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

OSCAR ANDRES VELASCO LOPEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

INGENIERÍA DE SISTEMAS

NEIVA

2021

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

OSCAR ANDRES VELASCO LOPEZ

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

DIRECTOR:
MSc. RAUL BAREÑO GUTIERREZ

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

NEIVA, 29 de noviembre de 2021

AGRADECIMIENTOS

Agradezco a Dios por bendecirme la vida, por guiarme a lo largo de mi existencia, ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad.

Gracias a mis padres: Honofre Velasco y Lucia López, por ser los principales promotores de mis sueños, por confiar y creer en mis expectativas, por los consejos, valores y principios que me han inculcado.

Mi profundo agradecimiento para cada uno de mis hermanos Daniel, Wendy, Juan Pablo, Nicolas, Julián y Camilo Velasco López a quienes quiero hacer sentir orgullosos y ser un ejemplo para su vida.

De igual manera quiero agradecer a mi compañera de vida Ginna Andrade, quien compartió y vivió cada momento de este recorrido, cada trasnocha, cada frustración y cada alegría, me apoyo y no permitio que desfalleciera.

Quiero expresar mi gratitud a mi tia Patricia Lopez quien fue la persona que me apoyo inicialmente en este camino, quien confio en mi y me brindo todo el apoyo para iniciar con este proyecto que hoy esta en su recta final.

Para mi abuela Maria Fatima Rivera quien desde pequeño me brindado su apoyo incondicional, siempre ha estado en los momentos en que mas la he necesitado, de igual forma tiene gran parte de reconocimiento por todos mis logros.

A Carolay Forero quien a pesar de la distancia siempre ha confiado en mi y me ha dado todo su apoyo desde que inicio este proceso.

Todo mi agradecimiento al Ingeniero Omar Dorado quien forjo mis bases de conocimiento y me mostro lo maravillosa que es la carrera de Ingenieria de Sistemas.

Gracias infinitas al Ingeniero Sergio Vasquez que complemento mi formacion y me motivo a continuar adelante confiando en mi y presentadome retos profesionales que me han permitido llegar hasta donde estoy hoy en dia.

Agradezco a mis docentes de la Escuela De Ciencias Básicas, Tecnología E Ingeniería – ECBTI de la Universidad Abierta y a Distancia - UNAD, por haber compartido sus conocimientos a lo largo de la preparación de mi profesión.

Finalemente a todos mis familiares y amigos que de una u otra forma me han motivado a continuar con mis metas, la lista seria bastante larga para agradecer sus enseñanzas y apoyo incondicional.

Muchas gracias a todos.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

IPV4: (Internet Protocol, version 4, protocolo de Internet, versión 4) Una versión del protocolo de Internet que admite un espacio de dirección de 32 bits. IPv4 en ocasiones se denomina simplemente IP.

SECUENCIA DE COMANDOS: Instrucciones que le indican a un módem la forma de establecer un enlace de comunicaciones entre en sí mismo y un par remoto. Tanto los protocolos PPP como los UUCP emplean secuencias de comandos de chat para establecer los enlaces por marcación telefónica y las llamadas de respuesta.

DNS: (domain name system, sistema de nombre de dominio) Un servicio que proporciona las directivas y los mecanismos de nomenclatura para la asignación de dominio y los nombres del equipo para direcciones fuera de la empresa, como las de Internet. DNS es el servicio de información de la red utilizado por Internet.

VLAN: (virtual local area network, red de área local virtual) Una subdivisión de una red de área local en la capa de enlace de datos de la pila de protocolo.

WAP: (Wireless Application Protocol, protocolo de aplicación inalámbrica) Un protocolo estándar para acceder a información a través de una red inalámbrica móvil.

RESUMEN

Dentro del presente trabajo encontraran la solución a dos problema planteado sobre redes CISCO, por medio del cual se utilizaran todas las herramientas que se conocieron durante el desarrollo del diplomado de profundización, de igual forma los elementos utilizados y los términos a los que se hará referencia vienen de lo aprendido en el diplomado, haciendo uso de líneas de comandos que nos van a permitir configurar las redes, el enrutamiento de cada uno de los dispositivos para finalmente lograr una correcta conmutación entre ellos.

Palabras Clave: CISCO, CCNA, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

Within this work, you will find the solution to two problems posed on CISCO networks, by means of which all the tools that were known during the development of the in-depth diplomat will be used, as well as the elements used and the terms to which reference will be made. They come from what was learned in the diploma, making use of command lines that will allow us to configure the networks, the routing of each of the devices to finally achieve a correct switch between them.

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

INTRODUCCIÓN

Las redes permiten por medio de su apoyo a que una organización logre su objetivo, ya que facilitan la comunicación y ayudar a transportar datos por todas partes del mundo e ahí la importancia de contar con redes que permitan un flujo de datos eficiente, dentro del presente trabajo conoceremos como aplicar los diferentes terminos y equipos dentro de las organizaciones.

El presente trabajo se realiza con el fin de dar respuesta a dos problemas planteados, esto es importante porque con ello vamos a demostrar lo aprendido dentro del diplomado de profundización en CISCO con el fin de aplicarlo en nuestra vida profesional.

DESARROLLO

1. ESCENARIO 1

Figura 1. Topología escenario 1

Fuente: Propia

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

Objetivos

Parte 1: Construir en el simulador la Red

Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2

Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta.

Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1

Parte 4: Configurar los hosts y verificar la conectividad entre los equipos

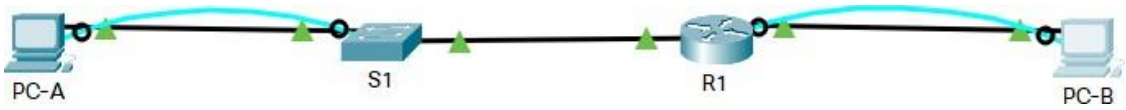
Aspectos básicos/situación

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

Parte 1: Construya la Red

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

Figura 2. Topología escenario 1 en Packet Tracer



Fuente: 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 (1080933522).

Tabla 1. Tabla de configuración de subredes

LAN	PC	Dirección de Red	Mascara	Primera IP	Ultima IP	Broadcast	Host
1	100	192.168.22.0	255.255.255.128	192.168.22.1	192.168.22.126	192.168.22.127	126
2	50	192.168.22.128	255.255.255.192	192.168.22.129	192.168.22.190	192.168.22.191	62

Fuente: Propia

Tabla 2. Tabla de direccionamiento

Item	Requerimiento
Dirección de Red	192.168.22.0
Requerimiento de host Subred LAN1	100

Requerimiento de host Subred LAN2	50
R1 G0/0/1	192.168.22.1
R1 G0/0/0	192.168.22.129
S1 SVI	192.168.22.2
PC-A	192.168.22.126
PC-B	192.168.22.190

Fuente: Propia

Parte 3: Configure aspectos básicos

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

Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 1. Tareas de configuración para R1

Tarea	Especificación	Comando
Desactivar la búsqueda DNS		Router(config)#no Ip domain-lookup
Nombre del router	R1	Router(config)#hostname R1
Nombre de dominio	ccna-lab.com	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	ciscoconpass	R1(config)#line console 0 R1(config-line) #password ciscoconpass R1(config-line)#login
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 de usuario: admin Password: admin1pass	R1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY		R1(config)#line vty 0 4 R1(config-line)#password ciscocisco

para que use la base de datos local		R1(config-line)#login local
Configurar VTY solo aceptando SSH		R1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado		R1(config-line)#service password-encryption
Configure un MOTD Banner		R1(config)#banner motd #Cofiguracion del router#
Configurar interfaz G0/0/0	Establezca la descripción Establece la dirección IPv4. Activar la interfaz.	R1(config)#int g0/0/0 R1(config-if)#Description LAN 2 R1(config-if)#Ip address 192.168.22.129 255.255.255.192 R1(config-if)#no shu
Configurar interfaz G0/0/1	Establezca la descripción Establece la dirección IPv4. Activar la interfaz.	R1(config-if)#int g0/0/1 R1(config-if)#Description LAN 1 R1(config-if)#Ip add 192.168.22.1 255.255.255.128 R1(config-if)#no shu
Generar una clave de cifrado RS	Módulo de 1024 bits	R1(config)#crypto key generate rsa

Fuente: Propia

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 2. Tareas de configuración de S1

Tarea	Especificación	Comandos
Desactivar la búsqueda DNS		Switch(config)#no ip domain-lookup
Nombre del switch	S1	Switch(config)#hostname S1
Nombre de dominio	ccna-lab.com	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass	S1(config)#Enable secret ciscoenpass S1(config)#Line console 0 S1(config-line)#Password ciscoconpass S1(config-line)#login

Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass	S1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local		S1(config)#Line vty 0 15 S1(config-line)#Password ciscocisco S1(config-line)#Login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH		S1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado		S1(config)#service password-encryption
Configure un MOTD Banner		S1(config)#Banner motd #Configuracion del switch#
Generar una clave de cifrado RSA	Módulo de 1024 bits	S1(config)#crypto key generate rsa
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento	S1(config)#Int vlan 1 S1(config-if)#Ip add 192.168.22.2 255.255.255.128 S1(config-if)#no shut
Configuración del Gateway predeterminado	Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento	S1(config-if)#Ip default-gateway 192.168.22.1

Fuente: Propia

Paso 2. Configurar los equipos

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

Tabla 3. PC-A Network Configuration

PC-A Network Configuration	
Descripción	FastEthernet0 Connection:(default port)
Dirección física	00E0.A31D.2153
Dirección IP	192.168.22.126

Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.22.129

Fuente: Propia

Tabla 4. PC-B Network Configuration

PC-B Network Configuration	
Descripción	FastEthernet0 Connection:(default port)
Dirección física	0001.4335.6020
Dirección IP	192.168.22.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.22.129

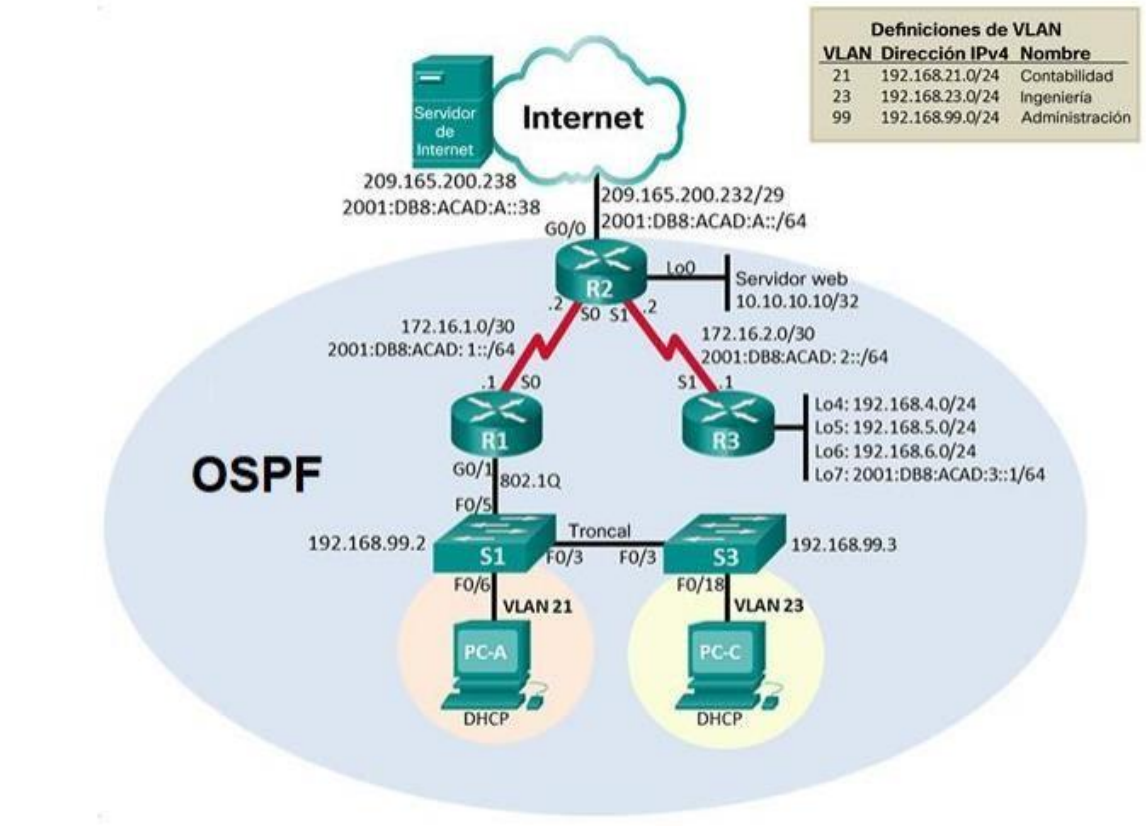
Fuente: Propia

2. ESCENARIO 2

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

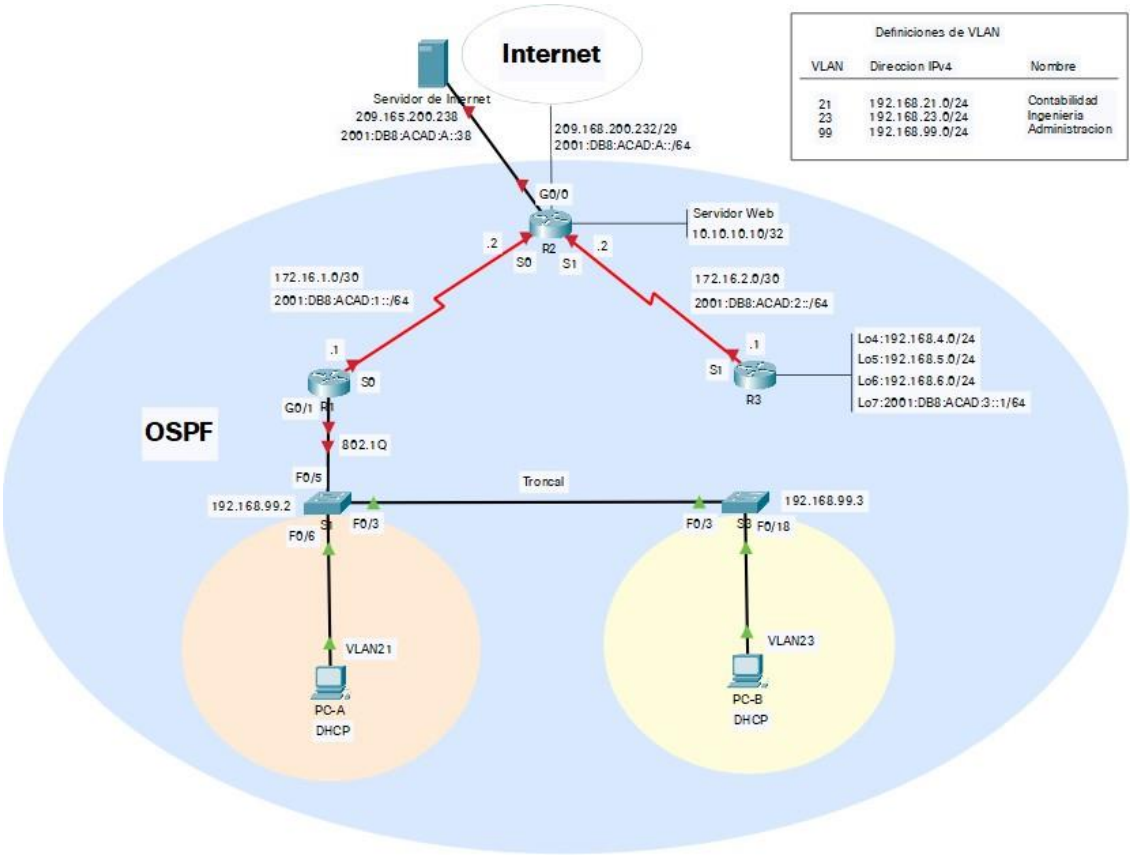
Figura 3. Topología escenario 2

Topología



Fuente: Propia

Figura 4. Topología escenario 2 en Packet Tracer



Fuente: Propia

Parte 1: Inicializar dispositivos

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

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

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

Tabla 5. Lista de tareas

Tarea	Comando de IOS	Comando
Eliminar el archivo startup-config de todos los routers		Router>enable Router#erase startup-config
Volver a cargar todos los routers		Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior		Switch>enable Switch#erase startup-config Switch#delete vlan.dat
Volver a cargar ambos switches		Switchr#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches		Switch#show flash

Fuente: Propia

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

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

Tabla 6. Elementos de configuración

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::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Fuente: 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.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 7. Elementos de configuración para R1

Elemento o tarea de configuración	Especificación	Comando
Desactivar la búsqueda DNS		Router>enable Router#configure terminal 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 console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	cisco	R1(config-line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado		R1(config-line)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado	R1(config)#banner 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	R1(config)#interface s0/0/0 R1(config-if)#description Conexion a R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown

	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	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Fuente: Propia

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 8. Elementos de configuración para R2

Elemento o tarea de configuración	Especificación	Comandos
Desactivar la búsqueda DNS		Router>enable Router#configure terminal 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 console 0 R2(config-line)#password cisco

		R2(config-line)#login
Contraseña de acceso Telnet	cisco	R2(config)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado		R2(config-line)# service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado	R2(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/0/0	Establezca 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	R2(config)#interface s0/0/0 R2(config-if)#description Conexion a R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown
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	R2(config-if)#interface s0/0/1 R2(config-if)#description Conexion a R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown

	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	R2(config-if)#interface g0/0 R2(config-if)#description Conexion a 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
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4	R2(config-if)#interface loopback 0 R2(config-if)#description Servidor Web Simulado R2(config-if)#ip address 10.10.10.10 255.255.255.255
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

Fuente: Propia

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 9. Elementos de configuración para R3

Elemento o tarea de configuración	Especificación	Comandos
Desactivar la búsqueda DNS		Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	R3	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	class	R3(config)#enable secret class
Contraseña de acceso a la consola	cisco	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	cisco	R3(config)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado		R3(config-line)# service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado	R3(config)#banner 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	R3(config)#interface s0/0/1 R3(config-if)#description Conexion a R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown

	información de direcciones. Activar la interfaz	
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config-if)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config-if)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config-if)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.	R3(config-if)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
Rutas prederminadas	Configurar una ruta IPv4 predeterminada de S0/0/1 Configurar una ruta IPv6 predeterminada de S0/0/1	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Fuente: Propia

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 10. Elementos de configuración para S1

Elemento o tarea de configuración	Especificación	Comandos
Desactivar la búsqueda DNS		Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch	S1	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	class	S1(config)#enable secret class
Contraseña de acceso a la consola	cisco	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	cisco	S1(config)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado		S1(config-line)# service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado	S1(config)#banner motd #Se prohíbe el acceso no autorizado#

Fuente: Propia

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 11. Elementos de configuración para S3

Elemento o tarea de configuración	Especificación	Comandos
Desactivar la búsqueda DNS		Switch>enable Switch#configure terminal

		Switch(config)#no ip domain-lookup
Nombre del switch	S3	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	class	S3(config)#enable secret class
Contraseña de acceso a la consola	cisco	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	cisco	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado		S3(config-line)# service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado	S3(config)#banner motd #Se prohíbe el acceso no autorizado#

Fuente: Propia

Paso 7: Verificar la conectividad de la red

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

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

Tabla 12. Parámetros para medir la conectividad

Desde	A	Direccion IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Realizado Correctamente
R2	R3, S0/0/1	172.16.2.1	Realizado Correctamente
PC de Internet	Gateway predeterminado	209.165.200.233	Realizado Correctamente

Fuente: Propia

Figura 5. Ping de R1 a R2, S0/0/0

```
R1#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/21/31 ms
```

Fuente: Propia

Figura 6. Ping de R2 a R3, S0/0/1

```
R2#ping 172.16.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 14/25/31 ms
```

Fuente: Propia

Figura 7. Ping de PC de Internet a Gateway predeterminado

```
Packet Tracer SERVER Command Line 1.0
C:\>ping 209.165.200.233

Pinging 209.165.200.233 with 32 bytes of data:

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

Ping statistics for 209.165.200.233:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: 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 13. Elementos de configuración de seguridad de S1

Elemento o tarea de configuración	Especificación	Comandos
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	S1#configure terminal S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingeniería S1(config-vlan)#vlan 99 S1(config-vlan)#name Administración
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología	S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa	S1(config)#interface 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	Utilizar la red VLAN 1 como VLAN nativa	S1(config)#interface 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	Utilizar el comando interface range	S1(config-if)#interface range Fa0/1-2, Fa0/4, Fa0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21		S1(config-if-range)#interface Fa0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar		S1(config-if)#interface range Fa0/1-2, Fa0/4, Fa0/7-24, g0/1-2 S1(config-if-range)#shutdown

Fuente: Propia

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 14. Elementos de configuración de seguridad de S3

Elemento o tarea de configuración	Especificación	Comandos
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.	S3#configure terminal S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingeniería S3(config-vlan)#vlan 99 S3(config-vlan)#name Administración

Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología	S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa	S3(config)#interface Fa0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range	S3(config-if)#interface range Fa0/1-2, Fa0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 21		S3(config-if-range)#interface Fa0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar		S3(config-if)#interface range Fa0/1-2, Fa0/4-17, Fa0/19-24, g0/1-2 S3(config-if-range)#shutdown

Fuente: Propia

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 15. Elementos de configuración de seguridad de R1

Elemento o tarea de configuración	Especificación	Comandos
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	R1(config)#interface g0/1.21 R1(config-subif)#description Vlan 21 R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
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	R1(config-subif)#interface g0/1.23 R1(config-subif)#description Vlan 23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz	R1(config-subif)#interface g0/1.99 R1(config-subif)#description Vlan 99 R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	Utilizar la red VLAN 1 como VLAN nativa	R1(config-subif)#interface g0/1 R1(configif)#no shutdown

Fuente: Propia

Paso 4: Verificar la conectividad de la red

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

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

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

Tabla 16. Parámetros para medir la conectividad

Desde	A	Direccion IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Realizado correctamente
S3	R1, dirección VLAN 99	192.168.99.1	Realizado correctamente
S1	R1, dirección VLAN 21	192.168.21.1	Realizado correctamente
S3	R1, dirección VLAN 23	192.168.23.1	Realizado correctamente

Fuente: Propia

Figura 8. Ping de S1 a R1, dirección VLAN 99

```
S1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/4/16 ms

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
```

Fuente: Propia

Figura 9. Ping de S3 a R1, dirección VLAN 99

```
S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/11/45 ms

S3#ping 192.168.99.1

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

Fuente: Propia

Figura 10. Ping de S1 a R1, dirección VLAN 21

```
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 80 percent (4/5), round-trip min/avg/max = 0/4/16 ms

S1#ping 192.168.99.1

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

S1#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
```

Fuente: Propia

Figura 11. Ping de S3 a R1, dirección VLAN 23

```
S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/11/45 ms

S3#ping 192.168.99.1

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

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
```

Fuente: Propia

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17. Configuración OSPF en el R1

Elemento o tarea de configuración	Especificación	Comandos
Configurar OSPF área 0		R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.	R1(config-router)#do show ip route connected R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas		R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática		R1(config-router)#no auto-summary

Fuente: Propia

Figura 12. Configuración R1

```
R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#do show ip route connected
 C   172.16.1.0/30  is directly connected, Serial0/0/0
 C   192.168.21.0/24  is directly connected, GigabitEthernet0/1.21
 C   192.168.23.0/24  is directly connected, GigabitEthernet0/1.23
 C   192.168.99.0/24  is directly connected, GigabitEthernet0/1.99

R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
R1(config-router)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
R1(config-router)#no auto-summary
```

Fuente: Propia

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 18. Configurar OSPF en el R2

Elemento o tarea de configuración	Especificación	Comandos
Configurar OSPF área 0		R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.	R2(config-router)#do show ip route connected R2(config-router)#network 10.10.10.10 0.0.0.255 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
Establecer la interfaz LAN		R2(config-router)#passive-interface loopback 0

(loopback) como pasiva		
Desactive la sumarización automática		R2(config-router)#no auto-summary

Fuente: Propia

Figura 13. Configuración R2

```
R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2
R2(config-router)#do show ip route connected
 C    10.10.10.10/32  is directly connected, Loopback0
 C    172.16.1.0/30  is directly connected, Serial0/0/0
 C    172.16.2.0/30  is directly connected, Serial0/0/1
 C    209.165.200.232/29  is directly connected, GigabitEthernet0/0

R2(config-router)#network 10.10.10.10 0.0.0.255 area 0
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0
R2(config-router)#
03:24:53: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL,
Loading Done

R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
R2(config-router)#passive-interface loopback 0
R2(config-router)#no auto-summary
```

Fuente: Propia

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 19. Configurar OSPFv3 en el R2

Elemento o tarea de configuración	Especificación	Comandos
Configurar OSPF área 0		R3(config)#router ospf 1 R3(config-router)#router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente		R3(config-router)#do show ip route connected R3(config-router)#network 172.16.2.0 0.0.0.3 area 0

		R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas		R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.		R3(config-router)#no auto-summary

Fuente: Propia

Figura 14. Configuración R3

```
R3>enable
Password:
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#do show ip route connected
 C    172.16.2.0/30  is directly connected, Serial0/0/1
 C    192.168.4.0/24  is directly connected, Loopback4
 C    192.168.5.0/24  is directly connected, Loopback5
 C    192.168.6.0/24  is directly connected, Loopback6

R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
R3(config-router)#
03:26:10: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to FULL,
Loading Done

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 loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
R3(config-router)#no auto-summary
```

Fuente: Propia

Paso 4: Verificar la información de OSPF

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

Tabla 20. Preguntas para verificar la 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 run | section router ospf

Fuente: Propia

Figura 15. Comando show ip protocols

```
R2#Show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.10.10.0 0.0.0.255 area 0
    172.16.1.0 0.0.0.3 area 0
    172.16.2.0 0.0.0.3 area 0
  Passive Interface(s):
    Loopback0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:06:01
    2.2.2.2              110      00:06:00
    3.3.3.3              110      00:06:00
  Distance: (default is 110)
```

Fuente: Propia

Figura 16. Comando show ip route ospf

```
R2#Show ip route ospf
     192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/65] via 172.16.2.1, 00:09:38, Serial0/0/1
     192.168.5.0/32 is subnetted, 1 subnets
O       192.168.5.1 [110/65] via 172.16.2.1, 00:09:38, Serial0/0/1
     192.168.6.0/32 is subnetted, 1 subnets
O       192.168.6.1 [110/65] via 172.16.2.1, 00:09:38, Serial0/0/1
O    192.168.21.0 [110/65] via 172.16.1.1, 00:09:38, Serial0/0/0
O    192.168.23.0 [110/65] via 172.16.1.1, 00:09:38, Serial0/0/0
O    192.168.99.0 [110/65] via 172.16.1.1, 00:09:38, Serial0/0/0
```

Fuente: Propia

Figura 17. Comando show run | section router ospf

```
R2#Show run | section router ospf
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 passive-interface Loopback0
 network 10.10.10.0 0.0.0.255 area 0
 network 172.16.1.0 0.0.0.3 area 0
 network 172.16.2.0 0.0.0.3 area 0
```

Fuente: Propia

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 21. Configuración de R1 como servidor de DHCP para las VLAN 21 y 23

Elemento o tarea de configuración	Especificación	Comandos
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 Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado	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)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1
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	R1(dhcp-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)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1

Fuente: Propia

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

La configuración del R2 incluye las siguientes tareas:

Tabla 22. Configuración de la NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación	Comandos
Crear una base de datos local con una	Nombre de usuario: webuser	R2(config)#username webuser secret cisco12345 privilege 15

cuenta de usuario	Contraseña: cisco12345 Nivel de privilegio: 15	
Habilitar el servicio del servidor HTTP		R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación		R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.238	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)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#interface s0/0/0 R2(config-if)#ip nat inside R2(config-if)#interface s0/0/1 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica		R2(config)#ip nat inside source list 1 pool INTERNET

Fuente: Propia

Paso 3: Verificar el protocolo DHCP y la NAT estática

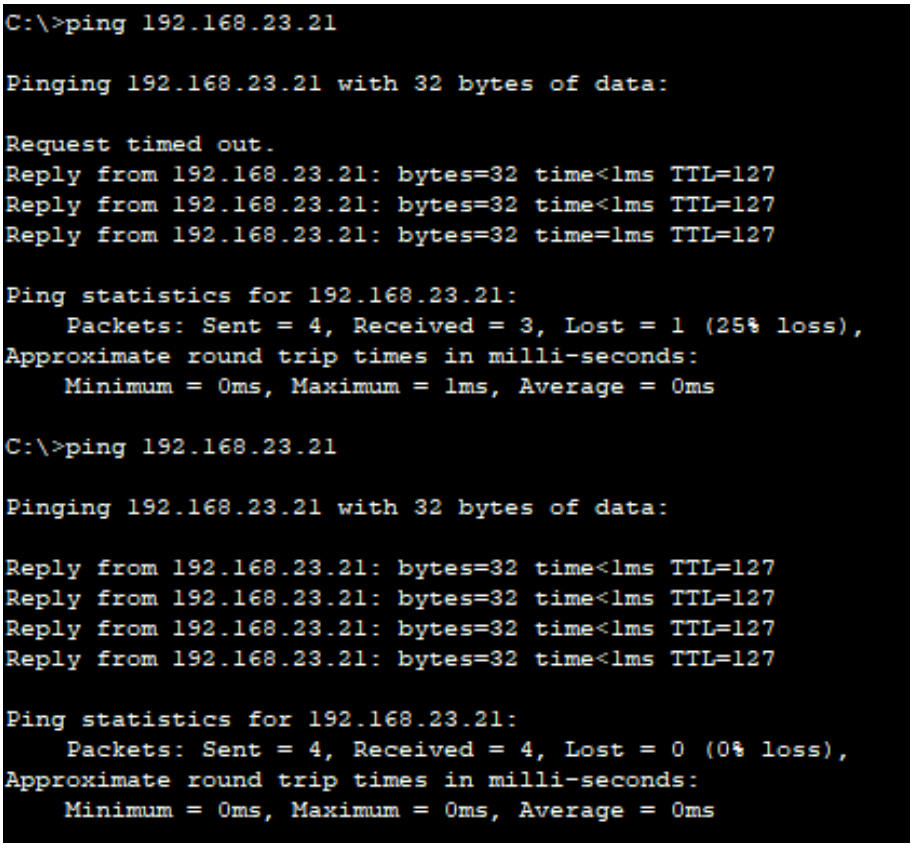
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 23. Parámetros para verificación el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	La PC-A adquirio una IP del servidor DHCP
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	La PC-B adquirio una IP del servidor DHCP
Verificar que la PC-A pueda hacer ping a la PC-B **Nota:** Quizá sea necesario deshabilitar el firewall de la PB.	Realizado correctamente
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.238) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Se realiza correctamente el procedimiento

Fuente: Propia

Figura 15. Ping de PC-A a PC-B



Fuente: Propia

Parte 6: Configurar NTP

Tabla 24. Configuración NTP

Elemento o tarea de configuración	Especificación	Comandos
Ajuste la fecha y hora en R2.	5 de marzo de 2016, 9 a. m.	R2#clock set 09:00:00 5 March 2016
Configure R2 como un maestro NTP	Nivel de estrato: 5	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Servidor: R2	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.		R1#show ntp associations

Fuente: Propia

Figura 16. Configuracion en R1

```
R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ntp server 172.16.1.2
R1(config)#ntp updatecalendar
                 ^
% Invalid input detected at '^' marker.

R1(config)#ntp update-calendar
R1(config)#show ntp associations
           ^
% Invalid input detected at '^' marker.

R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ntp associations

address         ref clock       st   when     poll    reach  delay          offset
disp
 ~172.16.1.2    127.127.1.1     5    12       16      7      15.00
726218610839.00   0.12
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

Fuente: Propia

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

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

Tabla 25. Restricciones del acceso a las líneas VTY en el R2

Elemento o tarea de configuración	Especificación	Comandos
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMINMGT**	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
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		R1#telnet 172.16.1.2

Fuente: Propia

Figura 17. Verificacion de conexion desde R1 a R2

```
R1#show ntp associations

address         ref clock       st   when     poll    reach  delay          offset
disp
 ~172.16.1.2    127.127.1.1     5    12       16      7      15.00
726218610839.00   0.12
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R1#
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenSe prohbe el acceso no autorizado
```

Fuente: Propia

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

Tabla 26. Pruebas finales

Descripción del comando	Entrada del estudiante (comando)	Comandos
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció		R2#show access-list
Restablecer los contadores de una lista de acceso		R2#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?		R2#show ip interface
¿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	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?		R2#clear ip nat translation *

Fuente: Propia

Figura 18. Comando show access-list

```
R2#show access-list
Standard IP access list 1
    10 permit 192.168.21.0 0.0.0.255
    20 permit 192.168.23.0 0.0.0.255
    30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
    10 permit host 172.16.1.1
```

Fuente: Propia

Figura 19. Comando show ip interface

```
R2#show ip interface
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 209.165.200.233/29
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
 --More--
```

Fuente: Propia

Figura 20. Comando show ip nat translations

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.229   10.10.10.10        ---                ---
---  209.165.200.237   10.10.10.10        ---                ---
```

Fuente: Propia

CONCLUSIONES

- El direccionamiento IP nos permite identificar cada uno de los componentes dentro de una red, nos permite saber qué dirección tiene cada host con el fin de poder ubicarlo dentro de la misma.

- Los componentes de red permiten ser manipulados por medio de consola en la cual se utilizan gran cantidad de comando que permiten configurar cada uno de los parámetros que hacen que los componentes se comuniquen entre sí.

- A la hora de configurar un componente de red debemos tener presente los puertos en los cuales hemos conectado cada uno de los cables con el fin de que las configuraciones aplicadas funcionen de la manera esperada.

- Las topologias de red realizadas dentro de los dos ejercicios practicos nos permitieron aplicar el uso y configuracion de routers, switchs, servidores y computadoras, permitiendo de esta forma tener una mejor adherencia del conocimiento.

- Cada uno de los escenarios planteados nos permitio adentrarnos en las configuraciones de los dispositivos de red permitiendo conocer cada comando y cada configuracion del mismo.

- La configuracion de los equipos nos permitio aprender el uso de configuracion de password, modo de usuario privilegiado, contraseñas encriptadas y reinicio de dispositivos.

BIBLIOGRAFIA

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

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

[3] BAREÑO, Gutiérrez, R., Sevillano, A. M. L., Díaz-Piraquive, F. N., & González-Crespo, R. (2021, July). Analysis of WEB Browsers of HSTS Security Under the MITM Management Environment. In International Conference on Knowledge Management in Organizations (pp. 331-344). Springer, Cham.

[4] BAREÑO, Gutiérrez, R., Cardenas-Urrea, S. E., Navarro-Nuñez, W., Sarmiento-Osorio, H., & Forero-Paez, N. (2017). Sistema de votación electrónico con características de seguridad SSL/TLS e IPsec en Colombia. Revista UIS Ingenierías, 16(1), 75-84.

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

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

[7] MOJICA S. Felipe, Andrés, L. V. S., & Raúl, B. G. (2019, October). Risks Found in Electronic Payment Cards on Integrated Public Transport System Applying the ISO 27005 Standard. Case Study Sitp DC Colombia. In 2019 Congreso Internacional de Innovación y Tendencias en Ingenieria (CONIITI) (pp. 1-6). IEEE.