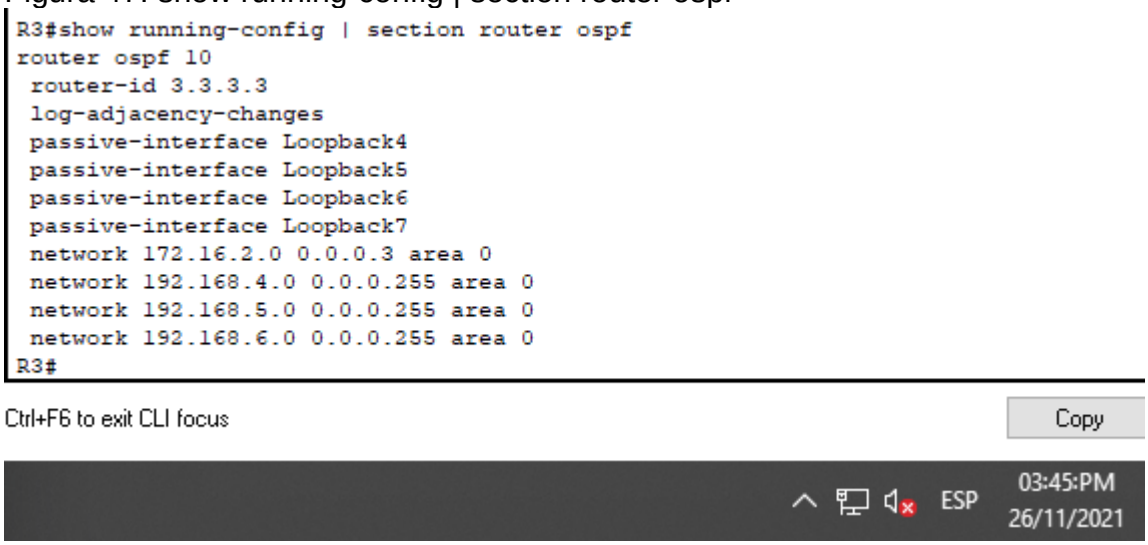
Figura 46. Comando show ip route ospf

```
R3#show ip route ospf
     10.0.0.0/32 is subnetted, 1 subnets
O       10.10.10.10 [110/65] via 172.16.2.2, 00:21:49, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O       172.16.1.0 [110/128] via 172.16.2.2, 00:21:49, Serial0/0/1
O    192.168.21.0 [110/129] via 172.16.2.2, 00:21:49, Serial0/0/1
O    192.168.23.0 [110/129] via 172.16.2.2, 00:21:49, Serial0/0/1
O    192.168.99.0 [110/129] via 172.16.2.2, 00:21:49, Serial0/0/1

R3#
```

Fuente: Propia.

Figura 47. show running-config | section router ospf



Fuente: 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:

Tabla 21. Configurar R1 como servidor DHCP

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	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(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** R1(config)#**network** 192.168.21.0 255.255.255.0 R1(config)#**default-router** 192.168.21.1 R1(config)#**dns-server** 10.10.10.10 R1(config)#**domain-name ccna-sa.com**

Crear un pool de DHCP para la VLAN 23	R1(config)#**ip dhcp pool ENGNR** R1(config)#**network 192.168.23.0 255.255.255.0** R1(config)#**default-router** 192.168.23.1 R1(config)#**dns-server 10.10.10.10** R1(config)#**domain-name** ccna-sa.com R1(config)#**exit**

Fuente: Propia.

Figura 48. Configurar R1 como servidor DHCP

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#exit
R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#exit
R1(config)#
```

Fuente: Propia.

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

La configuración del R2 incluye las siguientes tareas:

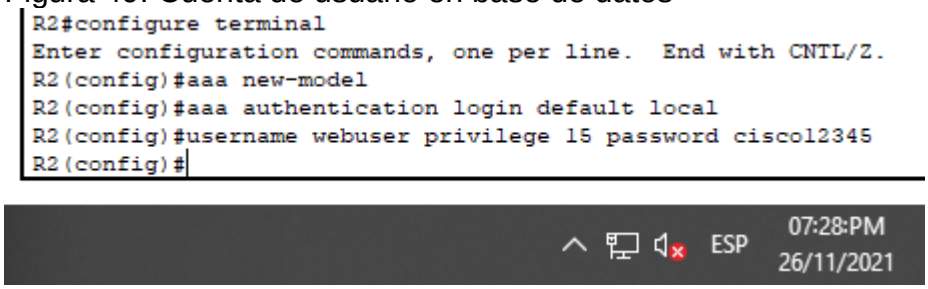
Tabla 22. Configuración de NAT estática y dinámica

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2# **configure terminal** R2(config)# **aaa new-model** R2(config)# **aaa authentication login default local** R2(config)# **username** webuser **privilege** 15 **password** cisco12345

Habilitar el servicio del servidor HTTP	**No aplica** (El escenario simulado en Packet Tracer no admite el protocolo HTTP). R2(config)# **ip http server** ^ **% Invalid input detected at '^' marker.**
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	**No aplica** (El escenario simulado en Packet Tracer no permite la inserción del protocolo HTTP). R2(config)#**ip http authentication local** ^ **% Invalid input detected at '^' marker.**
Crear una NAT estática al servidor web.	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 g 0/0** R2(config)#**ip nat outside** R2(config)#**exit** R2(config)#**interface loopback 0** R2(config)#**ip nat inside** R2(config)#**exit**
Configurar la NAT dinámica dentro de una ACL privada	R2# **configure terminal** 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** 192.168.0.0 0.0.3.255 R2(config)#**ip access-list standard** ADMIN-MGT R2(config-std-nacl)#**permit host** 172.16.1.1 R2(config-std-nacl)#**deny any**
Defina el pool de direcciones IP públicas utilizables.	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**

Fuente: Propia.

Figura 49. Cuenta de usuario en base de datos

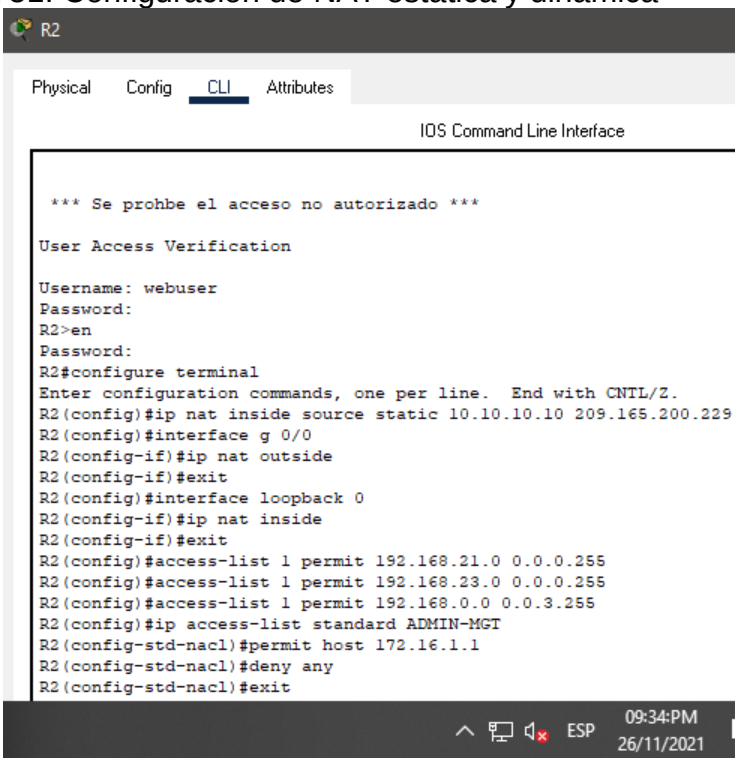


Fuente: Propia.

Figura 50. Evidencia de usuario creado

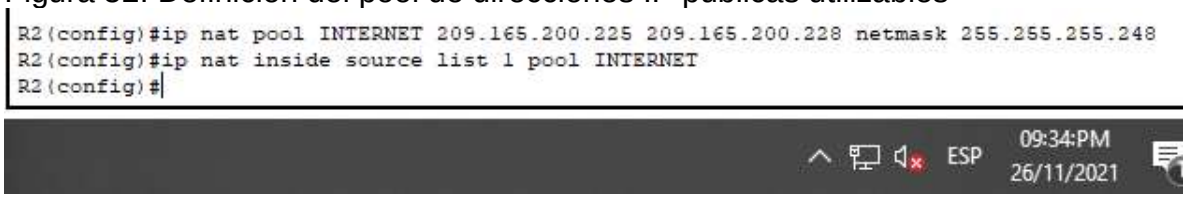
Fuente: Propia.

Figura 51. Configuración de NAT estática y dinámica



Fuente: Propia.

Figura 52. Definición del pool de direcciones IP públicas utilizables



Fuente: Propia.

Paso 3: Verificar el protocolo DHCP y la NAT estática

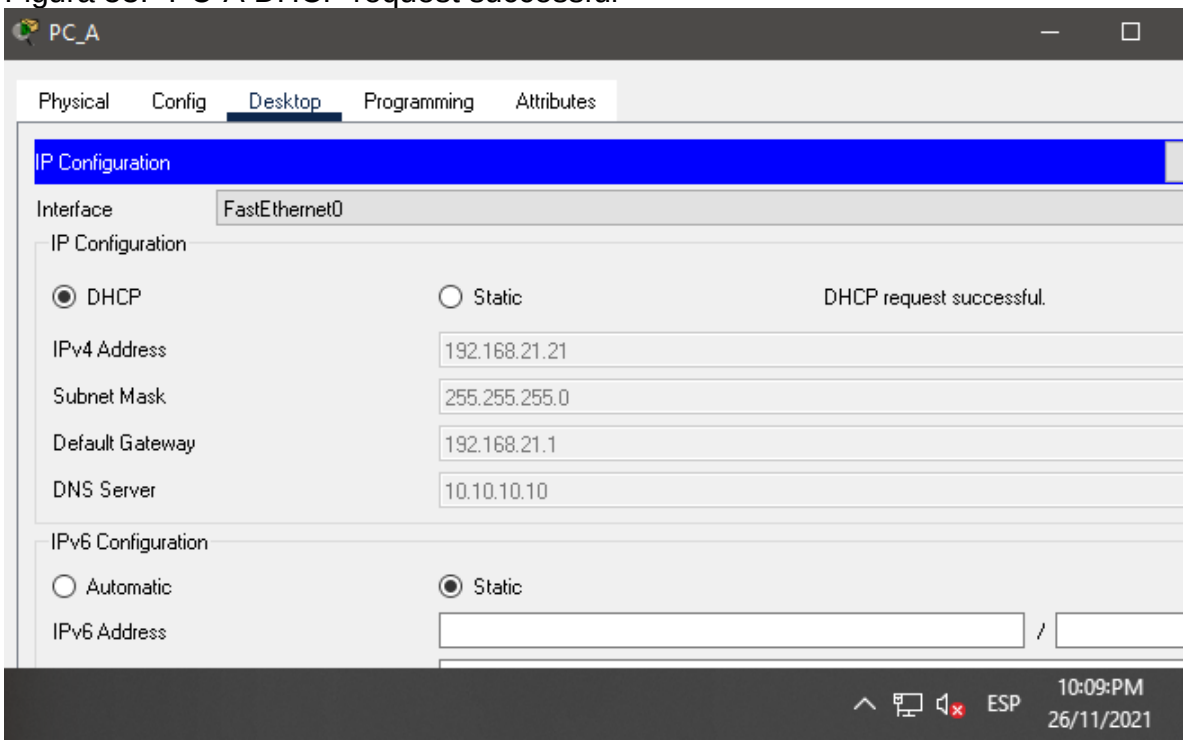
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 23. Verificación de configuraciones DHCP y NAT

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Ver figura 52
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Ver figura 53
Verificar que la PC-A pueda hacer ping a la PC-C	Ver figura 54
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Teniendo en cuenta que Packet Tracer no soporto los comandos de HTTP, no puede ser validado

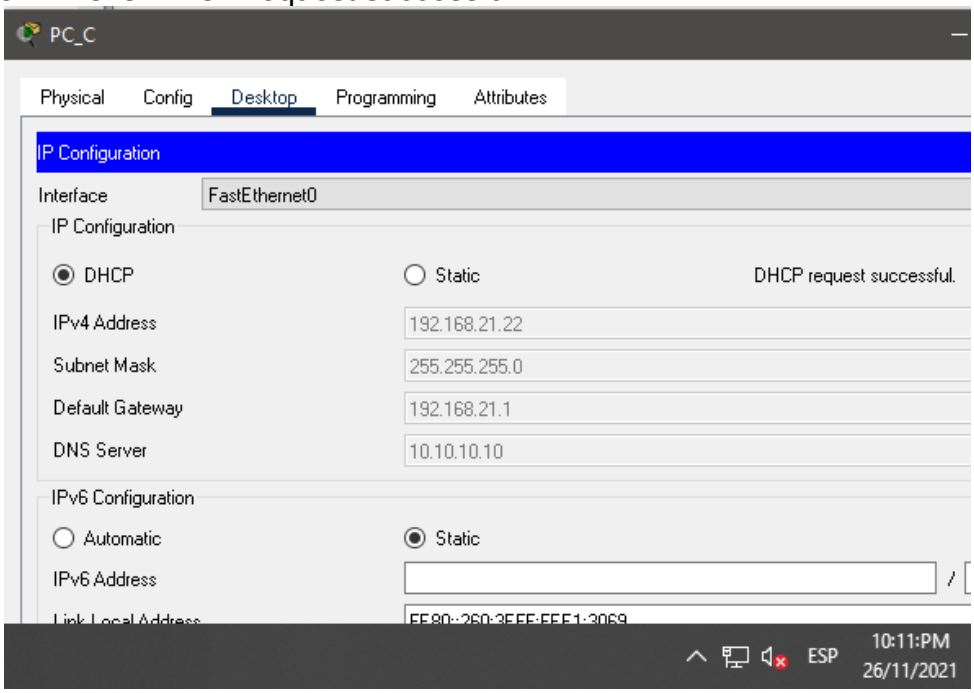
Fuente: Propia.

Figura 53. “PC-A DHCP request successful”



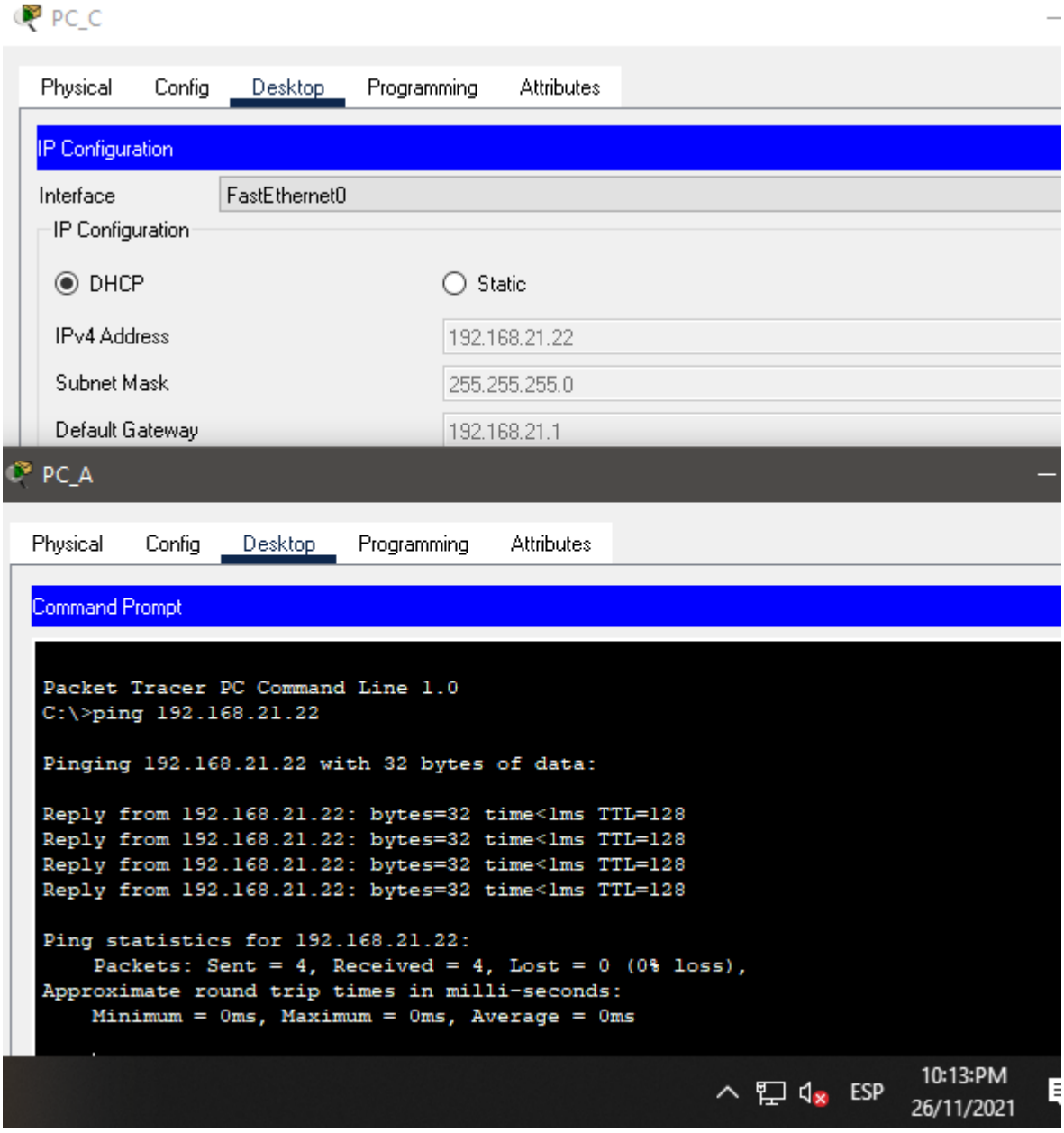
Fuente: Propia.

Figura 54. “PC-C DHCP request successful”



Fuente: Propia.

Figura 55. ping de PC-A a PC-C



Fuente: Propia.

Parte 6: Configurar NTP

Tabla 24. Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#**clock set** 09:00:00 05 March 2016
Configure R2 como un maestro NTP.	R2# **configure terminal** R2(config)#**ntp master 5**
Configurar R1 como un cliente NTP.	R1(config)#**ntp server 172.16.1.2**
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#**ntp update-calendar**
Verifique la configuración de NTP en R1.	Se aplica el comando **show ntp status**

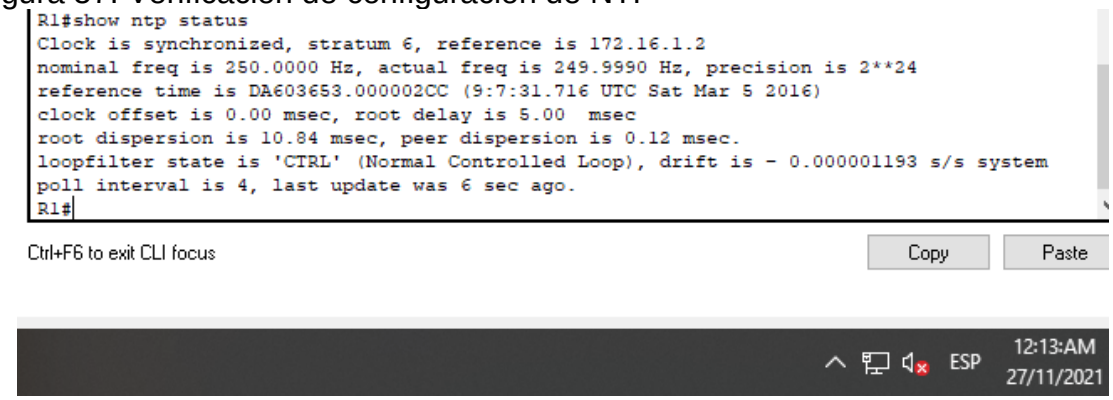
Fuente: Propia.

Figura 56. Configuración NTP

```
R2#clock set 09:00:00 05 March 2016
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ntp master 5
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente: Propia.

Figura 57. Verificación de configuración de NTP



Fuente: Propia.

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

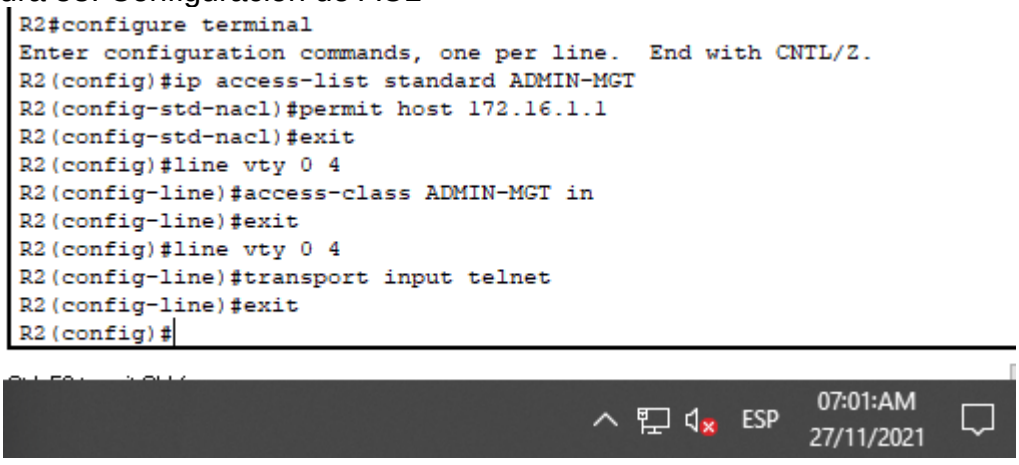
Paso 1: Restringir el acceso a las líneas VTY en el R2:

Tabla 25. Configurar y verificar ACL

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

Fuente: Propia.

Figura 58. Configuración de ACL



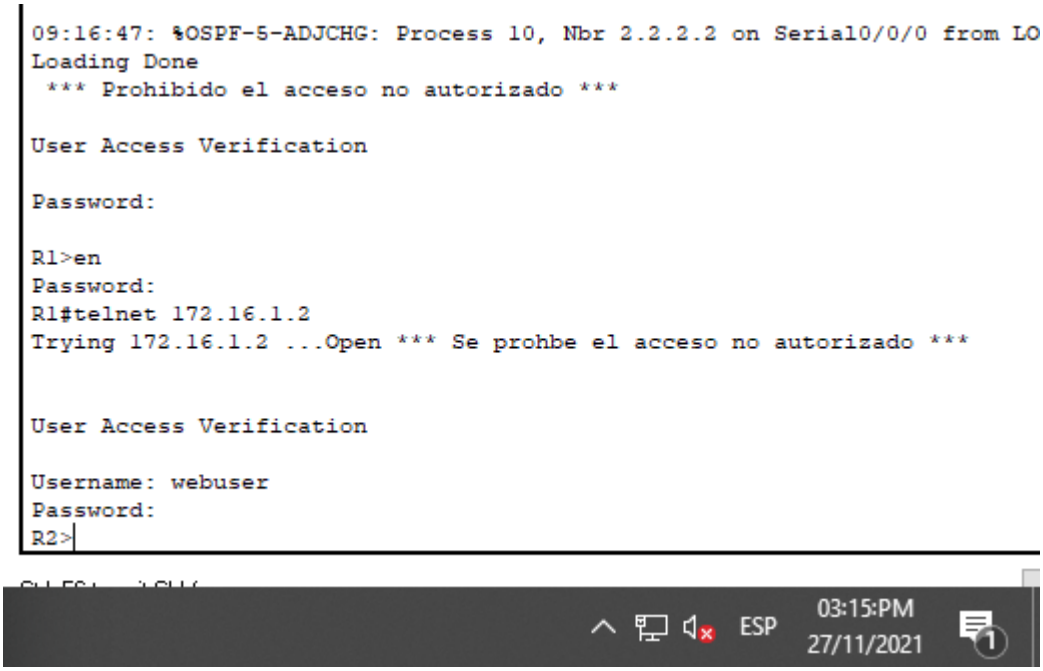
Fuente: Propia.

Figura 59. Verificación de ACL

```
R2#show access-lists
Standard IP access list 1
    10 permit 192.168.21.0 0.0.0.255
    20 permit 192.168.23.0 0.0.0.255
    30 permit 192.168.0.0 0.0.3.255
Standard IP access list ADMIN-MGT
    10 permit host 172.16.1.1 (1 match(es))
    20 deny any (30 match(es))
```

Fuente: Propia.

Figura 60. Validación de ACL



Fuente: Propia.

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

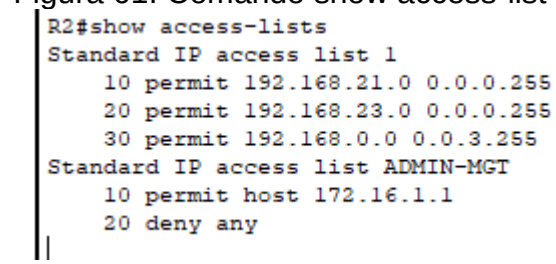
Tabla 26. Comandos para ACL y NAT

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 access-list counters** Este comando se puede utilizar solo o con el número o el nombre de una ACL específica
¿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**

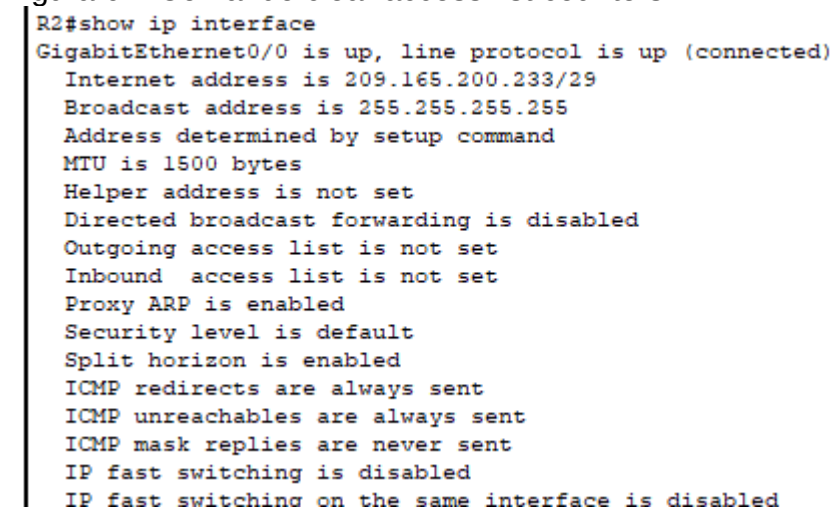
Fuente: Propia.

Figura 61. Comando show access-list



Fuente: Propia.

Figura 62. Comando clear access-list counters



Fuente: Propia.

Figura 63. 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        ---                ---
```

Fuente: Propia.

CONCLUSIONES

Con el desarrollo de esta prueba de habilidades se pudo conocer y aplicar cada uno de los comandos requeridos en cada una de las situaciones presentadas, evidenciar la importancia de los procesos de configuración de routers y switches para un buen proceso de enrutamiento y un excelente funcionamiento de la red.

Además, se diseñó el esquema de direccionamiento IPv4 para las LAN propuestas, las cuales ayudaron a comprender su aplicación y sus ventajas, en cuanto a seguridad y rendimiento de la red, así como también trabajar con una topología que contaba con IPv4 e IPv6 al mismo tiempo.

Se puede concluir que fue muy importante la práctica de este laboratorio ya que con estos dos escenarios se pudieron conocer y aplicar diferentes comandos requeridos para diferentes situaciones, que ayudaron a afianzar los conocimientos de 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).

Es muy útil a la hora de realizar este tipo de ejercicios el empleo del software packet tracert y SmartLab., ya que muestra un entorno bastante parecido al real, siendo muy importante para el entrenamiento de administración de una red.

BIBLIOGRÁFIA

ARIGANELLO, Ernesto. Redes cisco. Guía de estudio para la certificación CCNA Routing y Switching. Madrid. Grupo Editorial RA-MA. (2016). 508 p.

BARBANCHO CONCEJERO, Julio, BENJUMEA MONDÉJAR, Jaime, RIVERA ROMERO, Octavio, ROMERO TERNERO, Mª del Carmen, ROPERO RODRÍGUEZ, Jorge, SÁNCHEZ ANTÓN, Gemma, SIVIANES CASTILLO, Francisco. Redes locales. Ediciones Paraninfo, SA. (2020). 271 p.

GARCÍA APARICI, José. Características de las redes de área local. {En línea}. {Consultado el 6 de noviembre 2021}. Disponible en: https://publicacionesdidacticas.com/hemeroteca/articulo/084027

ICONTEC INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma técnica colombiana NTC 1486: documentación. Presentación de tesis, trabajos de grado y otros trabajos de investigación. Icontec. (2008). 41 p.

NUÑEZ MATUREL, Lissette. Interconexión de las redes mediante enrutadores. Cuba. Centro Nacional de Genética Medica. (2013). 18 p.

VALENCIA ARRIBAS, Francisco. (2011). Manual Básico de Configuración de Redes Cisco. Madrid. Francisco Valencia Arribas. (2009). 212 p.