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

DARLY YISELL QUINTERO OSSA

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

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

DARLY YISELL QUINTERO OSSA

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

TUTOR:
Msc. RAUL BAREÑO GUTIERREZ

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

NOTA DE ACEPTACION

_____
_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

La ¨Plata Huila, 29 de noviembre de 2021

AGRADECIMIENTOS

En primer lugar quiero agradecer a DIOS, quien me da las fuerzas, fortaleza y vitalidad para cumplir con mis objetivos en la vida, es mi apoyo incondicional en cada una de las tareas que me propongo a realizar.

En segundo lugar quiero agradecer a mi hermosa familia quienes me han brindado el apoyo incondicional en cada etapa de mi vida, son el motor de mi existencia, con sus palabras de ánimo, de no desistir y salir adelante me llevan a lograr cumplir con el objetivo que es ser una excelente Ingeniera de Sistemas.

También quiero agradecer a mi tutor Raúl Bareño Gutiérrez, quien con sus acertados aportes y conocimientos me guio y apoyo en el proceso de aprendizaje autónomo de cada una de las actividades presentes en el proyecto, y así lograr alcanzar los objetivos planteados en el logro de mi carrera.

Por ultimo quiero agradecer a cada uno de los compañeros de grupo quienes en ciertas ocasiones logramos culminar cada una de las actividades planteadas en cada guía, nos apoyamos y brindamos lo mejor de cada uno para dar cumplimiento a las responsabilidades adquiridas durante el grupo de trabajo en equipo.

Muchas gracias a todos.

CONTENIDO

AGRADECIMIENTOS 14
CONTENIDO 15
LISTAS DE TABLAS 16
LISTAS DE FIGURAS 17
GLOSARIO 19
RESUMEN 20
ABSTRACT 20
INTRODUCCION 21
DESARROLLO 22
1. ESCENARIO 1 22
DESARROLLO 32
1. ESCENARIO 2 32
CONCLUSIONES 74
BIBLIOGRAFIA 75

LISTAS DE TABLAS

Tabla 1. Esquema de direccionamiento IP....23
Tabla 2: Configuración del R1....23
Tabla 3. Configuración de S1....26
Tabla 4. Configuración del PC-A....28
Tabla 5. Configuración del PC-B....30
Tabla 6. Inicializar y volver a cargar los routers y switches....33
Tabla 7. Configuración del Servidor de Internet....36
Tabla 8. Configuración del R1....37
Tabla 9. Configuración del R2....38
Tabla 10. Configuración del R3....41
Tabla 11. Configuración del S1....43
Tabla 12. Configuración del S2....44
Tabla 13. Configuración del S3....45
Tabla 14. Verificación de conectividad en la red....46
Tabla 15. Configuración Seguridad S1, VLAN y Routing....48
Tabla 16. Configuración del S3....51
Tabla 17. Configuración del R1....54
Tabla 18. Verificación conectividad entre los switches y el R1....56
Tabla 19. Configuración OSPF en el R1....59
Tabla 20. Configuración OSPF en el R2....60
Tabla 21. Configuración OSPFv3 en el R2....61
Tabla 22. Configuración OSPFv3 en el R3....63
Tabla 22. Verificación de la información de OSPF....65
Tabla 23. Configuración del R1 como servidor DHCP, VLAN 21 y 23....65
Tabla 24. Configuración de la NAT estática y dinámica en el R2....67
Tabla 25. Verificación del protocolo DHCP y NAT estática....69
Tabla 26. Configuración NTP en el R2....70
Tabla 27. Configuración de ACL y restricción VTY en el R2....71
Tabla 28. Ejecución de comandos en el CLI del R2....72

LISTAS DE FIGURAS

Figura 1. Escenario 1 22
Figura 2. Simulación de escenario 1 22
Figura 3. Ejecución del comando show ip interface brief. 25
Figura 4. Comando Show running-config del R1 26
Figura 5 Ejecución del comando Show ip interface brief del S1 28
Figura 6 comando show running-config del S1 28
Figura 7. Ejecución Comando ipconfig / all en el PC-A 29
Figura 8 Conexión SSH desde el PC-A al R1 y S1 29
Figura 9 Ping al PC-B desde el PC-A 29
Figura 10 Ejecución del comando Ipconfig /all en el PC-B 30
Figura 11 Conexión SSH desde el PC-B al R1 y S1 30
Figura 12 Ping al PC-A desde el PC-B 31
Figura 13. Escenario 2 32
Figura 14. Simulación de escenario 2 32
Figura 15. Ejecución del comando show vlan y show flash al S1 34
Figura 16. Ejecución del comando show vlan y show flash al S2 35
Figura 17. Ejecución del comando show vlan y show flash al S3 35
Figura 18. Ping desde el R1 al R2 a la interfaz S0/2/0 47
Figura 19. Ping desde el R2 al R3 a la interfaz S0/2/1 48
Figura 20. Ping desde el PC de internet al Gateway predeterminado 48
Figura 21. Resultados del S1 con el comando show vlan 51
Figura 22 Resultados del S3 con el comando show vlan 54
Figura 23. Activación y configuración de las subinterfaces en el R1 56
Figura 24. Ping desde S1 a R1 de la VLAN 99 57
Figura 25. Ping desde S3 a R1 de la VLAN 99 58
Figura 26.. Ping desde S1 al R1 de la VLAN 23 58
Figura 27. Ping desde S3 a R1 de la VLAN 23 58
Figura 28. Comando show running-config verificando las OSPF en el R1 60
Figura 29. Comando show running-config verificando la Loopback 0 en el R2 61
Figura 30. Comando show running-config verificando la configuración OSPF en el R2 61
Figura 31. Resultado de la configuración del protocolo OSPF en la interfaz G0/0/0 del R2 62
Figura 32. Resultado de la configuración del protocolo OSPF en la interfaz S0/2/0 y S0/2/1 del R2 63
Figura 33. Resultado de la configuración del protocolo OSPF 62 63
Figura 34. Resultado de la configuración del protocolo OSPF en la interfaz S0/2/1 del R3 64
Figura 35. Resultado de la configuración del protocolo OSPF en la interfaz Loopback 4, 5, 6 del R3 64

Figura 36. Resultado de la configuración del protocolo OSPF en la interfaz Loopback 4, 5, 6 y 7 del R3 65
Figura 37. Resultados dhcp pool comando show running-config 67
Figura 38. Resultados de la configuración del R2 access-list 1 comando show running-config 69
Figura 39. Resultado del reloj cliente servidor R1 71
Figura 40. Resultado ntp server en R1 71
Figura 41. Resultados de la configuración del R2 72
Figura 42. Resultados ingresando telnet 172.16.1.2 desde el R1 al R2 72

GLOSARIO

ACL: Tiene como objetivo controlar el flujo de tráfico entre los equipos que posee una red, como lo son los enrutadores y conmutadores respectivamente.

DHCP: Dynamic Host Configuration Protocol, funciona en el modelo cliente/servidor y proporciona automáticamente direcciones IP y otra información relacionada como la máscara y el Gateway.

IPv4: Es aquella dirección que tiene una longitud de dirección de 32 bits en donde se requiere de un enrutador para la comunicación entre los dispositivos.

IPv6: Es aquella que posee una longitud de 128 bits, usando un tipo de fragmentación de extremo a extremo para llevar a cabo la comunicación entre los datagramas grandes en una red.

ISP: Se conoce como Internet Service Provider, el cual se identifica a aquellas compañías que proveen o prestan un servicio de acceso a internet.

NAT DINAMICA: Es un tipo de NAT en donde se mapea una dirección IP privada a una dirección IP pública mediante el enrutamiento de la tabla de direcciones de IP debidamente registradas de carácter público.

NAT ESTATICA: comúnmente reconocida como NAT 1:1, es un tipo de NAT la cual una dirección IP privada se puede convertir en una dirección IP pública, siempre y cuando la dirección pública sea siempre la misma.

NTP: Es el protocolo de internet que permite la sincronización de los relojes en cada uno de los routers de una determinada topología.

OSPFv3: Open Shortest Path First, protocolo de enrutamiento dinámico que detecta cambios en la topología, fallas de enlace y converge en una nueva estructura rápidamente, específicamente para IPv6

VLAN: Virtual LAN, método utilizado para crear varias redes lógicas dentro de una solo red física

RESUMEN

La realización de los dos escenarios propuestos por el curso de Diplomado Cisco, es con el objetivo de obtener el grado como profesional en la carrera de Ingeniería de Sistemas y electrónica, en donde se lleva a cabo habilidades practicas CCNA mediante la ejecución de dos escenarios propios con temas vistos durante el curso, a través de la herramienta de simulación como lo es el Packet Tracert y laboratorios Smartlab propios de CISCO, cabe destacar que fueron redes complejas para su configuración dentro de los parámetros establecidos por la guía propuesta para tal fin, como lo fue las tablas de enrutamiento las cuales debían ser tomadas en cuenta punto por punto para la configuración de los dispositivos presentes en cada topología, en donde se evidencio el trabajo de conmutación con parámetros del modelo OSI en dos capas específicas como lo fue la capa 2 y 3, sin dejar a un lado los elementos propios de seguridad, la comunicación entre los equipos, y la importancia de las redes y la tecnología en el entorno donde como egresados lograremos salvaguardar datos como futuro ingeniero de sistemas.

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

ABSTRACT

The realization of the two scenarios proposed by the Cisco Diploma course, is with the objective of obtaining the degree as a professional in the career of Systems and Electronics Engineering, where CCNP practical skills are carried out through the execution of two own scenarios With topics seen during the course, through the simulation tool such as Packet Tracert and CISCO's own Smartlabs laboratories, it should be noted that they were complex networks for their configuration within the parameters established by the guide proposed for this purpose, such as It was the routing tables which had to be taken into account point by point for the configuration of the devices present in each topology, where the switching work with parameters of the OSI model was evidenced in two specific layers such as layer 2 and 3, without leaving aside the elements of security, communication between teams, and the importance of networks and te cnology in the environment where as graduates we will be able to safeguard data as a future systems engineer.

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

INTRODUCCION

En el curso de Diplomado de Profundización CISCO (LAN/WAN) nos permite adquirir conocimientos básicos para llevar a cabo las diversas configuraciones planteadas en el Escenario 1 propuesto en la guía de actividades, para ello se hace necesario la utilización del software Packet Tracert en donde se plantea el esquema de red, conexiones adecuadas para el vital funcionamiento de la red, cabe destacar que fue muy importante el estudio de cada uno de los capítulos del curso y de esta manera se logra analizar el uso de cada uno de los protocolos indispensables en la construcción de dos redes LAN.

Además se llevó a cabo la realización de cada una de las configuraciones planteadas en cada tabla presentada en la guía, para ello fue indispensable crear la tabla de direccionamiento y a partir de dicho esquema se procede a identificar y supervisar cada uno de los comando empleados para establecer conexión segura y eficiente en la red, se identifican dichos protocolos presente en la IOS, se evalúa el comportamiento del router R1 y el Switch S1, como el paso a paso de cada línea de código nos permite visualizar al final que está conectado cada uno de los dispositivos.

Cabe destacar que la entrega de este avance del Escenario 1, corresponde al 50% del trabajo final como alternativa de grado, siendo un proyecto aplicado con dos escenarios específicos, con sus respectivas características y requerimientos básicos para la construcción desde la construcción de la red como en la configuración de cada uno de los dispositivos presentes en la guía de actividades.

Por último se lleva a cabo la realización del escenario 2 en donde se especifica comandos más específicos como lo son las ospf en versión 3 , la seguridad de las redes, las Vlan y el routing dinámico, de igual manera se llevóla implementación del DHCP para las VLAN 21, 23 y 99, el uso de las NAT dinámicas y estáticas, el tema de la configuración de NTP, lista de control de acceso (ACL), es ahí donde se aplican los conocimientos adquiridos en cada una de las actividades propuestas en cada actividad colaborativa del curso.

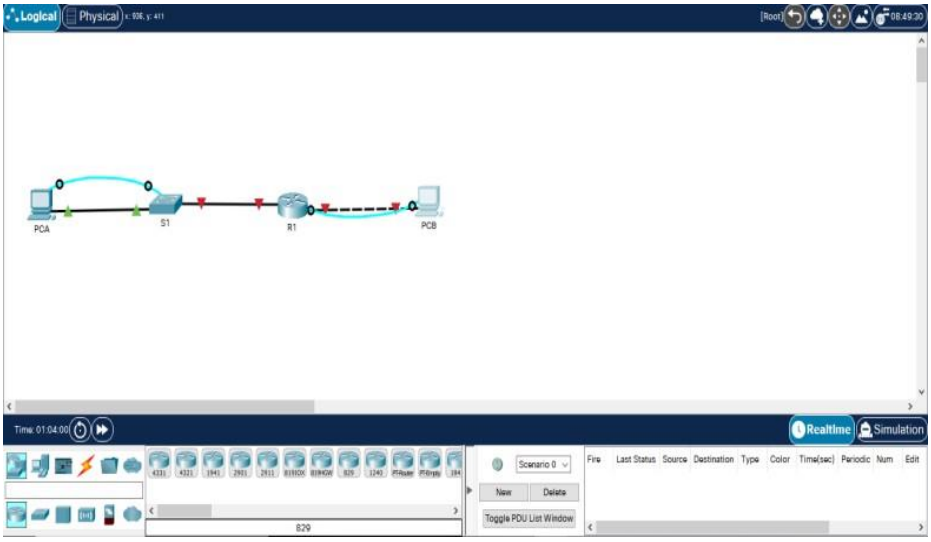
DESARROLLO

1. ESCENARIO 1

Figura 1. Escenario 1

Fuente: Autor

Figura 2. Simulación de escenario 1



Fuente: Autor

1.1 En este primer escenario se configuraran los dispositivos de una red pequeña, en donde se debe configurar:

a. Un Router.
b. Un Switch.
c. Y Dos Equipos (PCA – PCB).

En donde se debe diseñar el esquema de direccionamiento IPv4 para las LAN propuestas, el Router y el Switch también deben administrarse de forma segura. En el simulador de Packet tracert se construye la red de acuerdo a la topología

lógica presentada en la figura 1, con su respectivo cableado y conexión de los equipos.

1.2 Se procede a desarrollar el esquema de direccionamiento IP en donde se especifica las siguientes características:

a. Subred LAN1 con disponibilidad de 100 host.
b. Subred LAN2 con disponibilidad de 50 host.
c. Se tomara en cuenta la dirección IP 192.168.x.0 donde x será los últimos dos dígitos de la cedula del estudiante.

Tabla 1. Esquema de direccionamiento IP.

Item	Requerimiento
Dirección de Red	192.168.61.0/24
Requerimiento de host Subred LAN1	192.168.61.0/25
Requerimiento de host Subred LAN2	192.168.61.128/26
R1 G0/0/1	192.168.61.129/26
R1 G0/0/0	192.168.61.1/25
S1 SVI	192.168.61.2/25
PC-A	192.168.61.126/25
PC-B	192.168.61.190/26

Fuente: Autor

1.3 Configuración de ajustes básicos

Para la realización de las tareas de configuración planteadas en el escenario 1 es importante tener en consideración la información que nos proporcionan en la guía de actividades en donde se inicia con las configuraciones por consola de cada uno de los dispositivos que componen el trabajo individual.

A continuación identificaremos las tareas de configuración del R1 de acuerdo a la siguiente tabla:

Tabla 2: Configuración del R1

Ítem	Requerimiento
Desactivar la búsqueda DNS	
Nombre del router	R1
Nombre del dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoenpass

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

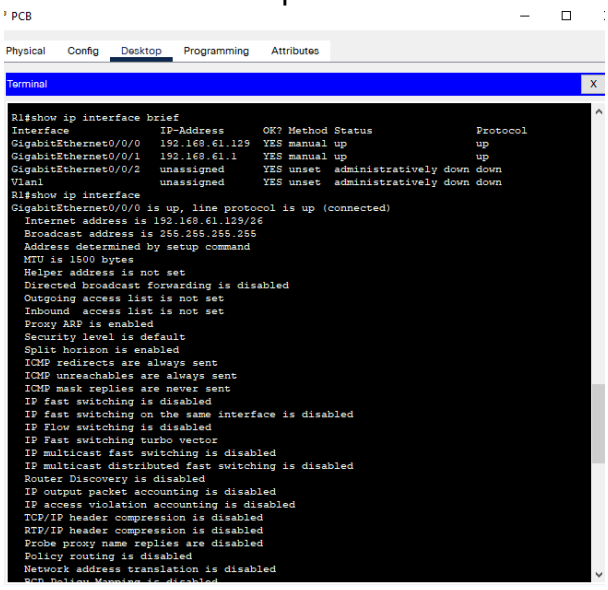
Fuente: Autor

Código del PC-B

```
Router>
Router>enable                                   Ingreso a modo privilegiado
Router#configure terminal                       Ingreso modo configuración
Router(config)#no ip domain-lookup              Desactivar búsqueda DNS
Router(config)#hostname R1                      Asigno nombre al router
R1(config)#ip domain-name ccna-lab.com          Asigno nombre de dominio
R1(config)#enable secret ciscoenpass            Contraseña Modo privilegiado
R1(config)#line console 0                       Ingreso a la consola 0 del R1
R1(config-line)#password ciscoenpass            Contraseña de la consola 0
R1(config-line)#login                           Activación Linea consola
R1(config-line)#exit                            Salida de consola
R1(config)#security password min-length 10      Asigno longitud contraseñas
R1(config)#username admin password admin1pass   Crear usuario y password BD
R1(config)#line vty 0 4                         Inicio de sesión line vty 0 4
R1(config-line)#password ciscocisco             Contraseña line vty 0 4
R1(config-line)#login local                     Activación de manera local
R1(config-line)#transport input SSH             Configuración solo SSH
R1(config-line)#exit                            Salida de consola
R1(config)#service password-encryption          Contraseña texto no cifrado
R1(config)#exit                                 Salida de consola
```

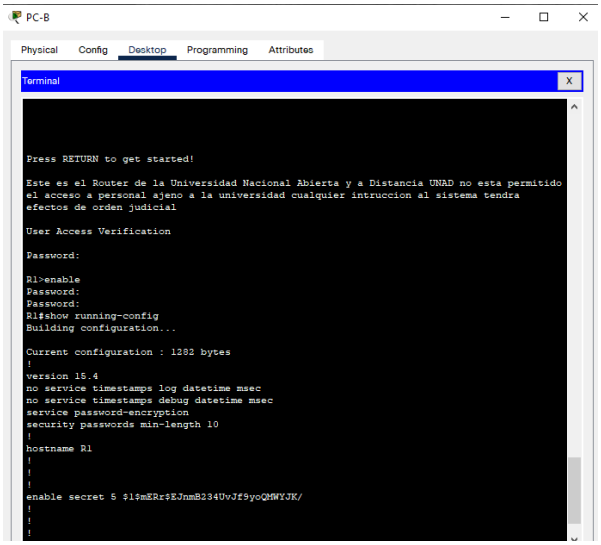
R1(config)#banner MOTD "Este es el Router de la Universidad Nacional Abierta y a Distancia UNAD no está permitido el acceso a personal ajeno a la universidad cualquier instrucción al sistema tendrá efectos de orden judicial" Banner MOTD
R1(config)#interface G0/0/0 Configuración interfaz G0/0/0
R1(config-if)#ip address 192.168.61.129 255.255.255.192 Dirección IP Interfaz
R1(config-if)#description "Esta es la Interfaz de la LAN2" Descripción de la interfaz
R1(config-if)#no shutdown Guardar la configuración
R1(config-if)#exit Salida de consola
R1(config)#interface G0/0/1 Configuración interfaz G0/0/1
R1(config-if)#description "Esta es la interfaz de la LAN1" Descripción de la interfaz
R1(config-if)#ip address 192.168.61.1 255.255.255.128 Dirección IP Interfaz
R1(config-if)#no shutdown Guardar la configuración
R1(config-if)#exit Salida de consola
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up
R1(config)#ip domain-name ccna-lab.com Generar clave de cifrado RSA
R1(config)#crypto key generate RSA general-keys modulus 1024
The name for the keys will be: R1.ccna-lab.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 2:2:25.206: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#ip ssh versión 2 Versión SSH
R1(config)#exit
R1#

Figura 3. Ejecución del comando show ip interface brief.



Fuente: Autor

Figura 4. Comando Show running-config del R1.



Fuente: Autor

Tabla 3. Configuración de S1.

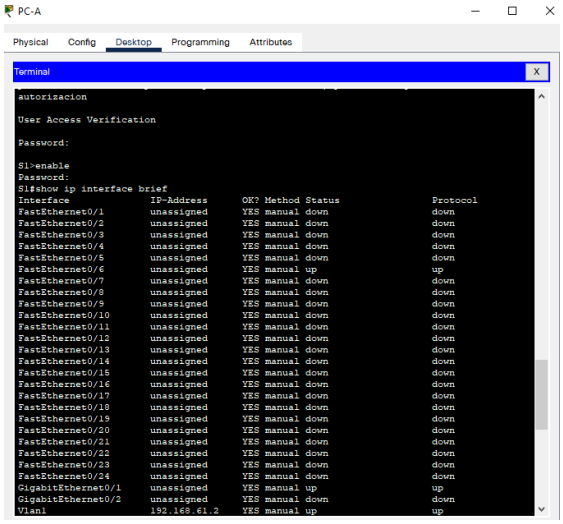
Tarea	Especificación
Desactivar la búsqueda DNS	
Nombre del switch	S1
Nombre de dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Ciscoenpass
Contraseña de acceso a la consola	Ciscoenpass
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass
Configurar 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	
Configure 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 a la tabla de direccionamiento.
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento.

Fuente: Autor

Se adjunta código y pantallazos de la configuración del Switch (S1) desde el PC-A

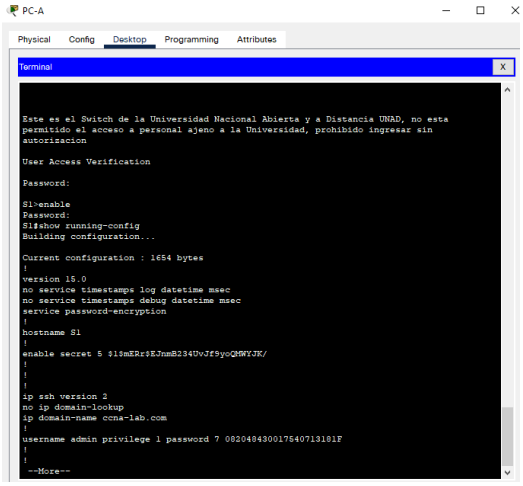
```
Switch>
Switch >enable                                          Ingreso a modo privilegiado
Switch #configure terminal                              Ingreso modo configuración
Switch (config)#no ip domain-lookup                     Desactivar búsqueda DNS
Switch (config)#hostname S1                             Asigno nombre al Switch
S1(config)#ip domain-name ccna-lab.com                  Asigno nombre de dominio
S1(config)#enable secret ciscoenpass                    Contraseña Modo
privilegiado
S1(config)#line console 0                               Ingreso a la consola 0 del S1
S1(config-line)#password ciscoenpass                    Contraseña de la consola 0
S1(config-line)#login
S1(config-line)#exit
S1(config)#username admin password admin1pass  Crear usuario y password BD
S1(config)#line vty 0 15                                Inicio de sesión line vty 0 15
S1(config-line)#password ciscocisco                     Contraseña line vty 0 15
S1(config-line)#login local                             Activación de manera local
S1(config-line)#transport input SSH                     Configuración solo SSH
S1(config-line)#exit
S1(config)#service password-encryption                  Contraseña texto no cifrado
S1(config)#exit
S1(config)#banner MOTD "Este es el Switch de la Universidad Nacional Abierta y
a Distancia UNAD, no está permitido el acceso a personal ajeno a la universidad,
prohibido ingresar sin autorización"                    Banner MOTD
S1(config)#ip domain-name ccna-lab.com                  Generar clave de cifrado RSA
S1(config)#crypto key generate RSA general-keys modulus 1024

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 1:0:35.393: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#ip ssh versión 2                             Versión del SSH
S1(config)#interface Vlan 1                             Configuración interfaz virtual SV1
S1(config-if)#ip address 192.168.61.2 255.255.255.128
S1(config-if)#no shutdown                               Guardar la configuración
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.61.1              Configuración Gateway
S1(config-if)#no shutdown                               Guardar la configuración
S1(config-if)#exit
S1#
```

Figura 5 Ejecución del comando Show ip interface brief del S1.



Fuente: Autor

Figura 6 comando show running-config del S1



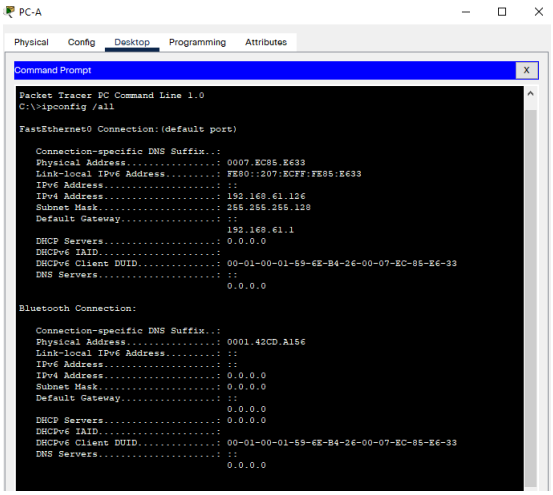
Fuente: Autor

Tabla 4. Configuración del PC-A

PC-A Network Configuration	
Descripción	Este es el Pc de la red LAN1.
Dirección física	0007.EC85.E633
Dirección IP	192.168.61.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.61.1

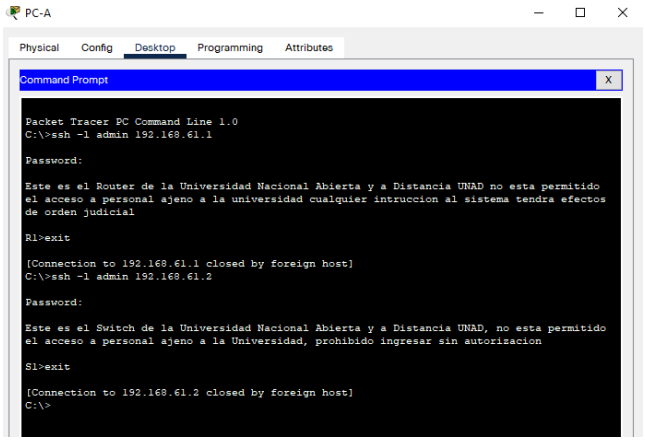
Fuente: Autor

Figura 7. Ejecución Comando ipconfig / all en el PC-A



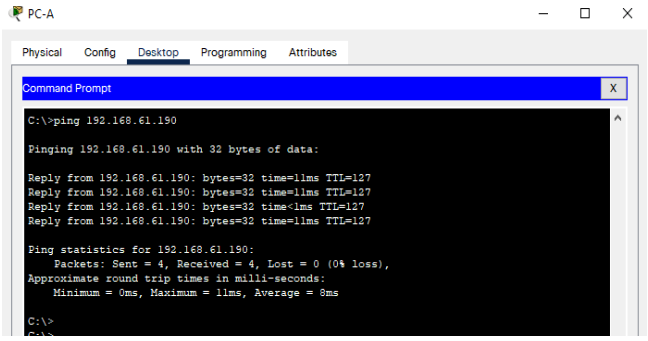
Fuente: Autor.

Figura 8 Conexión SSH desde el PC-A al R1 y S1



Fuente: Autor

Figura 9 Ping al PC-B desde el PC-A



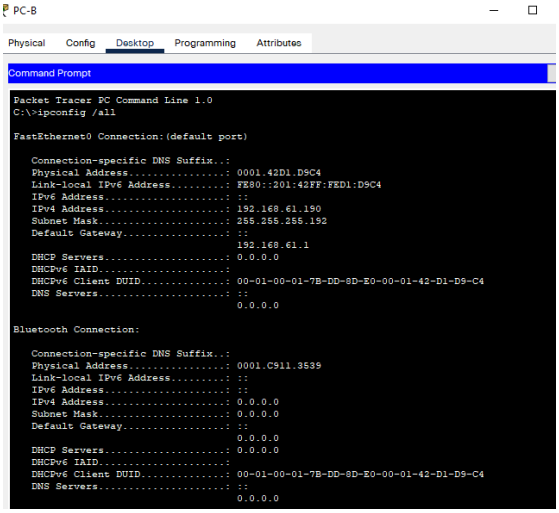
Fuente: Autor

Tabla 5. Configuración del PC-B

PC-B Network Configuration	
Descripción	Este es el Pc de la red LAN2.
Dirección física	0001.42D1.D9C4
Dirección IP	192.168.61.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.61.1

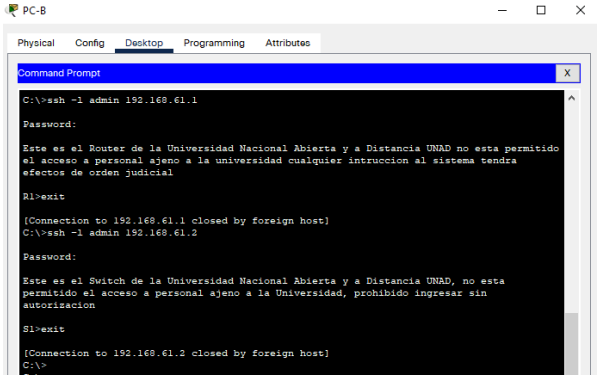
Fuente: Autor

Figura 10 Ejecución del comando Ipconfig /all en el PC-B



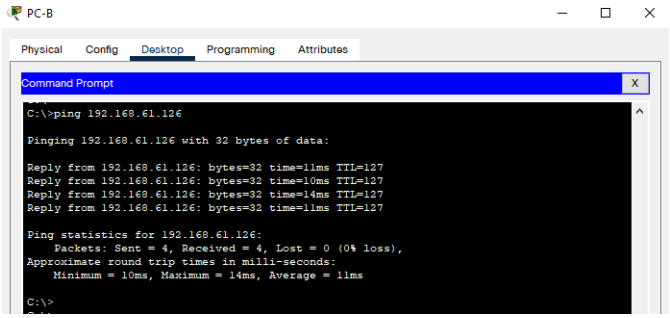
Fuente: Autor

Figura 11 Conexión SSH desde el PC-B al R1 y S1.



Fuente: Autor

Figura 12 Ping al PC-A desde el PC-B

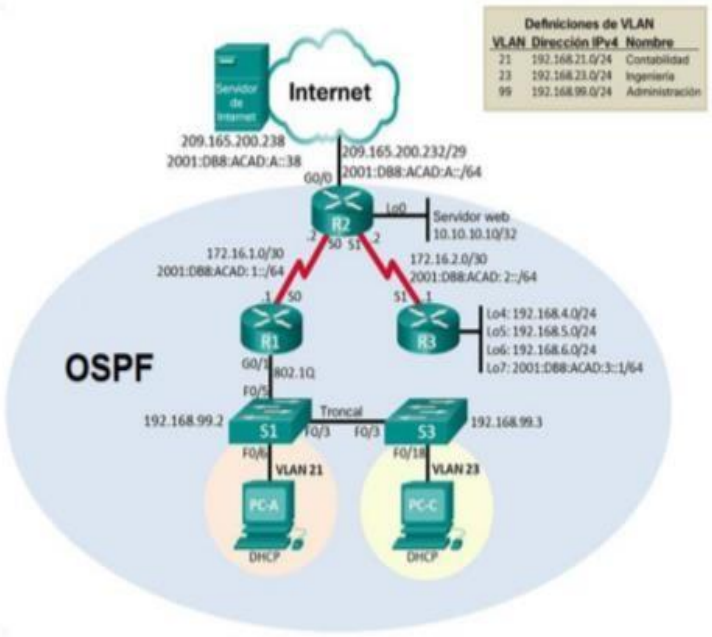


Fuente: Autor

DESARROLLO

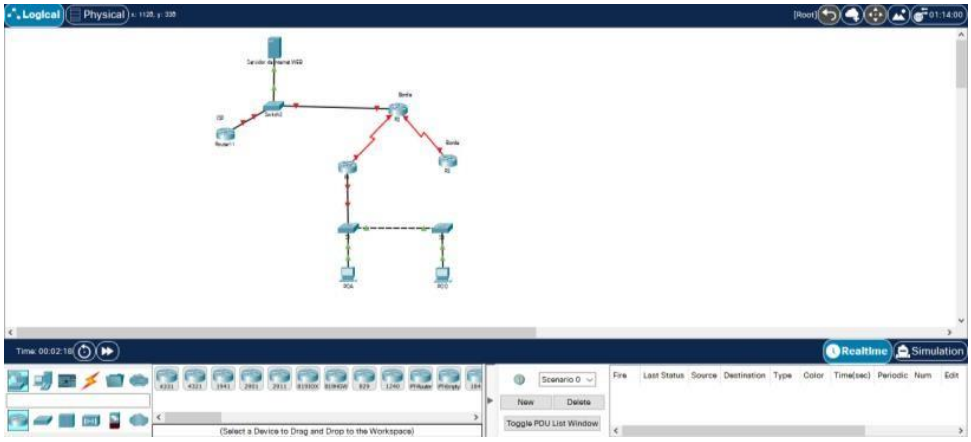
1. ESCENARIO 2

Figura 13. Escenario 2



Fuente: Autor

Figura 14. Simulación de 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 6. Inicializar y volver a cargar los routers y switches

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	R1#erase startup-config R2#erase startup-config R3#erase startup-config R11#erase startup-config
Volver a cargar todos los routers.	R1#reload R2#reload R3#reload R11#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior.	S1#erase startup-config S1#delete vlan.dat S2#erase startup-config S2#delete vlan.dat S3#erase startup-config S3#delete vlan.dat
Volver a cargar ambos switches.	S1#reload S2#reload S3#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches.	S1#show vlan S1#show flash S2#show vlan S2#show flash S3#show vlan S3#show flash

Fuente: Autor

Codigo del R1

Router>enable	Ingreso a modo privilegiado.
Router#erase startup-config	Borrar configuración del R1.

Código del R2

Router>enable	Ingreso a modo privilegiado.
Router#erase startup-config	Borrar configuración del R2.

Código del R3

Router>enable	Ingreso a modo privilegiado.
Router#erase startup-config	Borrar configuración del R3.

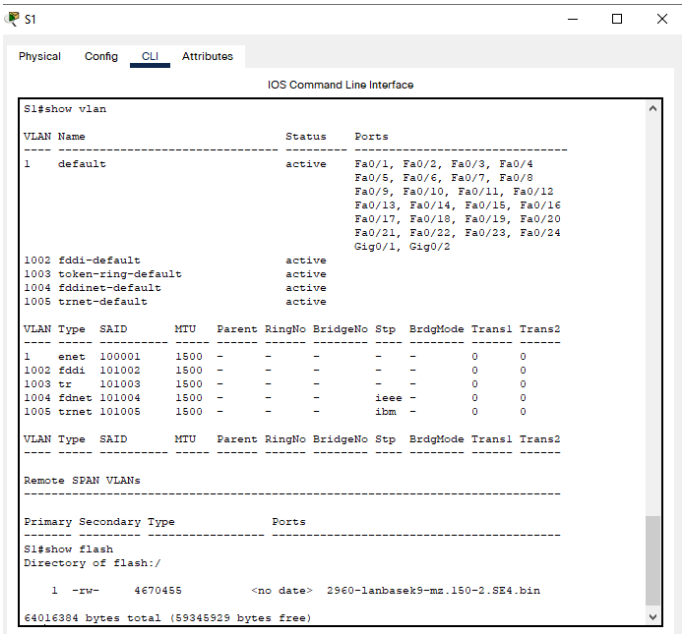
Código del Router11

Router>enable	Ingreso a modo privilegiado.
Router#erase startup-config	Borrar configuración del Router11.

CODIGO DEL S1

Switch>enable	Ingreso a modo privilegiado.
Switch#erase startup-config	Borrar configuración del S1.

Figura 15. Ejecución del comando show vlan y show flash al S1

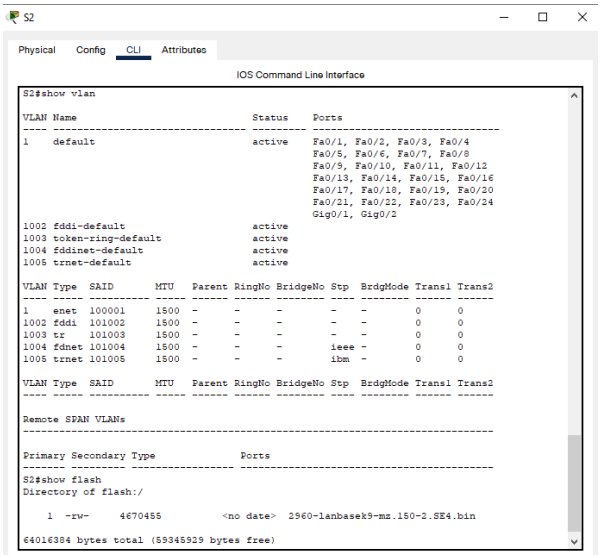


Fuente: Autor

Código del S2

Switch>enable	Ingreso a modo privilegiado.
Switch#erase startup-config	Borrar configuración del S2.

Figura 16. Ejecución del comando show vlan y show flash al S2

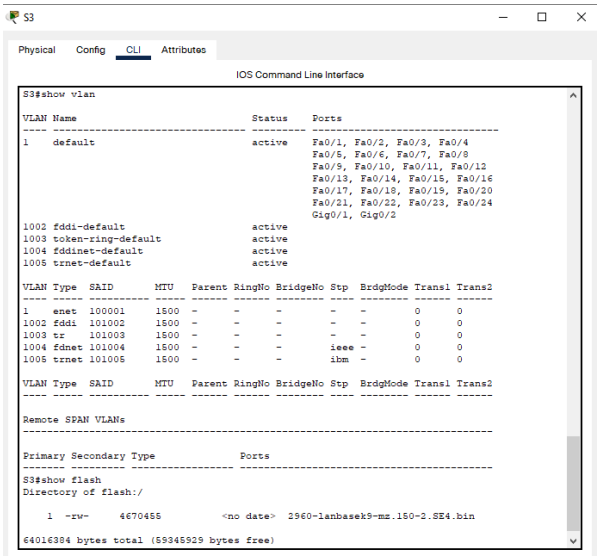


Fuente: Autor

Código del S3

Switch>enable	Ingreso a modo privilegiado.
Switch#erase startup-config	Borrar configuración del S3.

Figura 17. Ejecución del comando show vlan y show flash al S3



Fuente: Autor

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

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

Tabla 7. Configuración del Servidor de Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1/64

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.

Configuración del Router11

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface G0/0/1
Router(config-if)#ip address 209.165.200.234 255.255.255.248
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

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

Router#
```

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 8. Configuración del 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 S0/2/0	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.

Código del R1

```
Router>enable                                   Ingreso a modo privilegiado
Router#configure terminal                       Ingreso modo configuracion
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup              Desactivar búsqueda DNS
Router(config)#hostname R1                      Asigno nombre al Router
R1(config)#enable secret class                  Contraseña modo privilegiado
R1(config)#line console 0                       Ingreso a la consola 0 del R1
```

R1(config-line)#password cisco Contraseña de la consola 0
R1(config-line)#login Habilito la contraseña
R1(config-line)#exit Salida de línea de consola
R1(config)#line vty 0 4 Inicio de sesión vty 0 4
R1(config-line)#password cisco Contraseña line vty 0 4
R1(config-line)#login Habilito la contraseña
R1(config-line)#exit Salida de línea vty
R1(config)#service password-encryption Contraseña texto no cifrado
R1(config)#banner motd "Se prohibe el acceso no autorizado" Banner motd
R1(config)#interface S0/2/0 Configuración interfaz S0/2/0
R1(config-if)#description Interface hacia el Router R2 Descripción de la interfaz
R1(config-if)#exit Salida de la interfaz
R1(config)#ipv6 unicast-routing
R1(config)#interface S0/2/0 Ingreso a la interfaz serial
R1(config-if)#ip address 172.16.1.1 255.255.255.252 Direccion ip de la serial
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 Dirección IPv6 serial
R1(config-if)#clock rate 128000 Configuración del reloj
R1(config-if)#no shutdown Guardar la configuración
%LINK-5-CHANGED: Interface Serial0/2/0, changed state to down
R1(config-if)#exit Salida de la interfaz
R1(config)#ip route 0.0.0.0 0.0.0.0 S0/2/0 Configuracion del ip route
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#ipv6 route ::/0 S0/2/0 Configuración IPv6 route
R1(config)#exit Salida de consola
R1#

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 9. Configuración del 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
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Interfaz S0/2/0	Establezca la descripción Establecer la dirección IPv4 consultar el diagrama de topología para conocer la información de direcciones. Establecer la dirección IPv6 consultar el diagrama de topología para conocer la información de direcciones. Activar la interfaz.
Interfaz S0/2/1	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.
Interfaz G0/0/0 (Simulación de Internet)	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz.
Interfaz loopback 0 (Servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.
Rutas predeterminadas	Configure una ruta IPv4 predeterminado de G0/0/0. Configure una ruta IPv6 predeterminada de G0/0/0.

Fuente: Autor

Código del R2

```
Router>enable                                   Ingreso modo privilegiado
Router#configure terminal                       Ingreso modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup              Desactivar búsqueda DNS
Router(config)#hostname R2                      Asigno nombre al Router
R2(config)#enable secret class                  Contraseña modo privilegiado
R2(config)#line console 0                       Ingreso a la consola 0
R2(config-line)#password cisco                  Contraseña de la consola 0
R2(config-line)#login                           Habilito la contraseña
```

R2(config-line)#exit Salida de la consola 0
R2(config)#line vty 0 4 Ingreso a la Linea vty
R2(config-line)#password cisco Contraseña de la línea vty
R2(config-line)#login Habilito la contraseña
R2(config-line)#exit Salida de la línea vty
R2(config)#service password-encryption Contraseña de texto no cifrado
R2(config)#banner motd " Se prohibe el acceso no autorizado" Banner motd
R2(config)#interface S0/2/0 Configuración interfaz
R2(config-if)#description Conexion entre R2 a R1 Descripción interfaz
R2(config-if)#ip address 172.16.1.2 255.255.255.252 Dirección IP interfaz
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 Dirección IPv6 interfaz
R2(config-if)#no shutdown Guarda la configuración
R2(config-if)#exit Salida de la interfaz
R2(config)#ipv6 unicast-routing Activación IPv6
R2(config)#interface S0/2/1 Configuración interfaz
R2(config-if)#description conexion entre R2 a R3 Descripción interfaz
R2(config-if)#ip address 172.16.2.1 255.255.255.252 Dirección IP interfaz
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 Dirección IPv6 interfaz
R2(config-if)#clock rate 128000 Configuración reloj
R2(config-if)#no shutdown Guarda la configuración
R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/2/0, changed state to up
R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed state to up
R2(config-if)#exit Salida de la interfaz
R2(config)#interface G0/0/0 Configuracíon interfaz
R2(config-if)#description Interface hacia Internet Descripción interfaz
R2(config-if)#ipv6 unicast-routing Activación IPv6
R2(config)#interface G0/0/0 Configuración interfaz
R2(config-if)#ip address 209.165.200.233 255.255.255.248 Dirección IP interfaz
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 Dirección IPv6 interfaz
R2(config-if)#no shutdown Guarda la configuración
%SYS-5-CONFIG_I: Configured from console by console
R2(config-if)#exit Salida de la interfaz
R2(config)#interface loopback 0 Configurar Loopback0
R2(config-if)#description Servidor Web Descripción L0
R2(config-if)#ip address 10.10.10.10 255.255.255.255 Dirección L0
R2(config-if)#exit Salida de la L0
R2(config)#ip route 0.0.0.0 0.0.0.0 G0/0/0 Configuración ip route
%Default route without gateway, if not a point-to-point interface, may impact performance
R2(config)#ipv6 route ::/0 G0/0/0 Configurar IPv6 route
R2(config)#exit Salida de consola
R2#

Paso 4: configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 10. Configuración del 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 S0/2/1	Establezca la descripción Establecer la dirección IPv4 consultar el diagrama de topología para conocer la información de direcciones. Establecer la dirección IPv6 consultar el diagrama de topología para conocer la información de direcciones. Activar la interfaz.
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
Rutas predeterminadas	

Fuente: Autor

Código del R3

```
Router>enable                                   Ingreso modo privilegiado
Router#configure terminal                       Ingreso modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup              Desactivar búsqueda DNS
```

```
Router(config)#hostname R3                                  Asigno nombre al Router
R3(config)#enable secret class                              Contraseña modo privilegiado
R3(config)#line console 0                                   Ingreso a la consola 0
R3(config-line)#password cisco                              Contraseña de la consola 0
R3(config-line)#login                                       Habilito la contraseña
R3(config-line)#exit                                        Salida de la consola 0
R3(config)#line vty 0 4                                     Ingreso a la Linea vty
R3(config-line)#password cisco                              Contraseña de la línea vty
R3(config-line)#login                                       Habilito la contraseña
R3(config-line)#exit                                        Salida de la línea vty
R3(config)#service password-encryption                      Contraseña de texto no cifrado
R3(config)#banner motd " Se prohibe el acceso no autorizado" Banner motd
R3(config)#interface S0/2/1                                 Configuración de la interfaz
R3(config-if)#ipv6 unicast-routing                          Activación IPv6 interfaz
R3(config)#interface S0/2/1                                 Configuración interfaz
R3(config-if)#description conexion entre R3 a R2            Descripción interfaz
R3(config-if)#ip address 172.16.2.2 255.255.255.252 Dirección IP interfaz
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 Dirección IPv6 interfaz
R3(config-if)#no shutdown                                   Guarda la configuración
R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/2/1, changed state to up
R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/1, changed state
to up
R3(config-if)#exit                                          Salida de la interfaz
R3(config)#interface loopback 4                             Configuración Loopback 4
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state
to up
R3(config-if)#ip address 192.168.4.1 255.255.255.0          Dirección IP Loopback 4
R3(config-if)#exit                                          Salida de Loopback 4
R3(config)#interface loopback 5                             Configuración Loopback 5
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state
to up
R3(config-if)#ip address 192.168.5.1 255.255.255.           Dirección IP Loopback 5
R3(config-if)#exit                                          Salida de Loopback 5
R3(config)#interface loopback 6                             Configuración Loopback 6
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state
to up
```

R3(config-if)#ip address 192.168.6.1 255.255.255.0 Dirección IP Loopback 6
R3(config-if)#exit Salida de Loopback 6
R3(config)#interface loopback 7 Configuración Loopback 7

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback7, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 Dirección IPV6 L7
R3(config-if)#exit Salida de Loopback 7
R3(config)#ip route 0.0.0.0 0.0.0.0 S0/2/1 Dirección ip route serial
%Default route without gateway, if not a point-to-point interface, may impact performance
R3(config)#ipv6 route ::/0 S0/2/1 Dirección IPv6 route Serial
R3(config)#exit Salida de la consola
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 11. Configuración del 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

Código del S1

Switch>enable Ingreso modo privilegiado
Switch#configure terminal Ingreso modo configuración
Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#no ip domain-lookup Desactivar Búsqueda DNS
Switch(config)#hostname S1 Asigno nombre al Switch
S1(config)#enable secret class Contraseña modo privilegiado
S1 (config)#line console 0 Ingreso a la consola 0
S1 (config-line)#password cisco Contraseña de la consola 0
S1 (config-line)#login Habilito la contraseña
S1 (config-line)#exit Salida de la consola 0
S1 (config)#line vty 0 15 Ingreso a la Linea vty
S1 (config-line)#password cisco Contraseña de la línea vty
S1 (config-line)#login Habilito la contraseña
S1 (config-line)#exit Salida de la línea vty
S1 (config)#service password-encryption Contraseña de texto no cifrado
S1 (config)#banner motd " Se prohibe el acceso no autorizado" Banner motd
S1 (config)#exit Salida de consola
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#

Paso 5.1: Configurar S2

La configuración del S2 incluye las siguientes tareas:

Tabla 12. Configuración del S2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del switch	S2
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

Código del S2

Switch>enable Ingreso modo privilegiado
Switch#configure terminal Ingreso modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup Desactivar Búsqueda DNS
Switch(config)#hostname S2 Asigno nombre al Switch
S2(config)#enable secret class Contraseña modo privilegiado

S2 (config)#line console 0 Ingreso a la consola 0
S2 (config-line)#password cisco Contraseña de la consola 0
S2 (config-line)#login Habilito la contraseña
S2 (config-line)#exit Salida de la consola 0
S2 (config)#line vty 0 15 Ingreso a la Linea vty
S2 (config-line)#password cisco Contraseña de la línea vty
S2 (config-line)#login Habilito la contraseña
S2 (config-line)#exit Salida de la línea vty
S2 (config)#service password-encryption Contraseña de texto no cifrado
S2 (config)#banner motd " Se prohibe el acceso no autorizado" Banner motd
S2 (config)#exit Salida de consola
S2#
%SYS-5-CONFIG_I: Configured from console by console
S2#

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 13. Configuración del S3

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

Código del S3

Switch>enable Ingreso modo privilegiado
Switch#configure terminal Ingreso modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup Desactivar Búsqueda DNS
Switch(config)#hostname S3 Asigno nombre al Switch
S3(config)#enable secret class Contraseña modo privilegiado
S3 (config)#line console 0 Ingreso a la consola 0
S3 (config-line)#password cisco Contraseña de la consola 0
S3 (config-line)#login Habilito la contraseña

S3 (config-line)#exit Salida de la consola 0
S3 (config)#line vty 0 15 Ingreso a la Linea vty
S3 (config-line)#password cisco Contraseña de la línea vty
S3 (config-line)#login Habilito la contraseña
S3 (config-line)#exit Salida de la línea vty
S3 (config)#service password-encryption Contraseña de texto no cifrado
S3 (config)#banner motd " Se prohibe el acceso no autorizado" Banner motd
S3 (config)#exit Salida de consola
S3#
%SYS-5-CONFIG_I: Configured from console by console
S3#

Paso 7: Verificar la conectividad de la red

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

Tabla 14. Verificación de conectividad en la red

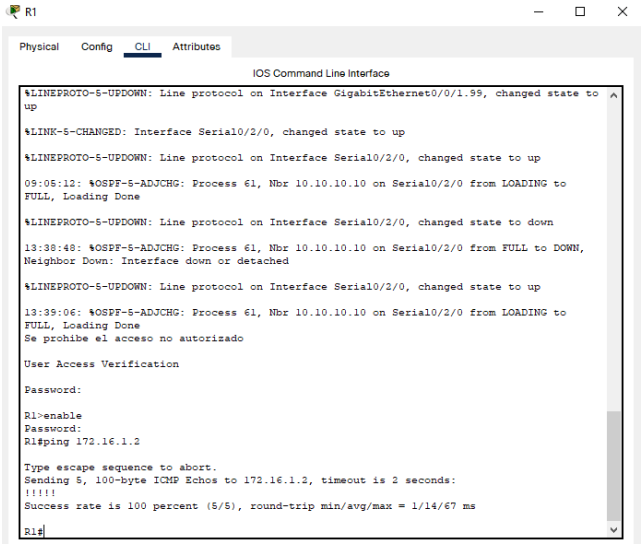
Desde	A	Dirección IP	Resultados de ping
R1	**R2, S0/2/0**	172.16.1.2	R1#ping 172.16.1.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/15/75 ms R1#
R2	**R3, S0/2/1**	172.16.2.2	R2#ping 172.16.2.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/25 ms R2#
PC de Internet	**Gateway predeterminado**	2001:DB8:ACAD:A::1	Packet Tracer SERVER Command Line 1.0 C:\>ping 2001:DB8:ACAD:A::1 Pinging 2001:DB8:ACAD:A::1 with 32

			bytes of data: Reply from 2001:DB8:ACAD:A::1: bytes=32 time=25ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 Ping statistics for 2001:DB8:ACAD:A::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 25ms, Average = 6ms C:\>

Fuente: Autor

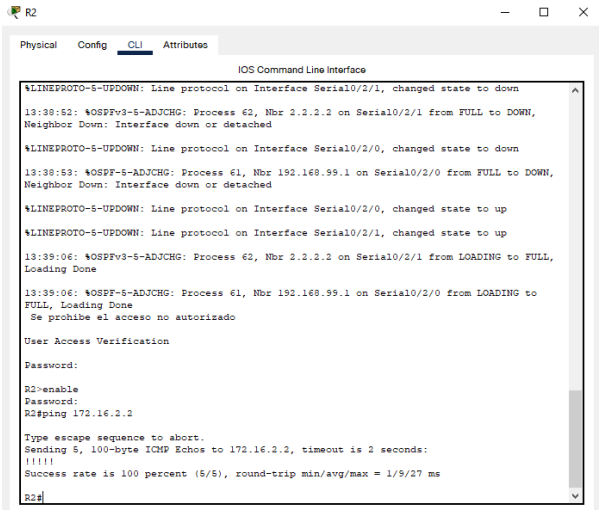
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Figura 18. Ping desde el R1 al R2 a la interfaz S0/2/0



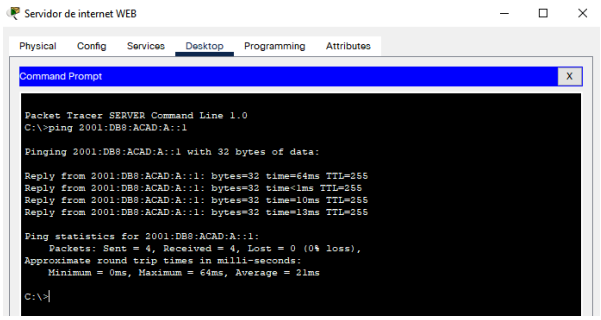
Fuente: Autor

Figura 19. Ping desde el R2 al R3 a la interfaz S0/2/1



Fuente: Autor

Figura 20. Ping desde el PC de internet al Gateway predeterminado



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 15. Configuración Seguridad S1, VLAN y Routing

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.
	Asigne la dirección IPv4 a la VLAN de

Asignar la dirección IP de administración.	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 de interface range.
Asignar f0/6 a la VLAN 21	
Apagar todos los puertos sin usar.	

Fuente: Autor

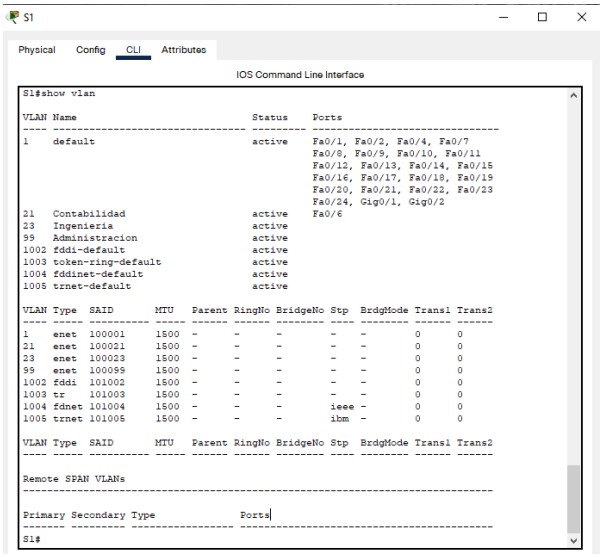
Código del S1

```
S1#configure terminal                          Ingreso modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 21                             Ingreso a la Vlan 21
S1(config-vlan)#name Contabilidad              Asigno nombre Vlan
S1(config-vlan)#vlan 23                        Ingreso a la Vlan 23
S1(config-vlan)#name Ingenieria                Asigno nombre Vlan
S1(config-vlan)#vlan 99                        Ingreso a la Vlan 99
S1(config-vlan)#name Administracion            Asigno nombre Vlan
S1(config-vlan)#exit                           Salida de las Vlans
S1(config)#exit                                Salida de consola
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#
S1#configure terminal                          Ingreso modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface F0/3                      Configuración de la interfaz
S1(config-if)#sw mode trunk                    Configurar modo Trunk
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to
up
S1(config-if)#sw trunk native vlan 1           Configurar modo trunk native
S1(config-if)#exit                             Salida de interfaz
S1(config)#interface F0/5                      Configuración de la interfaz
```

S1(config-if)#sw mode trunk Configurar modo Trunk
S1(config-if)#switchport trunk native vlan 1 Configurar modo trunk native
S1(config-if)#exit Salida de interfaz
S1(config)#int range F0/1 - F0/2 Configurar rango de interfaces
S1(config-if-range)#sw mode access Configurar modo de acceso
S1(config-if-range)#int range F0/7 - F0/24 Configurar rango de interfaces
S1(config-if-range)#sw mode access Configurar modo de acceso
S1(config-if-range)#exit Salida de interfaz
S1(config)#interface F0/6 Configuración de la interfaz
S1(config-if)#sw access vlan 21 Configurar modo de acceso
S1(config-if)#exit Salida de la interfaz
S1(config)#int range F0/7 - F0/24 Configurar rango de interfaces
S1(config-if-range)#shutdown Deshabilitar los rangos
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
S1(config-if-range)#exit Salida configuración rangos
S1(config)#exit Salida de consola
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#

Figura 21. Resultados del S1 con el comando show vlan



Fuente: Autor

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 16. Configuración del 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 y nombrar cada una de las VLAN que se indican.
Asignar la dirección IP de	Asigne la dirección IPv4 a la VLAN de administración.

administración.	Utilizar la dirección IP asignada al S3 en el diagrama de topología.
Asignar el gateway predeterminado.	Asigne 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 de interface range.
Asignar f0/18 a la VLAN 21	
Apagar todos los puertos sin usar.	

Fuente: Autor

Código del S3

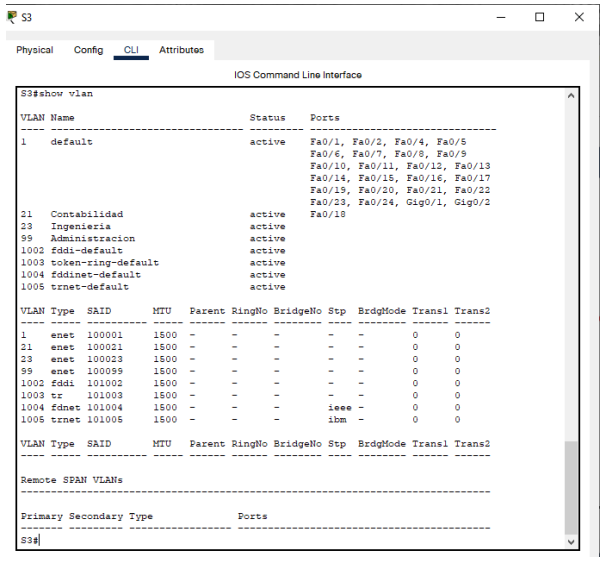
S3#configure terminal Ingreso modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vlan 21 Ingreso a la Vlan 21
S3(config-vlan)#name Contabilidad Asigno nombre Vlan
S3(config-vlan)#vlan 23 Ingreso a la Vlan 23
S3(config-vlan)#name Ingenieria Asigno nombre Vlan
S3(config-vlan)#vlan 99 Ingreso a la Vlan 99
S3(config-vlan)#name Administracion Asigno nombre Vlan
S3(config-vlan)#exit Salida de las Vlans
S3(config)#interface vlan 99 Configuración de la interfaz
S3(config-if)#

%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
S3(config-if)#ip address 192.168.99.3 255.255.255.0 Configurar IP Vlan 99
S3(config-if)#no shutdown Activar la interfaz
S3(config-if)#exit Salida de la interfaz Vlan99
S3(config)#ip default-gateway 192.168.99.1 Configurar gateway defecto
S3(config)#interface F0/3 Configuración de la interfaz
S3(config-if)#sw mode trunk Configurar modo Trunk
S3(config-if)#sw trunk native vlan 1 Configurar modo trunk native
S3(config-if)#exit Salida de la interfaz
S3(config)#int range F0/1 - F0/2 Configurar rango de interfaces
S3(config-if-range)#sw mode access Configurar modo de acceso
S3(config-if-range)#int range F0/7 - F0/24 Configurar rango de interfaces
S3(config-if-range)#sw mode access Configurar modo de acceso
S3(config-if-range)#exit Salida de la interfaz rango
S3(config)#interface F0/18 Configuración de la interfaz
S3(config-if)#sw access vlan 21 Configurar modo de acceso

S3(config-if)#exit Salida de la interfaz rango
S3(config)#int range F0/7 - F0/17 Configurar rango de interfaces
S3(config-if-range)#shutdown Desactivar las interfaces
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down
S3(config-if-range)#int range F0/19 - F0/24 Configurar rango de interfaces
S3(config-if-range)#shutdown Desactivar las interfaces
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
S3(config-if-range)#exit Salida configuración rangos
S3(config)#exit Salida de consola
S3#
%SYS-5-CONFIG_I: Configured from console by console
S3#

Figura 22 Resultados del S3 con el comando show vlan



Fuente: Autor

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17. Configuración del 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	

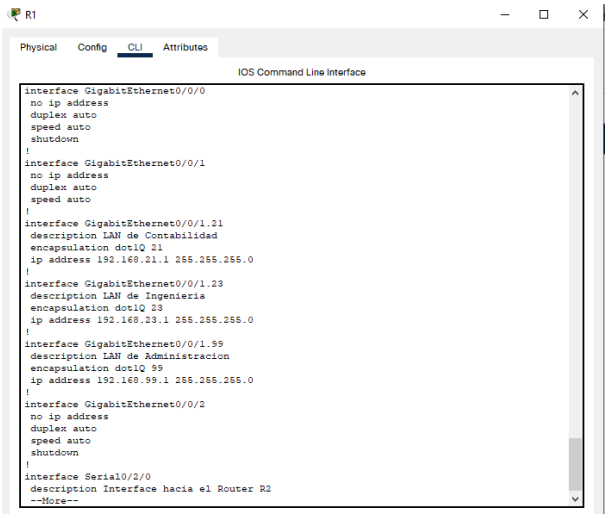
Fuente: Autor

Código del R1

R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

```
R1(config)#interface G0/0/1
R1(config-if)#no shutdown
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up
R1(config-if)#exit
R1(config)#interface G0/0/1.21
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.21, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.21, changed state to up
R1(config-subif)#description LAN de Contabilidad
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface G0/0/1.23
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.23, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.23, changed state to up
R1(config-subif)#description LAN de Ingenieria
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface G0/0/1.99
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.99, changed state to up
R1(config-subif)#description LAN de Administracion
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#exit
R1#

%SYS-5-CONFIG_I: Configured from console by console


R1#
```

Figura 23. Activación y configuración de las subinterfaces en el R1



Fuente: Autor

Paso 4: Verificar la conectividad de la red

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

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

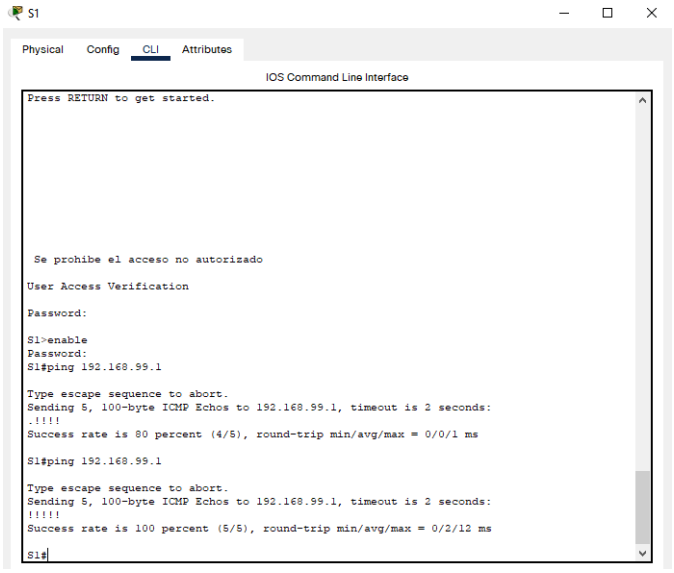
Tabla 18. Verificación conectividad entre los switches y el R1

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 = 0/0/1 ms S1#
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 = 0/2/11 ms S3#
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 = 0/0/1 ms S1#
S3	R1, dirección VLAN 23	192.168.23.1	S3#ping 192.168.23.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/6 ms S3#

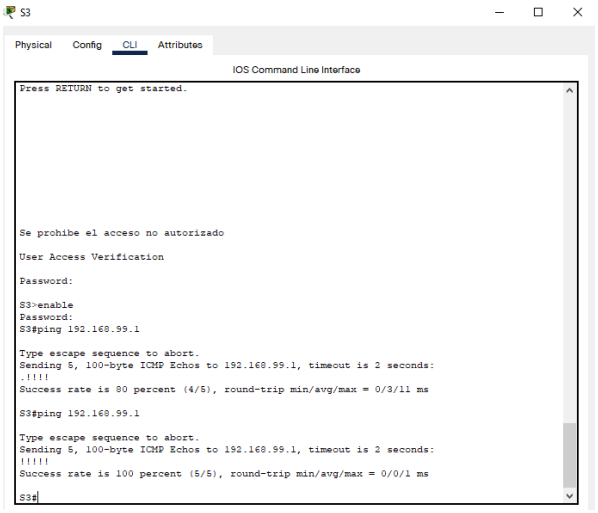
Fuente: Autor

Figura 24. Ping desde S1 a R1 de la VLAN 99



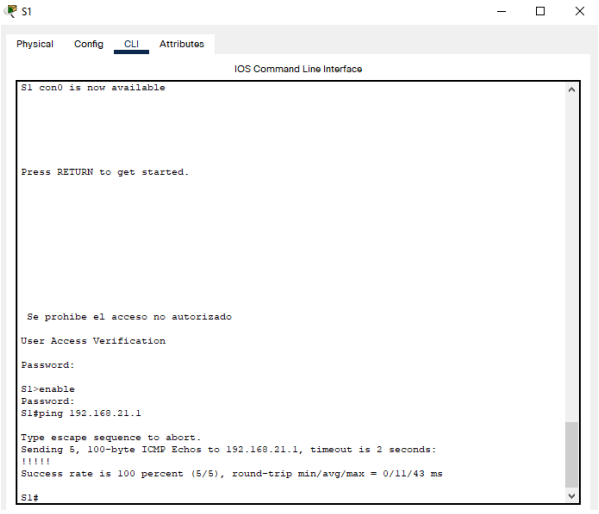
Fuente: Autor

Figura 25. Ping desde S3 a R1 de la VLAN 99



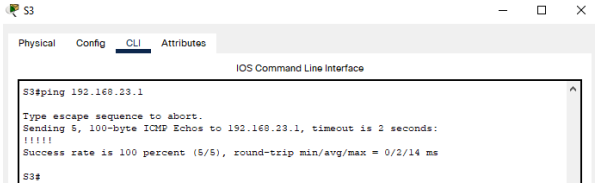
Fuente: Autor

Figura 26.. Ping desde S1 al R1 de la VLAN 23



Fuente: Autor

Figura 27. Ping desde S3 a R1 de la VLAN 23



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 19. Configuración OSPF en el R1

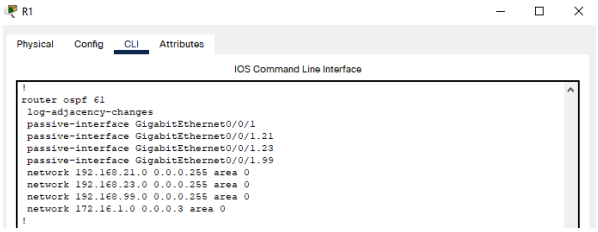
Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 61
Anunciar las redes conectadas directamente.	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas.	R1(config-router)#passive-interface G0/0/1 R1(config-router)#passive-interface G0/0/1.21 R1(config-router)#passive-interface G0/0/1.23 R1(config-router)#passive-interface G0/0/1.99
Desactive la sumarización.	Recuerda Ingeniero Raul que usted nos dijo que no se puede hacer en protocolo RIP solo se hace en protocolo EIGRP.

Fuente: Autor

Código del R1

```
R1#configure terminal                                    Ingreso modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 61                                Ingreso ospf 61
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0  Configurar Red Vlan 21
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0  Configurar Red Vlan 23
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0  Configurar Red Vlan 99
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 Configurar Red
R1(config-router)#passive-interface G0/0/1               Configurar int pasiva Gb
R1(config-router)#passive-interface G0/0/1.21            Configurar int pasiva Vlan 21
R1(config-router)#passive-interface G0/0/1.23            Configurar int pasiva Vlan 23
R1(config-router)#passive-interface G0/0/1.99            Configurar int pasiva Vlan 99
R1(config-router)#exit                                   Salida de configuración R1
R1(config)#exit                                          Salida de consola
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#
```

Figura 28. Comando show running-config verificando las OSPF en el R1



Fuente: Autor

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 20. Configuración OSPF en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	Router ospf 61
Anunciar las redes conectadas directamente.	Nota: Omitir la red G0/0.
Establecer la interfaz LAN (Loopback) como pasiva.	Passive-interface loopback 0
Desactive la sumarización.	No se puede hacer en este sistema de enrutamiento solo se hace en RIP y en EIGRP.

Fuente: Autor

Código del R2

```
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 61
R2(config-router)#network 10.10.10.10 0.0.0.0 area 0
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
R2(config-router)#passive-interface loopback 0
R2(config-router)#exit
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#
```

Figura 29. Comando show running-config verificando la Loopback 0 en el R2

Fuente: Autor

Figura 30. Comando show running-config verificando la configuración OSPF R2

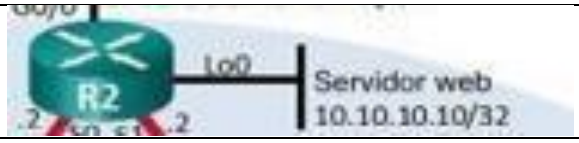
Fuente: Autor

Paso 3: Configurar OSPFv3 en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 21. Configuración OSPFv3 en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	Ipv6 router ospf 62 Router-id 1.1.1.1
Anunciar redes IPv4 conectadas directamente.	Ingeniero Raul hay un error de configuración ya que dice V3 y es IPv6, esto debe ser para redes IPv6, las cuales las interfaces van con el protocolo ospf 62. Ipv6 ospf 62 area 0 para todas las interfaces del R2 S0/2/0 S0/2/1 G0/0/0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas.	Ls Loopback no tiene direcciones bajo protocolo IPv6.

	
Desactive la sumarización automática.	En este protocolo eso no se hace para lo cual se coloca la wildcard y en IPv6 no se realiza.

Fuente: Autor

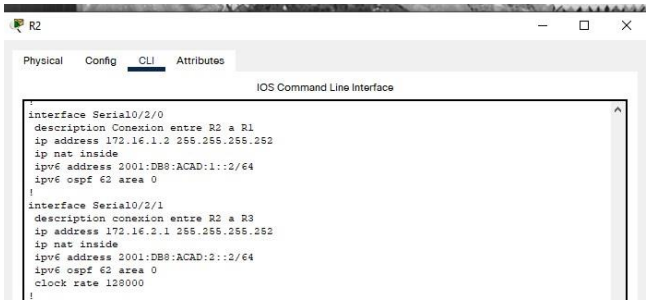
Código del R2

```
R2#configure terminal                          Ingreso a modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 router ospf 62                 Configurar IPv6 ospf 62
R2(config-rtr)#router-id 1.1.1.1               Configurar id router R2
R2(config-rtr)#exit                            Salida de consola IPv6 ospf 62
R2(config)#interface S0/2/0                    Configurar la interfaz serial
R2(config-if)#ipv6 ospf 62 area 0              Configurar IPv6 ospf 62
R2(config-if)#exit                             Salida de interfaz serial
R2(config)#interface S0/2/1                    Configurar la interfaz serial
R2(config-if)#ipv6 ospf 62 area 0              Configurar IPv6 ospf 62
R2(config-if)#exit                             Salida de interfaz serial
R2(config)#interface G0/0/0                    Configurar interfaz Gigabitethernet
R2(config-if)#ipv6 ospf 62 area 0              Configurar IPv6 ospf 62
R2(config-if)#exit                             Salida de interfaz GigabitEthernet
R2(config)#exit                                Salida de consola
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#
```

Figura 31. Resultado del protocolo OSPF en la interfaz G0/0/0 del R2

Fuente: Autor

Figura 32. Resultado del protocolo OSPF en la interfaz S0/2/0 y S0/2/1 del R2



Fuente: Autor

Figura 33. Resultado de la configuración del protocolo OSPF 62

Fuente: Autor

Paso 3.1: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 22. Configuración OSPFv3 en el R3

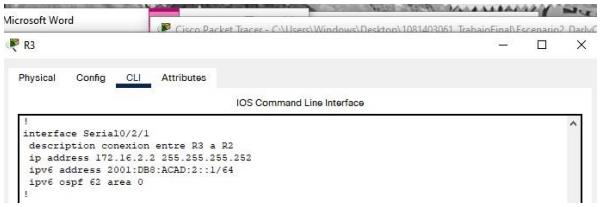
Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	Ipv6 router ospf 62 Router-id 2.2.2.2
Anunciar redes IPv4 conectadas directamente.	Ipv6 ospf 62 area 0 para todas las interfaces del R3 S0/2/1 Loopback 4, 5, 6 y 7.
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas.	Passive-interface loopback 4 Passive-interface loopback 5 Passive-interface loopback 6
Desactive la sumarización automática.	En este protocolo eso no se hace para lo cual se coloca la wildcard y en IPv6 no se realiza.

Fuente: Autor

Código del R3

```
R3#configure terminal                                  Ingreso a modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 router ospf 62                         Configurar IPv6 ospf 62
R3(config-rtr)#router-id 2.2.2.2                       Configurar id router R3
R3(config-rtr)#exit                                    Salida de consola IPv6 ospf 62
R3(config)#interface S0/2/1                            Configurar la interfaz serial
R3(config-if)#ipv6 ospf 62 area 0                      Configurar IPv6 ospf 62
R3(config-if)#exit                                     Salida de interfaz serial
R3(config)#interface loopback 7                        Configurar Loopback 7
R3(config-if)#ipv6 ospf 62 area 0                      Configurar IPv6 ospf 62
R3(config-if)#exit                                     Salida de consola
R3(config)#ipv6 router ospf 62                         Configurar IPv6 ospf 62
R3(config-rtr)#passive-interface loopback 4            Configurar interfaz pasiva L4
R3(config-rtr)#passive-interface loopback 5            Configurar interfaz pasiva L5
R3(config-rtr)#passive-interface loopback 6            Configurar interfaz pasiva L6
R3(config-rtr)#exit                                    Salida de consola IPv6 ospf 62
R3(config)#exit                                        Salida de consola R3
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#
```

Figura 34. Resultado de la configuración del protocolo OSPF en la interfaz S0/2/1 del R3

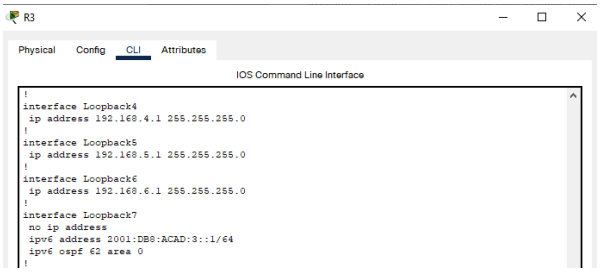


Fuente: Autor

Figura 35. Resultado del protocolo OSPF en la interfaz Loopback 4, 5, 6 del R3

Fuente: Autor

Figura 36. Resultado protocolo OSPF en la interfaz Loopback 4, 5, 6 y 7 R3



Fuente: Autor

Paso 4: Verificar la información de OSPF

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

Tabla 22. Verificación de la información de OSPF

Pregunta	Respuesta
¿Con que comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	R2#Show ip protocols – show running-config
¿Qué comando muestra solo las rutas OSPF?	R2#show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R2#show running-config

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 23. Configuración del R1 como servidor DHCP, VLAN 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas.	

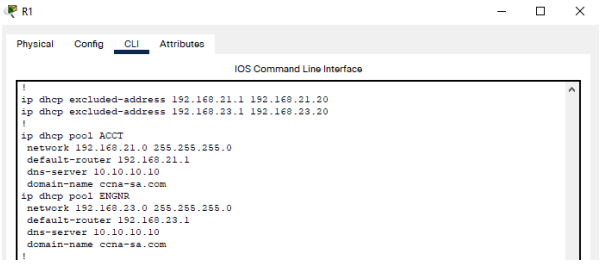
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas.	
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado.
Crear un pool de DHCP para la VLAN 23.	Nombre: ENGNR Servidor DNS: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

Fuente: Autor

Código del R1

```
R1#configure terminal                                  Ingreso modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20    Vlan21 DHCP
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20    Vlan23 DHCP
R1(config)#ip dhcp pool ACCT                           DHCP pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0     Configurar red Vlan21
R1(dhcp-config)#domain-name ccna-sa.com                Asignar nombre dominio
R1(dhcp-config)#dns-server 10.10.10.10                 Asignar IP Server
R1(dhcp-config)#default-router 192.168.21.1            Configurar por defecto R1
R1(dhcp-config)#exit                                   Salida de consola DHCP
R1(config)#ip dhcp pool ENGNR                          Configurar DHCP pool
R1(dhcp-config)#network 192.168.23.0 255.255.255.0     Configurar red Vlan23
R1(dhcp-config)#dns-server 10.10.10.10                  Asignar IP Server
R1(dhcp-config)#domain-name ccna-sa.com                 Asignar nombre dominio
R1(dhcp-config)#default-router 192.168.23.1            Configurar por defecto R1
R1(dhcp-config)#exit                                   Salida de consola DHCP
R1(config)#exit                                        Salida de consola
R1#

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

Figura 37. Resultados dhcp pool comando show running-config



Fuente: Autor

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

La configuración del R2 incluye las siguientes tareas:

Tabla 24. Configuración de la NAT estática y dinámica en el 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	Ip http server pero aparece un error de comandos en el Packet tracert.
Configurar el servidor HTPP para utilizar la base de datos local para la autenticación.	Ip http authentication local aparece un error de comandos
Crear NAT estática al servidor web.	Dirección global interna: 209.165.200.229 esta dirección está mal por lo tanto al realizar un conteo se procede a cambiarla a 209.165.200.233
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 publicas utilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 –

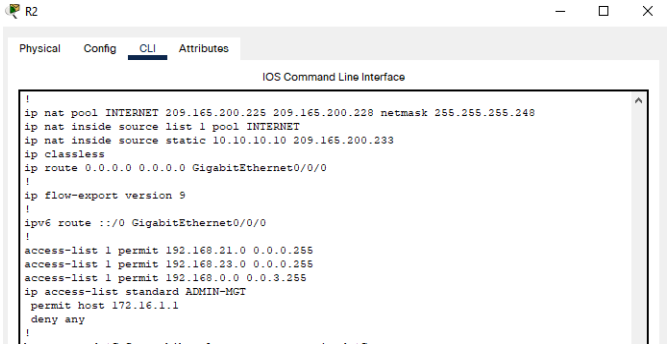
	209.165.200.228
Definir la traducción de NAT dinámica.	

Fuente: Autor

Código del R2

R2#configure terminal Ingreso modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#username webuser privilege 15 password cisco12345 Configuración del usuario y contraseña
R2(config)#ip http server Configurar IP http server
^
% Invalid input detected at '^' marker. No soporta el comando
R2(config)#ip http authentication local Configurar Authenticacion local
^
% Invalid input detected at '^' marker. No soporta el comando
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.233 Configuración de la IP Nat estática
R2(config)#interface G0/0/0 Configuración de la interfaz
R2(config-if)#ip nat outside Dirección IP nat fuera
R2(config-if)#interface S0/2/0 Configuración de la interfaz
R2(config-if)#ip nat inside Dirección IP nat activada
R2(config-if)#interface S0/2/1 Configuración de la interfaz
R2(config-if)#ip nat inside Dirección IP nat activada
R2(config-if)#interface loopback 0 Configuración Loopback 0
R2(config-if)#ip nat inside Dirección IP nat activada
R2(config-if)#exit Salida de la interfaz
R2(config)#exit Salida de consola
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#configure terminal Ingreso modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 Lista de acceso a la Vlan21
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 Lista de acceso a la Vlan23
R2(config)#access-list 1 permit 192.168.0.0 0.0.3.255 Lista de acceso IP
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248 IP nat para internet con mascara
R2(config)#ip nat inside source list 1 pool INTERNET IP nat en llista de acceso
R2(config)#exit Salida de consola
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#

Figura 38. Resultados del R2 access-list 1 comando show running-config

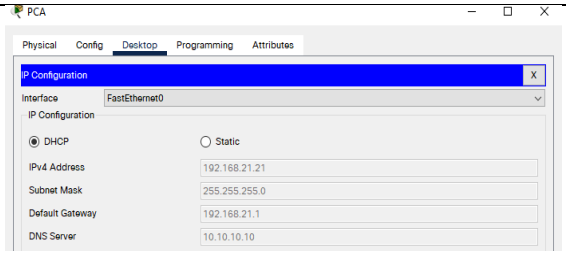
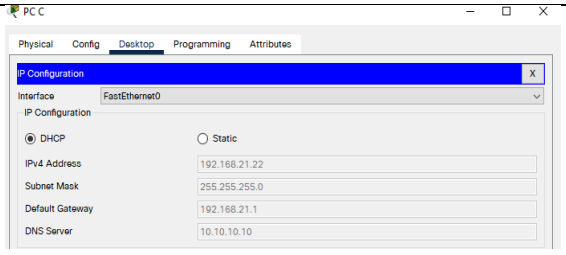


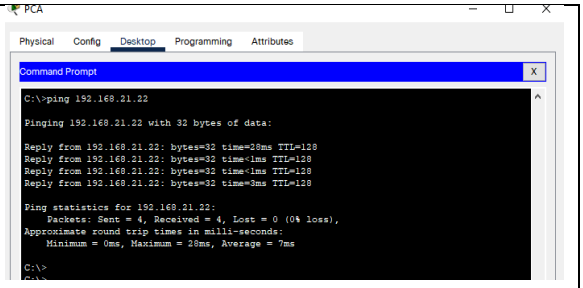
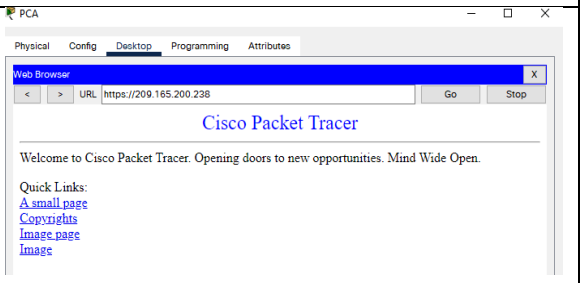
Fuente: Autor

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Tabla 25. Verificación del protocolo DHCP y 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

Tabla 26. Configuración NTP en el R2

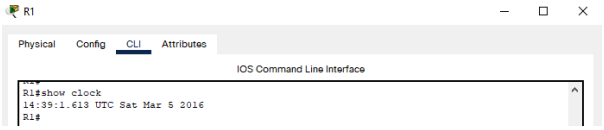
Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2	5 de marzo de 2016, 9 a.m.
Configure R2 como un maestro NTP	Nivel de estrato: 5
Configurar R1 como un cliente NTP	Servidor: R2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	
Verifique la configuración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

Fuente: Autor

Código del R2

```
R2#clock set 09:00:00 05 march 2016                Configurar hora y fecha R2
R2#configure terminal                              Ingreso modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp master 5                            Ingreso a maestro NTP
R2(config)#exit                                    Salida de consola
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#sh clock                                        Verificación hora y fecha R2
9:1:10.182 UTC Sat Mar 5 2016
R2#exit                                            Salida de consola R2
```

Figura 39. Resultado del reloj cliente servidor R1



Fuente: Autor

Figura 40. Resultado ntp server en R1

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 27. Configuración de ACL y restricción VTY en el 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 VTY.	
Verificar que la ACL funcione como se espera.	

Fuente: Autor

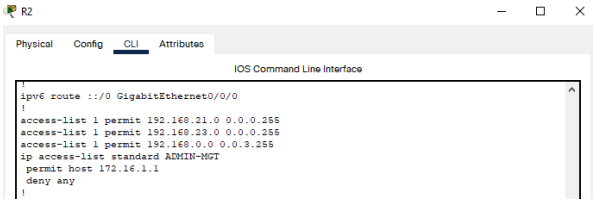
Código del R2

```
R2#configure terminal                              Ingreso modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip access-list standard ADMIN-MGT       Configurar IP lista de acceso
R2(config-std-nacl)#permit host 172.16.1.1         Permitir el PC
R2(config-std-nacl)#deny any                       Denegar cualquier host
R2(config-std-nacl)#exit                           Salida de lista de acceso
```

R2(config)#line vty 0 4	Configurar línea vty 0 4
R2(config-line)#ip access-class ADMIN-MGT in	Acceso class línea vty 0 4
R2(config-line)#transport input telnet	Entrada Transporte Telnet
R2(config-line)#exit	Salida de vty 0 4
R2(config)#exit	Salida de consola

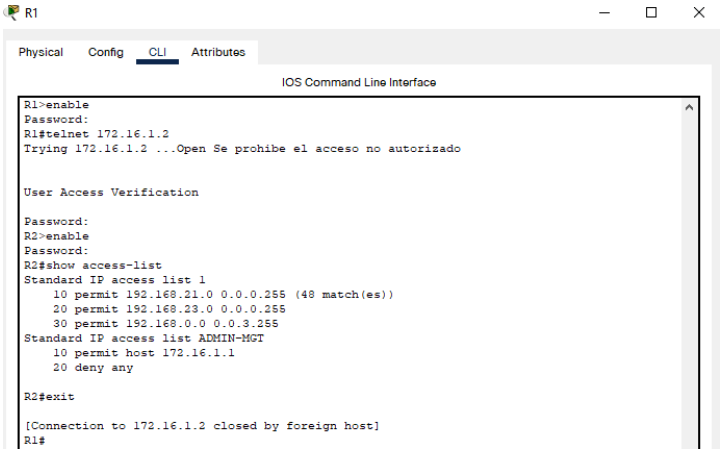
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#

Figura 41. Resultados de la configuración del R2



Fuente: Autor

Figura 42. Resultados ingresando telnet 172.16.1.2 desde el R1 al R2



Fuente: Autor

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

Tabla 28. Ejecución de comandos en el CLI del R2

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se	R2#show access-list Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 (56

restableció.	match(es)) 20 permit 192.168.23.0 0.0.0.255 30 permit 192.168.0.0 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 20 deny any R2#
Restablecer los contadores de una lista de acceso.	R2#clear ip access-list counters en este caso no se ejecuta por que no es soportado por el Packet tracert.
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface En donde se visualiza lainformacion completa de las interfaces entre las que se destacan las ACL aplicadas en la configuración.
¿Con que 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 agregaran las traducciones a la tabla debido al modo de simulación de internet en la red. R2#show ip nat translations Pro Inside global Inside local Outside local Outside global icmp 209.165.200.225:73192.168.21.21:73 209.165.200.238:73 209.165.200.238:73 icmp 209.165.200.225:74192.168.21.21:74 209.165.200.238:74 209.165.200.238:74 icmp 209.165.200.225:75192.168.21.21:75 209.165.200.238:75 209.165.200.238:75 icmp 209.165.200.225:76192.168.21.21:76 209.165.200.238:76 209.165.200.238:76 --- 209.165.200.233 10.10.10.10 --- --- R2#
¿Qué comando se utiliza para eliminar las traducciones de NAN dinámicas?	R2# Clear show ip nat translations

Fuente: Autor

CONCLUSIONES

- Para la realización del escenario 1 planteado como el 50% del trabajo final de grado con respecto al Diplomado CISCO, fue necesario el estudio de los contenidos y unidades presentes en el curso, en donde se realizó dos actividades colaborativas con más de 30 ejercicios prácticos para prepararnos en la configuración y practica de líneas de comando para el correcto esquema de direccionamiento de una red.
- Fue interesante realizar el paso a paso en cuanto a la tabla de direccionamiento de la red con respecto al Escenario 1, para ello fue necesario plantear en papel cada una de las direcciones y mascara de subred de cada dispositivo, cabe destacar el apoyo constante del tutor, quien en cada actividad nos brindó asesoría precisa para el desarrollo del trabajo a entregar en el paso 6.
- Se llevó a cabo la configuración de cada uno de los dispositivos planteados en el Escenario 1 propuesto en el curso, para lo cual se crea la red en el simulador de Packet Tracert, conectando adecuadamente el cableado, funcionando y adecuada de acuerdo a cada uno de los lineamientos establecidos en la actividad del curso.
- Se entrega dos archivos en una carpeta en .zip, en donde debe contener el documento en Word y el simulador en extensión .pka, ya con estas especificaciones se cumple a cabalidad con la intención de la construcción y desarrollo del Escenario 1.
- Dentro de los resultados de aprendizaje del escenario 2 se encuentra la utilización de herramientas simuladas con el software de Packet tracert , identificando escenarios de tipo LAN/WAN en donde se evidencia la utilización de protocolos de internet, ospf en versión 3 y las respectivas métricas de enrutamiento.
- Se logra resolver problemas dentro de la topología de red, por lo que se hace necesario la supervisión de protocolos disponibles en la IOS, mediante el desempeño de cada uno de los dispositivos presentes en la red proporcionada por la guía de actividades, además de la utilización de NAT estático y dinámico, como también el uso de esquemas de configuración de VLANs tanto de tipo comercial y residencial respectivamente.
- No dejar a un lado el tema del protocolo DHCP el cual al momento de direccionar correctamente la tabla de enrutamiento, nos permite visualizar que se conectan entre si desde la configuración de cada uno de los protocolos requeridos para tal fin.

BIBLIOGRAFIA

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

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

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

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

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

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

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

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

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

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