

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA
CISCO

VICTOR ALFONSO CORTES

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

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA
CISCO

VICTOR ALFONSO CORTES

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

DIRECTOR:
JAVIER RICARDO VASQUEZ

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

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

CHIQUINQUIRÁ, 28 de noviembre de 2021

CONTENIDO

CONTENIDO	4
LISTA DE TABLAS	5
LISTA DE FIGURAS	6
GLOSARIO	8
RESUMEN.....	9
ABSTRACT.....	10
INTRODUCCIÓN	11
DESARROLLO	12
1. ESCENARIO 1	12
2. ESCENARIO 2	23
CONCLUSIONES	70
BIBLIOGRAFÍA.....	71

LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento para el primer escenario.	13
Tabla 2. Direccionamiento para la Subred LAN1.	14
Tabla 3. Esquema de direccionamiento para la Subred LAN1.	14
Tabla 4. Direccionamiento para la Subred LAN2.	14
Tabla 5. Esquema de direccionamiento para la Subred LAN2.	14
Tabla 6. Tabla de direccionamiento general para el escenario 1.	14
Tabla 7. Lista de configuraciones para aplicar en R1.	15
Tabla 8. Lista de configuraciones para aplicar en S1.	17
Tabla 9. Lista de configuraciones para aplicar en PC-A.	19
Tabla 10. Lista de configuraciones para aplicar en PC-B.	20
Tabla 11. Lista de configuraciones de inicializar y volver a cargar los routers y los switches.	24
Tabla 12. Configuración de la computadora de Internet.	25
Tabla 13. Configuración del dispositivo R1.	26
Tabla 14. Configuración del dispositivo R2.	28
Tabla 15. Configuración del dispositivo R3.	31
Tabla 16. Configuración del dispositivo S1.	34
Tabla 17. Configuración del dispositivo S1.	35
Tabla 18. Verificación de la conectividad de la red.	36
Tabla 19. Configuración de seguridad, VLAN y routing entre VLAN en S1.	39
Tabla 20. Configuración de seguridad, VLAN y routing entre VLAN en S3.	41
Tabla 21. Configuración de subinterfaces en R1.	43
Tabla 22. Lista de verificaciones de la conectividad de la red.	45
Tabla 23. Tareas de configuración para R1.	48
Tabla 24. Tareas de configuración para R2.	49
Tabla 25. Tareas de configuración para R2.	50
Tabla 26. Verificación de la información de OSPF.	51
Tabla 27. Lista de tareas de configuración DHCP en R1 para las VLANS 21 y 23.	56
Tabla 28. Lista de tareas de configuración NAT estática y dinámica en R2.	58
Tabla 29. Lista de tareas de verificación del protocolo DHCP y la NAT estática. ...	59
Tabla 30. Lista de tareas de configuración NTP.	62
Tabla 31. Lista de tareas de configuración y verificación de listas de control de acceso en R2.	63
Tabla 32. Lista de tareas de verificación de comando CLI.	66

LISTA DE FIGURAS

Figura 1. Topología escenario 1.	12
Figura 2. Construcción de la topología de la red.....	13
Figura 3. Evidencia de la configuración del PC-A.	20
Figura 4. Evidencia de la configuración del PC-B.	21
Figura 5. Evidencia de la configuración general desde PC-A.	22
Figura 6. Topología escenario 2.	23
Figura 7. Configuración del Servidor de Internet.....	26
Figura 8. Validación de ping desde R1 a R2.....	38
Figura 9. Validación de ping desde R2 a R3.....	38
Figura 10. Validación de ping desde Servidor de Internet a su Gateway.....	39
Figura 11. Validación de ping desde S1 a R1, dirección VLAN 99.	46
Figura 12. Validación de ping desde S3 a R1, dirección VLAN 99.	46
Figura 13. Validación de ping desde S1 a R1, dirección VLAN 21.	47
Figura 14. Validación de ping desde S3 a R1, dirección VLAN 23.	47
Figura 15. Verificación del ID del proceso OSPF, del router, las redes de routing y las interfaces pasivas en R1.....	52
Figura 16. Verificación de las rutas OSPF en R1.....	52
Figura 17. Verificación de sección de OSPF de la configuración en ejecución en R1.....	53
Figura 18. Verificación del ID del proceso OSPF, del router, las redes de routing y las interfaces pasivas en R2.....	53
Figura 19. Verificación de las rutas OSPF en R2.....	54
Figura 20. Verificación de sección de OSPF de la configuración en ejecución en R2.....	54
Figura 21. Verificación del ID del proceso OSPF, del router, las redes de routing y las interfaces pasivas en R3.....	55
Figura 22. Verificación de las rutas OSPF en R3.....	55
Figura 23. Verificación de sección de OSPF de la configuración en ejecución en R3.....	56
Figura 24. Verificación del direccionamiento DHCP en PC-A.....	60
Figura 25. Verificación del direccionamiento DHCP en PC-C.....	61
Figura 26. Verificación del ping entre PC-A y PC-C.....	61
Figura 27. Verificación de la conexión al servidor web.	62
Figura 28. Verificación de la configuración NTP en R1.....	63
Figura 29. Verificación del funcionamiento de la ACL en PC-A.	65
Figura 30. Verificación del funcionamiento de la ACL en R1.	65

Figura 31. Mostrar las coincidencias recibidas luego de ser establecida en R2. ...	67
Figura 32. Restablecer los contadores de una lista de acceso.	67
Figura 33. Mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica.	68
Figura 34. Mostrar las traducciones NAT.	68
Figura 35. Comando utilizado para eliminar las traducciones de NAT dinámicas.	69

GLOSARIO

ACL: Una lista de control de acceso (ACL) es filtros de tráfico de una lista de redes y acciones correlacionadas usados para mejorar la Seguridad. Bloquea o permite que los usuarios accedan los recursos específicos. Un ACL contiene los hosts se permiten que o acceso negado al dispositivo de red. El router o el Switch examina cada paquete para determinar si remitir o caer el paquete, en base de los criterios especificados dentro de las Listas de acceso. Los criterios de lista de acceso podían ser la dirección de origen del tráfico, la dirección destino del tráfico, el Upper-Layer Protocol, o la otra información.

IPv4: El IPv4 es un sistema direccional de 32 bits usado para identificar un dispositivo en una red. Es el sistema direccional usado en la mayoría de las redes informáticas, incluyendo Internet.

IPv6: El IPv6 es un sistema direccional del 128-bit usado para identificar un dispositivo en una red. Es el sucesor al IPv4 y a la mayoría de la versión reciente del sistema direccional usado en las redes informáticas. El IPv6 se está desarrollando actualmente en todo el mundo. Un direccionamiento del IPv6 se representa en ocho campos de los números hexadecimales, cada campo que contiene 16 bits. Un direccionamiento del IPv6 se divide en dos porciones, cada parte integrada por 64 bits. La primera parte que es la dirección de red, y la segunda parte la dirección de host.

NAT: La traducción de direcciones de red, también llamado enmascaramiento de IP o NAT, es un mecanismo utilizado por routers IP para cambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados.

NTP: Network Time Protocol (NTP) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable.

OSPF: Open Shortest Path First, Abrir el camino más corto primero en español, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol, que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

VLA N basado en protocolos: Los grupos basados en protocolos pueden ser definidos y estar limitados a un puerto; por lo tanto, cada paquete que origina de los grupos de protocolos se asigna al VLAN configurado en la página. El VLA N basado en protocolos divide la red física en los grupos VLAN lógicos para cada protocolo requerido.

RESUMEN

En el desarrollo de esta actividad se configuran los dispositivos de una red pequeña. Esta red cuenta con una configuración de un router, un switch y equipos, se diseña el esquema de direccionamiento IPv4 para las LAN propuestas. El router y el switch también deben administrarse de forma segura. Esta seguridad que cuenta el dispositivo está ligada con la configuración inicial donde cuenta con la desactivación de la búsqueda DNS, el nombramiento del dispositivo, la asignación del nombre de dominio, el cifrado de la contraseña tanto del EXEC privilegiado como las líneas de consola y VTY. Las líneas de consola se configuran para aceptar SSH, se crea un usuario administrativo en la base de datos local y se asigna su contraseña cifrada.

Para el segundo escenario, se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, se debe realizar la configuración de la seguridad de switches, implementar el routing entre VLAN, asignar el protocolo de routing dinámico OSPF a las interfaces requeridas, el protocolo de configuración de hosts dinámicos, la traducción de direcciones de red dinámicas y estáticas, listas de control de acceso y el protocolo de tiempo de red (NTP) servidor/cliente.

Palabras clave: Protocolos, Enrutamiento, OSPF, NAT, NTP, VLAN, Cisco.

ABSTRACT

In the development of this activity, the devices of a small network are configured. This network has a configuration of a router, a switch and equipment, the IPv4 addressing scheme is designed for the LAN proposals. The router and switch must also be managed securely. This security that the device has is linked to the initial configuration where it has the deactivation of the DNS search, the naming of the device, the assignment of the domain name, the encryption of the password of both the privileged EXEC and the console lines and VTY . The console lines are configured to accept SSH, an administrative user is created in the local database, and its encrypted password is assigned.

For the second scenario, a small network must be configured to support IPv4 and IPv6 connectivity, switch security configuration must be performed, inter-VLAN routing must be implemented, the OSPF dynamic routing protocol assigned to the required interfaces, the protocol dynamic host configuration, static and dynamic network address translation, access control lists, and server / client Network Time Protocol (NTP).

Keywords: Protocols, Routing, OSPF, NAT, NTP, VLAN, Cisco.

INTRODUCCIÓN

En esta prueba de habilidades se ponen evidencia los conocimientos adquiridos a través del diplomado de profundización, llevando desde la construcción de la simulación de la red, el desarrollo de esquemas de direccionamiento ip detallando la estructura de los dispositivos, sean direcciones IPv4 e IPv6, la forma como obtener sus distintas subredes a partir de la dirección general y comprender internamente la operación para obtener su respectiva máscara de red. Además, se aplican conceptos que están relacionados con la aplicación de seguridad, que va desde la aplicación de SSH en vez de TELNET; la aplicación de servicios de cifrados de clave de texto plano, la asignación de claves a la línea de consola y la línea de terminal, la asignación de banners que informen al administrador, advertencias sobre el uso inadecuado o accesos no autorizados a los dispositivos, la configuración de direccionamiento en cada una de las interfaces, tanto físicas como lógicas y la verificación de la conectividad entre los host y los dispositivos.

Estos retos son representados a través de escenarios que varían su estructura, su diseño y su esquema de red, donde en el primer escenario se ponen a prueba los conceptos básicos de configuración y adecuación, mientras que en el segundo escenario, se realiza la implementación del protocolo de enrutamiento OSPF para conectar subredes distintas y la aplicación de conceptos inter-vlan en uno de ellos.

Cada uno de estos escenarios son una representación de las posibles situaciones a las que se están expuestas los administradores de redes y ponen a prueba los conceptos adquiridos como una preparación al constante avance tecnológico que estamos expuestos.

DESARROLLO

1. ESCENARIO 1

Topología.

Figura 1. Topología escenario 1.



Fuente: Autor.

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 switch 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. Construcción de la topología de la red.



Fuente: Autor.

Para la construcción de esta topología, se hace uso de la herramienta GNS3 con su respectivo servidor VM alojado en VirtualBox. Consta de 4 dispositivos, dos finales, un conmutador y un enrutador. Los PCs cuentan con configuración básica, para agregar direccionamiento ip, el conmutador cuenta con la versión de IOS Cisco IOS Software, ios_12 Software (ios_12-ADVENTERPRISEK9-M), Experimental Version 15.2(20170321:233949). Finalmente, el router cuenta con la versión de IOS 7200 Software (C7200-ADVENTERPRISEK9-M), Version 15.2(4)M7.

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.

En este caso, el número de cédula es 1073380945 por lo que el direccionamiento parte de la siguiente dirección de red 192.168.45.0.

Tabla 1. Tabla de direccionamiento para el primer escenario.

Item	Requerimiento
Dirección de red	192.168.45.0
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	Primera dirección de host de la subred LAN1
R1 G0/0/0	Primera dirección de host de la subred LAN2
S1 SVI	Segunda dirección de host de la subred LAN1

PC-A	Última dirección de host de la subred LAN1
PC-B	Última dirección de host de la subred LAN2

Fuente: Autor.

Tabla 2. Direccionamiento para la Subred LAN1.

Dirección de subred	192.168.45.0	
Gateway	192.168.45.1	255.255.255.128
1er Host	192.168.45.2	255.255.255.128
Último Host	192.168.45.126	255.255.255.128
Broadcast	192.168.45.127	255.255.255.128

Fuente: Autor.

Tabla 3. Esquema de direccionamiento para la Subred LAN1.

Dispositivo	Interfaz	Dirección	Máscara	Gateway
R1	Gi0/0	192.168.45.1	255.255.255.128	
S1	SVI	192.168.45.2	255.255.255.128	192.168.45.1
PC-A	Ethernet0	192.168.45.126	255.255.255.128	192.168.45.1

Fuente: Autor.

Tabla 4. Direccionamiento para la Subred LAN2.

Dirección de subred	192.168.45.128	
Gateway	192.168.45.129	255.255.255.192
1er Host	192.168.45.130	255.255.255.192
Último Host	192.168.45.190	255.255.255.192
Broadcast	192.168.45.191	255.255.255.192

Fuente: Autor.

Tabla 5. Esquema de direccionamiento para la Subred LAN2.

Dispositivo	Interfaz	Dirección	Máscara	Gateway
R1	Gi1/0	192.168.45.129	255.255.255.192	
PC-B	Ethernet0	192.168.45.190	255.255.255.192	192.168.45.129

Fuente: Autor.

Tabla 6. Tabla de direccionamiento general para el escenario 1.

Dispositivo	Interfaz	Dirección	Máscara	Gateway
R1	Gi0/0	192.168.45.1	255.255.255.128	
	Gi1/0	192.168.45.129	255.255.255.192	
S1	SVI	192.168.45.2	255.255.255.128	192.168.45.1
PC-A	Ethernet0	192.168.45.126	255.255.255.128	192.168.45.1
PC-B	Ethernet0	192.168.45.190	255.255.255.192	192.168.45.129

Fuente: Autor.

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 7. Lista de configuraciones para aplicar en R1.

Tarea	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R1
Nombre de 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 caracteres
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	Módulo de 1024 bits

Fuente: Autor.

Configuración de R1.

R1#configure terminal

R1(config)#no ip domain-lookup
búsqueda de dominio

Se desactiva la

R1(config)#hostname R1
del dispositivo

Se agrega el nombre

R1(config)#ip domain-name ccna-lab.com <i>del dominio</i>	Se agrega el nombre
R1(config)#enable secret ciscoenpass <i>contraseña de exec secreta</i>	Se agrega una
R1(config)#line con 0 <i>configuración de la línea de consola</i>	Se accede a la
R1(config-line)#password ciscoconpass <i>contraseña para el acceso a la línea de consola</i>	Se habilita una
R1(config-line)#login <i>de la contraseña</i>	Se habilita la revisión
R1(config-line)#exit	
R1(config)#security passwords min-length 10 <i>longitud de las contraseñas sea de mínimo 10 caracteres</i>	Se habilita que la
R1(config)#username admin password admin1pass <i>administrativo</i>	Se crea un usuario
R1(config)#crypto key generate rsa <i>de cifrado de 1024 bit RSA.</i>	Se genera una llave
R1(config)#ip ssh version 2 <i>versión 2</i>	Se habilita ip ssh
R1(config)#line vty 0 4	
R1(config-line)#login local <i>use la base de datos local.</i>	Se configura para que
R1(config-line)#transport input ssh <i>transporte por la línea solo ssh</i>	Se habilita el
R1(config-line)#exit	
R1(config)#interface gi0/0 <i>interfaz gi0/0</i>	Se accede a la
R1(config-if)#description LAN1 <i>descripción a la interfaz.</i>	Se agrega una
R1(config-if)#ip add 192.168.45.1 255.255.255.128 <i>direccionamiento a la interfaz gi0/0</i>	Se agrega el
R1(config-if)#no shutdown <i>gi0/0</i>	Se activa la interfaz
R1(config-if)#exit	
R1(config)#interface gi1/0 <i>interfaz</i>	Se accede a la
R1(config-if)#description LAN2 <i>descripción a la interfaz</i>	Se agrega una

R1(config-if)#ip add 192.168.45.129 255.255.255.192 Se agrega el direccionamiento a la interfaz gi1/0

R1(config-if)#no shutdown Se activa la interfaz gi1/0

R1(config-if)#exit

R1(config)#service password-encryption Se cifran las contraseñas de texto no cifrado.

R1(config)#banner motd #El acceso no autorizado esta prohibido# Se añade un banner que muestra un mensaje de alerta.

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 8. Lista de configuraciones para aplicar en S1.

Tarea	Especificación
Desactivar la búsqueda DNS.	
Nombre del switch	S1
Nombre de 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 las líneas VTY para que acepten únicamente las conexiones SSH	
Cifrar las contraseñas de texto no cifrado	
Configurar un MOTD Banner	
Generar una clave de cifrado RSA	Módulo de 1024 bits
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: Autor.

Configuración de S1.

IOU1#configure terminal

IOU1(config)#hostname S1 Se asigna el nombre del dispositivo

S1(config)#no ip domain-lookup <i>búsqueda de dominio</i>	Se desactiva la
S1(config)#ip domain-name ccna-lab.com <i>de dominio</i>	Se asigna un nombre
S1(config)#enable secret ciscoenpass <i>cifrado para exec</i>	Se habilita la clave de
S1(config)#line con 0 <i>de consola</i>	Se ingresa a la línea
S1(config-line)#password ciscoconpass <i>consola</i>	Se asigna la clave de
S1(config-line)#login <i>verificación de la contraseña de consola</i>	Se habilita la
S1(config-line)#exit	
S1(config)#username admin password admin1pass <i>administrativo</i>	Se crea un usuario
S1(config)#crypto key generate rsa <i>de cifrado RSA de 1024 bits</i>	Se genera una clave
S1(config)#ip ssh version 2 <i>versión 2</i>	Se habilita ssh en su
S1(config)#line vty 0 4 <i>de terminal</i>	Se accede a la línea
S1(config-line)#login local <i>valide el acceso con base de datos local</i>	Se configura para que
S1(config-line)#transport input ssh <i>ssh</i>	Se habilita la conexión
S1(config-line)#exit	
S1(config)#service password-encryption <i>contraseñas de texto no cifrado.</i>	Se cifran las
S1(config)#banner motd #El acceso no autorizado esta prohibido# <i>un mensaje de alerta</i>	Se configura
S1(config)#interface vlan 1 <i>interfaz vlan predeterminada</i>	Se accede a la
S1(config-if)#description SVI S1 <i>descripción a la SVI</i>	Se agrega un
S1(config-if)#ip add 192.168.45.2 255.255.255.128 <i>dirección ip de capa 3.</i>	Se asigna una
S1(config-if)#no shutdown <i>interfaz</i>	Se enciende la
S1(config-if)#exit	

S1(config)#ip default-gateway 192.168.45.1
 dirección Gateway predeterminada en S1
 S1(config)#

Se configura la

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 9. Lista de configuraciones para aplicar en PC-A.

PC-A Network Configuration	
Descripción	PC-A
Dirección física	00:50:79:66:68:00
Dirección IP	192.168.45.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.45.1

Fuente: Autor.

Configuración del equipo PC-A

PC-A> ip 192.168.45.126 255.255.255.128 192.168.45.1 Se configura la
 dirección ip del PC-A, se define su máscara de red y su dirección Gateway

PC-A> save Se utiliza este
 comando para guardar los cambios realizados en PC-A

PC-A> show Se utiliza este
 comando para mostrar la información del PC-A

```

NAME IP/MASK      GATEWAY      MAC          LPORT
RHOST:PORT
PC-A 192.168.45.126/25 192.168.45.1 00:50:79:66:68:00 20010
127.0.0.1:20011
      fe80::250:79ff:fe66:6800/64

```

PC-A>

Figura 3. Evidencia de la configuración del PC-A.



Fuente: Autor.

Tabla 10. Lista de configuraciones para aplicar en PC-B.

PC-B Network Configuration	
Descripción	PC-B
Dirección física	
Dirección IP	192.168.45.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.45.129

Fuente: Autor.

Configuración del equipo PC-B

PC-B> ip 192.168.45.190 255.255.255.192 192.168.45.129 Se configura la dirección ip del PC-B, se define su máscara de red y su dirección Gateway.

PC-B> show Se utiliza este comando para mostrar la información del PC-B

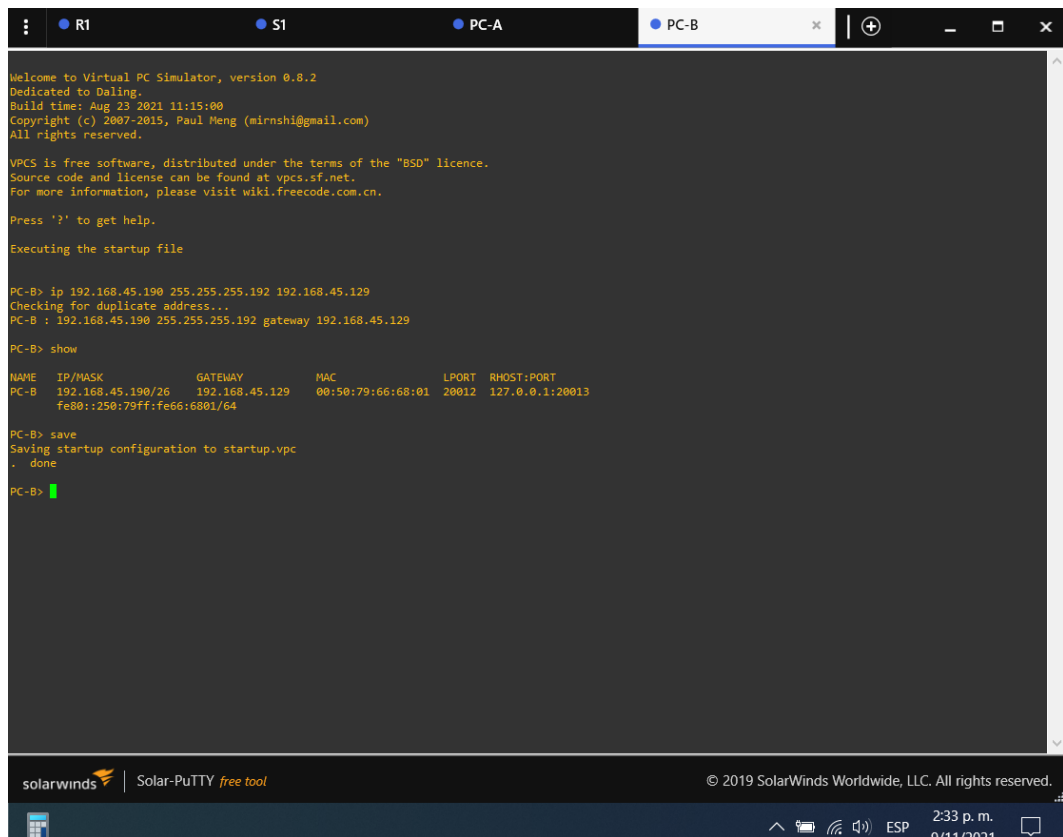
```

NAME IP/MASK      GATEWAY      MAC      LPORT
RHOST:PORT
PC-B 192.168.45.190/26 192.168.45.129 00:50:79:66:68:01 20012
127.0.0.1:20013
      fe80::250:79ff:fe66:6801/64

```

PC-B> save Se utiliza este
comando para guardar los cambios realizados en PC-B
PC-B>

Figura 4. Evidencia de la configuración del PC-B.



Fuente: Autor.

Finalmente, se hace ping de verificación a cada una de las interfaces desde el PC-A para verificar que funciona correctamente la topología de red.

Figura 5. Evidencia de la configuración general desde PC-A.



```
PC-A> ip 192.168.45.126 255.255.255.128 192.168.45.1
Checking for duplicate address...
PC-A : 192.168.45.126 255.255.255.128 gateway 192.168.45.1

PC-A> save
Saving startup configuration to startup.vpc
.
done

PC-A> show

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC-A 192.168.45.126/25 192.168.45.1 00:50:79:66:68:00 20010 127.0.0.1:20011
fe80::250:79ff:fe66:6800/64

PC-A> ping 192.168.45.1

84 bytes from 192.168.45.1 icmp_seq=1 ttl=255 time=13.854 ms
84 bytes from 192.168.45.1 icmp_seq=2 ttl=255 time=13.872 ms
84 bytes from 192.168.45.1 icmp_seq=3 ttl=255 time=9.273 ms
84 bytes from 192.168.45.1 icmp_seq=4 ttl=255 time=10.447 ms
84 bytes from 192.168.45.1 icmp_seq=5 ttl=255 time=13.609 ms

PC-A> ping 192.168.45.129

84 bytes from 192.168.45.129 icmp_seq=1 ttl=255 time=14.490 ms
84 bytes from 192.168.45.129 icmp_seq=2 ttl=255 time=8.411 ms
84 bytes from 192.168.45.129 icmp_seq=3 ttl=255 time=6.407 ms
84 bytes from 192.168.45.129 icmp_seq=4 ttl=255 time=7.562 ms
84 bytes from 192.168.45.129 icmp_seq=5 ttl=255 time=13.103 ms

PC-A> ping 192.168.45.2

84 bytes from 192.168.45.2 icmp_seq=1 ttl=255 time=5.998 ms
84 bytes from 192.168.45.2 icmp_seq=2 ttl=255 time=5.193 ms
84 bytes from 192.168.45.2 icmp_seq=3 ttl=255 time=5.263 ms
84 bytes from 192.168.45.2 icmp_seq=4 ttl=255 time=5.222 ms
84 bytes from 192.168.45.2 icmp_seq=5 ttl=255 time=7.947 ms

PC-A> ping 192.168.45.190

84 bytes from 192.168.45.190 icmp_seq=1 ttl=63 time=30.348 ms
84 bytes from 192.168.45.190 icmp_seq=2 ttl=63 time=27.583 ms
84 bytes from 192.168.45.190 icmp_seq=3 ttl=63 time=19.466 ms
84 bytes from 192.168.45.190 icmp_seq=4 ttl=63 time=24.165 ms
84 bytes from 192.168.45.190 icmp_seq=5 ttl=63 time=20.412 ms

PC-A>
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

2:36 p. m. 9/11/2021

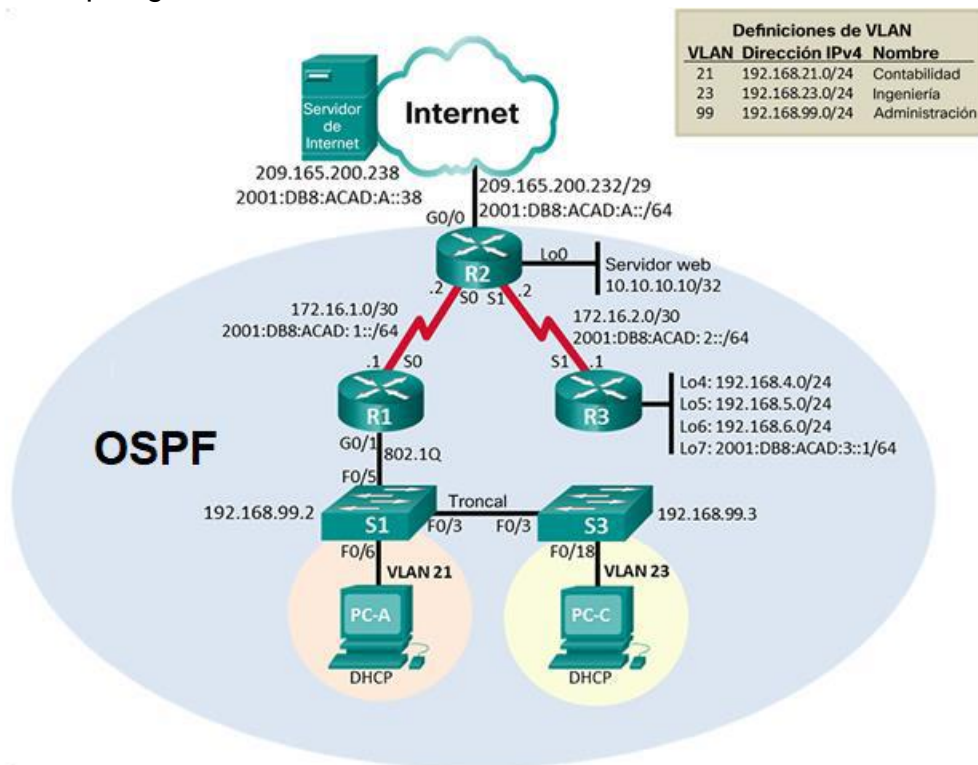
Fuente: Autor.

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 6. Topología escenario 2.



Fuente: Autor.

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 11. Lista de configuraciones de inicializar y volver a cargar los routers y los switches.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	
Volver a cargar todos los routers	
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	
Volver a cargar ambos switches	
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	

Fuente: Autor.

Configuración en R1

R1#erase startup-config
startup-config
 R1#reload
dispositivo

Elimina el archivo

Vuelve a cargar el

Configuración en R2

R2#erase startup-config
startup-config
 R2#reload
dispositivo

Elimina el archivo

Vuelve a cargar el

Configuración en R3

R3#erase startup-config
startup-config
 R3#reload
dispositivo

Elimina el archivo

Vuelve a cargar el

Configuración en S1

S1#erase startup-config
startup-config

Elimina el archivo

S1#reload
dispositivo

Vuelve a cargar el

Configuración en S3

S3#erase startup-config
startup-config

Elimina el archivo

S3#reload
dispositivo

Vuelve a cargar el

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):

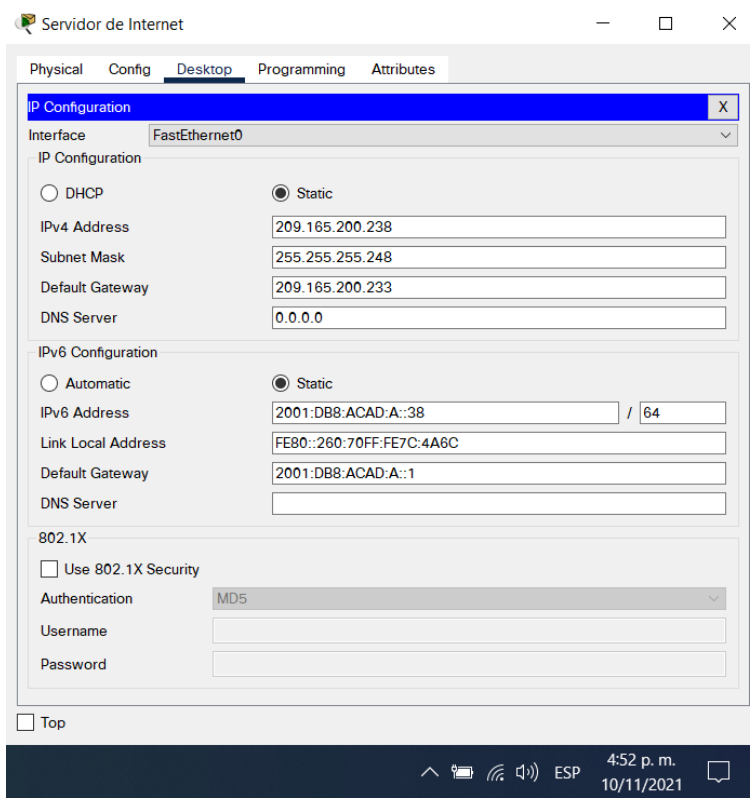
Tabla 12. Configuración de la computadora de Internet.

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Fuente: Autor.

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 7. Configuración del Servidor de Internet.



Fuente: Autor.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 13. Configuración del dispositivo R1.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	R1
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	Service password-encryption
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: Autor.

Nota: Todavía no configure G0/1.

Configuración en R1

R1#configure terminal	
R1(config)#no ip domain-lookup <i>búsqueda de dominio</i>	Se desactiva la
R1(config)#hostname R1 <i>de host a R1</i>	Se asigna un nombre
R1(config)#enable secret class <i>contraseña de exec privilegiado cifrada</i>	Se asigna la
R1(config)#line con 0 <i>de consola</i>	Se ingresa a la línea
R1(config-line)#password cisco <i>consola</i>	Se asigna la clave de
R1(config-line)#login <i>validación de contraseña</i>	Se habilita la
R1(config-line)#exit	
R1(config)#line vty 0 4 <i>telnet</i>	Se ingresa a la línea
R1(config-line)#password cisco <i>telnet</i>	Se asigna la clave de
R1(config-line)#login <i>validación de contraseña telnet</i>	Se habilita la

R1(config-line)#exit	
R1(config)#service password-encryption	Se activa el servicio de encriptación de contraseñas
R1(config)#banner motd #El acceso no autorizado esta prohibido#	Se agrega un mensaje de alerta
R1(config)#interface se0/0/0	Se accede a la interfaz serial1/0
R1(config-if)#description WAN a R2	Se agrega la descripción a la interfaz serial
R1(config-if)#ip add 172.16.1.1 255.255.255.252	Se asigna la dirección ipv4.
R1(config-if)#ipv6 add 2001:db8:acad:1::1/64	Se asigna la dirección ipv6
R1(config-if)#clock rate 128000	Se establece la velocidad de la conexión serial.
R1(config-if)#no shutdown	Se enciende la interfaz
R1(config-if)#exit	
R1(config)#ip route 0.0.0.0 0.0.0.0 se1/0	Se agrega una ruta estática predeterminada ipv4
R1(config)#ipv6 route ::/0 se1/0	Se agrega una ruta estática predeterminada ipv6
R1(config)#	

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 14. Configuración del dispositivo R2.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	R2
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	Service password-encryption
Habilitar el servidor HTTP	Ip http server

Mensaje 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
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.
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

Fuente: Autor.

Configuración en R2.

R2#configure terminal

R2(config)#no ip domain-lookup
búsqueda de dominio

Se desactiva la

R2(config)#hostname R2
de host

Se asigna el nombre

R2(config)#enable secret class <i>contraseña de EXEC</i>	Se	asigna	la
R2(config)#line con 0			
R2(config-line)#password cisco <i>contraseña de consola</i>	Se	asigna	la
R2(config-line)#login <i>verificación de contraseña de consola</i>	Se	habilita	la
R2(config-line)#exit			
R2(config)#line vty 0 4			
R2(config-line)#password cisco <i>contraseña de terminal de acceso telnet</i>	Se	asigna	la
R2(config-line)#login <i>verificación de contraseña de acceso telnet</i>	Se	habilita	la
R2(config-line)#exit			
R2(config)#service password-encryption <i>de encriptación de contraseñas de texto plano</i>		Se	habilita el servicio
R2(config)#ip http server		Se	activa el servidor
R2(config)#banner motd #Se prohíbe el acceso no autorizado# <i>mensaje de alerta</i>		Se	habilita un
R2(config)#interface se0/0/0			
R2(config-if)#description WAN a R1 <i>descripción de la interfaz</i>	Se	agrega	la
R2(config-if)#ip add 172.16.1.2 255.255.255.252 <i>direccionamiento de la interfaz</i>	Se	asigna	el
R2(config-if)#ipv6 add 2001:db8:acad:1::2/64 <i>direccionamiento IPv6 de la interfaz</i>	Se	asigna	el
R2(config-if)#no shutdown <i>interfaz</i>	Se	enciende	la
R2(config-if)#exit			
R2(config)#interface se0/0/1			
R2(config-if)#description WAN a R3 <i>descripción de la interfaz</i>	Se	agrega	la
R2(config-if)#ip add 172.16.2.2 255.255.255.252 <i>direccionamiento de la interfaz</i>	Se	asigna	el
R2(config-if)#ipv6 add 2001:DB8:ACAD:2::2/64 <i>direccionamiento IPv6 de la interfaz</i>	Se	asigna	el
R2(config-if)#clock rate 128000 <i>velocidad de la sincronización</i>	Se	configura	la

R2(config-if)#no shutdown <i>interfaz</i>	Se	<i>enciende</i>	<i>la</i>
R2(config-if)#exit			
R2(config)#interface gi0/0			
R2(config-if)#description Simulacion de Internet <i>descripción de la interfaz</i>	Se	<i>agrega</i>	<i>la</i>
R2(config-if)#ip add 209.165.200.233 255.255.255.248 <i>direccionamiento de la interfaz</i>	Se	<i>asigna</i>	<i>el</i>
R2(config-if)#ipv6 add 2001:DB8:ACAD:A::1/64 <i>direccionamiento IPv6 de la interfaz</i>	Se	<i>asigna</i>	<i>el</i>
R2(config-if)#no shutdown <i>interfaz</i>	Se	<i>enciende</i>	<i>la</i>
R2(config-if)#exit			
R2(config)#interface lo0			
R2(config-if)#description Servidor Web Simulado <i>descripción de la interfaz loopback</i>	Se	<i>agrega</i>	<i>la</i>
R2(config-if)#ip add 10.10.10.10 255.255.255.255 <i>direccionamiento de la interfaz</i>	Se	<i>asigna</i>	<i>el</i>
R2(config-if)#no shutdown <i>interfaz</i>	Se	<i>enciende</i>	<i>la</i>
R2(config-if)#exit			
R2(config)#ip route 0.0.0.0 0.0.0.0 gi0/0 <i>predeterminada para el direccionamiento IPv4 en la interfaz Gi0/0</i>		<i>Se asigna una ruta</i>	
R2(config)#ipv6 route ::/0 gi0/0 <i>predeterminada para el direccionamiento IPv6 en la interfaz Gi0/0</i>		<i>Se asigna una ruta</i>	
R2(config)#			

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 15. Configuración del dispositivo R3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
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	Service password-encryption
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	Configure una ruta IPv4 e IPv6 predeterminada en la interface S0/0/1

Fuente: Autor.

Configuración en R3

R3#configure terminal	
R3(config)#no ip domain-lookup	Se desactiva la
<i>búsqueda de dominio</i>	
R3(config)#hostname R3	Se asigna el nombre
<i>de host</i>	
R3(config)#enable secret class	Se asigna la
<i>contraseña de EXEC</i>	
R3(config)#line con 0	
R3(config-line)#password cisco	Se asigna la
<i>contraseña de consola</i>	
R3(config-line)#login	Se habilita la
<i>verificación de contraseña de consola</i>	

R3(config-line)#exit			
R3(config)#line vty 0 4			
R3(config-line)#password cisco	Se	asigna	la
<i>contraseña de terminal de acceso telnet</i>			
R3(config-line)#login	Se	habilita	la
<i>verificación de contraseña de acceso telnet</i>			
R3(config-line)#exit			
R3(config)#service password-encryption	Se	habilita	el servicio
<i>de encriptación de contraseñas de texto plano</i>			
R3(config)#banner motd #Se prohíbe el acceso no autorizado#	Se	habilita	un
<i>mensaje de alerta</i>			
R3(config)#interface se0/0/1			
R3(config-if)#description WAN a R2	Se	agrega	la
<i>descripción de la interfaz</i>			
R3(config-if)#ip add 172.16.2.1 255.255.255.252	Se	asigna	el
<i>direccionamiento de la interfaz</i>			
R3(config-if)#ipv6 add 2001:DB8:ACAD:2::1/64	Se	asigna	el
<i>direccionamiento IPv6 de la interfaz</i>			
R3(config-if)#no shutdown	Se	enciende	la
<i>interfaz</i>			
R3(config-if)#exit			
R3(config)#interface lo4	Se	agrega	la
<i>descripción de la interfaz loopback</i>			
R3(config-if)#ip add 192.168.4.1 255.255.255.0	Se	asigna	el
<i>direccionamiento de la interfaz</i>			
R3(config-if)#exit			
R3(config)#interface lo5	Se	agrega	la
<i>descripción de la interfaz loopback</i>			
R3(config-if)#ip add 192.168.5.1 255.255.255.0	Se	asigna	el
<i>direccionamiento de la interfaz</i>			
R3(config-if)#exit			
R3(config)#interface lo6	Se	agrega	la
<i>descripción de la interfaz loopback</i>			
R3(config-if)#ip add 192.168.6.1 255.255.255.0	Se	asigna	el
<i>direccionamiento de la interfaz</i>			
R3(config-if)#exit			
R3(config)#interface lo7	Se	agrega	la
<i>descripción de la interfaz loopback</i>			

R3(config-if)#ipv6 add 2001:db8:acad:3::1/64 Se asigna el
direccionamiento de la interfaz

R3(config-if)#exit

R3(config)#ip route 0.0.0.0 0.0.0.0 se0/0/1 Se asigna una ruta
predeterminada para el direccionamiento IPv4 en la interfaz Se0/0/1

R3(config)#ipv6 route ::/0 se0/0/1 Se asigna una ruta
predeterminada para el direccionamiento IPv6 en la interfaz Se0/0/1

R3(config)#

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 16. Configuración del dispositivo S1.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
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	Service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente: Autor.

Configuración de S1

S1#configure terminal

S1(config)#no ip domain-lookup Se desactiva la
búsqueda de dominio

S1(config)#hostname S1 Se asigna el nombre
de host

S1(config)#enable secret class Se asigna la
contraseña de EXEC

S1(config)#line con 0

S1(config-line)#password cisco Se asigna la
contraseña de consola

S1(config-line)#login *Se habilita la verificación de contraseña de consola*
S1(config-line)#exit
S1(config)#line vty 0 4
S1(config-line)#password cisco *Se asigna la contraseña de terminal de acceso telnet*
S1(config-line)#login *Se habilita la verificación de contraseña de acceso telnet*
S1(config-line)#exit
S1(config)#service password-encryption *Se habilita el servicio de encriptación de contraseñas de texto plano*
S1(config)#banner motd #Se prohíbe el acceso no autorizado# *Se habilita un mensaje de alerta*

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 17. Configuración del dispositivo S1.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
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	Service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente: Autor.

Configuración de S3

S3#configure terminal
S3(config)#no ip domain-lookup *Se desactiva la búsqueda de dominio*
S3(config)#hostname S3 *Se asigna el nombre de host*

S3(config)#enable secret class contraseña de EXEC	Se	asigna	la
S3(config)#line con 0			
S3(config-line)#password cisco contraseña de consola	Se	asigna	la
S3(config-line)#login verificación de contraseña de consola	Se	habilita	la
S3(config-line)#exit			
S3(config)#line vty 0 4			
S3(config-line)#password cisco contraseña de terminal de acceso telnet	Se	asigna	la
S3(config-line)#login verificación de contraseña de acceso telnet	Se	habilita	la
S3(config-line)#exit			
S3(config)#service password-encryption de encriptación de contraseñas de texto plano		Se	habilita el servicio
S3(config)#banner motd #Se prohíbe el acceso no autorizado# mensaje de alerta		Se	habilita un
S3(config)#			

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 18. Verificación de la conectividad de la red.

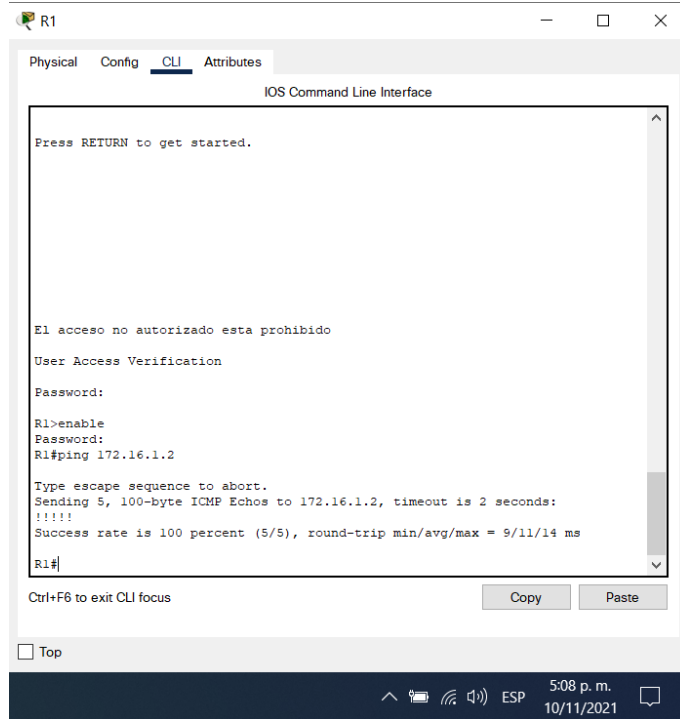
Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 8/12/16 ms

R2	R3, S0/0/1	172.16.2.1	<p>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 = 12/15/20 ms</p>
PC de Internet	Gateway predeterminado	209.165.200.233	<p>VPCS> ping 2001:DB8:ACAD:A::1</p> <p>2001:DB8:ACAD:A::1 icmp6_seq=1 ttl=64 time=23.481 ms</p> <p>2001:DB8:ACAD:A::1 icmp6_seq=2 ttl=64 time=10.394 ms</p> <p>2001:DB8:ACAD:A::1 icmp6_seq=3 ttl=64 time=1.070 ms</p> <p>2001:DB8:ACAD:A::1 icmp6_seq=4 ttl=64 time=4.563 ms</p> <p>2001:DB8:ACAD:A::1 icmp6_seq=5 ttl=64 time=5.842 ms</p>

Fuente: Autor.

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

Figura 8. Validación de ping desde R1 a R2.



```
R1
Physical Config CLI Attributes
IOS Command Line Interface

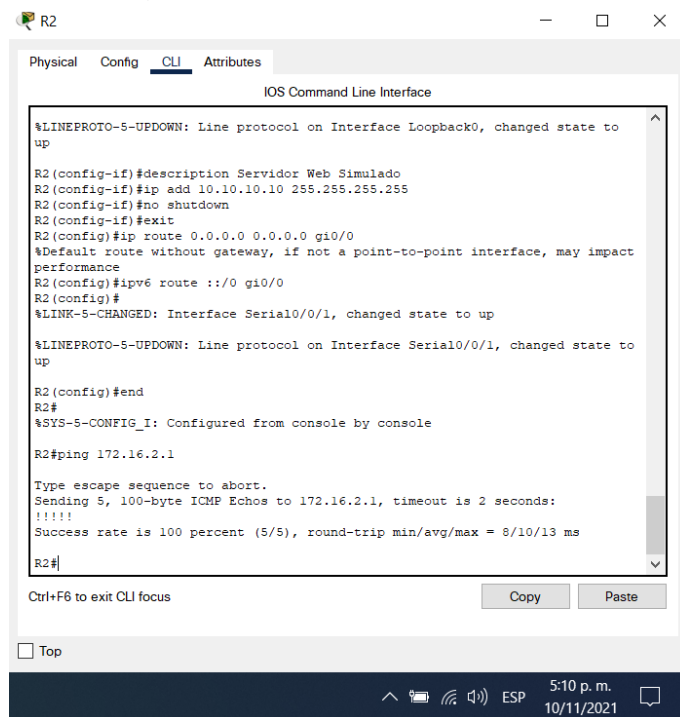
Press RETURN to get started.

El acceso no autorizado esta prohibido
User Access Verification
Password:
R1>enable
Password:
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 = 9/11/14 ms
R1#
```

Fuente: Autor

Figura 9. Validación de ping desde R2 a R3.



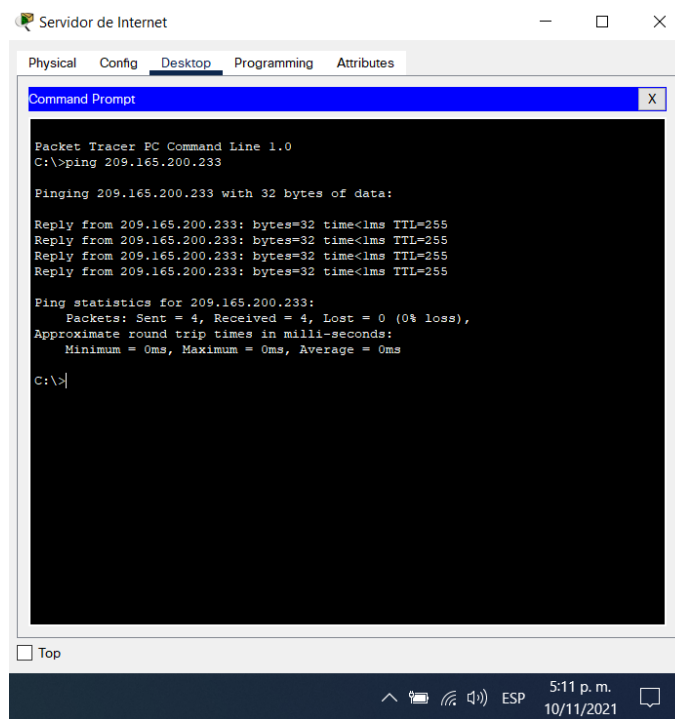
```
R2
Physical Config CLI Attributes
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to
up
R2(config-if)#description Servidor Web Simulado
R2(config-if)#ip add 10.10.10.10 255.255.255.255
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 gi0/0
%Default route without gateway, if not a point-to-point interface, may impact
performance
R2(config)#ipv6 route ::/0 gi0/0
R2(config)#
%LINK-5-CHANGED: Interface Serial10/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial10/0/1, changed state to
up
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
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 = 8/10/13 ms
R2#
```

Fuente: Autor

Figura 10. Validación de ping desde Servidor de Internet a su Gateway.



Fuente: Autor.

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 19. Configuración de seguridad, VLAN y routing entre VLAN en S1.

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: Autor.

Configuración en S1

S1(config)#vlan 21	<i>Se crea la VLAN21</i>
S1(config-vlan)#name Contabilidad de la VLAN	<i>Se asigna el nombre de la VLAN</i>
S1(config-vlan)#exit	
S1(config)#vlan 23	<i>Se crea la VLAN23</i>
S1(config-vlan)#name Ingenieria de la VLAN	<i>Se asigna el nombre de la VLAN</i>
S1(config-vlan)#exit	
S1(config)#vlan 99	<i>Se crea la VLAN99</i>
S1(config-vlan)#name Administracion de la VLAN	<i>Se asigna el nombre de la VLAN</i>
S1(config-vlan)#exit	
S1(config)#	
S1(config)#interface vlan 99 de la VLAN 99	<i>Se habilita la interfaz de la VLAN 99</i>
S1(config-if)#ip add 192.168.99.2 255.255.255.0	<i>Se asigna el direccionamiento de la interfaz</i>
S1(config-if)#no shutdown	<i>Se enciende la interfaz</i>
S1(config-if)#exit	
S1(config)#ip default-gateway 192.168.99.1	<i>Se configura la dirección de la puerta de acceso por defecto</i>
S1(config)#interface range fa0/5, fa0/3	<i>Se seleccionan las interfaces que son puertas troncales</i>
S1(config-if-range)#switchport mode trunk	<i>Se configuran en modo troncal</i>

S1(config-if-range)#switchport trunk native vlan 1 <i>como vlan nativa</i>	Se habilita la VLAN 1
S1(config-if-range)#exit	
S1(config)#interface fa0/6	
S1(config-if)#switchport mode access <i>interfaz con modo de acceso</i>	Se configura la
S1(config-if)#switchport access vlan 21 <i>para que circule en esta interfaz</i>	Se asigna la VLAN 21
S1(config-if)#exit	
S1(config)# interface range fa0/1-2,fa0/4,fa0/7-24,gi0/1-2 <i>interfaces que están inactivas</i>	Se seleccionan las
S1(config-if-range)#switchport mode Access <i>modo de acceso</i>	Se configuran en
S1(config-if-range)#shutdown <i>interfaces.</i>	Se desactivan las
S1(config-if-range)#exit	

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 20. Configuración de seguridad, VLAN y routing entre VLAN en S3.

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: Autor.

Configuración en S3

S3(config)#	
S3(config)#vlan 21	<i>Se crea la VLAN21</i>
S3(config-vlan)#name Contabilidad de la VLAN	<i>Se asigna el nombre</i>
S3(config-vlan)#exit	
S3(config)#vlan 23	<i>Se crea la VLAN23</i>
S3(config-vlan)#name Ingenieria de la VLAN	<i>Se asigna el nombre</i>
S3(config-vlan)#exit	
S3(config)#vlan 99	<i>Se crea la VLAN99</i>
S3(config-vlan)#name Administracion de la VLAN	<i>Se asigna el nombre</i>
S3(config-vlan)#exit	
S3(config)#interface vlan 99 de la VLAN 99	<i>Se habilita la interfaz</i>
S3(config-if)#ip add 192.168.99.3 255.255.255.0 direccionamiento de la interfaz	<i>Se asigna el</i>
S3(config-if)#no shutdown interfaz	<i>Se enciende la</i>
S3(config-if)#exit	
S3(config)#ip default-gateway 192.168.99.1 dirección de la puerta de acceso por defecto	<i>Se configura la</i>
S3(config)#interface fa0/3 interfaz que es puerta troncal	<i>Se selecciona la</i>
S3(config-if)#switchport mode trunk modo troncal	<i>Se configuran en</i>
S3(config-if)#switchport trunk native vlan 1 como vlan nativa	<i>Se habilita la VLAN 1</i>
S3(config-if)#exit	
S3(config)#interface fa0/18	
S3(config-if)#switchport mode access interfaz con modo de acceso	<i>Se configura la</i>
S3(config-if)#switchport access vlan 23 para que circule en esta interfaz	<i>Se asigna la VLAN 23</i>
S3(config-if)#exit	
S3(config)# interface range fa0/1-2,fa0/4-17,fa0/19-24,gi0/1-2 las interfaces que están inactivas	<i>Se seleccionan</i>

S3(config-if-range)#switchport mode access *Se configuran en modo de acceso*
 S3(config-if-range)#shutdown *Se desactivan las interfaces*
 S3(config-if-range)#

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 21. Configuración de subinterfaces en R1.

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	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz
Activar la interfaz G0/1	No shutdown

Fuente: Autor.

Configuración en R1.

R1#configure terminal
 R1(config)#interface gi0/1.21 *Se configura la subinterfaz*
 R1(config-subif)#encapsulation dot1q 21 *Se encapsula la subinterfaz y se le asigna la respectiva vlan*
 R1(config-subif)#description LAN de Contabilidad *Se agrega una descripción de la subinterfaz*
 R1(config-subif)#ip add 192.168.21.1 255.255.255.0 *Se asigna el direccionamiento de la subinterfaz*
 R1(config-subif)#exit
 R1(config)#

R1(config)#interface gi0/1.23 <i>subinterfaz</i>	Se configura la
R1(config-subif)#encapsulation dot1q 23 <i>subinterfaz y se le asigna la respectiva vlan</i>	Se encapsula la
R1(config-subif)#description LAN de Ingenieria <i>descripción de la subinterfaz</i>	Se agrega una
R1(config-subif)#ip add 192.168.23.1 255.255.255.0 <i>direccionamiento de la subinterfaz</i>	Se asigna el
R1(config-subif)#exit R1(config)#	
R1(config)#interface gi0/1.99 <i>subinterfaz</i>	Se configura la
R1(config-subif)#encapsulation dot1q 99 <i>subinterfaz y se le asigna la respectiva vlan</i>	Se encapsula la
R1(config-subif)#description LAN de Administracion <i>descripción de la subinterfaz</i>	Se agrega una
R1(config-subif)#ip add 192.168.99.1 255.255.255.0 <i>direccionamiento de la subinterfaz</i>	Se asigna el
R1(config-subif)#exit R1(config)#	
R1(config)#interface gi0/1 <i>interfaz</i>	Se ingresa a la
R1(config-if)#no shutdown <i>interfaz</i>	Se enciende la
R1(config-if)#exit R1(config)#	

Paso 4: Verificar la conectividad de la red

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

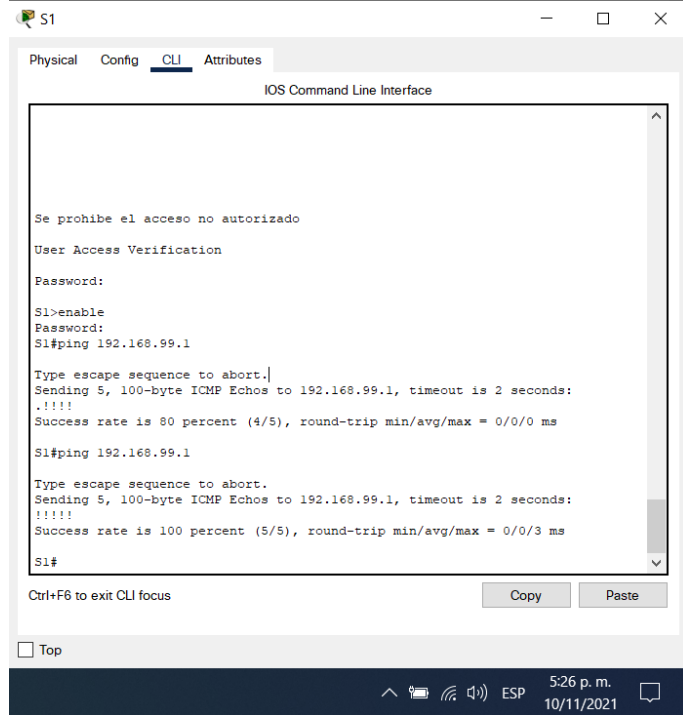
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 22. Lista de verificaciones de la conectividad de la red.

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/3 ms
S3	R1, dirección VLAN 99	192.168.99.1	S3#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S1	R1, dirección VLAN 21	192.168.21.1	S1#ping 192.168.21.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 23	192.168.23.1	S3#ping 192.168.23.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms

Fuente: Autor.

Figura 11. Validación de ping desde S1 a R1, dirección VLAN 99.

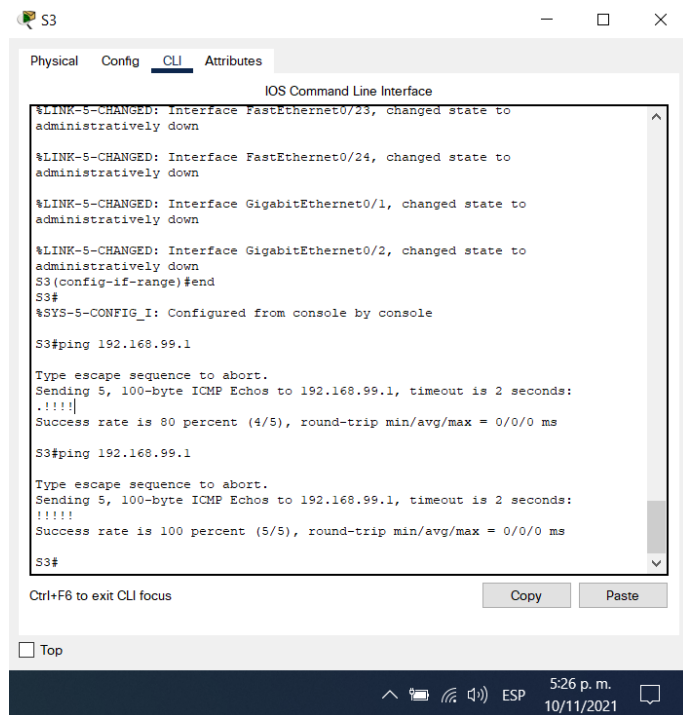


The screenshot shows the CLI of switch S1. The user has entered 'enable' and then 'ping 192.168.99.1'. The first ping attempt shows a success rate of 80 percent (4/5) with a round-trip time of 0/0/0 ms. The second ping attempt shows a success rate of 100 percent (5/5) with a round-trip time of 0/0/3 ms. The interface shows standard CLI prompts and escape sequence instructions.

```
S1#
S1>enable
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 = 0/0/0 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 = 0/0/3 ms
S1#
```

Fuente: Autor.

Figura 12. Validación de ping desde S3 a R1, dirección VLAN 99.

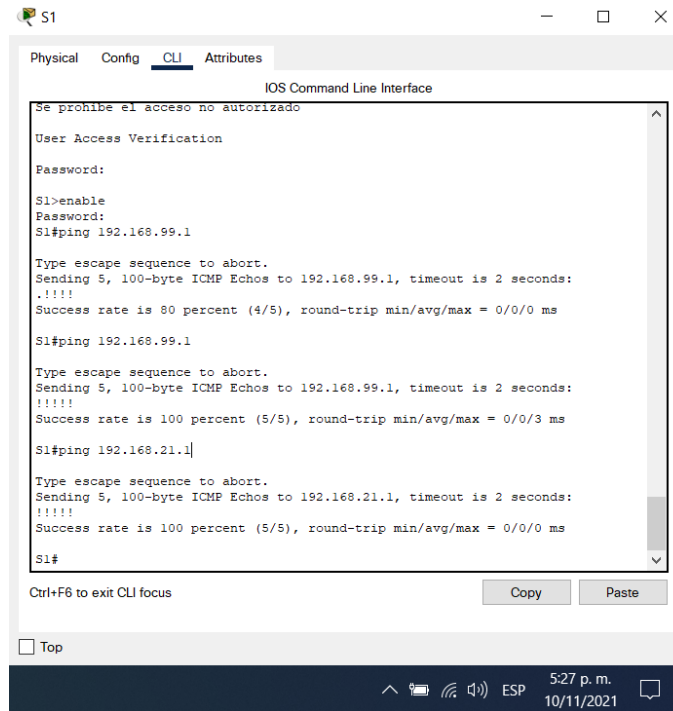


The screenshot shows the CLI of switch S3. The user has entered 'enable', then 'config-if-range', then 'end', and finally 'ping 192.168.99.1'. The first ping attempt shows a success rate of 80 percent (4/5) with a round-trip time of 0/0/0 ms. The second ping attempt shows a success rate of 100 percent (5/5) with a round-trip time of 0/0/0 ms. The interface shows standard CLI prompts and escape sequence instructions.

```
S3#
S3>enable
S3#config-if-range
S3(config-if-range)#end
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 = 0/0/0 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#
```

Fuente: Autor.

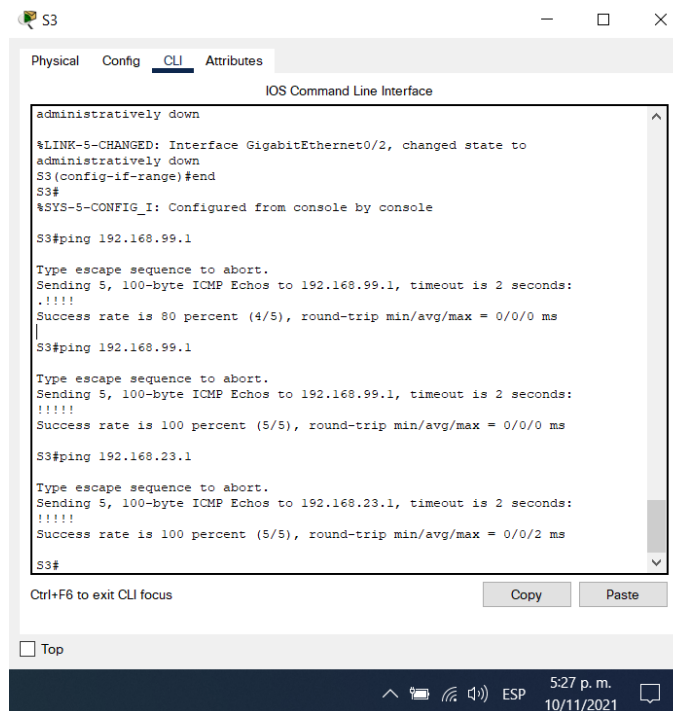
Figura 13. Validación de ping desde S1 a R1, dirección VLAN 21.



```
S1
Physical Config CLI Attributes
IOS Command Line Interface
Se prohíbe el acceso no autorizado
User Access Verification
Password:
S1>enable
Password:
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 = 0/0/0 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 = 0/0/3 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
S1#
```

Fuente: Autor.

Figura 14. Validación de ping desde S3 a R1, dirección VLAN 23.



```
S3
Physical Config CLI Attributes
IOS Command Line Interface
administratively down
%LINK-3-CHANGED: Interface GigabitEthernet0/2, changed state to
administratively down
S3(config-if-range)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console
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 = 0/0/0 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 = 0/0/2 ms
S3#
```

Fuente: Autor.

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 23. Tareas de configuración para R1.

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: Autor.

Configuración en R1.

R1(config)#router ospf 1 <i>protocolo OSPF</i>	Se <i>habilita el</i>
R1(config-router)#router-id 1.1.1.1 <i>identificador de router</i>	Se <i>asigna un</i>
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 <i>general de la red conectada directamente, su wildcard y el área a asignar</i>	Se <i>asigna la dirección</i>
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 <i>general de la red conectada directamente, su wildcard y el área a asignar</i>	Se <i>asigna la dirección</i>
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 <i>general de la red conectada directamente, su wildcard y el área a asignar</i>	Se <i>asigna la dirección</i>
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0 <i>general de la red conectada directamente, su wildcard y el área a asignar</i>	Se <i>asigna la dirección</i>
R1(config-router)#passive-interface gi0/1 <i>como pasiva</i>	Se <i>asigna la interfaz</i>
R1(config-router)#passive-interface gi0/1.21 <i>subinterfaz como pasiva</i>	Se <i>asigna la</i>
R1(config-router)#passive-interface gi0/1.23 <i>subinterfaz como pasiva</i>	Se <i>asigna la</i>
R1(config-router)#passive-interface gi0/1.99 <i>subinterfaz como pasiva</i>	Se <i>asigna la</i>

R1(config-router)#no auto-summary <i>sumarización automática</i>	Se desactiva la
R1(config-router)#exit	
R1(config)#interface gi0/1	
R1(config-if)#ip ospf 1 area 0	Se asigna a la interfaz
R1(config-if)#exit	
R1(config)#interface se0/0/0	
R1(config-if)#ip ospf 1 area 0	Se asigna a la interfaz
R1(config-if)#exit	

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 24. Tareas de configuración para R2.

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: Autor.

Configuración en R2.

R2(config)#router ospf 1 <i>protocolo OSPF</i>	Se habilita el
R2(config-router)#router-id 2.2.2.2 <i>identificador de router</i>	Se asigna un
R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 <i>general de la red conectada directamente, su wildcard y el área a asignar</i>	Se asigna la dirección
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 <i>general de la red conectada directamente, su wildcard y el área a asignar</i>	Se asigna la dirección
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 <i>general de la red conectada directamente, su wildcard y el área a asignar</i>	Se asigna la dirección
R2(config-router)#passive-interface lo0 <i>como pasiva</i>	Se asigna la interfaz
R2(config-router)#no auto-summary <i>sumarización automática</i>	Se desactiva la
R2(config-router)#exit	

```

R2(config)#interface se0/0/0
R2(config-if)#ip ospf 1 area 0
R2(config-if)#exit
R2(config)#interface se0/0/1
R2(config-if)#ip ospf 1 area 0
R2(config-if)#exit

```

Se asigna a la interfaz

Se asigna a la interfaz

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 25. Tareas de configuración para R2.

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: Autor.

Configuración en R3.

```

R3#configure terminal
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
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
R3(config-router)#passive-interface lo4

```

Se habilita el protocolo OSPF

Se asigna un identificador de router

Se asigna la dirección general de la red conectada directamente, su wildcard y el área a asignar

Se asigna la dirección general de la red conectada directamente, su wildcard y el área a asignar

Se asigna la dirección general de la red conectada directamente, su wildcard y el área a asignar

Se asigna la dirección general de la red conectada directamente, su wildcard y el área a asignar

Se asigna la interfaz como pasiva

R3(config-router)#passive-interface lo5 <i>como pasiva</i>	<i>Se asigna la interfaz</i>
R3(config-router)#passive-interface lo6 <i>como pasiva</i>	<i>Se asigna la interfaz</i>
R3(config-router)#passive-interface lo7 <i>como pasiva</i>	<i>Se asigna la interfaz</i>
R3(config-router)#exit	
R3(config)#ipv6 unicast-routing <i>direccionamiento unicast</i>	<i>Se habilita el</i>
R3(config)#ipv6 router ospf 1 <i>en el router</i>	<i>Se habilita OSPFv3</i>
R3(config-rtr)#router-id 3.3.3.3 <i>identificador de ospf</i>	<i>Se asigna un</i>
R3(config-rtr)#exit	
R3(config)#interface se0/0/1	
R3(config-if)#ipv6 ospf 1 area 0 <i>interfaz</i>	<i>Se configura la</i>
R3(config-if)#exit	
R3(config)#	

Paso 4: Verificar la información de OSPF

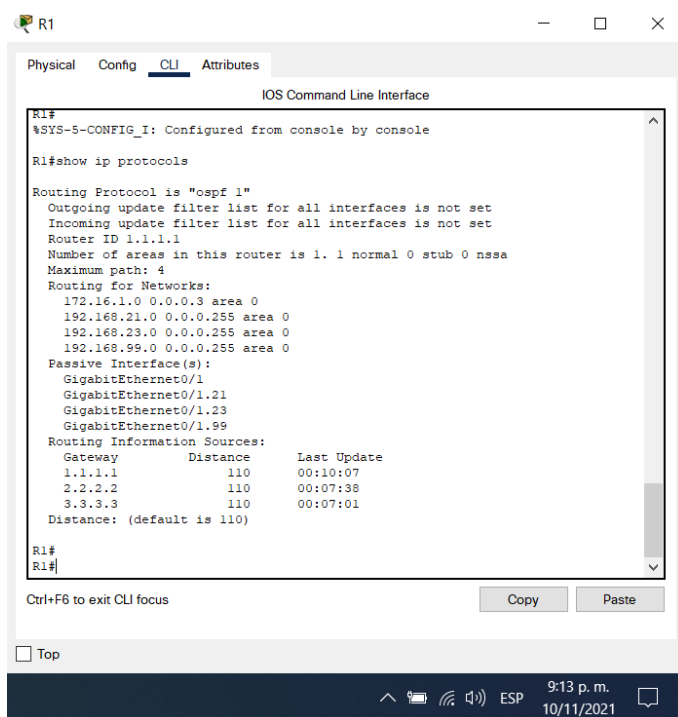
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 26. Verificación de 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 ip ospf interface

Fuente: Autor.

Figura 15. Verificación del ID del proceso OSPF, del router, las redes de routing y las interfaces pasivas en R1.



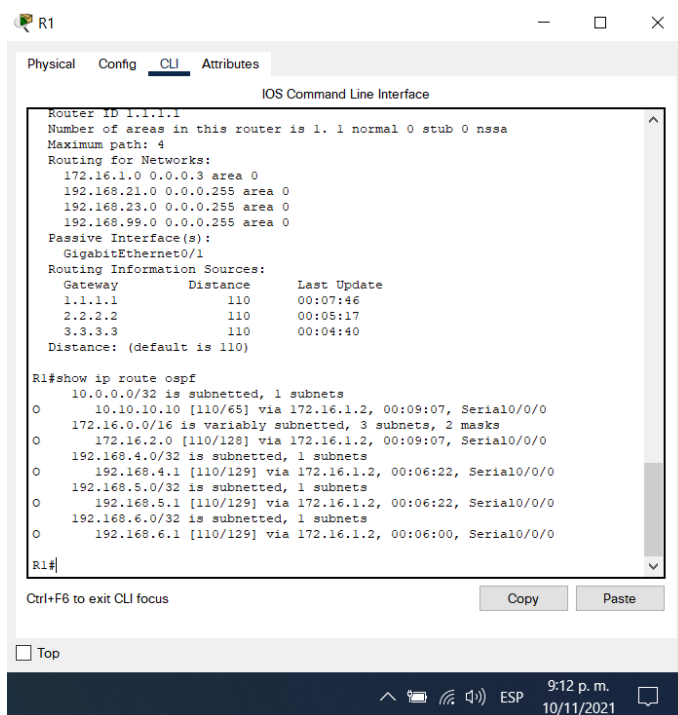
```
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.3 area 0
    192.168.21.0 0.0.0.255 area 0
    192.168.23.0 0.0.0.255 area 0
    192.168.99.0 0.0.0.255 area 0
  Passive Interface(s):
    GigabitEthernet0/1
    GigabitEthernet0/1.21
    GigabitEthernet0/1.23
    GigabitEthernet0/1.99
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:10:07
    2.2.2.2          110          00:07:38
    3.3.3.3          110          00:07:01
  Distance: (default is 110)

R1#
R1#
```

Fuente: Autor

Figura 16. Verificación de las rutas OSPF en R1.



```
R1#show ip route ospf

10.0.0.0/32 is subnetted, 1 subnets
O   10.10.10.10 [110/65] via 172.16.1.2, 00:09:07, Serial0/0/0
O   172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O   172.16.2.0 [110/128] via 172.16.1.2, 00:09:07, Serial0/0/0
O   192.168.4.0/32 is subnetted, 1 subnets
O   192.168.4.1 [110/129] via 172.16.1.2, 00:06:22, Serial0/0/0
O   192.168.5.0/32 is subnetted, 1 subnets
O   192.168.5.1 [110/129] via 172.16.1.2, 00:06:22, Serial0/0/0
O   192.168.6.0/32 is subnetted, 1 subnets
O   192.168.6.1 [110/129] via 172.16.1.2, 00:06:00, Serial0/0/0

R1#
```

Fuente: Autor.

Figura 17. Verificación de sección de OSPF de la configuración en ejecución en R1.

```
R1#show ip ospf interface
GigabitEthernet0/1.21 is up, line protocol is up
 Internet address is 192.168.21.1/24, Area 0
 Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State WAITING, Priority 1
 No designated router on this network
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
 Index 1/1, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 0, Adjacent neighbor count is 0
 Suppress hello for 0 neighbor(s)
GigabitEthernet0/1.23 is up, line protocol is up
 Internet address is 192.168.23.1/24, Area 0
 Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State WAITING, Priority 1
 No designated router on this network
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
 Index 2/2, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 0, Adjacent neighbor count is 0
--More--
```

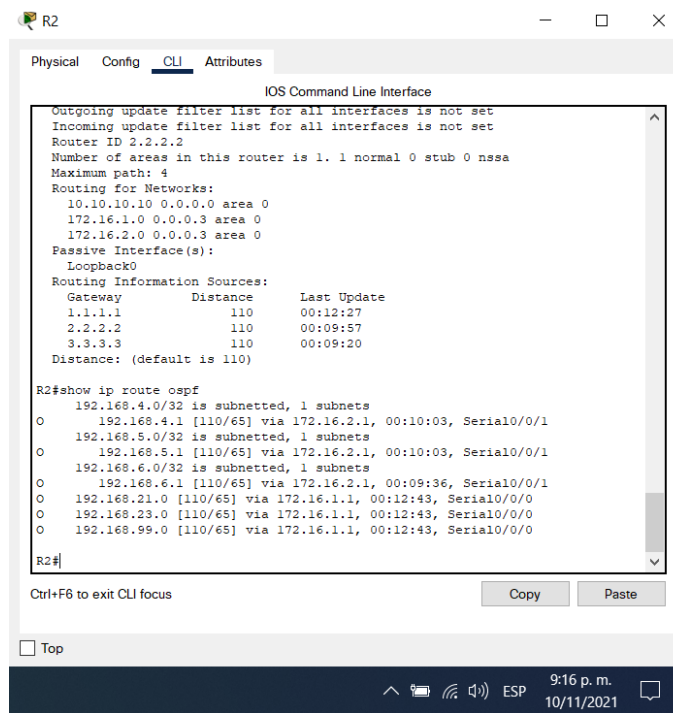
Fuente: Autor.

Figura 18. Verificación del ID del proceso OSPF, del router, las redes de routing y las interfaces pasivas en R2.

```
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:
 10.10.10.10 0.0.0.0 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 00:12:27
 2.2.2.2 110 00:09:57
 3.3.3.3 110 00:09:20
 Distance: (default is 110)
R2#
```

Fuente: Autor

Figura 19. Verificación de las rutas OSPF en R2.

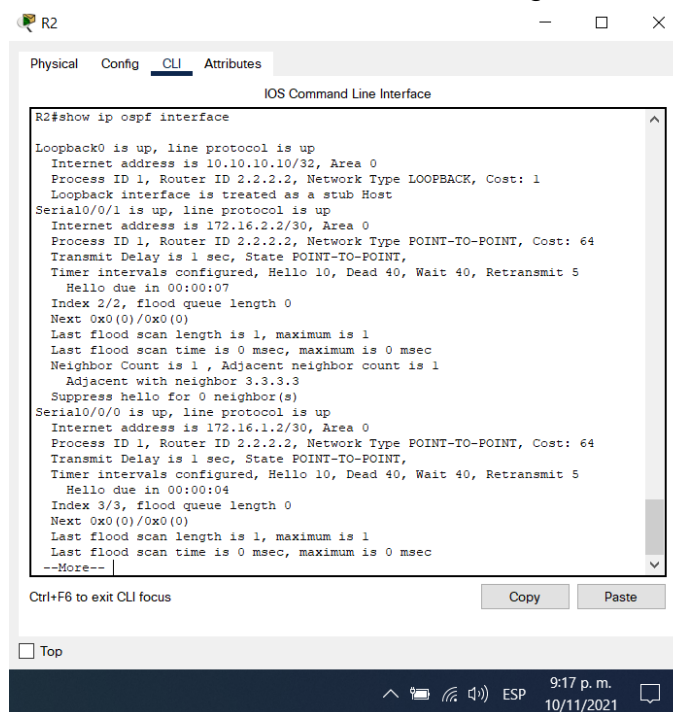


```
R2
Physical Config CLI Attributes
IOS Command Line Interface
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 2.2.2.2
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
 10.10.10.10 0.0.0.0 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          00:12:27
2.2.2.2          110          00:09:57
3.3.3.3          110          00:09:20
Distance: (default is 110)

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, 00:10:03, Serial0/0/1
O   192.168.5.0/32 is subnetted, 1 subnets
O   192.168.5.1 [110/65] via 172.16.2.1, 00:10:03, Serial0/0/1
O   192.168.6.0/32 is subnetted, 1 subnets
O   192.168.6.1 [110/65] via 172.16.2.1, 00:09:36, Serial0/0/1
O   192.168.21.0 [110/65] via 172.16.1.1, 00:12:43, Serial0/0/0
O   192.168.23.0 [110/65] via 172.16.1.1, 00:12:43, Serial0/0/0
O   192.168.99.0 [110/65] via 172.16.1.1, 00:12:43, Serial0/0/0
R2#
```

Fuente: Autor.

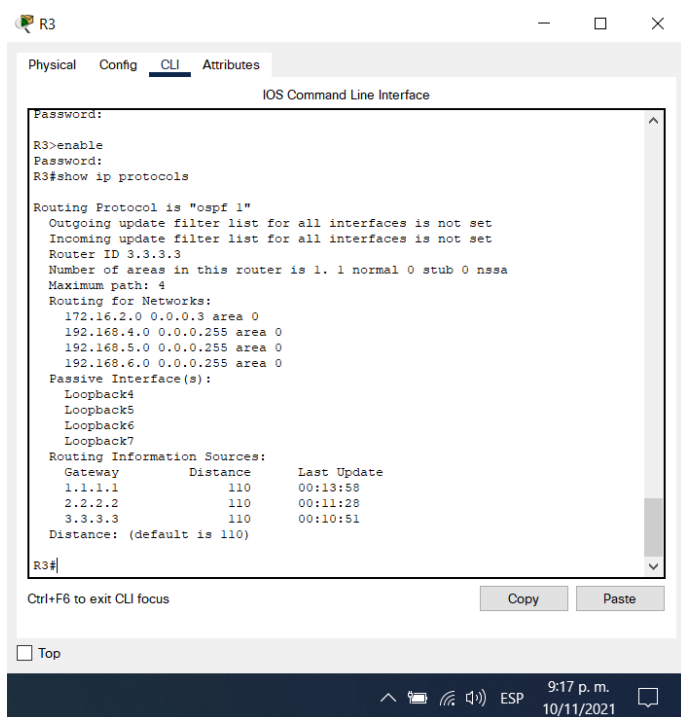
Figura 20. Verificación de sección de OSPF de la configuración en ejecución en R2.



```
R2
Physical Config CLI Attributes
IOS Command Line Interface
R2#show ip ospf interface
Loopback0 is up, line protocol is up
 Internet address is 10.10.10.10/32, Area 0
 Process ID 1, Router ID 2.2.2.2, Network Type LOOPBACK, Cost: 1
 Loopback interface is created as a stub Host
Serial0/0/1 is up, line protocol is up
 Internet address is 172.16.2.2/30, Area 0
 Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT, Cost: 64
 Transmit Delay is 1 sec, State POINT-TO-POINT,
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:07
 Index 2/2, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 1, Adjacent neighbor count is 1
   Adjacent with neighbor 3.3.3.3
 Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
 Internet address is 172.16.1.2/30, Area 0
 Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT, Cost: 64
 Transmit Delay is 1 sec, State POINT-TO-POINT,
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:04
 Index 3/3, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
--More--
```

Fuente: Autor.

Figura 21. Verificación del ID del proceso OSPF, del router, las redes de routing y las interfaces pasivas en R3.



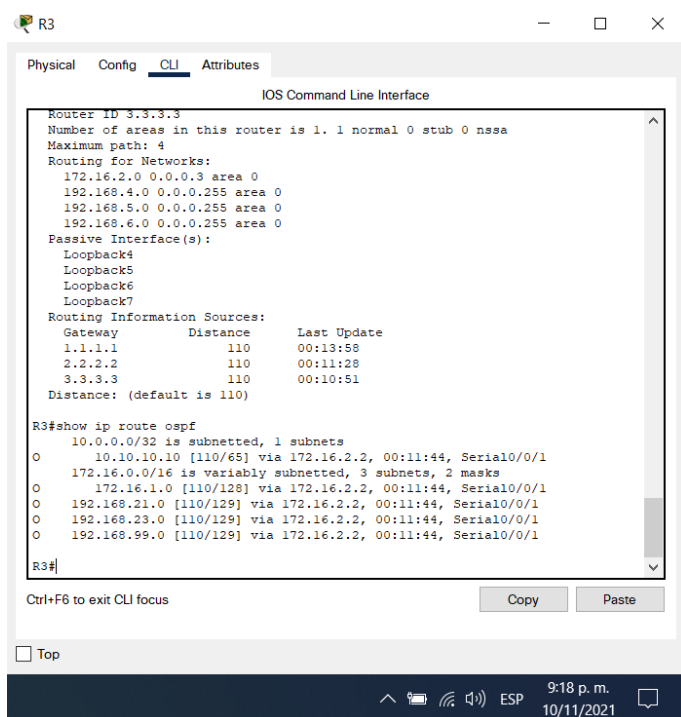
```
R3
Physical Config CLI Attributes
IOS Command Line Interface
Password:
R3>enable
Password:
R3#show ip protocols

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 3.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.2.0 0.0.0.3 area 0
    192.168.4.0 0.0.0.255 area 0
    192.168.5.0 0.0.0.255 area 0
    192.168.6.0 0.0.0.255 area 0
  Passive Interface(s):
    Loopback4
    Loopback5
    Loopback6
    Loopback7
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1           110          00:13:58
    2.2.2.2           110          00:11:28
    3.3.3.3           110          00:10:51
  Distance: (default is 110)

R3#
```

Fuente: Autor

Figura 22. Verificación de las rutas OSPF en R3.



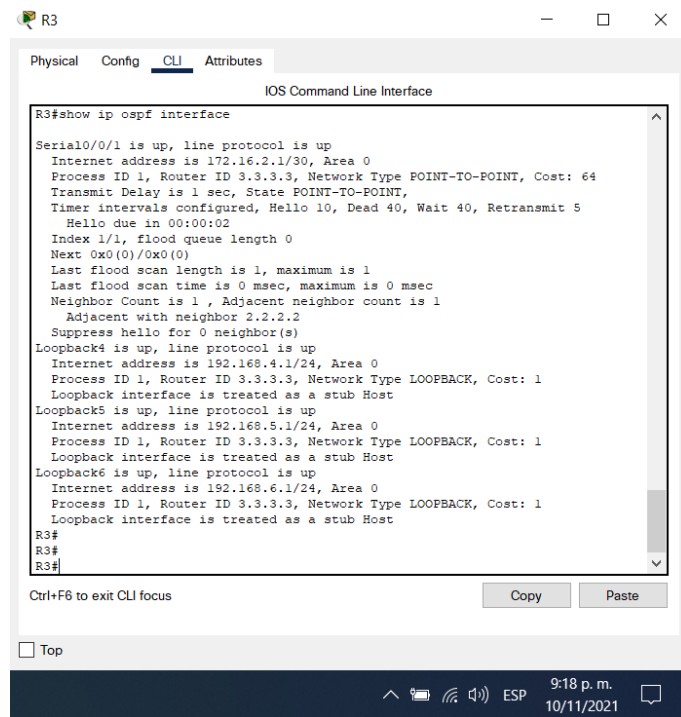
```
R3
Physical Config CLI Attributes
IOS Command Line Interface
Router ID 3.3.3.3
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
  172.16.2.0 0.0.0.3 area 0
  192.168.4.0 0.0.0.255 area 0
  192.168.5.0 0.0.0.255 area 0
  192.168.6.0 0.0.0.255 area 0
Passive Interface(s):
  Loopback4
  Loopback5
  Loopback6
  Loopback7
Routing Information Sources:
  Gateway         Distance      Last Update
  1.1.1.1           110          00:13:58
  2.2.2.2           110          00:11:28
  3.3.3.3           110          00:10:51
  Distance: (default is 110)

R3#show ip route ospf
  10.0.0.0/32 is subnetted, 1 subnets
  O   10.10.10.10 [110/65] via 172.16.2.2, 00:11:44, Serial0/0/1
  O   172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
  O   172.16.1.0 [110/129] via 172.16.2.2, 00:11:44, Serial0/0/1
  O   192.168.21.0 [110/129] via 172.16.2.2, 00:11:44, Serial0/0/1
  O   192.168.23.0 [110/129] via 172.16.2.2, 00:11:44, Serial0/0/1
  O   192.168.99.0 [110/129] via 172.16.2.2, 00:11:44, Serial0/0/1

R3#
```

Fuente: Autor.

Figura 23. Verificación de sección de OSPF de la configuración en ejecución en R3.



Fuente: Autor.

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 27. Lista de tareas de configuración DHCP en R1 para las VLANS 21 y 23.

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

<p>Crear un pool de DHCP para la VLAN 23</p>	<p>Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado</p>
--	---

Fuente: Autor.

Configuración en R1

```

R1#configure terminal
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20 Se excluyen
las primeras 20 direcciones de la VLAN 21
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20 Se excluyen
las primeras 20 direcciones de la VLAN 23
R1(config)#ip dhcp pool ACCT Se crea un pool de
DHCP para la VLAN 21
R1(dhcp-config)#network 192.168.21.0 255.255.255.0 Se asigna la dirección
de red
R1(dhcp-config)#default-router 192.168.21.1 Se asigna la dirección
de puerta de enlace
R1(dhcp-config)#dns-server 10.10.10.10 Se asigna el servidor
dns
R1(dhcp-config)#domain-name ccna-sa.com Se asigna el nombre
de dominio
R1(dhcp-config)#exit
R1(config)#ip dhcp pool ENGNR Se crea un pool de
DHCP para la VLAN 21
R1(dhcp-config)#network 192.168.23.0 255.255.255.0 Se asigna la dirección
de red
R1(dhcp-config)#default-router 192.168.23.1 Se asigna la dirección
de puerta de enlace
R1(dhcp-config)#dns-server 10.10.10.10 Se asigna el servidor
dns
R1(dhcp-config)#domain-name ccna-sa.com Se asigna el nombre
de dominio
R1(dhcp-config)#exit
R1(config)#

```

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

La configuración del R2 incluye las siguientes tareas:

Tabla 28. Lista de tareas de configuración NAT estática y dinámica en R2.

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta 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: 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	
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
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.233 – 209.165.200.236
Definir la traducción de NAT dinámica	

Fuente: Autor.

Configuración en R2

```
R2#configure terminal
```

```
R2(config)#username webuser privilege 15 password cisco12345 Se crea una cuenta de usuario con privilegios
```

```
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237 Se crea la NAT que asigna la dirección de origen estático del servidor web
```

```
R2(config)#interface gi0/0
```

```
R2(config-if)#ip nat inside Se configura que la dirección NAT es dentro
```

```
R2(config-if)#exit
```

```
R2(config)#interface s0/0/0
```

R2(config-if)#ip nat outside <i>dirección NAT es afuera</i>	<i>Se configura que la</i>
R2(config-if)#exit	
R2(config)#interface s0/0/1	
R2(config-if)#ip nat inside <i>dirección NAT es dentro</i>	<i>Se configura que la</i>
R2(config-if)#exit	
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 <i>acceso que permita la VLAN 21</i>	<i>Se crea una lista de</i>
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 <i>acceso que permita la VLAN 23</i>	<i>Se crea una lista de</i>
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255 <i>acceso que permita la dirección resumida de las loopback de R3</i>	<i>Se crea una lista de</i>
R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.24 <i>NAT de direcciones públicas que son utilizables</i>	<i>Se configura el pool</i>
R2(config)#ip nat inside source list 1 pool INTERNET <i>traducción de NAT dinámicamente</i>	<i>Se define la</i>
R2(config)#	

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.

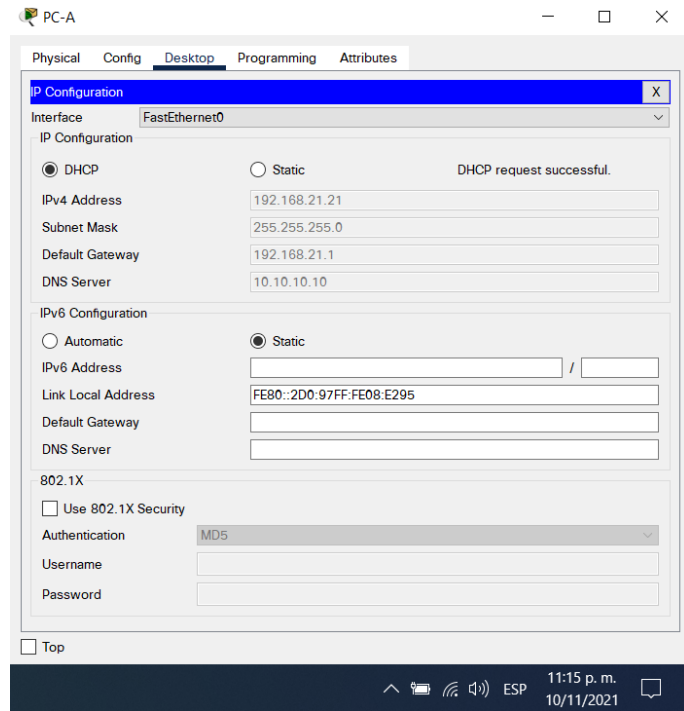
Tabla 29. Lista de tareas de verificación del protocolo DHCP y la NAT estática.

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

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

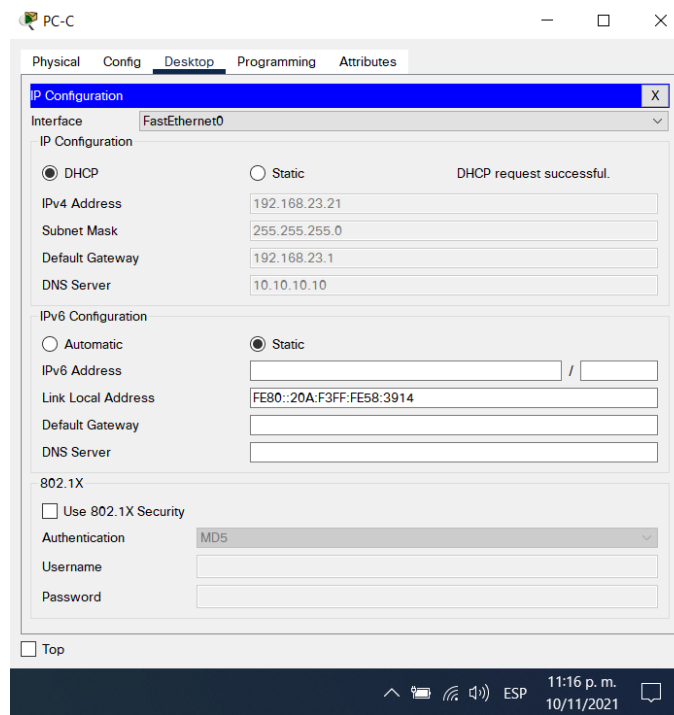
Fuente: Autor.

Figura 24. Verificación del direccionamiento DHCP en PC-A.



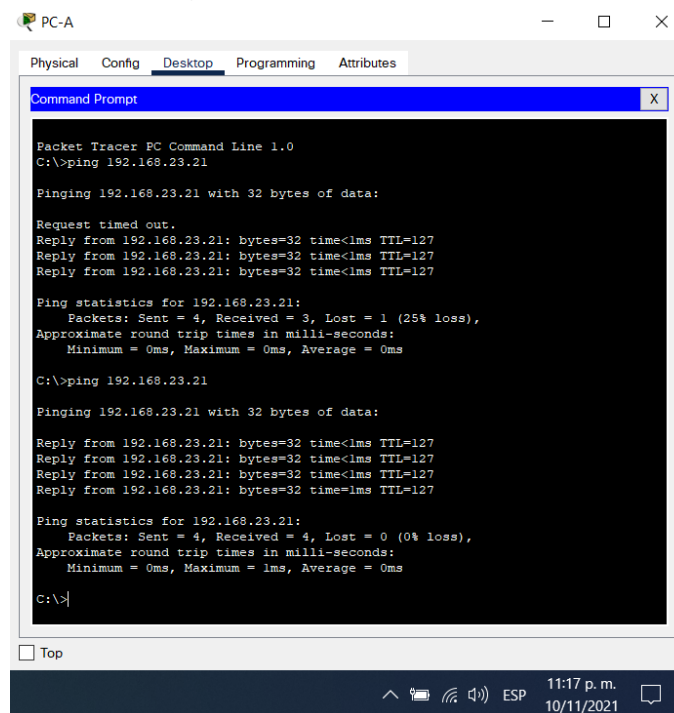
Fuente: Autor.

Figura 25. Verificación del direccionamiento DHCP en PC-C.



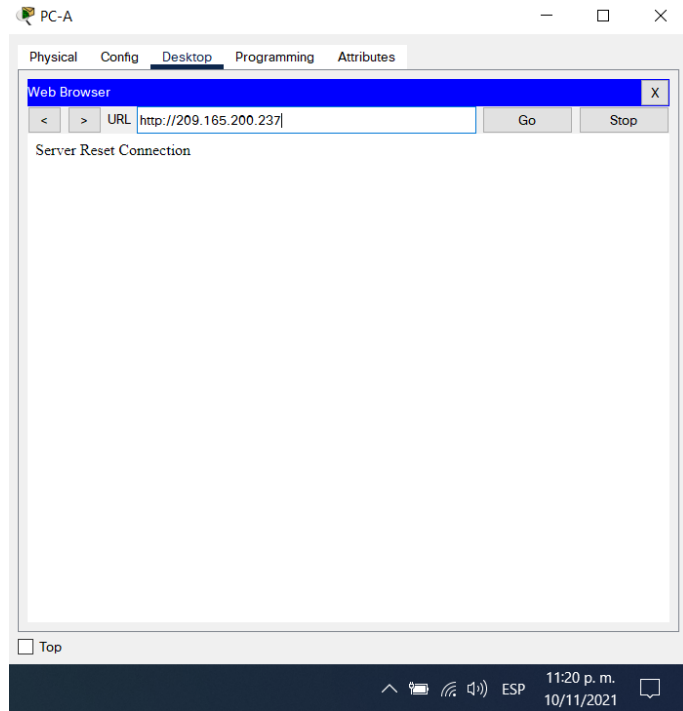
Fuente: Autor.

Figura 26. Verificación del ping entre PC-A y PC-C.



Fuente: Autor.

Figura 27. Verificación de la conexión al servidor web.



Fuente: Autor.

Parte 6: Configurar NTP

Tabla 30. Lista de tareas de configuración NTP.

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 hora NTP.	Ntp update-calendar
Verifique la configuración de NTP en R1.	Show ntp associations

Configuración en R2

R2#clock set 11:22:00 10 November 2021
en el router

Se configura la hora

R2(config)#ntp master 5
como maestro NTP

Se configura el router

Configuración en R1

R1#configure terminal

R1(config)#ntp server 172.16.1.2

Se configura el router como cliente NTP y se especifica la dirección serial que comunica el maestro NTP

R1(config)#ntp update-calendar

Se configura el router cliente NTP para que actualice el calendario periódicamente

Figura 28. Verificación de la configuración NTP en R1.

```

R1
Physical Config CLI Attributes
IOS Command Line Interface
User Access Verification
Password:
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 update-calendar
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ntp as
R1#show ntp associations

address      ref clock      st  when  poll  reach  delay
offset      disp
~172.16.1.2  127.127.1.1    5   11    16    17    11.00
905591056565.00  0.12
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R1#show clock
*2:20:7.551 UTC Mon Mar 1 1993
R1#show clock
*2:20:22.836 UTC Mon Mar 1 1993
R1#
R1#show clock
11:25:15.630 UTC Wed Nov 10 2021
R1#
Ctrl+F6 to exit CLI focus
Copy Paste
Top
    
```

Fuente: Autor.

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 31. Lista de tareas de configuración y verificación de listas de control de acceso en R2.

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca 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: Autor.

Configuración en R2.

R2#configure terminal

R2(config)#ip access-list standard ADMIN-MGT
acceso estándar nombrada

Se crea una lista de

R2(config-std-nacl)#permit host 172.16.1.1
permita la dirección ip del router R1

Se especifica que solo

R2(config-std-nacl)#exit

R2(config)#line vty 0 4

R2(config-line)#access-class ADMIN-MGT in
de acceso en la línea de telnet

Se configura la lista

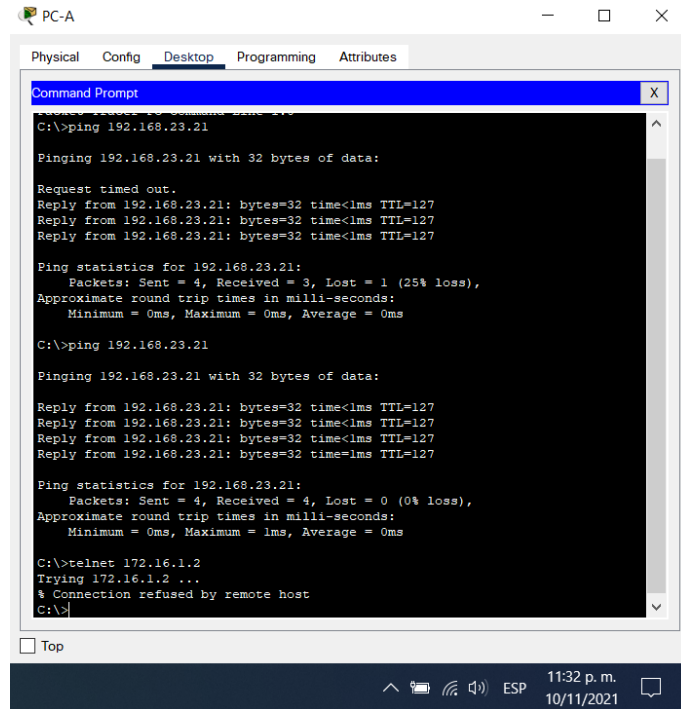
R2(config-line)#transport input telnet
transporte de entrada sea telnet

Se habilita que el

R2(config-line)#exit

R2(config)#

Figura 29. Verificación del funcionamiento de la ACL en PC-A.



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.23.21

Pinging 192.168.23.21 with 32 bytes of data:

Request timed out.
Reply from 192.168.23.21: bytes=32 time<1ms TTL=127
Reply from 192.168.23.21: bytes=32 time<1ms TTL=127
Reply from 192.168.23.21: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.23.21:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.23.21

Pinging 192.168.23.21 with 32 bytes of data:

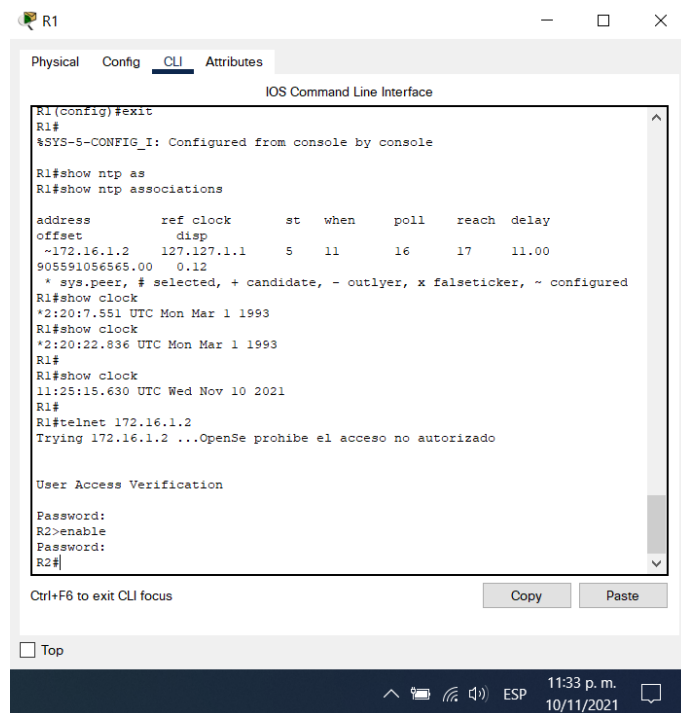
Reply from 192.168.23.21: bytes=32 time<1ms TTL=127
Reply from 192.168.23.21: bytes=32 time<1ms TTL=127
Reply from 192.168.23.21: bytes=32 time<1ms TTL=127
Reply from 192.168.23.21: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.23.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>telnet 172.16.1.2
Trying 172.16.1.2 ...
% Connection refused by remote host
C:\>
```

Fuente: Autor.

Figura 30. Verificación del funcionamiento de la ACL en R1.



```
R1
Physical Config CLI Attributes
IOS Command Line Interface
R1(Config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ntp as
R1#show ntp associations

address      ref clock      st  when  poll  reach  delay
offset      disp
~172.16.1.2  127.127.1.1    5   11    16    17     11.00
905591056565.00  0.12
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

R1#show clock
*2:20:7.551 UTC Mon Mar 1 1993
R1#show clock
*2:20:22.836 UTC Mon Mar 1 1993
R1#
R1#show clock
11:25:15.630 UTC Wed Nov 10 2021
R1#
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenSe prohíbe el acceso no autorizado

User Access Verification

Password:
R2>enable
Password:
R2#
```

Fuente: Autor.

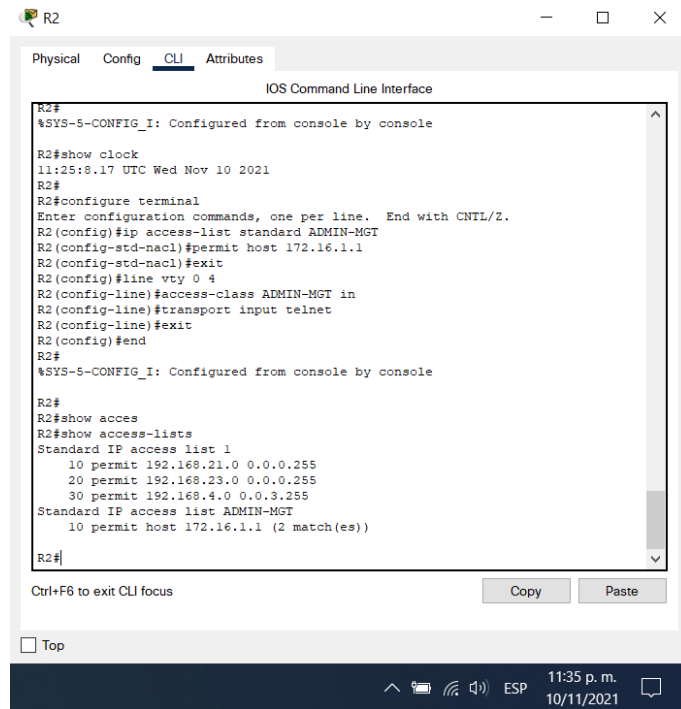
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 32. Lista de tareas de verificación de comando CLI.

Descripción del comando	Entrada del estudiante (comando)
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 ip 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.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Clear ip nat translation *

Fuente: Autor.

Figura 31. Mostrar las coincidencias recibidas luego de ser establecida en R2.



```
R2#
%SYS-5-CONFIG_I: Configured from console by console

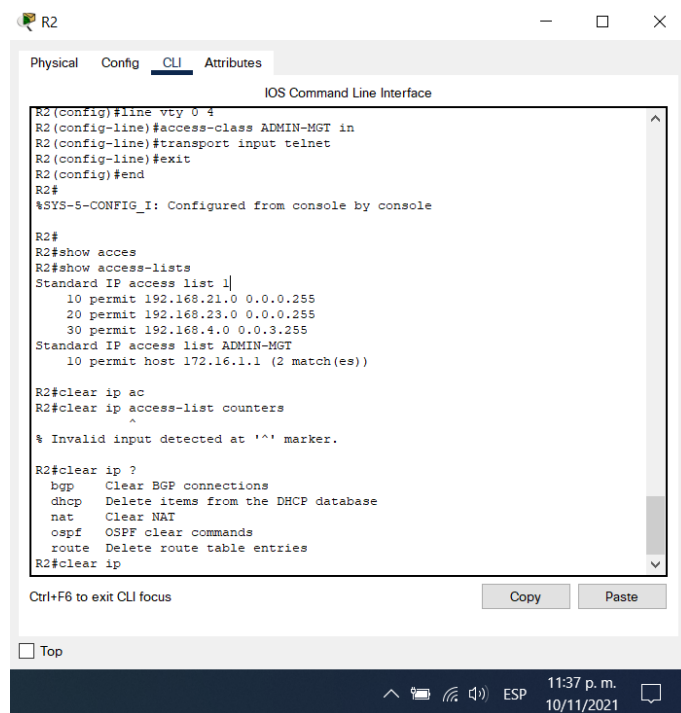
R2#show clock
11:29:08.17 UTC Wed Nov 10 2021
R2#
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#exit
R2(config)#line vty 0 4
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#transport input telnet
R2(config-line)#exit
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#
R2#show acces
R2#show access-lists
Standard IP access list 1
 10 permit 192.168.21.0 0.0.0.255
 20 permit 192.168.23.0 0.0.0.255
 30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
 10 permit host 172.16.1.1 (2 match(es))

R2#
```

Fuente: Autor.

Figura 32. Restablecer los contadores de una lista de acceso.



```
R2(config)#line vty 0 4
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#transport input telnet
R2(config-line)#exit
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

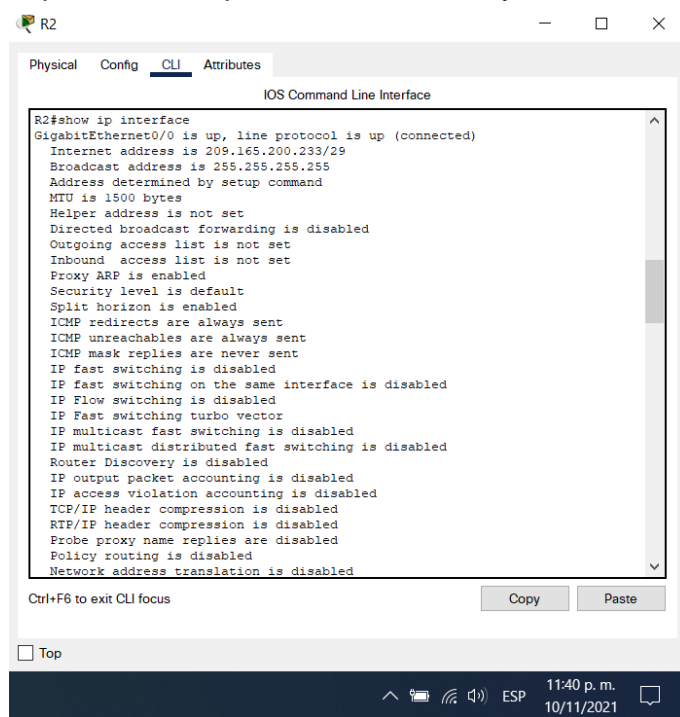
R2#
R2#show acces
R2#show access-lists
Standard IP access list 1
 10 permit 192.168.21.0 0.0.0.255
 20 permit 192.168.23.0 0.0.0.255
 30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
 10 permit host 172.16.1.1 (2 match(es))

R2#clear ip ac
R2#clear ip access-list counters
^
% Invalid input detected at '^' marker.

R2#clear ip ?
  bgp      Clear BGP connections
  dhcp     Delete items from the DHCP database
  nat      Clear NAT
  ospf     OSPF clear commands
  route    Delete route table entries
R2#clear ip
```

Fuente: Autor.

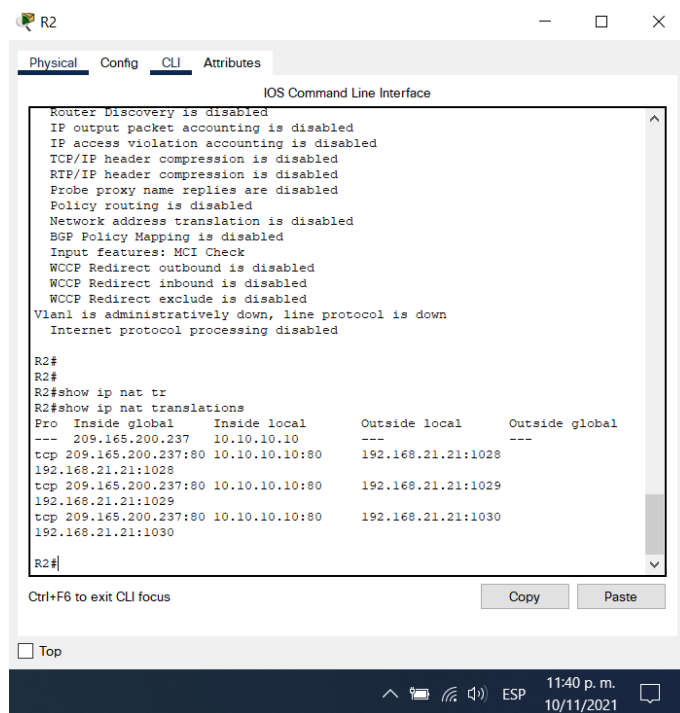
Figura 33. Mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica.



```
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 unreachable 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
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
```

Fuente: Autor.

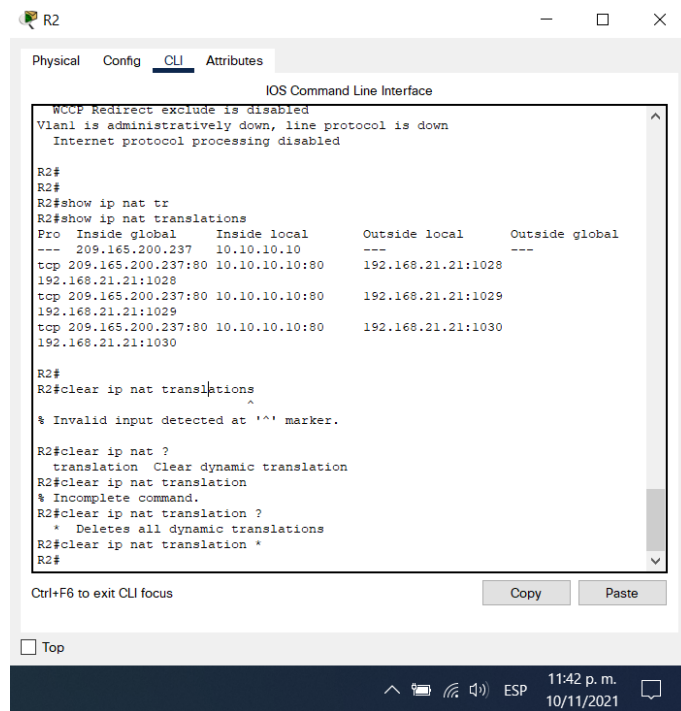
Figura 34. Mostrar las traducciones NAT.



```
R2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 209.165.200.237    10.10.10.10      ---                ---
tcp 209.165.200.237:80 10.10.10.10:80   192.168.21.21:1028
192.168.21.21:1028
tcp 209.165.200.237:80 10.10.10.10:80   192.168.21.21:1029
192.168.21.21:1029
tcp 209.165.200.237:80 10.10.10.10:80   192.168.21.21:1030
192.168.21.21:1030
```

Fuente: Autor.

Figura 35. Comando utilizado para eliminar las traducciones de NAT dinámicas.



```
R2
R2#
R2#show ip nat tr
R2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 209.165.200.237    10.10.10.10      ---              ---
tcp 209.165.200.237:80 10.10.10.10:80   192.168.21.21:1028
192.168.21.21:1028
tcp 209.165.200.237:80 10.10.10.10:80   192.168.21.21:1029
192.168.21.21:1029
tcp 209.165.200.237:80 10.10.10.10:80   192.168.21.21:1030
192.168.21.21:1030

R2#
R2#clear ip nat translations
^
% Invalid input detected at '^' marker.

R2#clear ip nat ?
translation Clear dynamic translation
R2#clear ip nat translation
% Incomplete command.
R2#clear ip nat translation ?
* Deletes all dynamic translations
R2#clear ip nat translation *
R2#
```

Fuente: Autor.

CONCLUSIONES

Desde la construcción de la simulación de red, el desarrollo de esquemas de direccionamiento IP que detallan la estructura del dispositivo, si son direcciones IPv4 e IPv6, y cómo obtener sus diferencias. de las subredes de direcciones comunes, comprenden internamente las operaciones para obtener sus respectivas máscaras de red.

Además, también se aplican conceptos relacionados con las aplicaciones de seguridad, partiendo de la aplicación de SSH en lugar de la aplicación de TELNET; la aplicación del servicio de cifrado de claves en texto plano, la distribución de claves a la línea de consola y línea de terminal, la distribución de banners. que notifican al administrador, y la Advertencia relacionada de uso indebido o acceso no autorizado al dispositivo, configuración de direcciones en cada interfaz, incluidas las físicas y lógicas

Finalmente, son complejos los escenarios a los que se pueden estar expuestos, pero con practica y aplicando los conceptos adquiridos se puede llevar a cabo la solución de cada uno de ellos y así poder desempeñar una gran labor en la sociedad.

BIBLIOGRAFÍA

CISCO. (2019). Acceso a la red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4>

CISCO. (2019). Capa de aplicación. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10>

CISCO. (2019). Capa de red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6>

CISCO. (2019). Capa de transporte. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9>

CISCO. (2019). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#1>

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2>

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11>

CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5>

CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10>

CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8>

CISCO. (2019). Direccionamiento IP. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7>

CISCO. (2019). División de redes IP en subredes. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8>

CISCO. (2019). Ethernet. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5>

CISCO. (2019). Exploración de la red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1>

CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7>

CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9>

CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3>

CISCO. (2019). Redes Conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4>

CISCO. (2019). Routing Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#3>

CISCO. (2019). Routing Estático. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2>

CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6>

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de <https://1drv.ms/u/s!AmlJYei-NT1lhqL9QChD1m9EuGqC>

UNAD (2017). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

Vesga, J. (2017). Ping y Tracer como estrategia en los procesos de Networking [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3>