DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ANGELICA RODRIGUEZ SUAREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

INGENIERÍA SISTEMAS

BOGOTÁ

2022

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ANGELICA RODRIGUEZ SUAREZ

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR ELTÍTULO DE INGENIERO *SISTEMAS*

DIRECTOR:
MSc. HECTOR JULIAN PARRA MOGOLLON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA SISTEMAS
BOGOTÁ
2022

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

BOGOTA D.C, 26 de junio de 2022

AGRADECIMIENTOS

En primer lugar, agradezco a Dios por darme las aptitudes y sabiduría en este proceso, ser mi guía y mi apoyo permitiendo en mí el tiempo, la fortaleza y las ganas de seguir saliendo adelante, enseñándome que con esfuerzo y dedicación se pueden cumplir los objetivos colocando todo en manos de él, su obra y su voluntad son maravillosos.

Mis hijos que han sido mi motor durante este proceso y por quienes no fallezco en mi camino para poder darles una mejor calidad de vida.

Por último, el tutor y director del programa que son un gran apoyo y forman un excelente equipo explicando y asesorando el estudiante para culminar sus procesos y hacerlo de la mejor manera.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Conectividad: Comunicación que establece un vínculo entre diferentes equipos por diferentes medios.

Dispositivos: Es un elemento físico como lo es una computadora, enrutadores, routers, switches, repetidores, cables, conectores etc.

Interfaz: Es conocida como la conexión o comunicación con el controlador de un equipo a una capa IP.

Red: Son varios equipos conectados entre si mediante un cable o señales que permiten comunicarse, compartir datos e información.

Seguridad: Se conoce como una capa de defensa que permite parametrizar o controlar las políticas para no tener malware dentro de los dispositivos y así mismo a su información.

Simulador de red: Es un software que permite reproducir sensaciones físicas, velocidades, percepción del entorno de cómo se comportan las computadoras o dispositivos conectados mediante una topología.

Topología de red: Es un mapa físico o lógico de una red para intercambiar datos, es la forma en la que se conectan las computadoras.

RESUMEN

Como conocemos la red ha sido parte de la evolución de la humanidad creada en 1969 donde contaba con solo 4 ordenadores, con el pasar de los años la red se implementa en muchos países que se convirtió en una red mundial donde nos permite comunicarnos de diferentes maneras. Gracias a la universidad se utiliza para este proyecto Cisco, un software que le permite a los estudiantes realizar simulaciones de redes para conocer e interactuar con diferentes dispositivos la interconexión entre ellos.

Este trabajo se realiza bajo el software de CISCO CCNP donde se construye una topología de red pequeña que permite la conmutación entre los dispositivos, configurando por medio de CLI enrutamientos de LAN-WAN, asignación de IP entre otras aplicando la electrónica.

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

ABSTRACT

As we know the network has been parto of the evolution of humanity created in 1969 where it had only 4 computers, over the years the network is implemented in many countries that became a global network where it allows us to communicate in different ways. Thanks to the university, Cisco is used for this Project, a software that allows students to perform network simulations to learn about and interact with different divices and the interconnection between them.

This work is carried out under the CISCO CCNP software where a small network topology is built that allows switching between devices, configuring LAN-WAN routing through CLI, IP assignment, among others, appying electronics.

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

INTRODUCCIÓN

El diplomado de profundización CISCO en un estudiante es lograr alcanzar los objetivos propuestos que nos entrega el diplomado CCNP fomentando el conocimiento en el área de la telecomunicación mediante estrategias como lo son las simulaciones y los dispositivos que encontramos en su herramienta de Packet Tracer.

Capacitar y formar en el estudiante su conocimiento en la red aplicando CCNP de CISCO en cada labor capaces de solucionar, planificar, verificar e implementar redes empresariales de LAN y WAN, fortaleciendo la importancia de los niveles de seguridad básicos

Dar a conocer al estudiante la capacidad que debe desarrollar de configurar y administrar los dispositivos de networking mediante el modelo OSI, la arquitectura TCP/IP, los protocolos y servicios de la capa física como lo es el soporte de comunicaciones.

El diplomado es dirigido a los técnicos, tecnólogos y profesionales que estén cursando electrónica, telecomunicaciones, sistemas o que tengan afines para una preparación en la certificación de CISCO CCNP, con diferentes módulos como el protocolo de enrutamiento, implementación de soluciones, configuración de sistemas de red en VLANS, administración y seguridad en las redes, su plataforma contiene evaluaciones que nos permiten como estudiante evaluar las capacidades adquiridas y en dado caso de no estar seguros ser corregidas.

Podremos ver una topología que permitirá la conectividad entre IPV4 e IPV6, la seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de host dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas NAT, listas de control de acceso (ACL) y

el protocolo de tiempo de red NTP servidores/cliente donde se configuro mediante los comandos en CLI

La metodología que ofrece el diplomado al estudiante es virtual que permite la facilidad como estudiante manejar el tiempo y posee con amplio contenido de los recursos necesarios para hacer posible la preparación en el desarrollo y habilidades dentro del curso.

Otro objetivo que brinda el curso y beneficia al estudiante es fortalecer los conocimientos necesarios para el diseño de redes con el fin de optimizar de manera adecuada un rendimiento en las topologías de red y protocolos de comunicación.

1. ESCENARIO 1

Figura 1. Escenario 1

Topología

Fuente propia

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

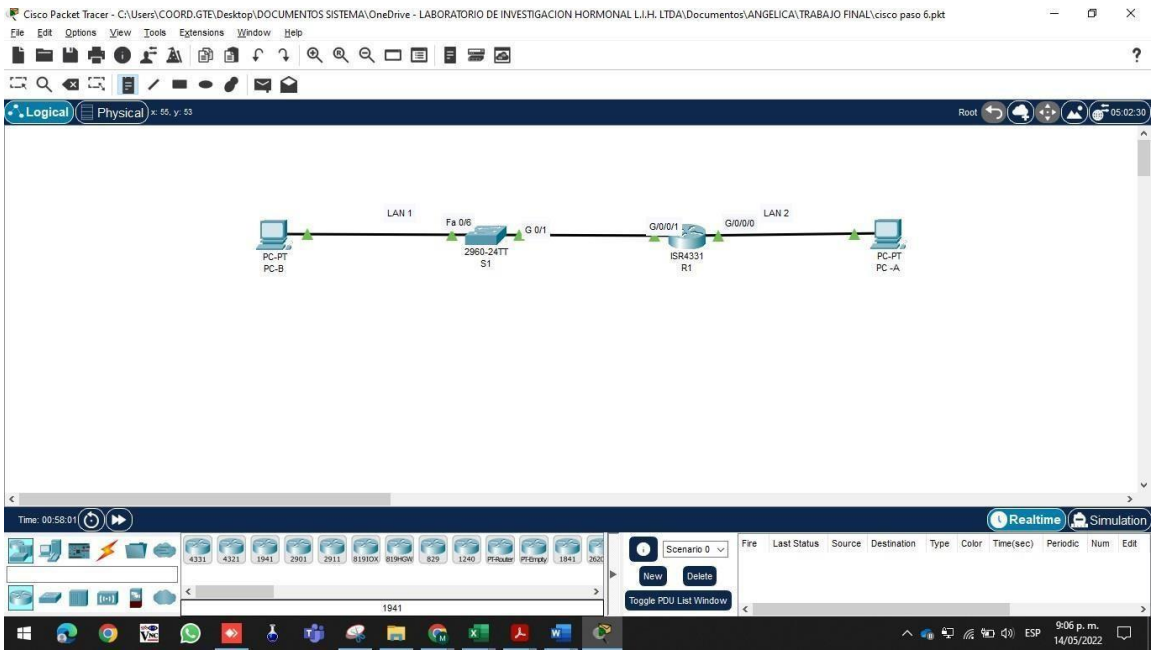
Objetivos

- Parte 1: Construir en el simulador la Red
- Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2
- Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta y los ajustes básicos de seguridad en el R1 y S1
- Parte 4: Configurar los hosts y verificar la conectividad entre los equipos

Parte 1: Construir en el simulador la Red

En el simulador se construye la red de acuerdo con la topología lógica que se plantea en la figura 1.2, cablee conforme se indica en la topología, y conecte los equipos de cómputo.

Figura 2. Simulación de escenario 1



Fuente propia

Se procede a configurar cada uno de los dispositivos solicitados. S1, R1 PCA, PCBSe asignan nombre y protocolos de comunicación entre sí.

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

Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento. Cada estudiante tomará el direccionamiento 192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula.

Tabla 1. Direccionamiento IP

Ítem	**Requerimiento**
Dirección de Red	192.168.52.0 / 25
Requerimiento de host Subred LAN 1	100
Requerimiento de host Subred LAN 2	50
R1 G 0/0/1	192.168.52.1
R1 G 0/0/0	192.168.52.129
S1 SV1.	192.168.52.2
PC-A	192.168.52.126
PC-B	192.168.52.190

Tabla 2. Descripción del Subneting obtenido

Descripción	**Subred 1**	**Subred 2**
Dirección de Subred	192.168.52.0/25	192.168.52.128 / 26
Mascara	255.255.255.128	255.255.255.192
Primera IP utilizable	192.168.52.1	192.168.52.129
Ultima IP utilizable	192.168.52.126	192.168.52.190
Dirección Broadcast	192.168.52.127	192.168.52.191
Hosts disponibles	126	62

Parte 3: Configurar los aspectos básicos de los dispositivos de la Red y los ajustes básicos de seguridad en el R1 y S1.

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

A. Tareas de configuración para el Router 1 o R1

Tabla 3. Desactivar la búsqueda DNS en R1

Comando	**Descripción**
Router>	Ingreso
Router> enable	Ingreso a modo privilegiado
Router# configure terminal	Ingreso a modo deconfiguración
Router (config)# no ip domain-lookup	Habilita nombre DNS Router
(config)# exit	Salir del modo configuración
Router# copy running-config startup-config	Guardar configuración
Router# show startup-config	Confirmación

Tabla 4. Nombrar R1

Comando	**Descripción**
Router> enable	Ingreso a modo privilegiado
Router# configure terminal	Ingreso a modo de configuración
Router(config)#hostname R1	Asignación nombre al router
R1(config)#exit	Salida del modo configuración

Tabla 5. Nombre del dominio en R1

Comando	**Descripción**
R1>enable	Ingreso a modo privilegiado
R1#configure terminal	Ingreso a modo configuración
R1(config)#ip domain-name ccna-lab.com	Configuración nombre dominio
R1(config)#exit	Salida del modo configuración

Tabla 6. Contraseña cifrada para el Modo EXCE en R1

Comando	**Descripción**
R1>enable	Ingreso modo privilegiado
R1#configure terminal	Ingreso configuración
R1(config)#enable secret ciscoenpass	Ingreso configuración mayor seguridad
R1(config)#exit	Salida modo configuración

Tabla 7. Contraseña de acceso a la consola en R1

Comando	**Descripción**
R1>enable	Ingreso a modo privilegiado
Password:	Ingreso contraseña configurada
R1#configure terminal	Ingreso a modo configuración
R1(config)#line console 0	Ingreso línea de consola
R1(config-line)#password ciscoenpass	Configurar contraseña
R1(config-line)#login	autenticación

Tabla 8. Establecer la longitud mínima para las contraseñas en R1

Comando	**Descripción**
R1>enable	Ingreso a modo privilegiado
Comando	**Descripción**
Password:	Contraseña configurada
R1#configure terminal	Ingreso terminal
R1(config)#security passwords min-length 10	Configurar longitud de contraseña

Tabla 9. Crear usuario administrativo en la base de datos local en R1

Comando	**Descripción**
R1>enable	Ingreso a modo privilegiado
Password	Contraseña configurada
R1#configure terminal	Ingreso a modo de configuración
R1(config)#username admin secret admin1pass	Configuración de usuario y contraseña

Tabla 10. Configurar inicio de sesión en las líneas VTY para que use la base de datos local en R1

Comando	**Descripción**
R1#configure terminal	Ingreso a modo de config
R1(config)#line vty 0 15	Establecer conexión Telne
R1(config-line)#login local	Configurar autenticación

Tabla 11. Configurar solo aceptando SSH en R1

Comando	**Descripción**
R1(config)#line vty 0 4	Acceso dispositivo Cisco
R1(config-line)#login local	Configurar autenticación
R1(config-line)#transport input ssh	Comunicar sedes remotas

Tabla 12. Cifrar las contraseñas de texto no cifrado en R1

Comando	**Descripción**
R1#configure terminal	Ingreso a modo configuración
R1(config)#service password-encryption	Configurar encriptacion

Tabla 13. Configure un MOTD banner en R1

Comando	**Descripción**
R1>enable	Ingreso a modo privilegiado
Password:	Contraseña configurada
R1#configure terminal	Ingreso a modo configuración
R1(config)#banner motd #acceso restringido, comuniquese con el administrador#	Configurar contenido del mensaje

Tabla 14. Configurar Interfaz G0/0/0 en R1

Comando	**Descripción**
R1>enable	Ingreso a modo privilegiado
Password:	Configuración de contraseña
R1#configure terminal	Ingreso a modo de configuración
R1(config)# interface gigabitethernet	Activación de interfaz

0/0/0	
R1(config)# description "Interface Red LAN 2"	Configurar interfaz
R1(config)# ip address 192.168.52.129 255.255.255.192	Asignación de IP y mascara subred
R1(config)# no shutdown	Guardar cambios

Tabla 15. Configurar Interfaz G0/0/1 en R1

Comando	**Descripción**
R1>enable	Ingreso a modo privilegiado
Password:	Configuración de contraseña
R1#configure terminal	Ingreso a modo configuración
R1(config)# interface gigabitethernet 0/0/1	Activar interfaz
R1(config)# description "Interface Red LAN 1"	Configurar interfaz
R1(config)# ip address 192.168.52.1 255.255.255.128	Asignación de IP y mascara subred
R1(config)# no shutdown	Guardar cambios

Tabla 16. Generar una clave de cifrado RSA en R1

.

Comando	**Descripción**
R1>enable	Ingreso a modo privilegiado
Password:	Configuración de contraseña
R1#configure terminal	Ingreso a modo configuración
R1(config)# crypto key generate rsa	Activar servidor SSH

B. Tareas de configuración para el Switch 1 o S1

Tabla 17. Desactivar la búsqueda DNS en S1

Comando	**Descripción**
Switch> enable	Ingreso a modo privilegiado
Switch#configure terminal	Ingreso a modo configuración
Switch(config)# no ip domain-lookup	Desactivar traducción
Switch#copyrunning-configstartup-config	Guardar configuración
Switch#show startup-config	para confirmar que quedo desactivada la búsqueda DNS

Tabla 18. Nombre del switch en S1

Comando	**Descripción**
Switch>enable	Ingreso a modo privilegiado
Switch#configure terminal	*Ingreso a modo deconfiguración*
Switch(config)#hostname S1	Asigno nombre de Switch

Tabla 19. Nombre del dominio en S1

Comando	**Descripción**
S1>enable	Ingreso a modo privilegiado
S1#configure terminal	Ingreso a modo de configuración
S1(config)#ipdomain-name ccna-lab.com	Configuración nombre de dominio

Tabla 20. Contraseña cifrada para el Modo EXCE en S1

Comando	**Descripción**
S1>enable	Ingreso a modo privilegiado
S1#configure terminal	Ingreso a modo configuración
S1(config)#enable secret ciscoenpass	Ingreso configuración mayor seguridad

Tabla 21. Contraseña de acceso a la consola en S1

Comando	**Descripción**
S1>enable	Ingreso a modo privilegiado

Password:	Ingreso contraseña configurada
S1#configure terminal	Ingreso a modo configuración
S1(config)#line console 0	Ingreso línea de consola
S1(config-line)#password ciscoenpass	Ingreso contraseña
S1(config-line)#login	Ingreso de autenticación

Tabla 22. Crear un usuario administrativo en la base de datos local en S1

Comando	**Descripción**
S1>enable	Ingreso a modo privilegiado
Password:	Ingreso de contraseña
S1#configure terminal	Ingreso a modo configuración
S1(config)#username admin secret admin1pass	Ingreso usuario y contraseña

Tabla 23. Configurar el inicio de sesión en las líneas VTY para que use la base de datos local en S1

Comando	**Descripción**
S1(config)#line vty 0 15	Establecer conexión Telnet
S1(config-line)#login local	Ingreso autenticación
S1(config-line)#exit	Salida del modo configuración

Tabla 24. Configurar las líneas VTY para que acepten únicamente las conexiones SSH en S1

Comando	**Descripción**
S1(config)#line vty 0 4	Acceso dispositivo a Cisco
S1(config-line)#login local	Ingreso autenticación
S1(config-line)#transport input ssh	Configuración sedes remotas
S1(config)#service password-encryption	Configuración contraseña encriptada

Tabla 25. Configurar un MOTD Banner en S1

Comando	**Descripción**
S1>enable	Ingreso a modo privilegiado
Password:	Ingreso contraseña asignada
S1#configure terminal	Ingreso a modo configuración

S1(config)#banner motd #no tiene acceso, comuniquese con el administrador#	Configurar contenido mensaje

Tabla 26. Generar una clave de cifrado RSA en S1

Comando	**Descripción**
S1>enable	Ingreso a modo privilegiado
Password:	Ingreso contraseña asignada
S1#configure terminal	Ingreso a modo configuración
S1(config)# crypto key generate rsa	Configuración global

Tabla 27. Configurar la interfaz de administración (SVI) en S1

Comando	**Descripción**
S1>enable	Ingreso a modo privilegiado
Password:	Ingreso contraseña asignada
S1#configure terminal	Ingreso a modo configuración
S1(config)#interface vlan 1	Configuración vlan
S1(config-if)#ip address 192.168.52.2 255.255.255.128	Configuración IP ymascara subred
S1(config-if)#no shutdown	Guardar configuración

Tabla 28. Configuración del Gateway predeterminado en S1

Comando	**Descripción**
S1>enable	Ingreso a modo privilegiado
Password:	Ingreso contraseña asignada
S1#configure terminal	Ingreso a modo configuración
S1(config)#ip default-Gateway 192.168.52.1	Configuración interfaz

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

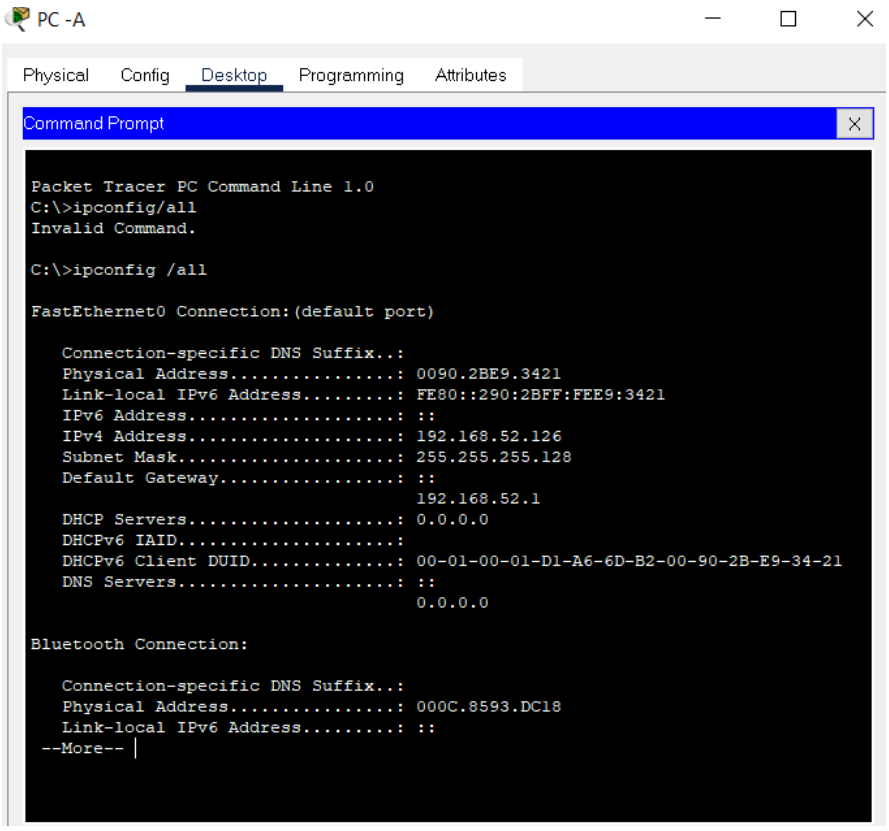
Configuración de los equipos host PC-A y PC-B conforme a la tabla de direccionamiento.

A. Configuración del equipo host PC-A

Tabla 29. Configuración de red del PC-A

Descripción	FastEthernet0
Dirección física	0090.2BE9.3421
Dirección IP	192.168.52.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.52.1

Figura 3. Configuración de red del PC-A



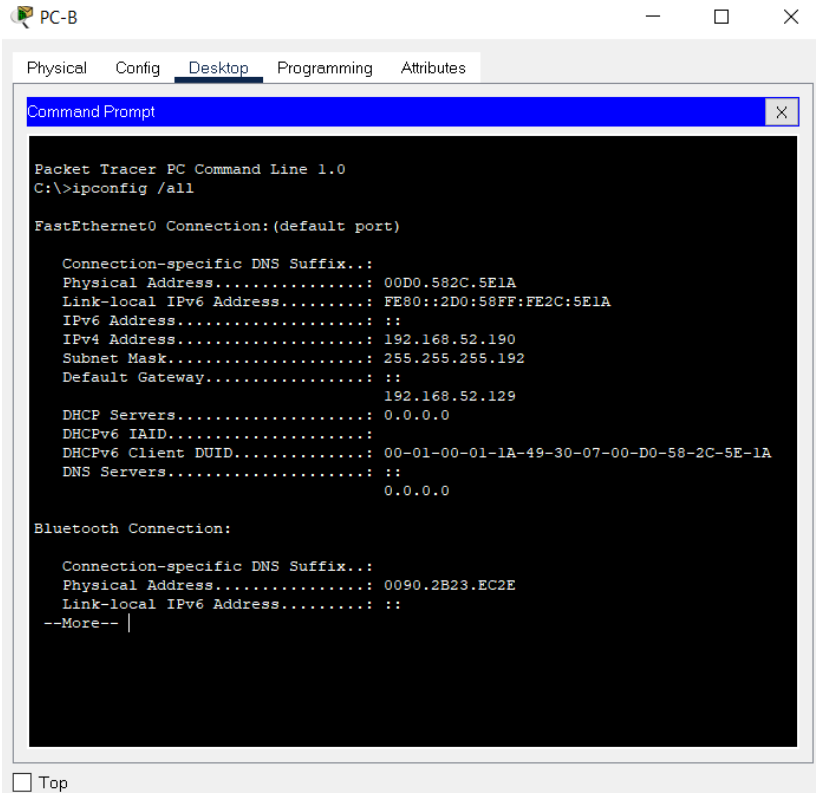
Fuente propia

B. Configuración del equipo host PC-B

Tabla 30. Configuración de red del PC-B

Descripción	FastEthernet0
Dirección física	00D0.582C.5E1A
Dirección IP	192.168.52.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.52.129

Figura 4. Configuración de red del PC-B

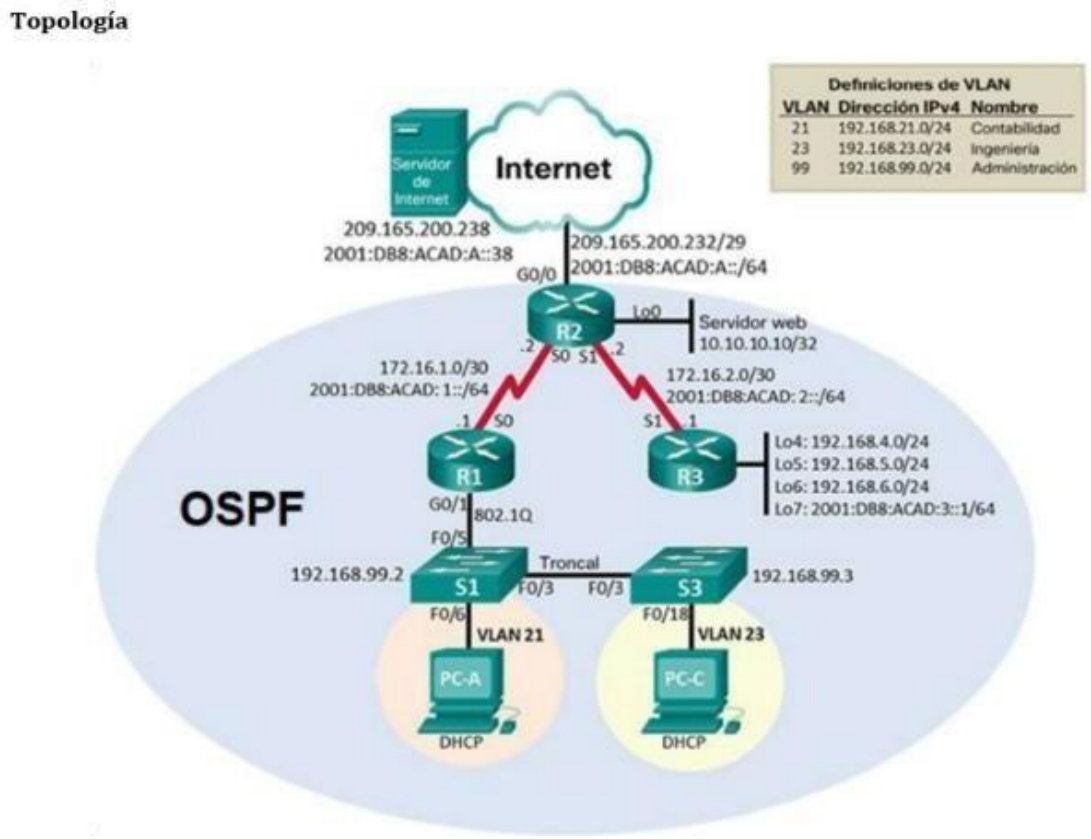


Fuente propia

2. ESCENARIO 2

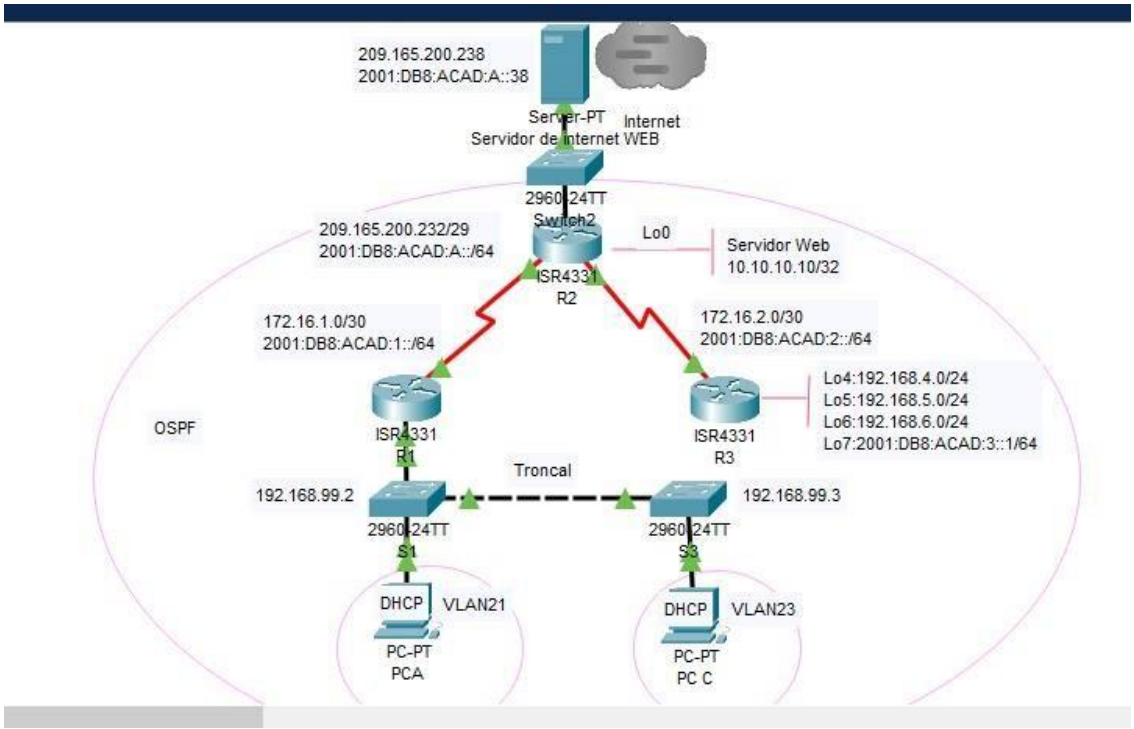
Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de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

Figura 5. Escenario 2.



Fuente Guía de Actividades Diplomado de profundización CISCO

Figura 6. Simulación de escenario 2



Fuente propia

NOTA ACLARATORIA: Para mejorar la seguridad del servidor de internet WEB se añadió un switch como conmutador entre el Router y el servidor, toda vez que la conexión directa a un Router desde un dispositivo final no es segura.

Parte 1: Inicializar los dispositivos

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

Se eliminan las configuraciones de inicio y recarga de los dispositivos.

Tabla 31. Inicialización de los Routers

Comando	**Descripción**
Router>enable	Ingreso a modo privilegiado
Router#erase startup-config	Borrado archivo config inicial
Router#reload	Recarga del Router

NOTA: Este procedimiento se realiza en los 3 Routers.

Tabla 32. Inicialización de los Switches

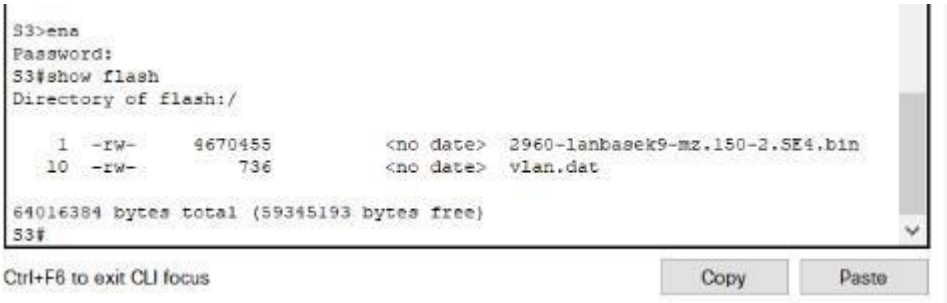
Comando	**Descripción**
Switch>enable	Ingresa a modo privilegiado
Switch#erase startup-config	Borra el archivo de configuracion inicial
Switch#delete flash:vlan.dat	Elimina la base de datos de la VLAN por default
Switch#reload	Recarga el Switch
Switch#show flash	Confirma que la base de datos no esta en la memoria flash del switch

NOTA: Este procedimiento se realiza en los 2 Switches.

Figura 7. Verificación de que la base de datos de VLAN no está en la memoria flash del Switch S1

Fuente propia

Figura 8. Verificación de que la base de datos de VLAN no está en la memoria flash del Switch S3



Fuente propia

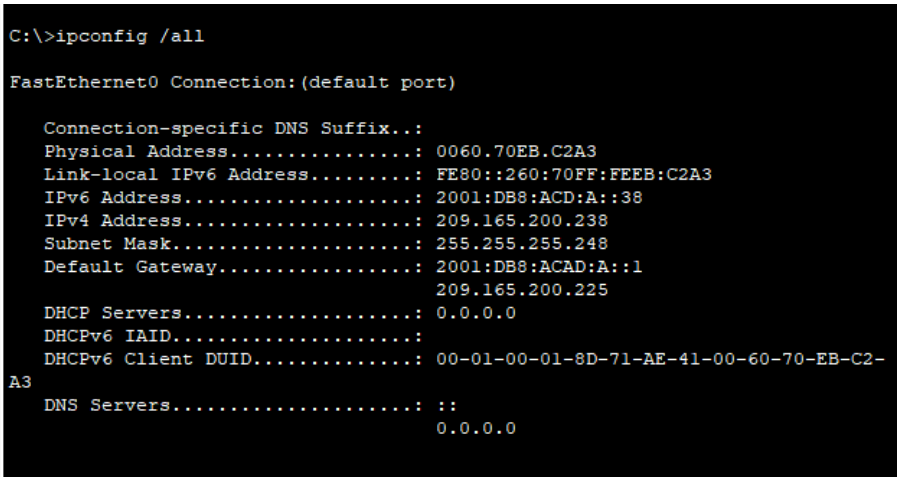
Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Tabla 33. Configuración del servidor de Internet

Descripción	**Dirección IP**
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Figura 9. Direccionamiento del servidor WEB



Fuente propia

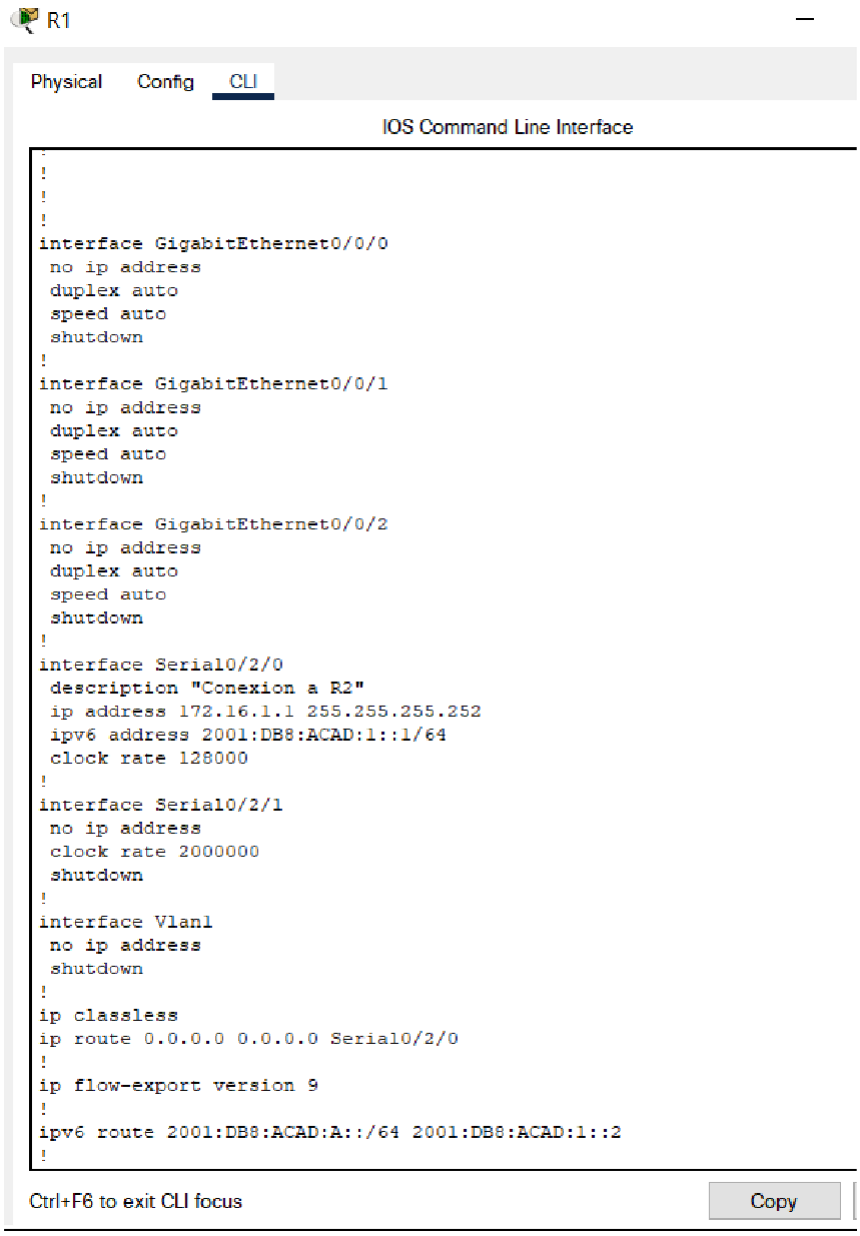
Paso 2: Configurar R1

Tabla 34. Configuración de R1

Tarea de configuración	**Comandos**
Desactivar la búsqueda DNS	R1(config)#no ip domain-lookup
Nombre del Router	R1(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto nocifrado	R1(config)#service password-encryption
Habilitar el servidor HTTP	R1(config)#ip http server
Mensaje MOTD	R1(config)#banner motd %Se prohibe el acceso no autorizado%

Interfaz S0/2/0	R1(config)#int s0/2/0	Ingreso a la interfaz serial
	R1(config-if)#description "Conexion a R2"	descripción interfaz
	R1(config-if)#ip address 172.16.1.1 255.255.255.252	Asignación de IPV4
	R1(config-if)#ipv6 address 2001:db8:acad:1::1/64	Asignación de IPV6
	R1(config-if)#clock rate 128000	Asignación frecuencia reloj
	R1(config-if)#no shutdown	Activando interfaz
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/2/0	Ruta estática ipv4
	R1(config)#ipv6 route 2001:db8:acad:a::/64 2001:db8:acad:1::2	Rutas predeterminadas ipv6

Figura 10. Configuración de R1



Fuente propia

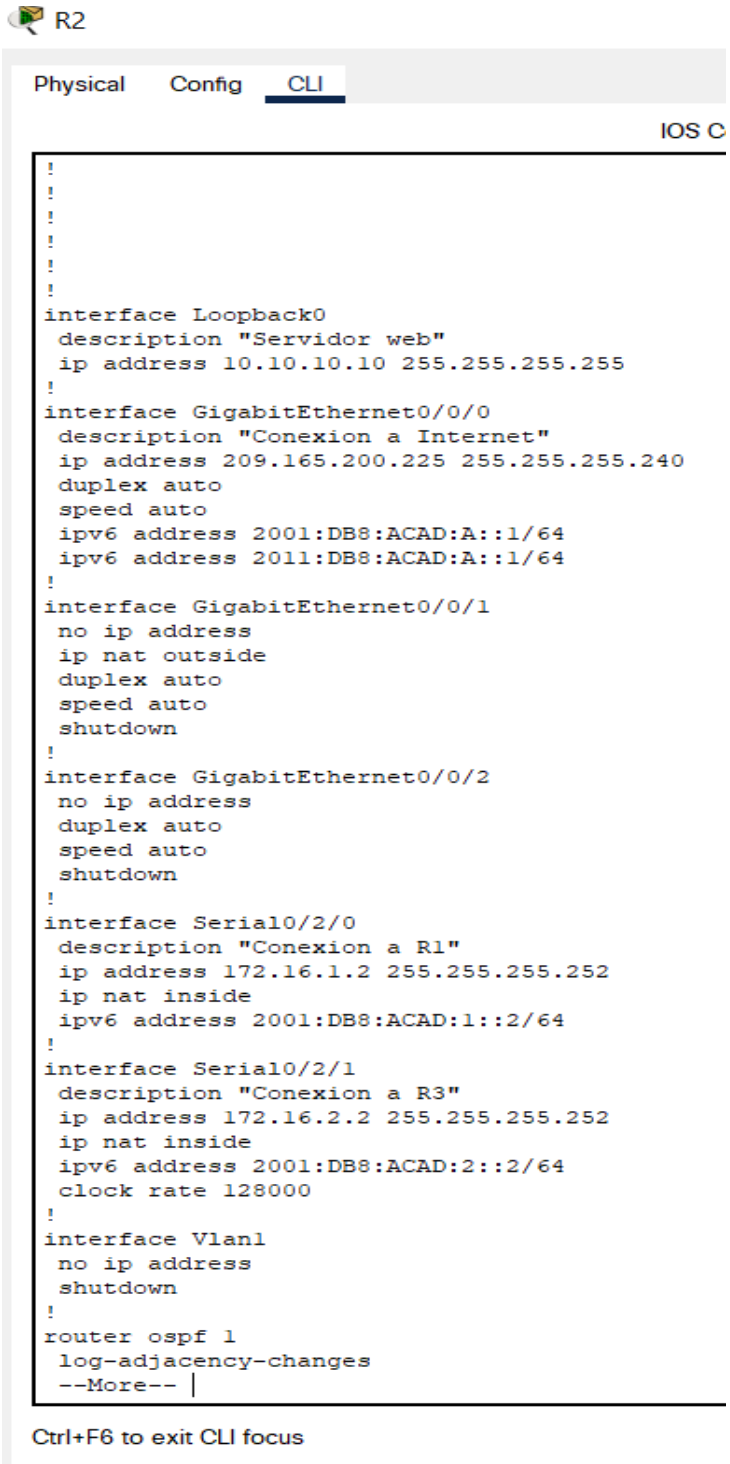
Paso 3: Configurar R2

Tabla 35. Configuración de R2

Tarea de configuración	**Comandos**	
Desactivar la búsqueda DNS	R2(config)#no ip domain-lookup	
Nombre del Router	R2(config)#hostname R2	
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class	
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login	
Contraseña de acceso Telnet	R2(config)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login	
Cifrar las contraseñas de texto nocifrado	R2(config)#service password-encryption	
Habilitar el servidor HTTP	R2(config)#ip http server	
Mensaje MOTD	R2(config)#banner motd %Se prohibe el acceso no autorizado%	
Interfaz S0/2/0	R2(config)#int s0/2/0	Ingreso a la interfaz serial
	R2(config-if)#description "Conexion a R1"	Descripción interfaz
	R2(config-if)#ip address 172.16.1.2 255.255.255.252	Asignación de IPV4
	R2(config-if)#ipv6 address 2001:db8:acad:1::2/64	Asignación de IPV6
	R2(config-if)#clock rate 128000	Asignación frecuencia reloj
	R2(config-if)#no shutdown	Activando interfaz
Interfaz S0/2/1	R2(config)#int s0/2/1	Ingreso a la interfaz serial
	R2(config-if)#description "Conexion a R3"	descripción interfaz
	R2(config-if)#ip address 172.16.1.1 255.255.255.252	Asignación de IPV4
	R2(config-if)#ipv6 address 2001:db8:acad:1::1/64	Asignación de IPV6
	R2(config-if)#no shutdown	Activando interfaz

Interfaz G0/0 (simulación de Internet)	R2(config)#int g0/0/0	Ingreso a la interfaz
	R2(config-if)#description "Conexion a Internet"	Descripción interfaz
	R2(config-if)#ip address 209.165.200.225 255.255.255.240	Asignación de IPV4
	R2(config-if)#ipv6 address 2001:db8:acad:a::1/64	Asignación de IPV6
	R2(config-if)#no shutdown	Activando interfaz
Interfaz loopback 0 (servidor web simulado)	R2(config-if)#int lo0	Ingreso a la interfaz
	R2(config-if)#description "Servidor web"	Descripción interfaz
	R2(config-if)#ip address 10.10.10.10 255.255.255.255	Asignación de IPV4
Rutas predeterminadas	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0/0	Ruta estática ipv4
	R2(config)#ipv6 route R2(config)#ipv6 route ::/0 g0/0/0	Rutas predeterminadas ipv6

Figura 11. Configuración de R2



Fuente propia

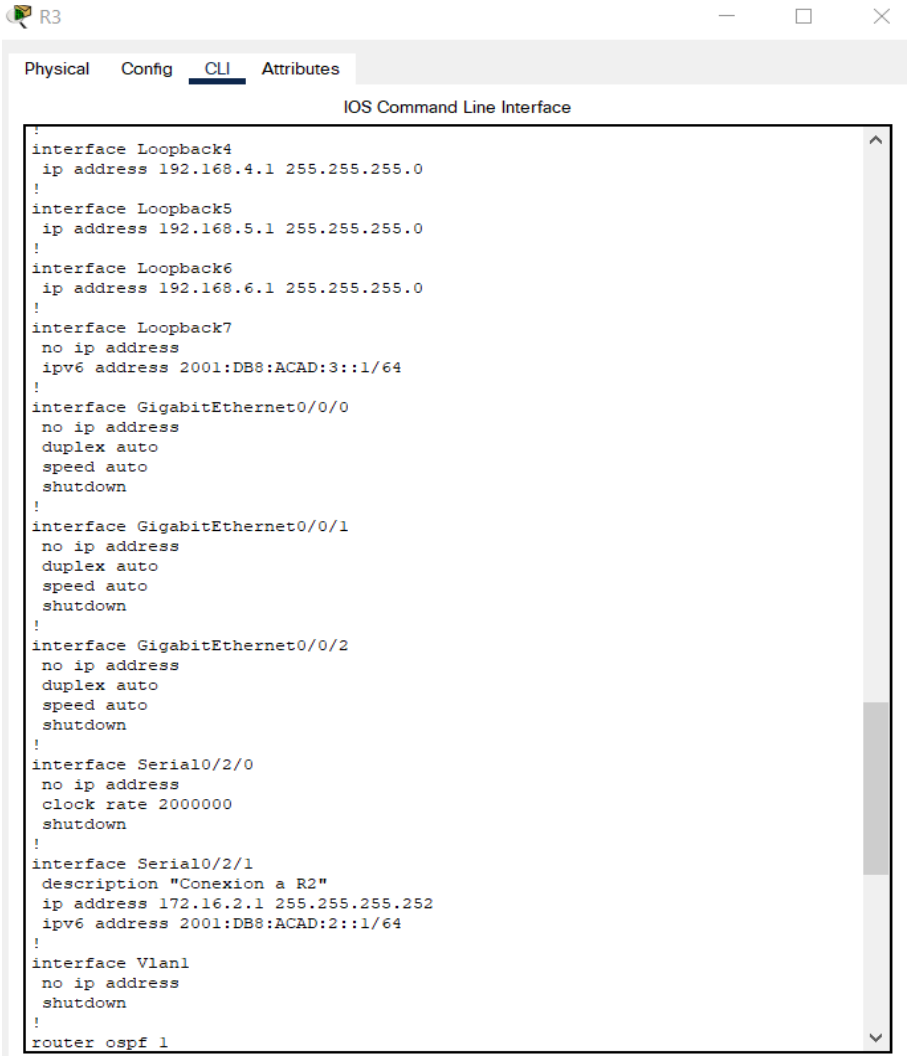
Paso 4: Configurar R3

Tabla 36. Configuración de R3

Tarea de configuración	**Comandos**	
Desactivar la búsqueda DNS	R3(config)#no ip domain-lookup	
Nombre del Router	R3(config)#hostname R3	
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class	
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login	
Contraseña de acceso Telnet	R3(config)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login	
Cifrar las contraseñas de texto nocifrado	R3(config)#service password-encryption	
Habilitar el servidor HTTP	R3(config)#ip http server	
Mensaje MOTD	R3(config)#banner motd %Se prohibe el acceso no autorizado%	
Interfaz S0/2/1	R3(config)#int s0/2/1	Ingreso a la interfaz serial
	R3(config-if)#description "Conexion a R2"	descripción interfaz
	R3(config-if)#ip address 172.16.2.1 255.255.255.252	Asignación de IPV4
	R3(config-if)#ipv6 address 2001:db8:acad:2::1/64	Asignación de IPV6
	R3(config-if)#no shutdown	Activando interfaz
Interfaz loopback 4	R3(config-if)#int lo4	Ingreso a la interfaz
	R3(config-if)#ip address 192.168.4.1 255.255.255.0	Asignación de IPV4
Interfaz loopback 5	R3(config-if)#int lo5	Ingreso a la interfaz
	R3(config-if)#ip address 192.168.5.1 255.255.255.0	Asignación de IPV4
Interfaz loopback 6	R3(config-if)#int lo6	Ingreso a la interfaz
	R3(config-if)#ip address 192.168.6.1 255.255.255.0	Asignación de IPV4

Interfaz loopback 7	R3(config-if)#int lo7	Ingreso a la interfaz
	R3(config-if)#ipv6 address 2001:db8:acad:3::1/64	Asignación de IPV6
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/2/1	Ruta estática ipv4
	R3(config)#ipv6 route R3(config)#ipv6 route ::/0 s0/2/1	Rutas predeterminadas ipv6

Figura 12. Configuración de R3



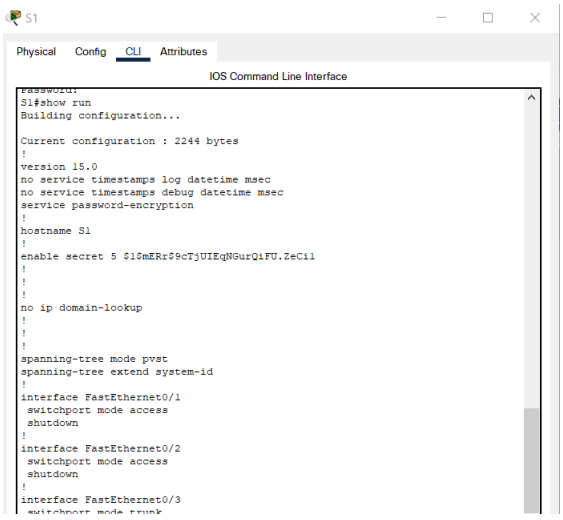
Fuente propia

Paso 5: Configurar S1

Tabla 37. Configuración básica de S1

Tarea de configuración	**Comandos**
Desactivar la búsqueda DNS	S1(config)#no ip domain-lookup
Nombre del Switch	S1(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto nocifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd %Se prohibe el acceso no autorizado%

Figura 13. Configuración básica de S1



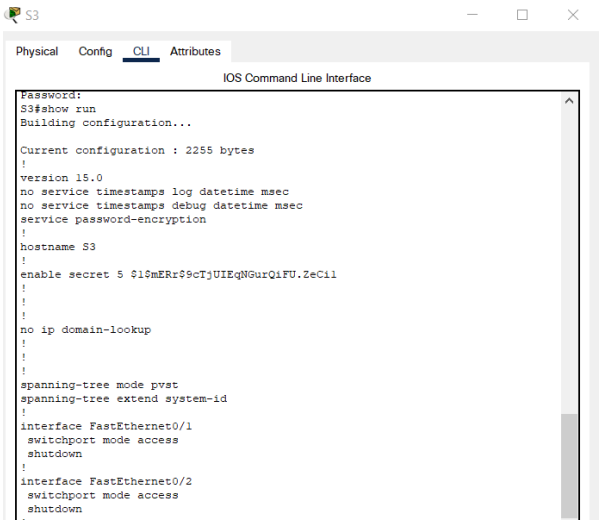
Fuente propia

Paso 6: Configurar el S3

Tabla 38. Configuración básica de S3

Tarea de configuración	**Comandos**
Desactivar la búsqueda DNS	S3(config)#no ip domain-lookup
Nombre del Switch	S3(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto nocifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd %Se prohibe el acceso no autorizado%

Figura 14. Configuración básica de S3



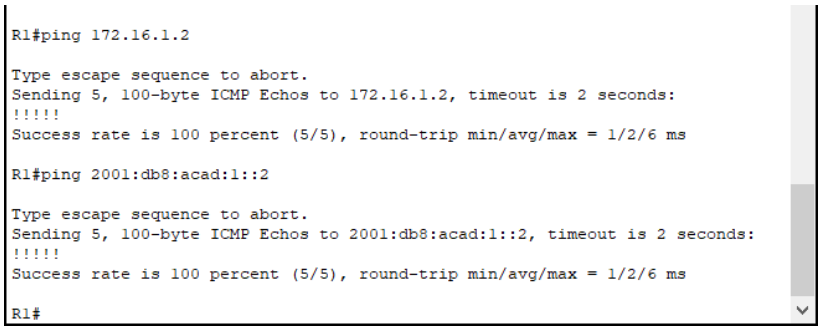
Fuente propia

Paso 7: Verificar la conectividad de la red

Tabla 39. Verificación de conectividad - Ping

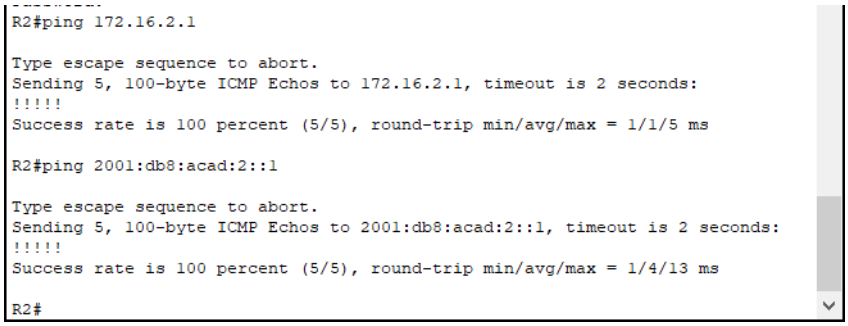
Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/2/0	172.16.1.2	Exitoso
R2	R3, S0/2/1	172.16.2.1	Exitoso
PC de Internet	Gateway predeterminado	209.165.200.233	Exitoso

Figura 15. Ping exitoso de R1 a R2 en s0/2/0



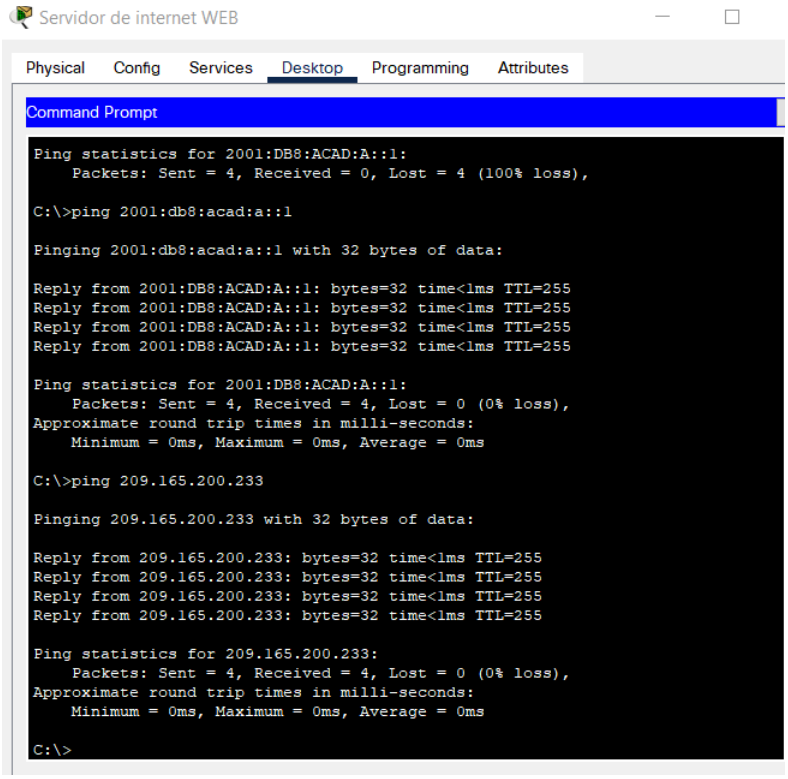
Fuente propia

Figura 16. Ping exitoso de R2 a R3 en s0/2/1.



Fuente propia

Figura 17. Ping exitoso de pc internet a Gateway predeterminado.



Fuente propia

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

Paso 1: Configurar avanzada de S1

Tabla 40. Configuración de S1 seguridad, VLAN y routing entre VLAN

Tarea de configuración	**Comandos**
Crear la base de datos de VLAN	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administración
Asignar la dirección IP de administración.	S1(config)#int vlan99 S1(config-if)#ip address 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfazF0/3	S1(config)#int fa0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfazF0/5	S1(config)#int fa0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S1(config)#interface range fa0/1-2,fa0/4,fa0/6-24,gi0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config)#int fa0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config)#interface range fa0/1/2,fa0/4,fa0/7-24,gi0/1/2 S1(config-if-range)#shutdown

Figura 18. Configuración de S1 seguridad, VLAN y routing entre VLAN

Fuente propia

Paso 2: Configurar avanzada el S3

Tabla 41. Configuración de S3 seguridad, VLAN y routing entre VLAN

Tarea de configuración	**Comandos**
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administración
Asignar la dirección IP de administración.	S3(config)#int vlan99 S3(config-if)#ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfazF0/3	S3(config)#int fa0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config)#interface range fa0/1-2,fa0/4-24,gi0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 21	S3(config)#int fa0/18 S3(config-if)#switchport access vlan 21 S3(config-if)#exit
Apagar todos los puertos sin usar	S3(config)#interface range fa0/1-2, fa0/4-17,fa0/19-24,gi0/1-2 S3(config-if-range)#shutdown

Figura 19. Configuración de S3 seguridad, VLAN y routing entre VLAN

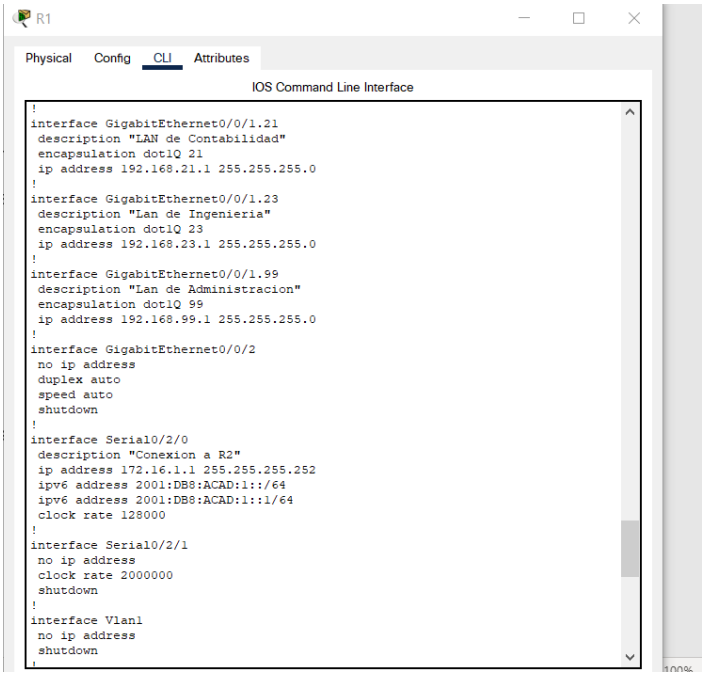
Fuente propia

Paso 3: Configurar Avanzada R1

Tabla 42. Configuración de R1 VLAN

Tarea de configuración	**Comandos**
Configurar la subinterfaz 802.1Q .21 enG0/1	R1(config)#int g0/0/1.21 R1(config-subif)#description "LAN de Contabilidad" R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 enG0/1	R1(config)#int g0/0/1.23 R1(config-subif)#description "LAN de Ingenieria" R1(config-subif)#encapsulation dot1Q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 enG0/1	R1(config)#int g0/0/1.99 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
Activar la interfaz G0/1	R1(config)#int g0/0/1 R1(config-if)#no shutdown

Figura 20. Configuración de R1 VLAN



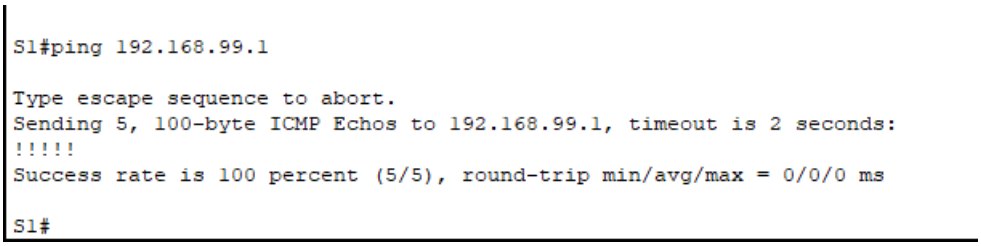
Fuente propia

Paso 4: Verificación de la conectividad de la red

Tabla 43. Verificación de la conectividad de la red

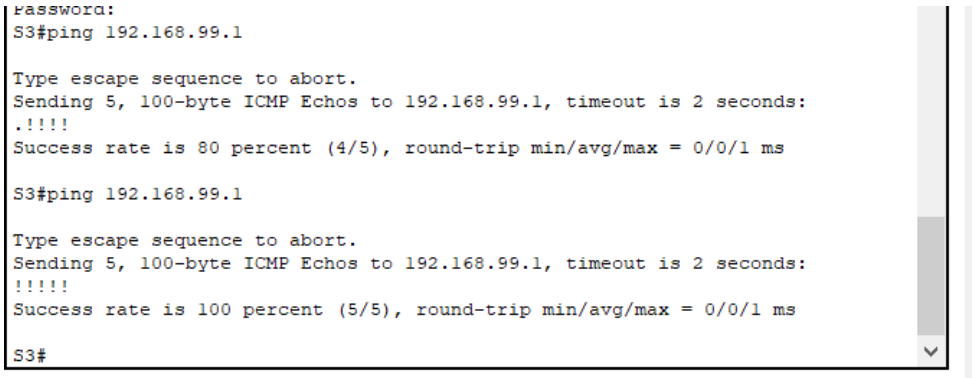
Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Exitoso
S3	R1, dirección VLAN 99	192.168.99.1	Exitoso
S1	R1, dirección VLAN 21	192.168.21.1	Exitoso
S3	R1, dirección VLAN 23	192.168.23.1	Exitoso

Figura 21. Ping exitoso de S1 a R1 en VLAN 99.



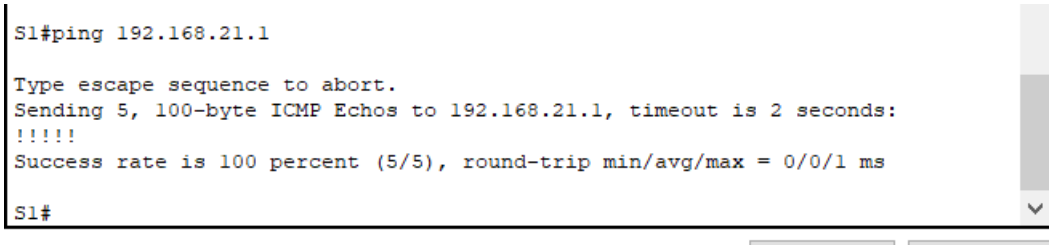
Fuente propia

Figura 22. Ping exitoso de S3 a R1 en VLAN 99.



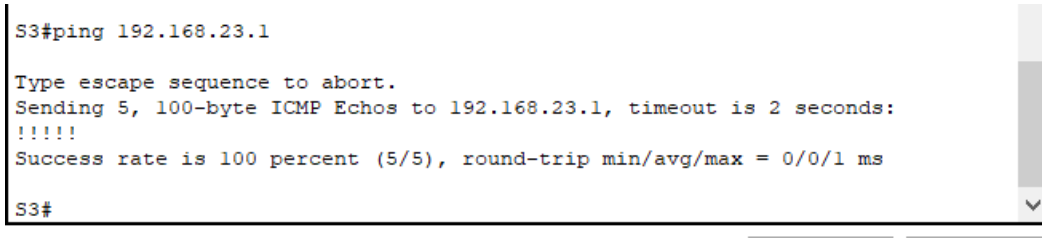
Fuente propia

Figura 23. Ping exitoso de S1 a R1 en VLAN 21.



Fuente propia

Figura 24. Ping exitoso de S3 a R1 en VLAN 23.



Fuente propia

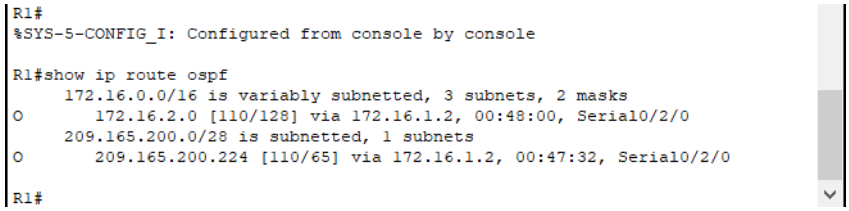
Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Tabla 44. Configuración OSPF en el R1

Tarea de configuración	**Comandos**
Configurar OSPF área 0	R1(config)#router ospf 1
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config)#router ospf 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 automática	En Ospf no hay sumarización automática.

Figura 25 – Configuración de OSPF en R1.



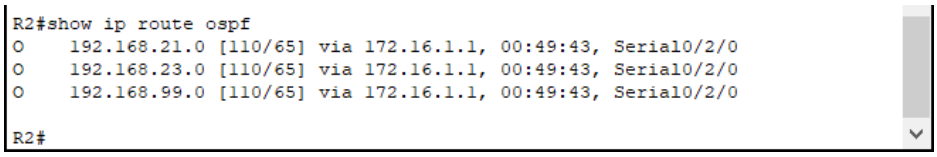
Fuente propia

Paso 2: Configurar OSPF en el R2

Tabla 45. Configuración OSPF en el R2

Tarea de configuración	**Comandos**
Configurar OSPF área 0	R2(config)#router ospf 1
Anunciar las redes conectadas directamente	R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 209.165.200.232 0.0.0.255 area 0.
Establecer la interfaz LAN (loopback) como pasiva	R2(config)#router ospf 1 R2(config-router)#passive-interface lo0
Desactive la sumarización automática	En Ospf no hay sumarización automática.

Figura 26. Configuración de OSPF en R2.



Fuente propia

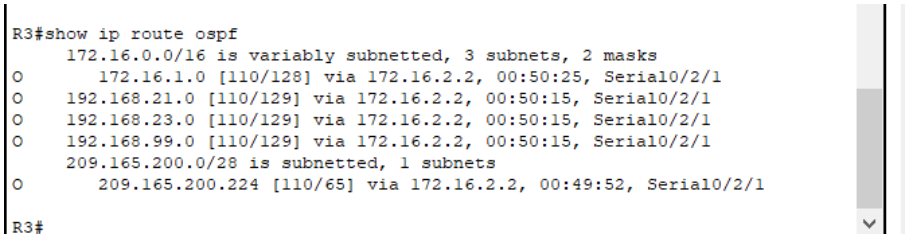
Paso 3: Configurar OSPFv3 en el R3

Tabla 46. Configuración OSPF en el R3

Tarea de configuración	**Comandos**
Configurar OSPF área 0	R3(config)#router ospf 1
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como	R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5

pasivas	R3(config-router)#passive-interface lo6 R3(config-router)#passive-interface lo7
Desactive la sumarización automática	En Ospf no hay sumarización automática.

Figura 27. Configuración de OSPF en R3



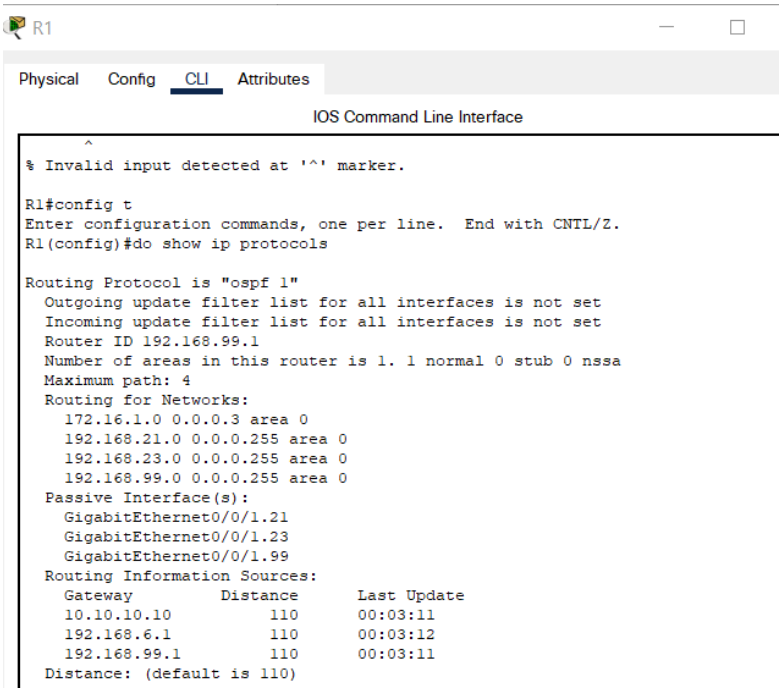
Fuente propia

Paso 4: Verificar la información de OSPF

Tabla 47. Verificación de OSPF

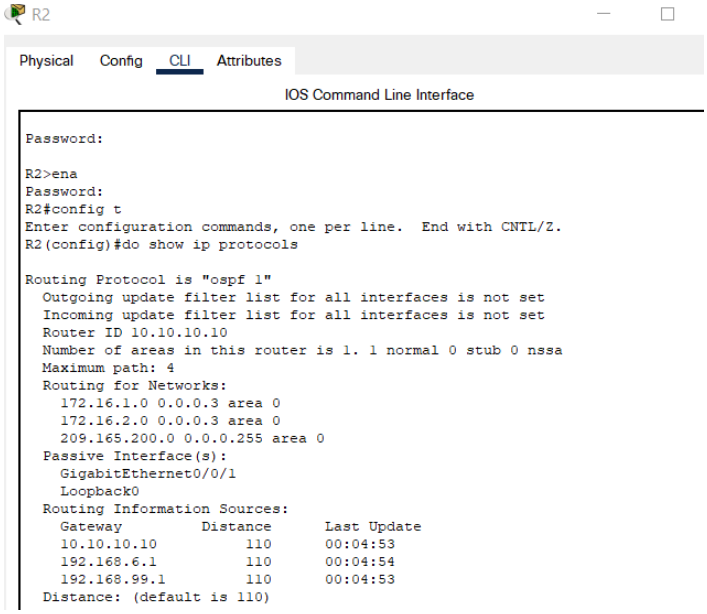
Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Con el comando do show ip protocols
¿Qué comando muestra solo las rutas OSPF?	Con el comando show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Con el comando show ip ospf interface, se puede ver una lista detallada de la configuración en ejecución del protocolo OSPF en el Router.

Figura 28. Comando do show ip protocols en R1.



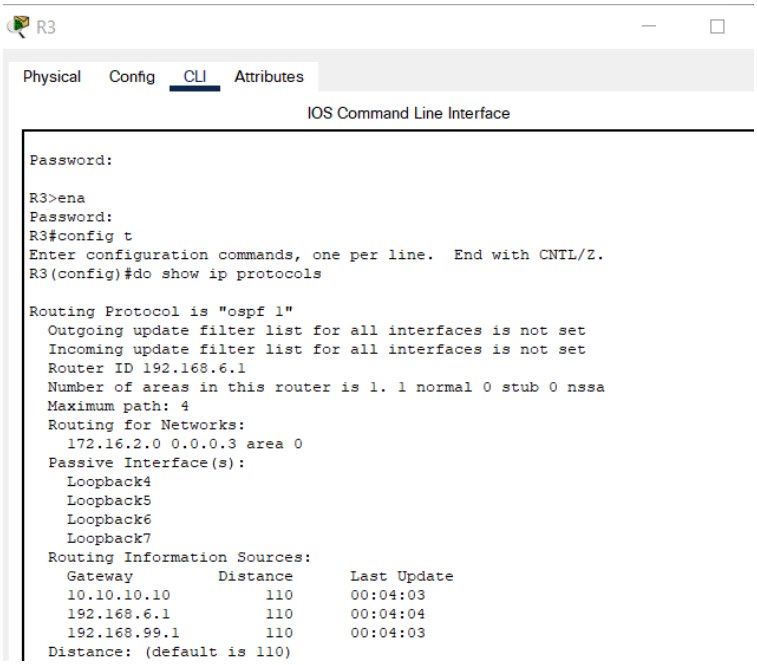
Fuente propia

Figura 29. Comando do show ip protocols en R2



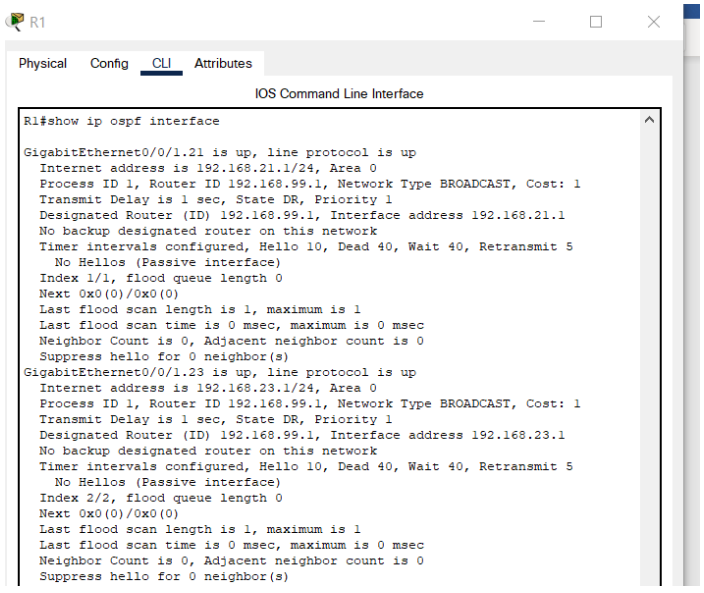
Fuente propia

Figura 30. Comando do show ip protocols en R3



Fuente propia

Figura 31. Comando show ip ospf interface en R1

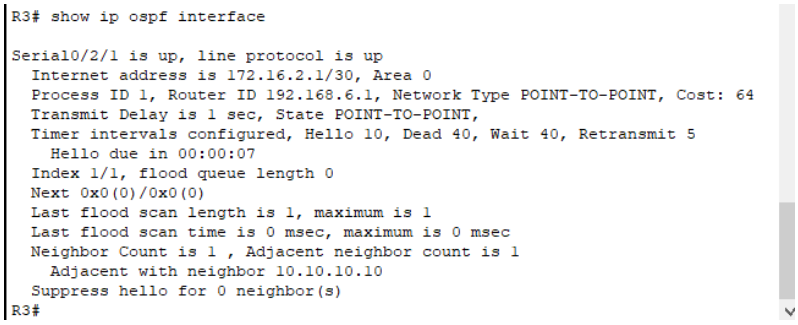


Fuente propia

Figura 32. Comando show ip ospf interface en R2

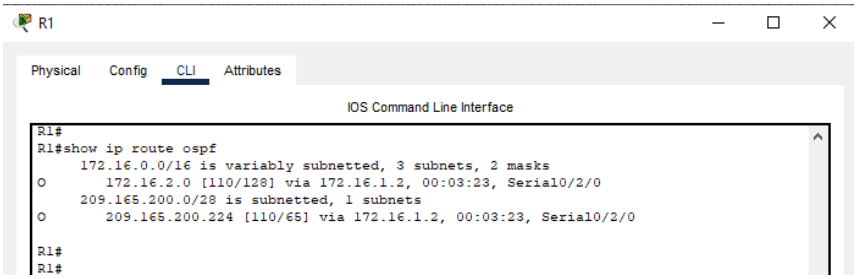
Fuente propia

Figura 33. Comando *show* ip ospf interface en R3



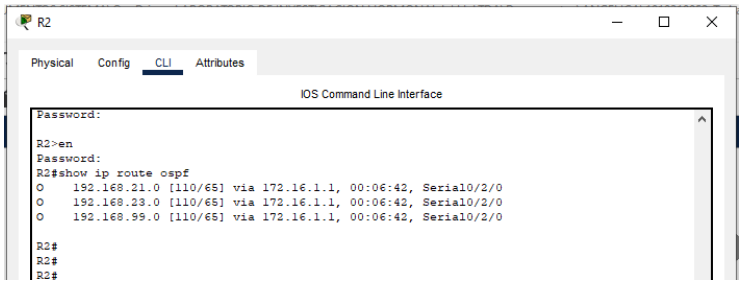
Fuente propia

Figura 34. Comando show ip route ospf en R1



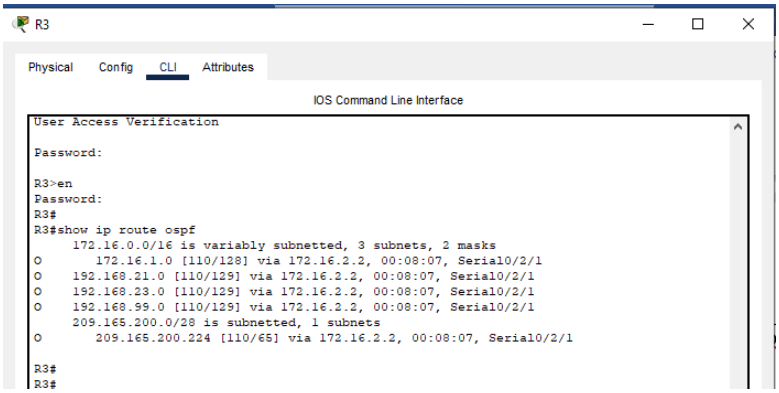
Fuente propia

Figura 35. Comando show ip route ospf en R2



Fuente propia

Figura 36. Comando show ip route ospf en R3



Fuente propia

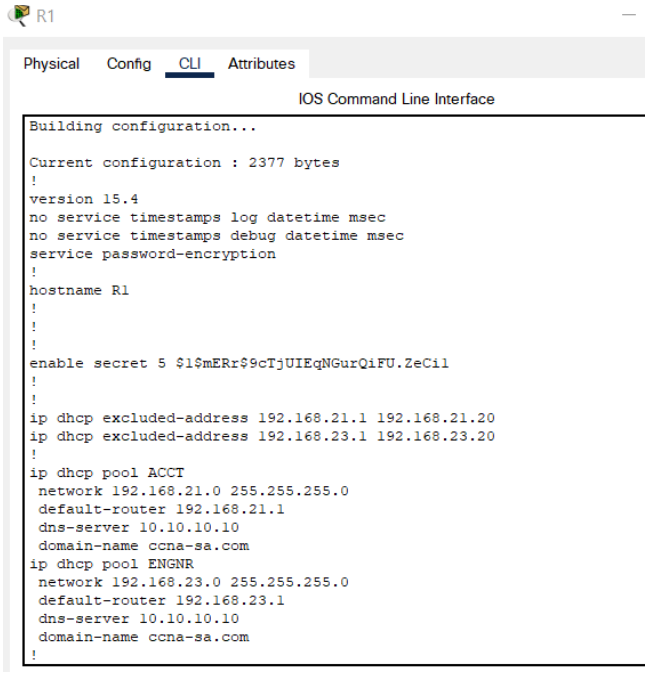
Parte 5: Implementar DHCP y NAT para IPv4

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

Tabla 48. Configuración R1 servidor de DHCP VLAN 21 y 23

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

Figura 37. Configuración DHCP en R1



Fuente propia

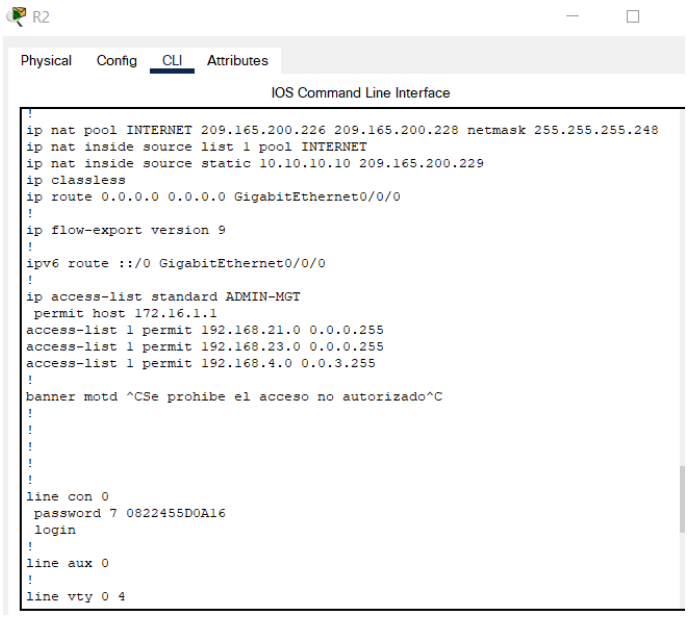
Paso 2: Configurar la NAT estática y dinámica en el R2

Tabla 49. Configuración de NAT estática y dinámica en el R2

Tarea de configuración	**Comandos**
Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http secure-server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	Solo funciona en equipos reales
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#int g0/0/1 R2(config-if)#ip nat outside Interfaz externa

	R2(config)#int s0/2/0 R2(config-if)#ip nat inside Interfaz interna R2(config-if)#int s0/2/1 R2(config-if)#ip nat inside Interfaz interna R2(config-if)#exit
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.226 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Figura 38. Configuración NAT estática y dinámica en R2



Fuente propia

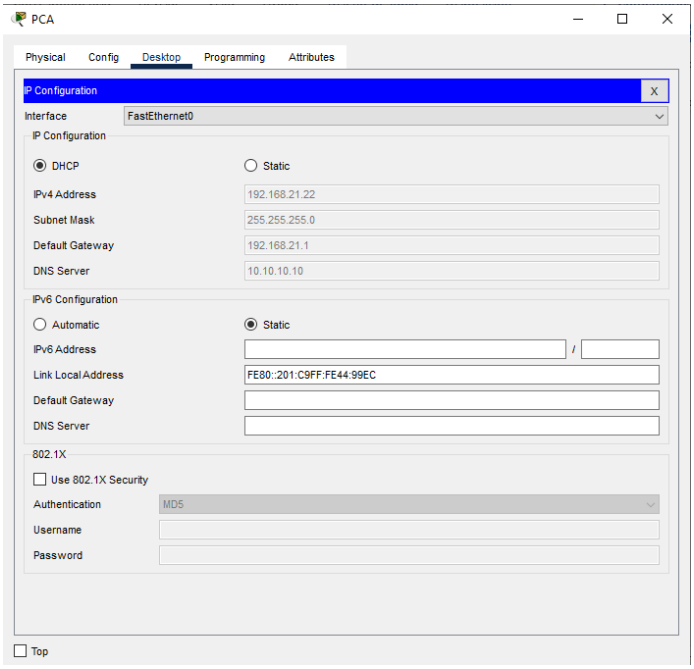
Paso 3: Verificar el protocolo DHCP y la NAT estática

Tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta.

Tabla 50. Pruebas de protocolo DHCP y la NAT estática

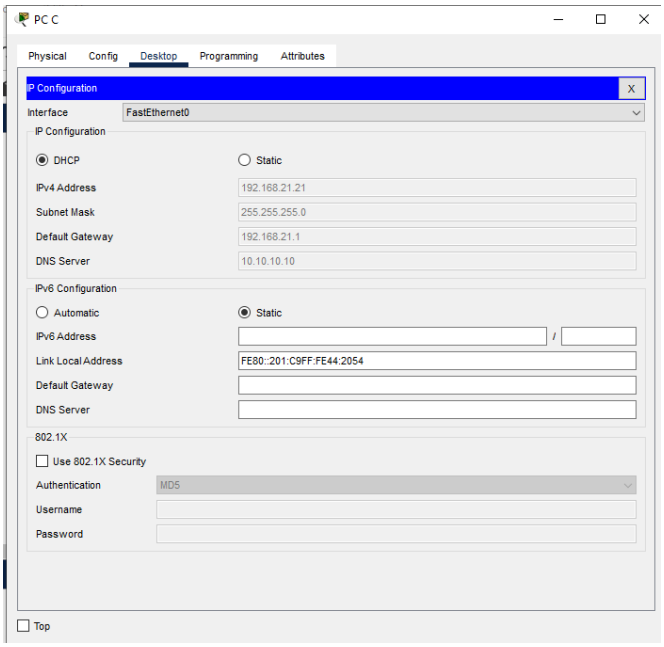
Prueba	Resultado
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-A pueda hacer ping a la PC-C	Exitoso
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	Exitoso para el acceso WEB, la autenticación de usuario local solo funciona en equipos reales

Figura 39. PC-A adquiere IP del servidor de DHCP



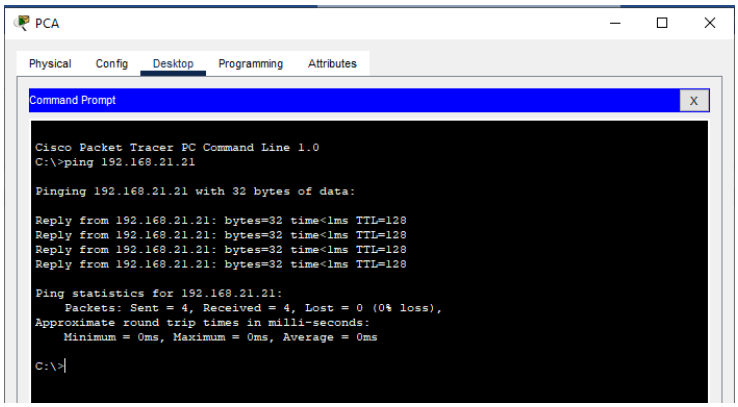
Fuente propia

Figura 40. PC-C adquiere IP del servidor de DHCP



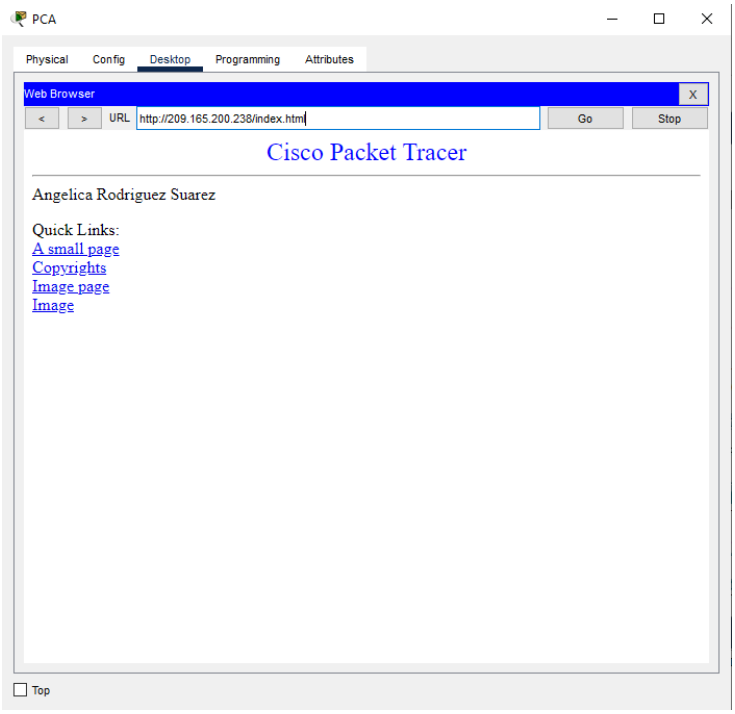
Fuente propia

Figura 41. Ping de PC-A a PC-C



Fuente propia

Figura 42. Acceso WEB



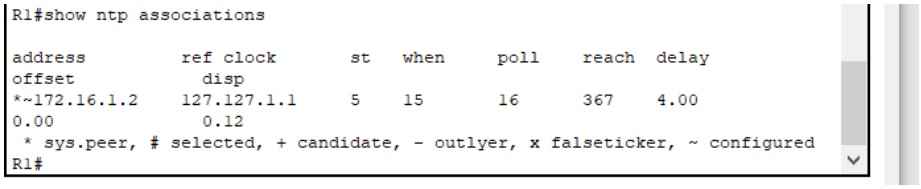
Fuente propia

Parte 6: Configurar NTP

Tabla 51. Configuración NTP

Tarea de configuración	**Comandos**
Ajuste la fecha y hora en R2.	R2#clock set 9:00:00 march 5 2016
Configure R2 como un maestro NTP	R2(config)#ntp master 5
Configurar R1 como un cliente NTP	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1	R1#show ntp associations

Figura 43. Configuración de NTP en R1



Fuente propia

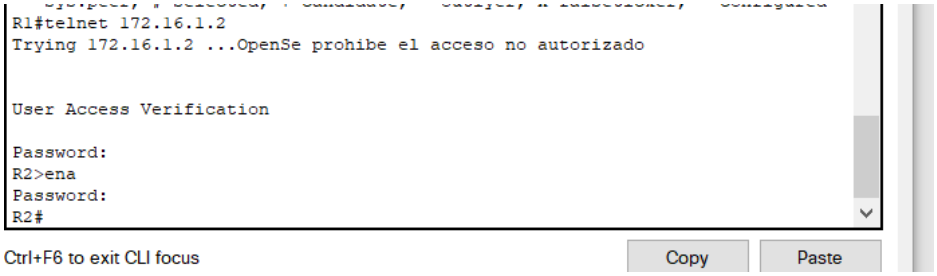
Parte 7: Configurar y verificar las listas de control deacceso (ACL)

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

Tabla 52. Restricción de acceso a las líneas VTY en el R2

Tarea de configuración	**Comandos**
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#end
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2

Figura 44. Ingreso por telnet de R1 a R2



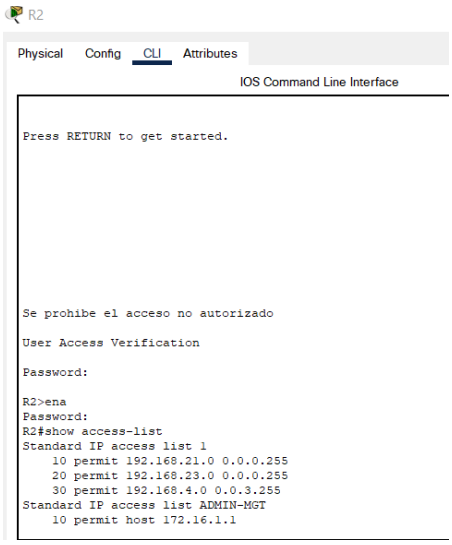
Fuente propia

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

Tabla 53. Comandos para Lista de acceso ACL y NAT

Descripción del comando	**Comando**
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Show access list
Restablecer los contadores de una listade acceso	Clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Show ip interface
¿Con qué comando se muestran las traducciones NAT?	Show ip nat translations
¿Qué comando se utiliza para eliminarlas traducciones de NAT dinámicas?	Clear ip nat translation

Figura 45. Listas de acceso en router R2.

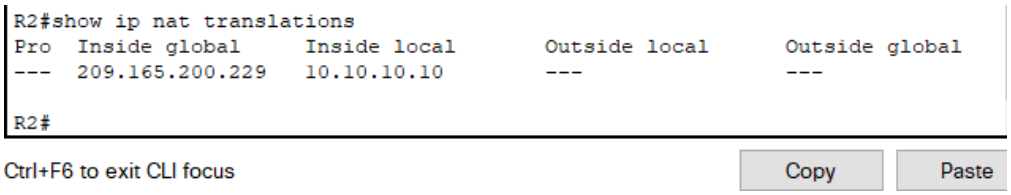


Fuente propia

Figura 46. Interfaz IP de router R2.

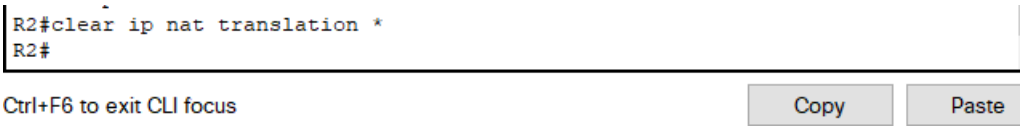
Fuente propia

Figura 47. NAT estáticas de servidor web en router 2.



Fuente propia

Figura 48. Borrando entradas dinámicas.



Fuente propia

CONCLUSIONES

Se construye la topología de red indicada en el escenario 1 mediante el software de packet tracer utilizando los dispositivos como lo es el Switch, Router, cableado y 2 PC diseñando un direccionamiento IPV4 para las redes LAN propuestas.

Se desarrolla el direccionamiento IPV4 para la LAN1 y LAN2 por medio de subneting con la cantidad requerida de hosts mediante la tabla de direccionamiento y según los requerimientos.
Cumpliendo con estos dos objetivos se realiza la configuración y ajustes básicos de seguridad en el R1 y S1, así mismo se configura el host y se verifica entre los equipos.

En el escenario 2 se realizó una configuración de una red en donde inicialmente se realizó una configuración inicial a los routers y switches pertenecientes al esquema, después de esto se le implemente seguridad en cada uno de ellos, además de esto se estableció el routing entre VLANs.

En la segunda parte del escenario 2 se empleó el protocolo de routing dinámico OSPF, además de esto se empleó DHCP y NAT, en donde por último se configuro NTP para dar por terminado el escenario.

BIBLIOGRÁFIA

CISCO. (2019). Conceptos de Routing. Principios de Enrutamiento y Conmutación. http://vapenik.s.cnl.sk/pcsiete/CCNA2/01_Routing_Concept.pdf

CISCO. (2019). Routing Estático. Principios de Enrutamiento y Conmutación. http://vapenik.s.cnl.sk/pcsiete/CCNA2/02_Static_R outing.pdf

CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. http://vapenik.s.cnl.sk/pcsiete/CCNA2/10_Discover_Manage_Maintenance.pdf

CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. http://vapenik.s.cnl.sk/pcsiete/CCNA2/09_NAT_for_IPv4.pdf

CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. http://www.ie.tec.ac.cr/einteriano/cisco/ccna4/Presentaciones/CCNA_Exploration_Accessing_the_WAN_-_Cap5.pdf

CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. http://vapenik.s.cnl.sk/pcsiete/CCNA2/08_DHCP.pdf

UNAD (2017). Configuración de Switches y Routers [OVA]. https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC