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

LISTER ANDRES CRUZ ERASO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA SISTEMAS
SAN JUAN DE PASTO
2021

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

LISTER ANDRES CRUZ ERASO

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

DIRECTOR:
MSc. NANCY AMPARO GUACA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA –ECBTI
INGENIERÍA SISTEMAS
SAN JUAN DE PASTO
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

SAN JUAN DE PASTO, 1 de diciembre de 2021

AGRADECIMIENTOS

A Dios por haberme dado todo lo que tengo en este momento, Él me ha premiado con una familia tan maravillosa como la que tengo y me ha brindado mil oportunidades para poder superarme y ser su orgullo hoy en día. A mi mamá porque me ha dado lo mejor, Por sus valiosos consejos y por brindarme amor, porque ella es lo más importante en mi vida y la amo demasiado.

Este es un triunfo que he logrado gracias al esfuerzo de Ella. A mi hermana Sandra, la personita que me comprendió, que fue siempre incondicional conmigo, que compartió mis momentos felices y tristes, y que me apoyó cuando la necesité. A mi compañera Nayibe Ijaji, por todos los momentos difíciles que tuvimos que pasar y las anécdotas que nos quedan de recuerdo, a mis amigos, compañeros, familiares y demás personas que siempre fueron un apoyo y una mano amiga en los momentos difíciles; siempre los llevaré en mi corazón.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Cisco CCNA: (Cisco Certified Networking Associate): Es una de las certificaciones más importantes dentro de la industria de la Tecnología de la Información. Esta certificación representa el nivel asociado, orientada a habilidades prácticas en el diagnóstico y solución de problemas específicos de redes Open Shortest Path First (OSPF) es un protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta (SPF). OSPF es un protocolo de pasarela interior (IGP)

.

Cisco Packet Tracer: Es un potente programa de simulación de red que permite a los estudiantes experimentar con el comportamiento de la red.

Packet Tracer: complementa equipo físico en el aula, al permitir a los estudiantes a crear una red con un número casi ilimitado de dispositivos, fomentar la práctica, el descubrimiento y solución de problemas.

RED: es un conjunto de equipos nodos y software conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios

ROUTER: permite interconectar computadoras que funcionan en el marco de una red, se encarga de establecer qué ruta se destinará a cada paquete de datos dentro de una red informática.

SWITCH: que son los encargados de la interconexión de equipos dentro de una misma red, o lo que es lo mismo, son los dispositivos que, junto al cableado, constituyen las redes de área local o LAN.

RESUMEN

El diplomado en CCNA permite adquirir conocimientos teóricos y prácticos en la implementación de redes de conocimientos básicos en electrónicas basados en redes informáticas y la forma de administrar los enrutadores y computadores de diferentes topologías asociadas a networking.

Este documento se centra en conocimientos, habilidades y soluciones encontrados a lo largo del proceso. En el primer escenario se construye una red, en la el esquema de direccionamiento IPV4 de LAN1 Y LAN2, está configurado y administrado de manera segura que permita probar la conectividad entre las equipos de cómputo. El segundo escenario próximo Escenario se configura una red que debe admitir conexiones IPv4 y IPv6, para garantizar la seguridad de los equipos VLAN y el protocolo de enrutamiento OSPF dinámico de configuración dinámica de host (DHCP), las direcciones de red (dinámica y estática) verifican Servidor / cliente de Access (ACL) y Network Time Protocol (NTP), y finalmente Utilice comandos CLI comunes para probar la conexión y registrar la red.

En el desarrollo del primer escenario también se realiza configuraciones en el routing, switching y equipos que admitan conmutación de IPV4, para diferentes hosts soportados, el switch también debe estar administrado de manera permanente con el fin de tener enrutamiento VLAN- DHCP, Etherchannel y port – security y establecer redes electrónicas

Palabras claves: CISCO, CCNA, conmutación, enrutamiento, redes, electrónicas

ABSTRACT

The diploma in CCNA allows to acquire theoretical and practical knowledge in the implementation of networks of basic knowledge in electronics based on computer networks and how to manage routers and computers of different topologies associated with networking.

This document focuses on knowledge, skills, and solutions found throughout the process. In the first scenario, a network is built, in the IPV4 addressing scheme of LAN1 AND LAN2, it is configured and managed in a secure way that allows testing the connectivity between the computer equipment. The second next scenario Scenario is configuring a network that must support IPv4 and IPv6 connections, to ensure the security of the VLAN computers and the dynamic host configuration (DHCP) OSPF routing protocol, the network addresses (dynamic and static) verify Access Server / Client (ACL) and Network Time Protocol (NTP), and finally Use common CLI commands to test the connection and register the network.

In the development of the first scenario, configurations are also made in the routing, switching and equipment that support IPV4 connectivity, for different supported hosts, the switch must also be permanently managed in order to route VLAN- DHCP, Etherchannel and port - security and establish electronic networks

Keywords: CISCO, CCNA, Routing, Swicthing, Networking, Electronics.

INTRODUCCIÓN

Mediante el desarrollo de la guía de actividades del diplomado CISCO, se ha comprobado todo el conocimiento adquirido en base al curso, el cual supera desarrollar ejercicios teóricos a modelo práctico para permitir a estudiantes conocer fortalezas y debilidades con temas de estudio en redes. Después de completar este proceso, todo en grupo podrá interactuar con sus compañeros conociendo diferentes opiniones de aprendizaje y definir el proceso de los ejercicios a desarrollar.

Debido al método de aprendizaje de este curso, permite a los estudiantes desarrollar un sentido de análisis de las cosas para obtener una nueva base para el desarrollo profesional. Cada alumno, de la misma forma, mediante el uso de un simulador de seguimiento de paquetes, explora cada elemento del dispositivo de cada ejercicio, lo que permite es adquirir nuevos conocimientos, habilidades y destrezas en el desarrollo académico, personal y profesional.

En el cuerpo del informe se desprende que el trabajo realizado se utiliza los diferentes temas del curso CISCO para realizar la aplicación directamente en respuesta a la situación dada por la guía del curso

ESCENARIO 1

Figura 1. Topología del escenario 1

Fuente: Guía de actividades

1.1 Esquema de direccionamiento

En este primer escenario se configurarán los dispositivos de una red pequeña, se debe configurar un router, un switch y equipos que permitan conectividad de IPV4 como IPV6 para los diferentes Hots soportados.

Para la dirección ipv4 se utiliza la dirección IP 192.168. x.0, donde x corresponde a los dos últimos números de mi cédula.

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.

Parte 2: Desarrolle 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 (1086223766).

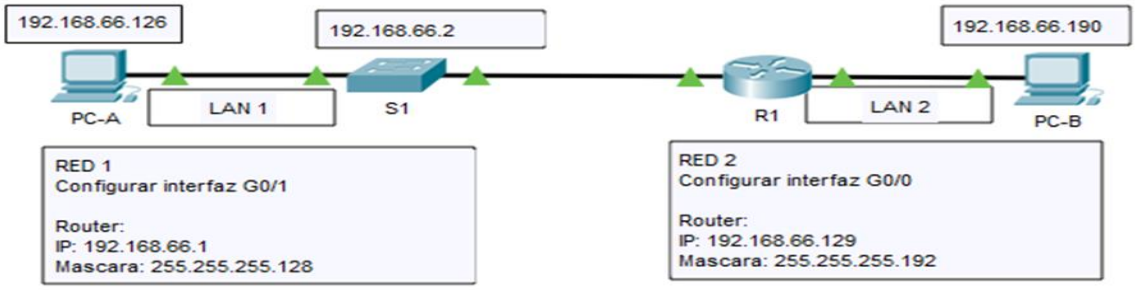
En la siguiente tabla podemos identificar la dirección IP de la red empleando el número de cédula.

Tabla 1. Requerimientos

Ítem	Requerimiento
Dirección de Red	LAN 1 192.168.66.0 255.255.255.128 LAN 2 192.168.66.128 255.255.255.128
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50

Fuente: Autoría propia

Figura 2. Simulación de escenario 1



Fuente: Autoría propia

Tabla 2. Direcciones IP

Dirección de Red	192.168.66.0/25
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
Dirección de Red	LAN 1 192.168.66.0/25 255.255.255.128 LAN 2 192.168.66.128/26 255.255.255.192
R1 G0/0/1	Primera dirección de host de la subred **LAN1** 192.168.66.1 255.255.255.128
R1 G0/0/0	Primera dirección de host de la subred **LAN2** 192.168.66.129 255.255.255.192
S1 SVI	Segunda dirección de host de la subred **LAN1** 192.168.66.2 255.255.255.128
PC-A	Última dirección de host de la subred **LAN1** 192.168.66.126 255.255.255.128
PC-B	Última dirección de host de la subred LAN2 192.168.66.190 255.255.255.192

Fuente: Autoría propia

Parte 3: Configure aspectos básicos

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

Parte 1: Inicializar, Cargar y Configurar aspectos básicos de los dispositivos

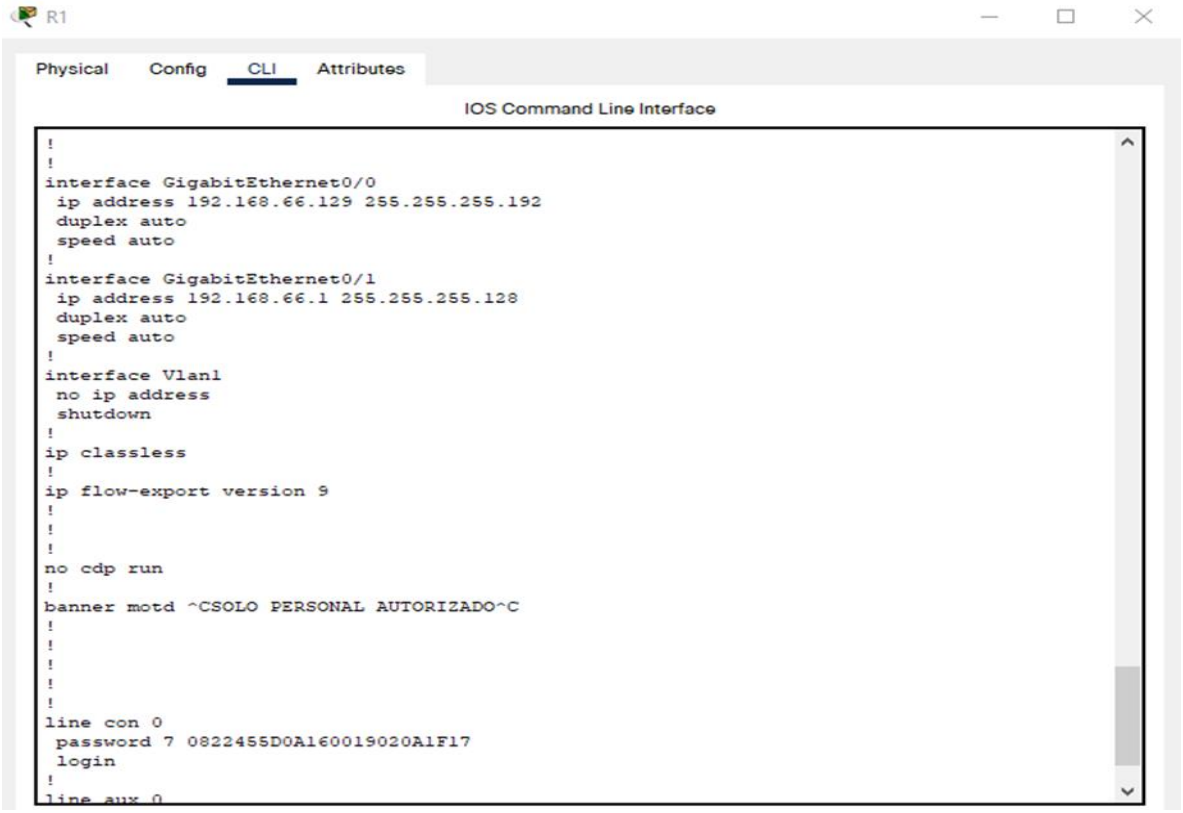
Tabla 3. Configuración para el Router 1

Tarea	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router R1	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 ciscoenpass
Contraseña de acceso a la consola ciscoenpass	R1(config)#line con 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas 10 caracteres	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local Nombre usuario: admin Password: admin1pass	R1(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	R1(config)#line vty 0 4 R1(config-line)#transport input ssh R1(config-line)#login local R1(config-line)#exit
Configure un MOTD Banner	R1(config)#banner motd # Solo personal Autorizado, Ingrese Password #

Configurar interfaz G0/0/0	R1(config)#description HACIA PCB R1(config)#int GigabitEthernet0/0/0 R1(config-if)#ip add 192.168.66.129 255.255.255.192 R1(config-if)#no shutdown R1(config-if)#exit
Configurar interfaz G0/0/1	R1(config)#int GigabitEthernet0/0/1 R1(config)#ip add 192.168.66.1 255.255.255.128 R1(config-if)#no shutdown R1(config-if)#exit

Fuente: Autoría propia

Figura 3. Configuración básica R1



Fuente: Autoría propia

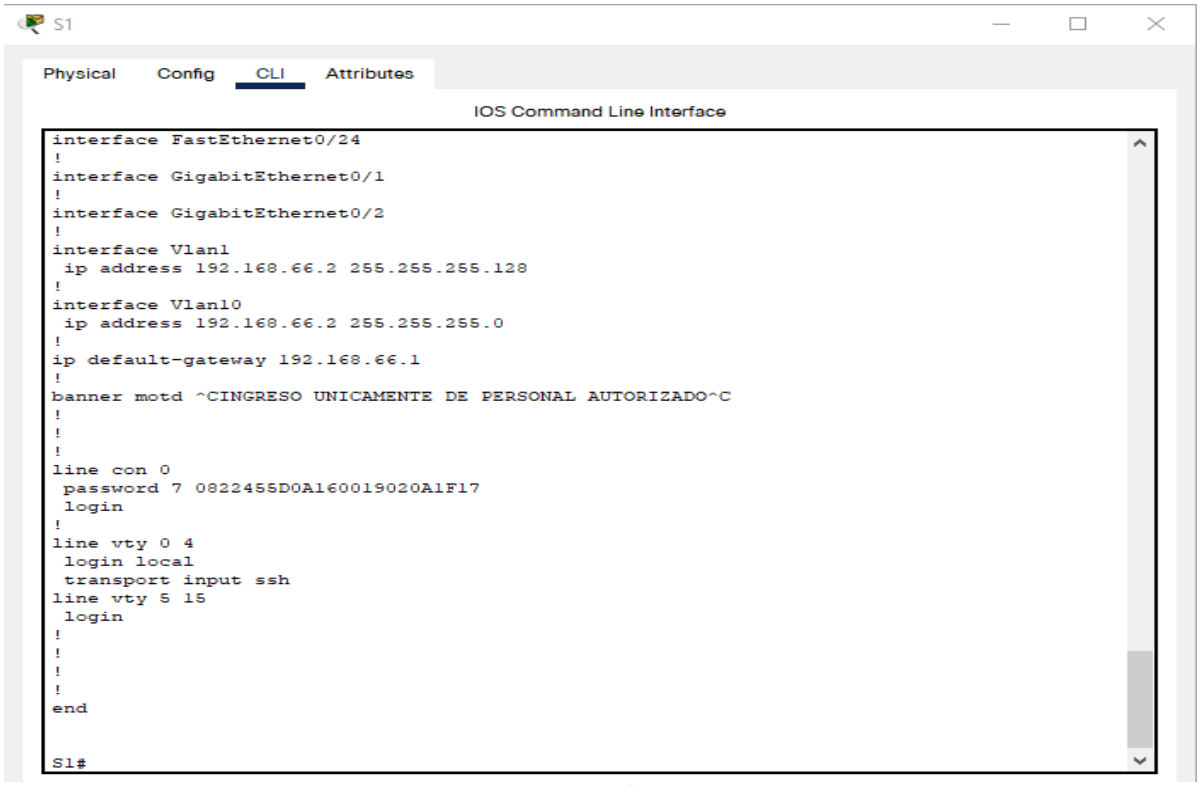
Configuración S1

Tabla 4. Configuración de switch

Desactivar la búsqueda DNS.	S1(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio	S1(config)#ip domain-name CCNA-Lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line con 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	S1(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY	S1(config)#line vty 0 15 S1(config-line)#login local S1(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)#line vty 0 15 S1(config-line)#transport input ssh S1(config-line)#login local S1(config-line)#exit
Configure un MOTD Banner	R1(config)#banner motd # Solo personal Autorizado, Ingrese Password #
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa general-keys modulus 1024
Configurar la interfaz de administración (SVI)	S1(config)#interface vlan 1 S1(config-if)#ip address 192.168.66.2 255.255.255.128 S1(config-if)#no sh S1(config-if)#exit
Configuración del gateway	S1(config)#ip default-gateway 192.168.66.1

Fuente: Autoría propia

Figura 4. Configuración básica S1



Fuente: Autoría propia

Paso 2. Configurar los equipos

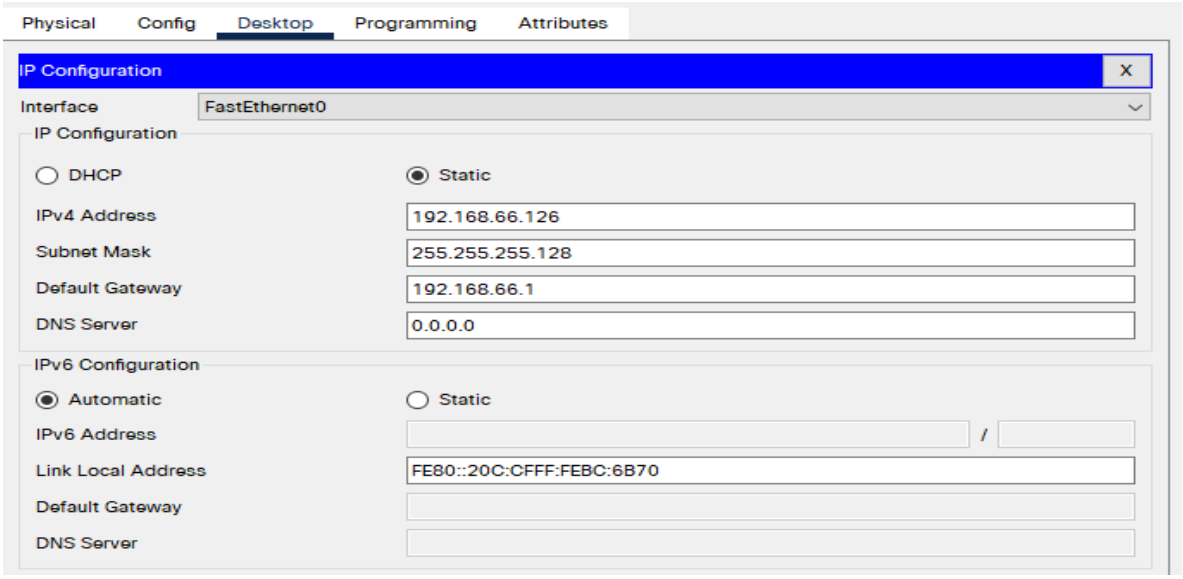
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all**.

Tabla 5: Configuración de equipos Host PC-A

PC-A Network Configuration	
Descripción	Pertenece a LAN 1
Dirección física	000C.CFBC.6B70
Dirección IP	192.168.66.126
Mascara de subred	255.255.255.128
Gateway predeterminado	192.168.66.1

Fuente: Autoría propia

Figura 5. Dirección PC A



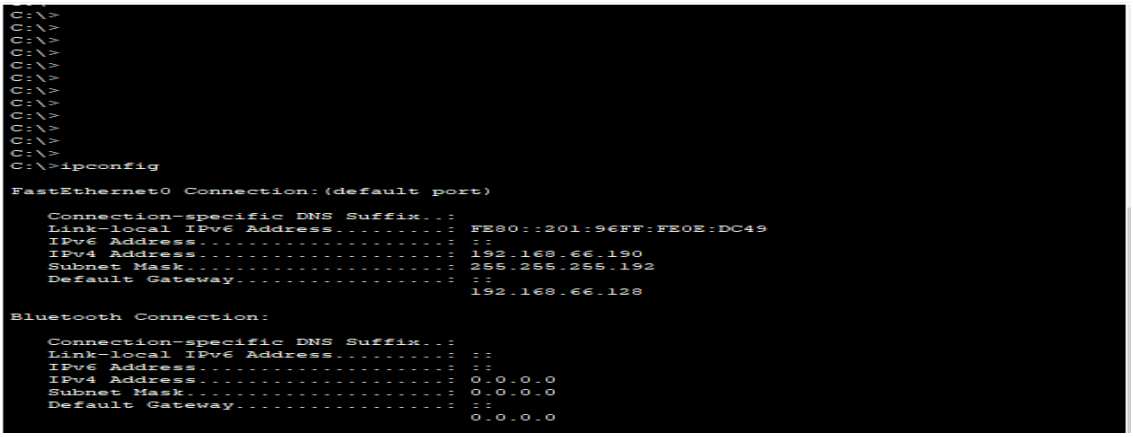
Fuente: Autoría propia

Tabla 6: PC-B Network Configuration

PC- PC-B Network Configuration	
Descripcion	Pertenece a LAN 1
Mac	000.0CCB.B9A0
Direccion IP	192.168.66.190
Mascara de subred	255.255.255.192
Gateway predeterminado	192.168.66.128

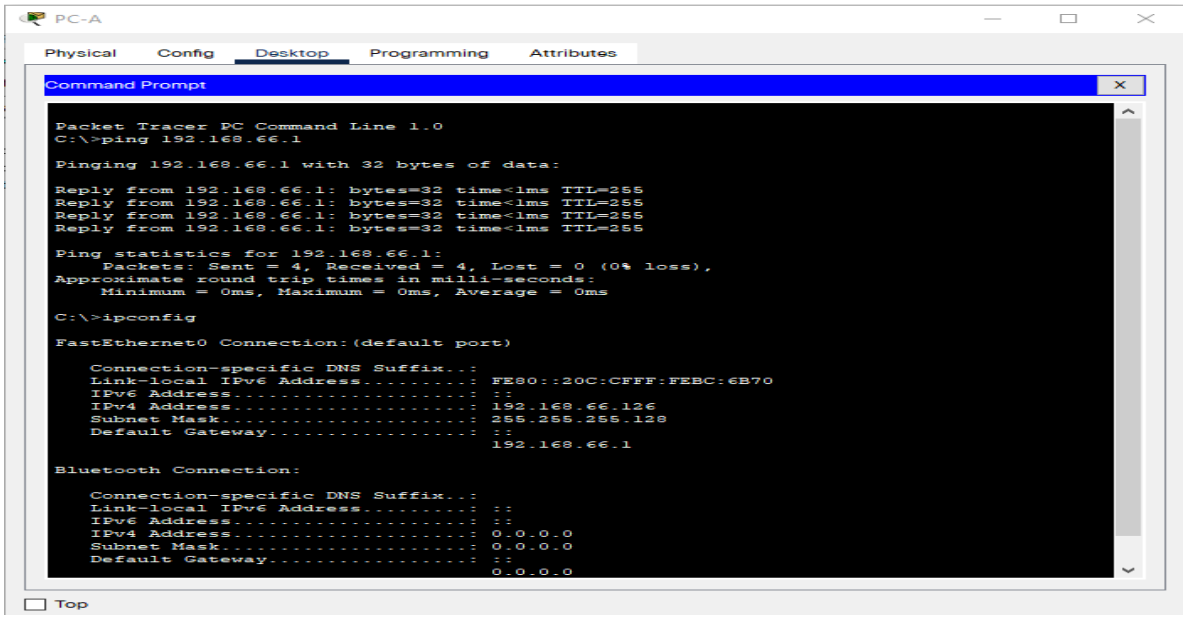
Fuente: Autoría propia

Figura 6. Dirección PC B



Fuente: Autoría propia

Figura 7. Ping de PC-A a R1 G0/0/1

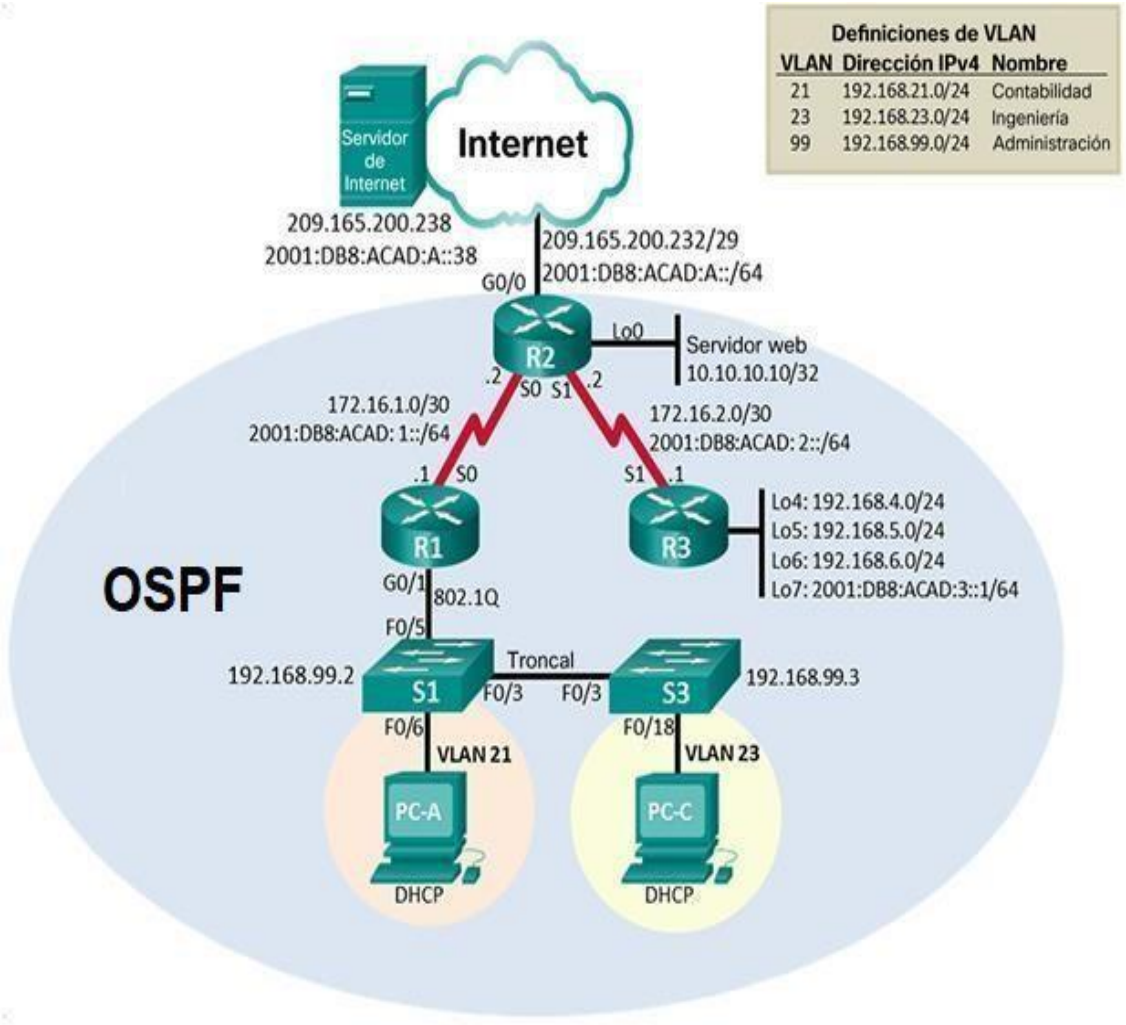


Fuente: Autoría propia

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 8. Topología escenario 2



Fuente: Guía de actividades

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.

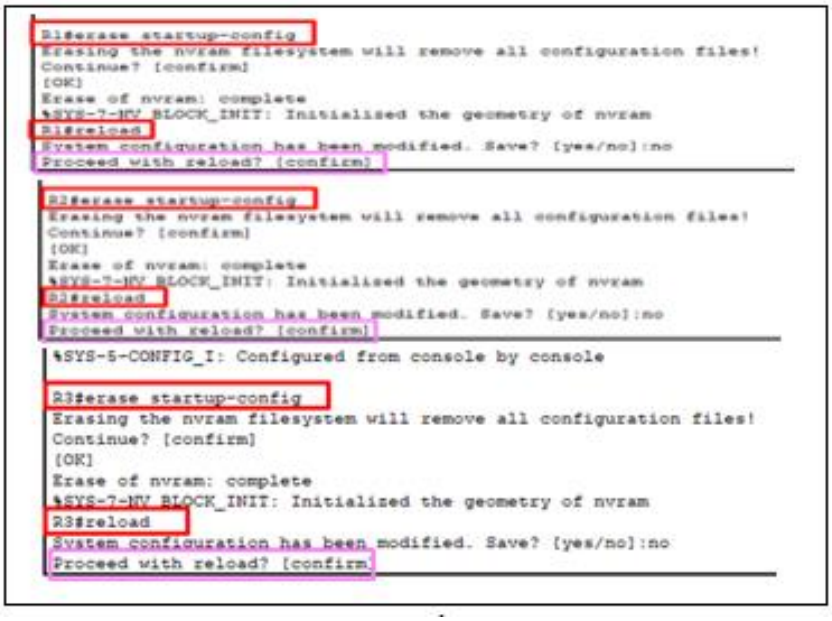
Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 7. Reinicio de dispositivos

Actividad	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>enable Router#erase Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete
Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm]
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch#erase sta Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete
Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm]
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>enable Switch#show flash: Directory of flash:/ 1 -rw- 4414921 <no date> c2960-lanbase- mz.122-25.FX.bin 64016384 bytes total (59601463 bytes free) Switch#

Fuente: Autoría propia

Figura 9. Reinicio de dispositivos



Fuente: Autoría propia

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

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

Tabla 8: Configuración de internet en el PC

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::2/64
Gateway predeterminado Ipv6	2001:DB8:ACAD:A::1

Fuente: Autoría propia

Paso 2: Configurar R1

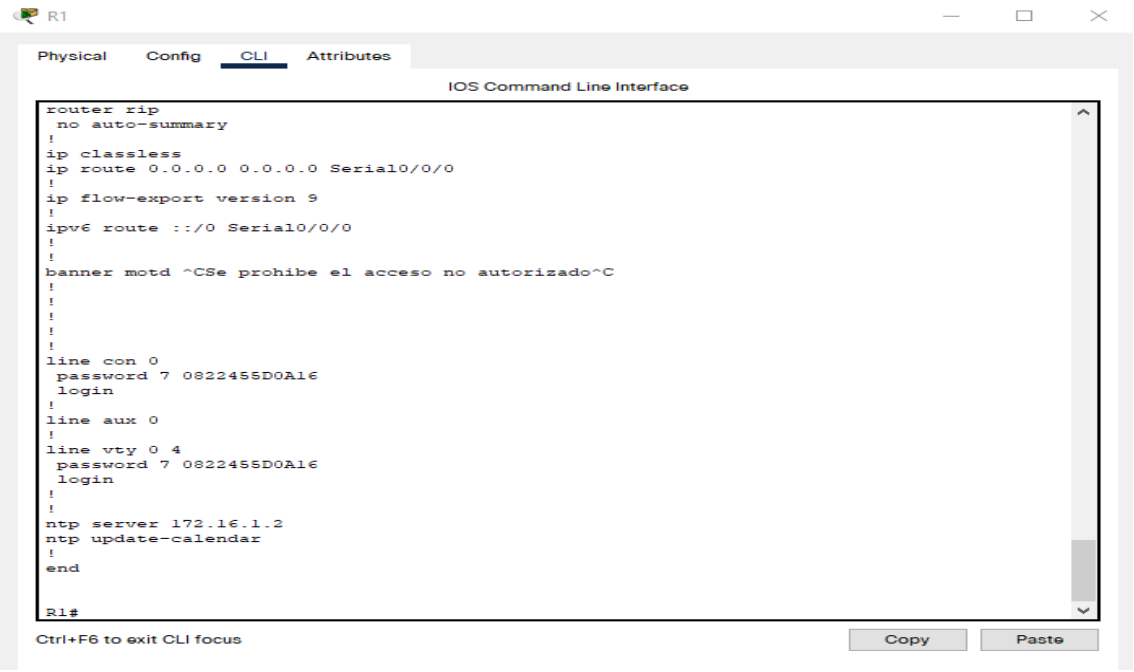
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 9: Configuración R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router 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 con 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet cisco	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD “Se prohíbe el acceso no autorizado”	R1(config)#banner motd #Se prohibe el acceso no autorizado# R1#
Interfaz S0/0/0	R1(config)#interface serial 0/0/0 R1(config-if)#description R1 a R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config-if)#exit
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0 R1(config)#ipv6 unicast-routing R1(config)#

Fuente: Autoría propia

Figura 10. Configuración básica R1 Escenario 2



Fuente: Autoría propia

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 10. Configuración de router R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router 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 con 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit

Contraseña de acceso Telnet **cisco**	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 soportado en packet tracer
Mensaje MOTD “Se prohíbe el acceso no autorizado”	R2(config)#banner motd #Se prohibe el acceso no autorizado# R2(config)#
Interfaz S0/0/0	R2(config)#interface serial 0/0/0 R2(config-if)#description R1 a R2 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown R2(config-if)# R2(config-if)#exit
Interfaz S0/0/1	R2(config)#interface serial 0/0/1 R2(config-if)#description R2 a R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown R2(config-if)#exit
Interfaz G0/0 (simulación de Internet)	R2(config)#interface gigabitEthernet 0/0 R2(config-if)#description R2 to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown R2(config-if)#exit
Interfaz loopback 0 (servidor web simulado)	R2(config)#interface lo0 R2(config-if)# R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#exit

Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 giga 0/0 R2(config)#ipv6 route ::/0 gigabitEthernet 0/0 R2(config)#

Fuente: Autoría propia

Figura 11. Configurar OSPF en R2

```
User Access Verification

Password:

R2>enable



R2(config)#interface serial 0/0/0
R2(config-if)#description R1 a R2
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64
R2(config-if)#no shutdown
R2(config-if)#exit
```

Fuente: Autoría propia

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

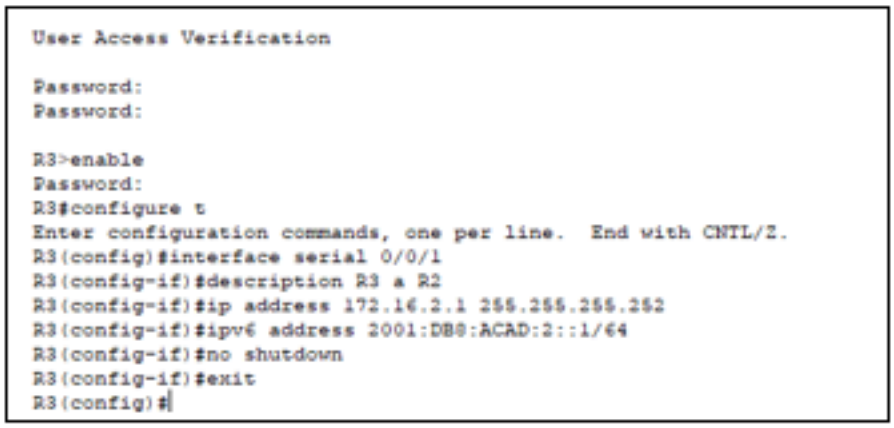
Tabla 11. Configuración R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router R3	Router(config)#hostname R3
Contraseña de exec privilegiado	R3(config)#enable secret class
Contraseña de acceso a la consola **cisco**	R3(config)#line con 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit

Contraseña de acceso Telnet cisco	R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Cifrar las contraseñas	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #Se prohibe el acceso no autorizado#
Interfaz S0/0/1	R3(config)#interface serial 0/0/1 R3(config-if)#description R3 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)# R3(config-if)#exit
Interfaz loopback 4	R3(config)#interface lo4 R3(config-if)# R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 5	R3(config)#interface lo5 R3(config-if)# R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 6	R3(config)#interface lo6 R3(config-if)# R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 7	R3(config)#interface lo7 R3(config-if)# R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#exit R3(config)#ipv6 unicast-routing R3(config)#
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

Fuente: Autoría propia

Figura 12. Configurar R3



Fuente: Autoría propia

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes actividades:

Tabla 12. Configuración Switch 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 S1(config)#
Contraseña de acceso a la consola	S1(config)#line con 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Contraseña de acceso Telnet	S1(config)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Cifrar las contraseñas	S1(config)#service password-encryption

Mensaje MOTD	S1(config)#banner motd #Se prohibe el acceso no autorizado# S1(config)#

Fuente: Autoría propia

Figura 13. Configuración del switch 1

```
Se prohibe el acceso no autorizado

User Access Verification

Password:
Password:

S1>enable
Password:
S1#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#no ip domain-lookup
S1(config)#hostname S1
S1(config)#enable secret class
```

Fuente: Autoría propia

Paso 6: Configuración del S3

La configuración del S3 incluye las siguientes tareas:

Tabla 13. Configuración Switch s3

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

Contraseña de acceso Telnet	S3(config)#line vty 0 15 S3(configline)#password cisco S3(config-line)#login
Cifrar las contraseñas	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd #Se prohibe el acceso no autorizado#

Fuente: Autoría propia

Figura 14. Configuración de S3

```
Press RETURN to get started!

Se prohibe el acceso no autorizado

User Access Verification

Password:

S3>enable
Password:
S3#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#no ip domain-lookup
S3(config)#hostname S3
S3(config)#enable secret class
S3(config)#line con 0 S3
                       ^
```

Fuente: Autoría propia

Paso 7: Verificar la conectividad de la red

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

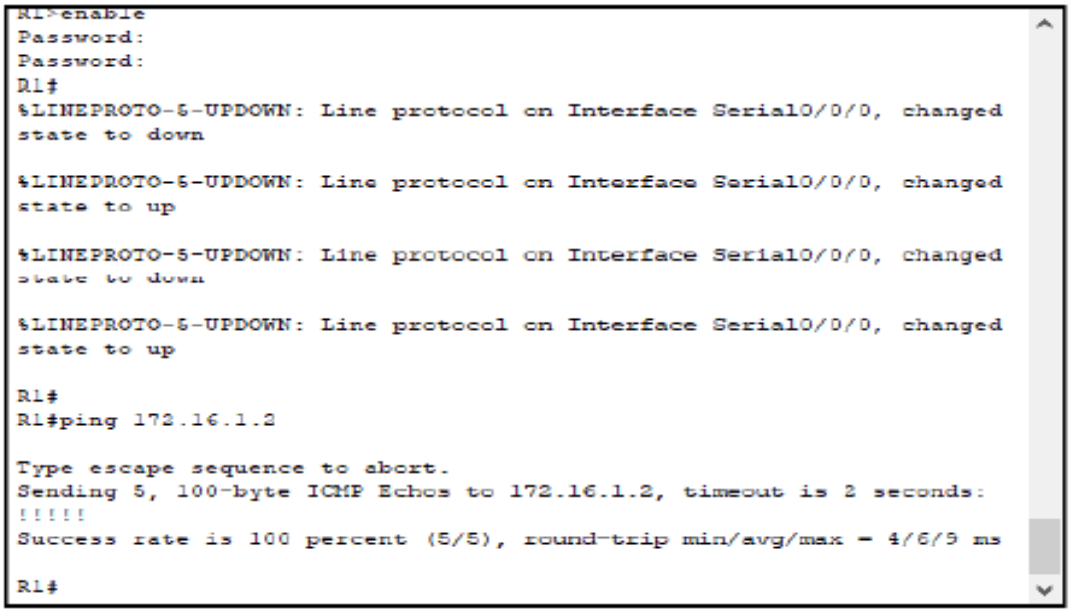
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 14. Verificación de conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/9 ms
R2	R3, S0/0/1	172.16.2.1	Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
PC de Internet	Gateway predeterminado	209.165.200.233	Pinging 2001:DB8:ACAD:A::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255 Ping statistics for 2001:DB8:ACAD:A::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms

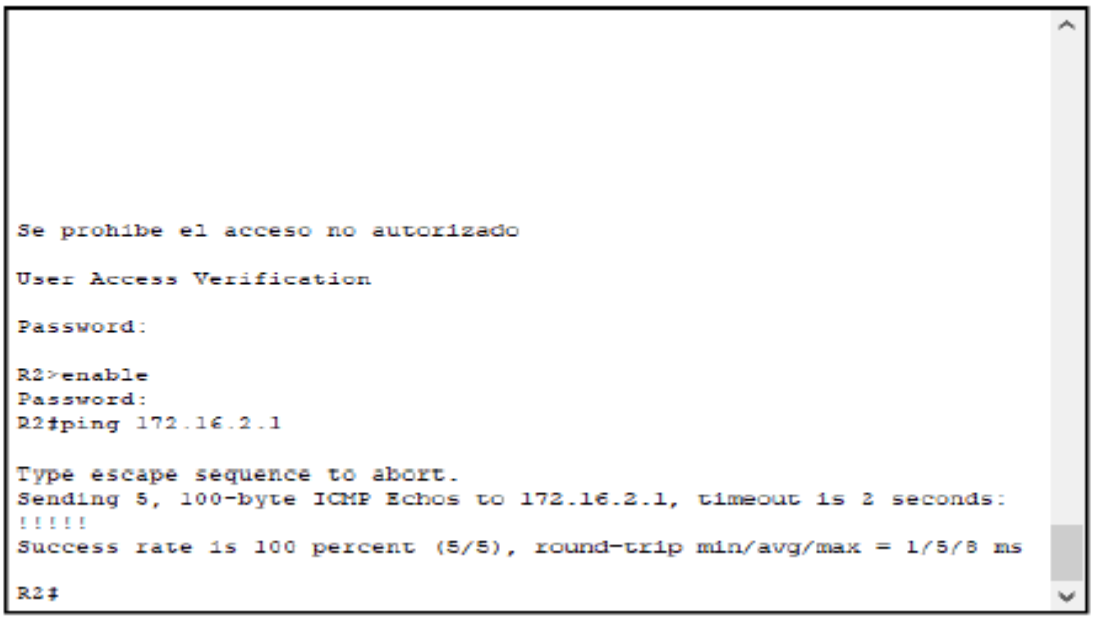
Fuente: Autoría propia

Figura 15. Ping de R1 a R2



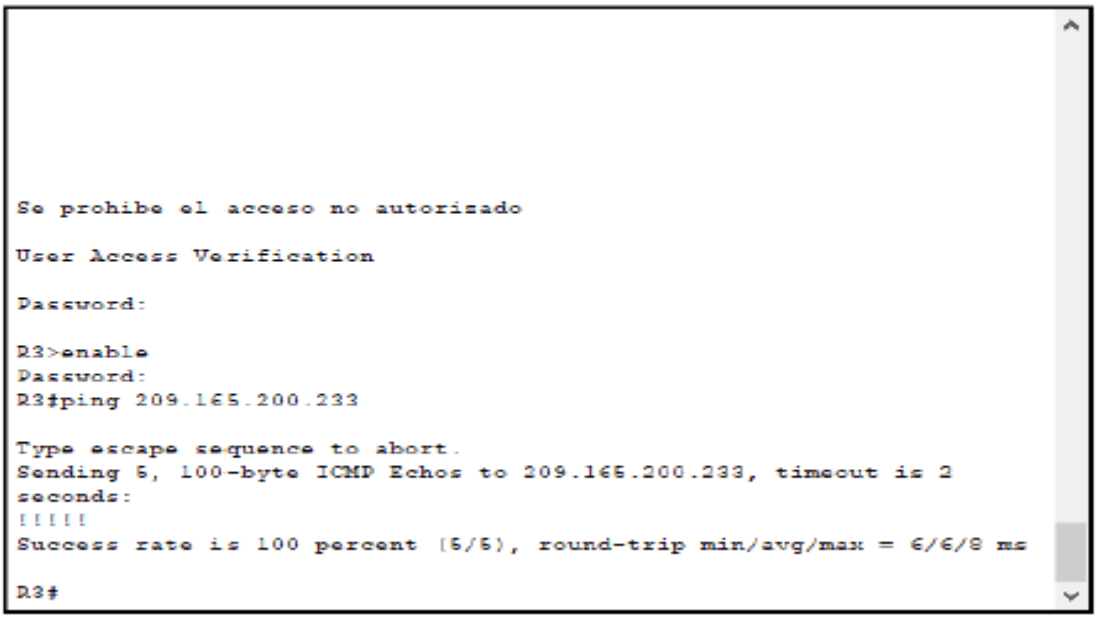
Fuente: Autoría propia

Figura 16. Ping de R2 a R3



Fuente: Autoría propia

Figura 17. Ping de PC de internet a Gateway predeterminado



Fuente: Autoría propia

Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN

La configuración del S1 incluye las siguientes tareas:

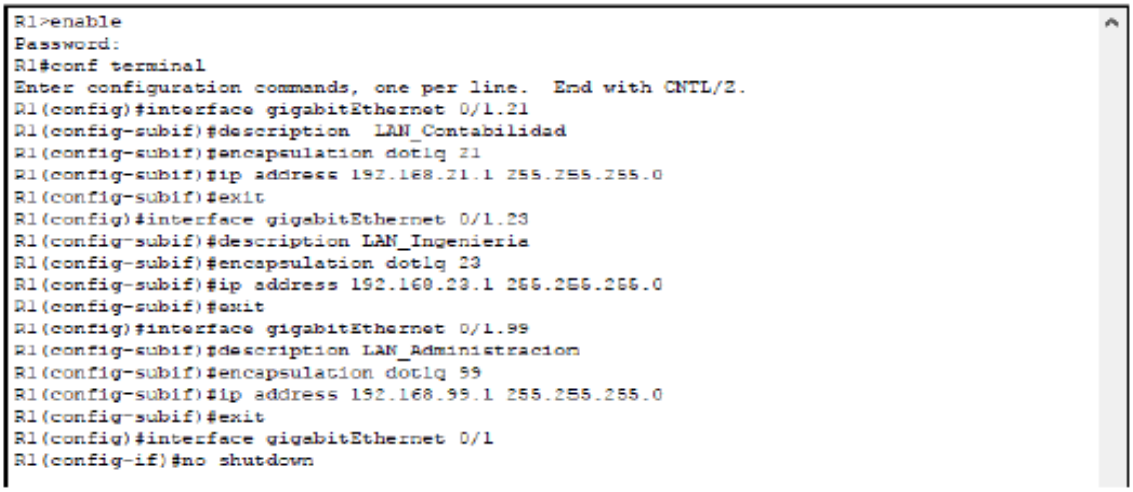
Tabla 15. Configuración de seguridad de switch

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	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

Asignar la dirección IP de administración.	S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
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-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit
Forzar el enlace troncal en la interfaz F0/5	S1(config)#interface fastEthernet 0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	S1(config)#interface range fa0/1-2, fa0/4, fa0/6-24 S1(config-if-range)#switchport mode access S1(config-if-range)#exit
Asignar F0/6 a la VLAN 21	S1(config)#interface range fa0/6 S1(config-if-range)#switchport access vlan 21 S1(config-if-range)#exit
Apagar todos los puertos sin usar	S1(config)#int range f0/1-2,f0/4,f0/7-24,g0/1-2 S1(config-if-range)#shutdown

Fuente: Autoría propia

Figura 18. Configuración de R1 de seguridad



```
R1>enable
Password:
R1#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface gigabitEthernet 0/1.21
R1(config-subif)#description  LAN_Contabilidad
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface gigabitEthernet 0/1.23
R1(config-subif)#description LAN_Ingenieria
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface gigabitEthernet 0/1.99
R1(config-subif)#description LAN_Administracion
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface gigabitEthernet 0/1
R1(config-if)#no shutdown
```

Fuente: Autoría propia

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

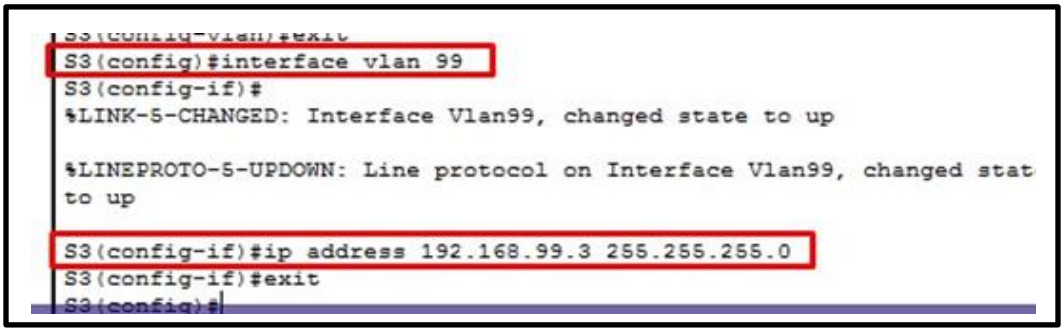
Tabla 16. Configuración S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	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	S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1

Forzar el enlace troncal en la interfaz F0/3	S3(config)#interface fastEthernet 0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	S1(config)#interface range fa0/1-2, fa0/4, fa0/6-24 S1(config-if-range)#switchport mode access S1(config-if-range)#exit
Apagar todos los puertos sin usar	S1(config)#int range f0/1-2,f0/4,f0/7-24,g0/1-2 S1(config-if-range)#shutdown

Fuente: Autoría propia

Figura 19. Configuración de S3 con IP



Fuente: Autoría propia

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

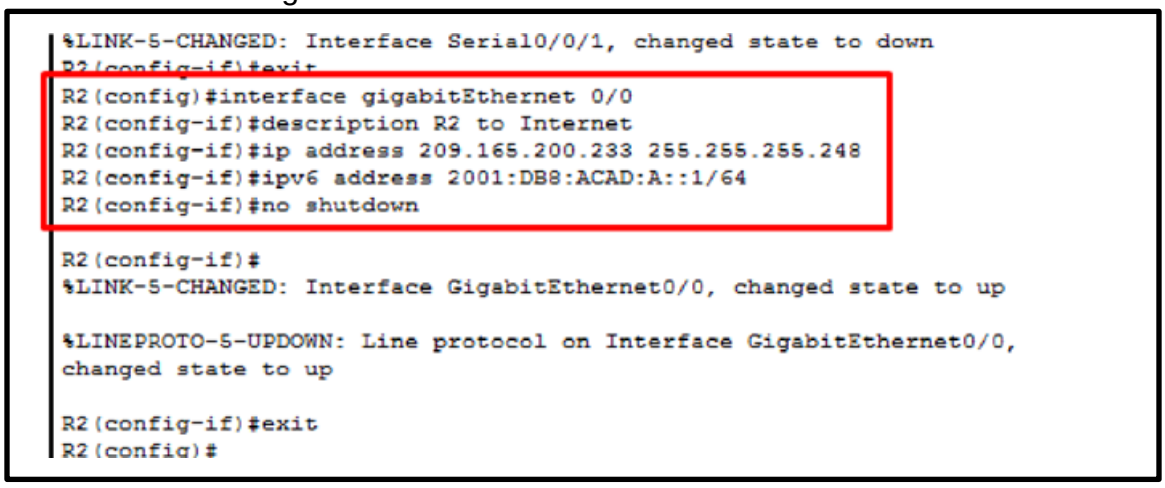
Tabla 17. Configuración R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#interface gigabitEthernet 0/1.21 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	R1(config)#interface gigabitEthernet 0/1.23 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	R1(config)#interface gigabitEthernet 0/1.23 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 gigabitEthernet 0/1 R1(config-if)#no shutdown R1(config-if)#exit

Fuente: Autoría propia

Figura 20. Simulación de internet en la consola



Fuente: Autoría propia

Paso 4: Verificar la conectividad de la red

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

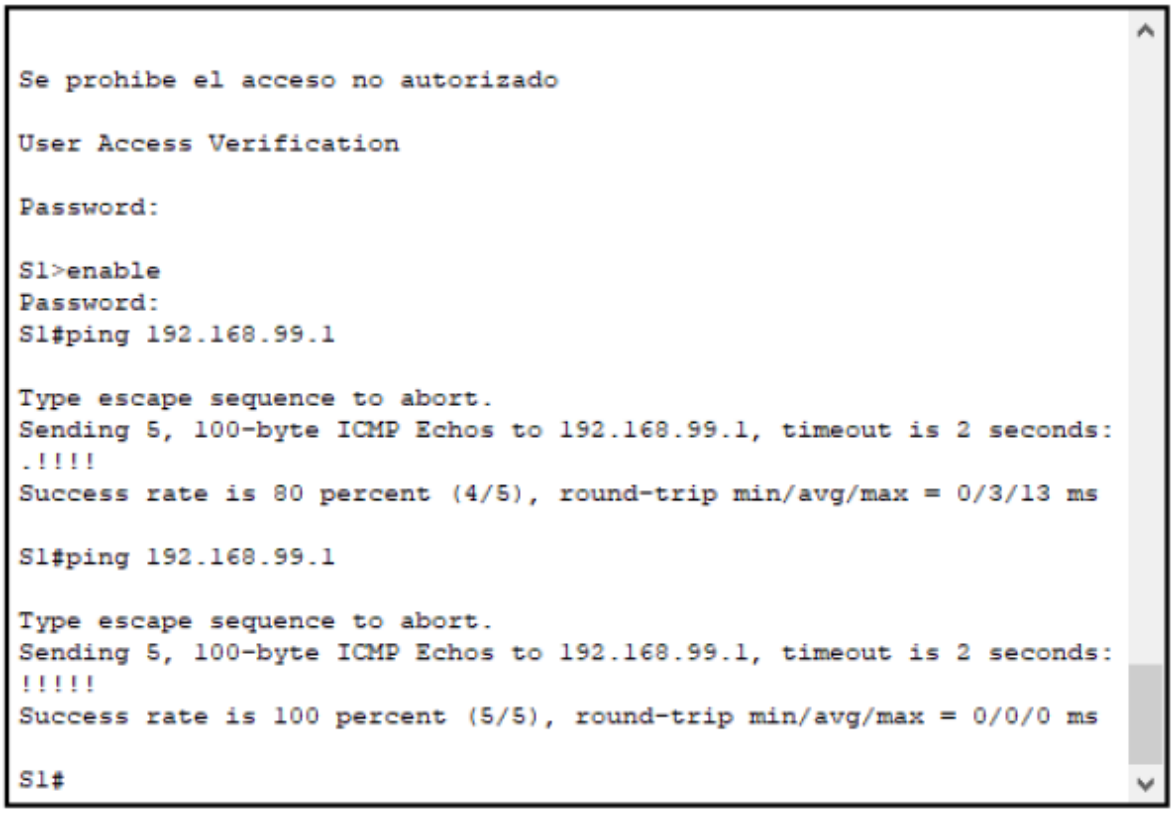
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 18. Verificación de conexión

DESDE	A	DIRECCION IP	RESULTADOS DE PING
S1	R1, dirección VLAN 99	192.168.99.1	S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100- byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 99	192.168.99.1	S3#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100- byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S1	R1, dirección VLAN 21	192.168.21.1	S1#ping 192.168.21.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: Success rate is 100 percent (5/5), round-trip min/avg/max =0/0/0 ms S1#
S3	R1, dirección VLAN 23	192.168.23.1	S3#ping 192.168.23.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: Success rate is 100 percent (5/5), round-trip min/avg/max =0/0/1 ms S3#

Fuente: Autoría propia

Figura 21. Ping en el S1 a VLAN



Fuente: Autoría propia

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

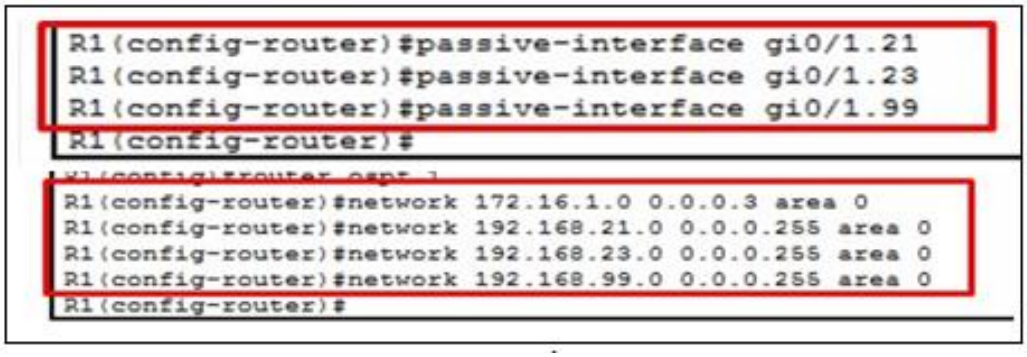
Tabla 19. Configuración OSPF en R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0

Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive- interface gi0/1.21 R1(config-router)#passive- interface gi0/1.23 R1(config-router)#passive- interface gi0/1.99
Desactive la sumarización automática	R1(config-router)#no auto- summary

Fuente: Autoría propia

Figura 22. Configuración de routing dinámico



Fuente: Autoría propia

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

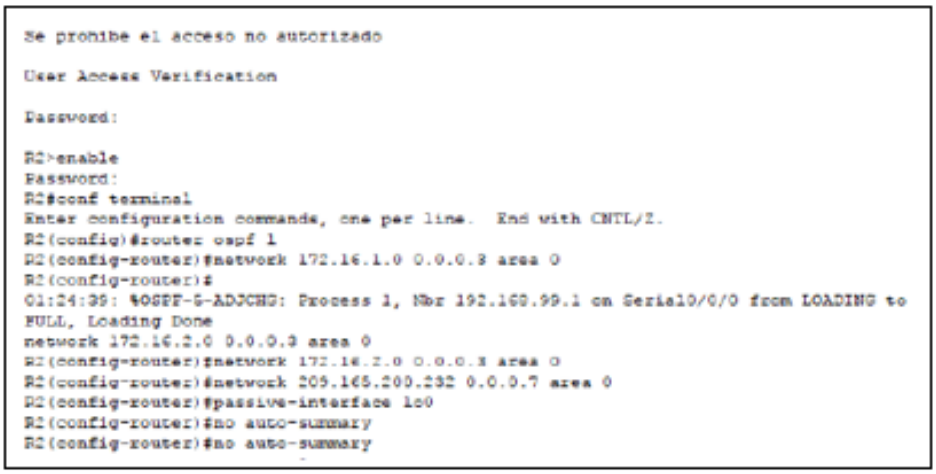
Tabla 20. Configuración OSF en R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1
Anunciar las redes conectadas directamente	R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 209.165.200.232 0.0.0.7 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive- interface lo0

Desactive la sumarización automática.	Aplica solo para RIP

Fuente: Autoría propia

Figura 23. Configuraciòn OSPF en el R2



Fuente: Autoría propia

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 21. Configuración en el R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 1
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 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 lo4 R3(config-router)#passive- interface lo5 R3(config-router)#passive- interface lo6
Desactive la sumarización automática.	Aplica solo para RIP

Fuente: Autoría propia

Figura 24. Configurar OSPFv3 en el R3

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
Se prohibe el acceso no autorizado

R3>
R3>enable
Password:
R3#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
R3(config-router)#
02:29:51: %OSPF-5-ADJCHG: Process 1, Nbr 10.10.10.10 on Serial0/0/1 from LOADING to FULL,
Loading Done
network 192.168.4.0 0.0.0.255 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
R3(config-router)#passive-interface lo4
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo6
R3(config-router)#no auto-summary
```

Fuente: Autoría propia

Paso 4: Verificar la información de OSPF

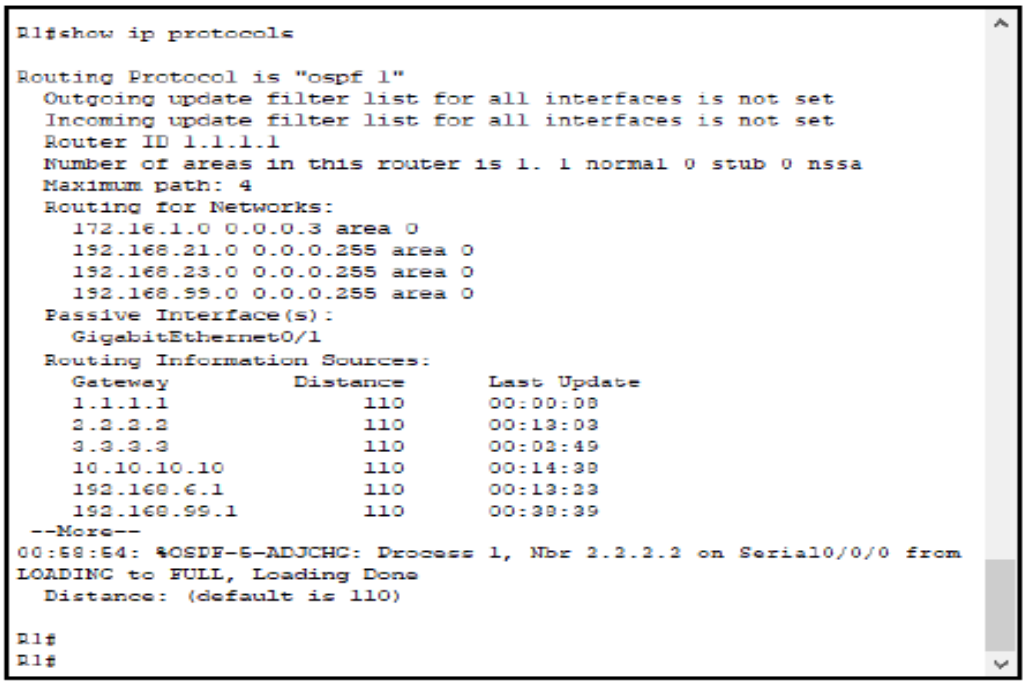
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 22. Verificar información de OSPF

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

Fuente: Autoría propia

Figura 25. Verificar la información de OSPF



Fuente: Autoría propia

Parte 5: Implementar DHCP y NAT para IPv4

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

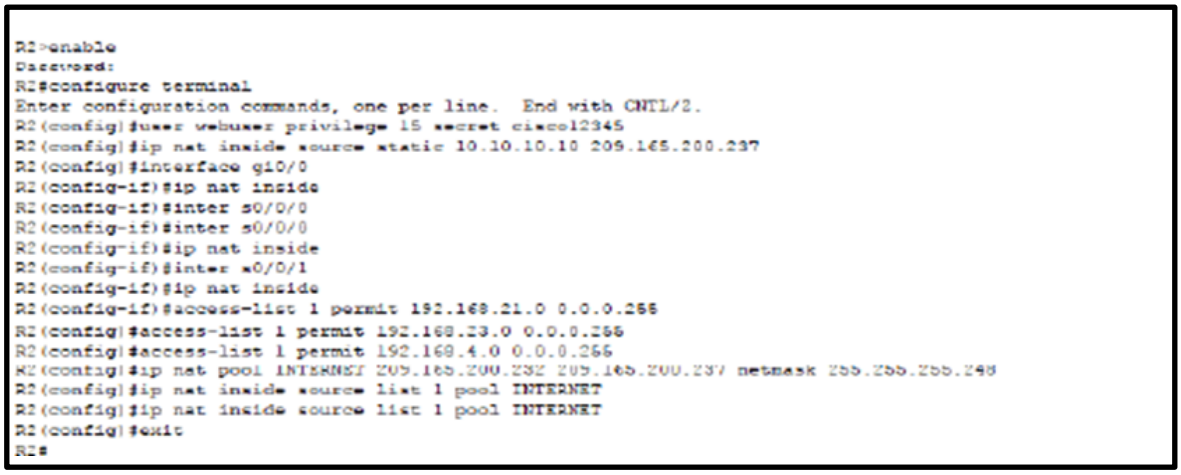
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 23. Configuración R1 para DHCP

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#exit
Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#exit

Fuente: Autoría propia

Figura 26. Configurar R1 como servidor de DHCP



Fuente: Autoría propia

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

La configuración del R2 incluye las siguientes tareas:

Tabla 24. Configuración de NAT

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	No soportado en packet tracert
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	No soportado en packet tracert
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.238
Asignar la interfaz interna y externa para la NAT estática	R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1

	R2(config-if)#ip nat inside R2(config-if)#ex
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.232 209.165.200.237 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Fuente: Autoría propia

Figura 27. Configurar la NAT estática y dinámica en el R2

```
R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#user webuser privilege 15 secret cisco12345
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
R2(config)#interface gi0/0
R2(config-if)#ip nat inside
R2(config-if)#inter s0/0/0
R2(config-if)#inter s0/0/0
R2(config-if)#ip nat inside
R2(config-if)#inter s0/0/1
R2(config-if)#ip nat inside
R2(config-if)#access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255
R2(config)#ip nat pool INTERNET 209.165.200.232 209.165.200.237 netmask 255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#exit
```

Fuente: Autoría propia

Paso 3: Verificar el protocolo DHCP y la NAT estática

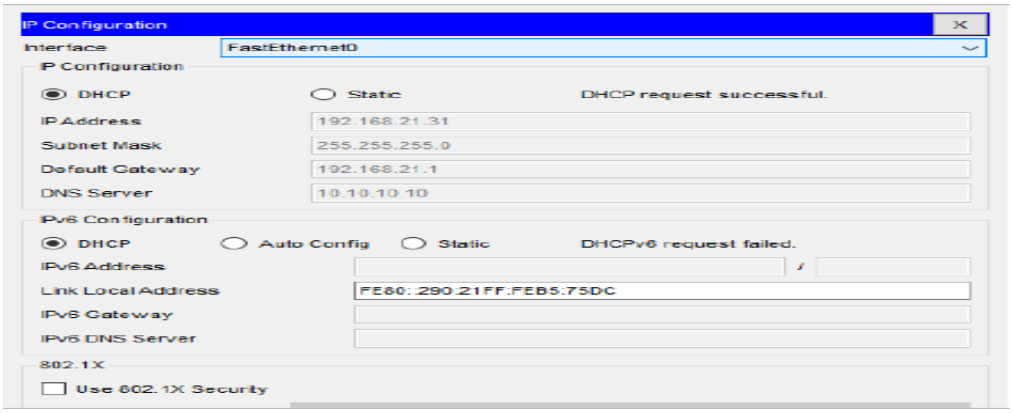
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 25. Configuración de protocolo

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

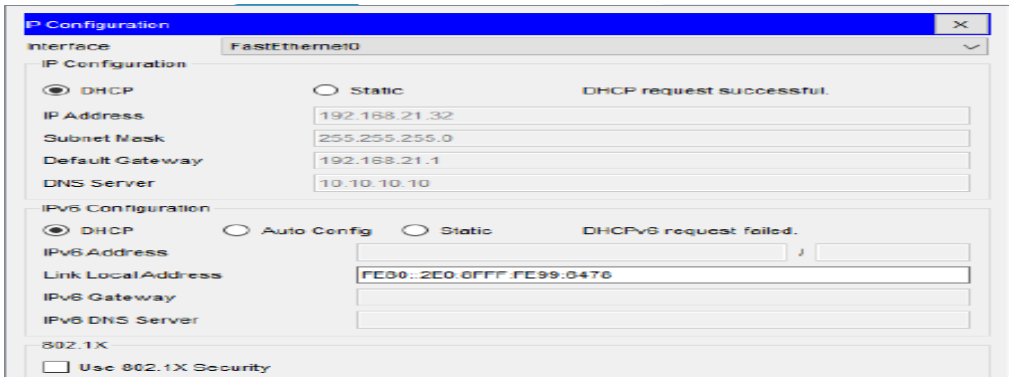
Fuente: Autoria propia

Figura 28. Configuración de PC-A IP con el servidor



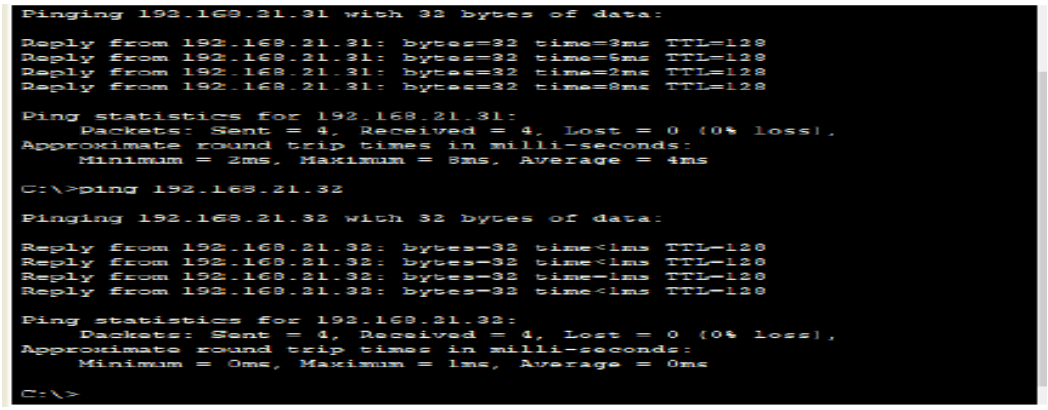
Fuente: Autoría propia

Figura 29. Dirección de PC a DHCP



Fuente: Autoría propia

Figura 30. Verificar ping PC-A a PC-C.



Fuente: Autoría propia

Figura 31. Acceder al servidor web (209.165.200.229)

Fuente: Autoría propia

Parte 6: Configurar NTP

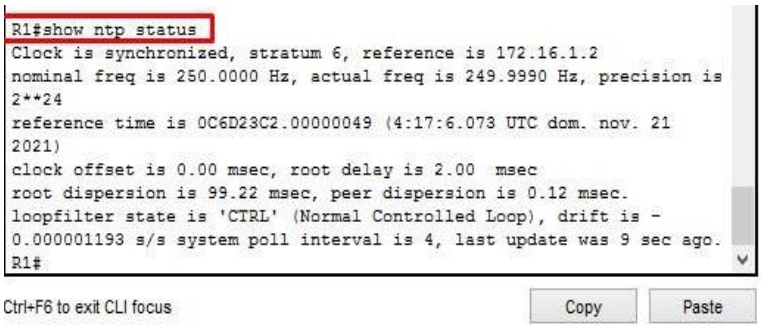
Tabla 26. Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 13:50 04 Dic 2021
Configure R2 como un maestro NTP.	R2(config)#ntp master 5

Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	

Fuente: Autoría propia

Figura 32. Verificación de configuración NTP R1



Fuente: Autoría propia

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

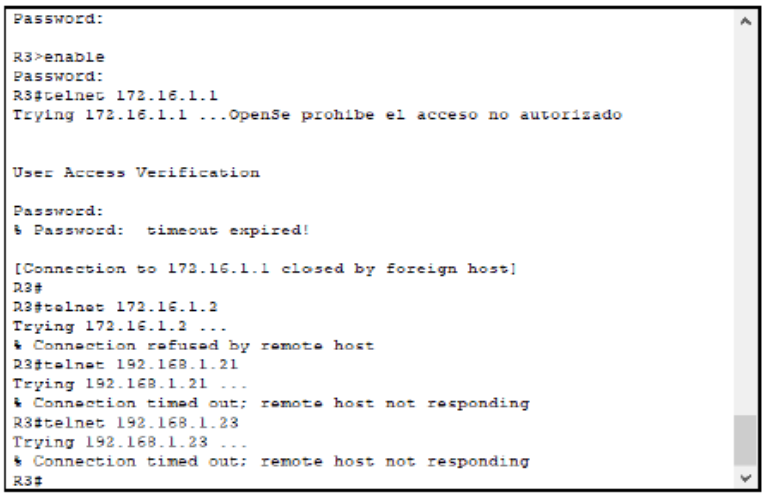
Paso 1. Restringir el acceso a las líneas VTY en el R2

Tabla 27: Configuración de listas de control de acceso

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

Fuente: Autoría propia

Figura 33. Verificación de funcionamiento de la ACL



Fuente: Autoría propia

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

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

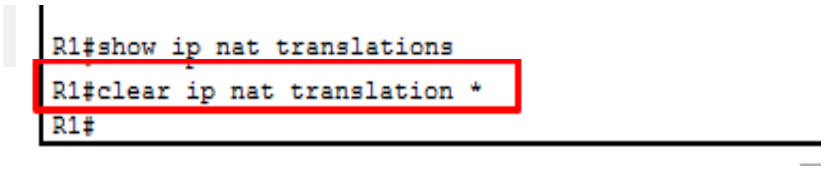
Tabla 28: Lista Acceso desde la última vez que se restableció

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

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

Fuente: Autoría propia

Figura 34. Verificación de funcionamiento lista de acceso



Fuente: Autoría propia

CONCLUSIONES

El curso de CCNA permite validar la capacidad de planificar, implementar, verificar y solucionar problemas de redes empresariales LAN y WAN, así como trabajar de manera conjunta con especialidades de soluciones de: seguridad, voz, inalámbricas y video.

Es importante establecer niveles de seguridad básicos, mediante la definición de criterios y políticas de seguridad aplicadas a diversos escenarios de red, bajo el uso de estrategias hardware y software, con el fin de proteger la integridad de la información frente a cualquier tipo de ataque que se pueda presentar en un instante de tiempo determinado; en especial en soluciones de red que involucren el uso de aplicaciones cliente-servidor.

Los conocimientos generados en el curso, son necesarios para el diseño de redes escalables mediante el uso del modelo jerárquico, con el fin de optimizar el rendimiento de la red e incorporar de manera adecuada el uso de tecnologías y protocolos de conmutación mejorados tales como: VLAN, Protocolo de enlace troncal de VLAN (VTP), Protocolo de árbol de expansión por VLAN (Spanning Tree per VLAN - PVSTP) y encapsulamiento por 802.1q.

Las configuraciones permiten configurar y administrar dispositivos de Networking orientados al diseño de redes escalables y de conmutación, mediante el estudio del modelo OSI, la arquitectura TCP/IP, y el uso de recursos y herramientas en función de los protocolos y servicios de la capa física como soporte de las comunicaciones a través de las redes de datos estableciendo alternativas a problemas de interconectividad.

BIBLIOGRAFIA

CISCO. (2017). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO. (2017). Soluciones de Red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

UNAD (2017). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

CISCO. (2017). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1