

SOLUCION DE DOS ESTUDIOS DE CASO BAJO EL USO DE LA TECNOLOGIA  
CISCO

MANUEL ALEXANDER PALACIOS MOSQUEA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA. ECBTI  
INGENIERIA DE TELECOMUNICACIONES  
MEDELLIN - ANTIOQUIA  
2020

SOLUCION DE DOS ESTUDIOS DE CASO BAJO EL USO DE LA TECNOLOGIA  
CISCO

MANUEL ALEXANDER PALACIOS MOSQUEA

Trabajo de grado para optar al título de grado de  
INGENIERO DE TELECOMUNICACIONES

Tutor  
Nilson Alberto Ferreira Manzanares

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA. ECBTI  
INGENIERIA DE TELECOMUNICACIONES  
MEDELLIN - ANTIOQUIA  
2020

NOTA DE ACEPTACION

---

---

---

---

---

---

---

---

---

---

---

Firma del Presidente del Jurado

---

Firma del Jurado

---

Firma del Jurado

Medellín, 15 de mayo 2020

## DEDICATORIA

Dedico este título a Dios a mi familia, en especial a tres personas muy valiosas en mi vida, mi madre Mary Luz Mosquera Jordán, mi abuela Maria Anuncia Mosquera Jordán que en paz descansa y a Luz Mila Flórez mi amiga

## AGRADECIMIENTOS

Quiero darle gracias a Dios por medio de nuestro Señor Jesús, a mi familia en especial a mi madre Mary Luz Mosquera Jordán, mis hermanos Salome Palacios, Peterson Agualimpia, Jonathan Camilo Mosquera, a profesores y compañeros de la UNAD por todo su apoyo durante estos años de formación académica, por todo el apoyo y acompañamiento brindado.

## TABLA DE CONTENIDO

	Pag
LISTA DE TABLAS .....	9
GLOSARIO .....	11
RESUMEN .....	13
ABSTRACT .....	15
INTRODUCCIÓN .....	17
JUSTIFICACION .....	18
OBJETIVOS .....	19
OBJETIVOS GENERAL .....	19
OBJETIVOS ESPECIFICOS .....	19
DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES .....	20
ESCENARIO 1 .....	20
DESARROLLO DEL ESCENARIO 1 .....	21
PARTE 1: INICIALIZAR DISPOSITIVOS .....	21
PASO 1: INICIALIZAR Y VOLVER A CARGAR LOS ROUTERS Y LOS SWITCHES .....	21
PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS .....	22
PASO 1: CONFIGURAR LA COMPUTADORA DE INTERNET .....	22
PASO 2: CONFIGURAR R1 .....	23
PASO 3: CONFIGURAR R2 .....	25
PASO 4: CONFIGURAR R3 .....	28
PASO 5: CONFIGURAR S1 .....	31
PASO 6: CONFIGURAR EL S3 .....	32
PASO 7: VERIFICAR LA CONECTIVIDAD DE LA RED .....	33
PARTE 3: CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN .....	35
PASO 1: CONFIGURAR S1 .....	35
PASO 2: CONFIGURAR EL S3 .....	37
PASO 3: CONFIGURAR R1 .....	39
PASO 4: VERIFICAR LA CONECTIVIDAD DE LA RED .....	41
PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPV2 ...	42

PASO 1: CONFIGURAR RIPV2 EN EL R1 .....	43
PASO 2: CONFIGURAR RIPV2 EN EL R2 .....	44
PASO 3: CONFIGURAR RIPV2 EN EL.....	44
PASO 4: VERIFICAR LA INFORMACIÓN DE RIP .....	45
PARTE 5: IMPLEMENTAR DHCP Y NAT PARA IPV4 .....	46
PASO 1: CONFIGURAR EL R1 COMO SERVIDOR DE DHCP PARA LAS VLAN 21 Y 23.....	46
PASO 2: CONFIGURAR LA NAT ESTÁTICA Y DINÁMICA EN EL R2.....	48
PASO 3: VERIFICAR EL PROTOCOLO DHCP Y LA NAT ESTÁTICA.....	49
PARTE 6: CONFIGURAR NTP .....	52
PARTE 7: CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL.....	53
PASO 1 PARTE 7: RESTRINGIR EL ACCESO A LAS LÍNEAS VTY EN EL R2.....	54
PASO 2: INTRODUCIR EL COMANDO DE CLI ADECUADO QUE SE NECESITA PARA MOSTRAR LO SIGUIENTE .....	54
DESARROLLO DEL ESCENARIO 2.....	56
PARTE 1: CONFIGURAR LA TOPOLOGÍA DE RED, DE ACUERDO CON LAS SIGUIENTES ESPECIFICACIONES .....	60
PARTE 1: CONFIGURACIÓN DEL ENRUTAMIENTO .....	60
A. CONFIGURAR PROTOCOLO OSPF V2 EN LA RED.....	60
B. CONFIGURAR RUTA POR DEFECTO AL ISP PARA LOS ROUTERS BOGOTA1 Y MEDELLIN1.....	68
C. RUTA ESTATICA DEL ISP HACIA LA REDES BOGOTA Y MEDELLIN 68	
E.....	69
PARTE 2: TABLA DE ENRUTAMIENTO. ....	69
A. TABLA DE ENRUTAMIENTO DE LA RED.....	69
B. BALANCEO DE CARGA DE LA RED .....	70
C. OBSÉRVAR LOS ROUTERS BOGOTÁ1 Y MEDELLÍN1.....	72
D. VERIFICAR LOS ROUTERS MEDELLÍN3 Y BOGOTÁ2 .....	72
LAS TABLAS RUTA POR DEFECTO ROUTERS RESTANTES .....	73
VER RUTAS ESTATICAS DEL ISP .....	74
PARTE 3: DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO OSPF.....	74

A. PROPAGACIÓN DEL PROTOCOLO OSPF EN LAS INTERFACES QUE NO LO NECESITEN .....	74
PARTE 4: VERIFICACIÓN DEL PROTOCOLO OSPF .....	76
A. VERIFICAR Y DOCUMENTAR LAS OPCIONES DE ENRUTAMIENTO OSPF EN LA RED.....	76
B. VERIFICAR Y DOCUMENTAR LA BASE DE DATOS DE OSPF DE CADA ROUTER .....	77
PARTE 5: CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP .....	79
A. AUTENTICACIÓN PAT ENLACE MEDELIN .....	79
B. CONFIGURAR CON AUTENTICACIÓN CHAT BOGOTA1 .....	80
PARTE 6: CONFIGURACIÓN DE PAT.....	81
A. ACTIVAR NAT EN CADA EQUIPO DE SALIDA BOGOTÁ1 Y MEDELLÍN1 .....	81
B. CONFIGURAR EL NAT EN EL ROUTER MEDELLÍN1.....	81
C. CONFIGURAR EL NAT EN EL ROUTER BOGOTÁ1 .....	82
PARTE 7: CONFIGURACIÓN DEL SERVICIO DHCP.....	83
A. CONFIGURAR ROUTER MEDELLÍN2 Y MEDELLÍN3, MEDELLÍN2 SERVIDOR DHCP PARA AMBAS REDES LAN.....	83
B. EL ROUTER MEDELLÍN3 DEBERÁ HABILITAR EL PASO DE LOS MENSAJES BROADCAST HACIA LA IP DEL ROUTER MEDELLÍN2 .....	84
C. CONFIGURAR BOGOTÁ2 Y BOGOTÁ3, BOGOTA2 SERVIDOR DHCP PARA LA LAN .....	85
D. CONFIGURE BOGOTÁ1 PARA QUE HABILITE EL PASO DE LOS DE BROADCAST HACIA BOGOTÁ2.....	86
CONCLUSIONES .....	87
REFERENCIA BIBLIOGRÁFICA .....	88



## LISTA DE TABLAS

	Pag
Tabla 1. Paso 1 - Parte 1: Inicializar y volver a cargar los routers y los switches ..	21
Tabla 2. Paso 1 - Parte 2: Configurar la computadora de Internet.....	22
Tabla 3. Paso 2 - Parte 2: Configurar R1 .....	23
Tabla 4. Paso 3 - Parte 2: Configurar R2 .....	25
Tabla 5. Paso 4 - Parte 2: Configurar R2 .....	29
Tabla 6. Paso 5 – Parte 2 Configurar S1 .....	31
Tabla 7. Paso 6 – Parte 2: Configurar S3 .....	32
Tabla 8. Paso 7 – Parte 2: Verificar la conectividad de la red .....	33
Tabla 9. Paso 1 – Parte 3 .....	35
Tabla 10. Paso 2 – Parte 3: Configurar S3 .....	38
Tabla 11. Paso 3 – Parte 3: Configurar R1 .....	39
Tabla 12. Paso 4 - Parte 3: Verificar la conectividad de la red.....	41
Tabla 13. Paso 1 - Parte 4: Configurar RIPv2 en el R1.....	43
Tabla 14. Paso 2 - Parte 4: Configurar RIPv2 en el R2.....	44
Tabla 15. Paso 3 - Parte 4: Configuración RIPv2 en el R2 .....	44
Tabla 16. Paso 4 - Parte 4: Verificar la información de RIP .....	45
Tabla 17. Paso 1 - Parte 5: Configurar R1 como servidor de DHCP para las VLAN 21 y 23 .....	47
Tabla 18. Paso 2 - Parte 5: Configurar la NAT estática y dinámica en el R2	48
Tabla 19. Paso 3 - Parte 5: Verificar el protocolo DHCP y la NAT estática.....	49
Tabla 20. Parte 6: Configurar NTP .....	52
Tabla 21. Paso 1: Restringir el acceso a las líneas VTY en el R2.....	54
Tabla 22. Paso 2 - Parte 7: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente.....	54
Tabla 23. Enrutamiento .....	69
Tabla 24. De interfaces activas.....	75

## LISTA DE FIGURAS

	Pag
Figura 1. Topología Escenario 1 .....	20
Figura 2. Configuración servidor de Internet .....	23
Figura 3. Configuración servidor web.....	28
Figura 4. Ping de R1 A R2, S0/0/0 .....	34
Figura 5. Ping R2 A R3, S0/0/1 .....	34
Figura 6. Ping del servidor de internet al Gateway predeterminado.....	35
Figura 7. Conectividad S1 A R1, VLAN 200 Y R1, dirección VLAN 21 .....	42
Figura 8. Conectividad S3 a R1, VLAN 200 Y R1, dirección VLAN 23.....	42
Figura 9. DHCP PC-A .....	50
Figura 10. DHCP PC-C .....	51
Figura 11. Ping de la PC-A a la PC-C.....	51
Figura 12. Para ingresar al servidor web .....	52
Figura 13. Parte 6: configurar NTP R2.....	53
Figura 14. Parte 6: configurar NTP R1.....	53
Figura 15. Topología de la red escenario 2.....	56
Figura 16. Topología de red en Packet Tracert.....	60
Figura 17. Balanceo de carga MEDELLIN3 .....	71
Figura 18. Balanceo de carga BOGOTA3.....	71
Figura 19. Rutas conectadas en los routers BOGOTA1 y MEDELLIN1 .....	72
Figura 20. Rutas conectadas en los BOGOTA2 y MEDELLIN3 .....	73
Figura 21. Rutas conectadas en los routers BOGOTA3 y MEDELLIN2 .....	73
Figura 22. Rutas conectadas en el router ISP.....	74
Figura 23. Información OSPF router MEDELLIN1 .....	77
Figura 24. Información OSPF router MEDELLIN1 .....	77
Figura 25. NAT MEDELLIN1 .....	81
Figura 26. NAT BOGOTA1 .....	82
Figura 27. Evidencia servicio DHCP red Medellín.....	84
Figura 28. Evidencia servicio DHCP red BOGOTA.....	86

## GLOSARIO

**DIRECCIONAMIENTO IP:** es la acción de asignar dirección IP a diferentes dispositivos en una topología de red; donde cada dirección está compuesta de un identificador de red y de un edificador de host; Las direcciones V4 están compuestas de 32 bits y debe ser única en la misma topología.

**DNS:** (Domain Name System o DNS, por sus siglas en inglés) sistema de nombres de dominio es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombre de dominio asignado a cada uno de los participantes. Su función más importante es "traducir" nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente

**DHCP:** (Dynamic Host Configuration Protocol), es un protocolo cliente/servidor automático con el cual un servidor asigna direccionamiento IP y otros parámetros de configuración a cada dispositivo host en una red para establecer una comunicación; las direcciones IP dinámicas se van asignando en la medida que van quedando libres; este servicio sabe en todo momento el tiempo y que NIC tiene una IP asignada.

**ENCAPSULAMIENTO PPP:** (Point-to-Point Protocol), es un protocolo que establece un enlace directo entre dos nodos sin dispositivo intermediarios; el encapsulamiento permite fácilmente la multiplexación de otros protocolos de capa de red de forma simultánea en la misma transmisión, igualmente es posible tener compatibilidad con el hardware utilizado durante el enlace.

**HTTP:** Hypertext Transfer Protocol (o Protocolo de Transferencia de Hipertexto en español) es un protocolo de la capa de aplicación para la transmisión de documentos hipertexto, como HTML. Fue diseñado para la comunicación entre los navegadores y servidores web, aunque puede ser utilizado para otros propósitos también. Sigue el clásico modelo cliente-servidor, en el que un cliente establece una conexión, realizando una petición a un servidor y espera una respuesta de este

**ISP:** (Internet service provider), es el nombre asignado en la red a la empresa que provee conexión a Internet; estas empresas interconectan a sus usuarios a Internet mediante diferentes tecnologías como dial-up, cabledem, GSM, y/o DSL, entre otras.

**NAT:** (Network Address Translation), es la forma de intercambio de paquetes entre redes con direccionamiento de dominio diferente; este protocolo proporcionar un enrutamiento transparente, de igual forma sólo funciona cuando el direccionamiento hace parte del protocolo en sí mismo.

OSPF: (Open Shortest Path First), es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos. Su medida de métrica se denomina cost, y tiene en cuenta diversos parámetros tales como el ancho de banda y la congestión de los enlaces. OSPF construye además una base de datos enlace-estado (Link-State Database, LSDB) idéntica en todos los routers de la zona.

RIP: (Routing Information Protocol) se usa para el intercambio de información de enrutamiento entre pasarelas y hosts en los router; igualmente se puede decir que es un algoritmo de vector de distancia muy básico y para el cual se desarrolló una versión 2.

Router: dispositivo de red que opera en la capa 3 del modelo OSI. permite la interconexión entre varios dominios de red; este comparte información mediante varios protocolos con otros router para determinar cuál es la ruta más rápida y adecuada.

Telnet: (Telecommunication Network) es el nombre de un protocolo de red que nos permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. También es el nombre del programa informático que implementa el cliente, para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

VLAN: Acrónimo de virtual LAN (red de área local virtual) es un método que permite crear redes que lógicamente son independientes, aunque estas se encuentren dentro de una misma red física.

## RESUMEN

Este trabajo tiene como propósito la implementación y simulación de dos escenarios de redes bajo la tecnología de cisco, las herramientas de software en la cuales se pudiesen simular son Packet Tracet o GNS3.

El escenario uno consta de varias actividades, la primera de ellas es lograr una comunicación entre un Switch principal y un Switch secundario por medio de una red troncal, y cada uno tiene VLANs diferentes configuradas, luego conseguir que el Router1 conectado al Switch principal, le entregue servicio de DHCP a los computadores conectados en ambos Switches, después de esto se configura comunicación por medio de un puerto serial entre Router1 y Router2 utilizando IPv4 e IPv6 y RIP v2 como protocolo de comunicación, se configura la ruta por defecto (ip route 0.0.0.0 0.0.0.0 Serial0/0/0); En el Router2 se configura en una interfaces con salida a un servidor de internet, esta interfaz se habilita como ruta por defecto (ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0), y también se configura NAT de salida (ip nat outside), va configura con IPv4 e IPv6, RIP v2; Posteriormente al Router2 se le configura comunicación con un servidor web, en esa interface se configura NAT de entrada (ip nat inside); A Route2 se le configuran los servicios de una NAT estática que va direccionada al servidor de web (ip nat inside source static 10.10.10.10 209.165.200.237) y una NAT dinámica por medio de pool de Internet, para que cualquier equipo que este autorizado y necesite salir a internet lo pueda hacer por medio de este pool de IPs (ip nat pool INTERNET 209.165.200.233 209.165.200.237 netmask 255.255.255.248), otro servicio que se habilita dentro de Router2 es (access-list 1 permit) que crea una lista de IPs autorizadas para salir a Internet, para este caso las IPs de las VLANs, del Router1 mencionadas con anterioridad y de las LoopBack configuradas en Router3 mencionado con posterioridad; Después se configura comunicación entre Router2 y Router3 por medio de comunicación serial allí también se utiliza IPv4 e IPv6 y RIP v2 como protocolo de comunicación, por último, en Router3 se configura tres LoopBack con direcciones IPv4 e IPv6, en Router3 la ruta por defecto es (ip route 0.0.0.0 0.0.0.0 Serial0/0/1)

El segundo escenario se simulan dos redes con salida a Internet, la infraestructura y configuración a nivel protocolos de ambas redes son las mismas, son tres routers en cada red, el router uno es el router de frontera conectado a un router ISP que simula la conexión a internet, hasta el cual solo debe llegar los mensajes de cada red, es decir la red1 y red2 solo deban alcanzar hasta el ISP no debe haber comunicación entre las redes 1 y 2, los tres routers dentro de cada red deben utilizar el protocolo de comunicación OSPF v2, esto permite que se cree una área para cada red, la cual accede por medio del protocolo OSPF que se compartan las tablas de enrutamiento entre routers conectadas, el router uno y el router dos están conectados entre si por medio de dos canales seriales de comunicación diferentes, tanto el router dos y el tres tienen conectados por su puerto G0/0 una LAN, el router dos tiene configurado el servicio de DHCP para LANs conectadas en ambos routers,

al router tres se le habilita y configura mensajes de broadcast provenientes del router dos, el router tres va conectado al router uno por un puerto serial, para el desarrollo de este escenario solo se utiliza IPv4 en cada.

Para cada escenario se tuvieron que desarrollar una serie de pasos como lo son ping, Tracert, conectividad hacia páginas web, en los cuales se debió evidenciar por medio de gráficas, tablas y explicaciones escritas como se realizó dicha actividad y cuáles fueron los pasos y configuraciones para desarrollar dichas actividades.

## ABSTRACT

This work aims to implement and simulate two network scenarios under Cisco technology, the software tools in which they could be simulated are Packet Tracer or GNS3.

Scenario one consists of several activities, the first of which is to achieve communication between a primary switch and a secondary switch over a backbone, and each has different VLANs configured, then get Router 1 connected to the main switch, deliver DHCP service to the connected computers on both switches, after this communication is configured via a serial port between Router1 and Router2 using IPv4 and IPv6 and RIP v2 as communication protocol, the default route is configured (ip route 0.0.0.0 0.0.0.0 Serial0/0/0); On Router2 is configured on an interfaces output to an Internet server, this interface is enabled as the default route (ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0), and outbound NAT is also configured (ip nat outside nat), it is configured with IPv4 and IPv6, RIP v2; Behind Router 2 is configured to communicate with a web server, on that interface, inbound NAT (ip nat inside) is configured; Router2 is configured with the services of a static NAT that is routed to the web server (ip nat inside source static 10.10.10.10 209.165.200.237) and a dynamic NAT via Internet pool, so that any computer that is authorized and needs to go out to the Internet can do so through this IP pool (ip nat (ip) pool INTERNET 209.165.200.233 209.165.200.237 netmask 255.255.255.248), another service that is enabled within Router2 is (access-list 1 permit) that creates a list of IPs authorized to go out to the Internet, for this case the IPs of VLANs, of Router 1 mentioned above and loopbacks configured on Router3 mentioned later; Then communication between Router2 and Router3 is configured via serial communication there IPv4 and IPv6 and IPv6 and RIP v2 are also used as a communication protocol, finally, in Router3 three loopbacks with IPv4 and IPv6 addresses are configured, on Router3 the default route is (ip route 0.0.0.0 0.0.0.0 Serial0/0/1)

The second scenario simulates two networks with Internet output, the infrastructure and configuration level protocols of both networks are the same, there are three routers in each network, router one is the border router connected to an ISP router that simulates the internet connection, to which only messages from each network must arrive, i.e. network1 and network2 should only reach until isP should not be communication between networks 1 and 2, the three routers within each network must use the OSPF v2 communication protocol, this allows an area to be created for each network, which is accessed via the OSPF protocol that the routing tables between connected routers are shared between connected routers, Router One and Router Two are connected to each other through two different serial communication channels, both Router two and router three have a LAN connected by its G0/0 port, Router two has configured DHCP service for LANs connected on both routers, Router three is enabled and configures broadcast messages from Router Two,

Router Three is connected to router one by a serial port, for the development of this scenario only IPv4 is used on each.

For each scenario, a series of steps had to be developed such as ping, Tracert, connectivity to web pages, in which it had to be evidenced by graphs, tables and written explanations how that activity was carried out and what were the steps and configurations to develop those activities.



## INTRODUCCIÓN

La actividad se centra en una prueba de habilidades técnico-prácticas en redes de datos con tecnología cisco, se presentan dos escenarios y para cada escenario se debe realizar una serie de pasos los cuales se deben evidenciar con imágenes y se deben sustentar lo realizado con los respectivos comandos de cisco utilizados, la llevar a cabo de forma correcta los pasos la simulación que se deberán llevar a cabo una buena comunicación entre los escenarios planteados.

Durante el desarrollo de estos dos escenarios para poder llevar a buen puerto las actividades de pondrán en práctica la mayor cantidad conceptos aprendidos en los cursos de CCNA1 Routing and Switching: Introducción a las redes, y CCNA2 Routing y switching: Principios básicos de routing y switching.

## JUSTIFICACION

Porque como es de conocimiento general, la tecnología de Networking juega un papel relevante en las tecnologías de la información y la comunicación, en especial las tecnologías implementadas en redes cisco, ya que es la empresa cisco quien tiene la mayor parte del mercado de Networking, es decir los routers, switches y otros dispositivos de redes que utilizan las empresas en su mayoría son de la marca cisco, por ende, las configuraciones, los protocolos, procesos y administración se basan en tecnologías de redes cisco.

Poseer las competencias necesarias en la administración, implementación, configuración, solución y análisis del funcionamiento de las redes basadas en tecnologías de cisco brinda una gran posibilidad de crecimiento académico y profesional en el ramo de la ingeniería de telecomunicaciones, es por esto por lo que el correcto desarrollo de este trabajo nos prepara para adquirir dichas competencias.

## OBJETIVOS

### OBJETIVOS GENERAL:

Brinda solución a dos escenarios de redes de datos LAN y WAM bajo el uso de la tecnología cisco.

### OBJETIVOS ESPECIFICOS:

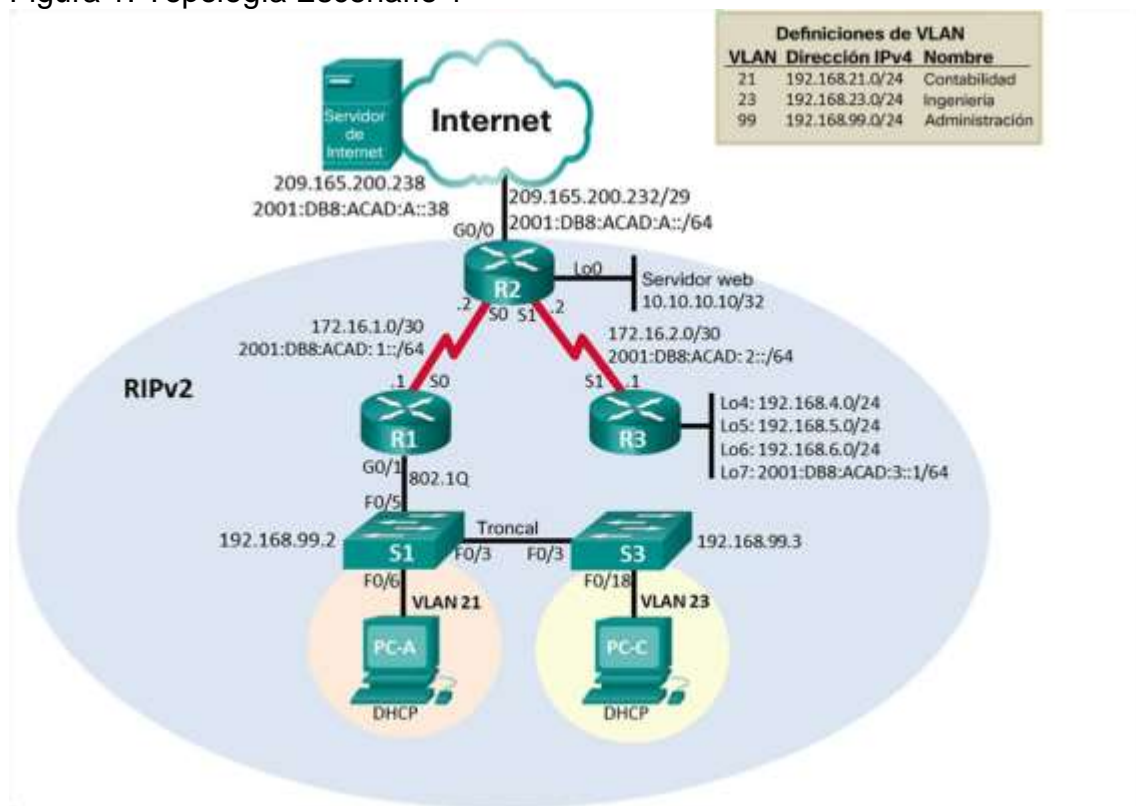
- Diseñar, configurar e implementar las redes de estudio en una herramienta de simulación (Packet Tracer o GSM3).
- Poner en práctica las competencias técnicas (uso e implementación de comandos para redes cisco) aprendidos durante el estudio del diplomado.
- Configurar los protocolos de comunicación para cada uno de los ejercicios
- Configurar e implementar direccionamiento IPv4 e IPv6
- Solucionar los errores que se presenten durante la implantación de los casos de estudio y garantizar que ambas simulaciones funcionen de acuerdo a los solicitado

## DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

### ESCENARIO 1

Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, 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 1. Topología Escenario 1



Fuente: Ejercicio

## DESARROLLO DEL ESCENARIO 1

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

Tabla 1. Paso 1 - Parte 1: Inicializar y volver a cargar los routers y los switches

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Se pueden utilizar los comandos Router#erase nvram: o Router#erase startup-config
Volver a cargar todos los routers	Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch# erase nvram: O Switch# erase startup-config Y Switch#delete vlan.dat
Volver a cargar ambos switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch# show vlan

Fuente: ejercicio

Con el comando "erase startup-config" y el comando reload, se restablece a fábrica la configuración de los router y para los switches los mismos comandos de los router más el comando delete vlan.dat, esto se hace antes de iniciar el proceso de configuración en los routers conectados a la red, se realiza este procedimiento como medida de seguridad y se aplica en cada uno de los equipos conectados a la red.

Se ingresa las líneas de comandos a continuación mencionados para los Switch 1 y 3, para cumplir con lo solicitado en esta parte del ejercicio

```
S1#erase startup-config  
S1#delete vlan.dat  
S1#reload
```

Se ingresa las líneas de comandos a continuación mencionados para los Routers 1, 2 y 3, para cumplir con lo solicitado en esta parte del ejercicio

```
R1#erase startup-config  
R1#reload
```

En los switches S1 y S3 con el comando "show vlan" se valida que la base de datos de VLAN no esté cargada en los switches.

```
Switch#sh vlan
```

## 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):

En esta parte se configuran los parámetros del servidor de Internet

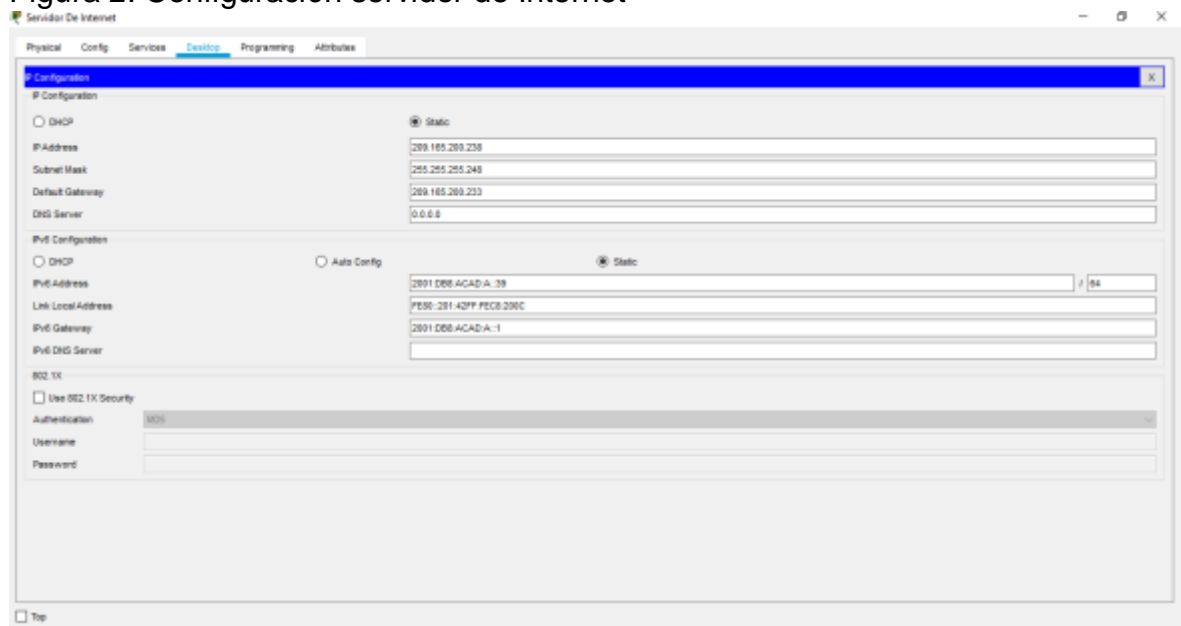
Tabla 2. Paso 1 - Parte 2: Configurar la computadora de Internet

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
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::39

Gateway predeterminado IPv6	2001:DB8:ACAD:A::1
-----------------------------	--------------------

Fuente: propia

Figura 2. Configuración servidor de Internet



Fuente: propia

## PASO 2: CONFIGURAR R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3. Paso 2 - Parte 2: Configurar R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco

Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	<p>Establezca la descripción (description connection R2)</p> <p>Establecer la dirección IPv4 (172.16.1.1 255.255.255.252) Consultar el diagrama de topología para conocer la información de direcciones</p> <p>Establecer la dirección IPv6 (2001:DB8:ACAD:1::1/64) Consultar el diagrama de topología para conocer la información de direcciones</p> <p>Establecer la frecuencia de reloj en 128000 (clock rate 128000)</p> <p>Activar la interfaz</p>
Rutas predeterminadas	<p>Configurar una ruta IPv4 predeterminada de S0/0/0</p> <p>Configurar una ruta IPv6 predeterminada de S0/0/0</p>

Fuente: ejercicio

## Configuración básica del router

```

Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd # Se prohíbe el acceso no autorizado #

```



## Configuración de las interfaces del router

```

R1(config)#int S0/0/0
R1(config-if)#description connection R2
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64
R1(config-if)#clock rate 128000
R1(config-if)# no sh
R1(config-if)#exit
Configuración de la ruta por defecto
R1(config)#ip route 0.0.0.0 0.0.0.0 S0/0/0
%Default route without gateway, if not a point-to-point interface, may impact
performance
R1(config)#ipv6 route ::/0 S0/0/0
R1(config)#exit
    
```

## PASO 3: CONFIGURAR R2

La configuración del R2 incluye las siguientes tareas:

Tabla 4. Paso 3 - Parte 2: Configurar R2

<b>Elemento o tarea de configuración</b>	<b>Esptaecificación</b>
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Habilitar el servidor HTTP	IP adres:10.10.10.10 Subnet Mask: 255.255.255.0 Default Gateway: 10.10.10.1
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Interfaz S0/0/0	<p>Establezca la descripción (description connection R1)</p> <p><b>Establezca la dirección IPv4(172.16.1.2 255.255.255.252). Utilizar la siguiente dirección disponible en la subred.</b></p> <p>Establezca la dirección IPv6 (2001:DB8:ACAD:1::2/64). Consulte el diagrama de topología para conocer la información de direcciones.</p> <p>Activar la interfaz</p>
Interfaz S0/0/1	<p>Establecer la descripción (description connection R3)</p> <p>Establezca la dirección IPv4 (172.16.2.2 255.255.255.252). Utilizar la primera dirección disponible en la subred.</p> <p>Establezca la dirección IPv6(2001:DB8:ACAD:2::2/64). Consulte el diagrama de topología para conocer la información de direcciones.</p> <p>Establecer la frecuencia de reloj en 128000.</p> <p>Activar la interfaz</p>
Interfaz G0/0 (simulación de Internet)	<p>Establecer la descripción (description connection Servidor De Internet).</p> <p>Establezca la dirección IPv4(209.165.200.233 255.255.255.248). Utilizar la primera dirección disponible en la subred.</p> <p>Establezca la dirección IPv6(2001:DB8:ACAD:a::1/64). Utilizar la primera dirección disponible en la subred.</p> <p>Activar la interfaz</p>
Interfaz loopback 0 (servidor web simulado)	<p>Establecer la descripción(description connection Servidor Web).</p> <p>Establezca la dirección IPv4(10.10.10.1 255.255.255.0).</p>
Ruta predeterminada	<p>Configure una ruta IPv4 predeterminada de G0/0.</p> <p>Configure una ruta IPv6 predeterminada de G0/0.</p>

Fuente: ejercicio

## Configuración básica del router

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#banner motd # Se prohíbe el acceso no autorizado #
Configuración de las interfaces del router
R2(config)#int S0/0/0
R2(config-if)#description connection R2
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64
R2(config-if)#clock rate 128000
R2(config-if)#no sh
R2(config-if)#exit
R2(config)#int S0/0/1
R2(config-if)#description connection R3
R2(config-if)#ip address 172.16.2.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64
R2(config-if)#clock rate 128000
R2(config-if)#no sh
R2(config-if)# exit
R2(config)#int G0/0
R2(config-if)#description connection Servidor De Internet
R2(config-if)#ip address 209.165.200.233 255.255.255.248
R2(config-if)#ipv6 address 2001:DB8:ACAD:a::1/64
R2(config-if)#no sh
R2(config-if)# exit
R2(config)#int G0/1
R2(config-if)#description connection Servidor Web
R2(config-if)#ip address 10.10.10.1 255.255.255.0
R2(config-if)#no sh
```

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

Configuración de la ruta por defecto

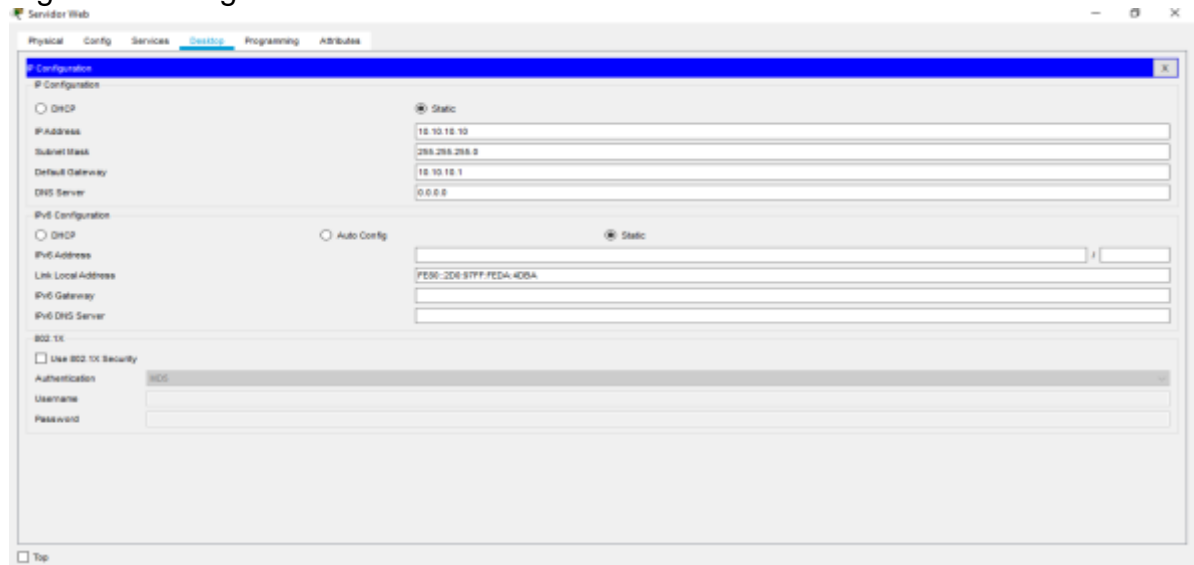
```
R2(config)#ip route 0.0.0.0 0.0.0.0 G0/0
```

%Default route without gateway, if not a point-to-point interface, may impact performance

```
R2(config)#ipv6 route ::/0 G0/0
```

```
R2(config)#exit
```

Figura 3. Configuración servidor web



Fuente: propia

## PASO 4: CONFIGURAR R3

La configuración del R3 incluye las siguientes tareas:

Tabla 5. Paso 4 - Parte 2: Configurar R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/1	<p>Establecer la descripción (description connection R3).</p> <p>Establezca la dirección IPv4(172.16.2.1 255.255.255.252). Utilizar la siguiente dirección disponible en la subred.</p> <p>Establezca la dirección IPv6(2001:DB8:ACAD:2::1/64). Consulte el diagrama de topología para conocer la información de direcciones.</p> <p>Activar la interfaz</p>
Interfaz loopback 4	Establezca la dirección IPv4(192.168.4.1 255.255.255.0). Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4(192.168.5.1 255.255.255.0). Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4(192.168.6.1 255.255.255.0). 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: ejercicio

## Configuración básica del router

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd # Se prohíbe el acceso no autorizado #
```

## Configuración de las interfaces del router

```
R3(config)#int S0/0/0
R3(config-if)#description connection R3
R3(config-if)#ip address 172.16.2.1 255.255.255.252
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64
R3(config-if)#no sh
Configuración de las Lo
R3(config)#int Lo4
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 add 192.168.4.1 255.255.255.0
R3(config-if)#no sh
R3(config-if)#int Lo5
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 add 192.168.5.1 255.255.255.0
R3(config-if)#no sh
```

```

R3(config-if)#int Lo6
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 add 192.168.6.1 255.255.255.0
R3(config-if)#no sh
R3(config)#int Lo7
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
R3(config-if)#no sh
Configuración de la ruta por defecto
R3(config)#ip route 0.0.0.0 0.0.0.0 S0/0/1
%Default route without gateway, if not a point-to-point interface, may impact
performance

```

## PASO 5: CONFIGURAR S1

La configuración del S1 incluye las siguientes tareas:

Tabla 6. Paso 5 – Parte 2 Configurar S1

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
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: ejercicio

## Configuración básica del Switch

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd # Se prohíbe el acceso no autorizado #
```

## PASO 6: CONFIGURAR EL S3

La configuración del S3 incluye las siguientes tareas:

Tabla 7. Paso 6 – Parte 2: Configurar S3

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
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: ejercicio



## Configuración básica de S3

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd # Se prohíbe el acceso no autorizado #
```

## PASO 7: VERIFICAR LA CONECTIVIDAD DE LA RED

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

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

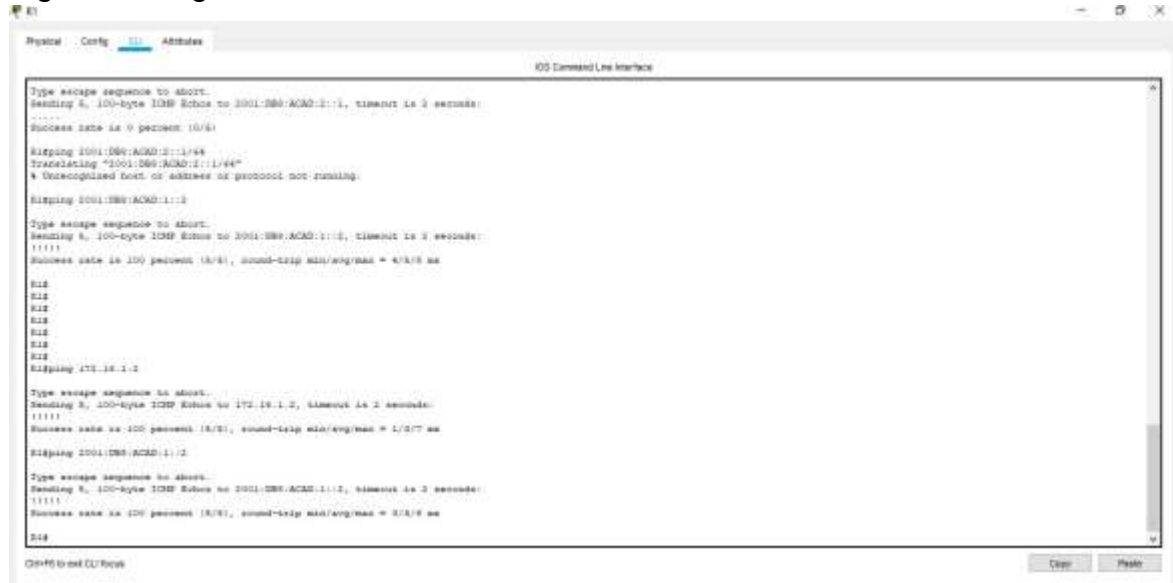
Tabla 8. Paso 7 – Parte 2: Verificar la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	IPv4 (172.16.1.2). IPv6 (2001:DB8:ACAD:1::2/64)	Exitoso
R2	R3, S0/0/1	IPv4(172.16.2.1) IPv6(2001:DB8:ACAD:2::1/64).	Exitoso
PC de Internet	Gateway predeterminado	IPv4:209.165.200.233 IPV6:2001:DB8:ACAD:A::1	Exitoso

Fuente: ejercicio

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

Figura 4. Ping de R1 A R2, S0/0/0



```
Router1#
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R1#ping 2001:DB8:ACAD:1::1/44
Translating "2001:DB8:ACAD:1::1/44"
% Unrecognized host or address or protocol: not running.

R1#ping 2001:DB8:ACAD:1::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/3/8 ms

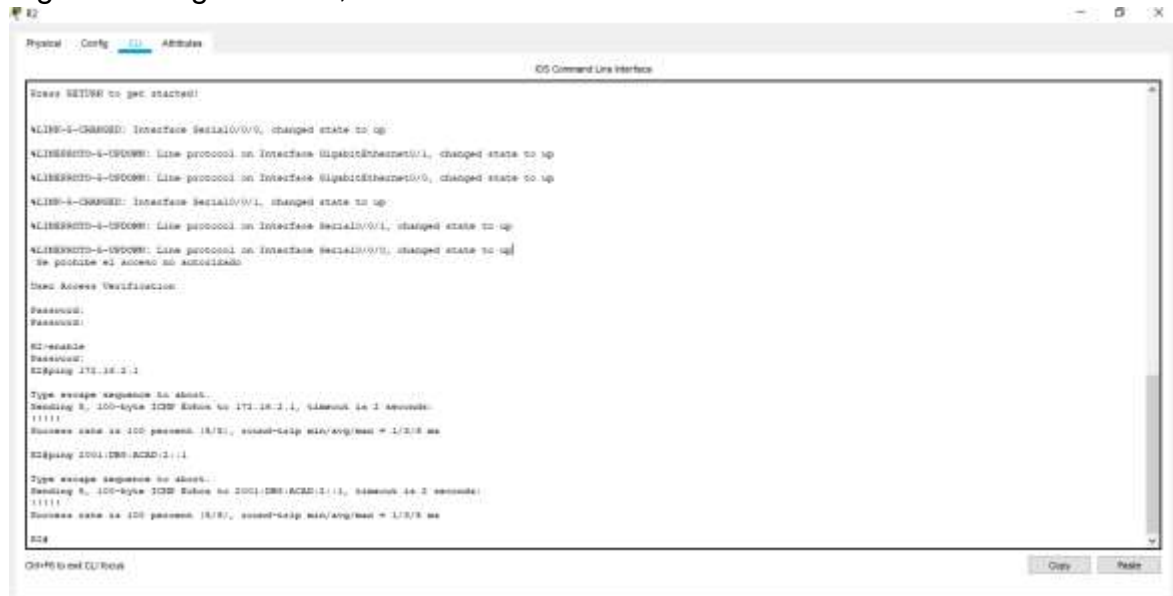
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#ping 172.16.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/0/7 ms

R1#ping 2001:DB8:ACAD:1::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/8 ms

R1#
```

Fuente: propia

Figura 5. Ping R2 A R3, S0/0/1



```
Router2#
Enter SETUP to get started.

%LINK-3-CHANGED: Interface Serial0/0/0, changed state to up
%LINKERR003-3-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
%LINKERR003-3-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINK-3-CHANGED: Interface Serial0/0/1, changed state to up
%LINKERR003-3-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%LINKERR003-3-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%> portable telnet access is autoenabled

Exec Access Verification...
Password:
Password:

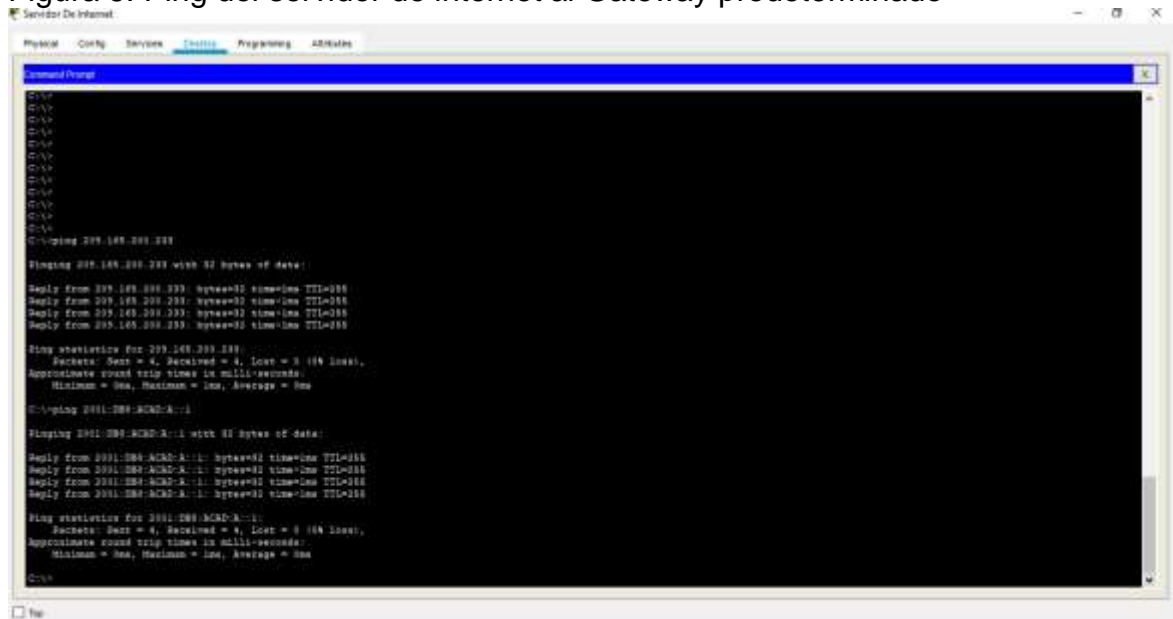
R2#enable
Password:
R2#ping 172.16.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/3 ms

R2#ping 2001:DB8:ACAD:2::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:2::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms

R2#
```

Fuente: propia

Figura 6. Ping del servidor de internet al Gateway predeterminado



Fuente: propia

### PARTE 3: CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN

#### PASO 1: CONFIGURAR S1

Nota: La vlan de Administración nombrada como 99 y con la IP 192.168.99.0/24, se cambia por la 200, con la IP 192.168.200.1, y la 99 se quedará llamando LAN\_S1\_S3 ya que de no ser así genérica un conflicto cuando se deba realizar la configuración la interface G0/1 del R1.

La configuración del S1 incluye las siguientes tareas:

Tabla 9. Paso 1 – Parte 3:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican

Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP (192.168.99.2) asignada al S1 en el diagrama de topología
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 (192.168.21.1) de la subred como el gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range int range f0/1-2, f0/4, f0/6-24, g0/1-2
Asignar F0/6 a la VLAN 21	int f0/6 switchport mode access switchport access vlan 21
Apagar todos los puertos sin usar	int range f0/1-2, f0/4, f0/7-23, g0/1-2 shutdown

Fuente: ejercicio

### Comandos de configuración

```

S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
Se nombran las vlans
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#vlan 200
S1(config-vlan)#name Administracion
Se nombra la vlan tronca entre S1 y S3
S1(config-vlan)#vlan 99
S1(config-vlan)#name LAN_S1_S3
S1(config-vlan)#exit
S1(config)#int vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up
Se le asigna una dirección IP conexión vlan tronca entre S1 y R1
S1(config-if)#ip address 192.168.99.2 255.255.255.0

```

```
S1(config-if)#no shut
S1(config-if)#exit
```

Se le asigna dirección IP a la vlan de contabilidad f0/3

```
S1(config)#ip default-gateway 192.168.21.1
S1(config)#int f0/3
S1(config-if)#switchport mode trunk
Se forzar el enlace troncal en la interfaz f0/5
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
S1(config)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
```

Se configuran los puertos como puertos de acceso

```
S1(config)#int range f0/1-2, f0/4, f0/6-24, g0/1-2
Se asigna la vlan 21 al puerto f0/6
S1(config-if-range)#switchport mode access
S1(config-if-range)#int f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 21
Se apagan los puertos que no están siendo utilizados
S1(config-if)#int range f0/1-2, f0/4, f0/7-23, g0/1-2
S1(config-if-range)#shutdown
```

## PASO 2: CONFIGURAR EL S3

La configuración del S3 incluye las siguientes tareas:

Tabla 10. Paso 2 – Parte 3: Configurar S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP (192.168.99.3) asignada al S3 en el diagrama de topología
Asignar el gateway predeterminado.	Asignar la primera dirección IP (192.168.21.1) en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range int range f0/1-2, f0/4-17, f0/19-24, g0/1-2
Asignar F0/18 a la VLAN 21	int f0/18 switchport mode access switchport access vlan 23
Apagar todos los puertos sin usar	int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 shutdown

Fuente: ejercicio

```

S3#config t
Se nombran las vlans
S3(config)#vlan 21
S3(config-vlan)#name Contabilidad
S3(config-vlan)#vlan 23
S3(config-vlan)#name Ingenieria
S3(config-vlan)#vlan 200
S3(config-vlan)#name Administracion
    
```

Se nombra la vlan tronca entre S1 y S3

```

S3(config-vlan)#vlan 99
S3(config-vlan)#name LAN_S1_S3
S3(config-vlan)#exit
    
```

```

S3(config)#int vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shut
S3(config-if)#exit

```

Se le asigna dirección IP a la vlan de contabilidad f0/3

```

S3(config)#ip default-gateway 192.168.23.1
S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
Se configuran los puertos como puertos de acceso
S3(config)#int range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode access
Se asigna la vlan 23 al puerto f0/18
S3(config)#int f0/18
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 23
Se apagan los puertos que no están siendo utilizados
S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2
S3(config-if)#shutdown
S3(config-if)#exit

```

### PASO 3: CONFIGURAR R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11. Paso 3 – Parte 3: Configurar R1

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad_LAN Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz (192.168.21.1)

Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería_LAN Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz (192.168.23.1)
Configurar la subinterfaz 802.1Q .200 en G0/1	Descripción: LAN de Administración_LAN Asignar la VLAN 200 Asignar la primera dirección disponible a esta interfaz (192.168.200.1)
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de S1_S3_LAN Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz (192.168.99.1)
Activar la interfaz G0/1	int G0/1 no shut

Fuente: ejercicio

Se configuran las subinterfaces

```
R1#config t
R1(config)#int G0/1.21
R1(config-subif)#description Contabilidad_LAN
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip add 192.168.21.1 255.255.255.0
R1(config-subif)#exit
```

```
R1(config)#int G0/1.23
R1(config-subif)#description Ingenieria_LAN
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip add 192.168.23.1 255.255.255.0
R1(config-subif)#exit
```

```
R1(config)#int G0/1.200
R1(config-subif)#description Administracion_LAN
R1(config-subif)#encapsulation dot1q 200
R1(config-subif)#ip add 192.168.200.1 255.255.255.0
R1(config-subif)#exit
```



```

R1(config)#int G0/1.99
R1(config-subif)#description S1_S3_LAN
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip add 192.168.99.1 255.255.255.0
R1(config-subif)#exit

```

```

R1(config)#int G0/1
R1(config-if)#no shut
R1(config-subif)#exit

```

#### 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 12. Paso 4 - Parte 3: Verificar la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 200	192.168.200.1	Exitoso
S3	R1, dirección VLAN 200	192.168.200.1	Exitoso
S1	R1, dirección VLAN 21	192.168.21.1	Exitoso
S3	R1, dirección VLAN 23	192.168.23.1	Exitoso

Figura 7. Conectividad S1 A R1, VLAN 200 Y R1, dirección VLAN 21



Fuente: propia

Figura 8. Conectividad S3 a R1, VLAN 200 Y R1, dirección VLAN 23



Fuente: propia

#### PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO RIPV2

Las tareas de configuración para R1 incluyen las siguientes:

**PASO 1: CONFIGURAR RIPv2 EN EL R1**

Tabla 13. Paso 1 - Parte 4: Configurar RIPv2 en el R1

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
Configurar RIP versión 2	
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	
Desactive la sumarización automática	

Fuente: ejercicio

```
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
R1#enable
R1#confi t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#route rip
R1(config-router)#version 2
R1(config-router)#network 172.16.1.0
R1(config-router)#network 192.168.21.0
R1(config-router)#network 192.168.23.0
R1(config-router)#network 192.168.99.0
R1(config-router)#network 192.168.200.0
R1(config-router)#passive-interface G0/1.21
R1(config-router)#passive-interface G0/1.23
R1(config-router)#passive-interface G0/1.200
R1(config-router)#passive-interface G0/1.99
R1(config-router)#no auto-summary
R1(config-router)#exit
```

## PASO 2: CONFIGURAR RIPv2 EN EL R2

La configuración del R2 incluye las siguientes tareas:

Tabla 14. Paso 2 - Parte 4: Configurar RIPv2 en el R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar las redes conectadas directamente	<b>Nota:</b> Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	
Desactive la sumarización automática.	

Fuente: ejercicio

```
R2(config-router)#route rip
R2(config-router)#version 2
R2(config-router)#network 10.10.10.10
R2(config-router)#network 172.16.1.0
R2(config-router)#network 172.16.2.0
R2(config-router)#passive-interface G0/1
R2(config-router)#no auto-summary
R2(config-router)#exit
```

## PASO 3: CONFIGURAR RIPv2 EN EL R3

La configuración del R3 incluye las siguientes tareas:

Tabla 15. Paso 3 - Parte 4: Configuración RIPv2 en el R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar redes IPv4 conectadas directamente	
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	

Desactive la sumarización automática.	
---------------------------------------	--

Fuente: ejercicio

```
R3>enable
Password:
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#route rip
R3(config-router)#version 2
R3(config-router)#network 172.16.2.0
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
R3(config-router)#network 192.168.6.0
R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
R3(config-router)#no auto-summary
R3(config-router)#exit
```

#### PASO 4: VERIFICAR LA INFORMACIÓN DE RIP

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

Tabla 16. Paso 4 - Parte 4: Verificar la información de RIP

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	
¿Qué comando muestra solo las rutas RIP?	Show ip route rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	show ip protocols

Fuente: ejercicio

```
R3#show ip protocol
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 10 seconds
```

Invalid after 180 seconds, hold down 180, flushed after 240  
Outgoing update filter list for all interfaces is not set  
Incoming update filter list for all interfaces is not set  
Redistributing: rip  
Default version control: send version 2, receive 2  
Interface Send Recv Triggered RIP Key-chain  
Serial0/0/1 2 2  
Automatic network summarization is not in effect  
Maximum path: 4  
Routing for Networks:  
172.16.0.0  
192.168.4.0  
192.168.5.0  
192.168.6.0  
Passive Interface(s):  
Loopback4  
Loopback5  
Loopback6  
Routing Information Sources:  
Gateway Distance Last Update  
172.16.2.2 120 00:00:10  
Distance: (default is 120)

Comando para ver rutas RIP

```
R3#show ip route rip
10.0.0.0/24 is subnetted, 1 subnets
R 10.10.10.0 [120/1] via 172.16.2.2, 00:00:22, Serial0/0/1
172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
R 172.16.1.0/30 [120/1] via 172.16.2.2, 00:00:22, Serial0/0/1
192.168.6.0 /24 is variably subnetted, 2 subnets, 2 masks
R 192.168.21.0/24 [120/2] via 172.16.2.2, 00:00:22, Serial0/0/1
R 192.168.23.0/24 [120/2] via 172.16.2.2, 00:00:22, Serial0/0/1
R 192.168.99.0/24 [120/2] via 172.16.2.2, 00:00:22, Serial0/0/1
R 192.168.200.0/24 [120/2] via 172.16.2.2, 00:00:22, Serial0/0/1
```

## 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 17. Paso 1 - Parte 5: Configurar R1 como servidor de DHCP para las VLAN 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	192.168.21.1 a 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	192.168.23.1 a 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado
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: ejercicio

```

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
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)#default-router 192.168.21.1
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#exit
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)#default-router 192.168.23.1
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#exit

```

## PASO 2: CONFIGURAR LA NAT ESTÁTICA Y DINÁMICA EN EL R2

La configuración del R2 incluye las siguientes tareas:

Tabla 18. Paso 2 - Parte 5: Configurar 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: <b>webuser</b> Contraseña: <b>cisco12345</b> Nivel de privilegio: <b>15</b>
Habilitar el servicio del servidor HTTP	ip http server comandos no soportados por Packet Tracer
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	ip http authentication local comandos no soportados por Packet Tracer
Crear una NAT estática al servidor web.	Dirección global interna: <b>209.165.200.237</b>
Asignar la interfaz interna y externa para la NAT estática	int G0/0 ip nat outside  G0/1 ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: <b>INTERNET</b> El conjunto de direcciones incluye: <b>209.165.200.225 – 209.165.200.228</b>
Definir la traducción de NAT dinámica	ip nat inside source list 1 pool INTERNET

Fuente: ejercicio

```
R2(config)#user webuser privilege 15 secret cisco12345
R2(config)#ip http server
```



```

^% Invalid input detected at '^' marker.
R2(config)#ip http authentication local
^
% Invalid input detected at '^' marker.
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
R2(config)#int G0/0
R2(config-if)#ip nat outside
R2(config-if)#int G0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
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
R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask
255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

```

### 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.

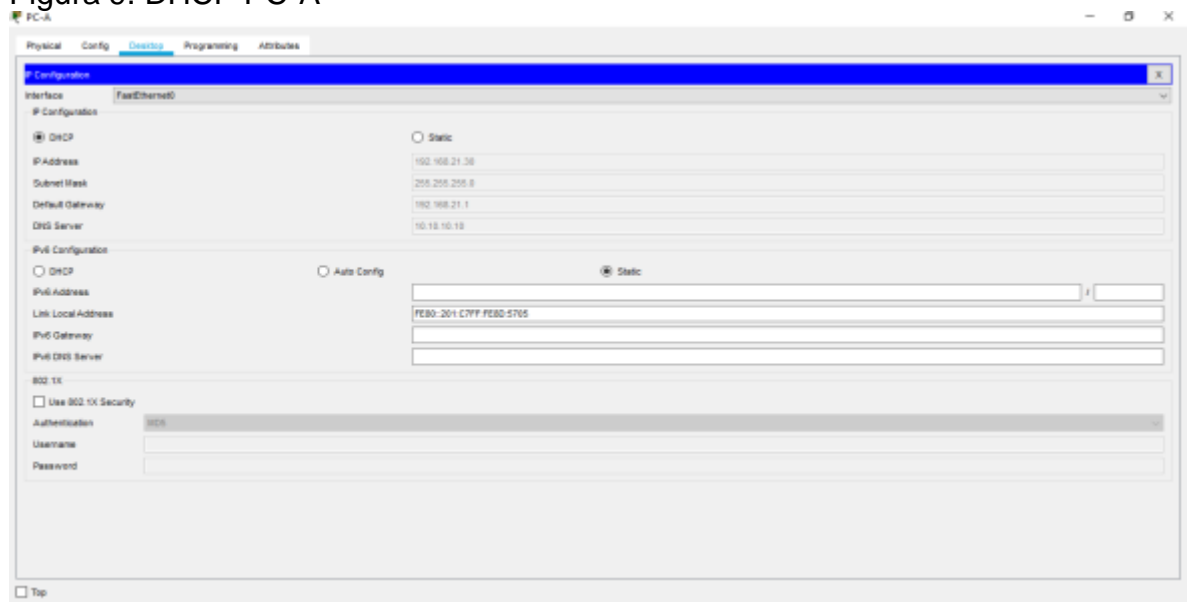
Tabla 19. Paso 3 - Parte 5: Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	IP Address..... : 192.168.21.30 Subnet Mask..... : 255.255.255.0 Default Gateway..... : 192.168.21.1 DNS Server..... : 10.10.10.10
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	IP Address..... : 192.168.23.30 Subnet Mask..... : 255.255.255.0 Default Gateway..... : 192.168.23.1 DNS Server..... : 10.10.10.10

<p>Verificar que la PC-A pueda hacer ping a la PC-C</p> <p><b>Nota:</b> Quizá sea necesario deshabilitar el firewall de la PC.</p>	<p>Exitoso</p>
<p>Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.238) Iniciar sesión con el nombre de usuario <b>webuser</b> y la contraseña <b>cisco12345</b></p>	

Fuente: ejercicio

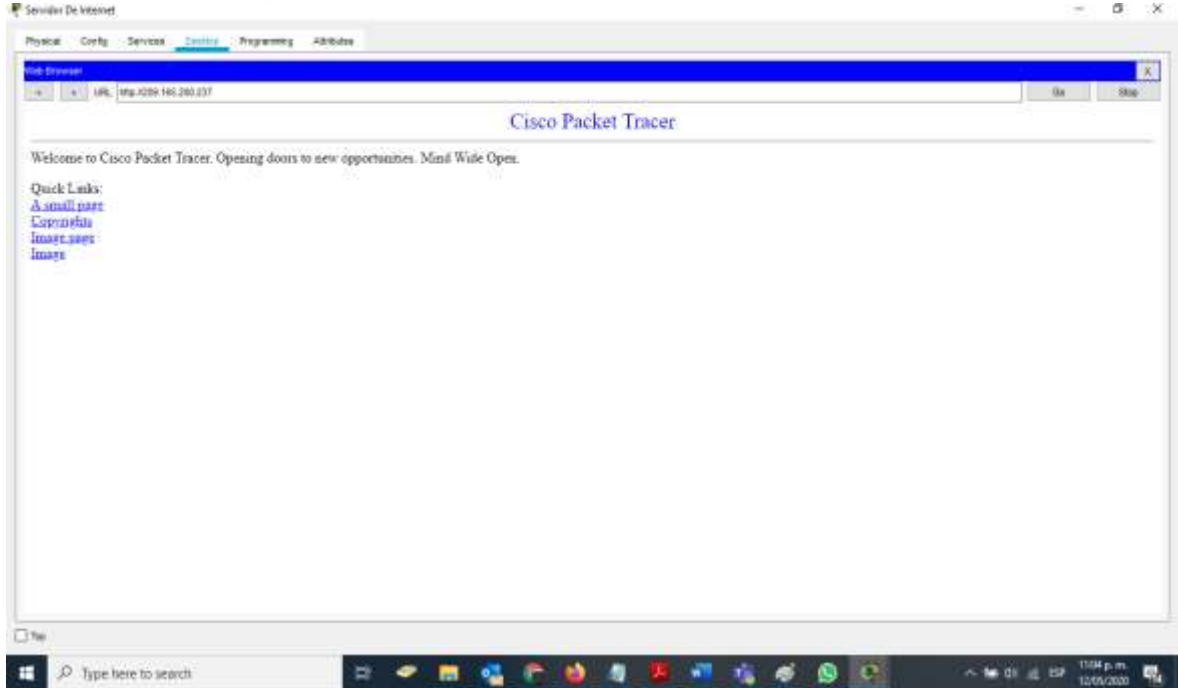
Figura 9. DHCP PC-A



Fuente: propia



Figura 12. Para ingresar al servidor web



Fuente: propia

## PARTE 6: CONFIGURAR NTP

Tabla 20. Parte 6: Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	<b>5 de marzo de 2016, 9 a. m.</b> clock set 9:00:00 March 5 2016
Configure R2 como un maestro NTP.	Nivel de estrato: <b>5</b> ntp master 5
Configurar R1 como un cliente NTP.	Servidor: <b>R2</b> ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	ntp update-calendar
Verifique la configuración de NTP en R1.	show ntp associations

Fuente: ejercicio



PASO 1 PARTE 7: RESTRINGIR EL ACCESO A LAS LÍNEAS VTY EN EL R2

Tabla 21. Paso 1: Restringir el acceso a las líneas 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: <b>ADMIN-MGT</b> ip access-list standard ADMIN-MGT
Aplicar la ACL con nombre a las líneas VTY	access-class ADMIN- MGT in transport input telnet
Permitir acceso por Telnet a las líneas de VTY	permit host 172.16.1.1 line vty 0 4
Verificar que la ACL funcione como se espera	

Fuente: ejercicio

conf t

Enter configuration commands, one per line. End with CNTL/Z.

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

R2(config-std-nacl)#permit host 172.16.1.1

R2(config-std-nacl)#line vty 0 4

R2(config-line)#transport input telnet

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

R2(config-line)#exit

PASO 2: INTRODUCIR EL COMANDO DE CLI ADECUADO QUE SE NECESITA PARA MOSTRAR LO SIGUIENTE

Tabla 22. Paso 2 - Parte 7: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	do show access-list

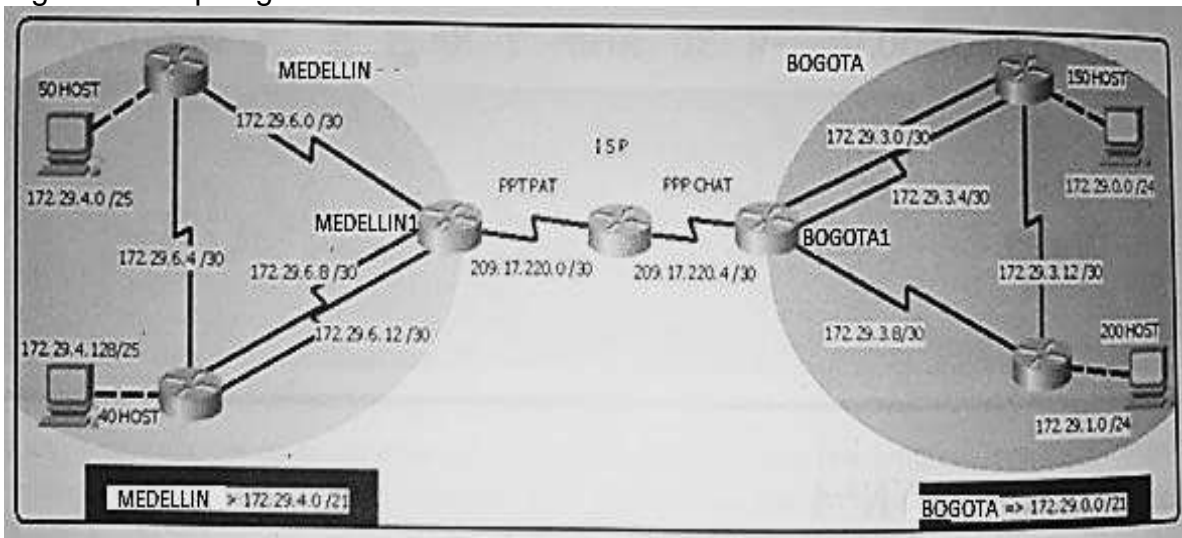
Restablecer los contadores de una lista de acceso	Do clear access-list counter 1
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Do show interfaces
¿Con qué comando se muestran las traducciones NAT?	<p><b>Nota:</b> Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.</p> <p>Do show ip nat translation</p>
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat translation

Fuente: ejercicio

## Escenario 2

Una empresa posee sucursales distribuidas en las ciudades de Bogotá y Medellín, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

Figura 15. Topología de la red escenario 2



Fuente: ejercicio

### DESARROLLO DEL ESCENARIO 2

Este escenario plantea el uso de OSPF como protocolo de enrutamiento, considerando que se tendrán rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación.

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.

Debe configurar PPP en los enlaces hacia el ISP, con autenticación.

Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

Como trabajo inicial se debe realizar lo siguiente.



- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).
  - Realizar la conexión física de los equipos con base en la topología de red
- Configuración básica de los routers de la red para el escenario dos

```

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname MEDELLIN3
MEDELLIN3(config)#enable secret class
MEDELLIN3(config)#line console 0
MEDELLIN3(config-line)#password cisco
MEDELLIN3(config-line)#login
MEDELLIN3(config-line)#line vty 0 4
MEDELLIN3(config-line)#password cisco
MEDELLIN3(config-line)#login
MEDELLIN3(config-line)#exit
MEDELLIN3(config)#service password-encryptio
MEDELLIN3(config)#banner motd # Se prohíbe el acceso no autorizado #
MEDELLIN3(config)#

```

```

Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname MEDELLIN2
MEDELLIN2(config)#enable secret class
MEDELLIN2(config)#line console 0
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#line vty 0 4
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#exit
MEDELLIN2(config)#service password-encryption
MEDELLIN2(config)#banner motd # Se prohíbe el acceso no autorizado #

```

```

Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup

```

```
Router(config)#hostname MEDELLIN1
MEDELLIN1(config)#enable secret class
MEDELLIN1(config)#line console 0
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#line vty 0 4
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#exit
MEDELLIN1(config)#service password-encryption
MEDELLIN1(config)#banner motd # Se prohíbe el acceso no autorizado #
```

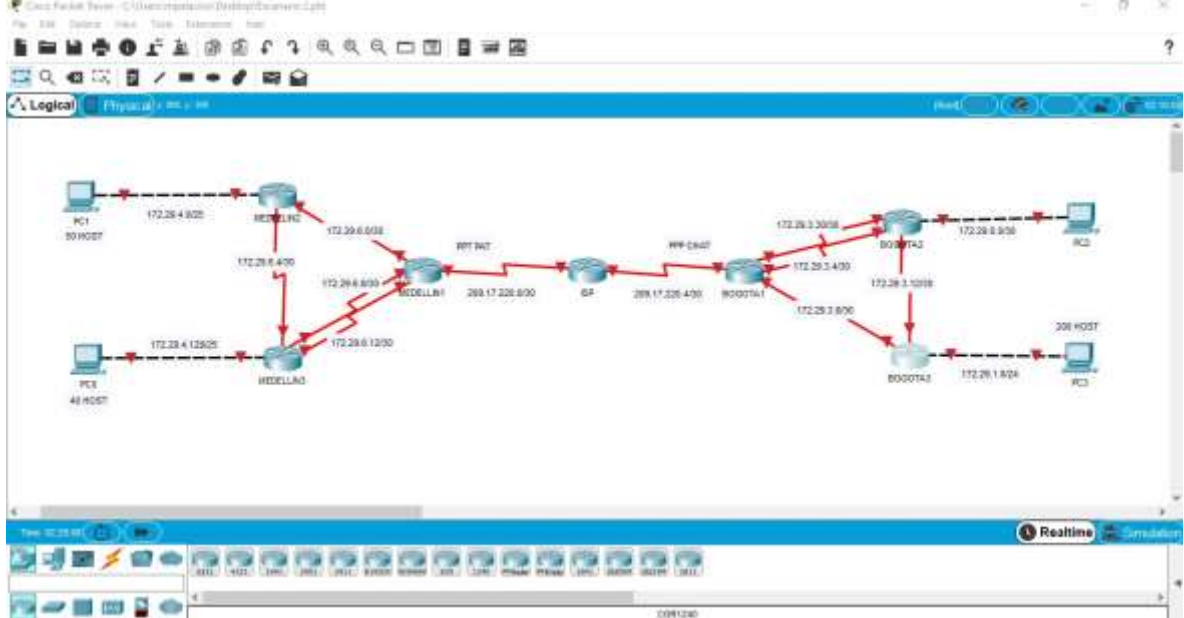
```
Router>enable
Router#no ip domain-lookup
Router(config)#no ip domain-lookup
Router(config)#hostname ISP
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#line vty 0 4
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#service password-encryption
ISP(config)#banner motd # Se prohíbe el acceso no autorizado #
```

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname BOGOTA1
BOGOTA1(config)#enable secret class
BOGOTA1(config)#line console 0
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login
BOGOTA1(config-line)#line vty 0 4
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login
BOGOTA1(config-line)#EXIT
BOGOTA1(config)#service password-encryption
BOGOTA1(config)#banner motd # Se prohíbe el acceso no autorizado #
```

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname BOGOTA2
BOGOTA2(config)#enable secret class
BOGOTA2(config)#line console 0
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#line vty 0 4
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#exit
BOGOTA2(config)#service password-encryption
BOGOTA2(config)#banner motd # Se prohíbe el acceso no autorizado #
```

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname BOGOTA3
BOGOTA3(config)#enable secret class
BOGOTA3(config)#line console 0
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login
BOGOTA3(config-line)#line vty 0 4
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login
BOGOTA3(config-line)#exit
BOGOTA3(config)#service password-encryption
BOGOTA3(config)#banner motd # Se prohíbe el acceso no autorizado #
```

Figura 16. Topología de red en Packet Tracer



Fuente: propia

PARTE 1: CONFIGURAR LA TOPOLOGÍA DE RED, DE ACUERDO CON LAS SIGUIENTES ESPECIFICACIONES

PARTE 1: CONFIGURACIÓN DEL ENRUTAMIENTO

A. CONFIGURAR PROTOCOLO OSPF V2 EN LA RED

Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática.

Configuración de las interfaces seriales del router ISP

```
ISP#confi t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#int S0/0/0
ISP(config-if)#ip address 209.17.220.10 255.255.255.252
ISP(config-if)#description connect to Medellin1
ISP(config-if)#exit
```

```
ISP(config)#int S0/0/1
ISP(config-if)#description connect to BOGOTA1
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
ISP(config-if)#no sh
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
ISP(config-if)#exit
```

```
ISP(config)#int S0/0/0
ISP(config-if)#description connect to MEDELLIN1
ISP(config-if)#no sh
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
ISP(config-if)# exit
```

```
Configuración router BOGOTA1
BOGOTA1(config)#int S0/0/1
BOGOTA1(config-if)#description to connect ISP
BOGOTA1(config-if)#ip address 209.17.220.6 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
This command applies only to DCE interfaces
BOGOTA1(config-if)#no sh
BOGOTA1(config-if)#exit
```

```
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
BOGOTA1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state
to up
BOGOTA1(config-if)#exit
```

```
BOGOTA1(config)#int S0/0/0
BOGOTA1(config-if)#description to connect BOGOTA2
BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252
BOGOTA1(config-if)#no sh
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
BOGOTA1(config-if)#exit
BOGOTA1(config)#int S0/1/1
BOGOTA1(config-if)#description to connect BOGOTA2
BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252
BOGOTA1(config-if)#no sh
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
BOGOTA1(config-if)#exit
```

```
BOGOTA1(config)#int S0/1/0
BOGOTA1(config-if)#description to connect BOGOTA3
BOGOTA1(config-if)#clock rate 1280000
Unknown clock rate
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no sh
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
BOGOTA1(config-if)#exit
```

Configuración router BOGOTA2

```
BOGOTA2#confi t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA2(config)#int s0/0/0
BOGOTA2(config-if)#ip address 172.29.3.2 255.255.255.252
BOGOTA2(config-if)#description to connect BOGOTA1
BOGOTA2(config-if)#Clock rate 128000
BOGOTA2(config-if)#no sh
BOGOTA2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
BOGOTA2(config-if)#exit
```

```
BOGOTA2(config)#int s0/1/1
BOGOTA2(config-if)#description to connect BOGOTA1
BOGOTA2(config-if)#ip address 172.29.3.6 255.255.255.252
BOGOTA2(config-if)#Clock rate 128000
BOGOTA2(config-if)#no sh
BOGOTA2(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to up
BOGOTA2(config-if)#exit
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state  
to up

```
BOGOTA2(config)#int s0/0/1
BOGOTA2(config-if)#description to connect BOGOTA3
BOGOTA2(config-if)#ip address 172.29.3.13 255.255.255.252
BOGOTA2(config-if)#no sh
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
BOGOTA2(config-if)#exit
```

```

BOGOTA2(config)#int G0/0
BOGOTA2(config-if)#description to connect LAN
BOGOTA2(config-if)#ip address 172.29.0.1 255.255.255.0
BOGOTA2(config-if)#no sh
BOGOTA2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
BOGOTA2(config-if)#exit

```

### Configuración router BOGOTA3

```

BOGOTA3#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA3(config)#int S0/1/0
BOGOTA3(config-if)#description to connect BOGOTA1
BOGOTA3(config-if)#ip address 172.29.3.10 255.255.255.252
BOGOTA3(config-if)#no sh
BOGOTA3(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
BOGOTA3(config-if)#exit

```

```

BOGOTA3(config)#ip address 172.29.3.10 255.255.255.252
%LINEPROTO-5-UPDOWN: Line protocol on Inter
BOGOTA3(config)#int S0/0/1
BOGOTA3(config-if)#description to connect BOGOTA2
BOGOTA3(config-if)#ip address 172.29.3.14 255.255.255.252
BOGOTA3(config-if)#Clock rate 128000
BOGOTA3(config-if)#no sh
BOGOTA3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,

```

```

BOGOTA3(config)#int G0/0
BOGOTA3(config-if)#description to connect LAN
BOGOTA3(config-if)#ip address 172.29.1.1 255.255.255.0
BOGOTA3(config-if)#no sh
BOGOTA3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up

```

```
BOGOTA3(config-if)#exit
```

### Configuración router MEDELLIN1

```
MEDELLIN1#confi t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#int S0/1/0
MEDELLIN1(config-if)#description to connect MEDELLIN2
MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no sh
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
MEDELLIN1(config-if)#exit
```

```
MEDELLIN1(config)#int S0/0/0
MEDELLIN1(config-if)#description to connect ISP
MEDELLIN1(config-if)#ip address 209.17.200.9 255.255.255.252
MEDELLIN1(config-if)#no sh
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
MEDELLIN1(config-if)#exit
```

```
MEDELLIN1(config)#int S0/0/1
MEDELLIN1(config-if)#description to connect MEDELLIN3
MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.252
MEDELLIN1(config-if)#no sh
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
MEDELLIN1(config-if)#exit
```

```
MEDELLIN1(config)#int S0/1/1
MEDELLIN1(config-if)#description to connect MEDELLIN3
MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.252
MEDELLIN1(config-if)#no sh
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
MEDELLIN1(config-if)#exit
```

### Configuración router MEDELLIN3

```
MEDELLIN3#config t
```



Enter configuration commands, one per line. End with CNTL/Z.

```
MEDELLIN3(config)#int S0/0/1
MEDELLIN3(config-if)#description to connect MEDELLIN1
MEDELLIN3(config-if)#ip address 172.29.6.10 255.255.255.252
MEDELLIN3(config-if)#clock rate 128000
MEDELLIN3(config-if)#no sh
MEDELLIN3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
MEDELLIN3(config-if)#exit
```

```
MEDELLIN3(config)#int S0/1/1
MEDELLIN3(config-if)#description to connect MEDELLIN1
MEDELLIN3(config-if)#ip address 172.29.6.14 255.255.255.252
MEDELLIN3(config-if)#clock rate 128000
MEDELLIN3(config-if)#no sh
MEDELLIN3(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state
to up
MEDELLIN3(config-if)#exit
```

```
MEDELLIN3(config)#int S0/0/0
MEDELLIN3(config-if)#description to connect MEDELLIN2
MEDELLIN3(config-if)#ip address 172.29.6.6 255.255.255.252
MEDELLIN3(config-if)#no sh
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
MEDELLIN3(config-if)#exit
```

```
MEDELLIN3(config)#int G0/0
MEDELLIN3(config-if)#description to connect LAN
MEDELLIN3(config-if)#ip address 172.29.4.1 255.255.255.128
MEDELLIN3(config-if)#no sh
MEDELLIN3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
MEDELLIN3(config-if)#exit
```

Configuración router MEDELLIN2

```
MEDELLIN2#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN2(config)#int S0/1/0
MEDELLIN2(config-if)#description to connect MEDELLIN1
MEDELLIN2(config-if)#ip address 172.29.6.2 255.255.255.252
MEDELLIN2(config-if)#no sh
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
```

```
MEDELLIN2(config)#int S0/0/0
MEDELLIN2(config-if)#description to connect MEDELLIN3
MEDELLIN2(config-if)#ip address 172.29.6.5 255.255.255.252
MEDELLIN2(config-if)#clock rate 128000
MEDELLIN2(config-if)#no sh
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
MEDELLIN2(config-if)#EXIT
MEDELLIN2(config)#int G0/0
MEDELLIN2(config-if)#description to connect LAN
MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.128
MEDELLIN2(config-if)#no sh
MEDELLIN2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
MEDELLIN2(config-if)#exit
```

### Configuración del protocolo OSPF en el router ISP

```
ISP#enable
ISP#config t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#router ospf 1
ISP(config-router)#router-id 4.4.4.4
ISP(config-router)#network 209.17.220.8 0.0.0.3 area 1
ISP(config-router)#network 209.17.220.4 0.0.0.3 area 1
```

### Configuración del protocolo OSPF en el router MEDELLIN1

```
MEDELLIN1#enable
```

```
MEDELLIN1#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#route ospf 1
MEDELLIN1(config-router)#router-id 3.3.3.3
MEDELLIN1(config-router)#network 209.17.200.8 0.0.0.3 area 1
MEDELLIN1(config-router)#network 172.29.6.12 0.0.0.3 area 2
MEDELLIN1(config-router)#network 172.29.6.8 0.0.0.3 area 2
MEDELLIN1(config-router)#network 172.29.6.0 0.0.0.3 area 2
```

#### Configuración del protocolo OSPF en el router MEDELLIN2

```
MEDELLIN2#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN2(config)#route ospf 1
MEDELLIN2(config-router)#router-id 2.2.2.2
MEDELLIN2(config-router)#network 172.29.4.0 0.0.0.127 area 2
MEDELLIN2(config-router)#network 172.29.6.0 0.0.0.3 area 2
MEDELLIN2(config-router)#network 172.29.6.4 0.0.0.3 area 2
```

#### Configuración del protocolo OSPF en el router MEDELLIN3

```
MEDELLIN3#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN3(config)#route ospf 1
MEDELLIN3(config-router)#router-id 1.1.1.1
MEDELLIN3(config-router)#network 172.29.4.0 0.0.0.127 area 2
MEDELLIN3(config-router)#network 172.29.6.4 0.0.0.3 area 2
MEDELLIN3(config-router)#network 172.29.6.8 0.0.0.3 area 2
MEDELLIN3(config-router)#network 172.29.6.12 0.0.0.3 area 2
```

#### Configuración del protocolo OSPF en el router BOGOTA1

```
BOGOTA1#confi t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA1(config)#route ospf 1
BOGOTA1(config-router)#router-id 5.5.5.5
BOGOTA1(config-router)#network 209.17.220.4 0.0.0.3 area 1
BOGOTA1(config-router)#network 209.17.3.0 0.0.0.3 area 4
BOGOTA1(config-router)#network 172.29.3.4 0.0.0.3 area 4
```

```
BOGOTA1(config-router)#network 172.29.3.8 0.0.0.3 area 4
```

Configuración del protocolo OSPF en el router BOGOTA3

```
BOGOTA3#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
BOGOTA3(config)#route ospf 1
```

```
BOGOTA3(config-router)#router-id 7.7.7.7
```

```
BOGOTA3(config-router)#network 172.29.1.0 0.0.0.255 area 4
```

```
BOGOTA3(config-router)#network 172.29.3.8 0.0.0.3 area 4
```

```
BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 4
```

Configuración del protocolo OSPF en el router BOGOTA2

```
BOGOTA2#enable
```

```
BOGOTA2#config t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
BOGOTA2(config)#route ospf 1
```

```
BOGOTA2(config-router)#router-id 6.6.6.6
```

```
BOGOTA2(config-router)#network 172.29.0.0 0.0.0.255 area 4
```

```
BOGOTA2(config-router)#network 172.29.3.0 0.0.0.3 area 4
```

```
BOGOTA2(config-router)#network 172.29.3.4 0.0.0.3 area 4
```

```
BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3 area 4
```

## B. CONFIGURAR RUTA POR DEFECTO AL ISP PARA LOS ROUTERS BOGOTA1 Y MEDELLIN1

Los routers Bogota1 y Medellín1 deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF

Comandos para el router MEDELLIN1 y BOGOTA1

```
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.10
```

```
BOGOTA11(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
```

## C. RUTA ESTATICA DEL ISP HACIA LA REDES BOGOTA Y MEDELLIN

El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se sumarizan las subredes de cada uno a /22

```
Comando para establecer las rutas estáticas del ISP
ISP(config)#ip route 172.29.4.0 255.255.252.0 S0/0/0
ISP(config)#ip route 172.29.0.0 255.255.252.0 S0/0/1
ISP(config)#ip route 172.29.4.128 255.255.255.128 S0/0/0
ISP(config)#ip route 172.29.1.0 255.255.255.0 S0/0/1
```

## PARTE 2: TABLA DE ENRUTAMIENTO.

### A. TABLA DE ENRUTAMIENTO DE LA RED

Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas

Tabla 23. Enrutamiento

Router	Puerto	IP de red	IP de puerto	Mascara	Clock Rate
ISP	S0/0/1	209.17.220.4/30	209.17.220.5	255.255.255.252	
Bogota1	S0/0/1	209.17.220.4/30	209.17.220.6	255.255.255.252	1
Bogota1	S0/0/0	172.29.3.0/30	172.29.3.1	255.255.255.252	
Bogota2	S0/0/0	172.29.3.0/30	172.29.3.2	255.255.255.252	1
Bogota1	S0/1/1	172.29.3.4/30	172.29.3.5	255.255.255.252	
Bogota2	S0/1/1	172.29.3.4/30	172.29.3.6	255.255.255.252	1
Bogota1	S0/1/0	172.29.3.8/30	172.29.3.9	255.255.255.252	1
Bogota3	S0/1/0	172.29.3.8/30	172.29.3.10	255.255.255.252	
Bogota2	S0/0/1	172.29.3.12/30	172.29.3.13	255.255.255.252	
Bogota3	S0/0/1	172.29.3.12/30	172.29.3.14	255.255.255.252	1
Bogota2	G0/0	172.29.0.0/24	172.29.0.1	255.255.255.0	

Bogota3	G0/0	172.29.1.0/24	172.29.1.1	255.255.255.0	
Medellin1	S0/0/0	209.17.220.0/30	209.17.220.9	255.255.255.252	
ISP	S0/0/0	209.17.220.0/30	209.17.220.10	255.255.255.252	1
Medellin1	S0/1/0	172.29.6.0/30	172.29.6.1	255.255.255.252	1
Medellin2	S0/1/0	172.29.6.0/30	172.29.6.2	255.255.255.252	
Medellin1	S0/0/1	172.29.6.8/30	172.29.6.9	255.255.255.252	
Medellin3	S0/0/1	172.29.6.8/30	172.29.6.10	255.255.255.252	1
Medellin1	S0/1/1	172.29.6.12/30	172.29.6.13	255.255.255.252	
Medellin3	S0/1/1	172.29.6.12/30	172.29.6.14	255.255.255.252	1
Medellin2	S0/0/0	172.29.6.4/30	172.29.6.5	255.255.255.252	1
Medellin3	S0/0/0	172.29.6.4/30	172.29.6.6	255.255.255.252	
Medellin2	G0/0	172.29.4.0/25	172.29.4.1	255.255.255.128	
Medellin3	G0/0	172.29.4.128/25	172.29.4.129	255.255.255.128	

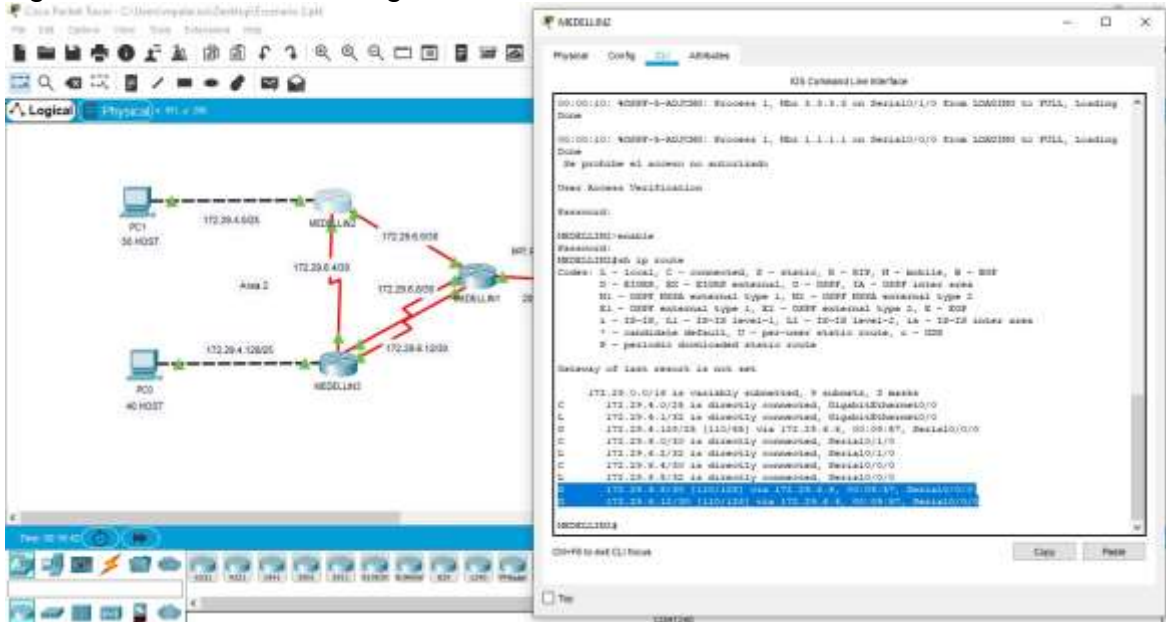
Fuente: propia

## B. BALANCEO DE CARGA DE LA RED

Verificar el balanceo de carga que presentan los routers

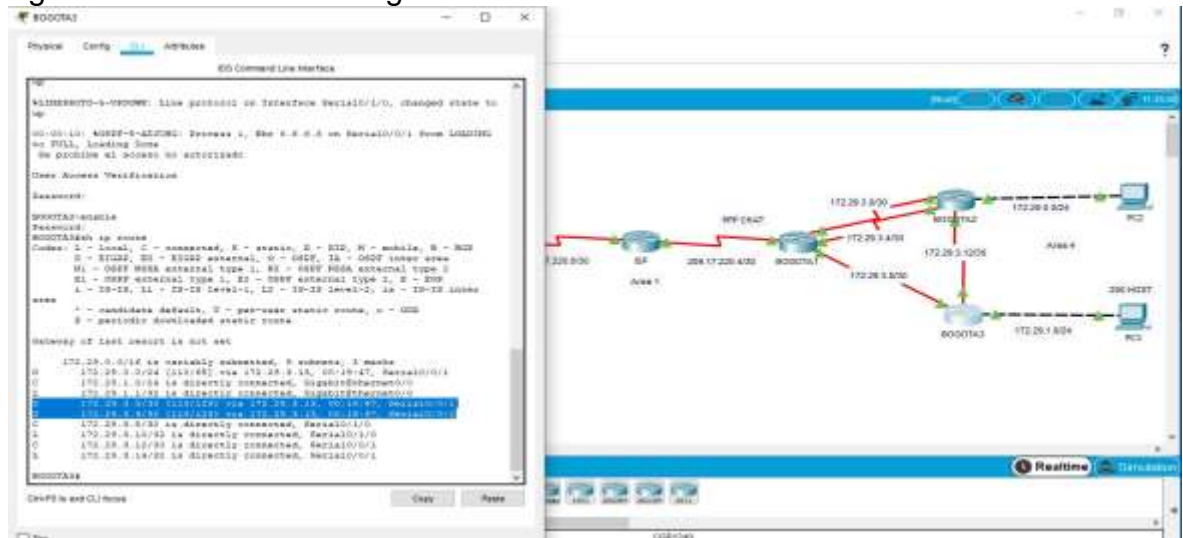
Digitando el comando show ip route se puede visualizar el balanceo de carga

Figura 17. Balanceo de carga MEDELLIN3



Fuente: propia

Figura 18. Balanceo de carga BOGOTA3

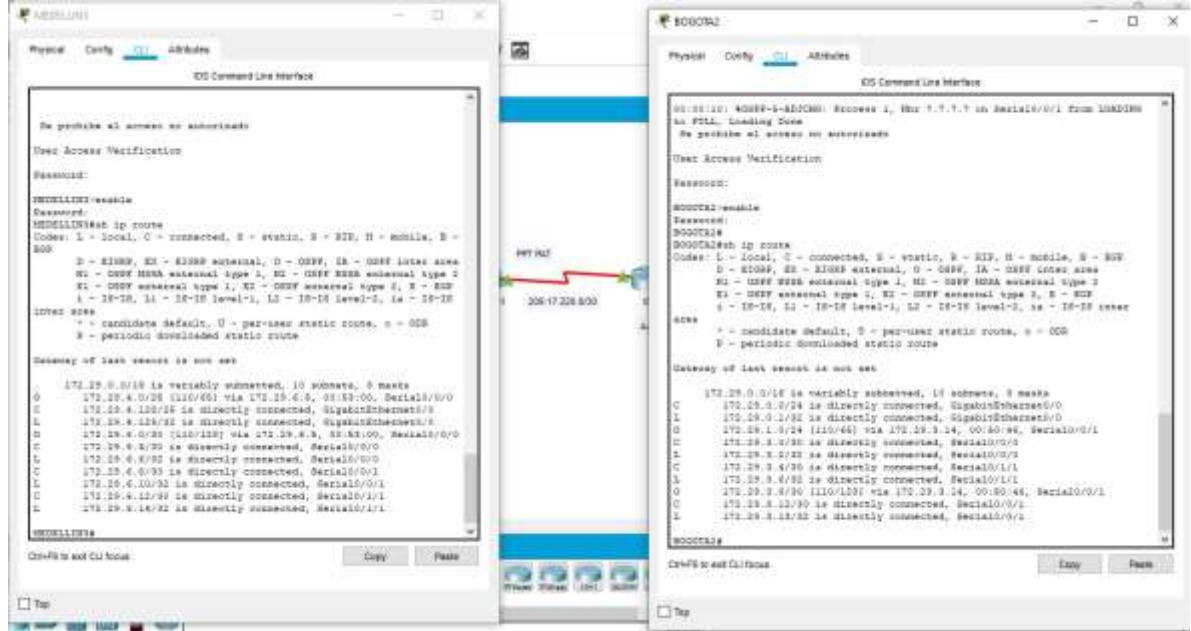


Fuente: propia





Figura 20. Rutas conectadas en los BOGOTA2 y MEDELLIN3



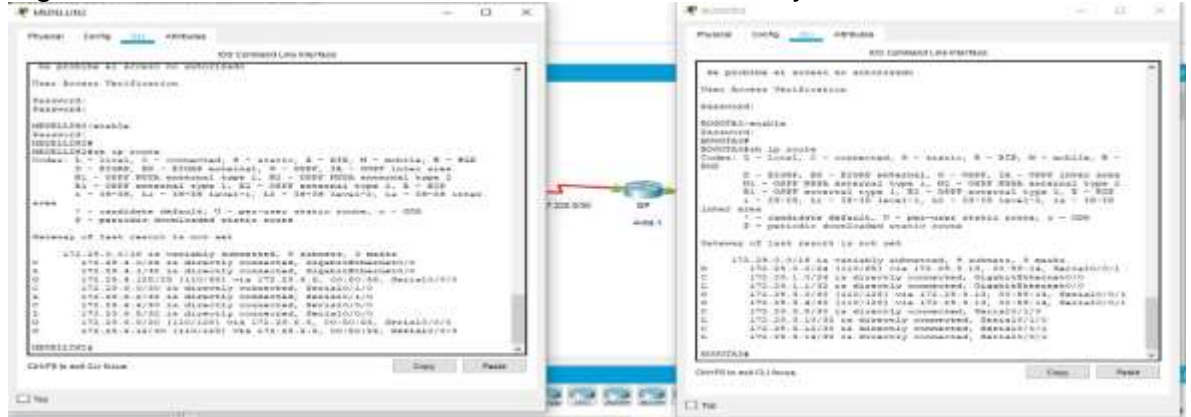
Fuente: propia

## LAS TABLAS RUTA POR DEFECTO ROUTERS RESTANTES.

Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto

Con el comando show ip route se puede visualizar la información solicitada

Figura 21. Rutas conectadas en los routers BOGOTA3 y MEDELLIN2



Fuente: propia



Tabla 24. De interfaces activas

<b>ROUTER</b>	<b>INTERFAZ</b>
<b>Bogota1</b>	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1
<b>Bogota2</b>	SERIAL0/0/0; SERIAL0/0/1
<b>Bogota3</b>	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
<b>Medellín1</b>	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/1
<b>Medellín2</b>	SERIAL0/0/0; SERIAL0/0/1
<b>Medellín3</b>	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
<b>ISP</b>	No lo requiere

Fuente: ejercicio

Comando para deshabilitar la propagación de OSPF en cada uno de los routers de la red

Para la red de Medellín

MEDELLIN2#config t

Enter configuration commands, one per line. End with CNTL/Z.

MEDELLIN2(config)#route ospf 1

MEDELLIN2(config-router)#passive-interface G0/0

MEDELLIN3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

MEDELLIN3(config)#route ospf 1

MEDELLIN3(config-router)#passive-interface G0/0

MEDELLIN1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

MEDELLIN1(config)#route ospf 1

MEDELLIN1(config-router)#passive-interface S0/0/0

Para la red de Bogota

BOGOTA1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

BOGOTA1(config)#route ospf 1

BOGOTA1(config-router)#passive-interface S0/0/1

```
BOGOTA2#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA2(config)#route ospf 1
BOGOTA2(config-router)#passive-interface G0/0
```

```
BOGOTA3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA3(config)#route OSPF 1
BOGOTA3(config-router)#passive-interface G0/0
```

#### PARTE 4: VERIFICACIÓN DEL PROTOCOLO OSPF.

##### A. VERIFICAR Y DOCUMENTAR LAS OPCIONES DE ENRUTAMIENTO OSPF EN LA RED

Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos

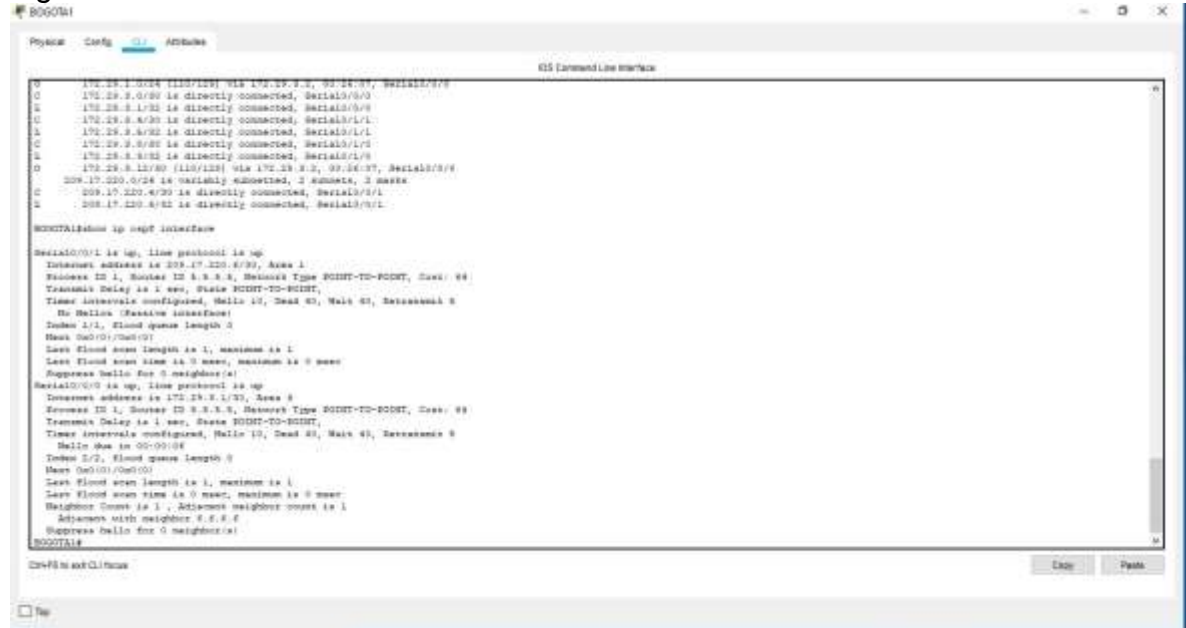
Utilizando los comandos show ip route y show ip ospf interface se puede visualizar la información solicitada.

Figura 23. Información OSPF router MEDELLIN1



Fuente: propia

Figura 24. Información OSPF router MEDELLIN1



Fuente: propia

**B. VERIFICAR Y DOCUMENTAR LA BASE DE DATOS DE OSPF DE CADA ROUTER**

Verificar y documentar la base de datos de OSPF de cada router, donde se informa de manera detallada de todas las rutas hacia cada red

Con el comando `do sh ip route connected` se puede visualizar la información solicitada

Para la red de Bogotá

```
BOGOTA1(config)#route ospf 1
BOGOTA1(config-router)#do sh ip route connected
C 172.29.3.0/30 is directly connected, Serial0/0/0
C 172.29.3.4/30 is directly connected, Serial0/1/1
C 172.29.3.8/30 is directly connected, Serial0/1/0
C 209.17.220.4/30 is directly connected, Serial0/0/1
```

BOGOTA3#config t

Enter configuration commands, one per line. End with CNTL/Z.

```
BOGOTA3(config)#route ospf 1
BOGOTA3(config-router)#do sh ip route connected
C 172.29.1.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.8/30 is directly connected, Serial0/1/0
C 172.29.3.12/30 is directly connected, Serial0/0/1
```

BOGOTA2#config t

Enter configuration commands, one per line. End with CNTL/Z.

```
BOGOTA2(config)#route ospf 1
BOGOTA2(config-router)#do sh ip route connected
C 172.29.0.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.0/30 is directly connected, Serial0/0/0
```

Para el ISP

ISP#conf t

Enter configuration commands, one per line. End with CNTL/Z.

```
ISP(config)#route ospf 1
ISP(config-router)#do sh ip route connected
C 209.17.220.0/30 is directly connected, Serial0/0/0
C 209.17.220.4/30 is directly connected, Serial0/0/1
```

Para la red de Medellín

```
MEDELLIN1#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
MEDELLIN1(config)#route ospf 1
```

```
MEDELLIN1(config-router)#do sh ip route connected
```

```
C 172.29.6.0/30 is directly connected, Serial0/1/0  
C 172.29.6.8/30 is directly connected, Serial0/0/1  
C 172.29.6.12/30 is directly connected, Serial0/1/1  
C 209.17.200.0/30 is directly connected, Serial0/0/0
```

```
MEDELLIN2#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
MEDELLIN2(config)#route ospf 1
```

```
MEDELLIN2(config-router)#do sh ip route connected
```

```
C 172.29.4.0/25 is directly connected, GigabitEthernet0/0  
C 172.29.6.0/30 is directly connected, Serial0/1/0  
C 172.29.6.4/30 is directly connected, Serial0/0/0
```

```
MEDELLIN3#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
MEDELLIN3(config)#route ospf 1
```

```
MEDELLIN3(config-router)#do sh ip route connected
```

```
C 172.29.4.128/25 is directly connected, GigabitEthernet0/0  
C 172.29.6.4/30 is directly connected, Serial0/0/0  
C 172.29.6.8/30 is directly connected, Serial0/0/1  
C 172.29.6.12/30 is directly connected, Serial0/1/1
```

## PARTE 5: CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP.

### A. AUTENTICACIÓN PAT ENLACE MEDELIN

Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT

Los comandos que se utilizan para activar este servicio son

```
Hostname MEDELLIN1
Username ISP password cisco
int S0/0/0
encapsulation ppp
ppp authentication pap
ppp pap sent-username ISP password cisco
```

Los comandos que se utilizan para activar este servicio son:

```
Hostname ISP
Username ISP password cisco
int S0/0/0
encapsulation ppp
ppp authentication pap
ppp pap sent-username ISP password cisco
```

## B. CONFIGURAR CON AUTENTICACIÓN CHAT BOGOTA1

El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT

Comandos para configurar el servicio de CHAT en el router BOGOTA1

```
hostname BOGOTA1
Username ISP password cisco
int S0/0/1
encapsulation ppp
ppp authentication chap
```

Comandos para configurar el servicio de CHAT en el router ISP

```
hostname ISP
Username BOGOTA1 password cisco
int S0/0/1
encapsulation ppp
ppp authentication chap
```







## Configuración para el router BOGOTA1

```
BOGOTA1(config-if)#ip nat inside source list 1 interface S0/0/1 overload
BOGOTA1(config-if)#Access-list 1 permit 172.29.0.0 0.0.3.255
BOGOTA1(config-if)#int S0/0/1
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#int S0/0/0
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int S0/1/0
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int S0/1/1
BOGOTA1(config-if)#ip nat inside
```

## PARTE 7: CONFIGURACIÓN DEL SERVICIO DHCP.

### A. CONFIGURAR ROUTER MEDELLÍN2 Y MEDELLÍN3, MEDELLÍN2 SERVIDOR DHCP PARA AMBAS REDES LAN.

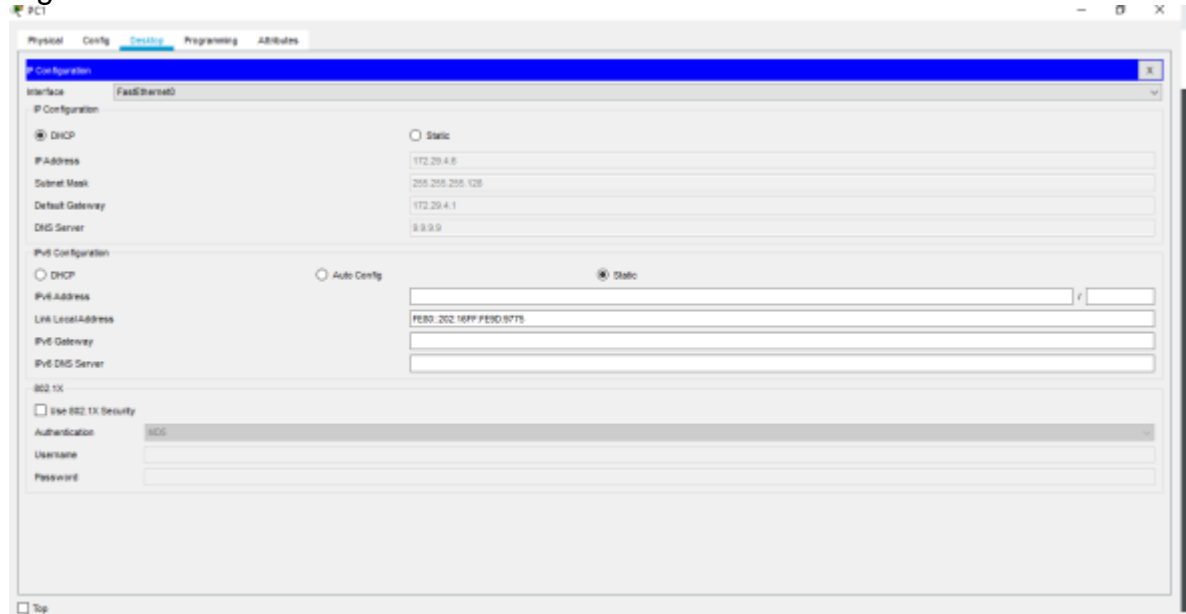
Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan

Configuración DHCP router MEDELLIN2 como servidor entre las redes MEDELLIN3 y MEDELLIN2

```
MEDELLIN2#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.5
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.133
MEDELLIN2(config)#ip dhcp pool MEDELLIN2
MEDELLIN2(dhcp-config)#Network 172.29.4.0 255.255.255.128
MEDELLIN2(dhcp-config)#Default-router 172.29.4.1
MEDELLIN2(dhcp-config)#Dns-server 9.9.9.9
MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#ip dhcp pool MEDELLIN3
```

```
MEDELLIN2(dhcp-config)#Network 172.29.4.128 255.255.255.128
MEDELLIN2(dhcp-config)#Default-router 172.29.4.129
MEDELLIN2(dhcp-config)#Dns-server 9.9.9.9
```

Figura 27. Evidencia servicio DHCP red Medellín



Fuente: propia

## B. EL ROUTER MEDELLÍN3 DEBERÁ HABILITAR EL PASO DE LOS MENSAJES BROADCAST HACIA LA IP DEL ROUTER MEDELLÍN2

Comando para activar el servicio de mensajes de broadcast hacia la IP del router MEDELLIN2

```
MEDELLIN3#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN3(config)#int G0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.5
MEDELLIN3(config-if)#exit
```

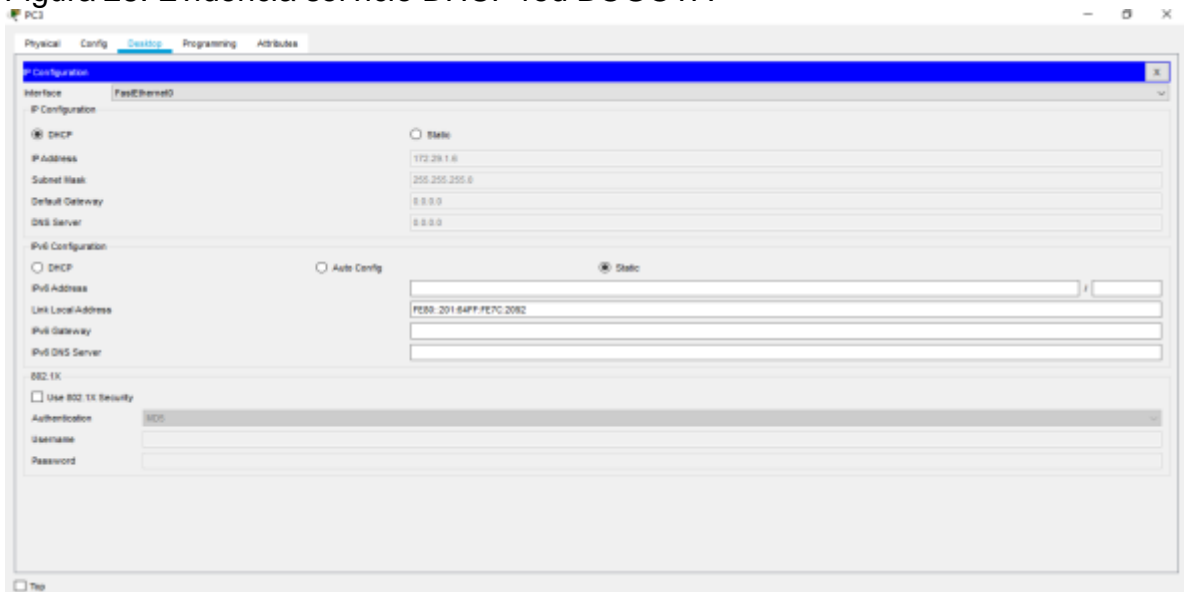
### C. CONFIGURAR BOGOTÁ2 Y BOGOTÁ3, BOGOTA2 SERVIDOR DHCP PARA LA LAN

Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan

Configuración DHCP router BOGOTA3 como servidor entre las redes BOGOTA2 y BOGOTA3

```
BOGOTA3#confi t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA3(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5
BOGOTA3(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.5
BOGOTA3(config)#ip dhcp pool BOGOTA3
BOGOTA3(dhcp-config)#Network 172.29.1.0 255.255.255.0
BOGOTA3(dhcp-config)#Default-router 172.29.0.1
BOGOTA3(dhcp-config)#Dns-server 9.9.9.9
BOGOTA3(dhcp-config)#exit
BOGOTA3(config)#ip dhcp pool BOGOTA2
BOGOTA3(dhcp-config)#Network 172.29.0.1 255.255.255.0
BOGOTA3(dhcp-config)#Default-router 172.29.0.1
BOGOTA3(dhcp-config)#Dns-server 9.9.9.9
BOGOTA3(dhcp-config)#
BOGOTA3(dhcp-config)#exit
```

Figura 28. Evidencia servicio DHCP red BOGOTA



Fuente: propia

#### D. CONFIGURE BOGOTÁ1 PARA QUE HABILITE EL PASO DE LOS DE BROADCAST HACIA BOGOTÁ2

Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

```
BOGOTA2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA2(config)#int G0/0
BOGOTA2(config-if)#ip helper-address 172.29.3.14
BOGOTA2(config-if)#exit
```

## CONCLUSIONES

En el desarrollo de esta actividad se pudo avanzar en el comprensión, solución e implementación de redes cisco a partir de dos escenarios, en el escenario uno en el cual trata sobre una red LAN con conexión entrante y saliente hacia Internet, se trataron conceptos desde lo más básico que fue la configuración elemental de los routers y switches, la correcta escogencia del cableado, tipo de conexiones físicas, puertos, configuración de puertos, configuración e implementación de direccionamiento IPv4 e IPv6 para redes públicas y privadas, la implementación de redes y subredes, se implementó el protocolo de routing dinámico acorde a la necesidad, se pudo solucionar el requerimiento de la configuración de la seguridad en los dispositivos de la red, logrando así una correcta comunicación entre cada una de los dispositivos a nivel de la cada de red correspondiente.

El segundo escenario es una propuesta de dos redes LAN en dos de sus routers con redes redundantes, interconectadas por medio de Internet las cuales necesitan establecer comunicación entrante y saliente entre sí, se implementó un servicio de routing de mayor complejidad, logrando así que los routers de cada red se pudieran comunicar, se utilizó un sistema de seguridad en los routers más avanzado, se pudo lograr la comunicación entre las dos redes

Después de terminados ambas actividades se lograron las competencias técnicas necesarias para la solución e implementación de rede datos tipo cisco, la utilización de los comandos y configuraciones necesarias para diseñar e implementar soluciones integrales en redes cisco a nivel LAN Y WAN

## REFERENCIA BIBLIOGRÁFICA

HOGG, Scott. CCNA routing and switching ICND2 200-105. Indianapolis: Editorial CISCO Press, 2017. 1452p.

LAMMLE, Todd. CCNA routing and switching. Indianapolis: Editorial Csybex, 2013. 408p.

LUCAS, Michael. Cisco routers for the desperate router and switch management. San Francisco: Editorial No Starch Press, 2009. 148p.

MACFARLANE, James. Network routing basics: understanding ip routing in cisco systems. INDIANÁPOLIS: Editorial Wiley, 2006. 159p.

WENDELL, Odon. CCENT/CCNA ISND1 100-105. Indianapolis: Editorial Csybex, 2016. 116p.