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

KIRMAN RAÚL CASAS GUTIÉRREZ

UNIVERSIDAD NACIONAL, ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ECBTI

INGENIERÍA DE SISTEMAS

BOGOTÁ

2021

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

KIRMAN RAÚL CASAS GUTIÉRREZ

Diplomado de opción de grado presentado para optar al

Título de INGENIERO DE SISTEMAS

DIRECTOR(A):

INGENIERA MARIA ALEJANDRA LOPEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICASM TECNOLOGÍA E INGENIERÍA ECTBI

INGENIERÍA DE SISTEMAS

BOGOTÁ

2021

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Noviembre, 2021

AGRADECIMIENTOS

Agradezco a mi familia el apoyo, a la universidad por haberme transmitido los conocimientos y las herramientas para llegar hasta el punto de estar finalizando el proceso como estudiante de pregrado en ingeniería de sistemas.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Dirección IPV4: una dirección IPv4 es un identificador de un host dentro de una red, está compuesto por dos partes, una que representa la red a la que pertenece el host y el otro el identificador del host mismo. Tiene una longitud de 32 bits. (Cisco, 2021)

DHCP: Dinamic Host Configuration Protocol: Es un protocolo cliente/servidor que provee automáticamente una dirección IP, está definido por el RFC 2131 y 2132.

NTP: Network Time Protocol, es un protocolo que se utiliza para sincronizar los relojes de las computadoras que intervienen en una conexión de red. El objetivo, es hacer coincidir las marcas de tiempo entre los distintos dispositivos. Utiliza el modelo cliente – servidor. (techlib, 2021)

OSPF: Open Shortest Path First. Es un protocolo de enrutamiento de estado de enlace, que es usado para entrar la mejor ruta entre la fuente y el destino.

Router: también llamado enrutador o encaminador de paquetes, es un dispositivo que proporciona la conectividad entre redes informáticas, su principal función es guiar y dirigir los datos en la red mediante paquetes. (Cisco, 2021)

Switch: son dispositivos electrónicos diseñados para conectar varios dispositivos como computadores, dispositivos móviles, impresoras en la misma red dentro de un edifico o campus (Cisco, 2021)

VTY: significa Virtual Teleype, es un tipo de interfaz virtual que es usada para obtener acceso por consola a un switch o Router utilizando Telnet o SSH (GNS3, 2021)

RESUMEN

El desarrollo de esta actividad se centra en la realización de dos escenarios virtuales donde se debe seguir una secuencia de pasos, con los cuales, se va mostrando la solución a diferentes problemas que se presentan en el desarrollo de la actividad y que tienen que ver con el tema de las redes de computadoras. En especial los temas de enrutamiento y los switches de computadoras.

El primer escenario, se plantea desarrollar una red sobre la cual se realiza el direccionamiento IP, configuración básica de un router, la configuración básica de un switch, configuración de hosts. El segundo escenario, plantea una complejidad mayor, al requerir además de las configuraciones básicas de routers y switches, se requiere configurar VLAN, enrutamiento dinámico OSPF, OSPF V3, implementación de DHCP Y NAT sobre IPv4, configuración de NTP y por último la configuración de listas de acceso ACL

Para el desarrollo de estas actividades se recurre al estudio de los temas en el portal netacad.com, la bibliografía consulta, así como varios sitios web donde se condensa los comandos a utilizar en el CLI del IOS de CISCO para lograr configurar los distintos dispositivos según los requerimientos planteados por la guía de desarrollo de las actividades.

PALABRAS CLAVE: Cli, Configuración, Enrutamiento, IP, Interface, HTTP, Protocolos, Redes, Router, Switch, Subneteo.

ABSTRACT

The development of this activity focuses on the realization of two virtual scenarios where a sequence of steps must be followed, with which, the solution to different problems that arise in the development of the activity and that have to do with the subject of computer networks. Especially routing issues and computer switches.

The first scenario is to develop a network on which the IP addressing, basic configuration of a router, the basic configuration of a switch, host configuration is carried out. The second scenario poses a greater complexity, as it requires in addition to the basic configurations of routers and switches, it is required to configure

VLAN, dynamic routing OSPF, OSPF V3, implementation of DHCP and NAT over IPv4, NTP configuration and finally the configuration of ACL access lists

For the development of these activities, the study of the topics is used in the netacad.com portal, the bibliography is consulted, as well as several websites where the commands to be used in the CISCO IOS CLI are condensed in order to configure the different devices according to the requirements set by the guide for the development of activities.

KEYWORDS: Cli, Configuration, Routing, IP, Interface, HTTP, Protocols, Networks, Router, Switch, Subnetting.

INTRODUCCIÓN

Este documento se elabora como parte del proceso de grado para la carrera de ingeniería de sistemas de la Universidad Nacional Abierta y a Distancia UNAD, en la opción de diplomado. En este documento se consigan la realización de dos escenarios para la demostración de habilidades adquiridas con el estudio de los materiales del curso, tanto de la plataforma netacad.com, como de los distintos materiales bibliográficos y presentación de los tutores del curso.

Como se mencionó anteriormente, el desarrollo de la actividad consta de la ejecución de dos escenarios virtuales, para ello, se recurre al software CISCO Packet Tracert, el cual permite simular los distintos dispositivos utilizando en las redes de computadores, generando un ambiente virtual, donde se puede simular gran parte de los procesos que se utilizan en la configuración de redes de computadoras.

En el primer escenario se solicita crear una red de acuerdo con una topología suministrada, sobre la cual se debe configurar 2 LAN y realizar ajustes básicos de seguridad en el Router y el Switch. Luego se realiza un Subneteo de acuerdo con las especificaciones dadas en el documento base y realizar los procesos requeridos para conseguir configurar los equipos de acuerdo con esas especificaciones. El segundo escenario, plantea la configuración de una red de mayor complejidad, que requiere de la configuración de VLAN, de NAT, de DHCP, OSPF y OSPFv3. En este escenario se trabaja con los protocolos IPv4 e IPv6.

El alcance de este documento es demostrar las habilidades adquiridas al largo del curso, así como la capacidad de resolución de problemas sobre redes de computadoras de pequeña y mediana escala que requieran de la solución a través de la correcta configuración de dispositivos de enrutamiento, switches y hosts. Utilizando herramientas de simulación de redes como lo es el software de CISCO Packet Tracert.

DESARROLLO

1. Escenario 1

Parte1: 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.

Descripción del Proceso de la parte 1:

Seleccionar el icono de end devices en la parte inferior izquierda.

En el cuadro aparece continuo aparece el icono pc, se seleccionan dos de estos iconos.

Seleccionar el ícono de Network devices, en la parte inferior seleccionar switches, en el cuadro continuo se seleccionar el icono 2960.

Volver al cuadro inferior y seleccionar Routers, en la ventana contigua seleccionar 4331

Para cambiar los nombres que se visualizan, doble clic en cada equipo y en la pestaña config, en display name se procede a cambiar los respectivos nombres según el mostrado en la guía.

Figura 1- Montaje según la guía de escenario 1

Fuente: elaboración propia

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.

Descripción del Proceso de la parte 2:

En mi caso la cédula termina en 13, por lo cual mi direccionamiento es 192.168.13.0

Tabla 1. Tabla de requerimientos de la guía para escenario 1

ITEM	REQUERIMIENTO
Dirección de red	192.168.13.0
Requerimiento de host subred LAN1	100
Requerimiento de host subred LAN2	50
R1 G0/0/1	Primera dirección de host de subred LAN1
R1 G0/0/0	Primera dirección de host de la subred LAN 2
S1 SVI	Segunda direccion del host de la subred lan1
PC-A	Ultima dirección de host de la subred LAN1
PC-B	Última dirección de host de la subred LAN2

Fuente: elaboración propia

El requerimiento incluye dos subredes, así que establecemos una máscara 25.

192.168.13.0/25

Cada subred tendría 126 hosts disponible

LAN1 ocuparia la primera subred 192.168.13.0/25

LAN2 ocuparía la segunda subred 192.168.13.128/25.

Como LAN 2 solo requiere 50 hosts podemos subdividir esta segunda subred en una porción más pequeña con máscara 26 con la cual tendríamos capacidad para 62 hosts

LAN2 ocuparía la subred 192.168.13.126 /26

La tabla de direccionamiento quedaría conformada así:

Tabla 2. Tabla con los datos obtenidos de Subneteo

ITEM	VALOR
LAN1	192.168.13.0 /25
MASCARA DE RED LAN1	255.255.255.128
PRIMER HOST LAN 1	192.168.13.1
ULTIMO HOST LAN 1	192.168.13.126
BROADCAST	192.168.13.127
LAN2	192.168.13.128 /26
MÁSCARA DE RED LAN2	255.255.255.192
PRIMER HOST LAN 2	192.168.13.129
ULTIMO HOST LAN 2	192.168.13.190
BROADCAST	192.168.13.191

Fuente: elaboración propia

NOTA: para calcular estos valores se toman las siguientes fórmulas, para calcular la cantidad de subredes 2^n donde n es la cantidad de 1 que tiene en la ultima porción del octeto de la máscara de subred. Cantidad de host disponibles $2^n - 2$ donde n es la cantidad de ceros en la última porción de la máscara de subred.

Tabla 3. Tabla con direcciones IP con Subneteo

ITEM	REQUERIMIENTO
Dirección de red	192.168.13.0
Requerimiento de host subred LAN1	100
Requerimiento de host subred LAN2	50
R1 G0/0/1	192.168.13.1 /25
R1 G0/0/0	192.168.13.129 /26
S1 SVI	192.168.13.2 /25
PC-A	192.168.13.126 /25
PC-B	192.168.13.190 /26

Fuente: elaboración propia

Configuración de la IP de PC-A y PC-B, hacer clic en el icono del computador

Seleccionar ventana desktop, seleccionar icono IP configuration y asignar las respectivas IP según la tabla de valores, la máscara de subred y el default gateway

Configuración del router, Ingresar los siguientes comandos por el CLI:

enable

configure terminal

interface gigabit0/0/0

ip address 192.168.13.129 255.255.255.192

no shutdown

exit

interface gigabit0/0/1

ip address 192.168.13.1 255.255.255.128

no shutdown

end

Configuración de switch:

enable

configure terminal

interface vlan2

ip address 192.168.13.2 255.255.255.128

no shutdown

Parte 3: Configure aspectos básicos

Paso 1: configurar los ajustes básicos

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 4. Tabla de tareas a realizar

Tarea	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R1
Nombre del dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Establecer la longitud mínima para las contraseñas	10
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar VTY solo aceptando SSH	
Cifrar las contraseñas de texto no cifrado	
Configure un MOTD Banner	
Configurar interfaz G0/0/0	Establezca la descripción Establece la dirección IPv4. Activar la interfaz.
Configurar interfaz G0/0/1	Establezca la descripción Establece la dirección IPv4. Activar la interfaz.
Generar una clave de cifrado RSA	

Fuente: elaboración propia

Desarrollo:

Para la ejecución de esta actividad se colocará en cursiva la actividad a realizar según la tabla y a continuación los comandos a introducir uno por línea cuando sean varios comandos para introducir.

Desactivar la búsqueda DNS:

enable

configure terminal

no ip domain-lookup
exit
Nombre del router:
enable
configure terminal
hostname R1
exit

Nombre del dominio:
enable
configure terminal
ip domain-name ccna-lab.com
exit

Contraseña cifrada para el modo EXEC privilegiado:

enable
configure terminal
enable secret ciscoenpass
exit
disable

Contraseña de acceso a la consola:
enable
configure terminal
line console 0
enable secret ciscoconpass
exit

disable

Establecer la longitud mínima para las contraseñas:

enable

configure terminal

security password min-length 10

exit

disable

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local:

enable

ciscoconpass

configure terminal

line vty 0 4

login local

exit

Configurar VTY solo aceptando SSH:

configure terminal

crypto key generate rsa

1024

ip ssh versión 2

line vty 0 15

login local

transport input ssh

exit

Cifrar las contraseñas de texto no cifrado:

configure terminal

service password-encryption

Configure un MOTD Banner

configure terminal

banner motd # no está permitido el ingreso sin autorización #

exit

copy running-config startup-config

Configurar interfaz G0/0/0:

Establezca la descripción.

Establece la dirección IPv4.

Activar la interfaz.

configure terminal

interface g0/0/0

description va al PC-B

ip address 192.168.13.129 255.255.255.192

no shutdown

exit

Configurar interfaz G0/0/1:

Establezca la descripción.

Establece la dirección IPv4.

Activar la interfaz.

configure terminal

interface g0/0/1

description va al PC-A

ip address 192.168.13.1 255.255.255.128

no shutdown

exit

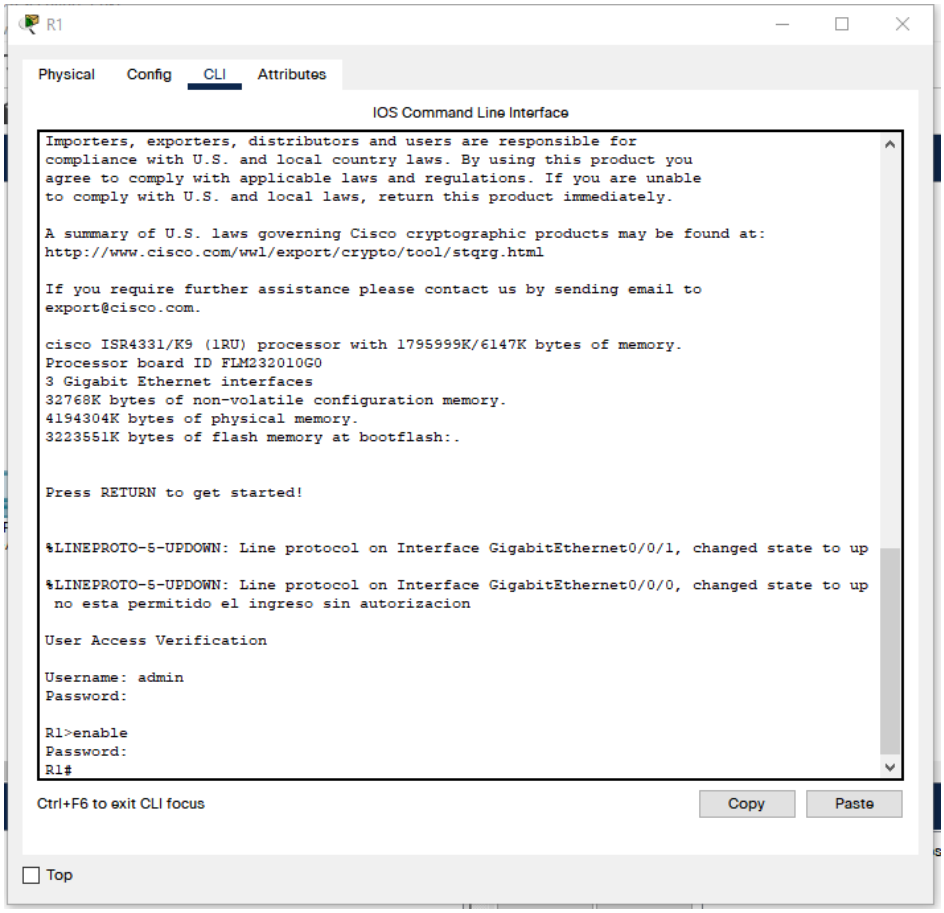
Generar una clave de cifrado RSA:

configure terminal

crypto key generate rsa

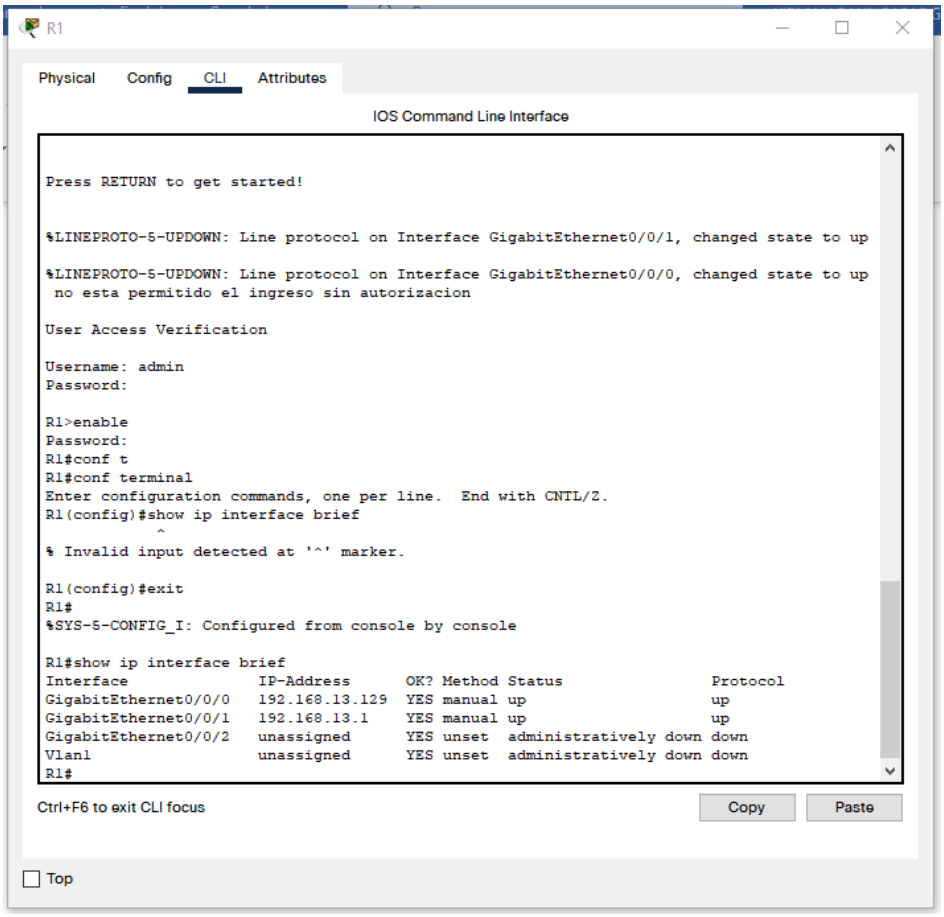
1024

Figura 2. Configuración de seguridad del Router



Fuente: elaboración propia

Figura 3. Configuración de direccionamiento en el router



Fuente: elaboración propia

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 5. Tabla de actividades a realizar en el switch

Tarea	Especificación
Desactivar la búsqueda DNS	
Nombre del switch	S1
Nombre del dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar VTY solo aceptando SSH	
Cifrar las contraseñas de texto no cifrado	
Generar una clave de cifrado RSA	Módulo de 1024 bits
Configure un MOTD Banner	
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento.

Fuente: elaboración propia

Para la ejecución de esta actividad se colocará en cursiva la actividad a realizar según la tabla y a continuación los comandos a introducir uno por línea cuando sean varios comandos para introducir, como en el caso anterior del router.

Desarrollo:

Desactivar la búsqueda DNS:

enable

configure terminal

no ip domain-lookup

Nombre del switch:

hostname S1

Nombre del dominio:

ip domain-name ccna-lab.com

Contraseña cifrada para el modo EXEC privilegiado:

enable secret ciscoenpass

Contraseña de acceso a la consola:

configure terminal

line console 0

enable secret ciscoconpass

Crear un usuario administrativo en la base de datos local:

configure terminal

username admin password admin1pass

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local:

configure terminal

line vty 0 4

login local

exit

Configurar las líneas VTY para que acepten únicamente las conexiones SSH:

Line vty 0 15

transport input ssh

Cifrar las contraseñas de texto no cifrado:

service password-encryption

Configurar un MOTD Banner:

banner motd # prohibido el acceso no autorizado #

Generar una clave de cifrado RSA:

crypto key generate rsa

1024

Configurar la interfaz de administración (SVI):

interface vlan 99

ip address 192.168.13.2 255.255.255.128

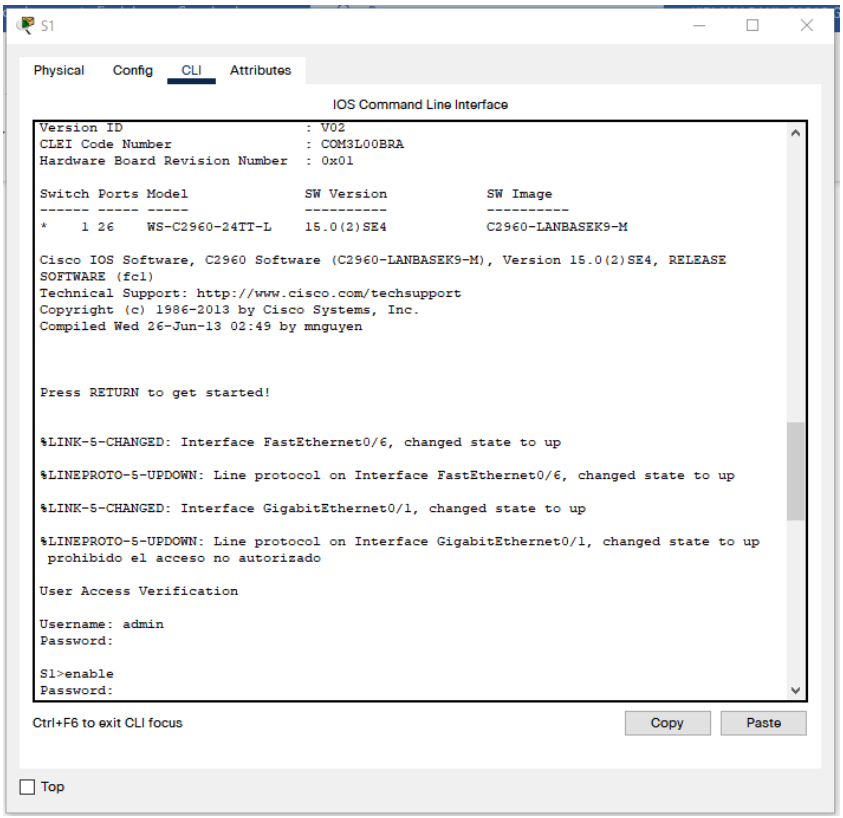
no shutdown

end

Configuración del gateway predeterminado:

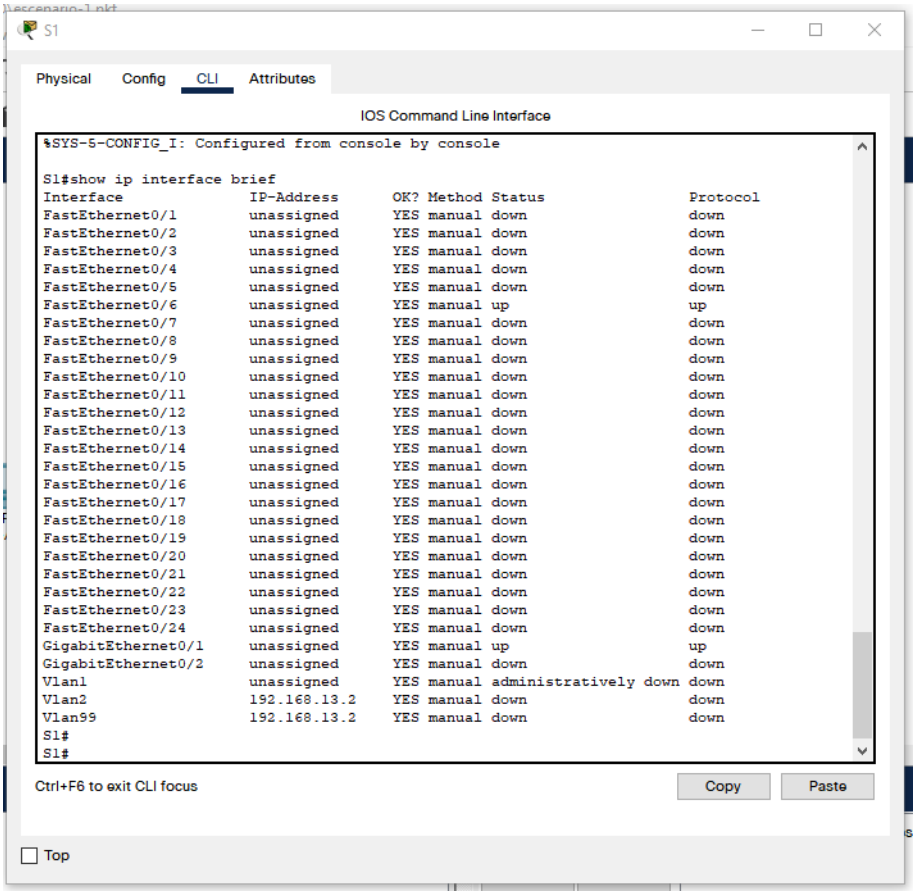
ip default-gateway 192.168.13.0

Figura 4. Configuración de seguridad para el switch



Fuente: elaboración propia

Figura 5. Configuración de las interfaces del switch



Fuente: elaboración propia

Configuración de seguridad para el switch

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.

PC-A network configuration

Tabla 6. Tabla de configuración PC-A

Descripción	PC-A
Dirección física	00E0.A342.687D

Dirección IP	192.168.13.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.13.0

Fuente: elaboración propia

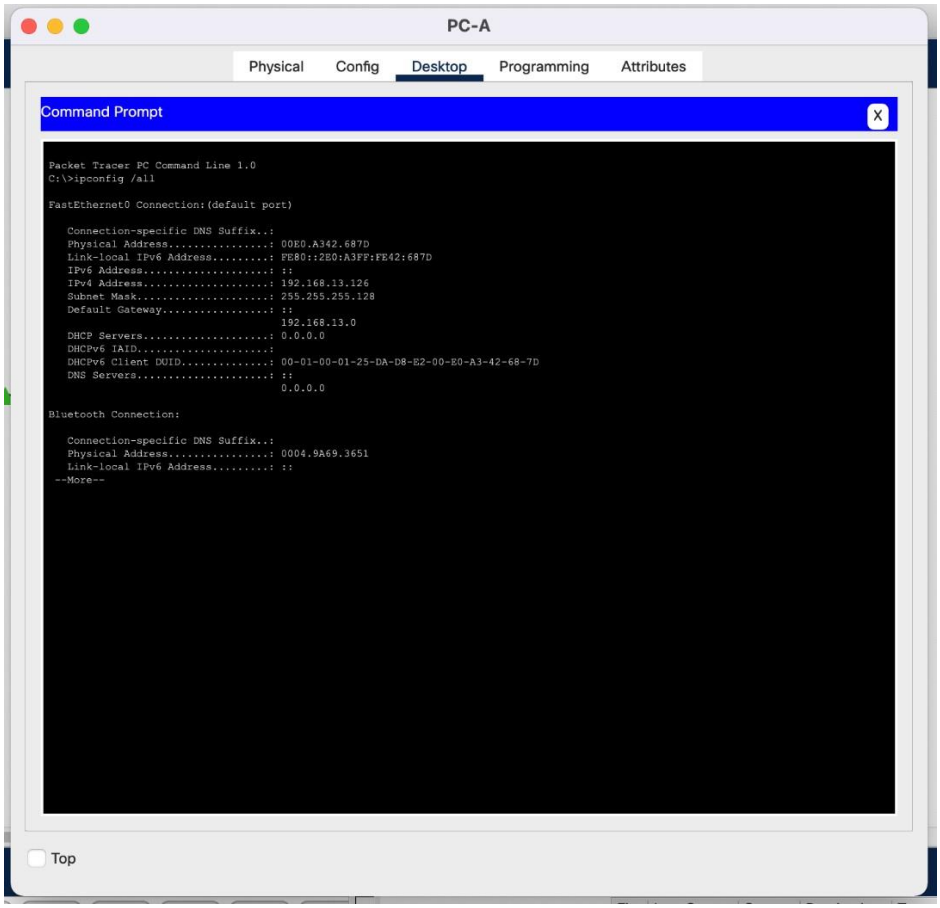
PC-B network configuration

Tabla 7. Tabla de configuración de PC-B

Descripción	PC-B
Dirección física	0000.0CA5.CB3C
Dirección IP	192.168.13.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.13.0

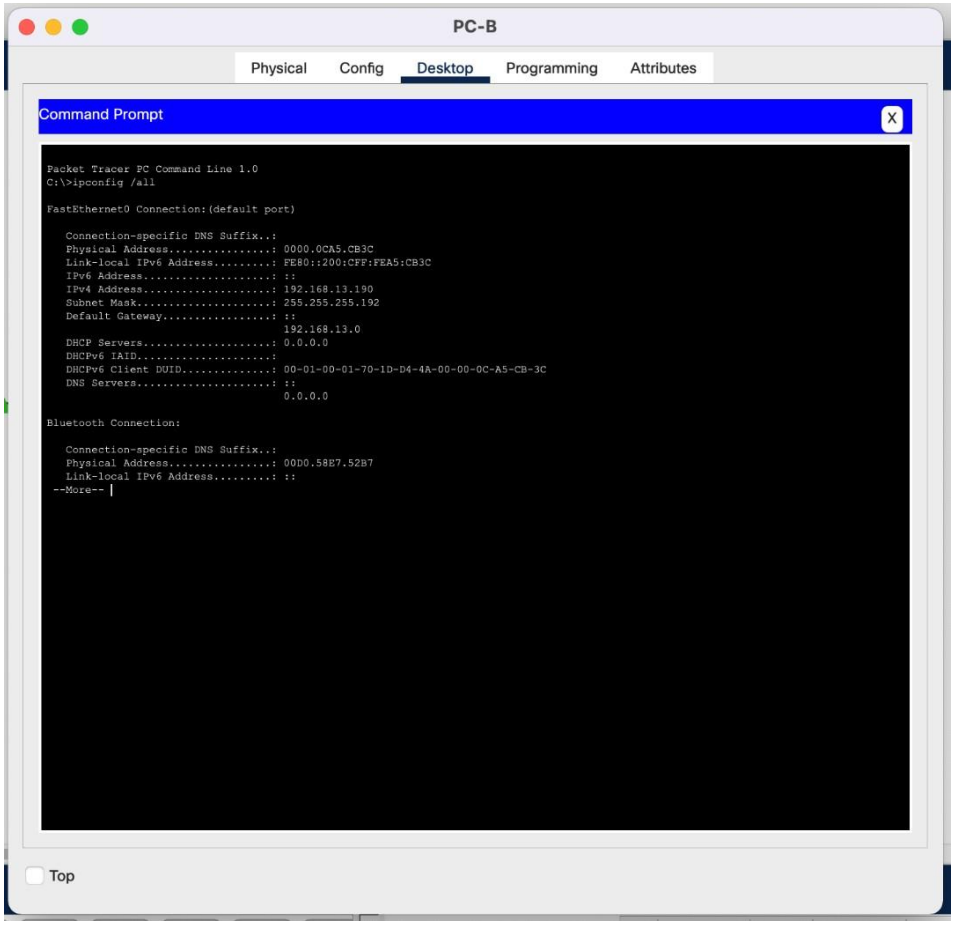
Fuente: elaboración propia

Figura 6. Configuración del PC-A



Fuente: elaboración propia

Figura 7. Configuración del PC-B



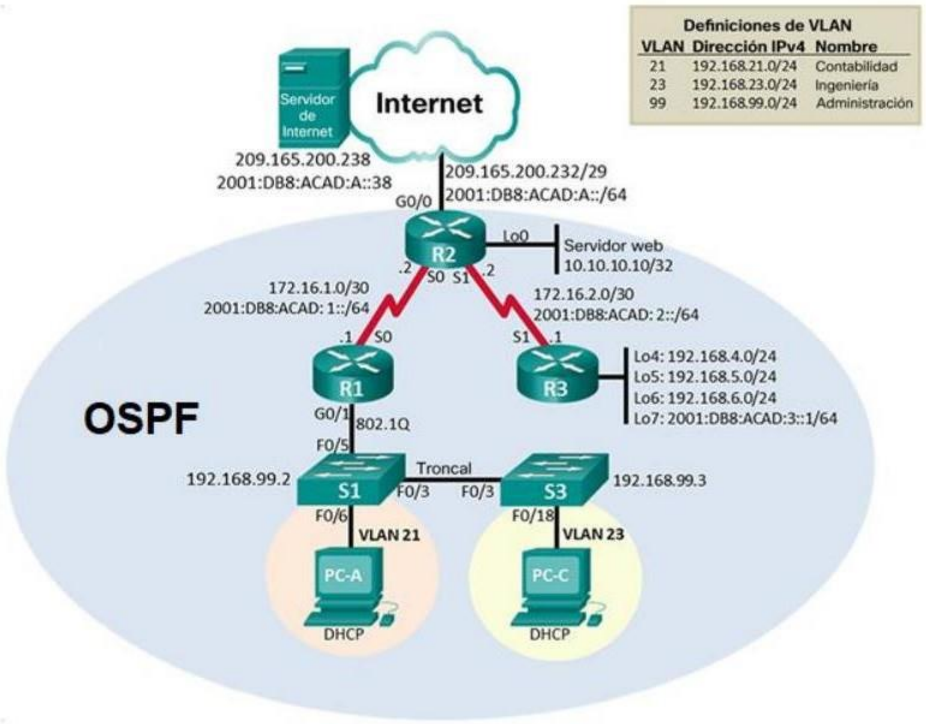
Fuente: elaboración propia

2. Escenario 2.

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

Topología

Figura 8. Topología



Fuente: Guía de actividades cisco

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 8. Actividad parte 1, paso 1

Tarea	Comandos del IOS
Eliminar el archivo startup-config de todos los routers	Router 1: R1>enable R1#erase startup-config Router 2: R2>enable R2#erase startup-config

	Router 3: R2>enable R2#erase startup-config
Volver a cargar los routers	Router 1: R1#reload System configuration has been modified. Save? [yes/no]:yes Router 2: R2#reload System configuration has been modified. Save? [yes/no]:yes Router 3: R3#reload System configuration has been modified. Save? [yes/no]:yes
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch 1: S1#enable S1#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] S1#delete flash:vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm] %Error deleting flash:/vlan.dat (No such file or directory) Switch 2: S2#enable S2#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] S2#delete flash:vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm] %Error deleting flash:/vlan.dat (No such file or directory)
Volver a cargar ambos switches	Switch 1: S1#reload System configuration has been modified. Save? [yes/no]:yes Switch 2:

	S2#reload System configuration has been modified. Save? [yes/no]:yes
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch 1: S1>enable S1#show vlan S1#show vlan brief Switch 2: S2>enable S2#show vlan S2#show vlan brief

Fuente: elaboración 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):

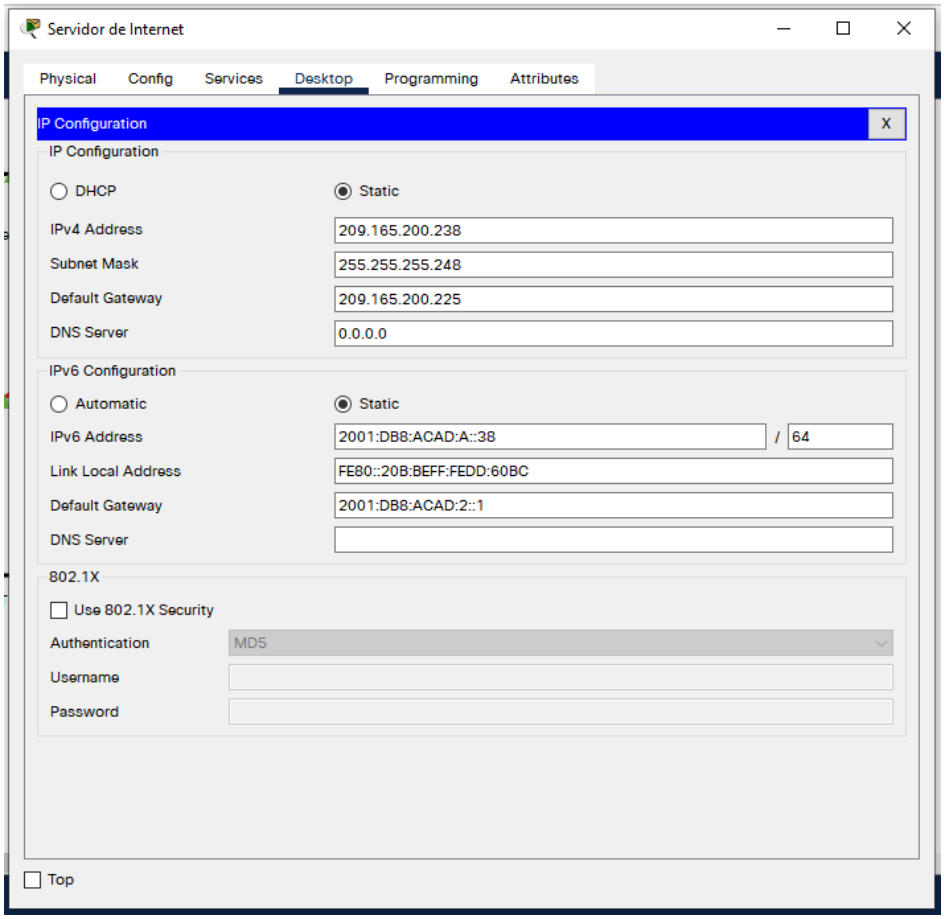
Tabla 9. Actividad parte 2, paso 1

Elemento o área de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.0
Gateway predeterminado	209.165.200.225
Dirección Ipv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Fuente: elaboración propia

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Figura 9. Configuración IPv4, IPv6 en servidor Internet



Fuente: elaboración propia

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 10. Tabla actividades parte 2, paso 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del Router	R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso a telnet	cisco

Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

Fuente: elaboración propia

Nota: Todavía no configure G0/1.

Desarrollo:

Cada paso solicitado en la tabla anterior se desarrolla a continuación:

Desactivar la búsqueda del DNS:

R1>enable

R1#configure terminal

R1(config)#no ip domain lookup

Nombre del Router:

R1>enable

R1#conf t

R1(config)#hostname R1

Contraseña de exec privilegiado cifrada:

R1(config)#enable secret class

Contraseña de acceso a la consola:

R1(config-line)#line console 0

R1(config-line)#password cisco

R1(config-line)#exit

Contraseña de acceso a telnet:

R1(config)#line vty 0 15

R1(config-line)#password cisco

R1(config-line)#exit

Cifrar las contraseñas de texto no cifrado:

R1(config)#service password-encryption

Mensaje MOTD:

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

Interfaz S0/0/0:

R1(config)#interface s0/0/0

Establezca la descripción

R1(config-if)#description "link to R2"

Establecer la dirección IPv4:

R1(config-if)#ip add 172.16.1.1 255.255.255.252

R1(config-if)#no shutdown

Establecer la dirección IPv6:

R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64

R1(config-if)#no shutdown

Establecer la frecuencia de reloj en 128000:

R1(config-if)#clock rate 128000

Activar la interfaz:

R1(config-if)#no shutdown

Rutas predeterminadas:

Configurar una ruta IPv4 predeterminada de S0/0/0;

R1(config-if)#ip route 0.0.0.0 0.0.0.0 172.16.1.2

Configurar una ruta IPv6 predeterminada de S0/0/0:

R1(config)#ipv6 route ::/0 2001:DB8:ACAD:1::2

Paso 3: Configurar R2

Tabla 11. Tabla actividades parte2, paso 3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del Router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso a telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Activar la interfaz

Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de G0/0 Configurar una ruta IPv6 predeterminada de G0/0

Fuente: elaboración propia

Desarrollo:

El desarrollo de las actividades indicadas en la tabla anterior se muestra a continuación:

Desactivar la búsqueda DNS:

R2>enable

R2#configure terminal

R2(config)#no ip domain lookup

Nombre del Router:

R2(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

Contraseña de acceso a telnet:

R2(config-line)#line vty 0 15

R2(config-line)#password cisco

Cifrar las contraseñas de texto no cifrado:

R2(config-line)#service password-encryption

Mensaje MOTD:

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

Interfaz S0/0/0:

R2(config)# interface s0/0/0

Establezca la descripción:

R2(config-if)#description "Link to R1"

Establezca la dirección IPv4:

R2(config-if)#ip add 172.16.1.2 255.255.255.252

Establecer la dirección IPv6:

R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64

Activar la interfaz:

R2(config-if)#no shutdown

Interfaz S0/0/1:

R2(config)#interface s0/0/1

Establecer la descripción:

R2(config-if)#description "Link to R3"

Establezca la dirección IPv4:

R2(config-if)#ip add 172.16.2.2 255.255.255.252

Establezca la dirección IPv6:

R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64

Establecer la frecuencia de reloj en 128000:

R2(config-if)#clock rate 128000

Activar la interfaz:

R2(config-if)#no shutdown

Interfaz G0/0:

R2(config)#interface g0/0

Establecer la descripción:

R2(config-if)#description "Internet"

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

R2(config-if)#ip address 209.165.200.233 255.255.255.248

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

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

Interfaz loopback 0 (servidor web simulado):

R2(config)#int lo0

Establezca la dirección IPv4:

R2(config-if)#description "Servidor Web"

R2(config-if)#ip address 10.10.10.10 255.255.255.255

Activar la interfaz:

R2(config-if)#no shutdown

Paso 4: Configurar R3

La configuración de R3 incluye las siguientes tareas:

Tabla 12. Tabla de actividades paso 4

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.

	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
Rutas predeterminadas	

Fuente: elaboración propia

Desarrollo:

Las actividades solicitadas en la tabla anterior se muestran a continuación:

Desactivar la búsqueda DNS:

R3>enable

R3#conf terminal

R3(config)#no ip domain lookup

Nombre del router:

R3(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

Contraseña de acceso Telnet:

R3(config-line)#line vty 0 15

R3(config-line)#password cisco

Cifrar las contraseñas de texto no cifrado:

R3(config-line)#service password-encryption

Mensaje MOTD:

R3(config)#banner motd # Se prohibe el acceso no autorizado #

Interfaz S0/0/1:

R3(config)#interface s0/0/1

Establecer la descripción:

(config-if)#description "Link to R2"

Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred:

R3(config-if)#ip address 172.16.2.1 255.255.255.252

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

R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64

Activar la interfaz:

R3(config-if)#no shutdown

Interfaz loopback 4:

R3(config)#inter Lo4

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

R3(config-if)#ip address 192.168.4.1 255.255.255.0

Interfaz loopback 5:

R3(config-if)#inter Lo5

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

R3(config-if)#ip address 192.168.5.1 255.255.255.0

Interfaz loopback 6:

R3(config)#int Lo6

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

R3(config-if)#ip address 192.168.6.1 255.255.255.0

Interfaz loopback 7:

R3(config)#int Lo7

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

R3(config-if)#ipv6 address 2001:DB8:ACAD:3::2/64

Rutas predeterminadas

R3(config-if)#ip route 0.0.0.0 0.0.0.0 172.16.2.2

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

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 13. Tabla de actividades paso 5

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda de DNS	
Nombre del switch	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente: elaboración propia

Desarrollo:

El desarrollo de las actividades solicitadas en la tabla anterior se muestra a continuación:

Desactivar la búsqueda de DNS:

S1>enable

S1#conf t

S1(config)#no ip domain lookup

Nombre del switch:

S1(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

Contraseña de acceso Telnet:

S1(config-line)#line vty 0 15

S1(config-line)#password cisco

Cifrar las contraseñas de texto no cifrado:

S1(config-line)#password cisco

S1(config-line)#service password-encryption

Mensaje MOTD:

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

Paso 6: Configurar S3

La configuración del S3 incluye las siguientes tareas:

Tabla 14. Tabla actividades paso 6

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda de DNS	
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente: elaboración propia

Desarrollo:

El desarrollo de las actividades solicitadas en la tabla anterior se muestra a continuación:

Desactivar la búsqueda de DNS:

S3>enable

S3#conf t

S3(config)#no ip domain lookup

Nombre del switch:

S3(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

Contraseña de acceso Telnet:

S3(config-line)#line vty 0 15

S3(config-line)#password cisco

Cifrar las contraseñas de texto no cifrado:

S3#S3(config-line)#password cisco

Mensaje MOTD:

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

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:

En la tabla se muestran los resultados de la actividad solicitada.

Tabla 15. Tabla de actividades y resultados paso 7

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2 2001:DB8:ACAD:1::2	Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 2/14/64 ms
R2	R3, S0/0/1	172.16.2.1 2001:DB8:ACAD:2::1	Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
Pc de internet	Gateway prdeterminado	209.165.200.238 2001:DB8:ACAD:A::38	Reply from 209.165.200.238: bytes=32 time=4ms TTL=128 Reply from 209.165.200.238: bytes=32 time=9ms TTL=128 Reply from 209.165.200.238: bytes=32 time=11ms TTL=128 Reply from 209.165.200.238: bytes=32 time=10ms TTL=128

			Reply from 2001:DB8:ACAD:A::38: bytes=32 time=6ms TTL=128 Reply from 2001:DB8:ACAD:A::38: bytes=32 time=9ms TTL=128 Reply from 2001:DB8:ACAD:A::38: bytes=32 time=10ms TTL=128 Reply from 2001:DB8:ACAD:A::38: bytes=32 time<1ms TTL=128 Ping statistics for 2001:DB8:ACAD:A::38: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 10ms, Average = 6ms

Fuente: elaboración propia

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

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 16. Tabla de actividades parte 3, paso1

Elemento o tarea de configuración	Especificación

Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	
Apagar todos los puertos sin usar	

Fuente: elaboración propia

Desarrollo:

El desarrollo de las actividades solicitadas en la tabla anterior se muestra a continuación:

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 Administración

Asignar la dirección IP de administración:

S1(config-vlan)#int vlan 99

S1(config-if)#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-if)#int fa0/3

S1(config-if)#switchport mode trunk

S1(config-if)#switchport trunk native vlan 1

Forzar el enlace troncal en la interfaz F0/5:

S1(config-if)#int fa0/5

S1(config-if)#switchport mode trunk

S1(config-if)#switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso:

S1(config-if)#int range fa0/1-2, fa0/4, fa0/6-24

S1(config-if-range)#switchport mode Access

Asignar F0/6 a la VLAN 21:

S1(config-if-range)#int fa0/6

S1(config-if)#switchport access vlan 21

Apagar todos los puertos sin usar:

S1(config-if)#int range fa0/1-2, fa0/4, fa0/7-24

S1(config-if-range)#shutdown

Paso 2: Configurar el s3

La configuración del S3 incluye las siguientes tareas:

Tabla 17. Tabla de actividades parte 3, paso 2

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 21	
Apagar todos los puertos sin usar	

Fuente: elaboración propia

Desarrollo:

El desarrollo de las actividades solicitadas en la tabla anterior se muestra a continuación:

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 Administración

Asignar la dirección IP de administración:

S1(config-vlan)#int 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)#int fa0/3

S3(config-if)#switchport mode trunkS1(config-if)#switchport mode trunk

S3(config-if)#switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso:

S3(config-if)#int range fa0/1-2,fa0/4-24

S3(config-if-range)#switch mode access

Asignar F0/18 a la VLAN 21:

S3(config-if-range)#int fa0/18

S3(config-if)#switchport access vlan 21

Apagar todos los puertos sin usar:

S3(config-if)#int range fa0/1-2,fa0/4-17,fa0/19-24

S3(config-if-range)#shutdown

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18. Tabla de actividades parte 3, paso 3

Elemento o tarea de configuración	Especificación

Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .99 en G0/1	G0/1 Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz
Activar la interfaz G0/1	

Fuente: elaboración propia

Desarrollo:

El desarrollo de las actividades solicitadas en la tabla anterior se muestra a continuación:

Configurar la subinterfaz 802.1Q .21 en G0/1:

R1(config)#int g0/1.21

Asignar la VLAN 21:

R1(config-subif)#encapsulation dot1q 21

Descripción: LAN de Contabilidad:

R1(config-subif)#description "LAN de Contabilidad"

Asignar la primera dirección disponible a esta interfaz:

R1(config-subif)#ip add 192.168.21.1 255.255.255.0

Configurar la subinterfaz 802.1Q .23 en G0/1:

R1(config-subif)#int g0/1.23

Asignar la VLAN 23:

R1(config-subif)#encapsulation dot1q 23

Descripción: LAN de Ingenieria:

R1(config-subif)#description "LAN de Ingenieria"

Asignar la primera dirección disponible a esta interfaz:

R1(config-subif)#ip add 192.168.23.1 255.255.255.0

Configurar la subinterfaz 802.1Q .99 en G0/1:

R1(config)#interface g0/1.99

Asignar la VLAN 99:

R1(config-subif)#encapsulation dot1q 99

Descripción: LAN de Administración:

R1(config-subif)#description "LAN de Administracion"

Asignar la primera dirección disponible a esta interfaz:

R1(config-subif)#ip add 192.168.99.1 255.255.255.0

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.

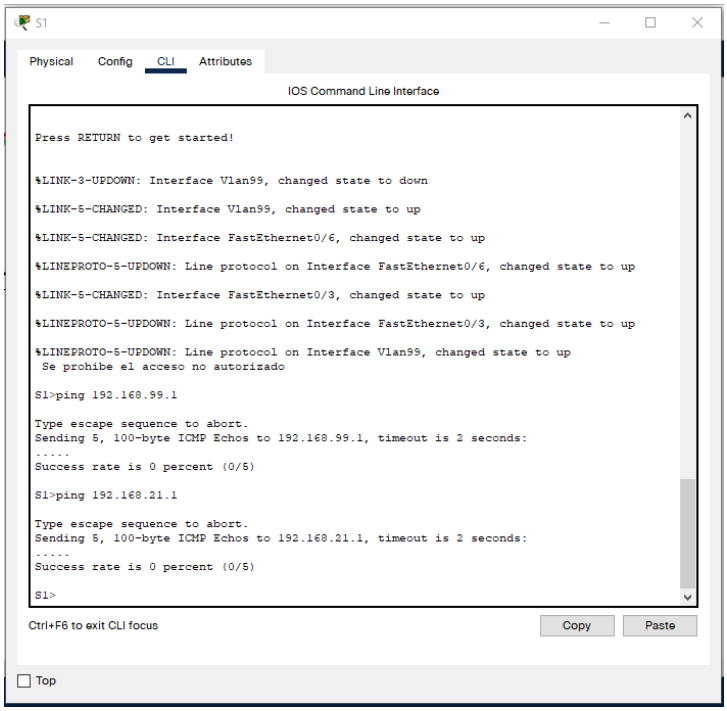
Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 19. Tabla de actividades y resultados paso 4

Desde	A	DIRECCIÓN IP	RESULTADOS DE PING
S1	R1, dirección VLAN 99	192.168.99.1	Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: ..... Success rate is 0 percent (0/5)
S3	R1, dirección VLAN 99	192.168.99.1	Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: ..... Success rate is 0 percent (0/5)
S1	R1, dirección VLAN 21	192.168.21.1	Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: ..... Success rate is 0 percent (0/5
S3	R1, dirección VLAN 23	192.168.23.1	Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: ..... Success rate is 0 percent (0/5)

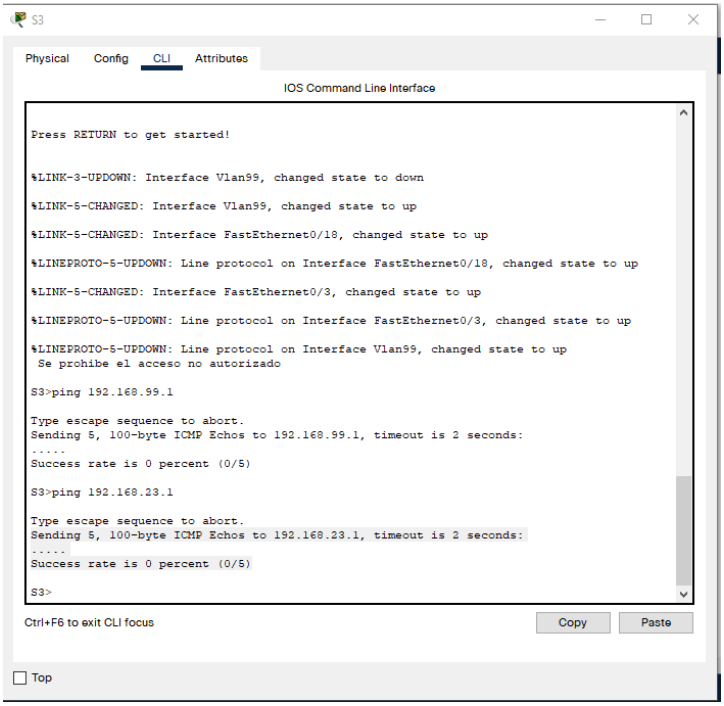
Fuente elaboración propia

Figura 10. Prueba de Ping desde S1



Fuente: elaboración propia

Figura 11. Prueba de Ping desde S3



Fuente: elaboración 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 20. Tabla de actividades parte 4, paso 1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	
Desactive la sumarización automática	

Fuente: elaboración propia

Desarrollo:

El desarrollo de las actividades solicitadas se muestra a continuación:

Configurar OSPF área 0:

R1(config)#router ospf 1

R1(config-router)#router-id 1.1.1.1

R1(config-router)#network 172.16.1.1 0.0.0.255 area 0

Anunciar las redes conectadas directamente:

R1(config-router)#network 172.16.1.0 0.0.0.255 area 0

R1(config-router)#network 10.10.10.10 0.0.0.0 area 0

R1(config-router)#network 192.168.4.0 0.0.0.255 area 0

R1(config-router)#network 192.168.5.0 0.0.0.255 area 0

R1(config-router)#network 192.168.6.0 0.0.0.255 area 0

R1(config-router)#network 192.168.7.0 0.0.0.255 area 0

Establecer todas las interfaces LAN como pasivas:

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

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

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

Desactive la sumarización automática:

No se requiere comando porque ospf no soporta auto-summary (Geek University, 2021)

Paso 2: Configurar OSPF en el R2

Las tareas de configuración para R2 incluyen las siguientes:

Tabla 21. Tabla actividades parte 4, paso 2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar las redes conectadas directamente	Nota: Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	
Desactive la sumarización automática	

Fuente: elaboración propia

Desarrollo:

El desarrollo de las actividades solicitadas en la tabla anterior se muestra a continuación:

Configurar OSPF área 0:

R2(config)#router ospf 1

R2(config-router)#router-id 2.2.2.2

Anunciar las redes conectadas directamente:

R2(config-router)#network 172.16.1.0 0.0.0.255 area 0

R2(config-router)#network 172.16.2.0 0.0.0.255 area 0

R2(config-router)#network 10.10.10.10 0.0.0.0 area 0

R2(config-router)#network 192.168.4.0 0.0.0.255 area 0

R2(config-router)#network 192.168.5.0 0.0.0.255 area 0

R2(config-router)#network 192.168.6.0 0.0.0.255 area 0

R2(config-router)#network 192.168.7.0 0.0.0.255 area 0

Establecer la interfaz LAN (loopback) como pasiva:

R2(config-router)#passive-interface lo0

Desactive la sumarización automática:

No se requiere comando porque ospf no soporta auto-summary (Geek University, 2021)

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 22. Tabla de actividades parte4, paso 3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar redes IPv4 conectadas directamente	
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	
Desactive la sumarización automática.	

Fuente: elaboración propia

Desarrollo:

El desarrollo de las actividades solicitadas en la tabla anterior se muestra a continuación:

Configurar OSPF área 0:

R3(config)#ipv6 unicast-routing

R3(config)#ipv6 router ospf 1

R3(config-rtr)#network 2001:DB8:ACAD:2::/64 area 0

Anunciar redes IPv4 conectadas directamente:

R3(config-rtr)#interface s0/0/1

R3(config-if)#ipv6 ospf 1 area 0

R3(config-if)#exit

R3(config)#interface lo7

R3(config-if)#ipv6 ospf 1 area 0

R3(config-if)#exit

R3(config)#router ospf 1

R3(config-router)#router-id 3.3.3.3

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

R3(config-router)#passive-interface lo7

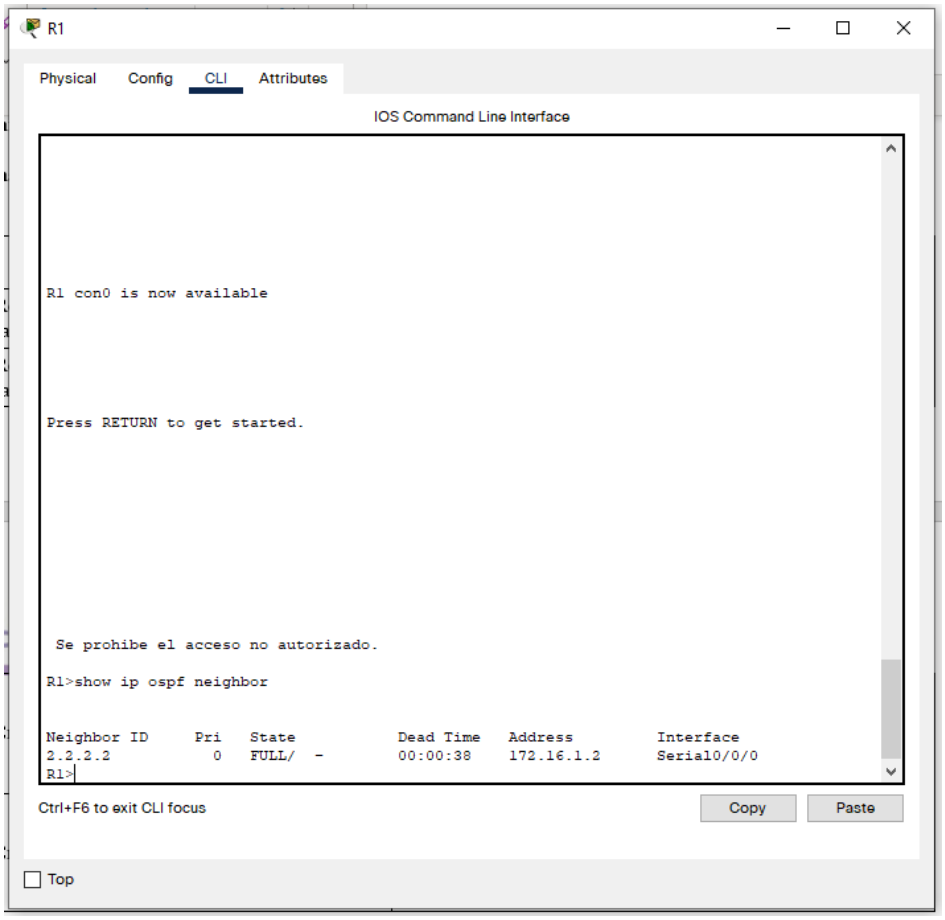
Desactive la sumarización automática:

No se requiere comando porque ospf no soporta auto-summary (Geek University, 2021)

Paso 4: Verificar la información de OSPF

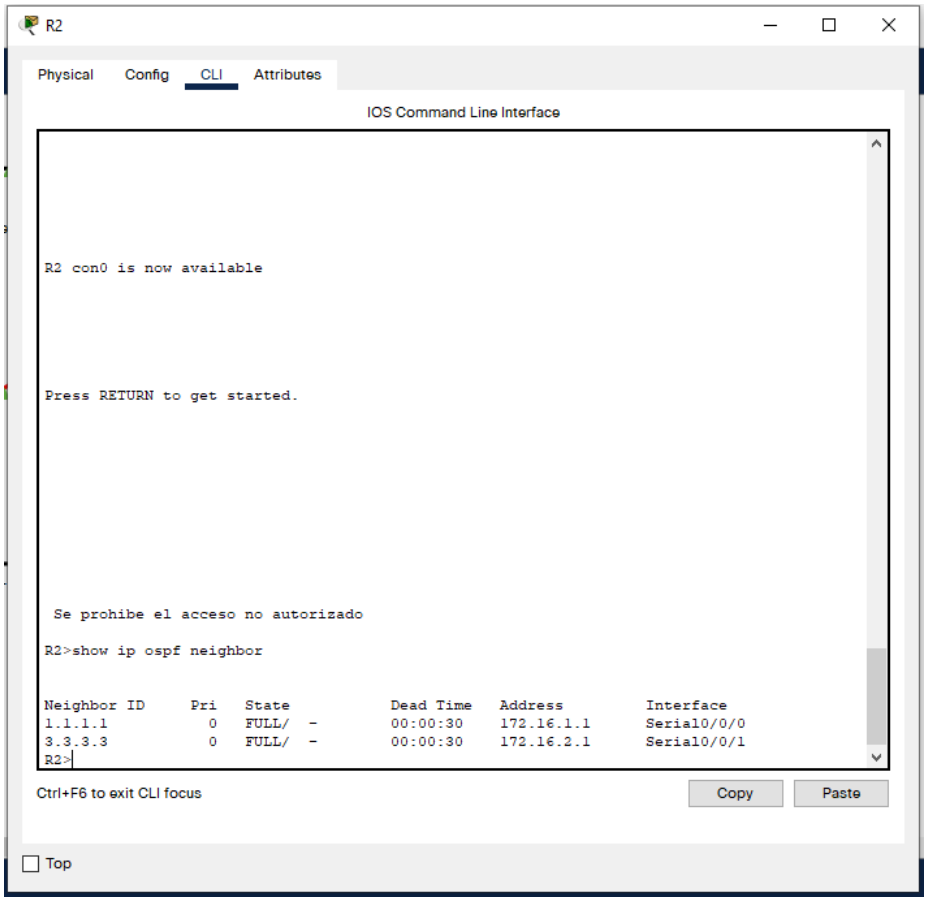
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Figura 12.Comando show ip ospf neighbor en el router R1



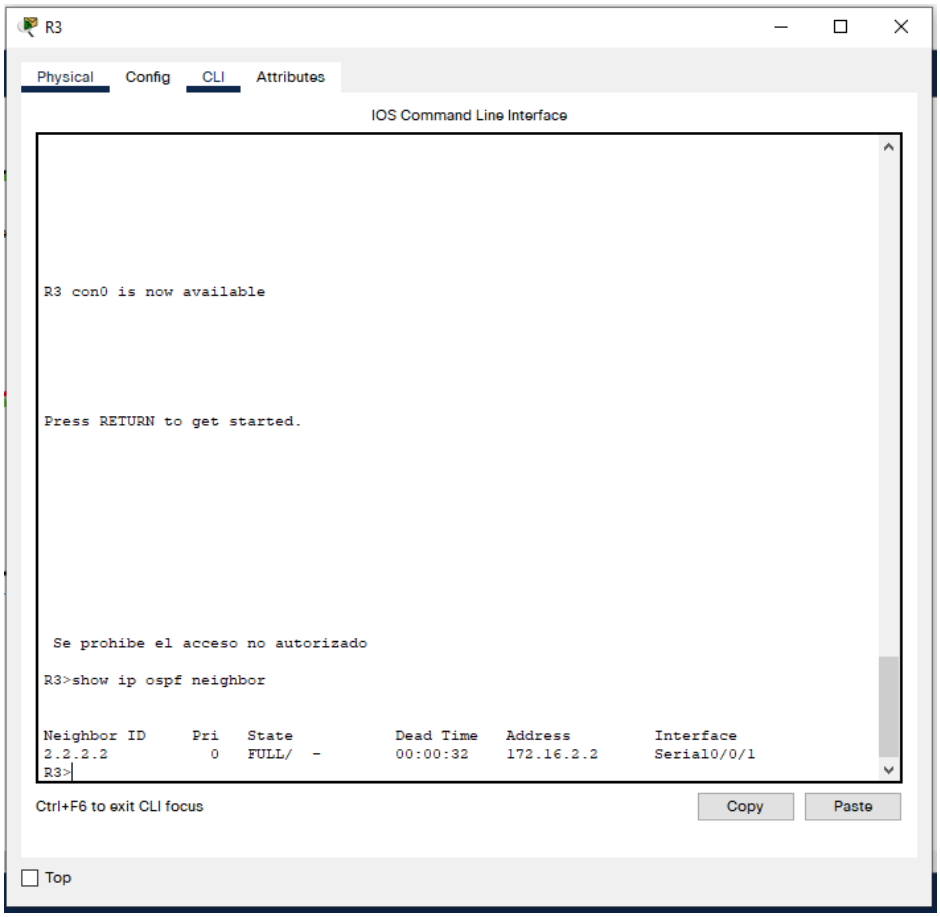
Fuente: elaboración propia

Figura 13. Comando show ip ospf neighbor en el router R2



Fuente: elaboración propia

Figura 14. Comando show ip ospf neighbor en el router R3



Fuente: elaboración propia

Tabla 23. Tabla de respuestas a las preguntas planteadas

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 ospf
¿Qué comando muestra solo las rutas OSPF?	show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	show run | sec ospf

Fuente elaboración 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 24. Tabla de actividades parte 5, paso 1

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

Fuente: elaboración propia

Desarrollo:

El desarrollo de las actividades solicitadas en la tabla anterior se muestra a continuación:

Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas:

R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20

Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas:

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

Crear un pool de DHCP para la VLAN 21:

Nombre ACCT:

R1(config)# ip dhcp pool ACCT

R1(dhcp-config)#network 192.168.21.0 255.255.255.0

Servidor DNS 10.10.10.10:

R1(dhcp-config)#dns-server 10.10.10.10

Nombre de dominio: ccna-sa.com:

R1(dhcp-config)#domain-name ccna-sa.com

Establecer el gateway predeterminado:

R1(dhcp-config)#default-router 192.168.21.1

Crear un pool de DHCP para la VLAN 23:

Nombre: ENGNR:

R1(config)#ip dhcp pool ENGNR

Servidor DNS: 10.10.10.10

R1(dhcp-config)#dns-server 10.10.10.10

Nombre de dominio: ccna-sa.com:

R1(dhcp-config)#domain-name ccna-sa.com

Establecer el gateway predeterminado:

R1(dhcp-config)#network 192.168.23.0

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

La configuración del R2 incluye las siguientes tareas:

Tabla 25. Tabla de actividades paso 2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con unacuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**
Habilitar el servicio del servidor HTTP	
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para laNAT estática	
Configurar la NAT dinámica dentro de unaACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y deIngeniería en el R1 Permitir la traducción de un resumen de las redes LAN(loopback) en el R3
Defina el pool de direcciones IP públicasutilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228
Definir la traducción de NAT dinámica	

Fuente: elaboración propia

Desarrollo:

El desarrollo de las actividades solicitadas en la tabla anterior se muestran a continuación:

Crear una base de datos local con una cuenta de usuario:

R2(config)#username webuser privilege 15 secret cisco12345

Habilitar el servicio del servidor HTTP:

R2(config)#ip http server

Nota: en cisco packet tracert esa función no está soportada

https://community.cisco.com/t5/routing/ip-http-server-command-not-working-on-packet-tracer/td-p/4172942

Configurar el servidor HTTP para utilizar labase de datos local para la autenticación:

R2(config)#ip http authentication local

Nota: en cisco packet tracert esa función no está soportada

https://community.cisco.com/t5/routing/ip-http-server-command-not-working-on-packet-tracer/td-p/4172942

Crear una NAT estática al servidor web:

R2(config)#ip nat source static 10.10.10.10 209.165.200.229

Asignar la interfaz interna y externa para la NAT estática:

R2(config)#int g0/0

R2(config-if)#ip nat outside

R2(config-if)#exit

R2(config)#int s0/0/0

R2(config-if)#ip nat inside

R2(config-if)#exit

R2(config)#int s0/0/1

R2(config-if)#ip nat inside

R2(config-if)#exit

Configurar la NAT dinámica dentro de una ACL privada:

R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255

R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255

R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255

Defina el pool de direcciones IP públicas utilizables:

R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 NETMASK 255.255.255.248

Definir la traducción de NAT dinámica:

ip nat inside source list 1 pool INTERNET

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 pingsse realicen correctamente.

Tabla 26. Tabla parte 5, paso3

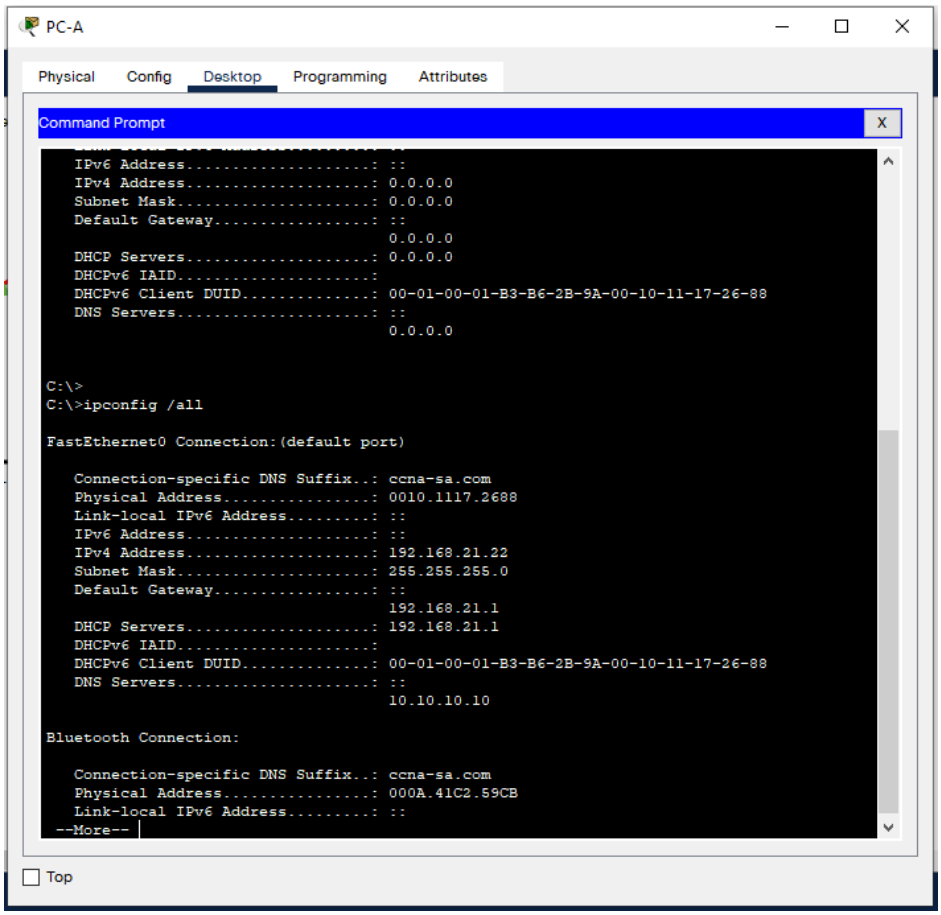
Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Ilustración 14
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Ilustración 15
Verificar que la PC-A pueda hacer ping ala PC-C **Nota:** Quizá sea necesario deshabilitar elfirewall de la PC.	Ilustración 16

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 elaboración propia

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

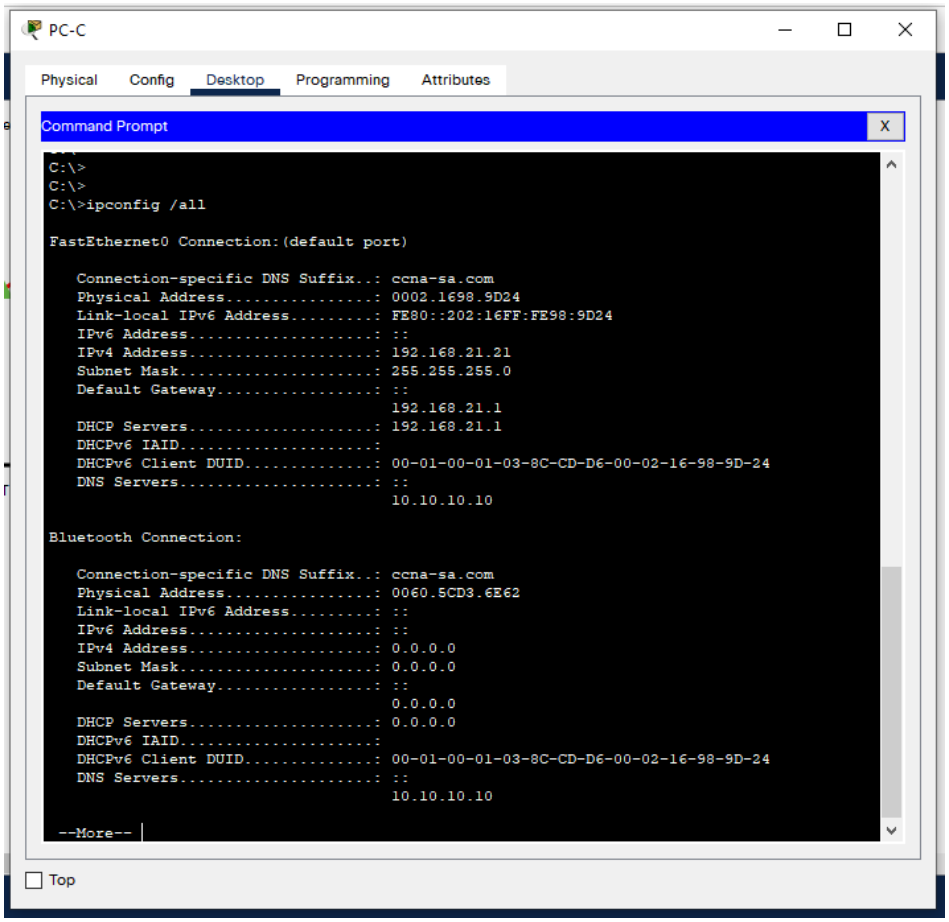
Figura 15. Verificaciòn DHCP en PC-A



Fuente: elaboración propia

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

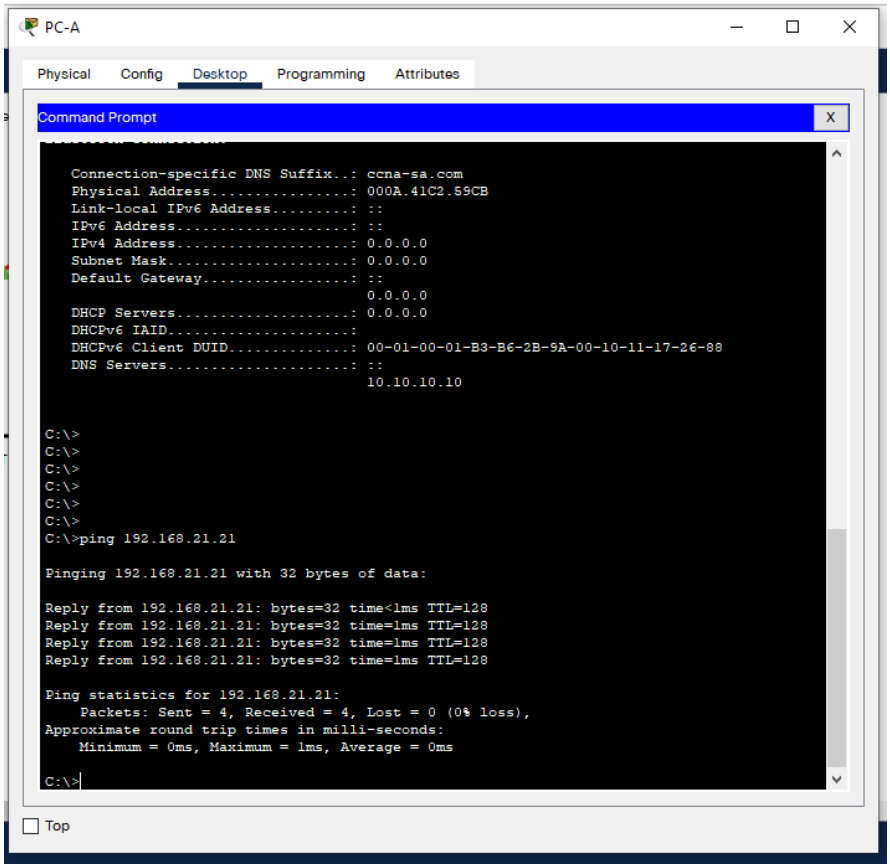
Figura 16. información DHCP en PC-C



Fuente: elaboración propia

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

Figura 17. Ping entre PC-A y PC-C



Fuente: elaboración propia

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

Esta prueba no se pudo realizar en cisco packet tracert

Nota: en cisco packet tracert esa función no está soportada

https://community.cisco.com/t5/routing/ip-http-server-command-not-working-on-packet-tracer/td-p/4172942

Parte 6: Configurar NTP

Tabla 27. Tabla Parte 6

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	5 de marzo de 2016, 9 a. m.
Configure R2 como un maestro NTP.	Nivel de estrato: **5**
Configurar R1 como un cliente NTP.	Servidor: **R2**
Configure R1 para actualizaciones de calendario periódicas con horaNTP.	
Verifique la configuración de NTP en R1.	

Fuente: elaboración propia

Desarrollo:

El desarrollo de las actividades solicitadas en la tabla anterior se muestra a continuación:

Ajuste la fecha y hora en R2:

R2#clock set 09:00:00 mar 5 2020

Configure R2 como un maestro NTP:

R2(config)#ntp master 5

Configurar R1 como un cliente NTP:

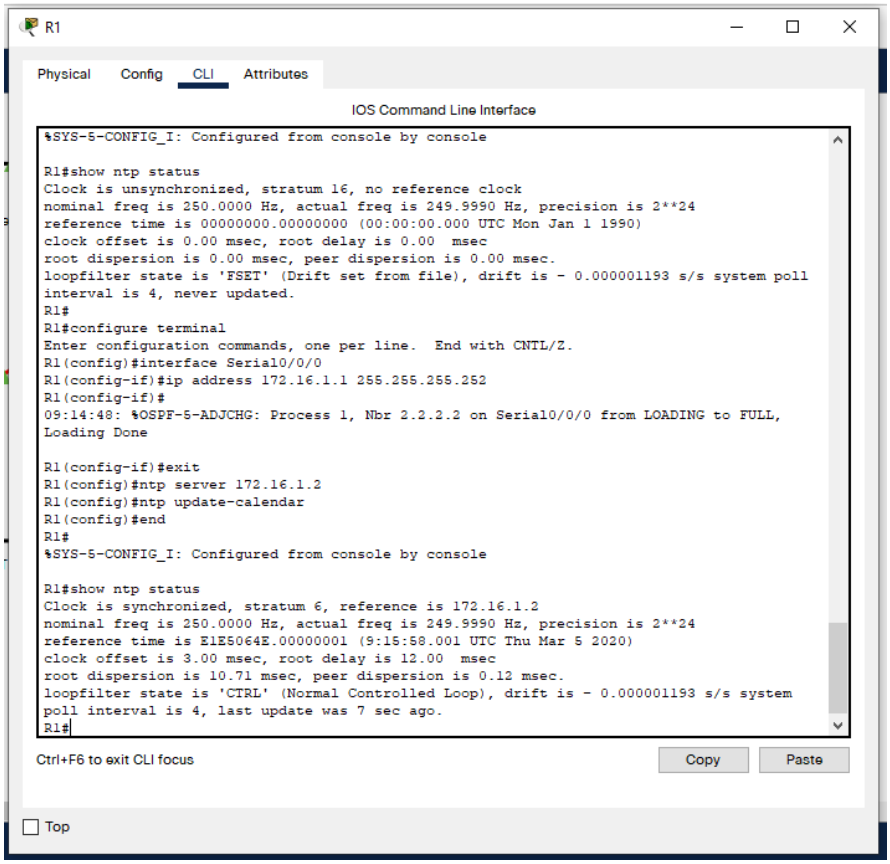
R1(config)#ntp server 172.168.1.2

Configure R1 para actualizaciones de calendario periódicas con horaNTP:

R1(config)#ntp update-calendar

Verifique la configuración de NTP en R1:

Figura 18. verificación de NTP en R1



Fuente: elaboración 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 28. Tabla actividades Parte 7, paso 1

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1establezca una conexión Telnet con R2	Nombre de la ACL: ADMIN-MGT
Aplicar la ACL con nombre a las líneas VTY	
Permitir acceso por Telnet a las líneas de VTY	
Verificar que la ACL funcione como se espera	

Fuente: elaboración propia

Desarrollo:

El desarrollo de las actividades solicitadas en la tabla anterior se muestra a continuación:

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

R2(config)#ip access-list extended ADMIN-MGT

R2(config-ext-nacl)#permit tcp host 172.16.1.1 host 172.16.1.2 eq 23

Aplicar la ACL con nombre a las líneas VTY

R2(config)#line vty 0 15

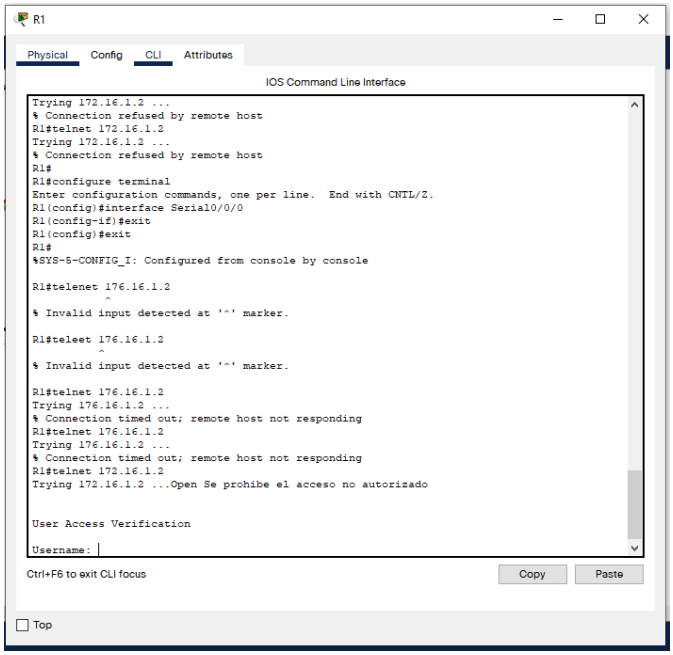
R2(config-line)#access-class ADMIN-MGT in

Permitir acceso por Telnet a las líneas de VTY

R2(config-line)#transport input telnet

Verificar que la ACL funcione como se espera

Figura 19. Verificaciòn del funcionamiento del ACL



Fuente: elaboración propia

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

Tabla 29. Tabla de actividades parte 7, paso 2

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	
Restablecer los contadores de una listade acceso	
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	
¿Con qué comando se muestran lastraducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-C se agregarona 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?	

Fuente: elaboración propia

Desarrollo:

Las actividades solicitadas en la tabla anterior se muestran a continuación:

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

R2#sh ip access-list

¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección enque se aplica?

R2#sh ip interface s0/0/0

¿Con qué comando se muestran lastraducciones NAT?

sh ip nat translations

¿Qué comando se utiliza para eliminarlas traducciones de NAT dinámicas?

R2#clear ip nat translation *

CONCLUSIONES

Para el diseño de subredes, se pueden establecer subredes con diferentes capacidades de hosts, realizando los cálculos adecuados que permitan administrar de manera más eficiente la capacidad de las redes para conectar hosts, además se puede de una manera modular permitir que las redes puedan crecer a medida que cambien los requerimientos en el tiempo.

ACL es una serie de comandos introducidos en el IOS que controlar si el router permite o bloquea los paquetes basados en la información que contienen en el header.

DHCP (Dynamic Host Configuration Protocol) es un protocolo usado para desplegar direcciones IP relacionadad con los dispositivos de red conectados a la red. El objetivo del DHCP es simplificar el proceso de la asignación de IP, existe DHCP para las dos versiones de protocolos IP, IPv4 e IPv6.

OSPF (Open Short Path First) es un protocolo de enrutamiento de estado de enlace, fue desarrollado como remplazo del protocolo de enrutamiento de vector de distancia. Este protocolo ofrece una ventaja sobre el protocolo RIP porque ofrece una mayor convergencia y escala mejor en implementaciones de red de gran escala.

El default Gateway, es la IP que identifica al enrutador que enviara el paquete fuera de la red del host, cuando la IP de destino no se encuentra en la misma red.

NAT (Network Address Translation) es utilizado principalmente para conservar lasIPv4, el objetio es permitir a las redes usar las IPv4 privadas internamente y proveer una traducción a la IP pública únicamente cuando sea necesario.

BIBLIOGRAFÍA

Academy, N. (21 de 11 de 2021). *Routing y switching de CCNA: Principios básicos de routing y switching*. Obtenido de Routing y switching de CCNA: Principios básicos de routing y switching: https://lms.netacad.com/course/view.php?id=542274

ccnadesdecero.es. (19 de 10 de 2021). *ccnadesdecero.es*. Obtenido de ccnadesdecero.es: https://ccnadesdecero.es/

Cisco. (20 de 10 de 2021). *cisco.com*. Obtenido de cisco.com: https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html#:~:text=-%20Definici%C3%B3n%20y%20usos%20-%20Cisco%20%C2%BFQu%C3%A9%20es,red%2C%20los%20m%C3%B3dems%20o%20los%20switch%20de%20red.

Cisco Press. (2014). *Routing and Switching Essentials.* Indiana: Cisco Press.

Geek University. (21 de 11 de 2021). Obtenido de Geek University: https://geek-university.com/ccna/ospf-route-summarization/

GNS3. (20 de 10 de 2021). *gns3network*. Obtenido de gns3network: https://www.gns3network.com/cisco-line-vty-0-4/#:~:text=VTY%20stands%20for%20Virtual%20Teletype.%20I%E2%80%99m%20sure%20you,so%20there%20is%20no%20hardware%20associated%20with%20it.

Networking Academy. (21 de 11 de 2021). *CCNA Routing and Switching*. Obtenido de CCNA Routing and Switching: https://lms.netacad.com/course/view.php?id=720351

techlib. (23 de 11 de 2021). Obtenido de techlb: https://techlib.net/definition/ntp.html